MỤC LỤC

1. Tổng quan về an toàn thông tin[1]

1.1 Tại sao cần bảo đảm an toàn thông tin?

Ngày nay, sự xuất hiện Internet và mạng máy tính đã giúp cho việc trao đổi thông tin trở nên nhanh gọn, dễ dàng. E-mail cho phép người ta nhận hay gửi thư ngay trên máy tính của mình, E-business cho phép thực hiện các giao dịch buôn bán trên mạng, ...Tuy nhiên lại phát sinh những vấn đề mới. Thông tin quan trọng nằm ở kho dữ liệu hay đang trên đường truyền có thể bị trộm cắp, có thể bị làm sai lệch, có thể bị giả mạo. Điều đó có thể ảnh hưởng tới các tổ chức, các công ty hay cả một quốc gia. Những bí mật kinh doanh, tài chính là mục tiêu của các đối thủ cạnh tranh. Những tin tức về an ninh quốc gia là mục tiêu của các tổ chức tình báo trong và ngoài nước. Để giải quyết tình hình trên, vấn đề bảo đảm an toàn thông tin (ATTT) đã được đặt ra trong lý luận cũng như trong thực tiễn.

1.2 Mục tiêu của an toàn thông tin.

* Bảo đảm bí mật (Bảo mật): Thông tin không bị lộ đối với người không được phép.

* Bảo đảm toàn vẹn (Bảo toàn): Ngăn chặn hay hạn chế việc bổ sung, loại bỏ và sửa dữ liệu không được phép.

* Bảo đảm xác thực (Chứng thực): Xác thực đúng thực thể cần kết nối, giao dịch. Xác thực đúng thực thể có trách nhiệm về nội dung thông tin (Xác thực nguồn gốc thông tin.)

* Bảo đảm sẵn sàng: Thông tin sẵn sàng cho người dùng hợp pháp.

1.3 Các nội dung an toàn thông tin.

a). Nội dung chính:

* An toàn máy tính (Computer Security): là sự bảo vệ các thông tin cố định bên trong máy tính (Static Informations), là khoa học về bảo đảm an toàn thông tin trong máy tính.

* An toàn truyền tin (Communication Security): là sự bảo vệ thông tin trên đường truyền tin (Dynamic Informations). (Thông tin đang được truyền từ hệ thống này sang hệ thống khác). Là khoa học về bảo đảm an toàn thông tin trên đường truyền tin.

b). Nội dung chuyên ngành (Nội dung hệ quả từ nội dung chính):

Để bảo vệ thông tin bên trong máy tính hay đang trên đường truyền tin, phải nghiên cứu các nội dung chuyên ngành sau:

+ An toàn Dữ liệu (Data Security).

+ An toàn Cơ sở dữ liệu (CSDL) (Data base Security).

+ An toàn Hệ điều hành (Operation system Security).

+ An toàn mạng máy tính (Network Security).

---

[1] *PGS.TS Trịnh Nhật Tiến - Giáo trình mật mã và an toàn dữ liệu, ĐHCN, ĐHQGHN*

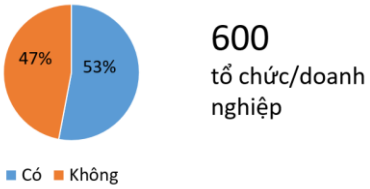
2. Phân tích tình hình an toàn thông tin tại Việt Nam năm 2015

2.1 Các chỉ số an toàn thông tin

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.

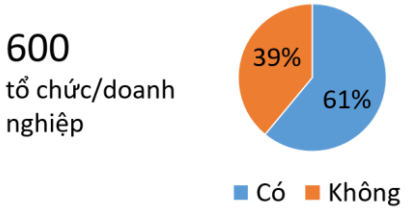
Một vài thống kê đáng lưu tâm trong báo cáo trên:

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



Hình 1.1 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 1.2 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.

→ Làm thế nào để quản lý được ***cấu hình mạng.***

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

Theo thống kê của VNCERT 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)*

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.

2.3 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).*
- 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*.

→ 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

2.4. Tầm quan trọng của việc quản lý cấu hình.

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.[2]

Năm 2012, tạp chí an toàn thông tin 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.[3]

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.*

---

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

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

3. Vấn đề quản lý cấu hình thiết bị mạng doanh nghiệp

3.1 Mục tiêu và phạm vi nghiên cứu

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 toàn bảo mật thông tin* của tổ chức đó hay không.

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).

