

# Kiểm thử & đánh giá an toàn hệ thống thông tin

## Module 3. Scanning

# Content

---

## → Scanning Goals, Types, and Tips

### ☐ Port Scanning

- Nmap
- Masscan
- Netcat

### ☐ Vulnerability Scanning

# Scanning

- ❑ Tương tác với mục tiêu nhằm thu thập thông tin về hệ thống và các dịch vụ.
  - Địa chỉ live host, firewall, routers và các thiết bị mạng.
  - Xác định topo mạng, thông tin hệ điều hành.
  - Liệt kê các port nghi ngờ đang chạy ngầm.
  - Tìm kiếm thông tin về các port và các dịch vụ đang chạy.
  - Dò quét lỗ hổng bảo mật.
- ❑ Một số công cụ thường được sử dụng.
  - Nmap, firewalk, hping3, Angry IP scanner...

# Scan Types

## ❑ Network scanning.

- Network Sweep: Thăm dò chủ động nhằm xác định live host.
- Network Tracing: Xác định topo mạng.
- OS Fingerprint: Xác định thông tin hệ điều hành.
- Version Scan: Xác định thông tin về các phiên bản của dịch vụ và giao thức .

## ❑ Port scanning.

- Xác định các cổng TCP & UDP đang hoạt động.

## ❑ Vulnerability scanning

- Tìm kiếm lỗ hổng bảo mật, lỗi cấu hình, dịch vụ chưa được vá...

Typically Performed In Order

# Scan Tips

- ❑ Cấu hình công cụ dò quét theo địa chỉ/dải địa chỉ IP chứ ko theo tên miền do nhiều mạng sử dụng DNS để thực hiện cân bằng tải.
  - Địa chỉ IP có thể được cập nhật trong quá trình test.
  - Kết quả dò quét 2 địa chỉ được gộp thành 1 có thể dẫn tới bỏ sót nhiều thông tin.
  - Cố gắng khai thác dịch vụ nhưng địa chỉ IP bị thay đổi.
- ❑ Thực tế có thể có trường hợp là cùng 1 địa chỉ IP tham chiếu tới nhiều máy chủ vật lý (do cân bằng tải) gây khó khăn cho quá trình test.

# Dealing with Very Large Scans

Example Scan Target: 1.000/10.000/100.000 hosts & all ports

- ❑ Đối với 1000 máy: 65535 port TCP & 65535 port UDP.
  - Giả sử 1port/1sec thì cần ~131 mil sec (~4.15 years).
  - Vậy 100.000 hosts thì sao?
- ❑ Lấy mẫu đại diện của các máy.
  - Nhược điểm: Làm thế nào để xác định được đại diện?
- ❑ Lấy mẫu đại diện của các port.
  - Dò quét các cổng phổ biến như 21, 22, 23, 25, 80, 135, 137, 139, 445...
  - Nhược điểm: Các cổng khác thì làm ntn?

# Handling Large Scans by Limiting Scope

Example Scan Target: 1.000/10.000/100.000 hosts & all ports

- ❑ Sử dụng nhiều máy dò quét cùng lúc.
- ❑ Di chuyển gần hơn đến mục tiêu (nếu có thể).
- ❑ Sử dụng các phương pháp/công cụ để tối ưu quá trình dò quét.
  - Tăng tốc độ gửi gói tin, giảm thời gian chờ
  - Công cụ: Masscan, ScanRand, Zmap, SuperScan, Unicornscan
  - Nhược điểm: Có thể dẫn tới tấn công DoS

# Content

---

❑ Scanning Goals, Types, and Tips

➔ **Port Scanning**

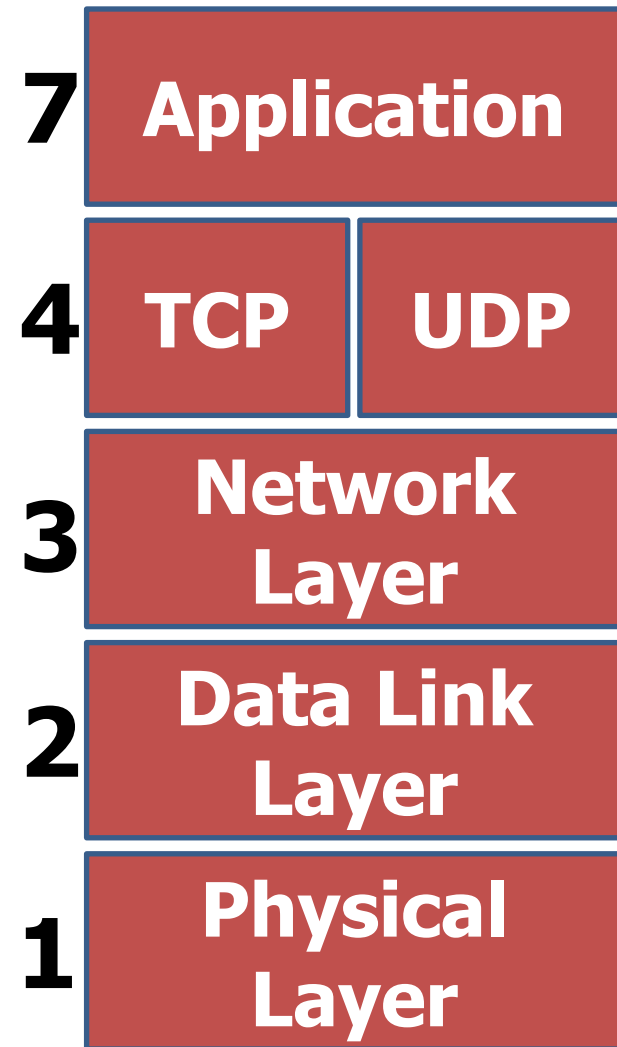
- Nmap
- Masscan
- Netcat

❑ Vulnerability Scanning



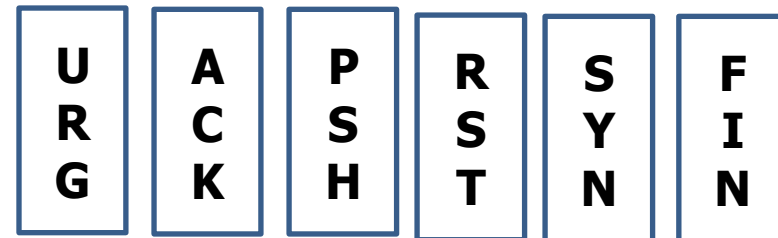
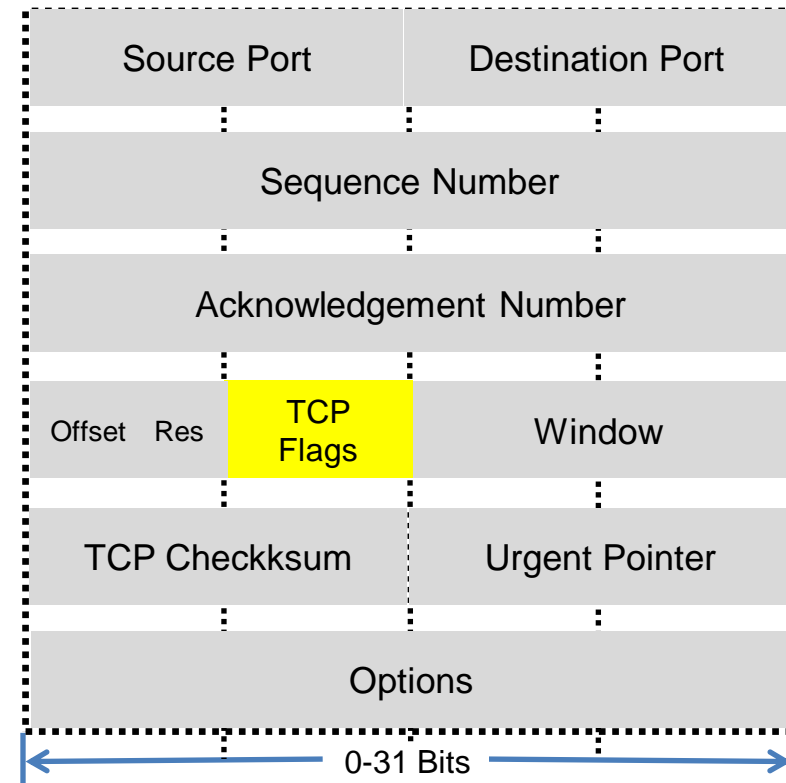
# Protocol Layers and TCP vs UDP

- ❑ Phần lớn các dịch vụ trên internet đều hoạt động dựa trên TCP hoặc UDP.
- ❑ TCP: truyền tải hướng kết nối (Connection oriented), cung cấp cơ chế báo nhận, đánh số thứ tự gói tin, phục hồi dữ liệu bị mất trên đường truyền.
- ❑ UDP: truyền tải hướng không kết nối (connectionless), không đảm bảo tính tin cậy khi truyền dữ liệu.



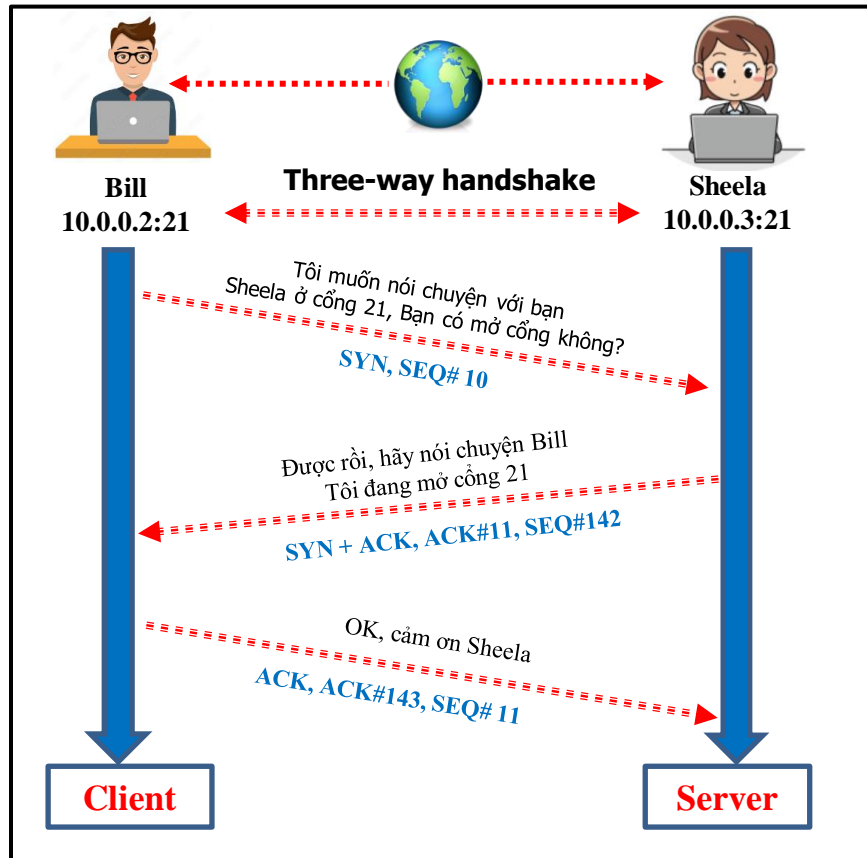
# TCP Communication Flags

- ❑ TCP Control Bits (Flags).
- ❑ Kết nối TCP hợp lệ bắt đầu bằng quá trình bắt tay 3 bước (three-way handshake).
- ❑ Handshake được sử dụng để trao đổi "Sequence Number" nhằm theo dõi việc gửi và truyền đạt thứ tự gói.

