OSINT (Open Source Intelligence)

🛠️ 1. theHarvester

Purpose: Gather emails, IPs, hostnames, and subdomains from public sources.

✅ Install:

```
bash
CopyEdit
sudo apt install theharvester
```

✅ Usage:

```
bash
CopyEdit
theHarvester -d example.com -b google
```

🔎 Replace `example.com` with a real domain (e.g., `emkei.cz`, `kplc.co.ke`).

✅ Flags:

- `-d`: target domain
- `-b`: source (google, bing, yahoo, etc.)
- `-l`: limit number of results
- `-f`: save to HTML

📥 Example:

```
bash
CopyEdit
theHarvester -d kplc.co.ke -b google -l 50
```

🛠️ 2. Recon-ng

Purpose: OSINT Framework for modular information gathering.

✅ Start:

```
bash
CopyEdit
recon-ng
```

✅ Basic Flow:

```
bash
CopyEdit
> workspaces create osintlab
> marketplace install recon/domains-hosts/bing_domain_web
> modules load recon/domains-hosts/bing_domain_web
```

```
> options set SOURCE example.com
> run
```

💡 Tip:

Use `show options` and `help` for guidance within modules.

🔎 Replace `example.com` with a domain you're investigating.

🛠️ 3. Shodan.io

Purpose: Search for exposed services/devices on the internet.

✅ Website:

Go to: https://www.shodan.io

✅ Create a free account for full access.

🔍 Search Queries:

- `port:22 country:KE`
- `apache`
- `cisco`
- `org:"Kenya Power"`
- Your lab IP: e.g. `197.248.X.X`

✅ What to look for:

- Devices: routers, webcams, printers
- Services: FTP, SSH, HTTP
- Version info and vulnerabilities