Wireless Penetration Test

Information Gathering

☐ Perform a full site walkthrough while collecting general info.

put interface into monitor mode sudo airmon-ng start wlan0

Write info to log file

airodump-ng --write wifi-walkthrough --wps --band abg wlan0mon

☐ Manually review the airodump output, looking for:

- ☐ A/V equipment broadcasting open or vendor-default networks.
- ☐ Unofficial APs connected to the corporate network.
- ☐ Client authentication attempts (who to evil-AP)

WPA2-PSK Stuff

☐ Grab the handshake and crack it.

☐ If cracked, carry out evil-AP / client-side attacks.

WPA2-Enterprise Stuff

☐ airgeddon automates basic username enum and hash theft for enterprise networks.

- ☐ Physically walk through all office areas while conducting attacks.
- ☐ Find areas where employees congregate that are out of range of the corporate APs and try attacks there (lobbys, cafe, etc)

Open, Guest-Portal Stuff

☐ Check for network isolation:

- ☐ ip neigh
- ☐ netdiscover
- ☐ nmap
- ☐ masscan

- ☐ Responder.
- ☐ Evil-AP, force challenge-response with a captive portal.
- ☐ Try to find the admin portal URL. It may be on the same domain name as the captive portal.
  - ☐ Log in with default creds.
  - ☐ See if it allows you to admin the non-guest networks.

Additional Client-Side Attacks

- ☐ EAPHammer

Web Application Pentest

Technology Stack Enumeration

☐ Wappalyzer helps with basic enumeration.

- ☐ Don't forget to disable extension when done reviewing!

Follow a Testing Methodology

☐ OWASP Testing Guide

☐ Web Application Hacker's Handbook Checklist summarized by jhaddix.