**BỘ TÀI NGUYÊN VÀ MÔI TRƯỜNG**

**TRƯỜNG ĐẠI HỌC TÀI NGUYÊN VÀ MÔI TRƯỜNG TP.HCM**

**KHOA: HỆ THỐNG THÔNG TIN VÀ VIỄN THÁM**

****

**ĐỒ ÁN MÔN HỌC**

**MẠNG MÁY TÍNH CƠ BẢN**

**MỘT SỐ VẤN ĐỀ AN NINH HỆ ĐIỀU HÀNH LINUX**

****

Giảng viên hướng dẫn: **ThS. Từ Thanh Trí**

Sinh viên thực hiện: **Võ Thị Thanh Giàu 0350080074**

**Phạm Thị Thủy Tiên 0350080114**

**Nguyễn Thị Thu Trang 0350080118**

Lớp: **03\_ĐHCNTT2**

Khóa: **2014 – 2018**

**TP. Hồ Chí Minh, tháng 3 năm 2016**

**MỞ ĐẦU**

1. Lý do chọn đề tài

Linux là HĐH hoàn toàn miễn phí, điều đó rất thích hợp cho quá trình học tập đặc biệt trong việc xem xét, chỉnh sửa, tạo ra các dòng lệnh của riêng bạn chứ không còn phải bó buộc vào việc viết các phần mềm trong Windows. Những tài liệu về các phần mềm mã nguồn mở thường có sẵn, chi tiết và được cập nhật thường xuyên. Những thắc mắc của bạn cũng có thể được giải đáp nhanh chóng thông qua các forum của các nhóm phát triển mã nguồn mở. Theo đánh giá của các chuyên gia về cơ chế bảo mật Linux có độ bảo mật cao hơn Window. Tại sao lại nói Linux có tính bảo mật cao hơn Windows? Linux có hệ thống bảo mật như thế nào? Đó là những vấn đề cần quan tâm đối với những ai muốn sử dụng Linux. Vì vậy, chúng em đã chọn nghiên cứu đề tài “Một số vấn đề an ninh của HĐH Linux” để nâng cao kiến thức cho mình.

1. Mục đích nghiên cứu

Nghiên cứu, tìm hiểu, phân tích một số vấn đề an ninh HĐH Linux.

1. Thực trạng

Hiện nay khi nhận thấy tính bảo mật cao thì số lượng người dùng HĐH Linux đang tăng một cách nhanh chóng. Nếu trước đây nó chỉ phù hợp cho những hacker và những ai đặc biệt yêu thích mã nguồn mở thì thực tế hiện nay phần lớn là người dùng trên toàn cầu và các nhóm chuyên nghiệp

1. Đối tương nghiên cứu

HĐH Linux có rất nhiều bản phân phối nhưng Ubuntu là một trong những sản phẩm sáng giá nhất, ngày càng được nhiều người sử dụng. Có thể nói đây là một hệ điều hành hoàn hảo cho lựa chọn sử dụng mã nguồn mở. Do đó đồ án này dựa vào bản phân phối Ubuntu 14.04 LTS (Long Term Support) để nghiên cứu. Tham khảo từ các diễn đàn về Linux và mã nguồn mở.

Sau đây nhóm sẽ trình bày các vấn đề an ninh của hệ điều hành Linux.

**LỜI CẢM ƠN**

Xin chân thành cảm ơn, thầy **ThS**.**Từ Thanh Trí** đã cho nhóm em có cơ hội tìm hiểu về “một số vấn đề an ninh hệ điều hành Linux”.

Để hoàn thiện đồ án này chúng em đã cố gắng và nỗ lực rất nhiều nhưng không tránh khỏi các thiếu sót trong quá trình làm bài. Chúng em mong thầy đóng góp ý kiến để bài làm của chúng em được hoàn thiện hơn.

Chúng em xin chân thành cảm ơn.

**NHẬN XÉT**

|  |
| --- |
| **Điểm** |

**Điểm sinh viên 1:**

**Điểm sinh viên 2:**

**Điểm sinh viên 3:**

**MỤC LỤC**

[CHƯƠNG 1: TỔNG QUAN VỀ MỘT SỐ VẤN ĐỀ AN NINH HỆ ĐIỀU HÀNH LINUX 1](#_Toc446924920)

[1.1 Giới thiệu về hệ điều hành Linux 1](#_Toc446924921)

[1.1.1 Sơ lược về hệ điều hành Linux 1](#_Toc446924922)

[Hình 1.1 Chú chim cánh cụt là biểu tượng quen thuộc của Linux 2](#_Toc446924923)

[1.1.2 Đặc điểm cơ bản của Linux 2](#_Toc446924924)

[1.1.3 Thành phần 2](#_Toc446924925)

[Hình 1.2 Thành phần của HĐH Linux 3](#_Toc446924926)

[1.1.4 Cấu trúc của HĐH Linux 3](#_Toc446924927)

[Hình 1.3 Cấu trúc của HĐH Linux 4](#_Toc446924928)

[1.2 Ưu điểm và nhược điểm của HĐH Linux 4](#_Toc446924929)

[1.3 So sánh HĐH Linux và Windows 6](#_Toc446924930)

[1.4 Các phiên bản Linux phổ biến 7](#_Toc446924931)

[CHƯƠNG 2: MỘT SỐ VẤN ĐỀ AN NINH CỦA HĐH LINUX 8](#_Toc446924932)

[2.1 An toàn hệ thống 8](#_Toc446924933)

[2.1.1 Bảo vệ môi trường vật lý 8](#_Toc446924934)

[2.1.2 Bảo mật truy cập vào hệ điều hành 9](#_Toc446924935)

[2.1.3 Vấn đề an ninh cơ bản của linux 10](#_Toc446924936)

[2.1.4 Một số công cụ bảo mật của linux 13](#_Toc446924937)

[2.2 Kiểm soát quyền truy cập người dùng 17](#_Toc446924938)

[2.2.1 To root or Not to root? 17](#_Toc446924939)

[2.2.2 Thực hiện một chính sách mật khẩu mạnh 20](#_Toc446924940)

[2.2.3 Sử dụng mật khẩu GRUB 21](#_Toc446924941)

[2.3 Bảo vệ tấn công chống lại mạng 22](#_Toc446924942)

[2.3.1 Giảm thiểu các lỗ hổng mạng 22](#_Toc446924943)

[2.3.2 Sử dụng TCP Wrappers 24](#_Toc446924944)

[Hình 2.1 Quy tắc hoạt động của TCP Wrappers 26](#_Toc446924945)

[2.3.3 Thực hiện mã hóa 27](#_Toc446924946)

[2.3.4 Thực hiện một bức tường lửa (Firewall) 28](#_Toc446924947)

[2.4 Phát hiện xâm nhập 32](#_Toc446924948)

[2.4.1 Phân tích tập tin đăng nhập Linux 32](#_Toc446924949)

[2.4.2 Thực hiện một hệ thống phát hiện xâm nhập (IDS) 34](#_Toc446924950)

[2.4.3 Thực hiện an kiểm toán với Tripwire 35](#_Toc446924951)

[CHƯƠNG 3: THỰC NGHIỆM 37](#_Toc446924952)

[3.1 Hướng dẫn cài đặt Ubuntu bằng USB 37](#_Toc446924953)

[3.2. Cài đặt hệ thống tường lửa IPtables 39](#_Toc446924954)

[3.3 Cài đặt phần mềm ClamTk thông qua Ubuntu Software Center 44](#_Toc446924955)

[3.4 Các lỗ hổng hiện nay và cách khắc phục 48](#_Toc446924956)

[3.4.1 Các lỗ hổng hiện nay 48](#_Toc446924957)

[3.4.2 Cách bảo vệ 54](#_Toc446924958)

[KẾT LUẬN 63](#_Toc446924959)

**DANH MỤC HÌNH ẢNH**

[Hình 1.1 Chú chim cánh cụt là biểu tượng quen thuộc của Linux 2](#_Toc446924923)

[Hình 1.2 Thành phần của HĐH Linux 3](#_Toc446924926)

[Hình 1.3 Cấu trúc của HĐH Linux 4](#_Toc446924928)

[Hình 2.1 Quy tắc hoạt động của TCP Wrappers 26](#_Toc446924945)

**KÝ HIỆU CÁC CỤM TỪ VIẾT TẮT**

* HĐH: hệ điều hành
* GNU: tổ chức Gnu’s Not Unix
* BSD: Berkeley Software Distribution
* FTP: File Transfer Protocol
* HTTP: HyperText Transfer Protocol
* IP: Internet Protocol
* TCP: Transmission Control Protocol
* GRUB: GRand Unified Bootloader

# 

# CHƯƠNG 1: TỔNG QUAN VỀ MỘT SỐ VẤN ĐỀ AN NINH HỆ ĐIỀU HÀNH LINUX

## Giới thiệu về hệ điều hành Linux

### Sơ lược về hệ điều hành Linux

#### Khái niệm

Linux còn được gọi là Open Source Unix (OSU).

Linux là một HĐH dạng Unix (Unix-like Operating System) chạy trên máy PC với bộ điều khiển trung tâm (CPU) intel 83086 trở lên, hay các bộ vi xử lý trung tâm tương thích ADM, Cyrix.

Một đặc điểm nổi bật của Linux là mã nguồn mở (Open Source) và hoàn toàn miễn phí dưới bản quyền của tổ chức GNU (Gnu’s Not Unix). Nó được sử dụng hiệu quả trong lĩnh vực tin học và những ứng dụng mới đang được xây dựng cho Linux mỗi ngày.

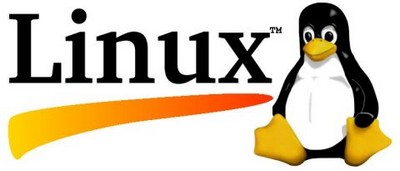
#### Hoàn cảnh lịch sử

Ngày 25/8/1991, Linus cho ra đời version 0.01 và thông báo trên comp.os.minix của Internet về dự án của mình.

Ngày 1/1992, Linus cho ra version 0.12 với shell và C compiler. Linus đặt tên hệ điều hành của mình là Linux.

Năm 1994, phiên bản chính thức 1.0 được phát hành.

Năm 1996, Linus Torvalds ghé thăm công viên hải dương học, tại đây, ông đã quyết định sử dụng hình ảnh chú chim cánh cụt để làm biểu tượng chính thức của Linux.



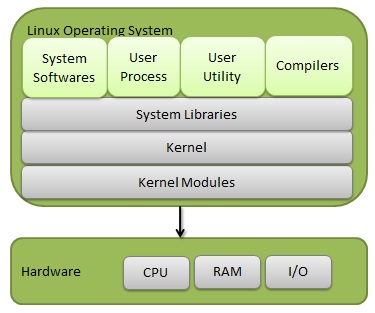
Hình 1.1 Chú chim cánh cụt là biểu tượng quen thuộc của Linux

### Đặc điểm cơ bản của Linux

* Linux có mã nguồn mở và hoàn toàn miễn phí
* Linux tương thích với nhiều HĐH
* Cho phép cài đặt Linux cùng với các HĐH khác trên cùng 1 ổ cứng.
* Do giữ được chuẩn của UNIX nên sự chuyển đổi giữa Linux và các hệ UNIX khác dễ dàng.
* Đa người dùng, đa chương trình và đa xử lý.
* Có giao diện đồ họa thừa hưởng từ hệ thống X-Window. Linux hỗ trợ nhiều giao thức mạng, bắt nguồn và phát trển từ dòng BSD. Thêm vào đó, Linux còn hỗ trợ việc tính toán thời gian thực
* Linux khá mạnh và chạy rất nhanh ngay cả khi có nhiều tiến trình và nhiều cửa sổ.
* Linux cung cấp sự bảo vệ sử dụng các tính năng xác nhận như mật khẩu bảo vệ/sự truy cập được kiểm soát tới các file đặc trưng.
* Linux rất ổn định ngay cả server Linux phục vụ những mạng lớn (hàng trăm máy trạm) cũng rất ổn định.

### Thành phần

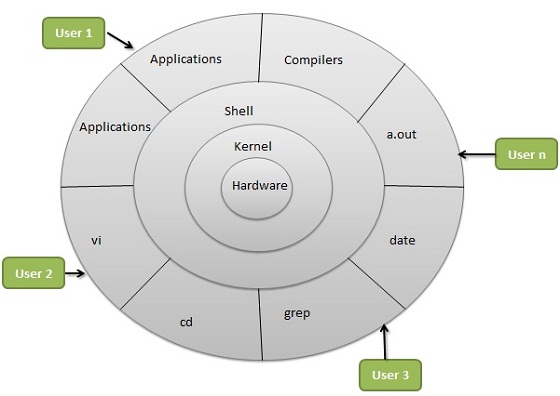
HĐH Linux đầu tiên có ba thành phần sau:



Hình 1.2 Thành phần của HĐH Linux

* **Kernel:** Là phần lõi của Linux. Nó có trách nhiệm cho tất cả các hoạt động của Hệ điều hành. Nó bao gồm các modun đa dạng và nó tương tác trực tiếp với phần cứng nằm bên dưới. Kernel cung cấp trạng thái cần thiết để che giấu các chi tiết phần cứng cấp thấp tới hệ thống hoặc các chương trình ứng dụng.
* **Thư viện hệ thống:** Là các chức năng đặc biệt hoặc chương trình sử dụng mà các chương trình ứng dụng hoặc các tiện ích hệ thống truy cập các tính năng của Kernel. Những thư viện này thực hiện hầu hết các chức năng của Hệ điều hành và không yêu cầu các quyền truy cập mã của modun hạt nhân.
* **Tiện ích hệ thống:** Các chương trình tiện ích hệ thống có trách nhiệm để thực hiện các nhiệm vụ mức độ đơn đặc biệt.

### Cấu trúc của HĐH Linux



Hình 1.3 Cấu trúc của HĐH Linux

Cấu trúc của hệ thống Linux gồm các lớp sau:

* **Lớp phần cứng:** bao gồm tất cả các thiết bị ngoại vi (RAM, I/O, CPU, HDD, …)
* **Kernel:** Thành phần lõi của Hệ điều hành, tương tác trưc tiếp với phần cứng, cung cấp các dịch vụ cấp thấp tới các thành phần lớp trên.
* **Shell:** Một giao diện tới kernel, ẩn giấu sự phức tạp của các chức năng của Kernel tới người sử dụng. Nhận các lệnh từ người sử dụng và thực hiện các tính năng của Kernel.
* **Các tiện ích:** Các chương trình tiện ích cung cấp cho người sử dụng hầu hết các tính năng của Hệ điều hành.

## Ưu điểm và nhược điểm của HĐH Linux

* **Ưu điểm:**
* Đây là một hệ điều hành miễn phí.
* Có khả năng đa chương đa nhiệm cùng lúc cho nhiều người sử dụng trên các phần cứng tương thích với PC của IBM.
* Nhiều ứng dụng cũng như mã nguồn hệ điều hành cũng được cung cấp miễn phí trên Internet, ta có thể tải về và cấu hình tuỳ theo sử dụng cá nhân.
* Linux giúp ta không bị ràng buộc về tính thương mại, giúp giảm bớt chi phí.
* Một tiện ích khác của Linux là gần như “miễn dịch” với các loại virus thông thường. Điều này rất lợi về mặt bảo mật.
* Linux có sẵn toàn bộ nghi thức mạng TCP/IP, giúp ta kết nối Internet và gửi thư điện tử dễ dàng.
* Hỗ trợ đa vi xử lý (Multi Processor Support) Linux có thể điều hành các hệ thống máy tính nhiều hơn một vi xử lý.
* Máy chủ (web server) Linux có thể được sử dụng để chạy như là một web server và đáp ứng các giao thức ứng dụng như HTTP hoặc FTP.  
  Linux có bao gồm hàng ngàn ứng dụng, bao gồm các bảng biểu, cơ sở dữ liệu, xử lí văn bản, ngôn ngữ điện toán…trò chơi, đồ hoạ…
* Với mã nguồn kernel (nhân) mở, khoá chuyển, điều này có ý nghĩa rằng linux có thể chạy trên nhiều loại CPU và phần cứng khác nhau hơn bất kỳ hệ điều hành nào.
* Tài liệu giới thiệu về linux ngày càng nhiều không thua kém bất cứ một Hệ điều hành khác.
* **Nhược điểm**
* Điều bất lợi lớn nhất của Linux là nó là 1 hệ điều hành với mã nguồn mở. Có thể nói đây là “đất dụng võ” của các tay hacker chuyên nghiệp.
* Không có một công ty nào chịu trách nhiệm phát triển hệ điều hành này cả.
* Linux thực sự không dễ cài đặt và dễ sử dụng như các hệ điều hành khác.
* Linux không dễ tương thích với một vài phần cứng nào đó. Có thể nói Linux không thể chạy trên tất cả mọi phần cứng của PC hiện nay.
* Ứng dụng mà ta đang sử dụng hệ điều hành như DOS, OS/2 sẽ không chạy được với Linux.
* Thiếu chuẩn hóa: Do Linux toàn miễn phí nên bất cứ ai thích đều có thể tự mình đóng gói, phân phối theo cách của mình. Có hàng chục nhà phân phối khác nhau trên thị trường, người dùng trước khi cài đặt thường phải tự mình so sánh để tìm ra sản phẩm thích hợp.

## So sánh HĐH Linux và Windows

|  |  |  |
| --- | --- | --- |
|  | Linux | Windows |
| Ưu điểm | Tốc độ nhanh, không đòi hỏi cấu hình máy cao. | Đòi hỏi cấu hình máy cao. Giao diện 3D đẹp mắt, chuyển đổi nhanh giữa các cửa sổ, tính năng search mạnh. |
| Nhược điểm | Giao diện đơn giản do đã lượt bớt để tối ưu hóa, không có chức năng ‘plug and play’. | Nhiều chương trình hện vẫn chưa tương thích với một số phiên bản Windows là một nguyên nhân khiến nhiều người dùng không muốn sử dụng. |
| Giá cả | Miễn phí | Tốn phí khá cao |
| Khả năng chống virus | Ít và hầu như không bị ảnh hưởng của virus. Phần mềm Aegis Virus Scanner tích hợp sẵn có thể chạy ở chế độ nền | Bạn cần phải mua một vài phần mềm chống virus. |
| Audio | Có đầy đủ các tính năng chơi nhạc, rip nhạc bằng sound juicer, rhythmbox thực hiện chức năng tổ chức và nghe internet radio,serpentine để burn CD và sound recorder để ghi âm. | Tốt hơn Linux, phiên bản Windows media Player mới cho phép bạn rip CD mua các bản nhạc mới và liên kết tới một Mp3 player. |

## Các phiên bản Linux phổ biến

* Một số phiên bản phổ biến nhất của Linux: Ubuntu, Fedora, Redhat, Open SUSE, Debian, Linux Mint, Turbo Linux, Mandriva Linux, Puppy Linux, Arch Linux cùng với Slackware, PCLinuxOS, …. Nhưng thông dụng nhất hiện nay đang là Ubuntu.

# CHƯƠNG 2: MỘT SỐ VẤN ĐỀ AN NINH CỦA HĐH LINUX

Bảo mật máy tính là một chủ đề rộng và sâu. Có rất nhiều khía cạnh khác nhau của bảo mật máy tính như mã hóa để xác thực, tạo bức tường lửa để hệ thống phát hiện xâm nhập. Hệ thống an ninh mạnh thường cung cấp sự bảo vệ mạnh mẽ cho vấn đề riêng tư của cá nhân và doanh nghiệp.

## 2.1 An toàn hệ thống

An toàn hệ thống bao quanh việc chọn phân phối hệ điều hành Linux, xây dựng kernel, an toàn tài khoản người dùng, cho phép truy cập thư mục tập tin….

### 2.1.1 Bảo vệ môi trường vật lý

#### 2.1.1.1 Máy chủ

Hạn chế những người có thể truy cập vào hệ thống, mức độ truy cập phụ thuộc vào loại hệ thống tham gia. Máy chủ server nên có mức độ bảo mật cao nhất về thể chất, phải đảm bảo không có ai từ cộng đồng có thể truy cập vào các máy chủ. Không nên giữ máy chủ trong một phòng hoặc trên bàn quản trị viên mà nên giữ trong một phòng máy chủ được khóa chỉ người quản trị hệ thống và một số người khác có thể truy cập.

