HỌC VIỆN KTQS
KHOA CÔNG NGHỆ THÔNG TIN

# Bài 13. Tấn công mạng máy tính

Học phần: ĐẢM BẢO VÀ AN TOÀN THÔNG TIN

# NỘI DUNG

1. Tổng quan an ninh mạng máy tính
2. Mô hình tấn công mạng máy tính
3. Một số kỹ thuật tấn công mạng máy tính

# 1. TỔNG QUAN AN NINH MẠNG MÁY TÍNH

- Ở Việt Nam "mọi thứ đều miễn phí"?





# Và "Trái đắng" chúng ta nhận được

Việt Nam thuộc

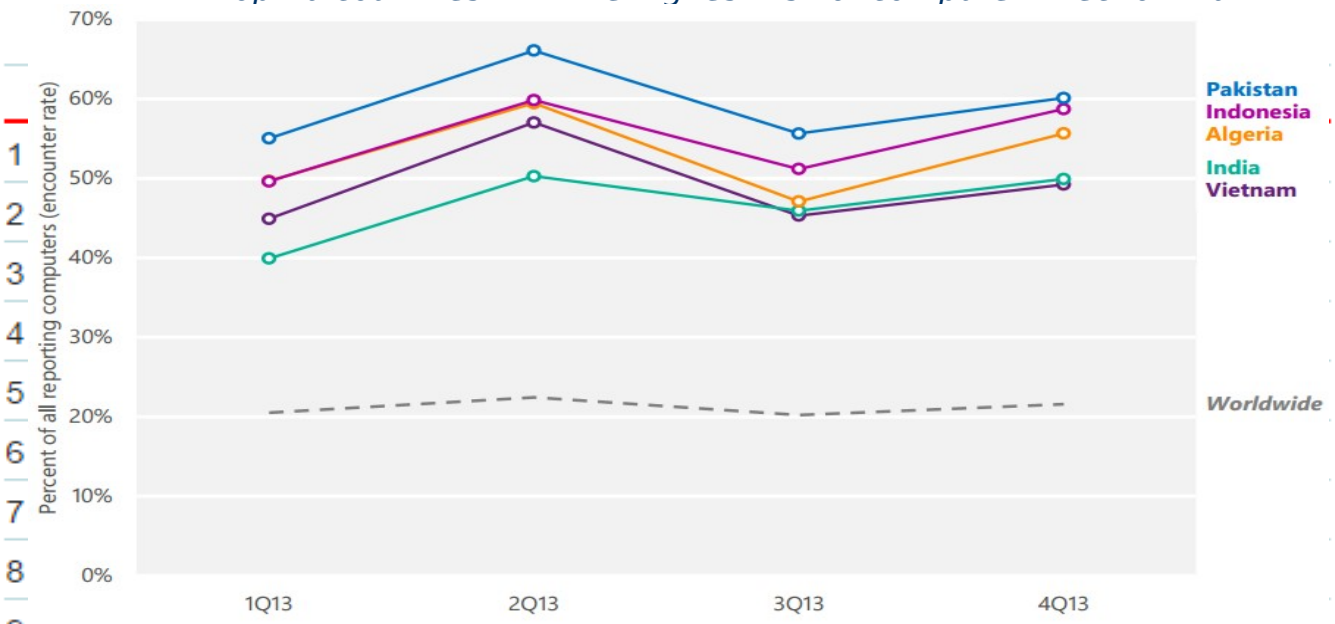
**TOP**

**5**

quốc gia có tỉ lệ nhiễm mã độc cao nhất thế giới

*Microsoft security intelligence report*

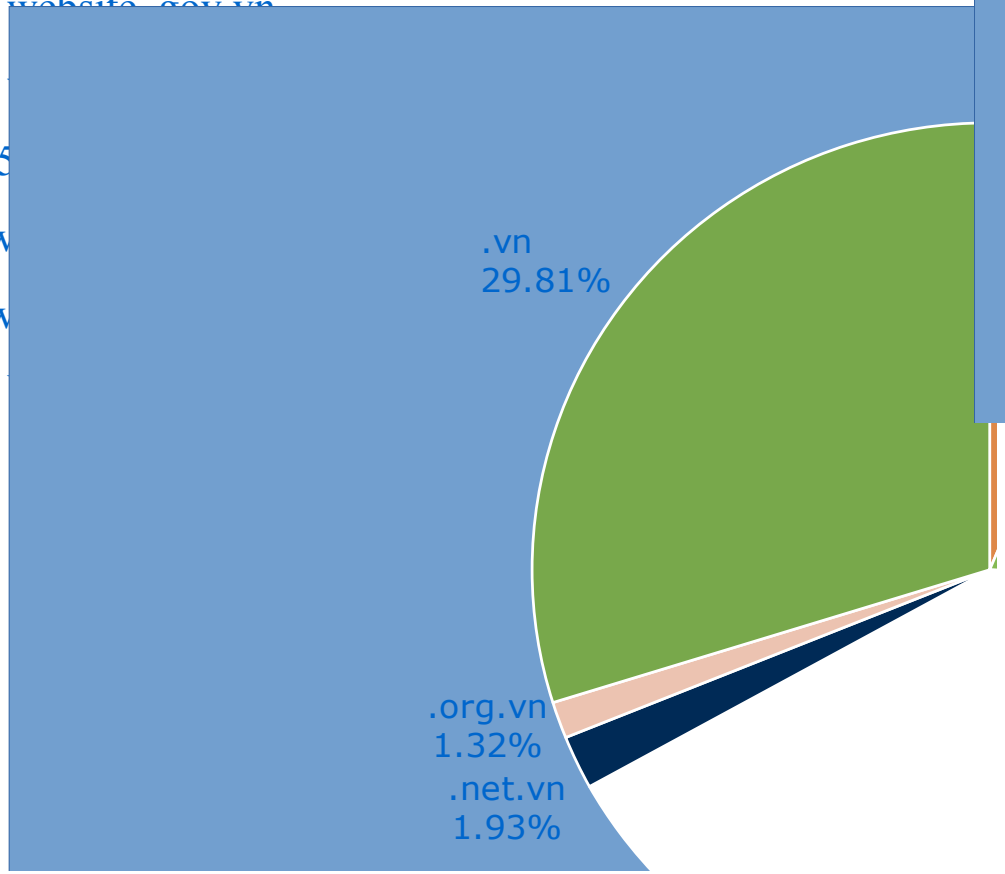
*Top 10 countries with the highest risk of computer infection via*

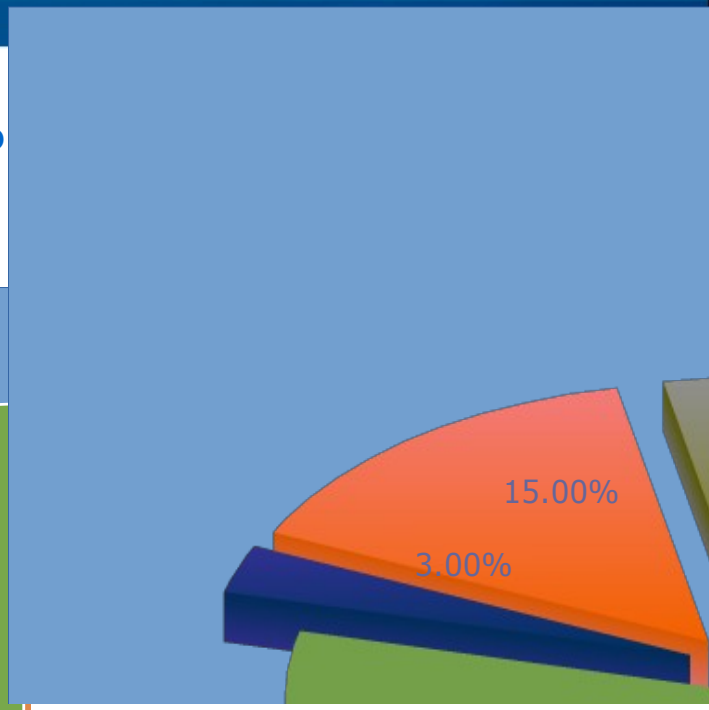


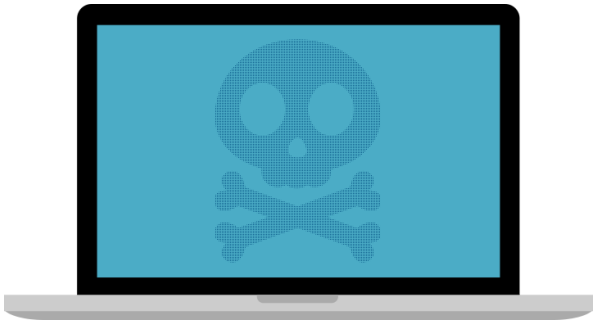

| | | |
|---|---|---|
| 9 | Ukraine | 46.66% |
| 10 | Kyrgyzstan | 44.04% |

**Trong 9 tháng đầu năm 2016 thống kê từ Zone-h ước lượng cho**

- Hơn 3000 website *.vn của Việt Nam bị tấn công trong đó có
  - 195 website .gov.vn
  - 607
  - 1275
  - 60 w
  - 41 w
  - 925



Con số trên liệu có dừng ở đó


NOTIFIER DOMAIN .VN

Special defacements only ☐ Fulltext/Wildcard ☑ Onhold (Unpublished) only ☐

Date : ALL Apply filter

Total notifications: **34,376** of which **10,313** single ip and **24,063** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

| Date | Notifier | H | M | R | L | ★ Domain | OS | View |
|---|---|---|---|---|---|---|---|---|
| 2016/10/05 | KkK1337 | | | | | mocongty.vn/ck.htm | Linux | mirror |
| 2016/10/05 | Dr.SiLnT HilL | | M | | | www.coollife.com.vn/eg.htm | Linux | mirror |
| 2016/10/05 | Dr.SiLnT HilL | | | | | www.canhotphcm.vn/eg.htm | Linux | mirror |
| 2016/10/05 | ./Synchronizer | | M | | | foodvietnam.vn/wk.html | Linux | mirror |
| 2016/10/04 | KkK1337 | | M | | | vinhhao.vn/security/lang.tmp | Win 2003 | mirror |
| 2016/10/04 | KkK1337 | | M | | | daotaoinet.edu.vn/security/lan... | Win 2003 | mirror |
| 2016/10/04 | KkK1337 | | | | | thachbich.vn/security/lang.tmp | Win 2003 | mirror |
| 2016/10/03 | Dx_Cyber | | | | | tie.rat.vn/assets/public/mimpi... | Linux | mirror |
| 2016/10/03 | ifactoryx | | M | | | support.gss.com.vn/i.html | Win 2008 | mirror |
| 2016/10/03 | ifactoryx | | M | R | | tratechcom.vn/i.html | Win 2008 | mirror |
| 2016/10/03 | ifactoryx | | M | R | | vanphongpham.net.vn/i.html | Win 2008 | mirror |
| 2016/10/03 | ifactoryx | | M | R | | sangha.vn/i.html | Win 2008 | mirror |
| 2016/10/03 | ifactoryx | | M | | | okyou.vn/i.html | Win 2008 | mirror |
| 2016/10/03 | ifactoryx | | M | R | | htaco.vn/i.html | Win 2008 | mirror |
| 2016/10/03 | ifactoryx | | M | | | dongphucthienchuagiao.vn/i.html | Win 2008 | mirror |
| 2016/10/03 | ifactoryx | | | | | boge.vn/i.html | Win 2008 | mirror |
| 2016/10/01 | Scorpiol | H | | | | mindschool.vn | Linux | mirror |

http://www.zone-h.org


NOTIFIER DOMAIN .GOV.VN

Special defacements only Fulltext/Wildcard Onhold (Unpublished) only

Date : ALL Apply filter

Total notifications: **1,968** of which **952** single ip and **1,016** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

