HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

AN TOÀN VÀ BẢO MẬT HỆ THỐNG THÔNG TIN

NỘI DUNG 3 – CÁC DẠNG TẤN CÔNG VÀ CÁC PHẦN MỀM ĐỘC HẠI

Giảng viên: TS. Đinh Trường Duy

Điện thoại/E-mail: duydt@ptit.edu.vn

Khoa: An toàn thông tin

Nội dung bài giảng dựa trên bài giảng và giáo trình Cơ sở an toàn thông tin của PGS.TS. Hoàng Xuân Dậu

NỘI DUNG 3

1. Khái quát về mối đe dọa, điểm yếu và tấn công
2. Các công cụ hỗ trợ tấn công
3. Các dạng tấn công phá hoại
4. Các dạng phần mềm độc hại

3.1 Khái quát về mối đe dọa, lỗ hổng và tấn công

- Mối đe dọa (Threat)
  - Mối đe dọa là bất kỳ một hành động nào có thể gây hư hại đến các tài nguyên hệ thống (gồm phần cứng, phần mềm, CSDL, các file, dữ liệu, hoặc hạ tầng mạng vật lý,…).
- Điểm yếu (Weakness)
  - Điểm yếu là một lỗi hoặc một khiếm khuyết tồn tại trong hệ thống.
  - Các hệ thống luôn tồn tại các điểm yếu.
- Lỗ hổng (Vulnerability)
  - Lỗ hổng là bất kỳ điểm yếu nào trong hệ thống cho phép mối đe dọa có thể gây tác hại.

3.1 Khái quát về mối đe dọa, lỗ hổng và tấn công

- Quan hệ giữa Mối đe dọa và Lỗ hổng:
  - Các mối đe dọa thường khai thác một hoặc một số lỗ hổng đã biết để thực hiện các cuộc tấn công phá hoại;
  - Nếu tồn tại một lỗ hổng trong hệ thống, sẽ có khả năng một mối đe dọa trở thành hiện thực;
  - Không thể triệt tiêu được hết các mối đe dọa, nhưng có thể giảm thiểu các lỗ hổng, qua đó giảm thiểu khả năng bị tận dụng để tấn công.

3.1 Khái quát về mối đe dọa, lỗ hổng và tấn công

- Các mối đe dọa thường gặp:
  - Phần mềm độc hại
  - Hư hỏng phần cứng hoặc phần mềm
  - Kẻ tấn công ở bên trong
  - Mất trộm các thiết bị
  - Kẻ tấn công ở bên ngoài
  - Tai họa thiên nhiên
  - Gián điệp công nghiệp
  - Khủng bố phá hoại.
- Không phải tất cả các mối đe dọa là độc hại (malicious)
  - Một số là là cố ý
  - Một số có thể là ngẫu nhiên/vô tình.

3.1 Khái quát về mối đe dọa, lỗ hổng và tấn công

- Các lỗ hổng tồn tại trong cả 7 vùng của nền tảng CNTT.
  - Lỗ hổng trong vùng người dùng
  - Lỗ hổng trong vùng máy trạm
  - Lỗ hổng trong vùng mạng LAN
  - Lỗ hổng trong vùng LAN-to-WAN
  - Lỗ hổng trong vùng WAN
  - Lỗ hổng trong vùng truy nhập từ xa
  - Lỗ hổng trong vùng hệ thống/ứng dụng

3.1 Khái quát về mối đe dọa, lỗ hổng và tấn công

- Các lỗ hổng tồn tại trong hệ điều hành và các phần mềm ứng dụng:
  - Lỗi tràn bộ đệm (buffer overflows)
  - Không kiểm tra đầu vào (unvalidated input)
  - Các vấn đề với điều khiển truy cập (access-control problems)
  - Các điểm yếu trong xác thực, trao quyền (weaknesses in authentication, authorization)
  - Các điểm yếu trong các hệ mật mã (weaknesses in cryptographic practices).

3.1 Khái quát về mối đe dọa, lỗ hổng và tấn công

- Tấn công độc hại/phá hoại (Malicious attacks)
  - Một cuộc tấn công (attack) vào hệ thống máy tính hoặc các tài nguyên mạng được thực hiện bằng cách khai thác các lỗ hổng trong hệ thống;
  - Tấn công = Mối đe dọa + Lỗ hổng

3.1 Khái quát về mối đe dọa, lỗ hổng và tấn công

- Các loại tấn công: 4 loại chính:
  - Giả mạo (Fabrications): Giả mạo thông tin thường để đánh lừa người dùng thông thường;
  - Chặn bắt (Interceptions): liên quan đến việc nghe trộm trên đường truyền và chuyển hướng thông tin để sử dụng trái phép;
  - Gây ngắt quãng (Interruptions): gây ngắt kênh truyền thông ngăn cản việc truyền dữ liệu;
  - Sửa đổi (Modifications): liên quan đến việc sửa đổi thông tin trên đường truyền hoặc sửa đổi dữ liệu file.

3.1 Khái quát về mối đe dọa, lỗ hổng và tấn công

- Hai kiểu tấn công:
  - Tấn công chủ động (Active attacks)
    - Sửa đổi dữ liệu trên đường truyền
    - Sửa đổi dữ liệu trong file
    - Giành quyền truy nhập trái phép vào máy tính hoặc hệ thống mạng
    - Tấn công chủ động là một đột nhập (intrusion) về mặt vật lý.
  - Tấn công thụ động (Passive attacks)
    - Không gây ra thay đổi trên hệ thống
    - Nghe lén
    - Giám sát lưu lượng trên đường truyền.

3.1 Khái quát về mối đe dọa, lỗ hổng và tấn công

- Một số dạng tấn công điển hình:
  - Tấn công vào mật khẩu
  - Tấn công bằng mã độc
  - Tấn công từ chối dịch vụ
  - Tấn công giả mạo địa chỉ, nghe trộm
  - Tấn công kiểu phát lại và người đứng giữa
  - Tấn công bằng bom thư và thư rác
  - Tấn công sử dụng cửa hậu
  - Tấn công kiểu Social Engineering
  - Tấn công phising, pharming

3.2 Các công cụ hỗ trợ tấn công

- Công cụ tấn công (Attack tools) là các công cụ phần cứng, phần mềm, hoặc các kỹ thuật hỗ trợ giúp kẻ tấn công (attacker) tấn công vào các hệ thống máy tính hoặc các tài nguyên mạng.
- Một số công cụ và kỹ thuật hỗ trợ tấn công:
  - Công cụ quét lỗ hổng (Vulnerability scanners)
  - Công cụ quét cổng dịch vụ (Port scanners)
  - Công cụ nghe lén (Sniffers)
  - Công cụ ghi phím gõ (Keyloggers)

3.2 Các công cụ hỗ trợ tấn công

- Công cụ quét lỗ hổng (Vulnerability scanners)
  - Thu thập các thông tin về các điểm yếu/lỗ hổng đã biết của hệ thống máy tính hoặc mạng;
  - Gửi những thông điệp được được tạo đặc biệt để kiểm tra điểm yếu/lỗ hổng đến hệ thống máy tính cần rà quét. Nếu hệ thống có phản hồi → điểm yếu vẫn tồn tại;
  - Kẻ tấn công sử dụng kết quả rà quét điểm yếu/lỗ hổng để quyết định dạng tấn công có khả năng thành công cao nhất.

3.2 Các công cụ hỗ trợ tấn công

❖ Một số công cụ quét lỗ hổng cho người quản trị:

- Microsoft Baseline Security Analyzer (đã được thay bằng Microsoft Defender Security Center and Microsoft Defender Advanced Threat Protection (ATP)):
  - Rà quét các lỗ hổng an ninh trong hệ điều hành Windows và các phần mềm của Microsoft;
  - Phân tích tình trạng lỗ hổng và có hướng dẫn khắc phục.
- Nessus vulnerability scanner;
  - Quét hệ thống hệ thống tìm lỗ hổng, điểm yếu
  - Độc lập với các nền tảng.
- Acunetix Web Vulnerability Scanner
  - Rà quét các ứng dụng web/trang web tìm các lỗ hổng.

3.2 Các công cụ hỗ trợ tấn công

- Công cụ quét cổng dịch vụ (Port scanners)
  - Các cổng TCP/IP, UDP năm trong khoảng từ 0 – 65535
    - Các cổng 0-1024 là các cổng chuẩn
    - Cổng lớn hơn 1024 là các cổng tùy gán.
  - Kẻ tấn công thường sử dụng công cụ quét cổng để nhận dạng các điểm yếu trong hệ thống;
  - Công cụ quét cổng kết nối đến máy tính để xác định cổng nào được mở và có thể truy nhập vào máy tính. Từ đó xác định được dịch vụ/ứng dụng nào đang chạy trên hệ thống:
    - Cổng 80/443 mở → dịch vụ web đang chạy
    - Cổng 25 mở → dịch vụ email SMTP đang chạy
    - Cổng 1433 mở → Máy chủ CSDL MS SQL Server đang chạy
    - Cổng 53 mở → dịch vụ DNS đang chạy,...

3.2 Các công cụ hỗ trợ tấn công

- Nguyên tắc tối thiểu các cổng được mở:
  - Đóng tất cả các cổng không sử dụng;
  - Chỉ mở những cổng có dịch vụ cần thiết cho người dùng.
- Một số công cụ quét cổng:
  - Nmap
  - Portsweep
  - Advanced Port Scanner (http://www.radmin.com)
  - Angry IP Scanner
  - Superscan
  - NetScanTools

3.2 Các công cụ hỗ trợ tấn công

- Công cụ nghe trộm (Sniffers)
  - Công cụ nghe trộm cho phép bắt các gói tin khi chúng được truyền trên mạng.
  - Công cụ nghe trộm có thể là mô đung phần cứng, phần mềm hoặc kết hợp.
  - Các thông tin nhạy cảm như mật khẩu nếu không được mã hóa thì có thể bị kẻ tấn công nghe trộm khi được truyền từ máy trạm đến máy chủ và bị lạm dụng.

3.2 Các công cụ hỗ trợ tấn công

- Một số công cụ cho phép bắt gói tin truyền:
  - Tcpdump
  - Pcap / Wincap (packet capture)
  - IP Tools (http://www.softpedia.com)
  - Wireshark

3.2 Các công cụ hỗ trợ tấn công

❖ Công cụ ghi phím gõ (Keyloggers)

- Công cụ ghi phím gõ là một dạng công cụ giám sát có thể bằng phần cứng hoặc phần mềm có khả năng ghi lại mọi phím người dùng gõ và lưu vào 1 file;
- Sau đó file đã ghi có thể được gửi cho kẻ tấn công theo địa chỉ chỉ định trước hoặc sao chép trực tiếp.
- Người quản lý có thể cài đặt Keylogger vào máy tính của nhân viên để theo dõi hoạt động của nhân viên;

3.2 Các công cụ hỗ trợ tấn công

- Cài đặt Keyloggers:
  - Bằng phần cứng: thường được cài như 1 khớp nối kéo dài giữa máy tính và dây bàn phím;
  - Bằng phần mềm: kẻ tấn công có thể tích hợp công cụ Keylogger vào một phần mềm thông thường và lừa người dùng cài đặt vào máy tính của mình.

3.3 Các dạng tấn công phá hoại thường gặp

- Tấn công vào mật khẩu
- Tấn công bằng mã độc
- Tấn công từ chối dịch vụ
- Tấn công giả mạo địa chỉ
- Tấn công nghe trộm
- Tấn công kiểu người đứng giữa
- Tấn công bằng bom thư và thư rác
- Tấn công sử dụng cửa hậu
- Tấn công kiểu Social Engineering
- Tấn công phishing, pharming

3.3 Các dạng tấn công - Tấn công vào mật khẩu

- Tấn công vào mật khẩu là dạng tấn công nhằm đánh cắp mật khẩu và thông tin tài khoản để lạm dụng;
  - Tên người dùng và mật khẩu không được mã hóa có thể bị đánh cắp trên đường truyền từ máy khách đến máy chủ;
  - Tên người dùng và mật khẩu có thể bị đánh cắp thông qua các dạng tấn công XSS hoặc Social Engineering (lừa đảo, bẫy người dùng cung cấp thông tin);
  - Nếu kẻ tấn công có tên người dùng và mật khẩu → có thể đăng nhập vào tài khoản và thực hiện các thao tác như người dùng bình thường.

3.3 Các dạng tấn công - Tấn công vào mật khẩu

❖ Các dạng tấn công vào mật khẩu:

- Tấn công dựa trên từ điển (Dictionary attacks): người dùng có xu hướng chọn mật khẩu là các từ đơn giản có trong từ điển cho dễ nhớ → kẻ tấn công thử các từ có tần suất sử dụng cao làm mật khẩu trong từ điển.
- Tấn công vét cạn (Brute force attacks): sử dụng tổ hợp các ký tự và thử tự động.
  - Phương pháp này thường sử dụng với các mật khẩu đã được mã hóa;
  - Kẻ tấn công sử dụng tổ hợp ký tự, sau đó mã hóa với cùng thuật toán hệ thống sử dụng, và so sánh chuỗi mã hóa với chuỗi mà mật khẩu thu thập được. Nếu hai bản mã trùng nhau → tổ hợp ký tự là mật khẩu.

3.3 Các dạng tấn công - Tấn công vào mật khẩu

- Phòng chống:
  - Chọn mật khẩu đủ mạnh: độ dài >= 8 ký tự gồm chữ cái hoa, thường, chữ số và ký tự đặc biệt (?#$...):
    - VD: Mật khẩu “Abc123$5” an toàn về mặt tính toán hơn “abc12345”.
  - Định kỳ thay đổi mật khẩu.
- Một số công cụ khôi phục mật khẩu:
  - Password Cracker (http://www.softpedia.com)
  - Ophcrack
  - Offline NT Password & Registry Editor
  - PC Login Now
  - L0phtCrack
  - John the Ripper

3.3 Các dạng tấn công - Tấn công bằng mã độc

- Tấn công bằng mã độc có thể gồm một số dạng:
  - Lợi dụng các lỗ hổng về lập trình, lỗ hổng cấu hình hệ thống để chèn và thực hiện mã độc trên hệ thống nạn nhân;
    - Tấn công lợi dụng lỗi tràn bộ đệm (Buffer Overflow) – đã học ở chương 2
    - Tấn công lợi dụng lỗi không kiểm tra đầu vào:
      - Tấn công chèn mã SQL (SQL Injection) – một phần đã học ở chương 2
      - Tấn công script kiểu XSS, CSRF
  - Lừa người sử dụng tải, cài đặt và thực hiện các phần mềm độc hại
    - Các phần mềm Adware, Spyware
    - Virus
    - Trojan

3.3 Các dạng tấn công - Tấn công bằng mã độc: Tấn công lợi dụng lỗi không kiểm tra đầu vào

- Các dữ liệu đầu vào (input data) cần được kiểm tra để đảm bảo đạt các yêu cầu về định dạng và kích thước;
- Các dạng dữ liệu nhập điển hình cần kiểm tra:
  - Các trường dữ liệu text
  - Các lệnh được truyền qua URL để kích hoạt chương trình
  - Các file âm thanh, hình ảnh, hoặc đồ họa do người dùng hoặc các tiến trình khác cung cấp
  - Các đối số đầu vào trong dòng lệnh
  - Các dữ liệu từ mạng hoặc các nguồn không tin cậy
- Kẻ tấn công có thể kiểm tra các dữ liệu đầu vào và thử tất cả các khả năng để khai thác.

