learnfly Pro
Up-skill Yourself

Advanced Penetration Testing With Kali Linux v2.0

➢Introduction to kali Linux

- Installing Kali Linux
- Configure Network Connection
- Administering Kali Linux
- Updating and Upgrading kali Linux
- Introduction to Bash Environment
- Automating Administration with Bash Scripting

➢Penetration Testing Standard

- Open Web Application Security Project (OWASP)
- Licensee Penetration Testing (LPT)

➢Penetration Testing Classification

- White Box and Black Box
- Penetration Testing vs. Vulnerability Assessment

➢Information Discovery

- Google hacking
- DNS Information Gathering
- Whois Information Gathering
- Email Tracking
- Route and Network information Gathering
- All-in-one information gathering

➢Scanning Target

- TCP Connect Port Scanning
- Stealth Port Scanning techniques
- UDP port Scanning
- Nmap Scripting Engine

- Advance Port Scanning Techniques
- Active Banners and System OS Enumeration
- Passive Banners and System OS Enumeration

➢**Enumerating Target**

- Enumerating users, groups and shares with SMB
- Enumerating DNS resource records
- Enumerating SNMP
- Enumerating SMTP

➢**Vulnerability Assessment Tools for System**

- Nmap
- Nessus
- Open Vas

➢**Discovering Zero Day**

- Vulnerability Research
- Introduction to fuzzing
- Memory Stack and Heap
- Introduction to Buffer Overflow
- DEP and ASLR
- Introduction to General Purpose CPU Registers

➢**Buffer Overflow in Action (Windows)**

- Detecting Crash
- Calculating Buffer Size
- Controlling Crash
- Checking for Bad Characters
- Calculating Shell code Space
- Determining Return Address
- Getting the Shell
- Improving the Exploit

➢ **Buffer overflow in Action (Linux)**

- Crashing Crossfire
- Controlling the Crash
- Calculating Shell code Space
- Improving Exploit Reliability
- Finding Bad characters
- Finding Return Address
- Getting the Shell

- **Using Custom Exploits**

  - Locating exploits in Kali
  - Locating Exploit on Web
  - Development Environment Setup
  - Analyzing Exploit Code Languages

- **Target Exploitation**

  - Setting up Metaslpoit
  - Different User Interfaces in Metasploit
  - Msfconsole
  - Msfcli
  - Msfvenom
  - Exploitation with Metasploit
  - Using Metasploit Auxiliary
  - Using Exploits Modules
  - Getting Familiar with Payloads
  - Staged and Non-staged Payloads
  - Working with Meterpreter Session
  - Working with Multi Handler
  - VNC Exploitation
  - Building Your Own MSF Modules
  - Using Post Exploitation Modules
  - Enabling RDP
  - Dumping Password Hashes

- **Privileges Escalation**

  - Escalating Local Privilege in Linux

- Bypassing UAC in Windows
- Escalating Privileges through Physical Access
- Misconfiguration Attacks for Privilege Escalation

- **Password Cracking**

  - Types of Password Attacks
  - Password Cracking Techniques
  - Generating Password Dictionary
  - Dictionary Attack
  - Rainbow Attack
  - Brute Force Attack
  - Introduction to Windows and Linux Password Hash
  - Pwdump and L0pthCrack
  - Breaking Password Hash
  - John the Ripper and OphCrack
  - Pass the Hash in Windows
  - Cracking Telnet and SSH password
  - Cracking FTP and HTTP password
  - Hydra , Fireforce and Ncrack
  - Using Metasploit Post Exploitation Modules

- **Bypassing Antivirus**

  - Encoding Payload using Msfencode
  - Using Veil Framework
  - Using Shellter
  - Using Custom Tools and Payloads

- **Maintaining Access**

  - Protocol Tunnelling
  - Proxy
  - Installing persistent Backdoor
  - Netcat, The Swiss Army Knife
  - Starting a Listener using Netcat
  - Connecting to Target using Netcat
  - Stealing Files with Netcat
  - Controlling Target with Netcat

- **Advance Sniffing**

  - Sniffing Concepts
  - Using WireShark for Sniffing
  - Capture And Display Filters
  - Follow TCP Stream
  - Analysing Graphs and Endpoints in Wireshark
  - Tracing Geo Location of IP in Wireshark
  - Using TCP Dump
  - ARP Poisoning
  - DHCP Starvation
  - Mac flooding
  - DNS Poisoning redirecting user to fake website
  - Sniffing Credentials From Secured Websites

- **DOS Attack**

  - SYN Flood Attack
  - Application request Flood Attack
  - Service request Flood
  - Permanent Denial of Service Attack

- **Web Application Penetration Testing**

  - Introduction to Web Application Vulnerabilities
  - Introduction to BurpSuite Proxy
  - Cross Site Scripting (XSS)
  - IFRAME Injection
  - Cookie Stealing
  - Session Hijacking
  - Cross Site Request Forgery (CSRF)
  - LFI and RFI
  - Hacking database using SQL injection
  - Enumerating Database
  - Extracting Database Records
  - SQL Injection with Automated Tools
  - Web Application Assessment and Exploitation with Automated Tools

- **Wireless Penetration Testing**

- Introduction to Wireless Security
- Cracking Wireless Encryptions
- Cracking WEP
- Cracking WPA and WPA2
- Configuring Fake Access Point
- Halting Wireless Network Through Dos Attack
- Restricting Wireless Access Through Wireless Jammer

- **Exploits and Client Side Attack**

  - Introduction to Client Side Attacks
  - Gathering Client Information
  - Exploiting Browser Vulnerability
  - Exploiting Internet Explorer Vulnerabilities
  - Exploiting Firefox vulnerabilities
  - Exploiting Safari Vulnerabilities
  - Metasploit Browser Autopwn

- **Social Engineering Toolkit**

  - Stealing passwords through phishing
  - Generating backdoors
  - Java Applet attack Method

- **Firewall Testing**

  - Introduction to Firewall
  - Testing Firewall
  - Testing Firewall Rules
  - Testing Ports

- **Document Management and Reporting**

  - Documentation and results verification
  - Dradis Framework
  - Magic Tree and Maltego

- **Data Collection ,Evidence Management and Reporting**

- Type of Report
- Presentation Report
- Post Testing Procedure