Information Gathering Challenge

By Inlighn Tech

Objective:

In this task, you will apply your **information gathering skills** to identify and collect as much data as possible about a given target. This is a critical step in any ethical hacking or penetration testing process and forms the foundation for later stages such as vulnerability assessment and exploitation.

Your Mission:

> You are provided with a target (domain or IP address). Your job is to act like a security researcher and gather all publicly available information about this target without performing any unauthorized or intrusive actions.

Target:

1. **Execution Context:** The malicious script runs in the victim's browser, within the security context of the target website.
2. **Attack Vector:** Typically involves injecting JavaScript, but other scripts (e.g., VBScript) or HTML elements can also be used.
3. **Impact:** Can lead to session theft, data leakage, account takeover, phishing, or malware distribution.
4. **Root Cause:** Failure to validate, sanitize, or escape user input before rendering it in the browser.

Your Goals:

Collect and document the following information (as applicable):

1. **Basic Information**

   - Domain/IP details
   - WHOIS information
   - Hosting provider and location

2. **Subdomain Enumeration**
   - Find as many subdomains as possible using tools like `assetfinder`, `Sublist3r`, `amass`, etc.

3. **DNS Information**
   - DNS records (A, MX, NS, TXT)
   - Zone transfer (if possible)

4. **Technology Fingerprinting**
   - Web server, CMS, frameworks
   - Tools: `whatweb`, `Wappalyzer`, `BuiltWith`

5. **Directory and File Discovery**
   - Hidden directories or sensitive files
   - Tools: `dirb`, `dirsearch`, `gobuster`

6. **Open Ports and Services**
   - Identify open ports and associated services
   - Tools: `nmap`, `masscan`

7. **Email Harvesting**
   - Extract emails using tools or search engines

    - Google dorking or `theHarvester`

8. **Social Media and Public Data**

    - Company or target’s online presence

    - Any exposed credentials or sensitive posts

Rules:

- **DO NOT** perform any exploitation or unauthorized access attempts.

- Stick to **passive** and **legal active** information gathering only.

- Respect ethical hacking boundaries.

Submission Guidelines:

- Submit a **report in PDF format** with screenshots and tools used.

- Clearly label each section and include findings with proper explanations.

- Mention any challenges or tools that didn’t work.

Suggested Tools:

- `whois`, `nslookup`, `dig`

- `nmap`, `gobuster`, `amass`

- `whatweb`, `theHarvester`, `subfinder`, `shodan`

- Google Dorking