**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: T1555: Credentials from Password Stores

Giảng viên hướng dẫn: TS. Nguyễn Ngọc Điệp

Sinh viên thực hiện: Trần Quang Huy – B20DCAT085

Lớp: D20CQAT01-B

**Hà Nội - 2025**

**MỤC LỤC**

[Bài thực hành: Tìm hiểu về technique T1555: Credentials from Password Stores 3](#_heading=h.gjdgxs)

[1.](#_heading=h.30j0zll) Giới thiệu chung về bài thực hành. 3

[2.](#_heading=h.1fob9te) Nội dung và hướng dẫn bài thực hành 3

[3.](#_heading=h.3znysh7) Phân tích yêu cầu bài thực hành 5

[4.](#_heading=h.2et92p0) Thiết kế bài thực hành 5

[5.](#_heading=h.3dy6vkm) Cài đặt và cấu hình các máy ảo 7

[6.](#_heading=h.3rdcrjn) Tích hợp và triển khai 9

[7.](#_heading=h.26in1rg) Thử nghiệm và đánh giá 12

**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. SSH vào máy victim

Hình 12. Tìm kiếm các file database và phát hiện file database của firefox

Hình 13. Truy xuất dữ liệu file database đó

Hình 14. Decode lại mật khẩu đã mã hóa base64 để lấy bản rõ

Hình 15. Truy cập trang web mục tiêu để đăng nhập với thông tin trích xuất được

Hình 16. Đăng nhập trang web mục tiêu thành công

Hình 17. Kiểm tra tiến độ hoàn thành bài lab

**Bài thực hành: Tìm hiểu về technique T1555:** Credentials from Password Stores

1. **Giới thiệu chung về bài thực hành.**

Bài thực hành "Tìm hiểu về technique T1555: Credentials from Password Stores" được thiết kế nhằm giúp sinh viên ngành An toàn thông tin hiểu rõ hơn về kỹ thuật trích xuất thông tin xác thực từ các kho lưu trữ mật khẩu. Đây là một phương pháp tấn công phổ biến trong các cuộc xâm nhập hệ thống, giúp kẻ tấn công chiếm được thông tin đăng nhập mà không cần thực hiện các hình thức đoán mật khẩu thông thường.

Trong bài thực hành này, sinh viên sẽ tìm hiểu cách truy cập vào các file lưu trữ thông tin mật khẩu trên hệ thống mục tiêu. Sinh viên sẽ thực hiện các bước cụ thể như truy cập hệ thống qua SSH, tìm kiếm file lưu trữ mật khẩu, sử dụng công cụ hỗ trợ để đọc nội dung file và trích xuất thông tin đăng nhập. Ngoài ra, sinh viên sẽ học cách giải mã các thông tin đã được mã hóa và thử nghiệm gửi thông tin đăng nhập thu thập được để chiếm quyền truy cập. Đây là một kỹ năng quan trọng giúp sinh viên hiểu cách thức kẻ tấn công khai thác các kho mật khẩu không được bảo mật chặt chẽ.

Thông qua bài thực hành này, sinh viên không chỉ hiểu cách trích xuất và giải mã thông tin mật khẩu mà còn nhận thức được những rủi ro bảo mật tiềm ẩn trong việc lưu trữ thông tin đăng nhập của hệ thống. Điều này sẽ giúp sinh viên nâng cao kiến thức và kỹ năng về bảo mật thông tin, đồng thời áp dụng kỹ thuật này trong công việc để kiểm thử, đánh giá kiến trúc một hệ thống trong môi trường thực tế sau này.

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

Giúp sinh viên biết được con đường mà một attacker dùng để trích xuất thông tin xác thực của nạn nhân, tìm kiếm và truy xuất thông tin, giải mã chúng để có quyền truy cập vào tài nguyên có chứa thông tin xác thực của nạn nhân.

* + - 1. *Yêu cầu đối với sinh viên*

Có kiến thức cơ bản về linux, biết các cú pháp truy vấn cơ sở dữ liệu cơ bản, biết phương pháp mã hóa cơ bản như Base64.

