RUNGTA COLLEGE OF ENGINEERING & TECHNOLOGY

TECHNICAL TRAINING PROJECT (CYBER SECURITY)

Name of Project: Installation, Configuration and Verification of Metasploitable with Mutillidae II

Branch: CSE (CORE) – 3rd Semester

Section: B

Student Name : ABHISHEK BAG YADAV

ERP ID: 6606929

Professor Name: Prashant Kamkar

Date of Submission: 26-12-25

Student Signature: ____________________

Professor Signature: ____________________

INDEX

1. Introduction

The Minor 2 project is designed to provide hands-on experience with vulnerable systems used in cybersecurity learning. In this project, Metasploitable, an intentionally vulnerable Linux-based virtual machine, is installed and configured in a virtualized environment. Metasploitable is widely used by students and security professionals to understand system vulnerabilities, services, and misconfigurations in a safe and controlled manner.

Along with Metasploitable, the project also focuses on Mutillidae II, which is a deliberately vulnerable web application developed by OWASP. Mutillidae II is used to understand common web-based attacks such as SQL Injection, Cross-Site Scripting (XSS), and authentication issues. During the setup, Mutillidae II may show database connection errors, which are part of the learning objective of this project.

The project not only focuses on installation but also emphasizes system administration tasks such as user creation, snapshot management, and service verification. Screenshots are used as proof of successful completion of each task. This project helps students understand the practical aspects of virtualization, Linux commands, and basic troubleshooting techniques used in cybersecurity environments.

2. Objectives of the Project

- To install and configure Metasploitable in a virtual environment
- To create a new user with the student’s own name
- To take a snapshot after user creation
- To identify and fix the Mutillidae II database error
- To verify successful execution using screenshots.

3. **System Requirements**

Hardware Requirements

- Minimum 4 GB RAM
- At least 20 GB free disk space

Software Requirements

- Windows OS / macOS
- VMware (for Windows) or UTM (for macOS)
- Metasploitable virtual machine image
- Web browser (Firefox / Chrome)

