Pen Test Hackfest

SUMMIT

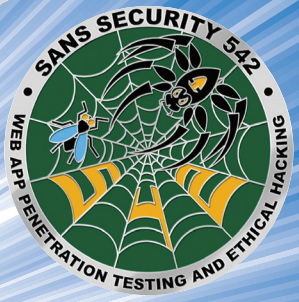
WASHINGTON, DC | NOV 13-14

Program Guide

Chairman: Ed Skoudis

#HackFestSummit

COIN-A-PALOOZA



Win Up To 4 Challenge Coins!

Each SANS pen test course offers a challenge coin for winners of the Day 6 Capture-the-Flag event, with 11 unique coins available, each with a special cipher on the coin itself. For those who have taken a given SANS course, but have not won the capture-the-flag challenge coin, Coin-a-palooza offers the ability to catch up by participating in the three nights of NetWars challenges. You'll have an opportunity to earn up to 4 challenge coins for your collection and extra bragging rights. Good luck!

Agenda

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

*All approved presentations will be available online following the Summit at **https://files.sans.org/summit/hackfest2014**.*
An e-mail will be sent out as soon as the presentations are posted, typically within 5 business days of the event.

Thursday, November 13

8:00-9:00 am

Registration & Coffee

9:00-10:00 am

How to Give the Best Pen Test of Your Life

Ed Skoudis, Fellow, SANS Institute

You know you have it in you – that drive to do the ULTIMATE penetration test: one that is technically deep, hyper current, super relevant, clever, and really helps the target organization understand their business risk and radically improve their security posture. In short, you want to perform the best penetration test of your life, your masterwork in the art of pen testing, something you can look back on with pride and say, "That. Was. The One." But, sadly, many penetration testers never realize this dream, due to lack of resources, time, capabilities, or even organization political backing.

But, as a thought experiment, what if you could, just once, conduct that dream penetration test? What would it look like? How would you approach it? How could you tell you had really given it your all? And, if such a test is impossible, why bother even thinking about it?

In this talk, Ed Skoudis explores these questions, focused on what we can learn from the hypothetical ultimate pen test that we can directly apply to our real-world pen tests today. Loaded with specific tips, tricks, and strategies, this talk strives to provide actionable advice for all security pros to up their game in providing great penetration tests.

10:00-10:20 am

Networking Break

10:20-11:10 am

iOS Game Hacking: How I Ruled the Worl^Hd and Built Skills For AWESOME Mobile App Pen Tests

Josh Wright, Senior Instructor, SANS Institute

I am a terrible video game player. I lack the skills to competitively arrange words with colleagues, crush jelly beans, or achieve a high score arranging numbers by threes. However, what I lack in video game competition, I make up for in iOS app hacking.

In this talk, we'll explore the profitable market of iOS games, looking at several techniques that are used to cheat, hack, or even steal from iOS game developers. You'll be able to apply these techniques to give yourself a leg up on your next gaming experience. Most importantly, each and every technique we'll discuss is also directly applicable to penetration testing and assessing the security of the iOS apps your organization uses each and every day. Learn to pwn games while becoming a better app pen tester! What's not to like?

11:10-11:55 am

Crazy Sexy Hacking

Mark Baggett, Technical Advisor to the DoD, SANS Institute

Paranoid? Concerned about space aliens reading your brain waves? Don't attend this talk. Mark Baggett will present a collection of research that borders the edge of insanity. These attacks are crazy sexy and didn't get the attention they deserve. Whitelist bypasses, Stealing Private Keys, backdoors in every phone and laptop, all these attacks lead to a very disturbing conclusion. Come learn what it is.

11:55am - 1:15 pm

Lunch

1:20-2:20 pm

Think Like a Champion: How to Dominate NetWars and Build Awesome Professional Skills Through Various Cyber Security Challenges

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

Panelists:

Matt Linton*, Digital Paramedic, Google*

Tim Medin*, Senior Technical Analyst, CounterHack and Certified Instructor, SANS Institute*

Josh Wright*, Senior Instructor, SANS Institute*

NetWars and CyberCity give pen testers a chance to push the envelope with real-world skills in a controlled environment. Additionally, there are countless other great challenges available on the Internet for people to develop their skills. The bragging rights alone are worth the long hours and late nights that competitors put in, but these challenges offer a unique and safe setting to try out new skills and take risks that would be unacceptable in any other environment. Hear from past NetWars champs how they clawed their way to the top.

