TRƯỜNG ĐẠI HỌC KHOA HỌC
KHOA CÔNG NGHỆ THÔNG TIN

TIỂU LUẬN MÔN HỌC

AN NINH MẠNG

DÒ TÌM HOST BẰNG NMAP

Giáo viên hướng dẫn:
Ths. Võ Việt Dũng

Sinh viên thực hiện :
1. Mai Anh Quân
2. Đặng Ngọc Nhật Tâm
3. Phan Văn Minh Trí
4. Cao Tuấn Anh
5. Huỳnh Châu Huy

Nhóm: 1
Lớp: An Ninh Mạng - Nhóm 2
Năm học: 2025-2026

Huế, 10/2025

I. DANH MỤC CÁC TỪ VIẾT TẮT

Từ viết tắt	Tiếng Anh	Giải thích
IP	Internet Protocol	Giao thức Internet
TCP	Transmission Control Protocol	Giao thức điều khiển truyền vận
UDP	User Datagram Protocol	Giao thức gói dữ liệu người dùng
ICMP	Internet Control Message Protocol	Giao thức thông điệp kiểm soát Internet (thường dùng để Ping)
ARP	Address Resolution Protocol	Giao thức phân giải địa chỉ (dùng trong mạng LAN)
MAC	Media Access Control	Địa chỉ vật lý của thiết bị mạng
TTL	Time To Live	Thời gian tồn tại của gói tin

II. MỤC LỤC

III. MỞ ĐẦU

Trong bối cảnh công nghệ thông tin ngày càng phát triển, hệ thống mạng máy tính đã trở thành nền tảng không thể thiếu trong hầu hết các tổ chức, doanh nghiệp và cá nhân. Cùng với sự phát triển đó, các mối đe dọa về an ninh mạng cũng ngày càng gia tăng cả về số lượng lẫn mức độ tinh vi. Việc đảm bảo an toàn cho hệ thống mạng không chỉ dừng lại ở việc bảo vệ dữ liệu, mà còn đòi hỏi khả năng **phát hiện, giám sát và quản lý các thiết bị đang hoạt động trong mạng**.

Một trong những bước quan trọng trong quá trình đánh giá và đảm bảo an ninh mạng là **dò tìm host**. Thông qua việc dò tìm host, người quản trị mạng và chuyên gia bảo mật có thể xác định được những thiết bị nào đang tồn tại và hoạt động trong hệ thống, từ đó xây dựng các biện pháp kiểm soát, giám sát và phòng chống tấn công phù hợp. Nếu không nắm rõ danh sách các host trong mạng, hệ thống có thể tồn tại những thiết bị trái phép hoặc cấu hình sai, tiềm ẩn nhiều rủi ro bảo mật nghiêm trọng.

Nmap (Network Mapper) là một trong những công cụ phổ biến và mạnh mẽ nhất hiện nay được sử dụng để quét mạng và dò tìm host. Với khả năng hỗ trợ nhiều kỹ thuật phát hiện host khác nhau, Nmap cho phép người dùng xác định trạng thái hoạt động của các thiết bị ngay cả trong những môi trường mạng có cơ chế bảo mật nghiêm ngặt. Nhờ đó, Nmap được ứng dụng rộng rãi trong quản trị mạng, kiểm thử xâm nhập và nghiên cứu an ninh mạng.

Xuất phát từ những lý do trên, đề tài **"Dò tìm host bằng Nmap"** được lựa chọn nhằm tìm hiểu nguyên lý, phương pháp và ứng dụng của Nmap trong việc phát hiện host trong mạng máy tính. Thông qua đề tài này, người học có thể nắm được quy trình dò tìm host cơ bản, hiểu rõ vai trò của từng kỹ thuật, đồng thời nâng cao nhận thức về việc sử dụng công cụ quét mạng một cách hiệu quả và đúng pháp luật.

IV. NỘI DUNG

1. Giới thiệu chung

1.1. Khái niệm host trong mạng máy tính

Trong mạng máy tính, **host** là bất kỳ thiết bị nào được kết nối vào mạng và có khả năng **gửi, nhận hoặc xử lý dữ liệu**. Mỗi host thường được định danh bằng **địa chỉ IP** (IPv4 hoặc IPv6) và có thể đi kèm với các thông tin khác như địa chỉ MAC, tên miền (hostname).

Host có thể là:

- Máy tính cá nhân (PC, laptop)
- Máy chủ (server)
- Thiết bị mạng (router, switch có IP quản lý)
- Thiết bị IoT (camera, máy in, smart TV…)

Trong an ninh mạng, khái niệm host không chỉ đơn thuần là một thiết bị, mà còn là **một thực thể có thể trở thành mục tiêu tấn công**, bởi mỗi host có thể đang chạy hệ điều hành, dịch vụ mạng hoặc ứng dụng tiềm ẩn lỗ hổng bảo mật.

