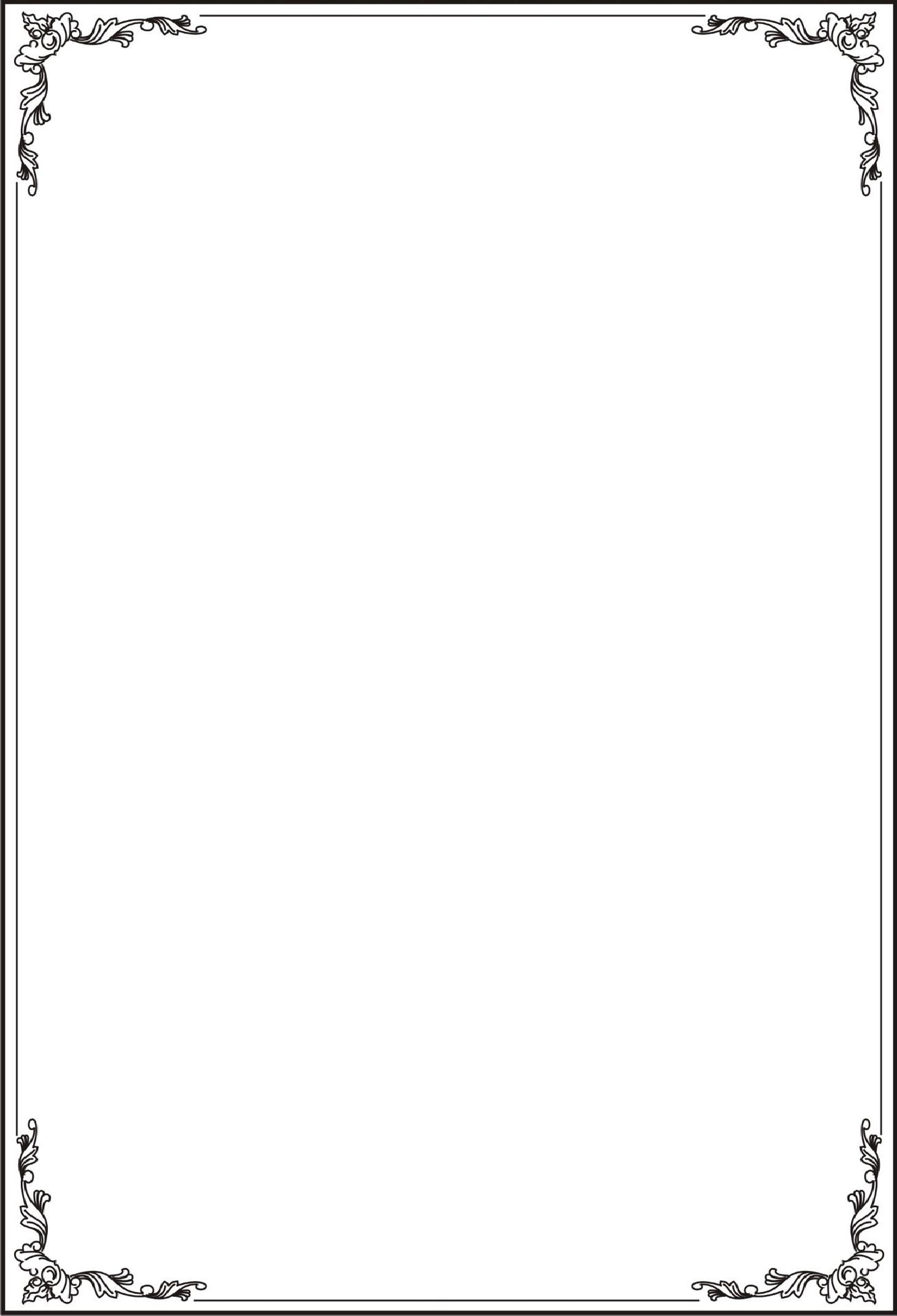
****

**TRƯỜNG ĐẠI HỌC TÀI NGUYÊN VÀ MÔI TRƯỜNG**

**THÀNH PHỐ HỒ CHÍ MINH**

**KHOA HỆ THỐNG THÔNG TIN VÀ VIỄN THÁM**



**BÁO CÁO ĐỒ ÁN MÔN HỌC**

**BẢO MẬT MẠNG MÁY TÍNH VÀ HỆ THỐNG**

**NGHIÊN CỨU GIAO THỨC SRP**

**(SECURE REMOTE PASWORD) VÀ ỨNG DỤNG**

Giảng viên hướng dẫn: **ThS. Phạm Trọng Huynh**

Nhóm sinh viên thực hiện: **06**

Lớp**: 09\_ĐH\_CNPM3**

Khoá**: 2020 - 2024**

***TP. Hồ Chí Minh, tháng 04 năm 2024***

**TRƯỜNG ĐẠI HỌC TÀI NGUYÊN VÀ MÔI TRƯỜNG**

**THÀNH PHỐ HỒ CHÍ MINH**

**KHOA HỆ THỐNG THÔNG TIN VÀ VIỄN THÁM**

A logo with a person holding a book

Description automatically generated

**BÁO CÁO ĐỒ ÁN MÔN HỌC**

**BẢO MẬT MẠNG MÁY TÍNH VÀ HỆ THỐNG**

**NGHIÊN CỨU GIAO THỨC SRP**

**(SECURE REMOTE PASWORD) VÀ ỨNG DỤNG**

|  |  |  |
| --- | --- | --- |
| **Nhóm sinh viên thực hiện: Nhóm 6** | | |
| **Nguyễn Thanh Hơn** | **:** | **0950080108** |
| **Phạm Quang Huy** | **:** | **0950080109** |
| **Âu Dương Đức Trung** | **:** | **0950080114** |

***TP. Hồ Chí Minh, tháng 01 năm 202******4***

**LỜI CẢM ƠN**

Để hoàn thành bài báo cáo này lời đầu tiên chúng em xin bày tỏ lòng biết ơn sâu sắc đến thầy Phạm Trọng Huynh đã tận tình hướng dẫn cũng như nhận xét, góp ý trong suốt quá trình học để chúng em có bài báo cáo được hoàn chỉnh nhất. Qua những buổi học thầy và cô đều truyền đạt bài học và kiến thức để chúng em dễ dàng tiếp thu được. Chúng em rất biết ơn thầy và cô vì những gì đã làm cho sinh viên nói chung và nhóm em nói riêng.

Tiếp theo xin chân thành gửi lời cảm ơn đến Ban giám hiệu trường Đại học Tài nguyên và môi trường, quý thầy cô khoa Hệ thống Thông tin và Viễn thám đã tận tâm giảng dạy và truyền đạt những kiến thức, kinh nghiệm quý báu cho chúng em. Không chỉ truyền đạt kiến thức, kinh nghiệm mà Ban giám hiệu nhà trường đã cố gắng hỗ trợ thiết bị và cơ sở vật chất để chúng em được học tập tốt hơn.

Nhóm sinh viên thực hiện

Nhóm 6 - 09\_ĐH\_CNPM3

**NHẬN XÉT**

**(Của giảng viên giảng dạy)**

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

………….., ngày….tháng….năm……

NGƯỜI NHẬN XÉT

*(ký tên)*

# MỤC LỤC

[DANH MỤC CÁC BẢNG, HÌNH 7](#_Toc164118476)

[Chương 1: TỔNG QUAN 2](#_Toc164118477)

[1.1 Xâm nhập mạng là gì ? 2](#_Toc164118478)

[1.2 Phát hiện xâm nhập mạng 2](#_Toc164118479)

[1.3 Các hình thức tấn công mạng 4](#_Toc164118480)

[1.3.1 Phân loại tấn công mạng 4](#_Toc164118481)

[1.3.2 Các kỹ thuật tấn công 6](#_Toc164118482)

[1.4 Dấu hiệu nhận dạng tấn công mạng 7](#_Toc164118483)

[1.4.1 Dựa vào các gói tin (packets) 7](#_Toc164118484)

[1.4.2 Dựa trên các cảnh báo từ hệ thống IDS 8](#_Toc164118485)

[1.4.3 Phát hiện dựa trên dòng dữ liệu bất thường 9](#_Toc164118486)

[1.5 Giải pháp phát hiện và phòng chống xâm nhập 10](#_Toc164118487)

[1.5.1 Phân chia mạng 10](#_Toc164118488)

[1.5.2 Điều chỉnh quyền truy cập Internet qua máy chủ proxy 11](#_Toc164118489)

[1.5.3 Đặt thiết bị bảo mật chính xác 11](#_Toc164118490)

[1.5.4 Sử dụng NAT (Network Address Translation) 11](#_Toc164118491)

[1.5.5 Giám sát lưu lượng mạng 11](#_Toc164118492)

[1.5.6 Sử dụng công nghệ “đánh lừa” 12](#_Toc164118493)

[Chương 2: GIAO THỨC SECURE REMOTE PASSWORD (SRP) 13](#_Toc164118494)

