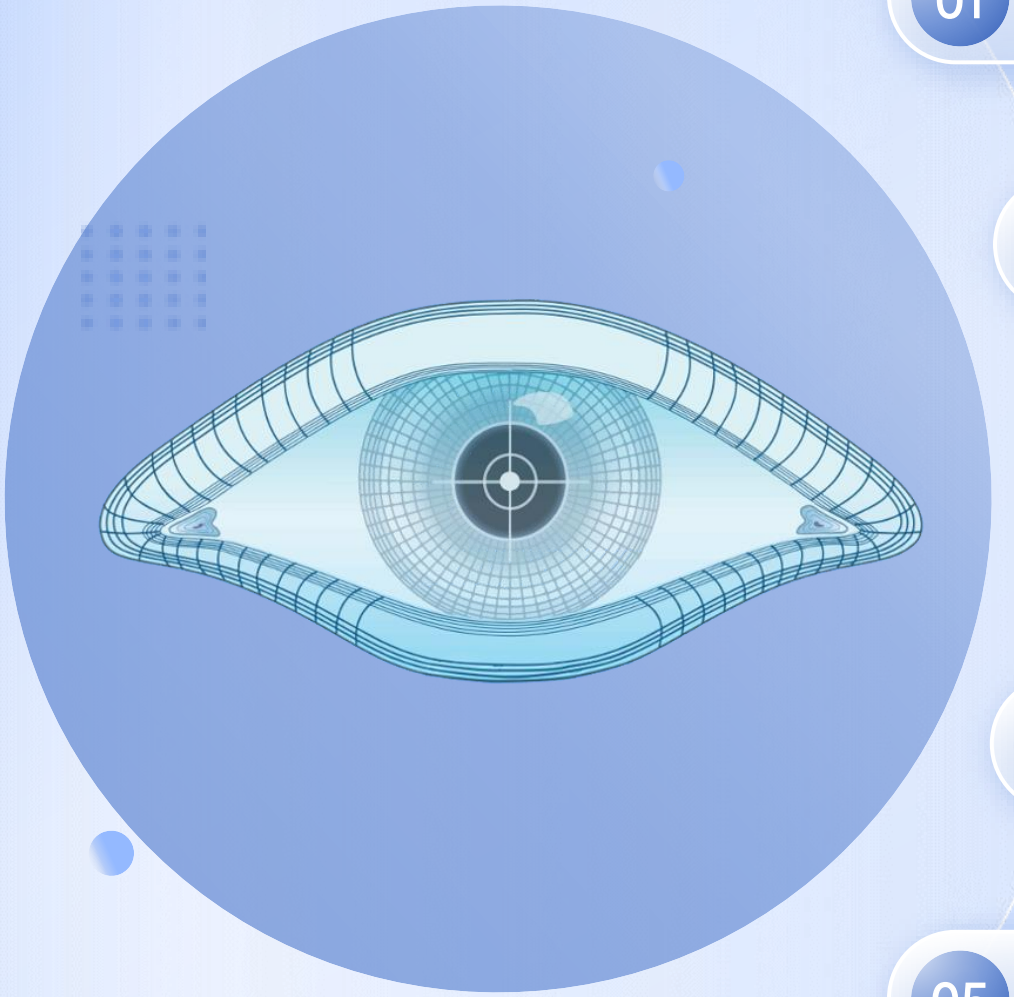
Khám Phá Nmap: Quét Mạng & Bảo Mật

NHÓM 1



01 Giới thiệu Nmap

02 Các lệnh và cổng thường gặp trong NMAP

03 Các công cụ quét lỗ hổng và lỗ hổng

04 Thực hành

05 Kết luận ưu điểm - nhược điểm

CONTENTS

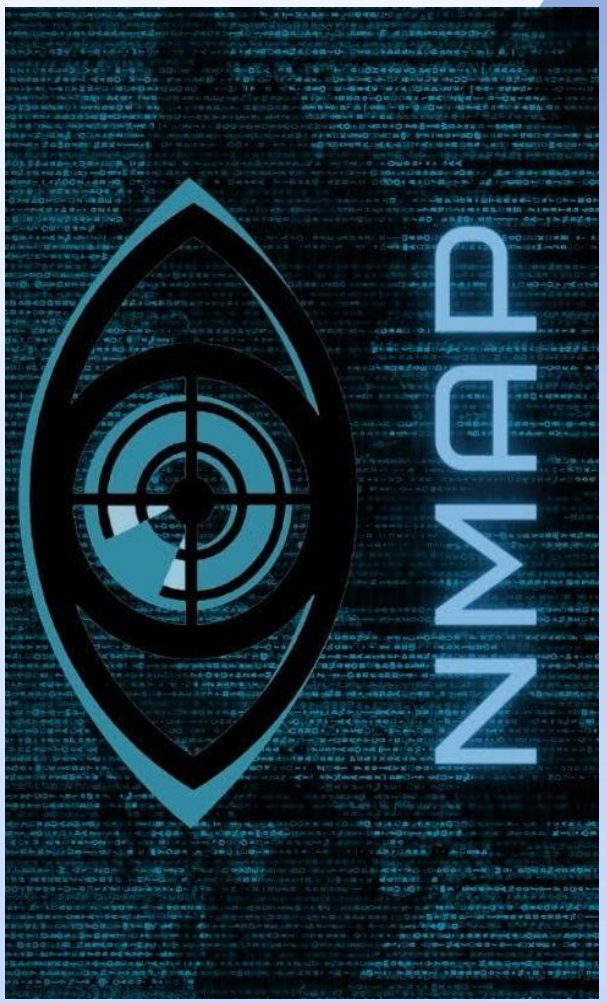
CONTENTS

01

PART 01

Giới thiệu Nmap

Nmap là gì?



Định nghĩa Nmap

Nmap, viết tắt của Network Mapper, là một công cụ mã nguồn mở miễn phí được thiết kế để khám phá mạng và kiểm tra bảo mật. Nó được sử dụng rộng rãi bởi quản trị viên mạng và an ninh để kiểm tra tình trạng bảo mật của hệ thống mạng.

Ứng dụng của Nmap

Nmap có thể xác định các thiết bị đang hoạt động trong mạng, dịch vụ đang chạy, hệ điều hành của các máy chủ và các thiết bị bảo mật như tường lửa. Nó là công cụ đắc lực trong quản lý và bảo mật mạng.

Hỗ trợ đa nền tảng

Nmap hỗ trợ chạy trên nhiều hệ điều hành phổ biến như Linux, Windows và macOS. Điều này giúp người dùng có thể sử dụng Nmap trên bất kỳ môi trường nào mà không gặp khó khăn.

Cách hoạt động của Nmap

