Gáy

**Gáy**

DƯƠNG THỊ MỸ SƯƠNG MSSV: N19DCAT066 Tên Đề tài: CIS CentOS 7 Lớp: D19CQAT01-N 2022-2023

Benchmark ứng dụng trong bài toán xác định Exposure Risk

**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

------------------------------

A red circle with a star and a book

Description automatically generated

**BÁO CÁO THỰC TẬP**

**TỐT NGHIỆP ĐẠI HỌC**

BÁO CÁO THỰC ĐỊNH KỲ THỰC TẬP TỐT NGHIỆP ĐẠI HỌC

***Đề tài*: “CIS CentOS 7 Benchmark và ứng dụng trong bài toán xác định Exposure Risk”**

**Người hướng dẫn : TS.NGUYỄN MINH HẢI**

**Sinh viên thực hiện : DƯƠNG THỊ MỸ SƯƠNG**

**Mã số sinh viên : N19DCAT066**

**Lớp : D19CQAT01-N**

**Khoá** **: 2019 – 2024**

**Hệ** **: ĐẠI HỌC CHÍNH QUY**

TP. HCM

2023

**TP.HCM, tháng 7/2023**

**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

-----------------------------

A red circle with a star and a book

Description automatically generated

**BÁO CÁO THỰC TẬP**

**TỐT NGHIỆP ĐẠI HỌC**

BÁO CÁO THỰC ĐỊNH KỲ THỰC TẬP TỐT NGHIỆP ĐẠI HỌC

***Đề tài*: “ CIS CentOS 7 Benchmark và ứng dụng trong bài toán xác định Exposure Risk”**

**Người hướng dẫn : TS.NGUYỄN MINH HẢI**

**Sinh viên thực hiện : DƯƠNG THỊ MỸ SƯƠNG**

**Mã số sinh viên : N19DCAT066**

**Lớp : D19CQAT01-N**

**Khoá** **: 2019 – 2024**

**Hệ** **: ĐẠI HỌC CHÍNH QUY**

**TP.HCM, tháng 7/2023**

**PHIẾU GIAO ĐỀ CƯƠNG THỰC TẬP TỐT NGHIỆP ĐƯỢC PHÊ DUYỆT**

**LỜI CẢM ƠN**

Để hoàn thành được báo cáo thực tập tốt nghiệp này thì em xin cảm ơn tới ban lãnh đạo Học viện, Khoa đào tạo – Khoa Công Nghệ Thông Tin 2 đã thiết lập khung chương trình có môn học “Thực tập” để em có thể vận dụng những kiến thức học được trên giảng đường áp dụng vào công việc và được tham quan, tìm hiểu về môi trường doanh nghiệp.

Ngoài ra, em xin gửi lời cảm ơn tới Thầy NGUYỄN MINH HẢI – Giảng viên hướng dẫn đã luôn nhiệt tình chỉ dẫn, giảng dạy cho em những kiến thức về “CIS CentOS 7 Benchmark và ứng dụng vào bài toán tính toán Exposure Risk”, những tài liệu và phương pháp để em có thể hoàn thiện đồ án thực tập này hơn. Nhờ Thầy luôn dìu dắt, giúp đỡ và chỉ dạy tận tình cho em để hoàn thành tốt Thực tập.

Trong quá trình thực hiện đồ án, tuy đã cố gắng nhưng em vẫn còn những hạn chế về thời gian tìm hiểu, kiến thức cũng như là kinh nghiệm và vẫn còn nhiều sai sót. Em rất mong được nhận những ý kiến đóng góp và nhận xét của giáo viên hướng dẫn cùng quý thầy cô để đồ án thực tập tốt nghiệp của em có thể hoàn thiện tốt hơn.

Em xin chân thành cảm ơn!

TP.HCM, ngày tháng năm 2023

Sinh viên thực hiện

Dương Thị Mỹ Sương

**MỤC LỤC**

[**MỞ ĐẦU** 1](#_Toc141608501)

[**CHƯƠNG 1.** **GIỚI THIỆU CIS CENTOS 7 BENCHMARK** 3](#_Toc141608502)

[**1.1** **Tổng quan về CIS Benchmark** 3](#_Toc141608503)

[**1.1.1** **CIS là gì?** 3](#_Toc141608504)

[**1.1.2** **Khái niệm CIS Benchmark** 3](#_Toc141608505)

[**1.1.3** **CIS Benchmark được tổ chức như thế nào?** 4](#_Toc141608506)

[**1.1.4** **Các cấp độ của CIS Benchmark** 6](#_Toc141608507)

[**1.1.5** **Lợi ích của CIS Benchmark** 7](#_Toc141608508)

[**1.1.6** **Làm thế nào để triển khai CIS Benchmark?** 7](#_Toc141608509)

[**1.2** **CIS CENTOS 7 BENCHMARK** 8](#_Toc141608510)

[**1.2.1** **Tổng quan về CentOS 7** 8](#_Toc141608511)

[**1.2.1.1** **CentOS 7 là gì?** 8](#_Toc141608512)

[**1.2.1.2** **Cấu trúc của CentOS 7** 8](#_Toc141608513)

[**1.2.1.3** **Ưu điểm của CentOS 7** 9](#_Toc141608514)

[**1.2.1.4** **Các phiên bản của CentOS 7** 9](#_Toc141608515)

[**1.2.2** **Tổng quan về CIS CentOS 7 Benchmark** 10](#_Toc141608516)

[**1.2.2.1** **Các tiêu chuẩn trong CIS CentOS 7 Benchmark** 11](#_Toc141608517)

[**CHƯƠNG 2.** **HIỆN THỰC VIỆC ĐO ĐẠC COMPLIANCE CỦA SERVER** 75](#_Toc141608518)

[**2.1** **Tổng quan về Compliance** 75](#_Toc141608519)

[**2.2** **Tại sao cần phải tuân thủ theo CIS Benchmark?** 75](#_Toc141608520)

[**2.3** **Cách hiện thực việc đo đạc Compliance của Server** 76](#_Toc141608521)

[**CHƯƠNG 3.** **EXPOSURE RISK** 77](#_Toc141608522)

[**3.1** **Tổng quan về Exposure Risk** 77](#_Toc141608523)

[**3.2** **Cơ sở lý thuyết để tính toán Exposure Risk theo Tenable** 77](#_Toc141608524)

[**3.2.1** **Các thành phần để tính toán Exposure Risk** 77](#_Toc141608525)

[**3.2.1.1** **VPR: Remediation Priority of a Single Vulnerability** 78](#_Toc141608526)

[**3.2.1.2** **ACR: Relative Business Criticality of a Given Asset** 78](#_Toc141608527)

[**3.2.2** **Cách tính toán Exposure Risk** 79](#_Toc141608528)

[**3.3** **Các yếu tố có thể xem xét khi đánh giá Exposure Risk** 79](#_Toc141608529)

[**3.4** **Tổng quan về Bài toán xác định Exposure Risk** 80](#_Toc141608530)

[**CHƯƠNG 4.** **THỰC THI COMPLIANCE TRÊN SERVER VÀ TÍNH TOÁN EXPOSURE RISK**  82](#_Toc141608531)

[**4.1** **Thực thi Compliance trên Server** 82](#_Toc141608532)

[**4.1.1** **Chuẩn bị** 82](#_Toc141608533)

[**4.1.1.1** **Máy chủ CentOS 7** 82](#_Toc141608534)

[**4.1.1.2** **File lưu trữ các script trên máy chủ CentOS 7** 82](#_Toc141608535)

[**4.1.2** **Thực hiện** 82](#_Toc141608536)

[**4.1.3** **Kết quả** 82](#_Toc141608537)

[**4.2** **Tính toán Exposure Risk** 82](#_Toc141608538)

[**CHƯƠNG 5.** **KẾT LUẬN** 83](#_Toc141608539)

[**DANH MỤC TÀI LIỆU THAM KHẢO** 84](#_Toc141608540)

**DANH MỤC CÁC BẢNG, SƠ ĐỒ, HÌNH VẼ**

[Hình 1.1: CIS là gì? 3](#_Toc141607852)

[Hình 1.2: CIS Benchmark là gì? 3](#_Toc141607853)

[Hình 1.3: CentOS 7 là gì? 8](#_Toc141607854)

[Table 1.1: Các phiên ban của CentOS 7 9](#_Toc141607855)

[Hình 3.1: Tổng quan các thành phần của Exposure Risk 77](#_Toc141607856)

**KÍ HIỆU CÁC CỤM TỪ VIẾT TẮT**

|  |  |  |
| --- | --- | --- |
| Từ viết tắt | Từ đầy đủ | Giải nghĩa |
| CNTT | Công nghệ thông tin | Công nghệ thông tin |
| CIS | Center for Internet Security | Trung tâm An ninh Internet |
| VPR | Vulnerability Priority Rating | Đánh giá ưu tiên lỗ hổng |
| ACR | Asset Criticality Rating | Đánh giá mức độ quan trọng của tài sản |
| AES | Asset Exposure Score |  |
| CES | Cyber Exposure Score |  |

# **GIỚI THIỆU CIS CENTOS 7 BENCHMARK**

## **Tổng quan về CIS Benchmark**

### **CIS là gì?**



Hình 1.1: CIS là gì?

CIS là viết tắt của “Center for Internet Security” – Trung tâm An ninh Internet: đây là một tổ chức phi lợi nhuận tập trung vào việc cải thiện khả năng sẵn sàng và ứng phó với an ninh mạng của các tổ chức, doanh nghiệp

Nhiệm vụ của tổ chức này là “xác định, phát triển, xác thực, thúc đẩy và duy trì các giải pháp thực tiễn tốt nhất cho phòng thủ mạng và xây dựng và dẫn dắt cộng đồng để tạo ra một môi trường tin cậy trong không gian mạng”

CIS được biết đến nhiều nhất với CIS Controls, một hướng dẫn toàn diện gồm 20 biện pháp bảo vệ và đối phó để phòng thủ an ninh mạng hiệu quả. CIS Controls cung cấp một danh sách biện pháp ưu tiên mà các tổ chức có thể thực hiện để giảm đáng kể tấn công bề mặt vào mạng của họ. CIS Benchmarks tham chiếu các kiểm soát này khi đưa ra những khuyến nghị để các cấu hình hệ thống được bảo mật tốt hơn.

### **Khái niệm CIS Benchmark**



Hình 1.2: CIS Benchmark là gì?

CIS Benchmarks là khuôn khổ để hiệu chỉnh một loạt các dịch vụ và sản phẩm CNTT nhằm đảm bảo các tiêu chuẩn cao nhất về an ninh mạng

CIS Benchmarks là sự hợp tác của Consensus Community và các thành viên CIS SecureSuite (một nhóm các thành viên CIS có quyền truy cập vào các bộ công cụ và tài nguyên bổ sung). Consensus Community bao gồm các chuyên gia trong lĩnh vực bảo mật CNTT, những người sử dụng kiến thức và kinh nghiệm của họ để giúp đỡ cộng đồng Internet toàn cầu. Các thành viên của CIS SecureSuite được tạo thành từ một số loại hình công ty khác nhau về quy mô, bao gồm các cơ quan chính phủ, trường cao đẳng và đại học, tổ chức phi lợi nhuận, chuyên gia tư vấn và kiểm toán CNTT, nhà cung cấp phần mềm bảo mật và các tổ chức khác.

Hiện tại, có tổng cộng hơn 140 CIS benchmark, trải dài trên 7 hạng mục công nghệ cốt lõi

CIS benchmark cung cấp hướng dẫn cho tất cả các khu vực của mạng CNTT, bao gồm hệ điều hành, hệ thống máy chủ, phần mềm văn phòng và thiết bị mạng.

CIS benchmark đại diện cho các cài đặt cơ bản để đảm bảo hệ thống CNTT hoặc sản phẩm được bảo mật. Mục đích là nâng cao các tiêu chuẩn an ninh mạng quốc tế trong tất cả các loại hình tổ chức. CIS benchmark được các tổ chức, chính phủ và viện nghiên cứu trên toàn thế giới sử dụng.

### **CIS Benchmark được tổ chức như thế nào?**

Mỗi CIS Benchmark gồm có nhiều đề xuất cấu hình dựa trên một trong hai cấp độ cấu hình:

* Cấu hình Benchmark cấp 1 gồm có các cấu hình cơ bản dễ dàng triển khai và ảnh hưởng không đáng kể đến hoạt động của doanh nghiệp.
* Cấu hình Benchmark cấp 2 dùng cho môi trường bảo mật cao và cần nhiều sự điều phối và kế hoạch hơn để ít gây trở ngại trong vận hành doanh nghiệp.

7 loại CIS Benchmark là:

* **Benchmark Hệ điều hành:**
* Gồm cấu hình bảo mật của các hệ điều hành cốt lõi như Microsoft Windows, Linux và Apple OSX
* CIS Benchmarks giúp các tổ chức định cấu hình chúng một cách an toàn, đóng các lỗ hổng bảo mật và giảm rủi ro từ các mối đe dọa mạng.
* Những điểm quy chuẩn này bao gồm các biện pháp thực hành tốt nhất dành cho các tính năng:
* Hạn chế truy cập cục bộ và từ xa
* Biện pháp kiểm soát truy cập hệ điều hành
* Chính sách nhóm, người dùng
* Cài đặt trình duyệt web
* Quản lý bản vá
* Giao thức cài đặt trình điều khiển
* **Benchmark Phần mềm máy chủ:**
* Gồm các cấu hình bảo mật của phần mềm máy chủ được sử dụng rộng rãi, bao gồm Microsoft Windows Server, SQL Server, VMware, Docker, và Kubernetes.
* Mục đích là tăng cường an ninh mạng thông qua các cấu hình thực tiễn tốt nhất trên các khu vực khác nhau của hệ thống máy chủ.
* Các CIS benchmark này gồm:
* các đề xuất để định cấu hình chứng chỉ Kubernetes PKI,
* cài đặt máy chủ API,
* kiểm soát quyền quản trị máy chủ,
* chính sách về Network
* các giới hạn lưu trữ
* **Benchmark Cơ sở hạ tầng và dịch vụ đám mây**
* Xử lý các cấu hình bảo mật cho Amazon Web Services (AWS), Microsoft Azure, Google, IBM và các đám mây công cộng (public cloud) phổ biến khác
* Những Benchmark này gồm:
* các hướng dẫn để định cấu hình quản lý truy cập và nhận dạng (IAM),

giao thức ghi nhật ký hệ thống,

* cấu hình mạng
* các biện pháp tuân thủ quy định an toàn.
* **Benchmark của Thiết bị di động**
* Dùng cho các hệ điều hành di động, bao gồm iOS và Android
* Benchmark này còn tập trung vào các lĩnh vực như:
* các tùy chọn và cài đặt dành cho nhà phát triển,
* cấu hình quyền riêng tư của hệ điều hành,
* cài đặt trình duyệt
* quyền truy cập ứng dụng
* **Benchmark của Thiết bị mạng**
* Các CIS benchmark này giúp cấu hình các thiết bị mạng và phần cứng được sử dụng trong hệ thống CNTT của tổ chức
* CIS benchmark này giúp cấu hình các thiết bị mạng và phần cứng được sử dụng trong hệ thống CNTT của tổ chức
* **Benchmark của Phần mềm máy tính để bàn**
* Gồm các cấu hình bảo mật cho một số ứng dụng phần mềm máy tính để bàn được sử dụng phổ biến nhất, bao gồm Microsoft Office và Exchange Server, Google Chrome, Mozilla Firefox và Trình duyệt Safari
* Các Benchamrk này bao gồm các biện pháp thực hành tốt nhất để quản lý tính năng phần mềm máy tính, như:
* Cài đặt máy chủ và quyền riêng tư email
* Chặn phần mềm máy tính bên thứ ba
* Cài đặt trình duyệt
* Đặc quyền truy cập
* Tài khoản người dùng
* Quản lý thiết bị khách
* **Benchmark của Thiết bị in ấn đa chức năng**
* CIS Benchmark này dành cho các thiết bị mạng ngoại vi như máy in đa chức năng, máy quét và máy photocopy
* Đề ra các phương pháp bảo mật cải tiến nhất để định cấu hình các máy in đa năng trong văn phòng đồng thời còn hoạt động trong những lĩnh vực như cập nhật chương trình cơ sở, cấu hình TCP/IP, cấu hình truy cập không dây, quản lý người dùng và chia sẻ tệp.

### **Các cấp độ của CIS Benchmark**

Để giúp các tổ chức đạt được mục tiêu bảo mật duy nhất của mình, CIS chỉ định cấp độ cấu hình cho từng hướng dẫn CIS Benchmark .

Mỗi cấu hình CIS bao gồm các đề xuất cung cấp một cấp độ bảo mật khác nhau. Các tổ chức có thể chọn cấu hình dựa trên những nhu cầu về bảo mật và tuân thủ của mình

**Level 1**

* Các đề xuất cấu hình dành cho Level 1 là đề xuất bảo mật cơ bản để cấu hình hệ thống CNTT
* Có thể dễ dàng thực hiện theo những đề xuất đó mà không tác động đến chức năng kinh doanh hay thời gian hoạt động.
* Những đề xuất này sẽ làm giảm số lượng điểm truy cập hệ thống CNTT, qua đó giúp bạn giảm rủi ro về an ninh mạng.

**Level 2**

* Các đề xuất cấu hình dành cho Level 2 rất phù hợp với dữ liệu có độ nhạy cảm cao cần ưu tiên bảo mật. Quá trình triển khai những đề xuất này đòi hỏi kiến thức chuyên môn từ chuyên gia và một kế hoạch thấu đáo để đạt được khả năng bảo mật toàn diện mà chỉ bị gián đoạn ở mức tối thiểu.

### **Lợi ích của CIS Benchmark**

CIS benchmark giúp các tổ chức thiết lập hệ thống CNTT và công nghệ để đảm bảo thực hành tốt nhất việc bảo vệ an ninh mạng.

Các hướng dẫn đóng một vai trò quan trọng trong việc hình thành chính sách an ninh mạng của tổ chức. Có các điểm chuẩn cho nhiều loại công nghệ, bao gồm các hệ điều hành và trình duyệt phổ biến.

Bằng cách tuân theo CIS benchmark, các tổ chức có thể bảo mật hệ thống CNTT bằng cách sử dụng một khuôn khổ được phát triển bởi các chuyên gia hàng đầu về an ninh mạng

Nhờ việc áp dụng CIS Benchmark, tổ chức của bạn có thể thu về một số lợi ích an ninh mạng như:

* CIS Benchmark cung cấp cho các tổ chức khung cấu hình bảo mật đã được chuyên gia kiểm định và chứng minh. Do đó, Các công ty, tổ chức có thể tránh được tình huống thử nghiệm và gặp lỗi khiến tính bảo mật bị đe dọa
* Miễn phí tải xuống và nhúng.
* Một công cụ rõ ràng trong việc nâng cao quy trình quản trị CNTT.
* Bảo vệ các hệ thống CNTT quan trọng trong tổ chức, từ hệ điều hành đến mạng.
* Kiến thức chuyên môn được thu thập của cộng đồng toàn cầu gồm các chuyên gia CNTT và an ninh mạng.
* Cập nhật thường xuyên, hướng dẫn từng bước để bảo mật mọi khu vực của cơ sở hạ tầng CNTT.
* Quản lý tuân thủ nhất quán.
* Một mẫu linh hoạt để áp dụng an toàn các dịch vụ đám mây mới và để thực hiện các chiến lược chuyển đổi kỹ thuật số.
* Các cấu hình dễ triển khai để cải thiện hiệu quả hoạt động và tính bền vững.

### **Làm thế nào để triển khai CIS Benchmark?**

Mỗi CIS Benchmark bao gồm một mô tả về đề xuất, lý do cho đề xuất đó và hướng dẫn mà quản trị viên hệ thống có thể thực hiện theo để triển khai đề xuất một cách chính xác. Mỗi điểm quy chuẩn có thể bao gồm vài trăm trang vì nó bao quát từng khía cạnh của hệ thống CNTT đích

Việc triển khai CIS Benchmark và cập nhật tất cả các phiên bản phát hành sẽ trở nên phức tạp nếu bạn thực hiện theo cách thủ công. Đó là lý do mà nhiều tổ chức sử dụng các công cụ tự động để theo dõi khả năng tuân thủ CIS. CIS cũng cung cấp các công cụ miễn phí và có trả phí mà bạn có thể sử dụng để quét hệ thống CNTT cũng như tạo báo cáo tuân thủ CIS. Những công cụ này sẽ cảnh báo quản trị viên hệ thống nếu cấu hình hiện tại không đáp ứng đề xuất CIS Benchmark.

## **CIS CENTOS 7 BENCHMARK**

### **Tổng quan về CentOS 7**

A blue sign with a logo

Description automatically generated

Hình 1.3: CentOS 7 là gì?

##### **CentOS 7 là gì?**

CentOS (**Community Enterprise Operating System** – Hệ điều hành doanh nghiệp Cộng đồng) là một trong những bản phân phối Linux được phát hành bởi Gregory Kurtzer. Nó hoàn toàn tương thích với chức năng thực tế của RHEL (Red Hat Enterprise Linux), cung cấp một hệ điều hành mã nguồn mở và miễn phí ở cấp doanh nghiệp.

Các nhà phát triển CentOS tạo ra sản phẩm bằng mã nguồn RHEL, và các sản phẩm được tạo ra rất giống với RHEL hoặc có thể cao cấp hơn. CentOS chỉ hỗ trợ kỹ thuật thông qua cổng thông tin cộng đồng hoặc web.

Hiện nay, CentOS là một trong những nền tảng phát triển mạnh mẽ nhất. Bản phân phối miễn phí này được phát hành với mục tiêu hướng tới cộng đồng, cung cấp cho cộng đồng mã nguồn mở một nền tảng mạnh mẽ để xây dựng và phát triển sản phẩm. Nhờ vào tính bảo mật cao ở một số bản cập nhật cấp công ty, khả năng tương thích nhị phân với RHEL, cũng như hoạt động một cách mạnh mẽ và ổn định, nó đã trở thành lựa chọn hàng đầu cho người dùng và doanh nghiệp, luôn mang đến những trải nghiệm tuyệt vời khi sử dụng với bất kỳ mục đích nào.

##### **Cấu trúc của CentOS 7**

CentOS cũng tuân theo kiến ​​trúc tương tự như bất kỳ bản phân phối Linux nào khác và chỉ hỗ trợ kiến ​​trúc x86-64. Điều đó có nghĩa là nó hỗ trợ cả máy 32 bit và 64 bit.

* Lớp dưới cùng là phần cứng hoặc thiết bị vật lý. Như máy tính, bộ lưu trữ và thiết bị mạng.
* Phía trên là kernel là thành phần cốt lõi của Hệ điều hành. Và nó tương tác trực tiếp với phần cứng.
* Phía trên kernel là shell đóng vai trò là giao diện giữa người dùng và kernel.
* Trên tất cả các lớp này là lớp ứng dụng tương tác với shell và kernel để thực hiện một số tác vụ do người dùng xác định. Các ứng dụng bao gồm trình duyệt web, phiên bản văn bản, trình duyệt file, trình phát phương tiện,…

##### **Ưu điểm của CentOS 7**

* CentOS nhẹ, đáng tin cậy và nhanh chóng.
* Nó miễn phí và nguồn mở và ở cấp doanh nghiệp.
* Cùng với CentOS, bạn cũng sẽ có được phần mềm máy chủ nguồn mở như Apache Web, CUPS, MySQL, v.v. Và các công cụ kiểm soát phiên bản như git được cài đặt theo mặc định.
* Hỗ trợ cộng đồng tuyệt vời với điều khoản báo cáo trực tiếp các lỗi đến bug.centos.org
* CentOS mới nhất cũng bao gồm công nghệ giám sát và ảo hóa như Docker, oVirt, Xen, v.v.
* Nó chia sẻ gần 95% các tính năng mà Red Hat Enterprise Linux thương mại có. Và điều này có sẵn miễn phí!
* So với các bản phát hành Linux nguồn mở và miễn phí khác, CentOS được ưa thích rộng rãi (thậm chí trên Ubuntu). Vì tính ổn định và các bản cập nhật gói ít thường xuyên hơn.

##### **Các phiên bản của CentOS 7**

CentOS 7 là 1 phiên bản của CentOS

Bắt đầu với phiên bản 7.0, CentOS số phiên bản cũng bao gồm một phần thứ ba chỉ ra dấu thời gian của mã nguồn phát hành dựa trên.

* Ví dụ: số phiên bản 7.0-1406 vẫn ánh xạ bản phát hành CentOS này sang bộ cập nhật zeroth của RHEL 7, trong khi "1406" chỉ ra rằng mã nguồn phát hành này dựa trên ngày từ tháng 6 năm 2014. Sử dụng tháng tháng cho phép hình ảnh cài đặt được phát hành lại để phát hành container và đám mây sắp tới, trong khi vẫn duy trì kết nối với phiên bản phát hành cơ sở có liên quan

|  |  |  |  |
| --- | --- | --- | --- |
| **Phiên bản CentOS** | **Kiến trúc** | **Nhân** | **Ngày phát hành CentOS** |
| 7.0-1406 | x86-64 | 3.10.0-123 | 7 tháng 7, 2014 |
| 7.1-1503 | x86-64 | 3.10.0-229 | 31 tháng 3, 2015 |
| 7.2-1511 | x86-64 | 3.10.0-327 | 14 tháng 12, 2015 |
| 7.3-1611 | x86-64 | 3.10.0-514 | 12 tháng 12, 2016 |
| 7.4-1708 | x86-64 | 3.10.0-693 | 13 tháng 9, 2017 |
| 7.5-1804 | x86-64 | 3.10.0-862 | 10 tháng 5, 2018 |
| 7.6-1810 | x86-64 | 3.10.0-957 | 3 tháng 12, 2018 |
| 7.7-1908 | x86-64 | 3.10.0-1062 |  |

Table 1.1: Các phiên ban của CentOS 7

Tính năng chủ yếu của CentOS 7:

* Git: Git phiên bản 1.8
* Hộp chứa: CentOS cung cấp sẵn Docker
* Kernel: Dự vào thượng nguồn kernel 3.10 và Fedora 19
* Quản lý lưu trữ: Trình quản lý khối lượng logic mặc định
* Bảo mật: CentOS hỗ trợ cho TLS 1.0 và OpenSSL 1.0.1
* NTP: Chronyd và NTP daemon đều khả dụng
* Quản lý phần mềm: Sử dụng YUM v3, được phân phối với RPM 4.11
* Java: OpenJDK 8
* Networking: Sử dụng iptables
* Hỗ trợ ngôn ngữ Python: Giới hạn hỗ trợ Python 2.7. CentOS 7 cũng hỗ trợ Python 2.7
* Ảo hóa: Sử dụng quản lý ảo và qemu-kvm
* httpd/Apache: HTTP Server 2.4
* Firewall: CentOS 7 sử dụng iptables làm framework lọc các gói tin
* ruby, php,perl; Ruby 2.0.0, PHP 5.4.16, Perl 5.16.3
* Cơ sở dữ liệu: MySQL 5.5, PostgreSQL 9.2, MariaDB 5.5
* Desktop Environment: Trong CentOS 7, máy chủ X.Org là trình quản lý hiển thị GNOME mặc định

### **Tổng quan về CIS CentOS 7 Benchmark**

Bộ tiêu chuẩn của CIS cho Centos 7 được gọi là CIS CentOS Linux 7 Benchmark

Phiên bản mới nhất của CIS CentOS 7 Benchmark hiện nay là v3.1.2 - 08-31-2021

Hiện tại, CIS Benchmark có sẵn miễn phí ở định dạng PDF cho mục đích sử dụng phi thương mại.

Tài liệu này cung cấp hướng dẫn quy định để thiết lập cấu hình an toàn cho các hệ thống CentOS Linux 7 chạy trên nền tảng x86 và x64.

Hướng dẫn bên trong giả định rộng rãi rằng các hoạt động đang được thực hiện với tư cách là người dùng gốc. Các hoạt động được thực hiện bằng sudo thay vì người dùng root có thể tạo ra kết quả không mong muốn, hoặc không thực hiện được những thay đổi dự kiến ​​đối với hệ thống. Người dùng không root có thể không thể truy cập vào một số khu vực nhất định của hệ thống, đặc biệt là sau khi việc khắc phục đã được thực hiện. Nó là nên xác minh tính toàn vẹn của đường dẫn người dùng root và tính toàn vẹn của bất kỳ chương trình nào đang chạy trước khi thực thi các lệnh và tập lệnh có trong tiêu chuẩn này

Đối tượng dự định: CIS Benchmark này dành cho quản trị viên hệ thống và ứng dụng, chuyên gia bảo mật, kiểm toán viên, bộ phận trợ giúp và nhân viên triển khai nền tảng có kế hoạch phát triển, triển khai, đánh giá hoặc bảo mật các giải pháp tích hợp centOS Linux 7.x trên nền tảng x86 hoặc x64

Tình trạng đánh giá:

* **Automated**: Trình bày các khuyến nghị để việc đánh giá kiểm soát kỹ thuật có thể được thực hiện đầy đủ tự động và xác thực ở trạng thái đạt/không đạt. Các khuyến nghị sẽ bao gồm những điều cần thiết thông tin để thực hiện tự động hóa.
* **Manual**: Thể hiện các khuyến nghị mà việc đánh giá kiểm soát kỹ thuật không thể được đầy đủ tự động và yêu cầu tất cả hoặc một số bước thủ công để xác thực rằng trạng thái đã định cấu hình đã được đặt như mong đợi. Trạng thái dự kiến ​​có thể thay đổi tùy thuộc vào môi trường.

##### **Các tiêu chuẩn trong CIS CentOS 7 Benchmark**

**1 Initial Setup**

**1.1 Filesystem Configuration**

**1.1.1 Disable unused filesystems**

**1.1.1.1 Ensure mounting of cramfs filesystems is disabled (Automated)**

* Đây là tiêu chuẩn “Đảm bảo việc gắn hệ thống tệp cramfs bị tắt”
* Loại hệ thống tệp cramfs là một hệ thống tệp Linux chỉ đọc được nén được nhúng trong hệ thống dấu chân. Một hình ảnh cramfs có thể được sử dụng mà không cần phải giải nén trước hình ảnh
* Loại bỏ hỗ trợ cho các loại hệ thống tập tin không cần thiết làm giảm bề mặt tấn công cục bộ của máy chủ. Nếu loại hệ thống tập tin này không cần thiết, hãy tắt nó

**1.1.1.2 Ensure mounting of squashfs filesystems is disabled (Automated)**

* Đảm bảo việc gắn các hệ thống tập tin squashfs bị vô hiệu hóa
* Loại hệ thống tệp squashfs là một hệ thống tệp Linux chỉ đọc được nén được nhúng trong hệ thống dấu chân nhỏ (tương tự như cramfs ). Một hình ảnh squashfs có thể được sử dụng mà không cần để giải nén hình ảnh đầu tiên
* Loại bỏ hỗ trợ cho các loại hệ thống tập tin không cần thiết làm giảm bề mặt tấn công cục bộ của hệ thống. Nếu loại hệ thống tập tin này không cần thiết, hãy tắt nó

**1.1.1.3 Ensure mounting of udf filesystems is disabled (Automated)**

* Đảm bảo việc gắn các hệ thống tập tin udf bị tắt
* Loại hệ thống tệp udf là định dạng đĩa chung được sử dụng để triển khai ISO/IEC 13346 và Thông số kỹ thuật ECMA-167. Đây là loại hệ thống tệp của nhà cung cấp mở để lưu trữ dữ liệu trên phạm vi rộng của các phương tiện truyền thông. Loại hệ thống tập tin này là cần thiết để hỗ trợ ghi DVD và mới hơn định dạng đĩa quang.
* Loại bỏ hỗ trợ cho các loại hệ thống tập tin không cần thiết làm giảm bề mặt tấn công cục bộ của hệ thống. Nếu loại hệ thống tập tin này không cần thiết, hãy tắt nó.

