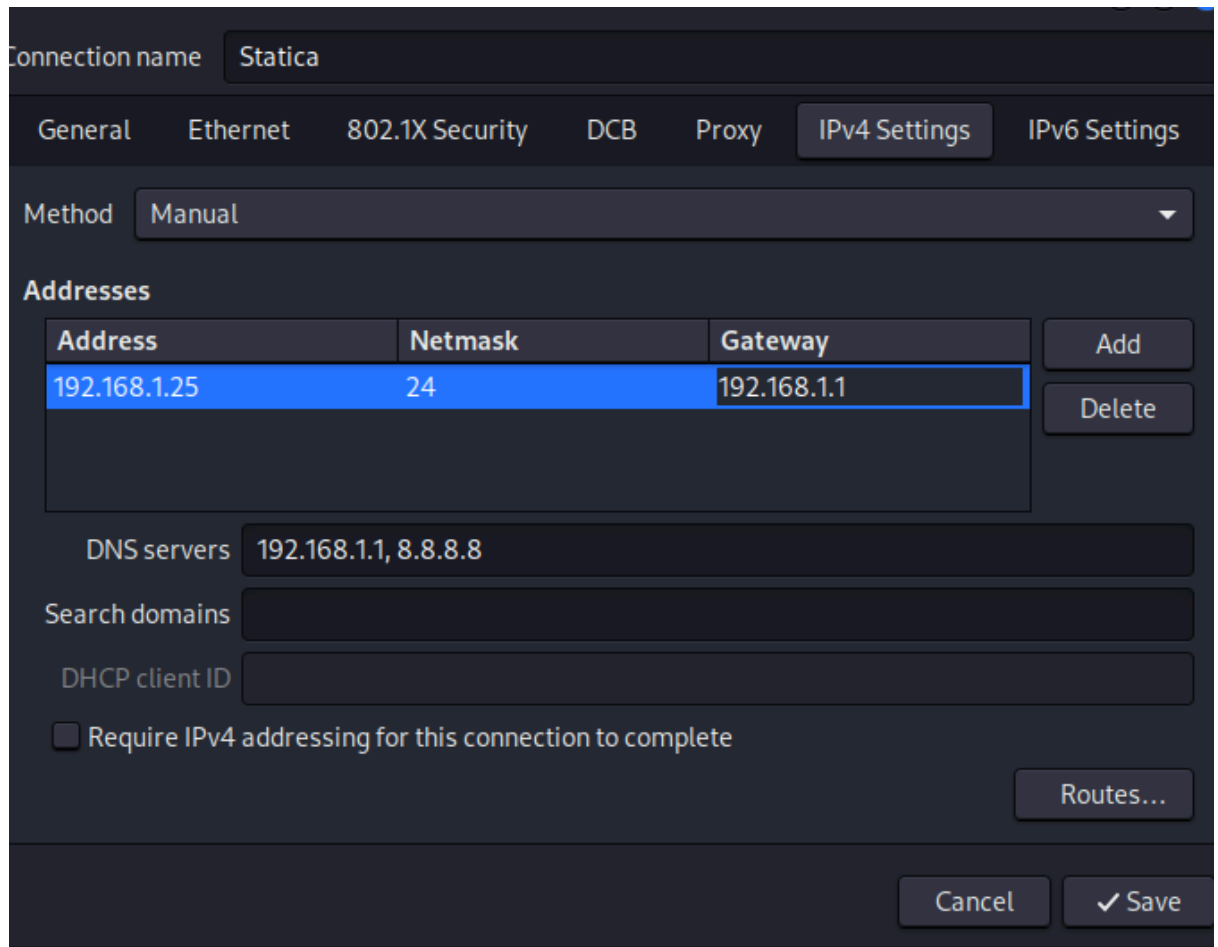


## Passo 1: Configurazione dell'indirizzo IP su Kali Linux



Nella **prima immagine** viene configurato manualmente l'indirizzo IP di Kali Linux:

- **Indirizzo IP:** 192.168.1.25
- **Netmask:** 255.255.255.0 (/24)
- **Gateway:** 192.168.1.1

-Questo assicura che Kali Linux sia sulla stessa rete di Metasploitable.