Gửi và phân tích gói tin

Nmap hoạt động bằng cách gửi các gói tin IP đặc biệt đến các thiết bị mạng và phân tích phản hồi từ các thiết bị đó. Qua đó, Nmap có thể xác định trạng thái của các cổng và dịch vụ đang chạy trên các thiết bị.

Xác định thông tin chi tiết

Ngoài việc xác định trạng thái cổng, Nmap còn có thể thu thập thông tin về hệ điều hành, phiên bản dịch vụ và các thiết bị mạng như tường lửa, giúp người dùng có cái nhìn toàn diện về mạng.

Tính năng nổi bật

Phát hiện lỗ hổng

Nmap có khả năng phát hiện các lỗ hổng bảo mật trên mạng bằng cách kiểm tra các dịch vụ và phiên bản phần mềm đang chạy. Điều này giúp quản trị viên kịp thời vá các lỗ hổng.

Quét mạng và dịch vụ

Nmap có thể quét toàn bộ mạng để tìm các thiết bị và dịch vụ đang hoạt động. Nó hỗ trợ nhiều loại quét như TCP, UDP, ICMP, giúp người dùng lựa chọn phương pháp phù hợp.

Xác định hệ điều hành

Nmap có thể xác định loại hệ điều hành đang chạy trên các thiết bị thông qua phân tích các gói tin phản hồi. Điều này giúp người dùng hiểu rõ hơn về môi trường mạng.