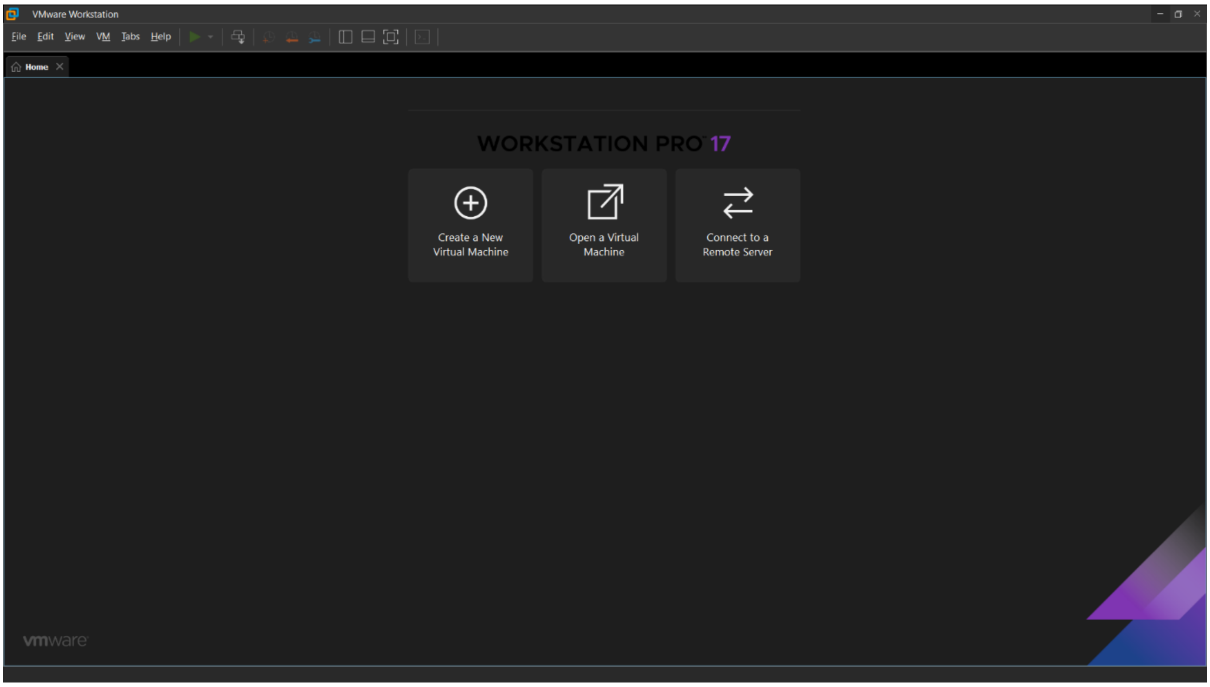
4. Metasploitable Setup

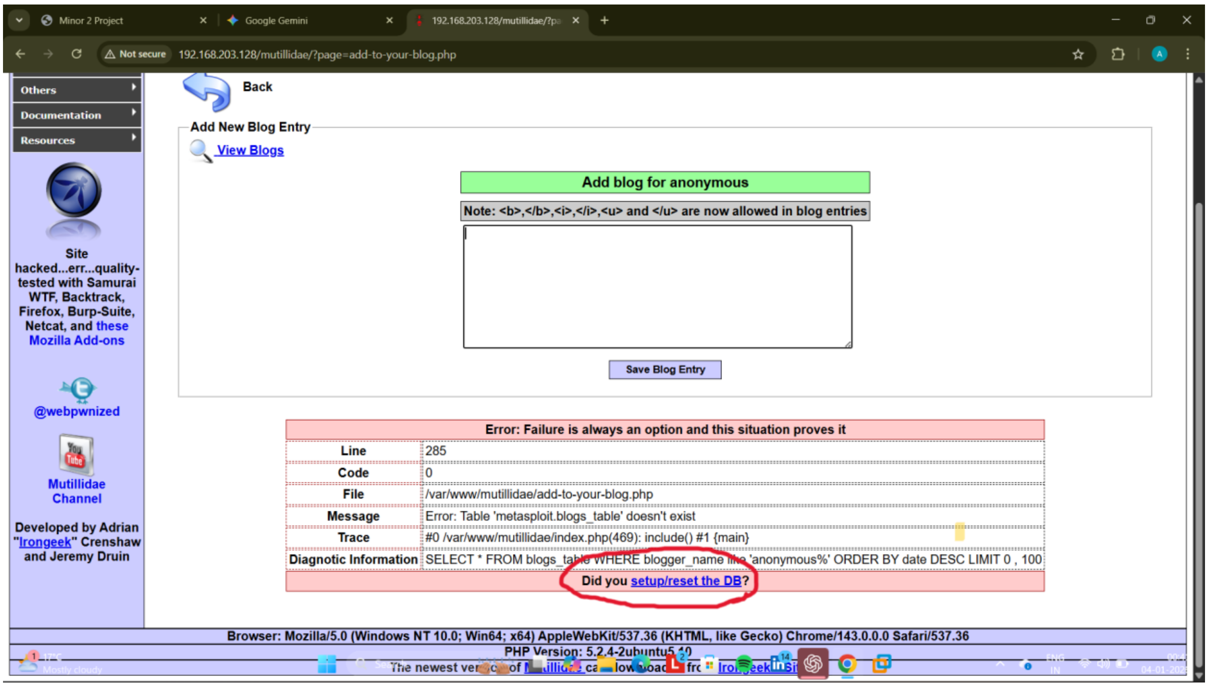
Metasploitable was set up using virtualization software to create an isolated and safe testing environment. For Windows systems, VMware was used, while macOS users can use UTM. The Metasploitable virtual machine image was first downloaded from a trusted source and then imported into the virtualization software.

After importing the image, the virtual machine settings were reviewed. Network configuration was set appropriately to allow communication between the host system and the virtual machine. Once configuration was completed, the Metasploitable virtual machine was powered on.

During startup, Metasploitable booted into the Linux operating system successfully. The login screen confirmed that the virtual machine was running properly. This step verified that the installation process was completed without errors and the system was ready for further configuration.

Step -1 First open the vmware


VMware Workstation
File Edit View VM Tabs Help
Home
WORKSTATION PRO 17
Create a New Virtual Machine
Open a Virtual Machine
Connect to a Remote Server
vmware



Add blog for anonymous

Note: <b>,</b>,<i>,</i>,<u> and </u> are now allowed in blog entries

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

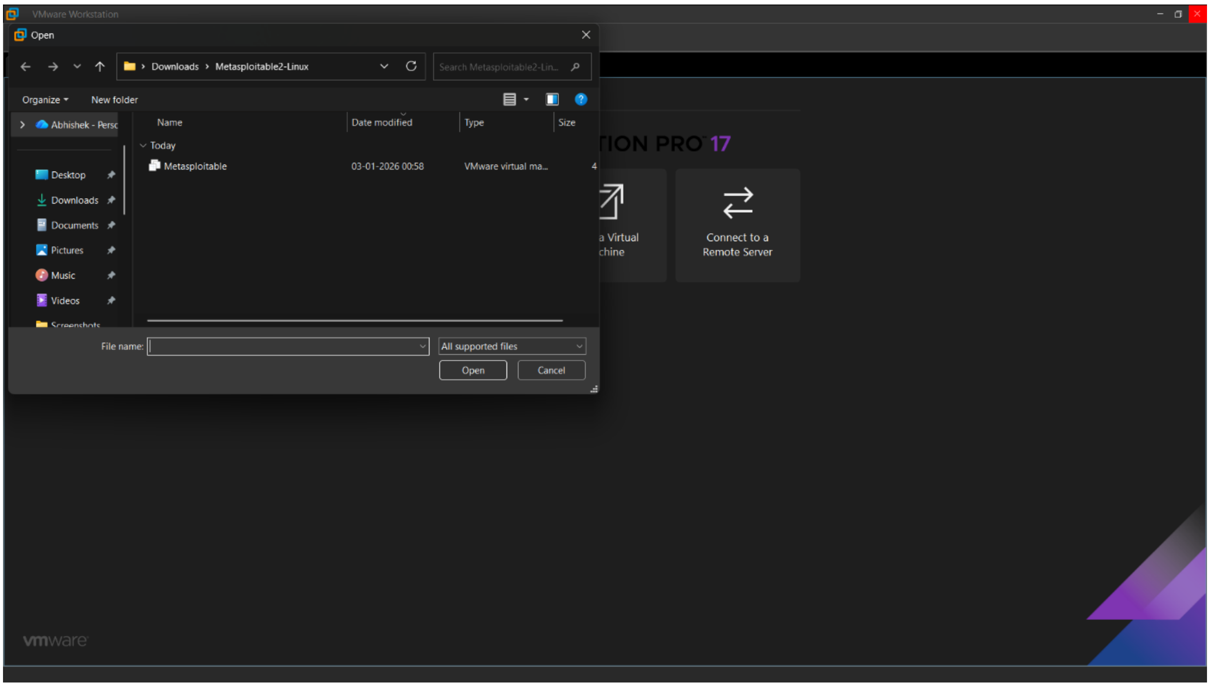
Developed by Adrian "Irongeek" Crenshaw and Jeremy Druin

Error: Failure is always an option and this situation proves it	
Line	285
Code	0
File	/var/www/mutillidae/add-to-your-blog.php
Message	Error: Table 'metasploit.blogs_table' doesn't exist
Trace	#0 /var/www/mutillidae/index.php(469): include() #1 {main}
Diagnotic Information	SELECT * FROM blogs_table WHERE blogger_name like 'anonymous%' ORDER BY date DESC LIMIT 0 , 100
Did you setup/reset the DB?	

