Penetration Testing Consumer Guide

The challenge of finding the right penetration tester

As an organisation that handles sensitive information, penetration testing is key to ensuring you have a secure environment, preventing your information from falling into the wrong hands.

But the penetration testing industry can be a complex and unknown art as there are many organisations out there that call themselves "professional" without any basis to that claim. Yet these are the people you rely on to interrogate your business systems, and use very complex tools to bombard your network. If they lack the right knowledge and experience on how to use the tools properly, you are likely to waste a significant sum of money. Even worse, they can damage, change, or takedown critical components if their tools are not configured specifically for your environment. Unfortunately, a quick Google search can't tell you who the great and equitable penetration testers are versus the ones you would never, ever want to use.

So, how do you identify and select a reliable partner for penetration testing? This guide outlines the 10 most important traits you should seek from a penetration tester to ensure that the identified risk to your organisation is accurate and meaningful, allowing you to be proactive in reducing the risks of cyber-attack.

10 traits of a reliable penetration testing partner

1 Conducts a penetration test

Unfortunately, some of the lower-priced and lower-skilled organisations sell you penetration testing, but in reality only conduct a vulnerability assessment. And, when compared to a proper penetration test, the results to your company will be substandard. To truly understand the risks your organisation faces, the penetration testers must actively try and exploit identified vulnerabilities, and flaws in your business logic, and not just use an automated vulnerability scanner.

2 Price is a factor

When it comes to penetration testing, you get what you pay for. We don't necessarily recommend you select the most expensive penetration testing company out there, but you should be careful and ensure the company is dedicated to spending time to learn and understand your environment, and your needs. This will help you get the best possible value for the amount you pay.

3 Dedicated penetration testers

There are many companies for whom penetration testing is not a core offering, but just a value-added service. However, being at the forefront of the security industry is paramount in penetration testing, and maintaining this position requires a daily dose of penetration testing and security research. It could easily be argued that a penetration tester without this exposure, and dedication, may not be aware of many attack vectors that the cyber criminals are currently deploying.

Did you know?

There is a distinct difference between a penetration test and vulnerability assessment.

A penetration test is a method of evaluating the security of a computer system or network by simulating an attack by a malicious hacker.

A vulnerability assessment, on the other hand, solely identifies publicly disclosed vulnerabilities in a system.

4 Proof of capability

Anybody can run hacking software, and call themselves a penetration tester. It's therefore key to select a capable partner with some proof of competence. A few things to look for are:

- Sample reports to make sure they are professional, thorough, and offer actionable remediation advice;
- Penetration testing certifications such as those from the SANS institute (GPEN, GWAPT), Offensive Security (OSCP, OSCE), or CREST; and Sufficient experience, so they won't set you up with a junior who ends up doing all the work.

Also ask for references from past clients, and find out what they valued about the company.

5 Customised, valuable reports

If a report is not written to a level that you can understand it, or the remediation activities and recommendations are not valid for either your budget or your environment, is it really worth your money? You need a penetration testing company that will provide you with a report that is meaningful and helpful. Be aware of software-driven, canned reports that are often generated through vulnerability assessments (see point #1). Instead, seek a partner that offers customised reports that are relevant for your environment. To do so, read a previous report or sample report from the penetration tester, and check that it's comprehensive and suited to your business goals.

6 Testing happens before an application is moved into production

Ideally, a penetration test for a new application should be conducted during the user acceptance testing phase, and just prior to moving it into production. This will allow a penetration tester to try different attack vectors without the risk of impacting business continuity, and, more importantly, prevent you from commissioning a vulnerable system. But it's never too late to conduct a penetration test, and the test can even be completed post production. A knowledgeable penetration tester will advise this.

7 An existing relationship is not a prerequisite

An existing business relationship shouldn't be a condition for selecting your penetration testing company. System administrators, for example, typically don't make good penetration testers as they've often already closed the holes they know about. Defending against and performing attacks is a completely different mindset and skill. Moreover, how keen would you be to admit that there are gaps in a system you just secured? Don't be afraid to search outside of your existing relationships, and seek a penetration testing expert.

8 No gimmicks

It may sound cool to have a company send out emails to exploit your staff and their PCs, or leave USB drives around your organisation to see who plugs them in. Most of the time, however, this is more gimmick than value. It is important to find an organisation that understands the underlying reason why you're getting a penetration test done, and that the methodologies used get you the best value per dollar spent.

9 Proactive security approach, not just a tick in the box

If there is a requirement for a penetration test, it's probably for a good reason. So, in selecting your penetration testing partner, don't go with a partner that will just help you get the "tick in the box" during an audit. Instead, engage a partner with a proactive security approach as this will deliver better, long-term results.

10 Scoping exercise

If there is a requirement for a penetration test, it's probably for a good Any penetration testing company worth their salt will conduct a thorough scoping exercise to flesh out your goals and objectives, as well as properly ascertain the size and breadth of the assessment. A common practice is for clients to request a black box (testing without prior knowledge) test. While in some cases this is beneficial, it usually ends up costing you a lot more money for less value. An ethical penetration testing company will guide you to get the most value out of your penetration test.

Did you know?

Penetration testing is a key component to securing your IT environment. Moreover, different compliance standards require different methods of penetration testing at varying intervals. In short, you need a penetration testing company to identify all your cyber security issues, prioritise them, and give you actionable and precise steps to remediate each issue discovered.

Did you know?

It's important for a penetration tester to have a structured approach that meets your requirements and timeframes. Each penetration test should be treated as a journey, and not as a one-off test. And, each stage of a penetration test should fit neatly together to form a complete project, and because of this it should be managed as such.

Did you know?

A penetration testing firm should work with you from build-up, where detailed requirements are defined, all the way to close-down, at which point you should have a clear path and understand the next steps you need to take to meet your business requirements.

Questions to ask a potential penetration tester

So, how do you find out if your potential penetration tester fits the bill? Don't be afraid to ask them a few tough questions before they start testing your systems:

- Are you certified to conduct the penetration test to a standard that will meet my compliance requirements?
- Does your company have a dedicated penetration testing team?
- Will you complete a scoping exercise in advance of the penetration test?
- What experience and qualifications do your penetration testers have?
- Do you use commercial software, or only open source software?
- Can you explain in detail your penetration testing methodology, and how it is different to a vulnerability scan?
- Will your report rank each finding and be specific to our organisation, and do you provide recommendations that are applicable and achievable for our environment?
- Does your company perform close down meetings where the findings are explained for both business and technical audiences?
- Can you provide any references?

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)
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