OFFENSE
INFORMS
DEFENSE

SANS

HackFest

INFORMATION SECURITY
SUMMIT

CRYSTAL CITY, VA

Program Guide

@SANSPenTest #SANSHackFest

Agenda

All Summit Sessions will be held in the Salon AB (unless noted).

All approved presentations will be available online following the Summit at
https://pen-testing.sans.org/resources/summit-archives
An e-mail will be sent out as soon as the presentations are posted, typically within 5 business days of the event.

Wednesday, November 2

8:00-9:00am	**Registration & Coffee** (LOCATION: CRYSTAL FOYER)
9:00-10:00am	***Welcome, Overview & Opening Keynote*** ***Ed Skoudis**, Fellow, SANS Institute*
10:00-10:30am	**Networking Break** (LOCATION: SALON C,D,E)
10:30-11:05am	***Go Ahead, Run Your Own Mail Server. What, Are You Chicken?*** No one likes a tool jockey or a script kiddie – and if all you know how to do are press buttons and read tool output, I have bad news for you – you're a crappy pen-tester. It's not enough to know how to use your tools, you have to know how things work. In this talk, I will make a logical case for ignoring @SwiftOnSecurity and doing something that no sane person in the late 2010s thinks is a good idea – run your own mail server. ***Matt Linton**, Chaos Specialist, Google*
11:05am-Noon	***Offense Informs Defense*** We've all heard it a bunch of times – offense must inform defense. But what does that really mean? In this panel, experienced offensive and defensive experts will share ideas about how to radically improve defenses based on lessons learned from in-the-trenches penetration tests, red team exercises, and other offensively minded work. The panelists will share their best tips and tricks that you can apply in your own environment to measurably improve your defensive posture against today's latest attack techniques. MODERATOR: ***Ed Skoudis**, Fellow, SANS Institute* PANELISTS: ***Rob "Mubix" Fuller**, Principal Security Engineer, Hak5/Silicon Valley* ***Lee Neely**, Senior Cyber Analyst, Cyber Security Program, Lawrence Livermore National Lab* ***Derek Rook**, Senior Security Infrastructure Engineer, Gaikai, Inc.* ***Yolonda Smith**, Director of Product Management, Pwnie Express*
Noon-1:15pm	**Lunch**

Wednesday, November 2

1:15-1:50pm

Your Fly Is Open: Perspectives on Pen Testing From a Professional Victim

Imagine what you could learn by watching real attackers 0wn your systems hundreds of times, every single day. That's my life: I'm a professional hacking victim. Over the last six years, my twittering honeypot, @netmenaces, has tweeted details on over 275,000 attacks. The lessons learned from examining some of those attacks have made me a better pen tester, and in this presentation, I want to pass along some highlights to you. Along the way, I'll interweave these lessons with a few interesting war stories highlighting their applicability. I may even tell about the time I 0wned the network infrastructure for an entire country.

FYI: Ed told me I could only do a talk involving a honeypot if it was "offensive," so, essentially, the sky's the limit. The front row of this talk should be considered a "splash zone." Ponchos recommended.

Tom Liston*, Consultant – Cyber Network Defense, DarkMatter*

1:50-2:25pm

Press Button For a Short Speech from Raphael Mudge

Raphael will discuss topics related to red team operations, payloads, and the evolving world of network defense.

Raphael Mudge*, Founder & Principal, Strategic Cyber LLC*

2:25-3:00pm

Six Degrees of Domain Admin:
Using BloodHound to Accelerate Red Team Operations

Active Directory domain privilege escalation is a critical component of most penetration tests and red team assessments, but standard methodology dictates a manual and often tedious process – gather credentials, analyze new systems we now have admin rights on, pivot, and repeat until we reach our objective. Then, and only then, we can look back and see the path we took in its entirety. But that may not be the only, nor shortest, path we could have taken.

By combining the concept of derivative admin (the chaining or linking of administrative rights), existing tools, and graph theory, we have developed a capability called BloodHound, which can reveal the hidden and unintended relationships in Active Directory domains. BloodHound is operationally focused, providing an easy-to-use web interface and PowerShell ingestor for memory-resident data collection and offline analysis.

