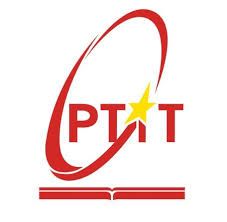
**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**

**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: T1564: Hide Artifacts

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 T1564: Hide Artifacts 3](#_Toc185901718)

[1. Giới thiệu chung về bài thực hành. 3](#_Toc185901719)

[2. Nội dung và hướng dẫn bài thực hành 3](#_Toc185901720)

[3. Phân tích yêu cầu bài thực hành 5](#_Toc185901721)

[4. Thiết kế bài thực hành 5](#_Toc185901722)

[5. Cài đặt và cấu hình các máy ảo 7](#_Toc185901723)

[6. Tích hợp và triển khai 8](#_Toc185901724)

[7. Thử nghiệm và đánh giá 11](#_Toc185901725)

**MỤC LỤC HÌNH ẢNH**

Hình 1. Giao diện Labedit của bài lab

Hình 2. Cài đặt phần Result

Hình 3. Dockerfiles của máy machine

Hình 4. Add và commit bài lab

Hình 5. Đẩy các vùng chứa lên dockerhub

Hình 6. Tạo imodule.tar chứa bài thực hành

Hình 7. Các vùng chứa được đẩy lên dockerhub

Hình 8. File imodule.tar chứa bài thực hành

Hình 9. Đẩy file imodule.tar lên github

Hình 10. Imodule bài lab về máy

Hình 11. Thư mục hiện tại khi khởi động lab

Hình 12. Đọc file log để phát hiện điều bất thường

Hình 13. Phát hiện mật khẩu dùng để ẩn giấu hình ảnh với Steganoraphy tool

Hình 14. Extract thông tin các file ảnh trong thư mục /image để tìm ảnh có chứa thông tin ẩn giấu

Hình 15. Đọc file trích xuất được để hiểu hành vi sau đó xóa file ảnh có chứa thông tin ẩn giấu

Hình 16. Kiểm tra tiến độ hoàn thành bài lab

Bài thực hành: Tìm hiểu về technique T1564: Hide Artifacts

1. Giới thiệu chung về bài thực hành.

Bài thực hành "Tìm hiểu về technique T1564: Hide Artifacts" được thiết kế nhằm giúp sinh viên hiểu rõ hơn về kỹ thuật ẩn giấu các dấu vết, một phương thức quan trọng và thường được sử dụng trong các cuộc tấn công mạng nhằm che giấu hoạt động độc hại của kẻ tấn công. Đây là một kỹ thuật thuộc nhóm các phương pháp tránh né (Evasion Techniques), được các hacker sử dụng để qua mặt hệ thống giám sát, phát hiện xâm nhập (IDS), hoặc để đánh lạc hướng đội ngũ bảo mật.

Trong bài thực hành này, sinh viên sẽ tìm hiểu về phương pháp phổ biến để ẩn giấu dấu vết, như sử dụng steganography (che giấu dữ liệu trong hình ảnh hoặc tập tin) để làm giảm sự chú ý. Sinh viên sẽ được hướng dẫn cách kiểm tra và tìm ra một hình ảnh đã được che dấu dữ liệu trên môi trường giả lập, qua đó hiểu được cách kẻ tấn công có thể lẩn tránh trong môi trường tấn công.

Bên cạnh việc thực hành, sinh viên còn được cung cấp kiến thức về các biện pháp giám sát, như truy kiểm tra file log, triển khai biện pháp phòng vệ đơn giản. Điều này không chỉ giúp sinh viên hiểu sâu hơn về kỹ thuật T1564 mà còn nhận thức được tầm quan trọng của việc bảo vệ và quản lý các dấu vết an ninh mạng.

Thông qua bài thực hành này, sinh viên sẽ nắm vững kiến thức về cách kẻ tấn công che giấu hành vi, cũng như cách thức các tổ chức có thể phát hiện và ứng phó. Đây là một bước chuẩn bị cần thiết, giúp sinh viên tự tin áp dụng kỹ năng trong các công việc liên quan đến điều tra sự cố (incident response), kiểm tra bảo mật (security assessment), và xây dựng các hệ thống phòng thủ mạng trong tương lai.

