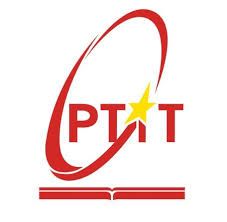
**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**

**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: T1110: Brute Force

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 T1110: Brute Force 3](#_Toc185385361)

[1. Giới thiệu chung về bài thực hành. 3](#_Toc185385362)

[2. Nội dung và hướng dẫn bài thực hành 3](#_Toc185385363)

[3. Phân tích yêu cầu bài thực hành 5](#_Toc185385364)

[4. Thiết kế bài thực hành 5](#_Toc185385365)

[5. Cài đặt và cấu hình các máy ảo 7](#_Toc185385366)

[6. Tích hợp và triển khai 9](#_Toc185385367)

[7. Thử nghiệm và đánh giá 11](#_Toc185385368)

**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. IP của máy attacker

Hình 13. IP máy victim

Hình 14. Dùng Hydra trên máy attacker để thực hiện brute force password của user ubuntu trên máy victim

Hình 15. Dùng máy attacker ssh thành công vào máy victim với mật khẩu vừa tìm được

Hình 16. Kiểm tra tiến độ hoàn thành bài lab

Bài thực hành: Tìm hiểu về technique T1110: Brute Force

1. Giới thiệu chung về bài thực hành.

Bài thực hành "Tìm hiểu về technique T1110: Brute Force" được thiết kế nhằm giúp sinh viên hiểu rõ hơn về kỹ thuật brute force, một phương thức tấn công phổ biến trong lĩnh vực an ninh mạng, đặc biệt là trong việc chiếm đoạt quyền truy cập thông qua việc đoán mật khẩu. Đây là bước khởi đầu quan trọng để sinh viên làm quen với các kỹ thuật tấn công mạng và nhận thức được cách thức các cuộc tấn công có thể được thực hiện.

Trong bài thực hành này, sinh viên sẽ tìm hiểu cách thực hiện brute force để khai thác hệ thống bị yếu kém trong việc quản lý mật khẩu. Sinh viên sẽ học cách sử dụng các công cụ như Hydra để thực hiện các cuộc tấn công brute force và thử nghiệm việc đoán mật khẩu cho tài khoản mục tiêu. Đây là một kỹ năng cơ bản nhưng rất quan trọng, vì nó giúp sinh viên nắm bắt được cách thức kẻ tấn công có thể lợi dụng các điểm yếu trong hệ thống xác thực để chiếm đoạt quyền truy cập.

Thông qua bài thực hành này, sinh viên không chỉ hiểu cách brute force hoạt động mà còn nhận thức được những rủi ro bảo mật tiềm ẩn trong việc bảo vệ 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 hay một kỹ thuật đơn giản có thể áp dụng trong công việc pentest để đánh giá các hệ thống trong công việc sau này.

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

Giúp sinh viên tìm hiểu được thế nào là Brute Force, cách dung Hydra để thực hiện một cuộc tấn công đơn giản nhằm tìm được mật khẩu đúng nhằm truy cập tới máy mục tiêu.

* + - 1. Yêu cầu đối với sinh viên

Có kiến thức cơ bản về hệ điều hành Linux, biết sử dụng ssh cơ bản công cụ Hydra.

* + - 1. Nội dung thực hành

Khởi động bài lab:

Vào terminal, gõ:

*startlab pen\_tool\_mitre\_t1110*

*(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***. Trên terminal ***attacker*** đã được cung cấp sẵn một file password\_list.txt, sinh viên sẽ sử dụng file này làm để brute force bằng Hydra.

* Bước 1: Sinh viên sử dụng ifconfig để kiểm tra địa chỉ ip máy victim:

***attacker:***

*ifconfig*

* Bước 2: Sinh viên sử dụng Hydra với password\_list.txt để cố gắng ssh đến

máy victim:

***attacker:***

*hydra -l <username> -P /path/to/passwords.txt ssh://<ip\_victim>*

* Bước 3: Sinh viên sử dụng password đúng sau khi tìm được ở trên để ssh đến

máy victim:

***attacker:***

*ssh <ip\_victim>*

Kết thúc bài lab:

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

*stoplab pen\_tool\_mitre\_t1110*

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\_tool\_mitre\_t1110*

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 Hydra để tìm ra mật khẩu của người dung máy victim và thực hiện ssh thành công tới đó.

