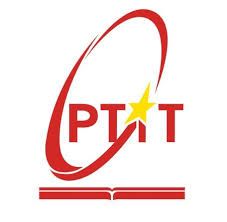
**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG KHOA AN TOÀN THÔNG TIN**

-----  -----



BÁO CÁO XÂY DỰNG LAB TRÊN NỀN TẢNG LABTAINER

Chủ đề: Nghiên cứu và xây dựng các bài thực hành dựa trên khung Mitre Att&ck trong kiểm thử xâm nhập

Lab: T1098: Account Manipulation

Giảng viên hướng dẫn: TS. Nguyễn Ngọc Điệp

Sinh viên thực hiện: Trần Quang Huy – B20DCAT085

Lớp: D20CQAT01-B

**Hà Nội - 2024**

**MỤC LỤC**

[Bài thực hành: Tìm hiểu về technique T1098: Account Manipulation 3](#_Toc185386918)

[1. Giới thiệu chung về bài thực hành. 3](#_Toc185386919)

[2. Nội dung và hướng dẫn bài thực hành 3](#_Toc185386920)

[3. Phân tích yêu cầu bài thực hành 5](#_Toc185386921)

[4. Thiết kế bài thực hành 5](#_Toc185386922)

[5. Cài đặt và cấu hình các máy ảo 8](#_Toc185386923)

[6. Tích hợp và triển khai 11](#_Toc185386924)

[7. Thử nghiệm và đánh giá 13](#_Toc185386925)

**MỤC LỤC HÌNH ẢNH**

Hình 1. Giao diện Labedit của bài lab

Hình 2. Cài đặt phần Result

Hình 3. Dockerfiles của máy attacker

Hình 4. Dockerfiles của victim

Hình 5. Add và commit bài lab

Hình 6. Đẩy các vùng chứa lên dockerhub

Hình 7. Tạo imodule.tar chứa bài thực hành

Hình 8. Các vùng chứa được đẩy lên dockerhub

Hình 9. File imodule.tar chứa bài thực hành

Hình 10. Đẩy file imodule.tar lên github

Hình 11. Imodule bài lab về máy

Hình 12. SSH vào máy victim

Hình 13. List ra các lệnh sudo mà user1 được phép dùng

Hình 14. Tạo user2 với quyền root và đặt mật khẩu cho user đó

Hình 15. Switch sang user2 và đổi thời hạn tối đa giữa các lần đổi mật khẩu cho user1

Hình 16. Kiểm tra tiến độ hoàn thành bài lab

Bài thực hành: Tìm hiểu về technique T1098: Account Manipulation

1. Giới thiệu chung về bài thực hành.

Bài thực hành *"Tìm hiểu về technique T1098: Account Manipulation"* được thiết kế nhằm giúp sinh viên hiểu rõ hơn về kỹ thuật Account Manipulation, một phương thức tấn công quan trọng trong lĩnh vực an ninh mạng. Kỹ thuật này tập trung vào việc thao túng tài khoản người dùng nhằm đạt được quyền truy cập hoặc duy trì sự hiện diện trong hệ thống mục tiêu.

Trong bài thực hành này, sinh viên sẽ tìm hiểu cách thao túng tài khoản trên hệ thống Linux để duy trì quyền truy cập và leo thang đặc quyền. Lấy bối cảnh là kẻ tấn công sau khi có thể truy cập được vào máy nạn nhân, sinh viên sẽ thực hiện các bước cụ thể như kết nối vào hệ thống qua SSH, kiểm tra quyền hạn của người dùng hiện tại, tạo tài khoản mới với quyền root, và chỉnh sửa thông tin tài khoản để kéo dài thời gian tồn tại của mật khẩu. Ngoài ra, sinh viên sẽ học cách kiểm tra các tệp tin hệ thống như /etc/shadow để xác minh các thay đổi đã thực hiện.

Thông qua bài thực hành này, sinh viên không chỉ hiểu cách thao túng và nâng quyền tài khoản, thay đổi thông tin tài khoản để duy trì quyền truy cập mà còn nhận thức được những rủi ro bảo mật tiềm ẩn trong việc quản lý và bảo vệ các tài khoản người dùng trên hệ thống. Điều này sẽ giúp sinh viên nâng cao kiến thức và kỹ năng về an toàn thông tin, đồng thời áp dụng kỹ thuật này trong công việc để kiểm thử, đánh giá khả năng bảo mật và phát hiện các lỗ hổng liên quan đến tài khoản trong môi trường thực tế sau này.