Browser: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36

PHP Version: 5.2.4-2ubuntu5.10

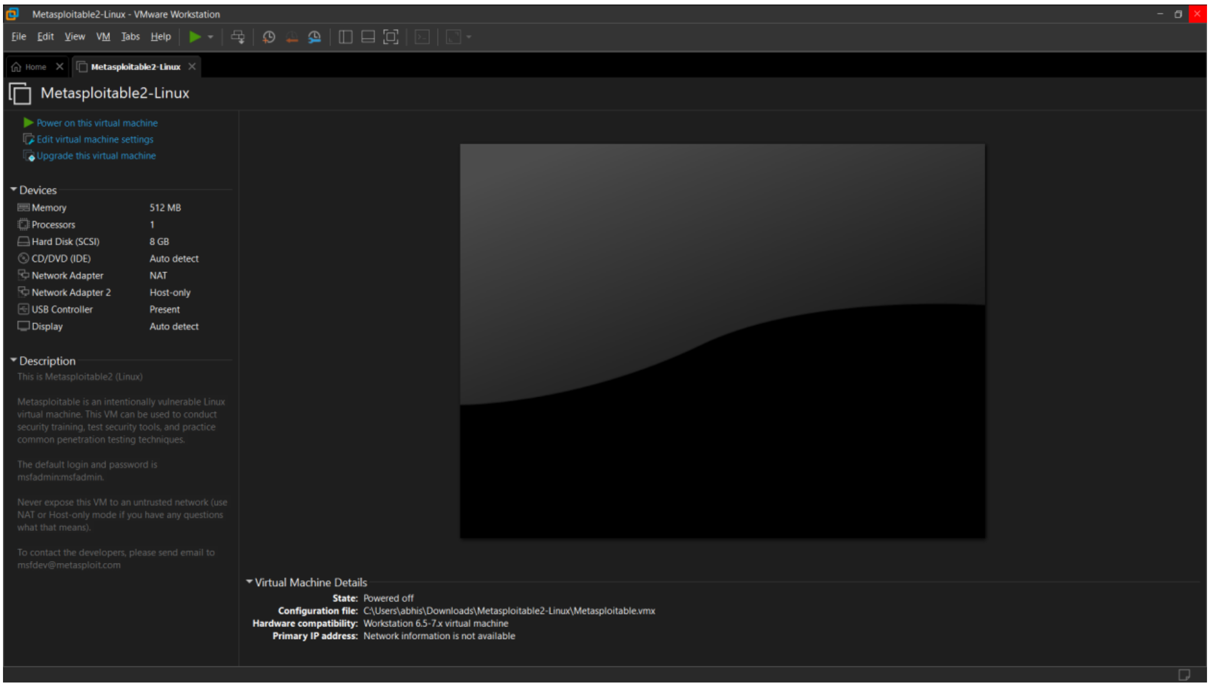
Step-2 Then select melspoiltable 2



Name	Date modified	Type	Size
Today			
Metasploitable	03-01-2026 00:58	VMware virtual ma...	4

File name:

Then run metaspolitable in vmware



Metasploitable2-Linux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
Power on this virtual machine
Edit virtual machine settings
Upgrade this virtual machine

Metasploitable2-Linux

Devices

Memory	512 MB
Processors	1
Hard Disk (SCSI)	8 GB
CD/DVD (IDE)	Auto detect
Network Adapter	NAT
Network Adapter 2	Host-only
USB Controller	Present
Display	Auto detect

Description

This is Metasploitable2 (Linux)

Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and practice common penetration testing techniques.

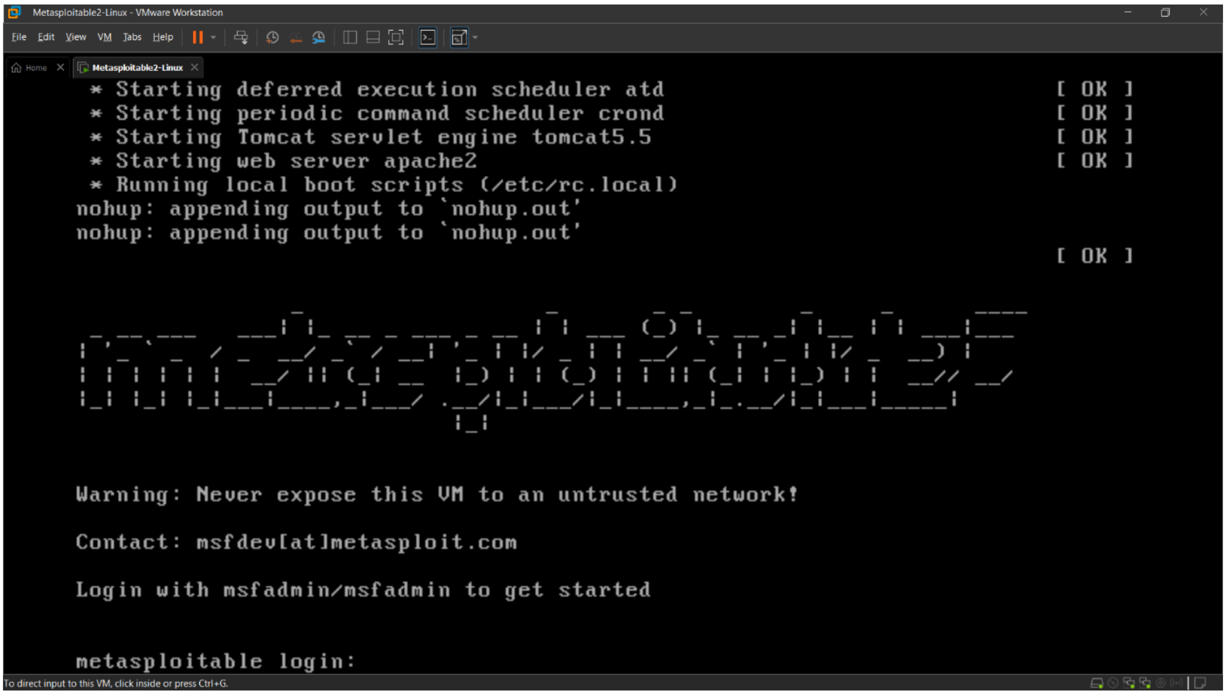
The default login and password is msfadmin:msfadmin.

Never expose this VM to an untrusted network (use NAT or Host-only mode if you have any questions what that means).

