**Nmap Live Host Discovery**

1. **Introduction**

Chúng tôi trình bày các cách tiếp cận khác nhau mà Nmap sử dụng để khám phá máy chủ trực tiếp. Cụ thể, chúng tôi đề cập đến:

* Quét ARP : Quét này sử dụng các yêu cầu ARP để khám phá các máy chủ trực tiếp (Giao thức phân giải địa chỉ)
* Quét ICMP: Quét này sử dụng các yêu cầu ICMP để xác định máy chủ trực tiếp
* Quét ping TCP/ UDP : Quét này gửi các gói tin đến các cổng TCP và cổng UDP để xác định máy chủ đang hoạt động.

Quét Nmap thường trải qua các bước được hiển thị trong hình bên dưới, mặc dù nhiều bước là tùy chọn và phụ thuộc vào các đối số dòng lệnh mà bạn cung cấp.

A screen shot of a computer

Description automatically generated

1. **Subnetworks**

Phân đoạn mạng là một nhóm máy tính được kết nối bằng một phương tiện chia sẻ. Ví dụ, phương tiện có thể là bộ chuyển mạch Ethernet hoặc điểm truy cập WiFi. Trong mạng IP, mạng con thường tương đương với một hoặc nhiều phân đoạn mạng được kết nối với nhau và được cấu hình để sử dụng cùng một bộ định tuyến. Phân đoạn mạng đề cập đến kết nối vật lý, trong khi mạng con đề cập đến kết nối logic.

Trong sơ đồ mạng sau, chúng ta có bốn phân đoạn mạng hoặc mạng con. Nói chung, hệ thống của bạn sẽ được kết nối với một trong những phân đoạn mạng/mạng con này. Một mạng con, hoặc đơn giản là một mạng con, có phạm vi địa chỉ IP riêng và được kết nối với một mạng rộng hơn thông qua một bộ định tuyến. Có thể có một tường lửa thực thi các chính sách bảo mật tùy thuộc vào từng mạng.

Nếu bạn ở Mạng A, bạn chỉ có thể sử dụng ARP để khám phá các thiết bị trong mạng con đó (10.1.100.0/24). Giả sử bạn được kết nối với một mạng con khác với mạng con của hệ thống đích. Trong trường hợp đó, tất cả các gói tin do máy quét của bạn tạo ra sẽ được định tuyến qua default gateway (router) để đến các hệ thống trên mạng con khác; tuy nhiên, các truy vấn ARP sẽ không được định tuyến và do đó không thể vượt qua bộ định tuyến mạng con. ARP is a link-layer protocol, and ARP packets are bound to their subnet.

A computer network diagram with icons

Description automatically generated

**Answer the questions below**

Send a packet with the following:

From computer1

To computer1 (to indicate it is broadcast)

Packet Type: “ARP Request”

Data: computer6 (because we are asking for computer6 MAC address using ARP Request)

How many devices can see the ARP Request?

4

Did computer6 receive the ARP Request? (Y/N)

N

Send a packet with the following:

From computer4

To computer4 (to indicate it is broadcast)

Packet Type: “ARP Request”

Data: computer6 (because we are asking for computer6 MAC address using ARP Request)

How many devices can see the ARP Request?

4

Did computer6 reply to the ARP Request? (Y/N)

Y

1. **Enumerating targets**

Chúng tôi đã đề cập đến các kỹ thuật khác nhau mà chúng ta có thể sử dụng để quét trong Nhiệm vụ 1. Trước khi giải thích chi tiết từng kỹ thuật và áp dụng vào mục tiêu trực tiếp, chúng ta cần chỉ định các mục tiêu mà chúng ta muốn quét. Nói chung, bạn có thể cung cấp danh sách, phạm vi hoặc mạng con. Ví dụ về chỉ định mục tiêu là:

* danh sách: MACHINE\_IP scanme.nmap.org example.comsẽ quét 3 địa chỉ IP.
* phạm vi: 10.11.12.15-20sẽ quét 6 địa chỉ IP: 10.11.12.15, 10.11.12.16,… và 10.11.12.20.
* mạng con: MACHINE\_IP/30sẽ quét 4 địa chỉ IP.

