

**HỌC VIỆN KỸ THUẬT QUÂN SỰ**

**Bộ môn An Toàn Thông Tin**

**-----🙞🙜🕮🙞🙜-----**

****

**BÁO CÁO BÀI TẬP NHÓM**

**Đề tài: Nmap**

**Môn học: Đảm bảo & an toàn thông tin**

Giáo viên hướng dẫn :Cao Văn Lợi

Sinh viên thực hiện :Kiều Trung Anh

Đặng Thị Hằng

Nguyễn Anh Hiếu

Lớp : CNTT17

**MỤC LỤC**

**[Chương I: Giới thiệu chung 2](#_Toc11613)**

**[1. Mục đích ra đời 2](#_Toc12668)**

**[2. Nmap là gì? 2](#_Toc10941)**

**[Chương II: Tính năng của Nmap 3](#_Toc25809)**

**[1. Tính năng của Nmap 3](#_Toc24833)**

**[2. Nmap Scripting Engine (NSE) và một số lệnh NSE cơ bản 4](#_Toc22872)**

**[a) Nmap Scripting Engine (NSE) là gì? 4](#_Toc9484)**

**[b) Một số lệnh NSE cơ bản: 4](#_Toc29049)**

**[3. Cách thức hoạt động 4](#_Toc21639)**

**[4. Một số ứng dụng và hạn chế 4](#_Toc3470)**

**[a) Ứng dụng của Nmap 4](#_Toc19029)**

**[b) Hạn chế của Nmap 5](#_Toc28953)**

**[Chương III: Môi trường làm việc với Nmap 5](#_Toc26485)**

**[1. Cài Nmap trên Window 5](#_Toc32406)**

**[2. Cài Nmap trên Linux 6](#_Toc23556)**

**[Chương IV: Cách sử dụng 6](#_Toc26363)**

**[1. Một số lệnh scan cơ bản 6](#_Toc31039)**

**[2. Demo 7](#_Toc4649)**

**[a) NSE 7](#_Toc23738)**

**[b) Command Scan 12](#_Toc28623)**

**Chương I: Giới thiệu chung**

1. **Mục đích ra đời**

Trong khi hiện nay có rất nhiều [công cụ giám sát](https://quantrimang.com/bo-cong-cu-giam-sat-mang-toan-dien-83716" \o "Bộ công cụ giám sát mạng toàn diện) tiên tiến đóng vai trò là những trợ thủ đắc lực giúp đỡ [các nhà quản trị mạng](https://quantrimang.com/quan-tri-mang-la-lam-gi-hoc-gi-131657" \o "Làm quản trị mạng là làm gì? Cần học những gì?) trong việc quét cổng và phát hiện các lỗ hổng mạng nhưng Nmap vẫn được coi là một công cụ chuẩn mực. Tại sao lại như vậy?

Các nhà quản trị mạng, quản lý công nghệ thông tin và chuyên gia bảo mật đã, đang, và sẽ phải đối mặt với một trận chiến không bao giờ kết thúc trên chiến trường mang tên an ninh mạng. Họ sẽ phải liên tục kiểm tra rà soát hệ thống mạng của của mình để tìm ra các tác nhân gây hại cũng như những[lỗ hổng bảo mật](https://quantrimang.com/lo-hong-bao-mat-nhung-hieu-biet-can-ban-93098" \o "Lỗ hổng bảo mật - những hiểu biết căn bản) ẩn chứa bên trong. Trong khi hiện nay có không ít các tiện ích giám sát có sẵn hỗ trợ cho các chuyên gia trong việc việc lập bản đồ hệ thống mạng và kiểm soát bảo mật, Nmap là sự lựa chọn số một về tính linh hoạt và khả năng vận hành, và cũng chính những ưu điểm này đã làm cho nó trở thành một công cụ quét cổng và lỗ hổng bảo mật tiêu chuẩn được thừa nhận rộng rãi trên toàn thế giới.

1. **Nmap là gì?**

Nmap được viết trên nền tảng C ++ và được giới thiệu lần đầu tiên cùng với mã nguồn trong tạp chí Phrack vào tháng 9 năm 1997. Sau đó nó được mở rộng với C, Perl và Python. Tác giả Gordon Lyon đã sử dụng bút danh Fyodor Vaskovitch.

Nmap (tên đầy đủ Network Mapper) là một công cụ bảo mật được phát triển bởi Floydor Vaskovitch. Nmap có [mã nguồn mở](https://quantrimang.com/10-dieu-can-biet-ve-phan-mem-ma-nguon-mo-79232" \o "10 điều cần biết về phần mềm mã nguồn mở), miễn phí, dùng để [quét cổng](https://quantrimang.com/huong-dan-quet-cong-mang-160032" \o "Hướng dẫn quét cổng mạng bằng Advanced Port Scanner ) và lỗ hổng bảo mật. Các chuyên gia quản trị mạng sử dụng Nmap để xác định xem thiết bị nào đang chạy trên hệ thống của họ, cũng như tìm kiếm ra các máy chủ có sẵn và các dịch vụ mà các máy chủ này cung cấp, đồng thời dò tìm các cổng mở và phát hiện các nguy cơ về bảo mật.

Nmap có thể được sử dụng để giám sát các máy chủ đơn lẻ cũng như các cụm mạng lớn bao gồm hàng trăm nghìn thiết bị và nhiều mạng con hợp thành.

Mặc dù Nmap đã không ngừng được phát triển, cải tiến qua nhiều năm và cực kỳ linh hoạt, nhưng nền tảng của nó vẫn là một công cụ quét cổng, thu thập thông tin bằng cách gửi các gói dữ liệu thô đến các cổng hệ thống. Sau đó nó lắng nghe và phân tích các phản hồi và xác định xem các cổng đó được mở, đóng hoặc lọc theo một cách nào đó, ví dụ như tường lửa. Các thuật ngữ khác được sử dụng để chỉ hoạt động quét cổng (port scanning) bao gồm dò tìm cổng (discovery) hoặc liệt kê cổng (enumeration).

**Chương II: Tính năng của Nmap**

1. **Tính năng của Nmap**

Các tính năng của Nmap bao gồm:

* Khám phá máy chủ (Host discovery) - Xác định máy chủ trên mạng. Ví dụ: liệt kê các máy chủ đáp ứng yêu cầu TCP hoặc ICMP hoặc có một cổng cụ thể đang mở.
* Quét cổng (Port Scanning) - Liệt kê các cổng đang mở trên máy chủ đích.
* Phát hiện phiên bản (Version detection) - Thẩm vấn các dịch vụ mạng trên thiết bị từ xa để xác định tên ứng dụng và số phiên bản.
* Phát hiện hệ điều hành (OS detection) - Xác định hệ điều hành và đặc điểm phần cứng của thiết bị mạng.
* Tương tác có thể tập lệnh với mục tiêu (Scriptable interaction with the target) - sử dụng Nmap Scripting Engine (NSE) và ngôn ngữ lập trình Lua.
* Nmap có thể cung cấp thêm thông tin về các mục tiêu, bao gồm tên DNS ngược, loại thiết bị và địa chỉ MAC.

1. **Nmap Scripting Engine (NSE) và một số lệnh NSE cơ bản**
2. Nmap Scripting Engine (NSE) là gì?