2:20-3:15 pm

Pen Testing Web Frameworks Like a Boss

Justin Searle*, Managing Partner, UtiliSec*

As penetration testers, we are always pitting our skills against the latest and greatest (or not so late nor so great...) web application. While most of these custom applications require us to look for, identify, and exploit 0-day vulnerabilities in that specific app, one technique that can help improve our ability to do this is knowing your various web frameworks. Most web applications are not only built upon a programming language, but an entire framework of pre-written code that allows developers to quickly create multiple web applications that mechanically work the same under the hood while looking entirely unrelated to the user. By identifying the framework being used, be it Struts, GWT, .NET, Rails, Django, or one of countless other frameworks, we can start finding more known vulnerabilities from the frameworks and further optimize our 0-day testing by focusing most of our efforts on the custom written, non-framework components. This will be a preview peek into a new module being added to SEC642, SANS' advanced web pentest course.

3:15-3:30 pm

Networking Break

3:30-4:15 pm

Exploitation in Meatspace: The Basics of Physical Penetration Testing

Matt Linton*, Digital Paramedic, Google*

Although remote network attacks are a great way to get what you want during a pen test, some organizations may be particularly difficult to exploit. Don't panic! When cyberspace isn't working out for you, there's always physical penetration in meatspace. This talk will walk you through some of the particular techniques and requirements for safely performing a physical pen test (like permission – you have permission, right?) and explore inexpensive methods for learning the skills involved.

4:15-5:00 pm

Kicking the Guard Dog of Hades: Attacking Microsoft Kerberos

Tim Medin, Senior Technical Analyst, CounterHack and Certified Instructor, SANS Institute

Kerberos, besides having three heads and guarding the gates of hell, protects services on Microsoft Windows Domains. Its use is increasing due to the growing number of attacks targeting NTLM authentication. Attacking Kerberos to access Windows resources represents the next generation of attacks on Windows authentication.

In this talk, Tim will discuss his research on new attacks against Kerberos, including a way to attack the credentials of a remote service without sending traffic to the service as well as rewriting tickets to access systems. He will also examine potential countermeasures against Kerberos attacks, with suggestions for mitigating the most common weaknesses in Windows Kerberos deployments.

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.

6:00-9:00 pm

CORE NETWARS TOURNAMENT

Join fellow attendees for an evening of hands-on, interactive learning scenarios of computer attacks and analyzing defenses that enable information security professionals to develop and master the real-world, in-depth skills. This event is designed to be accessible to a broad level of participant skill ranges.

Agenda

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

*All approved presentations will be available online following the Summit at **https://files.sans.org/summit/hackfest2014**.*
An e-mail will be sent out as soon as the presentations are posted, typically within 5 business days of the event.

Friday, November 14

8:00-9:00 am

Registration & Coffee

9:00-9:55 am

Penetration Testing is Dead!

***Katie Moussouris**, Chief Policy Officer, HackerOne*

It is hard to remember a world that didn't hire smart people to break into computers and networks. Many who actively practice these dark arts - for money, fame, or simply the pursuit of intellectual happiness - are part of a generation that grew up online. But some of us remember when it was difficult to convince businesses, telecommunication providers, and governments that skilled hackers were not only necessary for defense, but also that a legitimate professional industry would rise up to meet the challenge. Training and certification also co-evolved alongside this penetration testing industry, pioneered in large part by institutions like SANS providing broad access to art forms in hacking. These skills used to only be possible to learn in the darker corners of bulletin board systems, 2600 meetings, and hacker spaces. But the evolution of the trade of hacking for money, either lawfully or not, is far from over, as new markets are emerging for those who have mastered the skills of finding security bugs, and especially for those who develop new ways to bypass defenses to exploit those bugs. The past, present, and future of penetration testing is in the hands of those who possess the skills to hack not just computers, but also to hack markets. We are in the midst of a market interregnum, and no champion has yet to be crowned. You will be witness to the coronation. Long live penetration testing!

