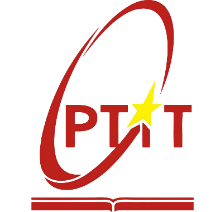
**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**

-------🙞🙜🕮🙞🙜-------



**Báo cáo bài thực hành**

**Tìm hiểu về công cụ libpam-pwquality**

Sinh viên thực hiện:

B20DCAT59 Nguyễn Cảnh HIếu

Giảng viên hướng dẫn: TS.Phạm Hoàng Duy

MỤC LỤC

[MỤC LỤC 1](#_Toc186697245)

[DANH MỤC CÁC HÌNH VẼ 2](#_Toc186697246)

[DANH MỤC CÁC BẢNG BIỂU 2](#_Toc186697247)

[1.1 Giới thiệu chung về bài thực hành 3](#_Toc186697248)

[1.2 Nội dung và hướng dẫn bài thực hành 3](#_Toc186697249)

[1.2.1 Mục đích 3](#_Toc186697250)

[1.2.2 Yêu cầu đối với sinh viên 3](#_Toc186697251)

[1.2.3 Nội dung thực hành 3](#_Toc186697252)

[1.3 Phân tích yêu cầu bài thực hành 4](#_Toc186697253)

[1.4 Thiết kế bài thực hành 4](#_Toc186697254)

[1.5 Cài đặt và cấu hình các máy ảo 6](#_Toc186697255)

[1.6 Tích hợp và triển khai 7](#_Toc186697256)

[***1.6.1 Docker Hub*** 7](#_Toc186697257)

[***1.6.2 Github*** 8](#_Toc186697258)

[1.7 Thử nghiệm và đánh giá 8](#_Toc186697259)

[TÀI LIỆU THAM KHẢO 16](#_Toc186697260)

DANH MỤC CÁC HÌNH VẼ

[Hình 1 Giao diện Labedit của bài lab 6](#_Toc186697261)

[Hình 2 Cài đặt phần Result 7](#_Toc186697262)

[Hình 3 Dockerfiles của máy libpam 7](#_Toc186697263)

[Hình 4 Treataslocal của libpam 7](#_Toc186697264)

[Hình 5 Đẩy các vùng chứa lên dockerhub 8](#_Toc186697265)

[Hình 6 Đã đẩy lên docker 8](#_Toc186697266)

[Hình 7 IP của máy libpam 8](#_Toc186697267)

[Hình 8 Version của libpam-pwquality 9](#_Toc186697268)

[Hình 9 Cấu hình mật khẩu trung bình 9](#_Toc186697269)

[Hình 10 Checkwork nhiệm vụ 1 10](#_Toc186697270)

[Hình 11 Cài đặt mật khẩu thành công 10](#_Toc186697271)

[Hình 12 Cập nhật mật khẩu mới thành công 11](#_Toc186697272)

[Hình 13 Checkwork nhiệm vụ 2 11](#_Toc186697273)

[Hình 14 Cấu hình mật khẩu mạnh 15](#_Toc186697274)

[Hình 15 Checkwork nhiệm vụ 3 15](#_Toc186697275)

[Hình 16 Thiết lập chính sách hết hạn mật khẩu 16](#_Toc186697276)

[Hình 17 Checkword nhiệm vụ 4 16](#_Toc186697277)

DANH MỤC CÁC BẢNG BIỂU

[Bảng 1. Bảng Result 5](#_Toc186697278)

* 1. Giới thiệu chung về bài thực hành

Bài thực hành " Tìm hiểu về công cụ libpam-pwquality " được thiết kế nhằm để tìm hiểu cách thức hoạt động, sự dụng libpam-pwquality để quản lý mật khẩu người dùng trong linux. Hiểu rõ tầm quan trọng của việc sử dụng mật khẩu mạnh trong bảo mật hệ thống, các tiêu chí đánh giá một mật khẩu mạnh (độ dài, tính phức tạp, không dễ đoán) và nhận thức về các nguy cơ bảo mật liên quan đến mật khẩu yếu. Việc cấu hình mật khẩu giúp nâng cao ý thức bảo vệ cũng như giảm nguy cơ bị tấn công và xâm nhập trái phép.

* 1. Nội dung và hướng dẫn bài thực hành
     1. Mục đích

Bài thực hành này nhằm giúp sinh viên nắm vững các tiêu chí đánh giá mật khẩu trong libpam-pwquality, qua đó thiết lập các cấu hình và áp dụng mật khẩu trung bình và mạnh với người dùng. Cũng như sẽ phát triển kỹ năng giải quyết vấn đề, làm quen với môi trường ảo hóa và áp dụng kiến thức vào thực tế, nâng cao sự tự tin khi làm việc với hệ điều hành Linux.