Nmap Scripting Engine (NSE) là 1 trong những tùy chọn khá lợi hại trong Nmap. Nó cho phép người dùng viết và chia sẻ những đoạn script đơn giản để thực hiện những công việc khác nhau trong lĩnh vực networking một cách tự động. Những đoạn script này có thể sử dụng để phát hiện các lỗ hổng và khai thác các lỗ hổng.

Mỗi một NSE là một kịch bản do người dùng lập trình cho Nmap với các mục đích khác nhau như :tự động hoá các tính năng như quét mạng, tấn công DoS, lấy mật khảu và tên người dùng, thu thập thông tin,… và cả quét lỗ hổng bảo mật.

Để sử dụng NSE với Nmap, thêm --script [tên NSE hoặc đường dẫn đến tệp NSE] đằng sau câu lệnh nmap.

1. Một số lệnh NSE cơ bản:

- Exploit: nmap - -script exploit <target>

Exploit là tên tập lệnh được sử dụng để quét lỗ hổng.

- nmap --script vuln <target>

Vuln là các tập lệnh liên quan đến phát hiện và khai thác lỗ hổng bảo mật.

- Vulscan: nmap -sV --script [đường dẫn] <target>

Vulners là một kịch bản NSE được lập trình lấy dữ liệu về lỗ hổng.

- nmap –sV –p [cổng] --script=ssl-heartbleed.nse <target>

Phát hiện lỗ hổng bảo mật OpenSSL HeartBleed bug .

1. **Cách thức hoạt động**

Nmap sử dụng các IP trên các gói tin theo những cách đặc biệt khác nhau để có thể xác định các host trên một hệ thống mạng. Từ đó xác định xem những services đang chạy trên hệ thống đó, hệ điều hành đang chạy và bộ lọc các gói tin cũng như tường lửa đang sủ dụng là gì.

1. **Một số ứng dụng và hạn chế**
2. Ứng dụng của Nmap

* Kiểm tra tính bảo mật của thiết bị hoặc tường lửa bằng cách xác định các kết nối mạng có thể được thực hiện với hoặc thông qua nó.
* Xác định các cổng mở trên máy chủ đích để chuẩn bị cho việc kiểm tra.
* Kiểm kê mạng, lập bản đồ mạng, bảo trì và quản lý tài sản.
* Kiểm tra tính bảo mật của mạng bằng cách xác định các máy chủ mới.
* Tạo lưu lượng truy cập đến các máy chủ trên mạng, phân tích phản hồi và đo thời gian phản hồi.
* Tìm kiếm và khai thác các lỗ hổng trong mạng.
* Truy vấn DNS và tìm kiếm tên miền phụ.
* Làm cho người quản trị mạng hiểu biết rõ về hệ thống mạng của mình và để biết cách bảo vệ dữ liệu của mình trên mạng.

1. Hạn chế của Nmap

Mặc dù tính năng quét cổng không phải là tính năng bất hợp pháp, ít nhất là theo luật liên bang của Hoa Kỳ, các tính năng của Nmap chắc chắn rất hữu ích đối với các tin tặc có mục đích xấu đang tìm kiếm những lỗ hổng bảo mật để khai thác. Một số ứng dụng nhất định của phần mềm, không được phép truy cập, nếu vẫn phớt lờ, có thể bạn sẽ bị sa thải hoặc gặp rắc rối về pháp lý, ngay cả khi bạn đang thực hiện quét các lỗ hổng không vì những mục đích xấu.

Trong khi một số bản quét Nmap khá nhẹ và không thể tắt cảnh báo, tốt nhất bạn nên tiến các bản quét được cho phép của mình với những cá nhân thích hợp trong tổ chức của bạn. Lưu ý rằng nhiều tùy chọn Nmap, chẳng hạn như OS fingerprinting, yêu cầu quyền truy cập vào các dữ liệu gốc. Do đó, khi nghi ngờ về tính hợp pháp của những những điều bạn muốn làm, đặc biệt là khi bạn làm việc một mình và không có đội ngũ pháp lý của tổ chức để tham khảo ý kiến, hãy nói chuyện với một luật sư có chuyên môn về gian lận và lạm dụng máy tính. Nó là công cụ hữu ích cho hacker.

**Chương III: Môi trường làm việc với Nmap**

Ngoài việc chạy Nmap trên ứng dụng Nmap thì còn có thể chạy trên Command Prompt hoặc Windows PowerShell.

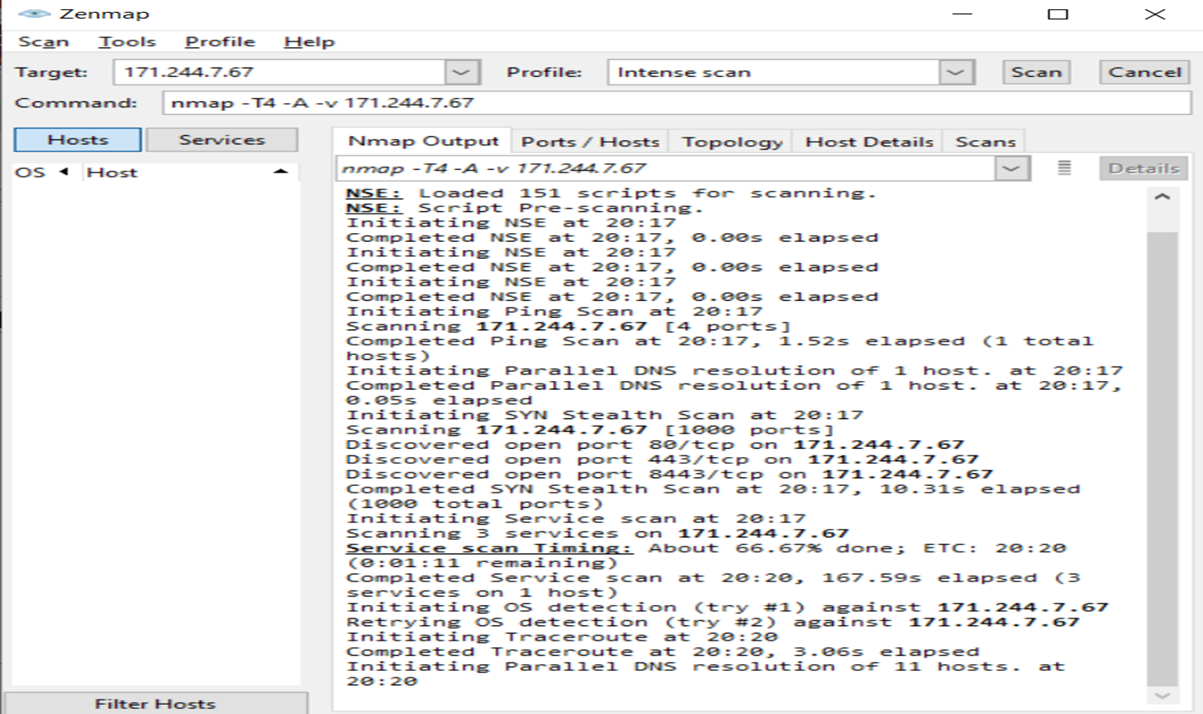
1. **Cài Nmap trên Window**

Bước 1: Truy cập đường link : <https://nmap.org/download.html>

Bước 2: Chọn đúng phiên bản hệ điều hành đang dùng. Đây là cài Nmap trên hệ điều hành Window.

