**🕵️‍♂️ OSINT Labs – Beginner-Friendly Notes**

**📚 What is OSINT?**

**OSINT** = Open-Source Intelligence

It means collecting information from **public sources** (not hacking!) to investigate people, companies, networks, or behaviors.

**🧩 PART 1: Using Neo4j + OffshoreLeaks, Paradise Papers**

**🛠️ Tools Covered:**

* **Neo4j**: A graph database — great for visualizing links between people, companies, emails, and locations.
* **OffshoreLeaks / Paradise Papers**: Huge leak databases exposing **secret offshore companies**, tax avoidance, and corruption.

**🧪 Why Use These in OSINT Labs?**

* Investigate **Pakistani companies** or individuals linked to offshore entities.
* Identify suspicious connections: same email, same address, fake company.
* Learn real-world corporate fraud detection.

**💡 Step-by-Step (Neo4j + OffshoreLeaks)**

**1. Go to:**

🌐 <https://offshoreleaks.icij.org/>

**2. Search for Pakistani companies or people (try examples like):**

* *Ittefaq Group*
* *National Fertilizer*
* *Sapphire Group*
* *Arif Habib*
* Or just type "Pakistan"

**3. See connected nodes:**

It shows links like:

Person --> Officer of --> Company --> Registered in --> Country

**4. Download data (optional)**

* You can import the CSV/JSON into Neo4j Desktop.
* Visualize the **network of offshore entities**.

✅ **Neo4j helps to see who is linked with whom**.

**🧩 PART 2: SpiderFoot — Detailed OSINT Tool**

**🕸️ What is SpiderFoot?**

A powerful **automated OSINT tool**. It collects and analyzes data about:

* IP addresses
* Domains
* Emails
* Usernames
* Phone numbers
* URLs

You can use it to **track someone or an entity** using just one small clue (e.g., IP, email).

**🚀 How to Use SpiderFoot (Step-by-Step)**

**📦 Install on Kali or Ubuntu:**

git clone https://github.com/smicallef/spiderfoot.git

cd spiderfoot

pip3 install -r requirements.txt

python3 sf.py

**🔌 Start the web UI:**

python3 sf.py -l 127.0.0.1:5001

* Then open: http://127.0.0.1:5001

**🔍 Example: Track an IP (like 123.45.67.89)**

1. Start a new scan → Enter IP 123.45.67.89
2. Enable modules like:
   * ipinfo
   * shodan
   * whois
   * geolocation
   * netblock ownership
3. Click **Run Scan**

**🧾 What You Might Discover:**

| **📌 Info** | **🔍 Use** |
| --- | --- |
| Country | Where the IP is registered |
| ISP | Which company owns the IP |
| Netblocks | Range of IPs owned |
| Domains | Which domains resolve to that IP |
| Open Ports | Find services running (via Shodan) |
| WHOIS | Domain/IP ownership info |
| DNS records | Subdomains, MX records, etc. |
| Leaked credentials | Found in public leaks |
| Social media | Emails linked to accounts |

**🧠 Use Cases**

* Investigate a **scammer's domain or IP**
* Check if a company uses suspicious hosting
* Track infrastructure of cybercriminal groups
* Connect leaked info from **OffshoreLeaks** to real identities

**🔐 Summary**

| **Tool** | **What It Does** |
| --- | --- |
| **Neo4j + OffshoreLeaks** | Visualize and investigate corporate fraud, tax evasion, hidden ownership |
| **SpiderFoot** | Automate tracking of IPs, domains, people, infrastructure |