|  |  |
| --- | --- |
| A blue and red text on a white background  Description automatically generated | BỘ GIÁO DỤC VÀ ĐÀO TẠO  **TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM** |

**ĐỒ ÁN HỆ ĐIỀU HÀNH LINUX**

**Đề Tài:**

**PHÁT HIỆN VÀ NGĂN CHẶN BRUTE-FORCE VỚI FAIL2BAN**

**Ngành: Công Nghệ Thông Tin**

***Giảng viên hướng dẫn:* Thầy Nguyễn Lê Văn**

*Sinh viên thực hiện:*

**01. Phan Tiến Sĩ**  **MSSV: 2180606302**

**02. Doãn Thành Trung**  **MSSV: 2180606829**

**03. Đoàn Hồ Nguyên Khải**  **MSSV: 2180606439**

**TP. Hồ Chí Minh, 2025**

# LỜI MỞ ĐẦU

Trong thời đại công nghệ thông tin phát triển mạnh mẽ, bảo mật hệ thống là một vấn đề quan trọng đối với các cá nhân, tổ chức và doanh nghiệp. Sự gia tăng của các cuộc tấn công mạng, đặc biệt là các cuộc tấn công brute-force, đặt ra thách thức lớn trong việc bảo vệ an toàn thông tin. Brute-force attack là một phương thức tấn công phổ biến, trong đó kẻ tấn công cố gắng đoán mật khẩu bằng cách thử nhiều tổ hợp khác nhau.

Nhận thấy tầm quan trọng của vấn đề này, chúng tôi thực hiện đề tài "PHÁT HIỆN VÀ NGĂN CHẶN TẤN CÔNG BRUTE-FORCE VỚI FAIL2BAN" dưới sự hướng dẫn của thầy Nguyễn Lê Văn. Mục tiêu của đồ án là nghiên cứu, triển khai và đánh giá hiệu quả của Fail2Ban - một công cụ bảo mật mạnh mẽ giúp phát hiện và ngăn chặn các cuộc tấn công brute-force trên hệ điều hành Linux.

Bài báo cáo sẽ trình bày từ cơ sở lý thuyết về brute-force attack, giới thiệu Fail2Ban, hướng dẫn cài đặt và cấu hình trên hệ điều hành CentOS 7, cũng như thử nghiệm thực tế để đánh giá hiệu quả của công cụ này. Chúng tôi hy vọng đề tài này sẽ giúp nâng cao nhận thức về an toàn thông tin và cung cấp một giải pháp hữu ích cho việc bảo vệ hệ thống khỏi các mối đe dọa từ tấn công brute-force.

Do thời gian nghiên cứu và kiến thức còn hạn chế, bài báo cáo không tránh khỏi những thiếu sót. Chúng em mong nhận được sự góp ý từ thầy cô để hoàn thiện đề tài hơn.

Chúng em xin chân thành cảm ơn!

Sinh viên thực hiện

**Phan Tiến Sĩ**

**Doãn Thành Trung**

**Đoàn Hồ Nguyên Khải**

# LỜI CẢM ƠN

Trước hết, chúng em xin gửi lời cảm ơn chân thành đến quý thầy cô Khoa Công Nghệ Thông Tin trường Đại học HUTECH đã nhiệt tình giảng dạy và truyền đạt những kiến thức quý báu về Công Nghệ Thông Tin, tạo nền tảng vững chắc cho chúng em trong quá trình thực hiện đồ án này.

Đặc biệt, chúng em xin bày tỏ lòng biết ơn sâu sắc đến thầy Nguyễn Lê Văn – người đã trực tiếp hướng dẫn, hỗ trợ, và cung cấp cho chúng em những kiến thức chuyên sâu cũng như các công nghệ cần thiết để hoàn thành đồ án " PHÁT HIỆN VÀ NGĂN CHẶN TẤN CÔNG BRUTE-FORCE VỚI FAIL2BAN ". Sự tận tâm và chỉ dẫn của thầy đã giúp chúng em vượt qua nhiều thử thách trong suốt quá trình thực hiện dự án.

Chúng em cũng xin gửi lời cảm ơn chân thành đến gia đình, các anh chị, và các bạn đã luôn ủng hộ, động viên, và đồng hành cùng chúng em trong suốt quá trình học tập, nghiên cứu và hoàn thành đồ án. Sự hỗ trợ và khích lệ của mọi người là động lực to lớn để chúng em cố gắng và hoàn thiện dự án.

Chúng em xin kính chúc Ban Giám Hiệu nhà trường cùng quý thầy cô luôn mạnh khỏe, hạnh phúc và gặt hái nhiều thành công trong sự nghiệp giảng dạy và nghiên cứu.

Chúng em xin chân thành cảm ơn!

# LỜI CAM ĐOAN

Chúng em xin cam đoan rằng nội dung đồ án "PHÁT HIỆN VÀ NGĂN CHẶN TẤN CÔNG BRUTE-FORCE VỚI FAIL2BAN" là kết quả của quá trình nghiên cứu và thực hiện nghiêm túc của nhóm chúng em. Toàn bộ nội dung trong báo cáo này là sản phẩm của sự tìm hiểu, phân tích và thử nghiệm thực tế trên hệ điều hành Linux (CentOS 7), không sao chép từ bất kỳ nguồn nào mà không trích dẫn rõ ràng.

Chúng em đã thực hiện các bước nghiên cứu, triển khai Fail2Ban để bảo vệ hệ thống trước các cuộc tấn công brute-force một cách khoa học và có hệ thống. Mọi kết quả thử nghiệm trong báo cáo đều phản ánh trung thực quá trình thực hiện, không có bất kỳ sự giả mạo hay chỉnh sửa không hợp lệ nào.

Tất cả tài liệu tham khảo sử dụng trong đồ án đều có nguồn gốc rõ ràng, được chọn lọc cẩn thận và trích dẫn theo đúng quy định. Chúng em cam kết tuân thủ đầy đủ các nguyên tắc về đạo đức nghiên cứu và không vi phạm bất kỳ quy định nào về bản quyền học thuật.