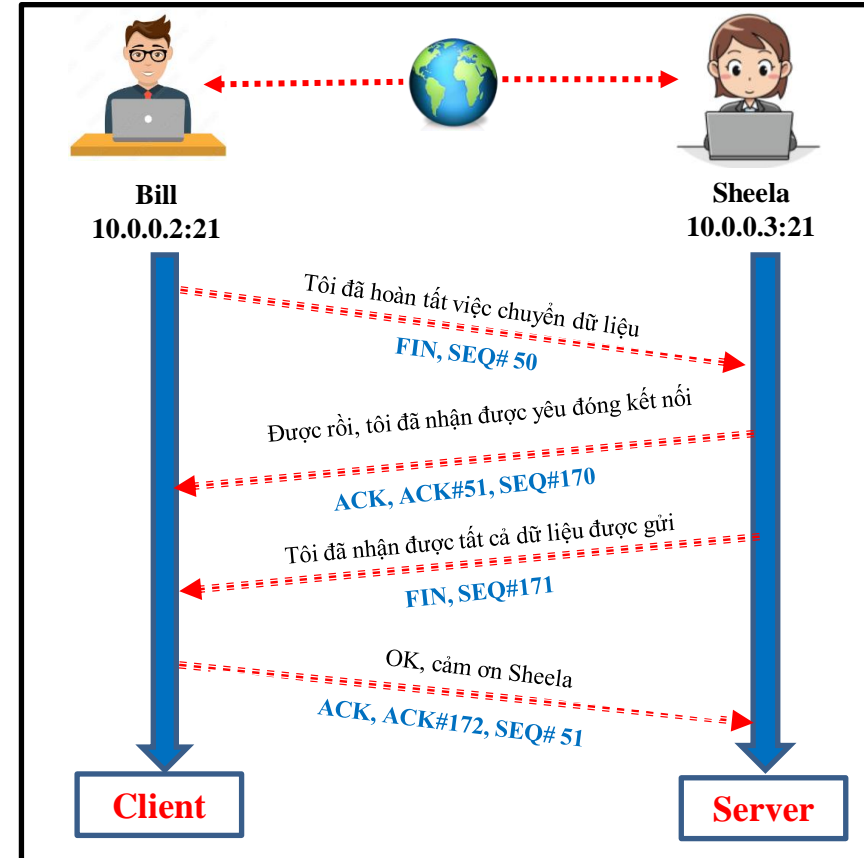


# TCP Three-Way Handshake (1/2)

## TCP Session Establishment (Three-way handshake)

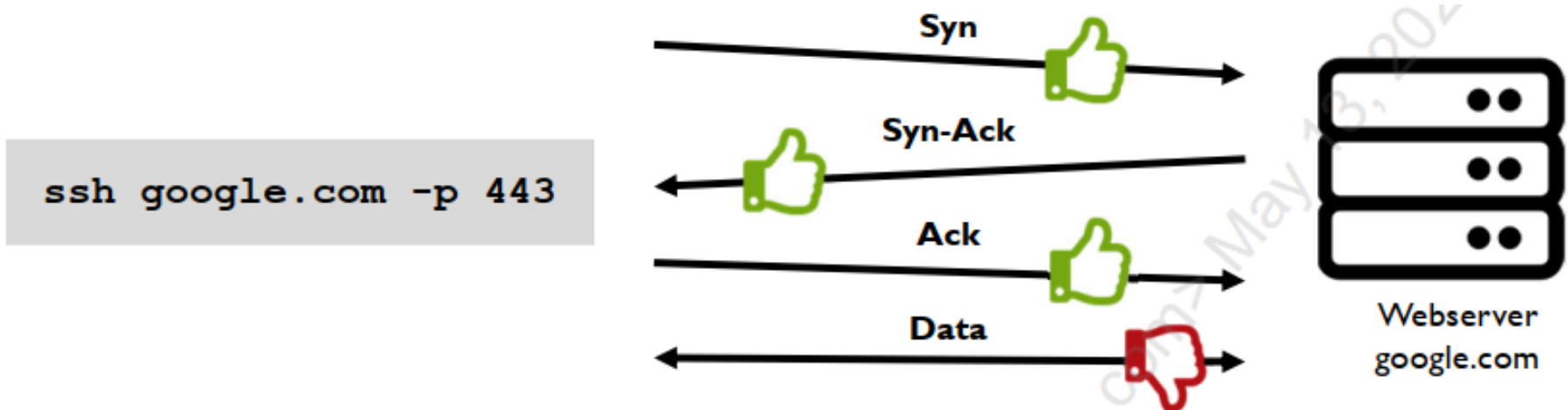


## TCP Session Termination



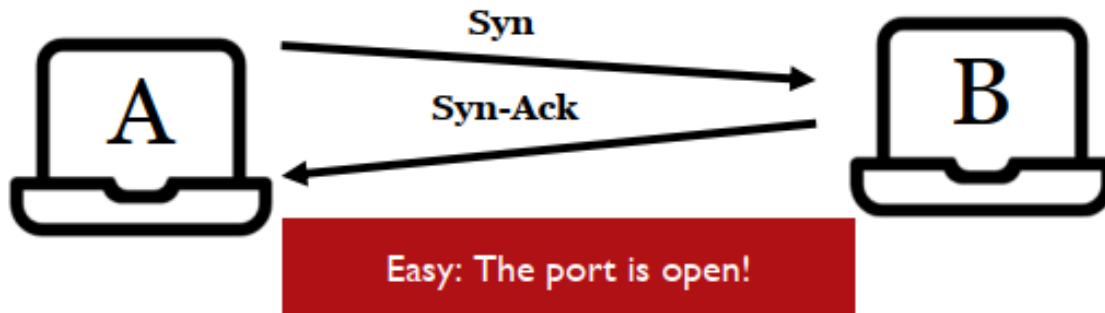
# TCP Three-Way Handshake (2/2)



- ❑ Quá trình bắt tay ba bước diễn ra bất kể giao thức ở tầng 7 (RFC 793).
  - Ví dụ: Nếu thực hiện SSH tới WebServer (port 443) thì handshake vẫn sẽ diễn ra nhưng sẽ có lỗi ở tầng ứng dụng.



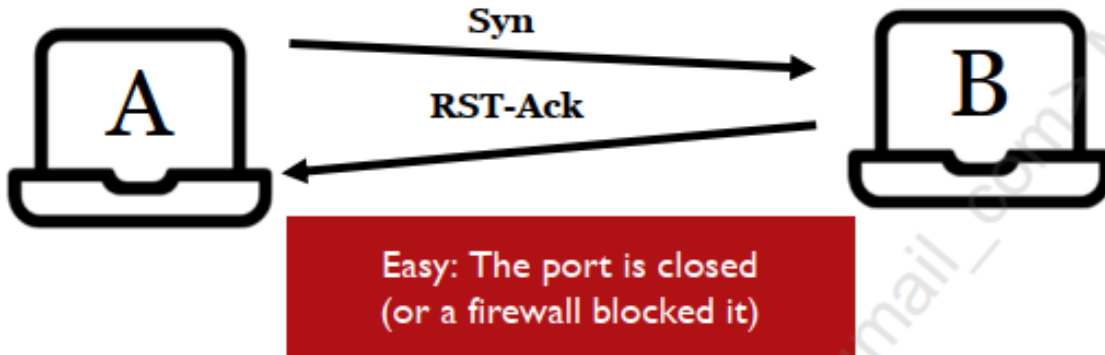
# TCP Behavior While Port Scanning (1/2)



**Case 1:**  
SYN-ACK back



Host	Port
Up	Open
	

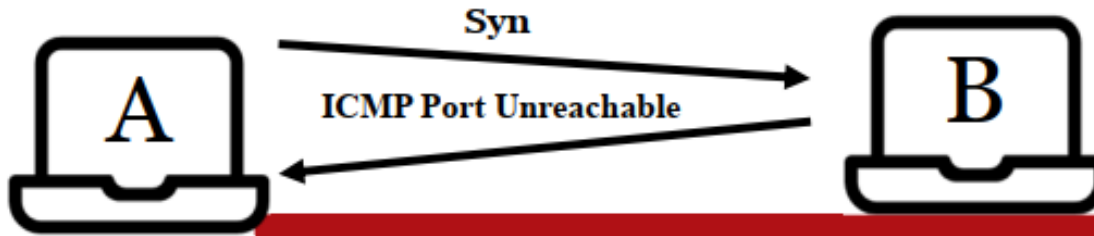
**Case 2:**  
RST-ACK back





Host	Port
Up	Closed
	

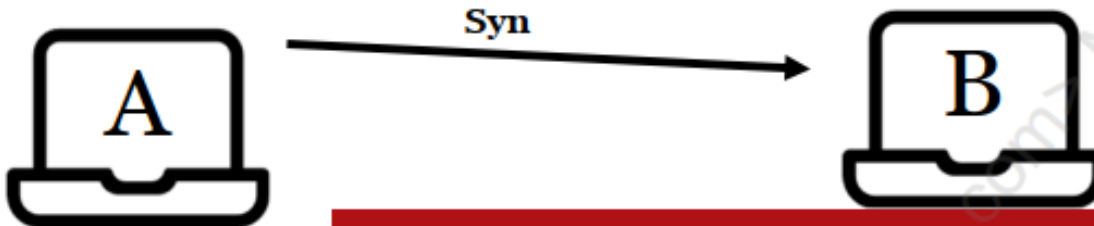
# TCP Behavior While Port Scanning (2/2)



**Case 3:**  
ICMP Port  
Unreachable back



Host	Port
Up	Closed
	

**Case 4:**  
Nothing Back



Host	Port
Unknown	Closed
	

# Results of Different TCP Behaviors

- ❑ Thông thường có nhiều cổng đóng hơn cổng mở.
  - Do đó hành vi của các cổng đóng sẽ ảnh hưởng đáng kể đến thời gian quét.
- ❑ Nếu scanner thu được gói tin phản hồi là RESET hoặc ICMP Port Unreachable thì quá trình quét sẽ diễn ra nhanh hơn nhiều.
- ❑ Nếu không nhận được phản hồi thì scanner sẽ phải đợi hết thời gian trước khi chuyển sang cổng tiếp theo.

