Dò tìm lỗ hổng bảo mật thông tin

WWW.UIT.EDU.VN

TS. Nguyễn Tấn Cầm

Nội dung

WWW.UIT.EDU.VN

- Các bước thực hiện của một cuộc tấn công mạng
- Các khái niệm dò quét
- Các công cụ dò quét
- Các kỹ thuật dò quét phổ biến
- Dò quét phía sau trình phát hiện xâm nhập và tường lửa
- Xác định phiên bản hệ điều hành và ứng dụng
- Các phương pháp giảm thiểu nguy cơ dò quét mạng
- Dò quét kiểm thử
- Câu hỏi ôn tập

Các bước thực hiện của một cuộc tấn công mạng

Các bước thực hiện của một cuộc tấn công

- Một cuộc tấn công có năm bước: Do thám, dò quét, tấn công, duy trì cuộc tấn công, và xóa dấu vết.

Các khái niệm dò quét

Các khái niệm dò quét

- Dò quét là quá trình thu thập thông tin chi tiết bổ sung về mục tiêu bằng cách sử dụng các kỹ thuật trinh sát tích cực và phức tạp.
- Dò quét mạng đề cập đến một tập hợp các thủ tục được sử dụng để xác định máy chủ, cổng và dịch vụ trong mạng.
- Đây là một trong những giai đoạn quan trọng nhất của việc thu thập thông tin tình báo đối với kẻ tấn công, cho phép họ tạo ra hồ sơ của tổ chức mục tiêu.
- Trong quá trình dò quét, kẻ tấn công cố gắng thu thập thông tin, bao gồm các địa chỉ IP cụ thể có thể được truy cập qua mạng, của hệ điều hành và kiến trúc của mục tiêu, và các dịch vụ đang chạy trên mỗi máy tính.

Các khái niệm dò quét

- Mục đích của việc quét là để khám phá các kênh giao tiếp có thể khai thác, thăm dò càng nhiều càng tốt và theo dõi những kênh đáp ứng hoặc hữu ích cho nhu cầu cụ thể của kẻ tấn công.
- Trong giai đoạn dò quét của một cuộc tấn công, kẻ tấn công cố gắng tìm nhiều cách khác nhau để xâm nhập vào trong một hệ thống mục tiêu.
- Các kẻ tấn công cũng cố gắng tìm hiểu xem có bất kỳ lỗi cấu hình nào trong đó không.
- Sau đó, kẻ tấn công sử dụng thông tin thu được trong quá trình dò quét để xây dựng chiến lược tấn công.

Các loại dò quét

Các loại dò quét

- Network scanning:
  - Liệt kê địa chỉ IP.
  - Network scanning là quá trình xác định các máy đang chạy trong hệ thống mạng mục tiêu.
  - Quá trình này bao gồm cả việc tấn công mạng hoặc đánh giá bảo mật mạng.

Các loại dò quét

- Port scanning:
  - Liệt kê các cổng được mở và các dịch vụ.
  - Port scanning là quá trình của kiểm tra các dịch vụ đang chạy trên máy tính mục tiêu bằng cách gửi một chuỗi tin nhắn để phân tích các kết quả trả về.
  - Port scanning liên quan đến việc kết nối hoặc thăm dò các cổng TCP và UDP trên hệ thống đích để xác định xem các dịch vụ đang chạy hay đang ở trạng thái lắng nghe.
  - Trạng thái lắng nghe cung cấp thông tin về hệ điều hành và ứng dụng hiện đang được sử dụng.
  - Đôi khi, các dịch vụ đang hoạt động đang lắng nghe có thể cho phép người dùng trái phép truy cập đến hệ thống cấu hình sai hoặc khởi chạy phần mềm có lỗ hổng.

Các loại dò quét

- Vulnerability scanning:
  - Liệt kê các lỗ hổng bảo mật đã biết đang tồn tại trong hệ thống mục tiêu.
  - Vulnerability scanning là một phương pháp được dùng để kiểm tra xem hệ thống có tồn tại lỗ hổng bảo mật nào hay không.
  - Một trình dò quét lỗ hổng bảo mật bao gồm một công cụ dò quét và danh mục các lỗ hổng bảo mật biết trước cùng với cách khai thác các lỗ hổng này.
  - Kết quả của quá trình này giúp ích rất nhiều cho kẻ tấn công trong việc tìm cách tấn công hệ thống mục tiêu.
  - Nó cũng đồng thời giúp nhà quản trị hệ thống biết cách vá các lỗ hổng được phát hiện

Mục tiêu của dò quét mạng (Network scanning)

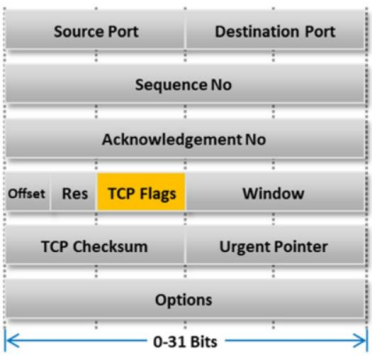
Mục tiêu của dò quét mạng (Network scanning)

