Penetration Testing

The increased frequency of high profile exploits reflects a continuous evolution of hacking techniques and an increased level of funding to compromise valuable information.

A Penetration Test provides the highest level of assurance that your IT systems and applications are not vulnerable to these security threats.

Benefits to Executive Management:

- Independently verify your organisation's security posture and processes.
- Reduce risk and incorporate Information Security into your organisation's overall risk management policy.
- Align information security with business goals. Security management continues to gain a foothold in the domain of executive management, not just the IT team. In 2014, the CEO of Target resigned due to a data breach fallout.
- Avoid the high costs, legal ramifications and damage to reputation that can result from information loss.
- Leverage good security practices as a competitive advantage with high profile breaches increasingly attracting public awareness.
- Ensure compliance with PCI DSS and other security standards.
- Incorporate business objectives into your overall security program.

Benefits to Internal Security Team:

- Harden your organisation's IT Systems against malicious attacks through a proactive approach that focuses on prevention not the cure.
- Leverage Shearwater's decade spanning expertise across enterprise and government security projects.
- Access Shearwater's comprehensive security report packed with prioritised actionable recommendations.
- Validate security measures and processes against industry best practices.
- Reduce time and costs associated with managing false positives produced by automated scans.
- Gain independent verification of systems and configurations before they go live on your network.
- Provide management with a proof of exploit, which outlines the assets that an attack can compromise.
- Validate expenditure on IT Security, demonstrate ROI of existing security tools and procedures, and facilitate management approval of required security measures.

Scope of the Service

Shearwater Ethical Hacking (SEH) has the expertise to test organisations'extended IT perimeters. Our Penetration Testing service covers Networks, Mobile Devices, Phishing, Applications and PCI DSS.

Networks

Networks are a lucrative target for cyber hackers. A Network Penetration Test examines the security stance and procedures around network assets such as:

External and Internal Facing Servers
Firewalls, Routers, and Switches
Remote Access and VPN
Wireless Access Points

Mobile Devices

This type of testing is an authorised attempt to bypass authentication on mobile devices including laptops, tablets and smartphones. The purpose is to assess if attackers can compromise stolen or lost devices and use them as a pivot to compromise an organisation's critical information. This test can also assess third party MDM implementations and devices configured with MDM policies.

Phishing

Shearwater's Phishing Penetration Testing is an authorised and simulated process of testing end users susceptibility to conduct attacker requested actions. This is often conducted via email phishing attacks or similar means. Shearwater's goal is to provide organisations with detailed information regarding the cyber risk to their email infrastructure, end user and Standard Operating Environment (SOE).

Applications

Our Application Penetration Testing provides the highest level of assurance that an application is secure. We can also scan applications for vulnerabilities all through the development process and provide guidance for developers on best security practices. Our penetration testing covers mobile and web applications, and web services.

PCI DSS

Shearwater's PCI Penetration Testing takes the complexity out of PCI requirements relating to vulnerability assessment and penetration testing. We will guide you through any complex scoping issues to ensure you achieve, maintain and prove compliance.

Shearwater: The Gold Standard in Penetration Testing

Transparent Approach

A valuable attribute to our clients is the level of interaction and communication we provide during engagement. We provide information in advance about our testing steps and are also readily available to answer any questions or concerns.

Comprehensive

We manually validate automated findings and eliminate false positives. We also look for vulnerabilities that automated tools are unable to find, such as business logic flaws.

Responsive

We listen to our clients to understand their goals. Our team also alerts security staff – in real time – to critical vulnerabilities and threats discovered.

Professional

Our testing is non-disruptive and the risk of a system downtime is minimal.

Post Engagement Follow-up

Our post engagement follow-up is an additional benefit that allows clients to engage us with questions, or seek guidance on issues referred to in our penetration testing report.

Comprehensive Reporting

Shearwater Ethical Hacking offers in-depth executive level reporting which serves as a risk minimisation tool for management, and a technical document – listing vulnerabilities prioritised according to risk level – for the internal security team. The report also provides private enterprise and government with access to mitigation strategies based on Shearwater's key insights into the cyber-threat landscape.

Penetration Testing Standards we follow:

The Open Web Application Security Project (OWASP)
The National Institute of Standards and Technology (NIST)
Open Source Security Testing Methodology Manual (OSSTMM)
Penetration Testing and Execution Standard (PTES)
Penetration Testing Framework
Australian Government Security Policies and Guidelines

Our Certifications

About Shearwater

Shearwater is a specialist Information Security service provider. Since 2003, the company has secured the technology and flow of information that have enabled millions of transactions across government organisations and private enterprise.

Shearwater's expertise and non-negotiable focus on the Information Security space has put it at the forefront of security education, penetration testing, operational security management and threat Intelligence. The company also enables organisations to implement rigorous security policies and helps them achieve, maintain and prove compliance with security standards.

Shearwater provides one of the most comprehensive security reports in Australia. Its Executive Level reporting highlights to businesses the risks associated with the security of their information, whilst also providing actionable recommendations to the internal security team. The company prides itself on its client communication, customer service, fast response, and on-time delivery. Learn more at www.shearwater.com.au.

Whatever your Information Security challenge, we're here to help you find the right solution.

Get in touch
1300 228 872
shearwater.com.au