

# **Minor 2 Project Report**

**Title:** Metasploitable Setup and Mutillidae II Configuration

**Name:** Vikrant

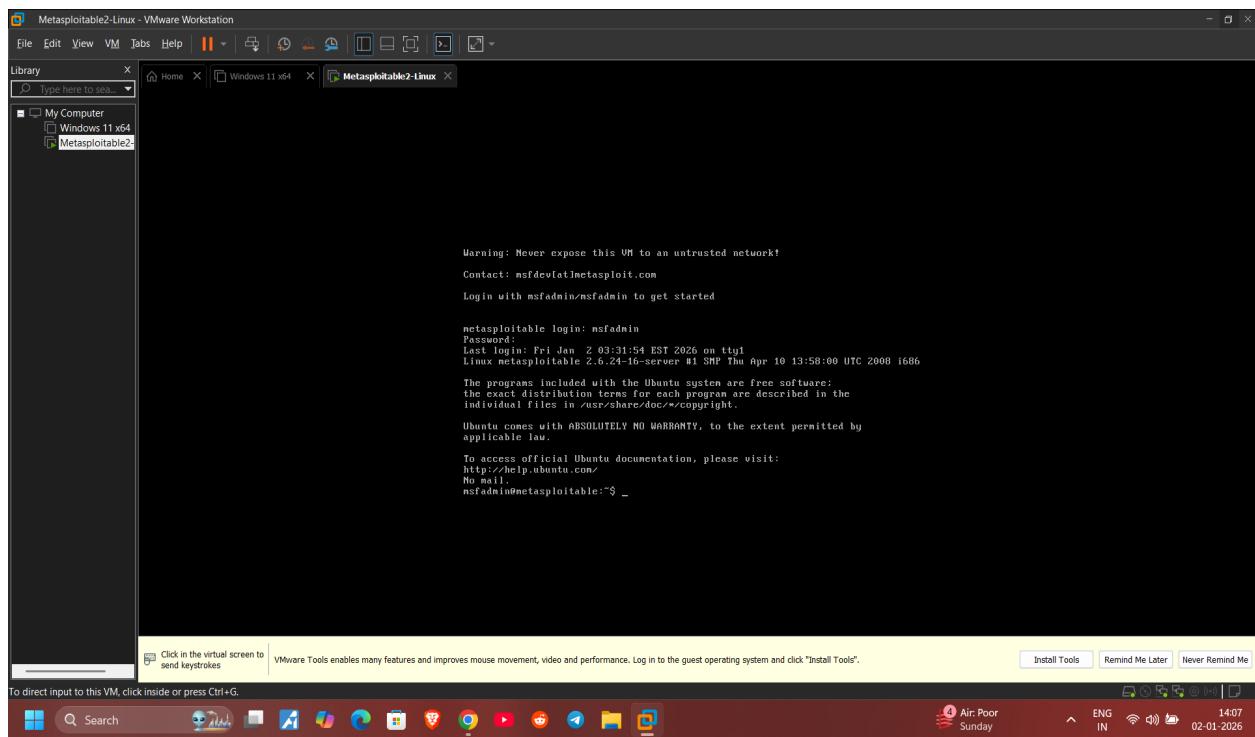
**Course:** B.Tech

## **1. Introduction**

Metasploitable is an intentionally vulnerable Linux virtual machine used for security testing and learning. In this project, Metasploitable was configured using VMware Workstation Player. A new user was created, a snapshot was taken, and the Mutillidae II web application database error was fixed.

