Ofenzivna sigurnost

Alati za emulaciju napadača: MITRE Caldera, Atomic Red Team

Marko Lipovac, 26.1.2026.

Pregled predavanja

- Motivacija
- Općenito o alatima za emulaciju napada
- MITRE ATT&CK
- Atomic Red Team
- MITRE Caldera
- Zaključak

Motivacija

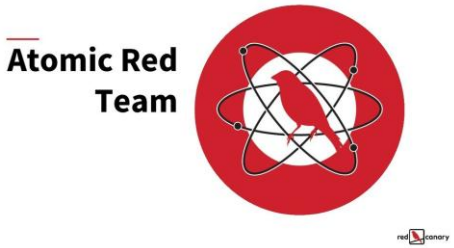
- Napadi su višefazni i složeni
- Teško razumijevanje ponašanja napada nakon početnog pristupa
- Ručno testiranje napada je sporo i teško skalabilno
- Nepoznavanje hoće li određene tehnike funkcionirati u stvarnom okruženju

Pitanja za ispite

- Što omogućuju alati za emulaciju napada?
- Što je Atomic Red Team?
- Nabroji četiri glavna elementa MITRE Caldera operacije.
- Koje su glavne razlike između Atomic Red Team i MITRE Caldera?
- Koja su ograničenja alata za emulaciju napadača?

Alati za emulaciju napadača

- Simuliraju ponašanja stvarnih napadača
- Oponašaju poznate taktike, tehnike i postupke (TTP)
- Najpoznatiji alati
  - MITRE Caldera
  - Atomic Red Team
  - Mordor