**1.1.2 Ensure /tmp is configured (Automated)**

* Thư mục /tmp là thư mục có thể ghi trên thế giới được sử dụng để lưu trữ tạm thời bởi tất cả người dùng và một số ứng dụng
* Tạo /tmp hệ thống tệp riêng của nó cho phép quản trị viên đặt tùy chọn noexec trên mount, khiến /tmp trở nên vô dụng đối với kẻ tấn công cài đặt mã thực thi. Nó cũng sẽ ngăn kẻ tấn công thiết lập liên kết cứng đến chương trình thiết lập hệ thống và đợi nó để được cập nhật. Khi chương trình được cập nhật, liên kết cứng sẽ bị hỏng và kẻ tấn công sẽ có bản sao chương trình của riêng mình. Nếu chương trình tình cờ có một lỗ hổng bảo mật, kẻ tấn công có thể tiếp tục khai thác lỗ hổng đã biết. Điều này có thể được thực hiện bằng cách gắn tmpfs vào /tmp hoặc tạo một tệp riêng phân vùng cho /tmp.

**1.1.3 Ensure noexec option set on /tmp partition (Automated)**

* Đảm bảo tùy chọn noexec được đặt trên phân vùng /tmp
* Tùy chọn gắn kết noexec chỉ định rằng hệ thống tệp không thể chứa các tệp nhị phân thực thi.
* Vì hệ thống tệp /tmp chỉ dành cho lưu trữ tệp tạm thời, hãy đặt tùy chọn này thành đảm bảo rằng người dùng không thể chạy các tệp nhị phân thực thi từ/tmp.

**1.1.4 Ensure nodev option set on /tmp partition (Automated)**

* Đảm bảo tùy chọn nút được đặt trên phân vùng /tmp
* Tùy chọn gắn kết nút xác định rằng hệ thống tệp không thể chứa các thiết bị đặc biệt.
* Vì hệ thống tệp /tmp không nhằm hỗ trợ các thiết bị, hãy đặt tùy chọn này để đảm bảo rằng người dùng không thể cố gắng tạo khối hoặc ký tự thiết bị đặc biệt trong /tmp

**1.1.5 Ensure nosuid option set on /tmp partition (Automated)**

* Đảm bảo tùy chọn nosuid được đặt trên phân vùng /tmp
* Tùy chọn gắn kết nosuid chỉ định rằng hệ thống tệp không thể chứa các tệp setuid.
* Vì hệ thống tệp /tmp chỉ dành cho lưu trữ tệp tạm thời, hãy đặt tùy chọn này thành đảm bảo rằng người dùng không thể tạo tệp setuid trong /tmp.

**1.1.6 Ensure /dev/shm is configured (Automated)**

* Đảm bảo /dev/shm được cấu hình
* /dev/shm là một khái niệm bộ nhớ dùng chung truyền thống. Một chương trình sẽ tạo ra một bộ nhớ phần mà các quy trình khác (nếu được phép) có thể truy cập. Gắn kết tmpfs tại/dev/shm là xử lý tự động bởi systemd.
* Bất kỳ người dùng nào cũng có thể tải lên và thực thi các tệp bên trong /dev/shm tương tự như phân vùng /tmp. Định cấu hình/dev/shm cho phép quản trị viên đặt tùy chọn noexec trên giá treo, khiến /dev/shm trở nên vô dụng đối với kẻ tấn công cài đặt mã thực thi. Nó cũng sẽ ngăn chặn một kẻ tấn công thiết lập một liên kết cứng đến một chương trình thiết lập hệ thống và đợi nó được cập nhật. Khi chương trình được cập nhật, liên kết cứng sẽ bị hỏng và kẻ tấn công sẽ có bản sao chương trình của riêng mình. Nếu chương trình xảy ra để có một bảo mật lỗ hổng, kẻ tấn công có thể tiếp tục khai thác lỗ hổng đã biết

**1.1.7 Ensure noexec option set on /dev/shm partition (Automated)**

* Đảm bảo tùy chọn noexec được đặt trên phân vùng/dev/shm
* Tùy chọn gắn kết noexec chỉ định rằng hệ thống tệp không thể chứa các tệp nhị phân thực thi.
* Đặt tùy chọn này trên hệ thống tệp sẽ ngăn người dùng thực thi các chương trình được chia sẻ ký ức. Điều này ngăn người dùng giới thiệu phần mềm độc hại tiềm ẩn trên hệ thống

**1.1.8 Ensure nodev option set on /dev/shm partition (Automated)**

* Đảm bảo tùy chọn nút được đặt trên phân vùng/dev/shm
* Tùy chọn gắn kết nút xác định rằng hệ thống tệp không thể chứa các thiết bị đặc biệt.
* Vì hệ thống tệp /dev/shm không nhằm mục đích hỗ trợ các thiết bị, hãy đặt tùy chọn này để đảm bảo người dùng không thể cố gắng tạo các thiết bị đặc biệt trong phân vùng /dev/shm

**1.1.9 Ensure nosuid option set on /dev/shm partition (Automated)**

* Đảm bảo tùy chọn nosuid được đặt trên phân vùng /dev/shm
* Tùy chọn gắn kết nosuid chỉ định rằng hệ thống tệp không thể chứa các tệp setuid.
* Đặt tùy chọn này trên hệ thống tệp sẽ ngăn người dùng giới thiệu các chương trình đặc quyền lên hệ thống và cho phép người dùng không phải root thực thi chúng.

**1.1.10 Ensure separate partition exists for /var (Automated)**

* Đảm bảo phân vùng riêng tồn tại cho /var
* Thư mục /var được daemon và các dịch vụ hệ thống khác sử dụng để lưu trữ tạm thời dữ liệu động. Một số thư mục được tạo bởi các quy trình này có thể ghi được trên thế giới.
* Vì thư mục /var có thể chứa các tệp và thư mục có thể ghi trên thế giới, nên có nguy cơ cạn kiệt tài nguyên nếu nó không bị ràng buộc vào một phân vùng riêng.

**1.1.11 Ensure separate partition exists for /var/tmp (Automated)**

* Đảm bảo phân vùng riêng tồn tại cho /var/tmp
* Thư mục /var/tmp là một thư mục có thể ghi trên thế giới được sử dụng để lưu trữ tạm thời bởi tất cả người dùng và một số ứng dụng và dành cho các tệp tạm thời được lưu giữ trên khởi động lại.
* Vì thư mục /var/tmp được thiết kế để có thể ghi trên thế giới, nên có nguy cơ về tài nguyên hết nếu nó không bị ràng buộc vào một phân vùng riêng biệt. Ngoài ra, biến /var/tmp thành của riêng nó hệ thống tệp cho phép quản trị viên đặt tùy chọn noexec khi gắn kết, giúp /var/tmp vô dụng đối với kẻ tấn công cài đặt mã thực thi. Nó cũng sẽ ngăn chặn một kẻ tấn công thiết lập một liên kết cứng đến một chương trình thiết lập hệ thống và đợi nó được cập nhật. Khi chương trình được cập nhật, liên kết cứng sẽ bị hỏng và kẻ tấn công sẽ có bản sao chương trình của riêng mình. Nếu chương trình xảy ra để có một bảo mật lỗ hổng, kẻ tấn công có thể tiếp tục khai thác lỗ hổng đã biết.

**1.1.12 Ensure /var/tmp partition includes the noexec option (Automated)**

* Đảm bảo phân vùng /var/tmp bao gồm tùy chọn noexec
* Tùy chọn gắn kết noexec chỉ định rằng hệ thống tệp không thể chứa các tệp nhị phân thực thi.
* Vì hệ thống tệp /var/tmp chỉ dành cho lưu trữ tệp tạm thời, hãy đặt tùy chọn này thành đảm bảo rằng người dùng không thể chạy các tệp nhị phân thực thi từ/var/tmp

**1.1.13 Ensure /var/tmp partition includes the nodev option (Automated)**

* Đảm bảo phân vùng /var/tmp bao gồm tùy chọn gật đầu
* Tùy chọn gắn kết nút xác định rằng hệ thống tệp không thể chứa các thiết bị đặc biệt.
* Vì hệ thống tệp /var/tmp không nhằm hỗ trợ các thiết bị, hãy đặt tùy chọn này để đảm bảo người dùng không thể cố gắng tạo khối hoặc ký tự thiết bị đặc biệt trong /var/tmp

**1.1.14 Ensure /var/tmp partition includes the nosuid option (Automated)**

* Đảm bảo phân vùng /var/tmp bao gồm tùy chọn nosuid
* Tùy chọn gắn kết nosuid chỉ định rằng hệ thống tệp không thể chứa các tệp setuid.
* Vì hệ thống tệp /var/tmp chỉ dành cho lưu trữ tệp tạm thời, hãy đặt tùy chọn này thành đảm bảo rằng người dùng không thể tạo tệp setuid trong /var/tmp

**1.1.15 Ensure separate partition exists for /var/log (Automated)**

* Đảm bảo phân vùng riêng tồn tại cho /var/log
* Thư mục /var/log được các dịch vụ hệ thống sử dụng để lưu trữ dữ liệu nhật ký.
* Có hai lý do quan trọng để đảm bảo rằng nhật ký hệ thống được lưu trữ trên một phân vùng: bảo vệ chống cạn kiệt tài nguyên (vì nhật ký có thể phát triển khá lớn) và bảo vệ dữ liệu kiểm toán

**1.1.16 Ensure separate partition exists for /var/log/audit (Automated)**

* Đảm bảo phân vùng riêng tồn tại cho /var/log/audit (Tự động)
* Trình nền kiểm tra, auditd, lưu trữ dữ liệu nhật ký trong thư mục /var/log/audit.
* Có hai lý do quan trọng để đảm bảo rằng dữ liệu do auditd thu thập được lưu trữ trên một phân vùng riêng biệt: bảo vệ chống cạn kiệt tài nguyên (vì tệp audit.log có thể phát triển khá lớn) và bảo vệ dữ liệu kiểm toán. Daemon kiểm toán tính toán bao nhiêu miễn phí không gian còn lại và thực hiện các hành động dựa trên kết quả. Nếu các quy trình khác (chẳng hạn như syslog ) tiêu tốn dung lượng trong cùng phân vùng với auditd , nó có thể không hoạt động như mong muốn

**1.1.17 Ensure separate partition exists for /home (Automated)**

* Đảm bảo phân vùng riêng tồn tại cho /home
* Thư mục /home được sử dụng để hỗ trợ nhu cầu lưu trữ đĩa của người dùng cục bộ.
* Nếu hệ thống nhằm hỗ trợ người dùng cục bộ, hãy tạo một phân vùng riêng cho /home thư mục để bảo vệ khỏi cạn kiệt tài nguyên và hạn chế loại tệp có thể được lưu trữ dưới /home

**1.1.18 Ensure /home partition includes the nodev option (Automated)**

* Đảm bảo phân vùng /home bao gồm tùy chọn gật đầu
* Tùy chọn gắn kết nút xác định rằng hệ thống tệp không thể chứa các thiết bị đặc biệt.
* Vì phân vùng người dùng không nhằm mục đích hỗ trợ thiết bị, hãy đặt tùy chọn này để đảm bảo rằng người dùng không thể cố gắng tạo các thiết bị đặc biệt khối hoặc ký tự.

**1.1.19 Ensure removable media partitions include noexec option (Automated)**

* Đảm bảo phân vùng phương tiện di động bao gồm tùy chọn noexec
* Tùy chọn gắn kết noexec chỉ định rằng hệ thống tệp không thể chứa các tệp nhị phân thực thi.
* Đặt tùy chọn này trên hệ thống tệp sẽ ngăn người dùng thực thi các chương trình từ phương tiện di động. Điều này ngăn cản người dùng có thể giới thiệu độc hại tiềm ẩn phần mềm trên hệ thống

**1.1.20 Ensure nodev option set on removable media partitions (Automated)**

* Đảm bảo tùy chọn nút được đặt trên các phân vùng phương tiện di động
* Tùy chọn gắn kết nút xác định rằng hệ thống tệp không thể chứa các thiết bị đặc biệt.
* Có thể sử dụng phương tiện di động có chứa ký tự và khối thiết bị đặc biệt để phá vỡ các biện pháp kiểm soát bảo mật bằng cách cho phép người dùng không root truy cập các tệp thiết bị nhạy cảm chẳng hạn như /dev/kmem hoặc phân vùng đĩa thô.

**1.1.21 Ensure nosuid option set on removable media partitions (Automated)**

* Đảm bảo tùy chọn nosuid được đặt trên các phân vùng phương tiện di động
* Tùy chọn gắn kết nosuid chỉ định rằng hệ thống tệp không thể chứa các tệp setuid.
* Đặt tùy chọn này trên hệ thống tệp sẽ ngăn người dùng giới thiệu các chương trình đặc quyền vào hệ thống và cho phép người dùng không root thực thi chúng

**1.1.22 Ensure sticky bit is set on all world-writable directories (Automated)**

* Đảm bảo bit dính được đặt trên tất cả các thư mục có thể ghi trên thế giới
* Đặt bit dính trên các thư mục có thể ghi trên thế giới sẽ ngăn người dùng xóa hoặc đổi tên các tệp trong thư mục không thuộc sở hữu của chúng.
* Tính năng này ngăn khả năng xóa hoặc đổi tên tệp trong các thư mục có thể ghi trên thế giới (chẳng hạn như /tmp ) thuộc sở hữu của người dùng khác

**1.1.23 Disable Automounting (Automated)**

* Vô hiệu hóa tự động
* autofs cho phép tự động gắn thiết bị, thường bao gồm ổ đĩa CD/DVD và USB.
* Khi bật tính năng tự động đếm, bất kỳ ai có quyền truy cập vật lý đều có thể đính kèm ổ USB hoặc đĩa và có sẵn nội dung của nó trong hệ thống ngay cả khi họ không có quyền gắn kết nó chúng tôi

**1.1.24 Disable USB Storage (Automated)**

* Vô hiệu hóa bộ lưu trữ USB
* Bộ lưu trữ USB cung cấp phương tiện để chuyển và lưu trữ các tệp đảm bảo tính bền bỉ và tính khả dụng của các tệp độc lập với trạng thái kết nối mạng. Sự phổ biến và tiện ích của nó đã khiến phần mềm độc hại dựa trên USB trở thành một phương tiện đơn giản và phổ biến để xâm nhập mạng và bước đầu tiên để thiết lập một mối đe dọa dai dẳng trong môi trường nối mạng.
* Hạn chế quyền truy cập USB trên hệ thống sẽ làm giảm bề mặt tấn công vật lý cho thiết bị và làm giảm các vectơ có thể để giới thiệu phần mềm độc hại

**1.2 Configure Software Updates**

**1.2.1 Ensure GPG keys are configured (Manual)**

* Đảm bảo các khóa GPG được định cấu hình
* Hầu hết các trình quản lý gói triển khai ký khóa GPG để xác minh tính toàn vẹn của gói trong quá trình cài đặt.
* Điều quan trọng là đảm bảo rằng các bản cập nhật được lấy từ một nguồn hợp lệ để bảo vệ chống lại giả mạo có thể dẫn đến việc vô tình cài đặt phần mềm độc hại trên hệ thống

**1.2.2 Ensure package manager repositories are configured (Manual)**

* Đảm bảo kho lưu trữ trình quản lý gói được định cấu hình
* Các hệ thống cần phải cấu hình kho lưu trữ trình quản lý gói để đảm bảo chúng nhận được các bản vá và cập nhật mới nhất.
* Nếu kho lưu trữ gói của hệ thống bị định cấu hình sai, các bản vá lỗi quan trọng có thể không được được xác định hoặc một kho lưu trữ giả mạo có thể giới thiệu phần mềm bị xâm nhập

**1.2.3 Ensure gpgcheck is globally activated (Automated)**

* Đảm bảo gpgcheck được kích hoạt trên toàn cầu
* Tùy chọn gpgcheck, được tìm thấy trong phần chính của /etc/yum.conf và riêng lẻ Các tệp /etc/yum/repos.d/\*.repo xác định xem chữ ký của gói RPM có được kiểm tra trước hay không để cài đặt của nó.
* Điều quan trọng là phải đảm bảo rằng chữ ký gói của RPM luôn được kiểm tra trước khi cài đặt để đảm bảo rằng phần mềm được lấy từ một nguồn đáng tin cậy

**1.3 Filesystem Integrity Checking**

**1.3.1 Ensure AIDE is installed (Automated)**

* Đảm bảo AIDE đã được cài đặt
* AIDE chụp nhanh trạng thái hệ thống tệp bao gồm thời gian sửa đổi, quyền và băm tệp mà sau đó có thể được sử dụng để so sánh với trạng thái hiện tại của hệ thống tệp với phát hiện các sửa đổi đối với hệ thống.
* Bằng cách theo dõi trạng thái hệ thống tệp, các tệp bị xâm phạm có thể được phát hiện để ngăn chặn hoặc hạn chế sự phơi bày của các cấu hình sai ngẫu nhiên hoặc độc hại hoặc các tệp nhị phân đã sửa đổi

**1.3.2 Ensure filesystem integrity is regularly checked (Automated)**

* Đảm bảo tính toàn vẹn của hệ thống tập tin được kiểm tra thường xuyên
* Cần kiểm tra định kỳ tính toàn vẹn của hệ thống tệp để phát hiện các thay đổi đối với hệ thống tệp.
* Kiểm tra tệp định kỳ cho phép quản trị viên hệ thống xác định một cách thường xuyên nếu các tệp quan trọng đã bị thay đổi theo cách trái phép

**1.4 Secure Boot Settings**

**1.4.1 Ensure bootloader password is set (Automated)**

* Đảm bảo mật khẩu bộ nạp khởi động được đặt
* Đặt mật khẩu bộ tải khởi động sẽ yêu cầu bất kỳ ai khởi động lại hệ thống phải nhập mật khẩu trước khi có thể đặt tham số khởi động dòng lệnh
* Yêu cầu mật khẩu khởi động khi thực thi bộ tải khởi động sẽ ngăn chặn truy cập trái phép người dùng nhập tham số khởi động hoặc thay đổi phân vùng khởi động. Điều này ngăn cản người dùng khỏi làm suy yếu bảo mật (ví dụ: tắt SELinux khi khởi động)

**1.4.2 Ensure permissions on bootloader config are configured (Automated)**

* Đảm bảo các quyền trên cấu hình bộ nạp khởi động được định cấu hình
* Tệp cấu hình grub chứa thông tin về cài đặt khởi động và mật khẩu cho mở khóa các tùy chọn khởi động. Cấu hình grub2 thường là grub.cfg. Trên grub2 mới hơn hệ thống, mật khẩu bộ nạp khởi động được mã hóa được chứa trong user.cfg. Nếu hệ thống sử dụng UEFI, /boot/efi là hệ thống tệp vfat. Bản thân hệ thống tập tin vfat không có khái niệm về quyền nhưng có thể được gắn trong Linux bằng bất cứ thứ gì quyền mong muốn.
* Đặt quyền đọc và ghi cho root chỉ ngăn người dùng không phải root nhìn thấy các tham số khởi động hoặc thay đổi chúng. Người dùng không root đã đọc khởi động tham số có thể xác định điểm yếu trong bảo mật khi khởi động và có thể khai thác họ

**1.4.3 Ensure authentication required for single user mode (Automated)**

* Đảm bảo yêu cầu xác thực cho chế độ một người dùng
* Chế độ một người dùng (chế độ cứu hộ) được sử dụng để khôi phục khi hệ thống phát hiện sự cố trong khi khởi động hoặc bằng cách chọn thủ công từ bộ nạp khởi động.
* Yêu cầu xác thực ở chế độ một người dùng (chế độ cứu hộ) ngăn người dùng trái phép từ việc khởi động lại hệ thống thành một người dùng để có được quyền root mà không cần thông tin xác thực

**1.5 Additional Process Hardening**

**1.5.1 Ensure core dumps are restricted (Automated)**

* Đảm bảo các bãi chứa lõi bị hạn chế
* Kết xuất lõi là bộ nhớ của một chương trình thực thi. Nó thường được sử dụng để xác định tại sao một chương trình bị hủy bỏ. Nó cũng có thể được sử dụng để thu thập thông tin bí mật từ một lõi tài liệu. Hệ thống cung cấp khả năng đặt giới hạn mềm cho các kết xuất lõi, nhưng điều này có thể bị ghi đè bởi người dùng.
* Đặt giới hạn cứng cho các kết xuất lõi ngăn người dùng ghi đè biến mềm. nếu lõi kết xuất là bắt buộc, hãy xem xét đặt giới hạn cho nhóm người dùng (xem giới hạn.conf(5) ). Ngoài ra, đặt biến fs.suid\_dumpable thành 0 sẽ ngăn các chương trình setuid đổ lõi.

**1.5.2 Ensure XD/NX support is enabled (Automated)**

* Đảm bảo hỗ trợ XD/NX được bật
* Các bộ xử lý gần đây trong dòng x86 hỗ trợ khả năng ngăn chặn việc thực thi mã trên mỗi cơ sở trang bộ nhớ. Nói chung và trên bộ xử lý AMD, khả năng này được gọi là Không thực thi (NX), trong khi trên bộ xử lý Intel, nó được gọi là Execute Disable (XD). Khả năng này có thể giúp ngăn chặn khai thác các lỗ hổng tràn bộ đệm và nên được kích hoạt bất cứ khi nào khả thi. Các bước bổ sung phải được thực hiện để đảm bảo rằng tính năng bảo vệ này được kích hoạt, đặc biệt là trên hệ thống 32-bit x86. Các bộ xử lý khác, chẳng hạn như Itanium và POWER, đã bao gồm hỗ trợ kể từ khi thành lập và hạt nhân tiêu chuẩn cho các nền tảng đó hỗ trợ tính năng này.
* Kích hoạt bất kỳ tính năng nào có thể bảo vệ chống lại các cuộc tấn công tràn bộ đệm giúp tăng cường bảo mật của hệ thống.

**1.5.3 Ensure address space layout randomization (ASLR) is enabled (Automated)**

* Đảm bảo bật ngẫu nhiên bố cục không gian địa chỉ (ASLR)
* Ngẫu nhiên bố trí không gian địa chỉ (ASLR) là một kỹ thuật giảm thiểu khai thác mà sắp xếp ngẫu nhiên không gian địa chỉ của các vùng dữ liệu chính của một quy trình.
* Đặt ngẫu nhiên các vùng bộ nhớ ảo sẽ gây khó khăn cho việc ghi trang bộ nhớ khai thác vì vị trí bộ nhớ sẽ liên tục thay đổi

**1.5.4 Ensure prelink is not installed (Automated)**

* Đảm bảo prelink chưa được cài đặt
* prelink là một chương trình sửa đổi các thư viện chia sẻ ELF và ELF được liên kết động nhị phân theo cách mà thời gian cần thiết để trình liên kết động thực hiện di chuyển khi khởi động giảm đáng kể.
* Tính năng liên kết trước có thể ảnh hưởng đến hoạt động của AIDE vì nó thay đổi nhị phân. Liên kết trước cũng có thể làm tăng tính dễ bị tổn thương của hệ thống nếu người dùng độc hại có thể thỏa hiệp một thư viện chung như libc

**1.6 Mandatory Access Control**

**1.6.1 Configure SELinux**

**1.6.1.1 Ensure SELinux is installed (Automated)**

* Đảm bảo SELinux đã được cài đặt
* SELinux cung cấp Kiểm soát truy cập bắt buộc.
* Không có hệ thống Kiểm soát truy cập bắt buộc chỉ được cài đặt Truy cập tùy ý mặc định Hệ thống điều khiển sẽ có sẵn.

**1.6.1.2 Ensure SELinux is not disabled in bootloader configuration (Automated)**

* Đảm bảo SELinux không bị tắt trong cấu hình bộ nạp khởi động
* Định cấu hình SELINUX để được bật khi khởi động và xác minh rằng nó không bị ghi đè bởi các tham số khởi động grub.
* SELinux phải được bật khi khởi động trong cấu hình grub của bạn để đảm bảo rằng điều khiển mà nó cung cấp không bị ghi đè

**1.6.1.3 Ensure SELinux policy is configured (Automated)**

* Đảm bảo chính sách SELinux được cấu hình
* Định cấu hình SELinux để đáp ứng hoặc vượt quá chính sách được nhắm mục tiêu mặc định, chính sách này hạn chế daemon và chỉ phần mềm hệ thống.
* Yêu cầu cấu hình bảo mật khác nhau từ trang này sang trang khác. Một số trang web có thể bắt buộc một chính sách chặt chẽ hơn chính sách mặc định, điều này hoàn toàn có thể chấp nhận được. mục này là nhằm đảm bảo rằng ít nhất các khuyến nghị mặc định được đáp ứng

**1.6.1.4 Ensure the SELinux mode is enforcing or permissive (Automated)**

* Đảm bảo chế độ SELinux được thực thi hoặc cho phép
* SELinux có thể chạy ở một trong ba chế độ: vô hiệu hóa, cho phép hoặc thực thi:
* Thực thi - Là chế độ hoạt động mặc định và được khuyến nghị; trong chế độ thực thi SELinux hoạt động bình thường, thực thi chính sách bảo mật đã tải trên toàn bộ hệ thống.
* Cho phép - Hệ thống hoạt động như thể SELinux đang thực thi chính sách bảo mật đã tải, bao gồm các đối tượng gắn nhãn và phát ra các mục từ chối truy cập trong nhật ký, nhưng nó không không thực sự từ chối bất kỳ hoạt động. Mặc dù không được khuyến nghị cho các hệ thống sản xuất, chế độ cho phép có thể hữu ích cho việc phát triển chính sách SELinux.
* Bị vô hiệu hóa - Không được khuyến khích mạnh mẽ; hệ thống không chỉ tránh thực thi các chính sách SELinux, nó cũng tránh gắn nhãn bất kỳ đối tượng liên tục nào chẳng hạn như tệp, làm cho nó khó kích hoạt SELinux trong tương lai
* Không khuyến khích chạy SELinux ở chế độ bị vô hiệu hóa; hệ thống không chỉ tránh thực thi chính sách SELinux, nó cũng tránh gắn nhãn bất kỳ đối tượng liên tục nào như tệp, gây khó khăn cho việc kích hoạt SELinux trong tương lai

**1.6.1.5 Ensure the SELinux mode is enforcing (Automated)**

* Đảm bảo chế độ SELinux đang thực thi
* SELinux có thể chạy ở một trong ba chế độ: vô hiệu hóa, cho phép hoặc thực thi:
* Thực thi - Là chế độ hoạt động mặc định và được khuyến nghị; trong chế độ thực thi SELinux hoạt động bình thường, thực thi chính sách bảo mật đã tải trên toàn bộ hệ thống.
* Cho phép - Hệ thống hoạt động như thể SELinux đang thực thi chính sách bảo mật đã tải, bao gồm các đối tượng gắn nhãn và phát ra các mục từ chối truy cập trong nhật ký, nhưng nó không thực sự từ chối bất kỳ hoạt động. Mặc dù không được khuyến nghị cho các hệ thống sản xuất, chế độ cho phép có thể hữu ích cho việc phát triển chính sách SELinux.
* Bị vô hiệu hóa - Không được khuyến khích mạnh mẽ; hệ thống không chỉ tránh thực thi các chính sách SELinux, nó cũng tránh gắn nhãn bất kỳ đối tượng liên tục nào chẳng hạn như tệp, làm cho nó khó kích hoạt SELinux trong tương lai
* Chạy SELinux ở chế độ bị vô hiệu hóa, hệ thống không chỉ tránh thực thi chính sách SELinux, nó cũng tránh gắn nhãn bất kỳ đối tượng cố định nào chẳng hạn như tệp, gây khó khăn cho việc kích hoạt SELinux trong tương lai. Chạy SELinux ở chế độ Cho phép, mặc dù hữu ích cho việc phát triển chính sách SELinux, nhưng chỉ nhật ký truy cập các mục từ chối, nhưng không từ chối bất kỳ hoạt động nào

**1.6.1.6 Ensure no unconfined services exist (Automated)**

* Đảm bảo không tồn tại các dịch vụ không giới hạn
* Các quy trình không bị giới hạn chạy trong các miền không được giới hạn
* Đối với các quy trình không được giới hạn, các quy tắc chính sách SELinux được áp dụng, nhưng tồn tại các quy tắc chính sách cho phép các quy trình chạy trong các miền không bị giới hạn gần như tất cả quyền truy cập. Các tiến trình đang chạy trong các miền không bị giới hạn sẽ quay trở lại sử dụng riêng các quy tắc DAC. Nếu một quá trình không giới hạn là bị xâm phạm, SELinux không ngăn kẻ tấn công giành quyền truy cập vào hệ thống tài nguyên và dữ liệu, nhưng tất nhiên, các quy tắc DAC vẫn được sử dụng. SELinux là một bảo mật cải tiến dựa trên các quy tắc của DAC – nó không thay thế chúng

**1.6.1.7 Ensure SETroubleshoot is not installed (Automated)**

* Đảm bảo SETroubleshoot chưa được cài đặt
* Dịch vụ SETroubleshoot thông báo cho người dùng máy tính để bàn về việc từ chối SELinux thông qua giao diện thân thiện với người dùng. Dịch vụ này cung cấp thông tin quan trọng xung quanh các lỗi cấu hình, xâm nhập trái phép và các lỗi tiềm ẩn khác.
* Dịch vụ SETroubleshoot là một trình nền không cần thiết để chạy trên máy chủ, đặc biệt là nếu X Windows bị vô hiệu hóa

**1.6.1.8 Ensure the MCS Translation Service (mcstrans) is not installed (Automated)**

* Đảm bảo Dịch vụ dịch thuật MCS (mcstrans) chưa được cài đặt
* Trình nền mcstransd cung cấp thông tin nhãn danh mục cho các tiến trình máy khách yêu cầu thông tin. Bản dịch nhãn được xác định trong /etc/selinux/targeted/setran.conf
* Vì dịch vụ này không được sử dụng thường xuyên, hãy loại bỏ nó để giảm số lượng khả năng mã dễ bị tổn thương chạy trên hệ thống.

