Red Hat Certified System Administrator

Password Management and Aging

Password requirements

Setting password requirements is essential in today's world full of security vulnerabilities.

There are two areas to look at when considering password requirements

1) Expiration/Longevity of a password
2) Actual password requirements

Longevity of a Password

We can use the `chage` command to change password expiry information.

`d` – Set number of days since the password was reset. 0 will force a password reset.

`M` – Maximum days a password will be valid for. Once that number passes a user will be required to reset their password.

`I` – Number of days of inactivity after expiration before locking the account

Longevity of a Password

More **chage** flags to be aware of:

`E` – Set the date when the user account will be locked out, requiring administrator intervention. -1 will mean the account never expires.

`W` - How many days before expiration will a user receive a warning that the password will expire

Password Complexity

Regardless of how often you require users to reset passwords, you'll end up with weak passwords.

Enforcing password complexity will remove some of that risk.

Password complexity is important to enforce and is done so using the `pam_pwquality` module.