PEN 111:
Network Ethical Hacking and Penetration Testing

A 30-Hour Training Course

Course Description

This course prepares you to be a professional ethical hacker and penetration tester who is able to conduct comprehensive and complete penetration testing either for your organizations or for your customers. The course covers in-depth techniques and methodologies, along with state-of-the-art tools, for a high-quality ethical hacking engagement. The course starts with pre-engagement preparatory works, then, it dives into reconnaissance, where you will learn how to build an information profile of your target. After that, you will learn advanced network scanning and vulnerability assessment methods. Then, you will be taught how you can effectively exploit vulnerable systems and maintain access. Furthermore, you will learn all the technical details of password cracking. Finally, and in addition to all the previous skills, you will learn how to break wireless networks.

The uniqueness of this course is that it combines theoretical knowledge with practical hands-on labs. Students will learn about the theories of vulnerabilities and exploitations, in addition, they will practice all the techniques of standard penetration testing in labs simulating real-world scenarios. In addition, each student will get an eBook as a course material covering all topics. At the end of the course, the students become confident at utilizing the best cybersecurity and hacking tools in the industry.

Who Should Attend?

This course is suitable for network security engineers, information security officers, network administrators, system analysts, IT specialists, and all those who are interested in technically advancing their network security skills.

Duration

- Total Hours: 30 hours
- Total Days: 5 days or 10 days

Prerequisites

- Laptop: students must bring their laptops with the following specifications:
  - 8GB or more of RAM
  - USB
  - Wi-Fi (built-in or card)
- Kali Linux Live CD/DVD.
- Technical Knowledge: it is highly recommended that attendees have a background in the following concepts:
  - TCP/IP protocols
  - Linux operating system
  - Programming

Outline

MODULE 01: INTRODUCTION TO PENETRATION TESTING

- Definitions
- Purpose and Value
- Information Security
- Paradigm of IT Security
- Types of Penetration Testing:
  - Black-Box, White-Box, and Grey-Box
  - External Testing vs. Internal Testing
- Penetration Testing Methodologies & Standards:
  - Open-Source Security Testing Methodology Manual (OSSTMM)
  - Penetration Testing Execution Standard (PTES)
  - Technical Guide to Information Security Testing and Assessment by NIST
  - Penetration Testing Framework

MODULE 02: PRE-ENGAGEMENT PREPARATION

- Importance of the preparation
- Scoping and questionnaire
- Success Criteria
- Rules of Engagement

MODULE 03: INTELLIGENCE GATHERING

- Definitions and Concepts
- Google Hacking
- WHOIS Information
- Web Site Reports and Searches
- Document Metadata Analysis
- DNS Records & Zone Transfer
- Tools: Maltego, and Recon-ng

MODULE 04: NETWORK TRAFFIC SNIFFING & INTERCEPTION

- Network Traffic Sniffing
- Tool: Wireshark and Tcpdump
- Network Traffic Interception
- ARP Poisoning Technique
- SSL Hijacking & SSL Stripping
- Tools: Arpspoof, Ettercap, and Sslstrip

MODULE 05: SCANNING & ENUMERATION

- Host Discovery
    - ICMP-Based Techniques
    - TCP-Based Techniques
    - UDP-Based Techniques
- Port Scanning
    - TCP vs. UDP Scanning
    - Windows vs. Unix/Linux Scanning
    - Full/Connect Scan
    - Half/SYN Scan
    - FIN, NULL, and XMAS Scans
    - ACK Scan
    - Idle Scan
    - Port Range Optimization
    - IPv6 Considerations
- Service Identification
- OS Fingerprinting
- Tracing Targets
- Tools: nmap, tcpdump, amap, scapy, netcat, and hping.
- Email Harvesting

MODULE 06: VULNERABILITY ANALYSIS

- What Vulnerabilities are and How they are Discovered
- Categories of Vulnerabilities
    - Input Validation Vulnerabilities
    - Cryptographic Vulnerabilities
    - Configuration Vulnerabilities
    - Session Management Vulnerabilities
    - Authentication Vulnerabilities
    - Authorization Vulnerabilities
    - Availability Vulnerabilities
    - Protocol Errors
- Vulnerability Databases and Scoring
    - Common Vulnerabilities and Exposure (CVE)
    - Common Vulnerability Scoring System (CVSS)
- Finding Vulnerabilities
    - Manual Process
    - Automated Process
- Tools: Nessus, and OpenVAS

MODULE 07: EXPLOITATION

- The Purpose of Exploitation
- Exploits and their Categories
    - Remote Exploits: client-side vs. server-side.
    - Local Exploits
- Privilege Escalation
- Overview of Shellcode/Payload
- Types of Shell:
    - Direct Shell
    - Bind Shell
    - Reverse Shell
- The Metasploit Tool:
    - Metasploit’s Exploits
    - Metasploit’s Payloads
    - Metasploit’s Encoders
    - Metasploit Auxiliar Modules
- Understanding Metasploit's Sessions
- Metasploit Database Integration

MODULE 08: POST-EXPLOITATION

- Overview of Meterpreter
- Meterpreter Libraries & Commands
- Enumerating the Victim
- Dumping Password Hashes
- System Control
- Downloading and Uploading Files
- Maintaining Access through RDP, SSH & VNC
- Creating Persistent Backdoors
- Deleting Event Logs and Covering Tracks
- Pivoting and Relays

MODULE 09: PASSWORD CRACKING

- Local Authentication vs. Remote Authentication
- Local Authentication Attack Vectors
- Remote Authentication Attack Vectors
- Offline Password Cracking
    - Capturing & Cracking Windows Hashes
    - Capturing & Cracking Linux Hashes
- Online Password Cracking
    - Cracking RDP Authentication
    - Cracking SMB Authentication
    - Cracking PostgreSQL Authentication
    - Cracking HTTP Authentication
    - Cracking SSH Authentication
- Tools: Cain, John, and Hydra

MODULE 10: HACKING WIRELESS NETWORK

- Overview of Wireless Technologies
- Wireless Security Concepts
- Wireless DoS Attacks
- Wired Equivalent Privacy (WEP) Protocol.
- Breaking WEP.
- Wi-Fi Protected Access (WPA) Protocol.
- WPA Pre-Shared Key (PSK) Cracking
- Tools: aircrack-ng, netSumbler, and InSSIDer