**BỘ CÔNG THƯƠNG**
**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP TP HỒ CHÍ MINH**

---

**Khoa: Công Nghệ Thông Tin**


# Bài Thường Kì

## Tóm tắt mục đích, các thức thực hiện tấn công Trojan và backdoor, Dos, buffer Overflow, wireless Hacking

Student's ID :
Student's name : Phúc Lâm
Subject : Triển khai an ninh hệ thống
Instructor : Đỗ Hà Phương
Faculty : Công Nghệ Thông Tin
Completed Date : 2024

# NHẬN XÉT CỦA GIÁO VIÊN HƯỚNG DẪN

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

**Điểm lab report:**

**Yêu cầu: Đọc tài liệu đã được cung cấp và hãy tóm tắt mục đích, các thức thực hiện tấn công Trojan và backdoor, Dos, buffer Overflow, wireless Hacking**

# I. TROJAN VÀ BACKDOOR

## 1.1. Trojan là gì?

Tên gọi "Trojan" lấy ý tưởng từ cuộc chiến tấn công thành Troy với tên gọi là Trojan Hoorse, xuất phát từ câu chuyện về con ngựa gỗ trong thần thoại Hy Lạp, nơi mà những người lính ẩn mình bên trong để xâm nhập vào thành và để nữa đêm xuất hiện công phá thành từ phía bên trong.

Trojan, hay còn gọi là Ngựa Trojan, là một loại phần mềm độc hại được ngụy trang dưới dạng phần mềm hợp lệ hoặc hữu ích để lừa người dùng tải xuống và cài đặt. Các hacker đã tạo sẵn các chương trình trên với tập tin crack đã được "khuyến mãi" thêm mã đọc (trojan).

## 1.2. Backdoor là gì?

Backdoor hay còn gọi là "cổng sau" là chương trình mà hacker cài đặt trên máy tính của nạn nhân để có thể điều khiển hay xâm nhập lại dễ dàng.

Một chức năng khác của backdoor là xóa tất cả những thông tin hay các chứng cứ mà hacker có thể để lại khi họ xâm nhập trái phép vào hệ thống, các backdoor tinh vi đôi khi tự nhân bản hay che dấu để có thể duy trì "cổng sau" cho phép các hacker truy cập hệ thống ngay cả khi chúng bị phát hiện.

Một trong các backdoor thường được đề cập trong CEH là Remote Administration Trojan (RAT) cho phép các hacker kiểm soát những máy tính đã bị chiếm quyền điều khiển với những chức năng xem và quản lý toàn bộ desktop, thực thi các tập tin, tương tác vào registry hay thậm chí tạo ra các dịch vụ hệ thống khác

## 1.3. Mục đích và các dạng tấn công Trojan

Trojan có thể được sử dụng cho nhiều dạng tấn công khác nhau từ **đánh cắp dữ liệu** cho đến **chạy chương trình từ xa, tấn công từ chối dịch vụ, tạo ra lỗ hổng bảo mật** …

| | |
|---|---|
| **Remote Access Trojan (RAT)** | dùng để truy cập từ xa vào hệ thống |
| **Data-Sending Trojan** | dùng để đánh cắp dữ liệu trên hệ thống và gởi về cho hacker |
| **Destructive Trojan** | sử dụng để phá hủy tập tin trên hệ thống |
| **Denial of Service Trojan** | dùng để phát động các đợt tấn công từ chối dịch vụ. |
| **Proxy Trojan** | được dùng để tạo ra các võ bọc truyền thông (tunnel) hay phát động tấn công từ một hệ thống khác. |
| **FTP Trojan** | dùng để tạo ra dịch vụ FTP nhằm sao chép dữ liệu lên hệ thống bị nhiễm. |
| **Security software disabler Trojan** | dùng để tắt các dịch vụ phòng chống virus, trojan. |