| Date | Notifier | H | M | R | L | ★ | Domain | OS | View |
|---|---|---|---|---|---|---|---|---|---|
| 2016/09/27 | RxR | H | | | | | sotuphapsoctrang.gov.vn | Linux | mirror |
| 2016/09/18 | D4RK 4NG31 | | | R | | | stnmt.gialai.gov.vn/robots.txt | Win 2008 | mirror |
| 2016/09/14 | cyber-71 | | M | R | | | www.iwem.gov.vn/images/prod/14... | Linux | mirror |
| 2016/09/14 | MuhmadEmad | | | R | | | soxaydung.bacgiang.gov.vn/imag... | Linux | mirror |
| 2016/09/13 | ProtoWave Reloaded | | | | | | www.omard.gov.vn/cool.htm | Win 2003 | mirror |
| 2016/09/13 | ProtoWave Reloaded | | M | | | | omard.mard.gov.vn/cool.htm | Win 2003 | mirror |
| 2016/09/13 | ProtoWave Reloaded | | M | | | | truyenthong.omard.gov.vn/cool.htm | Win 2003 | mirror |
| 2016/09/13 | ProtoWave Reloaded | | M | | | | law.omard.gov.vn/cool.htm | Win 2003 | mirror |
| 2016/09/12 | ProtoWave Reloaded | | | | | | ipc.tuyenquang.gov.vn/Image/fi... | Win 2008 | mirror |
| 2016/09/12 | ProtoWave Reloaded | | M | | | | thanhpho.tuyenquang.gov.vn/Ima... | Win 2008 | mirror |
| 2016/09/12 | ProtoWave Reloaded | | M | | | | santmdttuyenquang.gov.vn/Image... | Win 2008 | mirror |
| 2016/09/12 | ProtoWave Reloaded | | M | | | | sotttt.tuyenquang.gov.vn/Image... | Win 2008 | mirror |
| 2016/09/12 | ProtoWave Reloaded | | M | | | | sokehoach.tuyenquang.gov.vn/Im... | Win 2008 | mirror |
| 2016/09/12 | ProtoWave Reloaded | | M | | | | suoikhoangmylam.tuyenquang.gov... | Win 2008 | mirror |
| 2016/09/12 | ProtoWave Reloaded | | M | | | | sxdtuyenquang.gov.vn/Image/fil... | Win 2008 | mirror |
| 2016/09/12 | ProtoWave Reloaded | | | | | | stttttuyenquang.gov.vn/Image/f... | Win 2008 | mirror |
| 2016/09/12 | ProtoWave Reloaded | | | R | | | tuyenquang.gov.vn/Image/file/c... | Win 2008 | mirror |

http://www.zone-h.org


Hơn 700 website Việt Nam bị tin tặc tấn công dịp nghỉ lễ 02/09

Hơn 200 website Việt Nam bị tin tặc TQ tấn công xoay quanh vụ dàn khoan HD981 vi phạm lãnh thổ Việt Nam

# 7/2016: Cảng Tân Sơn Nhất và Nội Bài bị tấn công

- Những lỗ hổng cho phép tin tặc tấn công nhiều tổ chức trong nước thời gian qua phần lớn nằm trong OWASP Top 10

- Injection

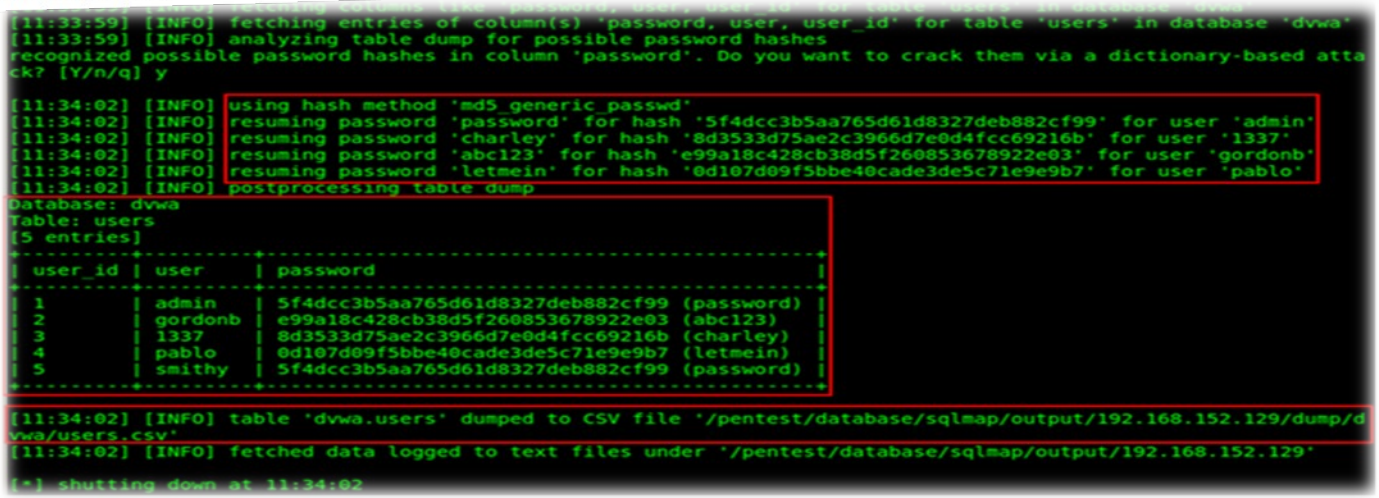
**1** CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

**Summary**

| | | | |
|---|---|---|---|
| Weakness Prevalence | High | Consequences | Data loss, Security bypass |
| Remediation Cost | Low | Ease of Detection | Easy |
| Attack Frequency | Often | Attacker Awareness | High |

**Discussion**

These days, it seems as if software is all about the data: getting it into the database, pulling it from the database, massaging it into information, and sending it elsewhere for fun and profit. If attackers can influence the SQL that you use to communicate with your database, then suddenly all your fun and profit belongs to them. If you use SQL queries in security controls such as authentication, attackers could alter the logic of those queries to bypass security. They could modify the queries to steal, corrupt, or otherwise change your underlying data. They'll even steal data one byte at a time if they have to, and they have the patience and know-how to do so. In 2011, SQL injection was responsible for the compromises of many high-profile organizations, including Sony Pictures, PBS, MySQL.com, security company HBGary Federal, and many others.

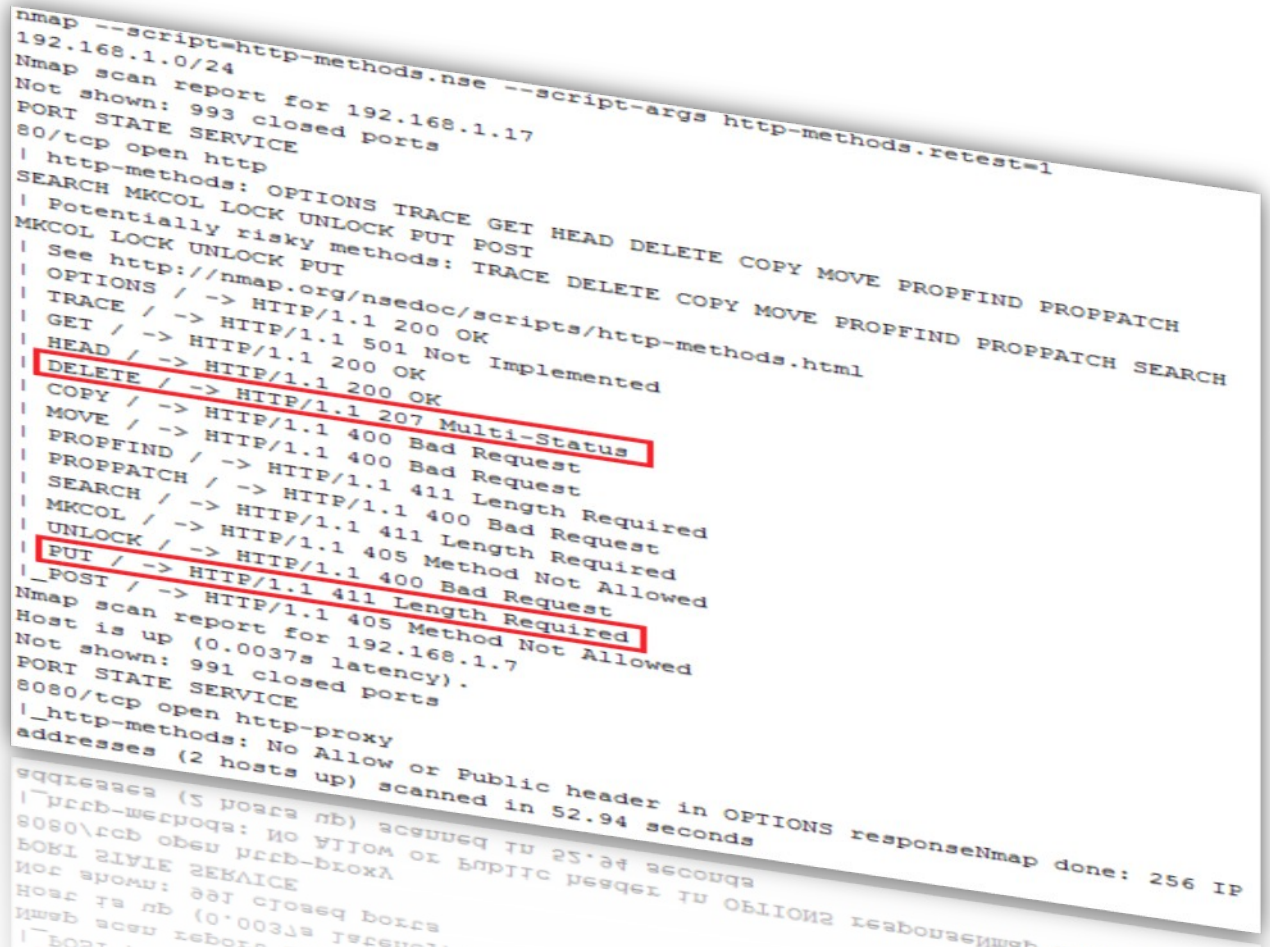


# Business Logic

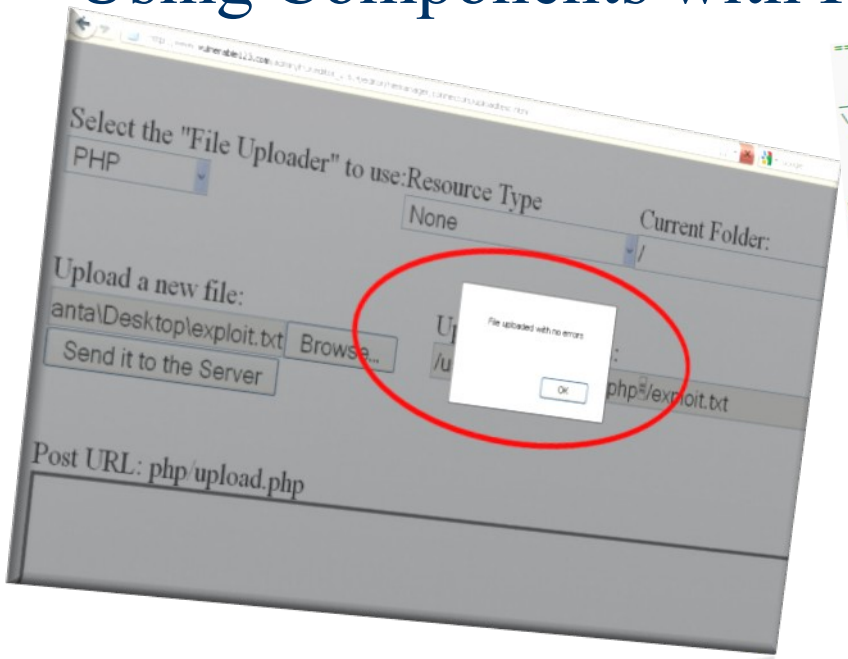
```php
<?php
        # checks if file is Gif or not
        if($_FILES['userfile']['type'] != "image/gif") {
             echo "Sorry, we only allow uploading GIF images";
             exit;
        }

        $uploaddir = 'uploads/';
        $uploadfile = $uploaddir . basename($_FILES['userfile']['name']);
        if (move_uploaded_file($_FILES['userfile']['tmp_name'], $uploadfile)) {
             echo "File is valid, and was successfully uploaded.\n";
        }
        else {
             echo "File uploading failed.\n";
        }
?>
```

