Øvelse 49 – MITRE ATT&CK: Taktikker, Teknikker, Mitigering og Detektering

Information

Formålet med denne øvelse er at opnå forståelse for, hvordan MITRE ATT&CK kan anvendes som et analytisk rammeværk til at strukturere og analysere angriberes adfærd.

Øvelsen har fokus på:

- Grundlæggende forståelse af begreber anvendt i MITRE ATT&CK
- Forståelse af rammeværkets struktur (taktik, teknik, procedure)
- Anvendelse af TTP'er til analyse og prioritering

Målet er, at I bliver i stand til selvstændigt at navigere i MITRE ATT&CK og anvende rammeværket som kilde og reference i analysearbejde.

Øvelsen danner fundament for senere arbejde med:

- Observerbarhed
- Detektion
- SIEM og IDS
- Design af detekteringsregler

MITRE ATT&CK er ikke en liste over værktøjer, men en struktureringsmodel for observeret angriberadfærd.

Øvelsen ligger primært på et videns- og forståelsesniveau og har til formål at opbygge et begrebsmæssigt fundament.

De teknikker og begreber, der introduceres her, vil senere blive anvendt i praksis, når vi arbejder med loganalyse og detektion i Wazuh.

Baggrund

MITRE ATT&CK er en struktureret og empirisk baseret model over observeret angriberadfærd dokumenteret i virkelige sikkerhedshændelser.

ATT&CK er ikke en liste over exploits eller konkrete værktøjer. Det er en systematiseret strukturering af adfærdsmønstre, der er observeret og dokumenteret gennem cyber threat intelligence.

Rammeværket organiserer denne adfærd i tre centrale niveauer:

- Taktikker (angriberens mål)
- Teknikker (metoder til at opnå målet)
- Procedurer (konkrete implementeringer af teknikker)

Formålet er at skabe et fælles sprog og en analytisk struktur til at beskrive, kategorisere og analysere angriberadfærd.

Se mere god information: https://26f-its-syssec-378707.gitlab.io/exercises/49_Mitre_ATT_CK/

TTP'er som abstraktionsniveauer

TTP'er (Taktik, Teknik og Procedure) kan forstås som tre forskellige abstraktionsniveauer, der strukturerer angriberadfærd.

```
Taktik → Teknik → Procedure
(mål)   (metode)   (konkret handling)
```

Disse niveauer gør det muligt at bevæge sig mellem det konkrete og det overordnede:

- Proceduren er det observerbare spor i systemet
- Teknikken beskriver metoden bag handlingen
- Taktikken repræsenterer angriberens overordnede mål

Analyse i systemsikkerhed starter typisk med det konkrete (procedure) og bevæger sig opad mod teknik og taktik.

MITRE ATT&CK som analytisk ramme

Efter gennemgangen af TTP-strukturen kan vi nu se, hvordan rammeværket anvendes i praksis.

Analyse med MITRE bevæger sig typisk gennem tre niveauer:

Operationelt niveau

Vi starter med det observerbare – proceduren.
Det kan være en kommando, en ændring i filrettigheder eller en loghændelse.

Taktisk niveau

Herefter kategoriseres handlingen:

- Hvilken teknik beskriver adfærden?

- Hvilken taktik understøtter den?

Strategisk niveau

Til sidst vurderes den bredere betydning:

- Hvilke trusselsaktører anvender teknikken?
- Hvor relevant er den i vores kontekst?
- Skal vi prioritere mitigering, detektion eller begge?

Instruktioner

I skal nu anvende rammeværket ved at udforske MITRE ATT&CK database gennem en række undersøgelser.

Undersøg TA0004 – Privilege Escalation

1. Hvad beskriver denne taktik?
   - Hvilket overordnet mål har angriberen?
   - Hvor i et angrebsforløb kan den forekomme?
   - Undersøg T1548 – Abuse Elevation Control Mechanism
2. Hvad beskriver teknikken?
   - Hvilke underteknikker findes?
   - Hvilke systemmekanismer kan misbruges?
   - Undersøg M1026 – Privilege Separation
3. Hvad er formålet med denne mitigering?
   - Hvordan relaterer den sig til T1548?
   - Undersøg relationen mellem ATT&CK og CTI
4. Hvad kan man finde om grupper i ATT&CK?
   - Hvad betyder APT?
   - Hvordan relaterer grupper sig til teknikker?

Løsning

1. Undersøg TA0004 – Privilege Escalation
   - Hvad beskriver denne taktik?
     - Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network.

- Hvilket overordnet mål har angriberen?
  - The adversary is trying to gain higher-level permissions.
- Hvor i et angrebsforløb kan den forekomme?
  - Common approaches are to take advantage of system weaknesses, misconfigurations, and vulnerabilities
- Undersøg T1548 – Abuse Elevation Control Mechanism
  - Abuse Elevation Control Mechanism, Technique T1548 - Enterprise | MITRE ATT&CK®
  - Hvad beskriver teknikken?
    - Adversaries may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions
- Hvilke underteknikker findes?

