

Lazarus v5.9 Installation and Usage Guide

1. Prerequisites

- Python 3.x
- Virtual environment (venv) or conda
- Dependencies: python-evtx, requests, beautifulsoup4

2. Installation

- a) Clone or download lazarus_v5.9.py to your working directory
- b) Create virtual environment and activate:
 - python3 -m venv venv
 - source venv/bin/activate (Linux/macOS)
 - venv\Scripts\activate (Windows)
- c) Install dependencies:
pip install python-evtx requests beautifulsoup4

3. Usage

Syntax: python lazarus_v5.9.py -m <module> -t <target>

Available modules:

- * crypto : decode hex, base64, ROT13
- * log : analyze log files for keywords
- * browser : extract URLs from history.txt
- * usb : detect USB artifacts from registry dump
- * web : scan HTML/JS for flags and exploits
- * evtx : parse Windows Event Logs for flag fragments
- * flag : rebuild flag from fragments
- * ssti : auto exploit SSTI and extract flag

4. Examples

```
python lazarus_v5.9.py -m crypto -t secret.txt
python lazarus_v5.9.py -m log -t auth.log
python lazarus_v5.9.py -m browser -t history.txt
python lazarus_v5.9.py -m usb -t registry_dump.hiv
python lazarus_v5.9.py -m web -t index.html
python lazarus_v5.9.py -m evtx -t Windows_Logs.evtx
python lazarus_v5.9.py -m flag -t Windows_Logs.evtx
python lazarus_v5.9.py -m ssti -t http://your-ctf-url/
```

5. Troubleshooting

- * ModuleNotFoundError: No module named 'Evtx' → pip install python-evtx
- * Missing requests or bs4 → pip install requests beautifulsoup4
- * Ensure venv is activated before running commands