Las Vegas
Jan 28 - Feb 2, 2018

Protect Your Business | Advance Your Career

Eight hands-on, immersion-style courses taught by real-world practitioners.

See inside for courses offered in:
- Cyber Defense
- Ethical Hacking
- Penetration Testing
- Intrusion Detection
- Digital Forensics
- Security Operations

“SANS provides a fantastic breadth of information that is very useful and delivered extremely well.”
- Adam Harrison, Verizon

www.sans.org/las-vegas
SANS 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, which guarantees what you learn in class will be up to date and relevant to your job. The SANS Las Vegas 2018 lineup of instructors includes:

- Adrien de Beaupre
  Certified Instructor
  @adriendb
- Jeff McJunkin
  Instructor
  @jeffmcjunkin
- Hal Pomeranz
  Faculty Fellow
  @hal_pomeranz
- Kevin Fiscus
  Principal Instructor
  @kevinbfiscus
- Seth Misenar
  Senior Instructor
  @sethmisenar
- Jonathan Ham
  Certified Instructor
  @jjhamcorp
- My-Ngoc Nguyen
  Certified Instructor
  @MenopM
- Stephen Sims
  Faculty Fellow
  @Steph3nSims
- Stephen Sims
  Faculty Fellow
  @Steph3nSims
- Seth Misenar
  Senior Instructor
  @sethmisenar

Evening Bonus Sessions

Take advantage of these extra evening presentations and add more value to your training. Learn more on page 9.

KEYNOTE: An Interactive Look at Cyber Crime & Today’s Threat Landscape
– Stephen Sims

Actionable Detects: Blue Team Cyber Defense Tactics
– Seth Misenar

HTTPDeux
– Adrien de Beaupre

Building Your Own Kickass Home Lab
– Jeff McJunkin

– My-Ngoc Nguyen

Save $400 when you register and pay by December 6th using code EarlyBird18

Courses at a Glance

<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>Page 1</td>
</tr>
<tr>
<td>SEC401</td>
<td>Security Essentials Bootcamp Style</td>
<td>Page 2</td>
</tr>
<tr>
<td>SEC503</td>
<td>Intrusion Detection In-Depth</td>
<td>Page 3</td>
</tr>
<tr>
<td>SEC504</td>
<td>Hacker Tools, Techniques, Exploits, and Incident Handling</td>
<td>Page 4</td>
</tr>
<tr>
<td>SEC511</td>
<td>Continuous Monitoring and Security Operations</td>
<td>Page 5</td>
</tr>
<tr>
<td>SEC560</td>
<td>Network Penetration Testing and Ethical Hacking</td>
<td>Page 6</td>
</tr>
<tr>
<td>SEC642</td>
<td>Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques</td>
<td>Page 7</td>
</tr>
<tr>
<td>FOR508</td>
<td>Advanced Digital Forensics, Incident Response, and Threat Hunting</td>
<td>Page 8</td>
</tr>
</tbody>
</table>

Register today for SANS Las Vegas 2018!
www.sans.org/las-vegas
For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/las-vegas-2018/courses

“SEC301 was an excellent course with enormous amounts of valuable and actionable information provided in a short period of time.”
-CARL MASSE, PUBLIC SAFETY

“The instructor was phenomenal, engaging, articulate, a master of the material, and made day one information very easy to follow.”
-KEVIN FLAHERTY, DARPA

My-Ngoc Nguyen  SANS Certified Instructor

My-Ngoc Nguyen (pronounced Mee-Nop Wynn) is the CEO/Principal Consultant for Secured IT Solutions. She has 15 years of experience in information systems and technology, with the past 12 years focused on cybersecurity and information assurance for both the government and commercial sectors. My-Ngoc is highly experienced in IT security and risk methodologies and in legal and compliance programs. She led a cybersecurity program under a federal agency for a highly-regulated, first-of-a-kind project of national importance. With that experience, she has been helping client organizations in both the public and private sectors implement secure and compliant business processes and IT solutions using defense-in-depth and risk-based approaches. Along with a master’s degree in management information systems, she has top security certifications that include GPEN, GCIH, GSEC, and CISSP, and is a former QSA. She is a member of the FBI’s InfraGard, the Information Systems Security Association (ISSA), the Information Systems Audit and Control Association (ISACA), and the International Information Systems Security Certification Consortium (ISC). My-Ngoc founded the non-profit organization CyberSafeNV to raise security awareness among Nevada residents and is currently the organization’s chairperson. @MenopN

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.
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 who 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 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.