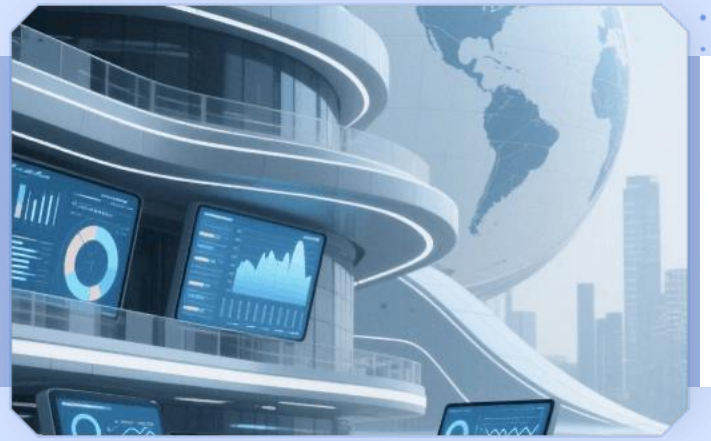
Tích hợp với các công cụ khác

Nmap hỗ trợ xuất kết quả ra nhiều định dạng như XML, CSV, giúp người dùng dễ dàng tích hợp với các công cụ quản lý và phân tích mạng khác như Metasploit, Nessus.

02

PART 02

Cài đặt và cách dùng



Cài đặt Nmap trên Windows

Tải và cài đặt

Người dùng Windows có thể tải Nmap từ trang web chính thức nmap.org/download. Sau khi tải về, chạy file cài đặt để hoàn tất quá trình cài đặt.

Sử dụng Zenmap

Sau khi cài đặt, người dùng có thể sử dụng giao diện dòng lệnh hoặc Zenmap, một giao diện đồ họa giúp dễ dàng thực hiện các lệnh quét mạng và xem kết quả.

Cài đặt Nmap trên macOS

Tải file .dmg

Trên macOS, người dùng có thể tải file .dmg từ trang web chính thức nmap.org/dist. Sau đó, mở file .dmg và kéo ứng dụng Nmap vào thư mục Applications để cài đặt.

Sử dụng terminal

Sau khi cài đặt, người dùng có thể sử dụng terminal để chạy lệnh Nmap hoặc mở Zenmap nếu muốn sử dụng giao diện đồ họa. Việc cài đặt và sử dụng đều khá đơn giản.

04

PART 03

Trạng thái cổng và dịch vụ

Open

Trạng thái Open: Cổng đang mở và có dịch vụ đang lắng nghe. Đây là trạng thái an toàn nếu dịch vụ cần thiết, nhưng có thể là lỗ hổng nếu không cần thiết.

Closed

Trạng thái Closed: Cổng đóng, không có dịch vụ đang lắng nghe. Tuy nhiên, cổng đóng vẫn cho biết thiết bị đang hoạt động, giúp người dùng biết thiết bị đang online.

Filtered

Trạng thái Filtered: Cổng bị tường lửa chặn, không có phản hồi từ thiết bị. Điều này giúp người dùng biết có sự can thiệp của tường lửa.

Cổng TCP thường gặp

Các cổng quan trọng

Các cổng TCP phổ biến như 21 (FTP), 22 (SSH), 23 (Telnet), 25 (SMTP), 53 (DNS), 80 (HTTP), 443 (HTTPS), 3389 (RDP), 3306 (MySQL). Mỗi cổng có một dịch vụ quan trọng và tiềm ẩn rủi ro bảo mật.

Ví dụ về rủi ro

Ví dụ, cổng 21 (FTP) có thể bị nghe lén nếu không sử dụng mã hóa. Cổng 22 (SSH) có thể bị brute-force nếu mật khẩu yếu. Quản trị viên cần bảo vệ các cổng này để tránh rủi ro.

