Certified advanced Penetration Tester

Setting up the Lab
- Installing and configuring VMware workstation
- Installing Kali Linux
- Configure Network Connection
- Updating and Upgrading kali Linux
- Introduction to Bash Environment
- Automating Administration with Bash Scripting

Penetration Testing Standard
- Penetration testing framework
- Pre-engagement interactions
- Intelligence gathering
- Threat modelling

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

Information Discovery
- Google hacking
- Discovering Devices using Shodan
- 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
- Buffer overflow in action

Target Exploitation
- Setting up Metaslpoit
- 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
- Adding 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)
- 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
- Revealing hidden SSID
- 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
- Metasploit Browser Autopwn

Social Engineering Toolkit
- Stealing passwords through phishing
- Generating backdoors
- Java Applet attack Method

Firewall and IDS Testing
- Introduction to Firewall and IDS
- Testing IDS rules
- Testing Firewall Rules
- Firewalking

Data Collection ,Evidence Management and Reporting
- Type of Report
- Presentation Report
- Post Testing Procedure