ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

NGUYỄN KHÁNH TÙNG

XÂY DỰNG PHƯƠNG PHÁP THU THẬP VÀ PHÂN TÍCH SỐ LIỆU LỖI CẤU HÌNH MẠNG MÁY TÍNH

Ngành: Hệ thống thông tin

Chuyên ngành: Hệ thống thông tin

Mã số: 60480104

LUẬN VĂN THẠC SĨ HỆ THỐNG THÔNG TIN

Hà Nội - 2016

LỜI CAM ĐOAN

Tôi cam đoan luận văn này không sao chép của ai. Nếu sao chép luận văn của người khác, tôi xin chịu hoàn toàn mọi trách nhiệm.

Người cam đoan

Nguyễn Khánh Tùng

MỤC LỤC

DANH MỤC CÁC BẢNG

DANH MỤC HÌNH VẼ VÀ ĐỒ THỊ

CHƯƠNG 1. TỔNG QUAN VỀ AN NINH MẠNG

1.1 Tổng quan về an ninh mạng

Đảm bảo an ninh mạng hiện nay là một yêu cầu cấp thiết trong việc quản trị một hệ thống mạng máy tính. An ninh mạng liên quan đến các giao thức, công nghệ, thiết bị, công cụ và kỹ thuật để đảm bảo an toàn dữ liệu và giảm thiểu các mối đe dọa. Ngay từ những năm 1960, vấn đề an ninh mạng đã được đề cập đến nhưng chưa phát triển thành một tập các giải pháp toàn diện. Cho đến những năm 2000, các giải pháp toàn diện về an ninh mạng mới thực sự được công bố. Các nỗ lực đảm bảo an ninh mạng xuất phát từ việc cần đi trước tin tặc (hacker) có ý đồ xấu một bước. Các chuyên gia an ninh mạng phải liên tục tìm ra các dấu hiệu tấn công, các lỗ hổng, để ngăn chặn các cuộc tấn công tiềm năng trong khi giảm thiểu những ảnh hưởng của các cuộc tấn công. Đảm bảo cho hệ thống hoạt động ổn định, luôn sẵn sàng đáp ứng với các nghiệp vụ kinh doanh cũng là một trong những động lực chính dẫn đến việc bảo đảm an ninh mạng.

Trên thế giới, các tổ chức an ninh mạng được thành lập. Các tổ chức này cung cấp một môi trường hoạt động cộng đồng cho các chuyên gia nhằm trao đổi thông tin, xây dựng những giải ý tưởng, giải pháp về an ninh. Nguồn tài nguyên được cung cấp bởi các tổ chức này (các tài liệu, khuyến nghị, giải pháp…) là rất hữu ích cho công việc hàng ngày của những người làm về an ninh mạng.

Chính sách an ninh mạng được tạo ra bởi các công ty và tổ chức chính phủ để cung cấp một khuôn khổ mà các nhân viên cần phải thực hiện trong công việc hằng ngày của họ. Các chuyên gia an ninh mạng ở cấp quản lý phải chịu trách nhiệm cho việc tạo ra và duy trì các chính sách an ninh mạng. Tất cả các biện pháp an ninh mạng liên quan đến và được hướng dẫn bởi các chính sách an ninh mạng.

Các kỹ thuật tấn công mạng thường được phân loại để tìm hiểu và xử lý một cách thích hợp. Virus, sâu, và Trojan là loại hình cụ thể của các cuộc tấn công mạng. Các cuộc tấn công mạng được phân loại thành các hình thức: tấn công do thám, tấn công truy cập, tấn công từ chối dịch vụ (DoS). Giảm nhẹ các cuộc tấn công mạng là công việc của một chuyên gia an ninh mạng.

1.1.1 Sự phát triển của lĩnh vực an ninh mạng

Năm 2011, sâu code red đã lây lan ra hệ thống mạng trên toàn thế giới. Ước tính có khoảng 350 nghìn máy tính bị lây nhiễm. Sâu code red làm cho các máy chủ không thể

truy cập được và do đó làm ảnh hưởng đến hàng triệu người dùng. Đây là một ví dụ điển hình minh chứng cho thấy nếu quản trị viên không luôn luôn sát sao với hệ thống mình quản lý, đặc biệt là tìm hiểu những lỗ hổng an ninh và cập nhật những bản vá lỗi, thì hậu quả xảy ra có thể là khôn lường. Những hậu quả thường xảy ra do các vụ tấn công mạng có thể gây ra:

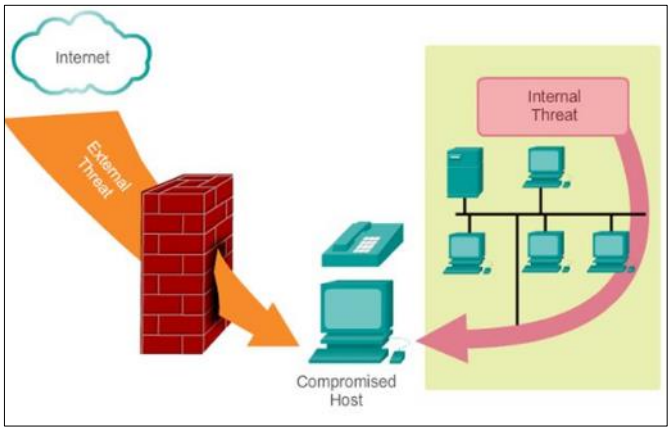
- Mất mát dữ liệu
- Lộ lọt thông tin
- Thông tin bị sửa đổi
- Không truy cập được dịch vụ

Năm 1985 khi các loại sâu, virus phát triển mạnh, những người làm về mạng bắt đầu quan tâm đến việc bảo vệ hệ thống mạng. Lúc đó những tin tặc có kiến thức và kỹ năng rất tốt nhưng những công cụ mà tin tặc tạo ra còn thô sơ. Nhưng đến nay, những công cụ sử dụng để tấn công mạng thường rất phức tạp. Kẻ tấn công không cần nhiều kiến thức và kỹ năng cũng có thể gây ra những cuộc tấn công gây nhiều thiệt hại khi sử dụng những công cụ trên.

Có thể liệt kê một số công cụ bảo vệ hệ thống mạng được xây dựng và phát triển:

- Năm 1990: DEC Packet Filter Firewall, AT&T Bell Labs Stateful Packet Firewall, DEC SEAL Application Firewall.
- Năm 1995: CheckPoint Firewall, NetRanger IDS, RealSecure IDS
- Năm 2000: Snort IDS
- Năm 2005: Cisco Zonebase Policy Firewall
- Năm 2010: Cisco Security Intelligent Operation

Những năm gần đây với sự phát triển của công nghệ điện toán đám mây, sự bùng nổ của các thiết bị di động, thiết bị IoT,…có thêm nhiều giải pháp an ninh mạng toàn diện được phát triển để đáp ứng các yêu cầu bảo vệ đa dạng. Các giải pháp không chỉ ngăn chặn những mối nguy cơ từ bên ngoài, mà cả những nguy cơ xuất phát từ bên trong hệ thống mạng nội bộ.



Hình 1.1 Mối nguy cơ đến từ bên ngoài và bên trong. Nguồn: CCNA Security

Những nguy cơ đến từ bên trong có thể do một nhân viên có kỹ năng nhưng bất mãn và có ý đồ phá hoại. Các nguy cơ xuất phát từ bên trong có thể chia làm 2 dạng: giả mạo (spoofing) hoặc tấn công DoS. Giả mạo là hình thức tấn công trong đó một máy tính thay đổi danh tính để trở thành một máy tính khác. Ví dụ: giả mạo địa chỉ MAC, giả mạo địa chỉ IP. Tấn công từ chối dịch vụ làm cho một máy tính (thường là máy chủ cung cấp dịch vụ) không thể phục vụ được các yêu cầu từ phía máy khách.

Những giải pháp về tường lửa (Firewall), phát hiện và phòng chống xâm nhập (IDS/IPS) có đặc điểm là ngăn chặn những luồng thông tin độc hại (malicious traffic). Bên cạnh đó, việc đảm bảo an ninh mạng là phải bảo vệ được dữ liệu. Mật mã được sử dụng rất phổ biến trong việc bảo đảm an ninh mạng hiện nay. Các dạng truyền tin khác nhau đều có những giao thức và kỹ thuật để che dấu các thông tin của dạng truyền tin đó. Ví dụ mã hóa các cuộc gọi điện thoại trên Internet, mã hóa các file được truyền trên mạng v.v. Mật mã đảm bảo tính bí mật cho dữ liệu. Tính bí mật là một trong ba tính chất của đảm bảo an toàn thông tin đó là: tính bí mật (Confidentiality), tính toàn vẹn (Intergrity) và tính sẵn sàng(Availability). Để đảm bảo tính bí mật của dữ liệu thì phương pháp thường được sử dụng là mã hóa. Để đảm bảo tính toàn vẹn, tức là đảm bảo dữ liệu không bị thay đổi, phương pháp thường được sử dụng là băm (hashing mechanism). Để đảm bảo tính sẵn sàng, tức là luôn có thể truy cập được thông tin khi cần, phương pháp là gia cố hệ thống và sao lưu dự phòng. Một vài giải pháp bảo vệ cho dữ liệu có thể kể đến:

- Năm 1997: giải pháp site-to-site IPSec VPN
- Năm 2001: giải pháp remote access IPSec VPN
- Năm 2005: giải pháp SSL VPN
- Năm 2009: GET VPN

1.1.2 Một số tổ chức an ninh mạng

Đặc thù công việc của các chuyên gia an ninh mạng là phải thường xuyên trao đổi, cập nhật thông tin với các đồng nghiệp cả trong và ngoài nước để nắm bắt được tình hình an ninh mạng trong nươc và thế giới.

Có thể liệt kê một số tổ chức nổi tiếng là:

- Viện SANS (SysAdmin, Audit, Network, Security)

Viện SANS được thành lập vào năm 1989, tập trung vào việc đào tạo và cấp chứng chỉ về an toàn thông tin. SANS xây dựng các tài liệu nghiên cứu về an toàn thông tin, sau đó công bố rộng rãi trên trang web của viện. Các tài liệu này thường xuyên được cập nhật và được đóng góp ý kiến bởi cộng đồng những người làm an ninh mạng.

Bên cạnh đó SANS xây dựng những khóa học về bảo mật từ cấp độ cơ bản đến nâng cao để trang bị những kỹ năng chuyên nghiệp cho những người làm bảo mật, ví như ví dụ các kỹ năng về giám sát an ninh, phát hiện xâm nhập, điều tra thông tin, các kỹ thuật của hacker, sử dụng tường lửa bảo vệ hệ thống mạng, lập trình ứng dụng an toàn…

- Trung tâm Phản Ứng Nhanh Sự Cố Máy Tính (Computer Emergency Response Team – CERT)

Tháng 12/1988, sau khi xảy ra sự cố sâu MORRIS phát tán và lây lan, văn phòng DARPA thuộc bộ quốc phòng Mỹ đã quyết định thành lập Trung tâm Phản Ứng Nhanh Sự Cố Máy Tính, viết tắt là CERT.

CERT giải quyết những sự cố an ninh lớn và phân tích các lỗ hổng phát hiện được. Từ việc phát hiện này, CERT phát triển các giải pháp kỹ thuật công nghệ, các giải pháp quản lý để chống lại và làm giảm thiệt hại do các vụ tấn công trong tương lai. Bằng những kinh nghiệm có được, CERT có thể sớm phát hiện tấn công và hỗ trợ cơ quan an ninh truy bắt kẻ tấn công.

Hiện nay CERT tập trung vào 5 mảng chính đó là: bảo hiểm phần mềm, bảo mật hệ thống, an toàn thông tin trong tổ chức, phối hợp tác chiến, giáo dục đào tạo.

- (ISC)2: International Information Systems Security Certification Consortium

Đây là tổ chức nổi tiếng với chứng chỉ CISSP danh giá, có thể coi là hàng đầu trong số các chứng chỉ quốc tế về an ninh mạng. Tuy nhiên nhiệm vụ chính của (ISC)2 là góp phần làm cho không gian mạng toàn cầu trở nên an toàn hơn bằng việc nâng cao nhận

thức về an toàn thông tin cho cộng đồng và xây dựng đội ngũ chuyên gia an ninh mạng trên toàn thế giới.

Hiện nay các sản phẩm và dịch vụ đào tạo của ISC2 đã có mặt ở trên 135 quốc gia và tổ chức này có hơn 75000 chuyên gia thành viên trên khắp thế giới. Khi bạn là thành viên của ISC2, bạn có thể tham gia trao đổi với mạng lưới các chuyên gia này.

-InfoSysSec

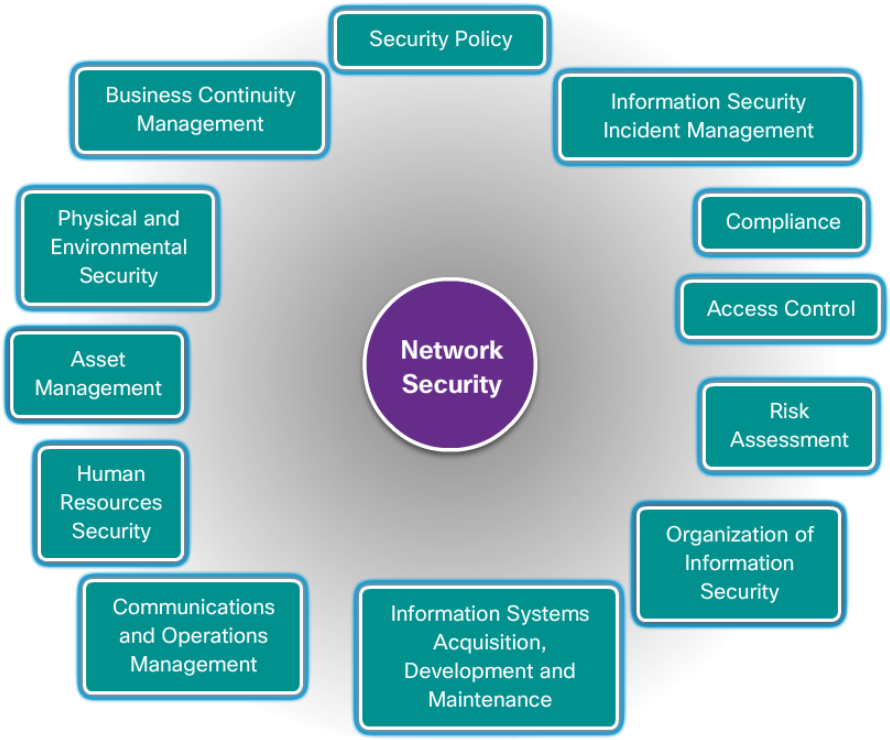
Là tổ chức về an ninh mạng, có các cổng thông tin cập nhật về các cảnh báo an ninh, các lỗ hổng, các khai thác.

- MITRE

Là tổ chức đang lưu trữ và công khai danh sách các lỗ hổng bảo mật phổ biến (Common Vulnerabilities and Exposures - CVE) phổ biến. Bạn có thể tra cứu thông tin bằng CVE-ID tại website này.

Bên cạnh đó còn có các diễn đàn và tổ chức như FIRST (Forum of Incident Response and Security Teams, Center for Internet Security (CIS).

1.1.3 Các lĩnh vực về an ninh mạng



Hình 1.2 Các lĩnh vực an ninh mạng

Được đề cập trong tiêu chuẩn ISO/IEC 27002, 12 lĩnh vực về an ninh mạng đóng vai trò là một cái nhìn tổng thể, giúp cho những người theo đuổi an ninh mạng có thể nắm được tổng quan và đi theo các lĩnh vực chuyên sâu. Bên cạnh đó, việc đưa ra 12 lĩnh vực về an ninh mạng còn giúp cho các tổ chức có thể xây dựng những tiêu chuẩn, những quy tắc thực thi tốt nhất, thúc đẩy sự trao đổi thông tin giữa các tổ chức.

- *Chính sách an ninh:* là một văn bản quy định các vấn đề liên quan đến việc đảm bảo an toàn khi sử dụng hệ thống công nghệ thông tin trong doanh nghiệp. Chính sách an ninh chỉ ra cách thức truy cập dữ liệu như thế nào và những dữ liệu nào được phép truy cập và truy cập bởi những ai.

- *Quản lý sự cố về an ninh:* mô tả cách thức đối phó và xử lý những lỗ hổng về an ninh có thể xảy ra.

- *Hợp chuẩn (compliance):* mô tả quá trình nhằm đảm bảo rằng hệ thống là tuân thủ các chính sách an ninh, các tiêu chuẩn, các quy tắc đặt ra từ trước.

- *Điều khiển truy cập (Access Control):* mô tả những quy tắc giới hạn việc truy cập vào mạng, hệ thống, ứng dụng, chức năng, và dữ liệu.

- *Đánh giá rủi ro (risk assessment):* là bước đầu tiên trong quá trình quản lý rủi ro. Nó ước tính về giá trị, số lượng tài sản gặp rủi ro trong những tình huống mất an ninh xảy ra.

- *Tổ chức an toàn thông tin (Organization of Information Security):* là mô hình mà tổ chức đề ra nhằm đảm bảo an toàn thông tin.

- *Xây dựng hệ thống thông tin, phát triển và bảo trì:* mô tả cách thức tích hợp yếu tố an ninh vào các ứng dụng.

- *Quản lý việc truyền thông và hoạt động:* mô tả việc quản lý các khía cạnh kỹ thuật về an ninh trong hệ thống và mạng.

- *An ninh nguồn nhân lực:* mô tả các thủ tục nhằm đảm bảo tính an ninh trong việc tuyển dụng nhân sự, điều động nhân sự nội bộ và nghỉ việc của nhân viên, trong một tổ chức.

- *Quản lý tài sản thông tin:* là bản kiểm kê, có sự phân loại các tài sản thông tin.

- *An ninh vật lý và môi trường:* mô tả việc bảo vệ về mặt vật lý cho hệ thống máy tính trong một tổ chức.

- *Quản lý tính liên tục trong kinh doanh:* mô tả việc bảo vệ, bảo trì và khôi phục những nghiệp vụ kinh doanh và hệ thống cốt lõi .

1.1.4 Chính sách an ninh mạng

Các chính sách an ninh mạng là một tài liệu được phổ biến rộng rãi cho người dùng hệ thống mạng, được viết một cách rõ ràng nhằm áp dụng cho hoạt động của một tổ chức. Chính sách này còn được sử dụng để hỗ trợ trong việc thiết kế mạng, truyền thông các nguyên tắc bảo mật, và tạo thuận lợi cho việc triển khai mạng.

Các chính sách an ninh mạng chỉ ra quy tắc cho việc truy cập vào mạng, xác định các chính sách được thực thi, và mô tả kiến trúc cơ bản của môi trường an ninh mạng của tổ chức. Do tính chất của chính sách an ninh là khá rộng, do vậy nó thường được biên soạn bởi một nhóm người có trách nhiệm liên quan. Chính sách an ninh là một tài liệu phức tạp bao gồm các mục, như truy cập dữ liệu, duyệt web, sử dụng mật khẩu, mã hóa, và đính kèm email.

Khi một chính sách được tạo ra, nó phải rõ ràng những gì dịch vụ phải được cung cấp cho người sử dụng cụ thể. Các chính sách an ninh mạng thiết lập một hệ thống các quyền truy cập, cho nhân viên chỉ có quyền truy cập tối thiểu cần thiết để thực hiện công việc của họ.

Các chính sách an ninh mạng chỉ ra những tài sản cần được bảo vệ và hướng dẫn về cách làm thế nào để bảo vệ các tài sản đó. Từ đó có thể xác định các thiết bị an ninh, chiến lược và quy trình làm giảm các vụ tấn công mạng.

1.1.5 Khái niệm lỗi cấu hình an ninh

Hạ tầng mạng trong các công ty/tổ chức bao gồm các máy chủ, thiết bị mạng. Những người quản trị mạng chịu trách nhiệm quản lý hạ tầng mạng. Một trong những nhiệm vụ của người quản trị mạng là cấu hình bảo đảm tính an ninh cho các thiết bị mạng. Các cấu hình an ninh (secure configuration) được thực hiện theo các chính sách an ninh của công ty/tổ chức. Cấu hình là những câu lệnh được quản trị viên nhập vào giao diện dòng lệnh trên thiết bị. Ví dụ một cấu hình an ninh "Bật giao thức SSH" trên thiết bị mạng:

```
!
hostname router
!
ip domain-name example.com
!
crypto key generate rsa modulus 2048
!
ip ssh time-out 60
ip ssh authentication-retries 3
```

```
ip ssh source-interface GigabitEthernet 0/1
!
ip ssh version 2
!
line vty 0 4
transport input ssh
!
```

Cấu hình an ninh là cấu hình nhằm bảo vệ an toàn cho thiết bị. Một vài ví dụ về cấu hình an ninh:

- Những dịch vụ mạng không được sử dụng thì nên tắt;

- Phải đổi mật khẩu tài khoản quản trị mặc định trên thiết bị;

- Khi tạo các kết nối quản lý từ xa tới thiết bị nên sử dụng giao thức an toàn như SSH (Secure Shell) thay vì sử dụng giao thức kém an toàn như Telnet…

Cần phân biệt khái niệm *"Cấu hình an ninh" và "An ninh cấu hình". Cấu hình an ninh* là những cấu hình nhằm bảo vệ cho thiết bị trước những nguy cơ tấn công có thể xảy ra. Ví dụ: cấu hình an ninh cổng switch để tránh tấn công làm tràn bảng MAC... Còn *"An ninh cấu hình"* nhằm bảo đảm an toàn cho những cấu hình đang hoạt động: phòng tránh bị lộ thông tin cấu hình, bị sửa đổi cấu hình trái phép.

Một hệ thống mạng được xem là quản lý yếu kém là mạng mà trong đó các thiết bị không được cấu hình đầy đủ các chính sách về an ninh. Từ đó trên các thiết bị mạng có các lỗ hổng, dẫn đến bị kẻ tấn công khai thác và thực hiện các hành vi có chủ đích của hắn.

1.1.6 Khái niệm về đường cơ sở an ninh (Security Baseline)

Đường cơ sở an ninh là một danh sách kiểm tra (checklist) mà theo đó các hệ thống được đánh giá và kiểm toán đối với tình hình an ninh trong một tổ chức. Đường cơ sở phác thảo ra những yếu tố an ninh chính đối với một hệ thống, và trở thành điểm xuất phát cho việc bảo vệ hệ thống đó.[1]

[1] *Theo giáo trình CompTIA Security+*

Trong y học, đường cơ sở là giá trị dữ liệu đã biết ban đầu, được xác định ngay từ khi bắt đầu nghiên cứu, dùng để so sánh với giá trị dữ liệu tích góp được về sau. Trong công nghệ thông tin, giá trị ban đầu đó không phải là trạng thái bảo mật hiện tại của một hệ thống, trái lại nó là một tiêu chuẩn, theo đó trạng thái hiện tại được so sánh.

Báo cáo đường cơ sở an ninh là việc so sánh trạng thái hiện tại của một hệ thống với đường cơ sở của nó. Mọi sự khác biệt cần được ghi nhận và giải quyết đúng đắn. Những sự khác biệt đó không chỉ là về vấn đề kỹ thuật, mà còn bao gồm về vấn đề quản lý và vận hành. Do vậy cần hiểu một điều là không phải mọi sai khác với đường cơ sở là có hại, bởi vì mỗi hệ thống có đặc điểm khác nhau. Tuy nhiên mọi sự khác biệt đều phải được ghi nhận, đánh giá và lập tài liệu rõ ràng.

