Software and Cybersecurity (CS 445)

Lab Assignment 07

Name: Darshan Hangoje

Student ID: 202251034

Objective:

The purpose of this lab is to :

- Get hands-on experience with Kali Linux, a professional ethical hacking and penetration testing distribution.
- Create a virtual environment using Oracle VirtualBox to run Kali Linux without affecting the host operating system.
- Learn the installation, configuration, and updating process of Kali Linux.
- Use Nmap and Zenmap for reconnaissance — identifying network devices, open ports, and possible vulnerabilities.
- Configure Metasploitable as a deliberately vulnerable machine for practical testing and scanning

Tools and Technologies

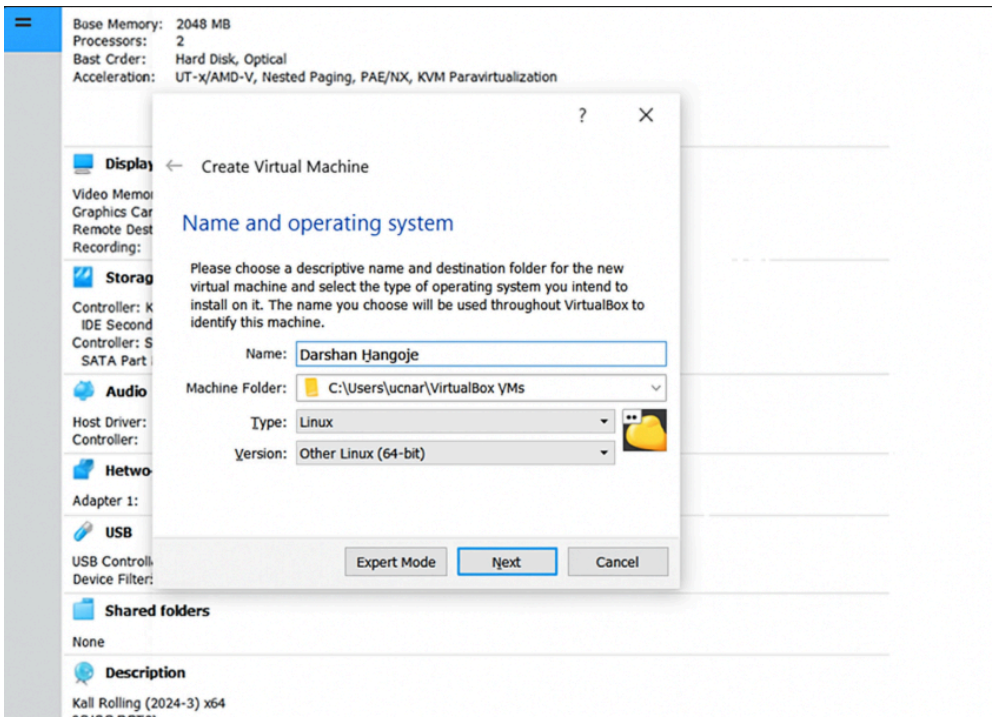
Used Tool	Purpose
Oracle VirtualBox	To create isolated virtual machines for Kali Linux and Metasploitable.
Kali Linux	Main operating system used for penetration testing and security analysis.
Metasploitable2	A purposely vulnerable virtual machine for practicing exploits and vulnerability assessments.
Nmap & Zenmap	Tools for network mapping, port scanning, and operating system detection.