Đầu tiên, luận văn khảo sát một mô hình mạng máy tính điển hình, được sử dụng phổ biến tại các doanh nghiệp. Sau đó luận văn chỉ ra những cấu hình an ninh trên thiết bị là gì; tại sao phải thực hiện những cấu hình đó; những hậu quả có thể xảy ra nếu không thực hiện, hoặc thực hiện sai các cấu hình an ninh cho thiết bị (lỗi cấu hình) ; cách khắc phục từng lỗi cấu hình như thế nào?

Tiếp theo luận văn đề xuất phương pháp thu thập file cấu hình của các thiết bị. Sau khi đã thu thập các file cấu hình, luận văn đề xuất phương pháp phân tích so sánh những cấu hình thu thập được với cấu hình được khuyến nghị trong chính sách an toàn bảo mật thông tin của tổ chức. Sau bước so sánh này, kết quả thu được là một báo cáo đánh giá về những lỗi cấu hình an ninh trên các thiết bị hạ tầng mạng. Dựa trên cáo cáo này người quản trị viên hệ thống sẽ tiến hành những biện pháp khắc phục những lỗi cấu hình đó.

Cuối cùng là những vấn đề đã thực hiện được và những vấn đề tồn tại của luận văn, hướng nghiên cứu mở rộng tiếp theo.

3.2 Khái niệm lỗi cấu hình an ninh

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…

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.

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

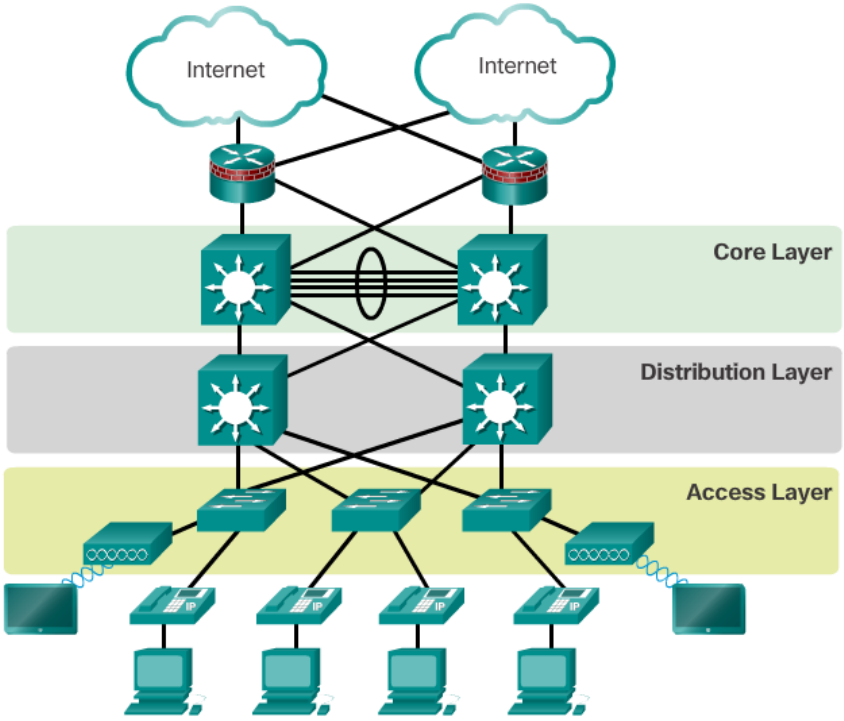
Đường cơ sở an ninh là một danh sách kiểm tra (checklist) mà theo đó các hệ thống được đánh giá và kiểm toán đối với tình hình an ninh trong một tổ chức. Đường cơ sở phác thảo ra những yếu tố an ninh chính đối với một hệ thống, và trở thành điểm xuất phát cho việc bảo vệ hệ thống đó.[4]

3.4 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 toàn bảo mật thông tin của tổ chức.

3.5 Khảo sát một mạng máy tính điển hình trong doanh nghiệp.



Hình 3.2. 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.
- *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.

[4] *Theo giáo trình CompTIA Security+*

- *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.

