

# **Kiểm thử & Đánh giá an toàn hệ thống thông tin**

Network Pentesting Methodology -  
Perimeter Devices



1

Kiểm thử xâm nhập  
tường lửa



2

Kiểm thử xâm nhập  
IDS

1

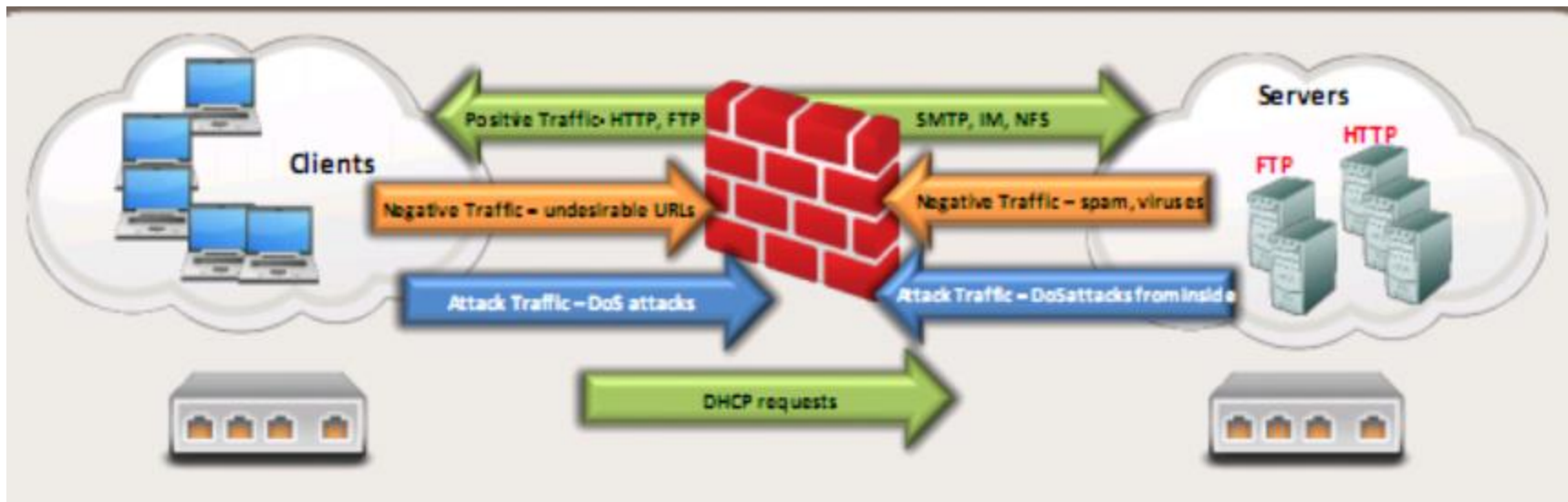
Kiểm thử xâm nhập  
tường lửa

2

Kiểm thử xâm nhập  
IDS

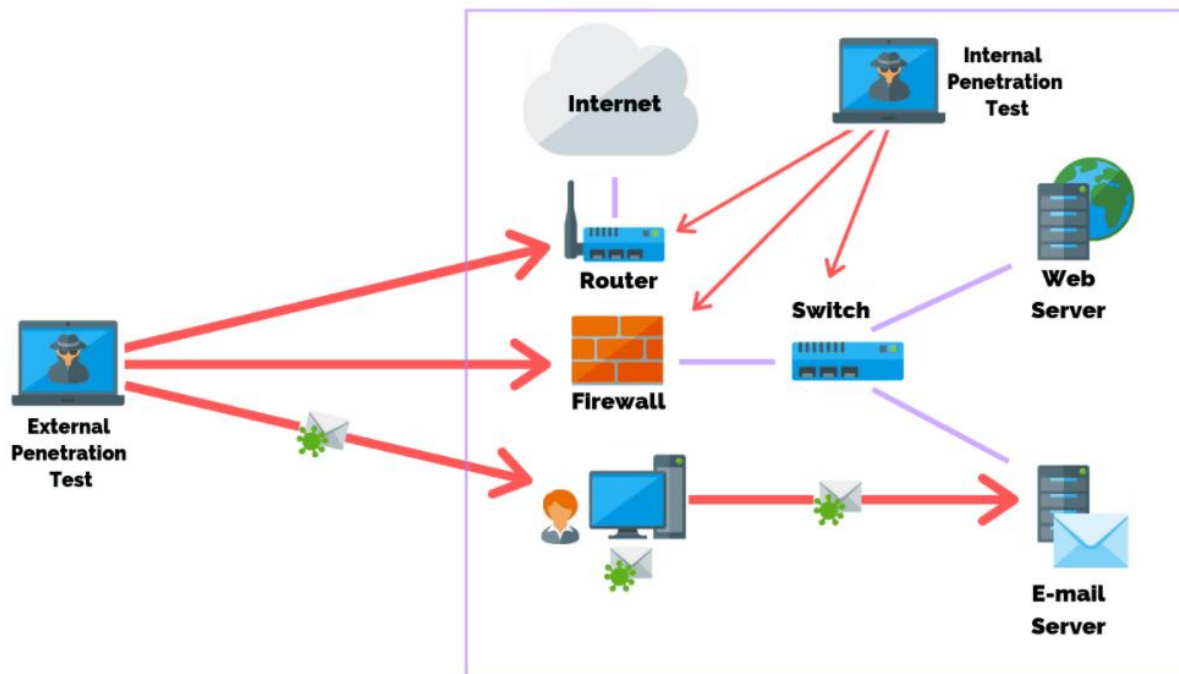
# Firewall Pentesting

- ❑ Kiểm thử tường lửa là quá trình xác định vị trí, phân tích cấu hình, xác định và tìm kiếm lỗ hổng trong quá trình hoạt động của tường lửa
- ❑ Là một phần quan trọng trong kiểm thử xâm nhập mạng từ bên ngoài



# Type of FW Pentesting

- ❑ Kiểm thử tường lửa từ bên ngoài, pentester cố gắng gửi các gói tin đến và kiểm tra xem gói tin có vượt qua được tường lửa hay chống lại được cấu hình luật trên tường lửa hay không
- ❑ Kiểm thử tường lửa từ bên trong, pentester sẽ phân tích các gói tin đi và kiểm tra xem tường lửa xử lý gói tin có đúng theo cấu hình luật hay không



# Testing the FW from Both sides

- ❑ Kiểm thử bên ngoài tường lửa (from outside) nhằm:
  - Phân tích cấu hình luật tường lửa (xác định cổng mở, protocol hỗ trợ, accept/deny policy)
  - Kiểm tra xem các kết nối trái phép có thể tạo ra với mạng bên trong tường lửa hay không
  - Kiểm tra xem hoạt động của tường lửa trước các gói tin giả mạo, gói tin phân mảnh, gói tin độc hại được gửi 1 cách có chủ đích

# Testing the FW from Both sides

- ❑ Kiểm thử bên trong tường lửa (from inside) nhằm:
  - Xác định các tập luật tường lửa
  - Kiểm tra xem các kết nối trái phép (có thể cần kiểm tra cả tunneled protocols) có thể tạo ra từ bên trong mạng ra ngoài Internet được hay không

