THE BUYER'S GUIDE TO PENETRATION TESTING SERVICES

Best practice when procuring penetration testing

chess®

The Buyer's Guide to Penetration Testing

Choosing a 3rd party organisation to conduct a penetration test can be a complex process. You need to know the right questions to ask, and how to interpret the answers to make the right choice for your business

With penetration testing (or pen testing as we'll call it throughout this document), issues such as trust, expertise, experience, professionalism, accreditation and honesty all come into play during the evaluation and purchase decision making process.

When selecting a provider to conduct your penetration testing – a provider that will effectively try and break into your network and gain access to your more sensitive systems – your decision must be made from a position of assured knowledge, not 'hope for the best'.

You need to know, or at least have a good understanding of, what will be covered in the test, how it will be carried out, what the nature of the findings might be, what kind of data might be accessed and what steps might be needed as a result.

In this Buyer's Guide to Penetration Testing our aim is to give you enough knowledge about what to look for in a potential pen test provider, along with a set of questions you can ask to help you make an informed decision.

The Importance of Penetration Testing

Penetration testing falls under the broad heading of "security assessment" along with a large number of other terms and buzzwords including ethical hacking, vulnerability testing and analysis, tiger teaming and attack simulations. For the non-expert, this can give rise to a great deal of confusion as to whether they actually need a penetration test, or something else.

It's such an important discipline that a certification body called CREST exists, firstly (and helpfully) to define what penetration testing actually is, and secondly to accredit providers of penetration testing (and other cybersecurity-related) services.

The CREST accreditation gives buyers confidence that the services they are buying are being provided by companies and individuals with the requisite skills and up-to-date knowledge of the techniques used by hackers.

What Is Penetration Testing?

CREST provides a very useful definition:

> *Penetration testing involves the use of a variety of manual and automated techniques to simulate an attack on an organisation's information security arrangements. It should be conducted by a qualified and independent penetration testing expert, sometimes referred to as an ethical security tester.*
>
> *Penetration testing looks to exploit known vulnerabilities but should also use the expertise of the tester to identify specific weaknesses – unknown vulnerabilities – in an organisation's security arrangements.*

Source: CREST definition of penetration testing

If any vulnerabilities are found, the tester attempts to penetrate further into the network, aiming to access confidential information, files and databases, and seeking to establish whether the network systems can be disrupted in some way.

Before deciding to invest in penetration testing services, most organisations document their requirements, paying attention to the business drivers that underpin the requirement for testing, and from there, the scope of the testing.

For many, penetration testing is necessary because their business activities involve highly sensitive processes (e.g. managing large volumes of sensitive customer data), an increase in cyberattacks noticed across their business sector or among similar types of organisation, or a need for compliance driven by a combination of factors.

Why Is Penetration Testing Needed?

For the reasons mentioned above, senior stakeholders in most organisations need assurances about the security of their networks and systems. Interestingly, this assurance is not restricted only to the external network defences. Another dimension to the threat landscape is 'insider threats' posed by human computing activity, either malicious or unintended, both of which can lead to data breach and security being compromised.

Consequently, they require an objective, documented, technically rigorous assessment of the network's ability to withstand an attack. This assessment process is called penetration testing.

As of 2018, another key reason for penetration testing is the requirement for compliance with article 32 of the GDPR (General Data Protection Regulation) which comes into law on May 25th.

This article requires certain types of organisation to ***"implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including (a process) for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring security."***

- As well as minimising and eliminating the risk of attack and data loss, other reasons for penetration testing include:
- Compliance with regulatory requirements such as PCI DSS and ISO 27001
- Demonstrating due diligence in cybersecurity to stakeholders, including shareholders and staff
- Guarding corporate brand reputation
- Establishment of best security practice
- Highlighting of areas for improvement

What Are the Key Elements of a Penetration Test?

As stated above, penetration testing is key to identifying network security weaknesses and vulnerabilities that could be used to gain unauthorised access. In particular, it's a way of seeing what your network looks like to criminal hackers, or to those inside such as employees with malicious intent.