# UDP Header

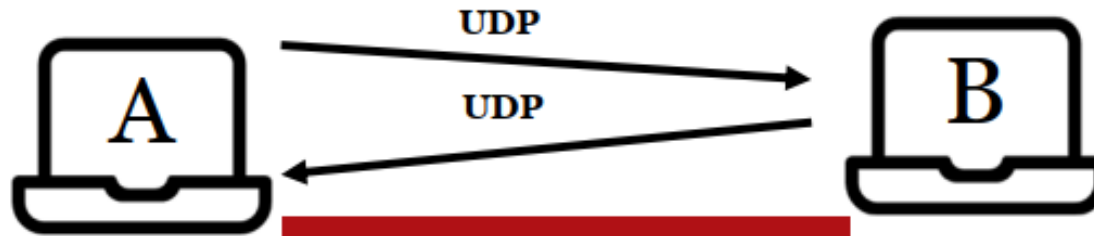
- ❑ UDP đơn giản hơn so với TCP, không có khái niệm “trạng thái kết nối”.
- ❑ Ít lựa chọn hơn cho việc dò quét.
- ❑ Dò quét chậm và ít tin cậy hơn.



Source Port	Destination Port
UDP Message Length	UDP Checksum
Data	
...	



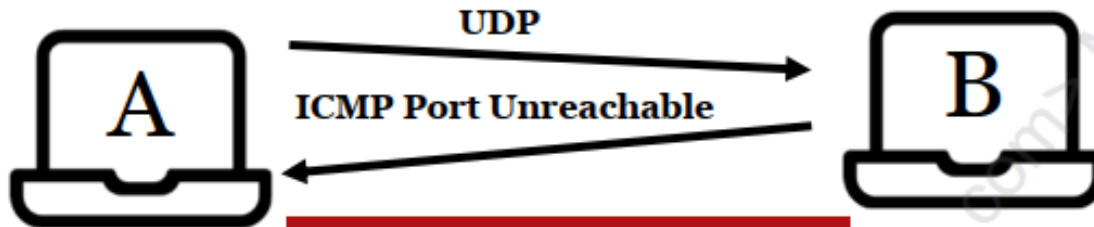
# UDP Behavior While Port Scanning (1/2)



**Case 1:**  
UDP back



Host	Port
Up	Open
	

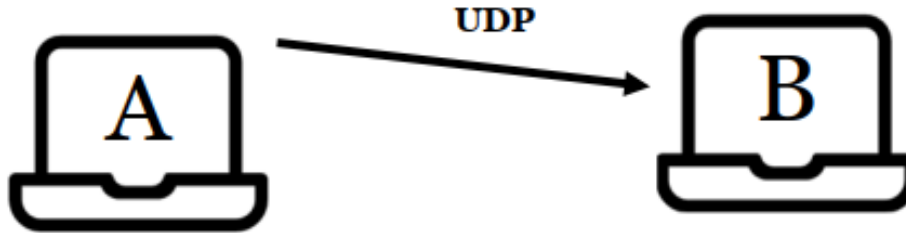
**Case 2:**  
UDP back



Host	Port
Up	Closed
	

# UDP Behavior While Port Scanning (2/2)

**Case 3:**  
No Response



**The port is inaccessible, but why?**

- Port is closed
- Firewall is blocking inbound UDP
- Firewall is blocking response
- Port is open, but the service does not respond unless it receives a valid payload

**We don't know why there wasn't a response**

Host	Port
Unknown	Unknown

?

?

## Nmap

Nmap sends a protocol-specific payload in an attempt to elicit a response for 35 protocols; other ports are sent an empty payload.

If Nmap does not receive a response, it marks it as:  
**open | filtered**

# Content

---

❑ Scanning Goals, Types, and Tips

➔ **Port Scanning**

- **Nmap**
- Masscan
- Netcat

❑ Vulnerability Scanning

# Nmap Port Scanner

- ❑ Nmap được phát triển bởi Gordon “Fyodor” Lyon & các cộng sự.
  - <https://nmap.org/> (version 7.93, 1 Sep 2022)
- ❑ Không đơn thuần là công cụ dò quét cổng.
  - Có khả năng dò quét lỗ hổng bảo mật thông qua Nmap Scripting Engine (NSE).

# Controlling Scan Speeds

- ❑ Nmap có nhiều tùy chọn khác nhau để điều chỉnh tốc độ quét (option -T)
  - 0 Paranoid: Gửi gói tin mỗi 5 phút (serial).
  - 1 Sneaky: Gửi gói tin mỗi 15 giây (serial).
  - 2 Polite: Gửi gói tin mỗi 0.4 giây (serial).
  - 3 Normal (default): Thực hiện quét song song, gửi nhiều gói tin tới nhiều cổng mục tiêu (parallel).
  - 4 Aggressive: Không bao giờ đợi phản hồi quá 1.25s và được khuyến cáo sử dụng cho các mạng nhanh & tin cậy (parallel).
  - 5 Insane: chỉ dành tối đa 15 phút cho mỗi máy chủ mục tiêu và chỉ đợi 0,3 giây phản hồi.

# Nmap Input and Output Options

- Import a list of hosts using: **-iL *filename***
  - Store output in the specified format with the following options:
    - oN *filename*** Normal format, saves what you see on the screen to the file
    - oG *filename*** Greppable format (technically deprecated), one line per host
- ```
Host: 1.2.3.4 (abc.def.com) Ports: 22/open/tcp//ssh//OpenSSH 4.3/, 443/...
```
- oX *filename*** XML format, useful as input for Metasploit
  - oS *filename*** Script kiddie format - "l33t speak", mixed case; not useful
  - oA *basename*** Store in all three major formats, Nmap adds the extension
    - normal → *basename.nmap*
    - greppable → *basename.gnmap*
    - XML → *basename.xml*

Tip: Always use the -oA option. Disk space is much cheaper than your time!

# Nmap and Address Probing (1/2)

- ❑ Theo mặc định, Nmap sẽ thực hiện thăm dò mục tiêu trước khi dò quét nó. Quá trình này được chia làm 2 pha:
  - Pha 1: Thăm dò địa chỉ mục tiêu
  - Pha 2: Dò quét cổng. Theo mặc định, Nmap chỉ thực hiện dò quét khi nhận được phản hồi từ Pha 1.
- ❑ Sử dụng tùy chọn `-Pn`, `-PN` hoặc `-P0` để bỏ qua Pha 1.
- ❑ Bên cạnh đó có thể sử dụng Nmap để thực hiện "Sweep scan".
  - `-sP` (Skip port scan): Không thực hiện dò quét cổng sau khi thực hiện thăm dò mục tiêu.

# Nmap and Address Probing (2/2)

## Windows & UID 0 User on Linux

- Same subnet:
  - ARP (Only)
- Different subnet:
  - ICMP Echo Request
  - TCP SYN tới cổng 443
  - TCP ACK tới cổng 80
  - ICMP Timestamp Request (Type 13)

\*Nmap gửi các gói tin trên tuần tự tới mục tiêu mà không chờ kết quả phản hồi giữa chúng

## Non-UID 0 on Linux

- TCP SYN tới cổng 80
- TCP SYN tới cổng 443
- ICMP không được sử dụng



# Nmap Network Probe/Sweeping Options

- **-PE** Send ICMP Echo Request (ICMP type 8)
- **-PSports** Use TCP SYN to specified ports in the port list, do not use a space between ports or after the **-PS** (for example, **-PS22,80**)
- sn -sP** Just to the host discovery scan (**-sP** is the old option, **-sn** is new)
- Pn** Don't probe and assume hosts are up, aliases: **-P0** (zero) or **-PN**
- PP** Send ICMP Timestamp Request (ICMP type 13)
- PM** Send ICMP Address Mask Request (ICMP type 17)
- PR** Use ARP to identify hosts (must be on Windows or UID 0 on Linux), this option only works with hosts on the same subnet and is used by default when targets are on the same subnet

# Optimizing Host Detection

- ❑ Để tối ưu hóa kết quả tìm kiếm “live” host, chúng ta có thể thêm vào 1 số port phổ biến.
  - Điều này có thể làm chậm quá trình tìm kiếm.
- ❑ Một số port phổ biến:
  - Windows: 137-139, 445, 3389.
  - Linux: 22, 111.
  - Top 20 port phổ biến: 80, 23, 443, 21, 22, 25, 3389, 110, 445, 139, 143, 53, 135, 3306, 8080, 1723, 111, 995, 993, 5900.

```
$nmap -PS21, 22, 23, 25, 80, 110, 111, 135, 137-139, 143, 443,  
445, 502, 993, 995, 1433, 1434, 1723, 3306, 3389, 5900, 8080 -  
PE -iL hosts.txt
```

# Nmap Port Scanning (After Host Detection)

❑ Theo mặc định, Nmap kiểm tra 1000 port thường được sử dụng.

