**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**

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

------o0o------



**BÁO CÁO NỘI DUNG 1**

**XÂY DỰNG LAB THỰC HÀNH**

**BUF64\_2 – Nhóm 08**

|  |  |
| --- | --- |
| Môn học: | Chuyên đề an toàn phần mềm |
| Giảng viên: | ThS. Ninh Thị Thu Trang |
| Thành viên: | Phạm Thị Thu Hương – B19DCAT098 |
|  | Đỗ Đức Quốc Anh – B19DCAT003 |
|  | Đoàn Việt Hưng – B19DCAT094 |
|  | Bùi Thanh Phong – B19DCAT135 |

**Hà Nội - 2023**

# MỤC LỤC

[MỤC LỤC 1](#_Toc152554626)

[DANH MỤC CÁC HÌNH VẼ VÀ BẢNG 2](#_Toc152554627)

[I. Nội dung và hướng dẫn thực hiện bài thực hành 3](#_Toc152554628)

[1. Mục đích 3](#_Toc152554629)

[2. Yêu cầu đối với sinh viên 3](#_Toc152554630)

[3. Nội dung thực hành 3](#_Toc152554631)

[II. Phân tích, thiết kế bài thực hành 5](#_Toc152554632)

[1. Phân tích yêu cầu bài thực hành 5](#_Toc152554633)

[2. Thiết kế bài thực hành 5](#_Toc152554634)

[III. Cài đặt và cấu hình các máy ảo 8](#_Toc152554635)

[IV. Thử nghiệm lab và kết quả 15](#_Toc152554636)

[V. Triển khai bài lab 16](#_Toc152554637)

[TÀI LIỆU THAM KHẢO 18](#_Toc152554638)

# DANH MỤC CÁC HÌNH VẼ VÀ BẢNG

[Hình 1. Sơ đồ thiết kế bài thực hành 6](#_Toc152551969)

[Hình 2. Giao diện labedit 8](#_Toc152551970)

[Hình 3. Tạo lab với tên buf64\_2 9](#_Toc152551971)

[Hình 4. Tạo container attacker 10](#_Toc152551972)

[Hình 5. Tạo container server 11](#_Toc152551973)

[Hình 6. Tạo container ghidra 12](#_Toc152551974)

[Hình 7. Tạo mạng mới cho lab 13](#_Toc152551975)

[Hình 8. Cài đặt service binary tại port 1810 14](#_Toc152551976)

[Hình 9. Chỉnh sửa file treataslocal trên máy attacker 14](#_Toc152551977)

[Hình 10. Cài đặt chấm điểm tự động 15](#_Toc152551978)

[Hình 11. build lab và chạy bài lab 15](#_Toc152551979)

[Hình 12. Run lab và thực hiện check work trước khi thực hiện bài lab 16](#_Toc152551980)

[Hình 13. Thực hiện bài lab sau đó check work 16](#_Toc152551981)

[Hình 14. Đẩy bài lab lên git 17](#_Toc152551982)

[Hình 15. Các images của vùng chứa được đẩy lên DockerHub 17](#_Toc152551983)

[Hình 16. Tạo file Imodule tra chứa bài thực hành 18](#_Toc152551984)

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

* Giúp sinh viên hiểu về lỗ hổng bảo mật buffer overflow thông qua việc thực hiện tấn công dịch vụ chứa lỗi.

1. **Yêu cầu đối với sinh viên**

* Có kiến thức cơ bản về hệ điều hành Linux, mô hình mạng khách chủ
* Có kiến thức cơ bản về ngôn ngữ assembly và C/C++
* Có kiến thức cơ bản về lỗ hổng bảo mật buffer overflow

1. **Nội dung thực hành**
   1. **Print win**

*Mục đích: Tìm được địa chỉ hàm win*

**Các bước thực hiện:**

* Từ 1 terminal của attacker sử dụng gdb để debug file binary của service:
* Tại cửa sổ debug của gdb sử dụng lệnh để in ra địa chỉ của hàm win. Output là địa chỉ của hàm win dưới dạng hexa, lưu giá trị này lại phục vụ cho mục đích viết payload
* Thoát khỏi cửa sổ gdb:

***Task 1 quest****: Tại sao cần tìm địa chỉ hàm win? (sử dụng ghidra để hiểu rõ)*

* 1. **Found pattern**

*Mục đích: Tìm được độ dài pattern gây ra lỗi*

**Các bước thực hiện:**

* Thực hiện sinh chuỗi pattern làm đầu vào bằng cách sử dụng lệnh trên cửa sổ terminal của attacker. Output của câu lệnh trên sẽ là chuỗi pattern có độ dài 200, copy chuỗi trên làm input để debug
* Tiến hành chạy trình debug để debug file binary một lần nữa
* Chạy trình debug
* Paste pattern đã gen khi tiến trình yêu cầu nhập input
* Sau khi ấn enter, chương trình sẽ báo lỗi segmentation fault
* Copy 4 ký tự đầu của thanh ghi RSP ở phần REGISTERS
* Thoát tiến trình debugger
* Tìm độ dài pattern gây ra lỗi bằng cách sử dụng cyclic. Output sẽ là độ dài của pattern được sử dụng để tạo payload