1.2. Vì sao cần dò tìm host trong an ninh mạng

Dò tìm host (Host Discovery) là bước **đầu tiên và bắt buộc** trong hầu hết các hoạt động kiểm tra, giám sát và đánh giá an ninh mạng. Mục đích của bước này là xác định **những host nào đang hoạt động (host up)** trong một mạng hoặc dải địa chỉ IP cụ thể.

Trong an ninh mạng, việc dò tìm host có vai trò quan trọng vì:

- Giúp **xác định phạm vi mạng thực tế** đang tồn tại
- Phát hiện các **thiết bị trái phép hoặc không được quản lý**
- Tránh quét cổng hoặc tấn công nhầm vào các IP không tồn tại
- Là cơ sở cho các bước tiếp theo như:
    - Quét cổng (Port Scanning)
    - Phát hiện dịch vụ
    - Phân tích lỗ hổng

Đối với quản trị viên hệ thống, dò tìm host giúp:

- Kiểm kê thiết bị trong mạng
- Phát hiện host “chết” hoặc host mới xuất hiện bất thường

- Hỗ trợ xử lý sự cố mạng

Đối với kiểm thử xâm nhập (Pentesting), dò tìm host giúp kẻ kiểm thử xác định **bề mặt tấn công (attack surface)** ban đầu của hệ thống.

1.3. Vai trò của Nmap trong việc phát hiện host

Nmap (Network Mapper) là một công cụ mã nguồn mở phổ biến, được sử dụng rộng rãi trong lĩnh vực an ninh mạng để **quét mạng và phát hiện host**. Một trong những chức năng quan trọng nhất của Nmap là **Host Discovery**.

Nmap hỗ trợ nhiều kỹ thuật dò tìm host khác nhau như:

- ICMP Ping
- TCP SYN Ping
- TCP ACK Ping
- UDP Ping
- ARP Scan (trong mạng LAN)

Nhờ các kỹ thuật này, Nmap có khả năng:

- Phát hiện host ngay cả khi **ICMP bị chặn**
- Hoạt động linh hoạt trong nhiều môi trường mạng khác nhau
- Giảm thiểu thời gian quét và lưu lượng mạng không cần thiết

Ngoài ra, Nmap còn cho phép người dùng:

- Tùy chỉnh phương thức dò tìm host
- Kết hợp host discovery với các kỹ thuật quét khác
- Phân tích và xuất kết quả dưới nhiều định dạng

Chính vì tính linh hoạt, chính xác và dễ sử dụng, Nmap trở thành công cụ tiêu chuẩn trong cả **quản trị mạng lẫn an ninh mạng**.

1.4. Phạm vi và mục tiêu của việc dò tìm host

Phạm vi của việc dò tìm host thường được giới hạn trong:

- Một mạng nội bộ (LAN)
- Một dải địa chỉ IP xác định
- Hệ thống được cho phép kiểm tra

Việc giới hạn phạm vi là cần thiết để:

- Tránh vi phạm pháp luật

- Tránh ảnh hưởng đến các hệ thống không liên quan
- Đảm bảo tính chính xác của kết quả

Mục tiêu chính của việc dò tìm host bao gồm:

- Xác định các host đang hoạt động trong mạng
- Thu hẹp phạm vi quét cho các bước phân tích tiếp theo
- Đánh giá mức độ "hiển thị" của hệ thống trên mạng
- Hỗ trợ phát hiện rủi ro và điểm yếu bảo mật

Tóm lại, dò tìm host là bước nền tảng trong quá trình đánh giá an ninh mạng, giúp người quản trị và chuyên gia bảo mật **nắm được toàn cảnh hệ thống** trước khi thực hiện các hoạt động chuyên sâu hơn.

2. Tổng quan về Nmap

2.1. Nmap là gì?

Nmap (viết tắt của *Network Mapper*) là một **công cụ mã nguồn mở** được sử dụng để quét mạng và đánh giá mức độ an toàn của hệ thống. Nmap cho phép người dùng khám phá các thiết bị đang hoạt động trong mạng, xác định các cổng mở, dịch vụ đang chạy cũng như thu thập nhiều thông tin quan trọng phục vụ cho quản trị và an ninh mạng.

Nmap hoạt động chủ yếu bằng cách **gửi các gói tin mạng được thiết kế đặc biệt** đến hệ thống mục tiêu và phân tích phản hồi nhận được. Dựa vào phản hồi này, Nmap có thể xác định trạng thái của host, cổng mạng, hệ điều hành và các dịch vụ đang hoạt động. Nhờ tính linh hoạt và độ chính xác cao, Nmap được sử dụng rộng rãi trong quản trị hệ thống, kiểm thử xâm nhập (penetration testing) và nghiên cứu bảo mật.

2.2. Lịch sử phát triển ngắn gọn

Nmap được phát triển lần đầu vào năm **1997** bởi Gordon Lyon (biệt danh *Fyodor*). Ban đầu, Nmap được tạo ra với mục đích giúp quản trị viên mạng **quản lý và giám sát các thiết bị trong mạng lớn**. Trải qua nhiều năm phát triển, Nmap không ngừng được cải tiến và bổ sung thêm nhiều tính năng mới.