# Locating the FW

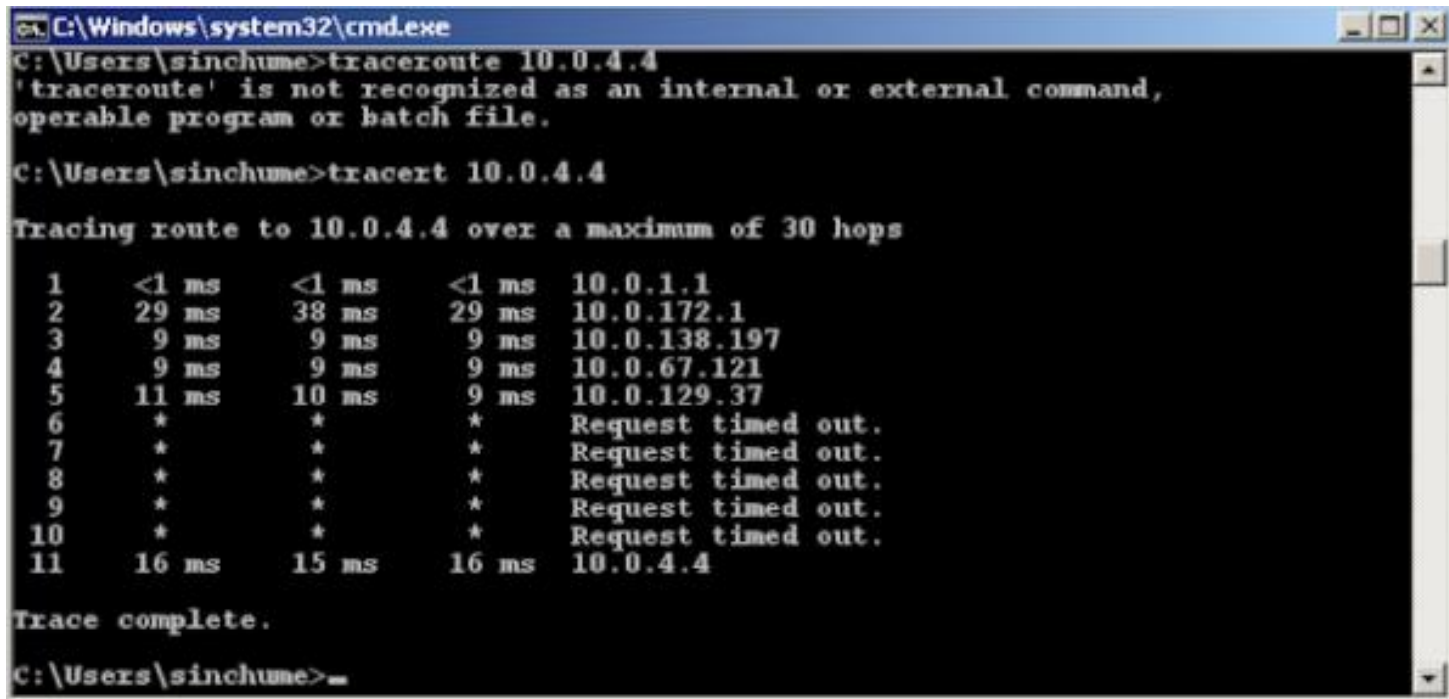
- ❑ Tìm kiếm các thông tin về tường lửa sẽ thực hiện kiểm thử (version, functions, features...) sử dụng OSINT
- ❑ Một vài FW có dấu hiệu rõ ràng:
  - Check Point's FW-1 lắng nghe trên TCP port 256-259
  - Check Point NG lắng nghe trên TCP port 18210, 18211, 18186, 18190, 18191, 18192
  - Microsoft's Proxy Server thường lắng nghe trên TCP port 1080 và 1745
- ❑ Sử dụng banner grabbing

```
C:\>nc -v -n 192.168.51.129 21
(UNKNOWN) [192.168.51.129] 21 (?) open
220 Secure Gateway FTP server ready.
```



# Locating the FW

- ❑ Sử dụng các công cụ tạo gói tin để xác định vị trí tường lửa
  - Sử dụng ***tracert*** để kiểm tra sự tồn tại của các thiết bị kiểm soát truy cập và thậm chí có thể là WAN IP của các thiết bị đó
  - Mặc định Windows tracert sử dụng ICMP, Linux/MacOS sử dụng UDP



