

QUÉT HỆ THỐNG VÀ NGHE LÉN

Khoa Công nghệ thông tin và Truyền thông
Trường Đại học Cần Thơ

Phần A

QUÉT HỆ THỐNG

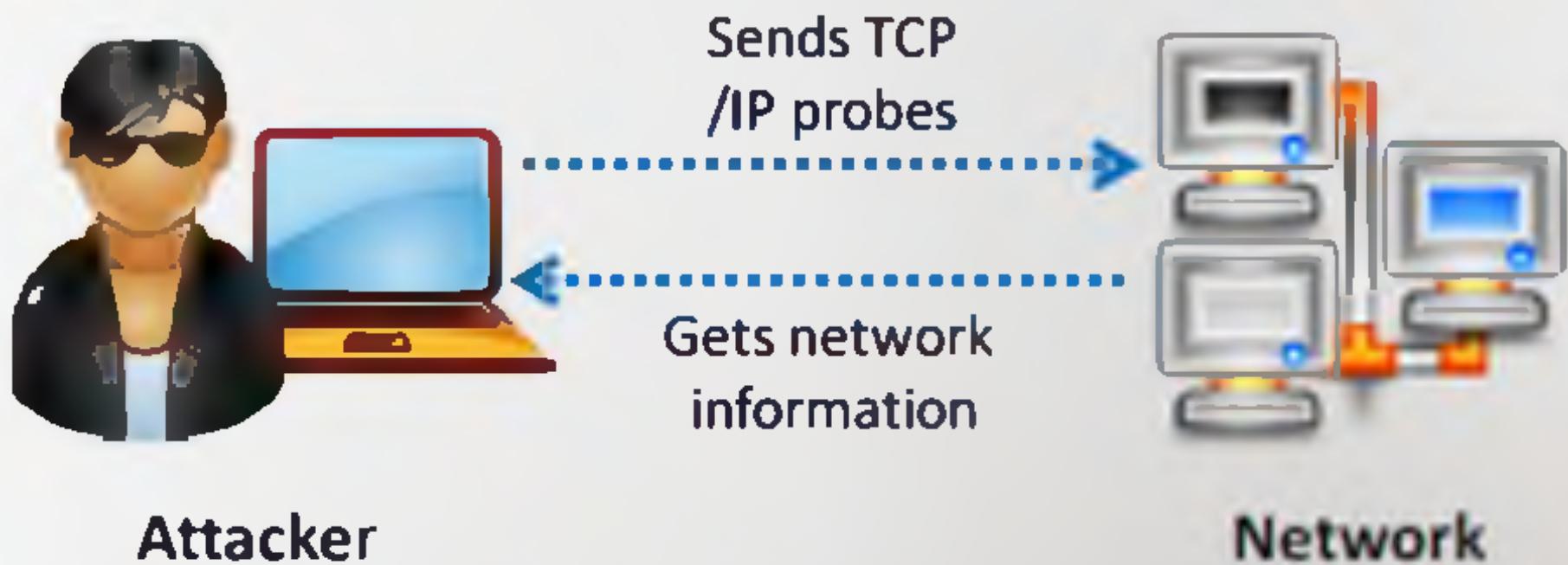
QUÉT HỆ THỐNG

- Định nghĩa và phân loại về quét hệ thống
- Các mục tiêu cần quét và các phương pháp quét
- Các biện pháp đối phó với quét hệ thống
- Tổng kết và thực hành

QUÉT HỆ THỐNG

- Quét hệ thống ám chỉ một tập các thao tác để xác định danh tính các máy tính trên mạng, các cổng đang mở và các dịch vụ đang chạy trên các máy đó.
- Quét hệ thống là một thành phần của các hành động thăm dò, cho phép kẻ tấn công thu thập hồ sơ mạng của tổ chức/cơ quan mục tiêu.

QUÉT HỆ THỐNG



CÁC KIỂU QUÉT HỆ THỐNG

- Quét mạng máy tính: Để tìm ra các địa chỉ IP cần thiết.
- Quét cổng: Để tìm ra các cổng TCP/UDP đang mở trên một máy tính cùng với các dịch vụ mạng gắn với các cổng đó.
- Quét lỗ hổng: Để tìm ra các điểm yếu từ cơ sở các địa chỉ IP và các cổng đang mở.

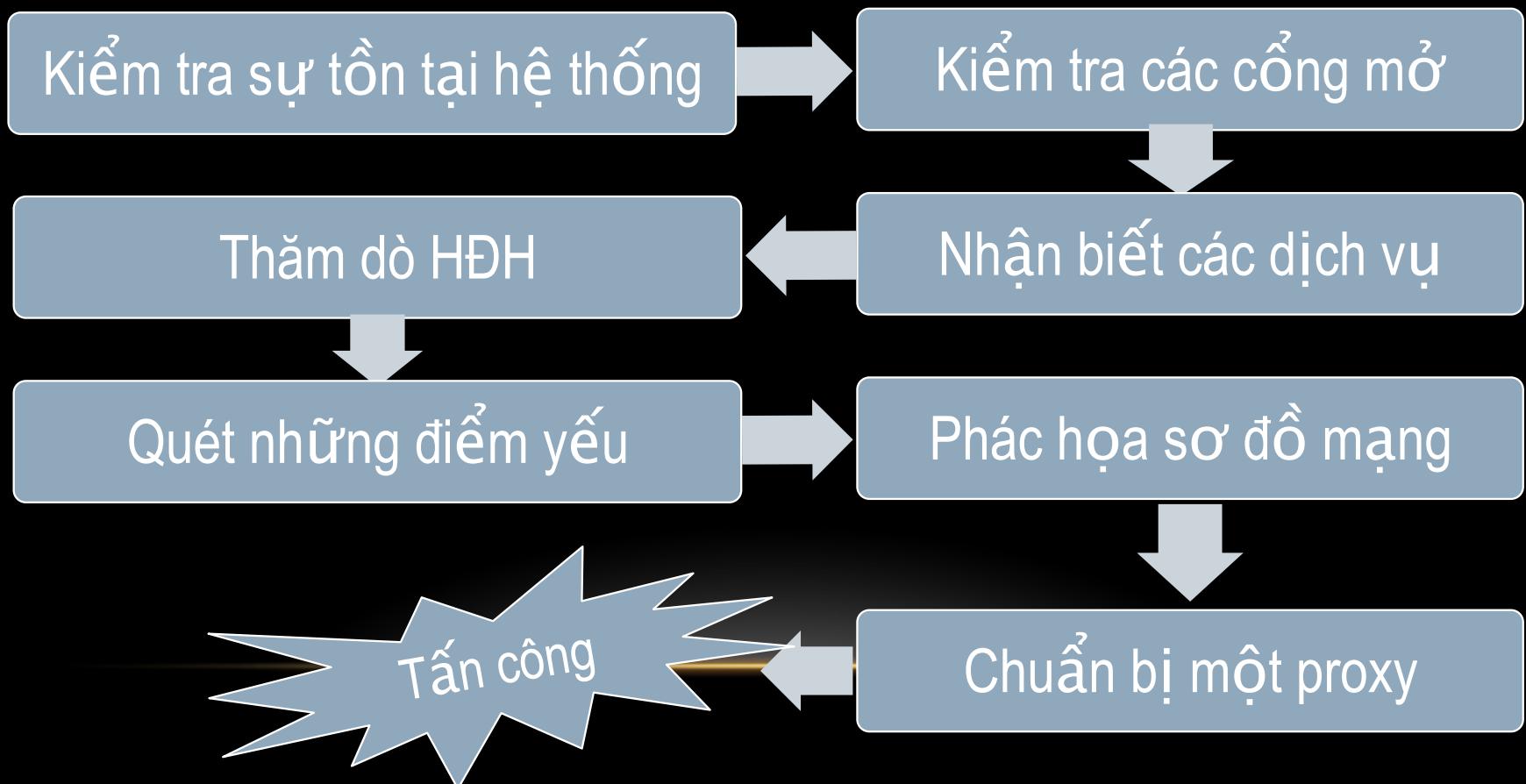
CÁC MỤC TIÊU CẦN QUÉT

Sau đây là các mục tiêu phổ biến:

- Các máy tính đang chạy, IP và các cổng đang mở.
- Các cổng đang mở là mục tiêu dễ dàng nhất để thâm nhập vào một hệ thống máy tính hoặc mạng máy tính.
- Hệ điều hành cũng như kiến trúc của hệ thống mục tiêu: Kẻ tấn công sẽ phát động tấn công dựa trên những điểm yếu đặc thù của từng hệ điều hành.