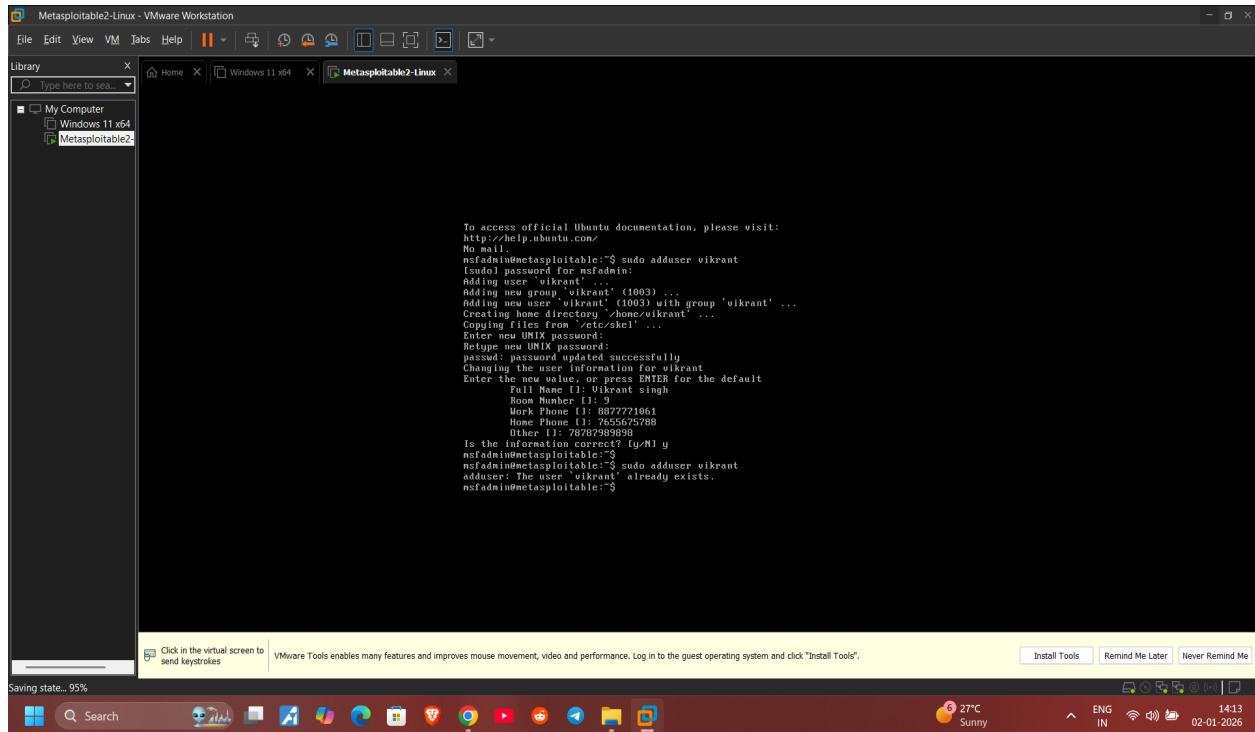
## 2. Metasploitable Running

The Metasploitable virtual machine was successfully powered on and logged in using default credentials.



### 3. User Creation

A new user named 'vikrant' was created inside Metasploitable using the following command:  
sudo adduser vikrant



```
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
nsfadmin@metasploitable:~$ sudo adduser vikrant  
(sudo) password for nsfadmin:  
Added user 'vikrant'.  
Adding new group 'vikrant' (1003) ...  
Adding new user 'vikrant' (1003) with group 'vikrant' ...  
Creating home directory '/home/vikrant' ...  
Copying files from '/etc/skel' ...  
Enter new UNIX password:  
Retype new UNIX password:  
password: password updated successfully  
Changing the user information for vikrant  
Enter the user's full name [Full Name]: Vikrant Singh  
Room Number [Room Number]: 9  
Work Phone [Work Phone]: 8077771061  
Mobile Phone [Mobile Phone]: 9876543210  
Other [Other]: 7828298989  
Is the information correct? [I/y]I y  
nsfadmin@metasploitable:~$ nsfadmin@metasploitable:~$ sudo adduser vikrant  
adduser: The user 'vikrant' already exists.  
nsfadmin@metasploitable:~$
```

VMware Tools status: Click in the virtual screen to send keystrokes. VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".

