University of Engineering and Technology

Department of Computer Science

CS-364 Information Security

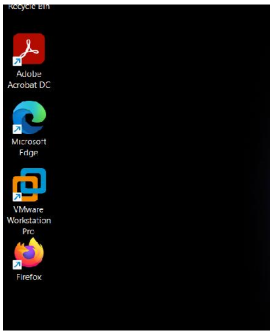
MANUAL

***Disclaimer**: All the labs in this course are prepared for educational purposes. we can't harm anyone all the commands are done within our own system and network.*

TASK 1: Introduction, Downloading & Installation of Kali Linux

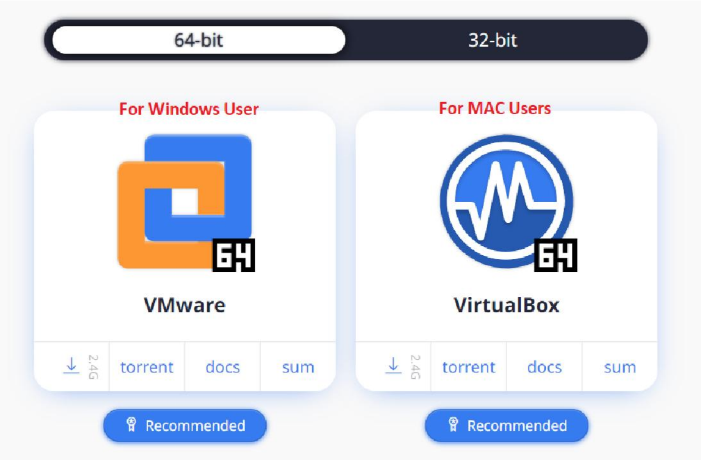
Steps:

a. Download and Install VMWorkstation 16 on your windows machine.



b. If you are a MAC user install Oracle Virtual Box.

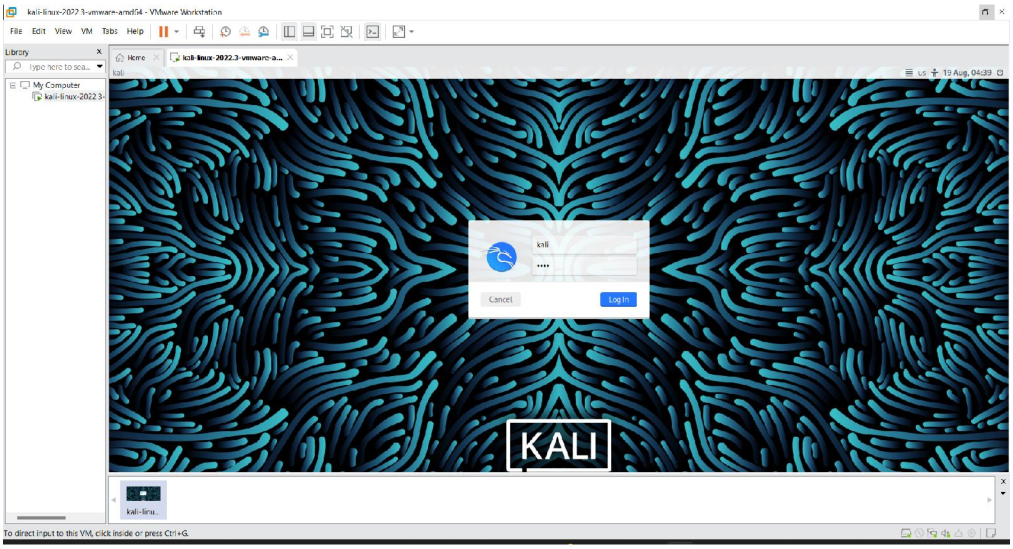
c. Download Kali VM from the above folder or download from kali official website https://www.kali.org/get-kali/#kali-virtual-machines



d. Use winrar to unzip kali file.

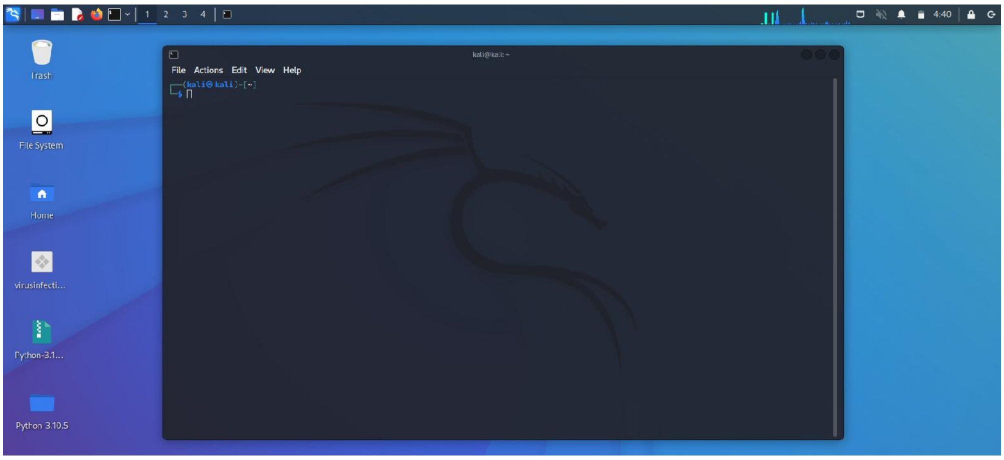
e. Open VMware Workstation. In the Home Tab -> click on Open a virtual machine. It will ask for path to kali. Select the kali VM from the folder.

