



S7/L2

METASPLOIT - TELNET

FLAVIO SCOGNAMIGLIO



TRACCIA

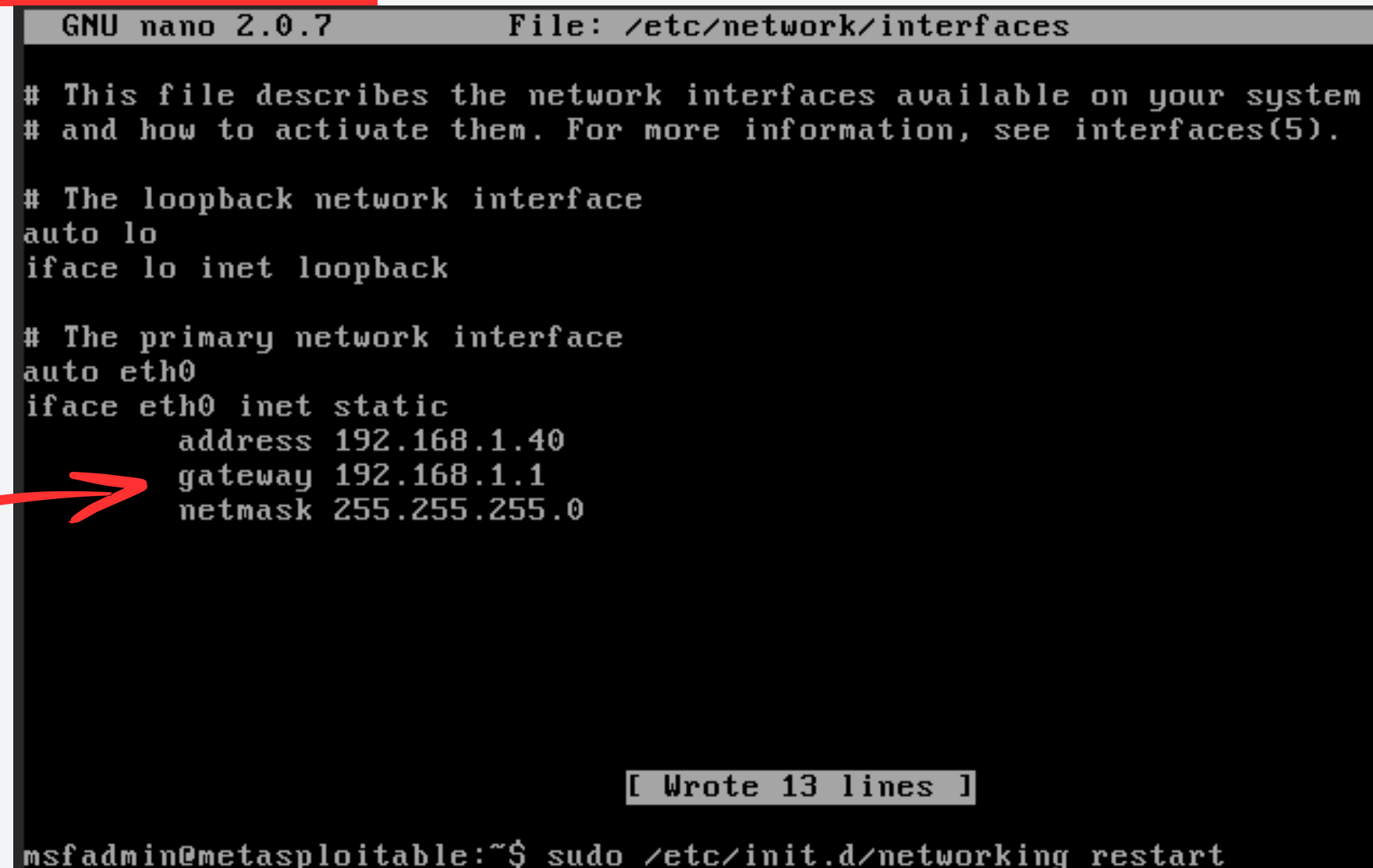
- *Traccia: Sulla base dell'esercizio visto in lezione teorica, utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable. Requisito: Seguire gli step visti in lezione teorica. Prima, configurate l'ip della vostra Kali con **192.168.1.25** e l'ip della vostra Metasploitable con **192.168.1.40***

CONFIGURAZIONE - META

Accendo le macchine (ParrotOS e Metasploitable) del mio laboratorio. Per questioni di apprendimento ed efficienza, utilizzo un hypervisor di tipo 1, **PROXMOX**. Dopodichè, come da traccia, imposto l'ip **192.168.1.25** per parrotOS, e **192.168.1.40** per Metasploitable.

```
msfadmin@metasploitable:~$ sudo nano /etc/network/interfaces
```