* + 1. Yêu cầu đối với sinh viên

Có kiến thức cơ bản về hệ điều hành Linux, và công cụ libpam-pwquality

* + 1. Nội dung thực hành

Khởi động bài lab:

* Vào terminal, gõ:

*Labtainer oss\_ac\_libpam\_n3\_hieu\_4 -r*

*(chú ý: sinh viên sử dụng mã sinh viên của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)*

Sau khi khởi động xong terminal **libpam** ảo sẽ xuất hiện

Trên terminal **libpam** thực hiện kiểm tra, cài đặt libpam-pwquality. Tìm hiểu các tính năng, tùy chọn để cấu hình mật khẩu libpam-pwquality với người dùng

* Kết thúc bài lab:

Trên terminal đầu tiên sử dụng câu lệnh sau để kết thúc bài lab:

*stoplab oss\_ac\_libpam\_n3\_hieu\_4 -r*

Khi bài lab kết thúc, một tệp zip lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới stoplab.

* Khởi động lại bài lab:

Trong quá trình làm bài sinh viên cần thực hiện lại bài lab, dùng câu lệnh:

*startlab oss\_ac\_libpam\_n3\_hieu\_4 -r*

* 1. Phân tích yêu cầu bài thực hành

Bài thực hành gồm một máy ảo **libpam**. Để hoàn thành bài thực hành sinh viên cần thực hiện quan sát, cấu hình, áp dụng mật khẩu trung bình với các yêu cầu có sẵn, sau đó nâng cấp mật khẩu phức tập hơn, cuối cùng thiết lập chính sách hết hạn mật khẩu.

* 1. Thiết kế bài thực hành

Trên môi trường máy ảo Ubuntu được cung cấp, sử dụng docker để tạo ra một container: container mang tên “**libpam**” là một máy tính ảo chạy hệ điều hành Linux đóng vai trò chính trong bài thực hành.

Cấu hình docker gồm có:

* config: lưu cấu hình hoạt động của hệ thống
* dockerfiles: mô tả cấu hình của container
* Các nhiệm vụ cần phải thực hiện để thực hành thành công:
* Cấu hình PAM để sử dụng libpam-pwquality với mật khẩu trung bình với yêu cầu “Người dùng được nhập lại mật khẩu tối đa 3 lần, Độ dài tối thiểu của mật khẩu là 8 ký tự, Mật khẩu mới phải khác mật khẩu cũ ít nhất 2 ký tự và có hai loại ký tự khác nhau”
* Tạo người dùng mới và tiến hành thay đổi mật khẩu để thử nghiệm các yêu cầu đã được đáp ứng hay chưa
* Tìm hiểu thêm các tùy chọn nâng cao trong libpam-pwquality để tiến hành nâng câp mật phức tạp và an toàn hơn với yêu cầu “Người dùng được nhập lại mật khẩu tối đa 3 lần, độ dài tối thiểu của mật khẩu là 12 ký tự, mật khẩu mới phải khác mật khẩu cũ ít nhất 2 ký tự và có 3 loại ký tự khác nhau, giới hạn số lượng ký tự giống nhau liên tiếp tối đa là 2, Giới hạn số lượng ký tự liên tiếp theo thứ tự tối đa là 3”
* Thiết lập chính sách hết hạn mật khẩu ở tệp /etc/login.defs với các tham số PASS\_MAX\_DAYS, PASS\_MIN\_DAYS, PASS\_WARN\_AGE

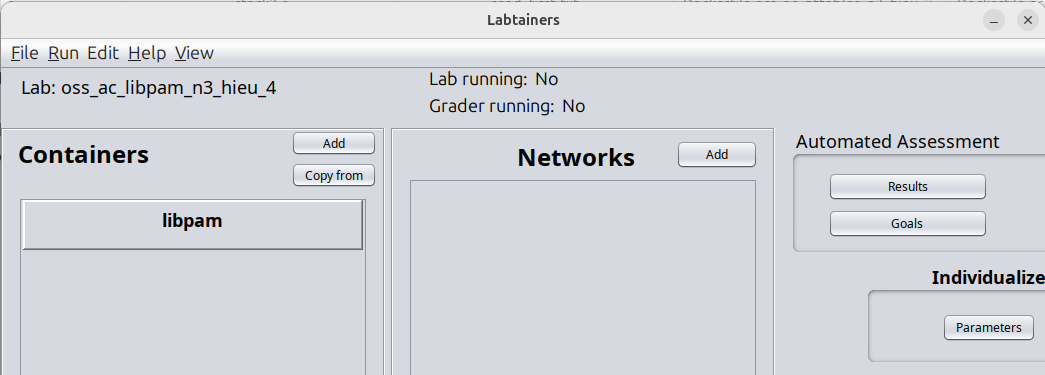
Kết thúc bài lab và đóng gói kết quả.