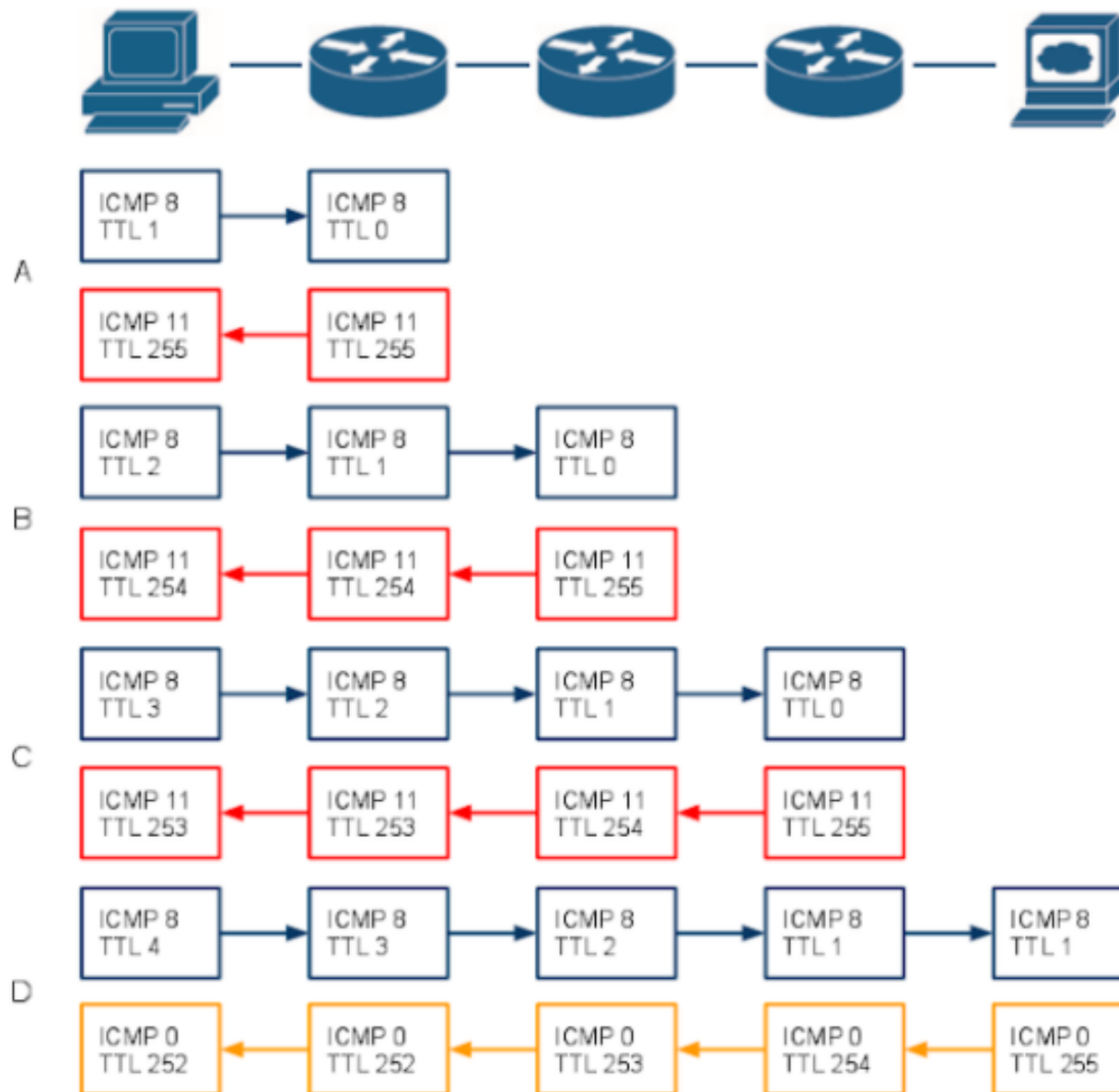
```
C:\Windows\system32\cmd.exe
C:\Users\sinchume>tracert 10.0.4.4
'tracert' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\sinchume>tracert 10.0.4.4

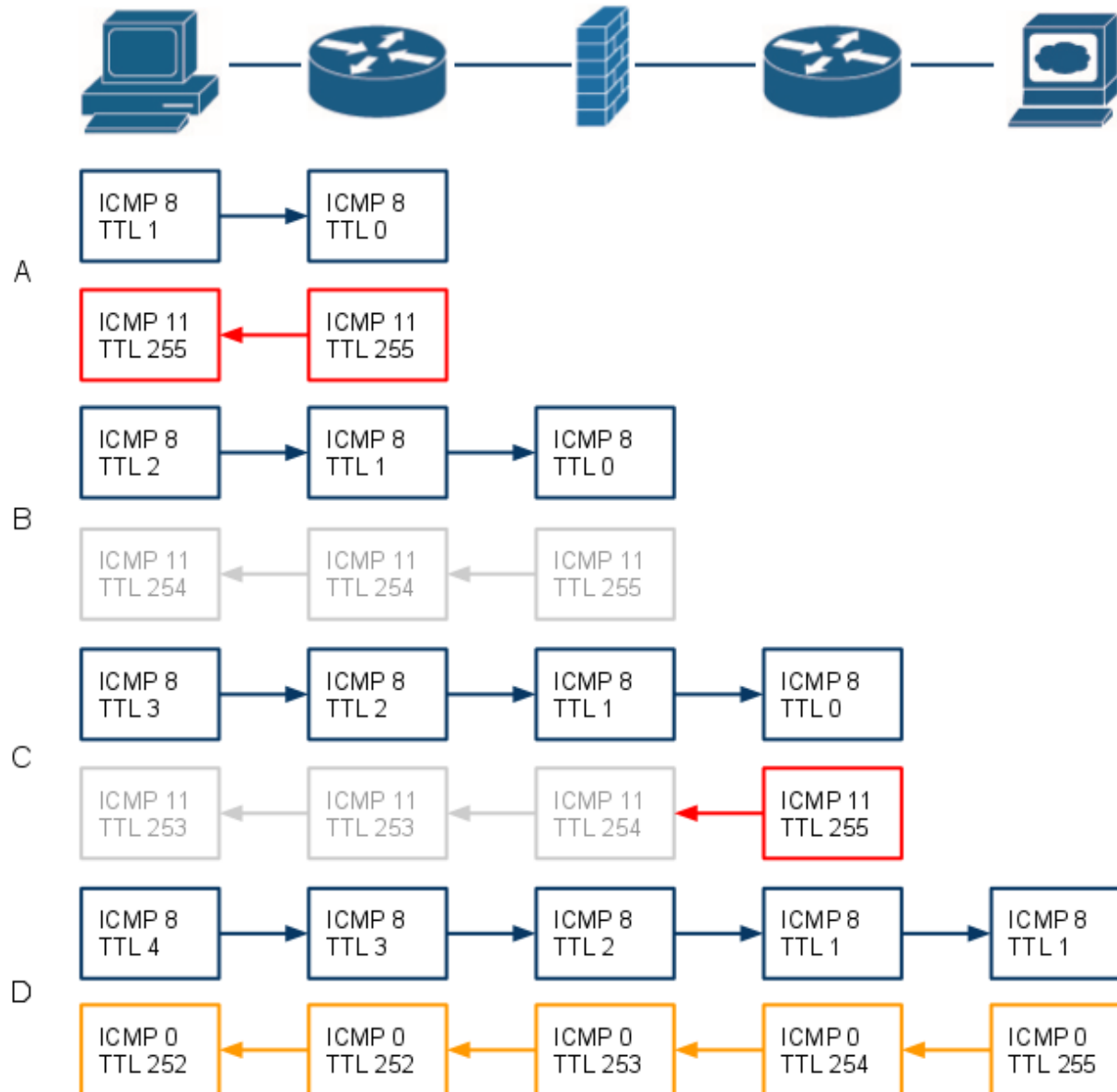
Tracing route to 10.0.4.4 over a maximum of 30 hops
  1  <1 ms    <1 ms    <1 ms    10.0.1.1
  2  29 ms    38 ms    29 ms    10.0.172.1
  3   9 ms     9 ms     9 ms    10.0.138.197
  4   9 ms     9 ms     9 ms    10.0.67.121
  5  11 ms    10 ms     9 ms    10.0.129.37
  6   *        *        *        Request timed out.
  7   *        *        *        Request timed out.
  8   *        *        *        Request timed out.
  9   *        *        *        Request timed out.
 10  *        *        *        Request timed out.
 11  16 ms    15 ms    16 ms    10.0.4.4

Trace complete.
C:\Users\sinchume>
```

# Locating the FW



# Locating the FW



# Detect Open Ports using Firewalking

- ❑ **Firewalking** – sử dụng các công cụ khác nhau như **tracert/traceroute**, **hping2/hping3**, **nmap scripts**, **firewalk...** để xây dựng lại FW ACL
- ❑ **Firewalk** có thể sử dụng để xác định các cổng dịch vụ đang mở và xác định ACL
- ❑ Nếu “TTL exceeded error” trả về nghĩa là cổng dịch vụ trên FW được mở

# Bypass through FW using Hping

- ❑ Hping là công cụ tạo và gửi đi các gói TCP/IP tùy chỉnh và phân tích các kết quả trả về

```
kali@kali:~$ sudo hping3 -1 -c 1 137.74.187.100
[sudo] password for kali:
HPING 137.74.187.100 (eth0 137.74.187.100): icmp mode set, 28 headers + 0 data bytes
len=46 ip=137.74.187.100 ttl=47 id=31 icmp_seq=0 rtt=184.0 ms

--- 137.74.187.100 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 184.0/184.0/184.0 ms
kali@kali:~$
```