SEC401: Security Essentials Bootcamp Style teaches 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.

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.

SEC401: Security Essentials Bootcamp Style teaches 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.

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.

SEC401: Security Essentials Bootcamp Style teaches 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.

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.

SEC401: Security Essentials Bootcamp Style teaches 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.

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.

SEC401: Security Essentials Bootcamp Style teaches 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.

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.

SEC401: Security Essentials Bootcamp Style teaches 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!
Six-Day Program  
Sun, Jan 28 - Fri, Feb 2  
9:00am - 5:00pm  
36 CPEs  
Laptop Required  
Instructor: Jonathan Ham

Who Should Attend
- Intrusion detection (all levels), system, and security analysts
- Network engineers/administrators
- Hands-on security managers

“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 to alerts and the ability to examine them in order to give them meaning and context. You will learn to investigate and reconstruct activity to determine 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.

Jonathan Ham  SANS Certified Instructor  
Jonathan is an independent consultant who specializes in large-scale enterprise security issues, from policy and procedure, through staffing and training, to scalable prevention, detection, and response technology and techniques. With a keen understanding of ROI and TCO (and an emphasis on process over products), he has helped his clients achieve greater success for over 20 years, advising in both the public and private sectors, from small start-ups to Fortune 500 companies. He’s been commissioned to teach NCIS investigators how to use Snort, performed packet analysis from a facility more than 2000 feet underground, and chartered and trained the Cyber Incident Response Team for one of the largest U.S. civilian federal agencies. He has held the CISSP, GSEC, GCIA, and GCIH certifications and is a member of the GIAC Advisory Board. A former combat medic, Jonathan still spends some of his time practicing a different kind of emergency response, volunteering and teaching for both the National Ski Patrol and the American Red Cross. @jhamcorp
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 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.”

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 those attacks. 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.

Kevin Fiscus
SANS Principal Instructor

Kevin Fiscus is the founder of and lead consultant for Cyber Defense Advisors, where he performs security and risk assessments, vulnerability and penetration testing, security program design, policy development, and security awareness with a focus on serving the needs of small and mid-sized organizations. Kevin has over 20 years of IT experience and has focused exclusively on information security for the past 12. He currently holds the CISA, GPEN, GREM, GMOB, GCED, GCFA-Gold, GCIA-Gold, GCIH, GAWN, GPAA, GCWN, GCSC-Gold, GSEC, SCAT, RCSE, and SnortCP certifications and is proud to have earned the top information security certification in the industry, the GIAC Security Expert. Kevin has also achieved the distinctive title of SANS Cyber Guardian for both red team and blue team. Kevin has taught many of SANS’s most popular classes including SEC401, SEC464, SEC503, SEC504, SEC542, SEC560, SEC561, SEC575, FOR508, and MG1414. #kevinbfiscus

See page 13 for details.
Continuous Monitoring and Security Operations

We continue to underestimate the tenacity of our adversaries! Organizations are investing significant time and financial and human resources trying 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, 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.

“We continue to underestimate the tenacity of our adversaries!”

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 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.

“The information is presented in real-world scenarios, which pushes me to think and better prepares me.”

-Reginald Rudolph, DoD

“SEC511 is a VERY worthwhile addition to the curriculum for Blue Teamers.”

-Robert Peden, NextGear Capital

Seth Misenar  SANS Senior Instructor

Seth Misenar is the founder 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 served as both a physical and network security consultant for Fortune 100 companies and the Health Insurance Portability and Accountability Act, as well as an 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 the CISSP, GPEN, GWAPT, GSEC, GCIA, GCHI, GCWN, GCFA, and MCSE. @sethmisenar

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/las-vegas-2018/courses
As a cybersecurity professional, you have a unique responsibility to find and understand your organization’s vulnerabilities and to work diligently to mitigate them before the bad guys pounce. Are you ready? SANS SEC560, our flagship course for penetration testing, fully arms you to address this task head-on.

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.

Jeff McJunkin is a senior staff member at Counter Hack Challenges with more than nine years of experience in systems and network administration and network security. His greatest strength is his breadth of experience, which includes network and web application penetration testing, digital/mobile forensics, technical training, and systems architecture. Jeff is a computer security/information assurance graduate of Southern Oregon University and holds many professional certifications. He has also competed in many security competitions, including taking first place at a regional NetWars competition and a U.S. Cyber Challenge capture-the-flag competition, as well as joining the Red Team for the Pacific Rim Collegiate Cyber Defense Competition. His personal blog can be found at http://jeffmcjunkin.com/.
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 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?

