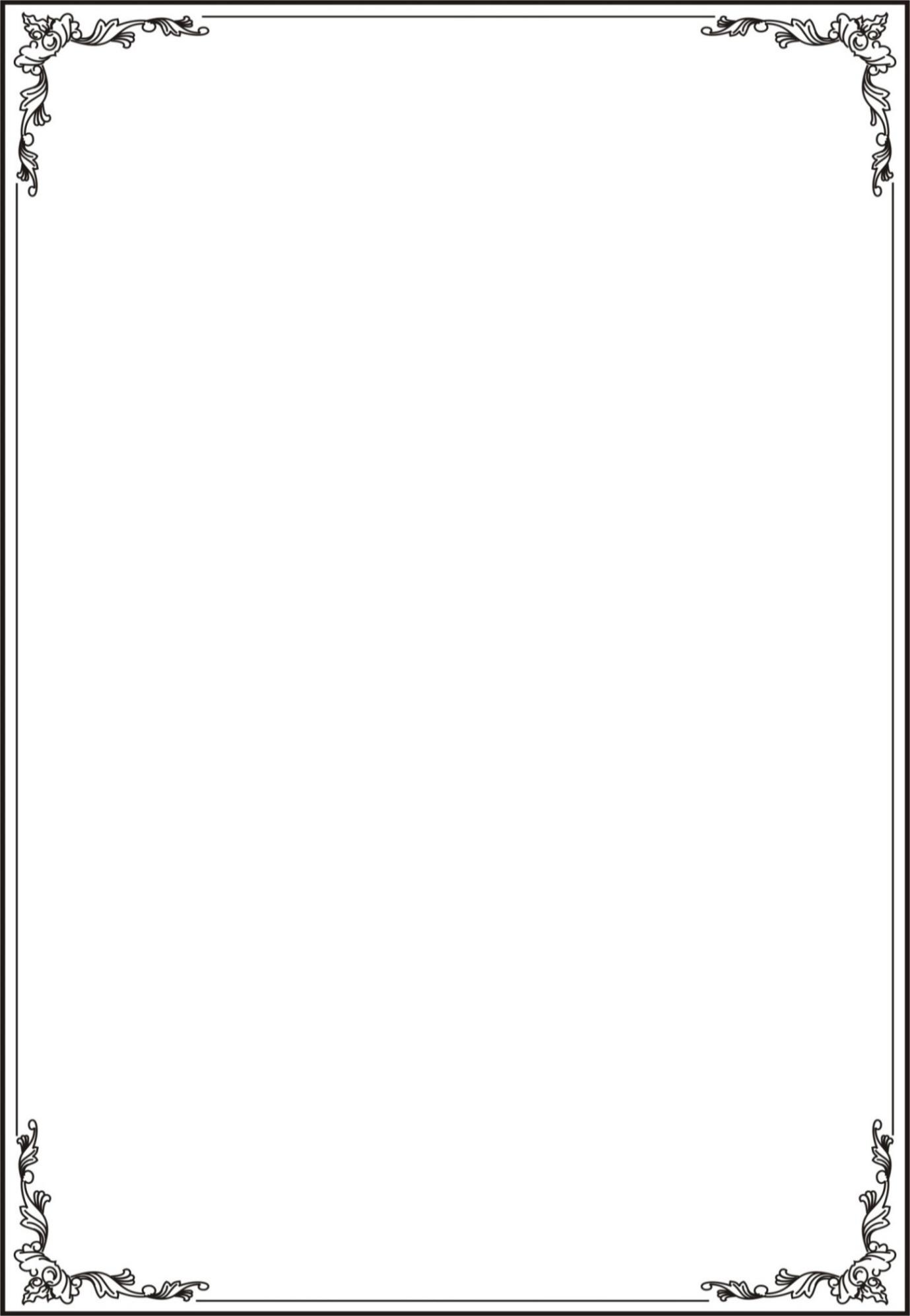
**ĐẠI HỌC ĐÀ NẴNG**

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG VIỆT – HÀN**



**BẢO MẬT VÀ AN TOÀN HỆ THỐNG THÔNG TIN**

**ĐỀ TÀI: TÌM HIỂU AN TOÀN MẠNG VÀ ĐÁNH GIÁ CÁC CÔNG CỤ AN NINH MẠNG**

**Sinh viên thực hiện:**

Nguyễn Ngọc Quang 18IT5

Nguyễn Trọng Tâm 18IT5

Tôn Đức Nam 18IT5

Phạm Văn Nhất 18IT5

**Giáo viên hướng dẫn:** TS. Hoàng Hữu Đức

***Đà nẵng, tháng 4 năm 2021***

**ĐẠI HỌC ĐÀ NẴNG**

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG VIỆT – HÀN**



**BẢO MẬT VÀ AN TOÀN HỆ THỐNG THÔNG TIN**

**ĐỀ TÀI: TÌM HIỂU AN TOÀN MẠNG VÀ ĐÁNH GIÁ CÁC CÔNG CỤ AN NINH MẠNG**

**Sinh viên thực hiện:**

Nguyễn Ngọc Quang 18IT5

Nguyễn Trọng Tâm 18IT5

Tôn Đức Nam 18IT5

Phạm Văn Nhất 18IT5

**Giáo viên hướng dẫn:** TS. Hoàng Hữu Đức

***Đà nẵng, tháng 4 năm 2021***

**LỜI CẢM ƠN**

Chúng em xin gửi lời cảm ơn đến thầy Hoàn Hữu Đức đã trực tiếp hướng dẫn, góp ý, chia sẻ nhiều kinh nghiệm quý báu, tận tình giúp đỡ để chúng em hoàn thành tốt đề tài. Xin cảm ơn nhà trường đã tạo cơ hội cho chúng em được học môn Bảo mật và An toàn hệ thống thông tin, môn học đã trang bị cho chúng em những kiến thức vô cùng quý giá trong vấn đề bảo mật và an toàn trong thời đại số hiện nay.

Xin chân thành cảm ơn!

MỤC LỤC

[Chương 1 TỔNG QUAN VỀ AN TOÀN MẠNG 2](#_Toc69966776)

[1.1 Lược sử hình thành và phát triển 2](#_Toc69966777)

[1.2 Mục tiêu của an ninh mạng 4](#_Toc69966778)

[1.2.1 Tính bảo mật (Confidentiality) 4](#_Toc69966779)

[1.2.2 Tính toàn vẹn (Integrity) 6](#_Toc69966780)

[1.2.3 Tính sẵn có (Availability) 6](#_Toc69966781)

[1.3 Đánh giá về các loại sự đe dọa an toàn mạng 7](#_Toc69966782)

[1.4 Lỗ hổng bảo mật và các loại tấn công phổ biến 7](#_Toc69966783)

[1.5 Các giai đoạn tấn công 10](#_Toc69966784)

[1.5.1 Thăm dò (Reconnaissace) 10](#_Toc69966785)

[1.5.2 Quét hệ thống (Scanning) 10](#_Toc69966786)

[1.5.3 Chiếm quyền điều khiển (Gainning access) 11](#_Toc69966787)

[1.5.4 Duy trì điều khiển hệ thống (Maitaining access) 11](#_Toc69966788)

[1.5.5 Xoá dấu vết (Clearning tracks) 11](#_Toc69966789)

[1.6 Các biện pháp phát hiện hệ thống bị tấn công 11](#_Toc69966790)

[Chương 2 ĐÁNH GIÁ CÁC CÔNG CỤ AN NINH MẠNG 13](#_Toc69966791)

[2.1 Nmap 13](#_Toc69966792)

[2.1.1 Nmap là gì? 13](#_Toc69966793)

[2.1.2 Các kiểu quét Nmap 13](#_Toc69966794)

[2.1.3 Các câu lệnh Nmap 14](#_Toc69966795)

[2.1.4 Sử dụng Nmap 16](#_Toc69966796)

[2.1.5 Ưu và nhược điểm 22](#_Toc69966797)

[2.2 Nessus 22](#_Toc69966798)

[2.2.1 Giới thiệu 22](#_Toc69966799)

[2.2.2 Sử dụng Nessus 25](#_Toc69966800)

[2.2.3 Ưu và nhược điểm 28](#_Toc69966801)

[2.3 Wireshark 29](#_Toc69966802)

[2.3.1 Giới thiệu 29](#_Toc69966803)

[2.3.2 Sử dụng Wireshark 29](#_Toc69966804)

[2.3.3 Một số tình huống có thể xảy với Wireshark 33](#_Toc69966805)

[2.3.4 Ưu và nhược điểm 34](#_Toc69966806)

**DANH MỤC HÌNH**

Trang

[Hình 1.1-Các giai đoạn tấn công an toàn mạng 10](#_Toc69966919)

[Hình 2.1 Kỹ thuật quét 15](#_Toc69966920)

[Hình 2.2 Khám phá máy chủ 15](#_Toc69966921)

[Hình 2.3 Đặc điểm kỹ thuật cổng 15](#_Toc69966922)

[Hình 2.4 Phiên bản dịch vụ và phát hiện hệ điều hành 15](#_Toc69966923)

[Hình 2.5 Thời gian và Hiệu suất 16](#_Toc69966924)

[Hình 2.6 Tập lệnh NSE 16](#_Toc69966925)

[Hình 2.7 DS trốn tránh 16](#_Toc69966926)

[Hình 2.8 Xem giúp đỡ của câu lệnh NMAP 17](#_Toc69966927)

[Hình 2.9 Kiểm tra đường mạng để xác định host. 18](#_Toc69966928)

[Hình 2.10 Kiểm tra để xác định các port đang mở 18](#_Toc69966929)

[Hình 2.11 Kiểm tra xem đường mạng đã mở các port hay chưa. 19](#_Toc69966930)

[Hình 2.12 Quét tên miền bên ngoài 20](#_Toc69966931)

[Hình 2.13 Xem các thông số trên server 20](#_Toc69966932)

[Hình 2.14 Mô hình mạng trong Zenmap 21](#_Toc69966933)

[Hình 2.15 Xuất file xml sau khi quét 21](#_Toc69966934)

[Hình 2.16 So sánh phiên bản Pro và Home 24](#_Toc69966935)

[Hình 2.17 So sánh phiên bản ProfessionFeed và Evaluation 24](#_Toc69966936)

[Hình 2.18 Giao diên Nessus 25](#_Toc69966937)

[Hình 2.19 Nessus add 25](#_Toc69966938)

[Hình 2.20 Nessus quét cổng 26](#_Toc69966939)

[Hình 2.21 Tạo thêm Policy 26](#_Toc69966940)

[Hình 2.22 Quá trình quét 27](#_Toc69966941)

[Hình 2.23 Kết quả quét 27](#_Toc69966942)

[Hình 2.24 Tạo báo cáo 28](#_Toc69966943)

[Hình 2.25 Giám sát thông tin Wi-Fi 30](#_Toc69966944)

[Hình 2.26 Color Coding 31](#_Toc69966945)

[Hình 2.27 Duyệt File trong WireShark 31](#_Toc69966946)

[Hình 2.28 Filtering Packets 32](#_Toc69966947)

[Hình 2.29 Hiển thị thông tin package 32](#_Toc69966948)

[Hình 2.30 Kiểm tra thông tin package cụ thể 33](#_Toc69966949)

**MỞ ĐẦU**

Diễn đàn Kinh tế Thế giới coi các mối đe dọa đối với an toàn mạng là một trong năm rủi ro toàn cầu hàng đầu mà các quốc gia trên thế giới phải đối mặt hiện nay. Các lỗ hổng về tổn thất tài chính từ vi phạm an toàn mạng đến trộm cắp tài sản trí tuệ đang là một vấn đề ngày càng gia tăng. Các mối đe dọa mạng đang ngày càng nhắm vào các chức năng cốt lõi của nền kinh tế ở các quốc gia trên toàn thế giới, cũng như chính phủ của các quốc gia đó ở cấp địa phương, khu vực và quốc gia. Khả năng xảy ra các cuộc tấn công mạng nhằm phá vỡ các dịch vụ quan trọng của cả doanh nghiệp tư nhân và các cơ quan phi chính phủ đang tăng lên ở mức báo động.

