

Ma1IPu11 Threat Feed Aggregator - User & Admin Guide

Version: Post Release Version 1

Developed By: Aaron Fitzpatrick

Project: Cybersecurity Capstone – Virelia Health Systems

Last Updated: June 5th 2025

Overview

Ma1IPu11 is a lightweight, open-source Bash-based threat feed aggregator designed to help small- to mid-sized organizations monitor and react to emerging cyber threats. It automatically fetches, parses, and aggregates malicious IPs from public threat intelligence feeds.

Key benefits:

- GUI and CLI modes (Zenity for non-terminal users)
 - Internal Role-based access control
 - Daily scheduled scan capability
 - Export formats: CSV or JSON
 - Minimal system overhead
-

System Requirements

Requirement	Details
OS	Linux (Ubuntu/Debian/RedHat/Arch)
Shell	Bash 4.x or higher
Required Tools	<code>curl</code> , <code>zenity</code> , <code>jq</code> (for JSON. Script will attempt to install all necessary dependencies)
Storage	The script itself is currently 37KB however you should allot at least 20MB to account for log/output files in the long run.

Access

Requires Sudo permissions for initial installation

Installation Instructions

To Download the script:

To download **MalIPull**, simply open you linux terminal and type in the following command in the directory that you would like the script to be downloaded to:

```
Wget https://raw.githubusercontent.com/Aaroncycy/MalIPull/refs/heads/main/malipull.sh
```

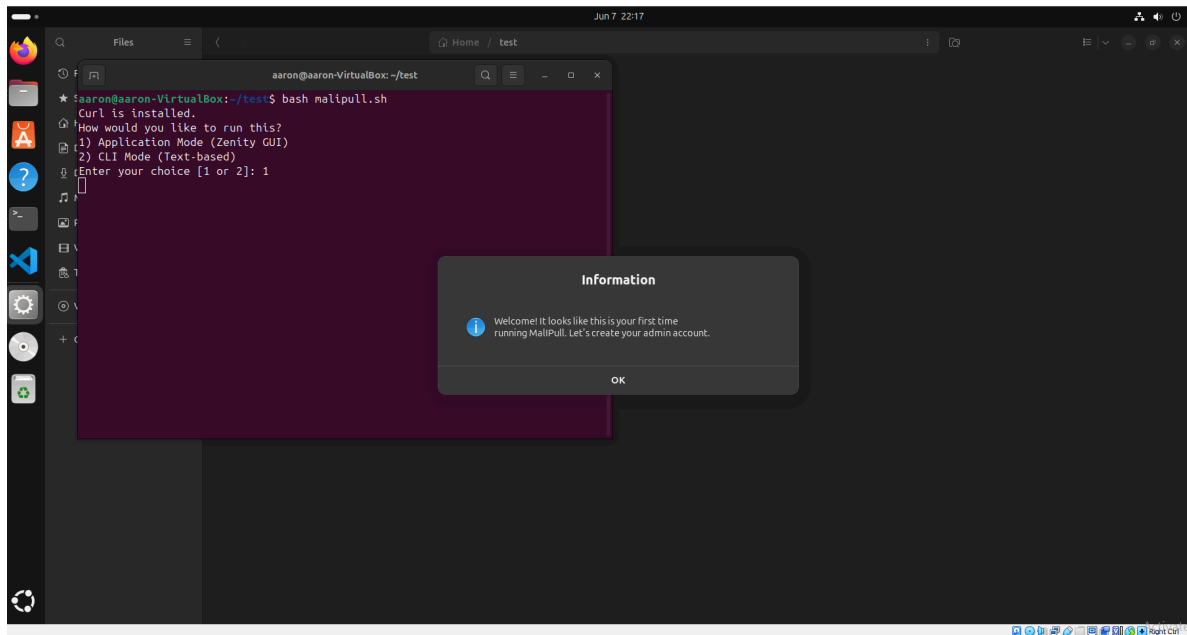
1. Run the script:

```
bash malipull.sh
```

2. The script will automatically:

- Check/install **curl**, **zenity**, **jq**
- Create config directories in **/etc/MalIPull_Configs** and logs in **/var/log/MalIPull_Logs/**

3. Prompt first-time admin setup



(img. Initial Launch of MalIPull will prompt admin user account creation)

Getting Started

When launched, you'll be prompted to select a mode:

- **1) Application Mode (GUI)** — For users preferring point-and-click navigation.
- **2) CLI Mode (Text-based)** — For terminal users or headless systems.

