SKILL HORIZON
NextGen Pvt. Ltd.

CYBER SECURITY INTERNSHIP

ASSIGNMENT 2- PASSIVE RECON

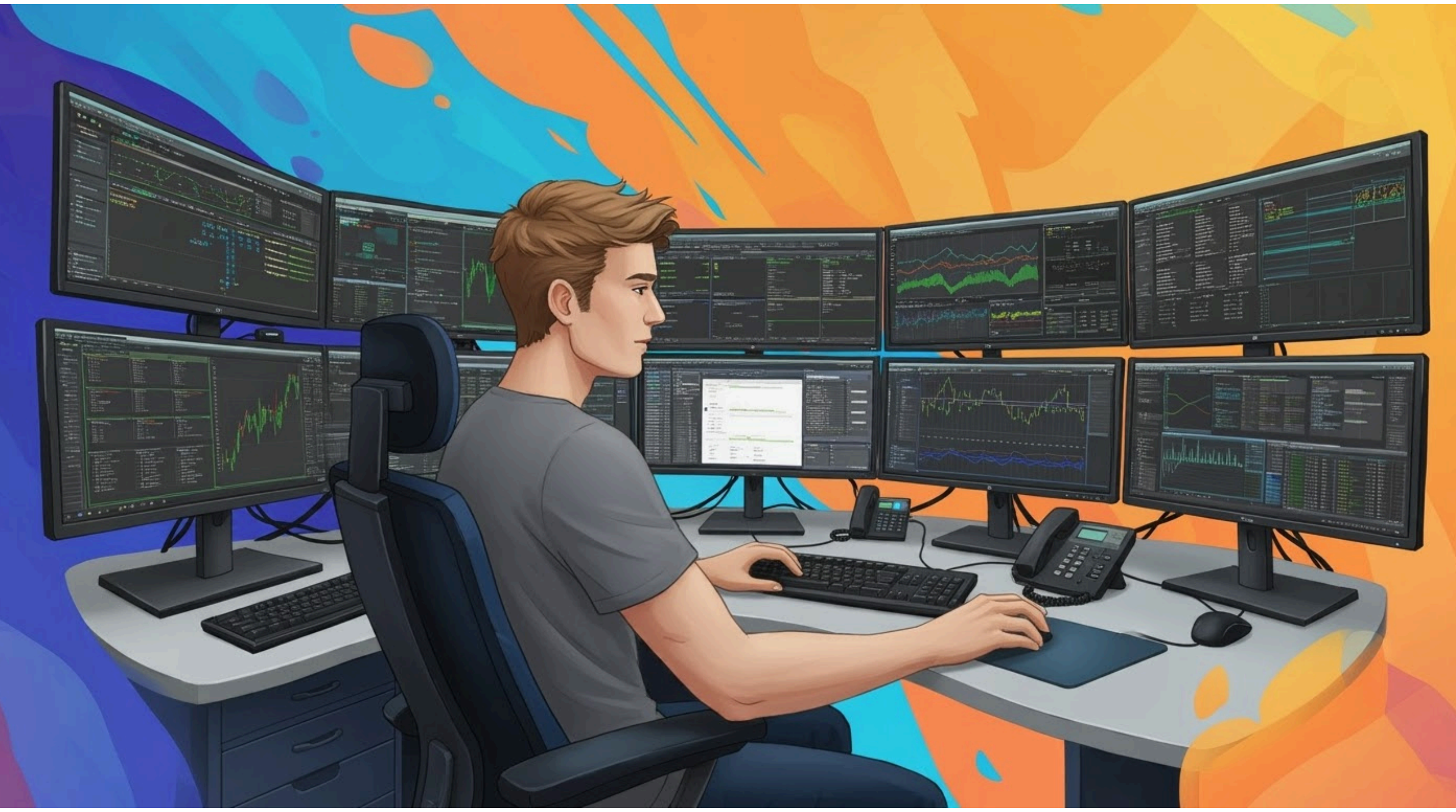
skillhorizon.org.in   Skill Horizon   skill.horizon.edtech   @ZERODAYVAULT

Task Title:

Passive footprinting & Reconnaissance of a web application using Kali Linux Tools

Objective:

You will learn how to gather publicly available information about a target without actively engaging with the target’s systems. This helps in understanding the initial phase of penetration testing and ethical hacking.



Instructions & Scope:

Target Selection

- Choose a **publicly available domain** (e.g., example.com) , make sure you will only pick legal targets like their own domain, test labs, or approved bug bounty targets.
- Avoid personal or unauthorized targets.

Tasks to Perform (Step-wise)

Step 1: Domain Information Gathering

- Use whois to find domain registration details.
- Use dig or nslookup to identify DNS records.
- Tools: whois, dig, nslookup.

Step 2: Subdomain Enumeration

- Perform passive subdomain discovery using tools like:
  - subfinder

        - assetfinder
        - amass (in passive mode)

Step 3: Email & Employee Information

- Use theHarvester to gather emails, names, and hosts from public sources (Google, Bing, LinkedIn, etc.).

Step 4: Metadata Extraction

- Download publicly available documents (PDF, DOCX, PPTX) and analyze metadata.
- Tool: exiftool, strings, metagoofil.

Step 5: Google Dorking

- Use Google search queries to find sensitive information.
- Example:
    - site:example.com filetype:pdf
    - site:example.com intitle:index of

Step 6: Social Media & Open Source Intelligence (OSINT)

- Identify target presence on LinkedIn, Twitter, GitHub, etc.
- Tools: Maltego (community edition), SpiderFoot.

Step 7 : Collect all the urls of the target & filter JS files

Step 8 : Search for possible secrets available in JS files using JSleak

Deliverables:

Each of you should submit a **Passive Recon Report** including:

1. Target domain name chosen.
2. WHOIS & DNS findings.
3. Subdomains discovered.
4. Email IDs or employee data (if found).
5. Metadata information (with screenshots).
6. Google dorks attempted (with results).
7. OSINT summary from social media/public platforms.
8. Urls & leak data in JS files
9. Conclusion: Possible attack surfaces identified from passive recon.

Tools to be Used (Kali Linux):

- whois, dig, nslookup
- subfinder, assetfinder, amass
- theHarvester
- metagoofil, exiftool
- Maltego (CE) / Spiderfoot
- Google Dorking
- gau , katana , linkfinder
- JSleak