3.3 Các dạng tấn công - Tấn công bằng mã độc: Tấn công lợi dụng lỗi không kiểm tra đầu vào

- Một số dạng tấn công lợi dụng lỗi không kiểm tra đầu vào:
  - Cố tình nhập dữ liệu quá lớn hoặc sai định dạng gây lỗi cho ứng dụng (đã học ở chương 2)
    - Gây lỗi ứng dụng/dịch vụ, có thể làm ứng dụng ngừng hoạt động
  - Chèn mã SQL để thực hiện trên máy chủ CSDL của ứng dụng (SQL Injection)

3.3 Các dạng tấn công - Tấn công bằng mã độc: Lợi dụng lỗi không kiểm tra đầu vào - SQL Injection

- SQL Injection (chèn mã độc SQL) là một kỹ thuật cho phép kẻ tấn công chèn mã SQL vào dữ liệu gửi đến máy chủ và được thực hiện trên máy chủ CSDL;
- Nguyên nhân:
  - Dữ liệu đầu vào từ người dùng hoặc từ các nguồn khác không được kiểm tra hoặc kiểm tra không kỹ lưỡng.
  - Ứng dụng sử dụng các câu lệnh SQL động, trong đó dữ liệu được kết nối với mã SQL gốc để tạo ra câu lệnh SQL hoàn chỉnh
- Tùy mức độ tinh vi, SQL Injection có thể cho phép kẻ tấn công:
  - Vượt qua các khâu xác thực người dùng;
  - Chèn, xóa hoặc sửa đổi dữ liệu;
  - Đánh cắp các thông tin trong CSDL;
  - Chiếm quyền điều khiển hệ thống;

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Vượt qua các khâu xác thực người dùng

❖ Ví dụ: form HTML đăng nhập:

```
<form method="post" action="/test_sql.asp">
        Tên đăng nhập: <input type=text name="username"><br \>
        Mật khẩu: <input type=password name="passwd"><br \>
        <input type=submit name="login" value="Log In">
</form>
```

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Vượt qua các khâu xác thực người dùng

```
<%
' Mã xử lý bằng asp xử lý đăng nhập trong file test_sql.asp:
' g.thiết đã k.nối với CSDL SQL qua đối tượng conn và bảng tbl_accounts lưu t.tin người dùng
Dim username, passwd, sqlString, rsLogin
' lấy dữ liệu từ form
username = Request.Form("username")
passwd = Request.Form("passwd")
' tạo và thực hiện câu truy vấn sql
sqlString = "SELECT * FROM tbl_accounts WHERE username='" &username&"' AND passwd='"
&passwd& "'"
set rsLogin = conn.execute(sqlString)
if (NOT rsLogin.eof()) then
        ' cho phép đăng nhập, bắt đầu phiên làm việc
else
        ' từ chối đăng nhập, báo lỗi
end if
%>
```

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Vượt qua các khâu xác thực người dùng

❖ Phân tích:

- Nếu người dùng nhập admin vào trường username và abc123 vào trường passwd của form, mã xử lý hoạt động đúng:
  - Nếu tồn tại người dùng với username và password sẽ cho phép đăng nhập;
  - Nếu không tồn tại người dùng với username và password sẽ từ chối đăng nhập và báo lỗi.
- Nếu người dùng nhập *aaaa' OR 1=1--* vào trường username và một chuỗi bất kỳ vào trường passwd của form, mã xử lý hoạt động sai:
  - Chuỗi chứa câu truy vấn SQL trở thành:

SELECT * FROM tbl_accounts WHERE username='*aaaa' OR 1=1--*' AND passwd='aaaa'

Câu truy vấn sẽ trả về mọi bản ghi trong bảng do mệnh đề OR 1=1 luôn đúng và phần kiểm tra mật khẩu đã bị loại bỏ bởi ký hiệu (--): phần lệnh sau ký hiệu (--) được coi là ghi chú và không được thực hiện.

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Sửa đổi, hoặc xóa dữ liệu

❖ Ví dụ: form HTML tìm kiếm sản phẩm:

```
<form method="post" action="/test_sql.asp">
  Nhập tên sản phẩm: <input type=text name="keyword">
  <input type=submit name="search" value="Search">
</form>
```

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Sửa đổi, hoặc xóa dữ liệu

Mã asp xử lý tìm kiếm trong file test_sql.asp:

```
<%
' giả thiết đã kết nối với CSDL SQL server qua connection conn
' và bảng tbl_products lưu thông tin sản phẩm
Dim keyword, sqlString, rsSearch
' lấy dữ liệu từ form
keyword = Request.Form(" keyword")
' tạo và thực hiện câu truy vấn sql
sqlString = "SELECT * FROM tbl_products WHERE product_name like '%" & keyword & "%'"
set rsSearch = conn.execute(sqlString)
if (NOT rsSearch.eof()) then
        ' hiển thị danh sách các sản phẩm
else
       ' thông báo không tìm thấy sản phẩm
end if
%>
```

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Sửa đổi, hoặc xóa dữ liệu

❖ Phân tích:

- Nếu người dùng nhập Samsung Galaxy S4 vào trường keyword của form, mã xử lý hoạt động đúng:
  - Nếu tìm thấy → hiển thị kết quả tìm kiếm;
  - Nếu không tìm thấy → thông báo không tìm thấy sản phẩm.
- Nếu người dùng nhập Samsung Galaxy S4';DELETE FROM tbl_products;-- vào trường keyword của form, mã xử lý hoạt động sai:
  - Chuỗi chứa câu truy vấn SQL trở thành:

SELECT * FROM tbl_products WHERE keyword like '%Samsung Galaxy S4';DELETE FROM tbl_products;--%'

Câu truy vấn mới gồm 2 lệnh SQL: câu lệnh tìm kiếm sản phẩm Samsung Galaxy S4 và câu lệnh xóa tất cả các sản phẩm trong bảng tbl_products. Sở dĩ kẻ tấn công có thể làm được điều này do SQL server cho phép chạy nhiều lệnh SQL và dùng dấu ; để ngăn cách các lệnh. Ký hiệu – dùng để hủy tác dụng của phần lệnh còn lại nếu có.

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Sửa đổi, hoặc xóa dữ liệu

❖ Phân tích:

- Bằng thủ thuật tương tự, kẻ tấn công có thể thay lệnh DELETE bằng lệnh UPDATE hoặc INSERT để xóa hoặc chèn dữ liệu.
- Cập nhật mật khẩu của người quản trị:

```
Galaxy S4';UPDATE tbl_administrators SET password=abc123
WHERE username = 'admin';--
```

- Chèn thêm bản ghi:

```
Galaxy S4';INSERT INTO tbl_administrators (username, password)
VALUES ('attacker', 'abc12345');--
```

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Đánh cắp các thông tin trong CSDL

Lỗ hổng chèn mã SQL có thể giúp kẻ tấn công đánh cắp dữ liệu trong cơ sở dữ liệu thông qua một số bước như sau:

- Tìm lỗ hổng chèn mã SQL và thăm dò các thông tin về hệ quản trị cơ sở dữ liệu:
  - Nhập một số dữ liệu mẫu để kiểm tra một trang web có chứa lỗ hổng chèn mã SQL, như các dấu nháy đơn, dấu --,…
  - Tìm phiên bản máy chủ cơ sở dữ liệu: nhập các câu lệnh lỗi và kiểm tra thông báo lỗi, hoặc sử dụng @@version (với MS-SQL Server), hoặc version() (với MySQL) trong câu lệnh ghép với UNION SELECT

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Đánh cắp các thông tin trong CSDL

- Tìm thông tin về số lượng và kiểu dữ liệu các trường của câu truy vấn hiện tại của trang web.
  - Sử dụng mệnh đề ORDER BY <số thứ tự của trường>
  - Sử dụng UNION SELECT 1, 2, 3, …
- Trích xuất thông tin về các bảng, các trường của cơ sở dữ liệu thông qua các bảng hệ thống (metadata).
- Sử dụng lệnh UNION SELECT để ghép các thông tin định trích xuất vào câu truy vấn hiện tại của ứng dụng

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Chiếm quyền điều khiển hệ thống

- Khả năng máy chủ cơ sở dữ liệu bị chiếm quyền điều khiển xảy ra khi website và CSDL của nó tồn tại 2 lỗ hổng:
  - Lỗ hổng cho phép tấn công chèn mã SQL;
  - Lỗ hổng thiết lập quyền truy nhập – sử dụng người dùng có quyền quản trị để truy nhập và thao tác dữ liệu website.

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Chiếm quyền điều khiển hệ thống

- Tin tặc có thể chèn mã để chạy các thủ tục hệ thống cho phép can thiệp vào hệ quản trị CSDL và hệ điều hành. Ví dụ, MS SQL cung cấp các thủ tục hệ mở rộng:
  - sp_send_dbmail: cho phép gửi email từ CSDL.
  - xp_cmdshell: cho phép chạy các lệnh và chương trình cài đặt trên HĐH windows. VD:
    - EXEC xp_cmdshell 'dir *.exe‘
    - EXEC xp_cmdshell 'shutdown /s /t 00' → tắt máy chủ chạy CSDL
    - EXEC xp_cmdshell 'net stop W3SVC' → dừng hoạt động máy chủ web
    - EXEC xp_cmdshell 'net stop MSSQLSERVER' → dừng hoạt động máy chủ CSDL

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Chiếm quyền điều khiển hệ thống

- Ngoài ra, tin tặc có thể thực hiện các thao tác nguy hiểm đến CSDL nếu có quyền của người quản trị CSDL hoặc quản trị hệ thống, như:
  - Xóa cả bảng: DROP TABLE <tên bảng>
  - Xóa cả CSDL: DROP DATABASE <tên CSDL>
  - Tạo 1 tài khoản mới: sp_addlogin <username> <password>
  - Đổi mật khẩu của người dùng hiện tại: sp_password <password>

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Phòng chống

- Các biện pháp phòng chống dựa trên kiểm tra và lọc dữ liệu đầu vào:
  - Kiểm tra tất cả các dữ liệu đầu vào, đặc biệt dữ liệu nhập từ người dùng và từ các nguồn không tin cậy;
  - Kiểm tra định dạng và kích thước dữ liệu đầu vào;
  - Tạo các bộ lọc để lọc bỏ các ký tự đặc biệt và các từ khóa của các ngôn ngữ trong các trường hợp cần thiết mà kẻ tấn công có thể sử dụng:
    - Các ký tự đặc biệt: *, ‘, =, --
    - Các từ khóa: SELECT, INSERT, UPDATE, DELETE, DROP,....

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Phòng chống

- Các biện pháp phòng chống dựa trên việc sử dụng thủ tục (stored procedures) trong CSDL:
  - Đưa tất cả các câu truy vấn (SELECT) và cập nhật, sửa xóa dữ liệu (INSERT, UPDATE, DELETE) vào thủ tục; dữ liệu truyền vào thủ tục thông qua các tham số → tách dữ liệu khỏi mã, giúp hạn ngăn chặn hiệu quả tấn công chèn mã SQL.
  - Hạn chế thực hiện các câu lệnh SQL động trong thủ tục.
- Cấm hoặc vô hiệu hóa (disable) việc thực hiện các thủ tục hệ thống – các thủ tục CSDL có sẵn cho phép can thiệp vào hệ quản trị CSDL và hệ điều hành nền.
  - Các Extended/system Stored Procedures trong MS-SQL như xp_cmdshell cho phép chạy lệnh của hệ điều hành.

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Phòng chống

- Các biện pháp phòng chống dựa trên thiết lập quyền truy nhập người dùng cho phù hợp:
  - Không sử dụng người dùng có quyền system admin hoặc database owner làm người dùng truy cập dữ liệu;
    - Ví dụ: không dùng user sa (MS-SQL) hoặc root (MySQL) làm user truy cập dữ liệu. Chỉ dùng các user này cho mục đích quản trị.
  - Chia nhóm người dùng, chỉ cấp quyền vừa đủ để truy cập các bảng biểu, thực hiện câu truy vấn và chạy các thủ tục.
  - Tốt nhất, không cấp quyền thực hiện các câu truy vấn, cập nhật, sửa, xóa trực tiếp dữ liệu; Thủ tục hóa tất cả các câu lệnh và chỉ cấp quyền thực hiện thủ tục.

2.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Công cụ kiểm tra và tấn công

- Sử dụng các công cụ rà quét để chủ động tìm lỗi SQL injection tồn tại trong hệ thống;
- SQLmap (có thể tải từ trang sqlmap.org) là một công cụ mã mở miễn phí viết bằng Python:
  - Cho phép kiểm tra website tìm lỗi chèn mã SQL
  - Cho phép khai thác lỗi để điều khiển máy chủ CSDL
  - Hỗ trợ hầu hết các máy chủ quản trị CSDL hiện nay: MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase và SAP MaxDB.

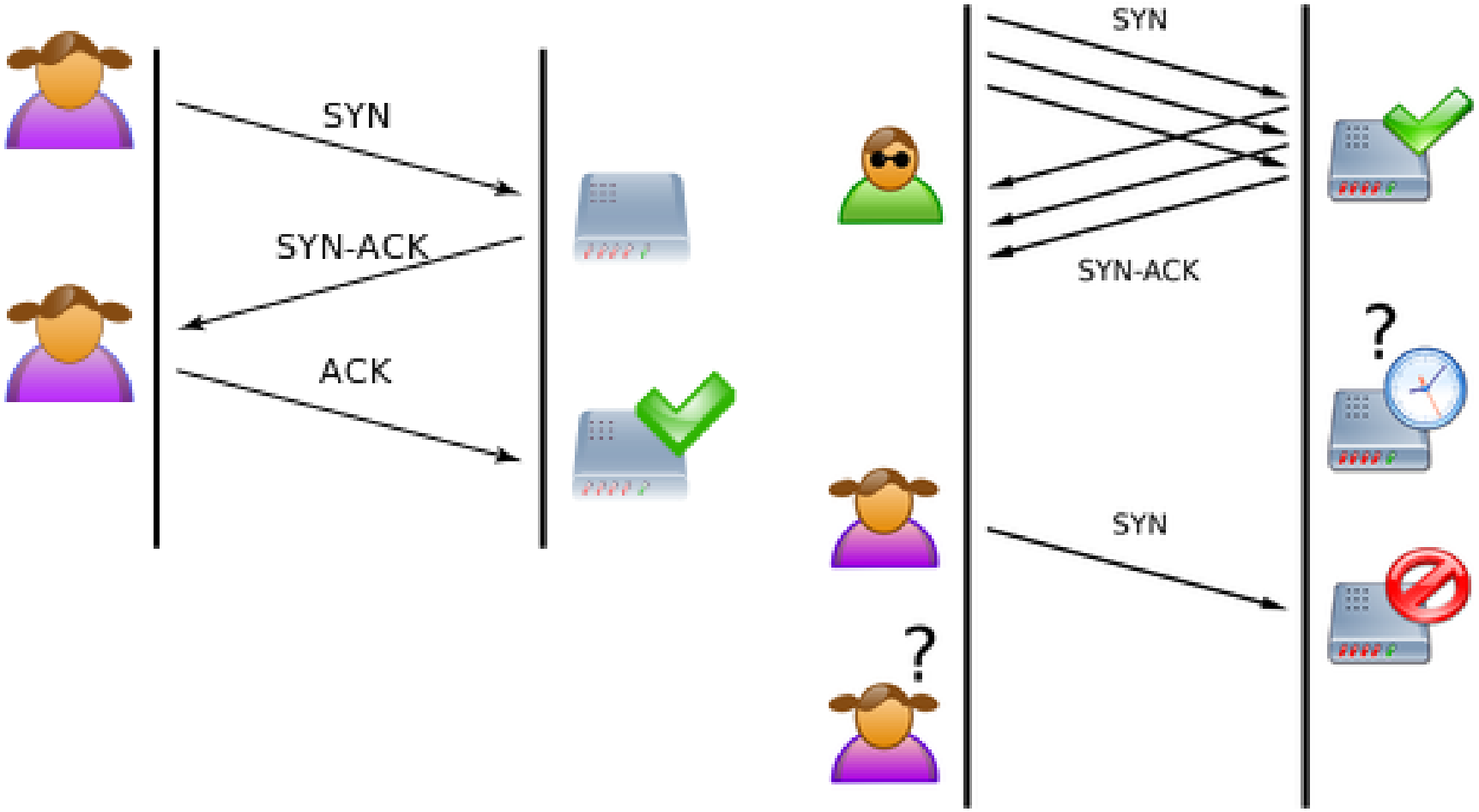
3.3 Các dạng tấn công - Tấn công từ chối dịch vụ

- Tấn công từ chối dịch vụ (DoS - Denial of Service Attacks) là dạng tấn công cản trở người dùng hợp pháp truy nhập các tài nguyên hệ thống;
- Hai loại tấn công DoS:
  - Tấn công logic (Logic attacks): tấn công dựa vào các lỗi phần mềm làm dịch vụ ngừng hoạt động hoặc làm giảm hiệu năng hệ thống.
    - Cần cài đặt các bản cập nhật thường xuyên để phòng chống.
  - Tấn công gây ngập lụt (Flooding attacks): Kẻ tấn công gửi một lượng lớn yêu cầu gây cạn kiệt tài nguyên hệ thống hoặc băng thông đường truyền mạng.
- Hai kỹ thuật tấn công gây ngập lụt:
  - SYN floods
  - Smurf

3.3 Các dạng tấn công - Tấn công DoS - SYN floods

- SYN floods là kỹ thuật gây ngập lụt các gói tin TCP.
  - SYN là bít điều khiển của TCP dùng để đồng bộ số trình tự gói.
- Kịch bản tấn công SYN floods:
  - Kẻ tấn công gửi 1 lượng lớn gói tin yêu cầu mở kết nối (SYN-REQ) đến máy tính nạn nhân;
  - Máy tính nạn nhân ghi nhận yêu cầu kết nối và dành 1 chỗ trong bảng lưu kết nối trong bộ nhớ cho mỗi yêu cầu kết nối;
  - Máy tính nạn nhân sau đó gửi gói tin xác nhận kết nối (SYN-ACK) đến kẻ tấn công;
  - Do kẻ tấn công không bao giờ trả lời xác nhận kết nối, nên máy tính nạn nhân vẫn phải lưu tất cả các yêu cầu kết nối chưa được xác nhận trong bảng kết nối → bảng kết nối đầy và người dùng hợp pháp không thể truy nhập;
  - Máy tính nạn nhân chỉ có thể xóa yêu cầu kết nối khi nó timed-out.

