**TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI**

**VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG**

──────── \* ───────



**BÀI TẬP LỚN**

**MÔN: Nhập Môn An Toàn Thông Tin**

**Đề tài: Rà quét lỗ hổng bảo mật cho Windows, Unix-Linux**

**Sinh viên thực hiện**:

Phạm Văn Thành - 20173380

Nguyễn Văn Thông - 20173390

Nguyễn Công Vượng - 20173475

**Lớp**  : **KHMT.02 – K62**

**Giáo viên hướng dẫn** : **PGS.TS. NGUYỄN LINH GIANg**

***Hà Nội, tháng 6 năm 2020***

**Mục Lục**

[LỜI NÓI ĐẦU 3](#_Toc42504545)

[1. Khái niệm lỗ hổng 4](#_Toc42504546)

[2. Nguyên nhân gây ra lỗ hổn bảo mật 5](#_Toc42504547)

[3. Các loại lỗ hổng bảo mật 5](#_Toc42504548)

[3.1. Lỗ hổng loại C: 6](#_Toc42504549)

[3.2. Lỗ hổng loại B: 7](#_Toc42504550)

[3.3. Lỗ hổng loại A: 9](#_Toc42504551)

[4. Đánh giá lỗ hổng bảo mật 10](#_Toc42504552)

[4.3.1. Tạo đường cơ sở 11](#_Toc42504553)

[4.3.2. Đánh giá lỗ hổng bảo mật 12](#_Toc42504554)

[5. Lỗ hổng của Window, Linux(Ví dụ) 15](#_Toc42504555)

[5.1. Các lỗ hổng bảo mật trên Window. 15](#_Toc42504556)

[5.2. Lỗ hổng bảo mật của Linux 17](#_Toc42504557)

[6. Rò quét lỗ hổng bảo mật 18](#_Toc42504558)

# 

## LỜI NÓI ĐẦU

An toàn bảo mật thông tin là vấn đề cấp bách và quan trọng hiện nay. Việc tấn công hệ thống ngày càng gia tăng cho thấy vẫn còn rất nhiều lỗ hổng trong hệ thống.

Để thực hiện được bài cáo này bọn em đã tham khảo rất nhiều tài liệu trên mạng để hiểu hơn về lỗ hổng, cách rò quét và vá lỗ hỗng . Tuy nhiên, chắc chắn vẫn còn những thiếu sót mắc phải trong quá trình tìm hiểu, rất mong nhận được sự góp ý và chỉ bảo từ thầy, để chúng em có thể hoàn thiện hơn.

## Khái niệm lỗ hổng

#### Khái niệm lỗ hổng được hiểu là những điểm yếu trên hệ thống hoặc ần chứa trong một dịch vụ nào đó của hệ thống. trở thành miếng mồi béo bở đối với các hacker, chúng thường cố gắng tìm ra các lỗ hổng này và dựa vào đó để thâm nhập trái phép chiếm đoạt hoặc hủy hoại tài liệu, hệ thống.

Hệ điều hành Microsoft Windows có nguồn gốc phát triển cho các máy tính cá nhân và các mạng an toàn, tuy nhiên nó lại không an toàn đối với mạng phi chính phủ như Internet.

Trong giai đoại ban đầu, Microsoft thiết kế hệ điều hành Microsoft Windows mà chưa nghĩ tới tầm quan trọng của Internet khi gắn liền với nó. Điều đó đã dẫn tới một số điểm yếu là các lỗ hổng bảo mật(Security holes).

Một lỗ hổng bảo mật cho phép một người nào đó xâm nhập vào máy tính của bạn qua đường kết nối Internet. Những lỗ hổng nhỏ có thể chỉ cho phép truy cập vào clipboard của bạn, nhưng những lỗ hổng lớn có thể cho phép họ tiếp quản hoàn toàn máy tính của bạn.

Các hệ điều hành khác như linux, mac os cũng có các lỗ hổng bảo mật. Như vậy lỗ hổng bảo mật là một trong những nguyên nhân dẫn đến sự mất an toàn của các hệ thống máy tính khi kết nối Internet.