- Một khi có nhiều thông tin về hệ thống mục tiêu, chúng ta có nhiều cơ hội để biết các nguy cơ bảo mật trên chúng. Điều này giúp ích rất nhiều cho cả quá trình tấn công và phòng thủ. Sau đây là một số mục tiêu của quá trình dò quét mạng:
  - Xác định các máy tính đang chạy trong hệ thống mạng. Xác định địa chỉ IP và các cổng đang mở trên các máy tính này. Việc biết được danh sách các cổng đang mở sẽ giúp biết được danh sách các dịch vụ mạng đang chạy trên máy tính mục tiêu cũng như khả năng thâm nhập vào trong máy tính này.
  - Xác định hệ điều hành và kiến trúc hệ thống của mục tiêu. Một khi biết được phiên bản của hệ điều hành và kiến trúc hệ thống, kẻ tấn công có thể suy ra các nguy cơ bảo mật tương ứng.
  - Xác định các dịch vụ đang chạy hoặc đang ở trạng thái lắng nghe trong hệ thống mục tiêu. Dựa trên thông tin này, chúng ta có thể biết được các lỗ hổng tương ứng cũng như cách khai thác chúng để xâm nhập vào máy tính mục tiêu.
  - Xác định ứng dụng và phiên bản của một dịch vụ cụ thể.
  - Xác định lỗ hổng bảo mật của bất kỳ hệ thống mạng nào. Thông tin này giúp kẻ tấn công có thể tấn công hệ thống mục tiêu thông qua các kỹ thuật tấn công khác nhau.

13

Các cờ trong gói tin TCP

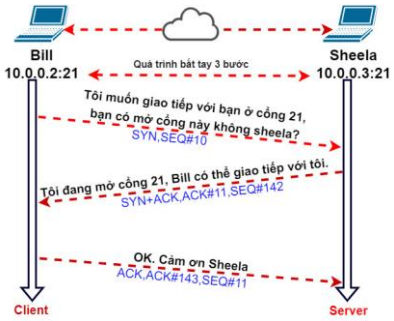
- Các cờ trong gói tin TCP giúp xác định được loại gói tin.
- Thông tin này giúp ích trong việc phân tích kết quả của quá trình dò quét mạng.
- TCP header chứa các cờ dùng để điều khiển quá trình trao đổi dữ liệu qua kết nối TCP.
- Có bốn cờ bao gồm SYN, ACK, FIN, và RST tương ứng với quá trình thiết lập, duy trì và kết thúc một kết nối.
- Bên cạnh đó chúng ta có hai cờ khác là PSH và URG cung cấp các chỉ thị cho hệ thống.
- Kích thước của mỗi cờ là một bit.
- Trong header của gói tin, có sáu bit cho phần TCP flags.
- Khi giá trị tại bit nào bằng 1 thì tự động cờ đó được bật

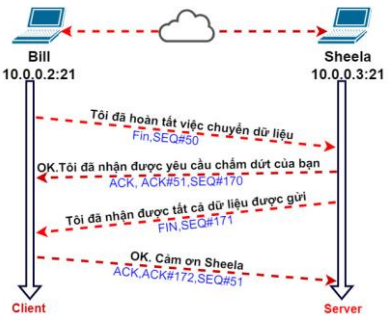


14

Các cờ trong gói tin TCP

- Quy tắc bắt tay ba bước





Các công cụ dò quét

Các công cụ dò quét

- Nmap

```
┌──(root💀kali)-[~]
└─# nmap -A -p 80,443 10.0.2.11
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-23 00:18 EDT
Nmap scan report for 10.0.2.11
Host is up (0.00038s latency).

PORT    STATE  SERVICE VERSION
80/tcp  open   http    Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Apache2 Debian Default Page: It works
443/tcp closed https
MAC Address: 00:0C:29:78:DA:F2 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.38 ms 10.0.2.11

OS and Service detection performed. Please report any incorrect resul
ts at https://nmap.org/submit/ .
```


Các công cụ dò quét

- Hping
  - Hping là công cụ dò quét mạng có giao diện dòng lệnh.
  - Nó cho phép người dùng tạo và gửi các gói tin có cấu trúc theo chủ đích để thực hiện đánh giá bảo mật, kiểm tra tường lửa, kiểm tra đường đi của gói tin, phát hiện thông tin hệ điều hành của máy tính mục tiêu, dự đoán thời gian chạy của máy tính mục tiêu và các chức năng khác.

```
┌──(root💀kali)-[~]
└─# hping3 -A 10.0.2.11 -p 80
HPING 10.0.2.11 (eth0 10.0.2.11): A set, 40 headers + 0 data bytes
len=46 ip=10.0.2.11 ttl=64 DF id=0 sport=80 flags=R seq=0 win=0 rtt=7
.8 ms
len=46 ip=10.0.2.11 ttl=64 DF id=0 sport=80 flags=R seq=1 win=0 rtt=7
.3 ms
len=46 ip=10.0.2.11 ttl=64 DF id=0 sport=80 flags=R seq=2 win=0 rtt=3
.0 ms
len=46 ip=10.0.2.11 ttl=64 DF id=0 sport=80 flags=R seq=3 win=0 rtt=6
.0 ms
len=46 ip=10.0.2.11 ttl=64 DF id=0 sport=80 flags=R seq=4 win=0 rtt=5
.5 ms
```