* + - 1. *Nội dung thực hành*

Khởi động bài lab:

Vào terminal, gõ:

*startlab nsec\_attk\_mitre-t1555*

*(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 tìm kiếm các file database có trên máy victim

***Victim:***

*find / -type f -name "\*.db" 2>/dev/null*

* ***find****: Lệnh tìm kiếm file và thư mục trên hệ thống.*
* ***/****: Thư mục gốc, tìm trên toàn bộ hệ thống.*
* ***-type f****: Chỉ tìm file (không bao gồm thư mục).*
* ***-name "\*.db"****: Tìm file có tên kết thúc với đuôi .db.*
* ***2>/dev/null****: Chuyển hướng các thông báo lỗi (ví dụ: truy cập bị từ chối) sang /dev/null để lệnh không bị gián đoạn.*
* Bước 3: Sinh viên phát hiện file .db khác với các file .db có sẵn thường thấy trên máy ubuntu thông thường đó là file .db của trình duyệt.
* Bước 4: Sinh viên dùng các thao tác cơ bản với database để truy xuất thông tin trong file .db đó. Sau đó giải mã và dùng thông tin có được để đăng nhập vào các trang web tương ứng.
* Bước 5: Các thông tin xác thực được lưu trong file .db này có thể chưa chính xác nếu mật khẩu chưa được cập nhật. Sinh viên sẽ dùng các thông tin thu thập được để đăng nhập vào các trang web tương ứng. Qua đó, xác định được thông tin xác thực đúng mà đã thu thập được để truy cập trang web.

Kết thúc bài lab:

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

*stoplab nsec\_attk\_mitre-t1555*

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 nsec\_attk\_mitre-t1555*

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 sử dụng thông tin xác thực đúng để đăng nhập thành công tới trang web có trong cơ sở dữ liệu được lưu của trình duyệt trên máy victim

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 cùng với cấu hình tương tự và được chạy sẵn dịch vụ ssh, các dịch vụ khác như apache2, sqlite3, firefox, apache2, php, libapache2-mod-php, php-sqlite3, curl

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

Sử dụng thông tin xác thực đã thu thập được để đăng nhập trang web có trong cơ sở dữ liệu được lưu của trình duyệt trên máy victim

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:

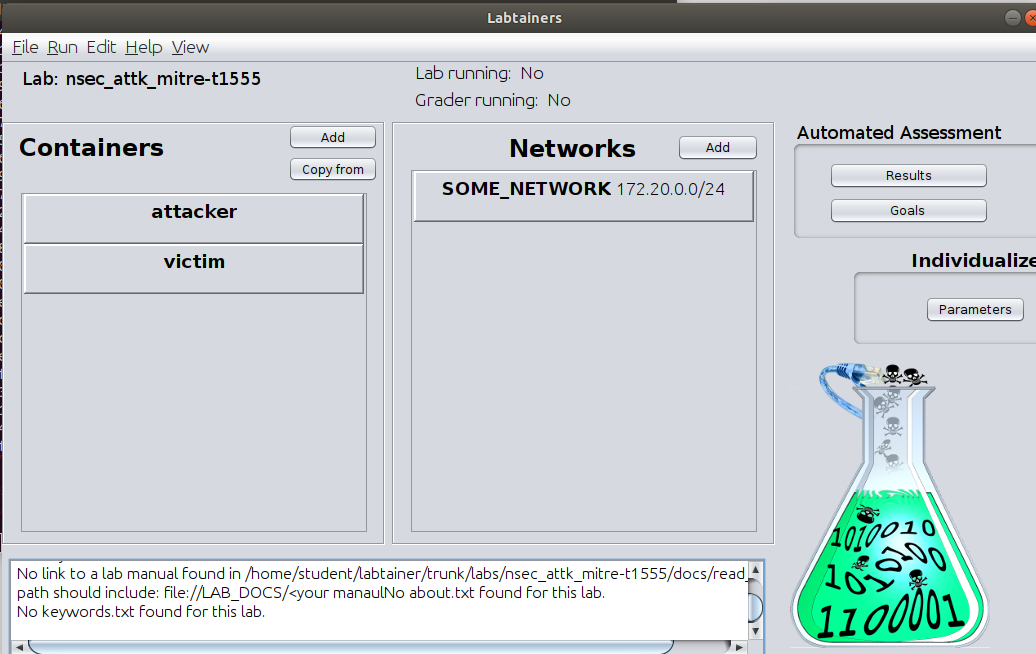
Bảng 1. Bảng Result

| Result Tag | Container | File | Field Type | Field ID | Timestamp Type |
| --- | --- | --- | --- | --- | --- |
| ssh | victim | /var/log/ssh.log | CONTAINS | Starting session | File |
| check\_login | victim | /var/log/apache2/access.log | CONTAINS | "POST /login.php HTTP/1.1" 200 | File |

