**Technology Stack :**

**In this project, we explored various cybersecurity tools to understand threats and solutions in the digital age:**

**1. Web Technologies :**

What it is: These are websites or services you use online, like online banking, social media, or e-commerce sites.

Threats: Hackers might trick the site into giving away or changing information, like stealing login details.

Solutions: Websites can use special tools to check for errors and make sure hackers can't interfere.

**2. Penetration Testing Tools :**

Kali Linux

* What it is: Kali Linux is an operating system (like Windows or Mac) that comes with a bunch of tools already installed for testing security. It's like a toolbox for hackers.
* Why it's used: It helps security experts find and fix vulnerabilities in systems.

Metasploit

* What it is: A tool that lets you test for weaknesses by simulating real hacker attacks. It has pre-built "exploits" (tools that take advantage of weaknesses) that can target different systems.
* Why it's used: Pen testers use it to safely test if a system is vulnerable to known attacks.

Nmap

* What it is: Nmap is a tool that scans networks and finds out which devices are connected, what software they’re running, and which ports are open.
* Why it's used: Pen testers use it to gather information about a network, which helps them figure out potential ways to attack.

Wireshark

* What it is: Wireshark is a network protocol analyzer that can "listen" to the data being sent over a network.
* Why it's used: It helps pen testers see if sensitive data (like passwords) is being sent unencrypted, or if there are any security problems in the data transmission.

**3. Vulnerable Testing Environments :**

Capture the Flag (CTF)

* What it is: A type of game or challenge where participants solve puzzles or find hidden "flags" in a virtual environment. Each flag represents a security vulnerability.
* Why it's used: It helps people practice hacking skills in a safe, competitive environment. It's like an educational puzzle hunt.

Hack The Box

* What it is: A platform where users can practice ethical hacking by attempting to "hack" into virtual machines (computers) set up with intentional security flaws.
* Why it's used: It’s like a virtual training ground for hackers to sharpen their skills and learn about real-world vulnerabilities.

OWASP Juice Shop

* What it is: A purposely vulnerable web application designed to teach about web security. It simulates a store where hackers can try exploiting common web app weaknesses.
* Why it's used: It’s a hands-on way to learn about the security problems in websites and how to fix them.

Damn Vulnerable Web Application (DVWA)

* What it is: A tool used for learning web application security. It contains many flaws that users can exploit to understand how hackers might break into a site.
* Why it's used: It's great for beginners who want to learn about web security and practice using tools to find weaknesses.

Metasploit

* What it is: A virtual machine set up with many security holes that can be used for testing with tools like Metasploit.
* Why it's used: It's used to safely practice hacking techniques, test penetration testing tools, and learn how to defend against attacks.