Các công cụ dò quét

- Hping
  - Một số tính năng chính của Hping như sau:
    - Xác định máy tính nào đó có đang chạy hay không, thậm chí khi máy tính đó chặn gói tin ICMP.
    - Xác định các cổng đang mở cũng như kiểm tra hiệu năng thông qua các giao thức khác nhau, kích thước gói tin khác nhau.
    - Xác định các cổng đang mở trên các máy tính đặt phía sau tường lửa.
    - Xác định thông tin hệ điều hành trên máy mục tiêu.
    - Giám sát hoạt động chồng giao thức TCP/IP.
  - Một số tính năng của hping3
    - ICMP Ping: hping3 -1 10.0.0.1
    - ACK Scan trên cổng 80: hping3 –A 10.0.0.1 –p 80
    - UDP Scan trên cổng 80: hping3 -2 10.0.0.1 –p 80
    - SYN Scan trên cổng 50-60: hping3 -8 50-60 –S 10.0.0.1 –V
    - FIN, PUSH, URG Scan trên cổng 80: hping3 –F –P –U 10.0.0.1 –p 80
    - SYN flooding: hping3 –S 192.168.1.1 –a 192.168.1.254 –p 22 --flood

Các kỹ thuật dò quét phổ biến

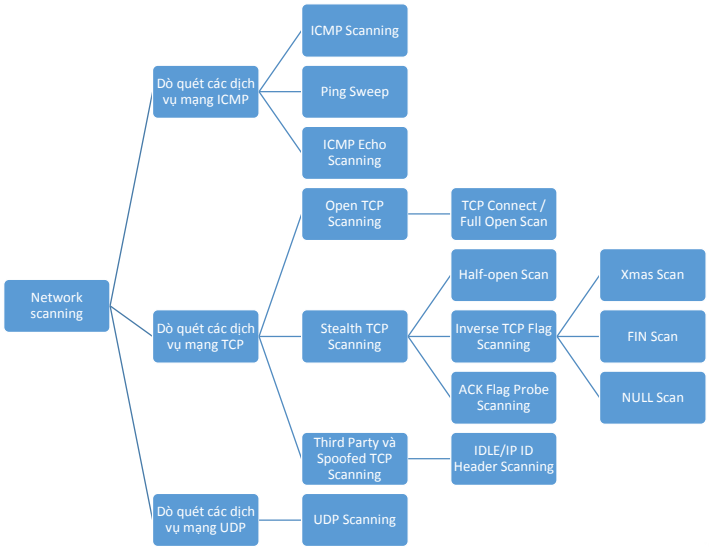
Các kỹ thuật dò quét phổ biến

- Scanning là quá trình thu thập thông tin trên các thiết bị đang hoạt động.
- Kỹ thuật dò quét cổng (port scanning) giúp kẻ tấn công xác định được các cổng đang mở trên máy tính mục tiêu.
- Trong khi đó, các quản trị viên dùng port scanning để kiểm tra các chính sách bảo mật của hệ thống mạng của họ.
- Điều này giúp họ phát hiện các nguy cơ bảo mật sớm và có kế hoạch vá các lỗ hổng bảo mật kịp thời.

Các kỹ thuật dò quét phổ biến

- Scanning là quá trình thu thập thông tin trên các thiết bị đang hoạt động.
- Kỹ thuật dò quét cổng (port scanning) giúp kẻ tấn công xác định được các cổng đang mở trên máy tính mục tiêu.
- Trong khi đó, các quản trị viên dùng port scanning để kiểm tra các chính sách bảo mật của hệ thống mạng của họ.
- Điều này giúp họ phát hiện các nguy cơ bảo mật sớm và có kế hoạch vá các lỗ hổng bảo mật kịp thời.
  - Bước đầu tiên của quá trình dò quét mạng là kiểm tra các máy tính đang hoạt động.
  - Bước tiếp theo là kiểm tra các cổng được mở trên các máy tính đang chạy.
  - Bước cuối cùng là xác định các lỗ hổng bảo mật nếu có.

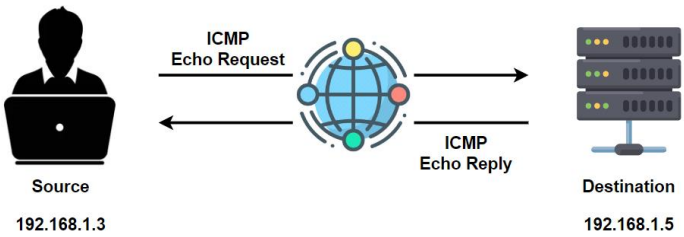
Các kỹ thuật dò quét phổ biến



ICMP Scanning

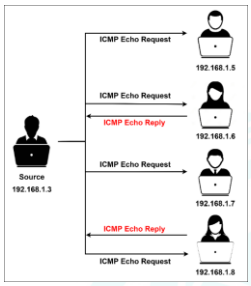
- Chúng ta dùng ICMP Scanning để gửi gói tin ICMP đến máy tính mục tiêu để thu thập các thông tin cần thiết về nó.
- Việc sử dụng ICMP Scanning rất hữu ích trong việc xác định xem các máy tính trong mạng có đang chạy hay không. (Nmap dùng tùy chọn –P để thực hiện việc ICMP Scanning).
- Người dùng cũng có thể tăng số lượng lệnh ping một cách đồng thời bằng cách sử dụng tùy chọn –L.
- Việc scan thông qua lệnh ping này bao gồm việc gửi yêu cầu ECHO (ECHO request) đến một máy. Nếu như máy đó đang chạy, nó sẽ trả về một gói ICMP ECHO phản hồi (ICMP ECHO reply). Cách này có ích trong việc định vị máy đang chạy cũng như kiểm tra khả năng gói tin ICMP có qua được tường lửa hay không

