INFORMATION SECURITY TRAINING

SANS 2018
Orlando, Florida | April 3-10

Protect Your Business | Advance Your Career
More than 45 hands-on, immersion-style courses taught by real-world practitioners

See inside for courses offered in:
- Cyber Defense
- Detection & Monitoring
- Penetration Testing
- Ethical Hacking
- Digital Forensics
- Security Management
- SIEM
- Audit | Legal
- Secure Development
- Incident Response
- Critical Security Controls
- Cyber Threat Intelligence

“SANS is the best information security training you’ll find anywhere. World-class instructors, hands-on instruction, actionable information you can really use, and...NetWars!”

-Jeff Stebelton, Netjets, Inc., a Division of Berkshire Hathaway

SAVE $400
Register and pay by Feb 7th
Use code EarlyBird18

www.sans.org/sans-2018
Dear Colleagues,

Attacks and breaches continue to be on the rise, and by now most of us have been directly affected by them one way or another. For example, a recent wave of ransomware called “Petya,” fueled by exploits allegedly leaked from an intelligence agency, cost a shipping company $300 million. Once in, Petya can move laterally via stolen credentials, just like penetration testers do.

The bad news is that this model, now proven to be successful, is likely to be copied by other types of malware. The good news is that you can stop it.

There is no service, appliance, or “shiny box” that can mitigate this threat, but defense in-depth can do it.

There are many layers to defense in-depth, but the most critical layer is you. Time and again the difference between success and failure often isn’t a product or a service; it’s the right people in the right places making the right decisions, with the right knowledge and experience, backed by supportive management.

Information security is continually evolving from the perspective of both the red team (offense), blue team (defense), forensics, management, auditing, software development, legal issues, industrial controls, and much more. Success in information security requires a commitment to a career of learning everything from the fundamentals to advanced techniques.

SANS provides the best information and software security training available, and it is my pleasure to announce that SANS 2018 will return to Orlando, Florida from April 3-10 with cutting-edge courses taught by leading industry professionals. I invite you to take this amazing opportunity to learn actionable steps that will have an impact on security, protect your enterprise, and help build your career.

SANS 2018 is one of our largest events worldwide, with more than 45 information security courses taught by SANS’s top instructors. Many of the courses prepare you for the prestigious GIAC certification. You’ll hear about the latest and most important issues facing the industry at our SANS@Night talks by SANS practitioners who are leading the global conversation on cybersecurity. And there will be numerous other opportunities to learn new skills, techniques, and trends at the vendor expo, lunch-and-learn sessions, and by networking with your fellow cybersecurity professionals.

SANS wants to teach you to become better at what you do, help you be that “right person in the right place,” and enable you and your organization to more effectively battle the growing wave of breaches and cyber attacks. I hope you can join me at SANS 2018 for these many exciting opportunities. Please visit www.sans.org/sans-2018 to review the full course list and conference details. Register soon to receive an early bird discount!

I look forward to seeing you in Orlando for SANS 2018!

Eric Conrad

P.S. Remember that your live, hands-on SANS training can also be applied towards a Graduate Certificate or Master’s Degree in Information Security Management or Engineering at the SANS Technology Institute (www.sans.edu).
<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC301</td>
<td>Intro to Information Security</td>
<td>12</td>
</tr>
<tr>
<td>SEC401</td>
<td>Security Essentials Bootcamp Style</td>
<td>8</td>
</tr>
<tr>
<td>SEC440</td>
<td>Critical Security Controls: Planning, Implementing, and Auditing</td>
<td>14</td>
</tr>
<tr>
<td>SEC501</td>
<td>Advanced Security Essentials – Enterprise Defender</td>
<td>P 89</td>
</tr>
<tr>
<td>SEC503</td>
<td>Intrusion Detection In-Depth</td>
<td>16</td>
</tr>
<tr>
<td>SEC504</td>
<td>Hacker Tools, Techniques, Exploits, and Incident Handling</td>
<td>10</td>
</tr>
<tr>
<td>SEC505</td>
<td>Securing Windows and PowerShell Automation</td>
<td>18</td>
</tr>
<tr>
<td>SEC506</td>
<td>Securing Linux/Unix</td>
<td>20</td>
</tr>
<tr>
<td>SEC511</td>
<td>Continuous Monitoring and Security Operations</td>
<td>22</td>
</tr>
<tr>
<td>SEC524</td>
<td>Cloud Security Fundamentals</td>
<td>P 90</td>
</tr>
<tr>
<td>SEC542</td>
<td>Web App Penetration Testing and Ethical Hacking</td>
<td>36</td>
</tr>
<tr>
<td>SEC566</td>
<td>Implementing and Auditing the Critical Security Controls – In-Depth</td>
<td>28</td>
</tr>
<tr>
<td>SEC555</td>
<td>SIEM with Tactical Analytics</td>
<td>26</td>
</tr>
<tr>
<td>SEC560</td>
<td>Network Penetration Testing and Ethical Hacking</td>
<td>34</td>
</tr>
<tr>
<td>SEC564</td>
<td>Red Team Operations and Threat Emulation</td>
<td>38</td>
</tr>
<tr>
<td>SEC573</td>
<td>Automating Information Security with Python</td>
<td>40</td>
</tr>
<tr>
<td>SEC575</td>
<td>Mobile Device Security and Ethical Hacking</td>
<td>42</td>
</tr>
<tr>
<td>SEC580</td>
<td>Metasploit Kung Fu for Enterprise Pen Testing</td>
<td>P 90</td>
</tr>
<tr>
<td>SEC599</td>
<td>Defeating Advanced Adversaries – Implementing Kill Chain Defenses</td>
<td>30</td>
</tr>
<tr>
<td>SEC600</td>
<td>Advanced Exploit Development for Penetration Tests</td>
<td>50</td>
</tr>
<tr>
<td>FOR500</td>
<td>Windows Forensic Analysis</td>
<td>52</td>
</tr>
<tr>
<td>FOR508</td>
<td>Advanced Digital Forensics, Incident Response, and Threat Hunting</td>
<td>60</td>
</tr>
<tr>
<td>FOR518</td>
<td>Mac Forensic Analysis</td>
<td>56</td>
</tr>
<tr>
<td>FOR526</td>
<td>Memory Forensics In-Depth</td>
<td>62</td>
</tr>
<tr>
<td>FOR572</td>
<td>Advanced Network Forensics and Analysis</td>
<td>58</td>
</tr>
<tr>
<td>FOR578</td>
<td>Cyber Threat Intelligence</td>
<td>66</td>
</tr>
<tr>
<td>FOR585</td>
<td>Advanced Smartphone Forensics</td>
<td>68</td>
</tr>
<tr>
<td>FOR610</td>
<td>Reverse-Engineering Malware: Malware Analysis Tools and Techniques</td>
<td>70</td>
</tr>
<tr>
<td>MGT415</td>
<td>A Practical Introduction to Cybersecurity Risk Management</td>
<td>76</td>
</tr>
<tr>
<td>MGT433</td>
<td>Securing The Human: How to Build, Maintain, and Measure a High-Impact Awareness Program</td>
<td>P 91</td>
</tr>
<tr>
<td>MGT512</td>
<td>SANS Security Leadership Essentials for Managers with Knowledge Compression™</td>
<td>74</td>
</tr>
<tr>
<td>MGT514</td>
<td>IT Security Strategic Planning, Policy, and Leadership</td>
<td>78</td>
</tr>
<tr>
<td>MGT517</td>
<td>Managing Security Operations: Detection, Response, and Intelligence</td>
<td>80</td>
</tr>
<tr>
<td>MGT525</td>
<td>IT Project Management, Effective Communication, and PMP® Exam Prep</td>
<td>82</td>
</tr>
<tr>
<td>MGT533</td>
<td>Physical Security Specialist – Full Comprehensive Edition</td>
<td>84</td>
</tr>
<tr>
<td>DEV531</td>
<td>Defending Mobile Applications Security Essentials</td>
<td>86</td>
</tr>
<tr>
<td>DEV540</td>
<td>Secure DevOps and Cloud Application Security</td>
<td>87</td>
</tr>
<tr>
<td>DEV544</td>
<td>Secure Coding in .NET: Developing Defensible Applications</td>
<td>88</td>
</tr>
<tr>
<td>AUD507</td>
<td>Auditing &amp; Monitoring Networks, Perimeters, and Systems</td>
<td>92</td>
</tr>
<tr>
<td>LEG523</td>
<td>Law of Data Security and Investigations</td>
<td>P 91</td>
</tr>
<tr>
<td>HOSTED</td>
<td>Physical Access Control Systems: Elements of Design, Offense, and Defense</td>
<td>P 92</td>
</tr>
<tr>
<td>Core</td>
<td>NetWars Experience</td>
<td>32</td>
</tr>
<tr>
<td>Cyber Defense</td>
<td>NetWars Tournament</td>
<td>32</td>
</tr>
<tr>
<td>DFIR</td>
<td>NetWars Tournament</td>
<td>32</td>
</tr>
</tbody>
</table>

**For an up-to-date course list, please check the website at**

[www.sans.org/event/sans-2018/schedule](http://www.sans.org/event/sans-2018/schedule)
# Training Roadmap | Choose Your Path

## Baseline Skills

You are experienced in technology, but need to learn hands-on, essential security skills and techniques

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Certification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC401</td>
<td>Security Essentials</td>
<td>GSEC Certification</td>
<td>Security Essentials (p. 8)</td>
</tr>
<tr>
<td>SEC504</td>
<td>Secure Bootcamp Style</td>
<td>GCxH Certification</td>
<td>Secure Bootcamp Style, Techniques, Exploits, and Incident Handling (p. 10)</td>
</tr>
</tbody>
</table>

You will be responsible for managing security teams or implementations, but you do not require hands-on skills

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Certification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGT152</td>
<td>SANS Security Leadership Essentials for Managers with Knowledge Compression™</td>
<td>GSLC Certification</td>
<td>SANS Security Leadership Essentials (p. 74)</td>
</tr>
<tr>
<td>SEC666</td>
<td>Implementing and Auditing the Critical Security Controls – In-Depth</td>
<td>GCCC Certification</td>
<td>Critical Security Controls (p. 28)</td>
</tr>
</tbody>
</table>

## Core Security Techniques

Defend & Maintain

Every security professional should know the defense-in-depth techniques taught in SEC401, and SEC504 completes the “offense informs defense” preparation that teaches defense specialists how attacks occur and how to respond. If you’ve got the core defense skills, start with SEC504.

## Focus Job Roles

You are experienced in security, preparing for a specialized job role or focus

### Security Monitoring & Detection

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Certification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC503</td>
<td>Intrusion Detection – In-Depth</td>
<td>GCIJA Certification</td>
<td>Certified Intrusion Analyst (p. 16)</td>
</tr>
<tr>
<td>SEC511</td>
<td>Continuous Monitoring and Security Operations</td>
<td>GMON Certification</td>
<td>Continuous Monitoring (p. 22)</td>
</tr>
</tbody>
</table>

### Penetration Testing & Vulnerability Analysis

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Certification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC560</td>
<td>Network Penetration Testing and Ethical Hacking</td>
<td>GPEN Certification</td>
<td>Penetration Tester (p. 34)</td>
</tr>
<tr>
<td>SEC562</td>
<td>Web Application Penetration Testing</td>
<td>GWAPT Certification</td>
<td>Web Application Penetration Tester (p. 36)</td>
</tr>
</tbody>
</table>

### Incident Response & Threat Hunting

Specializing? Take FOR508 before FOR506

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Certification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FOR508</td>
<td>Advanced Digital Forensics, Incident Response, and Threat Hunting</td>
<td>GCFCA Certification</td>
<td>Forensics Analyst (p. 56)</td>
</tr>
<tr>
<td>FOR572</td>
<td>Advanced Network Forensics and Analysis</td>
<td>GNFA Certification</td>
<td>Network Forensic Analyst (p. 58)</td>
</tr>
</tbody>
</table>

## Crucial Skills, Specialized Roles

You are a candidate for specialized or advanced training

### Cyber Defense Operations

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC505</td>
<td>Securing Windows and PowerShell Automation</td>
<td></td>
</tr>
<tr>
<td>SEC506</td>
<td>Securing Linux/Unix</td>
<td></td>
</tr>
<tr>
<td>SEC545</td>
<td>Cloud Security Architecture and Operations</td>
<td></td>
</tr>
<tr>
<td>SEC555</td>
<td>SIEM with Tactical Analytics</td>
<td></td>
</tr>
<tr>
<td>SEC566</td>
<td>Implementing and Auditing the Critical Security Controls – In-Depth</td>
<td></td>
</tr>
<tr>
<td>SEC579</td>
<td>Virtualization and Software-Defined Security</td>
<td></td>
</tr>
<tr>
<td>SEC599</td>
<td>Defeating Advanced Adversaries – Implementing Kill Chain Defenses</td>
<td></td>
</tr>
</tbody>
</table>

### Penetration Testing & Ethical Hacking

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC460</td>
<td>Enterprise Threat and Vulnerability Assessment</td>
<td></td>
</tr>
<tr>
<td>SEC550</td>
<td>Active Defense, Offensive Countermeasures and Cyber Deception</td>
<td></td>
</tr>
<tr>
<td>SEC561</td>
<td>Immersive Hands-On Hacking Techniques</td>
<td></td>
</tr>
<tr>
<td>SEC573</td>
<td>Automating Information Security with Python</td>
<td></td>
</tr>
<tr>
<td>SEC575</td>
<td>Mobile Device Security and Ethical Hacking</td>
<td></td>
</tr>
</tbody>
</table>

### Digital Forensics, Malware Analysis & Threat Intel

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FOR500</td>
<td>Windows Forensic Analysis</td>
<td></td>
</tr>
<tr>
<td>FOR550</td>
<td>Mac Forensic Analysis</td>
<td></td>
</tr>
<tr>
<td>FOR526</td>
<td>Memory Forensics In-Depth</td>
<td></td>
</tr>
<tr>
<td>FOR578</td>
<td>Cyber Threat Intelligence</td>
<td></td>
</tr>
<tr>
<td>FOR585</td>
<td>Advanced Smartphone Forensics</td>
<td></td>
</tr>
<tr>
<td>FOR610</td>
<td>Reverse-Engineering Malware: Malware Analysis Tools and Techniques</td>
<td></td>
</tr>
</tbody>
</table>

### Software Security

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEV522</td>
<td>Defending Web Applications Security Essentials</td>
<td></td>
</tr>
<tr>
<td>DEV540</td>
<td>Secure DevOps and Cloud Application Security</td>
<td></td>
</tr>
<tr>
<td>DEV541</td>
<td>Secure Coding in Java/JEE</td>
<td></td>
</tr>
<tr>
<td>DEV544</td>
<td>Secure Coding in .NET</td>
<td></td>
</tr>
</tbody>
</table>

### Management

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGT144</td>
<td>IT Security Strategic Planning, Policy, and Leadership</td>
<td></td>
</tr>
<tr>
<td>MGT157</td>
<td>Managing Security Operations: Detection, Response, and Intelligence</td>
<td></td>
</tr>
<tr>
<td>MGT255</td>
<td>IT Project Management, Effective Communication, and PMI® Exam Prep</td>
<td></td>
</tr>
</tbody>
</table>

### Audit | Legal

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUS507</td>
<td>Auditing &amp; Monitoring Networks, Perimeters, and Systems</td>
<td></td>
</tr>
<tr>
<td>SEC566</td>
<td>Implementing and Auditing the Critical Security Controls – In-Depth</td>
<td></td>
</tr>
<tr>
<td>LEG523</td>
<td>Law of Data Security and Investigations</td>
<td></td>
</tr>
</tbody>
</table>

## New to Cybersecurity?

If you are new to cybersecurity, consider these course options:

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Description</th>
</tr>
</thead>
</table>
| SEC301      | Intro to Information Security | | GISP Certification (Information Security Fundamentals (p. 12))

www.sans.org/roadmap
SANS World-Class Instructors

For instructor bios, visit: www.sans.org/event/sans-2018/instructors

SANS instructors are real-world practitioners who specialize in the subjects they teach. All instructors undergo rigorous training and testing in order to teach SANS courses. This guarantees that what you learn in class will be up to date and relevant to your job. The lineup of instructors for SANS 2018 includes:

Mark Baggett
Senior Instructor
@MarkBaggett
Teaching SEC573

Eric Conrad
Senior Instructor
@eric_conrad
Teaching MGT414

Christopher Crowley
Principal Instructor
@CCrowMontance
Teaching MGT517

Adrien de Beaupre
Certified Instructor
@adriendb
Teaching SEC642

Ted Demopoulos
Principal Instructor
@TedDemop
Teaching MGT512

Russell Eubanks
Certified Instructor
@russelleubanks
Teaching SEC640

Jason Fossen
Faculty Fellow
@JasonFossen
Teaching SEC505

Bryce Galbraith
Principal Instructor
@brycegalbraith
Teaching SEC401 & SEC580

Philip Hagen
Certified Instructor
@PhilHagen
Teaching FOR572

Paul A. Henry
Senior Instructor
@phenrycissp
Teaching SEC505

David Hoelzer
Faculty Fellow
@it_audit
Teaching SEC503

Eric Johnson
Certified Instructor
@emjohn20
Teaching DEV540

Frank Kim
Certified Instructor
@fykim
Teaching MGT514

Gregory Leonard
Instructor
Teaching DEV531

Aaron Cure
Instructor
Teaching DEV544

Jeff Frisk
Certified Instructor
Teaching MGT525

Justin Henderson
Instructor
Teaching SEC555

Sarah Edwards
Certified Instructor
@iamevltwin
Teaching FOR518

Micah Hoffman
Certified Instructor
@WebBreacher
Teaching SEC567

Rob Lee
Faculty Fellow
@robtlee, @sansforensics
Teaching FOR508
James Lyne  
Certified Instructor  
@jameslyne  
Teaching SEC660

Heather Mahalik  
Senior Instructor  
@HeatherMahalik  
Teaching FOR585

Tim Medin  
Principal Instructor  
@timmedin  
Teaching SEC561

Seth Misenar  
Senior Instructor  
@sethmisenar  
Teaching SEC542

Keith Palmgren  
Senior Instructor  
@kpalmgren  
Teaching SEC301

Larry Pesce  
Certified Instructor  
@haxorthematrix  
Teaching SEC617

Hal Pomeranz  
Faculty Fellow  
@hal_pomeranz  
Teaching SEC506

Clay Risenhoover  
Certified Instructor  
@AuditClay  
Teaching AUD507

Dave Shackleford  
Senior Instructor  
@daveshackleford  
Teaching SEC545 & SEC524

Bryan Simon  
Certified Instructor  
@BryanOnSecurity  
Teaching SEC511

Stephen Sims  
Faculty Fellow  
@Steph3nSims  
Teaching SEC660

Ed Skoudis  
Faculty Fellow  
@edskoudis  
Teaching SEC560

Lance Spitzner  
Certified Instructor  
@lspitzner  
Teaching MGT433

John Strand  
Senior Instructor  
@strandjs  
Teaching SEC504

Peter Szczepankiewicz  
Certified Instructor  
@_s14  
Teaching FOR578

James Tarala  
Senior Instructor  
@isaudit  
Teaching SEC566 & MGT415

Chad Tilbury  
Senior Instructor  
@chadtilbury  
Teaching FOR500

Alissa Torres  
Certified Instructor  
@sibertor  
Teaching FOR526

Erik Van Buggenhout  
Certified Instructor  
@ErikVaBu  
Teaching SEC599

Joe Vest  
Instructor  
@joevest  
Teaching SEC564

Jake Williams  
Certified Instructor  
@MalwareJake  
Teaching SEC760

Benjamin Wright  
Senior Instructor  
@benjaminwright  
Teaching LEG523

Joshua Wright  
Senior Instructor  
@joswr1ght  
Teaching SEC575

Lenny Zeltser  
Senior Instructor  
@lennyzeltser  
Teaching FOR610

Register at www.sans.org/sans-2018  |  301-654-SANS (7267)
The SANS Institute’s mission is to deliver cutting-edge information security knowledge and skills to companies, military organizations, and governments in order to protect people and assets.

**CUTTING-EDGE TRAINING**

More than 55 unique courses are designed to align with dominant security team roles, duties, and disciplines. The courses prepare students to meet today’s threats and tomorrow’s challenges.

The SANS curriculum spans Cyber Defense, Digital Forensics & Incident Response, Threat Hunting, Audit, Management, Penetration Testing, Industrial Control Systems Security, Secure Software Development, and more. Each curriculum area offers a progression of courses that can take professionals from a subject’s foundations right up to top-flight specialization.

We constantly update and rewrite these courses to teach the most cutting-edge tools and techniques that are proven to keep networks safe.

Our training is designed to be practical. Students are immersed in hands-on lab exercises designed for them to practice, hone, and perfect what they’ve learned.

**LEARN FROM EXPERTS**

SANS courses are taught by an unmatched faculty of active security practitioners. Each instructor brings a wealth of real-world experience to every classroom – both live and online. SANS instructors work for high-profile organizations as red team leaders, CISOs, technical directors, and research fellows.

Along with their respected technical credentials, SANS instructors are also expert teachers. Their passion for the topics they teach shines through, making the SANS classroom dynamic and effective.

**WHY SANS IS THE BEST TRAINING AND EDUCATIONAL INVESTMENT**

SANS immersion training is intensive and hands-on, and our courseware is unrivaled in the industry.

SANS instructors and course authors are leading industry experts and practitioners. Their real-world experience informs their teaching and training content. SANS training strengthens a student’s ability to achieve a GIAC certification.

**THE SANS PROMISE**

At the heart of everything we do is the SANS Promise: Students will be able to use the new skills they’ve learned as soon as they return to work.

**SANS FORMATS**

The most popular option to take SANS training is to attend a 5- or 6-day technical course taught live in a classroom at one of our 200+ training events held around the world throughout the year. SANS training events provide an ideal learning environment and offer the chance to network with other security professionals, as well as SANS instructors and staff.

SANS training can also be delivered online, with several convenient options to suit your learning style. All SANS online courses include at least four months of access to the course material anytime and anywhere, enabling students to revisit and rewind content.

**HOW TO REGISTER FOR SANS TRAINING**

Students can learn more and register online by visiting [www.sans.org](http://www.sans.org)
The foundation of a successful career in information security – whether technical or managerial – should be comprehensive and rooted in real-world expertise. Learn more about the SANS courses and certifications recommended for baseline skills below and on the pages that follow in this catalog.

**Summary:** Every hands-on technical professional should possess the baseline set of knowledge and skills taught in SEC401 and SEC504. These courses cover the essentials of defense-in-depth, the mental model for how attacks work, and the proven methods for handling incidents when they occur.

**Who This Path Is For:** Hands-on technical professionals such as network administrators and engineers, security analysts, and consultants who need well-rounded and effective baseline security skills.

**Why This Training Is Important:** This training gives you essential knowledge and understanding about how a variety of attacks occur and how to respond to them.

“The focus on methodologies was superb because the techniques taught are applicable to every environment regardless of the tools utilized.”

—Conrad Bovell, DSS

“Excellent resources for defense! Attackers’ perspectives are realistic and real-world scenarios are relevant.”

—Nathan P., U.S. Air Force
This course will teach you the most effective steps to prevent attacks and detect adversaries with actionable techniques you can directly apply when you get back to work. You’ll learn tips and tricks from the experts so you can win the battle against the wide range of cyber adversaries that want to harm your environment.

STOP and ask yourself the following questions:

▷ Do you fully understand why some organizations get compromised and others do not?
▷ If there were compromised systems on your network, are you confident that you would be able to find them?
▷ Do you know the effectiveness of each security device and are you certain they are all configured correctly?
▷ Are proper security metrics set up and communicated to your executives to drive security decisions?

If you do not know the answers to these questions, SEC401 will provide the information security training you need in a bootcamp-style format that is reinforced with hands-on labs.

Learn to build a security roadmap that can scale today and into the future.

SEC401: Security Essentials Bootcamp Style is focused on teaching you the essential information security skills and techniques you need to protect and secure your organization’s critical information assets and business systems. Our course will show you how to prevent your organization’s security problems from being headline news in the Wall Street Journal!

Prevention is ideal but detection is a must.

With the rise in advanced persistent threats, it is almost inevitable that organizations will be targeted. Whether the attacker is successful in penetrating an organization’s network depends on the effectiveness of the organization’s defense. Defending against attacks is an ongoing challenge, with new threats emerging all of the time, including the next generation of threats. Organizations need to understand what really works in cybersecurity. What has worked, and will always work, is taking a risk-based approach to cyber defense. Before your organization spends a dollar of its IT budget or allocates any resources or time to anything in the name of cybersecurity, three questions must be answered:

▷ What is the risk?  ▷ Is it the highest priority risk?  ▷ What is the most cost-effective way to reduce the risk?

Security is all about making sure you focus on the right areas of defense. In SEC401 you will learn the language and underlying theory of computer and information security. You will gain the essential and effective security knowledge you will need if you are given the responsibility for securing systems and/or organizations. This course meets both of the key promises SANS makes to our students: (1) You will learn up-to-the-minute skills you can put into practice immediately upon returning to work; and (2) You will be taught by the best security instructors in the industry.

“It covered a lot of material that is directly applicable to the duties for my new (and first!) InfoSec job. I have already applied knowledge in the two days back in the office after SEC401 boot camp.”

-Tracy Maleeff, GSK

Bryce Galbraith  SANS Principal Instructor
As a contributing author to the internationally bestselling book Hacking Exposed: Network Security Secrets & Solutions, Bryce helped bring the secret world of hacking out of the darkness and into the public eye. Bryce has held security positions at global ISPs and Fortune 500 companies, was a member of Foundstone’s renowned penetration testing team, and served as a senior instructor and co-author of Foundstone’s Ultimate Hacking: Hands-On course series. Bryce is currently the owner of Layered Security, where he provides specialized vulnerability assessment and penetration testing services for clients. He teaches several of the SANS Institute’s most popular courses and develops curriculum around current topics. He has taught the art of ethical hacking and countermeasures to thousands of IT professionals from a who’s who of top companies, financial institutions, and government agencies around the globe. Bryce is an active member of several security-related organizations, holds several security certifications, and speaks at conferences around the world. @brycegalbraith
Course Day Descriptions

401.1 HANDS ON: **Network Security Essentials**
A key way that attackers gain access to a company’s resources is through a network connected to the Internet. A company wants to try to prevent as many attacks as possible, but in cases where it cannot prevent an attack, it must detect it in a timely manner. Therefore, an understanding and ability to create and identify the goals of building a defensible network architecture are critical. It is just as important to know and understand the architecture of the system, types of designs, communication flow and how to protect against attacks using devices such as routers and firewalls. These essentials, and more, will be covered during 401.1, in order to provide a firm foundation for the consecutive days of training.

**Topics:** Defensible Network Architecture; Virtualization and Cloud Security; Network Device Security; Networking and Protocols; Securing Wireless Networks; Securing Web Communications

401.2 HANDS ON: **Defense-In-Depth and Attacks**
To secure an enterprise network, you must understand the general principles of network security. In 401.2, we look at threats to our systems and take a “big picture” look at how to defend against them. You will learn that protections need to be layered: a principle called defense-in-depth. We explain some principles that will serve you well in protecting your systems. You will also learn about key areas of network security.

**Topics:** Defense-in-Depth; Access Control and Password Management; Security Policies; Critical Controls; Malicious Code and Exploit Mitigations; Advanced Persistent Threat (APT)

401.3 HANDS ON: **Threat Management**
Whether targeting a specific system or just searching the Internet for an easy target, an attacker uses an arsenal of tools to automate finding new systems; mapping out networks; and probing for specific, exploitable vulnerabilities. This phase of an attack is called reconnaissance, and it can be launched by an attacker any amount of time before exploiting vulnerabilities and gaining access to systems and networks. In fact, evidence of reconnaissance activity can be a clue that a targeted attack is on the horizon.

**Topics:** Vulnerability Scanning and Penetration Testing; Network Security Devices; Endpoint Security; SIEM/log management; Active Defense

401.4 HANDS ON: **Cryptography, Risk Management, and Response**
There is no silver bullet when it comes to security. However, there is one technology that would help solve a lot of security issues, though few companies deploy it correctly. This technology is cryptography. Concealing the meaning of a message can prevent unauthorized parties from reading sensitive information. Sec401.4 looks at various aspects of encryption and how it can be used to secure a company’s assets. A related area called steganography, or information hiding, is also covered.

**Topics:** Cryptography; Cryptography Algorithms and Deployment; Applying Cryptography; Incident Handling and Response; Contingency Planning – BCP/DRP; IT Risk Management

401.5 HANDS ON: **Windows Security**
Remember when Windows was simple? Windows XP desktops in a little workgroup... what could be easier? A lot has changed over time. Now, we have Windows tablets, Azure, Active Directory, PowerShell, Office 365, Hyper-V, Virtual Desktop Infrastructure (VDI), and so on. Microsoft is battling Google, Apple, Amazon.com, and other cloud giants for supremacy. The trick is to do it securely, of course. Windows is the most widely-used and targeted operating system on the planet. At the same time, the complexities of Active Directory, PKI, BitLocker, AppLocker, and User Account Control represent both challenges and opportunities. This section will help you quickly master the world of Windows security while showing you the tools that can simplify and automate your work. You will complete the day with a solid grounding in Windows security, by looking at automation, auditing and forensics.

**Topics:** Windows Security Infrastructure; Service Packs, Hot Fixes, and Backups; Windows Access Controls; Enforcing Security Policy; Securing Windows Network Services; Automation, Auditing, and Forensics

401.6 HANDS ON: **Linux Security**
While organizations do not have as many Unix/Linux systems, those that they do have are often some of the most critical systems that need to be protected. Sec401.6 provides step-by-step guidance to improve the security of any Linux system. The course combines practical “how to” instructions with background information for Linux beginners, as well as security advice and best practices for administrators of all levels of expertise. This module discusses the foundational items that are needed to understand how to configure and secure a Linux system. It also provides an overview of the operating system and mobile markets. To lay a foundation, it provides an overview of the different operating systems that are based on Linux.

**Topics:** Linux Security: Structure, Permissions and Access; Hardening and Securing Linux Services; Monitoring and Attack Detection; Security Utilities

---

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/event/sans-2018/courses](http://www.sans.org/event/sans-2018/courses)

---

“The SEC401 program covered recent events and current technologies. I came away feeling that SANS is a top-notch organization that I am proud to be affiliated with and I highly recommend it to everyone.”

-Harry Halikias, Sony/ATV Music Publishing
John Strand  SANS Senior Instructor

John Strand is the instructor and course author of SEC464: Hacker Detection for System Administrators, as well as the instructor of SEC560: Network Penetration Testing and Ethical Hacking. When not teaching for SANS, John co-hosts PaulDotCom Security Weekly, the world’s largest computer security podcast. He also is the owner of Black Hills Information Security, specializing in penetration testing and security architecture services. He has presented for the FBI, NASA, the NSA, and at DefCon. In his spare time he writes loud rock music and makes various futile attempts at fly fishing. @strandjs

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection and one or two disgruntled employees (and whose does not!), your computer systems will get attacked. From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets, attackers are targeting your systems with increasing viciousness and stealth. As defenders, it is essential we understand these hacking tools and techniques.

“The hands-on labs and the technical background about how attacks work in SEC504 are very insightful and show us how hackers operate.”
-Christopher Miller, Global Payments Inc.

This course enables you to turn the tables on computer attackers by helping you understand their tactics and strategies in detail, giving you hands-on experience in finding vulnerabilities and discovering intrusions, and equipping you with a comprehensive incident handling plan. It addresses the latest cutting-edge insidious attack vectors, the “oldie-but-goodie” attacks that are still prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course provides a time-tested, step-by-step process for responding to computer incidents, and a detailed description of how attackers undermine systems so you can prepare for, detect, and respond to them. In addition, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence. Finally, students will participate in a hands-on workshop that focuses on scanning, exploiting, and defending systems. This course will enable you to discover the holes in your system before the bad guys do!

The course is particularly well-suited to individuals who lead or are a part of an incident handling team. General security practitioners, system administrators, and security architects will benefit by understanding how to design, build, and operate their systems to prevent, detect, and respond to attacks.

“The tools provided in SEC504 are ready-to-use in the real world, and I can already see how I’ll be using and applying this course to my job.” -Jennifer Chavarria, Freeport LNG
### Course Day Descriptions

#### 504.1 Incident Handling Step-by-Step and Computer Crime Investigation

The first part of this section looks at the invaluable Incident Handling Step-by-Step Model, which was created through a consensus process involving experienced incident handlers from corporations, government agencies, and educational institutes, and has been proven effective in hundreds of organizations. This section is designed to provide students a complete introduction to the incident handling process, using the six steps (preparation, identification, containment, eradication, recovery, and lessons learned) necessary to prepare for and deal with a computer incident. The second part of this section examines from-the-trenches case studies to understand what does and does not work in identifying computer attackers. This section provides valuable information on the steps a systems administrator can take to improve the chances of catching and prosecuting attackers.

**Topics:** Preparation; Identification; Containment; Eradication; Recovery; Special Actions for Responding to Different Types of Incidents; Incident Record-Keeping; Incident Follow-Up

#### 504.2 Hands On: Computer and Network Hacker Exploits – Part 1

Seemingly innocuous data leaking from your network could provide the clue needed by an attacker to blow your systems wide open. This day-long course covers the details associated with reconnaissance and scanning, the first two phases of many computer attacks.

**Topics:** Reconnaissance; Scanning; Intrusion Detection System Evasion; Hands-on Exercises for a List of Tools

#### 504.3 Hands On: Computer and Network Hacker Exploits – Part 2

Computer attackers are ripping our networks and systems apart in novel ways while constantly improving their techniques. This course day covers the third phase of many hacker attacks – gaining access. Attackers employ a variety of strategies to take over systems from the network level up to the application level. This section covers the attacks in depth, from the details of buffer overflow and format string attack techniques to the latest in session hijacking of supposedly secure protocols.

**Topics:** Network-Level Attacks; Gathering and Parsing Packets; Operating System and Application-Level Attacks; Netcat: The Attacker’s Best Friend; Hands-on Exercises with a List of Tools

#### 504.4 Hands On: Computer and Network Hacker Exploits – Part 3

This course day starts out by covering one of attackers’ favorite techniques for compromising systems: worms. We will analyze worm developments over the last two years and project these trends into the future to get a feel for the coming Super Worms we will face. Then the course turns to another vital area often exploited by attackers: web applications. Because most organizations’ homegrown web applications do not get the security scrutiny of commercial software, attackers exploit these targets using SQL injection, cross-site scripting, session cloning, and a variety of other mechanisms discussed in detail.

**Topics:** Password Cracking; Web Application Attacks; Denial of Service Attacks; Hands-on Exercises with a List of Tools

#### 504.5 Hands On: Computer and Network Hacker Exploits – Part 4

This course day covers the fourth and fifth phases of many hacker attacks: maintaining access and covering their tracks. Computer attackers install backdoors, apply Rootkits, and sometimes even manipulate the underlying kernel itself to hide their nefarious deeds. Each of these categories of tools requires specialized defenses to protect the underlying system. In this course, we will analyze the most commonly used malicious code specimens, as well as explore future trends in malware, including BIOS-level and combo malware possibilities.

**Topics:** Maintaining Access; Covering the Tracks; Putting It All Together; Hands-on Exercises with a List of Tools

#### 504.6 Hands On: Hacker Tools Workshop

Over the years, the security industry has become smarter and more effective in stopping hackers. Unfortunately, hacker tools are becoming smarter and more complex. One of the most effective methods to stop the enemy is to actually test the environment with the same tools and tactics an attacker might use against you. This workshop lets you put what you have learned over the past week into practice.

**Topics:** Hands-on Analysis

---

#### You Will Be Able To

- Apply incident handling processes in-depth, including preparation, identification, containment, eradication, and recovery, to protect enterprise environments
- Analyze the structure of common attack techniques in order to evaluate an attacker’s spread through a system and network, anticipating and thwarting further attacker activity
- Utilize tools and evidence to determine the kind of malware used in an attack, including rootkits, backdoors, and trojan horses, choosing appropriate defenses and response tactics for each
- Use built-in command-line tools such as Windows tasklist, wmic, and reg as well as Linux netstat, ps, and lsof to detect an attacker’s presence on a machine
- Analyze router and system ARP tables along with switch CAM tables to track an attacker’s activity through a network and identify a suspect
- Use memory dumps and the Volatility tool to determine an attacker’s activities on a machine, the malware installed, and other machines the attacker used as pivot points across the network
- Gain access to a target machine using Metasploit, and then detect the artifacts and impacts of exploitation through process, file, memory, and log analysis
- Analyze a system to see how attackers use the Netcat tool to move files, create backdoors, and build relays through a target environment
- Run the Nmap port scanner and Nessus vulnerability scanner to find openings on target systems, and apply tools such as tcpdump and netstat to detect and analyze the impacts of the scanning activity
- Apply the tcpdump sniffer to analyze network traffic generated by a covert backdoor to determine an attacker’s tactics
- Employ the netstat and lsof tools to diagnose specific types of traffic-flooding denial-of-service techniques and choose appropriate response actions based on each attacker’s flood technique
- Analyze shell history files to find compromised machines, attacker-controlled accounts, sniffers, and backdoors
To determine if the SANS SEC301 course is right for you, ask yourself five simple questions:

▸ Do you have basic computer knowledge, but are new to information security and in need of an introduction to the fundamentals?

▸ Are you bombarded with complex technical security terms that you don’t understand?

▸ Are you a non-IT security manager (with some technical knowledge) who lays awake at night worrying that your company will be the next mega-breach headline story on the 6 o’clock news?

▸ Do you need to be conversant in basic security concepts, principles, and terms, even if you don’t need “deep in the weeds” detail?

▸ Have you decided to make a career change to take advantage of the job opportunities in information security and need formal training/certification?

If you answer yes to any of these questions, the SEC301: Intro to Information Security training course is for you. Jump-start your security knowledge by receiving insight and instruction from real-world security experts on critical introductory topics that are fundamental to information security. This completely revised, five-day comprehensive course covers everything from core terminology to the basics of computer networks, security policies, incident response, passwords, and even an introduction to cryptographic principles.

This course is designed for students who have a basic knowledge of computers and technology but no prior knowledge of cybersecurity. The hands-on, step-by-step teaching approach will enable you to grasp all of the information presented, even if some of the topics are new to you. You’ll learn the fundamentals of information security that will serve as the foundation of your InfoSec skills and knowledge for years to come.

Written by a security professional with over 30 years of experience in both the public and private sectors, SEC301 provides uncompromising real-world insight from start to finish. The course prepares you for the Global Information Security Fundamentals (GISF) certification test, as well as for the next course up the line, SEC401: Security Essentials Bootcamp Style. It also delivers on the SANS promise: You will be able to use the knowledge and skills you learn in SEC301 as soon as you return to work.

“The SEC301 course was an amazing foundation builder. I highly suggest this course be taken by anyone who has a position, or interest, involving information security.” -Melanie Berryhill, Security On-Demand
For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/sans-2018/courses

PART 1

301.1 HANDS ON: Security’s Foundation

Every good security practitioner and every good security program begins with the same mantra: learn the fundamentals. SEC301 starts by instilling familiarity with core security terms and principles. By the time you leave the classroom after the first day, you will fully understand the Principle of Least Privilege and the Confidentiality, Integrity, and Availability (CIA) Triad, and you’ll see why those principles drive all security discussions. You will be conversant in the fundamentals of risk management, security policy, and authentication/authorization/accountability.

301.2 HANDS ON: Computer Functions and Networking

This course day begins with an explanation of how computers handle numbers using decimal, binary, and hexadecimal numbering systems. It also provides an understanding of how computers encode letters using ASCII (American Standard Code for Information Interchange). We then spend the remainder of the day on networking. All attacks or exploits have one thing in common: they take something that exists for perfectly valid reasons and misuse it in malicious ways. Always! So as security practitioners, to grasp what is invalid we must first understand what is valid – that is, how things like networks are supposed to work. Only once we have that understanding can we hope to understand the mechanics of malicious misuse of those networks – and only with that knowledge can we understand how security devices such as firewalls seek to thwart those attacks. Day two begins with a non-technical explanation of how data move across a network. From there we move to fundamental terminology dealing with network types and standards. You’ll learn about common network hardware such as switches and routers, and you’ll finally grasp what is meant by terms like “protocol” and “encapsulation.” We’ll give a very basic introduction to network addressing and port numbers and then work our way up the Open Systems Interconnection (OSI) protocol stack, introducing more detail only as we proceed to the next layer. In other words, we explain networking starting in non-technical terms and gradually progress to more technical detail as students are ready to take the next step. By the end of our discussions, you’ll have a fundamental grasp of any number of critical technical networking acronyms that you’ve often heard and never quite understood: TCP/IP, IP, TCP, UDP, MAC, ARP, NAT, ICMP, and DNS.

301.3 HANDS ON: An Introduction to Cryptography

Cryptography is one of the most complex issues faced by security practitioners and should not be explained in passing, so we will spend some time on it. Not to worry, we won’t take you through the math behind cryptography, but we’ll look at basic crypto terminology and processes. What is steganography? What is substitution and transposition? What is a “work factor” in cryptography and why does it matter? What do we mean by symmetric and asymmetric key cryptography and “cryptographic hash,” and why do you need to know? How are those concepts used together in the real world to create cryptographic systems?

301.4 HANDS ON: Cybersecurity Technologies – PART 1

Our fourth day in the classroom begins our exploration of cybersecurity technologies. We begin with wireless network security (WiFi and Bluetooth), and mobile device security (i.e., cell phones). We follow that with a brief look at some common attacks. We then move into a discussion of malware and anti-malware technologies. From there, we move into a discussion of network security technologies and methods including compartmentalization, firewalls, intrusion detection and prevention systems, sniffers, content filters, and so on. We end the day with an examination of several data protection protocols used for email encryption, secure remote access, secure web access, secure file transfer, and Virtual Private Network technologies.

301.5 HANDS ON: Cybersecurity Technologies – PART 2

The final day of our SEC301 journey continues the discussion of cybersecurity technologies. The day begins by looking at the system security to include hardening operating systems, patching, virtual machines, cloud computing, and backup. We move to application security to learn about browser security and web security, as well as email and instant messaging concerns. We discuss competitive intelligence gathering methods and how you can defend against them. We close the course with an explanation of awareness training and social engineering so that students understand what it is and why it’s so difficult to defend against.