QÚA TRÌNH QUÉT HỆ THỐNG

- Sau đây là các phương pháp trong tiến trình quét hệ thống:

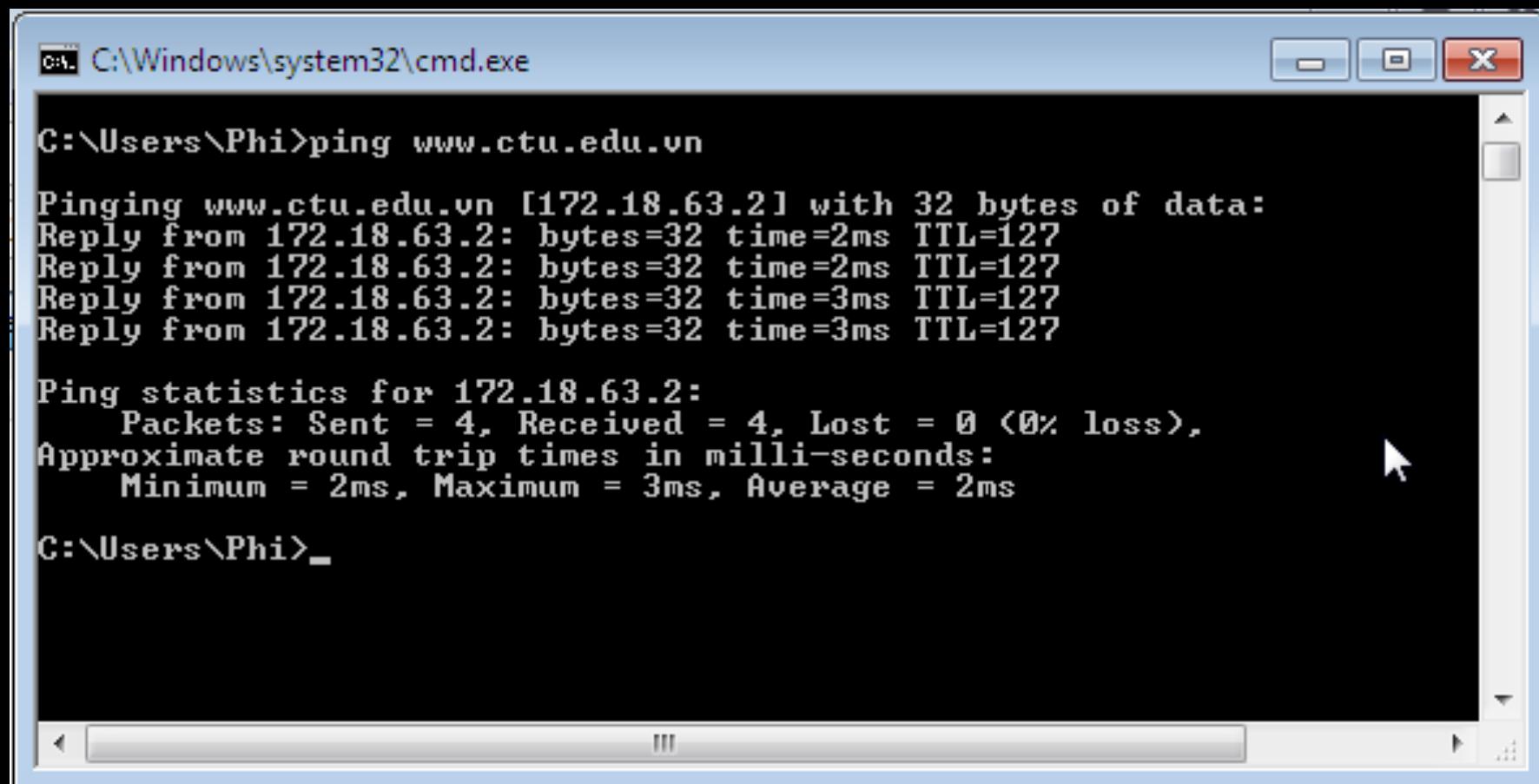


KIỂM TRA SỰ TỒN TẠI CỦA HỆ THỐNG

- Là phương pháp kiểm tra xem một hệ thống có tồn tại hay không bằng cách kiểm tra xem hệ thống này có phản ứng với các yêu cầu thăm dò hoặc kết nối từ xa hay không.
- Thông thường người ta hay dùng các gói tin ICMP để gửi đến mục tiêu, nếu thấy trả lời thì hệ thống mục tiêu đang tồn tại

KIỂM TRA SỰ TỒN TẠI CỦA HỆ THỐNG

- Sử dụng lệnh ping



```
C:\Windows\system32\cmd.exe
C:\Users\Phi>ping www.ctu.edu.vn

Pinging www.ctu.edu.vn [172.18.63.2] with 32 bytes of data:
Reply from 172.18.63.2: bytes=32 time=2ms TTL=127
Reply from 172.18.63.2: bytes=32 time=2ms TTL=127
Reply from 172.18.63.2: bytes=32 time=3ms TTL=127
Reply from 172.18.63.2: bytes=32 time=3ms TTL=127

Ping statistics for 172.18.63.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms

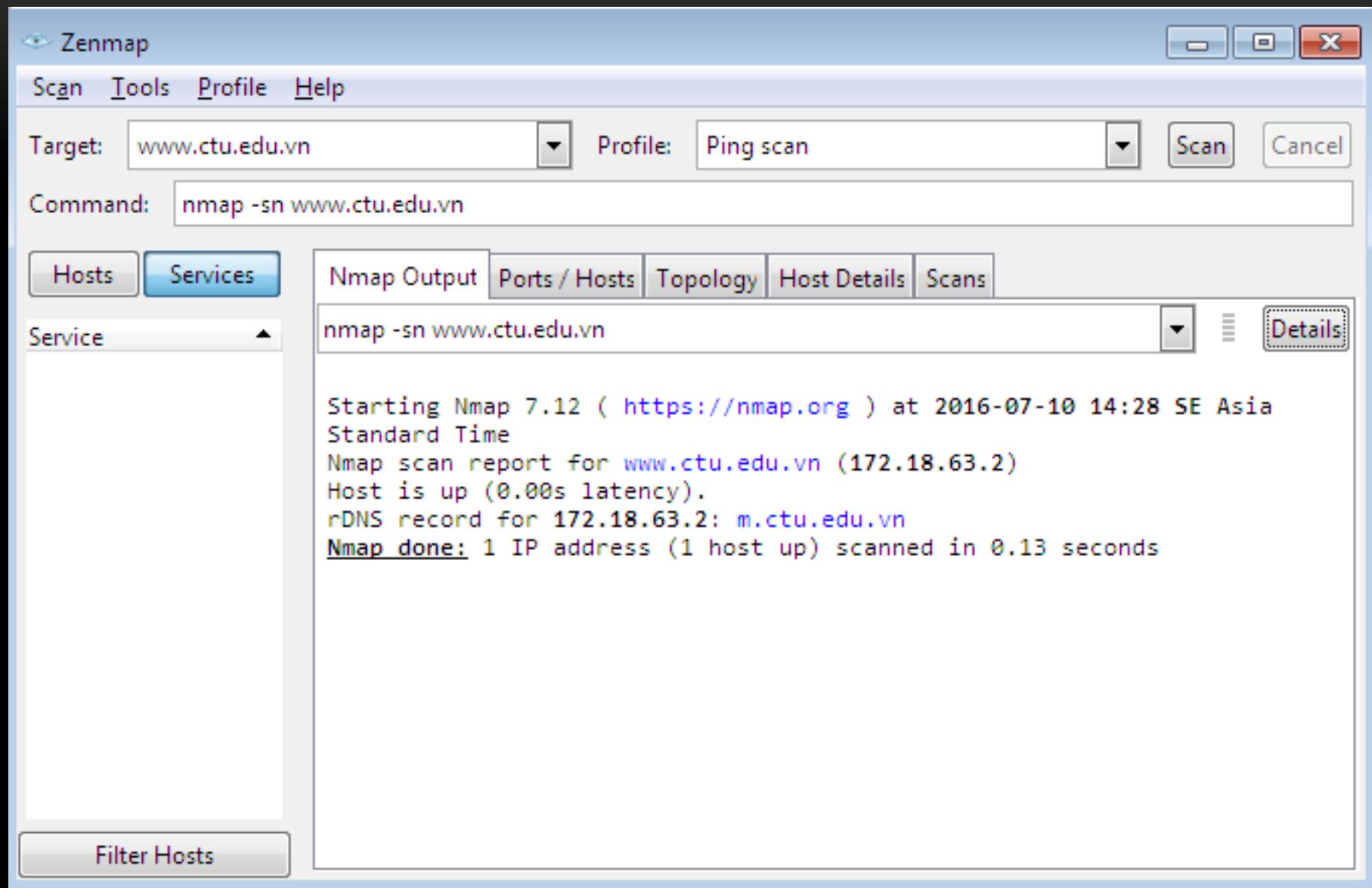
C:\Users\Phi>
```