Chúng em xin chịu hoàn toàn trách nhiệm đối với nội dung báo cáo và sẵn sàng giải trình mọi thắc mắc liên quan đến tính trung thực và chính xác của đồ án.

Chúng em xin chân thành cảm ơn!

TP. Hồ Chí Minh, ngày 12 tháng 03 năm 2025

Người cam đoan

**Phan Tiến Sĩ**

**Doãn Thành Trung**

**Đoàn Hồ Nguyên Khải**

**MỤC LỤC**

[LỜI MỞ ĐẦU 1](#_Toc193639212)

[LỜI CẢM ƠN 2](#_Toc193639213)

[LỜI CAM ĐOAN 3](#_Toc193639214)

[CHƯƠNG 1 TỔNG QUAN 6](#_Toc193639215)

[1.1BỐI CẢNH ĐỀ TÀI 6](#_Toc193639216)

[1.2 MỤC TIÊU NGHIÊN CỨU 6](#_Toc193639217)

[1.3 PHẠM VI NGHIÊN CỨU 6](#_Toc193639218)

[1.4 PHƯƠNG PHÁP NGHIÊN CỨU 6](#_Toc193639219)

[CHƯƠNG 2 CƠ SỞ LÝ THUYẾT 7](#_Toc193639220)

[2.1 GIỚI THIỆU VỀ LÝ THUYẾT 7](#_Toc193639221)

[**2.1.1 Tấn công brute-force là gì?** 7](#_Toc193639222)

[**2.1.2 Các loại brute-force attack** 7](#_Toc193639223)

[**2.1.3 Hậu quả của brute-force attack** 7](#_Toc193639224)

[**2.1.4 Các phương pháp phòng chống brute-force attack** 7](#_Toc193639225)

[CHƯƠNG 3 GIỚI THIỆU VỀ FAIL2BAN 9](#_Toc193639226)

[3.1 Fail2Ban là gì? 9](#_Toc193639227)

[**3.2 Nguyên lý hoạt động của Fail2Ban:** 9](#_Toc193639228)

[**3.4. Cấu hình cơ bản của Fail2Ban** 9](#_Toc193639229)

[CHƯƠNG 4 MÔ HÌNH THỬ NGHIỆM 11](#_Toc193639230)

[CHƯƠNG 5: KẾT LUẬN VÀ KIẾN NGHỊ 18](#_Toc193639231)

**Danh Mục Hình Ảnh**

[Hình 1 Cài đặt Fail2Ban 16](#_Toc194397767)

[Hình 2 Kiểm tra trạng thái 16](#_Toc194397769)

[Hình 3 Cấu hình jail 17](#_Toc194397770)

[Hình 4 status 17](#_Toc194397773)

[Hình 5 Tấn Công SSH 18](#_Toc194397774)

[Hình 6 Log SSH 18](#_Toc194397776)

[Hình 7 Script 19](#_Toc194397785)

[Hình 8 Tấn công apache 20](#_Toc194397803)

[Hình 9 Tấn công nginx 22](#_Toc194397812)

[Hình 10 Log Apache 23](#_Toc194397813)

# CHƯƠNG 1 TỔNG QUAN

## BỐI CẢNH ĐỀ TÀI

Trong thời đại công nghệ thông tin phát triển mạnh mẽ, an ninh mạng đã trở thành một trong những vấn đề quan trọng và cấp bách đối với các hệ thống máy chủ và doanh nghiệp. Các cuộc tấn công mạng ngày càng tinh vi, trong đó **brute-force attack** là một phương thức phổ biến được tin tặc sử dụng để dò tìm mật khẩu trái phép nhằm truy cập hệ thống.

Một trong những giải pháp hiệu quả để ngăn chặn **brute-force attack** trên hệ điều hành Linux là **Fail2Ban**. Đây là một công cụ giám sát nhật ký hệ thống, phát hiện các hành vi đăng nhập thất bại liên tục và tự động chặn địa chỉ IP có dấu hiệu tấn công.

## 1.2 MỤC TIÊU NGHIÊN CỨU

Mục tiêu chính của đồ án là nghiên cứu và triển khai **Fail2Ban** để bảo vệ hệ thống Linux khỏi các cuộc tấn công brute-force. Cụ thể, đồ án sẽ tập trung vào:

* Nghiên cứu về **brute-force attack**, cơ chế hoạt động và tác động của nó đối với hệ thống.
* Tìm hiểu cách hoạt động của **Fail2Ban** và ứng dụng trong bảo mật hệ thống Linux.
* Hướng dẫn cài đặt, cấu hình **Fail2Ban** trên hệ điều hành **CentOS 7** để bảo vệ các dịch vụ như **SSH, Apache/Nginx**.
* Thử nghiệm, đánh giá hiệu quả của **Fail2Ban** trong việc ngăn chặn các cuộc tấn công brute-force.

## 1.3 PHẠM VI NGHIÊN CỨU

* Tìm hiểu nguyên lý hoạt động của **brute-force attack** và tác động của nó.
* Nghiên cứu cách hoạt động và cơ chế bảo vệ của **Fail2Ban**.
* Cài đặt, cấu hình và thử nghiệm Fail2Ban trên hệ điều hành **CentOS 7**.
* Đánh giá hiệu quả của Fail2Ban trong việc bảo vệ dịch vụ SSH và Web Serve

## 1.4 PHƯƠNG PHÁP NGHIÊN CỨU

* **Nghiên cứu lý thuyết**: Tìm hiểu các tài liệu về brute-force attack, Fail2Ban và các phương pháp phòng chống.
* **Thực nghiệm**: Cài đặt Fail2Ban trên hệ thống Linux, mô phỏng các cuộc tấn công brute-force và quan sát cách Fail2Ban phản ứng.
* **Đánh giá và phân tích**: So sánh trước và sau khi áp dụng Fail2Ban để đo lường hiệu quả bảo mật.