***Task 2 quest 1****: Tại sao pattern muốn sinh ra có độ dài là 200, có thể thay đổi số này không, nếu có sẽ thay đổi như thế nào?*

***Task 2 quest 2:*** *Pattern sinh ra có định dạng như thế nào, tại sao phải có định dạng như vậy?*

***Task 2 quest 3:*** *Tại sao lại chọn 4 kí tự đầu tiên trên stack, có thể chọn số lượng kí tự khác được hay không, nếu có giải thích lý do?*

***Task 2 quest 4:*** *Mục đích của những bước trên là gì?*

* 1. **Flag**

*Mục đích: Tìm được nội dung flag được giấu trên server*

**Các bước thực hiện:**

* Sử dụng lệnh nano để mở file payload
* File solve.py là file template sử dụng để tấn công service, mặc định file đã được setup để debug tiến trình buf64\_2
* Payload sẽ có cấu trúc dạng: pattern + return\_address
* Sử dụng pwntools để gửi payload
* Lưu file và thoát sau đó tiến hành chạy
* Tại một cửa sổ terminal của attacker tiến hành chạy file pwnserver để bắt tiến trình debugger
* Tại cửa sổ terminal còn lại của attacker tiến hành chạy file payload
* Khi này cửa sổ pwnserver sẽ bắt lấy trình debugger để có thể tương tác
* Thực hiện gõ lệnh để tiếp tục chương trình
* Tại cửa sổ chạy file payload ấn phím bất kì để tiếp tục tiến trình đang bị tạm dừng. Output có thể thấy tại trình debugger là câu lệnh cat được thực hiện thành công và nội dung flag local được in ra tại cửa sổ chạy payload

***Task 3 quest:*** *Tại sao cần sửa địa chỉ muốn thực thi từ win thành win+16*

* Tiến hành sửa payload để tấn công server
* Tiến hành lưu và chạy lại file payload. Output là nội dung của file flag trên server
* Copy chuỗi số flag sau đó submit trên terminal của attacker

1. **Phân tích, thiết kế bài thực hành**
   * + 1. **Phân tích yêu cầu bài thực hành**

Bài thực hành cần có ba máy tính, trong đó có hai máy tính nằm trong cùng mạng LAN, một máy tính đóng vai trò là công cụ hỗ trợ. Cụ thể như sau, trong mạng LAN gồm có 2 máy, máy attacker là nơi mà sinh viên sẽ tương tác chủ yếu nhằm khai thác thành công binary, máy server sẽ chạy service là binary mà sinh viên cần khai thác, máy ảo còn lại là công cụ hỗ trợ decompile file binary. Để hoàn thành bài thực hành, sinh viên cần sử dụng máy attacker tiến hành khai thác thành công lỗ hổng buffer overflow trên máy chủ để lấy được chuỗi số bí mật.

Để đáp ứng yêu cầu bài thực hành, cần cung cấp 3 container docker. Trong đó, một container đóng vai trò là server, một container đóng vai trò là attacker, container còn lại đóng vai trò là công cụ hỗ trợ, sinh viên có thể dùng đến hoặc không (trong trường hợp sinh viên muốn dùng công cụ decompiler trực tiếp trên máy attacker). Hệ thống cần ghi lại được thao tác sử dụng các lệnh trên terminal container của sinh viên để tạo ra được kết quả đánh giá. Hệ thống yêu cầu sinh viên nhập email gắn liền với danh tính của sinh viên để thực hiện việc cá nhân hóa cho từng sinh viên.

Để bắt đầu bài thực hành sinh viên cần phải sử dụng các câu lệnh khởi tạo (labtainer -r <tên bài lab>) và câu lệnh kết thúc (stoplab <tên bài lab>) để hệ thống chạy bài lab cũng như lưu lại kết quả.

* + - 1. **Thiết kế bài thực hành**

Trên môi trường máy ảo Ubuntu được cung cấp, sử dụng docker tạo ra 3 container: 1 container mang tên “buf642” đóng vai trò là attacker và 1 container mang tên “server” đóng vai trò là server, 2 máy đều được mở các cổng cần thiết. Hình 1 mô tả sơ đồ thiết kế bài thực hành.