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 chủ, 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, được cài sẵn Hydra và chuẩn bị sẵn file password\_list.txt

victim: sử dụng các thư viện mặc định hệ thống cùng với cấu hình tương tự và được chạy sẵn dịch vụ ssh.

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 câu lệnh hydra để brute force thành công mật khẩu của user trên máy victim

Sử dụng ssh tới victim thành công với mật khẩu đúng đã thu thập được

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:

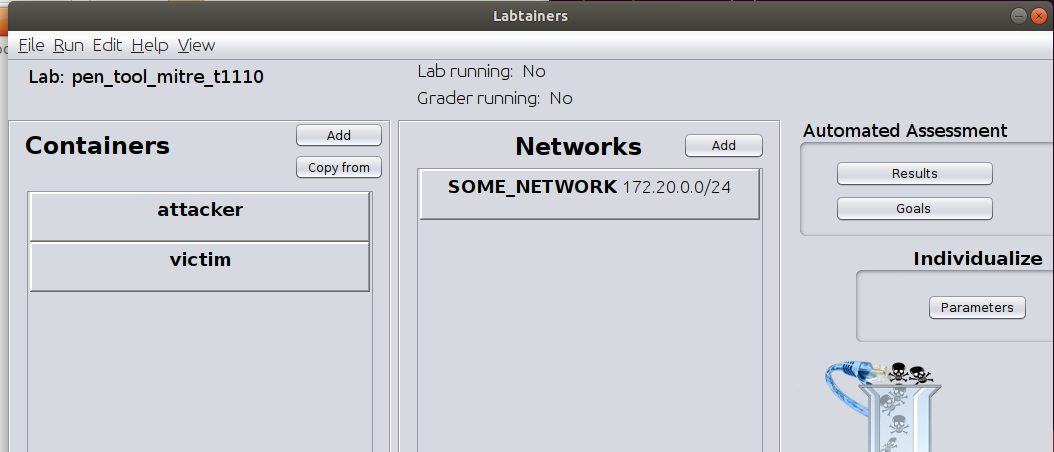
Bảng 1. Bảng Result

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Result Tag | Container | File | Field Type | Field ID | Timestamp Type |
| hydra | attacker | ~/.bash\_history | FILE\_REGEX | .\*hydra.\*172\.20\.0\.20.\* | File |
| ssh | victim | /var/log/ssh.log | CONTAINS | Starting session | File |

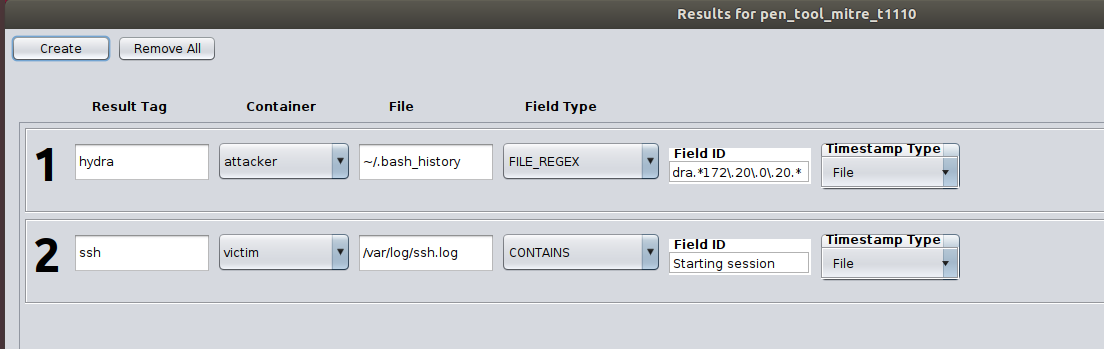
-hydra: brute force thành công password của user trên máy victim

