

Minor Project 2 Report

Title: Setup and Verification of Metasploitable2 and Mutillidae II Environment

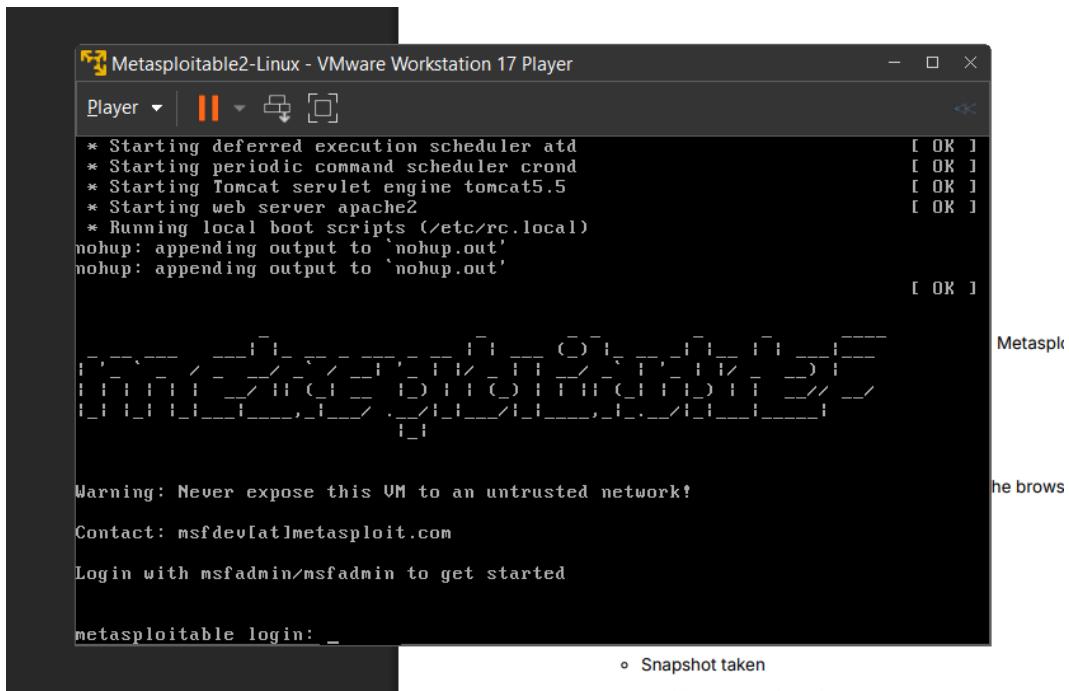
By Suryansh Sharma

Aim: To install and configure Metasploitable2, create a user, verify system state, and ensure Mutillidae II runs without errors.

Tools Used:

- VMware Workstation 17 Player
- Metasploitable2 Linux
- Windows 10
- Web Browser (Brave/Chrome)

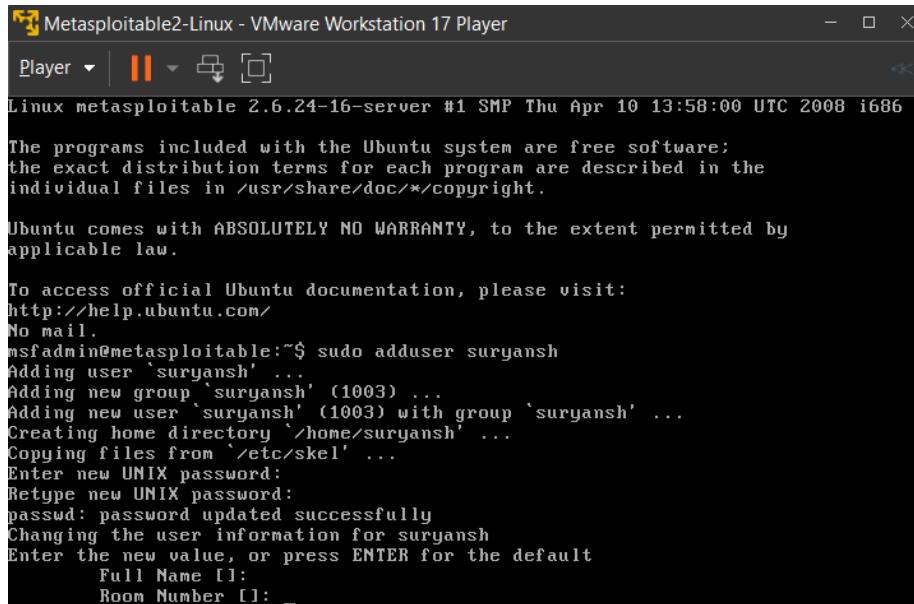
Metasploitable Setup: Metasploitable2 virtual machine was imported and executed using VMware Workstation Player. The system booted successfully to the login screen.