**1.7 Command Line Warning Banners**

**1.7.1 Ensure message of the day is configured properly (Automated)**

* Đảm bảo tin nhắn trong ngày được cấu hình đúng cách
* Nội dung của tệp /etc/motd được hiển thị cho người dùng sau khi đăng nhập và hoạt động như một tin nhắn trong ngày cho người dùng được xác thực. Các hệ thống dựa trên Unix thường hiển thị thông tin về bản phát hành và bản vá hệ điều hành cấp khi đăng nhập vào hệ thống. Thông tin này có thể hữu 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 như sau tùy chọn, chúng hiển thị thông tin hệ điều hành: \m - kiến trúc máy \r - bản phát hành hệ điều hành \s - tên hệ điều hành \v - phiên bản hệ điều hành
* Thông báo cảnh báo thông báo cho người dùng đang cố gắng đăng nhập vào hệ thống hợp pháp của họ tình trạng liên quan đến hệ thống và phải bao gồm tên của tổ chức sở hữu hệ thống và bất kỳ chính sách giám sát nào được áp dụng. Hiển thị hệ điều hành và cấp độ bản vá thông tin trong biểu ngữ đăng nhập cũng có tác dụng phụ là cung cấp hệ thống chi tiết thông tin cho những kẻ tấn công đang cố gắng nhắm mục tiêu khai thác cụ thể của một hệ thống. Người dùng được ủy quyền có thể dễ dàng lấy thông tin này bằng cách chạy lệnh " uname -a " sau khi họ đã đăng nhập

**1.7.2 Ensure local login warning banner is configured properly (Automated)**

* Đảm bảo biểu ngữ cảnh báo đăng nhập cục bộ được định cấu hình đúng cách
* Nội dung của tệp /etc/issue được hiển thị cho người dùng trước khi đăng nhập vào các thiết bị đầu cuối cục bộ. Các hệ thống dựa trên Unix thường hiển thị thông tin về bản phát hành và bản vá hệ điều hành cấp khi đăng nhập vào hệ thống. Thông tin này có thể hữu 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 như sau tùy chọn, chúng hiển thị thông tin hệ điều hành: \m - kiến trúc máy \r - bản phát hành hệ điều hành \s - tên hệ điều hành \v - phiên bản hệ điều hành - hoặc tên hệ điều hành
* Thông báo cảnh báo thông báo cho người dùng đang cố gắng đăng nhập vào hệ thống hợp pháp của họ tình trạng liên quan đến hệ thống và phải bao gồm tên của tổ chức sở hữu hệ thống và bất kỳ chính sách giám sát nào được áp dụng. Hiển thị hệ điều hành và cấp độ bản vá thông tin trong biểu ngữ đăng nhập cũng có tác dụng phụ là cung cấp hệ thống chi tiết thông tin cho những kẻ tấn công đang cố gắng nhắm mục tiêu khai thác cụ thể của một hệ thống. Người dùng được ủy quyền có thể dễ dàng lấy thông tin này bằng cách chạy lệnh " uname -a " sau khi họ đã đăng nhập

**1.7.3 Ensure remote login warning banner is configured properly (Automated)**

* Đảm bảo biểu ngữ cảnh báo đăng nhập từ xa được cấu hình đúng cách
* Nội dung của tệp /etc/issue.net được hiển thị cho người dùng trước khi đăng nhập từ xa kết nối từ các dịch vụ được cấu hình. Các hệ thống dựa trên Unix thường hiển thị thông tin về bản phát hành và bản vá hệ điều hành cấp khi đăng nhập vào hệ thống. Thông tin này có thể hữu 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 như sau tùy chọn, chúng hiển thị thông tin hệ điều hành: \m - kiến trúc máy \r - bản phát hành hệ điều hành \s - tên hệ điều hành \v - phiên bản hệ điều hành
* Thông báo cảnh báo thông báo cho người dùng đang cố gắng đăng nhập vào hệ thống hợp pháp của họ tình trạng liên quan đến hệ thống và phải bao gồm tên của tổ chức sở hữu hệ thống và bất kỳ chính sách giám sát nào được áp dụng. Hiển thị hệ điều hành và cấp độ bản vá thông tin trong biểu ngữ đăng nhập cũng có tác dụng phụ là cung cấp hệ thống chi tiết thông tin cho những kẻ tấn công đang cố gắng nhắm mục tiêu khai thác cụ thể của một hệ thống. Người dùng được ủy quyền có thể dễ dàng lấy thông tin này bằng cách chạy lệnh " uname -a " sau khi họ đã đăng nhập

**1.7.4 Ensure permissions on /etc/motd are configured (Automated)**

* Đảm bảo các quyền trên /etc/motd được cấu hình
* Nội dung của tệp /etc/motd được hiển thị cho người dùng sau khi đăng nhập và hoạt động như một tin nhắn trong ngày cho người dùng được xác thực.
* Nếu tệp /etc/motd không có quyền sở hữu chính xác thì nó có thể được sửa đổi bởi người dùng trái phép với thông tin không chính xác hoặc sai lệch

**1.7.5 Ensure permissions on /etc/issue are configured (Automated)**

* Đảm bảo các quyền trên/etc/vấn đề được định cấu hình
* Nội dung của tệp /etc/issue được hiển thị cho người dùng trước khi đăng nhập vào các thiết bị đầu cuối cục bộ.
* Nếu tệp /etc/issue không có quyền sở hữu chính xác thì nó có thể được sửa đổi bởi người dùng trái phép với thông tin không chính xác hoặc sai lệch

**1.7.6 Ensure permissions on /etc/issue.net are configured (Automated)**

* Đảm bảo các quyền trên /etc/issue.net được định cấu hình
* Nội dung của tệp /etc/issue.net được hiển thị cho người dùng trước khi đăng nhập từ xa kết nối từ các dịch vụ được cấu hình.
* Nếu tệp /etc/issue.net không có quyền sở hữu chính xác, nó có thể được sửa đổi bởi người dùng trái phép với thông tin không chính xác hoặc sai lệch

**1.8 GNOME Display Manager**

**1.8.1 Ensure GNOME Display Manager is removed (Manual)**

* Đảm bảo Trình quản lý hiển thị Gnome đã bị xóa
* Trình quản lý hiển thị GNOME (GDM) là một chương trình quản lý các máy chủ hiển thị đồ họa và xử lý đăng nhập người dùng đồ họa.
* Nếu Giao diện người dùng đồ họa (GUI) không được yêu cầu, nó sẽ bị loại bỏ để giảm bề mặt tấn công của hệ thống.

**1.8.2 Ensure GDM login banner is configured (Automated)**

* Đảm bảo biểu ngữ đăng nhập GDM được định cấu hình
* GDM là Trình quản lý hiển thị Gnome xử lý đăng nhập đồ họa cho Gnome dựa trên các hệ thống.
* Thông báo cảnh báo thông báo cho người dùng đang cố gắng đăng nhập vào hệ thống hợp pháp của họ tình trạng liên quan đến hệ thống và phải bao gồm tên của tổ chức sở hữu hệ thống và bất kỳ chính sách giám sát nào được áp dụng

**1.8.3 Ensure last logged in user display is disabled (Automated)**

* Đảm bảo hiển thị người dùng đăng nhập lần cuối bị tắt
* GDM là Trình quản lý hiển thị Gnome xử lý đăng nhập đồ họa cho Gnome dựa trên các hệ thống.
* Hiển thị người dùng đã đăng nhập lần cuối sẽ loại bỏ một nửa phương trình Userid/Mật khẩu mà một người không được ủy quyền sẽ cần phải đăng nhập. Thông báo cảnh báo thông báo cho người dùng đang cố gắng đăng nhập vào hệ thống hợp pháp của họ tình trạng liên quan đến hệ thống và phải bao gồm tên của tổ chức sở hữu hệ thống và bất kỳ chính sách giám sát nào được áp dụng

**1.8.4 Ensure XDCMP is not enabled (Automated)**

* Đảm bảo XDCMP không được bật
* X Display Manager Control Protocol (XDMCP) được thiết kế để cung cấp quyền truy cập được xác thực để hiển thị các dịch vụ quản lý cho màn hình từ xa
* XDMCP vốn không an toàn.
* XDMCP không phải là một giao thức mã hóa. Điều này có thể cho phép kẻ tấn công nắm bắt các lần nhấn phím được nhập bởi người dùng
* XDMCP dễ bị tấn công bởi người trung gian. Điều này có thể cho phép kẻ tấn công đánh cắp thông tin đăng nhập của người dùng hợp pháp bằng cách mạo danh máy chủ XDMCP

**1.9 Ensure updates, patches, and additional security software are installed (Manual)**

* Đảm bảo các bản cập nhật, bản vá và phần mềm bảo mật bổ sung được cài đặt
* Các bản vá định kỳ được phát hành cho phần mềm đi kèm do lỗi bảo mật hoặc do bao gồm chức năng bổ sung.
* Các bản vá mới hơn có thể chứa các cải tiến bảo mật không có sẵn thông qua cập nhật đầy đủ mới nhất. Do đó, nên sử dụng các bản vá lỗi phần mềm mới nhất để tận dụng các chức năng mới nhất. Như với bất kỳ cài đặt phần mềm nào, các tổ chức cần xác định xem một bản cập nhật nhất định có đáp ứng yêu cầu của họ hay không và xác minh tính tương thích và khả năng hỗ trợ của bất kỳ phần mềm bổ sung nào đối với bản sửa đổi cập nhật được chọn

**2 Services**

**2.1 inetd Services**

**2.1.1 Ensure xinetd is not installed (Automated)**

* Đảm bảo xinetd chưa được cài đặt
* eXtended InterNET Daemon ( xinetd ) là một siêu daemon mã nguồn mở đã thay thế trình nền inetd ban đầu. Trình nền xinetd lắng nghe các dịch vụ nổi tiếng và gửi trình nền thích hợp để đáp ứng đúng các yêu cầu dịch vụ.
* Nếu không có dịch vụ xinetd nào được yêu cầu, bạn nên xóa gói này khỏi giảm bề mặt tấn công của hệ thống

**2.2 Special Purpose Services**

**2.2.1 Time Synchronization**

**2.2.1.1 Ensure time synchronization is in use (Manual)**

* Đảm bảo đồng bộ hóa thời gian đang được sử dụng
* Thời gian hệ thống phải được đồng bộ hóa giữa tất cả các hệ thống trong một môi trường. Đây là thường được thực hiện bằng cách thiết lập một máy chủ thời gian có thẩm quyền hoặc một bộ máy chủ và có tất cả hệ thống đồng bộ hóa đồng hồ của họ với họ.
* Đồng bộ hóa thời gian rất quan trọng để hỗ trợ các cơ chế bảo mật nhạy cảm với thời gian như Kerberos và cũng đảm bảo các tệp nhật ký có bản ghi thời gian nhất quán trong toàn doanh nghiệp, hỗ trợ điều tra pháp y

**2.2.1.2 Ensure chrony is configured (Automated)**

* Đảm bảo chrony được cấu hình
* chrony là một trình nền thực hiện Giao thức thời gian mạng (NTP) và được thiết kế để đồng bộ hóa đồng hồ hệ thống trên nhiều hệ thống khác nhau và sử dụng một nguồn được đánh giá cao chính xác. Thông tin thêm về chrony có thể được tìm thấy tại http://chrony.tuxfamily.org/. niên đại có thể được cấu hình để trở thành máy khách và/hoặc máy chủ.
* Nếu đồng hồ bấm giờ được sử dụng trên hệ thống, cấu hình phù hợp là rất quan trọng để đảm bảo thời gian đồng bộ hóa đang hoạt động bình thường

**2.2.1.3 Ensure ntp is configured (Automated)**

* Đảm bảo ntp được cấu hình
* ntp là một trình nền thực hiện Giao thức thời gian mạng (NTP). Nó được thiết kế để đồng bộ hóa đồng hồ hệ thống trên nhiều hệ thống khác nhau và sử dụng một nguồn được đánh giá cao chính xác. Thông tin thêm về NTP có thể được tìm thấy tại http://www.ntp.org. ntp có thể là được cấu hình để trở thành máy khách và/hoặc máy chủ.
* Nếu ntp đang được sử dụng trên hệ thống, cấu hình phù hợp là rất quan trọng để đảm bảo đồng bộ hóa thời gian đang hoạt động bình thường.

**2.2.2 Ensure X11 Server components are not installed (Automated)**

* Đảm bảo các thành phần Máy chủ X11 chưa được cài đặt
* Hệ thống X Window cung cấp Giao diện người dùng đồ họa (GUI) nơi người dùng có thể có nhiều cửa sổ để chạy các chương trình và nhiều tiện ích bổ sung khác nhau. Hệ thống X Windows là thường được sử dụng trên các máy trạm nơi người dùng đăng nhập, nhưng không phải trên các máy chủ nơi người dùng thường không đăng nhập.
* Trừ khi tổ chức của bạn yêu cầu cụ thể quyền truy cập đăng nhập đồ họa qua X Windows, loại bỏ nó để giảm bề mặt tấn công tiềm năng

**2.2.3 Ensure Avahi Server is not installed (Automated)**

* Đảm bảo Avahi Server chưa được cài đặt
* Avahi là một triển khai zeroconf miễn phí, bao gồm một hệ thống cho DNS/DNS-SD phát đa hướng khám phá dịch vụ. Avahi cho phép các chương trình xuất bản và khám phá các dịch vụ và máy chủ chạy trên mạng cục bộ không có cấu hình cụ thể. Ví dụ, một người dùng có thể cắm một máy tính vào mạng và Avahi tự động tìm máy in để in, tệp để xem và những người để nói chuyện, cũng như các dịch vụ mạng đang chạy trên máy.
* Tự động phát hiện các dịch vụ mạng thường không cần thiết cho chức năng hệ thống. Nên loại bỏ gói này để giảm bề mặt tấn công tiềm năng

**2.2.4 Ensure CUPS is not installed (Automated)**

* Đảm bảo CUPS chưa được cài đặt
* Hệ thống in Unix chung (CUPS) cung cấp khả năng in cho cả cục bộ và máy in mạng. Một hệ thống đang chạy CUPS cũng có thể chấp nhận lệnh in từ các hệ thống từ xa và in chúng ra máy in cục bộ. Nó cũng cung cấp một quản trị từ xa dựa trên web khả năng.
* Nếu hệ thống không cần lệnh in hoặc chấp nhận lệnh in từ các hệ thống khác, thì đó là khuyến nghị loại bỏ CUPS để giảm bề mặt tấn công tiềm năng

**2.2.5 Ensure DHCP Server is not installed (Automated)**

* Đảm bảo DHCP Server chưa được cài đặt
* Giao thức Cấu hình Máy chủ Động (DHCP) là một dịch vụ cho phép các máy được địa chỉ IP được gán động.
* Trừ khi một hệ thống được thiết lập riêng để hoạt động như một máy chủ DHCP, chúng tôi khuyến nghị rằng gói dhcp bị xóa để giảm bề mặt tấn công tiềm ẩn

**2.2.6 Ensure LDAP server is not installed (Automated)**

* Đảm bảo máy chủ LDAP chưa được cài đặt
* Giao thức truy cập thư mục nhẹ (LDAP) đã được giới thiệu để thay thế cho NIS/YP. Là dịch vụ cung cấp phương thức tra cứu thông tin từ trung tâm cơ sở dữ liệu.
* Nếu hệ thống không cần hoạt động như một máy chủ LDAP, phần mềm nên được loại bỏ để giảm bề mặt tấn công tiềm năng

**2.2.7 Ensure DNS Server is not installed (Automated)**

* Đảm bảo Máy chủ DNS chưa được cài đặt
* Hệ thống tên miền (DNS) là một hệ thống đặt tên phân cấp ánh xạ tên tới IP địa chỉ cho máy tính, dịch vụ và các tài nguyên khác được kết nối với mạng.
* Trừ khi một hệ thống được chỉ định cụ thể để hoạt động như một máy chủ DNS, chúng tôi khuyến nghị rằng gói được gỡ bỏ để giảm bề mặt tấn công tiềm năng

**2.2.8 Ensure FTP Server is not installed (Automated)**

* Đảm bảo Máy chủ FTP chưa được cài đặt
* FTP (Giao thức truyền tệp) là một công cụ tiêu chuẩn truyền thống và được sử dụng rộng rãi để truyền các tệp giữa máy chủ và máy khách qua mạng, đặc biệt là khi không có xác thực cần thiết (cho phép người dùng ẩn danh kết nối với máy chủ).
* FTP không bảo vệ tính bảo mật của dữ liệu hoặc thông tin xác thực. Nó là nên sử dụng SFTP nếu cần truyền tệp. Trừ khi có nhu cầu chạy hệ thống như một máy chủ FTP (ví dụ: để cho phép tải xuống ẩn danh), bạn nên rằng gói được gỡ bỏ để giảm bề mặt tấn công tiềm ẩn.

**2.2.9 Ensure HTTP server is not installed (Automated)**

* Đảm bảo máy chủ HTTP chưa được cài đặt
* HTTP hoặc máy chủ web cung cấp khả năng lưu trữ nội dung trang web.
* Trừ khi có nhu cầu chạy hệ thống như một máy chủ web, chúng tôi khuyến nghị rằng gói được gỡ bỏ để giảm bề mặt tấn công tiềm năng

**2.2.10 Ensure IMAP and POP3 server is not installed (Automated)**

* Đảm bảo máy chủ IMAP và POP3 chưa được cài đặt
* dovecot là một máy chủ IMAP và POP3 nguồn mở cho các hệ thống dựa trên Linux.
* Trừ khi các máy chủ POP3 và/hoặc IMAP được cung cấp bởi hệ thống này, chúng tôi khuyến nghị rằng gói được gỡ bỏ để giảm bề mặt tấn công tiềm năng

**2.2.11 Ensure Samba is not installed (Automated)**

* Đảm bảo Samba chưa được cài đặt
* Trình nền Samba cho phép quản trị viên hệ thống định cấu hình hệ thống Linux của họ để chia sẻ hệ thống tệp và thư mục với máy tính để bàn Windows. Samba sẽ quảng cáo các hệ thống tập tin và các thư mục thông qua giao thức Server Message Block (SMB). Người dùng máy tính để bàn Windows sẽ có thể gắn các thư mục và hệ thống tệp này dưới dạng ổ đĩa ký tự trên hệ thống của họ.
* Nếu không cần gắn các thư mục và hệ thống tệp vào hệ thống Windows, thì điều này gói có thể được gỡ bỏ để giảm bề mặt tấn công tiềm năng

**2.2.12 Ensure HTTP Proxy Server is not installed (Automated)**

* Đảm bảo HTTP Proxy Server chưa được cài đặt
* Squid là một máy chủ proxy tiêu chuẩn được sử dụng trong nhiều bản phân phối và môi trường.
* Trừ khi một hệ thống được thiết lập riêng để hoạt động như một máy chủ proxy, chúng tôi khuyến nghị rằng gói mực được loại bỏ để giảm bề mặt tấn công tiềm năng

**2.2.13 Ensure net-snmp is not installed (Automated)**

* Đảm bảo net-snmp chưa được cài đặt
* Giao thức quản lý mạng đơn giản (SNMP) là một giao thức được sử dụng rộng rãi để giám sát sức khỏe và phúc lợi của thiết bị mạng, thiết bị máy tính và các thiết bị như UPS.
* Net-SNMP là bộ ứng dụng được sử dụng để triển khai SNMPv1 (RFC 1157), SNMPv2 (RFCs 1901-1908) và SNMPv3 (RFCs 3411-3418) sử dụng cả IPv4 và IPv6.
* Hỗ trợ cho SNMPv2 cổ điển (còn gọi là "SNMPv2 lịch sử" - RFC 1441-1452) đã bị loại bỏ với bản phát hành 4.0 của gói UCD-snmp.
* Máy chủ Giao thức quản lý mạng đơn giản (SNMP) được sử dụng để lắng nghe SNMP các lệnh từ hệ thống quản lý SNMP, thực hiện các lệnh hoặc thu thập thông tin và sau đó gửi kết quả trở lại hệ thống yêu cầu.
* Máy chủ SNMP có thể giao tiếp bằng SNMPv1, truyền dữ liệu rõ ràng và không yêu cầu xác thực để thực thi lệnh. SNMPv3 thay thế đơn giản/rõ ràng chia sẻ mật khẩu văn bản được sử dụng trong SNMPv2 với các tham số được mã hóa an toàn hơn. Nếu các Dịch vụ SNMP không bắt buộc, gói net-snmp nên được gỡ bỏ để giảm bề mặt tấn công của hệ thống.

**2.2.14 Ensure NIS server is not installed (Automated)**

* Đảm bảo máy chủ NIS chưa được cài đặt
* Gói ypserv cung cấp Dịch vụ Thông tin Mạng (NIS). Dịch vụ này, chính thức được gọi là Những trang vàng, là một giao thức dịch vụ thư mục máy khách-máy chủ để phân phối hệ thống tập tin cấu hình. Máy chủ NIS là một tập hợp các chương trình cho phép phân phối của các tập tin cấu hình.
* Dịch vụ NIS vốn là một hệ thống không an toàn dễ bị tấn công bởi DOS, tràn bộ đệm và xác thực kém để truy vấn bản đồ NIS. NIS thường có đã được thay thế bằng các giao thức như Giao thức truy cập thư mục nhẹ (LDAP). Nó là khuyến nghị nên gỡ bỏ gói ypserv và nếu được yêu cầu, một dịch vụ an toàn hơn được dùng

**2.2.15 Ensure telnet-server is not installed (Automated)**

* Đảm bảo máy chủ telnet chưa được cài đặt
* Gói máy chủ telnet chứa trình nền telnet, nó chấp nhận các kết nối từ người dùng từ các hệ thống khác thông qua giao thức telnet.
* Giao thức telnet không an toàn và không được mã hóa. Việc sử dụng đường truyền không được mã hóa phương tiện có thể cho phép người dùng có quyền truy cập đánh hơi lưu lượng mạng có khả năng đánh cắp thông tin đăng nhập. Gói ssh cung cấp phiên mã hóa và bảo mật mạnh hơn

**2.2.16 Ensure mail transfer agent is configured for local-only mode (Automated)**

* Đảm bảo tác nhân chuyển thư được định cấu hình cho chế độ chỉ cục bộ
* Đại lý chuyển thư (MTA), chẳng hạn như sendmail và Postfix, được sử dụng để lắng nghe thư đến thư và chuyển thư đến người dùng hoặc máy chủ thư thích hợp. Nếu hệ thống không dự định là một máy chủ thư, MTA nên được cấu hình để chỉ xử lý thư cục bộ.
* Phần mềm dành cho tất cả các Đại lý chuyển thư rất phức tạp và hầu hết đều có lịch sử lâu đời về Vân đê bảo mật. Mặc dù điều quan trọng là phải đảm bảo rằng hệ thống có thể xử lý thư cục bộ tin nhắn, không nhất thiết phải có daemon của MTA lắng nghe trên một cổng trừ khi máy chủ được dự định là một máy chủ thư nhận và xử lý thư từ các hệ thống khác

**2.2.17 Ensure nfs-utils is not installed or the nfs-server service is masked (Automated)**

* Đảm bảo nfs-utils chưa được cài đặt hoặc dịch vụ nfs-server bị ẩn
* Hệ thống tệp mạng (NFS) là một trong những hệ thống tệp đầu tiên và được phân phối rộng rãi nhất trong môi trường UNIX. Nó cung cấp khả năng cho các hệ thống gắn các hệ thống tệp của các máy chủ thông qua mạng.
* Nếu hệ thống không yêu cầu chia sẻ mạng, gói nfs-utils được khuyến nghị được loại bỏ để giảm bề mặt tấn công của hệ thống

**2.2.18 Ensure rpcbind is not installed or the rpcbind services are masked (Automated)**

* Đảm bảo rpcbind chưa được cài đặt hoặc dịch vụ rpcbind bị che
* Tiện ích rpcbind ánh xạ các dịch vụ RPC tới các cổng mà chúng lắng nghe. quy trình RPC thông báo cho rpcbind khi chúng bắt đầu, đăng ký các cổng mà chúng đang nghe và RPC số chương trình mà họ mong muốn phục vụ. Sau đó, hệ thống máy khách sẽ liên lạc với rpcbind trên máy chủ với một số chương trình RPC cụ thể. Dịch vụ rpcbind chuyển hướng máy khách đến số cổng thích hợp để nó có thể giao tiếp với dịch vụ được yêu cầu
* Portmapper là một dịch vụ RPC, luôn lắng nghe trên tcp và udp 111 và được sử dụng để ánh xạ các dịch vụ RPC khác (chẳng hạn như nfs, nlockmgr, quotad, mountd, v.v.) vào các dịch vụ tương ứng của chúng số cổng trên máy chủ. Khi một máy chủ từ xa thực hiện cuộc gọi RPC đến máy chủ đó, trước tiên nó tư vấn với portmap để xác định nơi máy chủ RPC đang lắng nghe.
* Một yêu cầu nhỏ (~82 byte qua UDP) được gửi tới Portmapper sẽ tạo ra một phản hồi lớn (7x đến khuếch đại 28 lần), khiến nó trở thành một công cụ phù hợp cho các cuộc tấn công DDoS. Nếu rpcbind không phải là bắt buộc, nên gỡ bỏ gói rpcbind để giảm bớt cuộc tấn công bề mặt của hệ thống.

**2.2.19 Ensure rsync is not installed or the rsyncd service is masked (Automated)**

* Đảm bảo rsync chưa được cài đặt hoặc dịch vụ rsyncd bị che
* Dịch vụ rsyncd có thể được sử dụng để đồng bộ hóa tệp giữa các hệ thống qua liên kết mạng.
* Trừ khi được yêu cầu, gói rsync nên được gỡ bỏ để giảm diện tích bề mặt tấn công của hệ thống. Dịch vụ rsyncd có rủi ro bảo mật vì nó sử dụng các giao thức không được mã hóa để giao tiếp.

**2.3 Service Clients**

**2.3.1 Ensure NIS Client is not installed (Automated)**

* Đảm bảo máy khách NIS chưa được cài đặt
* Dịch vụ thông tin mạng (NIS), trước đây gọi là Trang vàng, là máy khách-máy chủ giao thức dịch vụ thư mục được sử dụng để phân phối các tệp cấu hình hệ thống. Máy khách NIS (ypbind ) được sử dụng để liên kết máy với máy chủ NIS và nhận dữ liệu được phân phối tập tin cấu hình.
* Dịch vụ NIS vốn là một hệ thống không an toàn dễ bị tấn công bởi DOS, tràn bộ đệm và xác thực kém để truy vấn bản đồ NIS. NIS thường có đã được thay thế bằng các giao thức như Giao thức truy cập thư mục nhẹ (LDAP). Nó là đề nghị gỡ bỏ dịch vụ

**2.3.2 Ensure rsh client is not installed (Automated)**

* Đảm bảo máy khách rsh chưa được cài đặt
* Gói rsh chứa các lệnh máy khách cho các dịch vụ rsh.
* Các ứng dụng khách cũ này chứa nhiều rủi ro bảo mật và đã được thay thế bằng gói SSH an toàn hơn. Ngay cả khi máy chủ bị xóa, tốt nhất là đảm bảo các máy khách cũng bị xóa để ngăn người dùng vô tình cố gắng sử dụng các lệnh này và do đó tiết lộ thông tin đăng nhập của họ. Lưu ý rằng việc loại bỏ gói rsh sẽ loại bỏ ứng dụng khách cho rsh , rcp và rlogin

**2.3.3 Ensure talk client is not installed (Automated)**

* Đảm bảo máy khách nói chuyện chưa được cài đặt
* Phần mềm nói chuyện giúp người dùng có thể gửi và nhận tin nhắn trên các hệ thống thông qua một phiên cuối. Ứng dụng trò chuyện, cho phép khởi tạo các phiên trò chuyện, là được cài đặt theo mặc định.
* Phần mềm có rủi ro bảo mật vì nó sử dụng các giao thức không được mã hóa để liên lạc

**2.3.4 Ensure telnet client is not installed (Automated)**

* Đảm bảo telnet client chưa được cài đặt
* Gói telnet chứa ứng dụng khách telnet, cho phép người dùng bắt đầu kết nối với các hệ thống khác thông qua giao thức telnet.
* Giao thức telnet không an toàn và không được mã hóa. Việc sử dụng đường truyền không được mã hóa phương tiện có thể cho phép người dùng trái phép ăn cắp thông tin xác thực. Gói ssh cung cấp một phiên được mã hóa và bảo mật mạnh hơn và được bao gồm trong hầu hết các bản phân phối Linux

**2.3.5 Ensure LDAP client is not installed (Automated)**

* Đảm bảo máy khách LDAP chưa được cài đặt
* Giao thức truy cập thư mục nhẹ (LDAP) đã được giới thiệu để thay thế cho NIS/YP. Là dịch vụ cung cấp phương thức tra cứu thông tin từ trung tâm cơ sở dữ liệu.
* Nếu hệ thống không cần hoạt động như một ứng dụng khách LDAP, phần mềm nên được loại bỏ để giảm bề mặt tấn công tiềm năng.

**2.4 Ensure nonessential services are removed or masked (Manual)**

* Đảm bảo các dịch vụ không cần thiết được loại bỏ hoặc che giấu
* Một cổng mạng được xác định bởi số của nó, địa chỉ IP được liên kết và loại cổng mạng giao thức truyền thông như TCP hoặc UDP.
* Cổng lắng nghe là cổng mạng mà ứng dụng hoặc quy trình lắng nghe trên đó, hoạt động như một điểm cuối giao tiếp.
* Mỗi cổng nghe có thể được mở hoặc đóng (được lọc) bằng tường lửa. Nói chung, một cổng mở là một cổng mạng chấp nhận các gói đến từ các địa điểm từ xa.
* Các dịch vụ lắng nghe trên hệ thống có nguy cơ tiềm ẩn như một phương tiện tấn công. Những dịch vụ này nên được xem xét và nếu không bắt buộc, dịch vụ sẽ bị dừng và gói chứa dịch vụ nên được gỡ bỏ. Nếu các gói được yêu cầu có một phụ thuộc, dịch vụ nên được dừng lại và che dấu để giảm bề mặt tấn công của hệ thống

**3 Network Configuration**

**3.1 Disable unused network protocols and devices**

**3.1.1 Disable IPv6 (Manual)**

* Vô hiệu hóa IPv6
* Mặc dù IPv6 có nhiều ưu điểm hơn IPv4 nhưng không phải tất cả các tổ chức đều có IPv6 hoặc dual cấu hình ngăn xếp được triển khai.
* Nếu không sử dụng IPv6 hoặc ngăn xếp kép, nên tắt IPv6 để giảm bề mặt tấn công của hệ thống

**3.1.2 Ensure wireless interfaces are disabled (Automated)**

* Đảm bảo giao diện không dây bị vô hiệu hóa
* Mạng không dây được sử dụng khi không có mạng có dây.
* Nếu không sử dụng mạng không dây, nên tắt các thiết bị không dây để giảm khả năng bề mặt tấn công

**3.2 Network Parameters (Host Only)**

**3.2.1 Ensure IP forwarding is disabled (Automated)**

* Đảm bảo chuyển tiếp IP bị tắt
* Các cờ net.ipv4.ip\_forward và net.ipv6.conf.all.forwarding được sử dụng để thông báo cho hệ thống có thể chuyển tiếp gói tin hay không.
* Đặt các cờ thành 0 đảm bảo rằng một hệ thống có nhiều giao diện (ví dụ: giao diện cứng proxy), sẽ không bao giờ có thể chuyển tiếp các gói và do đó, không bao giờ đóng vai trò là bộ định tuyến

**3.2.2 Ensure packet redirect sending is disabled (Automated)**

* Đảm bảo gửi chuyển hướng gói bị vô hiệu hóa
* Chuyển hướng ICMP được sử dụng để gửi thông tin định tuyến đến các máy chủ khác. Như một máy chủ tự nó làm không hoạt động như một bộ định tuyến (trong cấu hình chỉ dành cho máy chủ lưu trữ), không cần gửi chuyển hướng.
* Kẻ tấn công có thể sử dụng máy chủ bị xâm nhập để gửi chuyển hướng ICMP không hợp lệ đến bộ định tuyến khác các thiết bị cố gắng làm hỏng định tuyến và yêu cầu người dùng truy cập hệ thống được thiết lập bởi kẻ tấn công trái ngược với một hệ thống hợp lệ

**3.3 Network Parameters (Host and Router)**

**3.3.1 Ensure source routed packets are not accepted (Automated)**

* Đảm bảo các gói định tuyến nguồn không được chấp nhận
* Trong mạng, định tuyến nguồn cho phép người gửi chỉ định một phần hoặc toàn bộ các gói định tuyến đi qua một mạng. Ngược lại, các gói được định tuyến không nguồn sẽ di chuyển theo một đường dẫn được xác định bởi các bộ định tuyến trong mạng. Trong một số trường hợp, các hệ thống có thể không định tuyến được hoặc không thể truy cập được từ một số vị trí (ví dụ: địa chỉ riêng so với Internet có thể định tuyến) và do đó, các gói được định tuyến nguồn sẽ cần phải được sử dụng.
* Đặt net.ipv4.conf.all.accept\_source\_route, net.ipv4.conf.default.accept\_source\_route, net.ipv6.conf.all.accept\_source\_route và net.ipv6.conf.default.accept\_source\_route thành 0 sẽ vô hiệu hóa hệ thống chấp nhận gói định tuyến nguồn. Giả sử hệ thống này có khả năng định tuyến các gói đến Internet địa chỉ có thể định tuyến trên một giao diện và địa chỉ riêng trên giao diện khác. Cho rằng rằng các địa chỉ riêng không thể định tuyến đến các địa chỉ có thể định tuyến trên Internet và ngược lại ngược lại. Trong các trường hợp định tuyến bình thường, kẻ tấn công từ Internet có thể định tuyến các địa chỉ không thể sử dụng hệ thống như một cách để tiếp cận các hệ thống địa chỉ riêng. Nếu như, tuy nhiên, các gói được định tuyến nguồn được cho phép, chúng có thể được sử dụng để truy cập vào hệ thống địa chỉ riêng vì tuyến đường có thể được chỉ định, thay vì dựa vào định tuyến các giao thức không cho phép định tuyến này

**3.3.2 Ensure ICMP redirects are not accepted (Automated)**

* Đảm bảo chuyển hướng ICMP không được chấp nhận
* Thông báo chuyển hướng ICMP là các gói truyền tải thông tin định tuyến và thông báo cho máy chủ của bạn (hoạt động như một bộ định tuyến) để gửi các gói thông qua một đường dẫn thay thế. Đó là một cách cho phép bên ngoài thiết bị định tuyến để cập nhật bảng định tuyến hệ thống của bạn. Bằng cách thiết lập net.ipv4.conf.all.accept\_redirects và net.ipv6.conf.all.accept\_redirects thành 0, hệ thống sẽ không chấp nhận bất kỳ thông báo chuyển hướng ICMP nào và do đó, sẽ không cho phép bên ngoài để cập nhật các bảng định tuyến của hệ thống.
* Kẻ tấn công có thể sử dụng tin nhắn chuyển hướng ICMP giả để thay đổi định tuyến hệ thống một cách ác ý các bảng và yêu cầu chúng gửi các gói đến các mạng không chính xác và cho phép các gói hệ thống của bạn bị bắt.