- Security Misconfiguration



# Using Components with Known Vulnerabilities



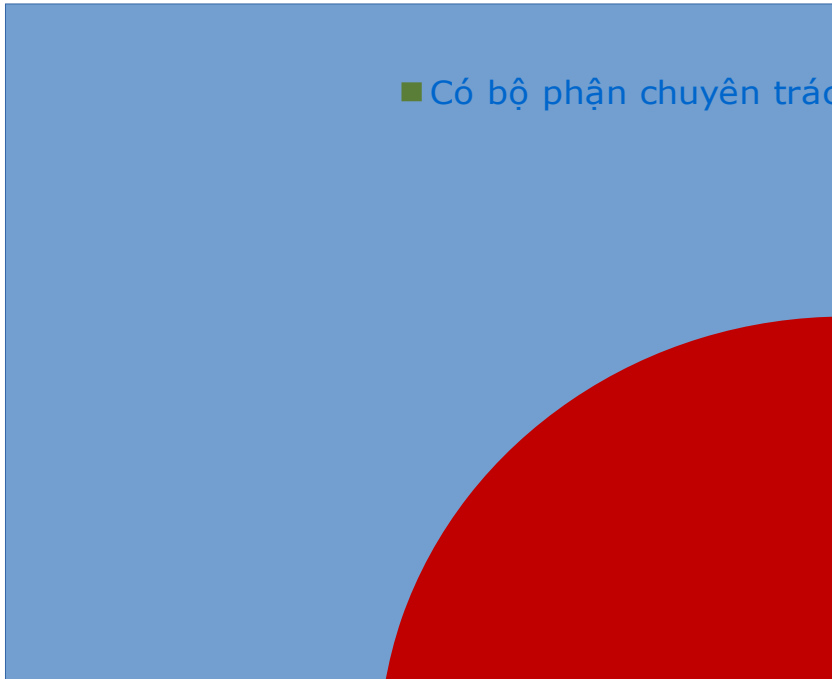

## Điều đặc biệt

- Tất cả những lỗ hổng trên không phải là Zero-day, nhưng lại là nguyên nhân chính của nhiều hệ thống trong nước bị khai thác được phát hiện gần đây.
- Trong đợt tấn công của tin tặc TQ nhằm vào Việt Nam, gần như hầu hết website bị khai thác thông qua các lỗi trên
- Ngay cả những tổ chức được trang bị đầy đủ các thiết bị, giải pháp bảo mật nhưng hệ thống của họ vẫn bị tấn công.

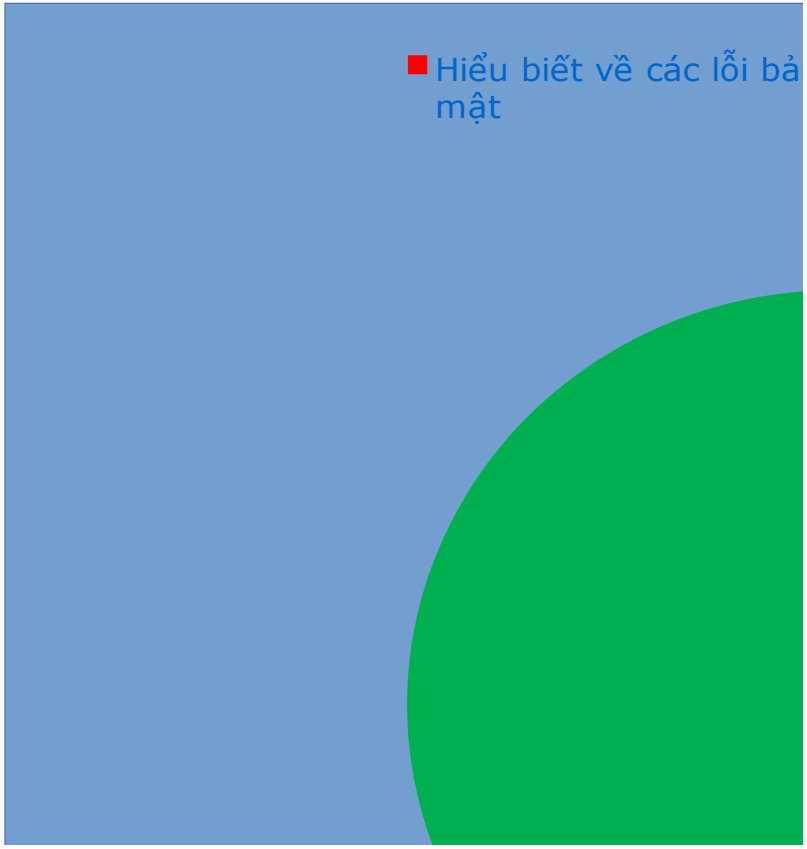
## ➢ Nguyên nhân của vấn đề

Dữ liệu khảo sát của các tổ chức ATTT về tình hình bảo mật và rà soát, đánh giá an ninh thông tin trên 170 tổ chức trong nước cho thấy.

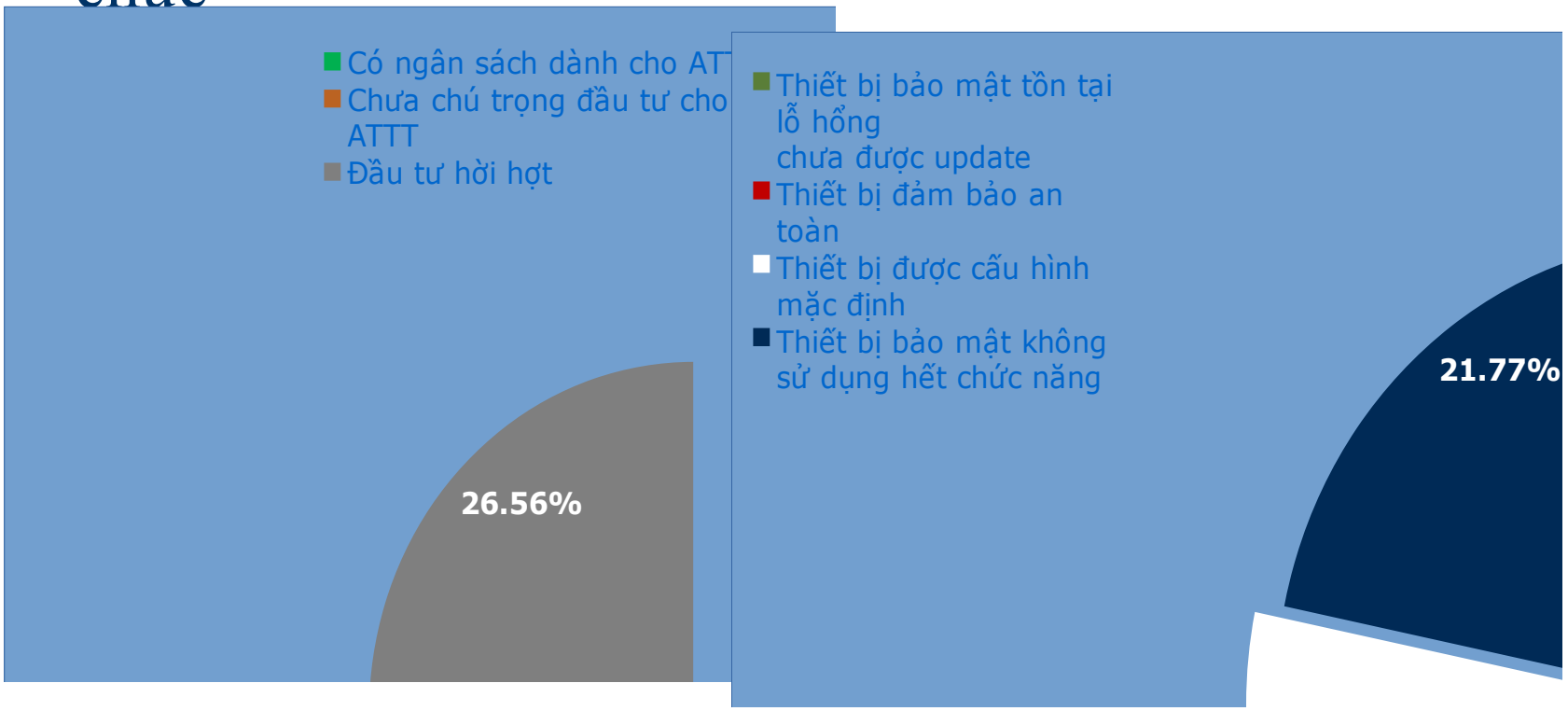
- Thiếu đội ngũ chuyên trách về ATTT trong các tổ chức




