Pen Test 101
Why it should be a key part of your Cyber Security Strategy

We shed light on the world of penetration testing and explain why more companies and organisations see it as a key part of their cyber security strategy

context

contextis.com

E info@contextis.com
T +44 (0)207 537 7515

Pen Test 101
Why it should be a key part of your Cyber Security Strategy

We shed light on the world of penetration testing and explain why more companies and organisations see it as a key part of their cyber security strategy

The main aim of penetration testing is to identify technical vulnerabilities in IT and communications systems that could leave your organisation open to attack – from a disgruntled employee or casual hacker to a state sponsored cybercriminal. Once identified, these weak points can be remediated to strengthen your overall security posture.

A penetration test provides a real-world attack experience by using the same attack vectors and techniques used by cyber criminals to identify vulnerabilities, exposing gaps in security policy and process and ultimately managing risk.

Size doesn't matter

While pen testing is often thought of as being something only large enterprises need, and have the budget for, the truth is that small and medium-sized business are firmly in the cybercrime cross-hairs. In fact, industry research suggests some 60 per cent of attacks are aimed at the SMB sector. When it comes to being targeted, size really doesn't matter: every organisation is at risk. As for budgets, you shouldn't be asking whether you can afford a penetration test but rather whether you can afford to be breached. Breach costs can be financially devastating by the time you've rolled forensic investigations, incident mitigation and reputational damage into the total. More recently, cyber criminals have been looking to directly monetise hacking using ransomware and cryptocurrency mining, while GDPR means that companies can be fined up to 4% of annual turnover if personal data is breached as a result of a compromise.

DIY disasters

With the number of readily available automated vulnerability scanning tools out there, the temptation is to do your own testing. But even if you were just looking to self-assess your security posture there are still plenty of good reasons not to do it alone. The main one comes down to skill sets as the technical knowledge and expertise required to carry out the various aspects of a penetration test are considerable. For example, you may need to perform a web application test, an internal infrastructure test and a Citrix review. Another benefit of using an external provider is what they provide to the organisation in terms of

> "A self-test may not provide a realistic picture, as an internal employee could bring additional access of knowledge about their own infrastructure that could skew test results."

E info@contextis.com
T +44 (0)207 537 7515

exposure. A self-test may not provide a realistic picture, as an internal employee could bring additional access or knowledge about their own infrastructure that could skew test results. The fact that an external provider will be unbiased and independent really cannot be stressed enough.

Manual dexterity

When it comes down to the use of automated vulnerability scanning tools, these actually do have their place and could help an organisation improve its security posture if identified issues are properly remediated. However, a vulnerability scan can only go so far. Anything more complicated than simple scans of infrastructure and web applications can lead to a lot of false positives and false negatives. In addition, any issues will need to be manually reviewed to ensure they are legitimate issues. This can easily become unmanageable, and when you throw in complex systems and applications, it becomes impossible. For example, a simple vulnerability scan will not identify vulnerabilities within business logic or complex multi-stage transactions. Automated scanning has its place but should only be used in conjunction with a more robust and manual penetration test approach.

The small matter of trust

Something that might be of concern, given the nature of the access being handed over to a pen testing team, is the not so small matter of trust. It's vital to ensure that any organisation carrying out penetration testing, and engaging an external company to provide that service, should be satisfied regarding appropriate qualifications. There are numerous certifications out there that can provide a level of assurance that the consultant is appropriately skilled and has the requisite knowledge. The recognised gold standard is CREST-related qualifications such as CREST Registered Tester (CRT), and Crest Certified Tester (CCT), which are technical qualifications that require a high level of knowledge and technical ability to be able to complete. Any external consultants will also require the necessary security clearances - at least Security Check (SC) level - if accessing protectively marked information and assets. These checks will give you a high degree of assurance that your pen testing partners are competent, trustworthy and appropriately skilled.

Legally speaking

From the legal perspective, any company carrying out unauthorised penetration testing could be in contravention of computer misuse, fraud and abuse legislation. A penetration test may also involve access to personal and corporate information that is covered by data protection and privacy laws such as GDPR; so the organisation also needs to ensure that the testing company is handling any data appropriately and securely. Industry standards such as ISO9001, ISO27001, and SOC 2 (USA) are designed to give assurance that any issues can be avoided.

Report and remediate

A successful penetration test does not end after the test has been completed. In order to deliver value to your business it has to assess the impact of any issues found. A properly conducted pen test will result in a comprehensive and focussed report; far more so than any automated process could hope to achieve. This is important, because the success of the testing should be measured less in what has been found and more in how those weaknesses can be addressed.

By providing clarity through detailed reports stating the technical impact and ease of exploitation, you can better understand the risk and be in a better position to implement the most appropriate and proportionate mitigation methods.

With network breach and data loss headlines appearing day-in, day-out, they threat to businesses is not going away. And whereas penetration testing was once seen as something only government departments, major corporations and financial institutions undertook, it is now an essential part of information security strategies for companies of all types and sizes.

