Incidentes seguridad

Velociraptor

Jennifer

Índice

Indicaciones

Para la recolección de evidencias es habitual emplear herramientas especializadas. Una de ellas es el velociraptor.. Instalar la herramienta y emplearla en una máquina virtual controlada para obtener archivos.

¿Qué es Velociraptor y para qué sirve?

Velociraptor es una herramienta de análisis forense y monitoreo de sistemas en tiempo real. Está diseñado para detectar, investigar y responder a incidentes de seguridad en tu red o infraestructura.

¿Qué se puede hacer con esta herramienta?

Realizar análisis forense en sistemas remotos.

- Buscar artefactos específicos (archivos, logs, procesos).
- Analizar memoria o disco en endpoints (servidores, PCs, etc.).
- Ejecutar búsquedas o "hunts" masivas.

Automatizar la recolección de datos en múltiples máquinas.

- Realizar búsquedas rápidas para detectar amenazas.
- Monitorear eventos y actividades sospechosas.

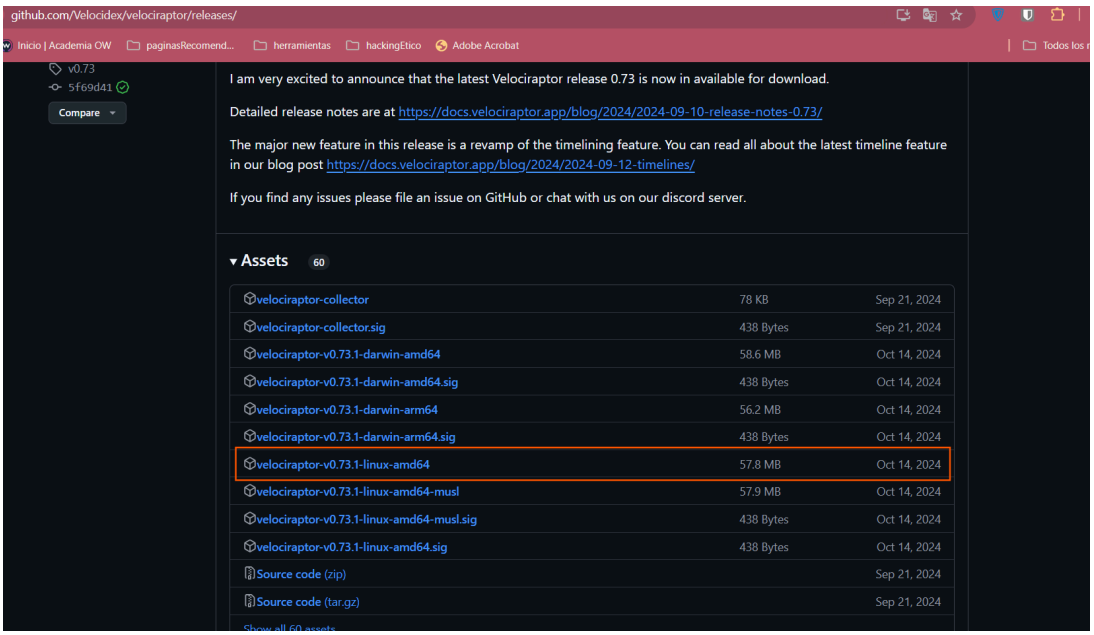
Detectar malware o comportamiento anómalo.

- Recolectar datos para investigaciones.
- Responder a incidentes.

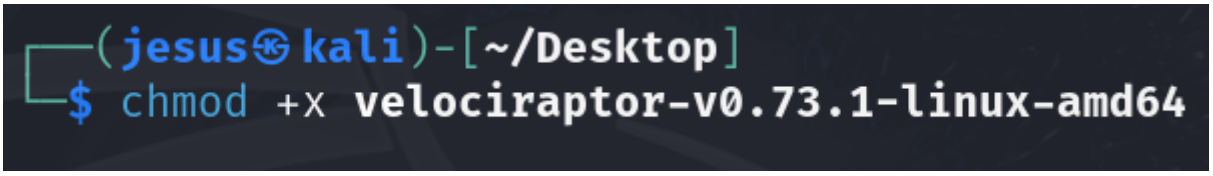
Ejecutar acciones remotas en endpoints afectados.

Instalación:

1. Primero nos descargamos el software de https://github.com/Velocidex/velociraptor/releases/



2. Le damos permisos al binario **chmod +x velociraptor-v0.73.1-linux-amd64**



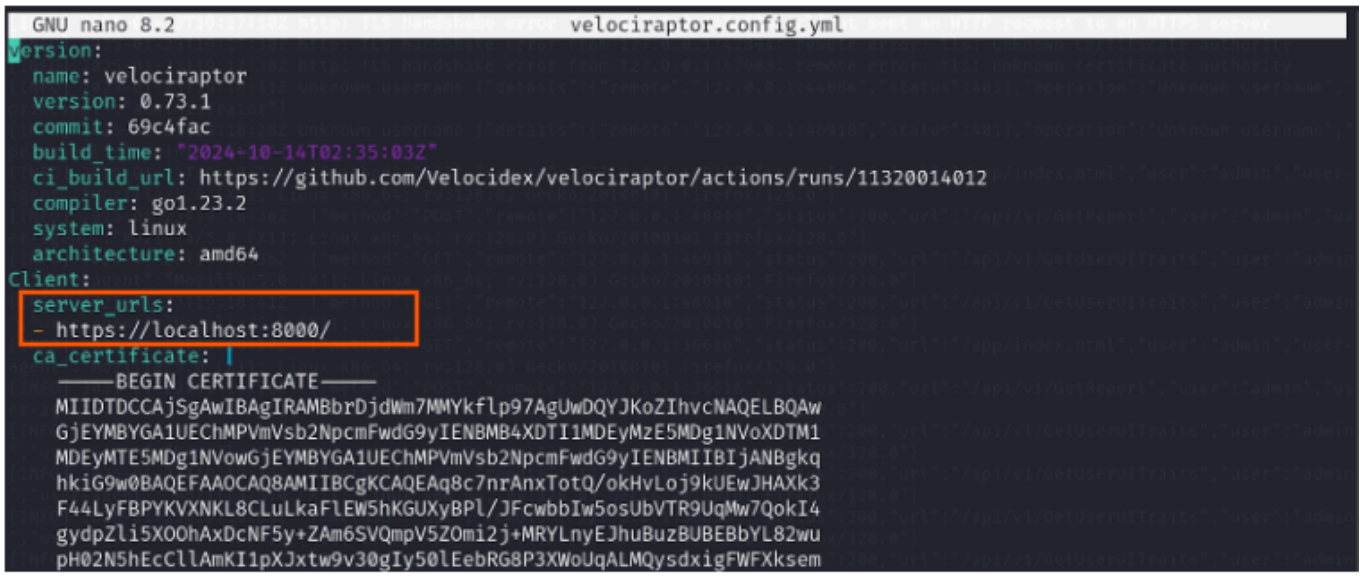
Configuración.

3. Generamos el fichero config.yaml

./velociraptor-v0.73.1-linux-amd64 config generate > velociraptor.config.yaml

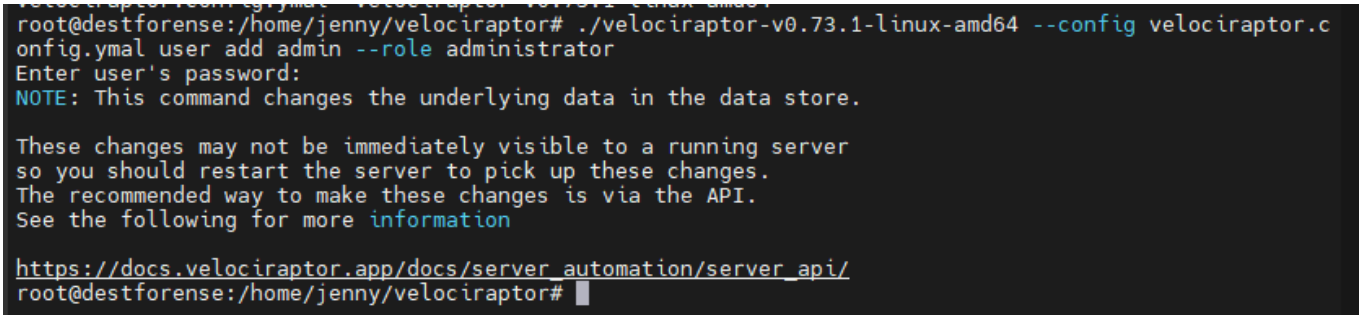
Editamos el fichero en caso real podriamos la IP del servidor en este caso lo dejaremos en localhost

nano /opt/velociraptor/config



4. Generamos el usuario administrador.

./velociraptor-v0.73.1-linux-amd64 --config velociraptor.config.yaml user add admin --role administrator