- Sử dụng cờ **T:** và **U:** để mix TCP và UDP port).

```
$sudo nmap -n -PN -sT -sU -p- scanme.nmap.org
```

|                            |                                                               |
|----------------------------|---------------------------------------------------------------|
| <code>--open</code>        | Only show open ports (use this often!)                        |
| <code>-F</code>            | Scan the top 100 ports ("Fast" mode)                          |
| <code>--top-ports N</code> | Scan for the N most popular ports                             |
| <code>-p -</code>          | Scan all ports (excluding zero)                               |
| <code>-p 0-</code>         | Scan all ports (including zero), also <code>-p 0-65535</code> |
| <code>-p 22,80-88</code>   | Check only those ports                                        |

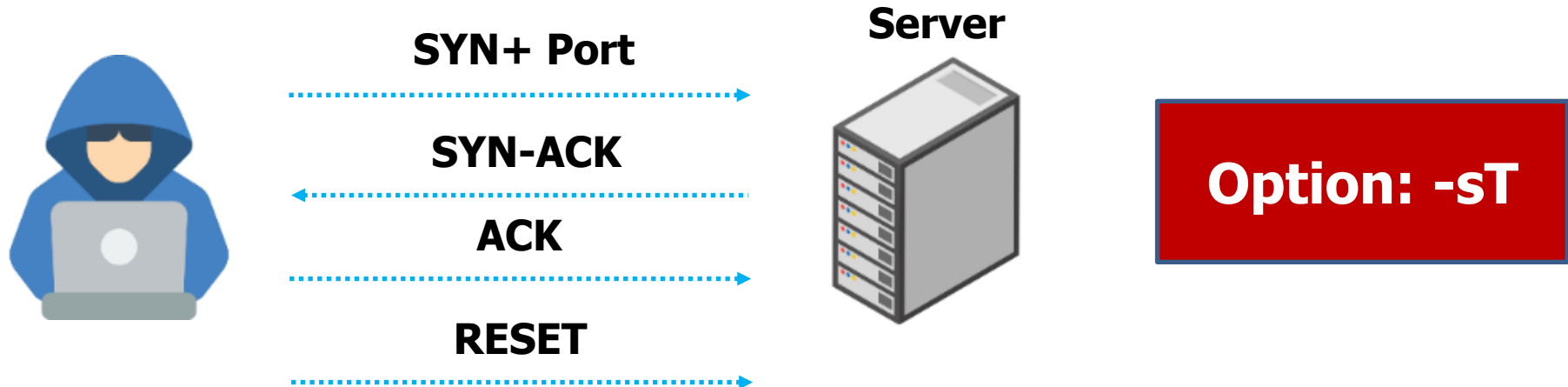
# Version Scanning

- ❑ Version scan sử dụng `-sV`.
- ❑ Có thể sử dụng `-A` cho OS fingerprinting, version scan, script scan (default scripts), traceroute

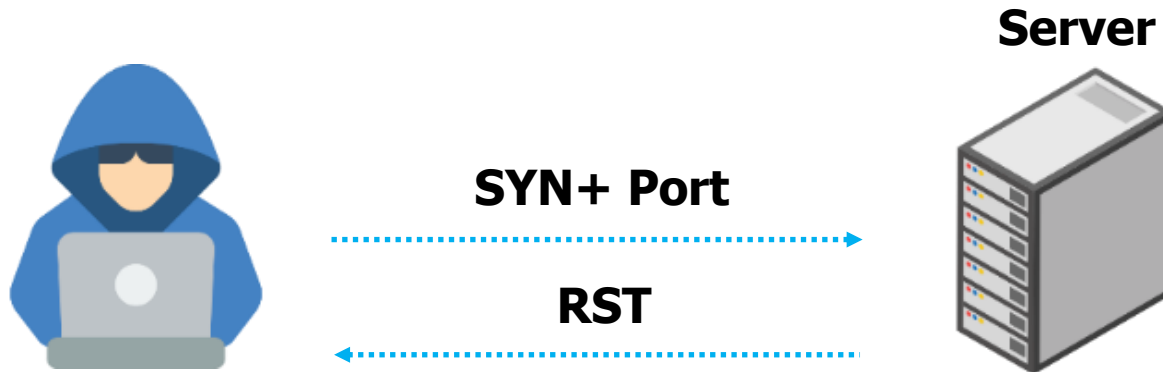
`-A = -O + -V + -sC + --traceroute`

# Nmap TCP Port Scan Types: Connect Scan

a) Cổng mở

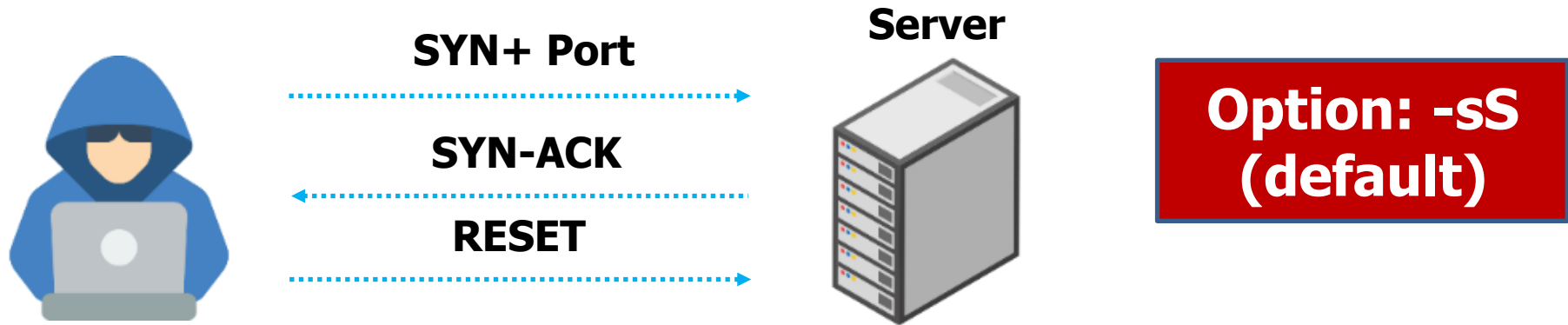


b) Cổng đóng

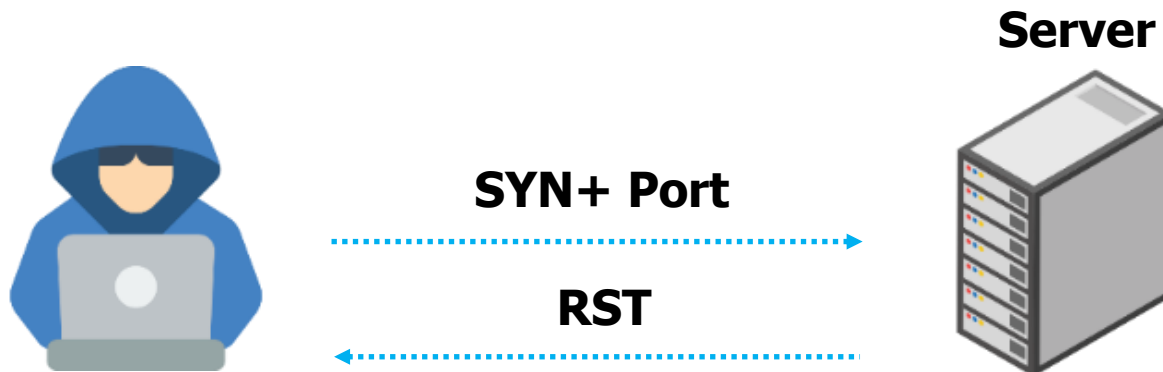


# Nmap TCP Port Scan Types: SYN Stealth Scan

a) Cổng mở



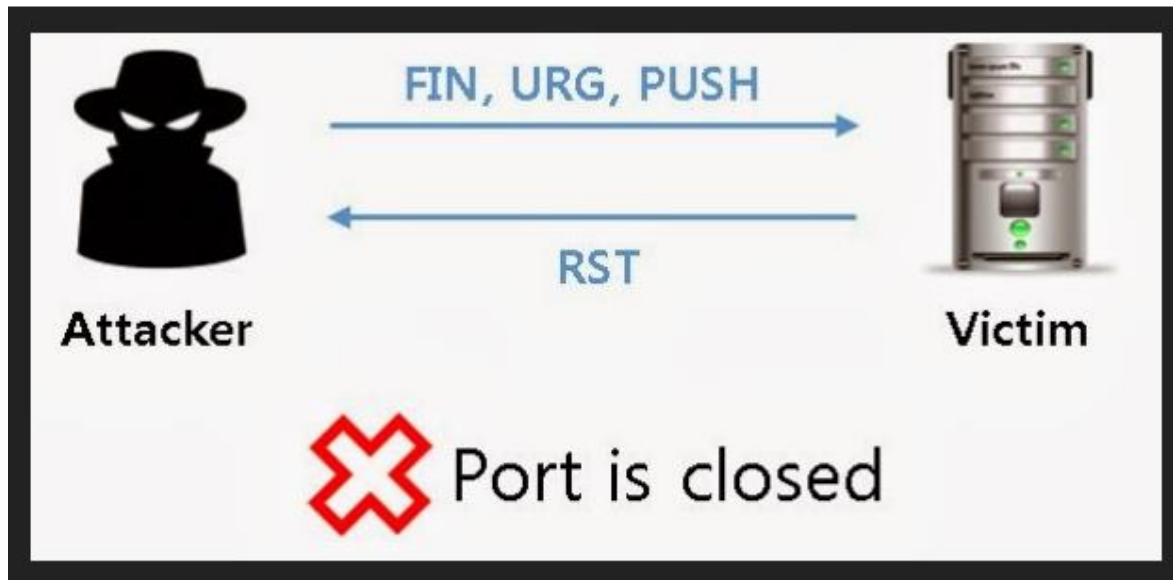
b) Cổng đóng (no response = filtered)



