Minor–2 Project Report

Project Title: Metasploitable Setup and Mutillidae II Configuration
Student Name: Ayush Tiwari
Platform Used: VMware Workstation Pro

1. Introduction

This project demonstrates the installation and configuration of the Metasploitable vulnerable virtual machine. The objective is to create a controlled lab environment for learning web application security concepts and verifying the successful execution of Mutillidae II.

2. Metasploitable Setup

Metasploitable was successfully installed and booted on VMware Workstation Pro. The system started all required services and was accessed using the default credentials **msfadmin** / **msfadmin**. This confirmed that the Metasploitable environment was properly set up and ready for use.

```
* Starting periodic command scheduler crond                              [ OK ]
* Starting Tomcat servlet engine tomcat5.5                               [ OK ]
* Starting web server apache2                                            [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
                                                                         [ OK ]



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: _
```

3. User Creation

A new user named 'govind' was created inside Metasploitable using the adduser command. This fulfills the project requirement of creating a custom user.

```
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 govind
[sudo] password for msfadmin:
Adding user `govind' ...
Adding new group `govind' (1004) ...
Adding new user `govind' (1004) with group `govind' ...
Creating home directory `/home/govind' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for govind
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:~$
```

4. User Verification

The newly created user was verified by checking the /etc/passwd file to ensure the user was successfully added to the system.

```
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
aayush:x:1003:1003::/home/aayush:/bin/bash
aaayush:x:1004:1004:,,,:/home/aaayush:/bin/bash
ayushtiwari:x:1005:1005:,,,,:/home/ayushtiwari:/bin/bash
msfadmin@metasploitable:~$ _
```

5. Mutillidae II Database Error Fix

Initially, Mutillidae II showed database connection errors. The issue was resolved by editing the configuration file located at /var/www/mutillidae/config.inc and ensuring correct database credentials.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:f1:18:95
          inet addr:192.168.17.129  Bcast:192.168.17.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fef1:1895/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:40 errors:0 dropped:0 overruns:0 frame:0
          TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4257 (4.1 KB)  TX bytes:6934 (6.7 KB)
          Interrupt:17 Base address:0x2000

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:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$ sudo nano /var/www/mutillidae/config.inc
[sudo] password for msfadmin: _
```
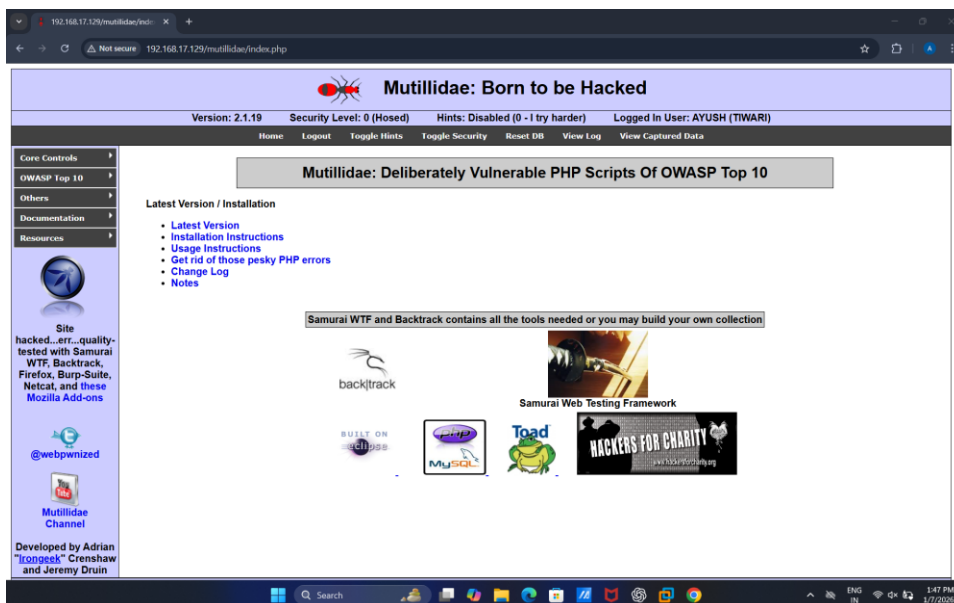
The Mutillidae II database error was resolved by editing the configuration file config.inc. The database name was changed from **metasploit** to **owasp10**, which matches the actual database used by Mutillidae II. After correcting the database name, the application connected successfully to the database and loaded without any errors.

```
  GNU nano 2.0.7        File: /var/www/mutillidae/config.inc        Modified

<?php
        /* NOTE: On Samurai, the $dbpass password is "samurai" rather than blan$

        $dbhost = 'localhost';
        $dbuser = 'root';
        $dbpass = '';
        $dbname = 'owasp10_';
?>




^G Get Help   ^O WriteOut   ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit       ^J Justify    ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
```

6. Successful Execution of Mutillidae II

After fixing the configuration, Mutillidae II loaded successfully in the browser without any errors, confirming the database connection and setup were correct.

7. Conclusion

This project successfully demonstrates the installation and configuration of the Metasploitable virtual machine using VMware Workstation Pro. A new user was created and verified within the system, fulfilling the project requirements. The Mutillidae II database error was identified and resolved by correcting the database configuration, after which the application worked successfully in the browser. Overall, this project provided practical exposure to virtual machine setup, Linux commands, and basic web application security concepts.