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

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

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. TEL NET không mã hóa thông tin nên có thể bị lộ mật khẩu	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. HTTP không mã hóa thông tin nên có thể bị xem trộm	Sử dụng giao thức HTTPS để truy cập vào thiết bị để quản lý
3	mnt-TFTP	Sử dụng giao thức truyền file đơn giản TFTP	Sử dụng SCP (Secure Copy Protocol) hoặc FTPS (FTP Secure)
4	mnt-int-ACL-BLK	Không ngăn chặn các máy tính người dùng truy cập tới giao diện quản lý thiết bị	Sử dụng kỹ thuật điều khiển truy cập.
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-PassENCRYPT	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 3.2. Những lỗi cấu hình an ninh trong quản lý thiết bị

Bảng dưới đây mô tả một mẫu cấu hình an ninh tiêu chuẩn cho việc quản lý thiết bị

STT	Mã số	Cấu hình trên thiết bị	Cấu hình khuyến nghị
1	mnt-TELNET	*line vty 0 15* *password [string]* *login*	*line vty 0 15* *transport input ssh*
2	mnt-HTTP	*ip http server*	*no ip http server* *ip http secure-server*
3	mnt-FTPTFTP	N/A	*Ip ftp server*
4	mnt-int-ACL-BLK	n/a	*Access-list*
5	mnt-SNMP	N/A	*username - password/secret*
6	mnt-PasswordLocal	N/A	*AAA new-model* *AAA authentication* *AAA authorize* *AAA accounting*
7	mnt-PasswordENCRYPT		*Service-password encryption*
8	mnt-NTP	N/A	*Ntp server [IP]*
9	mnt-SYSLOG	N/A	*Logging [IP]*

Bảng 3.3. Cấu hình lỗi và cấu hình khuyến nghị

3.6.2 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).

3.6.2.1 Lỗi cấu hình trên thiết bị switch lớp 2

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 3.4. Lỗi cấu hình an ninh trên swich và khuyến nghị

3.6.2.2 Lỗi cấu hình trên thiết bị định tuyến không dây

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

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

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 3.6. Lỗi cấu hình tầng phân phối

4. Phương pháp thu thập cấu hình từ các thiết bị mạng

4.1 Yêu cầu của việc thu thập số liệu cấu hình

- 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;
- 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)
- Bảo đảm các file cấu hình không bị lỗi khi thu thập.
- Phân biệt được các file cấu hình từ các thiết bị khác nhau

4.2 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, nhân viên phòng an toàn thông tin.

- *Quy trình:* sau khi nhận được yêu cầu từ phòng an toàn thông tin, 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.

- *Phần cứng:* phòng vận hành phải trang bị một máy chủ (server) lưu trữ tập trung cấu hình.

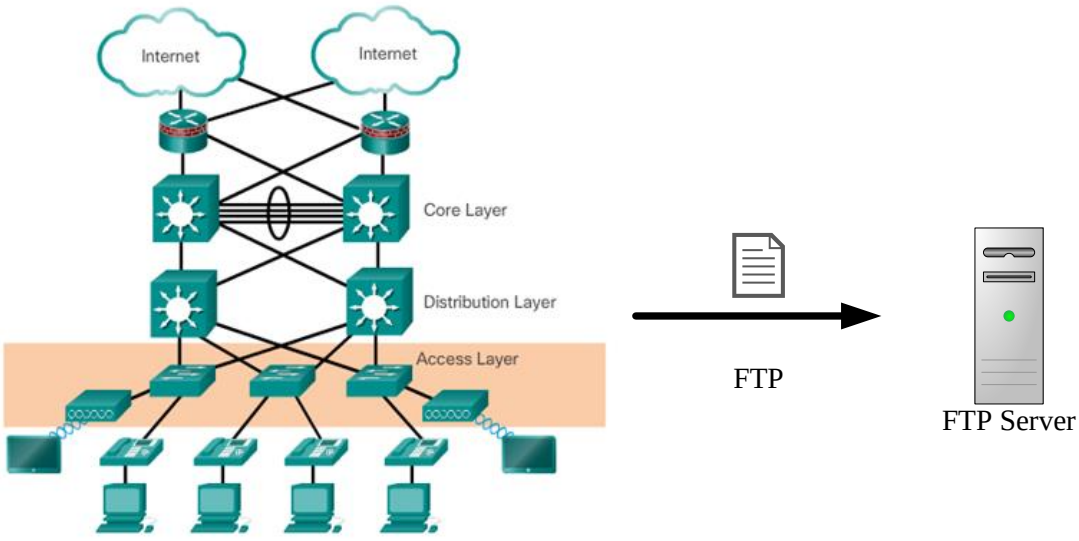
- *Phần mềm*:

+ Hệ điều hành cho Server có thể là Windows hoặc Linux.

+ Phần mềm 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.