# XMAS Scan



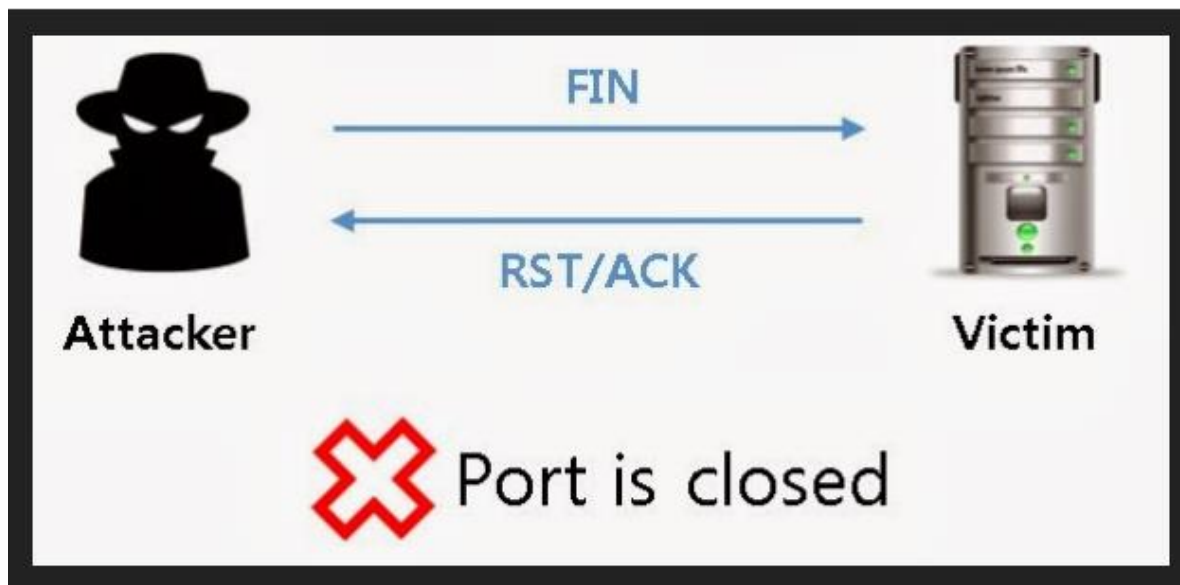
**Option: -sX**



# FIN Scan



**Option: -sF**

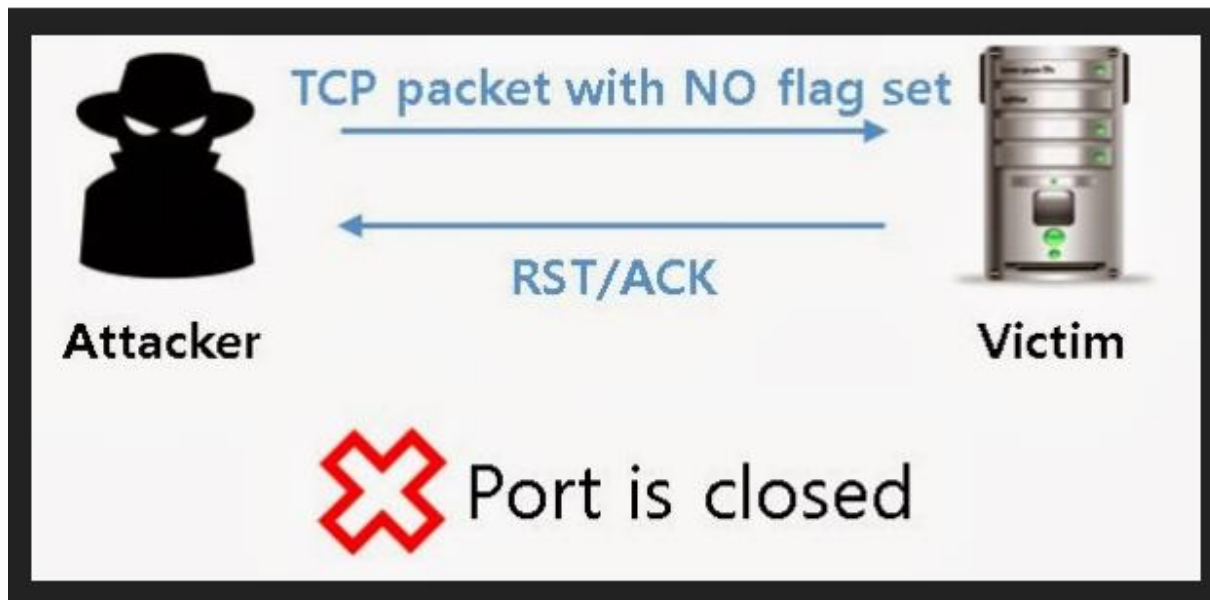




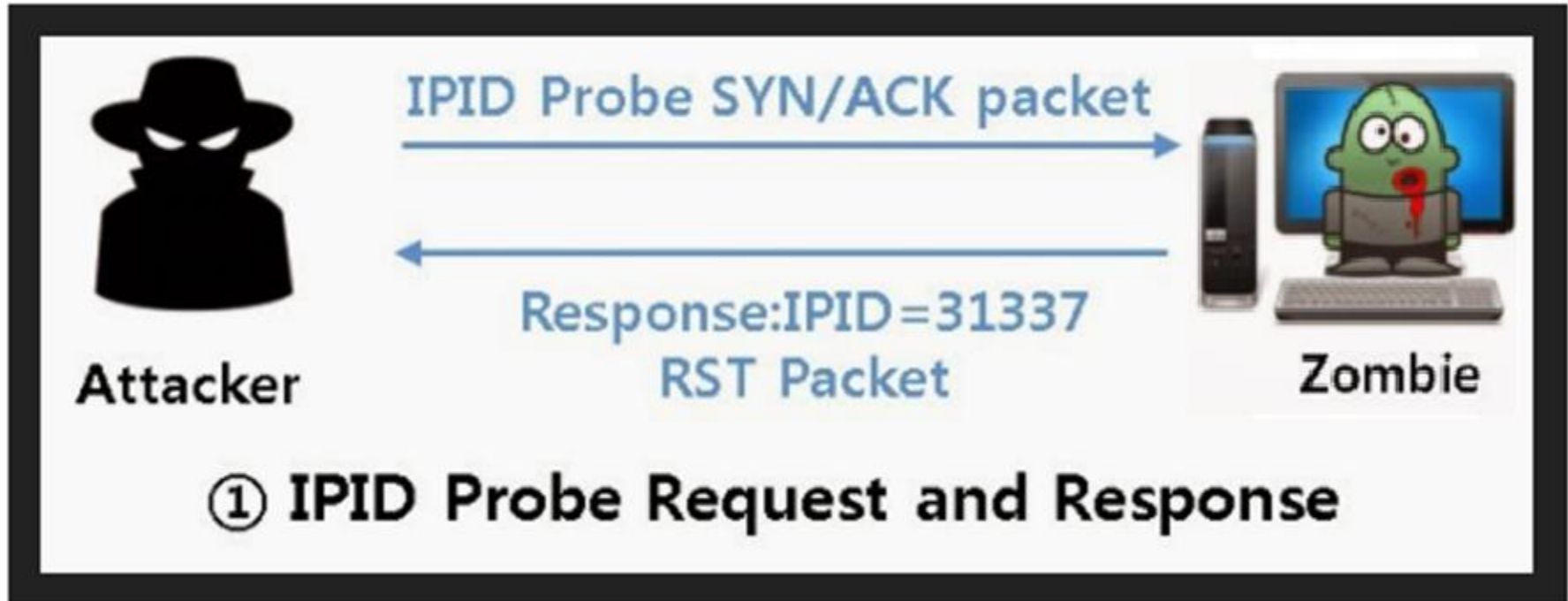
# NULL Scan



**Option: -sN**



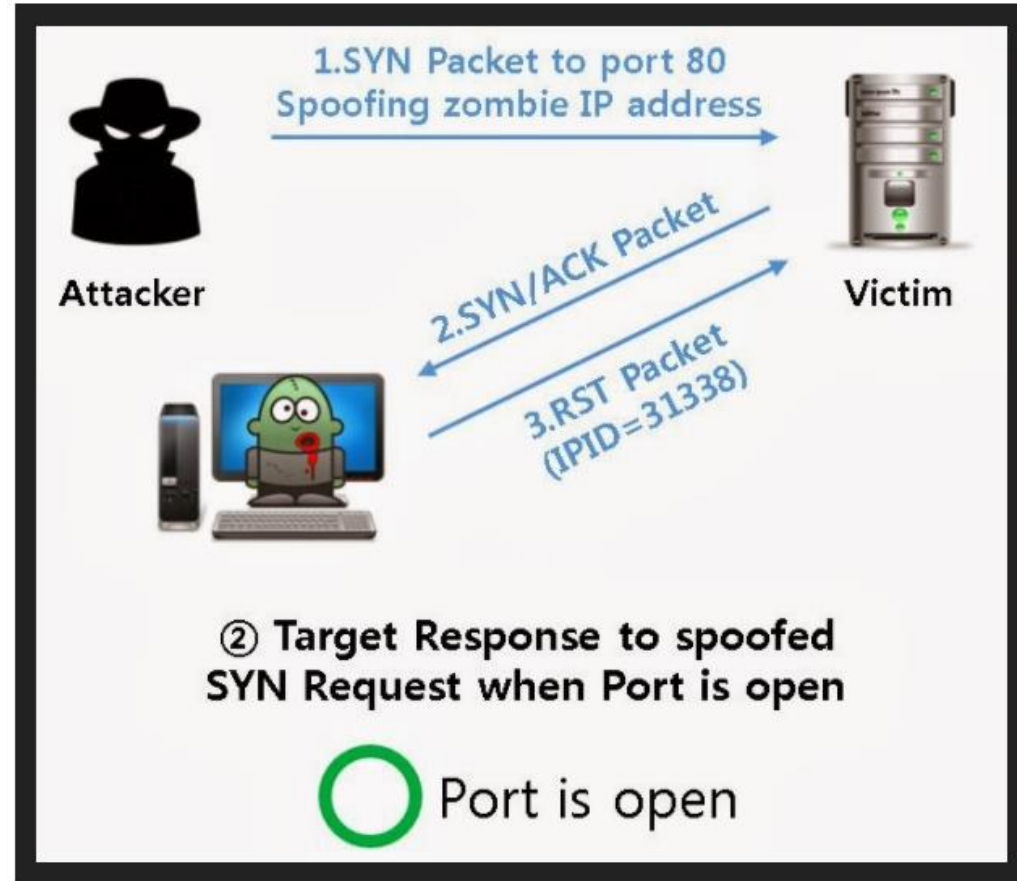
# IDLE/IPID Scan



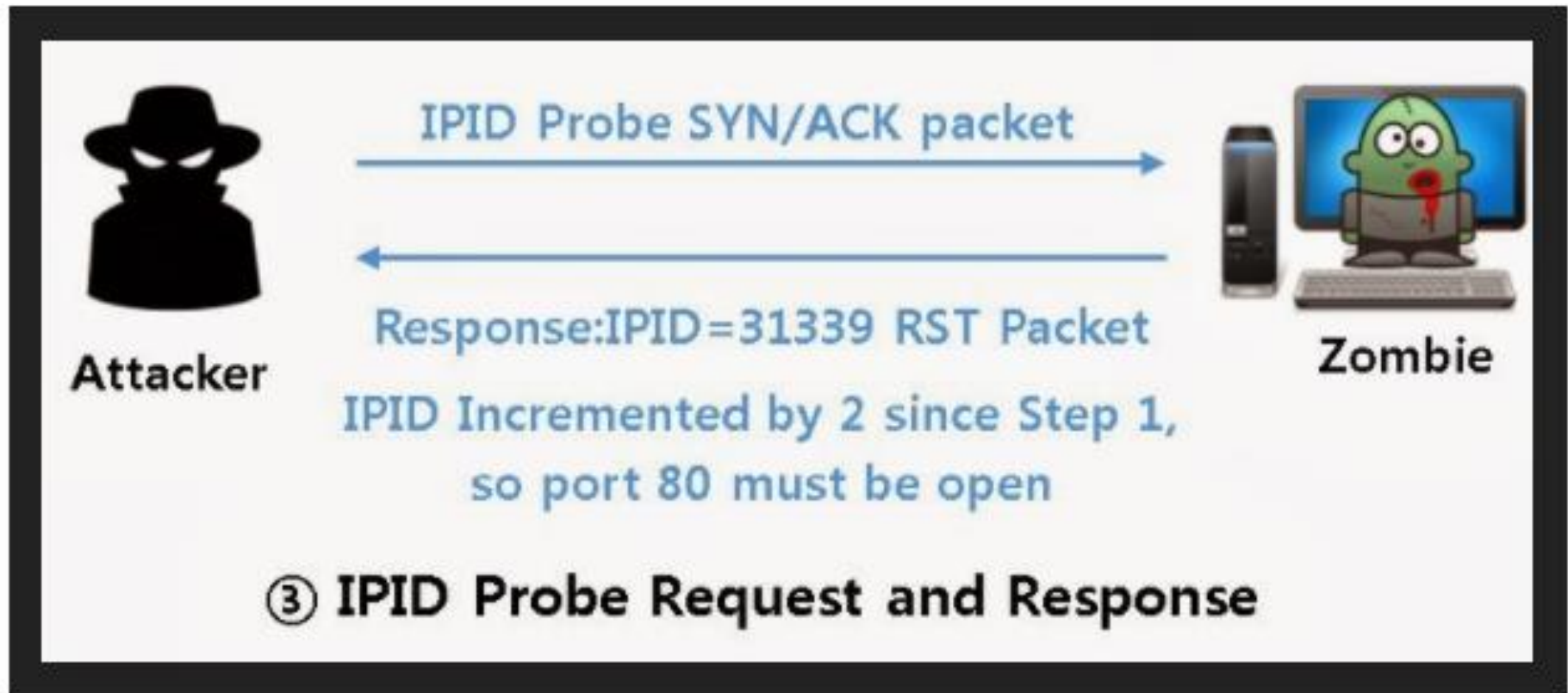
- ☐ Attacker gửi gói SYN/ACK tới Zombie
- ☐ Zombie gửi lại RST kèm IP ID

# IDLE/IPID Scan

- ❑ Attacker gửi gói tin SYN tới Victim với địa chỉ người gửi là Zombie
- ❑ Victim gửi trả SYN/ACK tới Zombie
- ❑ Zombie gửi RST kèm IP ID tăng lên (+1) trong trường hợp cổng mở

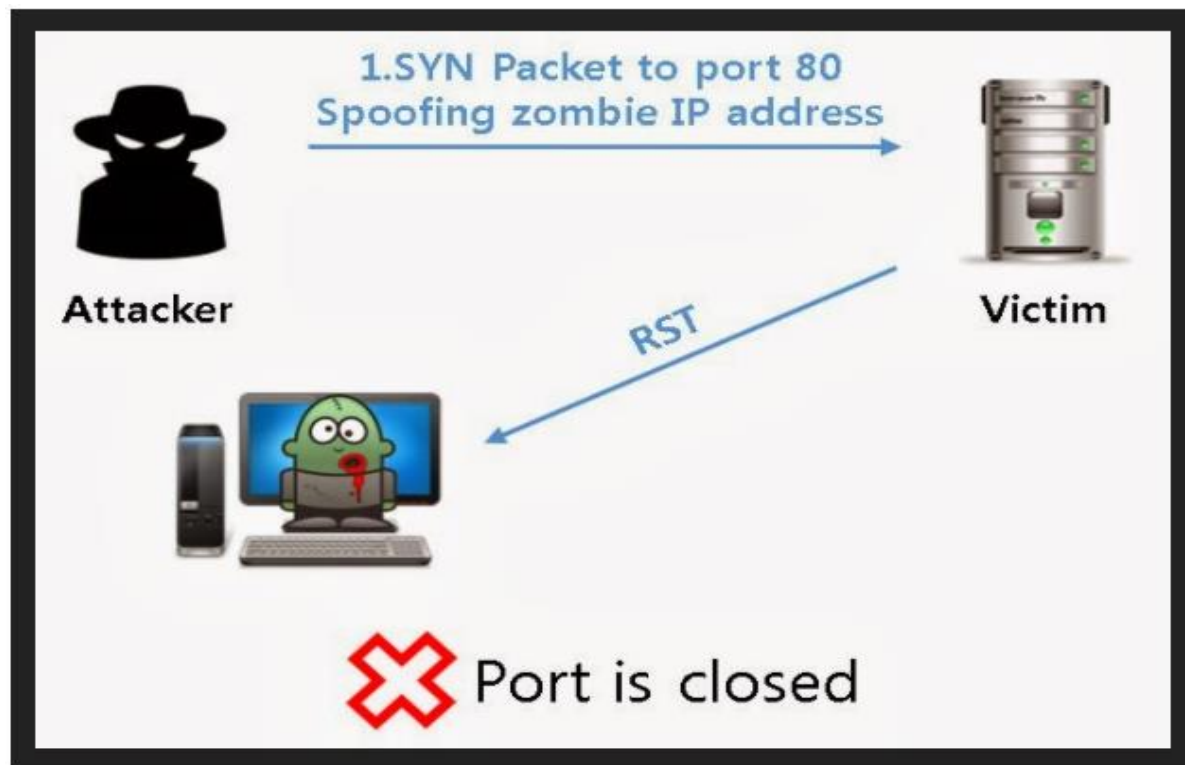


# IDLE/IPID Scan



- ❑ Attacker thăm dò IP ID một lần nữa
- ❑ Nếu IP ID của Zombie tăng lên 2 nghĩa là port mở

# IDLE/IPID Scan



- ❑ Trong trường hợp cổng đóng, Victim sẽ gửi lại Zombie gói tin RST và Zombie không có phản hồi gì.
- ❑ Nếu Attacker thăm dò IP ID thì chỉ thấy IP ID tăng thêm 1.

# Nmap Scripting Engine Scripts

- ❑ NSE được viết bằng Lua.

- ❑ Chạy tất cả scrips trong danh mục "default".

```
$sudo nmap -sC [target] -p [ports]
```

- ❑ Chạy scrips cá nhân, tất cả scripts, danh mục, tất cả trong thư mục.

```
$sudo nmap --script=[script, all, category, dir..] [target] -p [ports]
```

- ❑ Sử dụng `--script-help` để biết thêm thông tin chi tiết.

# NSE Script Categories

- **Auth:** Test authentication
- **Broadcast:** Look for target hosts via broadcasting
- **Brute:** Brute force auth attempts
- **Discovery:** Info gathering
- **Dos:** May cause denial-of-service
- **Exploit:** Exploit a vulnerability
- **External:** Send information to third party for lookup
- **Fuzzer:** Send unexpected data
