



Wireless Network Assurance

Security-Assessment.com approaches the scanning of Wireless networks in three different ways depending on the needs of the organisation. In most cases a simple snap-shot of the environment, repeated at regular intervals is a cost effective way to monitor airspace with a corporate campus. In a more data sensitive organization, an extended survey of the airspace will capture all activity over a set period of time.

- **Walkthrough / Snapshot**

Includes a walk-through and sweep of the office(s) scanning for any wireless access points, devices and networks within range. The scan and consulting with the client will identify any client owned or external wireless devices/networks. All suspicious, poorly configured and client owned devices will be traced to the source. Intrusion testing of the devices is available on completion of the scan if required.

- **Extended Survey**

The survey includes installation of Wireless network sensors to monitor the airspace for a period of time. Trend analysis of the use of Wireless networking is captured and analysed. The wireless survey includes: rogue AP management, wireless intrusion detection, continuous Vulnerability Assessment and Policy Monitoring. Intrusion testing of the devices is available on completion of the scan if required.

- **Network scanning**

Includes use of the QualysGuard Vulnerability Management service to map and identify any wireless access points currently attached to the network. Mapping the network up to twice daily over a period of time to discover the addition of any Wireless access points connected to the client LAN

Our Standard Methodology:

While wireless testing has come under a lot of scrutiny recently, the basic elements of the tests have been available for years. The major difference that has changed is the amount of the technology used for wireless audits. Our wireless auditing can cover the following:

- Electromagnetic Radiation (EMR) Testing
- 802.11 Wireless Networks Testing
- Bluetooth Networks Testing
- Wireless Input Device Testing
- Wireless Handheld Testing

- Cordless Communications Testing
- Wireless Surveillance Device Testing
- Wireless Transaction Device Testing
- RFID Testing
- Infrared Testing

The majority of the work today is for 802.11 and Bluetooth network scanning. For each of these tests we follow the Open Source Security Testing Methodology, utilizing the following steps:

1. **Evaluate Business Needs, Practices and Policies** – We check known uses of wireless technology and current business policy on its use.
2. **Perform Site Audit** – Utilizing standard passive detection techniques, we perform an audit and baseline of all detectable wireless access points and devices in the surrounding area of the site.
3. **Present Initial Findings** – We present the initial findings to the client, identifying as many devices as possible, this will define a list of devices that must be identified manually.
4. **Trace Potential Unauthorised Network Access Points** – We manually trace and identify all devices that have not been identified.
5. **Intrusion** – If authorization is given, we attempt to gain access to each of the devices identified as being part of the target infrastructure.
6. **Reporting** – For this component of work, the following will be covered: detailed site analysis including all discovered devices, detailed report of vulnerabilities discovered, recommendations for resolving vulnerabilities and also a gap analysis of the targets practice(s) versus current industry best practice.

The Security-Assessment.com team have been involved in wireless auditing for over 5 years and have experience working with a great majority of the different technologies that have evolved in the wireless space.

The tools used for wireless audits are still evolving rapidly and we utilize a set of both commercial and open source tools.

Contact us today on this service or any of our other service offerings.

Web www.security-assessment.com
Email info@security-assessment.com
Phone NZ +64 9 302 5093
Phone AUS +61 2 9570 2439

Most advanced industry solutions

Highly specialised service capability

Going beyond the audit process to provide practical solutions to real issues

Address environmental change in your business

Be proactive in managing security issues.

