SECURITY TRAINING IN A (VIRTUAL) BOX

Marcelle Lee
and
Joe Gray

November 14, 2017
About Marcelle

- Threat Researcher, LookingGlass Cyber Solutions, Inc.
- Co-founder and CEO, Fractal Security Group, LLC
- Adjunct faculty
- Compulsive volunteer - WSC, ISACA, ISSA, NIST
- Certifications - CSX-P, GCIA, GPEN, CISSP, to name a few
- Cyber competition enthusiast
About Joe

- Enterprise Security Consultant at Sword & Shield Enterprise Security
- 2017 DerbyCon Social Engineering Capture the Flag (SECTF) winner
- Served in the US Navy, Navigating Submarines
- Holds the CISSP-ISSMP, GSNA, and GCIH certifications
- Frequent Guest Blogger
- Maintains blog and podcast at https://advancedpersistentsecurity.net
- Trains (spoken taps out a lot) in Brazilian Jiu Jitsu
“There are only two types of companies: those that have been hacked, and those that will be.”

~ Robert Mueller, FBI Director, 2012
About Our Training

• In a “box”
• Demonstrates phases of an attack
• Features “capture the flag” elements
• Explores “red team” vs “blue team”
• Can be used as demo or for hands-on instruction
THE LEARNING CONE (EDGAR DALE 1969)

AFTER TWO WEEKS WE REMEMBER...

READING 10% OF WHAT WE READ

HEARING 20% OF WHAT WE HEAR

WATCHING 30% OF WHAT WE SEE

WATCHING A VIDEO 50% OF WHAT WE SEE & HEAR

PARTICIPATING 70% OF WHAT WE SAY

GETTING INVOLVED IN DISCUSSION 90% OF WHAT WE SAY & DO

PRESENTING / SIMULATING REAL EXPERIENCES
Intended Audience

- SOC analysts and other frontline staff
- C-level executives
- Users at all levels
- Students
The Set-Up

Ubuntu LAMP web server - victim box

Kali Linux - attacker box

Hypervisor of your choice (we like VirtualBox)

• Set-up is easily expandable
The Scenario

Small company called Initech. There are three legitimate corporate users.

Tip 1: The company website has clues about possible employee credentials.

Tip 2: There is also an important file the attacker will want to steal.

• Scenarios are customizable
The Goals

• Gain access to the Ubuntu box.
• Find the flags.
• Establish persistence.
• Exfiltrate the important file.
• Cover evidence of activities.
Phases of an Attack

- Reconnaissance
- Scanning
- Maintaining Access
- Clearing Tracks

Diagram showing the cycle of attack phases.
Reconnaissance

Recon consists of passive and often creative research and typically takes a significant amount of time and effort.
Recon Demo
Scanning is the process of using tools to identify weak points in an organization that allow attackers to gain access.
Scanning Demo
Gaining Access a.k.a. Exploitation

Exploit systems using discovered vulnerabilities to compromise and gain control.
Exploitation Demo
Maintaining Access

Keep a persistent connection to the target, often done via installation of backdoors.
Backdoor Demo
Covering Tracks

Variety of techniques and tools including log editing/cleaners, file hiding/deleting, spoofing, planting fake files/info, fake accounts, etc.
Associated “evidence” can also be created:
• Packet captures
• Memory captures
• Hard drive images
• External media images
• “Company” and “personnel” data
Marcelle
@marcelle_fsg

Joe
@C_3PJoe

Resources:  http://ow.ly/rtrN30gn3y2