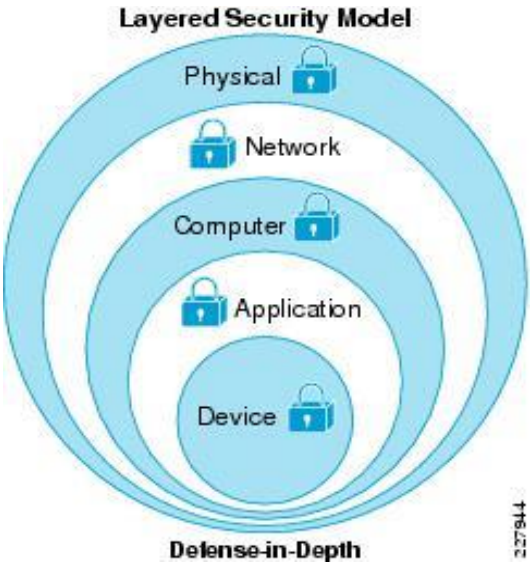
Theo Phòng an ninh máy tính của tổ chức nguyên tử châu Âu (CERN Computer Security), đường cơ sở an ninh xác định một tập hợp các mục tiêu cơ bản về an ninh mà bất kỳ một hệ thống hay dịch vụ nào đều phải đạt được. Để thực hiện các mục tiêu này, cần phải có tài liệu hướng dẫn kỹ thuật chi tiết đối với từng hệ thống cụ thể. (CERN).[2]

Theo Cisco, đường cơ sở an ninh mạng là một tập các khuyến nghị cần thực hiện để đảm bảo an ninh cho hệ thống mạng đó. Các khuyến nghị này được đúc kết từ kinh nghiệm triển khai thực tế, có tính cơ bản và tổng quát, không quá khó để triển khai. Đây cũng là cơ sở để thực hiện nguyên tắc phòng thủ theo chiều sâu (defence-in-depth). Để thực hiện nguyên tắc này thì việc đầu tiên cần đảm bảo đó là cần phải kiểm tra đánh giá xem hệ thống có đạt được các mục tiêu mà đường an ninh cơ sở đề ra hay không.[3]

---

[2] *https://security.web.cern.ch/security/rules/en/baselines.shtml*

[3] *http://www.cisco.com/c/dam/en/us/td/docs/solutions/CRD/Sep2015/WP-Enterprise-Security-Baseline-Sep15.pdf*



Hình 1.3 Cơ chế phòng thủ theo chiều sâu

1.1.7 Khái niệm gia cố thiết bị (device hardening)

Mục đích của việc gia cố thiết bị là làm giảm càng nhiều rủi ro càng tốt, và làm cho hệ thống an toàn hơn. Thiết bị hạ tầng mạng khi mua về đều có các thông số cấu hình mặc định từ nhà sản xuất (ví dụ: tài khoản và mật khẩu mặc định, dịch vụ chạy mặc định…). Khi đưa vào sử dụng, quản trị viên cần cấu hình lại những tham số này sao cho phù hợp với các tiêu chuẩn an ninh được đề cập đến trong chính sách an ninh của doanh nghiệp.

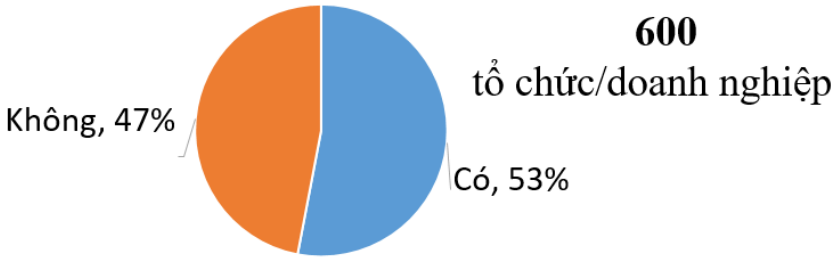
1.2 Lý do lựa chọn đề tài

1.2.1 Phân tích một vài chỉ số về ATTT tại Việt Nam năm 2015

Tại Hội thảo Ngày An toàn thông tin Việt Nam 2015, Hiệp hội An toàn thông tin Việt Nam (VNISA) đã công bố báo cáo *Kết quả khảo sát thực trạng an toàn thông tin Việt Nam năm 2015* và đưa ra Chỉ số An toàn thông tin Việt Nam 2015 - VNISA Index 2015. Theo đó, chỉ số trung bình của Việt Nam là 46,5%, tuy ở dưới mức trung bình và vẫn còn sự cách biệt với các nước như Hàn Quốc (hơn 60%), song so với năm 2014 thì đã có bước tiến rõ rệt (tăng 7,4%). Năm nay, VNISA tiến hành khảo sát với 600 tổ chức, doanh nghiệp (TC/DN) trong cả nước (trong đó có 40% tổ chức là trong khu vực nhà nước) với 36 tiêu chí đánh giá ở các cấp độ khác nhau. Trong số các TC/DN được khảo sát, có 51% là các TC/DN có quy mô nhỏ (sử dụng từ 1-50 máy tính), 27% (sử dụng từ 50-300 máy tính). Số còn lại có quy mô trên 300 máy tính.

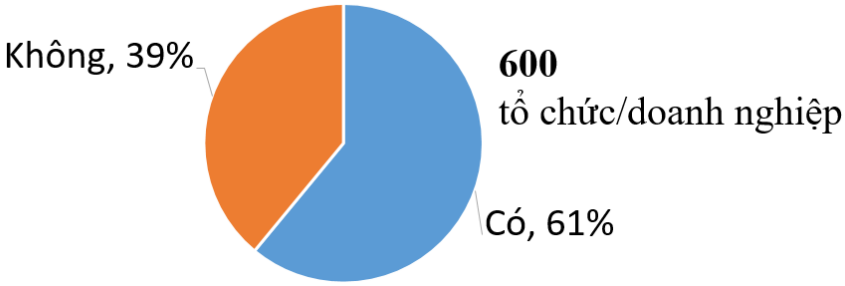
Một vài thống kê đáng lưu tâm trong báo cáo trên:

- Khi hỏi: Hệ thống của tổ chức có được kiểm tra, đánh giá ATTT (ATTT) hay không? **53% trả lời là có và 47% trả lời là không**.



Hình 1.4 Tỉ lệ đánh giá ATTT trong tổ chức doanh nghiệp

- Khi hỏi cán bộ vận hành, khai thác, sử dụng hệ thống của tổ chức đã tuân thủ các chính sách về ATTT hay không: **Có 61% cho rằng có tuân thủ và 39% không tuân thủ.**



Hình 1.5 Tỉ lệ tuân thủ các chính sách ATTT

- Quy trình đánh giá, quản lý và xử lý nguy cơ về ATTT trong các TC/DN vẫn còn nhiều hạn chế, **62% được đánh giá không theo quy trình, chỉ có 28% là tuân thủ theo đúng quy trình.**
- ***Một trong các vấn đề khó khăn nhất*** mà TC/DN gặp phải trong việc bảo đảm ATTT cho thông tin và hệ thống đó là *việc quản lý chặt chẽ cấu hình hệ thống mạng (Configuration Management).*

Qua các thông tin ở trên có thể thấy rằng:

→ Cần phải đẩy mạnh công tác đánh giá sự an toàn của một hệ thống CNTT.

→ Bên cạnh đó vì một trong những khó khăn lớn nhất mà doanh nghiệp gặp phải đó là làm thế nào để quản lý được cấu hình mạng. Hệ thống mạng trong doanh nghiệp có thể phức tạp, nhiều thiết bị. Mỗi thiết bị có nhiều cấu hình. Việc quản lý cấu hình thiết bị mạng đảm bảo cấu hình đó là an toàn theo đúng theo các khuyến nghị, các tiêu chuẩn là một vấn đề khó nhưng cần giải quyết.

1.2.2 Tầm quan trọng của việc quản lý cấu hình mạng

Năm 2011, trong một báo cáo của hãng phân tích Gartner chỉ ra rằng, *việc quản lý cấu hình an ninh* là một việc bắt buộc phải làm, và là ưu tiên số 1 trong danh sách các công việc bảo vệ cho máy chủ.[4]

Năm 2012, tạp chí ATTT SANS đã đưa ra 20 mức độ cấp thiết khi quản lý an ninh cho một tổ chức (SANS 20 Critical Security Control), trong đó xếp hạng mức độ cấp thiết của việc quản lý cấu hình an ninh cho máy chủ, hệ thống, thiết bị đầu cuối có mức độ 3; xếp hạng mức độ cấp thiết việc quản lý cấu hình an ninh trên các thiết bị mạng là cấp độ 10.[5]

Theo một khảo sát năm 2012 của tạp chí InformationWeek đối với 900 chuyên gia công nghệ thông tin, thì việc triển khai các chính sách an ninh là một việc có mức độ khó xếp hạng thứ 2. Tại sao? Bởi vì nó quá nặng nhọc. Với một hệ thống có hàng trăm, thậm chí hàng nghìn, hàng chục nghìn thiết bị mạng, làm thế nào để bảo đảm các thiết bị này có cấu hình an ninh tuân thủ theo đúng chính sách? Làm thế nào để biết những quản trị viên khác không thay đổi những cấu hình an ninh tiêu chuẩn? Khi cần gấp một việc gì đó, có thể phải thực thi một vài chính sách kém an ninh nhưng sau đó làm sao để khôi phục lại trạng thái an ninh ban đầu theo khuyến nghị? Làm thế nào để tự động hóa công việc triển khai cấu hình an ninh trên những hạ tầng không đồng nhất?...Đó là những câu hỏi luôn làm đau đầu những quản trị viên.[6]

Trong một báo cáo kinh doanh của hãng truyền thông Verizon (Mỹ), hacker thường xuyên khai thác thành công những lỗi cấu hình và những lỗ hổng đã được biết từ trước, để thực hiện xâm nhập vào hệ thống của nạn nhân.[7]

Qua những số liệu nêu trên, có thể thấy rằng việc quản lý cấu hình để ngăn ngừa những lỗi có thể xảy ra là một vấn đề rất cần được quan tâm trong công tác quản trị mạng. *Mặc dù việc này không đơn giản nhưng cần có những giải pháp để kiểm tra, đánh giá một hệ thống có tồn tại những lỗi cấu hình hay không, và từ đó đưa ra cách khắc phục.*

---

[4] *Neil MacDonald and Peter Firstbrook, "How To Devise a Server Protection Strategy," December 2011. www.gartner.com/id=1866915*

[5] *http://www.networkworld.com/article/2992503/security/sans-20-critical-security-controls-you-need-to-add.html*

[6] *http://reports.informationweek.com/abstract/21/8815/Security/research-2012-strategic-security-survey.html*

[7] *http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf*

1.2.3 Các hình thức tấn công mạng khai thác lỗi cấu hình.

Theo thống kê cho thấy, năm 2015, có nhiều hình thức tấn công với những kỹ thuật khác nhau, phổ biến nhất là các kỹ thuật: *Tấn công dò quét điểm yếu dịch vụ UPNP, tấn công gây từ chối dịch vụ phân giải tên miền DNS, tấn công dò mật khẩu dịch vụ FTP bằng phương pháp vét cạn (brute force login attempt) ...*

Số lượng các cuộc tấn công theo từng loại hình kỹ thuật đã được Trung tâm ứng cứu sự cố máy tính khẩn cấp (VNCERT) thống kê cụ thể hàng năm với con số không nhỏ. Dưới đây là bảng thống kê theo quý Top 5 kỹ thuật tấn công trong năm 2015 vào hệ thống thông tin nước ta:

STT	TÊN KỸ THUẬT TẤN CÔNG	SỐ LƯỢNG
QUÝ I		
1	Tấn công dò quét điểm yếu dịch vụ UPNP	1165518
2	Tấn công gây từ chối dịch vụ phân giải tên miền DNS	950146
3	Lạm dụng các dịch vụ của Google để tiến hành tấn công các hệ thống trang thông tin điện tử gây tình trạng từ chối dịch vụ	219061
4	Tấn công dò mật khẩu dịch vụ FTP bằng phương pháp vét cạn (brut force login attempt)	204926
5	Tấn công máy chủ website sử dụng phần mềm APACHE	154862
QUÝ II		
1	Tấn công dò quét điểm yếu dịch vụ UPNP	293015
2	Tấn công dò mật khẩu dịch vụ FTP bằng phương pháp vét cạn (brut force login attempt)	240912
3	Tấn công chuyển hướng tên miền nhằm vào người dùng thông qua dịch vụ DNS bằng kỹ thuật dns cache poisoning	217938
4	Tấn công vét cạn mật khẩu thông qua dịch vụ SSH	174910

5	Tấn công điểm yếu ứng dụng Web thông qua giao thức HTTP POST request khi tính năng file_uploads được kích hoạt	96052
QUÝ III		
1	Tấn công khai thác điểm yếu bảo mật của ứng dụng Web	2352175
2	Lây nhiễm mã độc, kết nối đến mạng lưới mã độc qua dịch vụ DNS	944694
3	Lạm dụng dịch vụ calendar access của các hệ thống trang thông tin điện tử để thu thập thông tin	327714
4	Tấn công chuyển hướng tên miền nhằm vào người dùng thông qua dịch vụ DNS bằng kỹ thuật dns cache poisoning	283958
5	Tấn công vét cạn mật khẩu thông qua dịch vụ SSH	248713
QUÝ IV		
1	Tấn công gây từ chối dịch vụ phân giải tên miền DNS bằng phương pháp truy vấn random DNS domain nhằm vào dịch vụ DNS	741184
2	Tấn công dò quét điểm yếu dịch vụ UPNP	234865
3	Lạm dụng dịch vụ calendar access của các hệ thống trang thông tin điện tử để thu thập thông tin	196255
4	Tấn công gây từ chối dịch vụ phân giải tên miền DNS	179827
5	Tấn công chuyển hướng tên miền nhằm vào người dùng thông qua dịch vụ DNS bằng kỹ thuật dns cache poisoning	173814

Bảng 1.1 Các kỹ thuật tấn công vào hệ thống mạng Việt Nam năm 2015

Thống kê trên cho thấy các kỹ thuật tấn công phổ biến vào hệ thống thông tin của nước ta là rất đa dạng và thay đổi liên tục. Trong đó có thể thấy ở thống kê trên, một trong những thủ đoạn của kẻ tấn công thường ngắm tới những *điểm yếu về về cấu hình*. Một số ví dụ có thể chỉ ra dưới đây:

Ví dụ 1: hình thức dò quét điểm yếu của giao thức UPNP, theo khuyến nghị cần tắt dịch vụ UPNP trên các thiết bị nếu không sử dụng bởi vì UPNP có rất nhiều lỗ hổng bảo mật. Tuy nhiên nếu người quản trị không thực hiện việc này thì rất có thể hệ thống mạng sẽ bị tấn công.

Ví dụ 2: là tấn công dò mật khẩu dịch vụ FTP, SSH bằng phương pháp vét cạn (brute force login attempt). Theo khuyến nghị, khi đặt mật khẩu cần phải đặt mật khẩu mạnh (thỏa mãn tiêu chí về độ dài, sư kết hợp các ký tự trên bàn phím). Nếu quản trị viên hệ thống/người dùng sử dụng mật khẩu yếu (đơn giản, dễ đoán) để cài đặt cho các dịch vụ SSH, FTP, thì sẽ trở thành nạn nhân của kỹ thuật tấn công dạng này.

Qua phân tích ở trên có thể thấy rằng nếu quản trị viên không tuân thủ các khuyến nghị về an ninh khi cấu hình hệ thống thì có thể dẫn đến hệ thống đó có những điểm yếu và bị khai thác bởi kẻ tấn công.

1.2.4 Hậu quả của những vụ tấn công mạng do lỗi cấu hình.

Tại Việt Nam trong năm 2015 và 2016, theo thống kê của công ty an ninh mạng BKAV, xảy ra một số vụ việc mất an toàn thông tin do việc cấu hình trên thiết bị mạng:

- Tháng 06/2016, có 70.624 máy chủ Remote Desktop Protocol (RDP) được rao bán trên thị trường chợ đen xDedic và giá chỉ 6 USD cho mỗi quyền truy cập, trong đó có 841 máy chủ ở Việt Nam. Sau khi các đơn vị an ninh mạng Việt Nam tiến hành tìm hiểu và kiểm tra trên thực tế thông tin các máy chủ Remote Desktop Protocol (RDP) tại Việt Nam được rao bán trên thị trường chợ đen xDedic, kết quả cho thấy, 153 máy chủ vẫn đang *mở cổng 3389 (RDP), trong đó có 51 máy chủ mở cả cổng 3389 (RDP) và 80 (HTTP)*. Những máy chủ này có nguy cơ bị khai thác, chiếm quyền điều khiển và bị lợi dụng cho những mục đích xấu. Chỉ từ 6 USD cho mỗi máy chủ, thành viên diễn đàn xDedic đã có thể truy cập vào tất cả dữ liệu của một máy chủ và sử dụng chúng như nền tảng để tấn công về sau, có thể bao gồm tấn công có chủ đích, phần mềm độc hại, DDoS, lừa đảo bằng email, tấn công bằng kỹ thuật xã hội và adware. Cũng theo kết quả kiểm tra, trong số 153 máy chủ này, có 7 máy chủ thuộc các cơ quan nhà nước, 20 máy chủ thuộc doanh nghiệp… Chúng có thể được dùng để tấn công hệ thống hoặc làm bệ phóng

cho những cuộc tấn công lớn hơn, trong khi đó, chủ hệ thống, bao gồm các tổ chức chính phủ, tập đoàn và trường đại học lại biết rất ít hoặc chẳng biết gì về chuyện đang xảy ra.[8]

- Cũng trong 4 tháng đầu năm 2015, theo báo cáo bảo mật từ công ty bảo mật BKAV, sau những ghi nhận từ hệ thống phòng vệ DDoS của mình cho thấy có nhiều cuộc tấn công-từ chối-dịch vụ (DDoS) xuất phát từ nhiều địa chỉ IP thuộc nhiều nhà cung cấp dịch vụ Internet (ISP) tại nhiều quốc gia. Những địa chỉ IP này xuất phát từ các router (bộ định tuyến mạng) kết nối Internet dùng trong gia đình hay doanh nghiệp nhỏ đã bị hack. *Và tất cả router "thây ma" đều không được người dùng thay đổi mật khẩu mặc định của tài khoản quản trị (admin) từ nhà sản xuất*. Hacker có thể lấy được tài khoản quản trị này rất dễ dàng, chỉ cần tham khảo tài liệu nhà sản xuất công bố rộng rãi trên mạng. Khi nắm trong tay tài khoản quản trị có đủ quyền thiết lập cho router, hacker có thể điều khiển hướng truy cập của các thiết bị kết nối Internet thông qua router đó đến các địa chỉ website mà chúng muốn. Từ đó có thể lây nhiễm mã độc, chiếm giữ thêm các tài khoản khác của người dùng hoặc gia tăng lưu lượng truy cập cho các website kiếm tiền từ quảng cáo, hay dùng các thiết bị của nạn nhân như di động hay máy tính tham gia đội quân "botnet" để tấn công-từ chối-dịch vụ (DDoS) nhắm vào các mục tiêu định sẵn. Hacker còn có thể đánh cắp dữ liệu ra vào mạng Internet gia đình hay doanh nghiệp.[9]

→ Vậy vấn đề đặt ra ở đây là làm thế nào để đánh giá một hệ thống được cấu hình có tuân thủ các khuyến nghị hoặc tiêu chuẩn an toàn hay không? Từ đó có các biện pháp khắc phục những điểm yếu về cấu hình, làm giảm khả năng bị hacker khai thác

---

[8] *http://vnreview.vn/tin-tuc-an-ninh-mang/-/view_content/content/1861042/thi-truong-cho-den-dang-rao-ban-hon-841-may-chu-viet-nam-bi-hack*

[9] *https://forum.whitehat.vn/forum/thao-luan/tin-tuc/57141-hon-300-nghin-he-thong-mang-tai-viet-nam-dang-trong-tinh-trang----bo-ngo---*

1.3 Phương pháp nghiên cứu và kết quả đạt được

1.3.1 Phương pháp nghiên cứu

Mục tiêu của luận văn này tập trung vào việc *phân tích và đánh giá xem cấu hình an ninh trên các thiết bị hạ tầng mạng của một tổ chức, doanh nghiệp có tuân thủ theo chính sách an ninh* của tổ chức đó hay không.

Để thực hiện được việc này, đầu tiên luận văn khảo sát một mô hình mạng máy tính điển hình, được sử dụng phổ biến tại các doanh nghiệp. Mặc dù các doanh nghiệp có quy mô khác nhau, yêu cầu khác nhau đối với hệ thống mạng máy tính, tuy nhiên khi xây dựng mạng, cần tuân thủ những nguyên lý chung về thiết kế, nhằm đảm bảo cho hệ thống mạng đạt được những tiêu chí về tính sẵn sàng, tính mở rộng, tính an ninh và khả năng quản lý. Luận văn sẽ khảo sát mô hình mạng tuân thủ theo nguyên lý thiết kế phân tầng: tầng truy nhập (access layer), tầng phân phối (distribution layer) và tầng lõi (core layer). Ở mỗi tầng sẽ có những thiết bị mạng đặc trưng, để thực hiện những chức năng của tầng đó. Trong luận văn sẽ đề cập đến các thiết bị mạng ở các tầng như sau:

- Tầng access: thiết bị switch lớp 2 (switch), thiết bị định tuyến không dây (Wireless Router – WR). Các thiết bị này đóng vai trò kết nối thiết bị đầu cuối người dùng vào mạng.
- Tầng distribution: thiết bị định tuyến (Router). Các thiết bị này thực hiện tính năng định tuyến liên mạng.
- Tầng Core: thiết bị định tuyến (Router). Các thiết bị này thực hiện tính năng chuyển mạch tốc độ cao.

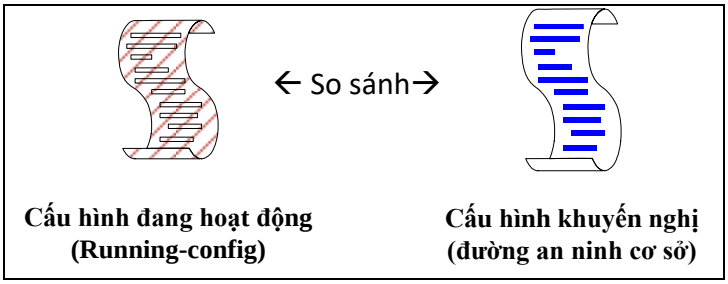
Tiếp theo, luận văn sẽ chỉ ra những lỗi cấu hình an ninh thường gặp trên các thiết bị ở từng tầng. Cấu hình an ninh là những cấu hình nhằm đảm bảo sự an toàn cho thiết bị khi hoạt động. Nếu không cấu hình hoặc cấu hình sai, sẽ dẫn đến sự mất an toàn cho hệ thống mạng. Luận văn sẽ làm rõ từng cấu hình an ninh; những nguy cơ mất an toàn có thể xảy ra khi không thực hiện cấu hình an ninh đó; cách thức cài đặt cấu hình an ninh như thế nào. Những lỗi cấu hình an ninh thường được tham khảo ở các tài liệu của hãng sản xuất thiết bị, các tài liệu khuyến nghị an ninh; các tiêu chuẩn an ninh trên thiết bị mạng.

