**Đề tài: Phân tích các phương pháp phát hiện giả mạo IP**

# **LỜI CẢM ƠN**

Trước tiên, em xin gửi lời cảm ơn chân thành và sâu sắc nhất đến Ban Giám hiệu và các thầy cô trong Khoa Công nghệ Thông tin, Trường Đại học ... đã giảng dạy và truyền đạt những kiến thức quý báu cho em trong suốt quá trình học tập.

Em xin bày tỏ lòng biết ơn đến thầy/cô ... (người hướng dẫn), người đã tận tình hướng dẫn, truyền đạt kiến thức, kinh nghiệm cũng như hỗ trợ và động viên em trong suốt quá trình nghiên cứu và hoàn thiện đề tài tốt nghiệp *“Phân tích các phương pháp phát hiện giả mạo IP”*. Sự hướng dẫn tận tâm và những góp ý quý báu của thầy/cô là nguồn động lực lớn lao giúp em hoàn thành đồ án này.

Em cũng xin gửi lời cảm ơn đến gia đình và bạn bè, những người đã luôn bên cạnh, động viên và tạo điều kiện tốt nhất để em có thể hoàn thành nhiệm vụ học tập cũng như đồ án này.

Cuối cùng, em xin chân thành cảm ơn tất cả những ai đã đóng góp ý kiến và hỗ trợ em trong suốt quá trình thực hiện đề tài. Mặc dù đã cố gắng hết sức, nhưng bài báo cáo vẫn có thể còn những thiếu sót, em rất mong nhận được những ý kiến đóng góp từ quý thầy cô và bạn bè để hoàn thiện hơn.

Xin chân thành cảm ơn!

**MỤC LỤC**

[**LỜI CẢM ƠN** 2](#_Toc182070963)

[**MỞ ĐẦU** 5](#_Toc182070964)

[1. Lý do chọn đề tài 5](#_Toc182070965)

[2. Mục tiêu nghiên cứu 5](#_Toc182070966)

[3. Đối tượng nghiên cứu 6](#_Toc182070967)

[4. Phạm vi nghiên cứu 7](#_Toc182070968)

[5. Phương pháp nghiên cứu 8](#_Toc182070969)

[6. Ý nghĩa khoa học và thực tiễn của đề tài 8](#_Toc182070970)

[7. Cấu trúc báo cáo đồ án tốt nghiệp 9](#_Toc182070971)

[**CHƯƠNG 1. TỔNG QUAN VỀ AN NINH MẠNG** 10](#_Toc182070972)

[1.1. Tổng quan về an ninh mạng 10](#_Toc182070973)

[1.2. Tầm quan trọng của an ninh mạng trong hạ tầng công nghệ thông tin 10](#_Toc182070974)

[1.3. Các mối đe dọa an ninh mạng và biện pháp phòng chống 10](#_Toc182070975)

[**CHƯƠNG 2. KỸ THUẬT TẤN CÔNG MẠNG GIẢ MẠO ĐỊA CHỈ IP (IP SPOOFING)** 11](#_Toc182070976)

[2.1. Định nghĩa và phương thức hoạt động của IP Spoofing 11](#_Toc182070977)

[2.2. Các loại tấn công liên quan đến IP Spoofing 11](#_Toc182070978)

[2.3. Tác động của IP Spoofing đến an ninh mạng 11](#_Toc182070979)

[2.4. Thử nghiệm mô phỏng tấn công IP Spoofing 11](#_Toc182070980)

[**CHƯƠNG 3. PHƯƠNG PHÁP PHÁT HIỆN GIẢ MẠO ĐỊA CHỈ IP** 12](#_Toc182070981)

[3.1. Ingress và Egress Filtering 12](#_Toc182070982)

[3.2. Phân tích lưu lượng bất thường 12](#_Toc182070983)

[3.3. Kỹ thuật IP Traceback 12](#_Toc182070984)

[3.4. Sử dụng giao thức bảo mật IPsec 12](#_Toc182070985)

[**CHƯƠNG 4. ĐÁNH GIÁ VÀ SO SÁNH CÁC PHƯƠNG PHÁP** 13](#_Toc182070986)

[**KẾT LUẬN** 13](#_Toc182070987)

[**TÀI LIỆU THAM KHẢO** 14](#_Toc182070988)

[**PHỤ LỤC** 15](#_Toc182070989)

# **MỞ ĐẦU**

## **1. Lý do chọn đề tài**

Trong bối cảnh công nghệ ngày càng phát triển, an ninh mạng trở thành một trong những mối quan tâm hàng đầu của các tổ chức và cá nhân. Các cuộc tấn công mạng ngày càng tinh vi, trong đó kỹ thuật giả mạo địa chỉ IP (IP Spoofing) là một trong những phương pháp được kẻ tấn công sử dụng phổ biến nhằm che giấu danh tính và thực hiện các hành vi gây hại, như tấn công từ chối dịch vụ (DDoS), chiếm quyền điều khiển phiên làm việc, hay can thiệp vào dữ liệu.