An toàn mạng hiện được coi là một trong những mối quan tâm hàng đầu của quốc gia chúng ta, vì tiềm năng cho các nhóm hoặc cá nhân có động cơ làm gián đoạn các dịch vụ quan trọng, tấn công bất kỳ một trong 16 cơ sở hạ tầng quan trọng của chúng ta và gây ra một loạt thiệt hại từ gián đoạn kinh tế lớn đến hủy hoại vật chất lớn đang trở nên khó chống lại hơn. Đáng báo động hơn nữa là mối đe dọa có thể xảy ra từ các cuộc tấn công mạng đối với Bộ Quốc phòng và tài sản quân sự của quốc gia chúng ta, vì các cuộc tấn công mạng có thể làm gián đoạn hoặc vô hiệu hóa nghiêm trọng các hệ thống chỉ huy và kiểm soát quân sự cũng như các hệ thống thông tin liên lạc, tình báo và chỉ huy chung của chúng ta, có thể gây nguy hiểm cho an ninh quốc gia của chúng ta. Mối đe dọa của chiến tranh mạng đang cận kề, và việc phát triển và tạo ra công cụ an toàn mạng đang được nhiều quốc gia theo đuổi.V

Với mong muốn tìm hiểu sâu hơn về an toàn mạng chúng em đã tiến hành tìm hiểu về các thông tin liên quan an toàn mạng và triển khai một số công cụ an ninh mạng.

# TỔNG QUAN VỀ AN TOÀN MẠNG

An ninh mạng là thực tiễn của việc bảo vệ các hệ thống điện tử, mạng lưới, máy tính, thiết bị di động, chương trình và dữ liệu khỏi những cuộc tấn công kỹ thuật số độc hại có chủ đích. Tội phạm mạng có thể triển khai một loạt các cuộc tấn công chống lại các nạn nhân hoặc doanh nghiệp đơn lẻ; có thể kể đến như truy cập, làm thay đổi hoặc xóa bỏ dữ liệu nhạy cảm; tống tiền; can thiệp vào các quy trình kinh doanh.

## Lược sử hình thành và phát triển

**1971 – Virus máy tính đầu tiên trên thế giới**: Nhà toán học John von Neumann (1903-1957) là người đầu tiên khái niệm hóa ý tưởng "virus máy tính" bằng bài báo của mình phát hành năm 1949, trong đó, ông đã phát triển nền tảng lý thuyết về một thực thể tự nhân bản tự động, làm việc trong máy tính. Mãi đến năm 1971, trong thời đại ARPANET (khởi nguyên của Internet), các máy tính DEC PDP-10 hoạt động trên hệ điều hành TENEX bất ngờ hiển thị dòng thông báo với nội dung "Tôi là Creeper. Hãy bắt tôi nếu bạn có thể!".

**1983 - Bằng sáng chế đầu tiên trong lĩnh vực an ninh mạng tại Hoa Kỳ:** Vào thời điểm khi máy tính bắt đầu phát triển, các nhà phát minh và chuyên gia công nghệ trên khắp thế giới trở nên gấp rút với mong muốn ghi dấu vào lịch sử và yêu cầu bằng sáng chế cho các hệ thống máy tính mới. Bằng sáng chế đầu tiên của Hoa Kỳ về an ninh mạng được công bố vào tháng 9 năm 1983, khi viện Công nghệ Massachusetts (MIT) được cấp bằng sáng chế 4.405.829 cho một "hệ thống và phương thức truyền thông mật mã".

**1993 – Hội nghị DEF CON đầu tiên:** DEF CON là một trong những hội nghị kỹ thuật an ninh mạng nổi tiếng nhất thế giới. Diễn ra lần đầu tiên vào tháng 6 năm 1993 bởi Jeff Moss, được tổ chức tại Las Vegas, số lượng tham gia chỉ với 100 người. Ngày nay, hội nghị thường niên này thu hút sự tham gia của hơn 20.000 chuyên gia an ninh mạng, hacker mũ trắng, nhà báo trong lĩnh vực công nghệ, chuyên gia IT từ khắp nơi trên thế giới.

**1995 – Sự ra đời của Security Sockets Layer (SSL) 2.0:** Đây là một tiêu chuẩn an ninh công nghệ toàn cầu tạo ra liên kết giữa máy chủ web (web server) và trình duyệt. Liên kết này đảm bảo cho việc tất cả các dữ liệu trao đổi giữa máy chủ web và trình duyệt luôn được bảo mật và an toàn, mang tính riêng tư, tách rời. SSL là một chuẩn công nghệ được sử dụng bởi hàng triệu trang web trong việc bảo vệ các giao dịch trực tuyến với khách hàng của họ.

**2003 – Sự xuất hiện của Anonymous:** "Anonymous" là nhóm hacker nổi tiếng toàn cầu đầu tiên được biết đến. Đây là một tổ chức không có lãnh đạo, thay vào đó, đại diện cho nhiều người dùng cộng đồng trực tuyến (online) và ngoại tuyến (offline). Được biết đến với việc đấu tranh cho tự do ngôn luận và tự do Internet bằng cách xuống đường biểu tình hay thực hiện tấn công từ chối dịch vụ (DDoS) vào website của các chính quyền, tôn giáo, và công ty quốc tế. Đeo lên chiếc mặt nạ Guy Fawkes – tổ chức này thu hút sự chú ý tầm cỡ quốc gia khi tấn công website của nhà thờ giáo phái Khoa luận giáo (Scientology).

**2010 - Chiến dịch Operation Aurora – Hacking tầm cỡ quốc gia:** Vào nửa cuối năm 2009, hãng Google tại Trung Quốc công bố đã dính hàng loạt vụ tấn công mạng mang tên "Chiến dịch ánh ban mai" (Operation Aurora). Google ban đầu cho rằng mục tiêu của kẻ tấn công là cố gắng truy cập vào tài khoản Gmail của các nhà hoạt động nhân quyền Trung Quốc. Tuy nhiên, các nhà phân tích sau đó đã phát hiện ra ý định thực sự đằng sau chiến dịch này là để tìm kiếm, xác định danh tính các nhà hoạt động tình báo Trung Quốc tại Hoa Kỳ - những đối tượng có thể nằm trong danh sách theo dõi của các cơ quan thực thi pháp luật ở xứ sở Cờ Hoa. Chiến dịch này cũng tấn công hơn 50 công ty trong lĩnh vực Internet, tài chính, công nghệ, truyền thông và hóa học.

**Ngày nay – An ninh mạng trở nên quan trọng hơn bao giờ hết:** Không gian mạng ngày nay đã trở thành một chiến trường kỹ thuật số bao gồm các quốc gia và những kẻ tấn công mạng. Để theo kịp xu hướng toàn cầu, ngành công nghiệp an ninh mạng phải không ngừng cải tiến, đổi mới và sử dụng các phương pháp tiếp cận dựa trên "máy học nâng cao" (Advanced Machine Learning) và AI tiên tiến, với mục tiêu phân tích các hành vi mạng và ngăn chặn sự tấn công của bọn tội phạm.

## Mục tiêu của an ninh mạng

Mục tiêu của an ninh mạng là bảo vệ thông tin khỏi bị đánh cắp, xâm phạm hoặc bị tấn công. Độ bảo mật an ninh mạng có thể được đo lường bằng ít nhất một trong ba mục tiêu sau: Bảo vệ tính bảo mật của dữ liệu, bảo toàn tính toàn vẹn của dữ liệu, thúc đẩy sự sẵn có của dữ liệu cho người dùng được ủy quyền. Những mục tiêu này tạo thành bộ ba "Bảo mật – Toàn vẹn – Sẵn có" (Confidentiality – Integrity – Availability), đây là cơ sở cốt lõi của tất cả các chương trình bảo mật thông tin. Tam giác CIA là một mô hình bảo mật được thiết kế để hướng dẫn thực thi các chính sách bảo mật thông tin trong khuôn khổ nội bộ một tổ chức hoặc một công ty. Mô hình này cũng được gọi là AIC để tránh sự nhầm lẫn với Cơ quan Tình báo Trung ương Hoa Kỳ (CIA - Central Intelligence Agency).

### Tính bảo mật (Confidentiality)

Bảo mật gần tương đương với quyền riêng tư và việc tránh tiết lộ thông tin trái phép. Liên quan đến việc bảo vệ dữ liệu, bảo mật cung cấp quyền truy cập cho những người được phép và ngăn chặn người khác tiếp xúc với bất kỳ thông tin nào về nội dung của chủ sở hữu. Yếu tố này ngăn chặn thông tin cá nhân tiếp cận sai người trong khi đảm bảo rằng người dùng mục tiêu có thể thu thập được thông tin cần thiết. Mã hóa dữ liệu là một ví dụ điển hình để đảm bảo tính bảo mật.

Các công cụ chính phục vụ cho tiêu chí "bảo mật":

-Mã hóa (Encryption): Mã hóa là một phương pháp chuyển đổi thông tin khiến dữ liệu trở nên không thể đọc được đối với người dùng trái phép bằng cách sử dụng thuật toán. Sử dụng khóa bí mật (khóa mã hóa) để dữ liệu được chuyển đổi, chỉ có thể được đọc bằng cách sử dụng một khóa bí mật khác (khóa giải mã). Công cụ này nhằm bảo vệ những dữ liệu nhạy cảm như số thẻ tín dụng, bằng cách mã hóa và chuyển đổi dữ liệu thành một văn bản mật mã không thể đọc được, dữ liệu này chỉ có thể được đọc một khi đã giải mã nó. Khóa bất đối xứng (asymmetric-key) và khóa đối xứng (symmetric-key) là hai loại mã hóa chính phổ biến nhất.

-Kiểm soát quyền truy cập (Access Control): Đây là công cụ xác định các quy tắc và chính sách để giới hạn quyền truy cập vào hệ thống hoặc các tài nguyên, dữ liệu ảo/vật lý. Kiểm soát quyền truy cập bao gồm quá trình người dùng được cấp quyền truy cập và một số đặc quyền nhất định đối với hệ thống, tài nguyên hoặc thông tin. Trong các hệ thống kiểm soát quyền truy cập, người dùng cần xuất trình thông tin đăng nhập trước khi có thể được cấp phép tiếp cận thông tin, có thể kể đến như danh tính, số sê-ri của máy chủ. Trong các hệ thống vận hành vật lý, các thông tin đăng nhập này có thể tồn tại dưới nhiều dạng, nhưng với các thông tin không thể được chuyển giao sẽ cung cấp tính bảo mật cao nhất.