**ICMP is enabled**

```
kali@kali:~$ sudo hping3 -S -c 1 -s 5151 -p 80 137.74.187.100
[sudo] password for kali:
HPING 137.74.187.100 (eth0 137.74.187.100): S set, 40 headers + 0 data bytes
len=46 ip=137.74.187.100 ttl=64 id=23875 sport=80 flags=SA seq=0 win=65535 rtt=184.3 ms

--- 137.74.187.100 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 184.3/184.3/184.3 ms
kali@kali:~$
```

**Port is opened**

```
kali@kali:~$ sudo hping3 -S -p 80 137.74.187.100 -a 137.74.187.100
HPING 137.74.187.100 (eth0 137.74.187.100): S set, 40 headers + 0 data bytes
^C

--- 137.74.187.100 hping statistic ---
8 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
kali@kali:~$
```

**Spoof IP address**

# Enumerate FW ACL using NMAP

- ❑ Phần lớn FW khi triển khai đều có các port mặc định được sử dụng cho mục đích truy cập từ xa, xác thực người dùng, kết nối VPN
- ❑ Sử dụng nmap có thể xác định được tình trạng các cổng trên tường lửa
- ❑ Nmap chỉ ra 06 trạng thái của port:
  - Open
  - Closed
  - Filtered
  - Unfiltered
  - Closed/Filtered
  - Open/Filtered

# Try to Bypass the FW

❑ Sử dụng nmap -f để gửi các gói phân mảnh nhằm vượt qua tường lửa sử dụng cơ chế “packet inspection, packet filtering”

- \$nmap -f [www.actvn.edu.vn](http://www.actvn.edu.vn)
- \$nmap -mtu 24 www.actvn.edu.vn

❑ Tại sao có thể bypass được các tường lửa này khi gói tin bị phân mảnh?

```
[x]-[r7909@parrot]-[~]cy
$ sudo nmap -f www.actvn.edu.vn
[sudo] password for r7909:
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-24 03:16 EDT
Nmap scan reports for www.actvn.edu.vn (103.21.148.154)
Host is up (0.0060s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
2000/tcp  open  cisco-sccp
3389/tcp  open  rdp
5060/tcp  open  sip
8008/tcp  open  http
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 4.69 seconds
```

```
[r7909@parrot]-[~] actvn.edu.vn (103.21.148.154)
$ sudo nmap -mtu 24 www.actvn.edu.vn
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-24 03:16 EDT
Nmap scan reports for www.actvn.edu.vn (103.21.148.154)
Host is up (0.033s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
2000/tcp  open  cisco-sccp
5060/tcp  open  sip
```

# Try to Bypass by Spoofing Packet

❑Chỉ thị cho nmap tạo ra các gói tin giả mạo nhằm tránh quá trình ghi log của tường lửa cũng như hệ thống. Ví dụ Decoy scan:

- `$nmap -D 216.58.203.164 192.168.0.101`
- `$nmap -D 10.10.10.10,121.10.10.125 192.168.0.101`

```
root@kali:~# nmap -D 216.58.203.164 192.168.0.101 ↩️

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-21 05:14 EST
Nmap scan report for 192.168.0.101
Host is up (0.00013s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
993/tcp   open  imaps
995/tcp   open  pop3s
MAC Address: 00:0C:29:6B:BA:A5 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.00s
```

```
root@ignite: ~
:ba:a5:00:0c:29:5b:8e:18:08:00 SRC=192.168.0.107 DST=192.168.0.101 LEN=
00 PREC=0x00 TTL=46 ID=60281 PROTO=TCP SPT=47835 DPT=4045 WINDOW=1024
YN URGP=0
Nov 21 02:14:03 mail kernel: [ 8163.589763] kaliNmapIN=eth0 OUT= MAC=
:ba:a5:00:0c:29:5b:8e:18:08:00 SRC=216.58.203.164 DST=192.168.0.101 LE
x00 PREC=0x00 TTL=37 ID=60281 PROTO=TCP SPT=47835 DPT=4045 WINDOW=1024
SYN URGP=0
Nov 21 02:14:03 mail kernel: [ 8163.589800] kaliNmapIN=eth0 OUT= MAC=
:ba:a5:00:0c:29:5b:8e:18:08:00 SRC=192.168.0.107 DST=192.168.0.101 LE
00 PREC=0x00 TTL=52 ID=29175 PROTO=TCP SPT=47835 DPT=9503 WINDOW=1024
YN URGP=0
Nov 21 02:14:03 mail kernel: [ 8163.589807] kaliNmapIN=eth0 OUT= MAC=
:ba:a5:00:0c:29:5b:8e:18:08:00 SRC=216.58.203.164 DST=192.168.0.101 LE
x00 PREC=0x00 TTL=50 ID=29175 PROTO=TCP SPT=47835 DPT=9503 WINDOW=1024
SYN URGP=0
Nov 21 02:14:03 mail kernel: [ 8163.589835] kaliNmapIN=eth0 OUT= MAC=
:ba:a5:00:0c:29:5b:8e:18:08:00 SRC=192.168.0.107 DST=192.168.0.101 LE
00 PREC=0x00 TTL=41 ID=62871 PROTO=TCP SPT=47835 DPT=2200 WINDOW=1024
YN URGP=0
Nov 21 02:14:03 mail kernel: [ 8163.589842] kaliNmapIN=eth0 OUT= MAC=
:ba:a5:00:0c:29:5b:8e:18:08:00 SRC=216.58.203.164 DST=192.168.0.101 LE
x00 PREC=0x00 TTL=55 ID=62871 PROTO=TCP SPT=47835 DPT=2200 WINDOW=1024
SYN URGP=0
```



# Try to Bypass by Spoofed Source

❑ Nếu firewall được cấu hình cho phép lưu lượng đến trên 1 port chỉ định, pentester có thể khai thác bằng cách giả mạo địa chỉ port nguồn

- `$nmap --source-port 53 [target]`
- `$nmap -g 53 [target]`

```
root@kali:~# nmap --source-port 53 10.10.10.10
Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-23 04:17 EST
Nmap scan report for 10.10.10.10
Host is up (0.00027s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:0C:29:36:30:D7 (VMware)
```

```
root@kali:~# nmap -g 53 10.10.10.10
Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-23 04:19 EST
Nmap scan report for 10.10.10.10
Host is up (0.00030s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:0C:29:36:30:D7 (VMware)
```

# MAC Address Spoofing

❑ Sử dụng **nmap --spoof-mac** để giả mạo địa chỉ MAC của nhà sản xuất

- Tạo MAC ngẫu nhiên **--spoof-mac 0**
- Chỉ định MAC **--spoof-mac 00:01:02:25:56:AE**
- Chỉ định MAC từ Vendor **--spoof-mac Dell/Apple...**

```
root@29471: ~  
File Edit View Search Terminal Help  
root@29471:~# nmap 139.162.17.246  
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-16 12:57 EST  
Nmap scan report for 139.162.17.246  
Host is up (0.00047s latency).  
All 1000 scanned ports on 139.162.17.246 are filtered  
  
Nmap done: 1 IP address (1 host up) scanned in 17.33 seconds  
root@29471:~#
```