[2.1 Khái niệm 13](#_Toc164118495)

[2.2 Ưu và nhược điểm của Secure Remote Password 13](#_Toc164118496)

[2.2.1 Ưu điểm 13](#_Toc164118497)

[2.2.2 Nhược điểm 14](#_Toc164118498)

[2.3 Ứng dụng Secure Remote Password 14](#_Toc164118499)

[Chương 3: CÀI ĐẶT THỬ NGHIỆM 16](#_Toc164118500)

[3.1 Phương pháp tính 16](#_Toc164118501)

[3.2 Demo 17](#_Toc164118502)

[Chương 4: KẾT LUẬN 21](#_Toc164118503)

[4.1 Kết quả đạt được của đề tài 21](#_Toc164118504)

[4.2 Hạn chế của đề tài 21](#_Toc164118505)

[4.3 Hướng phát triển 21](#_Toc164118506)

[TÀI LIỆU THAM KHẢO 22](#_Toc164118507)

# DANH MỤC CÁC BẢNG, HÌNH

[Hình 1: Định nghĩa các cảnh báo trong hệ thống IDS 9](#_Toc164118245)

[Hình 2: Phát hiện bất thường dựa trên dòng dữ liệu 10](#_Toc164118246)

[Hình 3 Trình tự xác thực giữa người dùng – máy chủ 17](#_Toc164118247)

[Hình 4 Điền tham số cho N, g, k 18](#_Toc164118248)

[Hình 5 Tính toán tham số x và v 18](#_Toc164118249)

[Hình 6 Người dùng điền mật khẩu và tính toán các tham số A, x và S 19](#_Toc164118250)

[Hình 7 Máy chủ tính toán các tham số B, u, b, S 20](#_Toc164118251)

[Hình 8 Thông báo khi trùng khớp tham số S 20](#_Toc164118252)

[Hình 9 Thông báo khi không trùng khớp tham số S 20](#_Toc164118253)

**KÍ HIỆU CÁC CỤM TỪ VIẾT TẮT**

|  |  |
| --- | --- |
| Từ viết tắt | Chú giải |
| SRP | Secure Remote Password |
| IDS | Intrusion Detection System |
| IPS | ntrusion Prevention System |
| DDoS | Distributed Denial of Service |
| IoT | Internet of Things |

**MỞ ĐẦU**

Mạng NSFnet được thành lập và đã kết nối năm trung tâm máy tính vào năm 1986. Cũng vì thế, nó đã đem đến sự bùng nổ trong việc kết nối, đặc biệt ở khu vực các trường đại học. Từ đó, ARPANET và NSF cùng tồn tại song song, sử dụng chung 1 giao thức, và chúng có sự kết nối lẫn nhau. Tiếp đến năm 1990, ARPANET giờ đây là một dự án dừng hoạt động nhưng vì mạng do ARPANET cùng NSF sinh ra đã được áp dụng, vào mục đích là dân dụng đây cũng là tiền thân của Internet ngày nay. Cho đến lúc này mạng Internet được sử dụng chủ yếu bởi đối tượng là những nhà nghiên cứu, đồng thời dịch vụ được dùng phổ biến nhất là FTP và email. Thời điểm này Internet đã được coi như là một phương tiện đại chúng.

Ngày nay Internet được sử dụng phổ biến mọi lúc mọi nơi, từ máy tính để bàn, cá nhân đến điện thoại cũng như các thiết bị thông minh, ngoài ra nó được áp dụng vào nhiều lĩnh vực của đời sống như giáo dục, y tế, kinh tế, quốc phòng. Từ đó cũng phát sinh nên nhiều vấn đề liên quan đến bảo mật cũng như an ninh trên mạng Internet. An ninh mạng là một vấn đề lớn và rất quan trọng với mục tiêu là đảm bảo an ninh môi trường làm việc của cá nhân hay tổ chức. Sự mất mát về thông tin và bảo mật của cho một người dùng có thể sẽ không quá lớn hoặc với một số trường hợp là không đáng để truy cứu, nhưng đối với các doanh nghiệp hay các tổ chức lớn tổn thất có thể lên tới hàng triệu đô la. Hoặc các cơ quan tổ chức thuộc nhà nước sẽ dẫn đến các nguy cơ lộ các thông tin bí mật dẫn đến mối nguy hại cho quốc gia. Hàng loạt các cuộc tấn công có thể nhắm vào mọi thứ như là dữ liệu cá nhân hoặc tổ chức, tài khoản ngân hàng, phần mềm, tài khoản người dùng, mạng cục bộ, … Đó là lý do tại sao các công cụ bảo mật phát triển ngày càng nhiều để đáp ứng các dạng phần mềm nguy hiểm, phần mềm độc hại và tin tặc ngày nay.

Trong thời buổi công nghệ thông tin hiện nay, một trong những yếu tố mà các doanh nghiệp phải ưu tiên xem xét đến là bảo mật thông tin hay an toàn an ninh mạng. Không ít các doanh nghiệp phải thuê đối tác thứ ba với mục đích bảo vệ hệ thống mạng và bảo mật thông tin, ngoài ra cũng có những doanh nghiệp lập nên các kế hoạch về việc tính toán chi phí để mua sản phẩm phần cứng hay phần mềm nhằm đáp

ứng việc đảm bảo an toàn dữ liệu của công ty. Tuy nhiên, những giải pháp này khiến các cơ quan doanh nghiệp luôn phải đau đầu vì phải thực hiện cân đối về chính sách và tài chính hằng năm để đáp ứng mục tiêu là có được giải pháp an toàn tối ưu và chi phí rẻ đảm bảo việc trao đổi thông tin được an toàn, bảo vệ thông tin của công ty trước những mối nguy cơ tấn công của các tội phạm công nghệ.

# TỔNG QUAN

## Xâm nhập mạng là gì ?

Xâm nhập mạng đề cập đến bất kỳ hoạt động trái phép nào trên mạng. Xâm nhập mạng có hai loại, một là xâm nhập mạng để kiểm thử hay còn gọi là pentest, hai là tấn công mạng. Kiểm thử xâm nhập là hành động xâm nhập nhằm tìm ra lỗ hổng bảo mật trong hệ thống để khắc phục. Sau khi tìm ra các lỗ hổng nghiêm trọng hoặc nguy hiểm, người kiểm thử sẽ đưa ra giải pháp để vá lỗ hổng nhằm bảo vệ tài nguyên của các tổ chức được bảo mật. Ngược lại, tấn công mạng là hành động lợi dụng mạng Internet để xâm nhập trái phép vào hệ thống website của cá nhân, tổ chức hay máy tính hoặc nguy hiểm hơn là cơ sở dữ liệu, … Mục đích chính của việc này là để đánh cắp thông tin, mã hóa dữ liệu hoặc làm gián đoạn các hoạt động vận hành của tổ chức cũng như doanh nghiệp. Những đối tượng của các cuộc tấn công này có thể là cá nhân, tổ chức, doanh nghiệp lớn nhỏ hoặc các cơ quan nhà nước. Đặc biệt, đối tượng phổ biến nhất bị nhắm đến là các doanh nghiệp bởi vì mục tiêu chính của những kẻ tấn công này là lợi nhuận. Những tin tặc tấn công chủ yếu nhằm trục lợi phi pháp, tống tiền các doanh nghiệp. Ngoài ra, cũng tồn tại một số doanh nghiệp cạnh tranh không lành mạnh tấn công mạng đối thủ của mình bằng cách đánh sập website của họ. Điều này gây ảnh hưởng ít nhiều đến hình ảnh và uy tín của công ty, thương hiệu.

## Phát hiện xâm nhập mạng

Phát hiện xâm nhập mạng là tập hợp các phương pháp và kỹ thuật dùng để dò tìm những hoạt động có dấu hiệu bất thường, đáng nghi ngờ trên mạng. Một tập hợp các phương thức, công cụ, và tài nguyên giúp cho người quản trị xác định, đánh giá, và báo cáo các hoạt động không được cho phép trên mạng được định nghĩa là hệ thống phát hiện xâm nhập (IDS). Phát hiện xâm nhập được hiểu là một tiến trình mà nó được quyết định khi một người dùng chưa được xác thực cố gắng xâm nhập trái phép vào hệ thống mạng. IDS với hàng triệu tình huống được trang bị để nhận dạng tấn công cũng như cập nhật thường xuyên sẽ kiểm tra tất cả các gói tin đi qua nó và quyết định liệu gói tin này có vấn đề gì khả nghi hay không. Vì thế, hệ thống này đã trở nên thực sự quan trọng, đồng thời là lựa chọn hàng đầu trong việc phát hiện và phòng chống xâm nhập mạng.

