

TRƯỜNG ĐẠI HỌC TRÀ VINH
KHOA KỸ THUẬT VÀ CÔNG NGHỆ



ISO 9001:2015

TRẦN QUANG TIỀN

**NGHIÊN CỨU CÁC VẤN ĐỀ BẢO MẬT
TRONG CÁC GIAO THỨC MẠNG**

ĐỒ ÁN TỐT NGHIỆP
NGÀNH CÔNG NGHỆ THÔNG TIN

TRÀ VINH, NĂM 2024

TRƯỜNG ĐẠI HỌC TRÀ VINH
KHOA KỸ THUẬT VÀ CÔNG NGHỆ

NGHIÊN CỨU CÁC VẤN ĐỀ BẢO MẬT
TRONG CÁC GIAO THỨC MẠNG

ĐỒ ÁN TỐT NGHIỆP
NGÀNH CÔNG NGHỆ THÔNG TIN

Sinh viên: **Trần Quang Tiến**

Lớp: **DA20TTA**

MSSV: **110120077**

GVHD: **ThS. Huỳnh Văn Thanh**

TRÀ VINH, NĂM 2024

LỜI MỞ ĐẦU

Trong thời đại số hóa hiện nay, mạng máy tính đã trở thành một phần không thể thiếu của cuộc sống hàng ngày, chúng không chỉ được ứng dụng trong các hoạt động cá nhân mà còn được ứng dụng trong các tổ chức, doanh nghiệp và cả quốc gia. Mạng máy tính không chỉ giúp kết nối con người với nhau, mà còn là nền tảng cho các hệ thống thông tin, quản lý dữ liệu, quân sự, giao dịch tài chính và nhiều lĩnh vực quan trọng khác. Tuy nhiên, sự phát triển của mạng máy tính cũng kéo theo những hệ lụy vô cùng lớn, các vấn đề bảo mật mạng đang dần trở nên phức tạp và đáng lo ngại.

Bảo mật mạng là một lĩnh vực nghiên cứu quan trọng nhằm bảo vệ thông tin khỏi các mối đe dọa như xâm nhập, đánh cắp, phá hoại dữ liệu và các hành vi tấn công khác. Các giao thức mạng, vốn là nền tảng cho việc truyền thông tin trên mạng, đóng vai trò then chốt trong việc đảm bảo tính bảo mật và toàn vẹn của dữ liệu. Mặc dù nhiều giao thức đã được thiết kế với các biện pháp bảo mật, nhưng chúng vẫn không thể tránh khỏi những lỗ hổng và rủi ro tiềm tàng.

Đề tài này sẽ tập trung nghiên cứu các vấn đề bảo mật trong các giao thức mạng, từ những lỗ hổng phổ biến cho đến các biện pháp và công nghệ mới nhằm tăng cường bảo mật. Qua đó, phân tích các nguy cơ, những thách thức đang phải đối mặt, và đề xuất những giải pháp khả thi nhằm nâng cao hiệu quả bảo mật trong môi trường mạng hiện đại. Hy vọng rằng qua nghiên cứu này, sẽ có cái nhìn tổng quan hơn về tầm quan trọng của bảo mật mạng và những bước tiến cần thiết để bảo vệ thông tin trong thời đại kỹ thuật số.

LỜI CẢM ƠN

Lời đầu tiên, tôi xin gửi lời cảm ơn chân thành và sự tri ân sâu sắc đến các thầy cô của trường Đại học Trà Vinh, đặc biệt là thầy Huỳnh Văn Thanh, người đã góp ý, truyền đạt kiến thức để tôi có thể thực hiện đề tài này. Với vốn kiến thức được tôi tiếp thu trong quá trình học tập, tìm hiểu từ những chỉ dẫn đó giúp tôi cũng cố nền tảng cho việc nghiên cứu đề tài và cũng là hành trang quý báu mà tôi có thể áp dụng vào tương lai gần. Tôi cũng xin gửi lời cảm ơn chân thành đến các giảng viên khác trong bộ môn đã tạo điều kiện thuận lợi để tôi có thể hoàn thành đề tài này. Mặc dù có hạn chế về kiến thức và kinh nghiệm, trong quá trình thực hiện đề tài cũng không tránh khỏi những sai sót. Tôi rất mong nhận được sự góp ý tận tình từ quý thầy cô và hội đồng để tôi có thể hoàn thiện hơn trong những công trình nghiên cứu sau này.

Xin chân thành cảm ơn!

Trà Vinh, ngày tháng năm 2024

Sinh viên thực hiện

Trần Quang Tiến

[illegible]

Giảng viên hướng dẫn
(ký và ghi rõ họ tên)

BẢN NHẬN XÉT ĐỒ ÁN, KHÓA LUẬN TỐT NGHIỆP
(*Của giảng viên hướng dẫn*)

Họ và tên sinh viên: MSSV:

Ngành: Khóa:

Tên đề tài:

.....

Họ và tên Giáo viên hướng dẫn:

Chức danh: Học vị:

NHẬN XÉT

1. Nội dung đề tài:

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

2. Ưu điểm:

.....

.....

.....

3. Nhược điểm:

.....

.....

.....

.....

4. Điểm mới đề tài:

.....

.....

.....

.....

.....

5. Giá trị thực trên đề tài:

.....

.....

.....

.....

.....

.....

.....

7. Đề nghị sửa chữa bổ sung:

.....

.....

.....

.....

.....

.....

.....

8. Đánh giá:

.....

.....

.....

.....

Trà Vinh, ngày tháng năm 2024
Giảng viên hướng dẫn
(Ký & ghi rõ họ tên)

MỤC LỤC

CHƯƠNG 1. ĐẶT VẤN ĐỀ.....	1
1.1. Lý do chọn đề tài.....	1
1.2. Mục tiêu	1
1.3. Nội dung.....	1
1.4. Đối tượng và phạm vi nghiên cứu	2
1.5. Phương pháp nghiên cứu	2
CHƯƠNG 2. CƠ SỞ LÝ THUYẾT.....	3
2.1. Tổng quan giao thức mạng	3
2.1.1. Giao thức mạng.....	3
2.1.2. Cách thức hoạt động	3
2.1.3. Vai trò của giao thức mạng.....	3
2.1.4. Các giao thức mạng phổ biến	4
2.1.5. Một số ứng dụng của giao thức mạng.....	7
2.2. Mô hình TCP/IP và mô hình OSI	8
2.2.1. Mô hình TCP/IP.....	8
2.2.2. Mô hình OSI	9
2.2.3. So sánh mô hình OSI với mô hình TCP/IP.....	10
2.3. Một số vấn đề bảo mật trong giao thức mạng.....	12
2.3.1. Nghe trộm gói tin (Sniffing)	12
2.3.2. Giả mạo (Spoofing)	14
2.3.3. Phần mềm độc hại (malware)	17
2.3.4. Tấn công xen giữa (man-in-the-middle).....	19
2.3.5. Zero-day	20
2.4. Bảo mật trong các giao thức cơ bản: DHCP, ARP và DNS	21
2.4.1. Giao thức DHCP.....	21
2.4.2. Giao thức ARP	26
2.4.3. Giao thức DNS.....	28
2.5. Một số biện pháp phòng chống các cuộc tấn công mạng	31
2.5.1. Sử dụng tường lửa.....	31
2.5.2. Sử dụng phần mềm diệt virus	33
2.5.3. Cập nhật phần mềm thường xuyên	34
2.5.4. Sử dụng mạng riêng ảo	35
2.5.5. Sao lưu dữ liệu định kỳ	36
2.5.6. Giám sát mạng	37
2.5.7. Quản lý quyền truy cập	38

2.5.8. Sử dụng công nghệ sandboxing	38
2.5.9. Nâng cao nhận thức về bảo mật.....	39
CHƯƠNG 3. HIỆN THỰC HÓA NGHIÊN CỨU	40
3.1. Cài đặt phần mềm giả lập mạng.....	40
3.1.1. Phần mềm mô phỏng giả lập mạng.....	40
3.1.2. Cài đặt ứng dụng Cisco Packet Tracer.....	41
3.2. Mô phỏng một cuộc tấn công DHCP spoofing và hướng khắc phục	42
3.2.1. Đặc tả yêu cầu.....	42
3.2.2. Cấu hình DHCP cho router để cấp phát địa chỉ IP động	43
3.2.3. Cấu hình DHCP cho server giả mạo	46
3.2.4. Giải pháp phòng chống tấn công DHCP spoofing.....	48
3.3. Mô phỏng một cuộc tấn công ARP snoofing và hướng khắc phục	51
3.3.1. Đặc tả yêu cầu.....	51
3.3.2. Cấu hình DHCP cho router để cấp phát địa chỉ IP tự động.....	52
3.3.3. Mô phỏng cách kẻ tấn công thực hiện	55
3.3.4. Giải pháp phòng chống tấn công ARP spoofing	58
CHƯƠNG 4. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN.....	63
4.1. Kết luận.....	63
4.2. Hướng phát triển	64
DANH MỤC TÀI LIỆU THAM KHẢO.....	65

DANH MỤC CÁC BẢNG, SƠ ĐỒ, HÌNH

Bảng 2-1 So sánh mô hình OSI và mô hình TCP/IP	11
Hình 2-1 Các thành phần của mô hình TCP/IP	9
Hình 2-2 Sự tương ứng giữa các tầng trong mô hình OSI và mô hình TCP/IP.....	10
Hình 2-3 Nghe trộm gói tin.....	12
Hình 2-4: Một số loại tấn công giả mạo phổ biến	17
Hình 2-5 Một số phần mềm độc hại phổ biến.....	18
Hình 2-6 Tấn công xen giữa (Man-in-the-middle)	20
Hình 2-7 Quá trình cấp phát địa chỉ IP thông qua DHCP	23
Hình 2-8 Quá trình phân giải địa chỉ trong giao thức ARP	27
Hình 2-9 Quá trình phân giải tên miền và giao tiếp HTTPS	30
Hình 2-10 Một số biện pháp phòng chống các cuộc tấn công mạng.....	31
Hình 3-1 Giao diện ứng dụng Packet Tracer sau khi khởi động	41
Hình 3-2 Mô hình mô phỏng một cuộc tấn công DHCP spoofing	42
Hình 3-3 Cấu hình DHCP cho RouterDHCP.....	44
Hình 3-4 PC0 sau khi nhận địa chỉ IP tự động thông qua DHCP của RouterDHCP	44
Hình 3-5 PC1 sau khi nhận địa chỉ IP tự động thông qua DHCP của RouterDHCP	45
Hình 3-6 PC2 sau khi nhận địa chỉ IP tự động thông qua DHCP của RouterDHCP	45
Hình 3-7 Mô hình mô phỏng sau khi được cấp phát địa chỉ IP.....	46
Hình 3-8 Thông tin về IP, subnet mask, gateway, DNS của server DHCP giả mạo	46
Hình 3-9 Cấu hình DHCP cho server FakeDHCP	47
Hình 3-10 PC0 sau khi nhận lại địa chỉ IP.....	47
Hình 3-11 PC2 sau khi nhận lại địa chỉ IP.....	48
Hình 3-12 PC1 sau khi nhận lại địa chỉ IP.....	48
Hình 3-13 Cấu hình DHCP snooping trên switch.....	50
Hình 3-14 PC0 sau khi cấu hình DHCP snooping trên switch	50
Hình 3-15 PC1 sau khi cấu hình DHCP snooping trên switch	50
Hình 3-16 PC2 sau khi cấu hình DHCP snooping trên switch	51
Hình 3-17 Mô hình mô phỏng tấn công ARP spoofing.....	52
Hình 3-18 Cấu hình DHCP cho router ở cả hai cổng	54
Hình 3-19 PC1 sau khi nhận IP	54
Hình 3-20 PC2 sau khi nhận IP	55
Hình 3-21 PC tấn công sau khi nhận IP.....	55
Hình 3-22 Kiểm tra kết nối giữa PC1 với PC2	55
Hình 3-23 Kiểm tra kết nối giữa PC1 với PC của kẻ tấn công.....	56
Hình 3-24 Kẻ tấn công gửi gói tin đến default gateway để lấy địa chỉ MAC	57
Hình 3-25 Đổi địa chỉ MAC của mỗi đe dọa thành địa chỉ MAC của gateway	57
Hình 3-26 Kẻ tấn công ping đến máy nạn nhân để cập nhật lại bảng ARP	57
Hình 3-27 Bảng ARP trên máy nạn nhân sau khi cập nhật	58
Hình 3-28 Bảng địa chỉ MAC lưu trữ trên switch đã bị kẻ tấn công thay đổi.....	58
Hình 3-29 PC1 không thể gửi gói tin đến PC2	58
Hình 3-30 Cấu hình DHCP snooping trên switch.....	59
Hình 3-31 Cấu hình DAI trên switch.....	60
Hình 3-32 Kiểm tra kết nối giữa PC của kẻ tấn công với default gateway và PC1.....	61
Hình 3-33 Bảng MAC sau khi dùng DAI	61
Hình 3-34 Kiểm tra kết nối giữa PC1 và PC2	62

DANH MỤC TỪ VIẾT TẮT

Từ viết tắt	Ý nghĩa
ARP	Address Resolution Protocol
ARPANET	Advanced Research Projects Agency Network
DAI	Dynamic ARP Inspection
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
MAC	Media Access Control
NGFW	Next Generation Firewall
OSI	Open Systems Interconnection
POP3	Post Office Protocol version 3
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol

SSH	Secure Shell
SSL/TLS	Secure Sockets Layer / Transport Layer Security
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UTM	Unified threat management
VPN	Virtual Private Network

CHƯƠNG 1. ĐẶT VẤN ĐỀ

1.1. Lý do chọn đề tài

Trong bối cảnh số hóa ngày càng được ứng dụng rộng rãi, mạng máy tính đã trở thành yếu tố không thể thiếu trong cuộc sống hàng ngày cũng như trong hoạt động của các tổ chức và doanh nghiệp. Sự kết nối liên tục và toàn cầu hóa thông tin mang lại nhiều lợi ích to lớn, nhưng đồng thời cũng đặt ra những thách thức nghiêm trọng về bảo mật. Các vụ tấn công mạng ngày càng gia tăng về số lượng và mức độ tinh vi, gây ra những thiệt hại đáng kể về kinh tế, quân sự, an ninh và uy tín của các cá nhân, tổ chức. Ngoài ra, trang bị kiến thức cần thiết về các vấn đề bảo mật trong mạng máy tính giúp tránh được sự tấn công của tin tặc.

Chính vì vậy, việc nghiên cứu và hiểu rõ các vấn đề bảo mật trong các giao thức mạng là vô cùng cần thiết. Các giao thức mạng đóng vai trò là cốt lõi cho việc truyền tải dữ liệu trên mạng, nhưng cũng là mục tiêu dễ bị tấn công nếu không được bảo vệ đúng mức. Nhận thức được tầm quan trọng của việc bảo vệ thông tin, tôi quyết định chọn đề tài “Nghiên Cứu Các Vấn Đề Bảo Mật Trong Các Giao Thức Mạng”.

1.2. Mục tiêu

Nghiên cứu về cơ chế hoạt động của các giao thức mạng, các lỗ hổng trong các giao thức, phân tích chi tiết về cách thức hoạt động của các giao thức mạng, từ đó nhận diện những lỗ hổng có thể bị khai thác bởi các mối đe dọa.

Nhận diện và phân loại các mối đe dọa bảo mật: Nhận diện và phân loại các loại hình tấn công phổ biến, đánh giá ưu nhược điểm và đưa ra giải pháp thích hợp.

Đánh giá các biện pháp bảo mật hiện tại: Xem xét và đánh giá hiệu quả của các biện pháp bảo mật hiện đang được áp dụng trong các giao thức mạng, như mã hóa, xác thực, và kiểm tra tính toàn vẹn dữ liệu.

Nâng cao nhận thức và kỹ năng bảo mật: Cung cấp thông tin và kiến thức cần thiết để nâng cao nhận thức về bảo mật mạng, từ đó trang bị các kỹ năng cần thiết để bảo vệ thông tin và dữ liệu. Qua đó, ứng dụng các kiến thức an toàn trong các giao thức để triển khai hệ thống mạng an toàn trong thực tế.

1.3. Nội dung

Nghiên cứu chuyên sâu về các dạng tấn công phổ biến nhắm vào giao thức mạng như

DHCP, ARP, DNS... Thông qua việc phân tích kỹ lưỡng cơ chế và bản chất của từng phương thức tấn công, từ đó đề xuất các giải pháp bảo mật hiệu quả để ngăn chặn và đối phó với các mối đe dọa mạng. Sau khi xác định các biện pháp phòng chống, tiến hành triển khai mô hình mô phỏng trên phần mềm Cisco Packet Tracer để kiểm nghiệm tính khả thi và hiệu quả của các giải pháp đề xuất.

1.4. Đối tượng và phạm vi nghiên cứu

Đối tượng nghiên cứu:

Các giao thức mạng: Nghiên cứu chi tiết về các giao thức mạng quan trọng như DHCP, ARP và DNS.

Các dạng tấn công nhắm vào các giao thức DHCP, ARP và DNS bao gồm: DHCP Starvation Attack, DHCP Spoofing, ARP Spoofing/Poisoning, DNS Spoofing/Cache Poisoning.

Các biện pháp bảo mật: Đánh giá các biện pháp bảo mật hiện có và mô phỏng trên phần mềm Cisco Packet Tracer.

Phạm vi nghiên cứu:

Các dạng tấn công phổ biến nhằm vào DHCP, ARP và DNS.

1.5. Phương pháp nghiên cứu

Nghiên cứu lý thuyết: Nghiên cứu, phân tích các tài liệu liên quan đến giao thức mạng, các lỗ hổng bảo mật và các phương pháp khắc phục những lỗ hổng bảo mật đó.

Phân tích lỗ hổng: Xác định các lỗ hổng bảo mật thường gặp và cụ thể trong các giao thức mạng như DHCP, ARP, DNS... thông qua các tài liệu nghiên cứu trước

Mô phỏng tấn công: Sử dụng công cụ Cisco Packet Tracer để mô phỏng các tấn công đối với giao thức mạng như DHCP, ARP....

Triển khai giải pháp: Thử nghiệm các biện pháp khắc phục, triển khai mô hình mô phỏng trên công cụ Cisco Packet Tracer.

Đánh giá giải pháp: Sử dụng các tiêu chuẩn đánh giá để kiểm tra hiệu quả của các biện pháp bảo mật đã triển khai.

CHƯƠNG 2. CƠ SỞ LÝ THUYẾT

2.1. Tổng quan giao thức mạng

2.1.1. Giao thức mạng

Giao thức mạng hay còn được biết với tên gọi giao thức truyền thông là tập hợp các quy tắc chuẩn cho phép hai hay nhiều thực thể trong một hệ thống thông tin có thể trao đổi thông tin, dữ liệu được với nhau thông qua các kênh truyền thông. Có nhiều loại giao thức mạng, mỗi loại phục vụ một mục đích cụ thể như truyền dữ liệu, kiểm soát mạng, quản lý mạng,... Các giao thức này làm việc cùng nhau để đảm bảo cho sự hoạt động ổn định và hiệu quả của mạng thông tin, cung cấp sự giao tiếp chính xác và đáng tin cậy giữa các thiết bị, đồng thời đảm bảo an toàn và bảo mật thông tin truyền tải. Một số giao thức phổ biến có thể kể tên là TCP/IP, UDP, HTTP, HTTPS, SSH, DHCP, DNS,...

2.1.2. Cách thức hoạt động

Thiết lập kết nối liên lạc: Trước khi bắt đầu truyền dữ liệu, các thiết bị cần thiết lập một kết nối liên lạc để đảm bảo dữ liệu được truyền đi đúng cách.

Chia dữ liệu thành các gói: Giao thức phân chia dữ liệu thành các gói nhỏ hơn để truyền tải. Mỗi gói chứa thông tin về nguồn gốc, đích đến, loại dữ liệu, v.v.

Gửi và nhận gói: Các gói tin được gửi qua mạng từ thiết bị nguồn đến thiết bị đích. Thiết bị đích nhận các gói tin và giải mã chúng để khôi phục dữ liệu gốc.

Kiểm tra và sửa lỗi: Giao thức có thể bao gồm các cơ chế để kiểm tra và sửa lỗi trong quá trình truyền tải, đảm bảo dữ liệu được truyền đi mà không bị lỗi.

Ngắt kết nối liên lạc: Sau khi hoàn tất việc truyền dữ liệu, các thiết bị sẽ ngắt kết nối liên lạc.

2.1.3. Vai trò của giao thức mạng

Sắp xếp dữ liệu: Đảm bảo rằng dữ liệu được truyền đi theo đúng thứ tự để đảm bảo tính toàn vẹn và chính xác của dữ liệu.

Luồng dữ liệu: Quản lý và điều chỉnh lưu lượng dữ liệu trong mạng để đảm bảo truyền thông hiệu quả và tối ưu hóa hiệu suất mạng.

Định tuyến dữ liệu: Xác định đường đi tối ưu cho dữ liệu từ nguồn đến đích để giảm thiểu thời gian truyền thông và đảm bảo tính toàn vẹn của dữ liệu.

Đóng gói dữ liệu: Bảo vệ thông tin bằng cách đóng gói dữ liệu trong các gói tin

thành một dạng hoặc một giao thức cụ thể để truyền qua mạng, đảm bảo tính bảo mật và toàn vẹn của dữ liệu.

Chia nhỏ và hợp nhất: Chia nhỏ dữ liệu lớn thành các phần nhỏ hơn để truyền đi hiệu quả và đảm bảo tính toàn vẹn của dữ liệu, sau đó tái hợp nhất các phần nhỏ này để khôi phục dữ liệu ban đầu.

Kiểm soát kết nối: Quản lý việc thiết lập, duy trì và chấm dứt kết nối giữa các thiết bị mạng để tăng cường hiệu suất và độ ổn định của mạng.

Đa kênh: Cho phép kết hợp nhiều luồng dữ liệu cùng trên một đường truyền để tối ưu hóa việc sử dụng tài nguyên mạng và tăng tốc độ truyền dữ liệu.

Sắp đặt gói tin theo thứ tự: Đảm bảo các gói dữ liệu được giao đến đích theo cùng một thứ tự như chúng đã được gửi đi, đặc biệt quan trọng đối với các ứng dụng như video hoặc âm thanh.

Dịch vụ truyền tải: Cho phép truyền tải dữ liệu giữa các thiết bị trong mạng một cách hiệu quả và đáng tin cậy.

Xác định địa chỉ: Xác định địa chỉ của các thiết bị trong mạng để đảm bảo truyền tải dữ liệu chính xác và hiệu quả.

Kiểm soát luồng: Kiểm soát lưu lượng dữ liệu giữa các thiết bị trong mạng để tránh tình trạng tắc nghẽn hoặc mất mát dữ liệu, đảm bảo truyền dẫn hiệu quả.

Kiểm soát lỗi: Phát hiện và sửa chữa các lỗi trong quá trình truyền tải dữ liệu để đảm bảo tính chính xác và tin cậy của thông tin.

2.1.4. Các giao thức mạng phổ biến

2.1.4.1 Giao thức TCP/IP và giao thức UDP

TCP là một tiêu chuẩn truyền thông cho phép trao đổi tin nhắn giữa các ứng dụng và thiết bị tính toán trên mạng. Nó được thiết kế để đảm bảo gửi các gói tin dữ liệu qua Internet và đảm bảo việc giao nhận dữ liệu và tin nhắn thành công trên mạng. TCP tổ chức và đảm bảo tính toàn vẹn của dữ liệu được truyền qua mạng bằng cách thiết lập kết nối giữa nguồn và đích trước khi truyền dữ liệu, chia dữ liệu thành các gói nhỏ, và đảm bảo tính toàn vẹn dữ liệu trong suốt quá trình truyền.

IP là phương tiện để gửi dữ liệu từ một thiết bị đến một thiết bị khác trên Internet.

Mỗi thiết bị có một địa chỉ IP duy nhất giúp xác định và cho phép nó trao đổi dữ liệu với các thiết bị khác trên Internet. IP định nghĩa cách các ứng dụng và thiết bị trao đổi các gói dữ liệu với nhau và là giao thức chính xác giữa các máy tính trên một mạng hoặc nhiều mạng kết nối với nhau.

Sự khác biệt giữa TCP và IP là TCP chịu trách nhiệm vận chuyển dữ liệu qua mạng và đảm bảo dữ liệu đến được đích, trong khi IP xác định và cung cấp địa chỉ IP của thiết bị hoặc ứng dụng mà dữ liệu cần được gửi đến. TCP và IP là hai giao thức hoạt động cùng nhau để đảm bảo dữ liệu được gửi đến đúng đích trên mạng. Khi được kết hợp, TCP/IP tạo nên một hệ thống an toàn và hiệu quả cho việc truyền dữ liệu giữa các thiết bị.

UDP là một giao thức mạng được sử dụng trên Internet để truyền dữ liệu một cách nhanh chóng và được ứng dụng trong các lĩnh vực đòi hỏi phải truyền dữ liệu theo thời gian thực như phát trực tuyến hoặc tìm kiếm DNS. Khác với các giao thức khác, UDP không thiết lập một kết nối chính thức trước khi dữ liệu được truyền đi. Điều này cho phép dữ liệu được truyền đi một cách nhanh chóng nhưng cũng có một nhược điểm chí mạng đó là có thể bị mất gói tin trong quá trình truyền dữ liệu, điều này tạo cơ hội cho các cuộc tấn công từ chối dịch vụ (DDoS). Do UDP là một giao thức không đảm bảo tính toàn vẹn hoặc thứ tự của dữ liệu khi chuyển đi, điều này có nghĩa là trong một số trường hợp gói tin có thể bị mất, bị trễ hoặc đến không đúng thứ tự trong trường hợp mạng không ổn định. Điều này có thể ảnh hưởng đến trải nghiệm người dùng, đặc biệt là trong các ứng dụng yêu cầu độ trễ thấp như trò chơi trực tuyến hay truyền phát video trực tuyến.

UDP là một giao thức truyền thông nhanh hơn nhưng ít đáng tin cậy hơn so với TCP, một giao thức vận chuyển phổ biến khác. Trong giao tiếp TCP, hai máy tính bắt đầu bằng việc thiết lập một kết nối thông qua một quy trình tự động gọi là 'bắt tay'. Chỉ khi quá trình bắt tay này hoàn thành, một máy tính mới chuyển gói tin dữ liệu đến máy tính khác.

Giao tiếp UDP không thông qua quá trình này. Thay vào đó, một máy tính có thể đơn giản bắt đầu gửi dữ liệu đến máy tính khác:

Ngoài ra, giao tiếp TCP chỉ ra thứ tự mà các gói tin dữ liệu nên được nhận và xác nhận rằng các gói tin đến đúng như ý muốn. Nếu một gói tin không đến, do tắc nghẽn trong các mạng trung gian, TCP sẽ yêu cầu gửi lại gói tin đó nhưng UDP sẽ không thực hiện yêu cầu này. Những khác biệt này tạo ra một số ưu điểm. Vì UDP không yêu cầu một 'bắt tay' hoặc kiểm tra xem dữ liệu đến đúng cách, nó có thể truyền dữ liệu nhanh hơn nhiều so với

TCP. Tuy nhiên, tốc độ này tạo ra các sự đánh đổi. Nếu một datagram UDP bị mất trong quá trình truyền, nó sẽ không được gửi lại.

2.1.4.2 Giao thức HTTP/HTTPS

HTTP là một giao thức hoặc một tập hợp các quy tắc giao tiếp cho việc giao tiếp giữa máy khách và máy chủ. Khi người dùng truy cập một trang web, trình duyệt sẽ gửi một yêu cầu HTTP đến máy chủ web, máy chủ phản hồi bằng một phản hồi HTTP. Máy chủ web và trình duyệt trao đổi dữ liệu dưới dạng văn bản thô. Nói một cách ngắn gọn, giao thức HTTP là công nghệ cơ bản đứng sau việc truyền thông mạng. Khi truy cập trang web, trình duyệt gửi yêu cầu HTTP đến máy chủ web, chứa thông tin về tài nguyên cần truy cập. Máy chủ xử lý yêu cầu và gửi phản hồi HTTP về trình duyệt, bao gồm mã trạng thái, tiêu đề, và dữ liệu. Trình duyệt nhận và hiển thị nội dung trên trang web dựa trên thông tin phản hồi.

