PEN 500 Pentesting & Network Exploitation

Course Overview

Pentesting & Network Exploitation exposes students to all manner of reconnaissance, scanning, enumeration, exploitation and pillaging for 802.3 networks.

Topics expose students to a variety of recon, discovery, scanning, enumeration, exploitation, post-exploitation, pillaging, covering one's tracks and persistence.

Objectives

- Provide in-depth exposure and hands-on practice with all facets of 802.3 hacking, vulnerability research, pivoting, exploitation, password/hash cracking, post-exploitation pillaging and methods of setting up persistence on a victim's network

Target Audience

- Penetration testers looking to broaden their overall penetration testing skill set, network engineers, system administrators, developers

Estimated Course Length: 24 hours

Day 1

Day 1 introduces students to host target analysis. Topics include Linux command line, bash scripting and simple programming to enumerate, attack and exploit Linux hosts later in the course. Once Linux is complete, students begin learning basic through intermediate Windows Command Line skills, PowerShell cmdlets and the PowerShell attack framework called PowerPreter.

Topics List

- Linux administration tools
- Navigation of *nix file systems
- Bash scripts writing for pentesting engagements
- Python socket program writing to connect to remote server
- Basic C programs in *nix environment compilation and modification
- Windows command line administration tools
- Windows file systems navigation
- PowerShell use for conducting enumeration and analysis of targets
- Nishang and PowerPreter for enumerating, attacking and deploying persistence on targets boxes

Day 2

Students learn how to conduct basic service scans and exploit vulnerable hosts on internal networks through hands-on challenges that force them to replicate a real-world penetration test. They learn how to map, discover and exploit web applications, which requires the tester to understand how they communicate and the role the server plays in the relationship. Students learn how to conduct reconnaissance against a web server, followed by mapping its architecture. They're also challenged with discovering vulnerabilities and misconfigurations for follow-on exploitation.

Topics List

- Discovering live hosts
- Scaning hosts to find vulnerabilities and misconfigurations with Nmap and manual techniques
- Determination of which ports are open and what services are running
- Use of Metasploit to scan and database target information
- Choosing exploit and payload for target host
- Use of various post-exploitation Meterpreter scripts to steal information from victim
- How web applications operate
- How HTTP operates
- Headers and session management techniques
- Authentication and post-authentication role assignment
- OWASP Top 10
- Web app recon, mapping, discovery and exploitation process
- Differentiation of URI, URL and URN
- Differences between server-side and client-side code
- Nikto for discovery of web app vulnerabilities and misconfigurations
- Code snippet analysis (HTML, PHP, JavaScript, JSON Arrays, AJAX, etc.)
- Manual SQL injection and XSS scripting attack techniques

Day 3

Students learn how to simulate an insider threat and escape restricted environments by abusing native services and functionality. Students then move to routed attacks against clients that have NAT devices, firewalls and DMZs deployed. They learn how to exploit a variety of web-facing services and gain access to the DMZ. Once in the DMZ they are asked to pillage the hosts and find additional information to assist in pivoting deeper into the network and into network segments that don't touch the web directly.

Topics List

- Escaping restricted Windows desktop environments
- Spawning unauthorized browsers for Internet access
- Enumerating firewalls and web-facing services with Nmap, Nikto and Dirbuster
- Burp Suite to proxy web application traffic to and from victim web server
- Accessing demilitarized zone
- Pillaging hosts to find additional information
- Moving files onto victim boxes using Netcat and Meterpreter
- Stealing files from victim boxes using Netcat and Meterpreter

Day 4

On Day 4 students learn how to create and host malicious binaries on their own webserver to facilitate network penetration with purpose-built shellcode. Building on techniques and access gained into the DMZ, students are challenged to burrow further into the victims network by adding routes and pivoting into internal network segments by exploiting additional victims. Having exploited a variety of hosts throughout the network deploying persistence is then taught to maintain hard earned access.

Topics List

- Using MSFvenom to create purpose-built binaries with a variety of payloads
- Hosting malware on web server for easy delivery to victims
- Adding routes to additional network segments to facilitate pivoting
- Using post-exploitation Meterpreter tools to pillage various hosts
- Deploying Visual Basic Script for persistence on various victims
- Modifying persistence mechanism to survive reboot

Day 5

Day 5 deals exclusively with hands-on challenges. Using all the skills, techniques and tools learned during the previous four days to lay waste to the company's network and computers, students will be tasked with owning "the CEO's" computer, and stealing as much sensitive information from the notional corporation as possible. The company's computers contain a wide variety of PII, corporate information and intellectual property for the taking. Can they own the CEO's box? Can they gain access to and modify the company's firewall settings?

Topics List

- Obtaining sensitive, non-public information from the company's computer
- Modifying the company's firewall settings
- Pwning the CEO's computer

CYBRScore®
Comtech Mission-Critical Technologies
275 West Street, Annapolis, MD 21401

www.cybrscore.io
ComtechMCT-CYBRScore@comtechtel.com