- Xác thực (Authentication): Xác thực là một quá trình đảm bảo và xác nhận danh tính hoặc vai trò của người dùng. Công cụ này có thể được thực hiện theo một số cách khác nhau, nhưng đa số thường dựa trên sự kết hợp với: một thứ gì đó mà cá nhân sở hữu (như thẻ thông minh hoặc khóa radio để lưu trữ các khóa bí mật), một thứ gì đó mà cá nhân biết (như mật khẩu) hoặc một thứ gì đó dùng để nhận dạng cá nhân (như dấu vân tay). Xác thực đóng vai trò cấp thiết đối với mọi tổ chức, vì công cụ này cho phép họ giữ an toàn cho mạng lưới thông tin của mình bằng cách chỉ cho phép người dùng được xác thực truy cập vào các tài nguyên dưới sự bảo vệ, giám sát của nó. Những tài nguyên này có thể bao gồm các hệ thống máy tính, mạng, cơ sở dữ liệu, website và các ứng dụng hoặc dịch vụ dựa trên mạng lưới khác.

- Cấp quyền (Authorization): Đây là một cơ chế bảo mật được sử dụng để xác định quyền hạn (privilege) một người nào đó đối với các tài nguyên như các chương trình máy tính, tệp tin, dịch vụ, dữ liệu và tính năng ứng dụng. Ủy quyền thường được đi sau xác thực nhằm xác định một user sau khi đã đăng nhập thành công thì được phép làm những gì đối với từng loại dữ liệu. Quản trị viên hệ thống thường là người chỉ định cấp phép hoặc từ chối quyền truy cập đối với cá nhân khi muốn tiếp cận thông tin dữ liệu và đăng nhập vào hệ thống.

- Bảo mật vậy lý (Physical Security): Đây là các biện pháp được thiết kế để ngăn chặn sự truy cập trái phép vào các tài sản công nghệ thông tin như cơ sở vật chất, thiết bị, nhân sự, tài nguyên và các loại tài sản khác nhằm tránh bị hư hại. Công cụ này bảo vệ các tài sản nêu trên khỏi các mối đe dọa vật lý như: trộm cắp, phá hoại, hỏa hoạn và thiên tai.

### Tính toàn vẹn (Integrity)

Tính toàn vẹn đề cập đến các phương pháp nhằm đảm bảo nguồn dữ liệu là thật, chính xác và được bảo vệ khỏi sự sửa đổi trái phép của người dùng.

Các công cụ chính phục vụ cho tiêu chí "toàn vẹn":

* Sao lưu (Backups): Sao lưu là lưu trữ dữ liệu định kỳ. Đây là một quá trình tạo lập các bản sao của dữ liệu hoặc tệp dữ liệu để sử dụng trong trường hợp khi dữ liệu gốc hoặc tệp dữ liệu bị mất hoặc bị hủy. Sao lưu cũng được sử dụng để tạo các bản sao phục vụ cho các mục đích lưu lại lịch sử dữ liệu, chẳng hạn như các nghiên cứu dài hạn, thống kê hoặc cho các ghi chép, hoặc đơn giản chỉ để đáp ứng các yêu cầu của chính sách lưu trữ dữ liệu
* Tổng kiểm tra (Checksums): Tổng kiểm tra là một giá trị số được sử dụng để xác minh tính toàn vẹn của tệp hoặc dữ liệu được truyền đi. Nói cách khác, đó là sự tính toán của một hàm phản ánh nội dung của tệp thành một giá trị số. Chúng thường được sử dụng để so sánh hai bộ dữ liệu, nhằm đảm bảo rằng chúng giống hệt nhau. Hàm tổng kiểm tra phụ thuộc vào toàn bộ nội dung của tệp, nó được thiết kế theo cách mà ngay cả một thay đổi nhỏ đối với tệp đầu vào (chẳng hạn như lệch một bit) có thể dẫn đến giá trị đầu ra khác nhau.
* Mã chỉnh dữ liệu (Data Correcting Codes): Đây là một phương pháp để lưu trữ dữ liệu theo cách mà những thay đổi nhỏ nhất cũng có thể dễ dàng được phát hiện và tự động điều chỉnh.

### Tính sẵn có (Availability)

Mọi hệ thống thông tin đều phục vụ cho mục đích riêng của nó và thông tin phải luôn luôn sẵn sàng khi cần thiết. Hệ thống có tính sẵn sàng cao hướng đến sự sẵn có, khả dụng ở mọi thời điểm, tránh được rủi ro, đảm bảo thông tin có thể được truy cập và sửa đổi kịp thời bởi những người được ủy quyền.

Các công cụ chính phục vụ cho tiêu chí "sẵn có":

* Bảo vệ vật lý (Physical Protections): Có nghĩa là giữ thông tin có sẵn ngay cả trong trường hợp phải đối mặt với thách thức về vật chất. Đảm bảo các thông tin nhạy cảm và công nghệ thông tin quan trọng được lưu trữ trong các khu vực an toàn.
* Tính toán dự phòng (Computational Redundancies): Được áp dụng nhằm bảo vệ máy tính và các thiết bị được lưu trữ, đóng vai trò dự phòng trong trường hợp xảy ra hỏng hóc.

## Đánh giá về các loại sự đe dọa an toàn mạng

Về cơ bản có 4 nối đe doạ đến vấn đề bảo mật mạng như sau :

- Đe doạ không có cấu trúc *(Unstructured threats)*

- Đe doạ có cấu trúc (*Structured threats)*

- Đe doạ từ bên ngoài (*External threats)*

- Đe doạ từ bên trong (*Internal threats)*

Đe dọa không có cấu trúc: Những mối đe doạ thuộc dạng này được tạo ra bởi những hacker không lành nghề, họ thật sự không có kinh nghiệm. Những người này ham hiểu biết và muốn download dữ liệu từ mạng Internet về. Họ thật sự bị thúc đẩy khi nhìn thấy những gì mà họ có thể tạo ra.

Đe dọa có cấu trúc: Hacker tạo ra dạng này tinh tế hơn dạng unstructured rất nhiều. Họ có kỹ thuật và sự hiểu biết về cấu trúc hệ thống mạng. Họ thành thạo trong việc làm thế nào để khai thác những điểm yếu trong mạng. Họ tạo ra một hệ thống có “cấu trúc” về phương thức xâm nhập sâu vào trong hệ thống mạng.

Các mối đe dọa bên ngoài: Xuất phát từ Internet, những người này tìm thấy lỗ hổng trong hệ thống mạng từ bên ngoài. Khi các công ty bắt đầu quảng bá sự có mặt của họ trên Internet thì cũng là lúc các hacker rà soát để tìm kiếm điểm yếu, đánh cắp dữ liệu và phá huỷ hệ thống mạng.

Đe dọa bên trong: Mối đe doạ này thật sự rất nguy hiểm bởi vì nó xuất phát từ ngay trong chính nội bộ, điển hình là nhân viên hoặc bản thân những người quản trị. Họ có thể thực hiện việc tấn công một cách nhanh gọn và dễ dàng vì họ am hiểu cấu trúc cũng như biết rõ điểm yếu của hệ thống mạng.

## Lỗ hổng bảo mật và các loại tấn công phổ biến

Lỗ hổng bảo mật là một điểm yếu của hệ thống trong quá trình thiết kế, thi công và quản trị. Phần lớn các lỗ hổng bảo mật được đã phát hiện ngày nay đều được ghi lại trong cơ sở dữ liệu Common Vulnerabilities and Exposures (CVE). Một lỗ hổng bị khai thác là một lỗ hổng mà đã bị lợi dụng để thực hiện hoạt động tấn công ít nhất một lần hoặc đã bị khai thác (exploit).

Để đảm bảo một hệ thống máy tính, điều quan trọng là phải hiểu các cuộc tấn công có thể được thực hiện chống lại nó, và các mối đe dọa thường được xếp vào một trong các mục dưới đây:

* Tấn công bằng phần mềm độc hại (Malware Attack): Malware là phần mềm độc hại, được kết hợp giữa hai từ "malicious" và "software". Đây là một trong những hình thức đe dọa mạng phổ biến nhất. Tội phạm mạng và các hacker tạo ra malware với mục đích làm phá vỡ hoặc hư hỏng máy tính của người dùng hợp pháp. Thông thường, hacker sẽ tấn công người dùng thông qua các lỗ hổng bảo mật, dụ dỗ người dùng click vào một đường link đính kèm trong thư rác hoặc tải các tệp tin được ngụy trang hợp-pháp để phần mềm độc hại tự động cài đặt vào máy tính. Malware thường được sử dụng nhằm phục vụ cho mục đích kiếm tiền hoặc tham gia vào các cuộc tấn công mạng có động cơ chính trị.
* Tấn công giả mạo (Phishing Attack): Phishing là hình thức giả mạo thành một đơn vị/cá nhân uy tín để chiếm lấy lòng tin của người dùng, với mục tiêu nhắm đến việc đánh cắp dữ liệu cá nhân nhạy cảm như thông tin thẻ tín dụng, mật khẩu, tài khoản đăng nhập hoặc cài đặt các phần mềm độc hại vào máy tính nạn nhân. Phishing thường được thực hiện bằng cách sử dụng thư điện tử (email) hoặc tin nhắn.
* Tấn công trung gian (Man-in-the-middle Attack): Xảy ra khi kẻ tấn công mạng xâm nhập vào một giao dịch đang diễn ra giữa 2 đối tượng, một khi đã xen vào thành công, chúng có thể chắt lọc và đánh cắp dữ liệu. Một số biến thể của tấn công trung gian có thể kể đến như đánh cắp mật khẩu, chuyển tiếp các thông tin không xác thực. Thông thường, khi sử dụng Wi-Fi công cộng thiếu bảo mật, kẻ tấn công có thể tự "chen" vào giữa thiết bị của người truy cập và mạng Wi-Fi đó, tất cả dữ liệu cá nhân mà nạn nhân gửi đi sẽ rơi vào tay bọn tội phạm mà không hề hay biết. Trong một số trường hợp, kẻ tấn công còn cài đặt các ứng dụng khác nhằm thu thập thông tin về nạn nhân thông qua phần mềm độc hại (malware).
* Tấn công từ chối dịch vụ (Denial of Service): Các cuộc tấn công từ chối dịch vụ (DoS) được thiết kế để làm cho tài nguyên mạng hoặc máy không sẵn sàng để phục vụ cho người dùng dự định của nó. [5] Kẻ tấn công có thể từ chối dịch vụ cho từng nạn nhân, chẳng hạn như cố tình nhập sai mật khẩu đủ lần liên tục để khiến tài khoản nạn nhân bị khóa hoặc chúng có thể làm quá tải khả năng của máy hoặc mạng và chặn tất cả người dùng cùng một lúc. Mặc dù một cuộc tấn công mạng từ một địa chỉ IP duy nhất có thể bị chặn bằng cách thêm quy tắc tường lửa mới, nhiều hình thức tấn công từ chối dịch vụ phân tán (DDoS) là có thể, trong đó cuộc tấn công đến từ một số lượng lớn mấy tính - và việc bảo vệ khó khăn hơn nhiều. Các cuộc tấn công như vậy có thể bắt nguồn từ các máy tính zombie của botnet, nhưng một loạt các kỹ thuật khác có thể bao gồm các cuộc tấn công phản xạ và khuếch đại, trong đó các hệ thống vô tội bị lừa gửi dữ liệu đến máy nạn nhân.
* Tấn công cơ sở dữ liệu (SQL Injection Attack): Hacker chèn một đoạn code độc hại vào server sử dụng ngôn ngữ truy vấn có cấu trúc (SQL), mục đích là để khiến máy chủ trả về những thông tin quan trọng mà lẽ ra không được tiết lộ. Các cuộc tấn công SQL Injection xuất phát từ lỗ hổng của website, hacker có thể tấn công đơn giản bằng cách chèn một đoạn mã độc vào thanh công cụ "Tìm kiếm" là đã có thể dễ dàng tấn công những website với mức bảo mật yếu.
* Tấn công "cửa hậu" (Backdoor Attack): Trong một hệ thống máy tính, Backdoor ("cửa hậu") là một phương pháp bí mật vượt qua thủ tục chứng thực người dùng thông thường hoặc để giữ đường truy nhập từ xa tới một máy tính, trong khi cố gắng không bị phát hiện bởi việc giám sát thông thường. Chúng tồn tại vì một số lý do, bao gồm từ thiết kế ban đầu hoặc từ cấu hình kém. Chúng có thể đã được thêm vào bởi một nhóm có thẩm quyền để cho phép một số truy cập hợp pháp, hoặc bởi những kẻ tấn công vì lý do độc hại; nhưng bất kể động cơ đưa tới sự tồn tại của chúng, chúng tạo ra một lỗ hổng.
* Khai thác lỗ hổng (Zero-day Exploits): Lỗ hổng Zero-day (hay còn gọi là 0-day) là thuật ngữ để chỉ những lỗ hổng phần mềm hoặc phần cứng chưa được biết đến và chưa được khắc phục. Các hacker có thể tận dụng lỗ hổng này để tấn công xâm nhập vào hệ thống máy tính của doanh nghiệp, tổ chức nhằm đánh cắp hoặc thay đổi dữ liệu.