Công cuộc nghiên cứu và xây dựng hệ thống ngăn chặn và phát hiện xâm nhập (IDS/IPS) đang được nhiều người quan tâm cũng như phát triển và sẽ không ngừng phát triển mạnh mẽ trong thời gian tới. Những sản phẩm thương mại hiện tại trên thị trường đều có chi phí cao, vượt ngoài khả năng đầu tư của nhiều doanh nghiệp lớn nhỏ dẫn đến hệ quả là những nghiên cứu mã nguồn mở về IDS/IPS được đầu tư nghiên cứu và triển khai. Nhìn chung, những nghiên cứu trong nước liên quan đến IDS/IPS bằng mã nguồn mở tuy nhiều nhưng lại tập trung vào Snort. Ngoài ra, các nghiên cứu này vẫn chưa được áp dụng rộng rãi, tồn đọng nhiều hạn chế như: không có giao diện thân thiện; chưa được tích hợp sẵn thành phần báo động, hoặc có thì cũng chỉ giới hạn qua giao diện console hay qua giao diện Web, chính vì thế nó chưa tạo được sự linh động và tiện dụng cho người dùng; do chỉ tập trung nghiên cứu về Snort làm cho các phần mềm mang tính chất đơn lẻ mặc dù nhu cầu tích hợp các tính năng giám sát khác nhằm đạt được hiệu quả sử dụng cao hơn chưa thật sự được chú trọng và phát triển.

Mặt khác, IDS/IPS phải luôn trong tình trạng cập nhật những dấu hiệu tấn công mới vì các kiểu tấn công mạng đang ngày một tinh vi và phức tạp kéo theo những dấu hiệu của chúng liên tục thay đổi. Chuyên viên quản trị mạng có thể dựa vào các phân tích khác chẳng hạn như dấu hiệu bất thường của lưu lượng vào hoặc ra khỏi hệ thống, hoạt động của RAM, CPU, ... để phản ứng kịp thời. Thêm vào đó, hệ thống báo động cần triển khai phải mang tính chất đa dạng với nhiều hình thức, tiện dụng và linh động sẽ mang lại sự hỗ trợ thiết thực cho nhân viên quản trị mạng. Hầu hết các hệ thống có hai đặc điểm chung là tính đa dạng và thay đổi, điều này đã được các nhà nghiên cứu tìm hiểu và chứng minh. Công việc nghiên cứu và triển khai hệ thống giám sát, phát hiện và phòng chống xâm nhập mạng tồn tại các yếu tố: nhanh chóng, chính xác, trực quan, tiện lợi và linh động là một vấn đề cấp thiết trong thực tế

Phát triển một hệ thống giám sát trực quan để theo dõi các diễn biến trên mạng như: lưu lượng ra/vào một Server, Switch hoặc hoạt động của CPU, bộ nhớ,… sẽ giúp người quản trị mạng có những phân tích rõ ràng, nhanh chóng để đưa ra quyết định ứng phó kịp thời khi bị hệ thống bị xâm nhập.

IDS căn cứ vào các dấu hiệu tấn công được triển khai có thể giúp phát hiện một cách nhanh chóng các cuộc tấn công mạng. Khi kết hợp hệ thống với tường lửa sẽ có thể chống lại các cuộc tấn công xâm nhập. Dù vậy, dấu hiệu của từng kiểu tấn công mỗi ngày một tinh vi phức tạp hơn thì hệ thống càng phải được cập nhật thường xuyên những dấu hiệu mới để có thể phát hiện nhanh chóng các bất thường trên mạng, người quản trị mạng có thể dựa vào những đồ thị trực quan về lưu lượng ra vào hệ thống để có những phản ứng kịp thời

Hệ thống báo động cũng cần thiết phải triển khai để gửi thông báo cho người quản trị trong một số trường hợp đặc biệt nghiêm trọng như: Server bỗng nhiên ngưng hoạt động, một dịch vụ mạng nào đó ngưng hoạt động hay có tấn công. Hệ thống có thể được triển khai qua nhiều hình thức khác nhau để phát thông báo như: qua Web, E-mail, tin nhắn SMS đến người quản trị mạng.

## Các hình thức tấn công mạng

### **Phân loại tấn công mạng**

Có nhiều loại tấn công mạng khác nhau theo đó mức độ nguy hiểm cũng khác nhau với từng loại, tuy nhiên có bốn loại tấn công nguy hiểm nhất mang sức mạnh phá hủy hạ tầng mạng một doanh nghiệp như:

#### **Tấn công từ chối dịch vụ(DDdos)**

Đây là loại tấn công rất phổ biến và cũng là một trong những tấn công mạng có khả năng phá hoại website doanh nghiệp lớn nhất. Những cuộc tấn công bằng DDoS đe dọa trực tiếp và ngay lập tức đến sự hoạt động của các trung tâm dữ liệu của các doanh nghiệp. Những kẻ tấn công mạng sẽ có nhiều cơ hội để xây dựng các mạng botnet rộng lớn và sau đó kích hoạt các tấn công DDoS toàn cầu bởi sự gia tăng không ngừng của các thiết bị có kết nối IoT với bảo mật kém. Một chứng minh rõ ràng của điều này là sự cố "tắc nghẽn mạng" vào tháng 6, 2019 đã làm cho Google Cloud phải ngừng hoạt động và nó cũng làm ít nhất 16 sản phẩm vệ tinh của Google phải ngừng hoạt động theo, các sản phẩm này chính là: Gmail, G-Suite, Google Cloud, Google Drive, Google Docs và YouTube…

#### **Tấn công Ransomeware**

Cơ sở hạ tầng doanh nghiệp là mục tiêu được những tội phạm mạng nhắm vào bằng ransomware vì thiệt hại của nó có thể ảnh hưởng lâu dài trên diện rộng. Dẫn chứng cho sự tấn công này là công ty lưu trữ Nayana (Hàn Quốc) bị tấn công bằng ransomware làm cho hàng nghìn website của khách hàng lưu trữ trên máy chủ của công ty bị đình trệ hoạt động suốt nhiều tuần liền. Mặc dù đã chi trả một triệu đô la Mỹ tiền chuộc, song vẫn còn nhiều dịch vụ chưa thật sự được phục hồi. Ngoài việc đe dọa dữ liệu của khách hàng trên máy chủ nhà cung cấp dịch vụ, loại tấn công này còn làm giảm sút lòng tin của khách hàng vào doanh nghiệp kinh doanh. Không chỉ có nguy cơ bị phát tán dữ liệu một cách công khai ở khắp mọi nơi, dữ liệu còn bị thay đổi, làm đe dọa đến tính toàn vẹn vốn có của dữ liệu.

#### **Tấn công từ bên thứ ba**

Vì có thêm một bên thứ ba khác mà các nhà cung cấp dịch vụ bảo mật thường hay gặp phải sự cố khi quản lý bảo mật cho trung tâm dữ liệu của khách hàng. Với mục đích gây hại cho các doanh nghiệp, những kẻ tấn công thường nhắm đến mục tiêu là những nhà cung cấp dịch vụ bảo mật. Cụ thể là vào năm 2019, tổ chức của NordVPN (công ty cung cấp dịch vụ mạng riêng ảo có tính năng bảo mật hàng đầu được đông đảo các doanh nghiệp sử dụng để bảo vệ những dữ liệu nhạy cảm) đã thừa nhận việc một trong số những trung tâm dữ liệu của họ bị tấn công vào năm 2018. Sự việc xảy ra khi họ cài đặt hệ thống truy cập từ xa bởi một bên thứ ba mà chưa thông báo nó cho khách hàng làm dẫn đến tình trạng máy chủ thiếu an toàn.

#### **Tấn công vào ứng dụng web do mật khẩu yếu**

Tuy không gây ảnh hưởng trực tiếp đến những dịch vụ của trung tâm dữ liệu nhưng bù lại những tấn công vào các ứng dụng web hoặc máy chủ, cụ thể như các form đăng nhập vào ứng dụng web vẫn có thể gây ra gián đoạn các dịch vụ web. Việc đặt mật khẩu yếu, kém hoặc mật khẩu dễ đoán của người dùng là nguyên nhân cho những loại tấn công này. Chúng có thể được thực hiện thông qua các cuộc tấn công đến từ ứng dụng web. Với những mục được nhắm từ trước việc tấn công tốn ít băng thông hơn nhưng nó vẫn có thể khiến các dịch vụ web ngừng hoạt động một cách dễ dàng.