KIỂM TRA SỰ TỒN TẠI CỦA HỆ THỐNG

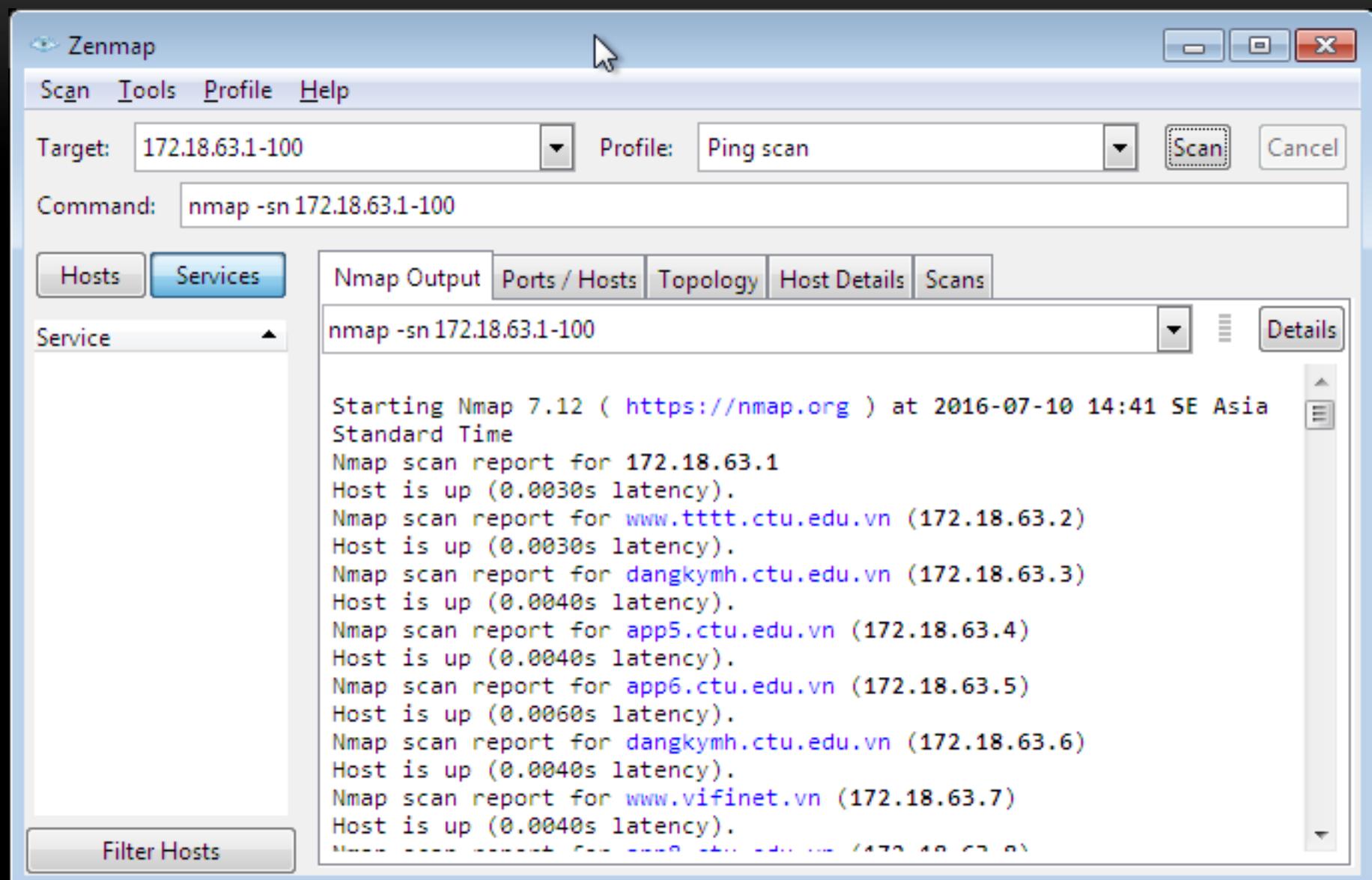
- Sử dụng công cụ Nmap:

- Nguồn: <http://nmap.org>
- Nmap là công cụ có thể được dùng để kiểm tra sự tồn tại của hệ thống cũng như các hệ thống trong một mạng sử dụng lệnh ping.
- Nmap thực hiện việc quét thông qua ping bằng cách gửi các gói tin yêu cầu ICMP ECHO đến tất cả các máy tính trong mạng, nếu có máy nào đang hoạt động thì nó sẽ trả lời cho yêu cầu ICMP ECHO này.
- Thao tác quét này cũng hữu ích để kiểm tra xem các gói tin ICMP có vượt qua bức tường lửa hay không.

- Sử dụng công cụ Nmap quét một máy



Sử dụng công cụ Nmap quét một mạng



KIỂM TRA SỰ TỒN TẠI CỦA HỆ THỐNG

- Các công cụ kiểm tra sự tồn tại của hệ thống khác:



Colasoft Ping Tool

<http://www.colasoft.com>



PacketTrap MSP

<http://www.packettrap.com>



Visual Ping Tester - Standard

<http://www.pingtester.net>



Ping Sweep

<http://www.whatsupgold.com>



Ping Scanner Pro

<http://www.digilextechnologies.com>



Network Ping

<http://www.greenline-soft.com>



Ultra Ping Pro

<http://ultraping.webs.com>



Ping Monitor

<http://www.niliand.com>



PingInfoView

<http://www.nirsoft.net>



Pinkie

<http://www.ipuptime.net>

KIỂM TRA CÁC CỔNG ĐANG MỞ

- Các dịch vụ mạng thường lắng nghe yêu cầu từ khách hàng trên các cổng cố định và trả lời cho khách hàng thông qua các cổng này.
- TCP sử dụng phương pháp bắt tay 3 chiều (three-way handshake) để thiết lập một kết nối giữa khách hàng và người phục vụ.

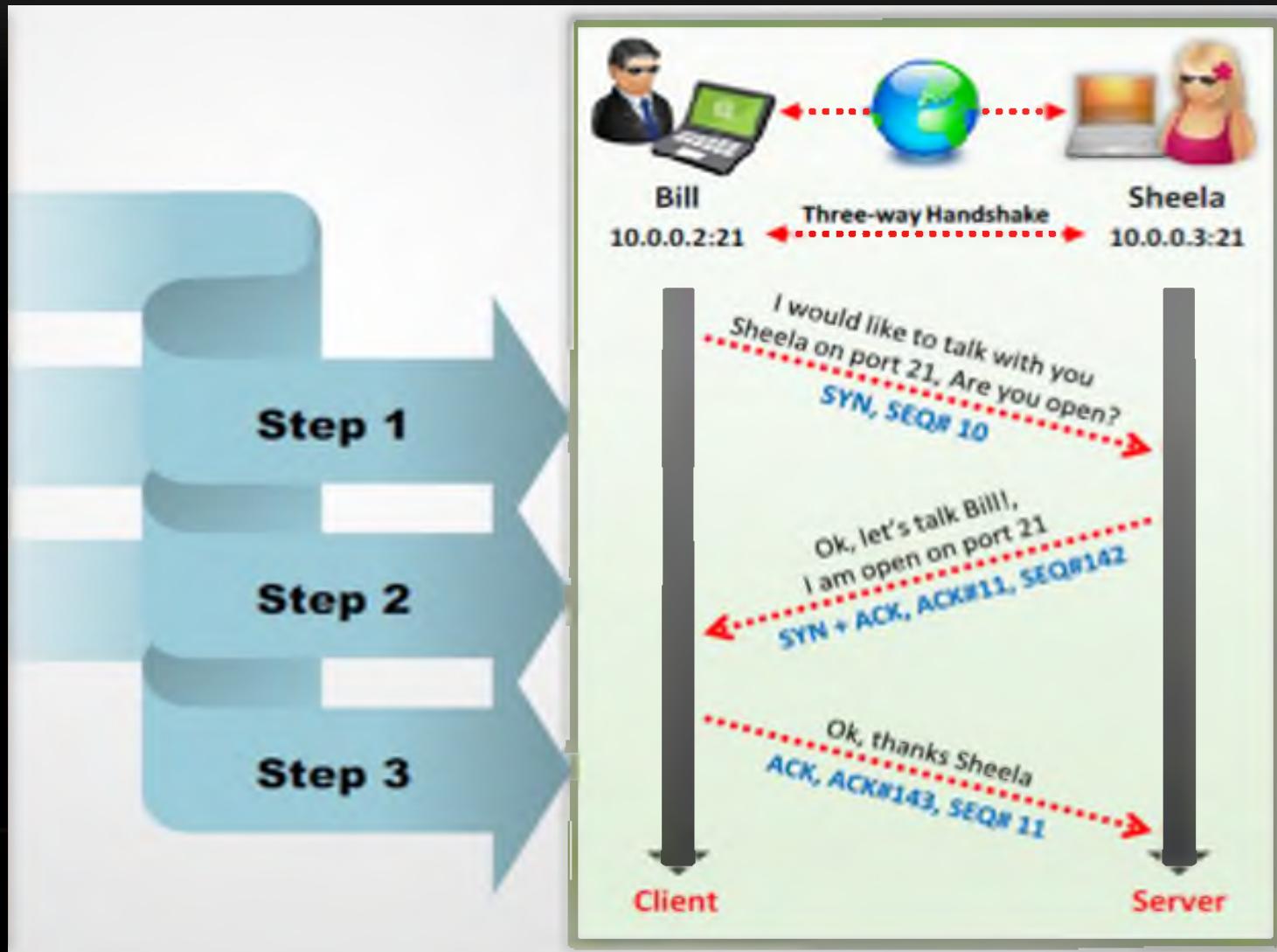
KIỂM TRA CÁC CÔNG ĐANG MỞ

BẮT TAY 3 CHIỀU

1. Khách hàng (10.0.0.2) khởi động một kết nối tới người phục vụ ở 10.0.0.3 thông qua gói tin bắt tay với chỉ cờ **SYN** được bật lên.
2. Người phục vụ trả lời với gói tin trong đó cả hai cờ **SYN** và **ACK** được bật lên.
3. Cuối cùng, khách hàng trả lời cho người phục vụ với gói tin với chỉ có cờ **ACK** được bật lên.
4. Nếu 03 bước trên hoàn thành suôn sẻ thì một kết nối TCP được thiết lập giữa khách hàng và người phục vụ. Từ đó, dữ liệu có thể được truyền qua lại giữa hai bên trên kết nối này đến khi một trong hai bên hủy kết nối bằng gói tin với cờ **FIN** hoặc **RST** được bật.