# CHƯƠNG 2 CƠ SỞ LÝ THUYẾT

## 2.1 GIỚI THIỆU VỀ LÝ THUYẾT

### **2.1.1 Tấn công brute-force là gì?**

Tấn công brute-force là một phương thức tấn công mà trong đó, tin tặc sử dụng **phương pháp thử và sai** (trial and error) để đoán đúng mật khẩu hoặc key bảo mật. Tin tặc sẽ thử hàng loạt các mật khẩu hoặc tên người dùng cho đến khi tìm được sự kết hợp chính xác. Các công cụ tấn công brute-force hiện đại có thể tự động hóa quá trình này và tấn công hàng nghìn tài khoản trong thời gian ngắn.

* Các dấu hiệu nhận diện tấn công brute-force có thể là:
* **Tần suất cao các yêu cầu đăng nhập thất bại** từ một IP trong khoảng thời gian ngắn.
* **Dùng nhiều tài khoản đăng nhập** với mật khẩu sai.
* **Quá trình đăng nhập liên tục** mà không có thời gian nghỉ.

### **2.1.2 Các loại brute-force attack**

* **Brute-force đơn giản**: Thử tất cả các kết hợp của tên đăng nhập và mật khẩu, phương pháp này rất đơn giản nhưng tốn thời gian. Ví dụ: Tin tặc thử lần lượt các mật khẩu như "password", "123456", "admin", v.v.
* **Brute-force dictionary**: Thay vì thử tất cả các tổ hợp có thể, tin tặc sử dụng một **danh sách các mật khẩu phổ biến** (dictionary) để thử nghiệm. Các từ như "qwerty", "welcome123", hay "letmein" là ví dụ.
* **Hybrid brute-force**: Kết hợp brute-force với các biến thể. Ví dụ, thử các mật khẩu có kèm theo số hoặc ký tự đặc biệt (ví dụ: "password123!", "welcome123@"...).
* **Reverse brute-force**: Thử nghiệm một mật khẩu phổ biến trên nhiều tài khoản khác nhau, ví dụ: sử dụng mật khẩu "123456" và thử trên hàng trăm tài khoản email khác nhau.
* **Credential stuffing**: Dựa trên **dữ liệu bị rò rỉ** từ các vi phạm bảo mật trước đó, tin tặc sử dụng thông tin đăng nhập đã bị lộ để tấn công các tài khoản ở các dịch vụ khác nhau.

**2.1.3 Hậu quả của brute-force attack**

Các cuộc tấn công brute-force có thể dẫn đến thiệt hại nghiêm trọng cho hệ thống và người sử dụng. Một số hậu quả chính của brute-force attack bao gồm:

* + **Xâm nhập hệ thống trái phép**: Các kẻ tấn công có thể truy cập các tài khoản và hệ thống quan trọng nếu họ thành công trong việc đoán mật khẩu.
  + **Đánh cắp thông tin nhạy cảm**: Tin tặc có thể đánh cắp thông tin cá nhân, tài chính hoặc các dữ liệu quan trọng từ hệ thống.
  + **Lợi dụng tài nguyên hệ thống**: Các cuộc tấn công brute-force có thể làm giảm hiệu suất của máy chủ do yêu cầu tài nguyên xử lý nhiều và làm tắc nghẽn mạng.
  + **Gián đoạn dịch vụ**: Các cuộc tấn công brute-force có thể gây ảnh hưởng đến hiệu suất của ứng dụng, đặc biệt nếu hệ thống không có biện pháp bảo vệ như Fail2Ban.
  + **Lây nhiễm phần mềm độc hại**: Trong một số trường hợp, tin tặc có thể khai thác quyền truy cập vào hệ thống để cài đặt phần mềm độc hại, khiến hệ thống bị xâm phạm nghiêm trọng.

### **2.1.4 Các phương pháp phòng chống brute-force attack**

Một trong những phương pháp bảo vệ hiệu quả chống lại brute-force attack là **sử dụng Fail2Ban**. Đây là công cụ giúp giám sát các file log của hệ thống, phát hiện hành vi tấn công brute-force (các lần đăng nhập thất bại liên tục), và tự động chặn địa chỉ IP của kẻ tấn công bằng cách sử dụng tường lửa.

Fail2Ban giúp giảm thiểu tác động của brute-force attack bằng cách:

* **Sử dụng Fail2Ban:** Giám sát log hệ thống, phát hiện và chặn IP tấn công brute-force tự động bằng tường lửa.
* **Giới hạn số lần đăng nhập:** Hạn chế số lần đăng nhập sai trong một khoảng thời gian để ngăn chặn tấn công.
* **Sử dụng CAPTCHA:** Ngăn chặn bot tự động tấn công bằng cách yêu cầu người dùng giải quyết câu hỏi hoặc xác nhận hình ảnh.
* **Xác thực đa yếu tố (MFA):** Thêm lớp bảo mật yêu cầu xác thực thêm ngoài mật khẩu (ví dụ: mã SMS).
* **Mật khẩu mạnh:** Khuyến nghị sử dụng mật khẩu phức tạp để làm giảm khả năng thành công của tấn công.
* **Đổi cổng SSH mặc định:** Thay đổi cổng SSH mặc định để giảm tấn công tự động.
* **Giới hạn truy cập từ IP đáng tin cậy:** Cho phép truy cập SSH chỉ từ một số địa chỉ IP cụ thể.
* **Giám sát log hệ thống:** Kiểm tra và giám sát nhật ký hệ thống để phát hiện tấn công sớm.

# 

# CHƯƠNG 3 GIỚI THIỆU VỀ FAIL2BAN

## 3.1 Fail2Ban là gì?

Fail2Ban là một công cụ bảo mật mã nguồn mở cho hệ điều hành Linux, được thiết kế để bảo vệ hệ thống khỏi các cuộc tấn công brute-force, tấn công từ chối dịch vụ (DoS), và các cuộc tấn công khác. Công cụ này hoạt động bằng cách theo dõi các **log hệ thống**, phát hiện hành vi bất thường như các lần đăng nhập sai liên tiếp, và tự động **chặn địa chỉ IP** của kẻ tấn công thông qua **tường lửa** (iptables hoặc firewalld).

Fail2Ban không chỉ phát hiện các cuộc tấn công brute-force mà còn có thể được cấu hình để bảo vệ các dịch vụ khác như **SSH**, **FTP**, **Apache**, **Nginx**.