- **Intrusive:** May leave logs, guess passwords, or otherwise impact the target
- **Malware:** Detect malware or backdoor
- **Safe:** Not designed to crash target
- **Version:** Detect service version
- **Vuln:** Look for a given vuln
- **Default:** Scripts run when Nmap is run with **-A** or **-sC** (no additional options)

❑ **script.db** chứa danh sách các script và danh mục của chúng

```
$grep safe /usr/local/share/nmap/scripts/script.db
```

```
$grep intrusive /usr/local/share/nmap/scripts/script.db
```

# Nmap UDP Scans (1/2)

- ❑ Nmap hỗ trợ UDP scan với tùy chọn **-sU**
- ❑ Nếu port có trong nmap-payloads file (cổng UDP cụ thể liên kết với dịch vụ UDP phổ biến) thì Nmap sẽ gửi "custom" payload, nếu không sẽ gửi blank payload.
  - Nmap 7.80 bao gồm 74 ports và 35 unique payloads.
  - Không phát hiện được các dịch vụ UDP phổ biến lắng nghe trên "unusual" port bởi vì blank payload sẽ được gửi tới các "unusual" port này.



## Nmap UDP Scans (2/2)

- ❑ “Close” port có thể phản hồi với ICMP Port Unreachable.
  - Nmap có tính năng thích ứng với tốc độ gửi gói tin phản hồi ICMP Port Unreachable -> điều chỉnh tốc độ gửi gói UDP phù hợp
  - Linux chỉ gửi 1 ICMP Port Unreachable mỗi giây (65535 port~18h/host), từ Nmap 7.40, tùy chọn `--defeat-icmp-ratelimit` giảm đáng kể thời gian dò quét UDP bằng việc gán nhãn các cổng không phản hồi (và có thể open) là “closed|filtered”.

# Common Ports

- ☐ DNS Server (??)
- ☐ TFTP Server (??)
- ☐ NTP Port (??)
- ☐ SNMP Port (??)
- ☐ Telnet Port (??)
- ☐ LDAP Port (??)
- ☐ Netbios Port (??)
- ☐ Citrix Port (??)
- ☐ Oracle Port (??)
- ☐ NFS Port (??)
- ☐ POP3 Port (??)
- ☐ POP3S Port (??)

