Bài: 3.1 Quét mạng - Tổng quan về Network Scanning (Phần 1)

Xem bài học trên website để ủng hộ Kteam: 3.1 Quét mạng - Tổng quan về Network Scanning (Phần 1)

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!

Tóm tắt

Sau công đoạn thăm dò, rất có thể ta đã có đủ thông tin về mục tiêu. Và bây giờ, công đoạn **Scanning Network** (quét mạng) sẽ cần một vài trong số những thông tin đó để có thể đi đến các công đoạn xa hơn.

Network Scanning là một phương pháp khai thác những thông tin mạng như: Nhận dạng máy chủ (host), thông tin cổng "port", và các dịch vụ bằng cách quét các mạng và cổng port.

Mục đích chính của Network Scanning là:

- Nhận dạng host hoạt động trên mạng
- Nhận dạng các cổng port đóng và mở
- Nhận dạng thông tin hệ điều hành
- Nhận dạng các dịch vụ đang chạy trên mạng
- Nhận dạng các quá trình đang diễn ra trên mang
- Nhận dạng sự hiện diện của thiết bị bảo mật, ví dụ như tường lửa
- Nhận dạng kiến trúc hệ thống
- Nhận dạng các dịch vụ đang chạy
- Nhận dạng các điểm yếu

Tổng quan về Network Scanning

Scanning network bao gồm việc thăm dò mục tiêu nhằm khai thác thông tin. Khi một người dùng thăm dò một người dùng khác, những phản hồi nhận được có thể tiết lộ nhiều thông tin hữu ích. Việc nhận dạng chuyên sâu một mạng máy máy tính, các cổng port và các dịch vụ đang chạy giúp tạo nên bức tranh tổng quan về kiến trúc mạng, và, kẻ tấn công có được bức tranh chi tiết hơn về mục tiêu của hắn.

Giao tiếp TCP

Có hai loại giao thức truy cập mạng. Đó là **TCP** (***T**ransmission **C**ontrol **P**rotocol*) và **UDP** (***U**ser **D**atagram **P**rotocol*).

- **TCP** là kết nối có định hướng. Giao tiếp hai chiều sẽ diễn ra sau khi thiết lập kết nối thành công. UDP là giao thức phi kết nối đơn giản hơn.
- Với UDP, những tin nhắn hàng loạt sẽ được gửi đi theo "gói" trong mảng. Khác với TCP, UDP không tăng cường độ tin cậy, điều chỉnh lưu lượng hay chứa chức năng phục hồi hỏng hóc cho gói IP.

Chính bởi sự đơn giản của mình, header của UDP chứa ít "bytes" và tiêu tốn ít mạng hơn hẳn TCP . Hãy theo dõi biểu đồ dưới đây để thấy được "**header**" của TCP"

Figure 3-02 TCP Header

Các flag được xếp trong TCP header thuộc 9 bits, bao gồm 6 flag sau đây

Flag	Use
SYN	Bắt đầu kết nối nhằm đạt được giao tiếp dễ dàng giữa hai máy chủ
ACK	Công nhận công thức của một gói
UrG	Chỉ ra những dữ liệu khẩn cấp của gói cần được giải quyết ngay lập tức
PSH	Chỉ dẫn hệ thống gửi gửi đi những dữ liệu đệm ngay lập tức
FIN	Báo cho hệ thống từ xa về điểm kết thúc giao tiếp. Về bản chất, điều này đóng kết nối một cách "thanh lịch"
RST	Đặt lại kết nối

Trong quá trình thiết lập kết nối **TPC** giữa các máy chủ, quá trình bắt tay 3 bước diễn ra. Quá trình bắt tay này đảm bảo chu kỳ kết nối thành công, đáng tin cậy và kết nối có định hướng giữa các máy chủ. Chu trình thiết lập một kết nối TCP bao gồm ba bước được thể hiện dưới đây:

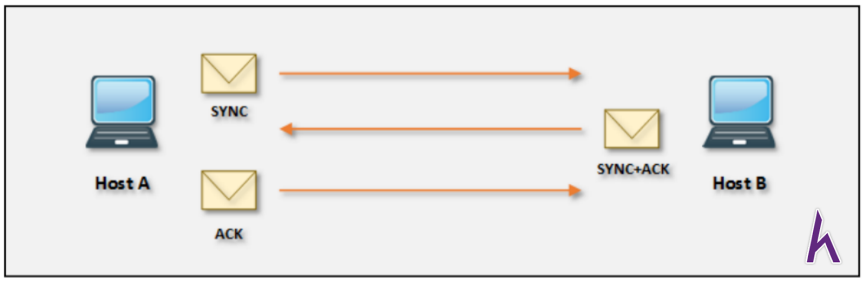

Figure 3-03 TCP Connection Handshaking

Hãy xem xét:

Host A muốn giao tiếp với host B, kết nối TCP được thiết lập khi host A gửi đến host B một gói **Sync**.

Host B theo đó xác nhận gói **Sync** từ host A, trả lời host A với gói **Sync+Ack**. Host A phản hồi với gói **Ack** khi đã nhận gói **Sync+Ack** từ host B. Sau khi bắt tay thành công, kết nối TCP sẽ được thiết lập.

U.S Dept đưa ra mô đen **TCP/IP**, of Defence bằng cách kết hợp OSI Layer Model và DOD. TCP và IP là hai trong số những tiêu chuẩn định ra Internet. IP định rõ bằng cách nào mỗi máy tính có thể đưa dữ liệu đến máy tính khác qua đường truyền liên kết mạng.

TCP định ra làm sao thiết bị có thể tạo ra kênh giao tiếp đáng tin cậy qua mạng. IP định rõ địa chỉ và đường truyền, trong khi TCP định ra cách thực hiện đoạn hội thoại qua liên kết mà không khiến dữ liệu bị cắt xén hay mất mát. Các lớp trong mô đen TCP/IP thể hiện chức năng tương tự với các chi tiết tương tự như trong OSI mô đen, điểm khác biệt duy nhất là chúng kết hợp ba tầng cao nhất thành một lớp chương trình đơn.

Tạo gói tùy chỉnh bằng flag TCP

Phần mềm **Colasoft Packet Builder** cho phép ta tạo gói mạng đặc chế. Những gói mạng này có thể chống chịu lại các cuộc tấn công. Sự tùy biến cũng có thể được dùng để thiết lập các gói chia nhỏ hơn. Bạn có thể tải phần mềm từ www.colasoft.com

Colasoft Packet Builder cung cấp các lựa chọn xuất và nhập để thiết đặt các gói. Bạn cũng có thể thêm các gói mới bằng cách nhấp chuột vào nút **Add**. Chọn loại gói từ hộp danh sách thả xuống. Bạn có những lựa chọn sau:

- Gói ARP

- Gói IP
- Gói TCP
- Gói UDP

Figure 3-05 Creating Custom Packet

Sau khi chọn loại gói, bạn đã có thể tùy biến gói, chọn Network Adapter và gửi nó tới điểm đích.

Phương thức quét

Phương thức quét bao gồm những bước dưới đây:

- Kiểm tra hệ thống đang hoạt động
- Khám phá những port mở
- Quét IDS ở tầm xa hơn
- Nắm bắt Banner
- Quét điểm yếu
- Biểu đồ mạng
- Proxies

Kiểm tra hệ thống hiện hành

Đầu tiên, bạn cần có hiểu biết về những host đang tồn tại trong mạng được đặt làm mục tiêu. Việc tìm kiếm host hiện hành trong mạng được thực hiện bởi gói ICMP. Mục tiêu hồi đáp gói ICMP bằng lời hồi đáp ICMP. Phản hồi đó xác nhận host đang hoạt động.