-ssh: từ máy attacker ssh thành công tới máy victim

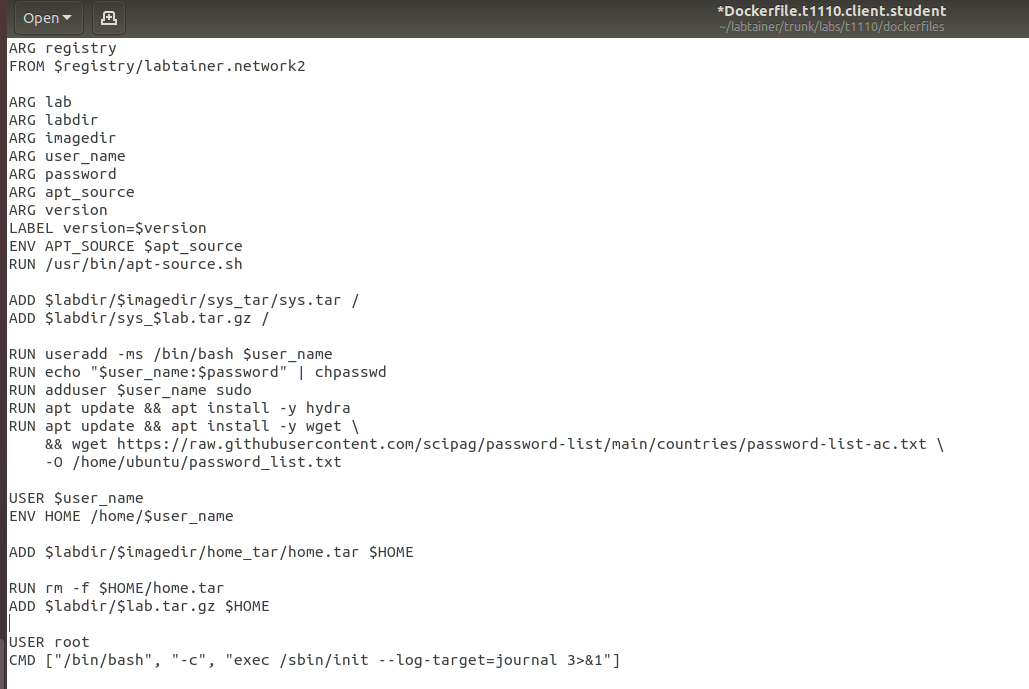
1. Cài đặt và cấu hình các máy ảo



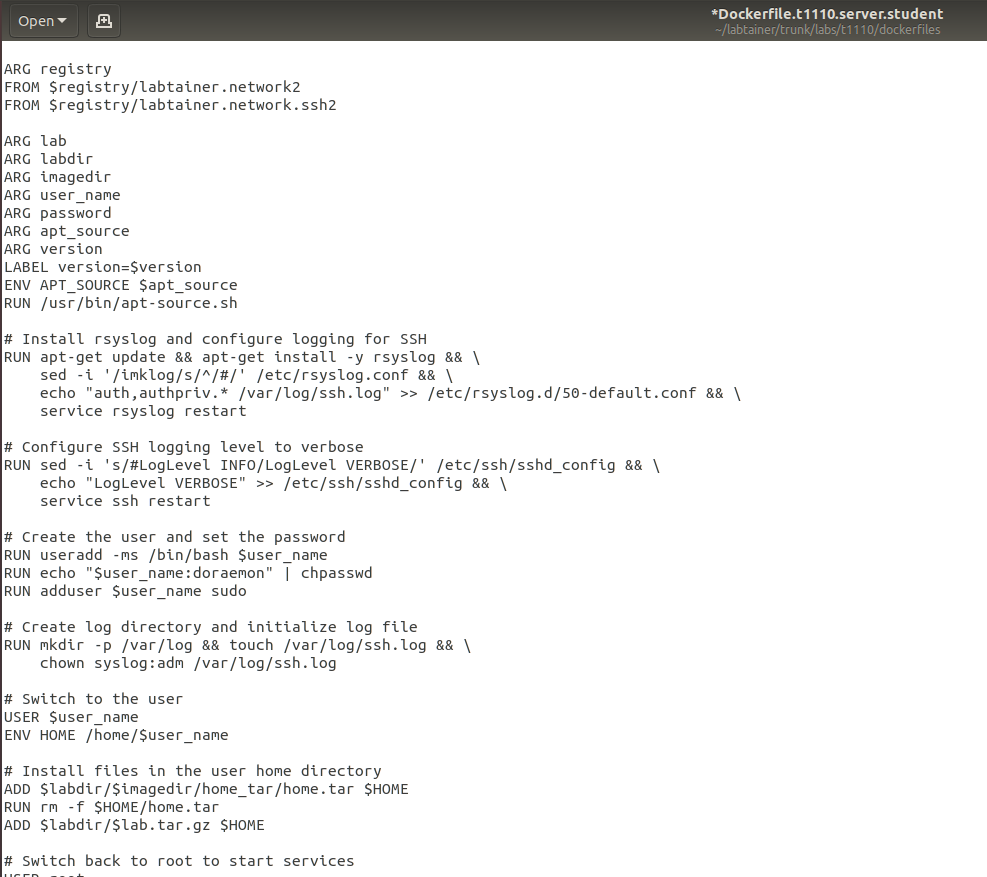
Hình 1. Giao diện Labedit của bài lab



Hình 2. Cài đặt phần Result



