SANS

2013 Pen Test Hackfest

SUMMIT & TRAINING EVENT

Program Guide

Ed Skoudis, Chairman

SANS SECURITY 504
504
HACKER TECHNIQUES, EXPLOITS, AND INCIDENT HANDLING
SANS SECURITY 542
WEB APP PENETRATION TESTING AND ETHICAL HACKING
SANS SECURITY 560
560
NETWORK PENETRATION TESTING AND ETHICAL HACKING
SANS SECURITY 575
MOBILE DEVICE SECURITY AND ETHICAL HACKING
SANS SECURITY 617
617
WIRELESS ETHICAL HACKING AND DEFENSES
SANS SECURITY 642
642
ADVANCED WEB APP PENETRATION TESTING AND ETHICAL HACKING
SANS SECURITY 660
660
ADVANCED PENETRATION TESTING, EXPLOITS, AND ETHICAL HACKING
SANS NetWars Competition
NETWARS
INTERACTIVE CYBER RANGE

Agenda

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

All approved presentations will be available online following the Summit at ***https://files.sans.org/summits/hackfest13****.*
An e-mail will be sent out within 5 business days once the presentations are posted.

Thursday, November 7

8:00-9:00 am

Registration

9:00-10:00 am

Opening Keynote:
How to Build a Completely Hackable City in Five Steps
(And Why You Should Build Your Own Skills in this Arena)

The NetWars CyberCity project involves an entire – and entirely functional - city, in miniature. There's a real power grid, real water systems, real traffic lights – and real systems to hack. Cyber warriors build skills and develop strategies and contingency plans by running missions in CyberCity. This talk will present an overview of the creation of CyberCity, step by step: concept, funding, architecture and design, implementation, testing, and finally, lessons learned.

But so what? You're not about to construct your own CyberCity – or are you? The border between the cyber and kinetic worlds is eroding, and some of the most interesting (and dangerous) hacks are in the interstitial space between software and hardware. The very cornerstones of society – the power grid, water treatment plants, medical devices, military equipment, and more – are at risk, and ideas such as air gaps and pressure valves are antiquated. The talk will also explore avenues for building your own skills in these various areas so you can help improve the security of our kinetic infrastructures. Find out what CyberCity teaches us about getting our act together in securing the cyber/kinetic space - and how you can build your own skills in this burgeoning arena.

Ed Skoudis*, Fellow, SANS Institute*

10:00-10:20 am

Networking Break

10:20-11:20 am

Pentesting with Metasploit 2013 Edition

Anyone who has used Metasploit for a security assessment knows that there are several ways to get the job done. During this presentation, we will take pen testing to the next level by demonstrating several techniques that need to be in your process. If you need to understand or demonstrate risk, you can't afford to miss this talk.

Josh Abraham*, Director of Services, Praetorian*

11:20 am-Noon

Hacking ASP.Net: Tips and Tricks

In this presentation, James Jardine will dive into some of the features that exist in the .Net framework and how they affect security testing. Learn how the features work, what to look for, and their weaknesses. Some of the features discussed will include Event Validation, ViewState and Request Validation.

James Jardine*, Principal Security Consultant, SecureIdeas LLC*

Noon-1:15 pm

Lunch

1:15-2:00 pm

Afternoon Keynote: Grok

Many critical aspects of our lives as hackers/pentesters are directly related to how well we understand and can identify a vast number of things. Sometimes success is determined by the simple recognition of a couple bytes of information. With cyberattacks having wide-ranging influence from banking to nuclear power, we have to be at the top of our game. Come reminisce about the past, ponder the present, and hear a bit of what's to come in cyber warfare.

@las of d00m

2:00-3:00 pm

Pen Testing Proprietary RF Communications

Exploring the connections between the cyber and kinetic worlds can lead to very many interesting, unexpected, and even frightening discoveries. But have you ever taken this exploration into your own enterprises? This talk will demonstrate practical techniques to identify, assess, and exploit a subclass of control systems found in your companies that use proprietary RF communications, such as fire alarms, proximity cards, automotive security gates, car alarms, conference rooms, and building automation systems.