You Will Be Able To

- Communicate with confidence regarding information security topics, terms, and concepts
- Understand and apply the Principles of Least Privilege
- Understand and apply the Confidentiality, Integrity, and Availability (CIA) Triad
- Build better passwords that are more secure while also being easier to remember and type
- Grasp basic cryptographic principles, processes, procedures, and applications
- Gain an understanding of computer network basics
- Have a fundamental grasp of any number of critical technical networking acronyms: TCP/IP, IP, TCP, UDP, MAC, ARP, NAT, ICMP, and DNS
- Utilize built-in Windows tools to see your network settings
- Recognize and discuss various security technologies including anti-malware, firewalls, and intrusion detection systems
- Determine your “Phishing IQ” to more easily identify SPAM email messages
- Understand physical security issues and how they support cybersecurity
- Understand incident response, business continuity, and disaster recovery planning at an introductory level
- Access a number of websites to better understand password security, encryption, phishing, browser security, etc.

“This was my very first IT training and it was a very informative class. I highly recommend this course if you’re starting to build your career in information security.”

-CHRISTIAN MERCADO, CIM GROUP

Bundle OnDemand with this course

www.sans.org/on-demand
Effective cybersecurity is more important than ever as attacks become stealthier, have a greater financial impact, and cause broad reputational damage. SEC501: Advanced Security Essentials – Enterprise Defender builds on a solid foundation of core policies and practices to enable security teams to defend their enterprise.

It has been said of security that “prevention is ideal, but detection is a must.” However, detection without response has little value. Network security needs to be constantly improved to prevent as many attacks as possible and to swiftly detect and appropriately respond to any breach that does occur. This PREVENT - DETECT - RESPONSE strategy must be in place both externally and internally. As data become more portable and networks continue to be porous, there needs to be an increased focus on data protection. Critical information must be secured regardless of whether it resides on a server, in a robust network architecture, or on a portable device.

Of course, despite an organization’s best efforts to prevent network attacks and protect its critical data, some attacks will still be successful. Therefore, organizations need to be able to detect attacks in a timely fashion. This is accomplished by understanding the traffic that is flowing on your networks, looking for indications of an attack, and performing penetration testing and vulnerability analysis against your organization to identify problems and issues before a compromise occurs.

Finally, once an attack is detected we must react quickly and effectively and perform the forensics required. Knowledge gained by understanding how the attacker broke in can be fed back into more preventive and detective measures, completing the security lifecycle.

You Will Learn

- How to build a comprehensive security program focused on preventing, detecting, and responding to attacks
- Core components of building a defensible network infrastructure and how to properly secure routers, switches, and network infrastructure
- Methods to detect advanced attacks on systems that are currently compromised
- Formal methods for performing a penetration test to find weaknesses in an organization’s security apparatus
- How to respond to an incident using the six-step process of incident response: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned
- Approaches to analyzing malware, ranging from fully automated analysis to static properties analysis, behavioral analysis, and code analysis

Paul A. Henry  SANS Senior Instructor

Paul Henry is one of the world’s foremost global information security and computer forensic experts, with more than 20 years of experience managing security initiatives for Global 2000 enterprises and government organizations worldwide. Paul is a principal at vNet Security, LLC and is keeping a finger on the pulse of network security as the security and forensic analyst at Lumension Security. Throughout his career, Paul has played a key strategic role in launching new network security initiatives to meet our ever-changing threat landscape. He also advises and consults on some of the world’s most challenging and high-risk information security projects, including the National Banking System in Saudi Arabia, the Reserve Bank of Australia, the U.S. Department of Defense’s Satellite Data Project, and both government as well as telecommunications projects throughout Southeast Asia. Paul is frequently cited by mainstream and trade print publications as an expert on computer forensics, technical security topics, and general security trends and serves as an expert commentator for network broadcast outlets such as FOX, NBC, CNN, and CNBC. In addition, Paul regularly authors thought leadership articles on technical security issues, and his expertise and insight help shape the editorial direction of key security publications, such as the Information Security Management Handbook, to which he is a consistent contributor. Paul serves as a featured and keynote speaker at seminars and conferences worldwide, delivering presentations on diverse topics including anti-forensics, network access control, cyber crime, DDoS attack risk mitigation, firewall architectures, security architectures, and managed security services. @phenrycissp
Course Day Descriptions

501.1 HANDS ON: Defensive Network Architecture

Section 1 will focus on security in the design and configuration of various enterprise infrastructures. From a security perspective, proper design and configuration protects both the components being configured, as well as the rest of the organization that depends on that gear to defend other components from attacks. In other words, a good house needs a good foundation!

Topics: Security Benchmarks, Standards, and the Role of Audit in Defending Infrastructure; Defense Using Authentication and Authorization, and Defending Those Services; The Use of Logging and Security Information and Event Management (SIEM) in Defending an Organization from Attack; Attacking and Defending Critical Protocols; Several Man-in-the-Middle Attack Methods, and Defenses against Each; Infrastructure Defense Using IPS, Next-Generation Firewalls, and Web Application Firewalls; Defense of Critical Servers and Services; Active Defense; Defense of Private and Public Cloud Architectures

501.2 HANDS ON: Penetration Testing

Security is all about understanding, mitigating, and controlling the risk to an organization’s critical assets. An organization must understand the changing threat landscape and have the capacity to compare itself against its own vulnerabilities that could be exploited to compromise the environment. On day two, students will learn about the variety of tests that can be run against an organization and how to perform effective penetration tests to better understand the security posture for network services, operating systems, and applications. In addition, we’ll talk about social engineering and reconnaissance activities to better emulate increasingly prevalent threats to users.

Topics: Introduction to Penetration Testing Concepts; Penetration Testing Scoping and Rules of Engagement; Online Reconnaissance and Offensive Counterintelligence; Social Engineering; Network Mapping and Scanning Techniques; Enterprise Vulnerability Scanning; Network Exploitation Tools and Techniques; Web Application Exploitation Tools and Techniques; Post-Exploitation and Pivoting; OS and Application Exploit Mitigations; Reporting and Debriefing

501.3 HANDS ON: Network Detection and Packet Analysis

“Prevention is ideal, but detection is a must” is a critical motto for network security professionals. While organizations always want to prevent as many attacks as possible, some adversaries will still sneak into the network. In cases where an attack is not successfully prevented, network security professionals need to analyze network traffic to discover attacks in progress, ideally stopping them before significant damage is done. Packet analysis and intrusion detection are at the core of such timely detection. Organizations need to not only detect attacks but also to react in a way that ensures those attacks can be prevented in the future.

Topics: Network Security Monitoring; IP, TCP, and UDP Refresher; Advanced Packet Analysis; Introduction to Network Forensics with Security Onion; Identifying Malicious Content and Streams; Extracting and Repairing Content from PCAP files; Traffic Visualization Tools; Intrusion Detection and Intrusion Prevention; Handling Encrypted Network Traffic

501.4 HANDS ON: Digital Forensics and Incident Response

In this section, you will learn the core concepts of both “Digital Forensics” and “Incident Response.” We’ll explore some of the hundreds of artifacts that can give forensic investigators specific insight into what occurred during an incident. You will also learn how incident response currently operates, after years of evolving, in order to address the dynamic procedures used by attackers to conduct their operations. We’ll look at how to integrate DFIR practices into a continuous security operations program.

Topics: DFIR Core Concepts: Digital Forensics; DFIR Core Concepts: Incident Response; Modern DFIR: A Live and Continuous Process; Widening the Net: Scaling the DFIR Process and Scoping a Compromise

501.5 HANDS ON: Malware Analysis

Malicious software is responsible for many incidents in almost every type of organization. Types of Malware vary widely, from Ransomware and Rootkits to Crypto Currency Miners and Worms. We will define each of the most popular types of malware and walk through multiple examples. The four primary phases of malware analysis will be covered: Fully Automated Analysis; Static Properties Analysis; Interactive Behavior Analysis; and Manual Code Reversing. You will complete various in-depth labs requiring you to fully dissect a live Ransomware specimen from static analysis through code analysis. You will get hands-on experience with tripping the malware through behavioral analysis techniques, as well as decrypting files encrypted by Ransomware by extracting the keys through reverse engineering. All steps are well defined and tested to ensure that the process to achieve these goals is actionable and digestible.

Topics: Introduction to Malware Analysis; The Many Types of Malware; ATM/Cash Machine Malware; Building a Lab Environment for Malware Analysis; Malware Locations and Footprints; Fully Automated Malware; Cuckoo Sandbox; Static Properties Analysis; Interactive Behavior Analysis; Manual Code Reversing; Tools such as IDA, PeStudio, ILSpy, Process Hacker, Process Monitor, NoFuserEx, etc.

501.6 HANDS ON: Enterprise Defender Capstone

The concluding section of the course will serve as a real-world challenge for students by requiring them to work in teams, use the skills they have learned throughout the course, think outside the box, and solve a range of problems from simple to complex. A web server scoring system and Capture-the-Flag engine will be provided to score students as they submit flags to score points. More difficult challenges will be worth more points. In this defensive exercise, challenges include packet analysis, routing protocols, scanning, malware analysis, and other challenges related to the course material.
Reports of prominent organizations being hacked and suffering irreparable reputational damage have become all too common. How can you prevent your company from becoming the next victim of a major cyber attack?

Preserving the security of your site in today’s threat environment is more challenging than ever before. The security landscape is continually changing from what was once only perimeter protection to protecting exposed and mobile systems that are almost always connected and sometimes vulnerable. Security-savvy employees who can help detect and prevent intrusions are therefore in great demand. Our goal in SEC503: Intrusion Detection In-Depth is to acquaint you with the core knowledge, tools, and techniques to defend your networks with insight and awareness. The training will prepare you to put your new skills and knowledge to work immediately upon returning to a live environment.

Mark Twain said, “It is easier to fool people than to convince them that they’ve been fooled.” Too many IDS/IPS solutions provide a simplistic red/green, good/bad assessment of traffic and too many untrained analysts accept that feedback as the absolute truth. This course emphasizes the theory that a properly trained analyst uses an IDS alert as a starting point for examination of traffic, not as a final assessment. SEC503 imparts the philosophy that the analyst must have access and the ability to examine the alerts to give them meaning and context. You will learn to investigate and reconstruct activity to deem if it is noteworthy or a false indication.

SEC503: Intrusion Detection In-Depth delivers the technical knowledge, insight, and hands-on training you need to defend your network with confidence. You will learn about the underlying theory of TCP/IP and the most used application protocols, such as DNS and HTTP, so that you can intelligently examine network traffic for signs of an intrusion. You will get plenty of practice learning to master different open-source tools like tcpdump, Wireshark, Snort, Bro, tshark, and SiLK. Daily hands-on exercises suitable for all experience levels reinforce the course book material so that you can transfer knowledge to execution. Basic exercises include assistive hints, while advanced options provide a more challenging experience for students who may already know the material or who have quickly mastered new material.

David Hoelzer  SANS Faculty Fellow

David Hoelzer is a high-scoring SANS instructor and author of more than 20 sections of SANS courseware. He is an expert in a variety of information security fields, having served in most major roles in the IT and security industries over the past 25 years. Recently, David was called upon to serve as an expert witness for the Federal Trade Commission for ground-breaking GLBA Privacy Rule litigation. David has been highly involved in governance at the SANS Technology Institute, serving as a member of the Curriculum Committee as well as Audit Curriculum Lead. As a SANS instructor, David has trained security professionals from organizations including the NSA, DHHS, Fortune 500 companies, various Department of Defense sites, national laboratories, and many colleges and universities. David is a research fellow at the Center for Cybermedia Research, as well as the Identity Theft and Financial Fraud Research Operations Center (ITFF/ROC). He also is an adjunct research associate for the UNLV Cybermedia Research Lab and a research fellow with the Internet Forensics Lab. David has written and contributed to more than 15 peer-reviewed books, publications, and journal articles. Currently, David serves as the principal examiner and director of research for Enclave Forensics, a New York/Las Vegas-based incident response and forensics company. He also serves as the chief information security officer for Cyber-Defense, an open-source security software solution provider. In the past, David served as the director of the GIAC Certification program, bringing the GIAC Security Expert certification to life. David holds a B.S. in IT, Summa Cum Laude, having spent time either attending or consulting for Stony Brook University, Binghamton University, and American Intercontinental University.
Course Day Descriptions

503.1 HANDS ON: Fundamentals of Traffic Analysis – PART 1
Day 1 provides a refresher or introduction, depending on your background, to TCP/IP. It describes the need to understand packet structure and content. It covers the essential foundations such as the TCP/IP communication model, and the theory of bits, bytes, binary and hexadecimal. We introduce the use of open-source Wireshark and tcpdump for analysis. We begin our exploration of the TCP/IP communication model with the study of the link layer, the IP layer, both IPv4 and IPv6 and packet fragmentation in both. We describe the layers and analyze traffic not just in theory and function, but from the perspective of an attacker and defender. All traffic is discussed and displayed using the two open-source tools, Wireshark and tcpdump.

Topics: Concepts of TCP/IP; Introduction to Wireshark; Network Access/Link Layer: Layer 2; IP Layer: Layer 3

503.2 HANDS ON: Fundamentals of Traffic Analysis – PART 2
Day 2 continues where the previous day ended in understanding the TCP/IP model. Two essential tools, Wireshark and tcpdump, are further explored, using their advanced features to give you the skills to analyze your own traffic. The focus of these tools on Day 2 is filtering traffic of interest in Wireshark using display filters and in tcpdump using Berkeley Packet Filters. We proceed with our exploration of the TCP/IP layers covering TCP, UDP, and ICMP. Once again, we describe the layers and analyze traffic not just in theory and function, but from the perspective of an attacker and defender.

Topics: Wireshark Display Filters; Writing tcpdump Filters; TCP; UDP; ICMP

503.3 HANDS ON: Application Protocols and Traffic Analysis
Day 3 introduces the versatile packet crafting tool Scapy. It is a very powerful Python-based tool that allows for the manipulation, creation, reading, and writing of packets. Scapy can be used to craft packets to test the detection capability of an IDS/IPS, especially important when a new user-created IDS rule is added, for instance for a recently announced vulnerability. The examination of TCP/IP culminates with an exploration of the application protocol layer. The concentration is on some of the most widely used, and sometimes vulnerable, crucial application protocols: DNS, HTTP(S), SMTP, and Microsoft communications. Our focus is on protocol analysis, a key skill in intrusion detection. IDS/IPS evasions are the bane of the analyst, so the theory and possible implications of evasions at different protocol layers are examined.

Topics: Scapy; Advanced Wireshark; Detection Methods for Application Protocols; DNS; Microsoft Protocols; HTTP(2)/TLS; SMTP; IDS/IPS Evasion Theory

503.4 HANDS ON: Network Monitoring: Snort and Bro
The fundamental knowledge gained from the first three days provides a fluid progression into one of the most popular days of SEC503. Snort and Bro are widely deployed open-source IDS/IPS solutions that have been industry standards for many years. The day begins with a discussion of network architecture, including the features of intrusion detection and prevention devices, along with a look at options and requirements of devices that can sniff and capture the traffic for inspection. Next, the topic of the analyst’s role in the detection process is examined. Before Snort and Bro are discussed, the capabilities and limitations are considered. Snort detection flow, running Snort, and rules are explored with an emphasis on writing efficient rules. It is likely that false positives and negatives will occur and tips for dealing with them are presented. Bro’s unique capability to use its own scripting language to write code to analyze patterns of event-driven behavior is one of the most powerful detection tools available to the analyst. We discuss how this enables monitoring and correlating activity and demonstrate with examples.

Topics: Network Architecture; Introduction to IDS/IPS Analysis; Snort; Bro

503.5 HANDS ON: Network Traffic Forensics
The penultimate day continues the format of less instruction and more hands-on training using three separate incidents that must be analyzed. The three incident scenarios are introduced with some new material to be used in the related hands-on analysis. This material includes an introduction to network forensics analysis for the first scenario. It continues with using network flow records to assist in analysis of the traffic from the second scenario. It concludes with the third scenario where Command and Control channels are discussed and managed analysis when very large packet capture files are involved is examined.

Topics: Introduction to Network Forensics Analysis; Using Network Flow Records; Examining Command and Control Traffic; Analysis of Large pcaps

503.6 HANDS ON: NetWars: IDS Version
The week culminates with a fun hands-on NetWars: IDS Version challenge. Students compete on teams to answer many questions that require using tools and theory covered in the first five days. This is a great way to end the week because it reinforces what was learned by challenging the student to think analytically and strengthens confidence to employ what was learned in a real-world environment.
SEC505

Securing Windows and PowerShell Automation

Six-Day Program
Tue, April 3 - Sun, April 8
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Jason Fossen

Who Should Attend
- Security Operations personnel
- Blue Team players who were terrified by SEC504
- Windows endpoint and server administrators
- Anyone who wants to learn PowerShell automation
- Anyone implementing the NSA Top 10 Mitigations
- Anyone implementing the CIS Critical Security Controls
- DoD admins applying the NSA/DISA Secure Host Baseline
- Individuals deploying or managing a PKI or smart cards
- Anyone wanting a more rugged Windows architecture

Hackers know how to use PowerShell for evil. Do you know how to use it for good? In SEC505 you will learn PowerShell and Windows security hardening at the same time. SecOps/DevOps requires automation, and Windows automation means PowerShell.

You’ve run a vulnerability scanner and applied patches – now what? A major theme of this course is defensible architecture: we have to assume that there will be a breach, so we need to build in damage control from the beginning. Whack-a-mole incident response cannot be our only defensive strategy – we’ll never win, and we’ll never get ahead of the game. By the time your monitoring system tells you a Domain Admin account has been compromised, IT’S TOO LATE.

For the assume-breach mindset, we must carefully delegate limited administrative powers so that the compromise of one administrator account is not a disaster across the board. Managing administrative privileges and credentials is a tough problem, so this course devotes an entire day to just this one critical task. Perhaps you’ve taken a hacking course at SANS and you now want to learn Windows mitigations: SEC505 is that course. SEC505 is the defense-only mirror image of SEC504 with regard to Windows and Active Directory.

Learning PowerShell is also useful for another kind of security: job security. Employers are looking for people with these skills. You don’t have to know any PowerShell to attend the course, we will learn it together. About half the labs during the week are PowerShell, while the rest use graphical security tools. Many of the PowerShell scripts written by the course author are available to download from GitHub for free.

This course is not a vendor show to convince you to buy another security appliance or to install yet another endpoint agent. The idea is to use built-in or free Windows and Active Directory security tools when we can (especially PowerShell and Group Policy) and then purchase commercial products only when absolutely necessary.

If you are an IT manager or CIO, the aim for this course is to have it pay for itself 10 times over within two years, because automation isn’t just good for SecOps/DevOps; it can save money too.

This course is designed for systems engineers, security architects, and the Security Operations (SecOps) team. The focus of the course is on how to automate the NSA Top 10 Mitigations and the CIS Critical Security Controls related to Windows, especially the ones that are difficult to implement in large environments.

SEC505 will also prepare you for the GIAC Certified Windows Security Administrator (GCWN) certification exam to prove your Windows security expertise. The GCWN certification counts towards a Master’s Degree in Information Security from the SANS Technology Institute (www.sans.edu) and satisfies the Department of Defense 8140 computing environment requirement. The GCWN is also a foundational certification for soldiers in the U.S. Army’s 255-S Information Protection Program. For DoD students, we will see how to apply the NSA/DISA Secure Host Baseline.

This is a fun course and a real eye-opener, even for Windows administrators with years of experience. We don’t cover patch management, share permissions, or other such basics – the aim is to go far beyond that. Come have fun learning PowerShell and Windows security at the same time!

Jason Fossen  SANS Faculty Fellow

Jason Fossen is a principal security consultant at Enclave Consulting LLC, a published author, and a frequent public speaker on Microsoft security issues. He is the sole author of the SANS week-long Securing Windows course (SEC505), maintains the Windows day of Security Essentials (SEC401.5), and has been involved in numerous other SANS projects since 1998. He graduated from the University of Virginia, received his master’s degree from the University of Texas at Austin, and holds a number of professional certifications. He currently lives in Dallas, Texas.  @JasonFossen

Most excellent, content-packed, skill-enhancing course.”

- JESUS PEREZ, Texas A&M UNIVERSITY
505.1 HANDS ON: PowerShell Automation and Security
This course section covers what you need to know to get started using PowerShell. You don’t need to have any prior scripting or programming experience. We have PowerShell labs throughout the week, so today is not the only PowerShell material. We start with the essentials, then go more in depth as the week progresses. Don’t worry, you won’t be left behind, the PowerShell labs walk you through every step.

Topics: PowerShell Overview and Tips; What Can We Do With PowerShell?; Write Your Own Scripts

505.2 HANDS ON: Continuous Secure Configuration Enforcement
Running a vulnerability scanner is easy, but remediating vulnerabilities in a large enterprise is hard. Most vulnerabilities are fixed by applying patches, but this course does not talk about patch management, you’re doing that already. What about the other vulnerabilities, the ones not fixed by applying patches? These vulnerabilities are, by definition, remediated by configuration changes. That’s the hard part. We need a secure architecture designed for SecOps/DevOps.

Topics: Continuous Secure Configuration Enforcement; Group Policy Precision Targeting; Server Hardening for SecOps/DevOps; PowerShell Desired State Configuration (DSC)

505.3 HANDS ON: Windows Public Key Infrastructure and Smart Cards
Don’t believe what you hear on the street: Public Key Infrastructure (PKI) is not that hard to manage on Windows! You’ll be pleasantly surprised at how much Group Policy, Active Directory, and PowerShell can help you manage your PKI. And we don’t really have a choice anymore: running a PKI is pretty much mandatory for Microsoft security and cloud computing. This day of the course is basically one long hands-on lab to install and configure a full Windows Server PKI. This includes a root Certification Authority (CA), Group Policy certificate auto-enrollment on endpoints, Online Certificate Status Protocol (OCSP) revocation checking, private key roaming for users, smart card certificate deployment, and, of course, more PowerShell examples.

Topics: Why Is a PKI Necessary?; How to Install the Windows PKI; How to Manage Your PKI; Deploying Smart Cards

505.4 HANDS ON: Administrative Compromise and Privilege Management
Why do submarines have pressure doors to seal off compartments? Because they are designed to assume a breach will occur. In a Windows environment, a security breach will occur, so we must design the architecture with an “assume breach” mindset as well. If we assume that some day the computers and credentials of our administrators will be compromised, then how do we build damage control into the network from the beginning? This is not about detection and incident response. The challenge here is how to design for damage control when we delegate administrative privileges. We need to proactively design damage control into the architecture, not wait until after there is a breach (when it’s too late).

Topics: Secure Architecture: Admin Privileges; Compromise of Administrative Powers; PowerShell Just Enough Admin (JEA); Active Directory Permissions and Delegation

505.5 HANDS ON: Endpoint Protection and Pre-Forensics
You are already applying patches and updating anti-virus signatures. But endpoint protection is much more than that. Because most advanced malware infections start with a compromised endpoint, we want to proactively build defensibility and damage control into our systems using a “zero trust” or “assume breach” model. How? AppLocker is an application whitelisting tool built into Windows to control which executables, scripts, DLLs and installer packages users may run. If hackers or malware attempt to launch an unauthorized process post-exploitation, the aim is to block it and log it. In the lab, we’ll use PowerShell and Group Policy to manage AppLocker. Application whitelisting can be hard to manage if used too aggressively, so we’ll also talk about how to get started without making the help desk phone ring off the hook.

Topics: Anti-Exploitation; IPSec Port Permissions; Host-Based Firewalls; Pre-Forensics

505.6 HANDS ON: Defensible Networking and Blue Team WMI
Hackers love the Windows Management Instrumentation (WMI) service, and so should we. We are the linebackers on the Blue Team and the WMI service was made to benefit us, not hackers. The WMI service is enabled by default and accessible over the network. Through WMI we can do remote command execution (without PowerShell being installed at the target), forcibly log off the user, reboot the machine, stop services, search for processes running as Administrator, kill any process, and much more. The WMI service is nearly all-powerful and it’s built for remote administration. PowerShell is tightly integrated into WMI, and we’ll look at several PowerShell examples.

Topics: PowerShell and WMI; Hardening DNS; Dangerous Protocols We Can’t Live Without

You Will Be Able To
- Execute PowerShell commands on remote systems and begin to write your own PowerShell scripts
- Harden PowerShell itself against abuse, and enable transcription logging
- Use Group Policy to execute PowerShell scripts on an almost unlimited number of hosts, while using Group Policy Object permissions, organizational units, and Windows Management Instrumentation (WMI) to target just the systems that need the scripts run
- Use PowerShell Desired State Configuration (DSC) and Server Manager scripting for the sake of SecOps/DevOps automation of server hardening
- Assuming a breach will occur, use Group Policy and PowerShell to grant administrative privileges in a way that reduces the harm if an attack succeeds
- Configure PowerShell remoting to use Just Enough Admin (JEA) policies to create a Windows version of Linux sudo and setuid root
- Configure mitigations against attacks such as pass-the-hash, Kerberos golden tickets, Remote Desktop Protocol (RDP) man-in-the-middle, Security Access Token abuse, and other attacks discussed in some SANS hacking courses
- Use PowerShell and Group Policy to manage the Microsoft Enhanced Mitigation Experience Toolkit (EMET), AppLocker whitelisting rules, INF security templates, Windows Firewall rules, IPSec rules, and many other security-related settings
- Install and manage a full Windows Public Key Infrastructure (PKI), including smart cards, certificate auto-enrollment, Online Certificate Status Protocol (OCSP) web responders, and detection of spoofed root Certification Authorities (CAs)
- Harden SSL/TLS, RDP, DNS, and SMB against attacks, including deploying DNSSEC, DNS sinkholes for malware, SMB encryption, and TLS cipher suite optimization
- Use PowerShell with the WMI service, such as remote command execution, searching event logs, and doing a remote inventory of user applications

“This class provided real-world examples and sample scripts to make a Windows-centric environment fundamentally more secure.”

-Nick Boardman, HRSD
SEC506: Securing Linux/Unix provides in-depth coverage of Linux and Unix security issues that includes specific configuration guidance and practical, real-world examples, tips, and tricks. We examine how to mitigate or eliminate general problems that apply to all Unix-like operating systems, including vulnerabilities in the password authentication system, file system, virtual memory system, and applications that commonly run on Linux and Unix.

The course will teach you the skills to use freely available tools to handle security issues, including SSH, AIDE, sudo, lsol, and many others. SANS’s practical approach uses hand-on exercises every day to ensure that you will be able to use these tools as soon as you return to work. We will also put these tools to work in a special section that covers simple forensic techniques for investigating compromised systems.

Topics
- Memory Attacks, Buffer Overflows
- File System Attacks, Race Conditions
- Trojan Horse Programs and Rootkits
- Monitoring and Alerting Tools
- Unix Logging and Kernel-Level Auditing
- Building a Centralized Logging Infrastructure
- Network Security Tools
- SSH for Secure Administration
- Server Lockdown for Linux and Unix
- Controlling Root Access with sudo
- SELinux and chroot() for Application Security
- DNSSEC Deployment and Automation
- mod_security and Web Application Firewalls
- Secure Configuration of BIND, Sendmail, Apache
- Forensic Investigation

Course Author Statement
“A wise man once said, ‘How are you going to learn anything if you know everything already?’ And yet there seems to be a quiet arrogance in the Unix community that we have figured out all of our security problems, as if to say, ‘Been there, done that.’ All I can say is that what keeps me going in the Unix field, and the security industry in particular, is that there is always something new to learn, discover, or invent. In 20 plus years on the job, what I have learned is how much more there is that I can learn. I think this is also true for the students in my courses. I regularly get comments back from students who say things like, ‘I have been using Unix for 20 years, and I still learned a lot in this class.’ That is really rewarding.”

- Hal Pomeranz

Hal Pomeranz  SANS Faculty Fellow

Hal Pomeranz is an independent digital forensic investigator who has consulted on cases ranging from intellectual property theft to employee sabotage, organized cybercrime, and malicious software infrastructures. He has worked with law enforcement agencies in the United States and Europe and with global corporations. Equally at home in the Windows or Mac environment, Hal is recognized as an expert in the analysis of Linux and Unix systems. His research on EXT4 file system forensics provided a basis for the development of open-source forensic support for this file system. His EXT3 file recovery tools are used by investigators worldwide. Hal is a SANS Lethal Forensicator, and is the creator of the SANS Linux/Unix Security track (GCUX). He holds the GCFA and GREM certifications and teaches the related courses in the SANS Forensics curriculum. He is a respected author and speaker at industry gatherings worldwide. Hal is a regular contributor to the SANS Computer Forensics blog and co-author of the Command Line Kung Fu blog.  @hal_pomeranz
Course Day Descriptions

506.1 HANDS ON: Hardening Linux/Unix Systems – PART 1
This course day tackles some of the most important techniques for protecting your Linux/Unix systems from external attacks, and it also covers what those attacks are so that you know what you’re defending against. This is a full-disclosure course with in-class demos of actual exploits and hands-on exercises to experiment with various examples of malicious software, as well as different techniques for protecting Linux/Unix systems.
Topics: Memory Attacks and Overflows; Vulnerability Minimization; Boot-Time Configuration; Encrypted Access; Host-Based Firewalls

506.2 HANDS ON: Hardening Linux/Unix Systems – PART 2
Continuing our exploration of Linux/Unix security issues, this course day focuses on local exploits and access control issues. What do attackers do once they gain access to your systems? How can you detect their presence? How do you protect against attackers with physical access to your systems? What can you do to protect against mistakes (or malicious activity) by your own users?
Topics: Rootkits and Malicious Software; File Integrity Assessment; Physical Attacks and Defenses; User Access Controls; Root Access Control with sudo; Warning Banners; Kernel Tuning For Security

506.3 HANDS ON: Hardening Linux/Unix Systems – PART 3
Monitoring your systems is critical for maintaining a secure environment. This course day digs into the different logging and monitoring tools available in Linux/Unix, and looks at additional tools for creating a centralized monitoring infrastructure such as Syslog-NG. Along the way, the course introduces a number of useful SSH tips and tricks for automating tasks and tunneling different network protocols in a secure fashion.
Topics: Automating Tasks With SSH; AIDE via SSH; Linux/Unix Logging Overview; SSH Tunneling; Centralized Logging with Syslog-NG

506.4 HANDS ON: Application Security – PART 1
This course day examines common application security tools and techniques. The SCP-Only Shell will be presented as an example of using an application under chroot() restriction, and as a more secure alternative to file-sharing protocols like anonymous FTP. The SELinux application whitelisting mechanism will be examined in-depth. Tips for troubleshooting common SELinux problems will be covered and students will learn how to craft new SELinux policies from scratch for new and locally developed applications. Significant hands-on time will be provided for students to practice these concepts.
Topics: chroot() for Application Security; The SCP-Only Shell; SELinux Basics; SELinux and the Reference Policy

506.5 HANDS ON: Application Security – PART 2
This course section is a full day of in-depth analysis on how to manage some of the most popular application-level services securely on a Linux/Unix platform. We will tackle the practical issues involved with securing three of the most commonly used Internet servers on Linux and Unix: BIND, Sendmail, and Apache. Beyond basic security configuration information, we will take an in-depth look at topics like DNSSec and Web Application Firewalls with mod_security and the Core Rules.
Topics: BIND; DNSSec; Apache; Web Application Firewalls with mod_security

506.6 HANDS ON: Digital Forensics for Linux/Unix
This hands-on course is designed to be an information-rich introduction devoted to basic forensic principles and techniques for investigating compromised Linux and Unix systems. At a high level, it introduces the critical forensic concepts and tools that every administrator should know and provides a real-world compromise for students to investigate using the tools and strategies discussed in class.
Topics: Tools Throughout; Forensic Preparation and Best Practices; Incident Response and Evidence Acquisition; Media Analysis; Incident Reporting

You Will Be Able To
> Significantly reduce the number of vulnerabilities in the average Linux/Unix system by disabling unnecessary services
> Protect your systems from buffer overflows, denial-of-service, and physical access attacks by leveraging OS configuration settings
> Configure host-based firewalls to block attacks from outside.
> Deploy SSH to protect administrative sessions, and leverage SSH functionality to securely automate routine administrative tasks
> Use sudo to control and monitor administrative access
> Create a centralized logging infrastructure with Syslog-NG, and deploy log monitoring tools to scan for significant events
> Use SELinux to effectively isolate compromised applications from harming other system services
> Securely configure common Internet-facing applications such as Apache, BIND
> Investigate compromised Unix/Linux systems with the Sleuthkit, lsof, and other open-source tools
> Understand attacker rootkits and how to detect them with AIDE and rkhunter/chkrootkit

“Excellent class – well worth the time and money spent on attending SANS training.”
-Jon Speak, Trans Union

“This course has helped my understanding of Linux/Unix security. I especially liked the thoughts on what to do with things you collect.”
-Ben Biggs, Campbell Scientific

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/sans-2018/courses
Who Should Attend

- Security architects
- Senior security engineers
- Technical security managers
- Security Operations Center (SOC) analysts, engineers, and managers
- CND analysts
- Individuals working to implement Continuous Diagnostics and Mitigation (CDM), Continuous Security Monitoring (CSM), or Network Security Monitoring (NSM)

Continuous Monitoring and Security Operations

We continue to underestimate the tenacity of our adversaries! Organizations are investing significant time and financial and human resources to combat cyber threats and prevent cyber attacks, but despite this tremendous effort, organizations are still getting compromised. The traditional perimeter-focused, prevention-dominant approach to security architecture has failed to prevent intrusions. No network is impenetrable, which is a reality that business executives and security professionals alike have to accept. Prevention is crucial, and we can’t lose sight of it as the primary goal. However, a new proactive approach to security is needed to enhance the capabilities of organizations to detect threats that will inevitably slip through their defenses.

The underlying challenge for organizations victimized by an attack is timely incident detection. Industry data suggest that most security breaches typically go undiscovered for an average of seven months. Attackers simply have to find one way into most organizations, because they know that the lack of visibility and internal security controls will then allow them to methodically carry out their mission and achieve their goals.

The Defensible Security Architecture, Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/Continuous Security Monitoring (CSM) taught in this course will best position your organization or Security Operations Center (SOC) to analyze threats and detect anomalies that could indicate cybercriminal behavior. The payoff for this new proactive approach will be early detection of an intrusion, or successfully thwarting the efforts of attackers altogether. The National Institute of Standards and Technology (NIST) developed guidelines described in NIST SP 800-137 for Continuous Monitoring (CM), and this course will greatly increase your understanding and enhance your skills in implementing CM utilizing the NIST framework.

SEC511 will take you on quite a journey. We start by exploring traditional security architecture to assess its current state and the attacks against it. Next, we discuss and discover modern security design that represents a new proactive approach to such architecture that can be easily understood and defended. We then transition to how to actually build the network and endpoint security, and then carefully navigate our way through automation, NSM/CDM/CSM. For timely detection of potential intrusions, the network and systems must be proactively and continuously monitored for any changes in the security posture that might increase the likelihood that attackers will succeed.

Your SEC511 journey will conclude with one last hill to climb! The final day (Day 6) features a Capture-the-Flag competition that challenges you to apply the skills and techniques learned in the course to detect and defend the modern security architecture that has been designed. Course authors Eric Conrad and Seth Misenar have designed the Capture-the-Flag competition to be fun, engaging, comprehensive, and challenging. You will not be disappointed!

Bryan Simon  SANS Certified Instructor

Bryan Simon is an internationally recognized expert in cybersecurity who has been working in the information technology and security field since 1991. Over the course of his career, Bryan has held various technical and managerial positions in the education, environmental, accounting, and financial services sectors. Bryan speaks on a regular basis at international conferences and with the press on matters of cybersecurity. He has instructed individuals from the FBI, NATO, and the UN in matters of cybersecurity on two continents. Bryan has specialized expertise in defensive and offensive capabilities. He has received recognition for his work in IT security and was most recently profiled by McAfee (part of Intel Security) as an IT Hero. Bryan holds 13 GIAC Certifications including GSEC, GCWN, GCCH, GCFA, GPEN, GWAPT, GAWN, GISP, GCIA, GCED, GCUX, GISF, and GMON. Bryan’s scholastic achievements have resulted in the honor of sitting as a current member of the SANS Institute Advisory Board and in his acceptance into the prestigious SANS Cyber Guardian program. Bryan teaches SEC401: Security Essentials Bootcamp Style; SEC501: Advanced Security Essentials – Enterprise Defender; SEC505: Securing Windows and Powershell Automaton; and SEC511: Continuous Monitoring and Security Operations. @BryanOnSecurity
511.1 HANDS ON: **Current State Assessment, SOCs, and Security Architecture**

We begin with the end in mind by defining the key techniques and principles that will allow us to get there. An effective modern Security Operations Center (SOC) or security architecture must enable an organization’s ability to rapidly find intrusions to facilitate containment and response. Both significant knowledge and a commitment to continuous monitoring are required to achieve this goal.

**Topics:** Current State Assessment, SOCs, and Security Architecture; Modern Security Architecture Principles; Frameworks and Enterprise Security Architecture; Security Architecture – Key Techniques/Practices; Security Operations Center

511.2 HANDS ON: **Network Security Architecture**

Understanding the problems with the current environment and realizing where we need to get to is far from sufficient; we need a detailed roadmap to bridge the gap between the current and desired state. Day 2 introduces and details the components of our infrastructure that become part of a defensible network security architecture and SOC. We are long past the days when a perimeter firewall and ubiquitous antivirus were sufficient security. There are many pieces and moving parts that make up a modern defensible security architecture.

**Topics:** SOCs/Security Architecture – Key Infrastructure Devices; Segmented Internal Networks; Defensible Network Security Architecture Principles Applied

511.3 HANDS ON: **Network Security Monitoring**

Designing a SOC or security architecture that enhances visibility and detective capabilities represents a paradigm shift for most organizations. However, the design is simply the beginning. The most important element of a modern security architecture is the emphasis on detection. The network security architecture presented in days one and two emphasized baking visibility and detective capabilities into the design. Now we must figure out how to look at the data and continuously monitor the enterprise for evidence of compromise or changes that increase the likelihood of compromise.

**Topics:** Continuous Monitoring Overview; Network Security Monitoring (NSM); Practical NSM Issues; Cornerstone NSM

511.4 HANDS ON: **Endpoint Security Architecture**

One of the hallmarks of modern attacks is an emphasis on client-side exploitation. The days of breaking into networks via direct frontal assaults on unpatched mail, web, or DNS servers are largely behind us. We must focus on mitigating the risk of compromise of clients. Day four details ways in which endpoint systems can be both more resilient to attack and also enhance detective capabilities.

**Topics:** Security Architecture – Endpoint Protection; Dangerous Endpoint Applications; Patching

511.5 HANDS ON: **Automation and Continuous Security Monitoring**

Network Security Monitoring (NSM) is the beginning; we need to not only detect active intrusions and unauthorized actions, but also to know when our systems, networks, and applications are at an increased likelihood for compromise. A strong way to achieve this is through Continuous Security Monitoring (CSM) or Continuous Diagnostics and Mitigation (CDM). Rather than waiting for the results of a quarterly scan or an annual penetration test to determine what needs to be addressed, continuous monitoring proactively and repeatedly assesses and reassesses the current security posture for potential weaknesses that need be addressed.

**Topics:** CSM Overview; Industry Best Practices; Winning CSM Techniques; Maintaining Situational Awareness; Host, Port and Service Discovery; Vulnerability Scanning; Monitoring Patching; Monitoring Applications; Monitoring Service Logs; Monitoring Change to Devices and Appliances; Leveraging Proxy and Firewall Data; Configuring Centralized Windows Event Log Collection; Monitoring Critical Windows Events; Scripting and Automation

511.6 HANDS ON: **Capstone: Design, Detect, Defend**

The course culminates in a team-based design, detect, and defend-the-flag competition that is a full day of hands-on work applying the principles taught throughout the week.

**Topics:** Security Architecture; Assess Provided Architecture; Continuous Security Monitoring; Using Tools/Scripts Assessing the Initial State; Quickly/Thoroughly Find All Changes Made

---

**You Will Be Able To**

- Analyze a security architecture for deficiencies
- Apply the principles learned in the course to design a defensible security architecture
- Understand the importance of a detection-dominant security architecture and Security Operations Center (SOC)
- Identify the key components of Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/Continuous Monitoring (CM)
- Determine appropriate security monitoring needs for organizations of all sizes
- Implement robust Network Security Monitoring/Continuous Security Monitoring (NSM/CSM)
- Utilize tools to support implementation of Continuous Monitoring per NIST guidelines SP800-137
- Determine requisite monitoring capabilities for a SOC environment
- Determine capabilities required to support continuous monitoring of key Critical Security Controls

“SEC511 was one of my favorite SANS training courses so far. I am walking away, as I always do, with a huge number of things on my to do list and the hands-on experience to get started. The capstone CTF event was challenging, exciting, and so much fun. I walked away knowing I already learned so much and will be in a position to use this training to make my organization more secure.”

-TIMOTHY POTTER, NORDAM
As more organizations move data and infrastructure to the cloud, security is becoming a major priority. Operations and development teams are finding new uses for cloud services, and executives are eager to save money and gain new capabilities and operational efficiency by using these services. But will information security prove to be an Achilles’ heel? Many cloud providers do not provide detailed control information about their internal environments, and quite a few common security controls used internally may not translate directly to the public cloud.

SEC545: Cloud Security Architecture and Operations will tackle these issues one by one. We’ll start with a brief introduction to cloud security fundamentals, then cover the critical concepts of cloud policy and governance for security professionals. For the rest of day one and all of day two, we’ll move into technical security principles and controls for all major cloud types (SaaS, PaaS, and IaaS). We’ll learn about the Cloud Security Alliance framework for cloud control areas, then delve into assessing risk for cloud services, looking specifically at technical areas that need to be addressed.

The course then moves into cloud architecture and security design, both for building new architectures and for adapting tried-and-true security tools and processes to the cloud. This will be a comprehensive discussion that encompasses network security (firewalls and network access controls, intrusion detection, and more), as well as all the other layers of the cloud security stack. We’ll visit each layer and the components therein, including building secure instances, data security, identity and account security, and much more. We’ll devote an entire day to adapting our offense and defense focal areas to cloud. This will involve looking at vulnerability management and pen testing, as well as covering the latest and greatest cloud security research. On the defense side, we’ll delve into incident handling, forensics, event management, and application security.