Cổng UDP thường gặp

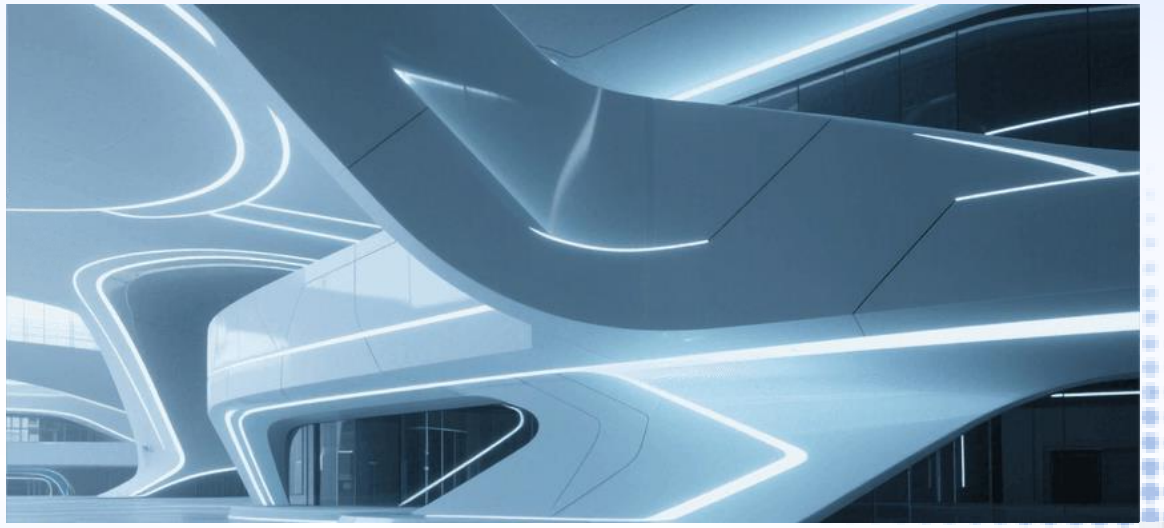
01 Các cổng phổ biến

Các cổng UDP phổ biến như 53 (DNS), 67/68 (DHCP), 69 (TFTP), 123 (NTP), 161/162 (SNMP), 1194 (OpenVPN), 1900 (SSDP). UDP không có cơ chế bắt tay nên dễ bị lợi dụng.

02 Rủi ro của UDP

UDP không có phản hồi rõ ràng nên dễ bị lợi dụng trong các cuộc tấn công như amplification DDoS. Ví dụ, cổng 53 (DNS) có thể bị lợi dụng để tấn công mạng nếu không được bảo vệ.

Xác định hệ điều hành



01 Lệnh -O

Lệnh nmap -O [IP] giúp xác định hệ điều hành đang chạy trên máy chủ. Nmap phân tích các gói tin phản hồi để đoán hệ điều hành, giúp người dùng hiểu rõ hơn về môi trường mạng.

Ứng dụng của lệnh -O 02

Biết được hệ điều hành của các thiết bị giúp quản trị viên đánh giá rủi ro bảo mật và có biện pháp bảo vệ phù hợp. Ví dụ, một hệ điều hành cũ có thể có nhiều lỗ hổng chưa vá.

03

PART 04

Các lệnh cơ bản

Lệnh cơ bản của NMAP

- Hiển thị thông số port TCP của thiết bị

```
# nmap -p T{ports}   {IP target or hostname}
```

hoặc

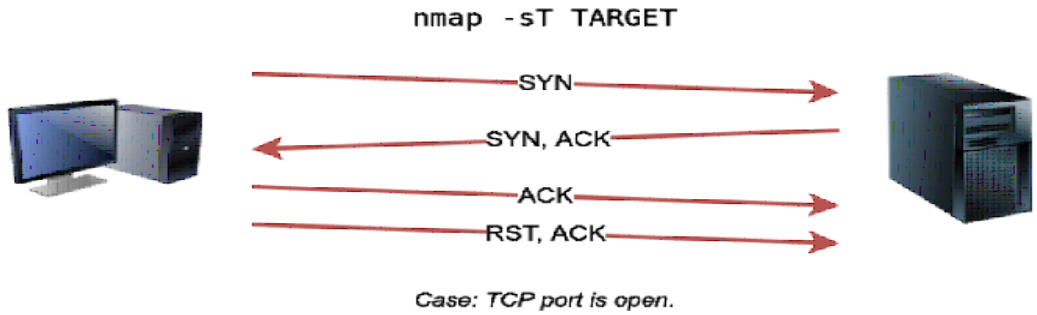
```
# nmap -sT {hostname} lệnh này tìm các port TCP
```

- Hiển thị thông số của Router, Interface và gói tin của mạng để việc dễ fix bug.

```
# nmap --iflist
```

- Ví dụ để muốn biết thông tin thiết bị trực tuyến đang sử dụng là gì, dùng options -sO