3.3 Các dạng tấn công - Tấn công DoS - SYN floods



3.3 Các dạng tấn công - Tấn công DoS - SYN floods

❖ Phân tích:

- Kẻ tấn công thường dùng địa chỉ IP giả mạo hoặc địa chỉ không có thực làm Source IP trong gói tin IP nên, thông điệp SYN-ACK của máy tính nạn nhân không bao giờ đến đích;
- Kẻ tấn công cố tình tạo một lượng rất lớn yêu cầu kết nối dở dang để:
  - Các yêu cầu kết nối SYN-REQ điền đầy bảng kết nối → máy nạn nhân không thể chấp nhận yêu cầu của những người dùng khác;
  - Làm cạn kiệt tài nguyên bộ nhớ của máy nạn nhân → có thể làm máy nạn nhân ngừng hoạt động;
  - Gây nghẽn đường truyền mạng.

3.3 Các dạng tấn công - Tấn công DoS - SYN floods

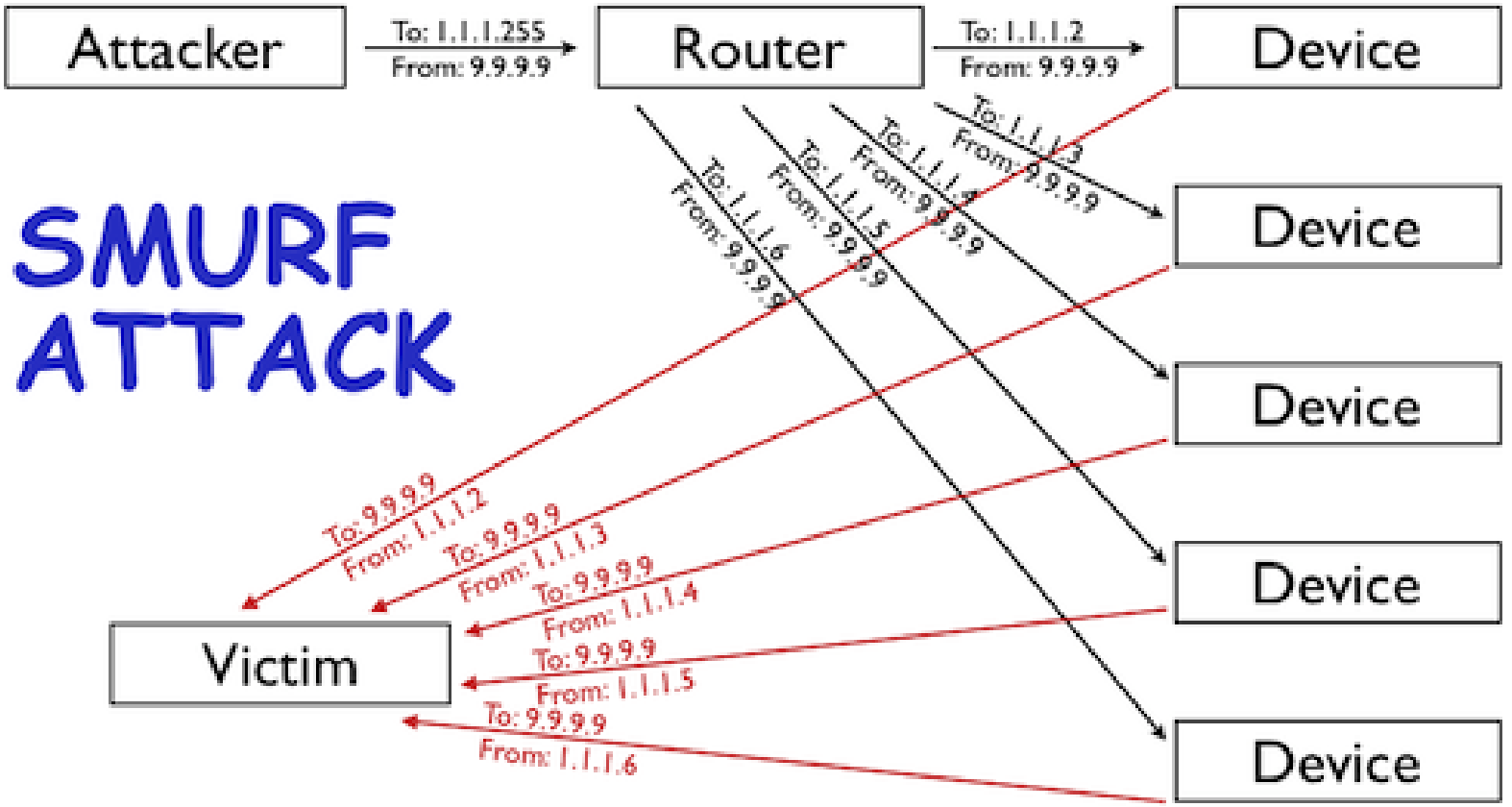
❖ Phòng chống:

- Sử dụng kỹ thuật lọc (Filtering): cần sửa đổi giao thức TCP không cho phép kẻ tấn công giả mạo địa chỉ;
- Tăng kích thước Backlog: tăng kích thước bảng Backlog lưu các yêu cầu → tăng khả năng phục vụ yêu cầu;
- Giảm thời gian chờ (SYN-RECEIVED Timer): các kết nối chưa được xác nhận sẽ bị xóa khi hết thời gian chờ;
- SYN cache: yêu cầu kết nối chỉ được cấp phát không gian nhớ đầy đủ khi nó được xác nhận;
- Sử dụng Firewalls và Proxies
  - Có khả năng nhận dạng các địa chỉ IP nguồn là địa chỉ không có thực;
  - Có khả năng tiếp nhận kết nối, chờ đến khi có xác nhận mới chuyển lại cho máy chủ đích.

3.3 Các dạng tấn công - Tấn công DoS - Smurf

- Tấn công smurf sử dụng kiểu phát quảng bá có định hướng để gây ngập lụt đường truyền mạng của máy nạn nhân.
- Kịch bản tấn công smurf:
  - Kẻ tấn công gửi quảng bá một lượng lớn gói tin ICMP (Ping) với địa chỉ IP nguồn là địa chỉ của máy nạn nhân đến một mạng sử dụng một địa chỉ quảng bá (IP Broadcast address);
  - Các máy khác trong mạng nhận được thông điệp ICMP sẽ gửi trả lời đến máy có địa chỉ nguồn IP (là máy nạn nhân);
    - Nếu lượng máy trong mạng rất lớn → máy nạn nhân sẽ bị ngập lụt đường truyền.

3.3 Các dạng tấn công - Tấn công DoS - Smurf



3.3 Các dạng tấn công - Tấn công DoS - Smurf

❖ Phòng chống:

- Cấu hình các máy và router không trả lời các yêu cầu ICMP hoặc các yêu cầu phát quảng bá;
- Cấu hình các router không chuyển tiếp yêu cầu gửi đến các địa chỉ quảng bá.

3.3 Các dạng tấn công - Tấn công DDoS

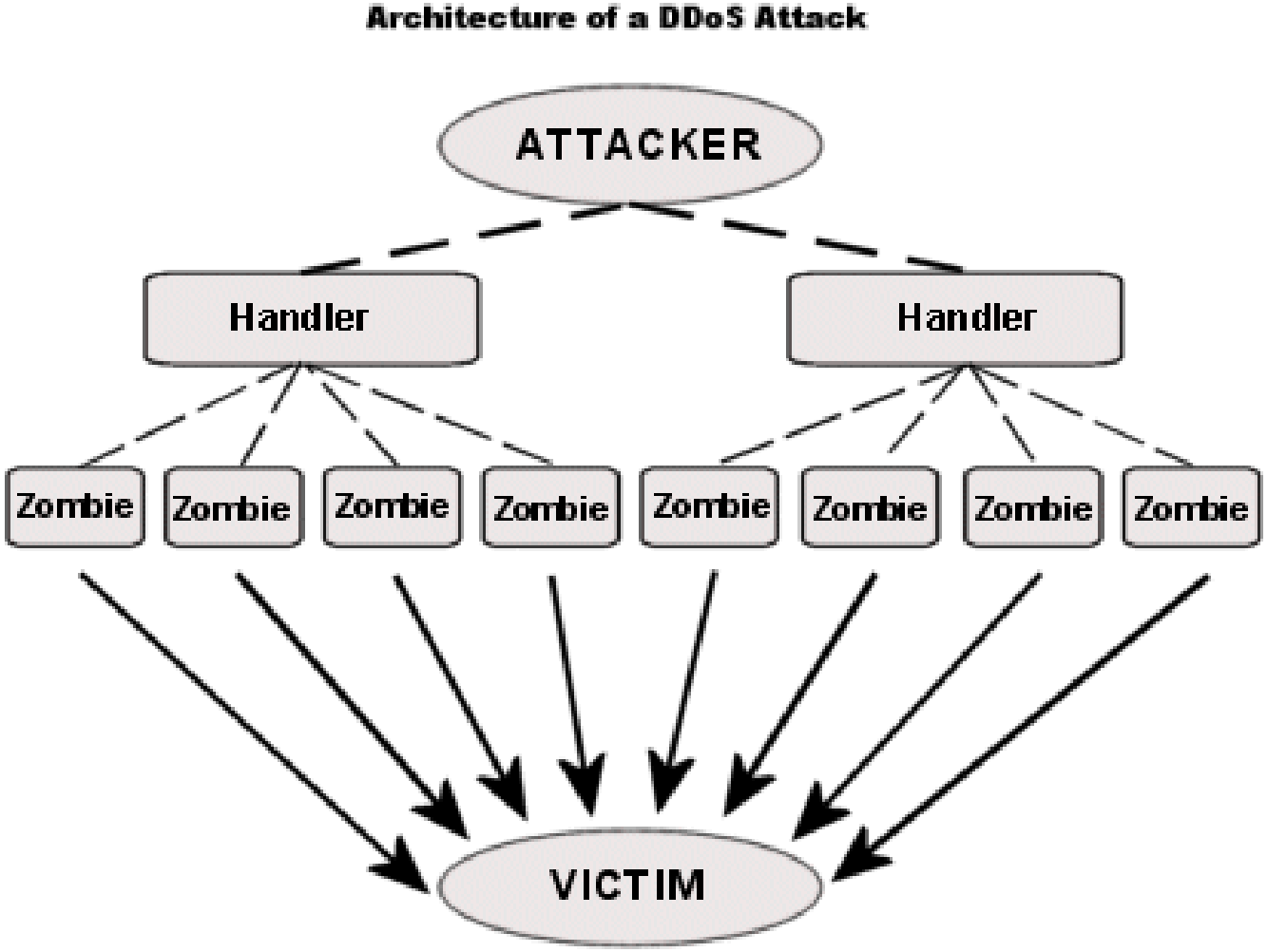
- Tấn công DDoS (Distributed Denial of Service Attacks) là một loại tấn công DoS:
  - Liên quan đến gây ngập lụt các máy nạn nhân với một lượng rất lớn các yêu cầu kết nối giả mạo;
  - DDoS khác DoS ở phạm vi tấn công (số lượng host tham gia)
    - Số host tham gia tấn công DoS thường giới hạn trong 1 hoặc 1 số máy
    - Số host tham gia tấn công DDoS có thể hàng chục ngàn và nằm phân tán trên mạng Internet.

3.3 Các dạng tấn công - Tấn công DDoS

❖ Kịch bản tấn công DDoS:

- Kẻ tấn công chiếm quyền điều khiển hàng trăm thậm chí hàng ngàn máy tính trên mạng Internet, sau đó cài các chương trình tấn công tự động (Automated agents) lên các máy này;
- Sau đó, kẻ tấn công ra lệnh cho các automated agents đồng loạt tạo các yêu cầu giả mạo gửi đến các máy nạn nhân;
- Lượng yêu cầu giả mạo có thể rất lớn và đến từ rất nhiều nguồn khác nhau nên rất khó đối phó và lần vết để tìm ra kẻ tấn công.

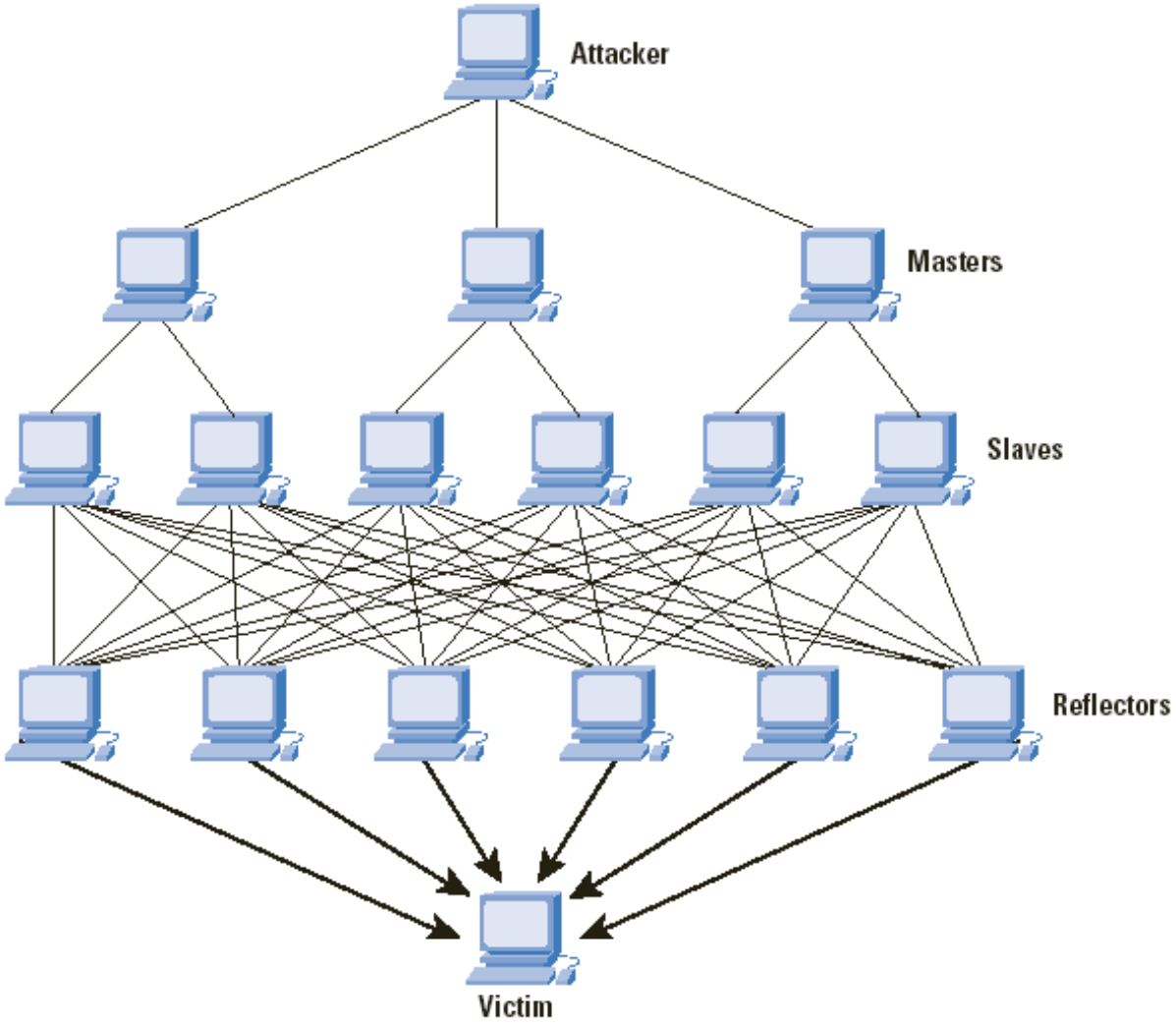
3.3 Các dạng tấn công - Tấn công DDoS



3.3 Các dạng tấn công - Tấn công Reflective DDoS

- Tấn công Reflective DDoS là một loại tấn công DDoS với một số điểm khác biệt:
  - Các máy tính do kẻ tấn công điều khiển (Slaves/Zombies) không trực tiếp tấn công máy nạn nhân;
  - Chúng gửi một lượng lớn yêu cầu giả mạo với địa chỉ nguồn là địa chỉ máy nạn nhân đến một số lớn các máy khác (Reflectors) trên mạng Internet;
  - Các Reflectors gửi Reply đến máy nạn nhân do địa chỉ của máy nạn nhân được đặt vào địa chỉ nguồn của yêu cầu giả mạo;
  - Nếu các Reflectors có số lượng lớn, số Reply sẽ rất lớn và gây ngập lụt máy nạn nhân.
- Tấn công Reflective DDoS khó lần vết và phòng chống hơn tấn công DDoS thông thường do có thể qua nhiều cấp.

