

# **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.

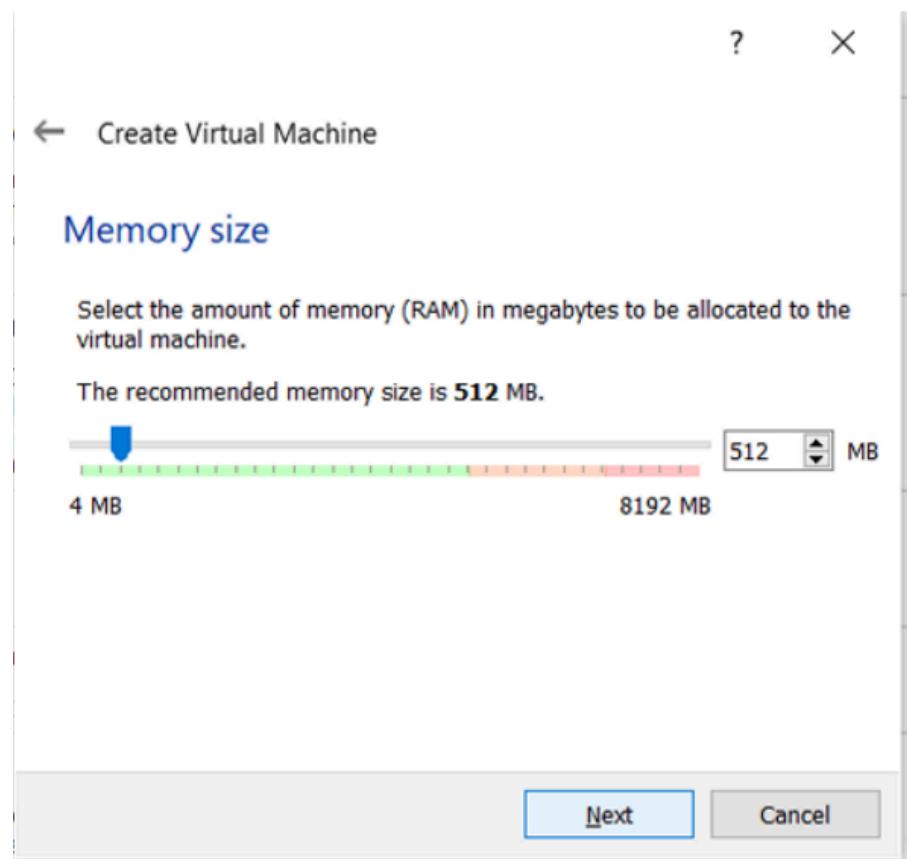
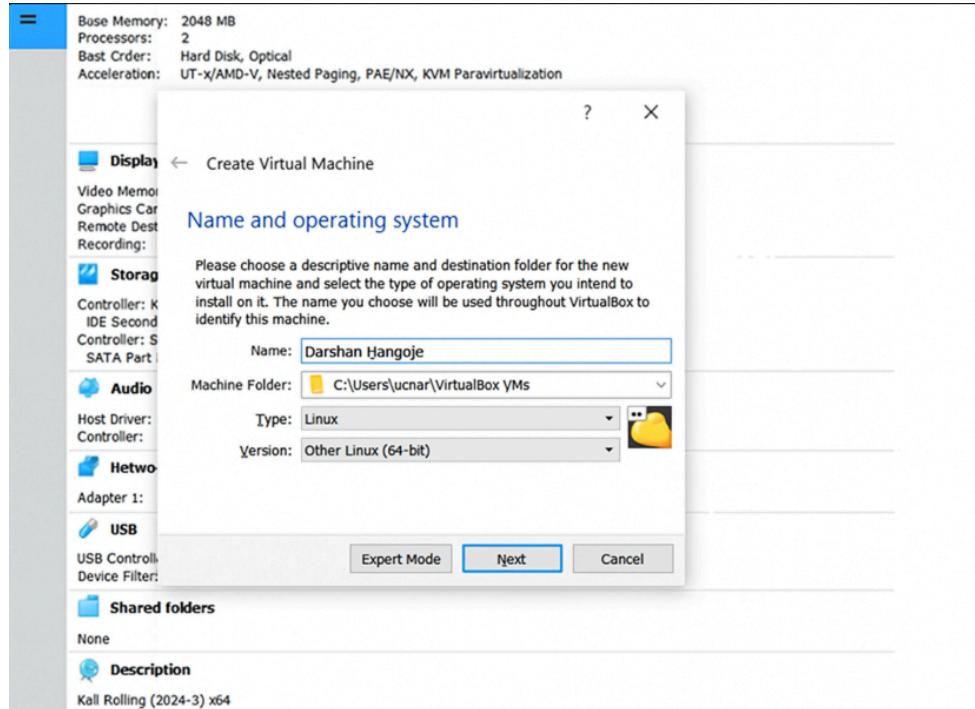
## Procedure:

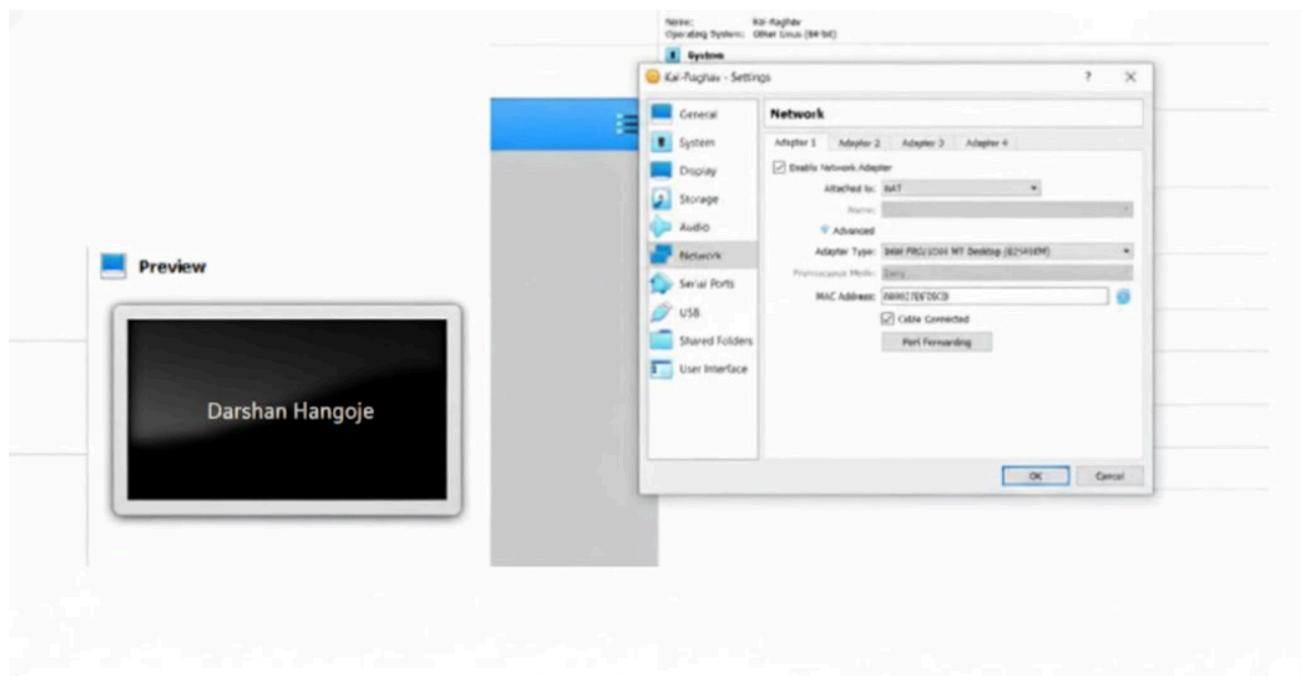
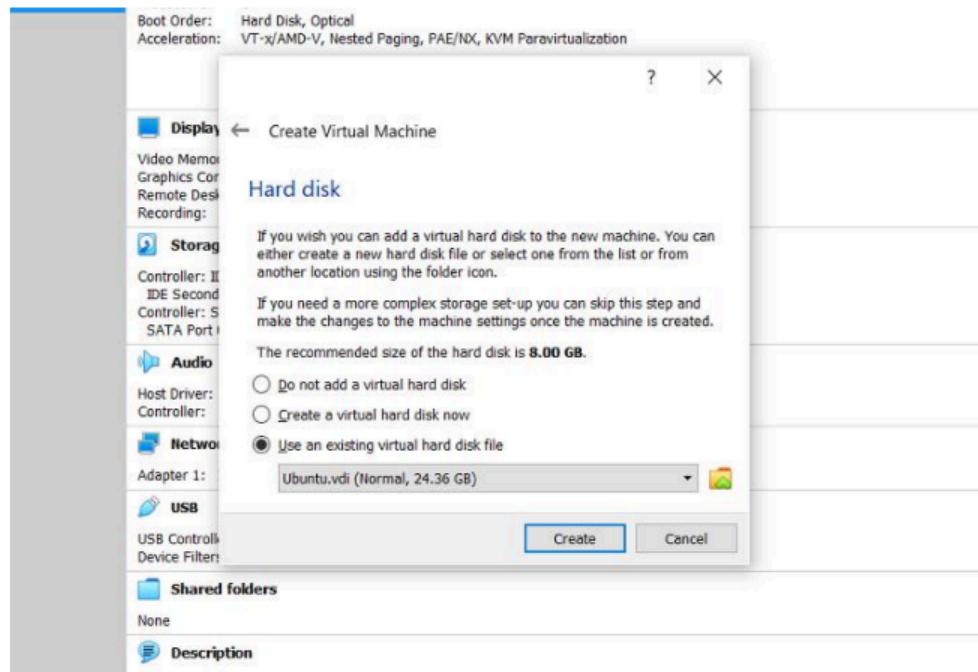
### 1. Setting Up VirtualBox