HTTPS là một phiên bản an toàn hơn hoặc một sự mở rộng của HTTP. Trong HTTPS, trình duyệt và máy chủ thiết lập một kết nối an toàn, mã hóa trước khi chuyển dữ liệu. HTTP truyền dữ liệu không được mã hóa, có nghĩa là thông tin gửi từ trình duyệt có thể bị chặn và đọc bởi bên thứ ba. Điều này không phải là một quá trình lý tưởng, vì vậy nó đã được mở rộng thành HTTPS để thêm một lớp bảo mật khác vào giao tiếp. HTTPS kết hợp yêu cầu và phản hồi HTTP với công nghệ SSL và TLS. Các trang web HTTPS phải nhận được một chứng chỉ SSL/TLS từ một cơ quan chứng nhận chứng chỉ độc lập. Những trang web này chia sẻ chứng chỉ với trình duyệt trước khi trao đổi dữ liệu để xác định sự tin cậy. Chứng chỉ SSL cũng chứa thông tin mật mã, vì vậy máy chủ và trình duyệt web có thể trao đổi dữ liệu được mã hóa hoặc lộn xộn.

2.1.4.3 Giao thức DHCP

DHCP là giao thức quản lý mạng giúp các thiết bị trên mạng tự động nhận các địa chỉ IP và thông tin cấu hình mạng khác mà không cần can thiệp thủ công. Khi một thiết bị kết nối vào mạng, nó gửi một yêu cầu DHCP tìm kiếm máy chủ DHCP. Máy chủ DHCP phản hồi bằng một đề xuất địa chỉ IP và thông tin cấu hình khác. Sau khi thiết bị chọn một địa chỉ IP từ các đề xuất, nó gửi một yêu cầu xác nhận đến máy chủ DHCP. Máy chủ DHCP sau đó cung cấp xác nhận cho thiết bị, kèm theo thời gian thuê địa chỉ IP. Cuối cùng, thiết bị cấu hình giao diện mạng của mình với địa chỉ IP được cung cấp và tham gia mạng. Địa chỉ IP này có thể được sử dụng trong một khoảng thời gian nhất định trước khi cần phải

gia hạn. DHCP giúp tự động hóa việc cấu hình mạng, giảm thiểu sự can thiệp thủ công và đơn giản hóa quản lý mạng.

2.1.4.4 Giao thức DNS

DNS là hệ thống cơ sở dữ liệu giúp chuyển đổi các tên miền dễ nhớ thành địa chỉ IP và ngược lại trên Internet. Khi một thiết bị muốn truy cập vào một tên miền, nó gửi một yêu cầu tới máy chủ DNS. Máy chủ DNS kiểm tra thông tin trong bộ nhớ cache, nếu không có, nó truy vấn các máy chủ DNS khác đến khi tìm thấy thông tin phân giải cho tên miền đó. Cuối cùng, máy chủ DNS trả về địa chỉ IP tương ứng cho tên miền và thiết bị có thể truy cập vào trang web hoặc dịch vụ mong muốn bằng địa chỉ IP này. DNS giúp người dùng truy cập Internet một cách dễ dàng và tiện lợi thông qua các tên miền dễ nhớ.

2.1.5. Một số ứng dụng của giao thức mạng

2.1.5.1 Truyền dữ liệu trên mạng

Giao thức được sử dụng để truyền dữ liệu giữa các thiết bị trong mạng, đảm bảo dữ liệu được gửi và nhận một cách hiệu quả và chính xác:

TCP/IP được sử dụng rộng rãi trên Internet để truyền tải dữ liệu. TCP chịu trách nhiệm chia nhỏ dữ liệu thành các gói tin và đảm bảo chúng được truyền đến đích một cách an toàn và đúng thứ tự. IP xử lý việc định tuyến các gói tin này đến đúng địa chỉ IP đích.

UDP được sử dụng cho truyền dữ liệu thời gian thực như video và âm thanh, nơi mà tốc độ là quan trọng hơn độ tin cậy. UDP không đảm bảo thứ tự hoặc kiểm tra lỗi, nên dữ liệu có thể bị mất mát hoặc nhận sai thứ tự, nhưng tốc độ truyền tải cao hơn.

HTTP được sử dụng để truyền dữ liệu web, bao gồm các trang HTML, hình ảnh, video, và các tài liệu khác cũng là nền tảng của World Wide Web, cho phép trình duyệt và máy chủ web giao tiếp với nhau.

FTP được sử dụng để truyền tải tệp giữa các thiết bị, cung cấp các lệnh để tải lên và tải xuống tệp từ máy chủ FTP, quản lý tệp trên máy chủ và bảo mật việc truy cập.

2.1.5.2 Truy cập mạng

Các giao thức được sử dụng để truy cập và quản lý các kết nối mạng:

DHCP tự động cấp phát địa chỉ IP cho các thiết bị trong mạng, giúp dễ dàng quản lý và tránh xung đột địa chỉ IP.

DNS dịch các tên miền dễ nhớ (ví dụ: www.example.com) thành địa chỉ IP (ví dụ: 192.168.1.1) để các thiết bị có thể giao tiếp với nhau.

SMTP sử dụng để gửi email từ máy khách tới máy chủ email và từ máy chủ này tới máy chủ khác.

POP3 Sử dụng để nhận email từ máy chủ email về máy khách, thường dùng cho việc tải email xuống máy tính cá nhân.

2.1.5.3 Quản lý mạng

Các giao thức được sử dụng để giám sát và quản lý các thiết bị mạng nhằm đảm bảo hiệu suất và bảo mật của hệ thống mạng:

SNMP được dùng để giám sát và quản lý các thiết bị mạng như bộ định tuyến, bộ chuyển mạch, máy chủ, và máy in từ xa đồng thời cung cấp các thông tin về trạng thái, hiệu suất và lỗi của các thiết bị.

SSH cho phép truy cập an toàn vào các thiết bị mạng từ xa, mã hóa kết nối, đảm bảo rằng dữ liệu không bị nghe lén và các phiên làm việc an toàn.

VPN tạo kết nối mạng an toàn giữa các mạng khác nhau thông qua Internet để đảm bảo dữ liệu được mã hóa và bảo mật, giúp truy cập từ xa vào mạng nội bộ một cách an toàn.

2.2. Mô hình TCP/IP và mô hình OSI

2.2.1. Mô hình TCP/IP

Mô hình TCP/IP là một khái niệm được sử dụng để hiểu các chức năng và quy trình liên quan đến việc truyền dữ liệu qua Internet hoặc bất kỳ mạng nào khác sử dụng giao thức TCP/IP. Nó dựa trên các giao thức được phát triển cho ARPANET (tiền thân của Internet hiện đại) và được sử dụng rộng rãi trong mạng hiện đại.

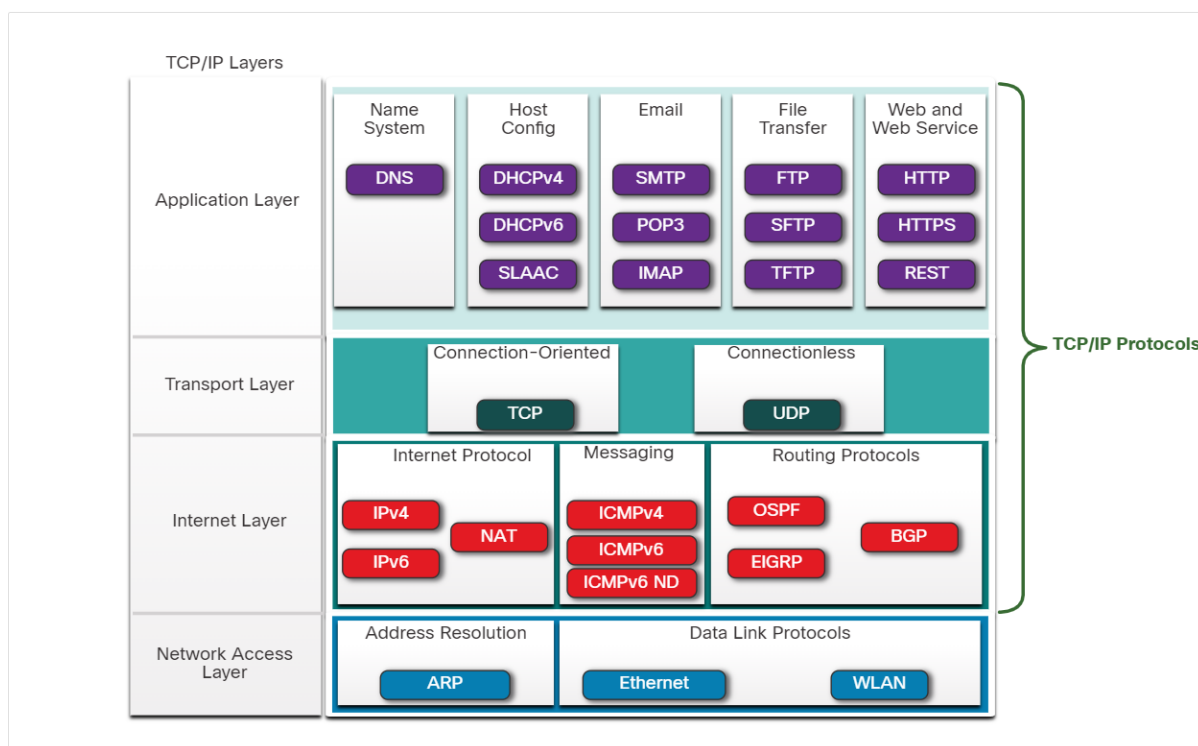
Mô hình TCP/IP được chia làm 4 tầng, mỗi tầng đảm nhận một phần của quá trình giao tiếp và truyền dẫn dữ liệu:

Tầng ứng dụng là giao diện người dùng với mạng. Nó cung cấp các dịch vụ mạng trực tiếp cho người dùng và ứng dụng. Trong tầng này có các thành phần như: DNS để dịch tên miền thành địa chỉ IP, giao thức SMTP cho việc gửi email, FTP để truyền tải file, HTTP cho việc truy cập web, và các giao thức khác.

Tầng vận chuyển quản lý việc đóng gói dữ liệu thành các gói tin và đảm bảo chúng được chuyển giao một cách đáng tin cậy. TCP là giao thức kết nối được sử dụng để truyền dữ liệu một cách tin cậy và đảm bảo gói tin được chuyển giao một cách chính xác. UDP cung cấp giao tiếp không tin cậy, nhưng nhanh hơn.

Tầng internet xử lý việc định tuyến các gói tin qua mạng. IP (IPv4 và IPv6) là giao thức chính của tầng này, xác định cách địa chỉ IP được gán và định tuyến các gói tin.

Tầng truy cập mạng chịu trách nhiệm cho việc truyền dẫn dữ liệu qua các phương tiện vật lý, như cáp Ethernet hoặc Wi-Fi. ARP được sử dụng để ánh xạ địa chỉ IP sang địa chỉ MAC, và các giao thức như Ethernet và WLAN quy định cách truyền dẫn dữ liệu trên các phương tiện vật lý.



Hình 2-1 Các thành phần của mô hình TCP/IP

2.2.2. Mô hình OSI

Mô hình OSI cung cấp một khung nhất quán về các chức năng và dịch vụ có thể xảy ra ở mỗi tầng. Thay vì chỉ định cách thực hiện, nó mô tả những gì cần được thực hiện ở mỗi tầng cụ thể. Các tầng bao gồm:

Tầng vật lý: Quản lý kết nối vật lý giữa các thiết bị, tập trung vào việc truyền dẫn ở mức bit và tín hiệu cơ bản.

Tầng liên kết dữ liệu: Đảm bảo truyền dữ liệu không lỗi giữa các nút, chia dữ liệu thành các khung và xử lý địa chỉ MAC.

Tầng mạng: Tạo điều kiện cho việc truyền dữ liệu qua các mạng khác nhau, xử lý định tuyến gói tin và địa chỉ IP.

Tầng vận chuyển: Quản lý việc giao dịch điểm cuối của tin nhắn, phân đoạn dữ liệu và cung cấp phản hồi và xử lý lỗi.

Tầng phiên: Thiết lập, duy trì và chấm dứt kết nối giữa các hệ thống, đảm bảo đồng bộ hóa và tạo điều kiện cho việc kiểm soát cuộc trò chuyện.

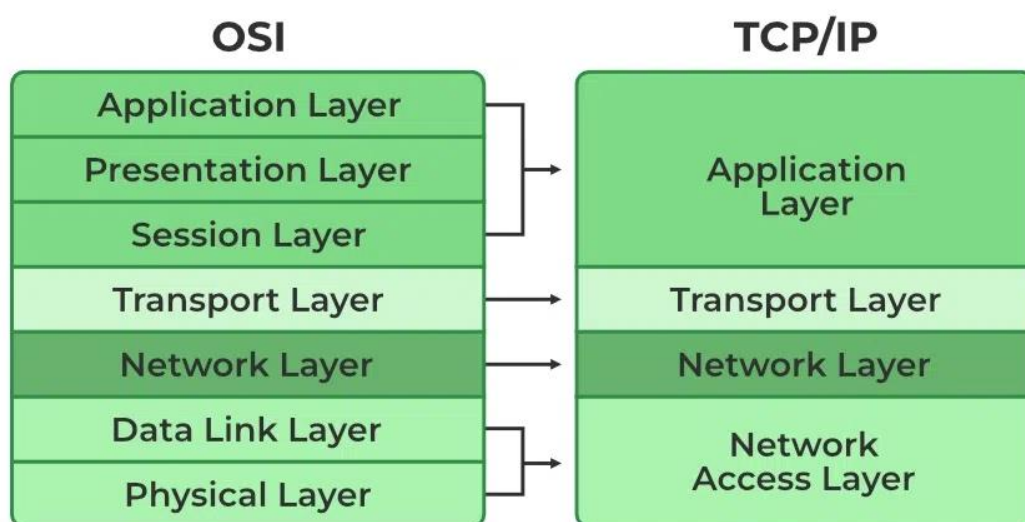
Tầng trình bày: Xử lý định dạng, dịch, mã hóa và nén dữ liệu, chuẩn bị dữ liệu để truyền qua mạng.

Tầng ứng dụng: Đại diện cho giao diện người dùng, cho phép các ứng dụng mạng truy cập vào mạng và hiển thị thông tin đã nhận.

Dữ liệu trong mô hình OSI truyền qua bảy tầng, bắt đầu từ tầng ứng dụng xuống tầng vật lý ở đầu gửi, sau đó đi ngược từ tầng vật lý trở lại tầng ứng dụng ở đầu nhận.

Mô hình OSI có các ưu điểm: Cung cấp một cấu trúc để hiểu quy trình giao tiếp mạng, tiêu chuẩn hóa giao tiếp mạng, tăng cường tương thích, dễ dàng trong việc chẩn đoán và sửa lỗi bằng cách phân tách thành các tầng riêng biệt.

2.2.3. So sánh mô hình OSI với mô hình TCP/IP



Hình 2-2 Sự tương ứng giữa các tầng trong mô hình OSI và mô hình TCP/IP

Giống nhau:

Cả hai mô hình OSI và TCP/IP đều là các mô hình logic quan trọng trong lĩnh vực mạng máy tính. Chúng cùng mô tả cách thông tin được truyền tải giữa các thiết bị trong mạng. Mỗi mô hình đều phân chia quá trình truyền dữ liệu thành các tầng riêng biệt, mỗi tầng có các chức năng và trách nhiệm cụ thể để đảm bảo việc truyền thông hiệu quả. Điểm tương đồng quan trọng khác là cả hai mô hình đều áp dụng khái niệm đóng gói theo đó dữ liệu được đóng gói thành các gói tin chứa thông tin về dữ liệu đang được truyền và các thông tin điều khiển khác, giúp mạng xác định cách xử lý dữ liệu một cách chính xác. Nhờ vào các đặc điểm này, cả hai mô hình OSI và TCP/IP đã trở thành cơ sở quan trọng để hiểu và thiết kế các hệ thống mạng phức tạp trong thế giới kết nối ngày nay.

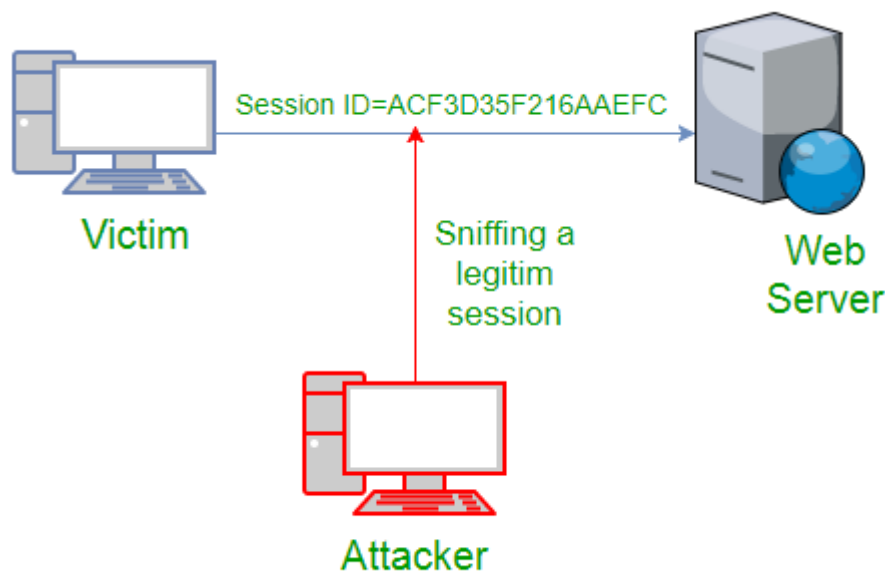
Khác nhau:

Bảng 2-1 So sánh mô hình OSI và mô hình TCP/IP

	Mô hình OSI	Mô hình TCP/IP
Độ tin cậy và phổ biến	Mô hình cũ, chỉ để tham khảo, số người sử dụng hạn chế	Được chuẩn hóa, nhiều người tin cậy và sử dụng phổ biến trên toàn cầu
Phương pháp tiếp cận	Tiếp cận theo chiều dọc	Tiếp cận theo chiều ngang
Sự kết hợp giữa các tầng	Mỗi tầng khác nhau sẽ thực hiện một nhiệm vụ khác nhau, không có sự kết hợp giữa bất cứ tầng nào.	Trong tầng ứng dụng có tầng trình bày và tầng phiên được kết hợp với nhau.
Thiết kế	Phát triển mô hình trước sau đó sẽ phát triển giao thức	Phát triển mô hình trước sau đó sẽ phát triển giao thức
Số tầng	7	4
Truyền thông	Hỗ trợ cả kết nối định tuyến và không dây	Hỗ trợ truyền thông không kết nối từ tầng mạng
Tính phụ thuộc	Các giao thức độc lập với nhau	Phụ thuộc vào giao thức

2.3. Một số vấn đề bảo mật trong giao thức mạng

2.3.1. Nghe trộm gói tin (Sniffing)



Hình 2-3 Nghe trộm gói tin

Kỹ thuật thu thập tất cả các gói dữ liệu truyền qua mạng bằng ứng dụng phần mềm hoặc thiết bị phần cứng được gọi là nghe trộm. Kỹ thuật này nếu được sử dụng bởi những chuyên gia an ninh mạng có thể giúp thu thập thông tin chi tiết về hoạt động mạng và hành vi của người dùng. Từ đó, có thể sử dụng những thông tin này để nâng cao an ninh mạng cho tổ chức. Tuy nhiên, khi được sử dụng bởi các tin tặc độc hại, việc nghe trộm có thể được sử dụng để khởi động các cuộc tấn công nhằm vào các mục tiêu không có phòng bị, gây ra những hậu quả vô cùng nghiêm trọng.

Có thể hiểu, nghe trộm gói tin là hành động chặn và giám sát lưu lượng truy cập trên mạng. Điều này có thể được thực hiện bằng cách sử dụng phần mềm ghi lại tất cả các gói dữ liệu đi qua giao diện mạng nhất định hoặc bằng cách sử dụng các thiết bị phần cứng được thiết kế nhằm cho mục đích này. Cuộc tấn công nghe trộm xảy ra khi kẻ tấn công sử dụng trình nghe lén gói để chặn và đọc dữ liệu nhạy cảm truyền qua mạng. Mục tiêu chung của các cuộc tấn công này bao gồm các email không được mã hóa, thông tin đăng nhập và thông tin tài chính. Trong một số trường hợp, kẻ tấn công cũng có thể sử dụng các công cụ tấn công nghe trộm và trình nghe lén gói để tiêm mã độc vào các gói dữ liệu vô hại nhằm chiếm quyền điều khiển máy tính hoặc các thiết bị khác của nạn nhân.

Có một số cách kẻ tấn công có thể nắm bắt các gói đi qua mạng. Một phương pháp

phổ biến là thiết lập trình nghe gói tin trên máy tính được kết nối với mạng của kẻ tấn công. Máy tính này hoạt động như một proxy giữa các thiết bị được nhắm mục tiêu và phần còn lại, cho phép kẻ tấn công nắm bắt được tất cả lưu lượng truy cập đi qua.

Một kỹ thuật phổ biến khác là đầu độc ARP, trong đó kẻ tấn công đánh lừa các thiết bị trên mạng khiến chúng nghĩ rằng chúng đang giao tiếp với một thiết bị khác trong khi thực tế không phải vậy. Điều này cho phép kẻ tấn công chặn và đọc tất cả lưu lượng truy cập giữa hai thiết bị.

Có hai loại tấn công đánh hơi chính: thụ động và chủ động.

Nghe trộm thụ động:

Trong một cuộc tấn công nghe trộm thụ động, hacker giám sát lưu lượng truy cập đi qua mạng mà không can thiệp dưới bất kỳ hình thức nào. Kiểu tấn công này có thể có lợi cho việc thu thập thông tin về các mục tiêu trên mạng và loại dữ liệu (ví dụ: thông tin xác thực đăng nhập, tin nhắn email) mà chúng đang truyền tải. Bởi vì nó không liên quan đến bất kỳ sự can thiệp nào vào hệ thống mục tiêu nên nó cũng ít gây nghi ngờ hơn các loại tấn công khác.

Nghe trộm chủ động:

Nghe trộm chủ động là một kiểu tấn công liên quan đến việc gửi các gói được tạo thủ công đến một hoặc nhiều mục tiêu trên mạng để trích xuất dữ liệu nhạy cảm. Bằng cách sử dụng các gói được chế tạo đặc biệt, kẻ tấn công thường có thể bỏ qua các biện pháp bảo mật vốn có thể bảo vệ dữ liệu khỏi bị chặn. Hoạt động đánh hơi cũng có thể liên quan đến việc tiêm mã độc vào hệ thống mục tiêu, cho phép kẻ tấn công chiếm quyền kiểm soát chúng hoặc đánh cắp thông tin nhạy cảm.

Một cuộc tấn công đánh hơi thành công có thể gây ra một số hậu quả nghiêm trọng cho mục tiêu. Chúng có thể bao gồm: Mất dữ liệu nhạy cảm, chẳng hạn như thông tin đăng nhập, thông tin tài chính và email, tiêm mã độc vào hệ thống mục tiêu, cho phép kẻ tấn công kiểm soát thiết bị hoặc truy cập thông tin nhạy cảm, gián đoạn lưu lượng mạng, có thể gây ra sự cố liên lạc và làm chậm hiệu suất mạng, tiết lộ thông tin bí mật, chẳng hạn như bí mật thương mại và dữ liệu độc quyền, thiệt hại về danh tiếng của tổ chức có mạng lưới bị xâm phạm.

Một số biện pháp chính để bảo vệ mạng khỏi các cuộc tấn công nghe trộm bao gồm:

Mã hóa dữ liệu nhạy cảm để bảo vệ khỏi các cuộc tấn công nghe trộm vì dù kẻ tấn công có lấy được dữ liệu đi chăng nữa nhưng nếu chúng không thể giải mã thì dữ liệu mà chúng lấy được cũng trở nên vô dụng.

Không bao giờ gửi thông tin nhạy cảm qua kết nối không được mã hóa. Điều này, có thể giúp tránh được sự nghe trộm của tin tặc, vì dữ liệu nhạy cảm vô cùng quan trọng, nên việc bảo đảm cho những thông tin này không rò rỉ là hành động cần thiết và thường xuyên.

Đảm bảo rằng tất cả các máy tính trên mạng đều được bảo vệ đầy đủ bằng phần mềm chống vi-rút và tường lửa. Điều này giúp hạn chế được phần mềm độc hại mà tin tặc có thể cài đặt trên máy tính của người dùng.

Thường xuyên cập nhật tất cả các phần mềm và thiết bị với các bản vá bảo mật mới nhất. Vì các phần mềm và hệ điều hành thường xuyên có các lỗ hổng bảo mật mà tin tặc có thể khai thác. Nhà sản xuất phần mềm phát hành các bản vá bảo mật để khắc phục những lỗ hổng này. Việc cập nhật đảm bảo rằng hệ thống được bảo vệ khỏi các mối đe dọa mới nhất.

Sử dụng VPN khi kết nối với mạng Wi-Fi công cộng. Vì mạng Wi-Fi công cộng thường không an toàn và dễ bị tin tặc tấn công. Sử dụng VPN giúp mã hóa dữ liệu, làm cho việc đánh cắp thông tin trở nên khó khăn hơn.

Liên tục theo dõi mạng để phát hiện hoạt động bất thường. Việc giám sát liên tục giúp phát hiện sớm các mối đe dọa và phản ứng kịp thời để ngăn chặn thiệt hại. Hoạt động bất thường có thể là dấu hiệu của một cuộc tấn công đang diễn ra.

2.3.2. Giả mạo (Spoofing)

Giả mạo là khi tội phạm mạng giả dạng thành một cá nhân, doanh nghiệp hoặc tổ chức để thực hiện hành vi độc hại nhằm chiếm lợi ích bất hợp pháp. Các tội phạm mạng sử dụng nhiều chiến thuật khác nhau để giả mạo danh tính của cá nhân, doanh nghiệp hoặc tổ chức, từ địa chỉ email, trang web hoặc số điện thoại giả mạo đến các chiến lược nâng cao hơn như giả mạo địa chỉ IP, Máy chủ tên miền (DNS) hoặc Giao thức phân giải địa chỉ (ARP). Bất kể chiến thuật được sử dụng là gì, mục tiêu của lừa đảo giả mạo là đánh cắp lợi ích của nạn nhân có thể là thông tin nhạy cảm hoặc tài sản và làm tổn hại danh tiếng của họ. Tội phạm mạng tận dụng các thủ đoạn kỹ thuật xã hội phổ biến và sử dụng địa chỉ

email, trang web hoặc số điện thoại giả để lừa nạn nhân tiết lộ thông tin bí mật, tải xuống tệp đính kèm hoặc nhấp vào liên kết cài đặt phần mềm độc hại.

Những kẻ lừa đảo xoa dịu sự nghi ngờ của nạn nhân thông thường bằng cách giả dạng các thực thể mà hầu hết mọi người đều quen thuộc như các thương hiệu nổi tiếng, các tổ chức tài chính, thậm chí là bạn bè hoặc người thân của nạn nhân. Kết quả là, sự cảnh giác của họ bị mất, khiến họ có thể bị lợi dụng.