To contact the developers, please send email to msfdev@metasploit.com

Virtual Machine Details

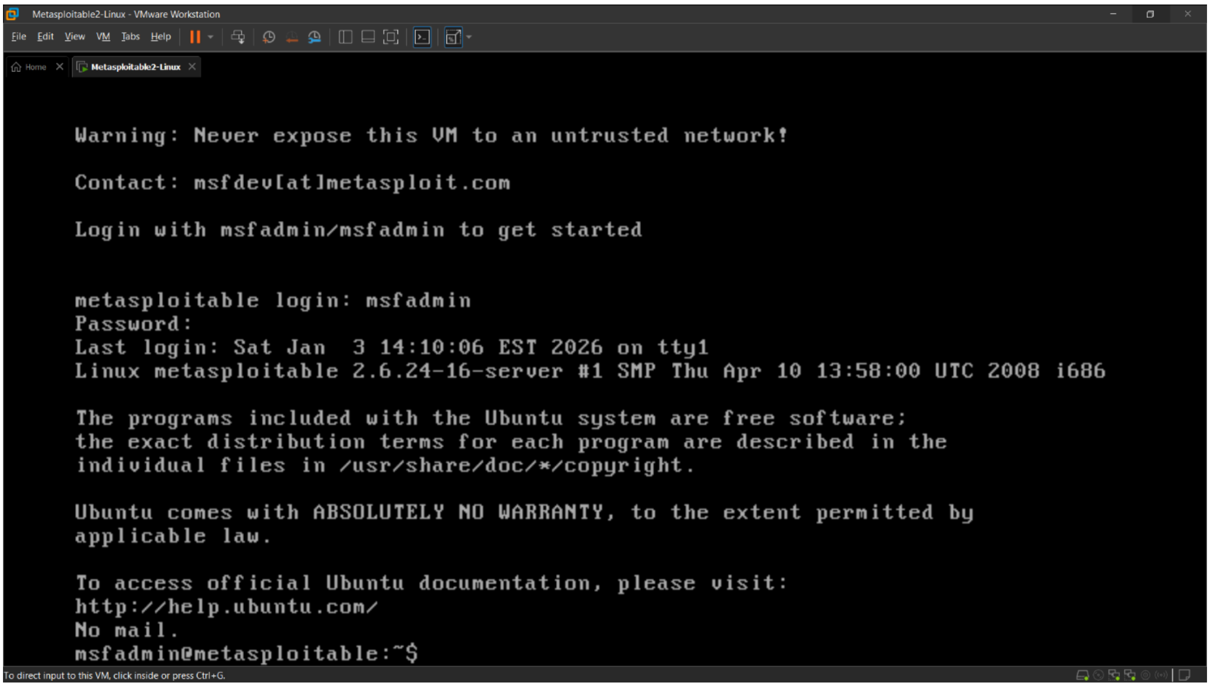
State: Powered off
Configuration file: C:\Users\abhis\Downloads\Metasploitable2-Linux\Metasploitable.vmx
Hardware compatibility: Workstation 6.5-7.x virtual machine
Primary IP address: Network information is not available



```
 * Starting deferred execution scheduler atd                              [ OK ]
 * 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:
```

THEN login this in login id :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: Sat Jan  3 14:10:06 EST 2026 on tty1
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:~$
```

5. User Creation in Metasploitable

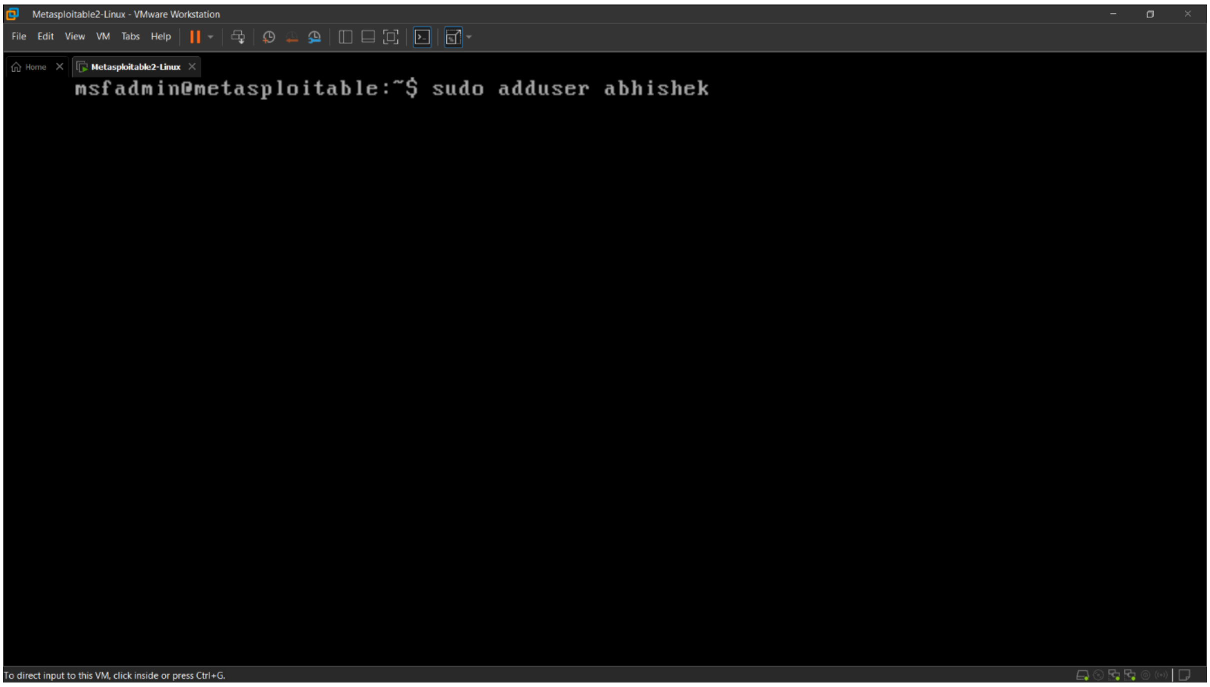
User management is an important part of Linux system administration. After logging into the Metasploitable system using the default credentials, a new user was created using the terminal. The user was created using the student’s own name to personalize the system and meet the project requirement.

The adduser command was used to create the new user account. A password was then assigned using the passwd command. During this process, the system prompted for user details and password confirmation. After successful creation, the user account was verified by switching from the default user to the newly created user.

This step confirms that the system allows proper user management and that the new user can log in without any issues. It also demonstrates understanding of basic Linux commands and permissions.

Commands Used

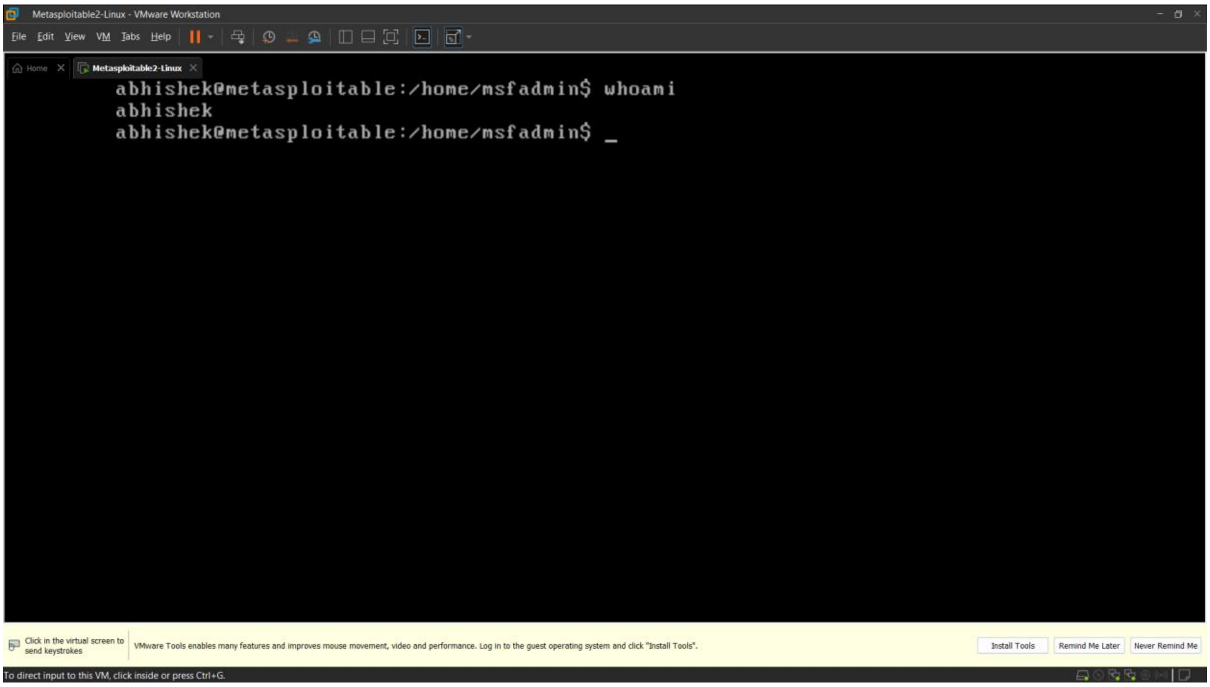
- adduser abhishek
- passwd abhishek



Metasploitable2-Linux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
To direct input to this VM, click inside or press Ctrl+G.