User Creation:

A new user was created inside Metasploitable using administrative privileges to verify user management capability.

Command used: sudo adduser suryansh



```
Metasploitable2-Linux - VMware Workstation 17 Player
Player | ||| □ □

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.

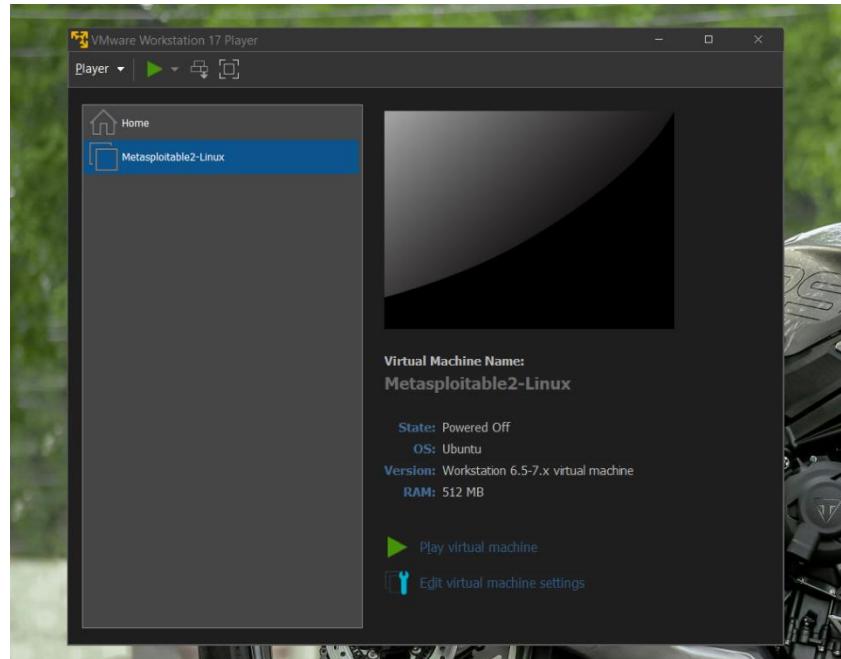
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo adduser suryansh
Adding user 'suryansh' ...
Adding new group 'suryansh' (1003) ...
Adding new user 'suryansh' (1003) with group 'suryansh' ...
Creating home directory '/home/suryansh' ...
Copying files from '/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for suryansh
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []: _
```

Snapshot Verification :

After user creation, the virtual machine state was preserved.

Since VMware Player does not support snapshots, the powered-off VM state is shown as verification.



Mutillidae II Configuration :

The Mutillidae II vulnerable web application was accessed successfully through the browser using the VM IP address, confirming proper database configuration and service availability.

URL:

<http://192.168.x.x/mutillidae>

The screenshot shows a web browser window with the URL <http://192.168.183.128/mutillidae/>. The page title is "Mutillidae: Born to be Hacked". The header includes version information (Version: 2.1.19), security level (0 - Hosed), hints status (Disabled), and user status (Not Logged In). A navigation bar with links to Home, Login/Register, Toggle Hints, Toggle Security, Reset DB, View Log, and View Captured Data. On the left, a sidebar titled "Core Controls" lists "OWASP Top 10", "Others", "Documentation", and "Resources". It features icons for a Tux logo, a gear, and a wrench. Below the sidebar, there's a note about the site being hacked and a link to Mozilla Add-ons. The main content area has a banner "Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10". It contains a section for "Latest Version / Installation" with links to "Latest Version", "Installation Instructions", "Usage Instructions", "Get rid of those pesky PHP errors", "Change Log", and "Notes". Another section titled "Samurai WTF and Backtrack contains all the tools needed or you may build your own collection" shows logos for "back|track", "Samurai Web Testing Framework", "BUILT ON ECLIPSE", "PHP MySQL", "Toad", and "HACKERS FOR CHARITY".

Conclusion:

All required tasks for Minor Project 2 were completed successfully, including VM setup, user creation, system verification, and Mutillidae II execution.