4.2 Cách copy cấu hình về máy chủ



Hình 4.1. Phương pháp thu thập cấu hình

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. Các bước copy file cấu hình từ thiết bị lên máy chủ. Lưu ý quý tắc đặt tên file

4.2.1 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]

4.2.2 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.

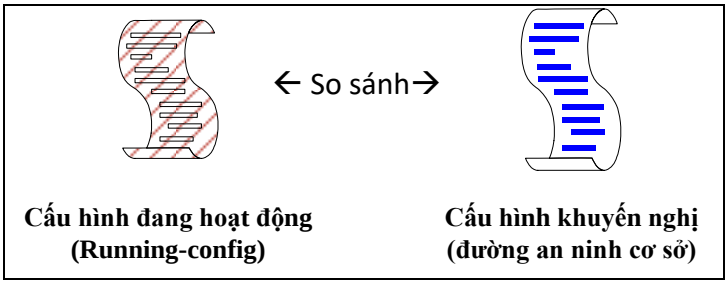
4.3. Kiểm tra các file cấu hình thu thập được

Sau khi copy cần kiểm tra lại số lượng file đã copy lên máy chủ FTP Server đã đầy đủ và chính xác hay chưa. Phương pháp kiểm tra về: số lượng file, tên file, nội dung file

5. Phương pháp đánh giá cấu hình an ninh trên thiết bị mạng

5.1 Phương pháp chung để đánh giá cấu hình an ninh

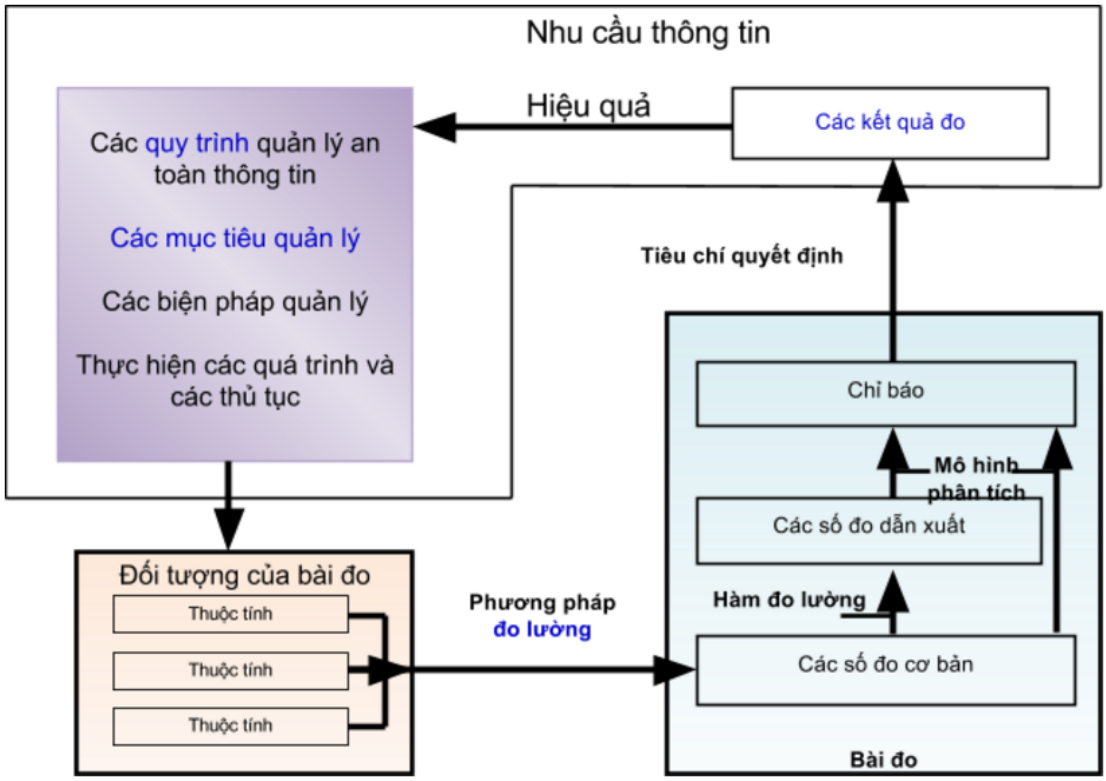
Để thực hiện đánh giá cấu hình an ninh trên thiết bị mạng có tuân thủ theo chính sách an toàn bảo mật thông tin hay không, thì cần so sánh cấu hình hiện tại đang hoạt động với cấu hình an ninh khuyến nghị (đường cơ sở an ninh).