BloodHound offers several advantages to both attackers and defenders. Otherwise invisible, high-level organizational relationships are exposed. Most possible escalation paths can be efficiently and swiftly identified. Simplified-data aggregation accelerates blue and red team analysis. BloodHound has the power and the potential to dramatically change the way you think about and approach Active Directory domain security.

Rohan Vazarkar*, Penentration Tester & Red Teamer – Adaptive Threat Division, Veris Group*

3:00-3:30pm **Networking Break** (LOCATION: SALON C,D,E)

Wednesday, November 2

3:30-4:05pm	***Everything You Ever Wanted to Know About Pen Testing (But Were Afraid to Ask)*** No fear here! John Strand will tackle ALL your burning pen testing questions, even the ones you never knew you had, and get you into places you didn't even know you wanted to go. How can you circumvent AV, bypass whitelisting, get around next-gen firewalls, use a JTAG;, perform a solid Red Team Assessment, and get your mom to go with you on a physical pen test? John has the answers. ***John Strand**, Senior Security Analyst, Black Hills Information Security*
4:05-4:40pm	***Building Your Own Kick-Ass Home Lab*** Building your own home lab is a great way to keep up with the ever-changing IT world. So how does one actually go about building a home lab? That's where it 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, capable of mocking up a pretty complicated network, including attacker systems and even incorporating wireless communications. This talk will walk you through both the hardware and software stacks Jeff uses and recommends, including a number of ways to incorporate Microsoft software without paying exorbitant licensing fees. He'll also outline a basic lab design that can be used for a number of scenarios. ***Jeff McJunkin**, Senior Staff, Counter Hack Challenges; Instructor, SANS Institute*
4:40-5:00pm	***Day One Wrap-Up*** ***Ed Skoudis**, Fellow, SANS Institute*
6:30-9:30pm	**Core NetWars Tournament** Core NetWars Tournament is a computer and network security challenge designed to test a participant's experience and skills in a safe environment. It is accessible to a broad level of player skill ranges and is split into separate levels so that advanced players may quickly move through earlier levels to the level of their expertise.

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.

@SANSPenTest **#SANSHackFest**

Thursday, November 3

8:00-9:00am

Registration & Coffee (LOCATION: CRYSTAL FOYER)

9:00-9:45am

I'm Not Being Evasive!

@jameslyne, instructor at the SANS institute and Global Head of Research at Sophos, takes us through the latest evasion techniques for payloads spanning the plethora of top penetration testing tools of today. From tricks at the network with bespoke TLV shifts to custom stages upgrade your tests with techniques the higher-end attackers employ and beyond!

James Lyne*, G, Sophos; Director – EMEA, SANS Institute*

9:45-10:20am

Mining Meteor

Meteor is a game-changing framework for rapid software development and is the top rated framework on GitHub. One of Meteor's nicest features is that it allows developers to build real-time applications quickly and easily. As part of the framework, data and code are pushed to the clients so rendering is done on the client. However, sometimes too much code or data is sent to the clients even though it isn't displayed. In this talk, I'll demonstrate how to extract data from the local databases, how to find hidden pages, and how to extract information you were not intended to have access to. We will mine Meteor for everything we can.

Tim Medin*, Senior Technical Analyst, Counter Hack; Certified Instructor, SANS Institute*

10:20-10:45am

Networking Break (LOCATION: SALON C,D,E)

10:45-11:20am

I'll Let Myself In: Tactics of Physical Pen Testers

Many organizations are accustomed to being scared at the results of their network scans and digital penetration tests, but seldom do these tests yield outright "surprise" across an entire enterprise. Some servers are unpatched, some software is vulnerable, and networks are often not properly segmented. No huge shocks there. As head of a Physical Penetration team, however, my deliverable day tends to be quite different. With faces agog, executives routinely watch me describe (or show video) of their doors and cabinets popping open in seconds. This presentation will highlight some of the most exciting and shocking methods by which my team and I routinely let ourselves in on physical jobs.

