STT	Người ký	Đơn vị	Thời gian ký	Ý kiến
1	Vĩnh Tuấn Bảo	Phó Tổng Giám đốc - Tổng công ty Viễn thông MobiFone	20/09/2024 11:18:12	-
2	Nguyễn Thái Hà	Phó Ban - Ban Công nghệ	20/09/2024 05:53:28	-
3	Lê Công Trung	Trưởng BU - BU An ninh mạng	19/09/2024 09:59:18	Kính trình anh ạ

TỔNG CÔNG TY VIỄN THÔNG MOBIFONE	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 1470/QĐ-MOBIFONE	*Hà Nội, ngày 20 tháng 9 năm 2024*

QUYẾT ĐỊNH

Về việc ban hành Bộ tiêu chuẩn đảm bảo an toàn bảo mật cho các hệ thống

TỔNG GIÁM ĐỐC TỔNG CÔNG TY VIỄN THÔNG MOBIFONE

Căn cứ Quyết định số 1798/QĐ-BTTTT ngay 01/12/2014 của Bộ trưởng Bộ Thông tin và Truyền thông về việc thành lập Tổng công ty Viễn thông MobiFone trên cơ sở tổ chức lại Công ty TNHH một thành viên Thông tin di động;

Căn cứ Quyết định số 45/QĐ-UBQLV ngày 22/02/2021 của Chủ tịch Ủy ban Quản lý vốn nhà nước tại Doanh nghiệp về việc Ban hành Điều lệ tổ chức và hoạt động của Tổng công ty Viễn thông MobiFone;

Căn cứ Quyết định số 595/QĐ-MOBIFONE ngày 29/3/2024 của Tổng công ty Viễn thông MobiFone về việc ban hành Quy định điều hành An ninh thông tin, Ứng cứu An ninh mạng (lần 2);

Căn cứ Quyết định số 1038/QĐ-MOBIFONE ngày 20/6/2024 của Tổng công ty Viễn thông MobiFone về việc ban hành Quy chế an toàn thông tin phục vụ sản xuất kinh doanh;

Xét đề nghị của Trưởng Ban Công nghệ và Trưởng Businesss Unit An ninh mạng tại Tờ trình số 52/TTr-CN-BUANM ngày 13/9/2024 của Ban Công nghệ và Businesss Unit An ninh mạng về việc phê duyệt chủ trương phát hành Bộ tiêu chuẩn đảm bảo an toàn bảo mật cho các hệ thống.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "**Bộ tiêu chuẩn đảm bảo an toàn bảo mật cho các hệ thống**".

Điều 2. Quyết định này có hiệu lực kể từ ngày ký cho đến khi cấp thẩm quyền có quyết định khác thay thế, bổ sung.

Điều 3. Trưởng các Ban, Văn phòng, BU thuộc khối cơ quan Tổng công ty, Giám đốc các đơn vị trực thuộc chịu trách nhiệm thi hành quyết định này./.

Nơi nhận:
- Như điều 3;
- HĐTV (để b/c);
- Ban kiểm soát (để b/c);
- Tổng giám đốc (để b/c);
- Các Phó TGĐ;
- Lưu: VT, CN, BUANM.

KT.TỔNG GIÁM ĐỐC
PHÓ TỔNG GIÁM ĐỐC

TỔNG CÔNG TY VIỄN THÔNG MOBIFONE

Vinh Tuấn Bảo

TỔNG CÔNG TY VIỄN THÔNG MOBIFONE

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

BỘ TIÊU CHUẨN ĐẢM BẢO AN TOÀN BẢO MẬT CHO CÁC HỆ THỐNG

(Kèm theo Quyết định số 1470/QĐ-MOBIFONE ngày 20 tháng 9 năm 2024 của Tổng công ty Viễn thông MobiFone)

CHƯƠNG I. CƠ SỞ XÂY DỰNG TIÊU CHUẨN ĐÁNH GIÁ

Điều 1. Mục đích

Việc xây dựng Bộ tiêu chuẩn đảm bảo an toàn bảo mật cho các hệ thống của MobiFone là vô cùng cần thiết, nhằm đảm bảo các hoạt động liên quan đến cài đặt và cấu hình hệ điều hành máy chủ luôn tuân thủ các tiêu chuẩn an toàn cao nhất. Bộ tiêu chuẩn này không chỉ là nền tảng để tham chiếu trong quá trình đưa hệ thống vào vận hành và khai thác, mà còn là cơ sở kỹ thuật quan trọng cho việc đánh giá mức độ an toàn và an ninh của các hệ điều hành máy chủ. Điều này giúp đảm bảo hệ thống của MobiFone hoạt động ổn định, bảo mật và tuân thủ các quy định bảo mật thông tin nghiêm ngặt. Dưới đây là một số lý do chính tại sao cần phải xây dựng Bộ tiêu chuẩn đảm bảo an toàn bảo mật cho các hệ thống:

- **Bảo vệ Thông tin Quan trọng**: Thông tin quan trọng của một tổ chức, bao gồm dữ liệu khách hàng, thông tin tài chính và công nghệ, cần phải được bảo vệ khỏi các mối đe dọa như trộm cắp dữ liệu, tấn công mạng và lừa đảo.

- **Mối đe dọa từ các hacker**: kẻ tấn công mạng và các nhóm tội phạm mạng ngày càng phổ biến. Xây dựng Bộ tiêu chuẩn đảm bảo an toàn bảo mật cho các hệ thống giúp ngăn chặn các cuộc tấn công và hạn chế việc bị xâm nhập hệ thống.

- **Tăng cường độ tin cậy**: Một hệ thống mạng an toàn và bảo mật giúp tăng cường hiệu suất hoạt động của tổ chức bằng cách ngăn chặn các sự cố an ninh mạng và giữ cho hệ thống hoạt động một cách liên tục và ổn định.

- **Hỗ trợ trong việc đánh giá và kiểm tra hệ thống**: Bộ tiêu chuẩn cung cấp các tiêu chuẩn rõ ràng để đánh giá và kiểm tra mức độ an toàn của các hệ thống hiện tại. Điều này giúp MobiFone có thể liên tục giám sát, đánh giá và cải thiện hệ thống của mình theo các tiêu chuẩn an ninh mới nhất.

- **Đảm bảo tính nhất quán trong triển khai và vận hành**: Khi các quy trình bảo mật được tiêu chuẩn hóa, mọi bộ phận và nhân viên trong tổ chức sẽ tuân thủ các tiêu chuẩn này một cách nhất quán. Điều này giảm thiểu sự khác biệt trong cách tiếp cận bảo

mật và đảm bảo rằng tất cả các bộ phận của MobiFone đều hoạt động theo cùng một tiêu chuẩn cao.

Điều 2. Các văn bản liên quan

- Quyết định số 1798/QĐ-BTTTT ngay 01/12/2014 của Bộ trưởng Bộ Thông tin và Truyền thông về việc thành lập Tổng công ty Viễn thông MobiFone trên cơ sở tổ chức lại Công ty TNHH một thành viên Thông tin di động;

- Quyết định số 45/QĐ-UBQLV ngày 22/02/2021 của Chủ tịch Ủy ban Quản lý vốn nhà nước tại Doanh nghiệp về việc Ban hành Điều lệ tổ chức và hoạt động của Tổng công ty Viễn thông MobiFone;

- Quyết định số 595/QĐ-MOBIFONE ngày 29/3/2024 của Tổng công ty Viễn thông MobiFone về việc ban hành Quy định điều hành An ninh thông tin, Ứng cứu An ninh mạng (lần 2);

- Quyết định số 1038/QĐ-MOBIFONE ngày 20/6/2024 của Tổng công ty Viễn thông MobiFone về việc ban hành Quy chế an toàn thông tin phục vụ sản xuất kinh doanh;

- Tờ trình số 52/TTr-BUANM ngày 13/9/2024 của Businesss Unit An ninh mạng về việc phê duyệt chủ trương phát hành Bộ tiêu chuẩn đảm bảo an toàn bảo mật cho các hệ thống;

Điều 3. Phạm vi, đối tượng áp dụng

- Phạm vi Bộ tiêu chuẩn đảm bảo an toàn bảo mật cho các hệ thống áp dụng cho các đối tượng

- Đối tượng bắt buộc: Áp dụng cho tất cả các hệ thống từ cấp độ 2 trở lên.
- Đối tượng khuyến nghị: Áp dụng cho tất cả các hệ thống.

- Bộ tiêu chuẩn đảm bảo an toàn bảo mật cho các hệ thống áp dụng đối với các Ban, BU, Phòng thuộc khối cơ quan Tổng công ty, các đơn vị trực thuộc Tổng công ty.

Điều 4. Nội dung

Bộ tiêu chuẩn đảm bảo an toàn bảo mật cho các hệ thống bao gồm các nội dung như sau:

- Chương I: Cơ sở xây dựng tiêu chuẩn đánh giá

- Chương II: Tiêu chuẩn an toàn bảo mật cho các hệ thống

- Phụ lục I: Tài liệu tham khảo hướng dẫn Bộ tiêu chuẩn đảm bảo an toàn bảo mật cho các hệ thống bao gồm:

- Hướng dẫn đảm bảo an toàn bảo mật trong vận hành hệ thống;
- Hướng dẫn đảm bảo an toàn bảo mật cho hệ điều hành Linux;
- Hướng dẫn đảm bảo an toàn bảo mật cho hệ điều hành Windows Server;
- Hướng dẫn đảm bảo an toàn bảo mật cho các thiết bị mạng.

Điều 5. Triển khai

Các đơn vị trực thuộc Tổng công ty Viễn thông MobiFone thực hiện triển khai các nội dung bao gồm:

- Triển khai cho tất cả các hệ thống từ cấp độ 2 (Khuyến nghị áp dụng cho tất cả các hệ thống).

- Triển khai, cấu hình máy chủ theo các yêu cầu về an toàn trong Bộ tiêu chuẩn đảm bảo an toàn bảo mật trước khi đưa vào sử dụng. Kiểm tra cấu hình máy chủ an toàn trước khi vận hành theo các yêu cầu an toàn trước khi đưa máy chủ vào sử dụng.

- Lập kế hoạch, thực hiện rà soát các máy chủ đang vận hành sử dụng do đơn vị quản lý đảm bảo tuân thủ các tiêu chuẩn đảm bảo an toàn.

- Chủ động thực hiện kiểm tra, đánh giá định kỳ cấu hình các thiết bị của các hệ thống theo các nội dung của bộ tiêu chuẩn.

- Sử dụng bộ tiêu chuẩn trong công tác đánh giá phát hiện điểm yếu bảo mật của hệ thống thông tin, công tác đánh giá thẩm định mức độ an toàn của hệ thống thông tin. Mỗi tiêu chuẩn không được đáp ứng cần được xử lý khắc phục như một điểm yếu bảo mật của hệ thống thông tin.

Điều 6. Hiệu lực thi hành và sửa đổi, bổ sung

Quy định này có hiệu lực kể từ ngày ký quyết định ban hành. Trong quá trình thực hiện, nếu có những điều chưa phù hợp hoặc có những vấn đề phát sinh, các đơn vị gửi ý kiến bằng văn bản về Ban Công nghệ và BU ANM Tổng Công ty để tổng hợp trình Tổng Giám đốc xem xét, quyết định sửa đổi, bổ sung.

CHƯƠNG II. TIÊU CHUẨN ĐẢM BẢO AN TOÀN BẢO MẬT CHO CÁC HỆ THỐNG

Điều 7. Tiêu chuẩn mô hình quản trị hệ thống

1. Mục đích

Tài liệu này mô tả các yêu cầu cần thiết để thiết lập an toàn cho các hệ thống với mục đích:

- Làm cơ sở tham chiếu khi trong khi đưa hệ thống vào vận hành khai thác;

- Làm cơ sở kỹ thuật cho công tác đánh giá an toàn bảo mật cho các hệ thống.

- Áp dụng trong công tác quản lý vận hành: hệ thống, ứng dụng, database.

Tài liệu được xây dựng với giả định rằng hệ thống hoạt động đầy đủ dịch vụ được cung cấp và được thực hiện dưới tư cách là quản trị viên (root).

Tài liệu được xây dựng dựa trên các bộ tiêu chuẩn thiết lập tham chiếu đến các tiêu chuẩn ATTT (TCVN, CIS,…), được chỉnh sửa cho phù hợp với tình hình của MobiFone, pháp luật và các yêu cầu an toàn bảo mật an toàn thông tin trong nước.

** Trường hợp khai thác dữ liệu database đặc thù (theo yêu cầu cần kết nối với Database trực tiếp qua port 1521) cần thực hiện truy cập qua Jump Server và gia cố hệ thống theo Phụ lục 04 "Tiêu chuẩn cấu hình đảm bảo an ninh cho Database", với các đơn vị không có Jump Server thì thực hiện truy cập qua VPN để kết nối tới Database.*

2. Tiêu chuẩn mô hình quản trị hệ thống

Để đảm bảo việc giám sát truy cập từ xa tập trung cung cấp cho các quản trị viên phương thức truy cập, quản trị hệ thống tập trung, đảm bảo an toàn thông tin thì tất cả các hệ thống MobiFone trong quy định cần thực hiện truy cập qua các hệ thống giám sát truy cập từ xa tập trung:

- Tiêu chuẩn mô hình quản trị hệ thống 1 :

  - Kết nối truy cập đến Database và quản trị ứng dụng: Client → Shell Control Box (SCB)/Cyber Ark → Jump Server → Database
  - Kết nối truy cập đến Database khi không có máy chủ Jump Server: Client → Internet → VPN System → Database

- Tiêu chuẩn mô hình quản trị hệ thống 2 :

- Kết nối truy cập đến Server qua Shell Control Box (SCB): Client →Shell Control Box (SCB) → Jump Server → Server.
- Kết nối truy cập đến Server qua Cyber Ark: Client →Cyber Ark → Server.

STT	Tiêu chuẩn	Mô tả
1	**Tích hợp giám sát log qua hệ thống giám sát tập trung Siem**	
1.1	Cấu hình rsyslog	Mục đích lấy log hệ thống đẩy sang hệ thống SIEM
1.2	Cấu hình đẩy command log sang SIEM	Mục đích đẩy log thực thi trong hệ thống sang hệ thống SIEM
1.3	Cấu hình đẩy acccess_log sang SIEM	Mục đích đẩy log truy cập trong hệ thống sang hệ thống SIEM
1.4	Cấu hình đẩy Audit_log sang SIEM	Mục đích đẩy log các sự kiện, hoạt động được thực thi trên hệ thống sang SIEM
2	**Thực hiện kết nối qua hệ thống giám sát truy cập từ xa CyberArk / SCB**	
3	**Thực hiện kết nối qua hệ thống Jump Server**	
3.1	Hệ điều hành Windows server mới nhất, có update bản vá	Khắc phục các lỗ hổng bảo mật qua các bản vá mới của Windows server
3.2	Cài đặt phần mềm Antivirus	Phòng chống Virus và các phần mềm độc hại
3.3	Không join domain	Cách ly với các hệ thống khác
3.4	Không kết nối Internet	Cách ly với mạng Internet
3.5	Cài đặt giám sát SIEM (Enable sysmon, audit log,…)	Mục đích để giám sát log qua hệ thống SIEM
3.6	Bật Firewall mềm, chặn any/any, chỉ mở port 3389 và các port cần thiết (đặc biệt chặn các port 445, 135)	Chặn các port có nguy cơ bị tấn công
3.7	Cài đặt xác thực MFA	Tăng cường bảo mật cho máy chủ JumpServer
3.8	Đổi mật khẩu định kỳ theo quy chế ATTT	Tăng cường bảo mật cho máy chủ JumpServer

Điều 8. Tiêu chuẩn đảm bảo an toàn bảo mật hệ điều hành Linux

1. Mục đích

Tài liệu này dựa trên đánh giá Tiêu Chuẩn CIS Linux, cung cấp 1 bản hướng dẫn miêu tả cấu hình bảo mật cho Linux chạy trên nền tảng x86 và x64.

- Đối tượng

Bản tiêu chuẩn Policy này hướng đến các chuyên viên quản trị hệ thống, chuyên viên bảo mật, chuyên viên audit hệ thống, bộ phận hỗ trợ (help desk) và các cá nhân muốn phát triển, triển khai, đánh giá hoặc bảo mật các giải pháp tích hợp Linux.

- Định nghĩa Profile

Level 1: Những mục trong profile này được đưa ra với các tiêu chí:

- Thiết thực và quan trọng;
- Cung cấp một lợi ích rõ ràng về bảo mật và không cản trở việc ứng dụng cũng như hiệu năng hệ thống.

Level 2: Profile này mở rộng profile "Level 1". Những mục trong profile này được đưa ra với các tiêu chí

- Dành cho các môi trường hoặc tình huống mà bảo mật cao hơn
- Là thước đó phòng thủ hệ thống
- Có thể ảnh hưởng đến ứng dụng hay hiệu năng (performance) của hệ thống.

2. Tiêu chuẩn an toàn bảo mật cho hệ điều hành Linux

STT	Tiêu chuẩn	Mô tả
1	**Cấu hình ban đầu**	
1.1	Cấu hình tập tin hệ thống (file system)	
1.1.1	Vô hiệu hóa filesystems không sử dụng	
1.1.1.1	Vô hiệu hóa mount với cramfs filesystems	Việc cài đặt nhiều hardware/software, mở nhiều program/service/connection không cần thiết sẽ làm tăng khả năng các lỗ hổng có thể tồn tại trong các "đối tượng" do đó có thể bị hacker khai thác. Vì vậy, nên disables nếu hệ thống files cramfs không cần thiết sử dụng
1.1.1.2	Vô hiệu hóa mount của squashhfs filesystems	Việc cài đặt nhiều hardware/software, mở nhiều program/service/connection không cần thiết sẽ làm tăng khả năng các lỗ hổng có thể tồn tại trong các "đối tượng" do đó có thể bị hacker khai thác. Vì vậy, nên disables nếu hệ thống files squashfs không cần thiết sử dụng.
1.1.1.3	Vô hiệu hóa mount với udf filesystems	Việc cài đặt nhiều hardware/software, mở nhiều program/service/connection không cần thiết sẽ làm tăng khả năng các lỗ hổng có thể tồn tại trong các "đối tượng" do đó có thể bị hacker khai thác. Vì vậy, nên disables nếu hệ thống files udf không cần thiết sử dụng
1.1.2	Đảm bảo phần vùng /tmp được cấu hình	Hacker có thể sử dụng các thư mục tạm thời như /tmp để lưu trữ hoặc thực thi các phần mềm độc hại. Do đó khi tạo partition cùng với thiết lập các option noexc (không gán quyền thực thi cho các file nhị phân trên

		phân vùng được mount), quyền nodev (không cho phép các thiết bị kiểu character hoặc kiểu block sử dụng trên phân vùng này), nosuid (các SUID/SGID sẽ mất hiệu lực trên phân vùng) sẽ ngăn chặn việc hacker chạy các file mã độc hại lưu trên phân vùng. Cũng như hacker có thể tạo hardlink đến các chương trình hệ thống được setuid để dò lỗ hổng bảo mật của chương trình tiếp tục tấn công vào hệ thống. Mặt khác, các file trong thư mục /tmp có thể được thực thi bởi tất cả các user (world-writable) nên có thể dẫn đến việc hết dung lượng ổ cứng nếu không tạo một phân vùng riêng cho thư mục
1.1.3	Thiết lập tùy chọn nodev cho phân vùng /tmp	Thiết lập quyền nodev để đảm bảo không cho phép user tạo các kết nối với các thiết bị kiểu character hoặc kiểu block sử dụng trên phân vùng này.
1.1.4	Thiết lập tùy chọn nosuid cho phân vùng /tmp	Thiết lập quyền nosuid để đảm bảo không cho phép user tạo hoặc thiết lập userid cho file trong phân vùng này. Bởi các file được thiết lập setuserid thì sẽ có thể được chay bởi bất kì một user nào kể cả không phải chủ sở hữu của file. Do đó, hacker có thể lợi dụng tạo một hardlink đến các file được thiết lập có quyền userid để thực hiện việc dò lỗ hổng tấn công vào hệ thống.
1.1.5	Thiết lập tùy chọn noexec cho phân vùng /tmp	Thiết lập quyền noexec để đảm bảo không cho phép user chạy các chương trình dạng binary trong thư mục để đảm bảo hacker không thể chạy các phần mềm độc hại dưới dạng binary trên hệ thống.
1.1.6	Đảm bảo phân vùng /dev/shm được cấu hình	Bất kỳ user đều có thể upload and execute file trong thư mục /dev/shm như trong thư mục /tmp. Do đó khi tạo partition cùng với thiết lập các option noexc (không gán quyền thực thi cho các file nhị phân trên phân vùng được mount), quyền nodev (không cho phép các thiết bị kiểu character hoặc kiểu block sử dụng trên phân vùng này), nosuid (các SUID/SGID sẽ mất hiệu lực trên phân vùng) sẽ ngăn chặn việc hacker chạy các file mã độc hại lưu trên phân vùng. Cũng như hacker có thể tạo hardlink đến các chương trình hệ thống được setuid để dò lỗ hổng bảo mật của chương trình tiếp tục tấn công vào hệ thống
1.1.7	Thiết lập tùy chọn nodev cho phân vùng /dev/shm	Thiết lập quyền nodev để đảm bảo không cho phép user tạo các kết nối với các thiết bị kiểu character hoặc kiểu block sử dụng trên phân vùng này.

1.1.8	Thiết lập tùy chọn nosuid cho phân vùng /dev/shm	Thiết lập quyền nosuid để đảm bảo không cho phép user tạo hoặc thiết lập userid cho file trong phân vùng này. Bởi các file được thiết lập setuserid thì sẽ có thể được chay bởi bất kì một user nào kể cả không phải chủ sở hữu của file. Do đó, hacker có thể lợi dụng tạo một hardlink đến các file được thiết lập có quyền userid để thực hiện việc dò lỗ hổng tấn công vào hệ thống.
1.1.9	Thiết lập tùy chọn noexec cho phân vùng /dev/shm	Thiết lập quyền noexec để đảm bảo không cho phép user chạy các chương trình dạng binary trong thư mục để đảm bảo hacker không thể chạy các phần mềm độc hại dưới dạng binary trên hệ thống.
1.1.10	Đảm bảo phân vùng /var được cấu hình	Do một số files hoặc thư mục trong thư mục /var được gán quyền world-wriables nên có thể sẽ bị hacker lợi dụng để tấn công hệ thống cũng như việc tạo quá nhiều dữ liệu trong thư mục dẫn đến cạn kiệt tài nguyên nên cần tạo phân vùng cho thư mục này.
1.1.11	Thiết lập tham số liên kết khi mount /var/tmp vào thư mục /tmp	Để ngăn việc người dùng tạo quá nhiều file trong /var/tmp vượt quá dung lượng cấp phát hoặc cố gắng để thực thi các files đã bị giới hạn được phân quyền trong phân vùng /tmp.
1.1.12	Tạo partition cho thư mục /var/log	Việc tạo partition cho thư mục /var/log nhằm đảm bảo log hệ thống được lưu trữ không chiếm hết tài nguyên hệ thống và bảo vệ các dữ liệu audit.
1.1.13	Tạo partition cho thư mục /var/log/audit	Việc tạo partition cho thư mục /var/log/audit nhằm đảm bảo log hệ thống được lưu trữ không chiếm hết tài nguyên hệ thống khi file audit.log tăng lên và bảo vệ các dữ liệu audit
1.1.14	Tạo partition cho thư mục /home	Việc tạo partition cho thư mục /home nhằm đảm bảo các file được user lưu trữ sẽ không chiếm hết tài nguyên hệ thống và giới hạn các quyền user được phép thực thi với thư mục /home của user bằng việc thiết lập các option khi thực hiện mount.
1.1.15	Thiết lập tùy chọn nodev cho /home	Thiết lập quyền nodev để đảm bảo không cho phép user tạo các kết nối với các thiết bị kiểu character hoặc kiểu block sử dụng trên phân vùng này.
1.1.16	Thiết lập sticky bit trên tất cả các thư mục world-writable	Để tăng thêm tính private cho các user trong các thư mục world-writable như /tmp
1.2	Kiểm tra tính toàn vẹn của filesystem	
1.2.1	Cài đặt AIDE	Sử dụng AIDE để theo dõi các tập tin quan trọng mà việc thay đổi cấu hình các tập tin này có thể ảnh hưởng đến sự an toàn của hệ thống.

1.2.2	Lập lịch kiểm tra định kỳ filesystem với AIDE	Lập lịch kiểm tra định kì đảm bảo cho người quản trị hệ thống nắm được thông tin khi có bất cứ sự thay đổi trong cấu hình files.
1.3	Bổ sung tiến trình Hardening	
1.3.1	Giới hạn coredump	Thiết lập hard limit trên core dumps để ngăn user ghi đè lên các giá trị soft limit. Nếu core dumps được yêu cầu, xem xét thiết lập giới hạn cho nhóm user. Thêm vào đó, thiết lập giá trị fs.suid_dumpable = 0 để ngăn setuid từ dumping core.
1.3.2	Khởi động vị trí vùng nhớ ảo tự động	Ngẫu nhiên vị trí bộ nhớ ảo sẽ làm cho cho việc khai thác tấn công bộ nhớ trở nên khó khăn do vị trí bộ nhớ sẽ luôn thay đổi.
1.3.3	Đảm bảo prelink không được cài đặt	Prelink có thể can thiệp vào hoạt động của AIDE, vì nó thay đổi các tệp nhị phân. Prelink cũng có thể làm tăng lỗ hổng của hệ thống nếu người dùng có thể xâm nhập một thư viện chung như libc.
1.4	Mandatory Access Control	
1.4.1	Cấu hình SELINUX	
1.4.1.1	Đảm bảo SELINUX được cài đặt	Nếu không có MAC (Mandatory Access Control), hệ thống chỉ sử dụng DAC (Discretionary Access Control) theo mặc định .
1.4.1.2	Thiết lập chính sách SELINUX	Cấu hình mặc định ở mức target policy để đảm bảo ít nhất có thể bảo mật hệ thống ở mức khuyến nghị. Còn đối với các trường hợp yêu cầu khắt khe hơn thì có thể thiết lập ở chính sách retrict.
1.4.1.3	Đảm bảo SELINUX được bật ở chế độ enforcing hoặc permissive	Việc chạy SELinux ở chế độ bị vô hiệu hóa không được khuyến khích, hệ thống không chỉ không thực thi chính sách SELinux mà còn không ghi log các hành động truy nhập bởi các user và proceess không được chứng thực.
1.4.1.4	Cấu hình SELINUX ở chế độ Enforcing	Việc chạy SELinux ở chế độ Enforcing bảo mật cao cho hệ thống nhưng người quản trị cần nắm rõ các services đang chạy trên hệ thống để mở quyền truy cập.
1.4.1.5	Xóa bỏ SETroubleshoot	SETroubleshoot không phải là một dịch vụ quan trọng khi chạy trên server đặc biệt là khi X Windows không được sử dụng. Vì vậy có thể disable dịch vụ.
1.4.1.6	Xóa bỏ dịch vụ MSC Translation	Nếu dịch vụ này không thường xuyên được sử dụng, nên disable để giảm thiểu khả năng bị khai thác lỗ hổng.
1.5	Banner cảnh báo	
1.5.1	Thiết lập banner cảnh báo cho các dịch vụ đăng nhập	Warning messages thông báo người dùng đang cố gắng để đăng nhập vào hệ thống về tình trạng pháp lý của họ liên quan đến hệ thống và phải bao gồm tên của tổ chức sở hữu các hệ thống và chính sách giám sát.

1.5.2	Loại bỏ thông tin hệ điều hành khỏi banner	Hiển thị hệ điều hành và thông tin các bản vá trong các biểu ngữ đăng nhập sẽ cung cấp thông tin cho attacker để khai thác lỗ hổng cụ thể hệ thống trên phiên bản hệ thống đang sử dụng.
1.6	Đảm bảo Update, patches, security software được cài đặt	Việc cập nhật thường xuyên các bản vá giúp server được an toàn hơn. Các bản vá mới cho kernel, phần mềm trên server trước khi cài đặt nên được thử nghiệm trên môi trường test trước khi update cho hệ thống production.
2	**Dịch vụ**	
2.1	Dịch vụ hệ thống	
2.1.1	Dịch vụ đồng bộ thời gian	
2.1.1.1	Đảm bảo thời gian được đồng bộ	Việc đồng bộ thời gian đảm bảo các file log được ghi có thời gian nhất quán trên toàn doanh nghiệp, hỗ trợ cho việc kiểm tra, check log, bug lỗi.
2.1.1.2	Đảm bảo dịch vụ chrony được cấu hình	Việc đồng bộ thời gian đảm bảo các file log được ghi có thời gian nhất quán trên toàn doanh nghiệp, hỗ trợ cho việc kiểm tra, check log, bug lỗi. Xác định service chrony đã được cấu hình đồng bộ time đến 3 server NTP server của MobiFone hay chưa
2.1.1.3	Đảm bảo dịch vụ ntpd được cấu hình	Việc đồng bộ thời gian đảm bảo các file log được ghi có thời gian nhất quán trên toàn doanh nghiệp, hỗ trợ cho việc kiểm tra, check log, bug lỗi. Xác định service NTP đã được cấu hình đồng bộ time đến 3 server NTP server của MobiFone hay chưa
2.1.2	Gỡ bỏ dịch vụ xined	Nếu không cần thiết sử dụng xinetd thì nên gỡ bỏ.
2.1.3	Gỡ bỏ X Windows	Trừ khi việc sử dụng yêu cầu đăng nhập vào server với giao diện đồ họa nếu không thì nên xóa bỏ cài đặt X Windows để chống việc bị attack surface.
2.1.4	Vô hiệu hóa avahi server	Khi server không sử dụng in thì dịch vụ này không cần thiết sử dụng do đó nên tắt dịch vụ để tránh bị attack surface.
2.1.5	Vô hiệu hóa print server CUPS	Khi server không sử dụng in ấn thì dịch vụ này không cần thiết sử dụng do đó nên tắt dịch vụ để tránh bị attack surface.
2.1.6	Gỡ bỏ DHCP server	Nếu server không được sử dụng làm DHCP server, khuyến nghị nên xóa dịch vụ để giảm thiểu khả năng bị attack surface.
2.1.7	Gỡ bỏ LDAP	Nếu server không cần sử dụng dịch vụ LDAP server/clinet thì không nên cho chạy dịch vụ nhằm giảm thiểu khả năng bị attack surface.
2.1.8	Gỡ bỏ DNS Server	Nếu server không cần sử dụng dịch vụ DNS Server thì không nên cho chạy dịch vụ nhằm giảm thiểu khả năng bị attack surface.

