WiFi Penetration Test Checklist

Prepared By:

James Shank

Potential Required Tools

- **aircrack-ng suite** - Tools for monitoring and cracking WiFi networks.
- **hcxtools** - For capturing and converting PMKID hashes.
- **Wireshark** - For capturing and analyzing network traffic.
- **sslstrip** - For redirecting HTTP traffic to HTTPS and capturing credentials.
- **ettercap** - For performing man-in-the-middle attacks on networks.
- **reaver** - For exploiting WPS vulnerabilities on WiFi networks.
- **hashcat** - For cracking hashes efficiently using GPU acceleration.
- **Kismet** - For wireless network detection, sniffing, and intrusion detection.
- **macchanger** - For changing the MAC address of a network interface.
- **nmap** - For network discovery and security auditing.
- **airbase-ng** - For setting up fake access points.
- **tcpdump** - For capturing network packets.
- **cowpatty** - For cracking WPA/WPA2 handshakes using dictionary attacks.
- **wpscrack** - For cracking WPS PINs.

Configuration:

- [ ] View network interface configurations
- [ ] Turn the network interface on/off
- [ ] Restart the network manager
- [ ] Check and set WLAN regulatory domain
- [ ] Adjust wireless interface power

Monitoring:

- [ ] Set wireless interface to monitoring mode
- [ ] Set wireless interface to specific channel in monitoring mode
- [ ] Kill interfering services
- [ ] Set wireless interface back to managed mode
- [ ] Search for WiFi networks in range
- [ ] Install reaver/wash on WiFi Pineapple (not necessary as this is remote)
- [ ] Monitor the network for handshakes/requests

Cracking:

- WPA/WPA2 Handshake:
    - [ ] Monitor network to capture handshake
    - [ ] Deauthenticate clients if necessary
    - [ ] Start dictionary attack against the captured handshake
- PMKID Attack:
    - [ ] Capture PMKID hashes for nearby networks
    - [ ] Extract PMKID hashes from PCAP file
    - [ ] Start dictionary attack against PMKID hashes
- ARP Request Replay Attack:
    - [ ] Conduct fake authentication to WiFi network
    - [ ] Monitor captured IVs
    - [ ] Start standard ARP request replay attack
    - [ ] Crack the WEP authentication
- HITRE Attack:
    - [ ] Set up fake access point for client targets

Network Segmentation and Isolation Checks:

- [ ] Guest Network Isolation, and no unintended access to internal resources

- [ ] Client-to-Client communication is disabled in Guest network
- [ ] Check for VLANs to separate WiFi traffic by department, user roles, or type

Encryption and Authentication:

- [ ] Verify WPA3 encryption where supported, WPA2 minimum
- [ ] WPA2/3-Enterprise mode with RADIUS authentication
- [ ] SSID visibility

Access Control and User Management:

- [ ] MAC Address Filtering for small or high-risk areas
- [ ] Access Control Policies in place to limit authorized devices
- [ ] Guest Access Policies are in place

Monitoring and Intrusion Detection:

- [ ] WIDS/WIPS presence
- [ ] Log Review Procedures

Rogue Access Point Detection:

- [ ] Site Surveys completed to detect unauthorized APs
- [ ] Automated tool usage for detection and alerts

Firmware and Software Patching:

- [ ] AP firmware update
- [ ] Patching Policies

Logging and IR:

- [ ] Centralized Logging
- [ ] IR Procedures for WiFi-related incidents

References:

WiFi Pentesting Guide
https://github.com/ricardojoserf/wifi-pentesting-guide

Wireless Penetration Testing Checklist
https://gbhackers.com/wireless-penetration-testing-checklist-a-detailed-cheat-sheet/

WiFi Penetration Testing Cheat Sheet
https://github.com/ivan-sincek/wifi-penetration-testing-cheat-sheet

NIST Technical Guide to Information Security Testing and Assessment
https://csrc.nist.gov/pubs/sp/800/115/final