Bước tiếp theo, luận văn sẽ đề xuất phương pháp thu thập cấu hình trên các thiết bị mạng về một máy chủ lưu trữ tập trung. Việc thu thập cấu hình cần thỏa mãn các yêu cầu nhất định. Do vậy luận văn đề xuất phương pháp thu thập số liệu bao gồm cả quy trình, con

người, máy móc, phần mềm, kỹ thuật thực hiện. Các yếu tố trên cần được kết hợp theo trình tự logic và có kiểm tra nhằm đảm bảo việc thu thập diễn ra thành công, thỏa mãn các yêu cầu đề ra từ đầu.

Hình 1.6 Phương pháp thu thập cấu hình

Sau khi đã thu thập cấu hình tập trung, luận văn đề xuất phương pháp đánh giá xem cấu hình an ninh trên từng thiết bị có tuân thủ theo quy định hay không. Phương pháp là so sánh giữa cấu hình thu thập được và cấu hình mẫu (khuyến nghị).



Hình 1.7 Phương pháp đánh giá cấu hình an ninh

Kết quả thu được sau bước đánh giá này là một báo cáo tổng hợp về tình trạng cấu hình an ninh trên các thiết bị mạng của tổ chức đó.

Để hỗ trợ cho việc đánh giá, luận văn đề xuất xây dựng một chương trình ứng dụng phân tích cấu hình tự động. Đầu vào của chương trình là một thư mục chứa các file cấu hình của các thiết bị mạng trong một hệ thống mạng. Đầu ra là kết quả báo cáo tổng hợp về tình trạng cấu hình an ninh của hệ thống mạng đó. Ngoài ra chương trình còn xuất ra báo cáo chi tiết những lỗi cấu hình an ninh trên từng thiết bị mạng. Đây có thể coi là một ưu điểm của chương trình so với một số phần mềm ứng dụng khác đang được sử dụng.

Thiết bị hạ tầng mạng đề cập đến trong luận văn là thiết bị định tuyến - Router, thiết bị chuyển mạch - switch, thiết bị định tuyến không dây - wireless router. Lựa chọn hãng

thiết bị là hãng **Cisco**, được sử dụng phổ biến trong mạng của các công ty, tổ chức tại Việt Nam.

Phạm vi phân tích là mạng máy tính của một doanh nghiệp tại trụ sở chính của doanh nghiệp đó. Tức là không bao gồm hệ thống mạng diện rộng (WAN).

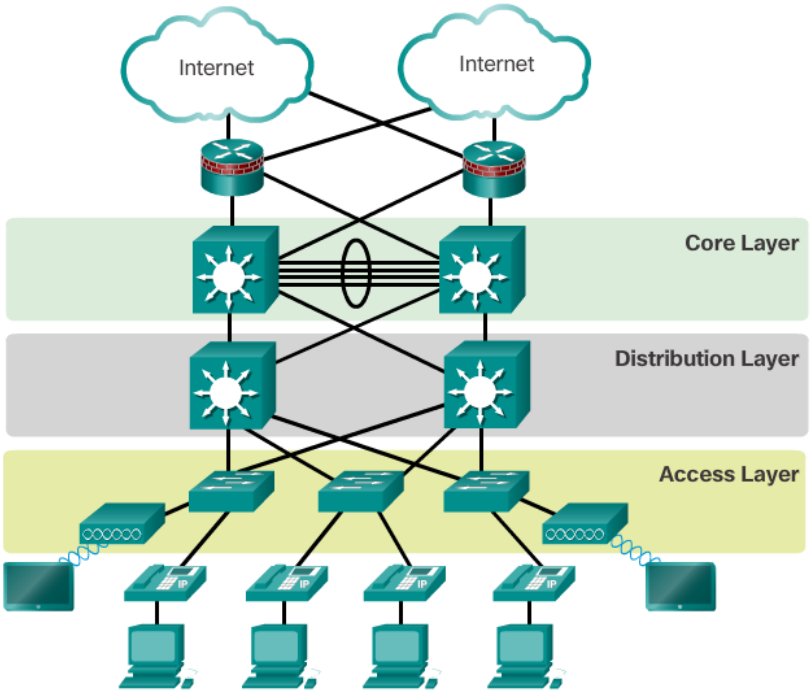
1.3.2 Kết quả đạt được của luận văn

- Phân tích được tầm quan trọng của việc quản lý cấu hình trong công tác đảm bảo an toàn cho hệ thống mạng máy tính của doanh nghiệp.
- Làm rõ được những lỗi cấu hình an ninh trên thiết bị mạng, những nguy cơ có thể xảy ra khi để tồn tại những lỗi này; cách cấu hình khắc phục lỗi.
- Đề xuất được phương pháp thu thập cấu hình tập trung
- Đề xuất được phương pháp đánh giá lỗi cấu hình.
- Xây dựng chương trình đánh giá cấu lỗi cấu hình có những ưu điểm hơn so với những chương trình hiện có.

CHƯƠNG 2. KHẢO SÁT MỘT MẠNG MÁY TÍNH ĐIỂN HÌNH

2.1 Mô hình hệ thống mạng doanh nghiệp

Dưới đây là mô hình thiết kế một mạng máy tính điển hình trong doanh nghiệp do Cisco đề xuất. Mô hình thiết kế này được sử dụng rộng rãi trong hệ thống mạng của các doanh nghiệp. Như đã nói ở mục 3.1, phạm vi khảo sát hệ thống mạng là tại trụ sở chính của doanh nghiệp đó. Tức là không bao gồm hệ thống mạng diện rộng (WAN).



Hình 2.1. Thiết kế mạng phân thành 3 tầng

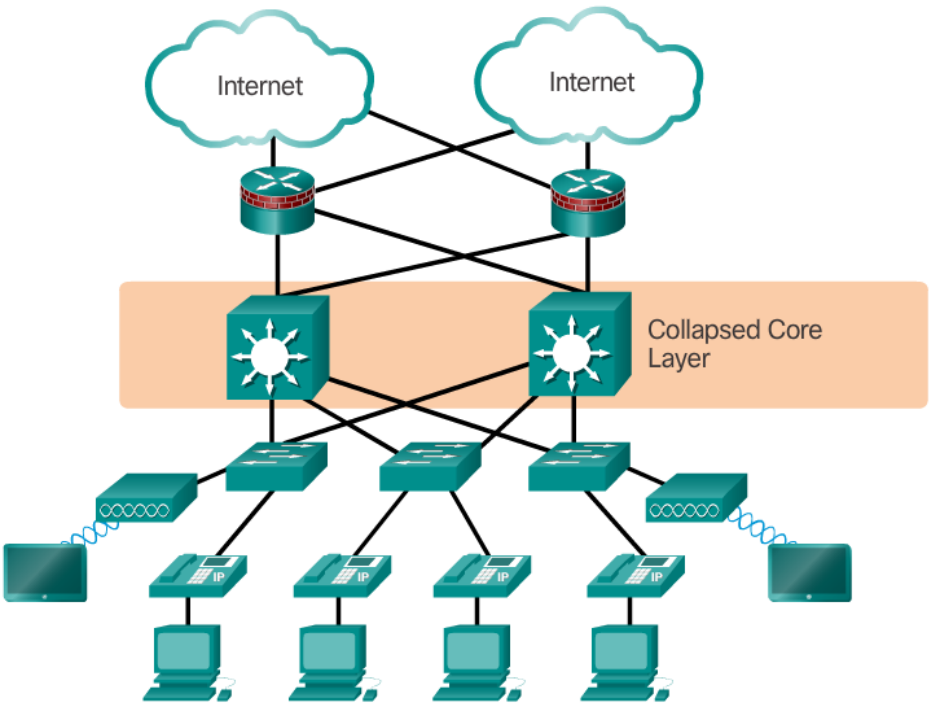
Cấu trúc mạng thường được thiết kế theo mô hình 3 tầng như trên hình. Thiết kế này nếu tuân thủ sẽ đảm bảo cho hệ thống mạng có tính sẵn sàng, linh hoạt, an ninh, tính quản lý. Được phân thành các tầng:

- *Tầng truy nhập (Access layer)*: để kết nối các thiết bị đầu cuối của người dùng vào mạng. Thông thường tầng Access bao gồm các thiết bị chuyển mạch (switch lớp 2), thiết bị định tuyến không dây (wireless router). Các thiết bị chuyển mạch, thiết bị định tuyến không dây ở tầng này hiện nay có những tính năng an ninh để chống lại sự tấn công của hacker .
- *Tầng phân phối (Distribution layer):* thực hiện gom lưu lượng từ tầng truy nhập và gửi tới tầng lõi để tầng lõi thực hiện định tuyến tới đích. Tầng phân phối có nhiều chức năng bao gồm định tuyến, chuyển mạch, thực hiện các chính sách truy nhập mạng, phân loại dịch vụ, đảm bảo tính dự phòng về mặt thiết bị và kết nối.

Các thiết bị ở tầng này thường là bộ định tuyến (router) hoặc thiết bị chuyển mạch lớp 3. Các thiết bị này có những tính năng an ninh để đảm bảo xác thực thông tin định tuyến được gửi giữa các thiết bị

- *Tầng lõi:* thực hiện gom lưu lượng từ tất cả các thiết bị ở tầng phân phối và chuyển tiếp lưu lượng này tới các trung tâm dữ liệu, trung tâm dịch vụ, hoặc ra mạng diện rộng. Thiết bị hoạt động ở tầng này là thiết bị chuyển mạch lớp 3 với khả năng chuyển mạch tốc độ cao.

Cũng theo Cisco, bên cạnh mô hình thiết kế 3 tầng, mạng doanh nghiệp còn có thể thiết kế kiểu 2 tầng như hình dưới.



Hình 2.2. Mô hình thiết kế mạng 2 tầng

Ở mô hình 2 tầng, tầng phân phối và tầng lõi được gộp lại thành một tầng gọi là tầng lõi rút gọn (collapsed core). Lợi ích chính của kiểu thiết kế này là tiết kiệm chi phí mua thiết bị. Với những doanh nghiệp vừa và nhỏ, nơi không có sự tăng trưởng đột biến về quy mô, thì thiết kế này hoàn toàn đáp ứng được nhu cầu sử dụng, nhưng vẫn thỏa mãn các tính chất của một hệ thống mạng là tính sẵn sàng, khả năng mở rộng và tối đa hiệu năng hoạt động. Thiết bị ở tầng lõi thường là thiết bị chuyển mạch lớp 3.

2.2 Những lỗi quản trị viên gặp phải khi cấu hình hệ thống mạng

2.2.1 Các lỗi liên quan đến cấu hình quản lý thiết bị

- Sử dụng giao thức TELNET để truy cập thiết bị từ xa: TELNET (viết tắt của TErminaL NETwork) là một giao thức mạng (network protocol) được dùng để truy cập từ xa đến một thiết bị mạng (switch, router, server...) để quản trị. TELNET là một giao thức giữa client-server, dựa trên một kết nối tin cậy. Giao thức này hoạt động ở tầng 7 và sử dụng giao thức TCP cổng 23. Tuy nhiên TELNET không an toàn vì theo mặc định, không mã hóa thông tin khi gửi trên đường truyền, và vì vậy có khả năng bị nghe trộm. TELNET là giao thức rất dễ bị tấn công bằng các kỹ thuật: Đánh hơi phiên TELNET (Telnet communication sniffing), tấn công vét cạn (Telnet brute force attack), tấn công từ chối dịch vụ (Telnet DoS – Denial of Service).

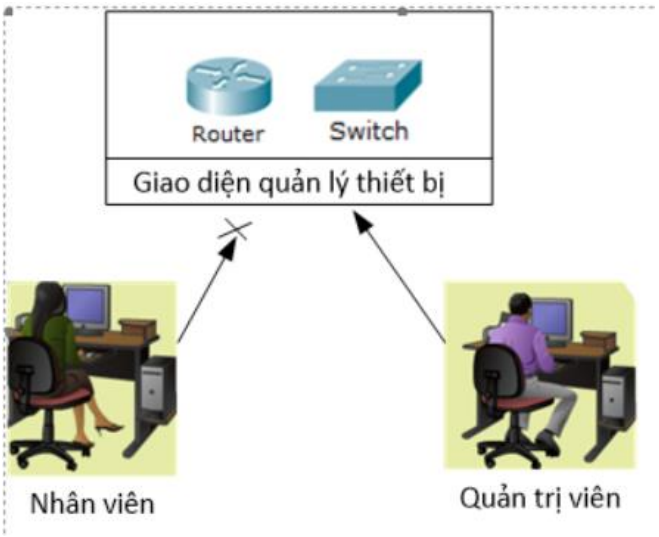
Chính vì lý do trên mà các tài liệu đều khuyến nghị sử dụng giao thức SSH (SecureShell) để truy cập tới thiết bị từ xa, thay thế cho TELNET (cần tắt giao thức TELNET trên thiết bị). SSH là giao thức thực hiện mã hóa thông tin trao đổi giữa máy tính của người quản trị và thiết bị. Do vậy khi sử dụng SSH sẽ đảm bảo tính bí mật cho thông tin được gửi đi. Ngoài ra SSH còn hỗ trợ cơ chế xác thực thông tin.

- Sử dụng giao thức HTTP để truy cập giao diện quản lý thiết bị: khi sử dụng HTTP, các thông tin trao đổi giữa máy tính của người quản trị và thiết bị sẽ ở dạng bản rõ. Kẻ tấn công có thể chặn bắt và xem được các thông tin này. Vì vậy, theo khuyến nghị, cần sử dụng giao thức HTTPS để truy cập vào thiết bị để quản lý thay cho giao thức HTTP (tắt giao thức HTTP trên thiết bị). Giao thức HTTPS sử dụng giao thức TLS/SSL(Transport Layer Security/Secure Socket Layer) để xác thực website, bảo đảm tính bí mật và tính toàn vẹn cho thông tin.

- Sử dụng giao thức truyền file TFTP: để copy các file cấu hình từ thiết bị đến máy chủ lưu trữ và ngược lại. Giao thức TFTP dựa trên giao thức UDP, ưu điểm là nhanh nhưng không có cơ chế báo nhận tin cậy, dẫn đến có thể xảy ra bị lỗi file cấu hình khi truyền. Khuyến nghị dùng giao thức FTP (sử dụng TCP) hoặc các giao thức an toàn như SSH-FTP để copy file cấu hình từ thiết bị đến máy chủ lưu trữ hoặc ngược lại.

- Không ngăn người dùng truy cập đến giao diện quản lý: Giao diện quản lý của thiết bị là một địa chỉ IP mà khi quản trị viên truy cập tới, sẽ cung cấp giao diện để quản lý thiết bị trên. Theo khuyến nghị thì chỉ có máy tính của quản trị viên mới được phép truy cập tới địa chỉ quản lý này. Bởi vì nếu bất kỳ một nhân viên nào đó có thể ngồi từ máy

tính của mình và truy xuất đến giao diện quản lý của thiết bị, thì có thể xảy ra những tình huống tấn công vào giao diện quản lý, ví dụ như tấn công DoS. Để thực hiện việc ngăn chặn này, cần sử dụng kỹ thuật điều khiển truy cập, chỉ cho phép các máy tính của quản trị viên có thể truy xuất tới giao diện quản lý của thiết bị mà thôi.

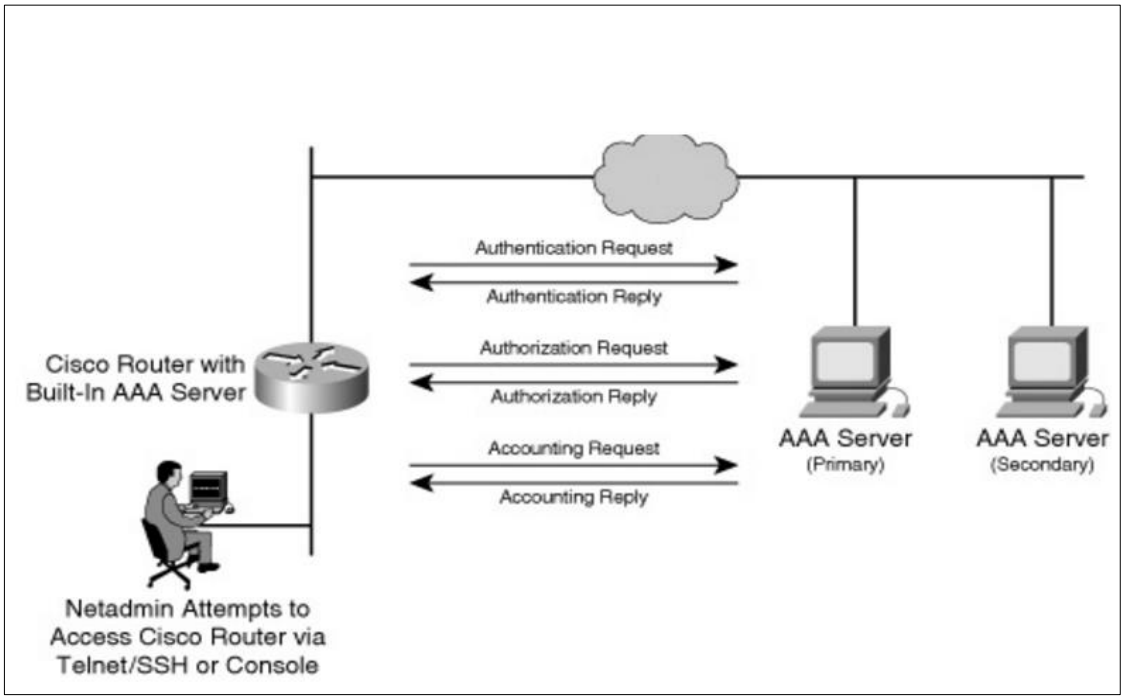


Hình 2.3. Cấu hình chỉ cho phép quản trị viên truy cập quản lý thiết bị

- Sử dụng giao thức quản trị mạng đơn giản SNMPv1 hoặc SNMPv2c: giao thức SNMP được sử dụng để quản lý các thiết bị mạng, cho phép người quản trị có thể xem thông tin trạng thái hoặc cấu hình trên thiết bị. Tuy nhiên nếu sử dụng SNMPv1 hoặc SNMPv2c, cả hai giao thức này đều không xác thực nguồn gốc thông tin được gửi từ máy quản lý đến. Bên cạnh đó, 2 giao thức trên cũng không hỗ trợ việc mã hóa thông tin. Do vậy hệ quả là các thông tin được truyền giữa máy của người quản lý và thiết bị có thể bị giả mạo bị xem trộm. Vì lý do đó theo khuyến nghị cần sử dụng giao thức SNMPv3. Giao thức SNMPv3 hỗ trợ mã hóa thông tin, xác thực nguồn gốc thông tin và đảm bảo tính toàn vẹn.

- Cài đặt mật khẩu xác thực cục bộ trên thiết bị: khi cài mật khẩu xác thực ngay trên thiết bị, thiết bị sẽ phải làm thêm công việc xác thực. Hơn nữa nếu trong mạng có nhiều thiết bị, sẽ khó quản lý tập trung. Khi xảy ra sự cố an ninh, sẽ rất khó khăn cho quản trị viên khi điều tra vì các thông tin nhật ký truy cập phân tán trên các thiết bị khác nhau. Vì vậy theo khuyến nghị cần thực hiện xác thực tập trung trên máy chủ AAA (Authenticatio - Authorization- Accounting). Máy chủ AAA sử dụng giao thức TACACS+ (Terminal Access Controller Access-Control System+) cung cấp chức năng xác thực tập trung cho các truy cập quản lý vào thiết bị. Tài khoản truy cập được lưu

trên máy chủ AAA. Khi truy cập vào thiết bị, người quản trị nhập username và password. Thiết bị sẽ gửi thông tin này tới máy chủ AAA để yêu cầu xem xét. Nếu tài khoản trên tồn tại trên AAA thì AAA sẽ gửi thông tin phản hồi tới thiết bị để cho phép đăng nhập. Khi xác thực tập trung trên máy chủ AAA, bản thân thiết bị không phải thực hiện chức năng xác thực nữa. Bên cạnh đó, nhật ký truy nhập thiết bị được lưu trữ tập trung trên máy chủ AAA, hỗ trợ cho việc điều tra các sự cố an ninh.



Hình 2.4. Quá trình xác thực, cấp quyền và ghi nhật ký trên máy chủ AAA

- Không mã hóa các mật khẩu lưu trên thiết bị: trên thiết bị mạng của hãng Cisco, một số dạng mật khẩu sau khi được cấu hình trên thiết bị mạng, sẽ lưu ở ở dạng bản rõ. Nếu người quản trị không thực hiện công việc mã hóa mật khẩu dạng bản rõ, kẻ tấn công có thể xem được mật khẩu nếu file cấu hình bị đánh cắp và xem.

Cấu hình chưa mã hóa mật khẩu	**Cấu hình sau khi đã mã hóa mật khẩu**
line con 0 *!* *line aux 0* *!* *line vty 0 4* *password abcxyz123* *login* *line vty 5 15* *password abcxyz123* *login* *!*	*line con 0* *!* *line aux 0* *!* *line vty 0 4* *password 7 08204E4D11001F464058* *login* *line vty 5 15* *password 7 08204E4D11001F464058* *login* *!*

!	*!*

- Không cấu hình đồng bộ về thời gian: trong một hệ thống mạng cần phải có máy chủ thời gian (NTP - Network Time Protocol Server). Các thiết bị mạng cần lấy đồng bộ thời gian theo máy chủ này. Như vậy các thiết bị trong mạng sẽ được đồng bộ về mặt thời gian. Khi cần truy vết những sự kiện an ninh, các mốc thời gian sẽ chính xác. Nếu không có NTP Server, đồng hồ cục bộ trên các thiết bị có thể bị sai lệch thời gian, dẫn đến sai lệch dấu thời gian trong các bản tin gửi ra từ thiết bị, gây khó khăn khi điều tra về an ninh.

- Không lưu nhật ký hoạt động (log): trong khi hoạt động, mỗi thiết bị đều gửi ra các cảnh báo hệ thống (syslog). Theo khuyến nghị cần cấu hình để thiết bị gửi các cảnh báo đến một máy chủ lưu syslog tập trung để phục vụ cho việc giám sát hệ thống mạng. Nếu không thực hiện công việc này thì sẽ không biết được trạng thái hệ thống đang hoạt động tại thời điểm hiện tại như thế nào.

Bảng dưới đây tóm tắt những lỗi gặp phải khi cấu hình quản lý thiết bị và cấu hình khuyến nghị.

