Penetration Testing Data Sheet

How effective is your current security system against a real-world targeted attack? Even with the most advanced cyber-security protection technologies in place, it's the unseen, 'blind-spot' vulnerabilities that can expose your business.

One of the most important tools that companies can use to defend themselves from cyber-attacks is that of penetration testing.

DID YOU KNOW?

Malicious or criminal attacks cause the most data breaches in Australia (50%) followed by human error (25%) and system glitches (25%). Source: Ponemon Institute 2018

What is a penetration test?

A penetration test (also known as a *pen test*) is an authorised hacking attempt that simulates real-world attack techniques used by a criminal hacker.

This service tests any web-exposed elements of your networking including:

- IP addresses
- Websites
- Applications
- Infrastructure

The typical issues detected in a penetration test include:

- ✓ Ports opened
- ✓ Vulnerability of systems to known exploits
- ✓ Misconfigured devices
- ✓ Devices left with default settings
- ✓ Unpatched systems
- ✓ Use of weak passwords
- ✓ Use of weak encryption
- ✓ Use of weak authentication mechanism
- ✓ Ability of systems to respond, react and alert on threats
- ✓ Users exposure to social engineering
- ✓ Adequacy of internal company processes (i.e. no user exit processes, no minimum password complexity)

You will be provided with recommendations on how to fix these issues. If you need help to implement any changes, Huon IT's security experts are on-hand to help your team.

Why get a penetration test?

Even the smartest technologies fall prey to the continually evolving nature of cybercrime and the growing intelligence of attacks.

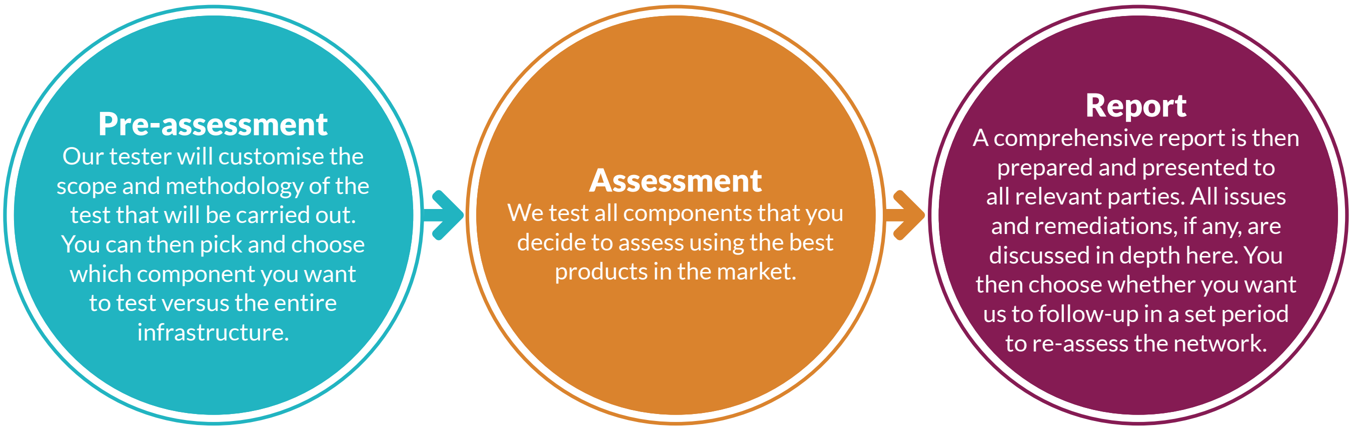
Often the gaps and vulnerabilities occur due to factors like a simple misconfiguration of systems or staff unwittingly exposing you to attack with the click of a link.

Here are some of the benefits to your organisation:

- Reduce your risk of financial, operational and reputational losses caused by a cyber-attack. According to IBM (2018), the average cost of a data breach is close to $4 million.
- It will help your business comply with Australia's data breach laws.
- You will proactively improve your organisation's IT systems against malicious attacks.
- Your business may be able to detect vulnerabilities which automated software scanning can't.

Our process

The penetration testing process typically involves:



Pre-assessment
Our tester will customise the scope and methodology of the test that will be carried out. You can then pick and choose which component you want to test versus the entire infrastructure.

Assessment
We test all components that you decide to assess using the best products in the market.

Report
A comprehensive report is then prepared and presented to all relevant parties. All issues and remediations, if any, are discussed in depth here. You then choose whether you want us to follow-up in a set period to re-assess the network.

How often should you conduct penetration testing?

It's recommended that your organisation conducts a penetration test approximately every 6-12 months, or when you make modifications to your network infrastructure. Ongoing testing is most effective.

Why Huon IT?

Our team includes highly skilled penetration testers who are certified and carry out testing in a safe and ethical manner.

LET'S CONNECT

Contact us today to find out how Huon IT's security experts can help your business.

SYDNEY – MELBOURNE
P: 1300 HUON IT (4866 48)
E: info@huonit.com.au
www.huonit.com.au

huonit
A KYOCERA GROUP COMPANY