## Passo 2: Configurazione dell'indirizzo IP su Metasploitable

```
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.1.40 netmask 255.255.255.0
```

Nella **seconda immagine**, viene configurato l'indirizzo IP della macchina **Metasploitable**:

**Comando:**

```
sudo ifconfig eth0 192.168.1.40 netmask 255.255.255.0
```

-Questo imposta l'indirizzo IP della macchina Metasploitable a **192.168.1.40** e garantisce che sia raggiungibile sulla stessa rete.

### Passo 3: Verifica della Configurazione di Rete

```
(kali㉿kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.1.25 netmask 255.255.255.0 broadcast 192.168.1.255  
    inet6 fe80::b91e:b71a:ca7c:e792 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:14:ae:9f txqueuelen 1000 (Ethernet)  
    RX packets 110 bytes 18683 (18.2 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 1194 bytes 93592 (91.3 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 108 bytes 10378 (10.1 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 108 bytes 10378 (10.1 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Nella **terza immagine** viene eseguito il comando `ifconfig` su Kali Linux.

- **Risultato:** Conferma che l'interfaccia di rete **eth0** ha l'IP **192.168.1.25** con netmask **255.255.255.0** e che la configurazione è corretta.

### Passo 4: Configurazione del Gateway su Metasploitable

```
msfadmin@metasploitable:~$ sudo route add default gw 192.168.1.1
```

Nella **quarta immagine**, viene configurato il **gateway** di default su Metasploitable utilizzando il comando:

```
sudo route add default gw 192.168.1.1
```

4.
  - Questo comando assicura che la macchina possa comunicare correttamente con il gateway della rete.
  - **Passo 5: Avvio di Metasploit Framework**



```
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        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 rhost 192.168.1.40
rhost => 192.168.1.40
```

Nella **settima immagine**, vengono configurate le opzioni del modulo:

- **RHOSTS**: Impostato a **192.168.1.40** (IP della macchina Metasploitable).
- **RPORT**: Porta **23** (default per Telnet).

Il modulo è ora pronto per essere eseguito.

---

## Passo 8: Primo Tentativo di Esecuzione del Modulo

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhost 192.168.1.40
rhost => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[*] 192.168.1.40:23 - No route to host ["/usr/lib/ruby/3.1.0/socket.rb:452:in `__read_nonblock'", "/usr/lib/ruby/3.1.0/socket.rb:452:in `read_nonblock'", "/usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/rex-core-0.1.32/lib/rex/io/stream.rb:91:in `block in read'", "/usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/rex-core-0.1.32/lib/rex/io/stream.rb:336:in `synchronize_access'", "/usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/rex-core-0.1.32/lib/rex/io/stream.rb:89:in `read'", "/usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/rex-core-0.1.32/lib/rex/io/stream.rb:223:in `get_once'", "/usr/share/metasploit-framework/lib/msf/core/exploit/remote/telnet.rb:160:in `recv_telnet'", "/usr/share/metasploit-framework/lib/msf/core/exploit/remote/telnet.rb:146:in `recv'", "/usr/share/metasploit-framework/lib/msf/core/exploit/remote/telnet.rb:125:in `block in connect'", "/usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/timeout-0.4.2/lib/timeout.rb:183:in `block in timeout'", "/usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/timeout-0.4.2/lib/timeout.rb:38:in `handle_timeout'", "/usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/timeout-0.4.2/lib/timeout.rb:192:in `timeout'", "/usr/share/metasploit-framework/lib/msf/core/exploit/remote/telnet.rb:123:in `connect'", "/usr/share/metasploit-framework/modules/auxiliary/scanner/telnet/telnet_version.rb:33:in `block in run_host'", "/usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/timeout-0.4.2/lib/timeout.rb:183:in `block in timeout'", "/usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/timeout-0.4.2/lib/timeout.rb:38:in `handle_timeout'", "/usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/timeout-0.4.2/lib/timeout.rb:192:in `timeout'", "/usr/share/metasploit-framework/modules/auxiliary/scanner/telnet/telnet_version.rb:32:in `run_host'", "/usr/share/metasploit-framework/lib/msf/core/auxiliary/scanner.rb:128:in `block (2 levels) in run'", "/usr/share/metasploit-framework/lib/msf/core/thread_manager.rb:105:in `block in spawn'"]
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Nella **ottava immagine**, viene eseguito il comando **exploit**.

- **Errore: No route to host** indica che la connessione non è riuscita, probabilmente a causa di un problema di rete. Questo problema è stato risolto configurando nuovamente l'indirizzo IP e il gateway di Metasploitable nei passaggi precedenti.

---

## Passo 9: Secondo Tentativo di Esecuzione del Modulo

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhost 192.168.1.40  
rhost => 192.168.1.40  
  
msf6 auxiliary(scanner/telnet/telnet_version) > exploit
```