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

Giúp sinh viên biết được một con đường mà một attacker có thể dùng để duy trì quyền truy cập bằng cách lạm dụng cấu hình sai của máy victim, qua đó thực hiện các đặc quyền cao hơn và sửa đổi thông tin người dùng.

* + - 1. Yêu cầu đối với sinh viên

Có kiến thức cơ bản về linux, biết các lệnh thao tác cơ bản, các lệnh sudo

* + - 1. Nội dung thực hành

Khởi động bài lab:

Vào terminal, gõ:

*startlab pen\_bsic\_mitre\_t1098*

*(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 hai terminal ảo sẽ xuất hiện, một máy là ***attacker***, một máy là ***victim***.

* Bước 1: Sinh viên sử dụng thông tin máy victim đã được cung cấp trong file credential.txt có sẵn để truy cập máy victim.

***Attacker:***

*ssh <username>@<ip\_victim>*

* Bước 2: Sau khi ssh thành công vào máy victim, sinh viên thực hiện kiểm tra các quyền sudo mà user này có.

*sudo -l*

* Bước 3: Sinh viên phát hiện có lệnh sudo là useradd, passwd mà user có thể dùng. Lợi dụng nó để tạo tài khoản mới với đặc quyền cao, sinh viên dùng lệnh tạo tài khoản với quyền root:

*sudo useradd -u 0 -g 0 -o -m <username>*

-u 0 : chỉ định uid với uid 0 là user với quyền root

-g 0: chỉ định groupid với groupid 0 là nhóm tài khoản root

-o : cho phép tạo tài khoản trùng uid

-m : tạo thư mục của user này

* Bước 4: Đặt mật khẩu cho tài khoản vừa tạo:

*sudo passwd <username>*

* Bước 5: Chuyển đổi sang tài khoản vừa tạo:

*su - <username>*

* Bước 6: Thay đổi thời gian đổi mật khẩu của user mà người dùng đã có được là user1

*sudo chage -I -1 -m 0 -M 123456789 -E -1 user1*

-I -1: Xác định số ngày sau khi mật khẩu hết hạn mà vô hiệu hóa tài khoản, với -1 là không bao giờ vô hiệu hóa

-m 0: Chỉ định số ngày tối thiểu giữa các lần thay đổi mật khẩu. Với 0 là có thể thay đổi mật khẩu bất cứ lúc nào

-M 123456789: Chỉ định số ngày tối đa giữa các lần thay đổi mật khẩu, thay đổi thành 1 khoảng thời gian rất lớn 123456789

-E -1: Xác định ngày hết hạn của tài khoản, với -1 là không bao giờ hết hạn.

Kết thúc bài lab:

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

*stoplab pen\_bsic\_mitre\_t1098*

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 –r pen\_bsic\_mitre\_t1098*

1. Phân tích yêu cầu bài thực hành

Bài thực hành gồm 2 máy tính nằm trong cùng mạng LAN. Trong đó 1 máy được gọi là attacker, máy còn lại là victim. Để hoàn thành bài thực hành sinh viên cần thay đổi số ngày tối đa giữa các lần thay đổi mật khẩu của user có được ban đầu thành 1 số rất lớn (123456789).

1. Thiết kế bài thực hành

Trên môi trường máy ảo Ubuntu được cung cấp, sử dụng docker tạo ra 2 container: 1 container mang tên “attacker” và 1 container mang tên “victim”

Tạo mạng LAN có cấu hình: 172.20.0.0/24 và gateway: 172.20.0.1

Cấu hình docker gồm có:

Attacker: lưu cấu hình cho máy thực hiện tấn công, trong đó gồm có:

Tên máy: attacker

Địa chỉ trong mạng LAN: 172.20.0.10

Gateway: 172.20.0.1

Victim: lưu cấu hình cho máy mục tiêu, trong đó gồm có:

Tên máy: victim

Địa chỉ trong mạng LAN: 172.20.0.20

Gateway: 172.20.0.1

config: lưu cấu hình hoạt động của hệ thống

dockerfiles: mô tả cấu hình của 2 container: attacker và victim, trong đó:

attacker: sử dụng các thư viện mặc định hệ thống và chạy hệ điều hành centos

server: sử dụng các thư viện mặc định hệ thống và chạy hệ điều hành centos

docs: lưu phần mô tả hướng dẫn làm bài thực hành cho sinh viên.

