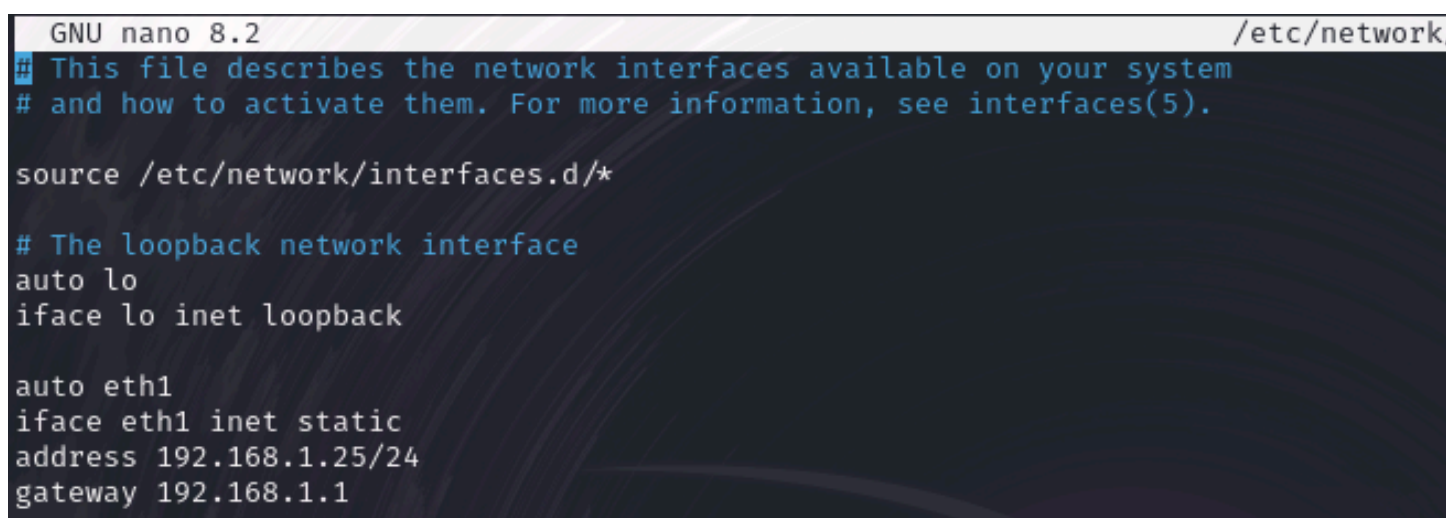


Exploit Telnet con Metasploit

Configurazione della Rete

Prima di iniziare, hai configurato gli indirizzi IP per Kali Linux e Metasploitable:

1. **Kali Linux:** Ho impostato l'indirizzo IP della macchina Kali a 192.168.1.25.



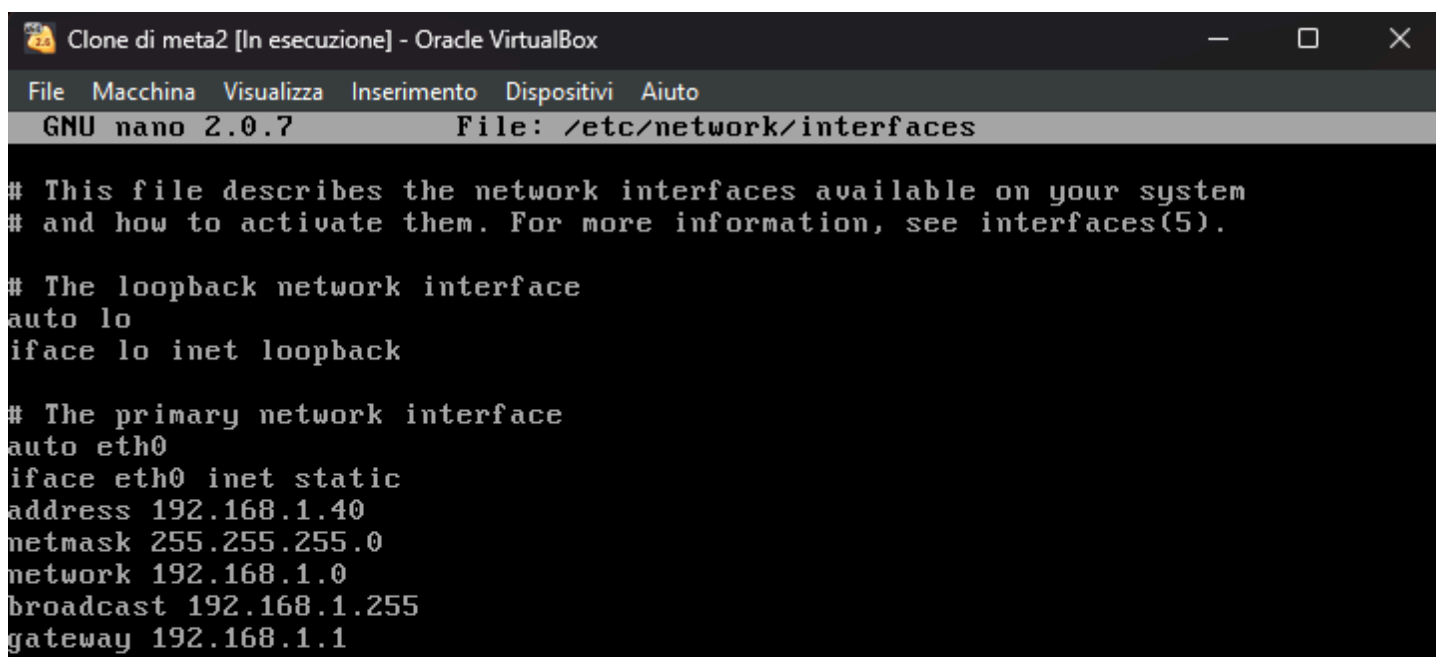
```
GNU nano 8.2 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth1
iface eth1 inet static
address 192.168.1.25/24
gateway 192.168.1.1
```