3.3 Các dạng tấn công - Tấn công Reflective DDoS

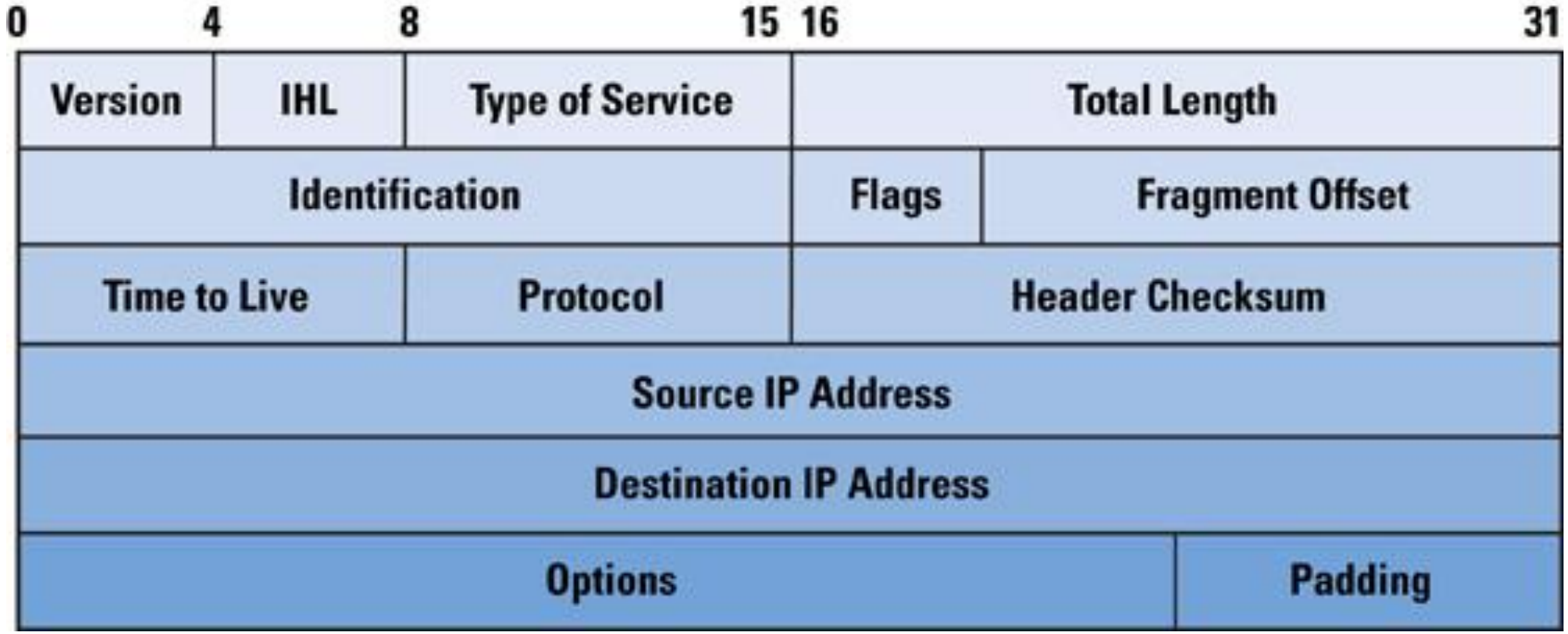


3.3 Các dạng tấn công - Tấn công giả mạo địa chỉ

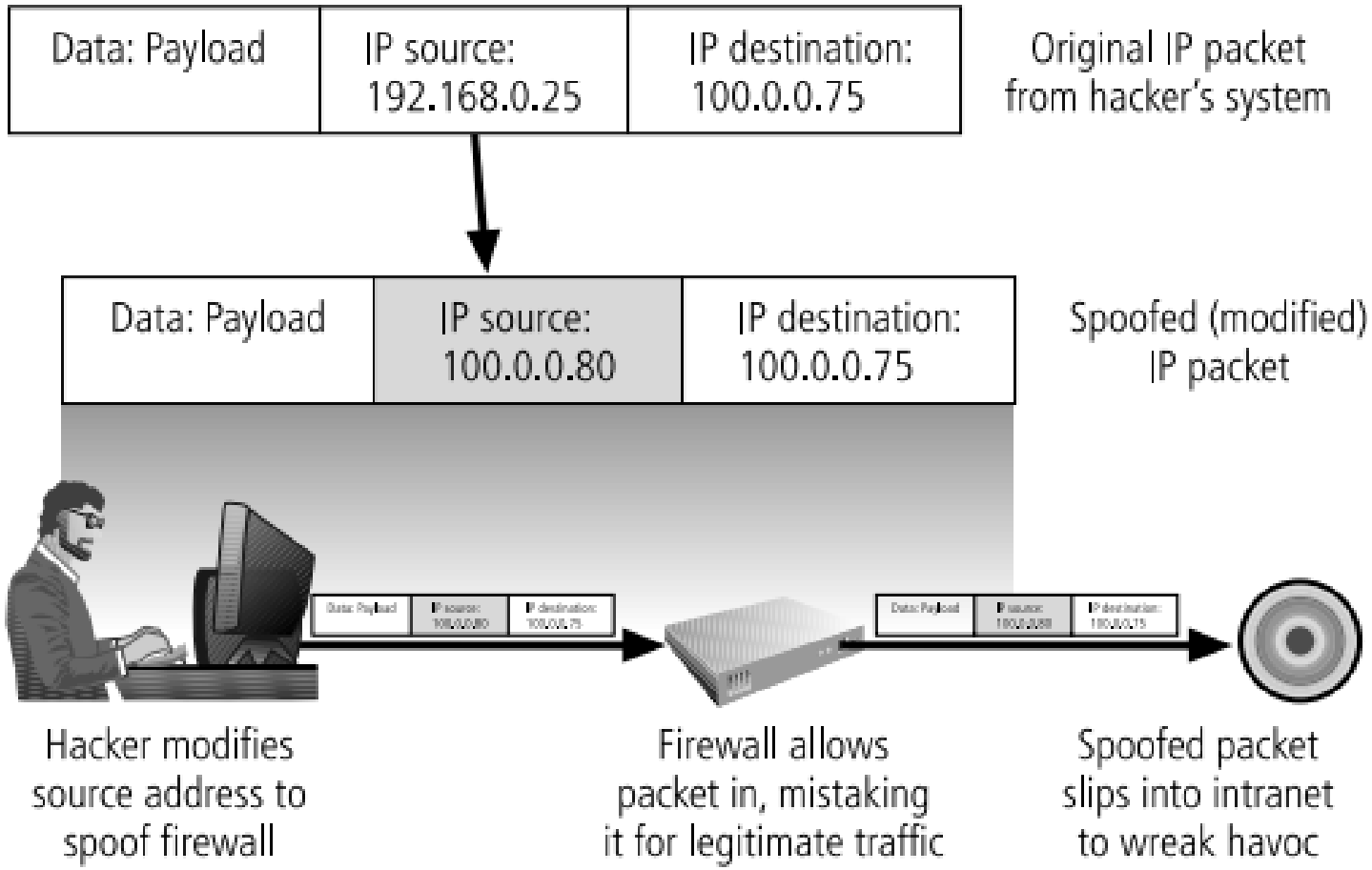
❖ Tấn công giả mạo địa chỉ IP (IP Spoofing) :

- Là dạng tấn công trong đó kẻ tấn công sử dụng địa chỉ IP giả, thường để đánh lừa máy nạn nhân để vượt qua các hàng rào kiểm soát an ninh;
- Nếu kẻ tấn công giả địa chỉ IP là địa chỉ cục bộ của mạng LAN, hắn có thể có nhiều cơ hội đột nhập vào các máy khác trong LAN do chính sách kiểm soát an ninh với các máy trong mạng LAN thường được giảm nhẹ.
- Nếu router hoặc firewall của mạng không được cấu hình để nhận ra IP giả mạo của mạng LAN nội bộ → kẻ tấn công có thể thực hiện.

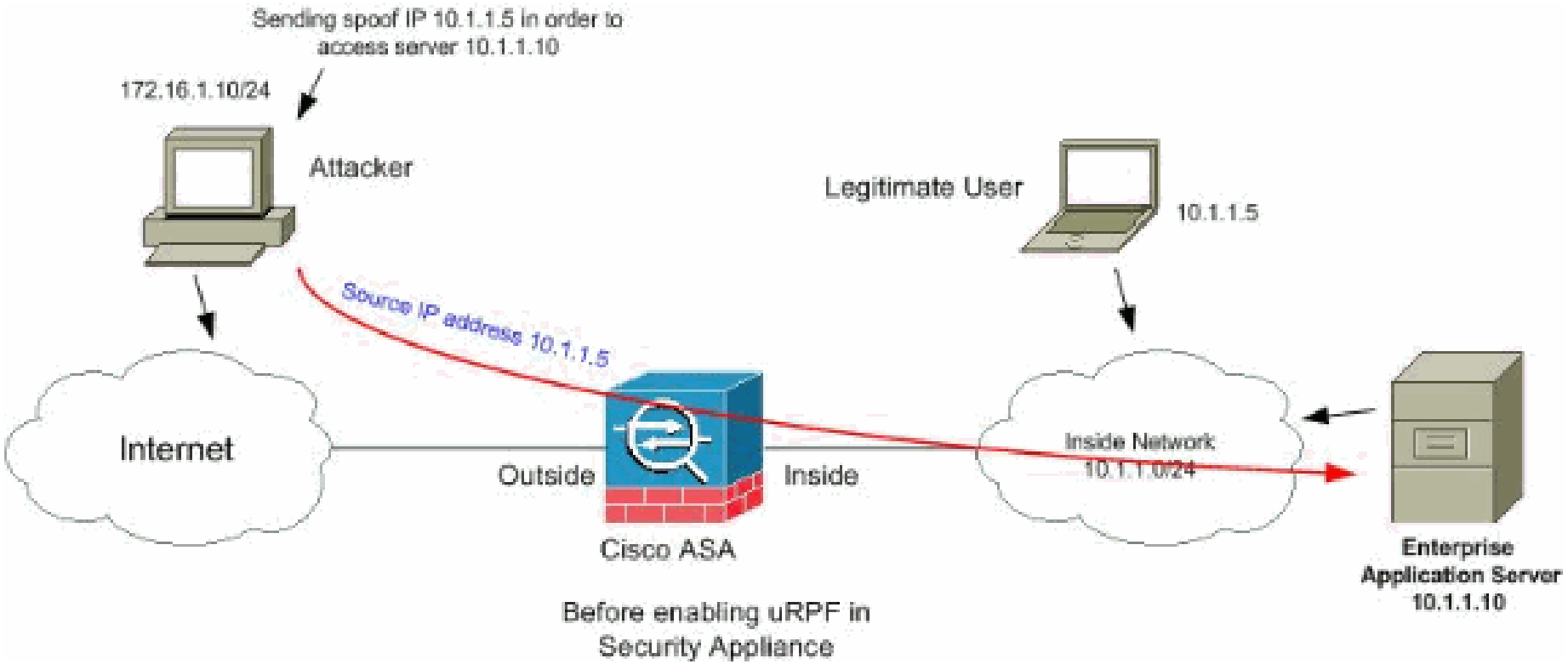
3.3 Các dạng tấn công - Tấn công giả mạo địa chỉ



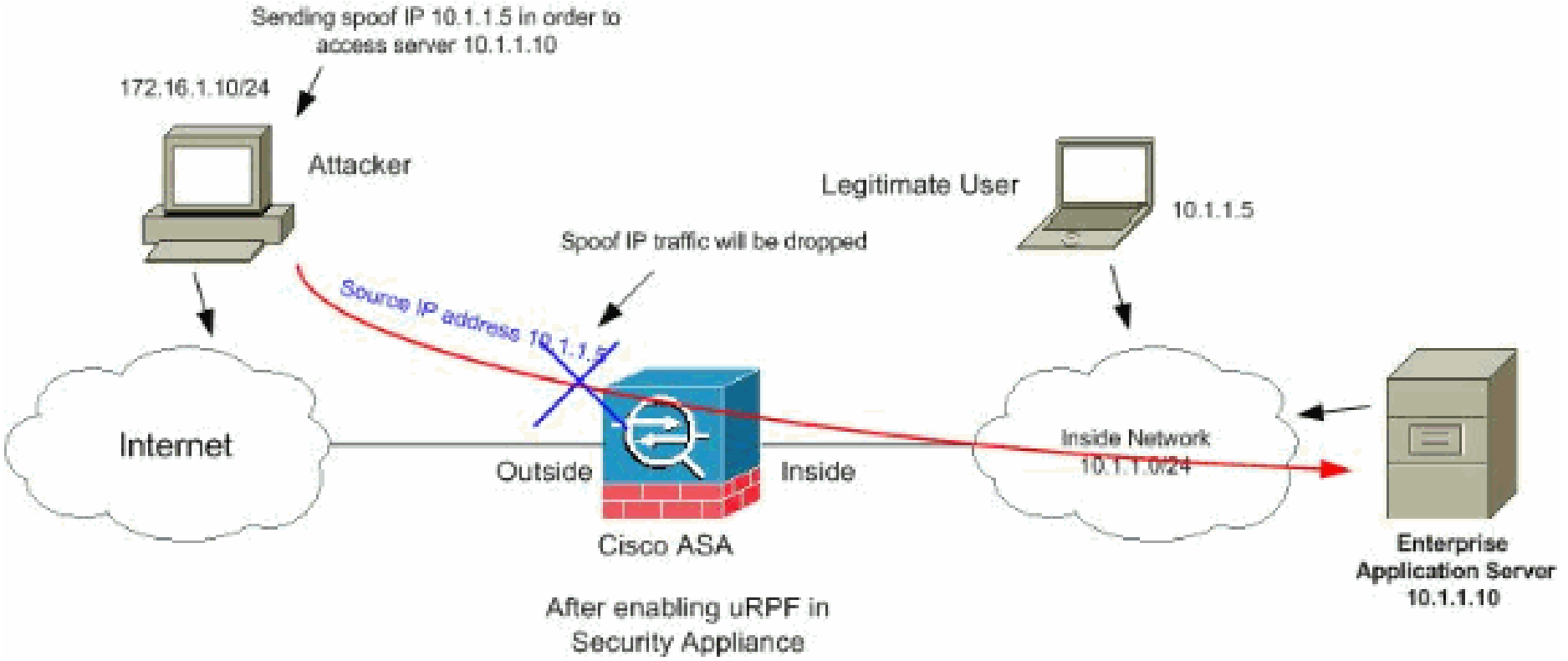
3.3 Các dạng tấn công - Tấn công giả mạo địa chỉ



