

LIMACHARLIE 🐍



Objetivos de la Guía 🐍

- Instalar LimaCharlie
- Instalar un sensor en una maquina Windows
- Realizar pruebas con Atomic Red Team Maquina
- Visualizar los datos recopilados por el sensor de LimaCharlie

¿Que es LimaCharlie ?

LimaCharlie es una herramienta que permite administrar una infraestructura a nivel de ciberseguridad, permite tener una cobertura completa de lo que sucede en los distintos equipos de una determinada organización.

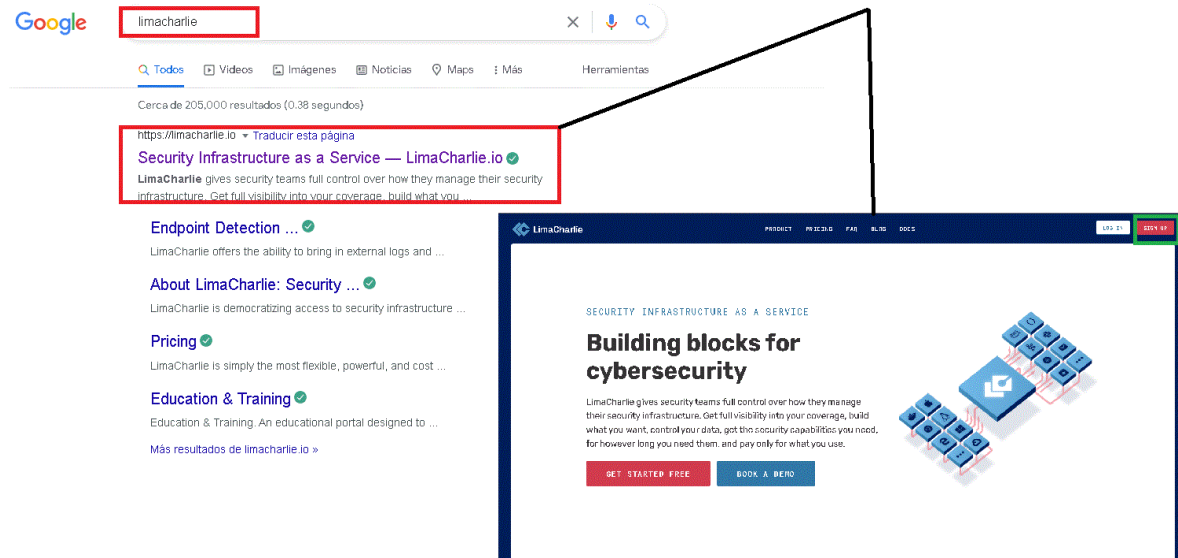
Requerimientos del Laboratorio

- VirtualBox <https://heyadvice.net/es/como-instalar-virtualbox-6-1-en-windows-10>
- Maquina Windows 10 Preferiblemente Virtual <https://www.ardilu.com/guias/instalar-windows-10-maquina-virtual>
- Maquina Ubuntu 20.0.4 con Atomic Red Team <https://github.com/redcanaryco/invoke-atomicredteam/wiki>
- Tener instalador Powershell 7 en la maquina Ubuntu
- Tener instalador Powershell 7 en la maquina Windows <https://www.thomasmaurer.ch/2020/04/enable-powershell-ssh-remoting-in-powershell-7/>

Pasos a seguir para instalar LimaCharlie en Windows 10

1. Registrarse en la plataforma de LimaCharlie

#Puedes registrarte con tu correo electrónico por medio de Gmail, Hotmail u otros.



2. A continuación, después de colocar tu correo lea los conceptos básicos sobre LimaCharlie y de Click en "Crear organización"

An Overview of LimaCharlie.

Before you get set up, here's the basics:

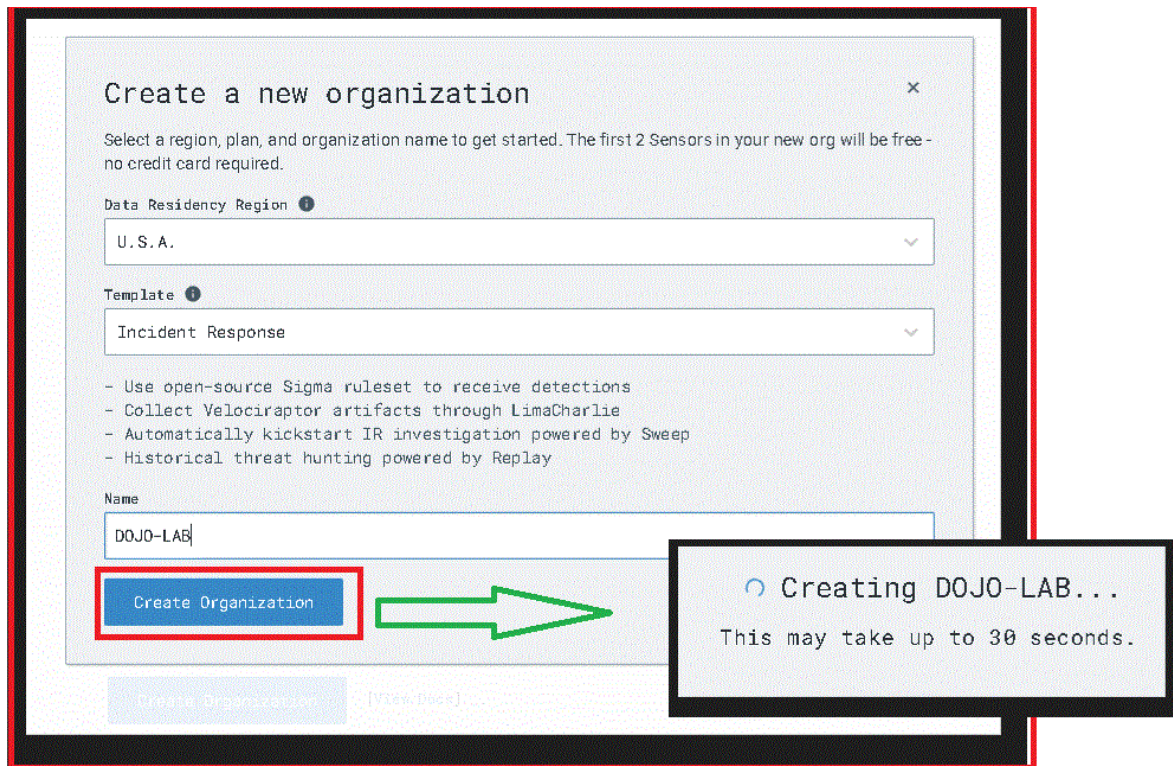
- Sensors** are the primary input for data into LimaCharlie. They run on a variety of supported platforms and send JSON events to LimaCharlie's cloud in real-time. Embedded platforms (e.g. Windows, Mac, Linux) expose deeper capabilities like sending commands and collecting artifacts.
- Organizations** are akin to "projects" - they're located in a chosen region and are where configuration and storage is located for a fleet of Sensors and their accompanying infrastructure.
- Outputs** allow you to forward your data to storage only you control — like an SFTP server or Amazon S3. Storage within LimaCharlie is optional and allows you to store artifacts (i.e. logs) as well as search, browse, and replay historical Sensor data.
- Add-ons** let you enable features within organizations à la carte, allowing you to run each org as lean or as sophisticated as your needs require.

The first step is to create an organization.

Create Organization

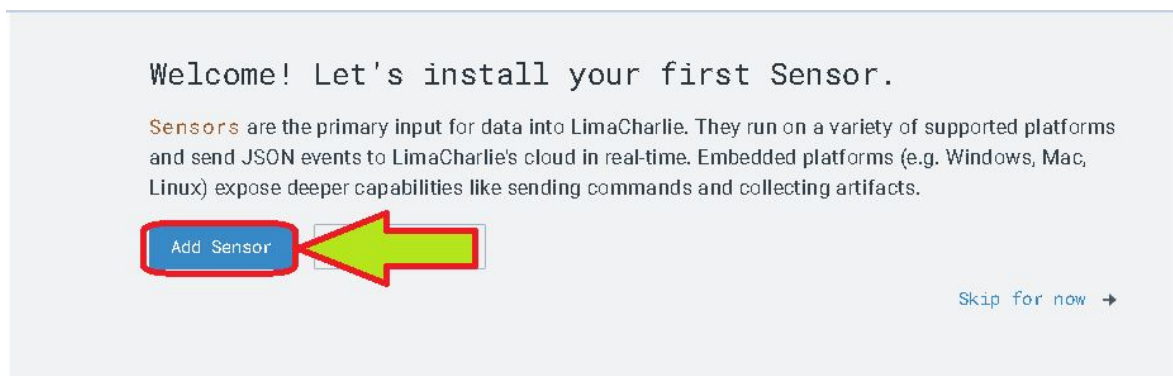
[View Docs]

3. Llene la información de la siguiente forma



The screenshot shows a web form titled "Create a new organization". It includes a close button (X) in the top right. Below the title is a note: "Select a region, plan, and organization name to get started. The first 2 Sensors in your new org will be free - no credit card required." The form has two dropdown menus: "Data Residency Region" with "U.S.A." selected, and "Template" with "Incident Response" selected. Below these are three bullet points: "Use open-source Sigma ruleset to receive detections", "Collect Velociraptor artifacts through LimaCharlie", and "Automatically kickstart IR investigation powered by Sweep". A "Name" field contains "DOJO-LAB". A red box highlights the "Create Organization" button, with a green arrow pointing to a secondary box on the right that says "Creating DOJO-LAB... This may take up to 30 seconds." At the bottom, there is a disabled "Create Organization" button and a "[View Docs]" link.

4. Vamos a instalar nuestro sensor en nuestra maquina Windows 10




The screenshot shows a "Welcome! Let's install your first Sensor." screen. It contains a paragraph explaining that sensors are the primary input for data into LimaCharlie and send JSON events to the cloud in real-time. Below the text is a red box around the "Add Sensor" button, with a green arrow pointing to it. To the right of the button is a "Skip for now" link with a right-pointing arrow.




5. Seleccionamos la plataforma a utilizar para instalar el sensor, Luego creamos una clave, las claves se utilizan para implementar sensores y vincularlos a una organización.

Choose a Sensor Type


AllEndpointCloud & External SourcesBrowserNetwork

 Windows

Select▼

 MacOS

Select▼

 Linux

Select▼

Select an Installation Key

No installation keys created yet. Installation keys are used to deploy Sensors and bind them to a particular organization. Installation keys also allow you to automatically tag sensors when they enroll.

Let's create the first installation key:

Description

DEMO

Tags (optional)

DEMO

Create

6. Seleccionar la llave y a continuación "Selecione" el instalador "x86" en instalación de un sensor windows, debes descargarlo dando "click" en Descargar, luego copiar el comando y utilizarlo para ejecutar el instalador desde el cmd como Administrador.

