IT Security

INTRODUCTION

DURATION : 0’30

 Version : 0.0.7 Update : 22/04/2022

Summary

Introduction to cybersecurity

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

- To maintain (CIA or DICP 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.

Kill Chain Frameworks

- Kill Chain are frameworks to prevent and identify cyber intrusions activity.
- The two main frameworks are :
  - ATT&CK : https://attack.mitre.org/
  - Cyber Kill Chain : https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
- ATT&CK and the Cyber Kill Chain are complementary.
- I prefer ATT&CK because tactics are unordered and may not all occur in a single intrusion because adversary tactical goals change throughout an operation, whereas the Cyber Kill Chain uses ordered phases to describe high level adversary objectives.

Cyber Kill chain : Attack phases

The kill chain is a framework methodology is a component of intelligence-driven defense for the identification and prevention of malicious intrusion activities.

Pre-attack

1. **Reconnaissance**: Gather information to probe for weak points
2. **Weaponization**: Create a deliverable malicious payload using an exploit and a backdoor.

Attack

3. **Delivery**: Send weaponized bundle to the victim using email, USB, etc.
4. **Exploitation**: Exploit a vulnerability by executing code on the victim's system.
5. **Installation**: Install malware on the system target.
6. **Command and Control / Persistence**: Create a command and control to communicate and pass data back and forth.
7. **Actions on Objective**: Perform actions to achieve intended objectives or goals.

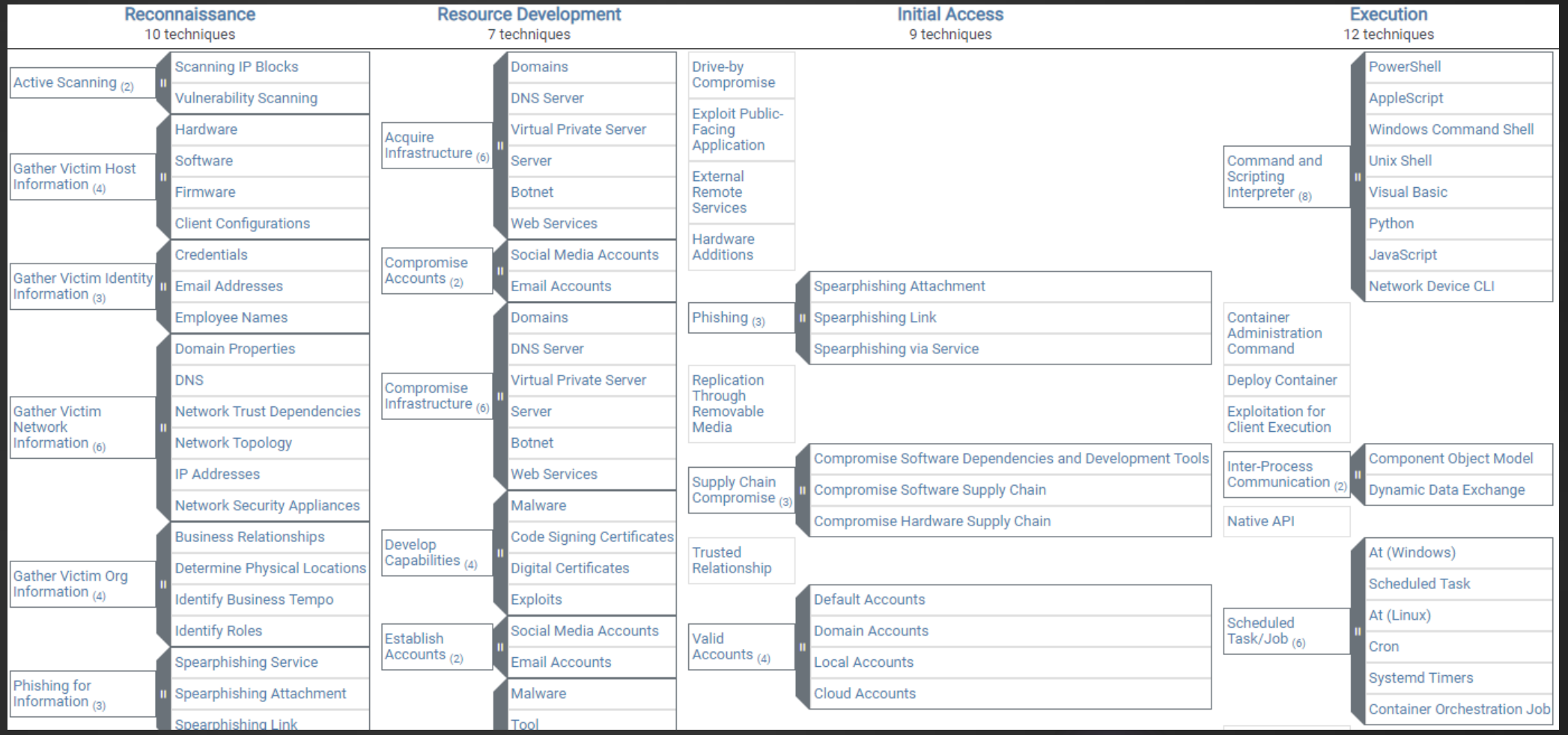
ATT&CK Tactics, Techniques and Procedures