Deviant Ollam*, Security Auditor & Pen Test Consultant, The CORE Group*

Thursday, November 3

11:20am-12:15pm

Offense Informs Forensics

Whenever really skilled attackers get into deep discussions with super experienced forensics experts, the exchange is fascinating, spinning off choice tips and tricks for better forensicating the bad guys' evidence and profound ideas for how pen testers can hide much better to mimic highly skilled attackers. In this lively panel, forensicators and pen testers alike will share some of the best ideas they've learned for finding attackers as well as avoiding getting detected. Whether you are a pen tester looking for ways to better mimic the bad guys, or a forensics person who wants to sharpen your skills in finding sophisticated attackers, this panel exchange will provide actionable recommendations for you to up your game big time.

MODERATOR: ***Ed Skoudis****, Fellow, SANS Institute*

PANELISTS: ***Jacquelyn Blanchard****, Computer Forensic Examiner (CFE)*
Matt Linton*, Chaos Specialist, Google*
Jake Williams*, Principal Consultant, Rendition InfoSec; Certified Instructor, SANS Institute*

12:15-1:30pm **Lunch**

1:30-2:05pm

I Don't Give One IoTA: Introducing the Internet of Things Attack Methodology

Attacking and assessing IoT can easily miss the forest for the trees. However we need to be comprehensive in our methodology and not end up down a rabbit hole; we need to know how the wind affects each tree, but also the forest as a whole. We even need to make sure we consider the trailer park adjacent to the forest, which may not be quite as resilient to a tornado. We're here to pass along a methodology for testing all of the components of any end-to end IoT solution; from end user hardware, proprietary and standards-based RF (Zigbee, Zwave, BLE/Bluetooth and all sorts of modulation), Wi-Fi, network protocols, mobile device applications (Android and iOS), internet-connected servers, web applications and databases. Come learn how to build a testing lab, investigate some testing tools, and how to apply to a real world test.

Larry Pesce*, Director of Research, InGuardians*

2:05-2:35pm

HTTPDeux and WebSockets?

Modern web applications more and more make use of HTTP/2 or WebSockets to deliver real time and richer content to their clients. As penetration testers, we not only have to be aware of newer protocols, we have to adapt to testing them with the unique and fascinating attack surfaces they provide. Unfortunately the tools we typically use have not adapted to the new reality quite yet. This presentation will discuss web application penetration techniques for HTTP/2 and WebSockets from a co-author of the SANS course SEC642 Advanced Web Application Penetration Testing and Exploitation Techniques.

Adrien de Beaupre*, Certified Instructor, SANS Institute*

Thursday, November 3

2:35-3:10pm

Jittery MacGyver: Testing the Coffee-Stained Giving Tree

These days, Keurig coffee makers are everywhere and they're jam-packed with interesting parts. In this talk, we'll see what makes a Keurig tick, talk about the challenges involved when repurposing them for complex builds, and finally, talk about the broader implications of rooting out potential in things most people deem common and unremarkable.

***Evan Booth**, Maker*

3:10-3:40pm

Networking Break (LOCATION: SALON C,D,E)

3:40-4:15pm

Ghost in the Droid

Ghost detection apps take many forms in the Google Play store, with an active social media community sharing screenshots, energy disturbance levels, and recorded audio and video for ethereal detection events. But what exactly do these apps do? How does an Android phone detect supernatural phenomena through EMF readings, ghost radar, visual observation, or ghost radio? Can it be explained, or do the answers lie beyond our realm of understanding? In this talk, I'll show you how I found these answers, demonstrating techniques for more efficient Android application analysis, and how I learned a thing or two about pen testing mobile apps in the process.

***Josh Wright**, Senior Technical Analyst, Counter Hack; Senior Instructor, SANS Institute*

4:15-10:00pm

Hackfest Hits the Road!

Join Ed Skoudis, Summit speakers and your fellow attendees for a very special off-site event. The details are top secret and will be revealed at the Summit, but it promises to be an unforgettable evening of education and networking. A light dinner and refreshments will be provided.