Log in with your credentials to begin using the tool. Admins can manage users and settings; analysts can run/schedule scans and view logs.

Operating Modes

GUI Mode (Zenity)

- Intuitive point-and-click interface
- Recommended for non-technical users
- Menu options include: Run Scan, Schedule, View Logs, Manage Feeds

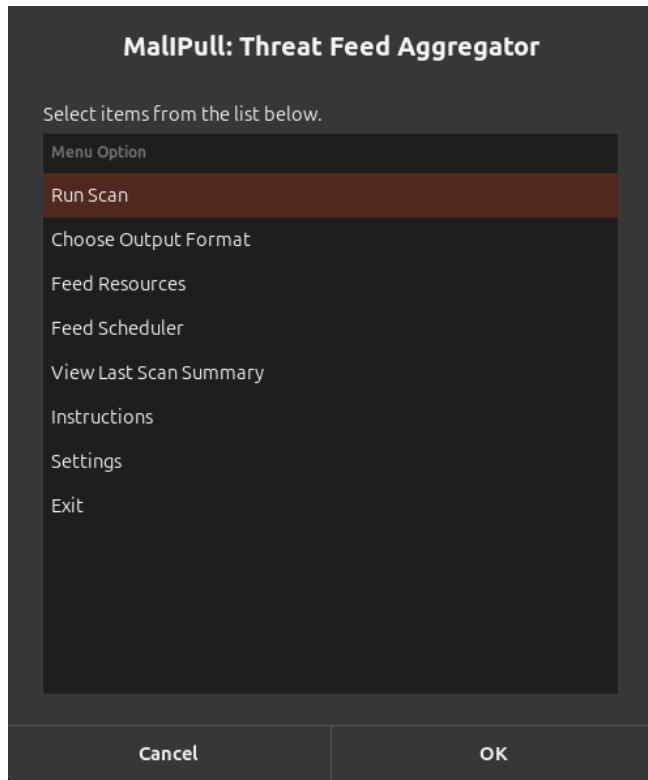
CLI Mode

- Text-based interaction
 - Suitable for terminal users and script automation
 - Semi-full feature parity with GUI
-

Main Features

Feature	Description
Run Scan	Pulls IPs from all sources and logs new indicators
Output Format Selection	Choose between CSV or JSON
Feed Management	Add/remove public threat feeds

Scheduling	Set a daily time for auto-scans
Role-based Login	Create Admins or Analysts with specific access levels
Log Summary	View last scan summary and differential IPs
Settings	Allow for Admins and Analyst to alter tool and user settings



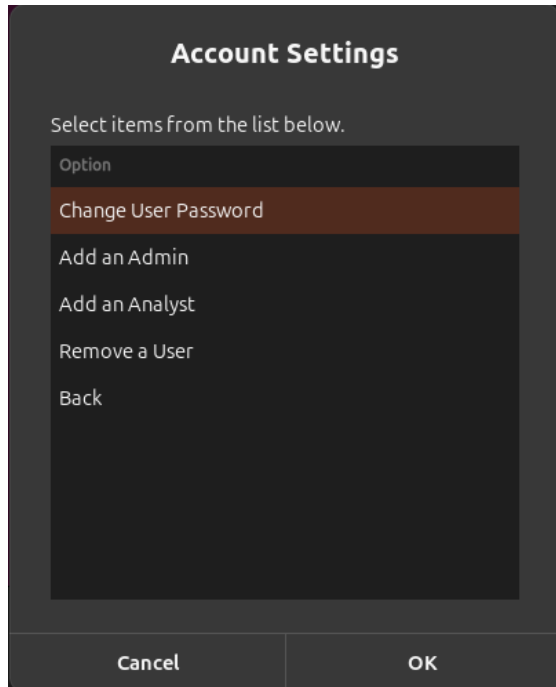
User Roles & Permissions

Role	Abilities
Admin	Full control, user creation/removal, feed edits, settings changes
Analyst	Can run and schedule scans, export data, view summaries

Admins **cannot be removed** if they are the last admin on the system. Passwords are stored using salted SHA-256 hashing.

