

**Metasploitable Limited Penetration Test**  
**Report Prepared For:** John Doe - CISO  
**Date:** 9/15/2018

Table of Contents

[2 Executive Summary 3](#_Toc524779324)

[3 Scope 3](#_Toc524779325)

[4 Methods 3](#_Toc524779326)

[5 Risk Rating 3](#_Toc524779327)

[6 Vulnerabilities 4](#_Toc524779328)

[6.1 Overview of Vulnerabilities 4](#_Toc524779329)

[6.2 Critical Vulnerabilities 5](#_Toc524779330)

[6.2.1 1 - Open Root Bind Shell 5](#_Toc524779331)

[6.2.2 2 – vsFTPd Backdoor 6](#_Toc524779332)

[6.2.3 3 - Information Disclosure in Telnet Banner 7](#_Toc524779333)

[6.2.4 4 – Weak Password on VNC Server 8](#_Toc524779334)

[6.2.5 5 – Tomcat Default Credentials 9](#_Toc524779335)

[6.2.6 6 – Postgres Default Credentials 10](#_Toc524779336)

[6.3 High-Risk Vulnerabilities 11](#_Toc524779337)

[6.3.1 7 – Anonymous Read and Write Access to Shared Directory 11](#_Toc524779338)

[6.4 Medium-Risk Vulnerabilities 12](#_Toc524779339)

[6.4.1 8 – Cleartext Protocols Are Used 12](#_Toc524779340)

# Executive Summary

In September 2018, GameOfPWNZ 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.

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

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

# Scope

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

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

# Methods

GameOfPWNZ 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>

# Risk Rating

GameOfPWNZ 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**xploitability – 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 |

# 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. | **Critical-Risk** |
| 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. | **Critical-Risk** |
| 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. | **Critical-Risk** |
| 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. | **Critical-Risk** |
| 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. | **Critical-Risk** |
| 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. | **Critical-Risk** |
| 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. | **High-Risk** |
| 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. | **Moderate-Risk** |

## Critical Vulnerabilities

### Open Root Bind Shell

#### Description

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





#### 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

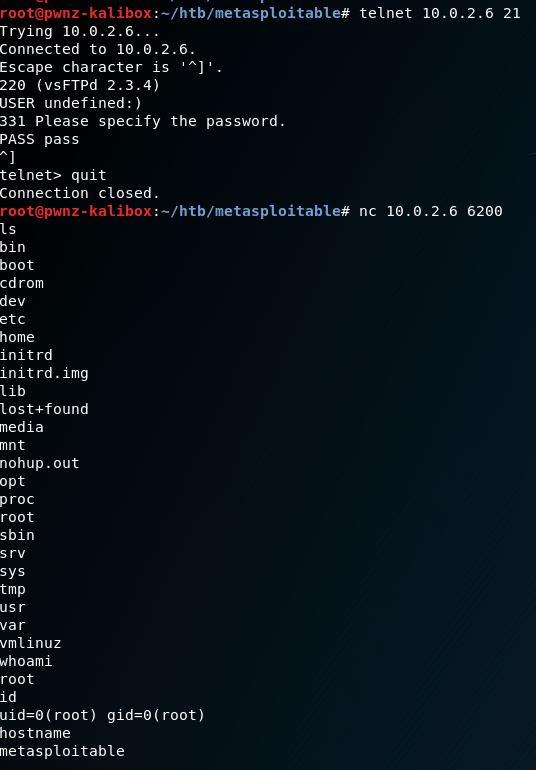
|  |  |
| --- | --- |
| Remediation Description | Level of Effort |
| Remove bind shell. | Easy |
| Enact Incident Response Plan if this is not authorized or expected behavior. | Moderate-High |

### vsFTPd Backdoor

#### Description

GameOfPWNZ 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.

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



#### 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 |

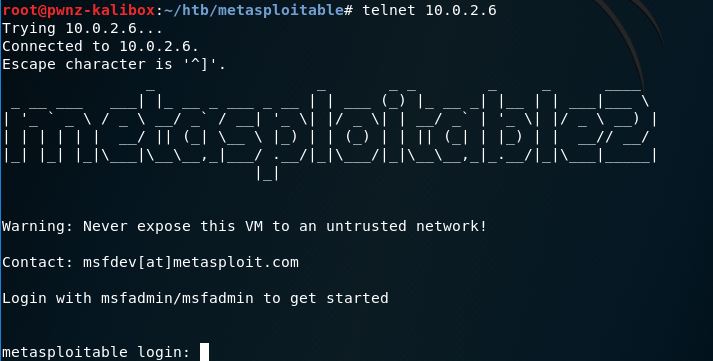
#### Remediation

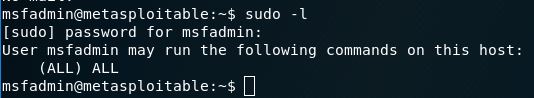
|  |  |
| --- | --- |
| Remediation Description | Level of Effort |
| Update and upgrade vsFTPd version. | Easy |

### Information Disclosure in Telnet Banner

#### Description

GameOfPWNZ 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.