Give some love to these awesome folks for helping make Hackfest possible:

BLACK HILLS Information Security • 2008 •

InGUARDIANS ADVANCED PERSISTENT TESTING

PWNIE EXPRESS

VERIS GROUP ATD ADAPTIVE THREAT DIVISION

COUNTER HACK

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.***

@SANSPenTest #SANSHackFest

SPEAKERS

Jacquelyn Blanchard, Computer Forensic Examiner (CFE)
From a teenage hacker to an accomplished information security professional hunting bad guys over a 15 year span, Jacquelyn Blanchard focuses on discovering and thwarting bad guys. Although she'd never say it herself, Jacque has done some seriously spooky stuff that helps keep your family safe at night. Once she discovers an intrusion, she clicks all the links, opens all the files, and conducts analysis on all the malware, making the world a little bit better of a place. She believes that, in order to be a good forensicator, one should learn pen testing skills, and vice-versa. By watching what real-world attackers do, Jacque has gained keen insights into how penetration testers can better model their nefarious activities with the goal of helping improve security big time. In her spare time, Jacquelyn enjoys running up and down very steep hills.

Evan Booth, Maker
Evan Booth loves to build stuff out of other stuff. As an engineer for Skookum, a full service software development company in Charlotte, North Carolina, he works to solve a variety of business problems through the creative use of technology. As a human for Earth, he tends to break things for curiosity's sake. Throughout 2013 and into 2014, in an effort to highlight hypocrisy and "security theater" brought about by the TSA, through a research project called "Terminal Cornucopia," Evan created an arsenal ranging from simple, melee weapons to reloadable firearms to remotely trigger incendiary suitcases—all solely comprised of items that anyone can purchase inside most airport terminals *after* the security checkpoint. Given the right ingredients, a big cardboard box can be a time machine, spaceship, minecart, or a telephone booth that only calls people named "Steve" who live in the future.

Adrien de Beaupre, Certified Instructor, SANS Institute
Adrien de Beaupre is a certified SANS instructor and 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.

Matt Linton, Chaos Specialist, Google
Matt is an incident responder with experience throughout the security process, from architecture through penetration. He is formally trained in disaster management and specializes in rapid response, remediation and hardening of compromised environments.

Tom Liston, Consultant - Cyber Network Defense, DarkMatter
Tom Liston is member of the Cyber Network Defense team at Dark Matter, a security consulting firm in the UAE. He is also a Handler for the SANS Institute's Internet Storm Center and co-author of the book Counter Hack Reloaded. Since it began publishing its "Sexiest Man Alive" issue, People Magazine has consistently overlooked Mr. Liston with what can only be described as a blatantly good taste.

James Lyne, Director of Technology Strategy, Sophos;
Director – EMEA, SANS Institute
Director, EMEA at SANS and Director of Technology Strategy at security firm Sophos. James comes from a background in cryptography but over the years has worked in a wide variety of security problem domains including anti-malware and hacking. James spent many years as a hands-on analyst dealing with deep technical issues and is a self-professed "massive geek." Eventually James escaped dark rooms and learned some social skills, and today is a keen presenter at conferences and industry events. With a wide range of experience working in a technical and a strategic capacity from incident response to forensics with some of the world's largest and most paranoid organisations James participates in industry panels, policy groups, and is a frequently-called-upon expert advisor all over the world. James is a frequent guest lecturer and often appears in the media including national TV. As a young spokesperson for the industry James is extremely passionate about talent development and participates in initiatives to identify new talent for the industry and to develop it. Ask James to show you his best geek party trick.

Jeff McJunkin, Senior Staff, CounterHack Challenges
Jeff McJunkin is a senior staff member at CounterHack Challenges with more than nine years of experience in systems and network administration and network security. His greatest strength is his breadth of experience – from network and web application penetration testing to digital/mobile forensics, and from technical training to 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.

Tim Medin, Senior Technical Analyst, Counter Hack;
Certified Instructor, SANS Institute
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 the majority 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. Currently Tim is a certified instructor for the SANS Institute.