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

Giúp sinh viên tìm hiểu được cách dùng steghide để trích xuất dữ liệu được che giấu trong hình ảnh.

* + - 1. Yêu cầu đối với sinh viên

Có kiến thức cơ bản về hệ điều hành Linux, biết sử dụng các lệnh cơ bản, sử dụng được steghide.

* + - 1. Nội dung thực hành

Khởi động bài lab:

Vào terminal, gõ:

*startlab pen\_bsic\_mitre\_t1564*

*(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 một terminal ảo sẽ xuất hiện là máy ***machine***. Trên terminal ***machine*** thư mục hiện tại bao gồm 2 thư mục image và log.

* Bước 1: Sinh viên sử dụng ls để kiểm tra các thư mục hiện có trên máy ***machine***:

*ls*

* Bước 2: Sinh viên truy cập thư mục log và đọc file log tìm hiểu xem có gì nhạy cảm đã được ghi lại không:

*cd log*

*cat daily.log*

* Bước 3: Sinh viên phát hiện password phát hiện được trong log để sau đó dùng steghide trích xuất thông tin các hình ảnh trong thư mục /image

*steghide extract -sf <image\_file> -p <password>*

* Bước 4: Dữ liệu đã được trích xuất ra 1 file. Đọc file đó để quan sát thông tin được ẩn giấu của attacker

*cat <extract\_file>*

* Bước 5: Sinh viên thực hiện biện pháp bảo vệ bằng cách xóa file ảnh có chứa thông tin này.

*rm <image\_file>*

Kết thúc bài lab:

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

*stoplab pen\_bsic\_mitre\_t1564*

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\_t1564*

1. Phân tích yêu cầu bài thực hành

Bài thực hành gồm 1 máy tính có tên machine. Để hoàn thành bài thực hành sinh viên cần sử dụng steghide để trích xuất thành công nội dung được attacker ẩn giấu. Sau đó xóa file hình ảnh có chứa thông tin ẩn giấu đó.

1. Thiết kế bài thực hành

Trên môi trường máy ảo Ubuntu được cung cấp, sử dụng docker tạo ra 1 container mang tên “machine”

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

Cấu hình docker gồm có:

Machine: lưu cấu hình cho máy chủ, trong đó gồm có:

Tên máy: machine

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 container: machine, trong đó:

machine: sử dụng các thư viện mặc định hệ thống và chạy hệ điều hành centos, được cài sẵn steghide, thư mục user hiện tại chứa sẵn các file hình ảnh và file log.

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 steghide trích xuất thành công nội dung ẩn giấu trong file hình ảnh

Xóa thành công file ảnh có chứa nội dung ẩn giấu.

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:

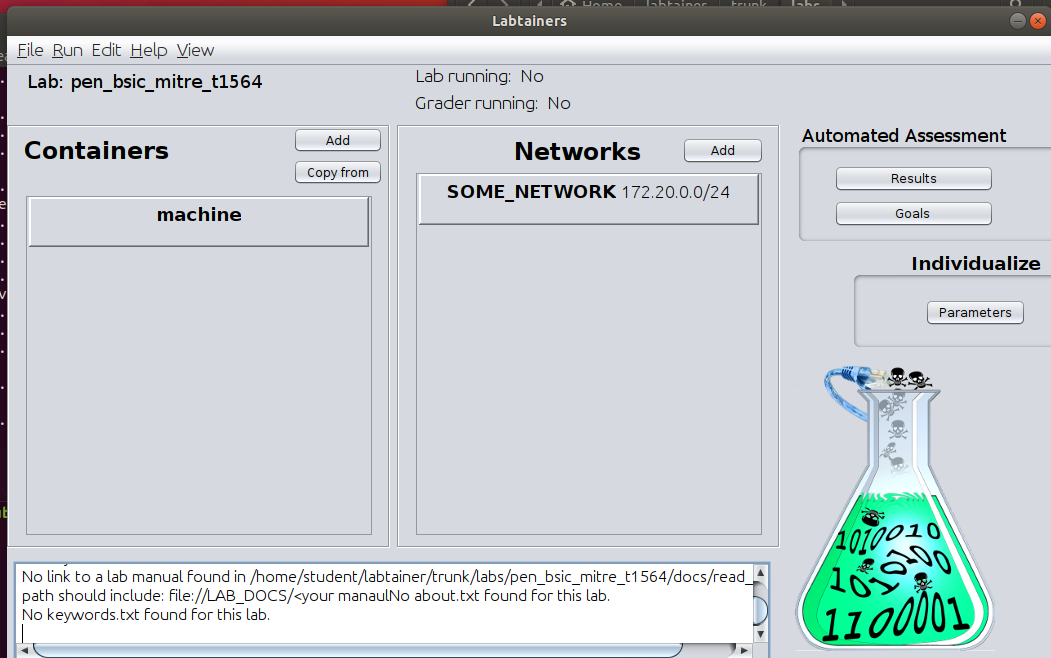
Bảng 1. Bảng Result

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Result Tag | Container | File | Field Type | Field ID | Timestamp Type |
| steghide | machine | ~/.bash\_history | FILE\_REGEX | \bsteghide\s+extract\b.\*\bimage7\.jpg\b | File |
| defense | machine | ~/.bash\_history | FILE\_REGEX | \brm\b.\*\bimage7\.sh\b | File |

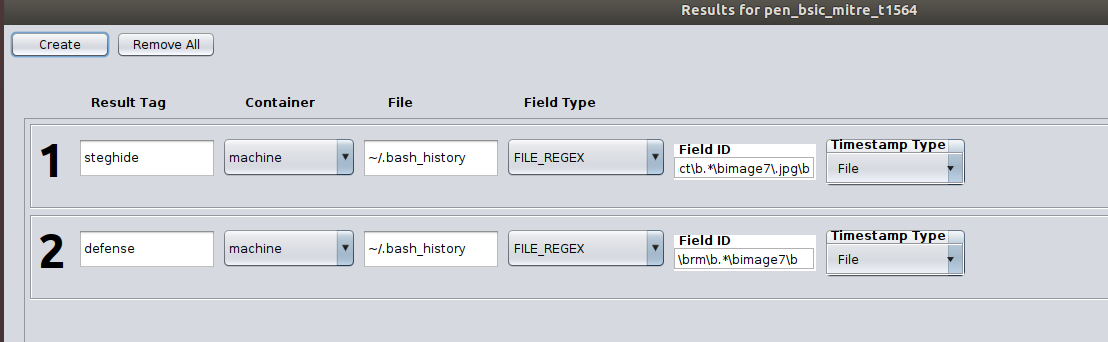
-steghide: trích xuất thành công từ file ảnh chứa thông tin được ẩn giấu

