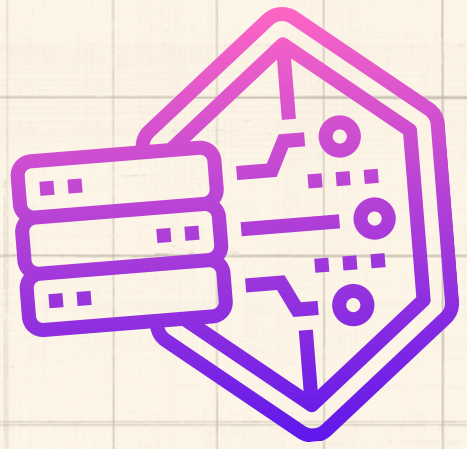
Cybersecurity

Pentest & its phases



Awareness →

Cybersecurity

What is it?

A **Pentest** or Penetration testingis a controlled simulation of a cyber attack designed to identify and correct vulnerabilities in systems, applications or networks. In other words, it's like "*ethical hacking*" where security experts try to find weak spots before actual attackers do.

Es como probar las cerraduras de una casa para asegurarte de que un ladrón no pueda entrar.

Awareness

Cybersecurity

It consist of 5 phases

Awareness

Cybersecurity

1. Reconnaissance

The goal is to collect as much information as possible about the target system, without directly interacting with it (passive reconnaissance) or by interacting directly with it (active reconnaissance).

- Search public information: domain names, IP addresses, web servers, emails.
- Examine social networks and forums to find sensitive data
- Scan networks to identify connected devices.

Awareness →

2. Scanning

In this stage, the pentester interacts more with the target system to identify possible weak points. Services, open ports and software versions are searched.

- Scan ports to identify exposed services (HTTP, SSH, etc.).
- Detect software versions to look for known vulnerabilities.
- Map the network structure of the organization.

3. Exploitation

Here the pentester tries to exploit the vulnerabilities found in the previous phase to access the system.

- Perform brute force attacks to crack weak passwords.
- Use known exploits to exploit bugs in the software.
- Upload malicious shells to gain remote access.

Cybersecurity

4. Post-Exploitation

If the system was accessed, this phase focuses on analyzing how the attackers could stay inside without being detected and how far they can go with that access.

- Escalate privileges to gain administrator access.
- Set up backdoors to re-enter the system in the future. (persistence)
- Exfiltrate sensitive data without alerting the security system

Awareness

5. Report

At this phase, all findings are documented, explaining the identified vulnerabilities, their impact and recommendations to resolve them.

- Create a prioritized list of vulnerabilities with their level of criticality.
- Propose technical solutions such as updates, configuration changes or additional monitoring.
- Present an executive summary so that non-technical decision makers understand the risks.

Cybersecurity

Follow me for more information and safety tips.

Save Share Follow

Awareness