

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

Metasploit utilizza due tipologie di moduli:

- **Moduli normali:**
 - eseguono attacchi diretti per sfruttare falle di sicurezza note;
 - eseguono attacchi diretti per sfruttare l'accesso al sistema;
 - eseguono azioni post-attacco per il mantenimento dell'accesso al sistema;
 - Utilizzano i payload.
- **Moduli ausiliari** (Auxiliary Modules):
 - Progettati per svolgere supporto durante il test della sicurezza (scansione della rete, Information Gathering etc.);
 - Non effettuano attacchi diretti, ma forniscono informazioni aggiuntive utili per ottenere il quadro completo della sicurezza della rete o del sistema;
 - Non utilizzano, quasi mai, i payload.

Esercizio:

Kali Linux IP **192.168.50.100** (Macchina attaccante)

Metasploitable 2 IP **192.168.50.101** (Macchina vittima)

Eseguito il comando «**nmap -sV 192.168.50.101**» per scansionare il target e raccogliere le informazioni sulle porte aperte, i servizi collegati e le relative versioni.

```
(root@kali) - [/home/kali]
# nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-23 06:47 EST
Nmap scan report for 192.168.50.101
Host is up (0.0031s 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?
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?
513/tcp   open  login?
514/tcp   open  shell?
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  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
MAC Address: 08:00:27:7F:2E:06 (Oracle VirtualBox virtual NIC)
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 194.13 seconds
```

Avviato Metasploit con il comando «**msfconsole**»

```
(root@kali)-[/home/kali]
# msfconsole
Metasploit tip: Use the 'capture' plugin to start multiple authentication-capturing and poisoning services
Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (reset)
PORT      ..:ok000kdc' SERVICE      'cdk000ko:.
21/tcp    .x00000000000000c      c0000000000000x.
22/tcp    :000000000000000k,      ,k000000000000000: Debian 8ubuntu1 (p
23/tcp    '000000000k00000: :0000000000000000'
24/tcp    o00000000. MMMM. o0000o0000L. MMMM, 00000000o
25/tcp    d00000000. MMMMMM. c00000c. MMMMMM, 00000000x
26/tcp    l00000000. MMMMMMMMM; d; MMMMMMMMM, 00000000L
27/tcp    .00000000. MMM. ; MMMMMMMMMMMMM; MMMM, 00000000.
28/tcp    c0000000. MMM. 00c. MMMMM 'o00. MMM, 0000000c - 4.X (workgroup:
29/tcp    o000000. MMM. 0000. MMM: 0000. MMM, 000000oX - 4.X (workgroup:
30/tcp    l00000. MMM. 0000. MMM: 0000. MMM, 000000L
31/tcp    ;0000' MMM. 0000. MMM: 0000. MMM; 0000;
32/tcp    .d00o' WM. 0000o000cX0000. MX' x00d.
33/tcp    ,kol' M. 00000000000000. M' d0k, spath grmiregistry
34/tcp    :kk; .00000000000000. ;ok: (nitable root shell
35/tcp    ;k000000000000000k: (RPC #1000003)
36/tcp    ,x000000000000x,
37/tcp    mv. l0000000L.
38/tcp    ,d0d, PostgreSQL DB 8.3.0 - 8.3.
39/tcp    vnc . VNC (protocol 3.3)
40/tcp    X11 (access denied)
41/tcp    = [ metasploit v6.3.51-dev | IRCd ]
+ -- -- [ 2384 exploits - 1235 auxiliary - 418 post (v1.3) ]
+ -- -- [ 1391 payloads - 46 encoders - 11 nops (JSP engine) ]
+ -- -- [ 9 evasion (7:7F:2E:06 (Oracle VirtualBox virtual) ]
Metasploit Documentation: https://docs.metasploit.com/
Service detection performed. Please report any incorrect res
msf6 >
```