-defense: xóa thành công file ảnh chứa thông tin ẩn giấu

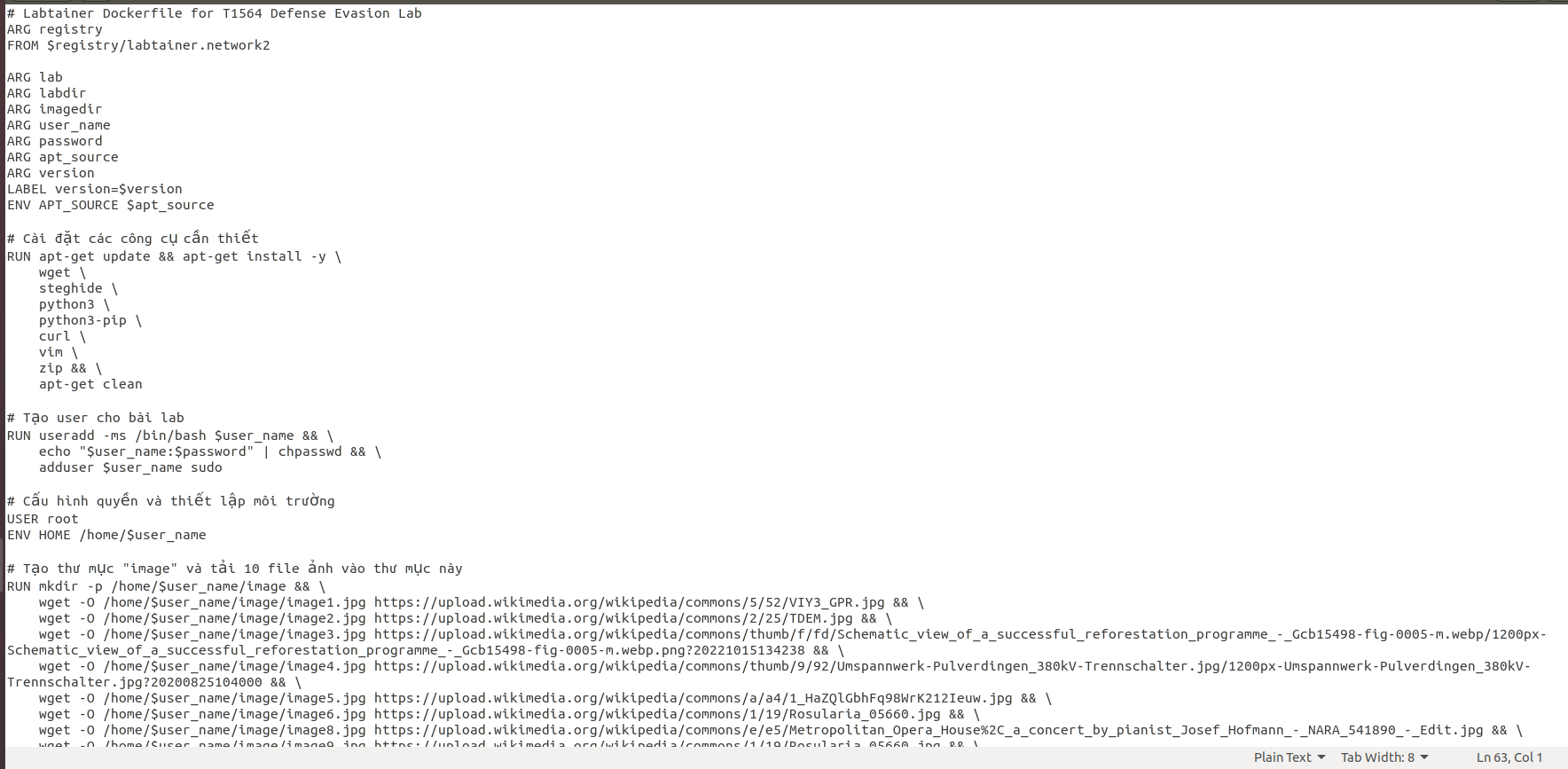
1. Cài đặt và cấu hình các máy ảo



Hình 1. Giao diện Labedit của bài lab



Hình 2. Cài đặt phần Result

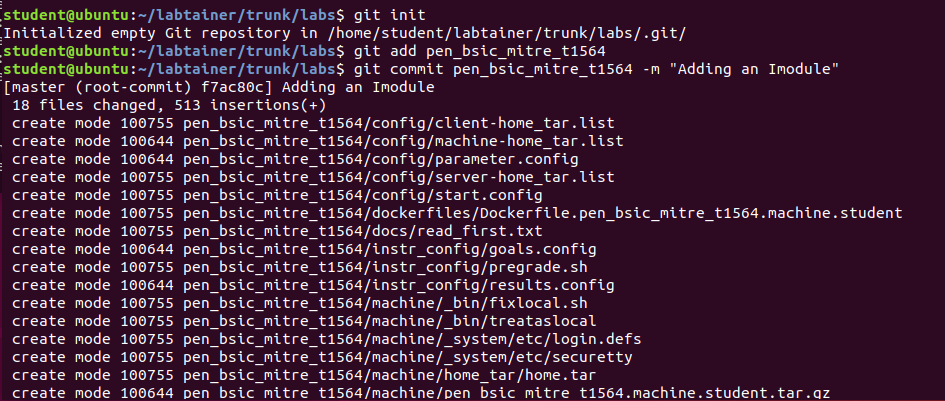


Hình 3. Dockerfiles của máy machine

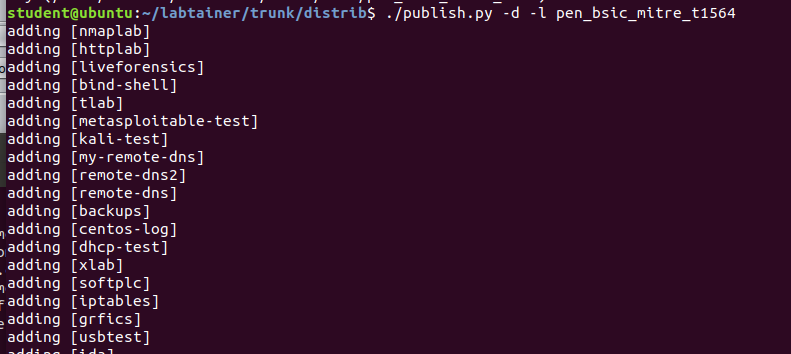