ICMP Scanning

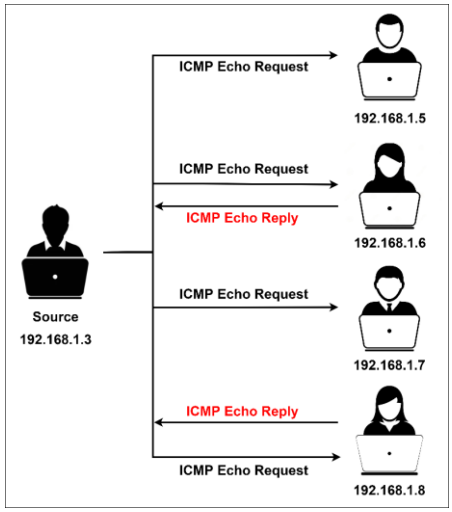


Ping Sweep

- Ping Sweep hay còn được gọi là ICMP Sweep.
- Nó là kỹ thuật dò quét mạng cơ bản để xác định danh sách các máy đang chạy trong hệ thống mạng.
- Thay vì ping đến một máy đích như cách ICMP ping làm, thì Ping Sweep ping cùng lúc đến hàng loạt địa chỉ khác nhau.
- Các địa chỉ đích có thể là một IP, một nhóm địa chỉ IP, thậm chí là một phân đoạn mạng.
- Một số công cụ Ping Sweep như sau:
  - SolarWinds Engineer's Toolset (http://www.solarwinds.com)
  - NetScanTools Pro (https://www.netscantools.com)
  - Colasoft Ping Tool (http://www.colasoft.com)
  - Visual Ping Tester (http://www.pingtester.net)



Ping Sweep



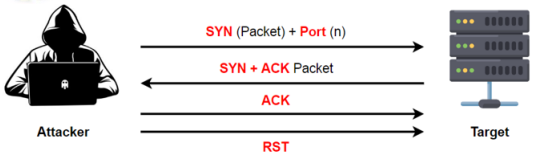
ICMP Echo Scanning

- Dò quét ICMP echo tiến hành ping tất cả các máy tính trong mạng mục tiêu để phát hiện các máy tính đang chạy.
- Kẻ tấn công gửi các gói tin ICMP đến địa chỉ Broadcast hoặc địa chỉ mạng để lắng nghe các gói tin phản hồi.
- Các máy tính đang chạy sẽ gửi các gói ICMP ECHO REPLY đến địa chỉ nguồn của gói tin ICMP Echo.
- Hệ điều hành Linux dùng ICMP echo scanning.
- Chồng giao thức TCP/IP trên hệ điều hành này được thiết kế để phản hồi cho các yêu cầu gói tin ICMP ECHO gửi đến địa chỉ Broadcast.
- Kỹ thuật này không hoạt động trên hệ điều hành Windows vì chồng giao thức TCP/IP trên chúng không phản hồi cho các gói tinh ICMP gửi trực tiếp đến địa chỉ Broadcast

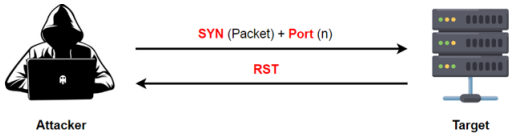
TCP Connect/ Full Open Scan

- Với loại dò quét này, lời gọi hàm hệ thống connection() thử mở một kết nối tới từng cổng trên máy mục tiêu.
  - Nếu cổng đang lắng nghe, hàm connect() sẽ trả về một kết nối thành công với địa chỉ máy tính và cổng cụ thể. Ngược lại, nó trả về thông báo lỗi thông báo rằng cổng này không thể kết nối được.
- TCP Connect scan hoàn tất quy trình bắt tay ba bước với máy tính mục tiêu.
  - Trong quy trình bắt tay ba bước, máy gửi thực hiện việc gửi gói tin SYN, sau đó máy nhận xác nhận bằng gói tin SYN+ACK. Đến lược mình, máy gửi xác nhận bằng gói tin ACK để hoàn tất một kết nối. Khi quá trình bắt tay kết thúc, máy thực hiện dò quét tiến hành gửi gói RST để kết thúc kết nối. Ưu điểm của loại dò quét này là không cần quyền quản trị.
- Như vậy, nếu kẻ tấn công gửi gói SYN đến máy nạn nhân ở cổng nào đó mà nhận được gói SYN+ACK thì chứng tỏ cổng đó đang mở. Ngược lại, nếu họ nhận được gói RST thì chứng tỏ cổng đó đang đóng.

