

Oggi eseguiremo un attacco al servizio telnet di metasploitable usando un modulo ausiliario di metasploit da kali. A differenza di un modulo normale, che esegue un attacco diretto sfruttando una vulnerabilità, un modulo ausiliario fornisce un ulteriore supporto alla fase di raccolta informazioni.

Telnet è un protocollo utilizzato tramite riga di comando per fornire ad un utente sessioni di login remoto che, a causa di vari problemi di sicurezza (vulnerabilità, trasmissione dei dati in chiaro e mancanza di uno schema di autenticazione sicuro), è stato sostituito da ssh.

Cominciamo con la classica scansione di nmap:

```
(kali@kali)-[~]
$ nmap -sV 10.0.2.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-23 12:59 CET
Nmap scan report for 10.0.2.19
Host is up (0.0030s latency).
Not shown: 978 closed tcp ports (conn-refused)
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
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
513/tcp   open  login          OpenBSD or Solaris rlogind
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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Proviamo a cercare un modulo per telnet su metasploit:

```
msf6 > search auxiliary telnet

Matching Modules

#  Name                                                                 Disclosure Date  Rank  Check  Description
-  -
0  auxiliary/server/capture/telnet                                     normal      No    Authentication Cap
ture: Telnet
1  auxiliary/scanner/telnet/brocade_enable_login                     normal      No    Brocade Enable Log
in Check Scanner
2  auxiliary/dos/cisco/ios_telnet_rocem                             2017-03-17    normal No    Cisco IOS Telnet D
enial of Service
3  auxiliary/admin/http/dlink_dir_300_600_exec_noauth               2013-02-04    normal No    D-Link DIR-600 / D
IR-300 Unauthenticated Remote Command Execution
4  auxiliary/scanner/ssh/juniper_backdoor                           2015-12-20    normal No    Juniper SSH Backdo
or Scanner
5  auxiliary/scanner/telnet/lantronix_telnet_password               normal      No    Lantronix Telnet P
assword Recovery
6  auxiliary/scanner/telnet/lantronix_telnet_version                normal      No    Lantronix Telnet S
ervice Banner Detection
7  auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof                     2010-12-21    normal No    Microsoft IIS FTP
Server Encoded Response Overflow Trigger
8  auxiliary/admin/http/netgear_pnp_getsharefolderlist_auth_bypass  2021-09-06    normal Yes   Netgear PNPX_GetSh
areFolderList Authentication Bypass
9  auxiliary/admin/http/netgear_r6700_pass_reset                    2020-06-15    normal Yes   Netgear R6700v3 Un
authenticated LAN Admin Password Reset
10 auxiliary/admin/http/netgear_r7000_backup.cgi_heap_overflow_rce  2021-04-21    normal Yes   Netgear R7000 back
up.cgi Heap Overflow RCE
11 auxiliary/scanner/telnet/telnet_ruggedcom                       normal      No    RuggedCom Telnet P
assword Generator
12 auxiliary/scanner/telnet/satel_cmd_exec                          2017-04-07    normal No    Satel Iberia SenNe
t Data Logger and Electricity Meters Command Injection Vulnerability
13 auxiliary/scanner/telnet/telnet_login                           normal      No    Telnet Login Check
Scanner
14 auxiliary/scanner/telnet/telnet_version                         normal      No    Telnet Service Ban
ner Detection
15 auxiliary/scanner/telnet/telnet_encrypt_overflow                normal      No    Telnet Service Enc
ryption Key ID Overflow Detection
```

Il modulo numero 14 sembra fare al caso nostro:

```
msf6 auxiliary(scanner/telnet/telnet_version) > info
Name: Telnet Service Banner Detection
Module: auxiliary/scanner/telnet/telnet_version
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
hdm <x@hdm.io>

Check supported:
No

Basic options:
```

Name	Current Setting	Required	Description
PASSWORD		no	The password for the specified username
RHOSTS		yes	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
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

```

Description:
Detect telnet services
```

Tramite il comando “info” vediamo che il modulo è in grado di scannerizzare il servizio telnet ed estrapolare le credenziali di accesso.

[illegible]

Come possiamo vedere dalla figura sopra ci vengono fornite le credenziali per il login con le quali possiamo accedere al servizio. Come detto prima il modulo ausiliario non effettua un attacco diretto, quindi dovremo eseguire l'accesso manualmente:

Warning: Never expose this VM to an untrusted network!

Login with msfadmin/msfadmin to get started

Password:

```
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
```

```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

<http://help.ubuntu.com/>

```
msfadmin@metasploitable:~$
```

```
eth0      Link encap:Ethernet  HWaddr 08:00:27:88:c1:59
          inet addr:10.0.2.19  Bcast:10.0.2.255  Mask:255.255.255.0
          Home    inet6 addr: fe80::a00:27ff:fe88:c159/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:86 errors:0 dropped:0 overruns:0 frame:0
          TX packets:102 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8322 (8.1 KB)  TX bytes:10518 (10.2 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:16384  Metric:1
        RX packets:97 errors:0 dropped:0 overruns:0 frame:0
        TX packets:97 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:21529 (21.0 KB)  TX bytes:21529 (21.0 KB)
```

```
msfadmin@metasploitable:~$ whoami
msfadmin
```