1. Tích hợp và triển khai

Bài thực hành đã được triển khai như sau:

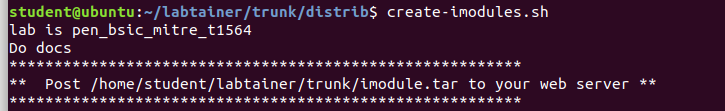
* + - * 1. Docker Hub



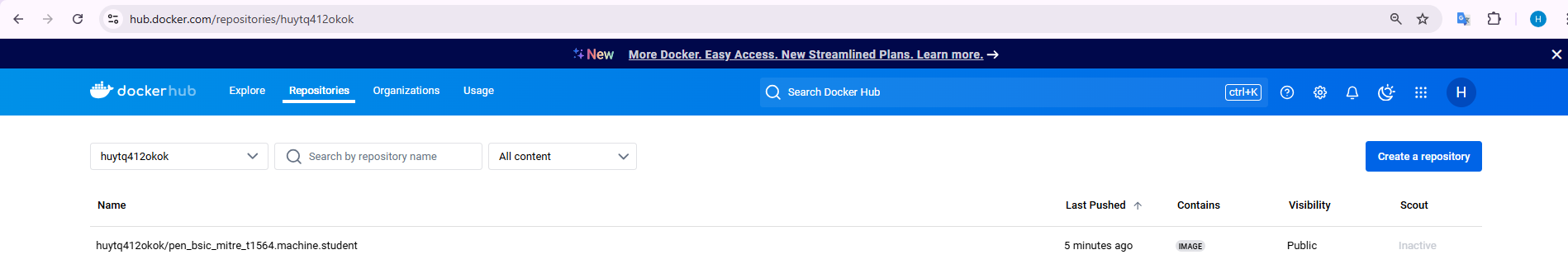
Hình 4. Add và commit bài lab



Hình 5. Đẩy các vùng chứa lên dockerhub



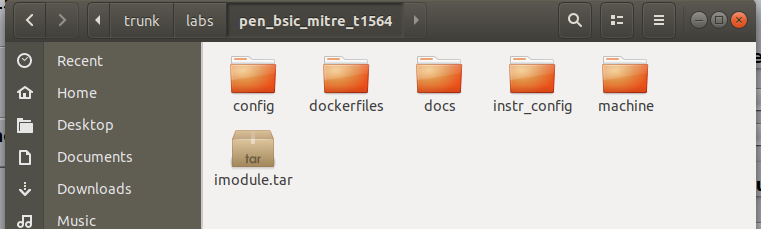
Hình 6. Tạo imodule.tar chứa bài thực hành



