Disabling UNIX accounts that are not in compliance with Cyber trainings

Erwin Lopez

Olga Bykov

August 27, 2020

U.S. DEPARTMENT OF ENERGY
Office of Science

SLAC NATIONAL ACCELERATOR LABORATORY

Summary

- Enforcement of training compliance policy for Unix accounts

- Requirement to complete as soon as possible, due to reporting requirements and increase in remote user community

- Three-phased effort to disable non-compliant Unix users

Background / why

Recently, a risk assessment have been conducted on the expired cyber security training automated process for disabling Unix accounts. The tests resulted in a 90% failure rate of the disablement process for non-compliance cyber security training Unix accounts.

The corrective action plan has been created to fix this issue.

In accordance with DOE reporting requirements, SLAC must **enforce the policy on Cyber training compliance** for account usage **as soon as possible**.

Phased approach
(more details and special cases – in the next slides)

Phase	Effort	ETA
Phase 1	Disable all UNIX accounts with expired password AND expired Cyber training *exclude accounts where password expired less than 2wks ago (gives new user accounts enough time to complete the training)	Wed 9/9
Phase 2	Disable all UNIX accounts with expired Cyber training *change in current practice of re-enabling the account, and THEN taking the training. No re-enabling until training is complete.	Wed 9/16
	Manual effort, disabling accounts with expired Cyber training on a daily basis *exclude accounts created 5 or fewer days ago	(between phases)
Phase 3	*Long term solution* Not allow the creation of new UNIX or AD accounts unless the user completed Cyber training.	TBD

Phase 1 – Disable all UNIX accounts with expired password AND expired Cyber training – 9/9

- Exclude accounts where password expired < 2wks ago

- Impact on users: minimal to small

Question to you:

There is a way for users to log in using ssh keys even if their password is expired. Most likely the number of such use is minimal – is that correct assumption?

- User communication includes direct communication (using institutional emails + SLAC emails) and utilizing existing channels via account managers
- HelpDesk awareness

Phase 2 – Disable all UNIX accounts with expired Cyber training – 9/16

- Impact:
  - Big impact on user community (LCLS, Fundamental Physics, etc.)
  - Potential critical impact on users who think they can re-enable their accounts, and *then* do their training (current practice)

- Communication: extensive starting now.
- User communication includes direct communication (using institutional emails + SLAC emails) and utilizing existing channels via account managers
- HelpDesk awareness

- No grace period

Between Phase 2 and Phase 3 – manual effort

- Daily generated report on accounts with expired Cyber training, John B will disable those

- Exclude the accounts created 5 or fewer days ago

Phase 3 – Not allow the creation of new UNIX or Windows accounts without Cyber training completion

Long term solution, and additional analysis is required.

- Discussion with groups involved in accounts creation: URAWI, LCLS User Gateway, HelpDesk.
- Unified process between UNIX and AD accounts creation
- Plan for more testing, bigger communication and change management effort

Special considerations

- Special UNIX role / service accounts (exclude from pool)
- Shared accounts
- **Any other special cases we need to think about?**

Discussion, questions

- Anything important we need to consider?

Accounts, timelines, user impact, processes, communication, groups to be involved in discussion, etc.

Please email questions/concerns to:

PM: Olga - obykov@slac.stanford.edu

Cyber: Otha - ols3rd@slac.stanford.edu