```
msfadmin@metasploitable:~$ sudo adduser abhishek
```

Check with command <whoami>



Metasploitable2-Linux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux

```
abhishek@metasploitable:/home/msfadmin$ whoami
abhishek
abhishek@metasploitable:/home/msfadmin$ _
```

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

To direct input to this VM, click inside or press Ctrl+G.

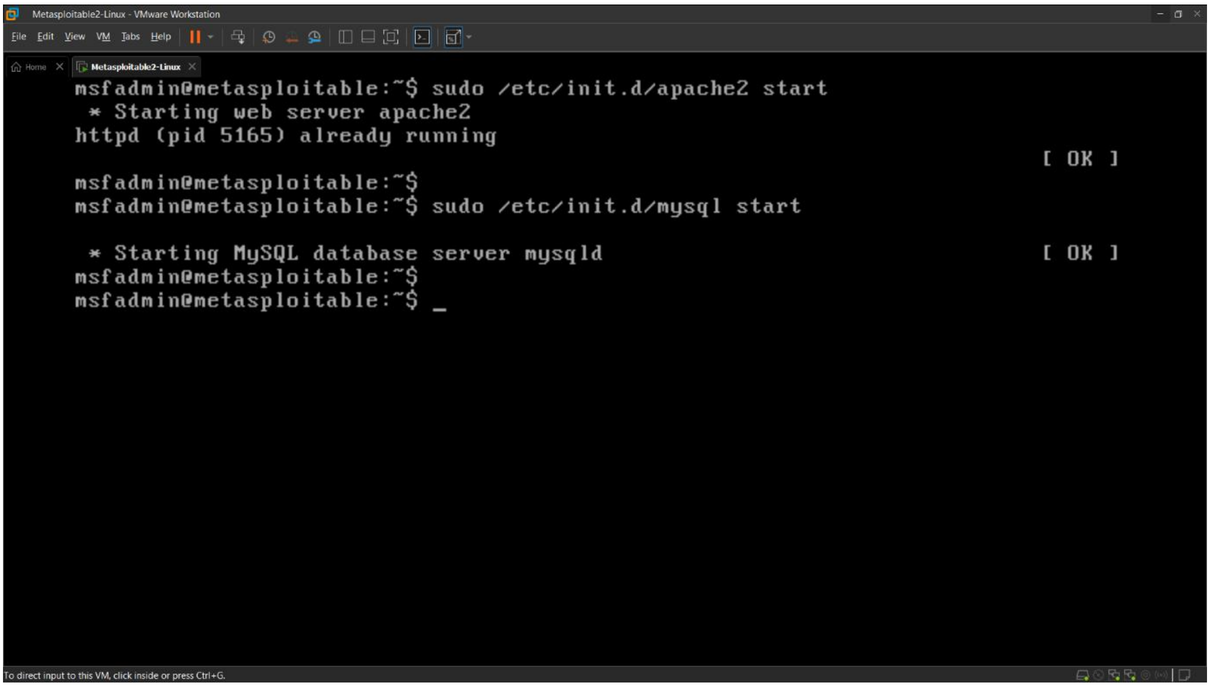
7. Mutillidae II Database Error Fix

When accessing Mutillidae II through the web browser, a database connection error was initially observed. This error commonly occurs when the MySQL database service is not running or the database is not properly configured. Identifying and resolving this issue is an important learning outcome of the project.

To fix the error, the MySQL database service was started using the terminal. After ensuring that the database service was running, the Mutillidae II setup page was accessed through the browser. The application provides an option to reset and configure the database automatically.

By clicking on the Reset DB option, the required database tables were created successfully. After completing this process, the Mutillidae II application reloaded without showing any errors. The application dashboard confirmed that Mutillidae II was functioning correctly.