Bạn nên đánh giá tình hình của mình và xem làm thế nào cho người khác khó có được quyền truy cập vào máy chủ của bạn.

#### 2.1.1.2 Máy con

Bảo vệ quyền truy cập vào các máy con thì gặp nhiều khó khăn hơn so với máy chủ. Vấn đề chính là việc sử dụng rộng rãi trong các phòng nhỏ trong môi trường làm việc hiện nay thì bất kỳ ai tiếp cận với văn phòng cũng có quyền truy cập vào hệ thống máy tính của tất cả mọi người. Điều này cho phép một kẻ xâm nhập giả dạng vào văn phòng và đi ra với một hệ thống máy con. Nếu làm đúng, họ thậm chí sẽ không gặp khó khăn gì khi đi ra ngoài. Ta có thể bảo vệ máy con và máy chủ của tổ chức bằng cách đảm bảo quyền truy cập vào HĐH.

### 2.1.2 Bảo mật truy cập vào HĐH

Sau khi đảm bảo quyền truy cập vào hệ thống máy tính, tiếp theo là bảo vệ các điều khiển truy cập được xây dựng trong HĐH Linux.

Linux sử dụng tài khoản người dùng và mật khẩu để kiểm soát những ai có thể thao tác với hệ thống, đây là một điều tốt. Tuy nhiên, trong một ngày, người sử dụng liên tục đến và đi khỏi nơi làm việc hoặc văn phòng của họ. Ví dụ như: người dùng có các cuộc họp, nghỉ ngơi, đi ăn trưa, và sử dụng nhà vệ sinh,…. Lúc đó kẻ xâm nhập dễ dàng tìm thấy một hoặc nhiều máy con đăng nhập mà không có ai giám sát, và khi đó chỉ mất ít thời gian để sao chép dữ liệu quan trọng vào ổ đĩa flash! Hay tệ hơn, kẻ xâm nhập có thể tải bất kỳ một chương trình nào đó vào hệ thống, chẳng hạn như phần mềm key-logging hoặc virus. Biện pháp để khắc phục điều đó là ta nên đặt mật khẩu bảo vệ màn hình, thoát hoặc khóa máy con kể cả trong những thời gian ngắn nhất.

Hầu hết các Linux desktop đồ họa cung cấp các môi trường tùy chọn khóa HĐH. Nếu bạn đang sử dụng một môi trường dựa trên văn bản, thì nên đăng xuất khi rời khỏi bàn làm việc và sau đó đăng nhập lại khi trở về. Và không bao giờ để lại một máy chủ đăng nhập nếu bạn không sử dụng các máy chủ giao diện điều khiển, đăng xuất.

Nhiều người sử dụng đặc biệt là các nhà phát triển phần mềm, muốn nghỉ ngơi trong khi hệ thống Linux đang làm việc trên một nhiệm vụ lớn, chẳng hạn như biên soạn chương trình, tải về một cập nhật cơ sở dữ liệu… Để cho phép người dùng đăng xuất mà lại không giết chết một quá trình quan trọng, bạn có thể sử dụng lệnh nohup để bước đầu tải nó. Bất kỳ quá trình nạp bởi nohup sẽ bỏ qua bất kỳ tín hiệu treo lên nó nhận được, chẳng hạn như những người gửi khi đăng nhập từ một dấu nhắc trình báo, tên & lệnh đã được nạp bằng cách sử dụng nohup, cho phép nó chạy ngay cả khi đã đăng xuất.

### 2.1.3 Vấn đề an ninh cơ bản của linux

An ninh là một built-in (và không phải là một bolt-on) tính năng và kéo dài ngay từ hạt nhân Linux cho máy tính để bàn. An ninh cần phải được làm việc trên hệ thống và cả cá nhân.

Linux có thể hạn chế sự xâm nhập của virus. Nhưng những kẻ tấn công có rất nhiều thủ đoạn để đến các bit và byte tạo nên mọi thứ từ Mugshot của bạn đến các chi tiết như thẻ tín dụng của bạn.

Các máy tính kết nối với internet là nơi có nhiều người tiếp xúc và dễ tấn công nhất, mặc dù các máy tính dễ bị xâm nhập nhưng không bao giờ ta có thể nhìn thấy được các hành động đó.

Đừng nghĩ rằng máy tính xách tay cũ hoặc đĩa cứng cũ chỉ cần bỏ đi thì các dữ liệu sẽ mất. Với các loại công cụ phục hồi dữ liệu ngày nay (hầu như được download miễn phí) nó không có vấn đề gì đối với HĐH được cài đặt trên đĩa. Nó có thể phục hồi dữ liệu và lấy dữ liệu ra, ví dụ tái tạo tài khoản ngân hàng, tái tạo bảng trò chuyện, hình ảnh…. Trong khi đó hầu như không thể làm cho một máy tính kết nối với internet trở nên bất khả xâm phạm, không thể tấn công. Nhưng với Linux, và một số phần mềm mã nguồn mở, nó không mất nhiều nỗ lực để bảo đảm cài đặt của bạn an toàn. Không có quy tắc vàng cho an ninh được áp dụng trong mọi trường hợp, và thậm chí nếu có nó sẽ bị nứt hay có những lỗ hổng.

Những nguyên nhân chính cho vấn đề bảo mật trong Linux

* **An ninh địa phương:** Người địa phương có thể tạo ra rất nhiều vấn đề cho hệ thống của bạn. Không cung cấp tài khoản cho những người mà bạn không biết hoặc không có thông tin liên lạc để đăng nhập vào hệ thống của bạn. Khi cung cấp tài khoản truy cập vào máy Linux của bạn thì nên: cung cấp cho người sử dụng đặc quyền tối thiểu, theo dõi khi nào và nơi nào họ đăng nhập, xóa các tài khoản không hoạt động và ngăn cấm việc tạo ra các ID người dùng nhóm.
* **An ninh root:**Kể cả khi tài khoản root có thẩm quyền trên toàn bộ máy, bạn nên sử dụng nó chỉ cho các nhiệm vụ cụ thể. Ngay cả một sai lầm nhỏ thực hiện trong khi đăng nhập như là một người sử dụng root có thể dẫn đến các vấn đề quan trọng. Nên thực hiện các quy tắc đơn giản sau:
* Khi chạy lệnh phức tạp, đầu tiên chạy chúng một cách không phá hủy. Một ví dụ đơn giản là làm một 'ls' trước khi làm một 'rm' để chắc chắn về các tập tin bạn đang xóa.
* Cung cấp cho người dùng một rm tương tác để xóa các tập tin.
* Trở thành root chỉ để làm nhiệm vụ cụ thể. Nếu bạn muốn thử nghiệm một cái gì đó, quay trở lại với vỏ dùng bình thường.
* Đường dẫn lệnh, xác định các thư mục trong đó, tìm kiếm vỏ cho các chương trình, là rất quan trọng. Hạn chế các đường lệnh và không bao giờ bao gồm '.' (Nghĩa thư mục hiện hành) trong đường dẫn lệnh của bạn.
* Các file / etc / securetty chứa một danh sách các thiết bị đầu cuối mà người chủ có thể đăng nhập. Hãy cẩn thận trong khi thêm một mục vào tập tin này.
* **An ninh hệ thống tập tin:**Nếu bạn đang xuất các hệ thống tập tin sử dụng NFS, cấu hình /etc /xuất với các truy cập hạn chế nhất có thể.Không sử dụng bất kỳ ký tự đại diện nào. / Var / log / wtmp và / var / run / utmp chứa những nỗ lực đăng nhập cho tất cả người dùng. Sự toàn vẹn của họ cần phải được duy trì, như họ giúp đỡ trong việc quyết định khi nào và từ đâu một người dùng đã nhập vào hệ thống của bạn. Không bao giờ thay đổi sự cho phép trên một tập tin chỉ vì nó là cách dễ dàng để có được những thứ cần thiết để làm việc.
* **An ninh hạt nhân:**Như hạt nhân điều khiển mạng của máy tính, nó là điều cần thiết để giữ cho máy tính an toàn. Hãy nhìn vào một số tùy chọn cấu hình hạt nhân phổ biến có liên quan đến an ninh.
* **Quyền tập tin:**Hãy chắc chắn rằng các tập tin hệ thống của bạn không được mở để chỉnh sửa bởi người dùng và nhóm người không có quyền thích hợp. Hệ điều hành Linux phân biệt sự kiểm soát truy cập dựa trên ba đặc điểm: sở hữu, nhóm và khác. Truy cập vào một tập tin sẽ được xác định bởi bit quyền và những thứ này là 'rwx' xác định nơi, 'r' xác định 'đọc', 'w' xác định "viết" và "x" xác định 'thực'. Bạn có thể thiết lập lại ba bit quyền dựa vào loại truy cập mà bạn đang quan tâm đến cho một người sử dụng. Đây được coi là mức độ căn bản ngăn chặn truy cập vào một tập tin từ các nguồn trái phép.
* **Kiểm tra toàn vẹn:**Có một cơ chế rất tốt để phát hiện các cuộc tấn công cục bộ trên hệ thống của bạn. Những người kiểm tra tính toàn vẹn sẽ chạy một số tổng kiểm tra trên tất cả các tập tin nhị phân quan trọng và các tập tin cấu hình và so sánh chúng với một cơ sở dữ liệu cụ thể, các giá trị được biết đến như một tài liệu tham khảo. Do đó bất kỳ thay đổi trong các tập tin có thể dễ dàng bị gắn cờ. Dựa trên những tín hiệu này, người quản trị hệ thống có thể thực hiện thay đổi phù hợp để bảo vệ các tập tin quan trọng .
* **Bảo mật mật khẩu:**Hầu hết các bản phân phối Linux đi kèm với chương trình 'password' không cho phép bạn thiết lập một mật khẩu có thể dễ dàng đoán ra. Vì vậy, nó là cần thiết để đảm bảo rằng chương trình password của bạn được cập nhật. Linux sử dụng một thuật toán mã hóa một chiều gọi là DES (Data Encryption Standard), được sử dụng để mã hóa mật khẩu của bạn. Các mật khẩu được mã hóa được lưu trữ trong / etc / passwd. Khi bạn cố gắng đăng nhập, mật khẩu bạn gõ lại được mã hóa và được so sánh với các mục trong tập tin lưu trữ mật khẩu của bạn.
* **Triển khai bảo mật khác:** Một xem xét ở đây là việc thực hiện của IPSEC cho Linux. IPSEC là một cơ chế để tạo ra thông tin liên lạc mã hóa an toàn ở cấp độ mạng IP. Ý tưởng chính ở đây là để cung cấp xác thực, tính toàn vẹn, kiểm soát truy cập và bảo mật thông tin của bạn.
* **Nguyên tắc bảo mật:** An ninh nhất thiết phải đặt ở đầu tiên. Vấn đề bảo mật có thể đến từ những người tích cực cố gắng thâm nhập vào bảo mật của bạn hoặc từ những vấn đề đơn giản như một người nào đó cung cấp đầu vào bất ngờ cho một chương trình hoặc chạy một số lệnh sai. Quá nhiều quyền truy cập vào hệ thống có thể có nghĩa là người sử dụng - ngay cả với truy cập hợp pháp - có thể gây rắc rối, hoặc là vô tình hay cố ý.
* **Có thể giảm thiểu các tác động nếu một kẻ xâm nhập cố gắng để tấn công hệ thống của bạn bằng cách sau:**
* Hãy chắc chắn rằng toàn bộ hệ thống của bạn được sao lưu.
* Chọn một lịch trình sao lưu tốt.
* Hãy chắc chắn rằng bạn kiểm tra các bản sao lưu của bạn để đảm bảo rằng chúng đang làm việc như bạn mong đợi.
* Áp dụng tất cả các hệ thống mới cập nhật nhanh chóng để mọi thứ được cập nhật.
* Theo dõi các dữ liệu hệ thống kế toán. Hãy chắc chắn rằng các tập tin trong thư mục / var / log đã đọc và ghi chỉ truy cập vào một số giới hạn của người sử dụng.

### 2.1.4 Một số công cụ bảo mật của linux

#### 2.1.4.1 Khả năng tấn công từ chối và hệ thống kiểm soát truy cập

Một tiền đề cơ bản đằng sau tất cả các hệ thống an ninh là có thể bảo vệ các bộ phận của hệ thống ngay cả khi các bộ phận khác đã bị xâm nhập bởi kẻ trộm. Hệ thống kiểm soát truy cập cung cấp một cơ chế để đảm bảo rằng người dùng hoặc chương trình chỉ được uỷ quyền có quyền truy cập với những gì họ được phép có. Hệ thống khả năng đảm bảo rằng một người dùng hoặc chương trình có thể thực hiện chỉ có những hành động mà họ được phép thực hiện. Hầu hết các hệ thống an ninh cung cấp kết hợp khả năng kiểm soát và truy cập, nhấn mạnh với mức độ nhiều hay ít.

* VServer : Các dự án Linux-Vserver thúc đẩy các chroot hạt nhân Linux hiện có và khả năng và cho biết thêm các khái niệm trừu tượng của một " bối cảnh an ninh" để tạo ra một hệ thống an ninh rất đơn giản nhưng rất mạnh mẽ. Gồm 3 yếu tố cơ bản:
* Các bối cảnh an ninh: Một quá trình trong một bối cảnh an ninh không thể nhìn thấy các quá trình trong bối cảnh an ninh khác, không phải bằng lệnh 'ps', cũng không phải với 'cat / proc' cũng không phải trong bất kỳ cách nào khác. Như tác dụng phụ, điều này có nghĩa là một quá trình trong một bối cảnh không có thể giết các quy trình trong các bối cảnh khác.
* Khả năng: Các hạt nhân Linux hiện có cung cấp một loạt các khả năng có thể được lấy đi từ các quá trình. Chúng bao gồm các khả năng để thay đổi địa chỉ mạng, để thay đổi quyền sở hữu của một tập tin, vv (Xem /usr/include/linux/capability.h để biết chi tiết.) Các vserver-utils cung cấp một công cụ để lấy đi khả năng từ một quá trình.
* Các nhà tù Chroot: Các hạt nhân Linux hiện có cung cấp một cách để hạn chế một quá trình để một thư mục con, bằng cách thay đổi “hệ thống rễ file” cho quá trình này là thư mục con. Kể từ khi một quá trình không thể “vượt ra khỏi root”, nó chỉ đơn giản là không thể truy cập bất cứ điều gì bên ngoài thư mục con.
* Những yếu tố này có thể được sử dụng riêng lẻ hoặc có thể được kết hợp để tạo ra các môi trường máy chủ ảo hoàn toàn độc lập đó là hoàn toàn vô hình với nhau, nhưng cùng tồn tại trên một máy duy nhất.
* Quy tắc thiết lập dựa trên Access Control (RSBAC) dành cho Linux: RSBAC thực hiện các Abrams và LaPadula khái quát hóa khung điều khiển truy cập (GFAC) trong lớp thấp nhất của nó. Các khuôn khổ thực thi các quyết định truy cập tại/ gần lớp gọi hệ thống quyết định truy cập dựa trên một quadruplet (loạitruy cập, mục tiêu truy cập, các thuộc tính về đề tài, các thuộc tính của đối tượng). Bằng cách cung cấp một khuôn khổ thuộc tính, RSBAC có thể thực hiện một loạt các mô hình chính sáchMAC, mỗi moduleriêng của mình.
* Tăng cường bảo mật Linux Security-Enhanced Linux(SeLinux): Các mô-đun thực thi thực hiện điều này bằng cách gán nhãn an ninh cho từng đối tượng. Nó sử dụng một lớp bảo mật để xác định các loại mối quan hệ một cặp nhãn có thể có. Các bộ ba bao gồm một cặp nhãn và một lớp học này sau đó được gửi đến một máy chủ chính sách để xác định nếu được phép truy cập.
* William & Mary DTE: Tên miền và kiểu thực thi dành cho Linux là một nghiên cứu của DTEban đầu từ các trường Cao đẳng William và Mary, dường như là một dự án phát triển tích cực, mặc dù có vẻ không nhiều cộng đồng người dùng. Mã là GPL'ed. Tích hợp với các mã Linux Security Modules. Bao gồm một mô-đun cấu hình PAM, và một tiện ích cấu hình đồ họa.
* Medusa DS9: Cung cấp một cơ chế để thực hiện các chức năng bảo mật nói chung, bao gồm cả MAC. Nó được thực hiện như một bản vá hạt nhân Linux nhỏ cung cấp một giao diện dịch vụ cho một trình an ninh không gian người dùng. Trình an ninh này thực hiện phần lớn các chức năng bảo mật mong muốn, bao gồm cả các quyết định chính sách, giữ các chi tiết ra của hạt nhân. Hiện nay, một daemon chính sách gọi là"constable" đã được triển khai hoạt động như một máy chủ ủy quyền.
* Phát hiện xâm nhập / Hệ thống Quốc phòng (Nắp): nắp đậy có vẻ là một mish-mash của các công cụ khác nhau không có mục tiêu rõ ràng, chức năng không rõ ràng, và không có nền tảng lý thuyết. Điều này làm cho nó khó hiểu những gì hệ thống thực sự có khả năng, cho dù nó hoàn toàn thực hiện một phần.
* Remus: Các Remus Linux Kernel Module can thiệp vào hệ thống giao diện cuộc gọi để thực hiện chức năng kiểm soát truy cập của nó. Remus cố gắng để hạn chế quá trình gốc có đặc quyền vàtrung gian sử dụng các cuộc gọi hệ thống bảo mật có liên quan. Người quản trị có thể cấu hình Remus để cho phép quá trình giới hạn để làm cho chỉ số cuộc gọi với các thông số nhất định. Remus dường như được định hướng vào nhận thấy hệ thống sử dụng bình thường.
* FreeVSD : FreeVSD là một cơ sở hạ tầng máy chủ ảo chroot. Cho phép nhiều máy chủ độc lập được thành lập, mỗi địa chỉ riêng của mình độc lập IP, quản trị riêng của nó, …

#### 2.1.4.2 Các công cụ không miễn phí hệ thống kiểm soát truy cập

* Immunix tên miền phụ: Tên miền phụ Immunix từ WireX thực hiện một hình thức MACtương tự như DTE, cấu hình của nó vẫn giữ qƯuan điểm của tên miền, nhưng không sử dụng cácloại. Tên miền phụ không tận dụng chuẩn chroot Linux để giúp cô lập giữa các lĩnh vực. Nó làm cho việc sử dụng một bản vá hạt nhân GPL, các công cụ cấu hình Userland là độc quyền.
* VXE: VXE các execution môi trường ảo, thực hiện một compartmentalized, máy chủ ảo môi trường MAC. Nó thực thi các nguyên tắc đặc quyền tối thiểu của các quá trình(như máy chủ có đặc quyền) để các môi trường ảo mà trong đó chỉ có tối thiểu các nguồn lực cần thiết cho hoạt động bình thường có sẵn. VXE môi trường ảo được thực hiện trong LKMs và hoạt động với sự giúp đỡ của một bản vá hạt nhân Linux. Kể từ những môi trường ảo có thể được thiết kế đặc biệt cho các nhu cầu tài nguyên của một ứng dụng cụ thể, VXE cung cấp hỗ trợ hạt mịn để hạn chế các ứng dụng để đặc quyền tối thiểu.
* PitbullLX: PitbullLX thực hiện một hình thức của tên miền và kiểu thực thi(DTE), mặc dù nó xuất hiện để làm mờ sự phân biệt giữa các lĩnh vực và các loại(chủ thể và đối tượng), đề cập đến tất cả mọi thứ như là một "tên miền", chế độ truy cập là rwx(đọc, viết thực hiện). Nó bao gồm một Kernel ModuleLinux(LKM), một modulePAM, và các tập tin cấu hình. Các quy tắc truy cập để liên kết với nhau lĩnh vực giống quy tắc tường lửa.