Bạn cũng có thể cung cấp một tệp làm dữ liệu đầu vào cho danh sách mục tiêu của mình: nmap -iL list\_of\_hosts.txt.

Nếu bạn muốn kiểm tra danh sách các máy chủ mà Nmap sẽ quét, bạn có thể sử dụng: nmap -sL TARGETS. Tùy chọn này sẽ cung cấp cho bạn danh sách chi tiết các máy chủ mà Nmap sẽ quét mà không cần quét chúng; tuy nhiên, Nmap sẽ thử phân giải DNS ngược trên tất cả các mục tiêu để lấy tên của chúng. Tên có thể tiết lộ nhiều thông tin khác nhau cho pentester. (Nếu bạn không muốn Nmap đến máy chủ DNS , bạn có thể thêm -n.)

**Answer the questions below**

What is the first IP address Nmap would scan if you provided 10.10.12.13/29 as your target?

10.10.12.8

How many IP addresses will Nmap scan if you provide the following range 10.10.0-255.101-125?

6400

1. **Discovery live hosts**

Let’s revisit the TCP/IP layers shown in the figure next. We will leverage the protocols to discover the live hosts. Starting from bottom to top, we can use:

* ARP from Link Layer
* ICMP from Network Layer
* TCP from Transport Layer
* UDP from Transport Layer

A diagram of a network layer

Description automatically generated

Trước khi thảo luận về cách máy quét có thể sử dụng từng giao thức một cách chi tiết, chúng ta sẽ xem xét sơ qua bốn giao thức này. ARP có một mục đích: gửi một khung đến địa chỉ phát trên phân đoạn mạng và yêu cầu máy tính có địa chỉ IP cụ thể phản hồi bằng cách cung cấp địa chỉ MAC (phần cứng) của nó.

ICMP có nhiều loại . ICMP ping sử dụng Loại 8 (Echo) và Loại 0 (Echo Reply).

Nếu bạn muốn ping một hệ thống trên cùng một mạng con, truy vấn ARP phải được thực hiện trước lệnh ICMP Echo.

Mặc dù TCP và UDP là các lớp vận chuyển, nhưng đối với mục đích quét mạng, máy quét có thể gửi một gói tin được thiết kế đặc biệt đến các cổng TCP hoặc UDP thông thường để kiểm tra xem mục tiêu có phản hồi hay không. Phương pháp này hiệu quả, đặc biệt là khi ICMP Echo bị chặn.

**Answer the questions below**

Send a packet with the following:

From computer1

To computer3

Packet Type: “Ping Request”

What is the type of packet that computer1 sent before the ping?

ARP Request

What is the type of packet that computer1 received before being able to send the ping?

ARP Response

How many computers responded to the ping request?

1

Send a packet with the following:

From computer2

To computer5

Packet Type: “Ping Request”

What is the name of the first device that responded to the first ARP Request?

router

What is the name of the first device that responded to the second ARP Request?

computer5

Send another Ping Request. Did it require new ARP Requests? (Y/N)

N

1. **Nmap host discovery using ARP**

Nmap sẽ áp dụng các phương pháp sau để khám phá máy chủ trực tiếp:

* Khi người dùng có đặc quyền cố gắng quét mục tiêu trên mạng cục bộ (Ethernet), Nmap sử dụng yêu cầu ARP. Người dùng có đặc quyền là root hoặc người dùng thuộc về sudoers và có thể chạy sudo.
* Khi người dùng có đặc quyền cố gắng quét các mục tiêu bên ngoài mạng cục bộ, Nmap sẽ sử dụng các yêu cầu phản hồi ICMP, TCP ACK (Xác nhận) tới cổng 80, TCP SYN (Đồng bộ hóa) tới cổng 443 và yêu cầu dấu thời gian ICMP.
* Khi người dùng không có đặc quyền cố gắng quét các mục tiêu bên ngoài mạng cục bộ, Nmap sẽ sử dụng bắt tay TCP 3 chiều bằng cách gửi các gói SYN đến các cổng 80 và 443.