Để đánh giá được sinh viên đã hoàn thành bài thực hành hay chưa, cần chia bài thực hành thành các nhiệm vụ nhỏ, mỗi nhiệm vụ cần phải chỉ rõ kết quả để có thể dựa vào đó đánh giá, chấm điểm. Do vậy, trong bài thực hành này hệ thống cần ghi nhận các thao tác, sự kiện được mô tả và cấu hình như bảng 1:

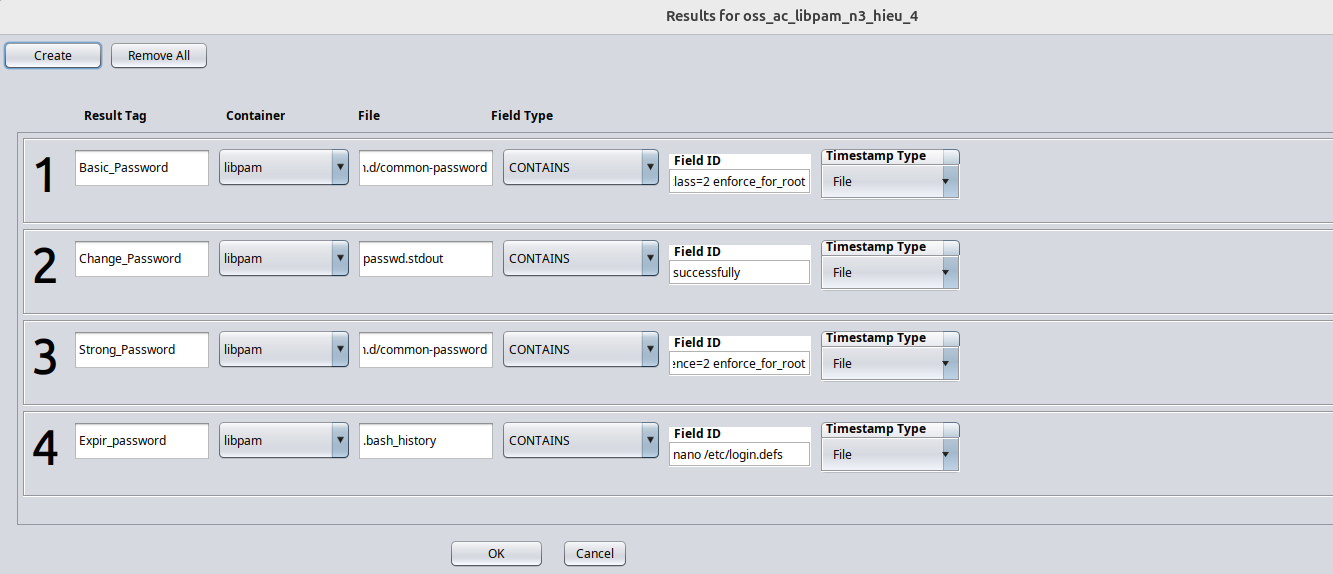
1. Bảng Result

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Result Tag | Container | File | Field Type | Field ID | Timestamp Type |
| Basic\_Password | libpam | /etc/pam.d/common-password | CONTAINS | retry=3 minlen=8 minclass=2 enforce\_for\_root | File |
| Change\_Password | libpam | passwd.stdout | CONTAINS | successfully | File |
| Strong\_Password | libpam | /etc/pam.d/common-password | CONTAINS | retry=3 minlen=12 difok=2 minclass=3 maxrepeat=2 maxsequence=2 enforce\_for\_root | File |
| Expir\_password | libpam | .bash\_history | CONTAINS | nano /etc/login.defs | File |

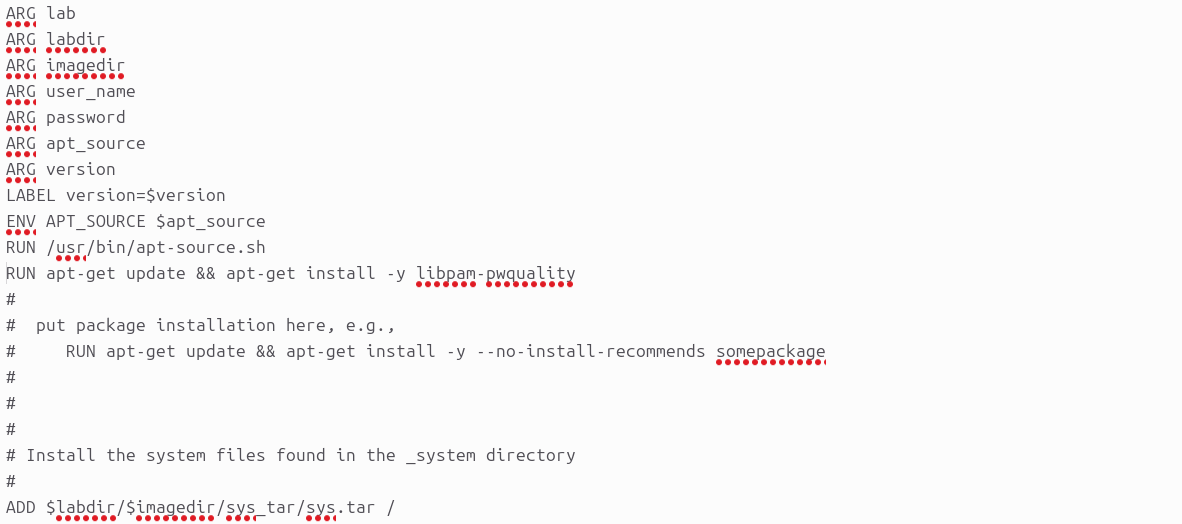
* Basic\_Password: Cấu hình PAM để sử dụng libpam-pwquality với mật khẩu trung bình.
* Change\_Password: Thêm người dùng mới và thực hiện thử nghiệm mật khẩu sau cấu hình
* Strong\_Password: Cấu hình PAM để sử dụng libpam-pwquality với mật khẩu khó.
* Expir\_password: Thiết lập chính sách hết hạn mật khẩu
  1. Cài đặt và cấu hình các máy ảo