Hiện nay, Nmap được duy trì và phát triển bởi cộng đồng mã nguồn mở cùng nhóm phát triển chính thức. Công cụ này hỗ trợ hầu hết các hệ điều hành phổ biến như Linux, Windows và macOS. Ngoài phiên bản dòng lệnh, Nmap còn có giao diện đồ họa mang tên **Zenmap**, giúp người dùng mới dễ tiếp cận và sử dụng hơn.

2.3. Các chức năng chính của Nmap

2.3.1. Dò tìm host

Dò tìm host là một trong những chức năng cơ bản và quan trọng nhất của Nmap. Chức năng này cho phép xác định **những thiết bị nào đang hoạt động (host up)** trong một dải địa chỉ IP hoặc mạng cụ thể.

Nmap hỗ trợ nhiều phương pháp dò tìm host như:

- ICMP Ping
- TCP SYN Ping
- TCP ACK Ping
- UDP Ping
- ARP Scan (trong mạng LAN)

Việc dò tìm host giúp người dùng thu hẹp phạm vi quét, giảm thời gian và tài nguyên hệ thống, đồng thời là bước tiền đề cho các hoạt động phân tích chuyên sâu hơn như quét cổng và phát hiện lỗ hổng.

2.3.2. Quét cổng

Quét cổng (Port Scanning) là chức năng cho phép Nmap xác định **các cổng mạng đang mở, đóng hoặc bị lọc** trên một host mục tiêu. Thông qua việc quét cổng, người dùng có thể biết được những dịch vụ nào đang sẵn sàng nhận kết nối từ bên ngoài.

Nmap hỗ trợ nhiều kỹ thuật quét cổng khác nhau như:

- TCP SYN Scan
- TCP Connect Scan
- UDP Scan
- FIN, NULL, Xmas Scan

Chức năng quét cổng đóng vai trò quan trọng trong an ninh mạng vì các cổng mở thường là **điểm xâm nhập tiềm năng** của kẻ tấn công nếu dịch vụ phía sau có lỗ hổng hoặc cấu hình không an toàn.

2.3.3. Phát hiện hệ điều hành và dịch vụ

Ngoài dò tìm host và quét cổng, Nmap còn có khả năng **phát hiện hệ điều hành (OS Detection)** và **nhận diện dịch vụ đang chạy trên các cổng**.

- Phát hiện hệ điều hành: Nmap phân tích các đặc điểm phản hồi của hệ thống mục tiêu để suy đoán hệ điều hành đang sử dụng (Windows, Linux, Unix, v.v.).

- Phát hiện dịch vụ và phiên bản: Nmap có thể xác định loại dịch vụ (HTTP, FTP, SSH,…) và thậm chí là phiên bản phần mềm đang chạy.

Thông tin này rất quan trọng trong việc:

- Đánh giá mức độ bảo mật của hệ thống
- Xác định các phiên bản phần mềm có lỗ hổng
- Hỗ trợ quá trình kiểm thử xâm nhập

2.4. Ưu điểm và hạn chế của Nmap

Ưu điểm:

- Là công cụ mã nguồn mở, miễn phí
- Hỗ trợ nhiều kỹ thuật quét linh hoạt
- Hoạt động tốt trong nhiều môi trường mạng
- Được cộng đồng sử dụng rộng rãi và tài liệu phong phú
- Có thể mở rộng thông qua Nmap Scripting Engine (NSE)

Hạn chế:

- Có thể bị phát hiện bởi hệ thống IDS/IPS
- Một số kỹ thuật quét có thể bị firewall chặn
- Cần kiến thức mạng để sử dụng hiệu quả
- Việc sử dụng không đúng phạm vi cho phép có thể vi phạm pháp luật

3. Khái niệm dò tìm host (Host Discovery)

3.1. Dò tìm host là gì?

Dò tìm host (Host Discovery) là quá trình **xác định sự tồn tại và trạng thái hoạt động của các thiết bị** trong một mạng hoặc một dải địa chỉ IP cụ thể. Mục tiêu của quá trình này là trả lời câu hỏi: *"Những host nào đang hoạt động trên mạng?"*.

Trong quá trình dò tìm host, công cụ quét sẽ gửi các gói tin mạng (ICMP, TCP, UDP hoặc ARP) đến các địa chỉ IP mục tiêu và phân tích phản hồi nhận được. Nếu host phản hồi theo một cách nhất định, công cụ sẽ kết luận host đó đang hoạt động. Ngược lại, nếu không nhận được phản hồi, host có thể đang tắt, không tồn tại hoặc bị chặn bởi các cơ chế bảo mật.

Dò tìm host thường là **bước đầu tiên** trong quá trình quét mạng và đánh giá an ninh hệ thống. Việc thực hiện đúng bước này giúp giảm thiểu thời gian quét, hạn chế

lưu lượng mạng không cần thiết và nâng cao độ chính xác cho các bước phân tích tiếp theo.