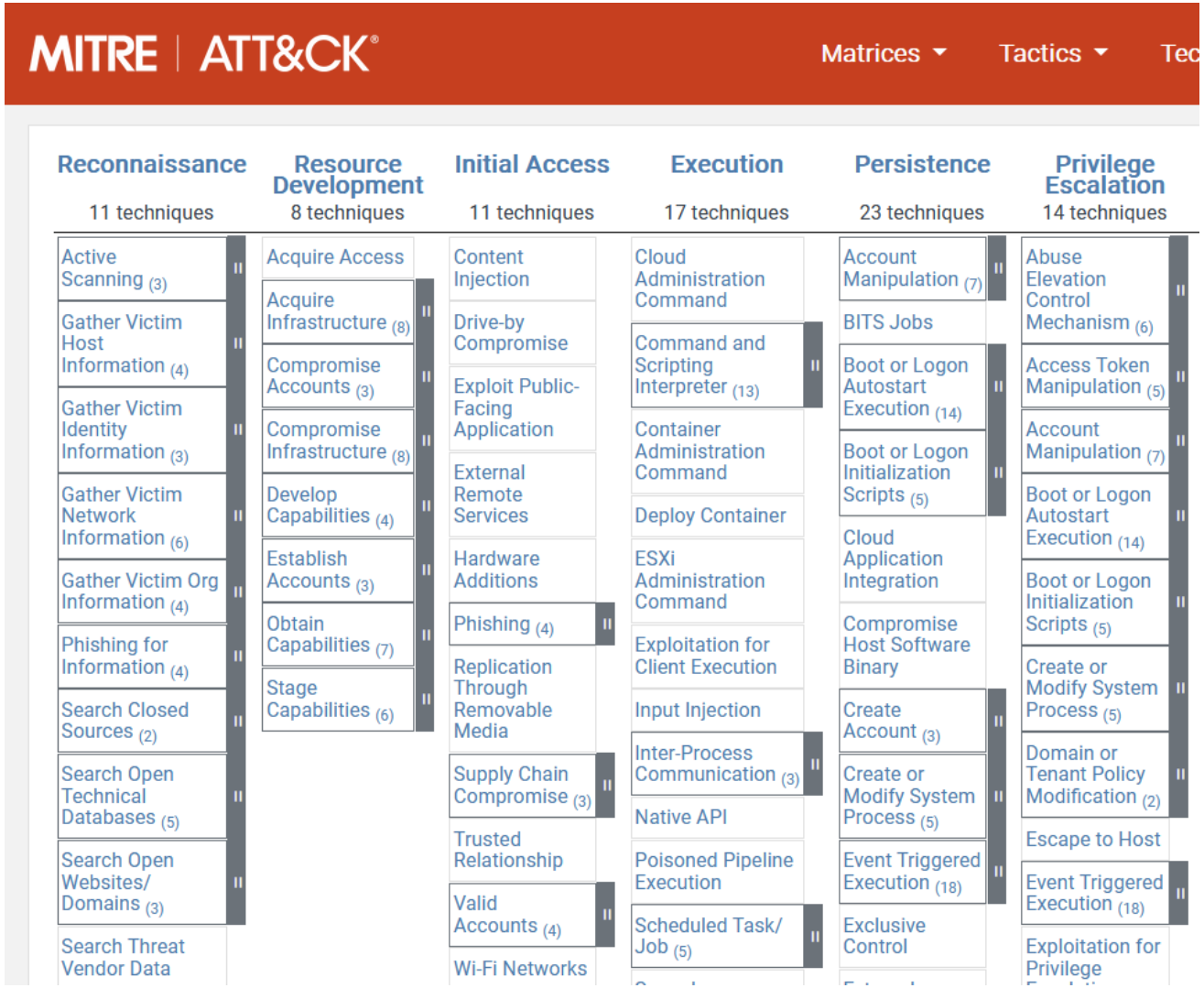
MITRE
CALDERA

Alati za emulaciju napadača

- Omogućuju realističnu simulaciju napada
- Pomažu u razumijevanju kako napadi napreduju nakon početnog pristupa
- Omogućuju ponovljivo i kontrolirano izvođenje napadačkih scenarija
- Koriste se za uvježbavanje i usavršavanje ofenzivne sigurnosne strategije
- Pomažu vidjeti kako sustav reagira na napade

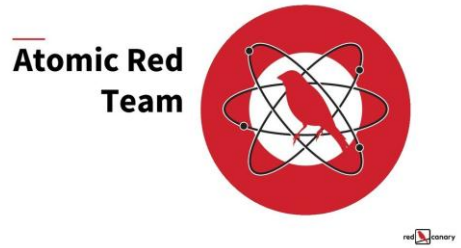
MITRE ATT&CK

- Okvir znanja koji opisuje kako stvarni napadači provode napade
- Temeljen na stvarnim napadima
- Svaka taktika i tehnika ima svoj ID



Atomic Red Team

- Zbirka malih, pojedinačnih ATT&CK tehnika
- Testovi su jednostavni i brzo izvedivi
- Fokus na pojedinačne akcije napadača, a ne na cijeli napad



Atomic Red Team

- T1016 - System Network Configuration Discovery
- „ShowDetailsBrief” – pokazuje pregled akcija koje tehnika koristi

```
PS C:\Users\destroy> Invoke-AtomicTest T1016 -ShowDetailsBrief
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

T1016-1 System Network Configuration Discovery on Windows
T1016-2 List Windows Firewall Rules
T1016-4 System Network Configuration Discovery (TrickBot Style)
T1016-5 List Open Egress Ports
T1016-6 Adfind - Enumerate Active Directory Subnet Objects
T1016-7 Qakbot Recon
```

- Opcija „-ShowDetails” pokazuje što i kako napad funkcionira
- Mogu se vidjeti sve naredbe koje su korištene