We wrap up the course by taking a deep dive into SecDevOps and automation, investigating methods of embedding security into orchestration, and every facet of the cloud life cycle. We’ll explore tools and tactics that work, and even walk through several cutting-edge use cases where security can be automated entirely in both deployment and incident detection-and-response scenarios using APIs and scripting.
You Will Be Able To

> Revise and build internal policies to ensure cloud security is properly addressed
> Understand all major facets of cloud risk, including threats, vulnerabilities, and impact
> Articulate the key security topics and risks associated with SaaS, PaaS, and IaaS cloud deployment models
> Evaluate Cloud Access Security Brokers (CASBs) to better protect and monitor SaaS deployments
> Build security for all layers of a hybrid cloud environment, starting with hypervisors and working to application layer controls
> Evaluate basic virtualization hypervisor security controls
> Design and implement network security access controls and monitoring capabilities in a public cloud environment
> Design a hybrid cloud network architecture that includes IPsec tunnels
> Integrate cloud identity and access management (IAM) into security architecture
> Evaluate and implement various cloud encryption types and formats
> Develop multi-tier cloud architectures in a Virtual Private Cloud (VPC), using subnets, availability zones, gateways, and NAT
> Integrate security into DevOps teams, effectively creating a DevSecOps team structure
> Build automated deployment workflows using AWS and native tools
> Incorporate vulnerability management, scanning, and penetration testing into cloud environments
> Build automated and flexible detection and response programs using tools like AWS-IR, CloudWatch, CloudTrail, and AWS Lambda
> Leverage the AWS CLI to automate and easily execute operational tasks
> Set up and use an enterprise automation platform, Ansible, to automate configuration and orchestration tasks
> Use CloudWatch, CloudFormation, and other automation tools to integrate automated security controls into your cloud security program

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/sans-2018/courses
Many organizations have logging capabilities but lack the people and processes to analyze them. In addition, logging systems collect vast amounts of data from a variety of data sources that require an understanding of the sources for proper analysis. This class is designed to provide individuals training, methods, and processes for enhancing existing logging solutions. This class will also help you understand the when, what, and why behind the logs. This is a lab-heavy course that utilizes SOF-ELK, a SANS-sponsored free Security Information and Event Management (SIEM) solution, to provide hands-on experience and the mindset for large-scale data analysis.

Today, security operations do not suffer from a “big data” problem but rather a “data analysis” problem. Let’s face it, there are multiple ways to store and process large amounts of data without any real emphasis on gaining insight into the information collected. Added to that is the daunting idea of an infinite list of systems from which one could collect logs. It is easy to get lost in the perils of data saturation. This class moves away from the typical churn-and-burn log systems and moves instead towards achieving actionable intelligence and developing a tactical Security Operations Center (SOC).

This course is designed to demystify the SIEM architecture and process by navigating the student through the steps of tailoring and deploying a SIEM to full SOC integration. The material will cover many bases in the “appropriate” use of a SIEM platform to enrich readily available log data in enterprise environments and extract actionable intelligence. Once the information is collected, the student will be shown how to present the gathered input into usable formats to aid in eventual correlation. Students will then iterate through the log data and events to analyze key components that will allow them to learn how rich this information is, how to correlate the data, start investigating based on the aggregate data, and finally, how to go hunting with this newly gained knowledge. They will also learn how to deploy internal post-exploitation tripwires and breach canaries to nimbly detect sophisticated intrusions. Throughout the course, the text and labs will not only show how to manually perform these actions, but also how to automate many of the processes mentioned so students can employ these tasks the day they return to the office.

The underlying theme is to actively apply Continuous Monitoring and analysis techniques by utilizing modern cyber threat attacks. Labs will involve replaying captured attack data to provide real-world results and visualizations.

“One can conquer the SIEM world with this course.”
–Robert Lee Smith, RL Smith & Associates

“The immediate value of the course material is unlike any course or training I’ve received. A++”
–David Savercool, Dart Container

Justin Henderson  SANS Instructor

Justin Henderson is a passionate and dedicated information technology professional who has been in the field since 2005. Justin focuses on providing comprehensive industry training and uses his knowledge and experience to mentor others. Justin has a high proficiency in technical platforms including operating systems, networking, security, storage, and virtualization, but he has also worked in governance, project management, as well as service management. He has a BS degree in network design and administration from Western Governors University and has over 40 certifications, including the GPEN and GCWN. Justin has also taught network security at Lake Land College. Some of his other achievements include mentoring individuals in the information technology field as well as developing the virtual dojo, a fully automated cloud computing solution showcase environment.
555.1 HANDS ON: SIEM Architecture and SOF-ELK

Logging and analysis is a critical component in cyber network defense and allows for both reactive and proactive detection of adversarial activities. When properly utilized it becomes the backbone for agile detection and provides understanding to the overall environment. Logging and analysis products and techniques have been around for many years and are quickly gaining more and more functionality. This section will introduce free logging and analysis tools and focus on techniques to make sense of and augment traditional logs. It also covers how to handle the big data problem of handling billions of logs and how advances in free tools are starting to give commercial solutions a run for their money. Day one is designed to bring all students up to speed on SIEM concepts and to bring all students to a base level to carry them through the rest of the class. It is designed to also cover SIEM best practices. During day one we will be introducing Elasticsearch, Logstash, and Kibana within SOF-ELK and immediately go into labs to get students comfortable with ingesting, manipulating, and reporting on log data.

**Topics:** State of the SOC/SIEM; Log Monitoring; Logging Architecture; SIEM Platforms; Planning a SIEM; SIEM Architecture; Ingestion Techniques and Nodes; Data Queuing and Resiliency; Storage and Speed; Analytical Reporting

555.2 HANDS ON: Service Profiling with SIEM

A vast majority of network communication occurs over key network protocols, yet it is uncommon for organizations to use or collect these data. The sheer volume can be overwhelming. However, these common data sources provide an opportunity to identify modern day attacks. This section covers how to collect and handle this massive amount of data. Methods for collecting these logs through service logs such as from DNS servers will be covered, as will be passive ways of pulling the same data from the network itself. Techniques will be demonstrated to augment and add valuable context to the data as they are collected. Finally, analytical principles will be covered for finding the needles in the stack of needles. We will cover how, even if we have the problem of searching through billions of logs, we can surface only meaningful items of interest. Active dashboards will be designed to quickly find the logs of interest and to provide analysts with additional context for what to do next.

**Topics:** Detection Methods and Relevance to Log Analysis; Analyzing Common Application Logs that Generate Tremendous Amounts of Data; Apply Threat Intelligence to Generic Network Logs; Active Dashboards and Visualizations

555.3 HANDS ON: Advanced Endpoint Analytics

The value in endpoint logs provides tremendous visibility in detecting attacks. In particular, with regard to finding post-compromise activity, endpoint logs can quickly become second to none. However, logs even on a single desktop can range in the tens if not hundreds of thousands of events per day. Multiply this by the number of systems in your environment and it is no surprise why organizations get overwhelmed. This section will cover the how and more importantly the why behind collecting system logs. Various collection strategies and tools will be used to gain hands-on experience and to provide simplification with handling and filtering the seemingly infinite amount of data generated by both servers and workstations. Workstation log strategies will be covered in depth due to their value in today's modern attack vectors. After all, modern-day attacks typically start and then spread from workstations.

**Topics:** Endpoint Logs

555.4 HANDS ON: Baselining and User Behavior Monitoring

Know thyself is often quoted to defenders as a key defense strategy, and yet this is one of the most difficult things to accomplish. Take something such as having a list of all assets in an organization and knowing if any non-company assets are on the network. The task sounds simple but ends up being incredibly difficult to maintain in today's ever-evolving networks. This section focuses on applying techniques to automatically maintain a list of assets and their configurations as well as methods to distinguish if they are authorized or unauthorized. Key locations to provide high-fidelity data will be covered and techniques to correlate and combine multiple sources of data together will be demonstrated to build a master inventory list. Other forms of knowing thyself will be introduced such as gaining hands-on experience in analyzing network and system baselining techniques. We will monitor network flows and identify abnormal activity such as C2 beaconing as well as look for unusual user activity. Finally, we will apply large data analysis techniques to sift through massive amounts of endpoint data. This will be used to find things such as unwanted persistence mechanisms, dual-homed devices, and more.

**Topics:** Identify Authorized and Unauthorized Assets; Identify Authorized and Unauthorized Software; Baseline Data

555.5 HANDS ON: Tactical SIEM Detection and Post-Mortem Analysis

Multiple security devices exist but often are designed to be independent. Analysts are commonly divided into specialty areas and focus on their respective area such as a network intrusion detection system. However, alerts from a single security device lack context and are akin to the common analogy of "looking up from the bottom of a well." This section focuses on combining multiple security logs for central analysis. More importantly, we will cover methods for combining multiple sources to provide improved context to analysts. We will also show how providing context with asset data can help prioritize analyst time, saving money and addressing risks that matter. After covering ways to optimize traditional security alerts, we will jump into new methods to utilize logging technology to implement virtual tripwires. While it would be ideal to prevent attackers from gaining access to your network, it is a given that at some point you will be compromised. However, preventing compromise is the beginning, not the end goal. Adversaries will crawl your systems and network to achieve their own ends. Knowing this, we will implement logging-based tripwires—and if a single one is stepped on, we can quickly detect it and respond to the adversary.

**Topics:** Centralize HIDS and HIDS Alerts; Analyze Endpoint Security Logs; Augment Intrusion Detection Alerts; Analyze Vulnerability Information; Correlate Malware Sandbox Logs with Other Systems to Identify Victims Across the Enterprise; Monitor Firewall Activity; SIEM Tripwires; Post Mortem Analysis

555.6 HANDS ON: Capstone: Design, Detect, Defend

The course culminates in a team-based design, detect, and defend the flag competition. Powered by NetWars, day six provides a full day of hands-on work applying the principles taught throughout the week. Your team will progress through multiple levels and missions designed to ensure mastery of the modern cyber defense techniques promoted all week long. From building a logging architecture to augmenting logs, analyzing network logs, analyzing system logs, and developing dashboards to find attacks, this challenging exercise will reinforce key principles in a fun, hands-on, team-based challenge.

**Topics:** Defend-the-Flag Challenge – Hands-on Experience

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/event/sans-2018/courses](http://www.sans.org/event/sans-2018/courses)
**Implementing and Auditing the Critical Security Controls – In-Depth**

Cybersecurity attacks are increasing and evolving so rapidly that it is more difficult than ever to prevent and defend against them. Does your organization have an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches? This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS).

As threats evolve, an organization’s security should too. To enable your organization to stay on top of this ever-changing threat scenario, SANS has designed a comprehensive course on how to implement the Critical Security Controls, a prioritized, risk-based approach to security. Designed by private and public sector experts from around the world, the Controls are the best way to block known attacks and mitigate damage from successful attacks. They have been adopted by the U.S. Department of Homeland Security, state governments, universities, and numerous private firms.

The Controls are specific guidelines that CISOs, CIOs, IGs, systems administrators, and information security personnel can use to manage and measure the effectiveness of their defenses. They are designed to complement existing standards, frameworks, and compliance schemes by prioritizing the most critical threats and highest payoff defenses, while providing a common baseline for action against risks that we all face.

The Controls are an effective security framework because they are based on actual attacks launched regularly against networks. Priority is given to Controls that (1) mitigate known attacks (2) address a wide variety of attacks, and (3) identify and stop attackers early in the compromise cycle. The British government’s Center for the Protection of National Infrastructure describes the Controls as the “baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence.”

SANS’s in-depth, hands-on training will teach you how to master the specific techniques and tools needed to implement and audit the Critical Controls. It will help security practitioners understand not only how to stop a threat, but why the threat exists, and how to ensure that security measures deployed today will be effective against the next generation of threats.

The course shows security professionals how to implement the Controls in an existing network through cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the Controls are effectively implemented.

---

**Who Should Attend**

- Information assurance auditors
- System implementers or administrators
- Network security engineers
- IT administrators
- Department of Defense personnel or contractors
- Staff and clients of federal agencies
- Private sector organizations looking to improve information assurance processes and secure their systems
- Security vendors and consulting groups looking to stay current with frameworks for information assurance
- Alumni of SEC/AUD440, SEC401, SEC501, SANS Audit classes, and MGT512

---

**James Tarala**  **SANS Senior Instructor**

James Tarala is a principal consultant with Enclave Security and is based in Venice, Florida. He is a regular speaker for the SANS Institute as well as a courseware author and editor for many SANS auditing and security courses. As a consultant, he has spent the past few years developing large enterprise IT security and infrastructure architectures, specifically working with many Microsoft-based directory services, e-mail, terminal services, and wireless technologies. He has also spent a large amount of time consulting with organizations to assist them with their security management, operational practices, and regulatory compliance issues, and he often performs independent security audits and assists internal audit groups in developing their internal audit programs. James completed his undergraduate studies at Philadelphia Biblical University and his graduate work at the University of Maryland. He holds numerous professional certifications. [@isaudit](https://twitter.com/isaudit)
You Will Be Able To

- Apply a security framework based on actual threats that is measurable, scalable, and reliable in stopping known attacks and protecting organizations’ important information and systems
- Understand the importance of each Control, how it is compromised if ignored, and explain the defensive goals that result in quick wins and increased visibility of networks and systems
- Identify and utilize tools that implement Controls through automation
- Learn how to create a scoring tool for measuring the effectiveness of each Control
- Employ specific metrics to establish a baseline and measure the effectiveness of the Controls
- Understand how the Critical Controls map to standards such as NIST 800-53, ISO 27002, the Australian Top 35, and more
- Audit each of the Critical Controls with specific, proven templates, checklists, and scripts provided to facilitate the audit process

“This course gives you attainable goals, actionable steps to take in your organization and metrics to ensure you don’t drift from the controls.”
- BRANDON POOLE, SOUTH CAROLINA STUDENT LOAN PROGRAM

“SEC566 provides the what/why/how to a more secure environment.”
- BRETT HAMMOND, ETC USA

Course Day Descriptions

566.1 HANDS ON: Introduction and Overview of the 20 Critical Controls
Day 1 will introduce you to all of the Critical Controls, laying the foundation for the rest of the class. For each Control, we will follow the same outline covering the following information:

- Overview of the Control
- How It Is Compromised
- Defensive Goals
- Quick Wins
- Visibility & Attribution
- Configuration & Hygiene
- Advanced
- Overview of Evaluating the Control

In addition, Critical Controls 1 and 2 will be covered in-depth.

**Topics:**
- Critical Control 1: Inventory of Authorized and Unauthorized Devices
- Critical Control 2: Inventory of Authorized and Unauthorized Software

566.2 HANDS ON: Critical Controls 3, 4, 5, and 6

**Topics:**
- Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
- Critical Control 4: Continuous Vulnerability Assessment and Remediation
- Critical Control 5: Controlled Use of Administrative Privileges
- Critical Control 6: Maintenance, Monitoring, and Analysis of Audit Logs

566.3 HANDS ON: Critical Controls 7, 8, 9, 10, and 11

**Topics:**
- Critical Control 7: Email and Web Browser Protections
- Critical Control 8: Malware Defenses
- Critical Control 9: Limitation and Control of Network Ports, Protocols, and Services
- Critical Control 10: Data Recovery Capability (validated manually)
- Critical Control 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

566.4 HANDS ON: Critical Controls 12, 13, 14, and 15

**Topics:**
- Critical Control 12: Boundary Defense
- Critical Control 13: Data Protection
- Critical Control 14: Controlled Access Based on the Need to Know
- Critical Control 15: Wireless Device Control

566.5 HANDS ON: Critical Controls 16, 17, 18, 19, and 20

**Topics:**
- Critical Control 16: Account Monitoring and Control
- Critical Control 17: Security Skills Assessment and Appropriate Training to Fill Gaps (validated manually)
- Critical Control 18: Application Software Security
- Critical Control 19: Incident Response and Management (validated manually)
- Critical Control 20: Penetration Tests and Red Team Exercises (validated manually)

“The 20 controls presented in the course are requirements found in most regulated industries. I found the format and layout of each control well explained and easy to follow.”
- JOSH ELLIS, IBERDROLA USA
You just got hired to help our virtual organization “SyncTechLabs” build out a cybersecurity capability. On your first day, your manager tells you: “We looked at some recent cybersecurity trend reports and we feel like we’ve lost the plot. Advanced persistent threats, ransomware, denial of service...We’re not even sure where to start!”

Cyber threats are on the rise: ransomware is affecting small, medium and large enterprises alike, while state-sponsored adversaries are attempting to obtain access to your most precious crown jewels. SEC599: Defeating Advanced Adversaries – Implementing Kill Chain Defenses will arm you with the knowledge and expertise you need to detect and respond to today’s threats. Recognizing that a prevent-only strategy is not sufficient, we will introduce security controls designed to stop advanced adversaries.

Course authors Erik Van Buggenhout and Stephen Sims (both certified as GIAC Security Experts) are hands-on practitioners who have achieved a deep understanding of how cyber attacks work through penetration testing and incident response. While teaching penetration testing courses, they were often asked “But how do I prevent this type of attack?” With more than 20 labs plus a full-day “Defend-The-Flag” exercise during which students attempt to defend our virtual organization from different waves of attacks against its environment, SEC599 gives students real-world examples of how to prevent attacks.

Our six-day journey will start with an analysis of recent attacks through in-depth case studies. We will explain what types of attacks are occurring and introduce the Advanced Persistent Threat (APT) Attack Cycle as a structured approach to describing attacks. In order to understand how attacks work, you will also compromise our virtual organization “SyncTechLabs” in our Day 1 exercises.

In designing the course and its exercises, the authors went the extra mile to ensure that attendees “build” something that can be used later on. For this reason, the different technologies illustrated throughout the course (e.g., IDS systems, web proxies, sandboxes, visualization dashboards, etc.) will be provided as usable virtual machines on the course USB.

SEC599 will finish with a bang. During the “Defend-the-Flag” challenge on the final course day you will be pitted against advanced adversaries in an attempt to keep your network secure. Can you protect the environment against the different waves of attacks? The adversaries aren’t slowing down, so what are you waiting for?

**Six-Day Program**
**Tue, April 3 - Sun, April 8**
9:00am - 5:00pm
36 CPEs
Laptop Required

Instructor: Erik Van Buggenhout

**Who Should Attend**
- Security architects
- Security engineers
- Technical security managers
- Security Operations Center analysts, engineers, and managers
- IT administrators
- Individuals looking to better understand how advanced persistent cyber adversaries operate and how the IT environment can be improved to better prevent, detect, and respond to incidents

“SANS provides world-class training that is regularly updated with the latest information, and taught by people who are working in the field.”

- Alan Waggoner,
  Siemer Milling Company

**Erik Van Buggenhout  SANS Certified Instructor**

Erik Van Buggenhout is the lead author of SEC599: Defeating Advanced Adversaries. In addition, Erik teaches SEC560: Network Penetration Testing and Ethical Hacking and SEC542: Web Application Penetration Testing and Ethical Hacking. He has been involved with SANS since 2009, starting as a Mentor, working his way to Community Instructor in 2012, and finally becoming a Certified Instructor in 2016. Erik loves explaining deeply technical concepts by using war stories, adding a few funny anecdotes here and there. As testimony to his technical expertise, he has obtained the GSE, GCIA, GNFA, GNAP, GWAPT, GCIH, and GSEC certifications. In addition to his work with SANS, Erik is the co-founder of the Belgian firm NVISO, which focuses on high-end cybersecurity services, specializing in government, defense and the financial sector. Together with his team of 20+ technical experts, Erik delivers a wide array of technical security services, including penetration testing, security monitoring and incident response. Prior to NVISO, Erik spent five years at Big 4 firm, starting as a junior penetration tester and evolving into a subject-matter expert for the EMEA region. Erik is a self-confessed speed walker, so if you see him rushing around at a conference, feel free to stop him and say “Hi!”

@ErikVaBu

Register at www.sans.org/sans-2018 | 301-654-SANS (7267)
Course Day Descriptions

599.1 HANDS ON: **Knowing the Adversary, Knowing Yourself**
Our six-day journey will start with an analysis of recent attacks through in-depth case studies. We will explain what's happening out there and introduce the APT Attack Cycle as a structured approach to describing attacks. In order to understand how attacks work, you will also compromise our virtual organization "SyncTechLabs" during the day's exercises.

**Topics:** Course Outline and Lab Set-up; Current Threat and Attack Landscape; Introducing the APT Attack Cycle; Recent Attacks – Case Studies; Knowing Yourself – Understanding Your Own Environment; Understanding and Limiting Your Organization’s Footprint

599.2 HANDS ON: **Hindering Reconnaissance and Stopping Delivery**
Day 2 will cover how attackers take their first steps. How do they perform reconnaissance and what can we do to hinder it? The courseware will cover technical controls, but will also touch upon "soft topics" such as security awareness. After reconnaissance is performed and vulnerabilities are spotted, the adversary will weaponize the payload and deliver it to the target. We will analyze how delivery of the payload can be detected and blocked. We will cover a variety of techniques, including mail-based controls (e.g., SMTP file and URL carving, sandboxing, etc.) and web-based controls (access controls using web proxies).

**Topics:** Strategies for Preventing/Detecting Payload Delivery; End-User Security Awareness; Leveraging Suricata IDS / IPS; Mail Security Controls (AV, SMTP File, and URL Carving); Mail Attachment Sandboxing; Zooming in on YARA Rules; Controlling Scripts in the Enterprise; Web Proxy Configuration to Defeat Drive-by Downloads

599.3 HANDS ON: **Preventing Exploitation**
Day 3 will explain how exploitation can be prevented. Attendees will gain an in-depth understanding of current exploitation tactics. We will introduce effective security controls to stop exploitation attempts dead in their tracks. We will assess tools and techniques aimed at protecting both your network and your hosts and applications. Typical items that will be discussed include network authentication, OS hardening, application threat modeling, client and OS patch management, and exploit mitigation techniques.

**Topics:** Protecting the Network; Protecting Your Hosts; Protecting Your Own Software; Protecting Other Software

599.4 HANDS ON: **Preventing Exploitation (continued); Avoiding Installation and Foiling Command and Control**
Day 4 will continue with discussion about exploit prevention techniques, but we'll also zoom in on persistence techniques typically employed by advanced adversaries and how command and control is established. If adversaries successfully exploit a vulnerability, their next step is to attempt to maintain their access, escalate privileges, and set up a command and control channel.

**Topics:** Network Architecture and Segmentation Recommendations; Monitoring the Active Directory Environment for Suspicious Behavior; Typical Persistence Strategies and Approaches; Detecting and Avoiding Persistence in the Enterprise; Full-Packet Capture and IDS Strategies; Traffic Profiling; NetFlow Analysis and Recommendations; Identifying Command and Control

599.5 HANDS ON: **Thwarting Exfiltration, Cyber Deception, and Incident Response**
Day 5 focuses on stopping the adversary during the final stages of the attack:
- How can data exfiltration be detected and stopped?
- How can cyber deception be used to slow down and stop advanced adversaries?
- How can threat intelligence aid defenders in the APT Attack Cycle?
- How can defenders perform effective incident response?

As always, theoretical concepts will be illustrated during the different exercises performed throughout the day.

**Topics:** Data Exfiltration; Vector-Oriented Defenses; Cyber Deception Strategies; Leveraging Threat Intelligence; Patrolling the Neighborhood; Incident Response

599.6 HANDS ON: **Advanced Persistent Threat Defender Capstone**
The course culminates in a team-based Defend the Flag competition. Day six provides a full day of hands-on work applying the principles taught throughout the week. Your team will progress through multiple levels and missions designed to ensure mastery of the modern cybersecurity controls taught all week long. This challenging exercise will reinforce key principles in a fun challenge that will put your new skills to the test in an environment just like the ones you’ll be working in when you return to your jobs.

**Topics:** Applying Previously Covered Security Controls In-depth; Reconnaissance; Weaponization; Delivery; Exploitation; Installation; Command and Control; Action on Objectives

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/event/sans-2018/courses](http://www.sans.org/event/sans-2018/courses)
“NetWars takes the concepts in the class and gives you an opportunity to put them into action. Highly recommended!”

– Kyle McDaniel, Lenovo
Focus Job Roles and Specialized Skills
Penetration Testing & Vulnerability Analysis

Summary: High-performing security organizations need specially trained professionals who can continuously challenge the defenses and monitoring systems set up by the cyber defense operating teams and discover vulnerabilities to be addressed that might otherwise be exploited by attackers. Professionals focusing on this career path must be able to test both network and wireless vulnerabilities and understand these environments before advancing to additional areas.

SEC560 and SEC542 teach you the skills that are core to this type of role. An additional nine SANS penetration testing courses, in advanced and specialized topics, allow you to mold your career into a particular practice area or task. Review the following pages for detailed information about all of these courses and the certifications that validate your acquired skills.

Who This Path Is For: Information Security Engineers, Analysts, and Risk Consultants need to master this coursework in particular to hone their penetration testing, ethical hacker, and vulnerability analysis skills.

Why This Training Is Important: These courses teach proper planning, scoping, and recon, while diving deep into scanning, target exploitation, password attacks, web app configuration, identity, authentication, custom scripting, and interception proxies. Filled with dozens of detailed, hands-on labs, this training allows you to go back to work with the practical, real-world examples and practice needed to do your job efficiently and masterfully.

“I was pleasantly humbled, challenged, encouraged and trained. I feel 100% more qualified to defend my company’s network after taking this training.”
-Ivan Dominguez, NWCU.com
Who Should Attend

- Security personnel whose job involves assessing networks and systems to find and remediate vulnerabilities
- Penetration testers
- Ethical hackers
- Defenders who want to better understand offensive methodologies, tools, and techniques
- Auditors who need to build deeper technical skills
- Red and blue team members
- Forensics specialists who want to better understand offensive tactics

This course has extended hours

Instructor: Ed Skoudis

SEC560 is the must-have course for every well-rounded security professional.

With comprehensive coverage of tools, techniques, and methodologies for network penetration testing, SEC560 truly prepares you to conduct high-value penetration testing projects step-by-step and end-to-end. Every organization needs skilled information security personnel who can find vulnerabilities and mitigate their effects, and this entire course is specially designed to get you ready for that role. The course starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, password attacks, and web app manipulation, with more than 30 detailed hands-on labs throughout. The course is chock-full of practical, real-world tips from some of the world’s best penetration testers to help you do your job safely, efficiently...and masterfully.

Learn the best ways to test your own systems before the bad guys attack.

SEC560 is designed to get you ready to conduct a full-scale, high-value penetration test—and on the last day of the course you’ll do just that. After building your skills in comprehensive and challenging labs over five days, the course culminates with a final full-day, real-world penetration test scenario. You’ll conduct an end-to-end pen test, applying knowledge, tools, and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organization, demonstrating the knowledge you’ve mastered in this course.

You will bring comprehensive penetration testing and ethical hacking know-how back to your organization.

You will learn how to perform detailed reconnaissance, studying a target’s infrastructure by mining blogs, search engines, social networking sites, and other internet and intranet infrastructures. Our hands-on labs will equip you to scan target networks using best-of-breed tools. We won’t just cover run-of-the-mill options and configurations, we’ll also go over the lesser known but super-useful capabilities of the best pen test toolsets available today. After scanning, you’ll learn dozens of methods for exploiting target systems to gain access and measure real business risk. You’ll dive deep into post-exploitation, password attacks, and web apps, pivoting through the target environment to model the attacks of real-world bad guys to emphasize the importance of defense in-depth.

Ed Skoudis  SANS Faculty Fellow

Ed Skoudis is the founder of Counter Hack, an innovative organization that designs, builds, and operates popular InfoSec challenges and simulations including CyberCity, NetWars, Cyber Quests, and Cyber Foundations. As director of the CyberCity project, Ed oversees the development of missions that help train cyber warriors to defend the kinetic assets of a physical, miniaturized city. Ed’s expertise includes hacker attacks and defenses, incident response, and malware analysis, with over 15 years of experience in information security. Ed authored and regularly teaches the SANS courses on network penetration testing (SEC560) and incident response (SEC504), helping over 3,000 information security professionals each year improve their skills and abilities to defend their networks. He has performed numerous security assessments; conducted exhaustive anti-virus, anti-spyware, Virtual Machine, and IPS research; and responded to computer attacks for clients in government, military, financial, high technology, healthcare, and other industries. Previously, Ed served as a security consultant with InGuardians, International Network Services (INS), Global Integrity, Predictive Systems, SAIC, and Bell Communications Research (Bellcore). Ed also blogs about command line tips and penetration testing. @edskoudis

"SEC560 provides practical, how-to material that I can use daily in my penetration testing activities – not only technically, but also from a business perspective.”

-Steve Nolan, General Dynamics
560.1 HANDS ON: Comprehensive Pen Test Planning, Scoping, and Recon

In this section of the course, you will develop the skills needed to conduct a best-of-breed, high-value penetration test. We will go in-depth on how to build penetration testing infrastructure that includes all the hardware, software, network infrastructure, and tools you will need to conduct great penetration tests, with specific low-cost recommendations for your arsenal. We will then cover formulating a pen test scope and rules of engagement that will set you up for success, including a role-play exercise. We’ll also dig deep into the reconnaissance portion of a penetration test, covering the latest tools and techniques, including hands-on document metadata analysis to pull sensitive information about a target environment, as well as a lab using Recon-ng to plunder a target’s DNS infrastructure for information such as the anti-virus tools the organization relies on.

Topics: The Mindset of the Professional Pen Tester; Building a World-Class Pen Test Infrastructure; Creating Effective Pen Test Scopes and Rules of Engagement; Detailed Recon Using the Latest Tools; Effective Pen Test Reporting to Maximize Impact; Mining Search Engine Results; Document Metadata Extraction and Analysis

560.2 HANDS ON: In-Depth Scanning

We next focus on the vital task of mapping the target environment’s attack surface by creating a comprehensive inventory of machines, accounts, and potential vulnerabilities. We will look at some of the most useful scanning tools freely available today and run them in numerous hands-on labs to help hammer home the most effective way to use each tool. We will also conduct a deep dive into some of the most useful tools available to pen testers today for formulating packets: Scapy and Netcat. We finish the day covering vital techniques for false-positive reduction so you can focus your findings on meaningful results and avoid the sting of a false positive. And we will examine the best ways to conduct your scans safely and efficiently.

Topics: Tips for Awesome Scanning; Tcptrace for the Pen Tester; Nmap In-Depth; Version Scanning with Nmap; Vulnerability Scanning with Nessus; False-Positive Reduction; Packet Manipulation with Scapy; Enumerating Users; Netcat for the Pen Tester; Monitoring Services During a Scan

560.3 HANDS ON: Exploitation

In this section, we look at the many kinds of exploits that penetration testers use to compromise target machines, including client-side exploits, service-side exploits, and local privilege escalation. We’ll see how these exploits are packaged in frameworks like Metasploit and its mighty Meterpreter. You’ll learn in-depth how to leverage Metasploit and the Meterpreter to compromise target environments. We’ll also analyze the topic of anti-virus evasion to bypass the target organization’s security measures, as well as methods for pivoting through target environments, all with a focus on determining the true business risk of the target organization.

Topics: Comprehensive Metasploit Coverage with Exploits/Stagers/Stages; Strategies and Tactics for Anti-Virus Evasion; In-Depth Meterpreter Analysis, Hands-On; Implementing Port Forwarding Relays for Merciless Pivots; How to Leverage Shell Access of a Target Environment

560.4 HANDS ON: Post-Exploitation and Merciless Pivoting

Once you’ve successfully exploited a target environment, penetration testing gets extra exciting as you perform post-exploitation, gathering information on compromised machines and pivoting to other systems in your scope. This section of the course zooms in on pilaging target environments and building formidable hands-on line skills. We’ll cover Windows command line skills in-depth, including PowerShell’s awesome abilities for post-exploitation. We’ll see how we can leverage malicious services and the incredible WMI/WinRM toolset to access and pivot through a target organization. We’ll then turn our attention to password guessing attacks, discussing how to avoid account lockout, as well as numerous options for plundering password hashes from target machines including the great Mimikatz Kiwi tool. Finally, we’ll look at Metasploit’s fantastic features for pivoting, including the msfconsole route command.

Topics: Windows Command Line Kung Fu for Penetration Testers; PowerShell’s Amazing Post-Exploitation Capabilities; Password Attack Tips; Account Lockout and Strategies for Avoiding It; Automated Password Guessing with THC-Hydra; Retrieving and Manipulating Hashes from Windows, Linux, and Other Systems; Pivoting through Target Environments; Extracting Hashes and Passwords from Memory with Mimikatz Kiwi

560.5 HANDS ON: In-Depth Password Attacks and Web App Pen Testing

In this section of the course, we’ll go even deeper in exploiting one of the weakest aspects of most computing environments: passwords. You’ll custom-compile John the Ripper to optimize its performance in cracking passwords. You’ll look at the amazingly full-featured Cain tool, running it to crack snipped Windows authentication messages. We’ll see how Rainbow Tables really work to make password cracking much more efficient, all hands-on. And we’ll cover powerful “pass-the-hash” attacks, leveraging Metasploit, the Meterpreter, and more. We then turn our attention to web application pen testing, covering the most powerful and common web app techniques with hands-on labs for every topic we address. We’ll cover finding and exploiting cross-site scripting (XSS), cross-site request forgery (XSRF), command injection, and SQL injection flaws in applications such as online banking, blog sites, and more.

Topics: Password Cracking with John the Ripper; Sniffing and Cracking Windows Authentication Exchanges Using Cain; Using Rainbow Tables to Maximum Effectiveness; Pass-the-Hash Attacks with Metasploit and More; Finding and Exploiting Cross-Site Scripting; Cross-Site Request Forgery; SQL Injection; Leveraging SQL Injection to Perform Command Injection; Maximizing Effectiveness of Command Injection Testing

560.6 HANDS ON: Penetration Test and Capture-the-Flag Workshop

This lively session represents the culmination of the network penetration testing and ethical hacking course. You’ll apply all of the skills mastered in the course so far in a full-day, hands-on workshop during which you’ll conduct an actual penetration test of a sample target environment. We’ll provide the scope and rules of engagement, and you’ll work with a team to achieve your goal of finding out whether the target organization’s Personally Identifiable Information (PII) is at risk. As a final step in preparing you for conducting penetration tests, you’ll make recommendations about remediating the risks you identify.

Topics: Applying Penetration Testing and Ethical Hacking Practices End-to-End; Scanning; Exploitation; Post-Exploitation; Merciless Pivoting; Analyzing Results

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/sans-2018/courses
Web App Penetration Testing and Ethical Hacking

Web applications play a vital role in every modern organization. However, if your organization doesn’t properly test and secure its web apps, adversaries can compromise these applications, damage business functionality, and steal data. Unfortunately, many organizations operate under the mistaken impression that a web application security scanner will reliably discover flaws in their systems.

SEC542 helps students move beyond push-button scanning to professional, thorough, and high-value web application penetration testing.

Customers expect web applications to provide significant functionality and data access. Even beyond the importance of customer-facing web applications, internal web applications increasingly represent the most commonly used business tools within any organization. Unfortunately, there is no “patch Tuesday” for custom web applications, and major industry studies find that web application flaws play a major role in significant breaches and intrusions. Adversaries increasingly focus on these high-value targets either by directly abusing public-facing applications or by focusing on web apps as targets after an initial break-in.

Modern cyber defense requires a realistic and thorough understanding of web application security issues. Anyone can learn to sling a few web hacks, but effective web application penetration testing requires something deeper.

SEC542 enables students to assess a web application’s security posture and convincingly demonstrate the impact of inadequate security that plagues most organizations.

In this course, students will come to understand major web application flaws and their exploitation. Most importantly, they’ll learn a field-tested and repeatable process to consistently find these flaws and convey what they have learned to their organizations. Even technically gifted security geeks often struggle with helping organizations understand risk in terms relatable to business. Much of the art of penetration testing has less to do with learning how adversaries are breaking in than it does with convincing an organization to take the risk seriously and employ appropriate countermeasures. The goal of SEC542 is to better secure organizations through penetration testing, and not just show off hacking skills. This course will help you demonstrate the true impact of web application flaws through exploitation.

In addition to high-quality course content, SEC542 focuses heavily on in-depth, hands-on labs to ensure that students can immediately apply all they learn.

In addition to having more than 30 formal hands-on labs, the course culminates in a web application pen test tournament, powered by the SANS NetWars Cyber Range. This Capture-the-Flag event on the final day brings students into teams to apply their newly acquired command of web application penetration testing techniques in a fun way that hammers home lessons learned.

Seth Misenar  SANS Senior Instructor

Seth Misenar is the founder of and lead consultant for Context Security, a Jackson, Mississippi-based company that provides information security thought leadership, independent research, and security training. Seth’s background includes network and web application penetration testing, vulnerability assessment, regulatory compliance efforts, security architecture design, and general security consulting. He has previously served as both a physical and network security consultant for Fortune 100 companies, as well as the Health Insurance Portability and Accountability Act, and as information security officer for a state government agency. Prior to becoming a security geek, Seth received a bachelor’s degree in philosophy from Millsaps College, where he was twice selected for a Ford Teaching Fellowship. Also, Seth is no stranger to certifications and thus far has achieved credentials that include CISSP, GPEC, GWAPT, GSEC, GCIA, GCHH, GCWN, GCFA, and MCSE.  @sethmisenar

Who Should Attend

- General security practitioners
- Penetration testers
- Ethical hackers
- Web application developers
- Website designers and architects

“SEC542 is high-quality training that I can apply to my job right away. The labs in this class are the best I’ve encountered so far.”

-Roselle Mariotti Jones, BPA

“As a web application developer, SEC542 gives me great insight into what I can do better and what to look for.”

-Joshua Barone, Geocent
542.1 HANDS ON: Introduction and Information Gathering
Understanding the attacker’s perspective is key to successful web application penetration testing. The course begins by thoroughly examining web technology, including protocols, languages, clients and server architectures, from the attacker’s perspective. We will also examine different authentication systems, including Basic, Digest, Forms and Windows Integrated authentication, and discuss how servers use them and attackers abuse them.

**Topics:** Overview of the Web from a Penetration Tester’s Perspective; Exploring the Various Servers and Clients; Discussion of the Various Web Architectures; Discovering How Session State Works; Discussion of the Different Types of Vulnerabilities; Defining a Web Application Test Scope and Process; Defining Types of Penetration Testing; Heartbleed Exploitation; Utilizing the Burp Suite in Web App Penetration Testing

542.2 HANDS ON: Configuration, Identity, and Authentication Testing
The second day starts the actual penetration testing process, beginning with the reconnaissance and mapping phases. Reconnaissance includes gathering publicly available information regarding the target application and organization, identifying the machines that support our target application, and building a profile of each server, including the operating system, specific software and configuration. The discussion is underscored through several practical, hands-on labs in which we conduct reconnaissance against in-class targets.

**Topics:** Discovering the Infrastructure Within the Application; Identifying the Machines and Operating Systems; Secure Sockets Layer (SSL) Configurations and Weaknesses; Exploring Virtual Hosting and Its Impact on Testing; Learning Methods to Identify Load Balancers; Software Configuration Discovery; Exploring External Information Sources; Learning Tools to Spider a Website; Scripting to Automate Web Requests and Spidering; Brute Forcing Unlinked Files and Directories; Discovering and Exploiting Shellshock

542.3 HANDS ON: Injection
This section continues to explore our methodology with the discovery phase. We will build on the information started the previous day, exploring methods to find and verify vulnerabilities within the application. Students will also begin to explore the interactions between the various vulnerabilities.

**Topics:** Python for Web App Penetration Testing; Web App Vulnerabilities and Manual Verification Techniques; Interception Proxies; Zed Attack Proxy (ZAP); Burp Suite; Information Leakage and Directory Browsing; Username Harvesting; Command Injection; Directory Traversal; SQL Injection; Blind SQL Injection; Local File Inclusion (LFI); Remote-File Inclusion (RFI); JavaScript for the Attacker

542.4 HANDS ON: JavaScript and XSS
On day four, students continue exploring the discovery phase of the methodology. We cover methods to discover key vulnerabilities within web applications, such as Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF/XSRF). Manual discovery methods are employed during hands-on labs.

**Topics:** Cross-Site Scripting (XSS); Cross-Site Request Forgery (CSRF); Session Flaws; Session Fixation; AJAX; Logic Attacks; Data Binding Attacks; Automated Web Application Scanners; w3af; XML and JSON

542.5 HANDS ON: CSRF, Logic Flaws, and Advanced Tools
On the fifth day, we launch actual exploits against real-world applications, building on the previous three steps, expanding our foothold within the application, and extending it to the network on which it resides. As penetration testers, we specifically focus on ways to leverage previously discovered vulnerabilities to gain further access, highlighting the cyclical nature of the four-step attack methodology.

**Topics:** Metasploit for Web Penetration Testing; The sqlmap Tool; Exploring Methods to Zombify Browsers; Browser Exploitation Framework (BeEF); Walking Through an Entire Attack Scenario; Leveraging Attacks to Gain Access to the System; How to Pivot Our Attacks Through a Web Application; Understanding Methods of Interacting with a Server Through SQL Injection; Exploiting Applications to Steal Cookies; Executing Commands Through Web Application Vulnerabilities

542.6 HANDS ON: Capture the Flag
On day six, students form teams and compete in a web application penetration testing tournament. This NetWars-powered Capture-the-Flag exercise provides students an opportunity to wield their newly developed or further-honed skills to answer questions, complete missions, and exfiltrate data, applying skills gained throughout the course. The style of challenge and integrated-hint system allows students of various skill levels to both enjoy a game environment and solidify the skills learned in class.

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/event/sans-2018/courses](www.sans.org/event/sans-2018/courses)
Immersive Hands-on Hacking Techniques

To be a top penetration testing professional, you need fantastic hands-on skills for finding, exploiting and resolving vulnerabilities. Top instructors at SANS engineered SEC561: Immersive Hands-On Hacking Techniques from the ground up to help you get good fast. The course teaches in-depth security capabilities through 80%+ hands-on exercises, maximizing keyboard time during in-class labs and making this SANS’s most hands-on course ever. With over 30 hours of intense labs, students experience a leap in their capabilities, as they come out equipped with the practical skills needed to handle today’s pen test and vulnerability assessment projects in enterprise environments. Throughout the course, an expert instructor coaches students as they work their way through solving increasingly demanding real-world information security scenarios using skills that they will be able to apply the day they get back to their jobs.

People often talk about these concepts, but this course teaches you how to actually do them hands-on and in-depth. SEC561 shows penetration testers, vulnerability assessment personnel, auditors, and operations personnel how to leverage in-depth techniques to get powerful results in every one of their projects. The course is overflowing with practical lessons and innovative tips, all with direct hands-on application. Throughout the course, students interact with brand new and custom-developed scenarios built just for this course on the innovative NetWars challenge infrastructure, which guides them through the numerous hands-on labs providing questions, hints, and lessons learned as they build their skills.