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 has a great teaching style. He is able to explain complex topics and break them down into simpler ideas.”

-ANDREW MITCHELL, HAPPY STATE BANK

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, GCIA, GSEC, CISSP, OPST, and OPSA. When not geeking out he can be found with his family, or at the dojo. @adriendb

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/las-vegas-2018/courses
“Many people lack good forensics skills; being able to figure out what happened is sometimes more important than fixing it.”

-Justin Davis,
St. Jude Medical

Who Should Attend

> Incident response team members
> Threat hunters
> Experienced digital forensic analysts
> Information security professionals
> Federal agents and law enforcement
> Red team members, penetration testers, and exploit developers
> SANS FOR500 (formerly FOR408) and SEC504 graduates

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!

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. Hal is recognized as an expert analyzer of Linux and Unix systems in Windows or Mac environments. 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

See page 13 for details.
Enrich your SANS training experience! Evening talks led by our instructors and selected subject-matter experts help you broaden your knowledge, hear from the voices that matter in computer security, and get the most for your training dollar.

**KEYNOTE: An Interactive Look at Cyber Crime and Today's Threat Landscape**  
Stephen Sims  
Let’s take a journey through the most common attack trends, malicious software, and techniques used by adversaries today. Cyber-criminals closely monitor the landscape for changes, actively respond to these changes, and remain one step ahead of our efforts to maintain an acceptable level of security. It is critical for our defenders to keep up with these ever-changing techniques. Surprisingly, the success of cyber-criminals often depends on basic mistakes still made by users. Join Stephen as he exploits publicly and privately disclosed vulnerabilities involving applications such as Internet Explorer/Edge and Skype and reverse engineers live Ransomware. This presentation will weave in and out of high-level definitions and concepts, all the way to advanced demonstrations and reverse engineering.

**Actionable Detects: Blue Team Cyber Defense Tactics**  
Seth Misenar  
Organizations relying on third parties to detect breaches can go almost a full year before finding out they have been compromised. Detect the breach yourself, and on average, you will find it within about a month of the initial occurrence. Mistaking detection and defense against modern adversaries as “too costly” to perform can result in a very expensive miscalculation – especially when you consider the substantially increased price of response and recovery with breach duration. Seth Misenar’s ever-evolving Actionable Detects presentation provides you with the tactics, techniques, and procedures to once again take pride in your Blue Team cyber capabilities. Not applying these lessons learned could prove costly in the face of adapting threat actors. Dig in and learn to hold your head high when talking about your defensive cyber operations capabilities.

**HTTPDeux**  
Adrien de Beaupre  
This presentation will discuss the relatively new HTTP2 protocol that has been recently adopted as a standard and widely implemented. Most browsers and web servers can support it, but relatively little security research has been done on the new protocol. There are very few tools to perform security testing, and penetration testing over HTTP2 is challenging. The presentation will be a live demo of a HTTP2 vulnerability being exploited.

**Building Your Own Kickass Home Lab**  
Jeff McJunkin  
Building your own home lab is a great way to keep up with the ever-changing IT world. Well, how does one actually go about building a home lab? That’s the part that gets more complicated. Do you really need a whole rack full of off-lease servers and some enterprise-grade switches? No! New-ish high-end servers and workstations are surprisingly powerful and capable of mocking up a pretty complicated network, including attacker systems and even incorporating wireless communications. In this talk, Jeff will walk through both the hardware and software stacks he uses and recommends, including a number of ways to incorporate Microsoft software without paying exorbitant licensing fees. Jeff will also outline a basic lab design that can be used for a number of scenarios.

My-Ngoc Nguyen  
“You take the blue pill, the story ends. You wake up in your bed and believe whatever you want to believe. You take the red pill, you stay in wonderland, and I show you how deep the rabbit hole goes.” – Morpheus, to Neo [src]  
Take the red pill, come join us down this rabbit hole, and get your head out of the sand to better protect yourself, your company/organization, and the things that matter to you (e.g., your loved ones, your finances, your identity). In this presentation, you will get insights into common misconceptions and trends that have led to many breaches, especially those that were headlined. We’ll touch on some details from those headlined breaches to show commonalities, address the main misconceptions, describe attackers’ approaches, provide some statistics, and most importantly, provide helpful tips applicable to all members of the audience.

