1. **Introduction**

1.1. Thông tin cơ bản

- **Nmap (Network Mapper)** là một công cụ mã nguồn mở được sử dụng để quét và khám phá mạng máy tính. Nó cung cấp các khả năng quét mạnh mẽ để kiểm tra các cổng mạng, xác định dịch vụ đang chạy, và thu thập thông tin về các máy chủ trong một mạng cụ thể. Nmap được sử dụng cho nhiều mục đích bao gồm:

+ Network Discovery: Nmap giúp xác định các thiết bị trong mạng, bao gồm cả các máy tính và các thiết bị mạng như máy chủ, máy in, bộ định tuyến, v.v. Bằng cách quét các địa chỉ IP, Nmap cho phép bạn biết được những máy chủ và dịch vụ đang hoạt động trong mạng.

+ Security Auditing: Nmap có thể được sử dụng để kiểm tra bảo mật mạng bằng cách tìm kiếm các lỗ hổng bảo mật và điểm yếu trong các hệ thống và dịch vụ. Bằng cách xác định các cổng mạng mở và các dịch vụ đang chạy, người quản trị có thể đánh giá các rủi ro bảo mật và thực hiện các biện pháp bảo mật

+ Service Enumeration: Nmap cho phép xác định những dịch vụ cụ thể đang hoạt động trên các máy chủ. Điều này có thể hữu ích để kiểm tra xem các dịch vụ có được cài đặt đúng cách và đang hoạt động hay không.

+ Network Performance Analysis: Bằng cách thực hiện các quét mạng, Nmap có thể giúp đánh giá hiệu suất mạng bằng cách xác định thời gian phản hồi của các máy chủ và dịch vụ.

+ Host Discovery: Nmap có thể giúp tìm ra các máy chủ đang hoạt động trong mạng bằng cách xác định các địa chỉ IP thực sự đang sử dụng.

- Các cách tiếp cận khác nhau mà Nmap sử dụng để khám phá các máy chủ trực tiếp. Đặc biệt có thể kể đến:

* ARP scan: This scan uses ARP requests to discover live hosts
* ICMP scan: This scan uses ICMP requests to identify live hosts
* TCP/UDP ping scan: This scan sends packets to TCP ports and UDP ports to determine live hosts.

- Quá trình 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 colorful arrows with text

Description automatically generated with medium confidence

1. **Enumerating Targets**

- Chúng ta đã đề cập đến các kĩ thuật khác nhau mà chúng ta có thể sử dụng để scan port. Trước khi giải thích chi tiết từng kỹ thuật và đưa nó vào sử dụng đối với mục tiêu trực tiếp, chúng tôi cần chỉ định các mục tiêu mà chúng tôi muốn quét. Nói chung, bạn có thể cung cấp một danh sách, một phạm vi hoặc một mạng con. Ví dụ về đặc tả mục tiêu là:

* List: ip1 ip2 ip3 sẽ quét 3 Ip address
* Range: 10.11.12.15-20 sẽ quét 6 Ip address: 10.11.12.15, 10.11.12.16, 10.11.12.17, …., 10.11.12.15.20
* Subnet:

- Ngoài ra chúng ta có thể cung cấp các tệp làm đầu vào cho danh sách mục tiêu của mình như **nmap -iL list\_of\_hosts.txt**

**+ -iL<inputfilename> :** tham số này cho phép chỉ định một tệp văn bản chứa danh sách các địa chỉ IP hoặc các tên miền mà chúng ta muốn quét bằng Nmap.

+ Lệnh này sẽ sử dụng nmap để quét các địa chỉ IP hoặc tên miền được liệt kê trong tệp list\_of\_hosts.txt.

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

A screenshot of a chat

Description automatically generated**- Câu hỏi:**

**Sol1:**

- Syntax Nmap:

+ **nmap [Scan Type(s)] [Options] [Target(s)]**

- Để liệt kê các địa chỉ IP từ target 10.10.12.13/29 ta sử dụng nmap đi kèm với **Scan Type** là **-sL** và **Options** là -n(do tôi chỉ muốn tìm ra các IP mà không muốn phân giải tên miền từ địa chỉ Ip tìm được).