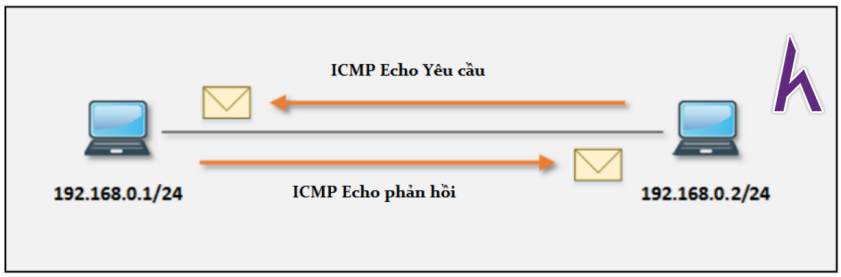

Figure 3-07 ICMP Echo Request & Reply Packets

Host với địa chỉ IP **192.168.0.2/24** đang cố nhận dạng host **192.168.0.1/24** hoạt động bằng cách gửi gói ICMP Echo được chỉ định đến địa chỉ IP đích **192.168.0.1**

Nếu host đích phản hồi thành công gói ICMP Echo, host đang hoạt động.

Nếu host không hoạt động, hãy quan sát phản hồi dưới đây của gói **ICMP Echo**:

Scan ICMP (ICMP Scanning)

Quét ICMP là một phương thức nhận dạng host nào đang hoạt động bằng cách gửi **ICMP echo request** tới một host. Gói trả lời **ICMP Echo** xác nhận host đang hoạt động. **Ping Scanning** là một công cụ hữu hiệu không chỉ cho việc nhận dạng host hoạt động mà còn cho việc quyết đinh gói ICMP nào vượt qua tường lửa và giá trị TTL

Ping Sweep

Ping Sweep định ra host hoạt động trên phạm vị rộng. **Ping Sweep** là một cách gửi gói **ICMP Echo Request** tới một số lượng lớn địa chỉ IP thay vì chỉ một địa chỉ IP rồi quan sát tín hiệu phản hồi.

Host hoạt động sẽ trả lời bằng gói **ICMP Echo Reply**. Vì vậy, thay vì thăm dò một cá nhân, ta có thể thăm dò một lượng lớn IP bằng **Ping Sweep**. Có rất nhiều công cụ có sẵn để thực hiện **Ping Sweep**. Ta có thể sử dụng những công cụ Ping Sweep như **SolarWinds Ping Sweep tool** hoặc **angry IP Scanner** để "ping" phạm vi của những địa chỉ IP. Thêm vào đó, chúng có thể thể hiện DNS tra cứu nghịch đảo, giải hostnames, mang đến địa chỉ MAC và quét các port.

Kiểm tra Port mở

Scan SSDP

Simple Service Discovey Protocol (SSDP) là một giao thức được dùng để phát hiện dịch vụ mạng mà không cần tới sự trợ giúp của cấu hình dựa vào máy chủ như **Dynamic Host Configuration Protocol** (DHCP) và **Domain Name System** (DNS) và cấu hình mạng host tĩnh. Giao thức **SSDP** có thể khám phá những thiết bị **Plug&Play** với **UPnP** (Universal Plug and Play). Giao thức **SSDP** tương thích với **IPv4** và **IPv6**.

Công cụ Scan

Nmap

Một cách khác để "ping" một host là thể hiện một "ping" với nmap. Sử dụng Windows hoặc Linux command prompt, gõ vào dòng lệnh sau:

> **nmap -sP –v** <target IP Address>

Cho tới khi host mục tiêu phản hồi thành công, nếu lệnh đó tìm được một host hoạt động, nó sẽ trả lại một tin nhắn chỉ ra địa chỉ IP của host mục tiêu đang, cùng với địa chỉ phương tiện kiểm soát truy cập (MAC) và cung cấp thẻ mạng.

Ngoại trừ những gói **ICMP Echo Request** và việc sử dụng **ping sweep**, **nmap** cũng thực hiện quét nhanh. Nhập dòng lệnh dưới đây để quét nhanh:

> **nmap -sP -PE -PA**<port number> <starting IP/ending IP>

Ví dụ:

Nmap là một bản tóm tắt, đưa ra khám phá Host , phát hiện Port, phát hiện dịch vụ, thông tin phiên bản hệ điều hành, thông tin địa chỉ phần cứng, dò tìm phiên bản dịch vụ, điểm yếu và phát hiện khai thác với Nmap Scripts.