Để thực hiện cơ chế an toàn , các hệ điều hành ( hoặc căc Website) phải được thiết kế để đáp ứng các yêu cầu về mặt an toàn đặt ra. Tuy nhiên, trên thực tế, việc thiết kế các hệ điều hành chỉ đạt đến mức độ tiếp cận các yêu cầu an toàn chứ không đáp ứng được chúng một cách hoàn toàn. Những nơi mà yêu cầu thiết kế bị phá vỡ gọi là các lỗ hổng.

Ví dụ về một số lỗ hổng thường gặp: Lỗi xử lý các yêu cầu không được dự kiến trước trong IIS; lỗi tràn bộ đệm;Điểm yếu trong việc xác thực đối với các tài khoản không mật khẩu hoặc mật khẩu yếu…

## 

## Nguyên nhân gây ra lỗ hổn bảo mật

Có nhiều nguyên nhân gây ra lỗ hổng bảo mật: có thể do lỗi của bản thân hệ thống, hoặc do người quản trị hệ thống yêu kém không hiểu sâu sắc các dịch vụ cung cấp hoặc do người sử dụng có ý thức bảo mật kém click vào các đường link lạ hay tải về các ứng dụng độc hại.

Lỗ hổng bảo mật có mức độ ảnh hưởng khách nhau. Có những lỗ hổng chỉ ảnh hưởng đến chất lượng dịch vụ cung cấp nhưng cũng có những lổ hổng ảnh hưởng tới cả hệ thống hoặc làm ngưng trệ dịch vụ.

Do lỗi bản thân hệ thống, do người quản trị yếu kém không hiểu sâu sắc các dịch vụ cung cấp, do người sử dụng có ý thức bảo mật kém. Điểm yếu ở yếu tố con người cũng được xem là lỗ hổng bảo mật.

Trong các lỗ hổng bảo mật khi **k**hái niệm lỗ hổng phần mềm được nhắc đến khác nhiều. Đây chính là lỗi phần mềm mà người khác có thể khai thác để thâm nhập thêm các đoạn mã, thay đổi cách vận hành…Hệ thống phần mềm càng đồ sợ, phức tạp việc kiểm soát các lổ hổng càng trở nên khó khăn

## Các loại lỗ hổng bảo mật

Có rất nhiều tổ chức khác nhau phân loại các lỗ hổng bảo mật. Theo Bộ Quốc Phòng Mỹ, các loại lỗ hổng bảo mật trên một hệ thống gồm:

### 3.1. Lỗ hổng loại C:

Các loại lỗ hổng này cho phép thực hiện các phương thức tấn công DoS (Dinal of Service – Từ chối dịch vụ). Mức độ nguy hiểm thấp, chỉ ảnh hưởng tới chất lượng dịch vụ, có thể làm ngưng trệ, gián đoạn hệ thống, không làm phá hỏng dữ liệu hoặc đạt được quyền truy cập bất hợp pháp.

DoS là hình thức tấn công sử dụng các giao thức ở tầng Internet trong bộ giao thức TCP/IP để làm hệ thống ngưng trệ dẫn đến tình trạng từ chối người sử dụng hợp pháp truy nhập hay sử dụng hệ thống. Một số lượng lớn gói tin được gửi tới server trong khoảng thời gian liên tục làm cho hệ thống trở nên quá tải, kết quả server đáp ứng chậm hoặc không thể đáp ứng các yêu cầu từ client gửi tới.

Các dịch vụ có chứa đựng lỗ hổng cho phép thực hiện các cuộc tấn công DoS có thể được nâng cấp hoặc sữa chữa bằng các phiên bản mới hơn của nhà cung cấp dịch vụ. Hiện nay chưa có giải pháp toàn diện nào khắc phục các lỗ hổng này vì bản thân việc thiết kế giao thức ở tầng Internet(IP) nói riêng và bộ giao thức TCP/IP đã chứa đựng những nguy cơ tiềm tàng của các lỗ hổng này.Tuy nhiên, mức độ nguy hiểm của các lỗ hổng loại này được xếp loại C; ít nguy hiểm vì chúng chỉ làm gián đoạn cung cấp dịch vụ của hệ thông trong một thời gian mà không làm nguy hại đến dữ liệu và người tấn công cũng không đạt được quyền truy nhập bất hợp pháp vào hệ thông.

