Vulnerability Assessment & System Setup Report

--METASPLOITABLE

---BY: VINAYAK CHAUHAN

Introduction 😊

Metasploitable 2 is an intentionally vulnerable Linux-based virtual machine designed for practicing vulnerability assessment and penetration testing in a controlled environment. It is widely used in cybersecurity education to demonstrate common system vulnerabilities and misconfigurations.

This report documents the process of downloading, installing, and verifying the Metasploitable 2 virtual machine using Oracle VirtualBox for educational purposes only.

1.1 Objective of the Report

The objectives of this report are:

- To document the procedure for downloading Metasploitable 2
- To explain the setup of the vulnerable machine in a virtual environment
- To verify successful deployment of the system
- To create a safe and isolated lab environment for security learning
- To follow ethical and legal guidelines during system setup

1.2 Scope of the Report

This report includes:

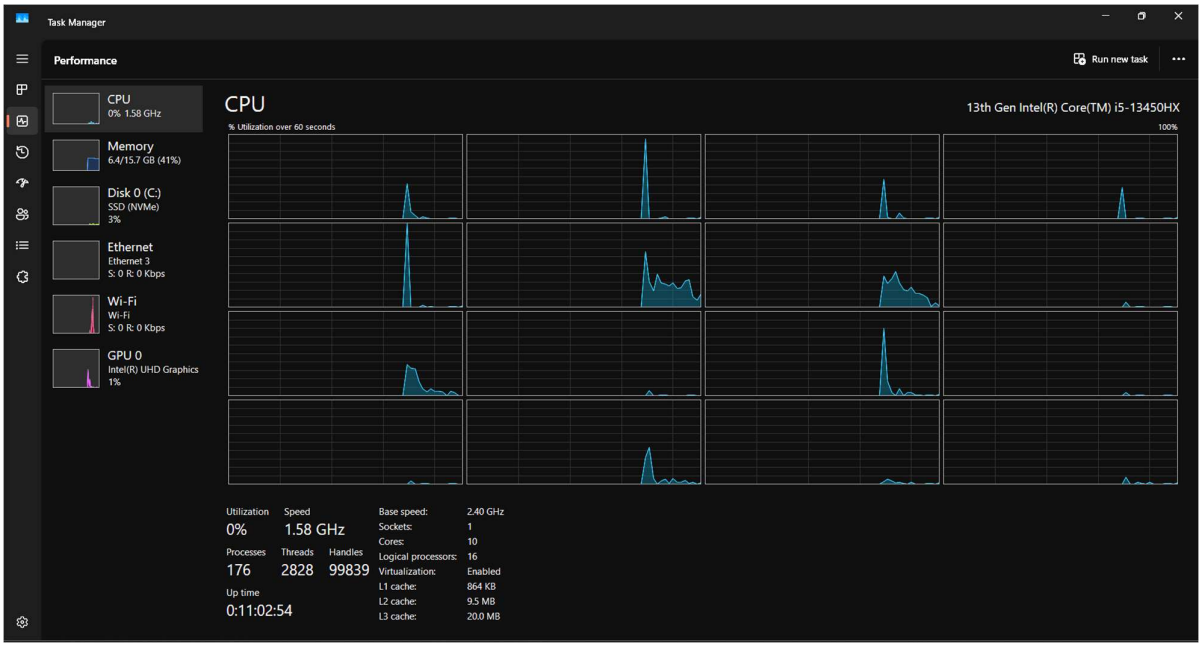
- System and software requirements
- Download procedure for Metasploitable 2
- Virtual machine configuration steps
- Post-installation verification
- Observations and challenges faced
- Security and ethical considerations

System Requirements

2.1 Hardware Requirements

Minimum hardware requirements:

- Processor: Intel/AMD 64-bit processor
- RAM: Minimum 1 GB
- Storage: Minimum 10 GB free disk space
- Virtualization: Enabled in BIOS/UEFI