TCP Connect/ Full Open Scan



Hình 3.9. Kết quả quét cổng đang mở



Hình 3.10. Kết quả quét cổng đang đóng

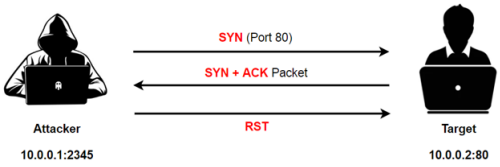
```
┌──(root💀kali)-[~]
└─# nmap -sT -v 10.0.2.11
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-23 08:09 EDT
Initiating ARP Ping Scan at 08:09
Scanning 10.0.2.11 [1 port]
Completed ARP Ping Scan at 08:09, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:09
Completed Parallel DNS resolution of 1 host. at 08:09, 13.00s elapsed
Initiating Connect Scan at 08:09
Scanning 10.0.2.11 [1000 ports]
Discovered open port 80/tcp on 10.0.2.11
Completed Connect Scan at 08:09, 0.09s elapsed (1000 total ports)
Nmap scan report for 10.0.2.11
Host is up (0.00084s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:78:DA:F2 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 13.29 seconds
           Raw packets sent: 1 (28B) | Rcvd: 1 (28B)
```

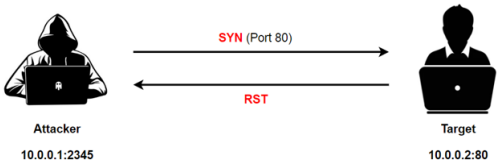
Hình 3.11. Hình minh họa kết quả dò quét bằng Nmap

Stealth Scan (Half-open Scan)

- Stealth Scan giống như Full-open Scan, tuy nhiên máy dò quét sẽ gửi gói RST ngay khi nhận gói SYN+ACK từ máy mục tiêu.
- Điều này làm cho kết nối bị ngắt trước khi hoàn tất quá trình bắt tay ba bước.
- Đó là lý do nó có tên gọi là Half-open Scan.

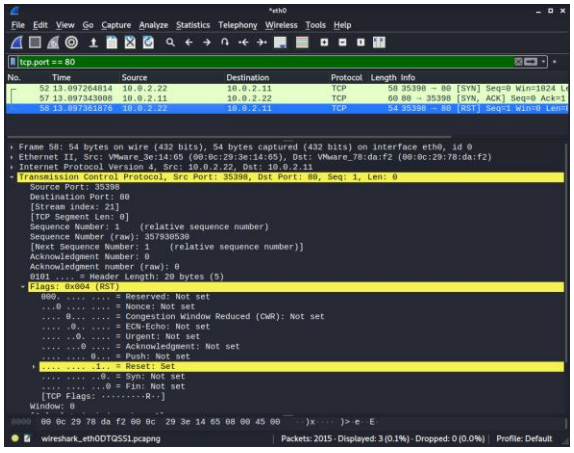


Hình 3.15. Minh họa kết quả dò thấy cổng đang mở



Hình 3.16. Minh họa kết quả dò quét cổng đang đóng

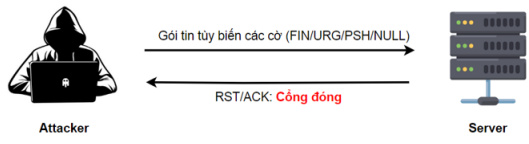
Stealth Scan (Half-open Scan)



Inverse TCP Flag Scanning

- Kẻ tấn công gởi các gói tin tùy biến với các cờ FIN, URG, PSH được bật hoặc không có cờ nào (trong trường hợp không có cờ nào được bật thì gọi là Null Scan).
- Khi cổng mục tiêu mở, kẻ tấn công không nhận được bất kỳ phản hồi nào.
- Ngược lại, khi cổng mục tiêu bị đóng, kẻ tấn công sẽ nhận được gói RST.

Hình 3.19. Minh họa kết quả dò quét cổng đang mở



Hình 3.20.Minh họa kết quả dò quét cổng đang đóng

Inverse TCP Flag Scanning

- Các chiến lược cấu hình các cờ trong việc tùy biến các gói tin như sau:
  - Gói tin bật cờ FIN
  - Gói tin bật cả ba cờ FIN, URG, và PUSH, gọi là XMAS Scan
  - Gói không bật cờ nào, gọi là Null Scan
  - Gói tin bật cờ SYN/ACK

```
┌──(root㉿kali)-[~]
└─# nmap -sF -v 10.0.2.11
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-23 09:07 EDT
Initiating ARP Ping Scan at 09:07
Scanning 10.0.2.11 [1 port]
Completed ARP Ping Scan at 09:07, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:07
Completed Parallel DNS resolution of 1 host. at 09:07, 13.00s elapsed
Initiating FIN Scan at 09:07
Scanning 10.0.2.11 [1000 ports]
Completed FIN Scan at 09:07, 1.25s elapsed (1000 total ports)
Nmap scan report for 10.0.2.11
Host is up (0.00013s latency).
Not shown: 999 closed ports
PORT   STATE         SERVICE
80/tcp open|filtered http
MAC Address: 00:0C:29:78:DA:F2 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 14.47 seconds
           Raw packets sent: 1002 (40.068KB) | Rcvd: 1000 (39.988KB)
```

```
.... 0000 0010 1001 = Flags: 0x029 (FIN, PSH, URG)
   000. .... .... = Reserved: Not set
   ...0 .... .... = Nonce: Not set
   .... 0... .... = Congestion Window Reduced (CWR): Not set
   .... .0.. .... = ECN-Echo: Not set
   .... ..1. .... = Urgent: Set
   .... ...0 .... = Acknowledgment: Not set
   .... .... 1... = Push: Set
   .... .... .0.. = Reset: Not set
   .... .... ..0. = Syn: Not set
   .... .... ...1 = Fin: Set
```