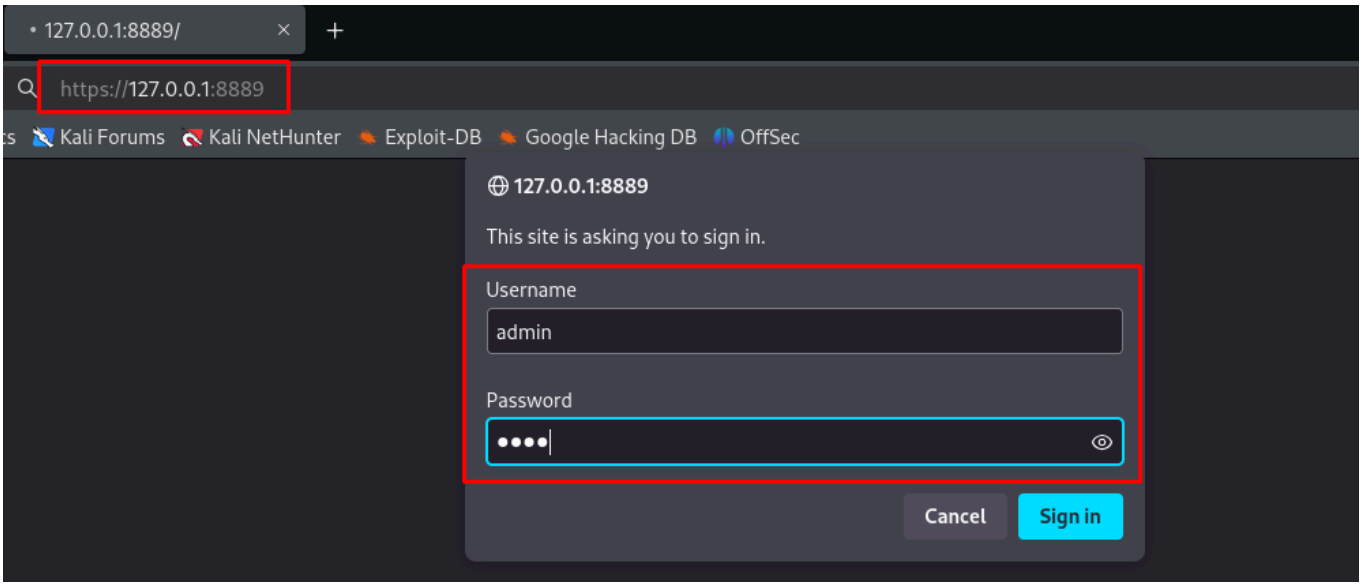


5. Inicializamos el software.

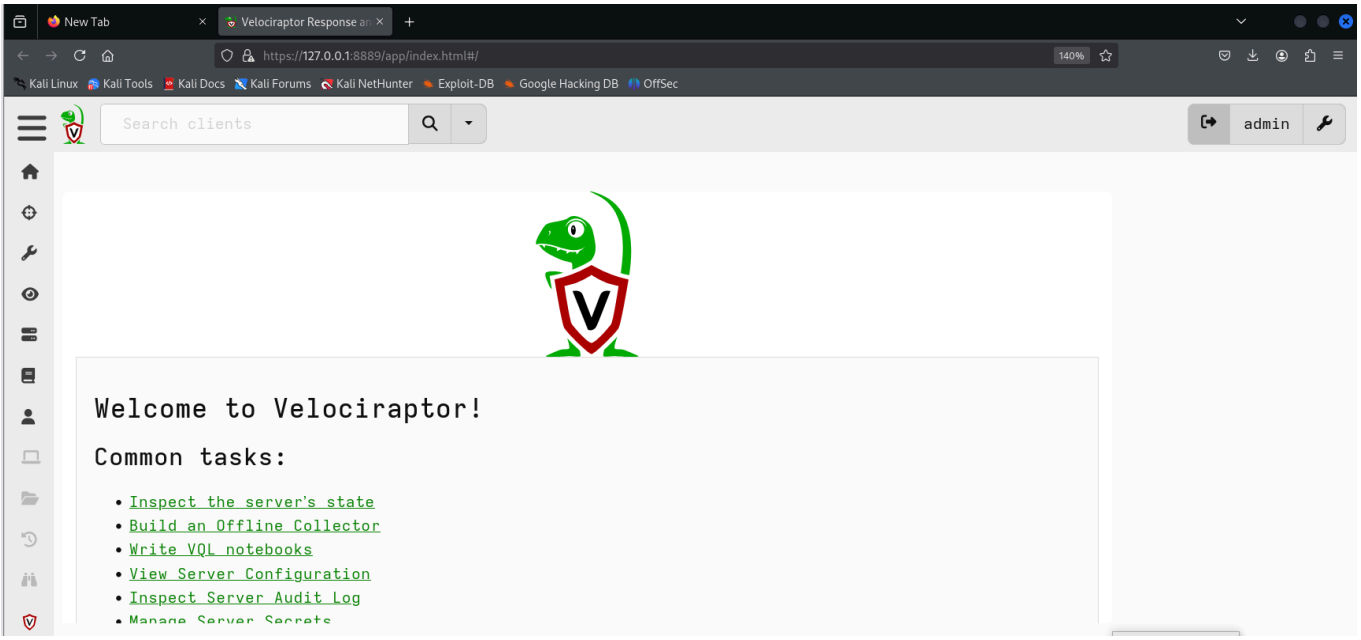
./velociraptor-v0.73.1-linux-amd64 --config velociraptor.config.yaml frontend -v

```
┌──(root㉿kali)-[/opt/velociraptor/config]
└─# ../../../home/jesus/Desktop/Velociraptor/velociraptor-v0.73.1-linux-amd64 --config velociraptor.config.yml frontend -v
[INFO] 2025-01-23T19:15:52Z  _     __            _  __           _
[INFO] 2025-01-23T19:15:52Z | |  / /__  / /___  _____(_)________ _____  / /_____  _____
[INFO] 2025-01-23T19:15:52Z | | / / _ \/ / __ \/ ___/ / ___/ __ `/ __ \/ __/ __ \/ ___/
[INFO] 2025-01-23T19:15:52Z | |/ /  __/ / /_/ / /__/ / /  / /_/ / /_/ / /_/ /_/ / /
[INFO] 2025-01-23T19:15:52Z |___/\___/_/\____/\___/_/_/   \__,_/ .___/\__/\____/_/
[INFO] 2025-01-23T19:15:52Z                                  /_/
[INFO] 2025-01-23T19:15:52Z Digging deeper!                https://www.velocidex.com
[INFO] 2025-01-23T19:15:52Z This is Velociraptor 0.73.1 built on 2024-10-14T02:35:03Z (69c4fac)
[INFO] 2025-01-23T19:15:52Z Loading config from file velociraptor.config.yml
[INFO] 2025-01-23T19:15:52Z Starting Frontend. {"build_time":"2024-10-14T02:35:03Z","commit":"69c4fac","version":"0.73.1"}
[INFO] 2025-01-23T19:15:52Z Increased open file limit to 999999
[INFO] 2025-01-23T19:15:52Z Setting temp directory to /tmp
[INFO] 2025-01-23T19:15:52Z Starting Org Manager service.
[INFO] 2025-01-23T19:15:52Z Starting services for Org <root> (root)
[INFO] 2025-01-23T19:15:52Z Starting Backup Services for Org <root> (root) every 24h0m0s
[INFO] 2025-01-23T19:15:52Z Frontend: Server will be master.
[INFO] 2025-01-23T19:15:52Z Filestore implementation FileBaseDataStore.
[INFO] 2025-01-23T19:15:52Z Starting Journal service for Org <root> (root).
[INFO] 2025-01-23T19:15:52Z Starting user manager service for org root
[INFO] 2025-01-23T19:15:52Z FrontendService: Watching for events from Server.Internal.FrontendMetrics
[INFO] 2025-01-23T19:15:52Z UserManagerService: Watching for events from Server.Internal.UserManager
[INFO] 2025-01-23T19:15:52Z Starting Server Scheduler Service for Org <root> (root)
[INFO] 2025-01-23T19:15:52Z Starting the notification service for Org <root> (root).
```

6. Nos conectamos al servidor.



Esta sería la interfaz del programa, en este punto vamos a configurar los hunter



¿Qué es un Hunt?