2.1.9	Gỡ bỏ FTP Server	Nếu server không cần sử dụng dịch vụ FTP Server thì không nên cho chạy dịch vụ nhằm giảm thiểu khả năng bị attack surface.
2.1.10	Gỡ bỏ HTTP Server	Nếu server không cần sử dụng dịch vụ HTTP Server thì không nên cho chạy dịch vụ nhằm giảm thiểu khả năng bị attack surface.
2.1.11	Gỡ bỏ dovecot (dịch vụ IMAP và POP3)	Nếu server không cần sử dụng dịch vụ POP3 và (hoặc) IMAP server thì không nên cho chạy dịch vụ nhằm giảm thiểu khả năng bị attack surface.
2.1.12	Gỡ bỏ Samba	Nếu server không cần chia sẻ files với hệ thống Windows, khuyến nghị nên gỡ bỏ dịch vụ để giảm thiểu khả năng bị attack surface.
2.1.13	Gỡ bỏ HTTP Proxy server	Nếu server không được sử dụng làm proxy server, khuyến nghị nên xóa dịch vụ để giảm thiểu khả năng bị attack surface.
2.1.14	Gỡ bỏ dịch vụ NIS server	Dịch vụ NIS là hệ thống bảo mật kém và dễ bị DOS, buffer overflows, xác thực lỏng lẻo bởi NIS maps. NIS giờ được thay thế bởi giao thức LDAP (Light Directory Access Protocol). Vì vậy dịch vụ NIS khuyến nghị là nên bỏ.
2.1.15	Gỡ bỏ dịch telnet server	Do giao thức telnet không sử dụng phương thức mã hóa nên việc thực hiện kết nối thông qua telnet có thể dẫn đến việc hệ thống mạng bị sniff và thông tin bị đánh cắp. Giao thức ssh được sử dụng thay thế do mã hóa các session và bảo mật mạnh mẽ.
2.1.16	Cấu hình MTA (Mail Transfer Agent) cho chế độ local-only	Nếu server không sử dụng dịch vụ MTA, khuyến nghị nên xóa dịch vụ để giảm thiểu khả năng bị attack surface
2.1.17	Vô hiệu hóa NFS và RPC	Nếu server không cần sử dụng dịch vụ NFS server thì không nên cho chạy dịch vụ nhằm giảm thiểu khả năng bị attack surface.
2.2	Dịch vụ Client	
2.2.1	Gỡ bỏ dịch vụ NIS Client	Dịch vụ NIS là hệ thống bảo mật kém và dễ bị DOS, buffer overflows, xác thực lỏng lẻo bởi NIS maps. NIS giờ được thay thế bởi giao thức LDAP (Light Directory Access Protocol). Vì vậy dịch vụ NIS khuyến nghị là nên bỏ.
2.2.2	Gỡ bỏ dịch vụ rsh	Những dịch vụ này chứa nhiều rủi ro an ninh và đã được thay thế bằng các gói SSH an toàn hơn.
2.2.3	Gỡ bỏ dịch vụ talk	Do phần mềm talk không sử dụng mã hóa khi truyền tải thông tin nên tính bảo mật rất yếu.
2.2.4	Gỡ bỏ LDAP Client	Nếu server không cần sử dụng dịch vụ LDAP clinet thì không nên cho chạy dịch vụ nhằm giảm thiểu khả năng bị attack surface.

3	**Cấu hình network và firewall**	
3.1	Chỉnh tham số network (chế độ host only)	
3.1.1	Vô hiệu hóa IP Forwarding	Thiết lập tham số net.ipv4.ip_forward bằng 0 để đảm bảo server sẽ không forward gói tin giữa các card mạng.
3.1.2	Vô hiệu hóa redirects gói tin gửi	Hacker sẽ sử dụng một máy chủ bị xâm nhập để gửi thông tin ICMP redirects không hợp lệ đến các thiết bị định tuyến nhằm gây ra lỗi định tuyến
3.2	Chỉnh tham số network (chế độ router)	
3.2.1	Vô hiệu hóa Source Router Packet Acceptance	Thiết lập tham số net.ipv4.conf.all.accept_source_route và net.ipv4.conf.default.accept_source_route bằng 0 để đảm bảo hệ thống không sử dụng source routed. Giả sử máy chủ có hai card mạng một card được kết nối đến mạng internet một card kết nối nội bộ. Trong trường hợp định tuyến bình thường, attacker không thể sử dụng địa chỉ kết nối public để phát hiện các sever trong mạng nội bộ. Nếu sử dụng source route, attacker có thể lợi dụng để có thể truy nhập vào mạng nội bộ với một định tuyến đã được chỉ định.
3.2.2	Vô hiệu hóa ICMP Redirect Acceptance	Những kẻ tấn công có thể sử dụng ICMP redirect messages không có thật để cố thay đổi bảng định tuyến và khi đó attacker có thể gửi các gói tin đến một mạng không chính xác và capture lại các gói tin hệ thống.
3.2.3	Vô hiệu hóa Secure ICMP Redirect Acceptance	Việc bị tấn công vẫn có thể xảy ra khi mà gateway được biết đến trong danh sách có khả năng bị xâm nhập. Thiết lập net.ipv4.conf.all.secure_redirects =0 để bảo vệ hệ thống khỏi việc cập nhật bảng định tuyến bởi gateway trong danh sách hệ thống mà khả năng đã bị xâm nhập.
3.2.4	Log các gói tin không đáng tin cậy	Việc kích hoạt ghi lại log các gói tin cho phép người quản trị để điều tra khả năng một kẻ tấn công đang gửi gói tin giả mạo đến máy chủ của họ.
3.2.5	Kích hoạt Ignore Broadcast Requests	Chấp nhận ICMP echo và timestamp gửi yêu cầu đến địa chỉ broadcast multicast trong mạng có thể khiến hệ thống bị tấn công bởi Smurf attack. Smurf attack dựa vào kẻ tấn công gửi một lượng lớn bản tin ICMP broadcast với một địa chỉ nguồn giả mạo. Tất cả các host khi nhận được bản tin ICMP request sẽ thực hiện gửi bản tin echo-reply lại cho các địa chỉ giả mạo, mà thể không được định tuyến. Nếu quá nhiều host trả gửi bản tin phản hồi, lưu lượng truy cập trên mạng có thể bị tăng lên đáng kể dẫn đến nghẽn mạng.

3.2.6	Kích hoạt Bad Error Message Protection	Tránh trường hợp một attacker sẽ gửi bản tin phản hồi và cố gắng làm đầy log file hệ thống với nhiều thông báo lỗi vô nghĩa.
3.2.7	Kích hoạt RFC – recommended Source Route Validation	Thiết lập này là một cách để ngăn chặn attacker gửi đến server những gói tin không có thật mà những gói tin này không thẻ được phản hồi.
3.2.8	Kích hoạt TCP SYN cookies	Attacker sử dụng SYN flood attacks để thực hiện DOS hệ thống bằng cách gửi rất nhiều bản tin SYN với địa chỉ nguồn không có thực khiến cho hệ thống nhận được các gói tin này sẽ không thể thực hiện được bắt tay ba bước. Điều này sẽ nhanh chóng sử dụng hàng đợi các kết nối (half-open) trên kernel bị đầy dẫn đến các kết nối hợp lệ sẽ không kết nối thành công. SYN cookie cho máy máy chủ chấp nhận các kết nối hợp lệ ngay cả khi đang bị tấn công bởi DOS.
3.3	**TCP wrappers**	
3.3.1	Cài đặt TCP wrapper	TCP cung cấp một danh sách truy cập đơn giản cho các dịch vụ mà nó có thể hỗ trợ. Khuyến nghị tất cả các dịch vụ nên sử dụng TCP Wrappers.
3.3.2	Cấu hình file /etc/host.allow	File /etc/hosts.allow hỗ trợ điều khiển quyền truy cập theo IP nhằm đảm bảo rằng chỉ những hệ thống thuộc IP được cho phép mới có thể kết nối đến máy chủ.
3.3.3	Xác thực quyền file /etc/host.allow	Để đảm bảo rằng file /etc/hosts.allows được bảo vệ không được ghi từ những truy cập trái phép. Mặc dù nó được bảo vệ theo mặc định, các quyền truy cập file có thể được thay đổi do vô tình hoặc thông qua các hành động độc hại.
3.3.4	Cấu hình file /etc/host.deny	File /etc/hosts.deny đảm bảo chỉ các host được cấu hình trong file /etc/host.allow được phép truy cập server.
3.3.5	Xác thực quyền file /etc/host.deny	Để đảm bảo rằng các /etc/hosts.deny tập tin được bảo vệ không được ghi từ những truy cập trái phép. Mặc dù nó được bảo vệ theo mặc định, các quyền truy cập file có thể được thay đổi do vô tình hoặc thông qua các hành động độc hại.
3.3.4	Enable Filewall	Iptables/firewalld cung cấp khả năng bảo vệ hệ thống Linux bằng việc giới hạn các kết nối được đi qua hệ thống qua địa chỉ IP và port.
3.3.4.1	Đảm bảo rule Iptable tồn tại cho tất cả các port đang mở	Nếu không có quy tắc tường lửa được định cấu hình cho các cổng mở, chính sách tường lửa mặc định sẽ loại bỏ tất cả các gói đến các cổng này.
3.4	Cấu hình SSH	

3.4.1	Cấu hình quyền cho file /etc/ssh/sshd_config	File /etc/ssh/sshd_config cần phải được bảo vệ khỏi các thay đổi trái phép bởi người dùng không có đặc quyền.
3.4.2	Cấu hình giao thức SSH sử dụng SSHv2	Phiên bản SSHv1 đã lỗi thời và tồn tại nhiều vấn đề bảo mật và nên thay thế sang phiên bản SSHv2.
3.4.3	Cấu hình LogLevel cho máy chủ SSH	SSH cung cấp một số cấp độ logging với số lượng thông tin khác nhau. DEBUG là cấp độ không được khuyến nghị sử dụng vì nó cung cấp rất nhiều dữ liệu, rất khó để xác định thông tin bảo mật quan trọng. INFO là cấp độ cơ bản, chỉ lưu trữ các hoạt động đăng nhập của người dùng SSH. Trong nhiều tình huống, như là ứng phó sự cố, việc xác định người dùng nào hoạt động trên hệ thống là một điều quan trọng. Các bản ghi đăng xuất có thể giúp loại bỏ những người dùng đã đăng xuất, thu hẹp phạm vi tìm kiếm.
3.4.4	Cấu hình vô hiệu hóa X11 Forwarding cho máy chủ SSH	Vô hiệu hóa X11 Forwarding trừ khi có yêu cầu về hoạt động cần sử dụng ứng dụng X11. Có một rủi ro nhỏ rằng người dùng đã đăng nhập thông qua SSH với X11 forwarding có thể bị phá hoại bởi người dùng sử dụng X11 khác.
3.4.5	Set SSH MaxAuthTries to 4 or Less	Tham số MaxAuthTries xác định số lần được phép xác thực không thành công cho một kết nối. Đặt tham số MaxAuthTries thấp để giảm thiểu tấn công brute-force vào máy chủ SSH. Khuyến nghị cho tham số MaxAuthTries là 4.
3.4.6	Đảm bảo việc đăng nhập root qua SSH bị vô hiệu hóa	Việc không cho phép đăng nhập root qua SSH yêu cầu các quản trị viên hệ thống phải xác thực bằng tài khoản cá nhân của họ trước khi sử dụng lệnh sudo để chuyển sang quyền root. Điều này giúp giảm thiểu cơ hội từ chối trách nhiệm và cung cấp một dấu vết kiểm toán rõ ràng trong trường hợp xảy ra sự cố bảo mật.
3.5	Logging and Auditing	
3.5.1	Cấu hình Logging	
3.5.1.1	Cấu hình kích hoạt rsyslog service	Rsyslog service là service thay thế cho syslogd với nhiều ưu điểm vượt trội (mã hóa dữ liệu gửi về server tập trung, sử dụng TCP …) hỗ trợ việc tùy chỉnh chuyên sâu log của hệ thống. Kích hoạt service này để đảm bảo log hệ thống được kiểm soát chặt chẽ và tránh tình trạng có log được ghi nhận hoặc ghi nhận thiếu.
3.5.1.2	Phân quyền đối với file log sinh ra từ rsyslog	Rsyslog sẽ tạo logfile chưa tồn tại trên hệ thống. Đảm bảo rằng các file logs có quyền

		chính xác để chắc chắn rằng dữ liệu nhạy cảm được lưu trữ và bảo vệ.
3.5.2	Cấu hình Auditing	
3.5.2.1	Đảm bảo Auditd được cài đặt (tự động hóa)	Việc ghi lại các sự kiện hệ thống cung cấp cho các quản trị viên hệ thống thông tin để giúp họ xác định xem có xảy ra truy cập trái phép vào hệ thống của họ hay không.
3.5.2.2	Đảm bảo dịch vụ Auditd được kích hoạt và đang chạy (tự động hóa)	Bật auditd để ghi lại các sự kiện hệ thống. Việc ghi lại các sự kiện hệ thống cung cấp cho quản trị viên hệ thống thông tin để giúp họ xác định xem có truy cập trái phép vào hệ thống của họ đang xảy ra hay không.
3.6	**Access, Authentication and Authorization**	
3.6.1	Cấu hình PAM	
3.6.1.1	Cấu hình điều kiện tạo mật khẩu	Mật khẩu mạnh bảo vệ hệ thống khỏi bị tấn công trước các kỹ thuật Brute force.
3.6.1.2	Cấu hình khóa truy cập do nhiều lần nhập mật khẩu thất bại	Khóa truy cập đối với người dùng sau n lần đăng nhập liên tiếp không thành công giảm khả năng tấn công Brute force vào hệ thống.
3.6.1.3	Giới hạn việc sử dụng lại mật khẩu	Bắt buộc người dùng không được sử dụng lại 5 mật khẩu cũ khiến cho kẻ tấn công khó đoán được mật khẩu đang sử dụng.
3.6.1.4	Cấu hình thuật toán hash mật khẩu sang SHA-512	Thuật toán SHA-512 cung cấp khả năng hashing mạng hơn MD5, hơn nữa nó còn cung cấp thêm cơ chế bảo vệ cho hệ thống bằng cách làm tăng mức độ khó khăn cho kẻ tấn công khi cố gắng đoán được mật khẩu.
3.7	Tài khoản người dùng và môi trường	
3.7.1	Thiết lập tham số cho shadow password	
3.7.1.1	Thiết lập ngày hết hạn mật khẩu	Việc giới hạn số ngày sử dụng mật khẩu đăng nhập đảm bảo việc giảm thiểu bị tấn công bởi brute force
3.7.1.2	Thiết lập giới hạn số ngày tối thiểu thay đổi mật khẩu	Bằng cách hạn chế tần suất thay đổi mật khẩu, quản trị viên có thể ngăn chặn người dùng liên tục thay đổi mật khẩu của họ trong một nỗ lực để phá vỡ quy tắc tái sử dụng mật khẩu
3.7.1.3	Thiết lập số ngày thực hiện cảnh báo hết hạn mật khẩu	Cung cấp trước cảnh báo rằng một mật khẩu sẽ được đáo hạn nhằm mục đích cho người sử dụng có thời gian để nghĩ ra một mật khẩu an toàn.
3.7.2	Khóa các tài khoản không hoạt động	Các tài khoản không hoạt động trong một thời gian dài gây ra một mối đe dọa cho an ninh hệ thống.

Điều 9. Tiêu chuẩn đảm bảo an toàn bảo mật cho hệ điều hành Windows Server

1. Mục đích

Tài liệu này mô tả chi tiết các yêu cầu cần thiết để thiết lập cấu hình an toàn cho hệ thống sử dụng Windows OS chạy trên cả hai nền tảng x86 và x64, với mục đích:

- Làm cơ sở tham chiếu khi cài đặt và cấu hình hệ điều hành máy chủ đảm bảo an toàn;

- Làm cơ sở kỹ thuật cho công tác đánh giá an toàn an ninh cho hệ điều hành các máy chủ.

- Tài liệu được xây dựng với giả định rằng hệ thống hoạt động với đầy đủ các dịch vụ được cung cấp cùng với OS và được thực hiện dưới tư cách là quản trị viên (administrator).

Tài liệu được xây dựng dựa trên các bộ tiêu chuẩn thiết lập tham chiếu đến các tiêu chuẩn ATTT (TCVN, CIS,…), được chỉnh sửa cho phù hợp với tình hình của MobiFone, pháp luật và các yêu cầu an ninh an toàn thông tin trong nước.

2. Tiêu chuẩn đảm bảo an toàn bảo mật cho hệ điều hành Windows server

STT	Tiêu chuẩn	Mô tả
1	**Chính sách tài khoản người dùng**	
1.1	Cấu hình độ dài tối thiểu của mật khẩu	Các cuộc tấn công cơ sở dữ liệu tài khoản bằng cách sử dụng các công cụ để tìm kiếm tài khoản và mật khẩu xảy ra rất nhiều. Việc cấu hình độ dài tối thiểu của mật khẩu được khuyến cáo ít nhất 8 ký tự trở lên.
1.2	Cấu hình yêu cầu độ phức tạp của mật khẩu	Các mật khẩu chỉ chứa các ký tự chữ số và chữ cái rất dễ dàng bị phát hiện bằng một số công cụ tấn công có sẵn.
1.3	Cấu hình mật khẩu mới không trùng mật khẩu gần nhất	Để thiết lập cấu hình giới hạn mật khẩu mới không trùng mật khẩu gần nhất được khuyến cáo thông qua Group Policy
1.4	Cấu hình không lưu trữ bản mã dịch ngược của mật khẩu	Việc lưu mã ngược của mật khẩu có nguy cơ bị giải mã bởi những người am hiểu về mã hóa.
1.5	Cấu hình chính sách khóa tài khoản	Việc triển khai một chính sách khóa tài khoản hợp lý là rất quan trọng vì nó sẽ giúp bảo vệ chống lại các cuộc tấn công rò quét mật khẩu.
2	**Audit Policy Setting**	
2.1	**Tài khoản đăng nhập**	
2.1.1	Cấu hình không hiển thị trạng thái hoạt động của user Guest	Tài khỏa Guest cho phép người dùng chưa xác thực truy cập vào hệ thống.
2.2	**Quản lý tài khoản**	
2.2.1	Cấu hình chính sách “Audit Application Group Management”	Bật chính sách “Audit Application Group Management” để ghi lại kiểm tra các sự

		kiện được tạo ra bởi thay đổi đối với các nhóm ứng dụng
2.2.2	Cấu hình chính sách "Audit Computer Account Management"	Bật chính sách "Audit Computer Account Management" để kiểm tra các sự kiện giúp hỗ trợ khi thực hiện điều tra số đối với các sự cố bảo mật (tài khoản được tạo, thay đổi, xoá, đổi tên, kích hoạt, vô hiệu hoá)
2.2.3	Cấu hình chính sách "Audit Distribution Group Management"	Bật chính sách "Audit Distribution Group Management" để kiểm tra chính sách này giúp quản trị viên có thể theo dõi các sự kiện nhằm phát hiện việc tạo nhóm tài khoản độc hại, ngẫu nhiên và được uỷ quyền
2.2.4	Cấu hình chính sách "Audit Other Account Management Events"	Bật chính sách "Audit Other Account Management Event" để kiểm tra các sự kiện giúp hỗ trợ khi thực hiện điều tra số đối với các sự cố bảo mật tài khoản (Password hash đã bị truy cập, Password policy checking API được gọi)
2.2.5	Cấu hình chính sách "Audit Security Group Management"	Bật chính sách "Audit Security Group Management" để kiểm tra các sự kiện giúp hỗ trợ khi thực hiện điều tra số đối với các sự cố bảo mật
2.3	**Theo dõi chi tiết**	
2.3.1	Cấu hình chính sách "Audit Process Creation"	Bật chính sách "Audit Process Creation" để kiểm tra các sự kiện giúp hỗ trợ khi thực hiện điều tra số bảo mật (Tạo tiến trình mới, Primary token được chỉ định xử lý)
2.4	**Truy cập thư mục dịch vụ**	
2.4.1	Cấu hình chính sách "Audit Directory Service Access"	Bật chính sách "Audit Directory Service Access" để kiểm tra các sự kiện giúp hỗ trợ khi thực hiện điều tra số đối với các sự cố bảo mật, được ghi lại khi một đối tượng AD DS (Active Directory Domain Services)
2.4.2	Cấu hình chính sách "Audit Directory Service Changes"	Bật chính sách "Audit Directory Service Changes" để kiểm tra các sự kiện giúp hỗ trợ khi thực hiện điều tra số đối với các sự cố bảo mật (Đối tượng DS đã bị sửa đổi, được tạo, được phục hồi, đã bị di chuyển)
2.5	**Đăng nhập/ đăng xuất**	
2.5.1	Cấu hình chính sách "Audit Account Lockout"	Bật chính sách "Audit account lockout" giúp ghi lại các lần khóa tài khoản, phát hiện các hành vi bất thường
2.5.2	Cấu hình chính sách "Audit Logoff" và "Audit Logon"	Bật chính sách "Audit Logoff" và "Audit Logon" để kiểm tra xác định người dùng nào đã truy cập hoặc cố gắng truy cập vào hệ thống
2.5.3	Cấu hình chính sách "Audit Other Logon/Logoff Events"	Bật chính sách "Audit Other Logon/Logoff Event" để kiểm tra các sự kiện đăng nhập/ đăng xuất khác (ví dụ:

		những sự kiện ngắn kết nối/ kết nối lại các phiên đăng nhập từ xa)
2.5.4	Cấu hình chính sách "Audit Special Logon"	Bật chính sách "Audit Special Logon" để kiểm tra các sự kiện đăng nhập với quyền tương đương quản trị viên hoặc cao hơn giúp hỗ trợ thực hiện điều tra số đối với các sự cố bảo mật
2.6	**Thay đổi chính sách**	
2.6.1	Cấu hình chính sách "Audit Audit Policy Change"	Bật chính sách "Audit audit policy change" để kiểm tra các sự kiện liên quan tới việc thay đổi chính sách (SACL)
2.6.2	Cấu hình chính sách "Audit Authentication Policy Change"	Bật chính sách "Audit Authentication Policy Change" để kiểm tra các sự kiện liên quan tới việc thay đổi chính sách xác thực (Trusted domain, Kerberos,…)
2.7	**Sử dụng đặc quyền**	
2.7.1	Cấu hình chính sách "Audit Sensitive Privilege Use"	Bật chính sách "Audit Sensitive Privilege Use" để ghi lại các sự kiệ khi tài khoản người sử dụng quyền thực thi tác vụ (Backup, tạo token object, gỡ lỗi, thay đổi giá trị firmware)
2.8	**Cấu hình Sysmon Setting**	Sysmon (System Monitor) là một công cụ từ Sysinternals suite của Microsoft, giúp ghi lại các sự kiện hệ thống chi tiết về các hoạt động như tạo tiến trình, kết nối mạng và thay đổi file. Sysmon là một công cụ mạnh mẽ cho việc giám sát bảo mật và phát hiện xâm nhập.
2.9	**Cấu hình Backup**	Để thực hiện phòng ngừa mất dữ liệu do hỏng phần cứng, phần mềm và đối phó với tấn công mạng, ransomeware, virus độc hại thì công việc Backup rất cần thiết.

Điều 10. Tiêu chuẩn đảm bảo an toàn bảo mật cho Database

1. Mục đích

Tài liệu này mô tả chi tiết các yêu cầu cần thiết để thiết lập cấu hình an toàn bảo mật cho nhóm hệ thống thiết bị Database với mục đích:

- Làm cơ sở tham chiếu khi cài đặt và cấu hình cho thiết bị mạng đảm bảo an toàn;

- Làm cơ sở kỹ thuật cho công tác đánh giá an toàn bảo mật cho các thiết bị mạng.

Tài liệu được xây dựng với giả định rằng hệ thống hoạt động với đầy đủ các tính năng và được thực hiện dưới tư cách là quản trị viên (root).

Tài liệu được xây dựng dựa trên các bộ tiêu chuẩn thiết lập tham chiếu đến các tiêu chuẩn ATTT (TCVN 11930:2017, CIS, …), được chỉnh sửa cho phù hợp với tình hình của MobiFone, pháp luật và các yêu cầu an toàn bảo mật an toàn thông tin trong nước.

2. Tiêu chuẩn đảm bảo an toàn bảo mật cho Database

2.1 Tiêu chuẩn cài đặt Oracle Database

STT	Tiêu chuẩn	Mô tả
1	**Mô hình**	
1.1	Mô hình kết nối	Oracle RAC (Active – Active) Oracle Active – Standby
1.2	Mô hình dự phòng	Các nghiệp vụ quan trọng, online thì phải có thêm mức dự phòng với công nghệ Oracle DataGuard (nếu cùng nền tảng) hoặc Oracle GoldenGate (nếu khác nền tảng) và phòng ngừa thảm họa (DR) với 1 trong 2 công nghệ trên.
2	**Cấu hình cài đặt**	
2.1	Vesion	Cài đặt phiên bản mới nhất hoặc gần phiên bản mới nhất 1 phiên bản (Ví dụ Oracle Database mới nhất là 19.15 thì có thể cài đặt 19.14). (Phiên bản mới nhất sẽ patch mọi lỗ hổng của phiên bản trước đó nhưng độ ổn định thì không bằng phiên bản phiên bản mới nhất - 1 được)
2.2	Patch	Patch đầy đủ theo phiên bản cài đặt
2.3	Control file	Tối thiểu 02 control file trên 02 phân vùng (mount point hoặc diskgroup) khác nhau
2.4	Redo Log Group	Có ít nhất 3 redo log group mỗi instance DB, mỗi redo log group có ít nhất 2 member trên 2 vùng khác nhau, đảm bảo mirror dự phòng cho nhau.
2.5	Database ở chế độ archived log	Database chạy ở chế độ archive log mode
2.6	Tablespace	Tablespace UNDO, TEMP, ứng dụng có các datafile nằm trên ít nhất 2 mount point khác nhau (nếu dạng file system) và ít nhất 02 datafile (nếu là ASM)
2.7	Bộ nhớ SGA, PGA	Dung lượng SGA + PGA tương đương 80% dung lượng RAM (trong đó nghiệp vụ OLTP thì SGA cấp 80%, PGA cấp 20%; với nghiệp vụ DSS thì SGA cấp tối thiểu 30%, PGA tối đa 70%)
2.8	Tham số db_files	DB_FILES khai báo từ 1000 – 10000.
2.9	Tham số resource_limit	Đặt tham số resource_limit = true để các chính sách user profile đặt trong DB có hiệu lực.
2.10	Tham số process	Đặt các tham số sessions, proceses (500-5000) phù hợp với yêu cầu nghiệp vụ của từng DB.
2.11	Chế độ dedacated server	DB chạy chế độ Dedacated server Nếu tài nguyên hữu hạn có thể đặt chế độ shared server (shared_server từ 50 – 400), các ứng dụng kết nối vào cũng đang chạy theo chế độ shared.

