

Rungta College of Engineering and Technology

Department of B.Tech CSE (Cybersecurity)

Minor-2 Project Report

Metasploitable 2 & Mutillidae II Lab

Submitted By:

Vaishnavi Verma

ERP No: 6605671

3rd Semester (2025–26)

Subject: Minor-2 Project

Guided By: Prasant Kamkar

Abstract

This project focuses on building a controlled vulnerable lab environment using Metasploitable 2 and the Mutillidae II web application. The objective is to gain hands-on experience with Linux system administration, virtualization safety mechanisms, and troubleshooting web application configuration issues.

1. Introduction

This project demonstrates the setup and configuration of an intentionally vulnerable virtual lab using Metasploitable 2 and the Mutillidae II web application. The objective is to understand vulnerable environments, perform basic Linux administrative tasks, and troubleshoot common configuration errors.

2. Environment Setup

Metasploitable 2 is an Ubuntu-based virtual machine designed for security testing and learning. The VM was imported into a virtualization

platform and accessed using default credentials (username: msfadmin, password: msfadmin)

```
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Mon Jan  5 23:44:41 EST 2026 on ttym1
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/
No mail.
msfadmin@metasploitable:~$
```

3. User Management

A new Linux user account was created using my own name to demonstrate system administration skills. The adduser command was used, followed by verification through the /etc/passwd file.

Commands Used:

```
sudo adduser vaishnavi
cat /etc/passwd | grep vaishnavi
```

```

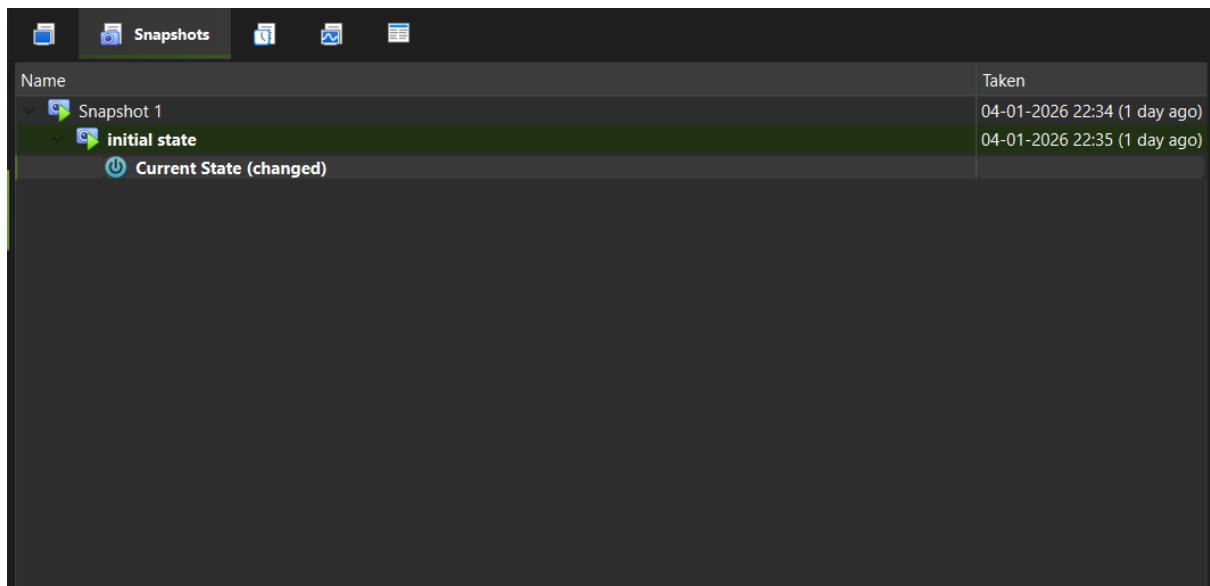
...done.
* Reloading Postfix configuration...
...done.

msfadmin@metasploitable:~$ sudo adduser vaishnavi
[sudo] password for msfadmin:
Adding user 'vaishnavi' ...
Adding new group 'vaishnavi' (1003) ...
Adding new user 'vaishnavi' (1003) with group 'vaishnavi' ...
Creating home directory '/home/vaishnavi' ...
Copying files from '/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for vaishnavi
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [y/N] y
msfadmin@metasploitable:~$ cat /etc/passwd | grep vaishnavi
vaishnavi:x:1003:1003:,:/home/vaishnavi:/bin/bash
msfadmin@metasploitable:~$ S_

```

4. Virtual Machine Snapshot

A snapshot was taken after user creation to preserve a safe system state. Snapshots allow easy rollback during testing and troubleshooting.



5. Mutilidae II Database Fix

Initially, Mutillidae II displayed database-related errors due to missing tables. The issue was resolved by using the Setup/Reset Database option within the application, which initialized the MySQL database successfully.

