Bài: 3.2 Quét mạng - Tổng quan về Network Scanning (Phần 2)

Xem bài học trên website để ủng hộ Kteam: 3.2 Quét mạng - Tổng quan về Network Scanning (Phần 2)

Mọi vấn đề về lỗi website làm ảnh hưởng đến bạn hoặc thắc mắc, mong muốn khóa học mới, nhằm hỗ trợ cải thiện Website. Các bạn vui lòng phản hồi đến Fanpage How Kteam nhé!

Tổng quan về Network Scanning

Công nghệ Scan

Công nghệ Scan bao gồm công nghệ **Scan UDP** và **TCP**. Quan sát mô tả dưới đây thể hiện sự phân loại các công nghệ Scan:

Kết nối TCP/ Full Open Scanning

Full Open Scanning là một hình thức của công nghệ scan, trong đó quy trình bắt tay ba bước bắt đầu và kết thúc. **Full Open Scanning** đảm bảo các phản hồi từ các host đích vẫn hoạt động và hoàn thiện việc kết nối. Đó là một ưu điểm phổ biến của Full Open Scanning. Tuy nhiên, nó có thể bị dò tìm, loại bỏ bởi các thiết bị bảo mật như **tường lửa** và **IDS**. Kết nối **TCP/ Full Open Scanning** không yêu cầu quyền ưu tiên người dùng cấp cao (**Super user Privileges**)

Khi đang sử dụng **Full Open Scanning** và gặp phải một port đóng, phản hồi **RST** được gửi tới các yêu cầu đang đi đến nhằm kết thúc thử nghiệm. Để thực hiện **Full Open Scan**, bạn cần sử dụng lựa chọn **–sT** cho việc kết nối Scan (Connect Scan)

Gõ lệnh để thực thi Full Open Scan:

```
nmap -sT <ip address or range>
```

Ví dụ, quan sát đầu ra được thể hiện dưới đây, sử dụng công cụ **Zenmap** để thực hiện **Full Open Scan**:

Stealth Scan (Half-open Scan)

Half Open Scan còn được biết đến như **Stealth Scan**. Để hiểu được quá trình **Half Open Scan**, xem xét cốt kịch của hai **host A** và **B**. Host A là điểm bắt đầu kết nối bắt tay TCP. Host A gửi gói tin **Sync** để bắt đầu bắt tay. Host nhận (host B) hồi đáp bằng gói tin **Sync+Ack**. Host A, thay vì nhận gói **Ack** từ host B, sẽ trả lời bằng RST.

Để biểu diễn kiểu scan này trong nmap, sử dụng cú pháp:

```
nmap -sS <ip address or range>
```

Hãy quan sát kết quả dưới đây :

Inverse TCP Flag Scanning

Inverse TCP Flag Scanning là quá trình Scan trong đó người gửi gửi đi thăm dò TCP với các TCP flag, i.e. FIN, URG và PSH hoặc không cần flag. Sự thăm dò bằng TCP flags được biết đến như **XMAS Scanning**. Trong trường hợp không có các flag, ta biết đến nó như **Null Scanning**

Xmas Scan

Xmas Scan là kiểu scan trong đó chứa nhiều **flag**. Các gói tin được gửi đi song song với URG, PSH và FIN, hoặc một gói tin với tất cả các flag tạo ra một tình huống bất thường đối với người nhận. Hệ thống nhận sẽ phải quyết định khi sự cố xảy ra. **Port** bị đóng phản hồi với gói tin RST đơn. Nếu port đang được mở, một số hệ thống sẽ phản hồi như một port mở, tuy rằng hệ thống modern sẽ phớt lờ hoặc làm ngừng lại các yêu cầu bởi sự kết hợp giả của các flag này. FIN Scan chỉ hoạt động với hệ điều hành nào có RFC-793 based TCP/IP Implementation. FIN Scan sẽ không hoạt động trên bất cứ phiên bản hiện tại nào của Windows, điển hình như Windows XP hoặc những phiên bản mới hơn.

