Password Policy Inject

Linux Team

Jeffrey Fonseca

2023-09-30

Purpose

Encourage users to create strong passwords, via a new password policy.

NIST Recommendations

The NIST recommendations for password policies have changed. Things like special characters, encourage users to create weaker passwords.

A short overview of NIST reccomendations, according to one article, and another:

- Human generated passwords are minimun 8 characters, machine generated one's are minimum 6
- Check passwords against a denylist, of already compromised passwords, or public dictionaries
- Special Character rules are optional
- Allow 64 character passwords
- Allow show password while typing, as increased chance of unfixable typos encourages users to create weaker passwords
- Enforce 2FA
- Regular password resets encourage weak passwords, so only reset unless a compromise is suspected

Personal Recommendations

With these guidelines in place, I suggest a *passphrase* policy, rather than a password one. Passphrases are easy to remember, and can be done with just as much entropy. In fact, I advocate for these rather than passwords.

- Passphrases must be at least 6 words
- Two of these words cannot be in the more common dictionaries, like those an attacker would use to do a brute force attack
- Easily guessable phrases, like full sentences (E.G. [name] loves [name] very much), should automatically fail.
    - An advanced way to implement this would be to have a large langauge model look at passwords,
    - An easier way to implement this is to simply ban verbs and adverbs.
- Password resets shoudl be done only when compromise is suspected
- Enforce 2FA authentication, but **no SMS**. SMS is insecure because it is trivial for an attacker to impersonate themselves as the owner of someone else's phone that they "lost". Either TOTP/OTP codes (Google, Microsoft authenticator), key based, or even biometric, if possible.
- Ban anything too close to any leaked or compromised passwords

Implementation Plan

Modern linux systems use `pam` to configure password rules. Available on almost all linux systems, including embedded systems like routers.

We can configure pam to set the rules we want.

For example, you can point pam to a dictionary to disallow any passwords with words from a dictionary:

```
....
password requisite pam_pwquality.so retry=3 dictcheck=/path/to/your/wordlist.txt
....
```

We can use this, in addition to other pam policies to ensure secure passwords.

For 2FA, we can set up something like google authenticator. Here is a guide by Red Hat on how to do so