Advance penetration testing with Kali Linux

- Introduction to kali Linux

    What is new in kali linux

    Installing kali linux

    Configure Network Connection

    Using kali Linux

    Update kali Linux

- 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

- Advance Penetration Methodology

    Target Framework and Scope

    Gathering client requirements

    Test plan checklist

    Profiling test boundaries

- Information Discovery

    Google hacking

    DNS Information Gathering

    Whois Information Gathering

    Route and Network information Gathering

    All-in-one information gathering

- Scanning Target

Advance Network Scanning

Port Scanning

Stealth Port scaning techniques

Udp port Scanning

Packet crafting using Hping

Nmap Scanning and Plug-ins

Active Banners and System OS Enumeration

Passive Banners and System OS Enumeration

- Vulnerability Assessment Tools for System

Nessus

Open Vas

- Enumerating Target

Enumerating users, groups and shares

Enumerating DNS resource records

Enumerating Network devices

- Target Exploitation

Setting up metaslpoit

Exploitation with Metasploit

Working with Meterpreter Session

VNC Exploitation

Stealing password Hash

Adding custom Modules to Metasploit

- Exploit Writing

Using Immunity Debugger

Writing Exploit for real world applications

- Privileges Escalation

Breaking Password hashes

Cracking telnet and ssh password

Craking FTP password

Using metasploit post exploitation modules

- Maintaining Access

  Protocol tunneling

  Proxy

  Installing persistent Backdoor

- Advance Sniffing

  ARP Poisoning

  DHCP Starvation

  Mac flooding

  DNS Poisoning: redirecting user to fake website

  Sniffing credentials from secured websites

- DOS Attack

  Syn Attack

  Application request Flood Attack

  Service request Flood

  Permanent denial of service atack

- Web Penetration Testing

  Introduction to Web Application Vulnerabilities

  Web Application Assessment and Exploitation with automation Tools

  Hacking database using SQL injection

  Hijacking web sessions

- Wireless Penetration Testing

  Introduction to Wireless Security

  Craking Wireless Encryptions (WEP,WPA,WPA2)

  Configuring Fake Access Point

  Halting wireless network through Dos attack

  Restricting wireless access through wireless jammer

- Exploits and Client Side Attack
  - Exploiting browser vulnerability
  - Introduction to Buffer overflow
  - Introduction to fuzzing
  - Fast-Track Hacking
- Social Engineering Toolkit
  - Stealing passwords through phishing
  - Generating backdoors
  - Java Applet attack
- 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