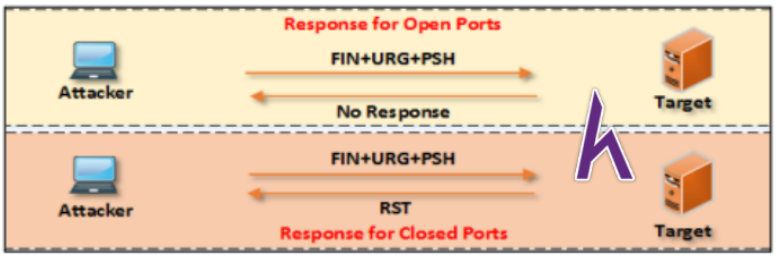


Figure 3-23 Xmas Scan

Để thực hiện kiểu scan này, sử dụng cú pháp:

> **nmap -sX -v** <ip address or range>

Lab 3-3: Xmas Scanning

Ví dụ thực tiễn

Sử dụng **Xmas Scanning** trên Kali Linux, ta đang "ghim" vào host Windows 2016 với tường lửa trong trạng thái hoạt động và không hoạt động để quan sát những phản hồi:

Thủ tục:

> Mở Window Server 2016 và xác nhận tường lửa đang trong trạng thái hoạt động

Mở một **terminal** trên **Kali Linux** và gõ vào lệnh dưới đây:

Quan sát kết quả được thể hiện như trên đây, tất cả những port được scan là **Open & Filtered** (Mở và được lọc). Có nghĩa là khi đó, tường lửa đang hoạt động. Một tường lửa thì cơ bản sẽ không phản hồi những gói tin giả định là các Open **@ filtered port**.

Giờ thì trở về với **Window Server 2016** và vô hiệu hóa tường lửa:

Giờ hãy chạy scan một lần nữa:

Trong trường hợp này, tường lửa bị vô hiệu hóa, vì vậy tất cả các port được hiển thị là đang đóng.

FIN Scan

FIN scan là quá trình gửi đi các gói tin chỉ chứa bộ FIN flag. Những gói tin này có thể có quyền tin cậy để vượt qua tường lửa. Gói FIN Scan khi được gửi tới mục tiêu, các port sẽ được xem như là đang mở nếu không có hồi đáp. Nếu port bị đóng, RST được trả lại.

Để thực hiện kiểu scan này, sử dụng cú pháp:

> **nmap -SF** <ip address or range>

Null Scan

Null Scan Là quy trình gửi đi các gói tin không chứa các bộ flag. Các phản hồi đều tương tự với **FIN** và **XMAS Scan**. Nếu gói tin **Null Scan** gửi tới một port mở, sẽ không có phản hồi. Nếu gói tin Null Scan gửi tới port đóng, nó sẽ mang theo gói RSR. Việc thực hiện kiểu scan này tương đối dễ dàng vì không có lý do hợp lý nào giải thích cho việc gửi đi gói tin mà không có flag nào.

Để thực hiện kiểu scan này, sử dụng cú pháp:

> **nmap -sN** <ip address or range>

Scan thăm dò Flag ACK

Scan thăm dò Flag ACK gửi đi gói tin TCP với bộ ACK flag đến mục tiêu. Người gửi kiểm tra thông tin của header bởi vì ngay cả khi gói tin ACK đã thành công đến với mục tiêu, nó sẽ trả lời bằng gói RST khi port mở hoặc đóng. Sau quá trình phân tích thông tin của header như TTL và phạm vi Windows của gói RST, kẻ tấn công nhận dạng được trạng thái của port đang đóng hay mở.

Scan thăm dò ACK cũng hỗ trợ trong việc nhận dạng hệ thống sàng lọc. Nếu gói RST nhận được từ mục tiêu, điều đó có nghĩa là gói tin đến port đó không được sàng lọc. Trong trường hợp không có phản hồi, có nghĩa là tường lửa trạng thái (Stateful firewall) đang lọc port.

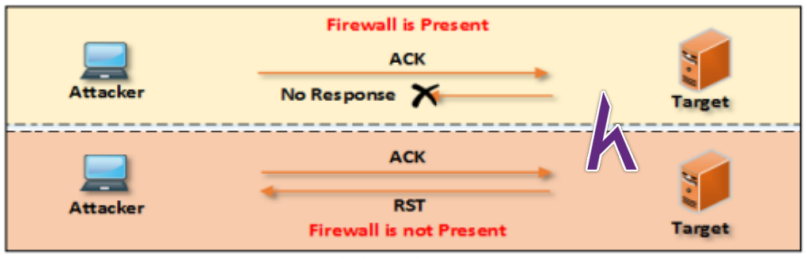


Figure 3-29 Ack Flag Probe Scanning Response

IDLE/IPID Header Scan

IDLE/IPID Header Scan là một công nghệ độc đáo và hiệu quả để nhận dạng trạng thái của port máy chủ mục tiêu. Khi sử dụng cách scan này, các profile không đáng kể có thể được giữ lại.