#### 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 |

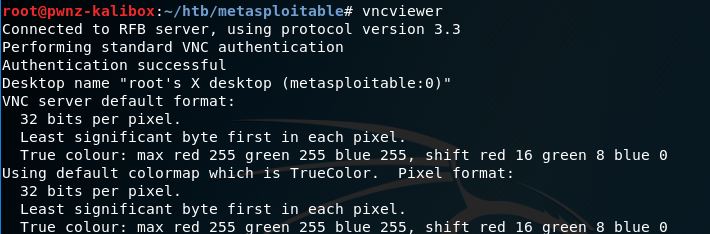
#### Remediation

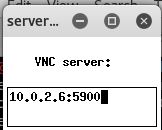
|  |  |
| --- | --- |
| Remediation Description | Level of Effort |
| Remove credentials from the Telnet banner. | Easy |
| Change password for msfadmin user. | Easy - Moderate |

### Weak Password on VNC Server

#### Description

GameOfPWNZ 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. GameOfPWNZ connected to the server with the password and was able to access a root shell.





#### 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 |

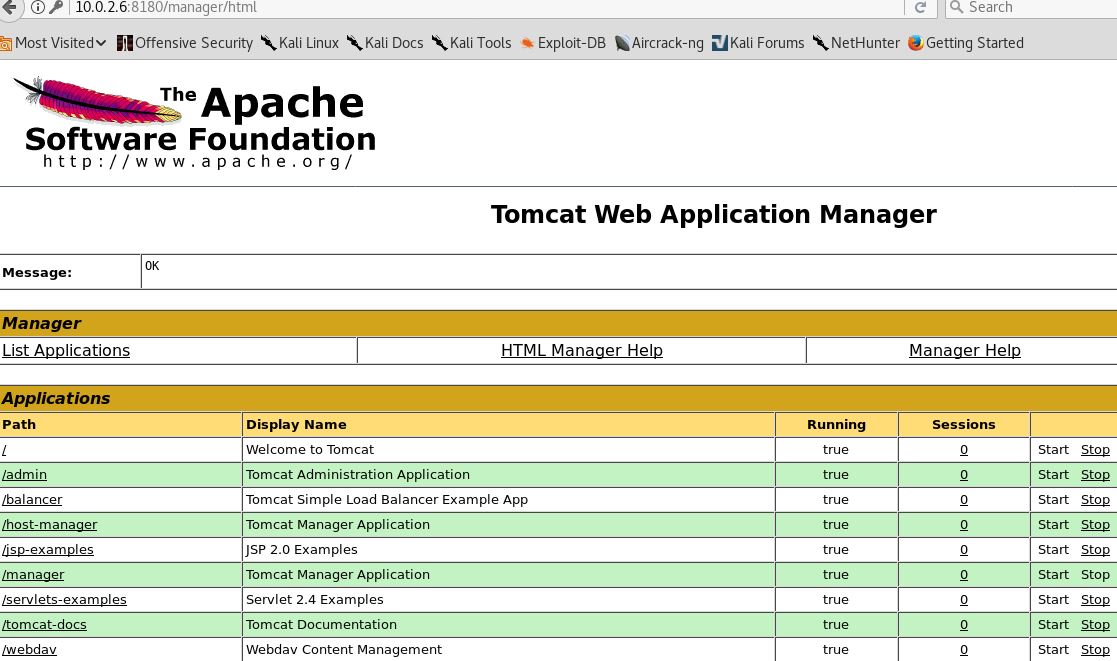
#### Remediation

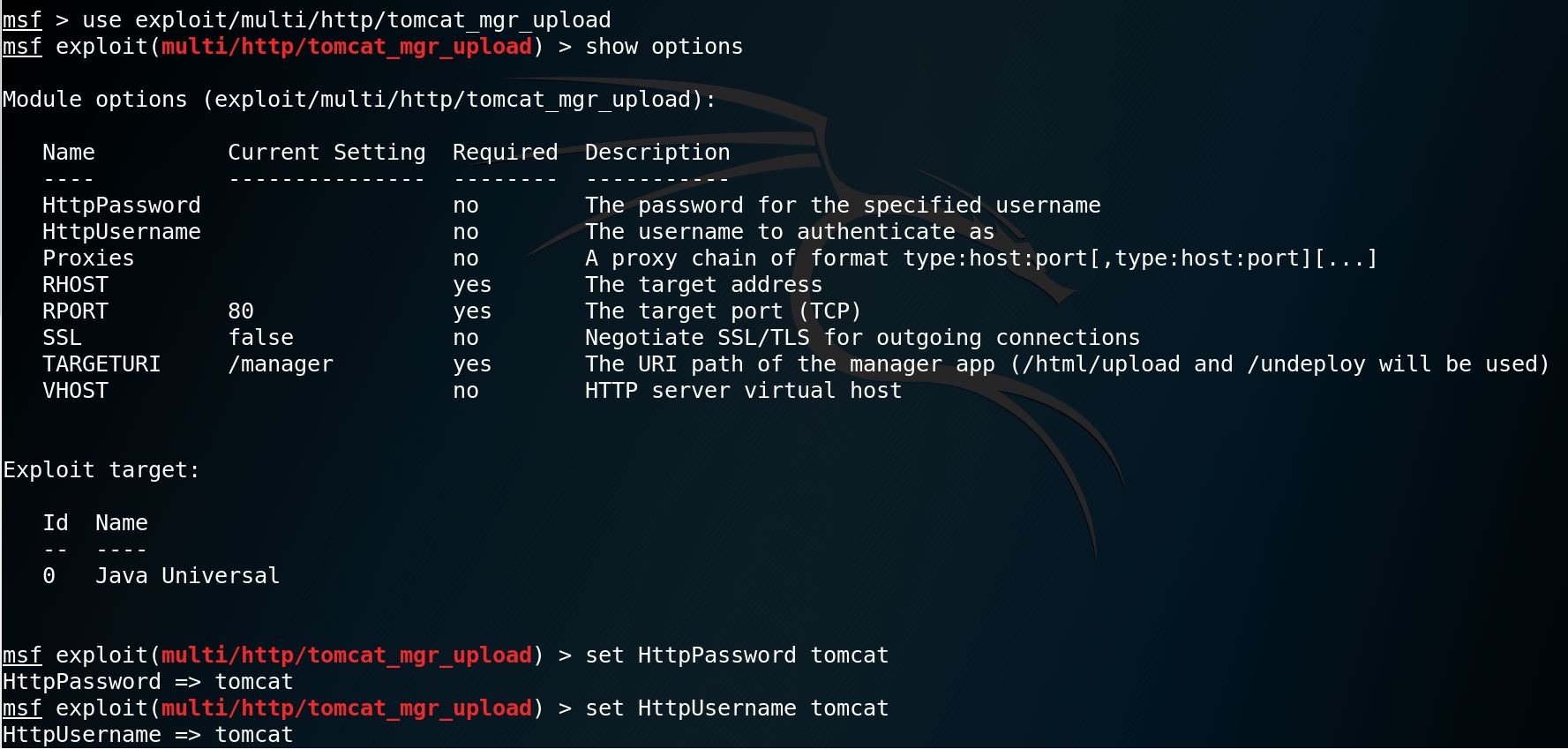
|  |  |
| --- | --- |
| Remediation Description | Level of Effort |
| Change password for VNC server. | Easy |