Cuộc tấn công giả mạo nhắm vào giao thức mạng được hiểu là một dạng tấn công trong đó kẻ tấn công giả mạo giao thức mạng để đánh lừa các hệ thống hoặc người dùng. Có nhiều giao thức mạng khác nhau có thể bị tấn công spoofing, có thể kể đến như:

Giả mạo ARP (ARP Spoofing)

ARP Spoofing là một dạng tấn công mạng trong đó kẻ tấn công gửi các thông điệp ARP giả mạo trên mạng cục bộ. Mục tiêu là liên kết địa chỉ MAC của kẻ tấn công với địa chỉ IP của một máy tính hợp lệ trên mạng. Khi đã thực hiện thành công, kẻ tấn công có thể chặn, thay đổi hoặc ngăn chặn lưu lượng mạng giữa các thiết bị.

Để thực hiện cuộc tấn công này, kẻ tấn công gửi gói tin ARP giả mạo đến các thiết bị trên mạng, gán địa chỉ MAC của chúng với địa chỉ IP của thiết bị mục tiêu. Các thiết bị trên mạng cập nhật bảng ARP của chúng với thông tin giả mạo. Lưu lượng mạng dành cho thiết bị mục tiêu bị chuyển hướng đến kẻ tấn công. Từ đó, kẻ tấn công có thể ngăn chặn, thay đổi lưu lượng mạng giữa các thiết bị trong hệ thống. Hậu quả là kẻ tấn công có thể chặn và thay đổi các gói tin giữa các thiết bị trên mạng, đánh cắp thông tin nhạy cảm như mật khẩu, thông tin tài chính, hoặc dữ liệu cá nhân, hay chèn mã độc vào các gói tin, dẫn đến việc lây nhiễm phần mềm độc hại trên các thiết bị mục tiêu, hoặc ngăn chặn lưu lượng mạng giữa các thiết bị, gây gián đoạn dịch vụ hoặc làm cho các thiết bị không thể giao tiếp với nhau, dữ liệu của nạn nhân có thể bị mất hoặc hỏng hóc do các gói tin bị thay đổi hoặc chặn.

Giả mạo DNS (DNS Spoofing)

DNS Spoofing (hay DNS cache poisoning) là một kỹ thuật mà kẻ tấn công thay đổi thông tin DNS để điều hướng người dùng đến một trang web giả mạo. Điều này có thể dẫn đến việc người dùng truy cập vào các trang web giả mạo mà họ tin là thật, từ đó kẻ tấn công có thể đánh cắp thông tin cá nhân hoặc cài đặt phần mềm độc hại.

Để thực hiện cuộc tấn công này, kẻ tấn công gửi các gói tin DNS giả mạo đến máy chủ DNS hoặc người dùng, cung cấp địa chỉ IP sai cho một tên miền hợp lệ. Tiếp theo, máy chủ DNS hoặc người dùng cập nhật thông tin DNS với địa chỉ IP giả mạo. Sau đó người dùng sẽ bị chuyển hướng đến trang web giả mạo khi truy cập tên miền hợp lệ. Hậu quả là nạn nhân có thể bị chuyển hướng đến trang web giả mạo, nơi họ có thể bị đánh cắp thông tin cá nhân hoặc tài chính, các trang web này có thể chứa phần mềm độc hại, lây nhiễm vào máy tính của người dùng khi họ truy cập.

Giả mạo IP (IP Spoofing)

Giả mạo IP là khi kẻ tấn công giả mạo địa chỉ IP nguồn trong gói tin mạng để che giấu danh tính của mình hoặc để giả mạo một máy tính hợp lệ. Kỹ thuật này thường được sử dụng trong các cuộc tấn công từ chối dịch vụ (DDoS) và các cuộc tấn công xâm nhập mạng.

Để thực hiện cuộc tấn công này, kẻ tấn công tạo ra các gói tin mạng với địa chỉ IP nguồn giả mạo. Sau đó chúng gửi các gói tin này đến mục tiêu, làm cho máy tính mục tiêu tin rằng các gói tin đến từ một nguồn hợp lệ. Sau đó máy tính mục tiêu xử lý các gói tin giả mạo này theo cách thông thường. Hậu quả là kẻ tấn công có thể sử dụng IP spoofing để gửi lưu lượng lớn đến một máy chủ mục tiêu, gây quá tải và làm gián đoạn dịch vụ, hoặc IP spoofing có thể được sử dụng để vượt qua các biện pháp bảo mật và xâm nhập vào mạng nội bộ của một tổ chức, chúng cũng có thể khiến hệ thống bảo mật dựa trên địa chỉ IP bị đánh lừa, cho phép kẻ tấn công truy cập vào các tài nguyên mà họ không được phép gây ra thiệt hại to lớn về tài chính.



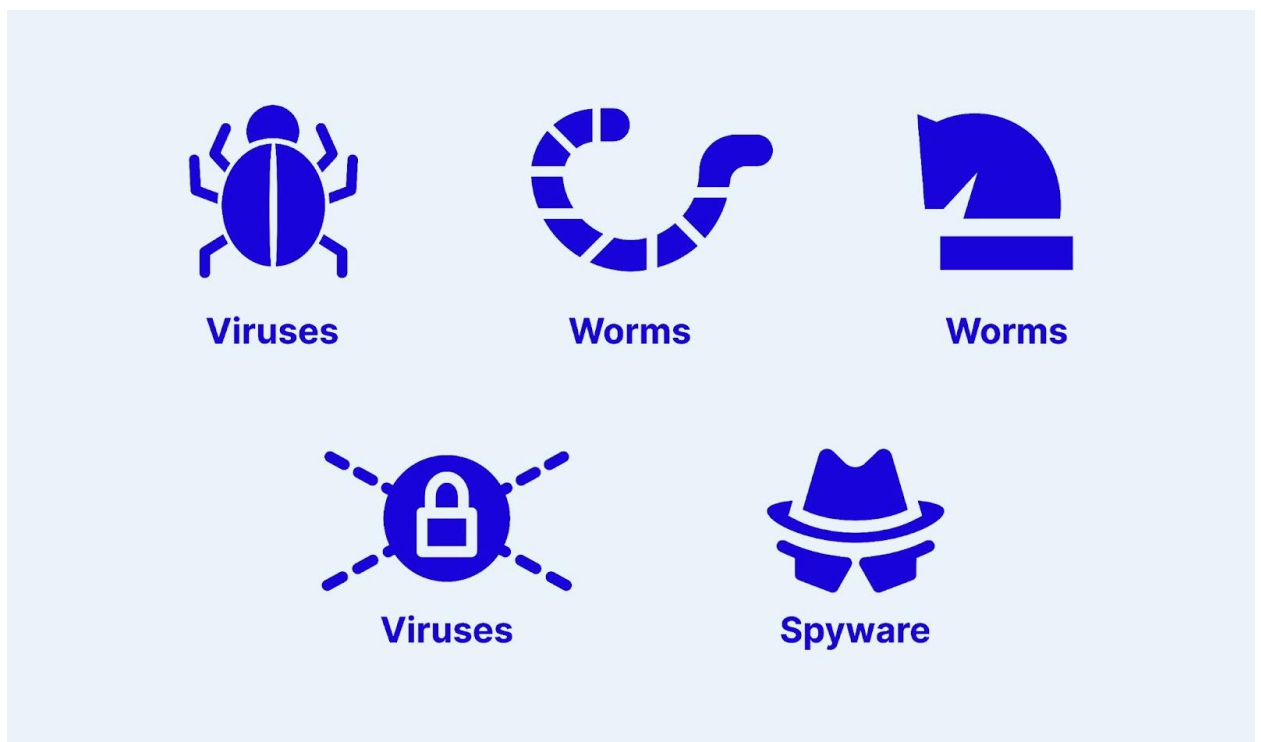
Hình 2-4: Một số loại tấn công giả mạo phổ biến

2.3.3. Phần mềm độc hại (malware)

Phần mềm độc hại là các phần mềm xâm nhập do các tin tặc phát triển để đánh cắp dữ liệu và làm hỏng hoặc phá hủy máy tính và hệ thống máy tính. Chúng được các tin tặc phát triển như một loại phần mềm có hại nhằm xâm nhập hoặc làm hỏng mạng máy tính của nạn nhân. Mục tiêu của chúng là gây rối loạn và đánh cắp thông tin hoặc tài nguyên vì mục đích tài chính hoặc để phá hoại. Chúng có thể xâm nhập và thu thập dữ liệu như email, kế hoạch và đặc biệt là thông tin nhạy cảm như mật khẩu. Điều này giúp kẻ tấn công tiếp cận và kiểm soát các thông tin quan trọng của cá nhân hoặc tổ chức, từ đó có thể thực hiện các hành động xấu xa hơn. Một trong những phương pháp phổ biến mà chúng sử dụng là

làm gián đoạn và tống tiền. Chúng có thể khóa các mạng và máy tính, làm cho hệ thống mạng và máy tính không thể sử dụng được. Khi nó chiếm quyền điều khiển máy tính, khiến máy tính của nạn nhân trở thành “con tin” và yêu cầu tiền chuộc để khôi phục quyền truy cập, nó được gọi là ransomware. Ngoài ra, chúng có thể phá hủy hệ thống máy tính, làm hỏng cơ sở hạ tầng mạng, gây ra tổn thất nghiêm trọng và làm gián đoạn hoạt động của tổ chức. Bên cạnh đó, chúng còn có thể ăn cắp tài nguyên máy tính bằng cách sử dụng sức mạnh tính toán để chạy các botnet (một tập hợp các rô bốt phần mềm hoặc các rô bốt hoạt động một cách tự chủ), chương trình khai thác tiền điện tử hoặc gửi email spam. Việc này không chỉ làm giảm hiệu suất máy tính mà còn sử dụng tài nguyên của nạn nhân cho các mục đích độc hại. Cuối cùng, chúng có thể kiếm tiền bằng cách bán tài sản trí tuệ của tổ chức trên web đen, từ đó thu lợi bất chính từ việc đánh cắp các thông tin nhạy cảm.

Một số loại phần mềm độc hại phổ biến:



Hình 2-5 Một số phần mềm độc hại phổ biến

Virus là phần mềm độc hại gắn vào các chương trình hoặc tệp tin hợp pháp và lây lan khi các tệp này được chia sẻ. Virus có thể gây hại bằng cách phá hủy dữ liệu hoặc làm hỏng hệ thống.

Worm là phần mềm độc hại tự sao chép và lây lan qua mạng mà không cần tệp chủ. Chúng có thể làm quá tải mạng và hệ thống, gây ra sự cố hoặc ngừng hoạt động.

Trojan Horse là phần mềm độc hại giả mạo là phần mềm hợp pháp để đánh lừa người dùng cài đặt. Một khi được cài đặt, Trojan có thể cho phép kẻ tấn công truy cập từ xa vào hệ thống, đánh cắp thông tin hoặc cài đặt thêm các phần mềm độc hại khác.

Ransomware là phần mềm độc hại mã hóa tệp tin hoặc khóa hệ thống, sau đó yêu cầu tiền chuộc từ nạn nhân để khôi phục quyền truy cập. Đây là một trong những loại malware nguy hiểm nhất hiện nay.

Spyware là phần mềm độc hại theo dõi và thu thập thông tin của người dùng mà họ không hề hay biết. Nó có thể ghi lại hoạt động bàn phím, chụp màn hình hoặc theo dõi lịch sử duyệt web để đánh cắp thông tin cá nhân.

Adware là phần mềm độc hại hiển thị quảng cáo không mong muốn trên thiết bị của người dùng. Dù không nguy hiểm như các loại phần mềm độc hại khác, nhưng nó có thể làm phiền và làm giảm hiệu suất của thiết bị.

Rootkit là một loại malware được thiết kế để giấu sự hiện diện của nó và các chương trình độc hại khác. Rootkit thay đổi hệ điều hành để tránh bị phát hiện bởi các phần mềm bảo mật, cho phép kẻ tấn công duy trì quyền truy cập vào hệ thống.

Keylogger là phần mềm độc hại ghi lại các phím bấm trên bàn phím và gửi thông tin này cho kẻ tấn công. Nó thường được sử dụng để đánh cắp mật khẩu, thông tin đăng nhập và các thông tin nhạy cảm khác.

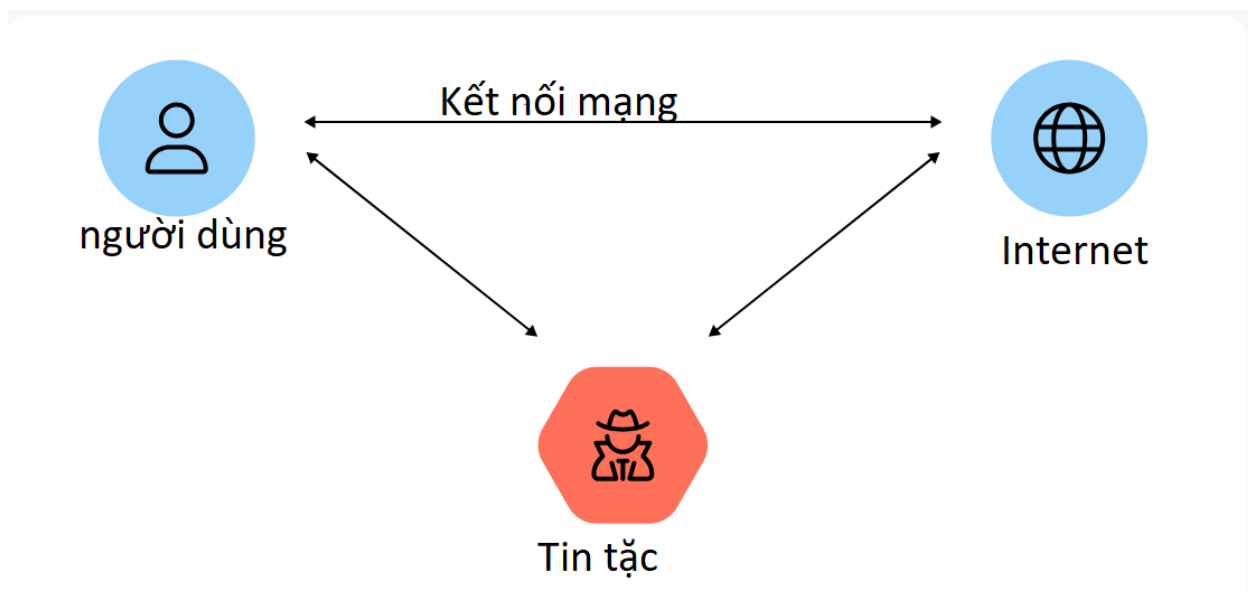
Cryptojacking là hành vi sử dụng trái phép tài nguyên máy tính của người khác để khai thác tiền điện tử. Nó có thể làm giảm hiệu suất hệ thống và tăng chi phí điện năng.

2.3.4. Tấn công xen giữa (man-in-the-middle)

Tấn công xen giữa (man-in-the-middle) là một loại tấn công mạng trong đó kẻ tấn công ngấm lầy và chuyển tiếp tin nhắn giữa hai bên tin rằng họ đang trực tiếp giao tiếp với nhau. Đây là một hình thức nghe trộm, trong đó kẻ tấn công ngắt và kiểm soát toàn bộ cuộc trò chuyện. Điều này cho phép các cuộc tấn công giám sát, can thiệp và thậm chí thay đổi việc trao đổi dữ liệu mà không bị phát hiện.

Các cuộc tấn công xen giữa thường liên quan đến việc đánh cắp thông tin nhạy cảm như thông tin đăng nhập của người dùng, chi tiết tài khoản ngân hàng hoặc số thẻ tín dụng. Các phương pháp thường được sử dụng bao gồm đánh cắp thông tin để thay đổi hoặc chen các gói mạng, lừa đảo người dùng để tiết lộ thông tin cá nhân thông qua kỹ thuật hack vào

trình duyệt web hoặc ứng dụng di động. năng động.



Hình 2-6 Tấn công xen giữa (Man-in-the-middle)

Một trong những kiểu tấn công xen giữa phổ biến nhất là tấn công man-in-the-browser, trong đó kẻ tấn công kiểm soát trực tiếp các hoạt động trên trình duyệt của nạn nhân. Chúng có thể tiêm phần mềm độc hại vào trình duyệt để ghi lại thông tin đăng nhập, thay đổi nội dung trang web ngân hàng hoặc thậm chí không cho phép giao dịch.

Để bảo vệ khỏi các cuộc tấn công xen giữa, người dùng cần triển khai các giải pháp bảo mật như sử dụng kết nối an toàn chẳng hạn như HTTPS, cập nhật tổ chức và quản lý cẩn thận phần mềm bảo mật cũng như các giới hạn. Tránh truy cập tất cả các liên kết hoặc gửi thông tin cá nhân qua các mạng không bảo mật.

2.3.5. Zero-day

Các cuộc tấn công zero-day là mối đe dọa bảo mật mạng nghiêm trọng, liên quan đến các lỗ hổng trong phần mềm được tin tặc khai thác trước khi các nhà phát triển có thể vá lỗi. Thuật ngữ "zero-day" chỉ ra rằng các nhà phát triển không có thời gian để sửa chữa lỗ hổng khi chúng được phát hiện bởi những kẻ tấn công. Những lỗ hổng này thu hút sự chú ý của tin tặc vì chúng cung cấp cửa sổ thời gian để xâm nhập vào hệ thống mà không bị phát hiện, có thể gây ra thiệt hại nghiêm trọng như đánh cắp dữ liệu hoặc xâm nhập vào hệ thống.

Việc khai thác một lỗ hổng zero-day thường bao gồm tạo và triển khai mã khai thác, tận dụng điểm yếu bảo mật trong phần mềm. Tin tặc thường sử dụng các chiến lược kỹ

thuật xã hội như email lừa đảo để phát tán phần mềm độc hại sử dụng các lỗ hổng này. Khi một hệ thống bị xâm nhập, tin tặc có thể đánh cắp dữ liệu nhạy cảm, cài đặt ransomware, hoặc sử dụng hệ thống bị nhiễm để thực hiện các cuộc tấn công mạng.

Phát hiện các cuộc tấn công zero-day là thách thức bởi vì những lỗ hổng này là mới và chưa được các chuyên gia an ninh mạng biết đến cho đến khi chúng bị khai thác. Các phương pháp truyền thống dựa vào phân tích hành vi và phát hiện bất thường để nhận diện các mẫu đáng ngờ trong lưu lượng mạng hoặc hành vi hệ thống. Ngoài ra, các thuật toán học máy ngày càng được sử dụng để phân tích các tập dữ liệu lớn và phát hiện sự khác biệt so với hành vi bình thường của hệ thống, có thể chỉ ra sự tồn tại của một cuộc tấn công zero-day đang diễn ra.

Các mục tiêu của các cuộc tấn công zero-day có sự đa dạng và có thể bao gồm cá nhân, doanh nghiệp, cơ quan chính phủ và cơ sở hạ tầng quan trọng. Tin tặc có thể nhắm đến các tổ chức cụ thể để đạt được lợi ích tài chính, gián điệp hoặc vì mục đích chính trị, hoặc họ có thể thực hiện các cuộc tấn công không nhắm mục tiêu nhằm vào việc xâm nhập vào càng nhiều hệ thống có lỗ hổng càng tốt.

Để đối phó với các mối đe dọa từ các cuộc tấn công zero-day, các tổ chức cần áp dụng các biện pháp an ninh chủ động, bao gồm cập nhật phần mềm định kỳ, giám sát mạng, giáo dục người dùng về nhận diện email lừa đảo và triển khai các công nghệ phát hiện mối đe dọa tiên tiến. Hợp tác với các chuyên gia an ninh mạng và cập nhật thông tin về các mối đe dọa mới cũng rất quan trọng để giảm thiểu rủi ro từ các cuộc tấn công zero-day.

2.4. Bảo mật trong các giao thức cơ bản: DHCP, ARP và DNS

2.4.1. Giao thức DHCP

2.4.1.1 Tổng quan về DHCP

IP là một phần quan trọng của cơ sở hạ tầng mạng hiện đại, cho phép các thiết bị trong mạng có thể nhận dạng và giao tiếp với nhau thông qua một địa chỉ duy nhất. Mỗi thiết bị kết nối vào mạng cần có một địa chỉ IP để được nhận diện và truy cập vào các dịch vụ mạng khác nhau. Đây là lý do tại sao IP ra đời và trở thành tiêu chuẩn quan trọng trong việc xác định các thiết bị trên Internet và các mạng nội bộ.

Để cấp phát IP cho từng máy tính, có hai phương pháp chính: cấp phát địa chỉ IP tĩnh và cấp phát địa chỉ IP động thông qua DHCP. Cấp phát tĩnh yêu cầu người quản trị

mạng phải gán địa chỉ IP thủ công cho từng thiết bị. Nếu sử dụng cách này, người quản trị mạng sẽ phải gán địa chỉ IP thủ công cho từng thiết bị. Điều này có thể gây ra rất nhiều rắc rối, chẳng hạn như:

Gây lãng phí thời gian: Việc phải thủ công cấu hình địa chỉ IP cho từng thiết bị trong mạng là một quá trình tốn thời gian và công sức. Đối với các mạng lớn với hàng trăm hoặc thậm chí hàng nghìn thiết bị, việc này có thể trở nên rất phức tạp và không hiệu quả.

Gây xung đột địa chỉ IP: Nếu không cẩn thận trong quản lý, có thể xảy ra xung đột địa chỉ IP. Điều này có thể xảy ra khi người quản trị gán một địa chỉ IP đã được sử dụng cho một thiết bị khác, dẫn đến sự cố khiến thiết bị được cấp phát địa chỉ IP trước đó không thể truy cập mạng và khó khăn trong việc xác định nguyên nhân.

Khó quản lý và theo dõi: Việc quản lý các địa chỉ IP tĩnh yêu cầu người quản trị phải thường xuyên cập nhật và theo dõi danh sách các địa chỉ đã được cấp phát. Điều này có thể gây ra sự nhầm lẫn và khó khăn trong việc bảo trì mạng.

Di chuyển thiết bị: Khi một thiết bị cần di chuyển đến một vị trí khác trong mạng, người quản trị phải thực hiện lại cấu hình địa chỉ IP cho thiết bị đó. Việc này không chỉ tốn thời gian mà còn có thể gây ra sự gián đoạn trong hoạt động của thiết bị và dịch vụ mạng.

Để giải quyết vấn đề này, người quản trị thường sử dụng DHCP để thay thế. DHCP là một giao thức quản lý mạng được sử dụng để tự động cấp phát địa chỉ IP cho các thiết bị hoặc nút trên mạng để chúng có thể giao tiếp sử dụng địa chỉ IP. DHCP tự động hóa và quản lý trung tâm các cấu hình này thay vì yêu cầu các quản trị mạng phải gán địa chỉ IP thủ công cho tất cả các thiết bị trên mạng.

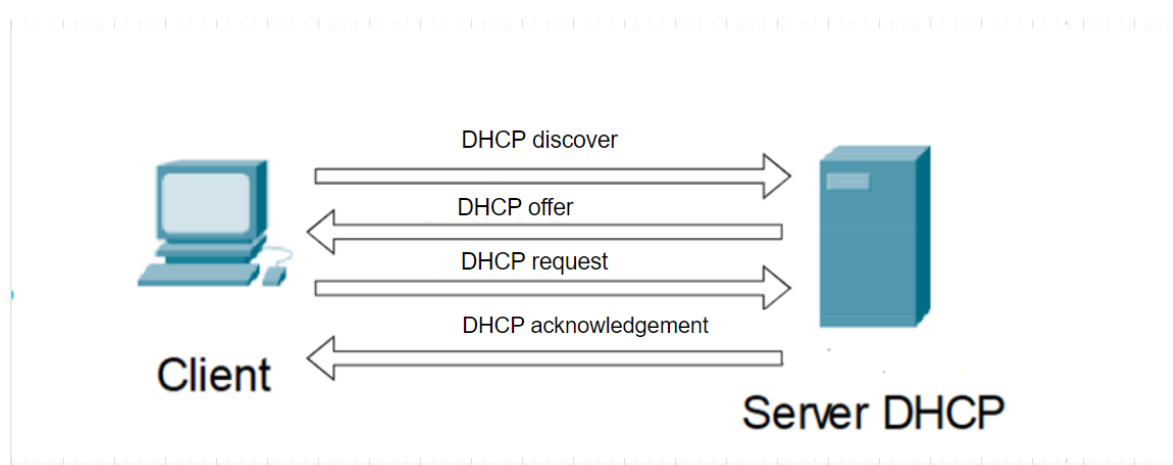
DHCP có thể triển khai trên các mạng cục bộ nhỏ cũng như các mạng doanh nghiệp lớn. Giao thức này cấp phát địa chỉ IP mới tại mỗi vị trí khi các thiết bị được di chuyển từ một nơi sang nơi khác trên mạng. Điều này có nghĩa là các quản trị mạng không cần phải cấu hình thủ công cho từng thiết bị với một địa chỉ IP hợp lệ hoặc cấu hình lại thiết bị với một địa chỉ IP mới nếu nó di chuyển đến vị trí mới trên mạng.

Có phiên bản của DHCP để sử dụng trong IPv4 và IPv6. IPv6 trở thành tiêu chuẩn ngành vào năm 2017 – gần 20 năm sau khi các thông số kỹ thuật của nó được công bố lần đầu. Mặc dù tỷ lệ sử dụng IPv6 ban đầu thấp, vào tháng 7 năm 2019, hơn 29% người dùng Google đã sử dụng IPv6 để truy vấn.

DHCP hoạt động tại tầng ứng dụng của mô hình TCP/IP. Nó tự động gán địa chỉ IP cho các máy khách DHCP và phân phối thông tin cấu hình TCP/IP cho các máy khách DHCP. Thông tin này bao gồm thông tin về subnet mask, địa chỉ IP, cổng mặc định và địa chỉ hệ thống tên miền DNS.

DHCP là một giao thức client-server, trong đó các máy chủ quản lý một tập hợp các địa chỉ IP duy nhất, cũng như thông tin về các tham số cấu hình máy khách. Các máy chủ sau đó gán địa chỉ từ các tập hợp địa chỉ đó. Các máy khách được kích hoạt DHCP sẽ gửi yêu cầu tới máy chủ DHCP mỗi khi chúng kết nối với mạng.

Các máy khách được cấu hình với DHCP sẽ phát đi một yêu cầu tới máy chủ DHCP và yêu cầu thông tin cấu hình mạng cho mạng cục bộ mà chúng kết nối. Một máy khách thường phát đi một truy vấn cho thông tin này ngay sau khi khởi động. Máy chủ DHCP đáp ứng yêu cầu của máy khách bằng cách cung cấp thông tin cấu hình IP đã được chỉ định trước bởi quản trị viên mạng. Thông tin này bao gồm một địa chỉ IP cụ thể, cũng như một khoảng thời gian – còn gọi là lease – mà việc phân bổ có hiệu lực. Cụ thể hơn, quá trình này gồm 4 bước chính. Khi máy khách kết nối vào mạng, nó tự động gửi một gói tin DHCP discover để tìm máy chủ DHCP phù hợp. Máy chủ DHCP nhận được yêu cầu và đáp lại bằng một gói tin DHCP offer chứa địa chỉ IP được đề xuất cho máy khách. Sau khi nhận gói tin này, máy khách gửi một gói tin DHCP request để xác nhận và yêu cầu sử dụng địa chỉ IP đã được chấp nhận từ máy chủ DHCP. Cuối cùng, máy chủ DHCP gửi một gói tin DHCP acknowledgement để xác nhận rằng việc cấp phát địa chỉ IP đã hoàn tất.



Hình 2-7 Quá trình cấp phát địa chỉ IP thông qua DHCP

Khi làm mới việc gán địa chỉ, một máy khách DHCP yêu cầu cùng các tham số đó, nhưng máy chủ DHCP có thể gán một địa chỉ IP mới dựa trên các luật được thiết lập bởi

quản trị viên. Các máy khách DHCP cũng có thể được cấu hình trên giao diện Ethernet.