Ngoài ra vẫn còn một số loại tấn công khác được sử dụng đến thời điểm hiện nay như:

* **Tấn công điểm cuối (Endpoint attacks)**: Các cuộc tấn công điểm cuối đã đạt được quyền truy cập trái phép vào các thiết bị người dùng, máy chủ hoặc các điểm cuối khác. Loại hình tấn công này gây ảnh hưởng đến các thiết bị khác bằng cách lây nhiễm bằng phần mềm độc hại.
* **Tấn công bằng các phần mềm độc hại (Malware attacks)**: loại tấn công này lây nhiễm tài nguyên CNTT với phần mềm độc hại, cho phép kẻ tấn công thỏa hiệp với các hệ thống, đánh cắp dữ liệu và gây tổn hại đến hại thống. Chúng bao gồm các cuộc tấn công Ransomware (mã độc tống tiền), Spyware (phần mềm gián điệp), Virus, Worm (phần mềm độc hại lây lan với tốc độ nhanh).
* **Các lỗ hổng, khai thác và tấn công (Vulnerabilities, exploits and attacks)**: các lỗ hổng khai thác trong phần mềm được sử dụng trong tổ chức, để có quyền truy cập trái phép, thỏa hiệp hoặc hệ thống phá hoại.
* **Chiến dịch tấn công sử dụng kỹ thuật cao (Advanced persistent threats),** đây là những mối đe dọa nhiều lớp phức tạp, không chỉ bao gồm các cuộc tấn công mạng mà còn cả các loại tấn công khác.

Trong một cuộc tấn công mạng, những kẻ tấn công tập trung vào việc thâm nhập chu vi mạng của công ty và đạt được quyền truy cập vào các hệ thống nội bộ. Thông thường, khi kẻ tấn công vào được bên trong hệ thống chúng sẽ kết hợp các loại tấn công khác, ví dụ như ảnh hưởng đến điểm cuối, lan truyền phần mềm độc hại hoặc khai thác lỗ hổng trong một hệ thống trong mạng.

### **Các kỹ thuật tấn công**

Bên cạnh các loại tấn công trên, các kỹ thuật tấn công mạng cũng chuyển biến khôn lường từ các kỹ thuật cơ bản, tuy nhiên mức độ nguy hiểm khi bị tấn công khó lường trước được và gây ra những hậu quả nghiêm trọng nếu không được phát hiện kịp thời. Một số các kỹ thuật tấn công mạng phổ biến như:

* **Truy cập trái phép (Unauthorized access):** Truy cập trái phép đề cập đến những kẻ tấn công truy cập mạng mà không nhận được sự cho phép. Các nguyên nhân của cuộc tấn công truy cập trái phép thường là do mật khẩu yếu, thiếu bảo vệ các tài khoản xã hội, các tài khoản bị xâm nhập trước đó và các mối đe dọa nội bộ.
* **Từ chối dịch vụ (Distributed Denial of Service - DDoS):** Những kẻ tấn công xây dựng botnet và sử dụng chúng để hướng lưu lượng truy cập sai vào mạng hoặc máy chủ. DDoS có thể xảy ra ở cấp độ mạng, ví dụ bằng cách gửi khối lượng khổng lồ của các gói SYN / ACK có thể áp đảo một máy chủ hoặc ở cấp độ ứng dụng.
* **Tấn công Man-in-the-Middle (MitM):** loại tấn công này liên quan đến những kẻ tấn công chặn lưu lượng, giữa các trang web và trang bên ngoài hoặc bên trong mạng. Nếu các giao thức truyền thông không được bảo mật hoặc kẻ tấn công tìm cách vượt qua bảo mật, họ có thể đánh cắp dữ liệu đang được truyền đi, có được thông tin đăng nhập của người dùng và chiếm quyền điều khiển tài khoản của họ.
* **Tấn công cơ sở dữ liệu (SQL Injection):** Nhiều trang web chấp nhận đầu vào của người dùng và không xác thực các đầu vào đó. Những kẻ tấn công sau đó có thể điền vào một biểu mẫu hoặc thực hiện cuộc gọi API, truyền mã độc thay vì các giá trị dữ liệu dự kiến. Mã được thực thi trên máy chủ và cho phép kẻ tấn công lợi dụng nó.
* **Tấn công leo thang đặc quyền (Privilege Escalation):** Khi kẻ tấn công xâm nhập mạng, họ có thể sử dụng sự leo thang đặc quyền để mở rộng tầm với của họ. Sự leo thang đặc quyền ngang liên quan đến những kẻ tấn công đạt được quyền truy cập vào các hệ thống bổ sung, liền kề và leo thang thẳng đứng có nghĩa là những kẻ tấn công có được một mức đặc quyền cao hơn cho cùng một hệ thống.
* **Tấn công nội bộ (Insider threats):** hay còn gọi là mối đe dọa nội bộ. Đây là mối đe dọa đối với tổ chức đến từ những người thuộc tổ chức đó, chẳng hạn như nhân viên, nhân viên cũ, nhà thầu hoặc cộng sự kinh doanh, những người có thông tin nội bộ liên quan đến các phương thức bảo mật, dữ liệu và hệ thống máy tính của tổ chức. Các mối đe dọa nội bộ có thể khó phát hiện và bảo vệ chống lại, vì người trong cuộc không cần thâm nhập mạng để gây hại. Các công nghệ mới như phân tích hành vi người dùng (UEBA) có thể giúp xác định hành vi đáng ngờ hoặc bất thường của người dùng nội bộ, có thể giúp xác định các cuộc tấn công nội bộ.

## Dấu hiệu nhận dạng tấn công mạng

### **Dựa vào các gói tin (packets)**

Nguồn gốc và biểu hiện của một gói tin có thể giúp dự đoán những kết quả của một gói tin được phân phối. Một gói có thể mang một đoạn mã không giống phần mềm độc hại, nhưng khi được lắp lại với các thành phần khác, tạo thành một chương trình phần mềm độc hại. Hoặc một gói có thể chứa dữ liệu để đột nhập vào hệ thống với ID giả có thể không bị phát hiện trong nhiều tuần hoặc vài tháng. Người sở hữu phần mềm độc hại sử dụng tất cả các loại thủ thuật để tránh bị phát hiện.

Bằng cách nhìn vào lưu lượng gói, có thể theo dõi hành vi của gói đó. Ngoài ra, có thể xác định một số loại gói nhất định đang "đánh hơi xung quanh" các khu vực cụ thể vài phút mỗi ngày hoặc vài giờ một tuần. Nếu để ý và quan sát các gói tin, sẽ có thể dễ dàng nhận thấy một cuộc tấn công sắp xảy ra. Thêm vào đó, có thể xác định một gói có khả năng đáng ngờ nếu nó đang giao tiếp với một máy chủ proxy ẩn danh hoặc với các máy chủ nằm ở các quốc gia giả mạo. Lĩnh vực nghiên cứu này, được gọi là phân tích hành vi, đang ngày càng trở nên quan trọng trong an ninh mạng. Các chuyên gia an ninh mạng phải xem xét các kỹ thuật mới để bảo vệ dữ liệu của tổ chức, các nhà cung cấp dịch vụ mạng toàn cầu cần có sự nhìn nhận về chuyển động của một lượng lưu lượng truy cập khổng lồ.

Nghiên cứu các gói tin và lưu lượng truy cập đang trở nên quan trọng hơn khi ngày càng có nhiều các đối tượng, thiết bị và máy móc được kết nối thông qua Internet of Things (IoT). Ngoài máy tính, những kẻ tấn công có thể tìm cách chiếm quyền điều khiển các bộ định tuyến, thiết bị và các thiết bị khác để thực hiện các cuộc tấn công mạng.

Bất cứ ai cũng có thể là một đồng phạm vô tình trong một cuộc tấn công. Một người dùng ngồi vui vẻ trên một tài khoản FaceTime hoặc Skype với đồng nghiệp thậm chí có thể không nhận ra điện thoại thông minh hoặc máy tính xách tay của họ đã bị biến thành một bot tấn công. Người dùng có thể nhận thấy rằng đột nhiên hình ảnh hoặc video bị mờ đi hoặc dừng lại, hoặc âm thanh bị cắt xén. Trong một số trường hợp, những trục trặc này là tác động của một cuộc tấn công đang được tiến hành.

Tin tặc là chuyên gia tìm kiếm các lỗ hổng trong các thiết bị hàng ngày thậm chí trước khi các nhà sản xuất sản phẩm nhận thấy những sai sót. Và một khi tin tặc tìm thấy lỗ hổng, họ sẽ tìm cách khai thác nó. Khi các nhà phân tích an ninh mạng phát hiện các chỉ số về thỏa hiệp (IOC), họ thông báo cho các mục tiêu - bao gồm các tổ chức không phải là khách hàng. Các công ty không biết họ đang bị tấn công cho đến khi các nhà phân tích an ninh mạng nói với họ rằng, giả sử dữ liệu đang được chuyển từ mạng của họ đến một máy chủ ở Đông Âu hoặc một số điểm đến ngoài ý muốn khác.