Các nhiệm vụ cần phải thực hiện để thực hành thành công:

Sử dụng thông tin xác thực có sẵn để ssh thành công tới máy victim

Tạo thành công tài khoản có quyền root

Thực hiện thay đổi số ngày tối đa giữa các lần thay đổi mật khẩu của user có được ban đầu thành 1 số rất lớn (123456789).

Kết thúc bài lab và đóng gói kết quả.

Thiết lập hệ thống mạng sao cho máy attacker và máy victim cùng một mạng LAN.

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:

Bảng 1. Bảng Result

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Result Tag | Container | File | Field Type | Field ID | Timestamp Type |
| ssh | victim | /var/log/ssh.log | CONTAINS | Starting session | File |
| show\_permission | victim | /var/log/ssh.log | CONTAINS | COMMAND=list | File |
| add\_user | victim | /var/log/ssh.log | FILE\_REGEX | victim\s+useradd\[\d+\]:\s+new user:\s+name=\S+,\s+UID=\d+,\s+GID=\d+ | File |
| check\_user\_root | victim | /var/log/ssh.log | CONTAINS | UID=0 | File |
| increase\_password\_change\_time | victim | /etc/shadow | FILE\_REGEX | ^user1:[^:]\*:[^:]\*:[^:]\*:123456789: | File |

-ssh: ssh thành công tới máy victim.

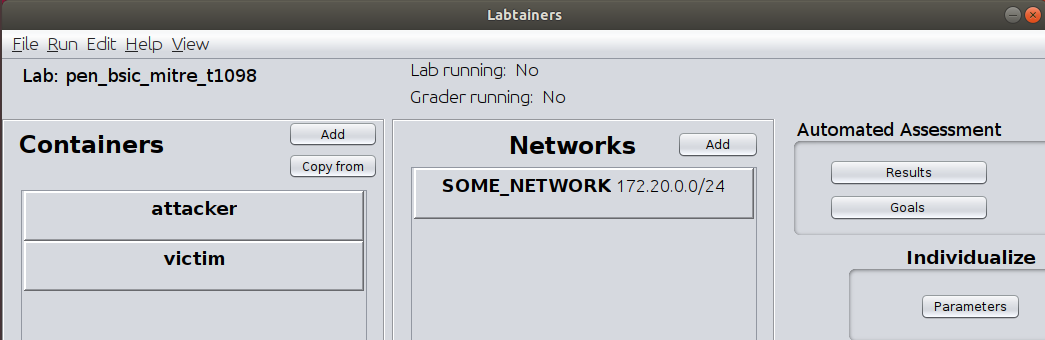
-show\_permission: list các lệnh sudo mà user có thể dùng

