BÁO CÁO BÀI TẬP

**Môn học: An toàn mạng**

**Tên chủ đề: Packet Sniffing and Spoofing**

*GVHD: Nghi Hoàng Khoa*

**Nhóm: 06**

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT140.O11.ANTT

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Họ và tên | MSSV | Email |
| 1 | Nguyễn Triệu Thiên Bảo | 21520155 | 21520155@gm.uit.edu.vn |
| 2 | Trần Lê Minh Ngọc | 21521195 | 21521195@gm.uit.edu.vn |
| 3 | Huỳnh Minh Khuê | 21522240 | 21522240@gm.uit.edu.vn |
| 4 | Nguyễn Thị Hồng Lam | 20521518 | 20521518@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |
| --- | --- | --- |
| STT | Nội dung | Tình trạng |
| 1 | Yêu cầu 1 | 90% |
| 2 | Yêu cầu 2 | 100% |

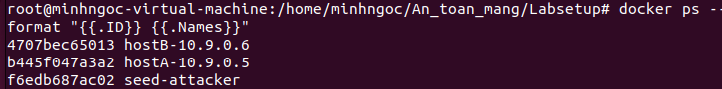
**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

**4 Lab Task Set 2: Writing Programs to Sniff and Spoof Packets**

**4.1 Task 2.1: Writing Packet Sniffing Program**

**Task 2.1A: Understanding How a Sniffer Works**



* Biên dịch và chạy file sniffex.

A screenshot of a computer code

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Câu hỏi 1:** Mô tả chuỗi các cuộc gọi thư viện cần thiết cho các sniffer programs.

* Pcap\_lookupdev: Tìm một thiết bị bắt gói tin (capture device) để theo dõi.

A computer screen shot of a program

Description automatically generated

* Pcap\_lookupnet: lấy number và mask của network cho thiết bị bắt gói tin.

A screen shot of a computer

Description automatically generated

* Pcap\_open\_live: mở và bắt đầu theo dõi thiết bị bắt gói tin.

A white screen with black text

Description automatically generated

* Pcap\_datalink: xác định loại thiết bị mà chúng ta đang sử dụng để bắt gói tin.

A computer screen shot of a computer

Description automatically generated

* Pcap\_compile: biên dịch biểu thức bộ lọc (filter expression)

A computer code with text

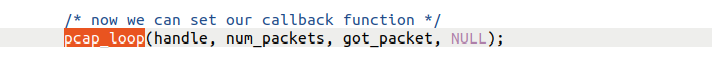
Description automatically generated with medium confidence

* Pcap\_setfilter: thiết lập bộ lọc đã được biên dịch

A computer screen shot of a computer

Description automatically generated

* Pcap\_loop: Thiết lập callback function cho các gói tin mới đã được lọc.



* Pcap\_freecode: giải phóng bộ nhớ đã được cấp phát bởi pcap\_compile.



* Pcap\_close: đóng phiên theo dõi.



**Câu hỏi 2:** Tại sao phải cần quyền root để chạy một chương trình theo dõi (sniffer program)? Chương trình sẽ gặp sự cố ở đâu nếu chạy mà không có quyền root?

* Nếu không mở quyền root khi chạy chương trình sẽ bị lỗi.

A computer screen shot of a program

Description automatically generated

* Đoạn code bị lỗi:

A close up of text

Description automatically generated

* Cần mở quyền root để thực thi vì:
* Chương trình theo dõi thường cần tương tác với giao diện mạng để bắt các gói tin mạng. Những giao diện này thường bị hạn chế để ngăn chặn truy cập trái phép. Nếu thiếu quyền root, người dùng sẽ không có quyền đọc gói tin từ những giao diện này.
* Các chương trình theo dõi thường đặt giao diện mạng vào chế độ promiscuous, cho phép chúng bắt tất cả lưu lượng mạng trên giao diện, không chỉ lưu lượng dành cho máy chủ của người dùng. Chế độ này chỉ có thể được bật bởi người dùng có quyền root.
* Thiếu quyền root, chương trình chỉ có thể bắt các gói tin được gửi đặc biệt đến máy chủ của người dùng, giới hạn gói tin bắt được.

**Câu hỏi 3:** Vui lòng bật và tắt chế độ Promiscuous trong chương trình theo dõi. Giá trị 1 của tham số thứ ba trong pcap\_open\_live() bật chế độ Promiscuous (sử dụng giá trị 0 để tắt nó). Có thể minh họa sự khác biệt khi chế độ này được bật và tắt không? Hãy mô tả cách làm.

* Khi chế độ Promiscuous được bật:

Khi giao diện mạng ở chế độ Promiscuous, nó sẽ nhận và ghi lại tất cả các gói tin mạng mà nó nhận được, bất kể địa chỉ nguồn và đích của gói tin. Điều này có nghĩa rằng chúng ta có thể bắt được tất cả các gói tin trên mạng.

A screen shot of a computer

Description automatically generated

* Khi chế độ Promiscuous bị tắt:

Khi chế độ Promiscuous bị tắt, giao diện mạng chỉ nhận và xử lý các gói tin mạng mà có địa chỉ nguồn hoặc đích là địa chỉ của nó. Nghĩa là nó chỉ nhận những gói tin mà dành riêng cho nó hoặc được gửi trực tiếp đến nó. Những gói tin khác trên mạng sẽ không được chấp nhận.

A close up of a computer screen

Description automatically generated

**Task 2.1B: Writing Filters.**

1. **Capture the ICMP packets between two specific hosts**

* Dùng filter\_exp để lọc các ICMP packets

A computer code with black text

Description automatically generated

* Kết nối đến 8.8.8.8

A screenshot of a computer program

Description automatically generated

* Biên dịch và thực thi tập tin sniffex

A computer screen shot of a program

Description automatically generated

1. **Capture the TCP packets with a destination port number in the range from 10 to 100.**

* Dùng filter\_exp để lọc các TCP packets có port đích từ 10 đến 100

A computer screen shot of a computer

Description automatically generated

* Biên dịch và thực thi tập tin sniffex

A screenshot of a computer program

Description automatically generated

**Task 2.3: Sniff and then Spoof**

* Kết nối đến máy ảo VMWARE và đăng nhập

A screenshot of a computer screen

Description automatically generated

* Dùng filter\_exp để lọc các TCP packets có port 23

A computer screen shot of a computer code

Description automatically generated

* Biên dịch và thực thi tập tin sniffex: các dòng phía dưới chữ password chính là password cần tìm “91…….”

A screenshot of a computer

Description automatically generated

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)