Việc nghiên cứu và phát triển các phương pháp phát hiện giả mạo IP đóng vai trò vô cùng quan trọng trong việc đảm bảo an ninh mạng, giảm thiểu rủi ro và bảo vệ hệ thống thông tin. Tuy nhiên, mỗi phương pháp đều có những ưu điểm và hạn chế riêng, đòi hỏi sự đánh giá và so sánh chi tiết để áp dụng hiệu quả trong từng tình huống cụ thể.

Với mong muốn đóng góp một phần nhỏ vào lĩnh vực bảo mật mạng, em đã chọn đề tài *“Phân tích các phương pháp phát hiện giả mạo IP”* nhằm nghiên cứu và so sánh các giải pháp phát hiện IP Spoofing, từ đó đề xuất các phương pháp tối ưu, hiệu quả hơn. Thông qua đề tài này, em hy vọng có thể giúp các nhà quản trị mạng có cái nhìn rõ ràng hơn về các kỹ thuật hiện có, đồng thời nâng cao khả năng ứng phó với các mối đe dọa tiềm tàng trong môi trường mạng phức tạp hiện nay.

## **2. Mục tiêu nghiên cứu**

Mục tiêu chính của đề tài *“Phân tích các phương pháp phát hiện giả mạo IP”* là nghiên cứu và đánh giá hiệu quả của các kỹ thuật phát hiện IP Spoofing trong môi trường mạng, từ đó đề xuất các giải pháp tối ưu nhằm nâng cao khả năng bảo mật mạng. Cụ thể, đề tài hướng tới:

* Tìm hiểu và phân tích các kỹ thuật giả mạo địa chỉ IP: Hiểu rõ nguyên lý hoạt động của IP Spoofing và các hình thức tấn công mạng liên quan. Phân tích những tác động và mối nguy hiểm mà IP Spoofing gây ra cho hệ thống mạng.
* Nghiên cứu và trình bày các phương pháp phát hiện giả mạo IP: Mô tả chi tiết các phương pháp phát hiện, bao gồm Ingress/Egress Filtering, Phân tích lưu lượng bất thường, IP Traceback, và sử dụng giao thức bảo mật như IPsec. Đánh giá hiệu quả của từng phương pháp thông qua các tiêu chí như độ chính xác, tính khả thi, chi phí, và tính hiệu quả.
* So sánh và đánh giá các phương pháp phát hiện giả mạo IP: So sánh ưu, nhược điểm của các kỹ thuật khác nhau và xác định phương pháp phù hợp nhất cho từng tình huống cụ thể. Đưa ra đề xuất cải tiến hoặc kết hợp các phương pháp để nâng cao hiệu quả phát hiện IP Spoofing.
* Xây dựng kịch bản thử nghiệm và trình bày kết quả: Phát triển các kịch bản thử nghiệm để minh họa và kiểm tra hiệu quả của các phương pháp phát hiện giả mạo IP. Phân tích kết quả thử nghiệm và rút ra những nhận xét, kết luận quan trọng cho nghiên cứu.

## **3. Đối tượng nghiên cứu**

Đối tượng nghiên cứu của đề *tài “Phân tích các phương pháp phát hiện giả mạo IP”* tập trung vào các khía cạnh chính sau:

* Các kỹ thuật giả mạo địa chỉ IP (IP Spoofing): Nghiên cứu nguyên lý hoạt động và các hình thức khác nhau của kỹ thuật IP Spoofing. Phân tích các loại tấn công mạng liên quan sử dụng IP Spoofing, chẳng hạn như tấn công từ chối dịch vụ phân tán (DDoS), chiếm quyền điều khiển phiên làm việc, và các cuộc tấn công trung gian (Man-in-the-Middle).
* Phương pháp phát hiện IP Spoofing: Tìm hiểu các phương pháp phát hiện IP Spoofing, bao gồm:
  + Ingress/Egress Filtering: Lọc gói tin dựa trên địa chỉ IP nguồn.
  + Phân tích lưu lượng bất thường: Sử dụng các hệ thống phát hiện xâm nhập (IDS) hoặc các công cụ học máy để nhận diện các mẫu lưu lượng khác thường.
  + IP Traceback: Theo dõi và xác định nguồn gốc của các gói tin giả mạo.
  + Giao thức bảo mật IPsec: Bảo vệ lưu lượng mạng bằng mã hóa và xác thực.
  + Đánh giá hiệu quả và các yếu tố ảnh hưởng đến hiệu suất của từng phương pháp.
* Mô hình và hệ thống mạng: Môi trường mạng thực tế và các kịch bản tấn công/ phòng thủ được sử dụng để thử nghiệm. Công cụ và phần mềm phân tích gói tin, như Wireshark, PyShark, và Scapy, để hỗ trợ việc phát hiện và đánh giá IP Spoofing.

