**CYB 403: SYSTEM VULNERABILITY ASSESSMENTS AND TESTING**

**Hidden vulnerabilities in an organization’s computer networks, systems and applications can lead to significant security risks, but how do pen testers go about uncovering them?**

Penetration testing plays a key role in identifying and addressing vulnerabilities by simulating the behavior of a potential attacker. A range of penetration testing methodologies have been developed to enable security professionals to achieve this safely and effectively. In this blog post, we discuss the leading pen testing methodologies, what they involve and the aspects they cover.

### Why is Penetration Testing Methodologies Important?

As an ethical cyber security assessment that helps organizations strengthens their cyber security posture, [penetration testing](https://www.redscan.com/services/penetration-testing/) is a complex process with the potential, if poorly executed, to miss important vulnerabilities and leave an organization exposed. Completing pen testing in alignment with structured frameworks and methodologies ensures that it meets specific goals and covers all the required areas. However, a one-size-fits-all approach to pen testing is not appropriate, as every organization and environment is different.

Penetration testing methodology is a specific course of action taken by a pentest provider to conduct the pentest of a target website or network. There are multiple penetration testing methodologies that can be put to use depending on the category of the target business, the goal of the pentest, and its scope

Penetration Testing Methodologies and Standards

There are various standards and methodologies that ensure the penetration test is authentic and covers all important aspects. Some of them are mentioned below:

1. [OSSTMM](https://www.getastra.com/blog/security-audit/penetration-testing-methodology/#osstmm)
2. [OWASP](https://www.getastra.com/blog/security-audit/penetration-testing-methodology/#owasp)
3. [NIST](https://www.getastra.com/blog/security-audit/penetration-testing-methodology/#nist)
4. [PTES](https://www.getastra.com/blog/security-audit/penetration-testing-methodology/#ptes)
5. [ISSAF](https://www.getastra.com/blog/security-audit/penetration-testing-methodology/#issaf)

### What is OSSTMM?

OSSTMM is short for [Open-Source Security Testing Methodology Manual](https://www.sciencedirect.com/topics/computer-science/open-source-security-testing-methodology-manual). It is one of the most widely used and recognized standards of penetration testing. It’s based on a scientific approach to penetration testing that contains adaptable guides for testers. You can use this to conduct an accurate assessment.

What is OWASP?

OWASP stands for [Open Web Application Security Project](https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies). Widely known, this pentest standard is developed and updated by a community keeping in trend with the latest threats. Apart from application vulnerabilities, this also accounts for logic errors in processes.

What is NIST?

[National Institute of Standards and Technology (NIST)](https://www.sciencedirect.com/topics/computer-science/open-source-security-testing-methodology-manual) offers very specific pentesting methodology for pentesters to help them improve the accuracy of the test. Both large and small companies, in various industries, can leverage this framework for a penetration test.

## What Is Security Analysis?

Security analysis refers to analyzing the value of securities like shares and other instruments to assess the business’s total value, which will be useful for investors to make decisions. There are three methods to analyze the value of securities – fundamental, technical, and quantitative analysis.

**Key Feature of Security Analysis**

* Security analysis involves diligently determining the intrinsic value of securities, such as stocks and financial instruments, to help investors make well-informed decisions for optimal returns.
* The three primary types of security analysis are fundamental, technical, and quantitative, each employing distinct methodologies to assess securities’ worth and market trends.
* Security analysis serves the pivotal purpose of enhancing individuals’ net worth by strategically investing their earnings in diverse financial instruments to achieve profitable outcomes.
* Ethical conduct, competence, and dedication are the guiding principles for security analysts, ensuring clients’ interests are safeguarded and prioritized throughout the investment process.

**SOCIAL ENGINEERING PENETRATING TESTING AND SECURITY ANALYSIS**

Social engineering penetration testing is the practice of attempting typical [social engineering](https://www.techtarget.com/searchsecurity/definition/social-engineering) scams on a company’s employees to ascertain the organization's level of vulnerability to that type of exploit.

