

BỘ CÔNG THƯƠNG  
TRƯỜNG ĐẠI HỌC SAO ĐỎ



**ĐỒ ÁN/KHOÁ LUẬN TỐT NGHIỆP**

**Ngành: CÔNG NGHỆ THÔNG TIN**

**TÊN ĐỀ TÀI: NGHIÊN CỨU XÂY DỰNG HỆ THỐNG  
CẢNH BÁO TẤN CÔNG MẠNG**

**Họ và tên sinh viên: Trương Hồng Hiệp**

**Lớp, khoá: DK10- CNTT**

**Giảng viên hướng dẫn: Nguyễn Thị Thu**

HẢI DƯƠNG – NĂM...

**NHIỆM VỤ ĐỒ ÁN/KHOÁ LUẬN TỐT NGHIỆP**

**1. Thông tin chung:**

Họ và tên sinh viên: Trương Hồng Hiệp      Mã SV:1900837  
Lớp, khoá: DK10- CNTT      Ngành đào tạo: Công nghệ thông tin  
Hệ đào tạo: Chính quy  
Thời gian thực hiện đồ án tốt/khoa luận: Từ ngày 01/08/2023 đến 01/12/2023  
Giảng viên hướng dẫn: Nguyễn Thị Thu      Học hàm, học vị: .....

**2. Tên đề tài: Nghiên cứu xây dựng hệ thống cảnh báo tấn công mạng**

**3. Điều kiện cho trước:**

- Hệ thống mạng máy tính
- Towards an Early Warning System for Network Attacks Using Bayesian Inference
- DOI: 10.1109/CSCloud.2015.35. Publish: IEEE

**4. Nhiệm vụ chính của đồ án/khoa luận:**

- Nghiên cứu kiến trúc cơ bản của hệ thống mạng máy tính LAN, WAN và Internet .
- Nghiên cứu một số kỹ thuật tấn công hệ thống mạng máy tính
- Nghiên cứu và xây dựng hệ thống cảnh báo tấn công mạng

**5. Sản phẩm:**

- Bản thuyết minh ĐA/KL: 02 bản bìa cứng, 05 bản bìa mềm.
- Hệ thống cảnh báo tấn công mạng
- Đĩa CD ( phần mềm, nội dung đồ án, silde thuyết trình)

*Hải Dương, ngày.....tháng.....năm .....*

**TL. HIỆU TRƯỞNG  
TRƯỜNG KHOA .....**  
(Ký, ghi rõ họ và tên và đóng dấu)

**GIẢNG VIÊN HƯỚNG DẪN**  
(Ký, ghi rõ họ và tên)

## **LỜI CAM ĐOAN**

Tôi xin cam đoan các kết quả đưa ra trong đồ án/khóa luận tốt nghiệp này là các kết quả thu được trong quá trình nghiên cứu, thực nghiệm của tôi dưới sự hướng dẫn của cô Nguyễn Thị Thu, không sao chép bất kỳ kết quả nghiên cứu nào của các tác giả khác.

Nội dung nghiên cứu có tham khảo và sử dụng một số thông tin, tài liệu từ các nguồn tài liệu đã được liệt kê trong danh mục các tài liệu tham khảo.

Nếu sai tôi xin chịu mọi hình thức kỷ luật theo quy định.

*Hải Dương, ngày..... tháng..... năm.....*

**Sinh viên thực hiện**

*(Ký, ghi rõ họ và tên)*

Đại học Sao Đỏ

**BẢN NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN**

Tên đề tài: Nghiên cứu xây dựng hệ thống cảnh báo tấn công mạng

Họ tên sinh viên: Trương Hồng Hiệp

Mã sinh viên: .....

Lớp: DK 10- CNTT

Khoa: 10

Giảng viên hướng dẫn: Nguyễn Thị Thu

Học hàm, học vị: .....

Đơn vị công tác: Đại học Sao Đỏ

**NỘI DUNG:**

1. Đánh giá về tinh thần, thái độ của sinh viên trong quá trình thực hiện đề tài:

.....  
.....  
.....

2. Đánh giá về bô cục, hình thức trình bày:

.....  
.....  
.....

3. Đánh giá về những kết quả đạt được:

.....  
.....  
.....

4. Kết luận: Tôi đồng ý (hoặc không đồng ý) cho sinh viên ..... được bảo vệ trước Hội đồng đánh giá đồ án, khóa luận tốt nghiệp.

5. Điểm đánh giá: \* .....

Hải Dương, ngày..... tháng.... năm 20...

**GIẢNG VIÊN HƯỚNG DẪN**

(Ký, ghi rõ họ và tên)

\* Điểm đồ án, khóa luận tốt nghiệp được đánh giá theo thang điểm 10 sau đó chuyển thành điểm chữ và thang điểm 4 theo quy định.

**BẢN NHẬN XÉT CỦA ỦY VIÊN PHẢN BIỆN**

Tên đề tài: Nghiên cứu xây dựng hệ thống cảnh báo tấn công mạng

Họ tên sinh viên: Trương Hồng Hiệp

Mã sinh viên: 1900837

Lớp:Dk10- CNTT

Khoá:10

Ủy viên phản biện:.....Học hàm, học vị:.....

Đơn vị công tác: .....

**NỘI DUNG:**

1. Đánh giá về bố cục, hình thức trình bày:

.....  
.....  
.....

2. Đánh giá về sự không trùng lặp, tính trung thực :

.....  
.....  
.....

3. Đánh giá về những kết quả đạt được:

.....  
.....  
.....

4. Các vấn đề cần làm rõ hay bổ sung, chỉnh sửa (*nếu có*):

5. Kết luận: Tôi đồng ý (hoặc không đồng ý) cho sinh viên ..... được bảo vệ trước Hội đồng đánh giá đồ án, khóa luận tốt nghiệp.

6. Điểm đánh giá:\*

Hải Dương, ngày.....tháng....năm 20...

**ỦY VIÊN PHẢN BIỆN**  
(Ký, ghi rõ họ và tên)

**Ghi chú:**

- Giảng viên phản biện chuẩn bị từ 2 đến 3 câu hỏi để sinh viên trả lời trước hội đồng khi chất lượng Đồ án/Khoa luận đủ điều kiện được bảo vệ trước Hội đồng.
- Điểm đồ án, khoa luận tốt nghiệp được đánh giá theo thang điểm 10 sau đó chuyển thành điểm chữ và thang điểm 4 theo quy định.

Đại học Sao Đỏ

**TRÌNH TỰ THỰC HIỆN CHẤM  
ĐỒ ÁN/KHOÁ LUẬN TỐT NGHIỆP ĐẠI HỌC CHÍNH QUY**

1. Thư ký Hội đồng công bố quyết định của Hiệu trưởng về việc thành lập các hội đồng chấm ĐA/KL;
2. Chủ tịch hội đồng thông báo số lượng thành viên hội đồng, tên đê tài và điều hành buổi bảo vệ ĐA/KL;
3. Người học báo cáo tóm tắt nội dung ĐA/KL trong khoảng từ 15 ÷ 25 phút.
4. Ủy viên phản biện đọc nhận xét và đặt câu hỏi cho người học.
5. Chủ tịch hội đồng điều hành, mời các thành viên của hội đồng đặt câu hỏi và người học trả lời các câu hỏi của ủy viên phản biện, uỷ viên hội đồng.
6. Chủ tịch hội đồng nhận xét đánh giá về tinh thần, thái độ, tác phong làm việc, kết quả nghiên cứu và nội dung trả lời của người học.
7. Hội đồng họp và chấm điểm độc lập; thư ký hội đồng tổng hợp kết quả, ghi biên bản;
8. Chủ tịch hội đồng công bố điểm ĐA/KL của từng người học (sau khi kết thúc buổi bảo vệ).
  - a. Điểm của giảng viên hướng dẫn.
  - b. Điểm của ủy viên phản biện.
  - c. Điểm trung bình của các ủy viên hội đồng.
  - d. Điểm ĐA/KL (trung bình cộng các điểm của: giảng viên hướng dẫn, giảng viên phản biện và điểm trung bình của thành viên hội đồng đánh giá).

**Ghi chú:**

- Thời gian bảo vệ cho 1 sinh viên từ 45 đến 60 phút.
- Điểm đồ án, khoá luận tốt nghiệp được đánh giá theo thang điểm 10 sau đó chuyển thành điểm chữ và thang điểm 4 theo quy định.

BỘ CÔNG THƯƠNG  
TRƯỜNG ĐẠI HỌC SAO ĐỎ

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM  
Độc lập – Tự do – Hạnh phúc

Hải Dương, ngày tháng năm 20

DANH SÁCH SINH VIÊN BẢO VỆ ĐỒ ÁN/KHOÁ LUẬN TỐT NGHIỆP

NGÀNH:CÔNG NGHỆ THÔNG TIN

HỘI ĐỒNG:.....

TT	Mã sinh viên	Họ và tên sinh viên	Lớp, khoá	Tên đề tài	GV hướng dẫn	UV phản biện	Ghi chú
1							
2							
3							
4							
5							
...							

TRƯỜNG KHOA

(Ký, ghi rõ họ tên)

NGƯỜI LẬP

(Ký, ghi rõ họ tên)

**PHIẾU ĐÁNH GIÁ ĐỒ ÁN/KHOÁ LUẬN TỐT NGHIỆP**  
**ĐẠI HỌC CHÍNH QUY KHÓA 10**

Họ tên sinh viên:.....

Lớp, khoá:..... Ngành: .....

Bảo vệ đồ án/khoa luận, ngày      tháng      năm

Các chỉ tiêu đánh giá	Điểm chuẩn	Điểm đánh giá	Nhận xét
<b>1. Nội dung trình bày (đầy đủ, xúc tích...)</b> ..... .....	7.0đ		
<b>2. Trả lời câu hỏi của uỷ viên phản biện</b> Câu 1: ..... .....	1.5đ	ĐỎ	
Câu 2: ..... .....			
Câu ....: .....			
<b>3. Trả lời các câu hỏi của uỷ viên hội đồng</b> Câu 1: ..... .....	1.5đ		
Câu 2: ..... .....			
Câu....			
<b>Tổng</b>	<b>10đ</b>		

**ỦY VIÊN HỘI ĐỒNG**

(Ký, ghi rõ họ tên)

**BẢNG TỔNG HỢP**  
**ĐIỂM ĐỒ ÁN/KHOÁ LUẬN TỐT NGHIỆP**  
HỘI ĐỒNG: .....  
NGÀNH: .....

TT	Họ và tên sinh viên	Lớp	Điểm thành phần			Điểm công nhận*	
			Điểm của GVHD	Điểm của GVPB	Điểm TB của UVHĐ	Điểm số	Điểm chữ
1							
2							
3							
4							
5							
6							
7							
8							
...							

CHỦ TỊCH HỘI ĐỒNG  
(Ký, ghi rõ họ tên)

Hải Dương, ngày tháng năm  
**THU KÝ**  
(Ký, ghi rõ họ tên)

\* Điểm đồ án, khoá luận tốt nghiệp được đánh giá theo thang điểm 10 sau đó chuyển thành điểm chữ và thang điểm 4 theo quy định.

**BIÊN BẢN TỔNG HỢP  
KẾT QUẢ ĐÁNH GIÁ ĐỒ ÁN/KHOÁ LUẬN TỐT NGHIỆP**

Họ và tên sinh viên: .....

Tên đề tài: .....

Lớp, khoá: ..... Ngành: .....

Bảo vệ đồ án/khoa luận tốt nghiệp, ngày      tháng      năm

**I. TRẢ LỜI CÁC CÂU HỎI CỦA ỦY VIÊN PHẢN BIỆN:**

**1. Nội dung câu hỏi:**

Câu 1: .....

Câu 2: .....

Câu ....: .....

**2. Nhận xét của giảng viên phản biện:**

.....

**II. TRẢ LỜI CÁC CÂU HỎI KHÁC:**

**1. Nội dung câu hỏi:**

Câu 1: .....

Câu 2: .....

Câu 3: .....

Câu ....: .....

.....

**2. Nhận xét:**

.....  
.....  
.....  
.....

**III. NHẬN XÉT VÀ KẾT LUẬN CỦA CHỦ TỊCH HỘI ĐỒNG**

**1. Nhận xét:**

.....  
.....  
.....

**2. Yêu cầu sinh viên sửa đồ án/khoa luận tốt nghiệp (nếu có)**

.....  
.....

**3. Đánh giá điểm đồ án/khoa luận tốt nghiệp:**

Điểm thành phần			Điểm công nhận*	
Điểm của GVHD	Điểm của GVPB	Điểm TB của UVHĐ	Điểm số	Điểm chữ

Biên bản được lập vào hồi ..... giờ ..... phút ngày ...../...../...../.

**CHỦ TỊCH HỘI ĐỒNG**  
(Ký, ghi rõ họ tên)

**THƯ KÝ**  
(Ký, ghi rõ họ tên)

\* Điểm đồ án, khoa luận tốt nghiệp được đánh giá theo thang điểm 10 sau đó chuyển thành điểm chữ và thang điểm 4 theo quy định.

Hải Dương, ngày tháng năm 20

**BẢN XÁC NHẬN CHỈNH SỬA ĐỒ ÁN/KHOÁ LUẬN TỐT NGHIỆP  
ĐẠI HỌC CHÍNH QUY**

Họ và tên sinh viên: .....

Đề tài:.....

Ngành:..... Mã số: .....

Giảng viên hướng dẫn và Hội đồng chấm đồ án/khoa luận tốt nghiệp xác nhận sinh viên..... đã sửa chữa, bổ sung theo Biên bản tổng hợp kết quả đánh giá đồ án/khoa luận tốt nghiệp ngày.....tháng.....năm.....với các nội dung sau:

1.....  
.....

2.....  
.....

3.....  
.....

**GIẢNG VIÊN HƯỚNG DẪN**

(Ký, ghi rõ họ tên)

**Sinh viên thực hiện**

(Ký, ghi rõ họ tên)

**CHỦ TỊCH HỘI ĐỒNG**

(Ký, ghi rõ họ tên)

# MỤC LỤC

LỜI NÓI ĐẦU .....	1
TỔNG QUAN VỀ ĐỀ TÀI NGHIÊN CỨU .....	2
CHƯƠNG 1: TỔNG QUAN VỀ MẠNG NỘI BỘ .....	3
1.1. Giới thiệu về mạng nội bộ .....	3
1.1.1. Mạng nội bộ là gì .....	3
1.1.2. Cách sử dụng trong hệ thống mạng nội bộ.....	4
1.1.3. Lợi ích của hệ thống mạng nội bộ .....	4
1.2. Công nghệ truyền dẫn mạng dây Ethernet .....	6
1.2.1. Khái niệm về Ethernet.....	6
1.2.2. Ethernet là một công nghệ mạng thiết bị và rộng rãi.....	7
1.2.3. Lịch sử phát triển của Ethernet.....	7
1.2.4. Các chuẩn và tốc độ của Ethernet.....	8
1.2.5.Các thành phần của Ethernet .....	11
1.2.6. Hoạt động của Ethernet .....	11
1.2.7. Sự khác nhau giữa Internet và Ethernet .....	12
1.3. Kỹ thuật chuyển mạch trong mạng nội bộ .....	13
1.3.1. Khái niệm chuyển mạch.....	13
1.3.2. Các công nghệ chuyển mạch .....	14
1.4. Kết luận .....	20
CHƯƠNG 2: TẤN CÔNG MẠNG NỘI BỘ VÀ GIẢI PHÁP PHÒNG CHỐNG TẤN CÔNG .....	22
2.1. Tổng quan về an toàn bảo mật thông tin .....	22
2.2. Một số kỹ thuật tấn công mạng nội bộ.....	24
2.2.1.Tấn công sử dụng phần mềm độc hại (Malware) .....	24
2.2.2. Tấn công giả mạo (Phishing).....	24
2.2.3. Tấn công từ chối dịch vụ(DoS và DDoS) .....	25
2.2.4. Tấn công cơ sở dữ liệu (SQL injection).....	30
2.2.5. Khai thác lỗ hổng Zero-day (Zero day attack) .....	31
2.2.6. Tấn công Man in the middle(MitM) .....	31
2.2.7. Các loại khác.....	34
2.3. Một số giải pháp phòng chống tấn công mạng nội bộ .....	34

2.4. Kết luận Chương 2 .....	35
<b>CHƯƠNG 3: THỰC NGHIỆM VÀ ĐÁNH GIÁ .....</b>	<b>36</b>
3.1. Xây dựng mô hình thử nghiệm.....	36
3.2. Kịch bản thử nghiệm.....	38
3.3. Tiến hành tấn công và phòng thủ trên mô hình thử nghiệm .....	38
3.4. Đánh giá công cụ và phát triển .....	61
3.5. Kết luận .....	66
<b>KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN .....</b>	<b>67</b>
<b>TÀI LIỆU THAM KHẢO .....</b>	<b>68</b>

Đại học Sao Đỏ

## **DANH MỤC ẢNH**

Hình 1.1. Tổng quan về mạng nội bộ.....	3
Hình 1.2. Cách sử dụng trong hệ thống mạng nội bộ .....	4
Hình 1.3. 10BASE5 transceivers, cables, and tapping tool.....	8
Hình 1.4. ETHERNET TRUNK CABLE 802.3 STYLE 1478 12 FT 10Base5 .....	9
Hình 1.5. 10Base2 cable.....	9
Hình 1.6. Ethernet over twisted-pair cable(10BaseT).....	9
Hình 1.7. Cáp 1000Base-Lx .....	10
Hình 1.8. Các thành phần của Ethernet.....	11
Hình 1.9. Khái niệm chuyển mạch.....	14
Hình 1.10. Chuyển mạch thông điệp.....	16
Hình 1.11. Chuyển mạch gói .....	17
Hình 1.12. Chuyển mạch ảo .....	18
Hình 2.1. Tấn công từ chối dịch vụ(DoS và DDoS .....	25
Hình 2.2. Tấn công Teardrop.....	27
Hình 2.3. Tấn công Smurf .....	27
Hình 2.4. Tấn công Ping of Death .....	29
Hình 2.5. Tấn công Botnet.....	30
Hình 2.6. Tấn công SQL injection .....	31
Hình 2.7. Khai thác lỗ hổng Zero-day (Zero Day Exploits) .....	31
Hình 2.8. Tấn công Man-in-the-Middle (MitM) .....	33
Hình 2.9. Tấn công Replay .....	33
Hình 3.1. Cài đặt Eve-ng trên VMware .....	36
Hình 3.2. Đăng nhập tài khoản sử dụng Eve-ng.....	36
Hình 3.3. Import sơ đồ lab đã tạo .....	37
Hình 3.4. Mô hình thử nghiệm.....	37
Hình 3.5. Minh họa bảng MAC .....	39
Hình 3.6. Sơ đồ tổng quan kịch bản MAC Overflow trên Eve-ng .....	40
Hình 3.7. Mở máy ảo Kali linux .....	40
Hình 3.8. Hiển thị bảng MAC thiết bị Switch3 ban đầu .....	41
Hình 3.9. Mở terminal máy kali linux.....	42
Hình 3.10. Cài đặt gói dnsiff .....	42

Hình 3.11. Sử dụng lệnh DoS thiết bị Switch3.....	43
Hình 3.12. Máy attacker gửi liên tục các địa chỉ MAC giả mạo .....	43
Hình 3.13. Hiển thị bảng MAC trên Switch3 sau khi bị tấn công Ddos.....	44
Hình 3.14. Clear bảng MAC trên Switch3 .....	44
Hình 3.15. Cấu hình port security trên SW14 .....	45
Hình 3.16. Từ máy attacker tấn công lại lần 2.....	45
Hình 3.17. Cổng Ether0/3 của Switch3 tự động ngắt khi thấy dấu hiệu attack .....	46
Hình 3.18. Kiểm tra lại bảng MAC của thiết bị Switch3 thấy bình thường .....	46
Hình 3.19. Sơ đồ bài lab tấn công ARP-Poisoning.....	48
Hình 3.20. Mở công cụ Ettercap trên máy Kali linux.....	48
Hình 3.21. Thực hiện Scan hosts .....	49
Hình 3.22. Kiểm tra thông tin các máy đã dò được .....	49
Hình 3.23. Kiểm tra thông tin các máy đã dò được .....	50
Hình 3.24. Trên máy attacker add 2 mục tiêu PC2 và Local Server3 .....	50
Hình 3.25. Thực hiện phương thức tấn công ARP Poisoning .....	51
Hình 3.26. Kiểm tra bảng MAC của thiết bị Local-Server .....	51
Hình 3.27. Kiểm tra bảng MAC của thiết bị PC7 .....	52
Hình 3.28. Thực hiện từ máy PC-7 telnet đến máy Local-Server .....	52
Hình 3.29. Máy attacker sử dụng công cụ Wireshark để nghe lén.....	53
Hình 3.30. Attacker dò được tài khoản telnet.....	53
Hình 3.31. Attacker đột nhập vào Local Server .....	54
Hình 3.32. Cấu hình ip snooping trên Switch3 để phòng vệ.....	55
Hình 3.33. Tấn công lại lần nữa từ máy Attacker thấy Switch3 hiện cảnh báo.....	55
Hình 3.34. Kiểm tra lại bảng Mac của thiết bị Local-Server .....	56
Hình 3.35. Kiểm tra lại bảng Mac của thiết bị Pc7.....	56
Hình 3.36. Sơ đồ mô phỏng tấn công Scanning .....	57
Hình 3.37. Địa chỉ IP của máy Kali linuxs.....	58
Hình 3.38. Thực hiện scan Firewall PFsense .....	58
Hình 3.39. Bật dịch vụ Snort trên PfSense .....	59
Hình 3.40. Thực hiện Scan hệ thống trên máy Kali linux.....	59
Hình 3.41. Cảnh báo về hoạt động bất thường của Snort .....	60
Hình 3.42. Thông tin về địa chỉ IP đã bị block bởi Snort .....	60
Hình 3.43. Đánh giá công cụ EVE-ng.....	61

Hình 3.44. Đánh giá hệ điều hành Kali linux .....	63
Hình 3.45. Đánh giá Firewall Pfsense.....	64

Đại học Sao Đỏ

## **DANH MỤC TỪ VIẾT TẮT**

<b>STT</b>	<b>Ký hiệu chữ viết tắt</b>	<b>Chữ viết đầy đủ</b>
1	LAN	Local Area Network
2	Mbps	Megabit per second
3	MAC	Medium Access Control
4	MITM	Man in the middle
5	DDoS	Distributed Denial of Service
6	SQL	Structured Query Language
7	ARP	Address Resolution Protocol
8	IP	Internet Protocol
9	WAN	Wide Area Network
10	CSMA	Carrier Sense Multiple Access

## LỜI NÓI ĐẦU

Trong những năm gần đây, ngành Công nghệ thông tin (CNTT) đã phát triển mạnh mẽ, đồng nghĩa với việc đem lại nhiều ưu điểm và tiện ích tích cực trong cuộc sống hàng ngày. Mọi công việc trở nên nhẹ nhàng, nhanh chóng và tiện lợi hơn nhờ số hóa. Ứng dụng của CNTT được áp dụng vào hầu hết các công việc hàng ngày, từ đi chợ, mua sắm hàng hóa, học tập, làm việc, các dịch vụ công. Rất nhiều doanh nghiệp, cơ quan nhà nước đã và đang tiến hành chuyển đổi số, nhằm đem các ứng dụng CNTT vào phục vụ công việc một cách triệt để. Tuy nhiên, cùng với những lợi ích đó, sự phát triển của CNTT cũng mang đến một loại hình tội phạm mới – tội phạm sử dụng công nghệ cao. Ví dụ điển hình là những vụ tấn công vào các hệ thống máy chủ, cài cắm mã độc, virus, mã hóa các thông tin nhạy cảm để đòi tiền chuộc, hoặc nguy hiểm hơn là xâm phạm an ninh quốc phòng. Các hình thức tấn công mạng ngày càng tinh vi hơn, và không chỉ trên môi trường Internet, những hệ thống mạng nội bộ, mạng diện rộng dùng đường truyền riêng cũng có nguy cơ bị tấn công rất cao.

Đối với các công ty lớn, việc bị tấn công mạng nội bộ có thể gây thiệt hại lớn về mặt tiền bạc, còn đối với các cơ quan nhà nước, mức độ thiệt hại có thể lớn hơn rất nhiều, thậm chí có thể ảnh hưởng tới nền an ninh Quốc gia. Chính vì thế, việc nghiên cứu về các phương pháp tấn công mạng, cũng như các biện pháp để phòng thủ là vô cùng cần thiết và là nhu cầu cấp bách hiện nay. Từ những lý do như vậy, em lựa chọn đề tài: “**Nghiên cứu xây dựng hệ thống cảnh báo tấn công mạng**”.

## **TỔNG QUAN VỀ ĐỀ TÀI NGHIÊN CỨU**

Hiện nay các phương pháp tấn công mạng và cách ngăn chặn được phổ biến khá nhiều trên Internet, một người có chút ít kiến thức về CNTT cũng có thể tự học cách tấn công mạng trên YouTube. Tuy nhiên, hầu hết các phương pháp này đều áp dụng trên nền tảng Internet, và đối tượng chủ yếu là người dùng cuối, với các mục tiêu như cài mã quảng cáo, điều hướng người dùng đến trang web giả mạo, virus mã hóa đòi tiền chuộc, lấy thông tin cá nhân, thẻ tín dụng, tài khoản ngân hàng. Còn đối với các mạng nội bộ, không có kết nối Internet, hoặc kết nối một phần với Internet thì các phương pháp tấn công và phòng thủ lại có sự khác biệt. Khác biệt từ các phương pháp tấn công, mục tiêu tấn công và mục đích tấn công.

Đối với các cơ quan, doanh nghiệp sử dụng mạng nội bộ thường thiếu sự phòng bị và đầu tư liên quan đến việc chống tấn công mạng. Lý do chính là chủ quan về việc không kết nối Internet thì không thể tấn công được. Quan niệm trên là không chính xác, các phương pháp tấn công mạng nội bộ vẫn có thể thực hiện được dù không có kết nối tới Internet, hoặc thông qua các vùng trung gian giữa mạng nội bộ và Internet, hoặc thông qua các thiết bị ngoại vi, như USB, đĩa CD,... Mặt khác, đa phần các vụ tấn công mạng đều xảy ra rồi thì phía nạn nhân mới biết, nên thường rơi vào tình trạng bị động, lo khắc phục sự cố. Chính vì thế cần có những giải pháp để có thể chủ động chống tấn công, phát hiện trong quá trình tấn công, tránh việc luôn phải đi sau để dọn dẹp hậu quả.

Đề tài nghiên cứu các phương pháp tấn công mạng nội bộ và phương pháp phòng chống sẽ tập trung vào phân tích khái quát về mạng nội bộ, phân tích các phương pháp tấn công qua mạng LAN đồng thời chỉ ra các điểm mạnh, điểm yếu của phương pháp đó và cách để phòng thủ hiệu quả nhất. Cùng với đó là nghiên cứu một số phương pháp chống tấn công chủ động.