## Các giai đoạn tấn công



Hình 1.1-Các giai đoạn tấn công an toàn mạng

### Thăm dò (Reconnaissace)

Thăm dò mục tiêu là một trong những bước qua trọng để biết những thông tin trên hệ thống mục tiêu. Hacker sử dụng kỹ thuật này để khám phá hệ thống mục tiêu đang chạy trên hệ điều hành nào, có bao nhiêu dịch vụ đang chạy trên các dịch vụ đó, cổng dịch vụ nào đang đóng và cổng nào đang mở, gồm hai loại:

-Passive: Thu thập các thông tin chung như vị trí địa lý, điện thoại, email của các cá nhân, người điều hành trong tổ chức.

-Active: Thu thập các thông tin về địa chỉ IP, domain, DNS, … của hệ thống

### Quét hệ thống (Scanning)

Quét thăm dò hệ thống là phương pháp quan trọng mà Attacker thường dùng để tìm hiểu hệ thống và thu thập các thông tin như địa chỉ IP cụ thể, hệ điều hành hay các kiến trúc hệ thống mạng. Một vài phương pháp quét thông dụng như: quét cổng, quét mạng và quét các điểm yếu trên hệ thống.

### Chiếm quyền điều khiển (Gainning access)

Đến đây hacker đã bắt đầu dần dần xâm nhập được hệ thống và tấn công nó ,đã truy cập được nó bằng các lệnh khai thác. Các lệnh khai thác luôn ở bất cứ không gian nào, từ mạng LAN cho tới INTERNET và đã lan rộng ra mạng không dây.

Hacker có thể chiếm quyền điều khiển tại:

* Mức hệ điều hành/ mức ứng dụng.
* Mức mạng.
* Từ chối dịch vụ.

### Duy trì điều khiển hệ thống (Maitaining access)

Đến đây hacker bắt đầu phá hỏng làm hại, hoặc có thể cài trojan, rootkit, backdoor để lấy thông tin thêm. Thường được thấy sử dụng để đánh cắp tài khoản tín dụng, ngân hàng...

### Xoá dấu vết (Clearning tracks)

Được đề cập đến hoạt động được thực hiện bằng cách hacker cố tình che dấu hành động xâm nhập của mình. Hacker phải tìm cách xóa đi dấu vết mỗi khi đột nhập bằng các phương thức như Steganography, tunneling, and altering log file.

## Các biện pháp phát hiện hệ thống bị tấn công

Không có một hệ thống nào có thể đảm bảo an toàn tuyệt đối, mỗi một dịch vụ đều có những lỗ hỏng bảo mật tiềm tàng. Người quản trị hệ thống không những nghiên cứu, xác định các lỗ hỏng bảo mật mà còn phải thực hiện các biện pháp kiểm tra hệ thống có dấu hiệu tấn công hay không. Một số biện pháp cụ thể :

1. Kiểm tra các dấu hiệu hệ thống bị tấn công : Hệ thống thường bị treo bằng những thông báo lỗi không rõ ràng. Khó xác định nguyên nhân do thiếu thông tin liên quan. Trước tiên, xác định các nguyên nhân có phải phần cứng hay không, nếu không phải hãy nghĩ đến khả năng máy tính bị tấn công.
2. Kiểm tra các tài khoản người dùng mới lạ, nhất là với các tài khoản có ID bằng không.
3. . Kiểm tra sự xuất hiện của các tập tin lạ. Người quản trị hệ thống nên có thói quen đặt tên tập theo mẫu nhất định để dễ dàng phát hiện tập tin lạ
4. . Kiểm tra thời gian thay đổi trên hệ thống.
5. Kiểm tra hiệu năng của hệ thống : Sử dụng các tiện ích theo dõi tài nguyên và các tiến trình đang hoạt động trên hệ thống.
6. Kiểm tra hoạt động của các dịch vụ hệ thống cung cấp.
7. . Kiểm tra truy nhập hệ thống bằng các tài khoản thông thường, đề phòng trường hợp các tài khoản này bị truy nhập trái phép và thay đổi quyền hạn mà người sử dụng hợp pháp không kiểm soát được.
8. . Kiểm tra các file liên quan đến cấu hình mạng và dịch vụ, bỏ các dịch vụ không cần thiết.
9. Kiểm tra các phiên bản của sendmaill, /bin/mail, ftp,.. tham gia các nhóm tin về bảo mật để có thông tin về lỗ hỏng của dịch vụ sử dụng.

Các biện pháp này kết hợp với nhau tạo nên một chính sách về bảo mật đối với hệ thống.

# ĐÁNH GIÁ CÁC CÔNG CỤ AN NINH MẠNG

Việc sử dụng các công cụ an ninh mạng giúp cho việc bảo vệ an toàn mạng hiệu quả, phát hiện các mối đe doạ nguy hiểm. Các công cụ phổ biến và được nhiều người tin dùng gồm có: Nmap, RogueScanner, SoftPerfect Network Scanner, Wireshark, SecurityBox, SQLMap, Metasploit Framework, Nessus,... Do hạn chế về thời gian thực hiện nên chúng em xin tìm hiểu và đánh giá 3 công cụ gồm: Nmap, Nessus và Wireshark.

## Nmap

### Nmap là gì?

Nmap (tên đầy đủ Network Mapper) là một công cụ bảo mật được phát triển bởi Floydor Vaskovitch. Nmap được các quản trị viên mạng sử dụng rộng rãi để quét:

* Mở các cổng và dịch vụ
* Khám phá các dịch vụ cùng với các phiên bản của chúng
* Đoán hệ điều hành đang chạy trên máy mục tiêu
* Nhận các tuyến gói chính xác cho đến máy mục tiêu
* Giám sát máy chủ

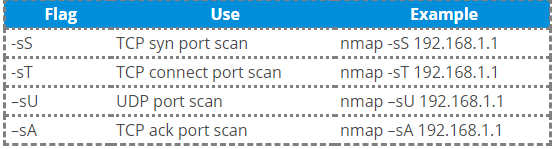
### Các kiểu quét Nmap

Có thể thực hiện nhiều kiểu quét bằng Nmap. Dưới đây là các loại quét:

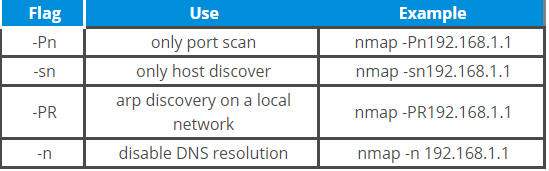
* TCP Connect() Scan: Trong kiểu scan này, gửi một gói tin SYN đến tất cả các cổng của máy mục tiêu.nếu một hoặc nhiều cổng được mở nó sẽ trả về một gói tin SYN|ACK, và kẻ tấn công sẽ hoàn thành một quá trình bắt tay bằng việc gửi lại gói tin ACK, Nếu các cổng đều đóng thì mục tiêu sẽ trả về gói tin RST để khởi động lại kết nối.
* SYN Scan: Đây là một kiểu scan khác với TCP Connect() Scan vì quá trình bắt tay 3 bước sẽ không được hoàn thành. Kẻ tấn công sẽ gửi một gói tin SYN đến tất cả các cổng của mục tiêu. Trong trường hợp các cổng tương ứng mở nó sẽ gửi trả lại một gói tin SYN | ACK. Tại điểm này kẻ tấn công sẽ kết thúc bằng một gói tin RST. Nếu cổng đóng mục tiêu sẽ gửi trở lại một gói tin RST. Trong cả 2 trường hợp quá trình bắt tay 3 bước đều sẽ không được hoàn thành.
* FIN Scan: Kẻ tấn công sẽ gửi một gói tin với cờ FIN tới tất cả các cổng của mục tiêu. Với các cổng được mở, mục tiêu sẽ bỏ qua gói tin và không phản hồi về cho kẻ tấn công. Các cổng đóng sẽ gửi về gói tin RST để khởi tạo kết nối.
* XMAS Scan: Gần giống như FIN scan nhưng trong kiểu scan này kẻ tấn công sẽ gửi một gói tin FIN|URG|PSH.
* NULL Scan: Kiểu scan này tương tự như FIN scan và XMAS scan nhưng kẻ tấn công sẽ gửi một gói tin mà không thiết lập bất cứ cờ nào trong Header của TCP.
* UDP Scan: Đây là kiểu scan để phát hiện một cổng UDP đang mở. Gói tin UDP sẽ được gửi tới tất cả các cổng của mục tiêu, nếu cổng mở mục tiêu sẽ không gửi lại gì, nếu cổng là đóng mục tiêu sẽ gửi lại một gói tin ICMP Port Unreachable.
* Decoy Scan: Decoy Scan là một kỹ thuật thực hiện một IP Spoofing (giả mạo). Mục đích nhằm ấn địa chỉ thực sự của kẻ tấn công (scanner).
* Idle Scan: Idel Scan là một kỹ thuật phức tạp cho phép ẩn hoàn toàn kẻ tấn công. trong Scan này sẽ có 3 thành phần: 1 là kẻ tấn công, một Zombie (một máy bị kẻ tấn công lợi dụng) và một là mục tiêu cần quét cổng. Điều kiện là máy Zombie không thực hiện các hoạt động khác ngoại trừ việc giao tiếp với Kẻ tấn công. IPID: Mỗi IP packet được gửi trên mạng có một số duy nhất được gọi là fragment identification (hay gọi là IPID)

### Các câu lệnh Nmap

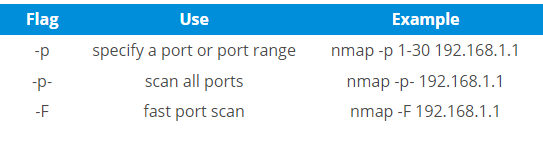
Sau đây là liêt kê các câu lệnh thường dùng và mô tả của chúng