3.3 Các dạng tấn công - Tấn công giả mạo địa chỉ

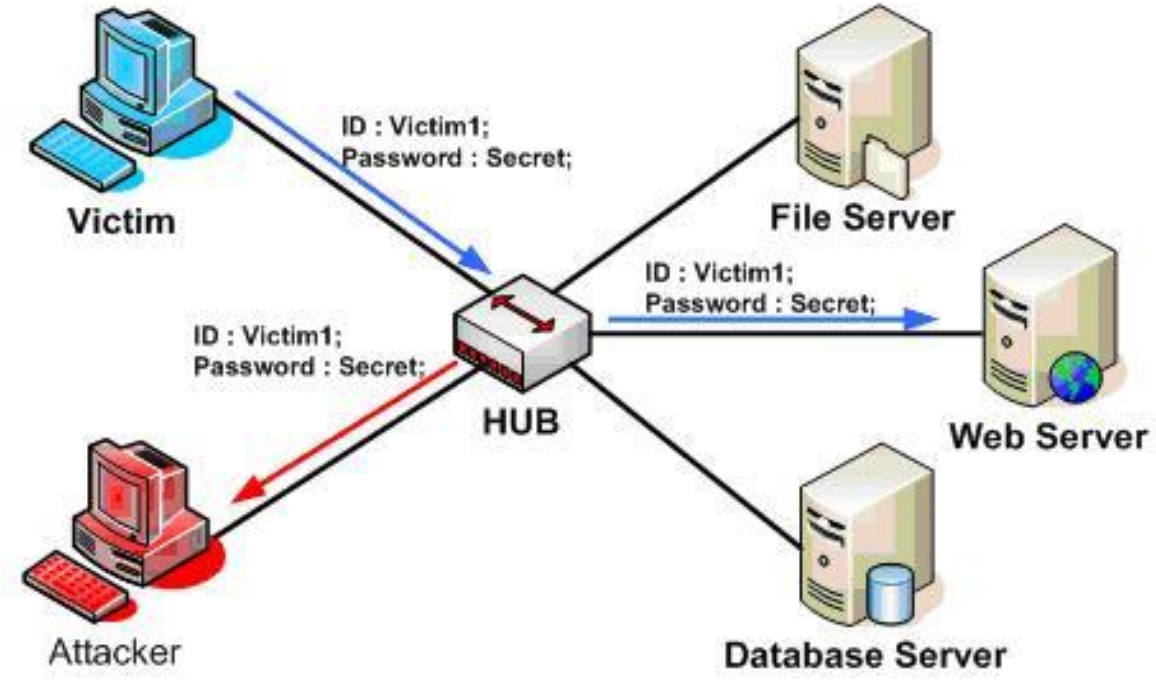


3.3 Các dạng tấn công - Tấn công giả mạo địa chỉ



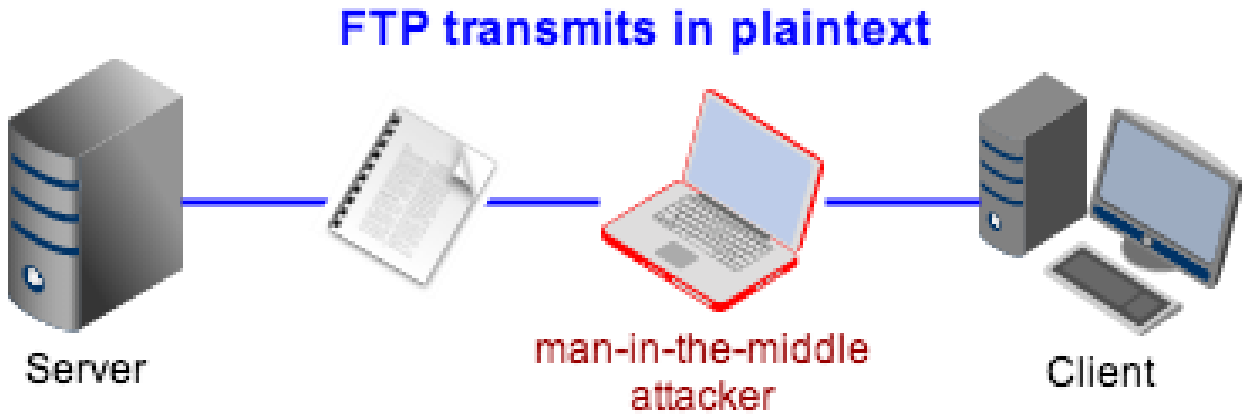
3.3 Các dạng tấn công - Tấn công nghe lén

- Tấn công nghe lén (Sniffing/Eavesdropping) :
  - Là dạng tấn công sử dụng thiết bị phần cứng hoặc phần mềm, lắng nghe trên card mạng, hub hoặc router để bắt các gói tin dùng cho phân tích về sau.

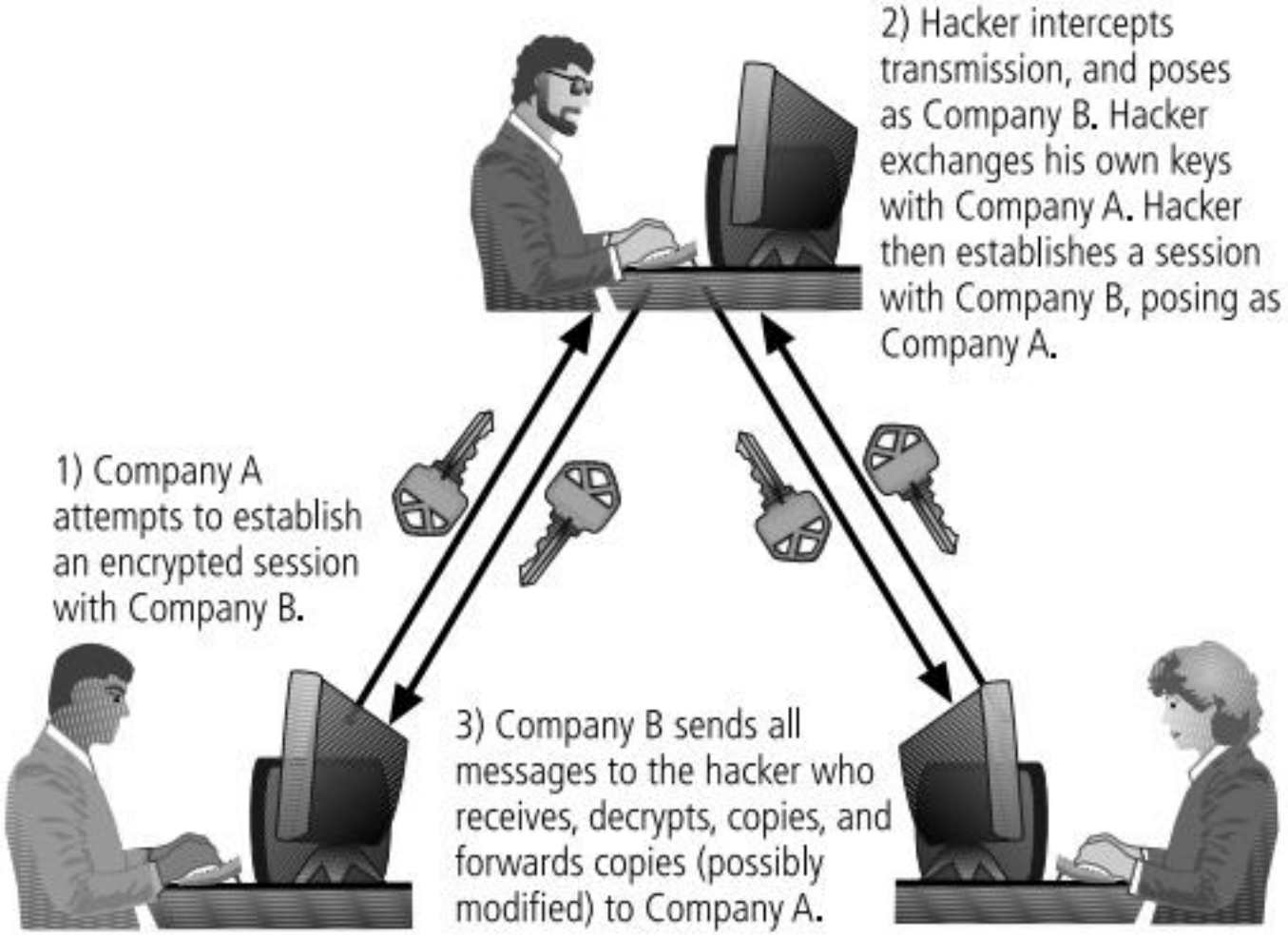


3.3 Các dạng tấn công - Tấn công kiểu người đứng giữa

- Tấn công người đứng giữa (Man in the middle)
  - Lợi dụng quá trình chuyển gói tin đi qua nhiều trạm (hop) thuộc các mạng khác nhau;
  - Kẻ tấn công chặn bắt các thông điệp giữa 2 bên tham gia truyền thông và chuyển thông điệp lại cho bên kia.
  - Thường được sử dụng để đánh cắp thông tin.



3.3 Các dạng tấn công - Tấn công kiểu người đứng giữa



3.3 Các dạng tấn công - Tấn công bằng bom thư và thư rác

❖ Tấn công bằng bom thư và thư rác

- Tấn công bằng bom thư (Mail bombing) là dạng tấn công DoS khi kẻ tấn công chuyển một lượng lớn email đến nạn nhân;
  - Có thể thực hiện được bằng kỹ thuật Social Engineering;
  - Hoặc khai thác lỗi trong hệ thống gửi nhận email SMTP.
  - Kẻ tấn công có thể lợi dụng các máy chủ email không được cấu hình tốt để gửi email cho chúng.
- Tấn công bằng thư rác (Spam emails)
  - Spams là nhưng email không mong muốn, thường là các email quảng cáo;
  - Spams gây lãng phí tài nguyên tính toán và thời gian của người dùng (phải lọc, xóa);
  - Spams cũng có thể dùng để chuyển các phần mềm độc hại.

3.3 Các dạng tấn công - Tấn công kiểu Social Engineering

- Tấn công kiểu Social Engineering là dạng tấn công sử dụng các kỹ thuật xã hội đã thuyết phục người dùng tiết lộ thông tin truy nhập hoặc các thông tin có giá trị cho kẻ tấn công.
  - Kẻ tấn công có thể giả danh làm người có vị trí cao hơn so với nạn nhân để có được sự tin tưởng;
  - Kẻ tấn công có thể mạo nhận là người được ủy quyền của người có thẩm quyền để yêu cầu các nhân viên tiết lộ thông tin về cá nhân/tổ chức.
  - Kẻ tấn công có thể lập trang web giả để đánh lừa người dùng cung cấp các thông tin cá nhân và thông tin tài khoản, thẻ tín dụng,…

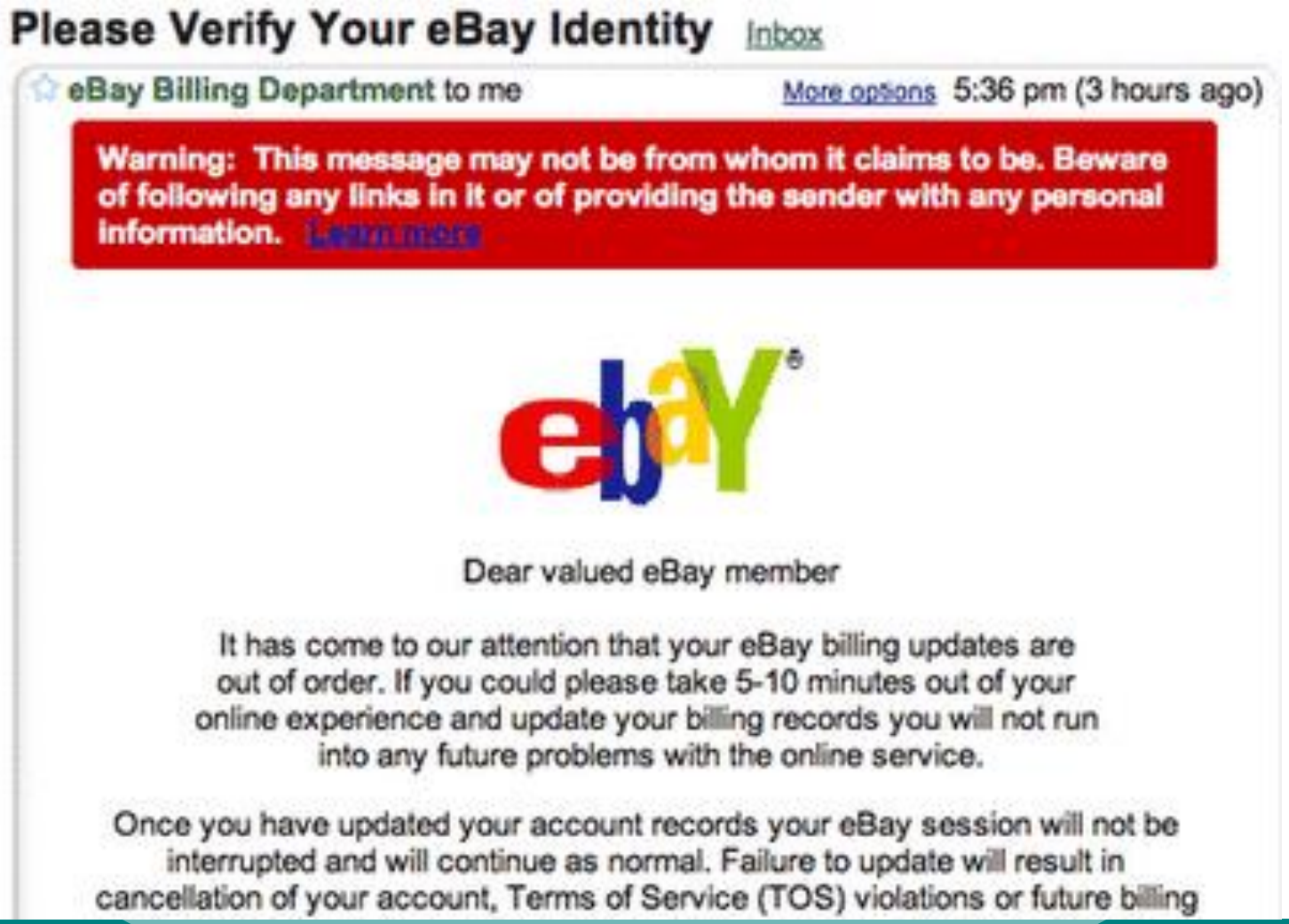
3.3 Các dạng tấn công - Tấn công kiểu Social Engineering

- Trò lừa đảo Nigeria 4-1-9: lợi dụng sự ngây thơ và lòng tham của nhiều người.
  - Kẻ lừa đảo gửi thư tay hoặc email đến nhiều người nhận, mô tả về việc có 1 khoản tiền lớn (thừa kế, lợi tức,..) cần chuyển ra nước ngoài, nhờ người nhận giúp đỡ để hoàn thành giao dịch. Khoản tiền có thể lên đến hàng chục hoặc trăm triệu USD. Kẻ tấn công hứa sẽ trả cho người tham gia một phần số tiền (20-30%);
  - Nếu người nhận có phản hồi và đồng ý tham gia, kẻ tấn công sẽ gửi tiếp thư/email khác, yêu cầu chuyển cho hắn 1 khoản phí giao dịch (từ vài ngàn đến hàng chục ngàn USD);
  - Nếu người nhận gửi tiền cho kẻ tấn công → người đó mất tiền, do giao dịch mà kẻ tấn công hứa là giả mạo.

3.3 Các dạng tấn công - Tấn công kiểu phishing

- Phishing là một dạng của tấn công Social Engineering, lừa người dùng để lấy thông tin cá nhân, thông tin tài khoản, thẻ tín dụng,…
  - Kẻ tấn công có thể giả mạo trang web của các tổ chức tài chính, ngân hàng;
  - Chúng gửi email cho người dùng (địa chỉ email thu thập trên mạng), yêu cầu xác thực thông tin;
  - Nếu người dùng làm theo hướng dẫn → cung cấp các thông tin cá nhân, thông tin tài khoản, thẻ tín dụng cho kẻ tấn công.

3.3 Các dạng tấn công - Tấn công kiểu phishing



Please Verify Your eBay Identity Inbox

eBay Billing Department to me More options 5:36 pm (3 hours ago)

Warning: This message may not be from whom it claims to be. Beware of following any links in it or of providing the sender with any personal information. Learn more

Dear valued eBay member

It has come to our attention that your eBay billing updates are out of order. If you could please take 5-10 minutes out of your online experience and update your billing records you will not run into any future problems with the online service.

Once you have updated your account records your eBay session will not be interrupted and will continue as normal. Failure to update will result in cancellation of your account, Terms of Service (TOS) violations or future billing

3.3 Các dạng tấn công - Tấn công kiểu phishing

From: CustomerSecurity@royalbank.com[1]
Sent: Monday, July 20, 2009 7:54 PM
To: Rob.Smith@hotmail.com
Subject: Renew your Online Account with Royal Bank Immediately – Final reminder[2]

Royal Bank

Dear valued Royal Bank customer,[3]

It has come to our attention that you have not logged into your online banking account for some time[4] now and, as a security measure, we must to suspend your online account.[5] If you would like to continue to use the online banking facilty[6] offered by Royal Bank, please click the link below and renew your security details[7] immediately. Failure to do so will result in your online account being suspended.[8]

Renew your security details immediately and continue to use our online banking facilty:
https://customerbankingrenewal.royalbank.com/[9]

We are sorry for any convenience[10] caused and hope you continue to use our online banking facilty.

