

TRƯỜNG ĐẠI HỌC NGOẠI NGỮ - TIN HỌC THÀNH PHỐ HỒ CHÍ MINH

KHOA CÔNG NGHỆ THÔNG TIN



**BÀI BÁO CÁO KẾT THÚC HỌC PHẦN
AN NINH MẠNG**

TÌM HIỂU VỀ SYSTEM HACKING

Giảng viên hướng dẫn: Ths. Phạm Đình Thắng

Sinh viên thực hiện:

- | | |
|---------------------|------------|
| 1. Nguyễn Hữu Tín | 22DH113757 |
| 2. Võ Văn Thần Thái | 22DH114737 |
| 3. Phạm Quốc Huy | 22DH111305 |

Thành phố Hồ Chí Minh, tháng 07/2024

MỤC LỤC

1. System hacking là gì?.....	3
2. Hệ phương pháp của system hacking:.....	3
3. Mục tiêu của System hacking:	3
I. CHI TIẾT CÁC PHƯƠNG PHÁP.....	3
1. Bẻ khóa mật khẩu:.....	3
a) Tấn công phi kỹ thuật:	4
b) Tấn công online chủ động:.....	4
c) Tấn công online thụ động:	5
d) Mật khẩu mặc định:	6
e) Tấn công offline:.....	6
f) Đoán mật khẩu:	7
g) USB Drive:.....	7
2. Tăng đặc quyền:	7
a) Khai thác lỗ hổng phần mềm:	7
b) Lợi dụng cấu hình sai lầm:.....	8
c) Sử dụng các công cụ tăng đặc quyền:	8
d) Tấn công lừa đảo (Social Engineering):	8
e) Khai thác các tính năng hợp pháp:.....	8
f) Sử dụng mật khẩu yếu và mặc định:.....	8
g) Lạm dụng dịch vụ và tiến trình:.....	8
h) Khai thác các dịch vụ mạng:.....	8
3. Chạy ứng dụng:	8
a) Quy trình AEM thường bao gồm các bước sau:	9
b) Một số kỹ thuật phổ biến được sử dụng trong AEM:	9
4. Giấu tệp:	9
a) Kỹ thuật dựa trên ứng dụng:	10
b) Kỹ thuật dựa trên ứng dụng:	10
5. Che dấu vết:.....	10
a) Kỹ thuật trước khi xâm nhập:	10
b) Kỹ thuật sau khi xâm nhập:	11
II. PHÂN LOẠI.....	11
1. White Hat Hacker (Hacker Mũ Trắng):	11

2. Black Hat Hacker (Hacker Mũ Đen).....	11
III. TRIỂN KHAI HỆ THỐNG	11
1. Hướng dẫn lấy mật khẩu của máy Windows 7	11
2. Sử dụng tool hashcat trên kali để dò mật khẩu win 7	17
IV. ĐÁNH GIÁ	23
1. Chúng tôi làm được những gì?	23
2. Chưa làm được những gì?	23
3. Điểm hạn chế:.....	23
4. Hướng phát triển trong tương lai:.....	23
V. KẾT LUẬN.....	23
VI. TÀI LIỆU THAM KHẢO	24

DANH MỤC HÌNH ẢNH

Hình 1. Mở cmd dưới quyền administrative	12
Hình 2. Màn hình hiển thị toàn bộ user và mật khẩu được mã hóa	12
Hình 3. Tên user và mã hash của mật khẩu	13
Hình 4. Copy toàn bộ vào file Hash.txt.....	13
Hình 5. File Hash.txt trong thư mục pwdump7	14
Hình 6. Chuyển file Hash.txt vào máy ảo Windows 10.....	14
Hình 7. Khởi động Ophcrack trên máy ảo Windows 10.....	15
Hình 8. Nhấn vào nút Load, chọn PWDUMP File	15
Hình 9. Chọn file Hash.txt	16
Hình 10. Cài đặt Vista free.....	16
Hình 11. Mật khẩu của các user	17
Hình 12. Tạo thư mục Share trên win 10.....	17
Hình 13. Cấp quyền everyone.....	18
Hình 14. Win 7 truy xuất share win 10	18
Hình 15. Lưu 2 file sam và system của win 7 cho máy win 10	18
Hình 16. Lấy file sam và system từ máy win 10 qua kali.....	19
Hình 17. Lệnh.....	20
Hình 18. Sam.txt.....	20
Hình 19. Copy đoạn mật khẩu chưa mã hóa	21
Hình 20. Pass.hash	21
Hình 21. Kết Quả	22

