Penetration Testing with Kali Linux

Duration 5 Days

COURSE DESCRIPTION

Penetration Testing with Kali Linux is Designed for IT Professionals who are new to Kali Linux. This course will actively engage students in task focused activities, lab-based knowledge checks, and facilitative discussions to ensure maximum skill transfer and retention. In addition, GUI-based Environment will be featured to build on the student's existing technical knowledge, while command line concepts will be introduced to provide a foundation for students planning to become full time kali Linux expert. Moreover, the course will also prepare students for the ***Offensive Security Certified Professional (OSCP) exam***, which typically proceeds the PWK course. Students should be familiar with Linux command line, common networking terminology, and basic Bash/Python scripting prior to attempting this course.

COURSE OBJECTIVES

After completing this course, the attendees will;

- Gain insight into the offensive security field, which will expand awareness for the need of real-world security solutions.
- Learn to implement various reconnaissance techniques, identify various attack vectors and identify various post exploitation techniques.
- To make you aware of the hazards of malicious activities perforated by the Black-hat hackers.
- This Kali Linux Training will give you in-depth knowledge about how actual hacking is done, and how to test an environment and its reliability which people term as highly secure.

COURSE OUTLINE

Topics and hands-on exercises for the course include:

- **Introduction to Kali**
  - Overview of Linux OS
  - Brief history and overview of Kali Linux
  - Overview of Kali tools and utilities
    - Hands-on exercise - Basic Linux usage: working with terminal (command line), using utilities for file and process viewing/manipulation
    - Hands-on exercise – Manipulating text files on Linux command line
    - Hands-on exercise – Tips on tricks for efficient use of command line
- **Information Gathering**
  - Overview of Kali Information Gathering tools
  - DNS analysis
  - OS fingerprinting
  - SNMP analysis
  - Network discovery
    - Hands-on exercise – Abusing DNS: using whois, dig, and dnsrecon to query DNS servers and performing reverse lookups
    - Hands-on exercise – Abusing SNMP: cracking SNMP community strings and enumerating information via SNMP

    - Hands-on exercise – TCP/IP for Hackers: using Wireshark to capture and examine TCP, UDP, and ICMP packets
    - Hands-on exercise – Network and Host Discovery: using netdiscover, traceroute, hping3, and nmap to identify network hosts

- **Port Scanning**
  - Nmap overview
  - Port scanning techniques
  - Service identification
    - Hands-on exercise - Port Scanning with Nmap: performing basic TCP, UDP, ping, and OS fingerprinting scans with Nmap
    - Hands-on exercise – Stealthy Scanning: using Nmap timing options, SYN, and idle scanning techniques
    - Hands-on exercise – Service Identification: using telnet, netcat, and Nmap –sV scans to identify running services
    - Hands-on exercise – Nmap Scripting Engine (NSE): using NSE to gather detailed information about network hosts
- **Sniffing/Spoofing/Main-in-the-Middle**
  - Overview of Kali Sniffing/Spoofing tools
  - ARP Spoofing
  - Wireshark and Dsniff
    - Hands-on exercise – Sniffing credentials: using arpspoof and Wireshark to perform a Man-in-the-Middle attack and capture FTP credentials
    - Hands-on exercise – Capturing images: using Dsniff tools to capture images from intercepted network traffic
- **Buffer Overflow**
  - Concept of Buffer Overflow
  - Stack and Heap overflows
- **Working with Exploits**
  - Exploit definition
  - Client-side exploits
  - Server-side exploits
  - Finding Exploits
    - Hands-on exercise – Server-side Exploit: running a Perl exploit script to exploit a vulnerable server application
- **Exploit Framework/Metasploit**
  - Metasploit Overview
  - Metasploit Modules and Payloads
  - The Meterpreter Payload
  - Adding Custom Exploits to Metasploit
    - Hands-on exercise - Exploiting Vulnerable Services: using a Metasploit exploit module to gain access to a remote system
    - Hands-on exercise – Additional Payloads: using Metasploit VNC and Meterpreter payloads on a compromised system
    - Hands-on exercise – Client-side Exploit DLL Hijack: compromising a system with Metasploit's WebDAV DLL Hijacker module
- **Password Attacks**
  - Types of Password Attacks
  - Overview of Kali Password Attacks Tools

    - Hands-on exercise – Post-exploit Password Cracking: dumping password hashes from a compromised system and cracking hashed passwords with John the Ripper

- **DoS Attack**
  - DoS/DDoS Attack Definition
  - Performing DoS attacks with Kali (hping3, Metasploit auxiliary modules)

- **Web Application Attacks**
  - Common Web Application Vulnerabilities and Attacks
  - Overview of Kali Web Applications Tools
  - Working with Burp Suite
    - Hands-on exercise – Unvalidated Parameters: using Burp Suite to intercept and modify HTTP POST requests
    - Hands-on exercise – Cross-Site Scripting (XSS): performing a stored XSS attack
    - Hands-on exercise – Basic SQL Injection: performing a SQL injection attack using common techniques
    - Hands-on exercise – SQL Injection Chained Exploit: combining SQL injection techniques for a sophisticated attack

- **Trojan Horses**
  - Trojan Horse Definition and Usage
  - Overview of Kali Maintaining Access Tools
  - Covert Channels
    - Hands-on exercise – Using Ncat as a Trojan: uploading ncat to a compromised system for maintaining access
    - Hands-on exercise – IDS Evasion: using SSL with ncat to evade Snort IDS
    - Hands-on exercise – Covert Channels: using Metasploit to create an HTTPS covert channel tool

- **Rootkits**
  - Rootkits Definition and Usage
  - Detecting Rootkits

- **Penetration Testing Techniques**
  - Review of Previously Discussed Techniques
  - Review of Kali Wireless Attacks, Reverse Engineering, Forensics, and Reporting Tools
  - Social Engineering
    - Hands-on exercise – Credential Harvesting: using Social Engineering Toolkit (SET) and arpspoofing to spoof a website and capture loging credentials in a Mand-in-the Middle attack
    - Hands-on exercise – Spear Phishing: using SET to create a malicious exploit script and deliver it via phishing email

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.