**Before**

```
root@29471: ~  
File Edit View Search Terminal Help  
root@29471:~# nmap --spoof-mac Cisco 139.162.17.246  
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-16 13:00 EST  
Spoofing MAC address 00:00:0C:07:1D:8E (Cisco Systems)  
Nmap scan report for 139.162.17.246  
Host is up (0.014s latency).  
Not shown: 996 filtered ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
443/tcp   open  https  
6001/tcp   open  X11:1  
  
Nmap done: 1 IP address (1 host up) scanned in 34.65 seconds  
root@29471:~#
```

**After**

# IP Address Spoofing

- ❑ Khi tường lửa cho phép truy cập dựa trên địa chỉ IP, pentester có thể giả mạo IP để truy cập
- ❑ Sử dụng **nmap -S <spoofed IP> -e [interface]** để giả mạo địa chỉ IP
  - \$nmap -e eth0 -S 192.168.1.120 192.168.1.117
  - nmap sử dụng giao diện eth0 và giả mạo địa chỉ IP 192.168.1.120 khi dò quét 192.168.1.117

```
root@kali:~# nmap -e eth0 -S 192.168.1.120 192.168.1.117
WARNING: If -S is being used to fake your source address, you
should use -e <interface> and -Pn . If you are using it to specify your
source address, you can ignore this warning.
Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-22 17:06 IST
NSOCK ERROR [0.4210s] mksock_bind_addr(): Bind to 192.168.1.120
): Cannot assign requested address (99)
NSOCK ERROR [0.4210s] mksock_bind_addr(): Bind to 192.168.1.120
): Cannot assign requested address (99)
Nmap scan report for 192.168.1.117
Host is up (0.00045s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:0C:29:DA:1E:98 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 16.49 seconds
```

# Bypass FW by Varying Packet Size

- ❑ Nhiều tường lửa được cấu hình để phát hiện dò quét cổng dựa trên phân tích kích thước gói tin bởi vì phần lớn các trình quét cổng đều gửi các gói tin thăm dò có kích thước cụ thể
- ❑ Để tránh bị phát hiện các nỗ lực dò quét, sử dụng **\$nmap --data-length <len>** để gửi các gói tin với kích thước khác nhau

```
root@kali:~# nmap --data-length 12 -p 80 192.168.0.19
Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-05 16:56 EET
Nmap scan report for 192.168.0.19
Host is up (0.00035s latency).

PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 08:00:27:00:54:B4 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
root@kali:~#
```

# Bypass FW by Varying Packet Size

`$iptables -I INPUT -p tcp -m length --length 1:100 -j REJECT -  
-reject-with tcp-reset`

```
root@kali:~# nmap --data-length 32 -p 80 192.168.0.19
Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-05 18:32 EET
Nmap scan report for 192.168.0.19
Host is up (0.00027s latency).
```

```
PORT      STATE SERVICE
80/tcp    closed http
MAC Address: 08:00:27:00:54:B4 (Oracle VirtualBox virtual NIC)
```

**Not working**

```
Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

```
root@kali:~# nmap --data-length 12 -p 80 192.168.0.19
```

```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-05 18:32 EET
Nmap scan report for 192.168.0.19
Host is up (0.00027s latency)
```

```
PORT      STATE SERVICE
80/tcp    closed http
MAC Address: 08:00:27:00:54:B4 (Oracle VirtualBox virtual NIC)
```

```
root@kali:~# nmap --data-length 113 -p 80 192.168.0.19
```

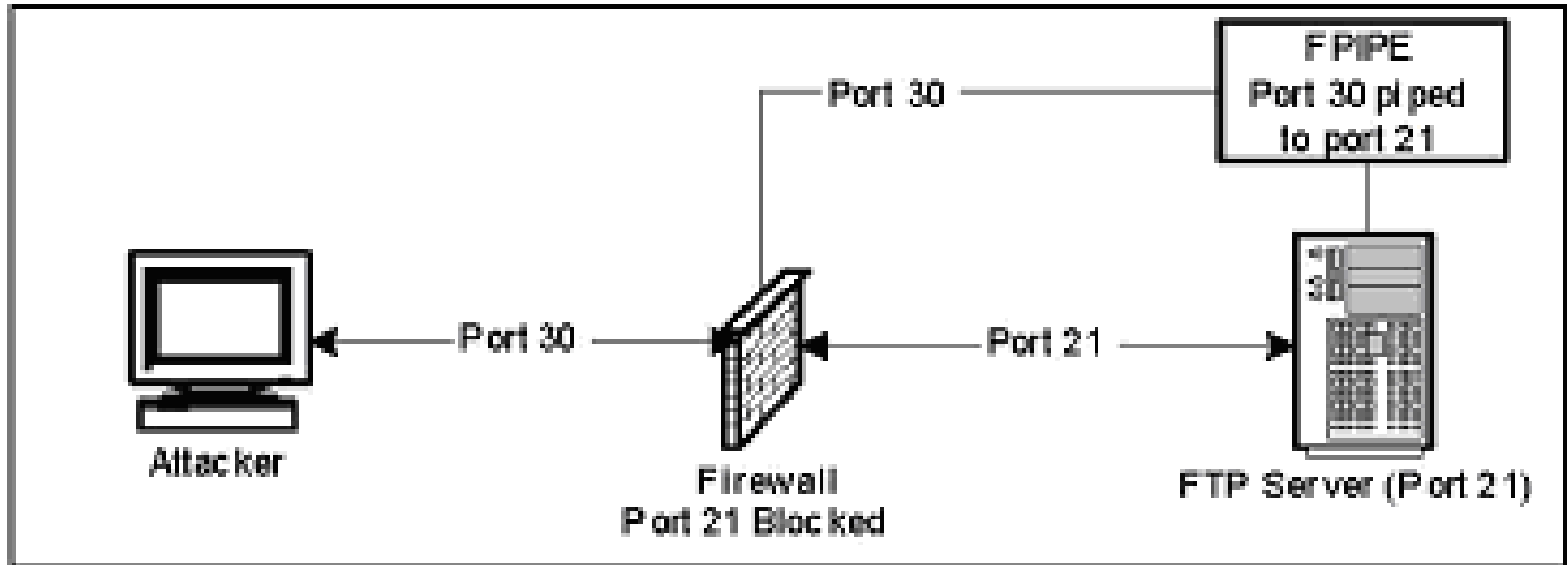
```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-05 18:32 EET
Nmap scan report for 192.168.0.19
Host is up (0.00027s latency).
```

**Working!!!**

