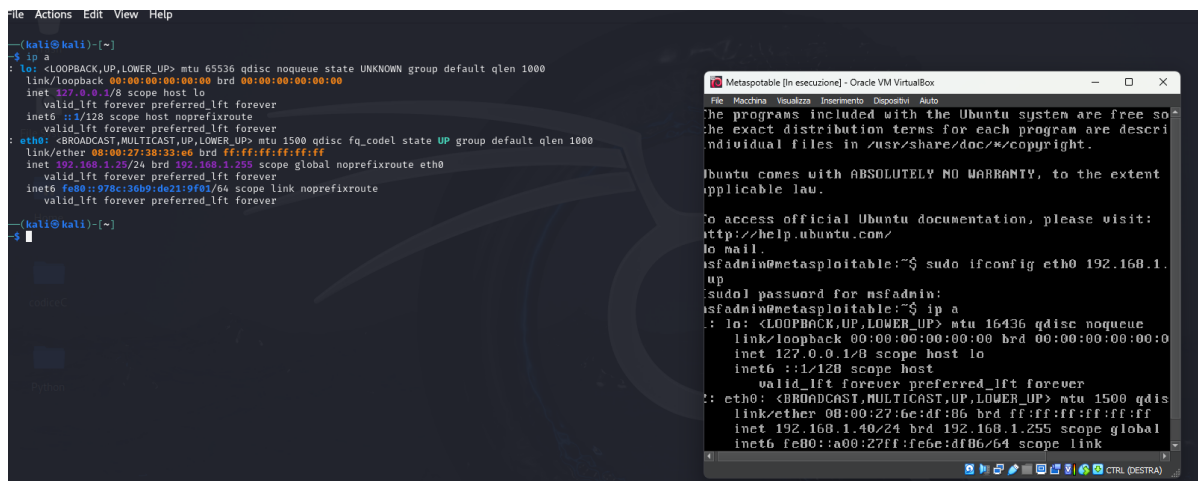


**1. Configurazione degli IP** Per garantire la corretta comunicazione tra la macchina **Kali Linux** e la macchina **Metasploitable**, è stato necessario assegnare indirizzi IP compatibili con la traccia fornitaci.

- **IP Kali Linux:** [Inserire l'IP indicato nella traccia]
- **IP Metasploitable:** [Inserire l'IP indicato nella traccia]



```
(kali@kali)~$ ip a
: 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
: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:38:33:e6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.40/24 brd 192.168.1.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::978c:36b9:de21:9f01/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali@kali)~$

Metasploitable [in esecuzione] - Oracle VM VirtualBox
The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
or mail.
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.1.255 up
msfadmin@metasploitable:~$ sudo ip a
: 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
        valid_lft forever preferred_lft forever
: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
    link/ether 08:00:27:6e:df:86 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.40/24 brd 192.168.1.255 scope global
    inet6 fe80::a00:27ff:fe6e:df86/64 scope link
```

**2. Avvio di msfconsole e utilizzo del modulo auxiliary** Dopo la configurazione degli IP, è stato avviato **msfconsole** su Kali Linux con il comando:

**msfconsole**

Una volta caricata la console, è stato utilizzato il modulo **msf6 auxiliary/scanner/telnet/telnet\_version** con il seguente comando:

**use auxiliary/scanner/telnet/telnet\_version**

Successivamente, sono stati configurati i parametri necessari per eseguire la scansione. In particolare, è stato impostato l'IP della macchina **Metasploitable** come target con il comando:

**set RHOSTS [IP della macchina Metasploitable]**

Infine, il modulo è stato avviato con il comando:

**run**

**Motivazione dell'uso del modulo:** Il modulo **telnet\_version** viene utilizzato per rilevare la versione del servizio **Telnet** in esecuzione sulla macchina target. Questa informazione è essenziale poiché consente di identificare eventuali vulnerabilità note associate a quella versione di Telnet. Inoltre, durante la scansione, il modulo potrebbe

