CloudSystems Limited
Ka-57/1, Kazi Tower 3rd Floor,
Kuril Bus Stand, Dhaka-1229.
☎+880 1712900654

Penetration Testing With Kali Linux

Course Overview:

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.

Penetration Testing with Kali Linux is a foundational security course, but still requires students to have certain knowledge prior to attending the training 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. This advanced penetration testing course is not for the faint of heart; it requires practice, testing, and the ability to want to learn in a manner that will grow your career in the information security field and overcome any learning plateau. Offensive Security challenges you to rise above the rest, dive into the fine arts of advanced penetration testing, and to Try Harder™.

What will learn?

- ✓ Enumerate/scan systems with Netdiscover, Nmap, Dirb, Nikto, etc.
- ✓ Perform remote exploitation of systems
- ✓ Escalate local privileges to root level
- ✓ Utilize a variety of industry standard penetration testing tools within the Kali Linux distro

Who should take this course?

- Security and Risk Management
- Asset Security
- Security Engineering
- Communications and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

Basic Requirement

- Basic Linux knowledge
- Basic networking knowledge

Course Duration

40 Hours

CloudSystems Limited
Ka-57/1, Kazi Tower 3rd Floor,
Kuril Bus Stand, Dhaka-1229.
☎+880 1712900654

Details Course Outline:

Course Title: Penetration Testing With Kali Linux

Course Duration in days: 5 Days	**Course Duration in hours: 40**

Course Details

1. **Penetration Testing : Methodologies, Standards and IT Acts**
   - Penetration Testing and Cyber Security
   - Vulnerability Assessment and Analysis
   - Phases of Penetration Testing
   - Cyber Security Standards, Policies and Acts

2. **Penetration Testing with Kali Linux: Lab Preparation**
   - Foundations of Kali Linux
   - Installation of Kali Linux in Virtual Machines
   - Updating Kali Linux with Apt-Get Command
   - Adding/Installing Penetration Testing Tools from GitHub
   - Preparing penetration Testing Labs
     Labs- OS Installation
     Ubuntu 17.04, Windows 10/16, MAC OS, Red Hat Linux
   - Basic Commands of Linux
   - Customizing Kali Linux for faster package updates
   - Customizing Kali Linux for faster operations
   - Configuring remote connectivity services - HTTP, TFTP, and SSH

3. **Introduction to Metasploit**
   - Metasploit Overview
   - Picking an Exploit
   - Setting Exploit Options
   - Multiple Target Types
   - Getting a remote shell on a Windows XP Machine
   - Picking a Payload
   - Setting Payload Options
   - Running the Exploit

14. **Network Exploitation**
    - Gathering information for credential cracking
    - Cracking FTP using custom wordlist
    - Cracking SSH using custom wordlist
    - Cracking HTTP using custom wordlist
    - Cracking MySql and PostgreSQL using custom wordlist
    - Cracking Cisco login using custom wordlist
    - Exploiting vulnerable services (Unix)
    - Exploiting vulnerable services (Windows)
    - Exploiting services using exploit-db scripts

15. **Web Application Information Gathering**
    - Setting up API keys for recon-ng
    - Using recon-ng for reconnaissance
    - Gathering information using theharvester
    - Using DNS protocol for information gathering
    - Web application firewall detection
    - HTTP and DNS load balancer detection
    - Discovering hidden files/directories using DirBuster
    - CMS and plugins detection using WhatWeb and p0f
    - Finding SSL cipher vulnerabilities

16. **Web Application Vulnerability Assessment**
    - Running vulnerable web applications in Docker
    - Using w3af for vulnerability assessment

- Connecting to a Remote Session

4. **Meterpreter Shell**
   - Basic Meterpreter Commands
   - Core Commands
   - File System Commands
   - Network Commands
   - System Commands
   - Capturing Webcam Video, Screenshots and Sound
   - Running Scripts
   - Playing with Modules - Recovering Deleted Files from Remote System