Một lỗ hổng loại C khác cũng thường thấy đó là các điểmyếu của dịch vụ cho phép thực hiện tấn công làm ngưng trệ hệ thống của người sử dụng cuối; chủ yếu với hình thức tấn công này là sử dụng dịch vụ Web. Giả sử: trên một Web Server có những trang Web trong đó có chứa các đoạn mã Java hoặc JavaScripts. làm "treo" hệ thông của người sử dụng trình duyệt Web của Netscape bằng các bước sau:

- Viết các đoạn mã để nhận biết được Web Browers sử dụng Netscape

- Nếu sử dụng Netscape. sẽ tạo một vòng lặp vô thời hạn sinh ra vô số các cửa số, trong mồi của số đó nối đến các Web Server khác nhau.

Với một hình thức tấn công đơn giản này, có thể làm treo hệ thông. Đây cũng là một hình thức tấn công kiểu DOS. Người sử dụng trong trường hợp này chỉ có thể khởi động lại hệ thống. Một lỗ hổng loại C khác cũng thường gặp đối với các hệ thống mail là không xây dựng các cơ chế anti-relay (chống relay) cho phép thực hiện các hành động spam mail. Như chúng ta đã biết, cơ chế hoạt động của dịch vụ thư điện tử là luu và chuyển tiếp; một số hệ thông mail không có các xác thực khi người dùng gửi thư. dân đến tình trạng các đối tượng tấn công lợi dụng các máy chủ mail này để thực hiện spam mail; Spam mail là hành động nhằm tê liệt dịch vụ mail của hệ thông bằngcách gửi một số lượng lớn các messages tới một địa chỉ không xác định, vì máy chủ mail luôn phải tốn năng lực đi tìm những địa chỉ không có thực dẫn đến tình trạng ngưng trệ dịch vụ. Số lượng các messages có thể sinh ra từ các chương trình làm bomthu rất phổ biến trên mạng Internet.

### 3.2. Lỗ hổng loại B:

Các lỗ hồng cho phép người sử dụng có thêm các quyền trên hệ thống mà không cần thực hiện kiểm tra tính hợp lệ. Mức độ nguy hiểm trung bình; Những lỗ hổng này thường có trong các ứng dụng trên hệ thống; có thể dân đến mất hoặc lộ thôngtin yêu cầu bảo mật. Lỗ hổng loại này có mức độ nguy hiểm hơn lỗ hổng loại C cho phép người sử dụng nội bộ có thể chiếm được quyền cao hơn hoặc truy nhập không hợp pháp.

Những lỗ hổng loại này thường xuất hiện trong các dịch vụ trên hệ thống. Người sử dụng “local" được hiểu là người đã có quyền truy nhập vào hệ thông với một số quyền hạn nhất định.

Ta sẽ phân tích một số lỗ hổng loại B thường xuất hiện trong các ứng dụng:

Sendmail: là một chương trình được sử dụng rất phổ biến trên hệ thống UNIX để thực hiện gửi thư điện từ cho những người sử dụng trong nội bộ mạng. Thông thường, sendmail là một daemon chạy ở chế độ nên được kích hoạt khi khởi động hệ thống. Trong trạng thái, hoạt động, sendmail mở port 25 đợi một yêu cầu tới sẽ thực hiện gửi hoặc chuyển tiếp thư.

Sendmail khi được kích hoạt sẽ chạy dưới quyền root hoặc quyền tương ứng (vì liên quan đến các hành động tạo file và ghi log file). Lợi dụng đặc điểm này và một số lỗ hổng trong các đoạn mã của sendmail. mà các đối tượng tấn công có thể dùng sendmail để đạt được quyền root trên hệ thống.

Để khắc phục lỗi của sendmail cân tham gia các nhóm tin về bảo mệt; vì sendmail là chương trình có khá nhiều lõi; nhưng cũng có nhiều người sử dụng nên các lỗ hổng bảo mặt thường được phát hiện và khắc phục nhanh chóng. Khi phát hiện lỗ hổng trong sendmail cần nâng cấp. thay thế phiên bản sendmail đang sử dụng.

Một loạt các vấn đề khác về quyền sử dụng chương trình trên UNIX cũng thường gây nên các lỗ hổng loại B. Vì trên hệ thống UNIX, một chương trình có thể được thực thi với 2 khả năng:

- Người chủ sở hữu chương trình đó kích hoạt chạy.

- Người mang quyền của người chủ sở hữu chủ nhân của file đó.

