IT Security

INTRODUCTION

DURATION : 0’45

 Version : 0.0.5 Update : 04/02/2022

Summary

Introduction to cybersecurity

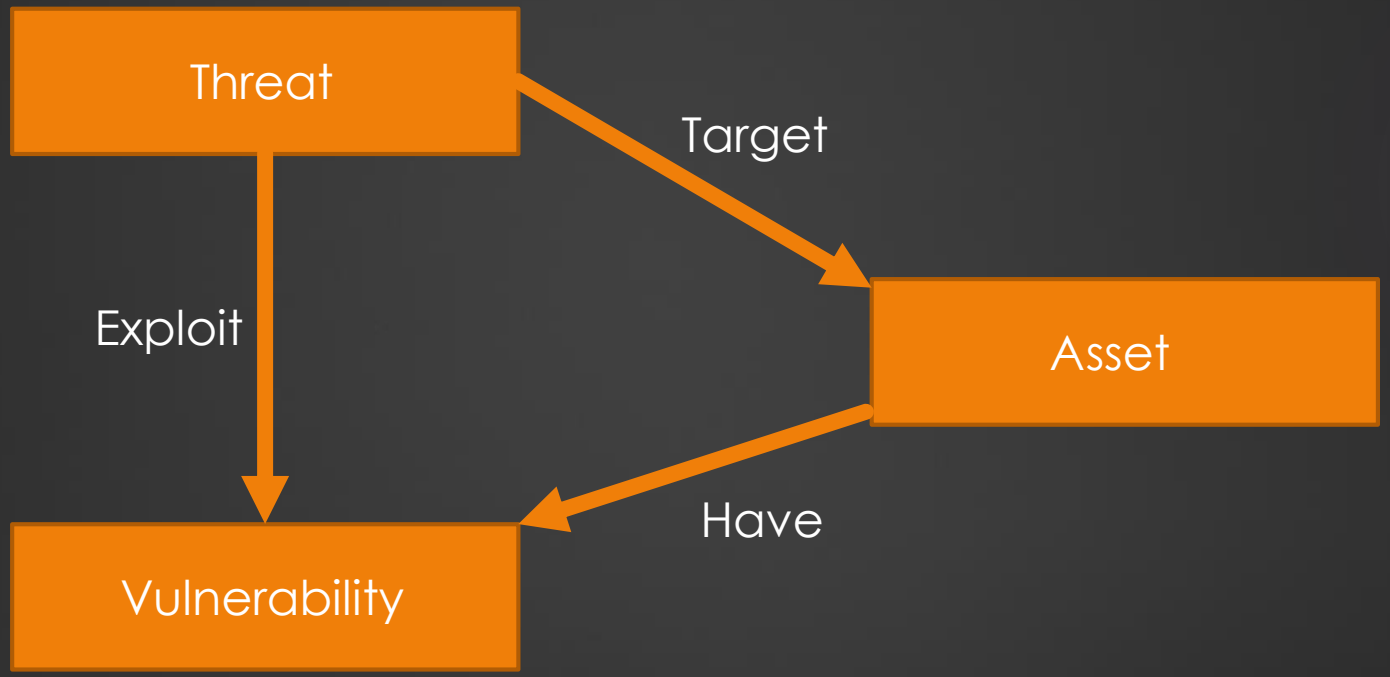
- Cybersecurity / IT security prevents unauthorized access to assets (computers, servers, networks, data, etc.).

- To maintain (CIA or DICP / DICPP in French)
  - **Confidentiality**:
    Cleartext or password stealing has an impact on confidentiality.
  - **Integrity**:
    Data tampering has an impact on integrity.
  - **Availability**:
    DoS attack has an impact on availability.
  - **Non repudiation**:
    Guarantee that the sender of a message cannot deny having sent the message and the recipient cannot deny having received it.

Terms

- **White Hats** is a good guys also called ethical hackers.
- **Black Hats** is a bad guys, malicious hackers.
- **Gray Hats** is a good and bad guys depends on the situation.
- **Threat** that could lead to a potential breach of security.
- **Exploit** takes advantage of a bug or vulnerability, leading to unauthorized access, privilege escalation, or Denial Of Service.
- **Vulnerability** is a software flaw or implementation error that can lead to an unexpected and undesirable event executing bad or damaging instructions to the system.
- **Risk analysis** aim to identify, assess and prioritize the risks associated with the activities of an organization.

Vocabularies



Testing types

- **Black box:** testing involves performing a security evaluation and testing with no prior knowledge of the infrastructure.
- **White box** testing involves performing a security evaluation and testing with complete knowledge of the infrastructure.
- **Gray box** testing involves a combination of white-box testing and black-box testing. The aim of this testing is to search for the defects if any due to improper structure or improper usage of applications.

All steps to execute a pentest

1. Talk to the client about the perimeter (IP, domain, etc.) and types of attacks that may create a risk for the customer (brute force, DoS, etc.).
2. Prepare and sign with the client the NDA (non-disclosure agreement)
3. Conduct the pentest and collect information in order to provide a report.
4. Write the report and have it proofread by a colleague.
5. Present the report findings to the client (report, documentation, etc.).

<u>Warning :</u> It is legally forbidden to scan / pentest / etc. if you haven't been commissioned for it or that the solution is not yours.

Kill chain : Attack phases

Kill chain is a term used to define the steps an enemy uses to attack a target.

Pre-attack

1. **Reconnaissance**: Information gathering and attempts to identify vulnerabilities.
2. **Weaponization**: Creates remote access (virus or worm).

Attack

3. **Delivery**: Transmits weapon to target (e-mail, websites or USB drives)
4. **Exploitation**: Malware weapon's program code triggers, which takes action on target network to exploit vulnerability (e.g., download code).
5. **Installation**: Malware weapon installs access point backdoor.
6. **Command and Control / Persistence**: Malware gives a hand on the keyboard.
7. **Actions on Objective**: Intruder takes action to achieve their goals (data exfiltration, data destruction, or encryption for ransomware).

Reconnaissances

- **Passive reconnaissance** there will be no traffic generated on the target's infrastructure, it is a matter of finding public data by conventional or specialized search engines (wireshark, shodan, etc.).

- **Active reconnaissance** it is a question of going directly to question the "target". For example, a server's ports can be scanned to see which services they are responding to.