**🕵️ Reconnaissance (OSINT Map)**

**🧠 What Is Reconnaissance?**

Reconnaissance (or **recon**) is the **first step in ethical hacking or penetration testing**.  
Think of it as **“digital spying”** — gathering as much information as possible **before attacking** a target.

**🔎 OSINT Map (Open Source Intelligence)**

OSINT means **collecting information from public sources** (no hacking yet!).

**🔧 Common OSINT Tools and Sources:**

| **Tool/Method** | **What You Can Find** |
| --- | --- |
| 🌐 **Whois** | Domain owner, emails, phone, hosting details |
| 🖥 **IP lookup** | Server location, ISP, threat level |
| 🧠 **Shodan** | Open ports, IoT devices, vulnerabilities |
| 🕸 **Google Hacking** | Sensitive files exposed online |
| 🧵 **Social Media** | Employee names, job roles, internal info |
| 🗃 **Data Leaks** | Pwned passwords, breached emails |
| 🕷 **SpiderFoot** | Automated OSINT (names, emails, IPs, DNS, breaches etc.) |
| 📜 **Maltego** | Graph-based investigation tool |
| 💡 **Hunter.io / Email Permutator** | Employee emails |
| 🗺 **Recon-ng / TheHarvester** | Domain emails, subdomains, metadata |

**🌐 WHOIS Lookup**

**🔍 What is it?**

**Whois** is a tool used to look up **domain registration data**.  
It shows **who owns a website**, when it was created, and where it's hosted.

**🧾 What Info You Can Get:**

* Domain owner name & email
* Domain registrar (GoDaddy, Namecheap, etc.)
* Creation/expiry dates
* Name servers (DNS)
* Hosting IPs
* Contact info (sometimes fake/private)

**🔧 Tools:**

* [whois.domaintools.com](https://whois.domaintools.com/)
* whois command in Linux
* [ICANN Lookup](https://lookup.icann.org/)

**🔁 Reverse WHOIS**

**🔍 What is it?**

**Reverse Whois** allows you to **search by owner details** (email, name, phone) to find **all domains** owned by the same person.

**🧾 Why It’s Useful:**

* Link **multiple websites** together
* Trace **malicious actors** who use many domains
* Identify **company infrastructure**
* Spot **attack surfaces** across domains

**🔧 Tools:**

* [ViewDNS.info Reverse Whois](https://viewdns.info/reversewhois/)
* [DomainTools Reverse Whois](https://research.domaintools.com/) *(limited free access)*

**🧠 Why You Should Learn This:**

* Helps build a **profile of your target**
* Supports **threat hunting & risk analysis**
* Shows how attackers gather info — and how to defend against it