Then we have to run command to start sql and apache2

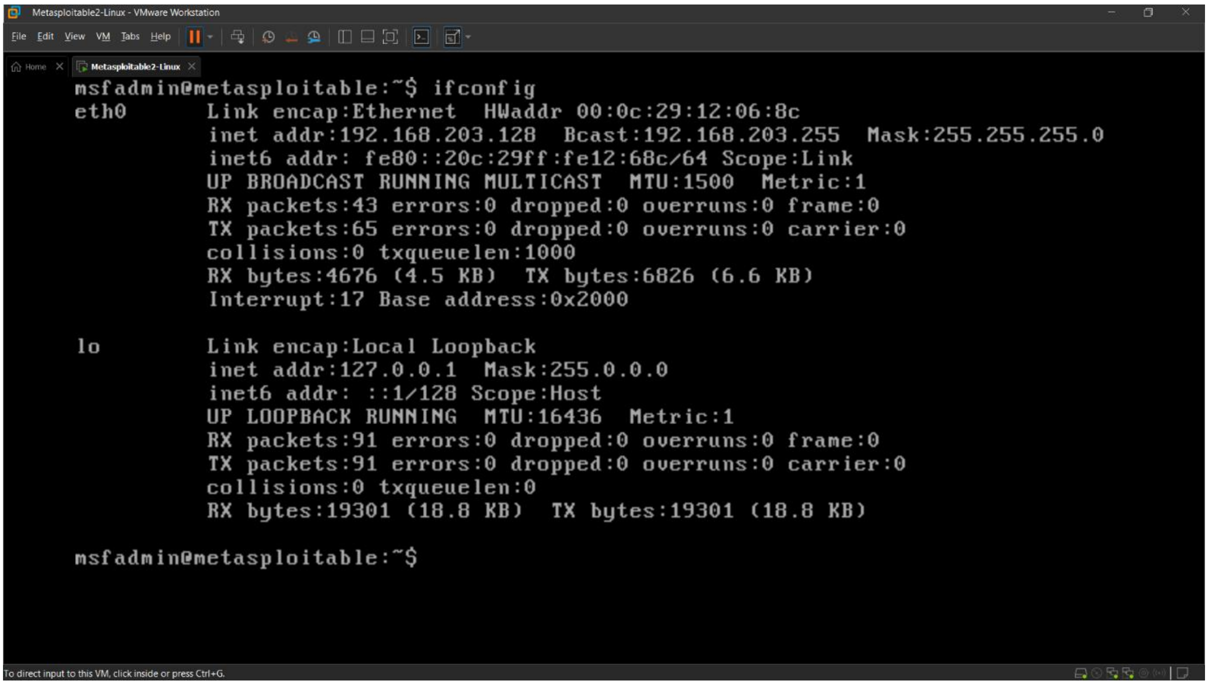


```
msfadmin@metasploitable:~$ sudo /etc/init.d/apache2 start
 * Starting web server apache2
httpd (pid 5165) already running
                                                                   [ OK ]
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ sudo /etc/init.d/mysql start

 * Starting MySQL database server mysqld                           [ OK ]
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ _
```

To direct input to this VM, click inside or press Ctrl+G.

NOW OPEN IN METASPLOITABLE AND RUN COMMAND <IPCONFIG>

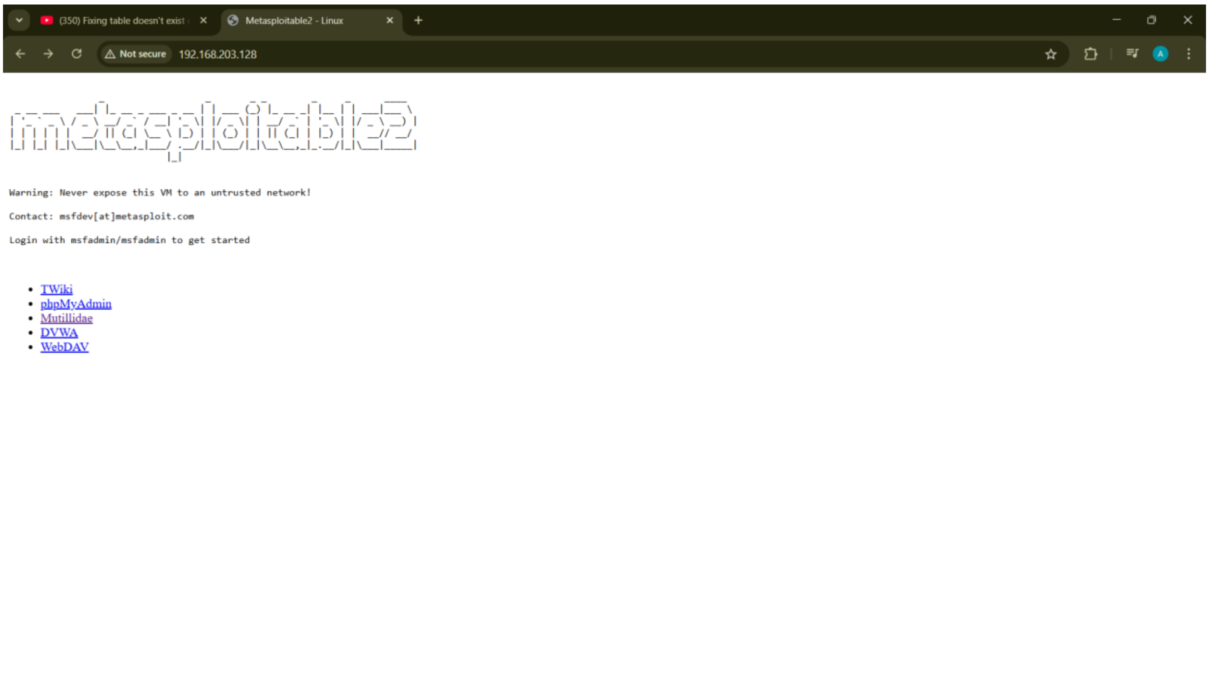
TO GENERATE IP



Metasploitable2-Linux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
To direct input to this VM, click inside or press Ctrl+G.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:12:06:8c
          inet addr:192.168.203.128  Bcast:192.168.203.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe12:68c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:43 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4676 (4.5 KB)  TX bytes:6826 (6.6 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:~$
```