Hình 3. Dockerfiles của máy attacker

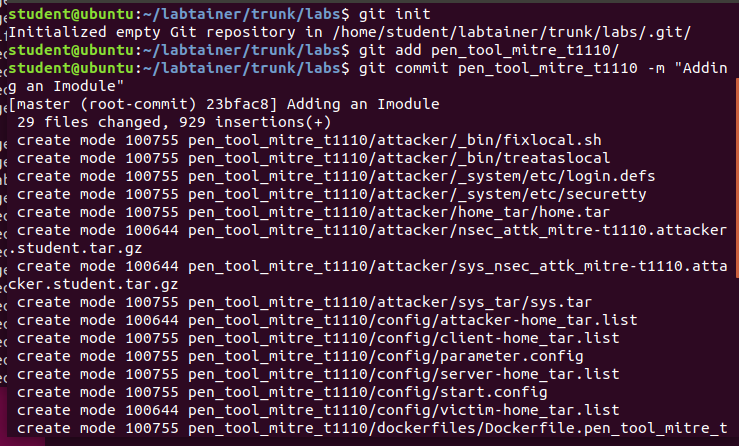


Hình 4. Dockerfiles của victim

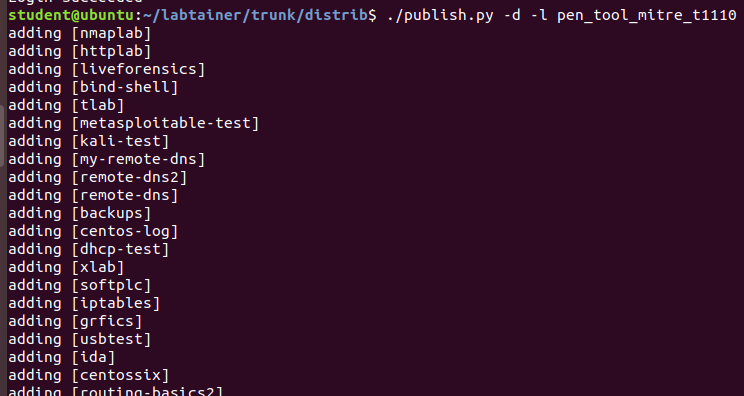
1. Tích hợp và triển khai

Bài thực hành đã được triển khai như sau:

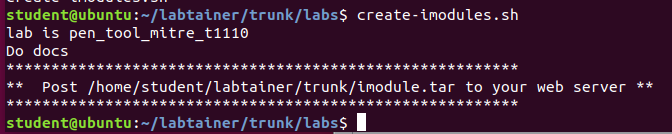
* + - * 1. Docker Hub



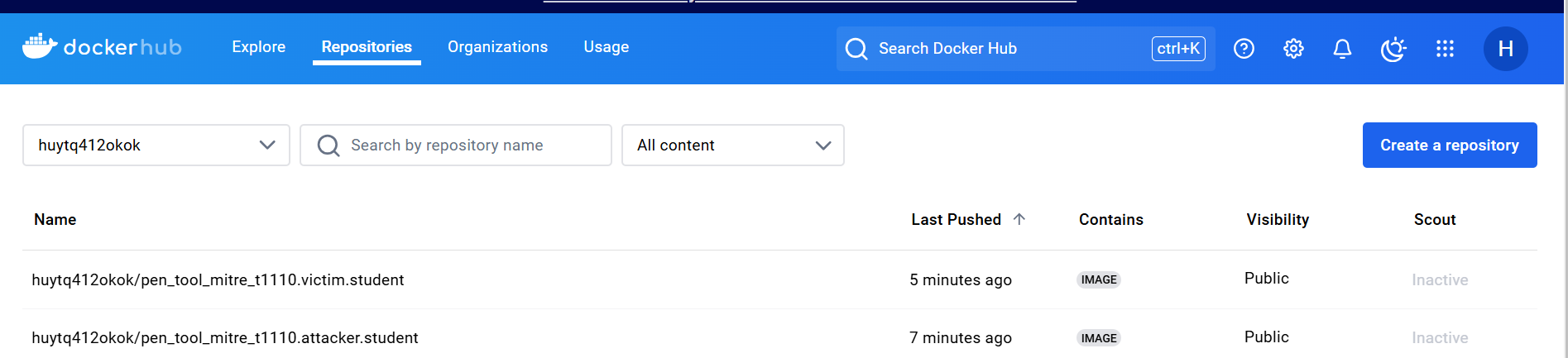
Hình 5. Add và commit bài lab



Hình 6. Đẩy các vùng chứa lên dockerhub



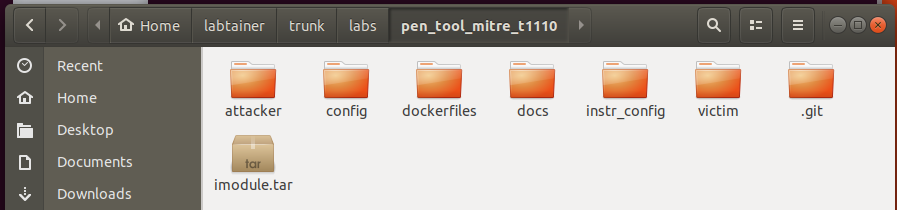
Hình 7. Tạo imodule.tar chứa bài thực hành