Topics addressed in the course include:

- Applying network scanning and vulnerability assessment tools to effectively map out networks and prioritize discovered vulnerabilities for effective remediation
- Manipulating common network protocols to reconfigure internal network traffic patterns, as well as defenses against such attacks
- Analyzing Windows and Linux systems for weaknesses using the latest enterprise management capabilities of the operating systems, including the super-powerful Windows Remote Management (WinRM) tools
- Applying cutting-edge password analysis tools to identify weak authentication controls leading to unauthorized server access
- Scouring through web applications and mobile systems to identify and exploit devastating developer flaws
- Evading anti-virus tools and bypassing Windows User Account Control to understand and defend against these advanced techniques
- Honing phishing skills to evaluate the effectiveness of employee awareness initiatives and your organization’s exposure to one of the most damaging attack vectors widely used today

SEC561
Immersive Hands-on Hacking Techniques

Six-Day Program
Tue, April 3 - Sun, April 8
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Tim Medin

Who Should Attend

- Security professionals who want to expand their hands-on technical skills in new analysis areas such as packet analysis, digital forensics, vulnerability assessment, system hardening, and penetration testing
- Systems and network administrators who want to gain hands-on experience in information security skills to become better administrators
- Incident response analysts who want to better understand system attack and defense techniques
- Forensic analysts who need to improve their analysis through experience with real-world attacks
- Penetration testers seeking to gain practical experience for use in their own assessments
- Red team members who want to build their hands-on skills and blue team members who want to better understand attacks and defend their environments

Tim Medin  SANS Principal Instructor

Tim Medin is a senior technical analyst at Counter Hack, a company devoted to the development of information security challenges for education, evaluation, and competition. Through the course of his career, Tim has performed penetration tests on a wide range of organizations and technologies. Prior to Counter Hack, Tim was a senior security consultant for FishNet Security, where most of his focus was on penetration testing. He gained information security experience in a variety of industries including previous positions in control systems, higher education, financial services, and manufacturing. Tim regularly contributes to the SANS Penetration Testing Blog (pen-testing.sans.org/blog/) and the Command Line Kung Fu Blog (blog.commandlinekungfu.com). He is also project lead for the Laudanum Project, a collection of injectable scripts designed to be used in penetration testing. @timmedin
**Course Day Descriptions**

**561.1 HANDS ON: Security Platform Analysis**

The first day of the course prepares students for real-world security challenges by giving them hands-on practice with essential Linux and Windows server and host management tools. First, students will leverage built-in and custom Linux tools to evaluate the security of host systems and servers, inspecting and extracting content from rich data sources such as image headers, browser cache content, and system logging resources. Next, students will turn their focus to performing similar analysis against remote Windows servers using built-in Windows system management tools to identify misconfigured services, scrutinize historical registry entries for USB devices, evaluate the impact of malware attacks, and analyze packet capture data. By completing these tasks, students build their skills in managing systems, applicable to post-compromise system host analysis, or defensive tasks such as defending targeted systems from persistent attack threats. By adding new tools and techniques to their arsenal, students are better prepared to complete the analysis of complex systems with greater accuracy in less time.

**Topics:** Linux Host and Server Analysis; Windows Host and Server Analysis

**561.2 HANDS ON: Enterprise Security Assessment**

In this section of the class, students investigate the critical tasks for a high-quality penetration test. We’ll look at the safest, most efficient ways to map a network and discover target systems and services. Once the systems are discovered, we look for vulnerabilities and reduce false positives with manual vulnerability verification. We’ll also look at exploitation techniques, including the use of the Metasploit Framework to exploit these vulnerabilities, accurately describing risk and further reducing false positives. Of course, exploits are not the only way to access systems, so we also leverage password-related attacks, including guessing and cracking techniques to extend our reach for a more effective and valuable penetration test.

**Topics:** Network Mapping and Discovery; Enterprise Vulnerability Assessment; Network Penetration Testing; Password and Authentication Exploitation

**561.3 HANDS ON: Web Application Assessment**

This section of the course will look at the variety of flaws present in web applications and how each of them is exploited. Students will solve challenges presented to them by exploiting web applications hands-on with the tools used by professional web application penetration testers every day. The websites students attack mirror real-world vulnerabilities including Cross-Site Scripting (XSS), SQL Injection, Command Injection, Directory Traversal, Session Manipulation and more. Students will need to exploit the present flaws and answer questions based on the level of compromise they are able to achieve.

**Topics:** Recon and Mapping; Server-side Web Application Attacks; Client-side Web Application Attacks; Web Application Vulnerability Exploitation

**561.4 HANDS ON: Mobile Device and Application Analysis**

With the accelerated growth of mobile device use in enterprise networks, organizations find an increasing need to identify expertise in the security assessment and penetration testing of mobile devices and the supporting infrastructure. In this component of the course, we examine the practical vulnerabilities introduced by mobile devices and applications, and how they relate to the security of the enterprise. Students will look at the common vulnerabilities and attack opportunities against Android and Apple iOS devices, examining data remnants from lost or stolen mobile devices, the exposure introduced by common weak application developer practices, and the threat introduced by popular cloud-based mobile applications found in many networks today.

**Topics:** Mobile Device Assessment; Mobile Device Data Harvesting; Mobile Application Analysis

**561.5 HANDS ON: Advanced Penetration Testing**

This portion of the class is designed to teach the advanced skills required in an effective penetration test to extend our reach and move through the target network. This extended reach will provide a broader and more in-depth look at the security of the enterprise. We’ll utilize techniques to pivot through compromised systems using various tunneling/pivoting techniques, bypass anti-virus and built-in commands to extend our influence over the target environment, and find issues that lesser testers may have missed. We’ll also look at some of the common mistakes surrounding poorly or incorrectly implemented cryptography and ways to take advantage of those weaknesses to access systems and data that are improperly secured.

**Topics:** Anti-Virus Evasion Techniques; Advanced Network Pivoting Techniques; Exploiting Network Infrastructure Components

**561.6 HANDS ON: Capture the Flag Challenge**

This lively session represents the culmination of the course, where attendees will apply the skills they have mastered throughout all the other sessions in a hands-on workshop. Students will participate in a larger version of the exercises presented in the class to independently reinforce skills learned throughout the course. They will then apply their newly developed skills to scan for flaws, use exploits, unravel technical challenges, and dodge firewalls, all while guided by the challenges presented by the NetWars Scoring Server. By practicing the skills in a combination workshop in which multiple focus areas are combined, participants will have the opportunity to explore, exploit, pillage, and continue to reinforce skills against a realistic target environment.

You Will Be Able To

- Use network scanning and vulnerability assessment tools to effectively map out networks and prioritize discovered vulnerabilities for effective remediation
- Use password analysis tools to identify weak authentication controls leading to unauthorized server access
- Evaluate web applications for common developer flaws leading to significant data loss conditions
- Manipulate common network protocols to maliciously reconfigure internal network traffic patterns
- Identify weaknesses in modern anti-virus signature and heuristic analysis systems
- Inspect the configuration deficiencies and information disclosure threats present on Windows and Linux servers
- Bypass authentication systems for common application implementations
- Exploit deficiencies in common cryptographic systems
- Bypass monitoring systems by leveraging IPv6 scanning and exploitation tools
- Harvest sensitive mobile device data from iOS and Android targets

“This class is a wonderful culmination of pentesting disciplines spread out over a week’s worth of hands-on labs. Significant gains in understanding and capability are imminent.”

- Chris Kelsey, Roche

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/event/sans-2018/courses](http://www.sans.org/event/sans-2018/courses)
**Automating Information Security with Python**

<table>
<thead>
<tr>
<th>Six-Day Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tue, April 3 - Sun, April 8</td>
</tr>
<tr>
<td>9:00am - 5:00pm</td>
</tr>
<tr>
<td>36 CPEs</td>
</tr>
<tr>
<td>Laptop Required</td>
</tr>
<tr>
<td>Instructor: Mark Baggett</td>
</tr>
</tbody>
</table>

**Who Should Attend**

- Security professionals who benefit from automating routine tasks so they can focus on what's most important
- Forensics Analysts who can no longer wait on someone else to develop a commercial tool to analyze artifacts
- Network Defenders who sift through mountains of logs and packets to find evildoers in their networks
- Penetration testers who are ready to advance from script kiddie to professional offensive computer operations operator
- Security professionals who want to evolve from security tool consumer to security solution provider

“SEC573 gave me exposure to tools and techniques I wouldn’t have normally considered, but now are part of my arsenal.”

- Allen C., Department of Defense

All security professionals, including Penetration Testers, Forensics Analysts, Network Defenders, Security Administrators, and Incident Responders, have one thing in common: CHANGE. Change is constant. Technology, threats, and tools are constantly evolving. If we don’t evolve with them, we’ll become ineffective and irrelevant, unable to provide the vital defenses our organizations increasingly require.

Maybe your chosen Operating System has a new feature that creates interesting forensics artifacts that would be invaluable for your investigation, if only you had a tool to access it. Often for new features and forensics artifacts, no such tool has yet been released. You could try moving your case forward without that evidence or hope that someone creates a tool before the case goes cold. Or you can write a tool yourself.

Perhaps an attacker bypassed your defenses and owned your network months ago. If existing tools were able to find the attack, you wouldn’t be in this situation. You are bleeding sensitive data and the time-consuming manual process of finding and eradicating the attacker is costing you money and hurting your organization big time. The answer is simple if you have the skills: Write a tool to automate your defenses.

Finally, what do you do when “off-the-shelf” tools and exploits fall short? As a penetration tester you need to evolve as quickly as the threats you are paid to emulate, so the answer is simple, if you have the skills: You write your own tool.

Writing a tool is easier said than done, right? Not really. Python is a simple, user-friendly language that is designed to make automating tasks that security professionals perform quick and easy. Whether you are new to coding or have been coding for years, **SEC573: Automating Information Security with Python** will have you creating programs to make your job easier and make you more efficient. This self-paced class starts from the very beginning assuming you have no prior experience or knowledge of programming. We cover all of the essentials of the language up front. If you already know the essentials, you will find that the pyWars lab environment allows advanced developers to quickly accelerate to more advanced material in the class. The self-paced style of the class will meet you where you are to let you get the most out of the class. Beyond the essentials we discuss file analysis, packet analysis, forensics artifact carving, networking, database access, website access, process execution, exception handling, object-oriented coding, and more.

This course is designed to give you the skills you need for tweaking, customizing, or outright developing your own tools. We put you on the path of creating your own tools, empowering you in automating the daily routine of today’s information security professional, and in achieving more value in less time. Again and again, organizations serious about security emphasize their need for skilled tool builders. There is a huge demand for people who can understand a problem and then rapidly develop prototype code to attack or defend against it. Join us and learn Python in-depth and fully weaponized.

**Mark Baggett** SANS Senior Instructor

Mark Baggett is the owner of Indepth Defense, an independent consulting firm that offers incident response and penetration testing services. Mark has more than 28 years of commercial and government experience ranging from software developer to chief information security officer. He is the author of the Python for Penetration testers course (SEC573). Mark has a master’s degree in information security engineering and many industry certifications, including being the 15th person in the world to receive the prestigious GIAC Security Expert certification (GSE). Mark is very active in the information security community. He is the founding president of The Greater Augusta ISSA (Information Systems Security Association) chapter, which has been extremely successful in bringing networking and educational opportunities to Augusta Information Technology workers. Since January 2011, Mark has served as the SANS Technical Advisor to the DoD, where he assists various entities in the development of information security capabilities. @MarkBaggett
Course Day Descriptions

573.1 HANDS ON: Essentials Workshop with pyWars
The course begins with a brief introduction to Python and the pyWars Capture-the-Flag game. We set the stage for students to learn at their own pace in the 100% hands-on pyWars lab environment. As more advanced students take on Python-based Capture-the-Flag challenges, students who are new to programming will start from the very beginning with Python essentials. Students will complete challenges at their own pace with a series of hands-on labs that are designed to cover a broad spectrum of Python programming topics.

Topics: Python Syntax; Variables; Math Operators; Strings; Functions; Modules; Control Statements; Introspection

573.2 HANDS ON: Essentials Workshop with MORE pyWars
You will never learn to program by staring at PowerPoint slides. The second day continues the hands-on, lab-centric approach established on day one. This section covers data structures and more detailed programming concepts. Next, we focus on invaluable tips and tricks to make you a better Python programmer and on how to debug your code.

Topics: Lists; Loops; Tuples; Dictionaries; The Python Debugger; Coding Tips, Tricks, and Shortcuts; System Arguments; ArgParser Module

573.3 HANDS ON: Defensive Python
Day three includes in-depth coverage of how defenders can use Python automation as we cover Python modules and techniques that everyone can use. Forensic professionals and offensive security professionals will also learn essential skills they will apply to their craft. We will play the role of network defenders who need to find the attackers on their network. We will discuss how to analyze network logs and packets to discover where the attackers are coming from and what they are doing. We will build scripts to empower continuous monitoring and disrupt the attackers before they exfiltrate your data.

Topics: File Operations; Python Sets; Regular Expressions; Log Parsing; Data Analysis Tools and Techniques; Long Tail/Short Tail Analysis; Geolocation Acquisition; Blacklists and Whitelists; Packet Analysis; Packet Reassembly; Payload Extraction

573.4 HANDS ON: Forensics Python
On day four we will play the role of a forensics analyst who has to carve evidence from artifacts when no tool exists to do so. Even if you don’t do forensics you will find that these skills covered on day four are foundational to every security role. We will discuss the process required to carve binary images, find appropriate data of interest in them, and extract that data. Once you have the artifact isolated, there is more analysis to be done. You will learn how to extract metadata from image files. Then we will discuss techniques for finding artifacts in other locations such as SQL databases and interacting with web pages.

Topics: Acquiring Images from Disk, Memory, and the Network; File Carving; The STRUCT Module; Raw Network Sockets and Protocols; Image Forensics and PIL; SQL Queries; HTTP Communications with Python Built-In Libraries; Web Communications with the Requests Module

573.5 HANDS ON: Offensive Python
On day five we play the role of penetration testers whose normal tricks have failed. Their attempts to establish a foothold have been stopped by modern defenses. To bypass these defenses, you will build an agent to give you access to a remote system. Similar agents can be used for incident response or systems administration, but our focus will be on offensive operations.

Topics: Network Socket Operations; Exception Handling; Process Execution; Blocking and Non-blocking Sockets; Asynchronous Operations; The Select Module; Python Objects; Argument Packing and Unpacking

573.6 HANDS ON: Capture the Flag
In this final section you will be placed on a team with other students. Working as a team, you will apply the skills and code they have developed over the previous five days as they exploit vulnerable systems, break encryption ciphers, analyze packets, parse logs, and automate code execution on remote systems. Test your skills! Prove your might!

“Best class ever! After just 2 days I’m getting comfortable with the nuances of Python. I never thought that would happen.” - JAY WILSON, NAVIENT

“Excellent class for beginners and advanced alike. It has something for everyone.” - MIKE PEREZ, DISNEY

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/sans-2018/courses
Imagine an attack surface spread throughout your organization and in the hands of every user. It moves from place to place regularly, stores highly sensitive and critical data, and sports numerous different wireless technologies all ripe for attack. You don’t need to imagine any further because this already exists today: mobile devices. These devices are the biggest attack surface in most organizations, yet these same organizations often don’t have the skills needed to assess them.

Mobile devices are no longer a convenience technology; they are an essential tool carried or worn by users worldwide, often displacing conventional computers for everyday enterprise data needs. You can see this trend in corporations, hospitals, banks, schools, and retail stores throughout the world. Users rely on mobile devices more today than ever before – we know it, and the bad guys do too.

This course is designed to give you the skills you need to understand the security strengths and weaknesses in Apple iOS, Android, and wearable devices including Apple Watch and Android Wear. With these skills, you will evaluate the security weaknesses of built-in and third-party applications. You’ll learn how to bypass platform encryption, and how to manipulate Android apps to circumvent obfuscation techniques. You’ll leverage automated and manual mobile application analysis tools to identify deficiencies in mobile app network traffic, file system storage, and inter-app communication channels. You’ll safely work with mobile malware samples to understand the data exposure and access threats affecting Android and iOS devices, and you’ll exploit lost or stolen devices to harvest sensitive mobile application data.

Understanding and identifying vulnerabilities and threats to mobile devices is a valuable skill, but it must be paired with the ability to communicate the associated risks. Throughout the course, you’ll review the ways in which we can effectually communicate threats to key stakeholders. You’ll leverage tools including Mobile App Report Cards to characterize threats for management and decision-makers, while identifying sample code and libraries that developers can use to address risks for in-house applications as well.

You’ll then use your new skills to apply a mobile device deployment penetration test in a step-by-step fashion. Starting with gaining access to wireless networks to implement man-in-the-middle attacks and finishing with mobile device exploits and data harvesting, you’ll examine each step in conducting such a test with hands-on exercises, detailed instructions, and tips and tricks learned from hundreds of successful penetration tests. By building these skills, you’ll return to work prepared to conduct your own test, and you’ll be better informed about what to look for and how to review an outsourced penetration test.

Mobile device deployments introduce new threats to organizations including advanced malware, data leakage, and the disclosure of enterprise secrets, intellectual property, and personally identifiable information assets to attackers. Further complicating matters, there simply are not enough people with the security skills needed to identify and manage secure mobile phone and tablet deployments. By completing this course, you’ll be able to differentiate yourself as being prepared to evaluate the security of mobile devices, effectively assess and identify flaws in mobile applications, and conduct a mobile device penetration test – all critical skills to protect and defend mobile device deployments.

Joshua Wright  SANS Senior Instructor

Joshua Wright is a senior technical analyst with Counter Hack, a company devoted to the development of information security challenges for education, evaluation, and competition. Through his experiences as a penetration tester, Josh has worked with hundreds of organizations on attacking and defending mobile devices and wireless systems, ethically disclosing significant product and protocol security weaknesses to well-known organizations. As an open-source software advocate, Josh has conducted cutting-edge research resulting in several software tools that are commonly used to evaluate the security of widely deployed technology targeting WiFi, Bluetooth, and ZigBee wireless systems, smart grid deployments, and the Android and Apple iOS mobile device platforms. As the technical lead of the innovative CyberCity, Josh also oversees and manages the development of critical training and educational missions for cyber warriors in the U.S. military, government agencies, and critical infrastructure providers. @joswr1ght
Course Day Descriptions

575.1 HANDS ON: Device Architecture and Common Mobile Threats

The first section of the course quickly looks at the significant threats affecting mobile device deployments, highlighted with a hands-on exercise evaluating network traffic from a vulnerable mobile banking application. As a critical component of a secure deployment, we will examine the architectural and implementation differences and similarities in Android (including Android Marshmallow), Apple iOS 10, and the Apple Watch and Google Wear platforms. We will also look at the specific implementation details of popular platform features such as iBeacon, AirDrop, App Verification, and more. Hands-on exercises will be used to interact with mobile devices running in a virtualized environment, including low-level access to installed application services and application data.

Topics: Mobile Problems and Opportunities; Mobile Device Platform Analysis; Wearable Platforms; Mobile Device Lab Analysis Tools; Mobile Device Malware Threats

575.2 HANDS ON: Mobile Platform Access and Application Analysis

With an understanding of the threats, architectural components and desired security methods, we dig deeper into iOS and Android mobile platforms focusing on sandboxing and data isolation models, and on the evaluation of mobile applications. This section is designed to help build skills in analyzing mobile device data and applications through rooting and jailbreaking Android and iOS devices and using that access to evaluate file system artifacts.

Topics: Static Application Analysis; Unlocking, Rooting, Jailbreaking Mobile Devices; Mobile Phone Data Storage and Filesystem Architecture; Network Activity Monitoring

575.3 HANDS ON: Mobile Application Reverse Engineering

One of the critical decisions you will need to make in supporting a mobile device deployment is to approve or disapprove of unique application requests from end-users in a corporate device deployment. With some analysis skills, we can evaluate applications to determine the type of access and information disclosure threats they represent. In this section we will use automated and manual application assessment tools to evaluate iOS and Android apps. We’ll build upon the static application analysis skills covered in day 2 to manipulate application components, including Android intents and iOS URL extensions. We’ll also learn and practice techniques for manipulating iOS and Android applications: method swizzling on iOS, and disassembly, modification, and reassembly of iOS apps. The day ends with a look at a standard system for evaluating and grading the security of mobile applications in a consistent way through the application report card project.

Topics: Application Report Cards; Automated Application Analysis Systems; Manipulating App Behavior

575.4 HANDS ON: Penetration Testing Mobile Devices — PART 1

An essential component of developing a secure mobile phone deployment is to perform an ethical hacking assessment. Through ethical hacking or penetration testing, we examine the mobile devices and infrastructure from the perspective of an attacker, identifying and exploiting flaws that deliver unauthorized access to data or supporting networks. Through the identification of these flaws we can evaluate the mobile phone deployment risk to the organization with practical, useful risk metrics.

Topics: Fingerprinting Mobile Devices; Wireless Network Probe Mapping; Weak Wireless Attacks; Enterprise Wireless Security Attacks; Network Manipulation Attacks; Sidejacking Attacks

575.5 HANDS ON: Penetration Testing Mobile Devices — PART 2

Continuing our look at ethical hacking and penetration testing, we turn our focus to exploiting weaknesses on iOS and Android devices. We will also examine platform-specific application weaknesses and look at the growing use of web framework attacks in mobile application exploitation.

Topics: SSL/TLS Attacks; Client-Side Injection (CSI) Attacks; Web Framework Attacks; Back-end Application Support Attacks

575.6 HANDS ON: Capture the Flag

On the last day of class we’ll pull in all the concepts and technology we’ve covered in the week for a comprehensive Capture-the-Flag (CTF) challenge. During the CTF event, you’ll have the option to participate in multiple roles, designing a secure infrastructure for the deployment of mobile phones, monitoring network activity to identify attacks against mobile devices, extracting sensitive data from a compromised iPad, and attacking a variety of mobile phones and related network infrastructure components. In the CTF, you’ll use the skills you’ve learned to practically evaluate systems and defend against attackers, simulating the realistic environment you’ll be prepared to protect when you get back to the office.

You Will Be Able To

- Use jailbreak tools for Apple iOS and Android systems
- Conduct an analysis of iOS and Android filesystem data to plunder compromised devices and extract sensitive mobile device use information
- Analyze Apple iOS and Android applications with reverse-engineering tools
- Change the functionality of Android and iOS apps to defeat anti-jailbreaking or circumvent in-app purchase requirements
- Conduct an automated security assessment of mobile applications
- Use wireless network analysis tools to identify and exploit wireless networks used by mobile devices
- Intercept and manipulate mobile device network activity
- Leverage mobile-device-specific exploit frameworks to gain unauthorized access to target devices
- Manipulate the behavior of mobile applications to bypass security restrictions

“SEC575 provides an incredible amount of information, and the hands-on labs are awesome. It is a must-have for mobile penetration testers.”

-RICHARD TAKACS, INTEGRITY360

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/sans-2018/courses
SEC617

Wireless Penetration Testing and Ethical Hacking NEW!

Who Should Attend

- Ethical hackers and penetration testers
- Network security staff
- Network and system administrators
- Incident response teams
- Information security policy decision-makers
- Technical auditors
- Information security consultants
- Wireless system engineers
- Embedded wireless system developers

Six-Day Program

Tue, April 3 - Sun, April 8
9:00am - 5:00pm

36 CPEs
Laptop Required
Instructor: Larry Pesce

This course is designed for professionals seeking a comprehensive technical ability to understand, analyze, and defend the various wireless technologies that have become ubiquitous in our environments and, increasingly, key entrance points for attackers.

The authors of SEC617, as penetration testers themselves, know that many organizations overlook wireless security as an attack surface, and therefore fail to establish required defenses and monitoring, even though wireless technologies are now commonplace in executive suites, financial departments, government offices, manufacturing production lines, retail networks, medical devices, and air traffic control systems. Given the known risks of insecure wireless technologies and the attacks used against them, SEC617 was designed to help people build the vital skills needed to identify, evaluate, and defend against these threats. These skills are "must-haves" for any high-performing security organization.

For many analysts, "wireless" was once synonymous with "WiFi," the ever-present networking technology, and many organizations deployed complex security systems to protect these networks. Today, wireless takes on a much broader meaning – not only encompassing the security of WiFi systems, but also the security of Bluetooth, ZigBee, Z-Wave, DECT, RFID, NFC, contactless smart cards, and even proprietary wireless systems. To effectively evaluate the security of wireless systems, your skillset needs to expand to include many different types of wireless technologies.

SEC617 will give you the skills you need to understand the security strengths and weaknesses of wireless systems. You will learn how to evaluate the ever-present cacophony of WiFi networks and identify the WiFi access points (APs) and client devices that threaten your organization. You will learn how to assess, attack, and exploit deficiencies in modern WiFi deployments using WPA2 technology, including sophisticated WPA2 Enterprise networks. You will gain a strong, practical understanding of the many weaknesses in WiFi protocols and how to apply that understanding to modern wireless systems. Along with identifying and attacking WiFi access points, you will learn to identify and exploit the behavioral differences in how client devices scan for, identify, and select APs, with deep insight into the behavior of the Windows 10, macOS, Apple iOS, and Android WiFi stacks.

A significant portion of the course focuses on Bluetooth and Bluetooth Low Energy (BLE) attacks, targeting a variety of devices, including wireless keyboards, smart light bulbs, mobile devices, audio streaming devices, and more. You will learn to assess a target Bluetooth device, identify the present (or absent) security controls, and apply a solid checklist to certify a device’s security for use within your organization.

Beyond analyzing WiFi and Bluetooth security threats, analysts must also understand many other wireless technologies that are widely utilized in complex systems. SEC617 provides insight and hands-on training to help analysts identify and assess the use of ZigBee and Z-Wave wireless systems used for automation, control, and smart home systems. The course also investigates the security of cordless telephony systems in the worldwide Digital Enhanced Cordless Telephony (DECT) standard, including audio eavesdropping and recording attacks.

Radio frequency identification (RFID), near field communication (NFC), and contactless smart card systems are more popular than ever in countless applications such as point of sale systems and data center access control systems. You will learn how to assess and evaluate these deployments using hands-on exercises and many organizations deployed complex security systems to protect these networks. Today, wireless systems take on a much broader meaning – not only encompassing the security of WiFi systems, but also the security of Bluetooth, ZigBee, Z-Wave, DECT, RFID, NFC, contactless smart cards, and even proprietary wireless systems. To effectively evaluate the security of wireless systems, your skillset needs to expand to include many different types of wireless technologies.

Radio frequency identification (RFID), near field communication (NFC), and contactless smart card systems are more popular than ever in countless applications such as point of sale systems and data center access control systems. You will learn how to assess and evaluate these deployments using hands-on exercises and many organizations deployed complex security systems to protect these networks. Today, wireless systems take on a much broader meaning – not only encompassing the security of WiFi systems, but also the security of Bluetooth, ZigBee, Z-Wave, DECT, RFID, NFC, contactless smart cards, and even proprietary wireless systems. To effectively evaluate the security of wireless systems, your skillset needs to expand to include many different types of wireless technologies.

SEC617 is great for someone looking for a top-to-bottom rundown in wireless attacks.”

—Garret Picchioni, Salesforce

Larry Pesce  SANS Certified Instructor

Larry is a senior security analyst with InGuardians after a long stint in security and disaster recovery in healthcare, performing penetration testing, wireless assessments, and hardware hacking. He also diverts a significant portion of his attention co-hosting the PaulDotCom Security Weekly podcast and likes to tinker with all things electronic and wireless, much to the disappointment of his family, friends, warranties, and his second Leatherman Multi-tool. Larry also co-authored Linksys WRTS4G Ultimate Hacking and Using Wireshark and Ethereal from Syngress. Larry is an Extra Class Amateur Radio operator (KB1TNF) and enjoys developing hardware and real-world challenges for the Mid-Atlantic Collegiate Cyber Defense Challenge. @haxorthematrix

For many analysts, “wireless” was once synonymous with “WiFi,” the ever-present networking technology, and many organizations deployed complex security systems to protect these networks. Today, wireless takes on a much broader meaning – not only encompassing the security of WiFi systems, but also the security of Bluetooth, ZigBee, Z-Wave, DECT, RFID, NFC, contactless smart cards, and even proprietary wireless systems. To effectively evaluate the security of wireless systems, your skillset needs to expand to include many different types of wireless technologies.

SEC617 will give you the skills you need to understand the security strengths and weaknesses of wireless systems. You will learn how to evaluate the ever-present cacophony of WiFi networks and identify the WiFi access points (APs) and client devices that threaten your organization. You will learn how to assess, attack, and exploit deficiencies in modern WiFi deployments using WPA2 technology, including sophisticated WPA2 Enterprise networks. You will gain a strong, practical understanding of the many weaknesses in WiFi protocols and how to apply that understanding to modern wireless systems. Along with identifying and attacking WiFi access points, you will learn to identify and exploit the behavioral differences in how client devices scan for, identify, and select APs, with deep insight into the behavior of the Windows 10, macOS, Apple iOS, and Android WiFi stacks.

A significant portion of the course focuses on Bluetooth and Bluetooth Low Energy (BLE) attacks, targeting a variety of devices, including wireless keyboards, smart light bulbs, mobile devices, audio streaming devices, and more. You will learn to assess a target Bluetooth device, identify the present (or absent) security controls, and apply a solid checklist to certify a device’s security for use within your organization.

Beyond analyzing WiFi and Bluetooth security threats, analysts must also understand many other wireless technologies that are widely utilized in complex systems. SEC617 provides insight and hands-on training to help analysts identify and assess the use of ZigBee and Z-Wave wireless systems used for automation, control, and smart home systems. The course also investigates the security of cordless telephony systems in the worldwide Digital Enhanced Cordless Telephony (DECT) standard, including audio eavesdropping and recording attacks.

Radio frequency identification (RFID), near field communication (NFC), and contactless smart card systems are more popular than ever in countless applications such as point of sale systems and data center access control systems. You will learn how to assess and evaluate these deployments using hands-on exercises to exploit the same kinds of flaws discovered in mass transit smart card systems, hotel guest room access systems, and more.

In addition to standards-based wireless systems, we also dig deeper into the radio spectrum using software-defined radio (SDR) systems to scour for signals. Using SDR, you will gain new insight into how widely pervasive wireless systems are deployed. With your skills in identifying, decoding, and evaluating the data these systems transmit, you will be able to spot vulnerabilities even in custom wireless infrastructures.
617.1 HANDS ON: WiFi Data Collection and Analysis
The first section of the course quickly looks at wireless threats and attack surfaces and analyzes where you will likely see non-WiFi systems deployed in modern networks. We start off with a look at fundamental analysis techniques for evaluating WiFi networks, including the identification and analysis of rogue devices, and finish with a dive into remote penetration testing techniques using compromised Windows 10 and macOS devices to pivot.
Topics: Characterize the Wireless Threat; Sniffing WiFi; Rogue Access Point (AP) Analysis

617.2 HANDS ON: WiFi Attack and Exploitation Techniques
After developing skills needed to capture and evaluate WiFi activity, we start our look at exploiting WiFi, targeting AP and client devices. We cover techniques that apply to any WiFi products, from consumer to enterprise-class devices, focusing on understanding protocol-level deficiencies that will continue to be applied throughout the course on non-WiFi wireless systems as well.
Topics: Exploiting WiFi Hotspots; WiFi Client Attacks; Exploiting WEP; Denial of Service (DoS) Attacks; WiFi Fuzzing for Bug Discovery

617.3 HANDS ON: Enterprise WiFi, DECT, and ZigBee Attacks
We finish our look at WiFi attack techniques with a detailed look at assessing and exploiting WPA2 networks. Starting with WPA2 consumer networks, we investigate the flaws associated with pre-shared key networks and WiFi Protected Setup (WPS) deployments, continuing with a look at exploiting WPA2 Enterprise networks using various Extensible Authentication Protocol (EAP) methods. We continue to investigate the security of wireless networks on day 3, switching to non-WiFi analysis with a look at exploiting the worldwide Digital Enhanced Cordless Telephony (DECT) standard to capture and export audio conversations from cordless headsets and phones. We also investigate the security of ZigBee and IEEE 802.15.4 networks, looking at cryptographic flaws, key management failures, and hardware attacks.
Topics: Attacking WPA2 Pre-Shared Key Networks; Attacking WPA2 Enterprise Networks; Attacking Digital Enhanced Cordless Telephony Deployments; Attacking ZigBee Deployments

617.4 HANDS ON: Bluetooth and Software Defined Radio Attacks
Bluetooth technology is nearly as pervasive as WiFi, with widespread adoption in smart phones, fitness trackers, wireless keyboard, smart watches, and more. In this module, we dig into the Bluetooth Classic, Enhanced Data Rate, and Low Energy protocols, including tools and techniques to evaluate target devices for vulnerabilities. Immediately following our look at Bluetooth technology, we jump into the practical application of Software Defined Radio (SDR) technology to identify, decode, and assess proprietary wireless systems. We investigate the hardware and software available for SDR systems and look at the tools and techniques to start exploring this exciting area of wireless security assessment.
Topics: Bluetooth Introduction and Attack Techniques; Bluetooth Low Energy Introduction and Attack Techniques; Practical Application of Software-Defined Radio (SDR)

617.5 HANDS ON: RFID, Smart Cards, and NFC Hacking
On day 5, we evaluate RFID technology in its multiple forms to identify the risks associated with privacy loss and tracking, while also building an understanding of both low-frequency and high-frequency RFID systems and NFC. We examine the security associated with contactless Point of Sale (PoS) terminals, including Apple Pay and Google Wallet, and proximity lock access systems from HID and other vendors. We also examine general techniques for attacking smart card systems, including critical data analysis skills needed to bypass the intended security of smart card systems used for mass transit systems, concert venues, bike rentals, and more.
Topics: RFID Overview; RFID Tracking and Privacy Attacks; Low-Frequency RFID Attacks; Exploiting Contactless RFID Smart Cards; Attacking NFC

617.6 HANDS ON: Capture-the-Flag Event
On the last day of class, we will pull together all the concepts and technology we have covered during the week in a comprehensive Capture the Flag event. In this hands-on exercise, you will have the option to participate in multiple roles: identifying unauthorized/rogue WiFi access points, attacking live and recorded WiFi networks, decoding proprietary wireless signals, exploiting smart card deficiencies, and more. During this wireless security event you will put into practice the skills you have learned in order to evaluate systems and defend against attackers, simulating the realistic environment you will be prepared to protect when you get back to the office.

Course Day Descriptions

You Will Be Able To
- Identify and locate malicious rogue access points using fre software and hardware tools.
- Conduct a penetration test against low-power wireless devices to identify control system and related security vulnerabilities.
- Identify vulnerabilities and bypass authentication mechanisms in Bluetooth networks.
- Utilize wireless capture tools to extract audio conversations and network traffic from DECT wireless phones.
- Implement a WPA2 Enterprise penetration test to exploit vulnerable wireless client systems for credential harvesting.
- Utilize Scapy to force custom packets to manipulate wireless networks in new ways, quickly building custom attack tools to meet specific penetration test requirements.
- Identify WiFi attacks using network packet captures traces and freely available analysis tools.
- Identify and exploit shortcomings in the proximity key card systems.
- Decode proprietary wireless signals using Software-Defined Radio.
- Mount a penetration test against numerous standards-based or proprietary wireless technologies.

Jumpstart your toolkit with software and hardware assessment tools supplied in class
SEC617 is a technical, hands-on penetration testing skill-development course that requires a wide variety of super-useful hardware and software tools to successfully build new skills. In this course, you will receive the SANS Wireless Assessment Toolkit (SWAT), which is a collection of hardware and software tools that will jumpstart your ability to assess wireless systems. The toolkit includes a high-powered 802.11a/b/g/n WiFi card, a long-range Bluetooth Classic/Low Energy adapter, a high-frequency RFID reader and writer, and a software-defined radio receiver. You will also receive a customized Linux software environment so you can work on assessing systems and avoid fighting hardware/software incompatibility.

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/sans-2018/courses
**SEC642**

**Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques**

Six-Day Program  
Tue, April 3 - Sun, April 8  
9:00am - 5:00pm  
36 CPEs  
Laptop Required  
Instructor: Adrien de Beaupre

Can Your Web Apps Withstand the Onslaught of Modern Advanced Attack Techniques?

Modern web applications are growing more sophisticated and complex as they utilize exciting new technologies and support ever more critical operations. Long gone are the days of basic HTML requests and responses. Even in the age of Web 2.0 and AJAX, the complexity of HTTP and modern web applications is progressing at breathtaking speed. With the demands of highly available web clusters and cloud deployments, web applications are looking to deliver more functionality in smaller packets, with a decreased strain on backend infrastructure. Welcome to an era that includes tricked-out cryptography, WebSockets, HTTP/2, and a whole lot more. Are your web application assessment and penetration testing skills ready to evaluate these impressive new technologies and make them more secure?

“SEC642 is the perfect course for someone who has a background in web app pen testing, but wants to really gain advanced skills.” - Matthew Sullivan, Webfilings

Are You Ready to Put Your Web Apps to the Test with Cutting-Edge Skills?

This pen testing course is designed to teach you the advanced skills and techniques required to test modern web applications and next-generation technologies. The course uses a combination of lecture, real-world experiences, and hands-on exercises to teach you the techniques to test the security of tried-and-true internal enterprise web technologies, as well as cutting-edge Internet-facing applications. The final course day culminates in a Capture-the-Flag competition, where you will apply the knowledge you acquired during the previous five days in a fun environment based on real-world technologies.

Hands-on Learning of Advanced Web App Exploitation Skills

We begin by exploring advanced techniques and attacks to which all modern-day complex applications may be vulnerable. We’ll learn about new web frameworks and web backends, then explore encryption as it relates to web applications, digging deep into practical cryptography used by the web, including techniques to identify the type of encryption in use within the application and methods for exploiting or abusing it. We’ll look at alternative front ends to web applications and web services such as mobile applications, and examine new protocols such as HTTP/2 and WebSockets. The final portion of the class will focus on how to identify and bypass web application firewalls, filtering, and other protection techniques.

**Adrien de Beaupre  SANS Certified Instructor**

Adrien de Beaupre works as an independent consultant in beautiful Ottawa, Ontario. His work experience includes technical instruction, vulnerability assessment, penetration testing, intrusion detection, incident response and forensic analysis. He is a member of the SANS Internet Storm Center (isc.sans.edu). He is actively involved with the information security community, and has been working with SANS since 2000. Adrien holds a variety of certifications including the GXPN, GPEN, GWAPT, GCIH, GCIA, GSEC, CISSP, OPST, and OPSA. When not geeking out he can be found with his family, or at the dojo.  

@adriendb

Register at [www.sans.org/sans-2018](http://www.sans.org/sans-2018) | 301-654-SANS (7267)
Course Day Descriptions

642.1 HANDS ON: Advanced Attacks
As applications and their vulnerabilities become more complex, penetration testers have to be able to handle advanced targets. We’ll start the course with a warm-up pen test of a small application. After our review of this exercise, we will explore some of the more advanced techniques for LFI/RFI and SQI server-based flaws. We will then take a stab at combined XSS and XSRF attacks, where we leverage the two vulnerabilities together for even greater effect. After discovering the flaws, we will then work through various ways to exploit these flaws beyond the typical means exhibited today. These advanced techniques will help penetration testers find ways to demonstrate these vulnerabilities to their organization through advanced and custom exploitation.

Topics: Review of the Testing Methodology; Using Burp Suite in a Web Penetration Test; Exploiting Local and Remote File Inclusions; Exploring Advanced Discovery Techniques for SQL Injection and Other Server-Based Flaws; Exploring Advanced Exploitation of XSS and XSRF in a Combined Attack; Learning Advanced Exploitation Techniques

You Will Be Able To
- Perform advanced Local File Include (LFI)/Remote File Include (RFI), Blind SQL injection (SQI), and Cross-Site Request Forger (XSRF) discovery and exploitation
- Exploit advanced vulnerabilities common to most backend language like Mass Assignments, Type Juggling, and Object Serialization
- Perform JavaScript-based injection against ExpressJS, Node.js, and NoSQL
- Understand the special testing methods for content management systems such as SharePoint and WordPress
- Identify and exploit encryption implementations within web applications and frameworks
- Discover XML Entity and XPath vulnerabilities in SOAP or REST web services and other datastores
- Use tools and techniques to work with and exploit HTTP/2 and Web Sockets
- Identify and bypass Web Application Firewalls and application filtering techniques to exploit the system

642.2 HANDS ON: Web Frameworks
We’ll continue exploring advanced discovery and exploitation techniques for today’s complex web applications. We’ll look at vulnerabilities that could affect web applications written in any backend language, then examine how logic flaws in applications, especially in Mass Object Assignments, can have devastating effects on security. We’ll also dig into assumptions made by core development teams of backend programming languages and learn how even something as simple as handling the data types in variables can be leveraged through the web with Type Juggling and Object Serialization. Next we’ll explore various popular applications and frameworks and how they change the discovery techniques within a web penetration test. Part of this discussion will lead us to cutting-edge technologies like the MEAN stack, where JavaScript is leveraged from the browser, web server, and backend NoSQL storage. The final section of the class examines applications in content management systems such as SharePoint and WordPress, which have unique needs and features that make testing them both more complex and more fruitful for the tester.

Topics: Web Architectures; Web Design Patterns; Languages and Frameworks; Java and Struts; PHP-Type Juggling; Logic Flaws; Attacking Object Serialization; The MEAN Stack; Content Management Systems; SharePoint; WordPress

642.3 HANDS ON: Web Cryptography
Cryptographic weaknesses are common, yet few penetration testers have the skill to investigate, attack and exploit these flaws. When we investigate web application crypto attacks, we typically target the implementation and use of cryptography in modern web applications. Many popular web programming languages or development frameworks make encryption services available to the developer, but do not inherently protect encrypted data from being attacked, or only permit the developer to use cryptography in a weak manner. These implementation mistakes are going to be our focus in this section, as opposed to the exploitation of deficiencies in the cryptographic algorithms themselves. We will also explore the various ways applications use encryption and hashing insecurely. Students will learn techniques ranging from identifying what the encryption technique is to exploiting various flaws within the encryption or hashing.

Topics: Identifying the Cryptography Used in the Web Application; Analyzing and Attacking the Encryption Keys; Exploiting Stream Cipher IV Sollisions; Exploiting Electronic Codebook (ECB) Mode Ciphers with Block Shuffling; Exploiting Cipher Block Chaining (CBC) Mode with Bit Flipping; Vulnerabilities in PKCS#7 Padding Implementations

642.4 HANDS ON: Alternative Web Interfaces
Web applications are no longer limited to the traditional HTML-based interfaces. Web services and mobile applications have become more common and are regularly being used to attack clients and organizations. As such, it has become very important that penetration testers understand how to evaluate the security of these systems. We will examine Flash, Java, Active X, and Silverlight flaws. We will explore various techniques to discover flaws within the applications and backend systems. These techniques make use of tools such as Burp Suite and other automated toolsets. We will use lab exercises to explore the newer protocols of HTTP/2 and WebSockets, exploiting flaws exposed within each of them.

Topics: Intercepting Traffic to Web Services and from Mobile Applications; Flash, Java, ActiveX, and Silverlight Vulnerabilities; SOAP and REST Web Services; Penetration Testing of Web Services; WebSocket Protocol Issues and Vulnerabilities; New HTTP/2 Protocol Issues and Penetration Testing

642.5 HANDS ON: Web Application Firewall and Filter Bypass
Applications today are using more security controls to help prevent attacks. These controls, such as Web Application Firewalls and filtering techniques, make it more difficult for penetration testers during their testing. The controls block many of the automated tools and simple techniques used to discover flaws. On this day we’ll explore techniques used to map the control and how that control is configured to block attacks. You’ll be able to map out the rule sets and determine the specifics of how the Web Application Firewall detects attacks. This mapping will then be used to determine attacks that will bypass the control. You’ll use HTML5, UNICODE, and other encodings that will enable your discovery techniques to work within the protected application.

