

Wireless Network

SECURITY AUDIT

Is your wireless network broadcasting your company's confidential data to the world? Are unauthorized users using your bandwidth?

Today's wireless networks offer users flexibility and convenience. Without careful security planning, encryption and frequent auditing, however, unauthorized users can view private data, link to network resources, carry out Trojan attacks, or steal your company's bandwidth.

Secure Enterprise Computing's **Wireless Network Security Audit** will assess your company's wireless network to discern its current security posture, then provide recommendations and assistance to secure your confidential information and protect your firm from outside attacks.

Methodology

Our experienced security engineers will work with your IT department staff to identify any Wi-Fi network access points within your building, as well as any "hidden" or "closed" access points (signals which do not broadcast their SSID). Our report will also list wireless equipment that employees may have installed without IT's knowledge.

Equipment used to perform this audit will be protected by a firewall to ensure that there will be no network connections or data transfer during the audit. Our methodology includes discovery and assessment of:

- Network inventory
 - Site survey
 - Inventory hardware
- Rogue deployments
 - Rogue and fake access points
 - WLAN stations
 - Ad hoc networks
 - Reconnaissance activity

- Vulnerability assessment
 - Usage of WEP or Extensible Authentication Protocols (EAP, LEAP, PEAP, EAP-TLS)
 - SSID broadcast
 - High / Low signal strengths
- Monitoring and Defense mechanisms
- Passive Analysis – protocol mapping

The following information will be noted for each network device found:

- SSID
- Wireless Encryption Protocol (WEP) settings
- MAC address
- Broadcast channel
- Equipment manufacturer(s)
- Abnormal signal strength or noise levels
- Configuration settings that may expose your network to risk.

Using the information uncovered in the audit, SEC's engineers will make recommendations and assist your IT personnel in making changes to your wireless network settings to improve your company's security.

SEC recommends that your company periodically repeat this audit to ensure security settings have not been changed, and that no "unexpected" equipment is bypassing your company's firewall.