

## **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

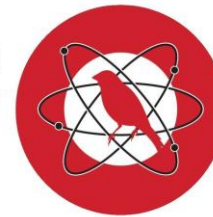
- Što omogućuju alati za emulaciju napada?
- Što je Atomic Red Team?
- Nabroji četiri glavna elementa MITRE Caldera operacije.
- Koje su glavne razlike između Atomic Red Team i MITRE Caldera?
- Koja su ograničenja alata za emulaciju napadača?

# Alati za emulaciju napadača

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



Atomic Red  
Team



redteam



# 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

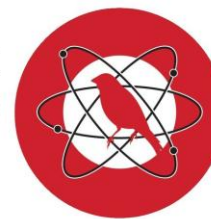
- Okvir znanja koji opisuje kako stvarni napadači provode napade
- Temeljen na stvarnim napadima
- Svaka taktika i tehnika ima svoj ID

MITRE   ATT&CK®					
Matrices ▾ Tactics ▾ Tec					
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation
11 techniques	8 techniques	11 techniques	17 techniques	23 techniques	14 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (13)	BITS Jobs	Access Token Manipulation (5)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (7)
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	ESXi Administration Command	Cloud Application Integration	Boot or Logon Initialization Scripts (5)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Exploitation for Client Execution	Compromise Host Software Binary	Create or Modify System Process (5)
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Input Injection	Create Account (3)	Domain or Tenant Policy Modification (2)
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Inter-Process Communication (3)	Create or Modify System Process (5)	Escape to Host
Search Open Websites/ Domains (3)		Trusted Relationship	Native API	Event Triggered Execution (18)	Event Triggered Execution (18)
Search Threat Vendor Data		Valid Accounts (4)	Poisoned Pipeline Execution	Exclusive Control	Exploitation for Privilege
		Wi-Fi Networks	Scheduled Task/ Job (5)		

# 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



red team



# 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 funkcioniра
- 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!!!!!!]