1. Giao diện Labedit của bài lab



1. Cài đặt phần Result



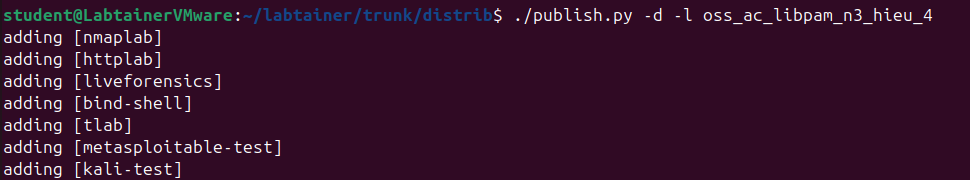
1. Dockerfiles của máy libpam



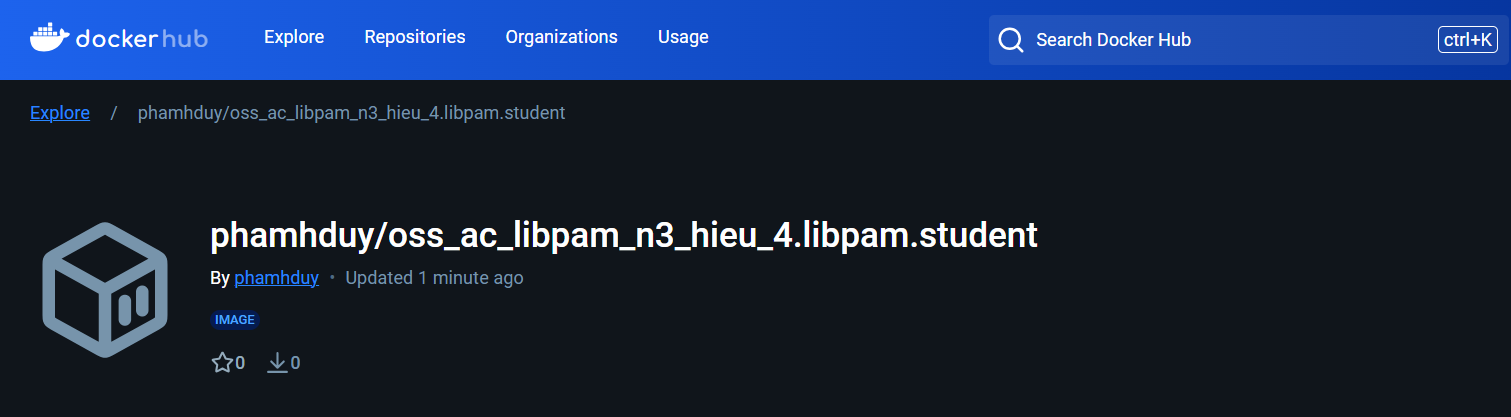
1. Treataslocal của libpam
   1. Tích hợp và triển khai

Bài thực hành đã được triển khai như sau:

***Docker Hub***

https://hub.docker.com/r/phamhduy/oss\_ac\_libpam\_n3\_hieu\_4.libpam.student

1. Đẩy các vùng chứa lên dockerhub

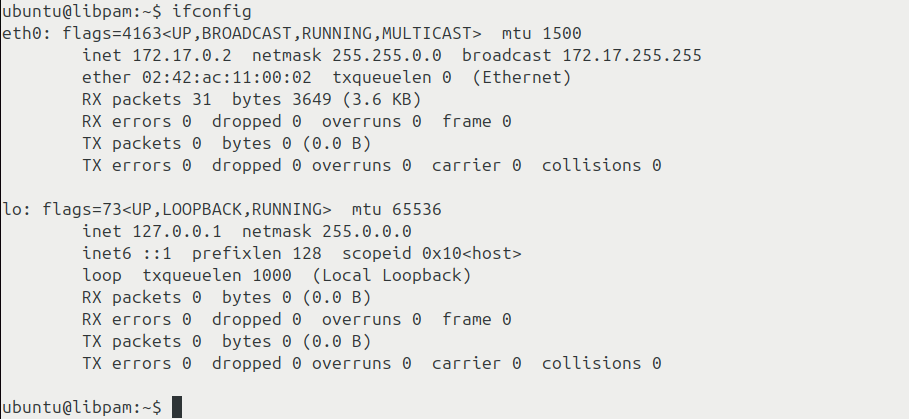


1. Đã đẩy lên docker

***Github***

* 1. Thử nghiệm và đánh giá

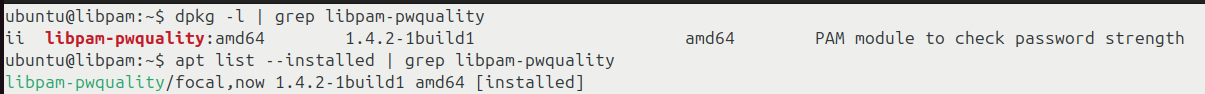
Bài thực hành đã được xây dựng thành công, dưới đây là hình ảnh minh họa về bài thực hành:



1. IP của máy libpam

kiểm tra libpam-pwquality đã được cài đặt thành công trên máy chưa sử dung: *“dpkg -l | grep libpam-pwquality”* hoặc *“apt list --installed | grep libpam-pwquality”*

kết quả mong muốn:



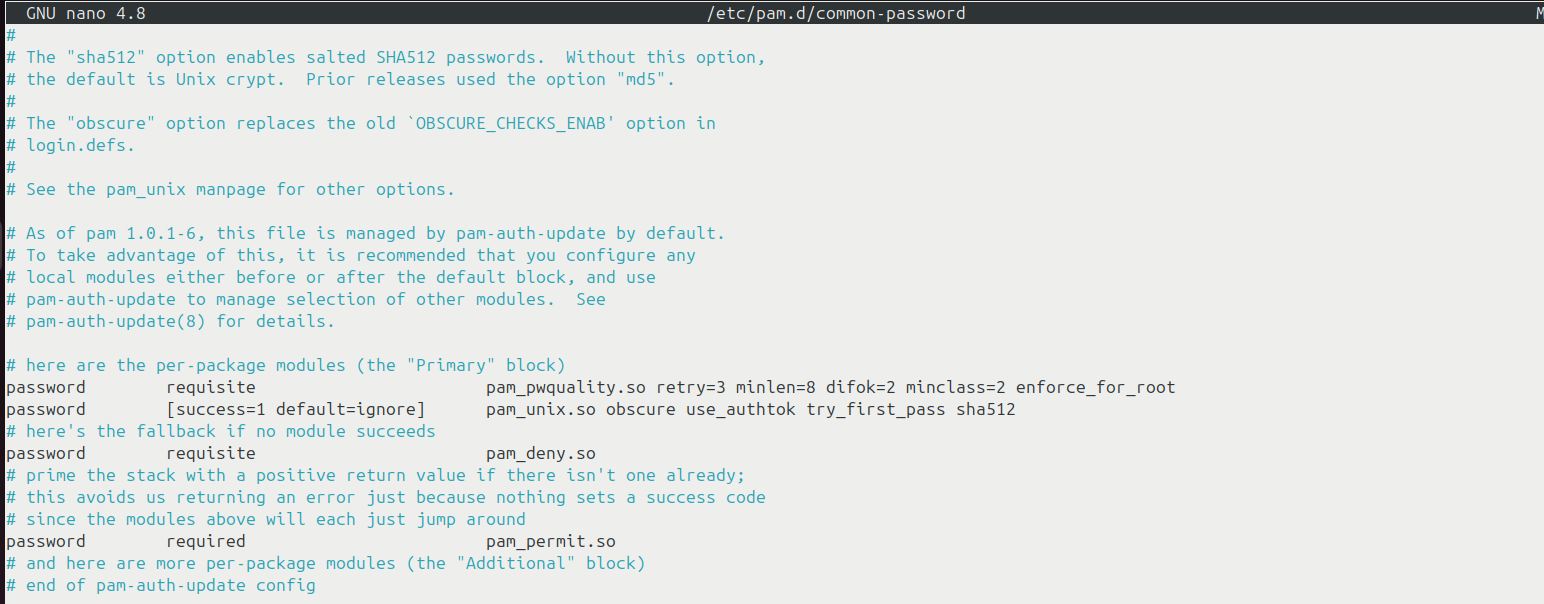
1. Version của libpam-pwquality

Nếu chưa được cài đặt thì sử dụng lệnh dưới để cài đặt và kiểm tra lại:

* *sudo apt-get update*
* *sudo apt-get install -y libpam-pwquality*
* ***Nhiệm vụ 1:***  Cấu hình PAM để sử dụng libpam-pwquality với mật khẩu trung bình

Mở tệp cấu hình: “*sudo nano /etc/pam.d/common-password”*, tiến hành cấu hình này yêu cầu một mật khẩu đủ bảo mật nhưng không quá nghiêm ngặt, thích hợp cho hệ thống có mức độ bảo mật vừa phải. lưu và đóng tệp.

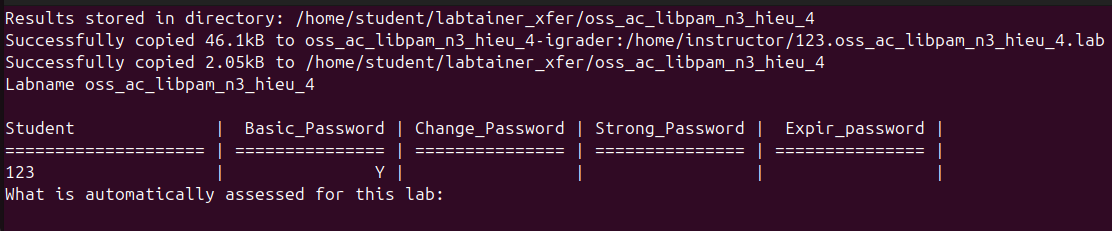
Yêu cầu: Người dùng được nhập lại mật khẩu tối đa 3 lần, Độ dài tối thiểu của mật khẩu là 8 ký tự, Mật khẩu mới phải khác mật khẩu cũ ít nhất 2 ký tự và có hai loại ký tự khác nhau.



