Update #6 - Fail2Ban Security Hardening - Longer Bans, Fewer Chances

After implementing a dynamic `ignoreip` rule using my DDNS hostname in Update #5, I proceeded to further harden my Fail2Ban configuration. The goal was to tighten lockout criteria and extend ban durations to reduce the risk of brute-force attacks on my VPS.

What I Changed

- **Increased Ban Duration:**
  Set `bantime` to `12h` so attackers are kept out for a long stretch.
- **Shortened Detection Window:**
  Set `findtime` to `10m`, limiting how far back Fail2Ban looks for failed attempts.
- **Stricter Retry Limit:**
  Set `maxretry` to `3`, meaning three failed login attempts trigger a ban.
- **Updated `jail.local` Configuration:**

```
[DEFAULT]
ignoreip = 127.0.0.1 <dynamic-ip-from-ddns>
bantime = 12h
findtime = 10m
maxretry = 3
```

Note: The `<dynamic-ip-from-ddns>` is automatically updated via a custom script that resolves my DDNS hostname and inserts the current IP.

Verification

To confirm the configuration was working as expected, I ran:

```
sudo fail2ban-client status sshd
sudo tail -f /var/log/fail2ban.log
```

This verified that failed attempts were being logged, and offenders were banned promptly after 3 failures.

Result

The system is now more secure, allowing fewer login attempts and keeping bad actors out longer. With dynamic DDNS-based whitelisting and aggressive jail parameters, my SSH service is much better protected going forward.

Revision #4
Created 9 May 2025 22:13:30 by Nate Nash
Updated 7 June 2025 00:14:24 by Nate Nash