2.12	Cấu hình backup	Cấu hình RMAN giữ ít nhất 2 bản full và đảm bảo các điều kiện sau: • Auto backup control file • MAXPIECESIZE tối đa 5-40GB Nên đặt db_block_checking
2.13	Yêu cầu ASM diskgroup, ASM disk	Đối với DB sử dụng ASM: • Có ít nhất 3 disk group khác nhau (CRS, DATA, RECO) • Mỗi disk group có ít nhất 4 LUN cùng size dạng external, nếu diskgroup lưu dữ liệu quan trọng nên dùng normal (CRS là bắt buộc phải dùng kiểu normal với tối thiểu 3 disk)
2.14	Thiết lập HugePage	DB có RAM 8GB cần thiết lập HugePage tối thiểu 2MB (vì mặc định page memory là 4K)
2.15	Audit_db	Đặt audit_db=none để tránh ảnh hưởng đến tải DB

2.2 Tiêu chuẩn thiết kế Database Oracle

STT	Tiêu chuẩn	Yêu cầu
1	Tiêu chuẩn chung của các objects	Các object đặt option noparallel.
		Drop các user không sử dụng, revoke quyền DBA của các user.
		Kiểm tra profile chứa user ứng dụng đảm bảo profile này đặt unlimited cho mọi tham số.
		Bảng dữ liệu ứng dụng không nằm trên tablespace mặc định là USERS
		Không xuất hiện corrupt block trong DB.
		Tất cả các object ở trạng thái valid (các object bị invalid thì phải drop).
		Tất cả index không ở trạng thái unusable.
		Định dạng tên partition đối với các bảng đánh partition theo thời gian là DATAyyyy, DATAyyyymm hay DATAyyyymmdd tuỳ theo loại partition (partition theo năm, tháng hoặc ngày tương ứng)
2	Cấu trúc bảng	Khi tạo bảng mới cần áp dụng các phương án như sau: Với bảng có dữ liệu dự kiến lớn, có tính lịch sự (như bảng log giao dịch) phải đánh partition: - Với dữ liệu lịch sử thì đánh theo By Range (thường theo Date) - Với dữ liệu xác định trước được giá trị thì đánh theo By list. - Với dữ liệu không có quy luật thì đánh theo By Hash.
		Với các bảng có đánh partition thì index phải đánh theo Local.
		Hạn chế sử dụng trigger trên bảng.

		Đánh giá trong câu lệnh select có trường nào xác định được đối tượng tìm kiếm chính xác nhất và có độ dài trường ngắn nhất (ưu tiên trường number) thì đánh index theo trường đó.
		Hạn chế dùng foreign key.
		Với các bảng có tần suất update hoặc insert lớn không nên dùng primary key.
3	Câu lệnh SQL nghiệp vụ	Khi viết câu lệnh tác động vào bảng cần làm theo hướng dẫn sau: Tất cả các câu lệnh đều phải có index, không câu lệnh nào được quét full bảng (với hệ thống Report/DSS khi quét full cần thêm hint parallel)
		Nếu bảng có partition thì trong câu lệnh phải có thêm trường partition (ngoại trừ một số trường hợp đặc biệt).
		Khi join hai bảng với nhau thì bảng có dữ liệu lớn hơn phải có index.
		Trong câu lệnh không dùng điều kiện is null, cần chuyển sang phương án dùng các toán tử : >, <, =.
		Hạn chế sử dụng câu lệnh delete, cần chuyển sang câu lệnh truncate.
		Hạn chế sử dụng câu lệnh update, cần chuyển sang câu lệnh insert và select.
		Với các bảng tmp có dữ liệu trong quá trình chạy và xóa dữ liệu sau khi chạy (không cần backup dữ liệu), cần chuyển bảng sang nologging và câu lệnh insert cần có thêm append.
4	View	Các lưu ý khi tạo view: Trong view không nên thêm trường mới vì khi câu lệnh select vào view có thể sẽ bị quét full bảng.
		Hạn chế sử dụng view lồng nhau.
5	Tạo tablespace:	Với mỗi DB thường, tạo các loại tablespace như sau: Các datafile có thể đặt auto extend để tiết kiệm dung lượng (nếu kiểm soát được), còn không thì không đặt auto extend, size 4GB, 8GB, 16GB, 32GB, 64GB. Loại tablespace USERS (mặc định): Lưu dữ liệu user cá nhân hỗ trợ nghiệp vụ
		Tablespace cố định: để lưu default các user ứng dụng, các bảng không có partition, các bảng danh mục, đặt trên là DATA, tương ứng lưu index là INDX
		Tablespace không cố định: lưu các bảng có partition, ví dụ DATA202212, tương ứng là INDX202212 và DATA2022, tương ứng là INDX2022,....
		Tablespace nghiệp vụ: lưu các bảng của nghiệp vụ tạo ra, ví dụ: DATA_NGHIEPVU1, INDX_NGHIEPVU1, DATA_NGHIEPVU2, INDX_NGHIEPVU2
		Tablespace DUMP: lưu các bảng temp, test, xoá liên tục,... không cần backup tablespace này

		Tablespace LOB: Lưu dữ liệu lob, nếu dữ liệu LOB lớn thì tách ra theo năm/tháng LOByyyy, LOByyyymm
		Loại tablespace USERS (mặc định): Lưu dữ liệu user cá nhân hỗ trợ nghiệp vụ

2.3 Tiêu chuẩn vận hành Database Oracle an toàn, tối ưu

STT	Tiêu chuẩn	Mô tả
1	Mô hình kết nối	Oracle RAC (Active – Active) hoặc Oracle Active – Standby
2	Mô hình dự phòng	Các nghiệp vụ quan trọng, online thì phải có thêm mức dự phòng với công nghệ Oracle DataGuard (nếu cùng nền tảng) hoặc Oracle GoldenGate (nếu khác nền tảng) và phòng ngừa thảm họa (DR) với 1 trong 2 công nghệ trên.
3	Cấu hình cảnh báo	Cấu hình cảnh báo DB như các DB khác đang chạy: Đặt cảnh báo Tablespace
		Đặt cảnh báo ASM disk group
		Đặt cảnh báo disk u01, /
		Đặt cảnh báo performance (ví dụ Gold > 250 active là timeout, lock > 50 là có nguy cơ timeout nghiệp vụ,…)
		Đặt cảnh báo alert log
		Đặt cấu hình Analyze bảng và index
		Đặt trigger Firewall DB
		Đặt cảnh báo tác động DDL
		Đặt cảnh báo tác động DML (FGA)
		Đặt cảnh báo Listener, instance, log backup
4	Cơ chế backup DB	Giữ ít nhất 2 bản backup full gần nhất
		Đẩy sớm lên backup tập trung (đối với các DB chạy trên local disk), 1 tuần có tối thiểu 01 bản backup full lưu trữ ở storage khác với phân vùng chứa datafile. Luôn có 03 bản backup full (dùng RMAN và datapump) vào đầu năm, giữa năm và hiện tại theo chu kỳ 01 năm.
		(RMAN để dựng lại cùng môi trường; còn bản datapump để ứng cứu import trên môi trường khác)
5	Phương án ứng cứu khi lỗi dữ liệu 1 phần	Có thủ tục step by step khả thi hướng dẫn ứng cứu khi lỗi 1 phần DB Thủ tục này đã được thử nghiệm chưa, thời gian khôi phục hết bao lâu?
6	Phương án ứng cứu khi lỗi toàn bộ DB	Có thủ tục step by step khả thi hướng dẫn ứng cứu khi lỗi toàn bộ DB Thủ tục này đã được thử nghiệm chưa, thời gian khôi phục hết bao lâu?
7	Profile cho user DB	User cá nhân và user ứng dụng đặt trên 2 profile có policy khác nhau (user cá nhân đặt giới hạn 3 session, expire password 45 ngày).

8	Audit DB	Với các dữ liệu nhạy cảm cần đặt audit bằng FGA hoặc công cụ bên thứ 3, các bảng log audit cần phải đặt trên tablespace riêng không thuộc system tablespace (ví dụ tablespace AUD).
9	Bảng lớn	Với bảng có dữ liệu lớn (2G trở lên) cần trao đổi sớm với nghiệp vụ để đánh partition. - Với dữ liệu lịch sử thì đánh theo By Range (thường theo ngay tháng) - Với dữ liệu xác định trước được giá trị thì đánh theo By list. - Với dữ liệu không có quy luật thì đánh theo By Hash. - Hoặc kết hợp các kiểu partition cho hợp lý Nguyên tắc: Chia để trị, chia nhỏ bảng lớn ra để việc quét dữ liệu ít hơn, tối ưu hơn cho câu lệnh SQL.
10	Drop các bảng không sử dụng (Lưu ý backup trước khi drop)	Drop tất cả các bảng ứng dụng không sử dụng. Drop tất cả các bảng rác do user cá nhân tạo ra.
11	Kiểm tra chính sách quay vòng dữ liệu	Xác định chính sách vòng đời của các bảng dữ liệu theo quy định.
12	Giám sát cảnh báo	Liên tục giám sát cảnh báo qua SMS, Polestar, email báo cáo hàng ngày, nghiệp vụ,… và xử lý
13	Tự động hóa	Bổ sung các job tự động dọn dẹp OS/DB, backup, báo cáo add datafile, partition,…
14	Cập nhật tài liệu vận hành	Bổ sung, cập nhật tài liệu vận hành khi có sự điều chỉnh phù hợp hơn hoặc khi có case lỗi phát sinh.
15	Cập nhật hệ thống	Có thủ tục, phương án rõ ràng, đầy đủ, đặc biệt phải backup và phải rollback được trong trường hợp cập nhật lỗi.

2.4 Tiêu chuẩn giám sát, kiểm soát truy cập người dùng Database Oracle

STT	Tiêu chuẩn	Mô tả
1	Xác thực 02 yếu tố	Xác thực thêm yếu tố IP trigger Firewall DB
2	Giám sát database	Tuân thủ quy định giám sát database mục 3. Bộ tiêu chuẩn vận hành database
3	Cấp phát user mới	Khi xin tạo mới user truy cập vào database cần cung cấp thông tin: Mô hình kết nối tổng thể của hệ thống; Chủ trương kết nối vào database để khai thác dữ liệu (như văn bản chỉ đạo, quy trình, quy định,…); Dự kiến tần suất truy cập vào các dữ liệu; Tuân thủ cam kết đảm bảo an toàn thông tin
4	Mật khẩu	Tối thiểu 8 ký tự, có số, chữ cái hoa thường và ký tự đặc biệt. Các thuộc tính của mật khẩu: Số lần login fail trước khi bị lock: 5 Thời gian lock: 1 giờ Thời hạn mật khẩu: User ứng dụng: Không cần đổi mật khẩu User thường: Đổi mật khẩu định kỳ theo quy chế ATTT (thường <=45 ngày)

<table>
<tr><td></td><td></td><td>Thời gian được sử dụng lại mật khẩu cũ: >= 365 ngày</td></tr>
<tr><td rowspan="2">5</td><td rowspan="2">Session</td><td>Tiêu chuẩn với nhóm user thông thường:
Số lượng tối đa session được mở của user <=4
Mật khẩu phải được thay đổi thường xuyên theo quy chế ATTT
Giới hạn active session <=4
Giới hạn parallel <=4
Các giới hạn khác theo nhu cầu (như RAM, undo, redo,…): Cấu hình khi cần thiết</td></tr>
<tr><td>Tiêu chuẩn với nhóm user ứng dụng: Thông thường sẽ không giới hạn để nghiệp vụ chủ động kiểm soát, trong trường hợp ứng dụng chiếm tải mà ảnh hưởng đến các nghiệp vụ khác khi dùng chung DB thì cần giới hạn tài nguyên về số số lượng session, active session, parallel, CPU.</td></tr>
<tr><td>6</td><td>Quyền truy cập</td><td>Khi xin bổ sung quyền truy cập vào database cần cung cấp thông tin:
Mô hình kết nối tổng thể của hệ thống;
Chủ trương kết nối vào database để khai thác dữ liệu (như văn bản chỉ đạo, quy trình, quy định,…);
Dự kiến tần suất truy cập vào các dữ liệu;
Tuân thủ cam kết đảm bảo an toàn thông tin.</td></tr>
<tr><td></td><td>Giám sát log tác động của user vào database</td><td>Với các tác động vào kho tài nguyên của MobiFone (kho sim, kho số, thẻ cào, hàng hóa,..); thông tin khách hàng (đấu nối, chặn cắt, thay đổi thông tin, chi tiết cước, thanh toán, công nợ,…) và các bảng quan trọng khác:
User ứng dụng chính khi kết nối vào DB cần phải ghi log đầy đủ và báo cáo theo quy chế ATTT.
User của ứng dụng của các hệ thống khác (CTKV, TT CNTT, TT MDS,…): cần phải ghi log đầy đủ, đẩy file log về hệ thống audit tập trung của TCT và có báo cáo định kỳ hàng ngày hoặc bất thường về Trung tâm TCTK, Ban CNTT
User vận hành nghiệp vụ: cần phải ghi log đầy đủ và có báo cáo định kỳ hàng ngày hoặc bất thường về Trung tâm TCTK, Ban CNTT
Ví dụ mẫu báo cáo:
Bao cao truy cap CSDL xxxx
<table>
<tr><th>NGAY</th><th>USER_NAME</th><th>CAU_LENH</th><th>SO_LUONG</th></tr>
<tr><td>dd/mm/yyyy</td><td>Username</td><td>SELECT</td><td>Số lượng</td></tr>
<tr><td>dd/mm/yyyy</td><td>Username</td><td>Update</td><td>Số lượng</td></tr>
<tr><td>dd/mm/yyyy</td><td>Username</td><td>Insert</td><td>Số lượng</td></tr>
<tr><td>…</td><td></td><td></td><td></td></tr>
</table>
</td></tr>
</table>

2.5 Tiêu chuẩn cho các DB khác (MySQL/MariaDB, PostgreSQL, SQL Server,…)

STT	Tiêu chuẩn	Mô tả
1	**Cài đặt**	
1.1	Mô hình kết nối	Active-Active hoặc Active - Standnby
1.2	Mô hình dự phòng	Có dự phòng ở site khác với DB quan trọng

1.3	Vesion	Cài đặt phiên bản mới nhất hoặc phiên bản mới nhất -1 phiên bản
1.4	Patch	Patch mới nhất đầy đủ, mới nhất
2	**Thiết kế**	
2.1	Tạo partiton của bảng lớn	Với các bảng dữ liệu lớn, có lịch sử cần tạo partition hợp lý
2.2	Tạo index	Index local và tối thiểu hóa index
3	**Vận hành**	
3.1	Giám sát DB	Liên tục giám sát cảnh báo qua Polestar hoặc TOAD,…
3.2	Tự động hóa	Bổ sung các job tự động dọn dẹp OS/DB, backup, báo cáo
3.3	Có vòng đời lưu trữ dữ liệu	Có vòng đời lưu trữ dữ liệu hợp lý
3.4	Nơi lưu trữ backup dữ liệu	Backup trên SAN khác với SAN lưu datafile
3.5	Bản backup dữ liệu	Luôn có 03 bản backup full vào đầu năm, giữa năm và hiện tại theo chu kỳ 01 năm
3.6	Phương án ứng cứu khi lỗi dữ liệu 1 phần	Có thủ tục step by step khả thi hướng dẫn ứng cứu khi lỗi 1 phần DB
3.7	Phương án ứng cứu khi lỗi toàn bộ DB	Có thủ tục step by step khả thi hướng dẫn ứng cứu khi lỗi toàn bộ DB
3.8	Cập nhật tài liệu vận hành	Khi có sự thay đổi tốt hơn cần bổ sung, cập nhật tài liệu vận hành hoặc khí có các case lỗi
3.9	Cập nhật hệ thống	Có thủ tục, phương án rõ ràng, đầy đủ, đặc biệt phải backup và phải rollback được trong trường hợp cập nhật lỗi
4	**Giám sát, kiểm soát truy cập người dùng**	Tương tự như tiêu chuẩn ATTT với Oracle Database

Điều 11. Tiêu chuẩn đảm bảo an toàn bảo mật cho thiết bị mạng

1. Mục đích

Tài liệu này mô tả chi tiết các yêu cầu cần thiết để thiết lập cấu hình an toàn bảo mật cho nhóm hệ thống thiết bị mạng với mục đích:

- Làm cơ sở tham chiếu khi cài đặt và cấu hình cho thiết bị mạng đảm bảo an toàn;

- Làm cơ sở kỹ thuật cho công tác đánh giá an toàn bảo mật cho các thiết bị mạng.

Tài liệu được xây dựng với giả định rằng hệ thống hoạt động với đầy đủ các tính năng và được thực hiện dưới tư cách là quản trị viên (administrator).

Tài liệu được xây dựng dựa trên các bộ tiêu chuẩn thiết lập tham chiếu đến các tiêu chuẩn ATTT (TCVN 11930:2017, CIS, …), được chỉnh sửa cho phù hợp với tình hình của MobiFone, pháp luật và các yêu cầu an toàn bảo mật an toàn thông tin trong nước.

2. Tiêu chuẩn cấu hình đảm bảo an toàn bảo mật cho các thiết bị Mạng

STT	Tiêu chuẩn	Mô tả
1	Cấu hình đặt tên thiết bị	Thực hiện đặt tên thiết bị: bao gồm tối thiểu tên đơn vị quản lý, địa điểm đặt thiết bị, tên vai trò thiết bị,…
2	Thiết lập cấu hình Banner khi truy cập thiết bị	Để thiết lập hiển thị cảnh báo banner khi truy cập vào thiết bị mạng
3	Cấu hình thời gian idle tự động ngắt sau phiên làm việc	Để cấu hình thời gian idle tự động ngắt kết nối sau một phiên làm việc trên các thiết bị mạng
4	Cấu hình giới hạn địa chỉ IP cho phép truy cập quản trị	Để thực hiến cấu hình giới hạn địa chỉ IP cho phép truy cập quản trị
5	Cấu hình tắt các Service và Interface không sử dụng	Hạn chế các Service và Interface không sử dụng gây mất an toàn bảo mật
6	Cấu hình xác thực cho các cổng AUX và Console	Để bảo vệ truy cập, quản lý phiên, theo dõi và ghi lại.
7	Cấu hình xác thực tập trung (Nếu có AAA)	Để quản lý người dùng, tăng cường bảo mật, quản lý quyền truy cập, theo dõi và ghi lại các hoạt động.
8	Cấu hình đồng bộ thời gian qua NTP tập trung	Để đồng bộ thời gian chính xác, ghi lại và phân tích các sự kiện phát hiện các xâm nhập lạ.
9	Cấu hình an toàn cho SNMP và giới hạn IP truy cập	Để bảo mật thông tin dữ liệu, hạn chế quyền truy cập, sử dụng các cơ chế xác thực và mã hóa
10	Cấu hình giao thức truy cập từ xa SSH	Để thực hiện truy cập từ xa có mã hóa và xác thực người dùng, ghi log truy cập.
11	Cấu hình mật khẩu	Tạo độ phức tạp cho mật khẩu đảm bảo an toàn bảo mật
12	Cấu hình đẩy log SIEM	Giám sát các hệ thống qua SIEM
13	Cấu hình số lần xác thực không thành công (Nếu có AAA)	Cấu hình số lần tối đa xác thực không thành công (Khuyến nghị tối đa 05 lần đăng nhập thất bại)
14	Cấu hình Backup	Để thực hiện phòng ngừa mất dữ liệu do hỏng phần cứng, phần mềm và đối phó với tấn công mạng, ransomeware, virus độc hại thì công việc Backup rất cần thiết.

Phụ lục I

TÀI LIỆU THAM KHẢO

HƯỚNG DẪN TRIỂN KHAI BỘ TIÊU CHUẨN ĐẢM BẢO AN TOÀN BẢO MẬT CHO CÁC HỆ THỐNG

(Kèm theo Quyết định số 1470/QĐ-MOBIFONE ngày 20 tháng 9 năm 2024 của Tổng công ty Viễn thông MobiFone)

I. HƯỚNG DẪN ĐẢM BẢO AN TOÀN BẢO MẬT TRONG KHI VẬN HÀNH HỆ THỐNG

1. Tiêu chuẩn cho mô hình quản trị hệ thống

Để đảm bảo việc giám sát truy cập từ xa tập trung cung cấp cho các quản trị viên phương thức truy cập, quản trị hệ thống tập trung, đảm bảo an toàn thông tin thì tất cả các hệ thống MobiFone trong quy định cần thực hiện truy cập qua các hệ thống giám sát truy cập từ xa tập trung:

- Tiêu chuẩn mô hình quản trị hệ thống 1 :

  - Kết nối truy cập đến Database và quản trị ứng dụng: Client → Shell Control Box (SCB)/Cyber Ark → Jump Server → Database
  - Kết nối truy cập đến Database khi không có máy chủ Jump Server: Client → Internet → VPN System → Database

- Tiêu chuẩn mô hình quản trị hệ thống 2 :

  - Kết nối truy cập đến Server qua Shell Control Box (SCB): Client →Shell Control Box (SCB) → Jump Server → Server.
  - Kết nối truy cập đến Server qua Cyber Ark: Client →Cyber Ark → Server.

2. Quản trị hệ thống qua máy chủ Jump Server

Máy chủ Jump Server là máy chủ trung gian được sử dụng để quản lý và kiểm soát truy cập tới các máy chủ khác trong một mạng nội bộ. Mục tiêu chính của Jump Server là tăng cường bảo mật và quản lý truy cập trong hệ thống mạng bằng cách tạo một điểm truy cập tập trung duy nhất cho các quản trị viên và người dùng có quyền.

2.1 Các yêu cầu cho máy chủ Jump Server

Máy chủ Jump Start đóng vai trò là điểm truy cập duy nhất cho các tài nguyên (có đặc quyền). Do đó, máy chủ Jump Server cần được bảo mật và củng cố giám sát tối đa.

Nên máy chủ Jump Start cần đảm bảo các yêu cầu sau:

- Hệ điều hành Windows server mới nhất (ít nhất 2019 trở lên), update bản vá mới nhất.

- Cài đặt phần mềm Antivirus

- Không join domain, không kết nối Internet

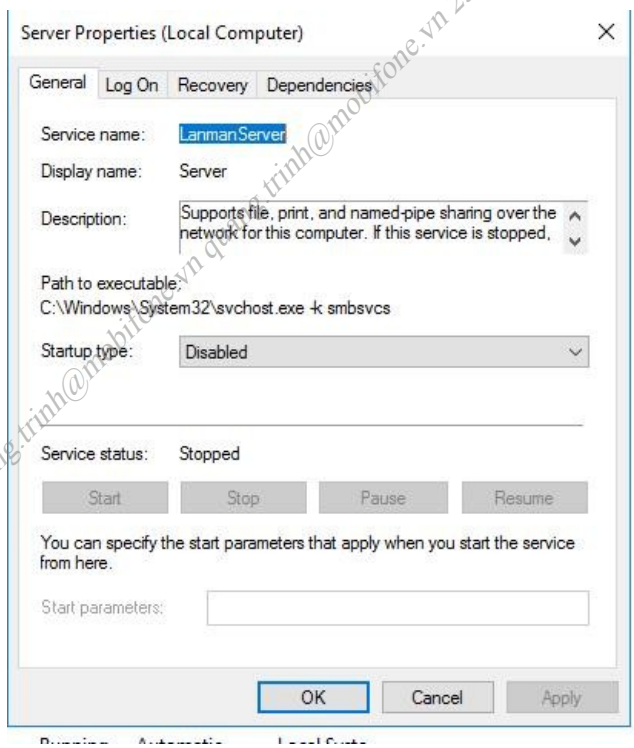
- Cài đặt giám sát SIEM (Enable Sysmon, audit log, đẩy log SIEM)

- Bật Firewall mềm, chặn any/any, chỉ mở port 3389 và các port cần thiết (đặc biệt chặn các port 445, 135)

- Cài đặt xác thực MFA – Kết nối qua CyberArk hoặc SCB của Tổng công ty

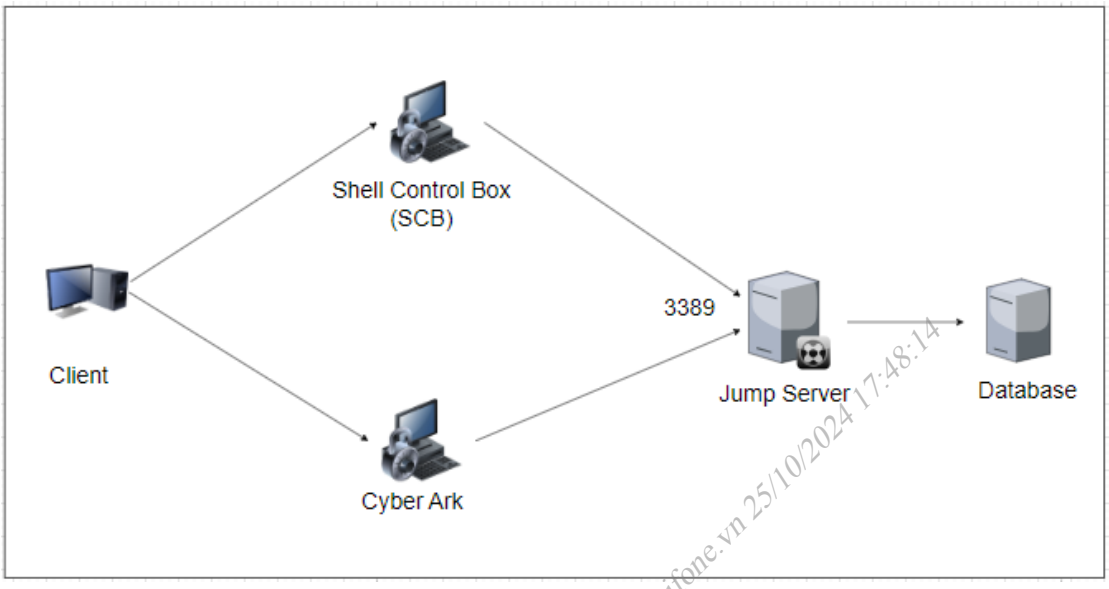
- Disable tài khoản Guest, đổi password có độ khó cao cho tài khoản administrator.

- Disable và Stop service server trên Server

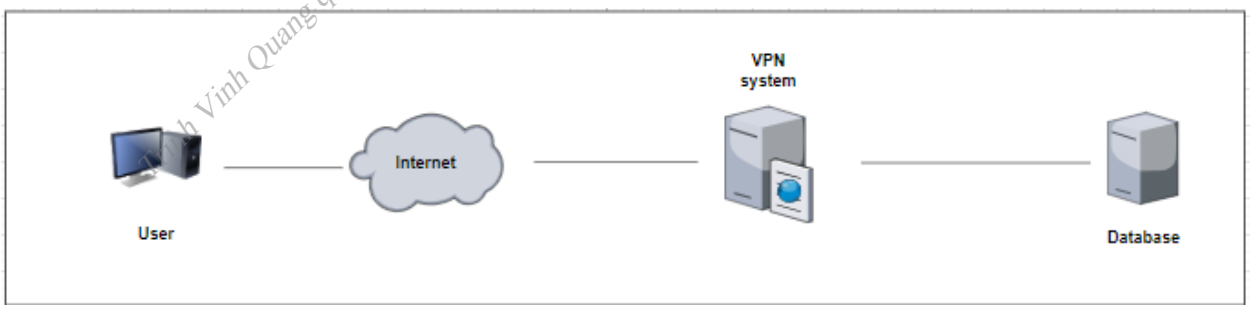


2.2 Mô hình kết nối

- Trường hợp 1: Kết nối truy cập đến Database và quản trị ứng dụng

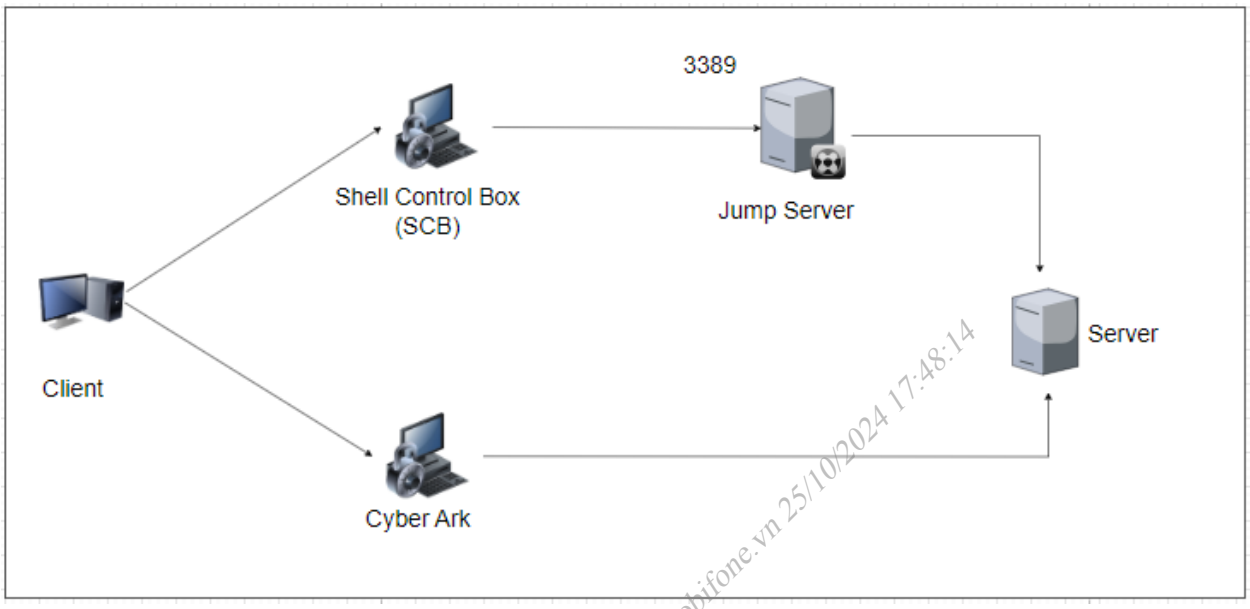


- Từ máy người dùng (Client) kết nối qua SCB (theo hướng dẫn tại *mục 3.2.2*) hoặc kết nối qua Cyber Ark (theo hướng dẫn tại mục 3.2.1) tới máy chủ Jump Server (port 3389).
- Từ máy chủ Jump Server kết nối đến Database hệ thống.
- Với trường hợp đặc biệt đơn vị không có máy chủ Jump Server có thể thực hiện truy cập qua VPN MobiFone để kết nối đến Database theo mô hình sau:



Trường hợp này máy máy PC cần đảm bảo tuân thủ theo đúng quy chế ATTT đã ban hành

- Trường hợp 2: Kết nối truy cập tới Server



II. HƯỚNG DẪN ĐẢM BẢO AN TOÀN BẢO MẬT CHO HỆ ĐIỀU HÀNH LINUX

1. Cấu hình ban đầu

1.1. Cấu hình tập tin hệ thống (file system)

1.1.1. Vô hiệu quá filesystems không sử dụng

1.1.1.1. Vô hiệu hóa mount với cramfs filesystems

Đánh giá :

- Level 1

Mô tả :

Hệ thống file cramfs là một hệ thống file nén chỉ đọc trên Linux, có thể được cài đặt trong các thiết bị flash. Đặc tính của cramfs là đơn giản và hiệu quả về không gian lưu trữ. Hệ thống file này được dùng trong các thiết kế nhúng kích thước nhỏ.