KIỂM TRA CÁC CỔNG ĐANG MỞ

BẮT TAY 3 CHIỀU



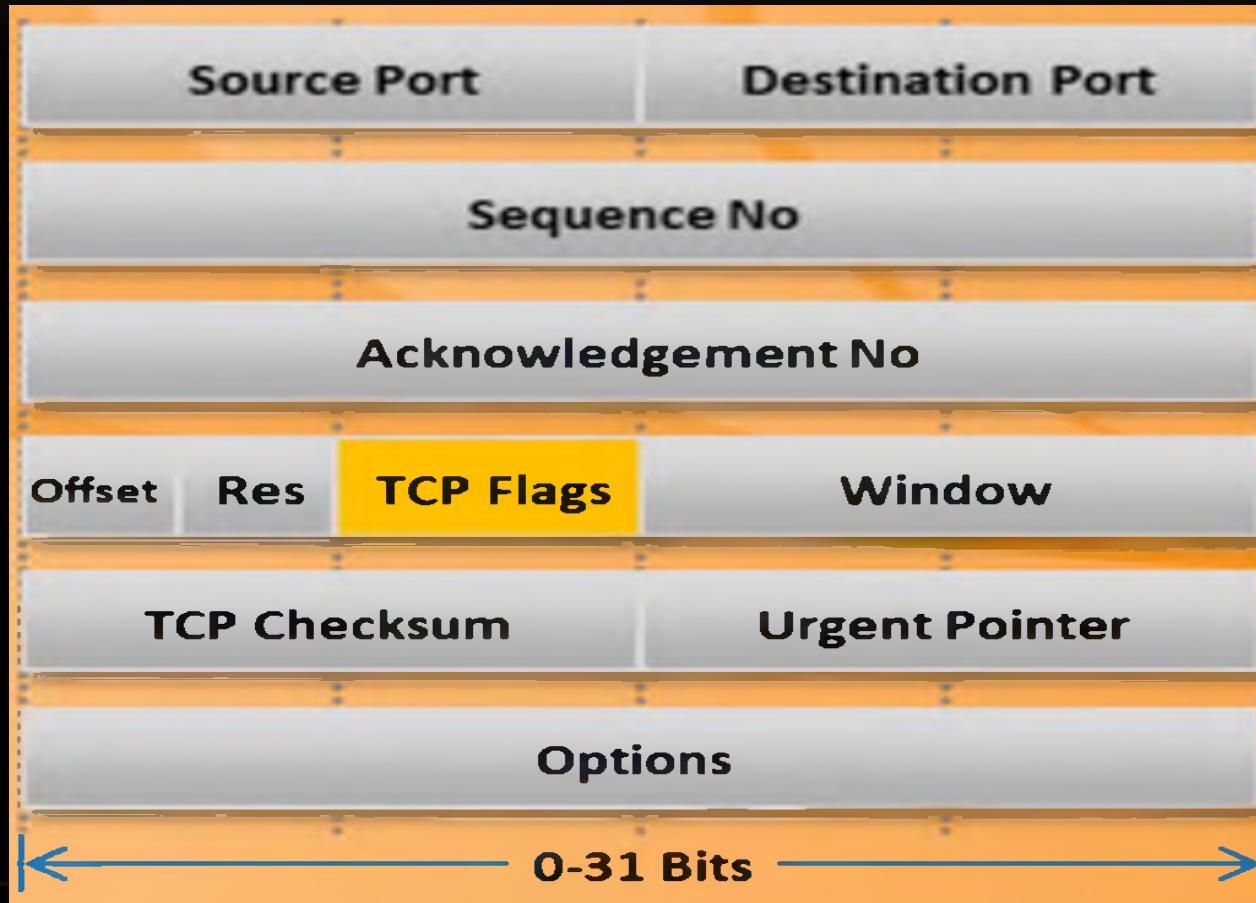
KIỂM TRA CÁC CÔNG ĐANG MỞ

CÁC LOẠI CỜ

- SYN: Thông báo bắt đầu kết nối hoặc gửi dữ liệu với số thứ tự byte bắt đầu được chỉ ra.
- ACK: Xác nhận đã nhận được thông báo kết nối hoặc dữ liệu cùng với với số thứ tự byte kế tiếp chờ nhận.
- PSH: Dùng cho hệ thống chuyển tiếp, để thông báo chấp nhận yêu cầu chuyển tiếp và chuyển tiếp dữ liệu đi.
- FIN: Thông báo không còn truyền dữ liệu đến hệ thống từ xa nữa (kết thúc phiên làm việc).
- RST: Làm lại phiên truyền dữ liệu.

KIỂM TRA CÁC CỔNG ĐANG MỞ

CẤU TRÚC GÓI TIN TCP



KIỂM TRA CÁC CỔNG ĐANG MỞ

CÁC CỔNG TCP/UDP PHỔ BIẾN

echo	7/udp	
discard	9/tcp	sink null
discard	9/udp	sink null
systat	11/tcp	Users
daytime	13/tcp	
daytime	13/udp	
netstat	15/tcp	
quotd	17/tcp	Quote
chargen	19/tcp	ttytst source
chargen	19/udp	ttytst source
ftp-data	20/tcp	ftp data transfer

KIỂM TRA CÁC CỔNG ĐANG MỞ

CÁC CỔNG TCP/UDP PHỔ BIẾN

ftp	21/tcp	ftp command
ssh	22/tcp	Secure Shell
telnet	23/tcp	
smtp	25/tcp	Mail
time	37/tcp	Timeserver
time	37/udp	Timeserver
rlp	39/udp	resource location
nicname	43/tcp	who is
domain	53/tcp	domain name server
domain	53/udp	domain name server
sql*net	66/tcp	Oracle SQL*net
sql*net	66/udp	Oracle SQL*net
bootps	67/tcp	bootp server
bootps	67/udp	bootp server
bootpc	68/tcp	bootp client

KIỂM TRA CÁC CỔNG ĐANG MỞ

CÁC CỔNG TCP/UDP PHỔ BIẾN

bootpc	68/udp	bootp client
tftp	69/tcp	Trivial File Transfer
tftp	69/udp	Trivial File Transfer
gopher	70/tcp	gopher server
finger	79/tcp	Finger
www-http	80/tcp	WWW
www-http	80/udp	WWW
kerberos	88/tcp	Kerberos
kerberos	88/udp	Kerberos
pop2	109/tcp	PostOffice V.2
Pop3	110/tcp	PostOffice V.3

KIỂM TRA CÁC CỔNG ĐANG MỞ

CÁC PHƯƠNG PHÁP QUÉT CỔNG PHỔ BIẾN

- Mở kết nối TCP hoàn chỉnh theo phương pháp bắt tay 3 chiều.
- Quét SYN: Quét nửa mở.
- Quét XMAS
- Quét FIN
- Quét NULL
- Quét cổng UDP

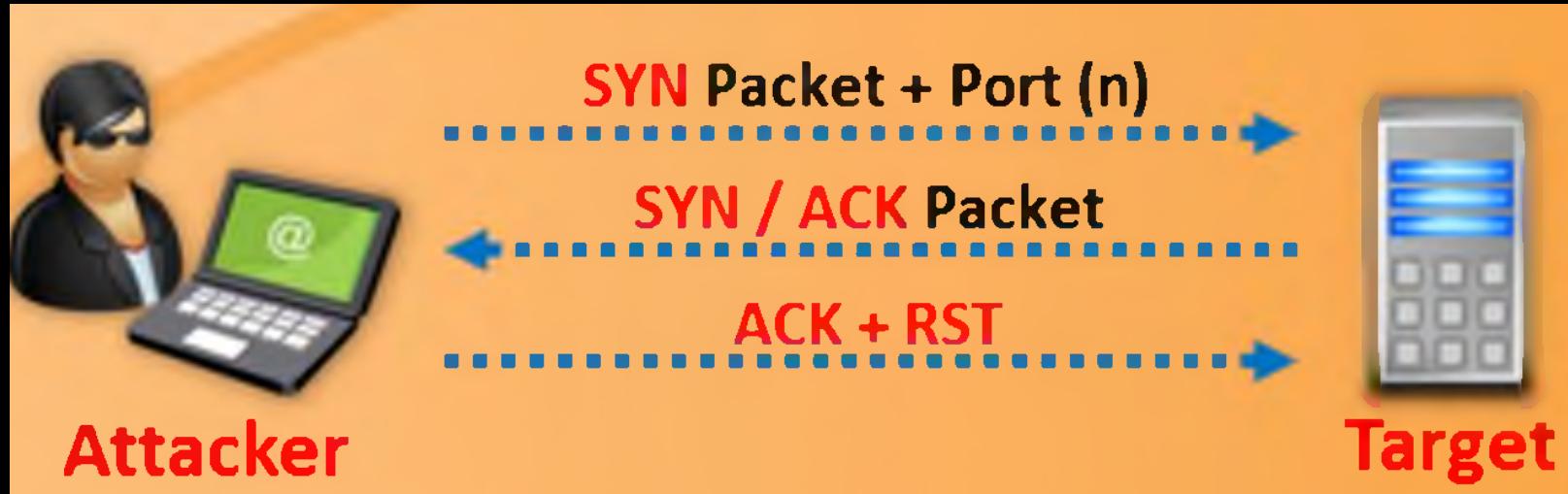
KIỂM TRA CÁC CỔNG ĐANG MỞ

QUÉT CỔNG BẰNG KẾT NỐI 3 CHIỀU

- Mở kết nối TCP hoàn chỉnh theo phương pháp bắt tay 3 chiều.
- Phương pháp này dễ bị phát hiện và lọc bỏ .