1. Cấu hình mật khẩu trung bình

Giải thích: “*retry=3 minlen=8 difok=2 minclass=2 enforce\_for\_root”*

* + retry = 3: Người dùng được nhập lại mật khẩu tối đa 3 lần.
  + minlen = 8: Độ dài tối thiểu của mật khẩu là 8 ký tự.
  + difok = 2: Mật khẩu mới phải khác mật khẩu cũ ít nhất 2 ký tự.
  + minclass = 2 có ít nhất hai loại ký tự trong (digits, uppercase, lowercase, others)



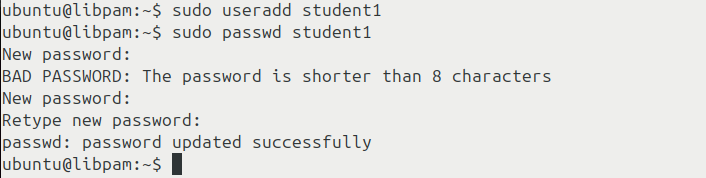
1. Checkwork nhiệm vụ 1

* ***Nhiệm vụ 2:*** Tiến hành adduser mới và thử ngiệm mật khẩu.

Sử dụng “*sudo useradd student1”* để thêm người dùng mới mang tên student1, sau đó thực hiện đặt mật khẩu mới bằng “*sudo paswd student*”.

Ở lần đầu thử với mật khẩu không đủ điều kiện: 123 🡺 yêu cầu kết quả cần nhận được là không chấp nhận và yêu cầu nhập mật khẩu khác.

Lần thứ hai sẽ nhập mật khẩu đúng yêu cầu: Test1357 🡺 yêu cầu kết quả cần nhận được là nhập lại mật khẩu và được thay đổi thành công.

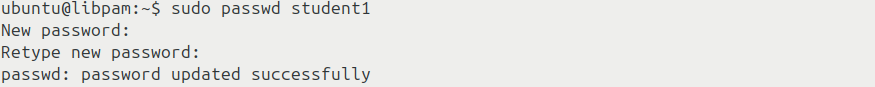


1. Cài đặt mật khẩu thành công

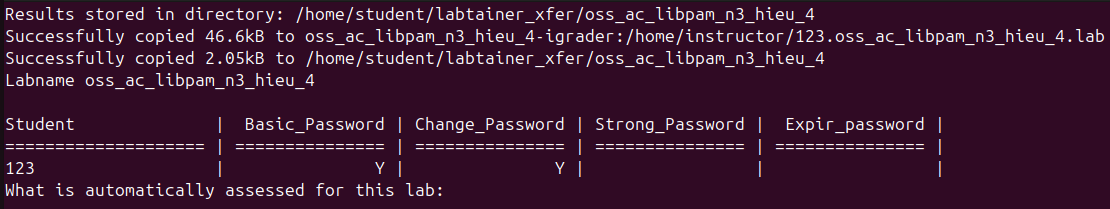
Tiếp tục ta thay đổi mật khẩu cho student1 khi đã có mật khẩu cũ

Lần đầu thử với mật khẩu : Test13578 🡺 kết quả yêu cần nhận được là mật khẩu không được chấp nhận do chỉ có 1 ký tự khác so với mật khẩu cũ.

Tiếp theo thử với một mật khẩu hợp lệ khác: Test123test 🡺 yêu cầu kết quả cần nhận được là nhập lại mật khẩu và được thay đổi thành công.



1. Cập nhật mật khẩu mới thành công



1. Checkwork nhiệm vụ 2

* ***Nhiệm vụ 3:*** Tìm hiểu thêm các tùy chọn nâng cao trong libpam-pwquality để tiến hành nâng câp mật khẩu phức tạp và an toàn hơn

1. retry

* Cú pháp: retry=N
* Ý nghĩa: Cho phép người dùng thử nhập lại mật khẩu tối đa N lần nếu mật khẩu không đáp ứng yêu cầu.
* Mặc định: 1
* Ví dụ: retry=3 🡺 người dùng có thể thử lại 3 lần

2. minlen

* Cú pháp: minlen=N
* Ý nghĩa: Độ dài tối thiểu của mật khẩu.
* Mặc định: 8
* Ví dụ: minlen=12 🡺 mật khẩu ít nhât có 12 ký tự

3. difok

* Cú pháp: difok=N
* Ý nghĩa: Số ký tự tối thiểu phải khác nhau giữa mật khẩu mới và mật khẩu cũ.
* Mặc định: 5
* Ví dụ: difok=4 🡺 cần có 4 ký tự với mật khẩu cũ(nếu đã có mật khẩu trước đó)

4. dcredit

* Cú pháp: dcredit=N
* Ý nghĩa: Số ký tự số (digits) yêu cầu trong mật khẩu:
* Nếu N > 0: Giảm yêu cầu, cho phép mật khẩu thiếu N ký tự số.
* Nếu N < 0: Bắt buộc mật khẩu phải chứa ít nhất |N| ký tự số.
* Mặc định: 0
* Ví dụ: dcredit=-1 🡺 Mật khẩu bắt buộc phải có ít nhất 1 chữ số.

