🛡️ PySecOps : Security Operations Toolkit Guide

1. Project Overview

PySecOps is an all-in-one Python security suite designed for network administrators and security enthusiasts. It combines network scanning, web reconnaissance, vulnerability testing, and file integrity monitoring into a single command-line interface.

---

2. Setup Instructions

A. System Requirements

1. **Python 3.x**: Ensure Python is installed (python --version).
2. **Nmap**: The network scanner requires the Nmap engine. Download it from nmap.org.

B. Dependency Installation

Run the following command in your terminal to install all required libraries:

Bash

- Head to **Toolkit directory** and run the Requirements.txt in terminal (cmd)

```
pip install -r Requirements.txt
```

or

```
pip install requests python-nmap tabulate colorama rich
pyfiglet whois PyPDF2 numpy scikit-learn watchdog
builtwith dnspython
```

- After Installation head to **PySecOps Directory** for running toolkit.

---

3. Feature Descriptions & Commands

🕹️ The Central Hub (Main Menu)

- **Description:** The entry point for the entire project. It allows you to navigate between all tools without restarting scripts.
- **Command:** python PySecOps.py

🔍 Network Operations

1. Network Scanner (NetworkScan.py)

- **Description:** A multi-threaded scanner that identifies live devices and open ports.

- **Key Features:** OS fingerprinting, service version detection, and host discovery.

2. Web Reconnaissance (WebRecon.py)

- **Description:** Gathers deep technical intel on a domain, including DNS records and IP geolocation.
- **Key Features:** Subdomain enumeration, MX/TXT record lookups, and Geolocation mapping.

3. Web Scraper (WebScrapper.py)

- **Description:** Analyzes a website's technology stack and hosting details.
- **Key Features:** Identifies CMS (like WordPress), server types, and WHOIS registration data.

🛡️ Defensive & File Security

4. File Integrity Monitor (FileIntegrity.py)

- **Description:** Uses AI (Isolation Forest) to detect suspicious changes in a directory.
- **Key Features:** Detects file tampering, unauthorized deletions, and real-time event logging.

5. Phishing Link Scanner (PhishingLinkScanner.py)

- **Description:** Scans URLs found in PDF, CSV, or TXT files for malicious characteristics.
- **Key Features:** Domain age check, HTTPS verification, and automated risk scoring.

6. File Keyword Scanner (File_scanner.py)

- **Description:** Scans specific files for a database of 200+ "red flag" security keywords.
- **Key Features:** Identifies mentions of "malware," "reverse shell," or "exploit" within documents.

🔑 Utility Tools

7. Clickjacking Tester (ClickJacking.py)

- **Description:** Tests if a website can be embedded in an iframe (a common UI hijacking technique).
- **Key Features:** Checks for X-Frame-Options and Content-Security-Policy headers.

8. Password Generator (PasswordGenerator.py)

- **Description:** Creates secure, context-aware passwords for specific platforms (e.g., Facebook, GitHub).
- **Key Features:** Personalized entropy, strength estimation, and platform-specific keyword injection.