### 2. Installing Kali Linux

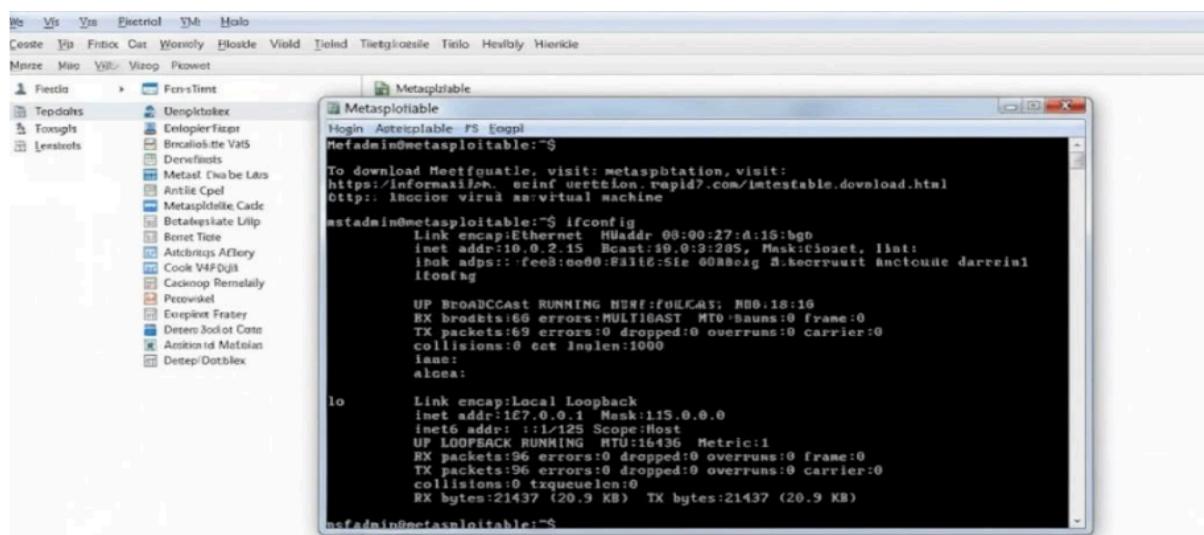
- Downloaded the latest Kali Linux ISO from the Kali website.
- In VirtualBox, selected “New”, provided the VM name, and attached the ISO file as boot media.
- Followed on-screen steps to install Kali Linux. Used credentials during setup (e.g., username: kali, password: kali).