#### **2.1.4.3 Công cụ phát hiện xâm nhập**

* Tripwire sẽ dò tìm tập tin sửa đổi (các tập tin mà người quản trị hệ thống được mong đợi không thay đổi, chỉ ra rằng một kẻ xâm nhập có thể đã cài đặt một con ngựa Trojan, backdoor, vv)
* Psionic cung cấp bản ghi sát các công cụ (phát hiện xâm nhập) chống cổng-sniffing. Port-sniffing thường là giai đoạn đầu tiên của một cuộc tấn công chống lại một trang web: các cracker đang cố gắng để tìm ra những cảng và dịch vụ được mở trên máy tính bị tấn công. Phát hiện khi một cracker là quan tâm đến trang web của bạn là một trong những bước đầu tiên trong một phản ứng tích cực để ngăn chặn sự cố trong tương lai.
* Snort là một hệ thống phát hiện xâm nhập GPL với một số giám sát giao thông và phát hiện tính năng. Chạy trên hầu hết Unix và cũng Win32 / 95/98/00.
* Remus có thể phát hiện không thích hợp sử dụng hệ thống gọi, chỉ ra rằng một kẻ xâm nhập đã bị phá vỡ trong, và đang thực hiện những nỗ lực để đạt được quyền truy cập và cơ quan chức năng tiếp tục.

## **2.2 Kiểm soát quyền truy cập người dùng**

Một khía cạnh quan trọng của cả hai máy trạm Linux và máy chủ bảo mật Linux là thực hiện và kiểm soát truy cập người dùng để hạn chế những gì người dùng có thể làm với hệ thống.

* **Root hoặc không root?**
* **Thực hiện một chính sách mật khẩu mạnh**
* **Sử dụng một mật khẩu GRUB**

### 2.2.1 To root or Not to root?

Mỗi hệ thống Linux, cho dù một máy trạm hoặc một máy chủ, bao gồm một tài khoản mặc định của siêu người dùng có tên gốc. Điều này tài khoản có quyền truy cập đầy đủ đến mọi khía cạnh của hệ thống. Như vậy nó nên được sử dụng với sự chăm sóc tuyệt vời.

* Sử dụng hợp lý các tài khoản người dùng root
* Sử dụng câu lệnh su
* Sử dụng câu lệnh sudo

#### 2.2.1.1 Sử dụng hợp lí tài khoản người dùng root

Một trong những sai lầm quan trọng do người mới dùng Linux là sử dụng quá nhiều tài khoản người dùng root. Có thời gian và địa điểm khi các tài khoản người dùng root nên được sử dụng.

Tuy nhiên, hầu hết các công việc của bạn trên một hệ thống Linux nên được thực hiện như là một người sử dụng không phải root. Các quy tắc mà bạn nên làm theo là:

* Chỉ sử dụng root khi tuyệt đối cần thiết.
* Nếu một nhiệm vụ có thể được hoàn thành khi một người sử dụng không phải root, thì nó nên được làm như vậy.

Tại sao sử dụng hợp lý tài khoản người dùng root là mối quan tâm?

Nguy cơ để lại của một hệ thống đăng nhập không được giám sát. Hãy tưởng tượng một sự tàn phá mà kẻ xâm nhập có thể gây ra nếu người đó xuất hiện trên hệ thống không được giám sát mà đã đăng nhập như là người chủ! Tất cả các dữ liệu trên hệ thống có thể được truy cập và sao chép. Thay đổi cấu hình chính có thể được thực hiện để cho các daemon chạy trên hệ thống. Và chúng ta không thể biết loại phần mềm độc hại nào có thể được cài đặt.

Tóm lại, hệ thống đăng nhập trong root đại diện cho 1 rủi ro bảo mật nghiêm trọng. Rời một hệ thống không được giám sát như vậy đại diện cho một nguy cơ bảo mật quan trọng. Tất cả mọi người, bao gồm cả các quản trị hệ thống nên có một tài khoản người dùng chuẩn mà bạn luôn luôn sử dụng để đăng nhập vào hệ thống.

Nếu bạn thấy rằng bạn cần truy cập mức độ root trong khi làm việc trên hệ thống, bạn có thể sử dụng dòng lệnh su.

#### 2.2.1.2 Sử dụng câu lệnh su

Lệnh này cho phép thay đổi tài khoản người dùng khác tại dấu nhắc shell. Cú pháp sử dụng su là **su\_ tùy chọn tài khoản người dùng**. Nếu không có tài khoản người dùng được xác định trong lệnh, **lệnh su** sẽ giả sử bạn muốn chuyển sang người dùng tài khoản root. Một số tùy chọn hữu ích bạn có thể sử dụng với su như sau:

Nạp các biến trong môi trường của người sử dụng. Chú ý rằng chúng ta đã luôn luôn sử dụng các dòng lệnh Su để chuyển sang tài khoản người dùng root. Điều này sẽ thay đổi root và nạp các biến trong môi trường của root.

* **–c *command*** Chuyển sang tài khoản người dùng và chạy các lệnh xác định.
* **–m** Chuyển sang tài khoản người dùng, nhưng vẫn bảo vệ môi trường hiện tại của các biến.

Sử dụng sudo để cung cấp cho họ quyền truy cập root hạn chế.

#### 2.2.1.3 Sử dụng câu lệnh sudo

Giả sử bạn có một người sử dụng trên hệ thống Linux của bạn. Thành viên này có thể là một lập trình viên, một người quản lý dự án, hoặc một quản trị cơ sở dữ liệu. Người sử dụng trong thể loại này có thể thường xuyên cần chạy một số lệnh cấp độ root. Nhưng bạn có thực sự muốn cho họ mật khẩu root của bạn? Chắc là không. Bạn muốn họ có thể chạy giới hạn ở một số dòng lệnh yêu cầu đặc quyền root, nhưng bạn không muốn họ có đầy đủ quyền truy cập root. Điều này có thể được thực hiện bằng cách sử dụng **lệnh sudo.**

Các lệnh sudo cho phép người dùng chạy một lệnh như một tài khoản người dùng khác. Như với **su**, nó có thể là bất kỳ tài khoản người dùng nào trên hệ thống. Tuy nhiên, đó thường là được sử dụng để chạy các lệnh như là root. Các lệnh sudo sử dụng tập tin / etc / sudoers để xác định những người dùng được ủy quyền để chạy những lệnh đó. Tập tin này sử dụng những bí danh sau đây để xác định người nào có thể làm những gì:

* User\_Alias: Chỉ định những người dung nào được phép chạy các lệnh.
* Cmnd\_Alias: Chỉ định các lệnh mà người dùng được phép chạy.
* Host\_Alias: Chỉ định chủ người dùng được phép chạy các lệnh trên.
* Runas\_Alias: Chỉ định tên người dùng mà các lệnh có thể được chạy.

Để chỉnh sửa tập tin / etc / sudoers của bạn, bạn cần phải chạy lệnh visudo như người dùng root của bạn

Tập tin / Etc / sudoers được tải vào trong trình soạn thảo mặc định của bạn, mà thường là vi. Thay đổi của bạn được ghi vào /etc/sudoers.tmp cho đến khi cam kết.

### 2.2.2 Thực hiện một chính sách mật khẩu mạnh

Một mật khẩu yếu kém là một mật khẩu có thể dễ dàng được đoán ra hoặc bẻ gãy. Đây là vài ví dụ:

* Tên của bạn
* Tên của người vợ hoặc chồng
* Tên thật của mẹ bạn
* Tên của con bạn
* Sinh nhật của bạn
* Tên của con vật cưng của bạn
* Bất kỳ từ ngữ có thể được tìm thấy trong từ điển
* Sử dụng "mật khẩu" cho mật khẩu của bạn
* Mật khẩu đơn ký tự
* Mật khẩu trống

Một mật khẩu mạnh:

* Sử dụng sáu ký tự hoặc nhiều hơn
* Sử dụng số bên cạnh những kí tự
* Sử dụng chữ in hoa và chữ thường
* Sử dụng từ ngữ không có trong từ điển

Ngoài ra, bạn cũng nên cấu hình tài khoản người dùng của bạn như là mật khẩu của bạn sẽ hết hạn sau một thời gian nhất định nào. Điều này được gọi là tuổi thọ mật khẩu. Tại sao mật khẩu lại có thời hạn? Nhiều hơn một người sử dụng có cùng mật khẩu, nhiều khả năng nó là được thỏa hiệp. Bằng cách buộc người sử dụng đổi mật khẩu định kỳ, giữ cho những kẻ xâm nhậpkhông thể đoán được. Thậm chí nếu họ tìm được cách để có được mật khẩu của người sử dụng, nó cũng sẽ được trả lại vô dụng tại một số điểm. Nhiều tổ chức quan tâm về an ninh thì nên tạo một password có hạn dùng là 30 ngày. Tổ chức ít hoang tưởng hơn có thể sử dụng một mật khẩu có hạn dùng là 60 hoặc thậm chí 90 ngày.Bạn có thể cấu hình tuổi thọ cho các mật khẩu của bạn bằng cách sử dụng **lệnh chage**. Cú pháp cho việc sử dụng lệnh change là **change\_ tùy chọn người dùng**. Bạn sử dụng các tùy chọn sau đây với chage:

* –m days: Xác định số ngày tối thiểu giữa những lần thay đổi mật khẩu.
* –M days: Xác định số ngày tối đa giữa những lần thay đổi mật khẩu.
* –W days: Xác định số lượng ngày được yêu cầu cảnh báo trước khi thay đổi mật khẩu.

Ngoài ra, hệ thống Linux của bạn không nên được cấu hình để lưu trữ mật khẩutrong file / etc / passwd. Nhiều tiến trình đang chạy trong hệ thống cần truy cập/ etc / passwd để hoàn thành những nhiệm vụ khác nhau.Lưu trữ mật khẩu của bạn trong đó sẽ phơi bày hồ sơ chúng tới các quá trình và mở ra một lỗ hổng bảo mật nghiêm trọng.Hầu hết những người làm việc trên hệ thống nhận ra rằng lưu trữ mật khẩu trong / etc / passwd là một ý tưởng rất xấu.Tuy nhiên, nếu bạn chạy trong một hệ thống như vậy, bạn có thể sử dụng lệnh pwconv để di chuyển mật khẩu người dùng ra khỏi / Etc / passwd và vào / etc / shadow.

### 2.2.3 Sử dụng mật khẩu GRUB

Bạn cũng nên xem xét thực hiện một mật khẩu GRUB trên hệ thống Linux của bạn.

Một trong những điểm yếu an ninh của GRUB là thực tế rằng một người không được phép thao tác và tùy chỉnh menu GRUB, để khởi động hệ thống vào runlevel 1 (chế độ người dung đơn). Với một số bản phân phối, điều này sẽ được hệ thống khởi động và mở một shell đăng nhập như là người chủ, mà không đòi hỏi phải có một mật khẩu!

Một số sẽ yêu cầu nhập mật khẩu root của bạn. Số khác cho phép bạn đăng nhập sử dụng bất kỳ tài khoản người dung nào trong runlevel 1.

Với một mật khẩu GRUB, người dùng phải xác thực trước khi họ có thể sử dụng tùy chọn khởi động trong menu khởi động GRUB. Bạn thậm chí có thể yêu cầu họ nhập vào một mật khẩu để chọn một trình mục đơn. Để thêm một mật khẩu GRUB, thực hiện các thao tác sau:

1. Mở terminal session và su – to root.

2. Tại dấu nhắc shell, nhập grub.

3. Mã hóa mật khẩu trong vỏ GRUB bằng cách nhập md5crypt tại dấu nhắc grub

4. Tại dấu nhắc Password, nhập mật khẩu mà bạn muốn sử dụng.

5. Nhập **quit** tại dấu nhắc grub.

6. Mở tập tin /boot/grub/menu.lst của bạn trong một trình soạn thảo văn bản.

7. Bên dưới chỉ dẫn gfxmenu, thêm như sau:

password --md5 hashed\_password

8. Lưu file và thoát khỏi trình soạn thảo.

Bây giờ người dùng sẽ phải nhấn P và nhập mật khẩu trong màn hình menu GRUB để tùy chọn cấu hình khởi động. Bạn cũng có thể cấu hình GRUB để yêu cầu mộtmật khẩu để khởi động từ bất kỳ tùy chọn menu GRUB. Điều này được thực hiện bằng cách thêm khóa để cuối mỗi mục menu mà bạn muốn khóa xuống, như trong những ví dụ sau đây:

title linux

kernel (hd0,4)/boot/vmlinuz root=/dev/sda5 vga=791

initrd (hd0,4)/boot/initrd

lock

## 2.3 Bảo vệ tấn công chống lại mạng

Một số vấn đề cơ bản có thể làm để bảo vệ chống lại các cuộc tấn công mạng là

* Giảm thiểu các lỗ hổng mạng
* Sử dụng TCP Wrappers
* Thực hiện mã hóa
* Thực hiện một bức tường lửa

### 2.3.1 Giảm thiểu các lỗ hổng mạng

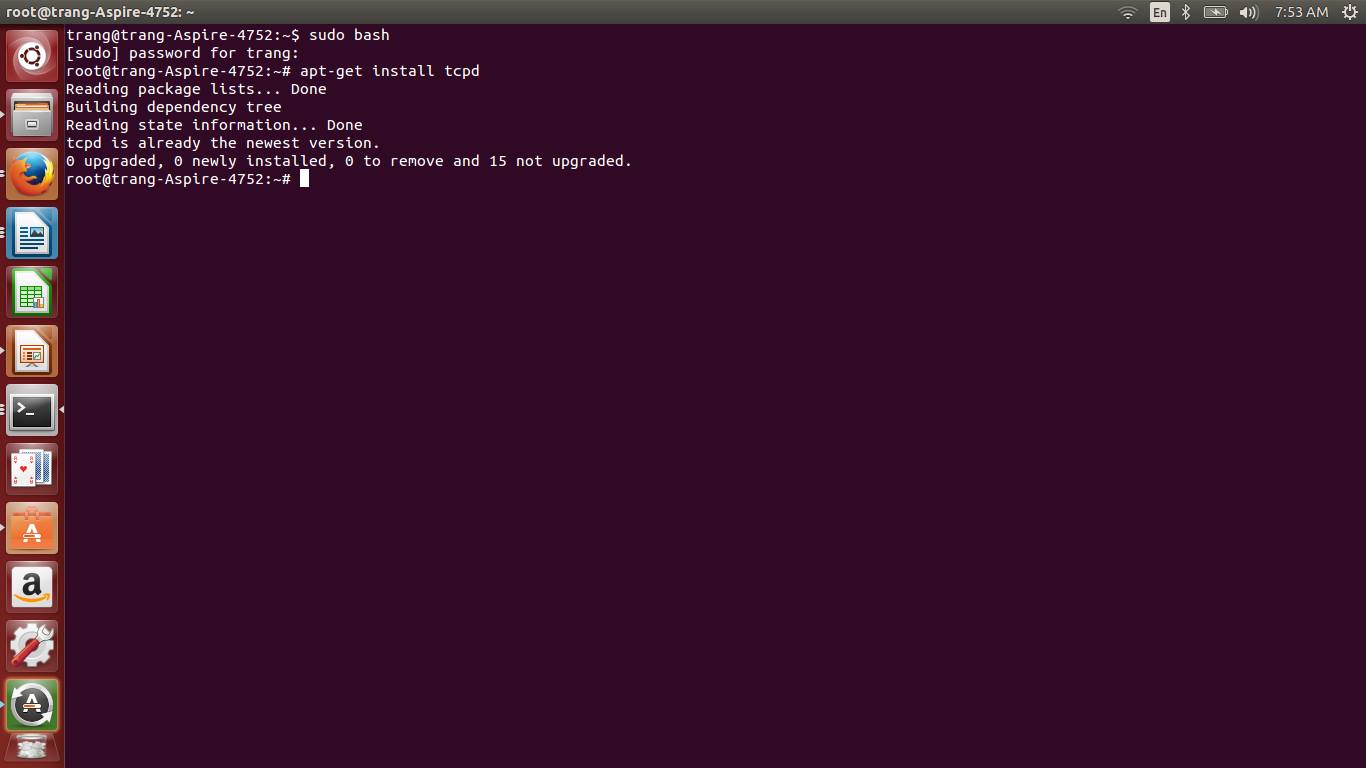
**Để giảm thiểu mối đe dọa cho hệ thống Linux của bạn từ các cuộc tấn công mạng ta có thể sử dụng các cách dưới đây:**

* **Luôn theo sát các mối nguy hại hiện tại.**
* Cách tốt nhất là ghé thăm các website bảo mật liên quan một cách thường xuyên.Những trang web thông báo cho bạn về những khai thác mới nhất và làm thế nào để bảo vệ mình chống lại chúng. Một trong những trang web tốt nhất để truy cập là http://www.cert.org, được duy trì bởi đội khẩn cấp máy tính Response (CERT) tại phần mềm Carnegie Mellon Viện Kỹ thuật. Các trang web CERT chứa liên kết đến các bảo mật mới nhất.
* Một nguồn tài nguyên tuyệt vời khác là http://www.us-cert.gov. Duy trì bởi United đội Readiness khẩn cấp máy tính quốc gia của chính phủ, các trang web US-CERT cung cấp thông tin về tấn cuộc tấn công mạng hiện tại
* **Gỡ các dịch vụ không cần thiết.**
* Một trong những điều đơn giản nhất bạn có thể làm để giảm thiểu các mối đe dọa từ một cuộc tấn công mạng là chỉ cần gỡ bỏ các dịch vụ mạng đang chạy trên hệ thống của bạn mà không cần thiết.
* Tùy thuộc vào phân phối của bạn và cách bạn cài đặt nó, bạn có thể có một số dịch vụ đang chạy trên hệ thống của bạn mà bạn không biết đã ở đó và bạn không cần. Bạn có thể xem danh sách các dịch vụ cài đặt và cho dù chúng chạy hay không bằng cách nhập chkconfig tại dấu nhắc shell.
* Tuy nhiên, Chkconfig không có sẵn trên tất cả các bản phân phối. Ban đầu nó chỉ có ở phân phối Red Hat và đã được chuyển đến nhiều bản phân phối khác, chẳng hạn như SUSE Linux.
* **Cập nhật các cài đặt**
* Một trong những điều quan trọng nhất chúng ta có thể làm để bảo vệ chống lại các cuộc tấn công mạng là thường xuyên cài đặt bản cập nhật hệ điều hành. Một thực tế đơn giản của cuộc sống mà chúng ta phải đối phó trong thế giới CNTT là phần mềm không được viết một cách hoàn hảo. Hầu hết các chương trình, dịch vụ này có một số khiếm khuyết. Ngay cả hạt nhân Linux cũng có những sai sót. Một vài sai sót là không quan trọng, một số chỉ là khó chịu, và một số khác khác đại diện cho rủi ro an ninh nghiêm trọng.
* Các phần mềm được phát hành và sử dụng, những sai sót đó được phát hiện bởi các quản trị viên hệ thống, người sử dụng, và (không may) tin tặc. Khi đó chúng được phát hiện, cập nhật viết và sửa chữa các sai sót. Với hầu hết các bản phân phối, bạn có thể định dạng cho hệ điều hành tự động khi không có Internet và kiểm tra định kỳ để cập nhật nhanh nhất.
* Chúng ta có thể đăng ký với Novell, hệ thống của bạn sẽ được kiểm tra định kỳ để cập nhật. Chúng ta có thể định dạng hệ thống hoặc là tự động cài đặt hoặc là nhắc chúng ta cài đặt chúng.
* Giới hạn quyền truy cập root: Hầu hết các bản phân phối ngày này không cho phép bạn đăng nhập bằng root vào lúc khởi động. Khi bạn phải thực hiện một công việc đòi hỏi đặc quyền siêu người dùng bạn sẽ được nhắc nhập mật khẩu. Nó có thể là một chút khó chịu nhưng nó đi một chặng đường dài để đảm bảo rằng công việc quản trị được phân lập từ người sử dụng. Bạn có thể hạn chế quyền truy cập cho một người sử dụng từ dưới System> Administration> Users and Groups. Trên dòng lệnh, lệnh su (trên Fedora) cho phép người sử dụng bình thường chuyển sang tài khoản gốc, trong khi lệnh sudo (trên Debian, Ubuntu, vv) các quyền ưu đãi hơn cho người dùng. Việc sử dụng các lệnh này có thể được giới hạn trong một nhóm cụ thể, trong đó ngăn chặn bất kỳ người sử dụng từ quản trị hệ thống. Sudo cũng là an toàn hơn, và nó giữ một bản ghi truy cập dưới /var/log/auth.log.

