SEC550

Active Defense, Offensive Countermeasures, and Cyber Deception

Five-Day Program
30 CPEs
Laptop Required

Who Should Attend

- General security practitioners
- Penetration testers
- Ethical hackers
- Web application developers
- Website designers and architects

You Will Be Able To

- Track bad guys with callback Word documents
- Use Honeybadger to track web attackers
- Block attackers from successfully attacking servers with honeyports
- Block web attackers from automatically discovering pages and input fields
- Understand the legal limits and restrictions of Active Defense
- Obfuscate DNS entries
- Create non-attributable Active Defense Servers
- Combine geolocation with existing Java applications
- Create online social media profiles for cyber deception
- Easily create and deploy honeypots

"SEC550 enumerates many useful tools for combating attackers, and the final, hands-on capture-the-flag exercise is a great culmination of all we learned."

-Jonathan Manafi, McLlhenny Company

SANS

SEC550 Training Formats
(subject to change)

Live Training
www.sans.org/security-training/by-location/all

Private Training
www.sans.org/onsite

The current threat landscape is shifting. Traditional defenses are failing us. We need to develop new strategies to defend ourselves. Even more importantly, we need to better understand who is attacking us and why. You may be able to immediately implement some of the measures we discuss in this course, while others may take a while. Either way, consider what we discuss as a collection of tools that will be at your disposal when you need them to annoy attackers, determine who is attacking you, and, finally, attack the attackers.

SEC550: Active Defense, Offensive Countermeasures, and Cyber Deception is based on the Active Defense Harbinger Distribution live Linux environment funded by the Defense Advanced Research Projects Agency (DARPA). This virtual machine is built from the ground up for defenders to quickly implement Active Defenses in their environments. The course is very heavy with hands-on activities – we won't just talk about Active Defenses, we will work through labs that will enable you to quickly and easily implement what you learn in your own working environment.

You Will Learn:

- **How to force an attacker to take more moves to attack your network – moves that in turn may increase your ability to detect that attacker**
- **How to gain better attribution as to who is attacking you and why**
- **How to gain access to a bad guy's system**
- **Most importantly, you will find out how to do the above legally**

What You Will Receive

- **A fully functioning Active Defense Harbinger Distribution ready to deploy**
- **Class books and a DVD with the necessary tools and the OCM virtual machine, which is a fully functional Linux system with the OCM tools installed and ready to go for the class and for the students' work environments**

Course Day Descriptions

550.1 HANDS ON: Setup and Baseline

Topics: Setup; Mourning Our Destiny, Leaving Youth and Childhood Behind; Bad Guy Defenses; Basics and Fundamentals (Or, Don't Get Owned Doing This); Playing With Advanced Backdoors; Software Restriction Policies; Legal Issues; Venom and Poison

550.2 HANDS ON: Annoyance

Topics: How to Connect to Evil Servers (Without Getting Shot); Remux.py; Recon on Bad Servers and Bad People; Honeypots; Honeyports; Kippo; Deny Hosts; Artillery; More Evil Web Servers; Cryptolocked

542.3 HANDS ON: Attribution

Topics: Dealing with TOR; Decloak; Word Web Bugs (Or Honeydocs); More Evil Web Servers; Cryptolocked

550.4 HANDS ON: More Attribution and Attack

Topics: Nova; Infinitely Recursive Windows Directories; Web Application Street Fighting with BeEF!; Wireless and Brotherly Love; Evil Java Applications with SET; AV Bypass (for the Good Guys!); Arming Word Documents; Python Injection; Ghostwriting; HoneyBadger; Let's Try to Trojan Some Java Applications

550.5 HANDS ON: Capture the Flag

The Capture-the-Flag challenge draws on what you have learned over the previous four days of the course.

SANS