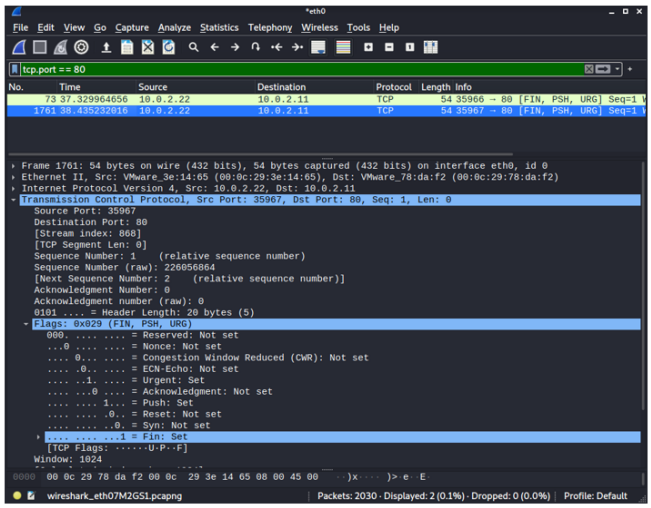
Hình 3.21. Minh họa kết quả dò quét bằng gói tin bật cờ FIN

Xmas Scanning

- Xmas Scanning giống như Inverse TCP Flag Scanning, tuy nhiên gói tin tùy biến bật cả ba cờ FIN, URG và PUSH.
- Khi cổng mục tiêu mở, kẻ tấn công không nhận được bất kỳ phản hồi nào.
- Ngược lại, khi cổng mục tiêu bị đóng, kẻ tấn công sẽ nhận được gói RST

Hình 3.24. Minh họa kết quả dò quét Xmas trường hợp cổng mở

Xmas Scanning

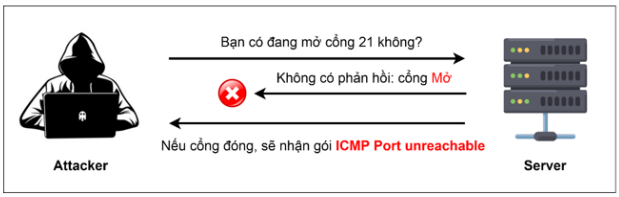


Hình 3.27. Kết quả bắt gói tin trong quá trình dò quét Xmas cổng 80 mở

UDP Scanning

- UDP Scanning sử dụng giao thức UDP thay vì giao thức TCP.
- Như vậy, không thể dựa trên quy trình bắt tay ba bước.
- Trong lĩnh vực dò quét mạng, giao thức UDP có nhiều thách thức hơn so với giao thức TCP.
- Bởi vì, khi chúng ta gửi gói tin bằng giao thức UDP, chúng ta không thể xác nhận được máy tính đó đang chạy không, hay đang bị tắt, hay bị lọc bỏ gói tin bởi tường lửa.
- Tuy nhiên, chúng ta có thể sử dụng ICMP để kiểm tra xem một cổng có đang mở hay không.
- Nếu chúng ta gửi một gói tin UDP đến một cổng mà không có ứng dụng nào đang dùng nó, chúng ta sẽ nhận được thông báo cổng đó không thể truy cập.
- Nếu bất kỳ cổng nào trả về thông báo lỗi ICMP này, chứng tỏ nó đang bị đóng.
- Ngược lại, nếu không nhận bất kỳ thông báo nào, chứng tỏ cổng đó đang được mở.

UDP Scanning



Hình 3.29. Minh họa kết quả dò quét UDP

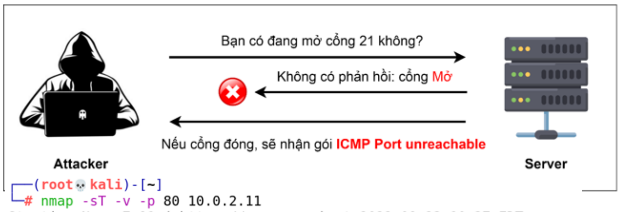
```
┌──(root💀kali)-[~]
└─# nmap -sU -v -p 80 10.0.2.11
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-23 10:34 EDT
Initiating ARP Ping Scan at 10:34
Scanning 10.0.2.11 [1 port]
Completed ARP Ping Scan at 10:34, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:34
Completed Parallel DNS resolution of 1 host. at 10:34, 13.01s elapsed
Initiating UDP Scan at 10:34
Scanning 10.0.2.11 [1 port]
Completed UDP Scan at 10:34, 0.04s elapsed (1 total ports)
Nmap scan report for 10.0.2.11
Host is up (0.00040s latency).

PORT   STATE  SERVICE
80/udp closed http
MAC Address: 00:0C:29:78:DA:F2 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds
           Raw packets sent: 2 (70B) | Rcvd: 2 (98B)
```

Hình 3.30. Kết quả dò quét UDP bằng Nmap

UDP Scanning




```
┌──(root💀kali)-[~]
└─# nmap -sT -v -p 80 10.0.2.11
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-23 10:37 EDT
Initiating ARP Ping Scan at 10:37
Scanning 10.0.2.11 [1 port]
Completed ARP Ping Scan at 10:37, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:37
Completed Parallel DNS resolution of 1 host. at 10:37, 13.00s elapsed
Initiating Connect Scan at 10:37
Scanning 10.0.2.11 [1 port]
Discovered open port 80/tcp on 10.0.2.11
Completed Connect Scan at 10:37, 0.00s elapsed (1 total ports)
Nmap scan report for 10.0.2.11
Host is up (0.00030s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:78:DA:F2 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 13.20 seconds
           Raw packets sent: 1 (28B) | Rcvd: 1 (28B)
```