3.2. Sự khác nhau giữa Host Discovery và Port Scanning

Mặc dù đều là các kỹ thuật quét mạng, **Host Discovery** và **Port Scanning** có mục đích và phạm vi khác nhau:

Host Discovery:

- Mục tiêu: Xác định host có tồn tại và đang hoạt động hay không
- Phạm vi: Toàn bộ dải địa chỉ IP
- Kết quả: Danh sách các host "up"
- Thường không quan tâm đến dịch vụ hoặc cổng cụ thể

Port Scanning:

- Mục tiêu: Xác định các cổng mở, đóng hoặc bị lọc trên một host cụ thể
- Phạm vi: Một hoặc nhiều host đã được xác định
- Kết quả: Danh sách các cổng và trạng thái của chúng
- Phục vụ cho việc phát hiện dịch vụ và lỗ hổng

Nói cách khác, **host discovery giúp trả lời "có host nào ở đó không?"**, còn **port scanning giúp trả lời "host đó đang mở những cổng nào?"**. Trong thực tế, host discovery thường được thực hiện trước, sau đó mới đến port scanning để tối ưu hiệu quả quét.

3.3. Các trạng thái host

Trong quá trình dò tìm host, Nmap có thể phân loại trạng thái của host thành nhiều dạng khác nhau. Tuy nhiên, phổ biến nhất là ba trạng thái sau:

3.3.1. Host up

Host up là trạng thái cho biết **host đang hoạt động và có phản hồi** đối với các gói tin dò tìm được gửi đến. Phản hồi này có thể là:

- ICMP Echo Reply
- TCP SYN/ACK
- TCP RST
- Phản hồi ARP

Khi một host được xác định là “up”, điều đó cho thấy thiết bị đang tồn tại trong mạng và có thể trở thành mục tiêu cho các bước quét tiếp theo như quét cổng hoặc phát hiện dịch vụ.

3.3.2. Host down

Host down là trạng thái cho biết **không nhận được bất kỳ phản hồi nào** từ địa chỉ IP mục tiêu sau khi gửi các gói tin dò tìm. Trạng thái này có thể xảy ra trong các trường hợp:

- Host không tồn tại
- Host đang tắt hoặc mất kết nối mạng
- Host không phản hồi các gói tin dò tìm

Trong một số trường hợp, host down không hoàn toàn có nghĩa là host không tồn tại, mà có thể do cấu hình mạng hoặc chính sách bảo mật ngăn chặn phản hồi.

3.3.3. Host bị firewall chặn

Đây là trạng thái khi host **có tồn tại và đang hoạt động**, nhưng các gói tin dò tìm bị **firewall hoặc hệ thống IDS/IPS** chặn lại. Kết quả là công cụ quét không nhận được phản hồi hoặc nhận được phản hồi không đầy đủ.

Đặc điểm của host bị firewall chặn:

- Không trả lời ICMP Ping
- Các cổng có thể ở trạng thái “filtered”
- Dễ bị nhầm lẫn với host down

Trong trường hợp này, Nmap thường cần sử dụng các kỹ thuật dò tìm nâng cao hoặc **bỏ qua bước host discovery** để tiếp tục quét. Việc nhận biết host bị firewall chặn giúp người dùng đánh giá được **mức độ bảo vệ của hệ thống mạng**.

4. Các phương pháp dò tìm host trong Nmap

Nmap hỗ trợ nhiều phương pháp dò tìm host khác nhau nhằm thích nghi với từng môi trường mạng và cơ chế bảo mật. Mỗi phương pháp dựa trên một loại gói tin mạng và có ưu, nhược điểm riêng. Việc lựa chọn phương pháp phù hợp giúp nâng cao độ chính xác của quá trình dò tìm host và giảm thiểu khả năng bị chặn.

4.1. ICMP Ping Scan

Nguyên lý hoạt động:

ICMP Ping Scan hoạt động dựa trên giao thức **ICMP (Internet Control Message Protocol)**, một giao thức được sử dụng chủ yếu để gửi các thông báo lỗi và kiểm tra khả năng kết nối trong mạng IP. Khi thực hiện ICMP Ping Scan, Nmap gửi các gói tin ICMP đến host mục tiêu để kiểm tra xem host có phản hồi hay không.

Nếu host đang hoạt động và không bị chặn ICMP, nó sẽ gửi phản hồi lại cho máy quét. Dựa vào phản hồi này, Nmap xác định host đang ở trạng thái "up".

Gói tin ICMP Echo Request / Reply:

- **ICMP Echo Request**: Gói tin được gửi từ máy quét đến host mục tiêu để yêu cầu phản hồi.
- **ICMP Echo Reply**: Gói tin phản hồi từ host mục tiêu gửi lại, xác nhận rằng host đang hoạt động.

Cơ chế này tương tự như lệnh ping thông thường trong hệ điều hành.

Lệnh:

```
nmap -sn 192.168.1.0/24
```

Lệnh trên yêu cầu Nmap quét toàn bộ dải mạng 192.168.1.0/24 và chỉ thực hiện **dò tìm host**, không quét cổng.

