PEN450 Hacking and Web Exploitation Bootcamp

Course Overview

Offensive Cyber Security tools and techniques are necessary to understand if you are either engaging in offensive activities or defending against them. It is also important to understand the basics of defense as well, either to employ them or to know their limitations and shortcomings.

This course will introduce the student to these tools and techniques, with 2 days spent on basic penetration testing techniques, 1 day on basic web application attacks, 1 day on defensive measures and cryptographic techniques, and the last day spent on a live Attack and Defend exercise, in which the students will team up in a shared environment and go head to head with the other students, attacking the shared machines, and when successful, defending them from the other students.

At the conclusion of this course, students will understand the basic tools of offensive Cyber Security and which situations each tool is appropriate for. They will also understand basic defense measures and will obtain some practice in counteracting them.

Objectives

- Learn how to use the basic tools of pentesting and web application security testing
- Learn how to find vulnerabilities in applications and exploit them
- Learn how to deploy basic defenses and what defenders may do to track down an attacker

Prerequisite Knowledge

Before taking this course, students should be familiar with:

- Basics of Cyber Security
- Be comfortable using Windows and Linux

Estimated Course Length: 5 Days

Day	Lab Activity
1	Scanning with Nmap
1	Hping3
1	Vulnerability Scanning with OpenVAS
1	Core Impact Vulnerability Scan
1	Metasploit
1	Post Exploitation and Pivoting
1	Snapd Privilege Escalation Exploit
2	Evasive Maneuvers and Post Exploitation
2	Linux Routing and SSH Tunnels
2	Client-Side Exploitation with Social Engineering
2	Windows Exploitation
2	Linux Exploitation
2	Password Cracking
2	Web Recon Tools
3	Injection
3	Broken Authentication
3	Sensitive Data Exposure
3	Local File Inclusion and Client-side Access Control
3	Security Misconfiguration
3	Cross Site Scripting
3	Insecure Deserialization
3	XML External Entities
3	Using Components with Known Vulnerabilities
3	Insufficient Logging and Monitoring
3	Web Challenge

Day	Lab Activity
4	Linux Firewalls
4	Advanced IP Tables
4	Linux Logs
4	Intrusion Detection Systems
4	Basic Network Forensics
4	Attacking Classic Ciphers
4	Breaking Repeated Key XOR Cipher
4	Breaking Weak RSA Keys
4	Steganography
4	Using the OpenSSL CLI Tool
4	Using GPG for Encryption and Key Management
5	Attack and Defend

About CyberStronger

Comtech provides cybersecurity solutions and services tailored to training and workforce development. The CyberStronger product portfolio was created by a team of former National Intelligence Community members who all possess the necessary hands-on, practical cybersecurity experience and abilities required to meet the needs of our demanding customer base. Our experts share the intellectual curiosity to constantly ask the 'why' and 'how' as they develop and deliver truly unique products and services to help close the growing cybersecurity skills gap. The Comtech CyberStronger offerings include off-the-shelf and custom training, hands-on skills labs, and competency-based assessments mapped to cybersecurity job roles.

Comtech
cyberstronger.com | comtechtel.com
275 West Street, Annapolis, MD 21401