-add\_user: thêm thành công user mới

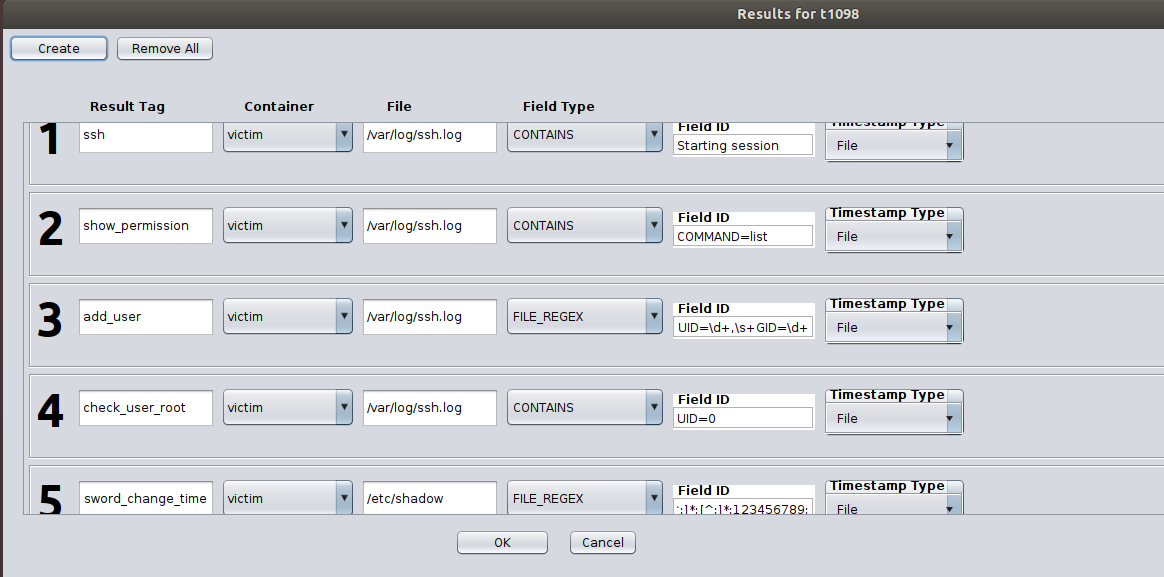
-check\_user\_root: kiểm tra xem có user nào mới là root không

-increase\_pasword\_change\_time: kiểm tra thời hạn tối đa đổi mật khẩu của user 1 có là 123456789 hay chưa