Scan tĩnh (Idle sca) mô tả khả năng ẩn nấp của kẻ tấn công. Kẻ tấn công che giấu những nét nhận dạng bằng cách, thay vì gửi đi gói tin qua hệ thống, quá trình quét sẽ được thực hiện với những gói tin đánh lừa từ hệ thống Zombie. Nếu mục tiêu khảo sát những mối đe dọa, nó sẽ lần theo Zombie thay vì dò tìm theo dấu kẻ tấn công.

Trước khi tìm hiểu về những bước cần thiết cho IDLE/IPID Scan, bạn cần phải nhớ lại một vài điểm quan trọng:

- Để xác định cổng nào đang mở, gửi gói tin SYN đến port
- Mục tiêu sẽ phản hồi bằng gói tin SYN+ACK nếu port đang mở
- Mục tiêu sẽ phản hồi bằng gói tin RST nếu port đang đóng.
- Gói tin SYN+ACK không yêu cầu có thể, hoặc phớt lờ, hoặc phản hồi bằng RST
- Mỗi gói IP đều có một số IPID
- Số gia OS

Bước 01:

- Gửi gói tin **Sync+Ack** đến Zombie để lấy được số **IPID** của nó
- Zombie không chờ **Sync+Ack** nên sẽ phản hồi bằng gói RST. Lời hồi đáp đó để lộ IPID
- Giải nén IPID từ gói tin

Bước 2:

- Gửi gói tin đến mục tiêu, đánh lừa địa chỉ IP của Zombie
- IP port mở,mục tiêu phản hồi bằng **Sync+Ack** cho Zombie và Zombie sẽ lại phản hồi cho mục tiêu với gói tin RST

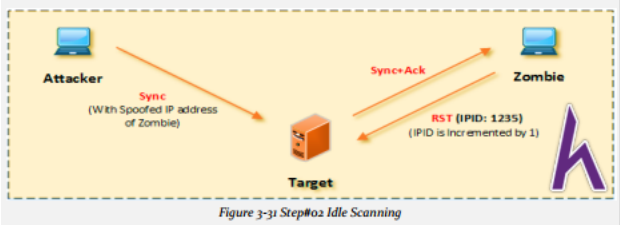
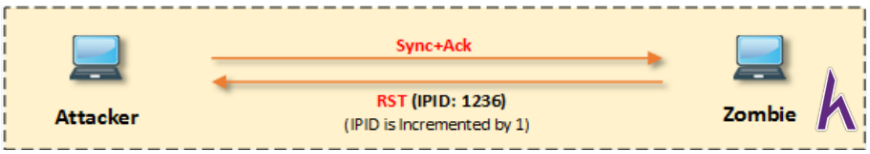


Figure 3-31 Step#02 Idle Scanning

- Nếu port đóng, mục tiêu phản hồi Zombie bằng gói tin RST và Zombie sẽ không phản hồi gì thêm tới mục tiêu. IPID của Zombie sẽ không được nhân lên.

Bước 3:

- Gửi gói tin **Sync+Ack** một lần nữa, để lấy được số IPID và so sánh với IPID đã được giải nén tại bước 1 (i.e.1234)
- Zombie phản hồi bằng gói RST. Lời phản hồi này tiết lộ IPID
- Giải nén IPID từ gói tin
- So sánh IPID
- Port đang mở nếu IPID được nhân lên bằng 2



- Port đang đóng nếu IPID được nhân lên bằng 1

Scan UDP

Giống như công nghệ scan dựa trên TCP, ta cũng có các phương pháp **Scan UDP**. Hãy nhớ rằng, UDP là giao thức phi kết nối. UDP không có các flag. Khi gói tin UDP đang hoạt động với các port, ta không cần đến các kết nối có định hướng. Sẽ chẳng có phản hồi nào nếu port mục tiêu đang mở. Tuy nhiên, nếu port bị đóng, tin nhắn phản hồi "**Port unreachable**" sẽ được gửi về. Hầu hết các chương trình độc hại, Trojans, phần mềm gián điệp sử dụng port UDP để truy cập vào mục tiêu.

Để thực hiện kiểu scan này, ta có thể sử dụng cú pháp sau đây:

> **nmap -sU -v** <ip address or range>

Quan sát kết quả được mô tả dưới đây:

Công cụ Scan

Netscan Tools Pro là một ứng dụng thu thập thông tin, thực hiện xử lý sự cố mạng, điều khiển, tìm hiểu và chẩn đoán bằng các công cụ được thiết kế cho hệ điều hành Window, cung cấp một cuộc kiểm tra tập trung của IPv4, IPv6, tên miền, email và URL bằng **Automatic and Manual Tool**.