Các loại lỗ hổng loại B khác: một dạng khác của lỗ hổng loại B xảy ra đối với các chương trình có mã nguồn viết bằng C.

Những chương trình viết bằng C thường sử dụng một vùng đệm là một vùng trong bộ nhớ sử dụng để lưu dữ liệu trước khi xử lý. Những người lập trình thường sử dụng vùng đệm trong bộ nhớ trước khi gán một khoảng không gian bộ nhớ cho từng khối dữ liệu. Ví dụ, người sử dụng viết chương trình nhập trường tên người sử dụng; qui định trường này dài 20 ký tự. Do đó họ sẽ khai báo:

**char first\_name [20];**

Với khai báo này. cho phép người sử dụng nhập vào tối đa 20 ký tự. Khi nhập dữ liệu, trước tiên dữ liệu được lưu ở vùng đệm; nếu người sử dụng nhập vào 35 ký tư; sẽ xảy ra hiện tượng tràn vùng đệm và kết quả 15 ký tự dư thừa sẽ nằm ở một vị trí không kiểm soát được trong bộ nhớ. Đối với những người tấn công. có thể lợi dụng lỗ hổng này để nhập vào những ký tự đặc biệt. để thực thi một số lệnh đặc biệt trên hệ thông. Thông thường, lỗ hổng này thường được lợi dụng bởi những người sử dụng trên hệ thông để đạt được quyền root không hợp lệ.

Việc kiểm soát chặt chẽ cấu hình hệ thống và các chương trình sẽ hạn chế được các lỗ hổng loại B.

### 3.3. Lỗ hổng loại A:

cảnh báo nguy hiểm cho phép người ngoài hệ thống có thể truy cập hợp pháp vào hệ thống dẫn đến phá hủy hệ thống.

Nguyên nhân của lỗ hổng này thường do quản trị yếu kém. Những lỗ hổng này có sẵn trên phần mềm mà người quản trị không nhận biết.

## Đánh giá lỗ hổng bảo mật

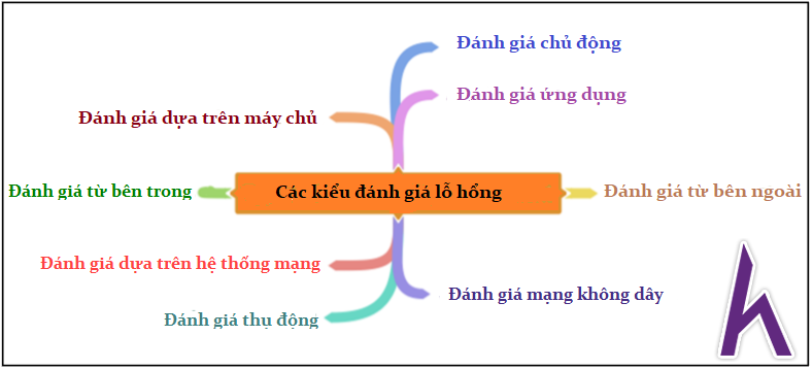
* 1. Khái niệm đánh giá lỗ hổng bảo mật

Đây là nhiệm vụ cơ bản **penetration tester** phải thực hiện để tìm ra các lỗ hổng bảo mật trong một môi trường hệ thống. Việc đánh giá lỗ hổng bảo mật bao gồm tìm ra những điểm yếu, lỗi thiết kế hay bất cứ vấn đề bảo mật nào có thể khai thác để sử dụng hệ điều hành, ứng dụng hay website sai mục đích. Những lỗ hổng gồm có sai sót cấu hình, cấu hình mặc định, lỗi tràn bộ đệm (buffer overflow), lỗi hệ điều hành, dịch vụ mở (open services) và các lỗ hổng khác.