### 1.4. Cách thực hiện tấn công

- **TROJ_OAZ** là một trojan thay đổi tên chương trình notepad.cexe thanh note.com sau đó sao chép chính nó thành notepad.exe vào thự mục hệ thống của Windows. Như vậy mỗi khi chúng ta mở chương trình notepad thì trojan cũng hoạt động và mở công hậu (backdoor) 7597 để hacker có thể thâm nhập vào máy tính từ xa. TROJ_OAZ còn nhiễm vào registry để nạp khi máy tính khởi động.
- **Tini** là một trojan có kích thươc rất nhỏ và đơn giãn hoạt động trên hệ điều hành Windows chuyên lắng nghe trên cổng 7777 cho phép hacker chạy lệnh từ xa thông qua chương trình telnet đến cổng này trên các máy tính bị lây nhiễm.
- **Donald Disk** là một dạng backdoor Trojan trên hệ thống Windows cho phép hacker toàn quyền kiểm soát qua môi trường internet. Hacker có thể đọc, ghi, xoa hay chạy bất kì ứng dụng nào trên hệ thống. Donald Disk kèm theo cả keylogger để bắt tín hiệu bàn phím và thay đổi registry để thực hiện các hành động như đóng mở khay CD-ROM. . Donald Disk hoạt động trên các cổng mặc định 23476 hay 23477

- **SubRoot** là trojan quản trị từ xa mà hacker có thể dùng để điều khiển máy tính bị nhiễm qua cổng 1700
- **LetMeRule** cũng thuộc loại trojan quản trị từ xa (RAT) và có thể lắng nghe trên bất kì cổng nào trên máy tính bị lây nhiễm, cho phép hacker xóa hay thực thi tập tin trên máy tính nạn nhân, xem và sữa đổi registry hay điều khiển máy tính này thông qua dòng lệnh.

# II. TẤN CÔNG DOS

## 2.1. Dos là gì?

DoS là dạng tấn công làm cho các hệ thống máy chủ, trang web bị tê liệt không thể đáp ứng lại các yêu cầu của người dùng. Đây là một trong các hình thức tấn công đem lại hiệu quả cao cho các hacker cũng như là giải pháp sau cùng nêu như không tìm được cách nào đột nhập vào mục tiêu.

DOS đánh vào bản chất tự nhiên của một quá trình truyền thông của client và server, nếu có quá nhiều clicent truy cập thì server sẽ bị quá tải, buộc lòng phải từ chối các yêu cầu truy cập khác

## 2.2. Mục đích của việc tấn công Dos

Một khi không thể tìm được cách thức xâm nhập vào hệ thống mục tiêu bằng cách dò tìm và khai thác lỗi thì các hacker sẽ áp dụng phương pháp tấn công từ chối dịch vụ hay còn gọi là Denial of Service (DoS).

**Mục đích của việc tấn công này:**

- Làm tê liệt hệ thống mạng bằng cách gửi lượng lớn dữ liệu.
- Khiến các giao dịch thông thường không thể thực hiện được.
- Ngắt kết nối giữa máy khách và máy chủ.
- Chặn quyền truy cập của một host vào dịch vụ.
- Ngăn cản phản hồi từ hệ thống, gây gián đoạn cho người dùng.

### 2.3. Cách thực hiện tấn công Dos

Các hacker thường sử dụng các công cụ nào đề tấn công DoS, dưới đây là một số ứng dụng điển hình :