Máy chủ DHCP quản lý một hồ sơ của tất cả các địa chỉ IP mà nó phân bổ cho các nút mạng. Nếu một nút được di chuyển trong mạng, máy chủ xác định nó bằng cách sử dụng địa chỉ MAC của nó, điều này ngăn chặn việc cấu hình nhầm nhiều thiết bị với cùng một địa chỉ IP. Việc cấu hình một máy chủ DHCP cũng yêu cầu tạo một tệp cấu hình, trong đó lưu trữ thông tin mạng cho các máy khách.

DHCP không phải là một giao thức có khả năng định tuyến, cũng không phải là một giao thức an toàn. DHCP bị giới hạn trong một mạng cục bộ cụ thể, điều này có nghĩa là một máy chủ DHCP duy nhất trên mỗi mạng LAN là đủ – hoặc hai máy chủ để sử dụng trong trường hợp dự phòng. Các mạng lớn hơn có thể có một mạng diện rộng (WAN) chứa nhiều địa điểm riêng lẻ. Tùy thuộc vào các kết nối giữa các điểm này và số lượng máy khách tại mỗi địa điểm, nhiều máy chủ DHCP có thể được thiết lập để xử lý việc phân phối địa chỉ.

Nếu các quản trị viên mạng muốn một máy chủ DHCP cung cấp địa chỉ cho nhiều mạng con trên một mạng nhất định, họ phải cấu hình các dịch vụ chuyển tiếp DHCP được đặt trên các bộ định tuyến kết nối mà các yêu cầu DHCP phải đi qua. Các điểm trung chuyển này chuyển tiếp các thông điệp giữa các máy khách DHCP và các máy chủ đặt trên các mạng con khác nhau.

DHCP không có bất kỳ cơ chế tích hợp nào cho phép các máy khách và máy chủ xác thực lẫn nhau. Do đó cả hai đều dễ bị đánh lừa. Điều này có nghĩa là khi một máy khách gửi yêu cầu để nhận địa chỉ IP, máy chủ không thể xác định chính xác liệu yêu cầu đó có thực sự đến từ một máy khách hợp lệ hay không. Ngược lại, máy khách cũng không thể biết chắc chắn rằng phản hồi nó nhận được là từ một máy chủ hợp lệ. Việc này gây ra một lỗ hổng nghiêm trọng, một máy tính có thể giả mạo làm máy chủ DHCP, gửi các phản hồi DHCP giả mạo tới các máy khách, khiến chúng nhận địa chỉ IP và thông tin cấu hình sai lệch. Điều này có thể dẫn đến việc máy khách bị chuyển hướng đến các trang web giả mạo hoặc bị chặn truy cập vào mạng thực sự. Hay các máy khách giả mạo có thể liên tục gửi yêu cầu DHCP tới máy chủ với mục đích làm cạn kiệt tập hợp địa chỉ IP có sẵn của máy chủ. Khi tất cả các địa chỉ IP đã được phân phát, các máy khách hợp lệ sẽ không thể nhận được địa chỉ IP, gây ra một cuộc tấn công từ chối dịch vụ.

Mặc dù DHCP rất hữu ích trong việc tự động cấu hình địa chỉ IP cho các thiết bị

mạng, nhưng nó cũng dễ bị lợi dụng nếu không có các biện pháp bảo mật bổ sung. Điều này đòi hỏi các quản trị viên mạng phải thực hiện các biện pháp bảo mật và xác thực thiết bị để bảo vệ mạng của họ khỏi các tấn công.

2.4.1.2 Các vấn đề bảo mật trong DHCP và giải pháp bảo mật

DHCP Starvation:

Cuộc tấn công DHCP starvation nhằm đến làm cho máy chủ DHCP bị cạn kiệt các địa chỉ IP có sẵn. Kẻ tấn công thực hiện cuộc tấn công này bằng cách gửi một lượng lớn các thông điệp DHCP Discover giả mạo với các địa chỉ MAC được giả mạo. Kết quả là, máy chủ DHCP sẽ gửi lại một thông điệp DHCP Offer cho mỗi thông điệp DHCP Discover đã nhận được trước đó.

Do đó, tất cả các địa chỉ IP sẵn có sẽ nhanh chóng bị dành riêng cho các máy khách DHCP của kẻ tấn công, và tình trạng này sẽ kéo dài trong một khoảng thời gian nhất định. Vì không có các máy khách thực sự tồn tại, máy chủ DHCP sẽ không nhận được thông điệp DHCP Request từ bất kỳ máy khách nào.

Trong thời gian này, được gọi là starvation, máy chủ DHCP sẽ không thể phục vụ được cho người dùng mạng yêu cầu thông tin IP từ máy chủ DHCP.

Ngoài ra, khi tài nguyên của máy chủ DHCP bị cạn kiệt, một máy chủ DHCP giả mạo có thể được khởi động trên thiết bị của kẻ tấn công mà không gặp phải bất kỳ sự cạnh tranh nào khi người dùng bình thường cố gắng kết nối với một máy chủ DHCP. Điều này có thể dẫn đến một cuộc tấn công DHCP spoofing.

Để ngăn chặn cuộc tấn công DHCP starvation, có thể triển khai các biện pháp bảo mật như tính năng bảo mật cổng trên switch, giới hạn số lượng địa chỉ MAC được phép trên mỗi cổng và thiết lập hành động như tắt cổng khi phát hiện vi phạm.

DHCP spoofing:

DHCP spoofing là kỹ thuật tấn công mạng, trong đó kẻ tấn công giả mạo một máy chủ DHCP hoặc trung gian để phân phối các thông tin cấu hình IP sai lệch cho các thiết bị trong mạng. Mục đích của kỹ thuật này thường là để kiểm soát lưu lượng mạng hoặc thực hiện các cuộc tấn công khác.

Khi kẻ tấn công vận hành một máy chủ DHCP giả mạo, người dùng có thể bắt đầu

giao tiếp DHCP với kẻ tấn công thay vì máy chủ DHCP hợp lệ trên mạng mà không hề hay biết. Điều này thường xảy ra khi máy chủ DHCP giả mạo đặt gần hơn với máy khách DHCP và phản hồi nhanh hơn máy chủ DHCP hợp lệ.

Kết quả là, kẻ tấn công có thể thực hiện cuộc tấn công xen giữa bằng cách tự chỉ định mình làm cổng mặc định hoặc máy chủ DNS trong các phản hồi DHCP gửi lại cho các máy khách DHCP. Điều này cho phép kẻ tấn công ngăn chặn giao tiếp IP giữa các máy khách được cấu hình và phần còn lại của mạng.

Ban đầu, người dùng cố gắng kết nối với một máy chủ DHCP để lấy thông tin IP. Sau đó, vì đây là một thông điệp phát sóng, switch sẽ truyền thông điệp này trên tất cả các giao diện, có nghĩa là một bản sao được gửi đến máy chủ DHCP hợp lệ và một bản sao khác đến máy chủ DHCP giả mạo.

Cuối cùng, nếu thiết bị của kẻ tấn công trả lời trước, toàn bộ giao tiếp DHCP sẽ tiếp tục chỉ với máy chủ này, và thông điệp DHCP offer từ máy chủ DHCP hợp lệ sẽ bị bỏ qua.

Có hai giải pháp để bảo vệ chống lại cuộc tấn công DHCP spoofing. Giải pháp đầu tiên là cấu hình thông tin IP thủ công trên tất cả các thiết bị trong mạng, điều này gần như không thể thực hiện được trong môi trường lớn. Giải pháp thứ hai là triển khai tính năng DHCP snooping trên các switch.

DHCP snooping là một tính năng bảo mật ở tầng 2 có thể triển khai trên switch để ngăn chặn cuộc tấn công DHCP spoofing và DHCP starvation đến một mức độ nhất định. Ý tưởng chính là switch xây dựng và duy trì một bảng liên kết DHCP snooping.

Mỗi mục nhập trong bảng này sẽ chứa thông tin về tất cả các giao diện trên switch và địa chỉ MAC và IP của máy khách có thể tiếp cận trên chúng, cũng như các thông tin khác như liên kết VLAN, ID cổng và những thông tin tương tự.

Khi các giao diện được cấu hình là tin cậy hoặc không tin cậy, switch sẽ lọc các thông điệp DHCP và cho phép hoặc từ chối dựa trên các mục dữ liệu trong bảng liên kết DHCP snooping.

2.4.2. Giao thức ARP

2.4.2.1 Tổng quan về ARP

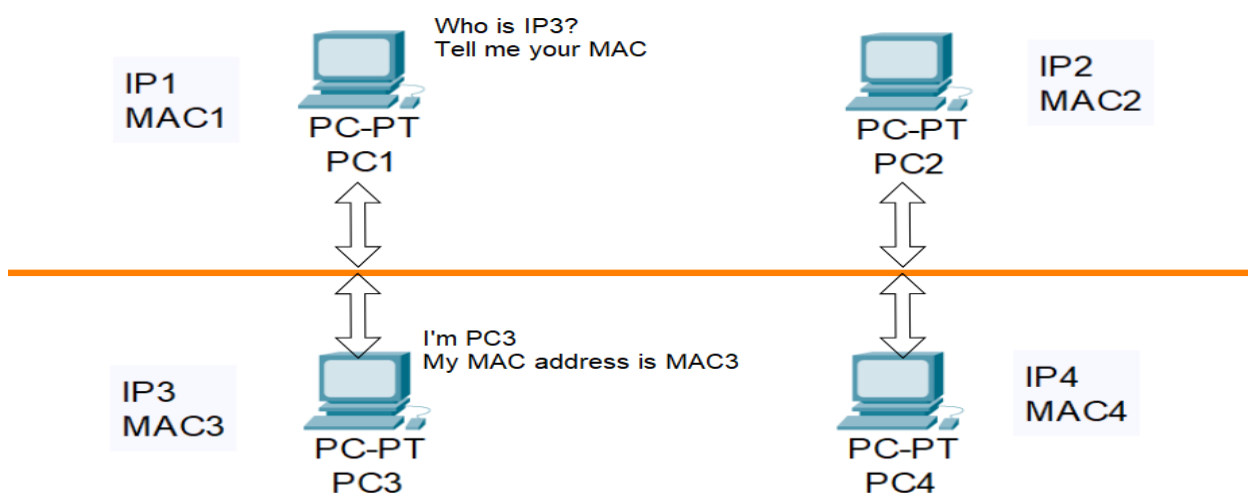
Giao thức ARP là một giao thức cho phép các thiết bị trong mạng liên lạc với một thiết bị cụ thể trên mạng. ARP dịch địa chỉ IP thành địa MAC và ngược lại. Thông thường,

các thiết bị sử dụng ARP để liên lạc với bộ định tuyến hoặc cổng mạng để kết nối với Internet.

Các máy chủ duy trì một bộ nhớ cache ARP, một bảng ánh xạ giữa địa chỉ IP và địa chỉ MAC, và sử dụng nó để kết nối đến các đích trên mạng. Khi máy chủ cần gửi dữ liệu đến một địa chỉ IP mà không biết địa chỉ MAC tương ứng, nó gửi một yêu cầu ARP request dưới dạng broadcast. Các thiết bị nhận được yêu cầu này sẽ phản hồi bằng một gói tin ARP reply chứa địa chỉ MAC của địa chỉ IP được yêu cầu. Máy chủ sẽ cập nhật thông tin này vào bảng ARP cache của mình để sử dụng trong các lần truyền sau, giúp tối ưu hóa quá trình kết nối và tránh việc gửi các yêu cầu ARP lặp đi lặp lại trên mạng.

Giao thức ARP không được thiết kế để bảo mật, do đó nó không xác minh rằng một phản hồi cho yêu cầu ARP thực sự đến từ một bên được ủy quyền. Nó cũng cho phép các máy chủ chấp nhận các phản hồi ARP mà chúng không bao giờ gửi đi yêu cầu. Điều này là điểm yếu của giao thức ARP, mở ra cánh cửa cho các cuộc tấn công ARP spoofing.

ARP chỉ hoạt động với địa chỉ IP 32-bit trong tiêu chuẩn IPv4 cũ. Giao thức IPv6 mới hơn sử dụng một giao thức khác là NDP, có tính bảo mật cao và sử dụng các khóa mật mã để xác minh danh tính của máy chủ. Tuy nhiên, vì hầu hết Internet vẫn sử dụng IPv4 cũ, ARP vẫn được sử dụng rộng rãi.



Hình 2-8 Quá trình phân giải địa chỉ trong giao thức ARP

2.4.2.2 Vấn đề bảo mật trong ARP

ARP spoofing là một kỹ thuật tấn công mạng mà tin tặc gửi các thông điệp ARP với thông tin giả mạo về địa chỉ MAC của các thiết bị trong mạng. Khi các thiết bị trong mạng

nhận được thông điệp này, chúng sẽ tin rằng địa chỉ MAC của kẻ tấn công là địa chỉ MAC của một thiết bị khác, thường là của gateway. Kẻ tấn công có thể lợi dụng điều này để nghe trộm, thay đổi hoặc chặn các gói tin trong mạng mà không bị phát hiện, gây nguy hiểm đến bảo mật thông tin trong hệ thống mạng.

Kỹ thuật này thường được sử dụng để thực hiện các cuộc tấn công xen giữa, nơi mà kẻ tấn công có thể nghe trộm và thậm chí can thiệp vào các trao đổi thông tin giữa hai bên mà không bị phát hiện. Điều này có thể dẫn đến nhiều hậu quả nghiêm trọng như đánh cắp dữ liệu, đánh cắp thông tin đăng nhập, thay đổi dữ liệu hoặc thậm chí kiểm soát hoàn toàn kết nối mạng của nạn nhân. ARP spoofing lợi dụng sự tin tưởng mà các máy chủ mạng đặt vào các phản hồi ARP, mà không được xác thực, làm cho nó trở thành một công cụ mạnh mẽ trong bộ công cụ của các kẻ tấn công mạng, nhằm vào sự toàn vẹn dữ liệu và quyền riêng tư.

Để ngăn chặn tấn công ARP spoofing, cần áp dụng một loạt các biện pháp bảo vệ nhằm tăng cường an ninh mạng. Trước hết, giám sát ARP có thể theo dõi các bảng ARP trong mạng và phát hiện sự thay đổi bất thường, giúp phát hiện sớm các dấu hiệu của tấn công. Cấu hình thiết bị mạng để xác thực các yêu cầu ARP, như sử dụng tính năng Dynamic ARP Inspection (DAI) trên các switch và router, giúp ngăn chặn các yêu cầu ARP giả mạo. Sử dụng mạng ảo giúp phân đoạn mạng, giảm thiểu nguy cơ kẻ tấn công có thể tấn công từ một phân đoạn khác. Áp dụng địa chỉ IP và MAC tĩnh cho các thiết bị quan trọng giúp ngăn chặn việc thay đổi thông tin ARP. Sử dụng VPN để mã hóa lưu lượng mạng, làm cho việc tấn công và nghe lén trở nên khó khăn hơn. Sử dụng các giao thức bảo mật như SSH, HTTPS, và SSL/TLS để bảo vệ dữ liệu truyền qua mạng khỏi bị can thiệp. Cập nhật phần mềm của các thiết bị mạng thường xuyên để bảo vệ khỏi các lỗ hổng bảo mật mới. Quan trọng nhất là nâng cao ý thức bảo mật cho người dùng qua việc giáo dục về các mối đe dọa bảo mật và các biện pháp phòng chống như không mở các liên kết hoặc tệp đính kèm đáng ngờ.

2.4.3. Giao thức DNS

2.4.3.1 Tổng quan về DNS

DNS là viết tắt của Domain Name System, là hệ thống phân giải tên miền. Nó là một hệ thống phân tán cho phép máy tính, dịch vụ hoặc bất kỳ tài nguyên nào kết nối với Internet hoặc mạng riêng. DNS chuyển đổi tên miền (ví dụ như `www.example.com`) thành

địa chỉ IP (ví dụ như 192.0.0.1) mà máy tính sử dụng để nhận diện lẫn nhau trên mạng.

Hệ thống DNS có cấu trúc phân cấp với nhiều cấp độ, bao gồm các miền cấp cao nhất như .com, .org và các mã quốc gia như .uk, .vn, .jp,... Mỗi tên miền được phân tích thành các phần cách nhau bởi dấu chấm (ví dụ như www.example.com).

DNS hoạt động thông qua một hệ thống cơ sở dữ liệu phân tán được duy trì bởi các máy chủ DNS khác nhau. Những máy chủ này lưu trữ các bản ghi của tên miền và các địa chỉ IP tương ứng hoặc thông tin khác.

DNS hỗ trợ nhiều loại bản ghi khác nhau như A Records (cho IPv4), AAAA Records (cho IPv6), MX Records (cho máy chủ thư), CNAME Records (cho tên miền thay thế) và TXT Records (cho thông tin văn bản liên quan đến tên miền).

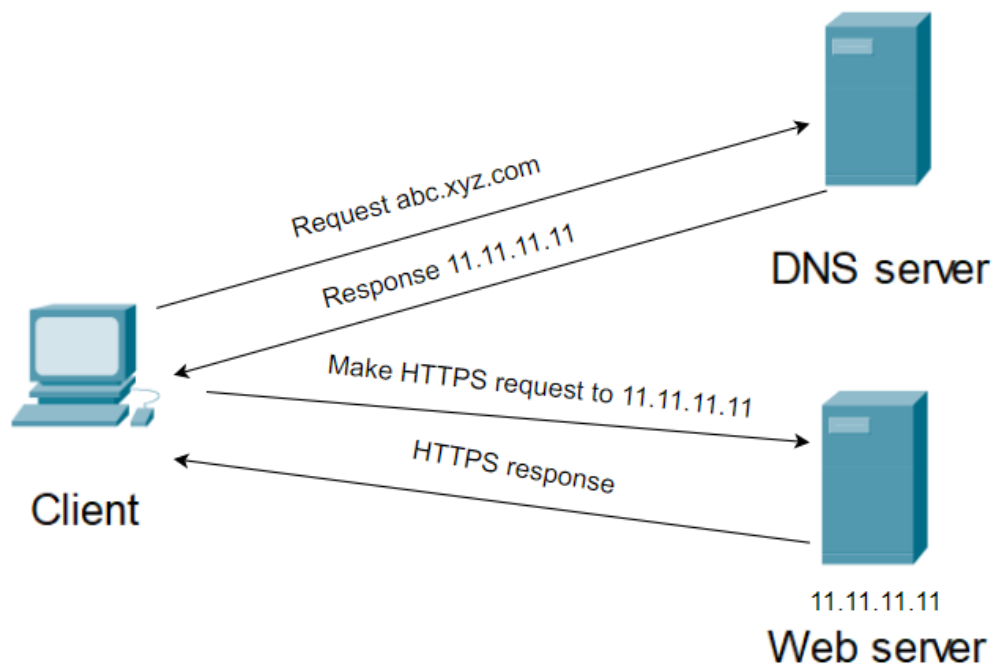
Khi người dùng nhập tên miền vào trình duyệt web, trình duyệt sẽ truy vấn các máy chủ DNS để lấy địa chỉ IP tương ứng. Nếu máy chủ được truy vấn không có thông tin trong bộ nhớ cache, nó sẽ truy vấn đệ quy các máy chủ DNS khác cho đến khi tìm được địa chỉ IP chính xác.

DNS đóng vai trò quan trọng trong hạ tầng của Internet bằng cách hỗ trợ giải quyết tên miền thành địa chỉ IP, từ đó cho phép giao tiếp và truy cập vào các dịch vụ trực tuyến một cách thuận tiện và dễ dàng.

DNS bắt đầu bằng việc chuyển đổi tên miền của máy chủ thành địa chỉ IP tương ứng. Mỗi tên miền đóng vai trò như một nhận dạng duy nhất cho một trang web cụ thể. Thay vì nhớ địa chỉ IP phức tạp, người dùng chỉ cần gõ tên miền để truy cập trang web dễ dàng hơn.

Hệ thống DNS hoạt động dựa trên cơ sở dữ liệu phân tán, lưu trữ thông tin về các tên miền và địa chỉ IP tương ứng của các máy chủ trên Internet. Khi người dùng gửi yêu cầu truy cập một tên miền, trình giải quyết DNS sẽ gửi yêu cầu đến máy chủ DNS để lấy địa chỉ IP. Nếu máy chủ DNS hiện tại không biết địa chỉ IP cho tên miền đó, nó sẽ tiếp tục chuyển tiếp yêu cầu đến các máy chủ DNS khác cho đến khi tìm thấy địa chỉ IP phù hợp.

Khi đã xác định được địa chỉ IP, trình giải quyết DNS trả về thông tin này cho máy tính người dùng, cho phép kết nối và giao tiếp với máy chủ của trang web thông qua giao thức Internet (HTTP, HTTPS,...)



Hình 2-9 Quá trình phân giải tên miền và giao tiếp HTTPS

2.4.3.2 Vấn đề bảo mật trong DNS

DNS Cache Poisoning là một loại tấn công nhắm vào hệ thống DNS, trong đó kẻ tấn công cố gắng làm thay đổi nội dung của bộ nhớ cache DNS trên một máy chủ DNS. Mục tiêu của tấn công này là để điều hướng người dùng đến các địa chỉ IP không mong muốn, thường là các trang web giả mạo hoặc độc hại, thay vì địa chỉ IP chính xác của tên miền yêu cầu.

Cách thức hoạt động của DNS Cache Poisoning thường bắt đầu bằng việc kẻ tấn công gửi các gói tin DNS giả mạo chứa thông tin tên miền và địa chỉ IP không chính xác tới một máy chủ DNS. Nếu máy chủ DNS không được cấu hình để chống lại loại tấn công này hoặc không có các biện pháp bảo mật phù hợp, nó có thể chấp nhận và lưu trữ thông tin sai lệch này vào bộ nhớ cache.

Khi người dùng khác gửi yêu cầu đến máy chủ DNS đó và yêu cầu tương tự, máy chủ DNS có thể trả về thông tin sai lệch từ bộ nhớ cache, dẫn đến người dùng bị điều hướng đến địa chỉ IP được điều khiển bởi kẻ tấn công. Kết quả là người dùng có thể bị đưa đến các trang web giả mạo, lừa đảo hoặc bị lây nhiễm phần mềm độc hại.

Để ngăn chặn DNS Cache Poisoning, các nhà quản trị hệ thống DNS thường áp

dụng các biện pháp bảo mật như sử dụng mã hóa DNS, giới hạn truy cập vào bộ nhớ cache, cập nhật phần mềm định tuyến DNS và thường xuyên kiểm tra và cập nhật các cấu hình bảo mật. Việc này giúp giảm thiểu nguy cơ và hậu quả của các cuộc tấn công DNS Cache Poisoning.

2.5. Một số biện pháp phòng chống các cuộc tấn công mạng

Trên mạng internet hiện nay, những tấn công mạng ngày càng trở nên phức tạp và tinh vi hơn bao giờ hết. Từ việc xâm nhập vào hệ thống để chiếm đoạt thông tin đến các hành động làm ngừng hoạt động hệ thống hoặc lan truyền các phần mềm độc hại, đều có thể gây ra những hậu quả nghiêm trọng. Vì vậy, việc nghiên cứu và áp dụng các biện pháp phòng chống tấn công mạng là bước cơ bản không thể thiếu để bảo vệ thông tin và hệ thống của cả cá nhân lẫn tổ chức. Để đảm bảo an toàn thông tin khi sử dụng mạng, các biện pháp này cần được triển khai một cách toàn diện và thường xuyên cập nhật để phòng ngừa và ứng phó với những mối đe dọa ngày càng tiến bộ trên không gian mạng. Dưới đây là một số biện pháp thường dùng.



Hình 2-10 Một số biện pháp phòng chống các cuộc tấn công mạng

2.5.1. Sử dụng tường lửa

Tường lửa là một thiết bị an ninh mạng giám sát lưu lượng mạng vào và ra và quyết định cho phép hoặc chặn lưu lượng cụ thể dựa trên một bộ quy tắc bảo mật nhất định.

Tường lửa đã trở thành lớp phòng thủ đầu tiên trong bảo mật mạng suốt hơn 25 năm qua. Chúng thiết lập một rào cản giữa các mạng nội bộ được kiểm soát và an toàn mà có

thể tin cậy và các mạng bên ngoài không được tin cậy như Internet.

Có nhiều loại tường lửa như phần cứng, phần mềm, dịch vụ dựa trên phần mềm, đám mây công cộng hoặc đám mây riêng.

Một số loại tường lửa có thể kể đến như:

Tường lửa proxy là một loại tường lửa hoạt động như công kết nối từ một mạng sang mạng khác cho một ứng dụng cụ thể. Máy chủ proxy cung cấp các chức năng như lưu trữ tạm thời nội dung và bảo mật bằng cách ngăn chặn các kết nối trực tiếp từ bên ngoài mạng. Tuy nhiên, việc sử dụng proxy có thể ảnh hưởng đến hiệu suất và khả năng hỗ trợ các ứng dụng.

Tường lửa kiểm tra trạng thái được xem như là một tường lửa "truyền thống" ngày nay, tường lửa kiểm tra trạng thái quản lý lưu lượng dựa trên trạng thái, cổng và giao thức. Nó giám sát từ khi mở kết nối cho đến khi đóng kết nối. Quyết định lọc được thực hiện dựa trên các quy tắc quản trị viên xác định cùng với ngữ cảnh từ các kết nối và gói tin trước đó.

Tường lửa quản lý mối đe dọa thống nhất (UTM)

Thiết bị UTM thường kết hợp các chức năng của tường lửa kiểm tra trạng thái với phòng ngừa xâm nhập và phần mềm diệt virus. Nó cũng có thể bao gồm các dịch vụ bổ sung và hỗ trợ quản lý đám mây. UTM tập trung vào đơn giản hóa và dễ sử dụng.

Tường lửa thế hệ tiếp theo (NGFW)

Tường lửa thế hệ tiếp theo đã tiến bộ hơn so với việc đơn giản lọc gói tin và kiểm tra trạng thái. Các công ty đang triển khai tường lửa này để chặn các mối đe dọa hiện đại như phần mềm độc hại tiên tiến và các cuộc tấn công ở tầng ứng dụng.

Theo định nghĩa của Gartner, một NGFW phải có:

Kiểm soát truy cập thông minh kết hợp với kiểm tra trạng thái.

Hệ thống phòng ngừa xâm nhập tích hợp.

Nhận thức ứng dụng và kiểm soát để phát hiện và chặn các ứng dụng nguy hiểm.

Các phương pháp nâng cấp để tích hợp các nguồn thông tin tương lai.

Kỹ thuật để đối phó với các mối đe dọa bảo mật mới.

Lọc URL dựa trên vị trí địa lý và uy tín.

Mặc dù những tính năng này đang trở thành tiêu chuẩn đối với nhiều công ty, tường lửa NGFW có thể cung cấp nhiều tính năng hơn.

Tường lửa tập trung vào mối đe dọa bao gồm tất cả tính năng của NGFW truyền thống và cũng cung cấp phát hiện và khắc phục các mối đe dọa tiên tiến. Với một tường lửa tập trung vào mối đe dọa, người quản trị có thể:

Xác định thiết bị có nguy cơ cao nhất với sự hiểu biết toàn diện về tình hình.

Phản ứng nhanh chóng với tự động hóa bảo mật thông minh để thiết lập chính sách và tăng cường phòng thủ.

Phát hiện các hoạt động nghi ngờ hoặc phức tạp với việc phối hợp sự kiện mạng và Endpoint.

Giảm thời gian phản ứng từ phát hiện đến xử lý, giám sát hoạt động và hành vi đáng ngờ.

Tường lửa ảo thường triển khai như một thiết bị ảo trong đám mây riêng hoặc đám mây công cộng để giám sát và bảo vệ lưu lượng trên cả mạng vật lý và ảo.

2.5.2. Sử dụng phần mềm diệt virus

Phần mềm diệt virus là một giải pháp bảo mật do các công ty chuyên về an ninh mạng cung cấp. Đây là một công cụ chạy trên các thiết bị kỹ thuật số khác nhau, tìm kiếm và loại bỏ các ứng dụng hoặc tệp không mong muốn có thể gây hại cho thiết bị. Phần mềm này có thể ngăn chặn phần mềm độc hại lây nhiễm vào các ứng dụng hợp pháp, gửi thư rác quảng cáo độc hại hoặc theo dõi thông tin nhạy cảm.

