Nmap Advanced Port Scans

1. **Introduction**

We will cover the following types of port scans:

* Null Scan
* FIN Scan
* Xmas Scan
* Maimon Scan
* ACK Scan
* Window Scan
* Custom Scan

Moreover, we will cover the following:

* Spoofing IP
* Spoofing MAC
* Decoy Scan
* Fragmented Packets
* Idle/Zombie Scan

We will discuss options and techniques to evade firewalls and IDS systems. We also cover options to get more verbose details from Nmap.

1. **TCP Null Scan, FIN Scan, Xmas Scan**

Let’s start with the following three types of scans:

* Null Scan
* FIN Scan
* Xmas Scan

Cả 3 cách quét này đều yêu cầu quyền root

Cả 3 kiểu quét này có thể qua mặt tường lửa không trạng thái, nếu là tường lửa có trạng

thái thì vô dụng

Tường lửa không trạng thái là:

Tường lửa không trạng thái (stateless firewall) là một loại tường lửa xử lý các gói dữ liệu độc lập mà không theo dõi trạng thái của các kết nối mạng. Điều này có nghĩa là tường lửa không trạng thái sẽ phân tích và quyết định chặn hoặc cho phép từng gói dữ liệu dựa trên các quy tắc định trước, mà không cần biết liệu gói đó có liên quan đến một kết nối hoặc phiên trước đó hay không.

1. **Null Scan (-sN)**

* Quét null không đặt bất kỳ cờ nào; tất cả sáu bit cờ đều được đặt thành 0.
* Cách hoạt đông:

+ Việc không có phản hồi trong quét null chỉ ra rằng cổng đang mở hoặc tường lửa đang chặn gói 🡪 không thể chắc chắn 100%

A red line with black text

Description automatically generated

+ Trường hợp cổng đóng:

A red and black lines with black text

Description automatically generated

1. **FIN Scan (-sF)**

* The FIN scan sends a TCP packet with the FIN flag set. You can choose this scan type using the -sF option.
* Cách hoạt động thì tương tự Null Scan, cụ thể:

+ open | filtered

+ =

A red line with black text

Description automatically generated

+ Closed

A diagram of a diagram

Description automatically generated with medium confidence

1. **Xmas Scan (-sX)**

* The Xmas scan gets its name after Christmas tree lights. An Xmas scan sets the FIN, PSH, and URG flags simultaneously. You can select Xmas scan with the option -sX.
* Cách hoạt động tương tự, cụ thể:

+ open | filtered:

A red line with black text

Description automatically generated

+ closed:

A diagram of a diagram

Description automatically generated with medium confidence

**Answer the questions below**

In a null scan, how many flags are set to 1?

0

In a FIN scan, how many flags are set to 1?

1

In a Xmas scan, how many flags are set to 1?

3

Start the VM and load the AttackBox. Once both are ready, open the terminal on the AttackBox and use nmap to launch a FIN scan against the target VM. How many ports appear as open|filtered?

7

A screen shot of a computer

Description automatically generated

Repeat your scan launching a null scan against the target VM. How many ports appear as open|filtered?

7

A computer screen shot of a computer

Description automatically generated

1. **TCP Maimon Scan (-sX)**

* Uriel Maimon lần đầu tiên mô tả quá trình quét này vào năm 1996. Trong quá trình quét này, các bit FIN và ACK được đặt = 1.
* Cách hoạt động:

+ Sau khi gửi, máy mục tiêu sẽ phản hồi gói RST 🡪 dự đoán là cổng mở

+ Tuy nhiên, một số hệ thống bắt nguồn từ BSD sẽ loại bỏ gói nếu đó là một cổng mở làm lộ các cổng mở. Quá trình quét này sẽ không hiệu quả với hầu hết các mục tiêu gặp phải trong các mạng hiện đại

A diagram of a diagram

Description automatically generated with medium confidence

**Answer the questions below**

In the Maimon scan, how many flags are set?

