**Tasks**

### Task 1: Basic Cybersecurity Concepts

* **What is CyberSecurity?**

**Cybersecurity** is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It encompasses a wide range of practices, tools, and concepts that protect the confidentiality, integrity, and availability of information.

* **The CIA Triad – Core Principles of Cybersecurity**

The CIA triad is a foundational model in information security that guides the development of policies and procedures to protect data. Comprising **Confidentiality**, **Integrity**, and **Availability**, the triad ensures that sensitive information remains secure, accurate, and accessible when needed. By emphasizing these three core principles, the CIA triad serves as a critical framework for safeguarding systems and defending against cyber threats.

**CIA stands for:**

* **Confidentiality**
* **Integrity**
* **Availability**

### ****Common Types of Cyber Attacks****

#### ****Phishing****

* Fraudulent attempts to trick users into revealing personal or financial information.
* Delivered via email, SMS, or fake websites.
* **Countermeasures**: Email filters, user training, MFA.

#### ****Malware (Malicious Software)****

* Software designed to disrupt, damage, or gain unauthorized access.
* Includes viruses, worms, ransomware, spyware, etc.
* **Countermeasures**: Antivirus, endpoint protection, patching.

#### ****SQL Injection (SQLi)****

* An attack where malicious SQL code is inserted into input fields to gain access to databases.
* **Example**: Bypassing login forms to access admin data.
* **Prevention**: Use parameterized queries and input validation.

#### ****Cross-Site Scripting (XSS)****

* Malicious scripts are injected into web pages viewed by other users.
* Can steal cookies or perform actions on behalf of users.
* **Prevention**: Sanitize inputs, Content Security Policy (CSP).

#### ****Denial-of-Service (DoS/DDoS)****

* Overwhelms a system or network to make it unavailable.
* DDoS involves multiple systems (botnet).
* **Mitigation**: Rate limiting, firewalls, cloud-based DDoS protection.

#### ****Man-in-the-Middle (MitM)****

* Attacker intercepts communication between two parties.
* **Example**: Eavesdropping on public Wi-Fi.
* **Prevention**: Use HTTPS, VPNs, encrypted protocols.

### ****Cybersecurity Defense Mechanisms****

#### ****Firewalls****

* Act as barriers between trusted and untrusted networks.
* Filter traffic based on rules.

#### ****Antivirus / Anti-malware****

* Detect and remove known malware from systems.
* Often includes real-time scanning.

#### ****IDS/IPS (Intrusion Detection/Prevention Systems)****

* IDS: Monitors for suspicious activity and alerts.
* IPS: Monitors and blocks suspicious traffic in real-time.
* **Patch Management**
* Keeping all systems and software updated.
* Prevents exploitation of known vulnerabilities.
* **Access Control**
* Restricts access based on role or necessity (RBAC, ABAC).
* Includes MFA, password policies.
* **Backup and Recovery**
* Regular backups ensure data can be restored after an incident.
* **Common Cybersecurity Tools**
* **Wireshark**

A powerful network protocol analyzer that captures and displays packets in real time. It's commonly used for network troubleshooting, protocol development, and educational purposes.

* **Burp Suite**

A web vulnerability scanner and proxy tool. It allows penetration testers to intercept, modify, and replay web traffic to discover vulnerabilities like XSS and SQL injection.

* **Nmap**

A network scanning tool used to discover hosts and services on a network. It’s useful for port scanning, vulnerability scanning, and network inventory.

* **Metasploit Framework**

A penetration testing platform that helps in developing and executing exploit code against remote systems. It contains a vast library of exploits, payloads, and post-exploitation tools.

* **Nikto**

A web server vulnerability scanner that checks for outdated software, misconfigurations, and common security issues across HTTP services.

* **John the Ripper**

A password cracking tool that identifies weak passwords using dictionary attacks, brute force, and various cryptanalysis techniques.

### ****Cybersecurity Best Practices****

* Use strong and unique passwords for all accounts
* Enable **Multi-Factor Authentication (MFA)**.
* Regularly update and patch software.
* Back up critical data and store securely (preferably offline/cloud).
* Educate employees and users about cyber hygiene.
* Monitor and audit network logs and user activities.