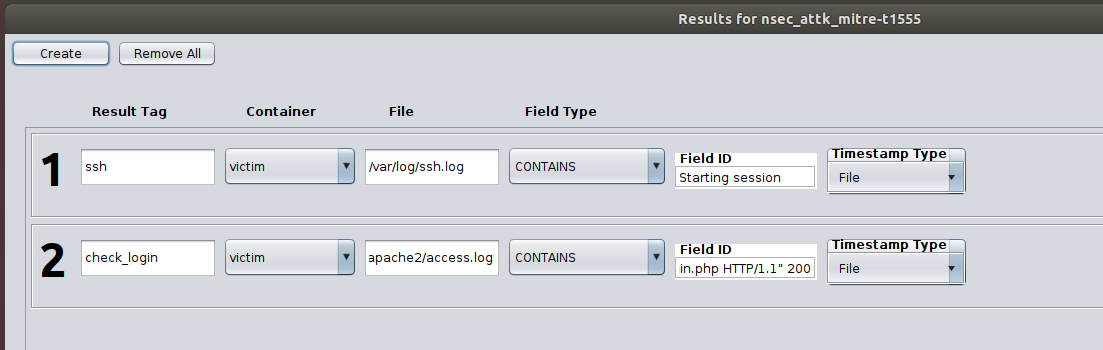
-ssh: ssh thành công tới máy victim.

-check\_login: login thành công trang web được lưu trên cơ sở dữ liệu máy victim.

