Théophane Paradis

M2 Cybsersecurity ; Security Audit, Threat and Risk Analysis

## Exercise 8 : What is Mitre Att&ck framework ?

*Review https://attack.mitre.org/ and present a synthesis of the framework :*

Made by MITRE to help companies or people to better understand, identify and prevent attacks. Attacks embrace attacks against entreprise, mobile and ICS (industrial Control System).

Main parts of the website :

- Matrix : agregates tactics and techniques related to a platform (mobile, entreprise…).

- Tactics : different steps of the good attack (against an entreprise for example).
  Tactics against entreprise are (in each case : the adversary trying to…) :
  - Reconnaissance : collect informations for future operations.
  - Resource Development : establish resources used to support operations.
  - Initial access : get into your network.
  - Execution : run malicious code.
  - Persistence : maintain their foothold.
  - Privilege Escalation : gain higher-level persmissions.
  - Defense Evasion : avoid to be detected.
  - Credential Access : steal account names and passwords.
  - Discovery : figure out your environment.
  - Lateral Movement : move through your environment.
  - Collection : gather data of interest to their goal.
  - Command and Control : communicate with compromised systems to control them.
  - Exfiltration : steal data.
  - Impact : manipulate, interrupt, or destroy your systems and data.

- Techniques : all techniques and sub-techniques that an attacker can use in order to reach his goal, means used.
  Some examples of techniques :
  - Abuse Elevation Control Mecanism
    - Setuid and Setgid
  - Account Discovery
    - Local account
    - Domain account

      …

    …
- Defenses :
  Data sources to protect ourselves from attacks, to detect it and also prevent it.
  - Ex : about the cloud storage…

Mitigations : actions, strategies, controls in order to limit a threat impact or attack impact.

- Ex : auditing, antivirus, antimalware, code signing...

Assets : devices and systems commonly found within Industrial Control System environments.

- Ex : Human-Machine Interaction, Jump Host, Remote Terminal Unit, Routers, VPN Server...

*Enrich the threat model against personal information exposed in the lab, with the tactics enumerated in the framework :*

With the tactics we can try to have more precise threat model with a better methodology.

Reconnaissance : collect informations for future operations.

- With OSINT tools we have seen before (google dorks, nmap...).

Resource Development : establish resources used to support operations.

- Register fake domains (that looks legitimate) to use them in phising attacks.

Initial access : get into your network.

- With a malicious link in a phishing mail for example.
  Malware examples : Emotet / TrickBot.

Execution : run malicious code.

- PowerShell scripts.

Persistence : maintain their foothold.

- Setting up scheduled tasks ← malicious code automatically run after reboots.

Privilege Escalation : gain higher-level persmissions.

- Do a privilege escalation attack to have administrator level access to do whatever we want.

Defense Evasion : avoid to be detected.

- By disabling antivirus.

Credential Access : steal account names and passwords.

- Use shoulder surfing, keyloggers (physical or logical).

Discovery : figure out your environment.

- Nmap could be a solution to have an overview of the environment.

Lateral Movement : move through your environment.

- Possible to use PsExec or Remote Desktop Protocol, to have the possibility to move through systems.
  Use the computer remotely and be free in the system.

Collection : gather data of interest to their goal.

- IMPORTANT PART FOR US : at this step we can find many informations.

Command and Control : communicate with compromised systems to control them.

- DNS tunelling, to stealthly transfer data. (bidirectional)
- C2 : communicate with malware installed on compromised systems ← send commands without detection.

Exfiltration : steal data.

- With DNS exfiltration for example or DropBox. (unidirectional)

Impact : manipulate, interrupt, or destroy your systems and data.

- Now, do a ransomware for example (if the goal is the money), maybe to ask to others informations we didn't find yet (= ask directly to the target).

Some tactics can just be skipped, our objective is just to have more personnal information about our target.