NMAP\_2

**I. Các giai đoạn của quá trình quét Nmap:**

1. Quét trước tập lệnh (Script pre-scanning):

+ Công cụ tạo tập lệnh NSE sử dụng một tập hợp các lệnh có mục đích đặc biệt để thu thập thêm thông tin về các hệ thống từ xa

+ NSE không được thực thi trừ khi user yêu cầu nó với các tùy chọn như --script hoặc -sC

=> Giai đoạn quét trước chỉ xảy ra khi các tập lệnh cần nó được chọn

2. Liêt kê mục tiêu:

+ Nmap nghiên cứu các chỉ định máy chủ do người dùng cung cấp (DNS máy chủ, địa chỉ IP, ký hiệu mạng CIDR, …)

+ Nmap phân giải các thông số xác định này thành danh sách địa chỉ IPv4 hoặc IPv6 để quét.

3. Khám phá máy chủ quét (ping):

+ Giai đoạn này được chạy theo mặc định

4. Độ phân giải DNS ngược:

+ Khi Nmap đã xác định được máy chủ nào cần quét, nó sẽ tra cứu tên DNS ngược của tất cả các máy chủ được tìm thấy trực tuyến bằng quá trình quét ping

(Bước này có thể được bỏ qua với option -n hoặc được mở rộng để bao gồm tất cả các IP mục tiêu (ngay cả những IP bị hỏng) với -R(giải quyết tất cả)

5. Quét cổng:

+ Là hoạt động cốt lõi của Nmap

+ Các đầu dò được gửi đi và các phản hồi (hoặc không phản hồi) đối với các đầu dò đó được sử dụng để phân loại các cổng từ xa thành các trạng thái như *open, closed*, hoặc *filtered*

6. Phát hiện phiên bản:

+ Nếu phát hiện thấy bất kỳ cổng nào đang mở, Nmap có thể xác định phần mềm máy chủ nào đang chạy trên hệ thống từ xa

+ Nó thực hiện điều này bằng cách gửi nhiều loại thăm dò đến các cổng mở và khớp mọi phản hồi với cơ sở dữ liệu gồm hàng nghìn hơn 6.500 chữ ký dịch vụ đã biết

7.Phát hiện hđh:

8. Quét tập lệnh

9. Đầu ra

**II. Host discovery (“Ping Scanning”):**

1. TCP SYN Ping () -Ps <port list>

+ Hoạt động:

* Gửi gói TCP trống với bộ cờ SYN. Cổng mặc định là 80, nếu có một danh sách các cổng, các đầu dò sẽ được thử song song từng cổng
* Nếu cổng mở, phản hồi bằng gói SYN/ACK. Sau đó, máy chạy nmap sẽ ngắt kết nối mới bằng phản hồi RST thay vì gửi gói ACK để hoàn thành bắt tay, thiết lập kết nối đầy đủ
* Trên Unix, chỉ có người dùng có đặc quyền root mới có thể gửi và nhận các gói TCP thô. Đối với user, giải pháp được tự động sử dụng để việc gọi hệ thống bắt đầu đối với từng cổng mục tiêu. Nếu nhận được cờ SYN/ACK hoặc RST ⬄ máy chủ có phản hồi và đang hoạt động. Hoặc nếu kết nối bị treo đến khi hết thời gian chờ, máy chủ được đánh dấu là không hoạt động

1. Ping TCP ACK () -PA<port list>

+ Hoạt động:

* Khá giống với SYN ping, nhưng sử dụng gói ACK. Gói ACK có mục đích xác nhận dữ liệu qua kết nối TCP đã thiết lập >< không tồn tại kết nối như vậy => Các máy chủ phản hồi bằng gói RST => Lộ sự tồn tại
* Lý do cung cấp cả đầu dò SYN và ACK để tối đa hóa cơ hội vượt tường lửa

+ Một số tường lửa được cấu hình để ngăn chặn chặn các gói SYN đến (trừ dvu công cộng: web công ty, máy chủ,…) => ngăn cản các kết nối đến khác với tổ chức + cho phép người dùng thực hiện kết nối gửi đi không bị cản trở tới Internet

+ Khi áp dụng quy tắc tường lửa như thế, các đầu dò có thể bị chặn khi cổng mục tiêu đã đóng => ACK vượt qua những quy tắc này

+ Một số tường lửa dựa vào đánh giá trạng thái gói để loại bỏ các gói không cần thiết => ACK bị chặn

1. Ping UDP () -PU<port list>

+ Hoạt động:

* Gửi gói UDP đến các cổng nhất định (Cổng mặc định - 40.125)
* Khi tới được 1 cổng đã đóng trên máy mục tiêu, đầu dò UDP sẽ gợi ra 1 gói không thể truy cập được cổng ICMP ⬄ Biểu thị cho NMAP máy đã hoạt động và sẵn sàng
* Nhiều loại lỗi ICMP khác như máy chủ/mạng không thể truy cập được hoặc vượt quá TTL là dấu hiệu của máy chủ không hoạt động hoặc không thể truy cập được => Thiếu phản hồi (nếu cổng mở ;Loại bỏ các gói trống, không trả lại phản hồi)
* Một số dịch vụ vẫn phản hồi các gói UDP rỗng => Tiết lộ cho Nmap máy đang hoạt động

1. Ping IP protocol () -PO<protocol list>

+ Hoạt động:

* Gửi các gói IP với số giao thức được chỉ định được đặt trong IP header.
* Nếu không có giao thức nào được chỉ định, mặc định là gửi nhiều gói cho ICMP (giao thức 1), IGMP (giao thức 2), IP-in-IP (Giao thức 4)
* đối với ICMP, IGMP, TCP (giao thức 6) và UDP (giao thức 17), các gói được gửi với tiêu đề giao thức thích hợp trong khi các giao thức khác được gửi mà không có dữ liệu bổ sung ngoài tiêu đề IP

1. ARP Scanning (-PR):

+ hầu hết các mạng LAN, đặc biệt là những mạng sử dụng dải địa chỉ riêng do [RFC 1918](http://www.rfc-editor.org/rfc/rfc1918.txt) cấp , phần lớn địa chỉ IP không được sử dụng tại bất kỳ thời điểm nào

+ Khi Nmap cố gắng gửi gói IP thô chẳng hạn như yêu cầu tiếng vang ICMP, hệ điều hành phải xác định địa chỉ phần cứng đích (ARP) tương ứng với IP mục tiêu để nó có thể xử lý khung ethernet đúng cách => Đòi hỏi nó phải đưa ra một loạt yêu cầu ARP => Thời gian xử lý lâu khi số lượng mục tiêu lớn

+ Quét ARP giải quyết cả hai vấn đề bằng cách đặt Nmap vào tầm kiểm soát. Nmap đưa ra các yêu cầu ARP thô và xử lý việc truyền lại cũng như thời gian chờ theo quyết định riêng của nó. Bộ nhớ đệm ARP của hệ thống bị bỏ qua

+  Các máy chủ thường chặn các gói ping dựa trên IP, nhưng nhìn chung chúng không thể chặn các yêu cầu hoặc phản hồi ARP mà vẫn liên lạc trên mạng. Ngay cả khi các loại ping khác nhau (chẳng hạn như -PEhoặc -PS) được chỉ định, Nmap vẫn sử dụng ARP thay thế cho bất kỳ mục tiêu nào trên cùng một mạng LAN