

SANS HackFest 2015

NOVEMBER 16-17

Program Guide

Summit Chairman: Ed Skoudis

#SANSHackFest  @SANSPenTest

Agenda


All Summit Sessions will be held in the Grand Ballroom (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.

Monday, November 16	
8:00-9:00am	Registration & Coffee (LOCATION: GRAND BALLROOM FOYER)
9:00-9:20am	<i>From Salmon to Scarlet: Getting The Most Out of The Many Shades of Red</i> From vuln assessors to pen testers... from security researchers to red teamers... many organizations have at least some mix of offensive skills among their personnel. But how can these different types of offensive capability support the ultimate goal of improving an organization's defenses? Also, how can individuals develop their offensive understanding and skills to serve that goal? In this talk, Ed Skoudis will analyze various offensive roles and share tips and tricks for operationalizing their effectiveness. We will focus on how defenders and attackers alike can provide significantly more value to their organizations through the development of powerful offensive skills. Ed Skoudis , Fellow, SANS Institute, @edskoudis
9:20-10:05am	<i>Hacking Ugly: How Doing Things the "Wrong" Way Sometimes Turns Out Right</i> We've all seen them: A smart and elegant hack that is – in its own way – a thing of beauty. This talk is not about those. While elegance and intelligence have their place, oftentimes brute force and ignorance win the day. While I can, at times, pull a little hacking elegance out of my hat, more often than not, I've found that knowing when "hacking purty" is a waste of time is the most useful tool you can have in your arsenal. I'll show you how "hacking ugly" can make you more productive, tell a few "war stories," and even pass on a few tricks that – if properly used – can make you look like a hacking god! Tom Liston , Principal Information Security Architect, Warner Brothers Entertainment, @tliston
10:05-10:30am	Networking Break and Vendor Expo (LOCATION: GRAND BALLROOM FOYER)



<p>10:30-11:15am</p>	<p>How I Detect Your Crappy Pen Test</p> <p>As pen testers and red teamers, we are increasingly called on to model the activities of ever-stealthier attackers. Indeed, more organizations are looking to pen testers to measure their blue teams' effectiveness and ability to detect attacks. Yet we're under some serious time crunches to get our work done on schedule and within allocated budgets. In this panel, we'll look at how pen test activities are most often detected in enterprises. More importantly, we'll look at how we can utilize effective stealth tactics without completely destroying the budget and schedule.</p> <p>Moderator: Ed Skoudis, Fellow, SANS Institute, @edskoudis Panelists: Tom Liston, Warner Brothers, @tliston Jorge Orchilles, Author, Microsoft Windows 7 Administrator's Reference, @jorgeorchilles Tim Medin, Senior Technical Analyst, CounterHack, @timmedin</p>
<p>11:15am-Noon</p>	<p>Live no Evil – Live on Evil!</p> <p>Hackers often waste obviously beneficial substance, especially reversing value and noise; true achievement requires examining your obfuscated understanding. Fifteen years of staying one step ahead of tens of thousands of hackers creating cryptographic puzzles and challenges shaped my problem solving process. Everything from reversing criminal activity to making things "Google-proof." Let's have a discussion on hacking how hackers think.</p> <p>Ryan "1o57" Clarke, Hacker, Intel Security, Official DEFCON Cryptographer and Puzzlemaster</p>
<p>Noon-1:15pm</p>	<p>Lunch & Learn Presentation (LOCATION: POTOMAC)</p> <p>Prevent - Detect - Respond Derrick Masters</p> <div data-bbox="803 1020 1331 1140" style="border: 1px solid black; padding: 5px;">  </div>
<p>1:15-2:00pm</p>	<p>IoT Devices Fall like Backward Capacitors (Or the Month Josh Was Forced to Wear Pants)</p> <p>Over the summer, Josh took on a special project. The setup was straightforward: login to Amazon, and buy 5 popular Internet of Things (IoT) devices. The goal was also straightforward: build remote exploits for the devices, winning bug bounty money to sufficiently cover the cost of the project.</p> <p>In this talk, Josh will present his findings from his Summer of IoT Hacking, presenting the techniques used for attacking these embedded, purpose-built devices. He will also share the entertaining and heart-breaking experiences from working with vendors to claim bug bounty prizes, and how you can apply these techniques to expand your breadth of skills and knowledge in your next penetration test.</p> <p>Josh Wright, Senior Technical Analyst, CounterHack, @joswright</p>

2:00-2:45pm

What Goes In Must Come Out: Egress-Assess and Data Exfiltration

Every organization faces the possibility of being hacked, and it's a good idea to adopt Microsoft's "assume breach" mentality. It's important to note that most hackers today aren't in it for the lulz, but are in it to steal data. Organizations are constantly facing targeted attacks by motivated attackers due to the data they've accumulated over time. Attackers can leverage this data, if stolen, for identity fraud or other nefarious purposes.