Công cụ Scan cho điện thoại

Có rất nhiều công cụ cơ bản và tiên tiến khả dụng cho các thiết bị di động trên các cửa hàng ứng dụng. Dưới đây là một vài công cụ hiệu quả cho network scanning:

Network Scanner:

> Công cụ " **Network Scanner** " cung cấp máy tính toán IP, DNS lookup, công cụ Whois, công cụ truy vết (Trace route) và máy scan Port

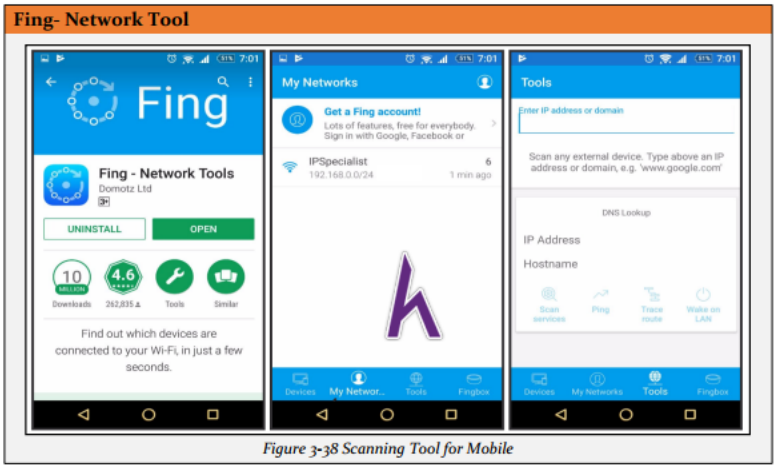


Figure 3-38 Scanning Tool for Mobile

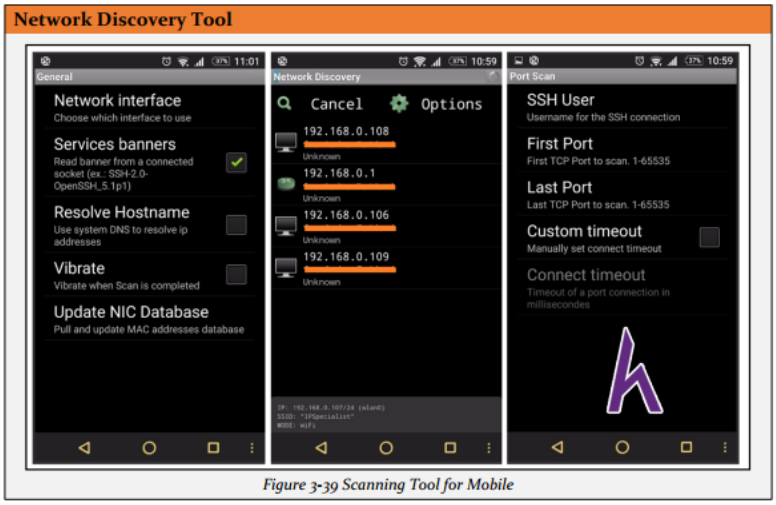


Figure 3-39 Scanning Tool for Mobile

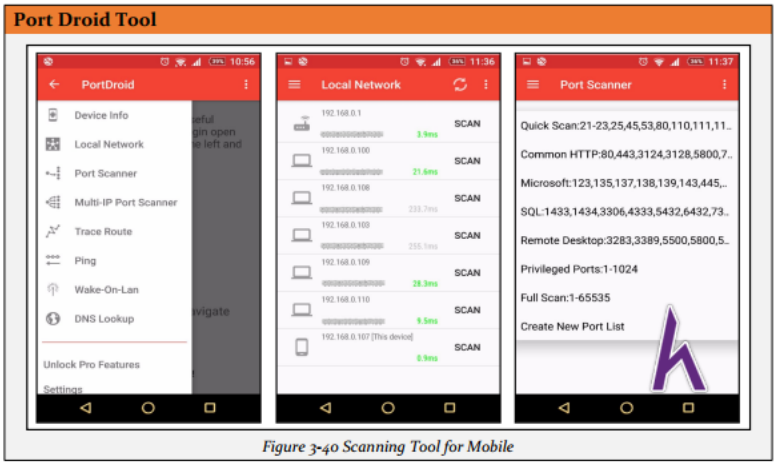


Figure 3-40 Scanning Tool for Mobile

Scan ngoài IDS

Kẻ tấn công sử dụng những gói phân mảnh và gói nhỏ nhằm tránh được các thiết bị bảo mật như tường lửa, IDS và IPS. Công nghệ cơ bản thường được sử dụng phổ biến là chia nhỏ số lượng thành các gói nhỏ hơn. IDS phải tập hợp lại những gói tin nhỏ đang tràn tới để kiểm tra và phát hiện cuộc tấn công. Gói tin nhỏ sẽ được điều chỉnh nhiều hơn khiến cho việc tập hợp và phát hiện trở nên phức tạp hơn.

