Trường Đại học Bách Khoa Hà Nội
Viện Công nghệ thông tin và Truyền thông

Báo cáo bài tập lớn môn học :
AN TOÀN VÀ BẢO MẬT THÔNG TIN

Đề tài: Network Scanning

Giảng viên hướng dẫn: **Đỗ Văn Uy**

Nhóm sinh viên thực hiện: ***Nhóm 8***
Nguyễn Văn Sao
Ngô Anh Huy
Nguyễn Văn Trung
Nguyễn Đức Nghị

Hà Nội, tháng 11 năm 2010

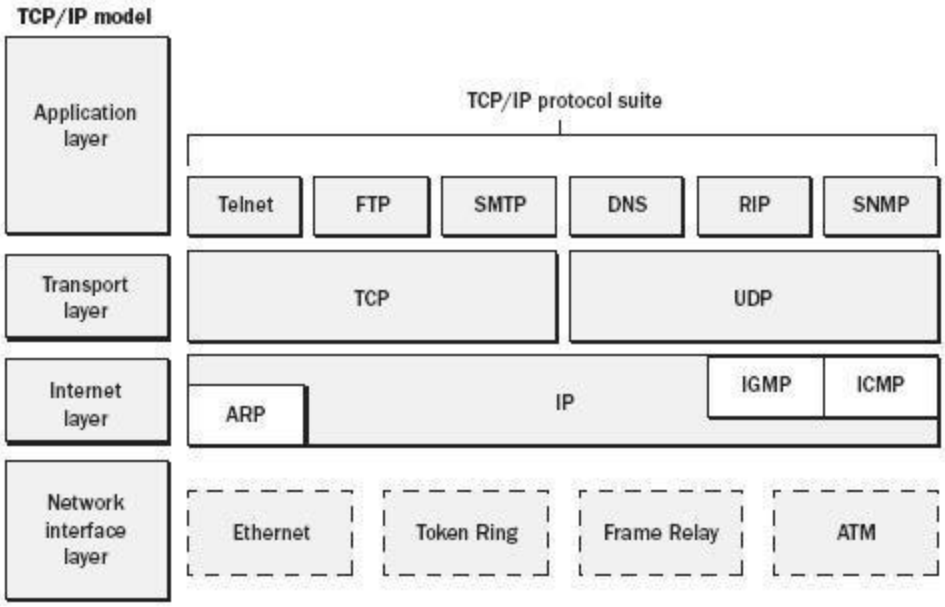
Mục lục

A. Mô hình TCP/IP 2
B. Network Scanning 4
I. Network Mapping: 4
1. ICMP scanning 4
2. TCP SYN ping, TCP ACK ping 5
II. Port scanning 5
1. Port là gì? 5
2. Một số phương pháp scan port phổ biến: 6
_Vanilla TCP connect scanning 6
_ Stealth scanning: 7
_IDLE scanning 9
_UDP scanning: 10
III. Service and version detection 11
IV. OS detection: 11

A. Mô hình TCP/IP

TCP/IP là bộ giao thức truyền thông mà Internet và hầu hết các mạng máy tính thương mại đang sử dụng. được phát triển bởi bộ quốc phòng Mỹ

Mô hình TCP/IP bao gồm 4 tầng:



<u>Tầng ứng dụng (Application Layer):</u>

Gồm nhiều giao thức cung cấp cho các ứng dụng người dùng. Được sử dụng để định dạng và trao đổi thông tin người dùng.

1 số giao thức thông dụng trong tầng này là:

- SNMP (Simple Network Management Protocol): Giao Thức Quản Lý Mạng Đơn Giản
- FTP (File Transfer Protocol): Giao Thức Truyền Tập Tin
- TFTP (Trivial File Transfer Protocol): Giao thức truyền tập tin bình thường
- SMTP (Simple Mail Transfer Protocol): giao thức truyền thư đơn giản
- TELNET

<u>Tầng giao vận (Transport Layer):</u>

Có trách nhiệm thiết lập phiên truyền thông giữa các tiến trình chạy

trên các máy tính và quy định cách truyền dữ liệu.