Các tính năng chính của phần mềm diệt virus

Bảo vệ thời gian thực: Phần mềm diệt virus có khả năng tự động chặn virus và phần mềm độc hại ngay khi chúng cố gắng chạy trên thiết bị. Nó cũng ngăn người dùng truy cập vào các trang web có nguy cơ lây nhiễm hoặc mở các email có chứa tệp phần mềm độc hại.

Quét thường xuyên: Chức năng này cho phép phần mềm chạy các lần quét toàn bộ hoặc quét nhanh trên thiết bị để kiểm tra và đảm bảo không bỏ sót phần mềm độc hại nào.

Cách ly tệp độc hại: Khi phát hiện tệp độc hại, phần mềm sẽ cách ly tệp đó, ngăn chặn tệp hoạt động tự do hoặc xóa tệp hoàn toàn. Cách ly tệp giúp các công ty phần mềm phân tích mối đe dọa và cải thiện hệ thống phòng thủ.

Quét theo yêu cầu: Khi mở một tệp, phần mềm sẽ nhanh chóng quét để kiểm tra xem có virus hoặc phần mềm độc hại nào không. Nếu không có gì đáng ngờ, người dùng có thể tiếp tục sử dụng tệp như bình thường.

Khám phá: Tính năng này giúp phát hiện các mối đe dọa mới hoặc đã được sửa đổi mà phần mềm diệt virus chưa biết đến. Nó giám sát hoạt động của tệp và ngăn cản tệp có hành vi đáng ngờ.

Quét toàn bộ hệ thống: Quét toàn bộ hệ thống là một tính năng quan trọng, giúp kiểm tra toàn bộ máy tính để phát hiện các mối đe dọa có thể đã tồn tại trước khi cài đặt phần mềm diệt virus. Việc thực hiện quét toàn bộ hệ thống định kỳ đảm bảo rằng máy tính luôn được bảo vệ với các bản cập nhật mới nhất.

Với sự phát triển không ngừng của các biến thể phần mềm độc hại, việc bảo vệ hệ thống máy tính cá nhân, doanh nghiệp hoặc chính phủ đòi hỏi các kỹ thuật tiên tiến, không chỉ quét virus hiệu quả mà còn cải tiến về dự đoán, phát hiện, loại bỏ và bảo vệ chống lại phần mềm độc hại.

2.5.3. Cập nhật phần mềm thường xuyên

Cập nhật phần mềm là quá trình cài đặt phiên bản mới nhất của một ứng dụng hoặc hệ điều hành. Các cập nhật này thường bao gồm vá lỗi, cải tiến hiệu suất, bảo mật, cũng như tính năng mới. Việc cập nhật đều đặn giúp đảm bảo hệ thống luôn hoạt động ổn định và an toàn nhất có thể.

Bảo mật là lý do quan trọng nhất để cập nhật phần mềm ngay lập tức. Các lỗ hổng trong phần mềm có thể cho phép tội phạm mạng truy cập vào thiết bị của người dùng, cài phần mềm độc hại, chiếm quyền kiểm soát và đánh cắp thông tin cá nhân. Các bản vá bảo mật giúp chặn các lỗ hổng này, bảo vệ thiết bị khỏi các cuộc tấn công.

Cập nhật phần mềm thường bổ sung các tính năng mới, cải tiến các tính năng cũ, hoặc thay thế và xóa các tính năng không cần thiết. Công nghệ luôn thay đổi và các bản cập nhật giúp người dùng có những tính năng và cải tiến mới nhất.

Khi tin tặc xâm nhập qua các lỗ hổng bảo mật, chúng thường tìm kiếm và đánh cắp

dữ liệu cá nhân như thông tin tài chính, mật khẩu, tên người dùng. Sau đó, chúng bán các thông tin này trên web đen. Cập nhật phần mềm giúp bảo vệ dữ liệu bằng cách vá các lỗ hổng bảo mật.

Không phải tất cả các bản cập nhật phần mềm đều liên quan đến bảo mật. Một số bản cập nhật sửa lỗi liên quan đến phần mềm hoặc cải tiến hiệu suất của các tính năng. Việc cập nhật giúp phần mềm hoạt động tốt hơn và giảm thiểu lỗi.

Việc cập nhật phần mềm thường xuyên là một biện pháp phòng ngừa đơn giản nhưng hiệu quả để bảo vệ hệ thống khỏi các mối đe dọa từ tội phạm mạng. Nó không chỉ bảo vệ thiết bị và dữ liệu mà còn đảm bảo rằng người dùng có được những cải tiến mới nhất và hiệu suất tốt nhất từ phần mềm mà họ sử dụng.

2.5.4. Sử dụng mạng riêng ảo

Mạng riêng ảo (VPN) là một công nghệ tạo ra một kết nối mạng an toàn và mã hóa qua mạng công cộng, chẳng hạn như Internet. VPN cho phép người dùng truy cập mạng riêng tư từ xa và bảo vệ dữ liệu cá nhân khỏi các cuộc tấn công mạng.

VPN sử dụng các giao thức mã hóa (như AES-256) để bảo vệ dữ liệu truyền qua mạng. Khi dữ liệu được mã hóa, nó trở nên khó đọc đối với bất kỳ ai không có khóa giải mã, bảo vệ thông tin khỏi bị đánh cắp. VPN tạo ra một đường hầm bảo mật giữa thiết bị của người dùng và máy chủ VPN. Dữ liệu truyền qua đường hầm này được bảo vệ khỏi sự theo dõi và can thiệp từ bên ngoài. Khi sử dụng VPN, địa chỉ IP của người dùng được ẩn đi và thay thế bằng địa chỉ IP của máy chủ VPN. Điều này giúp bảo vệ danh tính và vị trí thực của người dùng.

Với dữ liệu được mã hóa, hacker và gián điệp mạng khó có thể truy cập và đọc thông tin cá nhân hoặc dữ liệu nhạy cảm. Khi kết nối với mạng Wi-Fi công cộng, dữ liệu của người dùng dễ bị tấn công. VPN bảo vệ dữ liệu bằng cách mã hóa nó, giúp ngăn chặn việc nghe trộm. VPN cũng giúp người dùng tránh bị theo dõi và giám sát bởi các nhà cung cấp dịch vụ Internet, chính phủ hoặc các tổ chức khác bằng cách ẩn lưu lượng truy cập và danh tính trực tuyến. Ngoài ra, VPN cho phép người dùng vượt qua các hạn chế về địa lý và truy cập nội dung bị chặn ở một số khu vực hoặc quốc gia. Với những lợi ích này giúp VPN bảo vệ người dùng khỏi các cuộc tấn công mạng không mong muốn.

2.5.5. Sao lưu dữ liệu định kỳ

Sao lưu dữ liệu định kỳ là một biện pháp vô cùng quan trọng để bảo vệ thông tin và duy trì tính toàn vẹn của dữ liệu trong môi trường công nghệ ngày nay. Có nhiều lý do tại sao chúng ta nên thực hiện sao lưu dữ liệu thường xuyên. Trước hết, việc này bảo vệ dữ liệu khỏi mất mát do lỗi phần cứng. Các thiết bị lưu trữ như ổ cứng có thể gặp sự cố bất kỳ lúc nào, và nếu không có bản sao lưu, dữ liệu quan trọng có thể bị mất vĩnh viễn. Ngoài ra, sao lưu định kỳ còn là biện pháp hữu hiệu để khôi phục sau các cuộc tấn công mạng, đặc biệt là ransomware (mã độc tống tiền). Nếu máy tính bị nhiễm ransomware, dữ liệu có thể bị mã hóa và nạn nhân có thể bị đòi tiền chuộc để giải mã. Với các bản sao lưu định kỳ, người dùng có thể khôi phục dữ liệu mà không cần phải trả tiền chuộc. Tương tự, sao lưu cũng giúp bảo vệ dữ liệu khỏi các phần mềm độc hại khác như virus, vốn có thể xóa hoặc làm hỏng dữ liệu. Hơn nữa, sao lưu định kỳ còn bảo vệ dữ liệu khỏi các lỗi do người dùng gây ra. Những nhầm lẫn như xóa nhầm tệp, chỉnh sửa sai hoặc các lỗi khác có thể dẫn đến mất dữ liệu quan trọng. Sao lưu giúp khôi phục lại phiên bản trước của dữ liệu một cách dễ dàng. Trong môi trường kinh doanh, mất dữ liệu có thể gây ra gián đoạn lớn, ảnh hưởng đến doanh thu và uy tín của doanh nghiệp. Sao lưu định kỳ giúp đảm bảo hoạt động kinh doanh không bị gián đoạn do mất dữ liệu, đồng thời đáp ứng các yêu cầu pháp lý và quy định liên quan đến lưu trữ và bảo vệ dữ liệu trong thời gian dài.

Sao lưu dữ liệu định kỳ cũng đóng vai trò quan trọng trong việc phòng chống các cuộc tấn công mạng không mong muốn. Thứ nhất, sao lưu tạo ra nhiều bản sao của dữ liệu ở các thời điểm khác nhau. Nếu một bản sao bị tấn công hoặc bị hỏng, vẫn có các bản sao khác để khôi phục. Thứ hai, sao lưu ngoại tuyến không kết nối trực tiếp với hệ thống mạng, giúp bảo vệ dữ liệu khỏi các cuộc tấn công trực tuyến, đặc biệt là ransomware. Thứ ba, việc kiểm tra định kỳ và thử nghiệm khôi phục từ các bản sao lưu giúp đảm bảo rằng dữ liệu luôn có thể được khôi phục một cách hiệu quả khi cần thiết. Thứ tư, lưu trữ bản sao lưu ở nhiều vị trí khác nhau bảo vệ dữ liệu khỏi các thảm họa địa phương như hỏa hoạn, lũ lụt hoặc các sự cố khác. Cuối cùng, sử dụng mã hóa để bảo vệ các bản sao lưu khỏi truy cập trái phép, đảm bảo rằng ngay cả khi dữ liệu sao lưu bị đánh cắp, nó vẫn an toàn.

Tóm lại, sao lưu dữ liệu định kỳ không chỉ giúp bảo vệ dữ liệu khỏi mất mát và tấn công mà còn đảm bảo tính liên tục của hoạt động kinh doanh và tuân thủ các quy định pháp lý. Đây là một phần quan trọng trong chiến lược bảo mật tổng thể, giúp người dùng và

doanh nghiệp giảm thiểu rủi ro và duy trì sự an toàn, toàn vẹn của thông tin quan trọng trong bối cảnh các mối đe dọa mạng ngày càng tinh vi.

2.5.6. Giám sát mạng

Giám sát mạng là quá trình theo dõi và phân tích lưu lượng mạng để phát hiện, cảnh báo và phản ứng kịp thời với các hoạt động bất thường hoặc nguy cơ tấn công mạng. Đây là một phương pháp quan trọng và hữu hiệu để phòng chống các cuộc tấn công mạng vì nhiều lý do. Trước hết, giám sát mạng giúp phát hiện kịp thời các cuộc tấn công thông qua các hệ thống phát hiện xâm nhập có khả năng nhận diện các mẫu tấn công đã biết và đưa ra cảnh báo ngay lập tức. Đồng thời, các công cụ giám sát cũng có thể phát hiện các hành vi bất thường trong lưu lượng mạng, chẳng hạn như tăng đột biến về lưu lượng, truy cập từ các địa chỉ IP lạ hoặc các hoạt động không phù hợp với mô hình hành vi thông thường của người dùng và hệ thống. Khi phát hiện sự cố, hệ thống giám sát mạng có thể gửi cảnh báo tức thì đến quản trị viên mạng, cho phép họ can thiệp và xử lý sự cố kịp thời, giảm thiểu thiệt hại. Một số hệ thống tiên tiến thậm chí còn có khả năng tự động thực hiện các biện pháp phòng thủ như chặn lưu lượng đáng ngờ, cô lập các thiết bị bị xâm nhập, hoặc áp dụng các quy tắc bảo mật để ngăn chặn cuộc tấn công lan rộng.

Giám sát mạng còn cung cấp khả năng lưu trữ và phân tích lưu lượng mạng trong một khoảng thời gian nhất định, hỗ trợ điều tra và truy vết các cuộc tấn công, xác định nguyên nhân gốc rễ và tìm ra các lỗ hổng bảo mật. Bằng cách phân tích dữ liệu giám sát mạng, các chuyên gia bảo mật có thể nhận diện các xu hướng và mẫu tấn công mới, từ đó cập nhật và điều chỉnh chiến lược bảo mật cho phù hợp. Việc giám sát mạng cũng giúp phát hiện các lỗ hổng bảo mật chưa được khắc phục hoặc các cấu hình sai sót trong hệ thống, từ đó giúp quản trị viên mạng kịp thời khắc phục và tăng cường các chính sách bảo mật. Ngoài ra, giám sát mạng còn giúp các tổ chức tuân thủ các quy định và tiêu chuẩn bảo mật, đáp ứng các yêu cầu pháp lý và tránh các hình phạt liên quan đến vi phạm bảo mật. Các dữ liệu thu thập từ giám sát mạng cung cấp thông tin quan trọng cho các báo cáo và kiểm toán bảo mật, chứng minh rằng tổ chức đang thực hiện các biện pháp bảo vệ dữ liệu và hệ thống một cách hiệu quả.

Tóm lại, giám sát mạng là một phương pháp phòng chống tấn công mạng hữu hiệu nhờ khả năng phát hiện kịp thời, cảnh báo và phản ứng nhanh chóng, tăng cường khả năng phân tích và điều tra, cải thiện bảo mật tổng thể, và tuân thủ các quy định pháp lý. Việc

triển khai giám sát mạng giúp các tổ chức và cá nhân bảo vệ hệ thống của mình trước các mối đe dọa ngày càng phức tạp trong thế giới số.

2.5.7. Quản lý quyền truy cập

Quản lý quyền truy cập là một thành phần quan trọng trong bảo mật thông tin, đóng vai trò quyết định trong việc bảo vệ dữ liệu và hệ thống khỏi các cuộc tấn công mạng và truy cập trái phép. Việc quản lý quyền truy cập hiệu quả giúp đảm bảo rằng chỉ những người dùng được ủy quyền mới có thể truy cập vào các tài nguyên cụ thể trong hệ thống, đồng thời giảm thiểu rủi ro bị xâm nhập và lạm dụng. Bằng cách chỉ định quyền truy cập cụ thể cho từng người dùng dựa trên vai trò và trách nhiệm của họ, quản lý quyền truy cập giúp hạn chế quyền truy cập vào các tài nguyên nhạy cảm, giảm thiểu nguy cơ bị truy cập trái phép và lạm dụng quyền hạn. Đồng thời, việc này cũng giúp phát hiện và ngăn chặn các nỗ lực truy cập trái phép vào hệ thống, thông qua các cơ chế bảo mật như xác thực đa yếu tố và các chính sách mật khẩu mạnh. Các hệ thống quản lý quyền truy cập còn bao gồm chức năng ghi lại và theo dõi hoạt động của người dùng, giúp quản trị viên phát hiện các hành vi bất thường hoặc nghi ngờ để thực hiện các biện pháp phòng ngừa và phản ứng kịp thời. Quản lý quyền truy cập còn bảo vệ dữ liệu nhạy cảm khỏi bị truy cập và tiết lộ trái phép, đồng thời giảm thiểu rủi ro từ các mối đe dọa nội bộ bằng cách kiểm soát chặt chẽ quyền truy cập và giới hạn các quyền không cần thiết. Ngoài ra, việc tuân thủ các quy định và tiêu chuẩn bảo mật thông qua quản lý quyền truy cập giúp tổ chức tránh các hình phạt pháp lý và nâng cao uy tín, độ tin cậy. Các phương pháp và công cụ quản lý quyền truy cập như xác thực đa yếu tố chính sách mật khẩu mạnh, phân quyền theo vai trò, theo dõi và ghi lại hoạt động, và quản lý danh tính và truy cập đều góp phần tạo nên một hệ thống bảo mật hiệu quả. Tóm lại, quản lý quyền truy cập là một phương pháp hữu hiệu để phòng chống tấn công mạng và bảo vệ dữ liệu nhạy cảm, giúp các tổ chức giảm thiểu rủi ro bị xâm nhập và lạm dụng, đảm bảo an toàn thông tin và tuân thủ các quy định bảo mật.

2.5.8. Sử dụng công nghệ sandboxing

Công nghệ sandboxing là một phương pháp bảo mật tạo ra một môi trường ảo tách biệt để kiểm tra và chạy các chương trình hoặc mã độc mà không ảnh hưởng đến hệ thống chính và dữ liệu nhạy cảm. Sandboxing cho phép các chương trình được thực thi trong một môi trường kiểm soát, ngăn chặn các hành động nguy hiểm và bảo vệ hệ thống khỏi các mối đe dọa. Lợi ích của việc sử dụng sandboxing bao gồm khả năng kiểm tra và phân tích

mã độc một cách an toàn, ngăn chặn các cuộc tấn công zero-day, tăng cường bảo mật ứng dụng, và bảo vệ khỏi mã độc từ web. Sandboxing cũng giúp ngăn chặn phần mềm độc hại lây lan và đảm bảo rằng bất kỳ thay đổi nào do mã độc gây ra sẽ bị xóa bỏ ngay sau khi quá trình kiểm tra kết thúc. Các ứng dụng của công nghệ này rất đa dạng, từ trình duyệt web hiện đại như Google Chrome và Microsoft Edge, sử dụng sandboxing để bảo vệ người dùng khỏi các mối đe dọa từ web, đến các phần mềm diệt virus và bảo mật sử dụng để kiểm tra các tệp tải về trước khi cho phép chúng chạy trên hệ thống. Ngoài ra, sandboxing còn được sử dụng trong phát triển và thử nghiệm phần mềm, giúp các nhà phát triển kiểm tra phần mềm trong môi trường an toàn trước khi triển khai chính thức. Tóm lại, công nghệ sandboxing là một công cụ quan trọng trong việc bảo vệ hệ thống và dữ liệu khỏi các cuộc tấn công mạng và lỗ hổng bảo mật.

2.5.9. Nâng cao nhận thức về bảo mật

Nâng cao ý thức về bảo mật và an toàn thông tin là một bước quan trọng giúp cá nhân và tổ chức ngăn chặn các mối đe dọa mạng. Đầu tiên, chương trình đào tạo và giáo dục đóng vai trò then chốt, cung cấp kiến thức về nhận diện và phòng ngừa các cuộc tấn công, cùng với hành vi an toàn khi sử dụng internet. Thứ hai, việc thiết lập và tuân thủ các chính sách bảo mật thông tin trong tổ chức rất quan trọng. Điều này bao gồm việc đề ra các quy định về mật khẩu mạnh để ngăn chặn các cuộc tấn công từ điển và sử dụng an toàn của dữ liệu quan trọng. Các chính sách này cũng bao gồm việc áp dụng phân quyền truy cập chặt chẽ, chỉ cho phép nhân viên truy cập vào những thông tin cần thiết cho công việc của họ. Thứ ba, các chương trình nhận thức và thông tin cũng đóng vai trò quan trọng trong việc tăng cường ý thức và sự chủ động trong bảo vệ thông tin quan trọng. Đồng thời, việc tuân thủ các chính sách bảo mật không chỉ giúp đảm bảo tính bảo mật của hệ thống mà còn giúp tổ chức tuân thủ các quy định pháp luật liên quan đến bảo mật thông tin. Tóm lại, việc nâng cao ý thức về bảo mật và an toàn thông tin là trách nhiệm chung của từng cá nhân và cả tổ chức, góp phần quan trọng vào việc xây dựng một môi trường số an toàn và tin cậy.

CHƯƠNG 3. HIỆN THỰC HÓA NGHIÊN CỨU

3.1. Cài đặt phần mềm giả lập mạng

3.1.1. Phần mềm mô phỏng giả lập mạng

Phần mềm mô phỏng giả lập mạng là công cụ được sử dụng để mô phỏng các mạng máy tính và thiết bị mạng trong một môi trường ảo trên máy tính. Điều này cho phép người dùng thiết kế, triển khai và kiểm tra các mạng mà không cần phải có các thiết bị vật lý thực tế, tiết kiệm chi phí và thời gian. Cụ thể là:

Khi sử dụng phần mềm mô phỏng người dùng không cần mua các thiết bị vật lý. Thay vì phải mua các thiết bị mạng thật, các mô hình mạng có thể được triển khai hoàn toàn trong môi trường ảo trên máy tính. Điều này tiết kiệm chi phí đáng kể, đặc biệt là đối với các tổ chức hoặc sinh viên không có ngân sách lớn để đầu tư vào thiết bị mạng thật. Các thiết bị mạng thực yêu cầu chi phí bảo trì, nâng cấp phần cứng và phần mềm, cũng như chi phí điện năng và không gian lưu trữ. Sử dụng mô phỏng giả lập mạng loại bỏ những chi phí này hoặc giảm thiểu chúng đáng kể.

Mô phỏng giả lập mạng cho phép người dùng triển khai và thử nghiệm các mô hình mạng một cách nhanh chóng và linh hoạt hơn so với việc cấu hình và kết nối các thiết bị vật lý. Đặc biệt đối với sinh viên và nhân viên mới có thể học và thực hành mạng mà không cần phải đến trực tiếp với các thiết bị mạng thật. Điều này giúp rút ngắn thời gian học tập và cũng làm giảm thời gian cần thiết cho việc đào tạo. Với mô phỏng giả lập mạng, người dùng có thể dễ dàng thực hiện các kịch bản kiểm tra, phát hiện và sửa lỗi mạng một cách nhanh chóng và an toàn, mà không gây ảnh hưởng đến mạng sản xuất hoặc thực tế.

Để lựa chọn phần mềm mô phỏng giả lập mạng phù hợp, cần xem xét các yếu tố như mục đích sử dụng, tính năng cần thiết, và sự dễ dàng trong việc học tập và triển khai mạng. Một vài loại phần mềm mô phỏng giả lập mạng có thể kể đến như:

Cisco Packet Tracer: Được phát triển bởi Cisco Systems, là một trong những công cụ phổ biến để học và mô phỏng mạng. Với ưu điểm dễ sử dụng, hỗ trợ nhiều thiết bị Cisco, phù hợp cho việc học tập và giảng dạy.

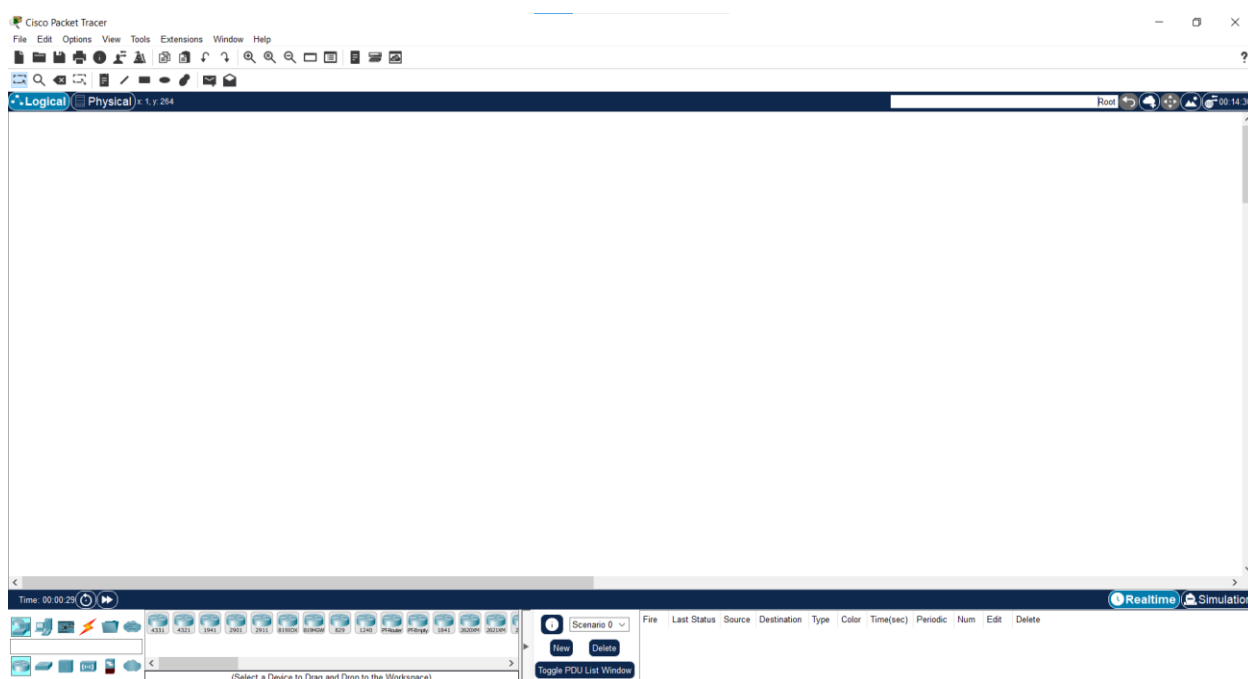
GNS3 là một phần mềm mã nguồn mở, mô phỏng được nhiều loại thiết bị mạng, cho phép mô phỏng các mạng phức tạp, phù hợp với người có nhiều kinh nghiệm trong lĩnh vực mạng cần nghiên cứu sâu hơn.

EVE-NG là phần mềm mô phỏng mạng phức tạp, hỗ trợ nhiều loại thiết bị từ nhiều nhà cung cấp khác nhau, đòi hỏi kiến thức kỹ thuật để cấu hình và sử dụng.

Tuy nhiên, để thuận tiện cho việc học tập và nghiên cứu thì cần lựa chọn một phần mềm mô phỏng phổ biến là Cisco Packet Tracer vì đây là công cụ dễ dàng sử dụng và học tập, có giao diện đồ họa thân thiện, dễ tiếp cận cho người mới bắt đầu. hỗ trợ nhiều thiết bị Cisco, cho phép mô phỏng một loạt các thiết bị mạng Cisco, từ bộ định tuyến đến bộ chuyển mạch và các mô đun mạng phức tạp. Được Cisco hỗ trợ và cập nhật thường xuyên để hỗ trợ các tính năng mới và các thiết bị mới của họ. Phù hợp với giáo dục đặc biệt phổ biến trong các khóa học Cisco CCNA và CCNP, giúp sinh viên và các chuyên gia mạng học tập và thử nghiệm mạng một cách hiệu quả.

3.1.2. Cài đặt ứng dụng Cisco Packet Tracer

Để cài đặt phần mềm mô phỏng giả lập mạng Cisco Packet Tracer, truy cập vào khóa học Cisco Packet Tracer tại trang chủ của Cisco Networking Academy hay Netacad tại đường dẫn <https://www.netacad.com/courses/packet-tracer>, sau đó đăng nhập, truy cập vào khóa học và tải phần mềm và cài đặt theo hướng dẫn của khóa học.