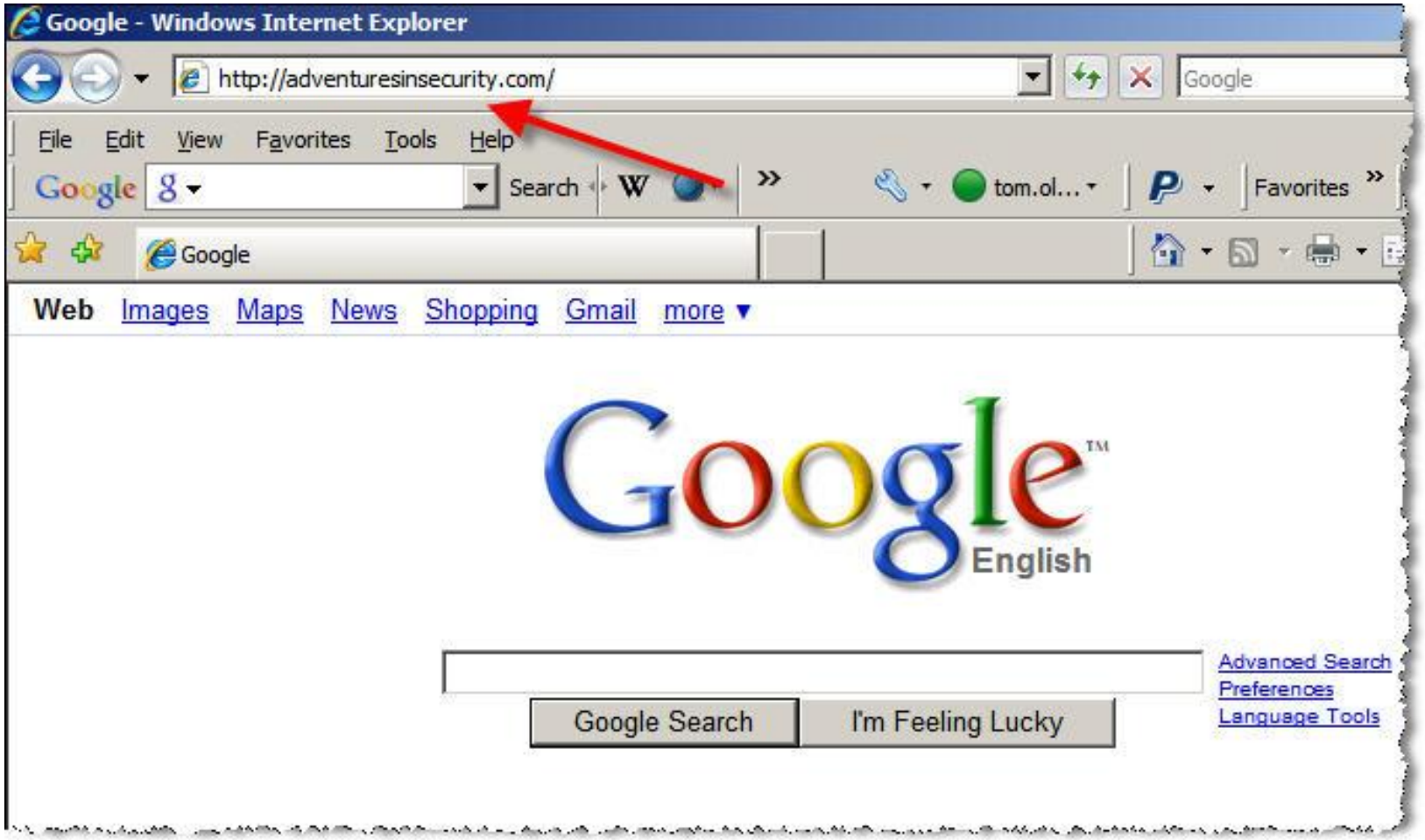
The Royal Bank Online Security Team[11]

Link: http://customerbankingrenewal.royalbank.com/

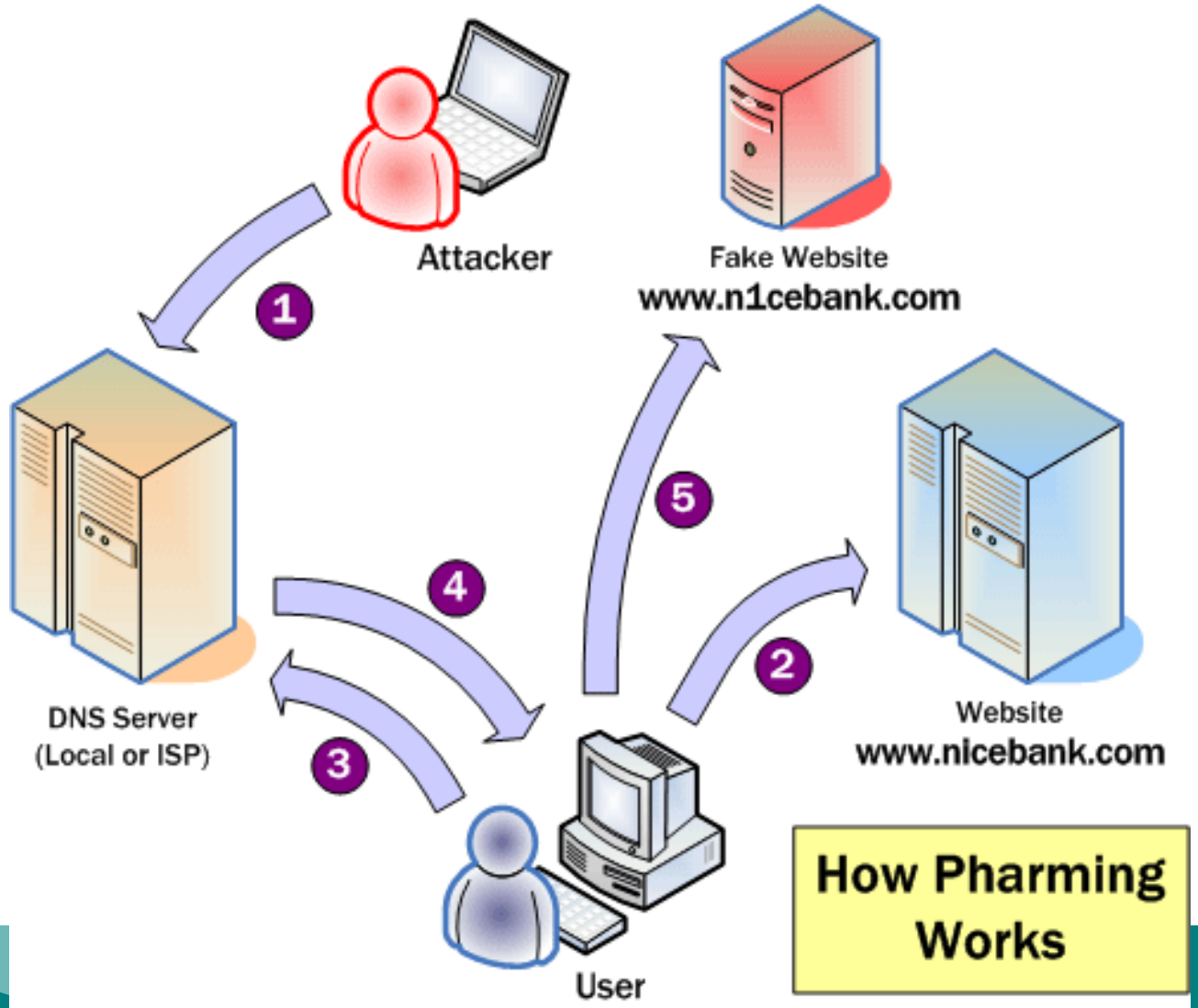
3.3 Các dạng tấn công - Tấn công kiểu pharming

- Pharming là kiểu tấn công vào trình duyệt người dùng:
  - Người dùng gõ địa chỉ 1 website, trình duyệt lại yêu cầu 1 website khác (độc hại);
  - Kẻ tấn công thường sử dụng sâu, virus hoặc các phần mềm độc hại cài vào hệ thống để điều khiển trình duyệt của người dùng;
  - Kẻ tấn công cũng có thể tấn công vào hệ thống DNS để thay đổi kết quả truy vấn: thay địa chỉ IP của website hợp pháp thành IP của website độc hại.

3.3 Các dạng tấn công - Tấn công kiểu pharming



3.3 Các dạng tấn công - Tấn công kiểu pharming



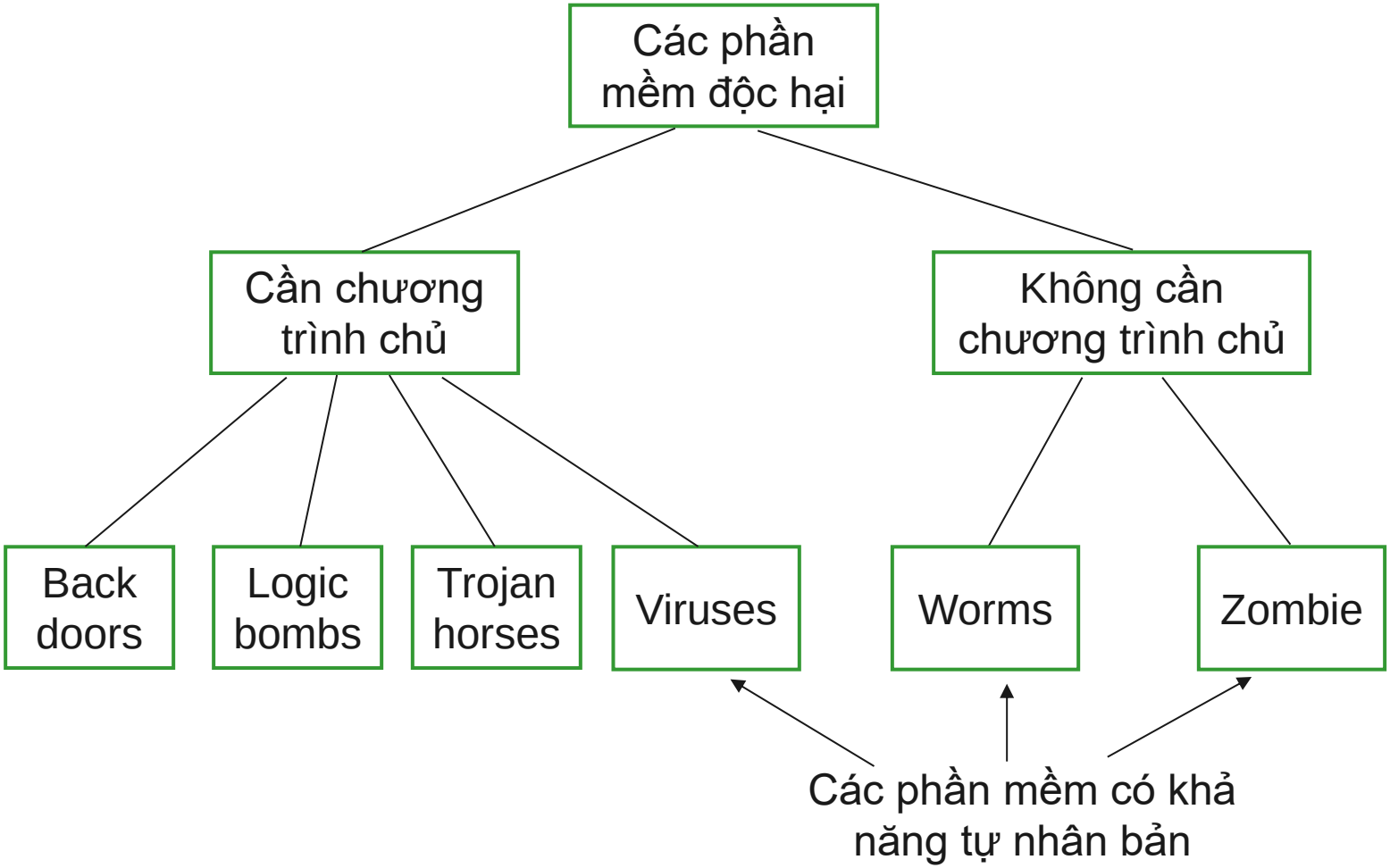
3.3 Các dạng tấn công - Tấn công APT

- Tấn công APT (Advanced Persistent Threat), hay còn được gọi là tấn công có chủ đích là hình thức tấn công tập trung, có chủ đích, được thiết kế riêng cho từng mục tiêu, từng đối tượng cụ thể nhằm mục đích tìm kiếm các thông tin giá trị và gửi ra bên ngoài.
- Hai thuộc tính quan trọng của tấn công APT
  - tiên tiến, hay cao cấp (Advanced): các kỹ thuật tiên tiến được sử dụng để tấn công vào hệ thống mục tiêu một cách bài bản.
  - Kiên trì, dai dẳng (Persistent): mục tiêu được xác định rất cụ thể để thực hiện tấn công, ẩn mình và khai thác theo từng giai đoạn

3.3 Các dạng tấn công - Tấn công APT

- Các giai đoạn điển hình của một cuộc tấn công APT:
  - Truy cập ban đầu,
  - Thâm nhập lần đầu và triển khai mã độc,
  - Mở rộng truy cập và di chuyển ngang,
  - Giai đoạn tấn công,
  - Gây thiệt hại,
  - Tấn công tiếp theo.

3.4 Các dạng phần mềm độc hại



3.4 Các dạng phần mềm độc hại - Logic bombs

- Bom logic (Logic bombs) thường được "nhúng" vào các chương trình bình thường và thường hẹn giờ để "phát nổ" trong một số điều kiện củ thể.
- Điều kiện để bom "phát nổ" có thể là:
  - Sự xuất hiện hoặc biến mất của các files cụ thể;
  - Một ngày nào đó, hoặc một ngày trong tuần.
- Khi "phát nổ" bom logic có thể xoá dữ liệu, files, tắt cả hệ thống...
- Ví dụ: Quả bom logic do Tim Lloyd cài lại đã "phát nổ" tại công ty Omega Engieering vào ngày 30/7/1996, 20 ngày sau khi Tim Lloyd bị sa thải. Bom logic này đã xoá sạch các bản thiết kế và các chương trình, gây thiệt hại 10 triệu USD. Tim Lloyd bị phạt 2 triệu USD và 41 tháng tù.

3.4 Các dạng phần mềm độc hại - Trojan horses

Trojan horses lấy tên theo tích "Con ngựa thành Troy"

3.4 Các dạng phần mềm độc hại - Trojan horses

- Trojan horses chứa mã độc, thường giả danh những chương trình có ích, nhằm lừa người dùng kích hoạt chúng.
- Trojan horses thường được sử dụng để thực thi gián tiếp các tác vụ, mà tác giả của chúng không thể thực hiện trực tiếp do không có quyền truy nhập.
- VD: trong một hệ thống nhiều users, một user có thể tạo ra một trojan đội lốt một chương trình hữu ích đặt ở thư mục chung. Khi trojan này được thực thi bởi một user khác, nó sẽ cho phép tất cả các users truy nhập vào các files của user đó.

3.4 Các dạng phần mềm độc hại - Tấn công sử dụng cửa hậu

❖ Tấn công sử dụng cửa hậu (Back doors)

- Cửa hậu thường được các lập trình viên tạo ra, dùng để gỡ rối và test chương trình.
- Cửa hậu thường cho phép truy nhập trực tiếp vào hệ thống mà không qua các thủ tục kiểm tra an ninh thông thường.
- Khi cửa hậu được lập trình viên tạo ra để truy nhập hệ thống bất hợp pháp, nó trở thành một mối đe doạ đến an ninh hệ thống.
- Rất khó phát hiện ra cửa hậu vì nó thường được thiết kế và cài đặt khéo léo: cửa hậu chỉ được kích hoạt trong một ngữ cảnh nào đó.

3.4 Các dạng phần mềm độc hại - Viruses

3.4 Các dạng phần mềm độc hại - Viruses

- Virus và một chương trình có thể "nhiễm" vào các chương trình khác, bằng cách sửa đổi các chương trình này.
- Nếu các chương trình đã bị sửa đổi chứa virus được kích hoạt thì virus sẽ tiếp tục "lây nhiễm" sang các chương trình khác.
- Giống như virus sinh học, virus máy tính cũng có khả năng tự nhân bản, tự lây nhiễm sang các chương trình khác mà nó tiếp xúc.