A black and white image of a router

Description automatically generated

Hình 1. Sơ đồ thiết kế bài thực hành

* Tạo mạng LAN “TEST” có cấu hình: 192.168.1.0/24 và gateway 192.168.1.1
* Cấu hình docker gồm có:
  + Buf64\_2: Lưu cấu hình cho máy attacker, trong đó gồm có:
    - Tên máy: attacker
    - Địa chỉ trong mạng LAN: 192.168.1.3
    - Gateway: 192.168.1.1
  + Server: Lưu cấu hình cho máy server, trong đó gồm có:
    - Tên máy: server
    - Địa chỉ trong mạng LAN: 192.168.1.2
    - Gateway: 192.168.1.1
  + Ghidra: sử dụng để decompile binary:
    - Tên máy: ghidra-vm
    - Địa chỉ trong mạng LAN: N/A
  + Config: Lưu cấu hình hoạt động của hệ thống
  + Dockerfiles: Mô tả cấu hình của 3 container: attacker, ghidra và server, trong đó:
    - Attacker sử dụng base image cần cài thêm netcat và git để setup tools
    - Server sử dụng network base image cần cài thêm rsync để setup service xinetd
    - Ghidra sử dụng ghidra base image không cần config gì thêm
  + Docs: Lưu phần mô tả hướng dẫn làm bài thực hành cho sinh viên
  + Instr\_config: Lưu cấu hình cho phần nhận kết quả và chấm điểm
* Thiết lập hệ thống mạng sao cho 2 container 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 đưa vào đó đánh giá, chấm điểm. Do vậy, trong bài thực hành này hệ thống cần ghi nhân các thao tác, sự kiện được mô tả và cấu hình như bảng 1

Bảng 1. Cấu hình cho kiểm tra thao tác

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Result Tag** | **Container** | **File** | **Field Type** | **Field ID** | **Timestamp Type** |
| \_print\_command | Buf64\_2 | \*.stdout | FILE\_REGEX | p.\*win | File |
| \_print\_win | Buf64\_2 | \*.stdout | CONTAINS | 0x400707 | File |
| \_crash | Buf64\_2 | \*.stdout | CONTAINS | Program received signal SIGSEGV, Segmentation fault. | File |
| \_stack\_pattern | Buf64\_2 | \*.stdout | FILE\_REGEX | RSP.\*saaataaa | File |
| \_find\_pattern | Buf64\_2 | \*.stdout | CONTAINS | 72 | File |
| \_ret\_win | Buf64\_2 | \*.stdout | FILE\_REGEX | RIP.\*win | file |
| \_echo | Buf64\_2 | echo.stdout | TOKEN | LAST | STARTWITH flag |

* Sau khi có đầu vào thao tác, tiến hành kiểm tra để cho ra kết quả cuối ‘Goal result’ như bảng 2

Bảng 2. Cấu hình cho kiểm tra kết quả

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| \_crash\_goal | boolean | (\_print\_command and \_print\_win) | | | |
| Print\_win | boolean | (\_crash and \_stack\_pattern) | | | |
| Found\_pattern | boolean | (\_crash\_goal and \_find\_pattern) | | | |
| flag | matchany | String\_contains | \_echo | Parameter | FLAG\_ |

* Sau khi nhận được file đóng gói từ sinh viên, giảng viên sử dụng chức năng chấm điểm để xem kết quả được thiết kế dưới dạng bảng trong đó có ghi rõ email của sinh viên thực hiện, từng tiêu chí chấm điểm được ghi nhận (ví dụ: ‘Y’ là đã hoàn thành, nếu không có là chưa hoàn thành) và kết luận là sinh viên đã hoàn thành bài thực hành đó hay chưa. Kiểm tra bài thực hành đúng do sinh viên làm bằng cách kiểm tra email (xem bảng 2).

Bảng 3. Kết quả chấm điểm

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Student** | **Print\_win** | **Found\_pattern** | **Flag** | **Secret** |
| Mã sinh viên | Y | Y | Y | Y |

Y: đã hoàn thành

1. **Cài đặt và cấu hình các máy ảo**

* Cần chạy file update-designer.sh để cập nhật bản mới nhất của labedit
* Từ đường dẫn bất kì trên terminal gõ lệnh labedit, sau đó màn hình sẽ hiển thị giao diện như hình 2:

**A screenshot of a computer

Description automatically generated**

Hình 2. Giao diện labedit

* Thực hiện tạo lab mới: File -> New Lab và đặt tên cho bài lab

**A screenshot of a computer

Description automatically generated**

Hình 3. Tạo lab với tên buf64\_2

* Sau khi lab được khởi tạo, tạo 3 container với base image lần lượt là: base2, network2, ghidra

A screenshot of a computer

Description automatically generated

Hình 4. Tạo container attacker

A screenshot of a computer

Description automatically generated

Hình 5. Tạo container server

A screenshot of a computer

Description automatically generated

Hình 6. Tạo container ghidra

* Tạo networks mới cho lab, đặt tên network, cài đặt giải mạng con và gateway cho mạng

