

Update #13: Fail2Ban IP Lookup & Enrichment Script with GeoIP, PTR, and AbuseIPDB

Date: May 11, 2025

Category: Security / Automation

Backlink: [Update #12 - Step-by-Step Breakdown of UFW DDNS Update Script](#)

Objective

Build a script to automatically extract and enrich the IP addresses banned by Fail2Ban, giving deeper insight into:

- Where attacks are coming from
- Whether they're part of known threat networks
- If they're associated with VPNs, datacenters, or residential ISPs

Tools Used

- `bash` - for scripting
- `fail2ban-client` - to fetch banned IPs from jails
- `ipinfo.io` - to get geolocation and ASN details
- `host` - to perform reverse DNS lookups (PTR)
- `AbuseIPDB` - to identify IPs with high abuse confidence scores
- `jq` - to parse and format JSON responses
- `tee` - to send output to both screen and log file

- **Logrotate** - to manage log size and history

Script Behavior Summary

1. Enumerates Fail2Ban Jails

- Targets: `sshd` and `ufw-block`
- Extracts unique banned IPs

2. Performs Lookup on Each IP

- `ipinfo.io`:
 - IP
 - Hostname
 - City, Region, Country
 - ASN & ISP
 - Coordinates & Timezone
- `host`: PTR (reverse DNS)
- `AbuseIPDB`:
 - Abuse confidence score
 - Total number of reports
 - Last reported timestamp

3. Emoji-based Output for Quick Review

- 📄 IP address
- 📄 PTR record
- 📄 Abuse summary

4. Writes to a Daily Log File

- File: `/var/log/fail2ban-ip-lookup.log`
- Rotated daily via Logrotate with:
 - 7-day history
 - Compression
 - Ownership: `root:root`

Logrotate Config

Path: `/etc/logrotate.d/fail2ban-ip-lookup`

```
/var/log/fail2ban-ip-lookup.log {  
    su root root  
    daily  
    rotate 7  
    compress  
    missingok  
    notifempty  
    create 644 root root
```

```
}
```

Example Output

```
IP: 137.74.246.152
"s03.cert.ssi.gouv.fr"
"Roubaix"
"Hauts-de-France"
"FR"
"AS16276 OVH SAS"
"50.6942,3.1746"
"Europe/Paris"
PTR: s03.cert.ssi.gouv.fr.
Abuse Score: 100 | Reports: 45 | Last Reported: 2025-07-10T18:22:33Z
```

API Keys & Notes

- `IPINFO_TOKEN` and `ABUSEIPDB_API_KEY` are **stored securely** in the script (omitted here).
- AbuseIPDB account was created under a free tier allowing 1000 queries/day.
- Shodan integration may be added in future releases.

Future Plans

- Create a filter to exclude known safe IPs from reports
- Output top countries, ASNs, or ISPs from historical logs
- Add optional email summary of banned IPs

Revision #3

Created 12 May 2025 22:49:00 by Nate Nash

Updated 7 June 2025 00:14:24 by Nate Nash