Justin Searle*, Certified Instructor, SANS Institute & Managing Partner , UtiliSec*

3:00-3:30 pm

Networking Break

3:30-4:15 pm

Panel: Worst. Pen Test. Ever.: Avoiding Pen Test Disasters

Everyone's got "a friend" who's suffered nearly-unspeakable indignities and humiliations during a pen test gone horribly wrong. No matter how good you are, mistakes happen. Hear from our brutally honest panelists as they confess to their mistakes, and learn from them to save yourself.

Moderator: ***Ed Skoudis****, Fellow, SANS Institute*
Panelists: ***Josh Abraham****, Director of Services, Praetorian*
@las of d00m
Kevin Johnson*, CEO, Secure Ideas*
Justin Searle*, Certified Instructor, SANS Institute & Managing Partner , UtiliSec*

4:15-5:00 pm

Cloud File Services: Adding Value to Penetration Tests Since 2007

Do your clients use Enterprise File Sharing Services (EFSS, e.g. Dropbox, SkyDrive, etc.) in your network environment? Are you using this in your penetration tests (hint: you should be). In this session, you'll learn how penetration testers can use EFSS software installed on target machines to compromise the network, exfiltrate data, and establish a covert command and control channel. We'll also examine some ways that you can use some services to pivot directly to other network servers. By demonstrating the risks these services pose, you can provide value added to your penetration testing clients.

Jake Williams*, Chief Scientist, CSRgroup*

5:00-8:00 pm

NetWars Tournament – Evening 1

Refreshments Provided By

beyondtrust®
Beyond Traditional Security

NetWars is an action-packed challenge environment where people can build their skills while having fun.

This event will include FOUR full evenings of NetWars challenges, doubling the amount of NetWars time over a traditional SANS conference.These sessions will give you more time than ever with SANS' awesome NetWars challenge series to even further build your skills in a fun, interactive, hands-on fashion.

The Competition

- Consists of an interactive, Internet-based environment for computer attacks and analyzing defenses
- Is designed to be accessible to a broad level of participant skill ranges
- Is split into separate levels so participants may quickly advance through earlier levels to the level of their expertise.

The entire challenge involves five levels:

Level 1 - Played on local Linux image without root
Level 2 - Played on local Linux image with root
Level 3 - Attack a DMZ
Level 4 - Pivot to intranet
Level 5 - Master of your domain... castle versus castle

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

Friday, November 8

8:00-9:00 am

Registration

9:00-9:45 am

Keynote: Getting Creative: A Story in Thinking Outside of the Box

Ever run in to a crazy configuration and secure setup that you just couldn't break into? It's rare, but it happens. As penetration testers, we need to think outside of the box and get creative. We are hackers and we need to think like them. This presentation goes over some examples that I've run in to during penetration tests that made me get creative and think outside the box. Often times we get complacent when we can't find MS08-67, the latest and greatest exploit, or a default password. We chalk it up and walk away as if they're secure. Instead, let's fight, work for it, and most importantly, pop a box. This presentation will have lots of demos, tricks that I use during penetration tests, and more.

David Kennedy *(@dave_rel1k), Founder & Principal Security Consultant, TrustedSec*

9:45-10:15 am

Networking Break

10:15-11:00 am

Offense in Depth

What does it take for an adversary to attain freedom of movement in your information systems? This talk examines defense in depth from the perspective of the attacker. We will cover the process leading to a foothold, the defenses one must bypass, and how a savvy attacker may map these defenses.

Raphael Mudge*, Founder, Strategic Cyber LLC*

11:00am - Noon

Panel: Pen Test Zen: Spreading the Wisdom

In this session, the panelists share their coolest, smartest, trickiest and slickest hacks, and attendees have a chance to chime in with their own pearls of wisdom. This session promises to be so enlightening, you're likely to reach pen test nirvana.