### **Dựa trên các cảnh báo từ hệ thống IDS**

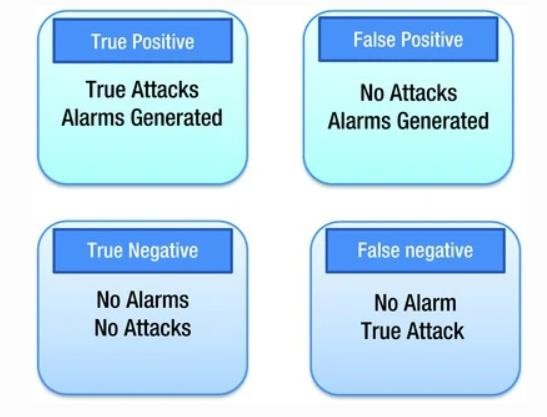
Ngay cả khi có một hệ thống tốt trong việc ghi nhận lịch sử tất cả các lưu lượng truy cập vào mạng nội bộ, thì việc kiểm tra một loạt các lịch sử này chưa mang lại hiệu quả cao. Không thể phân biệt thủ công giữa một gói độc hại và gói mạng tốt. Ngay cả với sự giúp đỡ của máy tính, đây là một công việc chuyên sâu đòi hỏi nhiều sức mạnh xử lý. Trong những năm qua, trong thế giới được kết nối chủ yếu thông qua nhiều phương tiện khác nhau bao gồm máy tính bảng và điện thoại di động, những người xấu với ý định xấu nhắm vào các tập đoàn khác nhau cũng như các cá nhân. Vì không thể phát hiện các cuộc tấn công như vậy theo cách thủ công để ngăn chặn hoặc giảm thiểu chúng, nên bắt buộc phải có một công cụ tự động để giúp giám sát hệ thống cho các cuộc tấn công. IDS đã trở thành một công cụ hữu ích để cung cấp giám sát này. Một số các thuật ngữ cảnh báo trong hệ thống IDS:

Dương tính thật (True Positives): Đây là những cảnh báo rằng một cái gì đó đúng và nó thật sự đúng. Ví dụ: IDS tìm thấy một gói có chứa mã độc và thực sự đúng là gói có mã độc, như được xác nhận bởi điều tra.

Âm tính thật (True Negatives): Đây là những cảnh báo rằng một cái gì đó là không đúng và nó thật sự không đúng. Ví dụ: IDS tìm thấy một gói là không có vấn đề gì và nó thực sự không có vấn đề gì.

Dương tính giả (False Positives): Đây là những cảnh báo chỉ ra rằng một cái gì đó đúng với một gói tin nhưng thực chất nó là không đúng. Ví dụ: IDS tìm thấy một gói có mã độc nhưng nó thực sự là một mã không độc.

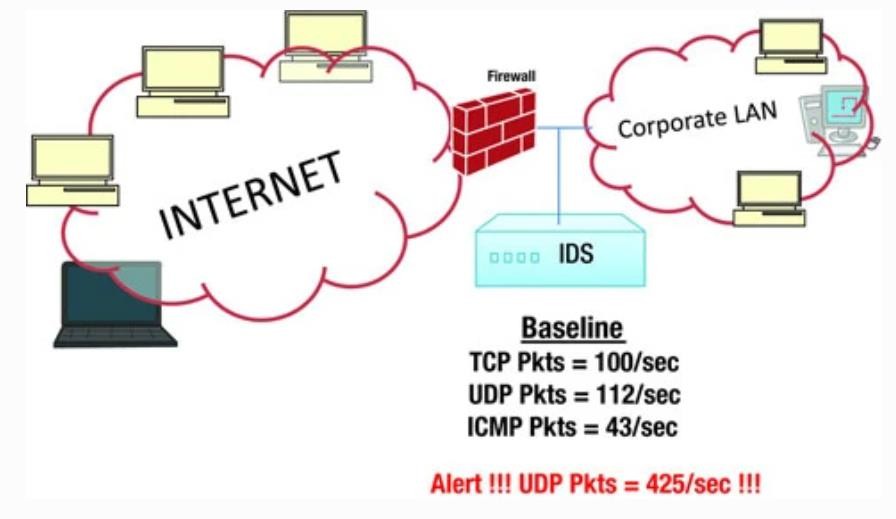
Âm tính giả (False Negatives): Đây là những cảnh báo rằng một cái gì đó là không đúng khi thực chất nó là đúng. Ví dụ: IDS thấy rằng một gói không có bất kỳ mã độc nào nhưng nó thực sự chứa một mã độc, như được tìm thấy thông qua điều tra.



Hình 1: Định nghĩa các cảnh báo trong hệ thống IDS

### **Phát hiện dựa trên dòng dữ liệu bất thường**

Phát hiện dựa trên bất thường bảo vệ chống lại các mối đe dọa chưa biết. Nếu bất kỳ lưu lượng truy cập nào được tìm thấy là bất thường từ đường cơ sở, thì một cảnh báo được kích hoạt bởi các ID bị nghi ngờ là sự xâm nhập. IDP trước tiên tạo ra một cấu hình cơ sở thể hiện hành vi bình thường của lưu lượng truy cập. Hồ sơ cơ sở được tạo bằng cách cho phép hệ thống IDS tìm hiểu lưu lượng truy cập trong một khoảng thời gian để IDP có thể nghiên cứu hành vi di chuyển trong giờ cao điểm, giờ không cao điểm, giờ đêm, giờ đầu kinh doanh. Sau khi học, sự di chuyển của lưu lượng được thu thập trong khoảng thời gian được nghiên cứu thống kê và một hồ sơ cơ sở được tạo ra. Khi IDS được thay đổi từ chế độ học tập sang chế độ phát hiện/phòng ngừa, nó bắt đầu so sánh lưu lượng thông thường với cấu hình được tạo và nếu tìm thấy bất kỳ sự bất thường hoặc sai lệch nào so với hồ sơ cơ sở sự xâm nhập sẽ được ngăn chặn nếu nó được cấu hình cho chế độ phòng ngừa. Cấu hình tùy chỉnh cũng có thể được tạo cho hành vi lưu lượng truy cập cụ thể, chẳng hạn như số lượng e-mail được gửi bởi các nỗ lực truy cập của người dùng.



Hình 2: Phát hiện bất thường dựa trên dòng dữ liệu

Một số dấu hiệu về các hành vi đáng ngờ: quá nhiều phiên đăng nhập Telnet trong một ngày, lưu lượng truy cập HTTP trên một cổng không chuẩn, lưu lượng SNMP bị quá tải.

Để phát hiện xâm nhập hiệu quả, IDS phải có hồ sơ cơ sở mạnh mẽ bao gồm toàn bộ mạng của tổ chức và các phân khúc. Nó sẽ bao gồm hành vi di chuyển bình thường của tất cả các thành phần nhằm mục đích được bao phủ bởi hệ thống phát hiện và phòng ngừa xâm nhập. Hồ sơ cơ sở có thể thay đổi về độ phức tạp từ một nội dung đơn giản đến toàn diện, tùy thuộc vào các đặc điểm của mạng và các thành phần của nó

## Giải pháp phát hiện và phòng chống xâm nhập

Ngoài việc nắm rõ các dấu hiệu của cuộc tấn công, ta cũng cần phải trang bị những giải pháp phát hiện và phòng chống chống xâm nhập mạng như:

### **Phân chia mạng**

Một phần cơ bản của việc tránh các mối đe dọa bảo mật mạng là phân chia mạng thành các khu vực dựa trên các yêu cầu bảo mật. Điều này có thể được thực hiện bằng cách sử dụng các mạng con trong cùng một mạng hoặc bằng cách tạo các mạng cục bộ ảo (VLANS), mỗi loại hoạt động giống như một mạng riêng biệt. Phân khúc giới hạn tác động tiềm ẩn của một cuộc tấn công vào một khu vực và yêu cầu kẻ tấn công thực hiện các biện pháp đặc biệt để thâm nhập và có quyền truy cập vào các khu vực mạng khác

### **Điều chỉnh quyền truy cập Internet qua máy chủ proxy**

Không cho phép người dùng mạng truy cập Internet không được kiểm tra. Vượt qua tất cả các yêu cầu thông qua một proxy trong suốt và sử dụng nó để kiểm soát và giám sát hành vi của người dùng. Đảm bảo rằng các kết nối bên ngoài thực sự được thực hiện bởi một con người và không phải là một bot hoặc cơ chế tự động khác. Các tên miền danh sách trắng để đảm bảo người dùng công ty chỉ có thể truy cập các trang web đã được phê duyệt một cách rõ ràng.

### **Đặt thiết bị bảo mật chính xác**

Tường lửa thường đặt tại vùng biên giới của hệ thống máy tính hay hệ thống mạng. Hoặc tùy vào loại tường lửa như tường lửa cá nhân (Internal Firewall) hay tường lửa hệ thống (System Firewall) mà vị trí đặt cũng như chức năng sẽ có sự khác nhau. Với Internal Firewall thì sau khi được cài đặt thì nó sẽ chiếm giữ việc quản lý tất cả các thông tin đi ra hay đi vào máy tính cá nhân của người dùng. System Firewall sẽ được lắp đặt ngay sau thiết bị kết nối WAN, như Router sử dụng các kênh thuê riêng (leased-line), hay Rounter ADSL … Nếu không thể triển khai tường lửa chính thức ở khắp mọi nơi, hãy sử dụng chức năng tường lửa tích hợp của các thiết bị chuyển mạch và bộ định tuyến, sử dụng hardware firewall hoặc thiết bị chống DdoS để chống tấn công DDoS… Xem xét cẩn thận nơi đặt các thiết bị chiến lược như bộ cân bằng tải - nếu chúng nằm ngoài vùng Demilitarized Zone (DMZ) – vùng nằm giữa LAN và internet (chứa các server và cung cấp các dịch vụ cho các host trong LAN cũng như các host từ các LAN ở bên ngoài), chúng sẽ không được bảo vệ bởi bộ máy bảo mật mạng.