Hiện nay **quản trị viên hệ thống**và **pentester** có nhiều công cụ khác nhau để quét lỗ hổng bảo mật trong một hệ thống mạng. Những lỗ hổng được tìm thấy chia thành ba loại khác nhau dựa trên mức độ an ninh của nó, ví dụ thấp, trung bình hay cao. Bên cạnh đó, chúng cũng được phân loại dựa trên quy mô khai thác như gần hay xa

**Đánh giá lỗ hổng bảo mật** là quá trình kiểm tra, tìm tòi, nhận diện các biện pháp an toàn cũng như lỗ hổng của hệ thống và ứng dụng. Các hệ thống và ứng dụng được kiểm tra để nhận định tính hiệu quả của các tầng bảo mật hiện thời trong việc chống lại các tấn công và lạm dụng. Đánh giá lỗ hổng bảo mật cũng giúp nhận diện những lỗ hổng có thể khai thác, sự thiếu tầng bảo mật và những thông tin máy quét có thể phát hiện

* 1. Các loại đánh giá lỗ hổng bảo mật
* **Đánh giá chủ động**: Đánh giá chủ động bao gồm việc trực tiếp gửi yêu cầu đến live network và kiểm tra các phản hồi. Nói ngắn gọn, quá trình đánh giá này yêu cầu thăm dò máy chủ mục tiêu.
* **Đánh giá thụ động**: Đánh giá thụ động bao gồm việc nghe trộm gói tin ( packet sniffing ) để tìm ra lỗ hổng, running services, open ports và các thông tin khác. Đây là quá trình đánh giá không can thiệp vào máy chủ mục tiêu.
* **Đánh giá từ bên ngoài**: Đây là quá trình đánh giá mà mục tiêu hacking là tìm ra lỗ hổng để khai thác từ bên ngoài.
* **Đánh giá từ bên trong**: Đánh giá từ bên trong bao gồm việc tìm ra lỗ hổng bảo mật bằng cách quét hệ thống mạng nội bộ và cơ sở hạ tầng mạng.



* 1. **Chu trình đánh giá lỗ hổng bảo mật** bao gồm các công đoạn sau đây:

### Tạo đường cơ sở

**Tạo đường cơ sở** là một công đoạn phải thực hiện trước trong chu trình đánh giá lỗ hổng bảo mật. Ở công đoạn này, **pentester**hay **quản trị viên hệ thống** phải nhận diện bản chất của hệ thống, ứng dụng và dịch vụ. Người đang thực hiện đánh giá sẽ tạo một bản kiểm nghiệm tất cả các tài nguyên và tài sản để dễ dàng quản lí và dành ưu tiên đánh giá. Bên cạnh đó, anh ta cũng lập bản vẽ cơ sở hạ tầng mạng, tìm hiểu kiểm soát an ninh, chính sách cũng như tiêu chuẩn mà tổ chức phải tuân thủ. Tóm lại, đường cơ sở giúp lên kế hoạch đánh giá một cách hiệu quả, lập thời gian biểu cho các công đoạn cũng như quản lí chúng theo thứ tự ưu tiên.

### Đánh giá lỗ hổng bảo mật

**Đánh giá lỗ hổng bảo mật** tập trung vào đánh giá mục tiêu. Quá trình đánh giá bao gồm**thăm dò** và **điều tra** các biện pháp an toàn như physical security hay các chính sách an ninh. Công đoạn này đánh giá mục tiêu về các phần sai sót cấu hình, cấu hình mặc định, lỗi hay các lỗ hổng bằng cách thăm dò từng thành phần riêng biệt hoặc sử dụng các công cụ đánh giá. Khi quét xong, các dữ liệu tìm thấy được xếp hạng dựa trên mức độ ưu tiên. Cuối công đoạn, báo cáo đánh giá lỗ hổng bảo mật sẽ cho thấy tất cả các lỗ hổng được phát hiện, phạm vi cũng như mức độ ưu tiên của chúng.



**Đánh giá rủi ro**bao gồm việc kiểm tra các lỗ hổng bảo mật và đánh giá ảnh hưởng của chúng lên hệ thống mạng hay tổ chức.

Công đoạn này bao gồm việc**giảm thiểu rủi ro** của những lỗ hổng bảo mật đã tìm thấy. Những lỗ hổng có mức độ ưu tiên được tiếp cận đầu tiên vì chúng có thể gây ra những ảnh hưởng nghiêm trọng.

Công đoạn **xác thực**để bảo đảm rằng tất cả các lỗ hổng bảo mật đã được loại bỏ.