Mục đích :

Việc cài đặt nhiều hardware/software, mở nhiều program/service/connection không cần thiết sẽ làm tăng khả năng các lỗ hổng có thể tồn tại trong các "đối tượng" do đó có thể bị hacker khai thác. Vì vậy, nên disables nếu hệ thống files cramfs không cần thiết sử dụng.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Xác thực hệ thống file cramfs đã được disables:

```
#/sbin/modprobe -n -v cramfs
install /bin/true
#/sbin/lsmod | grep cramfs
<No output>
```

Khắc phục :

Tạo file `/etc/modprobe.d/CIS.conf` và thêm dòng:

```
install cramfs /bin/true
```

Unload cramfs module :

```
#rmmod cramfs
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

- **Moule được tải như thế nào**

```
# modprobe -n -v cramfs | grep "^install"
install /bin/false
```

- **Moule hiện tại đã được tải chưa**

```
# lsmod | grep cramfs
<No output>
```

- **Moule có bị đưa vào Blacklist không**

```
# grep -E "^blacklist\s+cramfs" /etc/modprobe.d/*
blacklist cramfs
```

Khắc phục :

Chỉnh sửa hoặc tạo một tệp trong thư mục `/etc/modprobe.d/` kết thúc bằng `.conf` với một dòng ghi là `install cramfs /bin/false` và một dòng ghi là `blacklist cramfs`.

```
# printf "install cramfs /bin/false
blacklist cramfs
" >> /etc/modprobe.d/cramfs.conf
```

Chạy lệnh sau để gỡ bỏ module `cramfs`:

```
# modprobe -r cramfs
```


1.1.1.2. Vô hiệu hóa mount của squashfs filesystems

Đánh giá :

- Level 2

Mô tả :

Hệ thống file squashfs (tương tự như cramfs) là một hệ thống file nén chỉ đọc trên Linux, có thể được cài đặt trong các thiết bị flash. Đặc tính của squashfs là đơn giản và hiệu quả về không gian lưu trữ. Hệ thống file này được dùng trong các thiết kế nhúng kích thước nhỏ.

Mục đích :

Việc cài đặt nhiều hardware/software, mở nhiều program/service/connection không cần thiết sẽ làm tăng khả năng các lỗ hổng có thể tồn tại trong các "đối tượng" do đó có thể bị hacker khai thác. Vì vậy, nên disables nếu hệ thống files squashfs không cần thiết sử dụng.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Xác thực hệ thống file cramfs đã được disables:

```
#/sbin/modprobe -n -v squashfs
install /bin/true
#/sbin/lsmod | grep squashfs
<No output>
```

Khắc phục :

Tạo file `/etc/modprobe.d/CIS.conf` và thêm dòng:

```
install squashfs /bin/true
```

Unload cramfs module :

```
#rmmod squashfs
```


- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

- **Moule được tải như thế nào**

```
# modprobe -n -v squashfs | grep "^install"
install /bin/false
```

- **Moule hiện tại đã được tải chưa**

```
# lsmod | grep squashfs
<No output>
```

- **Moule có bị đưa vào Blacklist không**

```
# grep -E "^blacklist\s+squashfs" /etc/modprobe.d/*
/etc/modprobe.d/squashfs.conf:blacklist squashfs
```

Khắc phục :

Chỉnh sửa hoặc tạo một tệp trong thư mục `/etc/modprobe.d/` kết thúc bằng `.conf` với một dòng ghi là `install squashfs /bin/false` và một dòng ghi là `blacklist squashfs`.

```
# printf "install squashfs /bin/false
blacklist squashfs
" >> /etc/modprobe.d/squashfs.conf
```

Chạy lệnh sau để gỡ bỏ module `squashfs.conf`:

```
# modprobe -r squashfs
```

1.1.1.3. Vô hiệu hóa mount với udf filesystems

Đánh giá :

- Level 1

Mô tả :

Hệ thống file udf (universal disk format) là hệ thống định dạng hỗ trợ việc copy dữ liệu (burn) đĩa CD, DVD hay các thiết bị khác. Định dạng này cho phép chỉnh sửa sau khi đã burn trên thiết bị.

Mục đích :

Việc cài đặt nhiều hardware/software, mở nhiều program/service/connection không cần thiết sẽ làm tăng khả năng các lỗ hổng có thể tồn tại trong các "đối tượng" do đó có thể bị hacker khai thác. Vì vậy, nên disables nếu hệ thống files udf không cần thiết sử dụng.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Xác thực hệ thống file udf đã được disables:

```
#/sbin/modprobe -n -v udf
install /bin/true
#/sbin/lsmod | grep udf
<No output>
```

Khắc phục :

Tạo file `/etc/modprobe.d/CIS.conf` và thêm dòng:

```
install udf /bin/true
```

Unload cramfs module :

```
#rmmod udf
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

- **Moule được tải như thế nào**

```
# modprobe -n -v udf | grep "^install"
install /bin/false
```

- **Moule hiện tại đã được tải chưa**

```
# lsmod | grep udf
<No output>
```

- **Moule có bị đưa vào Blacklist không**

```
# grep -E "^blacklist[[:blank:]]*udf" /etc/modprobe.d/*
/etc/modprobe.d/udf.conf:blacklist udf
```

Khắc phục :

Chỉnh sửa hoặc tạo một tệp trong thư mục `/etc/modprobe.d/` kết thúc bằng `.conf` với một dòng ghi là `install udf /bin/false`.

```
# printf "install udf /bin/false
blacklist udf
" >> /etc/modprobe.d/udf.conf
```

Chạy lệnh sau để gỡ bỏ module `udf`:

```
# modprobe -r udf
```

1.1.2. Đảm bảo phân vùng /tmp được cấu hình

Đánh giá :

- Level 1

Mô tả :

Thư mục /tmp dùng để lưu lại các tập tin được tạo ra tạm thời (temporary files). Thư mục này được thiết lập quyền được ghi bởi tất cả các user (world-writable).

Mục đích :

Hacker có thể sử dụng các thư mục tạm thời như /tmp để lưu trữ hoặc thực thi các phần mềm độc hại. Do đó khi tạo partition cùng với thiết lập các option noexc (không gán quyền thực thi cho các file nhị phân trên phân vùng được mount), quyền nodev (không cho phép các thiết bị kiểu character hoặc kiểu block sử dụng trên phân vùng này), nosuid (các SUID/SGID sẽ mất hiệu lực trên phân vùng) sẽ ngăn chặn việc hacker chạy các file mã độc hại lưu trên phân vùng. Cũng như hacker có thể tạo hardlink đến các chương trình hệ thống được setuid để dò lỗ hổng bảo mật của chương trình tiếp tục tấn công vào hệ thống. Mặt khác, các file trong thư mục /tmp có thể được thực thi bởi tất cả các user (world-writable) nên có thể dẫn đến việc hết dung lượng ổ cứng nếu không tạo một phân vùng riêng cho thư mục.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Xác thực phân vùng /tmp được cấu hình trong file /etc/fstab:

```
# cat /etc/fstab |grep tmp
Or
#systemctl show "tmp.mount" | grep -i unitfilestate
```

Khắc phục :

Thêm dòng sau vào file `/etc/fstab` :

```
tmpfs /tmp tmpfs nosuid,nodev,noexec 0 0
```

Nếu systemd file `tmp.mount` : được sử dung, xóa file : `/etc/systemd/system/tmp.mount`

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Chạy lệnh sau và xác minh đầu ra hiển thị `/tmp` đến tmpfs hoặc một phân vùng hệ thống:

```
# findmnt --kernel /tmp
TARGET SOURCE FSTYPE OPTIONS
/tmp tmpfs tmpfs rw,nosuid,nodev,noexec,relatime,seclabel
```

Đảm bảo rằng systemd sẽ gắn phân vùng `/tmp` khi khởi động:

```
# systemctl is-enabled tmp.mount
static
```

Lưu ý rằng theo mặc định, systemd sẽ xuất ra cấu hình được tạo nếu có một mục trong `/etc/fstab cho /tmp`. Điều này có nghĩa là systemd sẽ sử dụng mục trong `/etc/fstab` thay vì tệp cấu hình đơn vị mặc định của nó cho `/tmp`.

Khắc phục :

Đầu tiên, hãy đảm bảo rằng systemd được cấu hình chính xác để phân vùng `/tmp` sẽ được gắn khi khởi động.

```
# systemctl unmask tmp.mount
```

Đối với các yêu cầu cấu hình cụ thể của phân vùng `/tmp` cho môi trường của bạn, hãy sửa đổi `/etc/fstab`.

Ví dụ về việc sử dụng `tmpfs` với các tùy chọn gắn kết cụ thể:

```
tmpfs                                   /tmp                                    tmpfs
defaults,rw,nosuid,nodev,noexec,relatime,size=2G 0 0
```

Ví dụ về việc sử dụng một phân vùng hoặc đĩa với các tùy chọn gắn kết cụ thể. Vị trí nguồn của phân vùng hoặc đĩa sẽ thay đổi tùy theo môi trường của bạn.

```
<device> /tmp <fstype> defaults,nodev,nosuid,noexec 0 0
```


1.1.3. Thiết lập tùy chọn nodev cho phân vùng /tmp

Đánh giá :

- Level 1

Mô tả :

Tùy chọn nodev sẽ không cho phép các thiết bị kiểu character hoặc block được thiết lập cho phân vùng được mount.

Mục đích :

Thiết lập quyền nodev để đảm bảo không cho phép user tạo các kết nối với các thiết bị kiểu character hoặc kiểu block sử dụng trên phân vùng này.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Xác thực option nodev cho phân vùng /tmp được cấu hình trong file /etc/fstab:

```
# cat /etc/fstab |grep tmp |grep nodev
# mount |grep tmp |grep nodev
```

Nếu câu lệnh thực thi không có ouput thì tức là hệ thống chưa được cấu hình mount tùy chọn nodev cho phân vùng /tmp

Khắc phục :

```
#mount -o remount,nodev /tmp
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Xác minh rằng tùy chọn nodev đã được thiết lập cho phân vùng /tmp.

Chạy lệnh sau để xác minh rằng tùy chọn nodev đã được thiết lập:

```
# findmnt --kernel /tmp | grep nodev
/tmp tmpfs tmpfs rw,nosuid,nodev,noexec,relatime,seclabel
```

Khắc phục :

Chỉnh sửa tệp /etc/fstab và thêm nodev vào trường thứ tư (tùy chọn gắn kết) cho phân vùng /tmp.

```
<device>                        /tmp                        <fstype>
defaults,rw,nosuid,nodev,noexec,relatime 0 0
```

Chạy lệnh sau để gắn lại phân vùng /tmp với các tùy chọn đã cấu hình:

```
# mount -o remount /tmp
```

1.1.4. Thiết lập tùy chọn nosuid cho phân vùng /tmp

Đánh giá :

- Level 1

Mô tả :

Tùy chọn nosuid để đảm bảo phân vùng được mount sẽ không lưu các file được set userid.

Mục đích :

Thiết lập quyền nosuid để đảm bảo không cho phép user tạo hoặc thiết lập userid cho file trong phân vùng này. Bởi các file được thiết lập setuserid thì sẽ có thể được chay bởi bất kì một user nào kể cả không phải chủ sở hữu của file. Do đó, hacker có thể lợi dụng tạo một hardlink đến các file được thiết lập có quyền userid để thực hiện việc dò lỗ hổng tấn công vào hệ thống.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Xác thực option nosuid cho phân vùng /tmp được cấu hình trong file /etc/fstab:

```
# cat /etc/fstab |grep tmp |grep nosuid
# mount |grep tmp |grep nosuid
```

Nếu câu lệnh thực thi không có ouput thì tức là hệ thống chưa được cấu hình mount tùy chọn nosuid cho phân vùng /tmp

Khắc phục :

```
# mount -o remount,nosuid /tmp
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Xác minh rằng tùy chọn nosuid đã được thiết lập cho phân vùng /tmp.

Chạy lệnh sau để xác minh rằng tùy chọn nosuid đã được thiết lập:

```
# findmnt --kernel /tmp | grep nosuid
/tmp tmpfs tmpfs rw,nosuid,nodev,noexec,relatime,seclabel
```

Khắc phục :

Chỉnh sửa tệp /etc/fstab và thêm nosuid vào trường thứ tư (tùy chọn gắn kết) cho phân vùng /tmp.

```
  <device>                        /tmp                        <fstype>
defaults,rw,nosuid,nodev,noexec,relatime 0 0
```

Chạy lệnh sau để gắn lại phân vùng /tmp với các tùy chọn đã cấu hình:

```
  # mount -o remount /tmp
```


1.1.5. Thiết lập tùy chọn noexec cho phân vùng /tmp

Đánh giá :

- Level 1

Mô tả :

Tùy chọn noexec để đảm bảo phân vùng được mount sẽ không lưu các file dạng binaries.

Mục đích :

Thiết lập quyền noexec để đảm bảo không cho phép user chạy các chương trình dạng binary trong thư mục để đảm bảo hacker không thể chạy các phần mềm độc hại dưới dạng binary trên hệ thống.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Xác thực option noexec cho phân vùng /tmp được cấu hình trong file /etc/fstab:

```
  # cat /etc/fstab |grep tmp |grep noexec
  # mount |grep tmp |grep noexec
```

Nếu câu lệnh thực thi không có ouput thì tức là hệ thống chưa được cấu hình mount tùy chọn noexec cho phân vùng /tmp

Khắc phục :

```
  # mount -o remount, noexec /tmp
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Xác minh rằng tùy chọn noexec đã được thiết lập cho phân vùng /tmp.

Chạy lệnh sau để xác minh rằng tùy chọn noexec đã được thiết lập:

```
# findmnt --kernel /tmp | grep noexec
/tmp tmpfs tmpfs rw,nosuid,nodev,noexec,relatime,seclabel
```

Khắc phục :

Chỉnh sửa tệp /etc/fstab và thêm noexec vào trường thứ tư (tùy chọn gắn kết) cho phân vùng /tmp.

```
<device>                        /tmp                        <fstype>
defaults,rw,nosuid,nodev,noexec,relatime 0 0
```

Chạy lệnh sau để gắn lại phân vùng /tmp với các tùy chọn đã cấu hình:

```
# mount -o remount /tmp
```


1.1.6. Đảm bảo phân vùng /dev/shm được cấu hình

Đánh giá :

- Level 1

Mô tả :

Thư mục /dev/shm là thư mục chia sẻ vùng memory. Thư mục này được các tiến trình truy cập chia sẻ dùng chung.

Mục đích :

Bất kỳ user đều có thể upload and execute file trong thư mục /dev/shm như trong thư mục /tmp. Do đó khi tạo partition cùng với thiết lập các option noexc (không gán quyền thực thi cho các file nhị phân trên phân vùng được mount), quyền nodev (không cho phép các thiết bị kiểu character hoặc kiểu block sử dụng trên phân vùng này), nosuid (các SUID/SGID sẽ mất hiệu lực trên phân vùng) sẽ ngăn chặn việc hacker chạy các file mã độc hại lưu trên phân vùng. Cũng như hacker có thể tạo hardlink đến các chương trình hệ thống được setuid để dò lỗ hổng bảo mật của chương trình tiếp tục tấn công vào hệ thống.

- **Đối tượng áp dụng**: CentOS 7 và CentOS 8

Kiểm tra :

Xác thực phân vùng /tmp được cấu hình trong file /etc/fstab:

```
#findmnt -n /dev/shm
```

```
Or
#grep -E '\s/dev/shm\s' /etc/fstab
```

Khắc phục :

Thêm dòng sau vào file `/etc/fstab` :

```
tmpfs /dev/shm tmpfs defaults,noexec,nodev,nosuid,seclabel 0
0
```

1.1.7. Thiết lập tùy chọn nodev cho phân vùng /dev/shm

Đánh giá :

- Level 1

Mô tả :

Tùy chọn nodev sẽ không cho phép các thiết bị kiểu character hoặc block được thiết lập cho phân vùng được mount.

Mục đích :

Thiết lập quyền nodev để đảm bảo không cho phép user tạo các kết nối với các thiết bị kiểu character hoặc kiểu block sử dụng trên phân vùng này.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Xác thực option nodev cho phân vùng /dev/shm được cấu hình trong file /etc/fstab:

```
# cat /etc/fstab |grep /dev/shm |grep nodev
# findmnt -n /dev/shm | grep nodev
```

Nếu câu lệnh thực thi không có ouput thì tức là hệ thống chưa được cấu hình mount tùy chọn nodev cho phân vùng /dev/shm

Khắc phục :

```
#mount -o remount,noexec,nodev,nosuid /dev/shm
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Xác minh rằng tùy chọn nodev đã được thiết lập nếu phân vùng /dev/shm tồn tại.

Chạy lệnh sau và xác minh rằng không có gì được trả về:

```
# mount | grep -E '\s/dev/shm\s' | grep -v nodev
```

Khắc phục :

Chỉnh sửa tệp /etc/fstab và thêm nodev vào trường thứ tư (tùy chọn gắn kết) cho phân vùng /dev/shm. Xem trang hướng dẫn fstab(5) để biết thêm thông tin.

Chạy lệnh sau để gắn lại phân vùng /dev/shm với các tùy chọn đã cập nhật từ /etc/fstab:

```
# mount -o remount /dev/shm
```

1.1.8. Thiết lập tùy chọn nosuid cho phân vùng /dev/shm

Đánh giá :

- Level 1

Mô tả :

Tùy chọn nosuid để đảm bảo phân vùng được mount sẽ không lưu các file được set userid.

Mục đích :

Thiết lập quyền nosuid để đảm bảo không cho phép user tạo hoặc thiết lập userid cho file trong phân vùng này. Bởi các file được thiết lập setuserid thì sẽ có thể được chay bởi bất kì một user nào kể cả không phải chủ sở hữu của file. Do đó, hacker có thể lợi dụng tạo một hardlink đến các file được thiết lập có quyền userid để thực hiện việc dò lỗ hổng tấn công vào hệ thống.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Xác thực option nosuid cho phân vùng /dev/shm được cấu hình trong file /etc/fstab:

```
# cat /etc/fstab |grep /dev/shm |grep nosuid
# findmnt -n /dev/shm | grep nosuid
```

Nếu câu lệnh thực thi không có ouput thì tức là hệ thống chưa được cấu hình mount tùy chọn nosuid cho phân vùng /dev/shm

Khắc phục :

```
# mount -o remount,noexec,nodev,nosuid /dev/shm
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Xác minh rằng tùy chọn nosuid đã được thiết lập nếu phân vùng /dev/shm tồn tại.

Chạy lệnh sau và xác minh rằng không có gì được trả về:

```
# mount | grep -E '\s/dev/shm\s' | grep -v nosuid
```

Khắc phục :

Chỉnh sửa tệp /etc/fstab và thêm nodev vào trường thứ tư (tùy chọn gắn kết) cho phân vùng /dev/shm. Xem trang hướng dẫn fstab(5) để biết thêm thông tin.

Chạy lệnh sau để gắn lại phân vùng /dev/shm với các tùy chọn đã cập nhật từ /etc/fstab:

```
# mount -o remount /dev/shm
```


1.1.9. Thiết lập tùy chọn noexec cho phân vùng /dev/shm

Đánh giá :

- Level 1

Mô tả :

Tùy chọn noexec để đảm bảo phân vùng được mount sẽ không lưu các file dạng binaries.

Mục đích :

Thiết lập quyền noexec để đảm bảo không cho phép user chạy các chương trình dạng binary trong thư mục để đảm bảo hacker không thể chạy các phần mềm độc hại dưới dạng binary trên hệ thống.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Xác thực option noexec cho phân vùng /dev/shm được cấu hình trong file /etc/fstab:

```
# cat /etc/fstab |grep /dev/shm |grep noexec
# findmnt -n /dev/shm |grep noexec
```

Nếu câu lệnh thực thi không có ouput thì tức là hệ thống chưa được cấu hình mount tùy chọn noexec cho phân vùng /dev/shm

Khắc phục :

```
# mount -o remount,noexec,nodev,nosuid /dev/shm
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Xác minh rằng tùy chọn noexec đã được thiết lập cho phân vùng /dev/shm.

Chạy lệnh sau để xác minh rằng tùy chọn noexec đã được thiết lập:

```
# findmnt --kernel /dev/shm | grep noexec
/dev/shm tmpfs tmpfs rw,nosuid,nodev,noexec,relatime,seclabel
```

Khắc phục :

Chỉnh sửa tệp /etc/fstab và thêm noexec vào trường thứ tư (tùy chọn gắn kết) cho phân vùng /dev/shm.

```
<device>                    /dev/shm                    <fstype>
defaults,rw,nosuid,nodev,noexec,relatime 0 0
```

Chạy lệnh sau để gắn lại phân vùng /dev/shm với các tùy chọn đã cấu hình:

```
# mount -o remount /dev/shm
```

LƯU Ý: Được khuyến nghị sử dụng tmpfs làm loại thiết bị/hệ thống tập tin vì /dev/shm được sử dụng làm không gian bộ nhớ chia sẻ bởi các ứng dụng.

1.1.10. Đảm bảo phân vùng /var được cấu hình

Đánh giá :

- Level 2

Mô tả :

Thư mục var để lưu lại tập tin ghi các số liệu biến đổi (variable files) như các tập tin dữ liệu và tập tin bản ghi (logs and databases). Một vài process trong thư mục /var có thể được thiết lập quyền ghi bởi tất cả các user (world-writable).

Mục đích :

Do một số files hoặc thư mục trong thư mục /var được gán quyền world-wriables nên có thể sẽ bị hacker lợi dụng để tấn công hệ thống cũng như việc tạo quá nhiều dữ liệu trong thư mục dẫn đến cạn kiệt tài nguyên nên cần tạo phân vùng cho thư mục này.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Xác thực phân vùng /var được cấu hình trong file /etc/fstab:

```
#findmnt /var
Or
# cat /etc/fstab |grep var
```

Khắc phục :

Tạo partition và mount point với /var ngay từ đâu khi install hệ điều hành

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Chạy lệnh sau và xác minh rằng đầu ra hiển thị /var đã được gắn:

```
# findmnt --kernel /var
TARGET SOURCE FSTYPE OPTIONS
/var /dev/sdb ext4 rw,relatime,seclabel,data=ordered
```

Khắc phục :

Đối với các cài đặt mới, trong quá trình cài đặt hãy tạo một cấu hình phân vùng tùy chỉnh và chỉ định một phân vùng riêng biệt cho /var.

Đối với các hệ thống đã được cài đặt trước đó, hãy tạo một phân vùng mới và cấu hình /etc/fstab theo cách phù hợp.

1.1.11. Thiết lập tham số liên kết (bind) khi mount /var/tmp vào thư mục /tmp

Đánh giá :

- Level 1

Mô tả :

Thư mục /var/tmp là một thư mục độc lập với thư mục /var. Thiết lập liên kết giữa /var/tmp với /tmp sẽ cho phép thư mục /var/tmp kế thừa các option của /tmp. Tất cả các chương trình sử dụng trong /var/tmp và /tmp thực hiện đọc, ghi các files tạm thời sẽ luôn được ghi vào /tmp.

Mục đích :

Để ngăn việc người dùng tạo quá nhiều file trong /var/tmp vượt quá dung lượng cấp phát hoặc cố gắng để thực thi các files đã bị giới hạn được phân quyền trong phân vùng /tmp..

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Xác thực cấu hình trong file /etc/fstab:

```
#findmnt /var/tmp
#cat /etc/fstab |grep tmp |grep /var/tmp
#mount |grep tmp |grep /var/tmp
```

Nếu câu lệnh thực thi không có ouput thì hệ thống chưa được cấu hình tham số bind thư mục /var/tmp với thư mục /tmp

Khắc phục :

```
# mount --bind /tmp /var/tmp
```

Chỉnh sửa file /etc/fstab thêm dòng:

```
# /tmp /var/tmp none bind 0 0
```


1.1.12. Tạo partition cho thư mục /var/log

Đánh giá :

- Level 2

Mô tả :

Thư mục /var/log được sử dụng để lưu log của hệ thống.

Mục đích :

Việc tạo partition cho thư mục /var/log nhằm đảm bảo log hệ thống được lưu trữ không chiếm hết tài nguyên hệ thống và bảo vệ các dữ liệu audit.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Xác thực phân vùng /var/log được cấu hình trong file /etc/fstab:

```
#findmnt /var/log
Or
# cat /etc/fstab |grep /var/log
```

Khắc phục :

Tạo partition và mount point với /var/log ngay từ đâu khi install hệ điều hành.

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Chạy lệnh sau và xác minh rằng đầu ra hiển thị /var/log đã được gắn:

```
# findmnt --kernel /var/log
TARGET SOURCE FSTYPE OPTIONS
/var/log /dev/sdb ext4 rw,relatime,seclabel,data=ordered
```

Khắc phục :

Đối với các cài đặt mới, trong quá trình cài đặt hãy tạo một cấu hình phân vùng tùy chỉnh và chỉ định một phân vùng riêng biệt cho /var/log.

Đối với các hệ thống đã được cài đặt trước đó, hãy tạo một phân vùng mới và cấu hình /etc/fstab theo cách phù hợp.

1.1.13. Tạo partition cho thư mục /var/log/audit

Đánh giá :

- Level 2

Mô tả :

Thư mục /var/log/audit được sử dụng để lưu log của daemon auditd.

Mục đích :

Việc tạo partition cho thư mục /var/log/audit nhằm đảm bảo log hệ thống được lưu trữ không chiếm hết tài nguyên hệ thống khi file audit.log tăng lên và bảo vệ các dữ liệu audit.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Xác thực phân vùng /var/log/audit được cấu hình trong file /etc/fstab:

```
#findmnt /var/log/audit
Or
# cat /etc/fstab |grep /var/log/audit
```

Khắc phục :

Tạo partition và mount point với /var/log/audit ngay từ đâu khi install hệ điều hành.

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Chạy lệnh sau và xác minh rằng đầu ra hiển thị /var/log/audit đã được gắn:


```
# findmnt --kernel /var/log/audit
TARGET SOURCE FSTYPE OPTIONS
/var/log/audit                /dev/sdb                ext4
rw,relatime,seclabel,data=ordered
```

Khắc phục :

Đối với các cài đặt mới, trong quá trình cài đặt hãy tạo một cấu hình phân vùng tùy chỉnh và chỉ định một phân vùng riêng biệt cho /var/log/audit.

Đối với các hệ thống đã được cài đặt trước đó, hãy tạo một phân vùng mới và cấu hình /etc/fstab cho phù hợp..

1.1.14. Tạo partition cho thư mục /home

Đánh giá :

- Level 2

Mô tả :

Thư mục /home được sử dụng để lưu file của user trong hệ thống.

Mục đích :

Việc tạo partition cho thư mục /home nhằm đảm bảo các file được user lưu trữ sẽ không chiếm hết tài nguyên hệ thống và giới hạn các quyền user được phép thực thi với thư mục /home của user bằng việc thiết lập các option khi thực hiện mount.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Xác thực phân vùng /home được cấu hình trong file /etc/fstab:

```
#findmnt /home
Or
# cat /etc/fstab |grep /home
```

Khắc phục :

Tạo partition và mount point với /home ngay từ đâu khi install hệ điều hành

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Chạy lệnh sau và xác minh rằng đầu ra hiển thị /home đã được gắn:

```
# findmnt --kernel /home
TARGET SOURCE FSTYPE OPTIONS
/home /dev/sdb ext4 rw,relatime,seclabel
```

Khắc phục :

For new installations, during installation create a custom partition setup and specify a separate partition for /home.

For systems that were previously installed, create a new partition and configure /etc/fstab as appropriate.

1.1.15. Thiết lập tùy chọn nodev cho /home

Đánh giá :

- Level 1

Mô tả :

Tùy chọn nodev sẽ không cho phép các thiết bị kiểu character hoặc block được thiết lập cho phân vùng được mount.

