Wireless Scanning Resources

NIST has two guides that describe good practices for securing wireless networks:

- "Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i"

  (http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-97.pdf)
- "Guide to Securing Legacy IEEE 802.11 Wireless Networks"

  (http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf)

Two books that might be useful to assessors conducting wireless network scans:

- Kali Linux Wireless Penetration Testing: Beginner's Guide

  (https://www.packtpub.com/networking-and-servers/kali-linux-wireless-penetration-testing-beginners-guide)
- Mastering Wireless Penetration Testing for Highly Secured Environments

  (https://www.packtpub.com/networking-and-servers/advanced-wireless-penetration-testing-highly-secured-environments)

Some free wireless scanning applications:

- iStumbler (for Macs)

  (https://istumbler.net/)
- Xirrus Wi-Fi Inspector

  (https://www.xirrus.com/inspector/)
- Vistumbler

  (https://www.vistumbler.net/)
- Kismet

  (http://www.kismetwireless.net/)

Some commercial wireless scanning solutions:

- InSSIDer Office from MetaGeek

  (http://www.metageek.com/products/inssider/)
- AirMagnet WiFi Analyzer PRO from NETSCOUT

  (http://enterprise.netscout.com/enterprise-network/wireless-network/AirMagnet-WiFi-Analyzer)
- SILICA from Immunity

  (http://www.immunityinc.com/products/silica/index.html)