Hình 3-1 Giao diện ứng dụng Packet Tracer sau khi khởi động

3.2. Mô phỏng một cuộc tấn công DHCP spoofing và hướng khắc phục

3.2.1. Đặc tả yêu cầu

Mục tiêu:

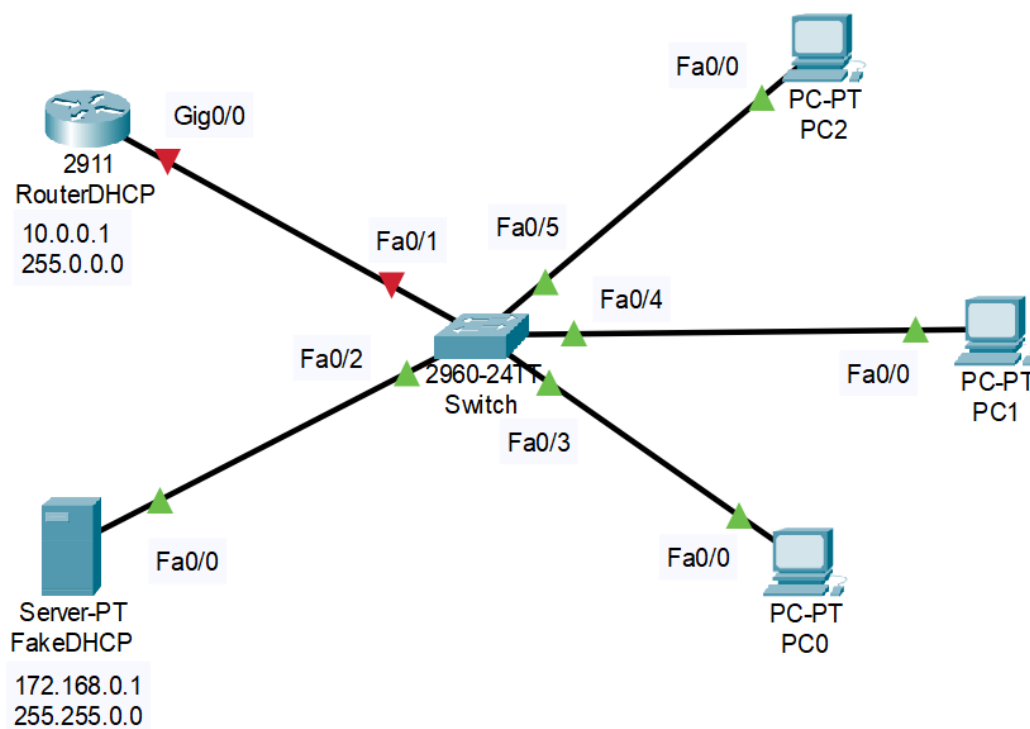
Mô phỏng các cuộc tấn công DHCP Spoofing trên Cisco Packet Tracer.

Đề xuất và triển khai các biện pháp khắc phục để ngăn chặn các loại tấn công này.

Nội dung thực hiện:

Môi trường mô phỏng:

Sử dụng Cisco Packet Tracer để tạo một mạng đơn giản mô phỏng một cuộc tấn công DHCP spoofing gồm một Router với tên gọi RouterDHCP đóng vai trò là máy chủ cấp phát địa chỉ IP động, một Server với tên gọi FakeDHCP đóng vai trò là một máy chủ của kẻ tấn công nhằm cấp phát địa chỉ IP giả, một switch và 3 PC đóng vai trò là các thiết bị cần cấp phát địa chỉ IP.



Hình 3-2 Mô hình mô phỏng một cuộc tấn công DHCP spoofing

Cài đặt DHCP Server: Cấu hình DHCP Server trên RouterDHCP để cung cấp IP động cho các máy trạm.

Giả lập tấn công DHCP Spoofing: Thêm một máy chủ giả mạo DHCP vào mạng, sau đó cấu hình máy chủ để chạy DHCP Server giả mạo, cung cấp các thông tin sai lệch về IP và các thông tin cấu hình mạng khác.

Quan sát phản ứng của các máy trạm: Kiểm tra các máy trạm để xem có nhận được địa chỉ IP từ DHCP Server giả mạo hay không. Xác định các vấn đề phát sinh do việc nhận IP và các thông tin cấu hình mạng khác từ Server giả mạo.

Hướng khắc phục: Cấu hình DHCP Snooping trên Switch để chỉ cho phép các cổng đáng tin cậy cung cấp dịch vụ DHCP.

3.2.2. Cấu hình DHCP cho router để cấp phát địa chỉ IP động

1. Vào router > CLI để mở giao diện dòng lệnh.
2. Khởi động router bằng lệnh *enable*.
3. Dùng lệnh *configure terminal* để vào chế độ cấu hình toàn cục cho router..
4. Truy cập vào chế độ cấu hình của cổng giao tiếp Gig0/0 trên router bằng lệnh *interface Gig0/0*.
5. Kích hoạt cổng giao tiếp Gig0/0 bằng lệnh *no shutdown* (mặc định là tắt)
6. Gán địa chỉ IP và subnet mask cho cổng Gig0/0 bằng lệnh *ip address 10.0.0.1 255.0.0.0*
7. Dùng lệnh *exit* để thoát cấu hình cổng Gig0/0 để trở về chế độ cấu hình toàn cục
8. Tạo và đặt tên cho một DHCP pool mới tên là "MYLAN" bằng lệnh *ip dhcp pool MYLAN*
9. Xác định dải địa chỉ IP sẽ được cấp phát bởi DHCP pool "LAN" bằng lệnh *network 10.0.0.0 255.0.0.0*
10. Cấu hình địa chỉ IP của default gateway cho các thiết bị nhận địa chỉ IP từ DHCP pool "MYLAN" bằng lệnh *default-router 10.0.0.1*
11. Dùng lệnh *dns-server 8.8.8.8* để cấu hình địa chỉ IP của DNS server cho các thiết bị nhận địa chỉ IP từ DHCP pool "MYLAN"
12. Dùng lệnh *exit* để thoát khỏi chế độ cấu hình DHCP pool và trở về chế độ cấu hình toàn cục.

13. Lưu cấu hình hiện tại vào NVRAM để đảm bảo cấu hình được giữ lại sau khi router khởi động lại bằng lệnh *do write*.

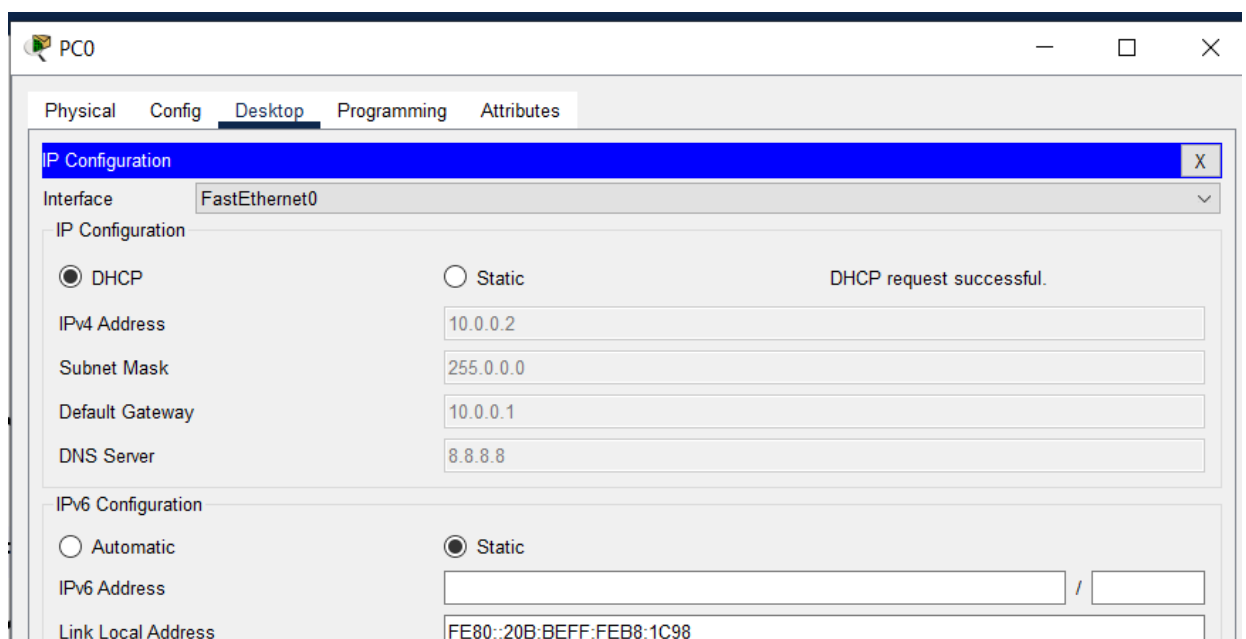
```
Router>
Router>
Router>
Router>
Router>
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int Gig0/0
Router(config-if)#no sh

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

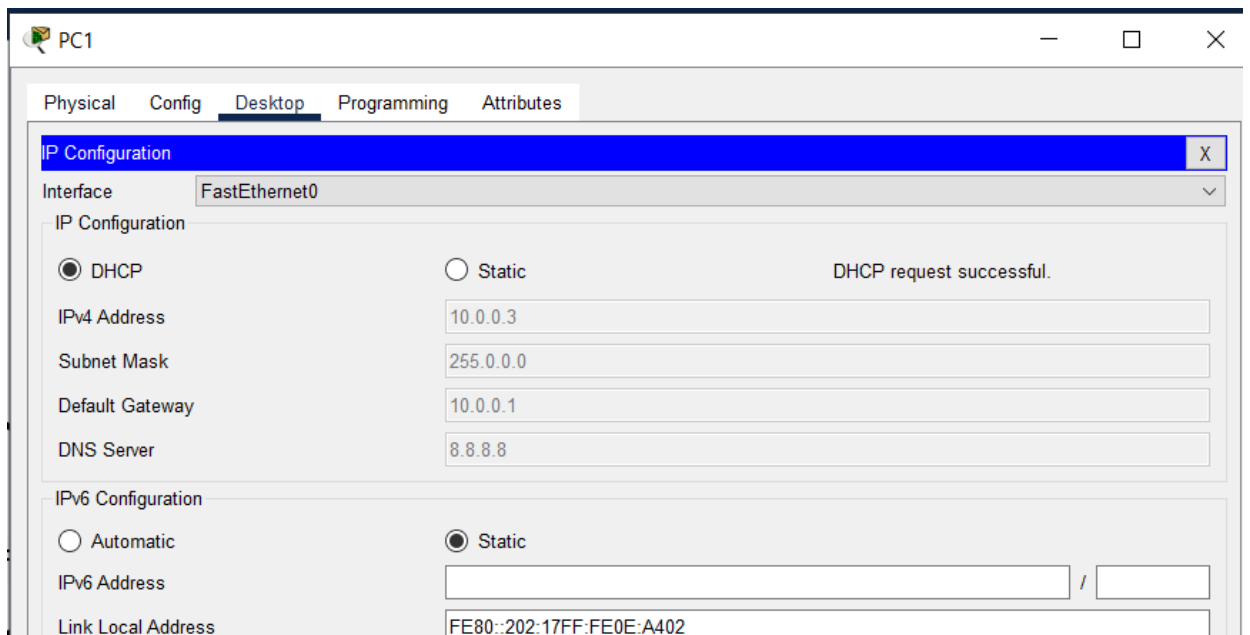
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
ip add 10.0.0.1 255.0.0.0
Router(config-if)#ip add 10.0.0.1 255.0.0.0
Router(config-if)#exit
Router(config)#ip dhcp pool MYLAN
Router(dhcp-config)#net 10.0.0.0 255.0.0.0
Router(dhcp-config)#default-router 10.0.0.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#do wri
Building configuration...
[OK]
Router(config)#
```

Hình 3-3 Cấu hình DHCP cho RouterDHCP

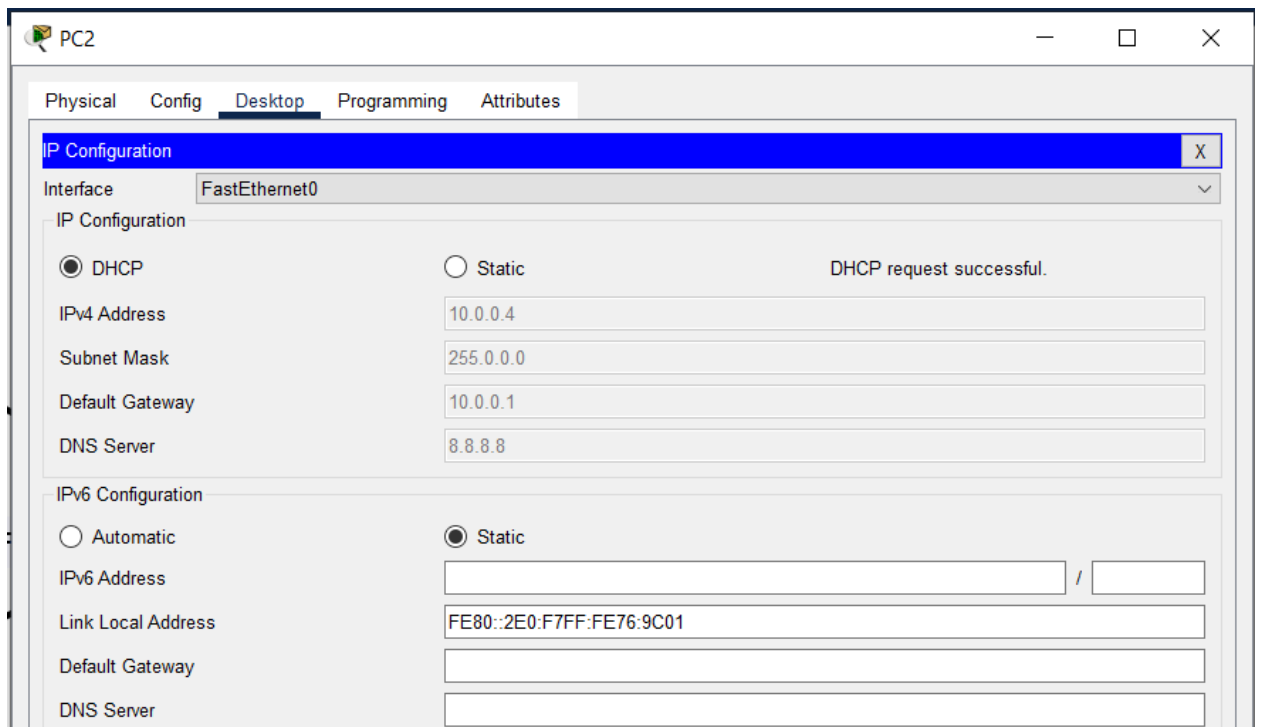
Sau khi cấu hình DHCP cho RouterDHCP, vào lần lượt chế độ IP configuration của các PC0, PC1, PC2, chọn DHCP để các PC này nhận tự động nhận địa chỉ IP.



Hình 3-4 PC0 sau khi nhận địa chỉ IP tự động thông qua DHCP của RouterDHCP

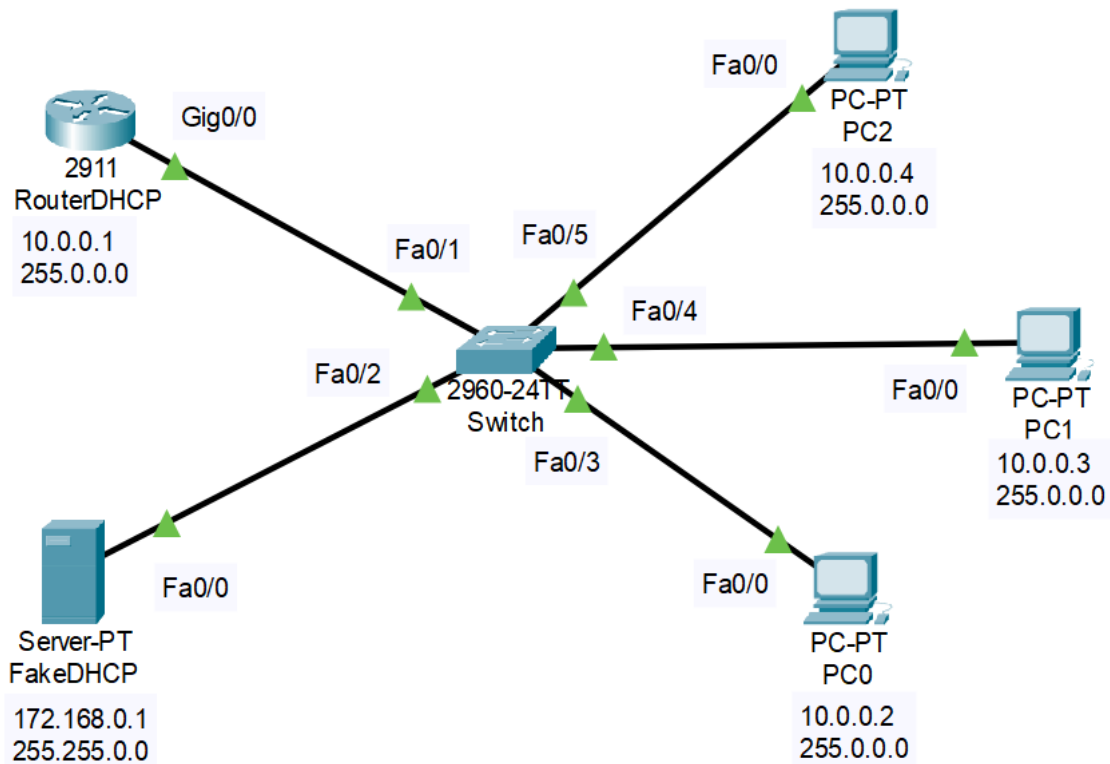


Hình 3-5 PC1 sau khi nhận địa chỉ IP tự động thông qua DHCP của RouterDHCP



Hình 3-6 PC2 sau khi nhận địa chỉ IP tự động thông qua DHCP của RouterDHCP

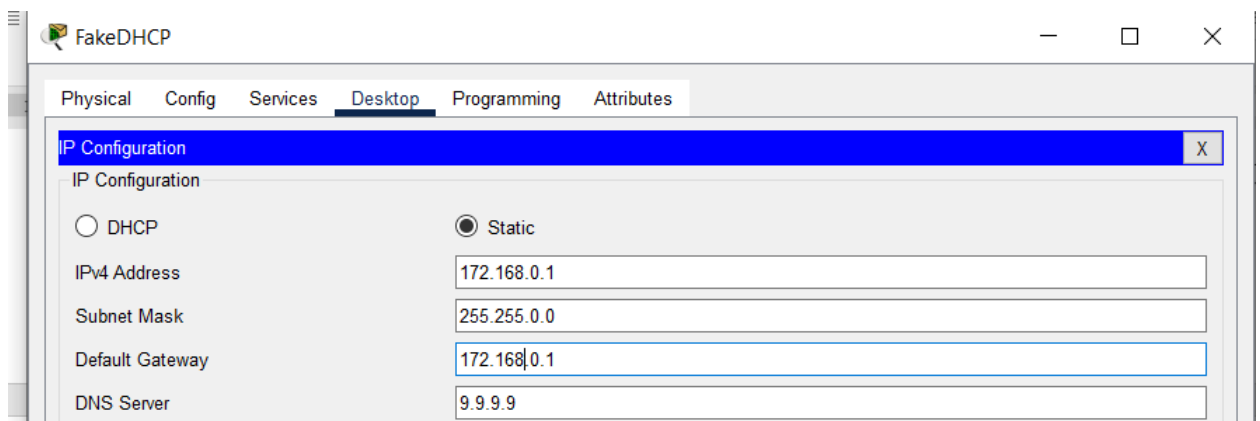
Sau khi nhận được IP mô hình sẽ có dạng:



Hình 3-7 Mô hình mô phỏng sau khi được cấp phát địa chỉ IP

3.2.3. Cấu hình DHCP cho server giả mạo

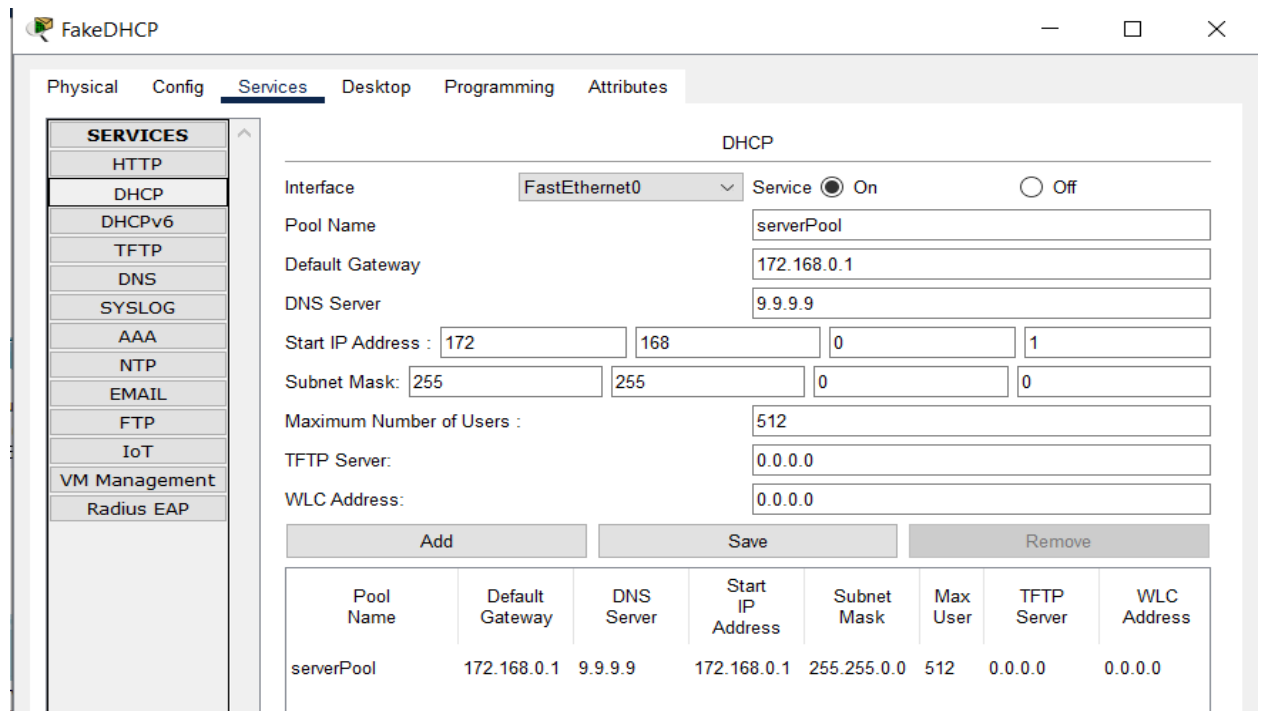
1. Đầu tiên thiết lập các thông số IP, subnet mask, default gateway, DNS cho server FakeDHCP bằng cách vào server FakeDHCP > Desktop > IP configuration chọn static đặt địa chỉ IPv4 cho máy chủ DHCP giả mạo là 172.168.0.1, subnet mask là 255.255.255.0, default gateway là 172.168.0.1, DNS là 9.9.9.9.



Hình 3-8 Thông tin về IP, subnet mask, gateway, DNS của server DHCP giả mạo

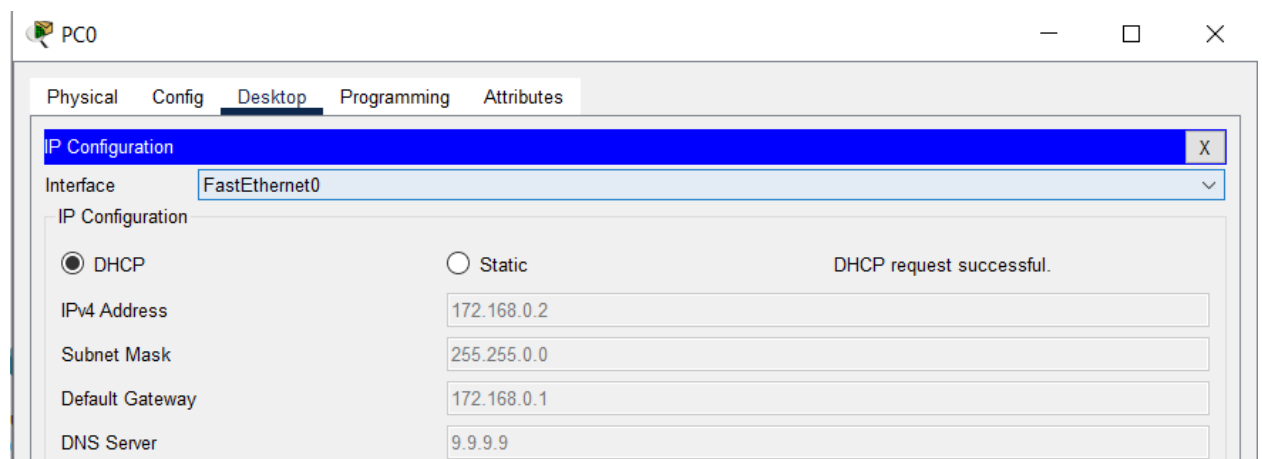
2. Tiếp theo để thiết lập DHCP cho server FakeDHCP để cấp phát địa chỉ IP trong mạng bằng cách vào server FakeDHCP > services > DHCP > Service On, thiết lập

các thông số default gateway là 172.168.0.1, DNS server là 9.9.9.9, thiết lập dãy địa chỉ IP cần cấp phát bắt đầu từ 172.168.0.1, subnet mask là 255.255.0.0, sau đó lưu lại.

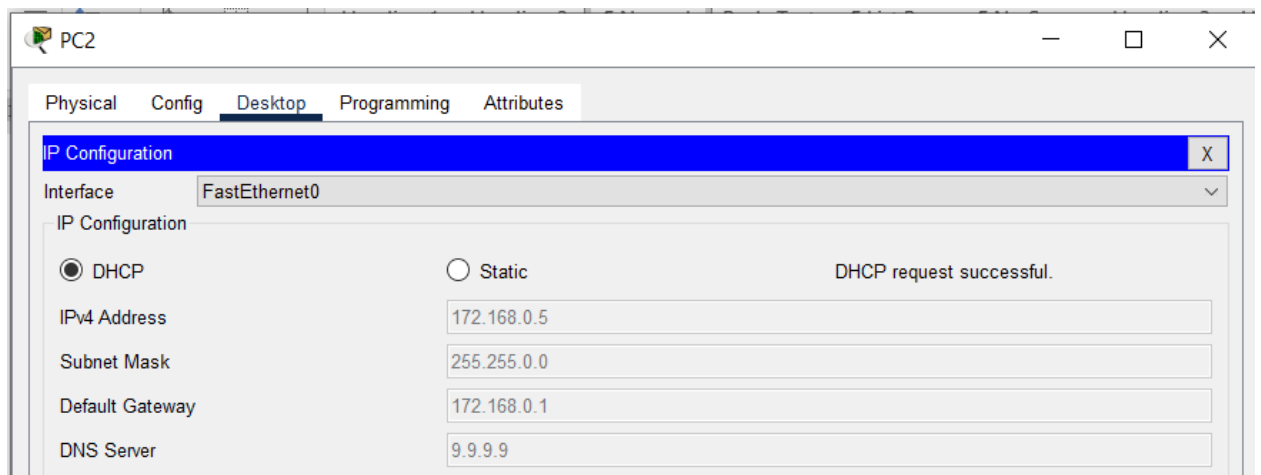


Hình 3-9 Cấu hình DHCP cho server FakeDHCP

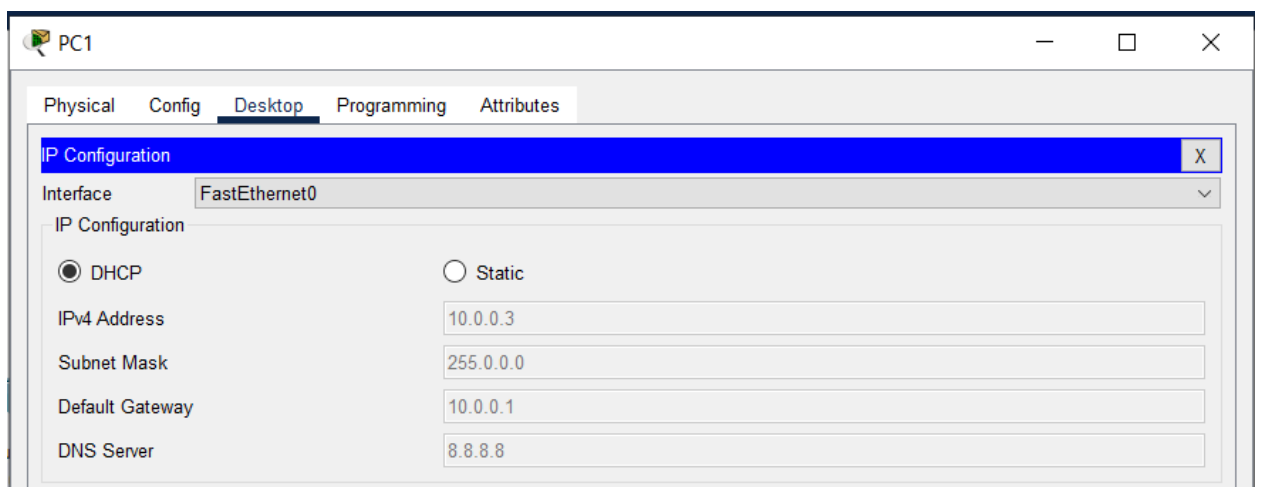
- Sau đó vào lần lượt các PC0, PC1, PC2 chuyển từ DHCP sang static IP và chuyển lại DHCP để các PC cập nhật lại địa chỉ IP, kết quả là PC0, PC2 đã bị thay đổi IP sang IP của máy chủ DHCP cung cấp, PC1 vẫn nhận IP từ router.