```
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 08:00:27:00:54:B4 (Oracle VirtualBox virtual NIC)
```

# Bypassing FW techniques

- Nếu không thể truy cập trực tiếp tới các port thì có thể thử sử dụng **port redirection**



# Bypassing FW techniques

- ❑ Để bypass firewall, thử truy cập bằng địa chỉ IP thay vì sử dụng địa chỉ tên miền.



- ❑ Sử dụng proxy online/offline

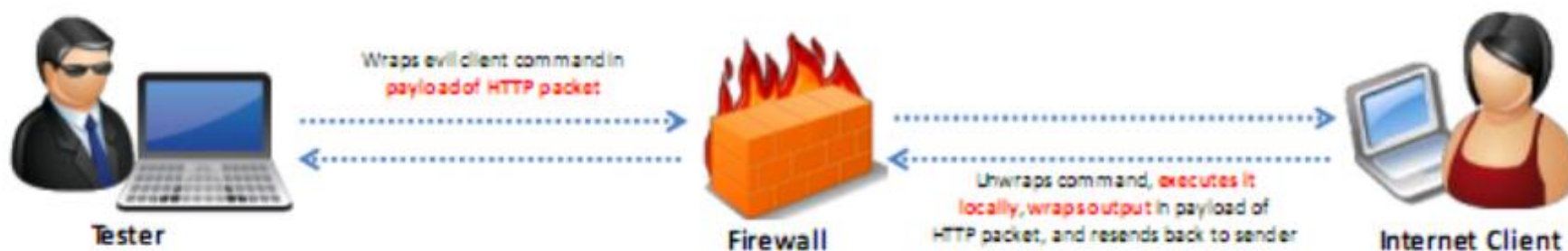
- <https://translate.google.com/?hl=vi>
- <https://www.proxysite.com/>
- <https://hide.me/en/proxy>
- <https://www.croxyproxy.com/>
- ...



# Bypassing FW techniques

## ❑ Sử dụng HTTP Tunneling

- Phương pháp này chỉ có thể thực hiện nếu cơ quan/ tổ chức có **public web server** với port 80 được sử dụng cho HTTP
- Nhiều tường lửa không kiểm tra nội dung gói tin HTTP do đó có thể sử dụng HTTP để truyền dữ liệu qua các tunnel
- Công cụ: Super Network Tunnel, HTTP Tunnel, HTTPORT





# Bypassing FW techniques

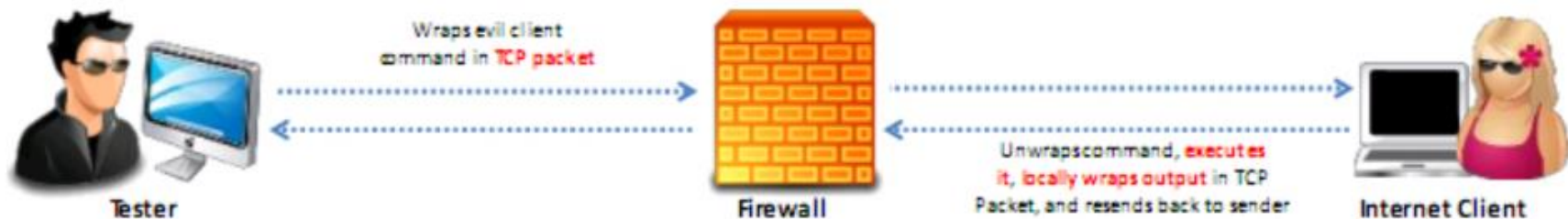
## ❑ Sử dụng ICMP Tunneling

- Nhiều quản trị viên cho phép ICMP và các tường lửa thường không kiểm tra phần dữ liệu trong gói tin ICMP



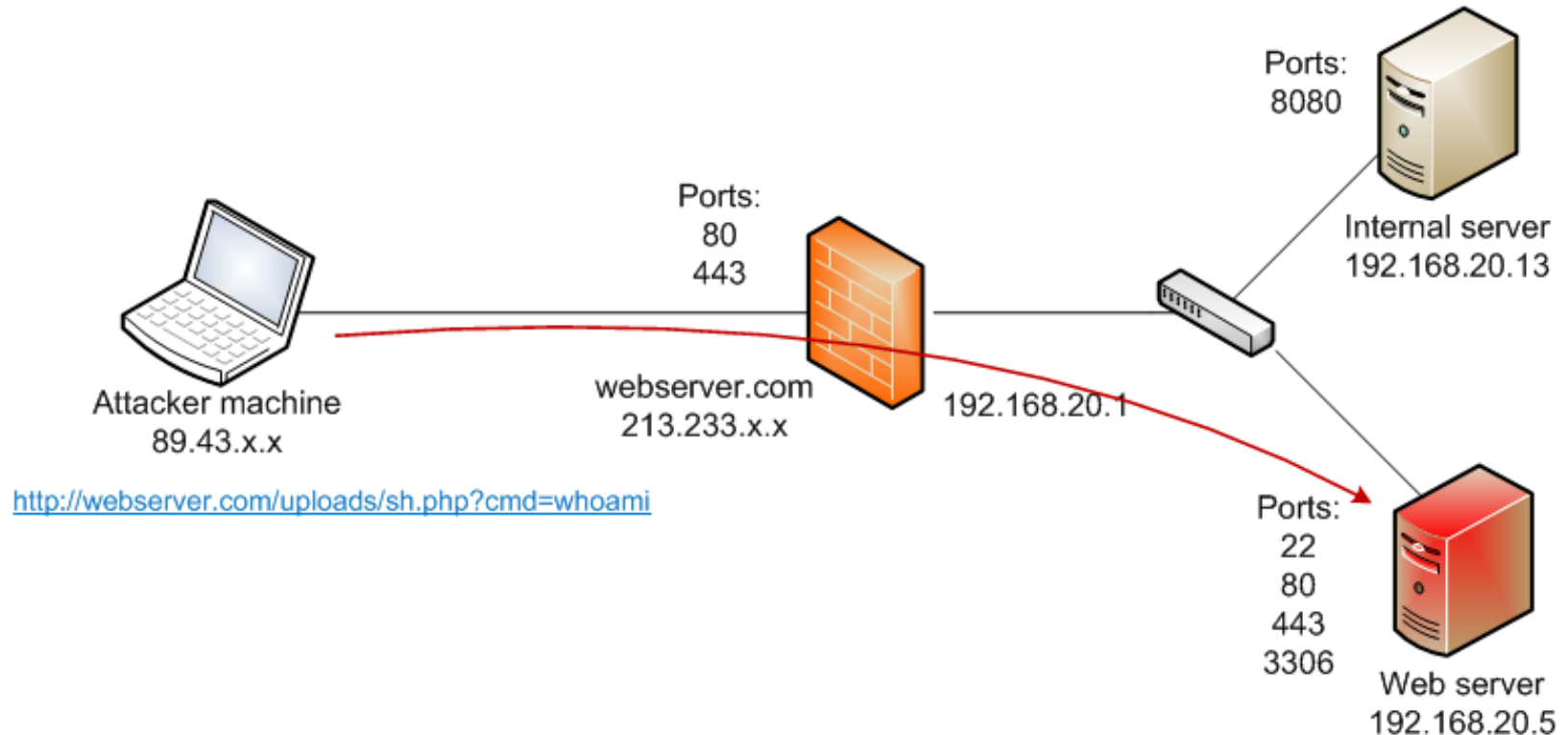
## Sử dụng ACK Tunneling

- Nhiều tường lửa không kiểm tra gói tin với bit ACK được set bởi vì bit ACK thường sử dụng cho các kết nối hợp lệ



# Bypassing FW techniques

## □ Sử dụng SSH tunneling



1

Kiểm thử xâm nhập  
tường lửa

2

Kiểm thử xâm nhập  
IDS

# Why IDS Pentesting

- ❑ Kiểm tra IDS có thực thi đúng chính sách an toàn tổ chức hay không
- ❑ Kiểm tra hiệu quả của IDS và tính đúng đắn trong việc thực thi các luật
- ❑ Kiểm tra các thông tin có thể truy cập từ attacker
- ❑ Kiểm tra sự tồn tại của các lỗ hổng bảo mật trên IDS

# Common IDS Evasion Techniques

---

- ❑ DoS
- ❑ Insertion
- ❑ Evasion
- ❑ Pattern-matching weakness
- ❑ Encryption & Tunneling
- ❑ Fragmentation

# Test for Resource Exhaustion

- ❑ Mỗi IDS có bộ nhớ, CPU, bandwidth hạn chế và dễ bị tấn công gây cạn kiệt tài nguyên
- ❑ Pentester có thể tạo và gửi một lượng lớn các gói tin đến IDS để kiểm tra khả năng xử lý của IDS
  - CPU DoS: Fragment/Segment reassembly/Encryption/Decryption
  - Memory DoS: TCP handshake, Fragment/Segment reassembly
  - Network Bandwidth DoS
  - Reactive System DoS: tạo ra nhiều cảnh báo giả, ngăn các kết nối hợp lệ bằng cách giả mạo địa chỉ