Select an Installation Key

Installation Key

DEMO

Select

Create New

Install Sensor on Endpoint(s)

Installing a Windows sensor

1. Select the installer for your architecture.

x86 (.exe)

x86 (.msi)

x86-64
(.exe)

x86-64
(.msi)

2. Download the [selected installer](#).

3. Open a shell with administrator privileges and navigate to the directory of the downloaded installer.

4. Copy the following command and use it to run the installer:

```
lc_sensor.exe -i AAAABgAAQsFAAAAIzkxNTc3OThjNTBhZjM3MmMubGMubGltYWNoYXJsaWUuaW8AAABE
```



5. Return here to see if any new sensors have successfully registered with LimaCharlie's cloud. It may take a moment for the sensor to enroll after you've installed it.

Note: this step is not strictly necessary to enroll sensors. You may leave this screen and enrollment will proceed normally.

Waiting for new sensor(s)...

7. Instalación del sensor desde el cmd como administrador, para ejecutar el instalador debes dirigirte a la carpeta de descargas donde descargaste el instalador x86 del paso anterior ahora pega y ejecuta el comando que copiamos antes.

Nota# Debes reemplazar "lc_sensor.exe" por el nombre del instalador de descargado de lo Contrario la ejecución fallara.



DOJO-LAB - Sensors - LimaCharlie x +

app.limacharlie.io/orgs/331af60a-de89-4d09-ba75-b96af28670c7/sensors

← Back to Key Type Key Install

2. Download the [selected installer](#).
3. Open a shell with administrator privileges and navigate to the directory of the downloaded installer.
4. Copy the following command and use it to run the installer:


```
lc_sensor.exe -i AAAABgAAQsFAAAAIzkxNTc30ThjNTBhZjM3MmMubGMubGltYWNoeX.
```
5. Return here to see if any new sensors have successfully registered with LimaCharlie's cloud. It may take a moment for the sensor to enroll after you've installed it.
Note: this step is not strictly necessary to enroll sensors. You may leave this screen and enrollment will proceed normally.

 Detected new sensor!
 desktop-hg4luui.home

All done!

Finish




8. ¡Hemos instalado con éxito nuestra EDR en la máquina virtual de Windows 10!

RESPOND 

Sensors [View Docs] + Add Sensor

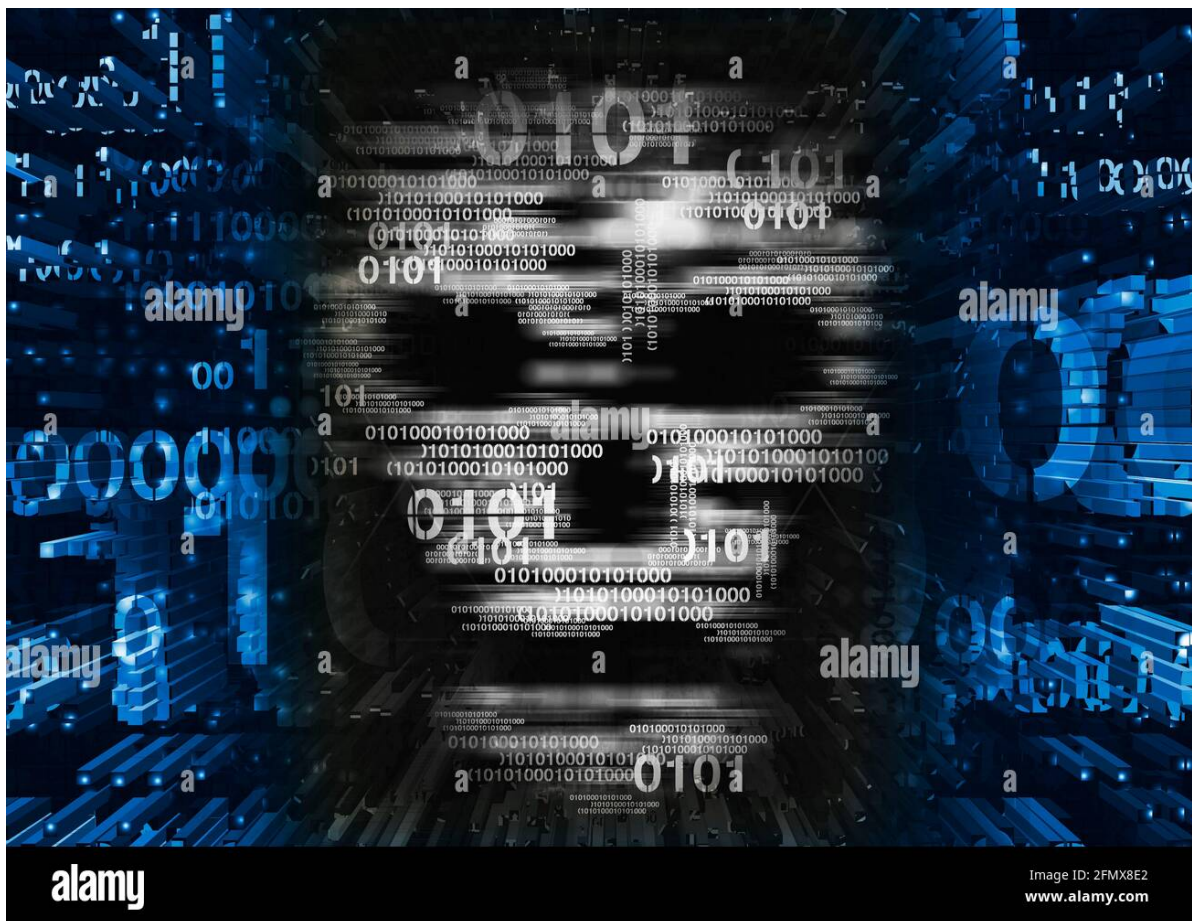
Search Filter Sensors: 1

Search by hostname, tag, IP, etc... Online Refresh

Hostname	Tags	Online	Isolated
 desktop-hg4luui.home	demo		

F

EJECUCIÓN DE PRUEBAS ATOMICAS CON ATOMIC RED TEAM



Importante saber

Atomic Red Team™ es una biblioteca de pruebas asignadas al marco MITRE ATT&CK®. Los equipos de seguridad pueden usar Atomic Red Team para probar sus entornos de forma rápida, portátil y reproducible.