## **4. Phạm vi nghiên cứu**

* **Phạm vi kỹ thuật**: Nghiên cứu và phân tích các phương pháp phát hiện giả mạo IP trong môi trường mạng, bao gồm Ingress/Egress Filtering, Phân tích lưu lượng bất thường, IP Traceback, và sử dụng giao thức bảo mật IPsec. Xây dựng và thực hiện các kịch bản mô phỏng tấn công và phòng thủ để thử nghiệm và đánh giá hiệu quả của các phương pháp phát hiện.
* **Phạm vi công cụ và công nghệ**: Sử dụng các công cụ phân tích mạng như Wireshark, PyShark, và Scapy để thu thập và phân tích gói tin mạng. Thử nghiệm các giải pháp phát hiện giả mạo IP trên một mô hình mạng giả lập, nhằm đánh giá hiệu quả của từng phương pháp trong các tình huống cụ thể. Áp dụng ngôn ngữ lập trình Python để phát triển các đoạn mã demo minh họa cho các kỹ thuật phát hiện.
* **Phạm vi thời gian**: Nghiên cứu thực hiện trong thời gian từ … đến …, bao gồm giai đoạn nghiên cứu lý thuyết, thử nghiệm thực tế, và đánh giá kết quả.
* **Phạm vi nội dung**: Nghiên cứu sẽ không đi sâu vào các khía cạnh bảo mật khác ngoài IP Spoofing. Đề tài sẽ chỉ tập trung vào phân tích các phương pháp phát hiện và không mở rộng sang các biện pháp phòng thủ khác như tường lửa hay các công nghệ mã hóa phức tạp không liên quan trực tiếp đến IP Spoofing.

## **5. Phương pháp nghiên cứu**

* Phương pháp nghiên cứu tài liệu: Thu thập và phân tích các tài liệu, bài báo khoa học, và công trình nghiên cứu liên quan đến an ninh mạng và IP Spoofing. Tìm hiểu các lý thuyết, mô hình, và giải pháp phát hiện IP Spoofing từ các nguồn tài liệu uy tín như sách chuyên ngành, tạp chí khoa học, và các hội thảo quốc tế về bảo mật mạng.
* Phương pháp phân tích và so sánh: Phân tích chi tiết từng phương pháp phát hiện IP Spoofing như Ingress/Egress Filtering, Phân tích lưu lượng bất thường, IP Traceback, và IPsec. So sánh các phương pháp theo các tiêu chí như độ chính xác, tính khả thi, chi phí triển khai, và hiệu quả trong các tình huống khác nhau. Xây dựng bảng so sánh để làm nổi bật ưu, nhược điểm của mỗi phương pháp.
* Phương pháp mô phỏng và thử nghiệm: Thiết kế các kịch bản mô phỏng tấn công giả mạo IP trong môi trường mạng giả lập, sử dụng các công cụ như Wireshark, PyShark, và Scapy để thu thập và phân tích gói tin. Phát triển các đoạn mã demo bằng Python để minh họa cách các phương pháp phát hiện giả mạo IP hoạt động. Thử nghiệm các phương pháp phát hiện trong điều kiện khác nhau để đánh giá tính hiệu quả và độ chính xác.
* Phương pháp đánh giá và tổng hợp: Đánh giá hiệu quả của từng phương pháp phát hiện IP Spoofing dựa trên kết quả mô phỏng và thử nghiệm. Tổng hợp các kết quả nghiên cứu để đưa ra kết luận và đề xuất giải pháp tối ưu cho việc phát hiện IP Spoofing.

## **6. Ý nghĩa khoa học và thực tiễn của đề tài**

Ý nghĩa khoa học:

* Nghiên cứu giúp làm rõ nguyên lý hoạt động và bản chất của các phương pháp phát hiện IP Spoofing, từ đó cung cấp một cơ sở lý thuyết vững chắc để phát triển các giải pháp bảo mật mạng tiên tiến hơn.
* Kết quả nghiên cứu là nền tảng cho các nhà khoa học và chuyên gia bảo mật trong việc tiếp tục nghiên cứu, cải tiến và kết hợp các phương pháp phát hiện hiệu quả hơn trong tương lai.

Ý nghĩa thực tiễn:

* Trong bối cảnh các cuộc tấn công mạng ngày càng phức tạp và nguy hiểm, việc phát hiện sớm các hành vi giả mạo IP có vai trò quan trọng trong việc bảo vệ hệ thống mạng của các tổ chức, doanh nghiệp, và cá nhân.
* Đề tài cung cấp những đánh giá và so sánh chi tiết về hiệu quả của các phương pháp phát hiện IP Spoofing, giúp các nhà quản trị mạng lựa chọn và triển khai giải pháp bảo mật phù hợp với hệ thống của họ.
* Các kịch bản thử nghiệm và đoạn mã demo có thể được áp dụng thực tế trong việc xây dựng các hệ thống phát hiện và phòng chống tấn công mạng, góp phần nâng cao mức độ an toàn và giảm thiểu rủi ro bị tấn công.
* Nghiên cứu có thể hỗ trợ các tổ chức trong việc xây dựng chính sách bảo mật và nâng cao nhận thức về an ninh mạng, đồng thời đưa ra những khuyến nghị để tối ưu hóa hệ thống bảo vệ trước các mối đe dọa tiềm ẩn.