STT	**Mã số lỗi**	**Mô tả về lỗi**	**Khuyến nghị**
1	mnt-TELNET	Sử dụng giao thức TELNET để truy cập thiết bị từ xa	Sử dụng giao thức SSH (SecureShell) để truy cập tới thiết bị từ xa
2	mnt-HTTP	Sử dụng giao thức HTTP để truy cập giao diện quản lý thiết bị	Sử dụng giao thức HTTPS để truy cập vào thiết bị để quản lý
3	mnt-TFTP	Sử dụng giao thức truyền file TFTP	Sử dụng các giao thức truyền file thay thế như FTP (hạn chế) hoặc SSH-FTP
4	mnt-int-ACL-BLK	Không ngăn chặn các máy tính khác truy cập	Sử dụng kỹ thuật điều khiển truy cập, chỉ cho phép các

		tới giao diện quản lý thiết bị	máy tính của người quản trị có thể truy xuất tới giao diện quản lý của thiết bị
5	mnt-SNMP	Sử dụng giao thức quản trị mạng đơn giản SNMPv1 hoặc SNMPv2c	Sử dụng giao thức SNMPv3
6	mnt-PasswordLocal	Cài đặt mật khẩu xác thực cục bộ trên thiết bị	Thực hiện xác thực tập trung trên máy chủ AAA
7	mnt-PasswordENCRYPT	Không mã hóa các mật khẩu lưu trên thiết bị	Mã hóa mật khẩu
8	mnt-NTP	Không cấu hình đồng bộ về thời gian	Cần lấy đồng bộ thời gian theo máy chủ NTP
9	mnt-SYSLOG	Không lưu nhật ký hoạt động (log)	Cấu hình để thiết bị gửi các cảnh báo đến một máy chủ lưu syslog tập trung

Bảng 2.1. Những lỗi cấu hình an ninh trong quản lý

Bảng dưới đây mô tả một mẫu cấu hình an ninh khuyến nghị cho việc quản lý thiết bị.

STT	**Mã số**	**Tên lỗi**	**Cấu hình trên thiết bị**	**Cấu hình khuyến nghị**
1	mnt-TELNET	Sử dụng giao thức TELNET để quản lý thiết bị	`line vty 0 15 password [string] login`	`line vty 0 15 transport input ssh`

2	mnt-HTTP	Sử dụng giao thức HTTP để quản lý thiết bị	ip http server	no ip http server ip http secure-server
3	Mnt-TFTP	Sử dụng giao thức truyền file TFTP	N/A	ip ftp user ip ftp password
4	mnt-int-ACL-BLK	Không chặn máy người dùng truy cập đến giao diện quản lý	N/A	Cần có ACL để chặn. Tên của ACL cần được thông báo cho người kiểm tra an ninh
5	mnt-SNMP	Dùng SNMPv1 hoặc SNMPv2c	Snmp-server host x.x.x.x version 2c	snmp-server group group1 v3 auth access lmnop
6	mnt-Password Local	Cài đặt mật khẩu xác thực cục bộ trên thiết bị	Login local	AAA new-model AAA authentication AAA authorize AAA accounting
7	mnt-Password ENCRYPT	Không mã hóa mật khẩu	N/A	Service-password encryption

8	mnt-NTP	Không lấy đồng bộ thời gian từ máy chủ NTP	N/A	Ntp server [IP]
9	mnt-SYSLOG	Không lưu trữ tập trung syslog	N/A	Logging [IP]

Bảng 2.2. Cấu hình quản lý có lỗi và cấu hình khuyến nghị

2.2.2 Các lỗi cấu hình trên thiết bị tầng truy nhập

Như đã đề cập, vai trò của tầng truy nhập trong mô hình thiết kế 3 tầng là để kết nối các thiết bị đầu cuối của người dùng vào mạng. Thông thường các thiết bị tầng truy nhập là các thiết bị chuyển mạch (switch lớp 2), thiết bị định tuyến không dây (wireless router).

Lỗi cấu hình trên thiết bị switch lớp 2

Theo một thống kê cho thấy, phần lớn các thiết bị switch lớp 2 trong nội mạng bộ doanh nghiệp luôn luôn có các cổng mạng được mở vì thế bất kì laptop của bất kì nhân viên trong doanh nghiệp có thể truy cập hệ thống mạng. Bởi vì máy laptop của nhân viên trước đó có thể đã bị nhiễm mã độc và khi truy xuất vào mạng một cách tự do, mã độc sẽ có thể lây lan ra toàn bộ hệ thống.

Đối với thiết bị định tuyến không dây, lợi ích là đem đến sự tiện lợi cho việc kết nối các thiết bị di động của người sử dụng, nhưng mặt trái là những thiết bị này dễ bị "nhòm ngó" bởi những kẻ tấn công có chủ đích muốn xâm nhập vào hệ thống mạng qua kết nối không dây. Kẻ tấn công có thể ngồi ở gần mạng của doanh nghiệp và sử dụng những công cụ dò quét để lấy được thông tin về mạng không dây. Sau đó sử dụng các kỹ thuật tấn công như tấn công mật khẩu theo hình thức vét cạn; hoặc giả mạo điểm truy cập không dây có tên giống như tên mạng không dây của doanh nghiệp, sau đó lừa người dùng truy cập để lấy mật khẩu...

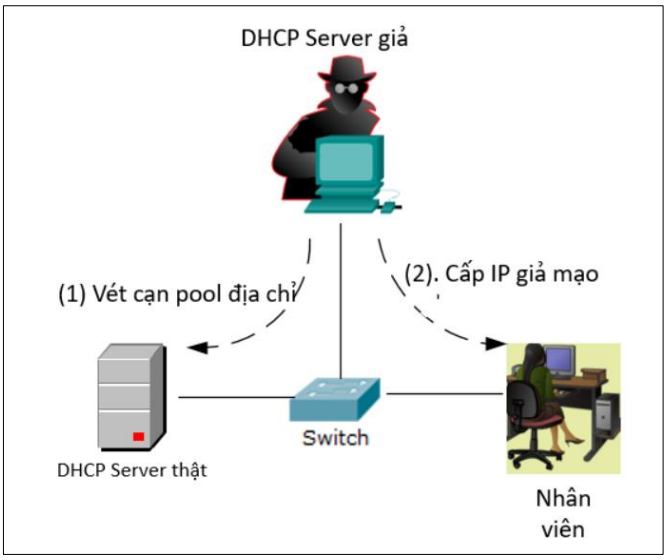
Thống kê cũng cho thấy sự gia tăng đáng kể từ các cuộc tấn công bên ngoài nhưng không làm giảm đi khả năng các vụ tấn công từ bên trong thậm chí các cuộc tấn công nội bộ còn mang tổn thất hiểm họa nghiêm trọng hơn rất nhiều so với từ bên ngoài. Hơn thế nữa nhiều quản trị viên dường như không quan tâm đến vấn đề an ninh từ bên trong vì họ nghĩ rằng bên trong họ "an toàn".

Các thiết bị tầng truy nhập được thiết kế theo xu hướng "khuyến khích truyền thông". Khi thực hiện chức năng truyền thông lớp 2 là cố gắng mở các kết nối, điều này có thể tạo ra các lỗ hổng bảo mật để cho những hacker xâm nhập hệ thống dễ dàng. Vì thế luôn có những tính năng bảo mật bên trong các thiết bị. *Quản trị viên khi cấu hình phải bật các tính năng này lên. Nhưng thông thường thì các tính năng này không được sử dụng, hoặc được sử dụng không đúng cách.*

Dưới đây liệt kê những dạng tấn công có thể xảy ra nếu quản trị viên không thực hiện bật cấu hình các tính năng an ninh trên ***thiết bị switch lớp 2:***

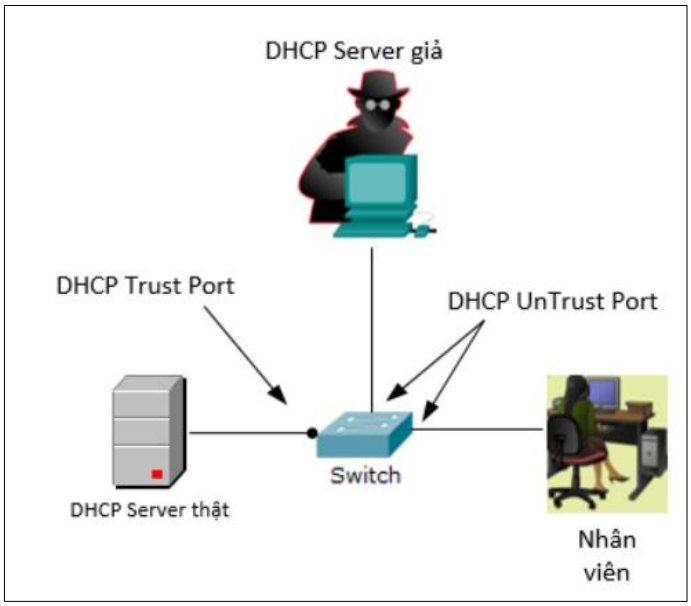
- Truy cập bất hợp pháp vào mạng vì quản trị viên không tắt các cổng switch mà đang không sử dụng: nếu không tắt các cổng trên switch đang không sử dụng, bất kỳ người nào cũng có thể cắm dây mạng vào những cổng đó và truy cập vào mạng. Điều này rất dễ xảy ra với những thiết bị switch được lắp đặt ở những nơi không an toàn. Nếu người đó có mục đích phát tán mã độc thông qua cổng đó hoặc chặn bắt thông tin gửi và nhận giữa các máy khác trên swich, thì sẽ rất khó để ngăn chặn. Vì vậy, theo khuyến nghị cần tắt những cổng đang không sử dụng trên swich.

- Giả mạo máy chủ DHCP: trong kiểu tấn công này, máy tính của hacker có thể giả mạo thành máy chủ DHCP. Đầu tiên máy của hacker sẽ gửi hàng loạt yêu cầu cấp phát địa chỉ IP tới máy chủ DHCP thật nhằm vét cạn toàn bộ pool địa chỉ IP. Sau khi máy chủ thật đã cạn kiệt IP, nó không thể cấp thêm IP mới khi máy client yêu cầu. Bước tiếp theo, hacker cài đặt dịch vụ DHCP Server trên máy của hắn và cấp phát thông tin về địa chỉ IP giả mạo cho các máy client có yêu cầu trong mạng LAN. Bằng cách này hacker có thể điều hướng truy cập các máy tính này theo ý đồ của hacker.



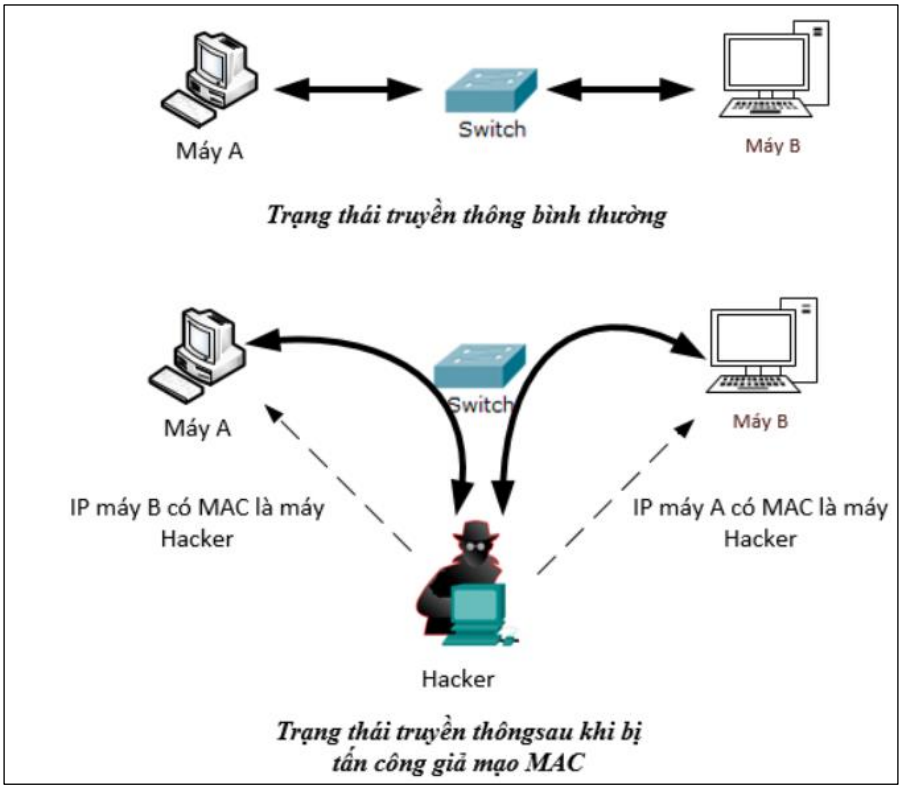
Hình 2.5. Tấn công giả mạo máy chủ DHCP

Để ngăn chặn hình thức tấn công này, theo khuyến nghị cần cài đặt chế độ giám sát các bản tin DHCP trên swich (DHCP Snooping). Với chế độ này, quản trị viên sẽ cấu hình cổng switch đấu nối với máy chủ thật là DHCP Trust Port (port cho phép gửi bản tin cấp phát địa chỉ IP là DHCP Offer đi qua), còn các cổng khác cấu hình là DHCP Untrust Port (Không cho phép gửi bản tin DHCP Offer đi qua). Với nguyên lý này, thiết bị máy tính của kẻ tấn công không thể cấp phát địa chỉ IP cho các máy tính khác trong mạng LAN.



Hình 2.6. Cấu hình DHCP Snooping

- Tấn công giả mạo địa chỉ MAC: trong kiểu tấn công này, hacker sẽ giả mạo địa chỉ MAC của các máy trong mạng LAN khiến cho các máy tính gửi gói tin tới máy của hacker. Sở dĩ hacker có thể thực hiện được việc trên là do điểm yếu của giao thức phân giải địa chỉ IP thành địa chỉ MAC – Address Resolution Protocol (ARP). Giao thức ARP cung cấp cơ chế ánh xạ IP thành MAC và ngược lại, giúp cho các máy tính cũng như các thiết bị liên lạc được với nhau trong môi trường hoạt động mạng. Tuy nhiên ARP không có cơ chế giúp xác thực quá trình phân giải này, tức là nếu các bản tin ARP bị giả mạo thì máy nhận cũng không thể phát hiện được. Do đó hacker có thể tạo ra các bản tin ARP giả mạo địa chỉ MAC, để đánh lừa các máy tính khác. Khi đó các máy tính trên mạng LAN sẽ gửi thông tin tới máy của hacker.



Hình 2.7. Kẻ tấn công giả mạo địa chỉ MAC của máy A và máy B

Theo khuyến nghị, cần bật tính năng DHCP Snooping, tính năng giám sát ARP trên switch. Với sự kết hợp của 2 tính năng này, các gói tin ARP sẽ được giám sát để đảm bảo rằng chúng không thể bị giả mạo.

- Tấn công làm tràn bảng MAC: trong kiểu tấn công này, hacker tạo ra rất nhiều gói tin có địa chỉ MAC nguồn và MAC đích giả mạo, sau đó gửi tới switch, làm cho switch bị tràn bảng địa chỉ MAC. Khi bị tràn bảng địa chỉ MAC, switch sẽ hoạt động theo phương thức quảng bá tất cả các gói tin mà nó nhận được. Do vậy thông tin trao đổi giữa hai máy bất kỳ trong mạng LAN có thể bị xem trộm bởi máy của hacker. Theo khuyến nghị cần bật tính năng an ninh cổng trên switch (Port security). Với tính năng này, kẻ tấn công sẽ không thể làm tràn bảng MAC của switch.

- Giả mạo địa chỉ IP: trong kiểu tấn công này, hacker có thể giả mạo địa chỉ IP nguồn để truy xuất vào những tài nguyên mà nếu sử dụng địa chỉ IP được cấp phát thì sẽ không thể truy xuất được; hoặc giả mạo IP nguồn để tấn công từ chối dịch vụ (DoS) theo kiểu gây mưa bão (smurf attack). Để chống lại hình thức tấn công này, cần bật tính năng bảo vệ IP nguồn trên cổng của swich.

- Tấn công IPv6 trên hạ tầng mạng truy nhập: các thiết bị định tuyến chạy giao thức IPv6 thường gửi các bản tin IPv6 RA (Router Advertisement) cho các thiết bị đầu cuối

ở chế độ cấu hình địa chỉ IPv6 auto-config. Nếu kẻ tấn công giả mạo bản tin RA và gửi cho các máy tính khác, hắn có thể gây ra vụ tấn công từ chối dịch vụ hoặc giả danh làm kẻ đứng giữa để chặn bắt thông tin. Ngoài ra kẻ tấn công còn có thể giả mạo máy chủ DHCPv6 để gửi địa chỉ IPv6 giả mạo. Theo khuyến nghị cần bật tính năng bảo vệ địa chỉ IPV6 trên tầng truy nhập.

- Tấn công từ chối dịch vụ: Trong mạng chuyển mạch lớp 2, để bảo đảm cho các thiết bị swich khi đấu nối dạng topo mạch vòng sẽ không bị loop, cần cài đặt giao thức spanning-tree. Các cổng đấu nối với thiết bị đầu cuối người sử dụng thường được cấu hình là cổng PortFast. Để đảm bảo rằng các cổng PortFast không gây ra loop khi cắm nhầm một thiết bị swich khác vào cổng này, cần bật tính năng BPDU Guard. Nếu không bật tính năng này, hệ thống mạng chuyển mạch có thể bị loop và gây ra từ chối dịch vụ. Bảng dưới đây tóm tắt lại những lỗi cấu hình an ninh trên thiết bị switch và cấu hình khuyến nghị.

STT	Mã lỗi	Mô tả lỗi	Khuyến nghị
1	acc-shutdown	Không tắt các cổng switch mà đang không sử dụng	Tắt các cổng không sử dụng
2	acc-dhcpsnooping	Không bật chế độ ngăn chặn các bản tin DHCP giả mạo	Bật DHCP Snooping
3	acc-DAI	Không bật chế độ giám sát các gói tin ARP	Bật tính năng giám sát gói tin ARP - Dynamic ARP Inspection
4	acc-portsecurity	Không bật chế độ an ninh cổng	Bật chế độ an ninh cổng
	acc-IPSouceGuard	Không bật chế độ chống giả mạo IP nguồn	Bật chế độ bảo vệ IP nguồn - IP Source Guard
5	acc-IPv6	Không bật chế độ ngăn chặn các bản tin IPv6 RA giả mạo	Bật chế độ ngăn chặn IPv6 RA giả mạo - IPV6 First Hop Security
6	acc-BPDUGuard	Không bật tính năng BPDU Guard trên các cổng Port Fast	Bật BPDU guard trên các cổng Port Fast

Bảng 2.3. Lỗi cấu hình an ninh trên swich và khuyến nghị

STT	Mã lỗi	Cấu hình trên thiết bị	Câú hình khuyến nghị
1	acc-shutdown	N/A	Interface x shutdown
2	acc-dhcpsnooping	N/A	Ip dhcp snooping
3	acc-DAI	N/A	ip arp inspection vlan
4	acc-portsecurity	N/A	Switchport port-security
	acc-IPSouceGuard	N/A	ip verify source vlan dhcp-snooping
5	acc-IPv6	N/A	ipv6 snooping policy policy1
6	acc-BPDUGuard	N/A	Bpudguard enable

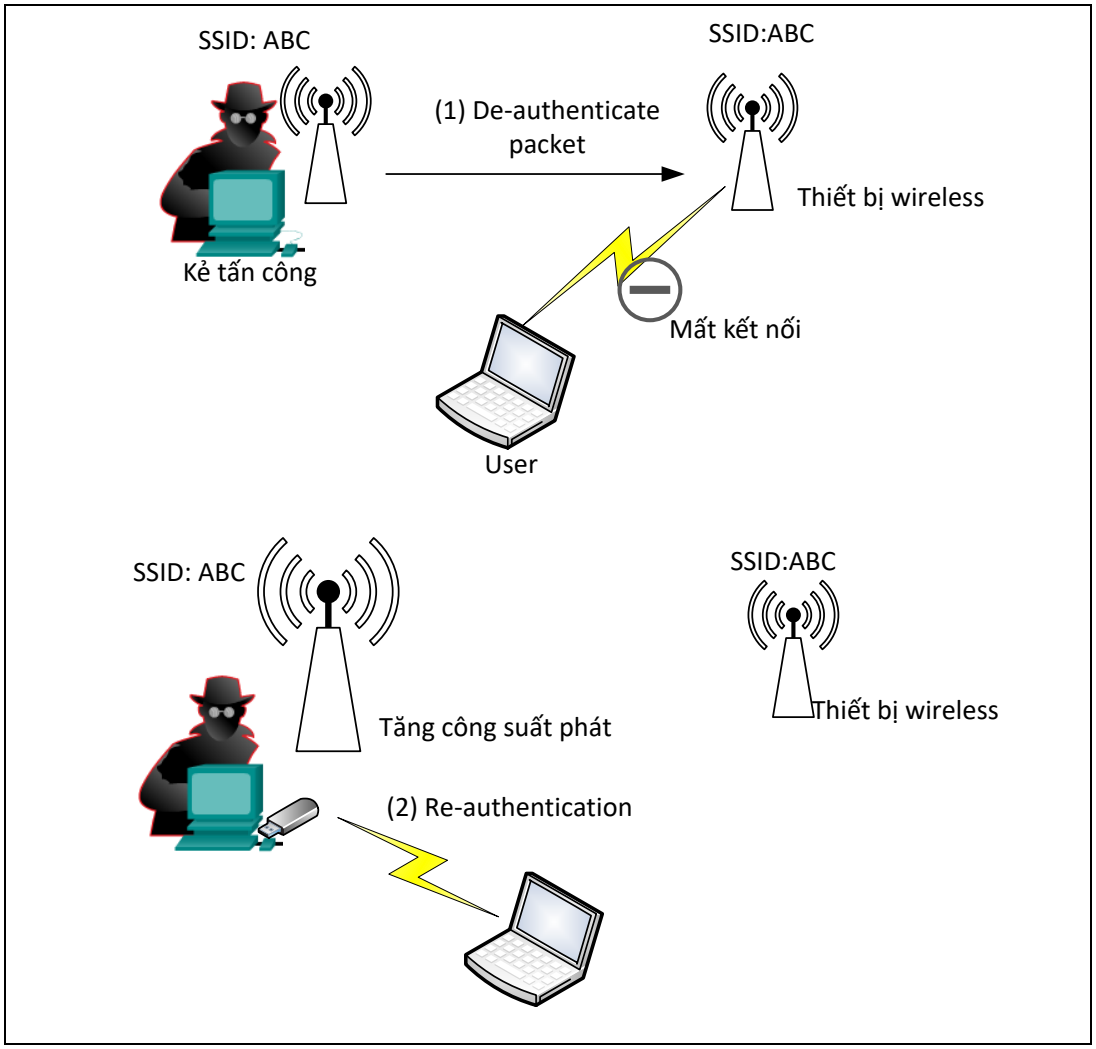
Bảng 2.4. Mẫu cấu hình an ninh khuyến nghị trên switch

3.6.2.2 Lỗi cấu hình trên thiết bị định tuyến không dây

Dưới đây liệt kê những dạng tấn công có thể xảy ra nếu quản trị viên không thực hiện bật cấu hình các tính năng an ninh trên ***thiết bị định tuyến không dây:***

- Không ẩn tên mạng không dây: để tấn công một mạng không dây thì bước đầu tiên là phát hiện ra tên của mạng không dây đó. Nếu quản trị viên ẩn tên mạng (SSID) thì kẻ tấn công có thể không phát hiện ra. Nếu không ẩn tên, bất kỳ người nào với thiết bị không dây cũng có thể phát hiện ra sự tồn tại của mạng. Đây cũng là nấc thang để kẻ tấn công thực hiện kiểu tấn công kẻ sinh đôi ma quỷ (Evil twins). Đầu tiên kẻ tấn công giả mạo tên mạng không dây. Sau đó gây nhiễu mạng không dây của doanh nghiệp khiến cho các máy tính không thể truy nhập vào mạng thật, và người dùng có xu hướng kết nối với mạng không dây giả mạo của kẻ tấn công tạo ra. Sau khi đã kết nối, kẻ tấn công có thể lấy được các thông tin tài khoản truy cập mạng không dây thật, hoặc điều hướng

truy cập người dùng đến một trang web giả mạo để đánh cắp thông tin (Facebook, Gmail, ngân hàng...)