A screenshot of a computer

Description automatically generated

Hình 7. Tạo mạng mới cho lab

* Cấu hình mạng cho Attacker và Server:
  + Attacker:
    - IP: 192.168.1.3/24
    - GW: 192.168.1.1
  + Server:
    - IP 192.168.1.2/24
    - GW: 192.168.1.1
    - Service port: 1810
* Cài đặt thêm công cụ pwntools và extension pwndbg cho container attacker
* Cài đặt service binary cho container server

A screenshot of a computer

Description automatically generated

Hình 8. Cài đặt service binary tại port 1810

* Chỉnh sửa file treataslocal để tạo task đánh giá cho từng container bằng cách chỉnh sửa file treataslocal từ labedit hoặc chỉnh sửa trực tiếp theo đường dẫn ~/labtainer/trunk/labs/<tên-lab>/<tên-container>/\_bin/treataslocal

A screenshot of a computer

Description automatically generated

Hình 9. Chỉnh sửa file treataslocal trên máy attacker

* Cài đặt Results ở phần Automated Assesment:

A screenshot of a computer

Description automatically generated

Hình 10. Cài đặt chấm điểm tự động

* Tiến hành save lab, sau đó build và chạy thử lab

A screenshot of a computer program

Description automatically generated

Hình 11. build lab và chạy bài lab

1. **Thử nghiệm lab và kết quả**

A screenshot of a computer program

Description automatically generated

Hình 12. Run lab và thực hiện check work trước khi thực hiện bài lab

A screenshot of a computer

Description automatically generated

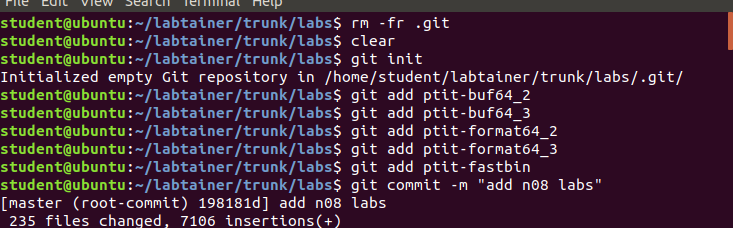
Hình 13. Thực hiện bài lab sau đó check work

1. **Triển khai bài lab**

* Chuyển tới thư mục chứa các bài thực hành: **labtainer/trunk/labs**
* Khởi tạo git: **git init** (chỉ khởi tạo một lần, không lặp lại với mỗi lần).
* Lấy tên của Docker Hub để đăng ký cho registry bài lab mới ở config/start.config (tại Labtainers GUI: Edit / Config (registry))
* Trong đường dẫn thư mục của bài lab bai-lab-moi. Chạy cleanlab4svn.py để xóa những files tạm.
* Sau đó trong đường dẫn cha của bài lab:

git add <tên bài lab> git commit <tên bài lab> -m

"Adding an IModule"



Hình 14. Đẩy bài lab lên git

* Đẩy images của vùng chứa (container) lên DockerHub

cd $LABTAINER\_DIR/distrib

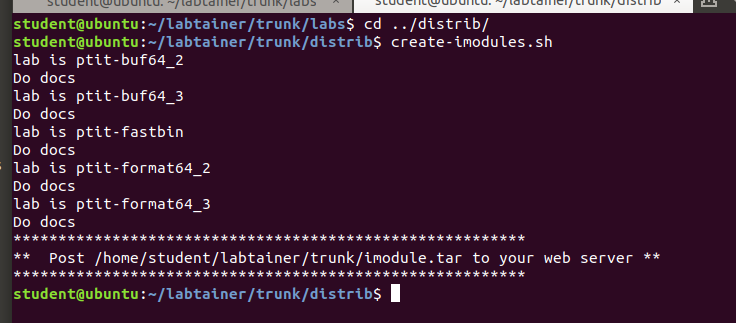
./publish.py -d -l my-new-lab

A computer screen shot of a computer

Description automatically generated

Hình 15. Các images của vùng chứa được đẩy lên DockerHub

* Tạo file IModule tar chứa bài thực hành: create-imodules.sh



Hình 16. Tạo file Imodule tra chứa bài thực hành

* Sau đó, copy và lưu lại file imodule.tar. Đường dẫn URL vào link imodule:

<https://github.com/iluvinn/cdatpm-ptit.git>

# TÀI LIỆU THAM KHẢO

[**Labtainer Lab Designer User Guide**](https://nps.edu/documents/107523844/117289221/labdesigner.pdf/9ab93fc3-7cfe-48f4-987b-2efda8d99346?t=1606868757623&fbclid=IwAR2yU821lOFKnv0lNBQBtKcPFzQpuag2uYt9QUBFJEyBsBObT1yVkvVHDaw)