**Task 2:- Set up a virtual lab (VirtualBox/VMware) with Kali Linux and a vulnerable machine (e.g., OWASP Juice Shop)**

### Required:

* **Hypervisor**: Install [VirtualBox](https://www.virtualbox.org/) or VMware Workstation Player
* **Kali Linux**: Download and import VM from https://www.kali.org/get-kali/
* **Vulnerable App**: OWASP Juice Shop setup:

### ****1. Install Virtualization Software****

Begin by installing VirtualBox (free) or VMware Workstation (paid). This lab uses **VirtualBox** for demonstration:

* **Download** from [VirtualBox.org](https://www.virtualbox.org/) and follow the default installation steps.

### ****2. Set Up Kali Linux Virtual Machine****

**Download Kali Linux ISO**

**https://www.kali.org**

Visit the Kali Linux Download Page and select the **64-bit ISO**.

**Create a New VM in VirtualBox**

* Open **VirtualBox** and click **New**.
* Name the VM (e.g., **"Kali Linux"**), set **Type** to **Linux**, and **Version** to **Debian (64-bit)**.
* Allocate **2+ GB RAM** and **1+ CPU core**.
* Create a **25+ GB dynamically allocated** virtual hard disk.

### ****3. Post-Installation Setup****

**Update Kali**

* Open a **terminal** in Kali Linux.
* Run the following commands to update the system:

sudo apt update

sudo apt upgrade –y

### ****4.Set Up OWASP Juice Shop (Vulnerable Machine)****

**Using Docker (Recommended)**

**Pull the Juice Shop Docker image**

* Open a **terminal** in Kali Linux.
* Run the following command to download the OWASP Juice Shop image:
* **Docker Installation in Kali:**

sudo apt install docker.io -y

sudo systemctl start docker

sudo systemctl enable docker

* **Run OWASP Juice Shop:**

sudo docker run -d -p 3000:3000 bkimminich/juice-shop

* **Access Juice Shop in Browser:**

<http://127.0.0.1:3000>

### Task 3: Install Necessary Tools

**Wireshark:**

sudo apt install wireshark -y

sudo usermod -aG wireshark $USER

**Burp Suite:**

Pre-installed in Kali. Launch with:

Burpsuite

**Other Tools Installed:**

**Nmap**

**Nikto**

**Metaspoilt**

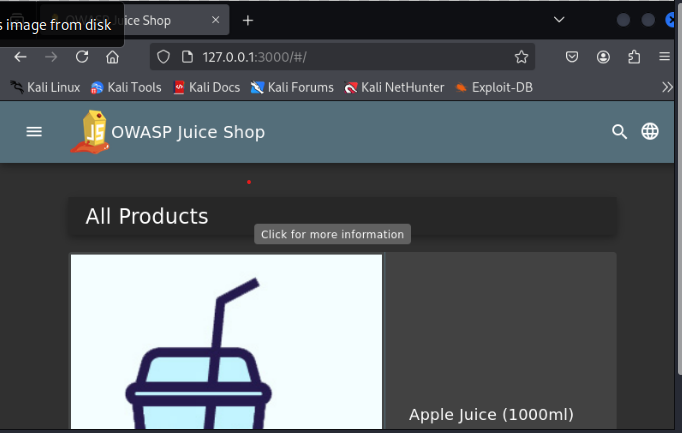
sudo apt install nmap nikto metasploit-framework –y

**Task 5: Screenshots to Include**

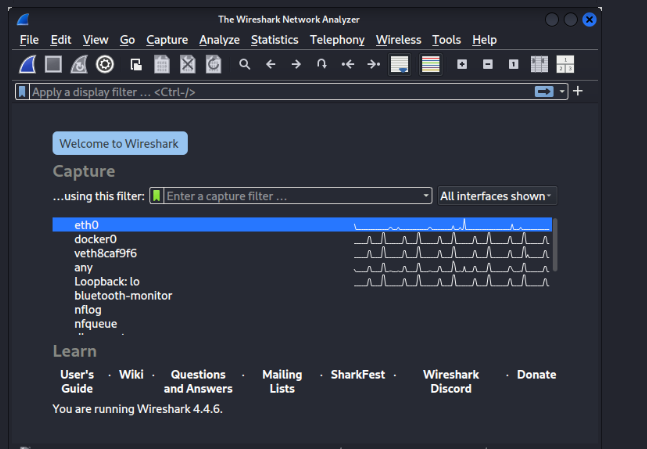
**1.Kali Linux Desktop Screenshot**



2. **OWASP Juice Shop in Browser**

****

3. **Wireshark Running**

****

4. **Burp Suite Running**

****

**\*\*\*\*\*\*\*\* “Stay Alert, Stay Secure.”\*\*\*\*\*\*\***