### 2.3.2 Sử dụng TCP Wrappers

* **Cài đặt TCP Wrappers ta dùng lệnh**

apt-get install tcpd



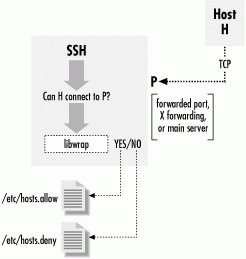
* TCP Wrappers có thể được sử dụng để cấp phép (allow) hoặc từ chối ( deny) các mạng khác nhau đến server của bạn.Dùng hai tập tin:

/etc/hosts.allow

/etc/hosts.deny

**Bước 1 :** Kiểm tra file hosts.allow và áp dụng rule đầu tiên được thiết lập. Nếu thấy phù hợp thì kết nối được thiết lập, nếu không phù hợp sẽ chuyển sang Bước 2

**Bước 2:** Tiến hành kiểm tra tiếp file hosts.deny và tìm rule phù hợp để deny



Hình 2.1 Quy tắc hoạt động của TCP Wrappers

* **Quy tắc TCP Wrappers :**
* Hosts.allow sẽ được ưu tiên hơn hosts.deny: Nếu xảy ra trường hợp cả 2 file này đều allow và deny cùng 1 IP, thì IP này sẽ vẫn được allow.
* Chỉ có 1 Rule cho mỗi dịch vụ trong hosts.allow và host.deny
* Nếu không có quy định phù hợp trong các tập tin hoặc các tập tin không tồn tại thì các máy tính từ xa được phép truy cập vào các dịch vụ
* Bất kỳ thay đổi nào trong hosts.allow và hosts.deny file có hiệu lực ngay lập tức.
* **Cú pháp TCP Wrappers :**

**daemon: client [:option1:option2:...]**

* **Deamon:** có thể là một sự kết hợp của deamon SSH, FTP deamon, Portmap deamon. Về cơ bản bất kỳ dịch vụ trong đó có hỗ trợ cho libwrap. Một thư viện biên dịch vào đó là một ứng cử viên tốt cho việc sử dụng các dịch vụ của TCP Wrapper.
* **Client:** là dấu phẩy tách ra danh sách các tên máy chủ, các địa chỉ IP của host, mô hình đặc biệt hoặc các kí hiệu đặc biệt để nhận biết các máy bị ảnh hưởng bởi quy luật đó.
* **Option:** là một hành động tùy chọn như nói gửi thư cho người quản trị khi quy định này là phù hợp, đăng nhập vào một tập tin cụ thể và như vậy. Nó có thể là một danh sách thư đại tràng tách của các hoạt động.

### 2.3.3 Thực hiện mã hóa

* Thực hiện mã hóa tất cả mọi thứ để bảo vệ dữ liệu của bạn. Đó là lời khuyên phổ biến nhất hiện nay.
* Một trong những vấn đề với các dịch vụ mạng như Telnet, rlogin, rcp, rshell, và FTP là một thực tế mà họ truyền tải dữ liệu như văn bản rõ ràng. Bất cứ ai chạy một sniffer có thể dễ dàng nắm bắt được tên người dùng, mật khẩu, và nội dung của truyền.Không phải là một điều tốt.
* Để thay thế, bạn có thể sử dụng mã hóa để mã hóa truyền. Mặc dù dữ liệu vẫn có thể được truyền tải bình thường và các hacker không thể đọc nó. Để mà truyền hoặc nhận dữ liệu được mã hóa, bạn cần phải có một khóa mã hóa. Keys là sử dụng để tranh giành và giải mã dữ liệu được mã hóa. Một số hệ thống mã hóa sử dụng một chìa khóa duy nhất để mã hóa và giải mã dữ liệu.
* Có một loạt các phương pháp mã hóa mà bạn có thể sử dụng để mã hóa dữ liệu giữa hai hệ thống Linux. Bao gồm:

1. Triple Data Encryption Standard (3DES) 3DES thường được sử dụng bởi

nhiều dịch vụ Linux. 3DES mã hóa dữ liệu trong ba giai đoạn. Nó sử dụng hoặc là một

112-bit hoặc một phím 168-bit.

1. Advanced Encryption Standard (AES) AES là một phiên bản cải tiến của

3DES. Nó hỗ trợ các phím 128-bit, 192-bit, và 256-bit.

1. Blowfish Blowfish sử dụng chiều dài khóa biến lên đến 448 bit.

* Bạn có thể sử dụng các gói OpenSSH để hoàn thành nhiệm vụ quản lý sử dụng

mã hóa. Điều quan trọng là phải nhớ rằng khi bạn đang sử dụng một tiện ích từ OpenSSH

gói có sử dụng mã hóa, hệ thống khách hàng phải được cấu hình để sử dụng cùng một

phương pháp mã hóa như hệ thống máy chủ.

### 2.3.4 Thực hiện một bức tường lửa (Firewall)

Ngày nay hầu hết các tổ chức, doanh nghiệp điều kết nối với internet, để trao đổi thông tin và liên lạc làm việc với nhau. Nhưng để những thông tin đó không bị đánh cắp hay bị vấn đề an ninh thì chúng ta cần thực hiện một bức tường lửa để bảo vệ máy chủ của mình.

Tường lửa là một sự kết hợp của phần cứng và phần mềm mà hành động như một người gác cổng giữa mạng của bạn và một mạng khác.

#### 2. 3.4.1 Dùng công cụ dò tìm để khảo sát hệ thống: như Nmap, strobe, sscan, SATAN, ...

* Nmap ("Network exploration tool and security scanner” Đây là chương trình quét hàng đầu với tốc độ cực nhanh và cực mạnh. Nó có thể quét trên mạng diện rộng và đặc biệt tốt đối với mạng đơn lẻ. NMAP giúp bạn xem những dịch vụ nào đang chạy trên server (services/ports:webserver,ftpserver,pop3,...), server đang dùng hệ điều hành gì, loại tường lửa mà server sử dụng, ... và rất nhiều tính năng khác
* Quét an toàn Nmap là một trong số công cụ quét an toàn được sử dụng rộng rãi nhất sẵn có. Nmap là một cổng quét mà chống lại các nhân tố, các cách khác tàn phá đến mạng của bạn. Nó có thể phát sinh ra nhiều kiểu gói mà thăm dò các ngăn xếp TCP/IP trên những hệ thống của bạn.
* Nmap có thể phát sinh ra một danh sách của những cổng mở dịch vụ trên hệ thống của bạn, thâm nhập firewalls, và cung cấp những tin quấy rầy, không tin cậy đang chạy trên host của bạn. Nmap security có sẵn tại : http://www.insecure.org

#### 2.3.4.2 Phát hiện sự xâm nhập qua mạng (IDS)

* Hệ thống phát hiện xâm nhập qua mạng (IDS “Intrusion Detection System”) theo dõi các thông tin truyền trên mạng và phát hiện nếu có hacker đang cố xâm nhập vào hệ thống (hoặc gây gây ra một vụ tấn công DoS(Denial of service )).
* Tính năng quan trọng nhất của IDS là:
* Giám sát lưu lượng mạng và các hoạt động khả nghi.
* Cảnh báo về tình trạng mạng cho hệ thống và nhà quản trị.
* Kết hợp với các hệ thống giám sát, tường lửa, diệt virus tạo thành một hệ thống bảo mật hoàn chỉnh.
* Có 2 loại chính là
* **NIDS:** hệ thống phát hện xâm nhập mạng.  Hệ thống sẽ tập hợp gói tin để phân tích sâu bên trong mà không làm thay đổi cấu trúc gói tin. NIDS có thể là phần mềm triển khai trên server hoặc dạng thiết bị tích hợp appliance.
* **HIDS:** hệ thống phát hiện xâm nhập host. Theo dõi các hoạt động bất thường trên các host riêng biệt. HIDS được cài đặt trực tiếp trên các máy (host) cần theo dõi.
* Các công cụ có thể được kết hợp để tạo một hệ thống phát hiện xâm nhập qua mạng. Chẳng hạn dùng TCPWRAPPER để điều khiển, ghi nhận các dịch vụ đã được đăng ký. Các chương trình phân tích nhật ký hệ thống, như swatch, có thể dùng để xác định các tác vụ dò tìm trên hệ thống. Và điều quan trọng nhất là các công cụ có thể phân tích cácthông tin trên mạng để phát hiện các tấn công DoS hoặc đánh cắp thông tin như tcpdump, ethereal, ngrep, NFR (Network Flight Recorder), PortSentry, Sentinel, Snort, ...
* Khi hiện thực một hệ thống phát hiện xâm nhập qua mạng bạn cần phải lưu tâm đến hiệu suất của hệ thống cũng như các chính sách bảo đảm sự riêng tư.

#### 2.3.4.3 Kiểm tra khả năng bị xâm nhập

* Các công cụ thường được sử dụng để thực hiện các kiểm tra loại này là ISS Scanner, Cybercop, Retina, Nessus, cgiscan, CIS, ...
* Kiểm tra khả năng bị xâm nhập cần được thực hiện bởi những người có trách nhiệm một cách cẩn thận. Sự thiếu kiến thức và sử dụng sai cách có thể sẽ dẫn đến hậu quả nghiêm trọng không thể lường trước được.

#### 2.3.4.4 Đối phó khi mạng bị tấn công

* Thiết lập tường lửa iptables cho linux
* Hầu hết các bản phân phối Linux đều có một vài công cụ tường lửa khác nhau. Nhưng công cụ phổ biến hơn, thích hợp với nhiều phiên bản hiện nay là Iptables.
* Iptables là một tường lửa ứng dụng lọc gói dữ liệu rất mạnh, miễn phí và có sẵn trên Linux. Gồm 2 phần là Netfilter (Dùng để xử lý hoặc từ chối các thông tin ra vào máy tính) ở trong nhân Linux và Iptables nằm ngoài nhân. Iptables chịu trách nhiệm giao tiếp giữa người dùng và Netfilter để đẩy các luật của người dùng vào cho Netfiler xử lí. Netfilter tiến hành lọc các gói dữ liệu ở mức IP. Netfilter làm việc trực tiếp trong nhân, nhanh và không làm giảm tốc độ của hệ thống.
* Cấu trúc của Iptables  
  Iptables được chia làm 4 bảng (table):
* Bảng filter dùng để lọc gói dữ liệu,
* Bảng NAT dùng để thao tác với các gói dữ liệu được NAT nguồn hay NAT đích.
* Bảng mangle dùng để thay đổi các thông số trong gói IP.
* Bảng conntrack dùng để theo dõi các kết nối. Mỗi table gồm nhiều mắc xích (chain).
* Chain gồm nhiều luật (rule) để thao tác với các gói dữ liệu. Rule có thể là ACCEPT (chấp nhận gói dữ liệu), DROP (thả gói), REJECT (loại bỏ gói) hoặc REFERENCE (tham chiếu) đến một chain khác.
* Quá trình chuyển gói dữ liệu qua Netfilter. Gói dữ liệu (packet) chạy trên cáp, sau đó đi vào card mạng (chẳng hạn như eth0). Đầu tiên packet sẽ qua chain PREROUTING (trước khi định tuyến). Tại đây, packet có thể bị thay đổi thông số (mangle) hoặc bị đổi địa chỉ IP đích (DNAT). Đối với packet đi vào máy, nó sẽ qua chain INPUT.
* Tại chain INPUT, packet có thể được chấp nhận hoặc bị hủy bỏ.

Tiếp theo packet sẽ được chuyển lên cho các ứng dụng (client/server) xử lí và tiếp theo là được chuyển ra chain OUTPUT.

* Tại chain OUTPUT, packet có thể bị thay đổi các thông số và bị lọc chấp nhận ra hay bị hủy bỏ.
* Đối với packet forward qua máy, packet sau khi rời chain PREROUTING sẽ qua chain FORWARD. Tại chain FORWARD, nó cũng bị lọc ACCEPT hoặc DENY. Packet sau khi qua chain FORWARD hoặc chain OUTPUT sẽ đến chain POSTROUTING (sau khi định tuyến). Tại chain POSTROUTING, packet có thể được đổi địa chỉ IP nguồn (SNAT) hoặc MASQUERADE. Packet sau khi ra card mạng sẽ được chuyển lên cáp để đi đến máy tính khác trên mạng.
* Tuy nhiên, việc sử dụng iptables đem lại nhiều bất tiện và khó khăn do đó cần nhiều thời gian để học hỏi. UFW sẽ giải quyết vấn đề đó cho bạn: mạnh và đơn giản.
* Mạnh vì nó cũng dựa trên iptables.
* Đơn giản vì : ***UFW trên terminal***
* UFW là một giao diện cấu hình tường lửa chạy trên dòng lệnh cho phép người dùng Ubuntu điều khiển traffic ra vào máy mình một cách đơn giản trên nền tảng tường lửa truyền thống iptables. Ta không thể làm mọi thứ với UFW. Đối với những tác vụ phức tạp hơn liên quan đến tường lửa, ta phải sử dụng iptables.

## 2.4 Phát hiện xâm nhập

Ngoài việc có một tường lửa, bạn nên xem xét thực hiện các bước sau để phát hiện bất kỳ kẻ xâm nhập nào trên hệ thống của bạn, một người nào đó phải vượt qua tường lửa của bạn hoặc xúi giục một cuộc tấn công từ phía sau tường lửa. Điều này được gọi là phát hiện xâm nhập. Chúng ta có thể phát hiện những kẻ xâm nhập bằng những cách làm như sau:

* Phân tích các tập tin đăng nhập Linux
* Thực hiện một hệ thống phát hiện xâm nhập (IDS)
* Thực hiện kiểm toán an ninh với Tripwire

### 2.4.1 Phân tích tập tin đăng nhập Linux

Một trong những nguồn lực tốt nhất của bạn trong vấn đề này là các tập tin bản ghi của bạn mà hệ thống Linux duy trì cho bạn.Bạn cần thực hành và có kinh nghiệm để phát triển một cảm giác trực quan tốt cho phép bạn biết khi nào có một cái gì đó trông khả nghi.Cách tốt nhất để phát triển trực giác này là dành nhiều thời gian xem xét tập tin bản ghi của bạn. Điều này sẽ giúp bạn phát triển một cảm giác về những gì là "bình thường" cho hệ thống của bạn. Một khi bạn biết những gì là bình thường, thì bạn có thể nhận ra rằng những thứ không phải là bình thường.

Đầu tiên là / var / log / file wtmp.log file. Tập tin này chứa danh sách của tất cả người dùng vào hệ thống đã được chứng thực. Các tập tin này được lưu ở định dạng nhị phân. Bạn không thể sử dụng cat, less, hoặc một trình soạn thảo văn bản, chẳng hạn như vi, để xem nó. Thay vào đó, bạn phải sử dụng câu lệnh **last** tại dấu nhắc shell. Tiện ích last hiển thị các tài khoản người dùng, thời gian đăng nhập, thời gian đăng xuất, và chứng thực họ đang ở đâu. Khi bạn xem lại tập tin này, tìm kiếm bất cứ thứ gì xuất hiện bất thường, ví dụ, thông tin đăng nhập đã xảy ra vào giữa đêm khi không có ai tại nơi làm việc là đáng nghi ngờ.

Bạn cũng có thể xem / var / log / file maillog. log file. Tập tin này có chứa một danh sách các nỗ lực xác thực thất bại. Tập tin này rất hiệu quả trong việc phát hiện các cuộc tấn công từ điển, chạy qua một danh sách các từ điển, cố gắng cho họ như mật khẩu cho các tài khoản người dùng.

Giống như wtmp, log file là một tập tin nhị phân. Để xem nó, bạn cần phải sử dụng các tiện ích maillog. Tiện ích này sẽ hiển thị cho người sử dụng những người đã cố gắng để xác thực, bao nhiêu lần họ thất bại trong việc đăng nhập, và khi các nỗ lực cuối cùng không thành công xảy ra. Bạn có thể sử dụng tùy chọn -u để xem các nỗ lực đăng nhập tài khoản người dùng cụ thể.

Khi xem xét tập tin nhật ký này, nhìn vào những nỗ lực đăng nhập bất thường, chẳng hạn như số lượng lớn các thông tin đăng nhập thất bại một cách bất thường, đặc biệt là nếu họ xảy ra vào đêm khuya. Bạn cũng có thể sử dụng tiện ích maillog để chỉ định cách hệ thống xử lý nỗ lực đăng nhập thất bại. Sau đó sử dụng các tùy chọn sau đây với lệnh faillog:

* **–l *seconds*** Cho số giây quy định khoá tài khoản sau khi một nỗ lực đăng nhập thất bại.
* **–m *number*** Thiết lập số lượng nỗ lực đăng nhập thất bại tối đa trước khi tài khoản người dùng bị vô hiệu hóa.

Các tập tin đăng nhập tiếp theo là / var / log / lastlog. Tập tin này có chứa một danh sách tất cả những người sử dụng trong hệ thống và khi họ đăng nhập cuối cùng trong hệ thống. Cũng giống như các tập tin nhật ký khác, bạn không thể xem lastlog với less, cat, hoặc một trình soạn thảo văn bản. Để xem lastlog, bạn phải sử dụng tiện ích lastlog từ dấu nhắc shell

Các tập tin bản ghi cuối cùng chúng ta sẽ xem xét ở đây là / var / log / messages. Tập tin đăng nhập này chứa các tin nhắn từ tất cả các dịch vụ đang chạy trên hệ thống. Như vậy nó có chứa rất nhiều dữ liệu có thể có hoặc không có liên quan đến sự cố gắng xâm nhập. Bạn có thể sử dụng **grep** để cô lập các mục có liên quan.

### 2.4.2 Thực hiện một hệ thống phát hiện xâm nhập (IDS)

Một số chức năng của hệ thống IDS tương tự như nhiều phần mềm chống virus, tìm kiếm những mẫu virus trong file. IDS có một cơ sở dữ liệu định nghĩa xâm nhập thứ mà được sử dụng để phát hiện xâm nhập. Cũng như các định nghĩa virus cần được cập nhật thường xuyên, thì các định nghĩa xâm nhập của hệ thống IDS cũng phải được cập nhật thường xuyên để có hiệu quả.

Một số hệ thống IDS không sử dụng các mẫu được xác định trước. Thay vào đó, họ giám sát hệ thống trong một khoảng thời gian, phát triển một cơ sở hoạt động. Một khi cơ sở được hoàn chỉnh, họ sẽ tìm kiếm giao thông mà không phù hợp với cơ sở và phân tích nó để xem nếu có một cuộc tấn công trong tiến trình. Một số hệ thống IDS có thể được liên kết với tường lửa mạng của bạn. Khi những hệ thống phát hiện sự xâm nhập,nó có thể liên hệ với tường lửa của bạn và ngay lập tức tắt phiên giao tiếp. Hệ thống IDS đang ngày càng trở nên phổ biến hơn do tính chất quỷ quyệt của việc nỗ lực xâm nhập. Chúng có thể rất lén lút đến nỗi các quản trị viên thậm chí không nhận ra chúng đang xảy ra cho đến khi đã quá muộn. Nhiều nhà quản trị hệ thống đã ngạc nhiên và sợ hãi biết bao khi họ nhận ra có bao nhiêu cuộc tấn công thường xuyên được phát hiện trên hệ thống của họ sau khi thực hiện một IDS.

Một IDS thường được thực hiện trên một hệ thống máy tính chuyên dụng mà không làm gì nhưng dành cả ngày tìm kiếm cho những nỗ lực xâm nhập. Ngày nay có một loạt các gói IDS sẵn có. Một trong những gói tốt nhất là gói Snort, đó là phần mềm mã nguồn mở có thể được thực hiện trên một hệ thống Linux. Các phần mềm phổ biến khác bao gồm PortSentry, Advanced Intrusion Detection Environment (AIDE), Integrity Checking Utility (ICU), Simple Watcher (SWATCH), và Linux Intrusion Detection System (LIDS).

### 2.4.3 Thực hiện an kiểm toán với Tripwire

Một số kẻ xâm nhập, nếu họ tìm được cách để đạt quyền truy cập vào một hệ thống, họ chỉ muốn chọc xung quanh và nhìn thấy những gì ở đó, là khá lành tính.Những người khác, tiếc, là không phải thân thiện như vậy.Mục tiêu của họ là để tàn phá hệ thống của bạn. Để làm điều này, họ có thể làm một loạt các thay đổi vào các tập tin hệ thống quan trọng của bạn.Để khắc phục tình trạng này, bạn có thể thực hiện một hệ thống kiểm toán. Có rất nhiều gói kiểm toán có sẵn, nhưng cho Linux + của bạn, bạn cần phải làm quen với Tripwire.