2

1. TCP ACK, Window, and Custom Scan
2. TCP ACK Scan (-sA)

* Quét ACK sẽ gửi một gói tin TCP với cờ ACK được đặt. Sử dụng tùy -sAchọn để chọn quét này
* Kiểu quét này bạn sẽ không biết cổng đóng hay mở, tuy nhiên nó sẽ cho biết bạn sẽ biết được cổng nào không bị tường lửa chặn. Nói cách khác, kiểu quét này phù hợp hơn để khám phá các bộ quy tắc và cấu hình tường lửa.

A diagram of a diagram

Description automatically generated with medium confidence

1. Window Scan (-sW)

Cách hoạt động khá giống TCP ACK Scan

A diagram of a diagram

Description automatically generated with medium confidence

1. Custom Scan (--scanflags CUSTOM\_FLAGS)

* Nếu bạn muốn thử nghiệm với một tổ hợp cờ TCP mới ngoài các loại quét TCP tích hợp , bạn có thể thực hiện bằng cách sử dụng --scanflags. Ví dụ, nếu bạn muốn đặt SYN, RST và FIN cùng lúc, bạn có thể thực hiện bằng cách sử dụng --scanflags RSTSYNFIN
* Cách hoạt động tương tự

A close-up of a flag

Description automatically generated

Answer the questions below

In TCP Window scan, how many flags are set?

1

You decided to experiment with a custom TCP scan that has the reset flag set. What would you add after --scanflags?

RST

The VM received an update to its firewall ruleset. A new port is now allowed by the firewall. After you make sure that you have terminated the VM from Task 2, start the VM for this task. Launch the AttackBox if you haven't done that already. Once both are ready, open the terminal on the AttackBox and use Nmap to launch an ACK scan against the target VM. How many ports appear unfiltered?

4

What is the new port number that appeared?

443

Is there any service behind the newly discovered port number? (Y/N)

N

A computer screen shot of a computer

Description automatically generated

1. Spoofing and Decoys (Lừa đảo và mồi nhử)

Trong một số thiết lập mạng, bạn sẽ có thể quét hệ thống mục tiêu bằng cách sử dụng địa chỉ IP giả mạo và thậm chí là địa chỉ MAC giả mạo. Việc quét như vậy chỉ có lợi trong trường hợp bạn có thể đảm bảo nắm bắt được phản hồi. Nếu bạn cố gắng quét mục tiêu từ một mạng ngẫu nhiên nào đó bằng cách sử dụng địa chỉ IP giả mạo, khả năng là bạn sẽ không có bất kỳ phản hồi nào được định tuyến đến bạn và kết quả quét có thể không đáng tin cậy.

Hình sau đây cho thấy kẻ tấn công khởi chạy lệnh **nmap -S SPOOFED\_IP 10.10.165.155**. Do đó, Nmap sẽ tạo tất cả các gói tin bằng cách sử dụng địa chỉ IP nguồn được cung cấp **SPOOFED\_IP**. Máy đích sẽ phản hồi các gói tin đến bằng cách gửi phản hồi đến địa chỉ IP đích **SPOOFED\_IP**. Để quá trình quét này hoạt động và đưa ra kết quả chính xác, kẻ tấn công cần theo dõi lưu lượng mạng để phân tích các phản hồi.

A diagram of a computer network

Description automatically generated

Tóm lại, quét bằng địa chỉ IP giả mạo có ba bước:

1. Kẻ tấn công gửi một gói tin có địa chỉ IP nguồn giả mạo đến máy mục tiêu.
2. Máy mục tiêu trả lời địa chỉ IP giả mạo là đích đến.
3. Kẻ tấn công sẽ thu thập các phản hồi để tìm ra các cổng mở.