Sub-techniques (6)

ID	Name
T1548.001	Setuid and Setgid
T1548.002	Bypass User Account Control
T1548.003	Sudo and Sudo Caching
T1548.004	Elevated Execution with Prompt
T1548.005	Temporary Elevated Cloud Access
T1548.006	TCC Manipulation

- Hvilke systemmekanismer kan misbruges?

ID	Mitigation	Description
M1047	Audit	Check for common UAC bypass weaknesses on Windows systems to be aware of the risk posture and address issues where appropriate.[7]
M1038	Execution Prevention	System settings can prevent applications from running that haven't been downloaded from legitimate repositories which may help mitigate some of these issues. Not allowing unsigned applications from being run may also mitigate some risk.
M1028	Operating System Configuration	Applications with known vulnerabilities or known shell escapes should not have the setuid or setgid bits set to reduce potential damage if an application is compromised. Additionally, the number of programs with setuid or setgid bits set should be minimized across a system. Ensuring that the sudo tty_tickets setting is enabled will prevent this leakage across tty sessions.
M1026	Privileged Account Management	Remove users from the local administrator group on systems. By requiring a password, even if an adversary can get terminal access, they must know the password to run anything in the sudoers file. Setting the timestamp_timeout to 0 will require the user to input their password every time sudo is executed.
M1022	Restrict File and Directory Permissions	The sudoers file should be strictly edited such that passwords are always required and that users can't spawn risky processes as users with higher privilege.
M1051	Update Software	Perform regular software updates to mitigate exploitation risk.
M1052	User Account Control	Although UAC bypass techniques exist, it is still prudent to use the highest enforcement level for UAC when possible and mitigate bypass opportunities that exist with techniques such as DLL.
M1018	User Account Management	Limit the privileges of cloud accounts to assume, create, or impersonate additional roles, policies, and permissions to only those required. Where just-in-time access is enabled, consider requiring manual approval for temporary elevation of privileges.

2. Undersøg M1026 – Privilege Separation
    - https://attack.mitre.org/mitigations/M1026/
    - Hvad er formålet med denne mitigering?
        - Privileged Account Management focuses on implementing policies, controls, and tools to securely manage privileged accounts (e.g., SYSTEM, root, or administrative accounts)
    - Hvordan relaterer den sig til T1548?
        - Den forebygger det, som T1548 vil udnytte.
3. Undersøg relationen mellem ATT&CK og CT
    - Hvad kan man finde om grupper i ATT&CK
        - For hver "Group" kan man typisk finde:
            - Alias/navne brugt af forskellige leverandører
            - Motivation og mål
            - Kendte kampagner/operationer
            - Anvendte teknikker (med evidens fra observationer)
            - Anvendt software/værktøjer
            - Beskrivelse af adfærd og TTP'er (tactics, techniques, procedures)
            - Eksempel på gruppe: APT28
    - Hvad betyder APT?
        - APT = Advanced Persistent Threat
            - Advanced: avancerede, tilpassede metoder
            - Persistent: langvarig, målrettet tilstedeværelse
            - Threat: organiseret og kapabel aktør (ofte statssponsoreret)
    - Hvordan relaterer grupper sig til teknikker?
        - ATT&CK dokumenterer hvilke **teknikker** konkrete **grupper** har anvendt i virkelige angreb.
        - Relation: Gruppe anvender **teknik** for at opnå **taktik**.
        - Praktisk anvendelse:
            - Man kan prioritere forsvar og detection ud fra de teknikker, en bestemt gruppe historisk bruger.

Refleksionsspørgsmål

- Hvad er forskellen på taktik, teknik og procedure?
  - **Proceduren** er det observerbare spor i systemet
  - **Teknikken** beskriver metoden bag handlingen
  - **Taktikken** repræsenterer angriberens overordnede mål
- Hvorfor er det nyttigt at strukturere angriberadfærd?
  - For at man forstår de angrebsvektorer, som trusselsaktørerer anvender, så man bedst muligt kan forebygge imod angreb.
- Hvordan kan MITRE ATT&CK hjælpe med at skabe overblik?
  - Fordi at det er en systematiseret strukturering af adfærdsmønstre, der er observeret og dokumenteret gennem CTI.
- Hvordan hænger ATT&CK og CTI sammen?
  - **CTI** beskriver *trusselsaktører*, deres mål og observerede angreb.
    - CTI-fund mappes til ATT&CK for at gøre angriberadfærd sammenlignelig
  - **ATT&CK&** strukturer denne viden om standardiserede taktikker og teknikker.

Ressourcer

- https://26f-its-syssec-378707.gitlab.io/exercises/49_Mitre_ATT_CK/

2026-02-20 08:38:27