2.2 Software Requirements

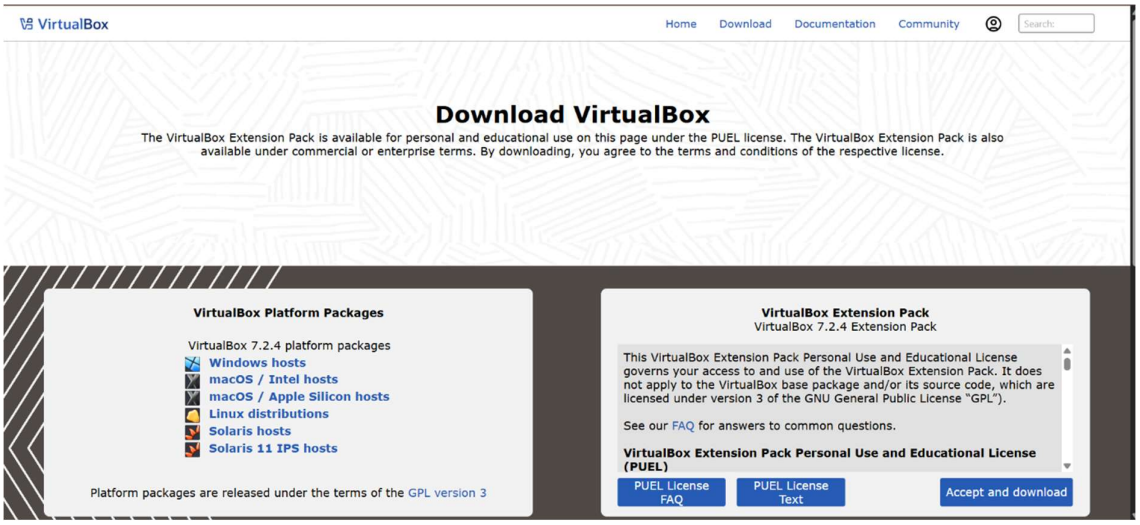
- Host Operating System: Windows 10 / Windows 11
- Virtualization Software: Oracle VirtualBox
- Guest OS: Metasploitable 2 Virtual Machine
- Internet Connection: Optional (not recommended during testing)

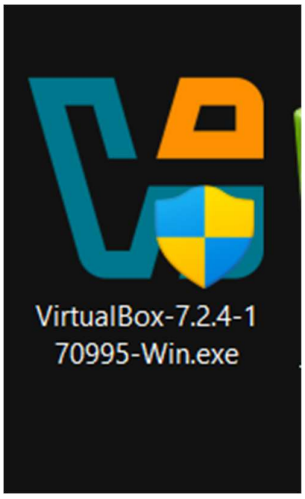
Download Procedure

3.1 Downloading Oracle VirtualBox

Steps followed:

1. Visited the official Oracle VirtualBox website
2. Downloaded the Windows host installer
3. Installed VirtualBox using default settings