# Common Ports

- ❑ DNS Server (TCP/UDP 53)
- ❑ TFTP Server (UDP 69)
- ❑ NTP Port (UDP 123)
- ❑ SNMP Port (UDP 161/162)
- ❑ Telnet Port (23)
- ❑ LDAP Port (389)
- ❑ Netbios Port (135-139,445)
- ❑ Citrix Port (1495)
- ❑ Oracle Port (1521)
- ❑ NFS Port (2049)
- ❑ POP3 Port (110)
- ❑ POP3S Port (995)

# Common Ports

---

- ☐ RDP Port (??)
- ☐ Sybase Port (??)
- ☐ SIP Port (??)
- ☐ VNC Port (??)
- ☐ FTP Port (??)
- ☐ Web Servers (??)
- ☐ HTTPS Servers (??)
- ☐ SSH Servers(??)
- ☐ SMTP Server(??)
- ☐ SMTPS Server(??)

# Common Ports

---

- ❑ RDP Port (3389)
- ❑ Sybase Port (5000)
- ❑ SIP Port (5060)
- ❑ VNC Port (5900/5800)
- ❑ FTP Port (20/21)
- ❑ Web Servers (80)
- ❑ HTTPS Servers (443)
- ❑ SSH Servers(22)
- ❑ SMTP Server(25)
- ❑ SMTPS Server(465)

# Content

---

❑ Scanning Goals, Types, and Tips

## ➔ Port Scanning

- Nmap
- **Masscan**
- Netcat

❑ Vulnerability Scanning

# Nmap limitations and Host Groups

- ❑ Nmap phải kết thúc dò quét 1 “host group” trước khi chuyển qua bất kỳ host nào trong group tiếp theo
  - Do đó hành vi của các cổng đóng sẽ ảnh hưởng đáng kể đến thời gian quét.
- ❑ Khi quét song song, Nmap chia mục tiêu thành “host groups”
  - Một host chậm dẫn đến toàn bộ “host group” bị chậm
  - <https://nmap.org/book/man-performance.html>
- ❑ Kích thước “host group” là động hoặc có thể điều chỉnh:
  - --min-hostgroup numhosts
  - --max-hostgroup numhosts

# Faster Scanning

- ❑ Nmap là “stateful” scanner – gửi SYN packet và đợi phản hồi.
  - “Stateless” scanner gửi SYN packet, không đợi phản hồi.
- ❑ Bypass “kernel” để tăng tốc độ và giảm tài nguyên
  - Bởi vì kernel bị bypass nên kernel sẽ không biết phải làm gì với gói phản hồi SYN-ACK -> kernel có thể gửi RESET.
  - Để ngăn ngừa kernel gửi RESET, có thể thiết lập “Drop” gói tin RESET (outbound) sử dụng tường lửa.



# Masscan

- ❑ Masscan hỗ trợ trên Windows, Linux, macOS -> tập trung vào “tốc độ”
  - Có thể quét toàn bộ Internet dưới 6 mins, gửi 10 triệu gói tin mỗi giây
- ❑ Sử dụng tương tự nmap:

```
masscan -p22, 445, 3389 --rate 15000 10.0.0.0/8
```

  - Kiểm tra port 22, 445, 3389
  - Giới hạn 15.000 gói tin mỗi giây
  - Scan 10.x.x.x subnet (16 triệu địa chỉ)
  - Hiển thị kết quả
- ❑ Luôn luôn sử dụng “rate limit” khi scan
- ❑ <https://github.com/robertdavidgraham/masscan>

# Masscan Output

- ❑ Đối với “large” scans, sử dụng định dạng binary của Masscan để lưu kết quả:

```
masscan -p0-65535 --rate 15000 -oB myscan.mass 10.0.0.0/8
```

- ❑ Output formats:

- List (-oL): status, protocol, port, IP, timestamp
- XML (-oX): XML format
- Binary (-oB): Custom Masscan format
- Grepable (-oG)/JSON (-oJ)/Uniconscan (-oU)

- ❑ Binary file format có thể chuyển đổi sang định dạng khác với --readscan

```
masscan --readscan myscan.mass -oX myscan.xml
```

# Extracting Live Host and Open Ports

❑ Chúng ta thường muốn trích xuất:

- Tất cả live hosts
- Tất cả live ports
- Tất cả live hosts với live port

❑ Trước hết chuyển đổi binary file qua greppable:

```
masscan --open --readscan myscan.mass -oG myscan.grep
```

❑ Sử dụng grep để trích xuất dữ liệu mong muốn.

- “Get all live hosts”

```
grep /open/ myscan.grep | cut -d ` ` -f 2 | sort -uV >newscan.txt
```

- “Get all ports”

```
grep /open/ myscan.grep | cut -d ` ` -f 4 | cut -d / -f 1 | sort -nk  
1 | uniq >newscan.txt
```

# Content

---

❑ Scanning Goals, Types, and Tips

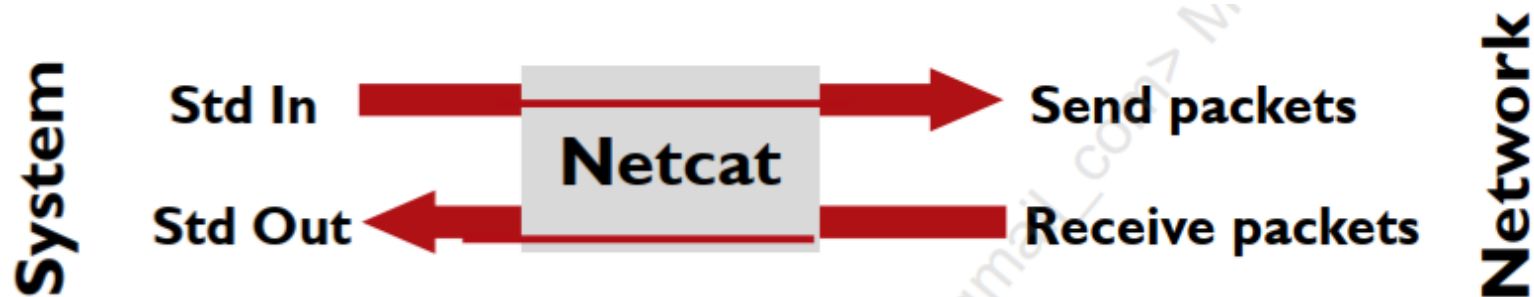
➔ **Port Scanning**

- Nmap
- Masscan
- **Netcat**

❑ Vulnerability Scanning

# Netcat for Pentester

- ❑ Netcat: General-purpose TCP/UDP network tool
  - Có sẵn trong nhiều phiên bản Linux (hoạt động trên cả Windows).
  - Phiên bản hiện tại của Nmap có sẵn ncat (có các tính năng của netcat + SSL).
- ❑ Netcat nhận dữ liệu từ "Standard In" và gửi chúng qua mạng.
- ❑ Nhận dữ liệu từ mạng và đẩy tới "Standard Out".
- ❑ Thông báo từ Netcat đẩy tới "Standard Error".



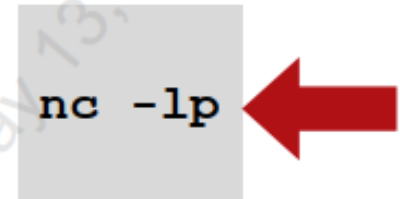
# Netcat Command Flags

**nc** [options] [targetIP] [remote\_port(s)]

- n** Don't resolve names
- v** Be verbose, printing when a connection is made
- l** Listen mode (default is client)
- L** Listen harder (Windows only)—make a persistent listener
- p N** Local port (In listen mode, this is the port on which Netcat is listening. In client mode, this is the source port for packets sent.)
- e bin** Program to execute after connection occurs
- wN** Timeout for connects, waits for N seconds
- z** Zero-I/O mode: Don't send any data, just emit packets
- u** UDP mode (default is TCP)



**Clients initiate one connection**



**Listeners wait for one connection**

Netcat options can be combined

For example, the options **-n -v -l -p** can be combined to **-nvlp**

# Netcat Client Grab Service Info

- ❑ Sử dụng netcat để lấy thông tin dịch vụ
  - Pentester có thể cần nhập vào chuỗi kết nối để thu được phản hồi.

Retrieve banner from SSH server

```
sec560@slingshot:~$ nc -nv 10.130.10.10 22
Connection to 10.130.10.10 22 port [tcp/*] succeeded!
SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
^C
```

Retrieve banner from SMTP Server

```
sec560@slingshot:~$ nc -nv 10.130.10.25 25
Connection to 10.130.10.25 25 port [tcp/*] succeeded!
220 mail01.hiboxy.com Microsoft ESMTPL MAIL Service ready
at Tue, 2 Feb 2022 02:02:22 +0000
```

Retrieve banner from Web server, requires extra input to get response

GET / HTTP/1.0<enter>  
<enter>

```
sec560@slingshot:~$ nc -nv 10.130.10.10 80
Connection to 10.130.10.10 80 port [tcp/*] succeeded!
GET / HTTP/1.0

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
...
```

# Automating Service String Information Gathering

- ❑ Netcat có thể lấy thông tin “chuỗi kết nối (connection strings)” từ một loạt cổng trên máy mục tiêu.
- ❑ Chỉ định phạm vi cổng X-Y.

```
nc -nvw2 [targetIP] [port-range]
```

```
$echo "" | nc -nvw2 [targetIP] [port-range]
```

```
sec560@slingshot:~$ nc -nvw2 10.130.10.10 20-81
nc: connect to 10.130.10.10 port 20 (tcp) failed: Connection refused
nc: connect to 10.130.10.10 port 21 (tcp) failed: Connection refused
Connection to 10.130.10.10 22 port [tcp/*] succeeded!
SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
nc: connect to 10.130.10.10 port 23 (tcp) failed: Connection refused
...
Connection to 10.130.10.10 80 port [tcp/*] succeeded!
nc: connect to 10.130.10.10 port 81 (tcp) failed: Connection refused
```

- ❑ Trên thực tế đây là một “port scanner” có thu thập banner.



