Update #10 - Fail2Ban IP Geolocation Lookup Script with Auto Filtering

Date: May 11, 2025
Category: Security / Automation

Backlink: Update #9 – Syncthing UFW Log Monitoring with Active Fail2Ban Enforcement

Overview

This update improves visibility into the origin of IP addresses actively banned by Fail2Ban on the VPS. The goal was to enrich situational awareness for brute-force SSH attempts and UFW-blocked Syncthing port scans by fetching country, city, and provider data for each offender.

What Was Implemented

- A Bash script named `fail2ban-ip-lookup.sh` was written to:
  - Pull current banned IPs from the `sshd` and `ufw-block` jails
  - Skip link-local IPv6 addresses (`fe80::/10`)
  - Query ipinfo.io for geolocation and network information
  - Format and display the results cleanly with color-coded output (when using `jq`)
- Optional `jq` integration was added to format the JSON neatly
- The script can easily be expanded to:
  - Save results to logs
  - Exclude private IPv4 ranges (`10.*`, `192.168.*`, etc.)
  - Run on a cron schedule for daily snapshots

Example Output

□□ IP: 116.110.12.54

"116.110.12.54"

"Thanh Khê"

"Da Nang"

"VN"

"AS24086 Viettel Corporation"

□□ IP: 8.222.230.39

"8.222.230.39"

"Singapore"

"Singapore"

"SG"

"AS45102 Alibaba (US) Technology Co., Ltd."

Script Location

Stored at:

```
~/fail2ban-ip-lookup.sh
```

Dependencies

`curl` (usually preinstalled)
`jq`: Install using:

```
sudo apt install jq -y
```


```
sudo apt install jq -y
```


Future Improvements

- Add logging with timestamps
- Auto-reporting for suspicious regions
- Integration into BookStack as a daily monitored report

Revision #4
Created 11 May 2025 14:07:44 by Nate Nash
Updated 7 June 2025 00:14:24 by Nate Nash