Nhìn chung, bạn mong đợi chỉ định giao diện mạng bằng cách sử dụng **-e**và để vô hiệu hóa quét ping một cách rõ ràng **-Pn**. Do đó, thay vì **nmap -S SPOOFED\_IP 10.10.165.155**, bạn sẽ cần phải phát hành **nmap -e NET\_INTERFACE -Pn -S SPOOFED\_IP 10.10.165.155**để cho Nmap biết rõ ràng giao diện mạng nào để sử dụng và không mong đợi nhận được phản hồi ping. Cần nhắc lại rằng quá trình quét này sẽ vô ích nếu hệ thống của kẻ tấn công không thể theo dõi mạng để biết phản hồi.

Khi bạn ở cùng mạng con với máy mục tiêu, bạn cũng có thể giả mạo địa chỉ MAC của mình. Bạn có thể chỉ định địa chỉ MAC nguồn bằng cách sử dụng **--spoof-mac SPOOFED\_MAC**. Việc giả mạo địa chỉ này chỉ khả thi nếu kẻ tấn công và máy mục tiêu ở cùng mạng Ethernet (802.3) hoặc cùng WiFi (802.11).

Việc giả mạo chỉ có hiệu quả trong một số ít trường hợp khi đáp ứng được một số điều kiện nhất định. Do đó, kẻ tấn công có thể dùng đến mồi nhử để khiến việc xác định vị trí trở nên khó khăn hơn. Khái niệm này rất đơn giản, hãy làm cho quá trình quét có vẻ như đến từ nhiều địa chỉ IP để địa chỉ IP của kẻ tấn công sẽ bị mất trong số đó. Như chúng ta thấy trong hình bên dưới, quá trình quét máy mục tiêu sẽ có vẻ như đến từ 3 nguồn khác nhau và do đó, các phản hồi cũng sẽ đến mồi nhử.

A computer network diagram with a few computers

Description automatically generated with medium confidence

Bạn có thể khởi chạy quét mồi nhử bằng cách chỉ định một địa chỉ IP cụ thể hoặc ngẫu nhiên sau **-D**. Ví dụ, **nmap -D 10.10.0.1,10.10.0.2,ME 10.10.165.155**sẽ làm cho quá trình quét 10.10.165.155 xuất hiện như đến từ các địa chỉ IP 10.10.0.1, 10.10.0.2, và sau đó **ME**để chỉ ra rằng địa chỉ IP của bạn sẽ xuất hiện theo thứ tự thứ ba. Một lệnh ví dụ khác sẽ là **nmap -D 10.10.0.1,10.10.0.2,RND,RND,ME 10.10.165.155**, trong đó địa chỉ IP nguồn thứ ba và thứ tư được chỉ định ngẫu nhiên, trong khi nguồn thứ năm sẽ là địa chỉ IP của kẻ tấn công. Nói cách khác, mỗi lần bạn thực hiện lệnh sau, bạn sẽ mong đợi hai địa chỉ IP ngẫu nhiên mới là nguồn mồi nhử thứ ba và thứ tư.

**Answer the questions below**

What do you need to add to the command sudo nmap 10.10.73.117 to make the scan appear as if coming from the source IP address 10.10.10.11 instead of your IP address?

-S 10.10.10.11

What do you need to add to the command sudo nmap 10.10.73.117 to make the scan appear as if coming from the source IP addresses 10.10.20.21 and 10.10.20.28 in addition to your IP address?

-D 10.10.20.21,10.10.20.28,ME

1. **Fragmented Packets**

- Phân mảnh gói tin sẽ giúp gói tin ít bị phát hiển bởi Firewall/IDS

-f: gói tin sẽ phân mảnh theo 8 byte

-ff: gói tin sẽ phân mảnh theo 16 byte

-mtu: thay đổi giá trị mặc định; tuy nhiên, bạn nên luôn chọn bội số của 8.

