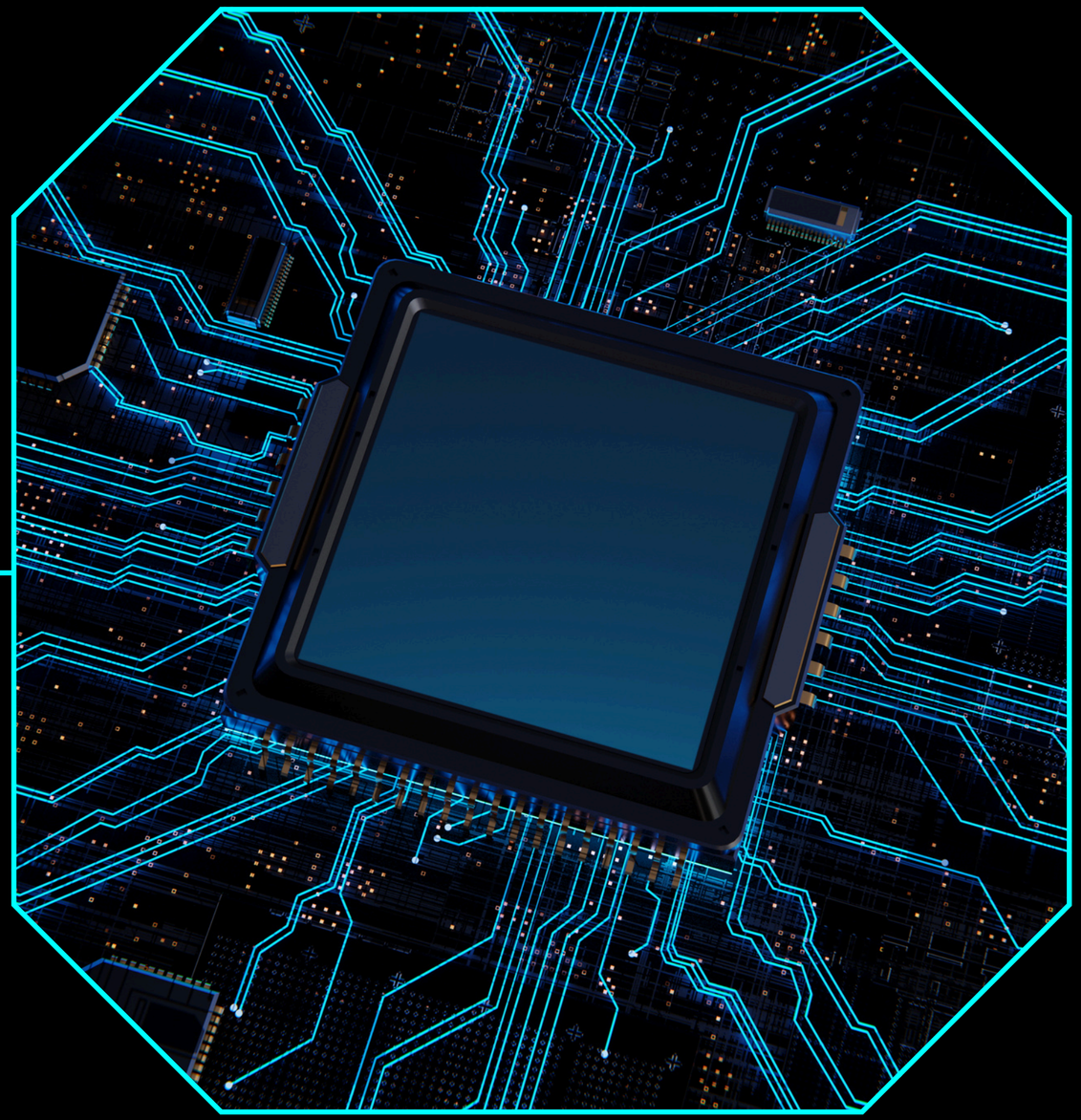
CYBER SECURITY

PROJECT

METASPLOITABLE & MUTILLIDAE SETUP

By~ PALLAVI KUMARI



Introduction

Metasploitable2 is an intentionally vulnerable Linux-based virtual machine used for learning and practicing cyber security concepts. In this Minor–2 project, Metasploitable2 is installed using VMware Workstation. A new user is created inside the system, a snapshot is taken for verification, and the Mutillidae II vulnerable web application is successfully configured and executed.