9:55-10:15 am

Networking Break

10:15-11:00 am

Secret Pen Testing Techniques, Part Two

***David Kennedy**, Founder, TrustedSec, LLC; Co-Founder & CTO, Binary Defense Systems*

Every pen test is a challenge or puzzle, a way to reveal doors into an organization no one else has even noticed. This talk will walk through a number of techniques, new and old, that Dave uses on a regular basis in order to perform some of the best pen tests ever. He'll also be releasing some new code and some fun surprises. Being a penetration tester isn't about running some commands and hoping for an expectation; it's a way of thinking. This talk will cover where we are as an industry, and where we need to move to continue to get better.

11:00am - Noon

Threat Replication: An Assessment Concept

***Raphael Mudge**, Founder, Strategic Cyber LLC, Creator of Cobalt Strike and Author of Armitage*

As public evidence of advanced compromises mounts, most of us have come to realize the sophistication of some adversaries we're up against. But how do we understand our ability to defend a network against these well-resourced actors and use this as a starting point to get better?

This talk will present a concept for threat replication as a new type of penetration testing service. Where most assessments focus on vulnerabilities or security controls, we will look at threat replication as a tool to exercise our intelligence and its support to computer network defense. This talk will also present ideas to make this possible.

Noon-1:15 pm

Lunch

1:15-2:00 pm

The Veil-Framework

Will Schroeder and Chris Truncer, Pen Testers, Veris Group, LLC

The Veil-Framework is a project that aims to bridge the gap between pen testing and red team toolsets. It began with Veil-Evasion, a tool to generate AV-evading payload executables, expanded into payload delivery with the release of Veil-Catapult, and branched into Powershell functionality with the release of Veil-PowerView for network situational awareness. A post-exploitation framework, Veil-Pillage, will be released around the Defcon timeframe. This talk will cover the genesis of the framework and the development of its various components, and will touch on everything from disclosure ethics to module development along the way.

2:00-2:45 pm

Use of Malware by Penetration Testers

Wesley McGrew, Assistant Research Professor -
Department of Computer Science and Engineering, Mississippi State University

If we are to simulate real threats to our clients environments, then that threat must also include sophisticated malicious software. Compared to many penetration testers are "hands-on" with each system compromised, utilizing remote-shell payloads, true cyber threats have seen the value in automation and mass-control. As penetration testers, we can utilize the tactics of advanced threats through the use of our own malicious software. Such techniques can not only make our tests more efficient, but may also reveal weaknesses in anti-virus and other end-point solutions. In this session, we will discuss the use of malicious software designed for penetration tester use, custom malware, and the use of reverse engineering techniques to adapt captured malware samples for our own use.

2:45-3:05 pm

Networking Break

3:05-4:00 pm

Tricked-Out Pen Tests: The Coolest Tools and How They Rocked Your World

Moderator: Ed Skoudis, Fellow, SANS Institute

Panelists:
Mark Baggett, Technical Advisor to the DoD, SANS Institute
Wesley McGrew, Assistant Research Professor -
Department of Computer Science and Engineering, Mississippi State University
Raphael Mudge, Founder, Strategic Cyber LLC, Creator of Cobalt Strike and Author of Armitage

The right tool – or lack thereof – can make or break a pen test. Our panelist share the coolest tool, or feature of a tool, to rock their worlds in the last 12 months, and how they used it to great advantage in a pen test.

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.

4:30-10:00 pm

Hackfest Hits the Road: Hosted by Ed Skoudis and SANS

Join Ed Skoudis, Summit speakers and your fellow attendees for a very special off-site event. The details are SUPER SECRET, but it promises to be an unforgettable evening of education and networking.

A light dinner and refreshments will be provided. Registration required by 8pm on Thursday, November 13 online at **sans.org/event/sans-pen-test-hackfest-2014/bonus-sessions** or at registration desk.

SAVE THE DATE!

Pen Test Hackfest

SUMMIT & TRAINING

FALL OF 2015
WASHINGTON, DC

For more information on speaking at an upcoming summit or sponsorship opportunities, e-mail SANS at **summit@sans.org**.

Visit **sans.org/summit**
for detailed summit agendas as they become available.