Hình 2.8 Cách thức tấn công kiểu kẻ sinh đôi ma quỷ

- Đặt mật khẩu truy cập mạng không dây đơn giản: khi đặt mật khẩu truy cập vào mạng không dây, cần đặt mật khẩu mạnh. Nếu mật khẩu được đặt đơn giản (ví dụ: có trong từ điển, dễ đoán,...) thì kẻ tấn công sẽ sử dụng kỹ thuật tấn công từ điển để dò tìm mật khẩu.

- Không cấu hình lọc địa chỉ MAC: vì mật khẩu truy cập mạng không dây thường ở dạng pre-share (chia sẻ với những người muốn truy cập) nên bản thân nó không còn an toàn nữa. Để tăng thêm một lớp bảo mật, cần lọc địa chỉ MAC bằng cách chỉ cho phép những địa chỉ MAC tin cậy mới được phép truy cập vào mạng không dây, sau khi đã nhập đúng mật khẩu.

- Không đổi tài khoản quản trị mặc định: thông thường các thiết bị định tuyến không dây đều có một tài khoản quản trị mặc định để quản trị viên có thể sử dụng để truy cập

vào cấu hình thiết bị. Tuy nhiên sau khi cấu hình xong, cần đổi tài khoản quản trị mặc định. Nếu không đổi thì kẻ tấn công có thể dò quét để lấy được thông tin này, sau đó truy cập vào thiết bị và thay đổi những tham số trên thiết bị, ví dụ DNS. Khi đó kẻ tấn công có thể điều hướng truy cập các máy nạn nhân qua máy tính của hắn, hoặc đến những máy chủ web giả mạo. Điều này gây hậu quả lộ lọt thông tin, mất mát thông tin.

Mã lỗi	**Mô tả**	**Khuyến nghị**
wl-SSID	Không ẩn tên mạng không dây	Ẩn tên mạng không dây
wl-SimplePass	Đặt mật khẩu truy cập mạng không dây đơn giản	Đặt mật khẩu mạnh
wl-MAC	Không cấu hình lọc địa chỉ MAC:	Cấu hình lọc địa chỉ MAC
wl-Default	Không đổi tài khoản quản trị mặc định:	Đổi tài khoản quản trị mặc định

Bảng 2.5. Tóm tắt các lỗi cấu hình trên thiết bị định tuyến không dây.

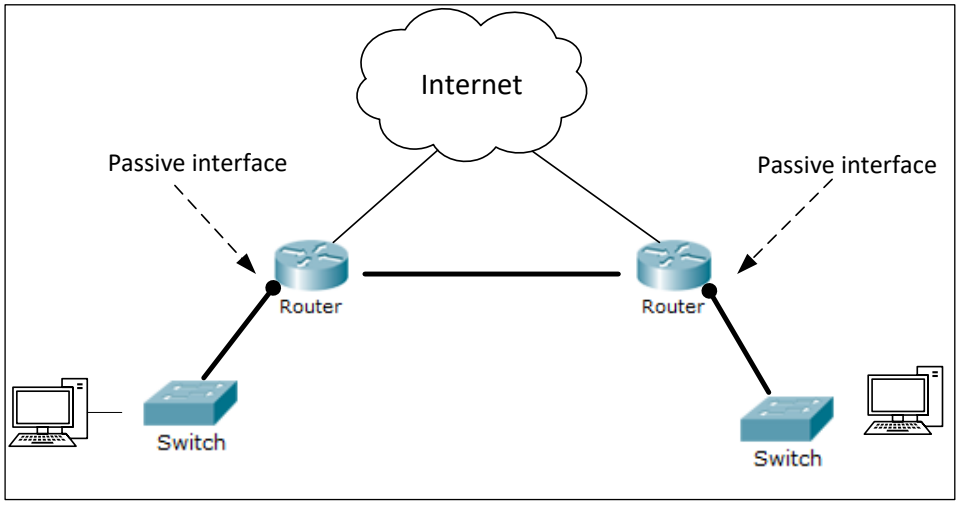
2.2.3 Các lỗi cấu hình trên thiết bị tầng phân phối và tầng lõi

Vì các thiết bị ở tầng phân phối và tầng lõi đều thực hiện chức năng định tuyến nên thông thường được cài đặt các giao thức định tuyến động. Khi giao thức định tuyến động được cấu hình chạy trên thiết bị, các thiết bị sẽ thiết lập mối quan hệ láng giềng và trên cơ sở đó trao đổi thông tin định tuyến để từ đó tính toán tìm ra con đường tối ưu đi đến đích.

Kẻ tấn công thường ngắm tới việc phá hoại quá trình định tuyến này bằng cách cố gắng tạo ra những mối quan hệ láng giềng giả mạo. Sau đó gửi những thông tin định tuyến sai lệch tới các thiết bị đang hoạt động. Điều này phá vỡ hạ tầng định tuyến được xây dựng từ trước, gây ra cuộc tấn công từ chối dịch vụ. Hơn nữa những thông tin định tuyến giả mạo có thể dẫn đến việc điều hướng lưu lượng truy cập mạng đến những máy chủ giả mạo để đánh cắp tài khoản người dùng. Ví dụ các website giả mạo ngân hàng, cửa hàng trực tuyến...

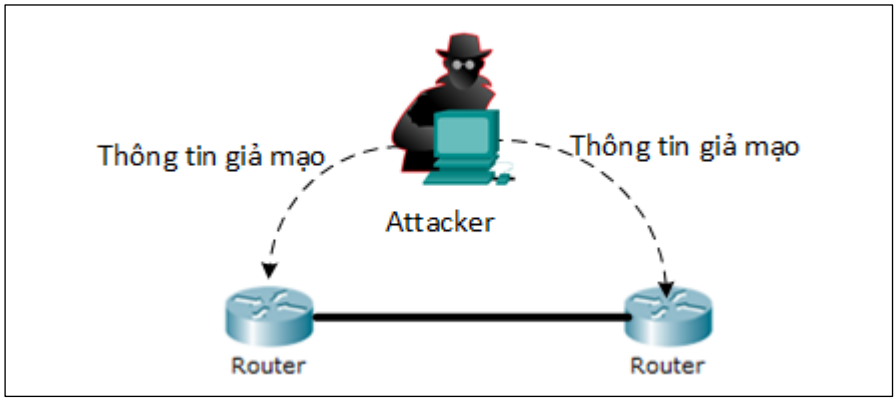
Nếu người quản trị không thực hiện những bước cấu hình an ninh sau thì việc tấn công vào hạ tầng định tuyến có thể xảy ra:

- Không đặt các cổng kết nối với tầng truy nhập ở chế độ passive-interface: vì các thiết bị ở tầng truy nhập không chạy giao thức định tuyến nên cần đặt các cổng thiết bị ở tầng phân phối/core kết nối với tầng truy nhập ở chế độ passive-interface. Trong chế độ này, thông tin định tuyến không được gửi qua các cổng nói trên. Nếu không thực hiện việc này, kẻ tấn công sử dụng máy tính có chạy phần mềm giả lập giao thức định tuyến động, có thể lấy được thông tin định tuyến được gửi ra từ các cổng này.



Hình 2.9. Cần đặt các cổng Router nối với tầng Access là Passive interface

- Không thực hiện cấu hình xác thực nguồn gốc thông tin định tuyến: các router chạy giao thức định tuyến động phải gửi các thông tin định tuyến cho nhau. Kẻ tấn công có thể tạo ra các bản tin định tuyến (routing information message) giả mạo và gửi tới các Router. Vì các thông tin định tuyến này là giả mạo, cho nên nếu Router tin tưởng và lưu vào bảng định tuyến để sử dụng, hệ thống mạng có thể gặp sự cố. Sự cố thường gặp là hệ thống mạng bị loop (làm cho các gói tin chạy lòng vòng không đi đến đích), hoặc điều hướng lưu lượng theo ý đồ của kẻ tấn công. Để phòng tránh, theo khuyến nghị cần xác thực thông tin định tuyến là được gửi từ nguồn tin cậy. Khi đó nếu hacker không thể chứng minh được thông tin hắn gửi là tin cậy thì các Router sẽ không chấp nhận các thông tin đó. Kỹ thuật thường được sử dụng để xác thực thông tin định tuyến là MD5. Nếu quản trị viên không cấu hình xác thực nguồn gốc thông tin định tuyến trên các thiết bị thì có thể sẽ bị tấn công dạng này.



Hình 2.10. Giả mạo thông tin định tuyến

STT	Mã lỗi	Mô tả lỗi	Khuyến nghị
1	core-Passive-Int	Không đặt các cổng nối với tầng Access là cổng chế độ Passive	Đặt các cổng nối với tầng Access là cổng chế độ Passive
2	Core-Routing-Info	Không xác thực thông tin định tuyến	Cấu hình xác thực thông tin định tuyến

Bảng 2.6 Bảng mô tả lỗi cấu hình và cách cấu hình khuyến nghị

Bảng dưới đây mô tả một mẫu cấu hình an ninh tiêu chuẩn cho các thiết bị ở tầng phân phối và tầng lõi

STT	Mã số	Tên lỗi	Cấu hình trên thiết bị	Cấu hình khuyến nghị
1	Passive-int	Không đặt các cổng nối với tầng truy nhập là cổng passive	*N/A*	*passive-interface [interface id]*
2	authentication	Không cài đặt xác thực giao thức định tuyến	*N/A*	*authentication mode md5*

Bảng 2.7. Mẫu cấu hình an ninh cho thiết bị tầng phân phối và tầng lõi.

CHƯƠNG 3. PHƯƠNG PHÁP THU THẬP CẤU HÌNH

3.1 Yêu cầu của việc thu thập số liệu cấu hình

Cấu hình đang hoạt động (running-config) của các thiết bị mạng thường được lưu trong bộ nhớ RAM của chính thiết bị đó. Sau đó người quản trị mạng lưu vào bộ nhớ NVRAM (Non-volatitle RAM) của thiết bị để đề phòng sự cố khi mất điện hoặc thiết bị khởi động lại thì cấu hình trên vẫn còn được lưu.

Để có thể đánh giá được cấu hình trên từng thiết bị có đảm bảo tuân thủ theo đường cơ sở an ninh hay không, thì giải pháp có thể là truy cập vào từng thiết bị, sau đó xem thông tin cấu hình trên bộ nhớ NVRAM, so sánh với cấu hình khuyến nghị. Tuy nhiên cách làm này chỉ khả thi với hệ thống mạng nhỏ (dưới 100 thiết bị mạng) vì hệ thống mạng lớn (trên 1000 thiết bị) sẽ mất rất nhiều thời gian và công sức. *Vì vậy yêu cầu của việc thu thập số liệu cấu hình là:*

i) Phải thu thập và lưu trữ tập trung số liệu cấu hình từ các thiết bị mạng về một máy chủ để thuận tiện cho việc đánh giá cấu hình.

ii) Bảo đảm cấu hình được thu thập là cấu hình hiện thời đang hoạt động trên các thiết bị (không phải là cấu hình cũ).

iii) Bảo đảm các file cấu hình không bị lỗi khi thu thập.

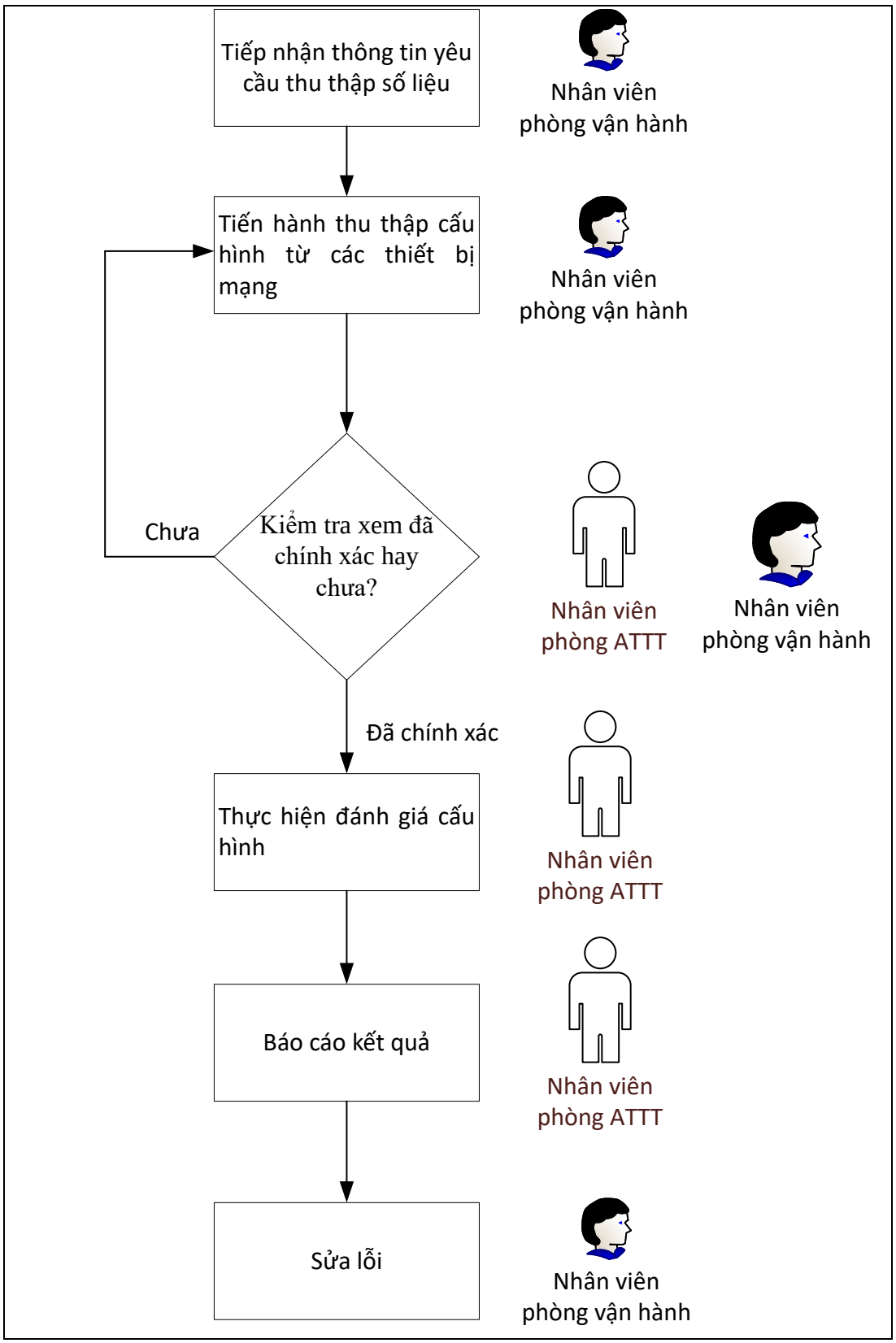
iv) Phân biệt được các file cấu hình từ các thiết bị khác nhau.

3.2 Chuẩn bị về con người, quy trình, phần cứng, phần mềm, dữ liệu

- *Con người:*

- *Người thực hiện công việc thu thập số liệu:* nhân viên phòng vận hành hệ thống mạng bởi vì phòng vận hành chịu trách nhiệm trong việc truy cập, cấu hình và quản lý thiết bị.
- *Người kiểm tra việc thu thập:* là trưởng phòng vận hành; nhân viên phòng ATTT.

- *Quy trình:* sau khi nhận được yêu cầu từ phòng ATTT, nhân viên phòng vận hành cần thu thập số liệu cấu hình *mới nhất* trên các thiết bị mạng về một thiết bị lưu trữ tập trung. Việc thu thập cấu hình về một máy chủ lưu trữ tập trung sẽ thuận tiện cho việc đánh giá, bởi vì nhân viên phòng ATTT chỉ cần đánh giá cấu hình đã lưu trên máy chủ, không cần phải đi từng thiết bị để xem cấu hình. Thời gian thu thập cấu hình phải được ghi lại.



Hình 3.1 Quy trình thu thập số liệu và báo cáo

- *Phần cứng:* phòng vận hành phải trang bị một máy chủ (server) lưu trữ tập trung cấu hình. Server này không nhất thiết cấu hình cao, có thể sử dụng một máy tính để bàn. Quan trọng phải đảm bảo máy tính này không có mã độc (phải quét virus trước khi sao

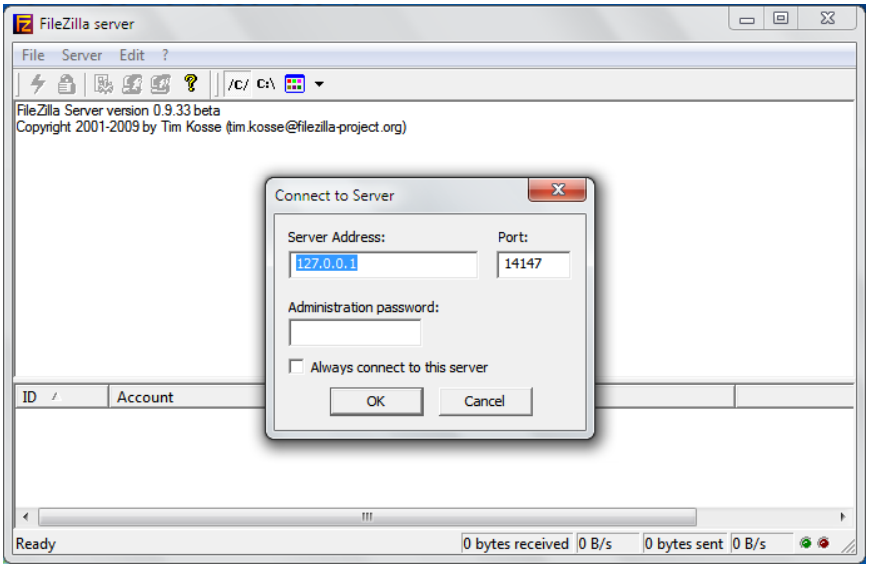
lưu) và ổ đĩa lưu trữ còn chỗ trống. (Thông thường mỗi file cấu hình chỉ có dung lượng vài chục KB).

Tiếp theo cần kết nối Server này vào vị trí hệ thống mạng sao cho các thiết bị mạng có thể truyền thông với server này.

- *Phần mềm*:

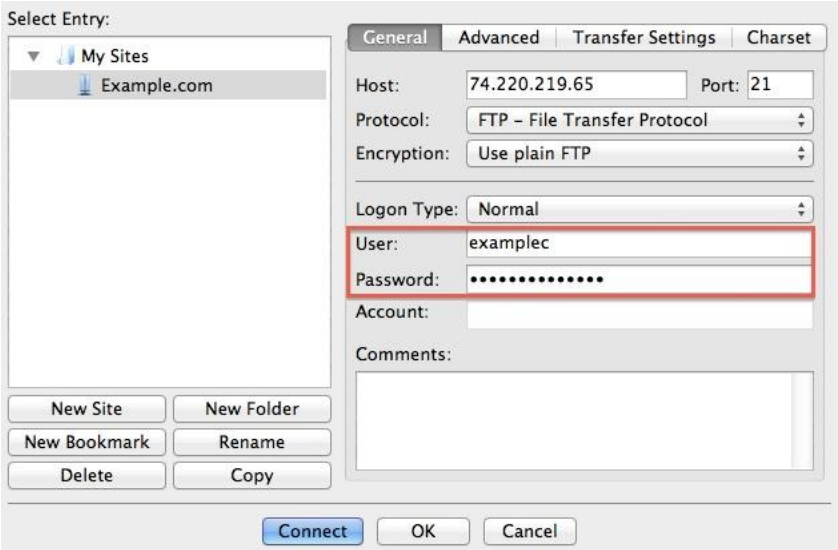
+ Hệ điều hành cho Server có thể là Windows hoặc Linux. Để tiết kiệm chi phí, có thể sử dụng một máy tính để bàn chạy hệ điều hành window 7/8/10.

+ Phần mềm FTP: cài đặt phần mềm FTP Server trên máy tính này. Khuyến nghị sử dụng phần mềm nguồn mở miễn phí FileZilla server (https://filezilla-project.org/download.php?type=server)



Hình 3.2 Giao diện chương trình Filezilla Server

Tạo một tài khoản ftp trên Filezilla server để khi truyền file từ thiết bị lên server sẽ sử dụng tài khoản này để xác thực. Tài khoản này được cấp quyền (permission) là *write* lên thư mục lưu cấu hình. Khai báo đường dẫn đến thư mục chứa các file cấu hình.



Hình 3.3 Tạo tài khoản FTP

- *Dữ liệu cấu hình:* nhân viên phòng vận hành cần truy cập vào các thiết bị để kiểm tra cấu hình đang hoạt động trên thiết bị để copy về server. Cần đảm bảo rằng, các cấu hình được thu thập là cấu hình *mới nhất*, tức là cấu hình hiện thời đang hoạt động trên thiết bị. Dưới đây là ví dụ về cấu hình trên thiết bị mạng hãng Cisco:

!

hostname router

!

ip domain-name example.com

!

crypto key generate rsa modulus 2048

!

ip ssh time-out 60

ip ssh authentication-retries 3

*ip ssh source-interface GigabitEthernet 0/1 *

!

ip ssh version 2

!

line vty 0 4

transport input ssh

!

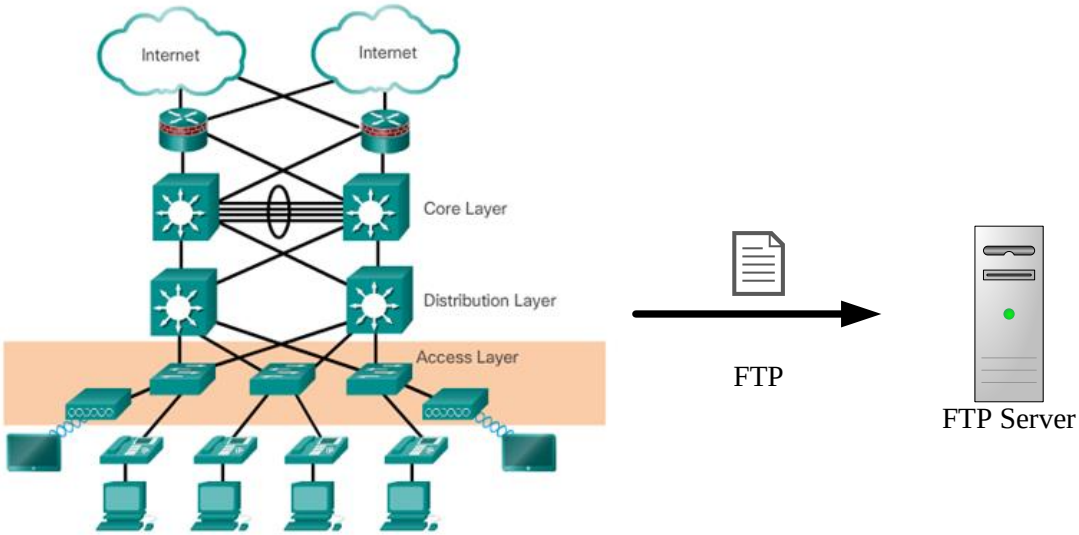
Thông thường, cấu hình đang hoạt động nằm ở bộ nhớ RAM của thiết bị và có tên gọi là *running-config.*

3.3 Cách copy cấu hình về máy chủ

Lưu ý: *Nếu trong trường hợp phòng vận hành đã thực hiện sao lưu cấu hình từ các thiết bị về máy chủ, thì bước này có thể bỏ qua.*

Nếu chưa thực hiện sao lưu, để copy cấu hình từ các thiết bị về máy chủ thì cần thực hiện các bước như sau

Cấu hình trên các thiết bị mạng thường được lưu ở bộ nhớ NVRAM của thiết bị và phải được sao lưu dự phòng tập trung trên một máy chủ. Mỗi thiết bị có một file cấu hình riêng, dưới dạng file text. Tên file thường được đặt theo tên của thiết bị.