- ***Ping of Death*** : Các công cụ tấn công *Ping of Death* gởi nhiều gói tin IP với kích thước lớn đến mục tiêu làm cho các máy này phải mất nhiều thời gian và tài nguyên hệ thống để xử lý, kết quả là không thể đáp ứng được các yêu cầu kết nối thông thường của những máy tính khác dẫn đến bị từ chối dịch vụ.
- ***LAND Attack*** : Những công cụ có chức năng tấn công *LAND Attack* sẽ gởi các gói tin có địa chỉ IP trùng lắp với các địa chỉ IP đích khiến cho việc xử lý các yêu cầu này có thể dẫn đến tình trạng bị lặp lại (*loop*) và không thể tiếp nhận thêm các yêu cầu truy cập khác.
- ***WinNuke*** : Chương trình này tìm kiếm các máy tính đang mở *port* 139 để gởi các gói tin IP rác đến mục tiêu. Dạng tấn công này còn được gọi là *Out of Bound* (OOB) và làm tràn ngập bộ nhớ đệm của giao thức IP.
- ***CPU Hog***: Công cụ này làm quá tải nguồn tài nguyên CPU của các máy bị tấn công .
- ***Bubonic***: Là công cụ DoS hoạt động bằng cách gởi các gói tin TCP với những thiết lập ngẫu nhiên làm cho mục tiêu bị tấn công bị quá tãi hay thậm chí bị gãy đổ.
- ***RPC Locator:*** Đây là một dịch vụ nhạy cảm nếu như không được vá lỗi có khả năng bị tấn công gây tràn bộ đệm. Dịch vụ này hoạt động trên các hệ thống Windows để phân phối các bản cài đặt hay ứng dụng trẹn toàn hệ thống, đây cũng là một dịch vụ dễ bị tấn công gây ra tình trạng từ chối dịch vụ trên các máy chủ.
- Ngoài ra còn có các công cụ như ***SSPing*** hay ***Targa*** có thể gởi các gói tin với kích thược lớn đến mục tiêu làm tê liệt khả năng đáp ứng cũng như xử lý các dữ liệu này, điều đó cũng có nghĩa nạn nhân sẽ không thể tiếp nhận các yêu cầu khác dẫn đến tình trạng "từ chối dịch vụ".

### 2.4. Cơ chế hoạt động của DDOS

Các cuộc tấn công thường gặp là *DDoS*, hình thức này sử dụng các hệ thống mạng máy tính "ma" gọi là *botnet*, và mỗi máy trạm trong hệ thống này gọi là một *bot* hay *zombie* đã được các hacker cài đặt *trojan* có thể điều khiển từ xa thông qua kênh IRC hay những dữ liệu tập trung (có thể là một tập tin điều khiển đặt trên một trang web nào đó.

Thông thường DDoS gồm có 3 thành phần :

- *Master* hay *Handler* : Chương trình dùng để điều khiển.

- *Slave* hay *zombie, bot* là các máy tính bị cài đặt hay lây nhiễm các chương trình

nguy hiểm và bị điều khiển bởi các *master / handler*.

- *Victim* : Những mục tiêu bị tấn công từ chối dịch vụ.

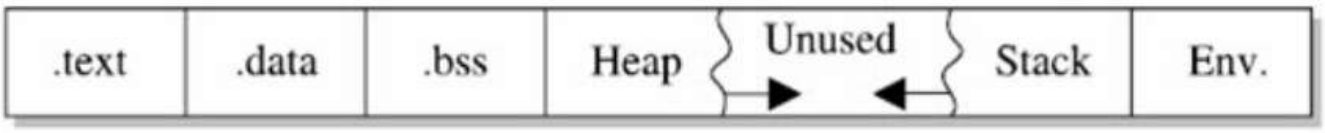
Trong các cuộc tấn công *DDoS* gần đây hacker thường sử dụng công cụ *Low Orbit Ion Cannon* (LOIC). Hiện nay, nhóm hacker hàng đầu thế giới là *Anonymous* sẽ phát triển một ứng dụng mới có tác dụng mạnh mẽ hơn có tên là *#RefRef* để thay thế cho *LOIC*.

## III. BUFFER OVERFLOW

### 3.1. Tấn công Buffer Overflow là gì?

**Buffer Overflow** hay **BoF** là lỗi tràn bộ đệm, có nguyên nhân gần giống với tình huốn tấn công SQL injection khi người dùng hay hacker cung cấp các biến đầu vào hay dữ liệu vượt quá khả năng xử lý của chương trình làm cho hệ thống bị treo dẫn đến từ chối dịch vụ (DoS) hay có khả năng bị các hacker lợi dụng chèn các chỉ thị trái phép nhằm thực thi các đoạn mã nguy hiểm từ xa. Có hai dạng lỗi tràn bộ đệm là **stack-based** và **heapbased**.