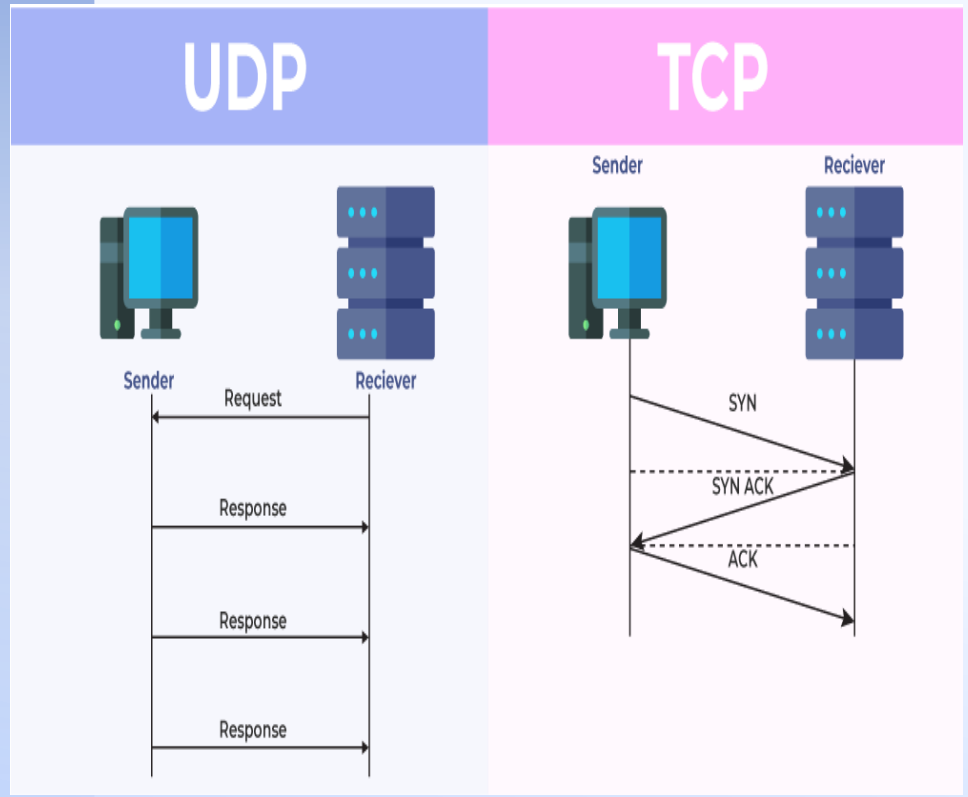
```
# nmap -sO {hostname}
```



Case: TCP port is open.

Kiểm tra xem host còn alive không : -sn
Kiểm tra hệ điều hành của server -O
Quét một port cụ thể -p
Quét kết nối TCP, Nmap sẽ thực hiện việc quét bắt tay 3 bước : -sT
Quét kết nối UDP -sU
Quét xác định phiên bản của dịch vụ đang chạy trên host : -PN -p [số_cổng] -sV

Quét cổng TCP và UDP



01

Quét cổng TCP

Lệnh nmap -sT [IP] thực hiện quét cổng TCP theo kiểu bắt tay 3 bước. Qua đó, Nmap có thể xác định các dịch vụ đang lắng nghe trên các cổng TCP của máy chủ.

02

Quét cổng UDP

Lệnh nmap -sU [IP] dùng để quét cổng UDP. Quét UDP giúp phát hiện các dịch vụ sử dụng giao thức UDP, tuy nhiên kết quả có thể không chính xác như TCP.

03

So sánh TCP và UDP

Quét TCP thường chính xác hơn và nhanh hơn so với UDP. UDP không có cơ chế bắt tay nên kết quả có thể bị bỏ sót hoặc không chính xác, đặc biệt với các dịch vụ không phản hồi.

Quét phiên bản dịch vụ

Lệnh -sV

Lệnh nmap -PN -p [cổng] -sV [IP] giúp xác định phiên bản của dịch vụ đang chạy trên cổng cụ thể. Việc này giúp phát hiện các phiên bản phần mềm lỗi thời có thể chứa lỗ hổng bảo mật.

05

PART 05

Lỗ hổng và NSE

Các lỗ hổng thường gặp

Lỗ hổng RCE

Lỗ hổng thực thi lệnh từ xa (RCE) cho phép kẻ tấn công chạy mã tùy ý trên máy chủ từ xa. Đây là lỗ hổng nghiêm trọng có thể dẫn tới chiếm quyền điều khiển và đánh cắp dữ liệu.

SQL Injection

Lỗ hổng SQL Injection xảy ra khi tham số đầu vào không được kiểm soát, cho phép kẻ tấn công chèn câu lệnh SQL độc hại. Điều này có thể dẫn tới rò rỉ dữ liệu.