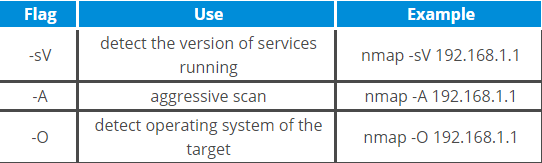
Hình 2.1 Kỹ thuật quét



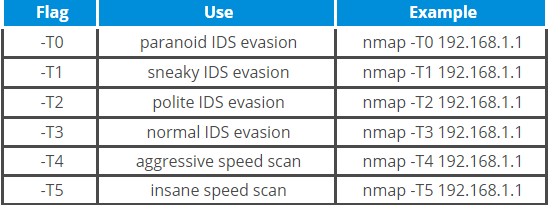
Hình 2.2 Khám phá máy chủ



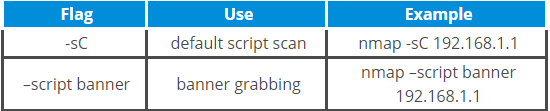
Hình 2.3 Đặc điểm kỹ thuật cổng

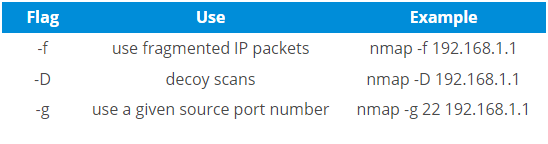


Hình 2.4 Phiên bản dịch vụ và phát hiện hệ điều hành



Hình 2.5 Thời gian và Hiệu suất

Hình 2.6 Tập lệnh NSE

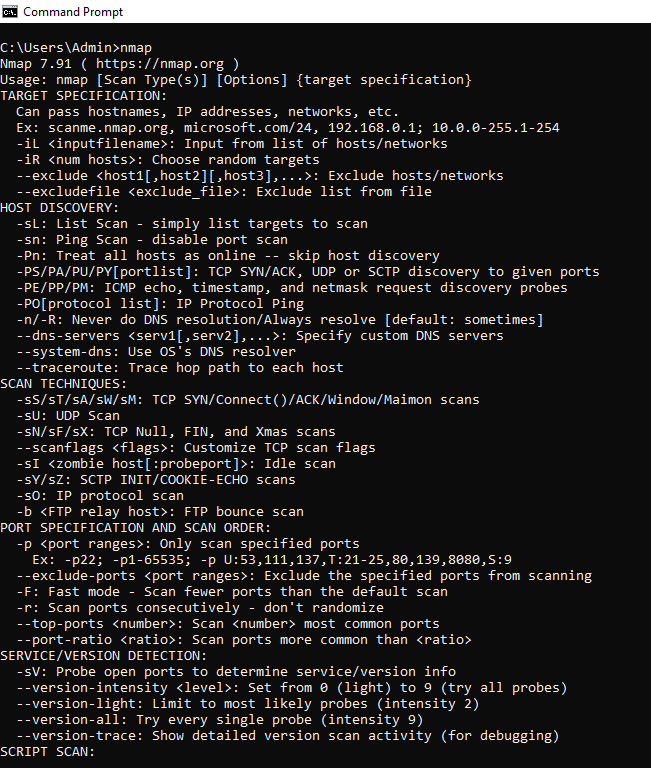


Hình 2.7 DS trốn tránh

### Sử dụng Nmap

Áp dụng các câu lênh Nmap vào thực tế

Bước 1: Xem giúp đỡ của câu lệnh NMAP

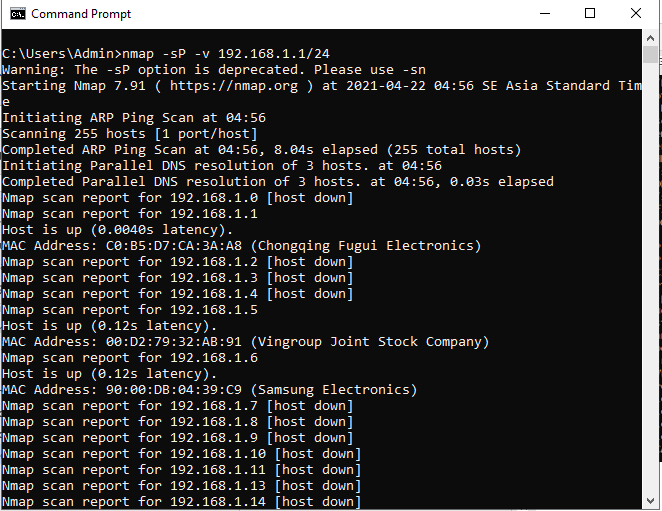


Hình 2.8 Xem giúp đỡ của câu lệnh NMAP

Bước 2: thực hiện quá trình ping sweep cho đường mạng 192.168.1.0/24 để

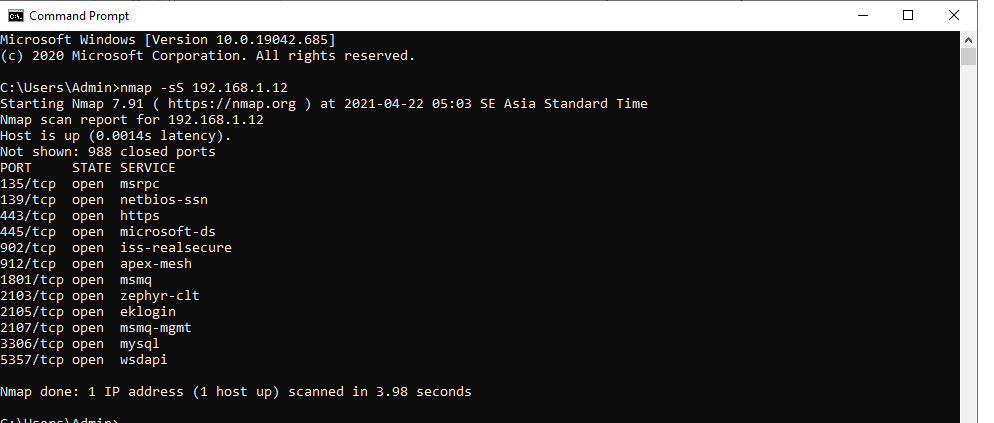
xác định các host đang có trong đường mạng bằng câu lệnh “nmap -sP -v

192.168.1.1/24”



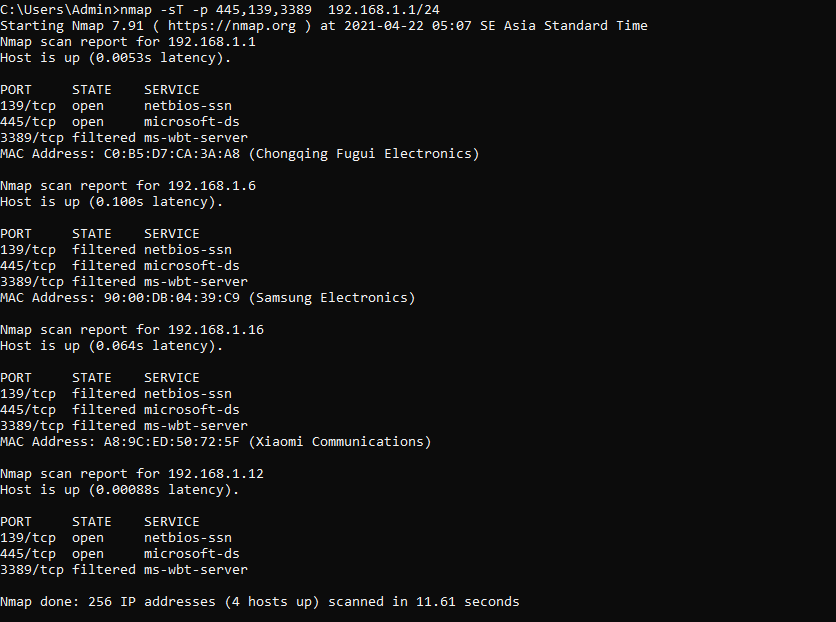
Hình 2.9 Kiểm tra đường mạng để xác định host.

Bước 3: Ta cần xác định xem ở IP 192.168.1.12 đang có nhưng port nào đang mở. Để làm việc này ta có thể sử dụng các dạng scan khác nhau. Ví dụ ở đây ta sử dụng kỹ thuật SYN scan với câu lệnh “nmap –sS 192.168.1.12”



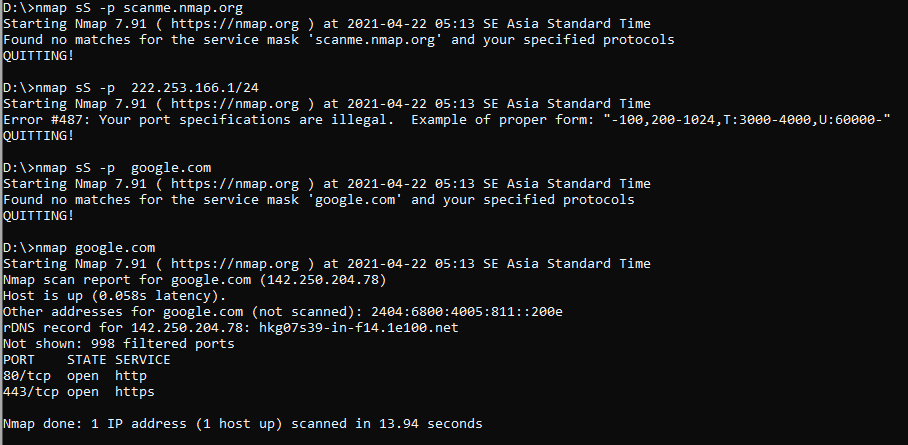
Hình 2.10 Kiểm tra để xác định các port đang mở

Bước 4: xác định giá trị port trong quá trình scan. Mặc định chương trình sẽ scan tất cả các port. Ví dụ ta cần xác định trong đường mạng 192.168.1.1/24 thì đang có bao nhiêu máy đang mở port 445,139,80,3389 ta có thể sử dụng câu lệnh “nmap -sT -p 445,139,3389 192.168.1.1/24”



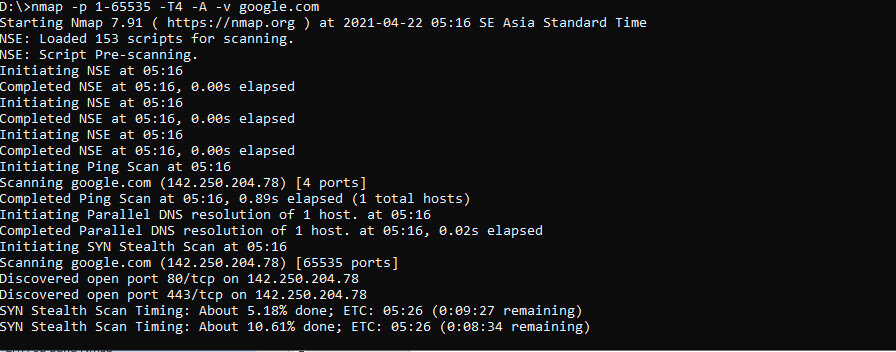
Hình 2.11 Kiểm tra xem đường mạng đã mở các port hay chưa.

Bước 5: Quét một máy chủ duy nhất cho 1000 cổng nổi tiếng. Các cổng này là những cổng được sử dụng bởi các dịch vụ phổ biến như SQL, SNTP, apache và các cổng khác.