The white-hat industry needs to emulate today's threats to better prepare our customers for the actions of attackers. Egress-Assess allows users to exfiltrating sensitive faux (PII, credit cards, etc.), and real, data out of their network to an endpoint they control over a variety of protocols. This capability can be used by both blue and red teamers to really test if their organization can detect and remediate sensitive data leaving their network boundaries.

Additionally, while detecting data leaving the network is important, an ideal world would allow defenders to catch malware or malicious groups before data exfiltration can take place. Egress-Assess is gaining the ability to emulate known malware, and will use documented indicators to simulate malware. This new feature will allow defenders and pen testers to better emulate documented threats and test if network defenses can catch malware operating in their environment.

Steve Borosh, *Application Security Tester, Veris Group, @424f424f*

Chris Truncer, *FireEye, @chrstruncer*

2:45-3:30pm

Flying a Cylon Raider

In Season 1, Episode 5 of Battlestar Galactica, Captain Kara Thrace finds herself marooned on a moon with a crashed Cylon Raider. To get home, Captain Thrace has to apply her knowledge of flight fundamentals to control the enemy platform and pilot it back to safety.

Let's apply this to hacking. Your favorite toolset is taken away from you. You need to operate. What do you do? This talk will explore some fundamental offensive concepts that will help you succeed, regardless of your platform.

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

3:30-4:00pm

Networking Break and Vendor Expo (LOCATION: GRAND BALLROOM FOYER)

4:00-4:45pm	<p><i>Mobile Apps, IoT, and Terrifying Grown Adults</i></p> <p>Over the past few months, Tim purchased some IoT devices that are controlled by mobile apps. The goal was to make the devices do things that the app doesn't allow you to do, or change the way the device works. In this talk, Tim will demonstrate some mobile application analysis and hacking techniques that he employed to hack the devices – the same practical techniques used in many mobile application assessments. Caution: the results may terrify small children</p> <p>Tim Medin, Senior Technical Analyst, CounterHack, @timmedin</p>
4:45-5:30pm	<p><i>Building an Empire with PowerShell</i></p> <p>Offensive PowerShell had a watershed year in 2014. But despite the multitude of useful projects, many pentesters still struggle to integrate PowerShell into their engagements in a secure manner. The Empire Project aims to solve the weaponization problem by providing a robust PowerShell post-exploitation agent built on cryptologically-secure communications and a flexible architecture. Empire implements the ability to run PowerShell agents without needing powershell.exe, rapidly deployable post-exploitation modules ranging from key loggers to Mimikatz, and adaptable communications to evade network detection, all wrapped up in a usability-focused framework. This is the post-exploitation agent you've been waiting for.</p> <p>Will Schroeder, Security Researcher, Veris Group, @harmj0y Justin Warner, Red Team Capability Lead, Veris Group, @sixdub</p>

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 17

8:00-9:00am

Registration & Coffee (LOCATION: GRAND BALLROOM FOYER)

9:00-9:45am

Car Wars Episode I: Hacker Menace

It is a time of relative peace in the Republic. Auto manufacturers have provided reliable automobiles to a large portion of the population, governments, and militaries throughout the known world. Convenience and safety have become a common expectations in life.

Little does the Auto Alliance know that opportunistic evil awaits. While preparing for the ultimate auto-driving experience, dark plans have been laid to leverage this new power for death and destruction, and the changing of the universe forever...

Matt Carpenter, Principal Security Researcher, Grimm, @Ma77Carpenter

9:45-10:30am

Pen Trends Report

We all know and love the yearly reports from Verizon and Mandiant. They break down the various Incident Response gigs they worked on during the previous year. But what about the other side of the coin? What about penetration testing companies? What are they seeing?

