Bản tiếng việt cs296

Introduction

Hệ điều hành được biết đến như một nền tảng hỗ trợ để giúp cho việc tương tác với các application của và hỗ trợ cho người dùng với các tác vụ phù hợp. Hệ đề hành được điều chỉnh phù hợp với nhu cầu và tác vụ, trong đó Hề điều hành dành cho server được tùy chỉnh phù hợp cho việc tương tác và tiếp nhận thông tin và process chúng với cường độ cao và trong đó có những hệ điều hành tiêu biểu được dùng cho các máy chủ, được sử dụng cho các doanh nghiệp được điều chỉnh riêng và được process để có thể tiếp nhận nhiều đối tượng cùng tương tác với máy chủ cùng một thời điểm. Vì tác vụ được dùng để nhận một lượng thông tin, xử lý thông tin và trả về lớn, cũng như giữ những thông tin quan trọng của doanh nghiệp và người dùng, độ ổn định và an toàn là những phần quan trọng của một hệ điều hành. Trong đó để tính an toàn của một hệ điều hành được xử lý một cách đặc trưng và tính quan trọng của nó nên trong các hệ điều hành được dùng cho máy chủ được sử dụng, Centos OS là một trong số chúng với việc áp dụng bảo mật trong hệ điều hành cho máy chủ. Và để giải thích về tính an toàn của hệ điều hành này sẽ được giải thích sơ bộ, lưu ý tìm hiểu có khả năng không đúng hoàn toàn và sẽ có những sai sót trong quá trình nghiên cứu vì không có quỹ tiền để có những bài báo, bài nghiên cứu. Bài nghiên cứu được chia làm 3 phần chính bao gồm, lịch sử hình thành của hệ điều hành Centos, RHEL nguồn code được dùng như một nguồn code cho linux O strong Centos, tính khả thù và cách thức và khả năng bảo mật của hệ điều hành dựa trên những điều trên. Đồng thời ngồn code của RHEL và khả năng báo mật của nó trong việc bị các hacker tấn công và lỗ hỗng được vá sau những khoản thời gian.

Lịch sử

Centos OS là một hệ điều hành được sử dụng và khá phổ biến khi được áp dụng cho những máy chủ của các doanh nghiệp, Theo Wikipedia Centos được lập trinhgf phiên bản đầu tiên với Centos ver 2 vào năm 2004 và phát triển dựa trên RHEL version 2 1SA được dùng trong hệ điều hành này cho tới version thứ 8 được nâng cấp và điều chỉnh cho thế hệ chip có cấu trúc là 64x để hỗ trợ cho các phần cứng với cấu trúc hiện hành và được phát triển, nâng cao hiệu suất làm việc của các phần cứng và các ứng dụng được sử dụng một cách tương thức và nguồn thông tin được xử lý nhanh, hiệu quả cũng như an toàn hơn. Với dự án Centos Os là một hệ điều hành miễn phí

Redhat

Trong centos được nhắc tới việc sử dụng nguồn code từ Red Hat Enterprise Linux đây là mã nguồn mở được Red Hat phân phối tự do cho các hệ điều hành bắt đầu từ version 2. Trong đó Community enterprise thuộc RED Hat, centos được tạo dựng từ mã nguồn mở của Red Hat Enterprise linux, (đoạn này bắt đầu nói về red hat và mã nguồn mở của nó và các phiên bản hiện tại của mã nguồn này.) cũng như mã nguồn được phát triển dựa trên ngôn ngữ lập trình C++.

* Tiếp theo nói về phần bảo mật của centos,

Nói về việc centos quan tâm tới việc ngăn chặn những loại tấn công từ troạn malware và firmware đến các hề điều hành, được đem đến bằng những (sample từ source)

Sau đấy giải thích cách thức hoạt động của hệ điều hành trong việc bảo vệ máy chủ khỏi nhũng cuộc tấn công, thủ công như sử dụng usb ddeeer tác động trực tiếp đến hệ điều hành của thiết bị đang sử Centos

Tiếp theo, hệ điều hành phân biệt và làm rõ các tính hiệu nhận về bằng cách sử scap như một công cụ hỗ trợ hệ điều hành trong việc phát hiện những cuộc tấn với lưu lượng thông tin tới lớn như DDos,

Explain:

Vì đây là mã nguồn mở cũng như là nền tảng của một hệ điều hành nó phát triển và chưa đựng nhưng thành phần cơ bản của một hệ điều hành (bắt đàu nói về các thành phần và ngon ngữ của nó)

Sau đấy nói đến ngôn ngữ lập trình được dùng để phát triển hệ điều hành ---. Vì tính chất đặc biệt của ngôn ngữ C++ nên có những bất cập cơ bản giwuax ngôn ngữ và có nhiều nguồn thư viện được dùng hỗ trợ nó.