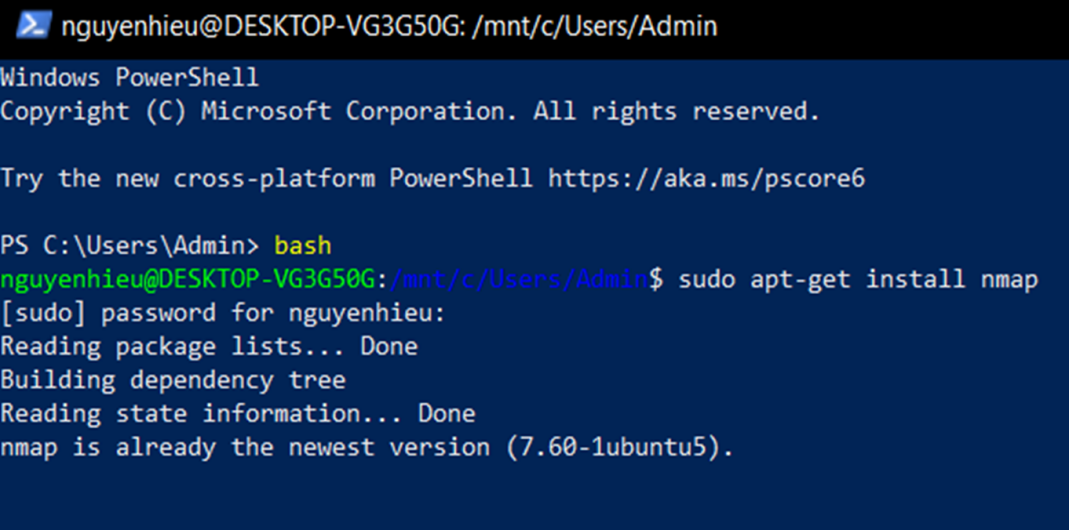


Bước 3: Tải về và cài đặt file exe.



1. **Cài Nmap trên Linux**

Cài đặt Nmap bằng câu lệnh: **sudo apt-get install nmap**



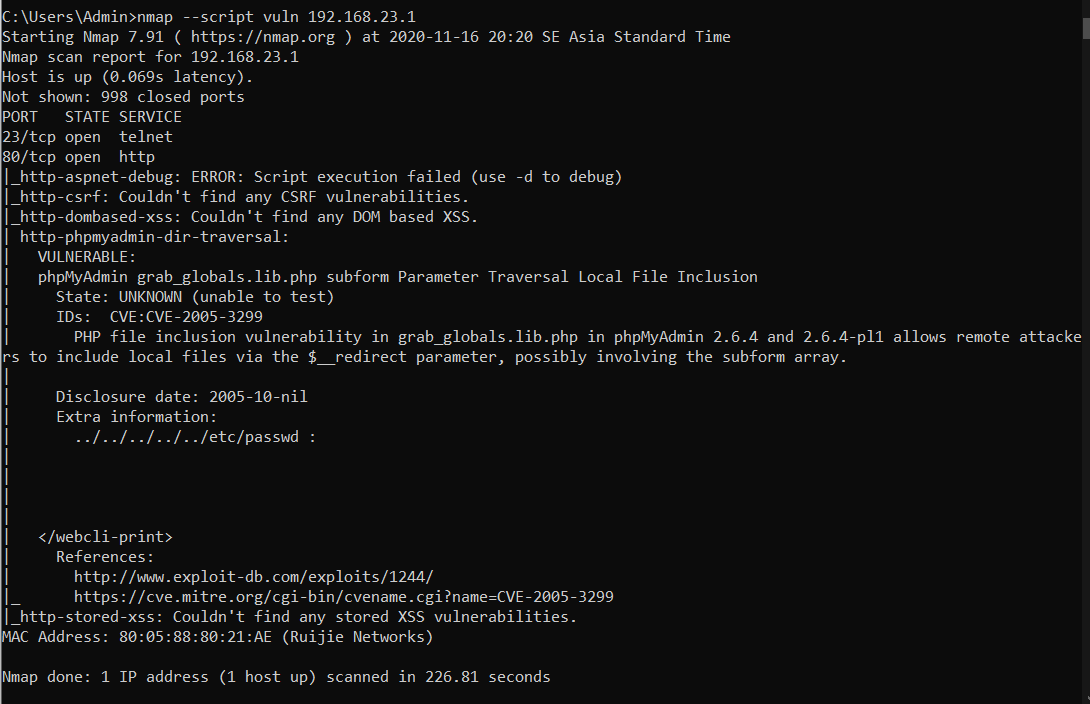
**Chương IV: Cách sử dụng**

1. **Một số lệnh scan cơ bản**

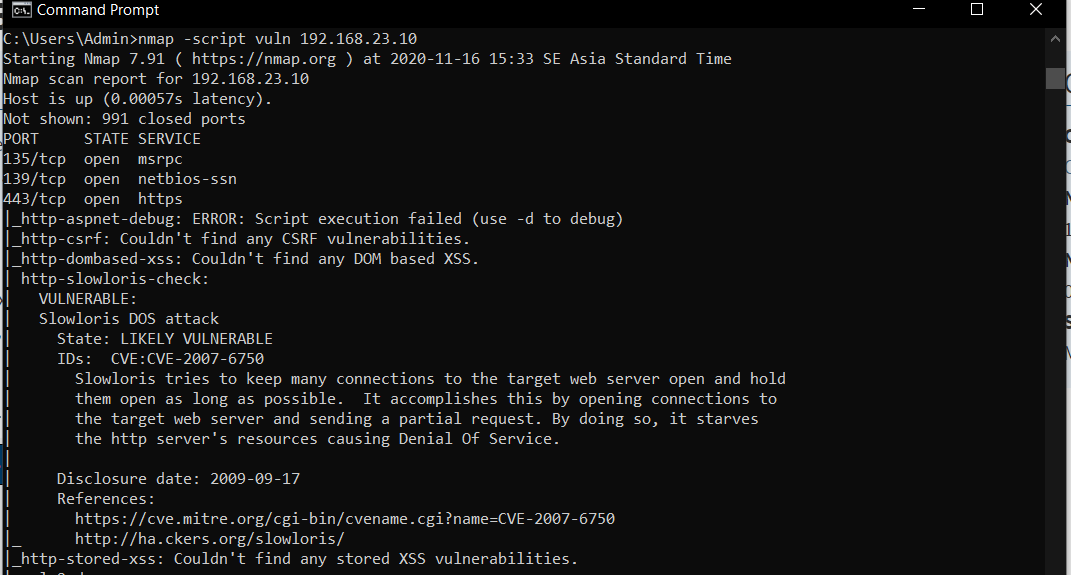
* Kiểm tra xem host còn alive không : #nmap -sn [IP\_của\_mục tiêu] .
* Kiểm tra hệ điều hành của server : #nmap -O [IP\_của\_mục tiêu] .
* Quét một port cụ thể : #nmap -p [số\_cổng] [IP\_của\_mục tiêu] .
* Quét kết nối TCP, Nmap sẽ thực hiện việc quét bắt tay 3 bước : #nmap -sT [IP\_của\_mục tiêu] .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

1. **Demo**
2. NSE

* Vuln Scan : nmap --script vuln <target> : Kiểu quét này có một trong những tập lệnh Nmap mạnh nhất vì nó có thể khai thác các dịch vụ tiềm năng đang chạy trên máy chủ từ xa. Nó có thể khai thác cửa hậu vsftpd, khai thác tải lên tệp HTTP, tải xuống mã nguồn Litespeed, khai thác SMB, cửa hậu UnrealIRCD, CVE 2013-7091, CVE 2017-5689, CVE 2005-3299, v.v.