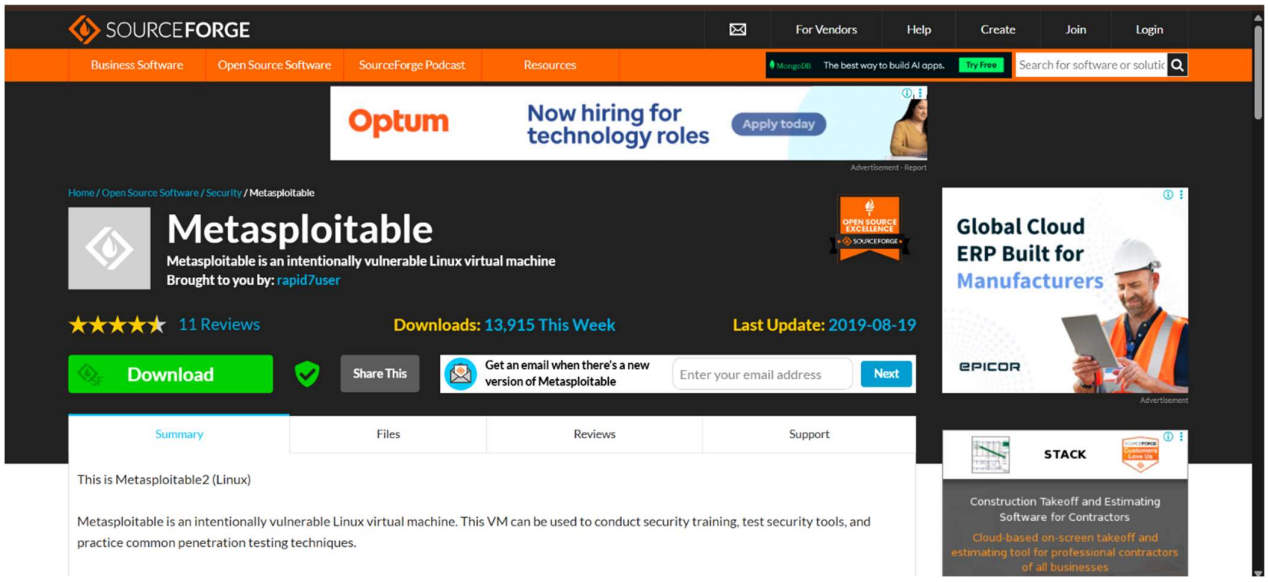
VirtualBox Installed Successfully

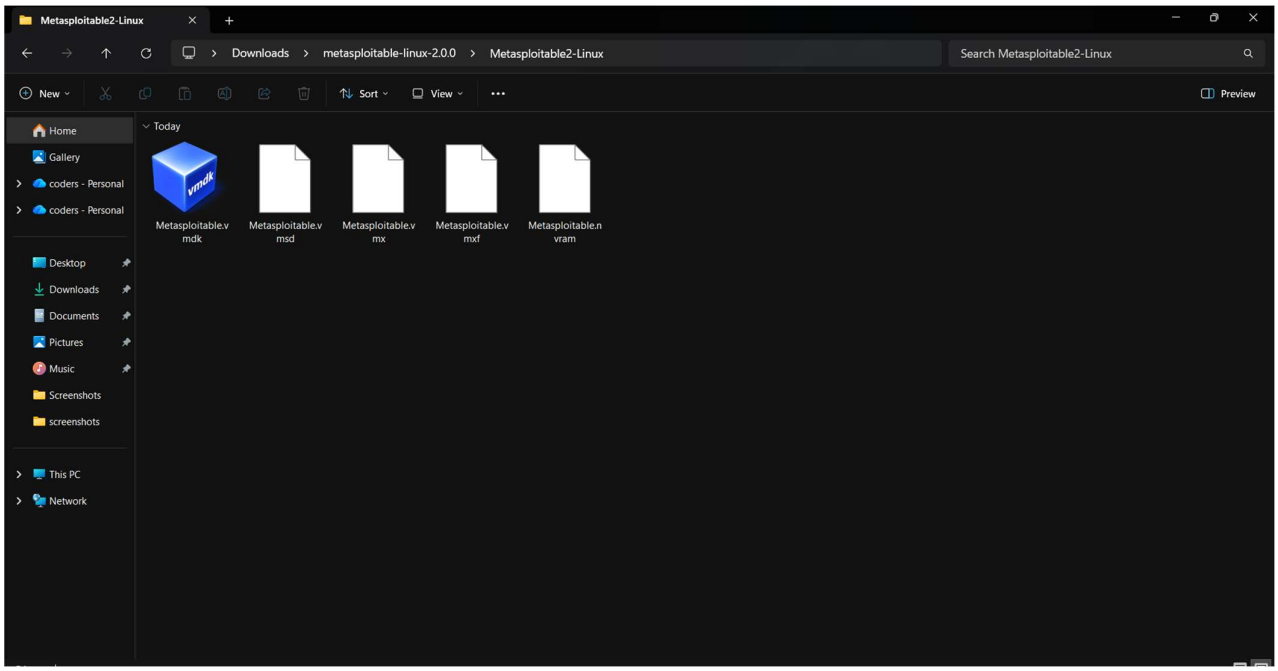
3.2 Downloading the Operating System Image

Steps followed:

1. Visited the official Metasploitable download source
2. Downloaded the Metasploitable 2 compressed file
3. Extracted the virtual machine files

Source used: Official Metasploitable download site.