Mục đích :

Thiết lập quyền nodev để đảm bảo không cho phép user tạo các kết nối với các thiết bị kiểu character hoặc kiểu block sử dụng trên phân vùng này.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Xác thực option nodev cho phân vùng /home được cấu hình trong file /etc/fstab:

```
# cat /etc/fstab |grep /home |grep nodev
# findmnt -n /home | grep nodev
```

Nếu câu lệnh thực thi không có ouput thì tức là hệ thống chưa được cấu hình mount tùy chọn nodev cho phân vùng /home

Khắc phục :

```
#mount -o remount,nodev /home
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Xác minh rằng tùy chọn nodev đã được thiết lập cho phân vùng /home.

Chạy lệnh sau để xác minh rằng tùy chọn nodev đã được thiết lập:

```
# findmnt --kernel /home| grep nodev
/home /dev/sdb ext4 rw,nosuid,nodev,noexec,relatime,seclabel
```

Khắc phục :

Chỉnh sửa tệp /etc/fstab và thêm nodev vào trường thứ tư (tùy chọn gắn kết) cho phân vùng /home.

```
<device>                    /home                    <fstype>
defaults,rw,nosuid,nodev,noexec,relatime 0 0
```

Chạy lệnh sau để gắn lại phân vùng /home với các tùy chọn đã cấu hình:

```
# mount -o remount /home
```


1.1.16. Thiết lập sticky bit trên tất cả các thư mục world-writable

Đánh giá :

- Level 1

Mô tả :

Thiết lập Sticky bit trên các thư mục world-writable nhằm mục đích các users có thể đọc hoặc ghi vào các file trong thư mục nhưng các user không thể đổi tên hoặc xóa các file không thuộc quyền sở hữu (owner) của user. User chỉ có thể xóa hoặc đổi tên các file do chính user đấy tạo ra.

Mục đích :

Để tăng thêm tính private cho các user trong các thư mục world-writable như /tmp.

- **Đối tượng áp dụng**: CentOS 7 và CentOS 8

Kiểm tra :

Đảm bảo sticky được cấu hình cho thư mục world-writable:

```
# df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev -type d \( -perm -0002 -a ! -perm -1000 \) 2>/dev/null
```

Nếu câu lệnh thực thi không có ouput thì tức là hệ thống đã thiết lập.

Khắc phục :

```
# df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -type d \( -perm -0002 -a ! -perm -1000 \) 2>/dev/null | xargs -I '{}' chmod a+t '{}'
```

1.2. Kiểm tra tính toàn vẹn của filesystem

AIDE là một công cụ kiểm tra tính toàn vẹn của file tương tự như Tripwire. AIDE không thể ngăn chặn việc xâm nhập mà chỉ có thể phát hiện được những thay đổi trái phép trong file cấu hình và thực hiện cảnh báo.

1.2.1. Cài đặt AIDE

Đánh giá :

- Level 1

Mô tả :

AIDE là một tool để kiểm tra tính toàn vẹn của file. Khi có bất kì thay đổi nào trong cấu hình files, AIDE sẽ phát hiện và thông báo cho người quản trị.

Mục đích :

Sử dụng AIDE để theo dõi các tập tin quan trọng mà việc thay đổi cấu hình các tập tin này có thể ảnh hưởng đến sự an toàn của hệ thống.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Xác thực AIDE đã được cài đặt:

```
# rpm -q aide
```

Nếu câu lệnh thực thi không có ouput thì tức là hệ thống chưa được cài đặt.

Khắc phục :

```
# yum install aide
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Xác thực AIDE đã được cài đặt:

```
# rpm -q aide
```

Nếu câu lệnh thực thi không có ouput thì tức là hệ thống chưa được cài đặt.

Khắc phục :

```
# dnf install aide
```

1.2.2. Lập lịch kiểm tra định kỳ filesystem với AIDE

Đánh giá :

- Level 1

Mô tả :

Lập lịch định kì kiểm tra tính toàn vẹn của files.

Mục đích :

Lập lịch kiểm tra định kì đảm bảo cho người quản trị hệ thống nắm được thông tin khi có bất cứ sự thay đổi trong cấu hình files.

- **Đối tượng áp dụng**: CentOS 7 và 8

Kiểm tra :

Đảm bảo AIDE được lập lịch kiểm tra định kì:

```
# crontab -u |grep aide
```

Nếu câu lệnh thực thi không có ouput thì tức là hệ thống chưa được lập lịch.

Khắc phục :

Chỉnh sửa thêm dòng sau vào crontab :

```
# 0 5 * * * /usr/sbin/aide --check
```

1.3. Bổ sung tiến trình hardening

1.3.1. Giới hạn coredump

Đánh giá :

- Level 1

Mô tả :

Core dump là bộ nhớ của một chương trình thực thi. Nó thường được sử dụng để xác định tại sao một chương tình bị hủy bỏ. Nó cũng được sử dụng thu nhận các thông tin từ core file. Hệ thống cung cấp khả năng thiết lập soft limit cho coredump, nhưng thiết lập này có thể bị ghi đè bởi user.

Mục đích :

Thiết lập hard limit trên core dumps để ngăn user ghi đè lên các giá trị soft limit. Nếu core dumps được yêu cầu, xem xét thiết lập giới hạn cho nhóm user. Thêm vào đó, thiết lập giá trị fs.suid_dumpable = 0 để ngăn setuid từ dumping core.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Xác định core dump đã được giới hạn:

```
# grep "hard core" /etc/security/limits.conf
* hard core 0
# sysctl fs.suid_dumpable
fs.suid_dumpable = 0
```

Kiểm tra hệ thống nếu systemd-coredump được cài đặt:

```
# systemctl is-enabled coredump.service
```

Nếu kết quả trả ra enable hoặc disabled là systemd-coredump đã được cài đặt

Khắc phục :

Thêm vào file cấu hình /etc/security/limits.conf dòng :

```
* hard core 0
```

Thêm vào file /etc/sysctl.conf dòng :

```
fs.suid_dumpable = 0
```

Nếu systemd-coredump được cài đặt sửa/thêm dòng sau vào file /etc/systemd/coredump.conf:

```
Storage=none
ProcessSizeMax=0
```

Chạy câu lệnh :

```
systemctl daemon-reload
```


1.3.2. Khởi động vị trí vùng nhớ ảo tự động

Đánh giá :

- Level 1

Mô tả :

Thiết lập cờ hệ thống để ngẫu nhiên tạo vị trí vùng bộ nhớ ảo.

Mục đích :

Ngẫu nhiên vị trí bộ nhớ ảo sẽ làm cho cho việc khai thác tấn công bộ nhớ trở nên khó khăn do vị trí bộ nhớ sẽ luôn thay đổi.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Xác định bộ nhớ ảo được thiết lập ngẫu nhiên:

```
#sysctl kernel.randomize_va_space
kernel.randomize_va_space = 2
```

Khắc phục :

Thêm vào file /etc/sysctl.conf dòng :

```
kernel.randomize_va_space = 2
```

Chạy câu lệnh để kích hoạt giá trị kernel :

```
sysctl -w kernel.randomize_va_space=2
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Chạy kịch bản sau để xác minh rằng kernel.randomize_va_space được thiết lập thành 2:

```
#!/usr/bin/env bash
{
```

```
   krp="" pafile="" fafile=""
   kpname="kernel.randomize_va_space"
   kpvalue="2"
   searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
   /usr/local/lib/sysctl.d/*.conf       /usr/lib/sysctl.d/*.conf
/lib/sysctl.d/*.conf
   /etc/sysctl.conf"
   krp="$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)"
   pafile="$(grep                        -Psl                          --
"^\h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?$"
   $searchloc)"
   fafile="$(grep -s -- "^\s*$kpname" $searchloc | grep -Pv -
   "\h*=\h*$kpvalue\b\h*" | awk -F: '{print $1}')"
   if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fafile"
]; then
   echo -e "\nPASS:\n\"$kpname\" is set to \"$kpvalue\" in the
running
   configuration and in \"$pafile\""
else
echo -e "\nFAIL: "
   [ "$krp" != "$kpvalue" ] && echo -e "\"$kpname\" is set to
\"$krp\" in
   the running configuration\n"
   [ -n "$fafile" ] && echo -e "\n\"$kpname\" is set incorrectly
in
   \"$fafile\""
   [ -z "$pafile" ] && echo -e "\n\"$kpname = $kpvalue\" is not
set in a
   kernel parameter configuration file\n"
   fi
   }
```


Khắc phục :

Thiết lập tham số sau trong tệp /etc/sysctl.conf hoặc một tệp trong thư mục /etc/sysctl.d/*:

```
   # printf "
   kernel.randomize_va_space = 2
   " >> /etc/sysctl.d/60-kernel_sysctl.conf
```

Chạy lệnh sau để thiết lập tham số kernel hiện tại:

```
# sysctl -w kernel.randomize_va_space=2
```

1.3.3. Đảm bảo prelink không được cài đặt

Đánh giá :

- Level 1

Mô tả :

Prelink là một chương trình sửa đổi các thư viện được chia sẻ ELF và các tệp nhị phân được liên kết động ELF.

Mục đích :

Prelink có thể can thiệp vào hoạt động của AIDE, vì nó thay đổi các tệp nhị phân. Prelink cũng có thể làm tăng lỗ hổng của hệ thống nếu người dùng có thể xâm nhập một thư viện chung như libc.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Xác định prelink không được cài đặt:

```
# rpm -q prelink
package prelink is not installed
```

Khắc phục :

Gỡ prelink khỏi hệ thống :

```
yum remove prelink
```

1.4. Mandatory Access Control

1.4.1. Cấu hình SELINUX

SELINUX cung cấp hệ thống MAC (Mandatory Access Control) có những chính sách bảo mật cao hơn so với mô hình DAC (Discretionary Access Control) mặc định. Khi sử dụng SELINUX, mỗi tiến trình, mỗi đối tượng (files, sockets, pipes) trên hệ thống được gán với một ngữ cảnh an ninh, với các label bao gồm các thông tin chi tiết về đối tượng. Kernel cho phép các truy cập các đối tượng chỉ khi được cho phép bởi chính sách có hiệu lực. Chính sách này xác định quá trình chuyển đổi xác định quá trình chuyển tiếp, tức là một user có thể được cho phép chạy phần mềm, những phần mềm đấy có thể chạy dưới một ngữ cảnh khác với user mặc định. Điều này sẽ hạn chế

các thiệt hại do phần mềm có thể tác động đến các file của user gọi thực hiện chạy phần mềm. Đối với mỗi tiến trình đã được thực hiện cần thỏa mãn cả hai quy tắc DAC và MAC. Một tiến trình sẽ không được cho phép thực thi nếu nó không thỏa mãn được một trong hai quy tắc này. Ba chính sách được được sử dụng với CentOS7 bao gồm: targeted, strict và mls.

1.4.1.1. Đảm bảo SELINUX được cài đặt

Đánh giá :

- Level 1

Mô tả :

SELINUX cung cấp hệ thống MAC (Mandatory Access Control).

Mục đích :

Nếu không có MAC (Mandatory Access Control), hệ thống chỉ sử dụng DAC (Discretionary Access Control) theo mặc định .

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Xác định SELinux được cài đặt:

```
#rpm -q libselinux
libselinux-<version>
```

Khắc phục :

Cài đặt SELinux :

```
# yum install libselinux
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Xác định SELinux được cài đặt:

```
#rpm -q libselinux
libselinux-<version>
```

Khắc phục :

Cài đặt SELinux :

```
# dnf install libselinux
```

1.4.1.2. Thiết lập chính sách SELINUX

Đánh giá :

- Level 1

Mô tả :

Cấu hình SELINUX mặc định được thiết lập ở mức targeted policy (sử dụng quy tắc TE và một phần nhỏ quy tắc RBAC nhằm giới hạn một số quyền thực thi của một vài chương trình nhưng không ảnh hưởng lớn đến users) hoặc nếu cần bảo mật hơn nữa có thể thiết lập ở là mức restrict (sử dụng quy tắc TE và RBASC trên nhiều chương trình và linh hoạt hơn).

Mục đích :

Cấu hình mặc định ở mức target policy để đảm bảo ít nhất có thể bảo mật hệ thống ở mức khuyến nghị. Còn đối với các trường hợp yêu cầu khắt khe hơn thì có thể thiết lập ở chính sách retrict.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Xác thực target policy được cấu hình trong file /etc/selinux/config:

```
# grep SELINUXTYPE=targeted /etc/selinux/config
SELINUXTYPE=targeted
#/usr/sbin/sestatus | grep 'Loaded policy'
Loaded policy name:             targeted
```

Khắc phục :

Chỉnh sửa file /etc/selinux/config và thiết lập tham số SELINUX:

```
SELINUXTYPE=targeted
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Chạy các lệnh sau và đảm bảo đầu ra khớp với "targeted" hoặc "mls":

```
# grep -E '^\s*SELINUXTYPE=(targeted|mls)\b'
/etc/selinux/config
SELINUXTYPE=targeted
# sestatus | grep Loaded
```

```
Loaded policy name: targeted
```

Khắc phục :

Chỉnh sửa file /etc/selinux/config và thiết lập tham số SELINUX:

```
SELINUXTYPE=targeted
```


1.4.1.3. Đảm bảo SELINUX được bật ở chế độ enforcing hoặc permissive

Đánh giá :

- Level 1

Mô tả :

SELINUX có thể chạy ở 3 chế độ :

- Enforcing: Chế độ mặc định sẽ cho phép và thực thi chính sách bảo mật SELinux trên hệ thống, từ chối các hành động truy cập. SELinux áp các policy trên toàn hệ thống và đảm bảo các truy nhập bởi các user và proceess không được chứng thực sẽ bị từ chối. Các truy cập bị từ chối sẽ được ghi vào log.

- Permissive: Trong chế độ Permissive, SELinux được kích hoạt nhưng sẽ không thực thi chính sách bảo mật, không từ chối bất kì truy nhập nào, chỉ cảnh báo và ghi lại log các hành động. Chế độ Permissive hữu ích cho việc khắc phục sự cố

- Disabled: SELinux bị vô hiệu hóa và không ghi lại log.

Mục đích :

Việc chạy SELinux ở chế độ bị vô hiệu hóa không được khuyến khích, hệ thống không chỉ không thực thi chính sách SELinux mà còn không ghi log các hành động truy nhập bởi các user và proceess không được chứng thực.

- **Đối tượng áp dụng**: CentOS 7 và 8

Kiểm tra :

Kiểm tra trạng thái SELinux:

```
#getenforce
Enforcing
-OR
Permissive
```

Hoặc kiểm tra trong file /etc/selinux/config :

```
#grep -Ei '^\s*SELINUX=(enforcing|permissive)' /etc/selinux/config
SELINUX=enforcing
-OR
SELINUX=permissive
```

Khắc phục :

Thiết lập SELinux ở chế độ Enforcing tạm thời:

```
setenforce 1
```

Thiết lập SELinux ở chế độ Enforcing cố định, Sửa file /etc/selinux.config dòng:

```
SELINUX=enforcing
```

Thiết lập SELinux ở chế độ Permissive tạm thời:

```
setenforce 0
```

Thiết lập SELinux ở chế độ Enforcing cố định, Sửa file /etc/selinux.config dòng:

```
SELINUX=permissive
```


1.4.1.4. Cấu hình SELINUX ở chế độ Enforcing

Đánh giá :

- Level 2

Mô tả :

SELINUX ở 3 chế độ Enforcing: Chế độ mặc định sẽ cho phép và thực thi chính sách bảo mật SELinux trên hệ thống, từ chối các hành động truy cập. SELinux áp các policy trên toàn hệ thống và đảm bảo các truy nhập bởi các user và proceess không được chứng thực sẽ bị từ chối. Các truy cập bị từ chối sẽ được ghi vào log.

Lệnh semodule được sử dụng để cài đặt, xóa, reload, upgrade, enable và disable các module SELinux policy. Ví dụ xem trạng thái đối với ftpd services bằng câu lệnh sau :

```
#semanage boolean -l | grep ftpd
```

Kiểm tra FTP user không có quyền full access, ftpd service cũng không thể chuyển sang chế độ passive mode sử dụng lệnh getsebool:

```
#getsebool ftpd_full_access
ftpd_full_access --> off
```

```
#getsebool ftpd_use_passive_mode
ftpd_use_passive_mode --> off
```

Để enable 2 tham số trên sử dụng setsebool:

```
#setsebool -P ftpd_full_access on
#setsebool -P ftpd_use_passive_mode on
```

Ví dụ thêm 1 port vào service http. Kiểm tra các port đang được SELinux cho phép :

```
#semanage port -l | grep -w http_port_t
Hoặc
#sepolicy network -t http_port_t
```

Kiểm tra port đã sử dụng:

```
# sepolicy network -p 8001
```

Cho phép httpd sử dụng port 8001 với các kết nối tcp:

```
# semanage port -a -t http_port_t -p tcp 8001
```

Không cho phép httpd sử dụng port 8001 với các kết nối tcp:

```
# semanage port -d -t http_port_t -p tcp 8001
```

Mục đích :

Việc chạy SELinux ở chế độ Enforcing bảo mật cao cho hệ thống nhưng người quản trị cần nắm rõ các services đang chạy trên hệ thống để mở quyền truy cập.

- **Đối tượng áp dụng**: CentOS 7 và 8

Kiểm tra :

Kiểm tra trạng thái SELinux:

```
#getenforce
Enforcing
```

Hoặc kiểm tra trong file /etc/selinux/config :

```
# grep -i SELINUX=enforcing /etc/selinux/config
SELINUX=enforcing
```

Khắc phục :

Thiết lập SELinux ở chế độ Enforcing tạm thời:

```
setenforce 1
```

Thiết lập SELinux ở chế độ Enforcing cố định, Sửa file /etc/selinux.config dòng:

```
SELINUX=enforcing
```

1.4.1.5. Xóa bỏ SETroubleshoot

Đánh giá :

- Level 1

Mô tả :

SETroubleshoot một dịch vụ chuẩn đoán lỗi của SELinux. Ứng dụng này sẽ đưa ra các thông báo trên desktop nếu như có vấn đề nào đó với SELinux (cấu hình lỗi, xâm nhập trái phép …).

Mục đích :

SETroubleshoot không phải là một dịch vụ quan trọng khi chạy trên server đặc biệt là khi X Windows không được sử dụng. Vì vậy có thể disable dịch vụ.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Đảm bảo SETroubleshoot không được cài đặt:

```
#rpm -q setroubleshoot
```

Khắc phục :

Gỡ SETroubleshoot :

```
# yum remove setroubleshoot
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Đảm bảo SETroubleshoot không được cài đặt:

```
#rpm -q setroubleshoot
```

Khắc phục :

Gỡ SETroubleshoot :

```
# dnf remove setroubleshoot
```

1.4.1.6. Xóa bỏ dịch vụ MSC Translation

Đánh giá :

- Level 1

Mô tả :

Mcstransd (SELinux Context Translation System Daemon) cung cấp các thông tin cho người sử dụng SELinux.

Mục đích :

Nếu dịch vụ này không thường xuyên được sử dụng, nên disable để giảm thiểu khả năng bị khai thác lỗ hổng.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Đảm bảo mcstrans không được cài đặt:

```
# rpm -q mcstrans
```

Khắc phục :

Gỡ mcstrans :

```
# yum remove mcstrans
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Đảm bảo mcstrans không được cài đặt:

```
# rpm -q mcstrans
```

Khắc phục :

Gỡ mcstrans :

```
# dnf remove mcstrans
```

1.5. Banner cảnh báo

Hiển thị thông tin cảnh báo trước khi người dùng đăng nhập có thể được những attacker lợi dụng những thông tin này để thực thực tấn công. Thay đổi banner đăng nhập ẩn thông tin phiên bản hệ điều hành hoặc một vài thông tin hệ thống để giảm thiểu ảnh hưởng việc attacker cố gắng tấn truy cập vào hệ thống.

1.5.1. Thiết lập banner cảnh báo cho các dịch vụ đăng nhập

Đánh giá :

- Level 1

Mô tả :

Nội dung của files /etc/issue được hiển thị trước khi đăng nhập vào PROMPT trên console hệ thống và các thiết bị serial, và cũng trước khi đăng nhập thông qua telnet. Nội dung của /etc/motd tập tin thường được hiển thị sau khi tất cả các thông tin đăng nhập thành công, thông tin này không có vấn đề với người dùng đang đăng nhập, nhưng được cho là ít hữu ích bởi vì nó chỉ cung cấp thông báo cho người sử dụng sau khi máy đã được truy nhập.

Mục đích :

Warning messages thông báo người dùng đang cố gắng để đăng nhập vào hệ thống về tình trạng pháp lý của họ liên quan đến hệ thống và phải bao gồm tên của tổ chức sở hữu các hệ thống và chính sách giám sát.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

```
# /bin/ls -l /etc/motd
-rw-r--r-- 1 root root 2055 May 09 16:30 /etc/motd
# ls /etc/issue
-rw-r--r-- 1 root root 2055 May 09 16:30 /etc/issue
# ls /etc/issue.net
-rw-r--r-- 1 root root 2055 May 09 16:30 /etc/issue.net
```

Khắc phục :

```
#touch /etc/motd
# echo "Authorized uses only. All activity may be \
monitored and reported." > /etc/motd
# echo "Authorized uses only. All activity may be \
monitored and reported." > /etc/issue
# echo "Authorized uses only. All activity may be \
monitored and reported." > /etc/issue.net
# chown root:root /etc/motd
# chmod 644 /etc/motd
# chown root:root /etc/issue
# chmod 644 /etc/issue
```

```
# chown root:root /etc/issue.net
# chmod 644 /etc/issue.net
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Chạy lệnh sau và xác minh rằng nội dung khớp với chính sách của trang:

```
# cat /etc/issue
```

Chạy lệnh sau và xác minh rằng không có kết quả nào được trả về:

```
# grep -E -i "(\\v|\\r|\\m|\\s|$(grep '^ID=' /etc/os-release | cut -d= -f2 | sed -e 's/"//g'))" /etc/issue
```

Khắc phục :

Chỉnh sửa tệp /etc/issue với nội dung phù hợp theo chính sách của trang của bạn, loại bỏ bất kỳ trường hợp nào của \m, \r, \s, \v hoặc các tham chiếu đến nền tảng HĐH.

```
# echo "Authorized uses only. All activity may be monitored and reported." >
/etc/issue
```


1.5.2. Loại bỏ thông tin hệ điều hành khỏi banner

Đánh giá :

- Level 1

Mô tả :

Nội Các hệ thống dựa trên Unix đã thường hiển thị thông tin về việc phát hành hệ điều hành và các bản vá cấp phát khi đăng nhập vào hệ thống. Thông tin này có thể có ích cho các nhà phát triển đang phát triển phần mềm cho một nền tảng hệ điều hành cụ thể. Nếu mingetty (8) hỗ trợ các tùy chọn sau đây, chúng hiển thị điều hành hệ thống thông tin:

\ m - kiến trúc máy tính (uname -m)

\ r - hệ điều hành phát hành (uname -r)

\ s - tên hệ thống

\ v - phiên bản hệ thống (uname -v)

Mục đích :

Hiển thị hệ điều hành và thông tin các bản vá trong các biểu ngữ đăng nhập sẽ cung cấp thông tin cho attacker để khai thác lỗ hổng cụ thể hệ thống trên phiên bản hệ thống đang sử dụng.

- **Đối tượng áp dụng**: CentOS 7 và 8

Kiểm tra :

```
#egrep '(\\v|\\r|\\m|\\s)' /etc/issue
#egrep '(\\v|\\r|\\m|\\s)' /etc/motd
#egrep '(\\v|\\r|\\m|\\s)' /etc/issue.net
```

Khắc phục :

Chỉnh sửa file /etc/motd, /etc/issue và /etc/issue.net xóa các dòng có chứa nội dung \m , \r, \s, \v

1.6. Đảm bảo updates, patches, security software được cài đặt

Đánh giá :

- Level 1

Mô tả :

Các bản vá định kỳ được phát hành cho phần mềm đi kèm do lỗi bảo mật cần được cập nhật cho server thường xuyên.

Mục đích :

Việc cập nhật thường xuyên các bản vá giúp server được an toàn hơn. Các bản vá mới cho kernel, phần mềm trên server trước khi cài đặt nên được thử nghiệm trên môi trường test trước khi update cho hệ thống production.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Đảm bảo không có bản cập nhật nào bị bỏ sót:

```
# yum check-update
```

Khắc phục :

Cập nhật các gói phần mềm có bản cập nhật :

```
# yum update
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Đảm bảo không có bản cập nhật nào bị bỏ sót:

```
# dnf check-update
```

Khắc phục :

Cập nhật các gói phần mềm có bản cập nhật :

```
# dnf update
```


2. Dịch vụ

2.1. Dịch vụ hệ thống

2.1.1. Dịch vụ đồng bộ thời gian

2.1.1.1. Đảm bảo thời gian được đồng bộ

Đánh giá :

- Level 1

Mô tả :

Đồng bộ thời gian là dịch vụ đồng bộ thời gian từ máy máy server đến máy client.

Mục đích :

Việc đồng bộ thời gian đảm bảo các file log được ghi có thời gian nhất quán trên toàn doanh nghiệp, hỗ trợ cho việc kiểm tra, check log, bug lỗi.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Kiểm tra 1 trong 2 service đồng bộ thời gian nếu được cài đặt:

```
#rpm -q chrony ntp
chrony-<version>
# rpm -q ntp
ntp-<version>
```

Khắc phục :

Cài đặt dịch vụ chrony :

```
# yum install chrony
```

Hoặc cài dịch vụ ntp :

```
# yum install ntp
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Kiểm tra 1 trong 2 service đồng bộ thời gian nếu được cài đặt:

```
#rpm -q chrony ntp
chrony-<version>
# rpm -q ntp
ntp-<version>
```

Khắc phục :

Cài đặt dịch vụ chrony :

```
# dnf install chrony
```

Hoặc cài dịch vụ ntp :

```
# yum install ntp
```


2.1.1.2. Đảm bảo dịch vụ chrony được cấu hình

Đánh giá :

- Level 1

Mô tả :

Chronyd là dịch vụ đồng bộ thời gian.

Mục đích :

Việc đồng bộ thời gian đảm bảo các file log được ghi có thời gian nhất quán trên toàn doanh nghiệp, hỗ trợ cho việc kiểm tra, check log, bug lỗi. Xác định service chrony đã được cấu hình đồng bộ time đến 3 server NTP server của MobiFone hay chưa

- **Đối tượng áp dụng**: CentOS 7 và 8

Kiểm tra :

Kiểm tra chrony đã được cấu hình đồng bộ đến NTP server chưa:

```
#grep -E "^(server 10.247.251.10|server 10.247.252.250|server
10.247.255.10)" /etc/chrony.conf
```

Khắc phục :

Thêm hoặc dòng sau vào file /etc/chrony.conf:

```
server 10.247.251.10
server 10.247.252.250
server 10.247.255.10
```

2.1.1.3. Đảm bảo dịch vụ ntpd được cấu hình

Đánh giá :

- Level 1

Mô tả :

NTP là dịch vụ đồng bộ thời gian.

Mục đích :

Việc đồng bộ thời gian đảm bảo các file log được ghi có thời gian nhất quán trên toàn doanh nghiệp, hỗ trợ cho việc kiểm tra, check log, bug lỗi. Xác định service NTP đã được cấu hình đồng bộ time đến 3 server NTP server của MobiFone hay chưa

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Đảm bảo NTP được enable trên server:

```
# systemctl is-enabled ntpd
enabled
```

Kiểm tra chrony đã được cấu hình đồng bộ đến NTP server chưa:

```
#grep -E "^(server 10.247.251.10|server 10.247.252.250|server
10.247.255.10)" /etc/ntp.conf
```

Khắc phục :

Thêm hoặc dòng sau vào file /etc/ntp.conf:

```
server 10.247.251.10
server 10.247.252.250
server 10.247.255.10
```

2.1.1.4. Gỡ bỏ dịch vụ xinetd

Đánh giá :

- Level 1

Mô tả :

xinetd là một dịch vụ hay còn gọi là daemon trong Linux. Nó là một máy chủ dịch vụ đa năng (super server) thay thế cho inetd đã lỗi thời. Nó cũng cung cấp những tuỳ chọn cấu hình để kiểm xoát truy cập, logging, binding, redirection và việc sử dụng tài nguyên.

