SANS

HackFest

SUMMIT

Program Guide

@SANSPenTest  #SANSHackFest

Agenda

All Summit Sessions will be held in the Regency Ballroom (unless noted).

All approved presentations will be available online following the Summit at ***sans.org/hackfest-archive***

Monday, November 12

7:00-9:00 am	**Registration & Coffee** (LOCATION: REGENCY BALLROOM FOYER)
9:00-9:15 am	***Opening Remarks*** ***Ed Skoudis****, Fellow, SANS Institute*
9:15-10:15 am	***Keynote: Accidental Hero: How a Minor Accounting Error Gave Birth to the Field of Cybersecurity*** You know the story – no, the legend – of Cliff Stoll's transformation from ivory tower astronomer to accidental international cyber counterspy. In fact, there's a good chance that you've not only read his *New York Times* bestselling account of this adventure, but that it inspired your own career. But you've never heard the story like this before – straight from the man himself. Cliff is feistier than ever and will delight us all with his anecdotes and wisdom in this very special keynote address to kick off the 5th annual Pen Test Hackfest. ***Clifford Stoll****, Author, "The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage"*
10:15-10:45 am	**Networking Break** (LOCATION: REGENCY BALLROOM FOYER)
10:45-11:20 am	***NoSQL Injection: It Isn't Just MongoDB*** This talk will cover NoSQL injection across multiple non-relational databases (including MongoDB). Adrien will also release a new NoSQLi SANS Pen Test Cheat Sheet. ***Adrien de Beaupre*** *(@adriendb), Principal Instructor, SANS Institute*
11:20-11:55 am	***Hatfields and McCoys: Feuds, Anti-Patterns and Other Crossed Connections in the Dev/Sec Relationship*** Developers want security to get out of their way. Security wants to stop finding the same old security flaws they found last month. Developers want fewer, sleepless nights before a big launch. Security wants everything to be tested properly before it goes out into the world. How do we reconcile our different missions to build fully featured, secure products, on time and on budget? Thoughts on broken tools and problematic systems from a front-line developer who has spent the last two years building broken things as teaching tools for budding infosec professionals. ***Rachelle Saunders*** *(@afterthree), Experience Team Lead, Helical Levity*
12:00-1:15 pm	**Lunch** (LOCATION: REGENCY BALLROOM FOYER)

Monday, November 12

1:15-1:50 pm	***Timelines: Not Just for Incident Response*** Incident handlers create timelines of an attack by pulling together network and file forensics as well as logs to create a picture of what an attacker did and when. Penetration testers also often need to recall what they did and when. There's nothing like that sinking feeling when the client calls and says their production database went down at 3:25 - and blames you. Keeping detailed records of your testing can help prove you did not cause an outage (or recreate the steps that did create one), keep track of what tests have and haven't been performed, and provide evidence during report writing or remediation. Integrating attack tools such as interception proxies and keyloggers with defensive tools such as SIEMs into your testing practices can help you automatically keep track of your activity. This allows you to recall all of the steps you took during testing, correlate results from different tools or testers, and create better reports faster. ***Joe Schottman*** *(@JoeSchottman), Security Analyst, BB&T*
1:50-2:45 pm	***The Top Ten Reasons It's GREAT to Be a Pen Tester...And How You Can Help Fix That PROBLEM*** Turns out, being a pen tester is actually quite wonderful. You get to hack stuff and someone else has to deal with the problems you find. But that's BAD! This presentation is loaded with practical tips for restructuring your pen tests to provide much more business value. With tons of recommendations for pen testers as well as non-pen testers, you'll gain knowledge of how to get a lot more from your very next pen test! ***Ed Skoudis****, Fellow, SANS Institute*
2:45-3:05 pm	**Networking Break** (LOCATION: REGENCY BALLROOM FOYER)
3:05-3:40 pm	***The Changing Landscape of Offense*** Defense is changing, and offense has to adapt accordingly. In this talk Tim will discuss the changes in the landscape he's seen in his decade of experience in offense, and how you can be more offensive. The goal of offense is to emulate real world attackers so the defenders can test the technology and make respond to attacks. Help the blue team by being more offensive. ***Tim Medin*** *(@timmedin), Principal Consultant, Red Siege; Principal Instructor, SANS Institute*
3:40-4:15 pm	***Wrangling Malware for Fun and Pen Testing*** As pen testers, we're always looking for ways to crack the perimeter and establish a foothold. But we're busy, so why reinvent the wheel? Malware is making it past companies' perimeters every day. This talk will explore the idea of leveraging malware delivery and obfuscation techniques for pen testing. We will take a phishing email with an obfuscated malware payload, deobfuscate it, review the code, replace the malware with a pen testing payload, repackage it, and deploy it for pen testing. ***John Freimuth****, Sr. Security Engineer, Dignity Health* ***Alex Stockwell*** *(@astockwell), Security Engineer, Dignity Health*
6:00-9:00 pm	***Summit Night Out: World of Hackfest*** Hackfest takes over a local watering hole for unlimited snacks, drinks, networking, and a custom challenge! Remember to wear your Summit badge and join us at World of Beer, 7200 Wisconsin Avenue, (a 5-minute walk from the hotel) to get in on all of the action.

Thank you for attending the SANS Summit.

Please remember to complete your evaluations for today.
You may leave completed surveys at your seat or turn them in to the SANS registration desk.