Un Hunt es una tarea o trabajo automatizado que puedes configurar para recolectar información específica de todos los clientes (endpoints) conectados al servidor Velociraptor. Los Hunts están diseñados para ser escalables, lo que significa que puedes ejecutar la misma tarea en cientos o miles de máquinas de manera eficiente.

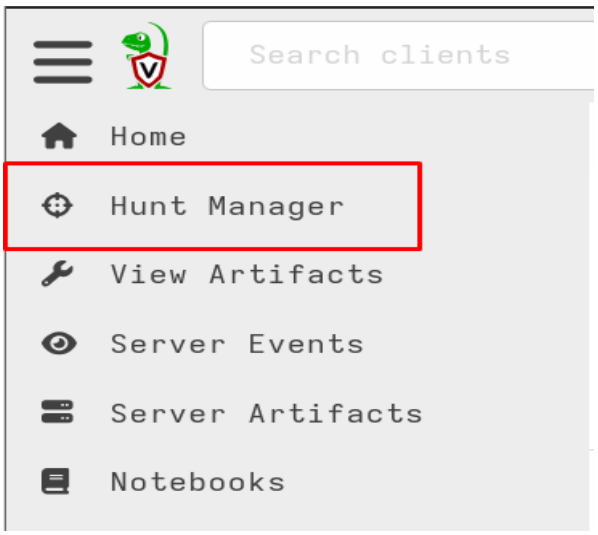
Por ejemplo:

Buscar procesos maliciosos en todas las máquinas Windows.

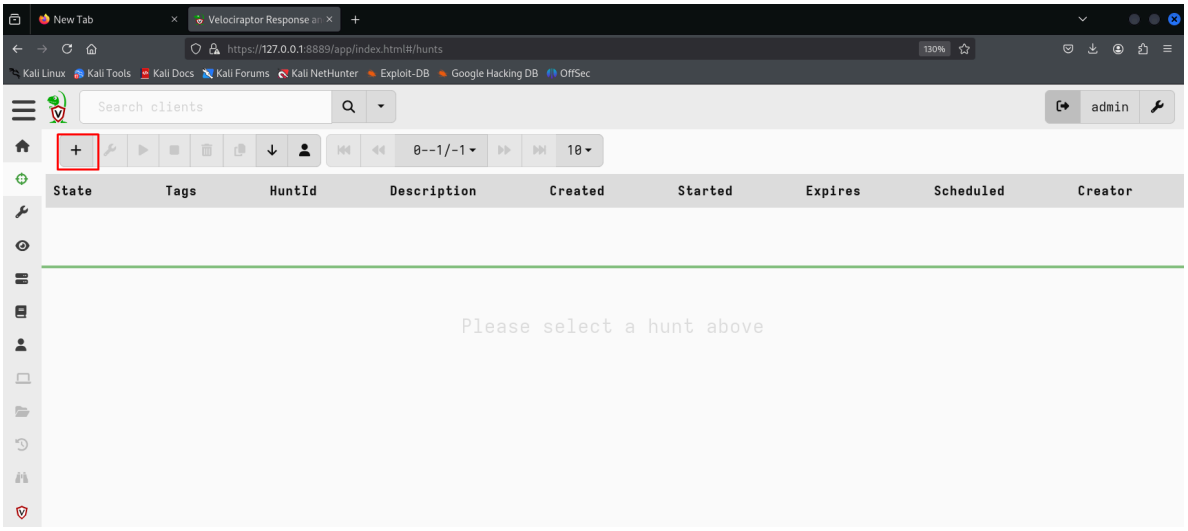
Recolectar logs del sistema en servidores Linux.

Buscar archivos específicos (como malware) en las máquinas conectadas.

7. Creación de Hunt Manager.



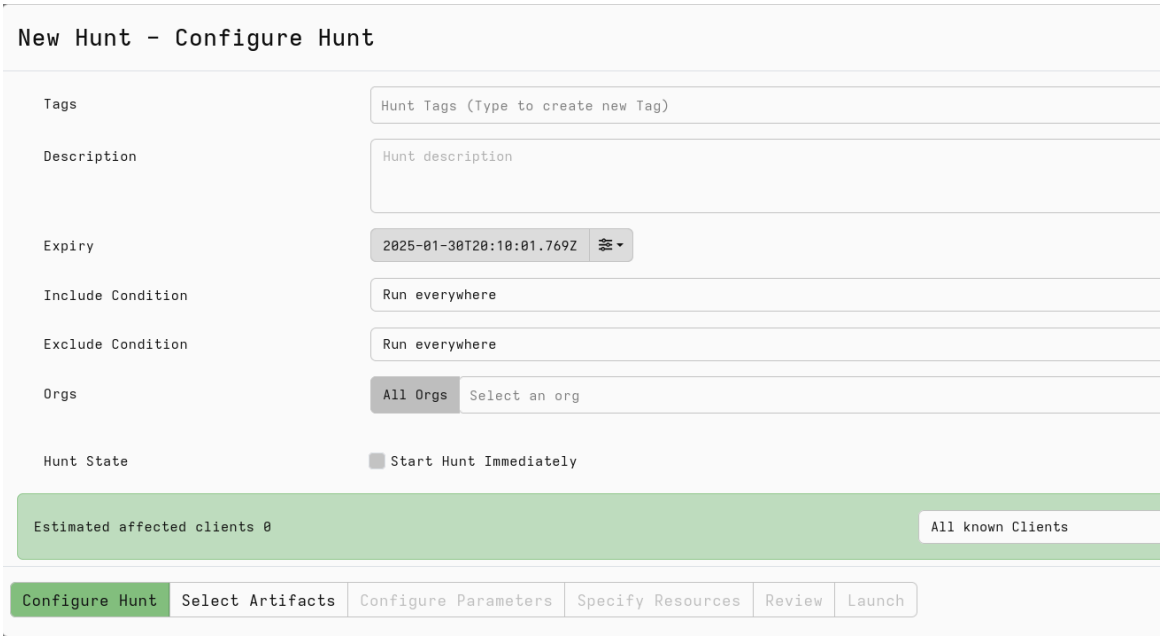
Le damos al símbolo + para añadirlo.