Moderator: ***Ed Skoudis****, Fellow, SANS Institute*
Panelists: ***David Kennedy*** *(@dave_rel1k), Founder & Principal Security Consultant, TrustedSec*
James Lyne*, Certified Instructor, SANS Institute*
John Strand*, GCIH, GCFW, Senior Security Analyst/Principal, Black Hills Information Security*
Jake Williams*, Technical Analyst, Dept. of Defense*

Noon-1:15 pm

Lunch

1:15-2:00 pm

Automating Android App Assessment

Performing mobile device application assessments is a time-consuming and difficult task. This session will cover tools and techniques to perform assessments to identify malicious code in Android applications. It will help you to automate routine tasks so you have more time to look for interesting and novel items, then fold that information back into subsequent app assessments.

Chris Crowley, *Certified Instructor, SANS Institute*

2:00-3:00 pm

Pen Testing with a TARDIS

Technology is changing in amazing and very neat ways. Indeed, in many ways it is changing at a faster pace than ever before with some of the most fundamental changes to the computing model since we shifted from the mainframe. With these changes come new challenges for penetration testers and new opportunities. James Lyne, Certified instructor at SANS and Global Head of Security Research at Sophos will review these changes and how we all need to prepare.

James Lyne, *Certified Instructor, SANS Institute*

3:00-3:20 pm

Networking Break

3:20-4:15 pm

How to Fail at a Pen Test

In this presentation, John will cover some key components that many penetration tests lack, including why it is important to get caught, why it is important to learn from real attackers and how to gain access to organizations without sending a single exploit.

John Strand, *GCIH, GCFW, Senior Security Analyst/Principal, Black Hills Information Security*

4:15-5:00 pm

Anti-Virus No Thanks

Antivirus software can bring an otherwise successful penetration test to an abrupt and unsuccessful conclusion. Understanding the limitation of antivirus software can make the difference between a shell and "exploit completed, but no session created". Our customers already place unmerited faith in their antivirus software. A failed test as a result of antivirus software keeping the penetration tester out only reinforces their misconceptions and fails to illustrate the risk that the company would face from a skilled adversary. Join us for this session where Mark Baggett will discuss the latest tools and techniques available for evading antivirus software. We will review the latest publicly disclosed techniques, discuss which ones really work, and introduce a new technique or two that haven't been publicly discussed until this talk.

Mark Baggett , *Owner, Indepth Defense*

Thank you for attending the Pen Test Hackfest 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.

Exhibitor

beyondtrust®
Beyond Traditional Security

Beyond Trust
BeyondTrust is the only security solution vendor providing Context-Aware Security Intelligence, giving customers the visibility and controls necessary to reduce their IT security risks, while at the same time simplifying their compliance reporting. BeyondTrust offers consistent policy-driven vulnerability and privilege management, role-based access control, monitoring, logging, auditing and reporting to protect internal assets from the inside out. The company's products empower IT governance to strengthen security, improve productivity, drive compliance, and reduce expense across physical, virtual, mobile and cloud environments.

beyondtrust®

Beyond Traditional Security

Vulnerability Management

A Unified Solution for IT & IS Risk

Privilege Identity Management

RETINA

Most comprehensive & actionable risk reporting in the industry

Fully-integrated patching & configuration management with unmatched flexibility & scalability