**3.3.3 Ensure secure ICMP redirects are not accepted (Automated)**

* Đảm bảo chuyển hướng ICMP an toàn không được chấp nhận
* Chuyển hướng ICMP an toàn giống như chuyển hướng ICMP, ngoại trừ chúng đến từ các cổng được liệt kê trong danh sách cổng mặc định. Người ta cho rằng các cổng này được biết đến với bạn hệ thống, và rằng chúng có khả năng được an toàn.
* Thậm chí các cổng đã biết vẫn có thể bị xâm phạm. Cài đặt net.ipv4.conf.all.secure\_redirects thành 0 bảo vệ hệ thống khỏi bảng định tuyến cập nhật bởi các cổng đã biết có thể bị xâm phạm.

**3.3.4 Ensure suspicious packets are logged (Automated)**

* Đảm bảo các gói đáng ngờ được ghi lại
* Khi được bật, tính năng này sẽ ghi các gói có địa chỉ nguồn không thể định tuyến vào nhân nhật ký.
* Kích hoạt tính năng này và ghi nhật ký các gói này cho phép quản trị viên điều tra khả năng kẻ tấn công đang gửi các gói giả mạo đến hệ thống của họ

**3.3.5 Ensure broadcast ICMP requests are ignored (Automated)**

* Đảm bảo các yêu cầu ICMP phát sóng bị bỏ qua
* Đặt net.ipv4.icmp\_echo\_ignore\_broadcasts thành 1 sẽ khiến hệ thống bỏ qua tất cả Yêu cầu ICMP echo và timestamp tới các địa chỉ quảng bá và phát đa hướng.
* Chấp nhận các yêu cầu dấu thời gian và tiếng vang ICMP với các đích quảng bá hoặc phát đa hướng cho mạng của bạn có thể được sử dụng để lừa máy chủ của bạn bắt đầu (hoặc tham gia) vào Smurf tấn công. Một cuộc tấn công Smurf dựa vào việc kẻ tấn công gửi một lượng lớn ICMP được phát tin nhắn với một địa chỉ nguồn giả mạo. Tất cả các máy chủ nhận được thông báo này và phản hồi sẽ gửi tin nhắn trả lời bằng tiếng vang trở lại địa chỉ giả mạo, điều này có thể không định tuyến được. Nếu nhiều máy chủ phản hồi các gói, lượng lưu lượng truy cập trên mạng có thể được nhân lên đáng kể

**3.3.6 Ensure bogus ICMP responses are ignored (Automated)**

* Đảm bảo các phản hồi ICMP không có thật bị bỏ qua
* Đặt icmp\_ignore\_bogus\_error\_responses thành 1 ngăn nhân ghi nhật ký không có thật phản hồi (không tuân thủ RFC-1122) từ các khung phát sóng, giữ cho hệ thống tệp không bị đầy những thông điệp bản ghi vô ích.
* Một số bộ định tuyến (và một số kẻ tấn công) sẽ gửi phản hồi vi phạm RFC-1122 và cố gắng để lấp đầy một hệ thống tệp nhật ký với nhiều thông báo lỗi vô dụng

**3.3.7 Ensure Reverse Path Filtering is enabled (Automated)**

* Đảm bảo Lọc đường dẫn đảo ngược được bật
* Đặt net.ipv4.conf.all.rp\_filter và net.ipv4.conf.default.rp\_filter thành 1 lực lượng nhân Linux để sử dụng tính năng lọc đường dẫn ngược trên gói nhận được để xác định xem gói đã hợp lệ. Về cơ bản, với tính năng lọc đường ngược lại, nếu gói trả về không đi ra cùng một giao diện mà gói nguồn tương ứng đến từ đó, gói được bị hủy (và được ghi lại nếu log\_martians được đặt).
* Đặt các cờ này là một cách tốt để ngăn chặn những kẻ tấn công gửi tin giả vào hệ thống của bạn các gói không thể được đáp ứng. Một trường hợp mà tính năng này bị hỏng là nếu định tuyến bất đối xứng được sử dụng. Điều này sẽ xảy ra khi sử dụng các giao thức định tuyến động (bgp, ospf, v.v.) trên hệ thống của bạn. Nếu bạn đang sử dụng định tuyến không đối xứng trên hệ thống của mình, bạn sẽ không thể bật tính năng này nếu không phá vỡ định tuyến

**3.3.8 Ensure TCP SYN Cookies is enabled (Automated)**

* Đảm bảo Cookie TCP SYN được bật
* Khi tcp\_syncookies được đặt, kernel sẽ xử lý các gói TCP SYN bình thường cho đến khi hàng đợi kết nối nửa mở đã đầy, tại thời điểm đó, chức năng cookie SYN sẽ bắt đầu hoạt động. SYN cookie hoạt động bằng cách hoàn toàn không sử dụng hàng đợi SYN. Thay vào đó, hạt nhân chỉ cần trả lời SYN bằng SYN|ACK, nhưng sẽ bao gồm một số thứ tự TCP được chế tạo đặc biệt để mã hóa địa chỉ IP nguồn và đích, số cổng và thời gian gói tin đã được gửi. Một kết nối hợp pháp sẽ gửi gói ACK của bắt tay ba bước với số thứ tự được chế tạo đặc biệt. Điều này cho phép hệ thống xác minh rằng nó có đã nhận được phản hồi hợp lệ đối với cookie SYN và cho phép kết nối, mặc dù không có SYN tương ứng trong hàng đợi.
* Những kẻ tấn công sử dụng các cuộc tấn công SYN lũ lụt để thực hiện một cuộc tấn công từ chối dịch vụ trên một hệ thống bằng cách gửi nhiều gói SYN mà không hoàn thành quá trình bắt tay ba bước. Điều này sẽ nhanh chóng sử dụng hết các vị trí trong hàng đợi kết nối nửa mở của hạt nhân và ngăn chặn các kết nối hợp pháp từ thành công. SYN cookie cho phép hệ thống tiếp tục chấp nhận các kết nối hợp lệ, ngay cả khi dưới một cuộc tấn công từ chối dịch vụ**.**

**3.3.9 Ensure IPv6 router advertisements are not accepted (Automated)**

* Đảm bảo quảng cáo bộ định tuyến IPv6 không được chấp nhận
* Cài đặt này vô hiệu hóa khả năng chấp nhận quảng cáo bộ định tuyến IPv6 của hệ thống.
* Khuyến nghị rằng các hệ thống không chấp nhận quảng cáo bộ định tuyến vì chúng có thể bị lừa trong việc định tuyến lưu lượng đến các máy bị xâm nhập. Đặt các tuyến cứng trong hệ thống (thường là một tuyến đường mặc định duy nhất đến một bộ định tuyến đáng tin cậy) bảo vệ hệ thống khỏi tuyến đường.

**3.4 Uncommon Network Protocols**

**3.4.1 Ensure DCCP is disabled (Automated)**

* Đảm bảo DCCP bị tắt
* Giao thức kiểm soát tắc nghẽn Datagram (DCCP) là một giao thức tầng vận chuyển hỗ trợ phương tiện truyền thông trực tuyến và điện thoại. DCCP cung cấp một cách để đạt được quyền truy cập vào kiểm soát tắc nghẽn mà không phải thực hiện ở lớp ứng dụng nhưng không cung cấp phân phối không theo trình tự.
* Nếu giao thức không được yêu cầu, không nên cài đặt trình điều khiển để giảm bề mặt tấn công tiềm năng

**3.4.2 Ensure SCTP is disabled (Automated)**

* Đảm bảo SCTP bị tắt
* Stream Control Transmission Protocol (SCTP) là một giao thức tầng vận chuyển được sử dụng để hỗ trợ giao tiếp theo định hướng tin nhắn, với một số luồng tin nhắn trong một sự liên quan. Nó phục vụ một chức năng tương tự như TCP và UDP, kết hợp các tính năng của cả hai. Nó là hướng thông báo như UDP và đảm bảo vận chuyển tin nhắn theo trình tự đáng tin cậy với kiểm soát tắc nghẽn như TCP.
* Nếu giao thức không được sử dụng, bạn không nên tải mô-đun hạt nhân, vô hiệu hóa dịch vụ để giảm bề mặt tấn công tiềm năng.

**3.5 Firewall Configuration**

**3.5.1 Configure firewalld**

**3.5.1.1 Ensure firewalld is installed (Automated)**

* Đảm bảo đã cài đặt tường lửa
* tường lửa là một công cụ quản lý tường lửa cho hệ điều hành Linux. Nó cung cấp tường lửa các tính năng bằng cách hoạt động như một giao diện người dùng cho khung bộ lọc mạng của nhân Linux thông qua iptables phụ trợ hoặc cung cấp các tính năng tường lửa bằng cách hoạt động như một giao diện người dùng cho nhân Linux netfilter framework thông qua tiện ích nftables. tường lửa thay thế iptables làm công cụ quản lý tường lửa mặc định. Sử dụng tiện ích tường lửa để cấu hình tường lửa cho tường lửa ít phức tạp hơn. Tiện ích này rất dễ sử dụng và bao gồm kịch bản trường hợp sử dụng điển hình. FirewallD hỗ trợ cả mạng IPv4 và IPv6 và có thể quản lý các vùng tường lửa riêng biệt với mức độ tin cậy khác nhau như được xác định trong hồ sơ vùng.
* Cần có tiện ích tường lửa để định cấu hình khung bộ lọc mạng của nhân Linux thông qua phụ trợ iptables hoặc nftables. Tường lửa dựa trên máy chủ khung bộ lọc mạng của nhân Linux có thể bảo vệ chống lại các mối đe dọa có nguồn gốc từ bên trong mạng công ty để bao gồm mã di động độc hại và kém phần mềm được cấu hình trên máy chủ

**3.5.1.2 Ensure iptables-services not installed with firewalld (Automated)**

* Đảm bảo dịch vụ iptables không được cài đặt với tường lửa
* Gói dịch vụ iptables chứa iptables.service và ip6tables.service. Các dịch vụ này cho phép quản lý Tường lửa dựa trên máy chủ được cung cấp bởi iptables bưu kiện.
* iptables.service và ip6tables.service vẫn được hỗ trợ và có thể được cài đặt với gói dịch vụ iptables. Chạy cả tường lửa và các dịch vụ có trong gói dịch vụ iptables có thể dẫn đến xung đột

**3.5.1.3 Ensure nftables either not installed or masked with firewalld (Automated)**

* Đảm bảo nftables không được cài đặt hoặc che bằng tường lửa
* nftables là một hệ thống con của nhân Linux cung cấp khả năng lọc và phân loại mạng packets/datagrams/frames và là phiên bản kế thừa của iptables.
* Chạy cả tường lửa và nftables có thể dẫn đến xung đột

**3.5.1.4 Ensure firewalld service enabled and running (Automated)**

* Đảm bảo bật và chạy dịch vụ tường lửa
* tường lửa.service cho phép thực thi các quy tắc tường lửa được định cấu hình thông qua tường lửa
* Đảm bảo rằng firewalld.service đã được bật và đang chạy để thực thi các quy tắc tường lửa cấu hình thông qua tường lửa

**3.5.1.5 Ensure firewalld default zone is set (Automated)**

* Đảm bảo vùng mặc định của tường lửa được đặt
* Vùng tường lửa xác định mức độ tin cậy cho liên kết kết nối, giao diện hoặc địa chỉ nguồn. Đây là mối quan hệ một-nhiều, có nghĩa là một kết nối, giao diện hoặc nguồn chỉ có thể là một phần của một vùng, nhưng một vùng có thể được sử dụng cho nhiều kết nối mạng, giao diện và nguồn.
* Vùng mặc định là vùng được sử dụng cho mọi thứ không rõ ràng buộc/gán cho một khu vực khác.
* Nếu không có vùng nào được gán cho kết nối, giao diện hoặc nguồn, thì chỉ có vùng mặc định được đã sử dụng.
* Vùng mặc định không phải lúc nào cũng được liệt kê là được sử dụng cho giao diện hoặc nguồn vì nó sẽ được sử dụng cho nó một trong hai cách. Điều này phụ thuộc vào người quản lý các giao diện.
* Các kết nối do Trình quản lý mạng xử lý được liệt kê dưới dạng yêu cầu Trình quản lý mạng để thêm liên kết vùng cho giao diện được sử dụng bởi kết nối. Ngoài ra các giao diện dưới sự kiểm soát của dịch vụ mạng cũng được liệt kê vì dịch vụ đó yêu cầu.
* Bởi vì vùng mặc định là vùng được sử dụng cho mọi thứ không rõ ràng bị ràng buộc/gán cho một vùng khác, điều quan trọng là phải đặt vùng mặc định

**3.5.1.6 Ensure network interfaces are assigned to appropriate zone (Manual)**

* Đảm bảo các giao diện mạng được gán cho vùng thích hợp
* vùng tường lửa xác định mức độ tin cậy của các kết nối hoặc giao diện mạng.
* Một giao diện mạng không được gán cho vùng thích hợp có thể cho phép các lỗi không mong muốn hoặc lưu lượng mạng không mong muốn được chấp nhận trên giao diện

**3.5.1.7 Ensure firewalld drops unnecessary services and ports (Manual)**

* Đảm bảo tường lửa loại bỏ các dịch vụ và cổng không cần thiết
* Các dịch vụ và cổng có thể được chấp nhận hoặc từ chối rõ ràng hoặc bị loại bỏ bởi một vùng. Đối với mọi vùng, bạn có thể đặt hành vi mặc định xử lý lưu lượng truy cập đến không được chỉ định thêm. Hành vi như vậy được xác định bằng cách đặt mục tiêu của vùng. có ba tùy chọn - mặc định, ACCEPT, REJECT và DROP.
* ACCEPT - bạn chấp nhận tất cả các gói đến ngoại trừ những gói bị vô hiệu hóa bởi một quy tắc cụ thể.
* REJECT - bạn vô hiệu hóa tất cả các gói đến trừ những gói bạn đã cho phép vào các quy tắc cụ thể và máy nguồn được thông báo về việc từ chối.
* DROP - bạn tắt tất cả các gói đến trừ những gói bạn đã cho phép vào các quy tắc cụ thể và không có thông tin nào được gửi đến máy nguồn.
* Để giảm bề mặt tấn công của hệ thống, tất cả các dịch vụ và cổng phải bị chặn trừ khi yêu cầu

**3.5.2 Configure nftables**

**3.5.2.1 Ensure nftables is installed (Automated)**

* Đảm bảo nftables đã được cài đặt
* nftables cung cấp khung phân loại gói trong nhân mới dựa trên Máy ảo (VM) dành riêng cho mạng và công cụ dòng lệnh không gian người dùng nft mới. nftables tái sử dụng các hệ thống con Netfilter hiện có, chẳng hạn như cơ sở hạ tầng hook hiện có, hệ thống theo dõi kết nối, NAT, hệ thống con xếp hàng và ghi nhật ký không gian người dùng.
* nftables là một hệ thống con của nhân Linux có thể bảo vệ chống lại các mối đe dọa bắt nguồn từ trong mạng công ty để bao gồm mã di động độc hại và cấu hình kém phần mềm trên máy chủ.

**3.5.2.2 Ensure firewalld is either not installed or masked with nftables (Automated)**

* Đảm bảo tường lửa không được cài đặt hoặc che giấu bằng nftables
* tường lửa (Trình quản lý tường lửa động) cung cấp tường lửa được quản lý động với hỗ trợ cho “khu vực” mạng/tường lửa để chỉ định mức độ tin cậy cho mạng và mạng của nó các kết nối, giao diện hoặc nguồn liên quan. Nó có hỗ trợ cho IPv4, IPv6, Ethernet cầu và cũng cho cài đặt tường lửa IPSet. Có sự tách biệt giữa thời gian chạy và tùy chọn cấu hình vĩnh viễn.
* Chạy cả nftables.service và firewalld.service có thể dẫn đến xung đột và kết quả bất ngờ.

**3.5.2.3 Ensure iptables-services not installed with nftables (Automated)**

* Đảm bảo dịch vụ iptables không được cài đặt với nftables
* Gói dịch vụ iptables chứa iptables.service và ip6tables.service. Các dịch vụ này cho phép quản lý Tường lửa dựa trên máy chủ được cung cấp bởi iptables bưu kiện.
* iptables.service và ip6tables.service vẫn được hỗ trợ và có thể được cài đặt với gói dịch vụ iptables. Chạy cả nftables và các dịch vụ có trong gói dịch vụ iptables có thể dẫn đến xung đột

**3.5.2.4 Ensure iptables are flushed with nftables (Manual)**

* Đảm bảo iptables được xóa bằng nftables
* nftables là sự thay thế cho iptables, ip6tables, ebtables và arptables
* Có thể kết hợp iptables và nftables. Tuy nhiên, điều này làm tăng độ phức tạp và cũng là cơ hội để giới thiệu lỗi. Để đơn giản, hãy loại bỏ tất cả các quy tắc iptables và đảm bảo rằng nó không nạp vào

**3.5.2.5 Ensure an nftables table exists (Automated)**

* Đảm bảo tồn tại một bảng nftables
* Bàn giữ dây chuyền. Mỗi bảng chỉ có một họ địa chỉ và chỉ áp dụng cho các gói gia đình này. Bàn có thể có một trong năm họ.
* nftables không có bất kỳ bảng mặc định nào. Không có bảng đang được xây dựng, nftables sẽ không lọc lưu lượng mạng.

**3.5.2.6 Ensure nftables base chains exist (Automated)**

* Đảm bảo chuỗi cơ sở nftables tồn tại
* Chuỗi là nơi chứa các quy tắc. Chúng tồn tại ở hai loại, chuỗi cơ sở và chuỗi thông thường. MỘT chuỗi cơ sở là một điểm vào cho các gói từ ngăn xếp mạng, một chuỗi thông thường có thể được sử dụng làm mục tiêu nhảy và được sử dụng để tổ chức quy tắc tốt hơn.
* Nếu một chuỗi cơ sở không tồn tại với một hook cho đầu vào, chuyển tiếp và xóa, các gói sẽ chảy qua các chuỗi đó sẽ không bị ảnh hưởng bởi nftables.

**3.5.2.7 Ensure nftables loopback traffic is configured (Automated)**

* Đảm bảo lưu lượng truy cập vòng lặp nftables được định cấu hình
* Định cấu hình giao diện loopback để chấp nhận lưu lượng. Định cấu hình tất cả các giao diện khác để từ chối lưu lượng truy cập vào mạng loopback
* Lưu lượng vòng lặp được tạo giữa các quy trình trên máy và thường rất quan trọng đối với hoạt động của hệ thống. Giao diện loopback là nơi duy nhất mà mạng loopback lưu lượng truy cập sẽ được nhìn thấy, tất cả các giao diện khác sẽ bỏ qua lưu lượng truy cập trên mạng này như một biện pháp chống giả mạo.

**3.5.2.8 Ensure nftables outbound and established connections are configured (Manual)**

* Đảm bảo các kết nối gửi đi và thiết lập của nftable được cấu hình
* Định cấu hình quy tắc tường lửa cho các kết nối ra ngoài và thiết lập mới
* Nếu các quy tắc không được áp dụng cho các kết nối gửi đi và kết nối mới được thiết lập, tất cả các gói sẽ được bị loại bỏ bởi chính sách mặc định ngăn chặn việc sử dụng mạng

**3.5.2.9 Ensure nftables default deny firewall policy (Automated)**

* Đảm bảo chính sách tường lửa từ chối mặc định của nftables
* Chính sách chuỗi cơ sở là phán quyết mặc định sẽ được áp dụng cho các gói đến cuối chuôi.
* Có hai chính sách: chấp nhận (Mặc định) và loại bỏ. Nếu chính sách được đặt thành chấp nhận, tường lửa sẽ chấp nhận bất kỳ gói nào không được cấu hình để bị từ chối và gói sẽ tiếp tục đi qua ngăn xếp mạng. Dễ dàng đưa vào danh sách trắng cách sử dụng được chấp nhận hơn là đưa vào danh sách đen cách sử dụng không được chấp nhận

**3.5.2.10 Ensure nftables service is enabled (Automated)**

* Đảm bảo dịch vụ nftables được bật
* Dịch vụ nftables cho phép tải bộ quy tắc nftables trong khi khởi động hoặc bắt đầu từ dịch vụ nftables
* Dịch vụ nftables khôi phục các quy tắc nftables từ các tệp quy tắc được tham chiếu trong /etc/sysconfig/nftables.conf tệp trong khi khởi động hoặc bắt đầu dịch vụ nftables

**3.5.2.11 Ensure nftables rules are permanent (Automated)**

* Đảm bảo quy tắc nftables là vĩnh viễn
* nftables là một hệ thống con của nhân Linux cung cấp khả năng lọc và phân loại mạng packets/datagrams/frames. Dịch vụ nftables đọc tệp /etc/sysconfig/nftables.conf cho tệp nftables hoặc các tệp để đưa vào bộ quy tắc nftables. Bộ quy tắc nftables chứa chuỗi cơ sở đầu vào, chuyển tiếp và đầu ra cho phép mạng lưu lượng cần lọc.
* Các thay đổi đối với bộ quy tắc nftables chỉ ảnh hưởng đến hệ thống trực tiếp, bạn cũng sẽ cần định cấu hình bộ quy tắc nftables để áp dụng khi khởi động

**3.5.3 Configure iptables**

**3.5.3.1 Configure iptables software**

**3.5.3.1.1 Ensure iptables packages are installed (Automated)**

* Đảm bảo các gói iptables được cài đặt
* iptables là một chương trình tiện ích cho phép quản trị viên hệ thống định cấu hình các bảng được cung cấp bởi tường lửa nhân Linux, được triển khai dưới dạng các mô-đun Netfilter khác nhau và chuỗi và quy tắc nó lưu trữ. Các mô-đun và chương trình hạt nhân khác nhau được sử dụng cho các mục đích khác nhau giao thức; iptables áp dụng cho IPv4, ip6tables cho IPv6, arptables cho ARP và ebtables cho khung Ethernet.
* Phương pháp định cấu hình và duy trì các quy tắc tường lửa là cần thiết để định cấu hình Máy chủ Tường lửa dựa trên.

**3.5.3.1.2 Ensure nftables is not installed with iptables (Automated)**

* Đảm bảo nftables không được cài đặt với iptables
* nftables là một hệ thống con của nhân Linux cung cấp khả năng lọc và phân loại mạng packets/datagrams/frames và là phiên bản kế thừa của iptables.
* Chạy cả iptables và nftables có thể dẫn đến xung đột.

**3.5.3.1.3 Ensure firewalld is either not installed or masked with iptables (Automated)**

* Đảm bảo tường lửa không được cài đặt hoặc che bằng iptables
* tường lửa (Trình quản lý tường lửa động) cung cấp tường lửa được quản lý động với hỗ trợ cho “khu vực” mạng/tường lửa để chỉ định mức độ tin cậy cho mạng và mạng của nó các kết nối, giao diện hoặc nguồn liên quan. Nó có hỗ trợ cho IPv4, IPv6, Ethernet cầu và cũng cho cài đặt tường lửa IPSet. Có sự tách biệt giữa thời gian chạy và tùy chọn cấu hình vĩnh viễn.
* Chạy iptables.service và\hoặc ip6tables.service với tường lửa.service có thể dẫn đến xung đột và kết quả không mong muốn.

**3.5.3.2 Configure IPv4 iptables**

**3.5.3.2.1 Ensure iptables loopback traffic is configured (Automated)**

* Đảm bảo lưu lượng truy cập loopback iptables được định cấu hình
* Định cấu hình giao diện loopback để chấp nhận lưu lượng. Định cấu hình tất cả các giao diện khác để từ chối lưu lượng truy cập vào mạng loopback (127.0.0.0/8).
* Lưu lượng vòng lặp được tạo giữa các quy trình trên máy và thường rất quan trọng đối với hoạt động của hệ thống. Giao diện loopback là nơi duy nhất mà mạng loopback (127.0.0.0/8) nên nhìn thấy lưu lượng, tất cả các giao diện khác sẽ bỏ qua lưu lượng trên này mạng như một biện pháp chống giả mạo

**3.5.3.2.2 Ensure iptables outbound and established connections are configured (Manual)**

* Đảm bảo các kết nối iptables outbound và thiết lập được cấu hình
* Định cấu hình các quy tắc tường lửa cho các kết nối ra nước ngoài mới và được thiết lập.
* Nếu các quy tắc không được áp dụng cho hướng đi mới và các kết nối được thiết lập thì tất cả các gói sẽ bị loại bỏ bởi chính sách mặc định ngăn chặn việc sử dụng mạng.

**3.5.3.2.3 Ensure iptables rules exist for all open ports (Automated)**

* Đảm bảo quy tắc iptables tồn tại cho tất cả các cổng đang mở
* Bất kỳ cổng nào đã được mở trên các địa chỉ không phải loopback đều cần các quy tắc tường lửa để quản lý giao thông.
* 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 gói tin đến các cổng này.

**3.5.3.2.4 Ensure iptables default deny firewall policy (Automated)**

* Đảm bảo chính sách tường lửa từ chối mặc định của iptables
* Chính sách từ chối tất cả các kết nối mặc định đảm bảo rằng mọi hoạt động sử dụng mạng chưa được định cấu hình sẽ bị từ chối.
* Với chính sách chấp nhận mặc định, tường lửa sẽ chấp nhận bất kỳ gói nào không được cấu hình thành từ chối. Việc đưa vào danh sách trắng cách sử dụng được chấp nhận sẽ dễ dàng hơn so với việc đưa vào danh sách đen cách sử dụng không thể chấp nhận được.

**3.5.3.2.5 Ensure iptables rules are saved (Automated)**

* Đảm bảo quy tắc iptables được lưu
* Gói dịch vụ iptables bao gồm tệp /etc/sysconfig/iptables. Các quy tắc iptables trong tệp này sẽ được tải bởi iptables.service trong khi khởi động hoặc khi nó được bắt đầu hoặc tải lại.
* Nếu các quy tắc iptables không được lưu và khởi động lại hệ thống xảy ra, các quy tắc iptables sẽ được mất.

**3.5.3.2.6 Ensure iptables is enabled and running (Automated)**

* Đảm bảo iptables được kích hoạt và đang chạy
* iptables.service là một tiện ích để cấu hình và duy trì iptables.
* iptables.service sẽ tải các quy tắc iptables được lưu trong tệp /etc/sysconfig/iptables khi khởi động, nếu không các quy tắc iptables sẽ bị xóa trong quá trình khởi động lại hệ thống.

**3.5.3.3 Configure IPv6 ip6tables**

**3.5.3.3.1 Ensure ip6tables loopback traffic is configured (Automated)**

* Đảm bảo lưu lượng truy cập vòng lặp ip6tables được định cấu hình
* Định cấu hình giao diện loopback để chấp nhận lưu lượng. Định cấu hình tất cả các giao diện khác để từ chối lưu lượng truy cập vào mạng loopback (::1).
* Lưu lượng vòng lặp được tạo giữa các quy trình trên máy và thường rất quan trọng đối với hoạt động của hệ thống. Giao diện loopback là nơi duy nhất mà mạng loopback (::1) lưu lượng sẽ được nhìn thấy, tất cả các giao diện khác sẽ bỏ qua lưu lượng trên mạng này như một biện pháp chống giả mạo

**3.5.3.3.2 Ensure ip6tables outbound and established connections are configured (Manual)**

* Đảm bảo các kết nối ra bên ngoài và thiết lập của ip6tables được cấu hình
* Định cấu hình các quy tắc tường lửa cho các kết nối IPv6 mới và các kết nối IPv6 đã thiết lập.
* Nếu các quy tắc không được áp dụng cho hướng đi mới và các kết nối được thiết lập thì tất cả các gói sẽ bị loại bỏ bởi chính sách mặc định ngăn chặn việc sử dụng mạng

**3.5.3.3.3 Ensure ip6tables firewall rules exist for all open ports (Automated)**

* Đảm bảo các quy tắc tường lửa ip6tables tồn tại cho tất cả các cổng đang mở
* Bất kỳ cổng nào đã được mở trên các địa chỉ không phải loopback đều cần các quy tắc tường lửa để quản lý giao thông.
* 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 gói tin đến các cổng này**.**

**3.5.3.3.4 Ensure ip6tables default deny firewall policy (Automated)**

* Đảm bảo chính sách tường lửa từ chối mặc định của ip6tables
* Chính sách từ chối tất cả các kết nối mặc định đảm bảo rằng mọi hoạt động sử dụng mạng chưa được định cấu hình sẽ bị từ chối.
* Với chính sách chấp nhận mặc định, tường lửa sẽ chấp nhận bất kỳ gói nào không được cấu hình thành từ chối. Dễ dàng đưa vào danh sách trắng cách sử dụng được chấp nhận hơn là đưa vào danh sách đen cách sử dụng không được chấp nhận

**3.5.3.3.5 Ensure ip6tables rules are saved (Automated)**

* Đảm bảo quy tắc ip6tables được lưu
* Gói dịch vụ iptables bao gồm tệp /etc/sysconfig/ip6tables. Các quy tắc ip6tables trong tệp này sẽ được tải bởi ip6tables.service trong khi khởi động hoặc khi nó được bắt đầu hoặc tải lại.
* Nếu quy tắc ip6tables không được lưu và xảy ra khởi động lại hệ thống, quy tắc ip6tables sẽ bị mất.

**3.5.3.3.6 Ensure ip6tables is enabled and running (Automated)**

* Đảm bảo ip6tables được kích hoạt và chạy
* ip6tables.service là một tiện ích để cấu hình và duy trì ip6tables.
* ip6tables.service sẽ tải các quy tắc iptables được lưu trong tệp /etc/sysconfig/ip6tables khi khởi động, nếu không các quy tắc ip6tables sẽ bị xóa trong quá trình khởi động lại hệ thống.

**4 Logging and Auditing**

**4.1 Configure System Accounting (auditd)**

**4.1.1 Ensure auditing is enabled**

**4.1.1.1 Ensure auditd is installed (Automated)**

* Đảm bảo đã cài đặt auditd (Tự động)
* auditd là thành phần không gian người dùng của Hệ thống kiểm tra Linux. Nó chịu trách nhiệm cho ghi hồ sơ kiểm toán vào đĩa
* Việc nắm bắt các sự kiện hệ thống cung cấp cho quản trị viên hệ thống thông tin để cho phép họ để xác định xem có xảy ra truy cập trái phép vào hệ thống của họ hay không.

