

EPICODE-CS0124

S7/L2 - Pratica

Flaviano Sedici

Indice

Traccia	3
1. Configurazione della rete e ricognizione preliminare	4
1.1.Modifica configurazione Metasploitable.....	4
1.2.Modifica configurazione Kali	4
1.3.Analisi preliminare con nmap	4
2. Metasploit.....	5
2.1.Avvio Metasploit e ricerca modulo	5
2.2.Configurazione modulo	5
2.3.Fase di Exploit	5
2.4.Connessione al protocollo telnet.....	5

Riferimenti e versioni

Responsabile/referente del documento: Flaviano Sedici

Versionamento

Versione	Descrizione	Ruolo	Data
1.0	Redazione documento	Responsabile	05/03/2024

Traccia

Exploit Telnet con Metasploit

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.

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.

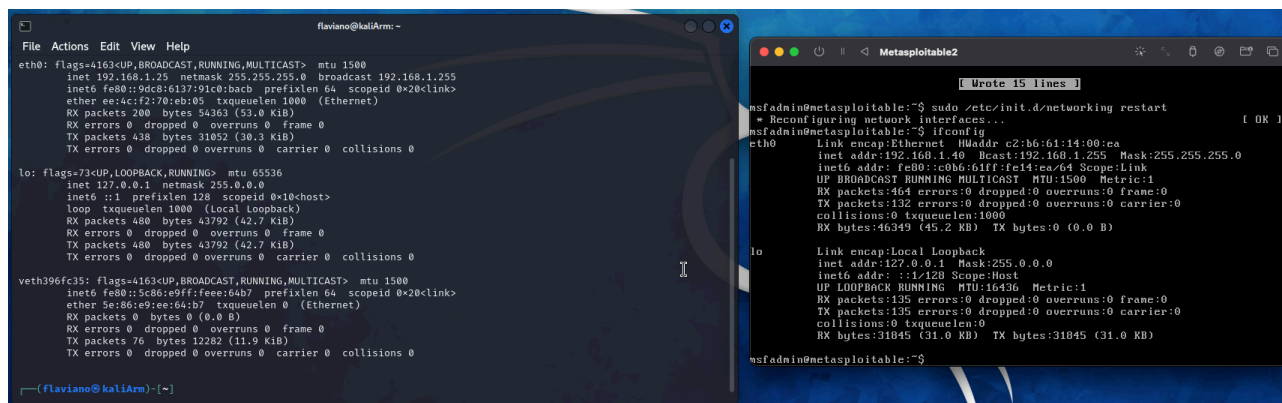
1. Configurazione della rete e ricognizione preliminare

1.1. Modifica configurazione Metasploitable

Come indicato dalla traccia, procediamo alla configurazione della rete su Metasploitable impostando l'indirizzo IP su 192.168.1.40/24.

1.2. Modifica configurazione Kali

Per completare la configurazione, procediamo alla modifica anche della rete di Kali, impostando l'indirizzo IP su 192.168.1.25/24.



```

flaviano@kaliArm: ~
File Actions Edit View Help
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.25 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::9dc8:6137:91c0:bach prefixlen 64 scopeid 0x20<link>
    ether e8:4c:12:70:eb:05 txqueuelen 1000 (Ethernet)
    RX packets 200 bytes 54363 (53.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 438 bytes 31052 (30.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 480 bytes 43792 (42.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 480 bytes 43792 (42.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

veth396fc35: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::5c86:c9ff:fee:6ab7 prefixlen 64 scopeid 0x20<link>
    ether 5e:86:e9:ee:64:b7 txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 76 bytes 12282 (11.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

--(Flaviano@kaliArm)~--

msfadmin@metasploitable:~$ sudo /etc/init.d/networking restart
* Reconfiguring network interfaces...
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr c2:b6:61:14:00:ea
          inet addr:192.168.1.40 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::c0b6:61ff:fe14:ee64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:464 errors:0 dropped:0 overruns:0 frame:0
          TX packets:132 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:46349 (45.2 KB)  TX bytes:0 (0.0 B)

lo        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:135 errors:0 dropped:0 overruns:0 frame:0
          TX packets:135 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:31045 (31.0 KB)  TX bytes:31045 (31.0 KB)

msfadmin@metasploitable:~$
  