## **7. Cấu trúc báo cáo đồ án tốt nghiệp**

# **CHƯƠNG 1. TỔNG QUAN VỀ AN NINH MẠNG**

## **1.1. Tổng quan về an ninh mạng**

An ninh mạng là tập hợp các biện pháp và kỹ thuật nhằm bảo vệ dữ liệu và hệ thống mạng trước các rủi ro như truy cập trái phép, xâm nhập, phá hoại, và tấn công mạng. Bằng cách thu thập kiến ​​thức về các cuộc tấn công mạng và an ninh mạng, chúng ta có thể bảo vệ và bảo vệ mình khỏi các cuộc tấn công mạng khác nhau như tấn công lừa đảo (Fishing) và DDoS.

An ninh mạng (Cybersecurity) là lĩnh vực bảo vệ các hệ thống thông tin, mạng máy tính và dữ liệu khỏi các mối đe dọa và tấn công nguy hiểm. Trong bối cảnh sự phát triển vượt bậc của công nghệ thông tin và việc kết nối mạng ngày càng trở nên phổ biến, an ninh mạng đã trở thành một trong những mối quan tâm hàng đầu của các tổ chức, doanh nghiệp, và cá nhân.

An ninh mạng rất quan trọng vì chính phủ, các tập đoàn và tổ chức y tế thu thập lượng dữ liệu quân sự, tài chính, xử lý và lưu trữ lượng dữ liệu chưa từng có trên máy tính cũng như các tài sản khác như thông tin cá nhân và việc tiết lộ thông tin cá nhân này có thể gây ra hậu quả tiêu cực.

Vai trò của an ninh mạng là đảm bảo tính toàn vẹn (integrity), tính bảo mật (confidentiality), và tính sẵn sàng (availability) của dữ liệu. Các hệ thống an ninh mạng được thiết kế để bảo vệ thông tin quan trọng, đảm bảo sự vận hành liên tục của các dịch vụ, và giảm thiểu thiệt hại trong trường hợp xảy ra tấn công.

Những mối đe dọa phổ biến trong an ninh mạng:

* Tấn công mạng (Cyber Attacks): Các mối đe dọa này bao gồm tấn công từ chối dịch vụ (DDoS), tấn công xâm nhập, và tấn công phần mềm độc hại (malware), có thể gây hại cho hệ thống mạng và dữ liệu.
* Kỹ thuật tấn công nâng cao: Kẻ tấn công có thể sử dụng các phương pháp như tấn công trung gian (Man-in-the-Middle), tấn công mạng xã hội (social engineering), và kỹ thuật giả mạo IP (IP Spoofing) để xâm nhập và tấn công hệ thống.
* Mối đe dọa nội bộ (Insider Threats): Các nhân viên hoặc người có quyền truy cập vào hệ thống có thể vô tình hoặc cố ý gây ra các sự cố an ninh nghiêm trọng.

Các lớp bảo vệ trong an ninh mạng:

* Bảo vệ mạng (Network Security): Sử dụng tường lửa, hệ thống phát hiện xâm nhập (IDS), và các giao thức mã hóa để bảo vệ mạng khỏi các cuộc tấn công từ bên ngoài.
* Bảo vệ ứng dụng (Application Security): Đảm bảo rằng các ứng dụng được phát triển và duy trì với các biện pháp an ninh cần thiết để ngăn chặn các lỗ hổng bảo mật.
* Quản lý rủi ro (Risk Management): Đánh giá và xác định rủi ro, sau đó triển khai các biện pháp bảo mật thích hợp để giảm thiểu nguy cơ.

Thách thức trong an ninh mạng:

* Tấn công ngày càng tinh vi: Kẻ tấn công ngày càng sử dụng những công nghệ tiên tiến như trí tuệ nhân tạo (AI) và học máy (Machine Learning) để thực hiện các cuộc tấn công có quy mô lớn và phức tạp.
* Thiếu hụt chuyên gia bảo mật: Sự thiếu hụt chuyên gia trong lĩnh vực an ninh mạng dẫn đến khó khăn trong việc bảo vệ hệ thống khỏi các mối đe dọa.
* Phát triển liên tục của công nghệ: Sự ra đời của các công nghệ mới như Internet of Things (IoT), điện toán đám mây (Cloud Computing), và 5G mang lại nhiều lợi ích nhưng cũng mở ra những lỗ hổng an ninh mới mà các hệ thống phải đối mặt.