Hình 3.4 Phương pháp thu thập cấu hình

Nếu doanh nghiệp chưa thực hiện việc sao lưu tập trung cấu hình thì cần thực hiện công việc này. Công việc sao lưu cấu hình do nhân viên phòng vận hành thực hiện. Các bước làm như sau:

Đầu tiên người quản trị truy cập vào từng thiết bị và sử dụng câu lệnh copy cấu hình *running-config* trên thiết bị về máy chủ lưu trữ tập trung. Giao thức sử dụng là FTP. Lưu ý quy tắc đặt tên file cấu hình khi copy để tránh bị trùng lặp tên file.

Bước	Câu lệnh	Mục đích
1	Router# **configure terminal**	Truy cập vào chế độ cấu hình

2	Router(config)# **ip ftp username** *username*	Khai báo FTP username (trên Filezilla)
3	Router(config)# **ip ftp password** *password*	Khai báo FTP Password (trên Filezilla)
4	Router(config)# **end**	Thoát khỏi chế độ cấu hình
5	Router# **copy system:running-config ftp:**[[[//[*username*[**:***password*]**@**]*location*] */directory*]/*filename*]	Copy cấu hình running-config lên FTP server. *Lưu ý tên file cấu hình phải khác nhau.*

Bảng 3.1 Các bước copy file cấu hình từ thiết bị lên máy chủ.

3.3.1 Quy định về đặt tên file cấu hình.

Ở bước số 5 bảng trên, khi thiết bị sẽ yêu cầu quản trị viên nhập tên file cấu hình sẽ lưu ở máy chủ FTP, cần đặt tên file cấu hình như sau:

[Mã tầng-Tên-thiết-bị-config]

Trong đó *[Mã tầng]* có ký hiệu sau:

- Tầng Core: C.
- Tầng Distribution:D
- Tầng Access: A
- Ghi chú: Nếu hệ thống mạng chỉ được thiết kế theo mô hình 2 lớp (Collapsed Core) thì ký hiệu *Mã tầng* ở tầng Collapsed Core là: CD

3.3.2 Phương pháp lấy mẫu nếu số lượng thiết bị lớn.

Trong trường hợp số lượng thiết bị lớn (>1000 thiết bị) thì có thể sử dụng phương pháp lấy mẫu ngẫu nhiên để đánh giá. Theo phương pháp này, có thể lấy danh sách các thiết bị, sau đó thu thập cấu hình ngẫu nhiên của 20% thiết bị. Như vậy tổng cộng sẽ lấy cấu hình của khoảng 200 thiết bị. Đây là mẫu đủ lớn để đánh giá được hiện trạng cấu hình an ninh trên các thiết bị hạ tầng mạng.

3.3.3 Kiểm tra các file cấu hình thu thập được

Sau khi copy cần kiểm tra lại số lượng file đã copy lên máy chủ FTP Server đã đầy đủ hay chưa. Phương pháp kiểm tra như sau:

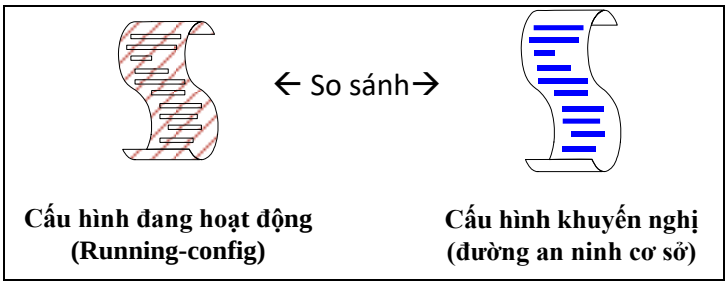
- *Về số lượng file thu thập được:* Số lượng file trên FTP Server phải bằng số thiết bị đã được copy cấu hình.
- *Về tên file cấu hình:* các file cấu hình phải được đặt tên theo đúng quy định ở mục 4.2.1.
- *Về nội dung của file cấu hình thu thập được:* Quản trị viên và nhân viên bảo mật có thể mở ngẫu nhiên một vài file cấu hình để kiểm tra nội dung. Sau đó so sánh lại với cấu hình running-config trên thiết bị để đảm bảo việc copy là chính xác.

CHƯƠNG 4. PHƯƠNG PHÁP ĐÁNH GIÁ CẤU HÌNH AN NINH

4.1 Phương pháp chung để đánh giá cấu hình an ninh

Sau khi đã thu thập được cấu hình trên các thiết bị mạng về máy chủ FTP, bước tiếp theo là đánh giá cấu hình an ninh.

Để thực hiện đánh giá cấu hình an ninh trên thiết bị mạng có tuân thủ theo chính sách an ninh hay không, thì cần so sánh cấu hình hiện tại đang hoạt động với cấu hình an ninh khuyến nghị (đường cơ sở an ninh).



Hình 4.1 Phương pháp đánh giá cấu hình an ninh

Phương pháp này có thể coi là một phương pháp đo kiểm tra giữa các tham số cấu hình đang hoạt động với một tham số cho trước. Có một số chuẩn đề cập tới mô hình, phương pháp đo lường, đánh giá ATTT thường được sử dụng đó là ISO 27004:2014, NIST SP800-55, ISO/IEC 15408:2009, FIPS 140-2. Hiện tại ở Việt Nam đã ban hành tiêu chuẩn TCVN 10542 :2014. Tiêu chuẩn này cung cấp hướng dẫn về việc phát triển và sử dụng các số đo và bài đo để đánh giá hiệu lực của một hệ thống quản lý an toàn thông tin (ISMS) đã triển khai và các biện pháp quản lý hay nhóm các biện pháp quản lý. Tiêu chuẩn này khuyến nghị áp dụng đối với tất cả các tổ chức ở mọi loại hình và quy mô (ví dụ, các doanh nghiệp thương mại, các cơ quan Chính phủ, các cơ quan quản lý Nhà nước, các tổ chức phi lợi nhuận). Vì vậy luận văn này đề xuất áp dụng mô hình đánh giá an ninh đề cập trong tiêu chuẩn này để đánh giá các tiêu chí về cấu hình an ninh trên các thiết bị mạng.

Sau khi so sánh giữa cấu hình đang hoạt động và cấu hình mẫu, chúng ta sẽ biết được cấu hình trên các thiết bị có tuân thủ đúng với chính sách an ninh của doanh nghiệp/ tổ chức đặt ra hay không. Kết quả báo cáo có 2 trạng thái là "*Đạt*" hoặc "*Không đạt*"

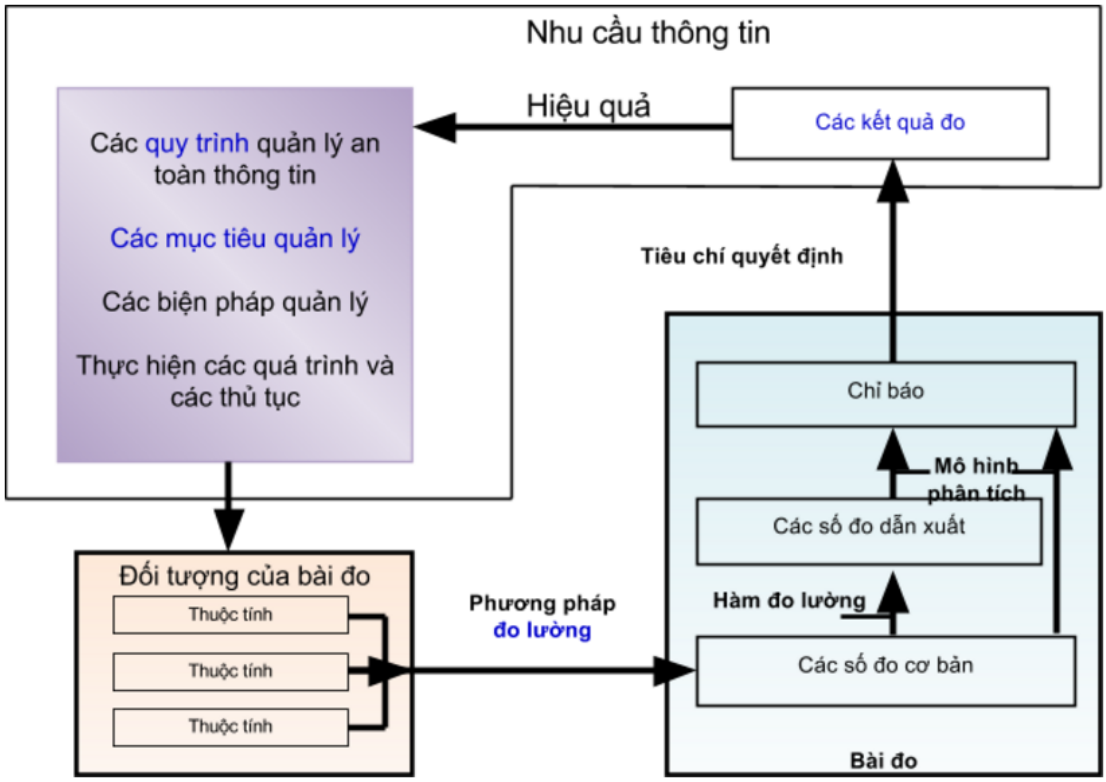
Mẫu báo cáo đường an ninh cơ sở tùy thuộc vào từng tổ chức. Trong báo cáo này, cần có kết quả của 3 bài đo kiểm tra cấu hình an ninh. Cột *"Lý do"* để lưu lại những lý do tại sao không đạt yêu cầu về việc cấu hình. Đây là kết quả của buổi làm việc giữa Phòng

vận hành và Phòng ATTT. Phòng vận hành có trách nhiệm giải trình tại sao những thuộc tính an ninh đó không được thực hiện; khi nào thì sẽ thực hiện.

Từ báo cáo trên, người quản trị mạng sẽ xem xét và thực hiện cấu hình lại những lỗi để đảm bảo cấu hình an ninh đang chạy tuân thủ theo chính sách an toàn bảo mật thông tin mà công ty đã đề ra.

4.2 Tiêu chuẩn đo lường an ninh TCVN 10542:2014

Mô hình đo lường ATTT là một cấu trúc liên kết một nhu cầu thông tin tới các đối tượng có liên quan của bài đo và các thuộc tính của chúng. Đối tượng đo lường có thể bao gồm kế hoạch đã định hoặc các quy trình, các thủ tục, các dự án và các nguồn lực đã triển khai. Mô hình đo lường an toàn thông tin mô tả làm sao để các thuộc tính liên quan được định lượng và chuyển đổi thành các chỉ báo cung cấp cơ sở cho việc ra quyết định.



Hình 4.2 Mô hình đo lường ATTT

Trong đó:

- Các quy trình quản lý ATTT, các mục tiêu quản lý, các biện pháp, các quy trình thủ tục.

Những thông tin này được lấy từ chính sách an ninh trong doanh nghiệp. Chính sách an ninh là một tập các quy tắc quy định liên quan đến việc bảo đảm an toàn bảo mật cho hệ thống công nghệ thông tin. Bên cạnh đó chính sách này còn xác định rõ trách nhiệm,

quyền hạn của người dùng tham gia vào việc sử dụng vào việc vận hành hệ thống công nghệ thông tin. Chính sách này được xây dựng từ các tiêu chuẩn, quy định, quy trình, các khuyến nghị về ATTT.

Người thực hiện công tác đánh giá an ninh cấu hình thiết bị có thể lọc ra những điều khoản quy định về an ninh cấu hình thiết bị trong tài liệu về chính sách an ninh của doanh nghiệp, tổ chức. Chính sách này sẽ liên tục được cập nhật theo thời gian. Việc đánh giá tiếp tục được thực hiện theo định kỳ dựa vào chính sách an ninh.

- Đối tượng của bài đo

Đối tượng (thực thể) được đặc trưng thông qua bài đo các thuộc tính của nó. Một đối tượng bao gồm các quy trình, các kế hoạch, các dự án, các nguồn lực, các hệ thống, và các thành phần.

Thuộc tính là tính chất hoặc đặc trưng của đối tượng của bài đo có thể được phân biệt về số lượng hoặc chất lượng bởi con người hoặc bởi tự động.

- Số đo cơ bản và phương pháp đo

Một số đo cơ bản là số đo đơn giản nhất mà có thể có được. Một số đo cơ bản là các kết quả việc ứng dụng một phương pháp đo lường tới các thuộc tính được lựa chọn của một đối tượng của bài đo. Đối tượng của bài đo có thể có nhiều thuộc tính, chỉ một số trong đó có thể cung cấp các giá trị hữu ích để được gán nhận cho một số đo cơ bản. Một thuộc tính đã cho có thể được sử dụng cho nhiều số đo cơ bản khác nhau.

Một phương pháp đo là một trình tự logic của các thuật toán được sử dụng trong việc định lượng một thuộc tính đối tượng tương ứng với một thang giá trị xác định. Thuật toán có thể bao gồm các hành động như đếm số lần xảy ra hay việc quan sát thời gian đã qua.

Phương pháp đo có thể áp dụng nhiều thuộc tính cho một đối tượng của đo lường. Đối tượng đo lường ở đây là những cấu hình an ninh trên thiết bị hạ tầng mạng đã đề cập ở Phần 2.

- Số đo dẫn xuất và hàm đo lường

Số đo dẫn xuất là kết hợp của hai hoặc nhiều số đo cơ bản. Một số đo cơ bản có thể phục vụ như là đầu vào một số số đo dẫn xuất.

Hàm đo lường là một sự tính toán được sử dụng để kết hợp các số đo cơ bản với nhau để tạo ra số đo dẫn xuất.

Thang giá trị và đơn vị của số đo dẫn xuất phụ thuộc vào các thang giá trị và các đơn vị của các số đo cơ bản mà có liên quan cũng như làm thế nào chúng được kết hợp với nhau bởi các hàm đo lường.

Hàm đo lường có thể liên quan đến một loạt các kỹ thuật, chẳng hạn như tính trung bình các số đo cơ bản, áp dụng các trọng số cho các số đo cơ bản, hoặc gán nhận các giá trị chất lượng cho các số đo cơ bản. Hàm đo lường có thể kết hợp các số đo cơ bản sử dụng các thang giá trị khác nhau, chẳng hạn như tỷ lệ phần trăm và các kết quả đo chất lượng.

- Chỉ báo và mô hình phân tích

Chỉ báo là một số đo mà cung cấp một ước tính và định lượng các thuộc tính xác định được rút ra/có nguồn gốc từ một mô hình phân tích đối với một nhu cầu thông tin cụ thể. Các chỉ báo thu được bằng cách áp dụng một mô hình phân tích cho một số đo cơ bản hay số đo dẫn xuất và kết hợp chúng với các tiêu chí quyết định. Thang giá trị và phương pháp đo ảnh hưởng đến sự lựa chọn của các kỹ thuật phân tích được sử dụng để tạo ra các chỉ báo.

- Kết quả đo và tiêu chí quyết định

Kết quả đo hoàn thiện sẽ gồm các chỉ báo có các diễn giải khả dụng dựa trên tiêu chí quyết định và nên được xem xét trong bối cảnh các mục tiêu đo lường tổng thể của việc đánh giá các hiệu lực của hệ thống ATTT (ISMS). Tiêu chí quyết định được sử dụng để xác định các hành động cần thiết hay các soát xét kỹ hơn, như là để miêu tả mức độ độ tin tưởng của kết quả đo. Tiêu chí quyết định cũng có thể được ứng dụng tới một chuỗi các chỉ báo, để làm cơ sở đưa ra các xu hướng phân tích dựa trên các chỉ báo nhận được từ những thời điểm khác nhau.

Các mục tiêu chỉ ra các khả năng đặc tả kỹ thuật chi tiết, có thể ứng dụng được cho tổ chức hay cho cả các bên liên quan, được lấy từ các đối tượng an toàn thông tin như là các mục tiêu của hệ thống quản lý an ninh (ISMS – Information Security Management System), các mục tiêu quản lý, và cần được thiết lập và đáp ứng để đạt được các mục tiêu này.

TÊN CÁC THÀNH PHẦN	**GIẢI THÍCH**
Thông tin chung của bài đo	
Tên bài đo	**Tên bài đo**

Số hiệu	Số định danh duy nhất, tùy ý theo quy định của tổ chức
Mục đích	Mô tả các lý do dẫn đến cần thiết của bài đo
Mục tiêu biện pháp quản lý	Quản lý các đối tượng trong bài đo (đã có kế hoạch hoặc đã được triển khai)
Biện pháp quản lý (1)	Biện pháp quản lý cần đo lường
Biện pháp quản lý (2)	Tùy chọn: biện pháp quản lý/ quy trình cao hơn trong nhóm đã bao gồm trong cùng bài đo, nếu có thể áp dụng (đã có kế hoạch hoặc đã được triển khai)
Đối tượng của bài đo và các thuộc tính	
Đối tượng	Đối tượng (thực thể) được đặc trưng thông qua bài đo các thuộc tính của nó. Một đối tượng bao gồm các quy trình, các kế hoạch, các dự án, các nguồn lực, các hệ thống, và các thành phần.
Thuộc tính	Tính chất hoặc đặc trưng của đối tượng của bài đo có thể được phân biệt về số lượng hoặc chất lượng bởi con người hoặc bởi tự động.
Thông tin đặc tả về số đo cơ bản (cho mỗi số đo cơ bản [từ 1 đến n])	
Số đo cơ bản	Một số đo cơ bản được xác định theo một thuộc tính và phương pháp đo cụ thể để định lượng thuộc tính (ví dụ như số người đã được đào tạo, số lượng các điểm/sites, chi phí tính đến nay). Theo dữ liệu thu thập, một giá trị được gán nhận cho một số đo cơ bản.
Phương pháp đo	Trình tự các hoạt động sử dụng trong định lượng thuộc tính về một phạm vi cụ thể.
Loại phương pháp đo	Dựa trên bản chất các hoạt động sử dụng để định lượng thuộc tính, phân thành hai Phương pháp đo: - Chủ quan: định lượng liên quan tới chủ định của con người. - Khách quan: định lượng dựa trên các quy tắc số học.

Thang giá trị	Tập hợp các giá trị có thứ tự, hoặc tập các danh mục được ánh xạ tới thuộc tính của số đo cơ bản
Loại thang giá trị	Dựa trên bản chất mối quan hệ giữa các giá trị, phân thành bốn loại thang giá trị phổ biến: Danh định; thứ tự; khoảng đoạn; tỷ lệ.
Đơn vị đo	Số lượng cụ thể, được xác định và phù hợp theo quy ước, với các số lượng khác cùng loại được so sánh theo một thứ tự để diễn tả mối tương quan với số lượng đó.
Thông tin đặc tả về số đo dẫn xuất	
Số đo dẫn xuất	Một số đo được rút ra từ hai hoặc nhiều hơn số đo cơ bản.
Hàm đo lường	Thuật toán hoặc tính toán được thực hiện để kết hợp hai hoặc nhiều số đo cơ bản. Thang giá trị và đơn vị của số đo dẫn xuất dựa trên thang giá trị của các số đo cơ bản mà nó bao gồm cũng như cách kết hợp các hàm đo lường với nhau.
Thông tin đặc tả về chỉ báo	
Chỉ báo	Số đo mà cung cấp những ước tính hay định lượng các thuộc tính xác định thông qua mô hình phân tích với những thông tin cần thiết. Các chỉ báo là cơ sở để phân tích và đưa ra quyết định.
Mô hình phân tích	Thuật toán hoặc việc kết hợp tính toán một hoặc nhiều số đo cơ bản hoặc các số đo dẫn xuất với tiêu chí quyết định phù hợp; Điều này dựa trên sự hiểu biết hoặc các dữ kiện, mối quan hệ dự tính giữa số đo cơ bản hoặc số đo dẫn xuất hoặc trạng thái của chúng. Nhờ mô hình phân tích sẽ giúp ước lượng hay định lượng mối quan hệ để xác định thông tin cần thiết.
Thông tin đặc tả về tiêu chí quyết định	
Tiêu chí quyết định	Ngưỡng, mục tiêu, hoặc các mẫu được sử dụng để xác định sự cần thiết phải hành động hay điều tra thêm, hoặc

	để mô tả mức độ chính xác của kết quả bài đo nhất định. Tiêu chí quyết định giúp làm rõ các kết quả của bài đo.
Kết quả bài đo	
Giải thích chỉ báo	Mô tả về chỉ báo, để chỉ báo được hiểu rõ ràng hơn.
Định dạng hồ sơ đo	Định dạng hồ sơ đo nên được đánh nhãn và lưu thành tài liệu. Mô tả các theo dõi, nhận xét về tổ chức hoặc người sở hữu thông tin có thể cần được ghi lại. Định dạng hồ sơ đo trực quan sẽ miêu tả các đánh giá và cung cấp giải thích rõ ràng về các chỉ dẫn. Định dạng hồ sơ đo nên được tùy chỉnh theo thông tin khách hàng.
Các bên liên quan	
Người trách nhiệm bài đo	Ban quản lý hoặc các bên quan tâm yêu cầu hoặc cần thông tin về hiệu lực của một hệ thống ISMS, các biện pháp quản lý hoặc nhóm biện pháp quản lý.
Người xem xét kết quả đo	Cá nhân hoặc tổ chức mà kiểm tra tính hợp lệ cho các cấu trúc bài đo đã tiến hành là đủ điều kiện cho việc đánh giá hiệu lực của một hệ thống ISMS, các biện pháp quản lý hoặc nhóm biện pháp quản lý.
Người sở hữu thông tin	Cá nhân hoặc tổ chức sở hữu thông tin về một đối tượng của bài đo và chịu trách nhiệm về bài đo.
Bộ phận thu thập thông tin	Cá nhân hoặc tổ chức chịu trách nhiệm về thu thập, ghi chép và lưu trữ dữ liệu.
Bộ phận trao đổi thông tin	Cá nhân hoặc tổ chức chịu trách nhiệm phân tích dữ liệu và trao đổi các kết quả bài đo.
Tần suất thực hiện	
Tần suất thu thập dữ liệu	Mức độ thường xuyên thu thập dữ liệu.
Tần suất phân tích dữ liệu	Mức độ thường xuyên phân tích dữ liệu.
Tần suất và hồ sơ đo	Mức độ thường xuyên của các kết quả đo được lập hồ sơ (mức độ này có thể thấp hơn Tần suất thu thập dữ liệu).