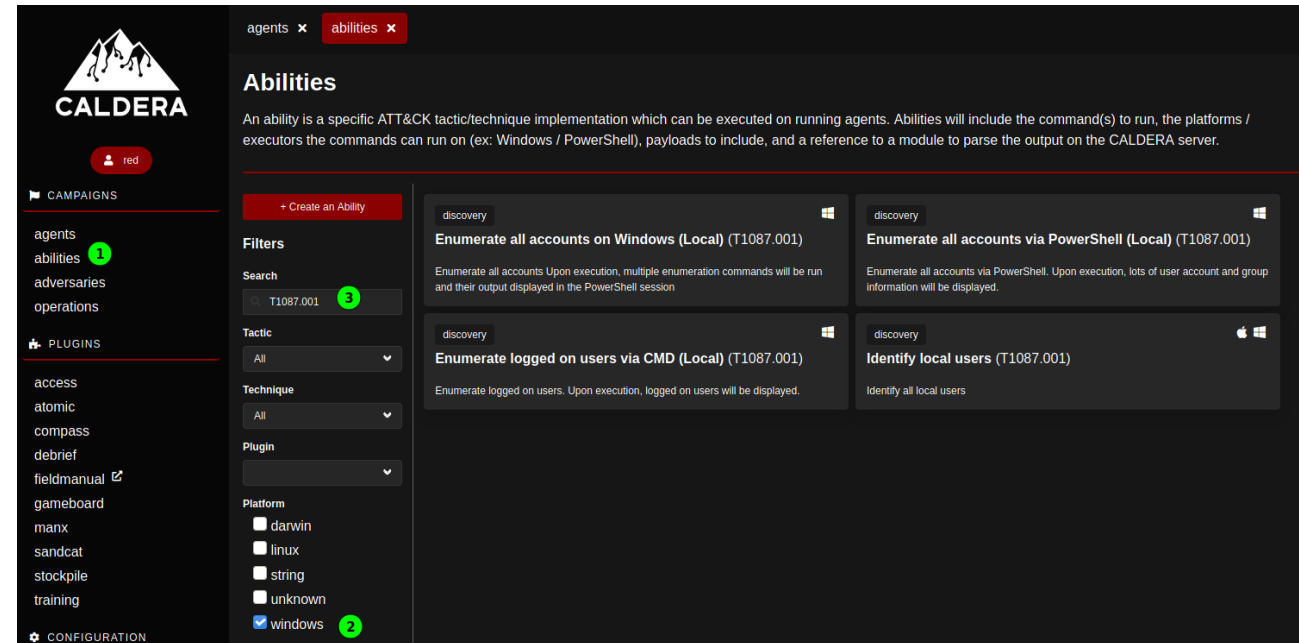
[*****BEGIN TEST*****]
```

# 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

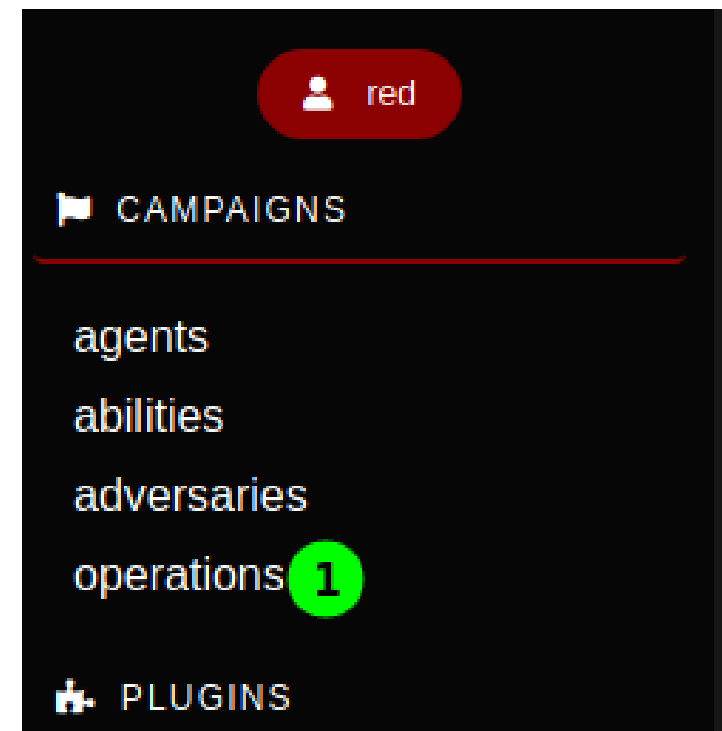
# MITRE Caldera

- 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







agents × abilities × adversaries × operations ×

demo Download Graph SVG +

+ Manual Command + Potential Link Operation Details Filters

running  1

Obfuscator: plain-text ▼ ☒ Autonomous

Time Ran	Status	Ability Name	Tactic	Agent	Host	pid	Link Command	Link Output
11/8/2024, 10:43:29 AM EST	success	Create staging directory	collection	kngfnw	caldera	3791	<a href="#">View Command</a>	<a href="#">View Output</a> 
11/8/2024, 10:43:34 AM EST	success	Find files	collection	kngfnw	caldera	3793	<a href="#">View Command</a>	<a href="#">View Output</a> 
11/8/2024, 10:43:39 AM EST	success	Stage sensitive files	collection	kngfnw	caldera	3796	<a href="#">View Command</a>	No output 
11/8/2024, 10:43:49 AM EST	success	Stage sensitive files	collection	kngfnw	caldera	3798	<a href="#">View Command</a>	No output 
11/8/2024, 10:43:59 AM EST	success	Stage sensitive files	collection	kngfnw	caldera	3800	<a href="#">View Command</a>	No output 
11/8/2024, 10:44:04 AM EST	collect	Compress staged directory	exfiltration	kngfnw	caldera	N/A	<a href="#">View Command</a>	No output 

# 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?”
  - Komplikiranija

# 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](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!