

Ejercicio 2: Trasladando TTPs a CALDERA para Simulación

Contexto del Ejercicio

En el ejercicio anterior, utilizamos **MITRE ATT&CK Navigator** para identificar tácticas y técnicas de un ataque simulado, analizar la cobertura actual de nuestras herramientas y proponer mejoras.

Ahora, vamos a trasladar esas técnicas a **CALDERA**, una plataforma de simulación de adversarios, para realizar una simulación práctica que permita validar nuestras detecciones y respuestas.

Objetivo

Configurar una simulación en **CALDERA** que utilice las tácticas y técnicas del Ejercicio 1 para evaluar la capacidad de detección y respuesta del entorno corporativo.

Tácticas y Técnicas Para Simular

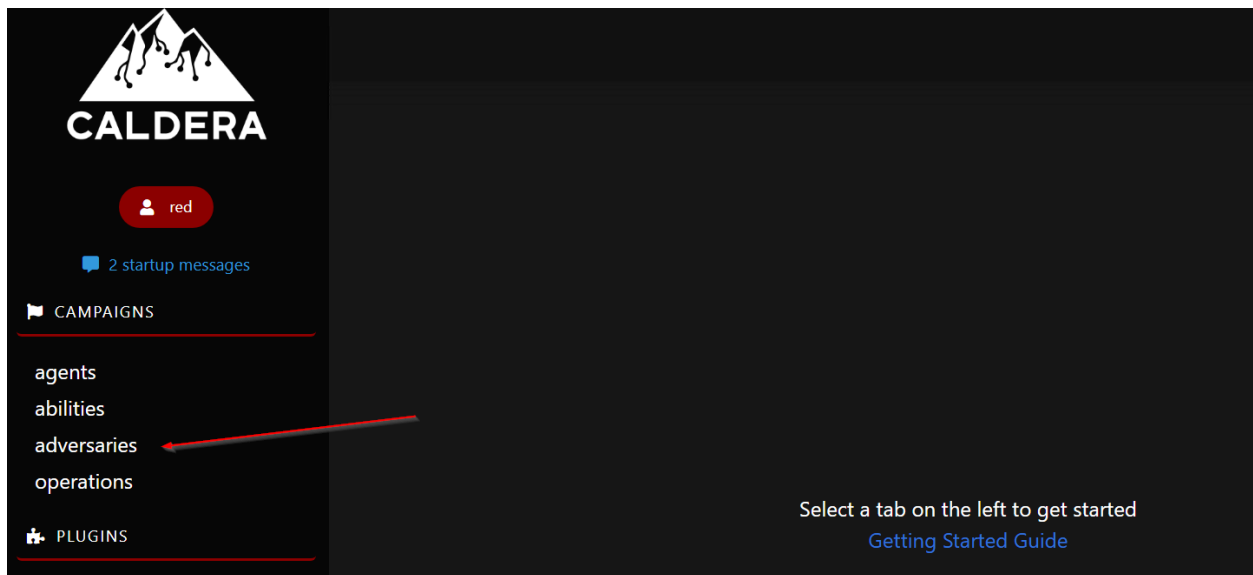
Tactic	Technique	MITRE ID
Initial Access	Spearphishing Attachment	T1566.001
Execution	User Execution: Malicious File	T1204.002
Persistence	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001
Privilege Escalation	Process Injection: Dynamic-link Library Injection	T1055.001
Defense Evasion	Obfuscated Files or Information: Command Obfuscation	T1027.010
	Impair Defenses: Disable or Modify Tools	T1562.001
	Indicator Removal on Host	T0872
Credential Access	OS Credential Dumping: LSASS Memory	T1003.001
Lateral Movement	Use Alternate Authentication Material: Pass the Hash	T1550.002
	Remote Services: SMB/Windows Admin Shares	T1021.002
Impact	Data Encrypted for Impact	T1486