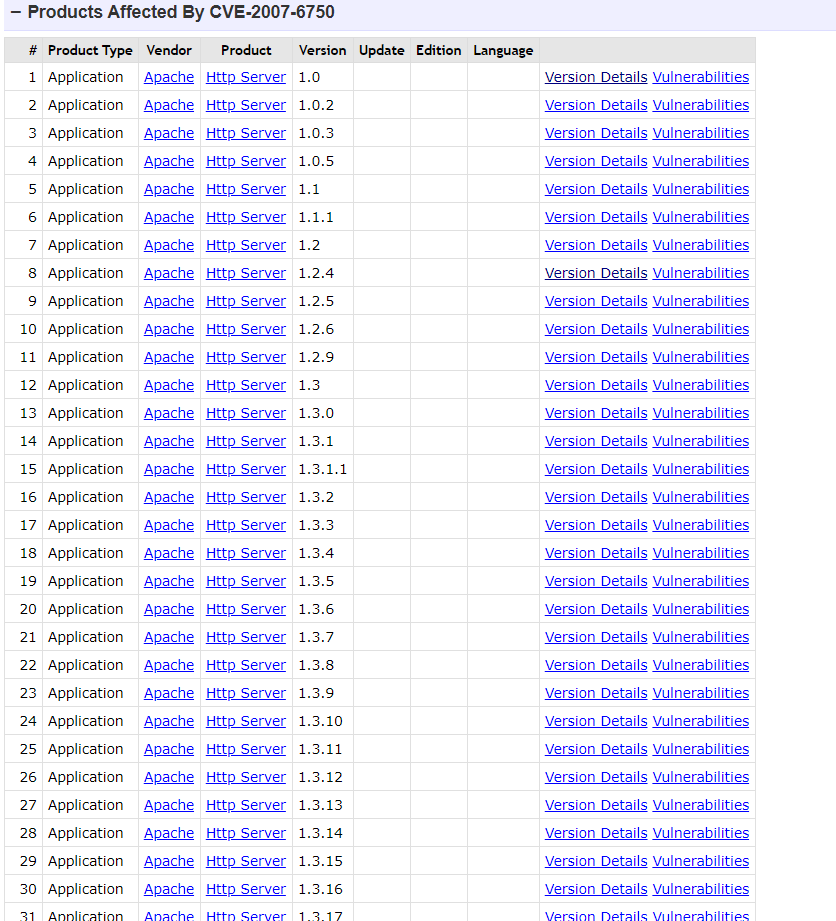
* Phát hiện lỗ hổng bảo mật CVE: CVE 2005-3299 được phát hiện vào 10/2005
* Lỗ hổng bao gồm tệp PHP trong grab\_globals.lib.php trong phpMyAdmin 2.6.4 và 2.6.4-pl1 cho phép những kẻ tấn công từ xa bao gồm các tệp cục bộ thông qua tham số $ \_\_ redirect, có thể liên quan đến mảng biểu mẫu con.
* Mức độ nghiêm trọng: Trung bình



* Phát hiện lỗ hổng bảo mật CVE 2007-6750 được phát hiện vào ngày 17/09/2009

Đây chính là cuộc tán công từ chối dịch vụ “DOS attack”

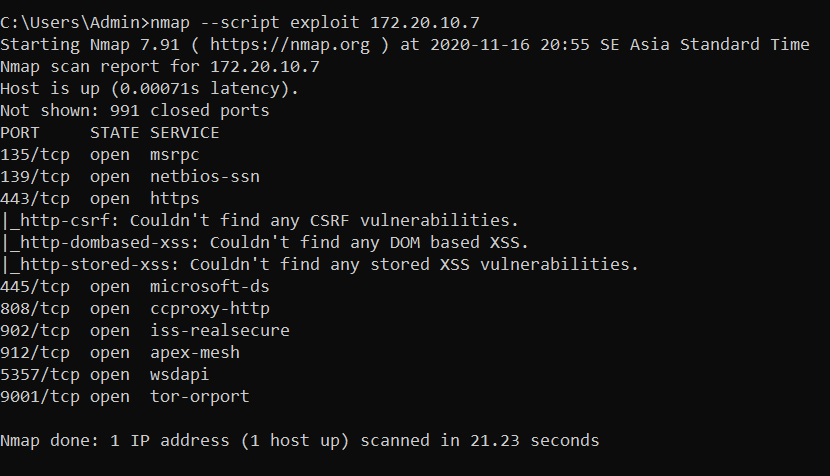
* Apache HTTP Server 1.x và 2.x cho phép kẻ tấn công từ xa gây ra từ chối dịch vụ (daemon ngừng hoạt động) thông qua các yêu cầu HTTP một phần
* Từ năm 2009 tới năm 2012 các cuộc tấn công từ chối dịch vụ xảy ra rất nhiều trên các application, và người ta tổng hợp có đến 117 các ứng dụng bị tấn công và xảy ra trong nhiều năm



