DEFENSE.com™

WHITE PAPER

Security first:

What is penetration testing?

Introduction

Penetration testing, also known as pen testing, is a controlled technical exercise that aims to methodically test the security of your IT infrastructure and your employees. Pen testers are security professionals that will use all the tips and tricks available to real-world hackers, to perform a simulated attack on your systems against a pre-defined scope. Pen tests should be considered a fundamental component of your risk management programme, as they are one of the most effective ways to discover your security weaknesses.

The aims of a penetration test include:

- Test your IT infrastructure, applications and workforce
- Protect your organisation and minimise your risk of a cyber attack or data breach
- Highlight your threats, provide remediation advice and offer guidance on how to reduce the impact of the identified vulnerabilities being exploited
- To satisfy your compliance requirements and enhance your reputation with customers and partners

The benefits of penetration testing

Stay a step ahead of the hackers

As the threat landscape is always changing, a penetration test will help measure your organisation's ability to withstand a cyber attack. It will find vulnerabilities across your network, infrastructure and employees before a cybercriminal can.

Protect your business

A security incident can be devastating and can cause irreparable financial damage that also has a negative impact on your brand's reputation. By identifying and remediating the vulnerabilities that a penetration test finds, you will drastically reduce the risk of your organisation being breached.

Remain compliant

To achieve compliance, many industry standards and regulatory obligations require or, at the minimum, recommend regular penetration tests to test the strength of your cyber security. These include PCI DSS, ISO 27001 and HIPAA, amongst many others. Though compliance does not guarantee security, these standards ensure your business has the necessary security measures in place to prevent a cyber attack.

Maintain business continuity

Cyber attacks can destabilise business operations and impact growth. Penetration tests can highlight vulnerabilities that exist within your organisation that could be a point of weakness for hackers to exploit. Regular pen tests will help to proactively find and fix vulnerabilities across your systems to ensure your business remains protected and allow you to maintain business continuity.

Build customer trust

Customer confidence in your services is important for businesses, as cyber attacks can drastically threaten your brand's reputation. With penetration testing, you can assure your customers, clients and partners, that your business is well-protected, that customer data is secure, and that your business is prepared to tackle a cyber incident.

Solid risk management

Each penetration test addresses your business risks and the impact to confidentiality, integrity and the availability of your data. This provides a good indication to management and the technical teams on how to best prioritise, plan, budget and remediate the risks in a structured manner.

> *Penetration tests should be considered a fundamental component of your risk management programme.*

Key considerations

So, you've learnt what penetration testing is, along with its benefits. Before we look into the different types of penetration tests available, there are several factors and limitations to consider.

Scope

A penetration test without a scope will be of little value. Understand what you want to test, your budgets, objectives and any constraints that may limit the effectiveness of a pen test.

Objectives

Understand what you aim to achieve with a penetration test to gain maximum value.

Budgets

Consider your budgets as the scale and complexity of your systems, applications and scope will impact heavily on the type of test you can accommodate.

Test type

There are several types of penetration tests available, so choosing the right one for your business and scope is important.

Provider

Ensure you conduct due diligence when selecting your penetration test provider. Assess a prospective company's certifications, knowledge and skill sets. If in doubt, request a sample pen test report to see what you're signing up to.

> *When it comes to security, is there ever really such a thing as 'too much'?*

Box clever

There are three primary approaches to penetration testing: black box, grey box and white box.

1

BLACK BOX

This is where a penetration test is carried out in a real-world scenario, where little to no prior knowledge of the environment is known to the pen tester. However, a lack of information means black box pen tests are not as efficient as grey or white box exercises. Penetration tests are time-sensitive, therefore pen testers are unable to test areas of your systems and network, searching for vulnerabilities that hackers may spend months on.

2

GREY BOX

A grey box test discloses partial information about the target systems to the penetration testers. This hybrid approach is the most common form of penetration test. Why? Because the pen tester can understand the potential damage that can be done by a hacker with partial knowledge and limited access to its target systems, network or applications. Consider a grey box exercise as the best distribution of time and resources during a penetration test.

3

WHITE BOX

If a black box test says nothing up front, then a white box test tells you everything, including a breakdown of target systems. Although a white box exercise is the most comprehensive, it is also the slowest due to the time taken to assess your organisation's entire infrastructure. Nonetheless, white box tests will help uncover vulnerabilities within a limited timeframe, as testers are given full disclosure of the systems and networks they are testing.

> *Be wary of tests that focus only on the technical infrastructure, as the human element can be just as important.*

How to position your penetration test

Understanding where a potential cyber attack will originate from is crucial to uncovering your security flaws. The main difference between internal and external penetration tests is pinpointing the initial access point of an attack.

External

External-based penetration testing simulates the ability of an attacker to gain access from external resources to the internal network. Or, to retrieve sensitive data from public-facing resources, such as web applications or email servers.

Internal

Internal-based penetration testing simulates an attack that has already bypassed the security perimeter.

This addresses what an attacker, or an insider, can see and what they can do internally, such as moving from one network to another, intercepting internal communications, and so on. An internal-based pen test will model the damage an attacker can do, once they've breached your system.

> *A cybercriminal doesn't care how big or small your organisation is: an easy target is an easy target.*

Test types

There are many different types of penetration test to choose from, depending on which systems and components are being tested. Here are the most common test types you'll encounter – note that testing modern, complex infrastructures may involve a mix of these different test types. Getting the right balance of these test types can be achieved at the scoping stage.