- The term TTP refers to the patterns of activities and methods associated with specific threat actors.
  - **Tactics** are the guidelines that describe the way of an attacker performs the attack from beginning to the end : https://attack.mitre.org/tactics/enterprise/
  - **Techniques** are the technical methodes used by an attacker to achieves intermediate results during the attack (exploitation , command and control, covering the tracks, etc.). https://attack.mitre.org/techniques/enterprise/
  - **Procedures** are organizational approaches that threat actors follow to launch an attack.
    Example how threat actor can gather informations ?

Tactics, Techniques and Procedures

Tactics

Techniques



Tactics, Techniques and Procedures

Active Scanning: Vulnerability Scanning

Other sub-techniques of Active Scanning (2)

Adversaries may scan victims for vulnerabilities that can be used during targeting. Vulnerability scans typically check if the configuration of a target host/application (ex: software and version) potentially aligns with the target of a specific exploit the adversary may seek to use.

These scans may also include more broad attempts to Gather Victim Host Information that can be used to identify more commonly known, exploitable vulnerabilities. Vulnerability scans typically harvest running software and version numbers via server banners, listening ports, or other network artifacts.[1] Information from these scans may reveal opportunities for other forms of reconnaissance (ex: Search Open Websites/Domains or Search Open Technical Databases), establishing operational resources (ex: Develop Capabilities or Obtain Capabilities), and/or initial access (ex: Exploit Public-Facing Application).

ID: T1595.002
Sub-technique of: T1595
Tactic: Reconnaissance
Platforms: PRE
Version: 1.0
Created: 02 October 2020
Last Modified: 15 April 2021

Version Permalink

Procedure Examples

ID	Name	Description
G0007	APT28	APT28 has performed large-scale scans in an attempt to find vulnerable servers.[2]
G0016	APT29	APT29 has conducted widespread scanning of target environments to identify vulnerabilities for exploit.[3]
G0034	Sandworm Team	Sandworm Team has scanned network infrastructure for vulnerabilities as part of its operational planning.[4]
G0139	TeamTNT	TeamTNT has scanned for vulnerabilities in IoT devices and other related resources such as the Docker API.[5]
G0123	Volatile Cedar	Volatile Cedar has performed vulnerability scans of the target server.[6][7]

Mitigations

ID	Mitigation	Description
M1056	Pre-compromise	This technique cannot be easily mitigated with preventive controls since it is based on behaviors performed outside of the scope of enterprise defenses and controls. Efforts should focus on minimizing the amount and sensitivity of data available to external parties.

Detection

ID	Data Source	Data Component
DS0029	Network Traffic	Network Traffic Content
		Network Traffic Flow

Monitor for suspicious network traffic that could be indicative of scanning, such as large quantities originating from a single source (especially if the source is known to be associated with an adversary/botnet). Analyzing web metadata may also reveal artifacts that can be attributed to potentially malicious activity, such as referer or user-agent string HTTP/S fields.

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

Indicators Of Compromise (IOCs)

- Indicators of Compromise (IOC) are the clues and pieces of forensic data found on the network or operating system of an organization that indicate a potential intrusion or malicious activity in the organization's infrastructure.
- Security professionals need to perform continuous monitoring of IOC to detect and respond to evolving cyber threats.

Definition of hacking

- Hacking refers to exploiting system vulnerabilities and compromising security controls to gain unauthorized or inappropriate access to a system's resources.
- It involves modifying system or application features to achieve a goal outside of the creator's original purpose.
- Hacking can be used to steal and redistribute intellectual property, leading to business loss.