Topics: Understanding of Web Application Firewalling and Filtering Techniques; Determining the Rule Sets Protecting the Application; Fingerprinting the Defense Techniques Used; Learning How HTML5 Injections Work; Using UNICODE, CTYPEs, and Data URIs to Bypass Restrictions; Bypassing a Web Application Firewall’s Best-Defended Vulnerabilities, XSS and SQI

642.6 HANDS ON: Capture the Flag
On this final course day you will be placed on a network and given the opportunity to complete an entire penetration test. The goal of this exercise is for you to explore the techniques, tools, and methodology you will have learned over the last five days. You’ll be able to use these skills against a realistic extranet and intranet. At the end of the day, you will provide a verbal report of the findings and methodology you followed to complete the test. Students will be provided with a virtual machine that contains the Samurai Web Testing Framework (SamuraiWTF). You will be able to use this both in the class and after leaving and returning to your jobs.

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/sans-2018/courses
SANS Training Formats

Whether you choose to attend a training class live or online, the entire SANS team is dedicated to ensuring your training experience exceeds expectations.

Live Classroom Instruction

**Featured Training Events**
Our most recommended format, live SANS training events feature SANS’s top instructors teaching multiple courses at a single time and location. This allows for:

- Focused, immersive learning without the distractions of your office environment
- Direct access to SANS Certified Instructors
- Interacting with and learning from other professionals
- Attending SANS@Night events, NetWars tournaments, vendor presentations, industry receptions, and many other activities

Our live training events in North America, serving thousands of students, are held in Orlando, Washington DC, Las Vegas, New Orleans, and San Diego. Regional events with hundreds of students are held in most major metropolitan areas during the year. See page 95 for upcoming training events in North America.

**Community SANS Courses**
The same SANS courses, courseware, and labs are taught by up-and-coming instructors in a regional area. Smaller classes allow for more extensive instructor interaction. No need to travel; commute each day to a nearby location.

**Private Classes**
Bring a SANS Certified Instructor to your location to train a group of your employees in your own environment. Save on travel and address sensitive issues or security concerns in your own environment.

**Summits**
SANS Summits focus one or two days on a single topic of particular interest to the community. Speakers and talks are curated to ensure the greatest applicability to participants.

Online Training

SANS also offers its most popular courses online, for those who cannot travel or who prefer extended self-study time. Our online courses deliver the same learning outcomes as live training, with completion and GIAC exam pass rates above 90%.

**Four flexible training formats are available to meet your unique learning preferences:**

- **OnDemand:** E-Learning Available Anytime, Anywhere
- **Simulcast:** Attend a Live SANS Training Event Without Leaving Home
- **vLive:** Live Evening Classroom Sessions That Meet Twice Each Week for Six Weeks
- **SelfStudy:** Self-Paced Training for the Disciplined Student

**All four online course formats allow you to:**

- Extend access to your course up to six months, in some cases with additional quizzes and tools
- Repeat labs to ensure proficiency with skills
- Save on travel costs
- Study at home or in your office
- Repeat labs to ensure proficiency with skills

Our OnDemand platform also allows you to test drive a SANS course. Visit [www.sans.org/demo](http://www.sans.org/demo) to select a course to preview.
Voucher Program

The SANS Voucher Program is a cybersecurity workforce training management system that allows you to easily procure and manage your organization’s training needs.

As a SANS Voucher Program participant, you will be able to:

- Provide your cybersecurity team with the highest standard of skill training and certification available
- Give employees a simple way to select and procure the training they need, when they need it
- Easily approve and manage student enrollment
- Monitor employee training progress and exam scores to ensure satisfactory completion
- Track investments, debits, and account balance for optimal budgeting

Voucher credits purchased can be applied to any live and online SANS training courses, SANS Summit events, GIAC Certifications, or certification renewals.* Credits must be used within 12 months, but the term can be extended with additional investments.

Get Started
Visit www.sans.org/vouchers and submit the contact request form to have a SANS representative in your region call or email you within 24 business hours. Within as little time as one week, your eligible team members can begin their training.

*Current exceptions from the SANS Voucher program are the Partnership program, Security Awareness training, and SANS workshops hosted at events run by other organizations.

www.sans.org/vouchers
Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

This course is designed as a logical progression point for those who have completed SEC560: Network Penetration Testing and Ethical Hacking, or for those with existing penetration testing experience. Students with the prerequisite knowledge to take this course will walk through dozens of real-world attacks used by the most seasoned penetration testers. The methodology of a given attack is discussed, followed by exercises in a real-world lab environment to solidify advanced concepts and allow for the immediate application of techniques in the workplace. Each day includes a two-hour evening bootcamp to allow for additional mastery of the techniques discussed and even more hands-on exercises. A sample of topics covered includes weaponizing Python for penetration testers, attacks against network access control (NAC) and VLAN manipulation, network device exploitation, breaking out of Linux and Windows restricted environments, IPv6, Linux privilege escalation and exploit-writing, testing cryptographic implementations, fuzzing, defeating modern OS controls such as ASLR and DEP, return-oriented programming (ROP), Windows exploit-writing, and much more!

SEC660 starts off by introducing the advanced penetration concept, and provides an overview to help prepare students for what lies ahead. The focus of day one is on network attacks, an area often left untouched by testers. Topics include accessing, manipulating, and exploiting the network. Attacks are performed against NAC, VLANs, OSPF, 802.1X, CDP, IPv6, VOIP, SSL, ARP, SNMP, and others. Day two starts off with a technical module on performing penetration testing against various cryptographic implementations. The rest of the day is spent on network booting attacks, escaping Linux restricted environments such as chroot, and escaping Windows restricted desktop environments. Day three jumps into an introduction of Python for penetration testing, Scapy for packet crafting, product security testing, network and application fuzzing, and code coverage techniques. Days four and five are spent exploiting programs on the Linux and Windows operating systems. You will learn to identify privileged programs, redirect the execution of code, reverse-engineer programs to locate vulnerable code, obtain code execution for administrative shell access, and defeat modern operating system controls such as ASLR, canaries, and DEP using ROP and other techniques. Local and remote exploits, as well as client-side exploitation techniques, are covered. The final course day is dedicated to numerous penetration testing challenges requiring you to solve complex problems and capture flags.

“..."I am very impressed at how well the instructor conveyed the material in SEC660. This is a hard topic, but I have a lot I can take home with me and practice. This material puts me at that next level.”

-ADAM LOGUE, SPECTRUM HEALTH

Who Should Attend

» Network and systems penetration testers
» Incident handlers
» Application developers
» IDS engineers

Stephen Sims  SANS Faculty Fellow

Stephen Sims is an industry expert with over 15 years of experience in information technology and security. Stephen currently works out of San Francisco as a consultant performing reverse engineering, exploit development, threat modeling, and penetration testing. Stephen has a MS in information assurance from Norwich University and is a course author and senior instructor for the SANS Institute. He is the author of SANS’s only 700-level course, SEC760: Advanced Exploit Development for Penetration Testers, which concentrates on complex heap overflows, patch diffing, and client-side exploits. Stephen is also the lead author on SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking. He holds the GIAC Security Expert (GSE) certification as well as the CISSP, CISA, Immunity NOP, and many other certifications. In his spare time Stephen enjoys snowboarding and writing music.  @Steph3n5ims

James Lyne  SANS Certified Instructor

James Lyne is Global Head of Security Research at the security firm Sophos. He is a self-professed “massive geek” and has technical expertise spanning a variety of the security domains from forensics to offensive security. James has worked with many organizations on security strategy, handled a number of severe incidents and is a frequent industry advisor. He is often a headline presenter at industry conferences. James firmly believes that one of the biggest challenges we face is making security accessible and interesting to those outside the industry. As a result, he takes every opportunity to educate on security threats and best practice — always featuring live demonstrations and scenarios of how cyber criminals operate in the real world. James has given multiple TED talks, including at the main TED event. He’s also appeared on a long list of national TV programs, including CNN, NBC, BBC News, Bill Maher and John Oliver. As a spokesperson for the industry, he is passionate about talent development, regularly participating in initiatives to identify and develop new talent.  @jameslyne
Course Day Descriptions

660.1 HANDS ON: **Network Attacks for Penetration Testers**
Day one serves as an advanced network attack module, building on knowledge gained from SEC560. The focus will be on obtaining access to the network; manipulating the network to gain an attack position for eavesdropping and attacks, and for exploiting network devices; leveraging weaknesses in network infrastructure; and taking advantage of client frailty.

**Topics:** Bypassing Network Admission Control; Impersonating Devices with Admission Control Policy Exceptions; Exploiting EAP-MD5 Authentication; Custom Network Protocol Manipulation with ettercap and Custom Filters; Multiple Techniques for Gaining Man-in-the-Middle Network Access; Exploiting OSPF Authentication to Inject Malicious Routing Updates; Using Evilgrade to Attack Software Updates; Overcoming SSL Transport Encryption Security with Sslstrip; Remote Cisco Router Configuration File Retrieval; IPv6 for Penetration Testers

---

660.2 HANDS ON: **Crypto and Post-Exploitation**
Day two starts by taking a tactical look at techniques penetration testers can use to investigate and exploit common cryptography mistakes. We finish the module with lab exercises that allow you to practice your new-found crypto attack skill set against reproduced real-world application vulnerabilities.

**Topics:** Pen Testing Cryptographic Implementations; Exploiting CBC Bit Flipping Vulnerabilities; Exploiting Hash Length Extension Vulnerabilities; Delivering Malicious Operating Systems to Devices Using Network Booting and PXE; PowerShell Essentials; Enterprise PowerShell; Post-Exploitation with PowerShell and Metasploit; Escaping Software Restrictions; Two-hour Evening Capture-the-Flag Exercise Using PXE, Network Attacks, and Local Privilege Escalation

---

660.3 HANDS ON: **Python, Scapy, and Fuzzing**
Day three starts with a focus on how to leverage Python as a penetration tester. It is designed to help people unfamiliar with Python start modifying scripts to add to their own functionality while helping seasoned Python scripters improve their skills. Once we leverage the Python skills in creative lab exercises, we move on to leveraging Scapy for custom network targeting and protocol manipulation. Using Scapy, we examine techniques for transmitting and receiving network traffic beyond what canned tools can accomplish, including IPv6.

**Topics:** Becoming Familiar with Python Types; Leveraging Python Modules for Real-World Pen Tester Tasks; Manipulating Stateful Protocols with Scapy; Using Scapy to Create a Custom Wireless Data Leakage Tool; Product Security Testing; Using Tauf for Quick Protocol Mutation Fuzzing; Optimizing Your Fuzzing Time with Smart Target Selection; Automating Target Monitoring While Fuzzing with Sulley; Leveraging Microsoft Word Macros for Fuzzing .docx files; Block-Based Code Coverage Techniques Using PAIME

---

660.4 HANDS ON: **Exploiting Linux for Penetration Testers**
Day four begins by walking through memory from an exploitation perspective as well as introducing x86 assembly and linking and loading. Processor registers are directly manipulated by testers and must be intimately understood. Disassembly is a critical piece of testing and will be used throughout the remainder of the course. We will take a look at the Linux OS from an exploitation perspective and discuss the topic of privilege escalation.

**Topics:** Stack and Dynamic Memory Management and Allocation on the Linux OS; Disassembling a Binary and Analyzing x86 Assembly Code; Performing Symbol Resolution on the Linux OS; Identifying Vulnerable Programs; Code Execution Redirection and Memory Leaks; Return-Oriented Programming (ROP); Identifying and Analyzing Stack-Based Overflows on the Linux OS; Performing Return-to-libc (ret2libc) Attacks on the Stack; Defeating Stack Protection on the Linux OS; Defeating ASLR on the Linux OS

---

660.5 HANDS ON: **Exploiting Windows for Penetration Testers**
On day five we start with covering the OS security features (ASLR, DEP, etc.) added to the Windows OS over the years, as well as Windows-specific constructs, such as the process environment block (PEB), structured exception handling (SEH), thread information block (TIB), and the Windows API. Differences between Linux and Windows will be covered. These topics are critical in assessing Windows-based applications. We then focus on stack-based attacks against programs running on the Windows OS.

**Topics:** The State of Windows OS Protections on Windows 7, 8, 10, Server 2008 and 2012; Understanding Common Windows Constructs; Stack Exploitation on Windows; Defeating OS Protections Added to Windows; Creating a Metasploit Module; Advanced Stack-Smashing on Windows; Using ROP; Building ROP Chains to Defeat DEP and Bypass ASLR; Windows 7 and 8; Porting Metasploit Modules; Client-side Exploitation; Windows Shellcode

---

660.6 HANDS ON: **Capture-the-Flag Challenge**
This day will serve as a real-world challenge for students by requiring them to utilize skills they have learned throughout the course, think outside the box, and solve a range of problems from simple to complex. A web server scoring system and Capture-the-Flag engine will be provided to score students as they capture flags. More difficult challenges will be worth more points. In this offensive exercise, challenges range from local privilege escalation to remote exploitation on both Linux and Windows systems, as well as networking attacks and other challenges related to the course material.

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/event/sans-2018/courses](www.sans.org/event/sans-2018/courses)
Vulnerabilities in modern operating systems such as Microsoft Windows 7/8, Server 2012, and the latest Linux distributions are often very complex and subtle. Yet these vulnerabilities could expose organizations to significant attacks, undermining their defenses when attacked by very skilled adversaries. Few security professionals have the skillset to discover let alone even understand at a fundamental level why the vulnerability exists and how to write an exploit to compromise it. Conversely, attackers must maintain this skillset regardless of the increased complexity. **SEC760: Advanced Exploit Development for Penetration Testers**, SANS Institute’s only 700-level course, teaches the skills required to reverse-engineer 32- and 64-bit applications, perform remote user application and kernel debugging, analyze patches for one-day exploits, and write complex exploits, such as use-after-free attacks, against modern software and operating systems.

Some of the skills you will learn in SEC760 include:

- How to write modern exploits against the Windows 7/8/10 operating systems
- How to perform complex attacks such as use-after-free, Kernel exploit techniques, one-day exploitation through patch analysis, and other advanced topics
- The importance of utilizing a Security Development Lifecycle (SDL) or Secure SDLC, along with Threat Modeling
- How to effectively utilize various debuggers and plug-ins to improve vulnerability research and speed
- How to deal with modern exploit mitigation controls aimed at thwarting success and defeating determination

“As always, I think SANS training is extremely valuable for any security professional. This course sits on top of the mountain of great SANS material.”

-Doug Rodgers, Wells Fargo

**Not sure if you are ready for SEC760?**

Take this 10 question quiz: [www.sans.org/sec760/quiz](http://www.sans.org/sec760/quiz)
Course Day Descriptions

760.1 HANDS ON: Threat Modeling, Reversing and Debugging with IDA
Many penetration testers, incident handlers, developers, and other related professionals lack reverse-engineering and debugging skills. This is a different skill than reverse-engineering malicious software. As part of the Security Development Lifecycle (SDL) and Secure-SDLC, developers and exploit writers should have experience using IDA Pro to debug and reverse their code when finding bugs or when identifying potential risks after static code analysis or fuzzing.

Topics: Security Development Lifecycle (SDL); Threat Modeling; Why IDA Is the #1 Tool for Reverse Engineering; IDA Navigation; IDA Python and the IDA IDC; IDA Plug-ins and Extensibility; Local Application Debugging with IDA; Remote Application Debugging with IDA

760.2 HANDS ON: Advanced Linux Exploitation
The ability to progress into more advanced reversing and exploitation requires an expert-level understanding of basic software vulnerabilities, such as those covered in SEC660. Heap overflows serve as a rite of passage into modern exploitation techniques. This day is aimed at bridging this gap of knowledge in order to inspire thinking in a more abstract manner, necessary for continuing further with the course. Linux can sometimes be an easier operating system to learn these techniques, serving as a productive gateway into Windows.

Topics: Linux Heap Management, Constructs, and Environment; Navigating the Heap; Abusing Macros such as unlink() and frontlink(); Function Pointer Overwrites; Format String Exploitation; Abusing Custom Doubly-Linked Lists; Defeating Linux Exploit Mitigation Controls; Using IDA for Linux Application Exploitation; Using Format String Bugs for ASLR Bypass

760.3 HANDS ON: Patch Diffing, One-Day Exploits, and Return-Oriented Shellcode
Attackers often download patches as soon as they are distributed by vendors such as Microsoft in order to find newly patched vulnerabilities. Vulnerabilities are usually disclosed privately, or even discovered in-house, allowing the vendor to more silently patch the vulnerability. This also allows the vendor to release limited or even no details at all about a patched vulnerability. Attackers are well aware of this and quickly work to find the patched vulnerability in order to take control of unpatched systems. This technique is also performed by incident handlers, IDS administrators and vendors, vulnerability and penetration testing framework companies, government entities, and others. You will use the material covered in this day to identify bugs patched by vendors and take them through to exploitation.

Topics: The Microsoft Patch Management Process and Patch Tuesday; Obtaining Patches and Patch Extraction; Binary Differing with BinDiff, patchdiff2, turbodiff, and DarunGrind4; Visualizing Code Changes and Identifying Fixes; Reversing 32-bit and 64-bit Applications and Modules; Triggering Patched Vulnerabilities; Writing One-Day Exploits; Handling Modern Exploit Mitigation Controls; Using ROP to Compiled Shellcode on the Fly (Return-Oriented Shellcode)

760.4 HANDS ON: Windows Kernel Debugging and Exploitation
The Windows Kernel is very complex and intimidating. This day aims to help you understand the Windows Kernel and the various exploit mitigations added into recent versions. You will perform Kernel debugging on various versions of the Windows OS, such as Windows 7 and 8, and learn to deal with its inherent complexities. Exercises will be performed to analyze vulnerabilities, look at exploitation techniques, and get a working exploit.

Topics: Understanding the Windows Kernel; Navigating the Windows Kernel; Modern Kernel Protections; Debugging the Windows 7/8 Kernels and Drivers; WinDbg; Analyzing Kernel Vulnerabilities and Kernel Vulnerability Types; Kernel Exploitation Techniques; Token Stealing and HAL Dispatch Table Overwrites

760.5 HANDS ON: Windows Heap Overflows and Client-Side Exploitation
The focus of this section is primarily on Windows browser and client-side exploitation. You will learn to analyze C++ vtable overflows, one of the most common mechanisms used to compromise a modern Windows system. Many of these vulnerabilities are discovered in the browser, so browser techniques will also be taught, including modern heap spraying to deal with Internet Explorer 8/9/10 and other browsers such as Firefox and Chrome. You will work towards writing exploits in the Use-After-Free/Dangling Pointer vulnerability class.

Topics: Windows Heap Management, Constructs, and Environment; Understanding the Low Fragmentation Heap (LFH); Browser-based and Client-side Exploitation; Remedial Heap Spraying; Understanding C++ vtable/vtable Behavior; Modern Heap Spraying to Determine Address Predictability; Use-after-free Attacks and Dangling Pointers; Using Custom Flash Objects to Bypass ASLR; Defeating ASLR, DEP, and Other Common Exploit Mitigation Controls

760.6 HANDS ON: Capture-the-Flag Challenge
Day 6 will feature a Capture-the-Flag event with different types of challenges taken from material taught throughout the week.

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/sans-2018/courses
Enhance Your Training Experience

Add an

**OnDemand Bundle** OR **GIAC Certification Attempt**

to your course within seven days of this event to get bundle pricing.*

---

**Extend Your Training Experience with an OnDemand Bundle**

- Four months of supplemental online review
- 24/7 online access to your course lectures, materials, quizzes, and labs
- Subject-matter-expert support to help you increase your retention of course material

*OnDemand Bundle price – $729*

---

**Get Certified with GIAC Certifications**

- Distinguish yourself as an information security leader
- 30+ GIAC cybersecurity certifications available
- Two practice exams included
- Four months of access to complete the attempt

*GIAC bundle price – $729*

---

"The course content and OnDemand delivery method have both exceeded my expectations."

-ROBERT JONES, TEAM JONES, INC.

"GIAC is the only certification that proves you have hands-on technical skills."

-CHRISTINA FORD, DEPARTMENT OF COMMERCE

---

**More Information**

[www.sans.org/ondemand/bundles](http://www.sans.org/ondemand/bundles) | [www.giac.org](http://www.giac.org)

*GIAC and OnDemand Bundles are only available for certain courses.*
Summary: Properly trained Incident Responders can hunt for and identify compromised systems, provide effective containment during a breach, and rapidly remediate an incident. They must have in-depth digital forensics knowledge of both host and network systems within the enterprise as well as know how to apply proactive threat intelligence – skills taught by SANS in FOR508, FOR572, and FOR578.

Specialized incident response and forensics skills are taught in six additional SANS courses, covering everything from Windows forensics to reverse engineering malware. Review the following pages for detailed information about all of these courses.

Who This Path Is For: Threat Hunters, Incident Responders, Cyber Threat Analysts, Forensic Examiners, Security Analysts and Engineers all utilize this training path to advance their threat hunting and responding skills.

Why This Training Is Important: This training will teach you to detect compromised and affected systems, how and when a breach occurred, what attackers took or changed, and how to contain and remediate incidents. Upon completing your focus path in Threat Hunting & Incident Response, you will be able to incorporate evidence from different sources such as networks, mobile devices, and more into your investigations, provide better findings, and get the job done faster.

“This material is directly relevant to what our analysts are doing daily. Highly useful.”
-Tom L., U.S. Air Force

“For our industry, you cannot beat the quality of SANS classes and instructors. I came back to work with a new malware case and was able to implement my skills learned in class on day one. Invaluable.”
-Melissa Sokolowski, Xerox
Rob Lee  SANS Faculty Fellow

Rob Lee is an entrepreneur and consultant in the Washington, DC area and currently the Curriculum Lead and author for digital forensic and incident response training at the SANS Institute in addition to owning his own firm. Rob has more than 15 years’ experience in computer forensics, vulnerability and exploit development, intrusion detection/prevention, and incident response. Rob graduated from the U.S. Air Force Academy and earned his MBA from Georgetown University. He served in the U.S. Air Force as a member of the 609th Information Warfare Squadron (IWS), the first U.S. military operational unit focused on information warfare. Later, he was a member of the Air Force Office of Special Investigations (AFOSI), where he led crime investigations and an incident response team. Over the next seven years, he worked directly with a variety of government agencies in the law enforcement, U.S. Department of Defense, and intelligence communities as the technical lead for vulnerability discovery and exploit development teams, lead for a cyber-forensics branch, and lead for a computer forensic and security software development team. Most recently, Rob was a Director for MANDIANT, a commercial firm focusing on responding to advanced adversaries such as the APT. Rob co-authored the book Know Your Enemy, 2nd Edition. Rob is also co-author of the MANDIANT threat intelligence report “M-Trends: The Advanced Persistent Threat.” @robtlee & @sansforensics

FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting will help you to:

» Detect how and when a breach occurred
» Identify compromised and affected systems
» Determine what attackers took or changed
» Contain and remediate incidents
» Develop key sources of threat intelligence
» Hunt down additional breaches using knowledge of the adversary

DAY 0: A 3-letter government agency contacts you to say an advanced threat group is targeting organizations like yours, and that your organization is likely a target. They won’t tell how they know, but they suspect that there are already several breached systems within your enterprise. An advanced persistent threat, aka an APT, is likely involved. This is the most sophisticated threat that you are likely to face in your efforts to defend your systems and data, and these adversaries may have been actively rummaging through your network undetected for months or even years.

This is a hypothetical situation, but the chances are very high that hidden threats already exist inside your organization’s networks. Organizations can’t afford to believe that their security measures are perfect and impenetrable, no matter how thorough their security precautions might be. Prevention systems alone are insufficient to counter focused human adversaries who know how to get around most security and monitoring tools.

This in-depth incident response and threat hunting course provides responders and threat hunting teams with advanced skills to hunt down, identify, counter, and recover from a wide range of threats within enterprise networks, including APT nation-state adversaries, organized crime syndicates, and hactivism. Constantly updated, FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting addresses today’s incidents by providing hands-on incident response and threat hunting tactics and techniques that elite responders and hunters are successfully using to detect, counter, and respond to real-world breach cases.

GATHER YOUR INCIDENT RESPONSE TEAM – IT’S TIME TO GO HUNTING!

“For508 analyzes Advanced Persistent Threat (APT) samples that are affecting our industry today. This training can’t get any better!”

-Neel Mehta, Chevron

www.sans.edu www.sans.org/cyber-guardian www.sans.org/8140

Register at www.sans.org/sans-2018  301-654-SANS (7267)
For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/sans-2018/courses

### Course Day Descriptions

#### 508.1 HANDS ON: Advanced Incident Response and Threat Hunting

Incident responders and threat hunters should be armed with the latest tools, memory analysis techniques, and enterprise methodologies to identify, track, and contain advanced adversaries and to remediate incidents. Incident response and threat hunting analysts must be able to scale their analysis across thousands of systems in their enterprise. This section examines the six-step incident response methodology as it applies to an enterprise's response to a targeted attack.

 Topics: Real Incident Response Tactics; Threat Hunting; Cyber Threat Intelligence; Threat Hunting in the Enterprise; Malware Persistence Identification; Remote and Enterprise Incident Response

#### 508.2 HANDS ON: Memory Forensics in Incident Response & Threat Hunting

Now a critical component of many incident response and threat hunting teams that detect advanced threats in their organization, memory forensics has come a long way in just a few years. Memory forensics can be extraordinarily effective at finding evidence of worms, rootkits, and advanced malware used by an APT group of attackers. This extremely popular section will introduce some of the most capable tools available and give you a solid foundation to add core and advanced memory forensic skills to your incident response and forensics capabilities.

 Topics: Memory Acquisition; Memory Forensics Analysis Process for Response and Hunting; Memory Forensics Examinations; Memory Analysis Tools

#### 508.3 HANDS ON: Intrusion Forensics

Cyber defenders have a wide variety of tools and artifacts available to identify, hunt, and track adversary activity in a network. Each attacker’s action leaves a corresponding artifact, and understanding what is left behind as footprints can be critical to both red and blue team members. Attacks follow a predictable pattern, and we focus our detective efforts on immutable portions of that pattern. In this section, we cover common attacker tradecraft and discuss the various data sources and forensic tools you can use to identify malicious activity in the enterprise.

 Topics: Advanced Evidence of Execution Detection; Window Shadow Volume Copy Analysis; Lateral Movement Adversary Tactics, Techniques, and Procedures (TTPs); Event Log Analysis for Incident Responders and Hunters

#### 508.4 HANDS ON: Timeline Analysis

Learn advanced incident response and hunting techniques uncovered via timeline analysis directly from the authors who pioneered timeline analysis tradecraft. This section will step you through the two primary methods of building and analyzing timelines created during advanced incident response, threat hunting, and forensic cases. Exercises will show analysts how to create a timeline and also how to introduce the key methods to help you use those timelines effectively in your cases.

 Topics: Timeline Analysis Overview; Memory Analysis Timeline Creation; Filesystem Timeline Creation & Analysis; Super Timeline Creation and Analysis

#### 508.5 HANDS ON: Incident Response and Hunting Across the Enterprise – Advanced Adversary and Anti-Forensics Detection

Over the years, we have observed that many incident responders and threat hunters have a challenging time finding threats without pre-built indicators of compromise or threat intelligence gathered before a breach. This is especially true in APT adversary intrusions. This advanced session will demonstrate techniques used by first responders to identify malware or forensic artifacts when very little information exists about their capabilities or hidden locations. We will discuss techniques to help funnel possibilities down to the candidates most likely to be evil malware trying to hide on the system.

 Topics: Evolution of Incident Response Scripting; Malware and Anti-Forensic Detection; Anti-Forensic Detection Methodologies; Identifying Compromised Hosts without Active Malware

#### 508.6 HANDS ON: The APT Incident Response Challenge

This incredibly rich and realistic enterprise intrusion exercise is based on a real-world advanced persistent threat (APT) group. It brings together techniques learned earlier in the week and tests your newly acquired skills in a case that simulates an attack by an advanced adversary. The challenge brings it all together using a real intrusion into a complete Windows enterprise environment. You will be asked to uncover how the systems were compromised in the initial intrusion, find other systems the adversary moved to laterally, and identify intellectual property stolen via data exfiltration. You will walk out of the course with hands-on experience investigating realistic attacks, curated by a cadre of instructors with decades of experience fighting advanced threats from attackers ranging from nation-states to financial crime syndicates and hacktivist groups.

 Topics: Identification and Scoping; Containment and Threat Intelligence Gathering; Remediation and Recovery

---

**You Will Be Able To**

- Learn and master the tools, techniques, and procedures necessary to effectively hunt, detect, and contain a variety of adversaries and to remediate incidents
- Detect and hunt unknown live, dormant, and custom malware in memory across multiple Windows systems in an enterprise environment
- Hunt through and perform incident response across hundreds of unique systems simultaneously using F-Response Enterprise and the SIFT Workstation
- Identify and track malware beaconing outbound to its command and control (C2) channel via memory forensics, registry analysis, and network connection residue
- Determine how the breach occurred by identifying the beachhead and spear phishing attack mechanisms
- Target advanced adversary anti-forensics techniques like hidden and time-stomped malware, along with utility-ware used to move in the network and maintain an attacker’s presence
- Use memory analysis, incident response, and threat hunting tools in the SIFT Workstation to detect hidden processes, malware, attacker command lines, rootkits, network connections, and more
- Track user and attacker activity second-by-second on the system you are analyzing through in-depth timeline and super-timeline analysis
- Recover data cleared using anti-forensics techniques via Volume Shadow Copy and Restore Point analysis
- Identify lateral movement and pivots within your enterprise, showing how attackers transition from system to system without detection
- Understand how the attacker can acquire legitimate credentials – including domain administrator rights – even in a locked-down environment
- Track data movement as the attackers collect critical data and shift them to exfiltration collection points
- Recover and analyze archives and .rar files used by APT-like attackers to exfiltrate sensitive data from the enterprise network
- Use collected data to perform effective remediation across the entire enterprise
FOR572
Advanced Network Forensics and Analysis

Six-Day Program
Tue, April 3 - Sun, April 8
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Philip Hagen

Who Should Attend

- Incident response team members and forensicators
- Hunt team members
- Law enforcement officers, federal agents, and detectives
- Information security managers
- Network defenders
- IT professionals
- Network engineers
- Anyone interested in computer network intrusions and investigations
- Security Operations Center personnel and information security practitioners

“...how to boil the ocean. Every network-focused investigator should be taking this course."

-Jacob Grant, Arctic Wolf Networks

Take your system-based forensic knowledge onto the wire. Incorporate network evidence into your investigations, provide better findings, and get the job done faster.

It is exceedingly rare to work any forensic investigation that doesn’t have a network component. Endpoint forensics will always be a critical and foundational skill for this career, but overlooking network communications is akin to ignoring security camera footage of a crime as it was committed. Whether you handle an intrusion incident, data theft case, employee misuse scenario, or are engaged in proactive adversary discovery, the network often provides an unparalleled view of the incident. Its evidence can provide the proof necessary to show intent, uncover attackers that have been active for months or longer, or even prove useful in definitively proving a crime actually occurred.

FOR572: Advanced Network Forensics and Analysis was built from the ground up to cover the most critical skills needed to mount efficient and effective post-incident response investigations. We focus on the knowledge necessary to expand the forensic mindset from residual data on the storage media from a system or device to the transient communications that occurred in the past or continue to occur. Even if the most skilled remote attacker compromised a system with an undetectable exploit, the system still has to communicate over the network. Without command-and-control and data extraction channels, the value of a compromised computer system drops to almost zero. Put another way: Bad guys are talking – we’ll teach you to listen.

This course covers the tools, technology, and processes required to integrate network evidence sources into your investigations, with a focus on efficiency and effectiveness. You will leave this week with a well-stocked toolbox and the knowledge to use it on your first day back on the job. We will cover the full spectrum of network evidence, including high-level NetFlow analysis, low-level tcpdump exploration, ancillary network log examination, and more. We cover how to leverage existing infrastructure devices that may contain months or years of valuable evidence as well as how to place new collection platforms while an incident is already under way.

Whether you are a consultant responding to a client’s site, a law enforcement professional assisting victims of cybercrime and seeking prosecution of those responsible, an on-staff forensic practitioner, or a member of the growing ranks of “threat hunters,” this course offers hands-on experience with real-world scenarios that will help take your work to the next level. Previous SANS SEC curriculum students and other network defenders will benefit from the FOR572 perspective on security operations as they take on more incident response and investigative responsibilities. SANS Forensics alumni from FOR500 (formerly FOR408) and FOR508 can take their existing knowledge and apply it directly to the network-based attacks that occur daily. In FOR572, we solve the same caliber of real-world problems without the use of disk or memory images.

The hands-on labs in this class cover a wide range of tools and platforms, including the venerable tcpdump and Wireshark for packet capture and analysis; NetworkMiner for artifact extraction; and open-source tools including nfldump, tcpxtract, tcpflow, and more. Newly added tools in the course include the SOF-ELK platform—a VMware appliance pre-configured with the ELK stack. This “big data” platform includes the Elasticsearch storage and search database, the Logstash ingest and parse utility, and the Kibana graphical dashboard interface. Together with the custom SOF-ELK configuration files, the platform gives forensicators a ready-to-use platform for log and NetFlow analysis. For full-packet analysis and hunting at scale, the Moloch platform is also used. Through all of the in-class labs, your shell scripting abilities will also be used to make easy work of ripping through hundreds and thousands of data records.

Philip Hagen  SANS Certified Instructor

Phil began his studies at the U.S. Air Force Academy’s Computer Science Department, where he focused on network security and was an inaugural member of the computer security extracurricular group. He served in the Air Force as a communications officer at Beale AFB and the Pentagon. Today, Phil’s career has spanned the full attack life cycle—tool development, deployment, operations, and the investigative aftermath—giving him rare and deep insight into the artifacts left behind. Phil has covered deep technical tasks, managed an entire computer forensic services portfolio, and handled executive responsibilities. He’s supported systems that demanded 24x7x365 functionality, managed a team of 85 computer forensic professionals in the national security sector, and provided forensic consulting services for law enforcement, government, and commercial clients. These experiences helped shape Phil’s role today as the DFIR strategist at Red Canary, where he supports the firm’s managed threat detection service. Phil also spends time developing and maintaining the SOF-ELK distribution, a virtual appliance free for the DFIR Community. @PhilHagen
Course Day Descriptions

572.1 HANDS ON: Off the Disk and Onto the Wire

Network data can be preserved, but only if captured directly from the wire. Whether tactical or strategic, packet capture methods are quite basic. You will re-acquaint yourself with tcpdump and Wireshark, the most common tools used to capture and analyze network packets, respectively. However, since long-term full-packet capture is still uncommon in most environments, many artifacts that can tell us about what happened on the wire in the past come from devices that manage network functions. You will learn about what kinds of devices can provide valuable evidence and at what level of granularity. We will walk through collecting evidence from one of the most common sources of network evidence, a web proxy server, then you’ll go hands-on to find and extract stolen data from the proxy yourself. The Linux SIFT virtual machine, which has been specifically loaded with a set of network forensic tools, will be your primary toolkit for the week.

Topics: Web Proxy Server Examination; Foundational Network Forensics Tools: tcpdump and Wireshark; Network Evidence Acquisition; Network Architectural Challenges and Opportunities

572.2 HANDS ON: Core Protocols & Log Aggregation/Analysis

Understanding log data and how it can guide the investigative process is an important network forensic skill. Examining network-centric logs can also fill gaps left by an incomplete or non-existent network capture. In this section, you will learn various logging mechanisms available to both endpoint and network transport devices. You will also learn how to consolidate log data from multiple sources, providing a broad corpus of evidence in one location. As the volume of log data increases, so does the need to consider automated analytic tools. You’ll use the SOF-ELK platform for post-incident log aggregation and analysis, bringing quick and decisive insight to a compromise investigation.

Topics: Hypertext Transfer Protocol (HTTP); Protocol and Logs; Domain Name Service (DNS); Protocol and Logs; Firewall, Intrusion Detection System, and Network Security Monitoring Logs; Logging Protocol and Aggregation; ELK Stack and the SOF-ELK Platform

572.3 HANDS ON: NetFlow and File Access Protocols

In this section, you will learn the contents of typical NetFlow protocols, as well as common collection architectures and analysis methods. You’ll also learn how to distill full-packet collections to NetFlow records for quick initial analysis before diving into more cumbersome pcap files. In additional, you’ll examine the File Transfer Protocol, including how to reconstruct specific files from an FTP session. While FTP is commonly used for data exfiltration, it is also an opportunity to refine protocol analysis techniques, due to its multiple-stream nature. Lastly, you’ll explore a variety of the network protocols unique to a Microsoft Windows or Windows-compatible environment. Attackers frequently use these protocols to “live off the land” within the victim’s environment. By using existing and expected protocols, adversaries can hide in plain sight and avoid deploying malware that could tip off the investigators to their presence and actions.

Topics: NetFlow Collection and Analysis; Open-Source Flow Tools; File Transfer Protocol (FTP); Microsoft Protocols

572.4 HANDS ON: Commercial Tools, Wireless, and Full-Packet Hunting

Commercial tools hold clear advantages in some situations a forensic analyst may typically encounter. Most commonly, this centers on scalability. Many open-source tools are designed for tactical or small-scale use. Whether they are used for large-scale deployments or for specific niche functionalities, these tools can immediately address many investigative needs. You’ll look at the typical areas where commercial tools in the network forensic realm tend to focus, and discuss the value each may provide for your organizational requirements or those of your clients. Additionally, we will address the forensic aspects of wireless networking.

Topics: Simple Mail Transfer Protocol (SMTP); Commercial Network Forensics; Wireless Network Forensics; Automated Tools and Libraries; Full-Packet Hunting with Moloch

572.5 HANDS ON: Encryption, Protocol Reversing, OPSEC, and Intel

Encryption is frequently cited as the most significant hurdle to effective network forensics, and for good reason. When properly implemented, encryption can be a brick wall in between an investigator and critical answers. However, technical and implementation weaknesses can be used to our advantage. Even in the absence of these weaknesses, the right analytic approach to encrypted network traffic can still yield valuable information about the content. We will discuss the basics of encryption and how to approach it during an investigation. The section will also cover flow analysis to characterize encrypted conversations.

Topics: Encoding, Encryption, and SSL; Man in the Middle; Network Protocol Reverse Engineering; Investigation OPSEC and Threat Intel

572.6 HANDS ON: Network Forensics Capstone Challenge

Students will test their understanding of network evidence and their ability to articulate and support hypotheses through presentations made to the instructor and class. The audience will include senior-level decision-makers, so all presentations must include executive summaries as well as technical details. Time permitting, students should also include recommended steps that could help to prevent, detect, or mitigate a repeat compromise.

Topics: Network Forensic Case

You Will Be Able To

- Extract files from network packet captures and proxy cache files, allowing follow-on malware analysis or definitive data loss determination
- Use historical NetFlow data to identify relevant past network occurrences, allowing accurate incident scoping
- Reverse-engineer custom network protocols to identify an attacker’s command-and-control abilities and actions
- Decrypt captured SSL traffic to identify attackers’ actions and what data they extracted from the victim
- Use data from typical network protocols to increase the fidelity of the investigation’s findings
- Identify opportunities to collect additional evidence based on the existing systems and platforms within a network architecture
- Examine traffic using common network protocols to identify patterns of activity or specific actions that warrant further investigation
- Incorporate log data into a comprehensive analytic process, filling knowledge gaps that may be far in the past
- Learn how attackers leverage man-in-the-middle tools to intercept seemingly secure communications
- Examine proprietary network protocols to determine what actions occurred on the endpoint systems
- Analyze wireless network traffic to find evidence of malicious activity
- Learn how to modify configuration on typical network devices such as firewalls and intrusion detection systems to increase the intelligence value of their logs and alerts during an investigation
- Apply the knowledge you acquire during the week in a full-day capstone exercise, modeled after real-world nation-state intrusions

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/sans-2018/courses

www.sans.edu

www.sans.edu

Bundle
OnDemand
WITH THIS COURSE
www.sans.org/ondemand

59
Six-Day Program

Tue, April 3 - Sun, April 8
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Chad Tilbury

Who Should Attend
- Information security professionals
- Incident response team members
- Law enforcement officers, federal agents, and detectives
- Media exploitation analysts
- Anyone interested in a deep understanding of Windows forensics

“This course is a must-do for all incident responders and computer security incident response team leads to be able to answer critical questions quickly and determine the scope of an incident.”
- Brad Milhorn, NTT Data Services

FOR500: Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of the Microsoft Windows operating systems. You can’t protect what you don’t understand, and understanding forensic capabilities and artifacts is a core component of information security. You’ll learn to recover, analyze, and authenticate forensic data on Windows systems. You’ll understand how to track detailed user activity on your network and how to organize findings for use in incident response, internal investigations, and civil/criminal litigation. You’ll be able to use your new skills to validate security tools, enhance vulnerability assessments, identify insider threats, track hackers, and improve security policies. Whether you know it or not, Windows is silently recording an unimaginable amount of data about you and your users. FOR500 teaches you how to mine this mountain of data.

Proper analysis requires real data for students to examine. The completely updated FOR500 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 7/8/10, Office and Office365, cloud storage, Sharepoint, Exchange, Outlook). Students leave the course armed with the latest tools and techniques and prepared to investigate even the most complicated systems they might encounter. Nothing is left out—attendees learn to analyze everything from legacy Windows XP systems to just-discovered Windows 10 artifacts.

FOR500 is continually updated. This course utilizes a brand-new intellectual property theft and corporate espionage case that took over six months to create. You work in the real world and your training should include real practice data. Our development team used incidents from their own experiences and investigations and created an incredibly rich and detailed scenario designed to immerse students in a true investigation. The case demonstrates the latest artifacts and technologies an investigator might encounter while analyzing Windows systems. The detailed step-by-step workbook meticulously outlines the tools and techniques that each investigator should follow to solve a forensic case.