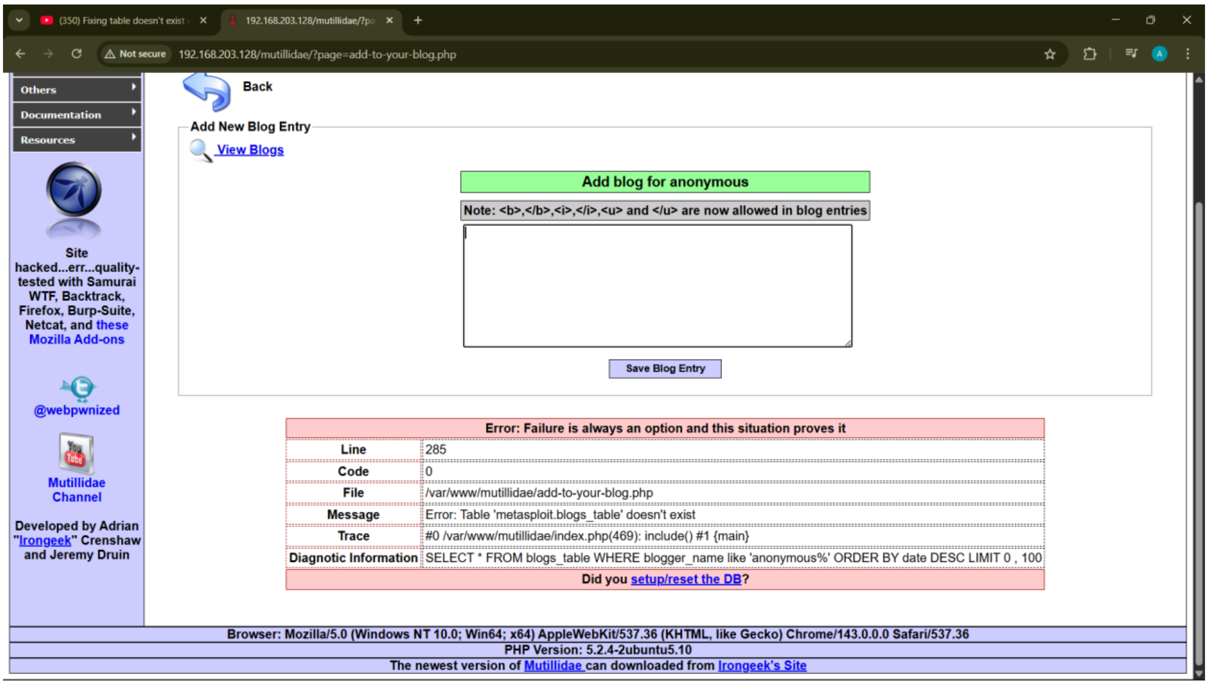
THEN AFTER THAT OPEN THIS COMMAND << http <metasploitable ip> /mutillidae



```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

Before error fix


(350) Fixing table doesn't exist
192.168.203.128/mutillidae/?pa
Not secure
192.168.203.128/mutillidae/?page=add-to-your-blog.php
Others
Documentation
Resources
Back

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

Add New Blog Entry

View Blogs

Add blog for anonymous

Note: <b>,</b>,<i>,</i>,<u> and </u> are now allowed in blog entries

Save Blog Entry

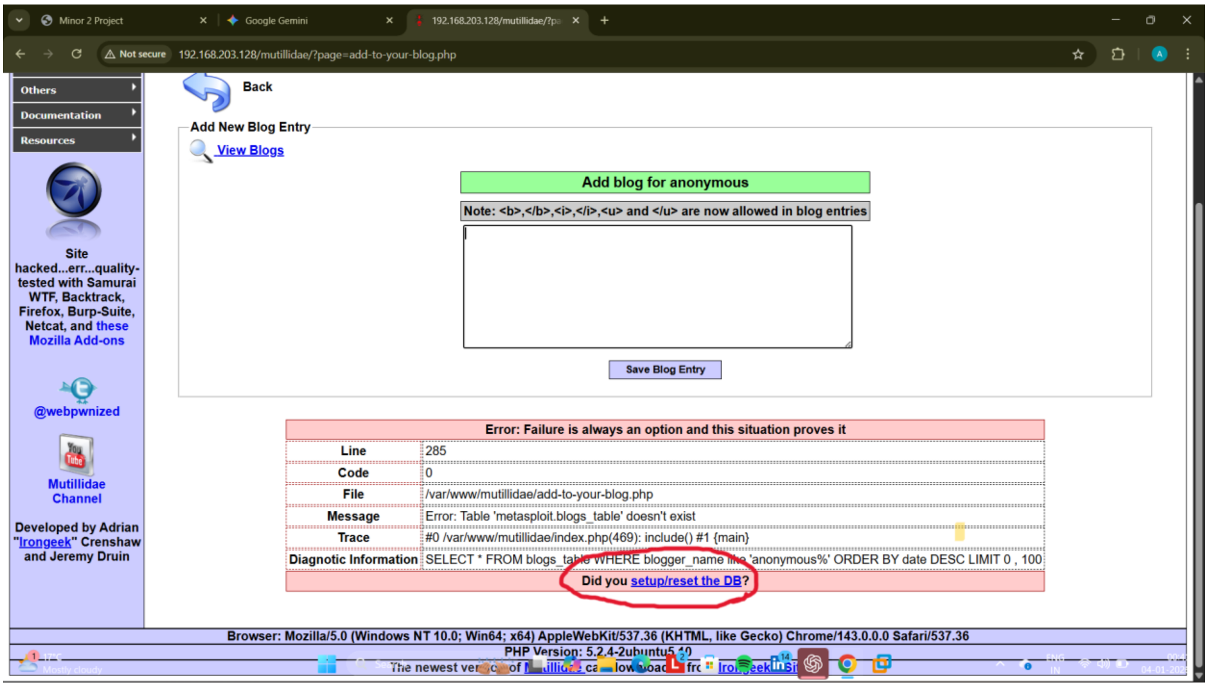
Error: Failure is always an option and this situation proves it	
Line	285
Code	0
File	/var/www/mutillidae/add-to-your-blog.php
Message	Error: Table 'metasploit.blogs_table' doesn't exist
Trace	#0 /var/www/mutillidae/index.php(469): include() #1 {main}
Diagnotic Information	SELECT * FROM blogs_table WHERE blogger_name like 'anonymous%' ORDER BY date DESC LIMIT 0 , 100
Did you setup/reset the DB?	

Browser: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
PHP Version: 5.2.4-2ubuntu5.10
The newest version of Mutillidae can downloaded from Irongeek's Site

AFTER CLICK SETUP/RESET THE DB

OR

RUN COMMAND <http://<Metasploitable-IP>/mutillidae/reset.php


Minor 2 Project
Google Gemini
192.168.203.128/mutillidae/?pa
Not secure
192.168.203.128/mutillidae/?page=add-to-your-blog.php
Others
Documentation
Resources
Back

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

Add New Blog Entry

View Blogs

Add blog for anonymous

Note: <b>,</b>,<i>,</i>,<u> and </u> are now allowed in blog entries

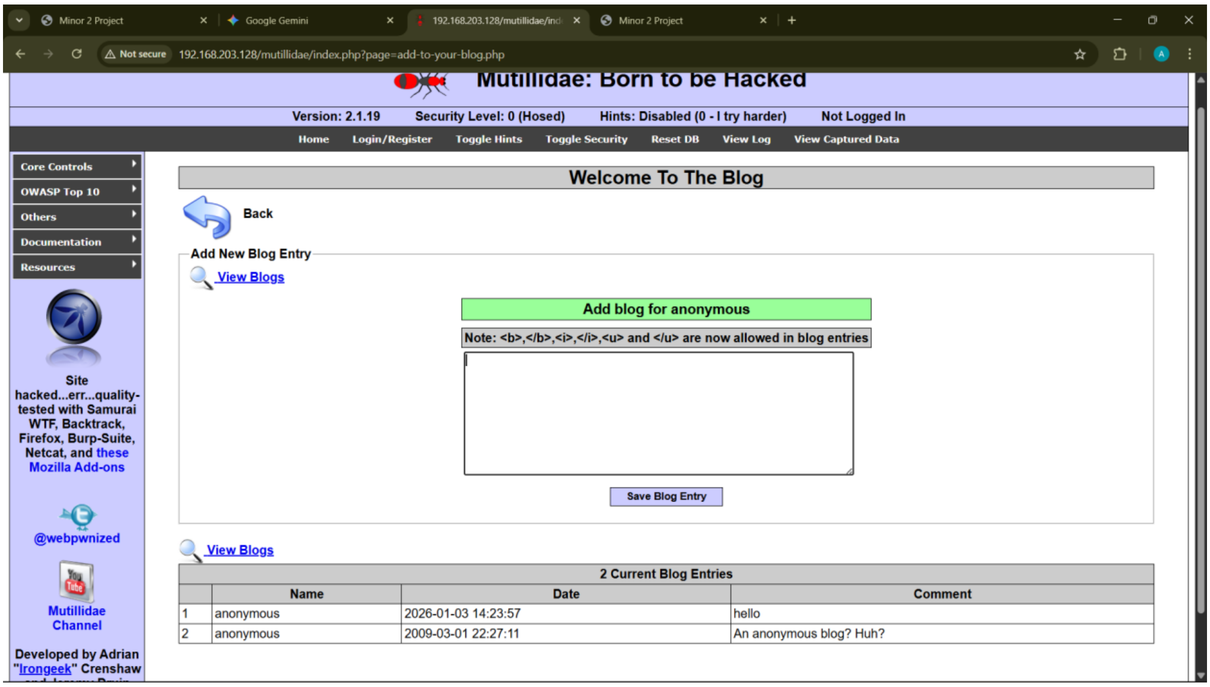
Save Blog Entry

Error: Failure is always an option and this situation proves it	