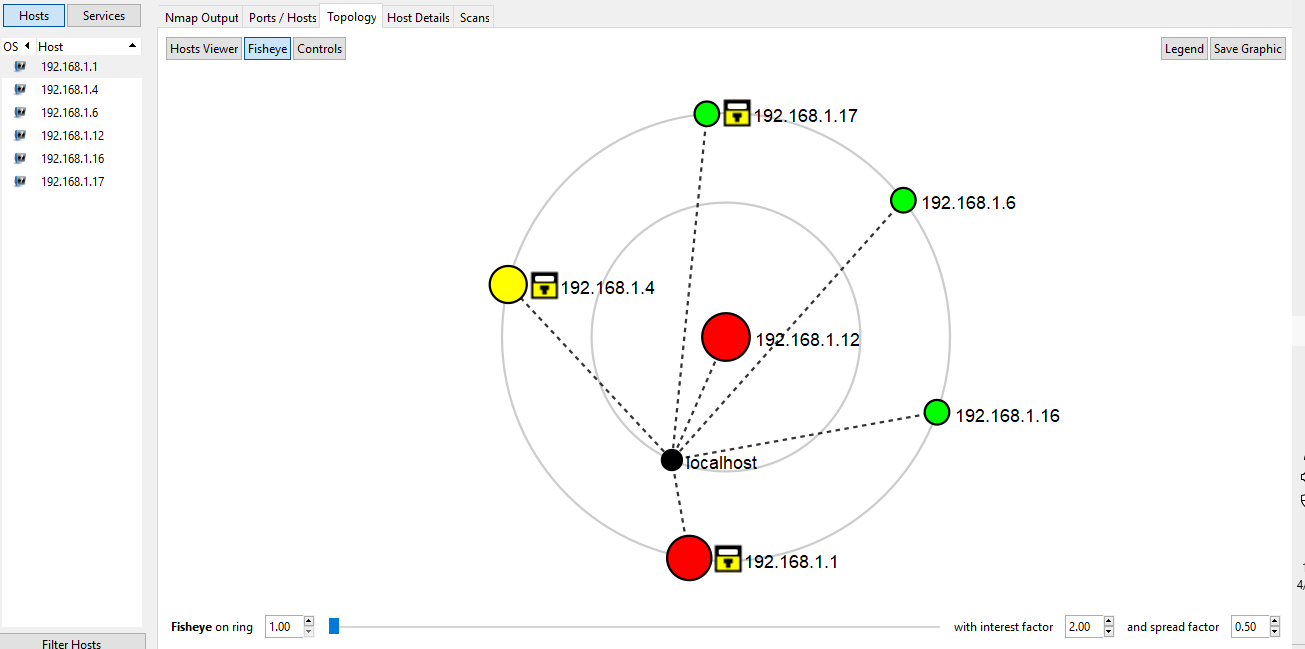
Hình 2.12 Quét tên miền bên ngoài

Bước 6: Sử dụng nmap để xác định các thông số của các ứng dụng được triển khai trên server. Ta sử dụng “nmap -p 1-65535 -T4 -A -v tên\_server”



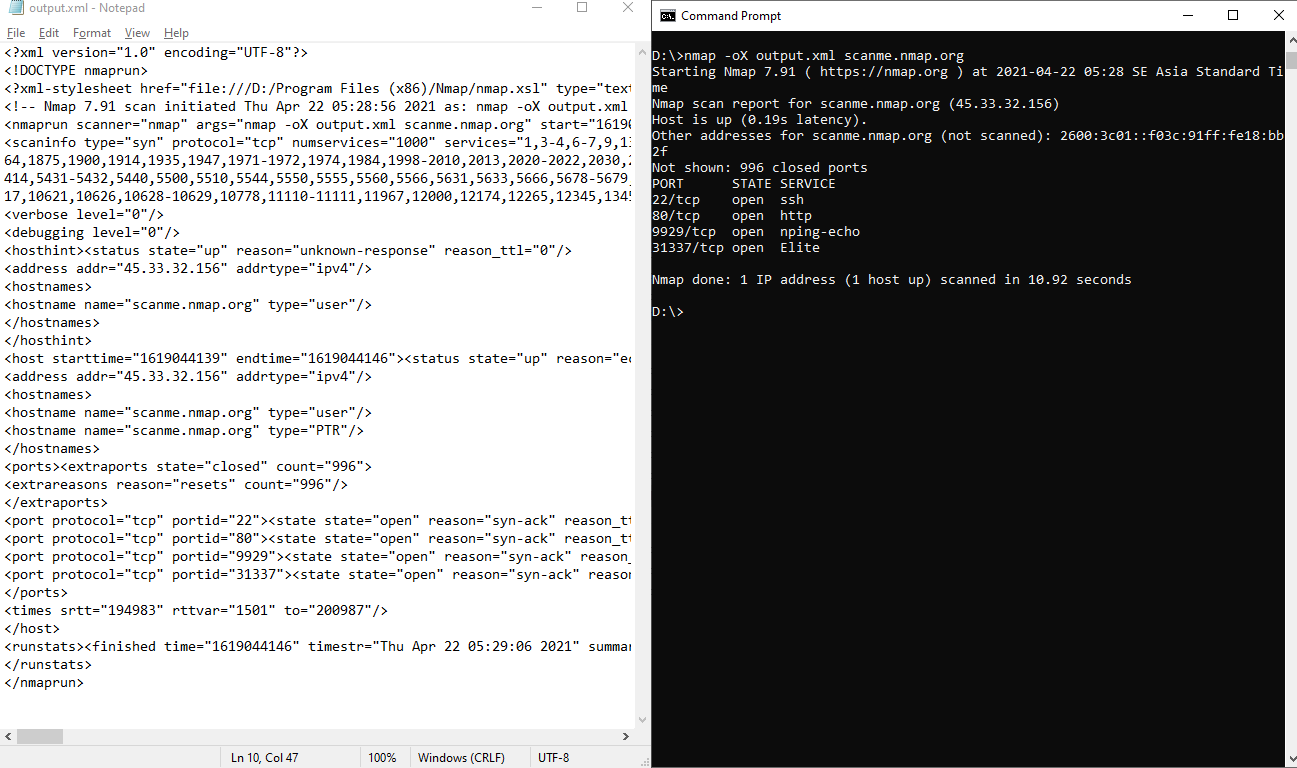
Hình 2.13 Xem các thông số trên server

Bước 7: Có thể dùng Zenmap là GUI của Nmap trong việc xem mô hình mạng



Hình 2.14 Mô hình mạng trong Zenmap

Bước 9: Bản quét Nmap cũng có thể được xuất sang XML. Đây cũng là định dạng tệp ưa thích của hầu hết các công cụ kiểm tra bằng bút, giúp dễ dàng phân tích cú pháp khi nhập kết quả quét.



Hình 2.15 Xuất file xml sau khi quét

### Ưu và nhược điểm

Ưu điểm:

* Các công cụ quét cổng TCP / UDP cực kỳ linh hoạt.
* Khả năng phát hiện dịch vụ / hệ điều hành.
* Khả năng tích hợp với Zenmap GUI để tạo bản đồ mạng trực quan và lưu trữ thông tin trên các máy cụ thể trong mạng.
* Rất nhiều tập lệnh NSE để trinh sát và phát hiện lỗ hổng bảo mật, thậm chí khai thác trong một số trường hợp.
* Các tùy chọn để trốn tránh tường lửa / tàng hình.
* Các định dạng đầu ra khác nhau cho phép phân tích cú pháp và xử lý kết quả bằng các chương trình khác. (XML, Grepable, v.v.)
* Tài liệu phong phú về các kỹ thuật và tập lệnh sử dụng.

Nhược điểm:

* Các tập lệnh NSE được viết bằng lua, thay vì một ngôn ngữ ít tối nghĩa như python hoặc ruby, làm cho việc mở rộng và tùy chỉnh các khả năng của Nmap hoạt động nhiều hơn bình thường.
* Việc quét các thiết bị yếu hơn và mạng bị tắc nghẽn đôi khi có thể gây ra lỗi DOS hoặc mạng chậm không chủ ý. Điều này có thể được khắc phục bằng cách làm chậm tốc độ quét mà Nmap cho phép, sử dụng cờ “-T” và bằng cách quét ít máy hơn cùng một lúc.
* Có nhiều cách để làm cho việc quét cổng lén lút hơn trong Nmap, nhưng chúng luôn yêu cầu tạo ra nhiều lưu lượng mạng và có mối quan hệ nghịch đảo giữa tính năng ẩn và tốc độ.
* Có thể khó học và thành thạo

## Nessus

### Giới thiệu

Nessus là một trong những sản phẩm bảo mật được đánh giá cao trên toàn thế giới. Với tính năng phát hiện nguy hiểm nhanh, thống kê toàn diện về hệ thống đầy đủ, phát hiện dữ liệu nhạy cảm và phân tích lỗ hổng , đáp ứng yêu cầu cao về bảo mật.

Nessus kiểm soát toàn bộ toàn hệ thống mạng doanh nghiệp bao gồm cả bên trong những khu vực DMZs (thường là những vùng chứa Email server, Web server ...) và từng đoạn mạng vật lý riêng biệt.

Nessus hỗ trợ kiểm tra các kiểu bảo mật sau đây:

* Quét các cổng đáng tin và không đáng tin.
* Quét lỗ hổng bảo mật mạng.
* Kiểm tra bản vá tin cậy cho Windows và hầu hết nền tảng Unix.
* Kiểm tra cấu hình tiêu chuẩn cao cho hầu hết nền tảng Windows và Unix.
* Nhanh chóng và dễ dàng kiểm tra độ tin cậy bảo mật một cách toàn diện cho các ứng dụng của phần mềm thứ 3 như iTunes, Java, Skype và Firefox.
* Kiểm tra lỗ hổng ứng dụng web được nhúng và tùy biến.
* Kiểm tra cấu hình CSDL SQL.
* Kiểm tra cấu hình Cisco Route.
* Thống kê phần mềm trên Unix và Windows.
* Kiểm tra phần cài đặt chữ ký số hết hạn và những lỗi cấu hình của phần mềm Anti-virus.

Nessus có thể chạy trên hầu hết các hệ điều hành: Linux, Windows, MacOS. Bạn có thể download chương trình tại trang chủ: http://www.nessus.org hoặc tải trực tiếp phiên bản mới nhất (5.0) qua đường link dưới đây: http://www.nessus.org/products/nessus/select-your-operating-system

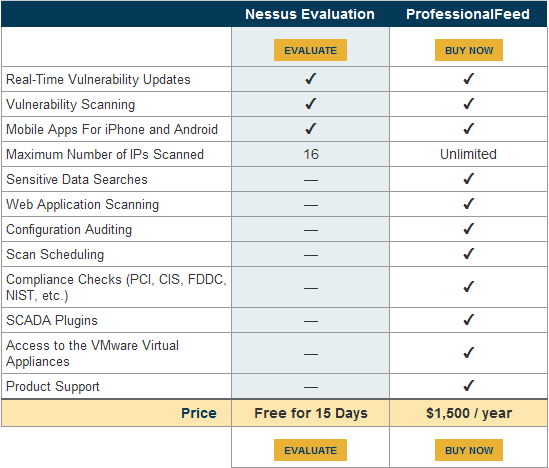
Sau khi cài đặt ta cần đăng ký key để active thông qua form đăng ký để quyết định tính năng dựa theo nhu cầu người sử dụng của Nessus. Có 3 phiên bản:

* HomeFeed: Phiên bản Free
* Evaluation: Phiên bản trial 15 ngày với 1 phần tính năng của bản ProfessionFeed.
* ProfessionFeed: Phiên bản tính phí.