Các loại an ninh mạng khác nhau:

* Network Security: Tập trung vào việc bảo vệ mạng máy tính khỏi bị truy cập trái phép, vi phạm dữ liệu và các mối đe dọa dựa trên mạng khác. Nó liên quan đến các công nghệ như tường lửa (Firewall), hệ thống phát hiện xâm nhập (IDS – Intrution detection system), mạng riêng ảo (VPN – Virtual private network) và phân đoạn mạng (Network segmentation). Bảo vệ mạng nội bộ khỏi các mối đe dọa bên ngoài bằng tính năng bảo mật mạng được tăng cường.
* Application Security (Bảo mật ứng dụng): Liên quan đến việc bảo mật các ứng dụng phần mềm và ngăn chặn các lỗ hổng có thể bị kẻ tấn công khai thác. Nó liên quan đến thực hành mã hóa an toàn, cập nhật và vá lỗi phần mềm thường xuyên cũng như tường lửa cấp ứng dụng. Hầu hết các ứng dụng hoạt động trên điện thoại android đều được bảo mật và hoạt động theo các quy tắc và quy định của cửa hàng Google Play. Nhiều ứng dụng giả vờ an toàn nhưng sau khi lấy tất cả thông tin từ người dùng, ứng dụng sẽ chia sẻ thông tin người dùng với bên thứ ba. Ứng dụng phải được cài đặt từ một nền tảng đáng tin cậy, không phải từ một số trang web của bên thứ 3 dưới dạng APK (Gói ứng dụng Android).
* Information or Data Security (Bảo mật thông tin hoặc dữ liệu): Tập trung vào việc bảo vệ thông tin nhạy cảm khỏi bị truy cập, tiết lộ, thay đổi hoặc phá hủy trái phép. Nó bao gồm các biện pháp mã hóa, kiểm soát quyền truy cập, phân loại dữ liệu và ngăn ngừa mất dữ liệu (DLP – Data loss prevention). Ứng phó sự cố đề cập đến quá trình phát hiện, phân tích và ứng phó kịp thời với các sự cố bảo mật.
* Cloud Security (Bảo mật đám mây): Nó liên quan đến việc bảo mật dữ liệu, ứng dụng và cơ sở hạ tầng được lưu trữ trên nền tảng đám mây và đảm bảo kiểm soát truy cập, bảo vệ dữ liệu và tuân thủ phù hợp. Nó sử dụng nhiều nhà cung cấp dịch vụ đám mây khác nhau như AWS, Azure, Google Cloud, v.v. để đảm bảo an ninh trước nhiều mối đe dọa. Lưu trữ dữ liệu dựa trên đám mây đã trở thành một lựa chọn phổ biến trong thập kỷ qua. Nó tăng cường quyền riêng tư và lưu dữ liệu trên đám mây, giúp dữ liệu có thể truy cập được từ mọi thiết bị có xác thực phù hợp.
* Mobile Security (Bảo mật di động): Nó liên quan đến việc bảo mật dữ liệu tổ chức và cá nhân được lưu trữ trên các thiết bị di động như điện thoại di động, máy tính bảng và các thiết bị tương tự khác trước các mối đe dọa độc hại khác nhau. Những mối đe dọa này là truy cập trái phép, mất thiết bị hoặc phần mềm độc hại, v.v. Thường xuyên sao lưu dữ liệu thiết bị di động là điều quan trọng để ngăn ngừa mất dữ liệu trong trường hợp bị mất cắp, hư hỏng hoặc hỏng thiết bị. Các thiết bị di động thường kết nối với nhiều mạng khác nhau, bao gồm cả Wi-Fi công cộng, điều này có thể gây ra rủi ro bảo mật. Điều quan trọng là sử dụng mạng an toàn bất cứ khi nào có thể, chẳng hạn như mạng Wi-Fi được mã hóa hoặc kết nối dữ liệu di động.
* Endpoint Security (Bảo mật điểm cuối): Đề cập đến việc bảo mật các thiết bị riêng lẻ như máy tính, máy tính xách tay, điện thoại thông minh và thiết bị IoT. Nó bao gồm phần mềm chống vi-rút, hệ thống ngăn chặn xâm nhập (IPS), mã hóa thiết bị và cập nhật phần mềm thường xuyên. Phần mềm chống vi-rút và chống phần mềm độc hại quét và phát hiện phần mềm độc hại, chẳng hạn như Virus, Worms, Trojan và Ransomware. Những công cụ này xác định và loại bỏ hoặc cách ly các tệp độc hại, bảo vệ điểm cuối và mạng khỏi tác hại tiềm ẩn. Tường lửa là thành phần thiết yếu của bảo mật điểm cuối giúp giám sát và kiểm soát lưu lượng mạng đến và đi, lọc ra các gói dữ liệu độc hại tiềm ẩn. Luôn cập nhật phần mềm và hệ điều hành với các bản vá và bản cập nhật bảo mật mới nhất là điều quan trọng đối với bảo mật điểm cuối.
* Critial Infrastructure Security (Bảo mật cơ sở hạ tầng quan trọng): Tất cả các tài nguyên, hệ thống và mạng vật lý và ảo cần thiết để nền kinh tế, an ninh của xã hội hoặc bất kỳ sự kết hợp nào ở trên hoạt động trơn tru đều được gọi là cơ sở hạ tầng quan trọng. Các ngành công nghiệp thực phẩm và nông nghiệp cũng như hệ thống giao thông vận tải bao gồm cơ sở hạ tầng quan trọng. Cơ sở hạ tầng được coi là quan trọng có thể khác nhau tùy thuộc vào nhu cầu, nguồn lực và mức độ phát triển cụ thể của một quốc gia, mặc dù cơ sở hạ tầng quan trọng có thể so sánh được ở tất cả các quốc gia do yêu cầu sinh hoạt cơ bản. Các hệ thống điều khiển công nghiệp (ICS), chẳng hạn như hệ thống điều khiển giám sát và thu thập dữ liệu (SCADA), được sử dụng để tự động hóa các hoạt động công nghiệp trong các ngành cơ sở hạ tầng quan trọng, thường được đưa vào cơ sở hạ tầng quan trọng. SCADA và các cuộc tấn công hệ thống điều khiển công nghiệp khác rất đáng lo ngại. Chúng có thể làm suy yếu nghiêm trọng cơ sở hạ tầng quan trọng, bao gồm giao thông vận tải, cung cấp dầu khí, lưới điện, phân phối nước và thu gom nước thải.
* Internet of Things (IoT) Security (Bảo mật IoT): Các thiết bị thường xuyên chạy trên phần mềm cũ, khiến chúng dễ bị tấn công trước các lỗ hổng bảo mật được xác định gần đây. Điều này thường là kết quả của sự cố kết nối hoặc yêu cầu người dùng cuối tải xuống các bản cập nhật theo cách thủ công từ trung tâm C&C. Các nhà sản xuất thường gửi các thiết bị Internet of Things (IoT) (chẳng hạn như bộ định tuyến gia đình) bằng mật khẩu dễ bẻ khóa, có thể do nhà cung cấp và người dùng cuối để sẵn. Các thiết bị này là mục tiêu dễ dàng cho những kẻ tấn công sử dụng tập lệnh tự động để khai thác hàng loạt khi chúng bị truy cập từ xa. API thường là đối tượng của các mối đe dọa như Man in the Middle (MITM), tiêm mã (như SQLI) và các cuộc tấn công từ chối dịch vụ phân tán (DDoS) vì chúng đóng vai trò là cổng vào trung tâm C&C.