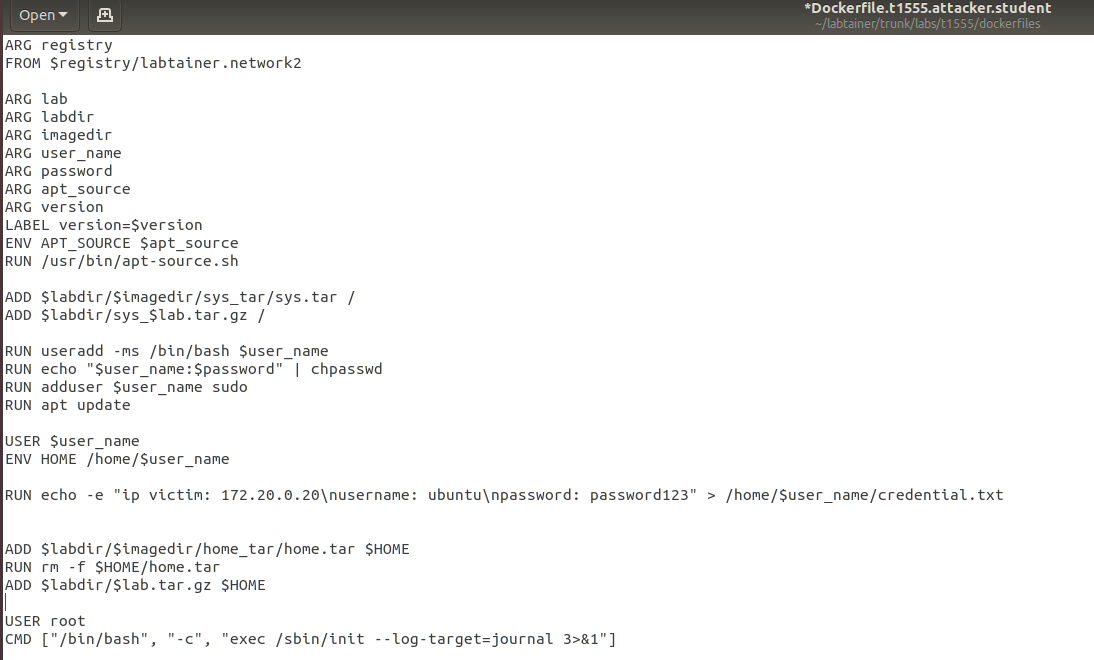
1. ***Cài đặt và cấu hình các máy ảo***



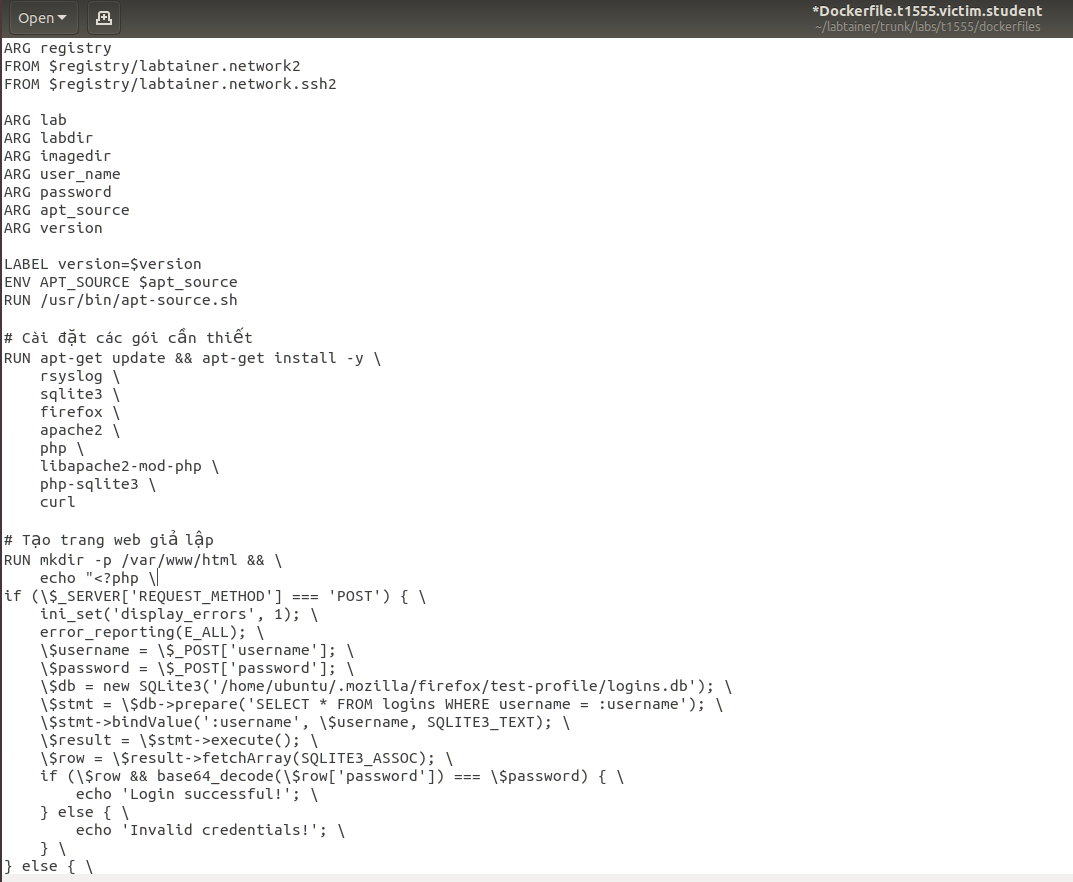
Hình 1. Giao diện Labedit của bài lab



Hình 2. Cài đặt phần Result



Hình 3. Dockerfiles của máy attacker

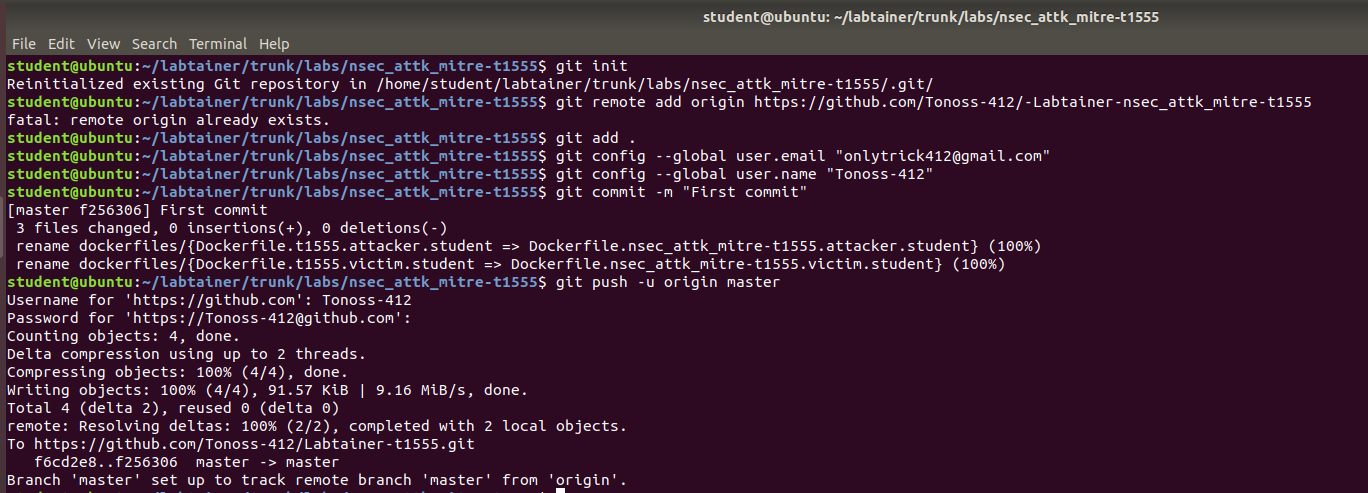