Tần suất sửa đổi bài đo	Ngày sửa đổi bài đo (thời hạn hiệu lực của tính hợp lệ của bài đo hoặc các thay đổi của bài đo)
Tần suất thực hiện bài đo	Xác định định kỳ thực hiện bài đo.

Bảng 4.1 Các thuật ngữ trong mô hình đo kiểm ATTT

4.3 Đánh giá lỗi cấu hình quản lý

Đối với cấu hình quản lý, sẽ thực hiện bài đo so sánh giữa cấu hình quản lý đang hoạt động và cấu hình quản lý khuyến nghị theo đường cơ sở an ninh. Các thuộc tính cơ bản là các thông số cấu hình trong Mục 3.6.1.

TÊN CÁC THÀNH PHẦN	GIẢI THÍCH
Thông tin chung của bài đo	
Tên bài đo	**Đo các tham số về cấu hình an ninh trong việc quản lý thiết bị.**
Số hiệu	Device-Management-Check
Mục đích	Kiểm tra các cấu hình quản lý trên thiết bị xem có tuân thủ theo chính sách an ninh hay không.
Mục tiêu biện pháp quản lý	Kiểm tra được cấu hình quản lý trên thiết bị xem có lỗi hay không để từ đó có biện pháp khắc phục.
Biện pháp quản lý (1)	Có sự tham gia của Phòng ATTT và Phòng vận hành. • Phòng vận hành: thu thập cấu hình. • Phòng ATTT: đánh giá cấu hình an ninh.
Biện pháp quản lý (2)	
Đối tượng của bài đo và các thuộc tính	
Đối tượng	Cấu hình quản lý trên thiết bị mạng.
Thuộc tính	Các cấu hình quản lý đề cập trong mục 3.6.1
Thông tin đặc tả về số đo cơ bản (cho mỗi số đo cơ bản [từ 1 đến n])	
Số đo cơ bản	mnt-TELNET mnt-HTTP mnt-FTPTFTP mnt-int-ACL-BLK mnt-SNMP

	mnt-PasswordLocal mnt-PasswordENCRYPT mnt-NTP mnt-SYSLOG
Phương pháp đo	So sánh cấu hình mẫu (khuyến nghị) với cấu hình hiện tại xem có khớp nhau hay không
Loại phương pháp đo	Khách quan: định lượng dựa trên các quy tắc số học.
Thang giá trị	Có/Không *Có*: tức là có thực hiện cấu hình tham số quản lý thiết bị *Không:* là không thực hiện cấu hình tham số quản lý thiết bị
Loại thang giá trị	
Đơn vị đo	
Thông tin đặc tả về số đo dẫn xuất	
Số đo dẫn xuất	
Hàm đo lường	
Thông tin đặc tả về chỉ báo	
Chỉ báo	Có/Không
Mô hình phân tích	
Thông tin đặc tả về tiêu chí quyết định	
Tiêu chí quyết định	Theo thang giá trị là “Có”/”Không”.
Kết quả bài đo	
Giải thích chỉ báo	Mô tả ý nghĩa từng tham số cấu hình quản lý thiết bị.
Định dạng hồ sơ đo	Báo cáo dưới dạng văn bản
Các bên liên quan	
Người trách nhiệm bài đo	Nhân viên phòng ATTT
Người xem xét kết quả đo	Trưởng phòng ATTT; Người phụ trách về CNTT trong doanh nghiệp.
Người sở hữu thông tin	Phòng ATTT

Bộ phận thu thập thông tin	Phòng vận hành
Bộ phận trao đổi thông tin	Phòng vận hành; Phòng ATTT
Tần suất thực hiện	
Tần suất thu thập dữ liệu	Tùy theo chính sách an ninh của tổ chức.
Tần suất phân tích dữ liệu	Tùy theo chính sách an ninh của tổ chức.
Tần suất và hồ sơ đo	
Tần suất sửa đổi bài đo	
Tần suất thực hiện bài đo	

Bảng 4.2 Bảng đo kiểm các lỗi cấu hình quản lý

4.4 Đánh giá lỗi cấu hình thiết bị tầng truy nhập

TÊN CÁC THÀNH PHẦN	GIẢI THÍCH
Thông tin chung của bài đo	
Tên bài đo	**Đo các tham số về cấu hình an ninh trên thiết bị ở tầng truy nhập**
Số hiệu	Access-Device-Check
Mục đích	Kiểm tra các cấu hình an ninh trên các thiết bị tầng truy nhập xem có tuân thủ theo chính sách an ninh hay không.
Mục tiêu biện pháp quản lý	Kiểm tra các cấu hình an ninh trên các thiết bị tầng truy nhập xem có tuân thủ theo chính sách an ninh hay không, để từ đó có biện pháp khắc phục.
Biện pháp quản lý (1)	Có sự tham gia của Phòng ATTT và Phòng vận hành. • Phòng vận hành: thu thập cấu hình. • Phòng ATTT: đánh giá cấu hình an ninh.
Biện pháp quản lý (2)	
Đối tượng của bài đo và các thuộc tính	

Đối tượng	Cấu hình an ninh trên trên thiết bị mạng ở tầng truy nhập (switch lớp 2, thiết bị định tuyến không dây).
Thuộc tính	Các cấu hình quản lý đề cập trong mục 3.6.2 Bảng số
Thông tin đặc tả về số đo cơ bản (cho mỗi số đo cơ bản [từ 1 đến n])	
Số đo cơ bản	**<u>Đối với switch lớp 2</u>** acc-shutdown acc-dhcpsnooping acc-DAI acc-portsecurity acc-IPSouceGuard acc-IPv6 acc-BPDUGuard **<u>Đối với thiết bị định tuyến không dây</u>** wl-SSID wl-SimplePass wl-MAC wl-Default
Phương pháp đo	So sánh cấu hình mẫu (khuyến nghị) với cấu hình hiện tại xem có khớp nhau hay không
Loại phương pháp đo	Khách quan: định lượng dựa trên các quy tắc số học.
Thang giá trị	Có/Không *Có*: tức là có thực hiện cấu hình tham số quản lý thiết bị *Không:* là không thực hiện cấu hình tham số quản lý thiết bị
Loại thang giá trị	
Đơn vị đo	
Thông tin đặc tả về số đo dẫn xuất	
Số đo dẫn xuất	
Hàm đo lường	
Thông tin đặc tả về chỉ báo	
Chỉ báo	Có/Không

Mô hình phân tích	
Thông tin đặc tả về tiêu chí quyết định	
Tiêu chí quyết định	Theo thang giá trị là “Có”/”Không”.
Kết quả bài đo	
Giải thích chỉ báo	Mô tả ý nghĩa từng tham số cấu hình trên thiết bị tầng truy nhập
Định dạng hồ sơ đo	Báo cáo dưới dạng văn bản
Các bên liên quan	
Người trách nhiệm bài đo	Nhân viên phòng ATTT
Người xem xét kết quả đo	Trưởng phòng ATTT; Người phụ trách về CNTT trong doanh nghiệp.
Người sở hữu thông tin	Phòng ATTT
Bộ phận thu thập thông tin	Phòng vận hành
Bộ phận trao đổi thông tin	Phòng vận hành; Phòng ATTT
Tần suất thực hiện	
Tần suất thu thập dữ liệu	Tùy theo chính sách an ninh của tổ chức.
Tần suất phân tích dữ liệu	Tùy theo chính sách an ninh của tổ chức.
Tần suất và hồ sơ đo	
Tần suất sửa đổi bài đo	
Tần suất thực hiện bài đo	

Bảng 4.3 Bảng đo kiểm các lỗi cấu hình tầng truy nhập

4.5 Đánh giá lỗi cấu hình thiết bị tầng phân phối và tầng core

Đối với cấu hình thiết bị tầng phân phối/lõi, sẽ thực hiện kiểm tra những vấn đề lỗi sau:

TÊN CÁC THÀNH PHẦN	GIẢI THÍCH

Thông tin chung của bài đo	
Tên bài đo	**Đo các tham số về cấu hình an ninh trên thiết bị ở tầng phân phối/tầng lõi.**
Số hiệu	Distribution-Core-Device-Check
Mục đích	Kiểm tra các cấu hình an ninh trên các thiết bị tầng truy nhập xem có tuân thủ theo chính sách an ninh hay không.
Mục tiêu biện pháp quản lý	Kiểm tra các cấu hình an ninh trên các thiết bị tầng truy nhập xem có tuân thủ theo chính sách an ninh hay không, để từ đó có biện pháp khắc phục.
Biện pháp quản lý (1)	Có sự tham gia của Phòng ATTT và Phòng vận hành. • Phòng vận hành: thu thập cấu hình. • Phòng ATTT: đánh giá cấu hình an ninh.
Biện pháp quản lý (2)	
Đối tượng của bài đo và các thuộc tính	
Đối tượng	Cấu hình an ninh trên trên thiết bị mạng ở tầng phân phối/tầng lõi (thiết bị định tuyến, thiết bị chuyển mạch lớp 3)
Thuộc tính	Các cấu hình quản lý đề cập trong mục 3.6.3 Bảng số
Thông tin đặc tả về số đo cơ bản (cho mỗi số đo cơ bản [từ 1 đến n])	
Số đo cơ bản	**Core-Passive-Int** **Core-Routing-Info**
Phương pháp đo	So sánh cấu hình mẫu (khuyến nghị) với cấu hình hiện tại xem có khớp nhau hay không
Loại phương pháp đo	Khách quan: định lượng dựa trên các quy tắc số học.
Thang giá trị	Có/Không - *Có*: tức là có thực hiện cấu hình tham số quản lý thiết bị - *Không:* là không thực hiện cấu hình tham số quản lý thiết bị
Loại thang giá trị	
Đơn vị đo	
Thông tin đặc tả về số đo dẫn xuất	
Số đo dẫn xuất	

Hàm đo lường	
Thông tin đặc tả về chỉ báo	
Chỉ báo	Có/Không
Mô hình phân tích	
Thông tin đặc tả về tiêu chí quyết định	
Tiêu chí quyết định	Theo thang giá trị là “Có”/”Không”.
Kết quả bài đo	
Giải thích chỉ báo	Mô tả ý nghĩa từng tham số cấu hình trên thiết bị tầng phân phối và tầng lỗi
Định dạng hồ sơ đo	Báo cáo dưới dạng văn bản
Các bên liên quan	
Người trách nhiệm bài đo	Nhân viên phòng ATTT
Người xem xét kết quả đo	Trưởng phòng ATTT; Người phụ trách về CNTT trong doanh nghiệp.
Người sở hữu thông tin	Phòng ATTT
Bộ phận thu thập thông tin	Phòng vận hành
Bộ phận trao đổi thông tin	Phòng vận hành; Phòng ATTT
Tần suất thực hiện	
Tần suất thu thập dữ liệu	Tùy theo chính sách an ninh của tổ chức.
Tần suất phân tích dữ liệu	Tùy theo chính sách an ninh của tổ chức.
Tần suất và hồ sơ đo	
Tần suất sửa đổi bài đo	
Tần suất thực hiện bài đo	

Bảng 4.4 Đo kiểm các lỗi cấu hình tầng phân phối và tầng lõi

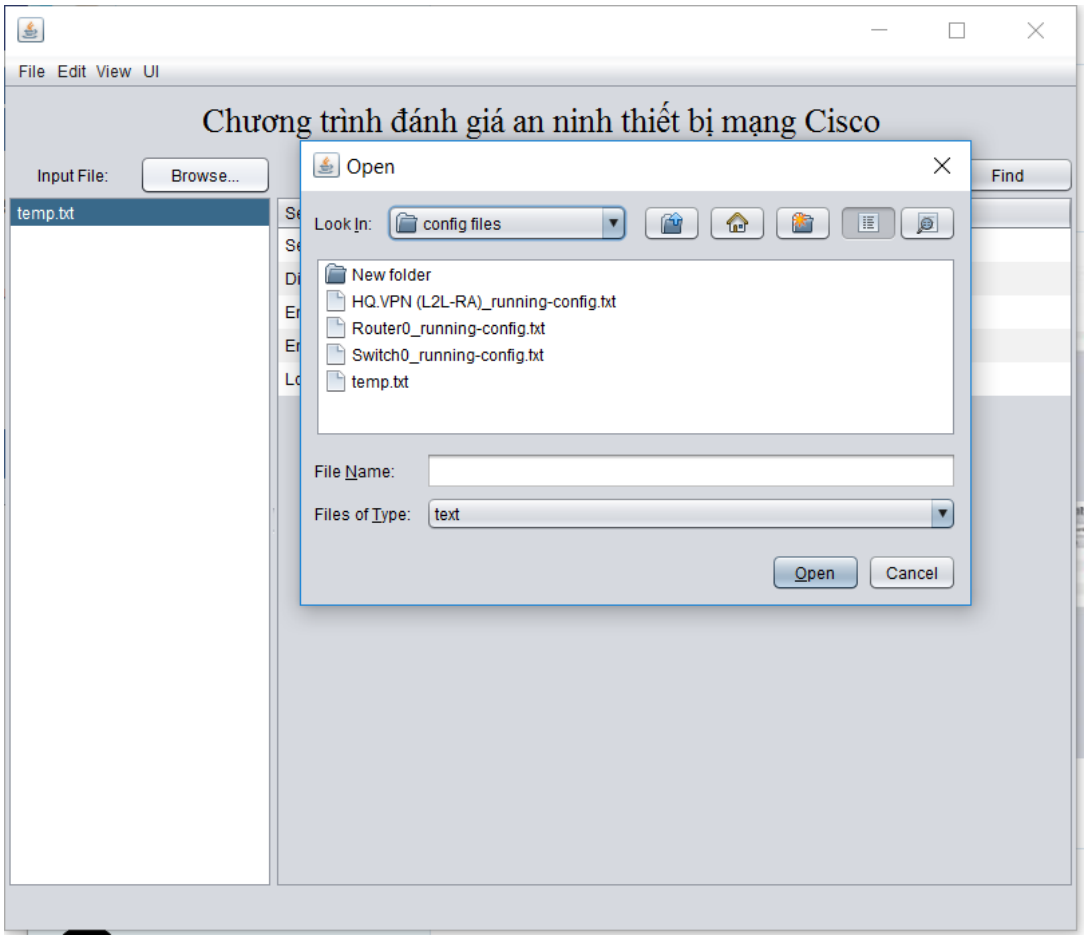
4.6 Chương trình đánh giá lỗi cấu hình

4.6.1 Những tính năng chính của chương trình

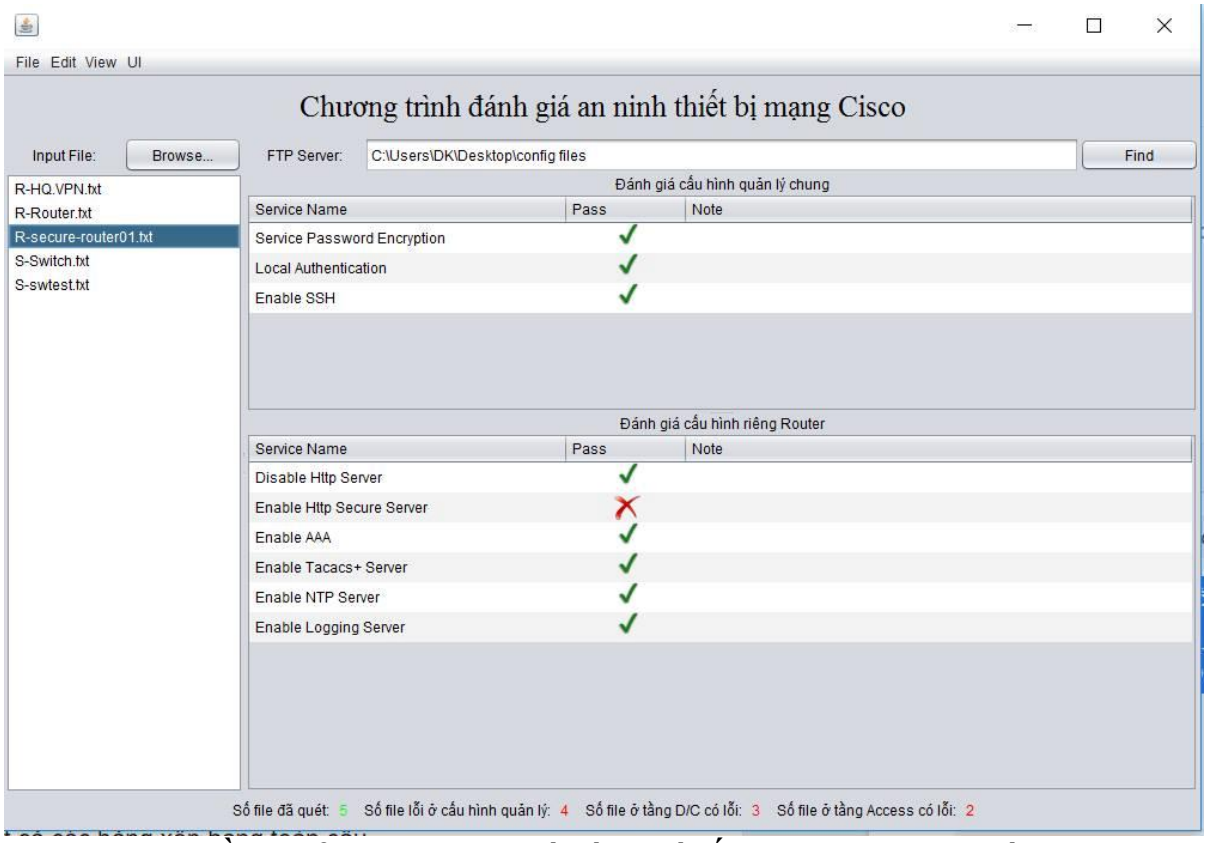
Để hỗ trợ cho việc đánh giá, luận văn đề xuất xây dựng một chương trình ứng dụng phân tích cấu hình tự động.

Đầu vào của chương trình là một thư mục chứa các file cấu hình của các thiết bị mạng trong một hệ thống mạng. Đầu ra là kết quả báo cáo tổng hợp về tình trạng cấu hình an ninh của hệ thống mạng đó.

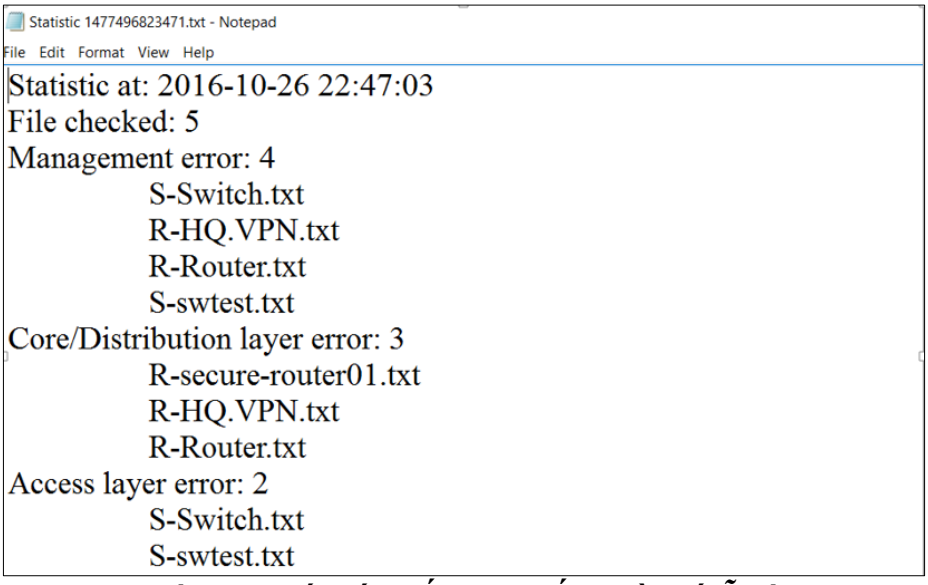
Ngoài ra chương trình còn xuất ra báo cáo chi tiết những lỗi cấu hình an ninh trên từng thiết bị mạng.



Hình 4.4 Đầu vào của chương trình là thư mục chứa các cấu hình cần đánh giá



Hình 4.5 Đầu ra của chương trình là đánh giá cấu hình an ninh trên từng Router



Hình 4.6 Báo cáo thống kê thiết bị nào có lỗi gì

```
<services>
    <service>
        <name>Service Password Encryption</name>
        <checkStrings>
            <startWith>service password-encryption</startWith>
        </checkStrings>
    </service>
    <service>
    <service>
        <name>Enable Http Secure Server</name>
        <checkStrings>
            <startWith>ip http secure-server</startWith>
        </checkStrings>
    </service>
    <service>
        <name>Enable SSH</name>
        <checkStrings>
    </service>
    <service>
        <name>Local Authentication</name>
        <checkStrings>
            <startWith>username </startWith>
            <contain>secret</contain>
            <contain>password</contain>
        </checkStrings>
    </service>

</services>
```

Hình 4.7 Điều chỉnh các quy định về cấu hình vào file XML

Công cụ phát triển:

Java Swing: là một bộ công cụ tiện ích, là một phần của ngôn ngữ lập trình Java tổng thể. **Java Swing** là một phần của Java Foundation Classes (JFC) được sử dụng để tạo các ứng dụng Window-Based. Lý do lựa chọn công cụ này là do Java Swing cung cấp các thành phần phát triển gọn nhẹ, độc lập. Do vậy chương trình khi biên dịch ra nhỏ gọn và chạy trên nhiều nền tảng (hệ điều hành) khác nhau.