Khi bạn lần đầu tiên thiết lập Tripwire, nó tạo ra một ảnh chụp cơ bản hệ thống của bạn bằng cách tạo ra một cơ sở dữ liệu của các tập tin hệ thống quan trọng của bạn.Sau đó, Tripwire tự động chạy kiểm tra trên hệ thống tập tin quan trọng của bạn 1 cách định kỳ.Sau đó sử dụng dữ liệu trong cơ sở dữ liệu của nó để xác định bất kỳ thay đổi.Nó cũng có thể xác định các tập tin đã được thêm vào hoặc xóa từ các hệ thống sử dụng cơ sở dữ liệu của nó.Thông báo được ghi lại bất cứ khi nào khi Tripwire thấy rằng một hệ thống tập tin đã bị thay đổi, tạo ra, hoặc đã bị xóa.

Để cấu hình Tripwire trên hệ thống của bạn, làm như sau:

1. Tải về các tripwire tarball mới nhất từ http://www.tripwire.org.
2. Chuyển sang tài khoản người dùng root của bạn.
3. Giải nén và cài Tripwire tarball.
4. Mở /etc/tripwire/twpol.txt trong một trình soạn thảo văn bản.
5. Thiết lập biến HOSTNAME bằng tên máy chủ hệ thống của bạn.
6. Lưu thay đổi các tập tin của bạn và thoát khỏi trình soạn thảo.
7. Chạy /etc/tripwire/twinstall.sh script từ dấu nhắc shell.
8. Khi được nhắc, nhập vào trang web và mật khẩu của bạn. Những mật khẩu sẽ được sử dụng để tạo ra các khóa mã hóa được sử dụng để mã hóa các tập tin cơ sở dữ liệu Tripwire.
9. Tạo cơ sở dữ liệu ban đầu Tripwire của bạn bằng cách nhập tripwire --init tại dấu nhắc shell
10. Cấu hình cron để chạy các lệnh tripwire-check ít nhất một lần một ngày.

Tại thời điểm này, Tripwire sẵn sàng để cuộn. Bạn có thể chờ cho cron chạy tripwire-check mỗi ngày hoặc bạn có thể tự chạy bằng tay tripwire-check tại dấu nhắc shell. Nếu tripwire-check tìm thấy bất kỳ bất thường nào, nó có thể ghi chúng vào các file báo cáo được mã hóa trong /var/lib/tripwire/report/.

Bởi vì nó được mã hóa, bạn không thể xem nó trực tiếp với less, cat, or vi.

Thay vào đó, bạn cần phải sử dụng các câu lệnh twprint –m r --twfile filename tại dấu nhắc shell.

# CHƯƠNG 3: THỰC NGHIỆM

## 3.1 Hướng dẫn cài đặt Ubuntu bằng USB

* Hiện nay, Linux có rất nhiều những phiên bản và các cách cài đặt HĐH này cũng khá đa dạng như: chạy trực tiếp bằng đĩa CD/DVD, cài máy ảo, cài bằng USB, phương pháp cài đặt từ Windows bằng Wubi hoặc có thể dùng thử online.
* Sau đây là cách cài đặt phiên bản ubuntu bằng USB.
* Cài đặt phần mềm Universal USB Installer trên máy tính.
* Sau đó ta có thể tải phiên bản mới nhất của Ubuntu tại <http://www.ubuntu.com/download/desktop>
* Và chuẩn bị một USB lớn hơn 2GB.
* Các bước cài đặt ubuntu

**Bước 1: Tạo USB Boot cài Ubuntu**

Mở chương trình vừa tải Universal USB Installer sau đó chọn **I agree**

Cửa sổ mới hiện lên, tại **Step 1** ta chọn **Ubuntu**, tại**Step 2** ta nhấp vào **Browse** tìm đường dẫn tới file .iso cài Ubuntu đã tải ở bước chuẩn bị, tại **Step 3** ta chọn tên USB của mình và click chọn “**Web will format….**” sau đó các ta nhấp vào **Create** để phần mềm bắt đầu quá trình Boot USB.

**Bước 2: Tạo phân vùng trên máy tính để cài Ubuntu**

Đầu tiên vào **My computer** nhấp chuột phải vào **My computer** (trên windows 7) ­­­­­­­­­­­­­­­­­­­­­ta chọn **manage**🡪 tiếp theo nhấp chọn **Management** đợi khoảng 1 phút thì danh sách các ổ đĩa và thông tin các ổ đĩa sẽ hiển thị lên. Ta chọn ổ đĩa còn dư dung lượng lớn đủ để cài Ubuntu, nhấp chuột phải vào ổ đĩa đó và chọn **Shrink Volume (**Để tạo phân vùng trống dùng để cài Ubuntu)

Một cửa sổ mới hiện lên, phần **Enter the amount of space to Shrink in MB** cho bạn điền dung lượng phân vùng cài Ubuntu, các bạn có thể chọn 50GB. Các bạn có thể điền theo MB hoặc lấy 1024\*(số GB) . Sau đó bạn nhấp vào **Shrink**

**Bước 3: Tiến hành cài Ubuntu**

Bạn khởi động lại máy tính và nhấn nút **F12** hoặc các phím tắt khác để vào **Boot Option**.

Sau đó các bạn các phím mũi tên lên xuống và nút Enter chọn **USB Storage Device**.

Cửa ổ mới hiện lên các bạn chọn **Install Ubuntu**

Vào phần cài đặt, đầu tiên bạn chọn ngôn ngữ, có thể chọn Tiếng Việt hoặc tiếng Anh

Tiếp theo sẽ có hai lựa chọn là **Download updates while installing** và **Install this third-party software**. Có thể chọn cả hai hoặc 1 cái. Sau đó bạn nhấp chọn **Continues**.

Cửa sổ tiếp theo có 1 số tùy chọn ta chọn **Something else** và nhấp vào **Continues**

Tiếp theo bạn sẽ thấy phân vùng trống mà bạn đã tạo, ở đây phân vùng của mình là 50GB. Bạn hãy chọn phân vùng đó sau đó nhấp vào dấu cộng.

Một cửa sổ mới hiện ra, ở đây cần *tạo phân vùng Swap cho Ubuntu*. Theo khuyến cáo của Ubuntu thì nên chọn dung lượng phân vùng Swap gấp đôi dung lượng Ram, do Ram máy mình là 2GB nên mình sẽ tạo phân vùng là 4GB. 4\*1024=4096 (1 GB = 1024MB) nên mình chọn 1024 MB. Phần **Type for the New artition** bạn chọn **Logical**, phần **Localtion for the new partition** bạn chọn **Beginning of this space** và phần **Use as** bạn chọn **Swap area** sau đó nhấp **OK**.

Tiếp theo bạn sẽ thu được 1 ổ đĩa có phân vùng Swap vừa tạo, ta lại tiếp tục chọn phân vùng trống **free space** và nhấp vào dấu cộng.

Tại đây, phần **Size** giữ nguyên để nó dùng hết dung lượng còn lại của phân vùng trống, phần **Type for the new partition** ta chọn **Primary**, phần **Location for the new partition**  chọn **Beginning of this space**, phần **Use as** chọn **Ext4 journaling File sytem** và phần **Mount point** chọn  **“/”** sau đó click **OK.**

Bây giờ bạn nhấp vào phân vùng vừa tạo có **Type** là **Ext4** sau đó click **Install now**

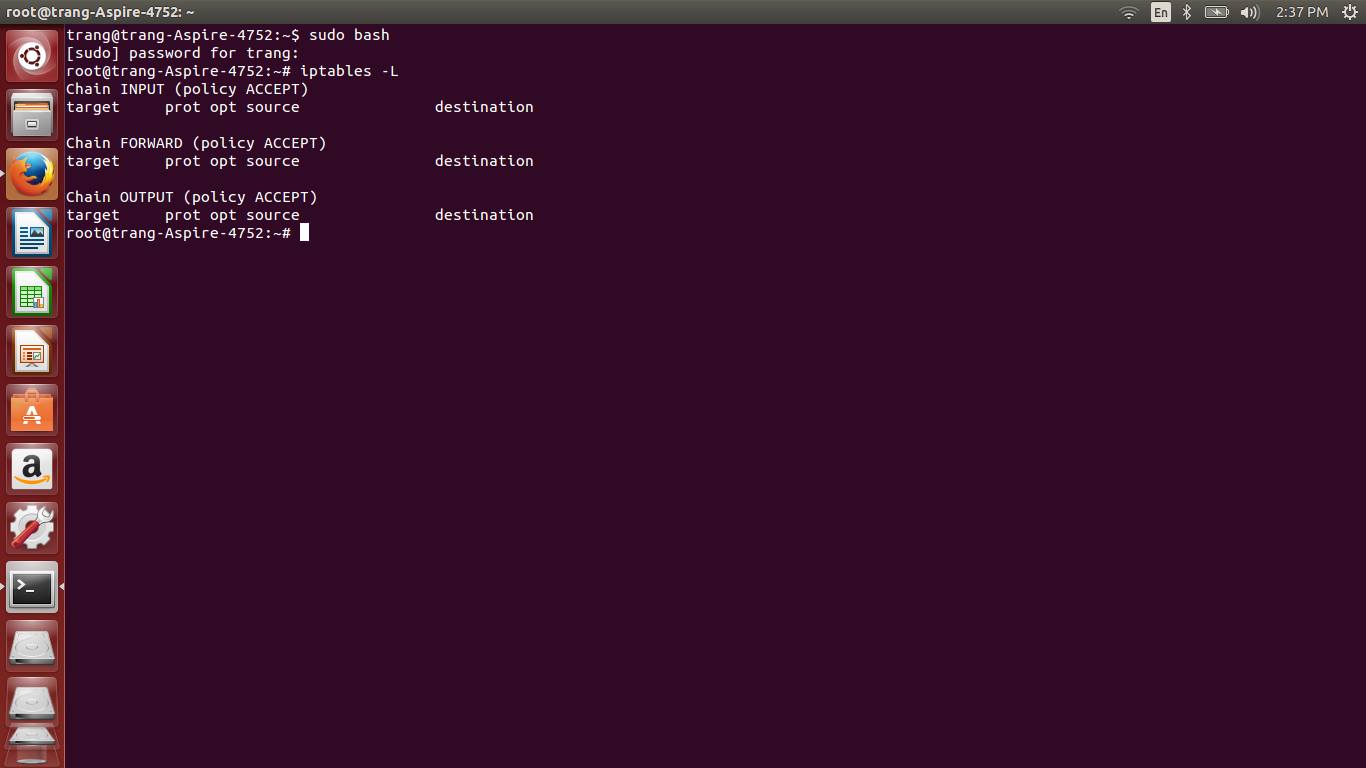
Tiếp tục chúng ta nhẹ nhàng nhấp vào thành phố Hồ Chí Minh để chọn giờ Việt Nam và chọn Continue.

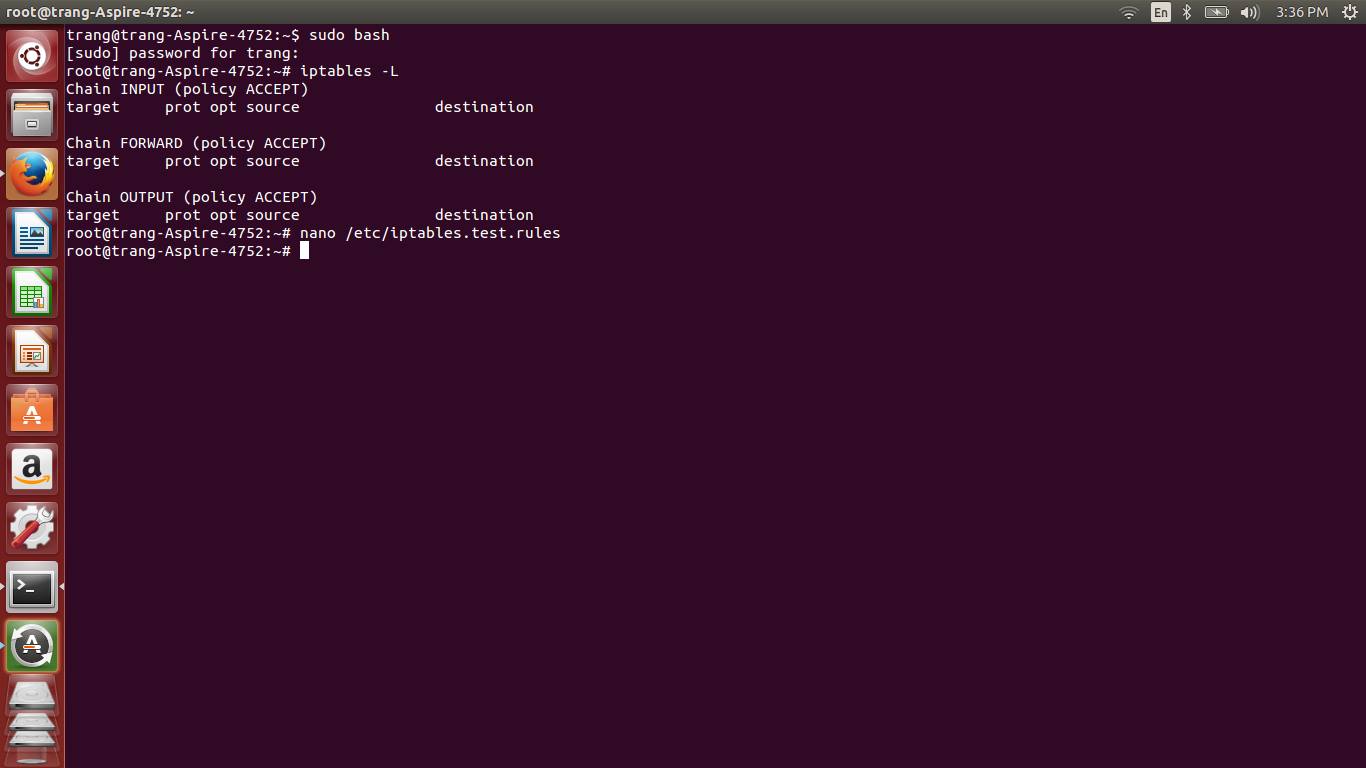
Sau đó bạn chọn kiểu bàn phím là English(US) sau đó lại click Continue.Bây giờ chúng ta điền thông tin đăng nhập tài khoản bao gồm tên người dùng, tên máy tính, tên user và mật khẩu, ta có thể chọn **Log in automotically** nếu bạn không muốn nhập mật khẩu mỗi lần khởi động vào Ubuntu, sau đó lại nhấp Continue.

Bây giờ các bạn cứ để đó, quá trình Ubuntu sẽ tự động cài và sau khi hoàn tất nó sẽ hiện thông báo yêu cầu bạn khởi động lại máy và sử dụng nó.

## 3.2. Cài đặt hệ thống tường lửa IPtables

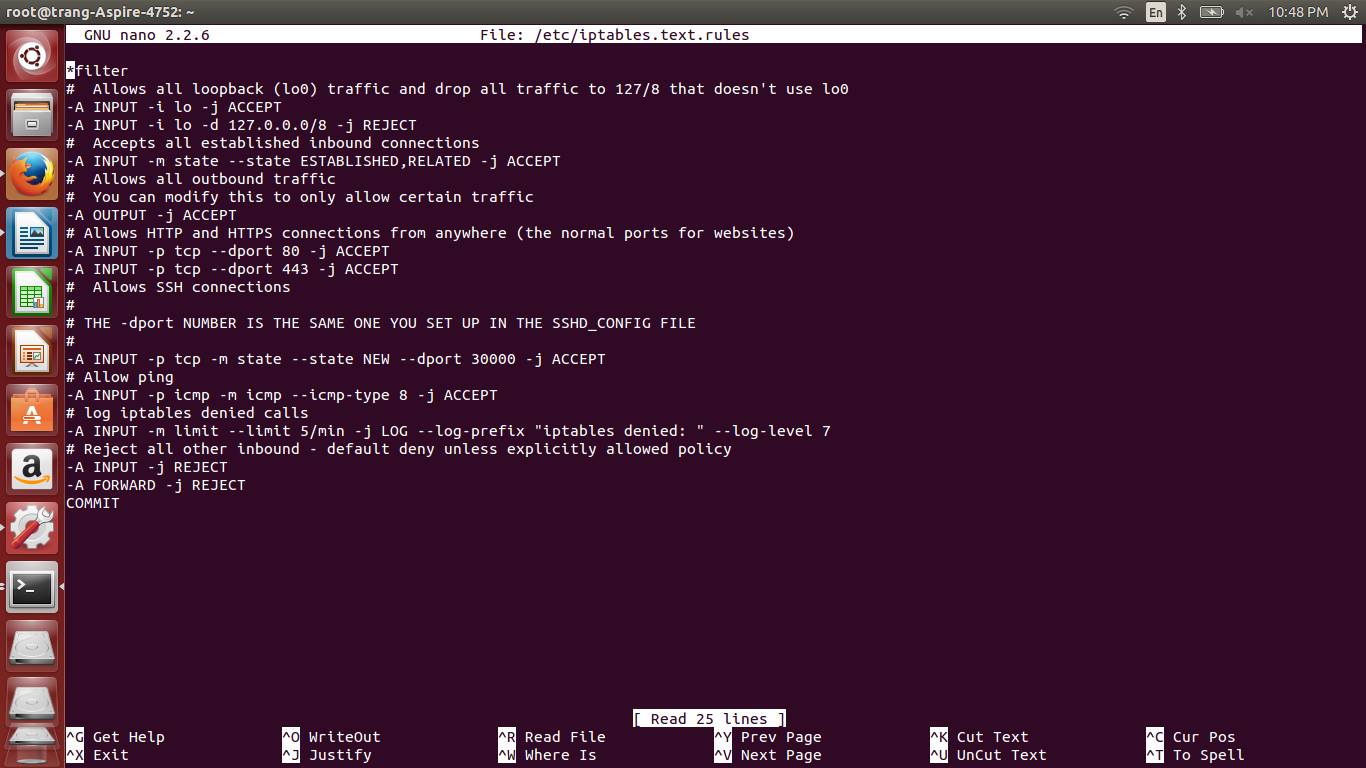
**Bước 1:** Truy cập với quyền root, mởterminal lên gõ lệnh: iptables –L



**Bước 2:** Nhập câu lệnh nano /etc/iptables.test.rules để tiến hành tạo file iptables.test.rules trong /etc

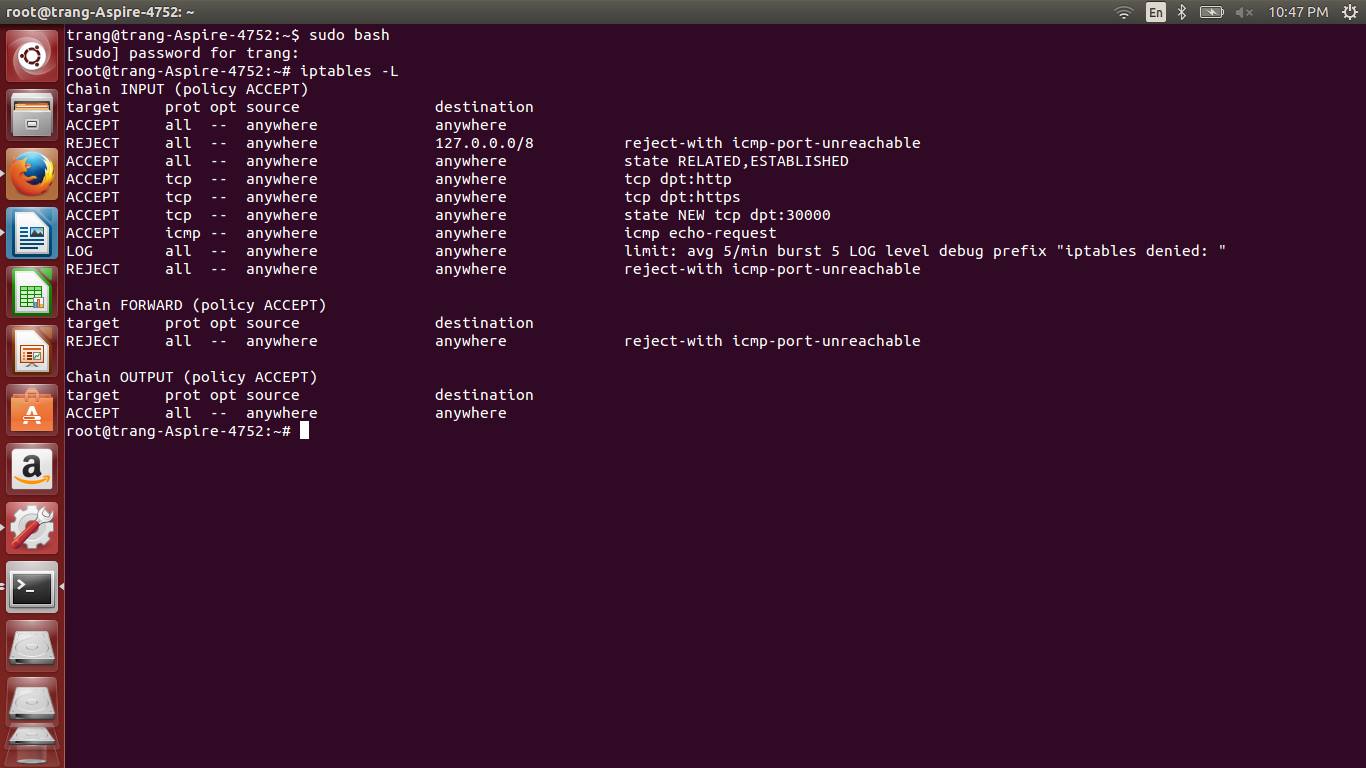
**Bước 3:** Thêm vào file vừa tạo đoạn code rồi lưu lại

Để lưu đoạn code ta bấm ctrl + o rồi enter.