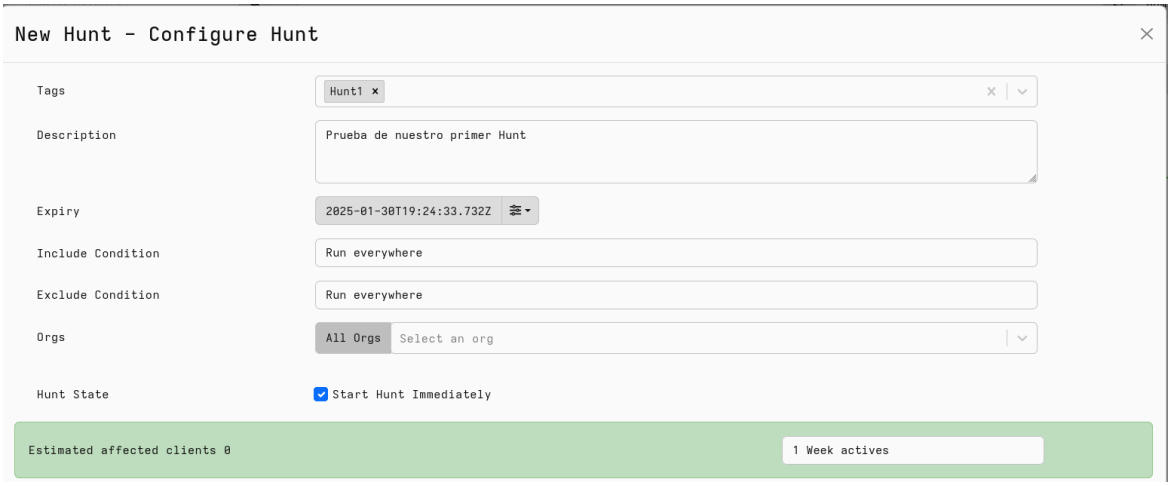
En esta interfaz hay varias ventanas en la planta baja que son:
Configure Hunt, Select Artifacts, Configure Parameters, Specify Resources, Review, Launch

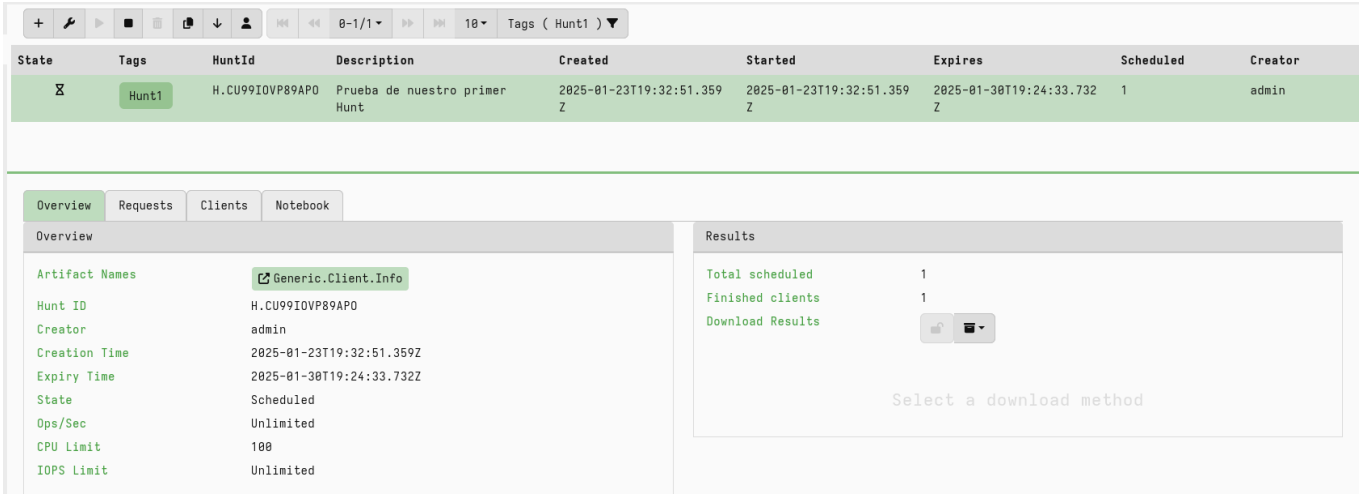
Configure Hunt:
Está compuesto por:

- Tags: Son etiquetas para clasificar el Hunt. Por ejemplo, si estás ejecutando un análisis relacionado con malware, podrías usar la etiqueta malware_scan.
- Description: Una breve descripción del propósito del Hunt, como "Recolectar procesos activos en Windows".
- Expiry: Define cuánto tiempo estará activo el Hunt antes de detenerse automáticamente.
    - Include Condition / Exclude Condition: Estas opciones te permiten especificar en qué máquinas debe ejecutarse el Hunt:
    - Include Condition: Define condiciones para incluir endpoints específicos (por ejemplo, "sólo máquinas Windows").
    - Exclude Condition: Excluye endpoints que cumplan ciertas condiciones.
- Artefactos:Los artefactos son colecciones de datos o scripts que definen qué hacer en cada endpoint. Por ejemplo:
    - Windows.System.Processes: Para listar procesos activos en Windows.
    - Linux.Syslog: Para recolectar logs del sistema Linux.
- Hunt State: Opción para decidir si el Hunt se ejecuta inmediatamente o si lo dejarás en pausa hasta iniciarlo manualmente.