- Hiểu biết về bảo mật của đội ngũ phát triển ứng dụng, vận hành hệ thống

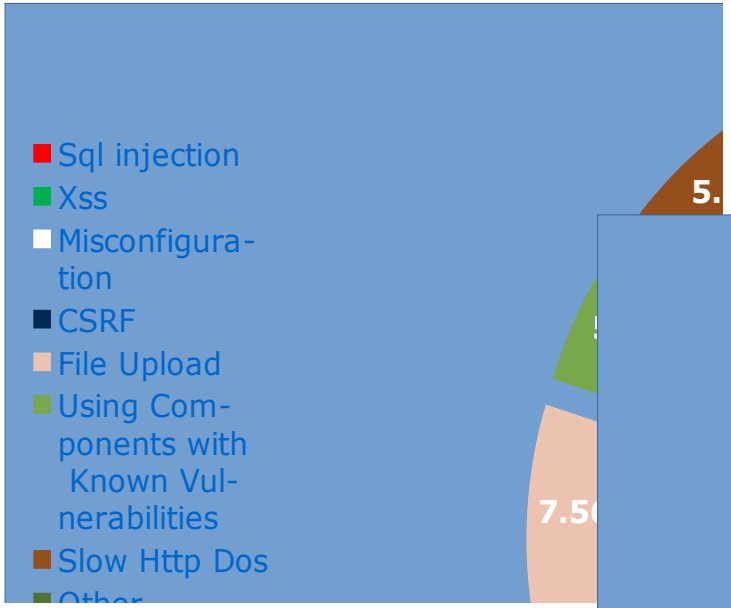


# Tỉ lệ đầu tư cho an ninh an toàn thông tin ở các tổ chức

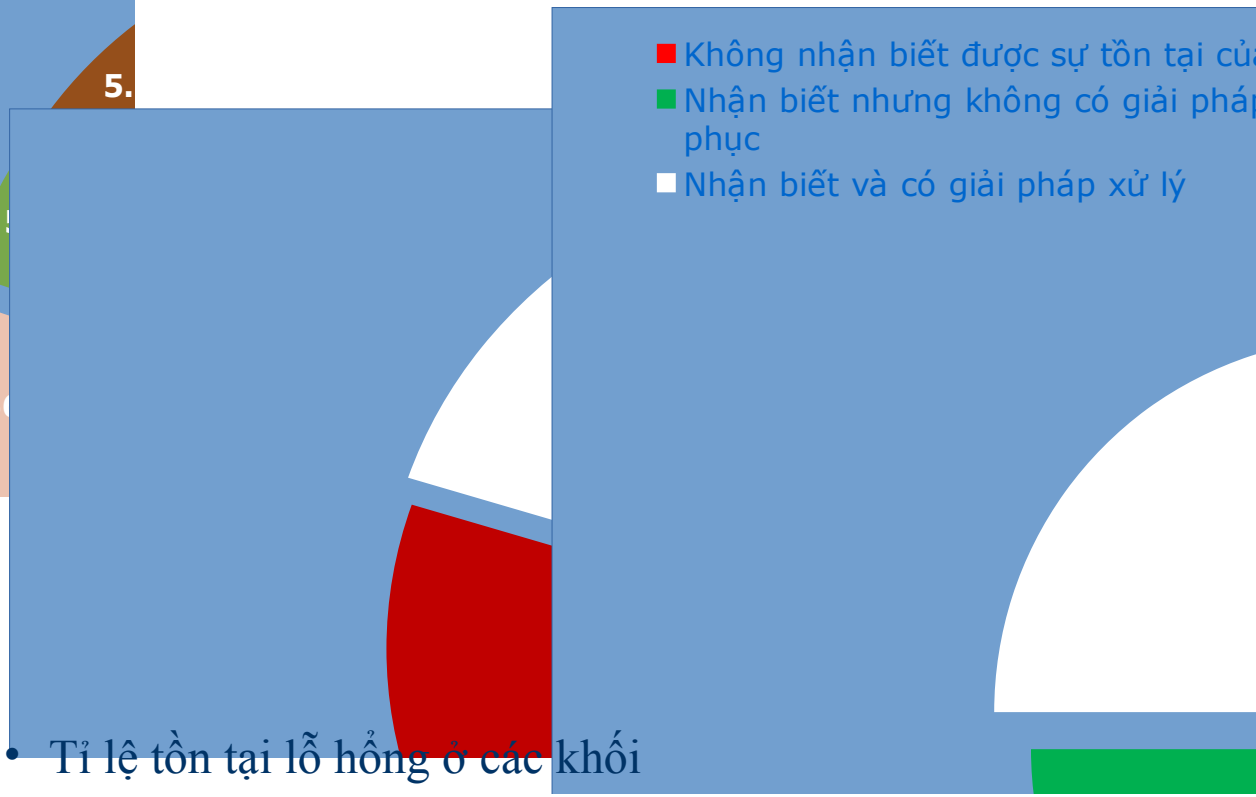



- Tỉ lệ các mối đe dọa từ bản thân các thiết bị bảo mật

- Những lỗ hổng thường gặp ở các tổ chức




- Tỉ lệ nhận biết sự tồn tại của lỗ hổng



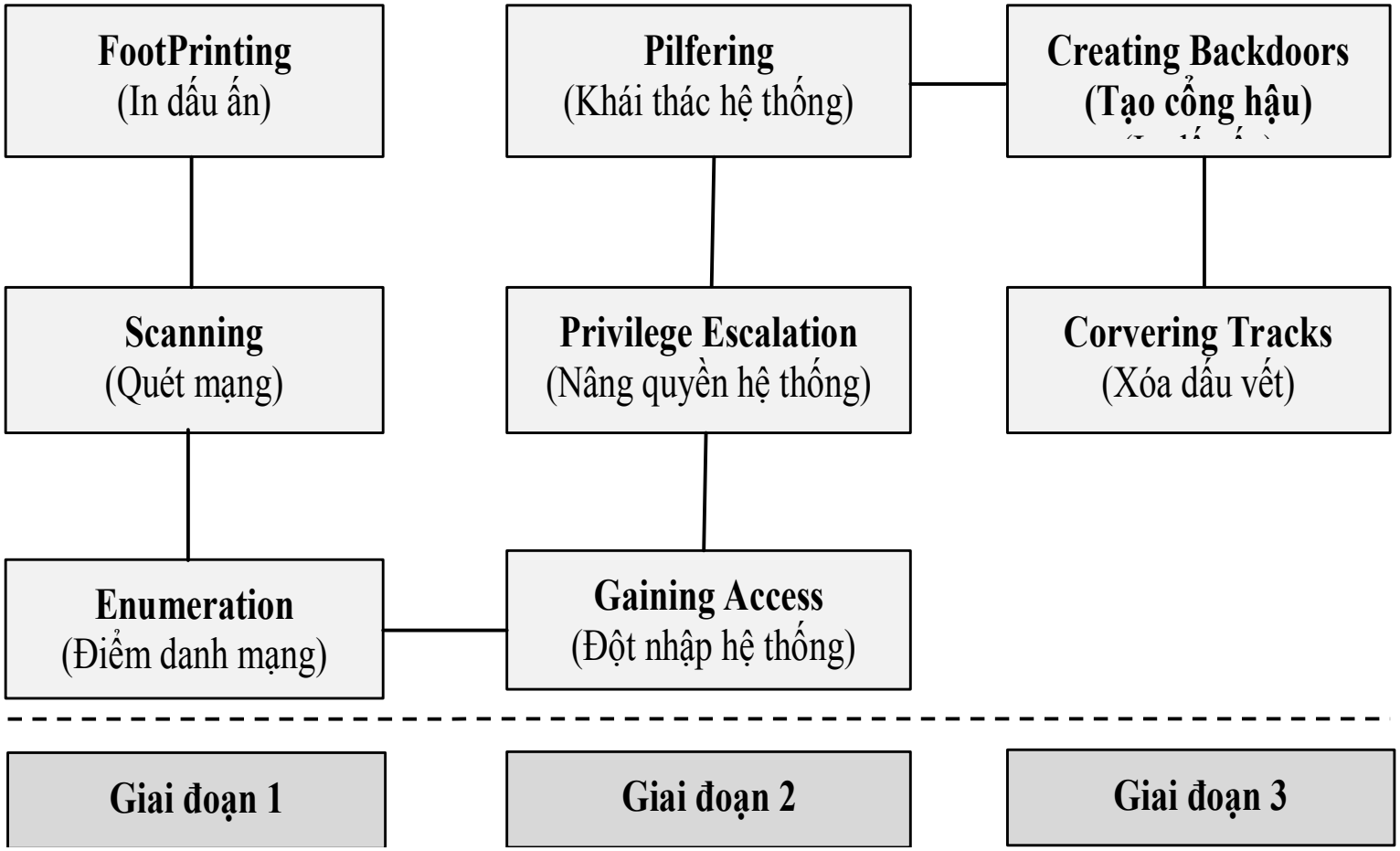

- Tỉ lệ tồn tại lỗ hổng ở các khối

# Phản ứng của các tổ chức khi bị tấn công?

## Chúng ta cần làm gì?


Vậy nếu thực sự một cuộc chiến tranh mạng diễn ra, Việt Nam đủ sức ứng phó?

# 2. Mô hình tấn công mạng máy tính

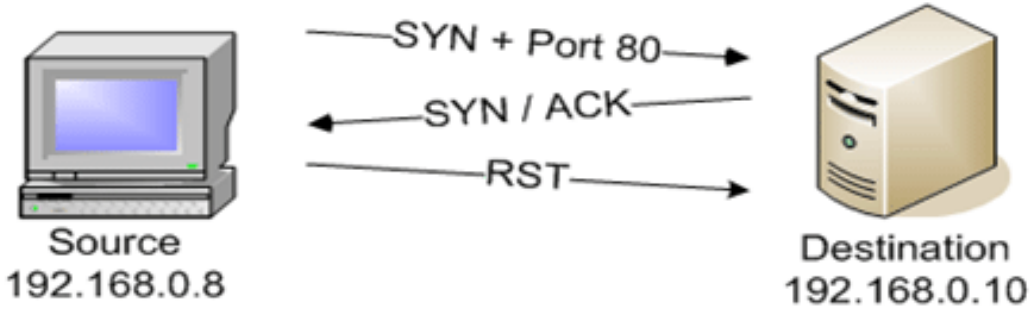


# Giai đoạn 1 – Trinh sát

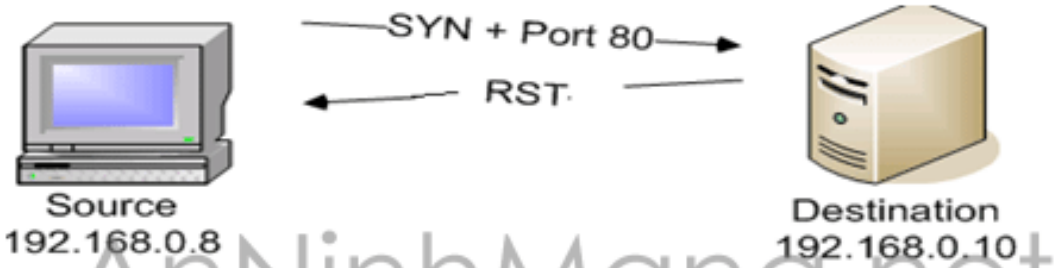
- Thăm dò thông tin trên hệ thống mục tiêu.
- Thu thập các thông tin của hệ thống:
  - hệ điều hành
  - dịch vụ
  - Cổng
  - …
- Thu thập passive: Thu thập các thông tin như vị trí địa lý, điện thoại, email của các cá nhân, người điều hành trong tổ chức.
- Thu thập active: Thu thập các thông tin về địa chỉ IP, domain, DNS,… của hệ thống

# Giai đoạn 1 – Quét hệ thống

- Quét thăm dò hệ thống là phương pháp để tìm hiểu hệ thống và thu thập các thông tin như địa chỉ IP cụ thể, hệ điều hành hay các kiến trúc hệ thống mạng.




Hình 1.2 Quét trộm đối với cổng không hoạt động






Hình 1.3 Đối với cổng hoạt động

# Giai đoạn 2 – Đột nhập & khai thác

- Chiếm quyền điều khiển (Gainning access)
  - Mức hệ điều hành/ mức ứng dụng
  - Mức mạng
  - Từ chối dịch vụ

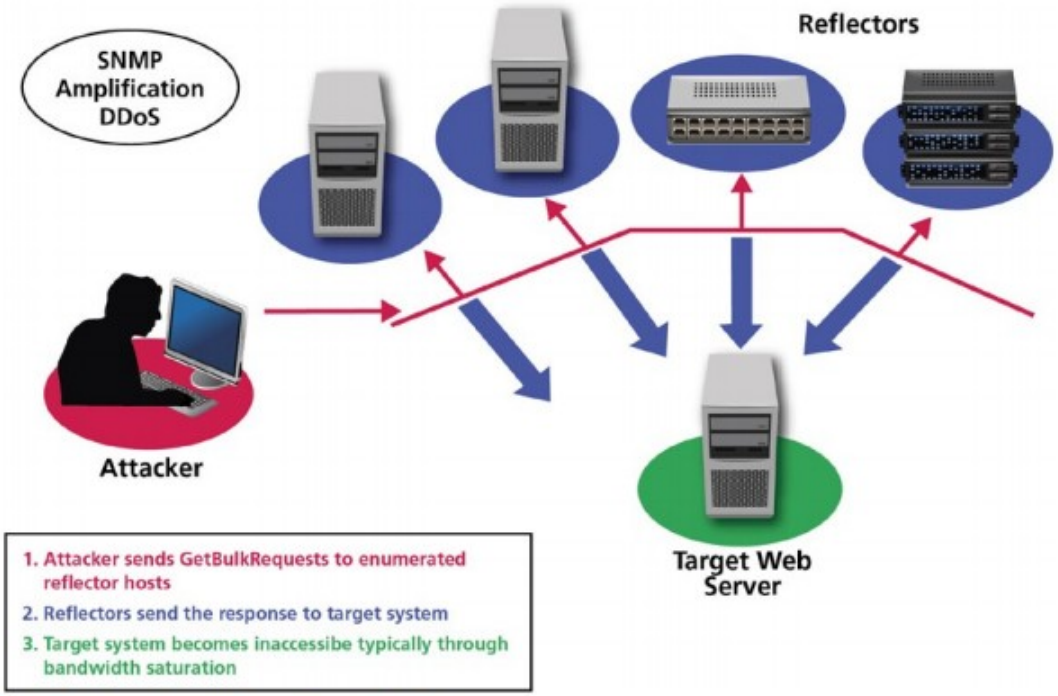



Figure 3: Topology of an SNMP amplification DDoS attack

# Giai đoạn 2 – Duy trì điều khiển

- Duy trì điều khiển hệ thống (Maitaining access)