### **Sử dụng NAT (Network Address Translation)**

NAT cho phép dịch địa chỉ IP nội bộ thành địa chỉ có thể truy cập trên các mạng công cộng. Có thể sử dụng nó để kết nối nhiều máy tính với Internet bằng một địa chỉ IP duy nhất. Điều này cung cấp thêm một lớp bảo mật, bởi vì bất kỳ lưu lượng truy cập nào cũng phải đi qua thiết bị NAT.

### **Giám sát lưu lượng mạng**

Đảm bảo có khả năng hiển thị hoàn toàn lưu lượng truy cập đến, đi và mạng nội bộ, với khả năng tự động phát hiện các mối đe dọa và hiểu bối cảnh và tác động của họ. Kết hợp dữ liệu từ các công cụ bảo mật khác nhau để có được một hình ảnh rõ ràng về những gì đang xảy ra trên mạng, nhận ra rằng nhiều cuộc tấn công trải rộng trên nhiều hệ thống CNTT, tài khoản người dùng.

Đạt được mức độ hiển thị này có thể khó khăn với các công cụ bảo mật truyền thống. CYNET 360 là một giải pháp bảo mật tích hợp cung cấp các phân tích mạng tiên tiến, liên tục theo dõi lưu lượng mạng, tự động phát hiện hoạt động độc hại và phản ứng với nó tự động hoặc vượt qua thông tin về ngữ cảnh cho nhân viên bảo mật.

### **Sử dụng công nghệ “đánh lừa”**

Không có biện pháp bảo vệ mạng nào thành công 100% và những kẻ tấn công cuối cùng sẽ thành công trong việc thâm nhập mạng. Nhận ra điều này và đặt công nghệ đánh lừa để tạo ra những mồi nhử trên mạng, những kẻ tấn công bị cám dỗ sẽ "tấn công" và nó cho phép chuyên viên quản trị quan sát kế hoạch và kỹ thuật của kẻ tấn công. Có thể sử dụng mồi nhử để phát hiện các mối đe dọa trong tất cả các giai đoạn của vòng đời tấn công: Tệp dữ liệu, thông tin xác thực và kết nối mạng.

# GIAO THỨC SECURE REMOTE PASSWORD (SRP)

## Khái niệm

Giao thức Secure Remote Password (SRP) là một phương thức xác thực mạnh mẽ dựa trên mật khẩu trong mạng máy tính. Nó cho phép người dùng xác thực mình cho một máy chủ mà không cần gửi mật khẩu thật qua mạng. Thay vào đó, SRP sử dụng một phiên bản dạng băm (hash) của mật khẩu và các thông tin ngẫu nhiên được tạo ra trong quá trình xác thực.

Giao thức SRP có một số tính chất mong muốn: nó cho phép một người dùng xác thực bản thân với một máy chủ, nó chống lại các cuộc tấn công từ điển do một kẻ nghe trộm thực hiện, và nó không yêu cầu một bên thứ ba đáng tin cậy. Nó hiệu quả truyền tải một bằng chứng mật khẩu không có kiến thức từ người dùng đến máy chủ. Trong phiên bản 6 của giao thức, chỉ có một mật khẩu có thể đoán được trên mỗi nỗ lực kết nối. Một trong những tính chất thú vị của giao thức là rằng ngay cả khi một hoặc hai trong số các nguyên tắc mật mã mà nó sử dụng bị tấn công, nó vẫn an toàn. Giao thức SRP đã được sửa đổi nhiều lần, và hiện đang ở phiên bản 6a.

Giao thức SRP tạo ra một khóa bí mật lớn được chia sẻ giữa hai bên một cách tương tự như trao đổi khóa Diffie-Hellman dựa trên việc máy khách có mật khẩu người dùng và máy chủ có một bộ chứng thực mật mã được tạo ra từ mật khẩu. Khóa công khai được chia từ hai số ngẫu nhiên, một được tạo ra bởi máy khách và một được tạo ra bởi máy chủ, mà đều độc nhất với mỗi lần đăng nhập. Trong những trường hợp cần giao tiếp được mã hóa cũng như xác thực, giao thức SRP an toàn hơn so với giao thức SSH thay thế và nhanh hơn khi sử dụng trao đổi khóa Diffie-Hellman với các thông điệp được ký. Nó cũng độc lập với bên thứ ba, không giống như Kerberos.

## Ưu và nhược điểm của Secure Remote Password

### **Ưu điểm**

* Xác thực người dùng: Cho phép người dùng xác thực với máy chủ.
* Chống tấn công từ điển: Bảo vệ khỏi các cuộc tấn công từ kẻ nghe trộm.
* Bảo mật cao: Không yêu cầu bên thứ ba đáng tin cậy.
* Hiệu quả: Truyền tải bằng chứng mật khẩu không có kiến thức hiệu quả.
* An toàn: Ngay cả khi một hoặc hai nguyên tắc mật mã bị tấn công, SRP vẫn an toàn.

### **Nhược điểm**

* Tính phức tạp: SRP phức tạp hơn so với các giao thức xác thực đơn giản như mật khẩu truyền thống. Việc triển khai và quản lý SRP có thể tốn nhiều thời gian và công sức hơn.
* Hiệu suất: SRP có thể tốn kém hơn về mặt tính toán so với các giao thức xác thực khác, đặc biệt là trên các thiết bị có tài nguyên hạn chế.
* Khả năng tương thích: SRP không được hỗ trợ rộng rãi như các giao thức xác thực khác, chẳng hạn như Kerberos hoặc NTLM. Điều này có thể gây ra vấn đề khi tích hợp SRP với các hệ thống và ứng dụng hiện có.
* Vấn đề mật khẩu: SRP vẫn dựa vào mật khẩu, vốn dễ bị tấn công nếu người dùng chọn mật khẩu yếu hoặc bị lộ.
* Tính bảo mật của máy chủ: SRP yêu cầu máy chủ lưu trữ mật khẩu của người dùng dưới dạng băm. Nếu máy chủ bị tấn công, kẻ tấn công có thể truy cập được mật khẩu của người dùng.
* Khả năng mở rộng: SRP có thể gặp khó khăn khi mở rộng quy mô cho một số lượng lớn người dùng.
* Vấn đề triển khai: Việc triển khai SRP có thể phức tạp và đòi hỏi chuyên môn kỹ thuật cao.
* Thiếu tiêu chuẩn: Hiện tại không có tiêu chuẩn chính thức cho SRP, dẫn đến việc triển khai không nhất quán và có thể gây ra vấn đề tương thích

## Ứng dụng Secure Remote Password

* Đăng nhập an toàn: SRP có thể được sử dụng trong các ứng dụng đăng nhập trực tuyến như email, trang web, dịch vụ ngân hàng trực tuyến, nơi cần độ tin cậy cao trong việc bảo vệ mật khẩu của người dùng.
* Xác thực người dùng trong hệ thống: SRP có thể được triển khai để xác thực người dùng khi truy cập vào hệ thống nội bộ của một tổ chức hoặc doanh nghiệp từ xa.
* Bảo vệ dữ liệu nhạy cảm: Bằng cách sử dụng SRP, dữ liệu nhạy cảm như thông tin tài khoản ngân hàng hoặc thông tin cá nhân có thể được bảo vệ hiệu quả mà không cần phải gửi mật khẩu qua mạng.
* Ứng dụng IoT (Internet of Things): Trong các hệ thống IoT, nơi các thiết bị kết nối với internet, việc sử dụng SRP có thể giúp đảm bảo tính bảo mật của dữ liệu được truyền từ các thiết bị tới các máy chủ hoặc dịch vụ điều khiển.
* Truy cập từ xa vào máy chủ: SRP có thể được sử dụng để xác thực người dùng khi truy cập từ xa vào máy chủ, cung cấp một cơ chế an toàn để truy cập dữ liệu hoặc tài nguyên từ xa.
* Ứng dụng trò chơi trực tuyến: Trong các trò chơi trực tuyến đòi hỏi tính bảo mật cao, SRP có thể được sử dụng để xác thực người dùng và đảm bảo rằng chỉ những người chơi được phép truy cập vào trò chơi.