**4.1.1.2 Ensure auditd service is enabled and running (Automated)**

* Đảm bảo dịch vụ auditd được kích hoạt và chạy (Tự động)
* Bật daemon kiểm toán để ghi lại các sự kiện hệ thống.
* Việc nắm bắt các sự kiện hệ thống cung cấp cho quản trị viên hệ thống thông tin để cho phép họ để xác định xem có xảy ra truy cập trái phép vào hệ thống của họ hay không

**4.1.1.3 Ensure auditing for processes that start prior to auditd is enabled (Automated)**

* Đảm bảo việc kiểm tra các quy trình bắt đầu trước khi kiểm toán được thực hiện đã bật (Tự động)
* Định cấu hình grub để các quy trình có khả năng được kiểm tra có thể được kiểm tra ngay cả khi họ khởi động trước khi khởi động auditd.
* Các sự kiện kiểm tra cần được ghi lại trên các quy trình khởi động trước auditd , để hoạt động độc hại tiềm tàng không thể không bị phát hiện

**4.1.2 Configure Data Retention**

**4.1.2.1 Ensure audit log storage size is configured (Automated)**

* Đảm bảo kích thước lưu trữ nhật ký kiểm tra được định cấu hình (Tự động)
* Định cấu hình kích thước tối đa của tệp nhật ký kiểm tra. Khi nhật ký đạt đến kích thước tối đa, nó sẽ được xoay và một tệp nhật ký mới sẽ được bắt đầu
* Điều quan trọng là xác định kích thước phù hợp cho các tệp nhật ký để chúng không ảnh hưởng đến hệ thống và dữ liệu kiểm toán không bị mất.

**4.1.2.2 Ensure audit logs are not automatically deleted (Automated)**

* Đảm bảo nhật ký kiểm tra không bị xóa tự động (Tự động)
* max\_log\_file\_action xác định cách xử lý tệp nhật ký kiểm tra đạt đến
* Kích thước tệp tối đa. Giá trị của keep\_logs sẽ xoay nhật ký nhưng không bao giờ xóa nhật ký cũ
* Trong bối cảnh bảo mật cao, lợi ích của việc duy trì lịch sử kiểm tra lâu dài vượt quá chi phí của lưu trữ lịch sử kiểm toán

**4.1.2.3 Ensure system is disabled when audit logs are full (Automated)**

* Đảm bảo hệ thống bị tắt khi nhật ký kiểm tra đầy (Tự động)
* Daemon kiểm toán có thể được cấu hình để tạm dừng hệ thống khi nhật ký kiểm toán đầy.
* Trong bối cảnh bảo mật cao, nguy cơ phát hiện truy cập trái phép hoặc không từ chối vượt quá lợi ích của sự sẵn có của hệ thống

**4.1.2.4 Ensure audit\_backlog\_limit is sufficient (Automated)**

* Đảm bảo đủ audit\_backlog\_limit (Tự động)
* Giới hạn tồn đọng có cài đặt mặc định là 64
* Trong quá trình khởi động nếu kiểm toán = 1, thì hồ sơ tồn đọng sẽ chứa 64 bản ghi. Nếu có hơn 64 bản ghi được tạo trong khi khởi động, các bản ghi kiểm toán sẽ bị mất và hoạt động độc hại tiềm ẩn có thể xảy ra không bị phát hiện

**4.1.3 Ensure events that modify date and time information are collected (Automated)**

* Đảm bảo các sự kiện sửa đổi thông tin ngày và giờ được thu thập
* Nắm bắt các sự kiện trong đó ngày và/hoặc thời gian hệ thống đã được sửa đổi. Các thông số trong phần này được đặt để xác định xem adjtimex (điều chỉnh đồng hồ kernel), settimeofday (Đặt thời gian, sử dụng cấu trúc múi giờ và múi giờ) thời gian (sử dụng giây kể từ ngày 1/1/1970) hoặc clock\_settime (cho phép cài đặt một số đồng hồ và bộ hẹn giờ bên trong) các lệnh gọi hệ thống đã được thực thi và luôn ghi một bản ghi kiểm toán vào tệp /var/log/audit.log khi thoát, gắn thẻ các bản ghi với mã định danh "thay đổi thời gian"
* Những thay đổi không mong muốn về ngày và/hoặc thời gian của hệ thống có thể là dấu hiệu của hoạt động độc hại trên hệ thống.

**4.1.4 Ensure events that modify user/group information are collected (Automated)**

* Đảm bảo các sự kiện sửa đổi thông tin người dùng/nhóm được thu thập
* Ghi lại các sự kiện ảnh hưởng đến nhóm , passwd (ID người dùng), shadow và gshadow (mật khẩu) hoặc /etc/security/opasswd (mật khẩu cũ, dựa trên tham số ghi nhớ trong PAM tập tin cấu hình). Các tham số trong phần này sẽ xem các tệp để xem chúng có đã được mở để ghi hoặc đã thay đổi thuộc tính (ví dụ: quyền) và gắn thẻ chúng với mã định danh "danh tính" trong tệp nhật ký kiểm tra.
* Những thay đổi không mong muốn đối với các tệp này có thể là dấu hiệu cho thấy hệ thống đã bị xâm phạm và người dùng trái phép đang cố gắng che giấu các hoạt động của họ hoặc thỏa hiệp các tài khoản bổ sung.

**4.1.5 Ensure events that modify the system's network environment are collected (Automated)**

* Đảm bảo các sự kiện sửa đổi môi trường mạng của hệ thống được thu thập
* Ghi lại các thay đổi đối với tệp môi trường mạng hoặc cuộc gọi hệ thống. Các thông số bên dưới theo dõi sethostname (đặt tên máy chủ hệ thống) hoặc setdomainname (đặt tên hệ thống tên miền) cuộc gọi hệ thống và viết sự kiện kiểm tra khi thoát cuộc gọi hệ thống. Cái khác các tham số giám sát các tệp /etc/issue và /etc/issue.net (thông báo được hiển thị trước khi đăng nhập), /etc/hosts (tệp chứa tên máy chủ và địa chỉ IP được liên kết) và /etc/sysconfig/network (thư mục chứa các tập lệnh giao diện mạng và tập tin cấu hình).
* Theo dõi sethostname và setdomainname sẽ xác định các thay đổi trái phép tiềm ẩn để lưu trữ và tên miền của một hệ thống. Việc thay đổi những tên này có khả năng phá vỡ các tham số bảo mật được đặt dựa trên các tên đó. Tệp /etc/hosts được theo dõi đối với những thay đổi trong tệp có thể cho thấy kẻ xâm nhập trái phép đang cố thay đổi liên kết máy với địa chỉ IP và lừa người dùng và quy trình kết nối với máy ngoài ý muốn. Giám sát /etc/issue và /etc/issue.net là rất quan trọng, vì những kẻ xâm nhập có thể đưa thông tin sai lệch vào các tệp đó và lừa người dùng cung cấp thông tin cho kẻ xâm nhập. Giám sát/etc/sysconfig/mạng rất quan trọng vì nó có thể hiển thị nếu giao diện mạng hoặc tập lệnh đang được sửa đổi theo cách có thể dẫn đến máy trở nên không khả dụng hoặc bị xâm phạm. Tất cả hồ sơ kiểm tra sẽ được gắn thẻ với mã định danh "ngôn ngữ hệ thống."

**4.1.6 Ensure events that modify the system's Mandatory Access Controls are collected (Automated)**

* Đảm bảo các sự kiện sửa đổi Quyền truy cập bắt buộc của hệ thống Kiểm soát được thu thập
* Giám sát các điều khiển truy cập bắt buộc của SELinux. Các thông số bên dưới giám sát bất kỳ ghi quyền truy cập (có khả năng bổ sung, xóa hoặc sửa đổi các tệp trong thư mục) hoặc thuộc tính thay đổi các thư mục /etc/selinux/ và /usr/share/selinux/.
* Các thay đổi đối với tệp trong thư mục /etc/selinux/ và /usr/share/selinux/ có thể chỉ ra rằng một người dùng trái phép đang cố sửa đổi các điều khiển truy cập và thay đổi bảo mật bối cảnh, dẫn đến một sự thỏa hiệp của hệ thống

**4.1.7 Ensure login and logout events are collected (Automated)**

* Đảm bảo các sự kiện đăng nhập và đăng xuất được thu thập
* Giám sát các sự kiện đăng nhập và đăng xuất. Các tham số bên dưới theo dõi các thay đổi đối với các tệp được liên kết với các sự kiện đăng nhập/đăng xuất.
* Tệp /var/log/lastlog duy trì các bản ghi về lần cuối cùng một người dùng thành công đăng nhập.
* Thư mục /var/run/faillock/ duy trì hồ sơ đăng nhập thất bại thông qua mô-đun pam\_faillock.
* Giám sát các sự kiện đăng nhập/đăng xuất có thể cung cấp thông tin cho quản trị viên hệ thống liên quan đến các cuộc tấn công vũ phu đối với thông tin đăng nhập của người dùng.

**4.1.8 Ensure session initiation information is collected (Automated)**

* Đảm bảo thông tin bắt đầu phiên được thu thập
* Giám sát các sự kiện bắt đầu phiên. Các thông số trong phần này theo dõi sự thay đổi của các tập tin liên kết với các sự kiện phiên. Tệp /var/run/utmp theo dõi tất cả người dùng hiện đang đăng nhập. Tất cả các bản ghi kiểm tra sẽ được gắn thẻ với mã định danh "phiên". Theo dõi tệp /var/log/wtmp các sự kiện đăng nhập, đăng xuất, tắt máy và khởi động lại. Tệp /var/log/btmp theo dõi không thành công lần đăng nhập và có thể được đọc bằng cách nhập lệnh /usr/bin/last -f /var/log/btmp . Tất cả các bản ghi kiểm tra sẽ được gắn thẻ với mã định danh "đăng nhập".
* Theo dõi các tệp này để biết các thay đổi có thể cảnh báo quản trị viên hệ thống về các lần đăng nhập xảy ra tại giờ bất thường, có thể cho thấy hoạt động của kẻ xâm nhập (tức là người dùng đăng nhập vào thời điểm khi họ thường không đăng nhập).

**4.1.9 Ensure discretionary access control permission modification events are collected (Automated)**

* Đảm bảo các sự kiện sửa đổi quyền kiểm soát truy cập tùy ý được thu thập
* Theo dõi các thay đổi đối với quyền, thuộc tính, quyền sở hữu và nhóm của tệp. Các thông số trong phần này theo dõi các thay đổi đối với các cuộc gọi hệ thống ảnh hưởng đến quyền và thuộc tính của tệp. Các lệnh gọi hệ thống chmod , fchmod và fchmodat ảnh hưởng đến các quyền được liên kết với tệp. Các các lệnh gọi hệ thống chown , fchown , fchownat và lcown ảnh hưởng đến các thuộc tính nhóm và chủ sở hữu trên một tài liệu. setxattr , lsetxattr , fsetxattr (đặt thuộc tính tệp mở rộng) và removexattr , lremovexattr , fremovexattr (xóa thuộc tính tệp mở rộng) kiểm soát tệp mở rộng thuộc tính. Trong mọi trường hợp, một bản ghi kiểm toán sẽ chỉ được viết cho id người dùng không thuộc hệ thống (auid >=1000) và sẽ bỏ qua các sự kiện Daemon (auid = 4294967295). Tất cả hồ sơ kiểm toán sẽ được được gắn thẻ với mã định danh "perm\_mod."
* Theo dõi các thay đổi trong thuộc tính tệp có thể cảnh báo quản trị viên hệ thống về hoạt động có thể chỉ ra hoạt động của kẻ xâm nhập hoặc vi phạm chính sách.

**4.1.10 Ensure unsuccessful unauthorized file access attempts are collected (Automated)**

* Đảm bảo các nỗ lực truy cập tệp trái phép không thành công thu thập
* Theo dõi các nỗ lực truy cập tệp không thành công. Các tham số dưới đây được liên kết với các lệnh gọi hệ thống kiểm soát việc tạo ( creat ), mở ( open , openat ) và cắt bớt (truncate , ftruncate ) của các tệp. Bản ghi nhật ký kiểm tra sẽ chỉ được ghi nếu người dùng là người dùng không có đặc quyền (auid>=1000), không phải là sự kiện Daemon (auid=4294967295) và nếu hệ thống cuộc gọi trả về EACCES (quyền bị từ chối đối với tệp) hoặc EPERM (một số lệnh vĩnh viễn khác lỗi liên quan đến cuộc gọi hệ thống cụ thể). Tất cả hồ sơ kiểm tra sẽ được gắn thẻ với định danh "truy cập".
* Các nỗ lực mở, tạo hoặc cắt bớt tệp không thành công có thể là dấu hiệu cho thấy một cá nhân hoặc tiến trình đang cố giành quyền truy cập trái phép vào hệ thống

**4.1.11 Ensure use of privileged commands is collected (Automated)**

* Đảm bảo việc sử dụng các lệnh đặc quyền được thu thập
* Giám sát các chương trình đặc quyền (những chương trình có bit setuid và/hoặc setgid được đặt khi thực thi) để xác định xem người dùng không có đặc quyền có đang chạy các lệnh này hay không.
* Việc thực thi các lệnh đặc quyền của người dùng không có đặc quyền có thể là dấu hiệu của ai đó đang cố gắng truy cập trái phép vào hệ thống.

**4.1.12 Ensure successful file system mounts are collected (Automated)**

* Đảm bảo các lần gắn kết hệ thống tệp thành công được thu thập
* Giám sát việc sử dụng cuộc gọi hệ thống gắn kết. Cuộc gọi hệ thống mount (và umount ) điều khiển gắn kết và ngắt kết nối các hệ thống tập tin. Các tham số bên dưới cấu hình hệ thống để tạo bản ghi kiểm tra khi lệnh gọi hệ thống gắn kết được sử dụng bởi người dùng không có đặc quyền
* Việc một người dùng không có đặc quyền gắn hệ thống tệp vào hệ thống là điều rất bất thường. Trong khi theo dõi các lệnh gắn kết cung cấp cho quản trị viên hệ thống bằng chứng rằng phương tiện bên ngoài có thể đã được gắn kết (dựa trên việc xem xét nguồn gốc của giá treo và xác nhận rằng nó một loại phương tiện bên ngoài), nó không chỉ ra một cách thuyết phục rằng dữ liệu đã được xuất sang phương tiện truyền thông. Quản trị viên hệ thống muốn xác định xem dữ liệu đã được xuất hay chưa, cũng sẽ phải theo dõi các cuộc gọi hệ thống mở, tạo và cắt bớt thành công yêu cầu quyền truy cập ghi vào một tệp dưới điểm gắn kết của hệ thống tệp phương tiện bên ngoài. Điều này có thể cho một công bằng dấu hiệu cho thấy một ghi xảy ra. Cách duy nhất để thực sự chứng minh điều đó, là theo dõi thành công ghi vào các phương tiện truyền thông bên ngoài. Theo dõi các cuộc gọi hệ thống ghi có thể nhanh chóng lấp đầy nhật ký kiểm tra và không được khuyến nghị. Khuyến nghị về các tùy chọn cấu hình để theo dõi xuất dữ liệu sang phương tiện nằm ngoài phạm vi của tài liệu này.

**4.1.13 Ensure file deletion events by users are collected (Automated)**

* Đảm bảo các sự kiện xóa tệp của người dùng được thu thập
* Giám sát việc sử dụng các cuộc gọi hệ thống liên quan đến việc xóa hoặc đổi tên tệp và tệp thuộc tính. Tuyên bố cấu hình này thiết lập giám sát cho các cuộc gọi hệ thống sau và gắn thẻ chúng với mã định danh "xóa":
* hủy liên kết - xóa tệp
* hủy liên kết - xóa thuộc tính tệp
* đổi tên - đổi tên một tập tin
* renameat - đổi tên một thuộc tính tập tin
* Theo dõi các cuộc gọi này từ những người dùng không có đặc quyền có thể cung cấp cho quản trị viên hệ thống với bằng chứng cho thấy việc xóa các tệp và thuộc tính tệp không phù hợp liên quan đến tập tin được bảo vệ đang xảy ra. Trong khi tùy chọn kiểm tra này sẽ xem xét tất cả các sự kiện, hệ thống quản trị viên sẽ muốn tìm các tệp đặc quyền cụ thể đang bị xóa hoặc bị thay đổi.

**4.1.14 Ensure changes to system administration scope (sudoers) is collected (Automated)**

* Đảm bảo thay đổi phạm vi quản trị hệ thống (sudoers) là thu thập
* Giám sát thay đổi phạm vi cho quản trị viên hệ thống. Nếu hệ thống đã hoạt động bình thường được định cấu hình để buộc quản trị viên hệ thống phải đăng nhập với tư cách là chính họ trước rồi sử dụng lệnh sudo để thực thi các lệnh đặc quyền, có thể theo dõi các thay đổi trong phạm vi. Tệp /etc/sudoers hoặc một tệp trong thư mục /etc/sudoers.d sẽ được ghi vào khi tập tin hoặc các thuộc tính của nó đã thay đổi.
* Các thay đổi trong tệp /etc/sudoers hoặc một tệp trong thư mục /etc/sudoers.d/ có thể cho biết rằng một thay đổi trái phép đã được thực hiện đối với phạm vi hoạt động của quản trị viên hệ thống.

**4.1.15 Ensure system administrator command executions (sudo) are collected (Automated)**

* Đảm bảo việc thực thi lệnh của quản trị viên hệ thống (sudo) được thu thập
* sudo cung cấp cho người dùng các đặc quyền nâng cao tạm thời để thực hiện các thao tác. giám sát các quản trị viên với các đặc quyền nâng cao tạm thời và (các) thao tác mà họ đã thực hiện.
* tạo nhật ký kiểm tra của quản trị viên với các đặc quyền nâng cao tạm thời và (các) hoạt động mà họ đã thực hiện là cần thiết để báo cáo. Quản trị viên sẽ muốn tương quan các sự kiện được ghi vào đường kiểm tra với các bản ghi được ghi vào sudo logfile để xác minh xem lệnh trái phép đã được thực hiện.

**4.1.16 Ensure kernel module loading and unloading is collected (Automated)**

* Đảm bảo tải và dỡ mô-đun hạt nhân được thu thập
* Giám sát quá trình tải và dỡ các mô-đun hạt nhân. Các chương trình insmod (cài đặt một mô-đun hạt nhân), rmmod (xóa mô-đun hạt nhân) và modprobe (một mô-đun phức tạp hơn chương trình tải và dỡ bỏ các mô-đun, cũng như một số tính năng khác) kiểm soát tải và dỡ các mô-đun. init\_module (tải mô-đun) và delete\_module (xóa mô-đun module) các cuộc gọi hệ thống điều khiển tải và dỡ các mô-đun. Bất kỳ việc thực hiện nào của tải và dỡ bỏ các chương trình mô-đun và các cuộc gọi hệ thống sẽ kích hoạt một bản ghi kiểm tra với một định danh của "mô-đun".
* Giám sát việc sử dụng insmod , rmmod và modprobe có thể cung cấp cho quản trị viên hệ thống với bằng chứng cho thấy một người dùng trái phép đã tải hoặc dỡ một mô-đun hạt nhân, có thể xâm phạm tính bảo mật của hệ thống. Giám sát init\_module và lệnh gọi hệ thống delete\_module sẽ phản ánh người dùng trái phép đang cố sử dụng chương trình khác nhau để tải và dỡ bỏ các mô-đun**.**

**4.1.17 Ensure the audit configuration is immutable (Automated)**

* Đảm bảo cấu hình kiểm tra là bất biến
* Đặt kiểm tra hệ thống để không thể sửa đổi các quy tắc kiểm tra bằng auditctl . Đặt cờ "-e2" buộc kiểm tra được đặt ở chế độ không thay đổi. Các thay đổi kiểm tra chỉ có thể được thực hiện trên hệ thống khởi động lại.
* Ở chế độ không thay đổi, người dùng trái phép không thể thực hiện các thay đổi đối với hệ thống kiểm tra để có khả năng che giấu hoạt động độc hại và sau đó đặt lại các quy tắc kiểm toán. Người dùng sẽ nhất có khả năng thông báo khởi động lại hệ thống và điều đó có thể cảnh báo quản trị viên về nỗ lực thực hiện thay đổi kiểm toán trái phép.

**4.2 Configure Logging**

**4.2.1 Configure rsyslog**

**4.2.1.1 Ensure rsyslog is installed (Automated)**

* Đảm bảo rsyslog được cài đặt
* Phần mềm rsyslog là một sự thay thế được khuyến nghị cho daemon syslogd ban đầu. rsyslog cung cấp các cải tiến so với syslogd, bao gồm:
* truyền nhật ký theo hướng kết nối (tức là TCP)
* Tùy chọn đăng nhập vào các định dạng cơ sở dữ liệu
* Mã hóa dữ liệu nhật ký trên đường đến máy chủ ghi nhật ký trung tâm
* Các cải tiến bảo mật của rsyslog chẳng hạn như truyền theo hướng kết nối (tức là TCP) nhật ký, tùy chọn đăng nhập vào các định dạng cơ sở dữ liệu và mã hóa dữ liệu nhật ký trên đường đến một máy chủ ghi nhật ký trung tâm) biện minh cho việc cài đặt và định cấu hình gói.

**4.2.1.2 Ensure rsyslog Service is enabled and running (Automated)**

* Đảm bảo Dịch vụ rsyslog được bật và đang chạy
* rsyslog cần được bật và đang chạy để thực hiện ghi nhật ký
* Nếu dịch vụ rsyslog không được kích hoạt, hệ thống có thể mặc định là dịch vụ syslogd hoặc thiếu thay vào đó đăng nhập

**4.2.1.3 Ensure rsyslog default file permissions configured (Automated)**

* Đảm bảo quyền truy cập tệp mặc định rsyslog được định cấu hình
* rsyslog sẽ tạo các tệp nhật ký chưa tồn tại trên hệ thống. Cài đặt này kiểm soát những quyền nào sẽ được áp dụng cho các tệp mới được tạo này. Tham số $FileCreateMode chỉ định chế độ tạo tệp mà rsyslogd tạo tập tin mới. Nếu không được chỉ định, giá trị 0644 sẽ được sử dụng.
* Điều quan trọng là phải đảm bảo rằng các tệp nhật ký có quyền chính xác để đảm bảo rằng các tệp nhạy cảm dữ liệu được lưu trữ và bảo vệ.

**4.2.1.4 Ensure logging is configured (Manual)**

* Đảm bảo đăng nhập được cấu hình
* Các tệp /etc/rsyslog.conf và /etc/rsyslog.d/\*.conf chỉ định các quy tắc để ghi nhật ký và những tệp nào sẽ được sử dụng để ghi lại các loại thông báo nhất định.
* Rất nhiều thông tin quan trọng liên quan đến bảo mật được gửi qua rsyslog (ví dụ: thành công và lần thử su thất bại, lần thử đăng nhập thất bại, lần thử đăng nhập root, v.v.)

**4.2.1.5 Ensure rsyslog is configured to send logs to a remote log host (Automated)**

* Đảm bảo rsyslog được định cấu hình để gửi nhật ký đến máy chủ lưu trữ nhật ký từ xa
* Tiện ích rsyslog hỗ trợ khả năng gửi nhật ký mà nó thu thập được tới máy chủ lưu trữ nhật ký từ xa đang chạy syslogd(8) hoặc để nhận tin nhắn từ máy chủ từ xa, giảm chi phí quản trị.
* Lưu trữ dữ liệu nhật ký trên máy chủ từ xa bảo vệ tính toàn vẹn của nhật ký khỏi các cuộc tấn công cục bộ. Nếu một kẻ tấn công giành được quyền truy cập root trên hệ thống cục bộ, họ có thể giả mạo hoặc xóa dữ liệu nhật ký được được lưu trữ trên hệ thống cục bộ

**4.2.1.6 Ensure remote rsyslog messages are only accepted on designated log hosts. (Manual)**

* Đảm bảo các tin nhắn rsyslog từ xa chỉ được chấp nhận trên máy chủ nhật ký được chỉ định
* Theo mặc định, rsyslog không lắng nghe các thông điệp tường trình đến từ các hệ thống từ xa. Các ModLoad yêu cầu rsyslog tải mô-đun imtcp.so để nó có thể nghe qua mạng qua TCP. Tùy chọn InputTCPServerRun hướng dẫn rsyslogd lắng nghe trên cổng TCP đã chỉ định.
* Hướng dẫn trong phần này đảm bảo rằng các máy chủ lưu trữ nhật ký từ xa được định cấu hình để chỉ chấp nhận dữ liệu rsyslog từ các máy chủ trong miền được chỉ định và những hệ thống không được thiết kế để trở thành máy chủ lưu trữ nhật ký không chấp nhận bất kỳ thông báo rsyslog từ xa nào. Điều này cung cấp bảo vệ khỏi dữ liệu nhật ký giả mạo và đảm bảo rằng quản trị viên hệ thống đang xem xét dữ liệu nhật ký hệ thống hoàn chỉnh hợp lý ở một vị trí trung tâm.

**4.2.2 Configure journald**

**4.2.2.1 Ensure journald is configured to send logs to rsyslog (Automated)**

* Đảm bảo rằng journald được định cấu hình để gửi nhật ký tới rsyslog
* Dữ liệu từ journald có thể được lưu trữ trong bộ nhớ dễ bay hơi hoặc được duy trì cục bộ trên máy chủ. Tuy nhiên, các tiện ích tồn tại để chấp nhận xuất nhật ký nhật ký từ xa, sử dụng dịch vụ rsyslog cung cấp một phương tiện nhất quán để thu thập và xuất nhật ký.
* Lưu trữ dữ liệu nhật ký trên máy chủ từ xa bảo vệ tính toàn vẹn của nhật ký khỏi các cuộc tấn công cục bộ. Nếu một kẻ tấn công giành được quyền truy cập root trên hệ thống cục bộ, họ có thể giả mạo hoặc xóa dữ liệu nhật ký được được lưu trữ trên hệ thống cục bộ.

**4.2.2.2 Ensure journald is configured to compress large log files(Automated)**

* Đảm bảo journald được cấu hình để nén các tệp nhật ký lớn
* Hệ thống nhật ký bao gồm khả năng nén các tệp quá lớn để tránh lấp đầy lên hệ thống bằng nhật ký hoặc làm cho nhật ký lớn đến mức khó quản lý.
* Các tệp lớn không nén có thể bất ngờ lấp đầy hệ thống tệp dẫn đến tài nguyên không có sẵn. Nén nhật ký trước khi ghi có thể ngăn hệ thống tệp đột ngột, không mong muốn tác động.

**4.2.2.3 Ensure journald is configured to write logfiles to persistent disk (Automated)**

* Đảm bảo journald được định cấu hình để ghi tệp nhật ký vào đĩa liên tục
* Dữ liệu từ journald có thể được lưu trữ trong bộ nhớ dễ bay hơi hoặc được duy trì cục bộ trên máy chủ. Nhật ký trong bộ nhớ sẽ bị mất khi khởi động lại hệ thống. Bằng cách duy trì các bản ghi vào đĩa cục bộ trên máy chủ họ được bảo vệ khỏi mất mát.
* Việc ghi dữ liệu nhật ký vào đĩa sẽ cung cấp khả năng tái tạo lại các sự kiện mà có thể đã ảnh hưởng đến hoạt động hoặc bảo mật của hệ thống ngay cả sau khi hệ thống gặp sự cố hoặc khởi động lại.

**4.2.3 Ensure permissions on all logfiles are configured (Manual)**

* Đảm bảo quyền trên tất cả các tệp nhật ký được định cấu hình
* Các tệp nhật ký được lưu trữ trong /var/log/ chứa thông tin được ghi từ nhiều dịch vụ trên hệ thống, hoặc trên máy chủ lưu trữ nhật ký khác.
* Điều quan trọng là phải đảm bảo rằng các tệp nhật ký có quyền chính xác để đảm bảo rằng các tệp nhạy cảm dữ liệu được lưu trữ và bảo vệ. Khác/thế giới không nên có khả năng xem này thông tin. Nhóm không được có khả năng sửa đổi thông tin này

**4.2.4 Ensure logrotate is configured (Manual)**

* Đảm bảo logrotate được cấu hình
* Hệ thống bao gồm khả năng luân phiên các tệp nhật ký thường xuyên để tránh làm đầy hệ thống có nhật ký hoặc làm cho nhật ký lớn đến mức khó quản lý. Tập tin /etc/logrotate.d/syslog là tệp cấu hình được sử dụng để xoay các tệp nhật ký được tạo bởi syslog hoặc rsyslog.
* Bằng cách giữ cho các tệp nhật ký nhỏ hơn và dễ quản lý hơn, quản trị viên hệ thống có thể dễ dàng lưu trữ các tệp này vào một hệ thống khác và dành ít thời gian hơn để xem qua tệp nhật ký lớn.