  Upload/download biến đổi thông tin

```
[11:33:59] [INFO] fetching columns like 'password, user, user_id' for table 'users' in database 'dvwa'
[11:33:59] [INFO] fetching entries of column(s) 'password, user, user_id' for table 'users' in database 'dvwa'
[11:33:59] [INFO] analyzing table dump for possible password hashes
recognized possible password hashes in column 'password'. Do you want to crack them via a dictionary-based atta
ck? [Y/n/q] y

[11:34:02] [INFO] using hash method 'md5_generic_passwd'
[11:34:02] [INFO] resuming password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99' for user 'admin'
[11:34:02] [INFO] resuming password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b' for user '1337'
[11:34:02] [INFO] resuming password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03' for user 'gordonb'
[11:34:02] [INFO] resuming password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7' for user 'pablo'
[11:34:02] [INFO] postprocessing table dump
Database: dvwa
Table: users
[5 entries]
+---------+---------+-------------------------------------------+
| user_id | user    | password                                  |
+---------+---------+-------------------------------------------+
| 1       | admin   | 5f4dcc3b5aa765d61d8327deb882cf99 (password) |
| 2       | gordonb | e99a18c428cb38d5f260853678922e03 (abc123)   |
| 3       | 1337    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  |
| 4       | pablo   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  |
| 5       | smithy  | 5f4dcc3b5aa765d61d8327deb882cf99 (password) |
+---------+---------+-------------------------------------------+

[11:34:02] [INFO] table 'dvwa.users' dumped to CSV file '/pentest/database/sqlmap/output/192.168.152.129/dump/d
vwa/users.csv'
[11:34:02] [INFO] fetched data logged to text files under '/pentest/database/sqlmap/output/192.168.152.129'

[*] shutting down at 11:34:02
```

# Giai đoạn 3 – Tạo cổng hậu

# Giai đoạn 3 – Xoá dấu vết

- Xoá dấu vết (Covering tracks)

Sau khi bị tấn công thì hệ thống sẽ lưu lại những vết do attacker để lại. Attacker cần xoá chúng đi nhằm tránh bị phát hiện.

# 3. Một số kỹ thuật tấn công mạng máy tính

- Port scan attack
- Eavesdropping attack
- IP spoofing attack
- Man-in-the-middle Attack
- Replay attack
- Hijacking Attack
- Denial of Service / Distributed Denial of Service (DoS/DDoS) Attacks
- Các loại tấn công phần mềm

# Nguyên tắc truyền thông tin

- Cấu tạo gói tin TCP
- Phần giữa IP và ứng dụng

| + | Bit 0 - 3 | 4 - 9 | 10 - 15 | 16 - 31 |
|---|---|---|---|---|
| 0 | Source Port | | | Destination Port |
| 32 | Sequence Number | | | |
| 64 | Acknowledgement Number | | | |
| 96 | Data Offset | Reserved | Flags | Window |
| 128 | Checksum | | | Urgent Pointer |
| 160 | Options (optional) | | | |
| 160/192+ | Data | | | |

# Nguyên tắc truyền thông tin

- Các gói tin chỉ ra địa chỉ, cổng đến từ đó hệ thống mạng sẽ định hướng chuyển gói tin
- Các gói tin chỉ ra nguồn gửi để nơi nhận có phản hồi phù hợp
- Sử dụng chỉ số thứ tự để xác định cách lắp ghép
- Sử dụng các bít cờ để xác định nội dung dữ liệu, và trạng thái điều khiển

# Nguyên tắc truyền thông tin

- Các pha kết nối
- thiết lập kết nối
- truyền dữ liệu
- kết thúc kết nối

# Nguyên tắc truyền thông tin

- Các trạng thái kết nối
- LISTEN
- SYN-SENT
- SYN-RECEIVED
- ESTABLISHED
- FIN-WAIT-1
- FIN-WAIT-2
- CLOSE-WAIT
- CLOSING
- LAST-ACK
- TIME-WAIT
- CLOSED

# Nguyên tắc truyền thông tin

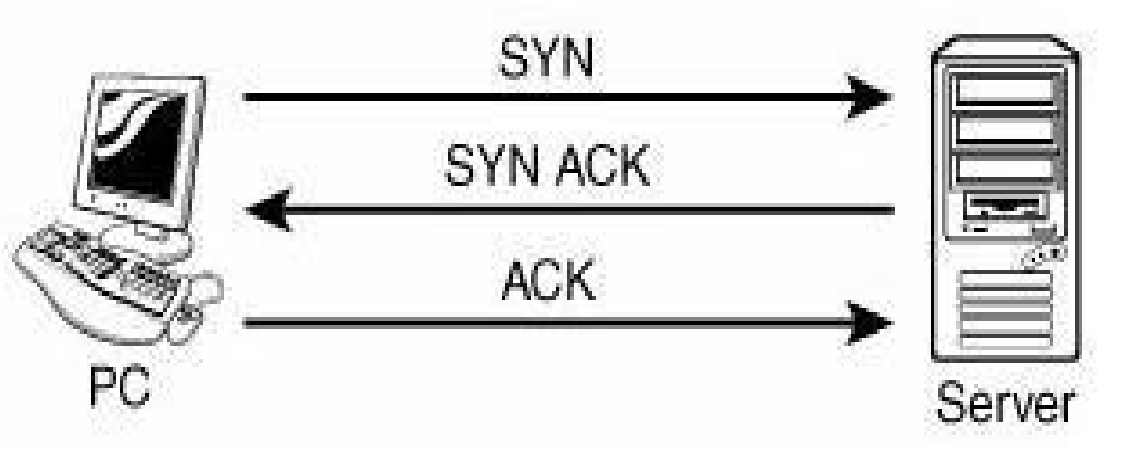
- Mô tả thông tin
  - LISTEN
    - đang đợi yêu cầu kết nối từ một TCP và cổng bất kỳ ở xa
  - SYN-SENT
    - đang đợi TCP ở xa gửi một gói tin TCP với các cờ SYN và ACK được bật
  - SYN-RECEIVED
    - đang đợi TCP ở xa gửi lại một tin báo nhận sau khi đã gửi cho TCP ở xa đó một tin báo nhận kết nối

# Nguyên tắc truyền thông tin

- Mô tả thông tin
  - ESTABLISHED
    - cổng đã sẵn sàng nhận/gửi dữ liệu với TCP ở xa (đặt bởi TCP client và server)
  - TIME-WAIT
    - đang đợi qua đủ thời gian để chắc chắn là TCP ở xa đã nhận được tin báo nhận về yêu cầu kết thúc kết nối của nó. Theo RFC 793, một kết nối có thể ở tại trạng thái TIME- WAIT trong vòng tối đa 4 phút.

# Kết nối

- Client: gửi gói tin SYN, tham số **sequence number** được gán cho một giá trị ngẫu nhiên **X**.
- Server: gửi lại SYN-ACK, tham số **acknowledgment number** X + 1, tham số **sequence number** được gán ngẫu nhiên **Y**
- Client: gửi ACK, tham số **sequence number** X + 1,tham số **acknowledgment number** Y + 1



# Kết thúc phiên

- + Bước I: Client gửi đến FIN ACK
  + Bước II: Server gửi lại c ACK
  + Bước III: Server lại gửi FIN ACK
  + Bước IV: Client gửi lại ACK

# Gói tin UDP

- Cấu trúc UDP

| offset (bits) | 0 – 15 | 16 – 31 |
|---|---|---|
| 0 | Source Port Number | Destination Port Number |
| 32 | Length | Checksum |
| 64+ | Data | |

# Gói tin UDP

- IPv4
  UDP

| bits | 0 – 7 | 8 – 15 | 16 – 23 | 24 – 31 |
|---|---|---|---|---|
| 0 | Source address | | | |
| 32 | Destination address | | | |
| 64 | Zeros | Protocol | UDP length | |
| 96 | Source Port | | Destination Port | |
| 128 | Length | | Checksum | |
| 160+ | Data | | | |

# Nguyên tắc Port scan

- 1. TCP Scan
- Trên gói TCP/UDP có 16 bit dành cho Port Number điều đó có nghĩa nó có từ 1 – 65535 port.
- Thường chỉ scan từ 1 - 1024.
- Một số phương pháp:

# Nguyên tắc Port scan

- SYN Scan:
  - Gửi SYN với một thông số Port
  - Nhận SYN/ACK thì Client biết Port đó trên Server được mở.
  - Ngược lại Client nhận gói RST/SYN.
- FIN Scan:
  - Client gửi gói FIN với số port nhất định.
  - Nhận ACK thì Server mở port đó,
  - Server gửi về gói RST thì Client biết Server đóng port đó.

# Nguyên tắc Port scan

- NULL Scan Sure:
  - Client gửi tới Server những gói TCP với số port cần Scan không chứa thông số Flag nào,
  - Server gửi lại gói RST thì tôi biết port đó trên Server bị đóng.
- XMAS Scan Sorry:
  - Client gửi gói TCP với số Port nhất định cần Scan chứa nhiều Flag như: FIN, URG, PSH.
  - Nếu Server trả về gói RST tôi biết port đó trên Server bị đóng.

# Nguyên tắc Port scan

- **TCP Connect:**
  - gửi đến Server những gói tin yêu cầu kết nối port cụ thể trên server.
  - Nếu server trả về gói SYN/ACK thì mở cổng đó.
- **ACK Scan:**
  - Scan này nhằm mục đích tìm những Access Controll List trên Server. Client cố gắng kết nối tới Server bằng gói ICMP
  - nhận được gói tin là Host Unreachable thì client sẽ hiểu port đó trên server đã bị lọc.

# Công cụ portscan

- Tự xây dựng dựa trên cấu mô tả
- RPC Scan: Kiểm tra dịch vụ RPC
- Windows Scan: tương tự như ACK Scan, nhưng nó có thể chỉ thực hiện trên một số port nhất định.
- FTP Scan: Có thể sử dụng để xem dịch vụ FTP có được sử dụng trên Server hay không
- IDLE: cho phép kiểm tra tình trạng của máy chủ.