# ARP Flood

## ☐ ARP Flood

- Gây “flood” mạng bằng tấn công ARP

## ☐ MAC Spoofing

- ☐ Kiểm tra IDS bằng cách giả mạo địa chỉ MAC

## ☐ IP Spoofing

- ☐ Thử “flood” IDS bằng cách giả mạo địa chỉ IP

## ☐ SYN Floods

- ☐ Thử tấn công vào việc thực thi kết nối TCP

## ☐ Replay attack

- ☐ Thử bắt các lưu lượng và phát lại trên mạng máy tính

# DoS Attack

- ❑ Nhiều IDS sử dụng các server lưu trữ log tập trung
- ❑ Pentest cần thử tấn công lên các server lưu trữ log tập trung để làm chậm hoặc crash hệ thống này
- ❑ Công cụ: HOIC, DDOSIM, DoS HTTP...



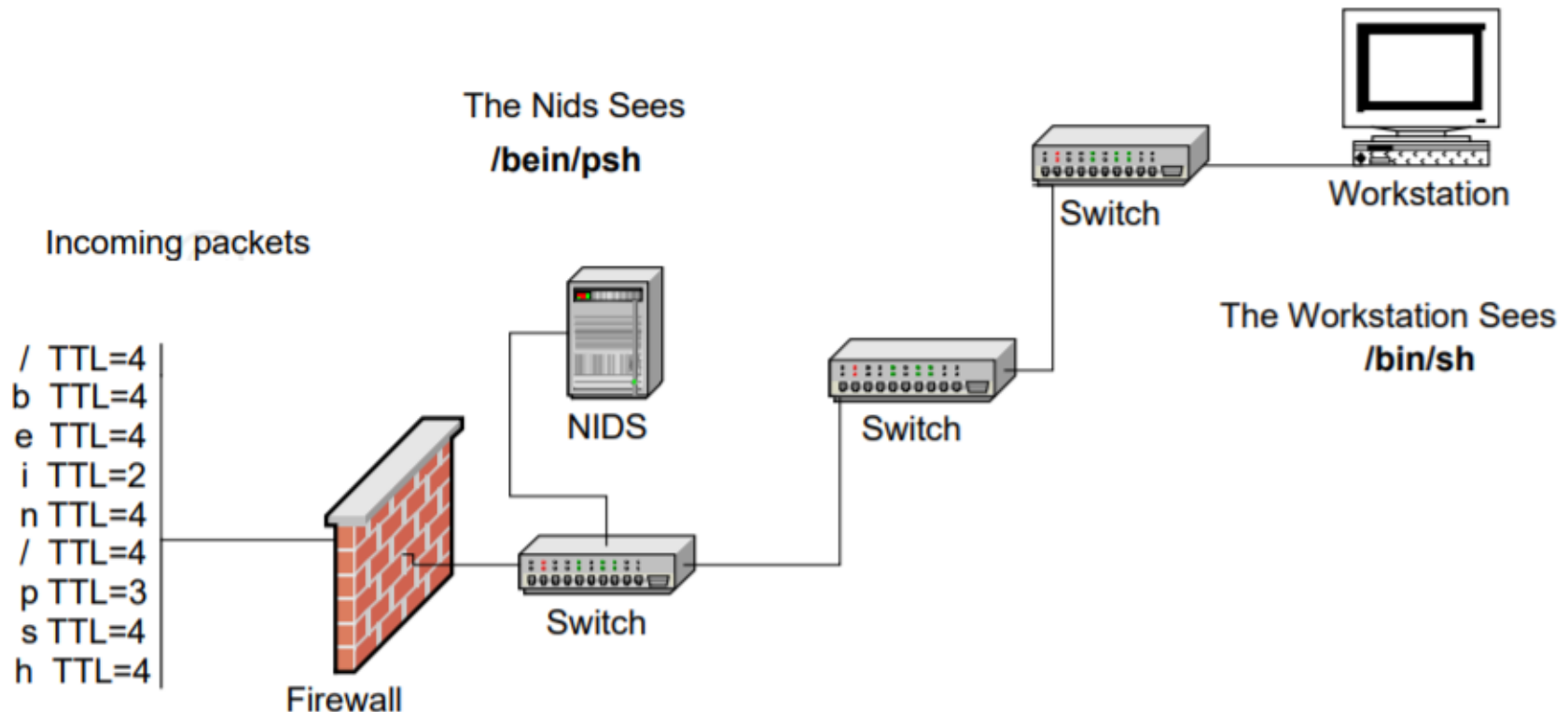
# Bypass IDS using Anonymous Website

❑ Sử dụng proxy, anonymous website online/offline

- <https://translate.google.com/?hl=vi>
- <https://www.proxysite.com/>
- <https://hide.me/en/proxy>
- <https://www.croxyproxy.com/>

# TTL Evasion

- ❑ Khi các thiết bị mạng nhận gói tin có TTL=1 nó sẽ không chuyển tiếp gói tin mà gửi lại thông báo "**TTL Expired in Transit**" tới địa chỉ nguồn và drop gói tin
- ❑ Ví dụ: Những gói tin có TTL<4 sẽ bị drop trước khi đến được đích



# TTL Evasion

□ Ví dụ:

- Packet 1: **GET /cgi-bin/p** TTL=15
- Packet 2: **some\_file.cgi?=** TTL=10
- Packet 3: **hf?** TTL=15

□ Giả sử End host cần  $TTL > 15$  để gói tin đến được đích (target host), đối với IDS thì TTL trong khoảng 10-14

- IDS nhận được: "**GET /cgi-bin/psome\_file.cgi?=hf?**"
- Target host nhận được: "**GET /cgi-bin/phf?**"

# TTL Evasion

❑ Attacker's data stream

2	3	3	5	4	1	6
T	T	X	C	A	A	K

❑ NIDS data steam: Chấp nhận gói tin thứ **3** ghi đề **3**

=> **ATXACK**

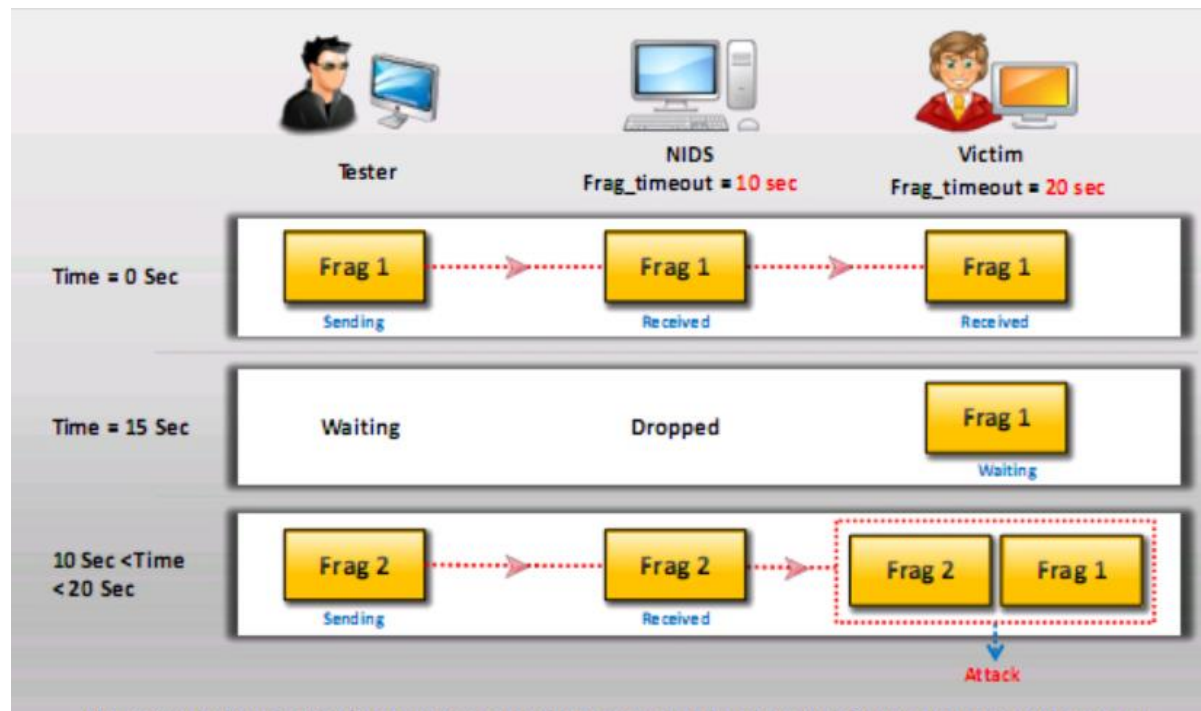
1	2	3	3	4	5	6
A	T	T	X	A	C	K

❑ End system data steam: Loại bỏ gói tin số **3** vì một vài nguyên nhân (vd: TTL) => **ATTACK**

1	2	3	<del>3</del>	4	5	6
A	T	T	<del>X</del>	A	C	K

# Session Splicing

- ❑ Trong trường hợp kích thước gói tin lớn hơn MTU thì nó sẽ bị phân mảnh và sau đó sẽ được lắp ráp lại ở phía bên nhận
  - Nhiều IDS sẽ dùng “reassembly” nếu nó không nhận được gói tin sau 1 khoảng thời gian nhất định.
  - Trên windows thời gian chờ mặc định là 60s
- ❑ Nếu  $\text{Frag\_timeout của IDS} < \text{Frag\_timeout của target host}$  thì có thể bị lợi dụng để khai thác