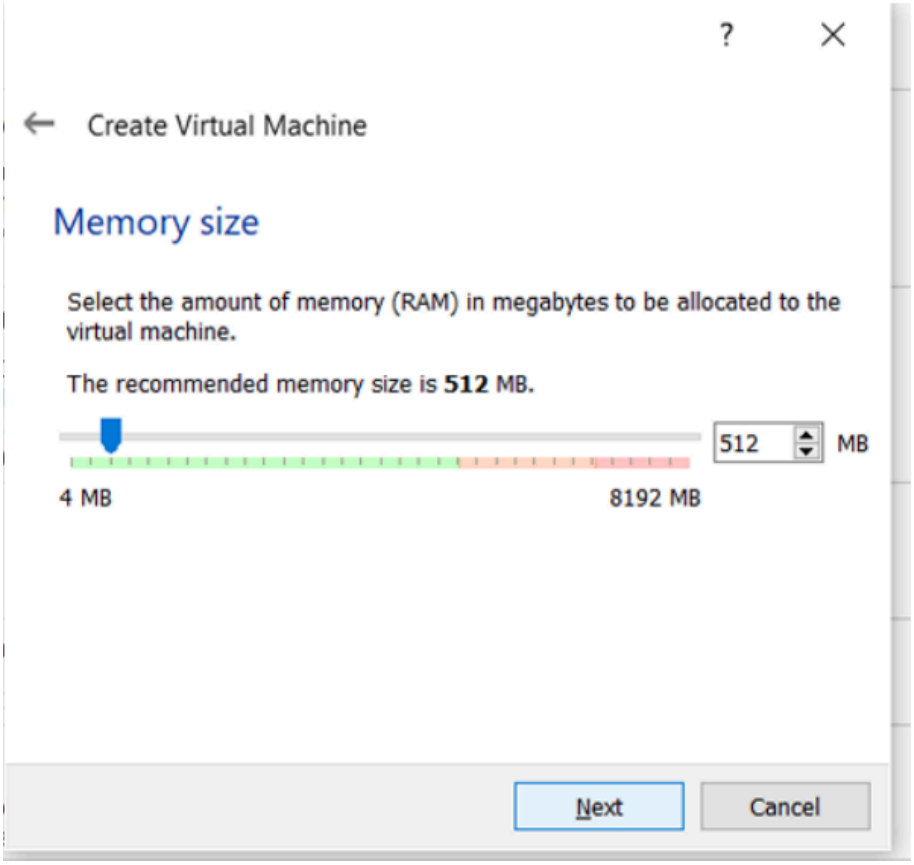
Procedure:

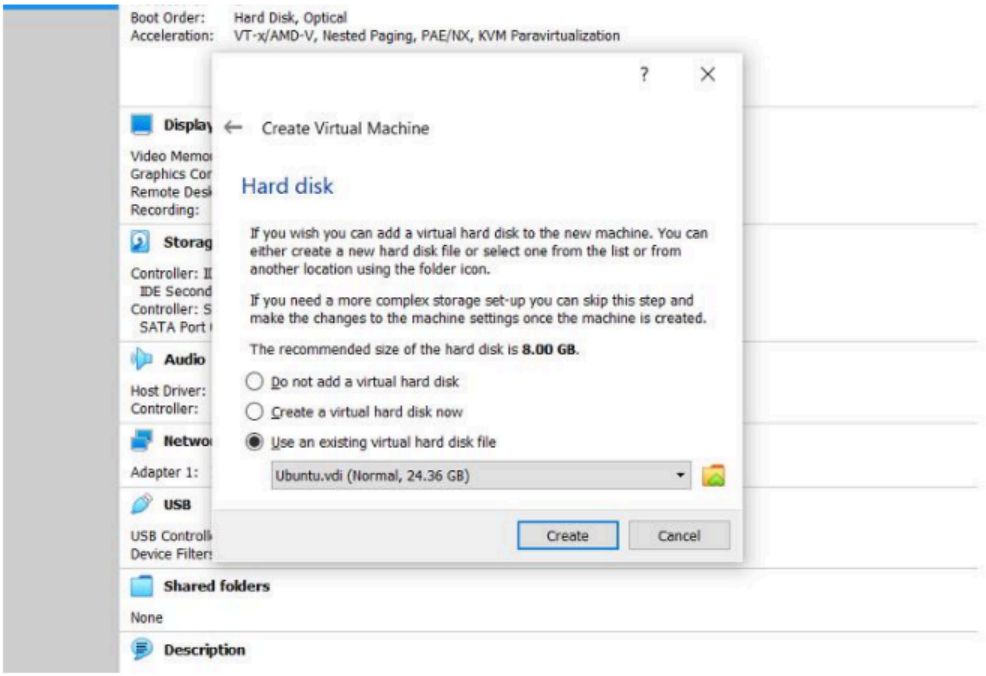
1. Setting Up VirtualBox

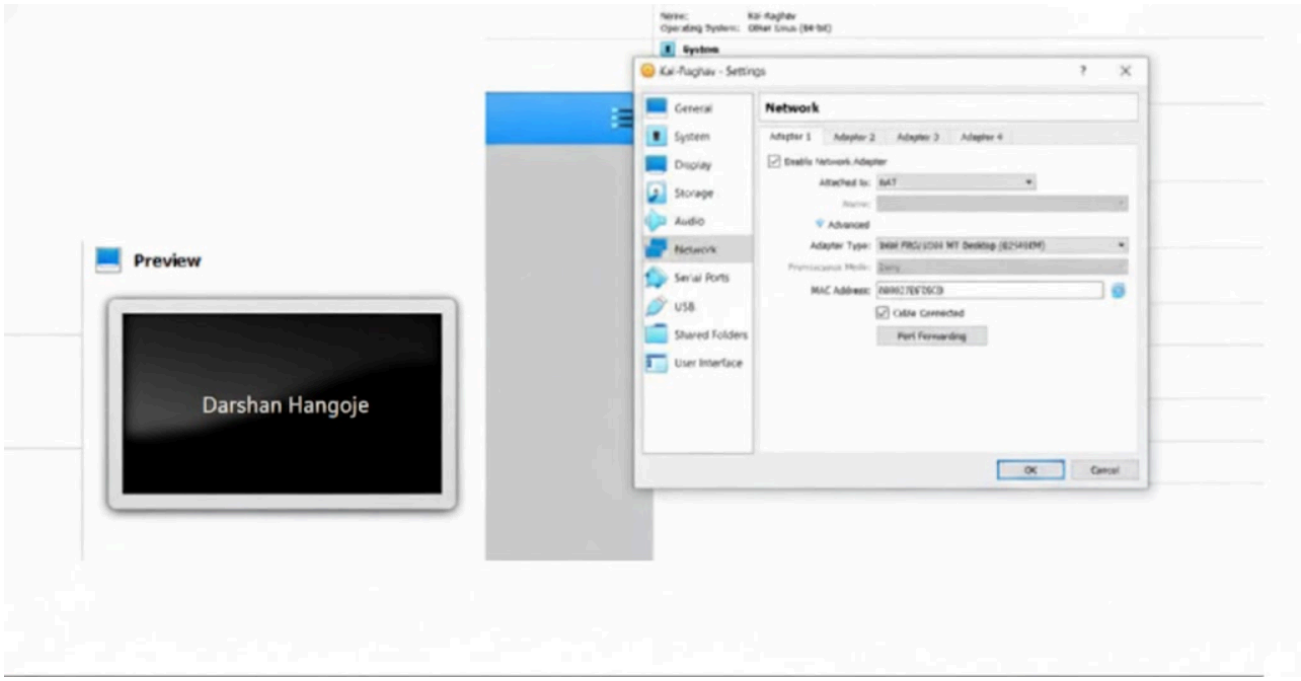
2. Installing Kali Linux

- Downloaded the latest Kali Linux ISO from the Kali website.
- In VirtualBox, selected “New”, provided the VM name, and attached the ISO file as boot media.
- Followed on-screen steps to install Kali Linux. Used credentials during setup (e.g., username: kali, password: kali).