# Eavesdropping attack

- Nghe lén
- Mục tiêu: thu nhận thông tin truyền
  - Nhận được các thông tin truyền không mã hóa
  - Nhận được các thông tin đã mã hóa, từ đó phục vụ các tấn công khác (replay attack)
- Không để dấu vết
- Khó phòng chống

# Eavesdropping attack

- Sử dụng các phương pháp vật lý
  - Nghe trộm qua đường truyền vật lý
  - Qua hệ thống sống vô tuyến
- Nghe lén mạng
  - Tham gia vào mạn
  - Nhận các gói tin được truyền đến cổng mạng
  - Nếu mạng sử dụng là switch thì cần phải sử dụng phương pháp man – in – the - middle
- Nghe lén bằng phần mềm gián điệp

# Eavesdropping attack

- Ettercap, Ethereal, dsniff, TCPdump,  Sniffit,...
- Nhiều công cụ phần cứng khác tham  gia vào các mạng, phương

# Eavesdropping attack

- Một số phương pháp phòng chống:
- Sử dụng switch thay cho hub
- Giám sát địa chỉ MAC
- Sử dụng cơ chế mã hóa truyền tin, và mã hóa theo thời gian

# Eavesdropping attack

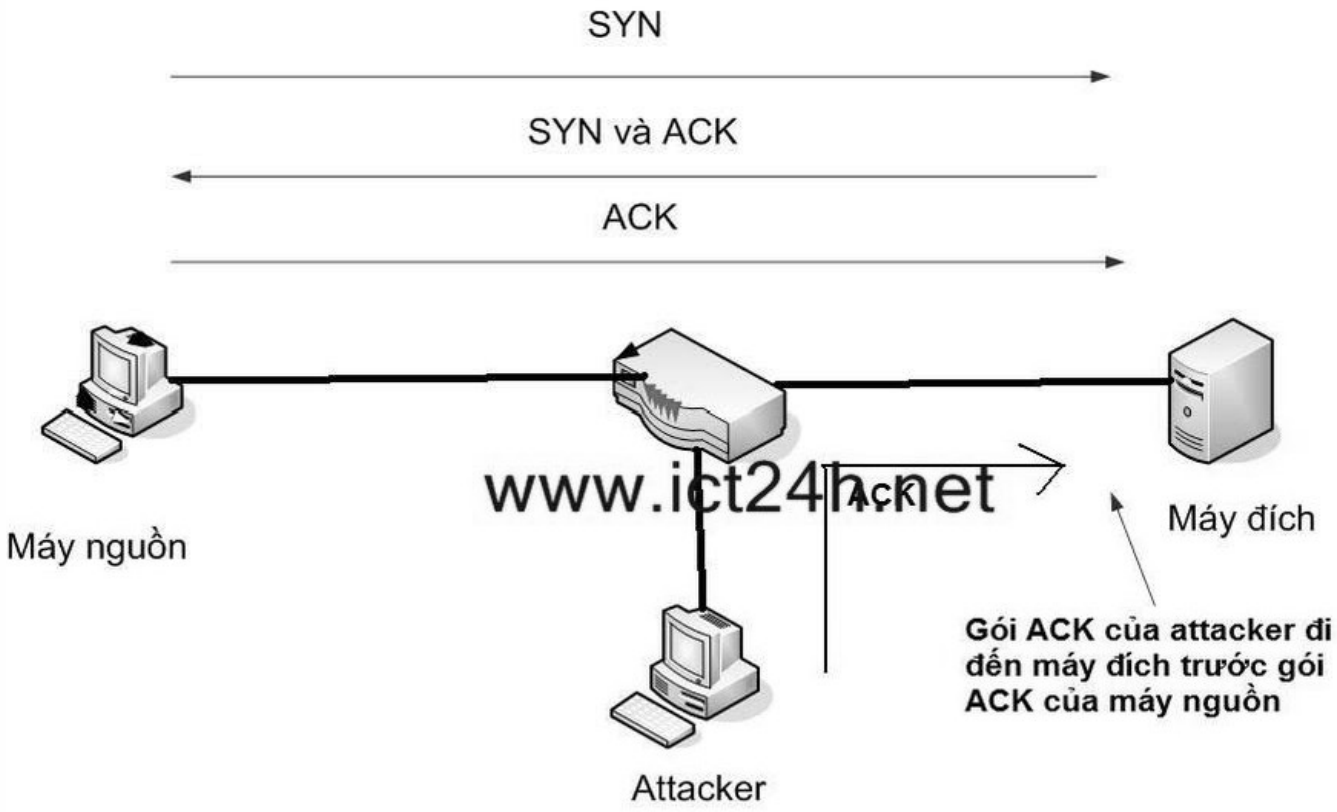
- Sử dụng các dịch vụ mã hóa trong liên kết: SSL (Secure Sockets Layer), thiết lập IPSec và mạng riêng ảo VNP (Virtual Private Network),… sử dụng SSH (Secure Shell Host) thay cho Telnet, Rlogin; dùng SFTP (secure FTP) thay vì FTP; dùng giao thức https thay cho http v.v…

# Eavesdropping attack

- Sử dụng các phần mềm phát hiện sự hoạt động của các chương trình nghe lén trên mạng như AntiSniff, PromiScan, Promqry and PromqryUI, ARPwatch, Ettercap, v.v… Riêngvới Ettercap (http://ettercap.sourceforge.net),
- Các công cụ chống tấn công gián điệp

# Eavesdropping attack

- Tạo ra các gói tin có địa chỉ IP giả mạo không là địa chỉ máy gửi gói tin
- Vượt qua các kiểm soát về nguồn góc địa chỉ ip
- Phục vụ các mô hình tấn công khác
  - Tấn công về phiên
  - Tấn công kiểu phản xạ
- Giải pháp
  - Không sử dụng xác thực là địa chỉ IP
  - Phát hiện các bất thường về kết nối mạng


SYN
SYN và ACK
ACK
www.ict24h.net
ACK
Máy nguồn
Máy đích
Attacker
Gói ACK của attacker đi đến máy đích trước gói ACK của máy nguồn

# MAN-IN-THE-MIDDLE IP Cục bộ

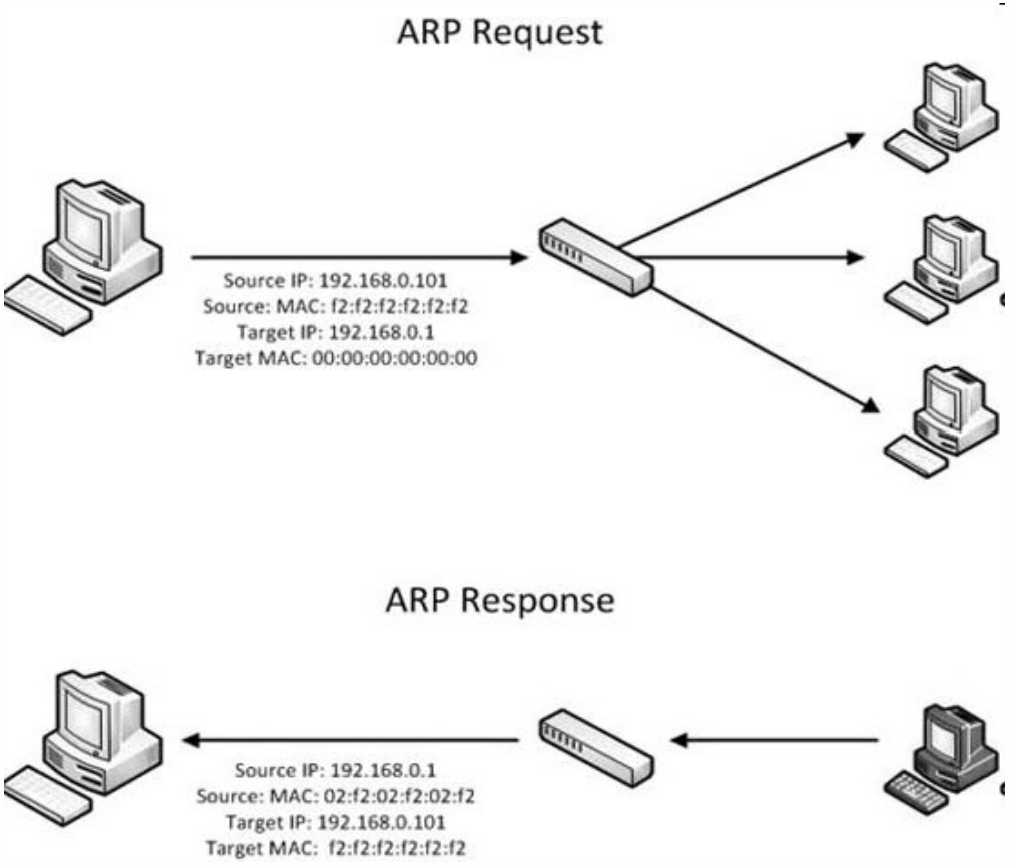
- Nếu một máy tấn công có cùng subnet với máy nạn nhân
- Yêu cầu máy nạn nhận gửi tin thông qua máy tấn công: gửi các gói tin ARP giả địa chỉ MAC của attacker là địa chỉ MAC của router kế tiếp (next- hop).

# Man-in-the-middle Attack

# 1.Khái niệm

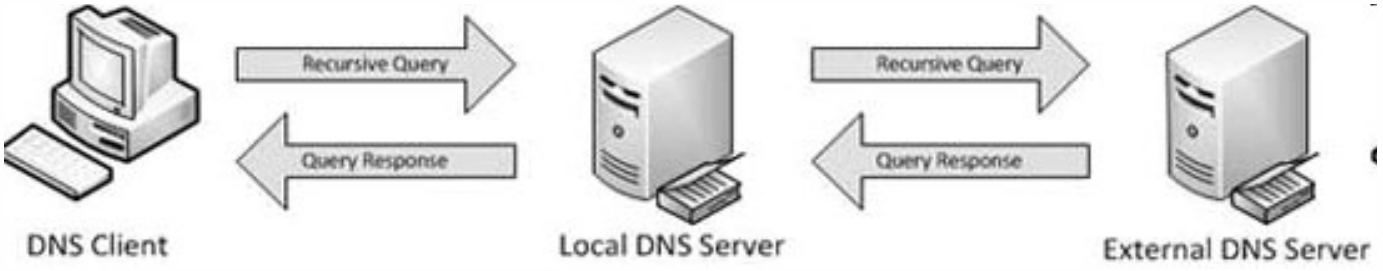
- Tấn công khi làm cho hai bên kết  nối, hiểu nhầm người thứ 3 là đối tác  của mình
- Tấn công bằng bộ phát sống giả mạo  (AP)
  - Sử dụng bộ phát có sóng mạnh hơn
  - Máy kết nối nhầm, hoặc xác thực nhầm
- Tấn công bằng làm giả tín hiệu tính  hiệu ARP
  - Gửi các thông điệp map giữa IP và MAC

# 1.Khái niệm


ARP Request
Source IP: 192.168.0.101
Source: MAC: f2:f2:f2:f2:f2:f2
Target IP: 192.168.0.1
Target MAC: 00:00:00:00:00:00
ARP Response
Source IP: 192.168.0.1
Source: MAC: 02:f2:02:f2:02:f2
Target IP: 192.168.0.101
Target MAC: f2:f2:f2:f2:f2:f2

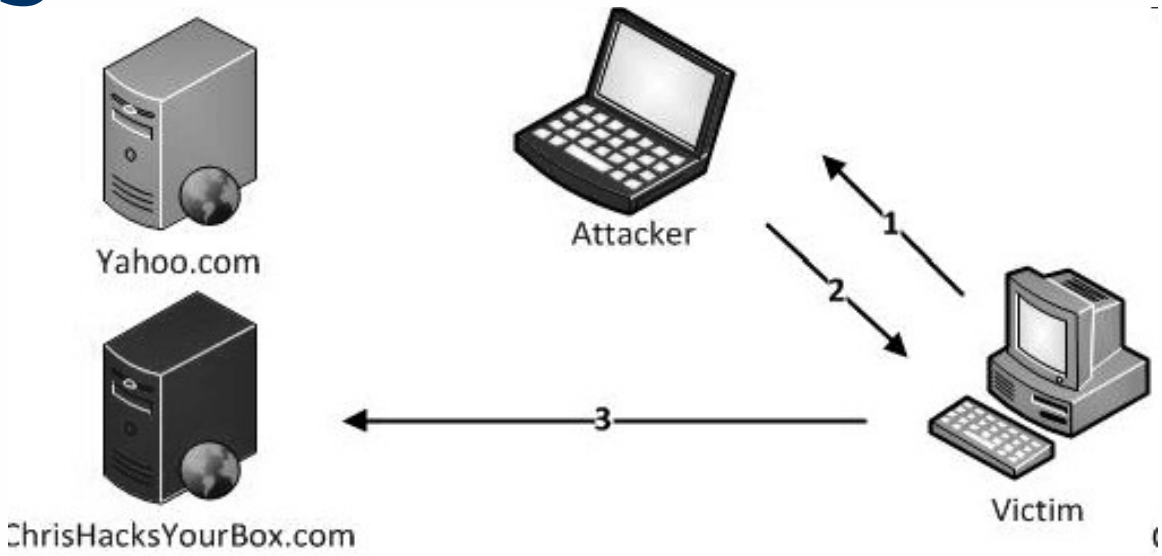
# 1.Khái niệm

- Tấn công  vào DNS
  - Dựa trên cơ chế gửi và nhận địa chỉ IP  thông qua tên miền
  - Gửi một địa chỉ IP khác với địa chỉ



# 1.Khái niệm

- Tấn công vào DNS




1. Legitimate DNS Request Destined for DNS Server
2. Fake DNS Reply from Listening Attacker
3. Victim begins communicating with malicious site as a result

# 4. Công cụ MITM tấn công

- PacketCreator
- Ettercap
- Dsniff
- Cain e Abel

# 5. Cách chống lại tấn công MITM

- Bảo mật vật lý (Physical security) là phương pháp tốt nhất để chống lại kiểu tấn công này.
- Ngoài ra, ta có thể ngăn chặn hình thức tấn công này bằng kỹ thuật mã hoá: mã hoá traffic trong một đường hầm IPSec, hacker sẽ chỉ nhìn thấy những thông tin không có giá trị.