Hình 3-10 PC0 sau khi nhận lại địa chỉ IP



Hình 3-11 PC2 sau khi nhận lại địa chỉ IP



Hình 3-12 PC1 sau khi nhận lại địa chỉ IP

Có thể thấy với vai trò là một kẻ tấn công, server FakeDHCP cũng cấu hình DHCP để cạnh tranh cấp phát địa chỉ IP với RouterDHCP. Khi có một thiết bị mới vào mạng nó gửi gói tin DHCP Discover để tìm kiếm máy chủ DHCP. Kẻ tấn công có thể cấu hình máy chủ DHCP giả mạo để phản hồi gói tin DHCP Discover nhanh hơn máy chủ DHCP hợp pháp, thiết bị nhận gói tin DHCP Offer từ máy chủ giả mạo trước khi nhận được phản hồi từ máy chủ hợp pháp. Do đó, nó sẽ gửi gói tin DHCP Request để chấp nhận địa chỉ IP từ máy chủ giả mạo. Máy chủ DHCP giả mạo cấp phát địa chỉ IP và các thông số mạng khác (như gateway, DNS server) sai lệch, có thể dẫn đến việc lưu lượng mạng của thiết bị bị chuyển hướng hoặc giám sát bởi kẻ tấn công.

3.2.4. Giải pháp phòng chống tấn công DHCP spoofing

Để ngăn chặn một cuộc tấn công DHCP spoofing, giải pháp được đề xuất là cấu hình DHCP snooping trên thiết bị switch. DHCP snooping là một cơ chế bảo vệ mạng được

triển khai trên các thiết bị switch để ngăn chặn các cuộc tấn công như DHCP spoofing. Khi bật chế độ DHCP snooping trên switch, thiết bị sẽ giám sát và xác nhận các gói tin DHCP được chấp nhận trên mỗi cổng mạng.

Cụ thể, DHCP snooping hoạt động bằng cách xây dựng một bảng CAM (Content Addressable Memory) chứa các thông tin về các cặp địa chỉ MAC và IP được gán cho từng cổng switch. Khi gói tin DHCP được gửi đi từ một cổng, switch sẽ kiểm tra nếu địa chỉ MAC và IP trong gói tin này khớp với bảng CAM. Nếu khớp, gói tin sẽ được chấp nhận. Ngược lại, nếu không khớp hoặc không có bản ghi trong bảng CAM, gói tin sẽ bị từ chối.

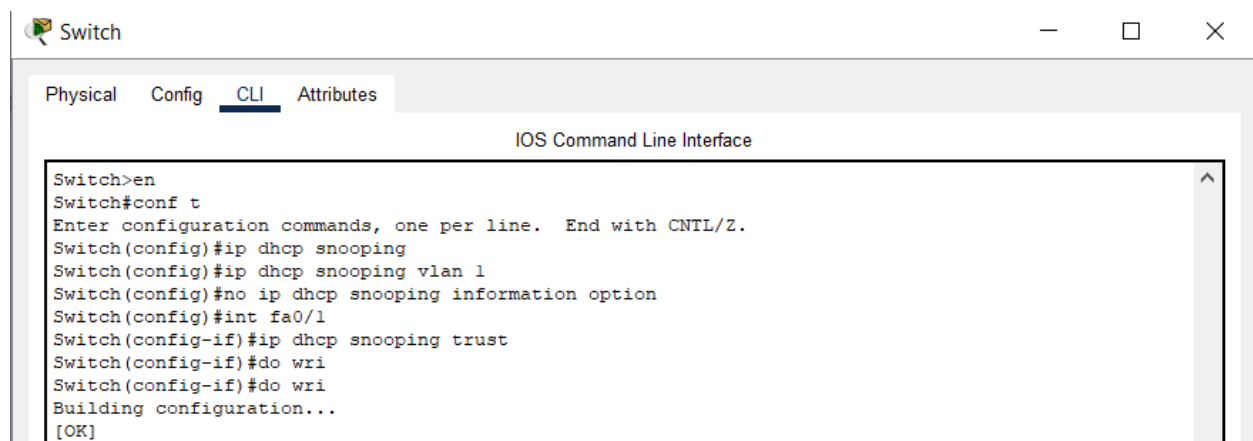
Lợi ích chính của DHCP snooping là ngăn chặn các cuộc tấn công DHCP spoofing, mà trong đó kẻ tấn công gửi các gói tin DHCP giả mạo với địa chỉ MAC và IP được thay đổi để đánh lừa thiết bị mạng khác. Bằng cách chỉ cho phép các gói tin DHCP hợp lệ được chấp nhận trên các cổng đã được xác thực, DHCP snooping giúp bảo vệ mạng khỏi các nguy cơ bảo mật này.

Để cấu hình DHCP snooping, thực hiện theo các bước sau:

1. Vào switch > CLI, khởi động thiết bị bằng lệnh *enable*
2. Vào chế độ cấu hình toàn cục bằng lệnh *configure terminal*
3. Dùng lệnh *ip dhcp snooping* để bật tính năng DHCP snooping trên switch. Khi tính năng này được bật, switch sẽ bắt đầu giám sát các gói tin DHCP trên các cổng mạng của nó.
4. Dùng lệnh *ip dhcp snooping vlan 1* để cấu hình DHCP snooping cho VLAN 1. Đây chỉ định rằng tính năng DHCP snooping sẽ được áp dụng cho các cổng thuộc VLAN 1 trên switch.
5. Vô hiệu hóa tùy chọn thông tin DHCP trên các gói tin DHCP snooping. Điều này có thể được thực hiện để ngăn chặn nguy cơ các cuộc tấn công thông qua các tùy chọn DHCP độc hại bằng lệnh *no ip dhcp snooping information option*.
6. Chuyển đến cổng cho phép cấp phát địa chỉ IP bằng lệnh *interface fa0/1*.
7. Dùng lệnh *ip dhcp snooping trust* để chỉ định rằng cổng này (fa0/1) là một cổng tin cậy đối với DHCP snooping. Nghĩa là switch tin tưởng vào các gói tin DHCP được nhận và gửi qua cổng này và không áp dụng các kiểm tra nghiêm ngặt về

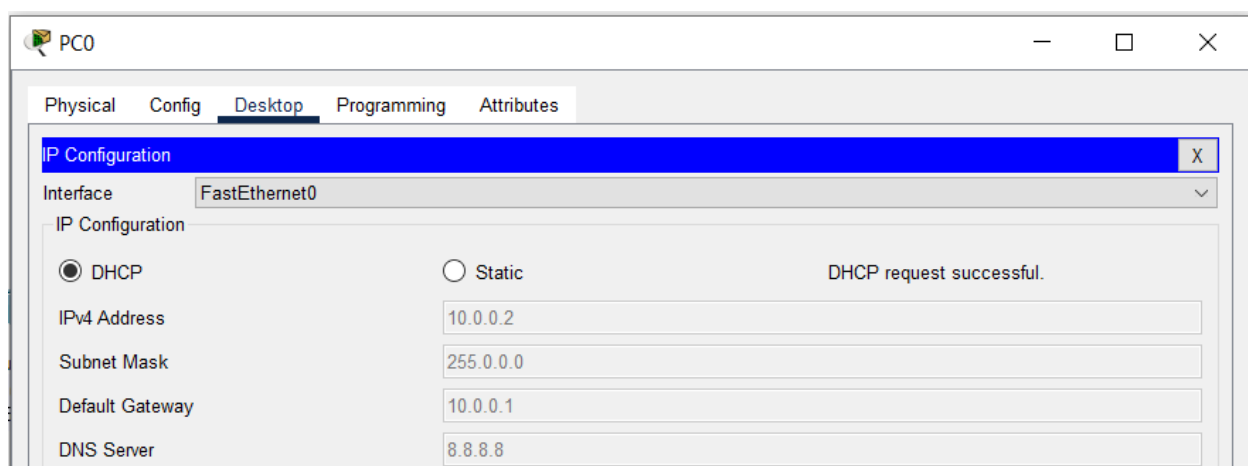
tính hợp lệ của các gói tin DHCP trên cổng này.

8. Dùng lệnh *do write* để lưu lại cấu hình.

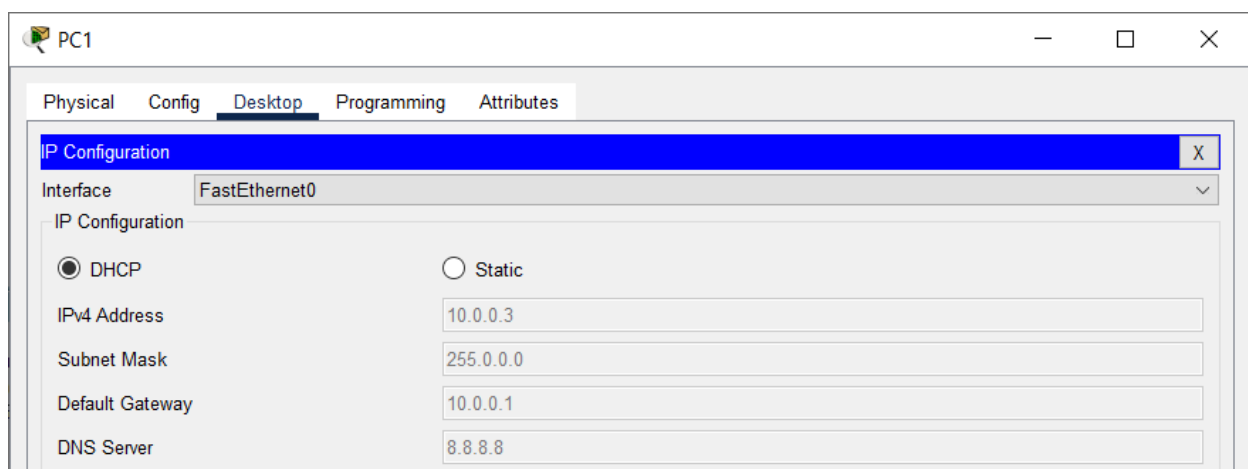


Hình 3-13 Cấu hình DHCP snooping trên switch

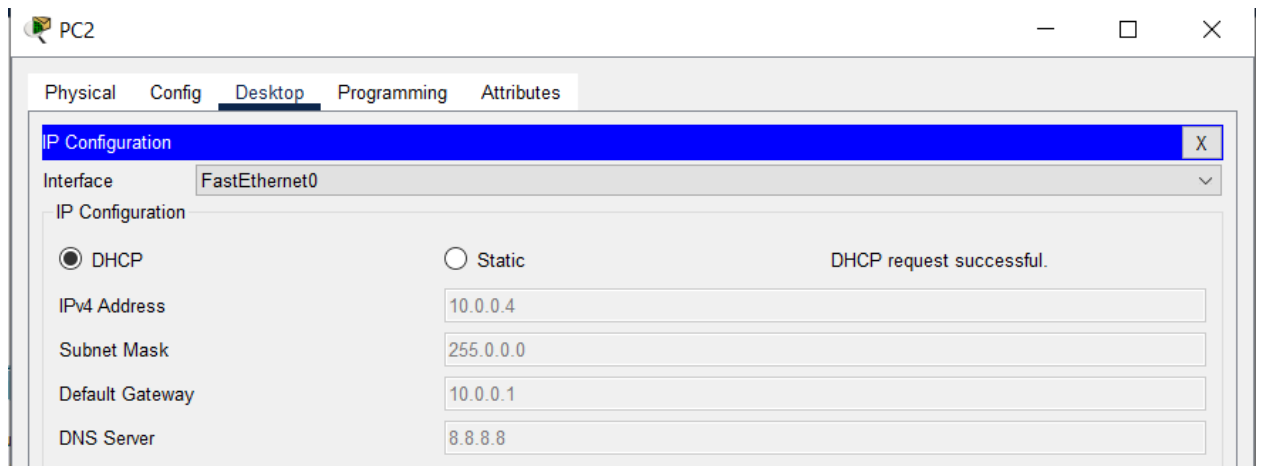
Sau khi lưu lại cấu hình, đặt lại địa chỉ IP trên các PC0, PC1, PC2 để xem kết quả



Hình 3-14 PC0 sau khi cấu hình DHCP snooping trên switch



Hình 3-15 PC1 sau khi cấu hình DHCP snooping trên switch



Hình 3-16 PC2 sau khi cấu hình DHCP snooping trên switch

Thử kết nối thêm vài PC vào switch thì vẫn tương tự, IP và các thông số khác như subnet mask, default gateway đã được nhận từ router thay vì server giả mạo.

3.3. Mô phỏng một cuộc tấn công ARP spoofing và hướng khắc phục

3.3.1. Đặc tả yêu cầu

Mục tiêu:

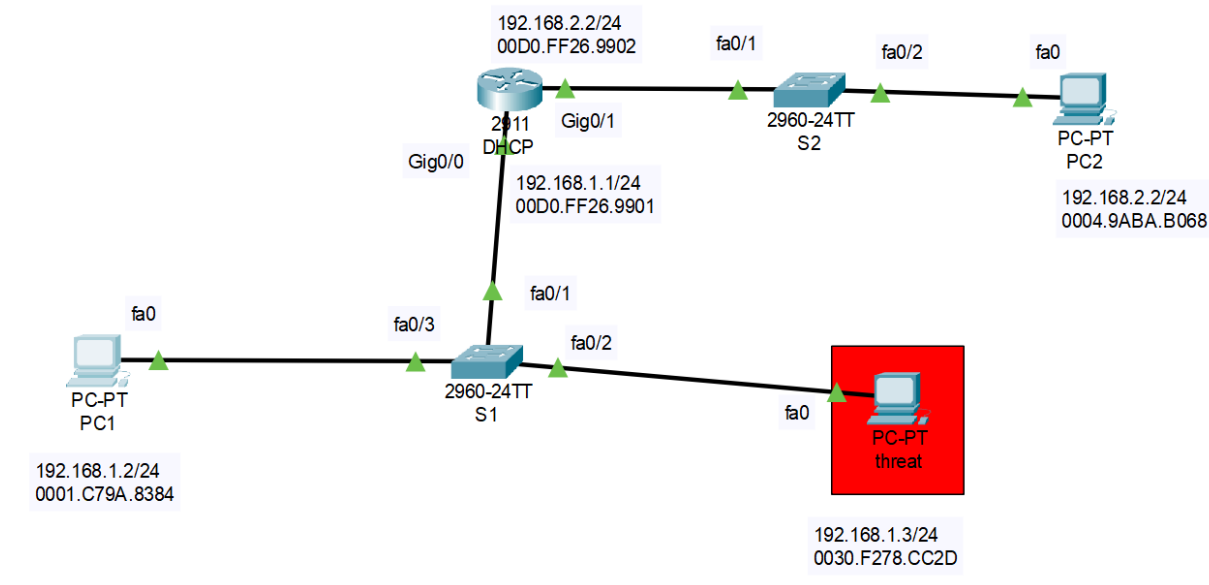
Mô phỏng các cuộc tấn công DHCP Spoofing trên Cisco Packet Tracer.

Đề xuất và triển khai các biện pháp khắc phục để ngăn chặn các loại tấn công này.

Nội dung thực hiện:

Môi trường mô phỏng:

Sử dụng Cisco Packet Tracer để tạo một mạng đơn giản mô phỏng một cuộc tấn công ARP spoofing gồm một Router với tên gọi DHCP đóng vai trò là máy chủ cấp phát địa chỉ IP động, 2 switch nối với 2 cổng của router, 3 PC trong đó có 2 PC thuộc cùng 1 LAN, trong 2 PC này có 1 PC đóng vai trò là kẻ tấn công, 1 PC là nạn nhân của kẻ tấn công, ngoài ra còn 1 PC đại diện cho máy tính không nằm trong LAN, dùng để kiểm tra kết nối của PC nạn nhân sau khi bị tấn công.



Hình 3-17 Mô hình mô phỏng tấn công ARP spoofing

Cài đặt DHCP server: Cấu hình DHCP trên router DHCP để cung cấp IP động cho các máy trạm để chúng có thể giao tiếp bình thường được với nhau.

Giả lập tấn công ARP spoofing: Thêm một máy tấn công vào mạng, sau đó cấu hình máy tấn công gửi các gói tin ARP giả mạo, mạo danh default gateway.

Quan sát phản ứng: Kiểm tra các máy trạm và thiết bị switch để xem sự thay đổi bảng ARP, từ đó xác định các vấn đề phát sinh do việc thay đổi bảng ARP.

Hướng khắc phục: Bật tính năng DHCP snooping trên switch và Cấu hình DAI trên Switch để kiểm tra các gói ARP và chỉ cho phép các gói tin hợp lệ.

3.3.2. Cấu hình DHCP cho router để cấp phát địa chỉ IP tự động

Cấu hình DHCP cho cổng Gig0/0

1. Vào router > CLI để mở giao diện dòng lệnh.
2. Khởi động router bằng lệnh *enable*.
3. Dùng lệnh *configure terminal* để vào chế độ cấu hình toàn cục cho router.
4. Truy cập vào chế độ cấu hình của cổng giao tiếp Gig0/0 trên router bằng lệnh *interface Gig0/0*.
5. Kích hoạt cổng giao tiếp Gig0/0 bằng lệnh *no shutdown* (mặc định là tắt)
6. Gán địa chỉ IP và subnet mask cho cổng Gig0/0 bằng lệnh *ip address 192.168.1.1*

255.255.255.0

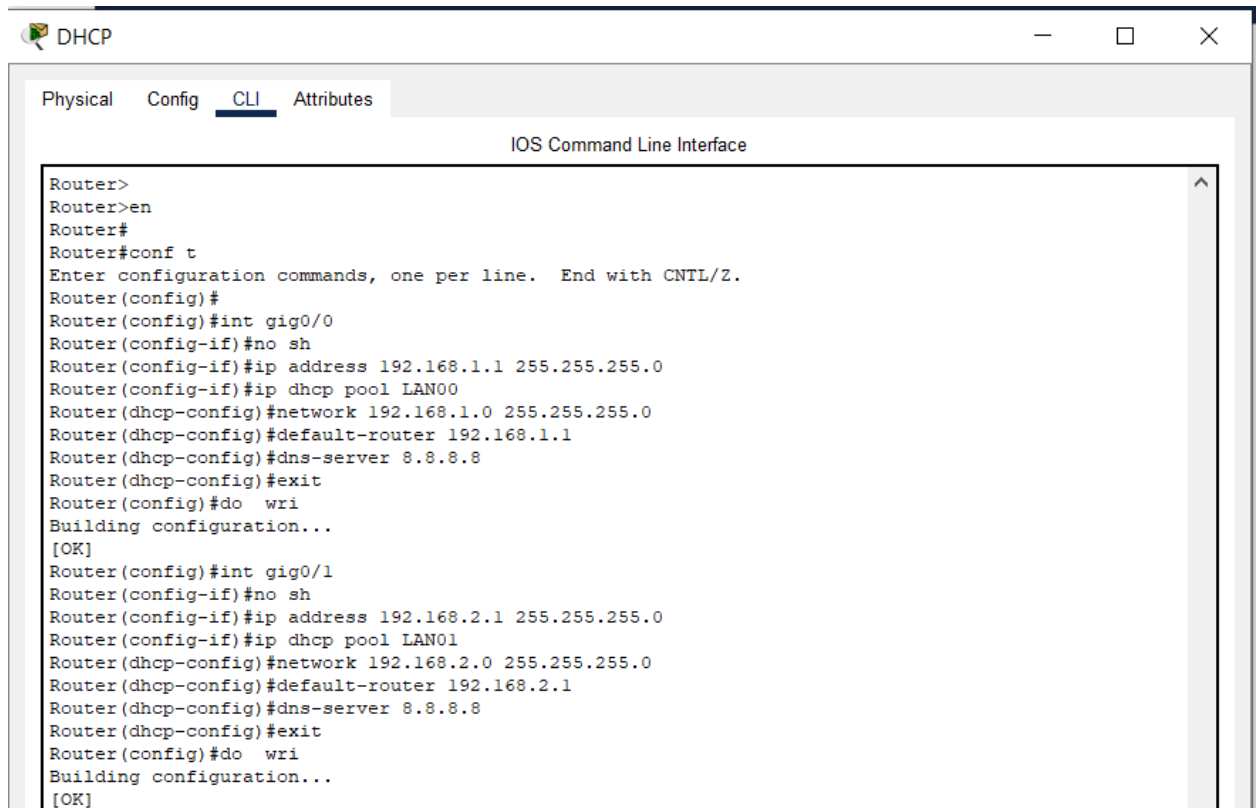
7. Tạo và đặt tên cho một DHCP pool mới tên là "LAN00" bằng lệnh `ip dhcp pool LAN00`
8. Xác định dải địa chỉ IP sẽ được cấp phát bởi DHCP pool "LAN00" bằng lệnh `network 192.168.1.0 255.255.255.0`
9. Cấu hình địa chỉ IP của default gateway cho các thiết bị nhận địa chỉ IP từ DHCP pool "LAN00" bằng lệnh `default-router 192.168.1.1`
10. Dùng lệnh `dns-server 8.8.8.8` để cấu hình địa chỉ IP của DNS server cho các thiết bị nhận địa chỉ IP từ DHCP pool "LAN00"
11. Dùng lệnh `exit` để thoát khỏi chế độ cấu hình DHCP pool và trở về chế độ cấu hình toàn cục.
12. Lưu cấu hình hiện tại vào NVRAM để đảm bảo cấu hình được giữ lại sau khi router khởi động lại bằng lệnh `do write`.

Cấu hình DHCP cho cổng Gig0/1

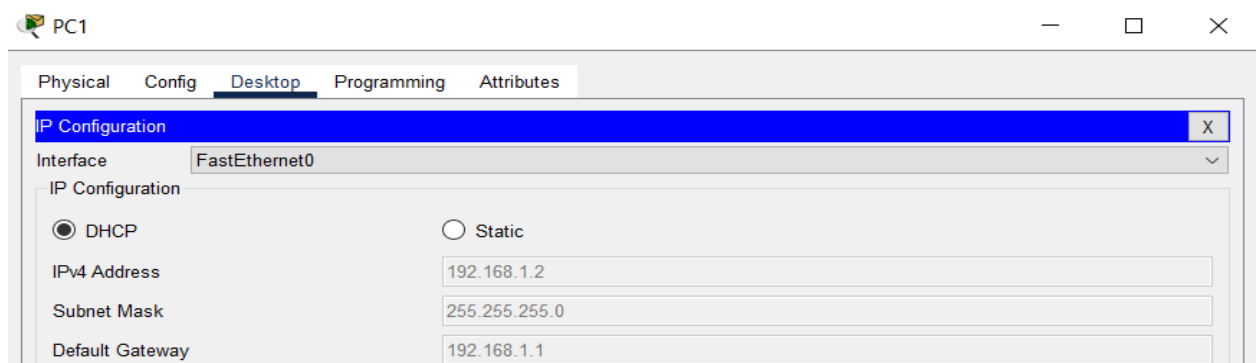
1. Truy cập vào chế độ cấu hình của cổng giao tiếp Gig0/0 trên router bằng lệnh `interface Gig0/1`.
2. Kích hoạt cổng giao tiếp Gig0/1 bằng lệnh `no shutdown` (mặc định là tắt)
3. Gán địa chỉ IP và subnet mask cho cổng Gig0/0 bằng lệnh `ip address 192.168.2.1 255.255.255.0`
4. Tạo và đặt tên cho một DHCP pool mới tên là "LAN01" bằng lệnh `ip dhcp pool LAN01`
5. Xác định dải địa chỉ IP sẽ được cấp phát bởi DHCP pool "LAN01" bằng lệnh `network 192.168.2.0 255.255.255.0`
6. Cấu hình địa chỉ IP của default gateway cho các thiết bị nhận địa chỉ IP từ DHCP pool "LAN01" bằng lệnh `default-router 192.168.2.1`
7. Dùng lệnh `dns-server 8.8.8.8` để cấu hình địa chỉ IP của DNS server cho các thiết bị nhận địa chỉ IP từ DHCP pool "LAN01"
8. Dùng lệnh `exit` để thoát khỏi chế độ cấu hình DHCP pool và trở về chế độ cấu hình

toàn cục.

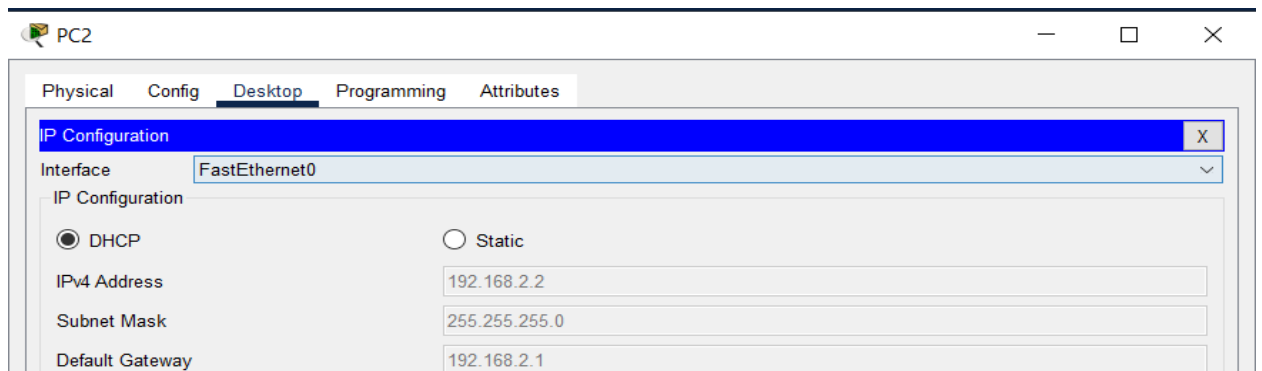
9. Lưu cấu hình hiện tại vào NVRAM để đảm bảo cấu hình được giữ lại sau khi router khởi động lại bằng lệnh `do write`.