System Setup Steps

VMware Workstation Player was installed on the system.
Metasploitable2 ZIP file was downloaded and extracted.
The .vmx file was opened using the Open a Virtual Machine option in VMware.
The virtual machine was powered on successfully.
Screenshot: Metasploitable2 running in VMware.

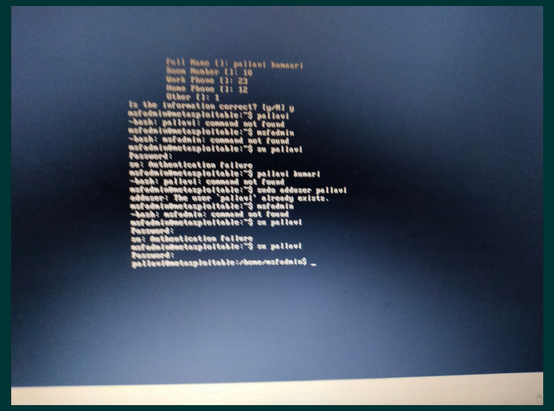
Login into Metasploitable2
Default credentials were used to log in:
Username: msfadmin
Password: msfadmin
After successful login, the terminal prompt appeared as:
msfadmin@metasploitable:~$
Screenshot: Successful login screen.

User Creation in Metasploitable2

A new user was created using the following command:
Copy code

sudo adduser pallavi
After entering the password and required details, the user was created successfully.
To verify the user, the following command was used:
Copy code

su pallavi
Screenshot: Output showing successful user creation.



Snapshot Creation

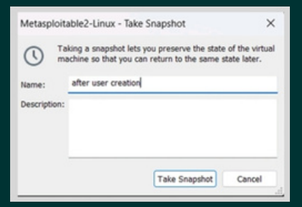
After creating the new user, a snapshot was taken to save the system state.

Steps:

Go to VM → Snapshot → Take Snapshot

Snapshot name: After User Creation

Screenshot: Snapshot window.



Mutillidae II Configuration
The Firefox browser was opened using:
Copy code

firefox &
Then the following URL was accessed:
Copy code

http://localhost/mutillidae
If a database error occurred, it was fixed by opening:
Copy code

http://localhost/mutillidae/setup.php
The database was reset successfully and Mutillidae II started working properly.

Result and Observation

Metasploitable2 was installed successfully.

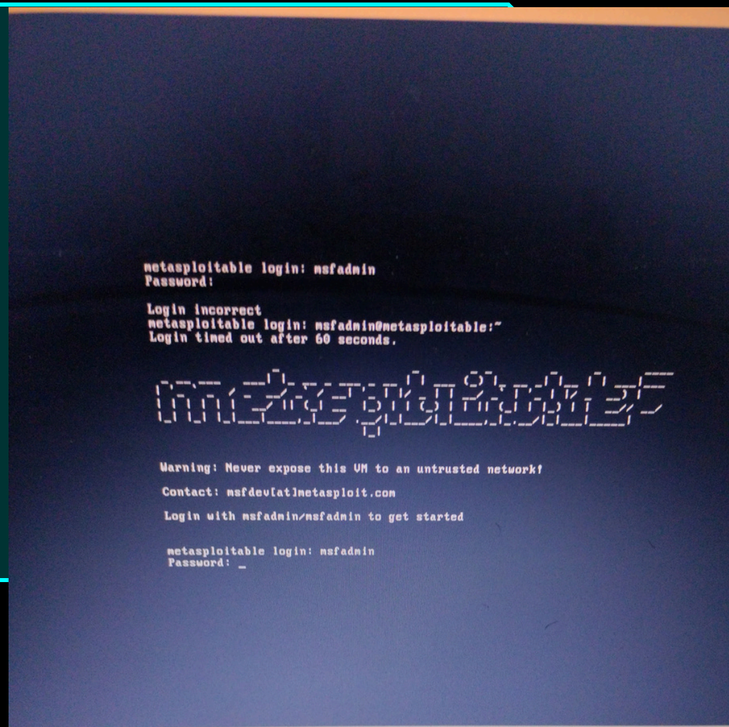
New user was created and verified.

Snapshot was taken successfully.

Mutillidae II web application was running without errors.

Conclusion

This project provided hands-on experience in setting up a vulnerable system and configuring a vulnerable web application. Metasploitable2 and Mutillidae II are very useful for learning and practicing cyber security concepts.



THANKYOU