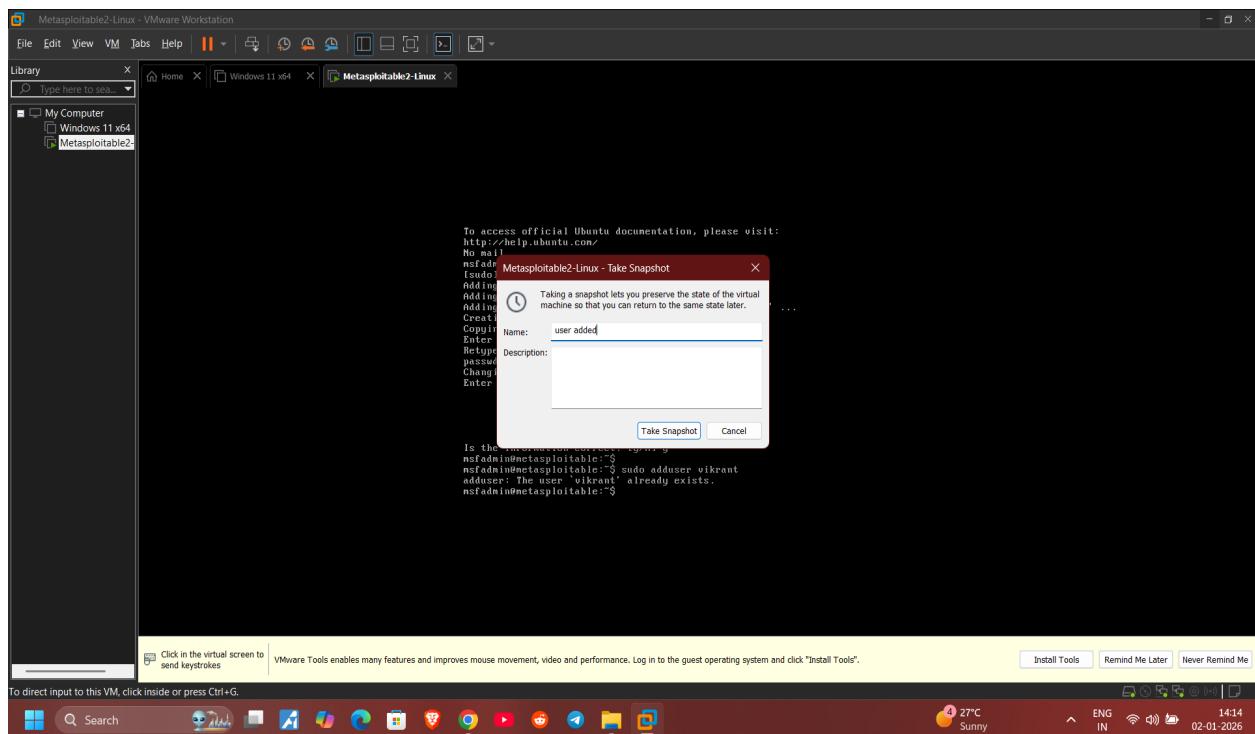
Install Tools Remind Me Later Never Remind Me

Saving state... 95%

Windows Search Start button Taskbar icons Weather (6 27°C Sunny) Language (ENG IN) Date (02-01-2026)