# Fragmentation

- ❑ Tương tự như Session Splicing, các gói tin được chia nhỏ để gửi tới IDS
- ❑ Pentester thử gửi các gói tin bị phân mảnh với các kích thước khác nhau với thứ tự bị xáo trộn tới hệ thống đối tượng
- ❑ Ví dụ:

- ❑ Packet 1: **GET /cgi-bin/**

- ❑ Packet 2: **aaaaaaaaaaaaaaaa/../../phxx**

- ❑ Packet 3: **f?**

**xx** bị ghi đè

=> **GET /cgi-bin/aaaaaaaaaaaaaaaa/../../phf?**

**xx** không bị ghi đè

=> **GET /cgi-bin/aaaaaaaaaaaaaaaa/../../phxx**

# Overlapping Fragments

❑ Attacker's data stream

2	3	3	5	4	1	6
T	T	X	C	A	A	K

❑ NIDS data steam: Loại bỏ gói tin số 3 => **ATXACK**

1	2	3	3	4	5	6
A	T	X	T	A	C	K

❑ End system data steam: Loại bỏ gói tin số 3 => **ATTACK**

1	2	<del>3</del>	3	4	5	6
A	T	<del>X</del>	T	A	C	K

# Session Splicing

- ❑ Pentester thử gửi các gói tin bị phân mảnh với các kích thước khác nhau với thứ tự bị xáo trộn tới hệ thống đối tượng
- ❑ Ví dụ: Thử gửi gói tin bị phân mảnh trong đó gói 1 có payload 80 byte nhưng gói 2 có payload bắt đầu từ byte thứ 76 tính từ gói tin thứ 1 => xem IDS và hệ thống sẽ lắp ráp và xử lý gói tin như thế nào



# Encryption & Tunneling

❑ Pentester thử sử dụng các kỹ thuật mã hóa, tạo đường hầm để bypass IDS

- SSH
- SSL
- IPSec
- RDP
- ...

# Application Hijack

- ❑ Nhiều dạng dữ liệu như audio, video, images có thể được nén thành kích thước nhỏ hơn để tối đa hóa tốc độ truyền dữ liệu
- ❑ IDS không thể kiểm tra các "signature" của các định dạng nén này
- ❑ Pentester thử nhúng các đoạn mã khai thác vào các tập tin media được nén và gửi tới hệ thống => kiểm tra việc IDS xác định và xử lý các đoạn mã khai thác này

# Ping of Death

## ❑ Ping of Death

- Pentester thử gửi gói tin ICMP không đúng định dạng, ví dụ như gửi gói tin ICMP có kích thước lớn hơn 65535 byte

## ❑ Unicode Evasion

- Thử sử dụng unicode characters để vượt qua các cơ chế đối sánh mẫu của IDS
- Thử Polymorphic/Obfuscated/Encoding Payload/URL để kiểm tra khả năng phát hiện của IDS
- Ví dụ: "cgi-bin" -> "%63%67%69%2d%62%69%6e"

## ❑ False-Positive Generation

- Tùy vào loại IDS được sử dụng, pentester cố gắng tạo ra các gói tin mà từ đó IDS có thể đưa ra 1 lượng lớn "**cảnh báo giả**"

# IDS Evasion Tools

---

- ☐ Evader
- ☐ Nmap
- ☐ Libemu
- ☐ Fragroute
- ☐ Fragrouter
- ☐ InTrace
- ☐ SniffJoke
- ☐ HxD
- ☐ Wireshark
- ☐ ...

# Thank you & Any questions?