3.4 Các dạng phần mềm độc hại - Viruses

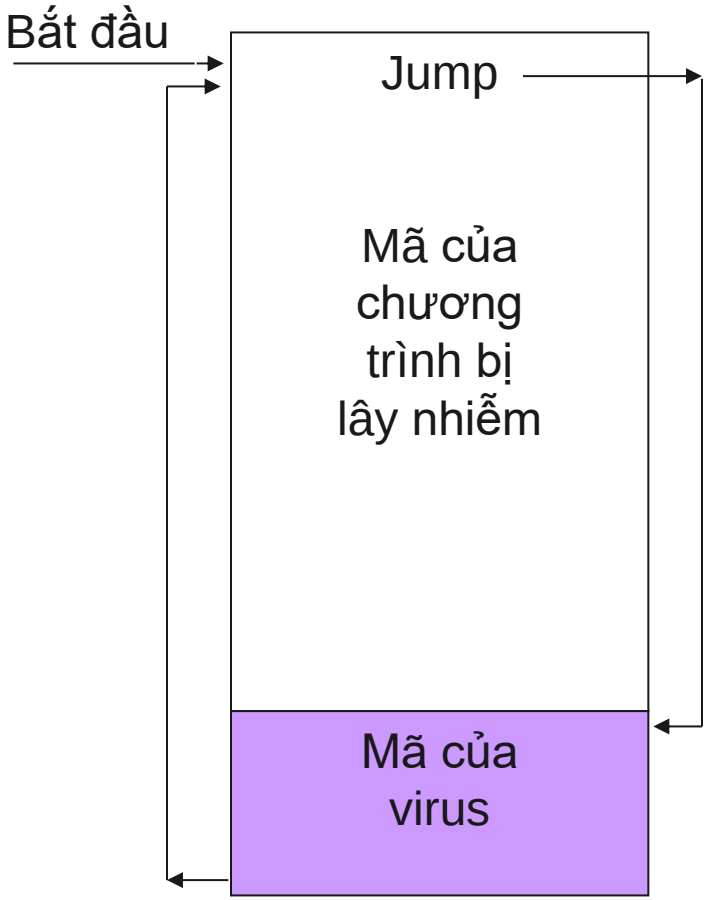
- Có nhiều con đường lây nhiễm virus:
  - Sao chép file
  - Email
  - Gọi các ứng dụng và dịch vụ qua mạng,...
- Virus có thể thực hiện được mọi việc mà một chương trình thông thường có thể thực hiện.
- Khi đã lây nhiễm vào một chương trình, virus tự động được thực hiện khi chương trình này chạy.

3.4 Các dạng phần mềm độc hại - Viruses

- 4 giai đoạn của vòng đời virus:
  - Giai đoạn "nằm im": Virus trong giai đoạn không được kích hoạt. Trong giai đoạn này virus có thể được kích hoạt nhờ một sự kiện nào đó.
  - Giai đoạn phát tán: Virus "cài" một bản sao của nó vào các chương trình khác.
  - Giai đoạn kích hoạt: virus được kích hoạt để thực thi các tác vụ đã thiết được định sẵn. Virus cũng thường được kích hoạt dựa trên một sự kiện nào đó.
  - Giai đoạn thực hiện: thực thi các tác vụ. Một số viruses có thể vô hại, nhưng một số khác có thể xoá dữ liệu, chương trình...

3.4 Các dạng phần mềm độc hại - Viruses

- Cơ chế chèn mã virus vào chương trình chủ:
  - Virus có thể chèn mã của nó vào đầu hoặc cuối của chương trình bị lây nhiễm.
  - Khi chương trình nhiễm virus được thực hiện, mã virus được thực hiện trước, sau đó mã chương trình mới được thực hiện.



3.4 Các dạng phần mềm độc hại – File Viruses

- File virus là dạng virus phổ biến nhất, đối tượng lây nhiễm của chúng là các file chương trình và các file dữ liệu. Mỗi khi chương trình được kích hoạt hoặc file dữ liệu được nạp vào bộ nhớ, vi rút được kích hoạt. Mọi chương trình tiếp theo được kích hoạt đều bị lây nhiễm virus này.
- File virus có thể làm hỏng chương trình, hỏng hoặc phá hủy các file dữ liệu, đánh cắp các dữ liệu nhạy cảm,…

3.4 Các dạng phần mềm độc hại – Boot Viruses

- Boot vi rút là dạng vi rút lây nhiễm vào cung khởi động (boot sector) của đĩa hoặc phần hệ thống của đĩa như cung khởi động chủ của đĩa cứng (master boot record).
- Do boot vi rút lây nhiễm vào cung khởi động nên nó luôn được nạp vào bộ nhớ mỗi khi hệ thống máy khởi động.
- Boot vi rút có thể gây hỏng phần khởi động của đĩa, thậm chí có thể làm cho đĩa không thể truy nhập được.

3.4 Các dạng phần mềm độc hại – Macro Viruses

- Macro viruses thường lây nhiễm vào các files tài liệu của MS-Word và ứng dụng office khác.
- Macro viruses hoạt động được nhờ tính năng cho phép tạo và thực hiện các đoạn mã macro trong các tài liệu của bộ ứng dụng MS Office.
- Các đoạn mã macro thường được dùng để tự động hóa 1 số việc và được viết bằng ngôn ngữ Visual Basic for Applications.

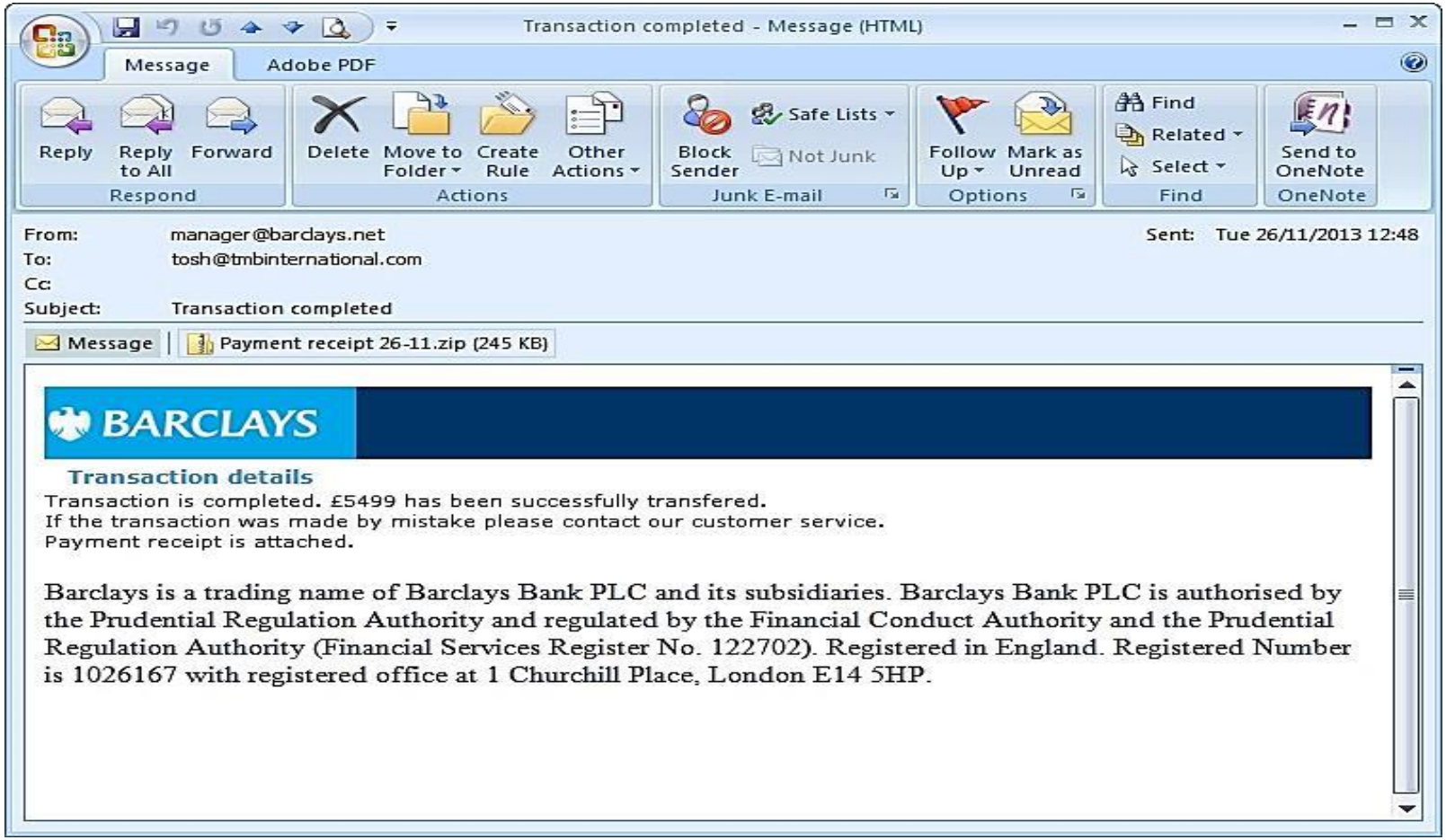
3.4 Các dạng phần mềm độc hại – Macro Viruses

- Macro viruses thường lây nhiễm vào các files định dạng chuẩn và từ đó lây nhiễm vào tất cả các files tài liệu được mở.
- Macro viruses cũng có thể được tự động kích hoạt nhờ các auto-executed macros: AutoExecute, Automacro và Command macro.
- Theo thống kê, macro viruses chiếm khoảng 2/3 tổng lượng viruses đã được phát hiện.

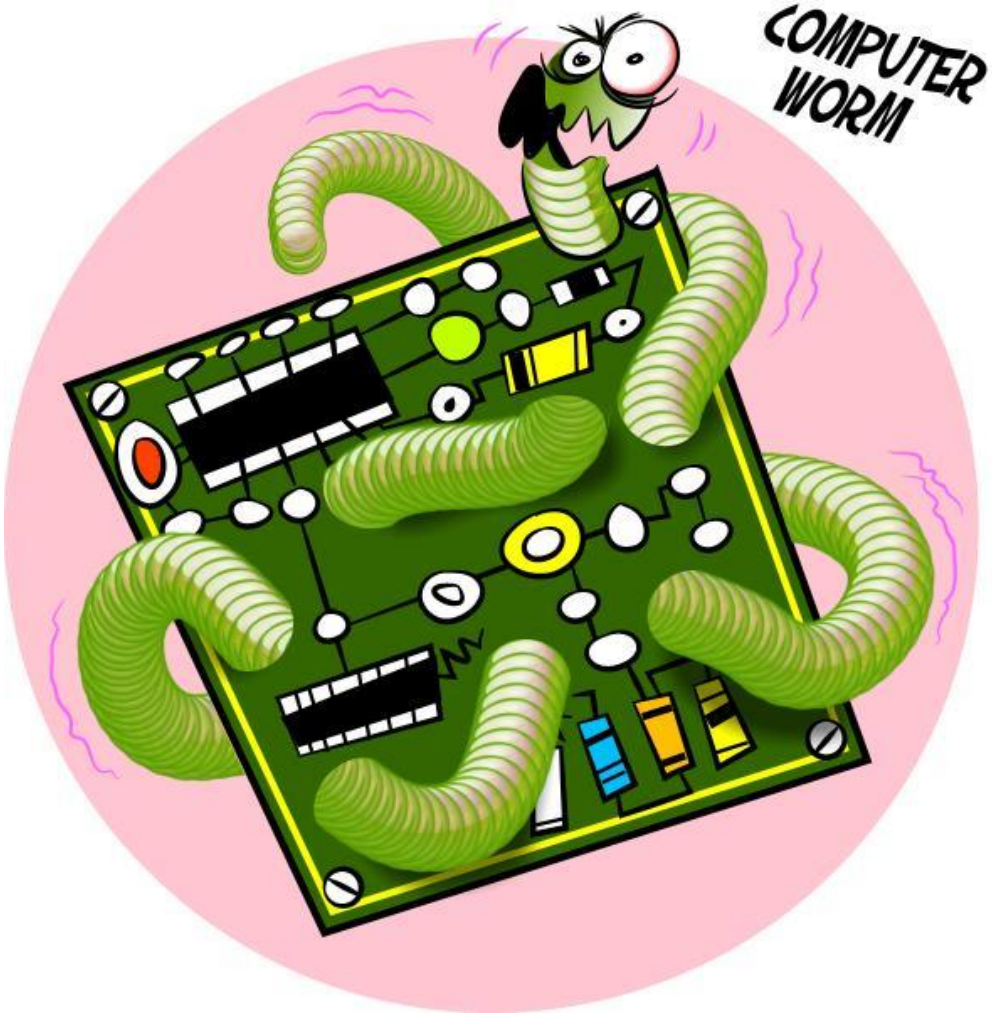
3.4 Các dạng phần mềm độc hại – E-mail Viruses

- E-mail viruses lây nhiễm bằng cách tự động gửi một bản copy của nó như 1 file đính kèm đến tất cả các địa chỉ email trong sổ địa chỉ của user trên máy bị lây nhiễm.
- Nếu user mở email hoặc file đính kèm, virus được kích hoạt.
- E-mail viruses có thể lây nhiễm rất nhanh chóng, lan tràn trên khắp thế giới trong một thời gian ngắn.

3.4 Các dạng phần mềm độc hại – E-mail Viruses



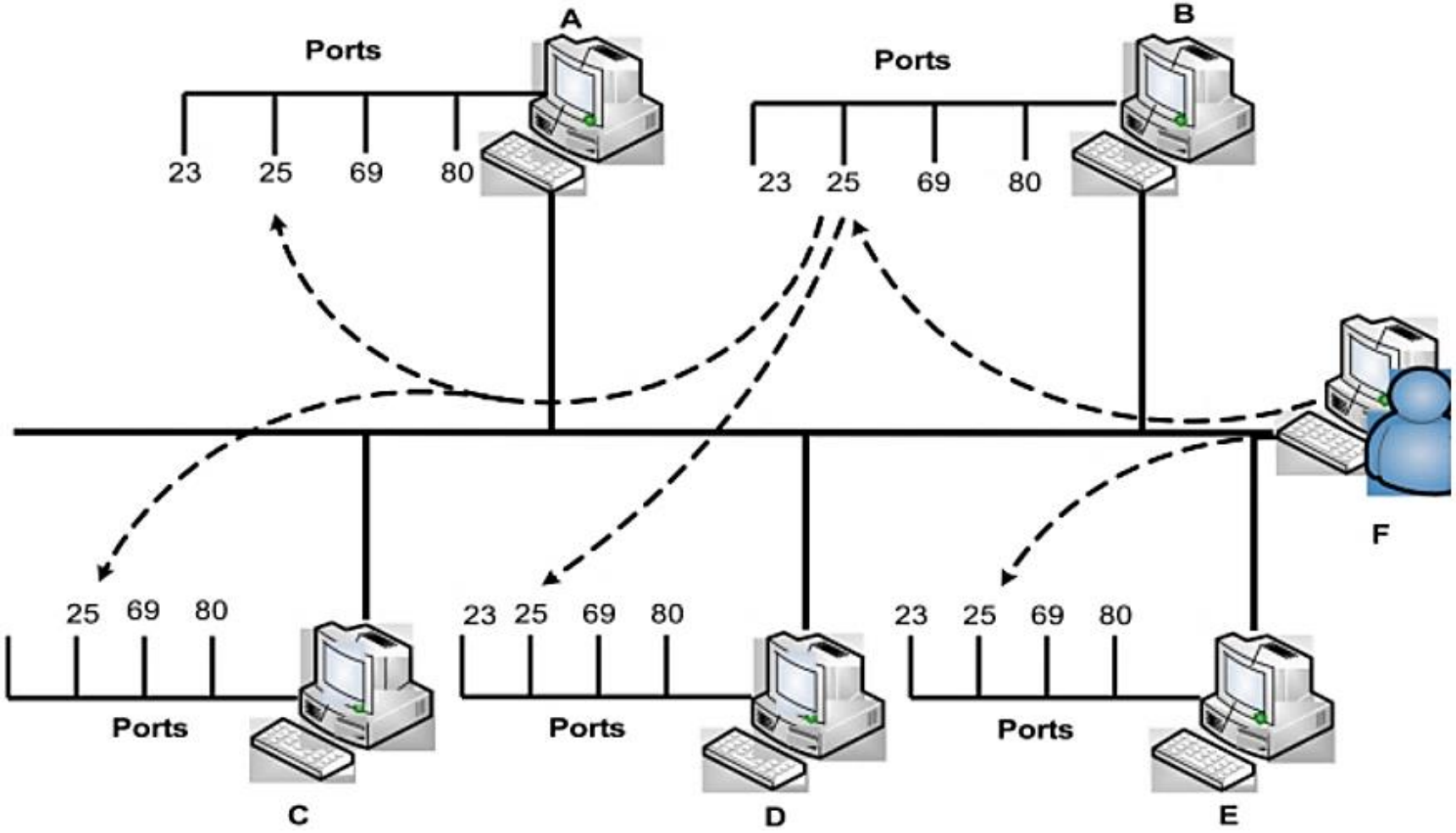
3.4 Các dạng phần mềm độc hại - Worms



3.4 Các dạng phần mềm độc hại - Worms

- Sâu (Worms) có khả năng tự lây nhiễm từ máy này sang máy khác mà không cần sự trợ giúp của người dùng (khác email viruses).
- Khi sâu lây nhiễm vào một máy, nó sử dụng máy này làm "bàn đạp" để tiếp tục tấn công các máy khác.
- Các sâu trên mạng sử dụng kết nối mạng để lây lan từ máy này sang máy khác.
- Khi sâu hoạt động, nó tương tự virus.