# CHƯƠNG 1: TỔNG QUAN VỀ MẠNG NỘI BỘ

## 1.1 Giới thiệu về mạng nội bộ

### 1.1.1 Mạng nội bộ là gì

Một mạng nội bộ là một mạng riêng chỉ có thể cho nhân viên của một tổ chức. Thông thường, một loạt thông tin và dịch vụ có sẵn trên mạng nội bộ của một tổ chức không được công khai cho tất cả mọi người, không giống như Internet . Mạng nội bộ của công ty có thể tự mình trở thành trung tâm quan trọng cho giao tiếp và hợp tác nội bộ, tạo ra một điểm truy cập thông tin làm việc duy nhất để tiếp cận tài nguyên cả nội và ngoại vi. Hệ thống mạng nội bộ này được xây dựng với sự kết hợp của công nghệ LAN và WAN để đảm bảo hiệu suất và tiện ích đa dạng. Nhiều mạng nội bộ hiện đại có công cụ tìm kiếm, hồ sơ người dùng, danh bạ, blog , ứng dụng di động có thông báo và lập kế hoạch cho các sự kiện trong cơ sở hạ tầng.



Hình 1.1 Tổng quan về mạng nội bộ

Không phải tất cả các nhân viên đều được ủy quyền truy cập vào mạng nội bộ của công ty; tuy nhiên, hầu hết họ đều có quyền truy cập. Có một số nhân viên, dựa trên loại công việc hoặc phân loại, không có nhu cầu truy cập thông tin trên mạng nội bộ. Thông tin này thường liên quan đến chất lượng đào tạo, thông tin sản phẩm, bài viết và thông tin khác liên quan đến hoạt động của công ty.

Mạng nội bộ từ các tổ chức khác nhau không được kết nối với nhau. Và họ không chia sẻ thông tin với nhau. Mạng nội bộ của một tổ chức được phát triển bởi chính nhân viên của doanh nghiệp và điều hành nội bộ.

### 1.1.2 Cách sử dụng trong hệ thống mạng nội bộ

Hiện nay, mạng nội bộ đang phát huy vai trò quan trọng trong việc cung cấp các công cụ và tính năng đa dạng như cộng tác nhóm, hội nghị trực tuyến, thư mục công ty, cùng các công cụ quản lý sản phẩm và dự án. Nó không chỉ đơn thuần là một nền tảng hỗ trợ công việc mà còn đóng vai trò quan trọng trong quá trình thay đổi văn hóa trong doanh nghiệp.



Hình 1.2 Cách sử dụng trong hệ thống mạng nội bộ

Trong mạng nội bộ, lưu lượng truy cập trang web thường có sự tương đồng với lưu lượng trang web công cộng, và việc hiểu rõ hơn về hoạt động này có thể được đạt được thông qua việc sử dụng phần mềm theo dõi web. Khảo sát người dùng cũng đóng góp vào việc cải thiện hiệu suất của trang web trong mạng nội bộ.

Các công ty lớn thường cho phép người dùng trong mạng nội bộ truy cập internet công cộng thông qua các server proxy, có khả năng sàng lọc thông điệp đến và đi để bảo vệ an toàn mạng. Khi một phần của mạng nội bộ trở thành một phần của internet thông qua việc truy cập cho phép bên ngoài công ty, các biện pháp bảo mật như mã hóa đặc biệt được sử dụng để giữ kết nối an toàn.

Việc phát triển trang web local thường đòi hỏi sự hợp tác giữa các đội phát triển, biên tập, và chuyên gia công nghệ trong mạng nội bộ. Quản lý của mạng local

thường nằm trong tay các bộ phận truyền thông, CIO hoặc nhân sự của tổ chức, hoặc có thể là sự kết hợp của chúng.

Với sự đa dạng và phạm vi lớn của nội dung và giao diện hệ thống, mạng nội bộ của nhiều tổ chức thường phức tạp hơn nhiều so với trang web công cộng của họ. Sự phát triển và sử dụng mạng nội bộ đang ngày càng phát triển nhanh chóng, và theo báo cáo của Tập đoàn Nielsen Norman năm 2008, số trang trung bình trên mạng nội bộ tăng lên từ 210.000 trong giai đoạn từ năm 2000 đến 2002 lên trung bình 6 triệu trang vào năm 2006.

### 1.1.3 Lợi ích của hệ thống mạng nội bộ

- Năng suất lao động: Mạng nội bộ giúp người dùng nhanh chóng định vị và truy cập thông tin liên quan đến vai trò và trách nhiệm của họ. Thông qua giao diện trình duyệt web, người dùng có thể truy cập dữ liệu từ bất kỳ cơ sở dữ liệu nào mà tổ chức cung cấp, đồng thời tuân theo các quy định bảo mật. Điều này giúp tăng cường khả năng thực hiện công việc của nhân viên, đảm bảo thông tin chính xác, và cải thiện dịch vụ cho người sử dụng.
- Linh hoạt về thời gian: Mạng nội bộ cho phép tổ chức phân phối thông tin linh hoạt đến nhân viên khi cần thiết. Ngược lại, nhân viên có thể dễ dàng liên kết với thông tin liên quan mà không cần phải tìm kiếm qua email hoặc nguồn thông tin không tự tổ chức.
- Giao tiếp dễ dàng: Mạng nội bộ đóng vai trò quan trọng trong việc tạo ra một công cụ liên lạc và giao tiếp trong tổ chức. Thông tin có thể dễ dàng truyền đạt, sáng kiến có thể được thúc đẩy, và mục tiêu của sáng kiến được rõ ràng xác định, giúp tăng cường sự hiểu biết của nhân viên và giảm khó khăn trong giao tiếp.
- Xây dựng website: Mạng nội bộ cho phép duy trì và truy cập thông tin phức tạp của doanh nghiệp thông qua các công nghệ thiết kế website. Điều này bao gồm hướng dẫn nhân viên, quyền lợi, chính sách công ty, và tài liệu đào tạo, giúp nhân viên có thể truy cập thông tin mới nhất một cách thuận tiện.
- Hoạt động kinh doanh và quản lý: Mạng nội bộ được sử dụng như một nền tảng để phát triển và triển khai các ứng dụng hỗ trợ quyết định và hoạt động kinh doanh toàn cầu.

- Quy trình làm việc: Mạng nội bộ giúp giảm độ trễ trong quy trình làm việc, chẳng hạn như tự động lên lịch họp hoặc lên kế hoạch nghỉ phép, tăng cường hiệu suất và tự động hóa các hoạt động quan trọng.
- Hiệu quả về chi phí: Người dùng có thể xem thông tin và dữ liệu qua trình duyệt web, giảm chi phí in ấn và bảo trì tài liệu in ấn.
- Tăng cường về hợp tác: Mạng nội bộ cho phép sự tham gia và làm việc theo nhóm, cũng như giao tiếp thời gian thực thông qua các công cụ tích hợp của bên thứ ba.
- Đa nền tảng: Mạng nội bộ hỗ trợ các trình duyệt web tuân thủ tiêu chuẩn trên nhiều hệ điều hành.
- Được xây dựng cho đối tượng: Mạng nội bộ có thể cá nhân hóa dựa trên vai trò của người dùng, đảm bảo rằng họ chỉ nhận được thông tin cần thiết cho công việc của mình.
- Quảng bá văn hóa công ty: Mạng nội bộ giúp đồng nhất thông tin và quảng bá văn hóa công ty trong toàn bộ tổ chức.
- Cập nhật ngay lập tức: Mạng nội bộ cho phép cập nhật nhanh chóng về thông tin mới nhất, đặc biệt quan trọng khi giao tiếp với nhân viên.
- Sự tham gia của nhân viên: Cung cấp các công cụ như diễn đàn hoặc khảo sát để thúc đẩy sự tham gia và đóng góp ý kiến từ nhân viên.
- **Công nghệ truyền dẫn mạng dây Ethernet**

### 1.2.1 Khái niệm về Ethernet

Ethernet là một họ công nghệ mạng đa dạng dựa trên khung dữ liệu, được thiết kế đặc biệt cho mạng LAN. Tên gọi "Ethernet" xuất phát từ lĩnh vực vật lý học và bao gồm nhiều chuẩn nối dây và phát tín hiệu tại tầng vật lý. Công nghệ này đặc trưng cho việc truy cập mạng tại tầng MAC, quản lý truy nhập môi trường truyền dẫn ở tầng liên kết dữ liệu và có một định dạng chung cho địa chỉ.

Ethernet là một công nghệ mạng cục bộ (LAN) được thiết kế để chuyển đổi thông tin dữ liệu giữa các máy tính với tốc độ từ 10 đến 100 triệu bit mỗi giây (Mbps). Hiện nay, công nghệ Ethernet thường sử dụng cáp đôi xoắn 10-Mbps.

Công nghệ Ethernet hiện đại thường sử dụng các phương tiện truyền thông như cáp đồng trục cỡ lớn, cáp đôi, và cáp quang để đạt tốc độ truyền dẫn 10-Mbps. Với sự

phát triển, tốc độ chuẩn cho hệ thống Ethernet hiện đại đã tăng lên đáng kể, thường là 100-Mbps. Điều này làm cho Ethernet trở thành một trong những công nghệ mạng phổ biến và ổn định nhất trong việc kết nối các thiết bị trên cùng một mạng cục bộ.

### **1.2.2 Ethernet là một công nghệ mạng thiết bị và rộng rãi**

Hiện nay, mặc dù có nhiều công nghệ LAN khác nhau, nhưng Ethernet vẫn là công nghệ được sử dụng rộng rãi nhất. Dựa vào ước tính năm 1993, có hơn 45 triệu nút Ethernet đã được triển khai trên toàn cầu.

Từ khi Ethernet ra đời, các đặc tính kỹ thuật và quy trình xây dựng mạng Ethernet đã trở nên dễ dàng hơn đối với mọi người. Những tính năng này, cùng với tính dễ sử dụng, đã tạo ra một thị trường Ethernet rộng lớn và là nguyên nhân chính đằng sau sự ứng dụng rộng rãi của Ethernet trong ngành công nghiệp máy tính.

Hiện nay, các nhà sản xuất máy tính trang bị sản phẩm của họ với thiết bị 10-Mbps Ethernet, làm cho các thiết bị của họ có khả năng kết nối vào mạng Ethernet. Với sự phổ biến của chuẩn Ethernet 100-Mbps, máy tính được trang bị thiết bị Ethernet hoạt động ở cả hai tốc độ 10-Mbps và 100-Mbps. Điều này đồng nghĩa rằng ngày nay, quản trị viên mạng Ethernet cần có khả năng kết hợp một lượng lớn máy tính từ nhiều nhà sản xuất khác nhau thông qua công nghệ mạng qua các thiết bị trung gian. Do đó, nhiều mạng LAN ngày nay hỗ trợ các máy tính sản xuất bởi nhiều hãng khác nhau.

### **1.2.3 Lịch sử phát triển của Ethernet**

Ethernet được phát minh tại Trung tâm Nghiên cứu Xerox Palo Alto vào những năm 1971 bởi tiến sĩ Robert M. Metcalfe, với mục đích phục vụ nghiên cứu trong hệ thống quản lý công ty trong tương lai. Trạm Ethernet đầu tiên chạy với tốc độ xấp xỉ 3-Mbps. Công nghệ này chính thức được công bố vào năm 1980 bởi liên minh DEC-Intel-Xerox (DIX), chuyển "tiền Ethernet" trở thành một hệ thống mở Ethernet với chất lượng và tốc độ 10 Mbps.

Công nghệ Ethernet được công nhận là tiêu chuẩn của Ban tiêu chuẩn LAN nằm trong Viện Kỹ thuật Điện và Điện tử Thế giới (IEEE 802). Chuẩn IEEE đã được thành lập lần đầu tiên vào năm 1985, mang tiêu đề "IEEE 802.3 khuyến nghị về lớp

vật lý và phương thức truy nhập đa truy nhập sóng mang phát hiện và chạm." Chuẩn IEEE đã được thừa nhận bởi Tổ chức Tiêu chuẩn Thế giới (ISO).

Chuẩn IEEE cung cấp Ethernet kiểu hệ thống dựa trên công nghệ DIX Ethernet. Tất cả các hệ thống Ethernet từ năm 1985 đều được xây dựng dựa trên tiêu chuẩn IEEE 802.3, chính xác hơn là công nghệ "IEEE 802.3 CSMA/CD". Mặc dù có các nâng cấp từng bước, như công nghệ mới và khuyến nghị mạng Ethernet nhanh 100 Mbps từ năm 1985, nhưng hầu hết các mạng Ethernet ngày nay vẫn phát triển từ mạng Ethernet nguyên thủy.

#### 1.2.4. Các chuẩn và tốc độ của Ethernet

##### Ethernet 10Mb/s

Chuẩn Ethernet 10Base5 là một trong những chuẩn Ethernet đầu tiên và sử dụng cáp đồng trực dày. Dạng "10Base5" mô tả các đặc điểm chính của chuẩn này:

- 10: Đây là tốc độ truyền dẫn dữ liệu, ở đây là 10 Mbps (Megabit mỗi giây).
- Base: Chữ "Base" đại diện cho "Baseband," một loại truyền dẫn dữ liệu trong đó toàn bộ băng thông của đường truyền được sử dụng bởi một tín hiệu duy nhất.
- 5: Số này thường chỉ ra sự sử dụng của cáp đồng trực dày. Cụ thể, đối với 10Base5, nó có nghĩa là chiều dài tối đa của mỗi đoạn cáp là 500 mét.



Hình 1.3 10BASE5 transceivers, cables, and tapping tool



*Hình 1.4 ETHERNET TRUNK CABLE 802.3 STYLE 1478 12 FT 10Base5*

-10Base2: Có tên khác là “thin Ethernet”, dựa trên hệ thống cáp đồng trục mỏng với tốc độ 10Mb/s, chiều dài cáp tối đa của phân đoạn là 185m (IEEE làm tròn thành 200m).



*Hình 1.5 10Base2 cable*

-10BaseT: chữ T viết tắt của twisted(cáp xoắn cặp), hoạt động tốc độ 10Mb/s dựa trên hệ thống cáp xoắn cặp Cat 3 trở lên.



*Hình 1.6 Ethernet over twisted-pair cable(10BaseT)*

-10BaseF: F viết tắt của Fiber optic (sợi quang), đây là chuẩn ethernet dùng cho sợi quang hoạt động ở tốc độ 10Mb/s, ra đời năm 1993.

### Ethernet 100Mb/s (có tên là Fast Ethernet)

Chuẩn Ethernet 100BaseT là một trong những chuẩn Ethernet phổ biến, hoạt động ở tốc độ 100 Mbps. Đây là một sự tiến bộ so với chuẩn Ethernet 10 Mbps trước đó. Đặc điểm chính của chuẩn này bao gồm khả năng hoạt động trên cả cáp xoắn và cáp quang.

- 100BaseX: Chuẩn này thể hiện sự cải tiến trong việc mã hóa đường truyền, sử dụng phương pháp mã hóa 4B/5B của chuẩn FDDI (Fiber Distributed Data Interface). Chữ "X" thường được sử dụng để chỉ đặc tính mã hóa của hệ thống.
- 100BaseFX: Sử dụng cáp sợi quang đa mode để truyền dẫn dữ liệu ở tốc độ 100 Mbps.
- 100BaseTX: Sử dụng cáp xoắn cặp (twisted pair) để truyền dẫn dữ liệu ở tốc độ 100 Mbps. Chuẩn này thường được sử dụng rộng rãi trong môi trường mạng LAN với cấu trúc vật lý dạng star.

#### 1.4.3. Hệ thống GigaEthernet

- 1000BaseX gồm 3 loại:
  - +1000Base-SX: sử dụng sợi quang với sóng ngắn.
  - +1000Base-LX: sử dụng sợi quang với sóng dài.
  - +1000Base-CX: sử dụng cáp đồng.



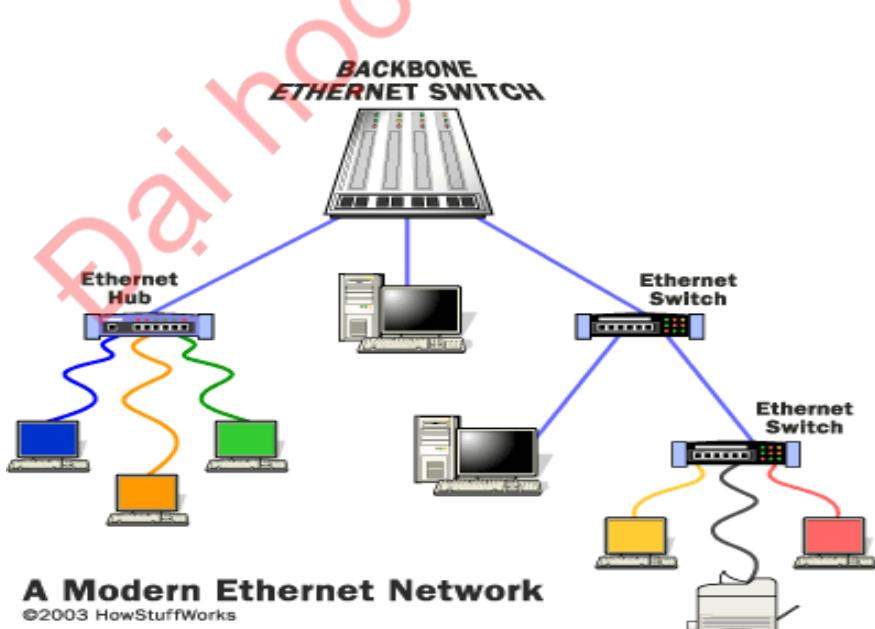
Hình 1.7 Cáp 1000Base-Lx

-1000BaseT: hoạt động ở tốc độ Gigabit, băng tần cơ sở trên cáp xoắn cặp Cat 5 trở lên và có sử dụng kiểu mã hóa đường truyền riêng.

### 1.2.5.Các thành phần của Ethernet

Hệ thống Ethernet bao gồm ba thành phần cơ bản quan trọng:

- Trung tâm truyền tín hiệu Ethernet giữa các máy tính: Trong một mạng Ethernet, có một hệ thống truyền tín hiệu tại trung tâm, thường được biết đến là "hub" hoặc "switch". Hub thường được sử dụng trong các mạng cổ điển, trong khi switch thường được ưa chuộng hơn do khả năng chuyển mạch thông minh hơn. Cả hai đều hoạt động như trung tâm kết nối giữa các máy tính trong mạng.
- Nhóm thiết bị trung gian: Nhóm thiết bị trung gian này đóng vai trò là giao diện Ethernet, cho phép nhiều máy tính kết nối đến cùng một kênh. Trung tâm này có thể là hub, switch, hoặc các thiết bị mạng tương tự.
- Các khung Ethernet: Các khung Ethernet là đơn vị cơ bản để truyền dữ liệu trên mạng. Chúng được đóng gói dữ liệu và có trách nhiệm vận chuyển dữ liệu từ một máy tính đến máy tính khác trong mạng. Các khung này đóng vai trò quan trọng trong việc đảm bảo việc truyền dữ liệu hiệu quả và đúng đắn.



Hình 1.8 Các thành phần của Ethernet

### 1.2.6 Hoạt động của Ethernet

**Hoạt Động Tự Động Của Máy Trạm Ethernet:**

- Máy trạm Ethernet, hay còn được biết đến với tên gọi là máy Ethernet, hoạt động độc lập với các thiết bị khác trên mạng mà không có sự điều khiển từ một trạm trung tâm. Mỗi máy trạm kết nối với mạng Ethernet thông qua một đường truyền chung, thường được gọi là trung gian.
- Trước khi máy trạm gửi dữ liệu, quy trình đầu tiên là lắng nghe để kiểm tra xem đường truyền có đang sử dụng không (Carrier Sense). Nếu đường truyền rảnh, máy trạm sẽ bắt đầu quá trình truyền dữ liệu của mình. Quá trình này không ưu tiên bất kỳ máy trạm nào khác, tức là mọi máy trạm có cơ hội tham gia truyền dữ liệu là bằng nhau.
- Để điều này xảy ra, mỗi máy trạm được trang bị một nhóm điều khiển truy nhập, còn được gọi là Medium Access Control (MAC), để quyết định thời điểm thích hợp để tham gia truyền dữ liệu. Giao thức sử dụng trong quá trình này được gọi là Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

#### **Giao Thức CSMA/CD:**

- CSMA/CD là giao thức sử dụng trong mạng Ethernet để quản lý việc truyền dữ liệu trên một đường truyền chung. Khi máy trạm phát hiện xung đột trong quá trình truyền dữ liệu, nó sẽ ngừng và thử lại sau một khoảng thời gian ngẫu nhiên. Quy trình này giúp giảm khả năng xung đột xảy ra lại.
- Xung Đột và Truyền Dữ Liệu: Xung đột xảy ra khi hai hoặc nhiều máy trạm cố gắng truyền dữ liệu đồng thời trên cùng một đường truyền. Giao thức CSMA/CD phát hiện xung đột và sử dụng quy tắc tái truyền để giải quyết tình huống này. Quy tắc này đảm bảo rằng mỗi máy trạm có cơ hội để tham gia vào quá trình truyền dữ liệu sau một khoảng thời gian chờ ngẫu nhiên.
- Thông qua quá trình này, máy trạm Ethernet duy trì sự đồng đều trong việc truyền dữ liệu trên mạng, tạo ra một hệ thống linh hoạt và tự động.

#### **1.2.7 Sự khác nhau giữa Internet và Ethernet**

##### **Ethernet:**

Công nghệ mạng hiện đại được coi là tiêu chuẩn và phổ biến trong hầu hết các doanh nghiệp. Máy tính được liên kết với nhau thông qua một loại cáp đặc biệt và một thiết bị được gọi là "mecca", với việc sử dụng tốc độ cao trong kỹ thuật truyền dẫn cơ

bản (kênh đơn). Ethernet, một trong những công nghệ mạng phổ biến, cho phép truyền dữ liệu theo chuỗi với tốc độ 10 megabit mỗi giây, có thực tế từ 2 đến 3 megabit mỗi giây. Để đảm bảo mạng hoạt động hiệu quả, Ethernet sử dụng kỹ thuật thăm nhập nhiều môi trường với cảm nhận sóng mang dò xung đột (CSMA/CD). Điều này giúp tránh xung đột khi có hai thiết bị cố gắng truy cập mạng đồng thời.

## **Internet:**

Hệ thống bao gồm các máy tính trong mạng được kết nối với nhau trên phạm vi toàn cầu, tạo điều kiện thuận lợi cho nhiều dịch vụ truyền dữ liệu như đăng nhập từ xa, drum, và thư tín điện tử.

Internet được xem là phương tiện kết nối các mạng máy tính, mở rộng tầm nhìn hoạt động của từng hệ thống một cách rộng lớn. Đa dạng và phổ biến, Internet mở cửa cho mọi người tham gia. Nếu bạn là sinh viên của một khoa thuộc mạng, hãy thảo luận với người quản trị trung tâm máy tính để biết cách kết nối với Internet. Tất cả các tổ chức, từ lớn đến vừa, đều có cổng kết nối với Internet để hỗ trợ các hệ thống thư điện tử.

## **1.2 Kỹ thuật chuyển mạch trong mạng nội bộ**

### **1.3.1 Khái niệm chuyển mạch**

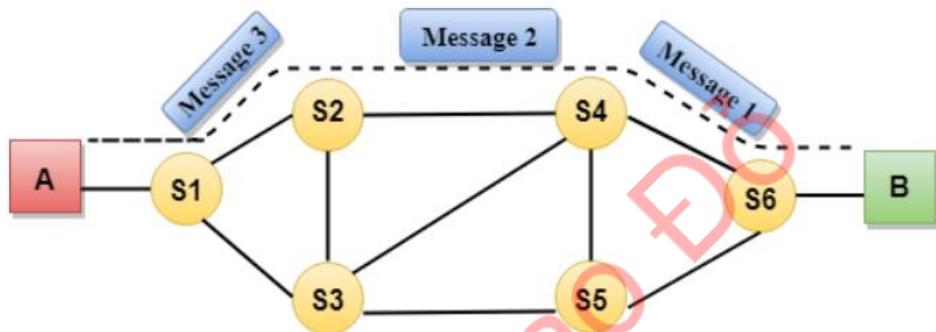
#### **Chuyển mạch:**

- ✓ Chuyển mạch kênh là một kỹ thuật chuyển mạch thiết lập một đường dẫn riêng giữa người gửi và người nhận.
- ✓ Trong Kỹ thuật chuyển mạch, một khi kết nối được thiết lập thì đường dẫn dành riêng sẽ vẫn tồn tại cho đến khi kết nối bị ngắt.
- ✓ Chuyển mạch kênh trong mạng hoạt động theo cách tương tự như hoạt động của điện thoại.
- ✓ Một đường dẫn end-to-end hoàn chỉnh phải tồn tại trước khi quá trình giao tiếp diễn ra.
- ✓ Đối với kỹ thuật chuyển mạch kênh, khi người dùng muốn gửi dữ liệu, thoại, video, tín hiệu yêu cầu được gửi đến máy thu thì máy thu sẽ gửi lại báo nhận để đảm bảo tính khả dụng của đường dẫn chuyên dụng. Sau khi nhận được xác nhận, đường dẫn dành riêng sẽ chuyển dữ liệu.

- ✓ Chuyển mạch kênh sử dụng trong mạng công cộng. Nó được sử dụng để truyền giọng nói.
- ✓ Dữ liệu cố định có thể được chuyển tại một thời điểm trong công nghệ chuyển mạch kênh.

**Giao tiếp thông qua chuyển mạch kênh có 3 pha:**

- ✓ Thành lập mạch
- ✓ Truyền dữ liệu
- ✓ Ngắt kết nối mạch



Hình 1.9 Khái niệm chuyển mạch

### 1.3.2 Các công nghệ chuyển mạch

**Chuyển mạch phân chia không gian:**

- ✓ Chuyển mạch phân chia không gian là một công nghệ chuyển mạch kênh trong đó một đường truyền duy nhất được thực hiện trong một bộ chuyển mạch bằng cách sử dụng một tập hợp các điểm chéo riêng biệt về mặt vật lý.
- ✓ Có thể đạt được Chuyển đổi Phân chia Không gian bằng cách sử dụng công tắc thanh ngang. Công tắc thanh ngang là một điểm giao nhau bằng kim loại hoặc cồng bán dẫn có thể được bật hoặc tắt bởi một bộ phận điều khiển.
- ✓ Công tắc Crossbar được thực hiện bằng cách sử dụng chất bán dẫn. Ví dụ, công tắc xà ngang Xilinx sử dụng FPGA.
- ✓ Chuyển mạch phân chia không gian có tốc độ cao, dung lượng lớn và chuyển mạch không chặn.