- Kết quả được hiển thị bên dưới:

A screen shot of a computer

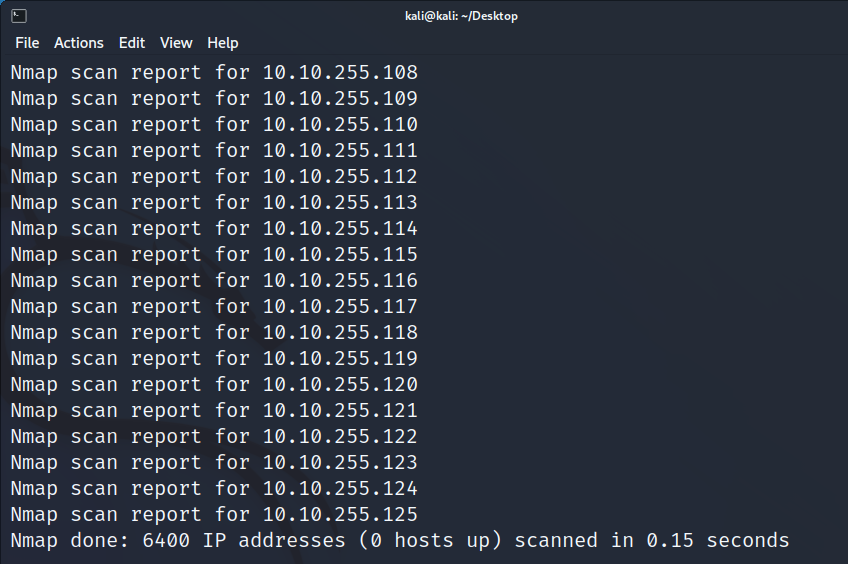
Description automatically generated+ Như vậy ta liệt kê được 8Ip từ target 10.10.12.13/29 với câu hỏi là ip address đầu tiên mà nmap scan được sẽ là: **10.10.12.8**

**Sol2:**

**-** Câu hỏi thứ 2 tương tự nhưng khác là ở đây target được cho dưới dạng range

**-** Ta sử dụng câu lệnh như sau: **nmap -sL -n 10.10.0-255.101-125**

- Kết quả được hiển thị ở bảng bên dưới



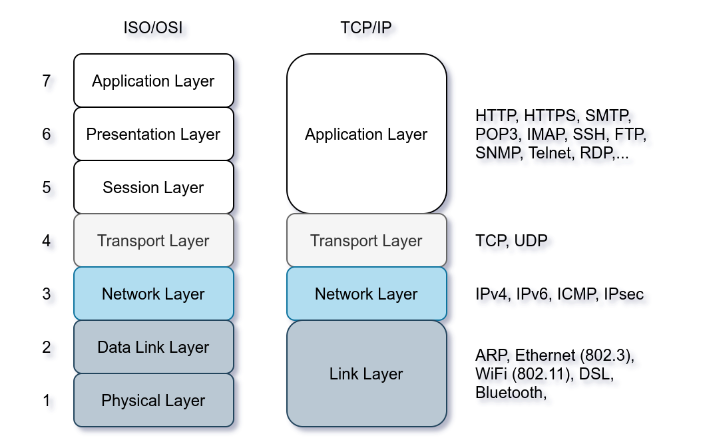
A screenshot of a chat

Description automatically generated- Số lượng IP được liệt kê là rất lớn, ta chỉ cần xem dòng cuối hiển thị tổng số Ip là được => 6400

1. **Discovey Live Hosts**

- Hãy cùng xem lại các lớp TCP/Ip được hiển thị trong hình bên dưới. Chúng ta sẽ tận dụng các giao thức để khám phá các máy chủ trực tiếp. Bắt đầu từ dưới lên chúng ta có thể sử dụng:

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



- Trước khi thảo luận chi tiết về cách máy quét có thể sử dụng từng loại, chúng tôi sẽ xem xét ngắn gọn bốn giao thức này. ARP có một mục đích: gửi một **frame** đến **broadcasr address** 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 Type 8 (Echo) và Type 0 (Echo Reply).

- Nếu bạn muốn ping một hệ thống trên cùng một mạng con, một truy vấn ARP nên đặt trước ICMP Echo.

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

1. **Nmap Host Discovery Using ICMP**

- Làm thế nào bạn biết máy chủ nào đang hoạt động? Điều cần thiết là tránh lãng phí thời gian của chúng ta khi quét cổng một máy chủ ngoại tuyến hoặc một địa chỉ IP không được sử dụng. Có nhiều cách khác nhau để khám phá các máy chủ trực tuyến. Khi không có tùy chọn khám phá máy chủ nào được cung cấp, Nmap tuân theo các phương pháp sau để khám phá các máy chủ trực tiếp:

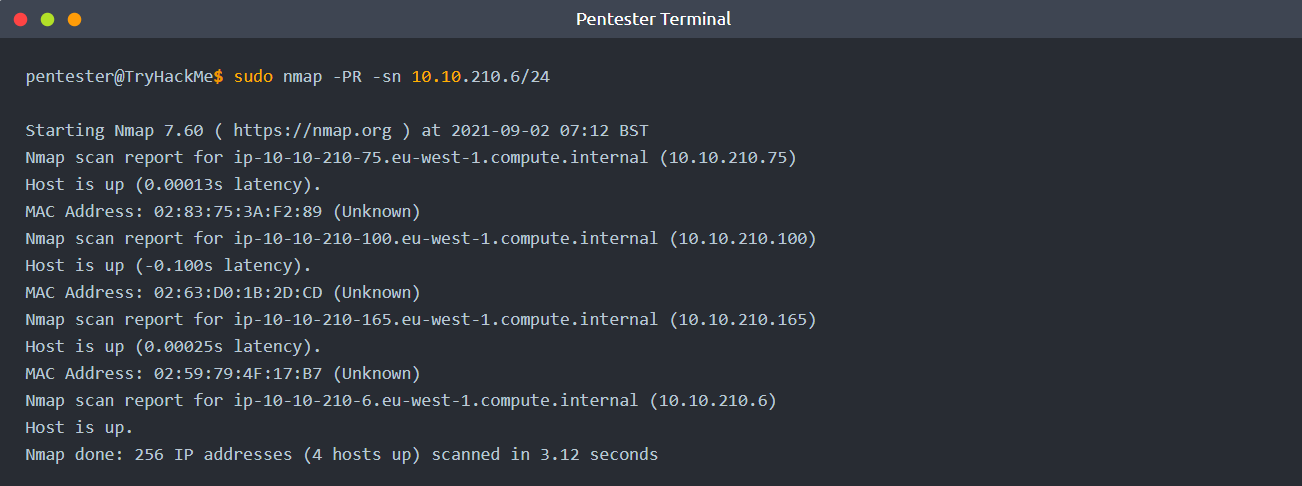
1. Khi người dùng là một **privileged user** đang cố gắng quét các mục tiêu trên mạng cục bộ(Ethernet), Nmap sử dụng các ARP Request, **privileged user** là **root** hoặc người dùng nào đó thuộc về **sudoers** và có thể chạy quyền **sudo.**

2.Khi người dùng là một **privileged user** đang cố gắng quét các mục tiêu bên ngoài các mạng cục bộ, Nmpa sử dụng ICMP echo requests, TCP ACK(Acknowledge) đến port 80 và 443.

3. Khi người dùng không phải **privileged user** đang cố gắng quét các mục tiêu bên ngoài các mạng cục bộ, Nmap sử dụng TCP 3 way bằng cách gửi các gói tin SYN đến các port 80 và 443.

- Theo mặc định, Nmap sử dụng quét ping để tìm các máy chủ trực tiếp, sau đó chỉ tiến hành quét các máy chủ trực tiếp. Nếu bạn muốn sử dụng Nmap để khám phá các máy chủ trực tuyến mà không cần quét cổng các hệ thống trực tiếp, bạn có thể phát hành **nmap -sn TARGETS**.

- Chỉ có thể quét ARP nếu bạn ở trên cùng mạng con với hệ thống đích. Trên Ethernet (802.3) và WiFi (802.11), bạn cần biết địa chỉ MAC của bất kỳ hệ thống nào trước khi có thể giao tiếp với hệ thống đó. Địa chỉ MAC là cần thiết cho tiêu đề lớp liên kết, tiêu đề chứa địa chỉ MAC nguồn và địa chỉ MAC đích trong số các trường khác. Để có được địa chỉ MAC, hệ điều hành sẽ gửi một truy vấn ARP. Một máy chủ trả lời các truy vấn ARP đã hoạt động. Truy vấn ARP chỉ hoạt động nếu mục tiêu nằm trên cùng một mạng con với bạn, tức là trên cùng một Ethernet/WiFi. Bạn sẽ thấy nhiều truy vấn ARP được tạo trong quá trình quét Nmap của mạng cục bộ. 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 rằng bạn chỉ muốn quét ARP. Ví dụ sau đây cho thấy Nmap sử dụng ARP để khám phá máy chủ mà không cần quét cổng. Chúng tôi chạy **nmap -PR -sn MACHINE\_IP/24** để khám phá tất cả các hệ thống trực tiếp trên cùng một mạng con với máy mục tiêu của chúng tôi.

- Trong trường hợp này, Target có địa chỉ IP là 10.10.210.6 và nó đã sử dụng các yêu cầu ARP để khám phá các máy chủ trực tiếp trên cùng một mạng con. Quét ARP hoạt động, như thể hiện trong hình bên dưới. Nmap gửi các yêu cầu ARP tới tất cả các máy tính mục tiêu và những máy tính trực tuyến sẽ gửi lại phản hồi ARP.

A couple of red lines with black text

Description automatically generated