POWERBROKER

Secure, manage & monitor privilege activities on UNIX, Linux, Mac & Windows

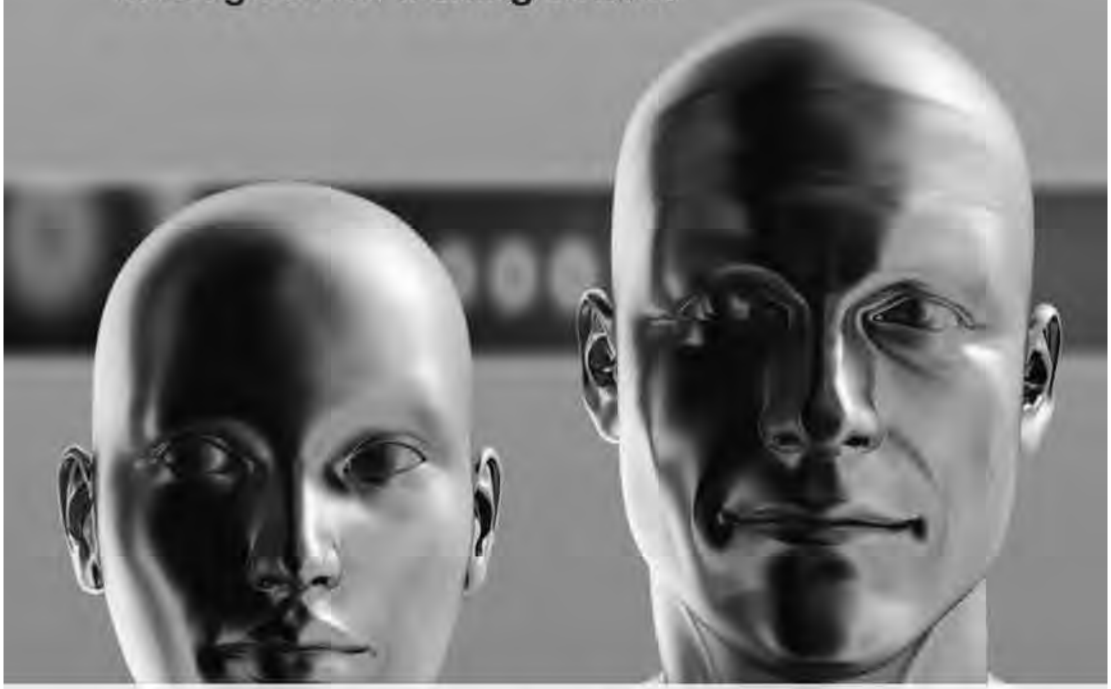
Real-time auditing, recovery & compliance reporting for critical servers

SECURITY AWARENESS

FOR THE 21ST CENTURY

End User - Utility - Developer - Phishing

- **Go beyond compliance and focus on changing behaviors.**
- **Create your own training program by choosing from a variety of modules:**
  - STH.End User is mapped against the Critical Security Controls.
  - STH.Developer uses the OWASP Top 10 web vulnerabilities as a framework.
  - STH.Utility fully addresses NERC-CIP compliance.
  - Compliance modules cover various topics including PCI DSS, Red Flags, FERPA, and HIPAA, to name a few.
- **Test your employees and identify vulnerabilities through STH.Phishing emails.**



SANS SECURING THE HUMAN

For a free trial visit us at:

www.securingthehuman.org

How Are You Protecting Your

- Data?
- Network?
- Systems?
- Critical Infrastructure?

Risk management is a top priority. The security of these assets depends on the skills and knowledge of your security team. Don't take chances with a one-size fits all security certification. **Get GIAC certified!**

GIAC offers over 20 specialized certifications in security, forensics, penetration testing, web application security, IT audit, management, and IT security law.

"GIAC is the only certification that proves you have hands-on technical skills."
-Christina Ford, Department of Commerce

"GIAC Certification demonstrates an applied knowledge versus studying a book."
-Alan C, USMC

Learn more about GIAC
and how to *Get Certified* at
www.giac.org

GLOBAL INFORMATION ASSURANCE CERTIFICATION
GIAC
www.giac.org

NEW!
GIAC CERTIFICATION

GIAC MOBILE DEVICE SECURITY ANALYST
GMOB

Coming Fall 2013!
GIAC Mobile Device Security Analyst

Registration now open at www.giac.org

UPCOMING SUMMITS & TRAINING COURSES

2013

Asia Pacific ICS Security Summit
Singapore | December 2-7

2014

AppSec Summit & Training
Austin, TX | February 3-8

Cyber Threat Intelligence Summit & Training
Washington, DC | February 2014

Industrial Control Systems Security Summit & Training
Orlando, FL | March 12-18

Digital Forensics & Incident Response Summit & Training
Austin, TX | June 3-10

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

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