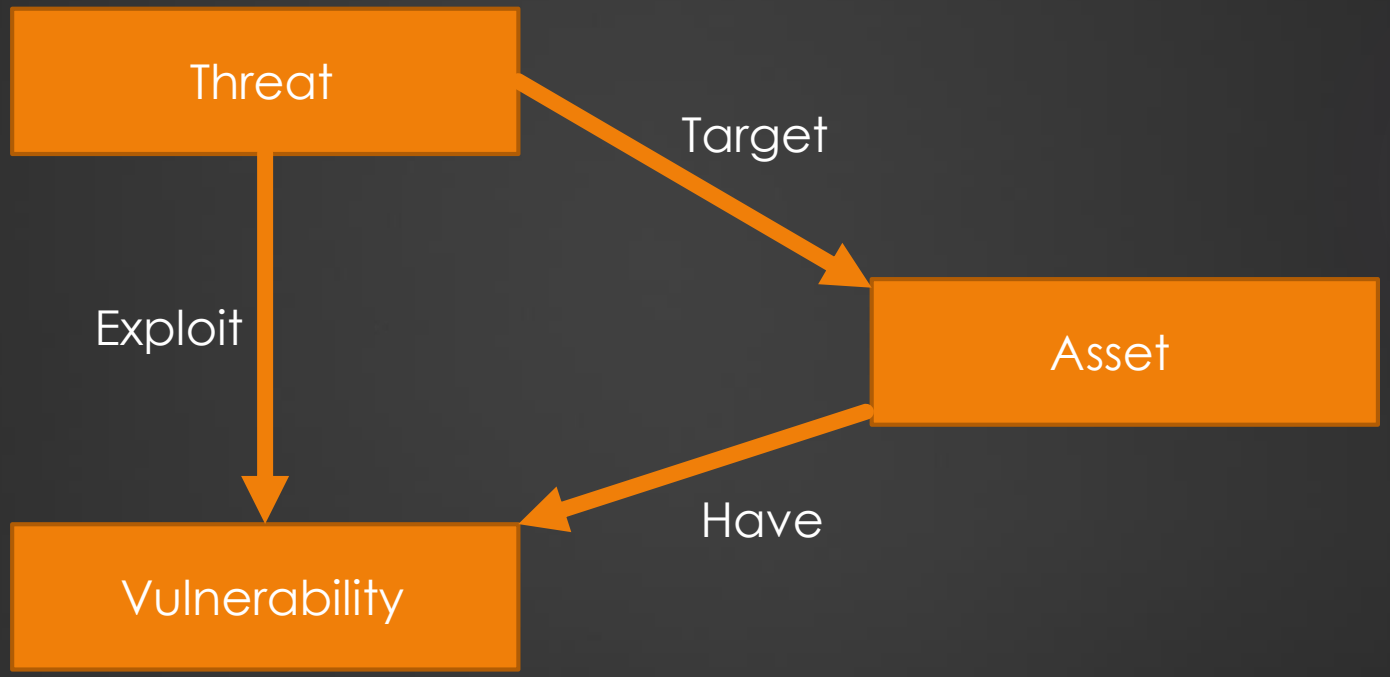
Different types of hacker

- **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.
- **Hacktivist** is a guy who defend a political opinion.
- **Script Kiddies** is an unskilled hacker who compromises a system by running scripts, tools, or other developed by real hackers.
- **Cyber Terrorists** are guys motivated by religious or political.
- **State-sponsored Hackers** are guys employed by the government to hack another government.

Other terms

- **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 in pentest

- **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.

Hacking phase

- In general there are five phases of hacking :
  - **Reconnaissance**
  - **Scanning**
  - **Gaining Access**
  - **Maintaining Access**
  - **Clearing Tracks**

Hacking phase : Reconnaissance

- Reconnaissance refers to the preparatory phase where an attacker seeks to gather information about a target prior to launching an attack.
- The reconnaissance target range may include the target organization's clients, employees, operations, network and systems.
  - **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.

Hacking phase : Scanning

- **Pre-attack** : Scanning refers to the pre-attack phase when the attacker scans the network for specific information based on information gathered during reconnaissance.
- **Port scanner** : Scanning can include many tools like port scanners, network mappers, ping tools, vulnerability scanners, etc.
- **Extract information** : Attackers extract information such as live machines, port, port status, OS details, device type, and system uptime to launch attack.

Hacking phase : Gaining Access

- Gaining access refers to the point where the attacker obtains access to the operating system or applications on the target computer or network.
- The attacker can gain access at the operating system, application or network levels.
- The attacker can escalate privileges to obtain complete control of the system.
- Examples include password cracking, buffer overflows, denial of service and session hijacking.

Hacking phase : Maintaining Access

- Maintaining access refers to the phase when the attacker tries to retain their ownership of the system.
- Attackers may prevent the system from being owned by other attackers by securing their exclusive access with backdoors, rootkits or trojans.
- Attackers can upload, download or manipulate data, applications and configurations on the owned system.
- Attackers use the compromised system to launch further attacks.

Hacking phase : Clearing Tracks

- Clearing tracks refers to the activities carried out by an attacker to hide malicious acts.
- The attacker's intentions include obtaining continuing access to the victim's system, remaining unnoticed and deleting evidence that might lead to their prosecution.
- The attacker overwrites the server, system and application logs to avoid suspicion.
- Attackers Always cover their tracks to hide their identity.

What is an Ethical Hacking ?

- Ethical hacking involves the use of hacking tools, tricks and techniques to identify vulnerabilities and secure system security.
- If focuses on simulating the techniques used by attackers to verify the existence of exploitable vulnerabilities in a system's security.
- Ethical hackers perform security assessments for an organization with the permission of concerned authorities.