OSINT Tools Guide for Ubuntu 24

Open Source Intelligence (OSINT) is the practice of collecting and analyzing information from publicly available sources. This guide introduces you to **SpiderFoot** and other popular OSINT tools you can use on Ubuntu 24, along with usage examples.

1. SpiderFoot

SpiderFoot is an OSINT automation tool that gathers information from over 200 public data sources. It can perform reconnaissance on IPs, domains, emails, names, and more. **Installation on Ubuntu 24:** sudo apt update sudo apt install python3-pip pip install spiderfoot **Usage Example:** python3 sf.py -s example.com -o tab -f This scans the domain *example.com* and outputs results in tabular format. SpiderFoot also provides a web interface: python3 sf.py -l 127.0.0.1:5001 Then open *http://127.0.0.1:5001* in your browser.

2. Maltego

Maltego is a powerful link analysis tool used for mapping relationships between entities like people, domains, IPs, companies, etc. **Installation:** sudo apt install maltego (or download from the official site). **Usage Example:** - Open Maltego, select a machine like *Footprint L1*. - Enter a domain (e.g., *example.com*). - The graph will expand to show connected DNS, WHOIS, IPs, and more.

3. theHarvester

theHarvester is a tool for gathering emails, subdomains, hosts, and employee names from public sources. **Installation:** sudo apt install theharvester **Usage Example:** theHarvester -d example.com -l 100 -b google This searches Google for up to 100 results related to *example.com*.

4. Shodan

Shodan is a search engine for Internet-connected devices. **Installation:** pip install shodan shodan init <API_KEY> **Usage Example:** shodan search apache This searches for devices running Apache exposed on the internet.

5. Recon-ng

Recon-ng is a reconnaissance framework with a command-line interface similar to Metasploit. **Installation:** sudo apt install recon-ng **Usage Example:** recon-ng modules load recon/domains-hosts/bing_domain_web set SOURCE example.com run This finds hosts associated with *example.com* using Bing search.

These tools provide powerful ways to collect intelligence on targets using publicly available information. Always ensure you use OSINT tools ethically and within legal boundaries.