Update #14 - Auto-Banning Fail2Ban IPs Based on AbuseIPDB Reputation

Date: May 22nd, 2025
Category: Security / Automation

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

Overview

Building upon the foundation established in Update #13, this update introduces **active enforcement logic** to **permanently block IPs** based on their reputation score from AbuseIPDB.

The goal is to automatically detect and firewall-block any IPs that:

- Are currently banned by **Fail2Ban**
- Have a high **abuse confidence score** (≥75) according to AbuseIPDB

What's New in This Update

Feature	Status
AbuseIPDB reputation score enforcement	
UFW rule auto-injection per IP	
Duplicate ban protection	
Detailed logging for all actions	

Feature	Status
Configurable abuse score threshold	

Script Location

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

Log Output

```
/var/log/fail2ban-ip-lookup.log
```

Logs include:

- Jail name
- IP
- Geo/IPInfo data
- PTR record (reverse DNS)
- AbuseIPDB score, reports, and last report time
- Auto-ban status

Script Logic Flow

1. Get banned IPs from `sshd` and `ufw-block` jails
2. For each IP:
   - Fetch GeoIP data from IPInfo
   - Perform reverse DNS lookup
   - Query AbuseIPDB for score and report count
   - If `abuseConfidenceScore` ≥ 75:
     - Check if IP is already blocked in UFW
     - If not, run `sudo ufw deny from [IP]` with a comment
3. Write all output to `/var/log/fail2ban-ip-lookup.log`

Script Excerpt (Auto-Ban Logic)

```
if [[ "$abuse_score" -ge "$ABUSE_THRESHOLD" ]]; then
    if sudo ufw status | grep -qw "$ip"; then
```

```
        echo -e "□ Already blocked: $ip" | tee -a "$LOG_FILE"
    else
        echo -e "□□ Auto-banning $ip due to high AbuseIPDB score ($abuse_score)" | tee -a "$LOG_FILE"
        sudo ufw deny from "$ip" comment "Auto-banned: AbuseIPDB score $abuse_score"
    fi
fi
```

Automation (Cron Job)

To run this script automatically once per day:

```
sudo crontab -e
```

Add this line (adjust path if needed):

```
0 3 * * * /home/<username>/fail2ban-ip-lookup-extended.sh
```

Security Note

This approach ensures that:

- Banned IPs with high global abuse reputation are **firewalled at the OS level**
- You retain full visibility and control over what's blocked
- Only IPs caught by **both** local behavior (Fail2Ban) and global reports (AbuseIPDB) are enforced

---

Revision #2
Created 22 May 2025 22:02:40 by Nate Nash
Updated 7 June 2025 00:14:24 by Nate Nash