**5 Access, Authentication and Authorization**

**5.1 Configure time-based job schedulers**

**5.1.1 Ensure cron daemon is enabled and running (Automated)**

* Đảm bảo cron daemon được kích hoạt và chạy
* Trình nền cron được sử dụng để thực hiện các công việc hàng loạt trên hệ thống.
* Mặc dù có thể không có công việc của người dùng cần được chạy trên hệ thống, nhưng hệ thống có công việc bảo trì có thể bao gồm giám sát an ninh phải chạy. Nếu một phương pháp khác để lập lịch tác vụ không được sử dụng, cron được sử dụng để thực thi chúng và cần được kích hoạt và chạy.
  + 1. **Ensure permissions on /etc/crontab are configured (Automated)**
* Đảm bảo các quyền trên/etc/crontab được định cấu hình
* Tệp /etc/crontab được cron sử dụng để kiểm soát các công việc của chính nó. Các lệnh trong mục này đảm bảo rằng root là người dùng và chủ sở hữu nhóm của tệp và chỉ chủ sở hữu mới có thể truy cập tập tin.
* Tệp này chứa thông tin về những công việc hệ thống nào được điều hành bởi cron. Viết quyền truy cập vào những các tệp có thể cung cấp cho người dùng không có đặc quyền khả năng nâng cao đặc quyền của họ. Đọc quyền truy cập vào các tệp này có thể cung cấp cho người dùng khả năng hiểu rõ hơn về các công việc hệ thống chạy trên hệ thống và có thể cung cấp cho họ cách để đạt được quyền truy cập đặc quyền trái phép.
  + 1. **Ensure permissions on /etc/cron.hourly are configured (Automated)**
* Đảm bảo các quyền trên /etc/cron.hourly được định cấu hình
* Thư mục này chứa các công việc định kỳ của hệ thống cần chạy hàng giờ. Các tập tin trong thư mục này không thể được thao tác bằng lệnh crontab, mà thay vào đó được chỉnh sửa bởi quản trị viên hệ thống bằng trình soạn thảo văn bản. Các lệnh bên dưới hạn chế đọc/ghi và tìm kiếm quyền truy cập vào thư mục gốc của người dùng và nhóm, ngăn người dùng thông thường truy cập vào thư mục này danh mục.
* Cấp quyền truy cập ghi vào thư mục này cho người dùng không có đặc quyền có thể cung cấp cho họ phương tiện để đạt được các đặc quyền nâng cao trái phép. Cấp quyền truy cập đọc vào thư mục này có thể cung cấp thông tin chi tiết cho người dùng không có đặc quyền về cách đạt được các đặc quyền nâng cao hoặc phá vỡ kiểm soát kiểm toán.
  + 1. **Ensure permissions on /etc/cron.daily are configured (Automated)**
* Đảm bảo các quyền trên /etc/cron.daily được định cấu hình
* Thư mục /etc/cron.daily chứa các công việc định kỳ của hệ thống cần chạy hàng ngày. Các tệp trong thư mục này không thể được thao tác bằng lệnh crontab, nhưng thay vào đó được chỉnh sửa bởi quản trị viên hệ thống bằng trình soạn thảo văn bản. Các lệnh dưới đây hạn chế đọc/ghi và tìm kiếm quyền truy cập vào người dùng và nhóm gốc, ngăn người dùng thông thường khỏi truy cập thư mục này.
* Cấp quyền truy cập ghi vào thư mục này cho người dùng không có đặc quyền có thể cung cấp cho họ phương tiện để đạt được các đặc quyền nâng cao trái phép. Cấp quyền truy cập đọc vào thư mục này có thể cung cấp thông tin chi tiết cho người dùng không có đặc quyền về cách đạt được các đặc quyền nâng cao hoặc phá vỡ kiểm soát kiểm toán.
  + 1. **Ensure permissions on /etc/cron.weekly are configured (Automated)**
* Đảm bảo các quyền trên /etc/cron.weekly được định cấu hình
* Thư mục /etc/cron.weekly chứa các công việc định kỳ của hệ thống cần chạy hàng tuần nền tảng. Các tệp trong thư mục này không thể được thao tác bằng lệnh crontab, nhưng thay vào đó được chỉnh sửa bởi quản trị viên hệ thống bằng trình soạn thảo văn bản. Các lệnh dưới đây hạn chế đọc/ghi và tìm kiếm quyền truy cập vào người dùng và nhóm gốc, ngăn người dùng thông thường khỏi truy cập thư mục này.
* Cấp quyền truy cập ghi vào thư mục này cho người dùng không có đặc quyền có thể cung cấp cho họ phương tiện để đạt được các đặc quyền nâng cao trái phép. Cấp quyền truy cập đọc vào thư mục này có thể cung cấp thông tin chi tiết cho người dùng không có đặc quyền về cách đạt được các đặc quyền nâng cao hoặc phá vỡ kiểm soát kiểm toán.
  + 1. **Ensure permissions on /etc/cron.monthly are configured (Automated)**
* Đảm bảo các quyền trên /etc/cron.monthly được định cấu hình
* Thư mục /etc/cron.monthly chứa các công việc định kỳ của hệ thống cần chạy hàng tháng nền tảng. Các tệp trong thư mục này không thể được thao tác bằng lệnh crontab, nhưng thay vào đó được chỉnh sửa bởi quản trị viên hệ thống bằng trình soạn thảo văn bản. Các lệnh dưới đây hạn chế đọc/ghi và tìm kiếm quyền truy cập vào người dùng và nhóm gốc, ngăn người dùng thông thường khỏi truy cập thư mục này.
* Cấp quyền truy cập ghi vào thư mục này cho người dùng không có đặc quyền có thể cung cấp cho họ phương tiện để đạt được các đặc quyền nâng cao trái phép. Cấp quyền truy cập đọc vào thư mục này có thể cung cấp thông tin chi tiết cho người dùng không có đặc quyền về cách đạt được các đặc quyền nâng cao hoặc phá vỡ kiểm soát kiểm toán.
  + 1. **Ensure permissions on /etc/cron.d are configured (Automated)**
* Đảm bảo các quyền trên /etc/cron.d được định cấu hình
* Thư mục /etc/cron.d/ chứa các công việc định kỳ của hệ thống cần chạy theo cách tương tự đến các công việc hàng giờ, hàng tuần và hàng tháng từ /etc/crontab , nhưng yêu cầu nhiều hơn kiểm soát chi tiết khi chúng chạy Các tập tin trong thư mục này không thể được thao tác bởi lệnh crontab, nhưng thay vào đó được quản trị viên hệ thống chỉnh sửa bằng trình soạn thảo văn bản. Các lệnh bên dưới hạn chế quyền truy cập đọc/ghi và tìm kiếm đối với người dùng và nhóm gốc, ngăn người dùng thông thường truy cập vào thư mục này.
* Cấp quyền truy cập ghi vào thư mục này cho người dùng không có đặc quyền có thể cung cấp cho họ phương tiện để đạt được các đặc quyền nâng cao trái phép. Cấp quyền truy cập đọc vào thư mục này có thể cung cấp thông tin chi tiết cho người dùng không có đặc quyền về cách đạt được các đặc quyền nâng cao hoặc phá vỡ kiểm soát kiểm toán.
  + 1. **Ensure cron is restricted to authorized users (Automated)**
* Đảm bảo cron được giới hạn cho người dùng được ủy quyền
* Nếu cron được cài đặt trong hệ thống, hãy định cấu hình /etc/cron.allow để cho phép người dùng cụ thể sử dụng các dịch vụ này. Nếu /etc/cron.allow không tồn tại, thì /etc/cron.deny sẽ được chọn. Bất kì người dùng không được xác định cụ thể trong các tệp đó được phép sử dụng cron. Bằng cách xóa tệp, chỉ người dùng trong /etc/cron.allow được phép sử dụng cron.
* Trên nhiều hệ thống, chỉ quản trị viên hệ thống mới được phép lên lịch các công việc định kỳ. sử dụng tệp cron.allow để kiểm soát ai có thể chạy các công việc định kỳ thực thi chính sách này. Nó là dễ dàng hơn để quản lý một danh sách cho phép hơn là một danh sách từ chối. Trong danh sách từ chối, bạn có thể thêm ID người dùng vào hệ thống và quên thêm nó vào các tập tin từ chối
  + 1. **Ensure at is restricted to authorized users (Automated)**
* Đảm bảo tại được giới hạn cho người dùng được ủy quyền
* Nếu at được cài đặt trong hệ thống, hãy định cấu hình /etc/at.allow để cho phép người dùng cụ thể sử dụng các dịch vụ. Nếu /etc/at.allow không tồn tại, thì /etc/at.deny sẽ được chọn. Bất kỳ người dùng nào không được xác định cụ thể trong các tệp đó được phép sử dụng tại. Bằng cách xóa tệp, chỉ người dùng trong /etc/at.allow được phép sử dụng at.
* Trên nhiều hệ thống, chỉ quản trị viên hệ thống mới được phép lên lịch công việc. sử dụng tệp at.allow để kiểm soát ai có thể điều hành công việc sẽ thực thi chính sách này. Nó dễ quản lý hơn một danh sách cho phép hơn là một danh sách từ chối. Trong danh sách từ chối, bạn có thể thêm ID người dùng vào hệ thống và quên thêm nó vào các tập tin từ chối.

**5.2 Configure sudo**

**5.2.1 Ensure sudo is installed (Automated)**

* Đảm bảo sudo được cài đặt
* sudo cho phép người dùng được phép thực thi lệnh với tư cách là siêu người dùng hoặc người dùng khác, như được chỉ định bởi chính sách bảo mật. ID người dùng thực (không hiệu quả) của người dùng đang gọi được sử dụng để xác định tên người dùng để truy vấn chính sách bảo mật.
* sudo hỗ trợ kiến ​​trúc plugin cho các chính sách bảo mật và ghi nhật ký đầu vào/đầu ra. Ngày thứ ba các bên có thể phát triển và phân phối các plugin ghi nhật ký I/O và chính sách của riêng họ để hoạt động liền mạch với giao diện người dùng sudo. Chính sách bảo mật mặc định là sudoers, đó là được cấu hình thông qua tệp /etc/sudoers. Chính sách bảo mật xác định đặc quyền nào, nếu có, mà người dùng phải chạy sudo. Chính sách có thể yêu cầu người dùng tự xác thực bằng mật khẩu hoặc xác thực khác cơ chế. Nếu yêu cầu xác thực, sudo sẽ thoát nếu mật khẩu của người dùng không được được nhập trong một giới hạn thời gian có thể định cấu hình. Giới hạn này là chính sách cụ thể.

**5.2.2 Ensure sudo commands use pty (Automated)**

* Đảm bảo các lệnh sudo sử dụng pty
* sudo có thể được cấu hình để chỉ chạy từ pseudo-pty
* Những kẻ tấn công có thể chạy một chương trình độc hại bằng cách sử dụng sudo, chương trình này sẽ lại rẽ nhánh một nền tiến trình vẫn còn ngay cả khi chương trình chính đã thực thi xong. Điều này có thể được giảm thiểu bằng cách định cấu hình sudo để chỉ chạy các lệnh khác từ một pty giả, ghi nhật ký I/O có được bật hay không.

**5.2.3 Ensure sudo log file exists (Automated)**

* Đảm bảo tệp nhật ký sudo tồn tại
* Sudo có thể sử dụng tệp nhật ký tùy chỉnh
* Tệp nhật ký sudo đơn giản hóa việc kiểm tra các lệnh sudo

**5.3 Configure SSH Server**

**5.3.1 Ensure permissions on /etc/ssh/sshd\_config are configured (Automated)**

* Đảm bảo các quyền trên /etc/ssh/sshd\_config được định cấu hình
* Tệp /etc/ssh/sshd\_config chứa thông số kỹ thuật cấu hình cho sshd. Các lệnh bên dưới đặt chủ sở hữu và nhóm của tệp thành gốc.
* Tệp /etc/ssh/sshd\_config cần được bảo vệ khỏi những thay đổi trái phép của người dùng không có đặc quyền.

**5.3.2 Ensure permissions on SSH private host key files are configured (Automated)**

* Đảm bảo quyền trên các tệp khóa máy chủ riêng SSH được định cấu hình
* Khóa riêng SSH là một trong hai tệp được sử dụng trong xác thực khóa chung SSH. trong này phương thức xác thực, Việc sở hữu khóa riêng là bằng chứng nhận dạng. Chỉ có một tư nhân khóa tương ứng với khóa chung sẽ có thể xác thực thành công. tư nhân các khóa cần được lưu trữ và xử lý cẩn thận và không được sao chép khóa riêng được phân phối.
* Nếu người dùng trái phép có được tệp khóa máy chủ SSH riêng tư, thì máy chủ có thể bị mạo danh

**5.3.3 Ensure permissions on SSH public host key files are configured (Automated)**

* Đảm bảo quyền trên các tệp khóa máy chủ công khai SSH được định cấu hình
* Khóa công khai SSH là một trong hai tệp được sử dụng trong xác thực khóa công khai SSH. trong này phương pháp xác thực, khóa công khai là khóa có thể được sử dụng để xác minh chữ ký số được tạo bằng khóa riêng tương ứng. Chỉ một khóa công khai tương ứng với một khóa riêng sẽ có thể xác thực thành công.
* Nếu tệp khóa máy chủ công khai bị sửa đổi bởi người dùng trái phép, dịch vụ SSH có thể bị bị tổn hại

**5.3.4 Ensure SSH access is limited (Automated)**

* Đảm bảo quyền truy cập SSH bị hạn chế
* Có một số tùy chọn có sẵn để giới hạn người dùng và nhóm nào có thể truy cập hệ thống thông qua SSH. Bạn nên tận dụng ít nhất một trong các tùy chọn sau:
* AllowUsers: Biến AllowUsers cung cấp cho quản trị viên hệ thống tùy chọn cho phép người dùng cụ thể ssh vào hệ thống. Danh sách bao gồm không gian tên người dùng riêng biệt. ID người dùng số không được nhận dạng với điều này Biến đổi. Nếu quản trị viên hệ thống muốn hạn chế quyền truy cập của người dùng hơn nữa bằng cách chỉ cho phép người dùng được phép đăng nhập từ một máy chủ cụ thể, mục nhập có thể được chỉ định ở dạng user@host.
* AllowGroups: Biến AllowGroups cung cấp cho quản trị viên hệ thống tùy chọn cho phép các nhóm người dùng cụ thể ssh vào hệ thống. Danh sách bao gồm tên nhóm được phân tách bằng dấu cách. ID nhóm số không được nhận dạng với biến này.
* DenyUsers: Biến DenyUsers cung cấp cho quản trị viên hệ thống tùy chọn từ chối người dùng cụ thể để ssh vào hệ thống. Danh sách bao gồm người dùng được phân tách bằng dấu cách tên. ID người dùng dạng số không được nhận dạng với biến này. Nếu một hệ thống quản trị viên muốn hạn chế quyền truy cập của người dùng hơn nữa bằng cách từ chối cụ thể một quyền truy cập của người dùng từ một máy chủ cụ thể, mục nhập có thể được chỉ định ở dạng người dùng @ máy chủ.
* DenyGroups: Biến DenyGroups cung cấp cho quản trị viên hệ thống tùy chọn từ chối các nhóm người dùng cụ thể để ssh vào hệ thống. Danh sách bao gồm tên nhóm được phân tách bằng dấu cách. ID nhóm số không được nhận dạng với biến này.
* Hạn chế người dùng nào có thể truy cập hệ thống từ xa qua SSH sẽ giúp đảm bảo rằng chỉ người dùng được phép truy cập hệ thống

**5.3.5 Ensure SSH LogLevel is appropriate (Automated)**

* Đảm bảo SSH LogLevel phù hợp
* Mức INFO là mức cơ bản chỉ ghi lại hoạt động đăng nhập của người dùng SSH. Trong nhiều tình huống, chẳng hạn như Phản hồi sự cố, điều quan trọng là phải xác định thời điểm một người dùng cụ thể hoạt động trên một hệ thống. Bản ghi đăng xuất có thể loại bỏ những người dùng đã ngắt kết nối, giúp thu hẹp lĩnh vực. Mức VERBOSE chỉ định rằng hoạt động đăng nhập và đăng xuất cũng như dấu vân tay chính cho bất kỳ Khóa SSH được sử dụng để đăng nhập sẽ được ghi lại. Thông tin này rất quan trọng đối với khóa SSH quản lý, đặc biệt là trong các môi trường kế thừa.
* SSH cung cấp một số cấp độ ghi nhật ký với mức độ chi tiết khác nhau. GỠ LỖI cụ thể là không được đề xuất ngoài việc nghiêm ngặt để gỡ lỗi giao tiếp SSH vì nó cung cấp nhiều dữ liệu đến mức khó xác định thông tin bảo mật quan trọng.

**5.3.6 Ensure SSH X11 forwarding is disabled (Automated)**

* Đảm bảo chuyển tiếp SSH X11 bị tắt
* Tham số X11Forwarding cung cấp khả năng tạo đường hầm cho lưu lượng X11 thông qua một phiên vỏ SSH hiện có để kích hoạt các kết nối đồ họa từ xa.
* Tắt chuyển tiếp X11 trừ khi có yêu cầu vận hành để sử dụng các ứng dụng X11 trực tiếp. Có một rủi ro nhỏ là máy chủ X11 từ xa của người dùng đã đăng nhập qua SSH với chuyển tiếp X11 có thể bị xâm phạm bởi những người dùng khác trên máy chủ X11. Ghi chú rằng ngay cả khi chuyển tiếp X11 bị tắt, người dùng luôn có thể cài đặt chuyển tiếp của riêng họ

**5.3.7 Ensure SSH MaxAuthTries is set to 4 or less (Automated)**

* Đảm bảo SSH MaxAuthTries được đặt thành 4 hoặc ít hơn
* Tham số MaxAuthTries chỉ định số lần thử xác thực tối đa được phép trên mỗi kết nối. Khi số lần đăng nhập thất bại đạt đến một nửa số, lỗi thông báo sẽ được ghi vào tệp nhật ký hệ thống nêu chi tiết lỗi đăng nhập.
* Đặt tham số MaxAuthTries thành một số thấp sẽ giảm thiểu rủi ro thành công các cuộc tấn công vũ phu vào máy chủ SSH. Mặc dù cài đặt được khuyến nghị là 4, hãy đặt số dựa trên chính sách trang web.

**5.3.8 Ensure SSH IgnoreRhosts is enabled (Automated)**

* Đảm bảo SSH IgnoreRhosts được bật
* Tham số IgnoreRhosts chỉ định rằng các tệp .rhosts và .shosts sẽ không được sử dụng trong RhostsRSAAuthentication hoặc HostbasedAuthentication.
* Đặt tham số này buộc người dùng phải nhập mật khẩu khi xác thực bằng ssh.

**5.3.9 Ensure SSH HostbasedAuthentication is disabled (Automated)**

* Đảm bảo SSH HostbasedAuthentication bị tắt
* Tham số HostbasedAuthentication chỉ định xem có cho phép xác thực thông qua máy chủ đáng tin cậy thông qua người dùng .rhosts hoặc /etc/hosts.equiv, cùng với công khai thành công xác thực máy chủ của khách hàng chính. Tùy chọn này chỉ áp dụng cho Giao thức SSH Phiên bản 2.
* Mặc dù các tệp .rhosts không hiệu quả nếu hỗ trợ bị tắt trong /etc/pam.conf, vô hiệu hóa khả năng sử dụng các tệp .rhosts trong SSH cung cấp thêm một lớp bảo vệ.

**5.3.10 Ensure SSH root login is disabled (Automated)**

* Đảm bảo đăng nhập root SSH bị tắt (Tự động)
* Tham số PermitRootLogin chỉ định liệu người dùng root có thể đăng nhập bằng ssh hay không. mặc định là không.
* Không cho phép đăng nhập root qua SSH yêu cầu quản trị viên hệ thống xác thực bằng chính họ tài khoản cá nhân, sau đó nâng cấp lên root thông qua sudo. Điều này lần lượt hạn chế cơ hội không từ chối và cung cấp một dấu vết kiểm tra rõ ràng trong trường hợp xảy ra sự cố bảo mật

**5.3.11 Ensure SSH PermitEmptyPasswords is disabled (Automated)**

* Đảm bảo SSH PermitEmptyPasswords bị tắt
* Tham số PermitEmptyPasswords chỉ định xem máy chủ SSH có cho phép đăng nhập vào tài khoản hay không với chuỗi mật khẩu trống.
* Việc không cho phép truy cập shell từ xa vào các tài khoản có mật khẩu trống sẽ giảm xác suất truy cập trái phép vào hệ thống

**5.3.12 Ensure SSH PermitUserEnvironment is disabled (Automated)**

* Đảm bảo SSH PermitUserEnvironment bị tắt
* Tùy chọn PermitUserEnvironment cho phép người dùng trình bày các tùy chọn môi trường cho trình nền ssh.
* Việc cho phép người dùng khả năng thiết lập các biến môi trường thông qua daemon SSH có thể có khả năng cho phép người dùng bỏ qua các biện pháp kiểm soát bảo mật (ví dụ: đặt đường dẫn thực thi có ssh thực thi các chương trình của Trojan)

**5.3.13 Ensure only strong Ciphers are used (Automated)**

* Đảm bảo chỉ sử dụng Mật mã mạnh
* Biến này giới hạn mật mã mà SSH có thể sử dụng trong quá trình giao tiếp.
* Không thể dựa vào các mật mã yếu được sử dụng để xác thực mô-đun mật mã để cung cấp tính bảo mật hoặc tính toàn vẹn và dữ liệu hệ thống có thể bị xâm phạm.
* Các mật mã DES, Triple DES và Blowfish, như được sử dụng trong SSH, có giới hạn ngày sinh là khoảng bốn tỷ khối, giúp kẻ tấn công từ xa dễ dàng hơn có được dữ liệu văn bản rõ ràng thông qua một cuộc tấn công sinh nhật đối với phiên được mã hóa trong thời gian dài, hay còn gọi là cuộc tấn công "Sweet32"
* Thuật toán RC4, như được sử dụng trong giao thức TLS và giao thức SSL, không hoạt động đúng kết hợp dữ liệu trạng thái với dữ liệu chính trong giai đoạn khởi tạo, làm cho nó dễ dàng hơn cho những kẻ tấn công từ xa để tiến hành các cuộc tấn công khôi phục văn bản gốc đối với ban đầu byte của luồng bằng cách đánh hơi lưu lượng mạng đôi khi dựa vào các khóa bị ảnh hưởng bởi Điểm yếu bất biến, sau đó sử dụng cách tiếp cận vũ phu liên quan đến LSB các giá trị, còn gọi là vấn đề "Bar Mitzvah"
* Mật khẩu được sử dụng trong phiên SSH được mã hóa bằng RC4 có thể được khôi phục bằng cách kẻ tấn công có thể nắm bắt và phát lại phiên
* Xử lý lỗi trong giao thức SSH; Máy khách và Máy chủ, khi sử dụng mật mã khối thuật toán ở chế độ Cipher Block Chaining (CBC), giúp điều khiển từ xa dễ dàng hơn những kẻ tấn công để khôi phục một số dữ liệu văn bản gốc từ một khối bản mã tùy ý trong phiên SSH qua các vectơ không xác định

**5.3.14 Ensure only strong MAC algorithms are used (Automated)**

* Đảm bảo chỉ sử dụng các thuật toán MAC mạnh
* Biến này Chỉ định các thuật toán MAC (mã xác thực thông báo) có sẵn. Các Thuật toán MAC được sử dụng trong giao thức phiên bản 2 để bảo vệ tính toàn vẹn của dữ liệu. Nhiều các thuật toán phải được phân tách bằng dấu phẩy.
* Các thuật toán MAC MD5 và 96 bit được coi là yếu và đã được chứng minh là tăng khả năng khai thác trong các cuộc tấn công hạ cấp SSH. Các thuật toán yếu tiếp tục có rất nhiều sự chú ý như một điểm yếu có thể được khai thác với sức mạnh tính toán mở rộng. MỘT kẻ tấn công phá vỡ thuật toán có thể lợi dụng vị trí MiTM để giải mã Đường hầm SSH và nắm bắt thông tin và thông tin đăng nhập

**5.3.15 Ensure only strong Key Exchange algorithms are used (Automated)**

* Đảm bảo chỉ sử dụng các thuật toán Trao đổi khóa mạnh
* Trao đổi khóa là bất kỳ phương pháp nào trong mật mã mà theo đó các khóa mật mã được trao đổi giữa hai bên, cho phép sử dụng thuật toán mật mã. Nếu người gửi và người nhận muốn trao đổi tin nhắn được mã hóa, mỗi người phải được trang bị để mã hóa tin nhắn đã gửi và giải mã tin nhắn nhận được
* Các phương pháp trao đổi khóa được coi là yếu nên bị loại bỏ. Trao đổi khóa phương pháp có thể yếu vì sử dụng quá ít bit hoặc thuật toán băm được xem xét quá yếu. Sử dụng các thuật toán yếu có thể khiến các kết nối bị tấn công trung gian

**5.3.16 Ensure SSH Idle Timeout Interval is configured (Automated)**

* Đảm bảo SSH Idle Timeout Interval được cấu hình
* Hai tùy chọn ClientAliveInterval và ClientAliveCountMax kiểm soát thời gian chờ của phiên ssh.
* ClientAliveInterval đặt khoảng thời gian chờ tính bằng giây sau khoảng thời gian đó nếu không có dữ liệu được nhận từ máy khách, sshd sẽ gửi một tin nhắn thông qua mã hóa kênh để yêu cầu phản hồi từ khách hàng. Mặc định là 0, cho biết rằng những tin nhắn sẽ không được gửi đến khách hàng.
* ClientAliveCountMax đặt số lượng tin nhắn còn sống của khách hàng có thể được gửi mà không cần sshd nhận lại bất kỳ tin nhắn nào từ máy khách. Nếu ngưỡng này là đạt được trong khi tin nhắn còn sống của máy khách đang được gửi, sshd sẽ ngắt kết nối máy khách, chấm dứt phiên làm việc. Giá trị mặc định là 3. Tin nhắn còn sống của khách hàng được gửi qua kênh được mã hóa.Đặt ClientAliveCountMax thành 0 sẽ tắt kết nối
* Không có giá trị thời gian chờ kết hợp với kết nối có thể cho phép người dùng trái phép quyền truy cập vào phiên ssh của người dùng khác (ví dụ: người dùng rời khỏi máy tính của họ và không khóa màn hình). Đặt giá trị thời gian chờ sẽ giảm rủi ro này.
* Cài đặt ClientAliveInterval được khuyến nghị không quá 900 giây (15 phút)
* Cài đặt ClientAliveCountMax được khuyến nghị là 0
* Ở khoảng thời gian 15 phút, nếu phiên ssh không hoạt động, phiên sẽ chấm dứt.

**5.3.17 Ensure SSH LoginGraceTime is set to one minute or less (Automated)**

* Đảm bảo Đăng nhập SSHGraceTime được đặt thành một phút hoặc ít hơn
* Tham số LoginGraceTime chỉ định thời gian cho phép xác thực thành công đối với máy chủ SSH. Thời gian Gia hạn càng dài thì càng có nhiều kết nối không được xác thực mở có thể tồn tại. Giống như các kiểm soát phiên khác trong phiên này, Thời gian gia hạn sẽ được giới hạn ở giới hạn tổ chức thích hợp để đảm bảo dịch vụ có sẵn cho truy cập cần thiết.
* Đặt tham số LoginGraceTime thành một số thấp sẽ giảm thiểu rủi ro thành công các cuộc tấn công vũ phu vào máy chủ SSH. Nó cũng sẽ giới hạn số lượng đồng thời kết nối không được xác thực Trong khi cài đặt được đề xuất là 60 giây (1 phút), hãy đặt số lượng dựa trên chính sách trang web

**5.3.18 Ensure SSH warning banner is configured (Automated)**

* Đảm bảo biểu ngữ cảnh báo SSH được định cấu hình
* Tham số Banner chỉ định một tệp có nội dung phải được gửi tới người dùng từ xa trước khi xác thực được cho phép. Theo mặc định, không có biểu ngữ nào được hiển thị.
* Biểu ngữ được sử dụng để cảnh báo người dùng kết nối về chính sách của trang web cụ thể liên quan đến sự liên quan. Trình bày một thông báo cảnh báo trước khi đăng nhập người dùng bình thường có thể hỗ trợ truy tố những kẻ xâm phạm hệ thống máy tính.

**5.3.19 Ensure SSH PAM is enabled (Automated)**

* Đảm bảo SSH PAM được bật
* UsePAM Bật giao diện Mô-đun xác thực có thể cắm. Nếu được đặt thành “có”, điều này sẽ bật xác thực PAM bằng ChallengeResponseAuthentication và PasswordAuthentication ngoài tài khoản PAM và xử lý mô-đun phiên cho tất cả các loại xác thực
* Khi usePAM được đặt thành có, PAM sẽ chạy đúng loại tài khoản và phiên. Đây là quan trọng nếu bạn muốn hạn chế quyền truy cập vào các dịch vụ dựa trên IP, thời gian hoặc các yếu tố khác của tài khoản. Ngoài ra, bạn có thể đảm bảo người dùng kế thừa các biến môi trường nhất định khi đăng nhập hoặc không cho phép truy cập vào máy chủ

**5.3.20 Ensure SSH AllowTcpForwarding is disabled (Automated)**

* Đảm bảo SSH AllowTcpForwarding bị tắt
* Chuyển tiếp cổng SSH là một cơ chế trong SSH để tạo đường hầm cho các cổng ứng dụng từ máy khách đến máy chủ hoặc máy chủ đến máy khách. Nó có thể được sử dụng để thêm mã hóa vào di sản ứng dụng, đi qua tường lửa và một số quản trị viên hệ thống và chuyên gia CNTT sử dụng nó để mở các cửa hậu vào mạng nội bộ từ các máy ở nhà của họ
* Việc bật tính năng chuyển tiếp cổng có thể khiến tổ chức gặp rủi ro bảo mật và cửa hậu. Các kết nối SSH được bảo vệ bằng mã hóa mạnh. Điều này làm cho nội dung của họ vô hình cho hầu hết các giải pháp giám sát mạng và lọc lưu lượng được triển khai. Sự tàng hình này mang tiềm ẩn rủi ro đáng kể nếu nó được sử dụng cho các mục đích xấu như đánh cắp dữ liệu. Tội phạm mạng hoặc phần mềm độc hại có thể khai thác SSH để che giấu thông tin liên lạc trái phép của chúng, hoặc để lọc dữ liệu bị đánh cắp khỏi mạng mục tiêu

**5.3.21 Ensure SSH MaxStartups is configured (Automated)**

* Đảm bảo SSH MaxStartups được định cấu hình
* Tham số MaxStartups chỉ định số lượng tối đa đồng thời không được xác thực kết nối với daemon SSH.
* Để bảo vệ hệ thống khỏi bị từ chối dịch vụ do có nhiều xác thực đang chờ xử lý nỗ lực kết nối, hãy sử dụng chức năng giới hạn tốc độ của MaxStartups để bảo vệ tính khả dụng của đăng nhập sshd và ngăn không cho daemon áp đảo

**5.3.22 Ensure SSH MaxSessions is limited (Automated)**

* Đảm bảo SSH MaxSessions bị giới hạn
* Tham số MaxSessions Chỉ định số phiên mở tối đa được phép mỗi kết nối mạng.
* Để bảo vệ hệ thống khỏi bị từ chối dịch vụ do có nhiều phiên đồng thời, sử dụng chức năng giới hạn tốc độ của MaxSessions để bảo vệ tính khả dụng của thông tin đăng nhập sshd và ngăn chặn áp đảo daemon.

**5.4 Configure PAM**

**5.4.1 Ensure password creation requirements are configured (Automated)**

* Đảm bảo các yêu cầu tạo mật khẩu được cấu hình
* Mô-đun pam\_pwquality.so kiểm tra độ mạnh của mật khẩu. Nó thực hiện kiểm tra như vậy vì đảm bảo mật khẩu không phải là một từ trong từ điển, nó có độ dài nhất định, chứa hỗn hợp ký tự (ví dụ: bảng chữ cái, số, khác) và hơn thế nữa. Sau đây là các định nghĩa về tùy chọn pam\_pwquality.so. Các tùy chọn sau được đặt trong tệp /etc/security/pwquality.conf:
* Độ dài mật khẩu: minlen = 14 - mật khẩu phải từ 14 ký tự trở lên
* Độ phức tạp của mật khẩu:
* minclass = 4 - Số lượng tối thiểu các lớp ký tự cần thiết cho phiên bản mới mật khẩu (chữ số, chữ hoa, chữ thường, những người khác)

HOẶC

* dcredit = -1 - cung cấp ít nhất một chữ số
* ucredit = -1 - cung cấp ít nhất một ký tự viết hoa
* ocredit = -1 - cung cấp ít nhất một ký tự đặc biệt
* lcredit = -1 - cung cấp ít nhất một ký tự chữ thường
* Phần sau đây được đặt trong các tệp /etc/pam.d/password-auth và /etc/pam.d/system-auth
* try\_first\_pass - truy xuất mật khẩu từ mô-đun PAM xếp chồng lên nhau trước đó. Nếu như không khả dụng, sau đó nhắc người dùng nhập mật khẩu.
* retry=3 - Cho phép 3 lần thử trước khi gửi lại lỗi.
* Các cài đặt được hiển thị ở trên là một chính sách có thể. Thay đổi các giá trị này để phù hợp với của bạn chính sách mật khẩu của tổ chức riêng.
* Mật khẩu mạnh và số lần thử hạn chế trước khi khóa tài khoản bảo vệ hệ thống khỏi bị hack thông qua các phương pháp vũ phu

**5.4.2 Ensure lockout for failed password attempts is configured (Automated)**

* Đảm bảo khóa cho các lần thử mật khẩu không thành công được định cấu hình
* Khóa người dùng sau n lần đăng nhập liên tiếp không thành công. Các cài đặt này thường được định cấu hình với mô-đun pam\_faillock.so. Một số môi trường có thể tiếp tục sử dụng mô-đun pam\_tally2.so, trong đó phương thức cũ hơn này có thể đơn giản hóa tự động hóa trong môi trường hỗn hợp. Đặt số khóa trong từ chối = thành chính sách có hiệu lực tại trang web của bạn. unlock\_time=\_n\_ là số giây tài khoản vẫn bị khóa sau số lần các nỗ lực được định cấu hình trong deny=\_n\_ đã được đáp ứng.
* Khóa ID người dùng sau n lần đăng nhập liên tiếp không thành công sẽ giảm thiểu bạo lực mật khẩu tấn công vào hệ thống của bạn

**5.4.3 Ensure password hashing algorithm is SHA-512 (Automated)**

* Đảm bảo thuật toán băm mật khẩu là SHA-512
* Các lệnh bên dưới thay đổi mã hóa mật khẩu từ md5 thành sha512 (mạnh hơn nhiều thuật toán băm). Tất cả các tài khoản hiện có sẽ cần thực hiện thay đổi mật khẩu thành nâng cấp các giá trị băm được lưu trữ lên thuật toán mới.
* Thuật toán SHA-512 cung cấp khả năng băm mạnh hơn nhiều so với MD5, do đó cung cấp bảo vệ bổ sung cho hệ thống bằng cách tăng mức độ nỗ lực cho kẻ tấn công để xác định thành công mật khẩu

**5.4.4 Ensure password reuse is limited (Automated)**

* Đảm bảo việc sử dụng lại mật khẩu bị hạn chế
* Tệp /etc/security/opasswd lưu trữ mật khẩu cũ của người dùng và có thể được kiểm tra để đảm bảo rằng người dùng không tái chế mật khẩu gần đây.
* Buộc người dùng không sử dụng lại 5 mật khẩu trước đây của họ khiến kẻ tấn công ít có khả năng có khả năng đoán mật khẩu.