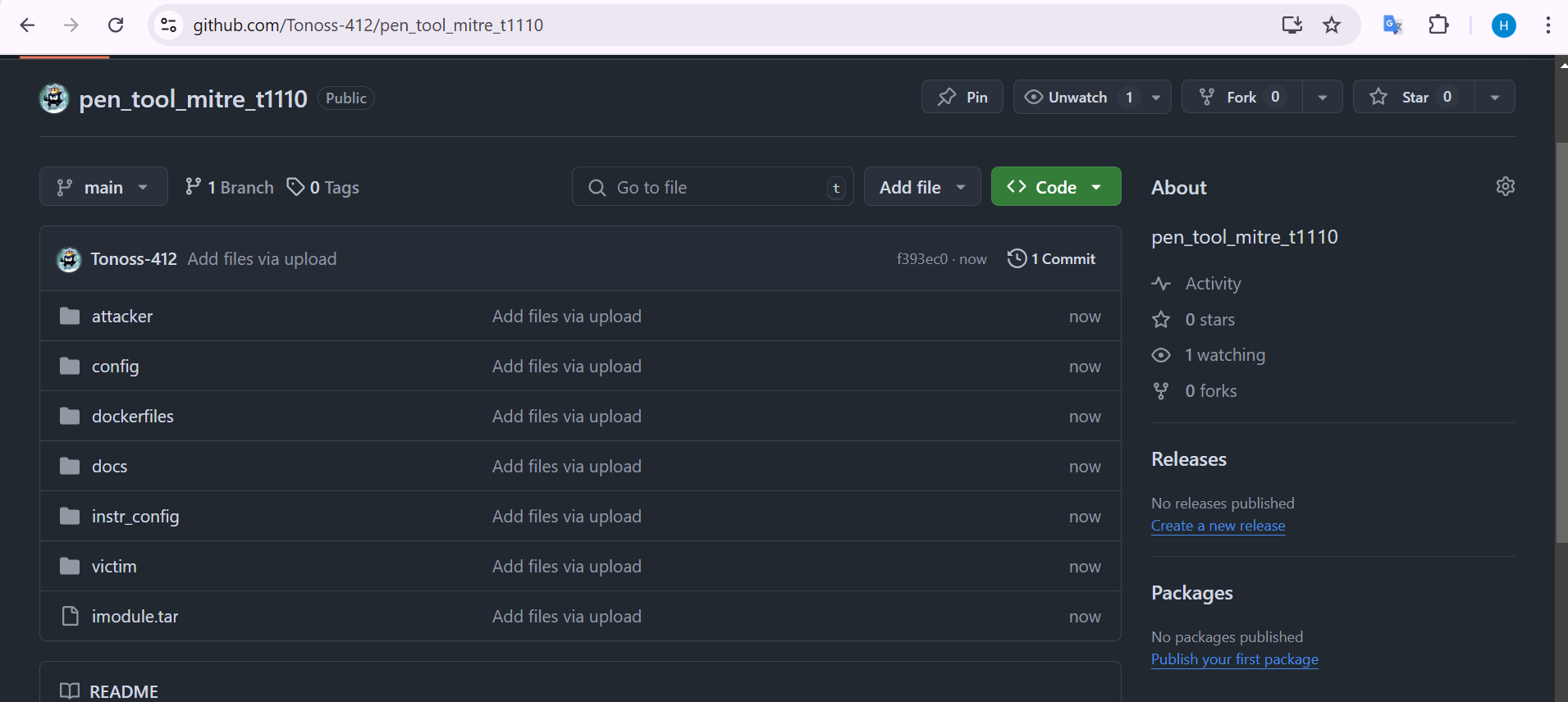
Hình 8. Các vùng chứa được đẩy lên dockerhub

* + - * 1. Github

https://github.com/Tonoss-412/pen\_tool\_mitre\_t1110



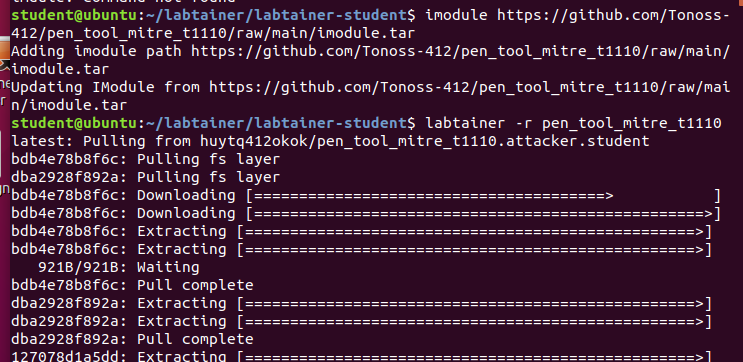
Hình 9. File imodule.tar chứa bài thực hành



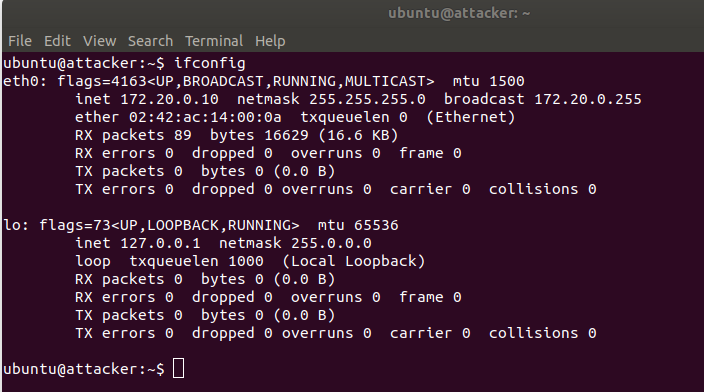
Hình 10. Đẩy file imodule.tar lên github

