

W16D1 - Exploit Telnet

verifichiamo la vulnerabilità con telnet_version su Metasploitable

avviamo msfconsole

```
kali@kali:~$ msfconsole
Metasploit tip: Use the edit command to open the currently active module
in your editor

      .~+P`~~~~~-o+!:..      -o+!:..
    .+000yssyysyysyddh++os-      -o+!:..
    ++++++sydhyoyso/:.```` ...`... -/// ::+ohhyosyosy/+om++:000///
    ++++++////////~//+++++ooysoysoosso+++++////////00SSO:
    --.`      .-.- ... -///+++++////////~////////+++++///
      .~+P`~~~~~-o+!:..      -o+!:..

      .:~+P`~~~~~-o+!:..      -o+!:..
    .hmMMMMMMMMMMNddds\ ... //M\\ ... /hdddmMMMMMMNo
    :Nm-/NMMMMMMMMMMMMM$$$NMMMMM66MMMMMMMMMMMMMMMy
    .sm/^-yMMMMMMMMMMMMM$$$NMMMMM66MMMMMMMMMMMMMMh`
    -Nd`  :MMMMMMMMMMMMM$$$NMMMMM66MMMMMMMMMMMMMMh`
    -Nh`  .yMMMMMMMMMMMMM$$$NMMMMM66MMMMMMMMMMMMMm/
    .sNd` :MMMMMMMMMMMMM$$$NMMMMM66MMMMMMMMMMMMMm/
    -mh`  :MMMMMMMMMMMMM$$$NMMMMM66MMMMMMMMMMMMMd
    `:`    -o+++o000+:/o0000+:+o+++o000++/
    `///omh//dMMMMMMMMMMMMMMN/::::/+ooso--/ydh//+s+/osssso:--syN///os:
    /MMMMMMMMMMMMMMMMMMMMMd.  /++-.-yy/ ... osydh/-+oo:-`o// ... oyodh+
    -hMMmssddd+:dMMmNMMh.  .-=mmk.//^^^\\.^^^:++:^^^0://^^^\\`::
    .sMMmo.      -dMd--:mN/`  ||—X—||      ||—X—||
```

cerchiamo telnet_version e lo selezioniamo, 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 '0'

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

Module options (auxiliary/scanner/telnet/telnet_version)

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

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

```
msf auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.50.101
rhosts => 192.168.50.101
msf auxiliary(scanner/telnet/telnet_version) > set username msfadmin
username => msfadmin
msf auxiliary(scanner/telnet/telnet_version) > set password msfadmin
password => msfadmin
msf auxiliary(scanner/telnet/telnet_version) > run
[+] 192.168.50.101:23 - 192.168.50.101:23 TELNET _
( ) | _ _ _ | | _ _ _ | \ \x0a| ' _ _ _ \ / _ _ \ _ _ / _ _ \ | ' _ \ | /
| || ( _ | | | _ ) | | _ // _ / \x0a| | | | | \ _ _ | \ _ _ \ , _ _ / . _ / | \ \
                                     \x0a\x0a\x0aWarning: Never expose this VM to a
admin/msfadmin to get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.50.101:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/telnet/telnet_version) >
```

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

```
(kali㉿kali)-[~]  
$ telnet 192.168.50.101 23  
Trying 192.168.50.101 ...  
Connected to 192.168.50.101.  
Escape character is '^]'.  
  
metasploitable  
  
Warning: Never expose this VM to an untrusted network!  
Contact: msfdev[at]metasploit.com  
Login with msfadmin/msfadmin to get started  
  
metasploitable login: Connection closed by foreign host.
```