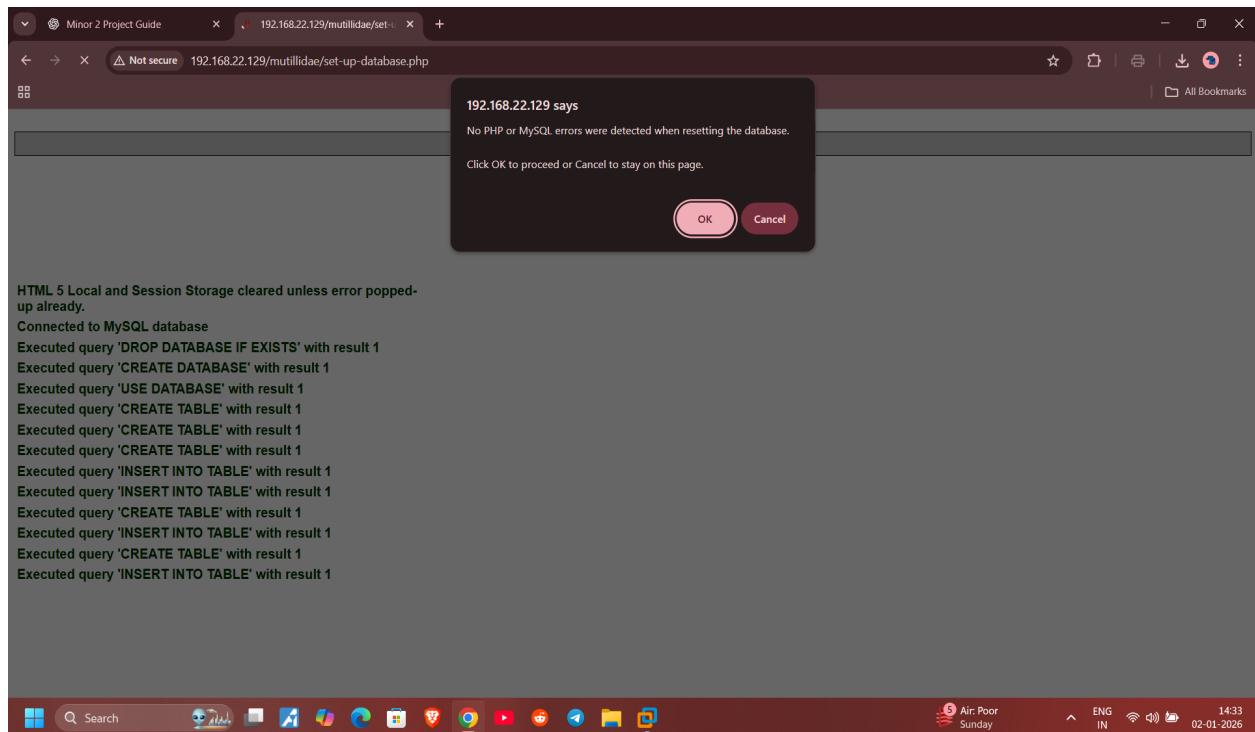
## 4. Snapshot Taken

After creating the user, a snapshot was taken to preserve the system state.



## 5. Mutillidae II Database Error

When Mutillidae II was accessed initially, a database error was displayed.



## 6. Mutillidae II Fixed

The database error was fixed by resetting the database using the setup page. After resetting, Mutillidae II worked successfully without errors.

A screenshot of a web browser window displaying the Mutillidae: Born to be Hacked website. The URL in the address bar is 192.168.22.129/mutillidae/. The page title is "Mutillidae: Born to be Hacked". The top navigation bar includes links for 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, and View Captured Data. On the left, there is a sidebar with a navigation menu: Core Controls, OWASP Top 10, Others, Documentation, and Resources. A logo for "Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons" is shown. Below the sidebar, there is a section titled "Latest Version / Installation" with a bulleted list: Latest Version, Installation Instructions, Usage Instructions, Get rid of those pesky PHP errors, Change Log, and Notes. A callout box highlights "Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10". The main content area features logos for back|track, Samurai Web Testing Framework, BUILT ON eclipse, Toad, and MySQL. A banner for "HACKERS FOR CHARITY" is also present. The bottom of the screen shows a Windows taskbar with various icons and system status information.

## **7. Conclusion**

The Metasploitable virtual machine was successfully configured. User creation, snapshot capture, and Mutillidae II database configuration were completed successfully.