Penetration Testing with Kali Linux (PWK) Training

Duration: **5 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Penetration Testing with Kali (PWK) is a pen testing course 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.

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.

What You Will Learn

- Penetration Testing with Kali Linux
- Penetration Testing: What You Should Know
- Getting Comfortable with Kali Linux
- The Essential Tools
- Passive Information Gathering
- Active Information Gathering
- Vulnerability Scanning
- Buffer Overflows
- Win32 Buffer Overflow Exploitation
- Linux Buffer Overflow Exploitation
- Working with Exploits
- File Transfers
- Privilege Escalation
- Client Side Attacks
- Web Application Attacks
- Password Attacks
- Port Redirection and Tunneling
- The Metasploit Framework
- Bypassing Antivirus Software
- Assembling the Pieces: Penetration Test Breakdown

Training Outline

Penetration Testing with Kali Linux (PWK) Training

Duration: **5 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

0 Penetration Testing: What You Should Know

- 0.1 About Kali Linux
- 0.2 About Penetration Testing
- 0.3 Legal
- 0.4 The megacorpone.com Domain
- 0.5 Offensive Security Labs
- 0.5.1 VPN Labs Overview
- 0.5.2 Lab Control Panel
- 0.5.3 Reporting

1. Getting Comfortable with Kali Linux

- 1.1 Finding Your Way around Kali
- 1.1.1 Booting Up Kali Linux
- 1.1.2 The Kali Menu
- 1.1.3 Find, Locate, and Which
- 1.1.4 Exercises
- 1.2 Managing Kali Linux Services
- 1.2.1 Default root Password
- 1.2.2 SSH Service
- 1.2.3 HTTP Service
- 1.2.4 Exercises
- 1.3 The Bash Environment
- 1.4 Intro to Bash Scripting
- 1.4.1 Practical Bash Usage – Example 1
- 1.4.2 Practical Bash Usage – Example 2
- 1.4.3 Exercises

2. The Essential Tools

- 2.1 Netcat
- 2.1.1 Connecting to a TCP/UDP Port
- 2.1.2 Listening on a TCP/UDP Port
- 2.1.3 Transferring Files with Netcat
- 2.1.4 Remote Administration with Netcat
- 2.1.5 Exercises
- 2.2 Ncat
- 2.2.1 Exercises
- 2.3 Wireshark
- 2.3.1 Wireshark Basics
- 2.3.2 Making Sense of Network Dumps
- 2.3.3 Capture and Display Filters
- 2.3.4 Following TCP Streams
- 2.3.5 Exercises
- 2.4 Tcpdump
- 2.4.1 Filtering Traffic
- 2.4.2 Advanced Header Filtering
- 2.4.3 Exercises

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

3. Passive Information Gathering

- 3.1 Open Web Information Gathering
- 3.1.1 Google
- 3.1.2 Google Hacking
- 3.1.3 Exercises
- 3.2 Email Harvesting
- 3.2.1 Exercise
- 3.3 Additional Resources
- 3.3.1 Netcraft
- 3.3.2 Whois Enumeration
- 3.3.3 Exercise
- 3.4 Recon--ng

4. Active Information Gathering

- 4.1 DNS
- 4.1.1 Interacting with a DNS Server
- 4.1.2 Automating Lookups
- 4.1.3 Forward Lookup Brute Force
- 4.1.4 Reverse Lookup Brute Force
- 4.1.5 DNS Zone Transfers
- 4.1.6 Relevant Tools in Kali Linux
- 4.1.7 Exercises
- 4.2 Port Scanning
- 4.2.1 TCP CONNECT / SYN Scanning
- 4.2.2 UDP Scanning
- 4.2.3 Common Port Scanning Pitfalls
- 4.2.4 Port Scanning with Nmap
- 4.2.5 OS Fingerprinting
- 4.2.6 Banner Grabbing/Service Enumeration
- 4.2.7 Nmap Scripting Engine (NSE)
- 4.2.8 Exercises
- 4.3 SMB Enumeration
- 4.3.1 Scanning for the NetBIOS Service
- 4.3.2 Null Session Enumeration
- 4.3.3 Nmap SMB NSE Scripts
- 4.3.4 Exercises
- 4.4 SMTP Enumeration
- 4.4.1 Exercise
- 4.5 SNMP Enumeration
- 4.5.1 MIB Tree
- 4.5.2 Scanning for SNMP
- 4.5.3 Windows SNMP Enumeration Example
- 4.5.4 Exercises