Hình 3.32. Kết quả dò quét bằng Full-open Scan trên cổng 80 TCP

```
┌──(root💀kali)-[~]
└─# nmap -sU -v -p 80 10.0.2.11
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-23 10:34 EDT
Initiating ARP Ping Scan at 10:34
Scanning 10.0.2.11 [1 port]
Completed ARP Ping Scan at 10:34, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:34
Completed Parallel DNS resolution of 1 host. at 10:34, 13.01s elapsed
Initiating UDP Scan at 10:34
Scanning 10.0.2.11 [1 port]
Completed UDP Scan at 10:34, 0.04s elapsed (1 total ports)
Nmap scan report for 10.0.2.11
Host is up (0.00040s latency).

PORT   STATE  SERVICE
80/udp closed http
MAC Address: 00:0C:29:78:DA:F2 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds
           Raw packets sent: 2 (70B) | Rcvd: 2 (98B)
```

Hình 3.30. Kết quả dò quét UDP bằng Nmap

Xác định phiên bản hệ điều hành và ứng dụng

Xác định phiên bản hệ điều hành và ứng dụng

- Banner grabbing là một phương pháp được sử dụng bởi những kẻ tấn công và đội bảo mật để lấy thông tin về hệ thống máy tính và dịch vụ chạy trên các cổng mở.
- Banner ở đây là một văn bản được hiển thị bởi máy chủ lưu trữ cung cấp các chi tiết như loại và phiên bản phần mềm đang chạy trên hệ thống hoặc máy chủ.
- Các thông tin này, tạo lợi thế cho tội phạm mạng trong các cuộc tấn công mạng.
- Kẻ tấn công có thể sử dụng công cụ OSINT (Open-source intelligence) để lấy các thông tin phiên bản hệ điều hành và ứng dụng theo cách thủ công hoặc tự động.
- Thu thập danh sách tên và phiên bản của ứng dụng và hệ điều hành là một trong những bước thiết yếu trong cả môi trường tấn công cũng như tấn công thử nghiệm.
- Có hai phương thức dùng để thu thập danh sách và phiên bản hệ điều hành và ứng dụng:
  - Thu thập thông tin thông qua các dịch vụ truyền tập tin như FTP. Ví dụ cụ thể như: kẻ tấn công có thể dùng dịch vụ FTP để tải tập tin /bin/ls để kiểm tra kiến trúc của hệ thống.
  - Ngoài ra, họ cũng có thể sử dụng các thông tin từ các gói tin TCP để dự đoán phiên bản của hệ điều hành và ứng dụng

Xác định phiên bản hệ điều hành và ứng dụng

```
┌──(root💀kali)-[~]
└─# nmap -A 10.0.2.11
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-26 04:43 EDT
Nmap scan report for 10.0.2.11
Host is up (0.00036s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Apache2 Debian Default Page: It works
MAC Address: 00:0C:29:78:DA:F2 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
```

Hình 3.42. Kết quả xác định phiên bản máy mục tiêu bằng Nmap

Xác định phiên bản hệ điều hành và ứng dụng

- Có hai loại kỹ thuật xác định phiên bản hệ điều hành và ứng dụng, bao gồm: kỹ thuật chủ động và kỹ thuật thụ động.
  - Kỹ thuật xác định phiên bản chủ động:
    - kỹ thuật này áp dụng nguyên tắc rằng chồng giao thức IP của hệ điều hành có một cách duy nhất để phản hồi cho các yêu cầu nhận được. Trong kỹ thuật này, kẻ tấn công gửi một số gói tin có chủ đích đến máy tính mục tiêu. Các phản hồi được so sánh với cơ sở dữ liệu các dấu hiệu xác định phiên bản có trước.
  - Kỹ thuật xác định phiên bản thụ động:
    - kỹ thuật này dựa trên kết quả của việc nghe lén các gói tin liên quan đến thông tin của phiên bản hệ điều hành và ứng dụng thay vì chủ động gửi gói tin đến máy tính mục tiêu. Các thông tin có thể phục vụ cho kỹ thuật này bao gồm thông tin từ các thông báo lỗi, thông tin từ các gói tin mạng, thông tin từ các phần mở rộng của các trang web. Ví dụ: trang web có phần mở rộng là .aspx, chúng ta có thể suy đoán ứng dụng web này được quản lý bởi dịch vụ IIS Server và hệ điều hành là Windows.

Xác định phiên bản hệ điều hành và ứng dụng

- Như vậy, chúng ta cũng có thể sử dụng các cách sau để giảm thiểu nguy cơ bị kẻ tấn công dò quét thông tin danh sách và phiên bản các ứng dụng và hệ điều hành:
  - Cố tình cấu hình cung cấp thông tin phiên bản không chính xác khi có yêu cầu từ phía kẻ tấn công. Ví dụ có thể dùng công cụ ServerMask [9] để thay đổi thông tin liên quan đến phiên bản, hoặc cấu hình thông tin trong mô-đun mod_header của tập tin httpd.conf để thay đổi tên máy chủ.
  - Tắt các dịch vụ không cần thiết.
  - Cấu hình để ẩn thông tin phần mở rộng của các trang web. Ví dụ thay đổi tất cả các phần mở rộng như .asp, aspx, .html sang .online.