**5.5 User Accounts and Environment**

**5.5.1 Set Shadow Password Suite Parameters**

**5.5.1.1 Ensure password expiration is 365 days or less (Automated)**

* Đảm bảo mật khẩu hết hạn từ 365 ngày trở xuống
* Tham số PASS\_MAX\_DAYS trong /etc/login.defs cho phép quản trị viên buộc mật khẩu hết hạn sau khi đạt đến độ tuổi xác định. Đó là khuyến cáo rằng Tham số PASS\_MAX\_DAYS được đặt nhỏ hơn hoặc bằng 365 ngày.
* Cửa sổ cơ hội cho kẻ tấn công tận dụng thông tin đăng nhập bị xâm phạm thông qua tấn công vũ phu, sử dụng thông tin đăng nhập đã bị xâm phạm hoặc lấy thông tin đăng nhập bằng cách các phương tiện khác, có thể bị giới hạn bởi tuổi của mật khẩu. Vì vậy, giảm tối đa tuổi của mật khẩu cũng có thể làm giảm cơ hội của kẻ tấn công. Yêu cầu thay đổi mật khẩu giúp giảm thiểu rủi ro do bảo mật kém thực hành sử dụng mật khẩu cho nhiều tài khoản và triển khai kém các chính sách thay đổi trách nhiệm và chuyển giao trách nhiệm. Điều này không nên được coi là một thay thế cho việc thực hiện đúng các chính sách và thông lệ này.

**5.5.1.2 Ensure minimum days between password changes is configured (Automated)**

* Đảm bảo số ngày tối thiểu giữa các lần thay đổi mật khẩu được định cấu hình
* Tham số PASS\_MIN\_DAYS trong /etc/login.defs cho phép quản trị viên ngăn người dùng thay đổi mật khẩu của họ cho đến khi một số ngày tối thiểu đã trôi qua kể từ khi lần trước người dùng đã thay đổi mật khẩu của họ. Bạn nên PASS\_MIN\_DAYS tham số được đặt thành 1 hoặc nhiều ngày.
* Bằng cách hạn chế tần suất thay đổi mật khẩu, quản trị viên có thể ngăn người dùng liên tục thay đổi mật khẩu của họ nhằm tránh các biện pháp kiểm soát sử dụng lại mật khẩu

**5.5.1.3 Ensure password expiration warning days is 7 or more (Automated)**

* Đảm bảo ngày cảnh báo hết hạn mật khẩu là 7 hoặc nhiều hơn
* Tham số PASS\_WARN\_AGE trong /etc/login.defs cho phép quản trị viên thông báo cho người dùng rằng mật khẩu của họ sẽ hết hạn sau một số ngày xác định. Đó là khuyến cáo rằng Tham số PASS\_WARN\_AGE được đặt thành 7 ngày trở lên.
* Cung cấp cảnh báo trước rằng mật khẩu sẽ hết hạn giúp người dùng có thời gian suy nghĩ một mật khẩu an toàn. Người dùng không biết có thể chọn một mật khẩu đơn giản hoặc viết nó ra nơi nó có thể được phát hiện.

**5.5.1.4 Ensure inactive password lock is 30 days or less (Automated)**

* Đảm bảo khóa mật khẩu không hoạt động là 30 ngày hoặc ít hơn
* Tài khoản người dùng không hoạt động trong một khoảng thời gian nhất định có thể được tự động tàn tật. Khuyến nghị rằng các tài khoản không hoạt động trong 30 ngày sau mật khẩu hết hạn bị vô hiệu hóa.
* Tài khoản không hoạt động gây ra mối đe dọa đối với bảo mật hệ thống do người dùng không đăng nhập vào thông báo các lần đăng nhập không thành công hoặc các điểm bất thường khác.

**5.5.1.5 Ensure all users last password change date is in the past (Automated)**

* Đảm bảo tất cả người dùng ngày thay đổi mật khẩu cuối cùng là trong quá khứ
* Tất cả người dùng phải có ngày thay đổi mật khẩu trong quá khứ.
* Nếu người dùng ghi lại ngày thay đổi mật khẩu trong tương lai thì họ có thể bỏ qua bất kỳ thiết lập nào hết hạn mật khẩu.

**5.5.2 Ensure system accounts are secured (Automated)**

* Đảm bảo tài khoản hệ thống được bảo mật
* Có một số tài khoản được cung cấp với hầu hết các bản phân phối được sử dụng để quản lý các ứng dụng và không nhằm mục đích cung cấp trình bao tương tác.
* Điều quan trọng là đảm bảo rằng các tài khoản không được người dùng thông thường sử dụng bị ngăn không cho sử dụng để cung cấp lớp vỏ tương tác. Theo mặc định, hầu hết các bản phân phối đặt trường mật khẩu cho các tài khoản này thành một chuỗi không hợp lệ, nhưng nó cũng được khuyến nghị rằng trường trình bao trong tệp mật khẩu được đặt thành trình bao nologin. Điều này ngăn cản việc tài khoản có khả năng được sử dụng để chạy bất kỳ lệnh nào

**5.5.3 Ensure default group for the root account is GID 0 (Automated)**

* Đảm bảo nhóm mặc định cho tài khoản gốc là GID 0
* Lệnh usermod có thể được sử dụng để chỉ định người dùng root thuộc nhóm nào. Cái này ảnh hưởng đến quyền của các tệp được tạo bởi người dùng root.
* Sử dụng GID 0 cho tài khoản root giúp ngăn chặn vô tình các tệp do root sở hữu có thể truy cập được đối với người dùng không có đặc quyền

**5.5.4 Ensure default user shell timeout is configured (Automated)**

* Đảm bảo thời gian chờ vỏ người dùng mặc định được định cấu hình
* TMOUT là cài đặt môi trường xác định thời gian chờ của shell tính bằng giây.
* TMOUT=n - Đặt thời gian chờ trình bao thành n giây. Cài đặt TMOUT=0 vô hiệu hóa hết giờ.
* TMOUT chỉ đọc- Đặt biến môi trường TMOUT là chỉ đọc, ngăn sửa đổi không mong muốn trong thời gian chạy.
* xuất TMOUT - xuất biến TMOUT
* Tệp cấu hình toàn hệ thống Shell:
* /etc/profile - được sử dụng để đặt các biến môi trường trên toàn hệ thống trên shell của người dùng. Tuy nhiên, các biến đôi khi giống với các biến trong .bash\_profile tệp này được sử dụng để đặt PATH hoặc PS1 ban đầu cho tất cả người dùng shell của hệ thống. la Duy nhât được thực thi đối với shell đăng nhập tương tác hoặc shell được thực thi với –login tham số.
* /etc/profile.d - /etc/profile sẽ thực thi các tập lệnh bên trong /etc/profile.d/\*.sh. Bạn nên đặt cấu hình của mình trong trình bao tập lệnh trong /etc/profile.d để đặt các biến môi trường trên toàn hệ thống của riêng bạn.
* /etc/bashrc - Phiên bản toàn hệ thống của .bashrc. Trong các bản phân phối có nguồn gốc từ Fedora, etc/bashrc cũng gọi /etc/profile.d/\*.sh nếu shell không đăng nhập, nhưng chuyển hướng đầu ra thành /dev/null nếu không tương tác. Chỉ được thực hiện cho các hệ vỏ tương tác hoặc nếu BASH\_ENV được đặt thành /etc/bashrc.
* Đặt giá trị thời gian chờ sẽ giảm cơ hội cho người dùng truy cập trái phép vào phiên trình bao của người dùng khác không được giám sát. Nó cũng kết thúc phiên không hoạt động và giải phóng các tài nguyên được liên kết với phiên đó.

**5.5.5 Ensure default user umask is configured (Automated)**

* Đảm bảo ô người dùng mặc định được định cấu hình
* Mặt nạ chế độ tạo tệp người dùng (umask) được sử dụng để xác định quyền đối với tệp mới thư mục và tập tin đã tạo. Trong Linux, các quyền mặc định cho mọi quyền mới được tạo thư mục là 0777 (rwxrwxrwx) và đối với bất kỳ tệp mới tạo nào là 0666 (rw-rw-rw-). Các umask sửa đổi các quyền mặc định của Linux bằng cách hạn chế (che giấu) các quyền này. Ô không chỉ đơn giản là bị trừ mà được xử lý theo từng bit. Các bit được đặt trong ô là xóa trong chế độ tập tin kết quả.
* umask có thể được đặt bằng giá trị bát phân hoặc tượng trưng:
* Giá trị bát phân (Số) - Được biểu thị bằng ba hoặc bốn chữ số. tức là ô 0027 hoặc ô 027. Nếu sử dụng ô có bốn chữ số, chữ số đầu tiên sẽ bị bỏ qua. Phần còn lại ba chữ số ảnh hưởng đến các quyền kết quả cho người dùng, nhóm và thế giới/khác tương ứng.
* Giá trị tượng trưng - Được biểu thị bằng danh sách được phân tách bằng dấu phẩy cho Người dùng u, nhóm g và thế giới/khác o. Các quyền được liệt kê không bị che bởi ô. tức là một ô được đặt bởi umask u=rwx,g=rx,o= là tương đương Tượng trưng của umask Bát phân 027. Cái này umask sẽ đặt một thư mục mới được tạo với chế độ tệp drwxr-x--- và một thư mục mới tệp đã tạo với chế độ tệp rw-r-----.
* Ô mặc định có thể được đặt để sử dụng mô-đun pam\_umask hoặc trong System Wide Shell Tập tin cấu hình. Người dùng tạo các thư mục hoặc tệp có toàn quyền quyết định thay đổi quyền thông qua lệnh chmod hoặc chọn một ô mặc định khác bằng cách thêm lệnh umask vào Tệp cấu hình Shell của người dùng, ( .bash\_profile hoặc .bashrc), trong thư mục chính của họ
* Đặt ô mặc định:
* mô-đun pam\_umask:
* sẽ đặt ô theo mặc định của hệ thống trong /etc/login.defs và cài đặt người dùng, giải quyết vấn đề cài đặt ô khác nhau với các shell, trình quản lý hiển thị, phiên từ xa, v.v.
* Giá trị umask=<mask> trong tệp /etc/login.defs được hiểu là Octal
* Đặt USERGROUPS\_ENAB thành yes trong /etc/login.defs (mặc định): sẽ cho phép cài đặt các bit nhóm ô giống như chủ sở hữu chút ít. (ví dụ: 022 -> 002, 077 -> 007) đối với người dùng không root, nếu uid giống với gid và tên người dùng giống với <nhóm chính tên>; userdel sẽ xóa nhóm của người dùng nếu nó không còn thành viên nào nữa, và useradd sẽ mặc định tạo một nhóm với tên của người dùng
* Tệp cấu hình Shell Wide Shell:
* /etc/profile - được sử dụng để đặt các biến môi trường trên toàn hệ thống cho người dùng vỏ sò. Các biến đôi khi là những biến giống nhau trong .bash\_profile, tuy nhiên tệp này được sử dụng để đặt PATH hoặc PS1 ban đầu cho tất cả người dùng shell của hệ thống. chỉ được thực thi đối với shell đăng nhập tương tác hoặc shell được thực thi với tham số --login.
* /etc/profile.d - /etc/profile sẽ thực thi các tập lệnh bên trong /etc/profile.d/\*.sh. Bạn nên đặt cấu hình của mình trong một tập lệnh shell trong /etc/profile.d để đặt toàn bộ hệ thống của riêng bạn biến môi trường.
* /etc/bashrc - Phiên bản toàn hệ thống của .bashrc. Trong Fedora có nguồn gốc bản phân phối, etc/bashrc cũng gọi /etc/profile.d/\*.sh nếu shell không đăng nhập, nhưng chuyển hướng đầu ra thành/dev/null nếu không tương tác. Chỉ được thực hiện cho shell tương tác hoặc nếu BASH\_ENV được đặt thành /etc/bashrc
* Tệp cấu hình Shell của người dùng:
* ~/.bash\_profile - Được thực thi để định cấu hình trình bao của bạn trước lệnh ban đầu lời nhắc. Chỉ được đọc bởi vỏ đăng nhập.
* ~/.bashrc - Được thực thi cho shell tương tác. chỉ được đọc bởi một shell đó là cả hai tương tác và không đăng nhập
* Đặt giá trị mặc định an toàn cho ô đảm bảo rằng người dùng đưa ra lựa chọn có ý thức về quyền tập tin của họ. Giá trị ô cho phép có thể dẫn đến các thư mục hoặc tệp có quá nhiều quyền có thể được đọc và/hoặc ghi bởi người dùng trái phép
  1. **Ensure root login is restricted to system console (Manual)**
* Đảm bảo đăng nhập root bị hạn chế đối với bảng điều khiển hệ thống
* Tệp /etc/securetty chứa danh sách các thiết bị đầu cuối hợp lệ có thể được đăng nhập trực tiếp dưới dạng nguồn gốc.
* Do bảng điều khiển hệ thống có các thuộc tính đặc biệt để xử lý các tình huống khẩn cấp nên điều quan trọng là đảm bảo rằng bảng điều khiển ở một vị trí an toàn về mặt vật lý và bảng điều khiển trái phép chưa được xác định.
  1. **Ensure access to the su command is restricted (Automated)**
* Đảm bảo quyền truy cập vào lệnh su bị hạn chế
* Lệnh su cho phép người dùng chạy lệnh hoặc shell với tư cách người dùng khác. Chương trình đã được thay thế bằng sudo, cho phép kiểm soát chi tiết hơn đối với đặc quyền truy cập. Thông thường, lệnh su có thể được thực thi bởi bất kỳ người dùng nào. Bằng cách bỏ ghi chú câu lệnh pam\_wheel.so trong /etc/pam.d/su, lệnh su sẽ chỉ cho phép người dùng trong một nhóm cụ thể để thực hiện su. Nhóm này phải trống để củng cố việc sử dụng sudo cho truy cập đặc quyền.
* Việc hạn chế sử dụng su và sử dụng sudo ở vị trí của nó sẽ giúp quản trị viên hệ thống tốt hơn kiểm soát sự leo thang của các đặc quyền người dùng để thực thi các lệnh đặc quyền. tiện ích sudo cũng cung cấp cơ chế kiểm tra và ghi nhật ký tốt hơn, vì nó có thể ghi nhật ký từng lệnh được thực thi thông qua sudo , trong khi su chỉ có thể ghi lại rằng người dùng đã thực hiện chương trình su

**6 System Maintenance**

**6.1 System File Permissions**

**6.1.1 Audit system file permissions (Manual)**

* Kiểm tra quyền đối với tệp hệ thống
* Trình quản lý gói RPM có một số tùy chọn hữu ích. Một trong số đó, tùy chọn -V, có thể được sử dụng để xác minh rằng các gói hệ thống được cài đặt chính xác. Tùy chọn V có thể được sử dụng để xác minh một gói cụ thể hoặc để xác minh tất cả các gói hệ thống. Nếu không có đầu ra nào được trả về, gói được cài đặt chính xác
* Điều quan trọng là phải xác nhận rằng các tệp và thư mục hệ thống được đóng gói được duy trì với các quyền mà họ dự định có từ nhà phân phối hệ điều hành hoặc theo chính sách trang web địa phương

**6.1.2 Ensure permissions on /etc/passwd are configured (Automated)**

* Đảm bảo quyền trên /etc/passwd được cấu hình
* Tệp /etc/passwd chứa thông tin tài khoản người dùng được sử dụng bởi nhiều hệ thống các tiện ích và do đó phải có thể đọc được để các tiện ích này hoạt động.
* Điều quan trọng là đảm bảo rằng tệp /etc/passwd được bảo vệ khỏi ghi trái phép truy cập. Mặc dù nó được bảo vệ theo mặc định, nhưng quyền của tệp có thể bị thay đổi vô tình hoặc thông qua các hành động ác ý

**6.1.3 Ensure permissions on /etc/passwd- are configured (Automated)**

* Đảm bảo các quyền trên /etc/passwd- được định cấu hình
* Tệp /etc/passwd- chứa thông tin tài khoản người dùng dự phòng.
* Điều quan trọng là đảm bảo rằng tệp /etc/passwd- được bảo vệ khỏi sự truy cập trái phép. Mặc dù nó được bảo vệ theo mặc định, nhưng quyền của tệp có thể bị thay đổi vô tình hoặc thông qua các hành động ác ý

**6.1.4 Ensure permissions on /etc/shadow are configured (Automated)**

* Đảm bảo các quyền trên /etc/shadow được định cấu hình
* Tệp /etc/shadow được sử dụng để lưu trữ thông tin về tài khoản người dùng quan trọng đối với bảo mật của các tài khoản đó, chẳng hạn như mật khẩu băm và bảo mật khác thông tin.
* Nếu kẻ tấn công có thể đọc được tệp /etc/shadow, chúng có thể dễ dàng chạy mật khẩu chương trình bẻ khóa mật khẩu băm để phá vỡ nó. Thông tin bảo mật khác mà được lưu trữ trong tệp /etc/shadow (chẳng hạn như hết hạn) cũng có thể hữu ích để thay thế tài khoản người dùng.

**6.1.5 Ensure permissions on /etc/shadow- are configured (Automated)**

* Đảm bảo các quyền trên /etc/shadow- được định cấu hình
* Tệp /etc/shadow- được sử dụng để lưu trữ thông tin sao lưu về tài khoản người dùng được quan trọng đối với tính bảo mật của các tài khoản đó, chẳng hạn như mật khẩu băm và các biện pháp bảo mật khác thông tin.
* Điều quan trọng là đảm bảo rằng tệp /etc/shadow- được bảo vệ khỏi sự truy cập trái phép. Mặc dù nó được bảo vệ theo mặc định, nhưng quyền của tệp có thể bị thay đổi vô tình hoặc thông qua các hành động ác ý

**6.1.6 Ensure permissions on /etc/gshadow- are configured (Automated)**

* Đảm bảo các quyền trên /etc/gshadow- được định cấu hình
* Tệp /etc/gshadow- được sử dụng để lưu trữ thông tin sao lưu về các nhóm quan trọng đối với bảo mật của các tài khoản đó, chẳng hạn như mật khẩu băm và bảo mật khác thông tin.
* Điều quan trọng là đảm bảo rằng tệp /etc/gshadow- được bảo vệ khỏi sự truy cập trái phép. Mặc dù nó được bảo vệ theo mặc định, nhưng quyền của tệp có thể bị thay đổi vô tình hoặc thông qua các hành động ác ý

**6.1.7 Ensure permissions on /etc/gshadow are configured (Automated)**

* Đảm bảo các quyền trên /etc/gshadow được định cấu hình
* Tệp /etc/gshadow được sử dụng để lưu trữ thông tin về các nhóm quan trọng đối với bảo mật của các tài khoản đó, chẳng hạn như mật khẩu băm và thông tin bảo mật khác.
* Nếu kẻ tấn công có thể có quyền truy cập đọc vào tệp /etc/gshadow, chúng có thể dễ dàng chạy mật khẩu chương trình bẻ khóa mật khẩu băm để phá vỡ nó. Thông tin bảo mật khác mà được lưu trữ trong tệp /etc/gshadow (chẳng hạn như quản trị viên nhóm) cũng có thể hữu ích để lật đổ nhóm.

**6.1.8 Ensure permissions on /etc/group are configured (Automated)**

* Đảm bảo các quyền trên/etc/group được định cấu hình
* Tệp /etc/group chứa danh sách tất cả các nhóm hợp lệ được xác định trong hệ thống. Các lệnh bên dưới cho phép quyền truy cập đọc/ghi đối với quyền root và quyền truy cập đọc đối với những người khác.
* Tệp /etc/group cần được bảo vệ khỏi những thay đổi trái phép bởi những người không có đặc quyền người dùng, nhưng cần phải đọc được vì thông tin này được sử dụng với nhiều người không có đặc quyền các chương trình

**6.1.9 Ensure permissions on /etc/group- are configured (Automated)**

* Đảm bảo các quyền trên /etc/group- được định cấu hình
* Tệp /etc/group- chứa danh sách dự phòng của tất cả các nhóm hợp lệ được xác định trong hệ thống.
* Điều quan trọng là đảm bảo rằng tệp /etc/group- được bảo vệ khỏi sự truy cập trái phép. Mặc dù nó được bảo vệ theo mặc định, nhưng quyền của tệp có thể bị thay đổi vô tình hoặc thông qua các hành động ác ý

**6.1.10 Ensure no world writable files exist (Automated)**

* Đảm bảo không tồn tại tệp có thể ghi trên thế giới
* Các hệ thống dựa trên Unix hỗ trợ cài đặt biến để kiểm soát quyền truy cập vào tệp. Tập tin có thể ghi trên thế giới là kém an toàn nhất. Xem trang hướng dẫn chmod(2) để biết thêm thông tin.
* Dữ liệu trong các tệp có thể ghi trên thế giới có thể được sửa đổi và xâm phạm bởi bất kỳ người dùng nào trên hệ thống. Các tệp có thể ghi trên thế giới cũng có thể chỉ ra một tập lệnh hoặc chương trình được viết không chính xác có thể có khả năng là nguyên nhân của sự thỏa hiệp lớn hơn đối với tính toàn vẹn của hệ thống.

**6.1.11 Ensure no unowned files or directories exist (Automated)**

* Đảm bảo không tồn tại các tệp hoặc thư mục không xác định
* Đôi khi quản trị viên xóa người dùng khỏi tệp mật khẩu mà họ bỏ qua xóa tất cả các tệp thuộc sở hữu của những người dùng đó khỏi hệ thống.
* Sau đó, một người dùng mới được chỉ định ID người dùng hoặc ID nhóm của người dùng đã xóa có thể kết thúc "sở hữu" các tệp này và do đó có nhiều quyền truy cập vào hệ thống hơn dự định.

**6.1.12 Ensure no ungrouped files or directories exist (Automated)**

* Đảm bảo không tồn tại các tệp hoặc thư mục chưa được nhóm
* Đôi khi quản trị viên xóa người dùng hoặc nhóm khỏi hệ thống mà họ bỏ qua xóa tất cả các tệp thuộc sở hữu của những người dùng hoặc nhóm đó.
* Sau đó, một người dùng mới được chỉ định ID người dùng hoặc ID nhóm của người dùng đã xóa có thể kết thúc "sở hữu" các tệp này và do đó có nhiều quyền truy cập vào hệ thống hơn dự kiến

**6.1.13 Audit SUID executables (Manual)**

* Kiểm tra SUID thực thi
* Chủ sở hữu tệp có thể đặt quyền của tệp để chạy với quyền của chủ sở hữu hoặc nhóm quyền, ngay cả khi người dùng đang chạy chương trình không phải là chủ sở hữu hoặc thành viên của nhóm. Lý do phổ biến nhất cho một chương trình SUID là cho phép người dùng thực hiện các chức năng (chẳng hạn như thay đổi mật khẩu) yêu cầu quyền root.
* Có những lý do chính đáng cho các chương trình SUID, nhưng điều quan trọng là phải xác định và xem xét những lý do đó. các chương trình để đảm bảo chúng là hợp pháp

**6.1.14 Audit SGID executables (Manual)**

* Kiểm tra các tệp thực thi SGID
* Chủ sở hữu tệp có thể đặt quyền của tệp để chạy với quyền của chủ sở hữu hoặc nhóm quyền, ngay cả khi người dùng đang chạy chương trình không phải là chủ sở hữu hoặc thành viên của nhóm. Lý do phổ biến nhất cho chương trình SGID là cho phép người dùng thực hiện các chức năng (chẳng hạn như thay đổi mật khẩu) yêu cầu quyền root.
* Có những lý do chính đáng cho các chương trình SGID, nhưng điều quan trọng là phải xác định và xem xét những lý do đó. các chương trình để đảm bảo chúng là hợp pháp. Xem lại các tệp được trả về bởi hành động trong quá trình kiểm tra phần và kiểm tra xem liệu nhị phân hệ thống có tổng kiểm tra md5 khác với những gì từ gói. Đây là một dấu hiệu cho thấy nhị phân có thể đã được thay thế

**6.2 User and Group Settings**

**6.2.1 Ensure accounts in /etc/passwd use shadowed passwords (Automated)**

* Đảm bảo các tài khoản trong /etc/passwd sử dụng mật khẩu ẩn
* Tài khoản cục bộ có thể sử dụng mật khẩu ẩn. Với mật khẩu ẩn, Mật khẩu được lưu trong tệp mật khẩu bóng tối, /etc/shadow, được mã hóa bằng hàm băm một chiều có muối. Các tài khoản có mật khẩu ẩn có dấu x trong trường thứ hai trong /etc/passwd.
* Tệp /etc/passwd cũng chứa thông tin như ID người dùng và ID nhóm được sử dụng bằng nhiều chương trình hệ thống. Do đó, tệp /etc/passwd phải có thể đọc được trên toàn thế giới. mặc dù mã hóa mật khẩu bằng hàm băm một chiều được tạo ngẫu nhiên, một kẻ tấn công vẫn có thể phá vỡ hệ thống nếu chúng có quyền truy cập vào tệp /etc/passwd. Điều này có thể là giảm thiểu bằng cách sử dụng mật khẩu ẩn, do đó di chuyển mật khẩu trong /etc/passwd tệp vào /etc/shadow. Tệp /etc/shadow được đặt sao cho chỉ root mới có thể đọc và ghi. Điều này giúp giảm thiểu nguy cơ kẻ tấn công giành được quyền truy cập vào mật khẩu được mã hóa bằng which để thực hiện một cuộc tấn công từ điển.

**6.2.2 Ensure /etc/shadow password fields are not empty (Automated)**

* Đảm bảo các trường mật khẩu /etc/shadow không trống
* Tài khoản có trường mật khẩu trống có nghĩa là bất kỳ ai cũng có thể đăng nhập với tư cách người dùng đó mà không cần cung cấp mật khẩu.
* Tất cả các tài khoản phải có mật khẩu hoặc bị khóa để ngăn tài khoản bị sử dụng người dùng trái phép

**6.2.3 Ensure all groups in /etc/passwd exist in /etc/group (Automated)**

* Đảm bảo tất cả các nhóm trong /etc/passwd tồn tại trong /etc/group
* Theo thời gian, các lỗi và thay đổi quản trị hệ thống có thể dẫn đến các nhóm được xác định trong /etc/passwd nhưng không có trong /etc/group .
* Các nhóm được xác định trong tệp /etc/passwd nhưng không có trong tệp /etc/group gây ra mối đe dọa đối với bảo mật hệ thống do quyền của nhóm không được quản lý đúng cách

**6.2.4 Ensure shadow group is empty (Automated)**

* Đảm bảo shadow group trống
* Nhóm bóng tối cho phép các chương trình hệ thống yêu cầu quyền truy cập để đọc /etc/shadow tập tin. Không có người dùng nào được chỉ định vào nhóm bóng tối.
* Bất kỳ người dùng nào được gán cho nhóm bóng tối sẽ được cấp quyền truy cập đọc vào /etc/shadow tài liệu. Nếu kẻ tấn công có thể đọc được tệp /etc/shadow, chúng có thể dễ dàng chạy mật khẩu chương trình bẻ khóa mật khẩu băm để phá vỡ chúng. Thông tin bảo mật khác được lưu trữ trong tệp /etc/shadow (chẳng hạn như hết hạn) cũng có thể hữu ích để lật đổ tài khoản người dùng bổ sung.

**6.2.5 Ensure no duplicate user names exist (Automated)**

* Đảm bảo không tồn tại tên người dùng trùng lặp
* Mặc dù chương trình useradd sẽ không cho phép bạn tạo tên người dùng trùng lặp, nhưng có thể để quản trị viên chỉnh sửa thủ công tệp /etc/passwd và thay đổi tên người dùng.
* Nếu người dùng được gán một tên người dùng trùng lặp, thì người dùng đó sẽ tạo và có quyền truy cập vào các tệp có UID đầu tiên cho tên người dùng đó trong /etc/passwd . Ví dụ: nếu "test4" có UID là 1000 và mục nhập "test4" tiếp theo có UID là 2000, đăng nhập bằng "test4" sẽ sử dụng UID 1000. Thực tế, UID được chia sẻ, đây là một vấn đề bảo mật.

**6.2.6 Ensure no duplicate group names exist (Automated)**

* Đảm bảo không tồn tại tên nhóm trùng lặp
* Mặc dù chương trình groupadd sẽ không cho phép bạn tạo một tên nhóm trùng lặp, nhưng nó quản trị viên có thể chỉnh sửa thủ công tệp /etc/group và thay đổi nhóm tên.
* Nếu một nhóm được gán một tên nhóm trùng lặp, nó sẽ tạo và có quyền truy cập vào các tệp có GID đầu tiên cho nhóm đó trong /etc/group . Thực tế, GID được chia sẻ, đó là một bảo mật vấn đề.

**6.2.7 Ensure no duplicate UIDs exist (Automated)**

* Đảm bảo không tồn tại UID trùng lặp
* Mặc dù chương trình useradd sẽ không cho phép bạn tạo ID người dùng (UID) trùng lặp, nhưng nó quản trị viên có thể chỉnh sửa thủ công tệp /etc/passwd và thay đổi UID cánh đồng.
* Người dùng phải được chỉ định UID duy nhất để chịu trách nhiệm và để đảm bảo quyền truy cập phù hợp bảo vệ.

**6.2.8 Ensure no duplicate GIDs exist (Automated)**

* Đảm bảo không tồn tại GID trùng lặp
* Mặc dù chương trình groupadd sẽ không cho phép bạn tạo ID nhóm (GID) trùng lặp, nhưng nó quản trị viên có thể chỉnh sửa thủ công tệp /etc/group và thay đổi trường GID.
* Các nhóm người dùng phải được chỉ định các GID duy nhất để chịu trách nhiệm và để đảm bảo phù hợp bảo vệ truy cập.

**6.2.9 Ensure root is the only UID 0 account (Automated)**

* Đảm bảo root là tài khoản UID 0 duy nhất
* Bất kỳ tài khoản nào có UID 0 đều có đặc quyền siêu người dùng trên hệ thống.
* Quyền truy cập này chỉ được giới hạn ở tài khoản gốc mặc định và chỉ từ hệ thống bảng điều khiển. Quyền truy cập quản trị phải thông qua tài khoản không có đặc quyền sử dụng tài khoản được phê duyệt cơ chế như đã lưu ý trong Mục 5.6 Đảm bảo quyền truy cập vào lệnh su bị hạn chế.

**6.2.10 Ensure root PATH Integrity (Automated)**

* Đảm bảo tính toàn vẹn của PATH gốc
* Người dùng root có thể thực thi bất kỳ lệnh nào trên hệ thống và có thể bị lừa khi thực thi chương trình ngoài ý muốn nếu PATH không được đặt chính xác.
* Bao gồm thư mục làm việc hiện tại (.) hoặc thư mục có thể ghi khác trong tệp thực thi của root đường dẫn khiến kẻ tấn công có thể có quyền truy cập siêu người dùng bằng cách buộc quản trị viên hoạt động với quyền root để thực thi chương trình ngựa thành Troy.