“MASTER WINDOWS FORENSICS – YOU CAN’T PROTECT WHAT YOU DON’T KNOW ABOUT

Chad Tilbury  SANS Senior Instructor

Chad has nearly 20 years of experience working with government agencies, defense contractors, and Fortune 500 companies. He has served as a special agent with the Air Force Office of Special Investigations, where he conducted computer forensics examinations for a variety of crimes and ushered counter-espionage techniques into the digital age. Chad has led international forensic teams and was selected to provide computer forensic support to the United Nations Weapons Inspection Team. In addition, Chad has worked as a computer security engineer and forensic lead for a major defense contractor and served as the vice president of worldwide Internet enforcement for the Motion Picture Association of America. In that role, he managed Internet anti-piracy operations for the seven major Hollywood studios in over 60 countries. Today, Chad brings his wealth of experience to his role as technical director at CrowdStrike, where he specializes in incident response, corporate espionage, and computer forensics. In addition to being a graduate of the U.S. Air Force Academy, Chad holds B.S. and M.S. in computer science, as well as GCFA, GCHI, GREM, and ENCE certifications.  @chadtilbury
Course Day Descriptions

500.1 HANDS ON: Windows Digital Forensics and Advanced Data Triage

The Windows forensics course starts with an examination of digital forensics in today’s interconnected environments and discusses challenges associated with mobile devices, tablets, cloud storage, and modern Windows operating systems. We will discuss how modern hard drives, such as Solid State Devices (SSD), can affect the digital forensics acquisition process and how analysts need to adapt to overcome the introduction of these new technologies.

Topics: Windows Operating System Components; Core Forensic Principles; Live Response and Triage-Based Acquisition Techniques; Acquisition Review with Write Blocker; Advanced Acquisition Challenges; Windows Image Mounting and Examination; NTFS File System Overview; Document and File Metadata; File Carving; Custom Carving Signatures; Memory, Pagefile, and Unallocated Space Analysis

500.2 HANDS ON: CORE WINDOWS FORENSICS PART 1 –
Windows Registry Forensics and Analysis

Our journey continues with the Windows Registry, where the digital forensic investigator will learn how to discover critical user and system information pertinent to almost any investigation. Each examiner will learn how to navigate and examine the Registry to obtain user-profile data and system data. The course teaches forensic investigators how to prove that a specific user performed key word searches, ran specific programs, opened and saved files, perused folders, and used removable devices.

Topics: Registry Basics; Profile Users and Groups; Core System Information; User Forensic Data; Tools Utilized

500.3 HANDS ON: CORE WINDOWS FORENSICS PART 2 –
USB Devices And Shell Items

Being able to show the first and last time a file was opened is a critical analysis skill. Utilizing shortcut (LNK) and jumplist databases, we are able to easily pinpoint which file was opened and when. We will demonstrate how to examine the pagefile, system memory, and unallocated space – all difficult-to-access locations that can offer the critical data for your case.

Topics: Shell Item Forensics; USB and Bring Your Own Device (BYOD) Forensic Examinations

500.4 HANDS ON: CORE WINDOWS FORENSICS PART 3 –
Email, Key Additional Artifacts, and Event Logs

This section discusses what types of information can be relevant to an investigation, where to find email files, and how to use forensic tools to facilitate the analysis process. We will find that the analysis process is similar across different types of email stores, but the real work takes place in the preparation – finding and extracting the email files from a variety of different sources. The last part of the section will arm each investigator with the core knowledge and capability to maintain this crucial skill for many years to come.

Topics: Email Forensics; Forensicating Additional Windows OS Artifacts; Windows Event Log Analysis

500.5 HANDS ON: CORE WINDOWS FORENSICS PART 4 –
Web Browser Forensics: Firefox, Internet Explorer, and Chrome

Throughout the section, investigators will use their skills in real hands-on cases, exploring evidence created by Chrome, Firefox, and Internet Explorer along with Windows Operating System artifacts.

Topics: Browser Forensics: History, Cache, Searches, Downloads, Understanding of Browser Timestamps, Internet Explorer; Firefox; Chrome; Examination of Browser Artifacts; Tools Used

500.6 HANDS ON: Windows Forensic Challenge

This complex case will involve an investigation into one of the most recent versions of the Windows Operating System. The evidence is real and provides the most realistic training opportunity currently available. Solving the case will require that students use all of the skills gained from each of the previous sections.

Topics: Digital Forensic Case; Windows 7 Forensic Challenge

You Will Be Able To

- Perform proper Windows forensic analysis by applying key techniques focusing on Windows 7/8/10
- Use full-scale forensic tools and analysis methods to detail nearly every action a suspect accomplished on a Windows system, including who placed an artifact on the system and how, program execution, file/folder opening, geo-location, browser history, profile USB device usage, and more
- Uncover the exact time that a specific user last executed a program through Registry and Windows artifact analysis, and understand how this information can be used to prove intent in cases such as intellectual property theft, hacker-breached systems, and traditional crimes
- Determine the number of times files have been opened by a suspect through browser forensics, shortcut file analysis (LNK), e-mail analysis, and Windows Registry parsing
- Identify keywords searched by a specific user on a Windows system in order to pinpoint the files and information the suspect was interested in finding and accomplish detailed damage assessments
- Use Windows shellbags analysis tools to articulate every folder and directory that a user opened up while browsing local, removable, and network drives
- Determine each time a unique and specific USB device was attached to the Windows system, the files and folders that were accessed on it, and who plugged it in by parsing key Windows artifacts such as the Registry and log files
- Use event log analysis techniques to determine when and how users logged into a Windows system, whether via a remote session, at the keyboard, or simply by unlocking a screensaver
- Determine where a crime was committed using registry data to pinpoint the geo-location of a system by examining connected networks and wireless access points
- Use free browser forensic tools to perform detailed web browser analysis, parse raw SQLite and ESE databases, and leverage session recovery artifacts and flash cookies to identify the web activity of suspects, even if privacy cleaners and in-private browsing are used

“Labs walk through practical steps that will teach how the applications work. Love it!”

-JONATHAN SINGER, GUIDEPOINT SECURITY
Digital forensic investigators have traditionally dealt with Windows machines, but what if they find themselves in front of a new Apple Mac or iDevice? The increasing popularity of Apple devices can be seen everywhere, from coffee shops to corporate boardrooms, yet most investigators are familiar with Windows-only machines.

“We have primarily a Mac OS environment and I don’t think I could find a tenth of this information through my own research.” - Kevin Neely, Pure Storage

Times and trends change and forensic investigators and analysts need to change with them. The new FOR518: Mac Forensic Analysis course provides the tools and techniques necessary to take on any Mac case without hesitation. The intense, hands-on forensic analysis skills taught in the course will enable Windows-based investigators to broaden their analysis capabilities and have the confidence and knowledge to comfortably analyze any Mac or iOS system.

FOR518: Mac Forensic Analysis will teach you:

- Mac and iOS Fundamentals: How to analyze and parse the Hierarchical File System (HFS+) by hand and recognize the specific domains of the logical file system and Mac-specific file types.
- User Activity: How to understand and profile users through their data files and preference configurations.
- Advanced Analysis and Correlation: How to determine how a system has been used or compromised by using the system and user data files in correlation with system log files.
- Apple Technologies: How to understand and analyze many Mac and iOS specific technologies, including Time Machine, Spotlight, iCloud, Document Versions, FileVault, Continuity, and FaceTime.

FOR518: Mac Forensic Analysis aims to form a well-rounded investigator by introducing Mac and iOS forensics into a Windows-based forensics world. This course focuses on topics such as the HFS+ file system, Mac-specific data files, tracking of user activity, system configuration, analysis and correlation of Mac logs, Mac applications, and Mac-exclusive technologies. A computer forensic analyst who successfully completes the course will have the skills needed to take on a Mac or iOS forensics case.

“Forensicate Differently!”

“There exist very few MAC forensic courses and none containing as much detail as this one.”

- John Cierpial, JP Morgan Chase

Sarah Edwards  SANS Certified Instructor

A self-described Mac nerd, Sarah Edwards is a forensic analyst, author, speaker, and both author and instructor of SANS FOR518: Mac Forensic Analysis. She has been a devoted user of Apple devices for many years and has worked specifically in Mac forensics since 2004, carving out a niche for herself when this area of forensics was still new. Although Sarah appreciates digital forensics in all platforms, she has a passion for working within Apple environments and is well known for her work with cutting-edge Mac OS X and iOS, and for her forensic file system expertise. Sarah has more than 12 years of experience in digital forensics, and her passion for teaching is fueled by the ever-increasing presence of Mac devices in today’s digital forensic investigations. Sarah has worked with federal law enforcement agencies on a variety of high-profile investigations in such areas as computer intrusions, criminal cases, counter-intelligence, counter-narcotics, and counter-terrorism. Her research and analytical interests include Mac forensics, mobile device forensics, digital profiling, and malware reverse engineering.  @iamevltwin
Course Day Descriptions

518.1 HANDS ON: Mac and iOS Essentials
This section introduces the student to Mac and iOS essentials such as acquisition, timestamps, logical file system, and disk structure. Acquisition fundamentals are the same with Mac and iOS devices, but there are a few tips and tricks that can be used to successfully and easily collect Mac and iOS systems for analysis. Students comfortable with Windows forensic analysis can easily learn the slight differences on a Mac system — the data are the same, only the format differs.

Topics: Apple Essentials; Mac Essentials and Acquisition; Disks & Partitions; iOS Essentials; iOS Acquisition; iOS Backups

518.2 HANDS ON: HFS+ File System & System Triage
The building blocks of Mac and iOS forensics start with a thorough understanding of the HFS+. Utilizing a hex editor, students will learn the basic principles of the primary file system implemented on Mac OS X systems. The students will then use that information to look at a variety of great artifacts that use the file system and that are different than other operating systems students have seen in the past. Rounding out the day, students will review Mac and iOS triage data.

Topics: HFS+ File System; Extended Attributes; File System Events Store Database; Spotlight; Portable Artifacts; Mac and iOS Triage; Most Recently Used (MRU)

518.3 HANDS ON: User Data, System Configuration, and Log Analysis
This section contains a wide array of information that can be used to profile and understand how individuals use their computers. The logical Mac file system is made up of four domains: User, Local, System, and Network. The User Domain contains most of the user-related items of forensic interest. This domain consists of user preferences and configurations. The System and Local Domains contain system-specific information such as application installation, system settings and preferences, and system logs. This section details basic system information, GUI preferences, and system application data. A basic analysis of system logs can give a good understanding of how a system was used or abused. Timeline analysis tells the story of how the system was used. Each entry in a log file has a specific meaning and may be able to tell how the user interacted with the computer. The log entries can be correlated with other data found on the system to create an in-depth timeline that can be used to solve cases quickly and efficiently. Analysis tools and techniques will be used to correlate the data and help the student put the story back together in a coherent and meaningful way.

Topics: User Data and System Configuration; Log Parsing and Analysis; Timeline Analysis and Data Correlation

518.4 HANDS ON: Application Data Analysis
In addition to all the configuration and preference information found in the User Domain, the user can interact with a variety of native Apple applications, including the Internet, email, communication, photos, locational data, etc. This data can provide analysts with the who, what, where, why, and how for any investigation. This section will explore the various databases and other files where data are being stored. The student will be able to parse this information by hand without the help of a commercial tool parser.

Topics: Application Permissions; Native Application Fundamentals; Safari Browser; Apple Mail; Communication; Calendar and Reminders; Contacts; Notes; Photos; Maps; Location Data; Random Apps; Apple Watch; Third-Party Apps

518.5 HANDS ON: Advanced Analysis Topics
Mac systems implement some technologies that are available only to those with Mac and iOS devices. These include data backup with Time Machine, Document Versions, and iCloud; and disk encryption with FileVault. Other advanced topics include data hidden in encrypted containers, live response, Mac intrusion and malware analysis, and Mac memory analysis.

Topics: Live Response; Time Machine; OS X Malware and Intrusion Analysis; iCloud; Versions; Memory Acquisitions and Analysis; Password Cracking and Encrypted Containers

518.6 HANDS ON: Mac Forensics Challenge
Students will put their new Mac forensics skills to the test by running through a real-life scenario with team members.

Topics: In-Depth HFS+ File System Examination; File System Timeline Analysis; Advanced Computer Forensics Methodology; Mac Memory Analysis; File System Data Analysis; Metadata Analysis; Recovering Key Mac Files; Volume and Disk Image Analysis; Analysis of Mac Technologies including Time Machine, Spotlight, and FileVault; Advanced Log Analysis and Correlation; iDevice Analysis and iOS Artifacts

You Will Be Able To
- Parse the HFS+ file system by hand, using only a cheat sheet and a hex editor
- Determine the importance of each file system domain
- Conduct temporal analysis of a system by correlating data files and log analysis
- Profile individuals’ usage of the system, including how often they used it, what applications they frequented, and their personal system preferences
- Determine remote or local data backups, disk images, or other attached devices
- Find encrypted containers and FileVault volumes, understand keychain data, and crack Mac passwords
- Analyze and understand Mac metadata and their importance in the Spotlight database, Time Machine, and Extended Attributes
- Develop a thorough knowledge of the Safari Web Browser and Apple Mail applications
- Identify communication with other users and systems through iChat, Messages, FaceTime, Remote Login, Screen Sharing, and AirDrop
- Conduct an intrusion analysis of a Mac for signs of compromise or malware infection
- Acquire and analyze memory from Mac systems
- Acquire iOS and analyze devices in-depth

“Pound for pound, dollar for dollar, there is no other forensic training I have seen, from FTK to EnCase to anything private, that holds a candle to what was presented in this course.”

-Kevin J. Ripa,
Computer Evidence Recovery, Inc.

Bundle OnDemand
With this course
www.sans.org/ondemand
Digital Forensics and Incident Response (DFIR) professionals need Windows memory forensics training to be at the top of their game. Investigators who do not look at volatile memory are leaving evidence at the crime scene. RAM content holds evidence of user actions, as well as evil processes and furtive behaviors implemented by malicious code. It is this evidence that often proves to be the smoking gun that unravels the story of what happened on a system.

FOR526: Memory Forensics In-Depth provides the critical skills necessary for digital forensics examiners and incident responders to successfully perform live system memory triage and analyze captured memory images. The course uses the most effective freeware and open-source tools in the industry today and provides an in-depth understanding of how these tools work. FOR526 is a critical course for any serious DFIR investigator who wants to tackle advanced forensics, trusted insider, and incident response cases.

In today’s forensics cases, it is just as critical to understand memory structures as it is to understand disk and registry structures. Having in-depth knowledge of Windows memory internals allows the examiner to access target data specific to the needs of the case at hand. For those investigating platforms other than Windows, this course also introduces OSX and Linux memory forensics acquisition and analysis using hands-on lab exercises.

There is an arms race between analysts and attackers. Modern malware and post-exploitation modules increasingly employ self-defense techniques that include more sophisticated rootkit and anti-memory analysis mechanisms that destroy or subvert volatile data. Examiners must have a deeper understanding of memory internals in order to discern the intentions of attackers or rogue trusted insiders. FOR526 draws on best practices and recommendations from experts in the field to guide DFIR professionals through acquisition, validation, and memory analysis with real-world and malware-laden memory images.

MALWARE CAN HIDE, BUT IT MUST RUN

FOR526: Memory Forensics In-Depth will teach you:

- Proper Memory Acquisition: Demonstrate targeted memory capture ensuring data integrity and overcoming obstacles to acquisition/anti-acquisition behaviors
- How to Find Evil in Memory: Detect rogue, hidden, and injected processes, kernel-level rootkits, Dynamic Link Libraries (DLL) hijacking, process hollowing, and sophisticated persistence mechanisms
- Effective Step-by-Step Memory Analysis Techniques: Use process timelining, high-low level analysis, and walking the Virtual Address Descriptors (VAD) tree to spot anomalous behavior
- Best Practice Techniques: Learn when to implement triage, live system analysis, and alternative acquisition techniques and how to devise custom parsing scripts for targeted memory analysis

Alissa Torres  SANS Certified Instructor

Alissa has more than 15 years of experience in computer and network security spanning government, academic, and corporate environments. She has the deep experience and technical savvy to take on even the most difficult computer forensics challenges that come her way. Her current role as an incident response advisor at Cargill provides daily challenges “in the trenches” and demands constant technical growth. Alissa is also founder of her own firm, Sibertor Forensics, and has taught internationally in more than 10 countries. Alissa has a B.S from the University of Virginia and a M.S. in information technology from the University of Maryland. She is a GIAC Certified Forensic Analyst (GGFA), and holds the GCFE, GCCH, GSEC, CISSP, and EnCE certifications. Alissa has served as a member of the GIAC Advisory Board since 2013 and was recognized by SC Magazine as one of its “2016 Women to Watch.” @sibertor
Course Day Descriptions

526.1 HANDS ON: Foundations in Memory Analysis and Acquisition

Simply put, memory analysis has become a required skill for all incident responders and digital forensics examiners. Regardless of the type of investigation, system memory and its contents often expose the first piece of the evidential thread that, when pulled, unravels the whole picture of what happened on the target system. Where is the malware? How did the machine get infected? Where did the attacker move laterally? Or what did the disgruntled employee do on the system? What lies in physical memory can provide answers to all of these questions and more.

Topics: Why Memory Forensics?; Investigative Methodologies; The Ubuntu SIFT and Windows 8.1 Workstations; The Volatility Framework; System Architectures; Triage versus Full Memory Acquisition; Physical Memory Acquisition

526.2 HANDS ON: Unstructured Analysis and Process Exploration

Structured memory analysis using tools that identify and interpret operating system structures is certainly powerful. However, many remnants of previously allocated memory remain available for analysis, and they cannot be parsed through structure identification. What tools are best for processing fragmented data? Unstructured analysis tools! They neither know nor care about operating system structures. Instead, they examine data, extracting findings using pattern matching. You will learn how to use Bulk Extractor to parse memory images and extract investigative leads such as email addresses, network packets, and more.

Topics: Unstructured Memory Analysis; Page File Analysis; Exploring Process Structures; List Walking and Scanning; Pool Memory; Exploring Process Relationships; Exploring DLLs; Kernel Objects

526.3 HANDS ON: Investigating the User via Memory Artifacts

An incident responder (IR) is often asked to triage a system because of a network intrusion detection system alert. The Security Operations Center makes the call and requires more information due to outbound network traffic from an endpoint and the IR team is asked to respond. In this section, we cover how to enumerate active and terminated TCP connections – selecting the right plugin for the job based on the OS version.

Topics: Network Connections; Virtual Address Descriptors; Detecting Injected Code; Analyzing the Registry via Memory Analysis; User Artifacts in Memory

526.4 HANDS ON: Internal Memory Structures

Day 4 focuses on introducing some internal memory structures (such as drivers), Windows memory table structures, and extraction techniques for portable executables. As we come to the final steps in our investigative methodology, “Spotting Rootkit Behaviors” and “Extracting Suspicious Binaries,” it is important to emphasize again the rootkit paradox. The more malicious code attempts to hide itself, the more abnormal and seemingly suspicious it appears. We will use this concept to evaluate some of the most common structures in Windows memory for hooking, the IDTs and SSDTs.

Topics: Interrupt Descriptor Tables; System Service Descriptor Tables; Drivers; Direct Kernel Object Manipulation; Module Extraction; Hibernation Files; Crash Dump Files

526.5 HANDS ON: Memory Analysis on Platforms Other than Windows

Windows systems may be the most prevalent platform encountered by forensic examiners today, but most enterprises are not homogeneous. Forensic examiners and incident responders are best served by having the skills to analyze the memory of multiple platforms, including Linux and Mac—that is, platforms other than Windows.

Topics: Linux Memory Acquisition and Analysis; Mac Memory Acquisition and Analysis

526.6 HANDS ON: Memory Analysis Challenges

This final section provides students with a direct memory forensics challenge that makes use of the SANS NetWars Tournament platform. Your memory analysis skills are put to the test with a variety of hands-on scenarios involving hibernation files, Crash Dump files, and raw memory images, reinforcing techniques covered in the first five sections of the course. These challenges strengthen students’ ability to respond to typical and atypical memory forensics challenges from all types of cases, from investigating the user to isolating the malware. By applying the techniques learned earlier in the course, students consolidate their knowledge and can shore up skill areas where they feel they need additional practice.

Topics: Malware and Rootkit Behavior Detection; Persistence Mechanism Identification; Code Injection Analysis; User Activity Reconstruction; Linux Memory Image Parsing; Mac OSX Memory Image Parsing; Windows Hibernation File Conversion and Analysis; Windows Crash Dump Analysis (Using Windows Debugger)

What You Will Receive

- SIFT Workstation 3
- This course extensively uses the SIFT Workstation 3 to teach incident responders and forensic analysts how to respond to and investigate sophisticated attacks. SIFT contains hundreds of free and open-source tools, easily matching any modern forensic and incident response commercial tool suite.
  - Ubuntu LTS base
  - 64 bit-based system
  - Better memory utilization
  - Auto-DFIR package update and customizations
  - Latest forensic tools and techniques
  - VMware Appliance ready to tackle forensics
  - Cross-compatibility between Linux and Windows
  - Expanded filesystem support (NTFS, HFS, EXFAT, and more)

- Windows 8.1 Workstation with license
  - 64 bit-based system
  - A licensed virtual machine loaded with the latest forensic tools
  - VMware Appliance ready to tackle forensics

- 32 GB Course USB 3.0
  - USB loaded with memory captures, SIFT workstation 3, tools, and documentation

- SANS Memory Forensics Exercise Workbook
  - Exercise book is over 200 pages long with detailed step-by-step instructions and examples to help you become a master incident responder

- SANS DFIR cheat sheets to help use the tools
- MP3 audio files of the complete course lecture

“"This class gives good insight into incident-response skills when interacting with a team doing memory forensics.”

VENKAT LUCKYREDDY, BMS

Bundle OnDemand

With this course

www.sans.org/ondemand

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/sans-2018/courses
Cyber Threat Intelligence

Every security practitioner should attend FOR578: Cyber Threat Intelligence. This course is unlike any other technical training you have experienced. It focuses on structured analysis in order to establish a solid foundation for any security skillset and to amplify existing skills. The course will help practitioners from across the security spectrum to:

- Develop analysis skills to better comprehend, synthesize, and leverage complex scenarios
- Identify and create intelligence requirements through practices such as threat modeling
- Understand and develop skills in tactical, operational, and strategic-level threat intelligence
- Generate threat intelligence to detect, respond to, and defeat focused and targeted threats
- Learn the different sources to collect adversary data and how to exploit and pivot off of it
- Validate information received externally to minimize the costs of bad intelligence
- Create Indicators of Compromise (IOCs) in formats such as YARA, OpenIOC, and STIX
- Move security maturity past IOCs into understanding and countering the behavioral tradecraft of threats
- Establish structured analytical techniques to be successful in any security role

It is common for security practitioners to call themselves analysts. But how many of us have taken structured analysis training instead of simply attending technical training? Both are important, but very rarely do analysts focus on training on analytical ways of thinking. This course exposes analysts to new mindsets, methodologies, and techniques that will complement their existing knowledge as well as establish new best practices for their security teams. Proper analysis skills are key to the complex world that defenders are exposed to on a daily basis.

The analysis of an adversary’s intent, opportunity, and capability to do harm is known as cyber threat intelligence. Intelligence is not a data feed, nor is it something that comes from a tool. Intelligence is actionable information that answers a key knowledge gap, pain point, or requirement of an organization. This collection, classification, and exploitation of knowledge about adversaries gives defenders an upper hand against adversaries and forces defenders to learn and evolve with each subsequent intrusion they face.

Cyber threat intelligence thus represents a force multiplier for organizations looking to establish or update their response and detection programs to deal with increasingly sophisticated threats. Malware is an adversary’s tool, but the real threat is the human one, and cyber threat intelligence focuses on countering those flexible and persistent human threats with empowered and trained human defenders.

Knowledge about the adversary is core to all security teams. The red team needs to understand adversaries’ methods in order to emulate their tradecraft. The Security Operations Center needs to know how to prioritize intrusions and quickly deal with those that need immediate attention. The incident response team needs actionable information on how to quickly scope and respond to targeted intrusions. The vulnerability management group needs to understand which vulnerabilities matter most for prioritization and the risk that each one presents. The threat hunting team needs to understand adversary behaviors to search out new threats.

In other words, cyber threat intelligence informs all security practices that deal with adversaries. FOR578: Cyber Threat Intelligence will equip you, your security team, and your organization in the tactical, operational, and strategic level cyber threat intelligence skills and tradecraft required to better understand the evolving threat landscape and to accurately and effectively counter those threats.

Peter Szczepankiewicz  SANS Certified Instructor

In his former work with the military, Peter responded to network attacks, and worked with both defensive and offensive red teams. Currently, Peter is a senior security engineer with IBM. Peter believes that people lead technology, not the other way around. He works daily to glean actionable intelligence from disparate security devices for customers, making systems interoperable. “Putting together networks only to tear them apart is just plain fun,” Peter explains, “and it allows students to take the information learned from books and this hands-on experience back to their particular work place.” @s14
Course Day Descriptions

578.1 HANDS ON: **Cyber Threat Intelligence and Requirements**

Cyber threat intelligence is a rapidly growing field. However, intelligence was a profession long before the word "cyber" entered the lexicon. Understanding the key points regarding intelligence terminology, tradecraft, and impact is vital to understanding and using cyber threat intelligence. This section introduces students to the most important concepts of intelligence, analysis tradecraft, and levels of threat intelligence, and the value they can add to organizations. It also focuses on getting your intelligence program off to the right start with planning, direction, and the generation of intelligence requirements. As with all sections, the day includes immersive hands-on labs to ensure that students have the ability to turn theory into practice.

**Topics:** Case-Study: Carbanak, The Great Bank Robbery; Understanding Intelligence; Understanding Cyber Threat Intelligence; Threat Intelligence Consumption; Positioning the Team to Generate Intelligence; Planning and Direction (Developing Requirements)

578.2 HANDS ON: **The Fundamental Skillset: Intrusion Analysis**

Intrusion analysis is at the heart of threat intelligence. It is a fundamental skillset for any security practitioner who wants to use a more complete approach to addressing security. Two of the most commonly used models for assessing adversary intrusions are the "kill chain" and the "Diamond Model." These models serve as a framework and structured scheme for analyzing intrusions and extracting patterns such as adversary behaviors and malicious indicators. In this section students will participate in and be walked through multi-phase intrusions from initial notification of adversary activity to the completion of analysis of the event. The section also highlights the importance of this process in terms of structuring and defining adversary campaigns.

**Topics:** Primary Collection Source: Intrusion Analysis; Kill Chain Courses of Action; Kill Chain Deep Dive; Handling Multiple Kill Chains; Collection Source: Malware

578.3 HANDS ON: **Collection Sources**

Cyber Threat Intelligence analysts must be able to interrogate and fully understand their collection sources. Analysts do not have to be malware reverse engineers as an example but they must at least understand that work and know what data can be sought. This section continues from the previous one in identifying key collection sources for analysts. There is also a lot of available information on what is commonly referred to as open-source intelligence (OSINT). In this section students will learn to seek and exploit information from Domains, External Datasets, Transport Layer Security/Secure Sockets Layer (TLS/SSL) Certificates, and more while also structuring the data to be exploited for purposes of sharing internally and externally.

**Topics:** Case Study: Axiom; Collection Source: Domains; Case Study: GlassRAT; Collection Source: External Datasets; Collection Source: TLS Certificates; Case Study: Trickbots; Exploitation: Storing and Structuring Data

578.4 HANDS ON: **Analysis and Dissemination of Intelligence**

Many organizations seek to share intelligence but often fail to understand its value, its limitations, and the right formats to choose for each audience. Additionally, indicator and information shared without analysis is not intelligence. Structured analytical techniques such as the Analysis of Competing Hypotheses can help add considerable value to intelligence before it is disseminated. This section will focus on identifying both open-source and professional tools that are available for students as well as on sharing standards for each level of cyber threat intelligence both internally and externally. Students will learn about YARA and generate YARA rules to help incident responders, security operations personnel, and malware analysts. Students will gain hands-on experience with STIX and understand the CybOX and TAXII frameworks for sharing information between organizations. Finally, the section will focus on building the singular intrusions into campaigns and being able to communicate about those campaigns.

**Topics:** Analysis: Exploring Hypotheses; Analysis: Building Campaigns; Dissemination: Tactical; Case Study: Sony Attack; Dissemination: Operational

578.5 HANDS ON: **Higher-Order Analysis and Attribution**

A core component of intelligence analysis at any level is the ability to defeat biases and analyze information. The skills required to think critically are exceptionally important and can have an organization-wide or national-level impact. In this section, students will learn about logical fallacies and cognitive biases as well as how to defeat them. They will also learn about nation-state attribution, including when it can be of value and when it is merely a distraction. Students will also learn about nation-state-level attribution from previously identified campaigns and take away a more holistic view of the cyber threat intelligence industry to date. The class will finish with a discussion on consuming threat intelligence and actionable takeaways for students to make significant changes in their organizations once they complete the course.

**Topics:** Logical Fallacies and Cognitive Biases; Dissemination: Strategic; Case Study: Stuxnet; Fine-Tuning Analysis; Case Study: Sofacy; Attribution

Author Statements

The author team of Mike Cloppert, Chris Sperry, and Robert M. Lee originally developed FOR578 with the understanding that the community was in need of a single concise collection of tradecraft. Cloppert and Sperry initiated the development of the course with the understanding that their schedules would not permit them to be able to constantly teach it. However, it was through their thought leadership that the class has become what it is today. Their influence on the course development remains, and SANS thanks them for their leadership.

“When considering the value of threat intelligence, most individuals and organizations ask themselves three questions: What is threat intelligence? When am I ready for it? How do I use it? This class answers these questions and more at a critical point in the development of the field of threat intelligence in the wider community. The course will empower analysts of any technical background to think more critically and be prepared to face persistent and focused threats.”

- Robert M. Lee

“Threat intelligence is a powerful tool in the hands of a trained analyst. It can provide insight to all levels of a security program, from security analysts responding to tactical threats against the network to executives reporting strategic-level threats to the Board of Directors. This course will give students an understanding of the role of threat intelligence in security operations and how it can be leveraged as a game-changing resource to combat an increasingly sophisticated adversary.”

- Rebekah Brown

“Before threat intelligence was a buzzword, it was something we all used to just do as part of incident response. But I’ll admit that most of us used to do it badly. Or more accurately, ad hoc at best. We simply lacked structured models for intrusion analysis, campaign tracking, and consistent reporting of threats. Today, we need analysts trained in intelligence analysis techniques ready to perform proper campaign modeling, attribution, and threat analysis. The Cyber Threat Intelligence course teaches students all of that, as well as how to avoid cognitive biases in reporting and the use of alternative competing hypotheses in intelligence analysis. These are critical skills that most in industry today absolutely lack.”

- Jake Williams

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/event/sans-2018/courses](http://www.sans.org/event/sans-2018/courses)
Who Should Attend

> Experienced digital forensic analysts who want to extend their knowledge and experience to forensic analysis of mobile devices, especially smartphones
> Media exploitation analysts who need to master Tactical Exploitation or Document and Media Exploitation operations on smartphones and mobile devices by learning how individuals used their smartphones, whom they communicated with, and what files they accessed
> Information security professionals who respond to data breach incidents and intrusions
> Incident response teams tasked with identifying the role that smartphones played in a breach
> Law enforcement officers, federal agents, and detectives who want to master smartphone forensics and expand their investigative skills beyond traditional host-based digital forensics
> Accident reconstruction investigators who need to determine how a phone was accessed or used during specific periods of time
> IT auditors who want to learn how smartphones can expose sensitive information
> Graduates of SANS SEC575, SEC563, FOR500, FOR508, FOR572, FOR526, FOR610, or FOR585 who want to take their skills to the next level

SMARTPHONES HAVE MINDS OF THEIR OWN. DON’T MAKE THE MISTAKE OF REPORTING SYSTEM EVIDENCE AS USER ACTIVITY. IT’S TIME TO GET SMARTER!

A smartphone lands on your desk and you are tasked with determining if the user was at a specific location at a specific date and time. You rely on your forensic tools to dump and parse the data. The tools show location information tying the device to the place of interest. Are you ready to prove the user was at that location? Do you know how to take this further to place the subject at the location of interest at that specific date and time? Tread carefully, because the user may not have done what the tools are showing!

Mobile devices are often a key factor in criminal cases, intrusions, IP theft, security threats, accident reconstruction, and more. Understanding how to leverage the data from the device in a correct manner can make or break your case and your future as an expert. FOR585: Advanced Smartphone Forensics will teach you those skills.

Every time the smartphone thinks or makes a suggestion, the data are saved. It’s easy to get mixed up in what the forensic tools are reporting. Smartphone forensics is more than pressing the find evidence button and getting answers. Your team cannot afford to rely solely on the tools in your lab. You have to understand how to use them correctly to guide your investigation, instead of just letting the tool report what it believes happened on the device. It is impossible for commercial tools to parse everything from smartphones and understand how the data were put on the device. Examination and interpretation of the data is your job and this course will provide you and your organization with the capability to find and extract the correct evidence from smartphones with confidence.

“This training is valuable to me because it is allowing me the opportunity to gain the core knowledge in mobile forensics with which I will be able to train my team.” - Tyler Young, Zurich

This in-depth smartphone forensic course provides examiners and investigators with advanced skills to detect, decode, decrypt, and correctly interpret evidence recovered from mobile devices. The course features 20 hands-on labs that allow students to analyze different datasets from smart devices and leverage the best forensic tools, methods, and custom scripts to learn how smartphone data hide and can be easily misinterpreted by forensic tools. Each lab is designed to teach you a lesson that can be applied to other smartphones. You will gain experience with the different data formats on multiple platforms and learn how the data are stored and encoded on each type of smart device. The labs will open your eyes to what you are missing by relying 100% on your forensic tools.

FOR585 is continuously updated to keep up with the latest malware, smartphone operating systems, third-party applications, and encryption. This intensive six-day course offers the most unique and current instruction on the planet, and it will arm you with mobile device forensic knowledge you can immediately apply to cases you’re working on the day you leave the course.

SMARTPHONE DATA CAN’T HIDE FOREVER — IT’S TIME TO OUTSMART THE MOBILE DEVICE!

Heather Mahalik  SANS Senior Instructor

Heather has worked on high-stress and high-profile cases, investigating everything from child exploitation to Osama Bin Laden’s media. She has helped law enforcement, eDiscovery firms, and the federal government extract and manually decode artifacts used in solving investigations around the world. All told she has more than 14 years of experience in digital forensics, including eight years focused on mobile forensics—there’s hardly a device or platform she hasn’t researched or examined or a commercial tool she hasn’t used. These days Heather is the Director of Forensic Engineering at ManTech CARD. Heather previously led the mobile device team for Basis Technology, where she focused on mobile device exploitation in support of the federal government. She also worked as a forensic examiner at Stroz Friedberg and the U.S. State Department Computer Investigations and Forensics Lab, where she handled a number of high-profile cases. She has also developed and implemented forensic training programs and standard operating procedures. @HeatherMahalik
Course Day Descriptions

585.1 HANDS ON: **Malware Forensics, Smartphone Overview, and SQLite Introduction**

Although smartphone forensic concepts are similar to those of digital forensics, smartphone file system structures differ and require specialized decoding skills to correctly interpret the data acquired from the device. On this first course day, students will apply what they know to smartphone forensic handling, device capabilities, acquisition methods, and SQLite database examination and query development. Students will also become familiar with the forensic tools required to complete comprehensive examinations of smartphone data structures. Malware affects a plethora of smartphone devices. This section will examine various types of malware, how it exists on smartphones, and how to identify and analyze it. Most commercial smartphone tools help you identify malware, but none of them will allow you to tear down the malware to the level we cover in class. Up to five labs will be conducted on this first day alone!

**Topics:** The SIFT Workstation; Malware and Spyware Forensics; Introduction to Smartphones; Smartphone Handling; Forensic Acquisition Concepts of Smartphones; Smartphone Forensics Tool Overview; JTAG Forensics; Smartphone Components; Introduction to SQLite

585.2 HANDS ON: **Android Forensics**

Android devices are among the most widely used smartphones in the world, which means they will surely be part of an investigation that will come across your desk. Android devices contain substantial amounts of data that can be decoded and interpreted into useful information. However, without honing the appropriate skills for bypassing locked Androids and correctly interpreting the data stored on them, you will be unprepared for the rapidly evolving world of smartphone forensics.

**Topics:** Android Forensics Overview; Handling Locked Android Devices; Android File System Structures; Android Evidentiary Locations; Traces of User Activity on Android Devices

585.3 HANDS ON: **Android Backups and iOS Devise Forensics**

Android backups can be created for forensic analysis or by a user. Smartphone examiners need to understand the file structures and how to parse these data. Apple iOS devices contain substantial amounts of data (including deleted records) that can be decoded and interpreted into useful information. Proper handling and parsing skills are needed for bypassing locked iOS devices and correctly interpreting the data. Without iOS instruction, you will be unprepared to deal with the iOS device that will likely be a major component in a forensic investigation.

**Topics:** Android Backup Files; iOS Forensics Overview and Acquisition; iOS File System Structures; iOS Evidentiary Locations; Handling Locked iOS Devices; Traces of User Activity on iOS Devices

585.4 HANDS ON: **iOS Backups, Windows, and BlackBerry 10 Forensics**

iOS backups are extremely common and are found in the cloud and on hard drives. Not only do users create backups, we often find that our best data can be derived from creating an iOS backup for forensic investigation. We realize that not everyone examines BlackBerry and Windows Phone devices, which is why we are focusing primarily on BlackBerry 10, Windows Phone 8 and 10 and application usage. Both the Windows Phone and BlackBerry 10 sections highlight pieces of evidence that can be found on multiple smartphones. BlackBerry smartphones are designed to protect user privacy, but techniques taught on this course day will enable the investigator to go beyond what the tools decode and manually recover data residing in database files of BlackBerry device file systems. The day ends with the students challenging themselves using tools and methods learned throughout the week to recover user data from a wiped Windows Phone before embarking on a BlackBerry 10 lab that covers tying SIM cards and application usage to a device.

**Topics:** iOS Backup File Forensics; Windows Phone/Mobile Forensics; BlackBerry 10 Forensic Overview; BlackBerry 10 File System, Evidentiary Locations, and Forensic Analysis

585.5 HANDS ON: **Third-Party Application and Knock-Off Forensics**

This day starts with third-party applications across all smartphones and is designed to teach students how to leverage third-party application data and preference files to support an investigation. The rest of the day focuses heavily on secure chat applications, recovering deleted application data and attachments, mobile browser artifacts, and knock-off phone forensics. The skills learned in this section will provide you with advanced methods for decoding data stored in third-party applications across all smartphones. We will show you what the commercial tools miss and teach you how to recover these artifacts yourself.

**Topics:** Third-Party Applications Overview; Third-Party Application Artifacts; Messaging Applications and Recovering Attachments; Secure Chat Applications; Mobile Browsers; Knock-off Phone Forensics

585.6 HANDS ON: **Smartphone Forensics Capstone Exercise**

This final course day will test all that you have learned during the course. Working in small groups, students will examine three smartphone devices and solve a scenario relating to a real-world smartphone forensic investigation. Each group will independently analyze the three smartphones, manually decode data, answer specific questions, form an investigation hypothesis, develop a report, and present findings.

**You Will Be Able To**

- Select the most effective forensic tools, techniques, and procedures for critical analysis of smartphone data
- Reconstruct events surrounding a crime using information from smartphones, including timeline development and link analysis (e.g., who communicated with whom, where, and when)
- Understand how smartphone file systems store data, how they differ, and how the evidence will be stored on each device
- Interpret file systems on smartphones and locate information that is not generally accessible to users
- Identify how the evidence got onto the mobile device – we’ll teach you how to know if the user created the data, which will help you avoid the critical mistake of reporting false evidence obtained from tools
- Incorporate manual decoding techniques to recover deleted data stored on smartphones and mobile devices
- Tie a user to a smartphone at a specific date/time and at various locations
- Recover hidden or obfuscated communication from applications on smartphones
- Decrypt or decode application data that are not parsed by your forensic tools
- Detect smartphones compromised by malware and spyware using forensic methods
- Decompile and analyze mobile malware using open-source tools
- Handle encryption on smartphones and bypass, crack, and/or decode lock codes manually recovered from smartphones, including cracking iOS backup files that were encrypted with iTunes
- Understand how data are stored on smartphone components (SD cards) and how encrypted data can be examined by leveraging the smartphone
- Extract and use information from smartphones and their components, including Android, iOS, BlackBerry 10, Windows Phone, Chinese knock-offs, and SD cards (bonus labs available focusing on BlackBerry, BlackBerry backups, Nokia [Symbian], and SIM card decoding)
- Perform advanced forensic examinations of data structures on smartphones by diving deeper into underlying data structures that many tools do not interpret
- Analyze SQLite databases and raw data dumps from smartphones to recover deleted information
- Perform advanced data-coring techniques on smartphones to validate results and extract missing or deleted data
- Apply the knowledge you acquire during the course to conduct a full-day smartphone capstone event involving multiple devices and modeled after real-world smartphone investigations

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/event/sans-2018/courses](http://www.sans.org/event/sans-2018/courses)
Learn to turn malware inside out! This popular course explores malware analysis tools and techniques in depth. FOR610 training has helped forensic investigators, incident responders, security engineers, and IT administrators acquire the practical skills to examine malicious programs that target and infect Windows systems.

Understanding the capabilities of malware is critical to an organization’s ability to derive threat intelligence, respond to information security incidents, and fortify defenses. This course builds a strong foundation for reverse-engineering malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger, and many other freely available tools.

The course begins by establishing the foundation for analyzing malware in a way that dramatically expands upon the findings of automated analysis tools. You will learn how to set up a flexible laboratory to examine the inner workings of malicious software, and how to use the lab to uncover characteristics of real-world malware samples. You will also learn how to redirect and intercept network traffic in the lab to explore the specimen’s capabilities by interacting with the malicious program.

Malware is often obfuscated to hinder analysis efforts, so the course will equip you with the skills to unpack executable files. You will learn how to dump such programs from memory with the help of a debugger and additional specialized tools, and how to rebuild the files’ structure to bypass the packer’s protection. You will also learn how to examine malware that exhibits rootkit functionality to conceal its presence on the system, employing code analysis and memory forensics approaches to examining these characteristics.

FOR610 malware analysis training also teaches how to handle malicious software that attempts to safeguard itself from analysis. You will learn how to recognize and bypass common self-defensive measures, including code injection, sandbox evasion, flow misdirection, and other measures.

Hands-on workshop exercises are a critical aspect of this course. They enable you to apply malware analysis techniques by examining malicious software in a controlled and systematic manner. When performing the exercises, you will study the supplied specimens’ behavioral patterns and examine key portions of their code. To support these activities, you will receive pre-built Windows and Linux virtual machines that include tools for examining and interacting with malware.