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

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

-ROBERT JONES, TEAM JONES, INC.

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

“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 | www.giac.org

*GIAC and OnDemand Bundles are only available for certain courses.
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? 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 this 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 skills and knowledge that a GIAC Certification provides. Exams are psychometrically designed to establish competency for related job tasks.
- Consider offering trade-offs for the investment. Many professionals build annual training expenses into their employment agreements even before joining a company. Some offer to stay for a year after they complete the training.
Future Training Events

Miami ........................................ Miami, FL ................ Nov 6-11
San Francisco Winter ............. San Francisco, CA . Nov 27 - Dec 2
Austin Winter ...................... Austin, TX ........ Dec 4-9

Cyber Defense Initiative
Washington, DC Dec 12-19

Security East
New Orleans, LA Jan 8-13, 2018

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
Orlando, FL Apr 3-10

Baltimore Spring ............... Baltimore, MD ........ Apr 21-28

Security West
San Diego, CA May 11-16

Future Summit Events

Pen Test HackFest ........... Bethesda, MD .......... Nov 13-20
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
Blue Team ..................... Louisville, KY .... Apr 23-30
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 for up-to-date Community course information.
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 January 3, 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.

SANS Voucher Program

Expand your training budget!
Extend your fiscal year. The SANS Voucher Program provides flexibility and may earn you bonus funds for training.

www.sans.org/vouchers

**Top 5 reasons to stay at the Tuscany Suites and Casino**

1. All SANS attendees receive complimentary high-speed Internet when booking in the SANS block.
2. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
3. By staying at the Tuscany Suites and Casino, you gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the training event.
4. SANS schedules morning and evening events at the Tuscany Suites and Casino that you won’t want to miss!
5. Everything is in one convenient location!

Inspired by the Tuscany region of Northern Italy, the Tuscany Suites and Casino hotel boasts a warm and welcoming atmosphere surrounded by lush gardens, some of the largest standard hotel suites in the city, and thoughtful amenities to ensure the most comfortable stay possible. Within walking distance to The Strip, experience the easygoing elegance and personalized service that sets the Tuscany Suites and Casino apart from other off-the-strip hotels.

**Special Hotel Rates Available**

A special discounted rate of $102.00 S/D will be honored based on space availability.

Should the prevailing government per diem rate fall below the SANS group rate, government per diem rooms will be made available with proper ID; you will need to call reservations and ask for the SANS government rate. Both rates include high-speed Internet in your room and are only available through January 5, 2018.

**Payment Information**

**Pay Early and Save**

<table>
<thead>
<tr>
<th>DATE</th>
<th>DISCOUNT</th>
<th>DATE</th>
<th>DISCOUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>12-6-17</td>
<td>$400.00</td>
<td>12-27-17</td>
<td>$200.00</td>
</tr>
</tbody>
</table>

*Some restrictions apply. Early bird discounts do not apply to Hosted courses.

**SANS Simulcast**

To register for a SANS Las Vegas 2018 Simulcast course, please visit www.sans.org/event/las-vegas-2018/attend-remotely.

**Registration Information**

REGISTER ONLINE AT www.sans.org/las-vegas

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.

**Hotel Information**

Tuscany Suites and Casino
255 E. Flamingo Road  | Las Vegas, NV  89169
702-893-8933

www.sans.org/event/las-vegas-2018/location
Create a SANS Account today to enjoy these free resources at sans.org/account

Newsletters

NewsBites
Twice-weekly, high-level executive summaries 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.

@RISK: The Consensus Security Alert
A reliable weekly summary of (1) newly discovered attack vectors, (2) vulnerabilities with active new exploits, (3) how recent attacks worked, and (4) other valuable data.

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.

WhatWorks Webcasts
The SANS WhatWorks webcasts bring powerful customer experiences showing how end users resolved specific IT security issues.

Tool Talks
Tool Talks are designed to give you a solid understanding of a problem, and how a vendor’s commercial tool can be used to solve or mitigate that problem.

Other Free Resources

- 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 when you pay for any 4-, 5-, or 6-day course and enter the code “EarlyBird18” by December 6th. www.sans.org/las-vegas

To be removed from future mailings, please contact unsubscribe@sans.org or (301) 654-SANS (7267). Please include name and complete address.