3.4 Các dạng phần mềm độc hại - Worms



3.4 Các dạng phần mềm độc hại - Worms

- Các phương pháp lây lan của sâu:
  - Lây lan qua thư điện tử: sử dụng email để gửi bản copy của sâu đến các máy khác.
  - Lây lan thông qua khả năng thực thi từ xa: Sâu thực thi một bản copy của nó trên một máy khác nhờ lợi dụng các lỗ hổng an ninh của hệ điều hành, các dịch vụ hoặc phần mềm ứng dụng.
  - Lây lan thông qua khả năng log-in (đăng nhập) từ xa: sâu đăng nhập vào hệ thống ở xa như một user và sử dụng lệnh để copy bản thân từ máy này sang máy khác.

3.4 Các dạng phần mềm độc hại – Worms – Ví dụ

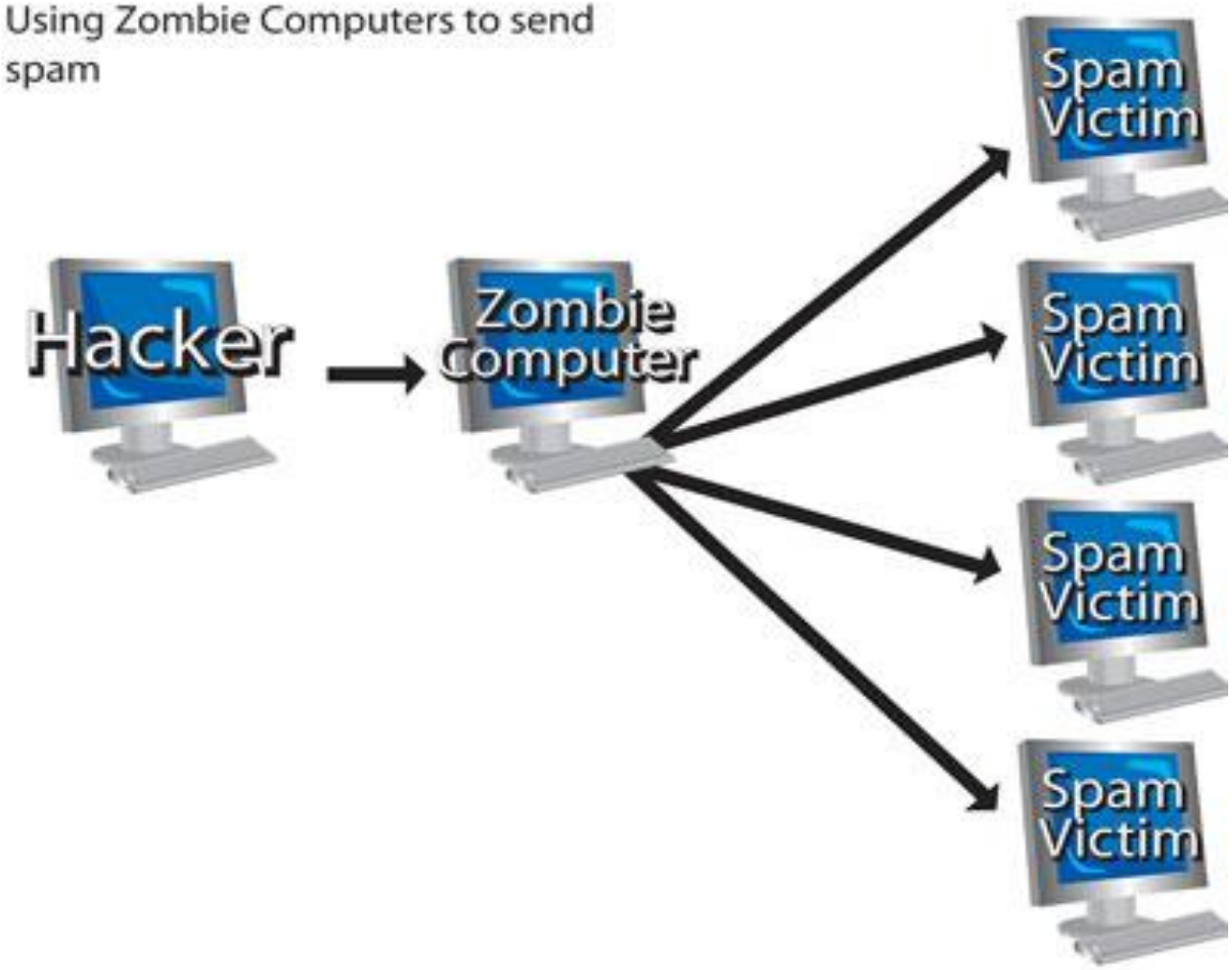
- Code Red (7/2001):
  - Lợi dụng một lỗi hổng an ninh trong MS IIS để lây lan (lỗi tràn bộ đệm khi xử lý các file .ida của IIS).
  - Quét các địa chỉ IP ngẫu nhiên để tìm các hệ thống có lỗi.
  - Lây nhiễm vào 360.000 máy chủ trong vòng 14 giờ.

3.4 Các dạng phần mềm độc hại – Worms – Ví dụ

- Nimda (9/2001): có khả năng lây lan theo nhiều con đường:
  - Qua email từ máy client sang client
  - Qua các thư mục chia sẻ trên mạng
  - Từ máy chủ web sang trình duyệt
  - Từ máy khách đến máy chủ nhờ khai thác các lỗi máy chủ.
  - 22 phút sau khi ra đời Nimda trở thành sâu có tốc độ lan truyền nhanh nhất trên Internet.

3.4 Các dạng phần mềm độc hại – Zombie/Bot

3.4 Các dạng phần mềm độc hại – Zombie/Bot



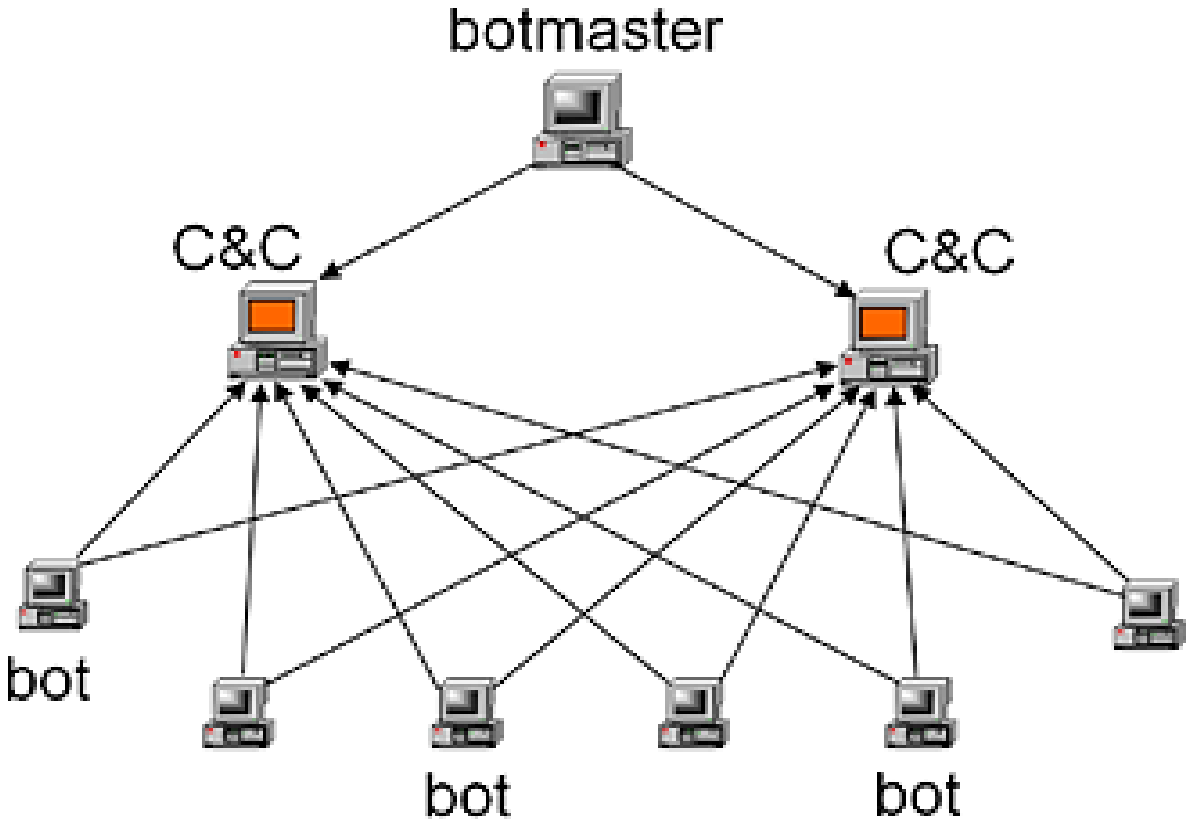
3.4 Các dạng phần mềm độc hại – Zombie/Bot

- Zombie (còn được gọi là bots) là một chương trình được thiết kế để giành quyền kiểm soát một máy tính có kết nối Internet, và sử dụng máy tính bị kiểm soát để tấn công các hệ thống khác.
- Các bot thường được dùng để tấn công DDoS các máy chủ/website lớn.
  - Tin tặc sử dụng bot để chiếm quyền điều khiển một lượng rất lớn máy tính, hình thành mạng máy tính ma, hoặc botnet sử dụng cho gửi spam mails và tấn công DDoS.
- Rất khó để lần vết và phát hiện ra tác giả tạo ra và điều khiển các bots.
- Tương tự như sâu, bots có khả năng tự lây nhiễm sang các hệ thống khác mà không cần chương trình chủ, vật chủ, hoặc hỗ trợ từ người dùng.

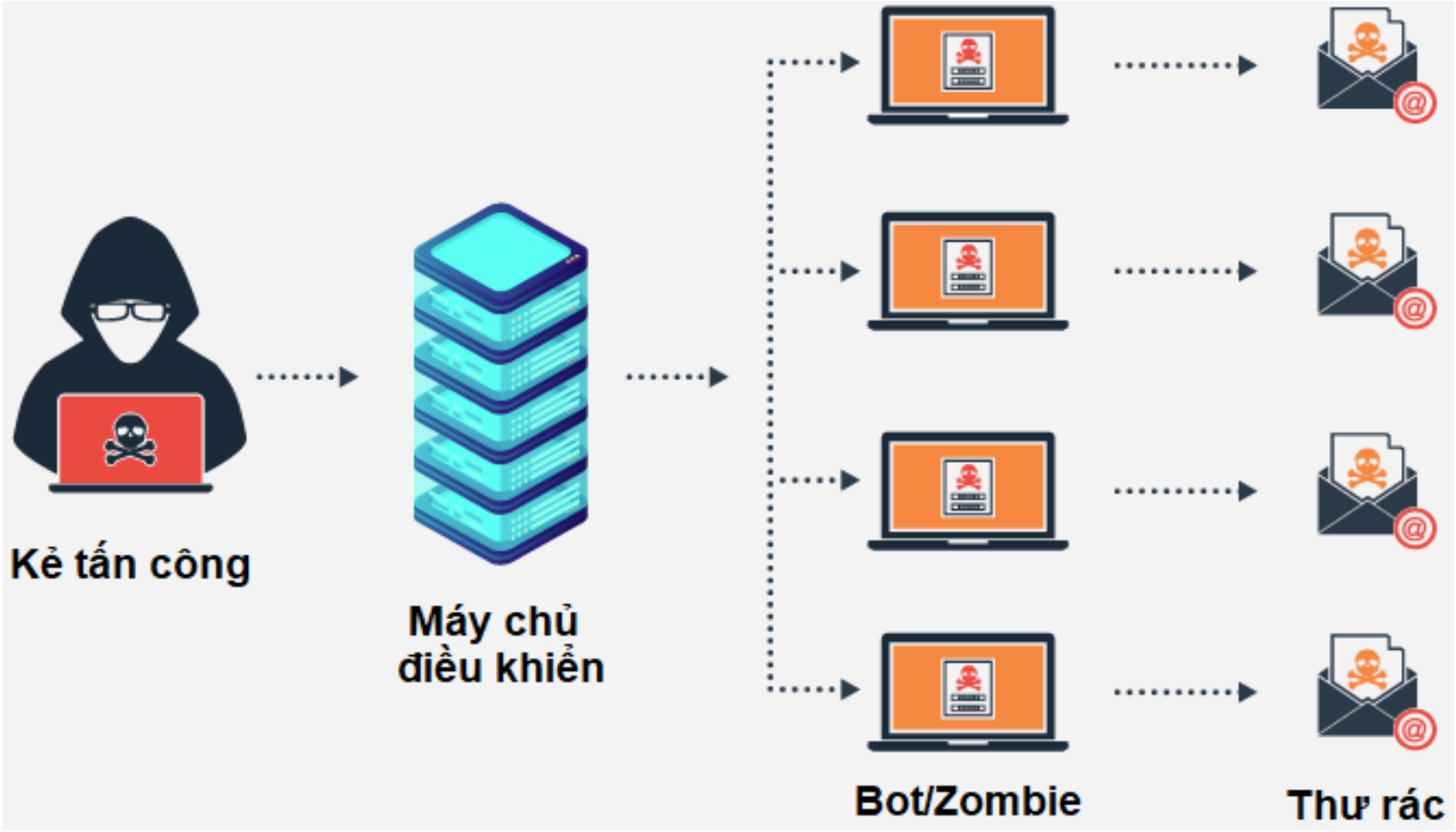
3.4 Các dạng phần mềm độc hại – Zombie/Bot

- Một tập hợp các máy tính bot dưới sự kiểm soát của một, hoặc một nhóm kẻ tấn công được gọi là mạng máy tính ma, hay botnet.
- Kẻ tấn công kiểm soát và điều khiển các bot trong botnet thông qua một hệ thống các máy chủ lệnh và điều khiển trung gian (Command and control – C&C) sử dụng các giao thức truyền thông thông dụng như HTTP, hoặc IRC.

2.4 Các dạng phần mềm độc hại – Zombie/Bot



3.4 Các dạng phần mềm độc hại – Zombie/Bot



3.4 Các dạng phần mềm độc hại - Rootkit

- Rootkit là một dạng phần mềm độc hại gồm một tập các công cụ có mục đích giành quyền truy nhập vào hệ thống máy tính mà người dùng không có thẩm quyền không thể truy nhập.
- Rootkit thường che giấu mình bằng cách đội lột một phần mềm khác.
- Rootkit có thể được cài đặt tự động, hoặc tin tặc cài đặt rootkit khi chiếm được quyền quản trị hệ thống.
- Do rootkit có quyền truy nhập hệ thống ở mức quản trị nên nó có toàn quyền truy nhập vào các thành phần trong hệ thống và rất khó bị phát hiện.

3.4 Các dạng phần mềm độc hại - Adware và Spyware

- Adware (advertising-supported software) là các phần mềm tự động hiển thị các bảng quảng cáo trong thời gian người dùng tải hoặc sử dụng các phần mềm.
- Adware thường được đóng gói chung với các phần mềm khác có thể dưới dạng như một phần của một phần mềm hoặc một dịch vụ miễn phí.
- Adware trong một số trường hợp có thể được coi là một phần mềm độc hại nếu chúng được tự động cài đặt và kích hoạt mà không được sự đồng ý của người dùng.

3.4 Các dạng phần mềm độc hại - Adware và Spyware

- Spyware là một dạng phần mềm độc hại được cài đặt tự động nhằm giám sát, thu thập và đánh cắp các thông tin nhạy cảm trên hệ thống nạn nhân.
- Có 4 loại spyware thường gặp, gồm:
  - system monitor (giám sát hệ thống),
  - trojan,
  - Adware,
  - tracking cookies (các cookie theo dõi).
- Spyware có thể được cài đặt vào hệ thống nạn nhân thông qua nhiều phương pháp, như tích hợp, đóng gói vào các phần mềm khác, bẫy nạn nhân tự tải và cài đặt, hoặc tin tặc có thể sử dụng vi rút, sâu để tải và cài đặt.
- Spyware thường được trang bị khả năng ẩn mình nên rất khó có thể phát hiện bằng các phương pháp thông thường.

3.4 Các dạng phần mềm độc hại – Phòng chống

- Ngăn chặn viruses lây nhiễm vào hệ thống:
  - Luôn cập nhật hệ thống để hạn chế các lỗi phần mềm
  - Sử dụng các biện pháp kiểm soát truy nhập
- Khi hệ thống đã bị nhiễm virus:
  - Phát hiện virus
  - Nhận dạng virus
  - Loại bỏ virus

3.4 Các dạng phần mềm độc hại – Phòng chống

- Một số phần mềm diệt virus và phần mềm độc hại:
  - Microsoft Security Essentials (Windows 7 trở lên)
  - Semantec Norton Antivirus
  - Kaspersky Antivirus
  - BitDefender Antivirus
  - AVG Antivirus
  - McAfee VirusScan
  - Trend Micro Antivirus
  - F-secure
  - BKAV Antivirus

3.4 Các dạng phần mềm độc hại – Phòng chống