**Chuyển mạch phân chia không gian có thể được phân loại theo hai cách:**

- ✓ Chuyển mạch xà ngang

- ✓ Chuyển mạch đa tầng
- ✓ **Chuyển mạch Crossbar:**

Chuyển mạch Crossbar là công tắc có n đường vào và n đường ra. Công tắc xà ngang có n 2 điểm giao nhau được gọi là điểm giao nhau.

#### Nhược điểm của công tắc Crossbar:

Số lượng các điểm giao nhau tăng lên khi số lượng các trạm được tăng lên. Do đó, nó trở nên rất đắt đối với một công tắc lớn. Giải pháp cho điều này là sử dụng một công tắc nhiều tầng.

#### Chuyển mạch đa tầng:

Công tắc đa tầng được thực hiện bằng cách chia công tắc xà ngang thành các đơn vị nhỏ hơn và sau đó kết nối chúng với nhau.

Nó làm giảm số lượng các điểm giao nhau.

Nếu một đường dẫn không thành công, thì sẽ có sẵn đường dẫn khác.

#### Ưu điểm của chuyển mạch:

- ✓ Trong trường hợp của kỹ thuật Chuyển mạch, kênh liên lạc được dành riêng.
- ✓ Nó có băng thông cố định.

#### Nhược điểm của chuyển mạch:

- ✓ Khi đường dẫn dành riêng được thiết lập, độ trễ duy nhất xảy ra đối với tốc độ truyền dữ liệu.
- ✓ Mất một thời gian dài để thiết lập kết nối, khoảng 10 giây trong đó không có dữ liệu nào có thể được truyền.
- ✓ Nó đắt hơn các kỹ thuật chuyển mạch khác vì cần có một đường dẫn dành riêng cho mỗi kết nối.
- ✓ Nó không hiệu quả để sử dụng vì một khi đường dẫn được thiết lập và không có dữ liệu nào được truyền đi, thì dung lượng của đường dẫn sẽ bị lãng phí.
- ✓ Trong trường hợp này, kết nối là dành riêng, do đó không thể truyền dữ liệu nào khác ngay cả khi kênh miễn phí.

## Chuyển mạch thông điệp

Chuyển mạch thông điệp là một kỹ thuật chuyển mạch trong đó thông điệp được chuyển như một đơn vị hoàn chỉnh và được định tuyến qua các nút trung gian mà tại đó nó được lưu trữ và chuyển tiếp.

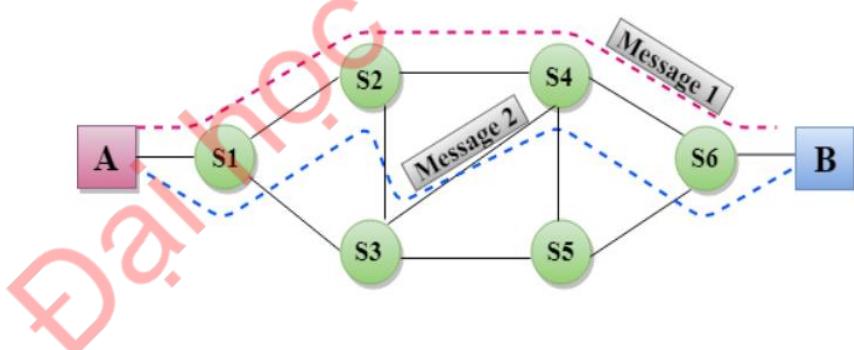
Trong kỹ thuật chuyển mạch thông điệp, không có thiết lập đường dẫn riêng giữa người gửi và người nhận.

Địa chỉ đích được thêm vào tin nhắn. Chuyển mạch thông báo cung cấp một định tuyến động vì thông báo được định tuyến qua các nút trung gian dựa trên thông tin có sẵn trong thông báo.

Chuyển mạch thông báo được lập trình theo cách để chúng có thể cung cấp các tuyến đường hiệu quả nhất.

Mỗi và mọi nút đều lưu trữ toàn bộ thông điệp và sau đó chuyển tiếp nó đến nút tiếp theo. Loại mạng này được gọi là mạng cửa hàng và mạng chuyển tiếp.

Chuyển mạch thông điệp coi mỗi tin nhắn như một thực thể độc lập.



Hình 1.10 Chuyển mạch thông điệp

### Ưu điểm Chuyển mạch thông điệp:

- ✓ Kênh dữ liệu được chia sẻ giữa các thiết bị giao tiếp giúp cải thiện hiệu quả sử dụng băng thông.
- ✓ Tắc nghẽn giao thông có thể được giảm bớt vì thông báo được lưu trữ tạm thời trong các nút.
- ✓ Ưu tiên tin nhắn có thể được sử dụng để quản lý mạng.
- ✓ Kích thước của tin nhắn được gửi qua mạng có thể khác nhau. Do đó, nó hỗ trợ dữ liệu có kích thước không giới hạn.

## Nhược điểm của Chuyển mạch thông điệp:

- ✓ Các công tắc tin nhắn phải được trang bị đủ dung lượng để cho phép chúng lưu tin nhắn cho đến khi tin nhắn được chuyển tiếp.
- ✓ Độ trễ lâu có thể xảy ra do phương tiện lưu trữ và chuyển tiếp được cung cấp bởi kỹ thuật chuyển mạch bắn tin.

## Chuyển mạch gói

Chuyển mạch gói là một kỹ thuật chuyển mạch trong đó thông điệp được gửi trong một lần, nhưng nó được chia thành nhiều phần nhỏ hơn và chúng được gửi riêng lẻ.

Thông điệp được chia thành các phần nhỏ hơn được gọi là các gói và các gói được cung cấp một số duy nhất để xác định thứ tự của chúng ở đầu nhận.

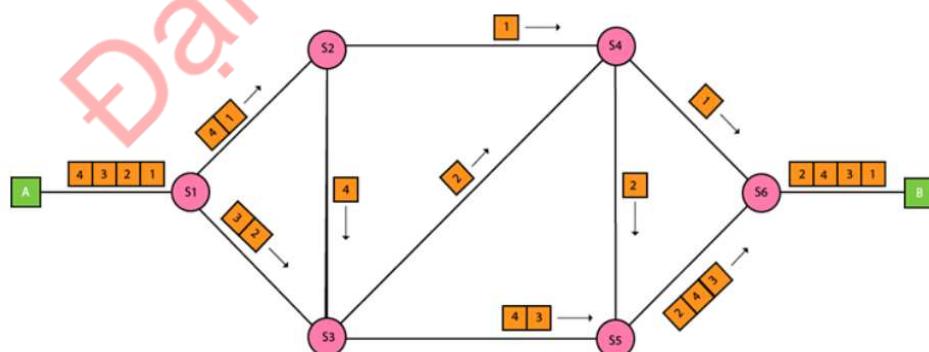
Mỗi gói chứa một số thông tin trong tiêu đề của nó như địa chỉ nguồn, địa chỉ đích và số thứ tự.

Các gói sẽ di chuyển trên mạng, đi theo đường ngắn nhất có thể.

Tất cả các gói được tập hợp lại ở đầu nhận theo đúng thứ tự.

Nếu bất kỳ gói nào bị thiếu hoặc bị hỏng, thì thông báo sẽ được gửi đi để gửi lại tin nhắn.

Nếu đạt được thứ tự chính xác của các gói, thì thông báo xác nhận sẽ được gửi.



Hình 1.11 Chuyển mạch gói

## Các phương pháp chuyển đổi gói

Có hai cách tiếp cận để chuyển đổi gói:

### Chuyển mạch gói dữ liệu:

Nó là một công nghệ chuyển mạch gói trong đó gói được biết đến như một gói dữ liệu, được coi như một thực thể độc lập. Mỗi gói chứa thông tin về đích và bộ chuyển mạch sử dụng thông tin này để chuyển gói đến đúng đích.

Các gói được tập hợp lại ở đầu nhận theo đúng thứ tự.

Trong kỹ thuật chuyển mạch gói dữ liệu, đường dẫn không cố định.

Các nút trung gian thực hiện các quyết định định tuyến để chuyển tiếp các gói tin.

Datagram Packet Switching còn được gọi là chuyển mạch không kết nối.

### Chuyển mạch ảo

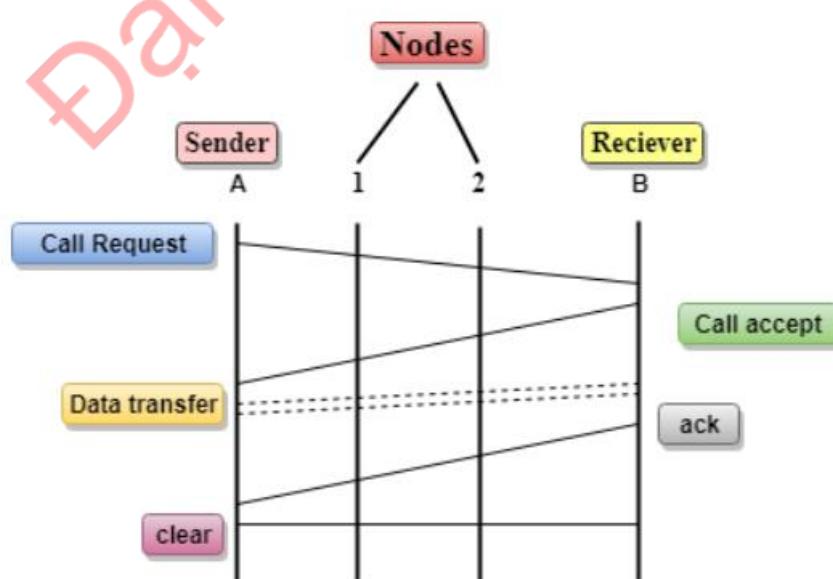
Chuyển mạch ảo còn được gọi là chuyển mạch hướng kết nối.

Trong trường hợp Chuyển mạch kênh ảo, một lộ trình dự kiến trước được thiết lập trước khi các thông điệp được gửi đi.

Các gói yêu cầu cuộc gọi và chấp nhận cuộc gọi được sử dụng để thiết lập kết nối giữa người gửi và người nhận.

Trong trường hợp này, đường dẫn được cố định trong khoảng thời gian của một kết nối logic.

Hãy hiểu khái niệm chuyển mạch ảo qua sơ đồ:



Hình 1.12 Chuyển mạch ảo

Trong sơ đồ trên, A và B lần lượt là người gửi và người nhận. 1 và 2 là các nút.

Các gói yêu cầu cuộc gọi và chấp nhận cuộc gọi được sử dụng để thiết lập kết nối giữa người gửi và người nhận.

Khi một tuyến đường được thiết lập, dữ liệu sẽ được chuyển.

Sau khi truyền dữ liệu, người nhận sẽ gửi tín hiệu báo nhận rằng tin nhắn đã được nhận.

Nếu người dùng muốn chấm dứt kết nối, một tín hiệu rõ ràng sẽ được gửi cho việc chấm dứt.

### **Ưu điểm của chuyển mạch gói:**

- ✓ Hiệu quả về chi phí: Trong kỹ thuật chuyển mạch gói, các thiết bị chuyển mạch không yêu cầu bộ nhớ thứ cấp lớn để lưu trữ các gói, do đó chi phí được giảm thiểu ở một mức độ nào đó. Do đó, chúng ta có thể nói rằng kỹ thuật chuyển mạch gói là một kỹ thuật tiết kiệm chi phí.
- ✓ Đáng tin cậy: Nếu bất kỳ nút nào đang bận, thì các gói tin có thể được định tuyến lại. Điều này đảm bảo rằng kỹ thuật chuyển mạch gói cung cấp thông tin liên lạc đáng tin cậy.
- ✓ Hiệu quả: Chuyển mạch gói là một kỹ thuật hiệu quả. Nó không yêu cầu bắt kỳ đường dẫn thiết lập nào trước khi truyền và nhiều người dùng có thể sử dụng cùng một kênh liên lạc đồng thời, do đó sử dụng rất hiệu quả băng thông có sẵn.

### **Nhược điểm của chuyển mạch gói:**

- ✓ Kỹ thuật chuyển mạch gói không thể được thực hiện trong những ứng dụng yêu cầu độ trễ thấp và dịch vụ chất lượng cao.
- ✓ Các giao thức được sử dụng trong kỹ thuật chuyển mạch gói rất phức tạp và đòi hỏi chi phí thực hiện cao.
- ✓ Nếu mạng bị quá tải hoặc bị hỏng, thì nó yêu cầu truyền lại các gói bị mất. Nó cũng có thể dẫn đến việc mất thông tin quan trọng nếu các lỗi không được khôi phục.

## 1.4 Kết luận

Sau khi hiểu rõ được các nội dung về tổng quan mạng nội bộ thì có thể đưa ra được một số tiêu chí về hệ thống mạng LAN cho các công ty như sau:

Nhu cầu sử dụng mạng trong việc xây dựng và thiết kế hệ thống mạng LAN và Internet phần lớn phụ thuộc vào yêu cầu cụ thể của doanh nghiệp. Có ba khía cạnh chính mà chúng ta thường quan tâm đến như sau:

- **Mục Đích Sử Dụng Mạng:** Điều quan trọng là hiểu rõ mục đích sử dụng mạng LAN và Internet. Ai là những người sử dụng? Mục đích sử dụng là gì? Các tác vụ công việc bao gồm những gì? Cần đạt được tốc độ bao nhiêu Mbps để thỏa mãn nhu cầu, từ việc duyệt web đến tải video đáp ứng công việc.
- **Số Lượng và Diện Tích Cần Phủ Sóng:** Nắm vững số lượng phòng và diện tích cần phủ sóng cho hệ thống mạng LAN và Internet. Điều này giúp định rõ khối lượng công việc và cung cấp dữ liệu cụ thể cho quá trình xây dựng và thiết kế.
- **Mật Độ và Số Lượng Thiết Bị:** Tính toán chính xác về mật độ và số lượng thiết bị trong văn phòng. Điều này đặc biệt quan trọng để đảm bảo mạng có thể đáp ứng đồng thời với số lượng người dùng và thiết bị.

### Lựa chọn thiết bị mạng:

Lựa chọn thiết bị mạng là một quá trình quan trọng trong việc thiết kế và triển khai hệ thống mạng LAN và Internet cho doanh nghiệp. Các yếu tố quan trọng cần xem xét bao gồm:

- **Thương Hiệu và Công Năng Thiết Bị Mạng:** Quyết định sử dụng thiết bị mạng của thương hiệu nào và các công năng cụ thể của chúng. Điều này đặc biệt quan trọng để đảm bảo thiết bị đáp ứng đầy đủ nhu cầu công việc.
- **Số Lượng Thiết Bị Cần Lắp Đặt:** Đặt câu hỏi về số lượng thiết bị cần lắp đặt để đáp ứng hiệu suất và nhu cầu của doanh nghiệp. Việc xác định đúng số lượng thiết bị là quan trọng để tránh tình trạng mạng yếu và không ổn định.
- **Tư Vấn Chọn Lựa Thiết Bị Chính Hãng:** Cần nhắc lựa chọn thiết bị mạng từ các đối tác chính hãng để đảm bảo chất lượng và tính ổn định. Các thiết bị chính hãng thường tích hợp nhiều chức năng lưu trữ và quản lý dữ liệu tốt hơn.

- Cân Nhắc Về Diện Tích và Nhu Cầu Sử Dụng: Xem xét diện tích của từng văn phòng và nhu cầu sử dụng của doanh nghiệp để đưa ra quyết định chính xác về công năng và số lượng thiết bị mạng.
- Quản Lý Đường Dây Cáp Mạng: Đặc biệt quan trọng là sắp xếp và quản lý dây dẫn một cách cẩn thận. Việc lắp đặt hệ thống máng cáp có thể giúp bảo vệ đường dây cáp mạng khỏi nhiễu điện, điện giật, và trầy xước vỏ dây, đảm bảo hoạt động ổn định.

Đại học Sao Đỏ

## **CHƯƠNG 2: TẤN CÔNG MẠNG NỘI BỘ VÀ GIẢI PHÁP PHÒNG CHỐNG TẤN CÔNG**

### **2.1 Tổng quan về an toàn bảo mật thông tin**

An ninh mạng ngày càng trở nên tăng cường về tầm quan trọng, đặc biệt khi điện thoại thông minh, máy tính, và máy tính bảng trở thành một phần quan trọng không thể thiếu trong cả công việc hàng ngày và cuộc sống cá nhân của chúng ta. Mức độ phụ thuộc vào các công cụ trực tuyến trong các khía cạnh khác nhau của hoạt động kinh doanh – từ mạng xã hội và tiếp thị qua email đến lưu trữ dữ liệu nhân viên và khách hàng trên đám mây – đặt ra nhu cầu bổ sung cho chúng ta trong việc bảo vệ những thông tin quý giá này.[2]

Sự phụ thuộc vào các công cụ số khiến nhiều doanh nghiệp gặp rủi ro từ các cuộc tấn công mạng. Kiến thức vững chắc về an ninh mạng là chìa khóa ở đây, vì các cuộc tấn công như vậy vẫn không ngừng phát triển và ngày càng tinh vi hơn. Nạn nhân của các cuộc tấn công mạng có thể có nguy cơ:

- Mất dữ liệu nhạy cảm
- Tổn thất tài chính do trộm cắp dữ liệu
- Chi phí cao cho việc khôi phục dữ liệu bị đánh cắp
- Mất đi danh tiếng
- Đóng cửa (trong trường hợp nghiêm trọng)

Với sự phát triển của việc chúng ta sử dụng internet, các công cụ trực tuyến và các thiết bị liên quan, tội phạm mạng đã lan rộng trong doanh nghiệp. Vì an ninh mạng không có giải pháp chung cho tất cả, bạn cần xem xét các lĩnh vực khác nhau có liên quan đến doanh nghiệp của bạn, dữ liệu của bạn và nơi nó được lưu trữ trực tuyến.

Các loại an ninh mạng quan trọng nhất mà các công ty đang tập trung xây dựng tuyến phòng thủ vững chắc nêu là:

- **Network security** – Bảo vệ chống lại việc truy cập trái phép vào cơ sở hạ tầng nội bộ, thường được cung cấp bởi các quản trị viên mạng, những người thực hiện các chính sách về mật khẩu và thông tin đăng nhập mạnh, tường lửa, mã hóa và phần mềm chống vi-rút.

- **App security** – Các bản cập nhật và thử nghiệm thường xuyên có thể bảo vệ ứng dụng của bạn khỏi các mối đe dọa.
- **Information and data security** – Mạng và ứng dụng lưu trữ dữ liệu cần được bảo vệ bổ sung thêm.
- **Endpoint protection** – giảm rủi ro khi truy cập từ xa.
- **Cloud security** – phần mềm giám sát và bảo vệ dữ liệu được lưu trữ trên đám mây.
- **Mobile security and IoT** – Điện thoại thông minh, máy tính bảng, và các thiết bị khác kết nối với Internet của Vạn vật (Internet of Things; IoT) đều đặt ra các yêu cầu an toàn riêng biệt.
- **Business continuity planning and emergency recovery** – Mọi doanh nghiệp cần có kế hoạch dự phòng trong trường hợp xảy ra tấn công bằng hack, thảm họa thiên nhiên hoặc các sự kiện khác đe dọa đến an ninh mạng của mình.

### Các nguy cơ ảnh hưởng đến an toàn mạng

Có nhiều loại tấn công mạng công khai và âm thầm – cả hai đều được thiết kế để làm gián đoạn hoạt động kinh doanh của doanh nghiệp theo những cách khác nhau. Khi ngày càng có nhiều công ty nhận thức được tầm quan trọng của việc bảo vệ tài nguyên của họ và thực hiện đào tạo về an ninh mạng, thì tin tặc và tội phạm mạng cũng đang phát triển các hình thức tấn công khác ngày càng tinh vi hơn.

Bằng cách cập nhật kiến thức của mình, bạn có thể bảo vệ doanh nghiệp của mình khỏi chúng tốt hơn. Có năm loại tấn công mạng phổ biến nhất:

- **Malware** là một lỗ hổng trên hệ thống bảo vệ mạng của bạn, chẳng hạn như phần mềm gián điệp, phần mềm tống tiền và vi rút.
- **Phishing** – Là những tin nhắn độc hại (thường là email) chứa các liên kết độc hại mà khi được nhấp vào, chúng sẽ gửi quyền truy cập vào thông tin nhạy cảm.
- **Denial of Service (DoS)** – Tin tặc tràn ngập mạng hoặc hệ thống của bạn với nhiều thông tin dư thừa nhằm làm quá tải và buộc hệ thống của bạn phải dừng lại.
- **Man in the middle (MitM)** – tội phạm mạng làm gián đoạn kết nối, thường là qua mạng wi-fi công cộng không an toàn và sau đó đánh cắp dữ liệu nhạy cảm.

- **Zero-day attack** – một cuộc tấn công ít phổ biến hơn nhưng xảy ra ngày càng nhiều giữa việc công bố bản cập nhật hoặc bản vá bảo mật và cài đặt của nó.

Những kiểu tấn công mạng này có thể ảnh hưởng đến nhiều doanh nghiệp, chẳng hạn như quán cà phê có mạng wi-fi không an toàn hoặc các shop online có nguy cơ bị tấn công zero-day.

## 2.2. Một số kỹ thuật tấn công mạng nội bộ

### 2.2.1. Tấn công sử dụng phần mềm độc hại (Malware)

Tấn công Malware là hình thức phổ biến và rộng rãi nhất. Gồm những loại như spyware( gián điệp), ransomware( mã độc), worm( phần mềm độc hại có khả năng lây lan các thiết bị khác). Thông thường, kẻ tấn công sẽ tấn công người dùng thông qua các lỗ hổng bảo mật, có thể là dụ các nạn nhân click vào một đường link để phần mềm độc hại tự động cài đặt vào máy tính. Một khi được cài đặt thành công, malware sẽ gây ra.

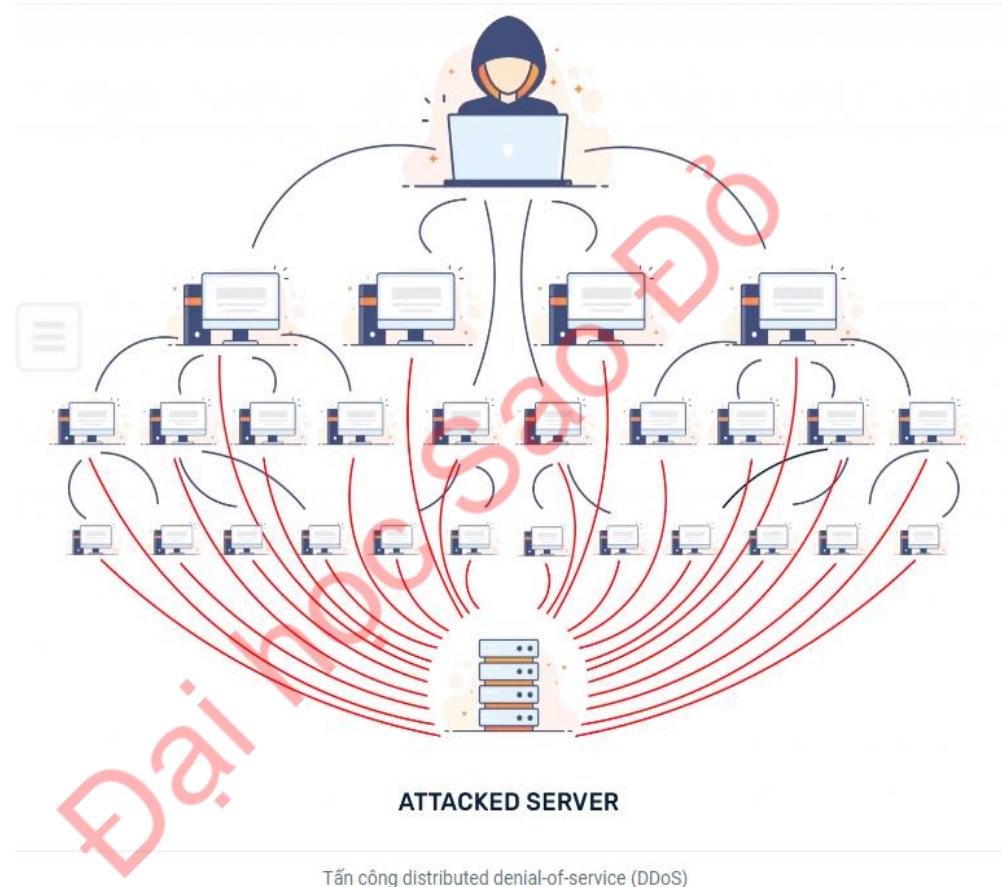
- ✓ Ngăn cản người dùng truy cập vào một đường link quan trọng( ransomware)
- ✓ Cài đặt thêm những phần mềm độc hại khác
- ✓ Nghe lén người dùng và đánh cắp dữ liệu( spyware)
- ✓ Phá hỏng phần mềm, phần cứng, làm gián đoạn hệ thống.

### 2.2.2 Tấn công giả mạo (Phishing)

Phishing là một kỹ thuật tấn công mà kẻ tấn công giả mạo thành một cá nhân hoặc tổ chức có uy tín để đánh lừa người dùng. Thông thường, chúng sử dụng các phương tiện như tin nhắn hoặc email để tạo ra sự nhầm lẫn và chiếm đoạt lòng tin của nạn nhân. Mục tiêu chính của phishing thường là đánh cắp thông tin nhạy cảm như thẻ tín dụng và mật khẩu. Đôi khi, phishing cũng có thể là một phần của chiến lược để cài đặt phần mềm độc hại vào thiết bị của nạn nhân, biến nó thành một phần trong cuộc tấn công malware.

### 2.2.3 Tấn công từ chối dịch vụ(DoS và DDoS)

Một cuộc tấn công DDoS sẽ tập trung vào việc chiếm đoạt tài nguyên của hệ thống, làm cho nó không thể xử lý các yêu cầu dịch vụ. Điều đặc biệt của cuộc tấn công DDoS là nó được thực hiện từ nhiều host khác nhau, mà đều bị nhiễm phần mềm độc hại do hacker kiểm soát. Mục tiêu của cuộc tấn công này là làm quá tải hệ thống bằng cách đẩy nó đến giới hạn chịu đựng, từ đó làm cho dịch vụ trở nên không khả dụng.



Hình 2.1 Tấn công từ chối dịch vụ(DoS và DDoS

Khác với các cuộc tấn công được thiết kế để cung cấp quyền truy cập cho kẻ tấn công, cuộc tấn công DDoS không đem lại lợi ích trực tiếp cho người tấn công. Với một số hacker, việc gây ra từ chối dịch vụ đã đủ để họ cảm thấy hài lòng. Tuy nhiên, nếu nguồn tấn công nhắm đến một đối thủ cạnh tranh kinh doanh, lợi ích mà kẻ tấn công có thể đạt được là khá lớn. Một mục tiêu khác của cuộc tấn công DDoS có thể là làm cho hệ thống trở nên offline để tạo điều kiện cho một loại tấn công khác, như việc chiếm quyền điều khiển (hijacking).