2 giao thức chính trong tầng này gồm:

- UDP (User Datagram Protocol): UDP cung cấp các kênh truyền thông phi kết nối nên nó không đảm bảo truyền dữ liệu 1 cách tin cậy. Các ứng dụng dùng UDP thường chỉ truyền những gói có kích thước nhỏ, độ tin cậy dữ liệu phụ thuộc vào từng ứng dụng
- TCP (Transmission Control Protocol): Ngược lại với UDP, TCP cung cấp các kênh truyền thông hướng kết nối và đảm bảo truyền dữ liệu 1 cách tin cậy. TCP thường truyền các gói tin có kích thước lớn và yêu cầu phía nhận xác nhận về các gói tin đã nhận.

<u>Tầng liên mạng (Internet Layer):</u>

Nằm bên trên tầng giao diện mạng. Tầng này có chức năng gán địa chỉ, đóng gói và định tuyến (route) dữ liệu. Tầng mạng không đảm bảo độ tin cậy trong truyền dữ liệu, tức là gói tin có thể bị mất hoặc đến đích không đúng thứ tự. Tuy nhiên, tầng mạng cung cấp các dịch vụ chọn đường (route) tối ưu nhất giữa 2 nút trên mạng

4 giao thức quan trọng nhất trong tầng này gồm:

- IP (Internet Protocol): Có chức năng gán địa chỉ cho dữ liệu trước khi truyền và định tuyến chúng tới đích.
- ARP (Address Resolution Protocol): Có chức năng biên dịch địa chỉ IP của máy đích thành địa chỉ MAC.
- ICMP (Internet Control Message Protocol): Có chức năng thông báo lỗi trong trường hợp truyền dữ liệu bị hỏng.
- IGMP (Internet Group Management Protocol): Có chức năng điều khiển truyền đa hướng (Multicast)

<u>Tầng giao diện mạng (Network Interface Layer):</u>

Tầng giao diện mạng có trách nhiệm đưa dữ liệu tới và nhận dữ liệu từ phương tiện truyền dẫn. Tầng này gồm các thiết bị phần cứng vật lí chẳng hạn như card mạng và cáp mạng.

1 số giao thức tiêu biểu thuộc tầng này gồm :

- ATM (Asynchronous Transfer Mode)
- Ethernet
- Token Ring
- FDDI (Fiber Distributed Data Interface)
- Frame Relay

B. Network Scanning

Network Scanning là 1 quá trình thu thập thông tin về 1 mạng của attacker, hoặc của 1 nhà quản trị mạng. Scanning thường là bước khởi đầu cho 1 cuộc tấn công, hoặc có thể được sử dụng bởi các nhà quản trị mạng để khảo sát các máy trong mạng, …

Mục tiêu của network scanning:

- xác định được IP của mục tiêu
- xác định được hệ điều hành đang chạy trên hệ thống đó
- xác định được cổng đang được mở, từ đó xác được các dịch vụ đang chạy trên hệ thống đó

Network Scanning bao gồm 4 kỹ thuật cơ bản sau:

- Network Mapping: các phương pháp để xác định các máy đang hoạt động trong mạng
- Port Scanning: các phương pháp xác định các cổng đang được mở trên từng máy ☾ từ đó xác định được các dịch vụ đang được chạy trên các máy này
- Service and version dectection: các phương pháp xác định các dịch vụ đang chạy trên và version của các dịch vụ này
- OS detection: các phương pháp xác định hệ điều hành và version của các OS đang được chạy trên các máy này

Ngoài ra cùng với các ký thuật cơ bản này là các kỹ thuật khác bổ sung thêm nhằm đạt được sự tối ưu về thời gian, tránh bị lọc (bởi firewall) hay bị phát hiện bởi các IDS (Intrusion detection system - hệ thống phát hiện truy nhập bất thường), …