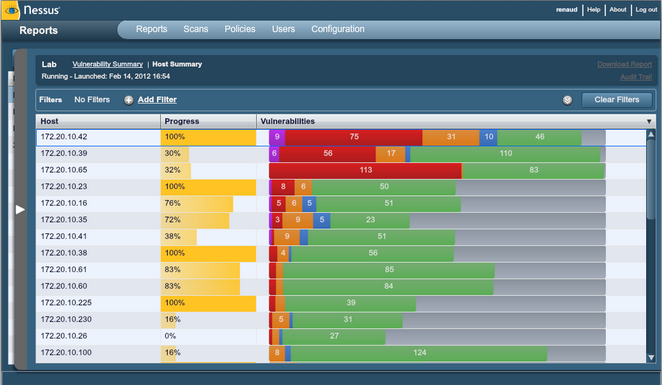
Tuy nhiên, về tính năng đương nhiên là có sự hạn chế giữa các phiên bản như hình dưới đây:



Hình 2.16 So sánh phiên bản Pro và Home



Hình 2.17 So sánh phiên bản ProfessionFeed và Evaluation



Hình 2.18 Giao diên Nessus

### Sử dụng Nessus

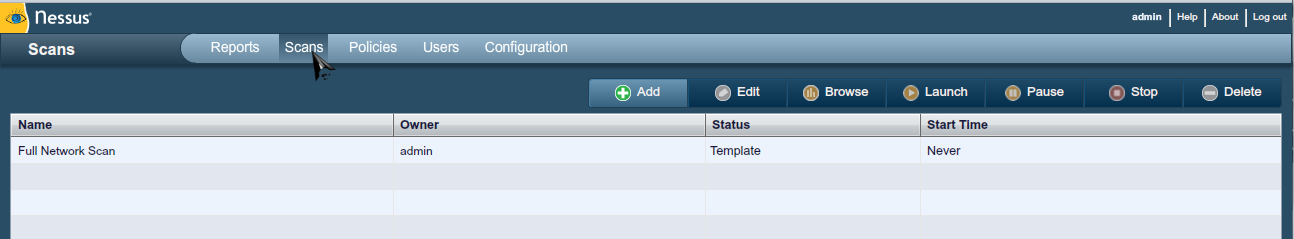
**Nội dung kịch bản:**

* Tiến hành quét lỗ hổng máy victim - máy ảo VMware WindowServer 2012 có địa chỉ 192.168.16.21 sử dụng tool Nessus
* In báo cáo thống kê những lỗ hổng mà Nexpose phát hiện được.

**Triển khai kịch bản và kết quả thu được:**

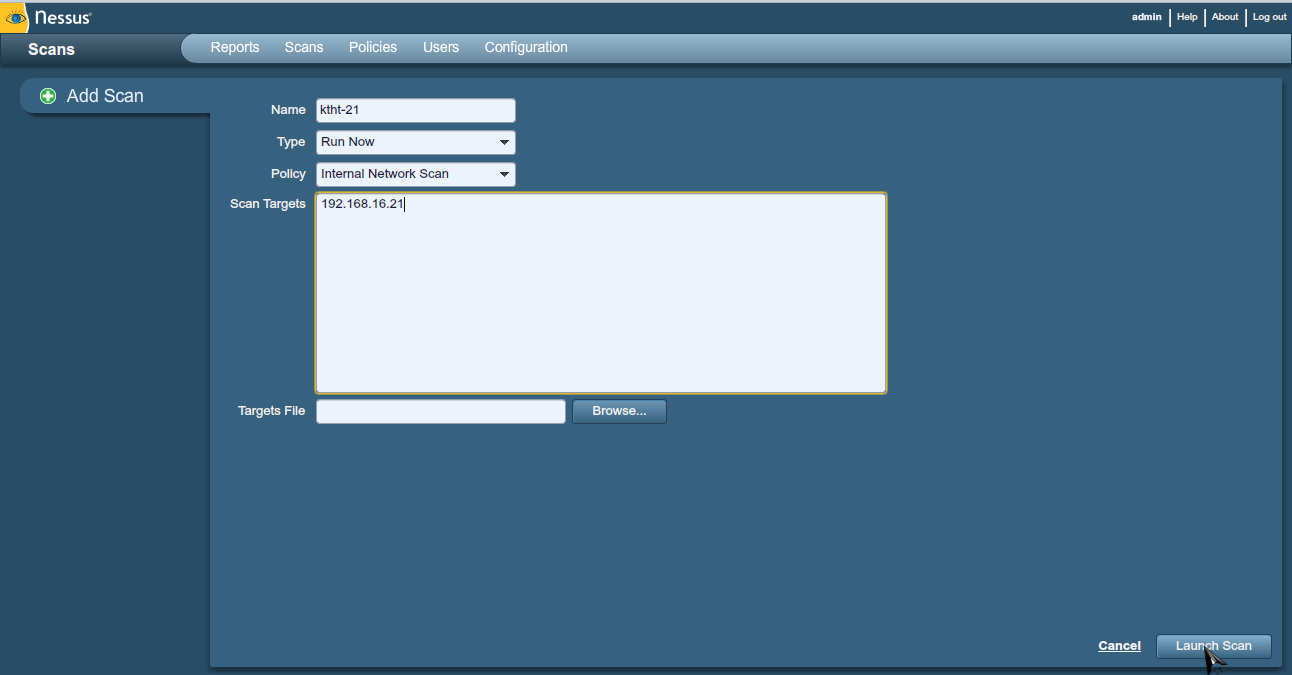
Truy cập vào giao diện web Nessus: https://localhost:8834

Thiết lập địa chỉ IP máy victim cần quét bằng cách vào tab Scan>Add



Hình 2.19 Nessus add

Ở đây máy victim có địa chỉ IP là: 192.168.16.21. Ta quét với Policy “Internal Network Scan”.

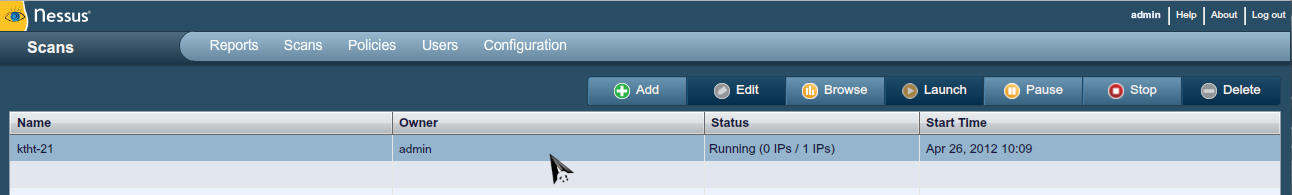


Hình 2.20 Nessus quét cổng

Tại option Policy trên, ngoài những Policy có sẵn ta cũng có thể tạo thêm nhiều Policy khác tùy theo mục đích người sử dụng bằng cách vào tab Policies>Add

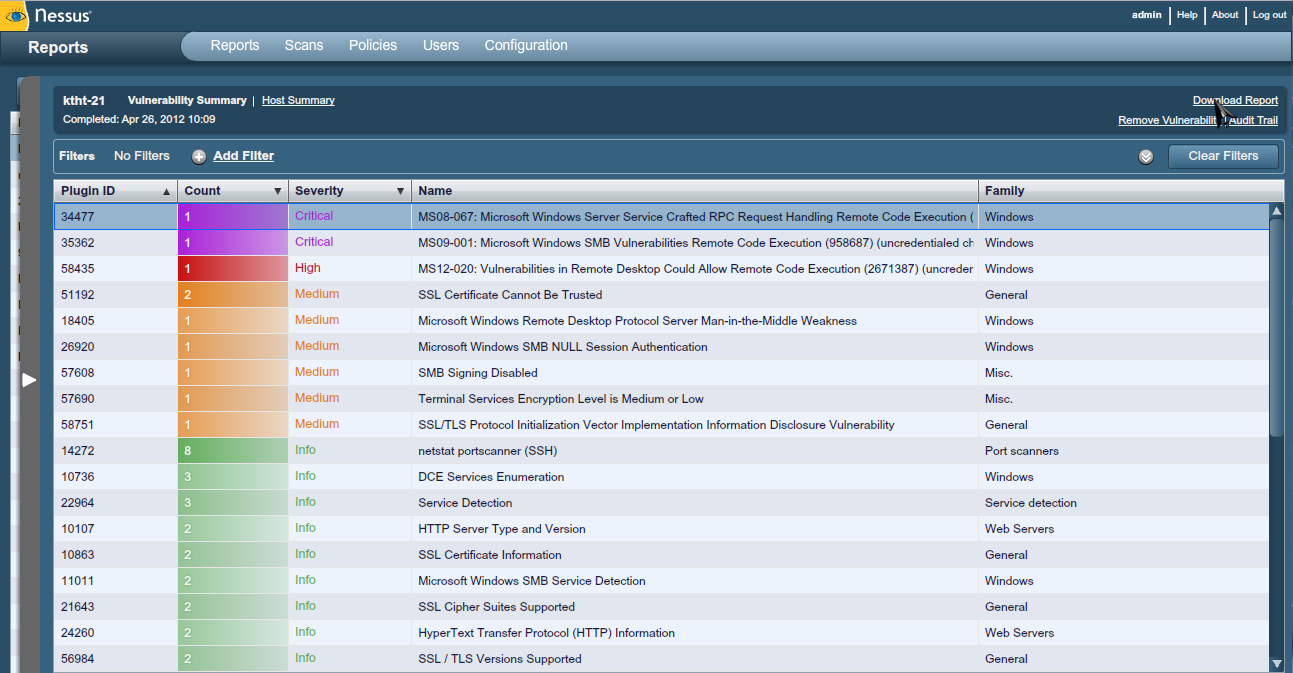


Hình 2.21 Tạo thêm Policy



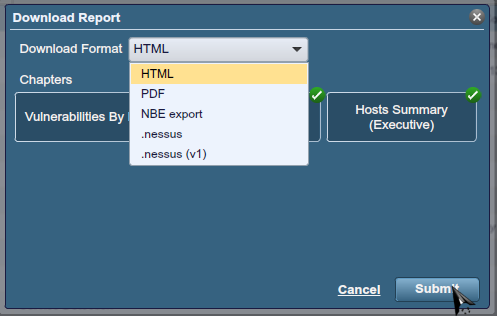
Hình 2.22 Quá trình quét

Sau khi quét xong, để xem kết quả quét ta chuyển qua tab Reports>Browse.



Hình 2.23 Kết quả quét

Ngoài ra, cũng có thể tải báo cáo về in ra dưới dạng file pdf hoặc những liên kết link HTML để dễ quản lý...



Hình 2.24 Tạo báo cáo

### Ưu và nhược điểm

Ưu điểm:

* Nessus giỏi nhất trong việc quét lỗ hổng bảo mật, trên thực tế, nó đưa ra những phát hiện và hơn nữa là những kết quả đánh giá chính xác. Nó không thực hiện kiểm tra thâm nhập hoặc khai thác các lỗ hổng vì nó lo ngại về việc quét các hệ thống / ứng dụng.
* Trên thực tế, Nessus có nhiều cấu hình / chính sách để thực hiện các kiểu quét khác nhau, chẳng hạn như quét theo định hướng PCI-DSS, quét phần mềm độc hại, quét ứng dụng web, quét phát hiện sốc shell xấu.
* Nessus có khả năng phân loại các lỗ hổng thành các danh mục dựa trên rủi ro từ quan trọng đến thậm chí là thông tin mà chúng ta nghĩ đó là một trong những điều tách biệt Nessus với các máy quét lỗ hổng khác.