Configuramos un hunter





Select Artifacts:

En esta interfaz seleccionamos los artefactos que hay disponibles. Cada artefacto representa una tarea específica o un tipo de datos que se puede recolectar desde los endpoints (máquinas clientes). Algunos ejemplos de artefactos en la lista incluyen:

- Admin.Client.Upgrade.Windows: Actualiza los clientes de Velociraptor en máquinas Windows.
- Generic.Client.DiskSpace: Recolecta información sobre el espacio en disco.
- Elastic.EventLogs.Sysmon: Recolecta logs de eventos del sistema con Sysmon (si está instalado).
- Generic.Client.Info: Obtiene información básica del cliente (el que está seleccionado en la imagen).

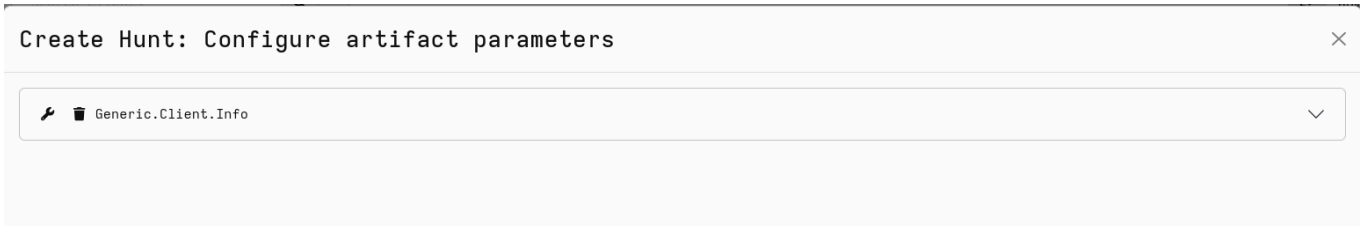
Configure artifact parameters

Indica que se están ajustando los parámetros del artefacto antes de que el Hunt sea lanzado.

En este caso, es Generic.Client.Info, que recolecta información básica sobre los endpoints.

- El icono de lápiz indica que puedes hacer clic para editar o ajustar los parámetros específicos de este artefacto. En algunos artefactos, puedes proporcionar valores personalizados o modificar las configuraciones predeterminadas.
- Si haces clic en la lista desplegable, se podra ver más detalles sobre el artefacto o tener acceso a configuraciones avanzadas, dependiendo del tipo de artefacto seleccionado.

Para algunos artefactos (aunque probablemente no en este caso específico, ya que Generic.Client.Info es bastante estándar)



Configuración Specify resource limits

Aquí es donde se definen los límites de recursos para un Hunt, que es una tarea de recopilación de datos forenses que se ejecuta en múltiples clientes al mismo tiempo.

Está compuesto por:

CPU Limit Percent: Define el porcentaje máximo del uso del CPU que Velociraptor puede usar en la máquina cliente mientras ejecuta el Hunt.

IOps/Sec: Limita la cantidad de operaciones de entrada/salida (disco, red) por segundo. **Unlimited** significa que no hay restricción. Esto puede ser útil en entornos controlados pero podría ralentizar máquinas con muchas tareas.

Max Execution Time in Seconds: Especifica el tiempo máximo que el Hunt puede ejecutarse en cada cliente, en segundos.

Max Idle Time in Seconds: Tiempo máximo en segundos que el cliente puede permanecer inactivo mientras intenta ejecutar el Hunt.

Max Rows: Especifica la cantidad máxima de filas de datos que el Hunt puede recolectar por cliente.

Max Bytes Uploaded: Define el tamaño máximo de datos (en bytes) que pueden ser recolectados y subidos al servidor por cada cliente.

Trace Frequency Seconds: Configura la frecuencia en segundos con la que el cliente actualiza el estado del Hunt en el servidor.

Urgent: Si se selecciona, el Hunt se ejecutará de manera urgente y omitirá las colas normales para iniciar inmediatamente en todos los clientes.

Configuración Review request

Aquí se muestra una vista previa de la configuración para la creación de un Hunt en Velociraptor.

Este Hunt recopila información básica sobre los clientes usando el artefacto Generic.Client.Info. Limita el uso de recursos del cliente (CPU al 100%, tiempo máximo de 600 segundos, máximo de 500 filas o 2 MB de datos por cliente). Se ejecuta en todos los clientes disponibles sin condiciones.