Raphael Mudge, Founder & Principal, Strategic Cyber LLC
Raphael Mudge is a programmer based in Washington, DC.

SPEAKERS

Lee Neely, CISSP, CISA, CISM, CRISC, GMOB, GPEN, CCUV, Cyber Security Program, OMBUDS, Lawrence Livermore National Lab
Lee Neely is a Senior Cyber Analyst at LLNL, SANS Mentor and Analyst paper author. He is also the IT Director for the ISC2 East Bay Chapter and Board Treasurer for the Uncle Credit Union. His areas of expertise include mobile device and new technology security.

Larry Pesce, Director of Research, InGuardians
Larry Pesce's history with hardware hacking began with the family TV when he was a kid, rebuilding it after it caught on fire. Both times. His core specialties include hardware and wireless hacking, often in the financial, energy and healthcare sectors. Larry leads research efforts at InGuardians, concentrating on IoT.

Derek Rook, Security Infrastructure Engineer, Gaikai, Inc.
Derek is a 15 year IT veteran specializing in Linux administration and system engineering. Making the shift to security 5 years ago his focus is now on raising security awareness and growing in the field of penetration testing. Derek holds GCIA, GNFA, and GCIH from GIAC, and Offensive Security's OSCP.

Ed Skoudis, Fellow, SANS Institute
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 which help train cyber warriors in how 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 three thousand 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.

Yolonda Smith, Director of Product Manager, Pwnie Express
Yolonda Smith is the Director of Product Management at Pwnie Express, responsible for product strategy and roadmap, and ensuring Pwnie provides security professionals with the visibility they need to identify, characterize and neutralize threats to their wired and wireless assets. A security professional herself, she spent eight years in the U.S. Air Force as a Cyberspace Operations Officer with duties and responsibilities varying from Mission Commander, Advanced Network Operations where her team developed & orchestrated the first DoD Cyber Hunting missions to Flight Commander, Cyber Defense Capabilities Development where her team developed the first and only malware neutralization tool for Predator Drones.

John Strand, Senior Security Analyst, Black Hills Information Security
John Strand is the owner of Black Hills Information Security, a firm specializing in penetration testing, Active Defense and Hunt Teaming services. He is the also the CTO of Offensive Countermeasures, a firm dedicated to tracking advanced attackers inside and outside your network. John is an experienced speaker, having done presentations to the FBI, NASA, the NSA and at various industry conferences.

Rohan Vazarkar, Penentration Tester & Red Teamer –
Adaptive Threat Division, Veris Group
Rohan Vazarkar is a penetration tester and red teamer for Veris Group's Adaptive Threat Division, where he helps assess fortune 500 companies and a variety of government agencies. Rohan has a passion for offensive development and tradecraft, and contributed heavily to EyeWitness and the EmPyre projects. He has presented at BSides DC, BSides Las Vegas, BlackHat Las Vegas, DefCon, and helps develop and teach the 'Adaptive Penetration Testing' course at BlackHat USA.

Jake Williams, Principal Consultant, Rendition InfoSec;
Certified Instructor, SANS Institute
Jake Williams is a Principal Consultant at Rendition Infosec. He has more than a decade of experience in secure network design, penetration testing, incident response, forensics, and malware reverse engineering. Before founding Rendition Infosec, Jake worked with various cleared government agencies in information security roles. Jake is the co-author of the SANS FOR610 course (Malware Reverse Engineering) and the FOR526 course (Memory Forensics). He is also a contributing author for the SEC760 course (Advanced Exploit Development). In addition to teaching these courses, Jake also teaches a number of other forensics and security courses. He is well versed in Cloud Forensics and previously developed a cloud forensics course for a U.S. Government client. Jake regularly responds to cyber intrusions performed by state-sponsored actors in financial, defense, aerospace, and healthcare sectors using cutting edge forensics and incident response techniques. He often develops custom tools to deal with specific incidents and malware reversing challenges.

Josh Wright, Senior Technical Analyst, Counter Hack;
Senior Instructor, SANS Institute
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 cyber warriors in the U.S. military, government agencies, and critical infrastructure providers.