**6.2.11 Ensure all users' home directories exist (Automated)**

* Đảm bảo tồn tại tất cả các thư mục chính của người dùng
* Người dùng có thể được xác định trong /etc/passwd mà không cần thư mục chính hoặc có thư mục chính điều đó không thực sự tồn tại.
* Nếu thư mục chính của người dùng không tồn tại hoặc chưa được chỉ định, người dùng sẽ được đặt trong "/" và sẽ không thể ghi bất kỳ tệp nào hoặc đặt các biến môi trường cục bộ

**6.2.12 Ensure users own their home directories (Automated)**

* Đảm bảo người dùng sở hữu thư mục chính của họ
* Thư mục chính của người dùng là không gian được xác định cho người dùng cụ thể để đặt môi trường cục bộ biến và để lưu trữ các tập tin cá nhân.
* Vì người dùng chịu trách nhiệm đối với các tệp được lưu trữ trong thư mục chính của người dùng, nên người dùng phải chủ sở hữu của thư mục

**6.2.13 Ensure users' home directories permissions are 750 or more restrictive (Automated)**

* Đảm bảo quyền thư mục chính của người dùng từ 750 trở lên hạn chế
* Trong khi quản trị viên hệ thống có thể thiết lập các quyền an toàn cho nhà của người dùng thư mục, người dùng có thể dễ dàng ghi đè lên chúng.
* Nhóm hoặc thư mục chính của người dùng có thể ghi trên thế giới có thể cho phép người dùng độc hại đánh cắp hoặc sửa đổi dữ liệu của người dùng khác hoặc để giành được đặc quyền hệ thống của người dùng khác

**6.2.14 Ensure users' dot files are not group or world writable (Automated)**

* Đảm bảo các tệp dấu chấm của người dùng không thể ghi theo nhóm hoặc trên thế giới
* Mặc dù quản trị viên hệ thống có thể thiết lập các quyền an toàn cho các tệp "chấm" của người dùng, người dùng có thể dễ dàng ghi đè lên những.
* Các tệp cấu hình người dùng có thể ghi trên thế giới hoặc nhóm có thể cho phép người dùng độc hại đánh cắp hoặc sửa đổi dữ liệu của người dùng khác hoặc để giành được đặc quyền hệ thống của người dùng khác

**6.2.15 Ensure no users have .forward files (Automated)**

* Đảm bảo không có người dùng nào có tệp .forward
* Tệp .forward chỉ định địa chỉ email để chuyển tiếp thư của người dùng tới.
* Việc sử dụng tệp .forward gây ra rủi ro bảo mật trong đó dữ liệu nhạy cảm có thể vô tình chuyển ra ngoài tổ chức. Tệp .forward cũng có rủi ro vì nó có thể được sử dụng để thực thi các lệnh có thể thực hiện các hành động ngoài ý muốn

**6.2.16 Ensure no users have .netrc files (Automated)**

* Đảm bảo không có người dùng nào có tệp .netrc
* Tệp .netrc chứa dữ liệu để đăng nhập vào máy chủ từ xa để truyền tệp qua FTP. Mặc dù quản trị viên hệ thống có thể thiết lập các quyền an toàn cho các tệp .netrc của người dùng, người dùng có thể dễ dàng ghi đè lên những.
* Tệp .netrc có rủi ro bảo mật đáng kể vì nó lưu trữ mật khẩu ở dạng không được mã hóa hình thức. Ngay cả khi FTP bị tắt, tài khoản người dùng có thể đã mang tệp .netrc từ tài khoản khác các hệ thống có thể gây rủi ro cho các hệ thống đó. Nếu tệp .netrc được yêu cầu và tuân theo chính sách trang web cục bộ, thì tệp đó phải có quyền từ 600 trở lên hạn chế hơn.

**6.2.17 Ensure no users have .rhosts files (Automated)**

* Đảm bảo không có người dùng nào có tệp .rhosts
* Mặc dù không có tệp .rhosts nào được vận chuyển theo mặc định, nhưng người dùng có thể dễ dàng tạo chúng.
* Hành động này chỉ có ý nghĩa nếu hỗ trợ .rhosts được cho phép trong tệp /etc/pam.conf . Mặc dù các tệp .rhosts không hiệu quả nếu hỗ trợ bị tắt trong /etc/pam.conf , nhưng chúng có thể đã được mang đến từ các hệ thống khác và có thể chứa thông tin hữu ích cho một kẻ tấn công cho những hệ thống khác

# **MỞ ĐẦU**

1. **Lý do chọn đề tài**

Sự quan trọng của bảo mật hệ thống: Bảo mật hệ thống là yếu tố cực kỳ quan trọng để đảm bảo tính toàn vẹn và an toàn của dữ liệu và hoạt động của hệ thống. Chuẩn bảo mật CIS CentOS 7 Benchmark cung cấp một tập hợp các hướng dẫn và best practice để tăng cường bảo mật hệ thống CentOS 7.

Tính khả thi của ứng dụng: Áp dụng CIS CentOS 7 Benchmark vào việc tính toán Exposure Risk giúp đánh giá rủi ro tiếp xúc của hệ thống, từ đó cung cấp thông tin quan trọng để đưa ra quyết định và biện pháp bảo mật hiệu quả.

1. **Mục đích nghiên cứu**

Hiểu và áp dụng tiêu chuẩn bảo mật CIS: Mục đích chính của đề tài là hiểu rõ các yêu cầu bảo mật được đề ra bởi CIS CentOS 7 Benchmark và áp dụng chúng vào hệ thống CentOS 7.

Tính toán Exposure Risk: Nghiên cứu sẽ tập trung vào việc tính toán Exposure Risk của hệ thống dựa trên các chỉ số bảo mật từ CIS CentOS 7 Benchmark. Điều này giúp đánh giá mức độ tiếp xúc với rủi ro bảo mật và ảnh hưởng của chúng đến hệ thống.

Đưa ra biện pháp bảo mật hiệu quả: Nghiên cứu này giúp đưa ra các biện pháp bảo mật cụ thể và hiệu quả để giảm thiểu Exposure Risk, đảm bảo tính bảo mật và an toàn của hệ thống CentOS 7.

1. **Tình hình nghiên cứu**

CIS CentOS 7 Benchmark là một tài liệu tiêu chuẩn được CIS công bố, cung cấp hướng dẫn chi tiết về cấu hình bảo mật cho hệ điều hành CentOS 7.

Tình hình nghiên cứu hiện tại đã có nhiều tài liệu và tài nguyên trực tuyến về CIS CentOS 7 Benchmark, cũng như các phương pháp tính toán rủi ro bảo mật

1. **Phạm vi và phương pháp nghiên cứu**

Phạm vi nghiên cứu: Nghiên cứu sẽ tập trung vào việc áp dụng CIS CentOS 7 Benchmark vào việc tính toán Exposure Risk của hệ thống CentOS 7. Phạm vi cũng có thể bao gồm đánh giá các lỗ hổng bảo mật, đề xuất biện pháp khắc phục, và đo lường hiệu quả của các biện pháp bảo mật.

Phương pháp nghiên cứu: Phương pháp nghiên cứu có thể bao gồm việc tìm hiểu tài liệu, áp dụng các chỉ số bảo mật từ CIS CentOS 7 Benchmark để tính toán Exposure Risk, đánh giá tác động của rủi ro, và đề xuất biện pháp bảo mật. Các phương pháp thực hiện bao gồm kiểm tra và đánh giá bảo mật, tính toán các chỉ số rủi ro, và triển khai các biện pháp bảo mật

1. **Kết cấu của đề tài**

Đề tài bao gồm 5 chương:

* Chương 1: Giới thiệu CIS CentOS7 Benchmark
* Chương 2: Hiện thực đo đạc Compliance của Server
* Chương 3: Exposure Risk
* Chương 4: Thực thi Compliance trên CentOS7 và áp dụng tính toán Exposure Risk
* Chương 5: Kết luận và hướng phát triển trong tương lai

# **HIỆN THỰC VIỆC ĐO ĐẠC COMPLIANCE CỦA SERVER**

## **Tổng quan về Compliance**

Compliance được hiểu là “tuân thủ” - Tuân thủ có nghĩa là một công ty tuân thủ các quy tắc và luật hiện hành. Điều này bao gồm cả luật cụ thể của quốc gia và các yêu cầu từ cơ quan quản lý cũng như các chỉ thị nội bộ của công ty. Một loạt các công cụ và quy trình có thể được thực hiện và sử dụng bởi một công ty để mang lại sự tuân thủ tốt. Chúng được thiết kế để đảm bảo rằng hành vi sai trái hoặc vi phạm có thể được phát hiện, ngăn chặn hoặc giải quyết ở giai đoạn đầu, trước mọi hậu quả nghiêm trọng như truy tố hình sự, phạt tiền hoặc tổn hại nghiêm trọng đến danh tiếng của công ty.

Đề cập đến quá trình giám sát và đánh giá liên tục các hệ thống mà các doanh nghiệp, công ty và tổ chức doanh nghiệp phải tuân theo để duy trì tuân thủ các quy định của ngành, tiêu chuẩn bảo mật cũng như các chính sách và yêu cầu của công ty

Tuân thủ là mối quan tâm phổ biến của doanh nghiệp, một phần là do số lượng quy định ngày càng tăng đòi hỏi các công ty phải thận trọng trong việc duy trì sự hiểu biết đầy đủ về các yêu cầu quy định của họ đối với việc tuân thủ. Để tuân thủ các tiêu chuẩn tuân thủ, một tổ chức phải tuân theo các yêu cầu hoặc quy định do tổ chức hoặc luật pháp của chính phủ áp đặt.

## **Tại sao cần phải tuân thủ theo CIS Benchmark?**

CIS (Center for Internet Security) Benchmark là một tập hợp các hướng dẫn bảo mật được công bố bởi tổ chức CIS, nhằm giúp các tổ chức và người dùng bảo vệ hệ thống máy tính và mạng của mình khỏi các lỗ hổng bảo mật phổ biến. CIS Benchmark cung cấp các hướng dẫn chi tiết về cấu hình an toàn cho các hệ điều hành và ứng dụng phổ biến

Tăng cường bảo mật: CIS Benchmark cung cấp hướng dẫn cụ thể về cấu hình an toàn, bao gồm việc tắt các dịch vụ không cần thiết, kiểm tra và cấu hình các tính năng bảo mật quan trọng, và áp dụng các biện pháp bảo mật khác. Tuân thủ theo CIS Benchmark giúp tăng cường bảo mật hệ thống và giảm khả năng bị tấn công.

Chống lại các lỗ hổng bảo mật đã biết: CIS Benchmark giúp người dùng xác định và khắc phục các lỗ hổng bảo mật phổ biến đã được công bố. Bằng cách tuân thủ các khuyến nghị trong CIS Benchmark, bạn có thể giảm nguy cơ bị tấn công từ các lỗ hổng đã biết.

Tuân thủ các tiêu chuẩn và quy định: Một số quy định và tiêu chuẩn an ninh, như PCI DSS (Payment Card Industry Data Security Standard), yêu cầu việc tuân thủ CIS Benchmark. Tuân thủ CIS Benchmark giúp đáp ứng các yêu cầu tuân thủ quy định và giúp xác định được các vấn đề bảo mật tiềm ẩn trong hệ thống.

Tăng đáng tin cậy và sẵn sàng: Bằng việc tuân thủ CIS Benchmark, bạn đảm bảo rằng hệ thống của mình được cấu hình một cách chuẩn mực và an toàn. Điều này giúp tăng đáng tin cậy và sẵn sàng của hệ thống, giảm nguy cơ sự cố và thời gian chết máy

## **Cách hiện thực việc đo đạc Compliance của Server**

Để đo đạc tuân thủ CIS CentOS 7 Benchmark trên Server (cụ thể là trên máy ảo chạy CentOS 7), bạn có thể thực hiện các bước sau:

* Tải xuống CIS CentOS 7 Benchmark: Truy cập trang web của CIS (https://www.cisecurity.org) và tải xuống phiên bản CIS CentOS 7 Benchmark: đối với người dùng bình thường thì chỉ download miễn phí file PDF từ trang web của CIS
* Đánh giá hiện trạng: Sử dụng công cụ đánh giá tuân thủ (compliance assessment tool) để kiểm tra hiện trạng tuân thủ CIS Benchmark trên máy chủ của bạn. Ở đây, em sẽ tự mình từng script cho từng tiêu chuẩn dựa trên phần Audit trong filr Document của CIS CentOS 7 Benchmark (file PDF) để kiểm tra xem các tiêu chuẩn nào pass (tuân thủ)/ fail (không tuân thủ
* Xác định các vấn đề chưa tuân thủ: Xem xét báo cáo được tạo bởi công cụ đánh giá tuân thủ và xác định các vấn đề chưa tuân thủ. Các vấn đề này có thể bao gồm cấu hình sai, dịch vụ không an toàn, quyền truy cập không đúng, hoặc các vấn đề bảo mật khác.
* Điều chỉnh cấu hình: Dựa trên báo cáo về các vấn đề chưa tuân thủ, điều chỉnh cấu hình hệ thống để đáp ứng các yêu cầu của CIS Benchmark. Theo dõi hướng dẫn cung cấp trong báo cáo để biết cách cấu hình lại hệ thống một cách đúng đắn.
* Kiểm tra lại tuân thủ: Sau khi điều chỉnh cấu hình, chạy lại công cụ đánh giá tuân thủ để kiểm tra lại tuân thủ CIS Benchmark. Đảm bảo rằng các vấn đề chưa tuân thủ đã được giải quyết và hệ thống đáp ứng các yêu cầu của CIS Benchmark.
* Thực hiện kiểm tra định kỳ: Để đảm bảo tuân thủ liên tục, lập lịch kiểm tra định kỳ để kiểm tra tuân thủ CIS Benchmark trên máy chủ của bạn. Kiểm tra định kỳ giúp phát hiện các vấn đề mới và đảm bảo rằng hệ thống không bị lỏng lẻo về mặt bảo mật theo thời gian

# **EXPOSURE RISK**

## **Tổng quan về Exposure Risk**

Exposure Risk đề cập đến tác hại tiềm tàng hoặc hậu quả tiêu cực có thể phát sinh từ việc tiếp xúc với một mối đe dọa hoặc lỗ hổng cụ thể. Trong bối cảnh an ninh mạng và hệ thống thông tin, rủi ro phơi nhiễm thường liên quan đến khả năng và tác động của sự cố hoặc vi phạm bảo mật xảy ra do lỗ hổng trong hệ thống.

Exposure Riskcó tính đến các yếu tố như khả năng xảy ra một cuộc tấn công hoặc sự cố và thiệt hại hoặc tổn thất tiềm ẩn có thể xảy ra từ đó. Nó xem xét cả xác suất xảy ra sự kiện và mức độ nghiêm trọng tiềm ẩn của tác động của nó đối với hệ thống, bao gồm tổn thất tài chính, vi phạm dữ liệu, thiệt hại về uy tín hoặc gián đoạn hoạt động.

Việc đánh giá Exposure Risk liên quan đến việc xác định và phân tích các lỗ hổng, đánh giá khả năng khai thác của chúng và đánh giá tác động tiềm ẩn đối với hệ thống hoặc tổ chức. Đánh giá này giúp các tổ chức ưu tiên các nỗ lực bảo mật của họ và phân bổ nguồn lực một cách hiệu quả để giảm thiểu hoặc giảm thiểu các rủi ro đã xác định.

Bằng cách hiểu Exposure Risk, các tổ chức có thể triển khai các biện pháp bảo mật thích hợp, chẳng hạn như triển khai các bản vá, định cấu hình cài đặt bảo mật, tiến hành đánh giá lỗ hổng thường xuyên và triển khai các kế hoạch ứng phó sự cố hiệu quả, để giảm khả năng và tác động của các sự cố bảo mật, đồng thời bảo vệ hệ thống và dữ liệu của họ khỏi sự cố trái phép truy cập hoặc khai thác.

## **Cơ sở lý thuyết để tính toán Exposure Risk theo Tenable**

### **Các thành phần để tính toán Exposure Risk**



Hình 3.1: Tổng quan các thành phần của Exposure Risk

Điểm phơi nhiễm không gian mạng được xác định về mặt khái niệm dựa trên việc định lượng rủi ro không gian mạng cho một tập hợp tài sản trên hai chiều; đầu tiên là mức độ nghiêm trọng và khả năng khai thác của tất cả lỗ hổng ảnh hưởng đến từng tài sản và thứ hai là mức độ quan trọng của từng tài sản đối với kinh doanh.

* Mức độ nghiêm trọng và khả năng khai thác của một lỗ hổng nhất định được thể hiện bằng Xếp hạng ưu tiên lỗ hổng (VPR).
* Mức độ quan trọng của tài sản được thể hiện bằng Xếp hạng mức độ nghiêm trọng của tài sản (ACR).

##### **VPR: Remediation Priority of a Single Vulnerability**

VPR - Vulnerability Priority Rating: Đánh giá ưu tiên lỗ hổng

VPR của lỗ hổng được biểu thị bằng số từ 0,1 đến 10, với các giá trị cao hơn tương ứng với khả năng dễ bị tổn thương cao hơn dẫn đến thỏa hiệp và tác động cao hơn đến tài sản. Dựa trên những giá trị đó, các lỗ hổng có thể đ (ược đánh giá theo thuật ngữ mức độ nghiêm trọng của chúng, bao gồm:

* Thấp (0,1-3,9),
* Trung bình (4,0-6,9),
* Cao (7,0-8,9)
* Quan trọng (9,0-10,0).

VPR là điểm số do máy tạo ra chỉ dựa trên lỗ hổng mà không tính đến môi trường nơi nó được tìm thấy; như vậy, nó không phụ thuộc vào những cân nhắc cụ thể của người dùng và không thể thay đổi hoặc tùy chỉnh.

Trình điều khiển chính được sử dụng để tính toán VPR bao gồm, nhưng không giới hạn ở những điều sau:

* Age of vulnerability (Tuổi dễ bị tổn thương), tính bằng ngày kể từ khi xuất bản trong NVD
* CVSSv3 Impact Score (Điểm tác động CVSSv3), nếu có, hoặc điểm tác động dự đoán khác cho các lỗ hổng trước NVD xuất bản theo đó mô hình phân tích văn bản từ tư vấn bảo mật làm đầu vào
* Exploit code maturity (Độ chín của mã khai thác), dựa trên sự tồn tại và độ phức tạp của mã khai thác có liên quan
* Product coverage (Phạm vi bảo hiểm của sản phẩm), xét về số lượng tương đối của các hệ thống duy nhất bị ảnh hưởng bởi lỗ hổng bảo mật
* Threat sources (Các nguồn đe dọa), chẳng hạn như các kênh truyền thông xã hội và diễn đàn dark web nơi thảo luận về việc khai thác
* Threat intensity (Cường độ đe dọa), dựa trên số lượng và tần suất của các sự kiện đe dọa gần đây
* Threat recency (Mối đe dọa gần đây) hoặc số ngày kể từ khi một sự kiện đe dọa xảy ra

##### **ACR: Relative Business Criticality of a Given Asset**

ACR - Asset Criticality Rating: Đánh giá mức độ quan trọng của tài sản

ACR của nội dung được biểu thị dưới dạng số nguyên từ 1 đến 10, với các giá trị cao hơn tương ứng với nội dung quan trọng hơn đối với doanh nghiệp. Dựa trên những giá trị đó, ACR của nội dung có thể được mô tả là

* Thấp (1-3),
* Trung bình (4-6),
* Cao (7-8)
* Nguy hiểm (9-10).

Một ACR ban đầu được gán vào lần đầu tiên Tenable quét và phát hiện ra một tài sản và giá trị được cập nhật tự động hàng ngày. Tự động gán ACR sử dụng kết quả quét để xác định các tính năng của nội dung, bao gồm loại và khả năng của nội dung. Sau đó, Tenable áp dụng một hệ thống chuyên gia, dựa trên quy tắc để tạo điểm số quan trọng trên cơ sở từng tính năng, đó là tổng hợp để tạo ra ACR tổng thể. Trình điều khiển chính được sử dụng để tính toán ACR cho một nội dung nhất định bao gồm:

* Device type (Loại thiết bị), chẳng hạn như trình ảo hóa, máy in hoặc máy chủ
* Device capability (Khả năng của thiết bị), thể hiện mục đích của nội dung, chẳng hạn như chia sẻ tệp hoặc gửi/nhận email
* Internet exposure (Mức độ tiếp xúc với Internet), dựa trên việc nội dung có nằm trên mạng LAN được kiểm soát và bảo vệ hay không

### **Cách tính toán Exposure Risk**

Cách tiếp cận tổng thể để tính toán điểm tiếp xúc là tính toán mức độ tiếp xúc với từng tài sản riêng lẻ - được gọi là AES - Asset Exposure Score — và sau đó để tìm Điểm Phơi nhiễm Mạng bằng cách tính trung bình cộng nhiều số liệu AES. Như trước đây lưu ý, Điểm tiếp xúc trên mạng là một số nguyên từ 1 đến 1.000 mô tả mức độ rủi ro đối với nhóm tài sản như một tổng thể. Nhóm nội dung đó có thể được xác định là nhóm nội dung được gắn thẻ, nội dung được liên kết với một doanh nghiệp cụ thể mục đích, hoặc toàn bộ tổ chức. Cả Điểm tiếp xúc với tài sản được tính toán và dự đoán đều được sử dụng khi tạo Điểm tiếp xúc trên mạng. Cấp cao các bước cho toàn bộ quá trình xác định điểm số này — được trình bày chi tiết hơn như sau:

* **Tính toán thành phần VPR (Vulnerability Priority Rating)** cho từng nội dung bằng cách phát hiện tất cả các lỗ hổng mở và dự đoán khả năng xảy ra cũng như tác động đến tài sản bị ảnh hưởng của từng lỗ hổng bị khai thác. Nếu khả năng hiển thị nội dung bị hạn chế do thiếu thông tin xác thực quét cục bộ, Tenable sẽ tạo VPR dự đoán điểm thành phần dựa trên các tính năng nội dung đã biết và mức trung bình của dữ liệu tương tự.

**P(any threat) = 1 - P(no threat)**

* **Áp dụng ngữ cảnh ACR (Asset Criticality Rating)** để tạo AES, tính đến mức độ quan trọng trong kinh doanh của từng nội dung bằng cách sử dụng các giá trị ACR do khách hàng cung cấp nếu có và các giá trị được chỉ định Có thể thuê nếu không. Bước này tạo AES cho từng nội dung. Điều này yêu cầu chia giá trị ACR (một số nguyên 1 – 10) cho 10 để phù hợp với mức độ của thành phần VPR (số thập phân từ 0,1 – 1), ví dụ ACR = 8 -> cACR = 0,8

**AES = ( ) x 1000**

* **Tính trung bình cộng tất cả các giá trị AES** để đạt được Điểm tiếp xúc trên mạng cho nhóm nội dung. CES : Cyber Exposure Score

**CES =**

## **Các yếu tố có thể xem xét khi đánh giá Exposure Risk**

Exposure là khuynh hướng của hệ thống đối với mối đe dọa dựa trên các yếu tố môi trường. Một số môi trường làm tăng khả năng xảy ra mối đe dọa. Ví dụ: nếu một tài sản được tiếp xúc với Internet, thì khả năng hệ thống bị xâm nhập do những kẻ xâm nhập bên ngoài sẽ tăng lên. Có nhiều yếu tố có thể ảnh hưởng đến giá trị phơi sáng. Một số yếu tố mà người đánh giá có thể muốn xem xét là:

* **Khả năng truy cập của nội dung** — Có thể truy cập nội dung qua Internet, từ xa qua VPN hay chỉ có thể truy cập qua mạng nội bộ. Một nội dung có thể truy cập Internet rõ ràng có mức độ tiếp xúc cao hơn với một số hình thức nhất định. các mối đe dọa bên ngoài.
* **Vị trí** — Nội dung có được đặt trong trung tâm dữ liệu hay không. Xét về hầu hết các mối đe dọa vật lý và môi trường, vị trí của các hệ thống cốt lõi của bạn đóng vai trò quan trọng phần lớn trong việc xác định khả năng.
* **Luồng dữ liệu** — Cho dù thông tin được truyền bên ngoài hay bên trong tổ chức (ví dụ: web, FTP, phương tiện di động). Liên quan đến danh mục này là đánh giá lượng dữ liệu nhạy cảm được chuyển. Luồng dữ liệu và chuyển giao thông tin đóng một vai trò quan trọng trong các mối đe dọa liên quan đến tính bảo mật. Ví dụ, một hệ thống chuyển một số lượng lớn dữ liệu nhạy cảm qua Internet, rõ ràng là có mức độ tiếp xúc cao hơn về mặt các mối đe dọa bảo mật hơn là một hệ thống chỉ truyền dữ liệu qua các kết nối nội bộ.
* **Số lượng người dùng** — Thông thường, số lượng người dùng càng lớn thì khả năng xảy ra các mối đe dọa đối với ứng dụng càng cao, đặc biệt là các mối đe dọa về tính khả dụng và tính toàn vẹn. Một yếu tố liên quan khác có thể là số lượng hoạt động vì mức độ hoạt động trên hệ thống càng cao thì khả năng tiếp xúc với các mối đe dọa tiềm ẩn về tính toàn vẹn và tính khả dụng càng lớn.
* **Hồ sơ người dùng** — Trong một số trường hợp, loại người dùng của hệ thống có thể làm tăng khả năng xảy ra một số loại mối đe dọa nhất định, đặc biệt là các mối đe dọa ảnh hưởng đến tính toàn vẹn và bảo mật. Ví dụ: các nhà thầu và nhà cung cấp được coi là ít “đáng tin cậy” hơn khi so sánh với các nhân viên của một tổ chức, vì vậy một hệ thống có nhiều người dùng bên ngoài có hồ sơ tiếp xúc khác với một hệ thống chỉ được truy cập bởi người dùng nội bộ.
* **Sự cố trước đó** — Mặc dù không phải luôn luôn như vậy, nhưng sự hiện diện của sự cố bảo mật trước đó hoặc sự kiện bảo mật liên quan đến một mối đe dọa cụ thể có thể là một dấu hiệu của một vấn đề mang tính hệ thống, do đó làm tăng khả năng xảy ra một sự kiện tương tự.
* **Các vấn đề hoặc kết quả được ghi lại** — Một điểm yếu được ghi lại và xác nhận sẽ làm tăng mức độ phơi nhiễm cho khu vực bị ảnh hưởng bởi vấn đề hoặc phát hiện và khả năng một mối đe dọa có thể tận dụng thành công các điểm yếu liên quan đến vấn đề hoặc phát hiện đó.

## **Tổng quan về Bài toán xác định Exposure Risk**

Trong lĩnh vực quản lý rủi ro, bài toán xác định Exposure Risk (rủi ro tiếp xúc) là quá trình đánh giá mức độ tiếp xúc với các rủi ro trong một hệ thống, quá trình hoặc môi trường cụ thể. Bài toán này định lượng và đánh giá các yếu tố có liên quan để đưa ra nhận định về mức độ tiếp xúc của một cá nhân, tổ chức hoặc hệ thống với các rủi ro cụ thể.

Khi xác định Exposure Risk, các yếu tố quan trọng cần được xem xét bao gồm:

* Xác định xác suất (**Probability**): Đánh giá mức độ xảy ra của một sự kiện, sự cố hoặc rủi ro cụ thể. Các yếu tố như lịch sử, thông tin từ nguồn đáng tin cậy, hoặc kinh nghiệm chuyên gia có thể được sử dụng để ước lượng xác suất.
* Xác định tác động (**Impact**): Đánh giá mức độ tác động hoặc thiệt hại tiềm năng do một rủi ro xảy ra. Điều này bao gồm việc đánh giá các yếu tố như giá trị tài sản, ảnh hưởng đến hoạt động kinh doanh, tiền mất giá, thiệt hại về danh tiếng hoặc hậu quả pháp lý.
* Đánh giá sự đáng tin cậy của dữ liệu (**Data Reliability):** Đối với việc tính toán Exposure Risk, sự đáng tin cậy của dữ liệu là yếu tố quan trọng. Điều này bao gồm đánh giá và sử dụng các nguồn thông tin có độ tin cậy cao để đảm bảo tính chính xác và tin cậy trong quá trình đánh giá rủi ro.
* Phân loại và đánh giá rủi ro (**Risk Classification and Assessment**): Dựa trên xác suất và tác động, rủi ro có thể được phân loại vào các mức độ khác nhau, ví dụ như rủi ro cao, trung bình hoặc thấp. Đánh giá này giúp xác định ưu tiên và ưu tiên tài nguyên và biện pháp bảo mật để giảm thiểu rủi ro

# **THỰC THI COMPLIANCE TRÊN SERVER VÀ TÍNH TOÁN EXPOSURE RISK**

## **Thực thi Compliance trên Server**

### **Chuẩn bị**

##### **Máy chủ CentOS 7**

##### **File lưu trữ các script trên máy chủ CentOS 7**

### **Thực hiện**

### **Kết quả**

## **Tính toán Exposure Risk**

# **KẾT LUẬN**

Trong phần kết thúc đề tài thực tập tốt nghiệp " ***CIS CentOS 7 Benchmark và ứng dụng trong bài toán xác định Exposure Risk***", em đã nghiên cứu và áp dụng chuẩn bảo mật CIS CentOS 7 Benchmark vào việc đánh giá Exposure Risk trong hệ thống CentOS 7. Qua quá trình nghiên cứu, em đã nhận ra những ưu điểm và ý nghĩa của việc sử dụng chuẩn bảo mật này để nâng cao tính bảo mật và giảm thiểu rủi ro trong môi trường hệ thống.

Áp dụng CIS CentOS 7 Benchmark đã cho em cái nhìn tổng quan về các yêu cầu bảo mật quan trọng và các biện pháp bảo mật cần được thực hiện trên hệ thống CentOS 7. Điều này giúp em định danh, đánh giá và khắc phục các lỗ hổng bảo mật tồn tại trong hệ thống, đồng thời giúp nâng cao mức độ tuân thủ chuẩn bảo mật và giảm thiểu rủi ro bảo mật.

Bài toán xác định Exposure Risk trong đề tài đã đặt ra mục tiêu đánh giá mức độ tiếp xúc với các rủi ro trong hệ thống CentOS 7. Chúng tôi đã xem xét các yếu tố như xác suất xảy ra các rủi ro, tác động của chúng và độ tin cậy của dữ liệu để xây dựng một đánh giá rủi ro toàn diện.

Qua quá trình thực hiện đề tài, em nhận thấy rằng việc áp dụng CIS CentOS 7 Benchmark vào bài toán Exposure Risk là một phương pháp hiệu quả để định danh, đánh giá và quản lý rủi ro bảo mật trong môi trường CentOS 7. Điều này giúp cung cấp thông tin quan trọng và căn cứ cho việc ra quyết định về bảo mật và triển khai biện pháp bảo mật hiệu quả.

Tổng kết lại, đề tài "CIS CentOS 7 Benchmark và ứng dụng trong bài toán xác định Exposure Risk" đã cung cấp một cái nhìn sâu sắc về việc áp dụng chuẩn bảo mật CIS CentOS 7 Benchmark vào việc đánh giá và quản lý rủi ro bảo mật trong hệ thống CentOS 7. Kết quả nghiên cứu và ứng dụng này có thể góp phần nâng cao tính bảo mật và giảm thiểu rủi ro trong môi trường hệ thống và đóng góp quan trọng cho việc bảo vệ thông tin và hoạt động của các tổ chức sử dụng CentOS 7.

# **DANH MỤC TÀI LIỆU THAM KHẢO**

**Tiếng Anh:**

CIS\_CentOS\_Linux\_7\_Benchmark\_v3.1.2.pdf, CIS, 08-31-2021

Whitepaper-Calculating\_Known\_and\_Unknown\_Risk.pdf, Tenable

**Danh mục các Website tham khảo:**

<https://vi.wikipedia.org/wiki/CentOS#CentOS_phi%C3%AAn_b%E1%BA%A3n_7>

<https://www.cisecurity.org/insights/blog/getting-to-know-the-cis-benchmarks>

https://aws.amazon.com/vi/what-is/cis-benchmarks/