Nmap Scripting Engine

Giới thiệu NSE

NSE là Nmap Scripting Engine, cho phép người dùng viết và chạy script tự động để kiểm tra bảo mật. NSE giúp mở rộng khả năng quét của Nmap.

01

Các loại script

NSE có 4 loại script: Host script, Prerule script, Service script, Postrule script. Mỗi loại script có chức năng riêng để hỗ trợ quá trình quét.

02

Ứng dụng của NSE

NSE giúp tự động hóa các tác vụ kiểm tra bảo mật như dò mật khẩu SSH, kiểm tra lỗ hổng web, thu thập thông tin SNMP, SMB, v.v. giúp người dùng tiết kiệm thời gian và công sức.

03

Các loại script NSE

Category vuln

Category vuln gồm các script dò các lỗ hổng đã biết như Heartbleed, MS17-010. Các script này giúp người dùng phát hiện các lỗ hổng bảo mật một cách nhanh chóng và chính xác.

Category auth

Category auth gồm các script kiểm tra các vấn đề liên quan đến xác thực. Ví dụ, script có thể kiểm tra mật khẩu yếu hoặc các lỗ hổng trong cơ chế xác thực của dịch vụ.

Category default

script mặc định, hay hữu dụng cho reconnaissance.

Category safe

các script an toàn (không gây ảnh hưởng lớn) — phù hợp để chạy trong môi trường sản xuất nếu có phép.

06

PART 06

Ưu điểm – nhược điểm

Ưu điểm của Nmap

Quét mạnh mẽ

Nmap hỗ trợ nhiều kiểu quét (TCP Connect, SYN scan, UDP scan, ping scan, OS detection, version detection, v.v.) giúp phát hiện chính xác các cổng và dịch vụ đang hoạt động trên mục tiêu.

Hỗ trợ đa nền tảng

Là công cụ miễn phí, mã nguồn mở, có thể chạy trên Windows, Linux và macOS — dễ cài đặt, dễ tùy chỉnh và được cộng đồng bảo trì thường xuyên.

Phát hiện chi tiết

Nmap có thể xác định loại hệ điều hành (OS fingerprinting) và phiên bản phần mềm (service version detection), giúp đánh giá lỗ hổng chính xác hơn.

Tích hợp script

Cho phép tự động hóa các tác vụ kiểm tra bảo mật (như dò mật khẩu SSH, kiểm tra lỗ hổng web, phát hiện SNMP, SMB, v.v.).

Nhược điểm của Nmap

Dễ bị phát hiện

Hoạt động quét của Nmap có thể bị firewall, IDS/IPS hoặc hệ thống bảo mật phát hiện và cảnh báo. Điều này có thể gây phiền hà cho quản trị viên mạng.

Quét UDP chậm

Quét UDP thường chậm và không chính xác như TCP. UDP không có cơ chế phản hồi rõ ràng nên kết quả có thể không đầy đủ, đặc biệt với các dịch vụ không phản hồi.

Yêu cầu kiến thức kỹ thuật

Người dùng cần hiểu rõ về các lệnh và giao thức mạng để sử dụng Nmap hiệu quả. Sai sót trong lệnh có thể dẫn tới kết quả không chính xác hoặc gây ảnh hưởng tới hệ thống.

Ảnh hưởng đến hệ thống mục tiêu

Một số kiểu quét (như -sS, -sU, -A) có thể làm tăng tải hoặc gây log cảnh báo, cần sử dụng thận trọng trong môi trường thật.