### **3.2 Nguyên lý hoạt động của Fail2Ban:**

Fail2Ban hoạt động dựa trên các bước sau:

* + Giám sát các file log: Fail2Ban theo dõi các file log của hệ thống (ví dụ: /var/log/auth.log, /var/log/secure), nơi các thông tin về các yêu cầu đăng nhập sai được ghi lại.
  + Phát hiện hành vi bất thường: Khi phát hiện một địa chỉ IP thực hiện quá nhiều lần đăng nhập sai, Fail2Ban coi đó là hành vi đáng ngờ (brute-force attack) và đưa địa chỉ IP đó vào danh sách chặn.
  + Chặn địa chỉ IP: Fail2Ban sử dụng iptables hoặc firewalld để chặn địa chỉ IP của kẻ tấn công, ngăn không cho chúng tiếp tục thực hiện tấn công.
  + Gỡ bỏ cấm sau thời gian nhất định: Sau một khoảng thời gian nhất định, địa chỉ IP sẽ được gỡ bỏ khỏi danh sách chặn, giúp hệ thống linh hoạt và không làm gián đoạn quá lâu.

**3.3. Cấu trúc của Fail2Ban**

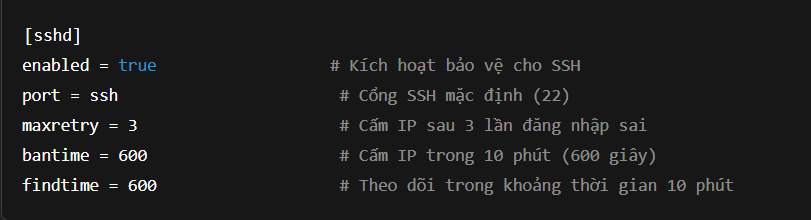
Fail2Ban bao gồm các thành phần chính sau:

* + **Jails**: Đây là các bộ lọc bảo vệ cho các dịch vụ cụ thể, ví dụ như **sshd** (SSH), **apache** (Web Server), **vsftpd** (FTP), v.v. Mỗi jail là một bộ cấu hình được Fail2Ban sử dụng để kiểm tra các hành vi tấn công đối với từng dịch vụ.
  + **Filters**: Filters giúp Fail2Ban nhận diện các hành vi tấn công từ các file log của dịch vụ. Các filter này chứa các biểu thức chính quy (regex) để tìm các lỗi đăng nhập sai.
  + **Actions**: Đây là hành động mà Fail2Ban thực hiện khi phát hiện một hành vi vi phạm. Các hành động này có thể là **chặn IP** bằng iptables, **gửi email cảnh báo**, hoặc thực hiện các biện pháp khác.
  + **Log files**: Các file này ghi lại thông tin về các cuộc tấn công bị chặn. Fail2Ban theo dõi các log này để phát hiện hành vi bất thường và quyết định hành động.

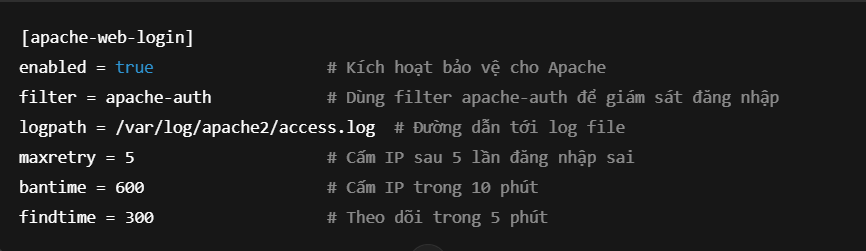
### **3.4. Cấu hình cơ bản của Fail2Ban**

Để cấu hình Fail2Ban, bạn cần chỉnh sửa tệp **/etc/fail2ban/jail.local**. Dưới đây là một ví dụ về cấu hình cơ bản cho dịch vụ **SSH** và **Apache**:

**Cấu hình cho SSH**:



**Cấu hình cho Apache (Web Login)**:



Giải thích:

* enabled = true: Kích hoạt jail này, tức là Fail2Ban sẽ giám sát các sự kiện trên trang web login của bạn.
* filter = apache-web-login: Đây là tên của filter mà Fail2Ban sẽ sử dụng. Filter này cần phải được cấu hình để nhận diện các lần đăng nhập sai trong file log của Apache.
* logpath = /var/www/html/login/login\_attempts.log: Đường dẫn đến file log nơi các thông tin đăng nhập sai được ghi lại. Fail2Ban sẽ giám sát file này để phát hiện các hành vi brute-force.
* maxretry = 3: Fail2Ban sẽ cấm IP sau 3 lần đăng nhập sai liên tiếp.
* findtime = 300: Khoảng thời gian tính từ lần đầu tiên đăng nhập sai đến lần cuối. Fail2Ban sẽ theo dõi hành vi này trong vòng 5 phút (300 giây).
* bantime = 600: Sau khi bị ban, IP sẽ bị cấm trong vòng 10 phút.
* action = %(action\_mwl)s: Hành động của Fail2Ban sau khi phát hiện tấn công. %action\_mwl% là một hành động gửi email cảnh báo.

**3.5. Các lợi ích của Fail2Ban**

* **Tự động chặn các cuộc tấn công brute-force**: Fail2Ban giúp giảm thiểu nguy cơ bị xâm nhập hệ thống.
* **Dễ dàng cấu hình và tùy chỉnh**: Người dùng có thể thay đổi số lần thử sai, thời gian cấm IP theo nhu cầu.
* **Tích hợp với iptables, firewalld, ufw**: Hỗ trợ nhiều phương pháp chặn IP.
* **Giúp phát hiện các cuộc tấn công sớm**: Fail2Ban không chỉ chặn mà còn giúp giám sát các hoạt động đáng ngờ trên hệ thống.

