BỘ GIÁO DỤC VÀ ĐÀO TẠO

**TRƯỜNG ĐẠI HỌC NHA TRANG**

**KHOA CÔNG NGHỆ THÔNG TIN**

****

**BÁO CÁO THỰC TẬP CƠ SỞ**

**TÌM HIỂU VÀ CÀI ĐẶT CHƯƠNG TRÌNH ĐỌC FILE PCAP XUẤT CẤU TRÚC GÓI TIN CỦA CÁC GIAO THỨC CƠ BẢN CỦA CHỒNG GIAO THỨC TCP/IP**

**Giảng viên hướng dẫn: ThS. Cấn Thị Phượng**

**Sinh viên thực hiện: Trần Phạm Cẩm Nhung**

**Đinh Thị Nhật Quỳnh**

**Mã số sinh viên: 61134141**

**61130956**

Khánh Hòa – 2021

BỘ GIÁO DỤC VÀ ĐÀO TẠO

**TRƯỜNG ĐẠI HỌC NHA TRANG**

**KHOA CÔNG NGHỆ THÔNG TIN**

****

**TÌM HIỂU VÀ CÀI ĐẶT CHƯƠNG TRÌNH ĐỌC FILE PCAP XUẤT CẤU TRÚC GÓI TIN CỦA CÁC GIAO THỨC CƠ BẢN CỦA CHỒNG GIAO THỨC TCP/IP**

**Giảng viên hướng dẫn: ThS. Cấn Thị Phượng**

**Sinh viên thực hiện: Trần Phạm Cẩm Nhung**

**Đinh Thị Nhật Quỳnh**

**Mã số sinh viên: 61134141**

**61130956**

Khánh Hòa – 2021

**LỜI CAM ĐOAN**

Chúng em xin cam đoan: Đề tài thực tập cơ sở“**Tìm hiểu và cài đặt chương trình đọc file pcap xuất cấu trúc gói tin của các giao thức của chồng giao thức TCP/IP**” là kết quả tự tìm hiểu, làm việc nhóm và cùng với sự hướng dẫn của ThS.Cấn Thị Phượng. Các kết quả nghiên cứu trong đề tài là dựa trên những kết quả có sẵn và chúng em đã tự đọc hiểu và trình bày lại. Những phần sử dụng tài liệu tham khảo trong đây đã được trích dẫn đầy đủ.

|  |
| --- |
| *Khánh Hòa, ngày tháng năm 2021*  **Sinh viên thực hiện**  Trần Phạm Cẩm Nhung Đinh Thị Nhật Quỳnh |

# **LỜI CẢM ƠN**

Để hoàn thành đề tài tốt nghiệp này, trước hết em xin gửi đến quý thầy, cô Khoa Công nghệ Thông tin - Trường Đại học Nha Trang lời cảm ơn chân thành.

Em xin gửi đến cô Cấn Thị Phượng, đã hướng dẫn, giúp đỡ nhóm em hoàn thành đề tài thực tập cơ sở này lời cảm ơn sâu sắc nhất.

Trong quá trình nghiên cứu thực hiện đề tài, cũng như là trong quá trình làm bài báo cáo tốt nghiệp, khó tránh khỏi sai sót, rất mong các thầy, cô bỏ qua. Đồng thời do kiến thức cũng như kinh nghiệm thực tiễn của bản thân còn hạn chế nên bài báo cáo này khó thể không tránh khỏi những thiếu sót, em rất mong nhận được ý kiến đóng góp từ quý thầy, cô để nhóm chúng em học hỏi thêm được nhiều kinh nghiệm, cũng như kỹ năng cần thiết.

Chúng em xin chân thành cảm ơn!

**TÓM TẮT KHÓA LUẬN**

Với thời gian thực hiện đồ án còn hạn chế nên đề tài “**Tìm hiểu và cài đặt chương trình đọc file pcap xuất cấu trúc gói tin của các giao thức cơ bản của chồng giao thức TCP/IP**” chỉ dừng ở mức tìm hiểu và trình bày được file pcap, tổ chức dữ liệu và cài đặt chương trình hoàn chỉnh đọc cấu trúc file của 1 số giao thức cơ bản như ARP, TCP, IP,HTTP...; tìm hiểu ứng dụng file pcap.

