PEN-200 Penetration Testing with Kali Linux

Course Overview

Penetration Testing with Kali Linux (PWK) is an online pentesting course designed for security professionals and network administrators who want to take a serious and meaningful step into the world of professional penetration testing. This best-in-class training course introduces students to the latest ethical hacking tools and techniques, including remote, virtual penetration testing labs for practicing the course materials. PWK simulates a full penetration test from start to finish by immersing the student into a target-rich and vulnerable network environment. Students who pass the exam earn the industry-leading OSCP certification.

Exam Reference: OffSec Certified Professional (OSCP)

Delivery Format: 5:1:6

- 5 weeks guided self-study pre-work
- 1 week Online Live immersive boot camp
- 6 bi-weekly Online Live post-immersive mentoring 3.5 hour sessions

Target Audience

- Infosec professionals transitioning into penetration testing
- Pentesters seeking one of the best pentesting certifications
- Those interested in pursuing a penetration tester career path
- Security professionals
- Network administrators
- Other technology professionals

Course Objectives

- Using information gathering techniques to identify and enumerate targets running various operating systems
- Writing basic scripts and tools to aid in the penetration testing process
- Analyzing, correcting, modifying, cross-compiling, and porting public exploit code
- Conducting remote, local privilege escalation, and client-side attacks
- Identifying and exploiting XSS, SQL injection, and file inclusion vulnerabilities in web applications
- Leveraging tunneling techniques to pivot between networks
- Creative problem solving and lateral thinking skills

Duration

5 Weeks

Certifications

PEN-200

Contact Us

(800) 674-3550

2151 W. Hillsboro Blvd.,
Suite 210
Deerfield Beach, FL 33442

Connect with us

APPLIED TECHNOLOGY ACADEMY

Sign Up Today!

AppliedTechnologyAcademy.com

PEN-200 Penetration Testing with Kali Linux

APPLIED TECHNOLOGY ACADEMY

Course Outline

Penetration Testing: What You Should Know

- This module introduces you to the course and sets expectations.
- About The PWK Course
- Overall Strategies for Approaching the Course
- Obtaining Support
- About Penetration Testing
- Legal
- The MegaCorpone.com and Sandbox. local Domains
- About the PWK VPN Labs
- Reporting
- About the OSCP Exam

Getting Comfortable with Kali Linux

- Kali Linux is the penetration testing platform used throughout PWK. In this module, we cover how to use Kali and understand the OS.
- Booting Up Kali Linux
- The Kali Menu
- Kali Documentation
- Finding Your Way Around Kali
- Managing Kali Linux Services
- Searching, Installing, and Removing Tools

Command Line Fun

- Learning how to interact with the
- terminal.
- The Bash Environment
- Piping and Redirection
- Text Searching and Manipulation
- Editing Files from the Command Line
- Comparing Files
- Managing Processes
- File and Command Monitoring
- Downloading Files
- Customizing the Bash Environment

Practical Tools

- Netcat
- Socat
- PowerShell and Powercat
- Wireshark
- Tcpdump

Bash Scripting – NEW in 2020

- Intro to Bash Scripting
- Variables
- If, Else, Elif Statements
- Boolean Logical Operations
- Loops
- Functions
- Practical Examples

Passive Information Gathering

- Using OSINT to gather information,
- including the use of shodan and pastebin.
- Taking Notes
- Website Recon
- Whois Enumeration
- Google Hacking
- Netcraft
- Recon-ng
- Open-Source Code
- Shodan
- Security Headers Scanner
- SSL Server Test
- Pastebin
- User Information Gathering
- Social Media Tools
- Stack Overflow
- Information Gathering Frameworks

Active Information Gathering

- DNS Enumeration
- Port Scanning
- SMB Enumeration
- NFS Enumeration
- SMTP Enumeration
- SNMP Enumeration

Vulnerability Scanning

- Vulnerability Scanning Overview and Considerations
- Vulnerability Scanning with Nessus
- Vulnerability Scanning with Nmap

Web Application Attacks

- Burp Suite, PHP Wrappers
- Web Application Assessment Methodology
- Web Application Enumeration
- Web Application Assessment Tools
- Exploiting Admin Consoles
- Cross-Site Scripting (XSS)
- Directory Traversal Vulnerabilities
- File Inclusion Vulnerabilities
- SQL Injection

Buffer Overflow Intro

- Introduction to the x86 Architecture
- Buffer Overflow Walkthrough

Windows Buffer Overflows

- Discovering the Vulnerability
- Win32 Buffer Overflow Exploitation

Linux Buffer Overflow

- About DEP, ASLR, and Canaries
- Replicating the Crash
- Controlling EIP
- Locating Space for Your Shellcode
- Checking for Bad Characters
- Finding a Return Address
- Getting a Shell

PEN-200 Penetration Testing with Kali Linux

APPLIED TECHNOLOGY ACADEMY

Course Outline

Client Side Attacks
- HTA Attacks, Microsoft Word Macros, Object Linking and Embedding (DDE)
- Know Your Target
- Leveraging HTML Applications
- Exploiting Microsoft Office

Using Public Exploits
- A Word of Caution
- Searching for Exploits
- Putting It All Together

Fixing Exploits
- Fixing Memory Corruption Exploits
- Fixing Web Exploits

File Transfers
- Considerations and Preparations
- Transferring Files with Windows Hosts

Bypassing Antivirus Software
- What is Antivirus Software
- Methods of Detecting Malicious Code
- Bypassing Antivirus Detection
- Wrapping Up

Privilege Escalation
- Information Gathering
- Windows Privilege Escalation Examples
- Linux Privilege Escalation Examples
- Enumerating Firewall and Status Rules, Bypassing UAC
- Wrapping Up

Password Attacks
- Mimikatz
- Wordlists
- Brute Force Wordlists
- Common Network Service Attack Methods
- Leveraging Password Hashes
- Wrapping Up

Port Redirection and Tunneling
- HTTP tunneling
- Port Forwarding
- SSH Tunneling
- PLINK.exe
- NETSH
- HTTPTunnel-ing Through Deep Packet Inspection
- Wrapping Up

Metasploit
- Advanced options with multi/handler, transport modules, Meterpreter
- Section: Metasploit User Interfaces and Setup
- Exploit Modules
- Metasploit Payloads
- Building Our Own MSF Module
- Post-Exploitation with Metasploit
- Metasploit Automation
- Wrapping Up

Active Directory attacks (Domains)
- Active Directory Theory
- Active Directory Enumeration
- Active Directory Authentication
- Active Directory Lateral Movement
- Active Directory Persistence
- Includes Kerberos attacks, password spraying AD
- Wrapping Up

PowerShell Empire
- Introduction to Powershell Empire and the use of Power-Up
- Installation, Setup, and Usage
- PowerShell Modules
- Switching Between Empire and Metasploit
- Wrapping Up

Assembling the Pieces: Penetration Test Breakdown
- Sandbox.local hands-on walkthrough
- Public Network Enumeration
- Targeting the Web Application
- Targeting the Database
- Deeper Enumeration of the Web Application Server
- Targeting the Database Again
- Targeting Poultry
- Internal Network Enumeration
- Targeting the Jenkins Server
- Targeting the Domain Controller

Prerequisites

All students are required to have:
- Solid understanding of TCP/IP networking
- Reasonable Windows and Linux administration experience
- Familiarity with basic Bash and/or Python scripting