CYBER SECURITY INTERNSHIP

ASSIGNMENT 4 - ACTIVE RECON

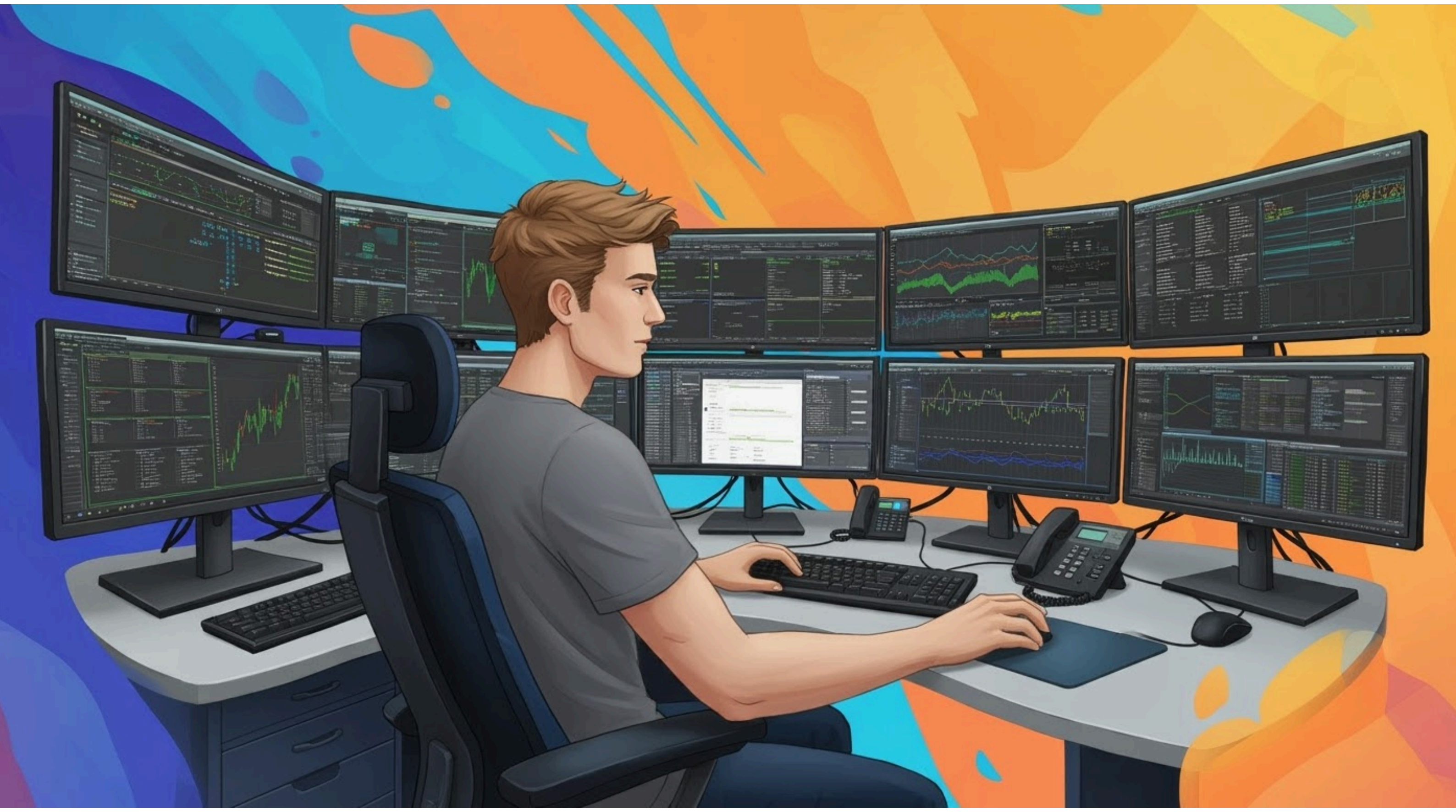
skillhorizon.org.in Skill Horizon skill.horizon.edtech @ZERODAYVAULT

Task Title:

Active Recon & Web Enumeration using Nmap & Directory Brute forcers

Objective:

You will perform controlled, legal active reconnaissance on an approved target to discover live hosts, open ports, running services, OS details, and web application directories/files. The goal is to learn Nmap scanning techniques, HTTP enumeration with Dirb/Gobuster, basic vulnerability discovery (non-exploitative), and professional reporting.



Instructions & Scope:

Important (Rule): Only run this task against targets you *own*, *manage*, or that are explicitly authorized for testing (own lab VM, VulnHub boxes, HackTheBox labs, OWASP Juice Shop, Bugcrowd/HackerOne programs that permit testing). Do **not** scan arbitrary public sites.

Some allowed target for your references

1. testphp.vulnweb.com
2. testfire.net
3. zero.webappsecurity.com

Tasks to Perform (Step-wise)

Step 1 — Host discovery

- Identify if the target is alive and its IP.
- Command-

```
nmap -sn  target.com          # Ping/ARP discovery (no port scan)
```

Step 2: Port & Service Scan using Nmap

- Do staged scans: quick, then deeper.

```
nmap -sS  target.com     # TCP SYN Scan
nmap -sV  -p 22,80,443 -sC target.com   # service/version + default NSE scripts on common ports
```

```
nmap  -sV  -p 1-65535  -sC target.com  #NSE scripts on all ports
```

```
nmap  -sV  -p-  targert.com   #full port scan
```

```
nmap -O --osscan-guess  target.com    # OS detection (if allowed)
```

Step 3: HTTP Enumeration using Dirb

- Brute-force directories & common files.

```
dirb https://target.com
```

```
dirb https://target.com  /usr/share/wordlists/dirb/common.txt
```

Step 4: Web fingerprinting & vulnerability checks using whatweb & nikto

```
whatweb http://target.com
```

```
nikto -h http://target.com  -o nikto.txt
```

Deliverables:

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

1. **Host discovery** results (IPs, alive/not).
2. **Nmap outputs** (include screenshots/important snippets).
3. **Open ports & services** with version info and confidence level.
4. **NSE scripts used** and findings (explain each result).
5. **HTTP enumeration** results (dirb output — list discovered directories/files).
6. **Web fingerprinting** (whatweb, nikto)

.Tools to be Used (Kali Linux):

Nmap , dirb , nikto , whatweb