# Replay attack  (tấn công phát lại)

# Thẻ phiên

- Sử dụng thông tin nghe lén
  - Lưu trữ
  - Gửi lại thông tin đến máy cần để xác thực
- Giải pháp
  - Xác thực theo phiên (chỉ số phiên)
  - Sử dụng phương pháp xác thực lại theo thời gian (sau thời gian kết nối)

# Kẻ tấn công chiếm quyền điều  khiển

# I. Thế nào là một kẻ tấn công chiếm quyền điều khiển?

- Nghe lén thông tin liên lạc
- Đợi kết thúc quá trình xác thực
- Gửi tín hiêu yêu cầu kết

# II. Giải pháp

- Tiến hành mã hóa phiên
- Xác thực phiên theo thời gian

# V. Công cụ kẻ tấn công chiếm quyền điều khiển sử dụng:

- Có một vài chương trình có sẵn có thể thực hiện được việc chiếm quyền điều khiển.
- Dưới đây là một vài chương trình thuộc loại này:
  - Juggernaut
  - Hunt
  - IP Watcher
  - T-Sight
  - Paros HTTP Hijacker

# Tấn công từ chối dịch vụ

- Tấn công làm cho một hệ thống nào đó bị quá tải không thể cung cấp dịch vụ hoặc phải ngưng hoạt động.
- Tấn công kiểu này chỉ làm gián đoạn hoạt động của hệ thống chứ rất ít có khả năng thâm nhập hay chiếm được thông tin dữ liệu của nó

# Các loại tấn công từ chối dịch vụ

- Tấn công từ chối dịch vụ cổ điển DoS (Denial of Service)
- Tấn công từ chối dịch vụ phân tán DDoS (Distributed Denial of Service)
- Tấn công từ chối dịch vụ theo phương pháp phản xạ DRDoS (Distributed Reflection Denial of Service).

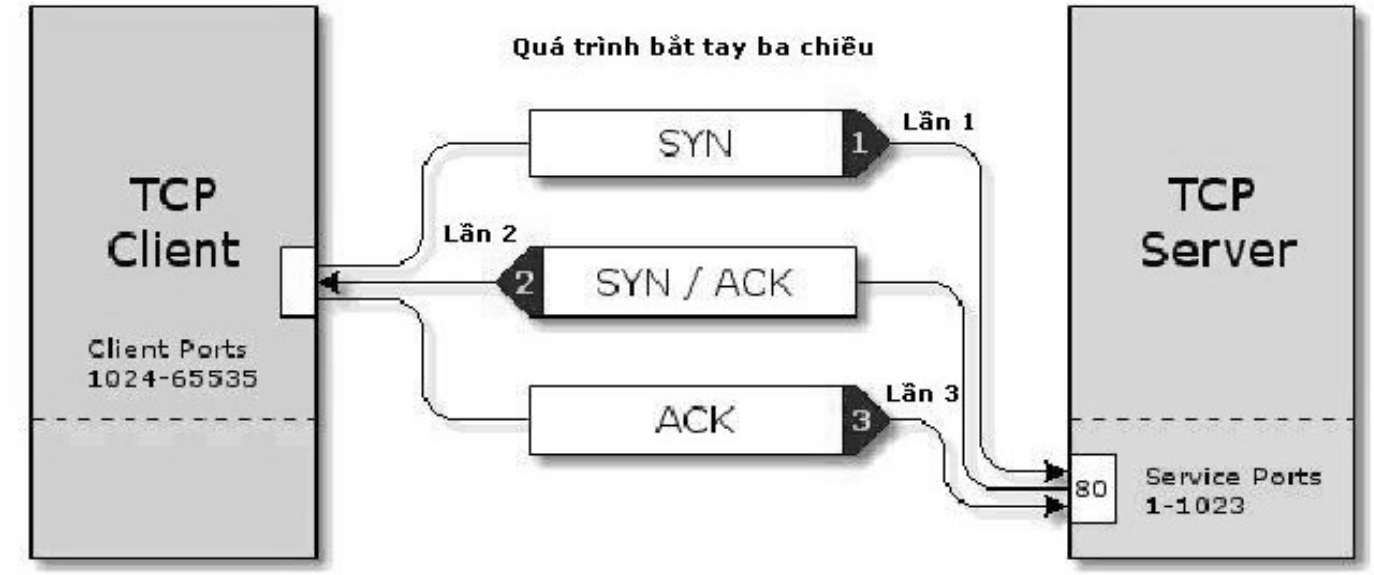
# Biến thể của tấn công DoS

- Broadcast Storms
- SYN
- Finger
- Ping
- Flooding,…

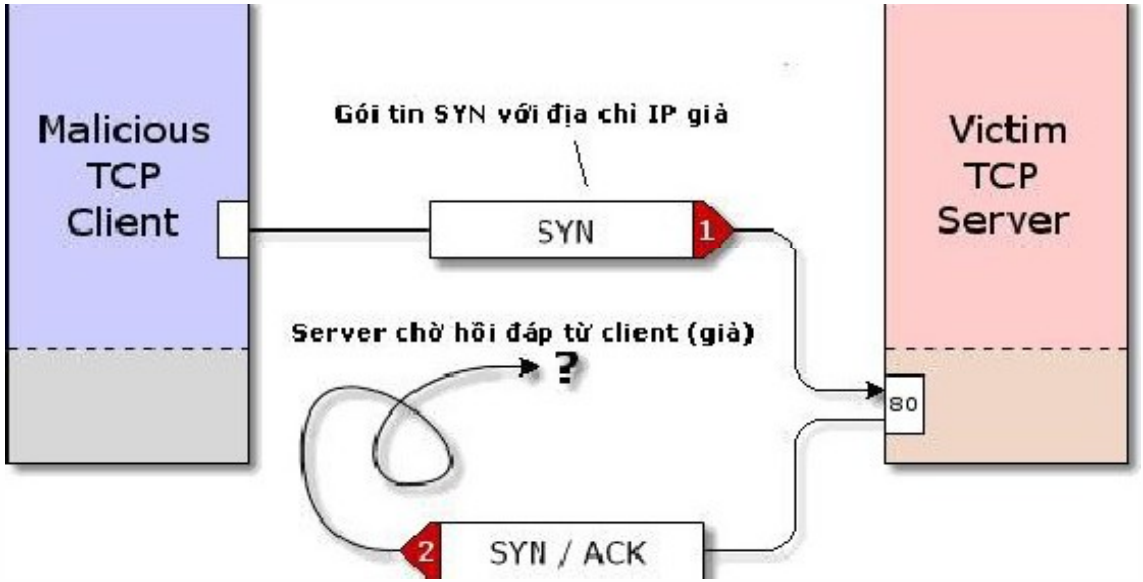
# Tấn công từ chối dịch vụ cổ điển

- Là phương thức xuất hiện đầu tiên, giản đơn nhất trong kiểu tấn công từ chối dịch vụ.Các kiểu tấn công thuộc phương thức này rất đa dạng
- Ví dụ một dạng tấn công tiêu biểu:
  - SYN Attack

# Bắt tay ba chiều trong kết nối TCP



# DoS dùng kỹ thuật SYN Flood



# DoS dùng kỹ thuật SYN

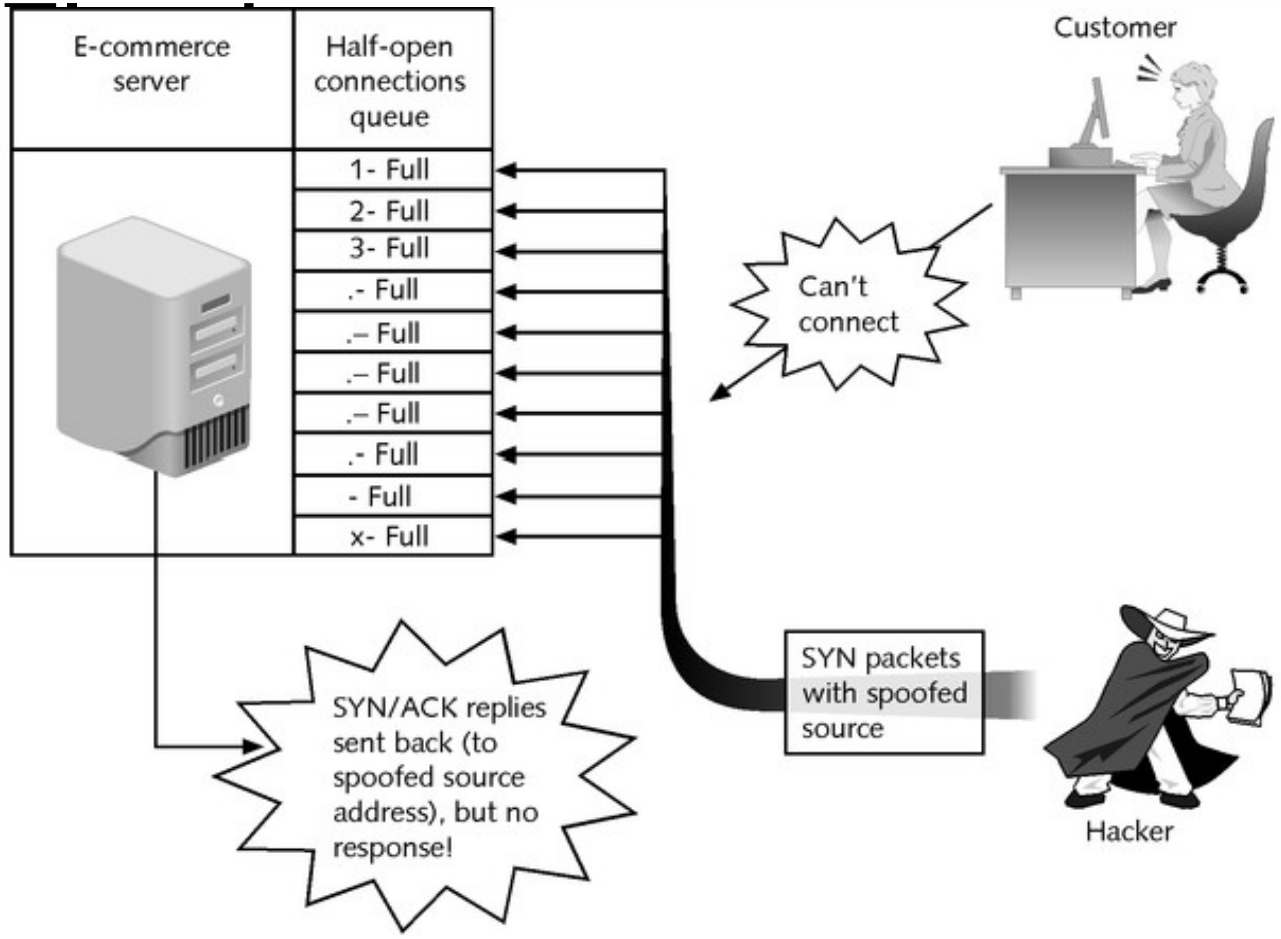
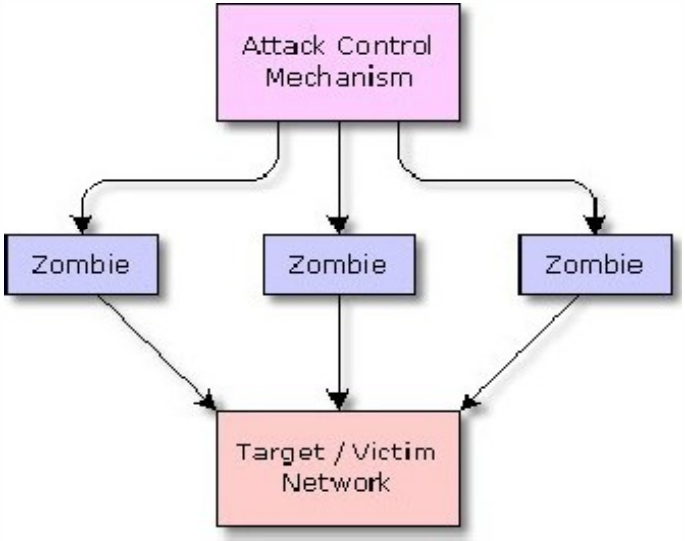