- *Ưu điểm của chương trình:*

- Cho phép thêm các quy định về an ninh khi cần
- Gọn nhẹ, xử lý nhanh, dễ sử dụng
- Chạy đa nền tảng
- Cho phép hiệu chỉnh các quy định về cấu hình

- *Nhược điểm:*

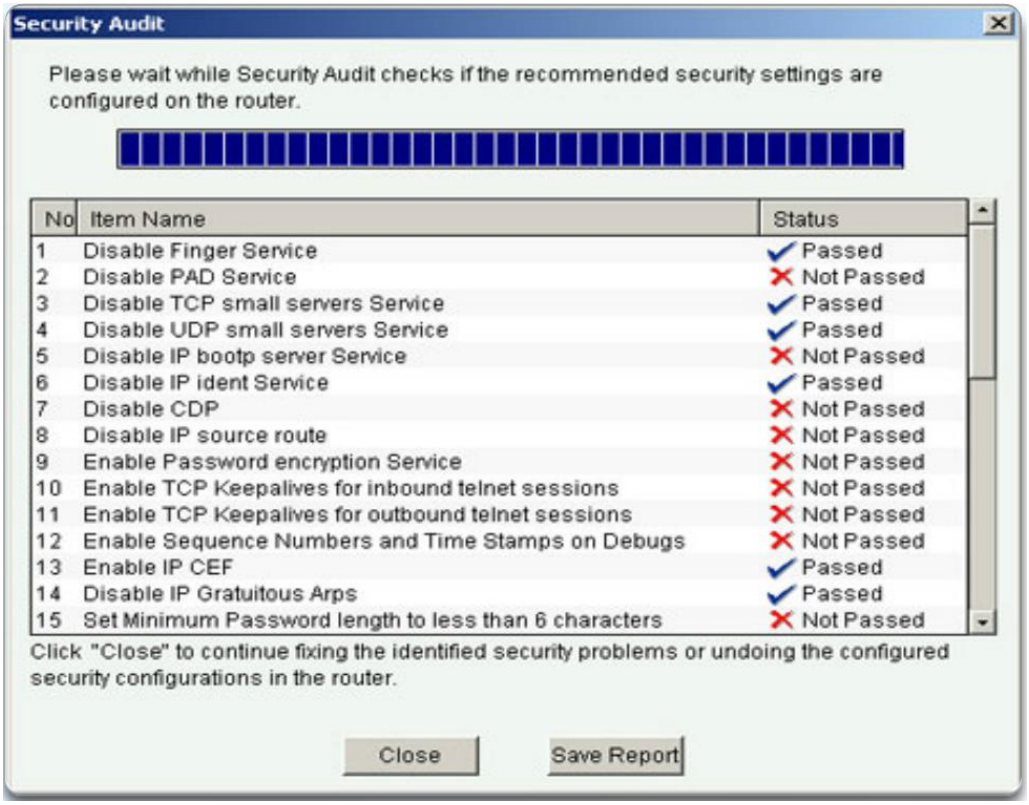
- Các báo cáo đưa ra cần cải thiện về giao diện để dễ quan sát hơn.
- Chưa có giao diện quản lý các luật (thêm, sửa, xóa) để điều chỉnh sao cho phù hợp với từng doanh nghiệp

- Mới chỉ thực hiện đánh giá được cấu hình trên thiết bị hãng Cisco

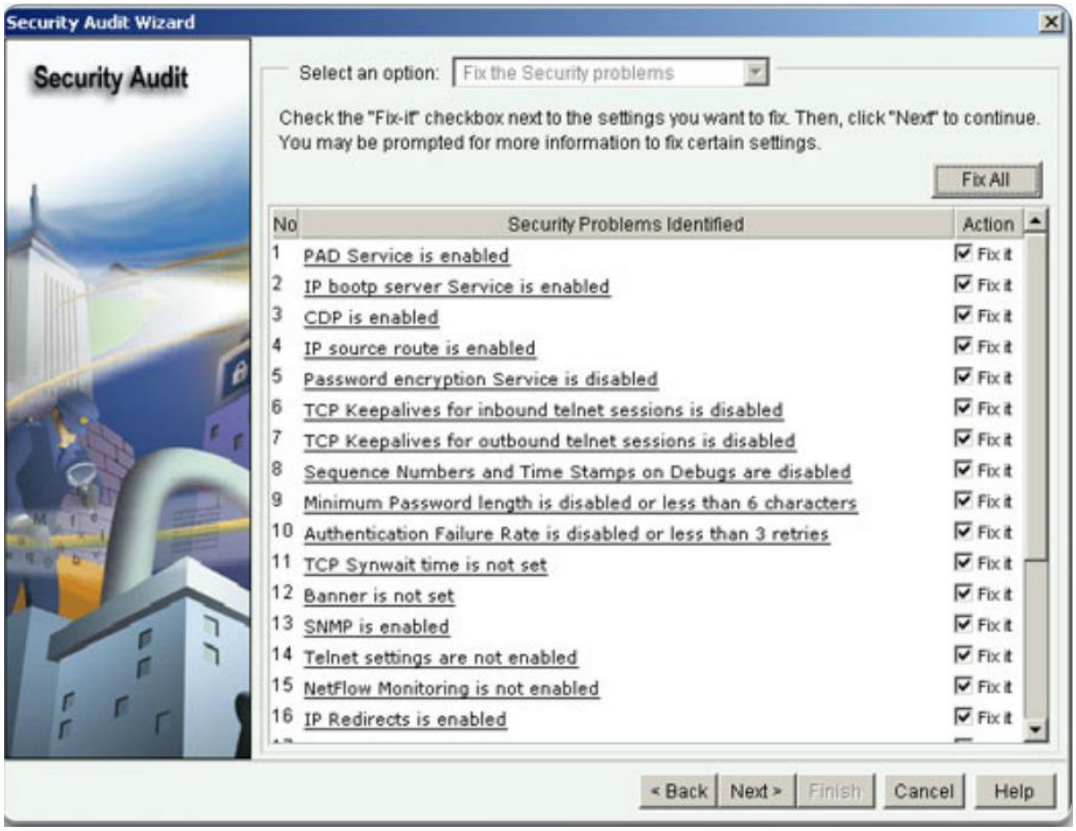
4.6.2 So sánh với một số chương trình đánh giá khác

Cisco Configuration Professional

Hiện nay hãng Cisco đưa ra chương trình Cisco Configuration Professional. Chương trình này mục tiêu chính là hỗ trợ quản trị viên cấu hình hệ thống mạng bằng giao diện web. Trong mục *Security Audit* cho phép quản trị viên so sánh cấu hình đang hoạt động trên một thiết bị mạng với cấu hình mẫu, từ đó đưa ra đánh giá.



Hình 4.8 Tính năng Security Audit trên ứng dụng CCP của Cisco



Hình 4.9 Báo cáo các lỗi cấu hình và cho phép tự động sửa lỗi

- *Ưu điểm:*

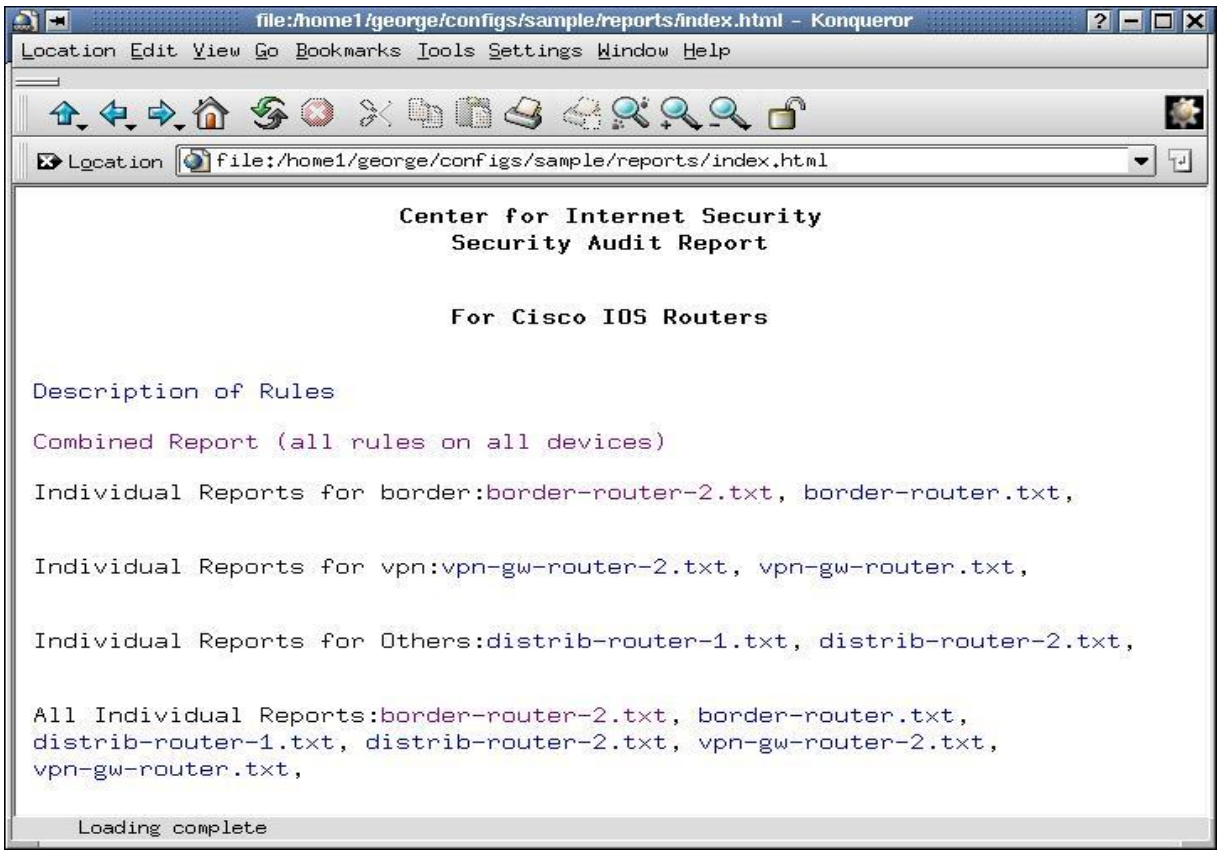
  - Giao diện thiết kế tốt, dễ sử dụng;
  - Tính năng tự động tìm kiếm lỗi cấu hình và sửa lỗi cấu hình hoạt động tốt.

- *Nhược điểm:*

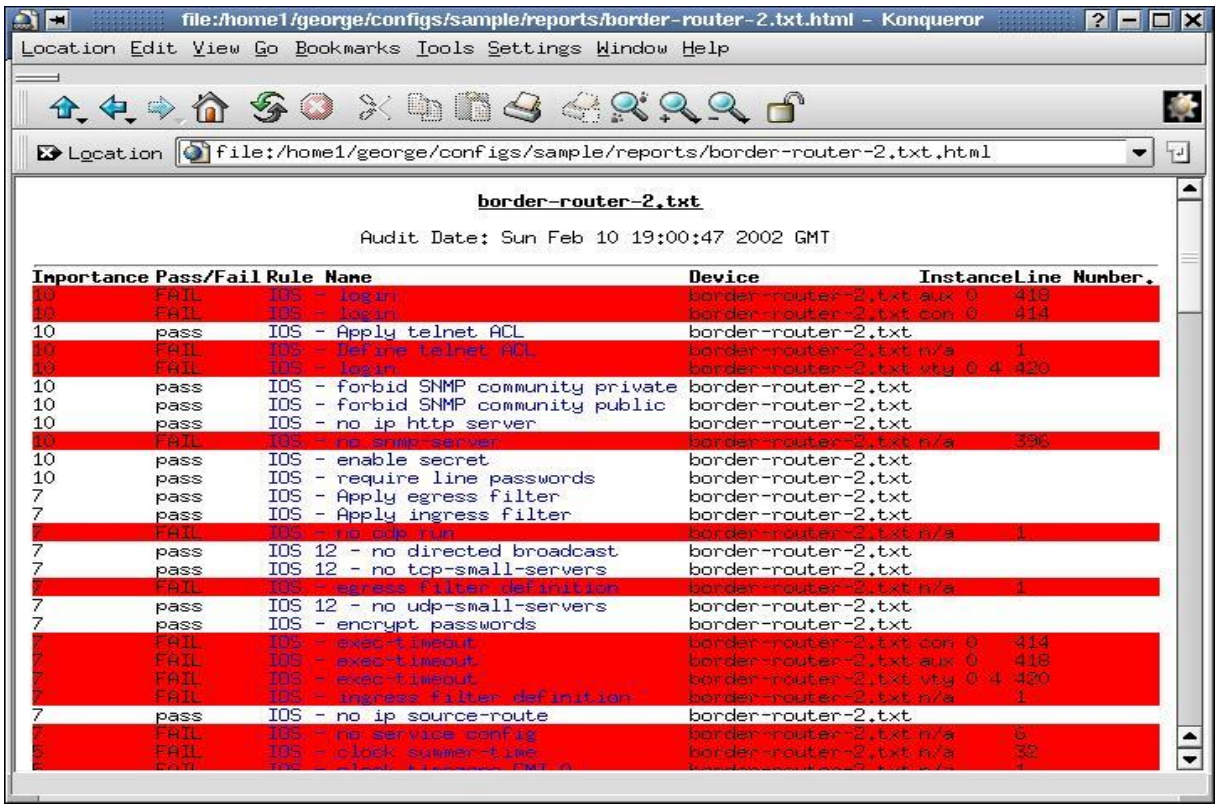
  - Chỉ cho phép đánh giá cấu hình và sửa lỗi cấu hình trên từng thiết bị.
  - Không cho phép sửa đổi quy định cấu hình

Router Audit Tool

Đây là một chương trình miễn phí, cho phép kiểm tra cấu hình trên các thiết bị mạng. Chương trình này có đầu vào là các file cấu hình, đầu ra là các báo cáo tổng hợp và các báo cáo chi tiết về các lỗi cấu hình.



Hình 4.10 Giao diện báo cáo tổng hợp



Hình 4.11 Báo cáo chi tiết lỗi cấu hình trên từng Router

- Ưu điểm:

- Gọn nhẹ, chạy chính xác.
- Các báo cáo đánh giá lỗi cấu hình rõ ràng và khoa học

- *Nhược điểm:*

- Chỉ đánh giá được cấu hình trên thiết bị Cisco
- Người dùng không thể tự thêm các quy định về cấu hình

Sau khi so sánh giữa cấu hình đang hoạt động và cấu hình mẫu, chúng ta sẽ biết được cấu hình trên các thiết bị có tuân thủ đúng với chính sách an ninh của doanh nghiệp/ tổ chức đặt ra hay không. Kết quả báo cáo có 2 trạng thái là "*Đạt"* hoặc "*Không đạt"*

Mẫu báo cáo đường an ninh cơ sở tùy thuộc vào từng tổ chức. Trong báo cáo này, cần có kết quả của 3 bài đo kiểm tra cấu hình an ninh. Cột *"Lý do"* để lưu lại những lý do tại sao không đạt yêu cầu về việc cấu hình. Đây là kết quả của buổi làm việc giữa Phòng vận hành và Phòng ATTT. Phòng vận hành có trách nhiệm giải trình tại sao những thuộc tính an ninh đó không được thực hiện; khi nào thì sẽ thực hiện.
Từ báo cáo trên, người quản trị mạng sẽ xem xét và thực hiện cấu hình lại những lỗi để đảm bảo cấu hình an ninh đang chạy tuân thủ theo chính sách an toàn bảo mật thông tin mà công ty đã đề ra.

CHƯƠNG 5. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

5.1 Tầm quan trọng của đề tài

Theo báo cáo Hiệp hội an toàn thông tin Việt Nam VNISA năm 2015, vấn đề quản lý lỗi cấu hình trên hệ thống mạng là một vấn đề khó khăn trong quá trình quản lý mạng máy tính của doanh nghiệp. Trên thế giới, vấn đề này được đánh giá là "bắt buộc phải làm" vì nếu không quản lý được cấu hình thì hệ thống mạng đó được coi là bỏ ngỏ đối với kẻ tấn công mạng[10]. Những hệ thống không được quản lý cấu hình còn được gọi là hệ thống quản lý tồi (mismanagement network). Và như đã phân tích thực trạng an ninh mạng Việt Nam năm 2015, các vụ khai thác lỗ hổng liên quan đến lỗi cấu hình mạng đã gây ra những vụ việc mất an toàn thông tin nghiêm trọng.

Từ nhu cầu thực tiễn trong việc quản lý cấu hình đã nêu ở trên, luận văn "*Xây dựng phương pháp thu thập và phân tích số liệu lỗi cấu hình của mạng máy tính"* tập trung vào việc phân tích và đánh giá xem cấu hình an ninh trên các thiết bị hạ tầng mạng của một tổ chức, doanh nghiệp có tuân thủ theo chính sách an ninh của tổ chức đó hay không. Để giải quyết vấn đề trên, luận văn khảo sát một mô hình mạng máy tính điển hình, được sử dụng phổ biến tại các doanh nghiệp. Tiếp đó luận văn liệt kê những lỗi cấu hình an ninh mà người quản trị mạng thường mắc phải trong khi cấu hình các thiết bị mạng; những lỗi cấu hình này sẽ tạo ra những điểm yếu gì; cách thức kẻ tấn công khai thác những điểm yếu này như thế nào; hậu quả xảy ra là gì.

Sau khi đã chỉ ra những điểm yếu nêu trên, luận văn đề xuất phương pháp thu thập số liệu cấu hình từ các thiết bị trên hệ thống mạng, đảm bảo tính đơn giản, thuận tiện, chính xác. Phương pháp thu thập cấu hình được đưa ra dựa trên giải pháp về quy trình, con người, kỹ thuật.

Sau khi đã thu thập được số liệu cấu hình luận văn đề xuất phương pháp đánh giá cấu hình để xem cấu hình đó có tuân thủ theo các khuyến nghị an ninh hay không. Luận văn đề xuất cách tiếp cận đánh giá theo Tiêu chuẩn đo lường an ninh TCVN 10542:2014 ISO/IEC 27004:2014. Tiêu chuẩn này cung cấp hướng dẫn về việc phát triển và sử dụng các số đo và bài đo để đánh giá hiệu lực của một hệ thống quản lý an toàn thông tin

---

[10] *https://forum.whitehat.vn/forum/thao-luan/tin-tuc/57141-hon-300-nghin-he-thong-mang-tai-viet-nam-dang-trong-tinh-trang----bo-ngo---*

Phương pháp chung là so sánh cấu hình đang hoạt động với mẫu cấu hình an ninh khuyến nghị. Nếu có sự khác biệt thì đánh dấu lại và cần có giải trình.

5.2 Những vấn đề đạt được:

- Phân tích được tầm quan trọng của việc quản lý cấu hình trong công tác đảm bảo an toàn cho hệ thống mạng máy tính của doanh nghiệp.
- Làm rõ được những lỗi cấu hình an ninh trên thiết bị mạng; những nguy cơ có thể xảy ra khi để tồn tại những lỗi này; cách cấu hình khắc phục lỗi.
- Đề xuất được phương pháp thu thập cấu hình tập trung. Phương pháp này đã được kiểm định trong thực tế làm việc của tác giả luận văn. Khi tuân thủ đúng phương pháp này thì việc thu thập cấu hình sẽ đạt được các yêu cầu ở Mục 3.1
- Đề xuất được phương pháp đánh giá lỗi cấu hình. Phương pháp đánh giá là so sánh cấu hình đang hoạt động với cấu hình khuyến nghị. Đây cũng là phương pháp mà các hãng thiết bị, các hãng phần mềm ứng dụng thường sử dụng khi muốn đánh giá lỗi cấu hình trên thiết bị mạng.
- Xây dựng chương trình đánh giá cấu lỗi cấu hình. Đầu vào của chương trình là một thư mục chứa các file cấu hình của các thiết bị mạng trong một hệ thống mạng. Đầu ra là kết quả báo cáo tổng hợp và chi tiết về tình trạng cấu hình an ninh của hệ thống mạng đó. Ưu điểm chính của chương trình so với các phần mềm khác là cho phép người đánh giá hiệu chỉnh các quy định về cấu hình an ninh, sao cho phù hợp với từng hệ thống mạng.

5.3 Những vấn đề còn tồn tại

- Luận văn mới chỉ đề cập đến mô hình mạng tại một địa điểm, chưa mở rộng việc khảo sát hệ thống mạng có nhiều chi nhánh.
- Thiết bị đề cập đến trong luận văn là của hãng Cisco. Thực tế ở Việt Nam hiện nay các doanh nghiệp sử dụng thiết bị của nhiều hãng, ví dụ Juniper v.v. Vì vậy cần xem xét đến đặc điểm cấu hình an ninh trên các thiết bị của các hãng khác nhau. Luận văn cũng mới đề cập đến các thiết bị cơ bản (Switch, Router, wireless router). Trong hệ thống mạng còn những thiết bị như Firewall, Server,…Vì vậy cần tiếp tục nghiên cứu những thiết bị này để đưa ra cấu hình an ninh phù hợp.

- Những lỗi cấu hình được chỉ ra trong luận văn là những lỗi cấu hình cơ bản, thường gặp. Còn nhiều các tham số cấu hình an ninh cần được bổ sung thêm để tăng cường tính an ninh cho thiết bị.

5.3 Hướng phát triển

- Tiếp tục tham khảo thêm những lỗi cấu hình an ninh được đề cập trong các tài liệu của hãng thiết bị, các khuyến nghị từ các tổ chức an ninh mạng, các tiêu chuẩn. Từ đó cập nhật thêm vào cơ sơ dữ liệu lỗi cấu hình trong luận văn.
- Mở rộng việc đánh giá lỗi cấu hình trên các thiết bị ở biên của mạng (Firewall, VPN gateway…). Cần nghiên cứu những yêu cầu về cấu hình an ninh cho những thiết bị này, từ đó bổ sung thêm một tầng kết nối mạng biên (Border network) cho mô hình mạng đã đề cập ở Chương 2. Đây là cách tiếp cận một mô hình mạng doanh nghiệp hoàn chỉnh hơn để đánh giá. Mô hình mạng hoàn chỉnh cần có thêm các kết nối với các chi nhánh, kết nối ra ngoài Internet. Hướng tới xây dựng một quy trình đánh giá lỗi cấu hình an ninh cho hệ thống mạng hoàn chỉnh; từ đó áp dụng vào các hệ thống mạng trong thực tế.
- Nghiên cứu thêm về cấu hình trên thiết bị hãng Juniper, được sử dụng khá phổ biến trong các doanh nghiệp vừa và lớn ở Việt Nam. Từ đó tích hợp vào chương trình ứng dụng để đánh giá các lỗi cấu hình an ninh trên các dòng thiết bị hãng này.

Để hoàn thiện luận văn này, tôi xin chân thành cám ơn sự chỉ bảo hướng dẫn nhiệt tình của TS Lê Đức Phong – giảng viên hướng dẫn và sự quan tâm chỉ bảo giúp đỡ của các thầy cô Trường ĐHCN-ĐHQGHN.

TÀI LIỆU THAM KHẢO

Tiếng Việt

1. PGS.TS Trịnh Nhật Tiến (2014), Giáo trình mật mã và an toàn dữ liệu, Đại học công nghệ, ĐHQGHN.
2. TS. Nguyễn Đại Thọ (2013), Bài giảng an toàn mạng, Đại học công nghệ, ĐHGHN.
3. Bộ khoa học công nghệ (2014), Tiêu chuẩn quốc gia TCVN 10542:2014, công nghệ thông tin - các kỹ thuật an toàn - quản lý an toàn thông tin - đo lường.
4. https://forum.whitehat.vn/forum/thao-luan/tin-tuc/57141-hon-300-nghin-he-thong-mang-tai-viet-nam-dang-trong-tinh-trang----bo-ngo---
5. http://antoanthongtin.vn/Detail.aspx?NewsID=29d680af-9286-4f19-9c40-4a32db7de523&CatID=e1999c9a-5eeb-418c-9ea8-ae4c5e850d0c
6. http://www.vncert.gov.vn/baiviet.php?id=1
7. http://vnreview.vn/tin-tuc-an-ninh-mang/-/view_content/content/1861042/thi-truong-cho-den-dang-rao-ban-hon-841-may-chu-viet-nam-bi-hack

Tiếng Anh

8. Jing Zhang, Zakir Durumeric, Michael Bailey, Mingyan Liu, Manish Karir (2014), On the mismanagement and maliciousness of networks.
9. Rostyslav Barabanov (2011), Information Security Metrics - State of the Art
10. Cisco CCNA Security 2.0 (2016), Cisco certified Network Association Security
11. “Hackers focus on misconfigured networks,” http://forums.cnet.com/7726-6132 102-3366976.html.
12. https://security.web.cern.ch/security/rules/en/baselines.shtml
13. https://en.wikipedia.org/wiki/Universal_Plug_and_Play#Problems_with_UPnP
14. https://tools.ietf.org/html/rfc2577
15. CompTIA Security+
16. https://en.wikipedia.org/wiki/File_Transfer_Protocol
17. http://k12linux.mesd.k12.or.us/cascadelink/text7.htm
18. http://www.cisco.com/c/dam/en/us/td/docs/solutions/CRD/Sep2015/WP-Enterprise-Security-Baseline-Sep15.pdf