Create Hunt: Review request


```
{
  "start_request": {
    "artifacts": [
      "Generic.Client.Info"
    ],
    "specs": [
      {
        "artifact": "Generic.Client.Info",
        "parameters": {
          "env": []
        }
      }
    ],
    "progress_timeout": 300,
    "cpu_limit": 100,
    "timeout": 600,
    "max_rows": 500,
    "max upload bytes": 2097152
  },
  "condition": {},
  "expires": 1738265073732000,
  "hunt_description": "Prueba de nuestro primer Hunt",
  "tags": [
    "Hunt1"
  ],
  "state": 2
}
```


Conexión con velociraptor


```
","user-agent":"Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"}
[INFO] 2025-01-23T20:26:01Z  {"method":"GET","remote":"127.0.0.1:58520","status":200,"url":"/api/v1/GetHuntTable","user":"admin","
user-agent":"Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"}
[INFO] 2025-01-23T20:26:01Z  {"method":"GET","remote":"127.0.0.1:58520","status":200,"url":"/api/v1/GetUserUITraits","user":"admin
","user-agent":"Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"}
[INFO] 2025-01-23T20:26:06Z  {"method":"GET","remote":"127.0.0.1:58520","status":200,"url":"/api/v1/GetHuntTable","user":"admin","
user-agent":"Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"}
[INFO] 2025-01-23T20:26:06Z  {"method":"GET","remote":"127.0.0.1:58520","status":200,"url":"/api/v1/GetUserUITraits","user":"admin
","user-agent":"Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"}
[INFO] 2025-01-23T20:26:11Z  {"method":"GET","remote":"127.0.0.1:58520","status":200,"url":"/api/v1/GetHuntTable","user":"admin","
user-agent":"Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"}
[INFO] 2025-01-23T20:26:11Z  {"method":"GET","remote":"127.0.0.1:58520","status":200,"url":"/api/v1/GetUserUITraits","user":"admin
","user-agent":"Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"}
[INFO] 2025-01-23T20:26:16Z  {"method":"GET","remote":"127.0.0.1:58520","status":200,"url":"/api/v1/GetHuntTable","user":"admin","
user-agent":"Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"}
[INFO] 2025-01-23T20:26:16Z  {"method":"GET","remote":"127.0.0.1:58520","status":200,"url":"/api/v1/GetUserUITraits","user":"admin
","user-agent":"Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"}
[INFO] 2025-01-23T20:26:21Z  {"method":"GET","remote":"127.0.0.1:58520","status":200,"url":"/api/v1/GetHuntTable","user":"admin","
user-agent":"Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"}
[INFO] 2025-01-23T20:26:21Z  {"method":"GET","remote":"127.0.0.1:58520","status":200,"url":"/api/v1/GetUserUITraits","user":"admin
","user-agent":"Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"}
[INFO] 2025-01-23T20:26:26Z  {"method":"GET","remote":"127.0.0.1:58520","status":200,"url":"/api/v1/GetHuntTable","user":"admin","
user-agent":"Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"}
[INFO] 2025-01-23T20:26:26Z  {"method":"GET","remote":"127.0.0.1:58520","status":200,"url":"/api/v1/GetUserUITraits","user":"admin
","user-agent":"Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"}
[INFO] 2025-01-23T20:26:31Z  {"method":"GET","remote":"127.0.0.1:58520","status":200,"url":"/api/v1/GetHuntTable","user":"admin","
```

Conexión con un cliente

El cliente en este ejercicio vamos a ser nosotros mismos, es importante configurarlo para que se vea como actúa este software

Generar un archivo de configuración del cliente basado en el servidor:

 # ./velociraptor-v0.73.1-linux-amd64 config client -c velociraptor.config.yaml > client.config.yaml

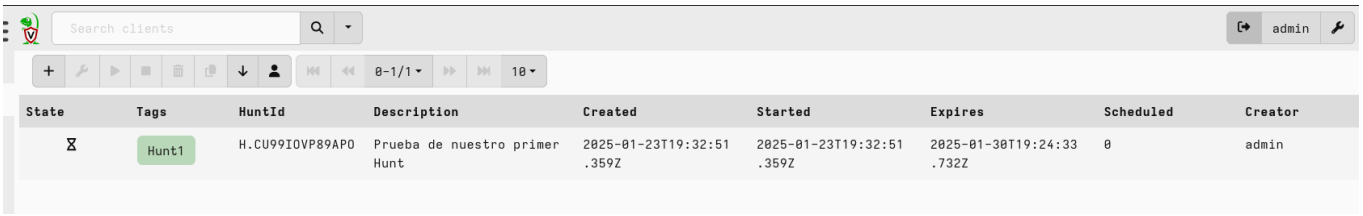
```
┌──(root㉿kali)-[/home/jesus/Desktop/Velociraptor]
└─# ./velociraptor-v0.73.1-linux-amd64 config client -c ../../../../opt/velociraptor/config/velocir
aptor.config.yml > ../../../../opt/velociraptor/config/client.config.yaml
```

Ejecutar el cliente en la misma máquina

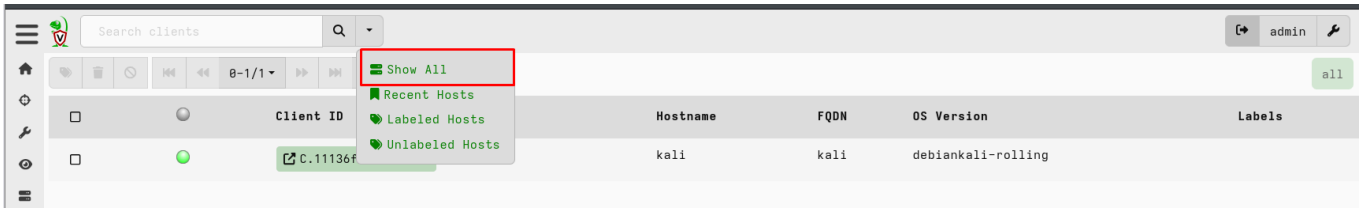
./velociraptor-v0.73.1-linux-amd64 --config client.config.yaml client

```
┌──(root㉿kali)-[/home/jesus/Desktop/Velociraptor]
└─# ./velociraptor-v0.73.1-linux-amd64 --config ../../../../opt/velociraptor/config/client.config.y
ml client
```