## Hoạt động của giao thức

Để đạt được mục tiêu xác thực không cần mật khẩu, Secure Remote Password hoạt động như sau:

* Bước 1: Người dùng đăng nhập vào hệ thống bằng cách cung cấp tên đăng nhập của mình.
* Bước 2: Hệ thống gửi cho người dùng một giá trị công khai (public value) được tính toán trước đó.
* Bước 3: Người dùng tính toán một giá trị bí mật (secret value) từ mật khẩu của mình và giá trị công khai được cung cấp bởi hệ thống.
* Bước 4: Người dùng tính toán một giá trị xác thực (authentication value) bằng cách sử dụng giá trị bí mật của mình và giá trị công khai của hệ thống.
* Bước 5: Người dùng gửi giá trị xác thực của mình cho hệ thống.
* Bước 6: Hệ thống tính toán một giá trị xác thực của chính nó bằng cách sử dụng giá trị bí mật chia sẻ được tính toán từ mật khẩu và giá trị công khai của hệ thống.
* Bước 7: Hệ thống so sánh giá trị xác thực của người dùng với giá trị xác thực của chính nó. Nếu hai giá trị này giống nhau, hệ thống cho phép người dùng đăng nhập vào hệ thống.

Secure Remote Password đã sử dụng các giá trị bí mật và công khai được tính toán từ mật khẩu để đảm bảo rằng chỉ có người dùng đúng mới có thể tính toán được giá trị xác thực duy nhất, giảm thiểu nguy cơ bị đánh cắp mật khẩu.

Secure Remote Password cũng cho phép người dùng đăng nhập vào hệ thống mà không cần phải gửi mật khẩu của mình qua mạng, từ đó giảm thiểu nguy cơ bị tấn công giả mạo định danh (spoofing attacks) và tấn công từ điển (dictionary attacks).

## Lợi ích của việc sử dụng Secure Remote Password

## Đối với hệ thống bảo mật

Là một giải pháp lý tưởng cho nhiều ứng dụng yêu cầu xác thực an toàn, Secure Remote Password đem đến nhiều lợi ích về bảo mật cho hệ thống máy chủ như:

* Chứng minh danh tính của máy chủ và máy khách với nhau và đảm bảo không có bên mạo danh nào tham gia.
* Một số hệ thống lưu trữ mật khẩu của người dùng dưới dạng bản rõ, điều này tạo ra rủi ro an ninh. Nhưng với Secure Remote Password, máy chủ chỉ cần giữ giá trị bí mật được tính toán từ mật khẩu của người dùng và không cần lưu trữ mật khẩu nguyên gốc. Điều này giảm thiểu rủi ro liên quan đến việc lưu trữ mật khẩu dưới dạng bản rõ.
* Ngoài ra, Secure Remote Password còn cung cấp khoá mã hoá phiên an toàn để máy khách và máy chủ có thể truyền dữ liệu được mã hoá mang lại khả năng bảo mật cao hơn trên Transport Layer Security (TLS).
* SRP có thể được sử dụng trong nhiều hệ thống khác nhau và với các thuật toán mã hóa khác nhau. Do đó, nó là một phương pháp đa nền tảng và có thể được tích hợp dễ dàng vào các hệ thống bảo mật hiện có.

## Đối với người dùng

Cách Secure Remote Password hoạt động và giải quyết các thách thức bảo mật liên quan đến mật khẩu đã mang đến nhiều lợi ích tuyệt vời cho người dùng như:

* Phòng tránh được cả các cuộc Tấn công chủ động và Tấn công thụ động, chẳng hạn như Man-in-the-middle hoặc các cuộc Tấn công Brute Force,…
* Với Secure Remote Password, mật khẩu của người dùng không bao giờ được gửi trực tiếp qua internet. Thay vào đó, giá trị bí mật được tính toán từ mật khẩu của người dùng và giá trị công khai được tạo bởi máy chủ sẽ được sử dụng để thực hiện quá trình đăng nhập. Từ đó giúp ngăn chặn các kẻ tấn công giả mạo.
* Secure Remote Password sử dụng mã hóa đường truyền để bảo vệ thông tin đăng nhập của người dùng khi gửi qua mạng. Vì vậy, người dùng không cần phải lo lắng về việc mật khẩu của mình bị đánh cắp trong quá trình truyền tải.
* Trong hầu hết các phương pháp xác thực đăng nhập, người dùng phải sử dụng bên thứ ba để xác thực danh tính của mình. Với SRP, quá trình xác thực được thực hiện giữa người dùng và máy chủ, không cần đến bên thứ ba nào.

# CÀI ĐẶT THỬ NGHIỆM

## Phương pháp tính

* N = Một số nguyên lớn công khai
* g = Một số nguyên được chọn công khai
* k = hash (N, g)

Phía Client:

* Tạo 1 số ngẫu nhiên a
* Tính giá trị ngẫu nhiên 'A' : A = ( g ^ a) % N
* Chuyển LoginRequest(Username, A) qua phía server

Phía Server

* Lấy salt 's' và xác thực 'v' từ Password database
* Tính giá trị công khai 'B': B = [k \* v + ((g  ^ b) % N)] % N
* Tính toán tham số xáo trộn'u': u = hash (A, B)
* Tính toán khóa 'K': K = hash(S), trong đó S = [A \* (( v ^ u ) % N) ^ b] % N
* Lưu trữ [A, B, K, s] để sử dụng sau

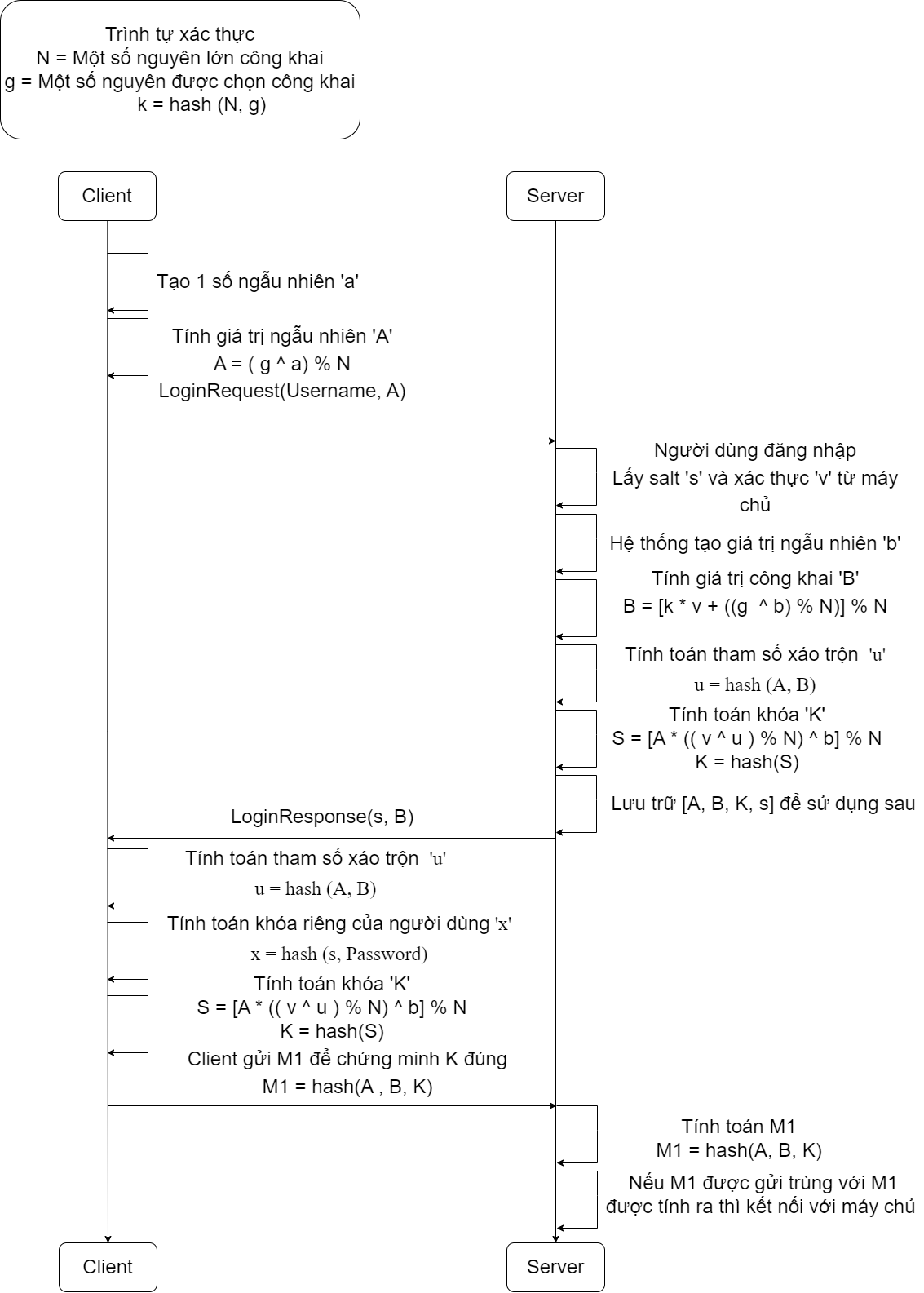
Phía Client

* Tính toán tham số xáo trộn 'u': u = hash (A, B)
* Tính toán khóa riêng của người dùng'x': x = hash (s, Password)
* Tính toán khóa 'K': K = hash(S), trong đó S = [A \* (( v ^ u ) % N) ^ b] % N
* Client gửi M1 để chứng minh K đúng: M1 = hash(A , B, K)