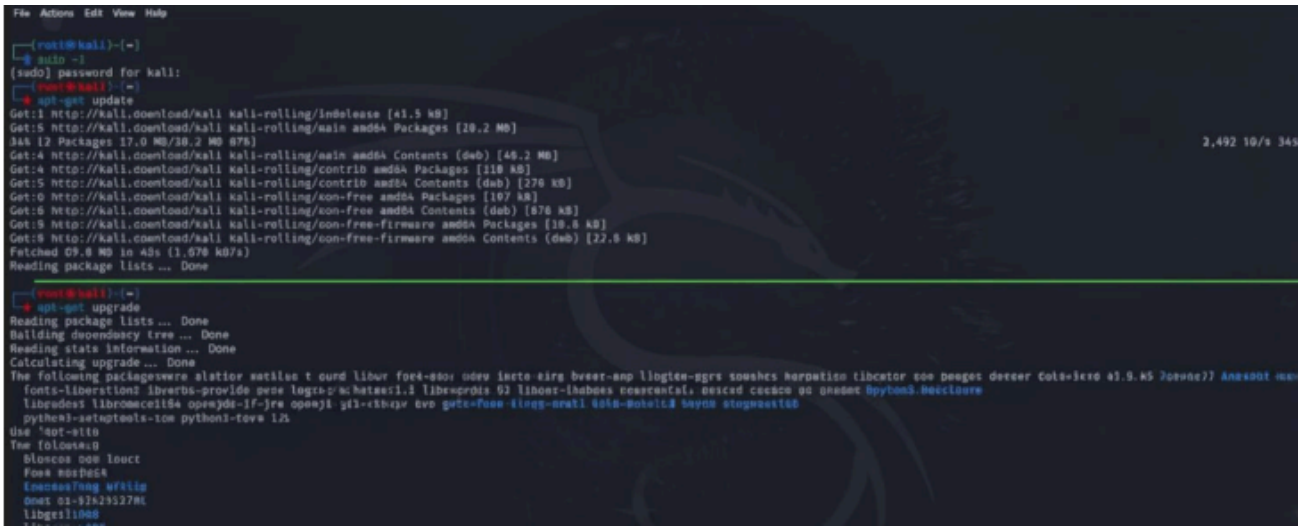

Base Memory: 2048 MB
Processors: 2
Bast Crder: Hard Disk, Optical
Acceleration: UT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization
Create Virtual Machine
Name and operating system
Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.
Name: Darshan Hangoje
Machine Folder: C:\Users\ucnar\VirtualBox VMs
Type: Linux
Version: Other Linux (64-bit)
Expert Mode
Next
Cancel
Shared folders
None
Description
Kali Rolling (2024-3) x64


Create Virtual Machine
Memory size
Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.
The recommended memory size is 512 MB.
512
MB
4 MB
8192 MB
Next
Cancel