Vận dụng ngôn ngữ lập trình C++, hoặc python, hoặc ngôn ngữ khác, lập trình

hướng đối tượng, tìm hiểu file pcap, củng cố cấu trúc gói tin của chồng giao thức TCP/IP,

tìm hiểu ứng dụng việc phân tích file pcap. Rèn luyện kỹ năng giải quyết vấn đề, làm việc

nhóm, quản lý mã nguồn.

**Chương 2: TỔNG QUAN FILEP CAP**

***2.1. Khái niệm File Pcap***

PCAP là viết tắt của dữ liệu bắt gói dữ liệu dạng tệp, sử dụng định dạng N / A do Wireshark phát triển.

Tệp dữ liệu được tạo bởi Wireshark (trước đây là Ethereal), là một chương trình miễn phí để phân tích mạng; chứa dữ liệu gói mạng được tạo ra trong quá trình chụp mạng; được sử dụng để "đánh hơi gói" và phân tích các đặc điểm của mạng dữ liệu; Phần mềm bao gồm thư viện libpcap hoặc WinPcap để phân tích.

***2.2. Ứng dụng của File Pcap***

Một số cách phổ biến nhất bao gồm giám sát việc sử dụng băng thông, xác định máy chủ DHCP độc hại, phát hiện phần mềm độc hại, phân giải DNS và phản ứng sự cố.

Dữ liệu PCAP cung cấp cho bạn thông tin thời gian thực mà bạn cần để tìm và giải quyết các vấn đề về hiệu suất để giữ cho mạng hoạt động sau sự cố bảo mật. Nếu không có PCAP và các công cụ bắt gói, việc theo dõi gói và quản lý rủi ro bảo mật sẽ khó phát hiện.

**Chương 3: TỔNG QUAN VỀ TCP/IP**

***3.1. Khái niệm về TCP/IP***

TCP / IP là một giao thức điều khiển đường truyền / giao thức Internet. Đây là từ viết tắt của Transmission Control Protocol / Internet Protocol. TCP / IP là một tập hợp các quy tắc, một tập hợp các giao thức trao đổi thông tin được tiêu chuẩn hóa cho phép các máy tính giao tiếp thông qua một mạng (chẳng hạn như Internet). TCP / IP có chức năng khôi phục tự động.

***3.2. Ưu – nhược điểm của TCP/IP***

Thiết lập kết nối giữa các loại máy tính.

Làm việc độc lập với hệ điều hành.

Hỗ trợ nhiều giao thức định tuyến.

Kiến trúc máy khách-máy chủ, khả năng mở rộng cao.

Có thể hoạt động độc lập.

Hỗ trợ nhiều giao thức định tuyến.

Dung lượng nhẹ, nó sẽ không gây quá nhiều áp lực cho máy tính hoặc mạng. Nhược điểm của TCP/IP

Việc cài đặt khá phức tạp và khó quản lý.

Lớp truyền tải không đảm bảo việc phân phối các gói dữ liệu.

Các giao thức trong TCP / IP không dễ thay thế.

Không có sự phân tách rõ ràng về các dịch vụ, giao diện và các khái niệm giao thức. Do đó, việc mô tả công nghệ mới trong mạng mới là không hiệu quả.

Dễ bị tấn công SYN - một cuộc tấn công từ chối dịch vụ.

***3.3. Ứng dụng của TCP/IP***

Giao thức TCP / IP có thể được sử dụng để đăng nhập từ xa, truyền tệp tương tác, truyền e-mail qua mạng, phân phối các trang web qua mạng và truy cập từ xa vào hệ thống máy chủ. Nói cách khác, nó được sử dụng để diễn đạt cách thông tin thay đổi liên tục được hình thành khi nó di chuyển qua mạng. Từ lớp vật lý cụ thể đến lớp ứng dụng trừu tượng. Với việc truyền thông tin, TCP / IP xác định chi tiết giao thức cơ bản hoặc phương thức truyền thông của từng lớp.

**Chương 4: TỔ CHỨC DỮ LIỆU VÀ CÀI ĐẶT CHƯƠNG TRÌNH HOÀN CHỈNH ĐỌC CẤU TRÚC FILE CỦA MỘT SỐ GIAO THỨC CƠ BẢN NHƯ ARP, TCP, IP, HTTP…**

***4.1. Tổ chức dữ liệu:***