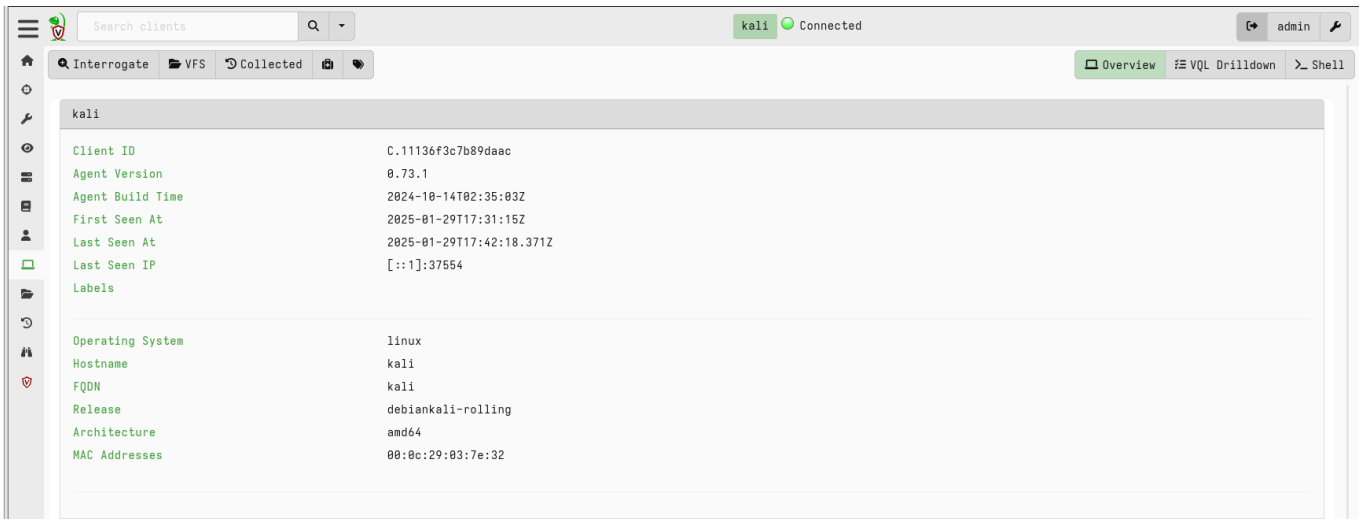
Estado del hunt



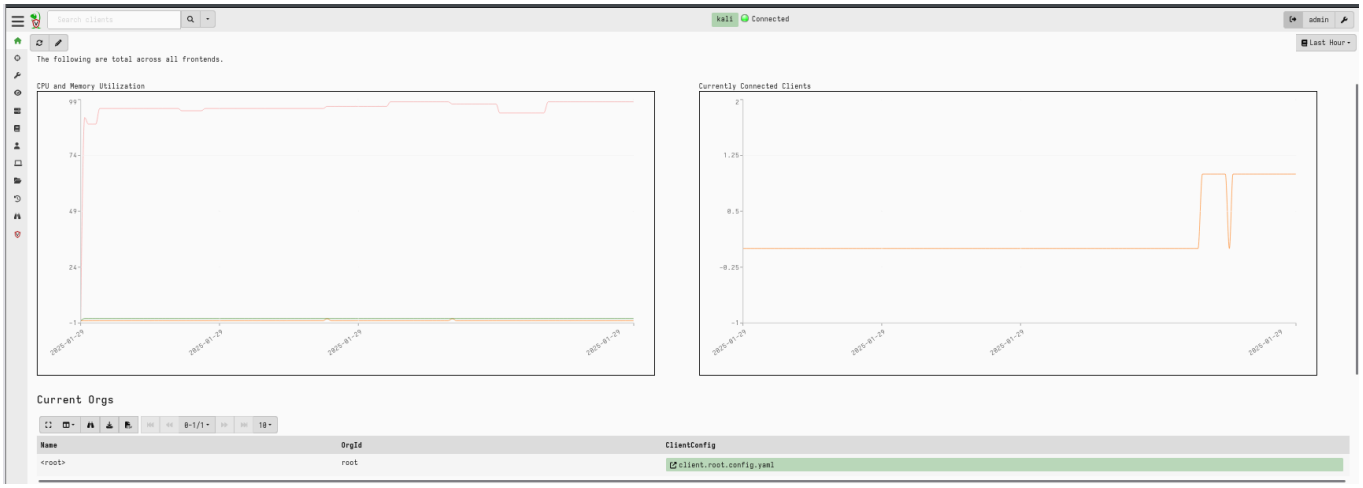
Podemos ver en show all que el cliente está activo



En el área izquierda en el ordenador podemos ver la información del cliente



En el inicio podemos ver la actividad del cliente.



Conclusiones:

Velociraptor es una herramienta poderosa, eficiente y altamente flexible para la recolección y análisis forense digital en sistemas distribuidos. Su diseño se centra en la rapidez y precisión, permitiendo que analistas forenses y equipos de respuesta a incidentes recopilen evidencia e información de múltiples sistemas de forma centralizada.

Una gran ventaja es que permite gestionar grandes cantidades de clientes desde un único servidor, ideal para investigaciones a gran escala o entornos corporativos.

Fuentes:

https://medium.com/@0xCybersec_Matt/setting-up-a-velociraptor-instance-af1a98098331
https://samsclass.info/152/proj/IR371.htm
https://www.youtube.com/watch?v=3M0IIROV-RU