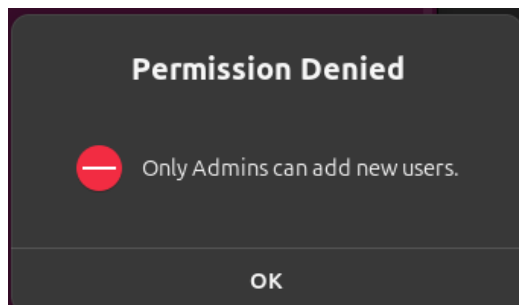
Settings:

Within the settings menu users can access account settings, where they can change the current users password, (all users can perform this function) Add an admin account, add an analyst, or remove a users account (only admins can perform these operations.)



(img. The account settings menu page in MallPull)

Upon logging in, the user's account type will be clearly stated as either an analyst or an Administrator. If an analyst attempts to make changes only permitted to Administrators, they will be notified that their account type does not permit that sort of action.



(img. Users who are not Administrators will be notified if they attempt to perform a task that they are not permitted to perform)

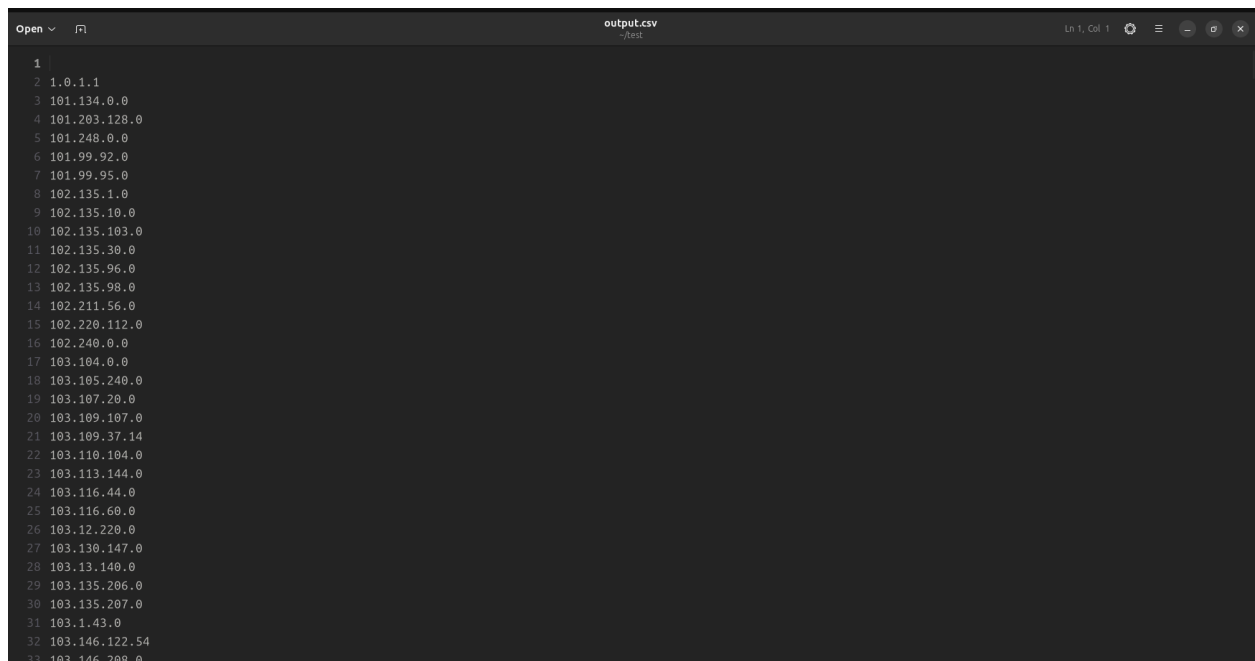
Scheduled Scans

Users may schedule daily scans using the **Feed Scheduler** option.