### 3. Updating Kali Linux

## 4. Setting Up Metasploitable



## 5. Information Gathering using Nmap and Zenmap

```
(kali㉿kali)-[~]
$ sudo apt install zenmap

[sudo] password for kali:
zenmap is already the newest version (7.94+git20230807.3be01efb1+dfsg-4kali2).
zenmap set to manually installed.
The following packages were automatically installed and are no longer required:
  fonts-liberation2      libgtk2.0-common    libqt6opengl6t64    python3-diskcache
  freerdp2-x11          libibusverbs1       libqt6openglwidgets6t64  python3-hatch-vcs
  hydra-gtk              libimobiledevice6   libqt6printsupport6t64  python3-hatching
  ibverbs-providers     libiniparser1      libqt6sql6t64      python3-jose
  libarmadillo12         libjim0.82t64       libqt6test6t64     python3-lib2to3
  libassuan0             libjsoncpp25      libqt6widgets6t64   python3-mistune0
  libavformat60          libjxl0.7        libqt6xml6t64     python3-pathspec
  libboost-iostreams1.83.0 libluas5.2-0       librados2          python3-pendulum
  libboost-thread1.83.0  libmfx1           librav1e0          python3-pluggy
  libcephfs2             libmimalloc2.0     librdmacm1t64     python3-pytzdata
  libdaxctl1             libndctl6          libre2-10         python3-rsa
  libfreerdp-client2-2t64 libnghttp3-3       libroc0.3         python3-setuptools-scim
  libfreerdp2-2t64       libplacebo338     libssh-gcrypt-4   python3-time-machine
  libgail-common          libplist3          libsvtavenc1d1   python3-trove-classifiers
  libgail18t64            libpmem1          libswscale7       python3.11
  libgdal34t64            libpoppler134     libu2f-udev       python3.11-dev
  libgeos3.12.1t64        libpostproc57    libusbmuxd6      python3.11-minimal
  libgfapi0               libpython3.11-dev   libwinpr2-2t64   rwho
  libgfpc0                libpython3.11-minimal libwireshark17t64 rwhod
  libgwdxdr0               libpython3.11-stdlib  libwirerapi4t64  samba-ad-provision
  libglusterfs0            libpython3.11t64    libwsutil15t64   samba-dsdb-modules
  libgspell-1-2             libqt6dbus6t64   libx265-199     samba-vfs-modules
  libgtk2.0-0t64            libqt6gui6t64     openjdk-17-jre
  libgtk2.0-bin             libqt6network6t64  openjdk-17-jre-headless
Use 'sudo apt autoremove' to remove them.

Summary:
 Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0

(kali㉿kali)-[~]
```

The screenshot shows the Zenmap interface with the following details:

- Hosts:** Shows a single host entry: 10.0.2.15 (0.0.0.2).
- Services:** Shows the Nmap Output tab.
- Nmap Output:** Displays the command used (nmap -O 10.0.2.15) and the scan report.

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-21 10:21 EDT
Nmap scan report for 10.0.2.15 (10.0.2.15)
Host is up (0.000067s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
389/tcp    open  ldap
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops

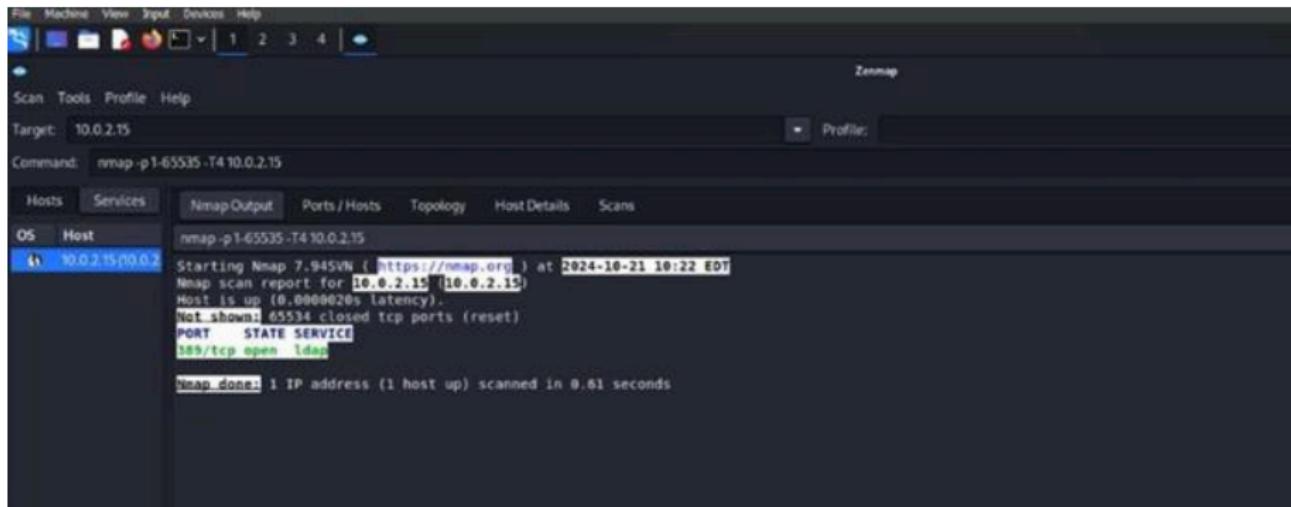
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.57 seconds
```

## 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.

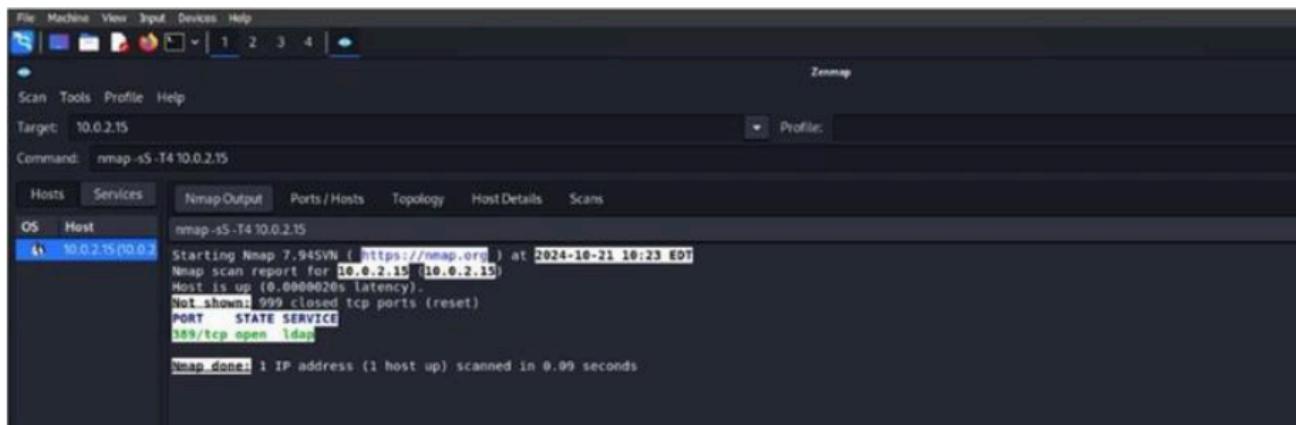


```
File Machine View Input Devices Help
Scan Tools Profile Help
Target: 10.0.2.15
Command: nmap -p1-65535 -T4 10.0.2.15
Hosts Services NmapOutput Ports / Hosts Topology Host Details Scans
OS Host
10.0.2.15(10.0.2.15)
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-21 10:22 EDT
Nmap scan report for 10.0.2.15 (10.0.2.15)
Host is up (0.0000020s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE
389/tcp    open  ldap

Nmap done: 1 IP address (1 host up) scanned in 8.61 seconds
```

## 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.



```
File Machine View Input Devices Help
Scan Tools Profile Help
Target: 10.0.2.15
Command: nmap -sS -T4 10.0.2.15
Hosts Services NmapOutput Ports / Hosts Topology Host Details Scans
OS Host
10.0.2.15(10.0.2.15)
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-21 10:23 EDT
Nmap scan report for 10.0.2.15 (10.0.2.15)
Host is up (0.0000020s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
389/tcp    open  ldap

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

## 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.