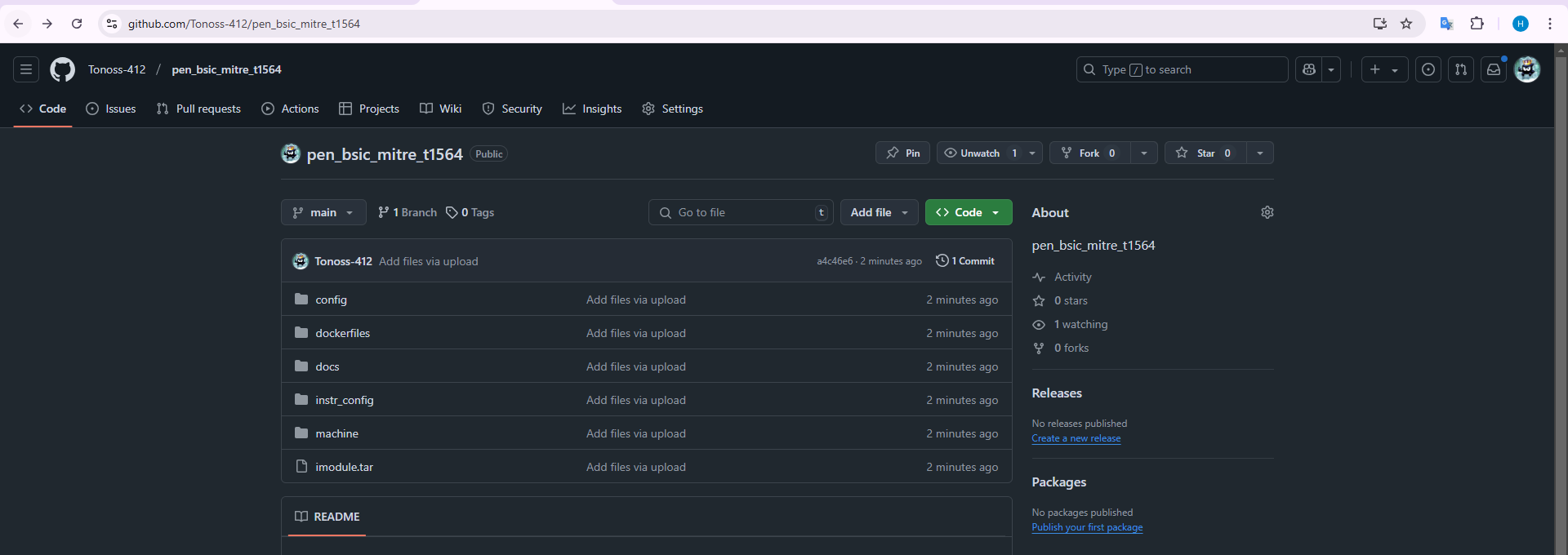
Hình 7. Các vùng chứa được đẩy lên dockerhub

* + - * 1. Github

https://github.com/Tonoss-412/pen\_bsic\_mitre\_t1564



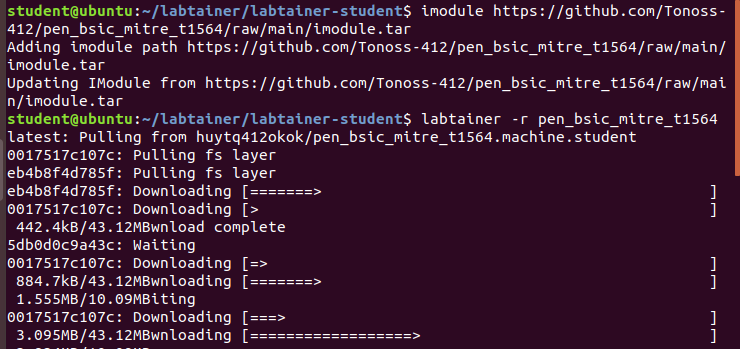
Hình 8. File imodule.tar chứa bài thực hành



