New Password Policy

Liaison Meeting
September 10, 2020

BROOKHAVEN
NATIONAL LABORATORY

U.S. DEPARTMENT OF
ENERGY

BROOKHAVEN SCIENCE ASSOCIATES

Introduction

- The SDCC is not compliant with Cyber Security regulations:
  - Passwords are not expired every 6 months, not checked for weak passwords, …

- Remediation plan was discussed - as ITD intends to move to 16+ characters, SDCC plan is to go for NIST800-63B compliance
  - The minimum length will increase from 8 to 16 characters.
  - The requirement for multiple character classes (uppercase, lowercase, numbers, and symbols) and password complexity will be eliminated, so multiple word passphrases will be allowed.
  - The history will be increased to 24 previously used passwords, new passwords that are found in the saved history, or in a DB of known compromised/bad passwords will not be allowed.
  - Passwords never expire

Proposed Plan

- Announce to users and open the new password system next Monday, September 14, 2020.
- Give users 2 weeks to login and update their passwords to comply with new policy (regular reminders will be sent during this time).
- Password changes will be allowed through a new WebUI:
  - https://web.sdcc.bnl.gov/apps/passwd/
- Or by logging into one of the ssh.sdcc.bnl.gov gateways and using the passwd command.
- After 2 weeks, we will disable user accounts that haven’t changed their passwords, on Monday September 28, 2020.
- After this, users will have to submit an RT ticket to request a password reset, like they do now for forgotten passwords.

Goals

- Make it easier to access the SDCC
    - avoids arbitrary password expirations
- Plan is to improve the scope of SSO services
    - Single password can be used everywhere
    - External access using password + OTP (MFA)
- Note: Grid services are not included in this.
- More information:
    - https://www.racf.bnl.gov/docs/authentication/passwords