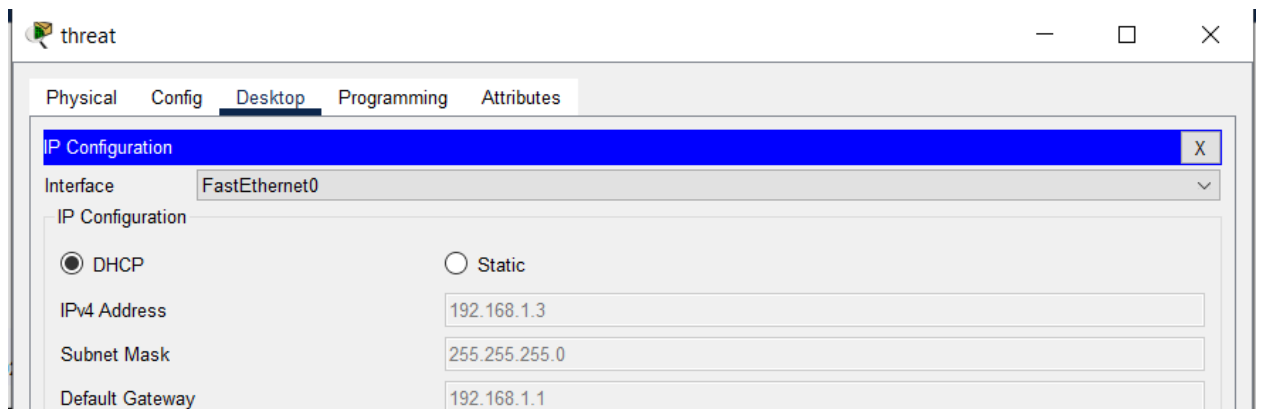
Hình 3-18 Cấu hình DHCP cho router ở cả hai cổng



Hình 3-19 PC1 sau khi nhận IP



Hình 3-20 PC2 sau khi nhận IP

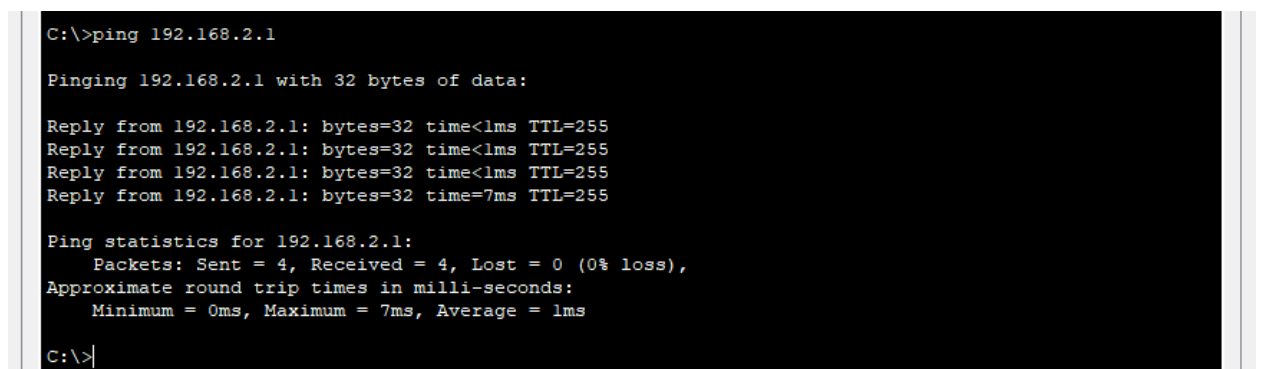


Hình 3-21 PC tấn công sau khi nhận IP

3.3.3. Mô phỏng cách kẻ tấn công thực hiện

Trước tiên cần kiểm tra kết nối giữa PC1 với PC2, PC1 đến PC của kẻ tấn công

Chọn PC1 > desktop > comand promt, sau đó dùng lệnh ping 192.168.2.1 để kiểm tra kết nối với PC2, ping 192.168.1.3 để kiểm tra kết nối với PC của kẻ tấn công.



Hình 3-22 Kiểm tra kết nối giữa PC1 với PC2

```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=7ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 7ms, Average = 1ms

C:\>|
```

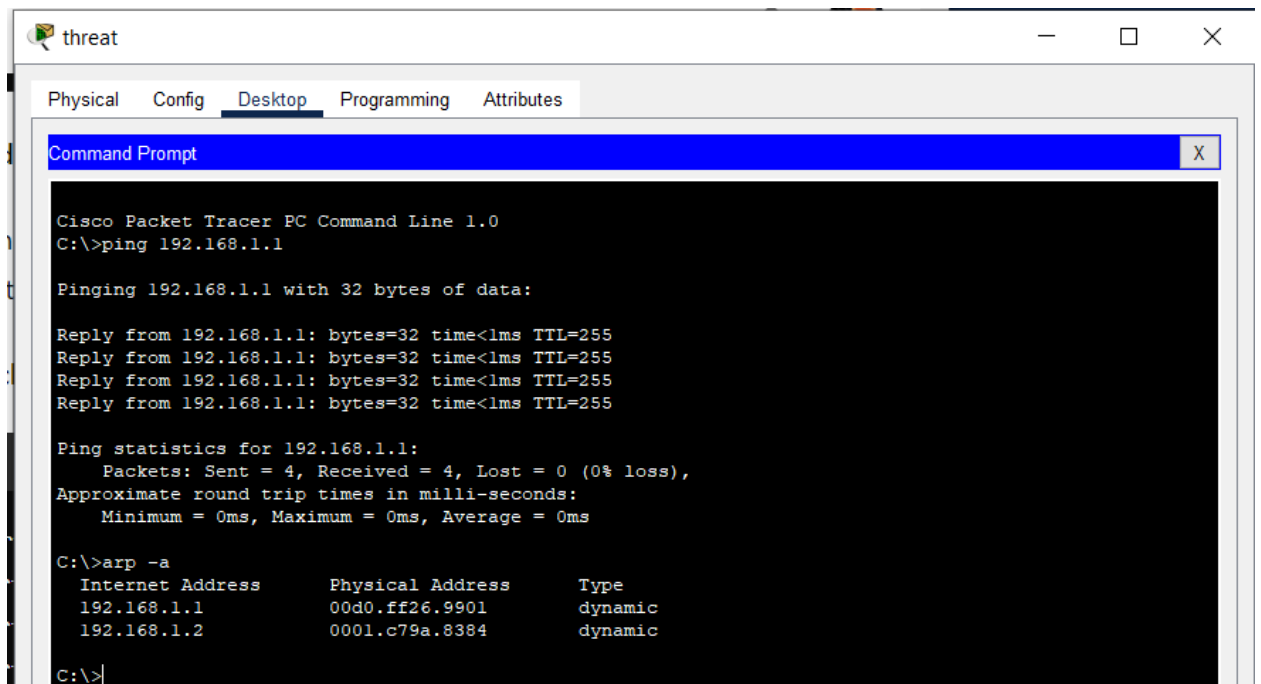
Hình 3-23 Kiểm tra kết nối giữa PC1 với PC của kẻ tấn công

Có thể thấy PC1 đã có thể giao tiếp với PC2 và PC của kẻ tấn công.

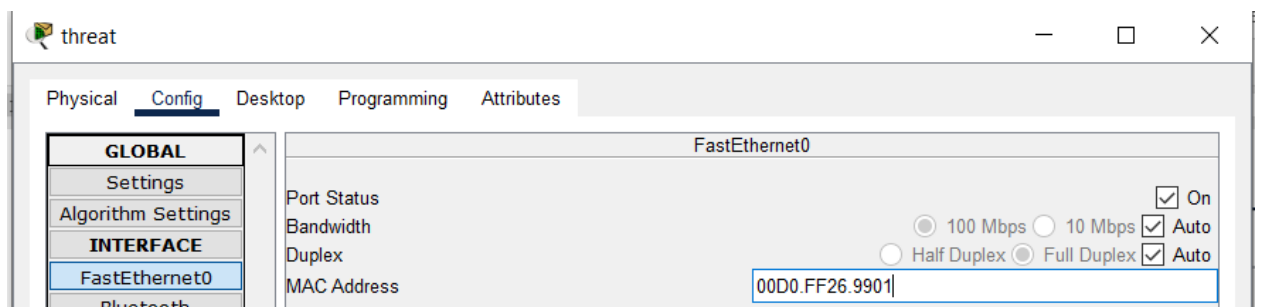
Khi các gói tin ARP di chuyển qua switch, switch sẽ học được địa chỉ MAC của các thiết bị gửi các gói tin đó. Switch sẽ lưu trữ địa chỉ MAC và cổng mà nó nhận được gói tin vào bảng MAC động. Điều này giúp switch biết được địa chỉ MAC nào nằm ở cổng nào, giúp chuyển tiếp các gói tin một cách hiệu quả mà không cần phải gửi đi toàn bộ cổng.

Để tấn công, kẻ tấn công thường giả làm default gateway để bắt gói tin bằng cách thay đổi địa chỉ MAC thành địa chỉ MAC của default gateway, sau đó sẽ ping đến PC của nạn nhân nhằm thay đổi ARP đã lưu trên máy nạn nhân, hậu quả là khi nạn nhân gửi gói tin đến default gateway sẽ bị chuyển hướng đến PC của kẻ tấn công. Để mô phỏng điều này thực hiện theo các bước.

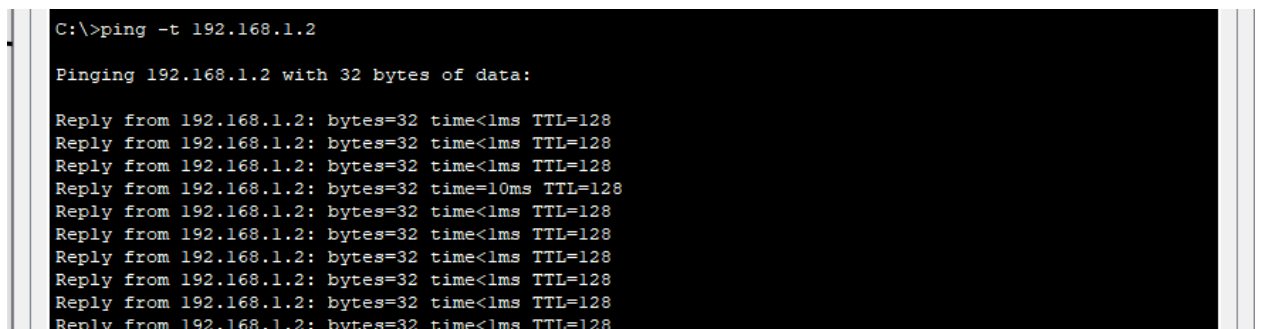
1. Kẻ tấn công ping đến default gateway để tìm kiếm địa chỉ MAC của default gateway, sau đó thay đổi địa chỉ MAC của bản thân thành địa chỉ MAC của default gateway.
2. Sau đó kẻ tấn công ping đến máy nạn nhân, nhằm thay đổi ARP có trên máy nạn nhân và địa MAC lưu trữ trên switch.



Hình 3-24 Kê tấn công gửi gói tin đến default gateway để lấy địa chỉ MAC



Hình 3-25 Đổi địa chỉ MAC của mỗi đe dọa thành địa chỉ MAC của gateway



Hình 3-26 Kê tấn công ping đến máy nạn nhân để cập nhật lại bảng ARP

```

C:\>arp -a
Internet Address      Physical Address      Type
192.168.1.1           00d0.ff26.9901       dynamic
192.168.1.3           0030.f278.cc2d       dynamic

C:\>arp -a
Internet Address      Physical Address      Type
192.168.1.1           00d0.ff26.9901       dynamic
192.168.1.3           00d0.ff26.9901       dynamic

```

Hình 3-27 Bảng ARP trên máy nạn nhân sau khi cập nhật

```

Switch#show mac-add dynamic
Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
1       0001.c79a.8384   DYNAMIC   Fa0/3
1       0030.f278.cc2d   DYNAMIC   Fa0/2
1       00d0.ff26.9901   DYNAMIC   Fa0/1
Switch>show mac-add dynamic
Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
1       0001.c79a.8384   DYNAMIC   Fa0/3
1       00d0.ff26.9901   DYNAMIC   Fa0/2
Switch>

```

Hình 3-28 Bảng địa chỉ MAC lưu trữ trên switch đã bị kẻ tấn công thay đổi

Hậu quả là sau khi thực hiện các bước đó, khi nạn nhân muốn gửi các gói tin đến PC2 (phải thông qua default gateway), gói tin không đi đến default gateway mà lại đi đến PC của kẻ tấn công, tại lúc này, kẻ tấn công có thể thực hiện một số cuộc tấn công khác để giám sát, đánh cắp dữ liệu từ nạn nhân.

```

C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>

```

Hình 3-29 PC1 không thể gửi gói tin đến PC2

3.3.4. Giải pháp phòng chống tấn công ARP spoofing

Để phòng chống ARP spoofing, có thể sử dụng kết hợp ba giải pháp là DHCP snooping, Dynamic ARP Inspection (DAI).

DHCP snooping giám sát và kiểm soát các giao tiếp DHCP trên mạng, xác định các cặp IP-MAC address hợp lệ mà máy chủ DHCP đã cấp phát. Điều này giúp ngăn chặn kẻ

tấn công sử dụng ARP spoofing để phân phối địa chỉ IP giả mạo.

DAI là tính năng giúp switch kiểm tra và từ chối các gói tin ARP không hợp lệ, nơi mà địa chỉ IP và MAC không khớp nhau. Điều này làm cho việc thực hiện ARP spoofing trở nên khó khăn đối với kẻ tấn công.

Để cấu hình DHCP snooping thực hiện theo các bước:

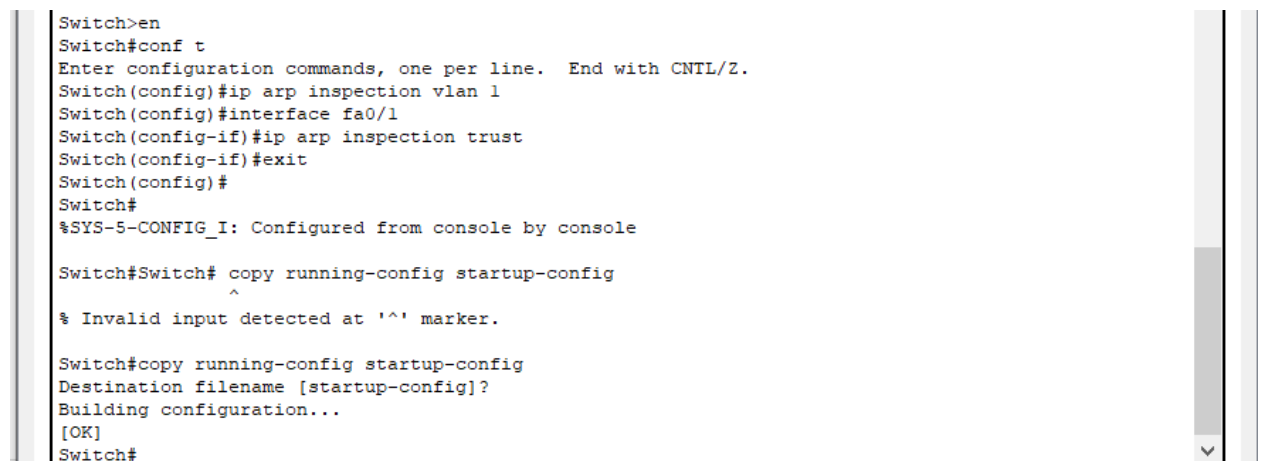
1. Dùng lệnh *enable* để có quyền thực hiện các lệnh cấu hình.
2. Dùng lệnh *configure terminal* để chuyển sang chế độ cấu hình toàn cục để bắt đầu cấu hình các thiết lập trên switch.
3. Dùng lệnh *no ip dhcp snooping information option* để loại bỏ tùy chọn gửi thông tin DHCP Snooping Option (option 82) từ client đến DHCP Server. Option 82 cung cấp thông tin về giao diện, VLAN và địa chỉ IP của client.
4. Dùng lệnh *ip dhcp snooping* để bật tính năng DHCP snooping trên switch. DHCP snooping giám sát các gói tin DHCP trên mạng và chống lại các cuộc tấn công từ kẻ tấn công sử dụng DHCP.
5. Dùng lệnh *ip dhcp snooping vlan 1* để cấu hình DHCP snooping trên VLAN 1.
6. Dùng lệnh *interface fa0/1* để chuyển sang cấu hình cổng FastEthernet 0/1 (cổng để đến default gateway).
7. Dùng lệnh *ip dhcp snooping trust* để đánh dấu cổng FastEthernet 0/1 là cổng tin cậy đối với các gói tin DHCP snooping. Điều này có nghĩa là switch sẽ tin tưởng các gói tin DHCP và không kiểm tra chúng nếu chúng đi qua cổng này.
8. Dùng lệnh *exit* để thoát khỏi chế độ cấu hình của giao diện Ethernet 0/1 và quay lại chế độ cấu hình toàn cục.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip dhcp snooping information option
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 1
Switch(config)#int f0/1
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#exit
Switch(config)#
```

Hình 3-30 Cấu hình DHCP snooping trên switch

Cấu hình tính năng DAI trên switch theo các bước:

1. Dùng lệnh *enable* để có quyền thực hiện các lệnh cấu hình.
2. Dùng lệnh *configure terminal* để chuyển sang chế độ cấu hình toàn cục để bắt đầu cấu hình các thiết lập trên switch.
3. Dùng lệnh *ip arp inspection vlan 1* để bật tính năng (DAI) trên VLAN 1. DAI là một tính năng bảo mật mạng giúp ngăn chặn các cuộc tấn công giả mạo ARP bằng cách kiểm tra tính hợp lệ của các gói tin ARP trên mạng.
4. Dùng lệnh *interface fa0/1* để chuyển sang cấu hình cổng FastEthernet 0/1 (cổng để đến default gateway).
5. Dùng lệnh *ip arp inspection trust* để đánh dấu cổng FastEthernet 0/1 là cổng tin cậy đối với các gói tin ARP Inspection. Khi cấu hình cổng này là tin cậy, switch sẽ không kiểm tra và áp dụng các chính sách DAI lên các gói tin ARP đi qua cổng này.
6. Lưu lại cấu hình trên switch bằng lệnh *copy running-config startup-config*.



```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ip arp inspection vlan 1
Switch(config)#interface fa0/1
Switch(config-if)#ip arp inspection trust
Switch(config-if)#exit
Switch(config)#
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#Switch# copy running-config startup-config
^
% Invalid input detected at '^' marker.

Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#
```

Hình 3-31 Cấu hình DAI trên switch

Sau khi cấu hình, kiểm tra lại xem rằng liệu PC của kẻ tấn công gửi gói tin đến cổng đến default gateway và PC1 có thành công không.


```

C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

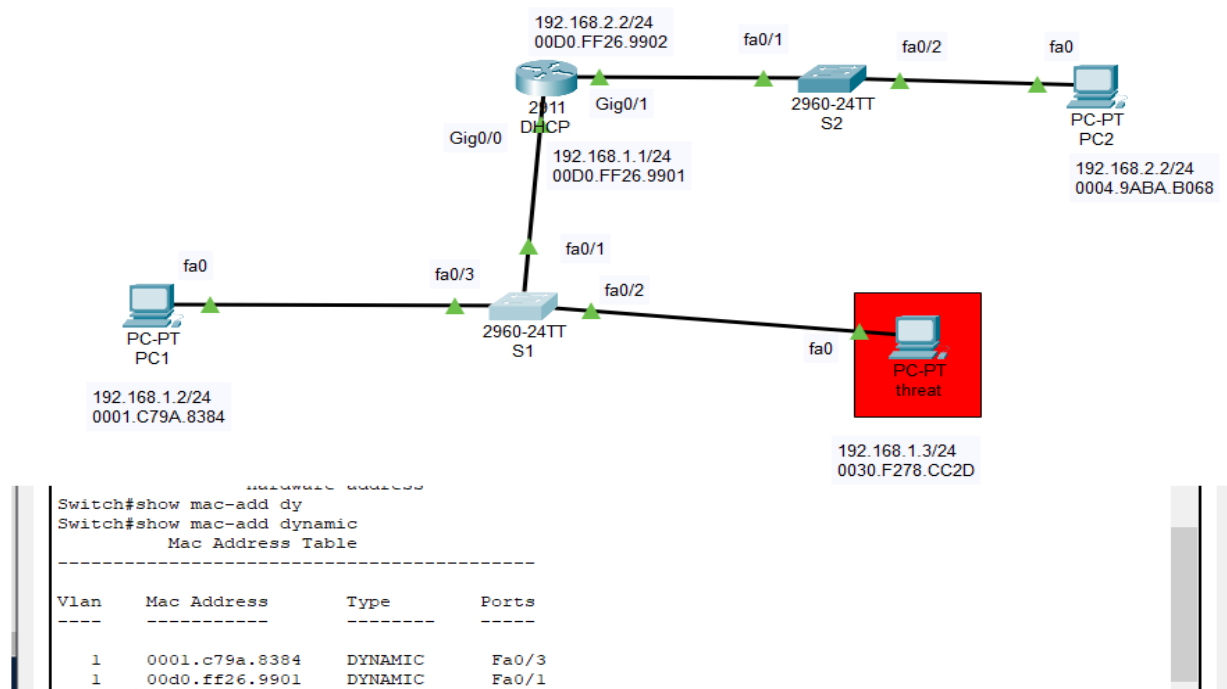
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>

```

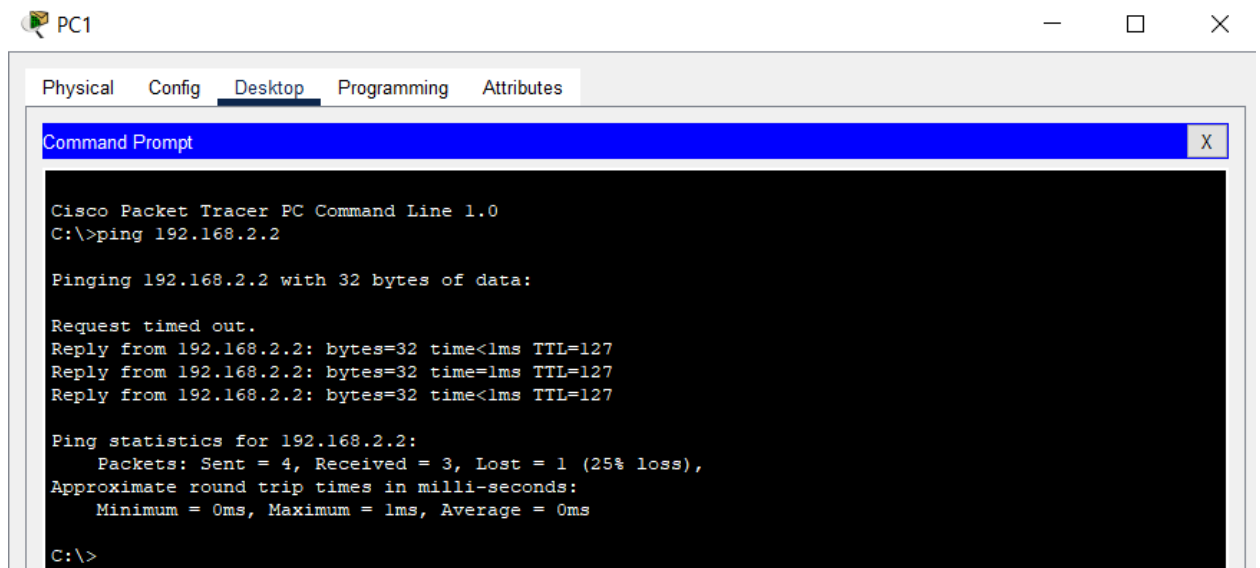
Hình 3-32 Kiểm tra kết nối giữa PC của kẻ tấn công với default gateway và PC1
 Có thể thấy, khi kẻ tấn công gửi gói tin đến default gateway thì sẽ bị bác bỏ.



Hình 3-33 Bảng MAC sau khi dùng DAI

Khi kẻ tấn công giả mạo MAC của cổng đến default gateway gửi gói tin đến PC1

thì switch đã không cập nhật lại địa chỉ MAC vì trên switch đã được cấu hình DAI để phòng chống cuộc tấn công giả mạo ARP.



Hình 3-34 Kiểm tra kết nối giữa PC1 và PC2

Có thể thấy sau khi cấu hình DAI thì PC1 có thể ping được PC2 vì gói tin đã đi qua default gateway để đến PC2 thay vì đi đến PC của kẻ tấn công.

CHƯƠNG 4. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

4.1. Kết luận

Bảo mật mạng không chỉ đơn giản là một vấn đề kỹ thuật, mà là một yếu tố cần thiết để đảm bảo tính bảo mật, toàn vẹn và sẵn sàng của hệ thống thông tin và dịch vụ mạng. Nghiên cứu đã chỉ ra rằng các giao thức mạng phổ biến như TCP/IP, DNS, và các giao thức ứng dụng như HTTP đều tồn tại nhiều lỗ hổng bảo mật. Các cuộc tấn công mạng có thể dẫn đến mất thông tin nhạy cảm, thất thoát dữ liệu, hoặc thậm chí là phá hủy hệ thống. Các giải pháp bảo mật như mã hóa, phân quyền, kiểm tra định kỳ và giám sát hệ thống đang ngày càng được phát triển và áp dụng để giảm thiểu nguy cơ. Để đối phó với các mối đe dọa ngày càng phức tạp, cần có các chiến lược phòng ngừa, phản ứng nhanh và khả năng khôi phục hệ thống sau khi xảy ra sự cố.

Kết quả đạt được:

Thông qua việc nghiên cứu giúp đưa ra một cái nhìn tổng quan về giao thức mạng, các lỗ hổng bảo mật phổ biến trong các giao thức mạng. Điều này cung cấp cơ sở để áp dụng các biện pháp bảo mật hiệu quả hơn, giúp hiểu sâu hơn về các giao thức cũng như các vấn đề bảo mật trong giao thức.

Thông qua nghiên cứu giúp nâng cao nhận thức và hiểu biết về mối đe dọa bảo mật mạng, hậu quả của chúng và tầm quan trọng của việc áp dụng các biện pháp bảo mật phù hợp để chống lại các mối đe dọa không mong muốn.

Hạn chế:

Do tính chất phức tạp và đa dạng của các vấn đề bảo mật mạng, nghiên cứu có thể chưa bao quát hoàn toàn mọi khía cạnh của các vấn đề bảo mật và chưa đưa ra được biện pháp đối với từng vấn đề bảo mật đó.

Nghiên cứu dựa trên các tài liệu công khai và môi trường thí nghiệm bằng phần mềm giả lập, giả định, thiếu đi các dữ liệu và thông tin thực tiễn.

Một số mô phỏng tấn công (cụ thể là tấn công DNS) và biện pháp phòng chống không thể triển khai trong môi trường giả lập Packet Tracer vì hạn chế về tính năng và công cụ mô phỏng tấn công.

4.2. Hướng phát triển

Phân tích sâu hơn về các vấn đề bảo mật trong các giao thức phổ biến, nghiên cứu các lỗ hổng và đưa ra biện pháp khắc phục tương ứng.

Sử dụng thêm nhiều công cụ mã nguồn mở như Wireshark, các công cụ trong Kali Linux để mô phỏng tấn công, phòng ngự, phân tích và đánh giá các lỗ hổng bảo mật đã biết và tiềm ẩn.

Nghiên cứu các chính sách bảo mật, áp dụng những chính sách đó vào môi trường thực tế nhằm hạn chế rủi ro về mạng.

DANH MỤC TÀI LIỆU THAM KHẢO

- [1] J. F. Kurose, Computer Networking: A Top-Down Approach, Boston: Pearson, 2017.
- [2] H. v. m. Cisco, "Khóa học CyberOps Associate," [Online]. Available: <https://www.netacad.com/>. [Accessed 18 04 2024].
- [3] A. S. Gillis, "DHCP (Dynamic Host Configuration Protocol)," [Online]. Available: <https://www.techtarget.com/searchnetworking/definition/DHCP>. [Accessed 10 6 2024].
- [4] Howard, "What Is DHCP Snooping and How It Works?," 24 12 2021. [Online]. Available: <https://community.fs.com/article/what-is-dhcp-snooping-and-how-it-works.html>. [Accessed 11 06 2024].
- [5] P. Global, "The Ultimate Guide to DHCP Spoofing and Starvation Attacks," 26 5 2022. [Online]. Available: <https://info.pivitglobal.com/resources/dhcp-spoofing-and-starvation-attacks>. [Accessed 12 06 2024].
- [6] geeksforgeeks, "What is Sniffing Attack in System Hacking?," 21 8 2022. [Online]. Available: <https://www.geeksforgeeks.org/what-is-sniffing-attack-in-system-hacking/>. [Accessed 13 06 2024].