Ưu điểm & hạn chế

Ưu điểm:

- Đơn giản, dễ sử dụng
- Tốc độ nhanh
- Ít gây tải cho mạng

Hạn chế:

- Dễ bị firewall chặn ICMP
- Nhiều hệ thống tắt phản hồi ICMP vì lý do bảo mật
- Độ chính xác thấp trong môi trường mạng có chính sách bảo mật nghiêm ngặt

4.2. TCP SYN Ping

Nguyên lý TCP SYN

TCP SYN Ping dựa trên **quá trình bắt tay ba bước (three-way handshake)** của giao thức TCP. Nmap gửi gói **TCP SYN** đến một hoặc nhiều cổng trên host mục tiêu. Nếu host tồn tại, nó sẽ phản hồi bằng:

- **SYN/ACK** (cổng mở), hoặc

- **RST** (cổng đóng)

Cả hai phản hồi này đều cho thấy host đang hoạt động.

Khi nào nên dùng

TCP SYN Ping được sử dụng khi:

- ICMP bị firewall chặn
- Cần dò tìm host trên Internet
- Muốn tăng độ chính xác so với ICMP Ping

Lệnh:

```
nmap -PS 192.168.1.0/24
```

Lệnh trên yêu cầu Nmap gửi gói TCP SYN để dò tìm host trong dải mạng chỉ định.

4.3. TCP ACK Ping

Cách hoạt động

TCP ACK Ping gửi các gói **TCP ACK** đến host mục tiêu. Theo chuẩn TCP, nếu host tồn tại, nó sẽ phản hồi bằng gói **RST**, bất kể cổng mở hay đóng. Dựa vào phản hồi RST này, Nmap xác định host đang hoạt động.

Phân biệt với SYN Ping

- **TCP SYN Ping**: Dựa trên phản hồi SYN/ACK hoặc RST
- **TCP ACK Ping**: Dựa chủ yếu vào phản hồi RST

TCP ACK Ping thường được dùng để **vượt qua firewall** cho phép gói ACK đi qua nhưng chặn gói SYN.

Lệnh:

```
nmap -PA 192.168.1.0/24
```

4.4. UDP Ping

Đặc điểm giao thức UDP

UDP là giao thức **không kết nối**, không có cơ chế bắt tay như TCP. Khi gửi gói UDP đến host mục tiêu, nếu cổng không mở, host thường phản hồi bằng gói **ICMP Port Unreachable**, từ đó cho thấy host đang tồn tại.

Trường hợp sử dụng

UDP Ping được sử dụng khi:

- ICMP và TCP bị chặn

- Cần dò tìm host trong môi trường có firewall nghiêm ngặt
- Muốn đa dạng phương pháp dò tìm để tăng độ chính xác

Lệnh:

nmap -PU 192.168.1.0/24

4.5. ARP Scan (trong mạng LAN)

ARP là gì?

ARP (Address Resolution Protocol) là giao thức dùng để ánh xạ **địa chỉ IP sang địa chỉ MAC** trong mạng nội bộ (LAN). ARP hoạt động ở tầng liên kết dữ liệu và không thể bị chặn bởi firewall tầng mạng.

Vì sao ARP scan chính xác trong LAN

Trong mạng LAN:

- Mọi thiết bị đều phải phản hồi ARP để giao tiếp
- Firewall không chặn ARP
- Tốc độ phản hồi nhanh và chính xác

Do đó, ARP Scan là phương pháp dò tìm host **chính xác nhất trong mạng nội bộ**.

Lệnh:

nmap -sn -PR 192.168.1.0/24

4.6. Bỏ qua dò tìm host

Khi nào cần bỏ qua bước host discovery

Trong một số trường hợp:

- Firewall chặn toàn bộ gói dò tìm host
- Host tồn tại nhưng không phản hồi bất kỳ phương thức ping nào
- Cần quét trực tiếp một host đã biết chắc tồn tại

Khi đó, người dùng có thể yêu cầu Nmap **coi host luôn ở trạng thái "up"** và tiến hành quét trực tiếp.

Lệnh:

nmap -Pn 192.168.1.10

5. So sánh các phương pháp dò tìm host trong Nmap

Do môi trường mạng và chính sách bảo mật khác nhau, không có một phương pháp dò tìm host nào phù hợp cho mọi trường hợp. Mỗi kỹ thuật dò tìm host trong Nmap

đều có những đặc điểm riêng về nguyên lý hoạt động, độ chính xác, khả năng bị chặn và phạm vi áp dụng. Việc so sánh các phương pháp này giúp người sử dụng lựa chọn được kỹ thuật phù hợp nhất với từng tình huống cụ thể.