5. Vulnerability Scanning

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- 5.1 Vulnerability Scanning with Nmap
- 5.2 The OpenVAS Vulnerability Scanner
- 5.2.1 OpenVAS Initial Setup
- 5.2.2 Exercises

6. Buffer Overflows

- 6.1 Fuzzing
- 6.1.1 Vulnerability History
- 6.1.2 DEP and ASLR
- 6.1.3 Interacting with the POP3 Protocol
- 6.1.4 Exercises

7. Win32 Buffer Overflow Exploitation

- 7.1 Replicating the Crash
- 7.2 Controlling EIP
- 7.2.1 Binary Tree Analysis
- 7.2.2 Sending a Unique String
- 7.2.3 Exercises
- 7.3 Locating Space for Your Shellcode
- 7.4 Checking for Bad Characters
- 7.4.1 Exercises
- 7.5 Redirecting the Execution Flow
- 7.5.1 Finding A Return Address
- 7.5.2 Exercises
- 7.6 Generating Shellcode with Metasploit
- 7.7 Getting a Shell
- 7.7.1 Exercises
- 7.8 Improving the Exploit
- 7.8.1 Exercises

8. Linux Buffer Overflow Exploitation

- 8.1 Setting up the Environment
- 8.2 Crashing Crossfire
- 8.2.1 Exercise
- 8.3 Controlling EIP
- 8.4 Finding Space for Our Shellcode
- 8.5 Improving Exploit Reliability
- 8.6 Discovering Bad Characters
- 8.6.1 Exercises
- 8.7 Finding a Return Address
- 8.8 Getting a Shell
- 8.8.1 Exercise

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

9. Working with Exploits

- 9.1 Searching for Exploits
- 9.1.1 Finding Exploits in Kali Linux
- 9.1.2 Finding Exploits on the Web
- 9.2 Customizing and Fixing Exploits
- 9.2.1 Setting Up a Development Environment
- 9.2.2 Dealing with Various Exploit Code Languages
- 9.2.3 Exercises

10. File Transfers

- 10.1 Anti-Virus Software
- 10.2 File Transfer Methods
- 10.2.1 The Non--Interactive Shell
- 10.2.2 Uploading Files
- 10.2.3 Exercises

11. Privilege Escalation

- 11.1 Privilege Escalation Exploits
- 11.1.1 Local Privilege Escalation Exploit in Linux Example
- 11.1.2 Local Privilege Escalation Exploit in Windows Example
- 11.2 Configuration Issues
- 11.2.1 Incorrect File and Service Permissions
- 11.2.2 Think like a Network Administrator
- 11.2.3 Exercises

12. Client Side Attacks

- 12.1 Know Your Target
- 12.1.1 Passive Client Information Gathering
- 12.1.2 Active Client Information Gathering
- 12.1.3 Social Engineering and Client Side Attacks
- 12.1.4 Exercises
- 12.2 MS12-037 Internet Explorer 8
- 12.2.1 Setting up the Client Side Exploit
- 12.2.2 Swapping Out the Shellcode
- 12.2.3 Exercises
- 12.3 Java Signed Applet Attack
- 12.3.1 Exercises

13. Web Application Attacks

- 13.1 Essential Iceweasel Add--ons
- 13.2 Cross Site Scripting (XSS)