MITRE ATT&CK® es una base de conocimiento accesible a nivel mundial de tácticas y técnicas del adversario basadas en observaciones del mundo real. La base de conocimientos de ATT&CK se utiliza como base para el desarrollo de metodologías y modelos de amenazas específicos en el sector privado, en el gobierno y en la comunidad de productos y servicios de ciberseguridad.

#Nota

Para realizar el ataque es importante que el equipo atacante cuente con los requerimientos necesarios para realizar las pruebas.

#Powershell 7 "Guía de instalación" <https://www.techlear.com/blog/2021/02/26/how-to-install-and-use-powershell-on-ubuntu-20-04/>

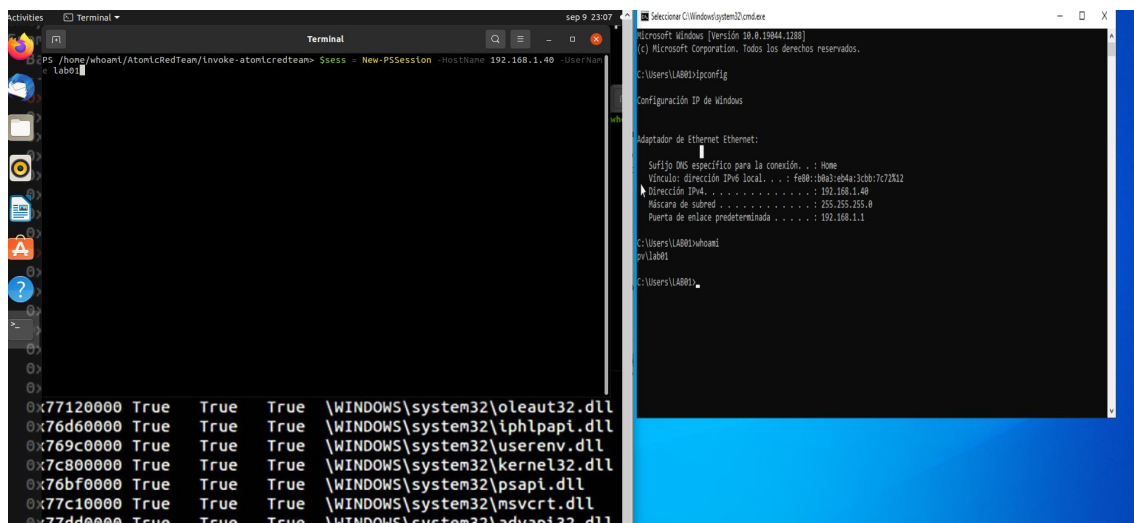
#Atomic Red "Guía de instalación" <https://github.com/redcanaryco/invoke-atomicredteam/wiki/Installing-Invoke-AtomicRedTeam>

Estableciendo conexión con nuestra maquina victima

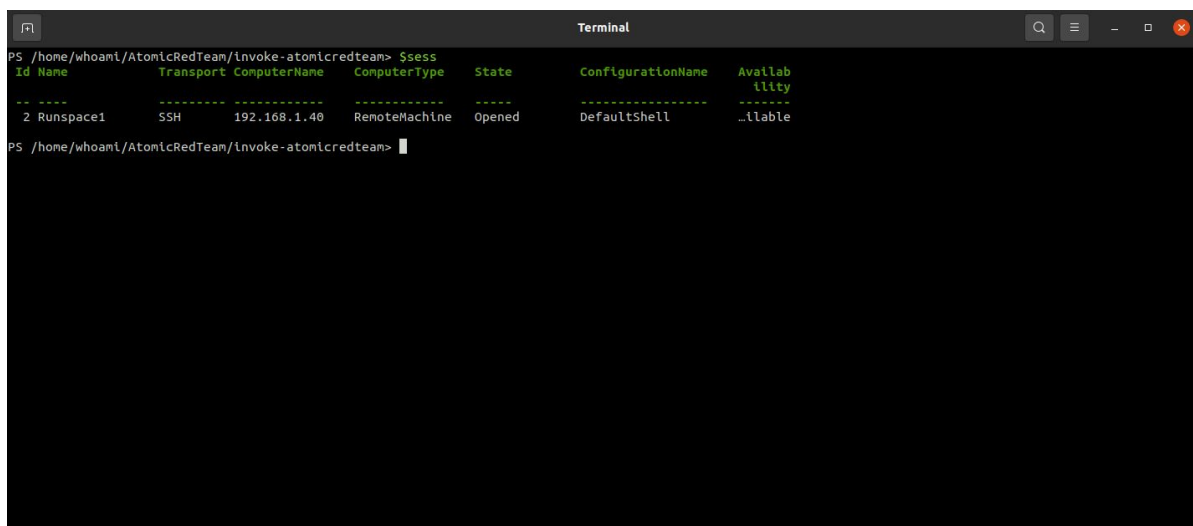
1.Teniendo instalado los requerimientos lo primero que haremos es conectarnos mediante Powershell Remoting a nuestra maquina Victima