Social engineering pen testing is designed to test employees' adherence to the security policies and practices defined by management. Testing should provide a company with information about how easily an intruder could convince employees to break security rules or divulge or provide access to sensitive information. The company should also get a better understanding of how successful their security training is and how the organization stacks up, security-wise, in comparison to their peers.

Social engineering testing may be conducted as part of more comprehensive penetration tests ([pen tests](https://www.techtarget.com/searchsecurity/definition/penetration-testing)). Like [ethical hacking](https://www.techtarget.com/searchsecurity/definition/ethical-hacker) methods, the tests themselves generally replicate the types of efforts that real-world intruders use.

Physical testing, for example, might involve a tester trying to enter a secured building at a time when many employees are entering, perhaps talking on a phone and carrying multiple items to see if someone just holds the door open rather than adhering to the approved procedure of letting the door close after them so any person following must use an employee card or badge for entry.

[Phishing](https://www.techtarget.com/searchsecurity/definition/phishing) exploits, a common social engineering method, are often used to test employee vulnerability. Testers might send an email purportedly from someone in management asking the employee to open an unexpected attachment, provide sensitive information or visit an unapproved website.

A tester might call employees pretending to be someone in IT, providing them with new passwords and telling them to change their current passwords to the new ones.

## Types of Social Engineering Attacks

Popular types of social engineering attacks include the following techniques:

* **Baiting.** An attacker leaves a malware-infected physical device, such as a [Universal Serial Bus flash drive](https://www.techtarget.com/searchstorage/definition/USB-drive), in a place it is sure to be found. The target then picks up the device and inserts it into their computer, unintentionally installing the malware.
* [**Phishing**](https://www.techtarget.com/searchsecurity/definition/phishing)**.** When a malicious party sends a fraudulent email disguised as a legitimate email, often purporting to be from a trusted source. The message is meant to trick the recipient into sharing financial or personal information or clicking on a link that installs malware.
* [**Spear phishing**](https://www.techtarget.com/searchsecurity/definition/spear-phishing)**.** This is like phishing, but the attack is tailored for a specific individual or organization.
* [**Vishing**](https://www.techtarget.com/searchunifiedcommunications/definition/vishing)**.** Also known as voice phishing, vishing involves the use of social engineering over the phone to gather financial or personal information from the target.
* [**Whaling**](https://www.techtarget.com/searchsecurity/definition/whaling)**.** A specific type of phishing attack, a whaling attack targets high-profile employees, such as the chief financial officer or chief executive officer, to trick the targeted employee into disclosing sensitive information.
* **Pretexting.** One party lies to another to gain access to privileged data. For example, a pretexting scam could involve an attacker who pretends to need financial or personal data to confirm the identity of the recipient.
* **Scareware.** This involves tricking the victim into thinking their computer is infected with malware or has inadvertently downloaded illegal content. The attacker then offers the victim a solution that will fix the bogus problem; in reality, the victim is simply tricked into downloading and installing the attacker's malware.
* [**Watering hole**](https://www.techtarget.com/searchsecurity/definition/watering-hole-attack)**.** The attacker attempts to compromise a specific group of people by infecting websites they are known to visit and trust with the goal of gaining network access.
* **Diversion theft.** In this type of attack, social engineers trick a delivery or courier company into going to the wrong pickup or drop-off location, thus intercepting the transaction.

## Preventing social engineering

There are a number of strategies companies can take to prevent social engineering attacks, including the following:

* Make sure information technology departments are regularly carrying out [penetration testing](https://www.techtarget.com/searchsecurity/definition/penetration-testing) that uses social engineering techniques. This will help administrators learn which types of users pose the most risk for specific types of attacks, while also identifying which employees require additional training.
* Start a [security awareness training](https://www.techtarget.com/searchsecurity/definition/security-awareness-training) program, which can go a long way toward preventing social engineering attacks. If users know what social engineering attacks look like, they will be less likely to become victims.
* Implement secure email and web [gateways](https://internetofthingsagenda.techtarget.com/definition/gateway) to scan emails for malicious links and filter them out, thus reducing the likelihood that a staff member will click on one.
* Keep antimalware and antivirus software up to date to help prevent malware in phishing emails from installing itself.
* Stay up to date with software and firmware patches on endpoints.