-IP address issued

```
DHCPACK of 10.0.6.72 from 10.0.0.1
bound to 10.0.6.72 -- renewal in 249722 seconds. [ OK ]
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:91:53:93
          inet addr:10.0.6.72 Bcast:10.0.63.255 Mask:255.255.192.0
          inet6 addr: fd8c:d698:b7ea:40cd:a00:27ff:fe91:5393/64 Scope:Global
            inet6 addr: fe80::a00:27ff:fe91:5393/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:7031 errors:0 dropped:0 overruns:0 frame:0
              TX packets:198 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:836003 (816.4 KB) TX bytes:30911 (30.1 KB)
              Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING MTU:16436 Metric:1
            RX packets:143 errors:0 dropped:0 overruns:0 frame:0
            TX packets:143 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:44197 (43.1 KB) TX bytes:44197 (43.1 KB)

msfadmin@metasploitable:~$ _
```

-Mutillidae II working.

The screenshot shows the Mutillidae: Born to be Hacked application running in a browser. The title bar reads "Mutillidae: Born to be Hacked". Below it, a navigation bar includes "Version: 2.1.19", "Security Level: 0 (Hosed)", "Hints: Disabled (0 - I try harder)", and "Not Logged In". The main menu on the left has sections like "Core Controls", "OWASP Top 10", "Others", "Documentation", and "Resources". The "Resources" section is currently selected. A sidebar on the left contains links for "Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Nmap, and these Mozilla Add-ons", "@webpwnized", and "Mutillidae Channel". The central content area displays a banner for "Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10". Below the banner, there's a "Latest Version / Installation" section with a bulleted list of links: "Latest Version", "Installation Instructions", "Usage Instructions", "Get rid of those pesky PHP errors", "Change Log", and "Notes". A note below says "Samurai WTF and Backtrack contains all the tools needed or you may build your own collection". It features logos for "back|track", "Samurai Web Testing Framework", "BUILT ON eclipses", "Toad", and "HACKERS FOR CHARITY". At the bottom, a footer notes "Developed by Adrian "irongeek" Crenshaw and Jeremy Dunn".

-Mutillidae II database error.

Error: Failure is always an option and this situation proves it	
Line	49
Code	0
File	/var/www/mutillidae/process-login-attempt.php
Message	Error executing query: Table 'metasploit.accounts' doesn't exist
Trace	#0 /var/www/mutillidae/index.php(96): include() #1 {main}
Diagnostic Information	SELECT * FROM accounts WHERE username='nht1' AND password='jhuek'

Did you [setup/reset the DB?](#)

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in /var/www/mutillidae/index.php on line 148

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in /var/www/mutillidae/index.php on line 254

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in /var/www/mutillidae/index.php on line 255

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in /var/www/mutillidae/index.php on line 256

 **Mutillidae: Born to be Hacked**

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Home Login/Register Toggle Hints Toggle Security Reset DB View Log View Captured Data

Login

Back

Please sign-in

Name

Password

Don't have an account? [Please register here](#).

Core Controls

- OWASP Top 10
- Others
- Documentation
- Resources



-Mutillidae II database fixed.

```
<?php
/* NOTE: On Samurai, the $dbpass password is "samurai" rather than blank */
$dbhost = 'localhost';
$dbuser = 'root';
$dbpass = '';
$dbname = 'owasp10';
?>

[ Wrote 8 lines ]

msfadmin@metasploitable:/var/www/mutillidae$ 
msfadmin@metasploitable:/var/www/mutillidae$ _
```

Mutillidae: Born to be Hacked

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Home Login/Register Toggle Hints Toggle Security Reset DB View Log View Captured Data

Login

Back

Authentication Error: Bad user name or password

Please sign-in

Name
Password

Login

Dont have an account? [Please register here](#)

Site
hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons

@webpwnized

Mutillidae Channel

Developed by Adrian "irongeek" Crenshaw and Jeremy Druin

Mutillidae: Born to be Hacked

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Home Login/Register Toggle Hints Toggle Security Reset DB View Log View Captured Data

View your details

Back

Please enter username and password to view account details

Name
Password

View Account Details

Dont have an account? [Please register here](#)

Results for . 1 records found.

Username=vaishnavi
Password=vaishnavi
Signature=

Site
hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons

@webpwnized

Mutillidae Channel

Developed by Adrian "irongeek" Crenshaw

6. Conclusion

This project successfully demonstrated the setup of a vulnerable lab using Metasploitable2 and the troubleshooting of a real-world configuration issue in Mutillidae II. It enhanced practical understanding of Linux administration, virtualization safety, and web application deployment issues, which are essential skills in cybersecurity.

Appendix: Linux Commands Used

- ifconfig
- sudo adduser vaishnavi
- cat /etc/passwd | grep vaishnavi
- service mysql start
- Accessing [http://\[IP\]/mutillidae/](http://[IP]/mutillidae/)