S7_L2

Traccia: Sulla base dell'esercizio visto in lezione teorica, utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

Requisito: Seguire gli step visti in lezione teorica. Prima, configurate l'ip della vostra Kali con 192.168.1.25 e l'ip della vostra Metasploitable con 192.168.1.40

1. **Apriamo la console di Metasploite con il comando di msfconsole**

```
msf6 > search telnet

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

   #   Name                                                  Disclosure Date
   -   ----                                                  ---------------
   0   exploit/linux/misc/asus_infosvr_auth_bypass_exec      2015-01-04
   1   exploit/linux/http/asuswrt_lan_rce                    2018-01-22
   2   auxiliary/server/capture/telnet                       .
   3   auxiliary/scanner/telnet/brocade_enable_login         .
   4   exploit/windows/proxy/ccproxy_telnet_ping             2004-11-11
   5     \_ target: Automatic                                .
   6     \_ target: Windows 2000 Pro All - English           .
   7     \_ target: Windows 2000 Pro All - Italian           .
   8     \_ target: Windows 2000 Pro All - French            .
   9     \_ target: Windows XP SP0/1 - English               .
   10    \_ target: Windows XP SP2 - English                 .
```

2. **Visualizziamo il servizio che ci serve**

```
73  auxiliary/scanner/telnet/telnet_version                    .          normal     No     Telnet Service Banner Detection
```

3. **Visualizziamo le opzioni disponibili**

```
msf6 > use 73
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 u
   RHOSTS                     yes       The target host(s), see https://
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate as
```

4. **Possiamo già visualizzare nella prima riga lo user e la password**

5. **Inserendo il comando telnet con l'indirizzo ip del target riusciamo a visualizzare il banner di Metasploitable e di conseguenza inserire le credenziali per accedere**