Lenny Zeltser  SANS Senior Instructor

Aply called the “Yoda” of malware analysis by his students, Lenny Zeltser keeps his eye on the big picture and focuses on the sum of events rather than individual occurrences. He lives by that philosophy and brings it to his job and classroom. A seasoned business and technology leader with extensive information security expertise, Lenny started his professional journey in a variety of technical Infosec roles before serving as the national lead of the U.S. security consulting practice at a major cloud services provider. Later in his career he oversaw a portfolio of security services at a Fortune 500 technology company. Today, as VP of Products at Minerva Labs, Lenny designs and builds creative anti-malware products. Lenny also developed the Linux toolkit REMnux to make it easier to use a variety of freely available malware analysis tools, many of which run well on Linux but can be difficult to find and install. Lenny earned the prestigious GIAC Security Expert professional designation, and he currently serves on the Board of Directors of the SANS Technology Institute. Lenny holds a bachelor’s degree in computer science from the University of Pennsylvania and a master’s in business administration from MIT Sloan and is the co-author of four books on malware, network security, and digital forensics.  @lennyzeltser
Course Day Descriptions

610.1 HANDS ON: Malware Analysis Fundamentals
Section one lays the groundwork for malware analysis by presenting the key tools and techniques useful for examining malicious programs. You will learn how to save time by exploring Windows malware in two phases. Behavioral analysis focuses on the program’s interactions with its environment, such as the registry, the network, and the file system. Code analysis focuses on the specimen’s code and makes use of a disassembler and debugger tools such as IDA Pro and OllyDbg. You will learn how to set up a flexible laboratory to perform such analysis in a controlled manner, and set up such a lab on your laptop using the supplied Windows and Linux (Remnux) virtual machines. You will then learn how to use the key analysis tools by examining a malware sample in your lab—with guidance and explanations from the instructor—to reinforce the concepts discussed throughout the day.

Topics: Assembling a Toolkit for Effective Malware Analysis; Examining Static Properties of Suspicious Programs; Performing Behavioral Analysis of Malicious Windows Executables; Performing Static and Dynamic Code Analysis of Malicious Windows Executables; Interacting with Malware in a Lab to Derive Additional Behavioral Characteristics

610.2 HANDS ON: Reversing Malicious Code
Section two focuses on examining malicious Windows executables at the assembly level. You will discover approaches for studying inner workings of a specimen by looking at it through a disassembler and, at times, with the help of a debugger. The section begins with an overview of key code-reversing concepts and presents a primer on essential x86 intel assembly concepts, such as instructions, function calls, variables, and jumps. You will also learn how to examine common assembly constructs, such as functions, loops, and conditional statements. The material will then build on this foundation and expand your understanding to incorporate 64-bit malware, given its growing popularity. Throughout the discussion, you will learn to recognize common characteristics at a code level, including HTTP command and control, keylogging, and command execution.

Topics: Understanding Core x86 Assembly Concepts to Perform Malicious Code Analysis; Identifying Key Assembly Logic Structures with a Disassembler; Following Program Control Flow to Understand Decision Points During Execution; Recognizing Common Malware Characteristics at the Windows API Level (Registry Manipulation, Keylogging, HTTP Communications, Droppers); Extending Assembly Knowledge to Include x64 Code Analysis

610.3 HANDS ON: Malicious Web and Document Files
Section three focuses on examining malicious web pages and documents, which adversaries can use to directly perform malicious actions on the infected system and launch attacks that lead to the installation of malicious executables. The section begins by discussing how to examine suspicious websites that might host client-side exploits. Next, you will learn how to de-obfuscate malicious scripts with the help of script debuggers and interpreters, examine Microsoft Office macros, and assess the threats associated with PDF and RTF files using several techniques.

Topics: Interacting with Malicious Websites to Assess the Nature of Their Threats; De-obfuscating Malicious JavaScript Using Debuggers and Interpreters; Analyzing Suspicious PDF Files; Examining Malicious Microsoft Office Documents, Including Files with Macros; Analyzing Malicious RTF Document Files

610.4 HANDS ON: In-Depth Malware Analysis
Section four builds on the approaches to behavioral and code analysis introduced earlier in the course, exploring techniques for uncovering additional aspects of the functionality of malicious programs. The section begins by discussing how to handle packed malware. We will examine ways to identify packers and strip away their protection with the help of a debugger and other utilities. We will also walk through the analysis of malware that employs multiple technologies to conceal its true nature, including the use of registry, obfuscated JavaScript and PowerShell scripts, and shellcode. Finally, we will learn how malware implements Usermode rootkit functionality to perform code injection and API hooking, examining this functionality from both code and memory forensics perspectives.

Topics: Recognizing Packed Malware; Getting Started with Unpacking; Using Debuggers for Dumping Packed Malware from Memory; Analyzing Multi-Technology and Fileless Malware; Code Injection and API Hooking; Using Memory Forensics for Malware Analysis

610.5 HANDS ON: Examining Self-Defending Malware
Section five takes a close look at the techniques malware authors commonly employ to protect malicious software from being examined. You will learn how to recognize and bypass anti-analysis measures designed to slow you down or misdirect you. In the process, you will gain more experience expanding static and dynamic analysis of other processes. You will also expand your understanding of how malware authors safeguard the data that they embed inside malicious executables. As with the other topics covered throughout the course, you will be able to experiment with such techniques during hands-on exercises.

Topics: Analyzing Malicious Microsoft Office (Word, Excel, PowerPoint) Documents; Analyzing Malicious Adobe PDF Documents; Analyzing Memory to Assess Malware Characteristics and Reconstruct Infection Artifacts; Using Memory Forensics to Analyze Rootkit Infections

610.6 HANDS ON: Malware Analysis Tournament
Section six assigns students to the role of a malware analyst working as a member of an incident response or forensics team. Students are presented with a variety of hands-on challenges involving real-world malware in the context of a fun tournament. These challenges further a student’s ability to respond to typical malware-reversing tasks in an instructor-led lab environment and offer additional learning opportunities. Moreover, the challenges are designed to reinforce skills covered in the first five sections of the course, making use of the hugely popular SANS NetWars tournament platform. By applying the techniques learned earlier in the course, students solidify their knowledge and can shine up skill areas where they feel they need additional practice. Students who score the highest in the malware analysis challenge will be awarded the coveted SANS Lethal Forensicator coin.

Topics: Behavioral Malware Analysis; Dynamic Malware Analysis (Using a Debugger); Static Malware Analysis (Using a Disassembler); JavaScript Deobfuscation; PDF Document Analysis; Office Document Analysis; Memory Analysis

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/sans-2018/courses

You Will Be Able To
- Build an isolated, controlled laboratory environment for analyzing code and behavior of malicious programs
- Employ network and system-monitoring tools to examine how malware interacts with the file system, registry, network, and other processes in a Windows environment
- Uncover and analyze malicious JavaScript and VBScript components of web pages, which are often used by exploit kits for drive-by attacks
- Control relevant aspects of the malicious program’s behavior through network traffic interception and code patching to perform effective malware analysis
- Use a disassembler and a debugger to examine the inner workings of malicious Windows executables
- Bypass a variety of packers and other defensive mechanisms designed by malware authors to misdirect, confuse and otherwise slow down the analyst
- Recognize and understand common assembly-level patterns in malicious code, such as DLL injection and anti-analysis measures
- Assess the threat associated with malicious documents, such as PDF and Microsoft Office files
- Derive Indicators of Compromise (IOCs) from malicious executables to strengthen incident response and threat intelligence efforts
Securing Approval and Budget for Training

Write a formal request

- All organizations are different, but because training requires a significant investment of both time and money, most successful training requests are made via a written document (short memo and/or a few powerpoint slides) that justifies the need and benefit. Most managers will respect and value the effort.
- Provide all the necessary information in one place. In addition to your request, provide all the right context by including the summary pages on Why SANS?, the Training Roadmap, the instructor bio, and additional benefits available at our live events or online.

Be specific

- How does the course relate to the job you need to be doing? Place the particular course you wish to take into the context on the SANS Career Roadmap. Are you establishing baseline skills? Transitioning to a more focused role? Decision-makers need to understand the plan and context for the decision.
- Highlight specifics of what you will be able to do afterwards. Each SANS course description includes a section titled “You Will Be Able To.” Be sure to include these in your request so that you make the benefits clear. The clearer the match between the training and what you need to do at work, the better.

Establish longer-term expectations

- Information security is a specialized career path within IT, with practices that evolve as attacks change. Because of this, organizations should expect to spend 6%-10% of salaries to keep professionals current and improve their skills. Training for such a dynamic field is an annual, per-person expense—not a once-and-done item.
- Take a GIAC Certification exam to prove the training worked. Employers value the validation of learning that passing a GIAC exam offers. Exams are psychometrically designed to establish competency for related job tasks.
- Consider offering trade-offs for the investment. Many professionals build annual training expense into their employment agreements even before joining a company. Some offer to stay for a year after they complete the training.
Summary: Professional security managers need broad and proven knowledge of policy, standards and practices in order to provide the greatest level of security to their organizations. They also need to speak their technicians’ language, and design security plans that withstand attack from all angles. SANS’s specialized management, audit, and legal courses deliver the tools and techniques required to lead with confidence.

More than 10 advanced and specialized training options in this practice area are detailed on the following pages.

Who This Path Is For: CISOs, IT directors, or others with responsibility for managing their organization’s security operations benefit from the experience-rich instruction in SANS management, audit, and legal courses. Security, system, and network administrators who are pursuing a CISSP® or a new management role should also prepare themselves for this type of training.

Why This Training Is Important: Professionals who train and certify in these skills are the leaders of cybersecurity. They master the specific techniques and tools needed to implement and audit the Critical Security Controls, they have a firm understanding of the eight domains of knowledge covered in the CISSP®, they can communicate information security best practices to executives and technical teams, and they are designing the Security Operation Centers of the future.

Software Security

Specialists in software security can find detailed information about three additional SANS courses available for SANS 2018 on page 87.

“SANS offers the best security training available.”

-David M., U.S. Air Force
This completely updated course is designed to empower advancing managers who want to get up to speed quickly on information security issues and terminology. You won’t just learn about security, you will learn how to manage security. Lecture sections are intense; the most common student comment is that it’s like drinking from a fire hose. The diligent manager will learn vital, up-to-date knowledge and skills required to supervise the security component of any information technology project. Additionally, the course has been engineered to incorporate the NIST Special Publication 800 (series) guidance so that it can be particularly useful to U.S. government managers and supporting contractors.

Essential security topics covered in this management track include network fundamentals and applications, power, cooling and safety, architectural approaches to defense in depth, cyber attacks, vulnerability assessment and management, security policies, contingency and continuity planning, awareness management, risk management analysis, incident handling, web application security, and offensive and defensive information warfare, culminating with our management practicum. The material uses Knowledge Compression™ special charts, and other proprietary SANS techniques to help convey the key points of critical slides and keep the information flow rate at a pace senior executives demand every teaching hour of the course. The course has been evaluated and approved by CompTIA’s CAQC program for Security+ 2008 to ensure that managers and their direct reports have a common baseline for security terminology and concepts. You will be able to put what you learn into practice the day you get back into the office.

Knowledge Compression™

Maximize your learning potential!

Knowledge Compression™ is an optional add-on feature to a SANS class that aims to maximize the absorption and long-term retention of large amounts of data over a relatively short period of time. Through the use of specialized training materials, in-class reviews, examinations and test-taking instruction, Knowledge Compression™ ensures students have a solid understanding of the information presented to them. By attending classes that feature this advanced training product, you will experience some of the most intense and rewarding training programs SANS has to offer, in ways that you never thought possible!
512.1 Managing the Enterprise, Planning, Network, and Physical Plant
The course starts with a whirlwind tour of the information an effective IT security manager must know to function in today’s environment. We will cover safety, physical security, and how networks and the related protocols like TCP/IP work, and equip you to review network designs for performance, security, vulnerability scanning, and return on investment. You will learn more about secure IT operations in a single day than you ever thought possible.

**Topics:** Budget Awareness and Project Management; The Network Infrastructure; Computer and Network Addressing; IP Terminology and Concepts; Vulnerability Management; Managing Physical Safety, Security, and the Procurement Process

512.2 IP Concepts, Attacks Against the Enterprise, and Defense-in-Depth
This course section examines information assurance foundations, which are presented in the context of both current and historical computer security threats, and how they have impacted confidentiality, integrity, and availability. You will also learn the methods of the attack and the importance of managing attack surface.

**Topics:** Attacks Against the Enterprise; Defense in Depth; Managing Security Policy; Access Control and Password Management

512.3 Secure Communications
This course section examines various cryptographic tools and technologies and how they can be used to secure a company’s assets. A related area called steganography, or information hiding, is also covered. Learn how malware and viruses often employ cryptographic techniques in an attempt to evade detection. We will learn about managing privacy issues in communications and investigate web application security.

**Topics:** Cryptography; Wireless Network Security; Steganography; Managing Privacy; Web Communications and Security; Operations Security, Defensive and Offensive Methods

512.4 The Value of Information
On this day we consider the most valuable resource an organization has: its information. You will learn about intellectual property, incident handling, and how to identify and better protect the information that is the real value of your organization. We will then formally consider how to apply everything we have learned, as well as practice briefing management on our risk architecture.

**Topics:** Managing Intellectual Property; Incident Handling Foundations; Information Warfare; Disaster Recovery/Contingency Planning; Managing Ethics; IT Risk Management

512.5 Management Practicum
On the fifth and final day, we pull it all together and apply the technical knowledge to the art of management. The management practicum covers a number of specific applications and topics concerning information security. We’ll explore proven techniques for successful and effective management, empowering you to immediately apply what you have learned your first day back at the office.

**Topics:** The Mission; Globalization; IT Business and Program Growth; Security and Organizational Structure; Total Cost of Ownership; Negotiations; Fraud; Legal Liability; Technical People

**You Will Be Able To**
- Speak the same language as a manager or auditor as system, security, and network administrators
- Establish a minimum standard for IT management knowledge, skills, and abilities.
- I keep running into managers who don’t know TCP/IP, and that is OK; but then they don’t know how to calculate total cost of ownership (TCO), leaving me quietly wondering what they do know
- Save the up-and-coming generation of senior and rapidly advancing managers a world of pain by sharing the things we wish someone had shared with us. As the saying goes, it is OK to make mistakes, just make new ones

“Offers management insight and resources to help foster growth.”
- STEVEN BERNSTEIN, USAA

“The SANS instructors are the cream of the crop. Top-shelf people. Smart, personable, and entertaining. Great way to learn.”
- THOMAS BARTON, SITES

Security leaders and managers earn the highest salaries (well into six figures) in information security and are near the top of IT. Needless to say, to work at that compensation level, excellence is demanded. These days, security managers are expected to have domain expertise as well as the classic project management, risk assessment, and policy review and development skills.
SANS MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that is specifically designed to prepare students to successfully pass the CISSP® exam.

MGT414 focuses solely on the eight domains of knowledge as determined by (ISC)² that form a critical part of the CISSP® exam. Each domain of knowledge is dissected into its critical components, and those components are then discussed in terms of their relationship with one another and with other areas of information security.

**Who Should Attend**

- Security professionals who are interested in understanding the concepts covered on the CISSP® exam as determined by (ISC)²
- Managers who want to understand the critical areas of information security
- System, security, and network administrators who want to understand the pragmatic applications of the CISSP®, eight domains
- Security professionals and managers looking for practical ways the eight domains of knowledge can be applied to their current job

**After completing the course students will have:**

- Detailed coverage of the eight domains of knowledge
- The analytical skills required to pass the CISSP® exam
- The technical skills required to understand each question
- The foundational information needed to become a Certified Information Systems Security Professional (CISSP®)

**External Product Notice:**

The CISSP® exam itself is not hosted by SANS. You will need to make separate arrangements to take the CISSP® exam. Please note as well that the GISP exam offered by GIAC is NOT the same as the CISSP® exam offered by (ISC)².

"Best security training I have ever received and just the right amount of detail for each domain."

-Tony Barnes, United States Sugar Corporation

"This training will provide me the necessary tools to obtain a certification that will greatly impact my career."

-Tom DiNonz, Exelon

"This training was a comprehensive overview of all topics covered in the CISSP® exam.
All in attendance were there for a common goal, including the instructor.
It was easy to follow, and the real-world examples given were priceless."

-Ron Pinnock, Navy Exchange Service Command

**Eric Conrad**  SANS Senior Instructor

Eric Conrad is lead author of the book The CISSP® Study Guide. Eric’s career began in 1991 as a UNIX systems administrator for a small oceanographic communications company. He gained information security experience in a variety of industries, including research, education, power, Internet, and healthcare. He is now president of Backshore Communications, a company focusing on intrusion detection, incident handling, information warfare, and penetration testing. He is a graduate of the SANS Technology Institute with a Master of Science degree in Information Security Engineering. In addition to the CISSP®, he holds the prestigious GIAC Security Expert (GSE) certification as well as the GIAC GPEC, GCIA, GCFA, GAWN, and GSEC certifications. Eric also blogs about information security at ericconrad.com.  @eric_conrad
414.1 Introduction; Security and Risk Management
On the first day of training for the CISSP® exam, MGT414 introduces the specific requirements needed to obtain certification. The exam update will be discussed in detail. We will cover the general security principles needed to understand the eight domains of knowledge, with specific examples for each domain. The first of the eight domains, Security and Risk Management, is discussed using real-world scenarios to illustrate the critical points.

Topics: Overview of CISSP® Certification; Introductory Material; Overview of the Eight Domains; Domain 1: Security and Risk Management

414.2 Asset Security and Security Engineering – Part 1
Understanding asset security is critical to building a solid information security program. The Asset Security domain, the initial focus of today’s course section, describes data classification programs, including those used by both governments and the military as well as the private sector. We will also discuss ownership ranging from business/mission owners to data and system owners. We will examine data retention and destruction in detail, including secure methods for purging data from electronic media. We then turn to the first part of the Security Engineering domain, including new topics for the 2018 exam such as the Internet of Things, Trusted Platform Modules, Cloud Security, and much more.

Topics: Domain 2: Asset Security; Domain 3: Security Engineering (Part 1)

414.3 Security Engineering – Part 2; Communication and Network Security
This section continues the discussion of the Security Engineering domain, including a deep dive into cryptography. The focus is on real-world implementation of core cryptographic concepts, including the three types of cryptography: symmetric, asymmetric, and hashing. Salts are discussed, as well as rainbow tables. We will round out Domain 3 with a look at physical security before turning to Domain 4, Communication and Network Security. The discussion will cover a range of protocols and technologies, from the Open Systems Interconnection (OSI) model to storage area networks.

Topics: Domain 3: Security Engineering (Part 2); Domain 4: Communication and Network Security

414.4 Identity and Access Management
Controlling access to data and systems is one of the primary objectives of information security. Domain 5, Identity and Access Management, strikes at the heart of access control by focusing on identification, authentication, and authorization of accounts. Password-based authentication represents a continued weakness, so Domain 5 stresses multi-factor authentication, biometrics, and secure credential management. The CISSP® exam underscores the increased role of external users and service providers, and mastery of Domain 5 requires an understanding of federated identity, SS0, SAML, and third-party identity and authorization services like OAuth and OpenID.

Topics: Domain 5: Identity and Access Management

414.5 Security Assessment and Testing; Security Operations
This course section covers Domain 6 (Security Assessment) and Domain 7 (Security Operations). Security Assessment covers types of security tests, testing strategies, and security processes. Security Operations covers investigatory issues, including eDiscovery, logging and monitoring, and provisioning. We will discuss cutting-edge technologies such as cloud, and we’ll wrap up day five with a deep dive into disaster recovery.

Topics: Domain 6: Security Assessment; Domain 7: Security Operations

414.6 Software Development Security
Domain 8 (Software Development Security) describes the requirements for secure software. Security should be “baked in” as part of network design from day one, since it is always less effective when it is added later to a poor design. We will discuss classic development models, including waterfall and spiral methodologies. We will then turn to more modern models, including agile software development methodologies. New content for the CISSP® exam update will be discussed, including DevOps. We will wrap up this course section by discussing security vulnerabilities, secure coding strategies, and testing methodologies.

Topics: Domain 8: Software Development Security

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/sans-2018/courses
As security professionals we have seen the landscape change. Cybersecurity is now more vital and relevant to the growth of your organization than ever before. As a result, information security teams have more visibility, more budget, and more opportunity. However, with this increased responsibility comes more scrutiny.

This course teaches security professionals how to do three things:

**Develop Strategic Plans**

Strategic planning is hard for people in IT and IT security because we spend so much time responding and reacting. We almost never get to practice until we get promoted to a senior position and then we are not equipped with the skills we need to run with the pack. Learn how to develop strategic plans that resonate with other IT and business leaders.

**Create Effective Information Security Policy**

Policy is a manager’s opportunity to express expectations for the workforce, set the boundaries of acceptable behavior, and empower people to do what they ought to be doing. It is easy to get wrong. Have you ever seen a policy and your response was, “No way, I am not going to do that?” Policy must be aligned with an organization’s culture. We will break down the steps to policy development so that you have the ability to develop and assess policy to successfully guide your organization.

**Develop Management and Leadership Skills**

Leadership is a capability that must be learned, exercised and developed to better ensure organizational success. Strong leadership is brought about primarily through selfless devotion to the organization and staff, tireless effort in setting the example, and the vision to see and effectively use available resources toward the end goal. Effective leadership entails persuading team members to accomplish their objectives while removing obstacles and maintaining the well-being of the team in support of the organization’s mission. Learn to utilize management tools and frameworks to better lead, inspire, and motivate your teams.

**How the Course Works**

Using case studies from Harvard Business School, team-based exercises, and discussions that put students in real-world scenarios, students will participate in activities that they can then carry out with their own team members when they return to work.

The next generation of security leadership must bridge the gap between security staff and senior leadership by strategically planning how to build and run effective security programs. After taking this course you will have the fundamental skills to create strategic plans that protect your company, enable key innovations, and work effectively with your business partners.

---

**Frank Kim**  
*SANS Certified Instructor*

Founder of ThinkSec, a security consulting and CISO advisory firm. Previously, as CISO at the SANS Institute, Frank led the information risk function for the most trusted source of computer security training and certification in the world. With the SANS Institute, Frank continues to lead the management and software security curricula, helping to develop the next generation of security leaders. Frank was also executive director of cybersecurity at Kaiser Permanente where he built an innovative security program to meet the unique needs of the nation’s largest not-for-profit health plan and integrated health care provider with annual revenue of $60 billion, 10 million members, and 175,000 employees. Frank holds degrees from the University of California at Berkeley and is the author and instructor of popular courses on strategic planning, leadership, application security, and DevOps. @fykim
**Course Day Descriptions**

### 514.1 Strategic Planning Foundations
Creating strategic plans for security requires a fundamental understanding of the business and a deep understanding of the threat landscape.

**Topics:** Vision & Mission Statements; Stakeholder Management; PEST Analysis; Porter's Five Forces; Threat Actors; Asset Analysis; Threat Analysis

### 514.2 Strategic Roadmap Development
With a firm understanding of business drivers as well as the threats facing the organization, you will develop a plan to analyze the current situation, identify the target situation, perform gap analysis, and develop a prioritized roadmap. In other words, you will be able to determine (1) what you do today, (2) what you should be doing in the future, (3) what you don’t do, and (4) what you should do first. With this plan in place you will learn how to build and execute your plan by developing a business case, defining metrics for success, and effectively marketing your security program.

**Topics:** Historical Analysis; Values and Culture; SWOT Analysis; Vision and Innovation; Security Framework; Gap Analysis; Roadmap Development; Business Case Development; Metrics and Dashboards; Marketing and Executive Communications

### 514.3 Security Policy Development and Assessment
Policy is one of the key tools that security leaders have to influence and guide the organization. Security managers must understand how to review, write, assess, and support security policy and procedure. Using an instructional delivery methodology that balances lecture, exercises, and in-class discussion, this course section will teach techniques to create successful policy that users will read and follow and business leaders will accept. Learn key elements of policy, including positive and negative tone, consistency of policy bullets, how to balance the level of specificity to the problem at hand, the role of policy, awareness and training, and the SMART approach to policy development and assessment.

**Topics:** Purpose of Policy; Policy Gap Analysis; Policy Development; Policy Review; Awareness and Training

### 514.4 Leadership and Management Competencies
Learn the critical skills you need to lead, motivate, and inspire your teams to achieve the goal. By establishing a minimum standard for the knowledge, skills, and abilities required to develop leadership you will understand how to motivate employees and develop from a manager into a leader.

**Topics:** Leadership Building Blocks; Creating and Developing Teams; Coaching and Mentoring; Customer Service Focus; Conflict Resolution; Effective Communication; Leading Through Change; Relationship Building; Motivation and Self-Direction; Teamwork; Leadership Development

### 514.5 Strategic Planning Workshop
Using the case study method, students will work through real-world scenarios by applying the skills and knowledge learned throughout the course. Case studies are taken directly from Harvard Business School, the pioneer of the case-study method, and focus specifically on information security management and leadership competencies. The Strategic Planning Workshop serves as a capstone exercise for the course, allowing students to synthesize and apply concepts, management tools, and methodologies learned in class.

**Topics:** Creating a Security Plan for the CEO; Understanding Business Priorities; Enabling Business Innovation; Working with BYOD; Effective Communication; Stakeholder Management

---

**You Will Be Able To**

- Develop security strategic plans that incorporate business and organizational drivers
- Develop and assess information security policy
- Use management and leadership techniques to motivate and inspire your teams

---

“**The leadership and management competencies module is packed with rich information. This is a must for any cybersecurity leader!”**

-MOBOLAJI MAYOSORE, TESORO CORPORATION

“**MGT514 targets the exact information needs of my organization.”**

-TIM HOFFMAN, UCSF

“**Frank was an excellent instructor who had a solid grasp of the material and provided unique insight into real-world scenarios and practice of examples faced by senior cybersecurity leaders in the work place.”**

-DAVE ODOM, BECHTEL

---

"This training was valuable because it helped me examine myself from an outside point of view.”

-DJ, ZOETIS

---

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/event/sans-2018/courses](http://www.sans.org/event/sans-2018/courses)
Managing Security Operations: Detection, Response, and Intelligence

Managing Security Operations covers the design, operation, and ongoing growth of all facets of the security operations capabilities in an organization. An effective Security Operations Center (SOC) has many moving parts and must be designed so that it can be adjusted to work within the context and constraints of the organization. To run a successful SOC, managers need to provide tactical and strategic direction and inform staff of the changing threat environment as well as provide guidance and training for employees. This course covers design, deployment, and operation of the security program to empower leadership through technical excellence.

The course covers the functional areas of Communications, Network Security Monitoring, Threat Intelligence, Incident Response, Forensics, and Self-Assessment. We discuss establishing Security Operations governance for:

- Business alignment and ongoing adjustment of capabilities and objectives
- Designing the SOC and the associated objectives of functional areas
- Software and hardware technology required for performance of functions
- Knowledge, skills, and abilities of staff as well as staff hiring and training
- Execution of ongoing operations

You will walk out of this course armed with a roadmap to design and operate an effective SOC tailored to the needs of your organization.

“This class is crucial to understanding how to improve an organization’s security posture.”

-JEFF McGRaw, PENSKE

“This course provides a comprehensive blueprint for all aspects of planning, building, staffing, and managing your SOC. It clearly establishes goals to shoot for.”

-MIKE Bowden, Webroot/BRIGHTCLOUD

Christopher Crowley  SANS Principal Instructor

Christopher has 15 years of industry experience managing and securing networks. He currently works as an independent consultant in the Washington, DC area. His work experience includes penetration testing, computer network defense, incident response, and forensic analysis. He is the course author for SANS MGT535: Incident Response Team Management and holds the GSEC, GCIA, GCIH (gold), GCFA, GPEN, GREM, GMOB, and CISSP certifications. His teaching experience includes SEC401, SEC503, SEC504, SEC560, SEC575, SEC580, FOR585, and MGT535; Apache web server administration and configuration; and shell programming. He was awarded the SANS 2009 Local Mentor of the Year Award, which is given to SANS Mentors who excel in leading SANS Mentor Training classes in their local communities.  @CCrowMontance
Course Day Descriptions

517.1 HANDS ON: **Design the Security Operations Center**

We will focus on how to align and deploy a Security Operations Center (SOC). This day lays the foundational aspects of the SOC by discussing the functional areas that form the basis of the build and operate days that follow. The first issue to address is how the SOC will serve the business. To understand what is to be built, we explore the business drivers for SOCs. Each company has its own circumstances and needs, but there are common drivers for setting out to build a SOC. From business alignment, systems analysis performed shows all the things that need to be done. This is an elaborate and substantial effort to undertake. Knowing what components are available and how the pieces fit together is critical. This analysis will be followed with design and build on day 2.

**Topics:** SOC Fundamentals; SOC Components; Sizing and Scoping; SOC Program

517.2 HANDS ON: **Build the Security Operations Center**

Once a clear picture of what should be done to secure the organization is produced from analysis of what the needs are, and what resources are available, we set out to build the SOC. The build-out starts with an operating plan decided on by the key stakeholders from the organization. The interactions, inputs, outputs, and actions within each of the process components are identified. Each functional area needs specific hardware and software to accomplish each process, so alternatives are discussed for all of these. Open-source, inexpensive, and enterprise-level solutions are presented for each need. We will discuss the available solutions in-depth, and help focus the budget available on the necessary tools. The output of this day is on all the procurement necessary for building out a SOC.

**Topics:** Governance Structure; Process Engineering; Technical Components

517.3 HANDS ON: **Operate and Mature the Security Operations Center**

Designing and building-out a SOC are considered projects. Operation is an ongoing and perpetual effort. If the design of the system is insufficient or short-sighted, then operating the system will be difficult and inefficient. The overarching challenge of management is discussed in terms of organizational dimensions. The analytical processes of competing hypotheses, the kill chain, and the diamond model are discussed to provide a context for the analytical currency of the SOC. We will evaluate the staffing structure, how to hire, and how to keep those staff continually trained and updated. A schedule of meetings, specific metrics to report, and specific metrics to use to measure the relationship within the functional areas of the SOC are shown. Specific processes and the data relationships when performing the processes are discussed to depict the standard operating procedures that the SOC must carry out.

**Topics:** People and Processes; Measurements and Metrics; Process Development

517.4 HANDS ON: **Incident Response Management — PART 1**

Further detail on incident response is developed to show the operation of the SOC. Since the response component is the action of defense, the operation of the incident response team is addressed in great detail. An examination of cloud-based systems shows a special case of incident response. The preparation of response capability in the cloud is insufficient because the contractual negotiations of the service rarely address incident response adequately. We discuss appropriate preparation and response action within cloud services. User training and awareness is developed as a basis for corrective action when incident response is required.

**Topics:** The Cloud; Incident Response Process; Creating Incident Requirements; Training, Education, and Awareness

517.5 HANDS ON: **Incident Response Management — PART 2**

Continuing the operation of incident response, we discuss the staffing requirements in detail. Common caveats of incidence response operations are discussed, and tabletop exercises are developed to mitigate those caveats. Communication requirements are laid out and incident tracking methods are discussed. We also look at how to make the most out of a response and damage control task. Tools for estimating and tracking costs associated with incidents are demonstrated, and overall recommendations are presented on how to interface with law enforcement. The final topic addressed is the development of appropriate response techniques for APT-style actors, including strategies for quickly differentiating APT-style compromise using threat intelligence, sufficient scope identification, and eradication of the current wave of compromise.

**Topics:** Staffing Considerations; Setting Up Operations; Managing Daily Operations; Cost Considerations; Legal and Regulatory Issues; Advanced Threat Response

---

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/event/sans-2018/courses](http://www.sans.org/event/sans-2018/courses)
This course is offered by the SANS Institute as a PMI® Registered Education Provider (R.E.P.). R.E.P.s provide the training necessary to earn and maintain the Project Management Professional (PMP)® and other professional credentials. PMP® is a registered trademark of Project Management Institute, Inc.

This course has been recently updated to fully prepare you for the 2018 PMP® exam changes. During this class you will learn how to improve your project planning methodology and project task scheduling to get the most out of your critical IT resources. We will utilize project case studies that highlight information technology services as deliverables. MGT525 follows the basic project management structure from the PMBOK® Guide – Sixth Edition and also provides specific techniques for success with information assurance initiatives. Throughout the week, we will cover all aspects of IT project management from initiating and planning projects through managing cost, time, and quality while your project is active, and to completing, closing, and documenting as your project finishes. A copy of the PMBOK® Guide – Sixth Edition is provided to all participants. You can reference the PMBOK® Guide and use your course material along with the knowledge you gain in class to prepare for the 2018 updated Project Management Professional (PMP)® Exam and the GIAC Certified Project Manager Exam.

“Honestly, this is one of the best courses I have had to date. I feel like I have thousands of things to take back to my job.”

-RYAN SPENCER, REED ELSEVIER INC.

The project management process is broken down into core process groups that can be applied across multiple areas of any project, in any industry. Although our primary focus is the application to the InfoSec industry, our approach is transferable to any projects that create and maintain services as well as general product development. We cover in-depth how cost, time, quality, and risks affect the services we provide to others. We will also address practical human resource management as well as effective communication and conflict resolution. You will learn specific tools to bridge the communications gap between managers and technical staff.

PMP®, PMBOK®, and the PMI Registered Education Provider® logo are registered trademarks of the Project Management Institute, Inc.

Jeff Frisk  SANS Certified Instructor

Jeff Frisk currently serves as the director of the GIAC certification program and is a member of the SANS Technology Institute Curriculum Committee. Jeff is a PMP® credential holder and a GIAC GSEC credential holder. He also is the course author for MGT525. He has worked on many projects for SANS and GIAC, including courseware, certification, and exam development. Jeff has an engineering degree from the Rochester Institute of Technology and more than 15 years of IT project management experience with computer systems, high-tech consumer products, and business development initiatives. Jeff has held various positions including managing operations, product development, and electronic systems/computer engineering. He has many years of international and high-tech business experience working with both big and small companies to develop computer hardware/software products and services.
**Course Day Descriptions**

525.1 **Project Management Structure and Framework**

This course offers insight and specific techniques that both beginner and experienced project managers can utilize. The structure and framework section lays out the basic architecture and organization of project management. We will cover the common project management group processes, the difference between projects and operations, project life cycles, and managing project stakeholders.

**Topics:** Definition of Terms and Process Concepts; Group Processes; Project Life Cycle; Types of Organizations; PDCA Cycle

525.2 **Project Charter and Scope Management**

During day two, we will go over techniques used to develop the project charter and formally initiate a project. The scope portion defines the important input parameters of project management and gives you the tools to ensure that your project is well defined from the outset. We cover tools and techniques that will help you define your project’s deliverables and develop milestones to gauge performance and manage change requests.

**Topics:** Formally Initiating Projects; Project Charters; Project Scope Development; Work Breakdown Structures; Scope Verification and Control

525.3 **Schedule and Cost Management**

Our third day details the schedule and cost aspects of managing a project. We will cover the importance of correctly defining project activities, project activity sequence, and resource constraints. We will use milestones to set project timelines and task dependencies along with learning methods of resource allocation and scheduling. We introduce the difference between resource and product-related costs and go into detail on estimating, budgeting, and controlling costs. You will learn techniques for estimating project cost and rates as well as budgeting and the process for developing a project cost baseline.

**Topics:** Process Flow; Task Lead and Lag Dependencies; Resource Breakdown Structures; Task Duration Estimating; Critical Path Scheduling; Cost Estimating Tools; Cost vs. Quality; Cost Baselining; Earned Value Analysis and Forecasting

525.4 **Communications and Project Resources**

During day four, we move into project and human resource management and building effective communications skills. People are the most valuable asset of any project and we cover methods for identifying, acquiring, developing and managing your project team. Performance appraisal tools are offered as well as conflict management techniques. You will learn management methods to help keep people motivated and provide great leadership. The effective communication portion of the day covers identifying and developing key interpersonal skills. We cover organizational communication and the different levels of communication as well as common communication barriers and tools to overcome these barriers.

**Topics:** Acquiring and Developing Your Project Team; Organizational Dependencies and Charts; Roles and Responsibilities; Team Building; Conflict Management; Interpersonal Communication Skills; Communication Models and Effective Listening

525.5 **Quality and Risk Management**

On day five you will become familiar with quality planning, assurance, and control methodologies, as well as learn the cost-of-quality concept and its parameters. We define quality metrics and cover tools for establishing and benchmarking quality control programs. We go into quality assurance and auditing as well as how to understand and use quality control charts. The risk section goes over known versus unknown risks and how to identify, assess, and categorize risk. We use quantitative risk analysis and modeling techniques so that you can fully understand how specific risks affect your project. You will learn ways to plan for and mitigate risk by reducing your exposure as well as how to take advantage of risks that could have a positive effect on your project.

**Topics:** Cost of Quality; Quality Metrics; Continual Process Improvement; Quality Baselines; Quality Control; Change Control; Risk Identification; Risk Assessment; Time and Cost Risks; Risk Probability and Impact Matrices; Risk Modeling and Response

525.6 **Procurement, Stakeholder Management, and Project Integration**

We close out the week with the procurement aspects of project and stakeholder management, and then integrate all of the concepts presented into a solid, broad-reaching approach. We cover different types of contracts and then the make-versus-buy decision process. We go over ways to initiate strong requests for quotations (RFQ) and develop evaluation criteria, then qualify and select the best partners for your project. Stakeholder communication and management strategies are reinforced. The final session integrates everything we have learned by bringing all the topics together with the common process groups. Using a detailed project management methodology, we learn how to finalize the project management plan and then execute and monitor the progress of your project to ensure success.

**Topics:** Contract Types; Make vs. Buy Analysis; Vendor Weighting Systems; Contract Negotiations; Stakeholder Communication and Stakeholder Management Strategies; Project Execution; Monitoring Your Project’s Progress; Finalizing Deliverables; Forecasting and Integrated Change Control

---

**You Will Be Able To**

- Recognize the top failure mechanisms related to IT and InfoSec projects, so that your projects can avoid common pitfalls
- Create a project charter that defines the project sponsor and stakeholder involvement
- Document project requirements and create a requirements traceability matrix to track changes throughout the project life cycle
- Clearly define the scope of a project in terms of cost, schedule and technical deliverables
- Create a work breakdown structure defining work packages, project deliverables and acceptance criteria
- Develop a detailed project schedule, including critical path tasks and milestones
- Develop a detailed project budget including cost baselines and tracking mechanisms
- Develop planned and earned value metrics for your project deliverables and automate reporting functions
- Effectively manage conflict situations and build communication skills with your project team
- Document project risks in terms of probability and impact, and assign triggers and risk response responsibilities
- Create project earned value baselines and project schedule and cost forecasts

“Over my 11-year relationship with SANS, they have continued to deliver the most complete education of any company across the board. This class is no exception.”

- Murdoch, GSE #99, Wellpoint
Auditing & Monitoring Networks, Perimeters, and Systems

Six-Day Program
Tue, April 3 - Sun, April 8
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Clay Risenhoover

Who Should Attend

➤ Auditors seeking to identify key controls in IT systems
➤ Audit professionals looking for technical details on auditing
➤ Managers responsible for overseeing the work of an audit or security team
➤ Security professionals newly tasked with audit responsibilities
➤ System and network administrators looking to better understand what an auditor is trying to achieve, how auditors think, and how to better prepare for an audit
➤ System and network administrators seeking to create strong change control management and detection systems for the enterprise
➤ Anyone looking to implement effective continuous monitoring processes within the enterprise

One of the most significant obstacles facing many auditors today is how exactly to go about auditing the security of an enterprise. What systems really matter? How should the firewall and routers be configured? What settings should be checked on the various systems under scrutiny? Is there a set of processes that can be put into place to allow an auditor to focus on the business processes rather than the security settings? How do we turn this into a continuous monitoring process? All of these questions and more will be answered by the material covered in this course.

This course is specifically organized to provide a risk-driven method for tackling the enormous task of designing an enterprise security validation program. After covering a variety of high-level audit issues and general audit best practices, the students will have the opportunity to dive deep into the technical how-to for determining the key controls that can be used to provide a level of assurance to an organization. Tips on how to repeatedly verify these controls and techniques for automatic compliance validation are taken from real-world examples.

“The entire course has been fantastic—it far exceeded my expectations. I think SANS training is far superior to other training programs.” —PAUL PETRASKO, BEMIS COMPANY

One of the struggles that IT auditors face today is helping management understand the relationship between the technical controls and the risks to the business that these controls address. In this course these threats and vulnerabilities are explained based on validated information from real-world situations. The instructor will take the time to explain how this can be used to raise the awareness of management and others within the organization to build an understanding of why these controls specifically and auditing in general are important. From these threats and vulnerabilities, we will explain how to build the ongoing compliance monitoring systems and automatically validate defenses through instrumentation and automation of audit checklists.

You’ll be able to use what you learn immediately. Five of the six days in the course will help you produce your own checklist, or provide you with a general checklist that can be customized for your audit practice. Each of these days includes hands-on exercises with a variety of tools discussed during the lecture sections so that you will leave knowing how to verify each and every control described in the class. Each of the six hands-on days gives you the chance to perform a thorough technical audit of the technology being considered by applying the checklists provided in class to sample audit problems in a virtualized environment.

A great audit is more than marks on a checklist; it is the understanding of what the underlying controls are, what the best practices are, and why. Sign up for this course and gain the mix of theoretical, hands-on, and practical knowledge to conduct a great audit.

Clay Risenhoover  SANS Certified Instructor

Clay is the president of Risenhoover Consulting, Inc., an IT management consulting firm based in Durant, Oklahoma. Founded in 2003, RCI provides IT audit and IT management consulting services to clients in multiple sectors. Clay’s past experience includes positions in software development, technical training, LAN and WAN operations, and IT management in both the private and public sectors. He has a master’s degree in computer science and holds a number of technical and security certifications, including the G Pen, GSNA, CISA, CISM, GWEB, and CISSP. @AuditClay
**Course Day Descriptions**

### 507.1 HANDS ON: Effective Auditing, Risk Assessment, and Reporting

After laying the foundation for the role and function of an auditor in the information security field, this day’s material will give you two extremely useful risk assessment methods that are particularly effective for measuring the security of enterprise systems, identifying control gaps and risks, and gaining the knowledge to be able to recommend additional compensating controls to address the risk. Nearly a third of the day is spent covering important audit considerations and questions dealing with virtualization and cloud computing.

**Topics:** Auditor’s Role in Relation to Policy Creation, Policy Conformance, and Incident Handling; Basic Auditing and Assessing Strategies; Risk Assessment; The Six-Step Audit Process; Virtualization and Cloud Computing

### 507.2 HANDS ON: Effective Network and Perimeter Auditing/Monitoring

On this day we will build from the ground up dealing with security controls, proper deployment, and effective auditing/continuous monitoring of configuration from Layer 2 all the way up the stack. Students will learn how to identify insecurely configured VLANs, determine perimeter firewall requirements, examine enterprise routers, and much more.

**Topics:** Secure Layer 2 Configurations; Router and Switch Configuration Security; Firewall Auditing, Validation, and Monitoring; Wireless; Network Population Monitoring; Vulnerability Scanning

### 507.3 HANDS ON: Web Application Auditing

Web applications have consistently been rated for the past several years as one of the top five vulnerabilities that enterprises face. Unlike the other top vulnerabilities, however, enterprises continue to accept this risk, since most modern corporations need an effective web presence to do business today. One of the most important lessons that we are learning as an industry is that installing an application firewall is not enough!