KIỂM TRA CÁC CỔNG ĐANG MỞ

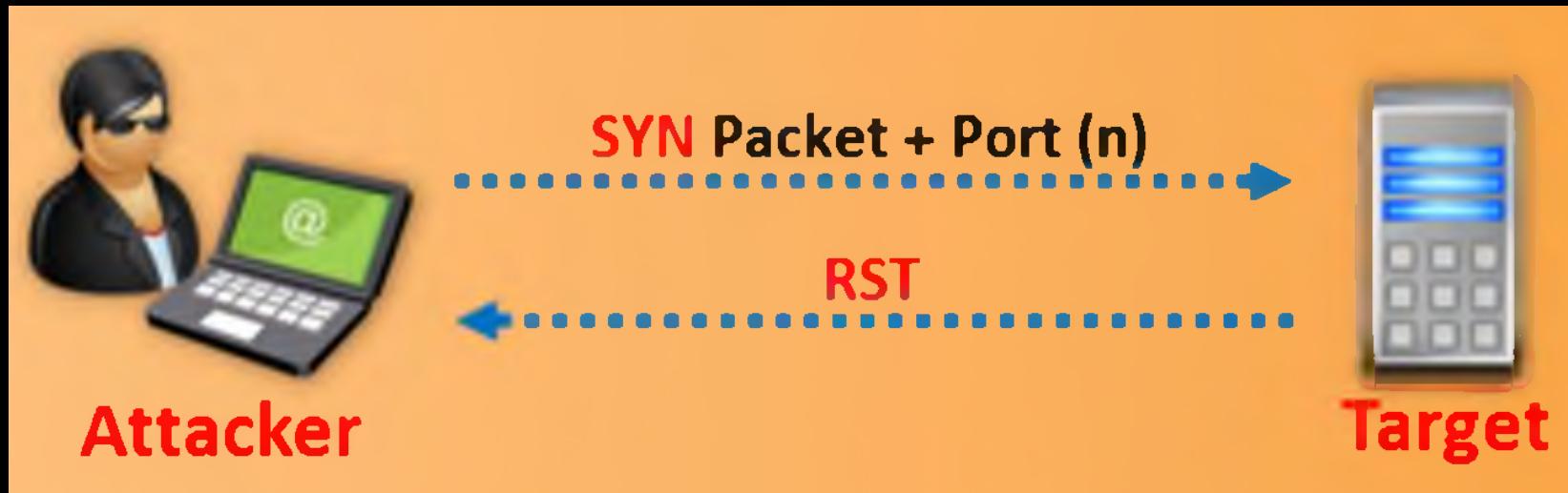
QUÉT CỔNG BẰNG KẾT NỐI 3 CHIỀU



Kết quả quét khi cổng mở

KIỂM TRA CÁC CỔNG ĐANG MỞ

QUÉT CỔNG BẰNG KẾT NỐI 3 CHIỀU



Kết quả quét khi cổng đóng

KIỂM TRA CÁC CỔNG ĐANG MỞ

QUÉT CỔNG BẰNG KẾT NỐI 3 CHIỀU

The screenshot shows the Zenmap interface. In the top left, it says "Zenmap". The menu bar includes "Scan", "Tools", "Profile", and "Help". The "Scan" tab is selected. The "Target:" field contains "www.ctu.edu.vn". The "Command:" field shows "nmap -sT -v www.ctu.edu.vn". Below the target field, there are tabs for "Hosts" (selected), "Services", "Nmap Output", "Ports / Hosts", "Topology", "Host Details", and "Scans". The "Nmap Output" tab is active, displaying the following text:

```
nmap -sT -v www.ctu.edu.vn
```

Starting Nmap 7.12 (https://nmap.org) at 2016-07-10 16:08 SE Asia
Standard Time
Initiating Ping Scan at 16:08
Scanning www.ctu.edu.vn (172.18.63.2) [4 ports]
Completed Ping Scan at 16:08, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:08
Completed Parallel DNS resolution of 1 host. at 16:08, 0.00s elapsed
Initiating Connect Scan at 16:08
Scanning www.ctu.edu.vn (172.18.63.2) [1000 ports]
Discovered open port 443/tcp on 172.18.63.2
Discovered open port 22/tcp on 172.18.63.2
Discovered open port 80/tcp on 172.18.63.2

On the left side, there's a tree view under "Hosts" showing various IP addresses and hostnames. At the bottom left, there's a "Filter Hosts" button.

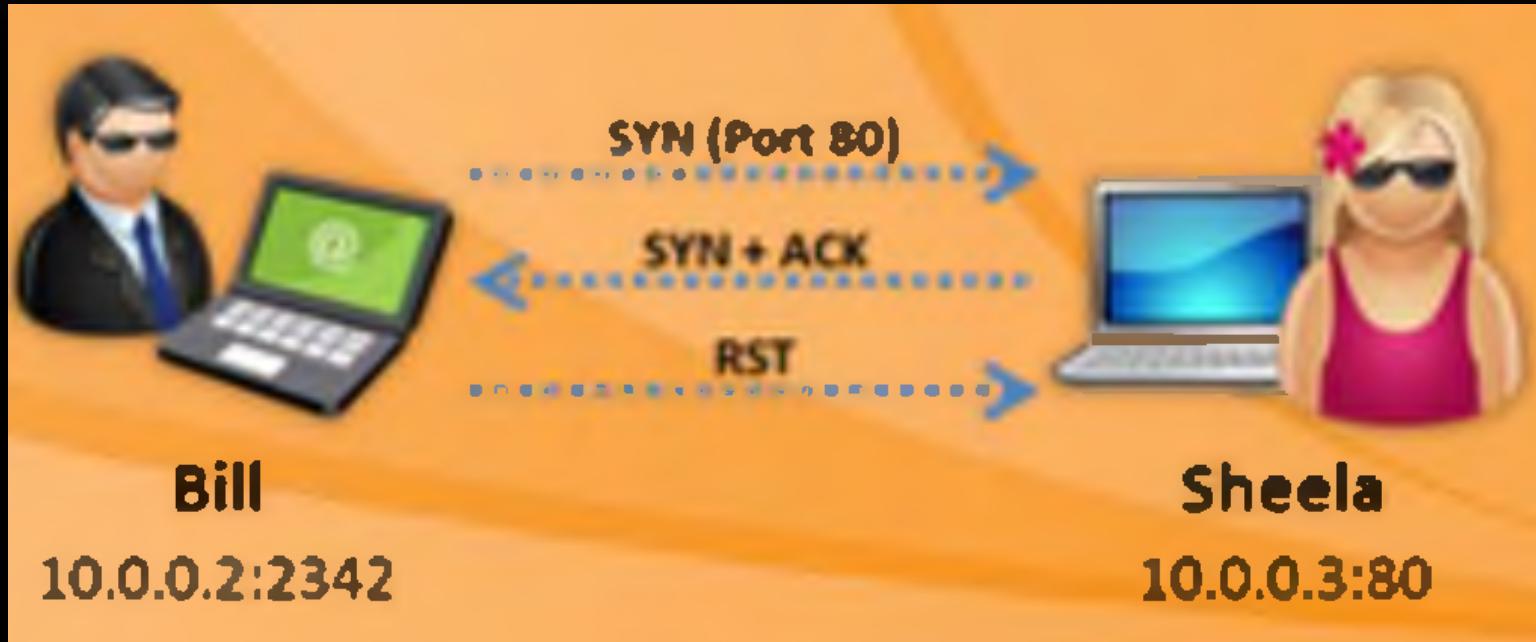
KIỂM TRA CÁC CỔNG ĐANG MỞ

QUÉT SYN – NỬA MỞ

- Khách hàng gửi gói tin chỉ bật cờ **SYN** đến mục tiêu.
- Nếu mục tiêu trả lời với “**SYN/ACK**” thì cổng đang mở.
- Nếu mục tiêu trả lời “**RST**” thì cổng đang đóng.
- Cuối cùng khách hàng gửi **RST** cho mục tiêu. Không có kết nối nào xảy ra. Vì thế cách quét này được gọi là nửa mở.