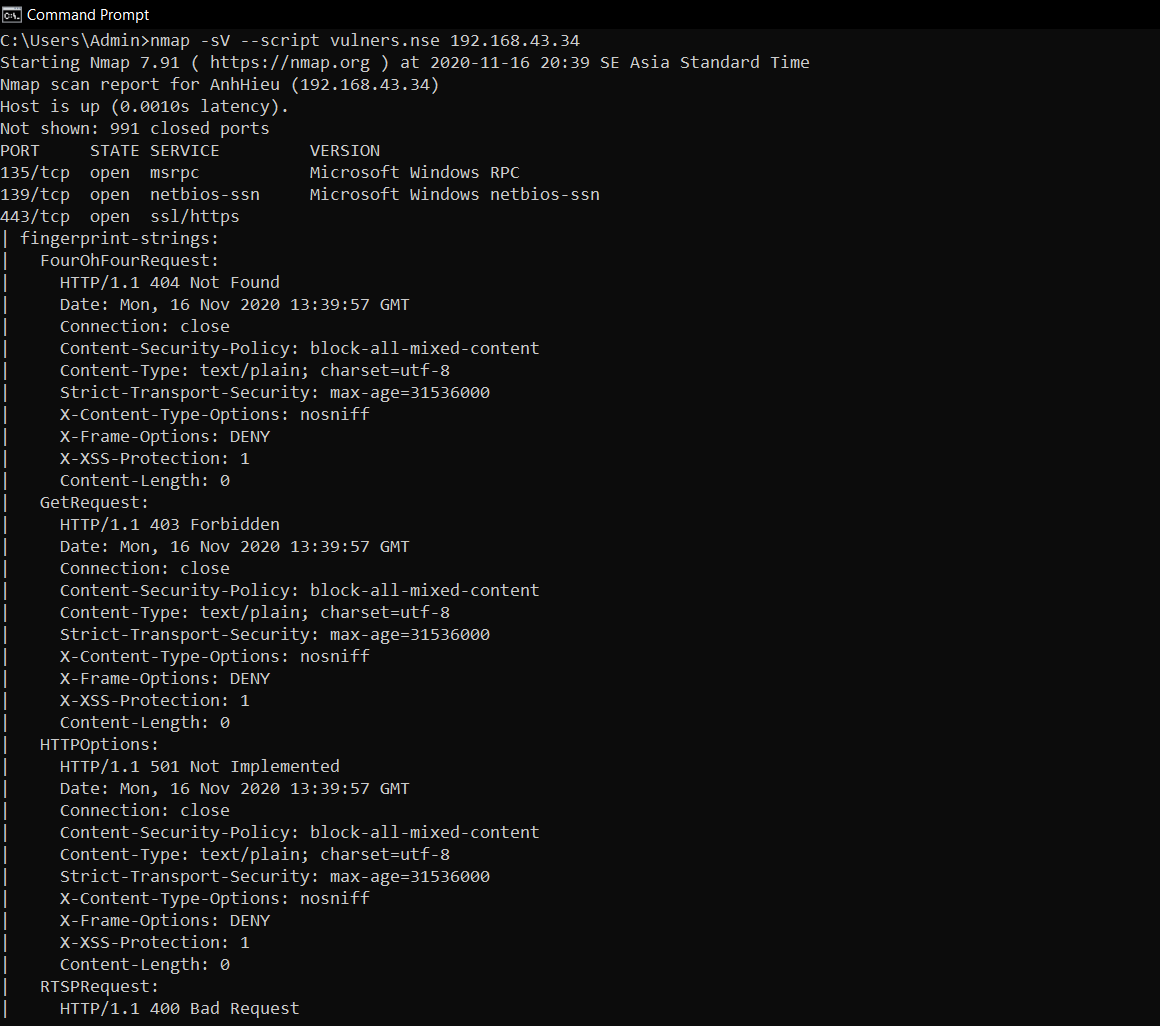
Cách tránh khỏi các cuộc tấn công từ chối dịch vụ ?

Thực sự không có một biện pháp cụ thể nào để tránh trở thành nạn nhân của DoS hay DDoS. Tuy nhiên vài bước với mục đích giảm bớt phần nào kiểu tấn công mà sẽ sử dụng:

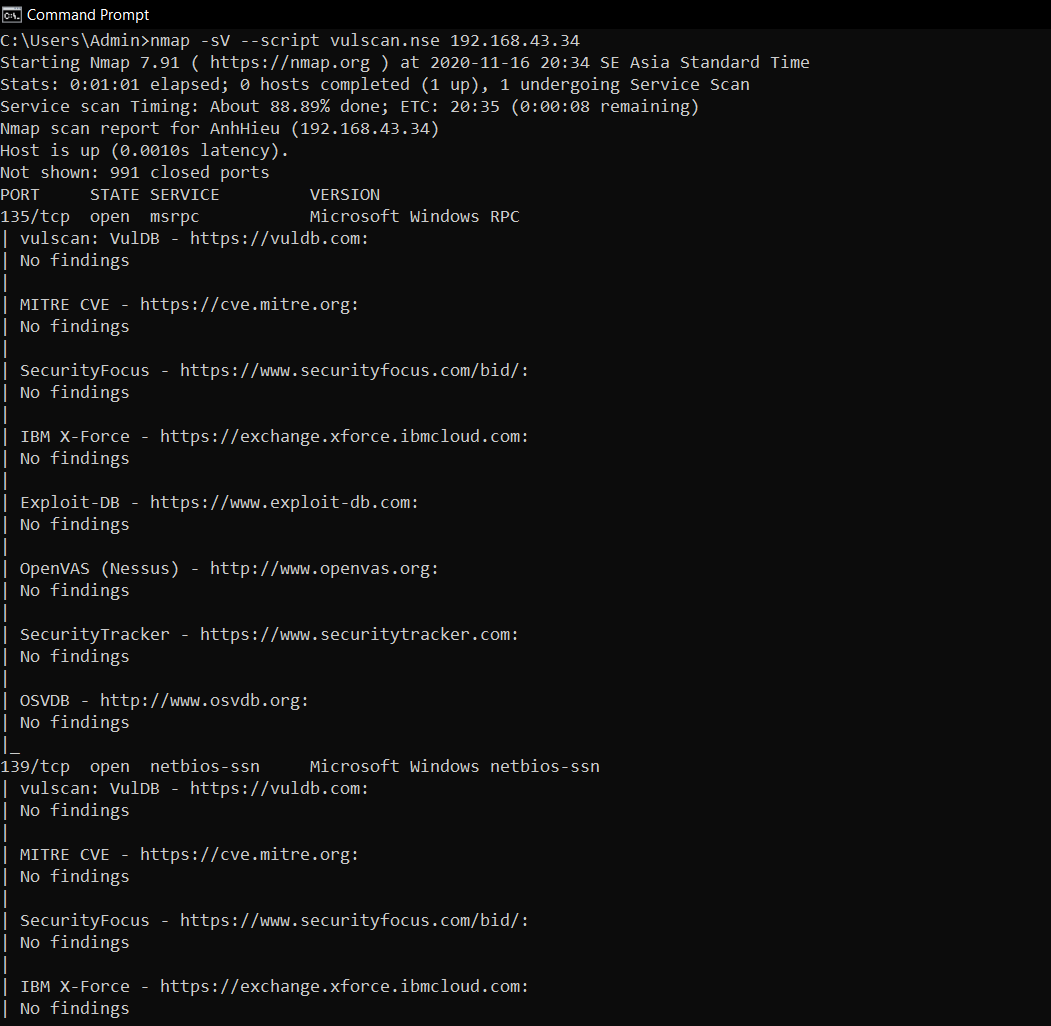
* Cài đặt và duy trì phần mềm chống virus.
* Cài đặt tường lửa và cấu hình nó để giới hạn lưu lượng đến và đi từ máy tính của bạn.
* Làm theo các hướng dẫn thực hành an toàn về phân phối địa chỉ email của bạn.
* Dùng các bộ lọc email để giúp bạn quản lý lưu lượng không mong muốn.
* Exploit Scan : nmap --script exploit <target> : Exploit là tên tập lệnh được sử dụng để quét lỗ hổng. lệnh này cũng khá mạnh gần tương đương như “vuln”.