5. **Metasploitable Tutorial - Part One**
   - Installing and Using Metasploitable
   - Scanning for Targets
   - Exploiting the Unreal IRC Service
6. **Metasploitable - Part Two: Scanners**
   - Using a Scanner
   - Using Additional Scanners
   - Scanning a Range of Addresses
   - Exploiting the Samba Service
7. Windows AV Bypass with Veil
   - Installing Veil
   - Using Veil
   - Getting a Remote Shell
8. **Windows Privilege Escalation by Bypassing UAC**
   - UAC Bypass
9. **Packet Captures and Man-in-the-Middle Attacks**
   - Creating a Man-in-the-Middle attack with Arpspoof
   - Viewing URL information with Urlsnarf
   - Viewing Captured Graphics with Driftnet
   - Remote Packet Capture in Metasploit
   - Wireshark
   - Xplico
10. **Using the Browser Exploitation Framework**
    - BeEF in Action
11. **Information Gathering and Tools on Kali Linux**
    - Using Nikto for web server assessment
    - Using Skipfish for vulnerability assessment
    - Using Burp Proxy to intercept HTTP traffic
    - Using Burp Intruder for customized attack automation
    - Using Burp Sequencer to check the session randomness

17. **Web Application Exploitation**
    - Using Burp for active/passive scanning
    - Using sqlmap to find SQL Injection on the login page
    - Using sqlmap to find SQL Injection on URL parameters
    - Using commix for automated OS command injection
    - Using weevely for file upload vulnerability
    - Exploiting Shellshock using Burp
    - Using Metasploit to exploit Heartbleed
    - Using the FIMAP tool for file inclusion attacks (RFI/LFI)

18. **System and Password Exploitation**
    - Using local password-attack tools
    - Cracking password hashes
    - Using Social-Engineer Toolkit
    - Using BeEF for Browser Exploitation
    - Cracking NTLM hashes using rainbow tables

19. **Privilege Escalation and Exploitation**
    - Using WMIC to find privilege-escalation vulnerabilities
    - Sensitive-information gathering
    - Unquoted service-path exploitation
    - Service permissions issues
    - Misconfigured software installations/insecure file permissions

- Discovering live servers over the network
- Bypassing IDS/IPS/firewall
- Discovering ports over the network
- Using unicornscan for faster port scanning
- Service fingerprinting
- Determining the OS using nmap and xprobe2
- Service enumeration
- Open-source information gathering
- Information Gathering And Vulnerability Assessment
- Network Packet Analysis-Sniffing
- Network Scanning
- Wireless Security Testing And Hardware Security Testing
- Web Applications Testing & Passwords Auditing
- Maintaining Access And Covering Tracks

12. **Information Gathering: Tools and Steps on Kali Linux**
    - Sub-Net Discovery with Netdiscover and P0f
    - Domain Analysis with Maltego(CE) and Dmitry
    - OS Fingerprinting with Nmap
    - Social Media Profiling with Recon-ng
    - Banner Grabbing with Whatweb
    - E-Mail Harvesting with Metasploit
    - Database Information using Metasploit
    - Penetration Testing Report Writing
13. **Network Vulnerability Assessment**
    - Using nmap for manual vulnerability assessment
    - Integrating nmap with Metasploit
    - Walkthrough of Metasploitable assessment with Metasploit
    - Vulnerability assessment with OpenVAS framework
    - Linux privilege escalation
20. **Vulnerability Assessment and Analysis**
    - Network Vulnerability Assessment with Nessus
    - Web Application Vulnerability Analysis with W3AF, Nessus, Skipfish, Vega and Burpsuite
    - Database Vulnerability Assessment with SQLMap and OSScanner(Oracle)
21. **Network Defence and Conclusion**
    - Patches & Updates
    - Firewalls and IPS
    - Anti-Virus/ Network Security Programs
    - Limit Services & Authority Levels
    - Use Script Blocking Programs
    - Use Long Complex Passwords
    - Network Security Monitoring
    - Logging
    - Educate your users
    - Scan your Network
    - Learn Offensive Computer Security
22. **Writing Penetration Testing Report : Concepts, Tools and Steps on Kali Linux :-**
    - Different Types of Penetration Testing Report
    - Different Types of Vulnerability Assessment Report
    - Different Types of Security Auditing/Compliance Auditing Report
    - Features of Good Penetration Testing Report
    - ***Designing Information Security Controls/Measures***
    - Writing Forensics Report with Dradis, Magic Tree and Casefile(Reporting Tool)