1. Cài đặt và cấu hình các máy ảo



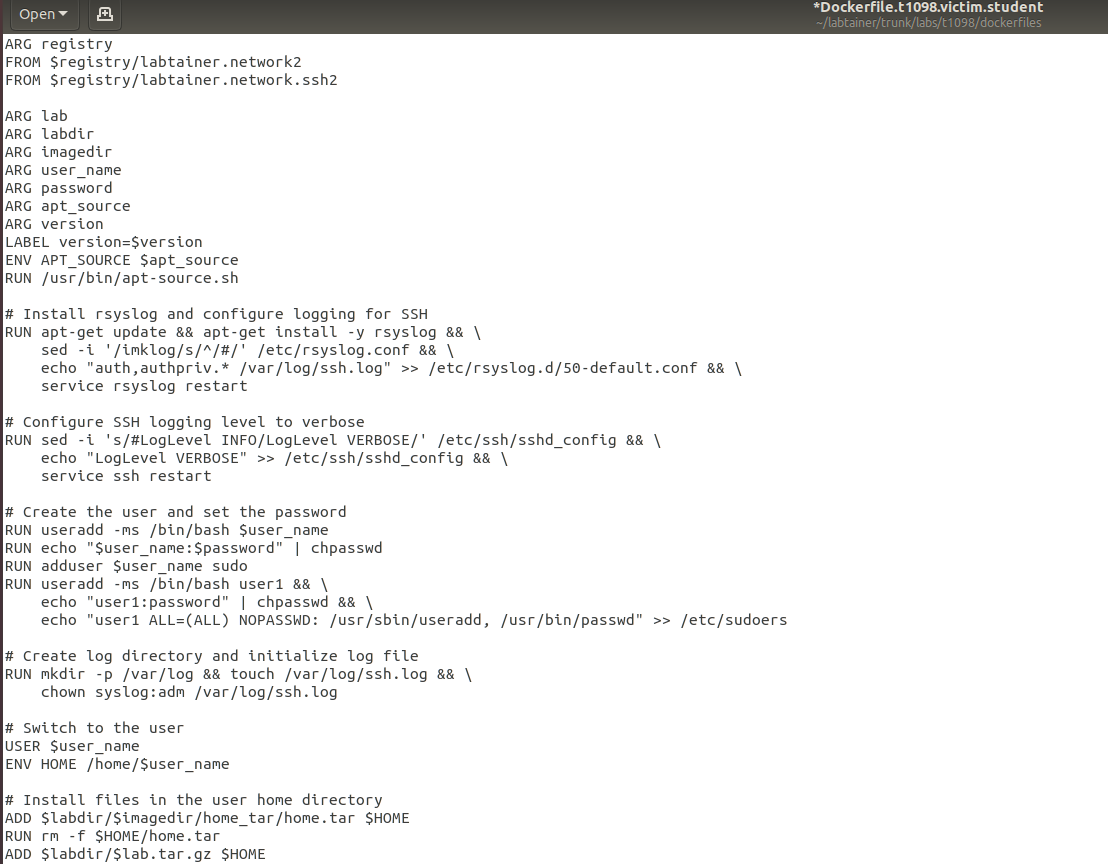
Hình 1. Giao diện Labedit của bài lab



Hình 2. Cài đặt phần Result



Hình 3. Dockerfiles của máy attacker

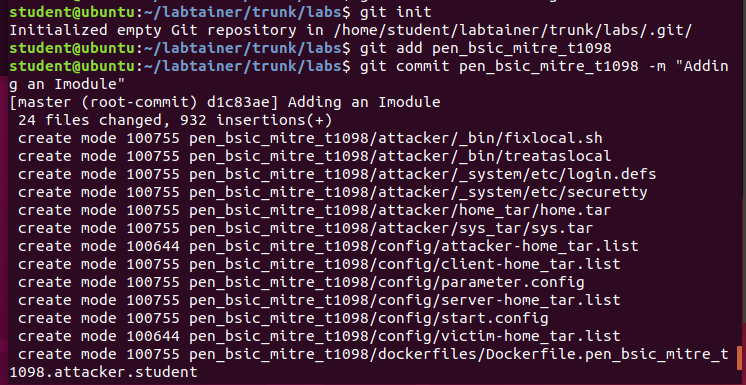


Hình 4. Dockerfiles của victim

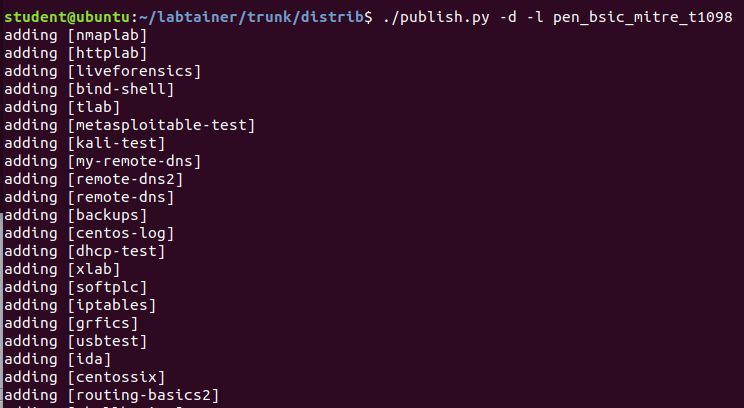
1. Tích hợp và triển khai

Bài thực hành đã được triển khai như sau:

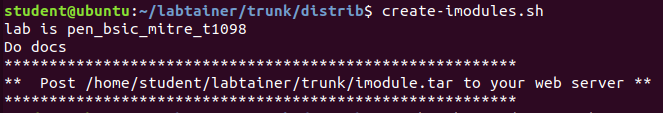
* + - * 1. Docker Hub



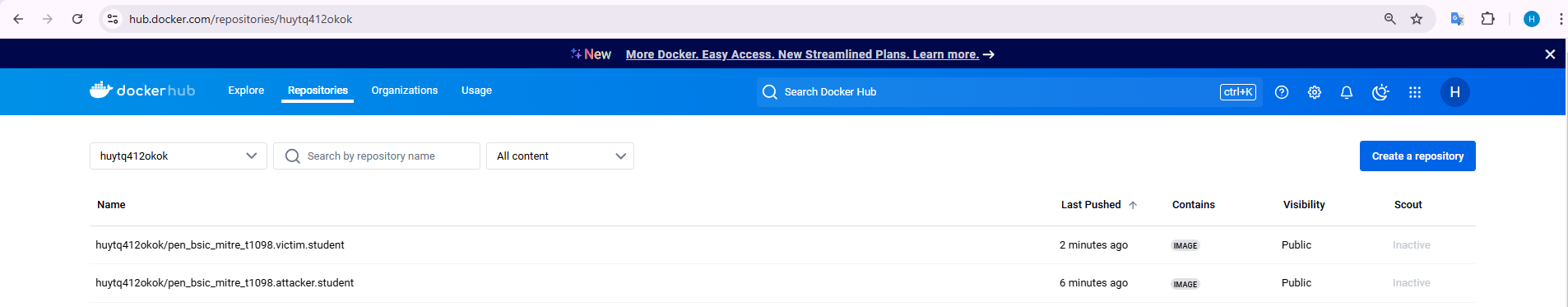
Hình 5. Add và commit bài lab



Hình 6. Đẩy các vùng chứa lên dockerhub

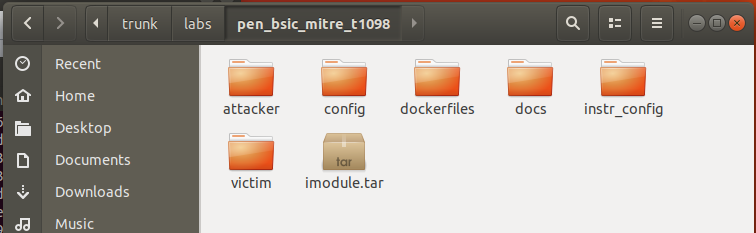


Hình 7. Tạo imodule.tar chứa bài thực hành

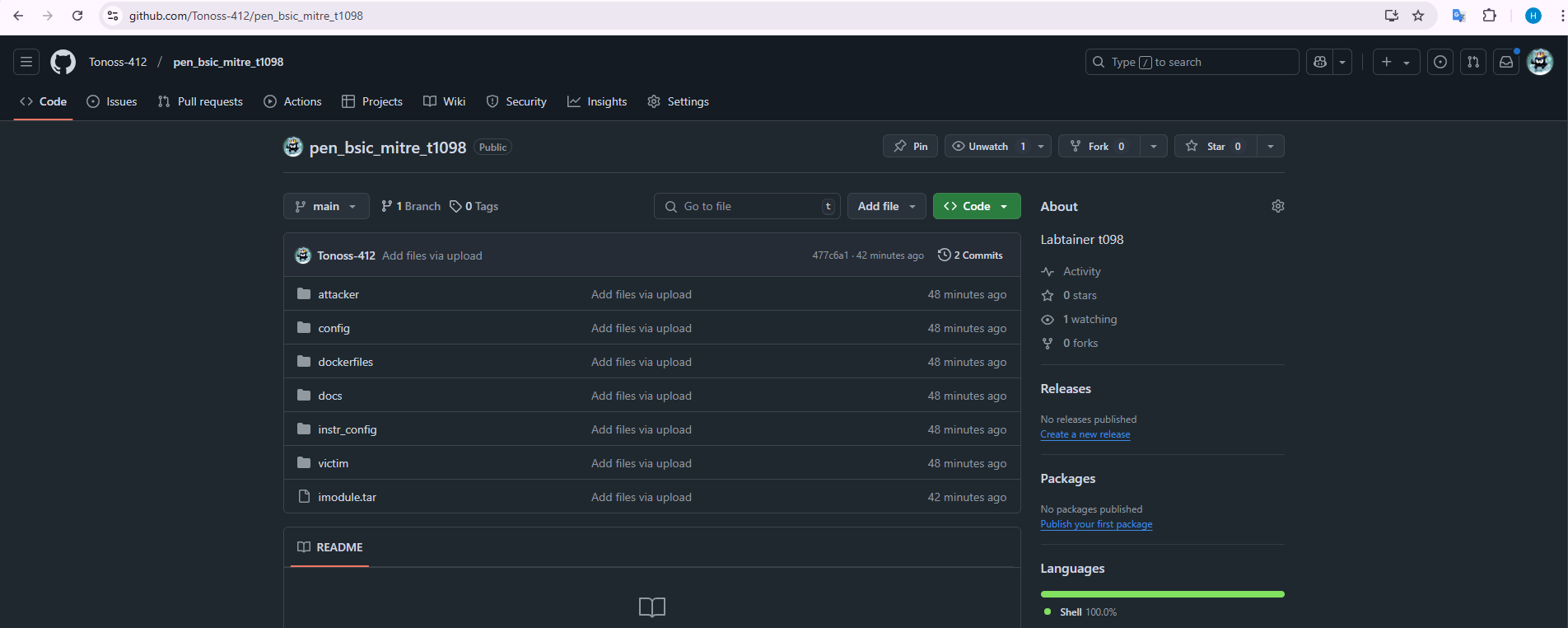


Hình 8. Các vùng chứa được đẩy lên dockerhub

* + - * 1. Github

https://github.com/Tonoss-412/pen\_bsic\_mitre\_t1098

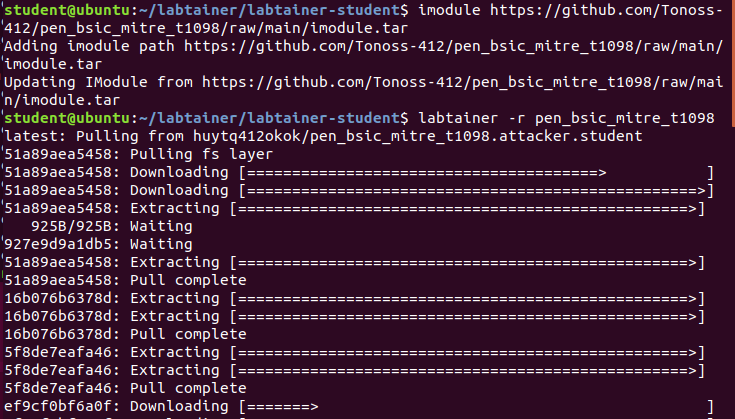
Hình 9. File imodule.tar chứa bài thực hành



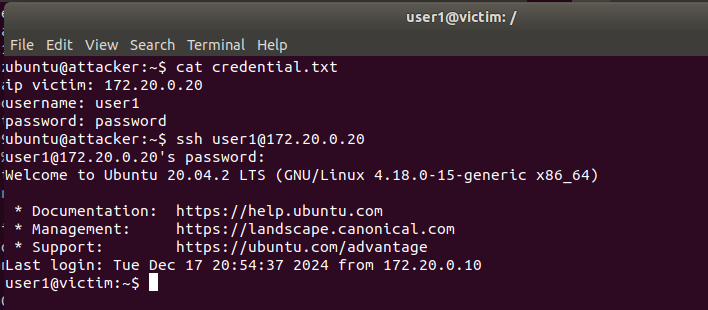
Hình 10. Đẩy file imodule.tar lên github