Hình. Phương pháp đánh giá cấu hình an ninh

5.2 Tiêu chuẩn đo lường an ninh TCVN 10542:2014

Mô hình đo lường an toàn thông tin 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.



Trong đó:

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.

5.3 Đánh giá lỗi cấu hình quản lý

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 toàn bảo mật thông tin 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 An toàn thông tin và Phòng vận hành. • Phòng vận hành: thu thập cấu hình. • Phòng An toàn thông tin: 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-TFTP 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 An toàn thông tin
Người xem xét kết quả đo	Trưởng phòng An toàn thông tin; Người phụ trách về CNTT trong doanh nghiệp.
Người sở hữu thông tin	Phòng An toàn thông tin
Bộ phận thu thập thông tin	Phòng vận hành
Bộ phận trao đổi thông tin	Phòng vận hành; Phòng An toàn thông tin
Tần suất thực hiện	
Tần suất thu thập dữ liệu	Tùy theo chính sách an toàn bảo mật thông tin của tổ chức.
Tần suất phân tích dữ liệu	Tùy theo chính sách an toàn bảo mật thông tin của tổ chức.

5.4 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 toàn bảo mật thông tin 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 toàn bảo mật thông tin hay không, để từ đó có biện pháp khắc phục.
Biện pháp quản lý (1)	Có sự tham gia của Phòng An toàn thông tin và Phòng vận hành. • Phòng vận hành: thu thập cấu hình. • Phòng An toàn thông tin: 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**
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 An toàn thông tin

Người xem xét kết quả đo	Trưởng phòng An toàn thông tin; Người phụ trách về CNTT trong doanh nghiệp.
Người sở hữu thông tin	Phòng An toàn thông tin
Bộ phận thu thập thông tin	Phòng vận hành
Bộ phận trao đổi thông tin	Phòng vận hành; Phòng An toàn thông tin
Tần suất thực hiện	
Tần suất thu thập dữ liệu	Tùy theo chính sách an toàn bảo mật thông tin của tổ chức.
Tần suất phân tích dữ liệu	Tùy theo chính sách an toàn bảo mật thông tin của tổ chức.

5.5 Đánh giá lỗi cấu hình thiết bị tầng phân phối và tầng lõi

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 toàn bảo mật thông tin 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 toàn bảo mật thông tin hay không, để từ đó có biện pháp khắc phục.
Biện pháp quản lý (1)	Có sự tham gia của Phòng An toàn thông tin và Phòng vận hành. • Phòng vận hành: thu thập cấu hình. • Phòng An toàn thông tin: 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**
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

