Øvelse 49 – (Eftermiddagsgruppeøvelse) Mitre ATT&CK: Taktikker, Teknikker, Mitigering og Detektering

Formål

Formålet med denne øvelse er at opnå praktisk forståelse for, hvordan **Mitre ATT&CK-rammeværket** kan bruges til at analysere angribernes metoder og opbygge modforanstaltninger. Øvelsen fokuserer på **Privilege Escalation** (TA0004) og den relaterede teknik **T1548**, samt relevante **mitigeringer (M1026)** og **detekteringsstrategier (DS0022)**.

Baggrund

Mitre ATT&CK er et globalt rammeværk, der dokumenterer taktikker, teknikker og procedurer (TTP'er), som trusselsaktører bruger til at gennemføre angreb. Rammeværket bruges i både offensiv og defensiv cybersikkerhed – fx til trusselsmodellering, incident response, detection engineering og sikkerhedsstrategi.

I denne øvelse skal I i grupper analysere én af de mest kritiske taktikker: **Privilege Escalation**, dvs. når en angriber forsøger at få højere privilegier på et system (fx administrator/root).

Instruktioner

1. **Undersøg taktikken TA0004 – Privilege Escalation**
2. Hvad dækker denne taktik over?
3. Hvorfor er det et centralt mål for angribere?
4. Hvordan hænger det sammen med resten af ATT&CK-processen?
5. **Undersøg teknikken T1548 – Abuse Elevation Control Mechanism**
6. Hvilke underteknikker findes under T1548?
7. Hvordan fungerer de i praksis?
8. Find eksempler fra virkelige angreb eller testmiljøer.
9. **Undersøg mitigeringen M1026 – Privilege Separation**
10. Hvad går denne mitigering ud på?

11. Hvordan begrænser eller forhindrer den Privilege Escalation?
12. Hvilke typer kontroller og politikker kan anvendes?
13. **Undersøg detekteringen DS0022 – File Monitoring**
14. Hvordan bruges denne detektering til at opdage eskaleringsforsøg?
15. Hvilke værktøjer (fx Wazuh, auditd, Sysmon) kan implementere denne detektering?
16. **Forbered en kort præsentation (maks. 5 minutter)**
    Jeres præsentation skal indeholde:
17. En forklaring på **Privilege Escalation-taktikken** og hvorfor den er vigtig
18. En oversigt over **T1548 og dens underteknikker**
19. En gennemgang af **M1026** og hvordan den implementeres
20. En beskrivelse af **DS0022** og hvordan den anvendes til detektering

> Fokusér på at formidle jeres pointer klart og overskueligt. Brug evt. slides eller whiteboard.

Nyttige links

- Mitre ATT&CK Framework Overview
- TA0004 – Privilege Escalation
- T1548 – Abuse Elevation Control Mechanism
- M1026 – Privilege Separation
- DS0022 – File Monitoring

Refleksionsspørgsmål

- Hvordan kan rammeværket bruges til at prioritere forsvar mod forskellige angrebstyper?
- Hvordan kunne man forbinde teknikken T1548 til konkrete hændelser i logfiler eller SIEM?
- Hvad er forskellen på mitigering og detektering i ATT&CK-kontekst – og hvorfor er begge vigtige?
- Hvilke fordele giver det at arbejde taktisk i forhold til sikkerhedsforanstaltninger?

2025-04-03 05:55:59