## **1.2. Tầm quan trọng của an ninh mạng trong hạ tầng công nghệ thông tin**

An ninh mạng đóng vai trò thiết yếu trong việc bảo vệ hạ tầng công nghệ thông tin (CNTT), đảm bảo sự an toàn và ổn định cho các hệ thống, dữ liệu, và giao dịch trực tuyến. Trong bối cảnh công nghệ ngày càng thâm nhập sâu vào mọi lĩnh vực của đời sống, từ doanh nghiệp, y tế, giáo dục, đến chính phủ, việc bảo vệ các hệ thống mạng trở thành ưu tiên hàng đầu. Dưới đây là những lý do vì sao an ninh mạng có tầm quan trọng đặc biệt trong hạ tầng CNTT:

Bảo vệ thông tin nhạy cảm và dữ liệu quan trọng:

* Hệ thống CNTT hiện nay lưu trữ khối lượng lớn thông tin nhạy cảm, như dữ liệu khách hàng, thông tin tài chính, và bí mật kinh doanh. Bất kỳ hành vi xâm nhập nào vào hệ thống có thể gây ra hậu quả nghiêm trọng, bao gồm rò rỉ dữ liệu, tổn thất tài chính, và mất lòng tin của khách hàng.
* An ninh mạng đảm bảo tính bảo mật (confidentiality) của dữ liệu, ngăn chặn việc truy cập trái phép và bảo vệ thông tin trước các mối đe dọa mạng.

Đảm bảo tính toàn vẹn và sẵn sàng của hệ thống:

* Các cuộc tấn công mạng, chẳng hạn như tấn công từ chối dịch vụ (DDoS), có thể làm gián đoạn hoạt động của các hệ thống và dịch vụ, gây ra thiệt hại lớn cho doanh nghiệp và người dùng. An ninh mạng đảm bảo tính toàn vẹn (integrity) của dữ liệu và tính sẵn sàng (availability) của hệ thống, giúp hệ thống hoạt động liên tục và không bị gián đoạn.
* Việc bảo vệ hệ thống mạng giúp ngăn chặn các hành vi phá hoại và đảm bảo rằng các dịch vụ trực tuyến luôn sẵn sàng phục vụ người dùng.