- creamos una sesión remota para Windows en la misma computadora Ubuntu. Usamos los cmdlets de PowerShell de forma interactiva, por lo que vemos indicaciones de SSH que solicitan verificar la computadora host y solicitan una contraseña

```
$sess = New-PSSession -HostName ip-de-la-maquina -UserName LAB12
```



2. Comprobamos que la sesión esta establecida



3. Hagamos una prueba y obtengamos los procesos que se ejecutan en la maquina victima "windows" con el siguiente comando

```
PS /home/whoant/AtomicRedTeam/invoke-atomicredteam> $sess
Id Name Transport ComputerName ComputerType State ConfigurationName Availability
-- --
2 Runspace1 SSH 192.168.1.40 RemoteMachine Opened DefaultShell _ilable

PS /home/whoant/AtomicRedTeam/invoke-atomicredteam> Invoke-Command $sess -ScriptBlock (Get-Process)

NPM(K) PM(M) WS(M) CPU(s) Id SI ProcessName PSComputerName
-----
21 7.00 28.61 0.17 6624 1 ApplicationFrameHost 192.168.1.40
5 2.27 4.00 0.02 3412 0 cmd 192.168.1.40
5 2.28 3.90 0.02 5820 1 cmd 192.168.1.40
10 6.49 13.11 0.03 3972 0 conhost 192.168.1.40
12 6.87 17.39 0.09 5764 1 conhost 192.168.1.40
20 1.57 4.97 0.31 488 0 csrss 192.168.1.40
15 1.64 5.03 0.31 484 1 csrss 192.168.1.40
17 4.27 20.63 0.31 4112 1 ctfmon 192.168.1.40
20 5.08 17.28 0.34 2748 0 dashost 192.168.1.40
17 3.42 11.48 0.12 3672 1 dllhost 192.168.1.40
34 36.41 64.18 0.48 908 1 dwm 192.168.1.40
72 31.14 103.35 2.38 3868 1 explorer 192.168.1.40
5 1.56 4.27 0.06 696 1 fontdrvhost 192.168.1.40
5 1.25 3.18 0.00 704 0 fontdrvhost 192.168.1.40
0 0.06 0.01 0.00 0 0 Idle 192.168.1.40
26 6.43 18.69 0.53 576 0 lsass 192.168.1.40
0 0.04 0.00 0.00 1480 0 Memory Compression 192.168.1.40
18 16.23 26.86 0.12 2400 1 msedge 192.168.1.40
20 10.54 31.31 0.50 3996 1 msedge 192.168.1.40
44 34.77 91.50 1.86 4164 1 msedge 192.168.1.40
9 1.88 6.89 0.02 5772 1 msedge 192.168.1.40
14 7.40 18.87 0.05 6008 1 msedge 192.168.1.40
17 74.06 120.51 4.06 6744 1 msedge 192.168.1.40
14 7.33 17.30 0.05 6836 1 msedge 192.168.1.40
15 14.68 32.01 0.11 6964 1 msedge 192.168.1.40
58 128.25 113.94 8.34 2560 0 MsMpEng 192.168.1.40
25 3.80 8.72 0.03 3680 0 NisSrv 192.168.1.40
48 19.04 60.04 1.03 5636 1 OneDrive 192.168.1.40
54 37.99 73.02 1.86 4048 0 pwsh 192.168.1.40
7 2.92 71.71 0.62 72 0 Registry 192.168.1.40
12 2.73 17.21 0.08 4852 1 RuntimeBroker 192.168.1.40
24 8.97 32.83 0.56 5068 1 RuntimeBroker 192.168.1.40
14 2.67 15.28 0.31 5556 1 RuntimeBroker 192.168.1.40

PS /home/whoant/AtomicRedTeam/invoke-atomicredteam>
```

Ejecutar Pruebas Atómicas (Local)

Para nuestra prueba podemos usar el sitio web de MITRE ATT&CK® para buscar la prueba que queremos ejecutar. Como podemos ver hay una gran cantidad de técnicas registradas. Para esta demostración vamos a utilizar una técnica de Credential Access, porque lo primero que quiere hacer un atacante cuando se infiltra dentro de su sistema es elevar sus permisos u obtener una cuenta con permisos más altos

Home > Tactics > Enterprise > Credential Access

Credential Access

The adversary is trying to steal account names and passwords.

Credential Access consists of techniques for stealing credentials like account names and passwords. Techniques used to get credentials include keylogging or credential dumping. Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals.

ID: TA0006
Created: 17 October 2018
Last Modified: 19 July 2019

Version Permalink

Techniques

Techniques: 16

ID	Name	Description
T1557	Adversary-in-the-Middle	Adversaries may attempt to position themselves between two or more networked devices using an adversary-in-the-middle (AITM) technique to support follow-on behaviors such as Network Sniffing or Transmitted Data Manipulation. By abusing features of common networking protocols that can determine the flow of network traffic (e.g. ARP, DNS, LLMNR, etc.), adversaries may force a device to communicate through an adversary controlled system so they can collect information or perform additional actions.
.001	LLMNR/NBT-NS Poisoning and SMB Relay	By responding to LLMNR/NBT-NS network traffic, adversaries may spoof an authoritative source for name resolution to force communication with an adversary controlled system. This activity may be used to collect or relay authentication materials.
.002	ARP Cache Poisoning	Adversaries may poison Address Resolution Protocol (ARP) caches to position themselves between the communication of two or more networked devices. This activity may be used to enable follow-on behaviors such as Network Sniffing or Transmitted Data Manipulation.
.003	DHCP Spoofing	Adversaries may redirect network traffic to adversary-owned systems by spoofing Dynamic Host Configuration Protocol (DHCP) traffic and acting as a malicious DHCP server on the victim network. By achieving the adversary-in-the-middle (AITM) position, adversaries may collect network communications, including passed credentials, especially those sent over insecure, unencrypted protocols. This may also enable follow-on behaviors such as Network

MITRE ATT&CK® nos muestra una breve descripción de la táctica que acabamos de seleccionar, así como una descripción de cada técnica y subtécnica.