Nella **nona immagine**, viene rieseguito il modulo dopo aver sistemato la configurazione di rete.

- **Risultato:**
  - Il modulo identifica correttamente il servizio **Telnet** sulla porta **23**.
  - Il banner visualizzato conferma che il servizio Telnet è attivo e in ascolto sulla macchina Metasploitable.

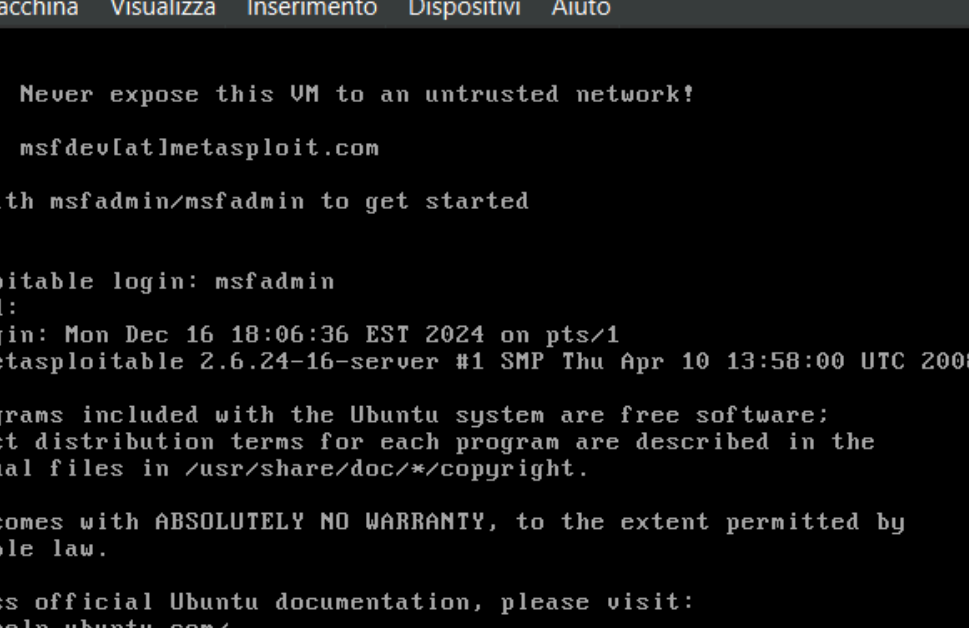
## Passo 10: Accesso Manuale al Servizio Telnet

```
msfadmin@metasploitable:~$ telnet 192.168.1.40
```

Nella **decima immagine**, viene tentata una connessione manuale al servizio Telnet:

```
telnet 192.168.1.40
```

- Viene richiesto il login, come confermato dal banner.



```
metasploit [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

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: Mon Dec 16 18:06:36 EST 2024 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:~$
```

Nella **undicesima immagine**, l'utente accede correttamente alla macchina Metasploitable inserendo:

- **Username:** msfadmin
- **Password:** msfadmin

Il prompt conferma che l'accesso è avvenuto con successo.

## Conclusione

L'esercizio ha dimostrato come configurare correttamente la rete tra due macchine virtuali, eseguire una scansione del servizio **Telnet** utilizzando Metasploit e accedere manualmente alla macchina vulnerabile. I passaggi critici sono stati la configurazione degli indirizzi IP e il corretto utilizzo del modulo `auxiliary/scanner/telnet/telnet_version` per identificare il servizio.