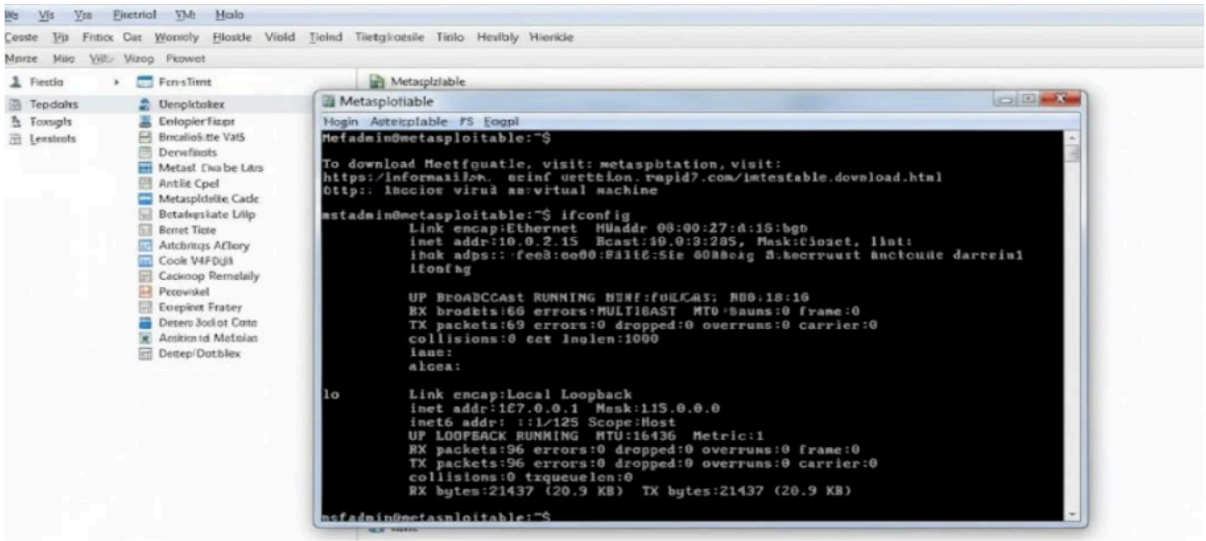

Boot Order: Hard Disk, Optical
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization
Create Virtual Machine
Hard disk
If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.
If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.
The recommended size of the hard disk is 8.00 GB.
Do not add a virtual hard disk
Create a virtual hard disk now
Use an existing virtual hard disk file
Ubuntu.vdi (Normal, 24.36 GB)
Create
Cancel
Audio
USB
Shared folders
None
Description


Preview
Darshan Hangoje
Kai-Raghav - Settings
Network
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
OK
Cancel