10. Cada prueba tiene un ID, el que vamos a utilizar es “T1003.002”.

T1003	OS Credential Dumping	Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform Lateral Movement and access restricted information.
.001	LSASS Memory	Adversaries may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). After a user logs on, the system generates and stores a variety of credential materials in LSASS process memory. These credential materials can be harvested by an administrative user or SYSTEM and used to conduct Lateral Movement using Use Alternate Authentication Material.
.002	Security Account Manager	Adversaries may attempt to extract credential material from the Security Account Manager (SAM) database either through in-memory techniques or through the Windows Registry where the SAM database is stored. The SAM is a database file that contains local accounts for the host, typically those found with the <code>net user</code> command. Enumerating the SAM database requires SYSTEM level access.

11. Ahora, regrese al indicador de PowerShell y use el interruptor "-ShowDetailsBrief" para enumerar las pruebas disponibles para un número de técnica dado, por lo que en nuestro caso necesitamos ejecutar "Invoke-AtomicTest T1003.002 -ShowDetailsBrief".

```

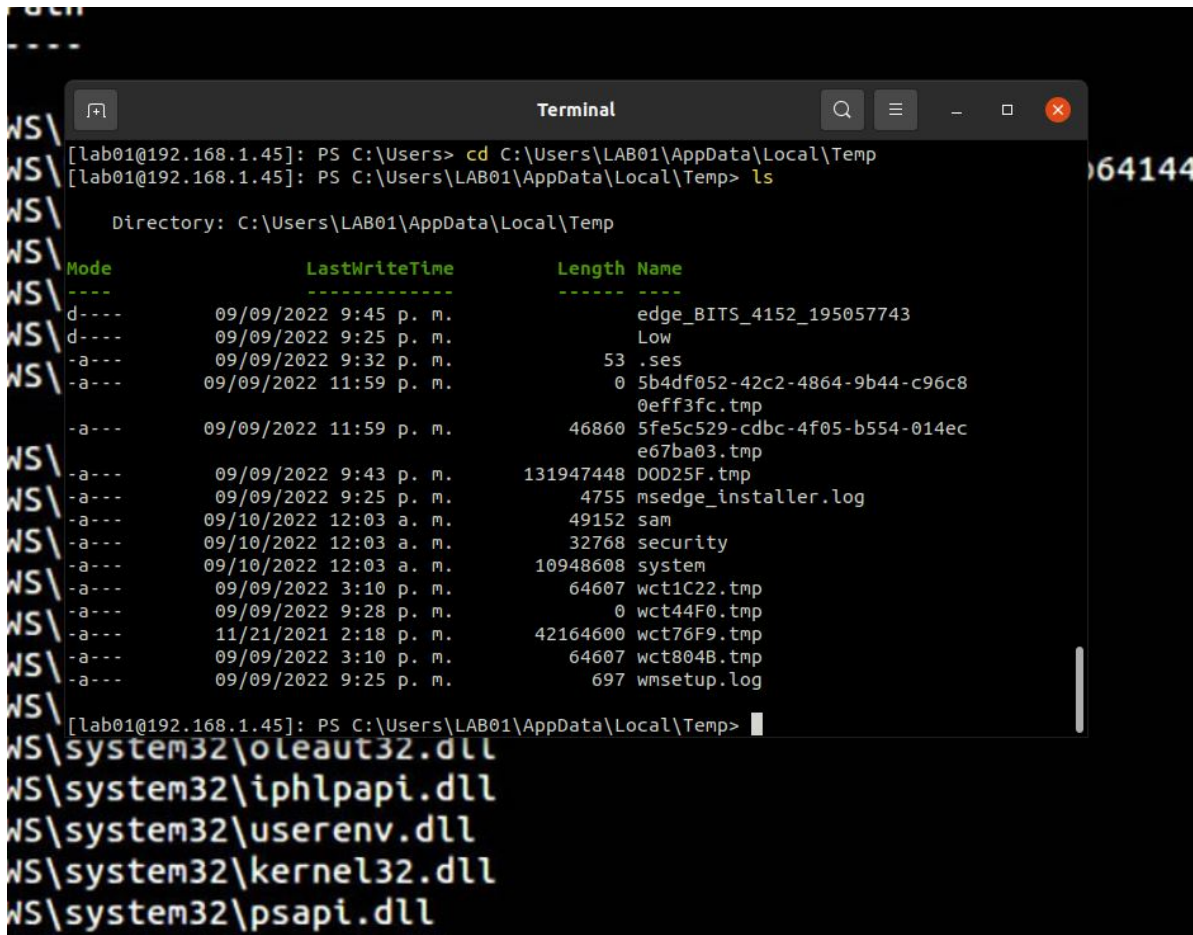
PS /home/whoami/AtomicRedTeam/Invoke-atomicredteam> Invoke-AtomicTest T1003.002 -Session $sess -ShowDetailsBrief
PathToAtomicsFolder = /home/whoami/AtomicRedTeam/atomics

T1003.002-1 Registry dump of SAM, creds, and secrets
T1003.002-2 Registry parse with pypykatz
T1003.002-3 esentutil.exe SAM copy
T1003.002-4 PowerDump Hashes and Usernames from Registry
T1003.002-5 dump volume shadow copy hives with certutil
T1003.002-6 dump volume shadow copy hives with System.IO.File
T1003.002-7 WinPwn - Loot local Credentials - Dump SAM-File for NTLM Hashes
PS /home/whoami/AtomicRedTeam/Invoke-atomicredteam>