- Tăng kích thước các gói tin để làm cho chúng trông vô hại: sử dụng tùy chọn

--data-length NUM, trong đó num chỉ định số byte bạn muốn thêm vào các gói tin của mình

**Answer the questions below**

If the TCP segment has a size of 64, and -ff option is being used, how many IP fragments will you get?

4

1. **Idle/Zombie Scan**

Việc giả mạo địa chỉ IP nguồn có thể là một cách tiếp cận tuyệt vời để quét lén lút. Tuy nhiên, việc giả mạo chỉ có hiệu quả trong các thiết lập mạng cụ thể. Nó yêu cầu bạn phải ở vị trí có thể theo dõi lưu lượng truy cập. Xem xét những hạn chế này, việc giả mạo địa chỉ IP của bạn có thể không có nhiều tác dụng; tuy nhiên, chúng ta có thể nâng cấp nó bằng cách quét Zombie.

Quét Idle, hay quét zombie, yêu cầu một hệ thống Zombie được kết nối với mạng mà bạn có thể giao tiếp. Trên thực tế, Nmap sẽ làm cho mỗi lần dò xuất hiện như thể đến từ máy chủ Zombie (zombie), sau đó nó sẽ kiểm tra các chỉ báo xem máy chủ Zombie (zombie) có nhận được bất kỳ phản hồi nào cho lần dò giả mạo hay không. Điều này được thực hiện bằng cách kiểm tra giá trị nhận dạng IP (IP ID) trong tiêu đề IP. Bạn có thể chạy quét Zombie bằng cách sử dụng **nmap -sI ZOMBIE\_IP 10.10.165.155**, trong đó **ZOMBIE\_IP** là địa chỉ IP của máy chủ Zombie (zombie).

Quét Zombie (zombie) yêu cầu thực hiện ba bước sau để phát hiện xem cổng có mở hay không:

1. Kích hoạt máy chủ Zombie để phản hồi để bạn có thể ghi lại ID IP hiện tại trên máy chủ Zombie.
2. Gửi một gói SYN đến một cổng TCP trên mục tiêu. Gói này phải được giả mạo để xuất hiện như thể nó đến từ địa chỉ IP của máy chủ Zombie (zombie).
3. Kích hoạt lại máy Zombie để phản hồi để bạn có thể so sánh ID IP mới với ID đã nhận trước đó.

Hãy giải thích bằng hình ảnh. Trong hình bên dưới, chúng ta có hệ thống kẻ tấn công đang thăm dò một máy Zombie, một máy in đa chức năng. Bằng cách gửi SYN/ACK, nó phản hồi bằng một gói RST chứa IP ID mới tăng của nó.

A computer screen shot of a printer

Description automatically generated

Kẻ tấn công sẽ gửi một gói SYN đến cổng TCP mà chúng muốn kiểm tra trên máy mục tiêu ở bước tiếp theo. Tuy nhiên, gói này sẽ sử dụng địa chỉ IP của máy chủ Zombie (zombie) làm nguồn. Có ba kịch bản sẽ xảy ra. Trong kịch bản đầu tiên, được hiển thị trong hình bên dưới, cổng TCP bị đóng; do đó, máy mục tiêu phản hồi máy chủ Zombie bằng một gói RST. Máy chủ Zombie không phản hồi; do đó, ID IP của nó không được tăng lên.

A computer screen shot of a printer

Description automatically generated

Trong kịch bản thứ hai, như được hiển thị bên dưới, cổng TCP mở, do đó máy đích phản hồi bằng SYN/ACK tới máy chủ Zombie (zombie). Máy chủ Zombie phản hồi gói tin bất ngờ này bằng gói tin RST, do đó tăng IP ID của nó.

A computer screen shot of a printer

Description automatically generated

Trong trường hợp thứ ba, máy đích không phản hồi gì cả do các quy tắc tường lửa. Việc không phản hồi này sẽ dẫn đến kết quả tương tự như với cổng đóng; máy chủ Zombie sẽ không tăng ID IP.