5.1. Bảng so sánh các phương pháp dò tìm host

Phương pháp	**Giao thức sử dụng**	**Môi trường phù hợp**	**Độ chính xác**	**Khả năng bị firewall chặn**
ICMP Ping	ICMP	Internet, LAN	Trung bình	Cao
TCP SYN Ping	TCP	Internet, LAN	Cao	Trung bình
TCP ACK Ping	TCP	Internet	Trung bình – Cao	Thấp hơn SYN
UDP Ping	UDP + ICMP	Internet	Thấp – Trung bình	Cao
ARP Scan	ARP	LAN	Rất cao	Rất thấp
Bỏ qua host discovery	Không dùng ping	Mọi môi trường	Phụ thuộc mục tiêu	Không bị chặn

5.2. So sánh theo môi trường mạng

5.2.1. Mạng nội bộ (LAN)

Trong môi trường mạng LAN, **ARP Scan** là phương pháp hiệu quả và chính xác nhất. Do ARP hoạt động ở tầng liên kết dữ liệu, firewall không thể chặn các gói ARP. Nhờ đó, Nmap có thể phát hiện gần như toàn bộ host đang tồn tại trong mạng nội bộ.

Các phương pháp khác như ICMP hoặc TCP Ping vẫn có thể sử dụng trong LAN, tuy nhiên độ chính xác thường không cao bằng ARP Scan.

5.2.2. Mạng Internet

Trong môi trường Internet, ARP Scan không còn hiệu quả do giới hạn phạm vi hoạt động của ARP. Lúc này, các phương pháp dựa trên TCP như **TCP SYN Ping** và **TCP ACK Ping** thường được ưu tiên sử dụng vì:

- Có khả năng vượt qua một số firewall
- Độ chính xác cao hơn ICMP Ping

ICMP Ping thường bị chặn trong môi trường Internet, trong khi UDP Ping có độ chính xác thấp và thời gian phản hồi chậm.

5.3. So sánh theo mức độ bảo mật của hệ thống

- **Hệ thống bảo mật thấp**: ICMP Ping và TCP SYN Ping thường đủ để phát hiện host.
- **Hệ thống có firewall cơ bản**: TCP ACK Ping cho kết quả tốt hơn ICMP và SYN Ping.
- **Hệ thống bảo mật cao**: Có thể không phản hồi bất kỳ phương pháp ping nào, buộc phải sử dụng tùy chọn **-Pn** để bỏ qua bước dò tìm host.

Qua đó có thể thấy, mức độ bảo mật của hệ thống càng cao thì khả năng phát hiện host càng khó khăn và cần kết hợp nhiều kỹ thuật khác nhau.

5.4. So sánh về hiệu năng và độ ồn (stealth)

- **ICMP Ping**: Nhanh, ít gói tin nhưng dễ bị phát hiện.
- **TCP SYN Ping**: Cân bằng giữa độ chính xác và độ ồn.
- **TCP ACK Ping**: Ít bị chú ý hơn SYN Ping.
- **UDP Ping**: Chậm, tạo nhiều lưu lượng mạng.
- **ARP Scan**: Rất nhanh, chính xác, nhưng chỉ dùng trong LAN.
- **-Pn**: Không tạo lưu lượng dò tìm host nhưng làm tăng thời gian quét cổng.

5.5. Đánh giá tổng quan

Không có phương pháp dò tìm host nào là "tốt nhất" trong mọi tình huống. Thay vào đó:

- **ARP Scan** là lựa chọn tối ưu trong mạng LAN
- **TCP SYN/ACK Ping** phù hợp cho Internet
- **-Pn** dùng trong các môi trường có firewall chặt chẽ

Việc kết hợp linh hoạt nhiều phương pháp dò tìm host giúp nâng cao khả năng phát hiện và đánh giá chính xác tình trạng của hệ thống mạng.

6. Thực hành minh họa

6.1. Mục tiêu thực hành

Phần thực hành nhằm minh họa cách sử dụng Nmap để dò tìm host trong một mạng cụ thể, qua đó giúp người học:

- Hiểu rõ cách hoạt động thực tế của các phương pháp dò tìm host
- Nhận biết sự khác nhau giữa các kỹ thuật ICMP, TCP, UDP và ARP
- Phân tích kết quả trả về từ Nmap

- Rút ra nhận xét về hiệu quả của từng phương pháp trong môi trường mạng cụ thể

6.2. Môi trường thử nghiệm

Môi trường thực hành được xây dựng với các thành phần sau:

- **Máy quét (Attacker/Scanner):**
  - Hệ điều hành: Linux (Kali Linux hoặc Ubuntu)
  - Công cụ: Nmap phiên bản mới nhất
- **Mạng mục tiêu:**
  - Mạng nội bộ (LAN)
  - Dải địa chỉ IP: 192.168.1.0/24
- **Các host trong mạng:**
  - Máy tính cá nhân
  - Router
  - Một số thiết bị đang bật và một số thiết bị đã tắt

Môi trường này mô phỏng một mạng nội bộ thực tế trong gia đình hoặc doanh nghiệp nhỏ.