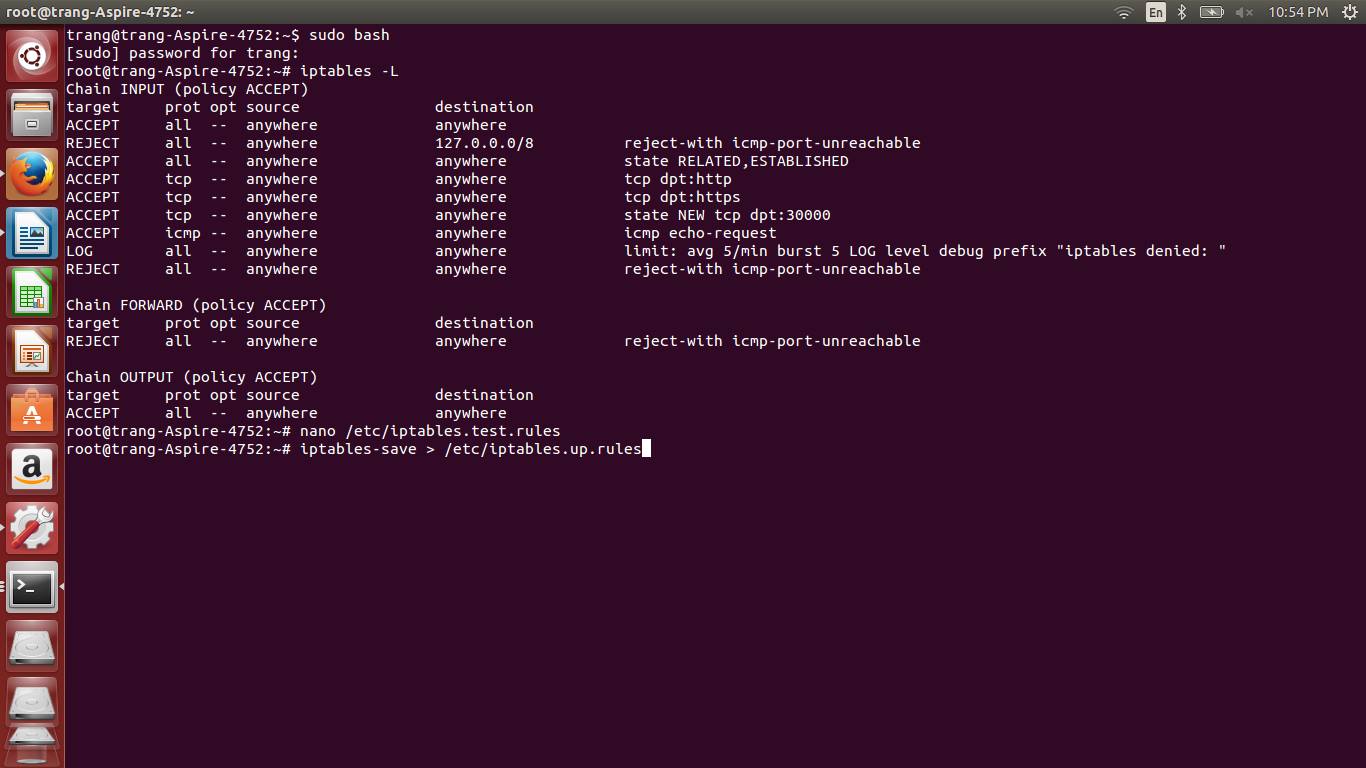
**Bước 4:** Ta nộp cấu hình cho bộ nhớ bằng lệnh iptables-restore < /etc/iptables.text.rules

**Bước 5:** Sau khi thực hiện các bước trên ta gõ lệnh iptables -L ta được như hình vẽ.



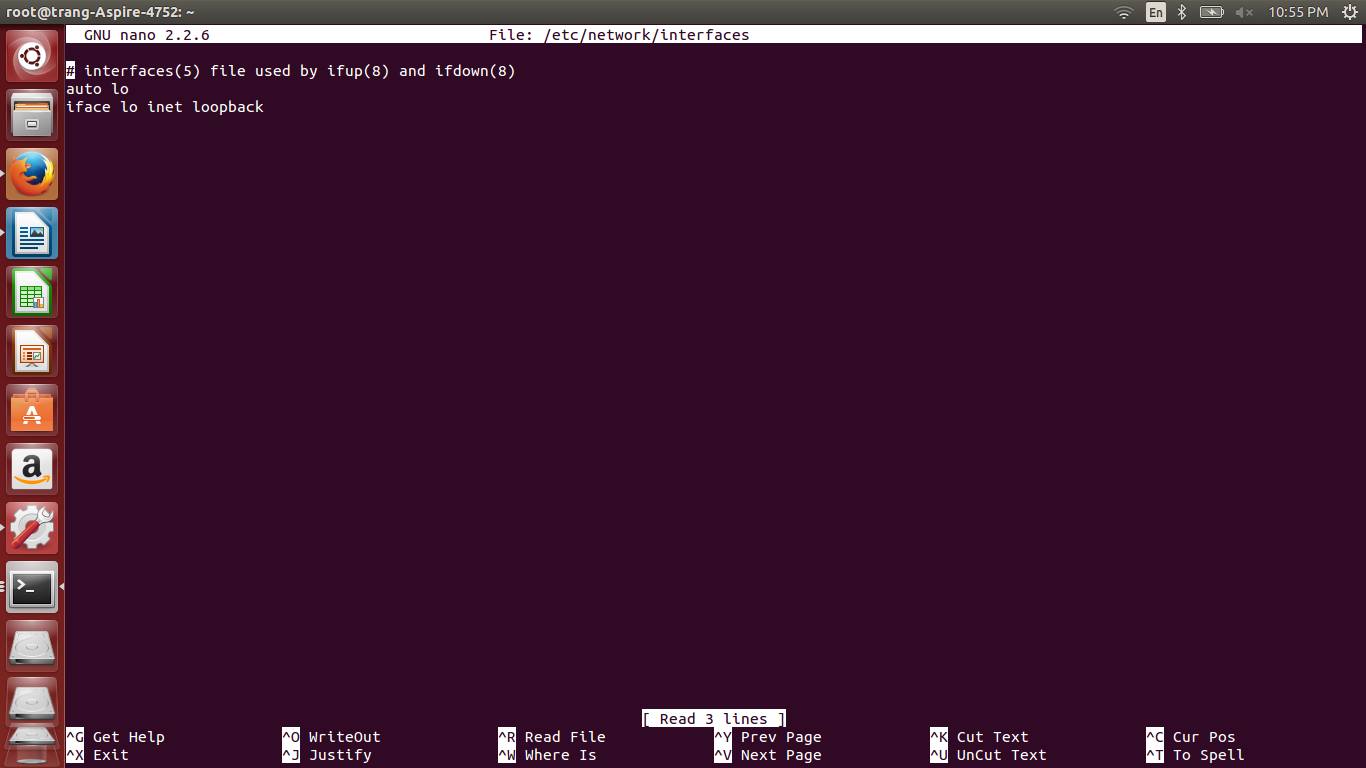
**Bước 6:** Lưu file với tên iptables.up.rules ta dùng lệnh

iptables-save> /etc/iptables.up.rules



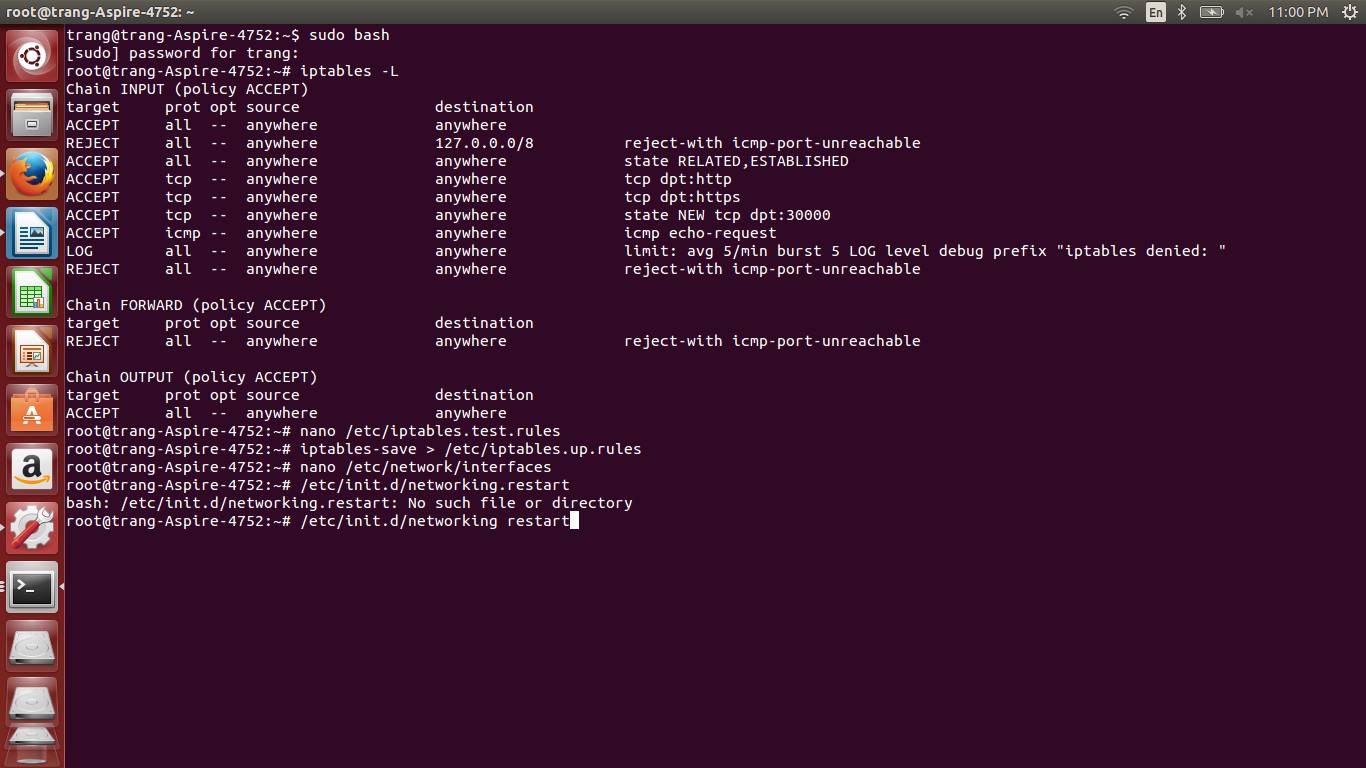
**Bước 7:** Bây giờ chúng ta cần phải đảm bảo là cấu hình sẽ được lưu lại mỗi khi ta khởi động máy, mở tệp tin ta dùng lệnh nano /etc/network/interfaces

Thêm vào dòng:”pre-up intables-restore < /etc/iptables.up.rules” ngay sau dòng “iface lo inet loopback”



**Bước 8**: restart the network card để hoàn tất, máy sẽ khởi động lại.

Dùng lệnh: /etc/init.d/networking restart

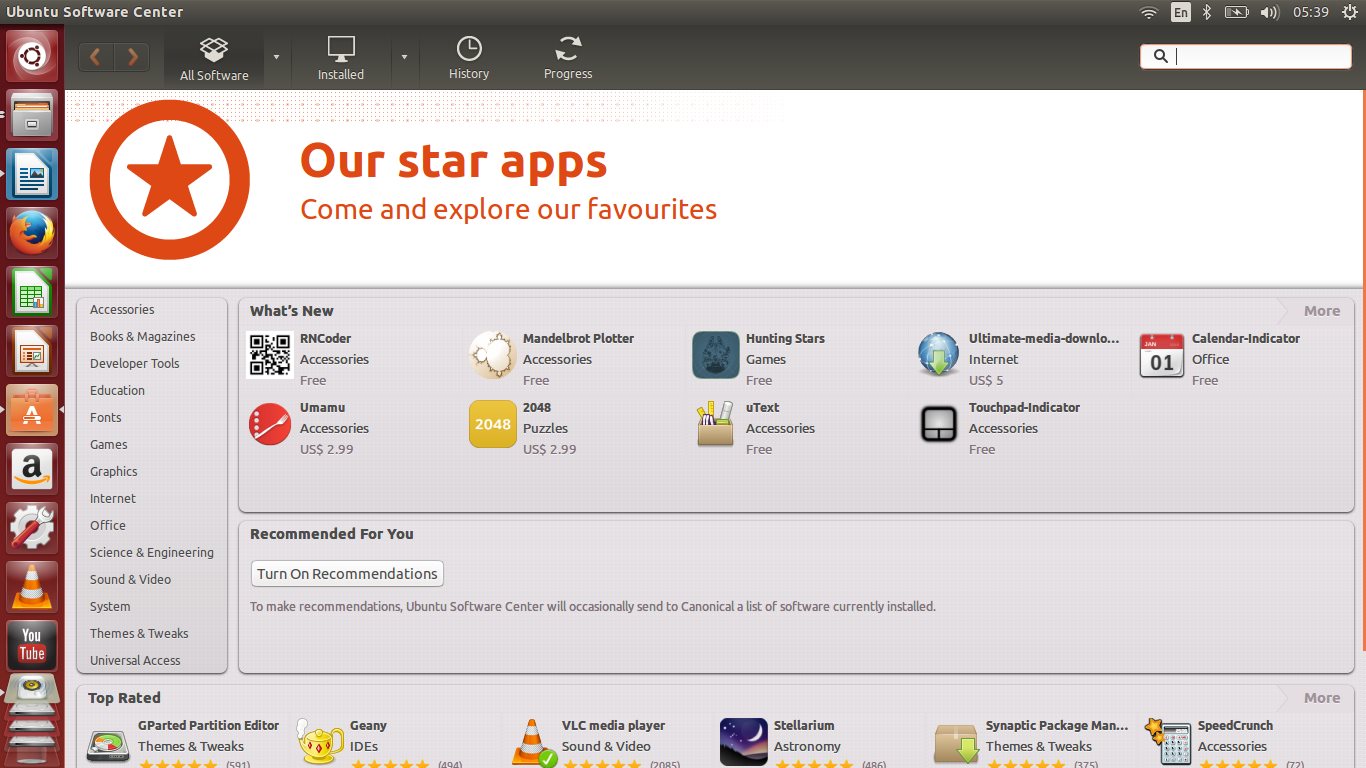


## 3.3 Cài đặt phần mềm ClamTk thông qua Ubuntu Software Center

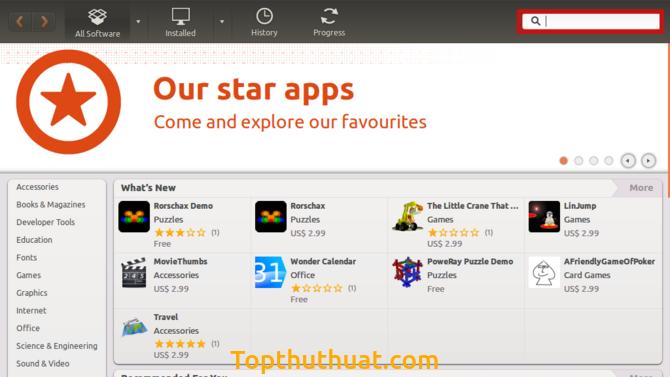
Trước tiên, bạn cần mở Ubuntu Software Center trên Ubuntu như sau:

Tìm kiếm **Ubuntu Software Center(USC)** và chạy nó

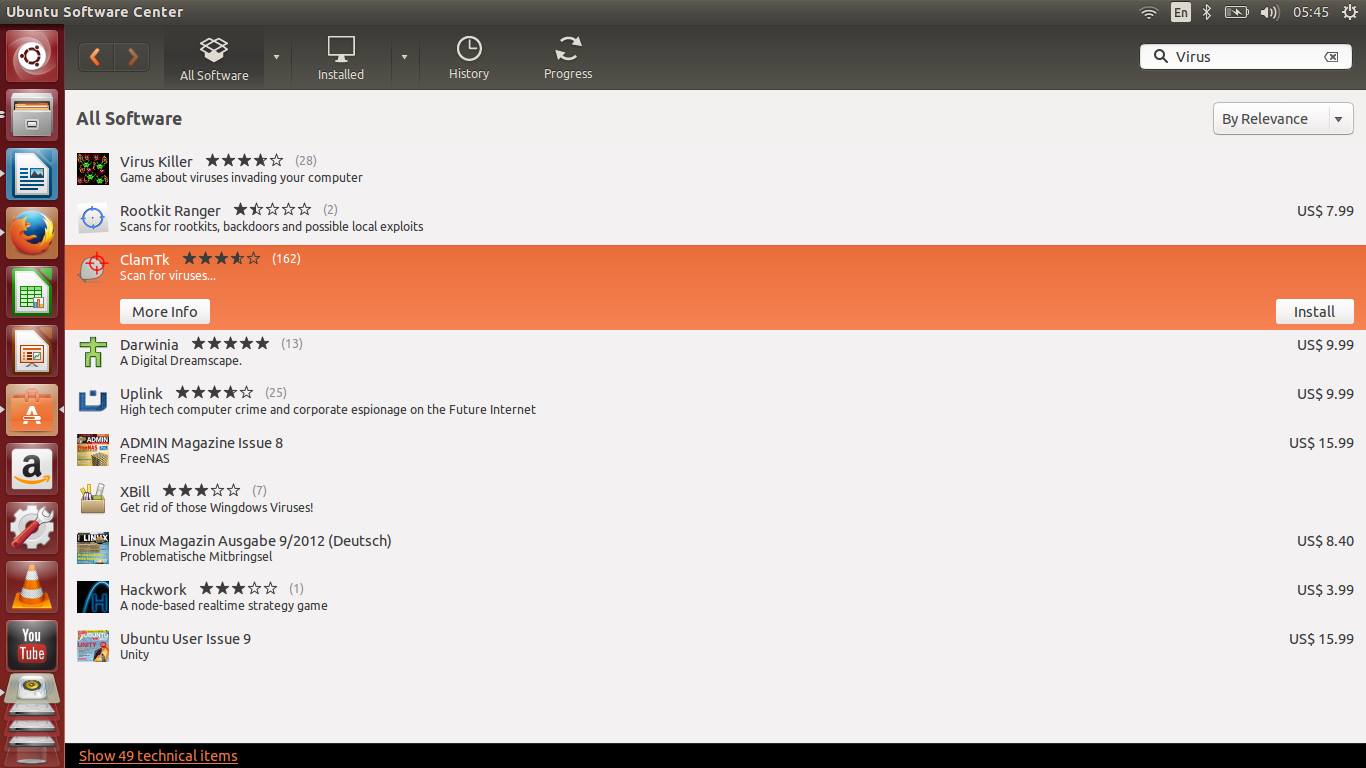
Giao diện USC xuất hiện:



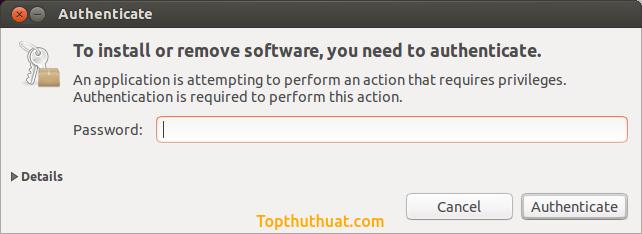
Tại giao diện USC, bạntìm tên phần mềm ClamTk mà bạn muốn cài đặt cho Ubuntu



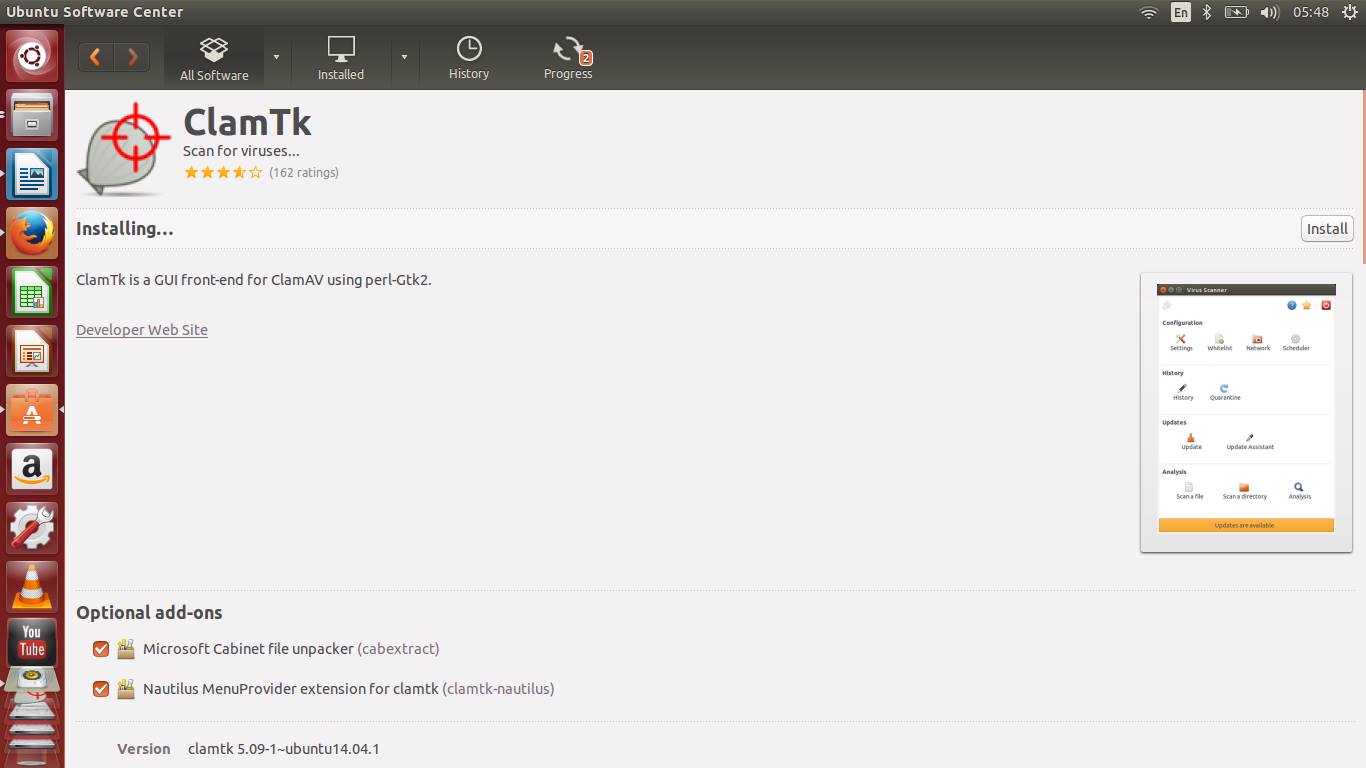
Sau khi đã tìm thấy, bạn chọn vào nút *Install* để tiến hành cài đặt phần mềm vào Ubuntu



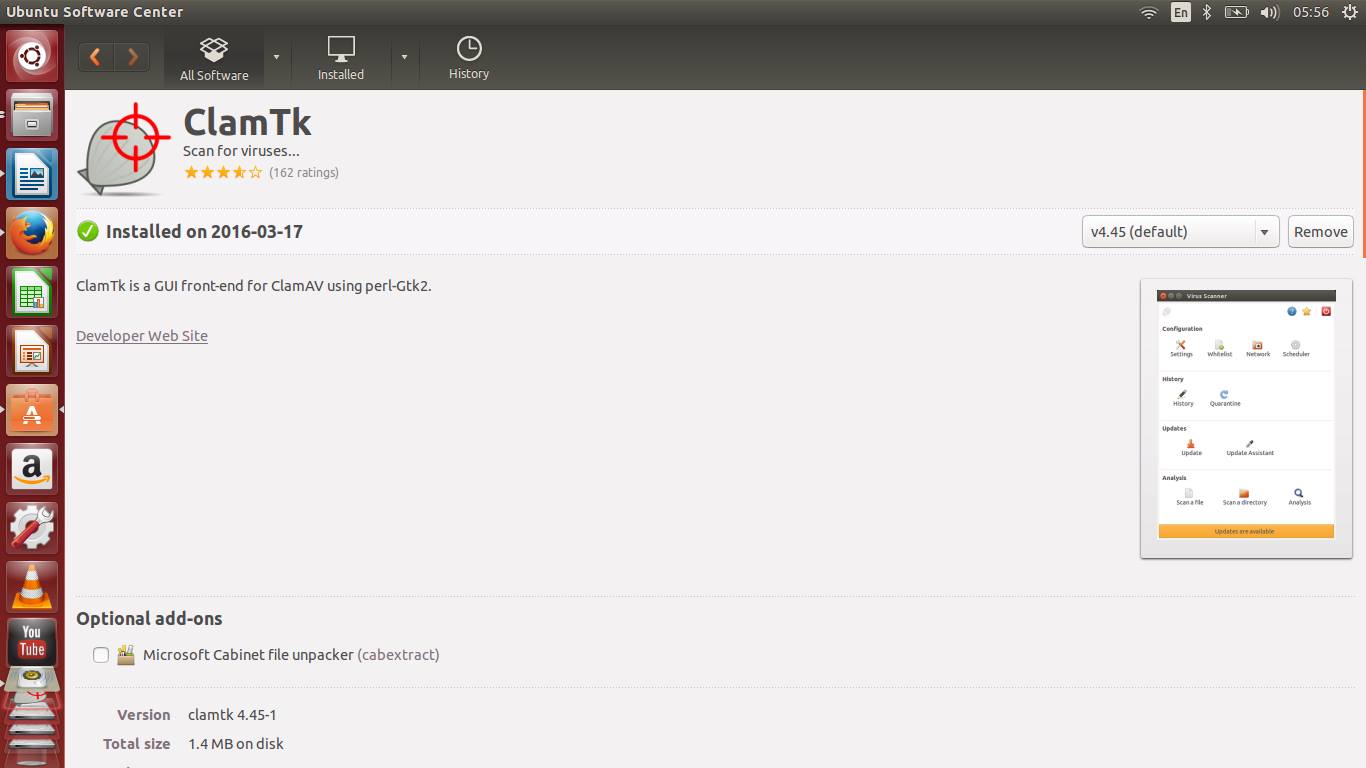
Khi đó, bạn sẽ được yêu cầu nhập mật khẩu tài khoản Ubuntu của bạn:



Sau đó, bạn chỉ cần đợi đến khi phần mềm được cài đặt hoàn tất.



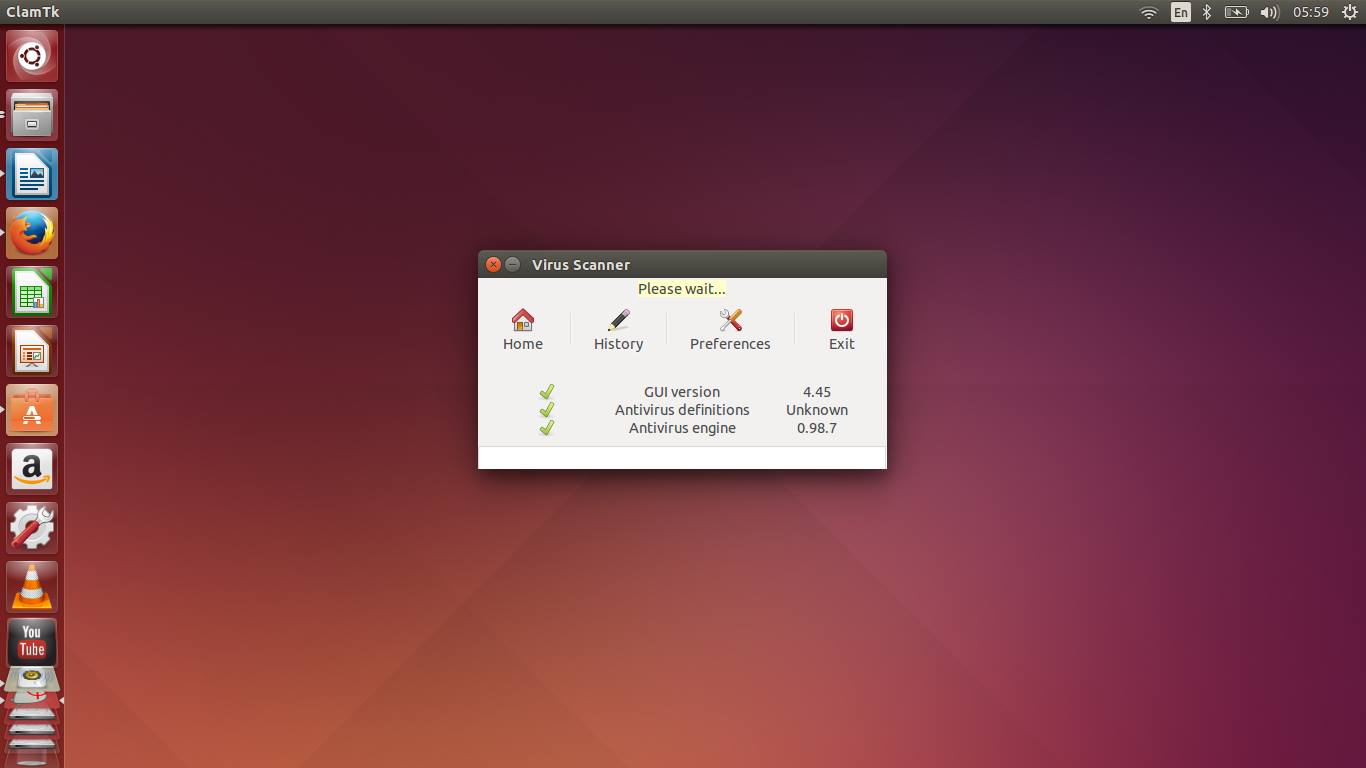
Sau khi cài đặt thành công:



Khi đó biểu tương Icons phần mềm sẽ xuất hiện trên Taskbar.



Giao diện của ClamTk



## 3.4 Các lỗ hổng hiện nay và cách khắc phục

### 3.4.1 Các lỗ hổng hiện nay

* **Hack Linux bằng cách nhấn phím Backspace 28 lần**



***Chỉ cần nhấn phím backspace 28 lần, bạn đã có thể bypass được hệ thống bảo vệ mật khẩu của máy tính Linux!***

Hai nhà nghiên cứu bảo mật đến từ đại học Valencia đã phát hiện ra một bug kì quái trên một vài bản phân phối Linux cho phép bất cứ ai cũng có thể bypass bất cứ loại xác thực nào trong quá trình khởi động bằng cách nhấn phím backspace 28 lần.

Vấn đề không nằm trong kernel hay một hệ điều hành cụ thể nào, nó thực chất là lỗ hổng trong Grub2, ***Grand Unified Bootloader***, thường được sử dụng trong hầu hết các hệ thống Linux để boot hệ điều hành khi máy tính khởi động.

Đây là một lỗ hổng tồn tại từ Grub version 1.98 (2009) –*b391bdb2f2c5ccf29da66cecdbfb7566656a704d*– ảnh hưởng đến hàm *grub\_password\_get ()*.

Để khai thác lỗ hổng trên thiết bị, bạn chỉ cần nhấn 28 lần phím backspace trong ô Grub username. Nó sẽ mở ra một “**Grub rescue shell**”. Điều này cho phép truy cập không cần ủy quyền vào máy tính và khả năng tải một môi trường khác.

Tin tặc có thể lợi dụng điều này để truy cập vào toàn bộ dữ liệu trên máy tính, rồi sau đó đánh cắp hoặc xóa chúng, hoặc có thể cài đặt các mã độc hoặc rootkit.

**Cách khắc phục**: Tin tốt là các nhà nghiên cứu đã tạo ra một bản vá khẩn cấp. Rất nhiều bản phân phối lớn bao gồm [Ubuntu](https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003218.html), [Red Hat](https://rhn.redhat.com/errata/RHSA-2015-2623.html), và [Debian](https://security-tracker.debian.org/tracker/CVE-2015-8370) cũng phát hành bản vá lỗ hổng này.

* **Lỗ hổng nghiêm trọng trong thư viện của Linux**

Một lỗ hổng nghiêm trọng mới được phát hiện trong GNU C Library (glibc), một thành phần cốt lõi trong hầu hết các bản phân phối Linux. Lỗ hổng ảnh hưởng tới gần như tất cả hệ thống Linux và hàng ngàn ứng dụng cũng như các thiết bị có nguy cơ bị tin tặc chiếm quyền kiểm soát.

Chỉ cần nhấn vào một đường dẫn hoặc kết nối đến một máy chủ có thể dẫn đến thực thi mã từ xa (RCE), cho phép tin tặc đánh cắp thông tin tài khoản, theo dõi người dùng, kiểm soát thiết bị và nhiều hơn nữa.

Lỗ hổng mới khá giống lỗ hổng GHOST (CVE-2015-0235) được phát hiện trong năm 2015. GNUC Library (glibc) là một tập hợp code mã nguồn mở được sử dụng trong hàng ngàn ứng dụng và các phiên bản Linux, bao gồm cả các thiết bị phần cứng như bộ định tuyến. Lỗ hổng mới có định danh CVE-2015-7547 là một lỗi tràn bộ nhớ stack trong bộ phân giải DNS phía client vốn được sử dụng để phiên dịch tên miền thành địa chỉ IP.

Lỗ hổng xảy ra khi *getaddrinfo () library function*thực hiện tra cứu tên miền đang được sử dụng, cho phép tin tặc thực hiện mã độc hại. Tin tặc có thể khai thác khi một thiết bị hay ứng dụng thực hiện truy vấn đến một máy chủ DNS độc hại sau đó sẽ được nhận lại mã độc trong bộ nhớ. Mã độc xâm hại ứng dụng và thiết bị sau đó kiểm soát toàn bộ hệ thống.

Các phần mềm bị ảnh hưởng:

* Gần như toàn bộ các bản phân phối Linux
* Các ngôn ngữ lập trình như Python, PHP và Ruby on Rails
* Các ứng dụng sử dụng code Linux để tra cứ địa chỉ IP của tên miền Internet
* Hầu hết các phần mềm Bitcoin

**Cách khắc phục**: Bản chứng minh [Proof-of-Concept](https://github.com/fjserna/CVE-2015-7547) mã khai thác đã được phát hành. Các nhà nghiên cứu Google cùng công ty Red Hat đã phát hành [bản vá](https://sourceware.org/ml/libc-alpha/2016-02/msg00416.html) ngay lập tức. Với các máy chủ, bản vá sẽ được tải về và cập nhật dễ dàng nhưng với những người dùng khác, các ứng dụng phải được biên dịch lại với thư viện glibc mới.

Nếu bạn chưa thể áp dụng bản vá ngay lập tức hãy giới hạn tất cả phản hồi TCP DNS xuống 1024 byte và loại bỏ gói tin UDP DNS lớn hơn 512 byte.

* **Linux Ransomware tấn công máy chủ và đe dọa webmaster**

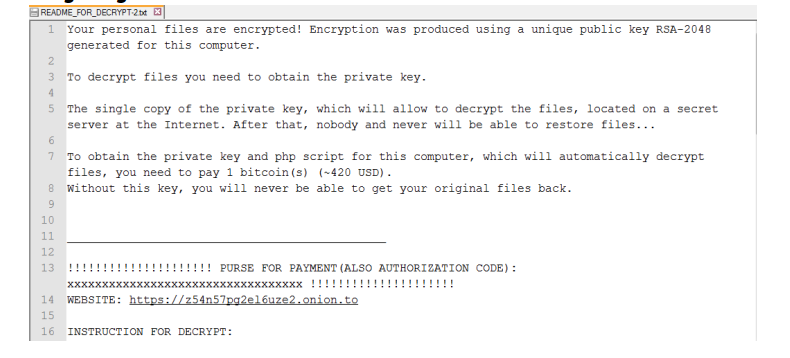
Chỉ trong một vài năm, Ransomware đã dần trở thành một trong những mã độc nguy hiểm nhất, mã hóa toàn bộ nội dung ổ đĩa cứng/máy chủ của nạn nhân và yêu cầu tiền chuộc (thường dưới dạng Bitcoin) để trao đổi khóa giải mã. Tin tặc không gian mạng nhắm đến máy tính, điện thoại thông minh, máy tính bảng, và giờ ảnh hưởng đến cả các website.

Hãng diệt virus Nga Dr.Web đã phát hiện ra Linux.Encoder.1 – một loại linux ransomware mới tấn công máy chủ website nền Linux và mã hóa MySQL, Apache và thư mục home/root rồi yêu cầu 1 Bitcoin (~300 USD) để giải mã file. Ransomware được đưa vào website thông qua các lỗ hổng phổ biến trong website plugin hoặc ứng dụng bên thứ ba.

Sau khi lây nhiễm, mã độc mã hóa toàn bộ file trong chỉ mục Home trên hệ thống cùng với Backup và System Folders chứa file, trang, hình ảnh, thư viện code và script. Sau khi được chạy, ransomware bắt đầu tải về:

* Thông điệp đòi tiền chuộc
* Một file chứa khóa công khai RSA

Sau đó nó bắt đầu xóa toàn bộ file gốc. Khóa RSA được sử dụng để lưu trữ khóa AES dùng để mã hóa file cục bộ trên thiết bị. Các file bị mã hóa sẽ có đuôi. Encrypt và có thông điệp trong mỗi thư mục.

[](http://securitydaily.net/wp-content/uploads/2015/11/ransomware_message.png)

Các file mã hóa thường nằm trong chỉ mục như home, root, MySQL, Apache và nơi có các từ như git, svn, webapp, www, public\_html hoặc backup. Thêm vào đó ransomware cũng tìm các file có phần mở rộng như .js, .css, .properties, .xml, .ruby, .php, .html, .gz, .asp, .rar, .7z, .xls, .pdf, .doc, .avi, .mov, .png, và .jpg.

**Cách khắc phục**: Cho đến khi các nhà nghiên cứu tạo ra được phần mềm giải mã, các webmaster được khuyến cáo sao lưu toàn bộ dữ liệu quan trọng và giữ an toàn trong trường hợp bị tấn công.

* **Lỗ hổng leo thang đặc quyền trong nhân linux**

Một lỗ hổng leo thang đặc quyền đã được xác định trong nhân Linux đang được sử dụng rộng rãi, có thể cho phép kẻ tấn công chiếm quyền kiểm soát hệ thống của người dùng.

Vào năm 2014 các nhà phân phối phổ biến nhất của hệ điều hành mã nguồn mở Linux OS là Debian đã cảnh báo về lỗ hổng này (CVE-2014-3153) trong một bản cập nhật bảo mật, cùng với một số lỗ hổng khác nằm trong nhân Linux có thể dẫn đến một tấn công từ chối dịch vụ.