Hình 4. Dockerfiles của victim

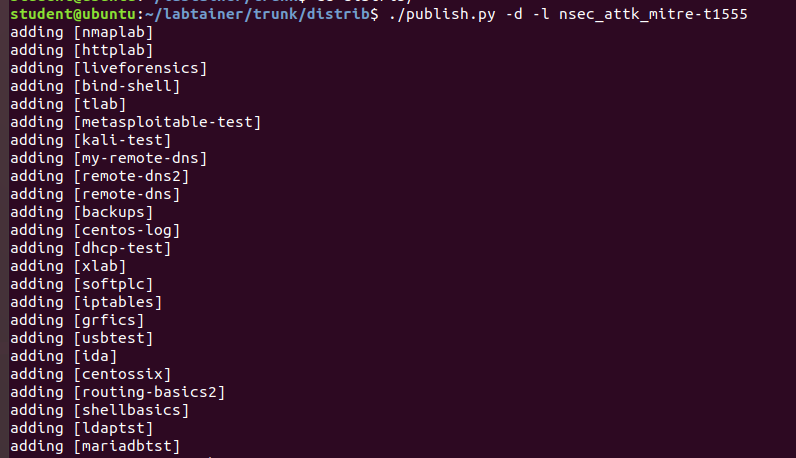
1. ***Tích hợp và triển khai***

Bài thực hành đã được triển khai như sau:

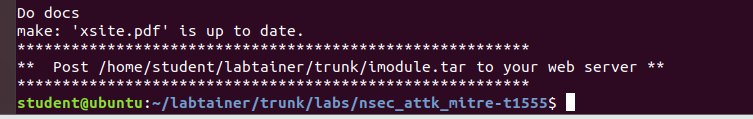
* + - * 1. Docker Hub

https://hub.docker.com/repository/docker/huytq412okok/nsec\_attk\_mitre-t1555****