6.3. Thực hành dò tìm host bằng ICMP Ping Scan

Lệnh sử dụng:

```
nmap -sn 192.168.1.0/24
```

Kết quả thu được:

- Nmap liệt kê các địa chỉ IP có phản hồi ICMP
- Các host trả lời ICMP được đánh dấu là **Host is up**
- Các IP không phản hồi không được liệt kê

Phân tích:

- Phương pháp này cho kết quả nhanh
- Một số host không xuất hiện do chặn ICMP
- Độ chính xác phụ thuộc vào cấu hình firewall của host

6.4. Thực hành dò tìm host bằng TCP SYN Ping

Lệnh sử dụng:

```
nmap -PS 192.168.1.0/24
```

Kết quả thu được:

- Phát hiện thêm một số host không phản hồi ICMP
- Host trả lời SYN/ACK hoặc RST được xác định là đang hoạt động

Phân tích:

- Độ chính xác cao hơn ICMP Ping
- Phù hợp khi ICMP bị chặn
- Thời gian quét lâu hơn ICMP Ping một chút

6.5. Thực hành dò tìm host bằng TCP ACK Ping

Lệnh sử dụng:

```
nmap -PA 192.168.1.0/24
```

Kết quả thu được:

- Một số host phản hồi bằng gói RST
- Phát hiện được các host phía sau firewall cho phép ACK

Phân tích:

- Hiệu quả trong một số môi trường có firewall
- Dễ bị nhầm lẫn với host không tồn tại nếu firewall chặn hoàn toàn

6.6. Thực hành dò tìm host bằng UDP Ping

Lệnh sử dụng:

```
nmap -PU 192.168.1.0/24
```

Kết quả thu được:

- Ít host phản hồi
- Một số phản hồi ICMP Port Unreachable

Phân tích:

- Thời gian quét lâu
- Độ chính xác thấp
- Chỉ nên dùng khi các phương pháp khác không hiệu quả

6.7. Thực hành dò tìm host bằng ARP Scan (LAN)

Lệnh sử dụng:

```
nmap -sn -PR 192.168.1.0/24
```

Kết quả thu được:

- Phát hiện đầy đủ các host đang hoạt động trong mạng LAN

- Hiển thị cả địa chỉ IP và địa chỉ MAC

Phân tích:

- Độ chính xác rất cao
- Thời gian quét nhanh
- Không bị firewall chặn
- Là phương pháp tối ưu trong mạng nội bộ

6.8. Thực hành bỏ qua dò tìm host

Lệnh sử dụng:

nmap -Pn 192.168.1.10

Kết quả thu được:

- Nmap tiến hành quét trực tiếp host mục tiêu
- Không kiểm tra trạng thái "host up" trước

Phân tích:

- Phù hợp khi chắc chắn host tồn tại
- Thời gian quét lâu hơn
- Hữu ích trong môi trường bảo mật cao

6.9. Nhận xét chung

Qua quá trình thực hành, có thể rút ra một số nhận xét:

- ARP Scan cho kết quả chính xác nhất trong mạng LAN
- TCP SYN và TCP ACK Ping hiệu quả hơn ICMP trong môi trường có firewall
- UDP Ping ít được sử dụng do hiệu quả thấp
- Việc lựa chọn phương pháp dò tìm host cần phù hợp với môi trường mạng và mục tiêu kiểm tra

7. Ứng dụng thực tế của dò tìm host bằng Nmap

Dò tìm host không chỉ mang ý nghĩa học thuật mà còn được ứng dụng rộng rãi trong thực tế, đặc biệt trong các lĩnh vực **quản trị mạng, an ninh mạng và kiểm thử hệ thống**. Việc xác định chính xác các host đang hoạt động giúp người quản trị và chuyên gia bảo mật có cái nhìn tổng quan về hệ thống, từ đó đưa ra các biện pháp quản lý và bảo vệ phù hợp.

7.1. Quản lý và giám sát hệ thống mạng

Trong môi trường doanh nghiệp, hệ thống mạng thường bao gồm nhiều thiết bị như máy trạm, máy chủ, router, switch, máy in và các thiết bị IoT. Việc dò tìm host giúp:

- Kiểm kê các thiết bị đang hoạt động trong mạng
- Phát hiện các thiết bị mới được kết nối mà chưa được cấp phép
- Theo dõi trạng thái hoạt động của host theo thời gian

Thông qua Nmap, quản trị viên có thể nhanh chóng xác định những host nào đang "up", từ đó dễ dàng phát hiện sự thay đổi bất thường trong hệ thống mạng.

7.2. Đánh giá rủi ro từ port mở

Các **port mở** là yếu tố tiềm ẩn rủi ro bảo mật lớn nhất trong hệ thống mạng. Mỗi cổng mở đồng nghĩa với việc:

- Có một dịch vụ đang chạy
- Có khả năng tiếp nhận kết nối từ bên ngoài

Rủi ro từ port mở bao gồm:

- Dịch vụ cấu hình sai (misconfiguration)
- Dịch vụ sử dụng phiên bản có lỗ hổng
- Dịch vụ không cần thiết nhưng vẫn mở cổng
- Nguy cơ bị brute-force, scan hoặc khai thác

Việc đánh giá rủi ro thường dựa trên:

- Số lượng cổng mở
- Loại dịch vụ và phiên bản
- Mức độ phơi bày ra Internet hay chỉ nội bộ

Từ kết quả quét port bằng Nmap, người quản trị có thể:

- Đóng các cổng không cần thiết
- Cập nhật hoặc vá lỗi dịch vụ
- Tăng cường firewall và cơ chế bảo vệ

7.3. Hỗ trợ kiểm thử xâm nhập (Penetration Testing)

Trong kiểm thử xâm nhập, dò tìm host là bước đầu tiên nhằm xác định **bề mặt tấn công (attack surface)** của hệ thống. Thông tin về các host đang hoạt động giúp:

- Xác định mục tiêu tiềm năng
- Tránh quét nhầm các IP không tồn tại

- Tối ưu thời gian và tài nguyên kiểm thử

Nmap thường được sử dụng trong giai đoạn **reconnaissance**, làm nền tảng cho các bước tiếp theo như quét cổng, phát hiện dịch vụ và khai thác lỗ hổng.