Bảo vệ cơ sở hạ tầng quan trọng quốc gia:

* Hạ tầng CNTT không chỉ bao gồm các mạng và hệ thống thông thường mà còn là nền tảng cho các dịch vụ quan trọng như điện, nước, giao thông, và các dịch vụ y tế. Các cuộc tấn công mạng nhắm vào những cơ sở hạ tầng này có thể gây ra hậu quả nghiêm trọng, làm gián đoạn các dịch vụ thiết yếu và ảnh hưởng trực tiếp đến đời sống của người dân.
* Do đó, an ninh mạng giúp bảo vệ những cơ sở hạ tầng quan trọng, giảm thiểu nguy cơ các cuộc tấn công có thể làm tê liệt hoặc gây thiệt hại lớn.

Ngăn chặn các cuộc tấn công ngày càng tinh vi:

* Tội phạm mạng không ngừng phát triển các kỹ thuật tấn công mới, từ việc sử dụng phần mềm độc hại (malware) đến việc khai thác lỗ hổng bảo mật trong hệ thống. An ninh mạng phải liên tục đổi mới và nâng cao để ngăn chặn các mối đe dọa này.
* Việc bảo vệ hạ tầng CNTT giúp các tổ chức duy trì tính cạnh tranh và sự ổn định, tránh được những tổn thất lớn từ các cuộc tấn công mạng tinh vi.

Tăng cường vào các dịch vụ công nghệ số:

* Khi các tổ chức và doanh nghiệp triển khai các dịch vụ trực tuyến, sự an toàn và bảo mật của hệ thống mạng ảnh hưởng trực tiếp đến mức độ tin cậy của người dùng. Một sự cố an ninh có thể làm giảm uy tín của tổ chức, gây mất lòng tin và thiệt hại nghiêm trọng.
* An ninh mạng góp phần củng cố niềm tin của người dùng vào các dịch vụ công nghệ số, thúc đẩy sự phát triển và ứng dụng công nghệ trong nhiều lĩnh vực khác nhau.

## **1.3. Các mối đe dọa an ninh mạng và biện pháp phòng chống**

Trong môi trường kỹ thuật số hiện đại, các hệ thống mạng và dữ liệu liên tục đối mặt với nhiều mối đe dọa an ninh phức tạp và ngày càng tinh vi. Dưới đây là những mối đe dọa phổ biến trong an ninh mạng và các biện pháp phòng chống:

Tấn công từ chối dịch vụ (DDoS):

* Mô tả: Tấn công DDoS (Distributed Denial of Service) là khi kẻ tấn công sử dụng một mạng lưới lớn các thiết bị bị xâm nhập (botnet) để gửi lượng lớn yêu cầu đến một máy chủ mục tiêu, khiến hệ thống không thể xử lý kịp và trở nên quá tải, dẫn đến gián đoạn dịch vụ.
* Biện pháp phòng chống:
  + Sử dụng tường lửa (firewall) và hệ thống phát hiện xâm nhập (IDS/IPS): Giúp ngăn chặn lưu lượng độc hại và giảm tải cho hệ thống.
  + Phân phối tài nguyên mạng (load balancing): Sử dụng các chiến lược cân bằng tải để phân phối lưu lượng đến nhiều máy chủ.
  + Giám sát mạng: Theo dõi lưu lượng mạng liên tục để phát hiện sớm và ứng phó kịp thời với các dấu hiệu của tấn công DDoS.

Tấn công phần mềm độc hại (Malware)

* Mô tả: Malware là các chương trình phần mềm độc hại như virus, trojan, ransomware, và spyware được thiết kế để xâm nhập và gây hại cho hệ thống, đánh cắp dữ liệu, hoặc mã hóa thông tin quan trọng để đòi tiền chuộc.
* Biện pháp phòng chống:
  + Cài đặt và cập nhật phần mềm diệt virus: Sử dụng các chương trình bảo mật cập nhật thường xuyên để phát hiện và tiêu diệt malware.
  + Cập nhật phần mềm và hệ điều hành: Bảo đảm rằng tất cả các phần mềm đều được cập nhật bản vá bảo mật mới nhất để giảm thiểu lỗ hổng.
  + Đào tạo người dùng: Hướng dẫn nhân viên về cách nhận biết các liên kết và tập tin đáng ngờ, đồng thời hạn chế truy cập vào các website không an toàn.