```

12. podemos usar el interruptor "-ShowDetails" para mostrar los detalles de la prueba, incluidos los comandos de ataque, los parámetros de entrada y los requisitos previos para un número de técnica determinado. En nuestro caso sería "Invoke-AtomicTest T1003.002 -ShowDetails"

"C:\Users{USERNAME}\AppData\Local\Temp" y ejecute "dir" para ver los archivos dentro de la carpeta temporal.



```
[lab01@192.168.1.45]: PS C:\Users> cd C:\Users\LAB01\AppData\Local\Temp
[lab01@192.168.1.45]: PS C:\Users\LAB01\AppData\Local\Temp> ls

Directory: C:\Users\LAB01\AppData\Local\Temp

Mode                LastWriteTime         Length Name
----                -
d-----          09/09/2022  9:45 p. m.         edge_BITS_4152_195057743
d-----          09/09/2022  9:25 p. m.             Low
-a----          09/09/2022  9:32 p. m.             53 .ses
-a----          09/09/2022 11:59 p. m.             0 5b4df052-42c2-4864-9b44-c96c8
                                0eff3fc.tmp
-a----          09/09/2022 11:59 p. m.        46860 5fe5c529-cdbc-4f05-b554-014ec
                                e67ba03.tmp
-a----          09/09/2022  9:43 p. m.    131947448 D0D25F.tmp
-a----          09/09/2022  9:25 p. m.         4755 msedge_installer.log
-a----          09/10/2022 12:03 a. m.         49152 sam
-a----          09/10/2022 12:03 a. m.        32768 security
-a----          09/10/2022 12:03 a. m.    10948608 system
-a----          09/09/2022  3:10 p. m.         64607 wct1C22.tmp
-a----          09/09/2022  9:28 p. m.             0 wct44F0.tmp
-a----          11/21/2021  2:18 p. m.    42164600 wct76F9.tmp
-a----          09/09/2022  3:10 p. m.         64607 wct804B.tmp
-a----          09/09/2022  9:25 p. m.          697 wmsetup.log

[lab01@192.168.1.45]: PS C:\Users\LAB01\AppData\Local\Temp>
```

Aquí podemos ver los archivos que se volcaron "sam, seguridad y sistema"

15. Ahora, regrese a LimaCharlie y vaya a la pestaña Detección para ver si puede atrapar algo

```
Terminal
[lab01@192.168.1.45]: PS C:\Users> cd C:\Users\LAB01\AppData\Local\Temp
[lab01@192.168.1.45]: PS C:\Users\LAB01\AppData\Local\Temp> ls

Directory: C:\Users\LAB01\AppData\Local\Temp

Mode                LastWriteTime         Length Name
----                -
d-----          09/09/2022 9:45 p. m.             edge_BITS_4152_195057743
d-----          09/09/2022 9:25 p. m.             Low
-a----          09/09/2022 9:32 p. m.              53 .ses
-a----          09/09/2022 11:59 p. m.             0 5b4df052-42c2-4864-9b44-c96c8
                                0eff3fc.tmp
-a----          09/09/2022 11:59 p. m.          46860 5fe5c529-cdbc-4f05-b554-014ec
                                e67ba03.tmp
-a----          09/09/2022 9:43 p. m.       131947448 DOD25F.tmp
-a----          09/09/2022 9:25 p. m.         4755 msedge_installer.log
-a----          09/10/2022 12:03 a. m.         49152 sam
-a----          09/10/2022 12:03 a. m.        32768 security
-a----          09/10/2022 12:03 a. m.       10948608 system
-a----          09/09/2022 3:10 p. m.         64607 wct1C22.tmp
-a----          09/09/2022 9:28 p. m.             0 wct44F0.tmp
-a----          11/21/2021 2:18 p. m.       42164600 wct76F9.tmp
-a----          09/09/2022 3:10 p. m.         64607 wct804B.tmp
-a----          09/09/2022 9:25 p. m.          697 wmsetup.log

[lab01@192.168.1.45]: PS C:\Users\LAB01\AppData\Local\Temp>
```

Recopilando la información del ataque con LimaCharlie

Podemos ver que detectó la actividad sospechosa dentro de nuestro sistema, ahora haga clic en una de las alertas. Nos muestra una descripción detallada de lo que acaba de pasar

Category	Source
Suspicious Execution of Task...	desktop-hg4luui...
Process Start From Suspicious...	desktop-hg4luui...
Grabbing Sensitive Hives via ...	desktop-hg4luui...
Registry Dump of SAM Creds an...	desktop-hg4luui...
Registry Dump of SAM Creds an...	desktop-hg4luui...
Registry Dump of SAM Creds an...	desktop-hg4luui...
Registry Dump of SAM Creds an...	desktop-hg4luui...
Suspicious Execution of Hostn...	desktop-hg4luui...
Local Accounts Discovery	desktop-hg4luui...
Whoami Execution	desktop-hg4luui...
Whoami Execution	desktop-hg4luui...
Local Accounts Discovery	desktop-hg4luui...
Whoami Execution	desktop-hg4luui...
Local Accounts Discovery	desktop-hg4luui...
...	...