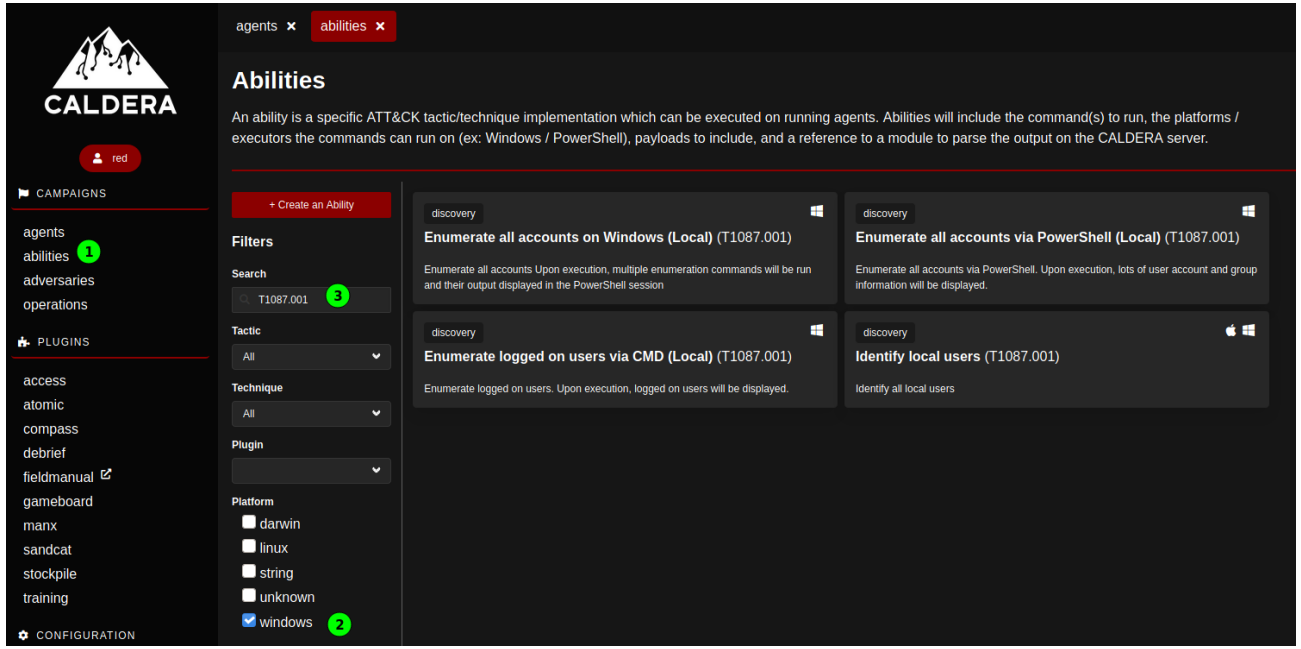
```
PS C:\Users\destroy> Invoke-AtomicTest T1016 -ShowDetails
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

[********BEGIN TEST*******]
Technique: System Network Configuration Discovery T1016
Atomic Test Name: System Network Configuration Discovery on Windows
Atomic Test Number: 1
Atomic Test GUID: 970ab6a1-0157-4f3f-9a73-ec4166754b23
Description: Identify network configuration information
Upon successful execution, cmd.exe will spawn multiple commands to
ill be via stdout.

Attack Commands:
Executor: command_prompt
ElevationRequired: False
Command:
ipconfig /all
netsh interface show interface
arp -a
nbtstat -n
net config
[!!!!!!!!END TEST!!!!!!!]


[********BEGIN TEST*******]
```

Atomic Red Team

- Omogućuje testiranje i provjeru napadačkih tehnika
- Pomaže u razumijevanju kako pojedine tehnike funkcioniraju u praksi
- Koristi se za pripremu i uvježbavanje napadačkih scenarija

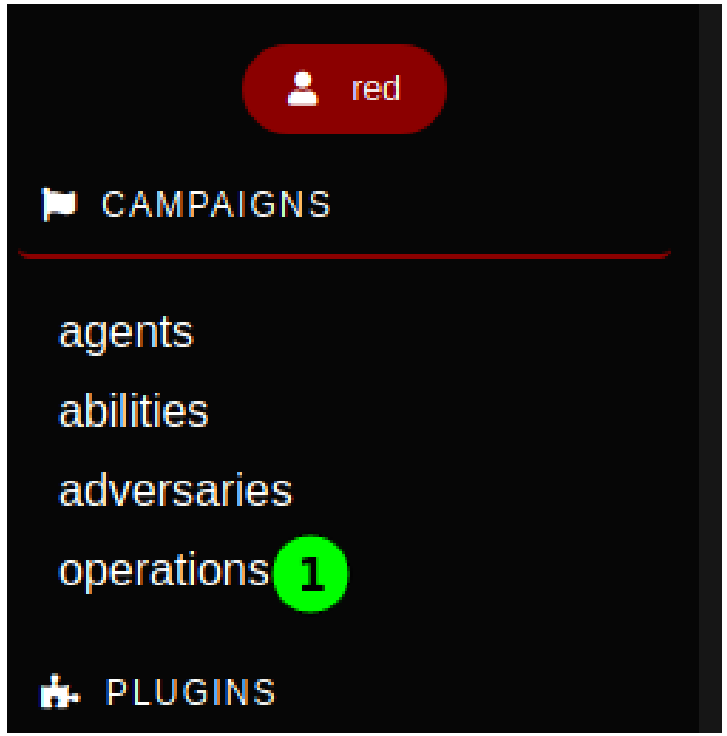
MITRE Caldera

- Automatizira izvođenje napadačkih tehnika
- Omogućuje ulančanje više faza napada