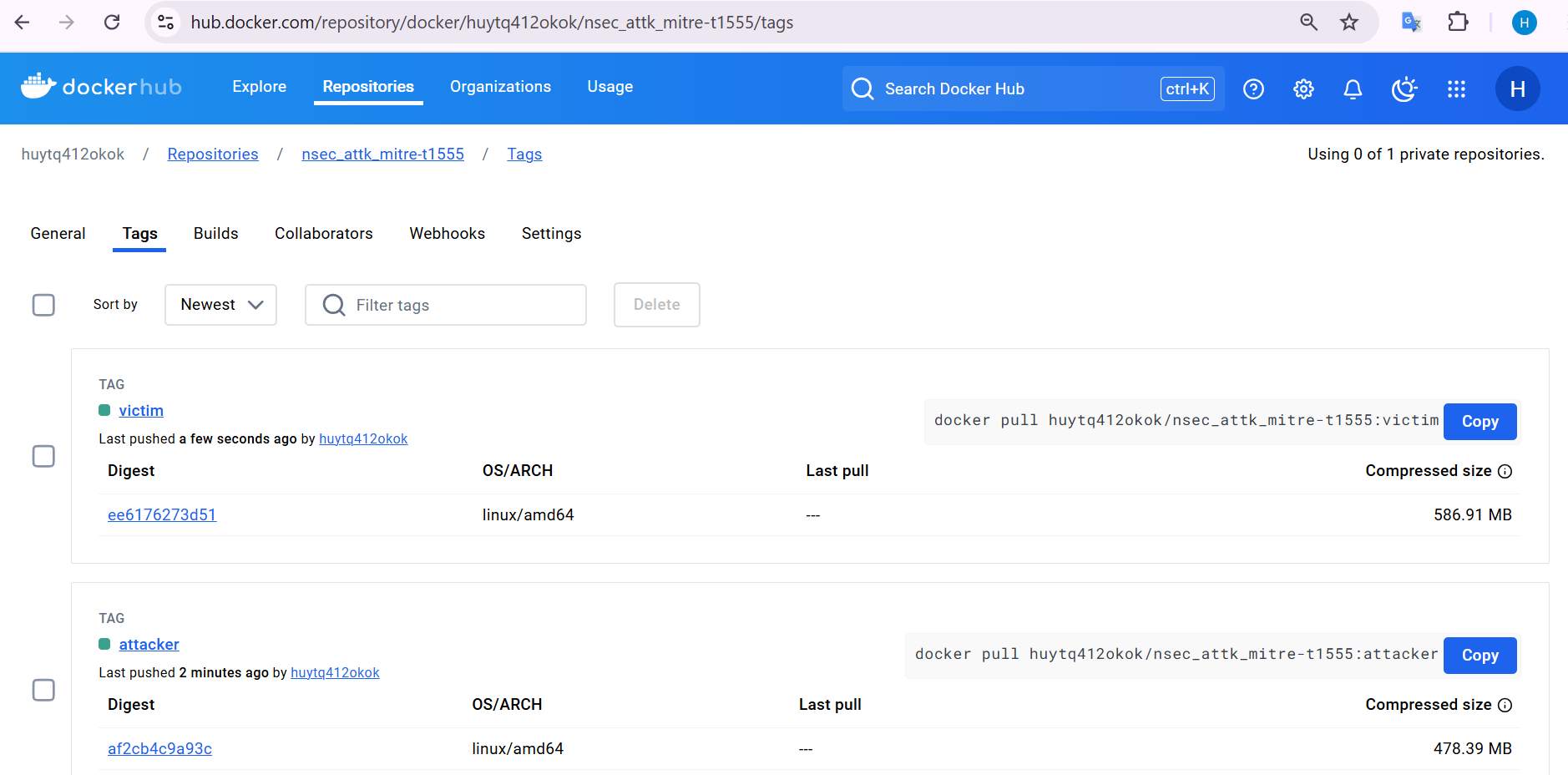
Hình 5. Add và commit bài lab



Hình 6. Đẩy các vùng chứa lên dockerhub

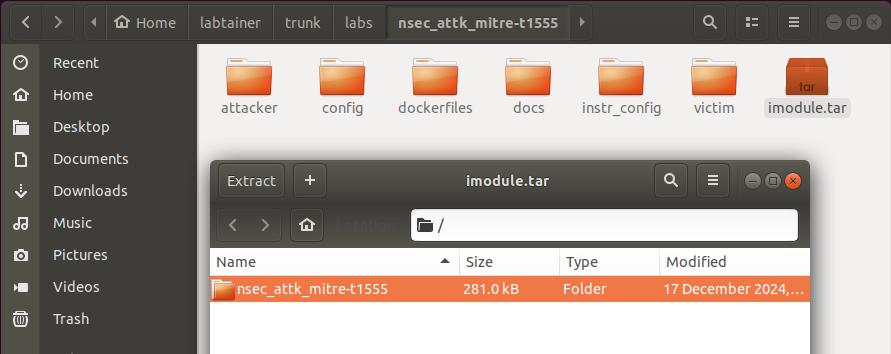


Hình 7. Tạo imodule.tar chứa bài thực hành

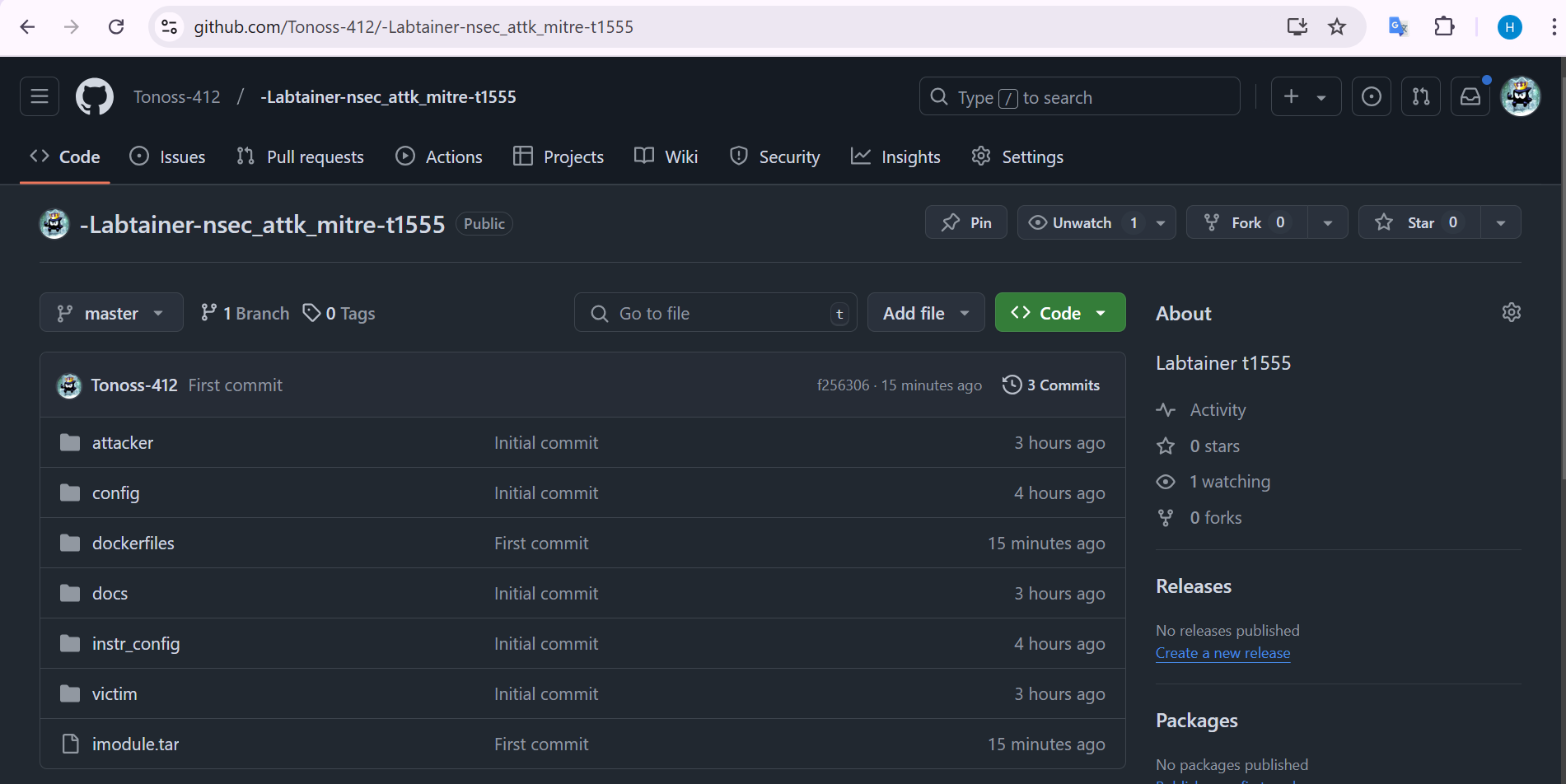