Line	285
Code	0
File	/var/www/mutillidae/add-to-your-blog.php
Message	Error: Table 'metasploit.blogs_table' doesn't exist
Trace	#0 /var/www/mutillidae/index.php(469): include() #1 {main}
Diagnotic Information	SELECT * FROM blogs_table WHERE blogger_name like 'anonymous%' ORDER BY date DESC LIMIT 0 , 100
Did you setup/reset the DB?	

Browser: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
PHP Version: 5.2.4-2ubuntu5.10

AFTER THAT ERROR WILL BE FIX

PROOF



Mutillidae: Born to be Hacked

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

Welcome To The Blog

Add New Blog Entry

Add blog for anonymous

Note: <b>,</b>,<i>,</i>,<u> and </u> are now allowed in blog entries

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

Developed by Adrian "Irongeek" Crenshaw

2 Current Blog Entries

	Name	Date	Comment
1	anonymous	2026-01-03 14:23:57	hello
2	anonymous	2009-03-01 22:27:11	An anonymous blog? Huh?

10. Conclusion

The Minor 2 project was completed successfully by installing and configuring Metasploitable and resolving the Mutillidae II database error. Through this project, practical knowledge of virtualization, Linux system administration, and web application troubleshooting was gained.

The project provided real-world exposure to vulnerable systems used in cybersecurity education. Creating users, managing snapshots, starting services, and fixing application errors helped in The use of screenshots as verification ensured transparency and proper documentation of each step.

Overall, this project strengthened the understanding of cybersecurity fundamentals and prepared a strong base for advanced security testing and ethical hacking concepts in future studies.