I. Network Mapping:

Network Mapping là những phương pháp xác định các máy đang hoạt động trong mạng. Phương pháp này bao gồm 1 số kỹ thuật sau:

1. **ICMP scanning**: đây là phương pháp cơ bản nhất dùng để xác định các máy đang hoạt động trong mạng, trong phương pháp này scanner sẽ gửi 1 gói ICMP echo request đến tất cả các máy cần scan, nếu thấy phản hồi từ máy nào nghĩa là máy đó vẫn đang hoạt động. Có nhiều kiểu gói tin ICMP có thể sử dụng:
    a. ICMP type 8 echo request sẽ mong nhận được ICMP type 0 echo reply từ phía active host

b. ICMP type 13 timestamp echo request sẽ mong nhận được ICMP type 14 timestamp echo reply từ phía active host
c. ICMP type 17 echo request sẽ mong nhận được ICMP type 18 echo reply từ phía active host

Đánh giá:

- Ưu điểm: đơn giản, nhanh do có thể quét nhiều máy 1 lúc
- Nhược điểm: có thể bị chặn bởi các firewall ☾ kết quả không chính xác, chỉ có thể xác định được các máy có đang hoạt động hay không.

2. **TCP SYN ping, TCP ACK ping**:

Phương pháp sử dụng các gói tin ở tầng transport để xác định xem những máy nào đang hoạt động

- Với TCP SYN ping: scanner sẽ send 1 gói tin SYN với cổng bất kỳ đến các máy, nếu máy đó đang hoạt động thì sẽ gửi lại SYN/ACK (cổng đó đang mở) hoặc RST (cổng đó đóng)
- TCP ACK ping: scanner sẽ tạo ra 1 gói tin ACK rồi gửi cho các máy, nếu máy nào đang hoạt động sẽ gửi trả lại gói tin RST

II. Port scanning

Port scanning là 1 trong các dạng trong quá trình scanning. Port scanning tập trung vào 2 giao thức TCP và UDP 2 giao thức cơ bản trong mô hình TCP/IP, xác định các port đang được mở trên các máy từ đó xác định các dịch vụ và trạng thái của các dịch vụ đang chạy trên các máy này. Việc xác định được các dịch vụ

1. Port là gì?

Port là 1 số 16-bit được các giao thức trong tầng Transport (TCP, UDP) dùng trong quá trình kết nối giữa các tiến trình trên các máy tính khác nhau. Mỗi 1 tiến trình khi trao đổi dữ liệu với máy tính khác dựa trên mô hình TCP/IP đều phải đăng ký 1 port dùng để truyền và nhận dữ liệu. khi nhận được dữ liệu từ tầng IP, tầng TCP sẽ dựa vào số port này để xác định được sẽ chuyển dữ liệu cho tiến trình nào. Mỗi số hiệu cổng được đăng ký duy nhất cho 1 tiến trình. Không thể có 2 tiến trình trên 1 máy tính có cùng số port cùng tham gia vào quá trình truyền dữ liệu

Những ứng dụng thực thi những dịch vụ phổ biến thường sử dụng những cổng dành riêng để nhận các yêu cầu từ các máy khác và sau đó thiết lập lại kết nối bằng 1 port riêng khác cho quá trình trao đổi dữ liệu tiếp sau giữa hai máy. Những cổng này được xác định bởi tổ chức IANA (Internet Assigned Numbers Authority), một số cổng cùng với các dịch vụ đi kèm phổ biến trên Internet:

Port	Giao thức tầng transport	Dịch vụ cung cấp
20, 21	TCP	ftp – file tranfer protocol
23	TCP	telnet
25	TCP	SMTP – simple mail tranfer protocol
80	TCP	http
53	UDP	DNS – domain name system