**3.6. Hạn chế của Fail2Ban**

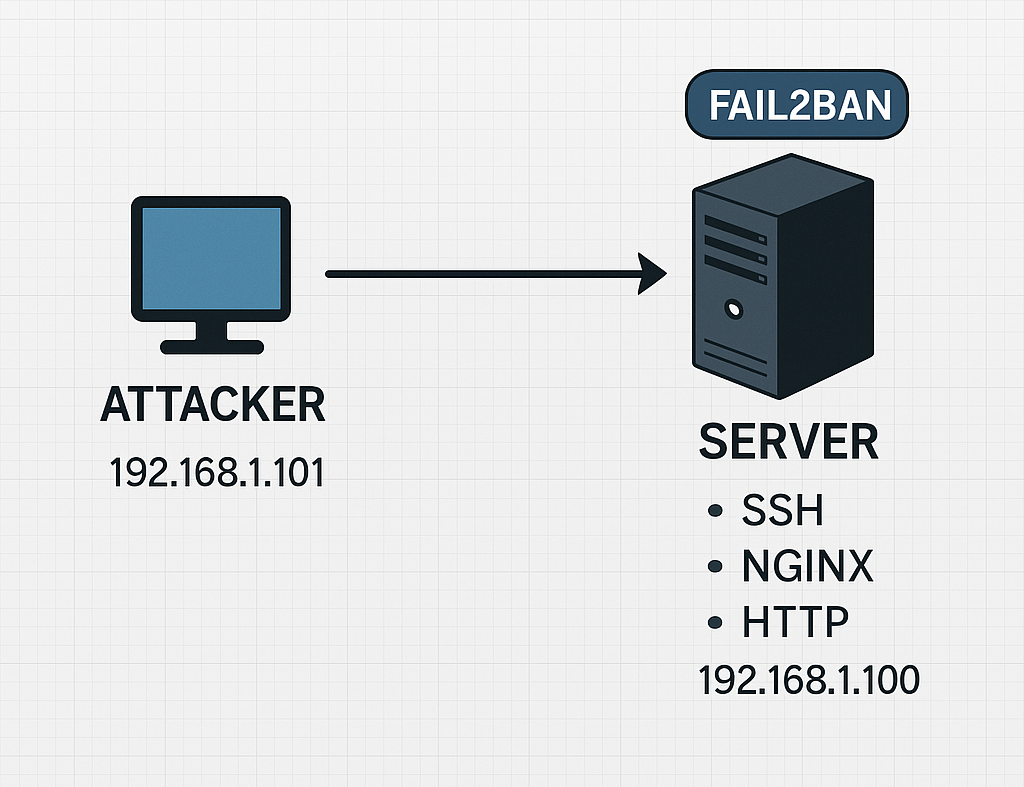
* **Không bảo vệ được trước các cuộc tấn công phân tán (Distributed Brute-force Attack)**: Nếu tin tặc sử dụng nhiều IP khác nhau để tấn công, Fail2Ban sẽ khó phát hiện.
* **Cần tùy chỉnh hợp lý để tránh false positive**: Nếu cấu hình quá nghiêm ngặt, người dùng hợp lệ có thể bị chặn nhầm.
* **Không thể chặn các cuộc tấn công khác ngoài brute-force**: Fail2Ban không thể ngăn chặn tấn công DDoS hoặc các hình thức tấn công nâng cao khác

# CHƯƠNG 4 MÔ HÌNH THỬ NGHIỆM

**4.1. Mục đích thử nghiệm**

Mô hình thử nghiệm được xây dựng nhằm kiểm tra hiệu quả của **Fail2Ban** trong việc phát hiện và ngăn chặn các cuộc tấn công **brute-force** trên hệ điều hành **CentOS 7**. Mô hình này sẽ giúp đánh giá mức độ bảo vệ của Fail2Ban đối với các dịch vụ **Web Login**