1. **Metasploitable:** Ho configurato l'IP della macchina Metasploitable a 192.168.1.40, modificando il file di configurazione della rete /etc/network/interfaces.



```
Clone di meta2 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
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).

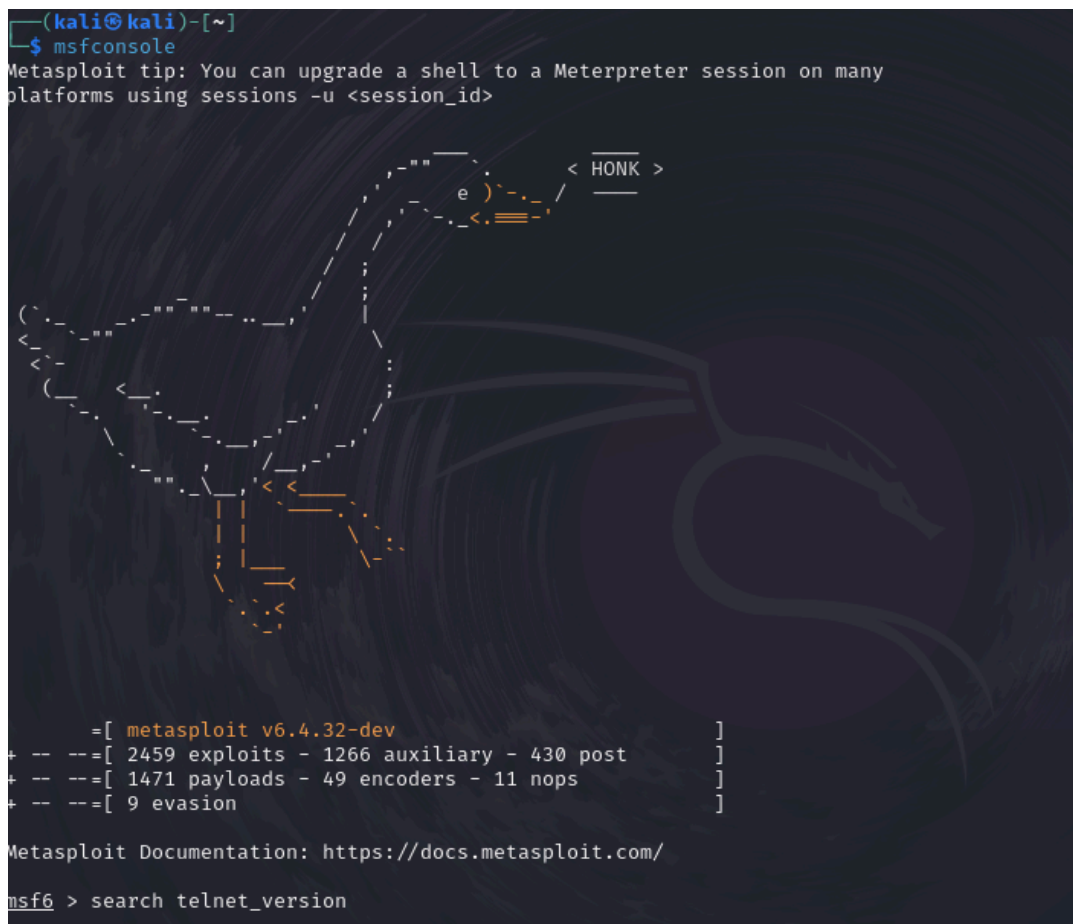
# The loopback network interface
auto lo
iface lo inet loopback

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

Per assicurarti che le due macchine fossero in grado di comunicare correttamente, ho eseguito un test di connessione tramite ping tra Kali e Metasploitable, ottenendo risposta positiva. Questo conferma che le due macchine si trovano sulla stessa rete e possono dialogare correttamente.

Scansione con Nmap

Dopo aver confermato la connessione, ho lanciato *msfconsole* in Metasploit per iniziare le tue attività.

A screenshot of a terminal window with a dark background. At the top, it shows the prompt '(kali@kali)-[~]' followed by '\$ msfconsole'. Below this, a message reads: 'Metasploit tip: You can upgrade a shell to a Meterpreter session on many platforms using sessions -u <session_id>'. In the center, there is a large, stylized ASCII art of a dragon. At the bottom, the terminal shows the output of the 'search telnet_version' command, listing various exploits, auxiliary modules, payloads, encoders, nops, and evasion techniques. The output is formatted as a table with columns for the number of items and their categories. The terminal also shows the Metasploit Documentation URL: 'https://docs.metasploit.com/'.

