

Wi-Fi vulnerability assessment checklist

Lisa Phifer, Core Competence Inc.

Vulnerability assessments can help you find and fix WLAN weaknesses before attackers take advantage of them. But where do you start? What should you look for? Have you covered all the bases? This checklist will help to answer these questions.

1. Discover nearby wireless devices

You can't assess your WLAN's vulnerabilities if you don't know what's out there. Start by searching for wireless devices in and around your office, creating a foundation for subsequent steps.

- ❑ Which channels have active traffic in the 2.4 GHz band?
- ❑ Which channels have active traffic in the 5 GHz band?
- ❑ Are there sources of non-802.11 interference in these frequency bands?
- ❑ For each discovered 802.11 access point, document
 - Media Access Control (MAC) address
 - Extended service set identifier (ESSID)
 - Channel
 - Average/Peak signal-to-noise ratio (SNR)
 - Beaconed security parameters (i.e., WEP, TKIP or AES-CCMP)
 - Approximate location and probable owner
- ❑ For each discovered 802.11 station, document
 - MAC address
 - Associated ESSIDs
 - Associated AP(s) or peer station(s)
 - Average/Peak SNR
 - If visible, 802.1X identity
 - Approximate location and probable owner

2. Investigate rogue devices

For non-802.11 sources of interference (e.g., microwave ovens, Bluetooth, cordless phones), a spectrum analyzer can help you fingerprint the source. For 802.11 devices, compare survey results to your existing inventory to isolate unknown devices that require further investigation. Note that looking for activity in bands and channels that you don't normally use can help you spot devices trying to evade detection. To learn more about how to investigate these "rogue" devices and the risks they may pose to your WLAN, please read our related tip, [Recipe for rogue hunting](#). [\[link to tip please\]](#)

3. Test your own access points

Next, turn your attention to your own WLAN resources, starting with the APs that deliver wireless services to your users. Those APs are located in a network that may contain both trusted and untrusted devices. As such, they should be subjected to the same penetration tests that you run against perimeter firewalls and access routers that face the Internet. Questions that you should try to answer about each AP include the following:

- Is the AP running the latest firmware and security patches?
- Has the factory default ESSID been changed?
- Has the default administrative login/password been changed?
- Is the administrative password easily cracked?
- Are stronger authentication options available (e.g., private keys)?
- Are there any unnecessary ports open (e.g., telnet, http, snmp, tftp)?
- Are those open ports vulnerable to known exploits?
- Are encrypted administrative interfaces available (e.g., ssh, https)?
- Have security alerts or logs been enabled (e.g., syslog, traps)?
- Have filters been used to prevent unauthorized protocols (e.g., ARP, RIP, SNMP, NetBIOS) from propagating through the AP into the wired network?
- Are filters available/used to block user-to-user wireless?
- Is the AP using the right ESSID and channel?
- Are its security parameters consistent with defined policy?
- If the AP is using WEP, how long does it take you to crack the key?
- Is the AP emitting any known weak initialization vectors (IVs)?
- If the AP is using a PreShared Key (PSK), is it easily cracked?
- If the AP is not using WPA2, are WPA2 upgrades available?
- Can the AP withstand simulated 802.11 DoS attacks (e.g., Authenticate floods)?

4. Test your own stations

Some stations may not have been active during your survey, so make sure to hit every 802.11-capable device on your asset inventory, including laptops, desktops, PDAs, VoIP handsets, printers, scanners and headsets. You may want to "ping scan" wireless subnets to locate stealth devices that eluded earlier detection. Then, try to answer the following questions about each wireless station that you own:

- Is the station running the latest OS and application security patches?
- Is boot or OS authentication used to prevent lost/stolen/unintended use?
- Are current antivirus and antispyware programs running?
- Is the wireless interface protected by a personal firewall?
- Are there unnecessary ports open (e.g., netbios-ns/ssn, microsoft-ds, ssdp)?
- Are there unnecessary protocols bound to wireless (e.g., file/printer sharing)?
- Are potential wireless intrusions (e.g., blocked sessions) being logged?
- Is the wireless client willing to associate to ANY network? ANY Ad Hoc?
- Is the client automatically re-associating with home or hotspot SSIDs?
- Are there wireless user credentials (e.g., passwords) saved on disk?
- Is the station scanning the right bands and using the right ESSID(s)?
- Are its security parameters consistent with defined policy?
- Is the station emitting any known weak IVs?
- If the station is using 802.1X, is its identity visible?
- If using 802.1X, is it using a vulnerable EAP type (e.g., LEAP)?
- If using 802.1X, is it checking the server's certificate?
- If not using WPA2, are WPA2 upgrades available?
- If a VPN client is used over wireless, is it configured properly?

5. Test your WLAN infrastructure

Finally, assess the security of any network infrastructure devices that participate in your wireless subnet, including wireless switches, firewalls, VPN gateways, DNS servers, DHCP servers, RADIUS servers, Web servers running captive portal login pages and managed Ethernet switches.

Like your APs, all of these devices should be subject to the same penetration tests normally run against Internet-facing servers. For example, captive portals should be subject to tests normally run against a DMZ Web server, including tests designed to assess that program/version for known vulnerabilities that may need to be patched.

Most infrastructure tests are not specific to wireless, but additional tests may be appropriate for 802.1X infrastructure. For example, you may wish to test your RADIUS server's ability to gracefully reject badly-formed EAP messages, including bad EAP lengths and EAP-of-death.

6. Apply your test results

Unfortunately, no checklist can help you with this final step. It's time to review your test results and assess the vulnerabilities you may have uncovered. Eliminate vulnerabilities where possible, and narrow the window of opportunity for exploiting the rest. For example, if you found Telnet on your APs, decide whether and how to disable that service. Can you use SSH instead of Telnet to administer your APs? Can you restrict SSH to Ethernet so the daemon can't be probed over wireless?

Once you've applied fixes, repeat tests to verify the result is now what you expected. Ideally, vulnerability assessments should be repeated at regular intervals to detect and assess new wireless devices and configuration changes. Also look for opportunities to automate your tests, making them faster, more consistent and more rigorous.