SecuLabs

Wireless Penetration Testing Framework

1. WLAN Discovery
2. Encrypted and Unencrypted WLAN configuration
3. SSID Scanning and Monitoring
4. IP Sniffing Detection
5. Wireless Data Collection
6. WI-FI Mac Analysis
7. Wireless Tools & Information Analysis
8. Client, Crypto & Enterprise Attacks Testing
9. Analyzing wireless traffic with TCPDump, Wireshark, Kismet
10. Mapping Wireless Networks with GPSMAP
11. Live Network Mapping
12. Identifying capabilities & Features of EAP
13. Packet Framing on Wireless Networks
14. Sniffing in Monitor Mode detection
15. Defining and Understanding rogue networks
16. Security from malicious Rogue Networks
17. Wired & Wireless side AP Fingerprinting
18. Wireless side warwalking & Client monitoring
19. Mobile Devices & hotspots Access testing
20. Defensive Measures for Administrators and Service Providers
21. WEP, WPA-PSK, WPA2-PSK Decryption Mechanism Configuration.
22. Applying WEP Failures to other network protocols
23. Testing Hotspot injection Attacks
24. Testing of PSPF & Wireless network isolation vulnerabilities
25. Establishing Amazon EC2 cloud computing systems for public and private networks
26. Testing of TKIP Plain text Recovery Attacks
27. Testing & Configuration of Protocol Fuzzing

28. Configuring Metasploit Framework Meterpreter Exploits
29. WLAN IDS Analyst Techniques
30. WIDS Deployment Models
31. Trend Analysis and Anomaly analysis
32. Evaluating Attacks through traffic Analysis
33. Managing an authentication Architecture
34. Managing Client certificate trust Policies
35. Different techniques for deploying a new root certificate authority – Manual , Web Server Delivery, Scripted Web Server Delivery, Automatic trust with GPO
36. Managing third party wireless manager tools
37. Create a custom installer with Odyssey manager
38. Implementing wireless specific GPO Policies

SecuLabs

Penetration testing process

Phase 1 – Reconnaissance

1. Responsive Access Points
2. Sniffing
3. Undetectable

Phase 2 – Attack & Penetration

1. Bypass or Attack security controls

Phase 3 – Client Side Attacks

1. Supplicant Attack
2. Capture and Crack Credentials

Phase 4 – Entering the Network

1. Hosts Identified
2. Network Size Determined

Phase 5 – Vulnerability Assessment

1. Manual and Automated

Phase 6 – Exploitation & Data Capture

1. Penetrate Compromise
2. Data Analysis