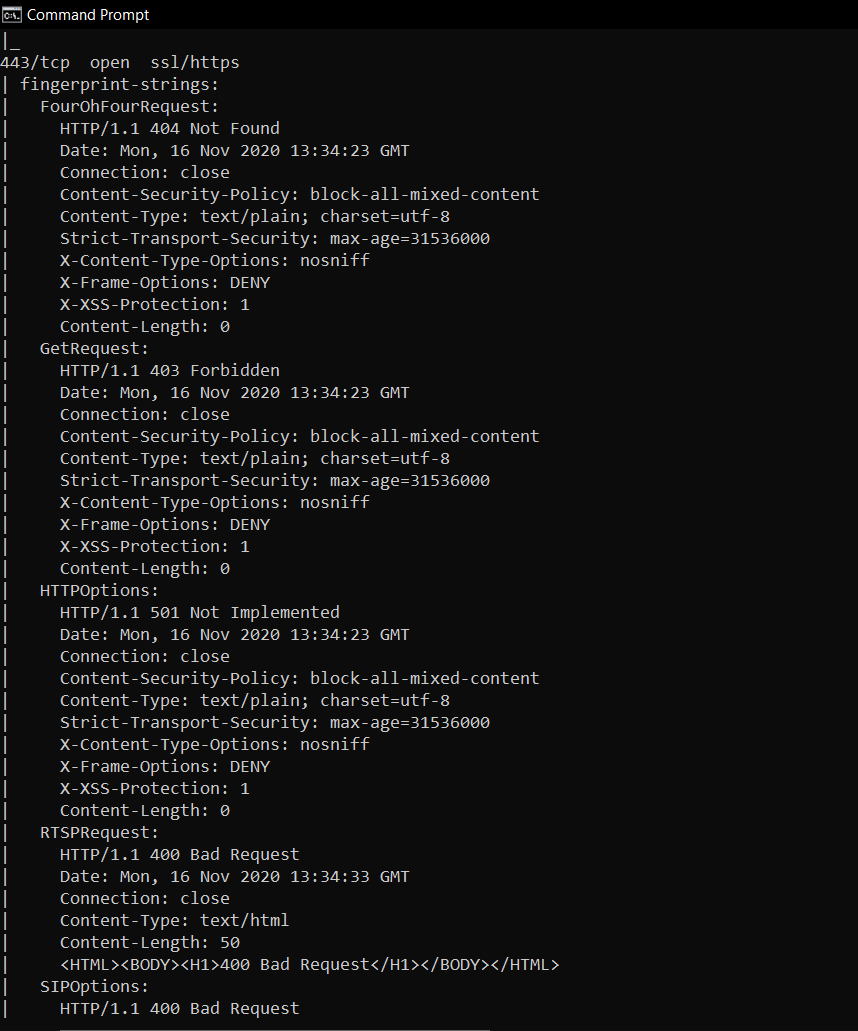


* Vulners scan : nmap -sV –script vulners.nse <target>: Vulners là một kịch bản NSE được lập trình lấy dữ liệu về lỗ hổng bảo mật thông qua APO của trang web Vulners.com. Cần internet để quét. Như với các tập lệnh Nmap khác, cách sử dụng khá giống nhau, ngoại trừ thẻ -sV là bắt buộc. -sV đang quét thông tin phiên bản, điều này rất quan trọng để Vulner hoạt động.



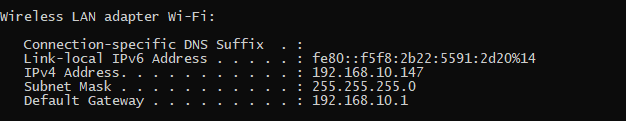
* Vulscan scan : nmap -sV –script vulscan.nse <target>: Vulscan là phần mở rộng NSE của nmap được lập trình bằng ngôn ngữ LUA để khai thác lỗ hổng bảo mật. Vulscan có thể chạy bất kì hệ điều hành nào cài nmap và cũng chạy khi không kết nối internet nhờ dữ liệu có sẵn. Về cơ bản Vulscan khá giống với Vulners nhưng khai thác sâu hơn.





1. Command Scan

***\* Kiểm tra địa chỉ IP mạng local*** : ipconfig



Địa chỉ của máy dùng để scan là: 192.168.10.147.

Subnetmark mạng local là: 255.255.255.255.0.

\* ***Scan TCP connect***: Scan dịch vụ đang chạy trên cổng.

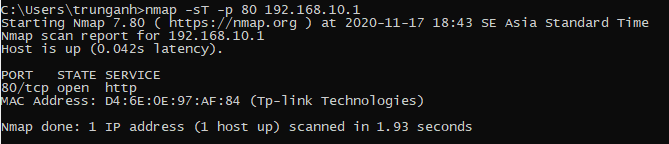
- Nmap sẽ gửi gói tin SYN đến tất cả các cổng của máy mục tiêu(target) nếu mục tiêu là 1 IP cụ thể, còn nếu là mạng local thì đầu tiên Nmap dò xem trong local có những host nào còn sống rồi Nmap gửi gói tin SYN đến tất cả các host đó. Nếu cổng nào sử dụng TCP protocol thì có 2 trường hợp:

+ Cổng mở thì sẽ gửi lại gói tin SYN+ACK . tiếp theo Nmap gửi tiếp gói ACK để hoàn thành kết nối.

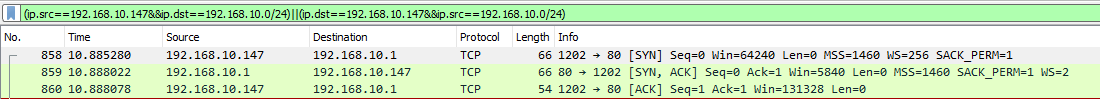
+ Cổng đóng thì gửi lại gói tin RST để yêu cầu thiết lập lại kết nối.

- Lệnh: nmap -sT [option1],… [IP Target]

- Ví dụ: nmap -sT -p 80 192.168.10.1



Phân tích bằng wireshark:



- Trình bày: Attacker gửi gói tin TCP SYN đến cổng 80 IP 192.168.10.1, sau đó 192.168.10.1 gửi lại gói [SYN+ACK] cho phép kết nối, tiếp theo Attacker gửi gói TCP ACK để hoàn thành bắt tay 3 bước.

=> cho kết quả cổng 80 đang mở và đang chạy dịch vụ http.

\* ***Scan TCP ACK***: Scan cách hoạt động của Firewall hay các biện pháp bảo vệ của host mục tiêu.

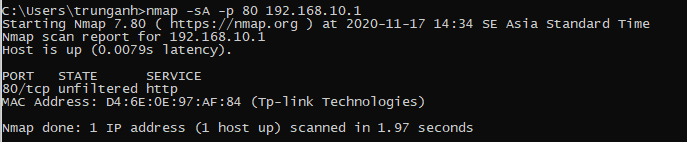
- ACK scan: Không xác định được cổng đóng hay mở. Chỉ dùng trong việc xác định quy tắc làm việc của tườngg lửa. nmap gửi đi gói tin ACK.

+)Nếu nhận được: RST=> gói tin không bị lọc

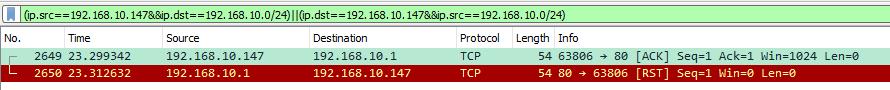
+)Nếu không nhận được phản hồi hoặc nhận được gói ICMP thông báo lỗi thì bị lọc.

- Lệnh: nmap -sA [option1],.. [IP Target]

- Ví dụ: nmap -sA -p 80 192.168.10.1



Phân tích bằng wireshark:



- Trình bày:

+)Tham số: -sA: scan TCP ACK.