**Quan sát network traffic**và **system behaviors**để phát hiện kịp thời nếu có xâm nhập.

* 1. Thực hiện đánh giá lỗ hổng bảo mật

Sau đây là một số bước cần thực hiện để việc đánh giá lỗ hổng bảo mật đạt hiệu quả. Quản trị viên hệ thống hay kiểm nghiệm viên cần áp dụng những bước sau:

Trước khi sử dụng bất cứ công cụ nào để đánh giá lỗ hổng bảo mật, kiểm nghiệm viên phải hiểu rõ mọi chức năng của công cụ, từ đó tìm được công cụ phù hợp nhất để thu thập thông tin cần thiết.

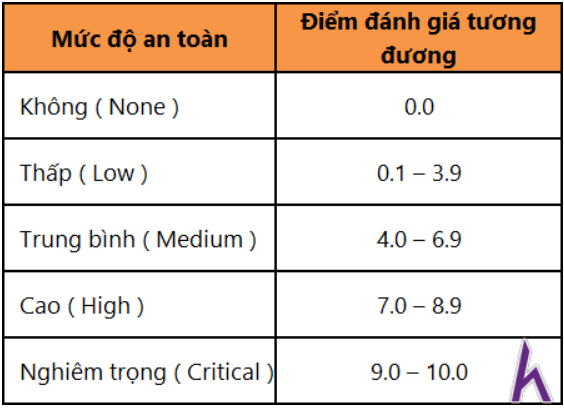
Đảm bảo công cụ sử dụng không gây tổn hại hoặc vô hiệu hóa những dịch vụ đang chạy của hệ thống mạng.

Xác định rõ source location của máy quét để thu hẹp phạm vi focus.

Quét thường xuyên để xác định lỗ hổng.

* 1. Hệ thống đánh giá lỗ hổng

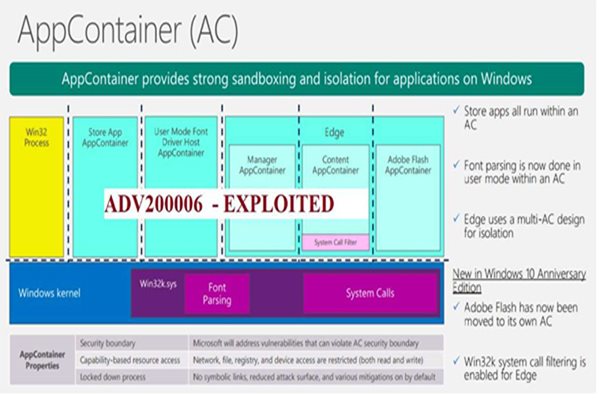
**Hệ thống đánh giá lỗ hổng** chung (CVSS) là một cách để nhận biết những tính chất cơ bản của lỗ hổng và đưa ra con số cụ thể cho mức độ nghiêm trọng của nó. Những con số này được sắp xếp vào các nhóm với một số đại diện định tính ( ví dụ như low, medium, high và critical ). Điều này giúp tổ chức đánh giá và dành thứ tự ưu tiên xử lí lỗ hổng một cách đúng đắn nhất.



## ****5. Lỗ hổng của Window, Linux(Ví dụ)****

### 5.1. Các lỗ hổng bảo mật trên Window.

Lỗ hổng bảo mật thư viện ATMFD.DLL là lỗ hổng nguy hiểm, ảnh hưởng đến nhiều phiên bản Windows khác nhau.



Theo Trung tâm thông tin - Bộ TT&TT, Microsoft ngày 23/3 vừa qua đã xác nhận thông tin tồn tại lỗ hổng bảo mật cho phép khai thác máy tính sử dụng hệ điều hành Windows để thực thi các lệnh điều khiển từ xa trái phép không cần xác thực, lỗ hổng được tấn công thông qua hai lỗi của các chức năng xử lý Font chữ Adobe Type 1 do thư viện ATMFD.DLL của hệ điều hành Windows cung cấp.

Người dùng sẽ bị ảnh hưởng khi mở hoặc sử dụng phần mềm Windows Explorer để xem nội dung tệp tin văn bản có mã tấn công khai thác do tin tặc tạo ra.

Nhấn mạnh đây là lỗ hổng khá nghiêm trọng, ảnh hưởng nhiều phiên bản Windows khác nhau, đại diện Trung tâm thông tin của Bộ TT&TT cũng cho biết, đến ngày 27/3 Microsoft vẫn chưa có bản vá chính thức.