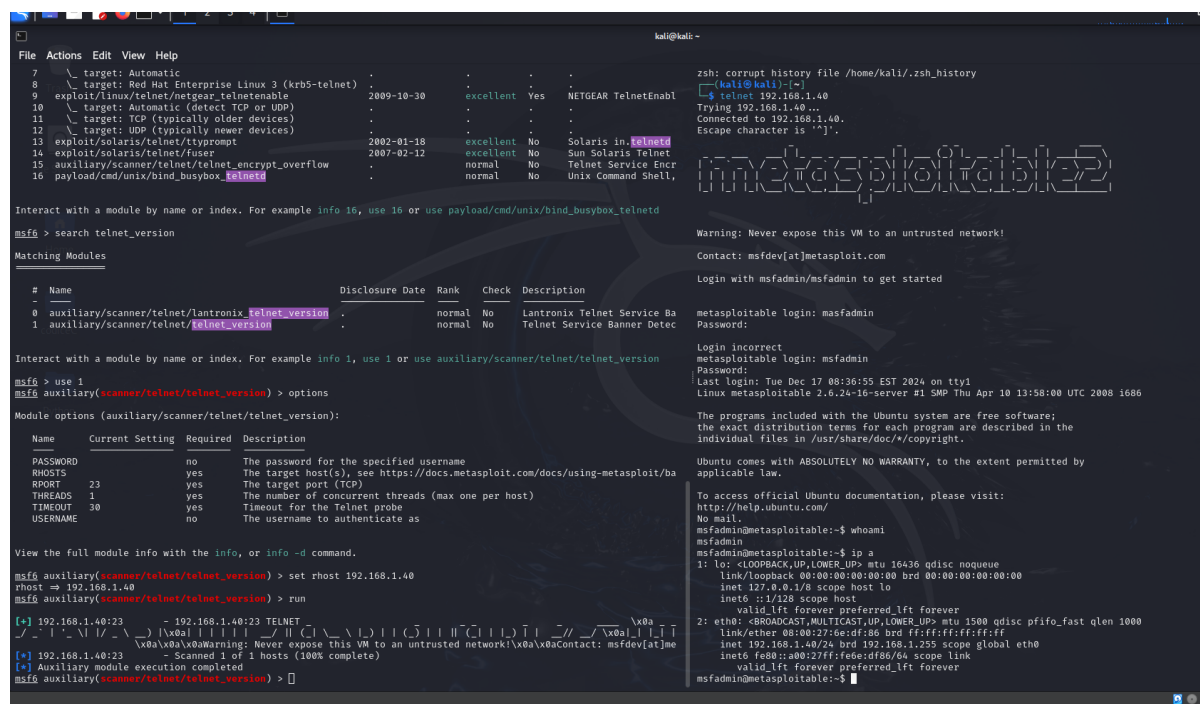
rivelare informazioni utili, come il banner del servizio o potenzialmente le credenziali di default, qualora il servizio fornisse indizi utili.

**3. Ricerca delle credenziali di accesso** Dopo aver identificato il servizio Telnet in esecuzione e la sua versione, sono state seguite le seguenti strategie per ottenere le credenziali:

- **Controllo delle credenziali predefinite:** Si è verificato se la macchina **Metasploitable** utilizza le credenziali di default comunemente associate a sistemi vulnerabili (ad esempio, **utente: msfadmin / password: msfadmin**). Questa è una pratica comune nei sistemi volutamente vulnerabili come Metasploitable.
- **Analisi del banner:** L'output fornito dal modulo **telnet\_version** può contenere informazioni relative al tipo di dispositivo, alla versione o persino a messaggi di benvenuto personalizzati, che a volte includono credenziali o suggerimenti per il login.

Una volta ottenute le credenziali, è stata stabilita una connessione Telnet dalla macchina Kali alla macchina Metasploitable con il comando:

telnet [IP della macchina Metasploitable]



```
kali@kali:~$ telnet 192.168.1.40
Trying 192.168.1.40...
Connected to 192.168.1.40.
Escape character is '^]'.

msfadmin@metasploitable:~$

msfadmin@metasploitable:~$ telnet 192.168.1.40
Trying 192.168.1.40...
Connected to 192.168.1.40.
Escape character is '^]'.

msfadmin@metasploitable:~$
```

Dopo aver inserito il nome utente e la password identificati, è stato possibile accedere alla shell della macchina Metasploitable