**4.2. Môi trường thử nghiệm**



**4.3. Quy trình thử nghiệm**

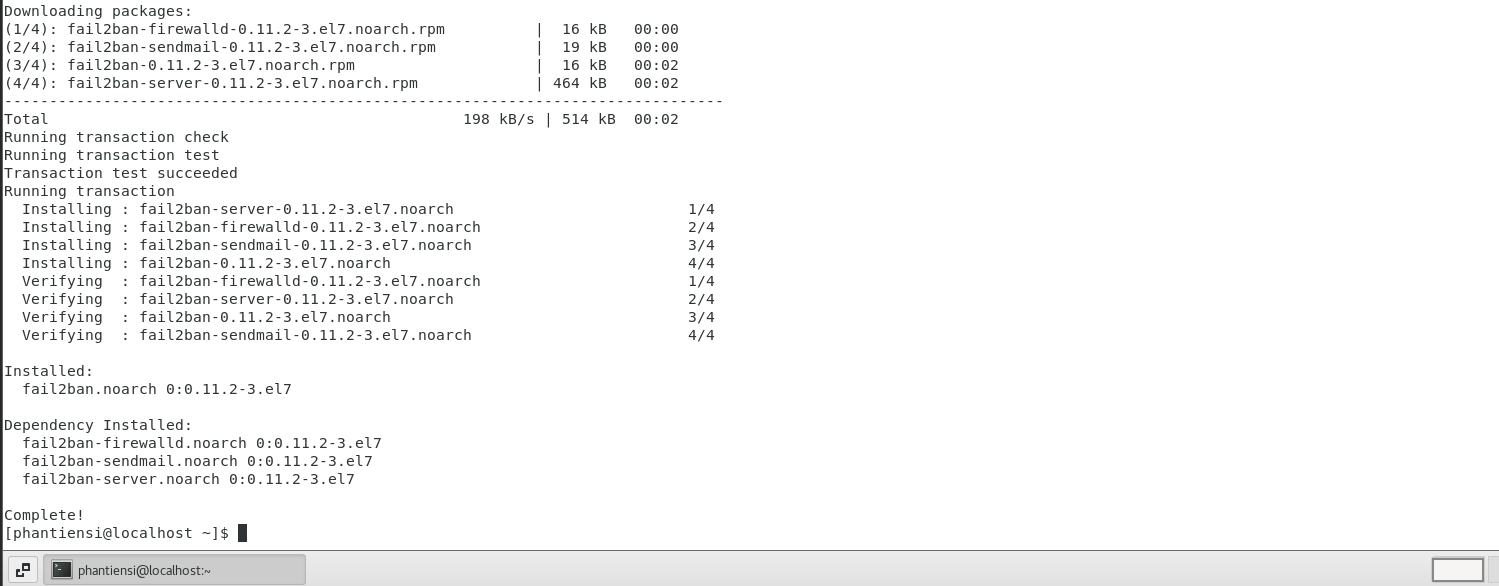
**Bước 1: Cài và bật Fail2ban**

sudo yum install epel-release -y

sudo yum install fail2ban -y

sudo systemctl enable fail2ban

sudo systemctl start fail2ban

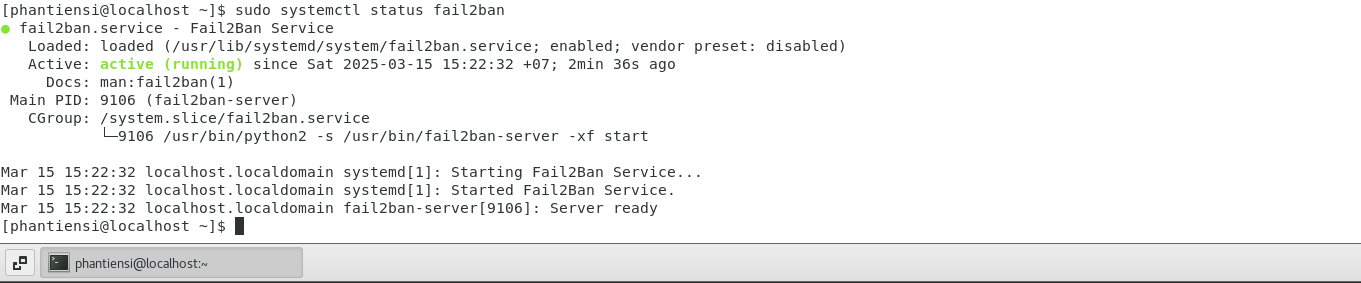


Hình 1 Cài đặt Fail2Ban

Khởi động lại Fail2Ban

Systemctl restart fail2ban

Kiểm tra trạng thái : sudo fail2ban-client status sshd



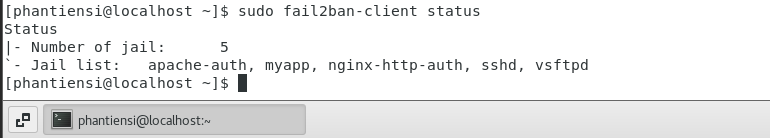
Hình 2 Kiểm tra trạng thái

**Bước 2: Cấu hình jail.local**

****

Hình 3 Cấu hình jail

sudo fail2ban-client status



Hình 4 status

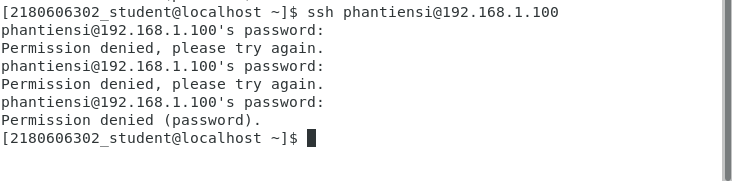
**Bước 4: Tấn Công**

**1 . SSH**

**Mục tiêu:** Đăng nhập sai nhiều lần vào SSH.

Nhập sai mật khẩu 3 lần → Fail2Ban sẽ chặn IP sau lần thứ 3.