# Moving Files

- ❑ Chúng ta có thể chuyển file với Netcat bằng cách chuyển hướng file (dữ liệu không được mã hóa).

```
sender#nc -w 3 [destination IP] 9899 < out.file
```

```
receiver#nc -lvp 9899 > out.file
```

- ❑ Kiểm tra lại dữ liệu với md5sum

```
sender#md5sum out.file
```

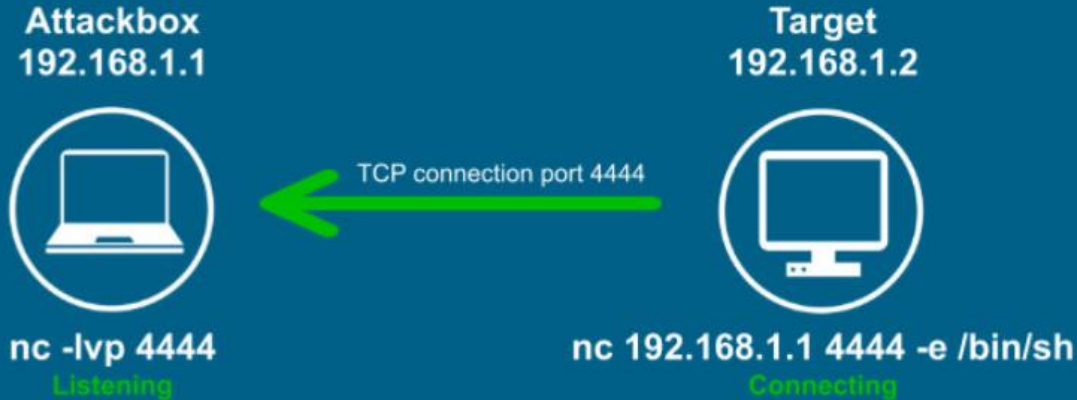
```
c6779ec2960296ed9a04f08d67f64422
```

```
receiver#md5sum out.file
```

```
c6779ec2960296ed9a04f08d67f64422
```

# Reverse & Bind shell with nc

## Netcat Reverse shell



## Netcat Bind shell



# Content

---

❑ Scanning Goals, Types, and Tips

❑ Port Scanning

- Nmap
- Masscan
- Netcat

➔ **Vulnerability Scanning**

# Vulnerability Scanner Goals

- ❑ Thực hiện tự động tìm kiếm, xác định lỗ hổng bảo mật.
  - Vấn đề cấu hình.
  - Không cập nhật bản vá, updates.
  - Sử dụng thông tin đăng nhập mặc định.
  - Sử dụng phần mềm lỗi thời, không còn được hỗ trợ.
- ❑ Output.
  - Danh sách lỗ hổng bảo mật (gắn với host/port tương ứng).
  - Đánh giá rủi ro.
  - Khuyến nghị và biện pháp phòng chống.
- ❑ Phân loại.
  - General Purpose (Nessus, Nexpose, Qualys, OpenVAS).
  - Web Application (AppScan, NetSparker).
  - Application Specific (SSLScan, OnesixtyOne, WPScan).

# Vulnerability Assessment

## ❑ Vulnerability assessment

- Xác định lỗ hổng của OS, thiết bị, ứng dụng
- Công cụ: Nessus, Acunetix, nmap

## ❑ Tìm kiếm các thông tin có liên quan về lỗ hổng

- Sử dụng Google
- Sử dụng Exploit Database

The image shows a Google search for "openssh 5.3 exploit" and a screenshot of the Exploit Database website. The Google search results show a link to "Openssh version 5.3 : Security vulnerabilities". The Exploit Database website displays details for a vulnerability titled "ProFTPD 1.3.7a - Remote Denial of Service".

**Google Search Results:**

- Search query: openssh 5.3 exploit
- Results (0.44 seconds)
- Link: Openssh version 5.3 : Security vulnerabilities

**Exploit Database Details:**

| EDB-ID: | CVE: | Author: | Type: | Platform: | Date:      |
|---------|------|---------|-------|-----------|------------|
| 49697   | N/A  | XYNMAPS | DOS   | MULTIPLE  | 2021-03-22 |

**Additional Information:**

- EDB Verified: ✗
- Exploit: 📄 / 📄
- Vulnerable App:

**Exploit Details:**

- # Exploit Title: ProFTPD 1.3.7a - Remote Denial of Service
- # Date: 22/03/2021
- # Exploit Author: xynmaps
- # Vendor Homepage: <http://www.proftpd.org/>

# Methods for Discovering Vulnerabilities

- ❑ Vulnerability scanner có thể giúp xác định sự tồn tại của lỗ hổng theo nhiều cách khác nhau.
- ❑ Kiểm tra phiên bản phần mềm (ít chính xác nhất trong tất cả các phương pháp)
  - Một vài bản phân phối Linux thực hiện cập nhật bản vá nhưng vẫn giữ số phiên bản cũ dẫn đến “false positives”.
- ❑ Kiểm tra phiên bản giao thức
- ❑ Kiểm tra hoạt động, cấu hình
- ❑ Chạy mã khai thác

# Scan Types

## ❑ Unauthenticated (Most common).

- Scanner không có thông tin xác thực trên hệ thống mục tiêu.
- Chỉ có thể xác định được lỗ hổng trong các dịch vụ cho phép truy cập từ xa (không xác định được lỗ hổng trên client-site software).

## ❑ Authenticated (Less common).

- Có khả năng tìm kiếm lỗ hổng trên client-site software, xác định việc thiếu bản vá, lỗi cấu hình trên máy mục tiêu.

## ❑ Agent-based (Rare).

- Agent được triển khai trên máy mục tiêu.
- Tương tự như authen-scanner nhưng agent gửi report về server tập trung.

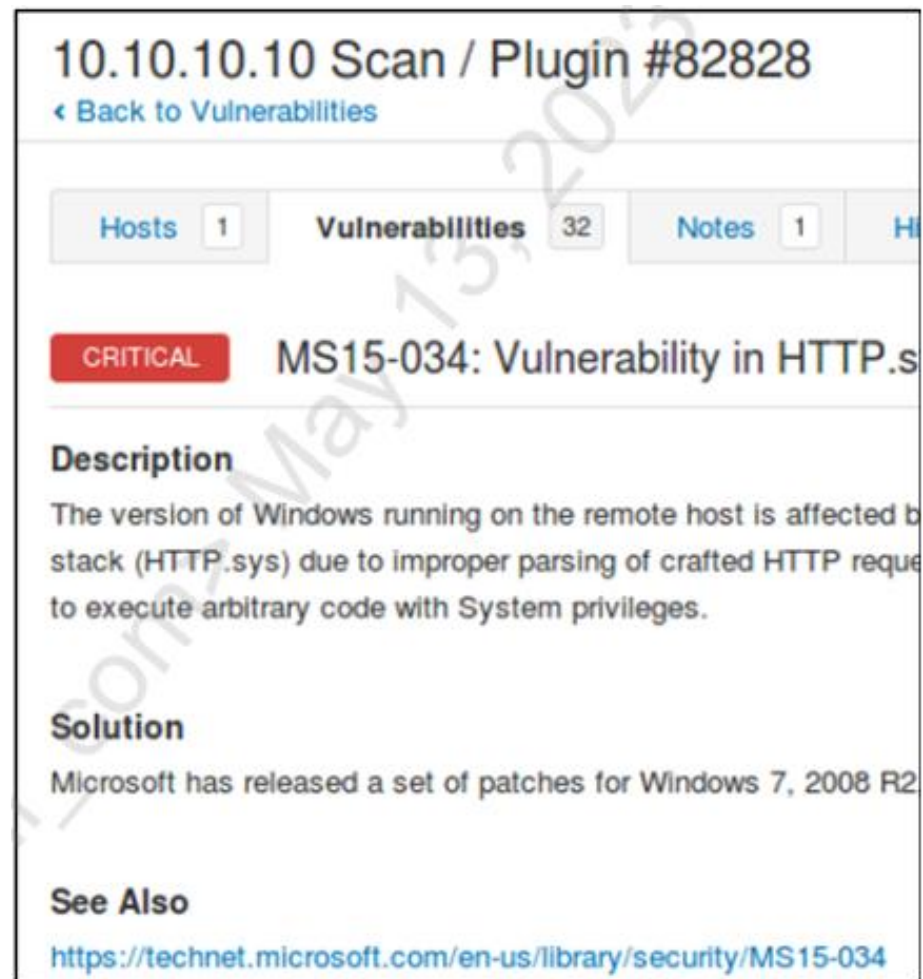
# Safe Checks and Dangerous Plugins

- ❑ Một vài plugins gây crash hoặc ảnh hưởng tiêu cực lên mục tiêu.
- ❑ Các plugins này thường được tắt theo mặc định và yêu cầu quản trị viên kích hoạt kiểm tra.
  - Kiểm tra RoE trước khi sử dụng plugins.
- ❑ Pentester thường hiếm khi thực hiện việc kiểm tra này
  - Các nhóm quản lý lỗ hổng nội bộ có nhiều khả năng được phép thực hiện các hoạt động kiểm tra này hơn.
- ❑ Attacker sẽ sử dụng các biện pháp kiểm tra nguy hiểm (hoặc tấn công) nếu nó mang lại lợi ích cho họ.
- ❑ Tip: ***Nhận được sự đồng ý trước khi sử dụng các plugin nguy hiểm để thực hiện dò quét.***



# Scan Results

- ❑ Mô tả danh sách lỗ hổng bảo mật (gắn với host/port tương ứng).
  - Giảm thiểu “false positives” bằng cách kiểm tra lại thủ công.
- ❑ Đánh giá, ước tính mức độ rủi ro.
- ❑ Khuyến nghị và biện pháp phòng chống.



10.10.10.10 Scan / Plugin #82828  
◀ Back to Vulnerabilities

| Hosts | Vulnerabilities | Notes |
|-------|-----------------|-------|
| 1     | 32              | 1     |

**CRITICAL** MS15-034: Vulnerability in HTTP.sys

**Description**  
The version of Windows running on the remote host is affected by a vulnerability in the HTTP.sys stack (HTTP.sys) due to improper parsing of crafted HTTP requests that can allow an attacker to execute arbitrary code with System privileges.

**Solution**  
Microsoft has released a set of patches for Windows 7, 2008 R2, and Windows Server 2008.

**See Also**  
<https://technet.microsoft.com/en-us/library/security/MS15-034>

# Thank you & Any questions?