Một cách khác để sử dụng phân mảnh là gửi đi những gói tin đã bị phân nhỏ đã hỏng. Những gói tin hỏng này được gửi đi bằng các máy chủ proxy hoặc qua các máy móc để bắt đầu tấn công.

OS Fingerprinting & Banner Grabbing

OS Fingerprinting (In dấu vân tay hệ điều hành) là một kỹ thuật sử dụng để nhận dạng các thông tin của hệ điều hành đang chạy trên máy mục tiêu. Bằng cách thu thập thông tin về hệ điều hành đang chạy, tin tặc có thể xác định được điểm yếu và những lỗi bug hệ điều hành có thể chứa.

Có hai loại **OS Fingerprinting** là:

1. OS Fingerprinting chủ động
2. OS Fingerprinting bị động

Banner Grabbing cũng tương tự như **OS fingerprinting**, nhưng trong thực tế, **Banner Grabbing** xác định những dịch vụ đang chạy trên máy đích. Tiêu biểu là **Telnet**, được sử dụng để khôi phục thông tin của banner.

OS Footprinting chủ động hay Banner Grabbing

NMAP có thể thực hiện **Banner Grabbing** chủ động dễ dàng. NMAP, như ta biết là một công cụ mạng mạnh mẽ hỗ trợ nhiều đặc điểm và lệnh điều khiển. Khả năng dò tìm của hệ điều hành cho phép gói tin TCP và UDP được gửi đi rồi quan sát phản hồi của host mục tiêu. Một bản đánh giá chi tiết về phản hồi này mang theo vài manh mối về bản chất của hệ điều hành, tiết lộ loại hệ điều hành.

Để thực hiện dò tìm OS với nmap, thực hiện như dưới đây:

> **nmap -O** <ip address>

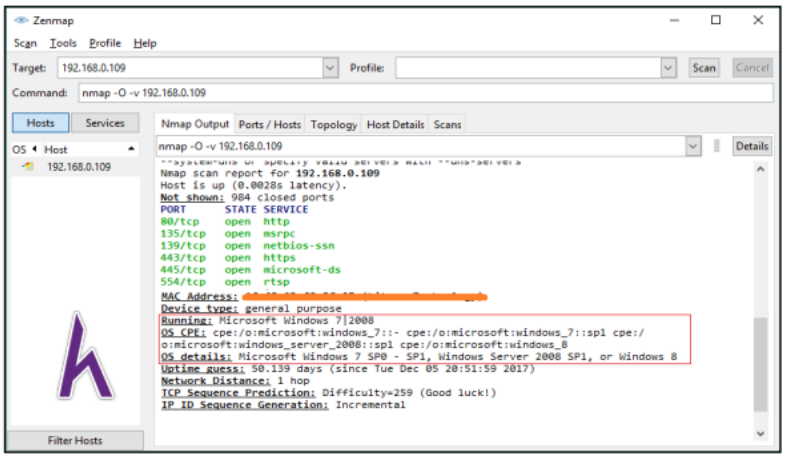


Figure 3-41 OS Fingerprinting

OS Fingerprinting hay Banner Grabbing bị động

OS Fingerprinting bị động đòi hỏi những mô tả chi tiết về đường truyền. Bạn có thể thực hiện Banner grabbing bị đồng bằng cách phân tích đường dẫn mạng cùng với sự kiểm duyệt đặc biệt của giá trị TTL và Window Size. Giá trị TTL và Window Size được kiểm tra từ header của gói tin TCP trong lúc quan sát đường truyền mạng. một vài giá trrij thường thấy cho hệ điều hành là:

Hệ điều hành	TTL	TCP Window Size
Linux	64	5840
Google customized Linux	64	5720
FreeBSD	64	65535
Window XP	128	65535
Window Vista, 7 và Server 2008	128	8192
Cisco Router (iOS 12.4)	255	4128

Công cụ Banner Grabbing

Có một vài công cụ có sẵn dành cho banner grabbing. Một vài trong số đó là:

- ID Server
- Netcraft
- Netcat

- Telnet
- Xprobe
- Pof
- Maltego

Mindmap