7.4. Hỗ trợ khắc phục sự cố mạng

Dò tìm host cũng được ứng dụng trong quá trình **xử lý sự cố mạng**, ví dụ:

- Kiểm tra host có đang hoạt động hay không
- Xác định thiết bị bị mất kết nối
- Phân biệt lỗi mạng và lỗi thiết bị

Trong những tình huống này, Nmap giúp quản trị viên nhanh chóng khoanh vùng nguyên nhân sự cố và đưa ra hướng xử lý phù hợp.

7.5. Đánh giá mức độ "hiển thị" của hệ thống trên mạng

Việc dò tìm host giúp đánh giá mức độ **hiển thị (visibility)** của hệ thống đối với bên ngoài. Nếu một host có thể dễ dàng bị phát hiện thông qua các phương pháp dò tìm, điều đó cho thấy:

- Host có thể đang phản hồi quá nhiều gói tin
- Chính sách firewall chưa chặt chẽ
- Tồn tại nguy cơ bị tấn công dò quét

Từ kết quả này, người quản trị có thể điều chỉnh cấu hình firewall, IDS/IPS nhằm giảm khả năng bị phát hiện từ bên ngoài.

7.6. Ứng dụng trong học tập và nghiên cứu

Đối với sinh viên ngành Công nghệ thông tin, đặc biệt là lĩnh vực mạng và an ninh mạng, Nmap là công cụ học tập hiệu quả giúp:

- Hiểu rõ cơ chế hoạt động của các giao thức mạng
- Thực hành các kỹ thuật dò tìm host trong môi trường an toàn
- Nâng cao tư duy phân tích và đánh giá hệ thống

Việc thực hành dò tìm host giúp sinh viên tiếp cận các khái niệm an ninh mạng một cách trực quan và thực tế hơn.

V. KẾT LUẬN

Trong bối cảnh hệ thống mạng ngày càng phát triển và các mối đe dọa an ninh mạng ngày càng phức tạp, việc **dò tìm host** đóng vai trò quan trọng trong quá trình quản lý, giám sát và bảo vệ hệ thống mạng. Dò tìm host không chỉ giúp xác định các thiết bị đang hoạt động trong mạng mà còn là bước nền tảng cho các hoạt động phân tích chuyên sâu như quét cổng, phát hiện dịch vụ và đánh giá lỗ hổng bảo mật.

Thông qua đề tài **"Dò tìm host bằng Nmap"**, bài báo cáo đã trình bày tổng quan về công cụ Nmap, khái niệm dò tìm host, các phương pháp dò tìm host phổ biến cũng như so sánh ưu, nhược điểm của từng phương pháp. Đồng thời, phần thực hành minh họa đã giúp làm rõ cách áp dụng Nmap trong môi trường mạng thực tế và phân tích kết quả thu được từ từng kỹ thuật dò tìm host.

Kết quả cho thấy không tồn tại một phương pháp dò tìm host nào là tối ưu trong mọi trường hợp. Việc lựa chọn kỹ thuật phù hợp phụ thuộc vào môi trường mạng, mức độ bảo mật của hệ thống và mục tiêu kiểm tra. Trong mạng nội bộ, ARP Scan cho độ chính xác cao nhất, trong khi các phương pháp dựa trên TCP phù hợp hơn trong môi trường Internet hoặc khi ICMP bị chặn. Đối với các hệ thống có cơ chế bảo mật nghiêm ngặt, việc bỏ qua bước dò tìm host là cần thiết để tiếp tục quá trình phân tích.

Qua đề tài này, người học có thể hiểu rõ hơn về quy trình dò tìm host, vai trò của từng phương pháp cũng như cách sử dụng Nmap một cách hiệu quả và đúng mục đích. Đây là nền tảng quan trọng giúp nâng cao kiến thức và kỹ năng trong lĩnh vực quản trị mạng và an ninh mạng, đồng thời góp phần hình thành tư duy đánh giá và bảo vệ hệ thống một cách chủ động và khoa học.

VI. TÀI LIỆU THAM KHẢO

[1] Gordon Lyon (Fyodor), Nmap Network Scanning, Insecure.Org

[2] Nmap Official Documentation – https://nmap.org/docs.html

[3] Nmap là gì? Cách sử dụng nmap Cơ bản. - Hướng dẫn TENTEN