1. Thử nghiệm và đánh giá

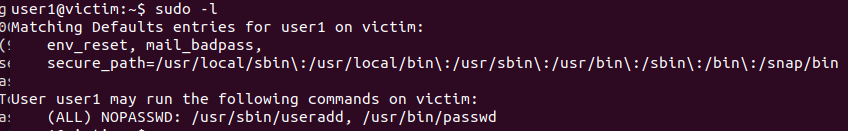
Bài thực hành đã được xây dựng thành công, dưới đây là hình ảnh minh họa về bài thực hành:



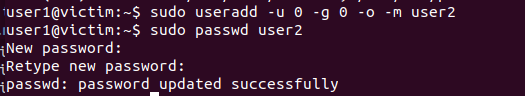
Hình 11. Imodule bài lab về máy



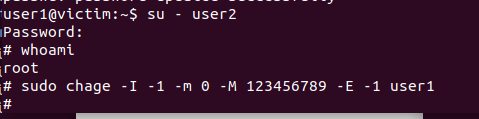
Hình 12. SSH vào máy victim



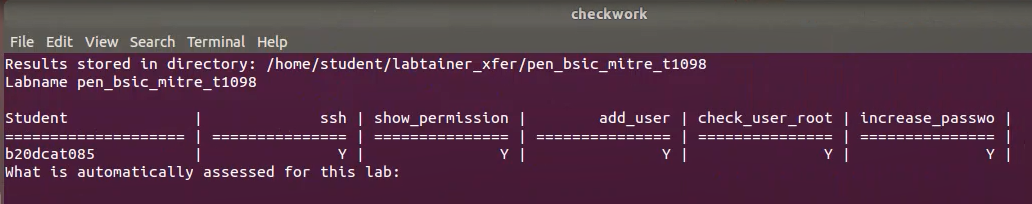
Hình 13. List ra các lệnh sudo mà user1 được phép dùng



Hình 14. Tạo user2 với quyền root và đặt mật khẩu cho user đó



Hình 15. Switch sang user2 và đổi thời hạn tối đa giữa các lần đổi mật khẩu cho user1



Hình 16. Kiểm tra tiến độ hoàn thành bài lab