07

PART 07

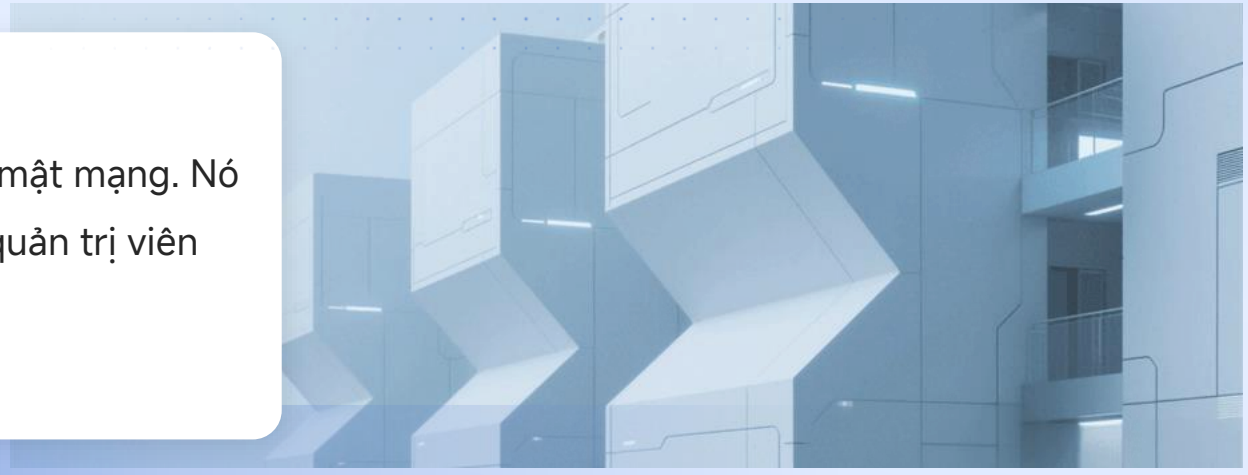
Thực hành và kết luận

Thực hành trong VMware

Kết luận về Nmap

Công cụ mạnh mẽ

Nmap là công cụ mạnh mẽ và cần thiết cho việc kiểm tra bảo mật mạng. Nó giúp phát hiện sớm các lỗ hổng, dịch vụ nguy hiểm và hỗ trợ quản trị viên bảo vệ hệ thống.



Sử dụng đúng cách

Để sử dụng Nmap hiệu quả, người dùng cần hiểu rõ về các lệnh và giao thức mạng. Kết hợp với các công cụ khác để đạt hiệu quả tối đa trong việc bảo vệ mạng.

Quan trọng với chuyên gia

Thành thạo Nmap là kỹ năng cơ bản và quan trọng đối với các chuyên gia an ninh mạng. Nmap giúp họ đánh giá bảo mật và đề xuất biện pháp bảo vệ phù hợp.

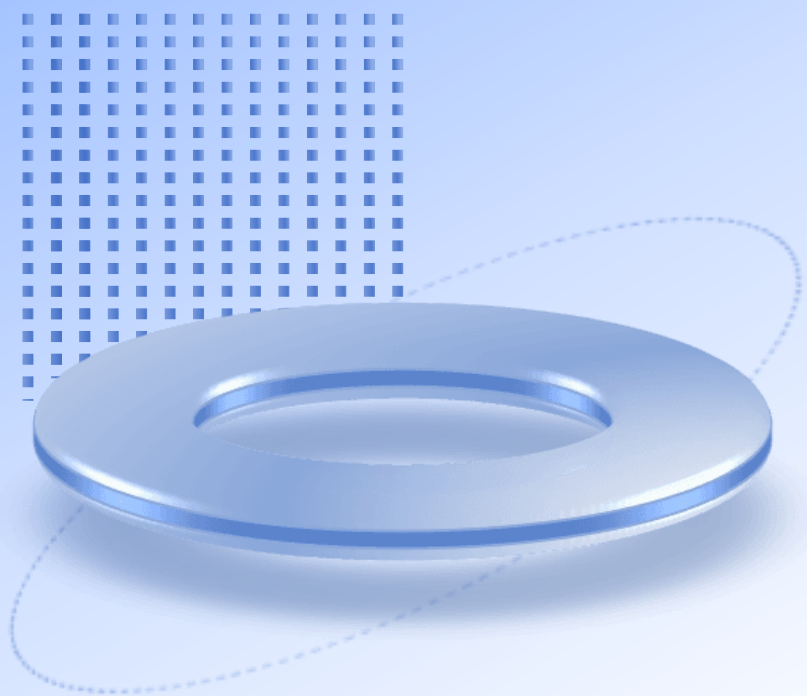
Ứng dụng thực tế

Kiểm toán bảo mật

Nmap được sử dụng trong kiểm toán bảo mật để phát hiện các lỗ hổng và dịch vụ nguy hiểm trong mạng. Kết quả giúp quản trị viên kịp thời vá lỗ hổng và bảo vệ mạng.

Quản lý mạng

Nmap giúp quản trị viên mạng kiểm tra tình trạng các thiết bị và dịch vụ trong mạng. Nó hỗ trợ quản lý mạng hiệu quả và kịp thời phát hiện các vấn đề bảo mật.



THANKS