Tuesday, November 13

8:00-9:00 am	**Registration & Coffee** (LOCATION: REGENCY BALLROOM FOYER)
9:00-10:00 am	***Keynote: A Year Of Gaining Superpowers*** Technical leaders have a responsibility to stay technical, and the work we do in vertical communications sometimes means that we get pulled away from actual technical work. Let's talk about how to stay technical in information security, where there's a huge premium on interpersonal communications skills—so much so that maintaining your skills takes a back seat. If you want to rise in infosec, you too will have to step away from the keyboard—but not all the way, ever, if you want to be brilliant at your work and still capable of speaking on, much less understanding, solid technical research at the major conferences. We'll discuss and show how to get involved in three real-world examples: CTFs, real directed offensive and defensive security studies, and participating in open projects. ***Tarah M. Wheeler*** *(@tarah), Senior Director, Data Trust & Threat and Vulnerability Management, Splunk*
10:00-10:35 am	***The Clouds Are Out to Get Me!*** There are so many tools for attacking traditional Active Directory environments, but what about cloud environments? What if more and more companies in the future bypass AD altogether and run everything as a cloud BYOD infrastructure? What happens to the tools and techniques you have been using against AD reliably since 1999? Ever want to use one cloud service to attack another? In this presentation we will answer these questions. We will also share numerous tools and techniques we have created at BHIS to successfully attack many cloud services. ***John Strand*** *(@strandjs), Owner, Black Hills Information Security; Senior Instructor, SANS Institute*
10:35-11:00 am	**Networking Break** (LOCATION: REGENCY BALLROOM FOYER)
11:00-11:35 am	***Extending Burp to Find Struts and XXE Vulnerabilities*** How do you test for Struts vulnerabilities in clients' web apps? Have you tried writing a Burp plug-in to help? Extending Burp is easier than you might think. We'll cover Burp Extension programming in Python, the power of Burp's Collaborator, and adapting Struts and XXE exploits to find vulnerabilities automatically. This will culminate in the discovery of a web app zero day. ***Chris Elgee*** *(@chriselgee), Pen Tester, Counter Hack Challenges*
11:35 am - 12:10 pm	***Come to the Dark Side: Python's Sinister Secrets*** The author of SANS's Python course (SEC573) will share secrets about: • Abusing the input function • Escaping restricted Python shells • Embedding a backdoor in PYC bytecode • Remote execution of code through serialized data (pickle). For every attack, Mark will also discuss mitigations. ***Mark Baggett*** *(@markbaggett), Senior Instructor, SANS Institute*
12:10-1:15 pm	**Lunch** (LOCATION: REGENCY BALLROOM FOYER)

Tuesday, November 13

1:15-1:50 pm	***Ubiquitous Shells*** Ubiquiti network gear has become a favorite among tech enthusiasts. Unfortunately, various Ubiquiti products have had some serious vulnerabilities and security incidents in recent history, and like most products, there are deployment decisions that can dramatically impact the security of the network. There are even features that can provide shell access to the network from the internet. Listen in as we discuss how to go from zero access from the Internet to a root shell via Ubiquiti gear. We'll also explore methods to weaponize the Unifi APs and Unifi Cloud Key devices and use them as attack platforms. ***Jon Gorenflo*** *(@flakpaket), Founder, Fundamental Security; Community Instructor, SANS Institute*
1:50-2:25 pm	***Grape Jelly: How Threat Intel Enhances a Red Team*** Before you RedTeam, get Threat Intel! • Get OSINT and passive recon for scoped ranges! Start your test planning with the most complete and up-to-date intelligence concerning your targets! • Leverage Threat Intelligence research (environmental data correlated to CVEs) to nominate exploitable candidates. • Intel reports extrapolating PoCs, malware behaviors, technique shift/evolution, and actual incidents relevant to your test methodology, select from a curated list for your test Red Team scenario design! ***Lori Stroud****, Cyber Threat Analyst, BB&T*
2:25-2:45 pm	**Networking Break** (LOCATION: REGENCY BALLROOM FOYER)
2:45-3:20 pm	***Domain Fronting for the Win!*** The advent of cloud technologies has provided significant advantages for malicious attackers and penetration testers. When combined with domain fronting, the cloud can be a deadly combination for defenders. This talk will explain what domain fronting is, how it works, and why you should use it in your penetration tests. ***Matthew George*** *(@sircosec), Analyst, phia, LLC*

Tuesday, November 13

3:20-3:45 pm	***Post Exploitation in Developer Environments*** This talk will zoom in to the cache of goodies which developers leave lying around that an attacker could leverage access valuable information and/or to pivot through a target environment. It will also highlight some of the tools available to developers and InfoSec professionals to find and prevent these sorts of information leakages. Every day, developers interact with a variety of source-code repositories and environments, often both inside their corporate firewalls and outside on public hosting platforms such as GitHub.com and Amazon AWS. These source-code repositories can provide a wealth of information about a target environment, in addition to being a potential value all on its own. Best of all, a large amount of information about an environment can be gleamed quietly without having to actively scan the network. If you are a penetration tester, are you able to find this information in your customer's environment? Do you know how to help their developers prevent these leakages in the first place? Remember "prevention is ideal, but detection is a must!" ***Ian Lee*** *(@IanLee1521), Computer Engineer, Lawrence Livermore National Lab*
3:45-4:20 pm	***"The Future is Going to be More Money" – Majority Reports*** If you have lived through enough disruption of the industry, you can start to develop a hypothesis about how changes will occur. Today, I present to you a story of hacking in the future, not quite with the precogs but with a higher level of entry and higher bar. What does hacking in the future look like and how will it impact us? What are the barriers today, and what can we expect? We will be exploring our modern infrastructure and showing examples of human interface devices that we can use for good – or for evil. Ok, Google, give me a shell. ***Moses Frost****, Security Architect, Cisco Systems; Instructor, SANS Institute*
3:45-4:20 pm	**Core NetWars Experience** *Hosted by* ***Matthew Toussain***

Thank you for attending the SANS Summit.

Please remember to complete your evaluations for today.
You may leave completed surveys at your seat or turn them in to the SANS registration desk.