Các phương pháp giảm thiểu nguy cơ dò quét mạng

Các phương pháp giảm thiểu nguy cơ dò quét mạng

- Cấu hình tường lửa và trình phát hiện xâm nhập để phát hiện và lọc bỏ các gói tin từ các cuộc dò quét mạng.
- Các tường lửa phải có đủ khả năng phát hiện các gói tin tùy biến được gửi bởi kẻ tấn công trong các quá trình dò quét mạng. Tường lửa phải có khả năng lọc bỏ các gói tin này.
- Chạy các công cụ dò quét mạng để dò quét kiểm thử nhằm đánh giá khả năng phát hiện các hành vi dò quét mạng của tường lửa.
- Đảm bảo rằng hệ điều hành của các bộ định tuyến, trình phát hiện xâm nhập, tường lửa được cập nhật phiên bản mới nhất.
- Cấu hình các tường lửa để đảm bảo nó có thể bảo vệ mạng máy tính chống lại quá trình dò quét cổng, ngập lụt gói tin SYN.
- Kẻ tấn công có thể dùng các công cụ để dò quét và thu thập các thông tin liên quan đến hệ điều hành của máy mục tiêu. Do đó cần thiết phải triển khai các hệ thống phát hiện xâm nhập trong các trường hợp này. Chúng ta có thể cài đặt các công cụ phát hiện xâm nhập như Snort [10].
- Chỉ mở các cổng cần thiết, đóng tất cả các cổng không cần thiết, hoặc thiết lập chính sách trên tường lửa để lọc tất cả các cổng không cần thiết.
- Kiểm tra không gian địa chỉ IP bằng cách dùng TCP hoặc UDP scan để đảm bảo cấu hình mạng đúng.
- Đảm bảo các luật liên quan đến anti-scanning cà anti-spoofing được thiết lập.

Dò quét kiểm thử

Thứ tự	Nội dung	Ghi chú
1	Dò tìm máy tính đang chạy	Dùng công cụ như Nmap, Angry IP Scanner,…
2	Dò quét các cổng	Dùng công cụ như Nmap, NetScanTools Pro, …
3	Dò quét phía trước tường lửa và trình phát hiện xâm nhập	Dùng các kỹ thuật như phân mảnh gói tin, định tuyến nguồn, …
4	Thu thập thông tin hệ điều hành	Gửi các gói tin tùy biến và phân tích kết quả phản hồi.
5	Vẽ sơ đồ mạng	Dùng các công cụ như Network Topology Mapper, OpManager,…
6	Ghi nhận các phát hiện	

Câu hỏi ôn tập

Câu hỏi ôn tập

- **Câu 1:** Trình bày các cờ trong gói tin TCP?
- **Câu 2:** Giải thích nguyên tắc hoạt động của ICMP Scanning?
- **Câu 3:** Trình bày cách thức hoạt động của Full Open Scanning?
- **Câu 4:** So sánh sự giống và khác nhau giữa Inverse TCP Flag Scanning và Xmas Scanning?
- **Câu 5:** Trình bày các kỹ thuật dò quét trong các trường hợp các máy mục tiêu được bảo vệ bởi tường lửa và trình phát hiện xâm nhập?
- **Câu 6:** Trình bày các phương pháp giúp giảm thiểu nguy cơ dò quét mạng?
- **Câu 7:** Trình bày các bước của quy trình dò quét kiểm thử?

Câu hỏi trắc nghiệm

- Câu 3.1:
- Có mấy bước chính để thực hiện một cuộc tấn công?
  - A. 3
  - B. 4
  - C. 5
  - D. 6

Câu hỏi trắc nghiệm

- Câu 3.2:
- Dò quét là bước thứ mấy trong đợt tấn công?
  - A. 1
  - B. 2
  - C. 3
  - D. 4

Câu hỏi trắc nghiệm

- Câu 3.3:
- Phát biểu nào sau đây đúng?
  - Phát biểu A: Port scanning là quá trình của kiểm tra các dịch vụ đang chạy trên máy tính mục tiêu bằng cách gửi một chuỗi tin nhắn để phân tích các kết quả trả về.
  - Phát biểu B: Network scanning là quá trình xác định các máy đang chạy trong hệ thống mạng mục tiêu
  - A. Phát biểu A đúng, Phát biểu B sai
  - B. Phát biểu B sai, Phát biểu B đúng
  - C. Cả hai phát biểu A và B đúng
  - D. Cả hai phát biểu A và B sai

Câu hỏi trắc nghiệm

- Câu 3.4:
- Cờ nào được sử dụng để xác nhận việc nhận gói tin thành công?
  - A. SYN
  - B. FIN
  - C. RST
  - D. ACK

Câu hỏi trắc nghiệm

- Câu 3.5:
- Kỹ thuật dò quét nào ping cùng lúc đến hàng loạt địa chỉ khác nhau?
  - A. Ping Sweep
  - B. ICMP Scanning
  - C. Full Open Scan
  - D. Half Open Scan

Cảm ơn!