KIỂM TRA CÁC CỔNG ĐANG MỞ

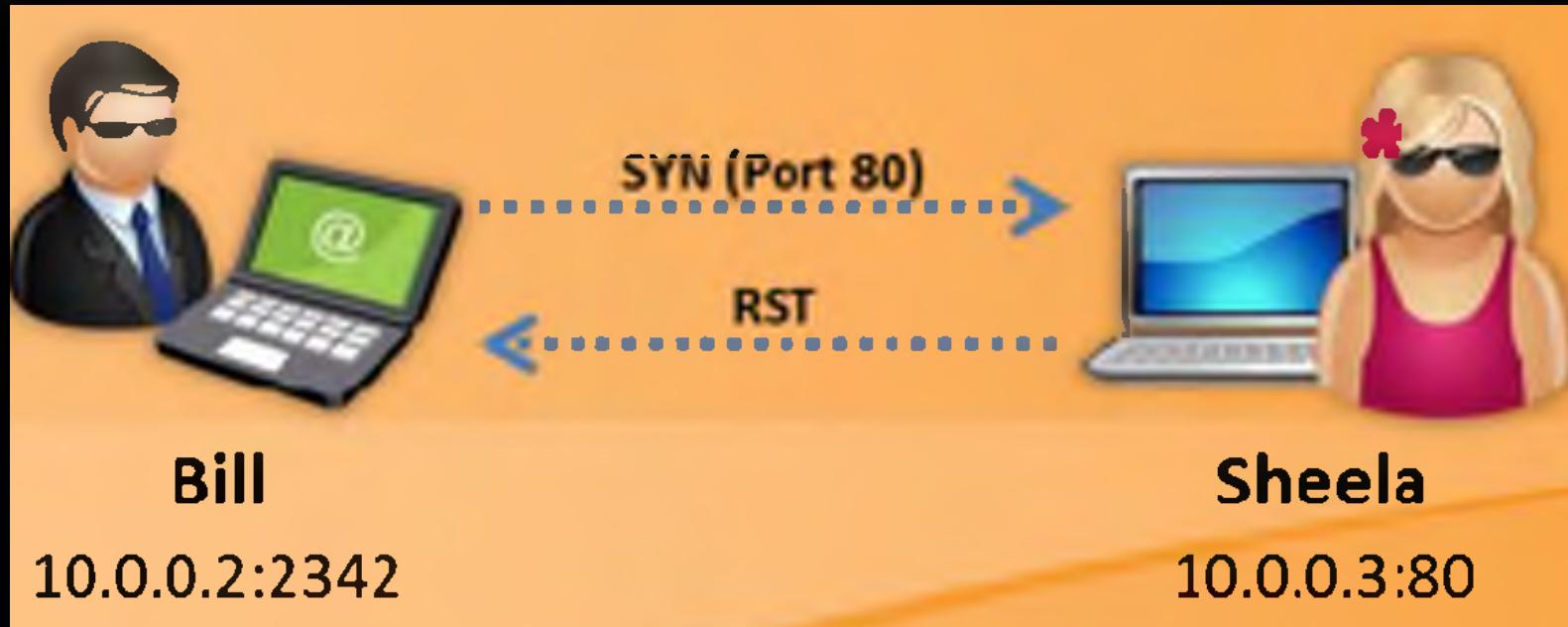
QUÉT SYN – NỬA MỞ



Cổng mở

KIỂM TRA CÁC CỔNG ĐANG MỞ

QUÉT SYN – NỬA MỞ



Cổng đóng

KIỂM TRA CÁC CỔNG ĐANG MỞ

QUÉT SYN – NỬA MỞ

Zenmap

Scan Tools Profile Help

Target: www.ctu.edu.vn Profile: Scan Cancel

Command: nmap -sS -v www.ctu.edu.vn

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

www.ctu.edu
172.18.63.1
172.18.63.51
172.18.63.50
dangkymh.ct
172.18.63.49
172.18.63.48
app5.ctu.edu
app6.ctu.edu
dangkymh.ct
www.vifinet.v
app8.ctu.edu
lms.vifinet.vn
kqts3.ctu.edu

nmap -sS -v www.ctu.edu.vn

```
Starting Nmap 7.12 ( https://nmap.org ) at 2016-07-10 16:37 SE Asia Standard Time
Initiating Ping Scan at 16:37
Scanning www.ctu.edu.vn (172.18.63.2) [4 ports]
Completed Ping Scan at 16:37, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:37
Completed Parallel DNS resolution of 1 host. at 16:37, 0.00s elapsed
Initiating SYN Stealth Scan at 16:37
Scanning www.ctu.edu.vn (172.18.63.2) [1000 ports]
Discovered open port 443/tcp on 172.18.63.2
Discovered open port 80/tcp on 172.18.63.2
Discovered open port 22/tcp on 172.18.63.2
Completed SYN Stealth Scan at 16:37, 4.97s elapsed (1000 total ports)
Nmap scan report for www.ctu.edu.vn (172.18.63.2)
Host is up (0.0018s latency).
rDNS record for 172.18.63.2: kqts4.ctu.edu.vn
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https

Read data files from: C:\Program Files\Nmap
Nmap done: 1 IP address (1 host up) scanned in 5.12 seconds
Raw packets sent: 2003 (88.100KB) | Rcvd: 6 (252B)
```

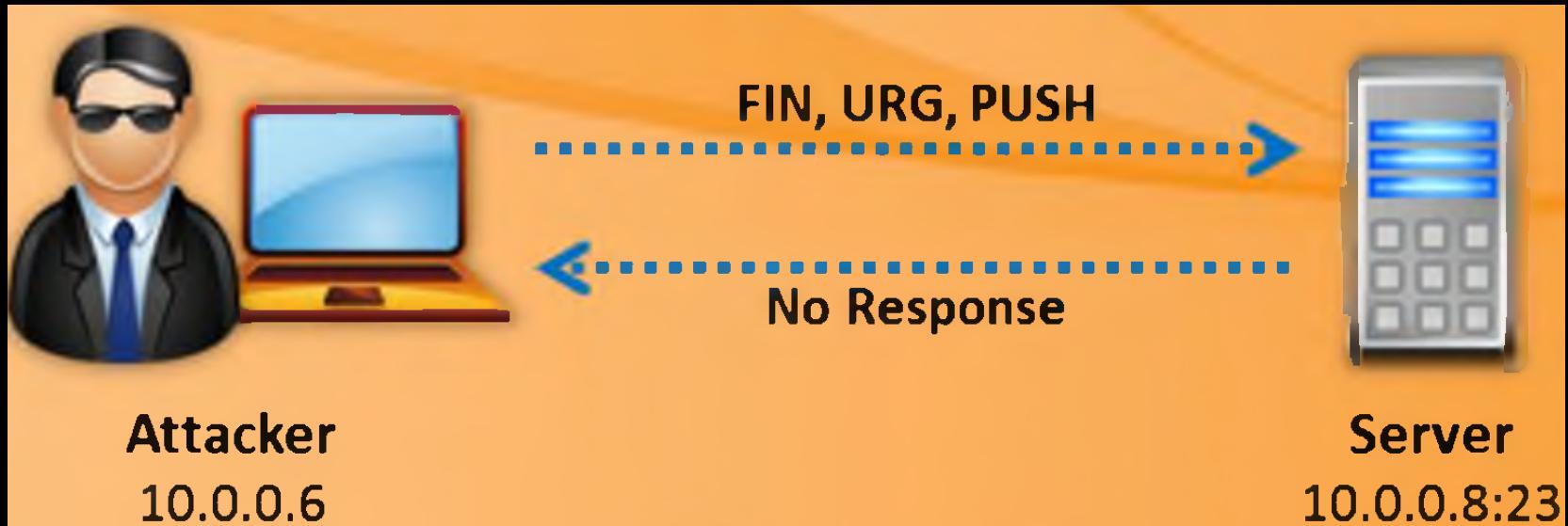
Filter Hosts

KIỂM TRA CÁC CỔNG ĐANG MỞ QUÉT XMAS

- Khách hàng gửi gói tin thông thường với 03 cờ **URG-PSH-FIN** đến mục tiêu. (Các cờ đều sáng như đèn giáng sinh).
- Nếu mục không trả lời (không hiểu gói tin ngớ ngẩn này) thì cổng đang mở.
- Nếu mục tiêu trả lời “**RST**” thì cổng đang đóng.
- Chú ý là phương pháp này chỉ áp dụng cho hệ thống Unix