Cercato l'exploit del servizio telnet nei moduli ausiliari con «**search auxiliary telnet**»

```
msf6 > search auxiliary telnet
Matching Modules
=====
#  Name
-  -
0  auxiliary/server/capture/telnet (Ubuntu) DAV/2)
1  auxiliary/scanner/telnet/brocade_enable_login
2  auxiliary/dos/cisco/ios_telnet_rocem
3  auxiliary/admin/http/dlink_dir_300_600_exec_noauth
4  auxiliary/scanner/ssh/juniper_backdoor
5  auxiliary/scanner/telnet/lantronix_telnet_password
6  auxiliary/scanner/telnet/lantronix_telnet_version
7  auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof
8  auxiliary/admin/http/netgear_pnp_getsharefolderlist_auth_bypass
9  auxiliary/admin/http/netgear_r6700_pass_reset
10 auxiliary/admin/http/netgear_r7000_backup.cgi_heap_overflow_rce
11 auxiliary/scanner/telnet/telnet_ruggedcom
12 auxiliary/scanner/telnet/satel_cmd_exec
13 auxiliary/scanner/telnet/telnet_login
14 auxiliary/scanner/telnet/telnet_version
15 auxiliary/scanner/telnet/telnet_encrypt_overflow

Disclosure Date  Rank  Check  Description
-----
2017-03-17      normal No  Cisco IOS Telnet Denial of Service
2013-02-04      normal No  D-Link DIR-600 / DIR-300 Unauthenticated Remote Command Execu
2015-12-20      normal No  Juniper SSH Backdoor Scanner
2011-09-06      normal No  Lantronix Telnet Password Recovery
2010-12-21      normal No  Lantronix Telnet Service Banner Detection
2021-09-06      normal Yes  Microsoft IIS FTP Server Encoded Response Overflow Trigger
2020-06-15      normal Yes  Netgear PNPX_GetShareFolderList Authentication Bypass
2021-04-21      normal Yes  Netgear R6700v3 Unauthenticated LAN Admin Password Reset
2021-04-21      normal Yes  Netgear R7000 backup.cgi Heap Overflow RCE
2017-04-07      normal No  RuggedCom Telnet Password Generator
2017-04-07      normal No  Satel Iberia SenNet Data Logger and Electricity Meters Comman
d Injection Vulnerability
2021-09-06      normal No  Telnet Login Check Scanner
2021-09-06      normal No  Telnet Service Banner Detection
2021-09-06      normal No  Telnet Service Encryption Key ID Overflow Detection

Interact with a module by name or index. For example info 15, use 15 or use auxiliary/scanner/telnet/telnet_encrypt_overflow
```

Identificato l'exploit usarlo con «**use 14**» o, al posto del numero, il suo percorso.

```
msf6 > use 14
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

  Name      Current Setting  Required  Description
  ----      -
  PASSWORD  The password for the specified username
  RHOSTS    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  The username to authenticate as
```

Controllare con «**show options**» le opzioni che possono essere configurate.

Configurare rhosts (remote host) con il comando «**set rhosts 192.168.50.101**» e ricontrollare se il settaggio è andato a buon fine digitando di nuovo «**show options**»

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.50.101
rhosts => 192.168.50.101
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

  Name      Current Setting  Required  Description
  ----      -
  PASSWORD  The password for the specified username
  RHOSTS    192.168.50.101  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  The username to authenticate as
```

Lanciare l'exploit con «**exploit**»

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

[*] 192.168.50.101:23 - 192.168.50.101:23 TELNET
a\x0a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x00
ametasploitable login:
[*] 192.168.50.101:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Notiamo che l'exploit lanciato sul servizio telnet è andato a buon fine riuscendo a trovare la Username e Password della macchina. (Vedi figura).

Opzionale:

Configurate l'IP della vostra Kali con **192.168.1.25** e l'IP della vostra Metasploitable con **192.168.1.40**

Controllato che le due macchina comunicassero con il comando «ping»

```
(kali㉿kali)-[~]
$ ping 192.168.1.40
PING 192.168.1.40 (192.168.1.40) 56(84) bytes of data.
64 bytes from 192.168.1.40: icmp_seq=1 ttl=64 time=0.759 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.449 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.411 ms
64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=0.493 ms
^C
— 192.168.1.40 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3070ms
rtt min/avg/max/mdev = 0.411/0.528/0.759/0.136 ms
```

Eseguita una scansione con nmap

```

root@kali:~# nmap -sV 192.168.1.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-23 07:27 EST
Nmap scan report for 192.168.1.40
Host is up (0.00083s 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?
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?
513/tcp   open  login?
514/tcp   open  shell?
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  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
MAC Address: 08:00:27:7F:2E:06 (Oracle VirtualBox virtual NIC)
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 194.00 seconds

```

Dopo aver avviato Metasploit, cercato il modulo ausiliare del servizio telnet ed utilizzato, configuriamo il rhosts con l'indirizzo IP 192.168.1.40 e lanciamo l'exploit.

[illegible]