OSINT Information Gathering Tool

A comprehensive OSINT (Open Source Intelligence) command-line tool that generates links to various online platforms where information about a target might be available.

Overview

This tool helps security researchers, investigators, and privacy-conscious individuals by aggregating search links across multiple OSINT resources. Rather than scraping data directly (which could violate terms of service or privacy laws), it provides organized links for manual investigation.

Features

- Searches across 12 different OSINT categories:
  - Social Media
  - Data Breach Sites
  - People Directories
  - Professional Data
  - Public Records
  - Web Presence
  - Images
  - Dark Web
  - Reverse Phone Lookup
  - Email Addresses
  - Geolocation
  - Blockchain
- Provides formatted output with the Rich library for improved readability
- Progress indicators for search operations
- JSON export for saving and sharing results
- Configurable rate limits and timeouts
- Error handling and logging

Installation

Requirements

- Python 3.6+
- Required libraries: requests, beautifulsoup4, rich

Setup

1. Clone the repository or download the script
2. Install required dependencies:

bash Copy

```bash
pip install requests beautifulsoup4 rich
```

3. Make the script executable (Linux/Mac):

bash Copy

```bash
chmod +x osintv3.py
```

Usage

Basic Usage

bash Copy

```bash
python osintv3.py "John Smith"
```

Save Results to JSON File

bash Copy

```bash
python osintv3.py "Jane Doe" --output results.json
```

Additional Options

bash Copy

```bash
python osintv3.py "Alex Johnson" --rate-limit 2 --timeout 15 --verbose
```

Command-Line Arguments

- `target_name`: Target name for OSINT search (required)
- `--output`: Output file path for JSON results
- `--rate-limit`: Rate limit between requests in seconds (default: 1)
- `--timeout`: Request timeout in seconds (default: 10)
- `--verbose`: Enable verbose output

Output

The tool generates a structured display in the terminal using tables for each category of OSINT sources. Each table includes:

- Source name
- Description of the source
- URL to search for the target

If the `--output` parameter is specified, the results are also saved to a JSON file with the following structure:

json Copy

```
{
  "target": "Target Name",
  "timestamp": "YYYY-MM-DD HH:MM:SS",
  "results": {
    "Category1": {
      "Source1": {
        "url": "https://example.com/search?q=target",
        "description": "Description of the source"
      },
      ...
    },
    ...
  }
}
```

Legal and Ethical Considerations

This tool is intended for:

- Security researchers conducting authorized assessments

- Individuals checking their own digital footprint
- Law enforcement with proper legal authorization
- Privacy advocates educating on digital exposure

Please use responsibly and ethically. Always respect privacy and adhere to applicable laws and regulations.

Limitations

- The tool only generates links for manual investigation and does not scrape or extract data
- No validation that the target exists on the specified platforms
- Some services referenced may require registration or payment for full functionality
- Dark web links require specialized browsers like Tor to access

Contributing

Contributions to improve the tool are welcome! Please feel free to submit issues or pull requests.

License