CONSEGNA U2 S7 L2

- **Parte 1 (Configurazione macchine)**

Come richiesto dall'esercizio, ho iniziato modificando gli indirizzi IP delle macchine Kali e Metasploitable. Rispettivamente in **192.168.1.24** e **192.168.1.40**.

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:33:90:f7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.40/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fe33:90f7/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

```
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default q
len 1000
    link/ether 08:00:27:b0:e9:cf brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.25/24 brd 192.168.1.255 scope global noprefixroute eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::8ef3:df8c:614d:4845/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

- **Parte 2 (Ricerca degli script e setting parametri)**

Aprendo **msfconsole**, ho usato il comando **search** per cercare lo script di tipo **auxiliary** nominato **telnet_version**. Ho trovato due scripts. Quello da scegliere, perché richiesto dall'esercizio, è **telnet_version** evidenziato in verde.

```
msf6 > search telnet version

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank    Check  Description
   -  ----                                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/telnet/lantronix_telnet_version     .                normal  No     Lantronix Telnet Servic
e Banner Detection
   1  auxiliary/scanner/telnet/telnet_version               .                normal  No     Telnet Service Banner D
etection


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_versio
n
```

Utilizzo il comando **use 1** per selezionare lo script.

Tramite il comando **show options**, dopo aver selezionato lo script, verifico i parametri necessari al corretto funzionamento dello stesso. In questo caso è richiesto il parametro **rhost** (IP della vittima, Remote Host). Inserisco quindi l'indirizzo IP della Metasploitable (**192.168.1.40**).

```
msf6 > use 1
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 https://docs.metasploit.com/docs/using-metaspl
                                        oit/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.
```

Eseguo una seconda verifica dei parametri con show options. Adesso **rhost** è settato correttamente.

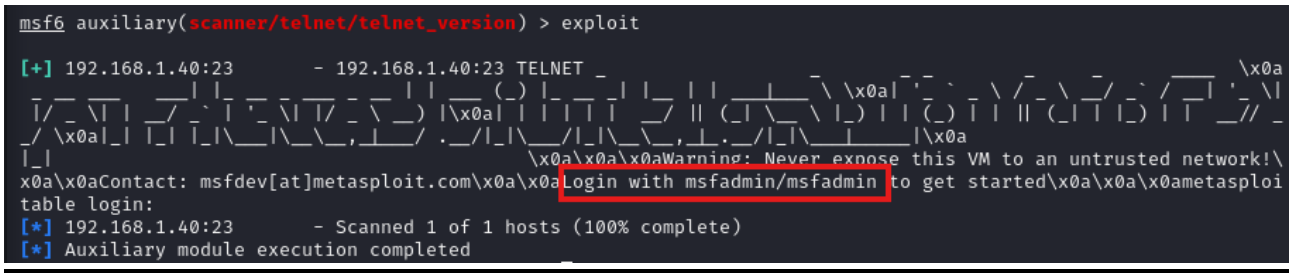
```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhost 192.168.1.40
rhost ⇒ 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > show options

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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS    192.168.1.40     yes       The target host(s), see https://docs.metasploit.com/docs/using-metaspl
                                        oit/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.
```

- **Parte 3 (Esecuzione attacco)**
  Con il comando exploit avvio l'attacco da **msfconsole**. Se l'attacco va a buon fine, visualizzerò a schermo la pagina di benvenuto del servizio **telnet** sulla Metasploitable e le credenziali che lo script ha trovato, necessarie ad effettuare il login. In questo caso le credenziali sono: **user = msfadmin** e **password = msfadmin** (sottolineati di rosso).



- **Verifica finale (Login su telnet all'IP di Metasploitable)**
  Infine eseguo la prova del nove. Provo ad accedere a telnet sulla Metasploitable con le credenziali recuperate dall'attacco. Il login è eseguito con successo! L'accesso è stato eseguito con privilegi di root ed è verificabile usando il comando **id**.