Các phiên bản hệ điều hành Windows bị ảnh hưởng mức nghiêm trọng bao gồm: phiên bản Windows cho máy trạm 7, Windows 8; Phiên bản Windows cho máy chủ Windows Server 2008, Windows Server 2012. Một số phiên bản mới hơn vẫn bị ảnh hưởng nhưng mức nguy hiểm thấp hơn bao gồm: Windows 10 dành cho máy trạm và Windows Server 2016, Windows Server 2019 dành cho máy chủ.

Việc không khắc phục kịp thời có thể dẫn đến tình trạng mất an toàn thông tin trên diện rộng, gây ảnh hưởng lớn đến dữ liệu, hoạt động của cơ quan, tổ chức.

### **5.2. Lỗ hổng bảo mật của Linux**

**Một lỗ hổng nghiêm trọng mới được phát hiện trong Linux kernel cho phép tin tặc chiếm quyền truy cập gốc thông qua ứng dụng Android hoặc Linux độc hại.** Lỗ hổng nghiêm trọng Linux kernel ([CVE-2016-0728](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2016-0728)) được phát hiện bởi một nhóm các nhà nghiên cứu Perception Point. Lỗ hổng nằm trong đoạn code từ năm 2012 và ảnh hưởng đến tất cả các hệ điều hành với Linux kernel 3.8 hoặc cao hơn. Hàng triệu máy tính (cả 32bit và 64bit) có nguy cơ bị ảnh hưởng. Tuy nhiên, vấn đề phiền toái nhất là lỗ hổng ảnh hưởng đến phiên bản Android KitKat và cao hơn – đồng nghĩa với việc hơn 66% thiết bị Android dễ bị tổn thương. Tin tặc chỉ có thể truy cập cục bộ để khai thác lỗ hổng trên Linux server. Nếu khai thác thành công cho phép tin tặc có quyền truy cập gốc như xóa file, xem thông tin riêng tư và cài đặt ứng dụng độc hại.Quét lỗ hổng

Thông thường lỗ hổng trong Linux kernel thường được vá ngay sau khi phát hiện ra nên hệ điều hành này được xem là an toàn hơn so với hệ điều hành khác. Tuy nhiên lỗ hổng zero-day mới phát hiện đã tồn tại gần 3 năm. Các nhà nghiên cứu hiện chưa phát hiện ra khai thác trong thực tế. Perception Point đã cung cấp phân tích kĩ thuật về lỗ hổng và cách khai thác, bao gồm cả bản code chứng minh đăng tải trên [Github](https://gist.github.com/PerceptionPointTeam/18b1e86d1c0f8531ff8f). Đội ngũ Linux đã được báo cáo về lỗ hổng và bản vá có thể sẽ được cập nhật tự động trên các thiết bị trong vòng vài ngày. Nhưng các thiết bị Android sẽ phải chờ lâu hơn để nhận được cập nhật từ nhà sản xuất hoặc nhà mạng. Để vá lỗ hổng Linux Kernel (CVE-2016-0728) bạn sử dụng lệnh:

Debian hoặc Ubuntu Linux: sudo apt-get update && sudo apt-get upgrade

RHEL / CentOS Linux: sudo yum update

## Rò quét lỗ hổng bảo mật

Trong thời đại công nghệ phát triển như hiện nay, việc tìm kiếm các lỗ hổng bảo mật trong một môi trường hệ thống nhất định đã trở nên dễ dàng hơn nhờ các công cụ khác nhau. Các công cụ từ tự động đến thủ công đều sẵn có để giúp đỡ việc tìm kiếm.

Máy quét lỗ hổng là công cụ tự động được thiết kế chuyên dung cho tìm kiếm lỗ hổng, điểm yếu, vấn đề cần giải quyết trong một hệ điều hành, mạng, phần mềm hay ứng dụng. Những công cụ quét này có thể thăm dò kĩ lưỡng scripts, open ports, banners, running services, configuration errors ( lỗi cấu hình ) và các khu vực khác.

Những công cụ quét lỗ hổng này bao gồm:

* Nessus
* OpenVAS
* Nexpose
* Retina
* GFI LanGuard
* Qualys FreeScan, và nhiều công cụ khác.

Không chỉ chuyên gia bảo mật mà cả những kẻ có ý định tấn công hệ thống mạng cũng sử dụng những công cụ trên để tìm ra rủi ro và lỗ hổng.