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- 13.2.1 Browser Redirection and IFRAME Injection
- 13.2.2 Stealing Cookies and Session Information
- 13.2.3Exercises
- 13.3 File Inclusion Vulnerabilities
- 13.3.1 Local File Inclusion
- 13.3.2 Remote File Inclusion
- 13.4 MySQL SQL Injection
- 13.4.1 Authentication Bypass
- 13.4.2 Enumerating the Database
- 13.4.3 Column Number Enumeration
- 13.4.4 Understanding the Layout of the Output
- 13.4.5 Extracting Data from the Database
- 13.4.6 Leveraging SQL Injection for Code Execution
- 13.5 Web Application Proxies
- 13.5.1 Exercises
- 13.6 Automated SQL Injection Tools
- 13.6.1 Exercises

14. Password Attacks

- 14.1 Preparing for Brute Force
- 14.1.1 Dictionary Files
- 14.1.2 Key-space Brute Force
- 14.1.3 Pwdump and Fgdump
- 14.1.4 Windows Credential Editor (WCE)
- 14.1.5 Exercises
- 14.1.6 Password Profiling
- 14.1.7 Password Mutating
- 14.2 Online Password Attacks
- 14.2.1 Hydra, Medusa, and Ncrack
- 14.2.2 Choosing the Right Protocol: Speed vs. Reward
- 14.2.3 Exercises
- 14.3 Password Hash Attacks
- 14.3.1 Password Hashes
- 14.3.2 Password Cracking
- 14.3.3 John the Ripper
- 14.3.4 Rainbow Tables
- 14.3.5 Passing the Hash in Windows
- 14.3.6 Exercises

15. Port Redirection and Tunneling

- 15.1 Port Forwarding/Redirection
- 15.2 SSH Tunneling
- 15.2.1 Local Port Forwarding
- 15.2.2 Remote Port Forwarding
- 15.2.3 Dynamic Port Forwarding
- 15.3 Proxychains
- 15.4 HTTP Tunneling

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- 15.5 Traffic Encapsulation
- 15.5.1 Exercises

16. The Metasploit Framework

- 16.1 Metasploit User Interfaces
- 16.2 Setting up Metasploit Framework on Kali
- 16.3 Exploring the Metasploit Framework
- 16.4 Auxiliary Modules
- 16.4.1 Getting Familiar with MSF Syntax
- 16.4.2 Metasploit Database Access
- 16.4.3 Exercises
- 16.5 Exploit Modules
- 16.5.1 Exercises
- 16.6 Metasploit Payloads
- 16.6.1 Staged vs Non--Staged Payloads
- 16.6.2 Meterpreter Payloads
- 16.6.3 Experimenting with Meterpreter
- 16.6.4 Executable Payloads
- 16.6.5 Reverse HTTPS Meterpreter
- 16.6.6 Metasploit Exploit Multi Handler
- 16.6.7 Revisiting Client Side Attacks
- 16.6.8 Exercises
- 16.7 Building Your Own MSF Module
- 16.7.1 Exercise
- 16.8 Post Exploitation with Metasploit
- 16.8.1 Meterpreter Post Exploitation Features
- 16.8.2 Post Exploitation Modules
- B10B7B11B12

17.Bypassing Antivirus Software

- 17.1 Encoding Payloads with Metasploit
- 17.2 Crypting Known Malware with Software Protectors
- 17.3 Using Custom/Uncommon Tools and Payloads
- 17.4 Exercise

18. Assembling the Pieces: Penetration Test Breakdown

- 18.1 Phase 0 – Scenario Description
- 18.2 Phase 1 – Information Gathering
- 18.3 Phase 2 – Vulnerability Identification and Prioritization
- 18.3.1 Password Cracking
- 18.4 Phase 3 – Research and Development
- 18.5 Phase 4 – Exploitation
- 18.5.1 Linux Local Privilege Escalation
- 18.6 Phase 5 – Post--Exploitation

BİLGİNÇ
IT Academy

info@bilginc.com
bilginc.com

- 18.6.1 Expanding Influence
- 18.6.2 Client Side Attack against Internal Network
- 18.6.3 Privilege Escalation Through AD Misconfigurations
- 18.6.4 Port Tunneling
- 18.6.5 SSH Tunneling with HTTP Encapsulation
- 18.6.6 Looking for High Value Targets
- 18.6.7 Domain Privilege Escalation
- 18.6.8 Going for the Kill