Su metasploitable modifico con l'editor di testo nano il file di configurazione in `/etc/network/interfaces`, dopodichè salvo e riavvio il demone che gestisce il networking.



```
GNU nano 2.0.7      File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

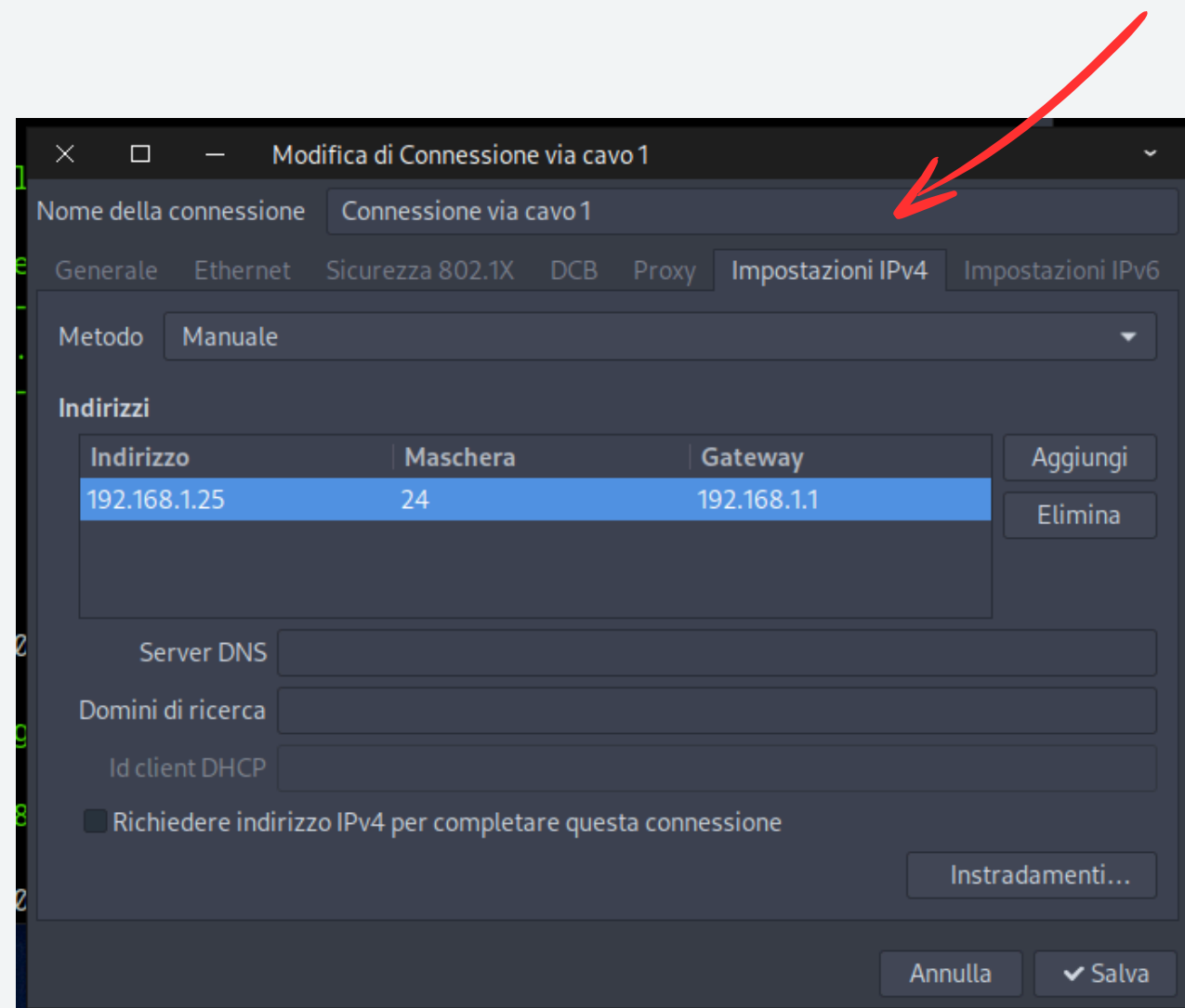
# The primary network interface
auto eth0
iface eth0 inet static
    address 192.168.1.40
    gateway 192.168.1.1
    netmask 255.255.255.0

[ Wrote 13 lines ]

msfadmin@metasploitable:~$ sudo /etc/init.d/networking restart
```