```

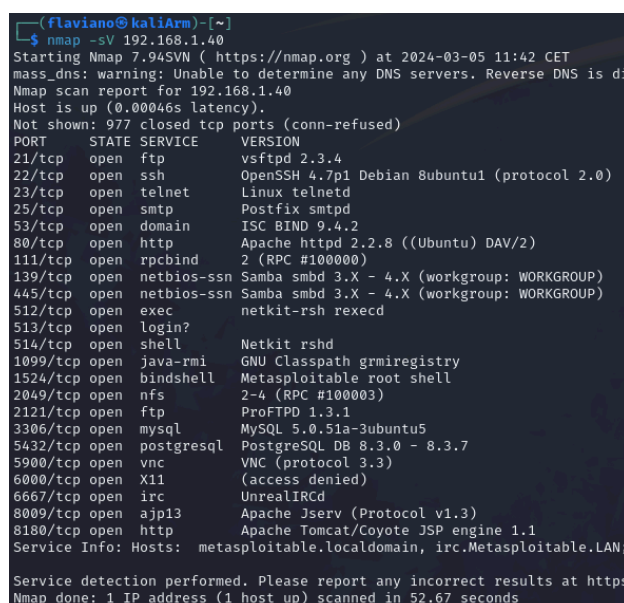
Configurazione Metasploitable e Kali

1.3. Analisi preliminare con nmap

Abbiamo effettuato una analisi esplorativa dei servizi esposti su Metasploitable tramite l'esecuzione del comando:

nmap -sV 192.168.1.40

Come si evince dall'immagine la porta 23 risulta aperta e funzionante con il demone **Linux Telnet**. Possiamo quindi procedere con Metasploit.



```

(flaviano@kaliArm)~$ nmap -sV 192.168.1.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-05 11:42 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Nmap scan report for 192.168.1.40
Host is up (0.00046s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN;

Service detection performed. Please report any incorrect results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 52.67 seconds
  
```

Scansione nmap sulla VM Metasploitable

2. Metasploit

2.1. Avvio Metasploit e ricerca modulo

Avviamo Metasploit tramite il comando **msfconsole** e procediamo alla ricerca del servizio con il comando **telnet_version**.

Il nostro interesse ricade sull'exploit e non sul modulo ausiliario, quindi procediamo a selezionarlo con il comando **use 1**

```
msf6 > search telnet_version

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -              -    -    -    -
0  auxiliary/scanner/telnet/lantronix_telnet_version  normal  No     Lantronix Telnet Service Banner Detection
1  auxiliary/scanner/telnet/telnet_version           normal  No     Telnet Service Banner Detection

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_version

msf6 > use 1
msf6 auxiliary(scanner/telnet/telnet_version) > show options

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

Name      Current Setting  Required  Description
--      -
PASSWORD  no               no        The password for the specified username
RHOSTS    yes              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) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
```

Risultati ricerca moduli Metasploit

2.2. Configurazione modulo

Procediamo con il comando **show options** che ci mostra tutte le impostazioni dell'exploit selezionato e notiamo come sia da configurare il parametro **RHOSTS**, che rappresenta la nostra VM target.

Con il comando **set RHOSTS 192.168.1.40** impostiamo Metasploitable come target.

2.3. Fase di Exploit

Procediamo con la fase di exploit tramite il comando **exploit** e attendiamo che il payload ci consenta di accedere alla shell di comando della macchina target.

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

[*] 192.168.1.40:23 - 192.168.1.40:23 TELNET
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Esecuzione del modulo con il comando exploit

L'esecuzione del modulo ci restituisce il nome utente e la password con i quali accedere alla macchina target.

2.4. Connessione al protocollo telnet

Proviamo ad utilizzare il protocollo telnet sulla macchina target con le credenziali ottenute per verificarne la correttezza.

```
(flaviano@kaliArm)-[~]
$ telnet 192.168.1.40
Trying 192.168.1.40...
Connected to 192.168.1.40.
Escape character is '^]'.
msfadmin

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 Mar  5 05:36:45 EST 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:~$
```

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr c2:b6:61:14:00:ea
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::c0b6:61ff:fe14:ea/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2049 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1582 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:152783 (149.2 KB)  TX bytes:0 (0.0 B)

lo        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:217 errors:0 dropped:0 overruns:0 frame:0
          TX packets:217 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:61373 (59.9 KB)  TX bytes:61373 (59.9 KB)

msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$
```

Esecuzione telnet e relativi comandi di verifica

La connessione è stata stabilita con successo tramite il comando **telnet 192.168.1.40** e le credenziali ottenute.

Abbiamo provato ad eseguire i comandi **ifconfig** e **ls** per verificare la correttezza dell'operazione, ottenendo i risultati presenti nell'immagine.