Máy tấn công

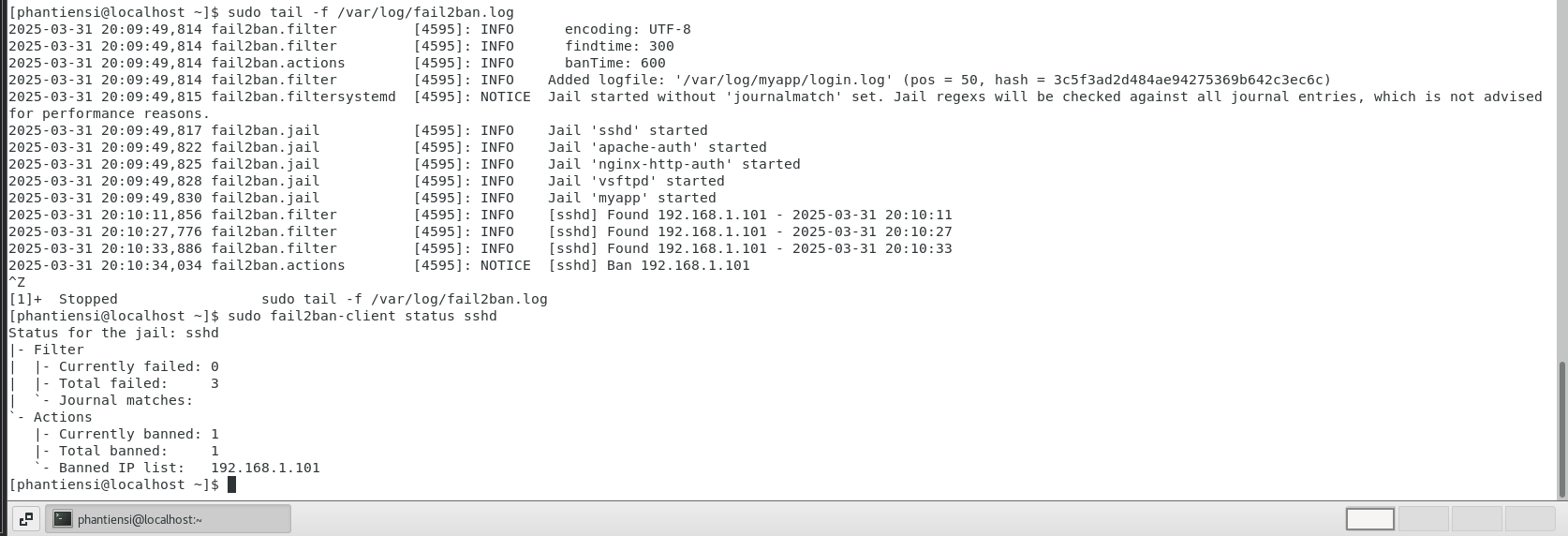


Hình 5 Tấn Công SSH

Kiểm tra máy server

sudo tail -f /var/log/fail2ban.log

sudo fail2ban-client status sshd

****

Hình 6 Log SSH

**Bước 5 :** Gỡ ban nếu cần

sudo fail2ban-client set sshd unbanip 192.168.1.101

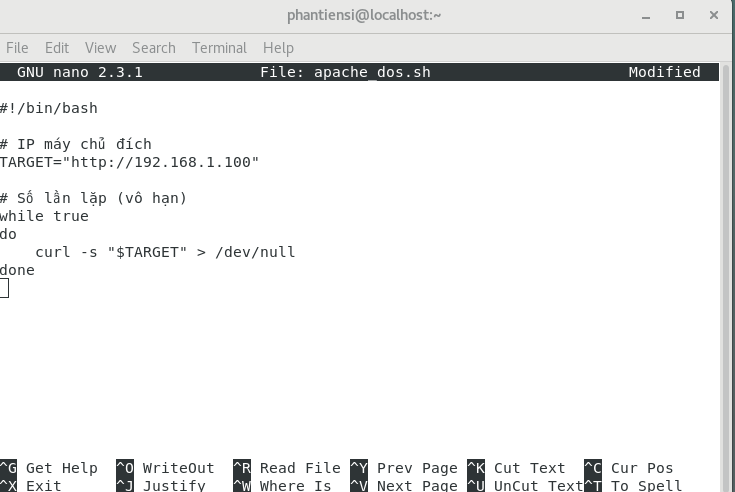
1. **. Apache**

Mục tiêu: Gửi **liên tục số lượng lớn các HTTP request** đến máy chủ Apache, gây:

* Tăng tải CPU, RAM máy chủ
* Gây chậm phản hồi hoặc nghẽn truy cập cho người dùng thật
* Ghi log dày đặc (tăng log /var/log/httpd/access\_log)

BƯỚC 1: Bước 1: Tạo file script

nano apache\_dos.sh



Hình 7 Script

BƯỚC 2: CẤU HÌNH JAIL

sudo nano /etc/fail2ban/jail.local

thêm

[apache-dos]

enabled = true

port = http,https

filter = apache-dos

logpath = /var/log/httpd/access\_log

maxretry = 20

findtime = 60

bantime = 600

BƯỚC 3: VIẾT CODE TẤN CÔNG (Từ máy tấn công)

for i in {1..100}; do curl -s http://192.168.1.100/ > /dev/null; done

BƯỚC 4: Kiểm tra

sudo fail2ban-client status apache-dos

sudo tail -f /var/log/fail2ban.log



Hình 8 Tấn công apache

Gỡ ban nếu cần

sudo fail2ban-client set apache-dos unbanip 192.168.1.101

**3 . Nginx (nginx-http-auth)**

**Mục tiêu:** Gửi nhiều request **401 Unauthorized** để vượt maxretry.

BƯỚC 1: CÀI ĐẶT NGINX (nếu chưa có)

sudo yum install epel-release -y

sudo yum install nginx -y

sudo systemctl start nginx

sudo systemctl enable nginx

BƯỚC 2: BẬT BASIC AUTH CHO NGINX

**2.1. Tạo thư mục bảo vệ (ví dụ /usr/share/nginx/html/secure)**

sudo mkdir /usr/share/nginx/html/secure

echo "This is a secure zone" | sudo tee /usr/share/nginx/html/secure/index.html

**2.2. Cài httpd-tools để dùng htpasswd**

sudo yum install httpd-tools -y

**2.3. Tạo user/password**

sudo htpasswd -c /etc/nginx/.htpasswd testuser

BƯỚC 3: CẤU HÌNH NGINX SỬ DỤNG BASIC AUTH

sudo nano /etc/nginx/conf.d/secure.conf

server {

listen 80;

server\_name localhost;

location /secure {

auth\_basic "Restricted";

auth\_basic\_user\_file /etc/nginx/.htpasswd;

root /usr/share/nginx/html;

index index.html;