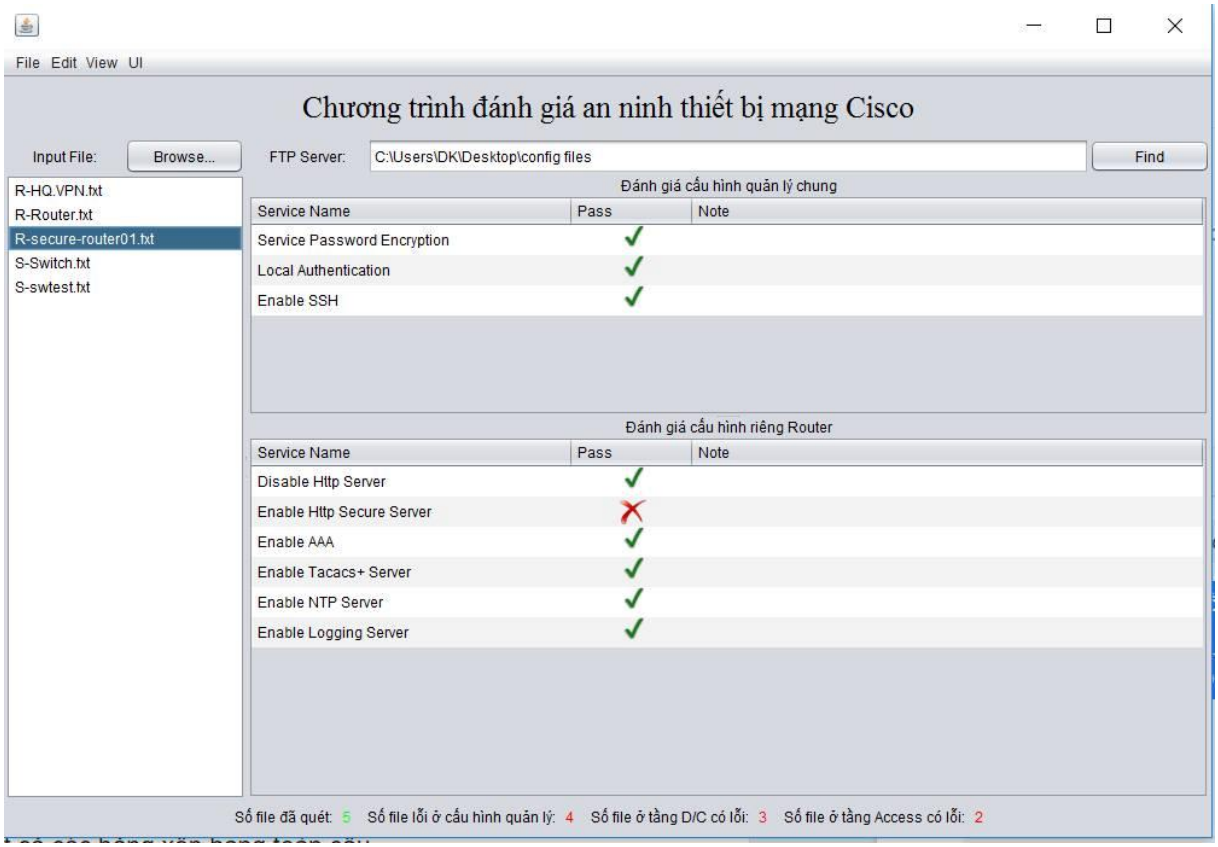
	- *Không:* là không thực hiện cấu hình tham số quản lý thiết bị
Loại thang giá trị	
Đơn vị đo	
Thông tin đặc tả về số đo dẫn xuất	
Số đo dẫn xuất	
Hàm đo lường	
Thông tin đặc tả về chỉ báo	
Chỉ báo	Có/Không
Mô hình phân tích	
Thông tin đặc tả về tiêu chí quyết định	
Tiêu chí quyết định	Theo thang giá 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 An toàn thông tin
Người xem xét kết quả đo	Trưởng phòng An toàn thông tin; Người phụ trách về CNTT trong doanh nghiệp.
Người sở hữu thông tin	Phòng An toàn thông tin
Bộ phận thu thập thông tin	Phòng vận hành
Bộ phận trao đổi thông tin	Phòng vận hành; Phòng An toàn thông tin
Tần suất thực hiện	
Tần suất thu thập dữ liệu	Tùy theo chính sách an toàn bảo mật thông tin của tổ chức.
Tần suất phân tích dữ liệu	Tùy theo chính sách an toàn bảo mật thông tin của tổ chức.

5.5 Xuất báo cáo đường cơ sở an ninh

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"*

Luận văn có xây dựng công cụ đánh giá cấu hình an ninh. Ưu điểm của công cụ này so với các công cụ của Cisco đó là:

- *Có thể đánh giá cấu hình an ninh của nhiều thiết bị*
- *Xuất báo cáo tổng hợp phân tích tình trạng cấu hình an ninh của toàn bộ mạng*



5.6 Những vấn đề đạt được của luận văn và những tồn tại

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
- Đề xuất được phương pháp đánh giá lỗi cấu hình.
- Xây dựng chương trình đánh giá cấu lỗi cấu hình

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 xem xét thêm để tăng cường tính an ninh cho thiết bị.

Những tồn tại của luận văn cũng chính là những vấn đề mà luận văn cần nghiên cứu phát triển thêm để hoàn thiện.

6. Kết luận

Luận văn "*Xây dựng phương pháp thu thập và đánh giá 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 toàn bảo mật thông tin 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 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.

Để hoàn thiện luận văn này, tôi xin chân thành cám ơn sự chỉ bảo hướng dẫn nhiệt tình của giảng viên hướng dẫn là TS Lê Đức Phong , 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. “Hackers focus on misconfigured networks,” http://forums.cnet.com/7726-6132 102-3366976.html.
10. https://security.web.cern.ch/security/rules/en/baselines.shtml
11. https://en.wikipedia.org/wiki/Universal_Plug_and_Play#Problems_with_UPnP
12. https://tools.ietf.org/html/rfc2577
13. CompTIA Security+
14. https://en.wikipedia.org/wiki/File_Transfer_Protocol
15. http://k12linux.mesd.k12.or.us/cascadelink/text7.htm
16. http://www.cisco.com/c/dam/en/us/td/docs/solutions/CRD/Sep2015/WP-Enterprise-Security-Baseline-Sep15.pdf