Có nhiều kiểu tấn công DoS và DDoS khác nhau, phổ biến nhất là tấn công TCP SYN flood, tấn công Teardrop, tấn công Smurf, tấn công ping-of-death và botnet.

## Tấn công TCP SYN flood

Tấn công TCP SYN flood là một kiểu tấn công mạng mà kẻ tấn công cố gắng làm cho máy chủ không thể phản hồi các yêu cầu kết nối TCP đến bằng cách gửi một lượng lớn các gói tin SYN (synchronize) mà không hoàn thành quá trình bắt tay 3 bước của quá trình thiết lập kết nối TCP.

Quá trình thực hiện tấn công SYN flood thường diễn ra như sau:

- Gửi Yêu Cầu SYN: Kẻ tấn công gửi một lượng lớn yêu cầu kết nối SYN đến máy chủ mục tiêu, mà không hoàn thành bước cuối cùng của quá trình thiết lập kết nối.
- Chờ Phản Hồi: Máy chủ nhận được các yêu cầu SYN và tạo ra một bản ghi trong bảng kết nối đang chờ. Tuy nhiên, vì các yêu cầu SYN không hoàn thành, máy chủ không thể hoàn tất quá trình thiết lập kết nối TCP.
- Quá Tải Bảng Kết Nối Chờ: Với lượng lớn yêu cầu SYN, bảng kết nối chờ trên máy chủ sẽ quá tải, dẫn đến tình trạng hết tài nguyên.
- Không Phản Hồi đến Yêu Cầu Hợp Lệ: Do tài nguyên bị quá tải, máy chủ không thể xử lý các yêu cầu kết nối hợp lệ từ người dùng thực.

Tấn công SYN flood có thể gây quá tải hệ thống, làm cho dịch vụ trở nên không khả dụng đối với người dùng hợp lệ. Để ngăn chặn tấn công này, có các biện pháp bảo mật như cấu hình tường lửa, sử dụng thiết bị chống tấn công SYN, hay triển khai các giải pháp phần cứng và phần mềm chống tấn công mạng.

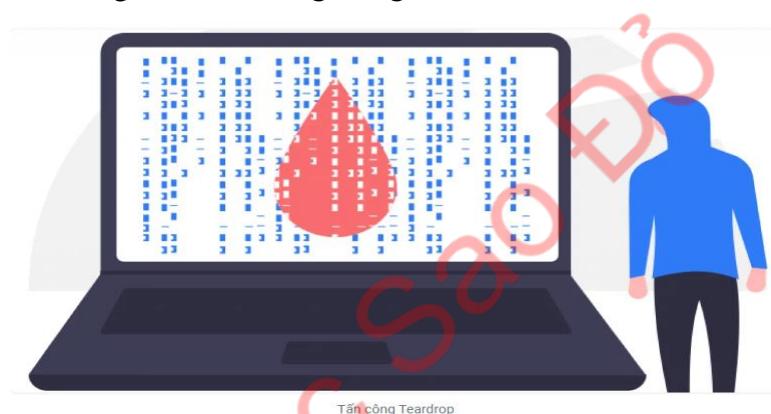
## Tấn công Teardrop

Tấn công Teardrop là một loại tấn công mạng mà kẻ tấn công gửi các gói tin IP với các đoạn dữ liệu đặc biệt được tạo để làm cho hệ điều hành và các ứng dụng trên máy chủ bị hỏng.

Cụ thể, tấn công Teardrop thường liên quan đến việc gửi các gói tin IP có các đoạn dữ liệu lặp lại hoặc chồng chéo lên nhau một cách không hợp lý. Điều này có thể gây ra lỗi trong quá trình tái tạo và xử lý gói tin trên máy chủ đích.

Quá trình thực hiện tấn công Teardrop thường diễn ra như sau:

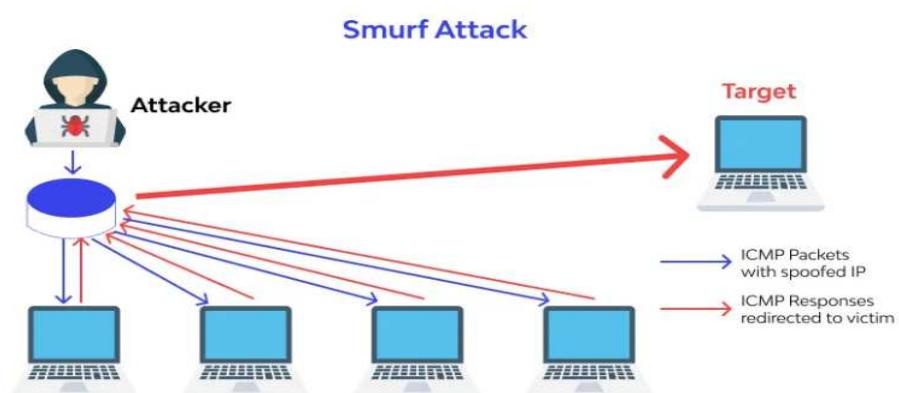
- Gửi Các Gói Tin Teardrop: Kẻ tấn công tạo ra các gói tin IP với các đoạn dữ liệu được thiết kế để làm hỏng quá trình xử lý trên máy chủ. Đoạn dữ liệu này thường có kích thước và cấu trúc đặc biệt.
- Nhận và Xử Lý: Máy chủ nhận các gói tin Teardrop và cố gắng tái tạo dữ liệu. Tuy nhiên, do cách các đoạn dữ liệu được thiết kế, quá trình xử lý có thể gặp lỗi.
- Lỗi Trong Quá Trình Xử Lý: Quá trình xử lý các gói tin Teardrop có thể gây ra lỗi trong việc tái tạo dữ liệu, làm cho hệ điều hành và ứng dụng trên máy chủ bị hỏng hoặc không thể hoạt động đúng cách.



Hình 2.2 Tấn công Teardrop

Tấn công Teardrop có thể dẫn đến việc làm cho hệ thống mục tiêu không khả dụng hoặc không thể thực hiện các chức năng quan trọng

### Tấn công Smurf



Hình 2.3 Tấn công Smurf

Tấn công Smurf là một loại tấn công mạng sử dụng kỹ thuật "ICMP Echo Request" (ping) để tạo ra một lưu lượng mạng lớn và quấy rối đối với một hệ thống mục tiêu. Tên "Smurf" được đặt theo tên của chương trình mẫu tấn công đầu tiên sử dụng kỹ thuật này.

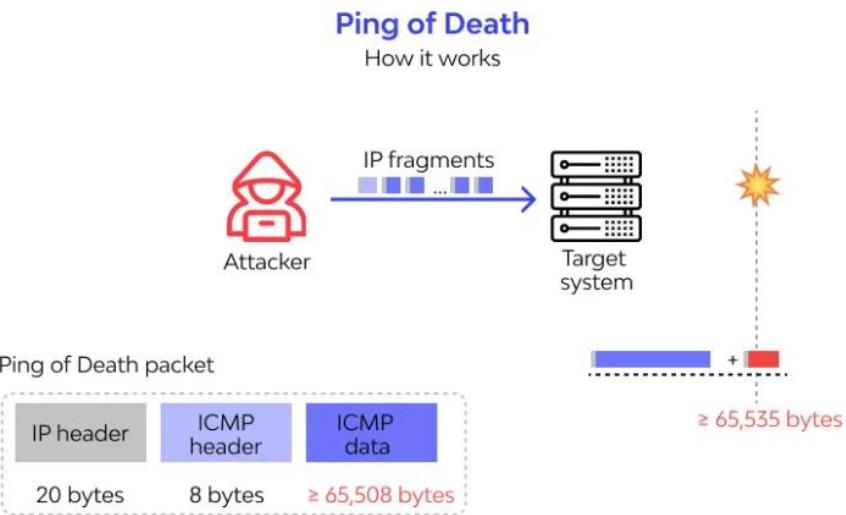
Quá trình thực hiện tấn công Smurf thường bao gồm các bước sau:

- Chọn Hệ Thống Tấn Công (Amplifier): Kẻ tấn công chọn một hoặc nhiều hệ thống mà họ muốn tấn công, thường là các hệ thống có thể hoạt động như "amplifiers" (bộ khuếch đại) trong tấn công.
- Sử Dụng Broadcast IP: Kẻ tấn công gửi các gói tin ICMP Echo Request đến một địa chỉ IP broadcast, thường là địa chỉ IP broadcast của một mạng con.
- Giả Mạo Địa Chỉ Người Được Tấn Công: Địa chỉ IP nguồn trong các gói tin được giả mạo để trở thành địa chỉ IP của hệ thống mục tiêu.
- Lưu Lượng Gửi Đến Amplifiers: Do sử dụng địa chỉ broadcast, mọi hệ thống trong mạng con đều nhận được gói tin và tạo ra một lưu lượng trả lời (ICMP Echo Reply) đồng loạt đến địa chỉ IP giả mạo, tức là hệ thống mục tiêu.
- Lưu Lượng Lớn Tập Trung: Kết quả là, lưu lượng mạng lớn tập trung đến hệ thống mục tiêu, gây quấy rối và có thể làm cho hệ thống trở nên không khả dụng.

Để ngăn chặn tấn công Smurf, người quản trị hệ thống có thể cấu hình các thiết bị mạng để không chấp nhận phản hồi từ địa chỉ broadcast hoặc triển khai các biện pháp bảo mật như lọc địa chỉ IP và sử dụng kỹ thuật giảm nhỏ "IP directed broadcast."

### Tấn công Ping of Death

Loại tấn công này sử dụng các gói IP để ping một hệ thống mục tiêu có kích thước IP tối đa là 65,535 byte. Các gói IP có kích thước này không được cho phép, vì vậy hacker sẽ phân mảnh gói IP. Khi hệ thống mục tiêu tập hợp lại gói tin, nó có thể bị quá tải bộ đệm và các sự cố khác.



Hình 2.4 Tân công Ping of Death

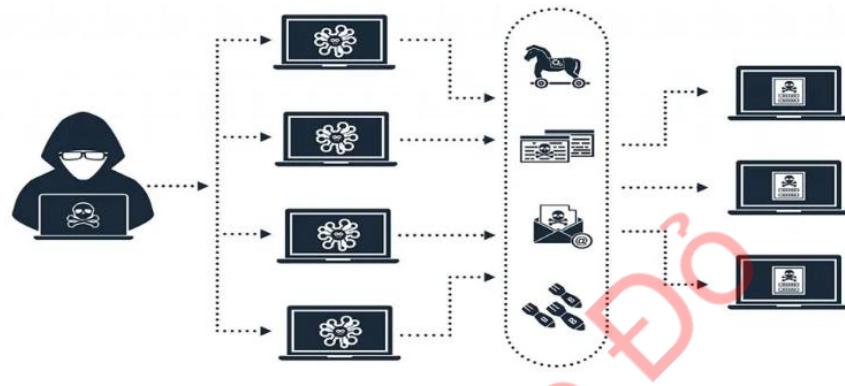
## Botnet

Botnet là một tập hợp các máy tính kết nối với internet và được kiểm soát từ xa bằng một hay nhiều máy tính chủ. Những máy tính trong botnet thường được nhiễm malware hoặc bot (robot) mà kẻ tấn công kiểm soát. Mục tiêu của việc tạo ra botnet thường là để thực hiện các hoạt động tấn công, thường làm hại hoặc kiểm soát mạng.

Dưới đây là một số đặc điểm chính của botnet:

- Máy Chủ Kiểm Soát (C&C Server): Botnet được điều khiển thông qua một hay nhiều máy chủ tập trung, thường được gọi là máy chủ kiểm soát (C&C server). Kẻ tấn công sử dụng C&C server để gửi các lệnh đến botnet.
- Bot (Robot): Bot là một loại phần mềm độc hại được cài đặt trên máy tính của người dùng mà kẻ tấn công muốn kiểm soát. Bot có thể thực hiện nhiều nhiệm vụ khác nhau, như gửi thư rác, tham gia vào các cuộc tấn công phân tán dịch vụ (DDoS), đánh cắp thông tin cá nhân, hoặc thậm chí chạy các hoạt động trái pháp luật khác.
- Rơi vào Hệ Thống Một Cách Bí Mật: Máy tính của người dùng thường rơi vào botnet một cách bí mật, thường qua việc mở các tệp đính kèm độc hại, truy cập các trang web độc hại, hoặc sử dụng lỗ hổng bảo mật trong hệ thống.

- **Sức Mạnh Đám Đông:** Botnet có sức mạnh lớn khi kết hợp nhiều máy tính. Việc kết hợp lực lượng của hàng nghìn hoặc thậm chí hàng triệu máy tính trong một cuộc tấn công có thể tạo ra một áp lực lớn đối với một hệ thống mục tiêu.
- **Sử Dụng Cho Các Mục Đích Độc Hại:** Botnet thường được sử dụng cho các mục đích độc hại như tấn công mạng, phát tán malware, thực hiện lừa đảo trực tuyến, hoặc thậm chí đòi tiền (ransomware).



*Hình 2.5 Tấn công Botnet*

Ngăn chặn botnet đòi hỏi sự hợp tác giữa cộng đồng an ninh mạng, người quản trị hệ thống, và các nhà cung cấp dịch vụ internet để phát hiện, chặn, và loại bỏ bot từ hệ thống. Các biện pháp bảo mật như phần mềm chống virus, tường lửa mạng, và cập nhật hệ thống thường xuyên đều quan trọng để bảo vệ khỏi sự lây lan của botnet.

#### 2.2.4 Tấn công cơ sở dữ liệu (SQL injection)

Tấn công SQL injection là một kỹ thuật tấn công thông dụng trong lĩnh vực an ninh mạng, nhắm vào các cơ sở dữ liệu. Trong tấn công này, kẻ tấn công chèn hoặc "đút" các đoạn mã SQL độc hại vào các truy vấn SQL được thực thi bởi ứng dụng web. Mục tiêu của tấn công SQL injection là tiếp cận, thay đổi, hoặc xóa dữ liệu trong cơ sở dữ liệu.

Dưới đây là một số đặc điểm và cách thức tấn công SQL injection thường được thực hiện:

- **Chèn Mã SQL Độc Hại:** Kẻ tấn công thường chèn các đoạn mã SQL độc hại vào các trường đầu vào của ứng dụng web, ví dụ như biểu mẫu tìm kiếm hoặc trang đăng nhập.

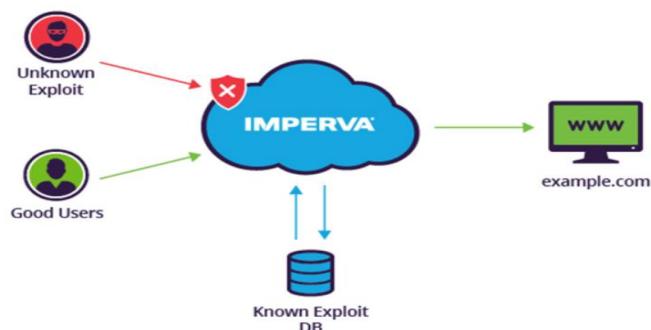
- **Bypass Cơ Chế Xác Thực:** Nếu ứng dụng web sử dụng xác thực bằng cách kiểm tra tên người dùng và mật khẩu từ cơ sở dữ liệu, kẻ tấn công có thể sử dụng SQL injection để bypass xác thực, đặc biệt khi ứng dụng web không kiểm tra đầu vào đúng cách.
- **Thực Hiện Truy Vấn Sai Lệnh:** Kẻ tấn công có thể làm sai lệnh truy vấn SQL đang được thực hiện bởi ứng dụng web để thu được dữ liệu nhạy cảm hoặc thực hiện các thao tác không cho phép.
- **Thực Hiện Các Lệnh SQL Độc Hại:** Các lệnh như UNION SELECT, OR '1'='1', DROP TABLE, hoặc sử dụng các hàm SQL độc hại là những cách thức phổ biến để thực hiện tấn công SQL injection.



Hình 2.6 Tấn công SQL injection

### 2.2.5 Khai thác lỗ hổng Zero-day (Zero day attack)

Khai thác lỗ hổng Zero-day (Zero Day Exploits) là một hình thức tấn công mà kẻ tấn công sử dụng một lỗ hổng bảo mật mà nhà cung cấp phần mềm hoặc tổ chức bảo mật chưa biết đến. Cụ thể, "Zero-day" ám chỉ thời gian từ khi lỗ hổng được phát hiện đến khi nhà cung cấp phần mềm cung cấp một biện pháp bảo vệ hoặc bản vá để khắc phục lỗ hổng.



Hình 2.7 Khai thác lỗ hổng Zero-day (Zero Day Exploits)

## 2.2.6 Tấn công Man in the middle(MitM)

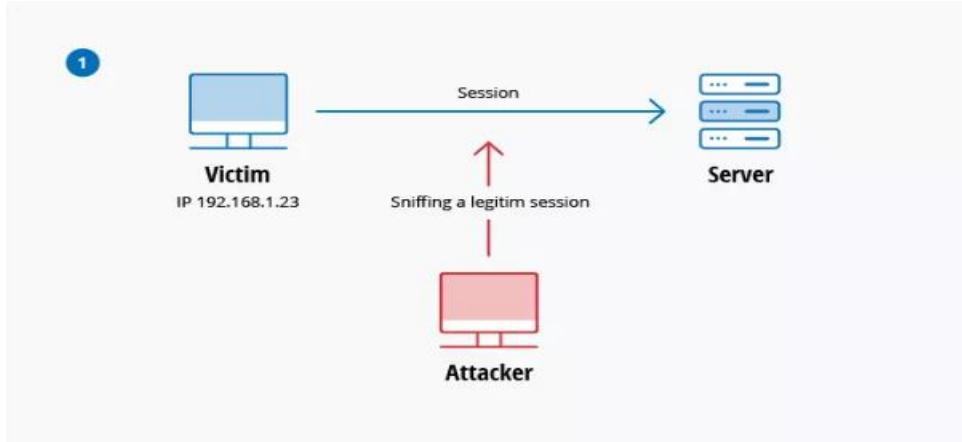
Tấn công Man-in-the-Middle (MitM) là một hình thức tấn công trong đó kẻ tấn công can thiệp vào giao tiếp giữa hai bên mà không bị phát hiện. Kẻ tấn công có thể đọc, sửa đổi hoặc thậm chí chặn hoặc chuyển hóa thông tin giữa các bên giao tiếp.

Dưới đây là một số đặc điểm và cách thức thực hiện tấn công MitM:

- Giả Mạo Bản Sao của Giao Dịch: Kẻ tấn công giả mạo bản sao của giao dịch giữa hai bên và can thiệp vào quá trình truyền tải thông tin.
- Kiểm Soát Giao Tiếp: Khi đã ở giữa, kẻ tấn công có thể kiểm soát toàn bộ giao tiếp giữa hai bên và thậm chí làm cho chúng tin rằng họ đang trò chuyện trực tiếp với nhau.
- Đánh Cắp Thông Tin Đăng Nhập: Kẻ tấn công có thể thu thập thông tin đăng nhập khi người dùng nhập vào các trang web hoặc ứng dụng qua kết nối mà kẻ tấn công kiểm soát.
- Phân Loại Tấn Công MitM:
- Tấn công trung gian chủ động (Active): Kẻ tấn công can thiệp vào giao tiếp và tạo ra một sự tương tác giả mạo.
- Tấn công trung gian chủ động (Passive): Kẻ tấn công lén ngụy ngực và chỉ nghe lén thông tin mà không làm thay đổi dữ liệu.

Các Phương Thức Thực Hiện MitM:

- ARP Spoofing: Sử dụng kỹ thuật ARP để giả mạo địa chỉ MAC của thiết bị mạng.
- DNS Spoofing: Can thiệp vào quá trình giải mã tên miền để chuyển hướng người dùng đến trang web giả mạo.
- SSL Stripping: Giả mạo trang web an toàn để chuyển hóa kết nối từ HTTPS sang HTTP.
- Packet Sniffing: Nghe lén và thu thập dữ liệu truyền qua mạng.



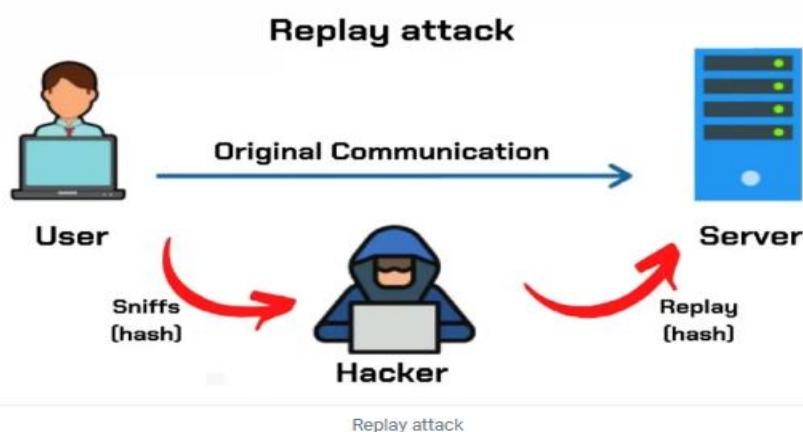
Hình 2.8 Tấn công Man-in-the-Middle (MitM)

### Giả mạo IP (IP Spoofing)

Giả mạo IP là phương pháp được các hacker sử dụng để làm cho hệ thống tin rằng nó đang tương tác với một thực thể đáng tin cậy, có sự hiểu biết và cung cấp cho hacker quyền truy cập vào hệ thống. Kỹ thuật này thường được thực hiện bằng cách hacker gửi một gói tin với địa chỉ IP nguồn được giả mạo, thường là của một server đáng tin cậy và đã biết, thay vì sử dụng địa chỉ IP nguồn của chính hacker. Host mục tiêu, nhận được gói tin này, có thể lầm tưởng và chấp nhận nó, thực hiện các hành động tương ứng.

### Replay

Cuộc tấn công phát lại xảy ra khi hacker ghi lại và lưu trữ các tin nhắn trước đó, sau đó cố gắng truyền lại chúng bằng cách giả mạo một trong những người tham gia. Để đối phó với loại tấn công này, có thể sử dụng biện pháp như việc ẩn phiên bản thời gian hoặc số nonce (một số ngẫu nhiên hoặc chuỗi thay đổi theo thời gian).



Hình 2.9 Tấn công Replay

Hiện tại, không có công nghệ hay cấu hình duy nhất nào có thể ngăn chặn mọi cuộc tấn công Man-in-the-Middle (MitM). Tuy nhiên, tổng thể, việc sử dụng mã hóa và chứng chỉ SSL là biện pháp bảo vệ hiệu quả chống lại nhiều loại cuộc tấn công MitM. Điều này đảm bảo tính bí mật và tính toàn vẹn của thông tin truyền tải. Tuy nhiên, cũng cần lưu ý rằng một số cuộc tấn công Man-in-the-Middle có thể xâm nhập vào giữa các giao tiếp một cách mà việc mã hóa cũng không thể ngăn chặn được.

### 2.2.7 Các loại khác

Ngoài ra, còn nhiều hình thức tấn công mạng khác như tấn công chuỗi cung ứng, tấn công qua email, tấn công từ bên trong tổ chức, và nhiều hình thức khác. Mỗi loại tấn công đều có đặc điểm riêng, và chúng liên tục phát triển, trở nên phức tạp và tinh vi, yêu cầu cá nhân và tổ chức duy trì tình trạng cảnh báo và liên tục cập nhật với các công nghệ phòng chống mới.

## 2.3. Một số giải pháp phòng chống tấn công mạng nội bộ

### Đối với cá nhân:

- Không nên truy cập vào các điểm Wifi công cộng mà không cần mật khẩu
- Không sử dụng phần mềm bẻ khóa (crack) trên mạng
- Bảo vệ mật khẩu cho cá nhân bằng cách đặt mật khẩu phức tạp, bật tính năng bảo mật 2 lớp – xác nhận qua điện thoại,...
- Cập nhật phần mềm, hệ điều hành lên phiên bản mới nhất.
- Cảnh thận khi duyệt Email, kiểm tra kỹ tên người gửi để phòng tránh mail lừa đảo.
- Không được tải các File hoặc nhấp vào đường link không rõ nguồn gốc.
- Không sử dụng các thiết bị ngoại vi như Usb dùng chung.
- Cài đặt phần mềm diệt Virus uy tín.

### Đối với tổ chức công ty, doanh nghiệp

- Cùng nhau xây dựng một chính sách bảo mật với các điều khoản rõ ràng, minh bạch.
- Lựa chọn các phần mềm, đối tác một cách kỹ lưỡng và ưu tiên những bên có cam kết bảo mật và cam kết cập nhật bảo mật thường xuyên.
- Không sử dụng các phần mềm Crack trên khi ở trong mạng nội bộ

- Cập nhật phần mềm, Firmware lên phiên bản mới nhất.
- Sử dụng các dịch vụ lưu trữ đám mây uy tín cho mục đích lưu trữ dữ liệu.
- Cần đánh giá bảo mật và xây dựng một chiến lược an ninh mạng tổng thể cho công ty, bao gồm các thành phần: bảo mật cho Website, bảo mật hệ thống máy chủ, mạng nội bộ,...
- Thường xuyên tổ chức các buổi đào tạo, Training kiến thức sử dụng Internet an toàn cho nhân viên.

## 2.4. Kết luận Chương 2

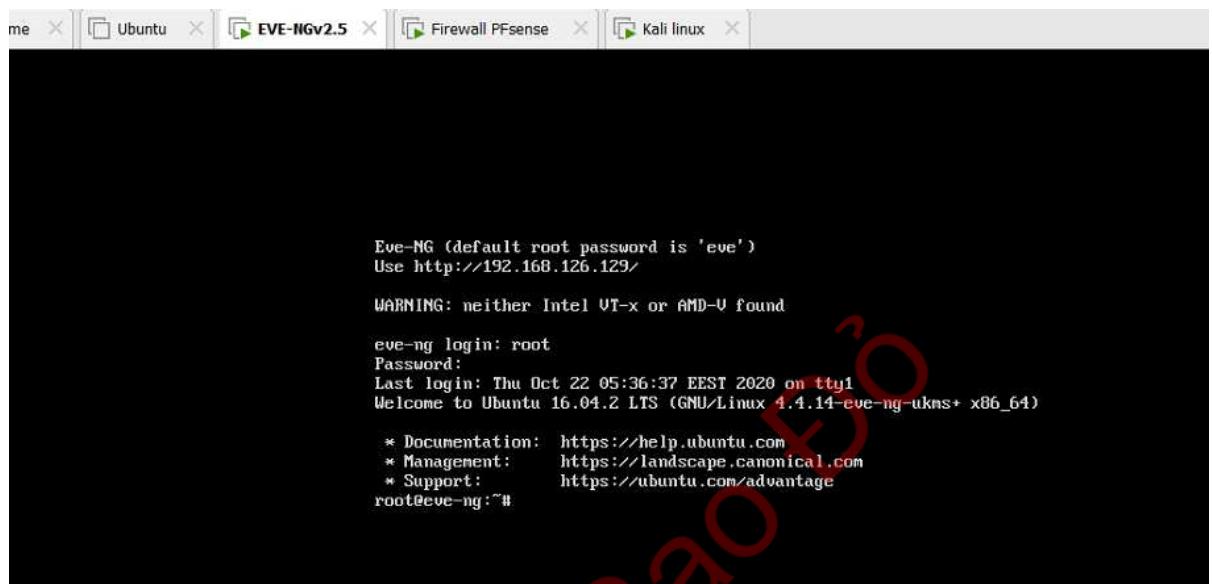
Để bảo vệ tất cả tài sản CNTT của cơ quan, tổ chức, cần đa dạng hóa chiến lược phát hiện mối đe dọa nội bộ thay vì chỉ dựa vào một giải pháp duy nhất. Một hệ thống phát hiện mối đe dọa nội bộ hiệu quả kết hợp một số công cụ để không chỉ theo dõi hành vi của nhân sự nội bộ mà còn lọc qua số lượng lớn các cảnh báo và loại bỏ các kết quả dương tính giả.