4768ad97-21aa-4d31-a04b-2d7562ff03f0

Category: Registry Dump of SAM Creds and Secrets
Time: 2022-08-18 20:59:41
Source: desktop-hg4luui.home

[View Event Timeline](#) [Mark False Positive](#)

```
{
  "detection": {
    "author": "_sigma[lock][segment][secret]"
    "cat": "Registry Dump of SAM Creds and Secrets"
  },
  "detect": {
    "event": {
      "COMMAND_LINE": "reg save HKLM\\security C:\\Users\\LAB1\\AppData\\Local\\Temp\\security"
      "FILE_IS_SIGNED": 1
      "FILE_PATH": "C:\\Windows\\system32\\reg.exe"
      "HASH": "c0e25b1f9b22de445298c1e96ddfcead265ca030fa6626f61a4a4786cc4a"
      "PARENT": {
        "COMMAND_LINE": "cmd.exe /c reg save HKLM\\sam %temp%\\sam & reg save HKLM\\system %temp%\\system & reg save HKLM\\security %temp%\\security"
        "FILE_IS_SIGNED": 1
      }
    }
  }
}
```

si nos desplazamos un poco hacia abajo, podemos ver un mensaje de cuál puede ser la intención del atacante dentro de nuestro sistema.

Category	Source	
Suspicious Execution of Taskk...	desktop-hg4luui.1	
Process Start From Suspicious...	desktop-hg4luui.1	
Grabbing Sensitive Hives via ...	desktop-hg4luui.1	
Registry Dump of SAM Creds an...	desktop-hg4luui.1	
Registry Dump of SAM Creds an...	desktop-hg4luui.1	
Registry Dump of SAM Creds an...	desktop-hg4luui.1	
Registry Dump of SAM Creds an...	desktop-hg4luui.1	
Suspicious Execution of Hostn...	desktop-hg4luui.1	
Local Accounts Discovery	desktop-hg4luui.1	
Whoami Execution	desktop-hg4luui.1	
Whoami Execution	desktop-hg4luui.1	
Local Accounts Discovery	desktop-hg4luui.1	
Whoami Execution	desktop-hg4luui.1	
Local Accounts Discovery	desktop-hg4luui.1	
Suspicious Execution of Hostn...	desktop-hg4luui.1	

```

    }
    "this" : "958a2c319d2ed5e6c624670f62fea83d"
  }
}
"detect_id" : "4768ad97-21aa-4d31-a04b-2d7562ff03f0"
"detect_mtd" : {
  "author" : "frack113"
  "description" :
    "Adversaries may attempt to extract credential material from the Security Account Manager (SAM) database either through Windows Registry where the SAM database is stored"
  "falsepositives" : [
    {
      "level" : "high"
      "references" : [
        {
          "url" : "https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdcfdd3742bfcf365fee2a9/atomics/T1003-test-1---registry-dump-of-sam-creds-and-secrets"
        }
      ]
      "tags" : [
        {
          "tag" : "attack.credential_access"
        }
        {
          "tag" : "attack.t1003.002"
        }
      ]
    }
  ]
}

```

Limpieza después de ejecutar pruebas atómicas



Muchas pruebas atómicas incluyen comandos de limpieza para eliminar archivos temporales generados durante la ejecución de la prueba o para devolver la configuración a sus valores anteriores o más seguros para que la prueba se pueda ejecutar nuevamente. Se recomienda ejecutar los comandos de limpieza después de cada ejecución de prueba.

COMANDO A UTILIZAR

```
Invoke-AtomicTest T1003.002 -Cleanup
```

```
Terminal
PS /home/whoami/AtomicRedTeam/invoke-atomicredteam> Invoke-AtomicTest T1003.002 -Session $sess -cleanup
PathToAtomicsFolder = /home/whoami/AtomicRedTeam/atomics
Executing cleanup for test: T1003.002-1 Registry dump of SAM, creds, and secrets
Done executing cleanup for test: T1003.002-1 Registry dump of SAM, creds, and secrets
Executing cleanup for test: T1003.002-2 Registry parse with pypykatz
Done executing cleanup for test: T1003.002-2 Registry parse with pypykatz
Executing cleanup for test: T1003.002-3 esentutl.exe SAM copy
Done executing cleanup for test: T1003.002-3 esentutl.exe SAM copy
Executing cleanup for test: T1003.002-4 PowerDump Hashes and Usernames from Registry
Done executing cleanup for test: T1003.002-4 PowerDump Hashes and Usernames from Registry
Executing cleanup for test: T1003.002-5 dump volume shadow copy hives with certutil
Done executing cleanup for test: T1003.002-5 dump volume shadow copy hives with certutil
Executing cleanup for test: T1003.002-6 dump volume shadow copy hives with System.IO.File
Done executing cleanup for test: T1003.002-6 dump volume shadow copy hives with System.IO.File
Executing cleanup for test: T1003.002-7 WinPwn - Loot local Credentials - Dump SAM-File for NTLM Hashes
Done executing cleanup for test: T1003.002-7 WinPwn - Loot local Credentials - Dump SAM-File for NTLM Hashes
PS /home/whoami/AtomicRedTeam/invoke-atomicredteam> 
```

Referencias

<https://github.com/redcanaryco/atomic-red-team>

<https://attack.mitre.org/>

<https://miracomosehace.com/habilitar-ejecucion-scripts-powershell-windows-10/>

<https://protegermipc.net/2018/11/22/permitir-la-ejecucion-de-scripts-powershell-en-windows-10/>