Mục đích :

Nếu không cần thiết sử dụng xinetd thì nên gỡ bỏ.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Đảm bảo xinetd không được cài đặt:

```
# rpm -qa |grep xinetd
```

Khắc phục :

Xóa bỏ gói xinetd :

```
# yum remove xinetd
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Đảm bảo xinetd không được cài đặt:

```
# rpm -qa |grep xinetd
```

Khắc phục :

Xóa bỏ gói xinetd :

```
# dnf remove xinetd
```

2.1.2. Gỡ bỏ X Windows

Đánh giá :

- Level 1

Mô tả :

Hệ thống X Windows là một hệ thống cửa sổ dành cho hiển thị đồ họa (ảnh bitmap). Hệ thống X Window cung cấp một bộ công cụ cho các ứng dụng GUI (Graphical User Interface) như GNOME hoặc KDE.

Mục đích :

Trừ khi việc sử dụng yêu cầu đăng nhập vào server với giao diện đồ họa nếu không thì nên xóa bỏ cài đặt X Windows để chống việc bị attack surface.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Xác định X Windows có được cài đặt trên hệ thống:

```
# rpm -qa xorg-x11-server*
```

Khắc phục :

Xóa bỏ gói X Windows :

```
# yum remove xorg-x11-server*
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Xác định X Windows có được cài đặt trên hệ thống:

```
# rpm -qa xorg-x11-server*
```

Khắc phục :

Xóa bỏ gói X Windows :

```
# dnf remove xorg-x11-server*
```

2.1.3. Vô hiệu hóa avahi server

Đánh giá :

- Level 1

Mô tả :

avahi là hệ thống có thể phát hiện các dịch vụ và các thiết bị đang chạy trong mạng cục bộ một cách dễ dàng. Điều này có nghĩa là khi máy tính trong một mạng LAN thì có thể ngay lập tức "nhìn thấy" những ai có thể chat, tìm thấy những máy in nào đang được chia sẻ, những file nào đang được chia sẻ trong mạng cục bộ. avahi sử dụng Zeroconf – một cách cho phép người dùng có thể tạo ra một mạng IP mà không cần tới việc phải có những server được cấu hình đặc biệt như DNS Servers.

Mục đích :

Khi server không sử dụng in thì dịch vụ này không cần thiết sử dụng do đó nên tắt dịch vụ để tránh bị attack surface.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Đảm bảo avahi không được bật và cài đặt:

```
# rpm -q avahi-autoipd avahi
# systemctl is-enabled avahi-daemon
```

Khắc phục :

Xóa bỏ gói avahi:

```
# systemctl stop avahi-daemon.socket avahi-daemon.service
# yum remove avahi-autoipd avahi
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Đảm bảo avahi không được bật và cài đặt:

```
# rpm -q avahi-autoipd avahi
# systemctl is-enabled avahi-daemon
```

Khắc phục :

Xóa bỏ gói avahi:

```
# systemctl stop avahi-daemon.socket avahi-daemon.service
# dnf remove avahi-autoipd avahi
```

2.1.4. Vô hiệu hóa print server CUPS

Đánh giá :

- Level 1

Mô tả :

CPUS (Common Unix Print System) là dịch vụ hỗ trợ việc in ấn.

Mục đích :

Khi server không sử dụng in ấn thì dịch vụ này không cần thiết sử dụng do đó nên tắt dịch vụ để tránh bị attack surface.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Đảm bảo cups không được bật và cài đặt:

```
# systemctl is-enabled cups
# rpm -q cups
```

Khắc phục :

Xóa bỏ gói cups:

```
#systemctl disable cups
# yum remove cups
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Đảm bảo cups không được bật và cài đặt:

```
# systemctl is-enabled cups
# rpm -q cups
```

Khắc phục :

Xóa bỏ gói cups:

```
#systemctl disable cups
# dnf remove cups
```

2.1.5. Gỡ bỏ DHCP server

Đánh giá :

- Level 1

Mô tả :

DHCP (Dynamic Host Configuration Protocol) là dịch vụ cho phép thiết bị tự động gán địa chỉ IP.

Mục đích :

Nếu server không được sử dụng làm DHCP server, khuyến nghị nên xóa dịch vụ để giảm thiểu khả năng bị attack surface.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Đảm bảo dhcp không được cài đặt:

```
# rpm -q dhcp
Package dhcp is not installed
```

Khắc phục :

Xóa bỏ gói dhcp:

```
# yum remove dhcp
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Đảm bảo dhcp không được cài đặt:

```
# rpm -q dhcp
Package dhcp is not installed
```

Khắc phục :

Xóa bỏ gói dhcp:

```
# dnf remove dhcp
```

2.1.6. Gỡ bỏ LDAP

Đánh giá :

- Level 1

Mô tả :

LDAP (Lightweight Directory Access Protocol) là một giao thức truy cập nhanh các dịch vụ thư mục. LDAP hoạt động theo mô hình TCP/IP (các dịch vụ hướng kết nối).

Mục đích :

Nếu server không cần sử dụng dịch vụ LDAP server/clinet thì không nên cho chạy dịch vụ nhằm giảm thiểu khả năng bị attack surface.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Đảm bảo ldap không được cài đặt:

```
# rpm -q openldap-servers
```

Khắc phục :

Xóa bỏ gói ldap:

```
# yum remove openldap-servers
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Đảm bảo ldap không được cài đặt:

```
# rpm -q openldap-servers
```

Khắc phục :

Xóa bỏ gói ldap:

```
# dnf remove openldap-servers
```


2.1.7. Gỡ bỏ DNS Server

Đánh giá :

- Level 1

Mô tả :

DNS (Domain Name System) là hệ thống phân giải tên miền được sử dụng để ánh xạ tên miền thành địa chỉ IP.

Mục đích :

Nếu server không cần sử dụng dịch vụ DNS Server thì không nên cho chạy dịch vụ nhằm giảm thiểu khả năng bị attack surface.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Đảm bảo dns server không được cài đặt:

```
# rpm -q bind
```

Khắc phục :

Xóa bỏ gói dns server:

```
# yum remove bind
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Đảm bảo dns server không được cài đặt:

```
# rpm -q bind
```

Khắc phục :

Xóa bỏ gói dns server:

```
# dnf remove bind
```

2.1.8. Gỡ bỏ FTP Server

Đánh giá :

- Level 1

Mô tả :

FTP (File Transfer Protocol) hỗ trợ trao đổi dữ liệu giữa các máy tính với nhau.

Mục đích :

Nếu server không cần sử dụng dịch vụ FTP Server thì không nên cho chạy dịch vụ nhằm giảm thiểu khả năng bị attack surface.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Đảm bảo ftp server không được cài đặt:

```
# rpm -q vsftpd
```

Khắc phục :

Xóa bỏ gói ftp server:

```
# yum remove vsftpd
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Đảm bảo ftp server không được cài đặt:

```
# rpm -q vsftpd
```

Khắc phục :

Xóa bỏ gói ftp server:

```
# dnf remove vsftpd
```


2.1.9. Gỡ bỏ HTTP Server

Đánh giá :

- Level 1

Mô tả :

HTTP (web server) cung cấp khả năng lưu trữ nội dung của trang web.

Mục đích :

Nếu server không cần sử dụng dịch vụ HTTP Server thì không nên cho chạy dịch vụ nhằm giảm thiểu khả năng bị attack surface.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Đảm bảo http server không được cài đặt:

```
# rpm -q httpd
```

Khắc phục :

Xóa bỏ gói http server:

```
# yum remove httpd
```

2.1.10. Gỡ bỏ dovecot (dịch vụ IMAP và POP3)

Đánh giá :

- Level 1

Mô tả :

Dovecot là một ứng dụng IMAP và POP3 mã nguồn mở, được thiết kế dành riêng cho hệ điều hành Linux/Unix.

Mục đích :

Nếu server không cần sử dụng dịch vụ POP3 và (hoặc) IMAP server thì không nên cho chạy dịch vụ nhằm giảm thiểu khả năng bị attack surface.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Đảm bảo dovecot không được cài đặt:

```
# rpm -q dovecot
```

Khắc phục :

Xóa bỏ gói dovecot:

```
# yum remove dovecot
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Chạy lệnh sau để xác minh rằng dovecot và cyrus-imapd không được cài đặt:

```
# rpm -q dovecot cyrus-imapd
package dovecot is not installed
package cyrus-imapd is not installed
```

Khắc phục :

Xóa bỏ gói dovecot:

```
# dnf remove dovecot cyrus-imapd
```

2.1.11. Gỡ bỏ Samba

Đánh giá :

- Level 1

Mô tả :

Samba là bộ công cụ ứng dụng mạnh mẽ cho phép các hệ thống như Linux hoạt động thông suốt với HĐH Windows cũng như các HĐH phổ biến khác. Về cơ bản, Samba cung cấp các dịch vụ chia sẻ file và máy in với các máy Windows.

Mục đích :

Nếu server không cần chia sẻ files với hệ thống Windows, khuyến nghị nên gỡ bỏ dịch vụ để giảm thiểu khả năng bị attack surface.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Đảm bảo samba không được cài đặt:

```
# rpm -q samba
```

Khắc phục :

Xóa bỏ gói samba:

```
# yum remove samba
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Đảm bảo samba không được cài đặt:

```
# rpm -q samba
```

Khắc phục :

Xóa bỏ gói samba:

```
# dnf remove samba
```


2.1.12. Gỡ bỏ HTTP Proxy server

Đánh giá :

- Level 1

Mô tả :

Gói HTTP proxy mặc định được sử dụng trong Red Hat Linux là squid.

Mục đích :

Nếu server không được sử dụng làm proxy server, khuyến nghị nên xóa dịch vụ để giảm thiểu khả năng bị attack surface.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Đảm bảo squid không được cài đặt:

```
# rpm -q squid
```

Khắc phục :

Xóa bỏ gói squid:

```
# yum remove squid
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Đảm bảo http server không được cài đặt:

```
# rpm -q squid
```

Khắc phục :

Xóa bỏ gói http server:

```
# dnf remove squid
```


2.1.13. Gỡ bỏ dịch vụ NIS server

Đánh giá :

- Level 1

Mô tả :

Dịch vụ thông tin mạng (NIS), trước đây gọi là Yellow Pages, là một giao thức dạng client-server được sử dụng để phân phối các file cấu hình hệ thống. NIS server bao gồm các chương chình để phân phối các file cấu hình đến NIS client.

Mục đích :

Dịch vụ NIS là hệ thống bảo mật kém và dễ bị DOS, buffer overflows, xác thực lỏng lẻo bởi NIS maps. NIS giờ được thay thế bởi giao thức LDAP (Light Directory Access Protocol). Vì vậy dịch vụ NIS khuyến nghị là nên bỏ.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Đảm bảo ypserv không được cài đặt:

```
# rpm -q ypserv
```

Khắc phục :

Xóa bỏ gói ypserv:

```
# yum remove ypserv
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Đảm bảo ypserv không được cài đặt:

```
# rpm -q ypserv
```

Khắc phục :

Xóa bỏ gói ypserv:

```
# dnf remove ypserv
```


2.1.14. Gỡ bỏ dịch vụ telnet server

Đánh giá :

- Level 1

Mô tả :

Dịch vụ telnet server cho phép user từ hệ thống khác kết nối đến hệ thống qua giao thức telnet. Daemon chạy dịch vụ là telnetd.

Mục đích :

Do giao thức telnet không sử dụng phương thức mã hóa nên việc thực hiện kết nối thông qua telnet có thể dẫn đến việc hệ thống mạng bị sniff và thông tin bị đánh cắp. Giao thức ssh được sử dụng thay thế do mã hóa các session và bảo mật mạnh mẽ.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Đảm bảo dịch vụ telnet-server không được cài đặt:

```
# rpm -q telnet-server
```

Khắc phục :

Xóa bỏ gói telnet-server:

```
# yum remove telnet-server
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Đảm bảo dịch vụ telnet-server không được cài đặt:

```
# rpm -q telnet-server
```

Khắc phục :

Xóa bỏ gói telnet-server:

```
# dnf remove telnet-server
```

2.1.15. Cấu hình MTA (Mail Transfer Agent) cho chế độ local-only

Đánh giá :

- Level 1

Mô tả :

MTA(Mail Transfer Agents) được sử dụng để gửi mail.

Mục đích :

Nếu server không sử dụng dịch vụ MTA, khuyến nghị nên xóa dịch vụ để giảm thiểu khả năng bị attack surface.

- **Đối tượng áp dụng**: CentOS 7 và 8

Kiểm tra :

Đảm bảo MTA được lắng nghe trên địa chỉ loopback:

```
#ss -lntu | grep -E ':25\s' | grep -E -v '\s(127.0.0.1|\[?::1\]?):25\s'
```

Khắc phục :

Chỉnh sửa file /etc/postfix/main.cf theo thêm cấu hình:

```
inet_interfaces = loopback-only
```

Khởi động lại dịch vụ postfix:

```
#systemctl restart postfix
```

2.1.16. Vô hiệu hóa NFS và RPC

Đánh giá :

- Level 1

Mô tả :

NFS (Network File System) là dịch vụ chia sẻ file qua mạng.

Mục đích :

Nếu server không cần sử dụng dịch vụ NFS server thì không nên cho chạy dịch vụ nhằm giảm thiểu khả năng bị attack surface.

- **Đối tượng áp dụng**: CentOS 7 và 8

Kiểm tra :

Đảm bảo dịch vụ nfs-utils, rpcbind không được bật:

```
# systemctl is-enabled rpcbind
# systemctl is-enabled nfs-utils
```

Khắc phục :

Dừng service rpcbind và nfs-server:

```
# systemctl disable rpcbind
# systemctl --now mask nfs-server
```


2.2. Dịch vụ clients

2.2.1. Gỡ bỏ dịch vụ NIS client

Đánh giá :

- Level 1

Mô tả :

Dịch vụ thông tin mạng (NIS), trước đây gọi là Yellow Pages, là một giao thức dạng client-server được sử dụng để phân phối các file cấu hình hệ thống. Các NIS (ypbind) được kết nối đến một NIS server để nhận cấu hình files.

Mục đích :

Dịch vụ NIS là hệ thống bảo mật kém và dễ bị DOS, buffer overflows, xác thực lỏng lẻo bởi NIS maps. NIS giờ được thay thế bởi giao thức LDAP (Light Directory Access Protocol). Vì vậy dịch vụ NIS khuyến nghị là nên bỏ.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Đảm bảo ypbind không được cài đặt:

```
# rpm -q ypbind
```

Khắc phục :

Xóa bỏ gói ypbind:

```
# yum remove ypbind
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Đảm bảo ypbind không được cài đặt:

```
# rpm -q ypbind
```

Khắc phục :

Xóa bỏ gói ypbind:

```
# dnf remove ypbind
```

2.2.2. Gỡ bỏ dịch rsh

Đánh giá :

- Level 1

Mô tả :

Gói rsh bao gồm tập lệnh của clients cho dịch vụ rsh.

Mục đích :

Những dịch vụ này chứa nhiều rủi ro an ninh và đã được thay thế bằng các gói SSH an toàn hơn.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Đảm bảo rsh không được cài đặt:

```
# rpm -q rsh
```

Khắc phục :

Xóa bỏ gói rsh:

```
# yum remove rsh
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Đảm bảo rsh không được cài đặt:

```
# rpm -q rsh
```

Khắc phục :

Xóa bỏ gói rsh:

```
# dnf remove rsh
```

2.2.3. Gỡ bỏ dịch vụ talk

Đánh giá :

- Level 1

Mô tả :

Phần mềm talk dùng để gửi và nhận tin nhắn trên hệ thống thông qua terminal.

Mục đích :

Do phần mềm talk không sử dụng mã hóa khi truyền tải thông tin nên tính bảo mật rất yếu.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Đảm bảo rsh không được cài đặt:

```
# rpm -qa |grep talk
```

Khắc phục :

Xóa bỏ gói talk:

```
# yum remove talk
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Đảm bảo rsh không được cài đặt:

```
# rpm -qa |grep talk
```

Khắc phục :

Xóa bỏ gói talk:

```
# dnf remove talk
```


2.2.4. Gỡ bỏ Ldap client

Đánh giá :

- Level 1

Mô tả :

LDAP (Lightweight Directory Access Protocol) là một giao thức truy cập nhanh các dịch vụ thư mục. LDAP hoạt động theo mô hình TCP/IP (các dịch vụ hướng kết nối).

Mục đích :

Nếu server không cần sử dụng dịch vụ LDAP clinet thì không nên cho chạy dịch vụ nhằm giảm thiểu khả năng bị attack surface.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Đảm bảo ldap không được cài đặt:

```
# rpm -q openldap-clients
package openldap-clients is not installed
```

Khắc phục :

Xóa bỏ gói ldap:

```
# yum remove openldap-clients
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Đảm bảo ldap không được cài đặt:

```
# rpm -q openldap-clients
package openldap-clients is not installed
```

Khắc phục :

Xóa bỏ gói ldap:

```
# dnf remove openldap-clients
```

3. Cấu hình network và firewalls

3.1. Chỉnh sửa tham số network (chế độ host only)

3.1.1. `Vô hiệu hóa IP Forwarding

Đánh giá :

- Level 1

Mô tả :

net.ipv4.ip_forward được sử dụng để cấu hình forward gói tin trên server. Nếu thiết lập bằng 1 server được sử dụng một router.

Mục đích :

Thiết lập tham số net.ipv4.ip_forward bằng 0 để đảm bảo server sẽ không forward gói tin giữa các card mạng.

- **Đối tượng áp dụng**: CentOS 7 và 8

Kiểm tra :

```
# /sbin/sysctl net.ipv4.ip_forward
```

Khắc phục :

Thiết lập net.ipv4.ip_forward=0 trong file /etc/sysctl.conf:

```
# /sbin/sysctl -w net.ipv4.ip_forward=0
# /sbin/sysctl -w net.ipv4.route.flush=1
```

3.1.2. Vô hiệu hóa redirects gói tin gửi

Đánh giá :

- Level 1

Mô tả :

ICMP redirects được sử dụng để gửi thông tin định tuyến đến các host khác

Mục đích :

Hacker sẽ sử dụng một máy chủ bị xâm nhập để gửi thông tin ICMP redirects không hợp lệ đến các thiết bị định tuyến nhằm gây ra lỗi định tuyến.

- **Đối tượng áp dụng**: CentOS 7 và 8

Kiểm tra :

```
#/sbin/sysctl net.ipv4.conf.all.send_redirects
net.ipv4.conf.all.send_redirects = 0
#/sbin/sysctl net.ipv4.conf.default.send_redirects
net.ipv4.conf.default.send_redirects = 0
```

Khắc phục :

Thiết lập net.ipv4.conf.all.send_redirects = 0 và net.ipv4.conf.default.send_redirects = 0 trong file /etc/sysctl.conf

Chỉnh sửa tham số kernel

```
#/sbin/sysctl -w net.ipv4.conf.all.send_redirects=0
#/sbin/sysctl -w net.ipv4.conf.default.send_redirects=0
#/sbin/sysctl -w net.ipv4.route.flush=1
```


3.2. Chỉnh sửa tham số network (Chế độ router)

3.2.1. Vô hiệu hóa Source Routed Packet Acceptance

Đánh giá :

- Level 1

Mô tả :

Trong hệ thống mạng, source route cho phép người gửi một phần hoặc toàn bộ gói tin định tuyến thông qua mạng. Ngược lại, không sử dụng source route các gói tin đi một con đường xác định bởi các định tuyến trong mạng.

Mục đích :

Thiết lập tham số net.ipv4.conf.all.accept_source_route và net.ipv4.conf.default.accept_source_route bằng 0 để đảm bảo hệ thống không sử dụng source routed. Giả sử máy chủ có hai card mạng một card được kết nối đến mạng internet một card kết nối nội bộ. Trong trường hợp định tuyến bình thường, attacker không thể sử dụng địa chỉ kết nối public để phát hiện các sever trong mạng nội bộ. Nếu sử dụng source route, attacker có thể lợi dụng để có thể truy nhập vào mạng nội bộ với một định tuyến đã được chỉ định.

- **Đối tượng áp dụng**: CentOS 7 và 8

Kiểm tra :

```
# /sbin/sysctl net.ipv4.conf.all.accept_source_route
net.ipv4.conf.all.accept_source_route = 0
# /sbin/sysctl net.ipv4.conf.default.accept_source_route
net.ipv4.conf.default.accept_source_route = 0
```

Khắc phục :

Thiết lập net.ipv4.conf.all.accept_source_route = 0 và net.ipv4.conf.default.accept_source_route = 0 trong file /etc/sysctl.conf

Chỉnh sửa tham số kernel

```
#/sbin/sysctl -w net.ipv4.conf.all.accept_source_route = 0
#/sbin/sysctl -w net.ipv4.conf.default.accept_source_route = 0
#/sbin/sysctl -w net.ipv4.route.flush = 1
```


3.2.2. Vô hiệu hóa ICMP Redirect Acceptance

Đánh giá :

- Level 1

Mô tả :

ICMP redirect messages truyền đạt các thông tin định tuyến tới host (đóng vai trò như một router) thông báo việc gửi các gói dữ liệu thông qua một hướng khác . Đây là một cách cho phép một thiết bị định tuyến bên ngoài có thể cập nhật bảng định tuyến hệ thống. Bằng cách đặt net.ipv4.conf.all.accept_redirects bằng 0, hệ thống sẽ không chấp nhận bất kỳ ICMP chuyển các bản tin, và do đó, sẽ không cho phép hệ thóng bên ngoài cập nhật bảng định tuyến của hệ thống.

Mục đích :

Những kẻ tấn công có thể sử dụng ICMP redirect messages không có thật để cố thay đổi bảng định tuyến và khi đó attacker có thể gửi các gói tin đến một mạng không chính xác và capture lại các gói tin hệ thống.

- **Đối tượng áp dụng**: CentOS 7 và 8

Kiểm tra :

```
#/sbin/sysctl net.ipv4.conf.all.accept_redirects
net.ipv4.conf.all.accept_redirects = 0
#/sbin/sysctl net.ipv4.conf.default.accept_redirects
net.ipv4.conf.default.accept_redirects = 0
```

Khắc phục :

Thiết lập net.ipv4.conf.all.accept_redirects = 0 và net.ipv4.conf.default.accept_redirects = 0 trong file /etc/sysctl.conf

Chỉnh sửa tham số kernel

```
#/sbin/sysctl -w net.ipv4.conf.all.accept_redirects=0
#/sbin/sysctl -w net.ipv4.conf.default.accept_redirects=0
#/sbin/sysctl -w net.ipv4.route.flush=1
```

3.2.3. Vô hiệu hóa Secure ICMP Redirect Acceptance

Đánh giá :

- Level 1

Mô tả :

Secure ICMP redirects cũng tương tự như ICMP redirect messages , ngoại trừ việc các gói tin sẽ đến từ một gateway đã có sẵn trong danh sách gateway mặc định(giả định các gateway đã được biết trên hệ thống và chúng an toàn).

Mục đích :

Việc bị tấn công vẫn có thể xảy ra khi mà gateway được biết đến trong danh sách có khả năng bị xâm nhập. Thiết lập net.ipv4.conf.all.secure_redirects =0 để bảo vệ hệ thống khỏi việc cập nhật bảng định tuyến bởi gateway trong danh sách hệ thống mà khả năng đã bị xâm nhập.

- **Đối tượng áp dụng**: CentOS 7 và 8

Kiểm tra :

```
#/sbin/sysctl net.ipv4.conf.all.secure_redirects
net.ipv4.conf.all.secure_redirects = 0
#/sbin/sysctl net.ipv4.conf.default.secure_redirects
net.ipv4.conf.default.secure_redirects = 0
```

Khắc phục :

Thiết lập net.ipv4.conf.all.accept_redirects = 0 và net.ipv4.conf.default.accept_redirects = 0 trong file /etc/sysctl.conf

Chỉnh sửa tham số kernel

```
#/sbin/sysctl -w net.ipv4.conf.all.secure_redirects=0
#/sbin/sysctl -w net.ipv4.conf.default.secure_redirects=0
#/sbin/sysctl -w net.ipv4.route.flush=1
```

3.2.4. Log các gói tin không đáng tin cậy

Đánh giá :

- Level 1

Mô tả :

Khi được kích hoạt, tính năng này sẽ ghi lại log các gói tin có địa chỉ nguồn không được định tuyến vào log kernel.

Mục đích :

Việc kích hoạt ghi lại log các gói tin cho phép người quản trị để điều tra khả năng một kẻ tấn công đang gửi gói tin giả mạo đến máy chủ của họ.

- **Đối tượng áp dụng**: CentOS 7 và 8

Kiểm tra :

```
#/sbin/sysctl net.ipv4.conf.all.log_martians
net.ipv4.conf.all.log_martians = 1
#/sbin/sysctl net.ipv4.conf.default.log_martians
net.ipv4.conf.default.log_martians = 1
```

Khắc phục :

Thiết lập net.ipv4.conf.all.log_martians = 0 và net.ipv4.conf.default.log_martians = 0 trong file /etc/sysctl.conf

Chỉnh sửa tham số kernel

```
#/sbin/sysctl -w net.ipv4.conf.all.log_martians=1
#/sbin/sysctl -w net.ipv4.conf.default.log_martians=1
#/sbin/sysctl -w net.ipv4.route.flush=1
```

3.2.5. Kích hoạt Ignore Broadcast Requests

Đánh giá :

- Level 1

Mô tả :

Thiết net.ipv4.icmp_echo_ignore_broadcasts bằng 1 khiến hệ thống bỏ qua tất cả các yêu cầu ICMP echo và timestamp gửi đến một địa chỉ broadcast và multicast

Mục đích :

Chấp nhận ICMP echo và timestamp gửi yêu cầu đến địa chỉ broadcast multicast trong mạng có thể khiến hệ thống bị tấn công bởi Smurf attack. Smurf attack dựa vào kẻ tấn công gửi một lượng lớn bản tin ICMP broadcast với một địa chỉ nguồn giả mạo. Tất cả các host khi nhận được bản tin ICMP request sẽ thực hiện gửi bản tin echo-reply lại cho các địa chỉ giả mạo, mà thể không được định tuyến. Nếu quá nhiều host trả gửi bản tin phản hồi, lưu lượng truy cập trên mạng có thể bị tăng lên đáng kể dẫn đến nghẽn mạng.

- **Đối tượng áp dụng**: CentOS 7 và 8

Kiểm tra :

```
#/sbin/sysctl net.ipv4.icmp_echo_ignore_broadcasts
net.ipv4.icmp_echo_ignore_broadcasts = 1
```

Khắc phục :

Thiết lập net.ipv4.icmp_echo_ignore_broadcasts=1 trong file /etc/sysctl.conf

Chỉnh sửa tham số kernel

```
#/sbin/sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1
#/sbin/sysctl -w net.ipv4.route.flush=1
```

3.2.6. Kích hoạt Bad Error Message Protection

Đánh giá :

- Level 1

Mô tả :

Thiết icmp_ignore_bogus_error_responses bằng 1 để ngăn kernel khỏi những log phản hồi không có thật, đảm bảo hệ thống log file không bị đầy bởi những log vô nghĩa.

Mục đích :

Tránh trường hợp một attacker sẽ gửi bản tin phản hồi và cố gắng làm đầy log file hệ thống với nhiều thông báo lỗi vô nghĩa.

- **Đối tượng áp dụng**: CentOS 7 và 8

Kiểm tra :

```
#/sbin/sysctl net.ipv4.icmp_ignore_bogus_error_responses
net.ipv4.icmp_ignore_bogus_error_responses = 1
```

Khắc phục :

Thiết lập net.ipv4.icmp_ignore_bogus_error_responses = 1 trong file /etc/sysctl.conf

Chỉnh sửa tham số kernel

```
#/sbin/sysctl -w net.ipv4.icmp_ignore_bogus_error_responses=1
#/sbin/sysctl -w net.ipv4.route.flush=1
```

3.2.7. Kích hoạt RFC- recommended Source Route Validation

Đánh giá :

- Level 1

Mô tả :

Thiết net.ipv4.conf.all.rp_filter và net.ipv4.conf.default.rp_filter bằng 1 để Linux kernel sử dụng reverse path filtering trên gói tin được nhận để xác định gói tin là hợp lệ. Về căn bản, với reverse path filtering, nếu một gói tin phản hồi không tương ứng với cổng mạng gói tin đến thì gói tin sẽ bị drop.

Mục đích :

Thiết lập này là một cách để ngăn chặn attacker gửi đến server những gói tin không có thật mà những gói tin này không thẻ được phản hồi.

- **Đối tượng áp dụng**: CentOS 7 và 8

Kiểm tra :

```
#/sbin/sysctl net.ipv4.conf.all.rp_filter
net.ipv4.conf.all.rp_filter = 1
#/sbin/sysctl net.ipv4.conf.default.rp_filter
net.ipv4.conf.default.rp_ filter=1
```

Khắc phục :

Thiết lập net.ipv4.conf.all.rp_filter=1 và net.ipv4.conf.default.rp_filter=1 trong file /etc/sysctl.conf

Chỉnh sửa tham số kernel

```
#/sbin/sysctl -w net.ipv4.conf.all.rp_filter=1
#/sbin/sysctl -w net.ipv4.conf.default.rp_filter=1
#/sbin/sysctl -w net.ipv4.route.flush=1
```

3.2.8. Kích hoạt TCP SYN cookies

Đánh giá :

- Level 1

Mô tả :

Khi tcp_syncookies được thiết lập, kernel vẫn sẽ xử lý các gói tin TCP SYN bình thường cho đến khi hàng đợi bị đầy bởi các kết nối half-open (các kết nối không thực hiện được việc đồng bộ giữa hai máy trong giao thức TCP), khi đó sẽ bỏ qua chức năng SYN cookie. Thay vào đó, kernel đơn giản trả lời lại SYN một SYN|ACK, nhưng chỉ bao gồm một chuỗi TCP đặc biệt mã hóa địa chỉ IP nguồn, IP đích, port và thời gian gói tin đã gửi. Một kết nối sẽ gửi gói tin ACK theo phương thức bắt tay ba bước với chuỗi TCP được mã hóa này. Nó cho phép server xác thực rằng nó đã nhận được một phản hồi hợp lệ đến SYN cookie và cho phép kết nối thậm chí nó không phù hợp với bản tin SYN trong hàng đợi.

Mục đích :

Attacker sử dụng SYN flood attacks để thực hiện DOS hệ thống bằng cách gửi rất nhiều bản tin SYN với địa chỉ nguồn không có thực khiến cho hệ thống nhận được các gói tin này sẽ không thể thực hiện được bắt tay ba bước. Điều này sẽ nhanh chóng sử dụng hàng đợi các kết nối (half-open) trên kernel bị đầy dẫn đến các kết nối hợp lệ sẽ không kết nối thành công. SYN cookie cho máy máy chủ chấp nhận các kết nối hợp lệ ngay cả khi đang bị tấn công bởi DOS.

- **Đối tượng áp dụng**: CentOS 7 và 8

Kiểm tra :

```
#/sbin/sysctl net.ipv4.tcp_syncookies
net.ipv4.tcp_syncookies = 1
```

Khắc phục :

Thiết lập net.ipv4.tcp_syncookies = 1 trong file /etc/sysctl.conf

Chỉnh sửa tham số kernel

```
#/sbin/sysctl -w net.ipv4.tcp_syncookies=1
#/sbin/sysctl -w net.ipv4.route.flush=1
```

3.3. TCP wrappers

3.3.1. Cài đặt TCP wrapper

Đánh giá :

- Level 1

Mô tả :

TCP Wrapper cung cấp một danh sách truy cập đơn giản và phương pháp khai thác log được chuẩn hóa cho các dịch vụ có khả năng hỗ trợ nó. Trong quá khứ, các dịch vụ như inetd và xinetd hỗ trợ sử dụng các TCP wrappers. bất kỳ dịch vụ nào hỗ trợ TCPwrapper sẽ có thư viện libwrap.so gắn liền với nó.

Mục đích :

TCP cung cấp một danh sách truy cập đơn giản cho các dịch vụ mà nó có thể hỗ trợ. Khuyến nghị tất cả các dịch vụ nên sử dụng TCP Wrappers.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Xác định TCP Wrappers đã được cài đặt:

```
# rpm -qa |grep tcp_wrappers
```

Để xác định dịch vụ hỗ trợ tcp_wrappers::

```
#ldd <path-to-daemon> | grep libwrap.so
Ví dụ với dịch vụ SSH:
#ldd /usr/sbin/sshd | grep libwrap.so
```

Khắc phục :

```
# yum install tcp_wrappers
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra :

Xác định TCP Wrappers đã được cài đặt:

```
# rpm -qa |grep tcp_wrappers
```

Để xác định dịch vụ hỗ trợ tcp_wrappers::

```
# ldd <path-to-daemon> | grep libwrap.so
Ví dụ với dịch vụ SSH:
# ldd /usr/sbin/sshd | grep libwrap.so
```

Khắc phục :

```
# dnf install tcp_wrappers
```

3.3.2. Cấu hình file /etc/host.allow

Đánh giá :

- Level 1

Mô tả :

File /etc/hosts.allow quy định các địa chỉ IP được phép kết nối đến host. Nó được sử dụng với file /etc/hosts.deny.