Kỹ thuật xã hội (Social Engineering)

* Mô tả: Kỹ thuật xã hội là khi kẻ xấu sử dụng các phương pháp tâm lý để lừa người dùng cung cấp thông tin nhạy cảm như mật khẩu hoặc thông tin tài chính. Phishing là một trong những hình thức phổ biến nhất, trong đó kẻ tấn công gửi email giả mạo để đánh lừa nạn nhân.
* Biện pháp phòng chống:
  + Đào tạo và nâng cao nhận thức: Tổ chức các buổi đào tạo để giúp người dùng hiểu cách nhận diện các email và tin nhắn giả mạo.
  + Xác thực đa yếu tố (MFA): Bảo vệ tài khoản bằng cách yêu cầu thêm bước xác thực ngoài mật khẩu, chẳng hạn như mã OTP.
  + Cảnh báo bảo mật: Sử dụng các công cụ để phát hiện và cảnh báo người dùng về các mối đe dọa tiềm ẩn.

Tấn công trung gian (Man-in-the-Middle - MITM)

* Mô tả: Tấn công trung gian xảy ra khi kẻ tấn công can thiệp và đánh chặn dữ liệu đang được truyền giữa hai bên mà họ không hay biết. Kẻ xấu có thể theo dõi, đánh cắp hoặc sửa đổi thông tin truyền tải.
* Biện pháp phòng chống:
  + Sử dụng giao thức bảo mật (HTTPS, SSL/TLS): Mã hóa dữ liệu truyền tải để đảm bảo rằng kẻ tấn công không thể đọc hoặc thay đổi thông tin.
  + Sử dụng mạng riêng ảo (VPN): Đảm bảo rằng dữ liệu truyền tải qua mạng công cộng được mã hóa và an toàn.
  + Giám sát và phát hiện hoạt động đáng ngờ: Triển khai các hệ thống giám sát để phát hiện và ngăn chặn các hoạt động can thiệp bất thường.

Tấn công xâm nhập hệ thống (Intrusion)

* Mô tả: Đây là các cuộc tấn công mà kẻ xâm nhập cố gắng khai thác lỗ hổng bảo mật để truy cập vào hệ thống một cách trái phép. Kẻ tấn công có thể đánh cắp, chỉnh sửa hoặc phá hoại dữ liệu.
* Biện pháp phòng chống:
  + Cập nhật và vá lỗi thường xuyên: Đảm bảo rằng các hệ thống và ứng dụng luôn được cập nhật để khắc phục các lỗ hổng bảo mật.
  + Hệ thống phát hiện xâm nhập (IDS/IPS): Sử dụng các công cụ tự động để phát hiện và ngăn chặn các cuộc xâm nhập.
  + Quản lý quyền truy cập: Hạn chế quyền truy cập vào hệ thống dựa trên vai trò và mức độ cần thiết.

Rò rỉ dữ liệu (Data Breach)

* Mô tả: Rò rỉ dữ liệu xảy ra khi thông tin nhạy cảm bị lộ ra ngoài do bị tấn công hoặc vô tình làm lộ thông tin. Hậu quả có thể rất nghiêm trọng, ảnh hưởng đến uy tín và tài chính của tổ chức.
* Biện pháp phòng chống:
  + Mã hóa dữ liệu: Bảo vệ thông tin quan trọng bằng cách mã hóa dữ liệu khi lưu trữ và truyền tải.
  + Quản lý chính sách bảo mật nghiêm ngặt: Thiết lập và thực thi các chính sách bảo mật chặt chẽ, đặc biệt đối với việc xử lý và lưu trữ dữ liệu nhạy cảm.
  + Kiểm tra bảo mật định kỳ: Thực hiện các cuộc kiểm tra bảo mật để đảm bảo hệ thống không có lỗ hổng nào.

# **CHƯƠNG 2. KỸ THUẬT TẤN CÔNG MẠNG GIẢ MẠO ĐỊA CHỈ IP (IP SPOOFING)**

## **2.1. Định nghĩa và phương thức hoạt động của IP Spoofing**

## **2.2. Các loại tấn công liên quan đến IP Spoofing**

Blind IP Spoofing: Kẻ tấn công gửi gói tin mà không cần phản hồi.

Non-blind IP Spoofing: Kẻ tấn công có thể nhìn thấy phản hồi từ máy chủ.

## **2.3. Tác động của IP Spoofing đến an ninh mạng**

## **2.4. Thử nghiệm mô phỏng tấn công IP Spoofing**

# **CHƯƠNG 3. PHƯƠNG PHÁP PHÁT HIỆN GIẢ MẠO ĐỊA CHỈ IP**

## **3.1. Ingress và Egress Filtering**

Lý thuyết + mô phỏng với mỗi phần

## **3.2. Phân tích lưu lượng bất thường**

## **3.3. Kỹ thuật IP Traceback**

## **3.4. Sử dụng giao thức bảo mật IPsec**

# **CHƯƠNG 4. ĐÁNH GIÁ VÀ SO SÁNH CÁC PHƯƠNG PHÁP**

# **KẾT LUẬN**

# **TÀI LIỆU THAM KHẢO**

# **PHỤ LỤC**