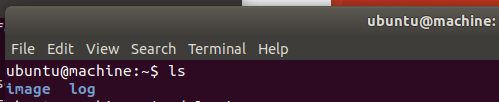
Hình 9. Đẩy file imodule.tar lên github

1. Thử nghiệm và đánh giá

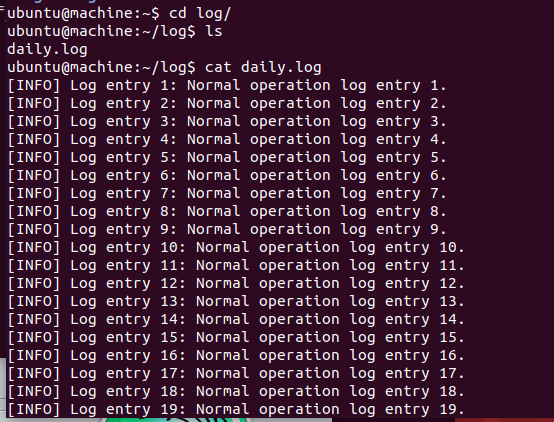
Bài thực hành đã được xây dựng thành công, dưới đây là hình ảnh minh họa về bài thực hành:



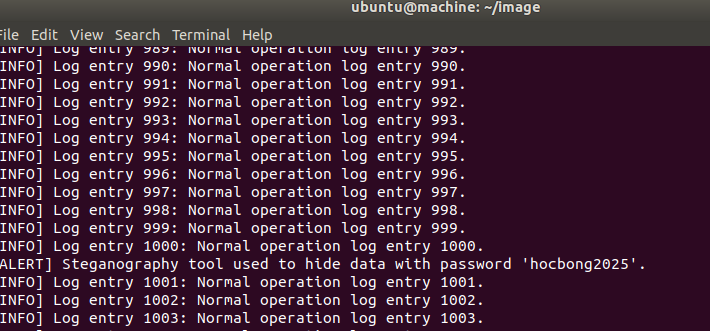
Hình 10. Imodule bài lab về máy



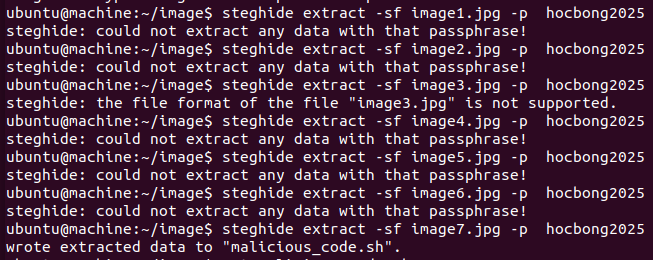
Hình 11. Thư mục hiện tại khi khởi động lab



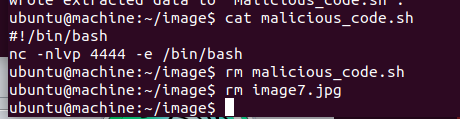
Hình 12. Đọc file log để phát hiện điều bất thường



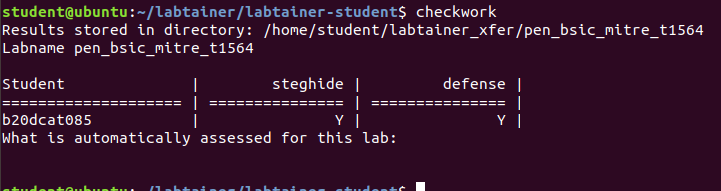
Hình 13. Phát hiện mật khẩu dùng để ẩn giấu hình ảnh với Steganoraphy tool



Hình 14. Extract thông tin các file ảnh trong thư mục /image để tìm ảnh có chứa thông tin ẩn giấu



Hình 15. Đọc file trích xuất được để hiểu hành vi sau đó xóa file ảnh có chứa thông tin ẩn giấu



Hình 16. Kiểm tra tiến độ hoàn thành bài lab