Mục đích :

File /etc/hosts.allow hỗ trợ điều khiển quyền truy cập theo IP nhằm đảm bảo rằng chỉ những hệ thống thuộc IP được cho phép mới có thể kết nối đến máy chủ.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Xác thực nội dung trong file /etc/hosts.allow:

```
# cat /etc/hosts.allow
[contents will vary, depending on your network configuration]
```

Khắc phục :

Cấu hình file /etc/host.allow với nội dung:

```
# echo "ALL: <net>/<mask>, <net>/<mask>, …" >/etc/hosts.allow
```

3.3.3. Xác thực quyền file /etc/host.allow

Đánh giá :

- Level 1

Mô tả :

File /etc/hosts.allow tập tin chứa thông tin kết nối mạng được sử dụng bởi nhiều ứng dụng và do đó các ứng dụng phải được cấp quyền đọc cho file này.

Mục đích :

Để đảm bảo rằng file /etc/hosts.allows được bảo vệ không được ghi từ những truy cập trái phép. Mặc dù nó được bảo vệ theo mặc định, các quyền truy cập file có thể được thay đổi do vô tình hoặc thông qua các hành động độc hại.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Xác thực quyền của file /etc/hosts.allow:

```
# /bin/ls -l /etc/hosts.allow
-rw-r--r-- 1 root root 2055 Jan 30 16:30 /etc/hosts.allow
```

Khắc phục :

```
#/bin/chmod 644 /etc/hosts.allow
```

3.3.4. Cấu hình file /etc/host.deny

Đánh giá :

- Level 1

Mô tả :

File /etc/hosts.deny quy định các địa chỉ IP không được phép kết nối đến host. Nó được sử dụng với file /etc/hosts.allow.

Mục đích :

File /etc/hosts.deny đảm bảo chỉ các host được cấu hình trong file /etc/host.allow được phép truy cập server.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Xác thực /etc/hostsdeny tồn tại và không gồm các IP có trong /etc/host.allow:

```
#grep "ALL: ALL" /etc/hosts.deny
```

```
ALL: ALL
```

Khắc phục :

Cấu hình file /etc/hosts.deny:

```
#echo "ALL: ALL" >> /etc/hosts.deny
```

3.3.5. Xác thực quyền file /etc/host.deny

Đánh giá :

- Level 1

Mô tả :

File /etc/hosts.deny tập tin chứa thông tin kết nối mạng được sử dụng bởi nhiều ứng dụng và do đó các ứng dụng phải được cấp quyền đọc cho file này.

Mục đích :

Để đảm bảo rằng các /etc/hosts.deny tập tin được bảo vệ không được ghi từ những truy cập trái phép. Mặc dù nó được bảo vệ theo mặc định, các quyền truy cập file có thể được thay đổi do vô tình hoặc thông qua các hành động độc hại.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra :

Xác thực quyền của file /etc/hosts.deny:

```
# /bin/ls -l /etc/hosts.deny
-rw-r--r-- 1 root root 2055 Jan 30 16:30 /etc/hosts.deny
```

Khắc phục :

```
#/bin/chmod 644 /etc/hosts.deny
```

3.4. Enable Firewall

Đánh giá :

- Level 1

Mô tả :

Iptables là một ứng dụng cho phép người quản trị hệ thống cấu hình các chains và các rules ipv4 được cung cấp bởi Linux kernel firewall. Firewalld cung cấp một dịch vụ tường lửa linh động hơn so với iptables cho phép thay đổi cấu hình mà không ảnh hưởng đến kết nối.

Mục đích :

Iptables/firewalld cung cấp khả năng bảo vệ hệ thống Linux bằng việc giới hạn các kết nối được đi qua hệ thống qua địa chỉ IP và port.

- **Đối tượng áp dụng**: CentOS 7 và 8

Kiểm tra :

Xác định Firewalld hoặc Iptables đã bật:

```
# systemctl is-enabled firewalld
Enabled
# systemctl is-enabled iptables
Enabled
```

Khắc phục :

```
# systemctl enable firewalld
Hoặc
# systemctl enable iptables
```

3.4.1. Đảm bảo rule iptables tồn tại cho tất cả các port đang mở

Đánh giá :

- Level 1

Mô tả :

Bất kỳ cổng nào đã được mở trên các địa chỉ không phải loopback đều cần có quy tắc tường lửa để quản lý lưu lượng.

Mục đích :

Nếu không có quy tắc tường lửa được định cấu hình cho các cổng mở, chính sách tường lửa mặc định sẽ loại bỏ tất cả các gói đến các cổng này.

- **Đối tượng áp dụng**: CentOS 7 và 8

Kiểm tra :

Xác định các cổng đang mở trên server:

```
#ss -4tuln
```

```
   Netid     State                                  Recv-Q     Send-Q
Local                                                  Address:Port
Peer Address:Port

   udp           UNCONN                    0                      0
*:123
*:*

   tcp           LISTEN                   0                     128
*:22
*:*
```

Kiểm tra rule firewalld hiện tại với chiều INPUT:

```
   # iptables -L INPUT -v -n
   Chain INPUT (policy DROP 0 packets, 0 bytes)
   pkts bytes target prot opt in out source
   destination
   0 0 ACCEPT all -- lo * 0.0.0.0/0 0.0.0.0/0
   0 0 DROP all -- * * 127.0.0.0/8 0.0.0.0/0
   0 0 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:22 state NEW
   # iptables -L IN_public_allow -v -n
   Chain IN_public_allow (1 references)
    pkts bytes target       prot opt in       out       source
destination
       7   464 ACCEPT      tcp  --  *       *         0.0.0.0/0
0.0.0.0/0            tcp dpt:22 ctstate NEW
```


Xác minh tất cả các cổng đang mở trên các địa chỉ không phải localhost đều có ít nhất một quy tắc tường lửa.

Ví dụ: Dòng cuối cùng được xác định bởi "tcp dpt:22 state NEW" xác định đây là quy tắc tường lửa cho phép các kết nối mới đến cổng tcp 22 (SSH)

Khắc phục :

Đối với mỗi cổng được xác định trong quá trình kiểm tra không có quy tắc tường lửa, hãy thiết lập quy tắc thích hợp để chấp nhận các kết nối gửi đến:

```
   # iptables -A INPUT -p <protocol> --dport <port> -m state --
state NEW -j ACCEPT
   Hoặc
   # iptables -A IN_public_allow -p <protocol> --dport <port> -m
state --state NEW -j ACCEPT
```

Ghi chú: Việc enadble firewall có thể gây gián đoạn dịch vụ, các đơn vị cần thống kê rà soát kỹ các Port kết nối cần thiết để tránh gây gián đoạn dịch vụ.

4. Cấu hình SSH

4.1. Cấu hình quyền cho file /etc/ssh/sshd_config

Đánh giá :

- Level 1

Mô tả:

File **/etc/ssh/sshd_config** cần phải được bảo vệ khỏi các thay đổi trái phép bởi người dùng không có đặc quyền.

- **Đối tượng áp dụng**: CentOS 7 và 8

Khắc phục :

Thực hiện các câu lệnh sau để đặt chủ sở hữu và quyền cho file **/etc/ssh/sshd_config**:

```
#chown root:root /etc/ssh/ssh_config
#chmod og-rwx /etc/ssh/sshd_config
```

4.2. Cấu hình giao thực SSH sử dụng SSHv2

Đánh giá :

- Level 1

Mô tả:

Phiên bản SSHv1 đã lỗi thời và tồn tại nhiều vấn đề bảo mật và nên thay thế sang phiên bản SSHv2.

- **Đối tượng áp dụng**: CentOS 7 và 8

Kiểm tra:

```
cat /etc/ssh/sshd_config | grep Protocol
```

Lệnh này sẽ hiển thị giao thức SSH đang được sử dụng. Nếu không có dòng Protocol trong tệp cấu hình, mặc định sẽ sử dụng giao thức 2.

Khắc phục :

Để cấu hình chuyển sang SSHv2 chỉnh sửa file /etc/ssh/sshd_config và thêm tham số như sau:

```
Protocol 2
```

4.3. Cấu hình LogLevel cho máy chủ SSH

Đánh giá :

- Level 1

Mô tả:

SSH cung cấp một số cấp độ logging với số lượng thông tin khác nhau. DEBUG là cấp độ không được khuyến nghị sử dụng vì nó cung cấp rất nhiều dữ liệu, rất khó để xác định thông tin bảo mật quan trọng. INFO là cấp độ cơ bản, chỉ lưu trữ các hoạt động đăng nhập của người dùng SSH. Trong nhiều tình huống, như là ứng phó sự cố, việc xác định người dùng nào hoạt động trên hệ thống là một điều quan trọng. Các bản ghi đăng xuất có thể giúp loại bỏ những người dùng đã đăng xuất, thu hẹp phạm vi tìm kiếm.

- **Đối tượng áp dụng**: CentOS 7 và 8

Khắc phục :

Chỉnh sửa file /etc/ssh/sshd_config và thêm tham số như sau:

```
LogLevel INFO
```

4.4. Cấu hình vô hiệu hóa X11 Forwarding cho máy chủ SSH

Đánh giá :

- Level 1

Mô tả:

Vô hiệu hóa X11 Forwarding trừ khi có yêu cầu về hoạt động cần sử dụng ứng dụng X11. Có một rủi ro nhỏ rằng người dùng đã đăng nhập thông qua SSH với X11 forwarding có thể bị phá hoại bởi người dùng sử dụng X11 khác.

- **Đối tượng áp dụng**: CentOS 7 và 8

Khắc phục :

Chỉnh sửa file /etc/ssh/sshd_config và đặt tham số như sau:

```
X11Forwarding no
```

4.5. Set SSH MaxAuthTries to 4 or Less

Đánh giá :

- Level 1

Mô tả:

Tham số MaxAuthTries xác định số lần được phép xác thực không thành công cho một kết nối. Đặt tham số MaxAuthTries thấp để giảm thiểu tấn công brute-force vào máy chủ SSH. Khuyến nghị cho tham số MaxAuthTries là 4.

- **Đối tượng áp dụng**: CentOS 7 và 8

Kiểm tra:

Kiểm tra tham số:

```
grep "^MaxAuthTries" /etc/ssh/sshd_config
```


Khắc phục :

Sửa tệp tin **/etc/ssh/sshd_config** và thiết lập tham số: **MaxAuthTries 4**

4.6. Đảm bảo việc đăng nhập root qua SSH bị vô hiệu hóa

Đánh giá :

- Level 1

Mô tả:

Việc không cho phép đăng nhập root qua SSH yêu cầu các quản trị viên hệ thống phải xác thực bằng tài khoản cá nhân của họ trước khi sử dụng lệnh sudo để chuyển sang quyền root. Điều này giúp giảm thiểu cơ hội từ chối trách nhiệm và cung cấp một dấu vết kiểm toán rõ ràng trong trường hợp xảy ra sự cố bảo mật.

- **Đối tượng áp dụng**: CentOS 7 và 8

Kiểm tra:

Chạy lệnh sau và kiểm tra xem đầu ra có khớp với kết quả mong đợi không:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep
$(hostname)
/etc/hosts | awk '{print $1}')" | grep permitrootlogin
permitrootlogin no
```

Chạy lệnh sau và xác minh kết quả đầu ra:

```
# grep -Ei '^\s*PermitRootLogin\s+yes' /etc/ssh/sshd_config
Nothing should be returned
```

Khắc phục :

Chỉnh sửa tệp /etc/ssh/sshd_config để thiết lập tham số như sau:

```
PermitRootLogin no
```


5. Logging and Auditing

5.1. Cấu hình Logging

5.1.1. Cấu hình kích hoạt rsyslog service

Đánh giá :

- Level 1

Mô tả:

Rsyslog service là service thay thế cho syslogd với nhiều ưu điểm vượt trội (mã hóa dữ liệu gửi về server tập trung, sử dụng TCP …) hỗ trợ việc tùy chỉnh chuyên sâu log của hệ thống. Kích hoạt service này để đảm bảo log hệ thống được kiểm soát chặt chẽ và tránh tình trạng có log được ghi nhận hoặc ghi nhận thiếu.

- **Đối tượng áp dụng**: CentOS 7 và 8

Khắc phục :

Thực hiện câu lệnh sau để kích hoạt rsyslog:

```
# systemctl enable rsyslog
```

5.1.2. Phân quyền đối với file log sinh ra từ rsyslog

Đánh giá :

- Level 1

Mô tả:

Rsyslog sẽ tạo logfile chưa tồn tại trên hệ thống. Đảm bảo rằng các file logs có quyền chính xác để chắc chắn rằng dữ liệu nhạy cảm được lưu trữ và bảo vệ.

- **Đối tượng áp dụng**: CentOS 7 và 8

Khắc phục :

Chỉnh sửa file /etc/rsyslog.conf và /etc/rsyslog.d/*.conf và đặt $FileCreateMode là 0604 hoặc nghiệm ngặt hơn:

```
$FileCreateMode 0640
```

Đảm bảo cấu hình này không bị viết đè bởi các thiết lập kém nghiêm ngặt hơn ở bất kỳ file conf nào trong /etc/rsyslog.d/*.

5.2. Cấu hình Auditing

5.2.1. Đảm bảo Auditd được cài đặt (tự động hóa)

Đánh giá :

- Level 1

Mô tả:

Việc ghi lại các sự kiện hệ thống cung cấp cho các quản trị viên hệ thống thông tin để giúp họ xác định xem có xảy ra truy cập trái phép vào hệ thống của họ hay không.

- **Đối tượng áp dụng**: CentOS 7

Kiểm tra:

Chạy lệnh sau và xác minh rằng auditd đã được cài đặt:

```
rpm -q audit audit-libs
```

Kết quả mong đợi:

```
audit-<version>
audit-libs-<version>
```

Khắc phục :

Ví dụ như đảm bảo dịch vụ auditd được cài đặt để thu thập log events

```
sudo yum install audit audit-libs
```

- **Đối tượng áp dụng**: CentOS 8

Kiểm tra:

Chạy lệnh sau và xác minh rằng auditd đã được cài đặt:

```
rpm -q audit audit-libs
```

Kết quả mong đợi:

```
audit-<version>
audit-libs-<version>
```

Khắc phục :

Ví dụ như đảm bảo dịch vụ auditd được cài đặt để thu thập log events

```
Sudo dnf install audit audit-libs
```


5.2.2. Đảm bảo dịch vụ auditd được kích hoạt và đang chạy (tự động hóa)

Đánh giá :

- Level 1

Mô tả:

Bật auditd để ghi lại các sự kiện hệ thống.

Việc ghi lại các sự kiện hệ thống cung cấp cho quản trị viên hệ thống thông tin để giúp họ xác định xem có truy cập trái phép vào hệ thống của họ đang xảy ra hay không.

- **Đối tượng áp dụng**: CentOS 7 và 8

Kiểm tra:

Chạy lệnh sau để xác minh auditd đã được kích hoạt

```
systemctl is-enabled auditd
```

Chạy lệnh sau để xác minh rằng auditd đang chạy

```
systemctl status auditd | grep 'Active: active (running)'
```

Khắc phục:

```
sudo systemctl --now enable auditd
```

6. Access, Authentication and Authorization

6.1. Cấu hình PAM

6.1.1. Cấu hình điều kiện tạo mật khẩu

Đánh giá :

- Level 1

Mô tả:

Mật khẩu mạnh bảo vệ hệ thống khỏi bị tấn công trước các kỹ thuật Brute force.

- **Đối tượng áp dụng**: CentOS 7 và 8

Kiểm tra:

Chạy lệnh sau để xác minh độ dài mật khẩu tối thiểu là 14 ký tự trở lên:

```
grep '^\s*minlen\s*' /etc/security/pwquality.conf
```

Kết quả mong đợi:

```
minlen = 14
```

Chạy một trong các lệnh sau để kiểm tra số lượng loại ký tự (minclass):

```
grep '^\s*minclass\s*' /etc/security/pwquality.conf
```

Kết quả mong đợi:

```
minclass = 4
```

Hoặc kiểm tra các yêu cầu về loại ký tự:

```
grep -E '^\s*[duol]credit\s*' /etc/security/pwquality.conf
```

Kết quả mong đợi:

```
dcredit = -1
ucredit = -1
lcredit = -1
ocredit = -1
```

Khắc phục:

- Chỉnh sửa file /etc/pam.d/password-auth và /etc/pam.d/system-auth để bao gồm các tùy chọn phù hợp cho pam_pwquality.so và tuân thủ chính sách của tổ chức:

```
Password requisite pam_pwquality.so try_first_pass retry=3
```

- Chỉnh sửa file /etc/security/pwquality.conf để thêm hoặc cập nhật những thiết lập sau:

```
minlen = 14
minclass = 4
dcredit = -1
ucredit = -1
ocredit = -1
lcredit = -1
```

- Các thiết lập trong file /etc/security/pwquality.conf phải sử dụng dấu cách xung quang dấu "=".

6.1.2. Cấu hình khóa truy cập do nhiều lần nhập mật khẩu thất bại

Đánh giá :

- Level 1

Mô tả:

Khóa truy cập đối với người dùng sau n lần đăng nhập liên tiếp không thành công giảm khả năng tấn công Brute force vào hệ thống.

- **Đối tượng áp dụng**: CentOS 7 và 8

Khắc phục:

- Chỉnh sửa file /etc/pam.d/password-auth và file /etc/pam.d/system-auth và thêm vào các dòng pam_faillock.so dưới đây xung quanh dòng pam_unix, chỉnh sửa dòng pam_unix thành [succes=1 default=bad] như dưới đây:

```
  Auth required pam_faillock.so preauth audit silent deny= 5
unlock_time=900
  Auth [success=1 default=bad] pam_unix.so
  Auth [default=die] pam_faillock.so authfail audit deny=5
unlock_time=900
  Authsufficient pam_faillock.so authsucc audit deny=5
unlock_time=900
```

- Nếu người dùng bị khóa do đã thử quá số lần cho phép, được định danh ở tham số deny= trong mô-dun pam_faillock.so, người dùng đó có thể được mở khóa bằng cách sử dụng lệnh faillock –u –reset. Câu lệnh này sẽ reset lại số lần thử không thành công xuống 0.

6.1.3. Giới hạn việc sử dụng lại mật khẩu

Đánh giá :

- Level 1

Mô tả:

Bắt buộc người dùng không được sử dụng lại 5 mật khẩu cũ khiến cho kẻ tấn công khó đoán được mật khẩu đang sử dụng.

- Đối tượng áp dụng: CentOS 7 và 8

Kiểm tra:

Chạy lệnh sau để kiểm tra các mật khẩu cũ trong tệp /etc/security/opasswd:

```
sudo cat /etc/security/opasswd
```

Khắc phục:

Chỉnh sửa file /etc/pam.d/password-auth và /etc/pam.d/system-auth để bao gồm tùy chọn remember và tuân thủ theo chính sách của tổ chức:

```
Password sufficient pam_unix.so remember=5
```

Hoặc

```
Password required pam_pwhistory.so remember=5
```


6.1.4. Cấu hình thuật toán hash mật khẩu sang SHA-512

Đánh giá :

- Level 1

Mô tả:

Thuật toán SHA-512 cung cấp khả năng hashing mạng hơn MD5, hơn nữa nó còn cung cấp thêm cơ chế bảo vệ cho hệ thống bằng cách làm tăng mức độ khó khăn cho kẻ tấn công khi cố gắng đoán được mật khẩu.

- Đối tượng áp dụng: CentOS 7 và 8

Kiểm tra:

Chạy lệnh sau để xác minh rằng tùy chọn sha512 đã được bao gồm trong các tệp cấu hình PAM /etc/pam.d/system-auth và /etc/pam.d/password-auth:

```
Grep -P '^\h*password\h+(sufficient|requisite|required)\h+pam_unix\.so\h+([^#\n\r]+)?sha512(\h+.*)?$'/etc/pam.d/system-auth /etc/pam.d/password-auth
```

Khắc phục:

Chỉnh sửa file /etc/pam.d/password-auth và /etc/pam.d/system-auth để có tùy chọn sha512 cho pam_unix.so như dưới đây:

```
  Password sufficient pam_unix.so sha512
```

7. Tài khoản người dùng và môi trường

7.1. Thiết lập tham số cho shadow password

7.1.1. Thiết lập ngày hết hạn mật khẩu

Đánh giá :

- Level 1

Mô tả:

Tham số PASS_MAX_DAYS trong /etc/login.defs cho phép người quản trị cấu hình số ngày mật khẩu có hiệu lực. Khuyến cáo PASS_MAX_DAYS tham số được thiết lập để ít hơn hoặc bằng 90 ngày.

Mục đích :

Việc giới hạn số ngày sử dụng mật khẩu đăng nhập đảm bảo việc giảm thiểu bị tấn công bởi brute force

- **Đối tượng áp dụng**: CentOS 7 và 8

Kiểm tra:

```
# grep PASS_MAX_DAYS /etc/login.defs
PASS_MAX_DAYS 90
# chage --list <user>
Maximum number of days between password change: 90
```

Khắc phục:

Thiết lập tham số trong file /etc/login.defs:

```
PASS_MAX_DAYS 90
```

Thiết lập tham số user active:

```
#chage --maxdays 90 <user>
```

7.1.2. Thiết lập giới hạn số ngày tối thiểu thay đổi mật khẩu

Đánh giá :

- Level 1

Mô tả:

Tham số PASS_MIN_DAYS trong /etc/login.defs cho phép người quản trị để ngăn chặn người dùng thay đổi mật khẩu của họ cho đến khi số lượng ngày tối thiểu cho phép kể từ lần cuối cùng người dùng thay đổi mật khẩu của họ. khuyến cáo rằng tham số PASS_MIN_DAYS được thiết lập đến 7 ngày hoặc hơn.

Mục đích :

Bằng cách hạn chế tần suất thay đổi mật khẩu, quản trị viên có thể ngăn chặn người dùng liên tục thay đổi mật khẩu của họ trong một nỗ lực để phá vỡ quy tắc tái sử dụng mật khẩu

- **Đối tượng áp dụng**: CentOS 7 và 8

Kiểm tra:

```
# grep PASS_MIN_DAYS /etc/login.defs
PASS_MIN_DAYS 7
# chage --list <user>
Miniumum number of days between password change: 7
```

Khắc phục:

Thiết lập tham số trong file /etc/login.defs:

```
PASS_MIN_DAYS 7
```

Thiết lập tham số user active:

```
#chage --mindays 7 <user>
```

7.1.3. Thiết lập số ngày thực hiện cảnh báo hết hạn mật khẩu

Đánh giá :

- Level 1

Mô tả:

Tham số PASS_WARN_AGE trong /etc/login.defs cho phép người quản trị để thông báo cho người dùng rằng mật khẩu của họ sẽ hết hạn trong một số quy định của ngày. Khuyến cáo_WARN_AGE tham số được thiết lập đến 7 ngày hoặc hơn.

Mục đích :

Cung cấp trước cảnh báo rằng một mật khẩu sẽ được đáo hạn nhằm mục đích cho người sử dụng có thời gian để nghĩ ra một mật khẩu an toàn.

- **Đối tượng áp dụng**: CentOS 7 và 8

Kiểm tra:

```
# grep PASS_WARN_AGE /etc/login.defs
PASS_WARN_AGE 7
# chage --list <user>
Number of days of warning before password expires: 7
```

Khắc phục:

Thiết lập tham số trong file /etc/login.defs:

```
PASS_WARN_AGE 7
```

Thiết lập tham số user active:

```
# chage --warndays 7 <user>
```


7.2. Khóa các tài khoản không hoạt động

Đánh giá :

- Level 1

Mô tả:

Tài khoản người dùng đã không hoạt động trong một khoảng thời gian nhất định có thể được tự động bị vô hiệu hóa. Khuyến cáo rằng các tài khoản không hoạt động trong 35 ngày hoặc hơn sẽ bị vô hiệu.

Mục đích :

Các tài khoản không hoạt động trong một thời gian dài gây ra một mối đe dọa cho an ninh hệ thống.

- **Đối tượng áp dụng**: CentOS 7 và 8

Kiểm tra:

```
# useradd -D | grep INACTIVE
```

Khắc phục:

Chỉnh sửa file /etc/bashrc và /etc/profile thêm tham số:

```
PASS_WARN_AGE 7
```

Thiết lập tham số user active:

```
# useradd -D -f 35
```

III. HƯỚNG DẪN ĐẢM BẢO AN TOÀN BẢO MẬT CHO HỆ ĐIỀU HÀNH WINDOWS SERVER

1. Hướng dẫn các yêu cầu an toàn bảo mật

1.1 Chính sách tài khoản người dùng (User account policies)

1.1.1 Cấu hình độ dài tối thiểu của mật khẩu

Các cuộc tấn công cơ sở dữ liệu tài khoản bằng cách sử dụng các công cụ để tìm kiếm tài khoản và mật khẩu xảy ra rất nhiều. Việc cấu hình độ dài tối thiểu của mật khẩu được khuyến cáo ít nhất 8 ký tự trở lên.

Để thiết lập cấu hình được khuyến cáo thông qua Group Policy, hãy sử dụng đường dẫn sau để cấu hình có ít nhất 8 ký tự cho mật khẩu:

> ***"Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\ Password Policy\Minimum password length"***

1.1.2 Cấu hình yêu cầu độ phức tạp của mật khẩu

Các mật khẩu chỉ chứa các ký tự chữ số và chữ cái rất dễ dàng bị phát hiện bằng một số công cụ tấn công có sẵn.

Để thiết lập cấu hình mật khẩu với độ phức tạp được khuyến cáo thông qua Group Policy, hãy sử dụng đường dẫn sau để cấu hình mật khẩu phức tạp (Chữ hóa, chữ thường, số, ký tự đặc biệt):

> ***"Computer Configuration\Policies\Windows Settings\Security Settings\AccountPolicies \Password Policy\Password must meet complexity requirements" → Lựa chọn Enable***

1.1.3 Cấu hình giới hạn mật khẩu mới không trùng mật khẩu gần nhất

Để thiết lập cấu hình giới hạn mật khẩu mới không trùng mật khẩu gần nhất được khuyến cáo thông qua Group Policy, hãy sử dụng đường dẫn sau để cấu hình:

> ***"Computer Configuration\Policies\Windows Settings\Security Settings\AccountPolicies \Password Policy\Enforce password history***

1.1.4 Cấu hình không lưu trữ bản mã dịch ngược của mật khẩu

Việc lưu mã ngược của mật khẩu có nguy cơ bị giải mã bởi những người am hiểu về mã hóa.

Cấu hình không lưu trữ mã dịch ngược của mật khẩu giúp hạn chế tấn công và giải mã.

"Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Store passwords using reversible encryption"

1.1.5 Cấu hình chính sách khóa tài khoản

Việc triển khai một chính sách khóa tài khoản hợp lý là rất quan trọng vì nó sẽ giúp bảo vệ chống lại các cuộc tấn công rò quét mật khẩu.

Để thiết lập cấu hình được khuyến cáo thông qua Group Policy, đặt các giá trị như sau:

- Thời gian tối thiểu khóa tài khoản: từ 15 phút trở lên.

"Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Account Lockout Policy"

- Ngưỡng khóa tài khoản: 10 lần đăng nhập không thành công.

"Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold "

1.2 Phân quyền người dùng (User rights asignment)

1.2.1 Đảm bảo quyền "Act as part of the operating system" được đặt "No one"

Quyền người dùng "Act as part of the operating system" có thể kiểm soát hoàn toàn thiết bị và xóa bỏ bằng chứng về các hoạt động của thiết bị. Trạng thái này được khuyến cáo cài đặt "No One" (Không ai cả) để đảm bảo an toàn.

Để thiết lập được cấu hình được khuyến cáo thông qua Group Policy, hãy sử dụng đường dẫn UI sau và chuyển trạng thái sang "No One":

"Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Act as part of the operating system"

1.2.2 Cấu hình banner bảo mật khi đăng nhập

Hiển thị thông báo cảnh báo trước khi đăng nhập có thể giúp ngăn chặn các cuộc tấn công bằng cách cảnh báo kẻ tấn công về hậu quả của hành vi không đúng đắn trước khi nó xảy ra. Ngoài ra, điều này cũng có thể giúp củng cố chính sách doanh nghiệp bằng cách thông báo cho nhân viên về chính sách thích hợp trong quá trình đăng nhập.

Để thiết lập được cấu hình Banner bảo mật khi đăng nhập thông qua Group Policy, hãy sử dụng đường dẫn Registry sau:

"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies \System: LegalNoticeCaption"

1.3 Audit Policy Setting

Thực hiện kích hoạt các chính sách kiểm tra sau đây để có thể sử dụng trong trường hợp xảy ra sự cố để thực hiện điều tra thêm.

1.3.1 Cấu hình không hiển thị trạng thái hoạt động của user Guest

Tài khỏa Guest cho phép người dùng chưa xác thực truy cập vào hệ thống.

Cần thực hiện cấu hình tắt kiểm tra tài khoản Guest đang hoạt động hay không theo đường dẫn như sau:

"Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Guest account status" → Disable

1.3.2 Quản lý tài khoản

- Bật chính sách "Audit Application Group Management" để ghi lại kiểm tra các sự kiện được tạo ra bởi thay đổi đối với các nhóm ứng dụng bằng cách thực hiện theo đường dẫn như sau:

"Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Application Group Management"

- Bật chính sách "Audit Computer Account Management" để kiểm tra các sự kiện giúp hỗ trợ khi thực hiện điều tra số đối với các sự cố bảo mật (tài khoản được tạo, thay đổi, xoá, đổi tên, kích hoạt, vô hiệu hoá) bằng cách thực hiện theo đường dẫn như sau:

"Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Computer Account Management"

- Bật chính sách "Audit Distribution Group Management" để kiểm tra chính sách này giúp quản trị viên có thể theo dõi các sự kiện nhằm phát hiện việc tạo nhóm tài khoản độc hại, ngẫu nhiên và được uỷ quyền bằng cách thực hiện theo đường dẫn sau:

"Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Distribution Group Management"

- Bật chính sách "Audit Other Account Management Event" để kiểm tra các sự kiện giúp hỗ trợ khi thực hiện điều tra số đối với các sự cố bảo mật tài khoản (Password hash đã bị truy cập, Password policy checking API được gọi) bằng cách thực hiện theo đường dẫn sau:

"Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\ Audit Other Account Management Event"

- Bật chính sách "Audit Security Group Management" để kiểm tra các sự kiện giúp hỗ trợ khi thực hiện điều tra số đối với các sự cố bảo mật qua đường dẫn như sau:

• ***Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Distribution Group Management***
• ***Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Security Group Management***

1.3.3 Theo dõi chi tiết

-Bật chính sách "Audit Process Creation" để kiểm tra các sự kiện giúp hỗ trợ khi thực hiện điều tra số bảo mật (Tạo tiến trình mới, Primary token được chỉ định xử lý) bằng cách thực hiện theo đường dẫn sau:

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit Process Creation

1.3.4 Truy cập thư mục dịch vụ

-Bật chính sách "Audit Directory Service Access" để kiểm tra các sự kiện giúp hỗ trợ khi thực hiện điều tra số đối với các sự cố bảo mật, được ghi lại khi một đối tượng AD DS (Active Directory Domain Services) được truy cập bằng cách thực hiện theo đường dẫn sau:

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\DS Access\Audit Directory Service Access

- Bật chính sách "Audit Directory Service Changes" để kiểm tra các sự kiện giúp hỗ trợ khi thực hiện điều tra số đối với các sự cố bảo mật (Đối tượng DS đã bị sửa đổi, được tạo, được phục hồi, đã bị di chuyển) bằng cách thực hiện theo đường dẫn sau:

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\ Audit Directory Service Changes

1.3.5 Đăng nhập/ đăng xuất

- Bật chính sách "Audit account lockout" qua đường dẫn như sau:

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Account Lockout

- Bật chính sách "Audit Logoff" và "Audit Logon" để kiểm tra xác định người dùng nào đã truy cập hoặc cố gắng truy cập vào hệ thống bằng cách thực hiện theo đường dẫn sau:

• ***Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Logoff***
• ***Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Logon***

- Bật chính sách "Audit Other Logon/Logoff Event" để kiểm tra các sự kiện đăng nhập/ đăng xuất khác (ví dụ: những sự kiện ngắn kết nối/ kết nối lại các phiên đăng nhập từ xa) bằng cách thực hiện theo đường dẫn sau:

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Other Logon/Logoff Event

- Bật chính sách "Audit Special Logon" để kiểm tra các sự kiện đăng nhập với quyền tương đương quản trị viên hoặc cao hơn giúp hỗ trợ thực hiện điều tra số đối với các sự cố bảo mật bằng cách thực hiện theo đường dẫn:

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\ Audit Special Logon

1.3.6 Thay đổi chính sách

- Bật chính sách "Audit audit policy change" để kiểm tra các sự kiện liên quan tới việc thay đổi chính sách (SACL) bằng cách thực hiện theo đường dẫn như sau:

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Audit Policy Change

- Bật chính sách "Audit Authentication Policy Change" để kiểm tra các sự kiện liên quan tới việc thay đổi chính sách xác thực (Trusted domain, Kerberos,…) bằng cách thực hiện theo đường dẫn sau:

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\ Audit Authentication Policy Change

1.3.7 Sử dụng đặc quyền

- Bật chính sách "Audit Sensitive Privilege Use" để ghi lại các sự kiệ khi tài khoản người sử dụng quyền thực thi tác vụ (Backup, tạo token object, gỡ lỗi, thay đổi giá trị firmware) bằng cách thực hiện theo đường dẫn như sau:

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Privilege Use\Audit Sensitive Privilege Use

1.4 Sysmon Setting

Sysmon (System Monitor) là một công cụ từ Sysinternals suite của Microsoft, giúp ghi lại các sự kiện hệ thống chi tiết về các hoạt động như tạo tiến trình, kết nối mạng và thay đổi file. Sysmon là một công cụ mạnh mẽ cho việc giám sát bảo mật và phát hiện xâm nhập.

1.4.1 Tải Sysmon

Truy cập trang Sysinternals trên web của Microsoft để tải Sysmon phiên bản mới nhất theo đúng hệ điều hành: https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon

1.4.2 Cài đặt Sysmon

- Bước 1: Giải nén file đã tải xuống.

- Bước 2: Mở Command Prompt với quyền quản trị (Run as Administrator).

- Bước 3: Di chuyển thư mục chứa Sysmon theo hướng dẫn:

```
cd path\to\sysmon
```

- Bước 4: Cài đặt Sysmon với cấu hình mặc định

```
sysmon -accepteula -i
```

1.4.3 Cấu hình Sysmon

- Bước 1: Tạo một file XML (ví dụ: `sysmonconfig.xml`).

- Bước 2: Cấu hình ghi lại các Event ID cần thiết (Khuyến nghị Event ID: 1, 3, 8, 11, 17, 18 và 22).

```
<Sysmon schemaversion="4.22">
  <!-- Capture process creation (Event ID 1) -->
  <EventFiltering>
    <ProcessCreate onmatch="include"/>
  </EventFiltering>

  <!-- Capture network connections (Event ID 3) -->
  <EventFiltering>
    <NetworkConnect onmatch="include"/>
  </EventFiltering>

  <!-- Capture create remote thread (Event ID 8) -->
  <EventFiltering>
    <CreateRemoteThread onmatch="include"/>
```

```
  </EventFiltering>

  <!-- Capture file creation (Event ID 11) -->
  <EventFiltering>
    <FileCreate onmatch="include"/>
  </EventFiltering>

  <!-- Capture named pipe creation (Event ID 17) -->
  <EventFiltering>
    <PipeEvent onmatch="include">
      <PipeCreate onmatch="include"/>
    </PipeEvent>
  </EventFiltering>

  <!-- Capture named pipe connection (Event ID 18) -->
  <EventFiltering>
    <PipeEvent onmatch="include">
      <PipeConnected onmatch="include"/>
    </PipeEvent>
  </EventFiltering>

  <!-- Capture DNS queries (Event ID 22) -->
  <EventFiltering>
    <DnsQuery onmatch="include"/>
  </EventFiltering>
</Sysmon>
```


1.4.4 Áp dụng File cấu hình

- Bước 1: Mở Command Prompt với quyền quản trị

- Bước 2: Di chuyển đến thư mục chứa Sysmon

- Bước 3: Áp dụng cấu hình mới theo hướng dẫn:

```
sysmon -c sysmonconfig.xml
```

1.4.5 Kiểm tra và giám sát

- Kiểm tra trạng thái Sysmon theo hướng dẫn sau:

```
sysmon -s
```

- Xem sự kiện Sysmon trong Event Viewer theo hướng dẫn sau:

  - Bước 1: Mở Event Viewer (Nhấn 'Windows + R', nhập **'eventvwr.msc**', và nhấn Enter).
  - Bước 2: Điều hướng đến 'Applications and Services Logs' → 'Microsoft' → 'Windows' → 'Sysmon' → 'Operational'.

1.4.6 Giải thích chi tiết các Event ID

- Event ID 1 (Process Creation): Ghi lại khi một tiến trình mới được tạo. Bao gồm chi tiết về tiến trình cha và tiến trình con.

- Event ID 3 (Network Connection): Ghi lại các kết nối mạng bao gồm địa chỉ IP, cổng nguồn và đích.

- Event ID 8 (Create Remote Thread): Ghi lại khi một tiến trình tạo một thread từ xa trong một tiến trình khác. Đây là một dấu hiệu thường thấy trong các cuộc tấn công chèn mã độc.

- Event ID 11 (File Creation): Ghi lại khi một file được tạo hoặc ghi lại trên hệ thống.

- Event ID 17 (Named Pipe Created): Ghi lại khi một pipe named mới được tạo.

- Event ID 18 (Named Pipe Connection): Ghi lại khi có một kết nối tới một pipe named đã được tạo.

- Event ID 22 (DNS Query): Ghi lại các truy vấn DNS, bao gồm tên miền và địa chỉ IP đích.

2. Cài đặt và cập nhật các bản vá bảo mật

Việc không cập nhật các bản vá bảo mật sẽ dẫn tới nguy cơ tồn tại những lỗ hổng mức độ cao, có thể bị lợi dụng để tấn công chiếm quyền điều khiển máy chủ hoặc làm hệ thống bị tê liệt. ngừng hoạt động.

Cập nhật các bản vá bảo mật quan trọng (Security Update) từ danh sách Windows Update hoặc theo chính sách của Tổng công ty với thời gian quy định.

***Lưu ý:** Tiến hành trên hệ thống thử nghiệm trước khi cập nhập bản vá và phải kiểm tra lạii các dịch vụ của máy chủ sau khi thực hiện nâng cấp.*

3. Kiểm tra cài đặt phần mềm Anti-virus

- Kiểm tra trạng thái phần mềm: Đảm bảo trạng thái bảo vệ luôn được bật Protected: On

- Kiểm tra tính năng tự động cập nhật để đảm bảo luôn sử dụng các phiên bản mới nhất: đảm bảo tính năng tự động cập nhật được cập nhật (1 ngày/lần).

***Lưu ý:** Việc thực hiện có thể thay đổi theo thời gian quy định từ chính sách ATTT của Tổng công ty ban hành.*

- Thực hiện lịch quét định kỳ máy chủ: Đảm bảo thực hiện lịch quét định kỳ máy chủ (1 tháng/ lần).

***Lưu ý**: Việc thực hiện có thể thay đổi theo thời gian quy định từ chính sách ATTT của Tổng công ty.*

4. Cấu hình Backup

Để thực hiện phòng ngừa mất dữ liệu do hỏng phần cứng, phần mềm và đối phó với tấn công mạng, ransomeware, virus độc hại thì công việc Backup rất cần thiết.

Cấu hình backup trên Windows Server có thể thực hiện bằng cách sử dụng công cụ Windows Server Backup. Dưới đây là hướng dẫn chi tiết về cách cấu hình backup cho Windows Server.

Bước 1: Cài Đặt Windows Server Backup

- Mở Server Manager:

  - Click vào nút **Start**, chọn **Server Manager**.

- Thêm Vai Trò và Tính Năng:

  - Trong **Server Manager**, chọn **Manage** > **Add Roles and Features**.
  - Trong wizard **Add Roles and Features**, nhấn **Next** cho đến khi bạn đến trang **Features**.

- Chọn Tính Năng:

  - Chọn **Windows Server Backup** và nhấn **Next**, sau đó nhấn **Install** để cài đặt.

Bước 2: Cấu Hình Backup

Tạo một lịch trình backup

- Mở Windows Server Backup:

  - Trong **Server Manager**, chọn **Tools** > **Windows Server Backup**.

- Tạo Lịch Trình Backup:

  - Trong Windows Server Backup, chọn **Local Backup**.
  - Trong panel **Actions**, chọn **Backup Schedule** để mở wizard **Backup Schedule**.

Cấu hình lịch trình backup trong Backup Schedule Wizard:

- Getting Started:

  - Nhấn **Next**.

- Select Backup Configuration:

  - Chọn **Full server (recommended)** để sao lưu toàn bộ máy chủ hoặc chọn **Custom** để chọn các ổ đĩa hoặc thư mục cụ thể.
  - Nhấn **Next**.

- Specify Backup Time:

  - Chọn **Once a day** hoặc **More than once a day** và cấu hình thời gian backup.
  - Nhấn **Next**.

- Specify Destination Type:

  - Chọn nơi lưu trữ backup, có thể là ổ đĩa cục bộ, ổ đĩa ngoài hoặc chia sẻ mạng.
  - Nhấn **Next** và làm theo các hướng dẫn để cấu hình vị trí lưu trữ.

- Confirmation:

  - Xác nhận các thiết lập và nhấn **Finish** để tạo lịch trình backup.

IV. HƯỚNG DẪN CẤU HÌNH ĐẢM BẢO AN TOÀN BẢO MẬT CHO THIẾT BỊ MẠNG

1. Đối tượng áp dụng: Cisco

1.1 Đặt tên thiết bị

Thực hiện đặt tên thiết bị: bao gồm tối thiểu tên đơn vị quản lý, địa điểm đặt thiết bị, tên vai trò thiết bị,…

VD: TCTK_YHA_INT_01

Để thực hiện đặt tên cho thiết bị thực hiện theo hướng dẫn sau:

```
Hostname <Tên thiết bị>
```


1.2 Thiết lập cấu hình Banner khi truy cập thiết bị

Để thiết lập hiển thị cảnh báo banner khi truy cập vào thiết bị mạng, có thể làm theo các bước sau:

```
configure terminal
banner motd $
Warning!!!
This is asset of MBF, only permit authorized person.
$
```

1.3 Cấu hình thời gian idle tự động ngắt sau phiên làm việc

Để cấu hình thời gian idle tự động ngắt kết nối sau một phiên làm việc trên các thiết bị mạng, bạn có thể thực hiện các dbước sau:

Khuyến nghị ngắt kết nối phiên sau 5 phút không sử dụng

```
line vty 0-15
    exec-timeout 5 0
line con 0
exec-timeout 5 0
     line aux 0
exec-timeout 5 0
```

1.4 Cấu hình giới hạn địa chỉ IP cho phép truy cập quản trị

Để thực hiến cấu hình giới hạn địa chỉ IP cho phép truy cập quản trị, ta thực hiện theo các bước sau:

```
ip access-list extended ADMINMBF
 permit host 1.1.1.1
 permit host 2.2.2.2
!
line vty 0-15
 access-class ADMINMBF in
!
login quiet-mode access-class ADMINMBF
```


1.5 Cấu hình tắt các Service và Interface không sử dụng Shutdown

Thực hiện cấu hình tắt các Service và Interface không sử dụnh theo hướng dẫn:

```
service tcp-keepalives-in
service tcp-keepalives-out
no service tcp-small-servers
no service udp-small-servers
no service pad
no service finger
no ip finger
no cdp run
no ip http server
no ip http secure-server
no ip domain-lookup
no ip source-route
no ip gratuitous-arps
no ip bootp server
no ip identd
no tftp server
no boot network
no service config
default interface <INTERFACE-ID>
interface <INTERFACE-ID>
shutdown
```

1.6 Cấu hình xác thực cho các cổng AUX và Console

Thực hiện cấu hình xác thực cho các cổng AUX và Console theo hướng dẫn sau:

```
line aux 0
no excec
line console 0
password <PASSWORD>
logging synchronous
login
```


1.7 Cấu hình xác thực tập trung (Nếu có AAA)

Thực hiện cấu hình xác thực tập trung (nếu có AAA) theo hướng dẫn sau:

```
aaa new-model
aaa group server tacacs+ TACACS_MBF
 server <TACACS SRRVER IP 01>
 server <TACACS SRRVER IP 02>
aaa authentication login default local group TACACS_MBF
aaa authorization exec default local group TACACS_MBF
aaa authorization commands 15 default local group TACACS_MBF
aaa accounting exec default start-stop group TACACS_MBF
aaa accounting commands 15 default start-stop group TACACS_MBF
ip tacacs source-interface <INTERFACE>
tacacs-server host <TACACS_SRV_01> key <KEY>
tacacs-server host <TACACS_SRV_02> key <KEY>
tacacs-server directed-request
```

1.8 Cấu hình đồng bộ thời gian qua NTP tập trung

Thực hiện cấu hình đồng bộ thời gian qua NTP tập trung theo hướng dẫn sau:

```
clock timezone GMT 7
ntp logging
ntp source <INTERFACE>
ntp server <NTP_SERVER_1>
## Cấu hình xác thực (nếu có)
ntp authentication-key 1 md5 <KEY>
ntp authenticate
```

```
ntp trusted-key 1
```

1.9 Cấu hình an toàn cho SNMP và giới hạn IP truy cập

Thực hiện cấu hình an toàn cho SNMP và giới hạn Ip truy cập theo hướng dẫn sau:

```
snmp-server trap-source <INTERFACE-ID>
snmp-server source-interface informs <INTERFACE-ID>
snmp-server location <LOCATION>
snmp-server contact <CONTACT>
!
# Đối với các thiết bị hỗ trợ SNMPv3:
ip access-list standard SNMP_ACCESS
     permit host <SERVER_01>
     permit host <SERVER_02>
     deny any log
snmp-server group SNMP_GROUP_RO v3 auth read v1default
 access SNMP_ACCESS
snmp-server user SNMP_USR_RO SNMP_GROUP_RO
 v3 auth md5 <STRING>
snmp-server host < SERVER_01> version 3 auth
 SNMP_USR_ReadOnly
snmp-server host < SERVER_02> version 3 auth
 SNMP_USR_RO
!
Đối với các thiết bị chưa hỗ trợ SNMPv3:
ip access-list standard SNMP_ACCESS
     permit host < SERVER_01>
     permit host < SERVER_02>
     deny any log
snmp-server community <COMMUNITY_STRING>
 ro SNMP_ACCESS
snmp-server host < SERVER_01> version 2c
snmp-server host < SERVER_02> version 2c
```

1.10Cấu hình giao thức truy cập từ xa SSH

- Mục đích: cấu hình giao thức truy cập từ xa SSH

- Thực hiện:

  - Kiểm tra cấu hình SSH

```
show ip ssh
```

  - Khi cấu hình SSH chưa được cấu hình, tiến hành cấu hình các bước sau:

```
username SSHadmin privilege 15 secret cisco123
line vty 0 4
login local
transport input ssh
```

  - Cấu hình tên miền cho thiết bị

```
Ip domain-name MobiFone.vn
```

  - Tạo cặp khóa RSA (Khóa này sử dụng cho các kết nối bảo mật như SSH)

```
crypto key generate rsa general-keys modulus 1024
```

  - Cấu hình thời gian Timeout: thời gian chờ cho các kết nối SSH là 60 giây và số lần xác thực tối đa cho acsc kết nối SSH là 3 lần, nhập sai quá 3 lần sẽ bị từ chối.

```
ip ssh version 2
ip ssh time-out 60
ip ssh authentication-retries 3
```

  - Cấu hình chặn đăng nhập trong 120 giây nếu có 3 lần đăng nhập thất bạu trong vòng 60 giây. Điều này giúp ngăn chặn các cuộc tấn ccoong Brute force.

```
login block-for 120 attemps 3 within 60
```

```
line vty 0-15
transport input ssh
```

- Cấu hình ghi log khi có đăng nhập (thành công và thất bại)

```
login on-success log
login on-failure log
```


1.11Cấu hình mật khẩu

- Mục đích: Cấu hình độ phức tạp của mật khẩu

- Thực hiện:

  - Độ dài tối thiểu
  - Mật khẩu lưu dạng mã hóa

```
enable secret <PASS>
username <LOCAL_USER> secret <PASS>
service password-encryption
```

1.12Cấu hình đẩy log lên SIEM

- Mục đích: Cấu hình đẩy log lên SIEM

- Thực hiện:

  - Thực hiện cấu hình theo hướng dẫn

```
(config)#logging host IP_SIEM
(config)# logging source-interface ethernet 1/0 <- Dùng cổng Eth1/0 để gởi log nhật ký
```

  - Kiểm tra cấu hình:

```
(config)#do show logging
```

1.13Cấu hình số lần xác thực không thành công (Nếu có AAA)

- Mục đích: Cấu hình số lần tối đa xác thực không thành công (Khuyến nghị tối đa 05 lần đăng nhập thất bại)

- Thực hiện:

```
Router# config terminal
Router(config)# username john-admin secret Lms!a2eZSf*%
Router(config)# aaa new-model
Router(config)# aaa local authentication attempts max-fail 5        <-
tối đa 5 lần đăng nhập
Router(config)# aaa authentication login default local
```


1.14Cấu hình Backup

- Mục đích: Để thực hiện phòng ngừa mất dữ liệu do hỏng phần cứng, phần mềm và đối phó với tấn công mạng, ransomeware, virus độc hại thì công việc Backup rất cần thiết.

- Thực hiện: Sử dụng công cụ Config Archive có sẵn

*Ví dụ: cấu hình config archive sao lưu tới server FTP(x.x.x.x) với lựa chọn (**write-memory**: sao lưu khi thực hiện lưu cấu hình và **time-period 1440**: sao lưu sau 1440 phút = 24 giờ) và giới hạn số lượng bản sao lưu là 14 (tới bản thứ 15 tự động xoá bản sao lưu cũ nhất).*

```
Switch# archive
Switch(config-archive)# path ftp://x.x.x.x/switch-backup
Switch(config-archive)# write-memory
Switch(config-archive)# period 1440
Switch(config-archive)# maximum 14
```

- Kiểm tra:

```
Switch# show archive
```

2. Đối tượng áp dụng: Juniper

2.1 Đặt tên thiết bị

Thực hiện đặt tên thiết bị: bao gồm tối thiểu tên đơn vị quản lý, địa điểm đặt thiết bị, tên vai trò thiết bị,…

VD: TCTK_YHA_INT_01

Để thực hiện đặt tên cho thiết bị thực hiện theo hướng dẫn sau:

```
set system host-name <Tên thiết bị>
```

2.2 Thiết lập cấu hình Banner khi truy cập thiết bị

Để thiết lập hiển thị cảnh báo banner khi truy cập vào thiết bị mạng, có thể làm theo các bước sau:

```
Set system login message

“Warning!!! This is asset of MBF, only permit authorized person”
```

2.3 Cấu hình thời gian idle tự động ngắt sau phiên làm việc

Để cấu hình thời gian idle tự động ngắt kết nối sau một phiên làm việc trên các thiết bị mạng, bạn có thể thực hiện các bước sau:

Khuyến nghị ngắt kết nối phiên sau 5 phút không sử dụng

```
set system login class “class-name” idle-time 5
```

2.4 Cấu hình giới hạn địa chỉ IP cho phép truy cập quản trị

Để thực hiến cấu hình giới hạn địa chỉ IP cho phép truy cập quản trị, ta thực hiện theo các bước sau:

```
set policy-options prefix-list admin-mbf-ip 10.x.y.z/24
set policy-options prefix-list admin-mbf-ip 10.x.y.z/24



set firewall filter MBFADMIN term DENY_NON_ADMIN from source-address 0.0.0.0/0
set firewall filter MBFADMIN term DENY_NON_ADMIN from source-prefix-list admin-mbf-ip except
set firewall filter MBFADMIN term DENY_NON_ADMIN from protocol tcp
```

```
set firewall filter MBFADMIN term DENY_NON_ADMIN from destination-port ssh
set firewall filter MBFADMIN term DENY_NON_ADMIN from destination-port telnet
set firewall filter MBFADMIN term DENY_NON_ADMIN then discard
set firewall filter MBFADMIN term ACCEPT_EVERYTHING then accept

set interfaces lo0 unit 0 family inet filter input MBFADMIN
!
```


2.5 Cấu hình tắt các Service và Interface không sử dụng Shutdown

Thực hiện cấu hình tắt các Service và Interface không sử dụnh theo hướng dẫn:

```
Set interface <interface name> disable
delete interfaces <interface name> unit <unit number> proxy-arp
```

2.6 Cấu hình xác thực cho các cổng AUX và Console

Thực hiện cấu hình xác thực cho các cổng AUX và Console theo hướng dẫn sau:

```
set system root-authentication plain-text-password
set ports auxiliary disable
```

2.7 Cấu hình xác thực tập trung (Nếu có AAA)

Thực hiện cấu hình xác thực tập trung (nếu có AAA) theo hướng dẫn sau:

```
set system authentication-order tacplus
set system authentication-order password
set system tacplus-server IP-SERVER secret secretpass
```

2.8 Cấu hình đồng bộ thời gian qua NTP tập trung

Thực hiện cấu hình đồng bộ thời gian qua NTP tập trung theo hướng dẫn sau:

```
set system ntp boot-server IP-NTP-SRV
set system ntp server IP-NTP-SRV version <version number>
set system ntp server IP-NTP-SRV prefer
```

2.9 Cấu hình an toàn cho SNMP và giới hạn IP truy cập

Thực hiện cấu hình an toàn cho SNMP và giới hạn Ip truy cập theo hướng dẫn sau:

```
[edit firewall family inet filter filter_name term PERMIT-SNMP]
set from source-address IP ADDRESS
set from protocol udp
set from destination-port snmp
set then accept
set then syslog
set then log
[edit firewall family inet filter filter_name term DENY-SNMP]
set from destination-port snmp
set then discard
set then syslog
set then log
```


2.10Cấu hình giao thức truy cập từ xa SSH

- Mục đích: cấu hình giao thức truy cập từ xa SSH, phân quyền user

- Thực hiện:

  - Bật giao thức SSH

```
set system services ssh
set system login user <username> class super-user
set system login user <username> authentication encrypted-password
deactivate system login user <user_unused>
```

2.11Thay đổi cấu hình mật khẩu

- Mục đích: Cấu hình mật khẩu

```
set system root-authentication encrypted-password password
```

2.12Cấu hình đẩy log lên SIEM

- Mục đích: Cấu hình đẩy log lên SIEM

- Thực hiện:

- Thực hiện cấu hình theo hướng dẫn

```
set system syslog host IP SIEM any any
set system syslog host IP SIEM port 514
```

2.13Cấu hình backup

- Mục đích: Các cấu hình thiết bị phải được backup

- Thực hiện:

  - Thực hiện cấu hình theo hướng dẫn:

```
Request system snapshot media usb
Show configuration | no-more and save to file.
```