Quan trọng nhất là lỗ hổng này (CVE-2014-3153) được phát hiện bởi Pinkie Pie, nằm trong Futex subsystem được gọi đến bởi nhân Linux các phiên bản 2.6.32.63/ 3.2.59/ 3.10.41/ 3.12.21/ 3.14.5, có thể được khai thác để thực thi các đoạn mã tùy ý với các đặc quyền của nhân hệ điều hành.

*“Pinkie Pie phát hiện ra một vấn đề trong các sybsytem futex, cho phép người dùng local có thể được cấp ring 0 control thông qua các lời gọi hệ thống trong futex”. “Một người dùng không có đặc quyền có thể lợi dụng lỗ hổng này để gây crash cho nhân hệ thống (kết quả là một cuộc tấn công từ chối dịch vụ) hoặc cho leo thang đặc quyền”.*

Pinkie Pie là một hacker trẻ vô danh có đạo đức và khả năng, người đã được trao thưởng

ít nhất là 100.000 đôla cho việc vượt qua các tính năng bảo mật của Google Chrome, đa phần trong số đó là khai thác sandbox, ở cả hai cuộc thi Pwnium và Pwn2Own hàng năm kể từ 2012.

**Cách khắc phục**: Lời khuyên của nhà nghiên cứu Kees Cook, một nhà nghiên cứu bảo mật về hệ điều hành Google Chrome và Ubuntu cho rằng lỗ hổng được tìm thấy đầu tiên bởi Pinkie Pie ở mức độ cần “sửa chữa khẩn cấp”.*Cook đã viết trên Seclists.org hôm thứ năm rằng:“Lỗ hổng này phải được sửa chữa khẩn cấp vì futex thường có sẵn trong hầu hết các hệ thống Sanboxes của Linux (vì nó được sử dụng như một pthread glibc)”.*

* **Chkrootkit – một lỗ hổng nguy hiểm khác**

Lỗ hổng được chú ý chỉ hai ngày sau khi Thomas Stangner báo cáo một lỗ hổng nghiêm trọng trong Chkrootkit (Check Rootkit) cho phép kẻ tấn công local có quyền truy cập root để giành quyền kiểm soát hệ thống bằng cách thực hiện mã độc bên trong thư mục */tmp*.

Một chương trình căn bản của dựa trên Unix là chkrootkit giúp quản trị hệ thống kiểm tra hệ thống của họ để biết về các rootkit. Các lỗ hổng trong chkrootkit là ***CVE-2014-0476***, thực chất nằm trong chức năng Slapper () trong gói chkrootkit shell script. Một người sử dụng không có quyền root có thể đặt bất kỳ tập tin thực thi độc hại có tên là “update” trong thư mục */tmp* mà sẽ được thực hiện dưới quyền root bất cứ khi nào chkrootkit quét thư mục này cho rootkit.

* **Lỗ hổng khác trong nhân linux**

Một vấn đề an ninh khác (***CVE-2014-3144 và CVE-2014-3145***) cũng đã được phát hiện trong nhân Linux có thể cho phép bất kỳ người dùng local nào cũng có thể gây ra một tấn công từ chối dịch vụ (DoS) thông qua cấu trúc BPF.

Debian đã ban hành bản vá lỗi cho lỗ hổng này và khuyến khích người sử dụng Linux nâng cấp các gói Linux của họ nhằm nhấn mạnh rằng vấn đề này đã được sửa chữa trong bản phân phối ổn định phiên bản 3.2.57-3 + deb7u2 và sẽ vá lỗi trong bản phân phối không ổn định càng sớm càng tốt.

### 3.4.2 Cách bảo vệ

* **25 cách tăng cường bảo mật cho một máy chủ Linux**

1. **Bảo vệ hệ thống vật lý**  
   Loại bỏ các nguy cơ bị boot hệ thống BIOS bằng CD/DVD, đĩa mềm và các thiết bị bên ngoài. Hãyđặt mật khẩu cho BIOS và GRUB để ngăn chặn tất cả các kết nối giữa hệ thống với các thiết bị vật lý bên ngoài.
2. **Phân vùng ổ cứng**  
   Việc phân chia dữ liệu không chỉ khiến cho nó được sắp xếp hợp lý hơn, mà còn giúp các dữ liệu được bảo vệ tốt hơn trong trường hợp có sự cố không mong muốn xảy ra. Khi đó, chỉ có các dữ liệu trong những vùng xảy ra sự cố bị ảnh hưởng, không gây hại tới các gói dữ liệu khác. Một mô hình phân chia bạn có thể học theo, trong đó, các ứng dụng của bên thứ ba nên được cài vào file ‘/opt’/boot/usr/var/home/tmp/opt
3. **Bớt đi các gói dữ liệu không cần thiết, hạn chế lỗ hổng bảo mật**Bạn có bao giờ sử dụng tất cả các gói dịch vụ? Theo chúng tôi, bạn nên bỏ đi những gói tin không cần thiết để tránh việc bị tấn công thông qua những lỗ hổng của gói đó. Hãy kiểm tra lại một lượt xem có những ứng dụng nào không cần đến và gỡ chúng đi.

* Sử dụng lệnh ‘chkconfig’ để tìm các dịch vụ đang được chạy ở mức độ 3

***# /sbin/chkconfig --list |grep '3: on'***

* Một khi đã phát hiện ra những dịch vụ không cần thiết, loại bỏ chúng bằng câu lệnh

***# chkcongfig serviceName off***

* Hoặc có thể sử dụng gói quản lý RPM ví dụ như “yum” hay “apt-get” để liệt kê tất cả các gói tin đã được cài đặt và loại bảo chúng bằng các câu lệnh sau
* ***#yum -y remove package-name***
* ***# sudo apt-get remove package-name***

1. **Kiểm tra các cổng kết nối mạng**Với sự trợ giúp của cú pháp ‘netstat’ bạn có thể kiểm tra tất cả các cổng kết nối mở và các chương trình có liên kết ra bên ngoài.

* Và giống như ở trên, hãy sử dụng ‘chkcongfig’ để loại bỏ chúng.

***# netstat -tulpn***

1. **Sử dụng Secure Shell (SSH)**Các giao thức cũ như Telnet và rlogin chỉ sử dụng những text đơn giản để truyền tin, không có cơ chế mã hóa thông tin. SSH là giao thức an toàn hơn, vì nó sử dụng sẽ mã hóa thông tin trước khi truyền đi trong suốt quá trình giao tiếp giữa người dùng với server.

* Hãy mở file cấu hình chính của SSH và sử dụng những cú pháp sau để giới hạn đăng nhập của người dùng

***# vi /etc/ssh/sshd\_config***

* Loại bỏ Root Login

***PermitRootLogin no***

* Chỉ chấp nhận một vài người dùng đặc biệt

***AllowUsers username***

* Sử dụng giao thức SSH version 2

***Protocol 2***

1. **Thường xuyên update hệ thống**

* Luôn giữ hệ thống của bạn được cập nhật những bản vá, sửa lỗi và nâng cấp phần nhân hệ thống ngay khi có thể.
* ***# yum update***
* ***# yum check-update***

1. **Khóa Cronjobs**Cron có những khả năng tự làm việc, tuy nhiên nó cũng cho phép người dùng tự điều khiển nếu như họ muốn. Có thể điều khiển thông qua các file có địa chỉ ‘/etc/cron.allow’ và ‘etc/cron.deny’. Thêm tên của một người sử dụng vào cron.deny nếu như không muốn họ chỉnh sửa cron, hoặc thêm vào cron.allow nếu cho phép họ sử dụng cron.

* Nếu như muốn tất cả những người sử dụng không thể sử  dụng cron, thêm dòng lệnh ALL vào file ‘cron.deny’

***# echo ALL >>/etc/cron.deny***

1. **Tắt USB stick**

Đã từng rất nhiều lần xảy ra chuyện chúng ta muốn hạn chế người sử dụng kết nối với hệ thống bằng USB để tránh tình trạng đánh cắp thông tin.

* Hãy tạo một file ‘/etc/modprobe.d/no-usb’ và thêm những dòng sau để hệ thống không nhận các thiết bị USB nữa

***install usb-storage /bin/true***

1. **Sử dụng SELinux**

Hệ thống bảo mật nâng cao(SELinux) là một cơ chế bảo mật cung cấp ở vùng nhân. Tắt nó đi đồng nghĩa với việc loại bỏ cơ chế bảo vệ ra khỏi hệ thống. Hãy suy nghĩ thật kĩ mỗi khi muốn tắt nó, đặc biệt nếu hệ thống của bạn cần kết nối internet và có chế độ truy cập là công khai.SELinux có ba chế độ điều khiển sau:

* Enforcing: Chế độ thông thường, kích hoạt SELinux và để nó toàn quyền hoạt động tự do
* Permissive: Trong chế độ này, SELinux sẽ phải gửi những báo cáo cũng như cảnh báo cho người dùng trước mỗi hoạt động. Chế độ này vô cùng hữu ích trong trường hợp chuẩn đoán và xử lý nếu có sự cố xảy ra.
* Disable:tắt SELinux

1. **Loại bỏ các màn hình kiểu KDE và GNOME**Rõ ràng là không cần thiết phải sử dụng các màn hình Window như là KDE hay GNOME cho server của bạn. Bạn có thể tắt hoặc gỡ nó đi để tăng cường bảo mật cho server. Để tắt nó, hãy mở file ‘etc/initab’ và đặt  chạy ở mức độ 3.

* Còn nếu muốn loại bỏ hoàn toàn khỏi hệ thống, hãy sử dụng câu lệnh sau:

***# yum groupmove "X Window System"***

1. **Tắt IPv6**Nếu như bạn không sử dụng IPv6, hãy tắt nó đi bởi vì phần lớn các ứng dụng không đòi hỏi giao thức này và hiện tại, nó cũng không cần thiết cho server nữa.

* Hãy vào file cấu hình mạng, thêm dòng lệnh sau để loại bỏ IPv6:
* ***# vi /etc/sysconfig/network***
* ***NETWORKING\_IPV6=no***
* ***IPV6INIT=no***

1. **Hạn chế sử dụng lại các mật khẩu cũ**Sẽ cực kỳ hữu ích nếu như bạn ngăn chặn việc những người sử dụng đặt lại một trong những mật khẩu cũ của họ. Các mật khẩu sẽ được lưu trữ tại /etc/pam.d/system-auth, file này chỉ có thể truy cập trong chế độ PAM.

* Mở file ‘etc/pam.d/system-auth’ trong RHEL/CentOS/Fedora.

***# vi /etc/pam.d/system-auth***

* Thêm dòng lệnh sau vào mục ‘auth’

***Authsufficientpam\_unix.so likeauth nullok***

* Mở file ‘etc/pam.d/common-password’ trong Ubuntu/Debian/Linux Mint

***# vi /etc/pam.d/common-password***

* Thêm dòng lệnh sau vào mục ‘password’ để ngăn người dùng sử dụng lại 1 trong 5 password gần nhất của họ.

***password sufficientpam\_unix.so nullok use\_authtok md5 shadow remember=5***

* Nếu như người dùng muốn sử dụng lại bất kỳ mật khẩu nào trong số 5 cái mới nhất, họ sẽ nhận được một dòng cảnh báo

***Password has been already used. Choose another.***

1. **Làm thế nào để kiểm tra thời gian sử dụng một password của người sử dụng**

Trong Linux, mật khẩu người dùng được lưu trữ trong file ‘/etc/shadow’ dưới dạng mã hóa. Để kiểm tra thời gian sử dụng password của người sử dụng, bạn sẽ cần sử dụng câu lệnh ‘chage’. Nó sẽ hiển thị lên các thông tin về thời hạn của một mật khẩu theo số liệu về thời gian thay đổi gần nhất. Những thông tin này được hệ thống sử dụng để quyết định khi nào người sử dụng cần thay đổi mật khẩu của họ

***#chage -l username***

* Để thay đổi giới hạn cho một password, sử dụng câu lệnh
* ***#chage -M 60 username***
* ***#chage -M 60 -m 7 -W 7 username***

-M: Số ngày tồn tại tối đa của mật khẩu

-m: Số ngày tối thiểu

-W: Số ngày để đưa ra cảnh báo

1. **Khóa và mở một tài khoản theo cách thủ công**Việc khóa và mở khóa rất hữu dụng, thay vì phải loại bỏ hẳn một tài khoản ra khỏi hệ thống, bạn chỉ cần khóa tài khoản đó lại trong vòng 1 tuần hoặc một tháng.

* Để khóa một tài khoản mà bạn muốn, sử dụng cú pháp sau:

***# paswd -l accountName***

* Lưu ý: Việc khóa thực chất chỉ là thay mật khẩu đã được mã hóa với một sâu kí tự khác. Nếu ai đó muốn truy cập bằng tài khoản này, nó sẽ hiện ra thông báo

***# su - accountName***

***This account is currently not available***

* Để mở khóa và cho phép một mật khẩu bị khóa có thể truy cập lại, sử dụng câu lệnh dưới đây, nó sẽ lại thay thế chuỗi ký tự với mật khẩu được mã hóa

***passwd -u accountName***

1. **Khuyến khích sử dụng những mật khẩu mạnh hơn**Một số lượng lớn người sử dụng chỉ đặt cho mình những mật khẩu yếu và dễ bị hack. ‘pam\_cracklib’ trong chế độ PAM sẽ buộc người dùng phải sử dụng cho mình những mật khẩu mạnh và an toàn hơn.

* Hãy thêm những dòng sau bằng một trình biên soạn:

***# vi etc/pam.d/system-auth***

* Và thêm dòng sau(lcredit,ucredit, dcredit hay ocredit tương ứng với chữ thường, chữ hoa, chữ số và các kí tự khác)

***/lib/security/$ÍA/pam\_cracklist.so retry = 3 minlen=8 lcredit =-1 ucredit=-2 dcredit=-2 ocredit=-1***

1. **Sử dụng Iptables (tường lửa):**Một điều được khuyến khích đó là bật chế độ tường lửa của Linux để kiểm soát những truy cập trái phép vào trong server của bạn. Hãy dùng iptable để có thể kiểm tra những gói tin đến, đi hoặc chuyển tiếp. Chúng ta hoàn toàn có thể xem xét địa chỉ nguồn và đích đến để có quyết định chấp nhận gói tin hay không
2. **Loại bỏ tổ hợp Ctrl+Alt+Delete**Trong hệ điều hành Linux, ấn tổ hợp phím ‘CTRL+ALT+DELETE’ sẽ bắt đầu quá trình reboot hệ thống. Rõ ràng đây không phải và một ý hay, giả sử nếu như có một ai đó lỡ tay ấn nhầm.  
   Tổ hợp phím được định nghĩa trong file’/etc/inttab’.

* Thông thường các dòng lệnh sẽ bị ẩn đi, vì thế chúng ta cần làm nó hiện ra trước.
* ***# Trap CTRL-ALT-DELETE***
* ***#ca:ctrlaltdel:/sbin/shutdown -t3 -r now***

1. **Kiểm tra các tài khoản không có password**Bất kể tài khoản nào mà không có mật khẩu đồng nghĩa với việc nó đang mở ra một lối truy cập trái phép cho bất kỳ ai. Vì thế bạn nên chắc chắn rằng tất cả các tài khoản đều sử dụng một mật khẩu mạnh và không ai có thể truy cập một cách trái phép được. Các tài khoản không có mật khẩu là một đe dọa về bảo mật.

* Để kiểm tra các tài khoản này sử dụng câu lệnh sau

***#cat /etc/shadow |awk -F:'($2=="") {print $1}'***

1. **Hiển thị những tiêu đề cảnh báo SSH trước khi đăng nhập**Sẽ là rất tốt nếu như bạn luôn đưa ra những tiêu đề về cảnh báo bảo mật SSH mỗi khi có người dùng đăng nhập.
2. **Giám sát các hành vi của người dùng**Nếu có quá nhiều người sử dụng server của bạn, việc thu thập và phân tích các thông tin về mỗi hành vi của họ là vô cùng quan trọng. Tuy nhiên, làm thế nào để có thể thực hiện được việc này?  
   Có hai công cụ vô cùng hữu ích cho chúng ta đó là ‘psacct’ và ‘acct’, giúp chúng ta quản lý mọi hành vi của những người sử dụng và các tiến trình diễn ra trong hệ thống.  
   Những công cụ này chạy ngầm trong hệ thống và ghi lại từng hành vi của người sử dụng, cũng như theo dõi việc sử dụng tài nguyên cho các dịch vụ, ví dụ như Apache, MySQL, SSH, FTP…
3. **Kiểm tra, đánh giá các hoạt động một cách thường xuyên**Hãy di chuyển các hoạt động vào log server, điều này tránh việc những kẻ tấn công có thể xâm nhập vào và chỉnh sửa các hoạt động hệ thống. Thông thường, các file lưu trữ các hoạt động được đặt tại địa chỉ ‘/var/log’.
4. **Xây dựng file Backup**Trong mọi hệ thống, luôn cần có một tệp tin làm nhiệm vụ sao lưu và phục hồi lại mỗi khi có sự cố xảy ra.
5. **Kết nối NIC:**

* Có hai loại kết nối NIC sau:
* mode=0 Round Robin
* mode=1 kích hoạt và backup
* Khi xây dựng kết nối, chúng ta “kéo” hai hoặc nhiều hơn những kết nối lại với nhau và dùng một trường kết nối ảo để sử dụng IP giao tiếp với các server khác, Nếu có một thẻ NIC bị tạm ngừng hoặc không thể sử dụng được, thì các hoạt động vẫn diễn ra bình thường.

1. **Đặt địa chỉ /boot ở chế độ read-only**Lõi Linux và những phần tử có liên quan đều nằm trong địa chỉ /boot vơi chế độ mặc định read-write. Chuyển về chế đọ read-only sẽ giảm thiểu các nguy cơ bị chỉnh sửa từ bên ngoài hoặc gây ra các lỗi với file boot.

* Để làm điều này, mở file ‘/etc/ftad’

***# vi/etc/fstad***

* Và thêm dòng lệnh sau vào cuối, lưu rồi đóng file lại

***LABEL=/boot/bootevt2default***

* Lưu ý rằng, nếu bạn muốn nâng cấp nhân hệ thống bạn cần phải đặt lại về chế độ read-write.

1. **Bỏ qua ICMP hoặc các yêu cầu quảng cáo**

* Thêm dòng sau vào “/etc/sysctl.conf” để bỏ qua các yêu cầu ping hay quảng cáo
* ***net.ipv4.icmp\_echo\_ignore\_all = 1***
* ***net.ipv4.icmp\_echo\_ignore\_broadcasts = 1***
* Lưu lại các thay đổi cấu hình trên bằng câu lệnh

***#sysct1 -p***

# KẾT LUẬN

Qua quá trình tìm hiểu và thực nghiệm cho thấy Linux có những nhược điểm và ưu điểm nhất định.Ngoài việc khó sử dụng cho những ai mới bắt đầu dùng thì Linux thực sự rất phù hợp cho những ai thích tìm tòi và sáng tạo trong lĩnh vực khoa học và công nghệ vì Linux có tính bảo mật cao có thể được xem như miễn nhiễm với virus.

**PHỤ LỤC**

**DANH MỤC TÀI LIỆU THAM KHẢO**

Tiếng việt

<https://123tailieu.com/luan-van-an-toan-va-bao-mat-tren-he-dieu-hanh-linux.html>

<http://doc.edu.vn/tai-lieu/bai-giang-tong-quan-ve-linux-58863/>

<http://blogtinhoc.vn/cach-cai-ubuntu-14-04-12-04-song-song-voi-windows-7-8.html>

<http://www.slideshare.net/babyinternet/l4u>

<https://vi.wikipedia.org/wiki/Linux>

<http://securitydaily.net/>

Tiếng anh

<http://www.linuxuser.co.uk/features/security-in-linux/2>

<https://websetnet.com/vi/set-up-a-firewall-using-iptables-on-ubuntu-14-04/>

<http://www.techradar.com/news/software/operating-systems/how-to-secure-your-linux-system-915651>

<http://www.aboutlinux.info/2005/10/using-tcp-wrappers-to-secure-linux.html>

<http://www.tuxradar.com/content/10-simple-ways-make-your-linux-box-more-secure>

<http://linas.org/linux/secure.html>

<http://www.tecmint.com/linux-server-hardening-security-tips/>

Robb H. Tracy, CompTIA® Linux+ Certification Study Guide Part 2 (Linux 2)