CONFIGURAZIONE - PARROT

Su parrotOS configuro l'ip **192.168.1.25**, per comodità lo faccio da GUI.



```
[flavio@parrot]~$ 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: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:58:6b:62 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 192.168.1.25/24 brd 192.168.1.255 scope global noprefixroute ens18
        valid_lft forever preferred_lft forever
    inet6 fe80::6658:95d5:ea2e:9a77/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

[flavio@parrot]~$ ping -c3 192.168.1.40
PING 192.168.1.40 (192.168.1.40) 56(84) bytes of data:
64 bytes from 192.168.1.40: icmp_seq=1 ttl=64 time=0.314 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.392 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.368 ms

--- 192.168.1.40 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2038ms
rtt min/avg/max/mdev = 0.314/0.358/0.392/0.032 ms

[flavio@parrot]~$
```

Controllo che le due macchine comunichino tra loro attraverso il comando ping.

NMAP

Nelle esercitazioni precedenti abbiamo constatato la versatilità del tool nmap, sottolineando quanto durante la fase di raccolta informazioni possa essere utile per evidenziare porte aperte e servizi esposti potenzialmente vulnerabili. Per questa specifica esercitazione, siamo interessati al servizio telnet esposto sulla porta 23:

```
[flavio@parrot]-[~]  
$nmap -sT -sV -p23 192.168.1.40  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-09 14:40 CEST  
Nmap scan report for 192.168.1.40  
Host is up (0.00072s latency).  
  
PORT      STATE SERVICE VERSION  
23/tcp    open  telnet  Linux telnetd  
Service Info: OS: 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 0.34 seconds  
[flavio@parrot]-[~]
```

Telnet è un servizio per l'amministrazione remota e la gestione dei sistemi in produzione, ed è considerato assolutamente obsoleto. Questo perché Telnet trasmette i dati, comprese le credenziali, in testo non criptato, rendendo le comunicazioni vulnerabili ad attacchi di intercettazione (sniffing) e di replay, come vedremo nelle slide successive.

TELNET - DATI IN CHIARO

Telnet è un protocollo **altamente insicuro** che serve per fornire all'utente sessioni di accesso remoto. Proprio per questo motivo è stato sostituito da altri protocolli più efficienti, come **ssh**. Quest'ultimo, a differenza di telnet, applica la crittografia al traffico tra un client e il server, inclusi i dati di autenticazione (user e password), e tutti i dati trasmessi durante la sessione. Telnet ovviamente, non prevede questo. Ma vediamo nel dettaglio con Wireshark, utilizzando il filtro evidenziato in foto, per escludere tutto tranne le connessioni tra parrotOS e metasploitable sulla porta 23.

The image displays a Telnet session in a Parrot Terminal window and the corresponding network traffic captured in Wireshark.

Parrot Terminal Output:

```
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 Jul 9 08:44:38 EDT 2024 from parrot on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC

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:~$
```

Wireshark Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
61	18.616262566	192.168.1.25	192.168.1.40	TCP	66	41938 → 23 [ACK] Seq=128 Ack=689 Win=64128 Len=
62	18.732858779	192.168.1.25	192.168.1.40	TELNET	67	Telnet Data ...
64	18.733384801	192.168.1.25	192.168.1.40	TCP	66	41938 → 23 [ACK] Seq=129 Ack=690 Win=64128 Len=
65	18.784557552	192.168.1.25	192.168.1.40	TELNET	67	Telnet Data ...
67	18.785131593	192.168.1.25	192.168.1.40	TCP	66	41938 → 23 [ACK] Seq=130 Ack=691 Win=64128 Len=
68	18.926222421	192.168.1.25	192.168.1.40	TELNET	67	Telnet Data ...
70	18.926617078	192.168.1.25	192.168.1.40	TCP	66	41938 → 23 [ACK] Seq=131 Ack=692 Win=64128 Len=
71	19.441169249	192.168.1.25	192.168.1.40	TELNET	68	Telnet Data ...
73	19.443986111	192.168.1.25	192.168.1.40	TCP	66	41938 → 23 [ACK] Seq=133 Ack=694 Win=64128 Len=
75	19.444246880	192.168.1.25	192.168.1.40	TCP	66	41938 → 23 [ACK] Seq=133 Ack=704 Win=64128 Len=
76	20.153801501	192.168.1.25	192.168.1.40	TELNET	67	Telnet Data ...
78	20.228751805	192.168.1.25	192.168.1.40	TELNET	67	Telnet Data ...
80	20.281137469	192.168.1.25	192.168.1.40	TELNET	67	Telnet Data ...
83	20.424895014	192.168.1.25	192.168.1.40	TELNET	67	Telnet Data ...
85	20.499549932	192.168.1.25	192.168.1.40	TELNET	67	Telnet Data ...
87	20.584498214	192.168.1.25	192.168.1.40	TELNET	67	Telnet Data ...
89	20.627642572	192.168.1.25	192.168.1.40	TELNET	67	Telnet Data ...
91	20.743235867	192.168.1.25	192.168.1.40	TELNET	67	Telnet Data ...
93	20.922302317	192.168.1.25	192.168.1.40	TELNET	68	Telnet Data ...
96	20.926184780	192.168.1.25	192.168.1.40	TCP	66	41938 → 23 [ACK] Seq=143 Ack=706 Win=64128 Len=
98	20.926594883	192.168.1.25	192.168.1.40	TCP	66	41938 → 23 [ACK] Seq=143 Ack=1215 Win=63744 Len=
100	20.930880859	192.168.1.25	192.168.1.40	TCP	66	41938 → 23 [ACK] Seq=143 Ack=1242 Win=64128 Len=

