What is Pentest? Learn about Penetration Testing (penetration testing)

Penetration testing, sometimes called pen testing or ethical hacking, is a simulation of a real-world cyber attack that tests an organization's cyber security and detects vulnerabilities.

What is penetration testing?

Penetration testing, sometimes called pen testing or ethical hacking, is a simulation of a real-world cyber attack that tests an organization's cyber security and detects vulnerabilities. Although some may consider pentests as a vulnerability scan that checks compliance requirements with security measures.

The purpose of a pentest is not only to test for vulnerabilities in the environment, but also to test people and processes against possible threats to the organization. Knowing which adversaries are most likely to target you allows penetration testers to mimic the specific tactics, techniques, and procedures (TTPs) of those specific adversaries – giving the organization the ability to target you. much more realistic idea of ??how a breach might occur.

Penetration testing steps

In most cases, penetration testing will follow the steps outlined in the MITER ATT&CK framework. If you are new to the MITER framework, it is a knowledge base of known adversarial tactics, techniques, and processes that occur during the various stages.

Following this framework provides a way for pentesters to model a specific adversary's behavior, thereby allowing them to more accurately mimic the attack during testing. Currently, there are 12 tactics in the Miter Enterprise matrix:

1. Initial access tactics refer to the vectors that hackers exploit to gain access to the environment
2. Execution refers to the techniques used to execute an adversary's code after gaining access to the environment.
3. Persistence tactics are actions that allow an attacker to maintain a presence in the network
4. Privilege escalation refers to actions taken by an adversary to gain higher access to a system
5. Defensive evasion tactics are techniques used by intruders that allow them to go unnoticed by a system's defenses.
6. Credential access refers to the techniques used to obtain credentials from users or administrators
7. Discovery refers to the learning process through which adversaries better understand the system and access they currently possess.
8. Horizontal movement is used by adversaries to gain remote access and control of systems
9. Collection tactics are the tactics used by attackers to collect target data
10. Command and control are tactics used to establish communication between a compromised network and a controlled system.

11. Exfiltration is the actions an adversary takes to remove sensitive data from the system
12. Influence tactics are tactics intended to influence business operations

It is important to note that the above tactics used in pentesting depend on the tactics of the opponent being imitated. However, in general, performing a penetration test usually includes the following phases: Planning, Reconnaissance, Gain/Maintain Access, Analysis, Remediation.

Types of penetration testing

When considering conducting penetration testing, it is important to remember that there is no one-size-fits-all test. The environment, industry risks, and competitors are different for each organization. Furthermore, there is not just one type of pen test that can meet all the needs of an organization.

There are several types of pentests designed to meet specific goals and threats to an organization. Below are some of the most popular types of pen tests.

1. Internal Pentest

Evaluate the organization's internal systems to determine how an attacker can move across the network: Testing includes system identification, enumeration, vulnerability detection, exploitation, privilege escalation, migration horizontal movement and target.

2. External pentest

Evaluate Internet access systems to determine if there are exploitable vulnerabilities that could expose data or unauthorized access to the outside world: Testing includes identification, enumeration, detection, and exploitation exploit security holes.

3. Pentest web applications

Evaluate web applications using a three-phase process: First is reconnaissance, in which the team discovers information such as the operating system, services, and resources being used. The second is the discovery phase, in which the team tries to identify vulnerabilities. The third is the exploitation phase, in which the group leverages discovered vulnerabilities to gain unauthorized access to sensitive data.

4. Internal threat pentest

Identify risks and vulnerabilities that could expose sensitive internal assets and resources to unauthorized persons: The team evaluates weaknesses such as de-authentication attacks, misconfigurations, session reuse, and unauthorized wireless devices.

5. Wireless pentest

Identify risks and vulnerabilities associated with wireless networks: The team evaluates weaknesses such as deauth attacks, misconfigurations, session reuse, and unauthorized wireless devices.

6. Physical Pentest

Identify physical security risks and vulnerabilities when gaining access to company computer systems: The team evaluates weaknesses such as social engineering, tail-gating attacks, badge cloning and security targets Other physics.

When should penetration testing be performed?

The most important time to conduct a pentest is before a breach occurs. Many organizations don't really pay attention until they're actually attacked - that is, after they've lost data, intellectual property and reputation. However, if you encounter a violation, you should conduct a post-breach remediation pentest to ensure mitigation measures are effective.

Best practices are that you should conduct pen testing while the system is being developed or installed and immediately before going into production. The danger of running pentests too late is that it takes a long time to update the code.

Pen testing is not a one-and-done proposition. They should be conducted whenever changes occur and/or at least annually. Factors including company size, infrastructure, budget, legal requirements and emerging threats will determine the appropriate frequency.

How often should a pen test be performed?

Businesses should perform extensive penetration testing at least once a year. This not only allows for regular deployment of security patches and upgrades, but also supports compliance with data security standards, such as PCI DSS (Debit Cardholder Industry Data Security Standard). maths).

However, bi-annual or even quarterly audits can detect potential security risks more frequently – and before they are compromised – giving you a more comprehensive overview of your health. your security status.

Penetration testing is designed to highlight specific vulnerabilities in a system or network. Therefore, pentesting should ideally be performed on any new additions to the network infrastructure or whenever there is a major overhaul to major applications. This is when the environment is most vulnerable to attack and weaknesses are most likely to be exposed.

Who performs pentesting?

Many independent cybersecurity businesses and experts offer these types of penetration testing as a service. And although pentesting can be done internally, external white hat hackers can provide more insight because they have no prior knowledge of the system.

However, the nature of business activities has many complexities. Legal considerations surrounding any 'hacking' activity mean that the entire pentest process needs to be handled with care.

Ensure all pentest activities meet legal requirements and all legal documents are accurate and complete. It is also important to perform background checks on pentesters to control their credentials. For example, CREST and NCSC are industry-recognized certifications issued to trusted penetration testing companies.

What should I do after performing a pentest?

Penetration testing is part of developing a long-term security strategy, based on patching tested real-world vulnerabilities.

Rapid processing of pentest results is important to avoid downtime and disruption associated with cybersecurity breaches, as well as hefty fines for those who violate data protection regulations.

After penetration testing, you should:

1. Review the final report and discuss the findings with both the external pentest team and the internal cybersecurity team
2. Develop a comprehensive cybersecurity strategy and remediation plan to address identified issues
3. Use repeatable testing and vulnerability scanning to track the success and progress of long-term patches and upgrades

Pen test is designed comprehensively. They provide detailed insights into the scope and severity of any potential vulnerabilities in the environment. So, there will always be many useful findings to help you increase your security.