f. And click on “Power On this Virtual Machine”. Once loaded use “kali” as username and password.


kali-linux-2022.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
kali-linux-2022.3-
Home
kali-linux-2022.3-vmware-a...
kali
19 Aug, 04:39
Cancel
Log In
KALI
kali-linu...
To direct input to this VM, click inside or press Ctrl+G.

kali

••••



```
┌──(kali㉿kali)-[~]
└─$ ▯
```

g. **<u>For MAC Users:</u>** https://www.youtube.com/watch?v=U2nzRtDVknk

h. Introduction to Kali environment and tools.

***************Kali Linux Successfully Installed***********

TASK 2: Understanding Threats, Vulnerabilities, Threat Agents, and Assets Using Kali Linux

Objective: Explore and understand the concepts of threats, vulnerabilities, threat agents, and assets through practical tasks using tools available in Kali Linux.

Lab Activities

Part 1: Identifying Assets

1. **Objective**: Learn to identify and categorize assets within a system.
2. **Steps**:
   - Open the terminal in Kali Linux.
   - Use the `ls` and `df` commands to explore files, folders, and system storage:

     ```
     bash
     CopyEdit
     ls -l
     df -h
     ```

   - Categorize assets into types:
     - Physical assets (e.g., hardware, servers).
     - Digital assets (e.g., files, databases).
     - People (e.g., users with sensitive information).
   - Use the following command to identify running services (potential assets):

     ```
     bash
     CopyEdit
     netstat -tuln
     ```

3. **Documentation**:
   - Document a list of critical assets in the system (e.g., sensitive files, running services).

Part 2: Identifying Vulnerabilities

1. **Objective**: Use vulnerability scanning tools to find system weaknesses.
2. **Steps**:
   - Open the terminal and start **Nmap** to perform a basic scan:

     ```
     bash
     CopyEdit
     nmap -sV <target-IP>
     ```

     Replace `<target-IP>` with the IP of your target system.

  - Use **OpenVAS** for a detailed vulnerability scan:
    - Start OpenVAS using:

      ```
      bash
      CopyEdit
      gvm-start
      ```

    - Access the OpenVAS interface in your browser: `https://127.0.0.1:9392.`
    - Scan your system for known vulnerabilities.
  - Analyze the output to identify open ports, outdated services, and weak configurations.

3. **Documentation**:
   - Document at least three vulnerabilities found in your system.

Part 3: Exploring Threat Agents

1. **Objective**: Simulate and analyze potential threat agents using Kali Linux tools.
2. **Steps**:
   - Use **Metasploit Framework** to simulate an attacker attempting to exploit a vulnerability:
     - Start Metasploit:

       ```
       bash
       CopyEdit
       msfconsole
       ```

     - Search for an exploit based on a service detected in Part 2:

       ```
       bash
       CopyEdit
       search <service-name>
       ```

     - Configure the exploit:

       ```
       bash
       CopyEdit
       use <exploit-path>
       set RHOSTS <target-IP>
       set PAYLOAD <payload-name>
       exploit
       ```

   - Use **Hydra** to simulate a brute force attack on a login service:

     ```
     bash
     CopyEdit
     hydra -l <username> -P <password-list> <target-IP> ssh
     ```

     Replace `<username>`, `<password-list>`, and `<target-IP>` accordingly.

3. **Documentation**:

    - Record observations on the effectiveness of the simulated threat agents.

Part 4: Understanding Threats to Assets

1. **Objective**: Map vulnerabilities and threat agents to potential threats.
2. **Steps**:
    - Review the vulnerabilities discovered in Part 2 and the actions of threat agents in Part 3.
    - Map each vulnerability to a potential threat, such as data theft, service disruption, or unauthorized access.
3. **Documentation**:
    - Create a table mapping assets, vulnerabilities, threats, and associated threat agents.

Home Tasks for Students

Task 1: Asset Classification

- Identify and classify the assets within your personal or organizational system.
- Use tools such as `ls`, `df`, and `netstat` to gather information.
- Submit a document categorizing these assets into:
    - Critical assets.
    - Non-critical assets.

Task 2: Vulnerability Research

- Choose one vulnerability identified during the lab session.
- Research online to find its:
    - Common Vulnerabilities and Exposures (CVE) ID.
    - Severity score using CVSS (Common Vulnerability Scoring System).
    - Possible mitigation strategies.
- Write a brief report summarizing your findings.

Task 3: Threat Simulation Practice

- Simulate a different type of threat using any Kali Linux tool not covered in the lab (e.g., Wireshark for sniffing or Nikto for web server scanning).
- Document:
    - The tool used.
    - The process followed.
    - Observations and results.

Task 4: Case Study Analysis

- Research a real-world cyberattack (e.g., ransomware or phishing).
- Identify:
  - The assets targeted.
  - The vulnerabilities exploited.
  - The threat agents involved.
  - The impact on the organization.
- Prepare a 1-2 page summary for class discussion.

Expected Deliverables

1. Reports for each task completed with clear documentation.
2. Screenshots to validate the steps performed.
3. Submission before the next lab session for review.