5. ucredit

* Cú pháp: ucredit=N
* Ý nghĩa: Số ký tự chữ cái viết hoa (uppercase) yêu cầu trong mật khẩu:
* Nếu N > 0: Giảm yêu cầu, cho phép mật khẩu thiếu N ký tự viết hoa.
* Nếu N < 0: Bắt buộc mật khẩu phải chứa ít nhất |N| ký tự viết hoa.
* Mặc định: 0
* Ví dụ: ucredit=-1 🡺 Mật khẩu bắt buộc phải có ít nhất 1 chữ cái viết hoa.

6. lcredit

* Cú pháp: lcredit=N
* Ý nghĩa: Số ký tự chữ cái viết thường (lowercase) yêu cầu trong mật khẩu:
* Nếu N > 0: Giảm yêu cầu, cho phép mật khẩu thiếu N ký tự viết thường.
* Nếu N < 0: Bắt buộc mật khẩu phải chứa ít nhất |N| ký tự viết thường.
* Mặc định: 0
* Ví dụ: lcredit=-1 🡺 Mật khẩu bắt buộc phải có ít nhất 1 chữ cái viết thường.

7. ocredit

* Cú pháp: ocredit=N
* Ý nghĩa: Số ký tự đặc biệt (như @, #, $, v.v.) yêu cầu trong mật khẩu.
* Nếu N > 0: Giảm yêu cầu, cho phép mật khẩu thiếu N ký tự đặc biệt.
* Nếu N < 0: Bắt buộc mật khẩu phải chứa ít nhất |N| ký tự đặc biệt.
* Mặc định: 0
* Ví dụ: ocredit=-1 🡺 Mật khẩu bắt buộc phải có ít nhất 1 ký tự đặc biệt.

8. enforce\_for\_root

* Cú pháp: enforce\_for\_root
* Ý nghĩa: Áp dụng các quy tắc kiểm tra mật khẩu cho cả tài khoản root.
* Mặc định: Không áp dụng (trừ khi được chỉ rõ).
* Ví dụ: enforce\_for\_root

9. maxrepeat

* Cú pháp: maxrepeat=N
* Ý nghĩa: Số ký tự lặp lại liên tiếp tối đa được phép trong mật khẩu.
* Mặc định: 0 (không kiểm tra).
* Ví dụ: maxrepeat=3 🡺 Không cho phép hơn 3 ký tự lặp lại liên tiếp (ví dụ: aaa, 111).

10. maxclassrepeat

* Cú pháp: maxclassrepeat=N
* Ý nghĩa: Số lần lặp lại tối đa cho các nhóm ký tự (như số, chữ hoa, chữ thường, ký tự đặc biệt).
* Mặc định: Không kiểm tra.
* Ví dụ: maxclassrepeat=2

11. reject\_username

* Cú pháp: reject\_username
* Ý nghĩa: Không cho phép mật khẩu chứa tên đăng nhập hoặc các chuỗi liên quan đến tên đăng nhập.
* Mặc định: Không áp dụng.
* Ví dụ: reject\_username

12. dictcheck

* Cú pháp: dictcheck
* Ý nghĩa: Kiểm tra mật khẩu trong từ điển (tệp từ điển được cấu hình trong /etc/security/pwquality.conf).
* Mặc định: Được bật.
* Ví dụ: dictcheck

13. badwords

* Cú pháp: badwords=word1,word2,...
* Ý nghĩa: Chỉ định danh sách các từ không được sử dụng trong mật khẩu.
* Mặc định: Không có từ nào.
* Ví dụ: badwords=password,1234 🡺 mật khẩu không được sử dụng password và 1234

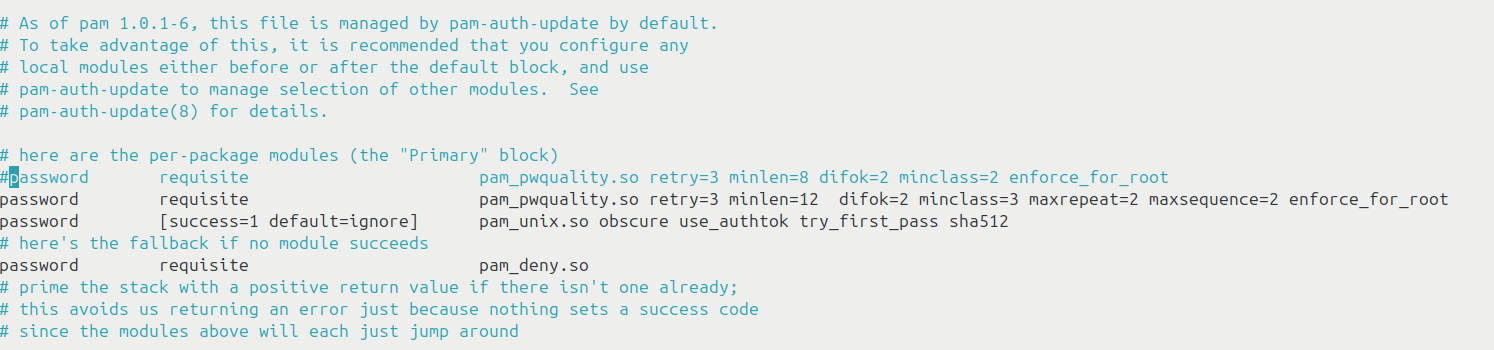
14. usercheck

* Cú pháp: usercheck
* Ý nghĩa: Kiểm tra mật khẩu để đảm bảo không giống với tên người dùng.
* Mặc định: Bật.

