**Trường Đại học Kinh tế Đà Nẵng**

**Nhóm 14**

Tên thành viên:

Nguyễn Thị Kim Tuyến ( Nhóm trưởng + nội dung + thời gian)

Lê Bá Kông (Nội dung + Văn bản)

Trần Thị Phúc ( Văn bản + nội dung)

Nguyễn Thị Hoài Phương ( Nội dung + slide)

Hoàng Thị Khánh Như ( Nội dung + slide)

**CHỦ ĐỀ: DHCP**

1. **Lý do chọn chủ đề**
2. **Phạm vi nghiên cứu**
3. **Phạm vi hẹp**
4. **Phạm vi rộng**
5. **Mục tiêu**
6. **Lý thuyết**

* Hiểu rõ được ý nghĩa của việc dùng DHCP server và các vấn đề của dịch vụ DHCP server.
* Nắm rõ cơ chế hoạt động, các ưu nhược điểm cũng như cách cài đặt DHCP.
* Đưa ra giải pháp bảo mật cho DHCP.

1. **Triển khai**
2. **Nội dung**
3. **CHƯƠNG 1: TỔNG QUAN VỀ DHCP**

**1.1** Lịch sử hình thành

1.2 Thực trạng tại Việt Nam

1.3 Xu hướng phát triển trong tương lai

***1.4 Khái niệm***

Đặc điểm chung của DHCP

1.3 Chức năng và vai trò của DHCP (ưu nhược điểm)

1.4 Xu hướng phát triển của DHCP

1.2 Đặc điểm chung của DHCP

1.3 Chức năng và vai trò của DHCP (ưu nhược điểm)

1.4 Xu hướng phát triển của DHCP

1. Lịch sử hình thành
2. Thực trạng tại Việt Nam
   1. Xu hướng pt trong tương lai

1.1.1. Tấn công mạng là gì?

1.1.2. Đối tượng bị tấn công

* 1. ***Đặc điểm của tấn công mạng hiện nay***

1.2.1. Mục đích tấn công?

1.2.2. Hacker là ai?

1.2.3. Phân biệt Hacker mũ đen và hacker mũ trắng?

1. **CHƯƠNG 2: CÁC HÌNH THỨC VÀ PHƯƠNG THỨC TẤN CÔNG MẠNG PHỔ BIẾN**
   1. ***Các phương thức tấn công***

2.1.1. Tấn công từ bên trong nội bộ

2.1.2. Tấn công gián tiếp

2.1.3. Tấn công theo tệp đính kèm

2.1.4. Tấn công ẩn danh

2.1.5. Tấn công vào con người

2.1.6. Tấn công với hình thức Fishing

**2.2. *Hình thức tấn công***

2.2.1. Tấn công bằng phần mềm độc hại (Malware attack)

2.2.2. Tấn công giả mạo (Phishing attack)

2.2.3. Tấn công trung gian (Man-in-the-middle attack)

2.2.4. Tấn công từ chối dịch vụ (DoS và DDoS)

2.2.5. Tấn công cơ sở dữ liệu (SQL injection)

2.2.6. Khai thác lỗ hổng Zero-day (Zero day attack)

1. **CHƯƠNG 3: GIẢI PHÁP VÀ ỨNG DỤNG CHỐNG TẤN CÔNG MẠNG**
   1. **Đối với cá nhân**

3.1.1 Trình bày các loại mã độc phổ biến tấn công qua email

3.1.1.1 Dịch vụ email và các nguy cơ bị tấn công qua mail

3.1.1.1.1 Tìm hiểu về dịch vụ email

3.1.1.1.2 Các nguy cơ tấn công qua email

3.1.1.2 Thực trạng tấn công qua emai năm 2017 – 2019

3.1.1.2.1 Số liệu các vụ tấn công mạng

3.1.1.2.2 Xu hướng tấn công qua email các năm gần đây

3.1.1.2.3 Các loại mã độc qua email phổ biến

3.1.1.3 Nguồn gốc và cách phòng chống

3.1.1.3.1 Tấn công mạng và hình thức Phishing

3.1.1.3.2 Tấn công theo tệp đính kèm

1. **CHƯƠNG 4:** **TỔNG KẾT**
   1. **Kết quả đạt được**
   2. **Ưu & nhược điểm của nhóm**
   3. **Hướng phát triển chủ đề**

**Nhóm 14**

Tên thành viên:

Nguyễn Thị Kim Tuyến ( Nhóm trưởng + nội dung + thời gian)

Lê Bá Kông (Nội dung + Văn bản)

Trần Thị Phúc ( Văn bản + nội dung)

Nguyễn Thị Hoài Phương ( Nội dung + slide)

Hoàng Thị Khánh Như ( Nội dung + slide)

**ĐỀ CƯƠNG SƠ BỘ**

**CHỦ ĐỀ: DHCP**

**I. MỤC TIÊU**

* Hiểu rõ được ý nghĩa của việc dùng DHCP server và các vấn đề của dịch vụ DHCP server.
* Nắm rõ cơ chế hoạt động, các ưu nhược điểm cũng như cách cài đặt DHCP.
* Đưa ra giải pháp bảo mật cho DHCP.

**CHƯƠNG 1: TỔNG QUAN VỀ DHCP**

1. Khái niệm

2. Chức năng và vai trò của DHCP (ưu nhược điểm)

3. đặc điểm chung của DHCP

4. XU hướng phát triển của DHCP

1. Lịch sử hình thành
2. Thực trạng tại Việt Nam

Xu hướng pt trong tương lai

**CHƯƠNG 2: CÁC CÔNG NGHỆ VÀ KỸ THUẬT CỦA DHCP**

1.3 Kiến trúc của DHCP

1.2. Cơ chế hoạt động của DHCP.

1.4 Cài đặt và cấu hình DHCP

1.5 Cấu hình các thông số cho DHCP Server.

1.6. giao thức

1.7 mô hình truyền thông

~~1.6 Ưu nhược điểm~~

**CHƯƠNG 3: TRIỂN KHAI DHCP CHO CÁ NHÂN/DOANH NGHIỆP**

3.1: Phương án triển khai

Cấu hình DHCP trên router

3.2: Giải pháp bảo mật cho DHCP

**CHƯƠNG 4: TỔNG KẾT**

4.1 Kết quả đạt được

4.2 Hướng phát triển cho đề tài