



## What Is It?

A **Wireless Penetration Test** is an evaluation of the *security* of your existing Wi-Fi service.

A penetration test is an in-depth assessment of a system, from the point of view of a would-be attacker. The tester constructs a barrage of tests that seeks to exploit vulnerabilities in the solution or the underlying technology.

The test is conducted by a skilled engineer using special software and/or hardware.

A penetration test is not necessarily a complete evaluation of the security posture of your solution, however it may be a crucial step in safeguarding your data and your network.

*Note: If you require a comprehensive evaluation of your entire solution, including from a performance and requirements perspective, please consider our Wireless Audit offering.*



## Do I Need One?

There are several reasons to conduct a penetration test on a wireless solution. For example:

- To eliminate or report on critical vulnerabilities in your environment
- To evaluate the risk and impact of security vulnerabilities in order to prioritise future work
- To comply with an industry standard or to achieve accreditation
- In response to a security incident in your organisation



If any of these situations apply, then a **Wireless Penetration Test** is something you should consider.

## What Will I Gain?

A penetration test should at a minimum:

- Confirm or deny whether you are protected from all *known* exploits applicable to your system
- Provide concrete evidence of that protection or lack of it
- List discovered vulnerabilities, including their risk and impact
- Recommend remediation steps

A thorough assessment may, in addition, provide the following:

- Indicate areas where best security practice has not been followed
- Highlight *potential* areas of vulnerability in your system
- Rate the overall level of security risk found in the system



## What is different about securing Wireless networks?

Wireless is somewhat different from traditional wired networking environments in that a would-be attacker does not require physical access to your premises or your equipment to launch an attack.

Wireless signals by their nature travel long distances. With a suitably powerful receiver/transmitter an attacker can exploit vulnerabilities in your site without ever setting foot near it.

These facts can make a Penetration Test *more critical* for wireless networks than for traditional wired networks – since physical security is never sufficient.

Further, a Wi-Fi services employ a complex but varied set of technologies, usually involving many different vendors & systems all working together. For example, identity, authentication and access layer systems are often different products from different vendors.

There are therefore many different opportunities to exploit the system in an enterprise wireless solution.



## Our Process

We adopt a 4-phase approach to penetration testing.

This approach has been applied and refined over the course of many small to very large Wi-Fi solutions with great result for you, the customer:

1. **Scope**
2. **Plan**
3. **Execute**
4. **Report**



### Phase 1: Scope

It is important to scope the work for your particular systems and solution. This ensures only relevant tests are performed and reported on. We also determine how and where the tests will be performed, and what pre-requisite information and equipment is needed to perform the tests. This phase takes place through a discovery process with the customer.

### Phase 2: Plan

The suite of tests is planned. A methodology for each test is determined.

### Phase 3: Execute

The tests are performed onsite.

### Phase 4: Report

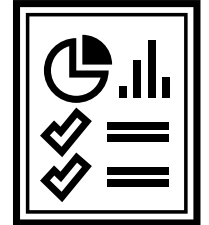
The results of the tests are reported on and analysed. Remediation steps are recommended.



## What Is Included?

Your comprehensive Wireless Penetration Testing Report will include:

- Executive Summary
- Technical Summary
- Details of Test Suite
- Detailed Technical Findings, including:
  - Risk
  - Impact
  - Recommended Remediation
- for each discovered vulnerability



## About Airxperts

Airxperts is an Australian company specialising in Information Technology Consulting in the networking and mobility spaces.

We have been operating successfully for over 4 years and served many large corporate and government customers. In that time, we have developed a reputation for our technical expertise & high-quality work.

We are lean and focused, but well-equipped to tackle large projects, with proven results in the University and Defence spaces, for example.

To enquire about our **Wireless Penetration Test** service, please contact:

Airxperts

[www.airxperts.net](http://www.airxperts.net)

[enquiries@airxperts.net](mailto:enquiries@airxperts.net)

+61 2 6116 8277

