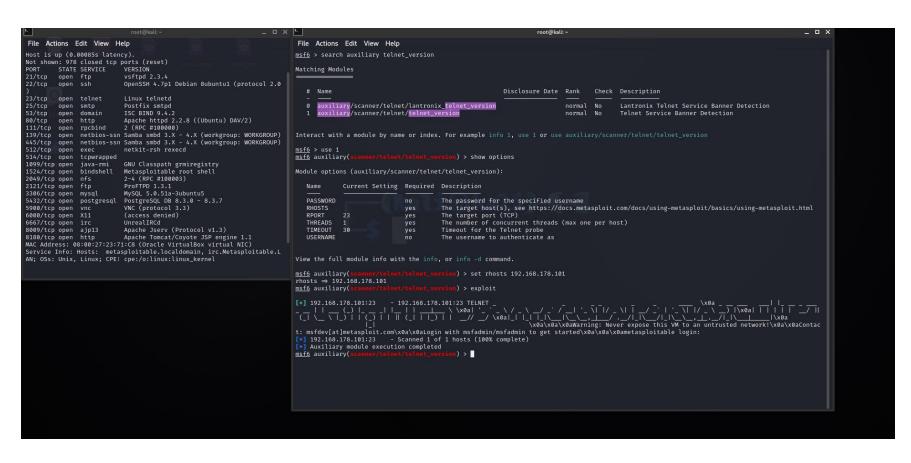
S7 L2

Davide Andreozzi

Andiamo ad utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

- 1- Scansioniamo l'ip target tramite nmap e vediamo il servizio attivo sulla porta 23
- 2- Avviamo Metasploit e cerchiamo il modulo ausiliario che ci serve tramite il comando «search auxiliary telnet_version», diamo invio e utilizziamo il #1 (use 1)
- 3- Settiamo il modulo, in particolare rhosts con l'ip target su cui eseguire l'exploit
- 4- Tramite il comando «exploit» avviamo l'exploit e analizziamo l'output, in particolare la riga «login with msfadmin/msfadmin» che ci va a indicare user e password per il login per telnet



Testiamo la connessione con le credenziali exploitate da Metasploit.

- 1- Tramite riga di comando ci colleghiamo con telnet sulla macchina target e inseriamo le credenziali che ci ha dato l'output di Metasploit (Screen 1).
- 2- Una volta entrati vediamo che tramite il comando ifconfig ci restituisce l'ip della macchina bersaglio (Screen 2).

```
telnet 192.168.178.101
Trying 192.168.178.101 ...
Connected to 192.168.178.101.
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
Last login: Tue Jan 23 07:41:50 EST 2024 from 192.168.178.100 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2
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/
```

```
msfadmin@metasploitable:~$ ifconfig
         Link encap:Ethernet HWaddr 08:00:27:23:71:c8
         inet addr:192.168.178.101 Bcast:192.168.178.255 Mask:255.2
55.255.0
         inet6 addr: 2002:5102:875a:0:a00:27ff:fe23:71c8/64 Scope:Glo
         inet6 addr: fe80::a00:27ff:fe23:71c8/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
         RX packets:21520 errors:0 dropped:0 overruns:0 frame:0
         TX packets:4458 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:1543245 (1.4 MB) TX bytes:394375 (385.1 KB)
         Base address:0×d020 Memory:f0200000-f0220000
         Link encap:Local Loopback
         inet addr:127.0.0.1 Mask:255.0.0.0
         inet6 addr: ::1/128 Scope:Host
         UP LOOPBACK RUNNING MTU:16436 Metric:1
         RX packets:1178 errors:0 dropped:0 overruns:0 frame:0
         TX packets:1178 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:536289 (523.7 KB) TX bytes:536289 (523.7 KB)
msfadmin@metasploitable:~$
```