

```
kali@kali: ~  
File Actions Edit View Help  
msf6 > search telnet  
Matching Modules  


| # | Rank      | Name                                               | Check | Description                                                       | Disclosure Date |
|---|-----------|----------------------------------------------------|-------|-------------------------------------------------------------------|-----------------|
| 0 | excellent | exploit/linux/misc/asus_infosvr_auth_bypass_exec   | No    | ASUS infosvr Auth Bypass Command Execution                        | 2015-01-04      |
| 1 | excellent | exploit/linux/http/asuswrt_lan_rce                 | No    | AsusWRT LAN Unauthenticated Remote Code Execution                 | 2018-01-22      |
| 2 | normal    | auxiliary/server/capture/telnet                    | No    | Authentication Capture: Telnet                                    |                 |
| 3 | normal    | auxiliary/scanner/telnet/brocade_enable_login      | No    | Brocade Enable Login Check Scanner                                |                 |
| 4 | average   | exploit/windows/proxy/ccproxy_telnet_ping          | Yes   | CCProxy Telnet Proxy Ping Overflow                                | 2004-11-11      |
| 5 | normal    | auxiliary/dos/cisco/ios_telnet_rocem               | No    | Cisco IOS Telnet Denial of Service                                | 2017-03-17      |
| 6 | normal    | auxiliary/admin/http/dlink_dir_300_600_exec_noauth | No    | D-Link DIR-600 / DIR-300 Unauthenticated Remote Command Execution | 2013-02-04      |
| 7 | excellent | exploit/linux/http/dlink_diagnostic_exec_noauth    | No    | D-Link DIR-645 / DIR-815 diagnostic.php Command Execution         | 2013-03-05      |
| 8 | excellent | exploit/linux/http/dlink_dir300_exec_telnet        | No    | D-Link DIR-300 Telnet Command Execution                           | 2013-04-22      |


```

Avvio msfconsole da terminale kali e cerco la vulnerabilita' telnet da sfruttare

```
kali@kali: ~  
File Actions Edit View Help  
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   |                 | 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    | 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) > set RHOSTS 192.168.1.40  
RHOSTS => 192.168.1.40  
msf6 auxiliary(scanner/telnet/telnet_version) >
```

una volta trovata la selezione col comando use e poi col comando show options vedo le impostazioni necessarie all'utilizzo, in questo caso devo impostare l'indirizzo ip target