Infrastructure or network

This type of penetration test is designed to test your network and infrastructure for vulnerabilities and the effectiveness of your existing security controls. Pen testers will attempt to identify and exploit security misconfigurations, and assess patch levels and threats, such as open ports and vulnerable devices.

Web application

This is a test of your website's API and web applications for security weaknesses, such as insecure functionality and misconfigurations. Web application pen tests will look for all critical security risks, including the OWASP Top 10.

Mobile application

Penetration testers are able to identify potential threats, vulnerabilities and misconfigurations in iOS and Android applications. This type of test will help to improve the software lifecycle of your mobile applications.

Cloud

Penetration testers will assess and identify security weaknesses within the cloud to evaluate the strength of your cloud's security posture. Cloud pen testing includes exposing weak access controls to your cloud and insecure functionality. Pen testers can assess vulnerabilities within cloud infrastructures, such as Microsoft Azure, Amazon AWS, Google's GCP, and IBM Cloud.

Social engineering

Social engineering is a penetration test of your first line of defence: people. Attack vectors such as phishing, vishing and tailgating, are all examples of online and physical social engineering methods that hackers will use to exploit weaknesses in your employees.

Red team

Red team assessments will provide your business with a comprehensive overview of your security, be it technical, physical or procedural. This type of penetration test enables pen testers to assess and identify your threat detection and response capabilities.

Penetration test methodology

There are 6 phases to our penetration testing that most pen testing companies will follow. Here's our methodology:

1. Defining your scope

By outlining your goals, a pre-defined scope will give you and our penetration testers a clear understanding of the requirements for your pen test. During this stage, timelines and expectations can be set to ensure a smooth and well-controlled exercise.

2. Reconnaissance

This step is where pen testers will gather as much information about your systems as possible. The scoping performed in the previous phase will help increase the efficiency of the recon stage. This intelligence will then be used as attack vectors when attempting to breach your systems during the vulnerability assessment and exploitation phases.

3. Vulnerability analysis

Using the intelligence gathered in the previous step, penetration testers will use the latest tools and expertise to uncover the source of your vulnerabilities.

4. Exploitation

During the exploitation phase, our penetration testers begin their assessment with the aid of the vulnerability analysis. Using a range of customised exploits and techniques, pen testers will scrutinise and test the security of your infrastructure and components to the pre-defined scope. This is where pen testers see how far they can breach your systems and understand the potential damage that could be done by a real-world hacker.

5. Post-exploitation

Here, the penetration tester will determine the value of a compromised target. Questions that will be asked, include:

- How easy was it to gain access into the system or application?
- How much access could an entry point yield?
- The severity of the risks found
- How much damage could the vulnerability cause?
- The likelihood of a vulnerability being exploited
- How long before you detect a breach?

The rules of engagement agreed upon during the scoping stage will determine to what extent a vulnerability can be exploited. During the post-exploitation stage, pen testers will be able to pivot to other systems and networks that have been defined within the scope.

6. Reporting

Each of the above phases must be documented. A good penetration testing company should provide you with a comprehensive and easy-to-read report, that includes the following:

- Details of all the risks found
- Actions taken to exploit each security issue
- Strengths and weaknesses of your overall security posture
- Recommended remediation measures

The reporting stage will give you the opportunity to ask questions and request further information on key aspects of your penetration test.

How to prepare for your Penetration Test

1 Before your test

Before your test begins, make sure you have a recent back up of key systems and data. You should also let the relevant departments within your organisation know when the pen test is being carried out. Depending on the type of test being conducted, we'll require the below information.

2 During the test

During the test itself we'll need contact details of someone we can quickly report critical security weaknesses to. We'll also supply details of the lead penetration tester to ensure the smooth execution of the testing activities.

3 After the test

After the test, you'll need to arrange for resources to be available in order to address the issues raised in the report. The report itself is split into a high-level executive summary and a technical breakdown, and includes helpful remediation advice.

Information required by pen testing team

External Infrastructure
- External URLs & IP addresses

Internal Infrastructure
- Internal URLs & IP addresses
- VPN details, including gateway URL and login credentials

APP
- URL & IP addresses
- Login credentials for all user role levels (authenticated tests only)

Wireless
- SSIDs/APs
- On-site address

API
- API info such as endpoints or requests
- Relevant API documentation
- Sample API requests

Social Engineering Campaigns
- Target employee details, including name, email address & telephone numbers (if appropriate)

Summary

Penetration tests are designed to help you understand your IT environment and ultimately guide your organisation to improving its cyber security. A cybercriminal doesn't care how big or small your organisation is: an easy target is an easy target. Penetration tests are crucial to identifying where your vulnerabilities lie and help you understand how a hacker could potentially exploit those weaknesses to gain a foothold in your systems.

Remember:

- Finding a penetration testing company that you trust is as important as the penetration test itself. It will give you greater peace of mind if you're entrusting your systems with certified pen testing experts.
- A pen test should outline every stage of the process, following a 6-step lifecycle, that concludes with you understanding where your risks lie, how to remediate and minimise your risk.
- Penetration tests should form part of your overall risk management program.
- Finally, always remember that true security is a holistic, overall approach that goes far beyond technical measures. Good security should be a culture within your company, based on a cycle of continuous improvement.

To learn more about how penetration testing can protect your business, or to get started with a test, get in touch today.

+44 (0)1438 500 500 **contact@defense.com** **www.defense.com**

DEFENSE.COM™