Course Topic Page: Advance Penetration Testing With Kali 20

1. Introduction to kali Linux

- What is new in kali linux
- Installing kali linux
- Configure Network Connection
- Using kali Linux
- Update kali Linux

2. Penetration Testing Standard

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

3. Penetration Testing Classification

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

4. Advance Penetration Methodology

- Target Framework and Scope
- Gathering client requirements
- Test plan checklist
- Profiling test boundaries
- Advance penetration testing with Kali Linux

5. Information Discovery

- Google hacking
- DNS Information Gathering
- Who is Information Gathering
- Route and Network information Gathering
- All-in-one information gathering

6. Scanning Target

- Advance Network Scanning
- Port Scanning
- Stealth Port scanning 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

7. Vulnerability Assessment Tools for System

- Nessus
- Open Vas

8. Enumerating Target

- Enumerating users, groups and shares
- Enumerating DNS resource records
- Enumerating Network devices

9. Target Exploitation

- Setting up metaslpoit
- Exploitation with Metasploit
- Working with Meterpreter Session
- VNC Exploitation
- Stealing password Hash
- Adding custom Modules to Metasploit

10. Exploit Writing

- Using Immunity Debugger
- Writing Exploit for real world applications

11. Privileges Escalation

- Breaking Password hashes
- Cracking telnet and ssh password
- Cracking FTP password
- Using metasploit post exploitation modules

12. Maintaining Access

- Protocol tunneling
- Proxy
- Installing persistent Backdoor

13. Advance Sniffing

- ARP Poisoning
- DHCP Starvation
- Mac flooding
- DNS Poisoning: redirecting user to fake website
- Sniffing credentials from secured websites

14. DOS Attack

- Syn Attack
- Application request Flood Attack

- Service request Flood
- Permanent denial of service attack

15. Web Penetration Testing

- Introduction to Web Application Vulnerabilities
- Web Application Assessment and Exploitation with automation Tools
- Hacking database using SQL injection
- Hijacking web sessions

16. Wireless Penetration Testing

- Introduction to Wireless Security
- Cracking Wireless Encryptions (WEP,WPA,WPA2)
- Configuring Fake Access Point
- Halting wireless network through Dos attack
- Restricting wireless access through wireless jammer

17. Exploits and Client Side Attack

- Exploiting browser vulnerability
- Introduction to Buffer overflow
- Introduction to fuzzing
- Fast-Track Hacking

18. Social Engineering Toolkit

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

19. Firewall Testing

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

20. Document Management and Reporting

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

21. Data Collection, Evidence Management and Reporting

- Type of Report
- Presentation Report

- Post Testing Procedure