Adversary Simulation with MITRE CALDERA

Marko Sokser, Luka Šulentić, Luka Kukec, Luka Hrupec

Uvod i koncept

- Dizajn i izvedba simuliranog kibernetičkog napada na virtualnu enterprise mrežu koristeći MITRE CALDERA
- Osnovni koncept je primjena Red/Blue Team metodologije, gdje jedan dio tima napada sustav (Red Team), a drugi ga brani i analizira napad (Blue Team).
- Svrha projekta je sustavna evaluacija učinkovitosti implementiranih sigurnosnih kontrola.

Ciljevi projekta

- Steći praktično iskustvo s emulacijom protivnika i Red/Blue Team radnim procesima.
- Naučiti postaviti i osigurati realistično enterprise okruženje, uključujući servere i radne stanice.
- Mapirati tehnike napada izvedene pomoću alata CALDERA na MITRE ATT&CK framework.
- Procijeniti učinkovitost sigurnosnih kontrola u detekciji i prevenciji specifičnih napada.
- Razviti tehničku dokumentaciju i izvještaj o incidentima.

Arhitektura okruženja

Potrebno:

1. Domain Controller (Windows Server)
2. Windows Workstation (Windows 11 – korisnik koji se napada)
3. Linux Server (Ubuntu Server)
4. CALDERA Operator VM (Ubuntu sa CALDERA serverom i agentom)
5. Logging / SIEM VM (Wazuh, Splunk)
6. Network Firewall (pfSense)

Ranjivosti

Uvodit će se namjerne ranjivosti:

1. Zastarjeli software
2. Slabe lozinke
3. Loša konfiguracija mreže (otvoreni nepotrebni portovi, slabo segmentirana mreža...)
4. Loša enkripcija podataka

Cilj: Stvoriti realistične napade

Plan rada po ulogama

Infrastructure Engineer

1. Izgradnja cijelog virtualnog okruženja (VM-ovi, mreža, domene).
2. Konfiguracija:
    a) AD domena, korisnički računi, grupne politike
    b) Linux server (servisi, SSH hardening)
    c) pfSense, segmentacija, osnovna pravila
3. Osigurati logging pipeline: Windows Event Forwarding, syslog prema SIEM-u
4. Jake lozinke, onemogućavanje guest/root, osnovne sigurnosne postavke

Blue Team Engineer

Implementacija višeslojne obrane:

1. Firewall: Konfiguracija pravila i prosljeđivanje logova u SIEM.
2. IDS/IPS: Instalacija na dedicated VM. Ažuriranje skupova pravila.
3. EDR (Wazuh): Postavljanje agenata na Windows i Linux hostove. Praćenje sumnjivih PowerShell aktivnosti, promjena u registru
4. SIEM (Splunk): Centralno prikupljanje svih logova (firewall, IDS/IPS, Wazuh, OS logovi

Plan rada po ulogama

Red team operator

Faza 1 - Planiranje i priprema:

a) Analiza mete u dogovoru s Infrastructure Engineerom.
b) Odabir scenarija
c) Dizajn višefazne kampanje
d) Kreiranje adversary profila u CALDERA-i

Faza 2 - Izvođenje i dokumentacija

Faza 3 - Analiza rezultata: suradnja s Threat Hunterom i Blue timom na izradi Attack–Defense matrice

Faza 4 - Re-run nakon pojačanja obrane

Threat Hunter/Analyst

1. Priprema i provjera telemetrije: Osigurati da je prikupljanje svih relevantnih logova pravilno konfigurirano.
2. Izrada detekcijskih pravila: Razvoj tri specifična pravila za detekciju napadačkih tehnika.
3. Aktivni nadzor: Pokretanje pretraga i analiza događaja u stvarnom vremenu tijekom CALDERA kampanje.
4. Prikupljanje dokaza: Bilježenje artefakata napada (snimke nadzornih ploča, izvoz sirovih logova).

Tijek projekta

Postavljanje okruženja i priprema obrane i postavljanje logginga

Prva CALDERA kampanja

Analiza i Attack–Defense matrica

Pojačavanje obrane

Re-run prve CALDERA kampanje

Analiza

Izrada finalne dokumentacije

Prezentacija projekta

Očekivani problemi

- Instalacija i kompatibilnost alata (CALDERA, Wazuh, IDS, Splunk).
- Prava i privilegije (admin pristup, portovi, agenti).
- Mrežna izolacija i firewall mogu blokirati CALDERA komunikaciju.
- Lažno pozitivni alarmi (False Positives).
- Prevelika količina logova (šum).

Potencijalna rješenja:

- Pravilno planiranje i dokumentacija verzija alata, korištenje snapshotova
- Fazno testiranje povezanosti i firewall pravila prije simulacije
- Kreiranje baselinea normalnog prometa i fino podešavanje (tuning) detekcijskih pravila i filtera za logove kako bi se smanjio šum i lažni alarmi.

Hvala na pažnji!