Hình 8. Các vùng chứa được đẩy lên dockerhub

* + - * 1. Github

https://github.com/Tonoss-412/-Labtainer-nsec\_attk\_mitre-t1555

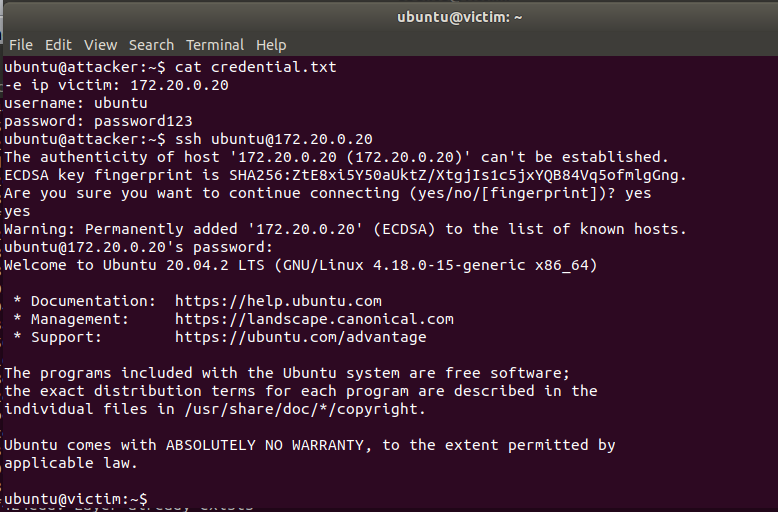
Hình 9. File imodule.tar chứa bài thực hành