Nhược điểm:

* Bắt đầu với chi phí của Nessus, mặc dù nó có sẵn miễn phí nhưng nó có một số hạn chế đối với phiên bản miễn phí.
* Nessus có thể cải thiện cách nó hiển thị trạng thái quét trong khi quá trình quét đang diễn ra. Khi quá trình quét được bắt đầu và chạy, đôi khi nó không thể hiển thị chính xác bao nhiêu phần trăm quá trình quét đã hoàn thành, ví dụ: nó hiển thị trực tiếp trạng thái quét từ 0% đến hoàn thành 100% mà không hiển thị phần trăm hoàn thành ở giữa.
* Quá trình quét có thể mất nhiều thời gian để hoàn thành. Phải chia chúng thành nhiều phần nhỏ.

## Wireshark

### Giới thiệu

WireShark là một chương trình phân tích lưu lượng mạng hàng đầu thế giới. Nó là một công cụ thiết yếu cho bất kỳ quản trị viên chuyên nghiệp hay hệ thống bảo mật nào. Phần mềm miễn phí này cho phép phân tích lưu lượng mạng trong thời gian thực (realtime). Bên cạnh đó, nó cũng thường là công cụ tốt nhất để khắc phục các sự cố mạng.

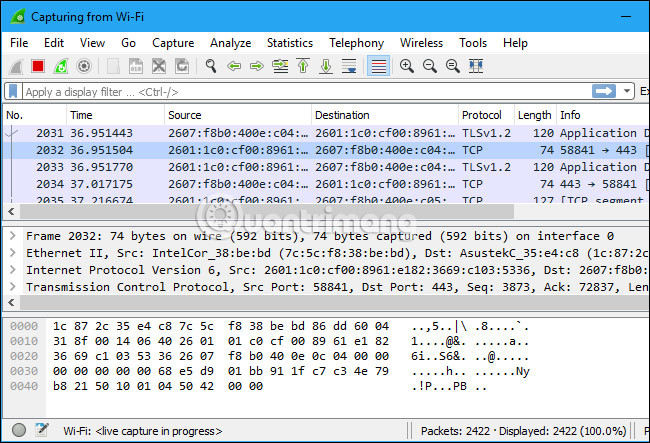
Các vấn đề phổ biến mà WireShark có thể khắc phục gồm: packet bị drop, vấn đề về độ trễ và các hoạt động độc hại. Nó cho phép quan sát cụ thể các lưu lượng mạng, cung cấp công cụ để lọc và đi sâu vào lưu lượng. Sau đó tìm ra nguyên nhân gốc rễ của vấn đề. Quản trị viên thường sử dụng nó để xác định các thiết bị mạng bị lỗi đang drop các packet.

WireShark là một công cụ mạnh mẽ, và nó cũng đòi hỏi kiến thức cơ bản về mạng để sử dụng. Đối với hầu hết các doanh nghiệp hiện đại, cần hiểu khái niệm stack TCP/IP là chưa đủ. Cần phải hiểu cách đọc và giải thích các header, biết cách hoạt động của router, port redirect, DHCP.

### Sử dụng Wireshark

**Capturing Packets:**

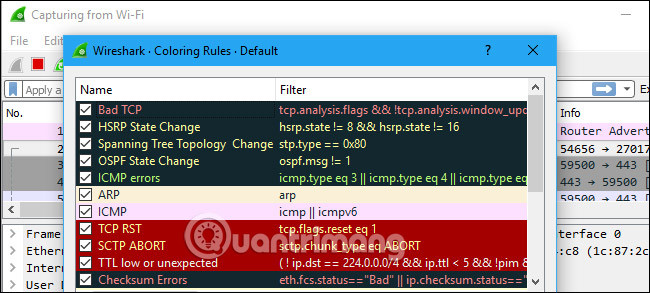
Sau khi cài đặt, các bạn hãy khởi động chương trình và chọn thành phần trong Interface List để bắt đầu hoạt động. Ví dụ, nếu muốn giám sát lưu lượng mạng qua mạng Wireless thì chọn card mạng Wifi tương ứng. Nhấn nút Capture Options để hiển thị thêm nhiều tùy chọn khác.



Hình 2.25 Giám sát thông tin Wi-Fi

**Color Coding:**

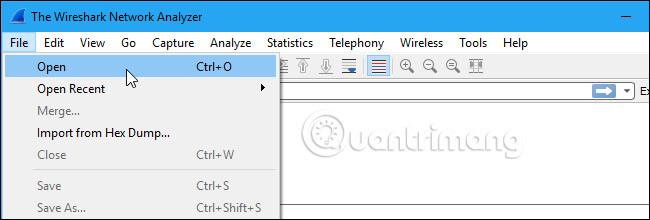
Có thể bạn sẽ thấy các packet được đánh dấu bằng nhiều màu khác nhau. Wireshark sử dụng màu sắc để giúp bạn xác định các loại lưu lượng truy cập trong nháy mắt. Ví dụ, theo mặc định, màu tím nhạt là lưu lượng TCP, màu xanh dương nhạt là lưu lượng UDP và màu đen là các packet có lỗi. Chúng có thể được phân phối theo thứ tự. Để xem chính xác ý nghĩa của các mã màu, hãy nhấp vào View > Coloring Rules. Bạn cũng có thể tùy chỉnh và sửa đổi các quy tắc về màu sắc từ đây, nếu bạn muốn



Hình 2.26 Color Coding

**Sample Captures:**

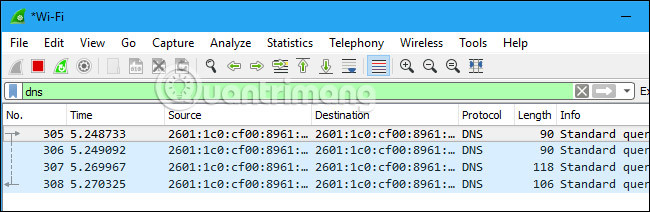
Nếu không có gì thú vị để kiểm tra trên mạng của riêng bạn, bạn có thể kiểm tra wiki của Wireshark (wiki.wireshark.org/SampleCaptures). Wiki chứa một trang các file mẫu mà bạn có thể tải và kiểm tra. Nhấp vào File > Open trong Wireshark và duyệt tìm file đã tải xuống để mở nó. Bạn cũng có thể lưu file của riêng bạn trong Wireshark và mở chúng sau này. Nhấp vào File > Save để lưu các packet của bạn.



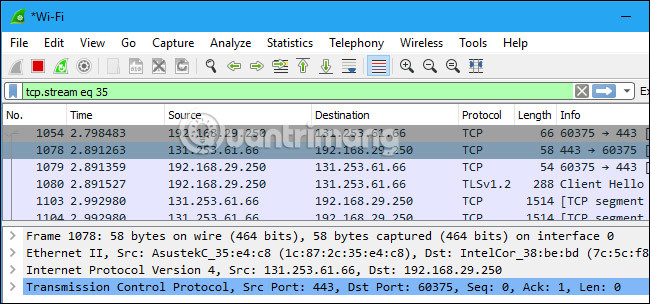
Hình 2.27 Duyệt File trong WireShark

**Filtering Packets:**

Cách cơ bản nhất để áp dụng filter là nhập thông tin vào ô Filter, sau đó nhấn Apply hoặc nhấn Enter. Ví dụ, nếu gõ dns thì chúng ta sẽ chỉ nhìn thấy các gói dữ liệu DNS. Ngay khi nhập từ khóa, Wireshark sẽ tự động hoàn chỉnh chuỗi thông tin này dựa vào gợi ý tương ứng. Hoặc nhấn menu Analyze > Display Filters để tạo filter mới.



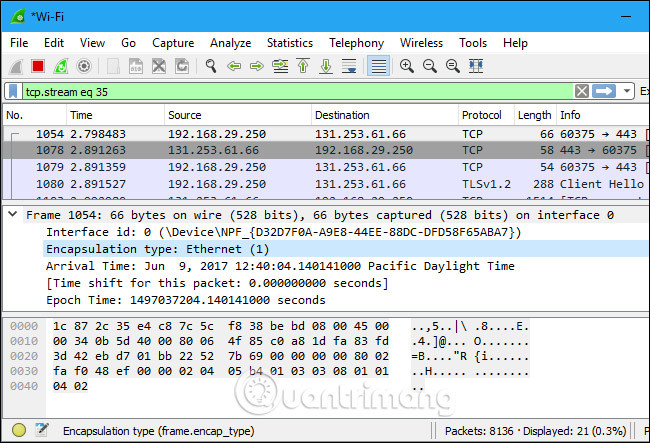
Hình 2.28 Filtering Packets



Hình 2.29 Hiển thị thông tin package

**Inspecting Packets:**

Nhấn và chọn 1 package bất kỳ để kiểm tra các phần thông tin cụ thể hơn.



Hình 2.30 Kiểm tra thông tin package cụ thể

### Một số tình huống có thể xảy với Wireshark

* Mất kết nối TCP: Một trong các vấn đề phổ biến nhất là mất kết nối mạng. Chúng ta sẽ bỏ qua nguyên nhân tại sao kết nối bị mất , chúng ta sẽ nhìn hiện tượng đó ở mức gói tin
* Không thể chạm tới điểm cuối và các mã ICMP: Một trong các công cụ khi kiểm tra kết nối mạng là công cụ ICMP ping. Nếu mục tiêu trả lời lại là bạn đã ping thành công, không sẽ nhận được thông báo không thể kết nối tới máy đích
* Không thể kết nối tới cổng: Một trong các nhiệm vụ thông thường khác là kiểm tra kết nối tới một cổng trên một máy đích. Việc kiểm tra này sẽ cho thấy cổng cần kiểm tra có mở hay không, có sẵn sang nhận các yêu cầu gửi đến hay không. Ví dụ, để kiểm tra dịch vụ FTP có chạy trên một server hay không, mặc định FTP sẽ làm việc qua cổng 21 ở chế độ thông thường. Ta sẽ gửi gói tin ICMP đến cổng 21 của máy đích, nếu máy đích trả lời lại gói ICMP loại o và mã lỗi 2 thì có nghĩa là không thể kết nối tới cổng đó

### Ưu và nhược điểm

**Ưu điểm:**

* Wireshark rất dễ sử dụng trong việc thu thập lưu lượng mạng.
* Mã màu Wireshark cho gói mạng dựa trên loại gói đã được bắt. Điều này làm cho phân tích nhanh hơn nhiều.
* Wireshark có rất nhiều bộ lọc khác nhau có thể được áp dụng trong khi chụp hoặc trong quá trình phân tích để lọc ra các gói không quan tâm khỏi nguồn cấp dữ liệu.
* Bạn có thể tải xuống và sử dụng phiên bản độc lập (không được cài đặt) để chạy trên ổ USB hoặc phương tiện bên ngoài khác trong trường hợp bạn muốn phân tích tại chỗ một hệ thống có khả năng bị xâm phạm.

**Nhược điểm:**

* Wireshark yêu cầu các đặc quyền nâng cao, có thể là xấu hoặc tốt tùy thuộc vào quan điểm của người dùng.
* Có thể khó phân tích cú pháp và lọc dữ liệu nếu không làm việc với Wireshark trong một thời gian. Số lượng dữ liệu có thể quá tải đối với người dùng lần đầu tiên.
* Không thể sửa đổi hoặc thao tác mọi thứ / dữ liệu trên mạng (chỉ ghi lại dữ liệu)

**DANH MỤC TÀI LIỆU THAM KHẢO**

[1] Angela Orebaugh and Becky Pinkard, Nmap in the Enterprise: Your Guide to Network Scanning, 2008

[2] Gordon Fyodor Lyon, Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning, 2008

[3] Nessus 8.0 User Guide, 2021

[4] Laura Chappell and Gerald Combs, Wireshark Network Analysis (Second Edition): The Official Wireshark Certified Network Analyst Study Guide, 2012