Penetration Testing with Kali Linux (PWK)

Course Code	QAOFFSECPWK
Duration	5 Day Course
Price	from £5,300

Course Description

Penetration Testing with Kali (PWK) is a pen testing course, updated in Feb 2020, designed for network administrators and security professionals who want to take a serious and meaningful step into the world of professional penetration testing. This unique penetration testing training course introduces students to the latest ethical hacking tools and techniques, including remote, virtual penetration testing labs for practicing the course materials. Penetration Testing with Kali Linux simulates a full penetration test from start to finish, by injecting the student into a target-rich, diverse, and vulnerable network environment.

Please note, there is an optional 24 hour lab based certification exam available to delegates who have sat this course. This exam leads to the Offensive Security Certified Professional (OSCP) certification and must be booked directly with Offensive Security.

Objectives

- Penetration Testing with Kali Linux: General Course Information
- Getting Comfortable with Kali Linux
- Command Line Fun
- Practical Tools
- Bash Scripting
- Passive Information Gathering
- Active Information Gathering
- Vulnerability Scanning
- Web Application Attacks
- Introduction to Buffer Overflows
- Windows Buffer Overflows
- Linux Buffer Overflows
- Client-Side Attacks
- Locating Public Exploits
- Fixing Exploits
- File Transfers
- Antivirus Evasion
- Privilege Escalation
- Password Attacks

- Port Redirection and Tunnelling
- Active Directory Attacks
- The Metasploit Framework
- PowerShell Empire
- Assembling the Pieces: Penetration Test Breakdown
- Trying Harder: The Labs

Course Modules

Penetration Testing with Kali Linux: General Course Information (10 topics)

- 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
- Wrapping Up

Getting Comfortable with Kali Linux (7 topics)

- Booting Up Kali Linux
- The Kali Menu
- Kali Documentation
- Finding Your Way Around Kali
- Managing Kali Linux Services
- Searching, Installing, and Removing Tools
- Wrapping Up

Command Line Fun (10 topics)

- 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
- Wrapping Up

Practical Tools (6 topics)

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

Bash Scripting (7 topics)

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

Passive Information Gathering (16 topics)

- 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
- Wrapping Up

Active Information Gathering (7 topics)

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

- SNMP Enumeration
- Wrapping Up

Vulnerability Scanning (4 topics)

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

Web Application Attacks (6 topics)

- Web Application Assessment Methodology
- Web Application Enumeration
- Web Application Assessment Tools
- Exploiting Web-based Vulnerabilities
- Extra Miles
- Wrapping Up

Introduction to Buffer Overflows (3 topics)

- Introduction to the x Architecture
- Buffer Overflow Walkthrough
- Wrapping Up

Windows Buffer Overflows (3 topics)

- Discovering the Vulnerability
- Win Buffer Overflow Exploitation
- Wrapping Up

Linux Buffer Overflows (8 topics)

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

Client-Side Attacks (4 topics)

- Know Your Target

- Leveraging HTML Applications
- Exploiting Microsoft Office
- Wrapping Up

Locating Public Exploits (4 topics)

- A Word of Caution
- Searching for Exploits
- Putting It All Together
- Wrapping Up

Fixing Exploits (3 topics)

- Fixing Memory Corruption Exploits
- Fixing Web Exploits
- Wrapping Up

File Transfers (3 topics)

- Considerations and Preparations
- Transferring Files with Windows Hosts
- Wrapping Up

Antivirus Evasion (4 topics)

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

Privilege Escalation (4 topics)

- Information Gathering
- Windows Privilege Escalation Examples
- Linux Privilege Escalation Examples
- Wrapping Up

Password Attacks (5 topics)

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

Port Redirection and tunnelling (6 topics)

- Port Forwarding
- SSH tunnelling
- PLINK.exe
- NETSH
- HTTP Tunnelling Through Deep Packet Inspection
- Wrapping Up

Active Directory Attacks (7 topics)

- Active Directory Theory
- Active Directory Enumeration
- Active Directory Authentication
- Low and Slow Password Guessing
- Active Directory Lateral Movement
- Active Directory Persistence
- Wrapping Up

The Metasploit Framework (7 topics)

- Metasploit User Interfaces and Setup
- Exploit Modules
- Metasploit Payloads
- Building Our Own MSF Module
- Post-Exploitation with Metasploit
- Metasploit Automation
- Wrapping Up

PowerShell Empire (4 topics)

- Installation, Setup, and Usage
- PowerShell Modules
- Switching Between Empire and Metasploit
- Wrapping Up

Assembling the Pieces: Penetration Test Breakdown (10 topics)

- 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
- Wrapping Up

Trying Harder: The Labs (8 topics)

- Real Life Simulations
- Machine Dependencies
- Cloned Lab Machines
- Unlocking Networks
- Routing
- Machine Ordering & Attack Vectors
- Firewall / Routers / NAT
- Passwords

Prerequisites

Penetration Testing with Kali Linux is a foundational course, but still requires students to have certain knowledge prior to attending the online class. A solid understanding of TCP/IP, networking, and reasonable Linux skills are required. Familiarity with Bash scripting along with basic Perl or Python is considered a plus.

Course Dates

Code	Location	Duration	Price	Feb	Mar	Apr	May	Jun	Jul
Later scheduled dates may be available for this course.									