

S7 L2

Davide Andreozzi

Andiamo ad utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

1- Scansioniamo l'ip target tramite nmap e vediamo il servizio attivo sulla porta 23

2- Avviamo Metasploit e cerchiamo il modulo ausiliario che ci serve tramite il comando «search auxiliary telnet_version», diamo invio e utilizziamo il #1 (use 1)

3- Settiamo il modulo, in particolare rhosts con l'ip target su cui eseguire l'exploit

4- Tramite il comando «exploit» avviamo l'exploit e analizziamo l'output, in particolare la riga «login with msfadmin/msfadmin» che ci va a indicare user e password per il login per telnet

```
root@kali: ~  
File Actions Edit View Help  
Host is up (0.00085s latency).  
Not shown: 978 closed tcp ports (reset)  
PORT      STATE SERVICE  
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  
514/tcp   open  tcpwrapped  
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  
MAC Address: 08:00:27:23:71:C8 (Oracle VirtualBox virtual NIC)  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
root@kali: ~  
File Actions Edit View Help  
msf6 > search auxiliary 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        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.  
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.178.101  
rhosts => 192.168.178.101  
msf6 auxiliary(scanner/telnet/telnet_version) > exploit  
[*] 192.168.178.101:23 - 192.168.178.101:23 TELNET  
t: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0ametasploitable login:  
[*] 192.168.178.101:23 - Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Testiamo la connessione con le credenziali exploitare da Metasploit.

1- Tramite riga di comando ci colleghiamo con telnet sulla macchina target e inseriamo le credenziali che ci ha dato l'output di Metasploit (Screen 1).

2- Una volta entrati vediamo che tramite il comando *ifconfig* ci restituisce l'ip della macchina bersaglio (Screen 2).

```
(root@kali)~# telnet 192.168.178.101
Trying 192.168.178.101...
Connected to 192.168.178.101.
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 Jan 23 07:41:50 EST 2024 from 192.168.178.100 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2
008 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/
```

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:23:71:c8
          inet addr:192.168.178.101  Bcast:192.168.178.255  Mask:255.2
          55.255.0
          inet6 addr: 2002:5102:875a:0:a00:27ff:fe23:71c8/64 Scope:Glo
          bal
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:21520 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4458 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1543245 (1.4 MB)  TX bytes:394375 (385.1 KB)
          Base address:0xd020 Memory:f0200000-f0220000

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:1178 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1178 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:536289 (523.7 KB)  TX bytes:536289 (523.7 KB)

msfadmin@metasploitable:~$
```