In this presentation, John will share a breakdown of the penetration tests BHIS performed over the last year. He will discuss how most organizations are improving – and where they are still failing. More importantly, he will share a frightening trend – a trend that could have earth-shattering repercussions for the entire security industry. Dum, dum, DUMMMMMMMMM!!!!

John Strand, Black Hills Information Security, @strandjs

10:30-11:00am

Networking Break and Vendor Expo (LOCATION: GRAND BALLROOM FOYER)

11:00-11:45am

Evil DNS Tricks

DNS is a weird and fantastic protocol that lets any system on even the most secure networks talk to an evil system (aka me) without ever sending it a packet. Who wouldn't love that? Every pen tester needs to know how to leverage the DNS infrastructure to find vulnerabilities, exploit vulnerabilities, and even set up a discreet two-way channel. This talk will cover the latest weaponization of DNS – including the newly re-written dnscat – and a pile of other fun DNS tricks!

Ron Bowes, Security Engineer, Google, @iagox86

11:45am-12:15pm

My Password Cracking Brings All the Hashes to the Yard...

...and they're like, it's better than yours. Damn right it's better than yours, but I can teach you, free of charge. Password cracking is serious business, from dictionaries, to word munging, to Amazon EC2 and massive GPU rigs. Yeah, that's a lot of stuff! When I started cracking passwords, I knew there had to be a better way than just straight brute force; quite frankly, I never had a complex password crack over 8 characters finish even with some GPUs. I started asking friends, Googling and all I ever got was technical advice on how to run a tool, but *never a methodology*. It seemed the methodology was either a secret or they had about as much clue as I did; little. In this talk I'll discuss the outcomes of all of my research AND the methodology for really effective password cracking that even my CFO will approve. I may not have all of the answers, but what answers I do have, I'm willing to share.

Larry Pesce, Senior Security Analyst, InGuardians, @haxorthematrix

12:15-1:30pm	Lunch
1:30-2:15pm	<p><i>DIY Vulnerability Discovery with DLL Side Loading</i></p> <p>In this talk, Jake will teach you how to discover vulnerabilities like a rock star using DLL side loading. This technique (ab)uses the way Windows searches for DLLs to load into a program. The behavior is nearly laughable and introduces serious risks, especially when developers don't understand filesystem permissions. Attackers know this and use it for privilege escalation and stealthy persistence. It is being seen in a number of APT compromises and antivirus software has abysmal detection rates.</p> <p><i>Jake Williams, Rendition Infosec, @MalwareJake</i></p>
2:15-3:00pm	<p><i>DLP FAIL!!! Using Encoding, Steganography, and Covert Channels to Evade DLP and Other Critical Controls</i></p> <p>It's all about the information! Two decades after the movie Sneakers, the quote remains as relevant, if not more so. The fact that someone hacks into an environment is interesting but not that relevant. What is important is what happens after the compromise. If the data is destroyed or modified, organizations are negatively impacted but the benefits to an attacker for destruction or alteration are somewhat limited. Stealing information however, is highly profitable. Identity theft, espionage, and financial attacks involve the exfiltration of sensitive data. As a result, organizations deploy tools to detect and/or stop that data exfiltration. While these tools can be extremely valuable, many have serious weaknesses; attackers can encode, hide, or obfuscate the data, or can use secret communication channels. This session will talk about and demonstrate a range of these methods.</p> <p><i>Kevin Fiscus, Founder, Cyber Defense Advisors, @kevinbfiscus</i></p>
3:00-3:20pm	Networking Break and Vendor Expo (LOCATION: GRAND BALLROOM FOYER)
3:20-4:15pm	<p><i>Droning On and On</i></p> <p>Drones have the potential to be the sexiest new toy in the world of pen testing, but do they live up to their promise? You can do a lot of cool stuff with a drone, but with what benefit? At what cost? Are we legal? Is there profit? What does the future look like? Pen-testing with drones sounds like fun, but let's discuss what we can do and what may be ethical for the future.</p> <p><i>Larry Pesce, Senior Security Analyst, InGuardians, @haxorthematrix</i></p>
4:30-10:00pm	<p>Hackfest Hits the Road</p> <p>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.</p>

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.*