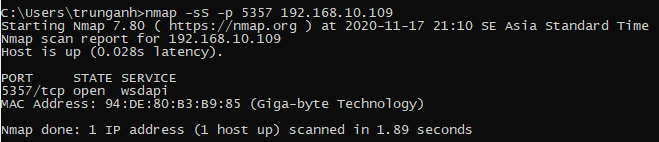
-p 80: scan tại cổng 80.

+)Phân tích: Attacker gửi gói tin ACK tới host có IP Target, ở đây là 192.168.10.1. Nếu host target phản hổi lại bằng gói RST thì gói tin bị lọc, ở đây host Target gửi lại RST nên cổng 80 không bị lọc. Nếu Attacker không nhận lại được phản hồi hoặc nhận được gói tin ICMP thông báo lỗi thì có nghĩa gói tin đã bị lọc.

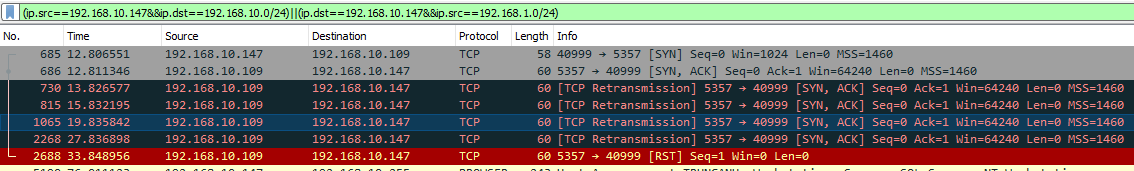
***\* Scan TCP SYN***: Hoạt động giống TCP connect nhưng khác ở chỗ nếu khi cổng mở thì sau khi nhận được gói [SYN+ACK] thì Attacker sẽ không gửi đi ACK nữa mà sẽ không gửi bất cứ thứ gì tới Target và sau khi hết thời gian time out thì Target gửi lại [SYN+ACK], cứ như vậy khi gửi nhiều [ACK+SYN] và không thấy phản hồi thì Target gửi RST để kết thúc.

- Lệnh: nmap -sS [opption1],… [IP Target]

- Ví dụ: nmap -sS -p 5357 192.168.10.109



Phân tích bằng wireshark:



- Trình bày: Atteacker gửi gói SYN đến cổng 5357 của Host 192.168.10.109, Host mở nên nhận được SYN và phản hồi bằng gửi lại gói [SYN+ACK], hết thời gian TIME OUT thì Host gửi lại [SYN+ACK], cứ như vậy khi vẫn không nhận được phản hồi thì Host sẽ gưi gói RST để kết thúc.

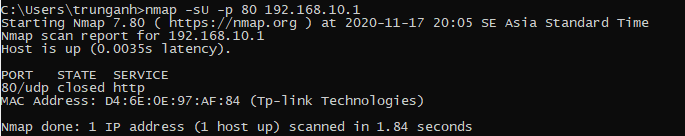
=>Cổng 5357 trên Host có IP 192.168.10.109 mở.

***\* Scan UDP***: Scan kiểm tra xem cổng đó đóng hay mở hoặc bị lọc.

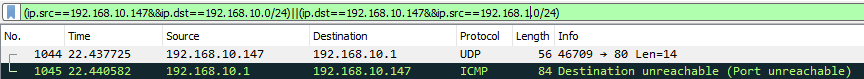
- Scan UDP: Nmap gửi đến các cổng gói UDP, nếu nhận lại được phản hồi ICMP thông báo lỗi có nghĩa cổng đóng. Nếu không nhận được phản hồi thì cổng mở hoặc đã bị lọc.

- Lệnh:nmap -sU [port] [IP Target]

- Ví dụ: nmap -sU -p 80 192.168.10.1



Phân tích bằng wireshark:

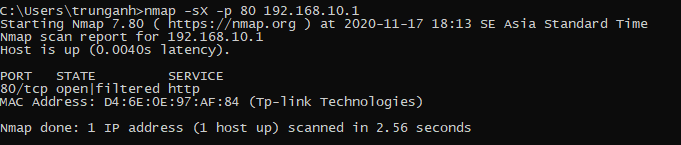


- Trình bày: Attacker gửi gói tin UDP cổng 80 của Host có IP 192.168.10.1, sau đó host phản hổi lại bằng gói tin ICMP => kết luận là cổng 80 đóng đối với giao thức UDP.

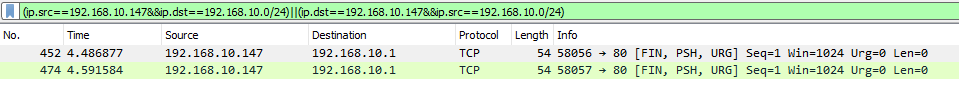
***\* Scan Xmas***: Scan kiểm tra xem cổng đóng hay mở

- Lệnh: nmap -sX -p [port] [IP target]

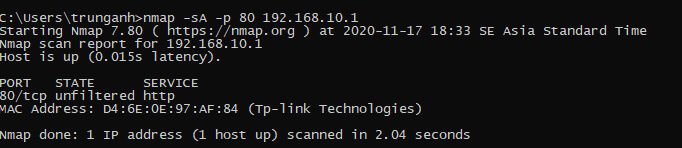
- Ví dụ:nmap -sX -p 80 192.168.10.1



Phân tích bằng wireshark:



- Trình bày: Attecker gửi gói tin TCP có Flag là 101001 (tương ứng với các cờ URG,PSH,FIN được thiết lập) đến cho Host có IP 192.168.10.1, sau đó không nhận lại được phản hồi nên kết luận là bị lọc (STATE=open|filtered) hoặc cổng đó mở(nếu nhận được phản hồi bằng gói tin RST thì cổng đó bị đóng). Để biết chính xác hơn chúng ta sử dụng thêm ACK scan:

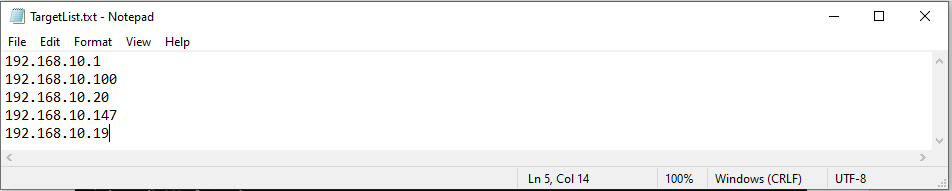


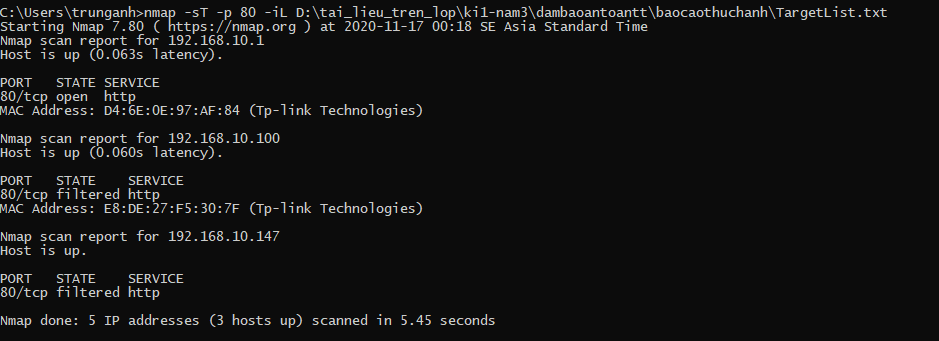
=>Ta thấy STATE=unfiltered nên kết luận cổng 80 trên host 192.168.10.1 là đang mở.