KIỂM TRA CÁC CỔNG ĐANG MỞ

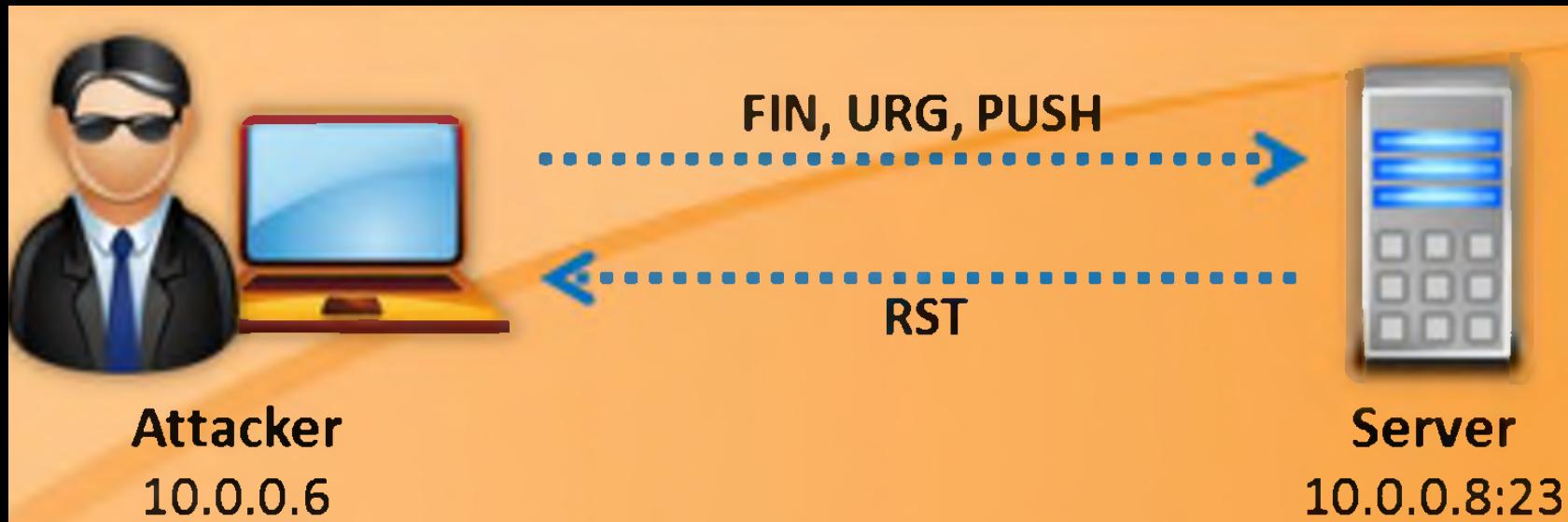
QUÉT XMAS



Cổng mở

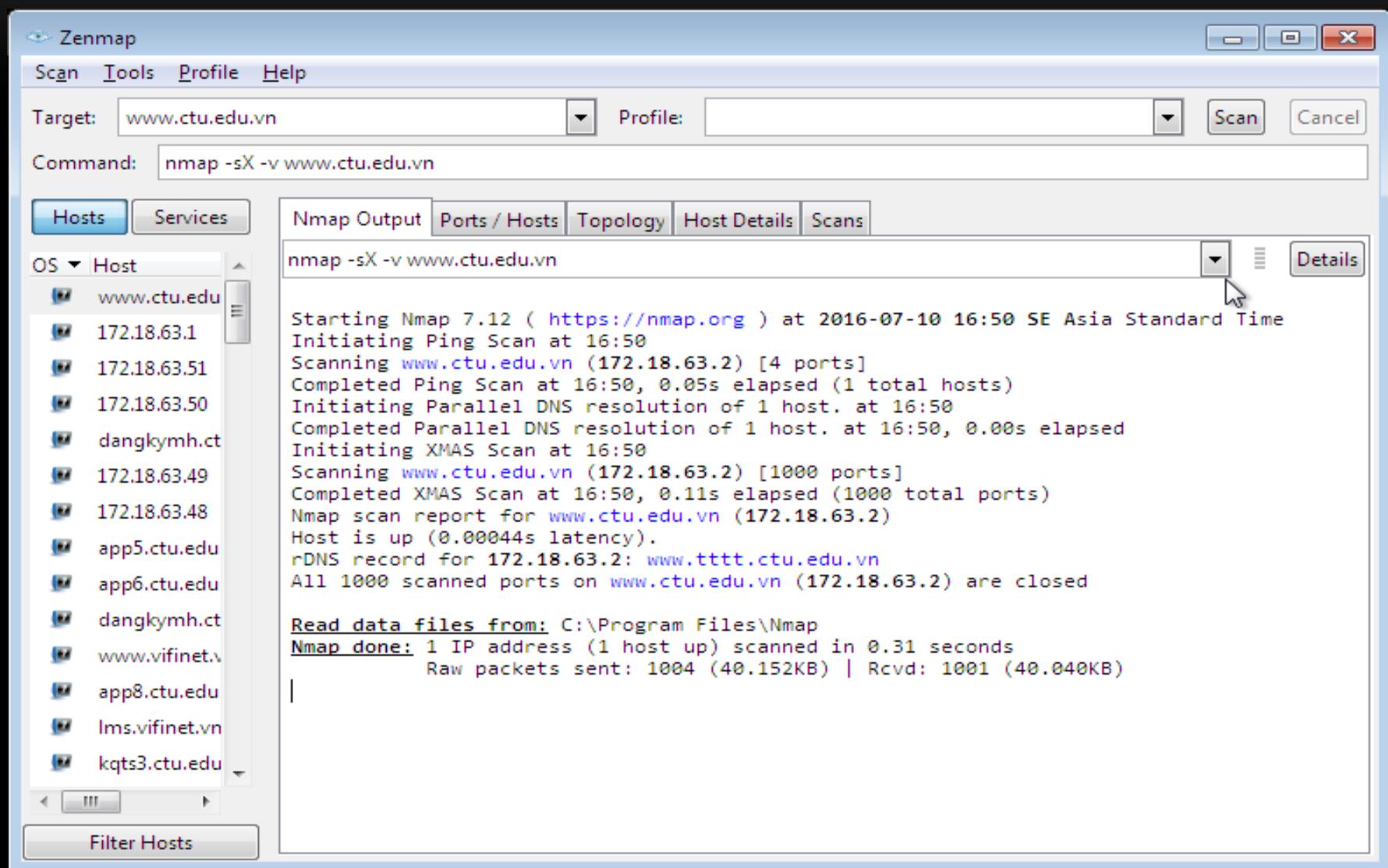
KIỂM TRA CÁC CỔNG ĐANG MỞ

QUÉT XMAS



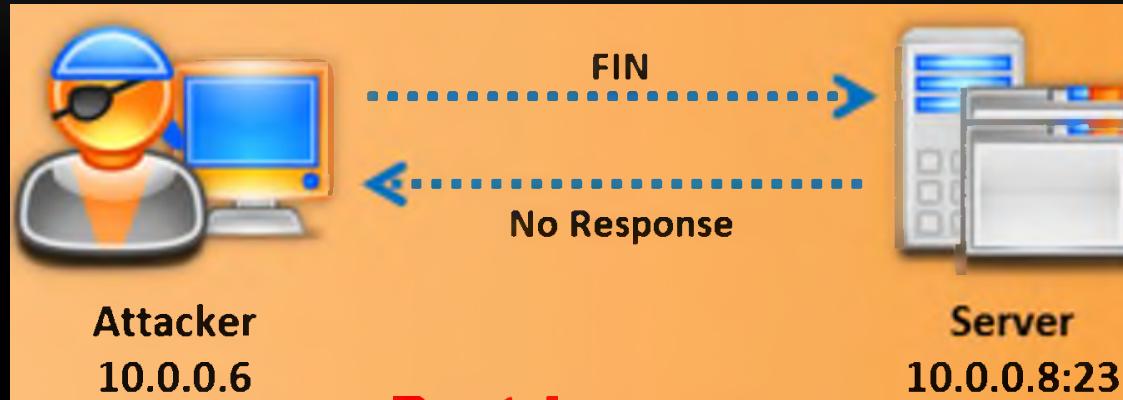
Cổng đóng

KIỂM TRA CÁC CÔNG ĐANG MỞ QUÉT XMAS



KIỂM TRA CÁC CỔNG ĐANG MỞ

QUÉT FIN – KHÔNG HOẠT ĐỘNG TRÊN WINDOWS



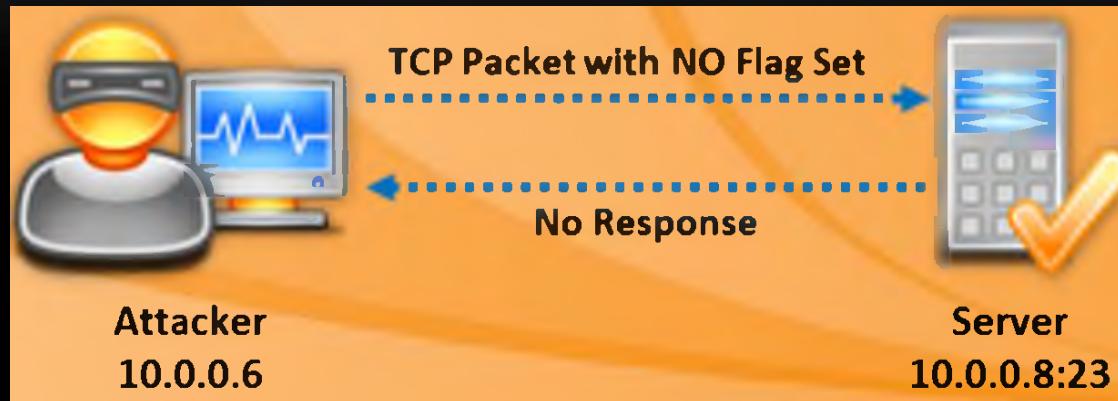
Cổng mở



Cổng đóng

KIỂM TRA CÁC CỔNG ĐANG MỞ

QUÉT NULL – KHÔNG HOẠT ĐỘNG TRÊN WINDOWS



Cổng mở



Cổng đóng

KIỂM TRA CÁC CỔNG ĐANG MỞ

QUÉT CỔNG UDP (THAM SỐ -SU CHO NMAP)

- UDP là phương thức truyền dữ liệu không có bắt tay kết nối trước.
- Bên khách hàng có thể gửi một gói tin đến mục tiêu mà không chắc cổng đích là mở, đóng hay gói tin bị chặn.
- Tuy nhiên nếu khách hàng gửi một gói tin ICMP đến một cổng mà không có dịch vụ nào lắng nghe thì máy phục vụ sẽ gửi trả lời bằng gói tin ICMP port unreachable. Nếu không nhận được trả lời nào thì có khả năng cổng đích đang mở hay gói tin bị chặn.



KIỂM TRA CÁC CÔNG ĐANG MỞ

MỘT SỐ CÔNG CỤ QUÉT CÔNG



PRTG Network Monitor

<http://www.paessler.com>



**Global Network Inventory
Scanner**

<http://www.magnetosoft.com>



Net Tools

<http://mabsoft.com>



SoftPerfect Network Scanner

<http://www.softperfect.com>



IP Tools

<http://www.ks-soft.net>



Advanced Port Scanner

<http://www.radmin.com>



MegaPing

<http://www.magnetosoft.com>



Netifera

<http://netifera.com>



Network Inventory Explorer

<http://www.10-strike.com>



Free Port Scanner

<http://www.nsauditor.com>

PHÒNG CHỐNG QUÉT CỔNG

- Bức tường lửa phải đủ tốt để phát hiện ra các gói tin mà kẻ tấn công gởi tới để thăm dò hệ thống.
- Chỉ mở những cổng cần thiết.
- Kiểm tra các địa chỉ IP trong mạng bằng cách quét thử để phát hiện cấu hình mạng rò rỉ và các cổng được mở không cần thiết.
- Luôn luôn cập nhật bức tường lửa khi có bản vá mới.

TÌM HIỂU HỆ ĐIỀU HÀNH CỦA MỤC TIÊU

- Biết được hệ điều hành là quan trọng cho việc tấn công mục tiêu bởi vì hầu hết các lỗ hổng thường gắn với một hệ điều hành cụ thể.
- Hành động tìm hiểu hệ điều hành mục tiêu còn được gọi là lấy banner.
- Có hai cách lấy banner: Chủ động và bị động.

TÌM HIỂU HỆ ĐIỀU HÀNH CỦA MỤC TIÊU

- Lấy banner chủ động:
 - Trực tiếp kết nối đến hệ thống mục tiêu.
 - Dựa trên nguyên tắc là: hệ thống TCP/IP của một hệ điều hành sẽ có một cách trả lời duy nhất cho các gói tin được sửa đổi một cách cụ thể.
 - Nguyên tắc này có được do cách mà các nhà phát triển hệ thống TCP/IP diễn dịch và cài đặt các thành phần của TCP/IP sẽ khác nhau trên từng hệ điều hành cụ thể.