Cả hai thành phần stack và heap đều được sử dụng để lưu trữ các biến người dùng khi chạy chương trình. Khi một chương trình được nạp vào bộ nhớ được chia thành 6 giai đoạn tương ứng với sơ đồ phân đoạn trong bộ nhớ như hình minh họa bên dưới :



### 3.2. Mục đích tấn công

- ***Khai thác lỗ hổng bảo mật*:** Tấn công nhằm làm tràn bộ nhớ đệm (buffer), dẫn đến ghi đè lên vùng nhớ quan trọng.
- ***Chạy mã độc***: Cho phép kẻ tấn công thực thi mã tùy ý trên hệ thống mục tiêu.
- ***Chiếm quyền điều khiển***: Đạt được quyền truy cập không hợp lệ vào hệ thống, có thể dẫn đến việc kiểm soát hoàn toàn.
- ***Làm rối loạn hoặc ngăn chặn dịch vụ***: Có thể gây ra sự cố cho ứng dụng hoặc hệ thống, dẫn đến từ chối dịch vụ.

### 3.3. Cách thức thực hiện

***Các bước tiến hành khai thác buffer overflow:***

1. Tìm vị trí hay các điểm gấy ra lỗi tràn bộ đệm của ứng dụng.
2. Ghi các dữ liệu có kích thước lớn để vượt quá khả năng kiểm soát của chương trình.
3. Ghi đè lên địa chỉ trả về của các hàm.
4. Thay đổi chương trình thực thi bằng đoạn mã của hacker.

## IV. WIRELESS HACKING

### 4.1. Tấn công trên mạng không dây là gì?

***Wireless hacking*** là quá trình xâm nhập vào mạng không dây với mục đích chiếm quyền truy cập hoặc gây rối loạn. Đây là một hình thức tấn công mà kẻ xâm nhập khai thác các lỗ hổng bảo mật trong giao thức mạng không dây.

### 4.2. Mục đích của tấn công wireless hacking

- ***Chiếm quyền truy cập***: Lấy quyền truy cập vào mạng để sử dụng tài nguyên, dịch vụ, hoặc dữ liệu mà không được phép.
- ***Nghe lén dữ liệu***: Theo dõi và thu thập thông tin nhạy cảm như mật khẩu, dữ liệu cá nhân, hoặc thông tin tài chính.
- ***Lây lan mã độc***: Phát tán virus hoặc mã độc qua mạng không dây đến các thiết bị kết nối.

- ***Gây rối loạn dịch vụ***: Ngăn chặn người dùng hợp pháp truy cập vào mạng thông qua các cuộc tấn công như jamming hoặc denial of service.
- ***Đánh cắp thông tin:*** Tận dụng các điểm yếu để thu thập thông tin người dùng hoặc doanh nghiệp.

### 4.3. Cách thức thực hiện

Trên mạng không dây (WLAN), tấn công phổ biến nhất là ***eavesdropping*** hay ***sniffing***, cho phép hacker nghe lén và đánh cắp thông tin từ các Access Point (AP) được cấu hình mặc định. Các gói tin không được mã hóa, dẫn đến việc mật khẩu và tài khoản trong các giao thức như FTP, POP3, SMTP dễ dàng bị đánh cắp.

Mạng WLAN được xác định qua SSID, được gửi không mã hóa, giúp hacker phát hiện dễ dàng. Dưới đây là một số hình thức tấn công phổ biến:

- **AP masquerading**: Hacker giả mạo AP hợp lệ. Người dùng kết nối sẽ bị đánh cắp thông tin.
- **MAC spoofing**: Giả mạo địa chỉ MAC để vượt qua kiểm soát của AP.
- **Denial of Service**: Gây nhiễu loạn mạng Wi-Fi, khiến nó không hoạt động. Hacker có thể gửi nhiều yêu cầu xác thực, làm tê liệt AP và đánh cắp thông tin./.