## What is an internal infrastructure penetration test?

As the name suggests, an internal penetration test focuses on testing the infrastructure and devices inside of your network perimeter. These tests look for vulnerabilities that could be exploited by a would-be attacker, who has already managed to get inside your IT infrastructure. Examples of these types of attackers could be disgruntled members of staff or attackers who have successfully got a foothold within your infrastructure via an externally exposed vulnerability, malware, or using stolen user credentials.

Internal penetration tests vary in scope (view our latest blog on [scoping a penetration test](https://evalian.co.uk/scoping-a-penetration-test/)); they can either focus on testing your internal network, hosts, applications – or all of the above, depending on your specific needs and concerns. The testers’ role is typically to see what they can access and how far they can move laterally across the environment. They may try to access file servers, databases, and systems and will seek to escalate their user privileges to the admin level to see which systems they could take control of.

## INTERNAL AND EXTERNAL PENETRATION TESTING SECURITY ANALYSIS

## What is the process of an internal infrastructure penetration testing?

An internal network pen test is performed to help gauge what an attacker could achieve with initial access to a network. An internal network pen test can mirror insider threats, such as employees intentionally or unintentionally performing malicious actions.

The test usually starts with a reconnaissance, where the tester uses mapping tools to determine the workings and layout of your internal infrastructure, and how its computers and servers interact.

The tester will then move through the target infrastructure looking for exploitable vulnerabilities. Common tactics used include brute force attacks to compromise employee accounts; exploiting network protocols to gain illegitimate access to endpoints and running malicious code that exploits known software vulnerabilities. Sometimes a tester may find a list of system passwords saved in plain text on one system which provides access to other systems.

On completion of the test, the tester will write up their [penetration testing report](https://evalian.co.uk/what-should-a-good-penetration-test-report-include/), setting out their findings, vulnerabilities found, recommended remediation steps, and their overall risk assessment for the target systems. A wash-up call is then scheduled to talk the client through the test and answer any questions.

While these tests help to identify internal vulnerabilities, it’s important to note that they aren’t the same as a mock cyber-attack scenario. This kind of assessment is called a red team assessment. These mimic a real-life attacker by using a combination of tactics, techniques and tools to access target systems or data.

While the goal of an internal penetration test is usually to uncover as many exploitable vulnerabilities as possible, the goal of a red team assessment is to evade detection and harvest sensitive data. For more information on this topic, read our blog: [red team assessments vs penetration tests](https://evalian.co.uk/penetration-testing-vs-red-team-testing/).

## What is an External Infrastructure Penetration Testing?

An external network pen test is designed to test the effectiveness of perimeter security controls to prevent and detect attacks as well as identifying weaknesses in internet-facing assets such as web, mail and FTP servers.

An external pen test focuses on testing your perimeter systems, which consist of internet-facing infrastructure and applications. These systems are your most vulnerable, as they are exposed and out in the open – making them easily visible to cyber attackers.

The goal of an external penetration test is to discover vulnerabilities within your external-facing systems and services. External testing is vitally important because anything exposed to the internet will be constantly scanned for vulnerabilities by attackers of all kinds – including those with limited sophistication.

The tester will look at your external systems from the outside in, just like a cyber-attacker would. They will try to find as much open-source intelligence as possible, to help them understand the layout of your organisation and identify suitable tools, tactics, and techniques to use.

From there, the tester will use a range of tools, including [vulnerability scanners](https://evalian.co.uk/the-difference-between-a-penetration-test-and-a-vulnerability-scan/), to discover exploitable vulnerabilities within your external infrastructure. Once this is done, the tester will then seek to exploit these vulnerabilities, to see how far they can get into your systems and networks.

At the end of the test, the tester will provide their report and attend a wash-up meeting, as with internal testing.