- Choose HH:MM (24-hour format)
- Script runs every day at selected time
- Logs stored in `scheduler.log`

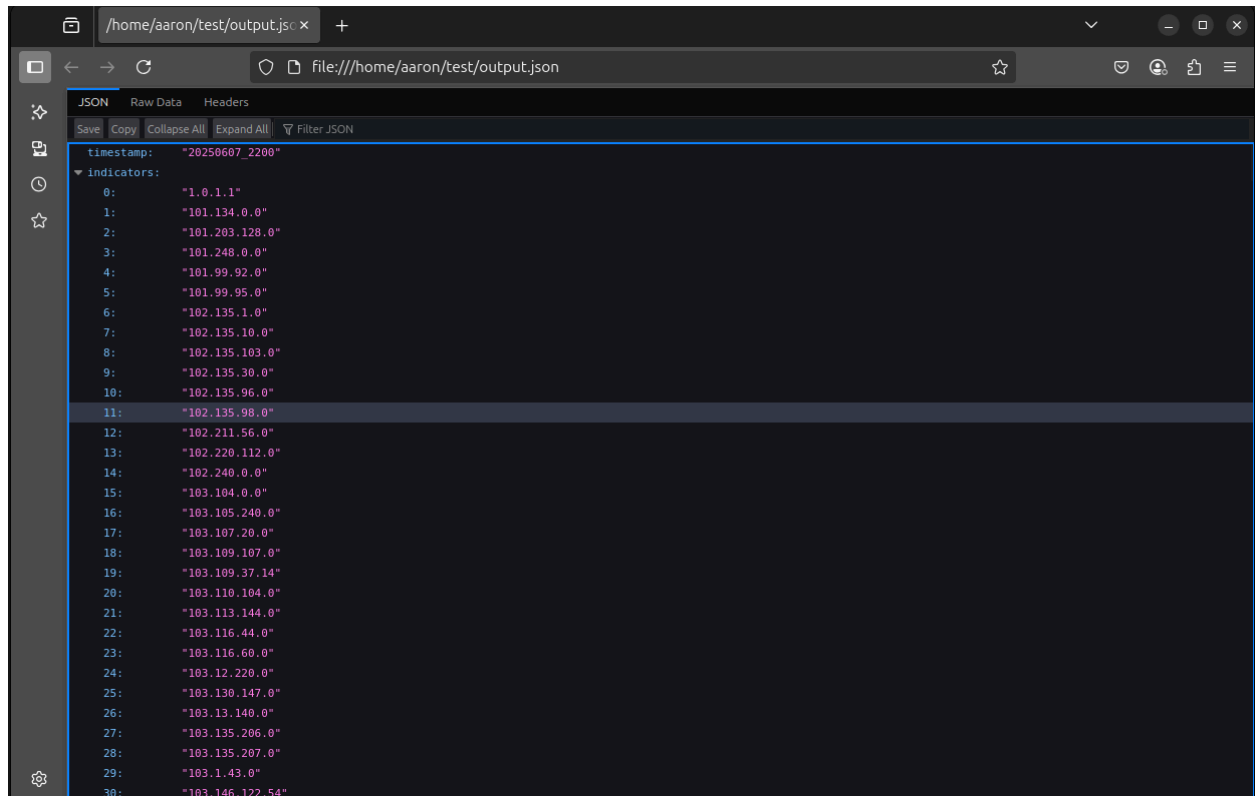
Scan Results:

Depending on the type of output that you select, scan output will either be constructed in CSV or JSON format. After a scan has been performed, you can navigate to the scripts directory and select the created scan file to manually review its contents. Below are the results of scans outputted in CSV and JSON formats respectively:



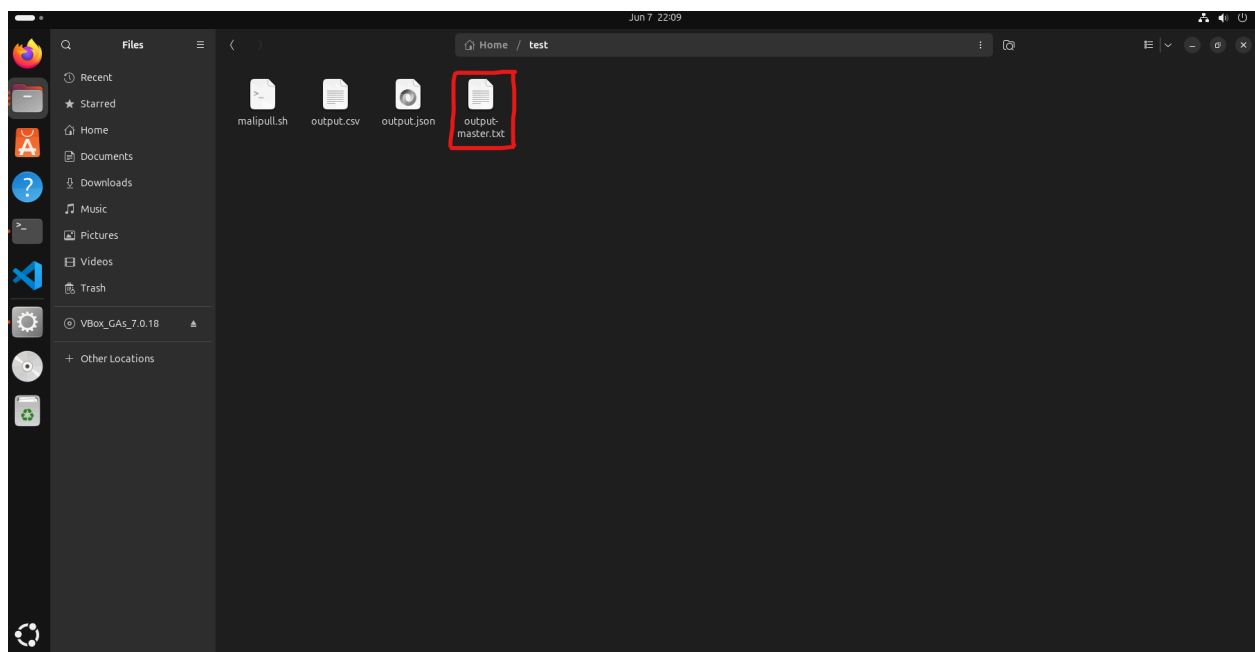
```
1
2 1.0.1.1
3 101.134.0.0
4 101.203.128.0
5 101.248.0.0
6 101.99.92.0
7 101.99.95.0
8 102.135.1.0
9 102.135.10.0
10 102.135.103.0
11 102.135.30.0
12 102.135.96.0
13 102.135.98.0
14 102.211.56.0
15 102.220.112.0
16 102.240.0.0
17 103.104.0.0
18 103.105.240.0
19 103.107.20.0
20 103.109.107.0
21 103.109.37.14
22 103.110.104.0
23 103.113.144.0
24 103.116.44.0
25 103.116.60.0
26 103.12.220.0
27 103.130.147.0
28 103.13.140.0
29 103.135.206.0
30 103.135.207.0
31 103.1.43.0
32 103.146.122.54
33 103.146.208.0
```

(img. MallPull IP results file in csv)



(img. MallPull IP results file in JSON)

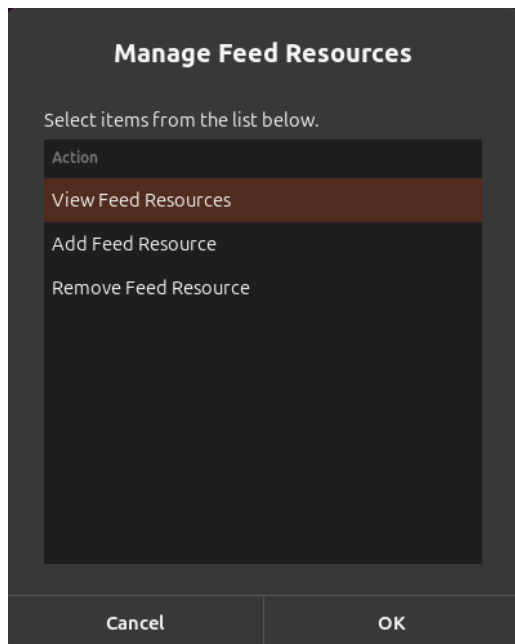
This directory will also contain the `output-master.txt` file, which serves as the master list of all known malicious IPs aggregated by the tool across all scans.