2. Một số phương pháp scan port phổ biến:

_***Vanilla TCP connect scanning***: đây là phương pháp cơ bản nhất trong các phương pháp scan port, phương pháp này sử dụng quá trình bắt tay 3 bước trong giao thức của TCP để xác định trạng thái của các cổng. Trong phương pháp này, scanner sẽ tạo 1 kết nối TCP (thông qua hàm connect được hỗ trợ bởi hệ điều hành) trên 1 cổng bất kỳ của target

_ scanner sẽ gửi 1 gói tin SYN với 1 số hiệu cổng xác định đến target, có 2 trường hợp

_ nếu cổng đó được mở trên target thì target sẽ gửi lại gói tin SYN/ACK cùng với số hiệu cổng đó lại cho scanner

_ nếu cổng đó không được mở thì target sẽ gửi lại gói tin RST/ACK để đóng kết nối

_ cuối cùng scanner gửi lại gói tin ACK (RST) kết thúc quá trình bắt tay 3 bước của TCP

```
Computer A                                  Computer B

192.168.1.2:2342 ------------syn--------------
   >192.168.1.3:80
192.168.1.2:2342 <---------syn/ack-----------
   192.168.1.3:80
192.168.1.2:2342-------------ack--------------
   >192.168.1.3:80
```

Đánh giá

- *ưu điểm:* nhanh, đưa ra kết quả chính xác, dễ dàng sử dụng và không yêu cầu đặc quyền cao của user sử dụng phương pháp này
- *nhược điểm:* dễ dàng bị phát hiện, bị lọc và để lại log trên target

_ ***TCP SYN scanning:*** phương pháp này giống với phương pháp trên, tuy nhiên thay vì sử dụng hàm connect() (được hỗ trợ bởi hệ điều hành) thiết lập quá trình bắt tay 3 bước của TCP, ở phương pháp này ta sẽ tạo ra 1 gói tin TCP với cờ SYN được thiết lập và 1 cổng xác định, sau đó gửi cho target nếu port đó được mở:

_ target sẽ gửi lại gói tin SYN/ACK tương ứng với cổng đó

_ sau đó phía scanner sẽ gửi lại luôn gói tin RST để đóng kết nối luôn

```
Computer A                                  Computer B

192.168.1.2:2342 ------------syn----------->192.168.1.3:80
192.168.1.2:2342 <---------syn/ack----------192.168.1.3:80
192.168.1.2:2342-------------RST----------->192.168.1.3:80
```

Nếu port đó không được mở:

_ target sẽ gửi lại gói tin RST/ACK

_ phía scanner không gửi gì tiếp nữa

```
Computer A                                  Computer B

192.168.1.2:2342 ------------syn----------->192.168.1.3:80
192.168.1.2:2342 <---------RST/ack----------192.168.1.3:80
```

Đánh giá:

- *ưu điểm*: khó bị phát hiện
- *nhược điểm*: do phải thao tác với gói tin nên phương pháp này đòi hỏi đặc quyền của user phải cao, vd: với Windows OS thì là quyền Administrator, với Unix/Linux OS thì là quyền root; để lại log ít hơn

_ ***Stealth scanning:*** bao gồm các kỹ thuật quét nhằm tránh sự phát hiện của các hệ thống IDS, tường lửa (firewall), bộ lọc (filter) và tránh bị ghi log lại trên target. Bao gồm 1 số kỹ thuật sau:

_ *SYN/ACK scanning*: ở phương pháp này, phía scanner thay vì gửi gói tin SYN để bắt đầu kết nối, scanner sẽ gửi 1 gói tin SYN/ACK với 1 cổng xác định đến target. Khi phí scanner nhận được gói tin này

+) nếu cổng đó đang được mở, target sẽ gửi lại 1 gói tin RST

```
client -> SYN/ACK
server -> RST
```

+) nếu cổng đó không được mở thì target sẽ không gửi trả lại gì

```
client -> SYN/ACK
server -> ---
```