Lab 3-1 : Lệnh Hping

Ví dụ thực tiễn

Sử dụng thiết bị **Zenmap** để thực hành quét Nmap với những lựa chọn khác nhau. Ta sẽ sử dụng Window 7 PC để quét mạng:

Quy trình :

> Thực hành quét ping mạng **10.10.50.0/24**, lập danh sách những máy phản hồi ping
>
> Lệnh: **nmap –sP 10.10.50.0/24**

Giờ hãy quét các chi tiết hệ điều hành của host mục tiêu **10.10.50.210**. Ta có thể quét tất cả các host với lệnh **nmap –O 10.10.50. ***

> Lệnh: **nmap –O 10.10.50.210**

Hping2 và Hping3

Hping là một công cụ tạo và phân tích với các dòng lệnh **TCP/IP** được sử dụng để gửi đi các gói **TCP/IP** tùy chỉnh, hiển thị phản hồi từ mục tiêu giống như lệnh ping hiển thị các gói **ICMP Echo Reply** từ host mục tiêu. **Hping** cũng có thể điều khiển việc phân mảnh, phần thân gói tin tùy chọn, kích cỡ và truyền dẫn tệp tin. **Hping** hỗ trợ các giao thức TCP, UUDP, ICMP và RAW-IP. Khi sử dụng Hping, ta có thể biểu diễn các thông số sau:

- Nguyên tắc kiểm tra tường lửa
- Scan port hiện đại
- Kiểm tra thực thi mạng
- Khám phá đường đi MTU
- Truyền dẫn tập tin thậm chí qua nguyên tắc tường lửa "phát xít"
- Công cụ truy vết dưới nhiều giao thức khác nhau
- Lấy vân tay OS và những thứ khác từ xa

Lab 3-2 : Các lệnh Hping

Ví dụ thực tiễn

Sử dụng lệnh **Hping** trên **Kali Linux**, ta sẽ "**ping**" một máy chủ window với nhiều gói tin tùy chọn khác nhau trong thử nghiệm này:

Lệnh

- Tạo một gói tin ACK

> root@kali:**-# hping3 –A 192.168.0.1**

- Tạo trình quét SYN chống lại những cổng port khác nnhau

> root@kali:**-# hping3 -8 1-600 –S 10.10.50.202**

- Để tạo gói tin với FIN, URG và bộ flag PSH

> root@kali:**~# hping3 –F –P –U 10.10.50.202**

Dưới đây là một số lựa chọn được sử dụng với lệnh **Hping**:

-h	--help	Thể hiện sự hỗ trợ
-v	--version	Thể hiện phiên bản
-c	--count	Bộ đếm
-I	--interface	Tên cổng giao tiếp
	--flood	Gửi gói tin nhanh nhất có thể mà không hiển thị hồi đáp
-V	--verbose	chế độ Verbose
-o	--rawip	Chế độ RAW IP
-i	--icmp	Chế độ ICMP
-2	--udp	Chế độ UDP
-8	--scan	Chế độ Scan
-9	--listen	Chế độ nghe
	--rand-dest	Chế độ địa chỉ đích đến ngẫu nhiên
	--rand-source	Chế độ địa chỉ nguồn ngẫu nhiên
-s	--baseport	Nguồn cổng port cơ sở (Mặc định ngẫu nhiên)
-P	--destport	[+][+]<port> port đích (mặc định o) ctrl+z inc/dec
-Q	--seqnum	Chỉ hiển thị số thứ tự (sequence number) TcP
-F	--fin	Thiết lập flag FIN
-S	--syn	Thiết lập flag SYN
-P	--push	Thiết lập flag PUSH
-A	--ack	thiết lập flag ACK
-U	--urg	thiết lập flag URG
	--TCP-timestamp	Cho phép lựa chọn dấu hiệu thời gian của TcP để đoán HZ/uptime (thời gian chạy máy)