Instrucciones del Ejercicio

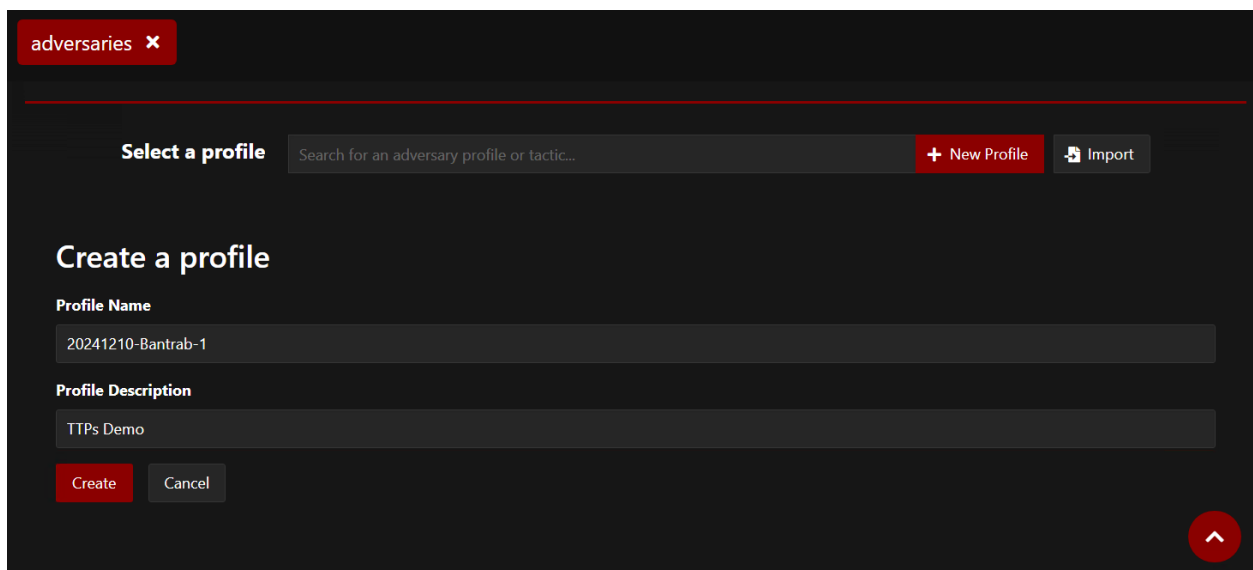
Preparación

1. Configuración inicial:

- Acceder a la interfaz de CALDERA.
- Crear un nuevo perfil de adversario.



- Introduce un nombre descriptivo para el perfil, como: "20241210-Bantrab-1".

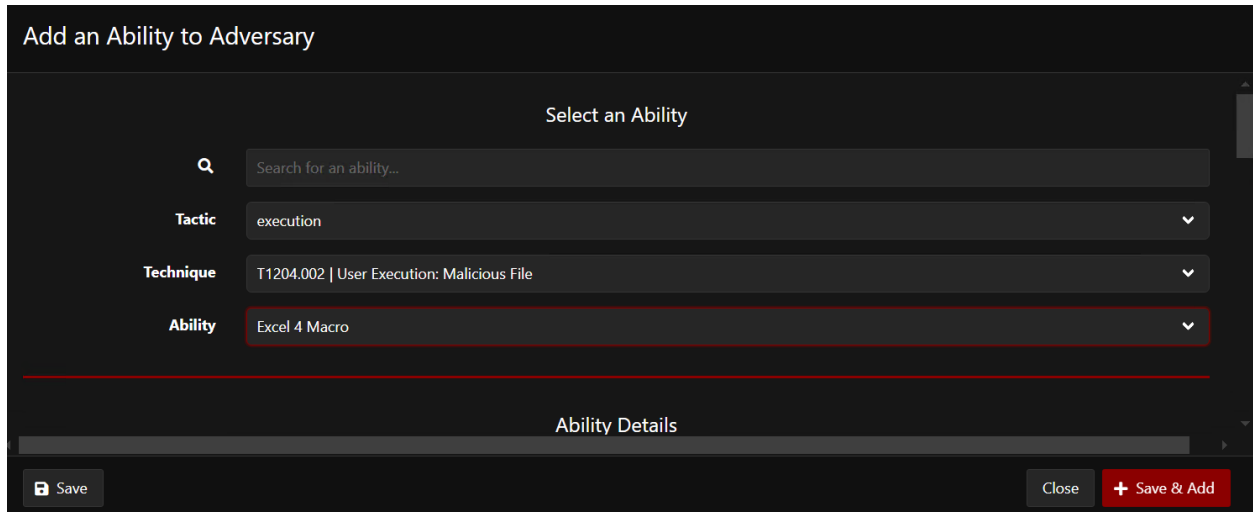


Creación del Perfil del Adversario

1. Agregar TTPs:

- Para cada técnica del ejercicio, selecciona la táctica correspondiente en el árbol de MITRE ATT&CK dentro de CALDERA.
- Añade las técnicas al perfil agregando los abilities necesarios.