**Figure 3-2** SYN flood attack

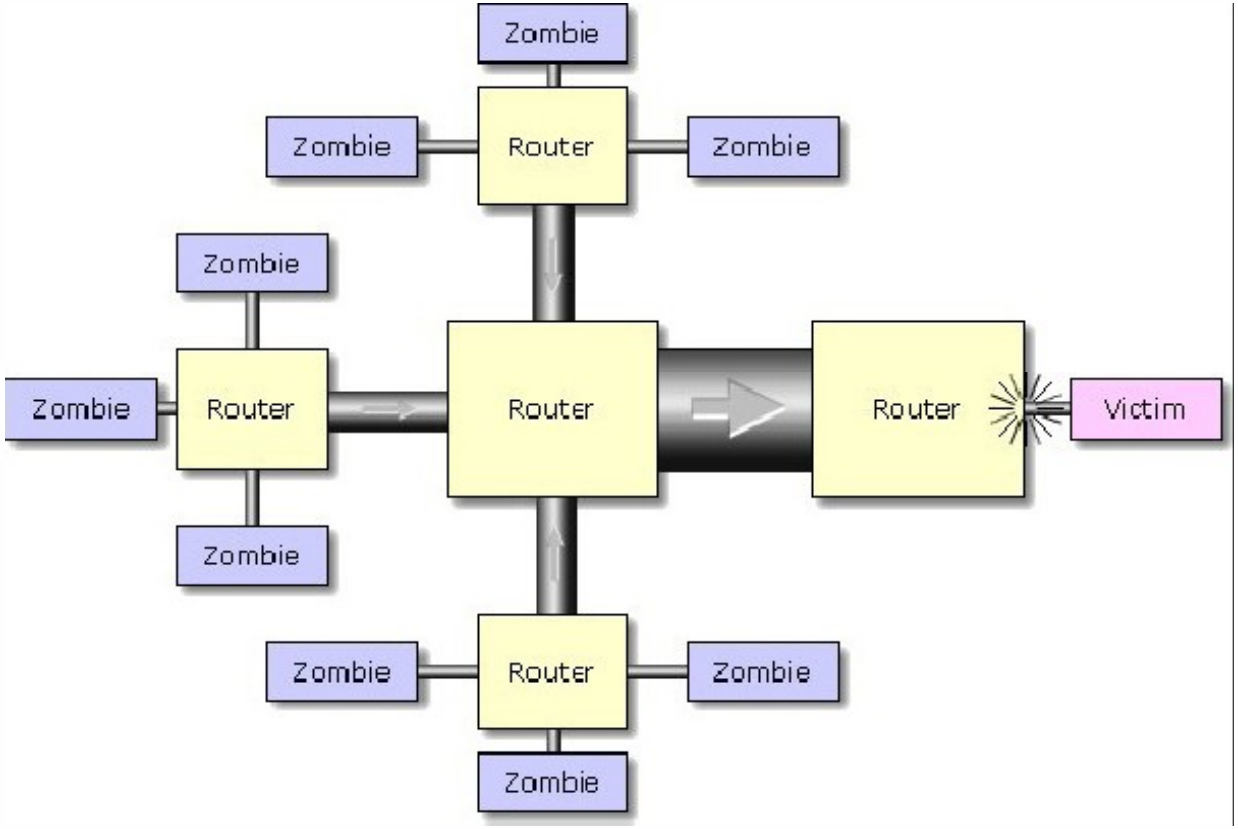
# Tấn công từ chối dịch vụ kiểu phân tán (DDoS)

- Xuất hiện vào mùa thu 1999
- So với tấn công DoS cổ điển, sức mạnh của DDoS cao hơn gấp nhiều lần.
- Hầu hết các cuộc tấn công DDoS nhằm vào việc chiếm dụng băng thông (bandwidth) gây nghẽn mạch hệ thống dẫn đến hệ thống ngưng hoạt động.

# Tấn công từ chối dịch vụ kiểu phân tán (DDoS)



# Tấn công từ chối dịch vụ kiểu phân tán (DDoS)



# Password attack

- Định nghĩa
  - Tấn công bằng mật khẩu là một kiểu phần mềm tấn công, trong đó kẻ tấn công cố gắng đoán mật khẩu hoặc crack mật khẩu mã hóa các file.

# Password attack

- Tấn công reset mật khẩu
- Nghe lén mật khẩu
- Tấn công dò mật khẩu

# Password attack

- Tấn công reset mật khẩu
  - Biết cơ chế mã hóa
  - Biết vị trí mã hóa
  - Khả năng truy xuất vào khu vực lưu trữ mã hóa
  - Tiến hành tính toán mật khẩu mới lưu vào vị trí lưu trữ

# Password attack

- Nghe lén
  - Nghe lén, trộm mật khẩu lưu trữ vật lý
  - Nghe lén thông tin từ đó nhận được được  mật khẩu không mã hóa
  - Nghe lén và lưu nhận mật khẩu đã mã hóa  từ đó tiến hành gửi lại xác thực sau

# Password attack

- Dò mật khẩu
  - Dò mật khẩu từ thông tin thu nhận được từ đối tượng bị tấn công
  - Dò tìm mật khẩu thông qua từ điển (đưa ra các mật khẩu có thể có theo thống kê)
  - Dò mật theo kiểu vét cạn, tất cả các trường hợp mật khẩu có thể có

# Password attack

- Cách phòng tránh
  - Không cho phép user dùng cùng password trên các hệ thống.
  - Làm mất hiệu lực account sau một vài lần login không thành công.
  - Không dùng passwords dạng clear text
  - Dùng strong passwords

# Misuse of Privilege Attack

- **Định nghĩa**
  - Misuse of Privilege Attack ( Cuộc tấn công sử dụng sai các đặc quyền) là một loại phần mềm tấn công, trong đó kẻ tấn công sử dụng đặc quyền quản trị hệ thống để truy cập dữ liệu nhạy cảm. Loại tấn công này thường liên quan đến một nhân viên, với một số quyền quản trị trên một máy tính, một nhóm các máy móc hay một số phần của hệ thống mạng

# Misuse of Privilege Attack

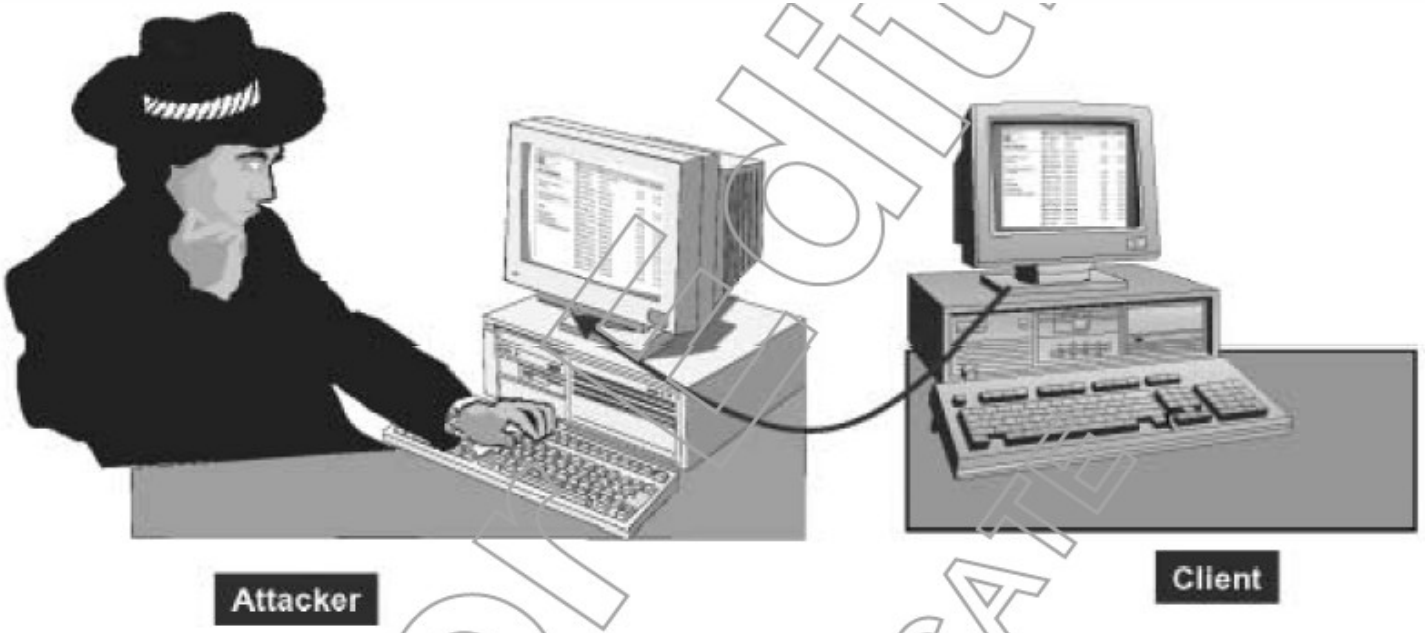



**Figure 1-13:** *Misuse of privilege attacks.*

# Misuse of Privilege Attack

- Ví dụ

  Một quản trị mạng có khả năng truy cập vào các tập tin về thông tin cá nhân được lưu trữ trong cơ sở dữ liệu là một trong những tài nguyên quan trọng như là cơ sở dữ liệu nhận dạng của công an. Từ các tập tin về thông tin cá nhân này, anh ta có thể lấy tên đầy đủ, địa chỉ, số an sinh xã hội, và các dữ liệu khác, mà có thể có thể bán cho những người có thể sử dụng nó cho tội phạm liên quan đến gian lận nhận dạng.

# Misuse of Privilege Attack

- Nguyên lý tấn công.

  Nhân viên có quyền truy cập hệ thống và các dữ liệu nhạy cảm, nhân viên này sử dụng các hình thức để ăn cắp dữ liệu nhạy cảm để bán ra ngoài:
- Lấy cắp dữ liệu nhạy cảm và chuyển ra ngoài hệ thống
- Cung cấp username, password cho những người ngoài hệ thống để xâm nhập hệ thống
- Cấp quyền truy cập cho những người ngoài hệ thống, dẫn đến mất mát dữ liệu

# Misuse of Privilege Attack

- Cách phòng chống.
  - Mỗi nhân viên chỉ được cung cấp một quyền rất nhỏ để truy cập vào từng phần của hệ thống, không cho phép 1 nhân viên có quyền can thiệp vào hệ thống
  - Những chức năng quan trọng của hệ thống phải được đảm bảo do admin tin cậy của hệ thống quản lý

- Software Exploitation Attacks
  - Tấn công vào lỗ hổng của các ứng dụng
  - Hệ điều hành
  - Các ứng dụng thông dụng của bên thứ 3 cung cấp: SQL server, Oracle server, IE, Firefox, …


Q&A