E info@contextis.com
T +44 (0)207 537 7515

Pen testing in a changing world

There was a time when we had a network perimeter and everything and everyone sat inside the boundary and was protected by firewalls and a host of other perimeter security technologies. This made the scoping of pen testing a relatively focused exercise. But times and technologies change and the corporate network is no longer defined by a perimeter. It is far more disparate and complex – posing new challenges for CISO and pen testers.

In particular, the maturity of cloud offerings is driving businesses and organisations to shift core functions to the next-generation of IT hosting and application delivery, which has major implications for information security.

Where the cloud infrastructure is managed separately from the deployed applications, the configuration of the underlying operating system is usually not visible to the developer or application owner. Many organisations have adopted a DevOps approach and toolset to managing cloud IT infrastructure with tools such as CloudFoundry, Docker Swarm or Kubernetes. But while these tools bring flexibility and speed, they are also widely understood by attackers.

The configuration of each instance or node is commonly defined from a 'gold' standard build or based on a pre-existing configuration. In some circumstances, this level of abstraction can lead to security weaknesses where application components rely on OS level security controls that are not implemented. The attack surface is also increased by the presence of cloud management tools and internal network services related to management of the infrastructure available from within deployed containers or compute instances, such as a local loopback interface, overlay networks and internal cloud networks.

How do you pen test the cloud?

Traditionally, pen tested systems are denominated by their IP address, DNS or NetBIOS name. In a cloud environment a transient host may only exist for a few weeks, so by the time the pentest report is delivered, the identified vulnerabilities have been moved onto a different system.

Vulnerability scanning and application layer penetration testing is still required, but to establish the root cause problem, the responsible component must be identified, be it a deployed application, shared service or cloud management tool. For example, an application penetration test may identify an internet accessible Kubernetes API service, accessed by modifying the HTTP Host header in requests to the application. This exploit targets vulnerabilities within the reverse proxy. To fix the issue, a change must be made to the deployment scripts rather than the application codebase to ensure the reverse proxy is deployed without the vulnerability in future iterations. This would require those responsible for managing cloud infrastructure to work closely with the application teams.

While the goal posts have shifted, not considering a full penetration testing lifecycle could leave your organisation vulnerable to attacks. A comprehensive penetration testing program will not only provide a point-in-time assessment of security posture but will also help resolve questions such as:

- How much do I have to trust my cloud service provider?
- How is my code and data protected against attacks from the hosting provider, container breakout or other tenants of the same cloud environment?
- If and when one of my apps is compromised, will the attacker be able to traverse the cloud and gain access to other compute nodes / applications / resources in the cloud?
- If the cloud is compromised, will the attacker be able to traverse to my company's internal infrastructure?

E info@contextis.com
T +44 (0)207 537 7515

Defining the scope of an end-to-end penetration test can be difficult with multiple stakeholders and third-parties. This is further compounded where network segregation as well as access automation controls prevent hands-on access to the underlying systems, forcing the pen tester to use alternative streams of communication such as web shells, to gain access to components. Other potential weak points include the connectivity between corporate networks and the cloud and containerisation, which can impact the security of cloud environments. If the cloud and other emerging technologies are to become the de-facto for enterprise computing, penetration testing needs to constantly evolve.

Maximise the value of your penetration test

So, to summarise, here are our top tips to get the most out of your penetration tests and maximise their value:

Define the scope of the test accurately

When planning your penetration test you will need to decide the level and depth of testing you want to conduct. How extensive or comprehensive do you want the test to be? Is it a high-risk system with multiple layers or are you just looking for a single layer to be tested? If the expected range of testing, or scope, is not defined accurately, you may not end up testing everything that needs to be tested which immediately reduces the value of the test.

Provide enough detail of the environment to the testing team

To maximise the value of your penetration test you will want to provide enough detail of your target systems so the penetration testing team can quickly understand the environment and provide useful and accurate results. White box testing provides the tester with knowledge of the internal structure of the system so the penetration testing team can quickly familiarise itself and get straight to identifying security issues.

Make sure you think a system is secure before spending time on a test

It is likely you will already be aware of some of the existing vulnerabilities within a system, make sure to fix these before you start your pen test so you do not waste testing time on issues you already know exist. The test also provides the opportunity to test your remediation of those issues.

Know your objectives

What is the reason you are conducting your penetration test; is it regulatory or to generally improve the security of that system or the overall network? What are you hoping to achieve from the test? Are there any particular concerning threats that you would want addressed? Make sure you have clearly defined and communicated this before the test so the results are meaningful and can be utilised effectively.

Ensure the right people are conducting the test

Penetration tests should be carried out by experienced consultants with the necessary technical skill set and qualifications. They should have strong technical knowledge to ensure you get the best value and most accurate results.

Insist on quality reporting

The report is the only formal output from a penetration test and must clearly explain the threats the business faces from the findings so the level of risk can be determined. It should have sections that concisely explain the issues to executive or board members, sections that explain the vulnerabilities and business impacts to system owners and sections dedicated to helping the technical team understand, re-create and fix the identified problems.

Fix the identified issues and retest

Perhaps most importantly but often not planned for is the remediation of issues found. Build time into the project to fix the issues identified & re-test them to ensure the effectiveness of the fixes. This will also verify that no new problems were introduced by the fixes.

E info@contextis.com
T +44 (0)207 537 7515