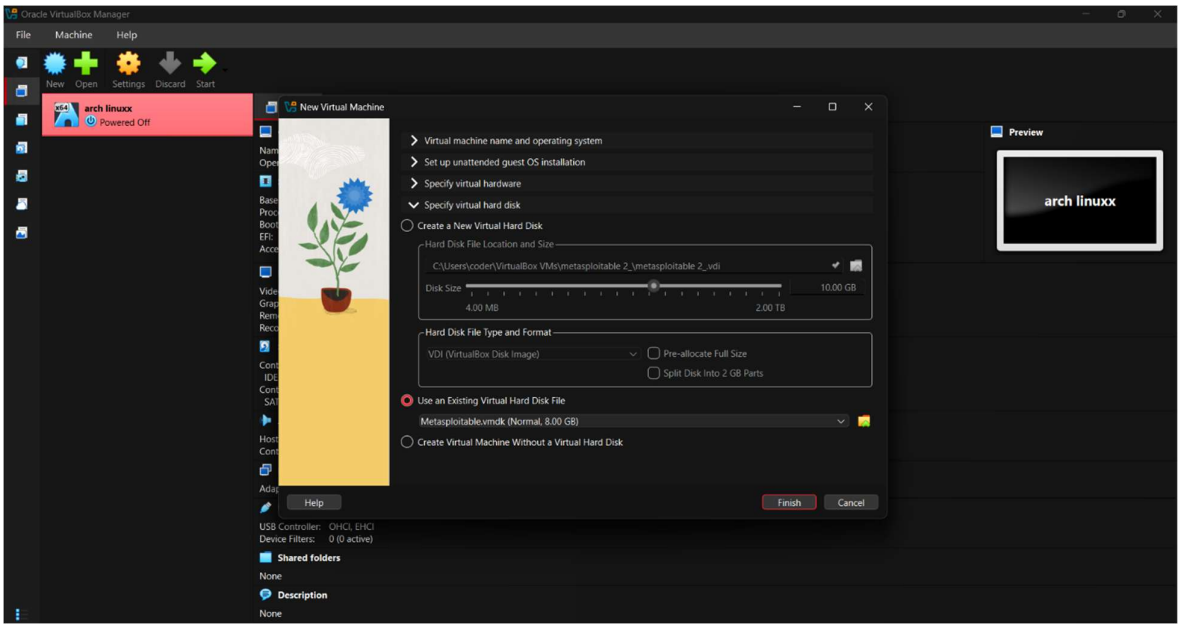


Installation and Configuration

4.1 Virtual Machine Creation

Steps followed:

1. Opened Oracle VirtualBox
2. Selected **New** or **Add Existing VM**
3. Imported Metasploitable 2 virtual machine
4. Named the VM as **Metasploitable 2**
5. Selected Type: Linux
6. Selected Version: Other Linux (32-bit)

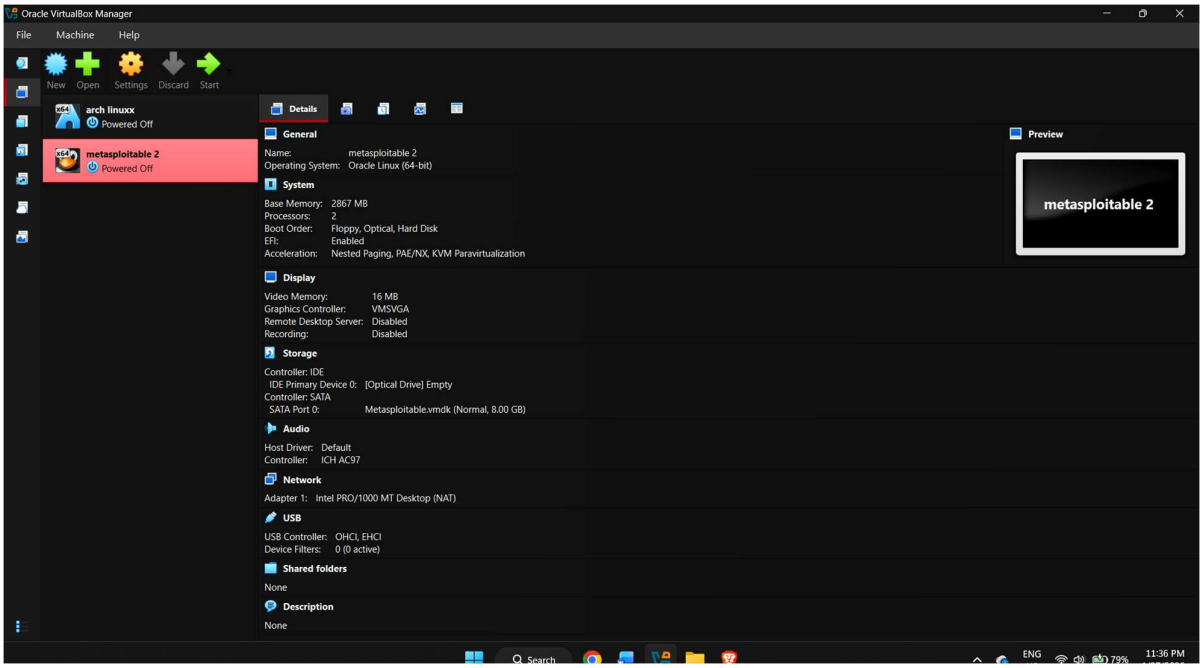


4.2 Resource Allocation (RAM, CPU, Storage)

Resources allocated:

- RAM: 1024 MB
- CPU Cores: 1
- Storage: Pre-configured virtual disk

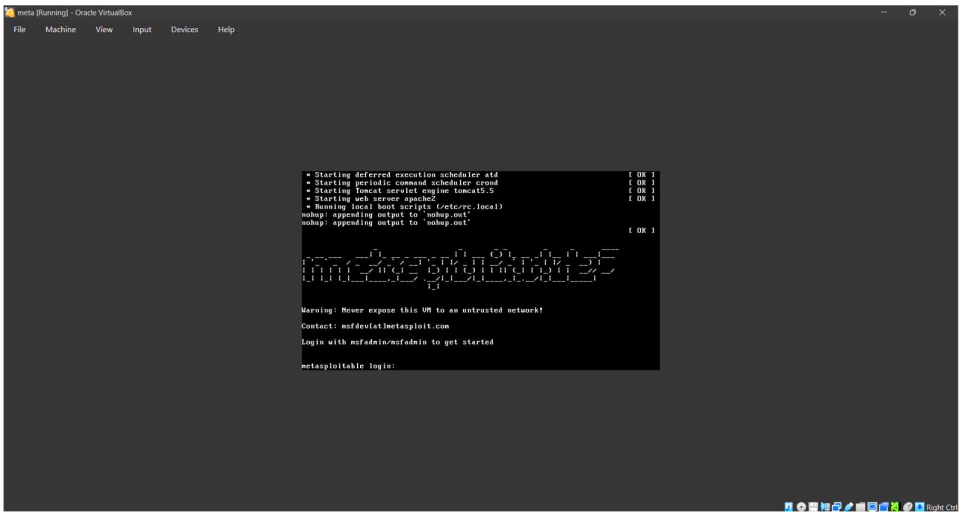
Minimal resources were allocated as Metasploitable is designed to be lightweight.



4.3 Operating System Installation Steps

Metasploitable 2 does not require a traditional installation process.
Steps followed:

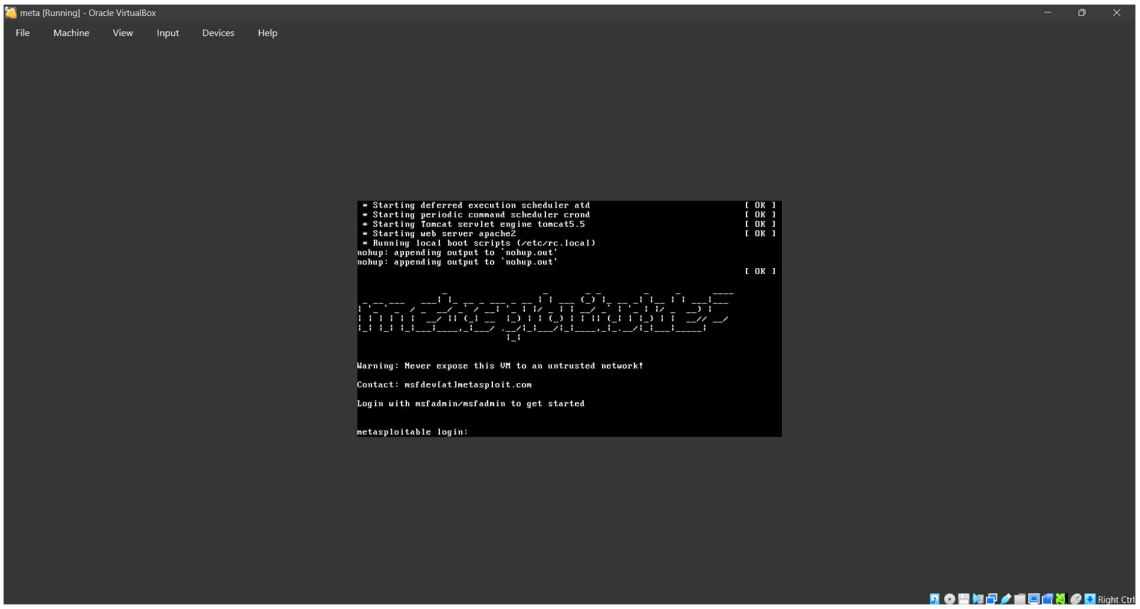
1. Imported the VM into VirtualBox
2. Configured network settings
3. Started the virtual machine
4. Verified system boot



Post-Installation Verification

5.1 Successful Boot Verification

The system booted successfully into the Metasploitable 2 login prompt without errors.