Wireshark Filter: `ip.src==192.168.1.25 and ip.dst==192.168.1.40 and tcp.port 23`

Wireshark Packet Details:

Frame 19: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: ProxmoxS_58:6b:62 (bc:24:11:58:6b:62), Dst: 08:00:27:00:00:00
Internet Protocol Version 4, Src: 192.168.1.25, Dst: 192.168.1.40
Transmission Control Protocol, Src Port: 41938, Dst Port: 23, Seq: 128, Ack: 689, Win: 64128, Len: 0

Effettuo un login con telnet da parrotOS a metasploitable per dimostrare il traffico in chiaro

TELNET - DATI IN CHIARO

```
..&..&.....!.."..'.....#.....#..'&.....!..".....#.....'.....P....  
.. .38400,38400.....#.parrot:0.....'..DISPLAY.parrot:0.....XTERM-256COLOR.....  
  
[ ASCII art logo ]  
  
Warning: Never expose this VM to an untrusted network!  
Contact: msfdev[at]metasploit.com  
Login with msfadmin/msfadmin to get started  
  
metasploitable login: mmssffaaddmminn  
Password: msfadmin  
Last login: Tue Jul 9 08:44:38 EDT 2024 from parrot 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:~$
```

22 pacchetti client, 19 pacchetti server, 27 turni.

Conversazione intera (1.383 bytes) Mostra dati come ASCII Flusso 0

Trova: Trova successivo

Seguendo il **flusso TCP** grazie a wireshark, possiamo notare lo username e la password inseriti durante la sessione di login. Questo a dimostrazione del fatto che telnet non è affatto un protocollo sicuro.



PROVE CON METASPLOIT

In questo caso sfrutteremo il modulo **/auxiliary/scanner/telnet/telnet_version** presente su Metasploit, per fare ulteriori esperimenti. Un modulo ausiliare in Metasploit esegue funzioni di supporto (es. scansioni), mentre un modulo normale (exploit) tenta di compromettere un sistema. In questo caso ci occuperemo di carpire informazioni dal **banner**!

Dal momento che si tratta di un modulo atto a raccogliere informazioni, non specifichiamo alcun payload. Lo imposto, guardo le impostazioni, e setto l'host **target**. Ovviamente, non trattandosi di un dispositivo Lantronix, ci interessa il numero 1.

```
Parrot Terminal
sea[msf](Jobs:0 Agents:0) >> search telnet_version

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  auxiliary/scanner/telnet/lantronix_telnet_version  normal  No    Lantronix Telnet Service Banner Detection
1  auxiliary/scanner/telnet/telnet_version           normal  No    Telnet Service Banner Detection

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_version

[msf](Jobs:0 Agents:0) >> use 1
[msf](Jobs:0 Agents:0) auxiliary(scanner/telnet/telnet_version) >>

Parrot Terminal
[msf](Jobs:0 Agents:0) auxiliary(scanner/telnet/telnet_version) >> show options

Module options (auxiliary/scanner/telnet/telnet_version):

Name      Current Setting  Required  Description
----      -
PASSWORD  no               no        The password for the specified username
RHOSTS    yes              yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-me
            tasplit.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               no        The username to authenticate as

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

[msf](Jobs:0 Agents:0) auxiliary(scanner/telnet/telnet_version) >> set RHOSTS 192.168.1.40
```


METASPLOIT - EXPLOIT

A questo punto lancio l'exploit, ed effettua una connessione Telnet raccogliendo le informazioni dal banner del servizio. In questo caso ha raccolto username e password di default del servizio. Come abbiamo già visto nella pratica di prima attraverso Wireshark, telnet è un protocollo assolutamente **insicuro**!

[illegible]

GRAZIE