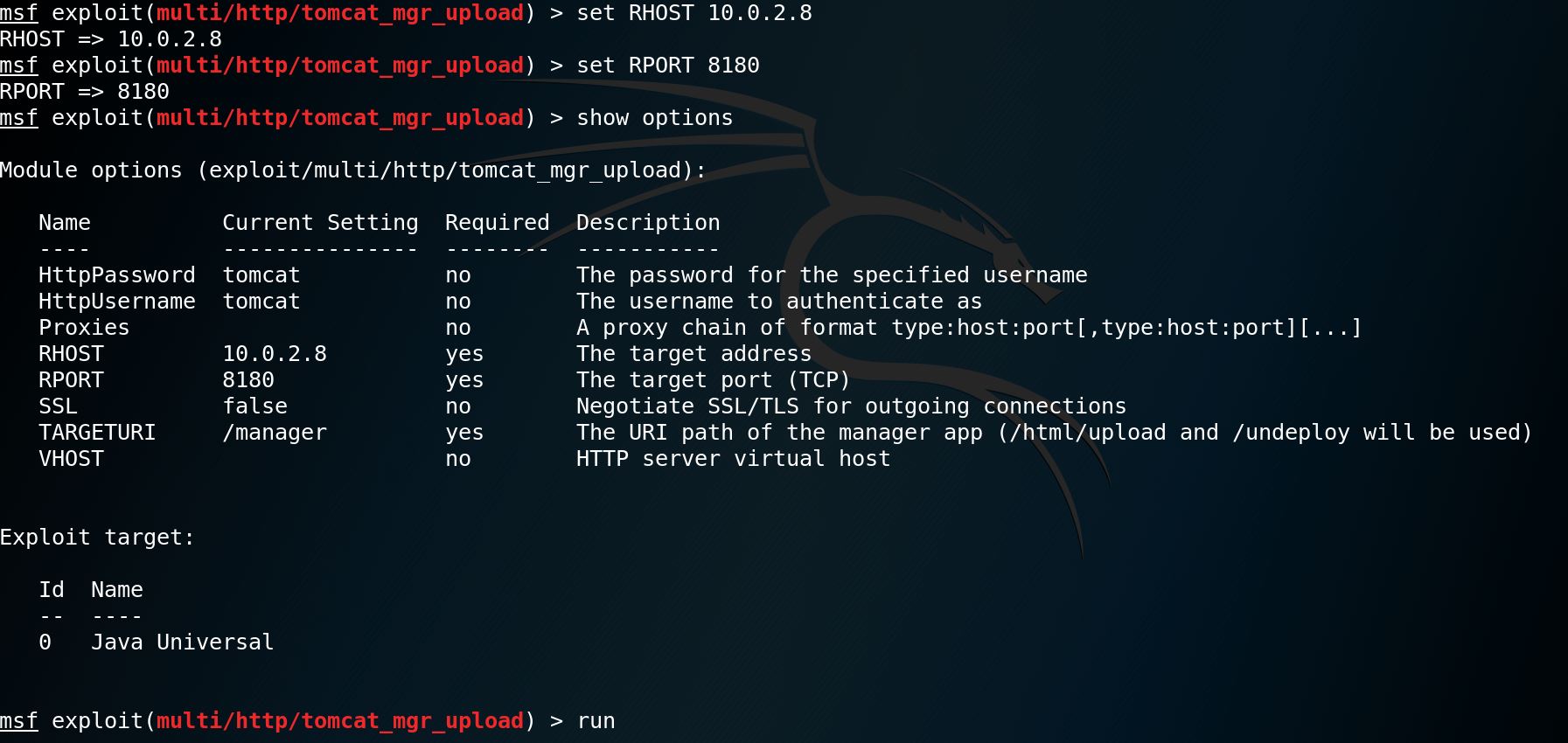
### Tomcat Default Credentials

#### Description

GameOfPWNZ identified that the Tomcat service running on port 8180 has default credentials for the Tomcat Web Application Manager. GameOfPWNZ 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.











#### 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

GameOfPWNZ identified that the postgres service was running on the Metasploitable host. The postgres user is using default credentials. GameOfPWNZ 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

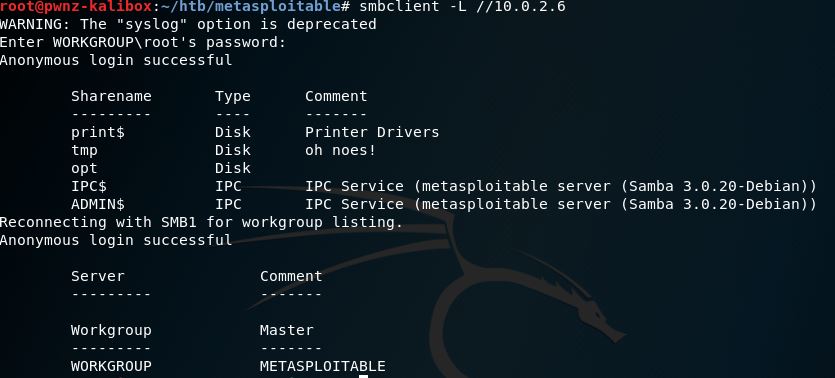
|  |  |
| --- | --- |
| Remediation Description | Level of Effort |
| Change password for postgres. | Easy-Moderate |

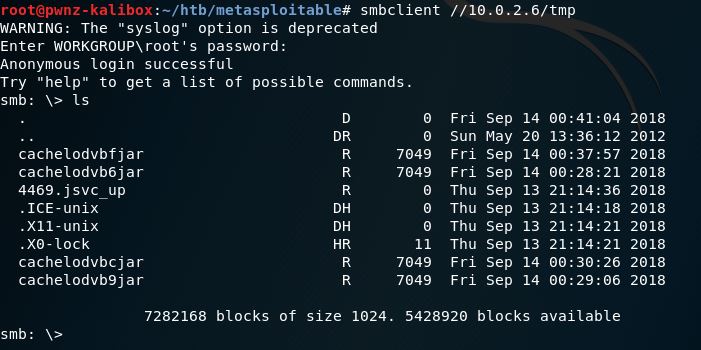
## High-Risk Vulnerabilities

### Anonymous Read and Write Access to Shared Directory

#### Description

GameOfPWNZ 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.





#### 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 Are Used

#### Description

GameOfPWNZ 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 |