đánh giá:

- *ưu điểm:* tránh bị phát hiện bởi 1 số hệ thống IDS, firewall đơn giản
- *nhược điểm:* không tin cậy, có thể đưa ra những kết luận sai trong 1 số trường hợp gói tin trả lại của target bị mất hoặc gói tin đến của scanner bị firewall chặn

_ *NULL scanning*: phương pháp này chỉ hoạt động với target chạy hệ điều hành UNIX/ LINUX. Phía scanner sẽ gửi 1 gói tin cờ ACK, RST, FIN, SYN, URG, PSH đều không được thiết lập (ta gọi gói tin này là gói tin NULL), khi target nhận được gói tin này:

+) nếu cổng đó mở thì target sẽ không gửi lại gì

```
client -> NULL (no flags)
server -> -
```

+) nếu cổng đó không mở, target sẽ gửi lại gói tin RST

```
client -> NULL (no flags)
```

```
server -> RST
```

Đánh giá:

- *ưu điểm*: tránh được hệ thống IDS
- *nhược điểm*: chỉ áp dụng được với hệ điều hành UNIX, có thể đưa ra kết luận không chính xác

_ *XMAS scanning*: phương pháp này cũng chỉ hoạt động với target chạy hệ điều hành UNIX/ LINUX. Thay vì gửi 1 gói tin NULL (tất cả các cờ trong TCP header đều không được thiết lập) như phương pháp NULL scanning, XMAS scanning sẽ gửi 1 gói tin mà tất cả các cờ trong TCP header đều được thiết lập, khi target nhận được gói tin này:

+) nếu cổng đó mở thì target sẽ không gửi lại gì

```
client -> XMAS (all flags)
server -> -
```

+) nếu cổng đó không mở, target sẽ gửi lại gói tin RST

```
client -> NULL (all flags)
server -> RST
```

Đánh giá:

- ưu điểm: tránh được hệ thống IDS
- nhược điểm: chỉ áp dụng được với hệ điều hành UNIX, có thể đưa ra kết luận không chính xác

_IDLE scanning: phương pháp này dựa vào 1 số nhận xét như sau:

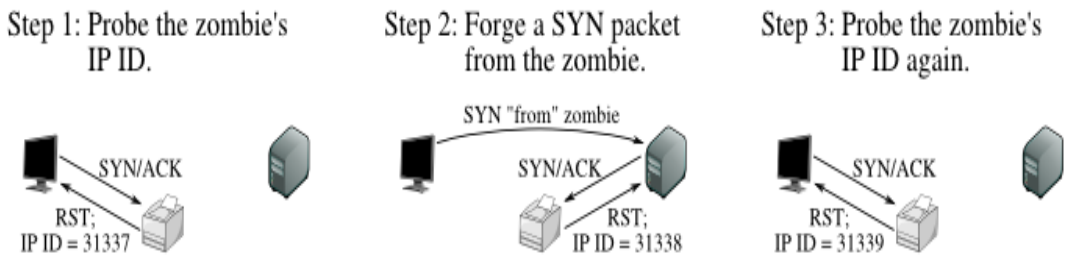
- mỗi gói tin được truyền đi đều có 1 id xác định
- 1 số hệ điều hành chỉ đơn giản là tăng số id này lên cho mỗi gói tin IP mà nó truyền
- dựa vào số id này, có thể xác định số gói tin IP đã được gửi đi

Dựa vào các nhận xét trên ta sẽ làm như sau:

- chọn 1 máy có rất ít hoặc không có trao đổi dữ liệu với máy khác làm máy trung gian (vd như máy in)
- từ máy scanner gửi 1 gói tin thăm dò đến máy trung gian này để xác định số id của các gói tin IP trên máy đó
- sử dụng ip của máy trung gian để send 1 gói tin SYN với cổng xác định đến target
- nếu cổng đó được mở, target sẽ gửi 1 gói tin SYN/ACK đến may trung gian, máy trung gian sẽ gửi lại gói tin RST ☾ số gói tin gửi đi ở máy trung gian tăng lên 1
- nếu cổng đó không được mở, target sẽ gửi gói tin RST đến máy trung gian, máy trung gian sẽ không gửi lại gói tin nào ☾ số gói tin được

gửi đi trên máy trung gian không tăng lên

☾ dựa vào 2 sự khác biệt trên ta có thể biết được trạng thái của cổng cần xác định



Ví dụ trong hình vẽ trên (với trường hợp cổng cần xác định đang mở):

_ bước 1: scanner gửi gói tin SYN/ACK đến để thăm dò IP ID của máy trung gian

_ bước 2:

- scanner sẽ giả mạo IP của máy trung gian để gửi gói tin SYN với số hiệu cổng cần xác định đến cho target
- target (dựa theo giao thức bắt tay 3 bước của TCP) sẽ gửi 1 gói SYN/ACK đến cho máy trung gian
- máy trung gian khi nhận được gói tin SYN/ACK nhưng trước đó chưa hề gửi gói tin ACK nào ☾ kết nối lỗi ☾ gửi trả lại gói tin RST với ID của IP tăng lên 1

_ bước 3: scanner gửi tiếp gói tin thăm dò (SYN/ACK) thấy IP ID tăng lên 2 ☾ cổng ở trên target đang được mở

Đánh giá:

- *ưu điểm:* có thể tránh được các hệ thống firewall, các bộ lọc (filter), khó bị phát hiện
- *khuyết điểm:* tốn nhiều thời gian, khó tìm được 1 máy trung gian hợp lý

_UDP scanning: UDP là giao thức không hướng nối (connectionless), do đó sẽ không có các gói tin phản hồi kiểu như ACK, SYN, … giống như TCP nên việc quét các cổng sử dụng giao thức UDP là khá khó khăn. Tuy nhiên ta có thể sử dụng tính chất sau của UDP để có thể quét các cổng UDP đang bị đóng ☾ từ đó có thể suy ra các cổng đang được mở: khi gửi 1 gói tin UDP đến cổng đang đóng thì bên phía target sẽ gửi trả lại 1 gói tin ICMP báo lỗi (thường là ICMP_PORT_UNREACHABLE), nếu cổng đó đang mở

thì không có gói tin nào được trả lại

Đánh giá:

- *ưu điểm:* có thể quét được các cổng sử dụng giao thức UDP
- *nhược điểm:* không đáng tin cậy, do UDP là giao thức không hướng nối ☾ gói tin truyền trên mạng có thể bị mất, hoặc bị firewall phía target chặn ☾ đưa ra kết luận không chính xác

III. Service and version detection:

Để xác định service và version của từng service , ta chủ yếu dựa vào các đặc trưng riêng của các gói tin phản hồi ứng với từng service và từng version để xác định được:

_ service sử dụng giao thức gì? (HTTP, SMTP, …)
_ tên service đó? (Microsoft IIS, Apache, …)
_ version của service là bao nhiêu? (Microsoft IIS version 5, …)
...

IV. OS detection:

Thường có 2 phương pháp chính để có thể tìm ra HĐH và version của HĐH đang chạy trên máy target:

- Phương pháp bị động: lắng nghe các trao đổi dữ liệu trên máy target rồi so sánh với 1 cơ sở dữ liệu ứng với từng HĐH (đã được thiết lập trước) để xác tên và version của HĐH. phương pháp này phía scanner chỉ lắng nghe ở máy target mà không gửi bất kỳ gói tin nào đến target

- Phương pháp chủ động: chủ động gửi các gói tin đến target và phân tích các phản hồi từ target, so sánh với 1 tập CSDL ứng với từng HĐH (đã được thiết lập trước) để xác tên và version của HĐH