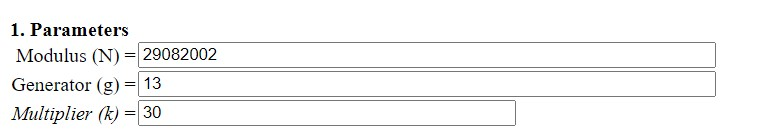
Phía Server

* Tính toán M1: M1 = hash(A, B, K)
* Nếu M1 được gửi trùng với M1 được tính ra thì kết nối với máy chủ

## Demo



Hình 3 Trình tự xác thực giữa người dùng – máy chủ

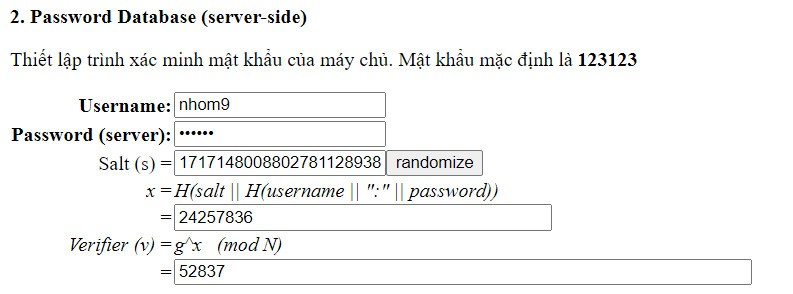


Hình 4 Điền tham số cho N, g, k

N: Đây là một số nguyên lớn dương, thường là một số nguyên tố, được chọn để tạo ra một nhóm số nguyên có thứ tự lớn. N được sử dụng như một phần của phép toán trong giao thức SRP.

g: Đây là một số nguyên dương nhỏ hơn N, thường là một gốc nguyên thủy trong nhóm số nguyên đã được chọn. g được sử dụng như một phần của phép toán trong giao thức SRP để tạo ra giá trị public key.

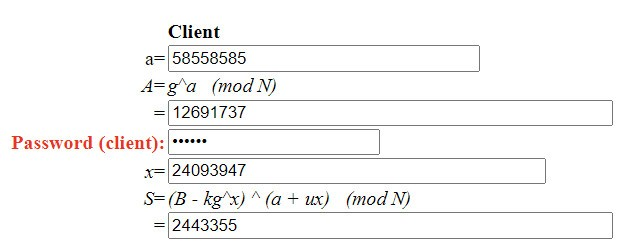
k: Đây là một hằng số, thường là một hàm băm, được sử dụng trong quá trình tính toán để tạo ra giá trị xác thực trong giao thức SRP.



Hình 5 Tính toán tham số x và v

Từ những tham số như Username và Password ta tính ra được giá trị bí mật x và giá trị public key v. Trong đó:

* Salt (s): Là một số ngẫu nhiên.
* x: Giá trị bí mật được tính theo công thức
* v: Giá trị public key được tính theo công thức



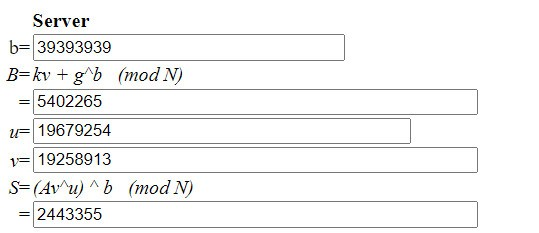
Hình 6 Người dùng điền mật khẩu và tính toán các tham số A, x và S

Người dùng điền mật khẩu và hệ thống sẽ dựa vào mật khẩu và các tham số sẽ tính ra được A, x và S dùng để xác thực với máy chủ. Trong đó:

A: Là giá trị public key của người dùng, được người dùng tính toán và gửi cho máy chủ trong quá trình xác thực. Được tính theo công thức

x: Là giá trị bí mật của người dùng, thường được tính từ mật khẩu của người dùng và salt.

S: Là giá trị chia sẻ bí mật (shared secret), là kết quả của quá trình trao đổi thông tin xác thực giữa người dùng và máy chủ. Được tính theo công thức



Hình 7 Máy chủ tính toán các tham số B, u, v, S

Máy chủ sẽ tính toán các tham số bằng các mã hóa các giá trị và tính toán dựa trên các công thức.

Từ giá trị b được cho ngẫu nhiên từ máy chủ, giá trị A được gửi từ người dùng và những dữ liệu được điền ở trên, máy chủ sẽ tính toán ra được B, u, b và S. Trong đó:

* B: Là giá trị public key của máy chủ, được máy chủ tính toán và gửi cho người dùng trong quá trình trao đổi xác thực. Theo công thức

* u: Là một giá trị ngẫu nhiên được tính toán từ các giá trị public key của cả máy chủ và người dùng.
* v: Giá trị public key được tính theo công thức
* S: Là giá trị chia sẻ bí mật, là kết quả của quá trình trao đổi xác thực giữa máy chủ và người dùng. Theo công thức



Hình 8 Thông báo khi trùng khớp tham số S

Sau khi máy chủ tính toán tham số S trùng khớp với tham số S của người dùng thì thông báo Đăng nhập thành công



Hình 9 Thông báo khi không trùng khớp tham số S

Sau khi máy chủ tính toán tham số S trùng khớp với tham số S của người dùng thì thông báo Đăng nhập thất bại. Thử lại.

# KẾT LUẬN

## Kết quả đạt được của đề tài

Trong quá trình thực hiện đề tài, nhóm chúng em đã được học hỏi và trau dồi nhiều kiến thức bổ ích về lĩnh vực an ninh mạng. Đề tài này tập trung nghiên cứu về Secure Remote Password (SRP), một giao thức xác thực mật khẩu từ xa an toàn. Tìm hiểu về an ninh mạng, nắm được nguyên tắc hoạt động của Secure Remote Password, ứng dụng của Secure Remote Password trong thực tế.

SRP cung cấp một phương pháp xác thực mật khẩu an toàn và hiệu quả trên mạng không an toàn, giúp ngăn chặn các cuộc tấn công từ điển và tránh việc truyền mật khẩu qua mạng.

Sử dụng SRP giúp tăng cường tính bảo mật bằng cách tạo ra một khóa phiên chia sẻ mạnh mẽ, từ đó cung cấp một cơ chế an toàn cho việc truyền thông giữa người dùng và máy chủ.

## Hạn chế của đề tài

Mặc dù SRP có nhiều ưu điểm, nhưng triển khai nó có thể phức tạp đối với các ứng dụng lớn hoặc các hệ thống phức tạp, đặc biệt là khi cần tương thích với các hệ thống hiện có.

SRP cần tối ưu hóa và bảo mật mạnh mẽ để đảm bảo khả năng chống lại các cuộc tấn công từ chối dịch vụ (DoS) hoặc tấn công thời gian thực.

Chưa triển khai được ứng dụng kết sử dụng phương thức xác thực Secure Remote Password.

Chưa đánh giá hiệu suất của Secure Remote Password so với các giao thức khác.

## Hướng phát triển

Nghiên cứu và phát triển các biến thể của SRP để cải thiện hiệu suất và tính linh hoạt trong việc triển khai trên các hệ thống phức tạp.

Tăng cường tính bảo mật bằng cách tích hợp các biện pháp bảo vệ chống lại các cuộc tấn công mới và tiến hóa của hacker.

**TÀI LIỆU THAM KHẢO**

1. **Gerardus Blokdyk**, Secure Remote Password Protocol A Complete Guide, Nhà xuất bản 5STARCooks , 13/04/2021
2. **Quinn Kiser**, Computer Networking and Cybersecurity: A Guide to Understanding Communications Systems, Internet Connections, and Network Security Along with Protection from Hacking and Cyber Security Threats, Nhà xuất bản độc lập, 05/09/2020
3. **Adam Woodbeck**, Network Programming with Go: Code Secure and Reliable Network Services from Scratch, 25/03/2021.
4. **Christof Paar và Jan Pelzl**, Understanding Cryptography: A Textbook for Students and Practitioners, nhà xuất bản Springer, 2010.
5. William Stallings, Cryptography and Network Security: Principles and Practice, nhà xuất bản Pearson. 2017.
6. <https://en.wikipedia.org/wiki/Secure_Remote_Password_protocol>
7. <https://doc.edu.vn/tai-lieu/giao-trinh-an-toan-mang-6773/>
8. <https://locker.io/passwords/blog/secure-remote-password>