15. gecoscheck

* Cú pháp: gecoscheck
* Ý nghĩa: Kiểm tra mật khẩu để đảm bảo không chứa các thông tin cá nhân từ trường gecos (ví dụ: tên đầy đủ, số điện thoại).
* Mặc định: Không bật.
* Ví dụ: gecoscheck

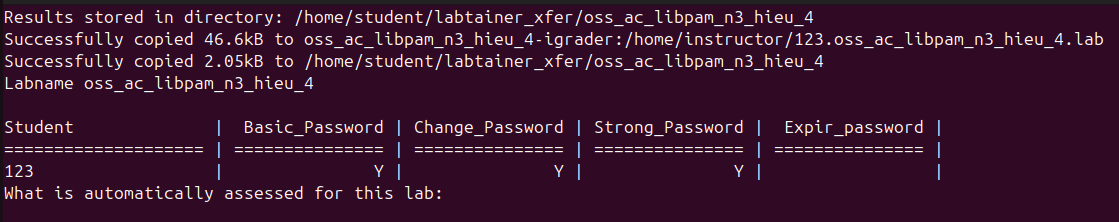
Yêu cầu “Người dùng được nhập lại mật khẩu tối đa 3 lần, độ dài tối thiểu của mật khẩu là 12 ký tự, mật khẩu mới phải khác mật khẩu cũ ít nhất 2 ký tự và có 3 loại ký tự khác nhau, giới hạn số lượng ký tự giống nhau liên tiếp tối đa là 2, Giới hạn số lượng ký tự liên tiếp theo thứ tự tối đa là 3”.

******

1. Cấu hình mật khẩu mạnh

Tiến hành thay đổi mật khẩu người dùng như ở nhiệm vụ hai để xác nhận cấu hình mật khẩu đẫ được áp dụng.

Lưu ý cần # dòng cấu hình mật khẩu trung bình để có thể lưu giữ bằng chứng checkword



1. Checkwork nhiệm vụ 3

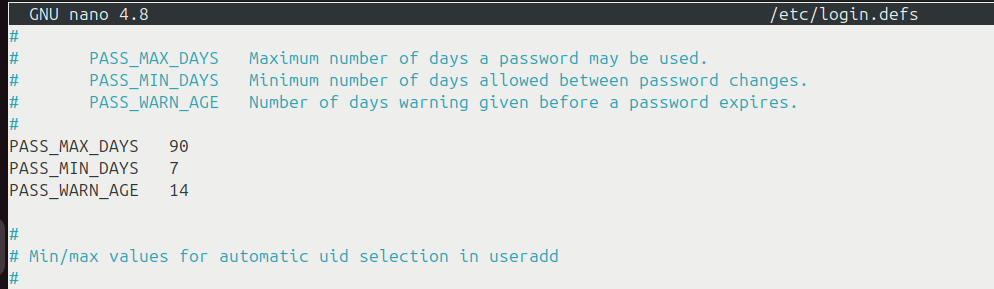
* ***Nhiệm vụ 4:*** Thiết lập chính sách hết hạn mật khẩu

Để thiết lập chính sách hết hạn mật khẩu, cần chỉnh sửa tệp /etc/login.defs

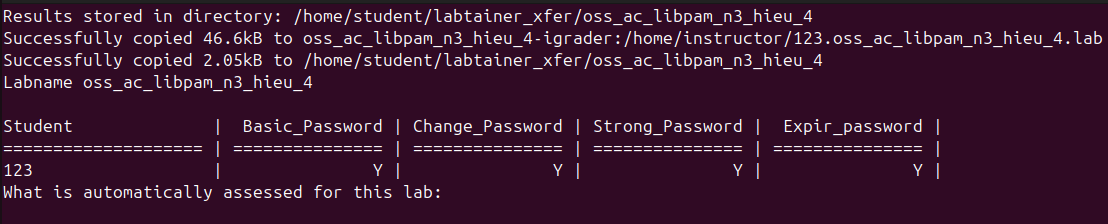
* *sudo nano /etc/login.defs*

Chỉnh sửa các tham số sau rồi lưu và đóng tệp:

* PASS\_MAX\_DAYS: Số ngày tối đa mật khẩu có thể được sử dụng.
* PASS\_MIN\_DAYS: Số ngày tối thiểu giữa các lần thay đổi mật khẩu.
* PASS\_WARN\_AGE: Số ngày trước khi mật khẩu hết hạn mà người dùng sẽ được cảnh báo



1. Thiết lập chính sách hết hạn mật khẩu



1. Checkword nhiệm vụ 4

TÀI LIỆU THAM KHẢO