Các công cụ như ứng dụng Học máy, cập nhật tri thức các mối đe dọa an toàn thông tin có thể giúp phân tích luồng dữ liệu và ưu tiên các cảnh báo phù hợp nhất. Có thể sử dụng các công cụ phân tích và điều tra số như Phân tích hành vi người dùng và sự kiện để giúp phát hiện, phân tích và cảnh báo cho nhóm bảo mật về bất kỳ mối đe dọa nội bộ tiềm ẩn nào. Phân tích hành vi của người dùng có thể thiết lập đường cơ sở cho hoạt động truy cập dữ liệu bình thường, trong khi giám sát hoạt động cơ sở dữ liệu có thể giúp xác định các vi phạm chính sách.

## CHƯƠNG 3: THỰC NGHIỆM VÀ ĐÁNH GIÁ

### 3.1 Xây dựng mô hình thử nghiệm

- Tải và cài đặt máy ảo Eve-Ng trên Vmware
- Màn hình sau khi đăng nhập vào eve với user : **root** và password : **eve**

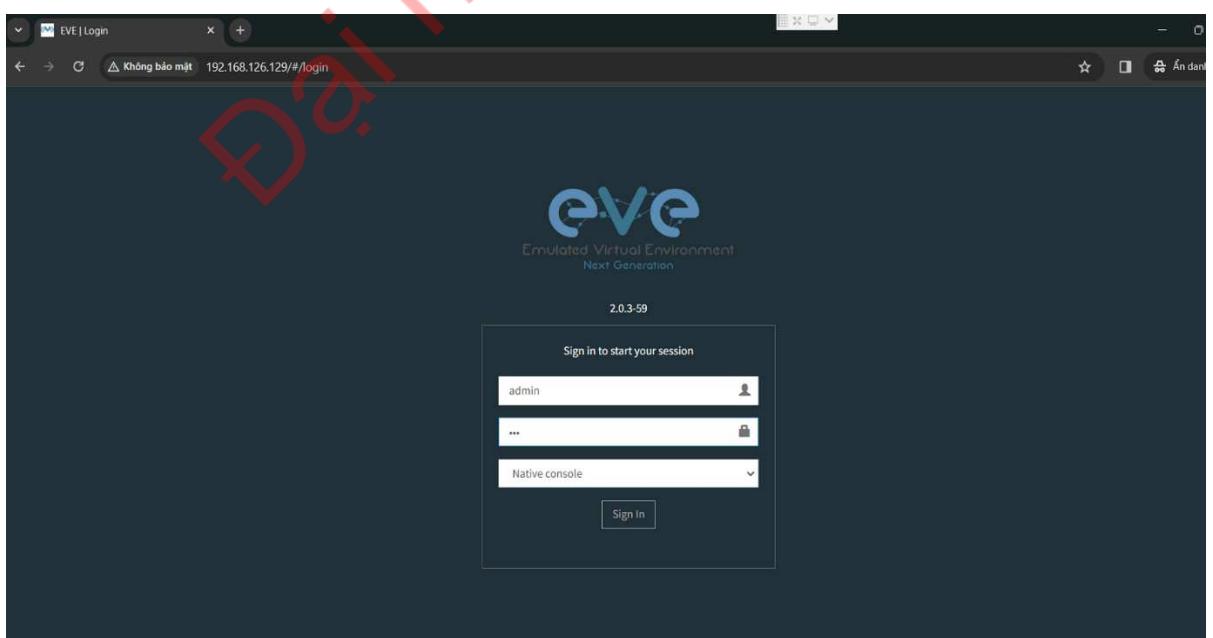


```
Eve-NG (default root password is 'eve')
Use http://192.168.126.129/
WARNING: neither Intel VT-x or AMD-V found
eve-ng login: root
Password:
Last login: Thu Oct 22 05:36:37 EEST 2020 on tty1
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.14-eve-ng-ukms+ x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage
root@eve-ng:~#
```

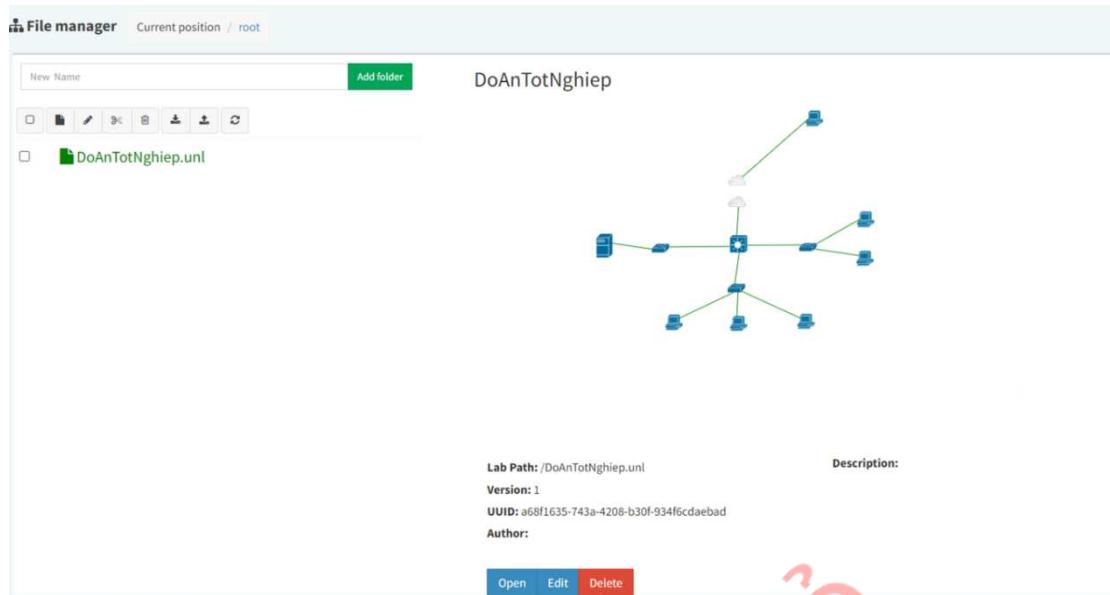
Hình 3.1 : Cài đặt Eve-ng trên VMware  
Truy cập [http://IP\\_Eve/](http://IP_Eve/) bằng trình duyệt để đăng nhập vào eve bằng

Username : **admin** và password : **eve**.



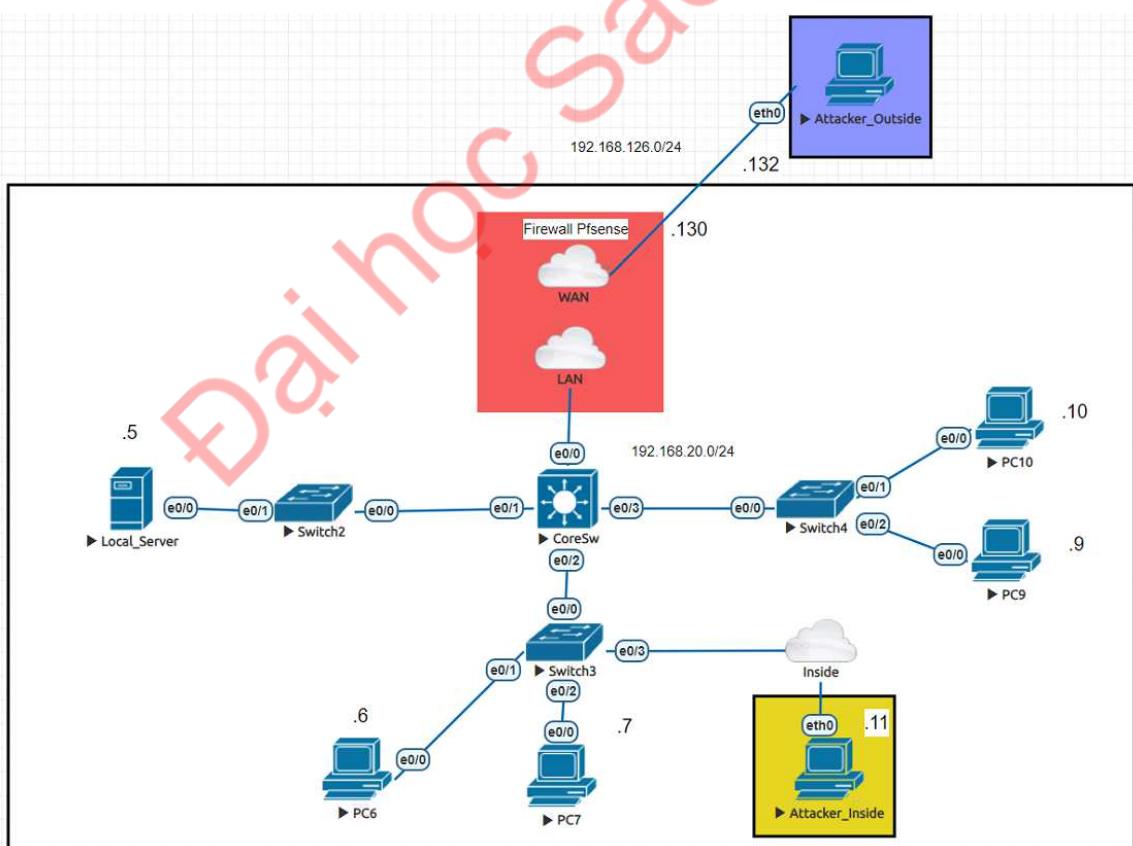
Hình 3.2 : Đăng nhập tài khoản sử dụng Eve-ng

- Sau khi đăng nhập vào Eve, import file Lab đã dựng sẵn:



Hình 3.3 : Import sơ đồ lab đã tạo

Mô hình mạng được sử dụng trong demo:



Hình 3.4 : Mô hình thử nghiệm

### **3.2 Kịch bản thử nghiệm**

Tấn công nội bộ theo 2 kịch bản:

- ✓ MAC-Overflow: Máy attacker sẽ nắm cùng mạng nội bộ với máy nạn nhân sau đó thực hiện tấn công DDoS thiết bị Switch dẫn đến Switch bị sập nguồn, reset ảnh hưởng đến hệ thống mạng.
- ✓ ARP- Poisoning: Kẻ tấn công sẽ giả mạo và từ đó đánh cắp thông tin dữ liệu trong nội bộ khi các PC nạn nhân giao tiếp trong mạng nội bộ.

Tấn công vào hệ thống từ bên ngoài internet:

- ✓ Scanning: Scanning là quá trình kiểm tra một hệ thống mạng để xác định các cổng mạng mở, dịch vụ đang chạy và một số thông tin hệ thống khác. Scanning có thể thực hiện để phát hiện lỗ hổng bảo mật hoặc để lập bản đồ cấu trúc mạng từ bên ngoài internet.

### **3.3 Tiến hành tấn công và phòng thủ trên mô hình thử nghiệm**

#### **3.3.1 Kỹ thuật tấn công MAC-Overflow**

##### **1. Khái niệm địa chỉ MAC**

Địa chỉ MAC( Media Access Control): là kiểu địa chỉ vật lý, đặc trưng cho một thiết bị hay một nhóm các thiết bị trong LAN. Thường được dùng để nhận diện các thiết bị giúp cho các gói tin lớp 2 có thể đến đúng đích cần đến.

##### **2. Cấu trúc địa chỉ IP và MAC**

Một địa chỉ MAC bao gồm 6 byte và thường được viết dưới dạng hexa, mỗi thiết bị(card mạng, modem, router...) được nhà sản xuất (NSX) chỉ định và được gắn sẵn một địa chỉ nhất định , thường là 2 dạng : MM:MM:MM:SS:SS:SS (cách nhau bởi dấu :) hay MM-MM-MM-SS-SS-SS (cách nhau bởi dấu -).

Địa chỉ MAC được phân làm 3 loại:

- **Unicast:** là loại địa chỉ dùng để đại diện một thiết bị duy nhất.
- **Multicast:** là loại địa chỉ đại diện một nhóm các thiết bị trong LAN. Thường được dùng trong trường hợp có một ứng dụng muốn trao đổi với một nhóm thiết bị. Bằng cách là gửi đi một bản tin có địa chỉ multicast thì tất cả các thiết bị trong nhóm đều nhận và xử lí gói tin trong khi các thiết bị còn lại trong mạng

sẽ bỏ qua. Giao thức IP cũng hỗ trợ truyền multicast. Khi một gói tin IP multicast được truyền qua một LAN.

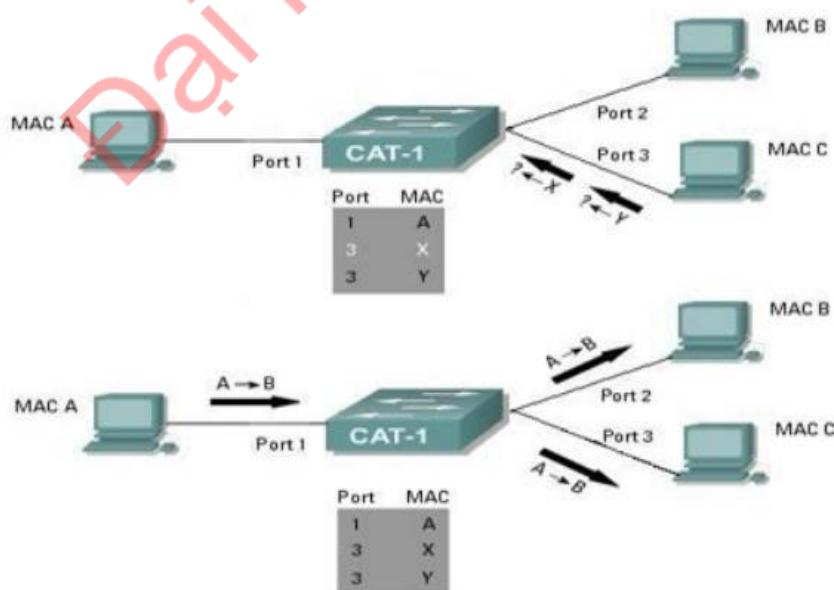
- **Broadcast:** là địa chỉ đại diện cho tất cả các thiết bị trong cùng LAN.

### 3. Tấn công làm tràn bảng MAC

Tấn công theo nguyên lý như sau:

Tấn công làm tràn bảng MAC dựa vào điểm yếu của thiết bị chuyển mạch cụ thể là thiết bị Switch: bảng MAC chỉ chứa được một số hữu hạn các ánh xạ(như switch Catalyst 6000 có thể chứa tối đa là 128000 ánh xạ) và các ánh xạ này không phải tồn tại mãi trong bảng MAC [4]. Sau một khoảng thời gian nào đó thường là 300 s nếu địa chỉ này không được dùng trong việc trao đổi thông tin thì nó sẽ bị gỡ bỏ. Khi bảng MAC được điền đầy, tất cả thông tin đến sẽ được gửi đến tất cả các cổng của nó trừ cổng nó nhận được do đó lúc này chức năng của switch không khác gì chức năng của một hub.

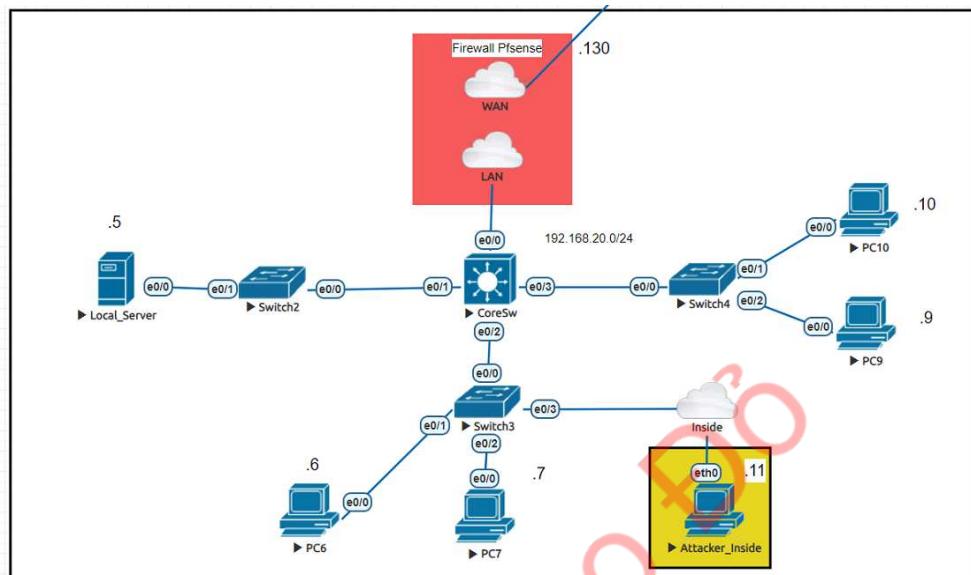
Hình minh họa dưới ta thấy host C của attacker gửi liên tục hàng loạt các bản tin có địa chỉ MAC giả mạo là host X và host Y. Từ đó switch sẽ cập nhật địa chỉ của các host giả mạo này vào bảng MAC. Kết quả là từ host A gửi tin đến cho host B thì địa chỉ của B không tồn tại trong bảng nên gói tin được switch gửi ra các cổng của nó và bản tin A chỉ gửi riêng cho B cũng sẽ được chuyển qua C.



Hình 3.5: Minh họa bảng MAC

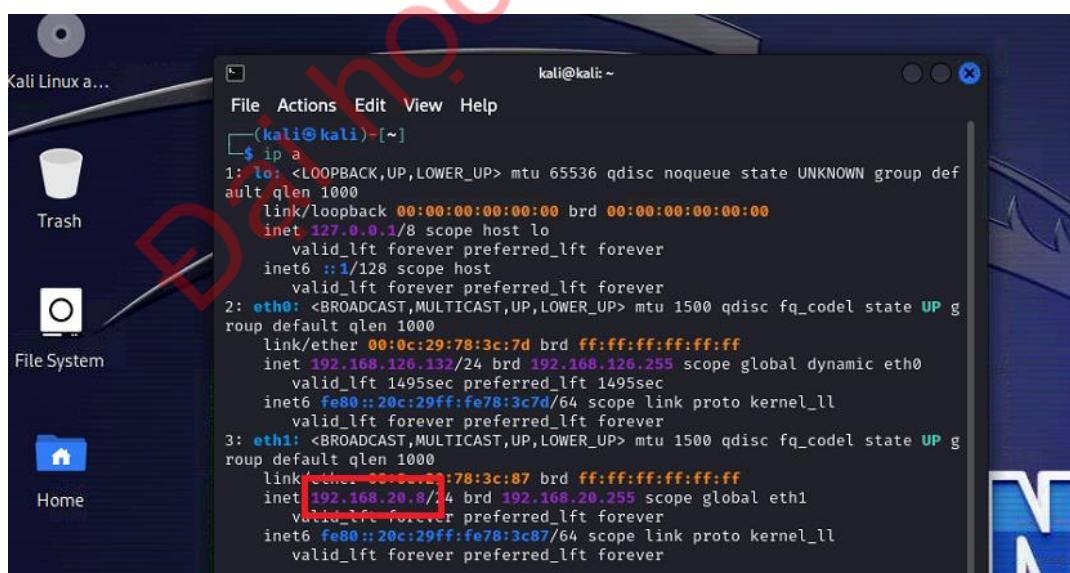
#### 4. Mô phỏng tấn công MAC-Overflow

Kẻ tấn công đang ẩn nấp bên trong sau khi thành công trong việc chiếm quyền hoặc mua chuộc nhân viên để thực hiện nhiệm vụ gián điệp. Từ vị trí nội bộ, họ tiến hành tấn công trực tiếp từ bên trong khu vực "inside".



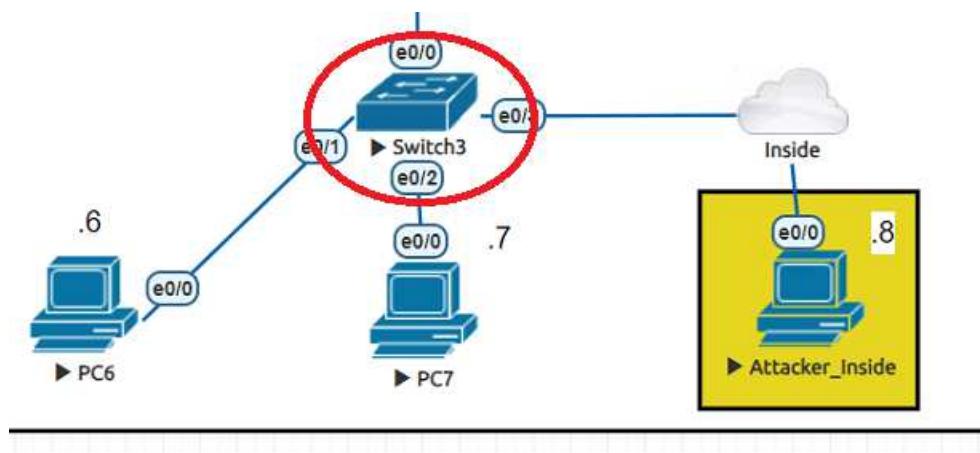
Hình 3.6 : Sơ đồ tổng quan kịch bản MAC Overflow trên Eve-ng

Mở máy ảo Kali linux, địa chỉ IP của máy Kali linux là 192.168.20.8:



Hình 3.7 : Mở máy ảo Kali linux

Mục tiêu của cuộc tấn công là nhầm vào kích thước bảng MAC của thiết bị switch3, với các tác động sau:



- Tấn công bằng cách liên tục gửi địa chỉ MAC giả mạo có thể làm treo switch.
- Gây tấn công từ chối dịch vụ (DoS) trực tiếp lên switch.
- Bảng MAC bị lấp đầy, dẫn đến việc không có chỗ cho các địa chỉ MAC của các máy tính hợp lệ nữa. Điều này khiến switch hoạt động theo kiểu "flooding," trong đó các máy tính hợp lệ không thể được định vị đúng cổng, và dữ liệu truyền đi được chuyển đến các cổng khác mà không xác định đúng địa chỉ MAC, tạo cơ hội cho kẻ tấn công để nghe lén.