At the same time, your penetration test will identify areas of compliance weakness. The findings will be instrumental in assessing how effective your organisation would be in responding to and managing the fallout of an attack, as well as acting as a vehicle to enhance your workers' awareness of their personal responsibilities regarding security practice across the organisation.

There are DIY approaches to penetration testing, but the ideal solution is to appoint an objective 3rd party expert to undertake it for you.

The number and nature of key elements involved may vary between different potential providers, depending on their depth of expertise and the thoroughness of the process they use.

In summary, you should be looking to work with a provider that covers at least the following six steps:

1. **Scoping and Planning:** determining the reasons you need a penetration test and documenting the process you are going to use. Understand your drivers and motivations for requiring a penetration test. Is it regulatory compliance? Or the fact that your business holds commercially sensitive intellectual property? Your motivations will influence the scope of your pen test.

2. **Reconnaissance:** researching the network and establishing what details and data can be found. Your pen tester will review and gather information on the system or systems where entry points might exist and how they could be accessed. These will include elements such as employees, IP addresses, email addresses, websites, social media and other network-based systems.

3. **Threat Assessment:** using various tools and techniques to identify potential vulnerabilities, gateways and vectors into the network. Commonly, pen testers use a mix of automated and manual tools to examine attack avenues and find network vulnerabilities.

4. **Exploitation of Vulnerabilities:** attempts to penetrate the network defences and (if in scope) gain of control over a target system. The aim, having first gained access to the network, is to see how far the attack can go, establishing administrative privileges where possible and then using them to effect lateral movement to other systems.

5. **Reporting:** having completed the exploitation phase, the pen tester will create a penetration test report which includes findings on the vulnerabilities discovered, the full extent of access that was gained, detail of systems that were breached, changes (if any) that could be made and a set of recommended remediation actions.

6. **Remediation:** if required, your penetration tester may provide consultancy services to reduce or fix any vulnerabilities found and improve overall security.

It's also worth saying that your pen testing provider will ideally offer a social engineering test, such as a phishing exercise. The human security interface is always a difficult area because internal employees may unwittingly be duped into giving hackers security information or may click on bogus links. Your pen testing provider may also provide security awareness training.

What Should You Look for in a Penetration Test Provider?

Appointing an external provider of penetration testing services is not just about finding a tester who can technically implement a pen testing process. Your chosen provider must be trustworthy, credible and deliver securely on their promises of testing, reporting and remediation, and must have the potential to make decisions and add value throughout the procedure.

It's possible that during the testing process your penetration tester will gain access to confidential and sensitive data. Because of this you are strongly advised to:

- Carry out thorough background checks on the pen testing organisation and its testers/engineers.
- Follow up any references you receive to assure yourself of their track record.
- Interview the pen testing organisation so that you can be comfortable that they have the skills, experience and expertise to test your network defences.
- Find out the precise steps they take if/when they manage to gain access to further systems.
- Use a confidentiality agreement to ensure that your testers will keep any information they uncover or to which they gain access completely confidential.

In summary, you'll need to assure yourself that the penetration testing company you are about to hire is fully trustworthy, has all the required technical capabilities, can demonstrate a strong track record of expertise and has the capability to restore and repair any systems that may be affected during the pen testing process.

To help you further, we've compiled a set of questions for you to ask your penetration testing provider before engaging with them.

Questions to ask your penetration testing company

1

What industry certifications do you have?

When considering companies that might perform your penetration testing, ask them what certifications they have. Certifications you should expect include CREST, OSCP and SANS. Security firms that are CREST approved and/or have CREST certified testers can be considered credible, as they have invested heavily in security testing skills and expertise. Those without such certifications should probably be disregarded.

2

Where are your penetration testers based?

Find out where the people who will do the testing are physically based. Some penetration testing companies outsource their work to testers in countries other than the UK; in such cases it can occasionally be difficult to maintain a documented audit trail. It's down to your personal preference and position, but many UK-based companies prefer to use UK-based engineers with recognised certifications.

3

Can you provide testimonials, references or case studies?

Credibility of your penetration testing company. Ask to see two or three of these, and if possible speak with at least one other customer to find out about their experiences.

