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:

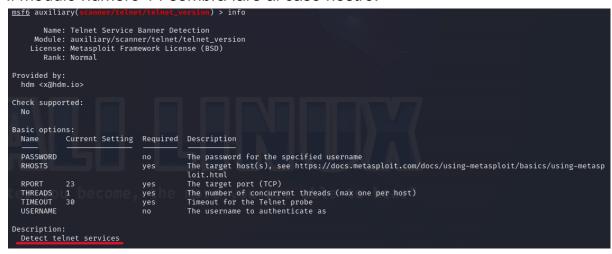
```
Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-23 12:59 CET Nmap scan report for 10.0.2.19 Host is up (0.0030s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
21/tcp open ftp
22/tcp open ssh
                                           OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
Linux telnetd
              open
              open smtp Postfix smtpd
open http Apache httpd 2,2.8 ((Ubuntu) DAV/2)
25/tcp
80/tcp
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)
                          exec
                                              netkit-rsh rexecd
OpenBSD or Solaris rlogind
513/tcp
                          login
              open
514/tcp open
                          tcpwrapped
                         tcpwrapped
java-rmi GNU Classpath grmiregistry
bindshell Metasploitable root shell
nfs 2-4 (RPC #100003)
ftp ProFTPD 1.3.1
1099/tcp open
 1524/tcp open
2049/tcp open nfs
2121/tcp open ftp
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)
5900/tcp open vnc
6000/tcp open X11
                                              (access denied)
UnrealIRCd
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open http
 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:

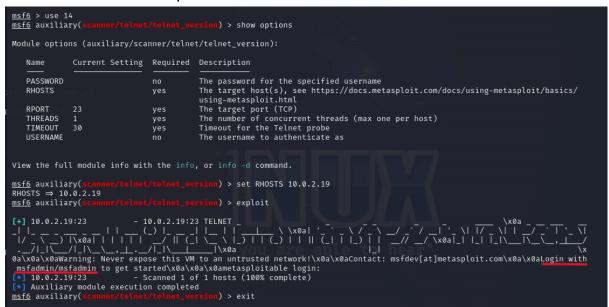
```
msf6 > search auxiliary telnet
Matching Modules
   # Name
                                                                                              Disclosure Date Rank
                                                                                                                              Check Description
       auxiliary/server/capture/telnet
                                                                                                                    normal No
                                                                                                                                       Authentication Cap
1 auxiliary/scanner/telnet/brocade_enable_login
in Check Scanner
                                                                                                                    normal No
                                                                                                                                       Brocade Enable Log
2 auxiliary/dos/cisco/ios_telnet_rocem
enial of Service
                                                                                              2017-03-17
                                                                                                                    normal No
                                                                                                                                       Cisco IOS Telnet D
3 auxiliary/admin/http/dlink_dir_300_600_exec_noauth
IR-300 Unauthenticated Remote Command Execution
                                                                                                                                       D-Link DIR-600 / D
                                                                                              2013-02-04
                                                                                                                    normal No
         auxiliary/scanner/ssh/juniper_backdoor
                                                                                              2015-12-20
                                                                                                                    normal No
                                                                                                                                        Juniper SSH Backdo
or Scanner
5 auxiliary/scanner/telnet/lantronix_telnet_password assword Recovery
                                                                                                                    normal No
                                                                                                                                       Lantronix Telnet P
         auxiliary/scanner/telnet/lantronix_telnet_version
                                                                                                                                       Lantronix Telnet S
ervice Banner Detection
7 auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof
Server Encoded Response Overflow Trigger
                                                                                              2010-12-21
                                                                                                                                       Microsoft IIS FTP
                                                                                                                    normal No
8 auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass 2021-09-06
areFolderList Authentication Bypass
                                                                                                                    normal Yes
                                                                                                                                        Netgear PNPX GetSh
9 auxiliary/admin/http/netgear_r6700_pass_reset 2020-06-15
authenticated LAN Admin Password Reset
10 auxiliary/admin/http/netgear_r7000_backup_cgi_heap_overflow_rce 2021-04-21
up.cgi Heap Overflow RCE
                                                                                                                                        Netgear R6700v3 Un
                                                                                                                    normal Yes
                                                                                                                    normal Yes
                                                                                                                                        Netgear R7000 back
    11 auxiliary/scanner/telnet/telnet_ruggedcom
                                                                                                                    normal No
                                                                                                                                        RuggedCom Telnet P
auxiliary/scanner/tetnet/tetnet_ruggedcom
assword Generator
12 auxiliary/scanner/telnet/satel_cmd_exec
t Data Logger and Electricity Meters Command Injection Vulnerability
13 auxiliary/scanner/telnet/telnet_login
                                                                                              2017-04-07
                                                                                                                    normal No
                                                                                                                                        Satel Iberia SenNe
                                                                                                                    normal No
                                                                                                                                        Telnet Login Check
 Scanner

14 auxiliary/scanner/telnet/telnet version
                                                                                                                                        Telnet Service Ban
                                                                                                                    normal No
ner betection
15 auxiliary/scanner/telnet/telnet_encrypt_overflow
ryption Key ID Overflow Detection
                                                                                                                    normal No
                                                                                                                                        Telnet Service Enc
```

Il modulo numero 14 sembra fare al caso nostro:



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



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:

```
-(kali⊕kali)-[~]
Trying 10.0.2.19 ...
Connected to 10.0.2.19.
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 04:01:05 EST 2024 from 10.0.2.5 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 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/
No mail.
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ifconfig
          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
eth0
           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:0×d020 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: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