1. Thử nghiệm và đánh giá

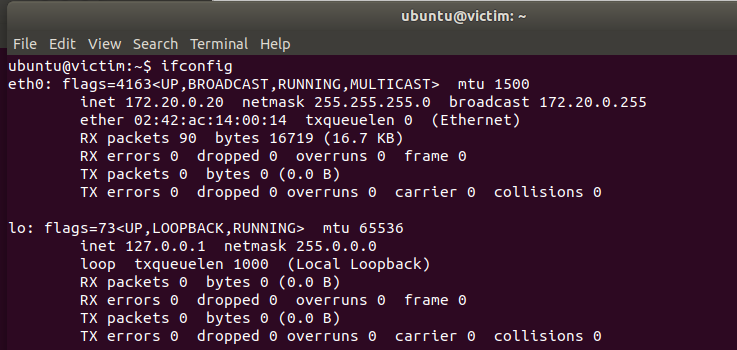
Bài thực hành đã được xây dựng thành công, dưới đây là hình ảnh minh họa về bài thực hành:



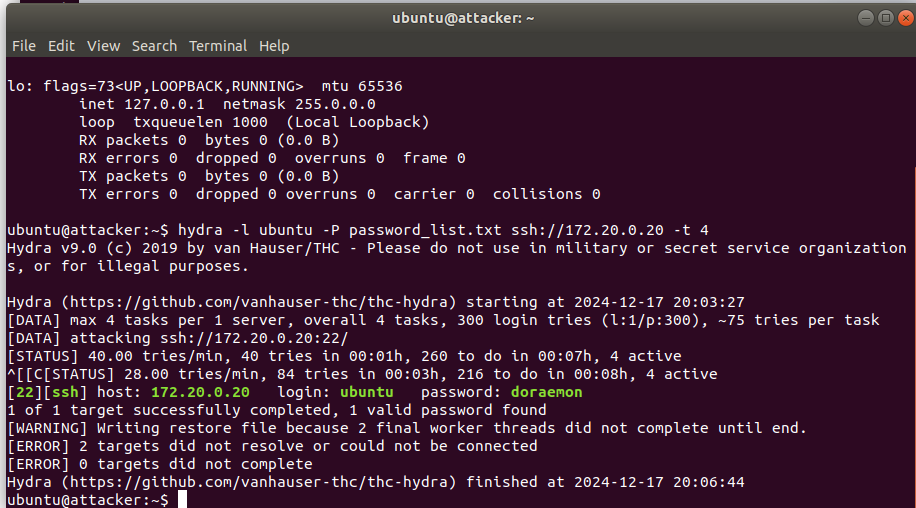
Hình 11. Imodule bài lab về máy



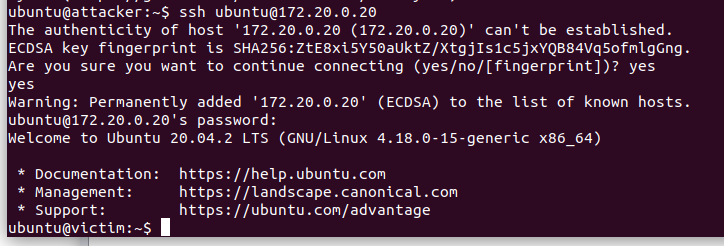
Hình 12. IP của máy attacker



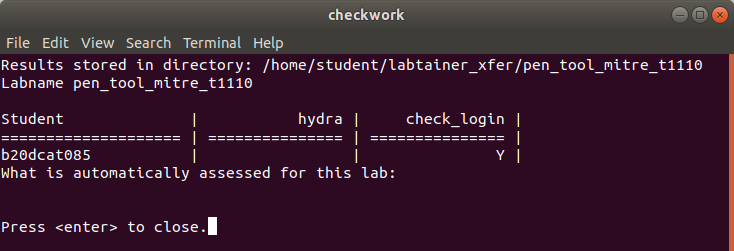
Hình 13. IP máy victim



Hình 14. Dùng Hydra trên máy attacker để thực hiện brute force password của user ubuntu trên máy victim



Hình 15. Dùng máy attacker ssh thành công vào máy victim với mật khẩu vừa tìm được



Hình 16. Kiểm tra tiến độ hoàn thành bài lab