Đối với bước cuối cùng, kẻ tấn công gửi một SYN/ACK khác đến máy chủ Zombie. Máy chủ Zombie phản hồi bằng một gói RST, tăng IP ID thêm một lần nữa. Kẻ tấn công cần so sánh IP ID của gói RST nhận được ở bước đầu tiên với IP ID của gói RST nhận được ở bước thứ ba này. Nếu chênh lệch là 1, điều đó có nghĩa là cổng trên máy mục tiêu đã bị đóng hoặc bị lọc. Tuy nhiên, nếu chênh lệch là 2, điều đó có nghĩa là cổng trên máy mục tiêu đã mở.

Cần nhắc lại rằng quá trình quét này được gọi là quét Zombie vì việc chọn máy chủ Zombie là điều cần thiết để quét chính xác. Nếu "máy chủ Zombie" đang bận, tất cả các ID IP được trả về sẽ vô dụng.

**Answer the questions below**

You discovered a rarely-used network printer with the IP address 10.10.5.5, and you decide to use it as a zombie in your idle scan. What argument should you add to your Nmap command?

-sI 10.10.5.5

1. **Getting More Details**

|  |  |
| --- | --- |
| **--reason** | giải thích cách Nmap đưa ra kết luận của mình |
| **-v** | dài dòng |
| **-vv** | rất dài dòng |
| **-d** | gỡ lỗi |
| -dd | thêm chi tiết để gỡ lỗi  **Answer the questions below**  Launch the AttackBox if you haven't done so already. After you make sure that you have terminated the VM from Task 4, start the VM for this task. Wait for it to load completely, then open the terminal on the AttackBox and use Nmap with nmap -sS -F --reason 10.10.73.117 to scan the VM. What is the reason provided for the stated port(s) being open?  syn-ack |

A computer screen shot of a computer program

Description automatically generated

1. **Summary**

This room covered the following types of scans.

| **Port Scan Type** | **Example Command** |
| --- | --- |
| TCP Null Scan | **sudo nmap -sN 10.10.165.155** |
| TCP FIN Scan | **sudo nmap -sF 10.10.165.155** |
| TCP Xmas Scan | **sudo nmap -sX 10.10.165.155** |
| TCP Maimon Scan | **sudo nmap -sM 10.10.165.155** |
| TCP ACK Scan | **sudo nmap -sA 10.10.165.155** |
| TCP Window Scan | **sudo nmap -sW 10.10.165.155** |
| Custom TCP Scan | **sudo nmap --scanflags URGACKPSHRSTSYNFIN 10.10.165.155** |
| Spoofed Source IP | **sudo nmap -S SPOOFED\_IP 10.10.165.155** |
| Spoofed MAC Address | **--spoof-mac SPOOFED\_MAC** |
| Decoy Scan | **nmap -D DECOY\_IP,ME 10.10.165.155** |
| Idle (Zombie) Scan | **sudo nmap -sI ZOMBIE\_IP 10.10.165.155** |
| Fragment IP data into 8 bytes | **-f** |
| Fragment IP data into 16 bytes | **-ff** |

| **Option** | **Purpose** |
| --- | --- |
| **--source-port PORT\_NUM** | specify source port number |
| **--data-length NUM** | append random data to reach given length |

Các loại quét này dựa vào việc thiết lập cờ TCP theo những cách không mong muốn để nhắc các cổng trả lời. Quét Null, FIN và Xmas kích hoạt phản hồi từ các cổng đóng, trong khi quét Maimon, ACK và Window kích hoạt phản hồi từ các cổng mở và đóng.

| **Lựa chọn** | **Mục đích** |
| --- | --- |
| **--reason** | giải thích cách Nmap đưa ra kết luận của mình |
| **-v** | dài dòng |
| **-vv** | rất dài dòng |
| **-d** | gỡ lỗi |
| **-dd** | thêm chi tiết để gỡ lỗi |