Bảng MAC của Switch 3 trước khi bị tấn công :

```

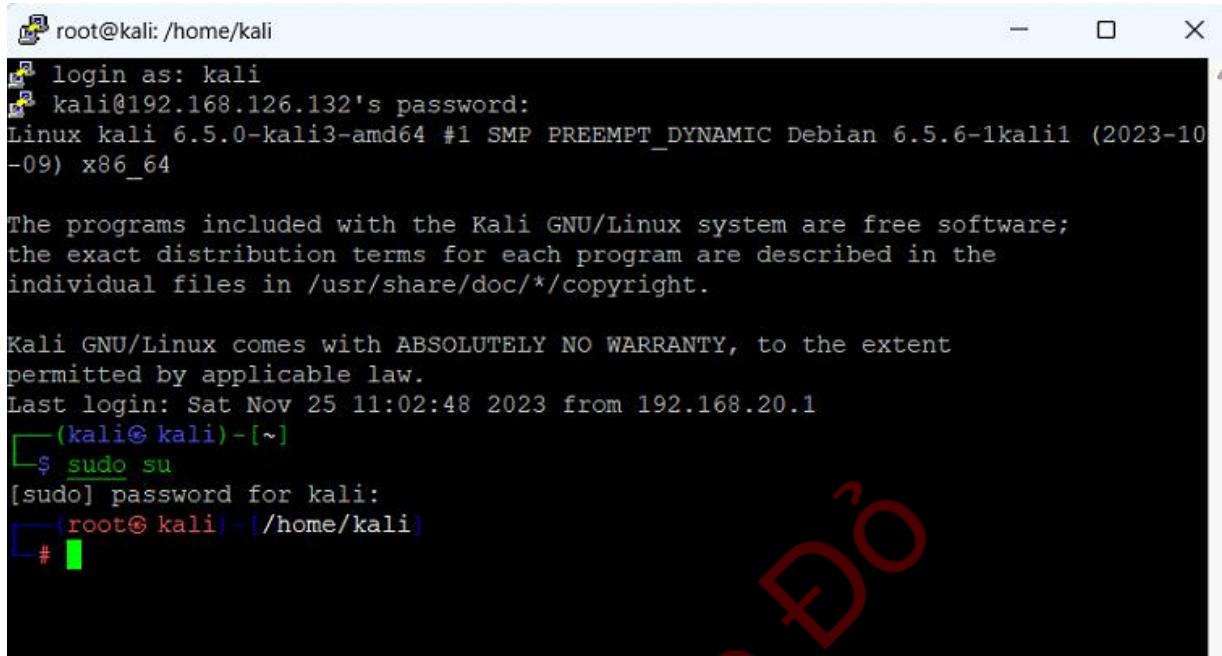
Switch>
Switch>en
Switch#show mac ad
Switch#show mac address-table
Mac Address Table
-----
Vlan    Mac Address        Type      Ports
---  -----
  1    000c.2978.3c87  DYNAMIC   Et0/3
  1    0050.56c0.0002  DYNAMIC   Et0/3
  1    aabb.cc00.1000  DYNAMIC   Et0/3
  1    aabb.cc00.2000  DYNAMIC   Et0/3
  1    aabb.cc00.3000  DYNAMIC   Et0/3
  1    aabb.cc00.4000  DYNAMIC   Et0/3
  1    aabb.cc00.5000  DYNAMIC   Et0/1
  1    aabb.cc00.6000  DYNAMIC   Et0/2
  1    aabb.cc00.7000  DYNAMIC   Et0/3
  1    aabb.cc00.a000  DYNAMIC   Et0/3
Total Mac Addresses for this criterion: 10
Switch#
Switch#
Switch#
Switch#

```

Hình 3.8 : Hiển thị bảng MAC thiết bị Switch3 ban đầu

Truy cập terminal máy Kali:

- ✓ Mở terminal Kali:



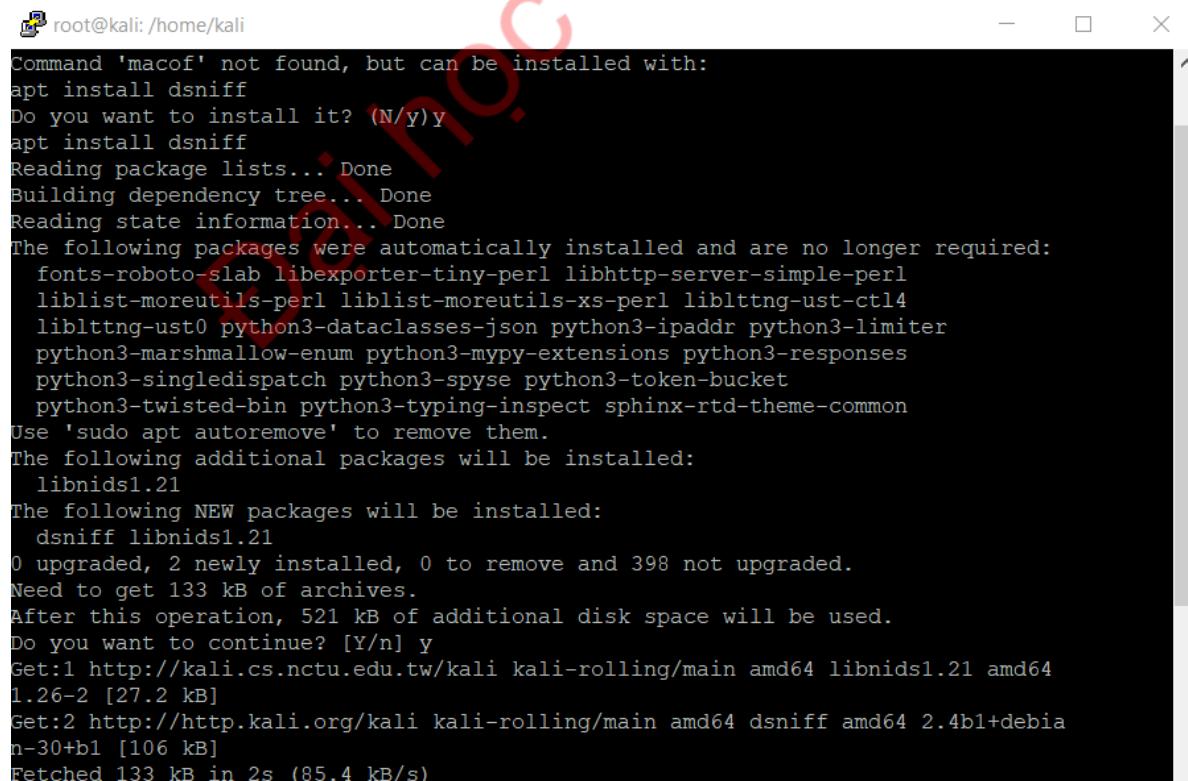
```
root@kali: /home/kali
login as: kali
kali@192.168.126.132's password:
Linux kali 6.5.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (2023-10-09) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Nov 25 11:02:48 2023 from 192.168.20.1
[kali㉿ kali) ~]
$ sudo su
[sudo] password for kali:
[root@kali ~] /home/kali
#
```

Hình 3.9: Mở terminal máy kali linux

- ✓ Cài đặt gói dnsiff



```
root@kali: /home/kali
Command 'macof' not found, but can be installed with:
apt install dsniff
Do you want to install it? (N/y)y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  fonts-roboto-slab libexporter-tiny-perl libhttp-server-simple-perl
  liblist-moreutils-perl liblist-moreutils-xs-perl liblttng-ust-ctl14
  liblttng-ust0 python3-dataclasses-json python3-ipaddr python3-limiter
  python3-marshmallow-enum python3-mypy-extensions python3-responses
  python3-singledispatch python3-spyse python3-token-bucket
  python3-twisted-bin python3-typing-inspect sphinx-rtd-theme-common
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libnids1.21
The following NEW packages will be installed:
  dnsiff libnids1.21
0 upgraded, 2 newly installed, 0 to remove and 398 not upgraded.
Need to get 133 kB of archives.
After this operation, 521 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 libnids1.21 amd64 1.26-2 [27.2 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 dnsiff amd64 2.4b1+debian-30+b1 [106 kB]
Fetched 133 kB in 2s (85.4 kB/s)
```

Hình 3.10: Cài đặt gói dnsiff

- Sử dụng câu lệnh macof –i eth1

```
root@kali: /home/kali
# macof -i eth1
```

Hình 3.11: Sử dụng lệnh DoS thiết bị Switch3

Xuất hiện các MAC giả mạo được Kali gửi liên tục :

```
root@kali: /home/kali
1949698980(0) win 512
f0:da:b6:7d:58:f0 ce:b6:cf:38:bf:ce 0.0.0.0.27931 > 0.0.0.0.23779: s 194359038:1
94359038(0) win 512
66:2:67:6b:cf:e8 f1:34:79:4e:6d:f3 0.0.0.0.10595 > 0.0.0.0.30115: s 781296239:78
1296239(0) win 512
5c:a3:16:58:b5:9f 1c:d4:3b:16:f2:8c 0.0.0.0.54390 > 0.0.0.0.45936: s 643640660:6
43640660(0) win 512
25:41:2b:34:58:2c d1:a7:d9:1c:ef:64 0.0.0.0.47771 > 0.0.0.0.59443: s 828011068:8
28011068(0) win 512
f4:e8:97:7a:64:91 19:ed:e6:70:f6:66 0.0.0.0.48085 > 0.0.0.0.11829: s 183335171:1
83335171(0) win 512
f5:c4:9b:28:63:7f b9:77:d3:34:e8:d7 0.0.0.0.46220 > 0.0.0.0.57549: s 1559758970:1
1559758970(0) win 512
8d:38:92:7c:c2:5a e:7f:88:35:c9:f9 0.0.0.0.49278 > 0.0.0.0.64077: s 2003869810:2
003869810(0) win 512
33:ef:4a:0:6e:fb 69:53:10:22:7e:4d 0.0.0.0.23499 > 0.0.0.0.40507: s 712113679:71
2113679(0) win 512
f4:4f:1e:5b:13:16 1d:85:1:5a:9e:d7 0.0.0.0.35232 > 0.0.0.0.8840: s 1196459249:11
96459249(0) win 512
55:1c:71:e:61:1 7a:a6:5a:23:5c:df 0.0.0.0.36619 > 0.0.0.0.15274: s 1524803826:15
24803826(0) win 512
2d:e9:91:36:52:f3 64:a1:f8:0:39:95 0.0.0.0.36741 > 0.0.0.0.40091: s 803566359:80
3566359(0) win 512
```

Hình 3.12 : Máy attacker gửi liên tục các địa chỉ MAC giả mạo

Bên Switch3 ta chạy lại câu lệnh show mac address-table để xem MAC address từ các cổng:

Vlan	Mac Address	Type	Ports
1	000b.502c.8b0f	DYNAMIC	Et0/3
1	0012.bd31.80b7	DYNAMIC	Et0/3
1	0015.e800.02e9	DYNAMIC	Et0/3
1	001c.4d06.5af7	DYNAMIC	Et0/3
1	001c.7232.7755	DYNAMIC	Et0/3
1	001f.1660.4a00	DYNAMIC	Et0/3
1	0022.0d2f.dad9	DYNAMIC	Et0/3
1	0024.fb3b.042f	DYNAMIC	Et0/3
1	0025.7c08.978c	DYNAMIC	Et0/3
1	0027.e462.bdc0	DYNAMIC	Et0/3
1	002c.1e02.887c	DYNAMIC	Et0/3
1	0032.5118.527d	DYNAMIC	Et0/3
1	0036.a73f.495a	DYNAMIC	Et0/3
1	003f.6723.8d5e	DYNAMIC	Et0/3
1	0041.7677.b014	DYNAMIC	Et0/3
1	0047.6173.d887	DYNAMIC	Et0/3
1	0048.6c78.a16a	DYNAMIC	Et0/3
1	0050.56c0.0002	DYNAMIC	Et0/3
1	0050.b159.2b68	DYNAMIC	Et0/3
1	0056.cb7f.27c0	DYNAMIC	Et0/3
1	005a.d110.9511	DYNAMIC	Et0/3
1	0066.0842.08ef	DYNAMIC	Et0/3
1	0066.9d02.75ae	DYNAMIC	Et0/3
1	0069.2418.11ad	DYNAMIC	Et0/3
1	0069.d367.0e92	DYNAMIC	Et0/3
1	006d.de57.cf40	DYNAMIC	Et0/3
1	0078.9073.bcf9	DYNAMIC	Et0/3
1	007f.616d.e950	DYNAMIC	Et0/3
1	0085.e61c.8ce9	DYNAMIC	Et0/3

Hình 3.13 : Hiển thị bảng MAC trên Switch3 sau khi bị tấn công Ddos

Ta thấy xuất hiện rất nhiều MAC giả mạo traffic từ cổng E0/3.

Sử dụng câu lệnh clear để xoá các MAC giả mạo

```
Switch#clear mac address-table dynamic
Switch#show mac address-table
      Mac Address Table
-----
Vlan      Mac Address          Type      Ports
----      -----
  1      0050.56c0.0002        DYNAMIC   Et0/3
Total Mac Addresses for this criterion: 1
Switch#
Switch#
Switch#
```

Hình 3.14 : Clear bảng MAC trên Switch3

## 5. Giải pháp phòng vệ

Giải pháp ta cấu hình port security bằng các câu lệnh sau cho Switch3 :  
*interface e0/3*

```
switchport mode access  
switchport port-security  
switchport port-security maximum 12  
switchport port-security mac-address sticky  
switchport port-security violation shutdown
```

Giải pháp port security trên một cổng này chúng ta chỉ cho 1 số lượng MAC nhất định nào đó để kết nối vào và nếu có nhiều mac gửi kết nối vào sẽ shutdown cổng:

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface e0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 12
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#exit
Switch(config)#
Switch(config)#
Switch(config)#
```

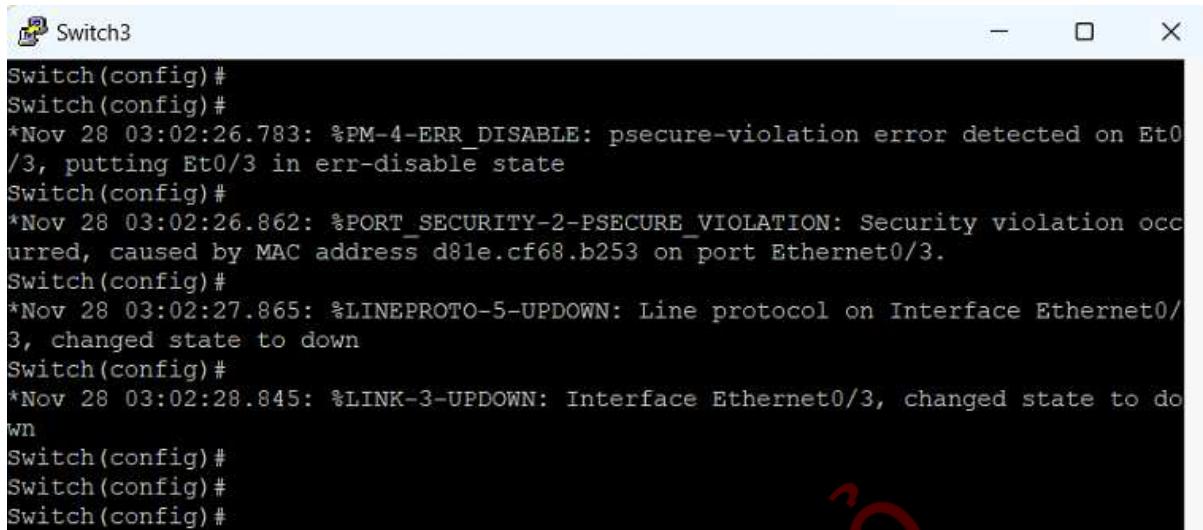
Hình 3.15 : Cấu hình port security trên SW14

Sau đó bên kali ta gửi lại MAC địa chỉ giả mạo lần nữa :

```
root@kali: /home/kali
81775664(0) win 512
db:42:82:5a:55:59 be:2e:ae:2f:24:eb 0.0.0.0.26335 > 0.0.0.0.15157: s 1531338279:
1531338279(0) win 512
14:68:70:10:e9:1b 9:4:31:67:9c:c2 0.0.0.0.38614 > 0.0.0.0.41067: s 858484250:858
484250(0) win 512
9d:ab:1c:d3:6a b6:35:7d:20:a5:be 0.0.0.0.34085 > 0.0.0.0.11508: s 1840700735:1
840700735(0) win 512
59:eb:5d:6:53:68 b9:a4:57:5e:23:50 0.0.0.0.54238 > 0.0.0.0.14935: s 848160554:84
8160554(0) win 512
35:1d:bf:25:3c:92 c0:ab:74:7d:2e:2e 0.0.0.0.12844 > 0.0.0.0.27567: s 1504379067:
1504379067(0) win 512
8f:46:7b:5a:20:13 41:f4:3:4a:3d:f7 0.0.0.0.42907 > 0.0.0.0.22250: s 859360056:85
9360056(0) win 512
fd:91:a8:27:f0 b3:7f:31:5b:b6:83 0.0.0.0.25145 > 0.0.0.0.37929: s 75392053:75
392053(0) win 512
6b:38:a:69:a:7:ab 80:21:ad:6c:ab:4a 0.0.0.0.33957 > 0.0.0.0.3075: s 1853546555:18
53546555(0) win 512
bd:6e:b7:70:c:0:6f 99:fc:91:75:b9:9d 0.0.0.0.28470 > 0.0.0.0.36506: s 1460749258:
1460749258(0) win 512
4:85:28:7c:82:1b 58:e:0:77:7d:11:5c 0.0.0.0.35438 > 0.0.0.0.369: s 734922359:7349
22359(0) win 512
d8:c9:89:33:bb:53 76:45:54:59:90:b 0.0.0.0.61078 > 0.0.0.0.41739: s 1256110533:1
256110533(0) win 512
```

Hình 3.16 : Từ máy attacker tấn công lại lần 2

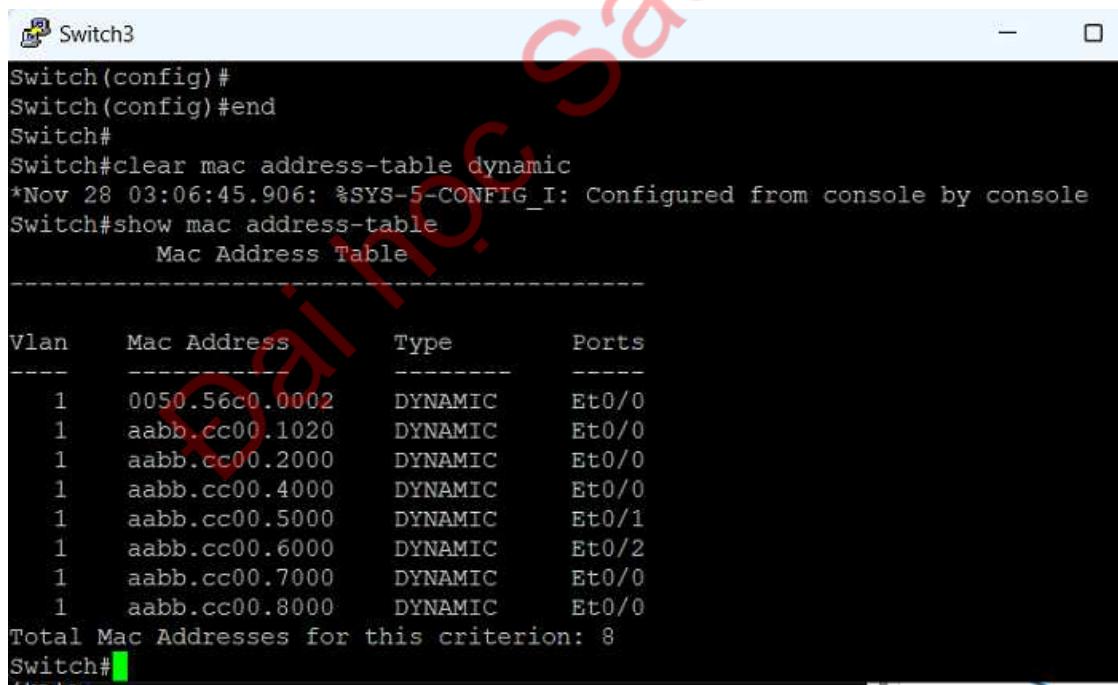
Sau đó kiểm tra thấy cổng Ether0/3 của Switch3 đã shutdown sau khi xuất hiện thông báo bật tính năng port security:



```
Switch(config)#
Switch(config)#
*Nov 28 03:02:26.783: %PM-4-ERR_DISABLE: psecure-violation error detected on Et0/3, putting Et0/3 in err-disable state
Switch(config)#
*Nov 28 03:02:26.862: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address d81e.cf68.b253 on port Ethernet0/3.
Switch(config)#
*Nov 28 03:02:27.865: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3, changed state to down
Switch(config)#
*Nov 28 03:02:28.845: %LINK-3-UPDOWN: Interface Ethernet0/3, changed state to down
Switch(config)#
Switch(config)#
Switch(config)#
```

Hình 3.17 : Cổng Ether0/3 của Switch3 tự động ngắt khi thấy dấu hiệu attack

Kiểm tra lại địa chỉ MAC thấy không có thay đổi bất thường.



```
Switch(config)#
Switch(config)#end
Switch#
Switch#clear mac address-table dynamic
*Nov 28 03:06:45.906: %SYS-5-CONFIG_I: Configured from console by console
Switch#show mac address-table
      Mac Address Table
-----
Vlan     Mac Address           Type      Ports
----     -----
  1      0050.56c0.0002    DYNAMIC   Et0/0
  1      aabb.cc00.1020    DYNAMIC   Et0/0
  1      aabb.cc00.2000    DYNAMIC   Et0/0
  1      aabb.cc00.4000    DYNAMIC   Et0/0
  1      aabb.cc00.5000    DYNAMIC   Et0/1
  1      aabb.cc00.6000    DYNAMIC   Et0/2
  1      aabb.cc00.7000    DYNAMIC   Et0/0
  1      aabb.cc00.8000    DYNAMIC   Et0/0
Total Mac Addresses for this criterion: 8
Switch#
```

Hình 3.18 : Kiểm tra lại bảng MAC của thiết bị Switch3 thấy bình thường

**Kiểu tấn công này có 2 hậu quả :**

Vì lượng traffic quá lớn, bảng MAC trên switch bị đầy, gây tốn kém ô nhớ RAM và dẫn đến hiện tượng treo switch. Hiện tượng này có thể xuất hiện trên cả hệ

thống cũ, được báo hiệu bằng việc đèn trên switch nhấp nháy liên tục và cuối cùng switch sẽ tự khởi động lại do cạn kiệt tài nguyên.

Với số lượng MAC address nhiều, nhiều máy tính hợp lệ kết nối với nhau, khi trao đổi dữ liệu, switch sẽ thực hiện flooding, làm gia tăng áp lực trên mạng và tăng cường tình trạng quay tải.

### 3.3.2 Kỹ thuật tấn công ARP-Poisoning

#### 1. Lỗ hổng của ARP

ARP (viết tắt của Address Resolution Protocol) là một giao thức truyền thông được sử dụng phổ biến để tìm ra các địa chỉ tầng liên kết dữ liệu từ các địa chỉ mạng.

Khi đó một gói tin được gửi từ một máy đến máy khác trong mạng cục bộ thì địa chỉ IP đích phải được giải quyết thành địa chỉ MAC ~~đến~~ truyền qua tầng liên kết dữ liệu. Sau đó khi biết được địa chỉ IP của máy đích và địa chỉ MAC của nó mà cần truy cập, một gói tin là broadcast được gửi đi trên mạng nội bộ. Gói này được gọi là ARP request. Máy destination với IP trong ARP request sẽ trả lời với thông tin ARP reply, nó chứa một địa chỉ MAC cho IP đó ARP là một giao thức phi trạng thái.

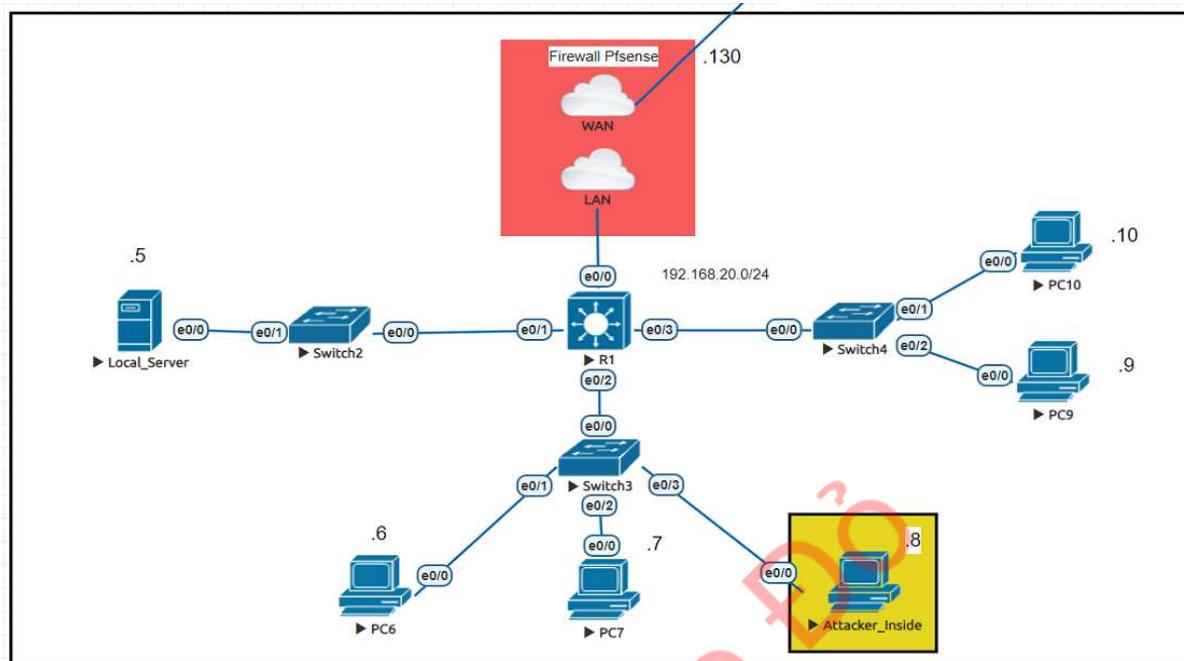
Máy chủ trong mạng sẽ tự động lưu trữ bất kỳ ARP reply nào mà chúng có thể nhận được, bất kể máy khác có yêu cầu hay không. Và ngay cả các ARP chưa hết hạn sẽ bị đè khi nhận được gói tin ARP mà reply mới. Do đó không có phương pháp nào trong giao thức ARP mà giúp một máy có thể xác nhận máy mà từ đó gói tin bắt nguồn. Cơ chế hoạt động này chính là lỗ hổng cho phép ARP spoofing xảy ra.

#### 2. Mô phỏng tấn công ARP-Poisoning

Trong hệ thống mạng, ARP spoofing hay ARP poisoning, ARP poisoning routing là một kỹ thuật thông qua đó kẻ tấn công giả mạo thông điệp ARP trong mạng cục bộ. Mục tiêu sẽ là kết hợp địa chỉ MAC của kẻ tấn công cùng với địa chỉ IP của máy khác, như cổng mặc định(default gateway) làm cho bất kỳ lưu lượng truy cập nào dành cho địa chỉ IP đó được gửi đến kẻ tấn công ARP spoofing.

Qua đó cho phép kẻ tấn công chặn các khung dữ liệu trên mạng, sửa đổi lưu lượng, hoặc dừng tất cả lưu lượng. Thông thường cuộc tấn công này được sử dụng như là một sự mở đầu cho các cuộc tấn công khác, chẳng hạn như tấn công từ chối dịch vụ,

tấn công Man-in-the-middle attack( nghe lén) hoặc các cuộc tấn công đánh cắp dữ liệu. Cuộc tấn công này chỉ giới hạn trong mạng cục bộ.[4]



Hình 3.19 Sơ đồ bài lab tấn công ARP-Poisoning

Theo sơ đồ trên mục tiêu tấn công là 2 thiết bị là PC-7, Local-Server. Bây giờ ta thực hiện tấn công từ máy Kali với kỹ thuật ARP-Poisoning sử dụng công cụ Ettercap:



Hình 3.20 : Mở công cụ Ettercap trên máy Kali linux

Sau đó thực hiện Scan các host có trong hệ thống:



Hình 3.21 : Thực hiện Scan hosts

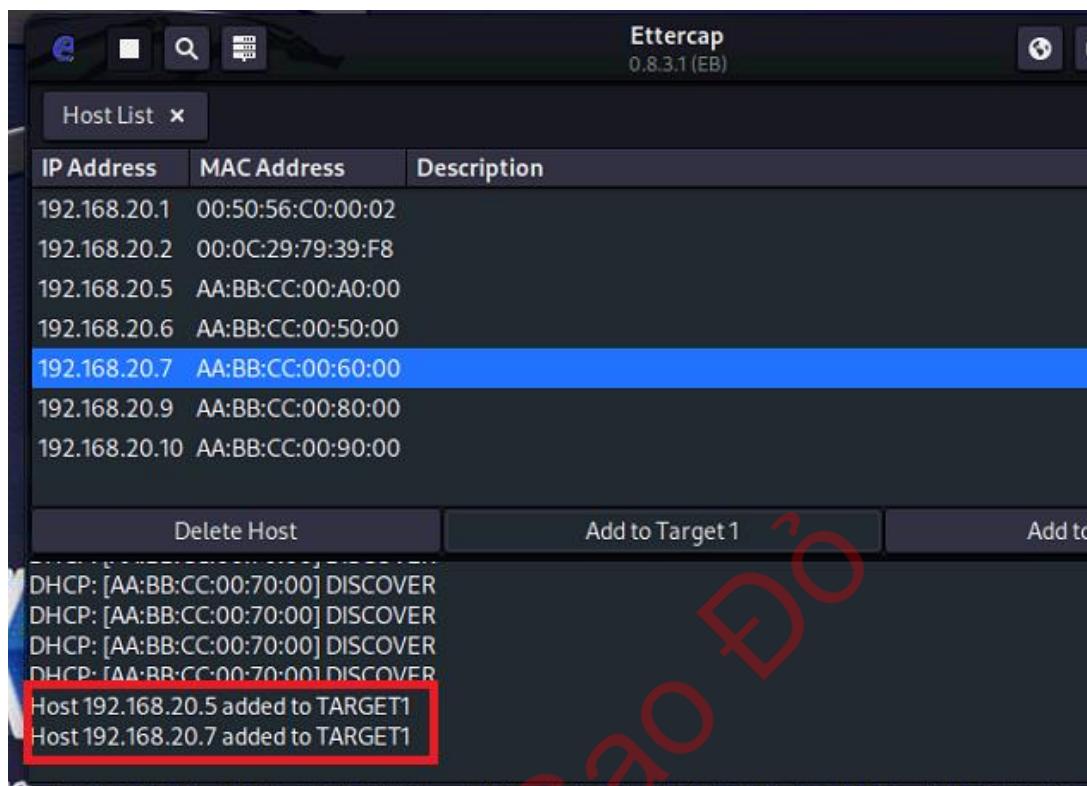
Sau khi thực hiện Scan máy attacker có được tất cả thông tin của các thiết bị trong hệ thống nội bộ:

IP Address	MAC Address	Description
192.168.20.1	00:50:56:C0:00:02	
192.168.20.2	00:0C:29:79:39:F8	
192.168.20.5	AA:BB:CC:00:A0:00	
192.168.20.6	AA:BB:CC:00:50:00	
192.168.20.7	AA:BB:CC:00:60:00	
192.168.20.9	AA:BB:CC:00:80:00	
192.168.20.10	AA:BB:CC:00:90:00	

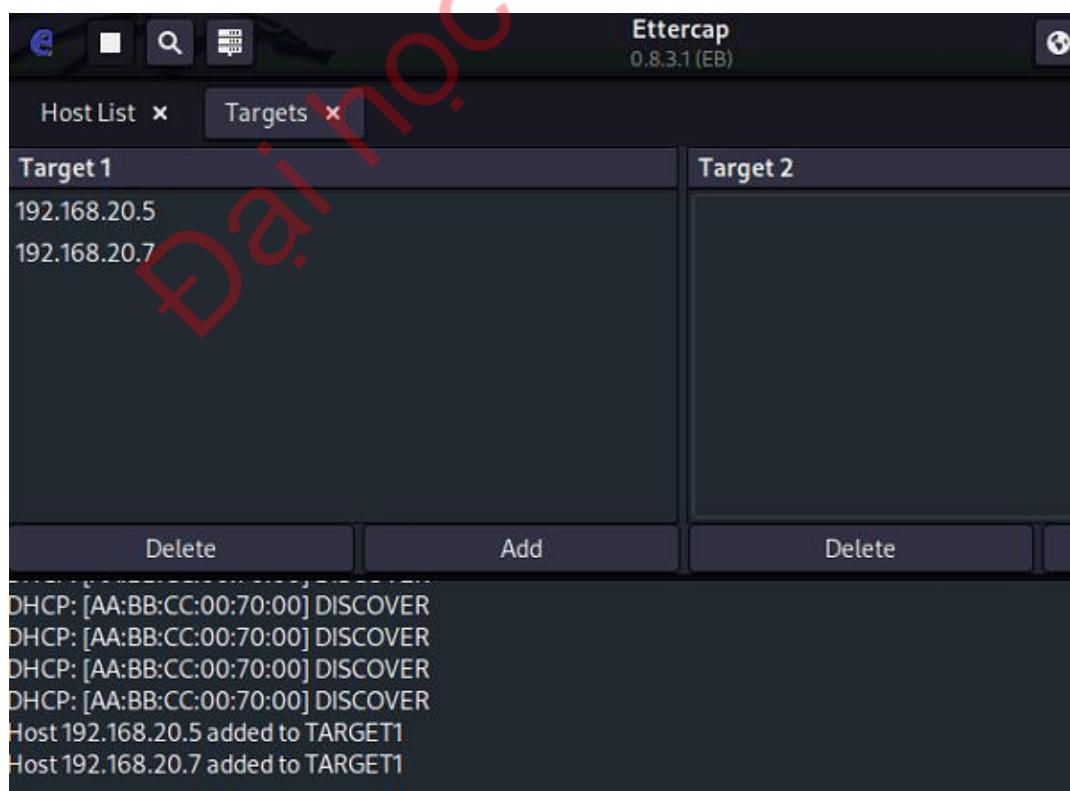
Below the table, there are buttons: "Delete Host", "Add to Target 1", and "Add to Target 2". The terminal window at the bottom shows repeated "DHCP: [AA:BB:CC:00:70:00] DISCOVER" messages.

Hình 3.22 : Kiểm tra thông tin các máy đã dò được

Tiếp theo chọn 2 thiết bị mục tiêu tấn công là Local-Server có IP là 192.168.20.5 và PC7 có IP là 192.168.20.7:

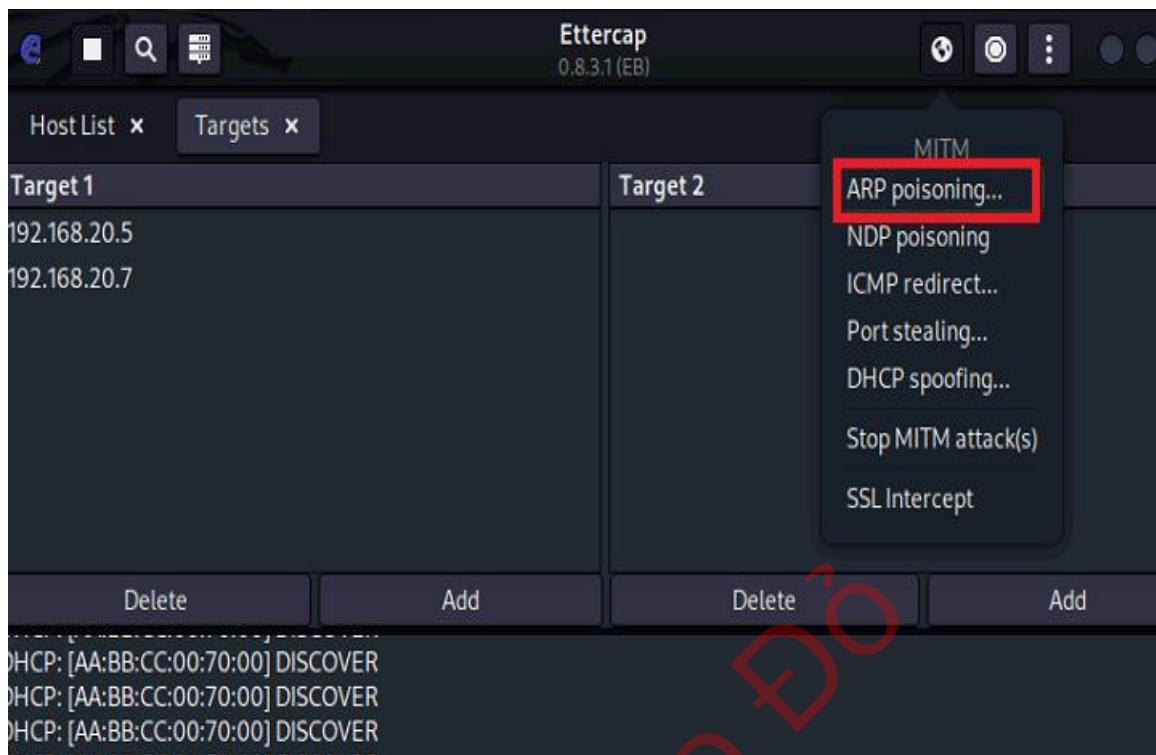


Hình 3.23 : Kiểm tra thông tin các máy đã dò được



Hình 3.24 Trên máy attacker add 2 mục tiêu PC2 và Local Server3

Tiếp theo chọn phương thức tấn công ARP- Poisoning:



Hình 3.25 : Thực hiện phương thức tấn công ARP Poisoning

Sau khi thực hiện tấn công, ta xem thông tin arp của 2 thiết bị nạn nhân đều thấy các thiết bị cùng 1 địa chỉ MAC, ở đây chính là địa chỉ MAC của máy Kali:

```
LocalServer>
LocalServer>
LocalServer>en
Password:
LocalServer#show arp
Protocol Address          Age (min) Hardware Addr Type Interface
Internet 192.168.20.1      0 000c.2978.3c87 ARPA Ethernet0/0
Internet 192.168.20.2      0 000c.2978.3c87 ARPA Ethernet0/0
Internet 192.168.20.5      - aabb.cc00.a000 ARPA Ethernet0/0
Internet 192.168.20.6      0 000c.2978.3c87 ARPA Ethernet0/0
Internet 192.168.20.7      0 000c.2978.3c87 ARPA Ethernet0/0
Internet 192.168.20.8      1 000c.2978.3c87 ARPA Ethernet0/0
Internet 192.168.20.9      0 000c.2978.3c87 ARPA Ethernet0/0
Internet 192.168.20.10     0 000c.2978.3c87 ARPA Ethernet0/0
LocalServer#
```

Hình 3.26 : Kiểm tra bảng MAC của thiết bị Local-Server

```
PC7>
PC7>en
PC7#show arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.20.1 0 000c.2978.3c87 ARPA Ethernet0/0
Internet 192.168.20.2 0 000c.2978.3c87 ARPA Ethernet0/0
Internet 192.168.20.5 0 000c.2978.3c87 ARPA Ethernet0/0
Internet 192.168.20.6 0 000c.2978.3c87 ARPA Ethernet0/0
Internet 192.168.20.7 - aabb.cc00.6000 ARPA Ethernet0/0
Internet 192.168.20.8 1 000c.2978.3c87 ARPA Ethernet0/0
Internet 192.168.20.9 0 000c.2978.3c87 ARPA Ethernet0/0
Internet 192.168.20.10 0 000c.2978.3c87 ARPA Ethernet0/0
PC7#
```

Hình 3.27 Kiểm tra bảng MAC của thiết bị PC7

Sau đó thực hiện máy PC-7 telnet đến máy Local-Server:

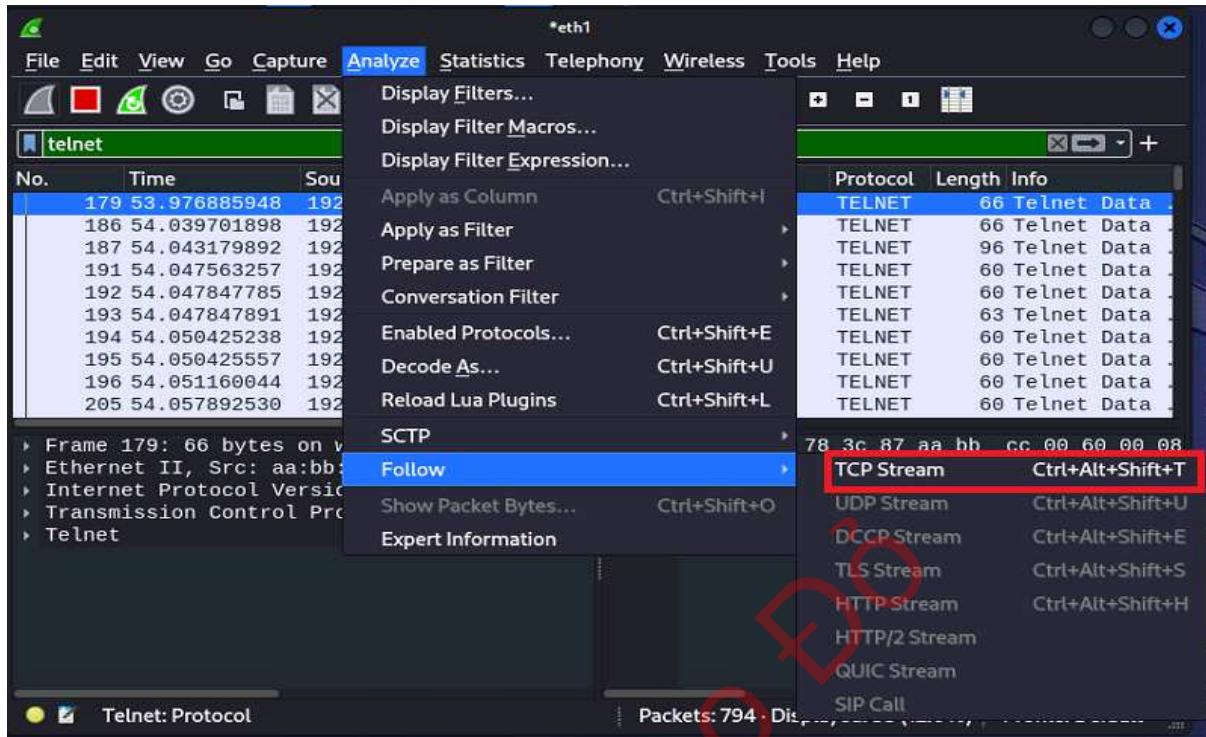
```
PC7>
PC7#telnet 192.168.20.5
Trying 192.168.20.5 ... Open

User Access Verification

Username: admin
Password:
LocalServer>en
Password:
LocalServer#conf t
Enter configuration commands, one per line. End with CNTL/Z.
LocalServer(config)#
LocalServer(config)#
LocalServer(config)#
```

Hình 3.28 Thực hiện từ máy PC-7 telnet đến máy Local-Server

Từ đây máy kali có thể thực hiện nghe lén tài khoản và mật khẩu sử dụng công cụ Wireshark:



Hình 3.29 Máy attacker sử dụng công cụ Wireshark để nghe lén

Ta có thể thấy hiện tài khoản và mật khẩu để telnet đến Local-Server, cũng như các thao tác câu lệnh của máy PC7:

```
Wireshark - Follow TCP Stream (tcp.stream eq 0) - eth1
.... . . . . !
User Access Verification
Username: . . . . . P . . . . . ! . . . . . aaddmmiinn
Password: password
LocalServer>eenn
Password: co....cisco
LocalServer#ccoonnff tt
Enter configuration commands, one per line. End with CNTL/Z.
LocalServer(config)#
LocalServer(config)#
LocalServer(config)#
Packet 439. 50 client pkts, 45 server pkts, 61 turns. Click to select.
Entire conversation (507 bytes) Show data as ASCII Stream 0
```

Hình 3.30 Attacker dò được tài khoản telnet

Sau khi có được thông tin máy attacker hoàn toàn có thể truy cập đột nhập vào Server:

```
root@kali: /home/kali
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(root㉿kali)-[/home/kali]
# telnet 192.168.20.5
Trying 192.168.20.5 ...
Connected to 192.168.20.5.
Escape character is '^]'.

User Access Verification

Username: admin
Password:
LocalServer>enable
Password:
LocalServer#conf t
Enter configuration commands, one per line. End with CNTL/Z.
LocalServer(config)#
```

Hình 3.31 Attacker đột nhập vào Local Server

### 3. Giải pháp phòng vệ

Giải pháp được áp dụng ở đây là sử dụng tính năng IP snooping trên Switch3, với mục đích chặn các gói ARP giả mạo được gửi từ kẻ tấn công. Dưới đây là cấu hình chi tiết trên Switch3:

```
interface e0/3
ip arp inspection limit rate 2048
exit
ip dhcp snooping
ip dhcp snooping vlan 1
ip arp inspection vlan 1
arp access-list host192
permit ip host 192.168.20.2 mac host 000c.2979.39f8
permit ip host 192.168.20.5 mac host aabb.cc00.a000
permit ip host 192.168.20.6 mac host aabb.cc00.5000
permit ip host 192.168.20.7 mac host aabb.cc00.6000
permit ip host 192.168.20.9 mac host aabb.cc00.8000
permit ip host 192.168.20.10 mac host aabb.cc00.9000
ip arp inspection filter host192 vlan 1
show ip dhcp snooping binding
```

```
Switch#
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface e0/3
Switch(config-if)#ip arp inspection limit rate 2048
Switch(config-if)#exit
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 1
Switch(config)#ip arp inspection vlan 1
Switch(config)#arp access-list host192
Switch(config-arp-nacl)#permit ip host 192.168.20.7 mac host aabb.cc00.6000
Switch(config-arp-nacl)#ip arp inspection filter host192 vlan 1
Switch(config)#show ip dhcp snooping binding
```

Hình 3.32 Cấu hình ip snooping trên Switch3 để phòng vệ

Sau khi cấu hình máy kali thực hiện tấn công lại sẽ xuất hiện các dòng thông báo chặn gói ARP của cổng e0/3 Switch3:

```
ET Thu Nov 30 2023]
Switch(config)#
*Nov 30 08:29:23.836: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et0/3, vlan 1.([000c.2978.3c87/192.168.20.11/0000.0000/192.168.20.178/10:29:17 EET Thu Nov 30 2023])
*Nov 30 08:29:23.836: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et0/3, vlan 1.([000c.2978.3c87/192.168.20.11/0000.0000/192.168.20.195/10:29:17 EET Thu Nov 30 2023])
*Nov 30 08:29:24.841: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et0/3, vlan 1.([000c.2978.3c87/192.168.20.11/0000.0000/192.168.20.60/10:29:17 EET Thu Nov 30 2023])
*Nov 30 08:29:24.841: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et0/3, vlan 1.([000c.2978.3c87/192.168.20.11/0000.0000/192.168.20.42/10:29:17 EET Thu Nov 30 2023])
*Nov 30 08:29:24.841: %SW_DAI-4-SPECIAL_LOG_ENTRY: 228 Invalid ARP packets [10:29:18 EET Thu Nov 30 2023]
Switch(config)#
*Nov 30 08:29:26.853: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et0/3, vlan 1.([000c.2978.3c87/192.168.20.11/0000.0000/192.168.20.10/10:29:26 EET Thu Nov 30 2023])
*Nov 30 08:29:26.853: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et0/3, vlan 1.([0050.56c0.0002/192.168.20.1/0000.0000.0000/192.168.20.9/10:29:26 EET Thu Nov 30 2023])
Switch(config)#3~
```

Hình 3.33 Tấn công lại lần nữa từ máy Attacker thấy Switch3 hiện cảnh báo

Và địa chỉ MAC của 2 thiết bị PC7 và Local-SERVER không bị thay đổi

```
LocalServer>show arp
Protocol Address          Age (min)  Hardware Addr  Type  Interface
Internet 192.168.20.1      2  0050.56c0.0002  ARPA  Ethernet0/0
Internet 192.168.20.2      2  000c.2979.39f8  ARPA  Ethernet0/0
Internet 192.168.20.5      -  aabb.cc00.a000  ARPA  Ethernet0/0
Internet 192.168.20.6      2  aabb.cc00.5000  ARPA  Ethernet0/0
Internet 192.168.20.7      1  aabb.cc00.6000  ARPA  Ethernet0/0
Internet 192.168.20.9      2  aabb.cc00.8000  ARPA  Ethernet0/0
Internet 192.168.20.10     2  aabb.cc00.9000  ARPA  Ethernet0/0
LocalServer>
LocalServer>
LocalServer>
```

Hình 3.34 Kiểm tra lại bảng Mac của thiết bị Local-Server

```
PC7>!!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
PC7#show arp
Protocol Address          Age (min)  Hardware Addr  Type  Interface
Internet 192.168.20.2      4  000c.2979.39f8  ARPA  Ethernet0/0
Internet 192.168.20.5      0  aabb.cc00.a000  ARPA  Ethernet0/0
Internet 192.168.20.6      0  aabb.cc00.5000  ARPA  Ethernet0/0
Internet 192.168.20.7      -  aabb.cc00.6000  ARPA  Ethernet0/0
PC7#
PC7#
PC7#
```

Hình 3.35 Kiểm tra lại bảng Mac của thiết bị PC7

### 3.3.3 Kỹ thuật Scanning từ bên ngoài hệ thống

#### 1. Kỹ thuật tấn công Scanning

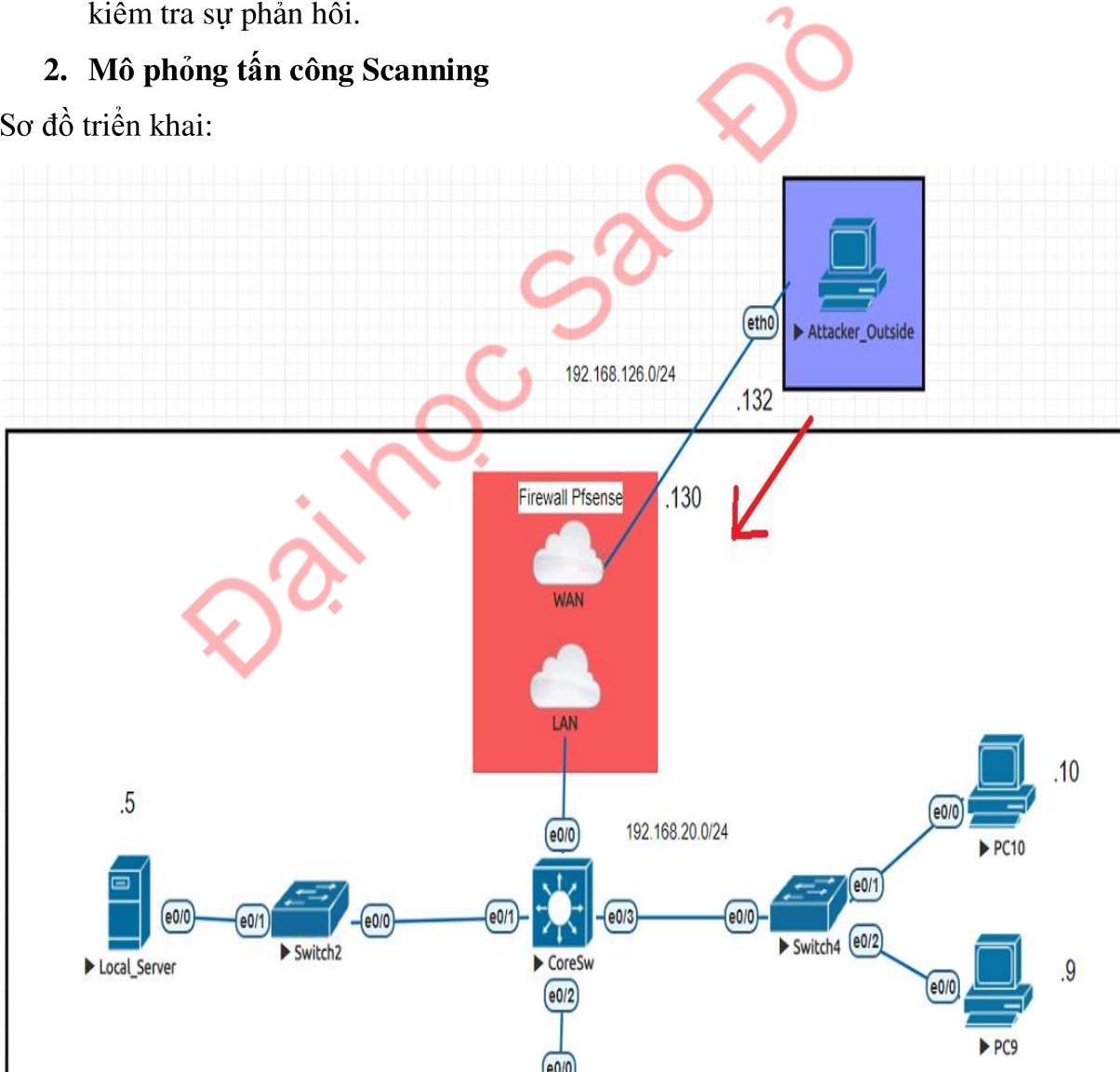
Kỹ thuật tấn công scanning từ bên ngoài internet vào hệ thống thường liên quan đến việc kẻ tấn công sử dụng các công cụ quét mạng để tìm kiếm thông tin về các cổng mạng, dịch vụ và các lỗ hổng bảo mật trong một hệ thống mục tiêu. Dưới đây là mô tả chi tiết về một số kỹ thuật tấn công scanning phổ biến:

- Port Scanning (Quét Cổng): Kẻ tấn công thực hiện quét các cổng mạng trên hệ thống mục tiêu để xác định những cổng nào đang mở và sẵn sàng tiếp nhận kết nối. Các công cụ quét như Nmap thường được sử dụng cho mục đích này.
- Service Scanning (Quét Dịch Vụ): Sau khi xác định các cổng mạng mở, kẻ tấn công tiếp tục quét để xác định loại dịch vụ đang chạy trên mỗi cổng. Điều này giúp họ hiểu rõ hơn về cấu trúc hệ thống và các dịch vụ đang hoạt động.

- Vulnerability Scanning (Quét Lỗ Hổng): Sau khi biết về cổng mạng và dịch vụ đang chạy, kẻ tấn công sử dụng các công cụ quét lỗ hổng để tìm kiếm các lỗ hổng bảo mật trong phần mềm hoặc hệ điều hành đang chạy trên hệ thống mục tiêu.
- OS Fingerprinting (Xác Định Hệ Điều Hành): Kẻ tấn công có thể cố gắng xác định hệ điều hành đang chạy trên máy chủ bằng cách phân biệt cách máy chủ xử lý các gói tin. Điều này có thể giúp họ chọn ra các lỗ hổng cụ thể phù hợp với hệ điều hành đó.
- Ping Sweeps (Quét Ping): Kỹ thuật này nhằm xác định những máy chủ hoặc thiết bị nào đang hoạt động trong một mạng bằng cách gửi các gói tin ping để kiểm tra sự phản hồi.

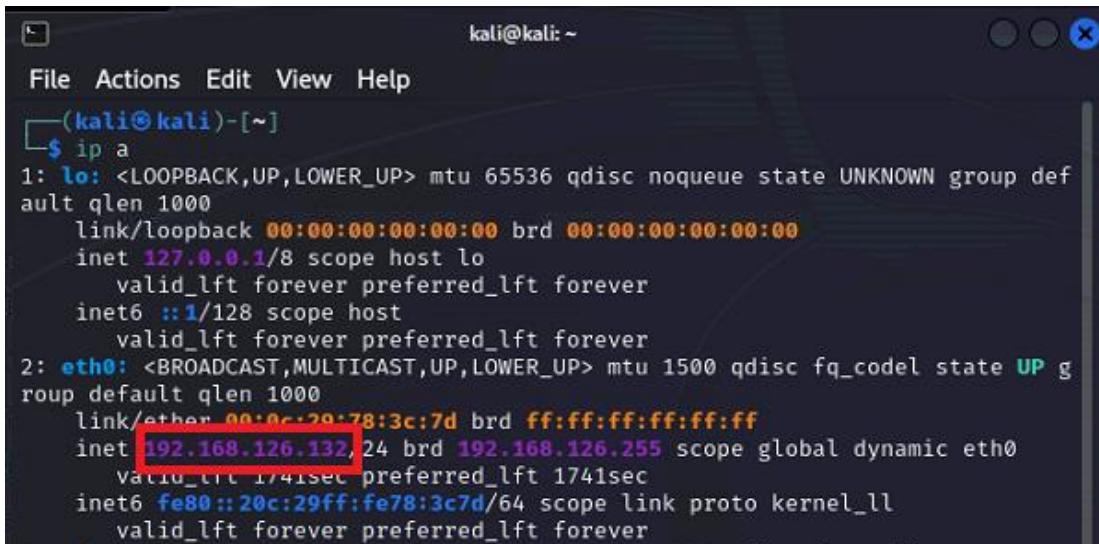
## 2. Mô phỏng tấn công Scanning

Sơ đồ triển khai:



Hình 3.36 Sơ đồ mô phỏng tấn công Scanning

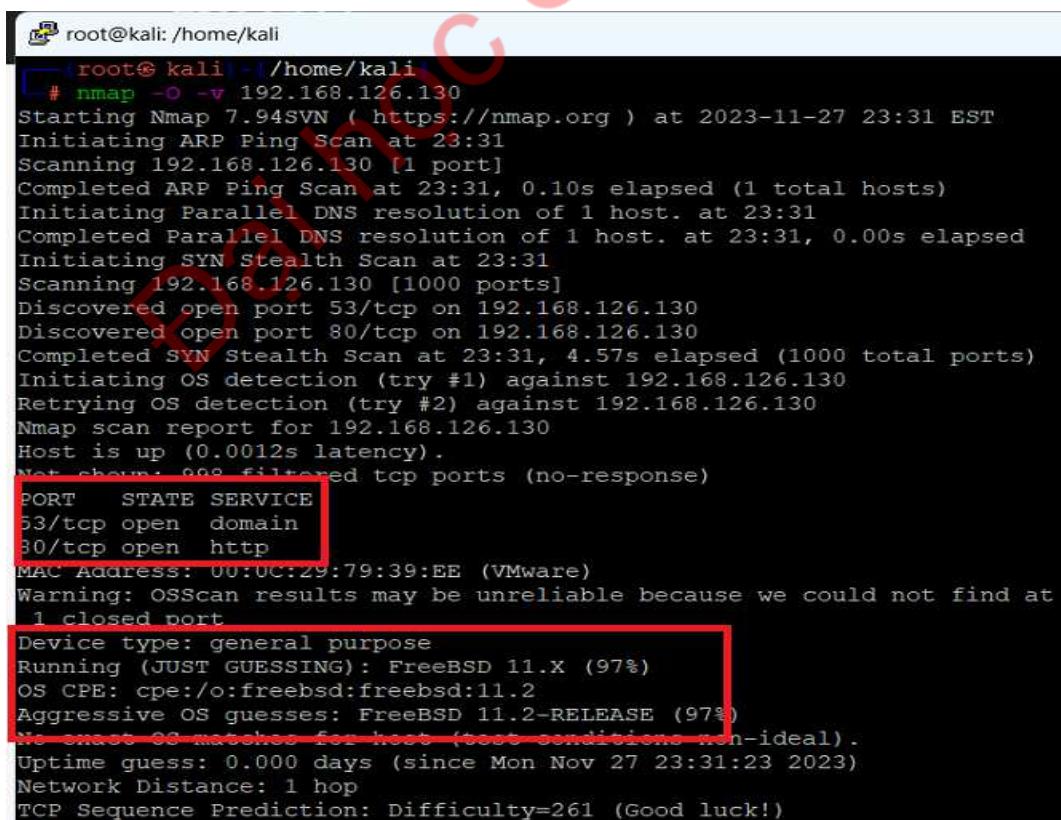
Địa chỉ IP của máy Kali linux là 192.168.126.132:



```
kali@kali:~  
File Actions Edit View Help  
(kali㉿kali)-[~]  
$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 00:0c:29:78:3c:7d brd ff:ff:ff:ff:ff:ff  
    inet 192.168.126.132/24 brd 192.168.126.255 scope global dynamic eth0  
        Valid_lft 1741sec preferred_lft 1741sec  
    inet6 fe80::20c:29ff:fe78:3c7d/64 scope link proto kernel ll  
        valid_lft forever preferred_lft forever
```

Hình 3.37 Địa chỉ IP của máy Kali linux

Đầu tiên từ máy Kali linux (địa chỉ IP: 192.168.126.132) thực hiện lệnh scan địa chỉ IP cổng OUTSIDE của Firewall PFsense (địa chỉ IP 192.168.126.130) bằng lệnh “nmap -O -v 192.168.126.130”:



```
root@kali:~/home/kali  
# nmap -O -v 192.168.126.130  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-27 23:31 EST  
Initiating ARP Ping Scan at 23:31  
Scanning 192.168.126.130 [1 port]  
Completed ARP Ping Scan at 23:31, 0.10s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 23:31  
Completed Parallel DNS resolution of 1 host. at 23:31, 0.00s elapsed  
Initiating SYN Stealth Scan at 23:31  
Scanning 192.168.126.130 [1000 ports]  
Discovered open port 53/tcp on 192.168.126.130  
Discovered open port 80/tcp on 192.168.126.130  
Completed SYN Stealth Scan at 23:31, 4.57s elapsed (1000 total ports)  
Initiating OS detection (try #1) against 192.168.126.130  
Retrying OS detection (try #2) against 192.168.126.130  
Nmap scan report for 192.168.126.130  
Host is up (0.0012s latency).  
Not shown: 992 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
53/tcp    open  domain  
80/tcp    open  http  
MAC Address: 00:0C:29:78:3C:7D (VMware)  
Warning: OSScan results may be unreliable because we could not find at  
1 closed port  
Device type: general purpose  
Running (JUST GUESSING): FreeBSD 11.X (97%)  
OS CPE: cpe:/o:freebsd:freebsd:11.2  
Aggressive OS guesses: FreeBSD 11.2-RELEASE (97%)  
No exact OS matches for host (test conditions non-ideal).  
Uptime guess: 0.000 days (since Mon Nov 27 23:31:23 2023)  
Network Distance: 1 hop  
TCP Sequence Prediction: Difficulty=261 (Good luck!)
```

Hình 3.38 Thực hiện scan Firewall PFsense

Ta có thể thấy một số thông tin về cổng và dịch vụ nào đang mở, ngoài ra còn xác định được hệ điều hành của thiết bị tường lửa Firewall PfSense cũng như phiên bản. Từ những thông tin này kẻ tấn công hoàn toàn có thể khai thác lỗ hổng để tấn công.

### 3. Giải pháp phòng vệ

Ở kịch bản ta sẽ bật tính năng Snort trên PfSense:

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
WAN (em0)	✓	AC-BNFA	LEGACY MODE	WAN	

Hình 3.39 Bật dịch vụ Snort trên PfSense

Sau đó trên máy Kali Linux ta thực hiện tấn công lại:

```
root@kali: /home/kali
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Nov 27 21:40:03 2023 from 192.168.126.1
[kali㉿ kali) ~]
$ sudo su
[sudo] password for kali:
root@kali: /home/kali
# nmap -O -v 192.168.126.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-27 23:27 EST
Initiating ARP Ping Scan at 23:27
Scanning 192.168.126.130 [1 port]
Completed ARP Ping Scan at 23:27, 0.12s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:27
Completed Parallel DNS resolution of 1 host. at 23:27, 0.01s elapsed
Initiating SYN Stealth Scan at 23:27
Scanning 192.168.126.130 [1000 ports]
Completed SYN Stealth Scan at 23:28, 21.13s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.126.130
Retrying OS detection (try #2) against 192.168.126.130
Nmap scan report for 192.168.126.130
Host is up (0.0039s latency).
All 1000 scanned ports on 192.168.126.130 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:0C:29:79:39:EE (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Read data files from: /usr/bin/.../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.14 seconds
    Raw packets sent: 2049 (94.700KB) | Rcvd: 1 (28B)

root@kali: /home/kali
#
```

Hình 3.40 Thực hiện Scan hệ thống trên máy Kali Linux

Sau đó kiểm tra thông tin về Snort của Firewall Pfsense sẽ thấy những cảnh báo về các hoạt động bất thường từ cuộc tấn công trên máy Kali linux:

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2023-11-28 11:28:16	⚠️	2	UDP	Attempted Information Leak	192.168.126.132	61257	192.168.126.130	41746	1:2018489	ET SCAN NMAP OS Detection Probe
2023-11-28 11:28:16	⚠️	2	UDP	Attempted Information Leak	192.168.126.132	61257	192.168.126.130	41746	1:2018489	ET SCAN NMAP OS Detection Probe
2023-11-28 11:28:16	⚠️	2	UDP	Attempted Information Leak	192.168.126.132	61257	192.168.126.130	41746	1:2018489	ET SCAN NMAP OS Detection Probe
2023-11-28 11:28:16	⚠️	2	UDP	Attempted Information Leak	192.168.126.132	61257	192.168.126.130	41746	1:2018489	ET SCAN NMAP OS Detection Probe
2023-11-28 11:28:15	⚠️	2	UDP	Attempted Information Leak	192.168.126.132	61257	192.168.126.130	32453	1:2018489	ET SCAN NMAP OS Detection Probe
2023-11-28 11:28:15	⚠️	2	UDP	Attempted Information Leak	192.168.126.132	61257	192.168.126.130	32453	1:2018489	ET SCAN NMAP OS Detection Probe

Hình 3.41 Cảnh báo về hoạt động bất thường của Snort

Kiểm tra thông tin về địa chỉ IP đã bị block bởi Snort, ta sẽ thấy đây chính là địa chỉ IP của máy Kali linux :

#	IP	Alert Descriptions and Event Times	Remove
1	192.168.126.132	ET SCAN Suspicious inbound to MySQL port 3306 – 2023-11-28 11:27:54 ET SCAN Potential VNC Scan 5900-5920 – 2023-11-28 11:27:58 ET SCAN Suspicious inbound to PostgreSQL port 5432 – 2023-11-28 11:28:03 ET SCAN Suspicious inbound to Oracle SQL port 1521 – 2023-11-28 11:28:03 ET SCAN Potential VNC Scan 5800-5820 – 2023-11-28 11:28:07 ET SCAN Suspicious inbound to MSSQL port 1433 – 2023-11-28 11:28:13 ET SCAN NMAP OS Detection Probe – 2023-11-28 11:28:16	✖️

1 host IP address is currently being blocked Snort on Legacy Blocking Mode interfaces.

Hình 3.42 Thông tin về địa chỉ IP đã bị block bởi Snort

### 3.4. Đánh giá công cụ và phát triển

#### 3.4.1 Công cụ giả lập Eve-ng

EVE-NG (viết tắt của Emulated Virtual Environment – Next Generation) là một trong các công cụ giả lập (emulator) tốt nhất hiện nay. Cùng các tính năng của UnetLab, Eve-ng có thể giả lập được rất nhiều loại thiết bị mạng đang được sử dụng rộng rãi như router, switch của Cisco (sử dụng Cisco IOL hoặc IOS), thiết bị mạng của Juniper, nhiều loại firewall thông dụng khác như ASA, Pfsense.



Hình 3.43 Đánh giá công cụ EVE-ng

Cisco IOL – Cisco IOS on Linux, hoặc một dạng khác là Cisco IOU – Cisco IOS on Unix là loại IOS chuyên dụng cho việc test tính năng của Cisco được viết để chạy trên nền hệ điều hành Linux (IOL), cho kiến trúc i386 hoặc trên nền hệ điều hành Unix (IOU), cho kiến trúc Sparc. Các hệ điều hành loại này chỉ được sử dụng cho nội bộ của hãng Cisco hoặc cho các khách hàng được ủy quyền và được cấp license. Trong thực tế, hai thuật ngữ IOL và IOU thường được sử dụng hoán đổi với nhau.

Các sinh viên đang theo học các khóa học của Cisco như CCNA, CCNP, CCIE cùng giải pháp giả lập thiết bị mạng sử dụng Cisco IOL là một giải pháp đang rất hiệu quả. Ưu điểm của giải pháp khi sử dụng là hoạt động giả lập rất nhẹ, ít tiêu tốn tài nguyên của máy tính, có thể giả lập được một số lượng lớn các thiết bị mạng mà không kém phần chính xác khi so sánh với giải pháp giả lập truyền thống thường được sử dụng là phần mềm GNS3.

## **Ưu điểm vượt trội của EVE-NG**

- Hỗ trợ thêm giao diện người dùng html5, triển khai thêm các tính năng telnet, vnc, và rpd kết nối trên các thiết bị mà không cần phải mở thêm một TCP port mới. Điều này cho phép dễ dàng hơn trong việc chạy EVE trên các máy chủ server ở bất kì đâu và cung cấp cơ chế remote để có thể làm việc với nhiều người dùng hơn.
- Các node đã tắt giờ đã được phân biệt các node khác thông qua màu sắc (màu xám cho các node đã tắt thay vì chỉ toàn màu xanh cho mọi node), do đó có thể dễ dàng nhận ra node nào đang chạy và node nào đã tắt.
- UKSM được thực hiện và kích hoạt mặc định, làm giảm thiểu đáng kể bộ nhớ khi so sánh với Unetlab.
- Nhiều loại image được hỗ trợ hơn.Thêm vào đó, bạn có thể tìm và lọc ra image khi thêm node mới, điều này thật tuyệt vời bởi vì nếu một list dài các image thì sẽ làm tốn công tìm image mà mình mong muốn.

### **3.4.2 Hệ điều hành Kali Linux**

Kali cung cấp một loạt các tính năng không thể tìm thấy trên các bản phân phối Linux truyền thống:

- Trên **600 công cụ** kiểm thử bảo mật hacking, pentest,...
- Các công cụ **thu thập thông tin mạng** Nmap, Wireshark,...
- Các công cụ **tập trung tấn công, khai thác** vào **Wifi** như Aircrack-ng, Kismet và Pixie.
- Đối với các nhu cầu **kiểm thử tấn công khai thác** vào **mật khẩu** sẽ có Hydra, Crunch, Hashcat và John the Ripper
- Có rất nhiều các công cụ hacking được **cập nhật liên tục**

#### **Ưu điểm**

**Tính an toàn:** Đội ngũ phát triển của Kali Linux là những cá nhân được tin cậy được cam kết về các gói và sự tương tác với các kho lưu trữ - tất cả được thực hiện bằng nhiều giao thức bảo mật.

Phần hạt nhân của Kali Linux cần được đưa vào các bản sửa lỗi mới nhất để đảm bảo an toàn và được liên tục cập nhật để phòng nhiễm virus.

**Hệ thống mã nguồn mở và miễn phí:** Linux luôn phát triển theo mô hình mã nguồn mở nên Kali Linux luôn được miễn phí, và tất nhiên tất cả các mã nguồn của Kali Linux cũng là mã nguồn mở, tất cả mọi người có thể tuỳ chỉnh và thay đổi theo nhu cầu.



Hình 3.44 Đánh giá hệ điều hành Kali linux

### **Ưu điểm về phần mềm và phần cứng**

Kali có thể sử dụng các repository của Debian hỗ trợ việc cài đặt được nhiều phần mềm và cập nhật phần mềm nhanh chóng

Kali Linux liên tục cải tiến khả năng tương thích với thiết bị phần cứng của rất nhiều loại như điện thoại, raspberry, laptop, server, cloud,... để bạn có thể cài đặt trên bất kì thiết bị nào

### **Ưu điểm về kết nối wifi và thiết bị không dây**

**Wifi:** Kali Lunux hỗ trợ rất tốt cho mạng wifi(không dây), điều này giúp các chuyên gia bảo mật có thể thực hiện tấn công và kiểm thử khả năng bảo mật của Wifi.

### **Hỗ trợ đa dạng thiết không dây:**

Kali Linux được cải tiến để hỗ trợ nhiều thiết bị không dây nhất có thể, cho phép nó hoạt động tốt trên nhiều loại phần cứng và làm cho nó tương thích với nhiều thiết bị không dây và USB khác nhau.

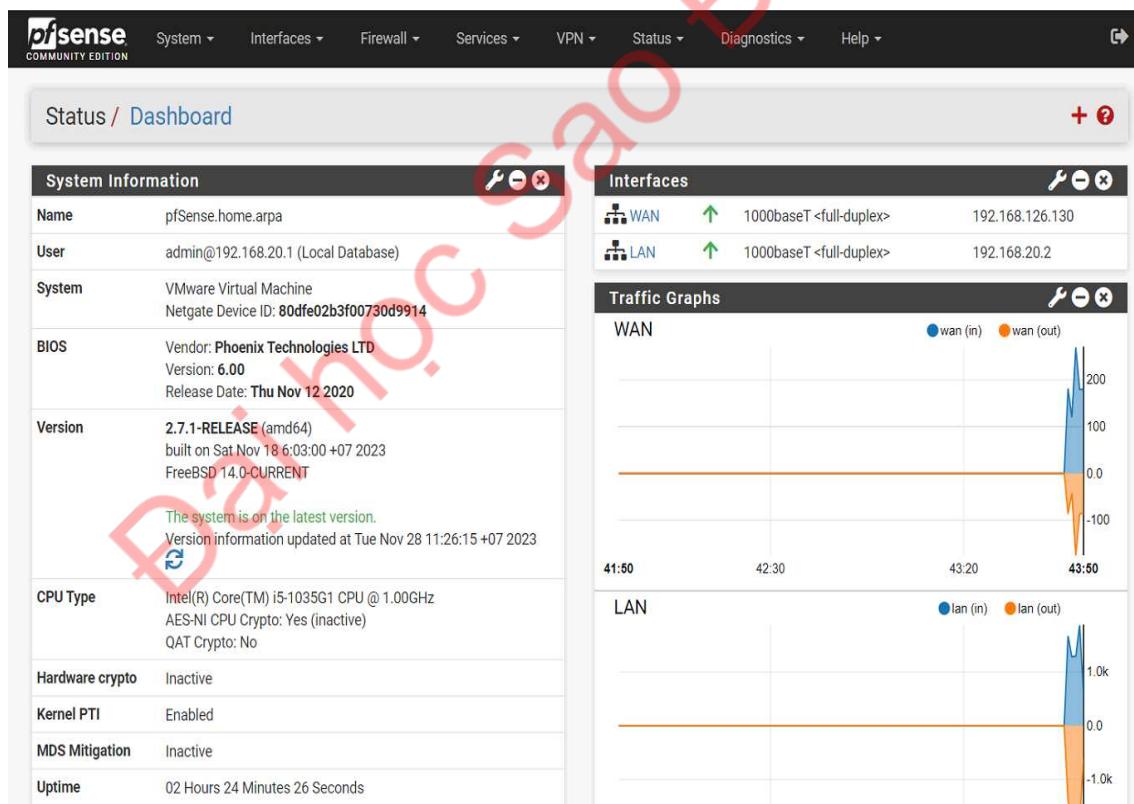
Số lượng phần mềm hỗ trợ hạn chế, không đa dạng và thông dụng như các hệ điều hành khác.

Nền tảng Linux không được một số nhà sản xuất hỗ trợ phát triển drive.

Khó tiếp cận người dùng: Kali Linux được xem như là hệ điều hành dành cho người chuyên nghiệp. Rất khó làm quen và mang đến nhiều rủi ro cho người không thành thạo.

### 3.4.3 Firewall PFsense

pfSense là một hệ thống tường lửa và cổng chia mạng mã nguồn mở, được xây dựng dựa trên hệ điều hành FreeBSD. pfSense là một giải pháp tường lửa và cổng chia mạng mạnh mẽ với nhiều ưu điểm, đặc biệt là với những người quản trị có kinh nghiệm và muôn tùy chỉnh cao.



Hình 3.45 Đánh giá Firewall Pfsense

#### Ưu Điểm của pfSense:

- Mã Nguồn Mở (Open Source):

Ưu điểm: pfSense là một dự án mã nguồn mở, giúp cộng đồng người dùng có thể kiểm soát và tùy chỉnh theo nhu cầu của họ mà không phải lo lắng về chi phí cấp phép.

- Tính Linh Hoạt và Đa Chức Năng:

Ưu điểm: pfSense không chỉ là một tường lửa mạng, mà còn cung cấp nhiều tính năng bảo mật như VPN, cân bằng tải, proxy, và nhiều tính năng khác, tạo ra một giải pháp đa chức năng cho hệ thống mạng.

- Giao Diện Người Dùng Thân Thiện:

Ưu điểm: pfSense có một giao diện người dùng web thân thiện và dễ sử dụng, giúp người quản trị dễ dàng cấu hình và giám sát.

- Hiệu Suất Cao:

Ưu điểm: pfSense có khả năng chạy trên nhiều loại phần cứng và cung cấp hiệu suất cao, làm cho nó phù hợp cho cả các môi trường mạng có yêu cầu cao.

- Cộng Đồng Lớn:

Ưu điểm: pfSense có một cộng đồng người sử dụng lớn, cung cấp hỗ trợ, tài liệu, và giải đáp các vấn đề thông qua các diễn đàn và nguồn tài trợ khác nhau.

### Nhược Điểm của pfSense:

- Khả Năng Quản Lý Phức Tạp:

Nhược điểm: Việc cấu hình và quản lý pfSense có thể phức tạp đối với người mới sử dụng, đặc biệt là trong các môi trường mạng lớn và phức tạp.

- Yêu Cầu Phần Cứng Cao:

Nhược điểm: Mặc dù pfSense có thể chạy trên nhiều loại phần cứng, nhưng một số tính năng yêu cầu phần cứng có hiệu suất cao để đảm bảo hoạt động mượt mà.

- Hỗ Trợ Thương Mại Phí:

Nhược điểm: Dịch vụ hỗ trợ thương mại của pfSense có thể đòi hỏi chi phí, điều này có thể là một rắc rối đối với các tổ chức đang tìm kiếm hỗ trợ cao cấp.

- Cập Nhật Tài Liệu:

Nhược điểm: Có thể xảy ra tình trạng tài liệu không được cập nhật kịp thời với các phiên bản mới, gây khó khăn cho người dùng trong quá trình triển khai và duy trì hệ thống.

### 3.4.4 Hướng phát triển

Sau khi đã thực hiện thành thạo các công cụ trên hệ điều hành Kali Linux và trau dồi được kỹ năng lập trình với ngôn ngữ Python thì hoàn toàn có thể xây dựng riêng một ứng dụng hoặc một trang web để sử dụng pentest cho hệ thống. Hoặc có thể tập hợp các công cụ đánh giá an toàn thông tin cho người dùng với mục đích học tập để sử dụng.

## 3.5 Kết luận

Qua quá trình mô phỏng, ta có thể phát hiện và khắc phục các lỗ hổng bảo mật, đồng thời nâng cao khả năng đối phó với các mối đe dọa tiềm ẩn. Những ưu điểm quan trọng như:

- Phát Hiện Rủi Ro: Tạo ra môi trường an toàn để tái tạo các kịch bản tấn công giúp xác định rủi ro bảo mật.
- Kiểm Tra Bảo Mật Hệ Thống: Mô phỏng giúp kiểm tra hiệu suất và tính an toàn của hệ thống, từ đó cung cấp những cơ hội để cải thiện.

Tuy nhiên, cũng cần lưu ý một số thách thức và hạn chế:

- Chi Phí và Thời Gian: Quá trình mô phỏng có thể đòi hỏi nhiều chi phí và thời gian, đặc biệt là khi cần sử dụng các chuyên gia và công cụ chuyên nghiệp.
- Giả Lập Không Hoàn Toàn Chính Xác: Không thể tái tạo môi trường thực tế một cách hoàn toàn chính xác, làm giảm độ chính xác của quá trình đánh giá.

Hiện nay các hình thức tấn công mạng LAN rất đa dạng và tinh vi. Nội dung trình bày lại các loại hình tấn công cơ bản để những người kỹ thuật bắt đầu bước lĩnh vực an toàn thông tin có sự đầu tư nghiên cứu, khi vận hành hệ thống Network cần có sự cân nhắc, triển khai các giải pháp phù hợp nhằm đảm bảo an toàn thông tin nhưng cũng đáp ứng yêu cầu về performance cho hệ thống.

## KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

Những kết quả đạt được trong đề tài:

- ✓ Mô phỏng được mô hình mạng thiết kế trên công cụ EVE-NG.
- ✓ Tìm hiểu được các lỗ hổng về mặt cấu hình cũng như các kiểu tấn công phổ biến.
- ✓ Thành thạo một số công cụ có sẵn trên hệ điều hành Kali Linux, Firewall PFsense.
- ✓ Đưa ra được các giải pháp ngăn chặn các cuộc tấn công.

Những hạn chế:

- ❖ Do kinh nghiệm thực tế chưa được nhiều và kiến thức về lỗ hổng còn hạn chế do vậy chưa khai thác được thêm nhiều các kiểu tấn công mới.
- ❖ Chưa vận dụng được nhiều công cụ để tạo ra mã khai thác hoặc công cụ không có sẵn để thực hiện tấn công và phòng chống.

Hướng phát triển tương lai:

Sau khi đã thực hiện thành thạo các công cụ trên hệ điều hành Kali Linux và trau dồi được kỹ năng lập trình với ngôn ngữ Python thì hoàn toàn có thể xây dựng riêng một ứng dụng hoặc một trang web để sử dụng pentest cho hệ thống. Hoặc có thể tập hợp các công cụ đánh giá an toàn thông tin cho người dùng với mục đích học tập để sử dụng.

Qua đây em xin được gửi lời cảm ơn tới những người đã quan tâm, theo dõi tới nội dung đề tài này.

Em Xin Chân Thành Cảm

## TÀI LIỆU THAM KHẢO

- [1] “Vulnerability Management Process”, <https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/>
- [2] “Pacify ARP Poisoning attack , International Journal of computer Applications(0975-8887) Volume 116 No.11, April 2015
- [3] “CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks”. Carnegie Mellon University Software Engineering Institute. Retrieved 18 September 2019
- [4] “What is a DDoS Attack”. Cloudflare. Retrieved 4 May 2020
- [5] “Vulnerability Management Process”, <https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/>
- [6] “Pacify ARP Poisoning attack , International Journal of computer Applications(0975-8887) Volume 116 No.11, April 2015
- [7] “CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks”. Carnegie Mellon University Software Engineering Institute. Retrieved 18 September 2019
- [8] “What is a DDoS Attack”. Cloudflare. Retrieved 4 May 2020
- [9] D Son, Sooel; Shmatikov, Vitaly (14 August 2017), "The Hitchhiker's Guide to DNS Cache Poisoning" (PDF). Cornell University. Archived (PDF) from the original on. Retrieved 3 April 2017.
- [10] Ramachandran, Vivek & Nandi, Sukumar (2005), "Detecting ARP Spoofing: An Active Technique". In Jajodia, Suchil & Mazumdar, Chandan (eds.). Information systems security: first international conference, ICISS 2005, Kolkata, India, December 19–21, 2005 .Birkhauser. p. 239. ISBN 978-3-540-30706-8. Computer Network.
- [11] Forouzan, Behrouz (2012-02-17), “Data Communications and Networking. McGraw-Hill”. p. 14. ISBN 9780073376226.
- [12] Gary A. Donahue (June 2007), “Network Warrior”. O'Reilly.