Quét ARP chỉ khả thi nếu bạn ở cùng mạng con với hệ thống đích.

A diagram of a system

Description automatically generated with medium confidence

Nếu bạn muốn sử dụng Nmap để khám phá máy chủ trực tuyến mà không cần quét cổng hệ thống trực tiếp, bạn có thể phát hành nmap -sn TARGETS (như mục III)

Nếu bạn chỉ muốn Nmap thực hiện quét ARP mà không quét cổng, bạn có thể sử dụng nmap -PR -sn TARGETS, trong đó -PR cho biết bạn chỉ muốn quét ARP. Chúng tôi chạy nmap -PR -sn MACHINE\_IP/24

Answer the questions below

We will be sending broadcast ARP Requests packets with the following options:

From computer1

To computer1 (to indicate it is broadcast)

Packet Type: “ARP Request”

Data: try all the possible eight devices (other than computer1) in the network: computer2, computer3, computer4, computer5, computer6, switch1, switch2, and router.

How many devices are you able to discover using ARP requests?

3

1. **Nmap host discovery using ICMP**

Chúng ta có thể ping mọi địa chỉ IP trên mạng đích và xem ai sẽ phản hồi yêu ping cầu (ICMP Type 8/Echo) của chúng ta bằng phản hồi ping (ICMP Type 0). Đơn giản phải không? Mặc dù đây là cách tiếp cận trực tiếp nhất, nhưng không phải lúc nào cũng đáng tin cậy. Nhiều tường lửa chặn ICMP echo; các phiên bản mới của MS Windows được cấu hình với tường lửa máy chủ chặn các yêu cầu ICMP echo theo mặc định. Hãy nhớ rằng truy vấn ARP sẽ đi trước yêu cầu ICMP nếu mục tiêu của bạn nằm trên cùng một mạng con.

Vì các yêu cầu ICMP echo có xu hướng bị chặn, bạn cũng có thể cân nhắc các yêu cầu ICMP Timestamp hoặc ICMP Address Mask để biết hệ thống có trực tuyến hay không. Nmap sử dụng yêu cầu timestamp (ICMP Type 13) và kiểm tra xem nó có nhận được phản hồi Timestamp (ICMP Type 14) hay không. Thêm -PP tùy chọn này sẽ cho Nmap biết sử dụng các yêu cầu ICMP timestamp. Như thể hiện trong hình bên dưới, bạn mong đợi các máy chủ trực tiếp phản hồi.

A close-up of a red cable

Description automatically generated

Để sử dụng yêu cầu phản hồi ICMP để khám phá máy chủ trực tiếp, hãy thêm tùy chọn -PE. (Nhớ thêm -sn nếu bạn không muốn theo sau là quét cổng.) Như thể hiện trong hình sau, quét phản hồi ICMP hoạt động bằng cách gửi yêu cầu phản hồi ICMP và mong đợi mục tiêu trả lời bằng phản hồi ICMP nếu mục tiêu trực tuyến.

Adding the -PP option tells Nmap to use ICMP timestamp requests

Adding the -PM option required to tell Nmap to use ICMP Address Mask to discover live hosts

Adding -PE option required to tell Nmap to use ICMP Echo to discover live hosts

**Answer the questions below**

What is the option required to tell Nmap to use ICMP Timestamp to discover live hosts?

-PP

What is the option required to tell Nmap to use ICMP Address Mask to discover live hosts?

-PM

What is the option required to tell Nmap to use ICMP Echo to discover live hosts?