1er ability, damos en botón save y add.



Add an Ability to Adversary

Select an Ability

Search for an ability...

Tactic execution

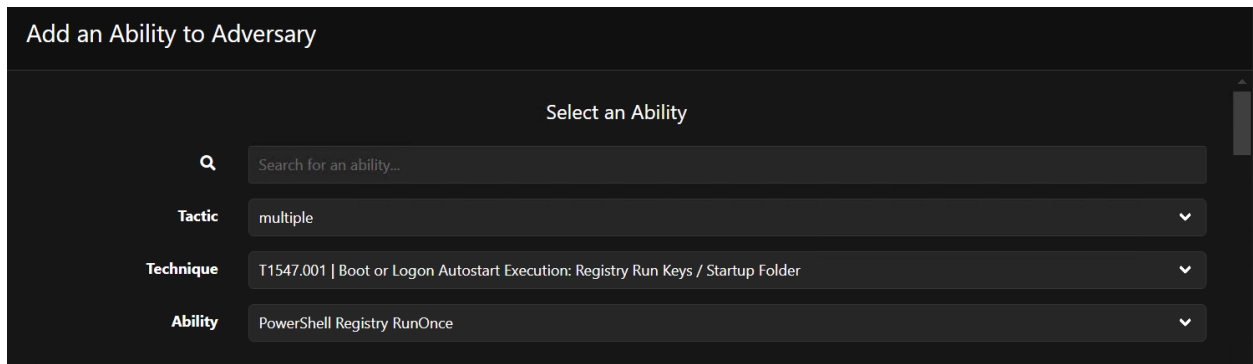
Technique T1204.002 | User Execution: Malicious File

Ability Excel 4 Macro

Ability Details

Save Close + Save & Add

2do ability



Add an Ability to Adversary

Select an Ability

Search for an ability...

Tactic multiple

Technique T1547.001 | Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

Ability PowerShell Registry RunOnce

3er ability

Add an Ability to Adversary

Select an Ability

Q

Search for an ability...

Tactic

multiple

▼

Technique

T1055.001 | Process Injection: Dynamic-link Library Injection

▼

Ability

WinPwn - Get SYSTEM shell - Bind System Shell using Usoclient DLL load technique

▼

Ability Details

Save

Close

+ Save & Add

4to ability

Add an Ability to Adversary

Select an Ability

Q

Search for an ability...

Tactic

defense-evasion

▼

Technique

T1027.007 | Obfuscated Files or Information: Dynamic API Resolution

▼

Ability

Dynamic API Resolution-Ninja-syscall

▼

Ability Details

Save

Close

+ Save & Add

5to ability

Add an Ability to Adversary

Select an Ability

Q

Search for an ability...

Tactic

defense-evasion

▼

Technique

T1562.001 | Impair Defenses: Disable or Modify Tools

▼

Ability

Uninstall Sysmon

▼

Ability Details

Save

Close

+ Save & Add

6to ability

Add an Ability to Adversary

Select an Ability

Search for an ability...

Tactic: defense-evasion

Technique: T1070 | Indicator Removal on Host

Ability: Indicator Removal using FSUtil

7mo ability

Add an Ability to Adversary

Select an Ability

Search for an ability...

Tactic: credential-access

Technique: T1003.001 | OS Credential Dumping: LSASS Memory

Ability: Dump LSASS.exe using imported Microsoft DLLs

8vo ability

Add an Ability to Adversary

Select an Ability

Search for an ability...

Tactic: multiple

Technique: T1550.002 | Use Alternate Authentication Material: Pass the Hash

Ability: Invoke-WMIExec Pass the Hash

Ejecución de la Simulación

1. Ejecutar el perfil del adversario:

- Selecciona el perfil creado en el paso anterior.
- Configura los agentes en los sistemas objetivo dentro del entorno de laboratorio.
- Iniciar la simulación y monitorear su ejecución en tiempo real.