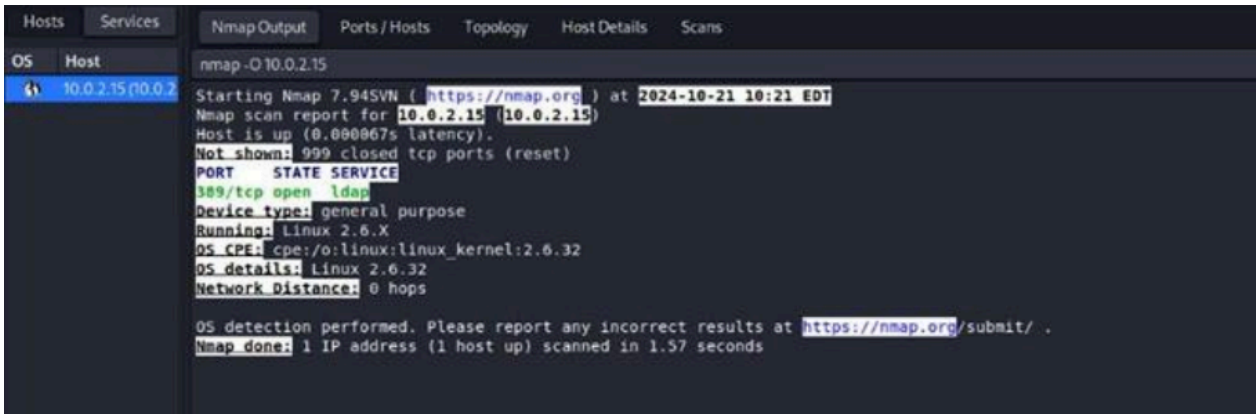
3. Updating Kali Linux



4.Setting Up Metasploitable



5. Information Gathering using Nmap and Zenmap

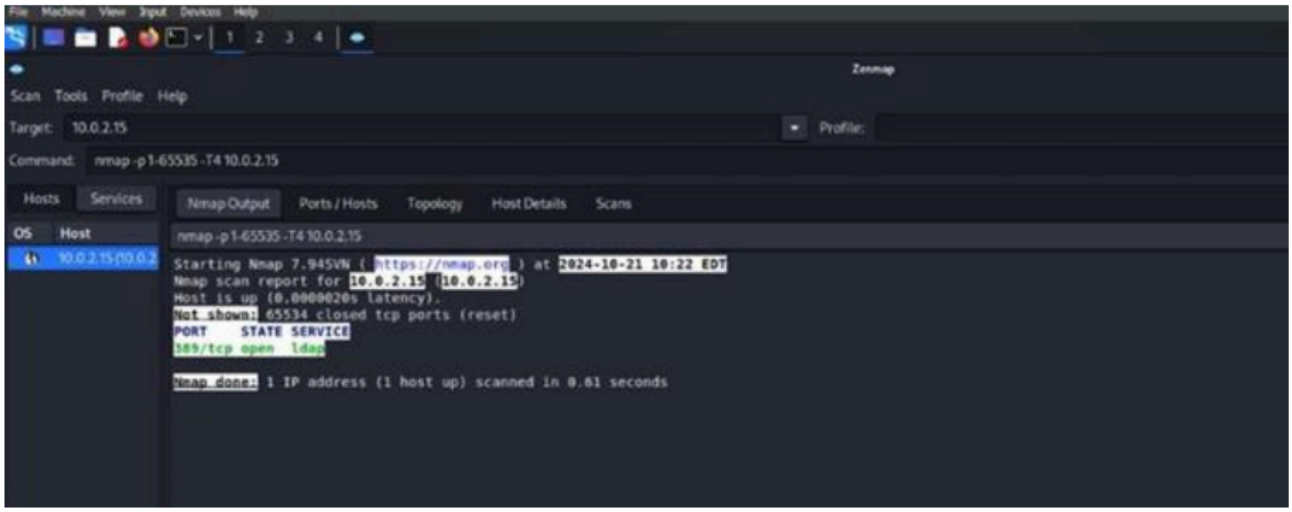


Understanding the Scans Operating System Detection

- Purpose: Identify the OS and version running on the target.
- How it Works: Nmap sends crafted packets to the host and matches responses with its OS fingerprint database.
- Importance: Helps in determining known vulnerabilities specific to that os

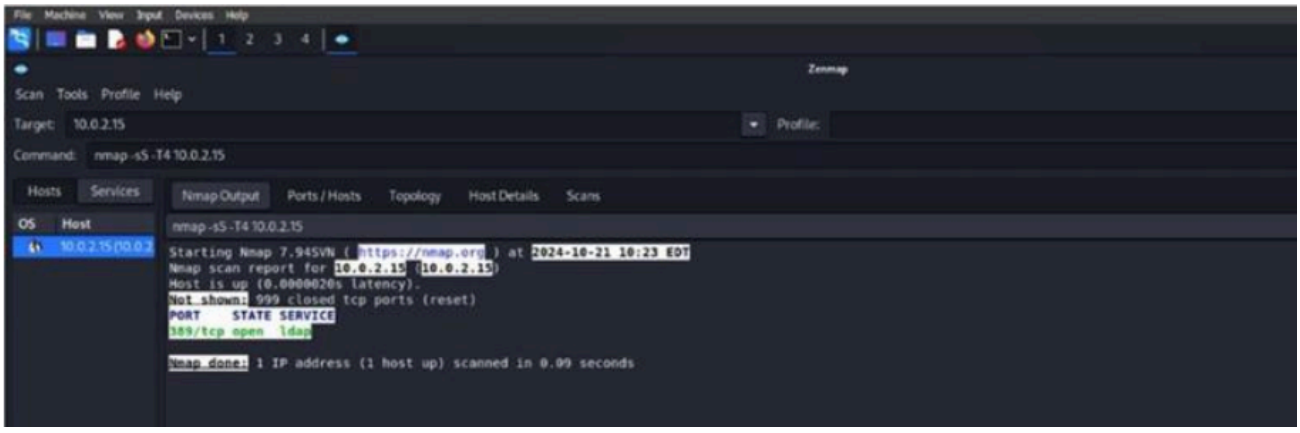
Full TCP Port Scan

- Purpose: Examine all 65,535 TCP ports to find active services.
- How it Works: Nmap sends SYN requests to every port and listens for responses.
- Benefit: Reveals open or misconfigured services that could be exploited.



Stealth Scan (SYN Scan)

- Purpose: Detect open ports without completing a full TCP handshake, minimizing detection.
- How it Works: Sends SYN → receives SYN-ACK → responds with RST instead of ACK.
- Use Case: Effective for silent reconnaissance during penetration testing.



Conclusion

In this lab, we successfully:

- Installed Kali Linux and Metasploitable in VirtualBox.
- Performed network reconnaissance using Nmap and Zenmap.
- Understood how to gather OS, port, and service-level data for security analysis.

This practical exercise provided a foundational understanding of ethical hacking methodologies, focusing on the reconnaissance phase of penetration testing.