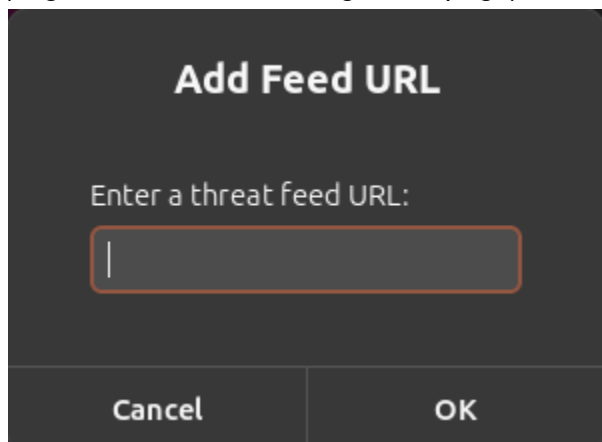
(img. Location of `output-master.txt` file)

Adding feeds:

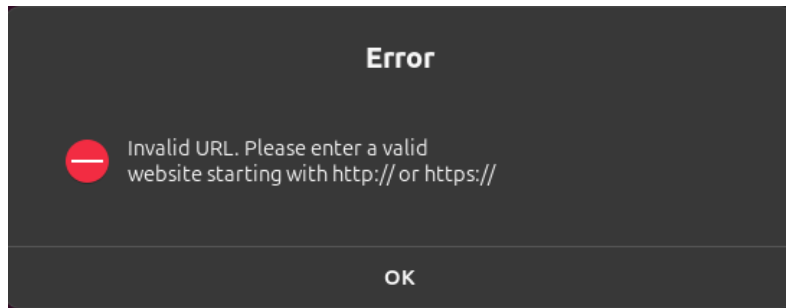
When a user selects “Feed Resources”, they will be brought to the Feed Resources Management Page. Here they will be able to View all of the current feed sources that the tool is retrieving data from. They can also Add feed sources or remove feed sources. URLs being added to the feed sources MUST begin with <http://> or <https://>, otherwise MallPull will not use the added source.



(img. Feed Sources Management page)



(img. Users can paste the weblink/ URL of the feed that they would like MallPull to draw from)



(img. MallPull will not accept URLs that do not start with http:// or https://)

Log Files & Output Formats

File	Location Default	Purpose
Output File	Defaults to same Directory as Script (Customizable)	Structured list of malicious IPs
Scan Logs	/var/log/MalIPull_Logs/<user>/scan-*.log	Scan activity logs
Differential IPs	/var/log/MalIPull_Logs/<user>/diff-*.txt	New IPs found during scans
User Registry	/etc/MalIPull_Configs/UserShadow.s.txt	Encrypted user credentials
Feed Config	/etc/MalIPull_Configs/feeds.txt	Threat feed URLs
Format Config	/etc/MalIPull_Configs/config.cfg	Output preferences

Security Notes

- Passwords are **salted and hashed** using `sha256sum`.
 - The script performs **role validation** before executing sensitive operations.
 - Output files are stored in local-only directories to reduce risk of external leaks.
 - If Zenity is unavailable, a **CLI fallback mode** is offered.
-

Troubleshooting

Issue	Fix
Zenity not found:	Script prompts to install, or offers CLI fallback. If script installation fails, users can install Zenity manually using their Distro's installation command.
Invalid threat feed URL:	Ensure resource/ feed begins with <code>http://</code> or <code>https://</code> and returns raw data
Permissions errors:	Ensure script is executed with user having sudo rights
No new IPs found:	May be a duplicate scan or static feeds — validate URLs (Scan eliminates duplicates automatically)
Scheduler not working:	Confirm system time is accurate and the background process is alive

FAQ

Q: Can I add private threat feeds?

A: Yup, *IF* the feed is accessible via `curl` and outputs IPs in plain text or HTML.

Q: Is this script safe to run on production systems?

A: Yes, but always test in a VM first and review all code before full integration. (Yes, I am literally telling you *not* to trust me... scan the script or peek into the code before running it. That's just a good general rule for life tbh...)

Q: Can I automate integration with firewalls or SIEM?

A: Yes! You can use the `output.csv` or `output.json` as inputs for other scripts or APIs.

Support & Contribution

This tool is developed for operational equity AND educational purposes.

To suggest improvements, report bugs, or contribute:

 **Contact:** aaron.fitzpatrick@email.com

 **Repository:** [GitHub](#) 

License: Open-source under MIT License