}

}

3.1. Kiểm tra cấu hình và reload

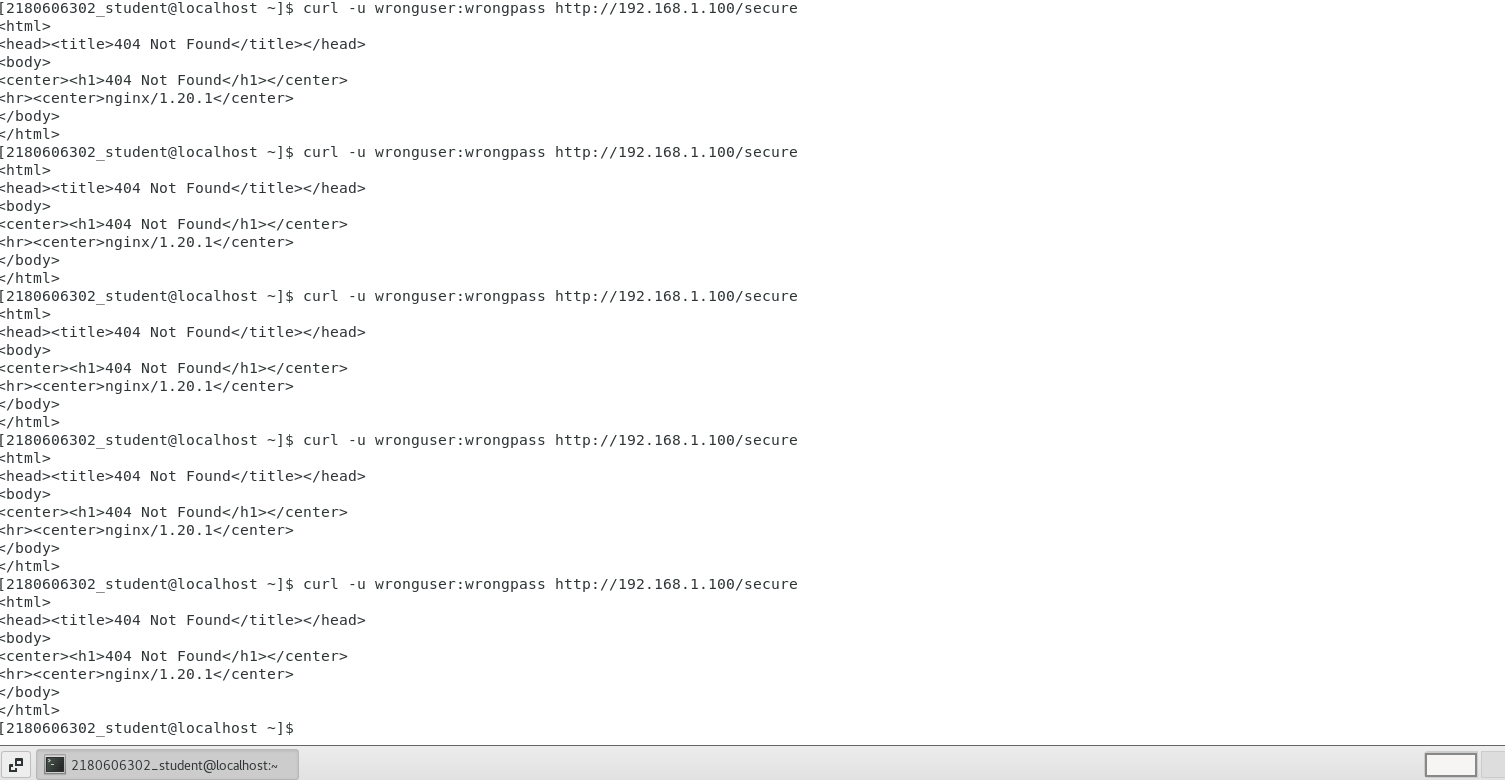
sudo nginx -t

sudo systemctl restart nginx

BƯỚC 4: TẤN CÔNG

Chạy lệnh trên **4-5 lần liên tiếp** để vượt maxretry=3.

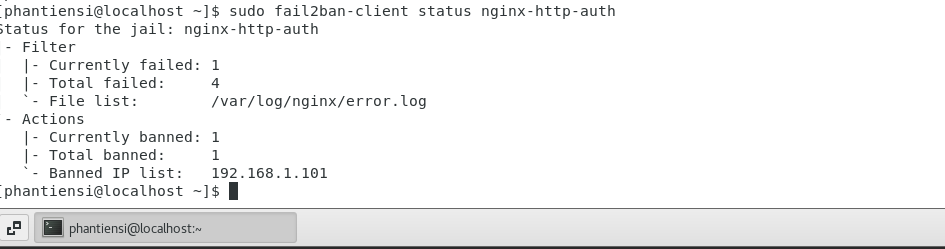
curl -u wronguser:wrongpass <http://192.168.1.100/secure>



Hình 9 Tấn công nginx

Kiểm tra trên server





Hình 10 Log Apache

Gở ban nếu cần

sudo fail2ban-client set nginx-http-auth unbanip 192.168.1.101

# **CHƯƠNG 5: KẾT LUẬN VÀ ĐÁNH GIÁ**

**5.1 Kết luận**

1. Fail2Ban là một công cụ hiệu quả trong việc phát hiện các cuộc tấn công brute-force và ngăn chặn các địa chỉ IP của kẻ tấn công.
2. Quá trình triển khai Fail2Ban đã thành công khi cấu hình đúng các filter, jail, và log path. Fail2Ban đã giúp bảo vệ hệ thống web login khỏi các cuộc tấn công đăng nhập sai liên tiếp và cấm các địa chỉ IP trong thời gian quy định.
3. Cảnh báo email: Fail2Ban đã được cấu hình để gửi cảnh báo qua email khi một địa chỉ IP bị chặn, giúp quản trị viên kịp thời nhận diện và xử lý các cuộc tấn công.
4. Tính bảo mật cao: Với cấu hình Fail2Ban, hệ thống có thể tự động bảo vệ mà không cần sự can thiệp thủ công, giúp giảm thiểu các mối đe dọa bảo mật từ các cuộc tấn công brute-force.

**5.2 Đánh giá kết quả**

1. **Hiệu quả của Fail2Ban**:

* Fail2Ban đã hoạt động hiệu quả trong việc **phát hiện và ngăn chặn các cuộc tấn công brute-force**. Trong quá trình thử nghiệm, hệ thống đã **ban địa chỉ IP** sau khi đạt giới hạn số lần đăng nhập sai và đã **gửi email cảnh báo** đúng như kỳ vọng.
* Việc **gửi email cảnh báo** thành công đã giúp hệ thống bảo mật được giám sát tự động và dễ dàng nhận diện hành vi tấn công.

1. **Các thử nghiệm**:

* Qua các thử nghiệm **đăng nhập sai mật khẩu** trên web login, Fail2Ban đã thực hiện **cấm IP tấn công** sau một số lần đăng nhập sai theo cấu hình, và quá trình này diễn ra hoàn toàn tự động.
* Email cảnh báo đã được gửi đúng khi IP bị ban, cho thấy hệ thống bảo mật hoạt động hiệu quả.

1. **Khả năng mở rộng**:

* Hệ thống **Fail2Ban** có thể dễ dàng mở rộng để bảo vệ thêm nhiều dịch vụ khác (SSH, FTP, v.v.) chỉ với một vài thay đổi nhỏ trong cấu hình.
* Việc áp dụng **Fail2Ban** vào các hệ thống khác sẽ giúp tăng cường bảo mật tổng thể và giảm thiểu nguy cơ tấn công.

**TÀI LIỆU THAM KHẢO**

1. **Fail2Ban Documentation:** <https://www.fail2ban.org/wiki/index.php/Main_Page>
2. **Hydra Official Documentation**:
3. <https://github.com/vanhauser-thc/thc-hydra>
4. **CentOS Security Guide:**

<https://www.centos.org/docs/>