

W16D1 - Exploit Telnet

verifichiamo la vulnerabilità con telnet_version su Metasploitable

avviamo msfconsole

cerchiamo telnet version e lo selezionamo, verifichiamo le impostazioni con options

```
msf > search telnet_version

Matching Modules
=====
#  Name
-
0  auxiliary/scanner/telnet/lantronix_telnet_version
1  auxiliary/scanner/telnet/telnet_version

Interact with a module by name or index. For example info

msf > use 1
msf auxiliary(scanner/telnet/telnet_version) > options

Module options (auxiliary/scanner/telnet/telnet_version)

Name      Current Setting  Required  Description
----      ----           ----       -----
PASSWORD          no        The password for
RHOSTS           yes       The target host()
RPORT            23        yes       The target port
THREADS          1         yes       The number of co
TIMEOUT          30        yes       Timeout for the
USERNAME          no        The username to
```

settiamo RHOSTS con 192.168.50.101 (ip Metasploitable), USERNAME msfadmin e
PASSWORD msfadmin, infine run

in conclusione possiamo verificare la vulnerabilità con telnet, come in figura sotto proprio ci dice di loggarci con le credenziali scritte