***\* Scan các địa chỉ IP có trong danh sách file TXT***:

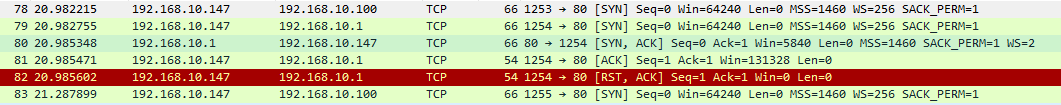
- Lệnh: nmap [option1],.. -iL [đường dẫn đến file chứa danh sách địa chỉ ip]

- Ví dụ: nmap -sT -p 912 -iL D:\tai\_lieu\_tren\_lop\ki1-nam3\dambaoantoantt\baocaothuchanh\TargetList.txt





Phân tích bằng wireshark:



- Trình bày:

+) Tham số: -sT: TCP scan

-p 80: scan cổng 80

-iL D:\tai\_lieu\_tren\_lop\ki1-nam3\dambaoantoantt\baocaothuchanh\TargetList.txt: scan các IP trong file D:\tai\_lieu\_tren\_lop\ki1-nam3\dambaoantoantt\baocaothuchanh\TargetList.txt

+) Nội dung: ban đầu nmap ping đến từng địa chỉ IP trong file TXT xem host nào còn sống, tiếp theo gửi gói tin TCP [SYN] đến những host còn sống, ở đây là host có IP 192.168.10.1 và Ip 192.168.10.100

192168.10.1: Host có IP 192.168.10.1 gửi lại gói [SYN+ACK] cho phép kết nối, tiếp theo Nmap gửi gói ACK để hoàn thành kết nối.

192.168.10.100: Sau khi Nmap gửi SYN đến host có IP 192.168.10.100 không nhận lại được phản hồi thì Nmap gửi lại gói SYN 1 lần nữa. Khi này vẫn không nhận lại được phản hồi nên Nmap cho rằng gói SYN đã bị lọc(có thể bị lọc do tường lửa hoặc các biện pháp bảo vệ khác).

***\* Scan IDLE(ZOOMBIE):*** Scan bằng cách gửi các gói tin thông qua IP của zombie đến IP của target, làm cho khi bị phát hiện thì IP nguồn trên các gói tin là IP của zombie. Mục đích là che giấu IP của người Scan thực sự.

- Lệnh: nmap -sI [IP zombie] [option] [IP target]

- Ví dụ: nmap -Pn -sI 172.20.10.8 -p80 172.20.10.3(-Pn là tham số để không ping sang IP khác nhằm che dấu IP thật).

- Cách hoạt động: đầu tiên phải xác định được Zombie còn sống

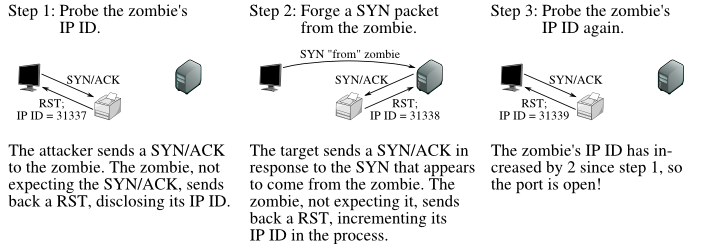
+Nmap gửi gói SYN+ACk đến IP zombie, Zombie nhận đc SYN+ACk sẽ gửi lại RST(vì SYN+ACK là gói không xác định đối với Zombie), Nmap gửi nhiều lần như vậy rồi xem trương IPID mỗi lần có tăng lên 1 không, nếu tăng đều mỗi lần lên 1 thì Zombie có thể đang không giao tiếp với địa chỉ khác và tăng tính chính xác của Scan IDLE.

+Nmap nhận đc RST từ Zombie sẽ lấy đc thông tin trường ID-IP và ghi nhớ giá trị ID-IP(lần cuối nhận RST).

+Nmap tạo gói tin SYN giả với IP là IP của Zombie tới cho mục tiêu.

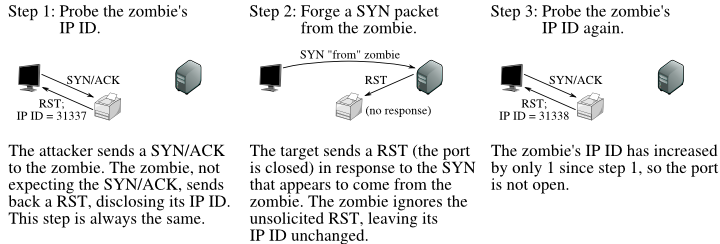
+Mục tiêu nhận đc SYN thì xảy ra 3 trường hợp:

.Open port: Target gửi gói SYN+ACK đến cho zombie, Zombie nhận được gói không xác định nên sẽ gửi lại RST => ID IP của zombie tăng lên 1.Tiếp theo Nmap gửi SYN+ACK đến Zombie, zombie nhận đc gói không xác định nên gửi lại RST, Nmap phân tích ID IP vừa nhận được rồi so sánh với ID IP đã lưu lại trước đó và thấy ID IP tăng lên 2 nên Nmap xác định được cổng đó của Target mở.

**Trường hợp cổng mở. ****

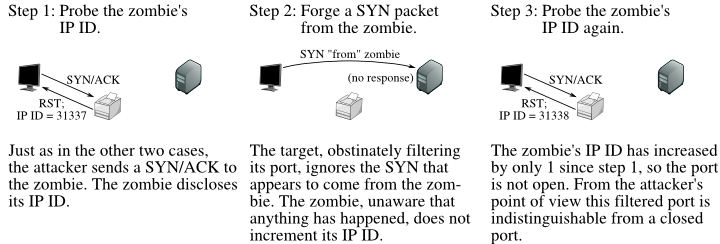
.Close port:Target sẽ gửi lại gói tin RST cho Zombie. Tiếp theo Nmap gửi lại SYN+ACK cho Zombie. Zombie gửi RST cho Nmap. Nmap phân tích thấy ID IP của Zombie tăng lên 1 nên Nmap xác định cổng đó của Target là đóng hoặc gói tin đã bị lọc do các bộ bảo vệ trên thiết bị đó ví dụ như Firewall.

**Trường hợp cổng đóng.**



.Filter port:Target sẽ k phản hồi gói tin đó vì đã bị lọc. Tiếp theo Nmap gửi lại SYN+ACK cho Zombie. Zombie gửi RST cho Nmap. Nmap phân tích thấy ID IP của Zombie tăng lên 1 nên Nmap xác định cổng đó của Target là đóng hoặc gói tin đã bị lọc.

**Trường hợp cổng bị lọc.**

******

\*NOTE: phương pháp này chỉ hiệu quả tương đối bởi vì trong quá trình Nmap thực hiện thì Zombie cũng có thể đang tương tác với một nguồn khác nên ID IP được xác định là không tuyệt đối.