**Topics:** Identifying Controls Against Information Gathering Attacks; Processing Controls to Prevent Hidden Information Disclosures; Control Validation of the User Sign-on Process; Examining Controls Against User Name Harvesting; Validating Protections Against Password Harvesting; Best Practices for OS and Web Server Configuration; How to Verify Session Tracking and Management Controls; Identification of Controls to Handle Unexpected User Input; Server-side Techniques for Protecting Your Customers and Their Sensitive Data

### 507.4 HANDS ON: Advanced Windows Auditing and Monitoring

Microsoft’s business-class system makes up a large part of the typical IT infrastructure. Quite often, these systems are also the most difficult to effectively secure and control because of the enormous number of controls and settings within the operating system. This course day will provide you with the techniques and tools to build an effective long-term audit program for your Microsoft Windows environment. More importantly, during the course a continuous monitoring and reporting system is built out, allowing you to easily and effectively scale the testing discussed within your enterprise when you return home.

**Topics:** Progressive Construction of a Comprehensive Audit Program; Automating the Audit Process; Windows Security Tips and Tricks; Maintaining a Secure Enterprise

### 507.5 HANDS ON: Advanced Unix Auditing and Monitoring

Students will gain a deeper understanding of the inner workings and fundamentals of the Unix operating system as applied to the major Unix environments in use in business today. Students will have the opportunity to explore, assess and audit Unix systems hands-on. Lectures describe the different audit controls that are available on standard Unix systems, as well as access controls and security models.

**Topics:** Auditing to Create a Secure Configuration; Auditing to Maintain a Secure Configuration; Auditing to Determine What Went Wrong

### 507.6 HANDS ON: Audit the Flag: A NetWars Experience

This final day of the course presents a capstone experience with additional learning opportunities. Leveraging the well-known NetWars engine, students have the opportunity to connect to a simulated enterprise network environment. Building on the tools and techniques learned throughout the week, each student is challenged to answer a series of questions about the enterprise network, working through various technologies explored during the course.

**Topics:** Network Devices; Servers; Applications; Workstations

---

**You Will Be Able To**

- Understand the different types of controls (e.g., technical vs. non-technical) essential to perform a successful audit
- Conduct a proper risk assessment of a network to identify vulnerabilities and prioritize what will be audited
- Establish a well-secured baseline for computers and networks, constituting a standard against which one can conduct audits
- Perform a network and perimeter audit using a seven-step process
- Audit firewalls to validate that rules/settings are working as designed, blocking traffic as required
- Use vulnerability assessment tools effectively to provide management with the continuous remediation information necessary to make informed decisions about risk and resources
- Audit web application configuration, authentication, and session management to identify vulnerabilities attackers can exploit
- Use scripting to build a system to baseline and automatically audit Active Directory and all systems in a Windows domain

---

“I was exploring the idea of redirecting my career towards system auditing, and this course convinced me it’s a good move. I’m really eager to put my newfound knowledge to work.”

-RON BANDES, SOFTWARE ENGRG INST – CERT
Leg 523 Law of Data Security and Investigations

Five-Day Program
Tue, April 3 - Sat, April 7
9:00am - 5:00pm
30 CPEs
Laptop NOT Needed
Instructor: Benjamin Wright

Who Should Attend
Investigators
Security and IT professionals
Lawyers
Paralegals
Auditors
Accountants
Technology managers
Vendors
Compliance officers
Law enforcement personnel
Privacy officers
Penetration testers
Cyber incident and emergency responders around the world (including private sector, law enforcement, national guard, civil defense and the like)

NEW!

Students will receive a form contract for inviting outside incident responders – including police, contractors, National Guard, or civil defense agency anywhere in the world – to help with a cyber crisis

EU’s new General Data Protection Regulation and its impact around the world

The impact of the Trump presidency and Brexit on data security law and regulatory enforcement

How to improve the assessment and interpretation of digital evidence, such as evidence of a breach or other cyber event

New law on privacy, e-discovery and data security is creating an urgent need for professionals who can bridge the gap between the legal department and the IT department. SANS Leg 523 provides this unique professional training, including skills in the analysis and use of contracts, policies, and records management procedures.

This course covers the law of fraud, crime, policy, contracts, liability, IT security and active defense—all with a focus on electronically stored and transmitted records. It also teaches investigators how to prepare credible, defensible reports, whether for cyber crimes, forensics, incident response, human resource issues or other investigations.

“I have gained many valuable ideas and tools to support and defend my organization and to strengthen security overall. I wish I’d taken LEG523 three or four years ago.”

-TOM S., CASE WESTERN RESERVE UNIVERSITY

Each successive day of this five-day course builds upon lessons from the earlier days in order to comprehensively strengthen your ability to help your enterprise (public or private sector) cope with illegal hackers, botnets, malware, phishing, unruly vendors, data leakage, industrial spies, rogue or uncooperative employees, or bad publicity connected with IT security.

Recent updates to the course address hot topics such as legal tips on confiscating and interrogating mobile devices, the retention of business records connected with cloud computing and social networks like Facebook and Twitter, and analysis and response to the risks and opportunities surrounding open-source intelligence gathering.

Over the years this course has adopted an increasingly global perspective. Non-U.S. professionals attend LEG523 because there is no training like it anywhere else in the world. For example, a lawyer from the national tax authority in an African country took the course because electronic filings, evidence and investigations have become so important to her work. International students help the instructor, U.S. attorney Benjamin Wright, constantly revise the course and include more content that crosses borders.

Benjamin Wright SANS Senior Instructor

Benjamin Wright is the author of several technology law books, including Business Law and Computer Security, published by the SANS Institute. With 26 years in private law practice, he has advised many organizations, large and small, on privacy, e-commerce, computer security, and e-mail discovery and has been quoted in publications around the globe, from the Wall Street Journal to the Sydney Morning Herald. He is known for spotting and evaluating trends, such as the rise of whistleblowers wielding small video cameras. In 2010, Russian banking authorities tapped him for experience and advice on the law of cyber investigations and electronic payments.

@benjaminwright
This course covers how developers and security professionals can build and deliver secure software using DevOps and cloud services, specifically Amazon Web Services (AWS). It explains how principles, practices, and tools in DevOps and AWS can be leveraged to improve the reliability, integrity, and security of applications.

The first two days of the course cover how Secure DevOps can be implemented using lessons from successful DevOps security programs. Students build a secure DevOps CI/CD toolchain and understand how code is automatically built, tested, and deployed using popular open-source tools such as git, Puppet, Jenkins, and Docker. In a series of labs you learn to inject security into your CI/CD toolchain using various security tools, patterns, and techniques.

The final three days of the course cover how developers and security professionals can utilize AWS services to build secure software in the cloud. Students leverage the CI/CD toolchain to push application code directly to the cloud instead of to local servers on their class virtual machines. Students analyze and fix applications hosted in the cloud using AWS services and features such as API Gateway, IAM, signed cookies, Security Token Service, autoscaling, KMS, encryption, WAF, and Lambda for Serverless computing.

The course makes extensive use of open-source materials and tooling for automated configuration management (“Infrastructure as Code”), Continuous Integration, Continuous Delivery, Continuous Deployment, containerization, micro-segmentation, automated compliance (“Compliance as Code”), and Continuous Monitoring.

This course also makes extensive use of AWS and associated developer tools such as CloudFormation, CodeCommit, CodeBuild, CodePipeline, and other cloud application services so students can experience how these services can be utilized in their applications.

“SANS training is solid, useful, and well-rounded. It benefits anyone who attends, regardless of time in the industry.”

-D. Turner, Texas Workforce Commission
Secure Coding in .NET: Developing Defensible Applications

Four-Day Program
Tue, Apr 3 - Fri, Apr 6
9:00am - 5:00pm
24 CPEs
Laptop Required
Instructor: Aaron Cure

ASP.NET and the .NET framework have provided web developers with tools that allow them an unprecedented degree of flexibility and productivity. However, these sophisticated tools make it easier than ever to miss the little details that allow security vulnerabilities to creep into an application. Since ASP.NET 2.0, Microsoft has done a fantastic job of integrating security into the ASP.NET framework, but the responsibility is still on application developers to understand the limitations of the framework and ensure that their own code is secure.

Have you ever wondered if the built-in ASP.NET validation is effective? Have you been concerned that Windows Communication Foundation (WCF) services might be introducing unexamined security issues into your application? Should you feel uneasy relying solely on the security controls built into the ASP.NET framework?

“This class should be required for anyone in the field of software development.”
- Chad Reuss, Meljer

This comprehensive course covers a huge set of skills and knowledge. It is not a high-level theory course. It is about real programming. Students examine actual code, work with real tools, build applications, and gain confidence in the resources they need to improve the security of .NET applications.

Rather than teaching students to use a set of tools, the course teaches students concepts of secure programming. This involves looking at a specific piece of code, identifying a security flaw, and implementing a fix for flaws found on the OWASP Top 10 and CWE/SANS Top 25 Most Dangerous Programming Errors.

The class culminates with a security review of a real-world open-source application. Students will conduct a code review, review a penetration test report, perform security testing to actually exploit real vulnerabilities, and finally, using the secure coding techniques that they have learned in class, implement fixes for these issues.

PCI Compliance
Section 6.5 of the Payment Card Industry (PCI) Data Security Standard (DSS) instructs auditors to verify processes that require training in secure coding techniques for developers. This is the course for you if your application processes cardholder data and you are required to meet PCI compliance.

“DEV544 definitely opened my eyes to security vulnerabilities that I have missed in the past.”
- Scott Shepski, Pentec Health

“The information is valuable, and makes me want to continue my education with SANS.”
- Alan Baldridge, Meljer

Aaron Cure  SANS Instructor
Aaron is a senior security consultant at Cypress Data Defense and an instructor and contributing author for the DEV544: Secure Coding in .NET course. After 10 years in the U.S. Army as a Russian linguist and a satellite repair technician, he worked as a database administrator and programmer on the Iridium project, with subsequent positions as a telecommunications consultant, senior programmer, and security consultant. He also has experience developing security tools, performing secure code reviews, vulnerability assessments, and penetration testing, as well as risk assessments, static source code analysis, and security research. Aaron holds the GIAC GSSP-.NET, GWAPT, GMOB, and CISSP certifications and is located in Arvada, CO. Outside the office Aaron enjoys boating, traveling, and playing hockey.
SEC440 Critical Security Controls: Planning, Implementing, and Auditing

This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS). These Critical Security Controls are rapidly becoming accepted as the highest priority list of what must be done and proven before anything else at nearly all serious and sensitive organizations. These controls were selected and defined by the U.S. military and other government agencies (including NSA, DHS, GAO, and many others) and private organizations that are the most respected experts on how attacks actually work and what can be done to stop them. They defined these controls as their consensus for the best way to block known attacks and find and mitigate damage from the attacks that get through. For security professionals, the course enables you to see how to put the controls in place in your existing network through effective and widespread use of cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the controls are effectively implemented. **SEC440 does not contain any labs. Students looking for hands-on labs involving the Critical Controls should take SEC566.**

The Critical Security Controls are listed below. You will find the full document describing the Critical Security Controls posted at the Center for Internet Security. [www.cisecurity.org/controls](http://www.cisecurity.org/controls)

One of the best features of the course is that it uses offense to inform defense. In other words, you will learn about the actual attacks that you'll be stopping or mitigating. That makes the defenses very real, and it makes you a better security professional.

**CIS Controls:**

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software
4. Continuous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges
6. Maintenance, Monitoring, and Analysis of Audit Logs
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports
10. Data Recovery Capability
11. Secure Configurations for Network Devices
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment and Appropriate Training to Fill Gaps
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

SEC524 Cloud Security Fundamentals

SEC524: Cloud Security Fundamentals teaches you how to properly evaluate cloud providers, and perform risk assessment and review, with a focus on risk assessment versus technical implementation and operations. The course starts with a detailed introduction to the various cloud computing delivery models, ranging from Software as a Service (SaaS) to Infrastructure as a Service (IaaS) and everything in between. Each of these delivery models represents an entirely separate set of security conditions to consider, especially when coupled with various cloud types, including public, private, and hybrid. We'll take a close look at the security issues and the risks involved within each of these models.

The course will also touch on architecture and infrastructure fundamentals for the private, public, and hybrid clouds, including a wide range of topics such as patch and configuration management, virtualization security, application security, and change management. Policy, risk assessment, and governance within cloud environments will also be covered, with recommendations for both internal policies and contract provisions. This will lead us to a discussion of compliance and legal concerns. The first day will wrap up with an examination of disaster recovery and business continuity planning using cloud models and architecture.

Day 2 starts with a discussion about the challenges of identity and access management in cloud environments. As more and more businesses are using the cloud to store data, we will discuss how to protect your critical data in the cloud. New approaches for data encryption, network encryption, key management, and data lifecycle concerns will be covered in detail. This will be followed by a discussion on intrusion detection and incident response in cloud environments, along with how to best manage these critical security processes and the technologies that support them, given that most controls are managed by the Cloud Service Provider (CSP). We'll wrap up with a deep dive into risk assessments and risk management that will provide students with a framework to properly assess and review current cloud provider controls.
Red Team Operations and Threat Emulation

Two-Day Program
Mon, April 9 - Tue, April 10
9:00am - 5:00pm
12 CPEs
Laptop Required
Instructor: Joe Vest

This course provides the foundation needed to manage and operate a Red Team and conduct Red Team engagements. What is Red Teaming? Red Teaming is the process of using tactics, techniques, and procedures (TTPs) to emulate a real-world threat with the goals of training and measuring the effectiveness of people, processes and technology used to defend an environment.

Red Teaming is built on the fundamentals of penetration testing, yet focuses on specific scenarios and goals used to evaluate and measure an organization’s overall security defense posture. That posture includes people, processes, and technology. This course will explore Red Teaming concepts in-depth to provide a clear understanding of what a Red Team is and its role in security testing.

Organizations spend a great deal of time and money on the security of their systems. Red Teaming uses a comprehensive approach to gain insight into an organization’s overall security. Red Teams have a unique goal of testing an organization’s ability to detect, respond to, and recover from an attack. When properly conducted, Red Team activities significantly improve an organization’s security controls, help hone defensive capabilities, and measure the effectiveness of security operations.

The Red Team concept requires a different approach from a typical security test, and it relies heavily on well-defined TTPs. These are critical if a Red Team is to successfully emulate a realistic threat or adversary. Red Team results exceed a typical list of penetration test vulnerabilities, provide a deeper understanding of how an organization would perform against an actual threat, and identify where security strengths and weaknesses exist.

Social Engineering for Penetration Testers

Two-Day Program
Mon, April 9 - Tue, April 10
9:00am - 5:00pm
12 CPEs
Laptop Required
Instructor: Micah Hoffman

SEC567 provides the blend of knowledge required to add social engineering skills to your penetration testing portfolio. Successful social engineering utilizes psychological principles and technical methodologies to measure your success and manage the risk. SEC567 covers the principles of persuasion and the psychological foundations required to craft effective attacks, then bolsters this with many examples of what works, drawing on the work of cyber criminals as well as the experience of the instructor in combating them. On top of these principles we provide a number of tools (produced in our engagements over the years and now available in the course) as well as labs centered around the key technical skills required to measure your social engineering success and report it to your company or client.

You’ll learn how to perform recon on targets using a wide variety of sites and tools, create and track phishing campaigns, and develop media payloads that effectively demonstrate compromise scenarios. You’ll also learn how to conduct pretexting exercises, and we wrap the course with a fun “Capture the Human” exercise to put what you’ve learned into practice. This is the perfect course to open up new attack possibilities, to better understand the human vulnerability in attacks, and to let you practice snares that have proven themselves in tests time and time again.

Metasploit Kung Fu for Enterprise Pen Testing

Two-Day Program
Mon, April 9 - Tue, April 10
9:00am - 5:00pm
12 CPEs
Laptop Required
Instructor: Bryce Galbraith

Many enterprises today face regulatory or compliance requirements that mandate regular penetration testing and vulnerability assessments. Commercial tools and services for performing such tests can be expensive. While really solid free tools such as Metasploit are available, many testers do not understand the comprehensive feature sets of such tools and how to apply them in a professional-grade testing methodology. Metasploit was designed to help testers confirm vulnerabilities using an open-source and easy-to-use framework. This course will help students get the most out of this free tool.

This class will show students how to apply the incredible capabilities of the Metasploit Framework in a comprehensive penetration testing and vulnerability assessment regimen according to a thorough methodology for performing effective tests. Students who complete the course will have a firm understanding of how Metasploit can fit into their penetration testing and day-to-day assessment activities. The course will provide an in-depth understanding of the Metasploit Framework far beyond simply showing attendees how to exploit a remote system. The class will cover exploitation, post-exploitation reconnaissance, token manipulation, spear-phishing attacks, and the rich feature set of the Meterpreter, a customized shell environment specially created for exploiting and analyzing security flaws.

The course will also cover many of the pitfalls that a tester may encounter when using the Metasploit Framework and how to avoid or work around them, making tests more efficient and safe.
MGT415
A Practical Introduction to Cybersecurity Risk Management

In this course students will learn the practical skills necessary to perform regular risk assessments for their organizations. The ability to perform a risk assessment is crucial for organizations hoping to defend their systems. There are simply too many threats, too many potential vulnerabilities, and not enough resources to create an impregnable security infrastructure. Therefore every organization, whether it does so in an organized manner or not, will make priority decisions on how best to defend its valuable data assets. Risk assessment should be the foundational tool used to facilitate thoughtful and purposeful defense strategies.

Two-Day Program
Mon, April 9 - Tue, April 10
9:00am - 5:00pm
12 CPEs
Laptop Required
Instructor: James Tarala

You Will Learn:
- How to perform a risk assessment step-by-step
- How to map an organization’s business requirements to implemented security controls
- The elements of risk assessment and the data necessary for performing an effective risk assessment
- In-depth risk management models for implementing a deeper risk management program in your organization

MGT433
Securing The Human: How to Build, Maintain and Measure a High-Impact Awareness Program

Organizations have invested a tremendous amount of money and resources into securing technology, but little if anything into securing their employees and staff. As a result, people, not technology, have become their weakest link in cybersecurity. The most effective way to secure the human element is to establish a high-impact security awareness program that goes beyond just compliance and changes behaviors. This intense two-day course will teach you the key concepts and skills needed to build, maintain, and measure just such a program. All course content is based on lessons learned from hundreds of security awareness programs from around the world. You will learn not only from your instructor, but from extensive interaction with your peers as well. Please bring example materials from your security awareness program that you can show and share with other students during the course. Finally, through a series of labs and exercises, you will develop your own custom security awareness plan that you can implement as soon as you return to your organization.

Two-Day Program
Mon, April 9 - Tue, April 10
9:00am - 5:00pm
12 CPEs
Laptop Not Needed
Instructor: Lance Spitzner

Who Should Attend
- Security awareness officers
- Chief security officers and security management officials
- Security auditors, and governance and compliance officers
- Training, human resources, and communications staff
- Representatives from organizations regulated by industries such as HIPAA, FISMA, FERPA, PCI-DSS, ISO/IEC 27001 SOX, NERC, or any other compliance-driven standard
- Anyone involved in planning, deploying or maintaining a security awareness program

DEV531
Defending Mobile Applications Security Essentials

Mobile application development is growing exponentially year after year. As of late 2015, over 3 million apps had been deployed in the Apple and Google app stores. These apps are consumed by over 700 million users world-wide and account for 33% of the traffic on the Internet. Average users have over 100 mobile apps installed on their device, many of which provide business-critical services to customers and employees. Unfortunately, these apps are often rushed to market to gain a competitive advantage with little regard for security. As seen in web applications for the past 20 years, software vulnerabilities always exist where code is being written, and mobile apps are no different. Mobile apps are vulnerable to a whole new class of vulnerabilities, as well as most traditional issues that have long plagued web and desktop applications. This problem will only continue to grow unless managers, architects, developers, and QA teams learn how to test and defend their mobile apps.

DEV531: Defending Mobile Applications Security Essentials covers the most prevalent mobile app risks, including those from the OWASP Mobile Top 10. Students will participate in numerous hands-on exercises available in both the Android and iOS platforms. Each exercise is designed to reinforce the lessons learned throughout the course, ensuring that you understand how to properly defend your organization’s mobile applications.
Physical Security Specialist – Full Comprehensive Edition

Six-Day Program
Tue, April 3 - Sun, April 8
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: The CORE Group

You’ve worked hard to secure your servers, workstations, and network. But increasingly, your physical security is tied into electronic access control systems, bringing major exposure to your enterprise if these systems aren’t secured properly. How can you trust your systems if their physical security is in jeopardy? Every security pro should have some skills in assessing access control systems, and this class provides exactly what you need.

Whether an enterprise is using HID Prox cards, NXP Hitag chips, Mifare credentials, or even iCLASS technology, students who have taken this course will be well-versed in the functionality, weaknesses, and attack vectors of such systems. From how to perform practical card cloning attacks in the field to advanced format downgrade attacks, students are prepared for real-world red team scenarios after having learned how to exploit access control technology with the latest attack hardware. There are also modules detailing the back end of such systems, which opens the door to Man-in-the-Middle and Denial-of-Service attacks.

By the end of this course, students will be very prepared to make educated and fiscally-responsible security decisions not only for their respective organizations but also for themselves. Participants will be able to approach any target, site unseen, and then either conduct a walk-through assessment highlighting attack vectors, or proceed directly with an attack—gaining physical access to critical areas and infrastructure. Additionally, these newly-minted professionals in our training will also be able to provide sound documentation while making recommendations to management or to their insurance providers, saving money for their companies.

The training concludes on days five and six with an intense specialization focus: electronic access control systems and badge readers. Students will be immersed in the world of 125KHz (low frequency) credentials, vehicle transponders, 13.56MHz (high frequency) credentials, and smart cards. Whether an enterprise is using HID Prox cards, NXP Hitag chips, Mifare credentials, or even iCLASS technology, students who have taken this course will be well-versed in the functionality, weaknesses, and attack vectors of such systems. From how to perform practical card cloning attacks in the field to advanced format downgrade attacks, students will be prepared for real-world red team scenarios after having learned how to exploit access control technology with the latest attack hardware. There are also modules detailing the back end of such systems, which opens the door to Man-in-the-Middle and Denial-of-Service attacks.

By the end of this course, students will be very prepared to make educated and fiscally-responsible security decisions not only for their respective organizations but also for themselves. Participants will be able to approach any target, site unseen, and then either conduct a walk-through assessment highlighting attack vectors, or proceed directly with an attack—gaining physical access to critical areas and infrastructure. Additionally, these newly-minted professionals in our training will also be able to provide sound documentation while making recommendations to management or to their insurance providers, saving money for their companies.

The CORE Group

The CORE Group provides specialized consulting that focuses on physical security solutions, including training blended penetration testing, and innovative tools for clients who seek security on all surfaces. Their senior team’s combined experience in the physical security sector represents decades of hard knowledge and applied work. The CORE Group finds innovative ways to augment typical security auditing, assessment, and training by approaching topics that others often fail to consider: mechanical locks, electronic locks, safes, alarm systems, elevator systems, and much more. @TC6sec
For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/sans-2018/courses

**KEYNOTE: Threat Hunting via Windows Event Logs**

**Eric Conrad**  
Windows event logs continue to be the best source to centrally hunt malware in a Windows environment. Virtually all malware may be detected via event logs after making small tweaks to the logging configuration. Recent malware attacks leverage “fileless malware,” typically using PowerShell for post exploitation. Why? No EXE for antivirus or HIPS to squash, nothing saved to the filesystem, sites that use application whitelisting allow PowerShell, and little to no default logging. We will discuss DeepBlueCLI, an open-source PowerShell framework for threat hunting via Windows Event Logs (including the latest PowerShell-fueled post exploitation). DeepBlueCLI will go toe-to-toe with the latest attacks; this talk will explore the evidence malware leaves behind, leveraging Windows command line auditing (now natively available in Windows 7+) and PowerShell logging. We will also discuss DeepWhite, an open-source detective application whitelisting framework that relies on Microsoft Sysinternals’s Sysmon and supports auto-submission of EXE, DLL and driver hashes via a free VirusTotal Community API key.

**Infosec Rock Star: Geek Will Only Get You So Far**

**Ted Demopoulos**  
Some of us are so effective and well known that the term “Rock Star” is entirely accurate. What kind of skills do Rock Stars have and wannabe Rock Stars need to develop? Although we personally may never be swamped by groupies, we can learn the skills to be more effective, well respected, and well paid. Obviously it’s not just about technology; in fact most of us are very good at the technology part. The fact is that increasing our skills on the social and business side will make most of us more effective at what we do, rather than learning how to read hex better while standing on our heads, becoming “One with Metasploit,” or understanding the latest hot technologies.

**The Seven Deadly Sins of Incident Response**

**Jake Williams**  
In this session, Jake will walk you through the seven deadly sins of incident response. Incident response is not for the faint of heart and it’s far easier to get wrong than it is to get right. Jake’s been in the trenches working incident response with a huge number of clients on cases ranging in size from a few credit card records to one case where hundreds of millions of dollars were at stake. You’ll take away some valuable lessons to help prevent an incident response catastrophe that you can’t walk back.

**Stuck in the Box, a SIEM’s Tale**

**Justin Henderson**  
Organizations often spend excessive amounts of money on SIEM products only to end up with a log collection box when they thought they purchased a tactical detection system. Most organizations find themselves with a SIEM but unsure how to use its capabilities. Point solutions are quick to defend deficiencies by stating that each environment is different, so you, the customer, must tell them what you want the SIEM to do, then they’ll help with professional services or replace your current SIEM with something “better and more advanced.” This is complete hogwash. Organizations tend to have a lot of overlap in the use of Windows systems or network protocols such as DNS. As such there are high-fidelity detectors that can be implemented in every organization. Enough is enough. If you are looking for techniques and methods to get value out of your current SIEM or are interested in seeing how a new, open-source big data solution, such as the Elastic Stack (formerly ELK), can most likely beat what you have today, then this talk is for you. It is time to think outside the box. Come find out how one organization spent 14 months deploying a top Magic Quadrant SIEM solution to have it beaten by ELK in two weeks.

**Speaking to the Board on Cybersecurity**

**Lance Spitzner**  
Time and time again we understand the need for leadership support on cybersecurity. However it can be challenging communicating to senior leaders, especially Board members, in their terms. How do you translate the technical world of cyber into concise business terms? Who is a Board member, how do they think and what do they want to know? Learn how senior leaders think and operate, what their priorities are, and how you can effectively engage them. Make your security program a success by gaining the support you need.

**Securing Your Kids**

**Lance Spitzner**  
Technology is an amazing tool. It allows our kids to access a tremendous amount of information, meet new people, and communicate with friends around the world. In addition, for them to be successful in the 21st century they have to know and understand how to leverage these new tools. However, with all these capabilities come a variety of new risks, risks that as parents you may not understand or even be aware of. In this one-hour presentation we cover the top three risks to kids online and the top steps you can take to protect them.

**An Evening of Hacking the Internet of Things (IoT)**

**James Lyne, Stephen Sims, Jim Shewmaker, and Guests**  
**Thursday, April 5**  
**7:15pm - 10:00pm**

Join James, Jim, and Steve in this “limited-seating” SANS special event. Somewhere along the line product developers thought it would be a good idea to connect things like pet food dispensers, BBQ grills, refrigerators, and many other “items” to the Internet. What could possibly go wrong? We will have a collection of “things” for you to try and find vulnerabilities in. If you find something interesting you may even be able to take the item home! We’ll walk through an introduction of how to extract and analyze firmware, and the types of bugs that are most commonly found, along with some examples.

So how do you gain entry? We will have a limited number of passes available. There will be a few instructors from whom you can get a pass. The list of these instructors and locations will be announced at the event. What do you need to bring? A laptop with VMware Player, Workstation, or Fusion. We will provide you with a Linux virtual machine to use for analysis.
### The 14 Absolute Truths of Security

Keith Palmgren has identified 14 absolute truths of security—things that remain true regardless of circumstance, network topology, organizational type, or any other variable. Recognizing these 14 absolute truths and how they affect a security program can lead to the success of that program. Failing to recognize these truths will spell almost certain doom. Here we will take a non-technical look at each of the 14 absolute truths in turn, examine what they mean to the security manager, what they mean to the security posture, and how understanding them will lead to a successful security program.

### So, You Wanna Be a Pen Tester?

Adrien de Beaupre

This presentation will discuss the things that you will actually need to become a penetration tester. Be prepared for a no-fluff honest discussion. You will need attitude, aptitude, initiative, desire, dedication, discipline, integrity, ethics, experience, knowledge, and tools.

### Secure DevOps: A Puma’s Tail

Aaron Cure

DevOps is changing the way that organizations design, build, deploy, and operate online systems. Engineering teams are making hundreds or even thousands of changes per day, and traditional approaches to security are struggling to keep up. Security must be reinvented in a DevOps world to take advantage of the opportunities provided by continuous integration and delivery pipelines. In this talk, we start with a case study of an organization trying to leverage the power of Continuous Integration (CI) and Continuous Delivery (CD) to improve its security posture. After identifying the key security checkpoints in the pre-commit, commit, acceptance, and deployment lifecycle phases, we will explore how unit testing and static analysis fit into SecDevOps. Live demonstrations will show how to identify vulnerabilities inside the Visual Studio development environment before they are committed to source control, and how to enforce security unit tests and static analysis in a Jenkins CI build pipeline. Attendees will walk away with a better understanding of how security fits into DevOps and an open-source .NET static analysis engine to help secure their organization’s applications.

### Let’s Go Hunting Bad Guys

John Strand

In this presentation, John will share custom free tools with you to hunt bad guys inside and outside of your network – with awesomeness and math. But mostly math.

### Defeating Advanced Adversaries: Dismantling Their Attacks One Step at a Time

Erik Van Buggenhout

Cyber threats are on the rise: ransomware is affecting small, medium and large enterprises alike, while state-sponsored adversaries are attempting to obtain access to your most precious crown jewels. Is it all doom and gloom? No! Defense is doable (though not always easy)! During this hands-on talk, we will run through a typical “advanced attack” using a kill chain approach. We will highlight, implement and demonstrate security controls that can help you detect, fool and ultimately defeat advanced adversaries.

### Hacking Dumberly, Just Like the Bad Guys

Tim Medin and Derek Banks

Tim Medin and Derek Banks will discuss the dumbest red team tricks and hacks we’ve encountered over the years. We are going to take the A out of APT, because so few attackers really need to use advanced techniques. We’ll also discuss the simple defenses that make an attacker’s life much more difficult.

### Malware Vaccination: Its Potential and Limitations

Lenny Zeltser

Some malicious software is designed to avoid infecting the system more than once by looking for predefined infection markers. Incident responders can vaccinate endpoints against such malware families by distributing the corresponding markers. The vaccines can take the form of specific registry keys, file names, mutex objects, and so on. Enterprises already know to treat such artifacts as indicators of compromise (IOCs). Vaccination entails using some IOCs to not only detect, but also prevent infections. This session will examine the potential for and limitations of malware vaccination and will explore several malware samples that could be controlled using this technique.

### Coffee & Donuts with the Graduate Students

Hosted by SANS Technology Institute

Get the inside scoop on what it’s like to pursue a graduate degree in cybersecurity from SANS from like-minded information security professionals currently enrolled in SANS graduate programs. SANS’s regionally accredited graduate program, the SANS Technology Institute, combines SANS technical training and certifications with leadership and management curriculum specifically designed for the unique needs of aspiring leaders. Find out how the class you’re taking this week may be applied towards a master’s degree or graduate certificate program. Visit www.sans.edu for complete information on curriculum, admissions, and funding options.

### Vendor-Sponsored Events

**Vendor Expo**

Thursday, April 5

12:00pm - 1:30pm & 5:30pm - 7:30pm

Given that virtually everything in security is accomplished with a tool, exposure to those tools is a very important part of the SANS training experience. Leading solution providers will be on hand for a one-day Vendor Expo, an added bonus to registered SANS 2018 attendees. Attendees can visit sponsors during the lunch-time and evening Vendor Expo hours to receive stamps on the Passport-to-Prizes form. Prize drawings will occur at the Vendor Welcome Reception taking place during the evening expo hours on Thursday, April 5.

**Networking Lunch**

Thursday, April 5

12:00pm - 1:30pm

Join the sponsoring vendors and others on the expo floor for an introduction to leading solutions and services that showcase the best options in information security.

**Lunch & Learn Presentations**

Throughout SANS 2018, vendors will provide sponsored lunch presentations where attendees can interact with peers and learn about vendor solutions. Take a break and get up-to-date on security technologies!
Future Training Events

**Security East**

Northern VA Winter – Reston ........ Reston, VA ............ Jan 15-20
Las Vegas .................. Las Vegas, NV .......... Jan 28 - Feb 2
Miami ..................... Miami, FL ........... Jan 29 - Feb 3
Scottsdale ................... Scottsdale, AZ .... Feb 5-10
Southern CA – Anaheim .... Anaheim, CA ......... Feb 12-17
Dallas ...................... Dallas, TX ........ Feb 19-24
New York City Winter ...... New York, NY .... Feb 26 - Mar 3
San Francisco Spring ...... San Francisco, CA .... Mar 12-17
Northern VA Spring – Tysons ... McLean, VA ........ Mar 17-24
Pen Test Austin ............. Austin, TX ....... Mar 19-24
Boston Spring ............... Boston, MA ........ Mar 25-30

**SANS 2018**

Baltimore Spring ............ Baltimore, MD ........ Apr 21-28
Seattle Spring ................ Seattle, WA ........ Apr 23-28

**Security West**

San Diego, CA ................ May 11-16

Future Summit Events

SIEM & Tactical Analytics .... Scottsdale, AZ ...... Nov 28 - Dec 5
Cyber Threat Intelligence ...... Bethesda, MD .... Jan 29 - Feb 5, 2018
Cloud Security ................. San Diego, CA ....... Feb 19-26
ICS Security .................... Orlando, FL ....... Mar 19-26
Automotive Cybersecurity ...... Chicago, IL .......... May 1-8

Future Community SANS Events

Local, single-course events are also offered throughout the year via SANS Community. Visit [www.sans.org/community](http://www.sans.org/community) for up-to-date Community course information.
Nothing beats the SANS live training experience, but if you are unable to travel, learn how you can attend a SANS 2018 course remotely via SANS Simulcast. Visit www.sans.org/event/sans-2018/attend-remotely

**SANS SIMULCAST**

We recommend you register early to ensure you get your first choice of courses.

Select your course and indicate whether you plan to test for GIAC certification. If the course is still open, the secure, online registration server will accept your registration. Sold-out courses will be removed from the online registration. Everyone with Internet access must complete the online registration form. We do not take registrations by phone.

### Pay Early and Save*

<table>
<thead>
<tr>
<th>PAY &amp; ENTER CODE BY</th>
<th>DATE</th>
<th>DISCOUNT</th>
<th>DATE</th>
<th>DISCOUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2-7-18</td>
<td>$400.00</td>
<td>2-28-18</td>
<td>$200.00</td>
</tr>
</tbody>
</table>

*Some restrictions apply. Early bird discounts do not apply to Hosted courses.

**Cancellation & Access Policy**

If an attendee must cancel, a substitute may attend instead. Substitution requests can be made at any time prior to the event start date. Processing fees will apply. All substitution requests must be submitted by email to registration@sans.org. If an attendee must cancel and no substitute is available, a refund can be issued for any received payments by March 14, 2018. A credit memo can be requested up to the event start date. All cancellation requests must be submitted in writing by mail or fax and received by the stated deadlines. Payments will be refunded by the method that they were submitted. Processing fees will apply.
### Job-Based Long Courses

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Early Bird Price</th>
<th>Regular Price</th>
<th>Add GIAC Cert</th>
<th>Add OnDemand</th>
<th>Add NetWars Continuous</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC301</td>
<td>Intro to Information Security</td>
<td>$4,980</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC401</td>
<td>Security Essentials Bootcamp Style</td>
<td>$5,810</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC501</td>
<td>Advanced Security Essentials – Enterprise Defender</td>
<td>$5,810</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC503</td>
<td>Intrusion Detection In-Depth</td>
<td>$5,810</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC504</td>
<td>Hacker Tools, Techniques, Exploits, and Incident Handling</td>
<td>$5,810</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC505</td>
<td>Securing Windows and PowerShell Automation</td>
<td>$5,810</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC506</td>
<td>Securing Linux/Unix</td>
<td>$5,810</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC511</td>
<td>Continuous Monitoring and Security Operations</td>
<td>$5,810</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC542</td>
<td>Web App Penetration Testing and Ethical Hacking</td>
<td>$5,810</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC545</td>
<td>Cloud Security Architecture and Operations NEW!</td>
<td>$4,980</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC555</td>
<td>SIEM with Tactical Analytics NEW!</td>
<td>$5,810</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC560</td>
<td>Network Penetration Testing and Ethical Hacking</td>
<td>$5,810</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC561</td>
<td>Immersive Hands-on Hacking Techniques</td>
<td>$5,810</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC566</td>
<td>Implementing and Auditing the Critical Security Controls – In-Depth</td>
<td>$4,980</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC573</td>
<td>Automating Information Security with Python</td>
<td>$5,810</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC575</td>
<td>Mobile Device Security and Ethical Hacking</td>
<td>$5,810</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC599</td>
<td>Defeating Advanced Adversaries – Implementing Kill Chain Defenses NEW!</td>
<td>$5,810</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC607</td>
<td>Wireless Penetration Testing and Ethical Hacking NEW!</td>
<td>$5,810</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC642</td>
<td>Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques</td>
<td>$5,810</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC660</td>
<td>Advanced Penetration Testing, Exploit Writing, and Ethical Hacking</td>
<td>$5,810</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC760</td>
<td>Advanced Exploit Development for Penetration Testers</td>
<td>$5,810</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FOR500</td>
<td>Windows Forensic Analysis</td>
<td>$5,810</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FOR508</td>
<td>Advanced Digital Forensics, Incident Response, and Threat Hunting</td>
<td>$5,810</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FOR518</td>
<td>Mac Forensic Analysis</td>
<td>$5,810</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FOR526</td>
<td>Memory Forensics In-Depth</td>
<td>$5,810</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FOR530</td>
<td>Advanced Network Forensics and Analysis</td>
<td>$5,810</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FOR578</td>
<td>Cyber Threat Intelligence</td>
<td>$4,980</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FOR585</td>
<td>Advanced Smartphone Forensics</td>
<td>$5,810</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FOR610</td>
<td>Reverse-Engineering Malware: Malware Analysis Tools and Techniques</td>
<td>$5,810</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MGT414</td>
<td>SANS Training Program for CISSP® Certification</td>
<td>$5,810</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MGT512</td>
<td>SANS Security Leadership Essentials for Managers with Knowledge Compression*</td>
<td>$5,420</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MGT514</td>
<td>IT Security Strategic Planning, Policy, and Leadership</td>
<td>$4,980</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MGT517</td>
<td>Managing Security Operations: Detection, Response, and Intelligence</td>
<td>$5,420</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MGT525</td>
<td>IT Project Management, Effective Communication, and PMP® Exam Prep</td>
<td>$5,810</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DEV530</td>
<td>Secure DevOps and Cloud Application Security NEW!</td>
<td>$4,980</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DEV544</td>
<td>Secure Coding in .NET: Developing Defensible Applications</td>
<td>$4,470</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AUD507</td>
<td>Auditing &amp; Monitoring Networks, Perimeters, and Systems</td>
<td>$5,810</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LEG523</td>
<td>Law of Data Security and Investigations</td>
<td>$4,980</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HOSTED</td>
<td>Physical Security Specialist – Full Comprehensive Edition</td>
<td>$6,910</td>
<td>$1,260</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Skill-Based Short Courses

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Early Bird Price</th>
<th>Regular Price</th>
<th>Add GIAC Cert</th>
<th>Add OnDemand</th>
<th>Add NetWars Continuous</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC440</td>
<td>Critical Security Controls: Planning, Implementing, and Auditing</td>
<td>$1,860</td>
<td>$2,480</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC524</td>
<td>Cloud Security Fundamentals</td>
<td>$1,860</td>
<td>$2,480</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC564</td>
<td>Red Team Operations and Threat Emulation</td>
<td>$1,860</td>
<td>$2,480</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC567</td>
<td>Social Engineering for Penetration Testers</td>
<td>$1,860</td>
<td>$2,480</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC580</td>
<td>Metasploit Kung Fu for Enterprise Pen Testing</td>
<td>$1,860</td>
<td>$2,480</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MGT415</td>
<td>A Practical Introduction to Cybersecurity Risk Management</td>
<td>$1,860</td>
<td>$2,480</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MGT433</td>
<td>Securing The Human: How to Build, Maintain &amp; Measure a High-Impact Awareness Program</td>
<td>$1,860</td>
<td>$2,480</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DEV531</td>
<td>Defending Mobile Applications Security Essentials</td>
<td>$1,860</td>
<td>$2,480</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HOSTED</td>
<td>Physical Access Control Systems: Elements of Design, Offense, and Defense</td>
<td>$2,905</td>
<td>$2,480</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SPECIAL</td>
<td>Core NetWars Experience – Tournament Entrance Fee</td>
<td>FREE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SPECIAL</td>
<td>DFIR NetWars Tournament – Tournament Entrance Fee</td>
<td>FREE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SPECIAL</td>
<td>Cyber Defense NetWars Tournament – Tournament Entrance Fee</td>
<td>FREE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Early Bird Discounts

Pay for any long course using the code EarlyBird18 at checkout by February 7th to get $400 OFF* or by February 28th to get $200 OFF*.

*Some restrictions apply. Early bird discounts do not apply to Hosted courses.

---

**Register online at [www.sans.org/sans-2018](http://www.sans.org/sans-2018)**
Create a **SANS Account** today to enjoy these Free resources at www.sans.org/account

**Newsletters**

**NewsBites**
Twice-weekly, high-level executive summary of the most important news relevant to cybersecurity professionals.

**OUCH!**
The world’s leading monthly, free security awareness newsletter designed for the common computer user.

**Webcasts**

**Ask the Experts Webcasts**
SANS experts bring current and timely information on relevant topics in IT Security.

**Analyst Webcasts**
A follow-on to the SANS Analyst Program, Analyst Webcasts provide key information from our whitepapers and surveys.

**Other Free Resources** (*No portal account is necessary*)

- InfoSec Reading Room
- Top 25 Software Errors
- 20 Critical Controls
- Security Policies
- Intrusion Detection FAQs
- Tip of the Day
- Security Posters
- Thought Leaders
- 20 Coolest Careers
- Security Glossary
- SCORE (Security Consensus Operational Readiness Evaluation)

**SAVE $400**
Register and pay by Feb 7th
Use code EarlyBird18

www.sans.org/sans-2018

As the leading provider of information defense, security, and intelligence training to military, government, and industry groups, the SANS Institute is proud to be a Corporate Member of the AFCEA community.