-PE

1. **Nmap Host Discovery Using TCP and UDP**

**TCP SYN Ping (-PS)**

Chúng ta có thể gửi một gói tin với cờ SYN (Synchronize) được đặt thành cổng TCP , mặc định là 80 và chờ phản hồi. Một cổng mở sẽ trả lời bằng SYN/ACK (Acknowledge); một cổng đóng sẽ dẫn đến RST (Reset). Trong trường hợp này, chúng ta chỉ kiểm tra xem chúng ta có nhận được phản hồi nào không để suy ra máy chủ có hoạt động hay không. Trạng thái cụ thể của cổng không quan trọng ở đây. Hình bên dưới là lời nhắc nhở về cách bắt tay 3 chiều TCP thường hoạt động.

A three red wires with white text

Description automatically generated

A three red wires with white text

Description automatically generated

**TCP ACK Ping (-PA)**

A red lines with black text

Description automatically generated

**UDP** Ping (-PU)

A diagram of a product

Description automatically generated

**Masscan**

Một lưu ý nhỏ, Masscan sử dụng cách tiếp cận tương tự để khám phá các hệ thống khả dụng. Tuy nhiên, để hoàn thành quá trình quét mạng nhanh chóng, Masscan khá quyết liệt với tốc độ các gói tin mà nó tạo ra. Cú pháp khá giống nhau: -pcó thể theo sau là số cổng, danh sách hoặc phạm vi. Hãy xem xét các ví dụ sau:

* masscan MACHINE\_IP/24 -p443
* masscan MACHINE\_IP/24 -p80,443
* masscan MACHINE\_IP/24 -p22-25
* masscan MACHINE\_IP/24 ‐‐top-ports 100

Masscan không được cài đặt trên AttackBox; tuy nhiên, nó có thể được cài đặt bằng cách sử dụng apt install masscan.

**Answer the questions below**

Which TCP ping scan does not require a privileged account?

TCP SYN Ping

Which TCP ping scan requires a privileged account?

TCP ACK Ping

What option do you need to add to Nmap to run a TCP SYN ping scan on the telnet port?

-PS23

1. **Using Reverse-DNS Lookup**

Đây là hành động mặc định trong nmap

-n: để bỏ qua bước này

-R: để truy vấn máy chủ DNS ngay cả đối với các máy chủ ngoại tuyến

Nếu bạn muốn sử dụng một máy chủ DNS cụ thể , bạn có thể thêm --dns-servers DNS\_SERVER tùy chọn

**Answer the questions below**

We want Nmap to issue a reverse DNS lookup for all the possibles hosts on a subnet, hoping to get some insights from the names. What option should we add?

-R

1. **Summary**

you have learned how ARP, ICMP, TCP, and UDP can detect live hosts by completing this room. Any response from a host is an indication that it is online. Below is a quick summary of the command-line options for Nmap that we have covered.

| **Scan Type** | **Example Command** |
| --- | --- |
| ARP Scan | **sudo nmap -PR -sn MACHINE\_IP/24** |
| ICMP Echo Scan | **sudo nmap -PE -sn MACHINE\_IP/24** |
| ICMP Timestamp Scan | **sudo nmap -PP -sn MACHINE\_IP/24** |
| ICMP Address Mask Scan | **sudo nmap -PM -sn MACHINE\_IP/24** |
| TCP SYN Ping Scan | **sudo nmap -PS22,80,443 -sn MACHINE\_IP/30** |
| TCP ACK Ping Scan | **sudo nmap -PA22,80,443 -sn MACHINE\_IP/30** |
| UDP Ping Scan | **sudo nmap -PU53,161,162 -sn MACHINE\_IP/30** |

Remember to add **-sn** if you are only interested in host discovery without port-scanning. Omitting **-sn** will let Nmap default to port-scanning the live hosts.

| **Option** | **Purpose** |
| --- | --- |
| **-n** | no DNS lookup |
| **-R** | reverse-DNS lookup for all hosts |
| **-sn** | host discovery only |