Bảo mật trong Centos:

Về phần bảo mật của hệ điều hành red hat đã phát triển vì nó dựa trên mã nguồn mở từ red hat, nên dựa trên tài liệu về mã nguồn tiêm được, nó giải và cung cấp khả năng SCAP để hỗ trợ trong việc bảo vệ của từ nhưng cuộc tấn công mạng, đồng thơi hỗ trợ quan sát , kiểm tra bằng những log như một cách để Monitoring device activity cũng như phòng được việc máy chủ bị tấn công và phát hiện sớm có cuộc tấn công đê có những phương án phòng thủ phù hợp.

Nói them nhiều nữa về cái đấy cũng như quote từ references

Nói về centos,

Vì đi

Nếu lên cách thức về hiểu biết bảo mật của hệ điều hành khi có một cuộc tấn công xảy ra

RHEL USBGuard về việc bảo vệ chống lại trojan và có thể làm bảo vệ máy khỏi cuộc tấn công mạng, loại khác nhau nhá

Cryptography policies

Advance Security: In this chapter, we looked at three important tasks that provide advanced security for your CentOS server. Specifically, we looked at how to generate and use digital certificates to secure TCP connections with TLS. We also looked at using the RPM and AIDE tools to monitor the disk for unauthorized changes, as well as how to use netfilter to monitor the network for connection attempts. Finally, we looked at the core aspects of running SELinux such as selecting the mode, the importance of context information, and how to maintain it. In the next chapter, we will take an in-depth look at netfilter and how to build an advanced firewall. We will also look at restricting network services using tcp\_wrappers and setting up a central log server.

Mặc dù hệ điều hành Centos không kế thừa các chứng nhận hoặc đánh giá từ chính RED Hat Enterrprise Linux. Nhưng Centos vẫn sử dụng mã nguồn từ RHEL để bổ sung cũng như cũng cố tính an toàn của hệ điều hành.

Trong hệ điều hành centos việc sử dụng mã nguồn từ red hat để nâng cao cũng như bảo vệ máy khỏi những cách tấn công thủ công như sử USB attack. Centos OS, sử dụng USBGuard từ mã nguồn RHEL để tranh khỏi những cuộc tấn công như: spyware, malware, or trojan. Nhầm ngăn chặn việc bị đánh cấp thông tin từ máy chủ và tổn thương khỏi hệ thống đang được sử dụng. Việc sử dụng USBGuard cho phép hệ điều hành có thể ngăn chặn và authorizing cho các thiết bị USB cũng như tác động và chỉnh sửa quyền truy cập thiết bị USB với hệ điều hành. Điều này cho phép thiết bị đang vận hành hệ điều hành Centos có thể tránh sự xâm nhập từ thiết bị khác và nhận những mã độc một cách gián tiếp.

Mặc khác , CentOS thường được sử dụng cho các ứng dụng Linux yêu cầu hiệu suất thời gian thực hoặc cho các máy chủ hệ thống. CentOS tương đối có chu kỳ hỗ trợ và phát hành dài hơn, dẫn đến một hệ thống rất ổn định. Dù vậy công nghệ gia cố an ninh. Đây là cơ sở bản đầu để tạo các lệnh được sử dụng trong đề xuất từ CentOS 7 của Fank Caviggia. Mục tiêu của các tập lệnh là cấu hình và củng cố

cơ sở CentOS ISO sử dụng Hướng dẫn bảo mật SCAP (SSG). Red Hat duy trì một RHEL ngã ba dựa trên dự án của Caviggia [9]. Việc tăng cường bảo mật được thực hiện bằng cách sử dụng công nghệ khởi động tiêu chuẩn của RHEL.

Dù vậy mã nguồn mà CentOS vẫn có mặc hạn chế của nó trong việc đảm tính an toàn của hệ điều hành