5.2 Network Connectivity Verification

Network configuration was verified to ensure proper communication within the virtual lab.

Command used:

“Ipconfig”

```
msfadmin@metasploitable:~$ ifcofig
-bash: ifcofig: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:75:13:32
          inet addr:[redacted]  Bcast:[redacted]  Mask:[redacted]
          inet6 addr: [redacted]:fe75:1332/64 Scope:Global
          inet6 addr: [redacted]:fe75:1332/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:33 errors:0 dropped:0 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4522 (4.4 KB)  TX bytes:7748 (7.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:[redacted]  Mask:[redacted]
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:109 errors:0 dropped:0 overruns:0 frame:0
          TX packets:109 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:27661 (27.0 KB)  TX bytes:27661 (27.0 KB)

msfadmin@metasploitable:~$ _
```

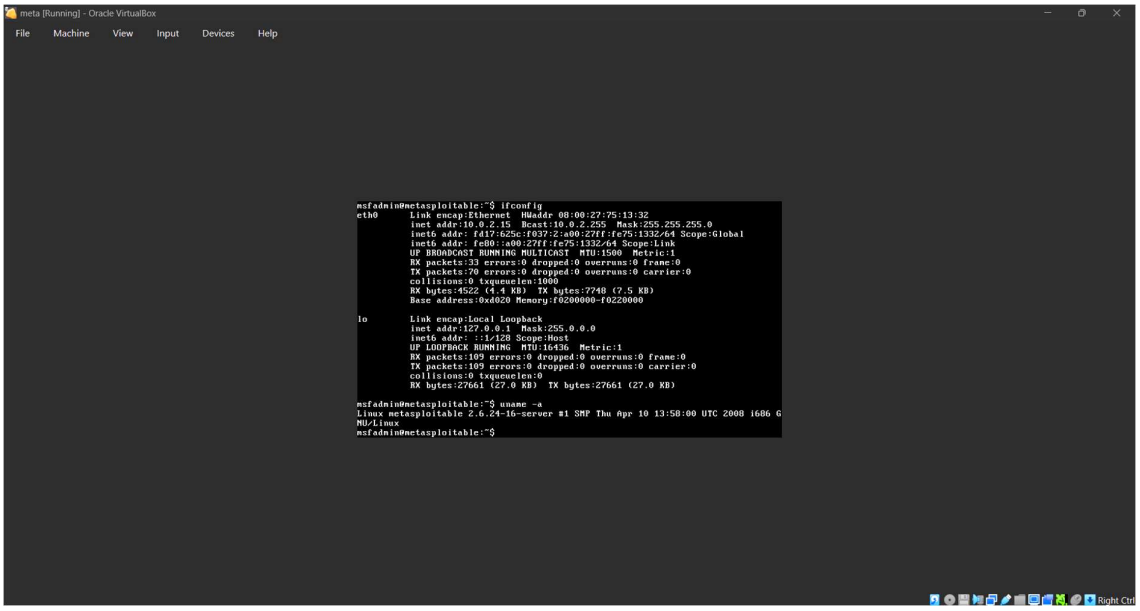
5.3 System Information Verification

System details verified:

- OS Type: Linux
- Kernel Information
- IP Address Assignment

Command used:

“Uname -a”



Observations

 Metasploitable 2 contains intentionally vulnerable services

 System boots quickly with minimal resources

 Designed strictly for security testing practice

 Useful for understanding real-world vulnerabilities in a lab environment

---

Challenges Faced and Solutions

7.1 Errors Encountered

Issue	Cause
VM not starting	Incorrect OS type selected
Network issues	Improper adapter configuration

7.2 Troubleshooting Steps

Issue	Solution
VM boot issue	Selected correct Linux version
Network fixed	Adapter set to Host-only / Internal Network

Security Considerations

⚠️ **Important Security Notice**

- Metasploitable 2 is intentionally vulnerable
- The system was used only in an isolated virtual lab
- No internet-facing deployment was performed
- No attacks were conducted on real-world systems
- This setup complies with ethical hacking guidelines

Conclusion

This report successfully documents the setup of Metasploitable 2 in a controlled virtual environment. The exercise provided practical exposure to vulnerable systems and reinforced the importance of ethical practices in cybersecurity education.

References

- Metasploitable Official Documentation
- Oracle VirtualBox – https://www.virtualbox.org
- Cybersecurity Training Resources