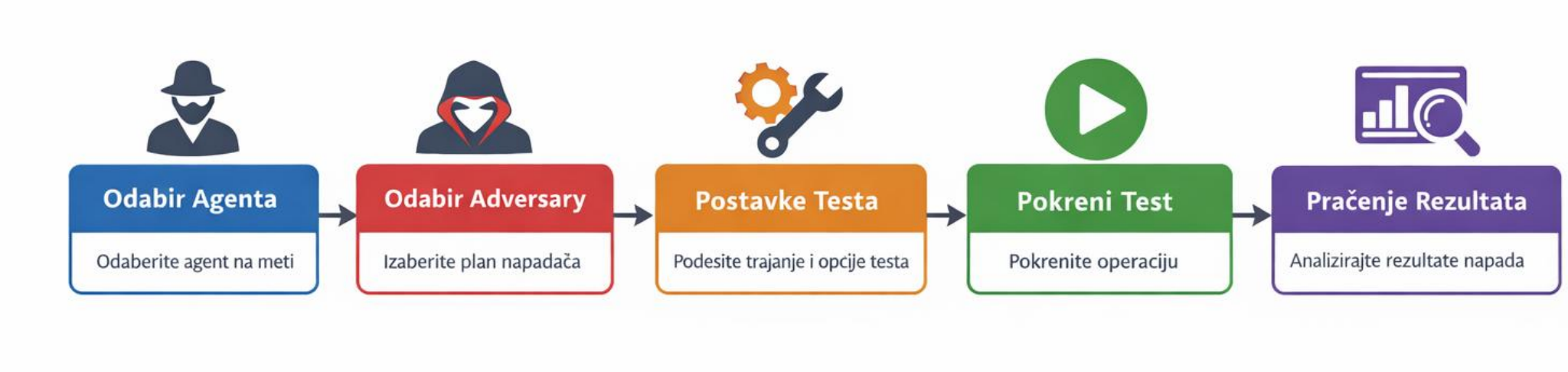


MITRE Caldera – glavni elementi

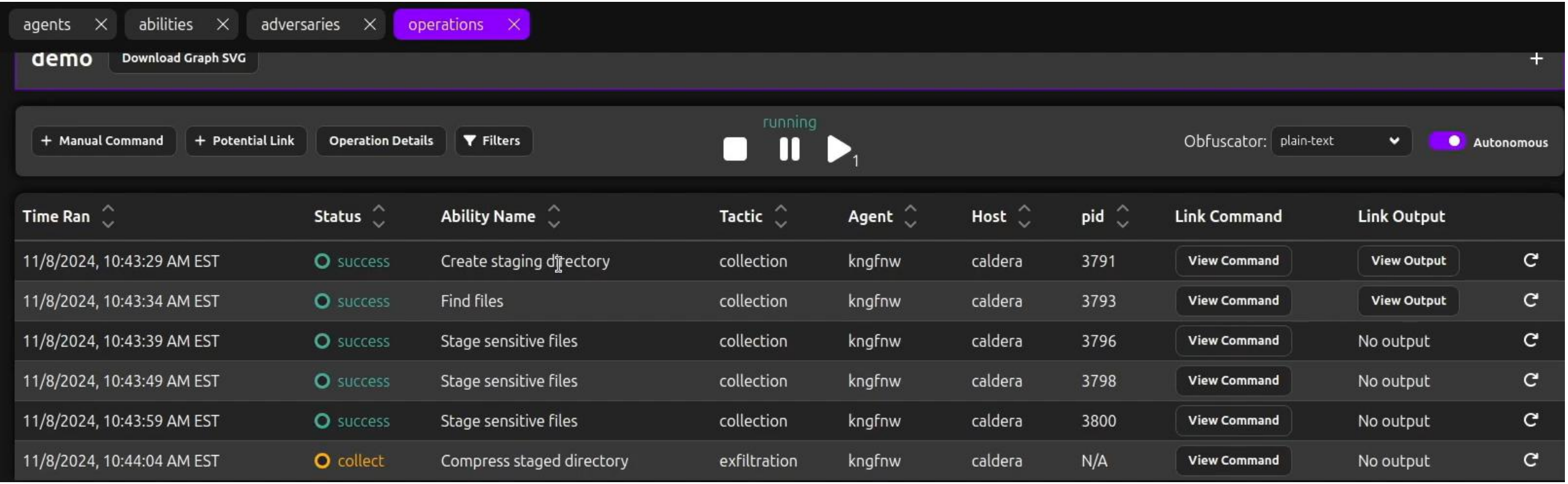
- Agenti – predstavljaju kompromitirane sustave
- Tehnike – pojedinačne ATT&CK tehnike (preko 1800 pojedinačnih tehnika)
- „Adversaries” – model napadača (plan)
- Operacije – povezane napadačke aktivnosti