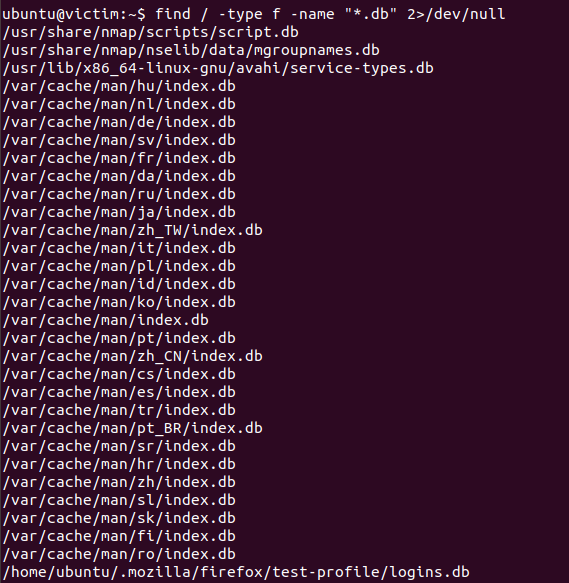
Hình 10. Đẩy file imodule.tar lên github

1. ***Thử nghiệm và đánh giá***

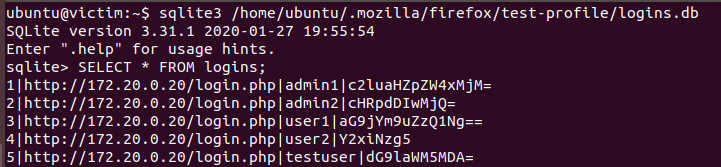
Bài thực hành đã được xây dựng thành công, dưới đây là hình ảnh minh họa về bài thực hành:



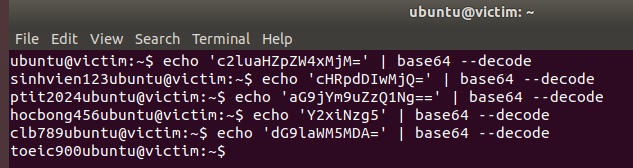
Hình 11. SSH vào máy victim



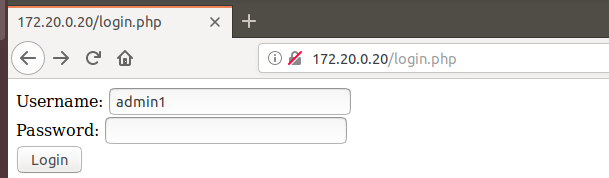
Hình 12. Tìm kiếm các file database và phát hiện file database của firefox



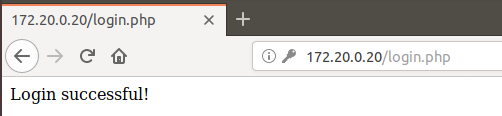
Hình 13. Truy xuất dữ liệu file database đó



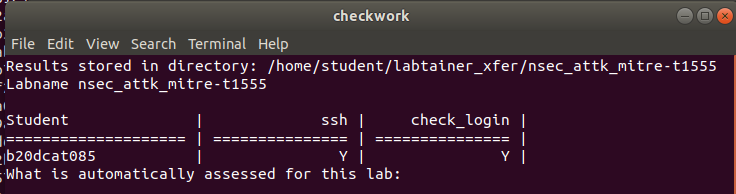
Hình 14. Decode lại mật khẩu đã mã hóa base64 để lấy bản rõ



Hình 15. Truy cập trang web mục tiêu để đăng nhập với thông tin trích xuất được



Hình 16. Đăng nhập trang web mục tiêu thành công



Hình 17. Kiểm tra tiến độ hoàn thành bài lab