```
(kali@kali)-[~]  
$ msfconsole  
Metasploit tip: You can upgrade a shell to a Meterpreter session on many  
platforms using sessions -u <session_id>  
  
+ -- ==[ 2459 exploits - 1266 auxiliary - 430 post ]  
+ -- ==[ 1471 payloads - 49 encoders - 11 nops ]  
+ -- ==[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 > search telnet_version
```

Successivamente, ho effettuato una scansione di rete con Nmap per rilevare i servizi attivi sulla macchina Metasploitable. Il comando che hai utilizzato:

```
nmap -sV -T4 192.168.1.40
```

Questo comando esegue una scansione per rilevare le versioni dei servizi (-sV) con una velocità più elevata (-T4). Il risultato della scansione ha rivelato la presenza di un servizio Telnet attivo sulla macchina Metasploitable, un possibile vettore di attacco che ho deciso di analizzare più a fondo.

Ricerca del Payload in Metasploit

Una volta individuato il servizio Telnet, ho cercato un modulo appropriato per raccogliere informazioni sulla versione di Telnet. Usando il comando:

```
msf6 > 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

msf6 > use 0
```

ho trovato due moduli disponibili, uno dei quali hai selezionato per testare la connessione. Ho scelto il primo modulo visualizzato nella lista e l'ho attivato con il comando **"use 0"**.

Configurazione e Utilizzo del Modulo Telnet Version

Dopo aver selezionato il modulo, ho visualizzato le opzioni disponibili con **show options**. Dallo screenshot allegato, posso vedere che il modulo richiedeva alcune configurazioni, come **PASSWORD**, **RHOSTS**, **RPORT**, **THREADS**, **TIMEOUT** e **USERNAME**. Ho quindi impostato il campo **RHOSTS** con l'indirizzo IP della macchina Metasploitable:

```
msf6 > use 0
msf6 auxiliary(scanner/telnet/lantronix_telnet_version) > show options

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

Name      Current Setting  Required  Description
-      -
RHOSTS    9999            yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     9999            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

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

msf6 auxiliary(scanner/telnet/lantronix_telnet_version) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf6 auxiliary(scanner/telnet/lantronix_telnet_version) > exploit

[*] 192.168.1.40:9999 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Il primo modulo non ha prodotto alcun risultato rilevante. Ho quindi deciso di provare il secondo modulo trovato nella ricerca **telnet_version**, e anche qui ho impostato **RHOSTS** a **192.168.1.40** e ho lanciato nuovamente l'exploit.

```
msf6 auxiliary(scanner/telnet/lantronix_telnet_version) > use 1
msf6 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     no               yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      no               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) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
```

[illegible]

L'obiettivo di usare un modulo come `telnet_version` in Metasploit non era quello di sfruttare una vulnerabilità per ottenere accesso alla macchina, ma di raccogliere informazioni sulla versione del servizio Telnet attivo. Sapere quale versione è in esecuzione può aiutare a identificare eventuali vulnerabilità già conosciute per quella specifica versione, un passo fondamentale nella fase di ricognizione.

Questo esercizio mi ha fornito un buon esempio di ricognizione passiva e identificazione delle vulnerabilità di rete, permettendomi di vedere come informazioni dettagliate sui servizi possono essere raccolte in modo sistematico per preparare un attacco mirato o un test di penetrazione.