TÌM HIỂU HỆ ĐIỀU HÀNH CỦA MỤC TIÊU

- Lấy banner bị động:
 - Cũng dựa trên cùng nguyên tắc như ở phần chủ động, nhưng phương pháp lấy banner bị động không kết nối trực tiếp đến mục tiêu mà chỉ cố nghe lén thông tin ra vào mục tiêu để tìm ra các chỉ dấu nổi bật thể hiện hệ điều hành của mục tiêu.

Zenmap

Scan Tools Profile Help

Target: www.ctu.edu.vn Profile: Quick scan plus Scan Cancel

Command: nmap -sV -T4 -O -F --version-light www.ctu.edu.vn

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

www.ctu.edu.vn (1)

nmap -sV -T4 -O -F --version-light www.ctu.edu.vn

Starting Nmap 7.12 (https://nmap.org) at 2016-07-10
22:38 SE Asia Standard Time
Nmap scan report for www.ctu.edu.vn (123.30.143.225)
Host is up (0.0078s latency).
rDNS record for 123.30.143.225: static.vdc.vn
Not shown: 97 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.2.14
113/tcp closed ident
443/tcp open ssl/http Apache httpd 2.2.14 ((Ubuntu))
Device type: bridge
Running: Oracle Virtualbox
OS CPE: cpe:/o:oracle:virtualbox
OS details: Oracle Virtualbox
Service Info: Host: www.ctu.edu.vn

OS and Service detection performed. Please report any
incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 18.25
seconds

Filter Hosts

CÁC CÔNG CỤ THĂM DÒ HỆ ĐIỀU HÀNH

- Nmap
- Netcraft: <http://toolbar.netcraft.com>
- Netcat: <http://netcat.sourceforge.net>
- telnet

PHÒNG CHỐNG THĂM DÒ HỆ ĐIỀU HÀNH

- Hiển thị banner sai để đánh lừa kẻ tấn công.
- Tắt các dịch vụ không cần thiết để tránh bộc lộ thông tin.
- Người dùng IIS có thể sử dụng các công cụ sau để vô hiệu hóa hoặc đổi thông tin banner:
 - IIS Lockdown Tool (<http://microsoft.com>)
 - ServerMask (<http://www.port80software.com>)
- Apache 2. đổi dòng ServerSignature trong tập tin *httpd.conf* thành ServerSignature Off.

QUÉT CÁC LỖ HỔNG CỦA HỆ THỐNG

- Quét lỗ hổng nhằm tìm ra các điểm yếu trong:
 - Hình thái mạng hoặc của hệ điều hành.
 - Các cổng đang mở và các dịch vụ đang chạy.
 - Các lỗi cấu hình của các ứng dụng và dịch vụ.

Online Vulnerability Scanner

[DASHBOARD](#)[LAUNCH SCAN](#)[SCAN TARGETS ▾](#)[SCANS ▾](#)[REPORTS ▾](#)

Your evaluation expires in 14 days. Click [here](#) to purchase a subscription.

[Alerts \(247\)](#)[Knowledge Base \(0\)](#)

73

106

10

58

[Generate Report](#)**Start Date** 10 Jul 2016 23:28**Host Name** <http://testmetasploitable.vulnweb.com>**End Date** 10 Jul 2016 23:28**Scan Target Name** Test**Duration** 0h 0m 5s**Scan Type** Network

Demo scan results.

Name	Module
+ Apache Multiple Security Vulnerabilities (1)	Web Servers
+ Check for Backdoor in unrealircd (2)	Gain a shell remotely
+ GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC) - 03 (1)	General
+ GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC) - 04 (1)	General
+ GNU Bash Stacked Redirects aka 'redir_stack' Memory Corruption Vulnerability (LSC) (1)	General
+ ISC DHCP Client Buffer Overflow Vulnerability (1)	Buffer overflow
+ Microsoft IIS Multiple Remote Denial of Service Vulnerabilities (1)	Denial of Service

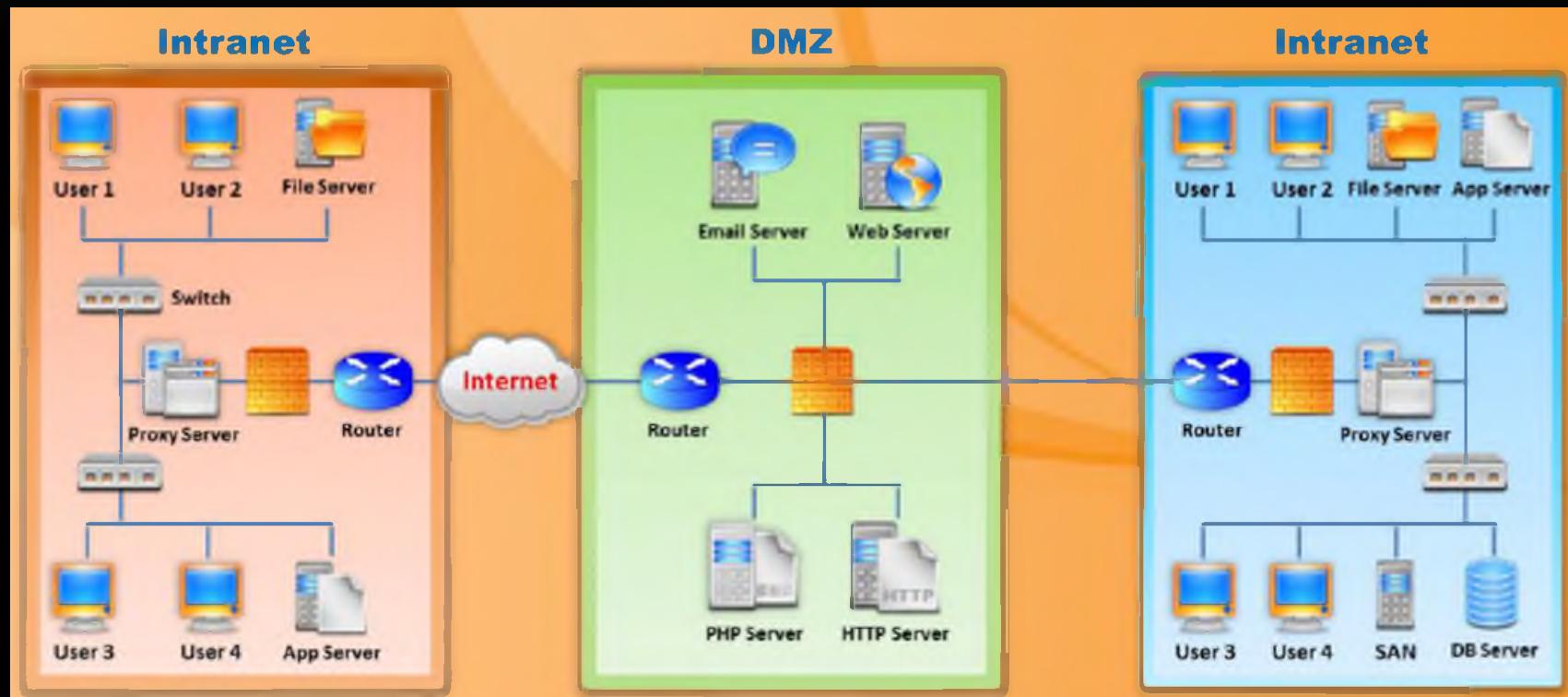
CÁC CÔNG CỤ QUÉT LỖ HỒNG

- Acunetix: <http://www.acunetix.com>
- Nexus: <http://www.tenable.com>
- GFI LanGuard: <http://www.gfi.com>
- ...

VẼ SƠ ĐỒ MẠNG

- Việc vẽ sơ đồ mạng cho phép xác định hình thái hoặc kiến trúc của mạng mục tiêu.
- Có được sơ đồ mạng cho phép việc lần vết đến một máy tính cụ thể trong mạng, hiểu được vị trí của các bức tường lửa, các bộ vạch đường và các thiết bị kiểm soát truy cập khác.
- Nhà quản trị mạng dùng sơ đồ mạng để quản lý các mạng máy tính của họ, trong khi hacker có thể sử dụng các công cụ khám phá và vẽ sơ đồ mạng tự động để phác thảo ra sơ đồ của mạng mục tiêu.

VẼ SƠ ĐỒ MẠNG – VÍ DỤ



MỘT SỐ CÔNG CỤ VẼ SƠ ĐỒ MẠNG

- LANsurveyor : www.solarwinds.com
- OpManager: www.manageengine.com
- The Dude: www.mikrotik.com

CHUẨN BỊ PROXY

- Chuẩn bị máy chủ proxy là bước cuối cùng trong tiến trình quét .
- Một proxy server là một máy tính hoạt động trung gian giữa hacker và máy tính mục tiêu.
- Sử dụng một proxy server cho phép hacker trở thành vô danh trên mạng.
- Dễ dàng tìm proxy server miễn phí với từ khóa “*free proxy server*” trên Google.

CÁC BIỆN PHÁP ĐỐI PHÓ VỚI QUÉT

- **Firewall:** Các công cụ quét đều khó vượt qua Firewall.
- Hệ thống phát hiện xâm nhập (IDS) phát hiện và cảnh báo các hành động quét.
- Chỉ nên mở những cổng cần thiết và đóng những cổng không cần để tránh hacker lợi dụng.
- Những thông tin nhạy cảm không nên đưa lên Internet