MITRE Caldera –pregled



MITRE Caldera – UI prikaz



MITRE Caldera

- Omogućuje ponovljive i kontrolirane napade
- Smanjuje potrebu za ručnim izvođenjem tehnika -> smanjuje cijenu
- Pomaže u razumijevanju cijelog tijeka napada
- Nadograđuje alate poput ART-a (Atomic Red Team) automatizacijom

Automatizacija

- Zašto se automatizira
  - Skaliranje napadačke operacije
  - Smanjio ručni rad
  - Povećala dosljednost napada
- Pomicanje uloge operatora sa izvođenja na donošenje odluka
  - odabir ciljeva, prilagodba strategije…

ART vs Caldera

- Atomic Red Team
  - Testiranje na razini pojedinačnih tehnika
  - Odgovara na pitanje: „Radi li ova ranjivost?”
  - Jednostavnija
- MITRE Caldera
  - Izvođenje napada na razini kampanje
  - Odgovara na pitanje: „Kako dolazimo do cilja?”
  - Kompliciranija

Ograničenja

- Fokusiraju se na faze napada gdje je uspostavljen početni pristup
- Alati za emuliranje napadača ne mogu
  - Razumjeti kontekst okruženja
  - Donijeti odluke na temelju nepredviđenih situacija
  - Stvoriti nova rješenja
- ART testovi su jednostavni
  - često koriste „sirove” naredbe (Powershell) koje moderni sustavi lagano prepoznaju

Zaključak

- Alati značajno pomažu automatizaciji, učenju i pripremi napada
- Omogućuju ponovljive i realistične simulacije
- Međutim, ne mogu zamijeniti ljudsku kreativnost i iskustvo
- Uspješna ofenzivna sigurnost zahtijeva kombinaciju alata i operatera

Literatura

- MITRE Caldera, "*MITRE Caldera v5 – Basics – 2 – Overview*," **YouTube**, 12.2.2025. Dostupno: https://www.youtube.com/watch?v=W7fi0RVYiJE. [Pristupljeno: 26.1.2026].
- J. B., "Comparing open source adversary emulation platforms for red teams," *Red Canary Blog*, 2026. Dostupno: https://redcanary.com/blog/testing-and-validation/atomic-red-team/comparing-red-team-platforms/. [Pristupljeno: 26.1.2026].
- CyberSecurityUP, "*Adversary-Emulation-Guide*," **GitHub**. Dostupno: https://github.com/CyberSecurityUP/Adversary-Emulation-Guide. [Pristupljeno: 26.1.2026].
- Cyber Peachh, "*How to Setup and Generate Attacks with Atomic Red Team / Let's Drop Bombs* 💣," **YouTube**, 27.7.2022. Dostupno: https://www.youtube.com/watch?v=_xW3fAumh1c. [Pristupljeno: 26.1.2026].

Dodatna literatura

- MITRE, “*MITRE Caldera*,” *Caldera.mitre.org*. Dostupno: https://caldera.mitre.org/. [Pristupljeno: 26.1.2026].
- redcanaryco, “*Atomic Red Team*,” **GitHub**. Dostupno: https://github.com/redcanaryco/atomic-red-team. [Pristupljeno: 26.1.2026].
- MITRE, “*MITRE ATT&CK®*,” *Attack.mitre.org*. Dostupno: https://attack.mitre.org/. [Pristupljeno: 26.1.2026].

Hvala!