4

Can we see your pen testing methodology?

It's not unreasonable to expect that before undertaking a penetration test on your organisation, your 3rd party pen testing provider should provide a copy of their testing methodology. Most penetration tests follow a similar, established methodology, which is designed to be as close as possible to the techniques used by cybercriminals to find and exploit vulnerabilities in your security infrastructure. .

5

What's included in your pen testing service?

You need to know what type of testing your provider can do. At minimum look for internal and external penetration testing, web application testing, patch auditing, password auditing, firewall auditing, phishing assessment and physical security/social engineering.

6

Can you help us scope our pen test?

What assistance can the penetration testing company provide in scoping the tests? They should be more than happy to help you establish the key business drivers for the penetration test, and hence identify the key systems to be tested. The scope of the penetration testing must therefore include efforts to access and, if appropriate, assume control of such systems and potentially to remove or change key data.

7

Is there a manual element to the pen testing?

Most penetration tests incorporate an element of both automated and manual testing. In many ways the manual testing is more important, because only a skilled and experienced human tester can truly imitate the moves of a criminal hacker. Manual testing by an expert penetration tester will result in on-the-fly decisions to leverage vulnerabilities and gain higher levels of access to additional systems via applications, endpoint computers and servers where valuable data may reside.

8

Do you offer social engineering and phishing testing?

While not strictly speaking within the definition of penetration testing, many organisations that offer pen tests are cybersecurity specialists and offer a broader set of security services. Of these, the 'human' security interface is also a major potential vulnerability, and it therefore makes sense to test it.

9

Do you offer cybersecurity awareness training?

Where a pen testing provider does include social engineering testing as part of the process, they may also offer security awareness training as a form of remediation service. It's worth asking, if only because you may want to use the service later. Having this string to their bow may also add to your view of the provider's credibility.

10

How much will the penetration test cost?

Typical 'base' pricing models are built around the number of external IP addresses. More advanced penetration testing will encompass pricing for testing of specific operational systems, undertaking bespoke tests, assessments or audits. They may also involve a specific end goal such as achieving a compliance standard.

11 What guarantees do you offer?

Any penetration testing provider worth its salt will back its services with a guarantee to deliver full satisfaction. That means that if for any reason you are not satisfied with the service provided, they will complete the work to the standard promised or offer a refund.

12 What will be included in my report?

Clearly your penetration test report should detail any threats or vulnerabilities found and recommended remedial actions, ranked in order of importance. The report should be a quality document that helps senior staff understand where a vulnerability has been found, the potential security implications of a breach and what needs to be done to fix the issue. bused to pose a security risk to the organisation.

13 Can you provide sample reports?

Having reviewed the pen testing methodology proposed by your provider, it follows that you would want to see one or two example reports. Of course, you wouldn't expect to see a real report from a real customer – but a sample template or redacted report showing what's covered and what can be expected is a reasonable request. When you review it, be careful to verify that it's a 'like for like' report i.e. a pen test report for the sort of specific test you are having done.

14 Do you provide remediation services?

It's worth asking your potential pen test provider whether they can either offer guidance on remediation of issues, or even better carry out remediation works. Any work they carry out would clearly be contingent on documented evidence in the report of the existence of any issues.

Conclusion

As with virtually every service purchased in the B2B world, the key fact is that you'll 99.99% likely get what you pay for.

Price is not everything however, so we do recommend that you obtain at least three quotes. Just remember that the lower the cost, the less experienced or qualified the tester is likely to be, and the less thorough the testing regime may be.

Note too that your penetration test report may reveal some fascinating results about what you previously thought was water-tight network security. Yet once the report is done, and remediation steps are complete, your pen test becomes a simple 'snapshot in time' of your security situation.

Things can change and become outdated very quickly. So once you start doing pen tests, they should probably be a regular event, ideally annually but based on the specific nature of your systems.

Want more information about penetration testing?

Chess CyberSecurity is one of four specialist divisions within Chess. With over 25 years' experience we protect over 3 million UK business users across Chess' 40,000 customers. Chess CyberSecurity is ISO 27001 accredited and certified by CREST for penetration testing services.