OSINT & Recon Cheat Sheet 🕵️

From Phone Number to Full Profile

Phase 1: Network Reconnaissance – IP Address Acquisition 🌐

Objective: To capture a target's public IP address through a direct peer-to-peer connection.

Prerequisites:

- WhatsApp Desktop App installed
- Wireshark installed

Steps:

1. **Find Your Local IP:**
    - Open **Command Prompt** (cmd).
    - Run the command:
    - ipconfig
    - Note your **IPv4 Address** (e.g., 10.0.2.15 as shown in the video).
2. **Capture Traffic with Wireshark:**
    - Launch **Wireshark** and select your primary network adapter (e.g., Ethernet).
    - Apply the following display filter to isolate call traffic:
    - ip.addr == [Your.Local.IP.Address] && stun
    - Start the capture.
3. **Initiate Connection:**
    - Place a voice call to the target using **WhatsApp Desktop**.
    - **Crucial:** The target must answer the call to establish the connection.
4. **Identify Target IP:**
    - In Wireshark, look for packets with **"Binding Request"** in the information column.
    - The public IP address that is *not* yours is the target's IP.

Phase 2: Geolocation & Initial OSINT 🗺️

Objective: To turn the captured IP address and phone number into actionable intelligence.

- **IP Geolocation:**
    - Use an IP lookup service (the video shows whatismyipaddress.com).
    - Enter the captured IP to find the **city and country** (e.g., Berlin, Germany).
- **Phone Number Analysis:**
    - Use a WhatsApp profile checker (the video shows whatsapp.checkleaked.cc).
    - Enter the phone number to retrieve the public **profile picture, name, and bio**.
    - Download the profile picture for the next phase.

Phase 3: Data Enrichment & Pivoting 🔍

Objective: To use initial findings to uncover more detailed Personal Identifiable Information (PII).

- **Reverse Image Search:**
    - Upload the downloaded profile picture to a search engine like **Google Images**.
    - Look for matches linking to social media (**LinkedIn**), personal websites, or articles.
- **Advanced Google Searching ("Google Dorking"):**
    - Once a name is found (e.g., "Thomas Pfeffer"), use precise search queries:
    - "[Full Name]"
    - "[Full Name]" "[University/Company Name]"
    - This helps find professional profiles and publications containing details like email addresses or date of birth.
- **Data Breach & Leak Analysis:**
    - **Intelligence X (intelx.io):** Search the discovered email address to find it in public data leaks, which may include associated passwords.
    - **Have I Been Pwned (haveibeenpwned.com):** Check the email to see which data breaches it was involved in, revealing the *type* of data compromised (e.g., physical addresses).

Phase 4: Deep Data Analysis 💾

Objective: To search through downloaded breach data to find specific PII.

- **Acquire Data:**
    - Based on your findings, identify and acquire relevant data breach collections (the video mentions the **"Lead Hunter"** dataset as an example containing physical addresses).
- **Offline Search:**
    - Use a local file search tool like **Agent Ransack** to scan the contents of large data files.
    - Search for the target's email or other unique identifiers to find comprehensive information like a full address, birthday, gender, etc.

⚠️ **Disclaimer**

This document is for educational purposes only. The techniques described should only be used in a legal and ethical manner, such as during authorized penetration tests or for learning about cybersecurity defenses. Using these methods on individuals or systems without explicit permission is illegal and unethical.