# What is Penetration Testing?

A penetration test or pen test is a simulated cyber-attack against computer systems, application systems, and IT infrastructure to discover loopholes. These simulated cyber-attacks come in diverse forms with the intent of breaching a system through its servers, web or mobile applications, and other endpoints. The purpose of pen testing is to discover exploitable vulnerabilities in a controlled setting before cybercriminals take advantage of them.

Penetration testing is an IT security niche with diverse testing methods and requires a skilled tester to execute. Why attempt to penetrate your cyber systems, you may ask? The short answer is that the insight it provides can be used to patch detected loopholes, while the longer answer is what this article covers.

## How Does Penetration Testing Work?

Penetration testing is a process that follows a defined pathway to gain insight into vulnerabilities. The process consists of five stages: planning, scanning, gaining access, maintaining access, and result analysis. The first four stages simulate the actions of a cybercriminal's attempt to gain a foothold within computer systems, while the last stage focuses on how IT security teams can prevent and respond to similar security incidents. The importance of these five stages includes:

- Planning – The planning stage is where goals and strategies are set. Here, the system to be tested is pinpointed, and the penetration testing method or methods to be used are outlined.
- Scanning – This stage involves exploring how the target application or system responds to diverse intrusion attempts. The scanning phase involves the use of scanning tools such as vulnerability scanners or network sniffers to collect datasets that provide essential information about the target.
- Gaining Access – Knowledge from the scanning phase is then used to gain access to the target. Here, tools and techniques simulating attacks are used. These tools could be cross-site scripting, SQL injection, or backdoor breaching attempts to gain access into applications, servers, and systems.
- Maintaining Access – Successful cyber-attacks are generally detected months after access has been gained. The slow discovery process is due to the efforts made to maintain access to a target.

Thus, this phase focuses on analyzing if discovered vulnerabilities can be exploited for extended durations to gain prolonged access.

- Analysis – A formal report outlining detected vulnerabilities, the vulnerabilities that were exploited to gain access successfully, and how long access was maintained is provided. The insight from the pen test report is used by security teams to patch vulnerabilities and to take a preventive approach to tackle future attacks.

## Penetration Testing Methods

Five methods can be applied to test for system and firewall vulnerabilities within an IT infrastructure. These methods can be applied as singular processes or meshed together depending on the planning stage's stated goals. The five methods include:

1. External Testing – External testing methods target the most visible online assets of an enterprise. This includes web applications, emails, and other online platforms. The testing process involves using phishing attacks to glean data from these visible assets.
2. Internal Testing – The internal test method is conducted behind an application's firewall which means the attacker has either gained access to an employee's credentials or made some lucky guesses. The internal test simulates scenarios where an employee has been compromised or gone rogue. Approximately 90% of successful data breaches are due to human error, highlighting the importance of the internal testing method.
3. Blind Testing – The blind test method involves using brute force to gain access into an enterprise network without any inside information or employee credentials. The blind test provides security teams with insight into how cybercriminals work and how an application or system assault occurs.
4. Double-Blind Testing – The double-blind test simulates real-world scenarios where the cybercriminal has no inside knowledge, and security teams have no prior knowledge of when the attack will come and what type of attack will be used. Thus, security teams respond in real-time as the attacker adapts to changing security situations.
5. Targeted Testing – Targeted testing is the opposite of the double-blind test method and in this case, both the attacker and the security personnel are in sync as the test occurs. Targeted test is more or less a training process to get security teams up to speed with new attack methodologies and understand the behavioral patterns of hackers.

## Who Does Pen Testing?

An authorized penetration tester handles penetration testing, and pen testers are also broadly classified as information security analysts. The penetration tester actively searches for the vulnerabilities and flaws in exiting cyber systems using the methods outlined above. The tester uses existing hacking tools to simulate actual attacks, thus assisting security teams with patching flaws and developing high-performing incidence response strategies.

Professional penetration testers are expected to be skilled security analysts with excellent knowledge of scripting and coding. The tester is expected to have gained knowledge of the particular operating system to be tested and understand the tools hackers use to target that system. Finally, knowledge of network protocols like DNS is required to understand how cybercriminals target vulnerabilities and breach systems.

## Why Does Penetration Testing Matter?

The evolving security threats IT infrastructure face and the regular additions of new applications mean constant vigilance is needed to forestall breaches. Penetration testing provides a means to continuously test your enterprise's security posture to detect vulnerabilities and craft remediation strategies to eliminate vulnerabilities. It also serves as a training and validation tool for cybersecurity teams tasked with developing mitigation strategies to respond to cybersecurity incidents.

Penetration testing is also done to ensure cyber systems stay updated to regulatory compliance standards such as the European Union Cybersecurity Act. An annual penetration test keeps your business on the right side of the law while protecting your data from cybercriminals.

## Conclusion

The fallout from successful cyber-attacks is why comprehensive penetration tests must be done if optimal security is the goal. Statistics show that approximately 60% of SMBs go out of business within 6 months of a data breach. Penetration testing provides a means to secure your business applications and reputation from criminal intent.