GIỚI THIỆU

1. System hacking là gì?

- Hacking hệ thống là hành động xâm nhập trái phép vào hệ thống máy tính, mạng máy tính hoặc thiết bị điện tử với mục đích không chính đáng. Kẻ tấn công (hacker) có thể sử dụng các kỹ thuật và công cụ khác nhau để đột nhập vào hệ thống.

2. Hệ phương pháp của system hacking:

- Chu trình hacking được phân loại thành một số phương pháp hacking chính. Những phương pháp này được EC Council đặt tên là Hệ phương pháp hacking CEH. Hệ phương pháp này gồm:

- Bẻ khóa mật khẩu.
- Tăng đặc quyền.
- Chạy ứng dụng.
- Giấu tệp.
- Che dấu vết.

3. Mục tiêu của System hacking:

- Theo hệ phương pháp của system hacking, việc tránh kiểm soát truy cập cũng như chính sách bảo mật bằng cách bẻ khóa mật khẩu hay tấn công phi kỹ thuật sẽ giúp chúng ta truy cập vào hệ thống thành công.

- Những thông tin về hệ điều hành cho phép lợi dụng những lỗ hổng bảo mật để tăng đặc quyền. Khi đã truy cập được vào hệ thống và nhận đặc quyền, người tấn công có thể duy trì truy cập từ xa với mục tiêu bằng cách cho chạy các ứng dụng như Trojans, backdoors và spyware.

- Bây giờ, để đánh cắp thông tin, dữ liệu hay tài sản của tổ chức đó, người tấn công phải che giấu những hành động ác ý của họ. Rootkits và steganography là những phần mềm quen thuộc nhất phục vụ công đoạn che giấu này. Một khi hacker đã đánh cắp tài liệu và che giấu thành công, công đoạn cuối cùng để đảm bảo không bị phát hiện là chỉnh sửa hoặc xóa nhật ký truy cập (logs).

I. CHI TIẾT CÁC PHƯƠNG PHÁP

1. Bẻ khóa mật khẩu

- Trước khi đến công đoạn bẻ khóa mật khẩu, bạn phải biết về ba nhân tố xác thực:

- Thứ tôi có, ví dụ như username và mật khẩu.
- Thứ tôi là, ví dụ như sinh trắc học.
- Thứ tôi sở hữu, ví dụ như thiết bị đã được đăng ký/ được cấp phép.

- Bẻ khóa mật khẩu là quá trình rút mật khẩu để nhận quyền truy cập vào mục tiêu như user chính thống. Thông thường, chỉ có quyền xác minh mật khẩu hay tên tài khoản được thiết lập. Tuy nhiên hiện nay, quyền xác minh mật khẩu

được tạo thành từ nhiều nhân tố, bao gồm những thứ bạn có như tên tài khoản, mật khẩu và sinh trắc học.

- Do đó, có thể sử dụng tấn công phi kỹ thuật hoặc quấy nhiễu đường truyền tin để bẻ khóa mật khẩu. Mật khẩu ngắn, dễ đoán, độ mã hóa thấp hay chỉ gồm số và chữ là những loại mật khẩu có thể bẻ khóa dễ dàng. Một mật khẩu dài và khó đoán sẽ là biện pháp phòng thủ đầu tiên trước những tấn công như thế này. Một mật khẩu mạnh tiêu biểu sẽ chứa:

- Các kiểu chữ khác nhau (chữ hoa, chữ thường).
- Ký tự đặc biệt.
- Số.
- Độ dài thường nhiều hơn 8 ký tự.

- Các kiểu tấn công mật khẩu:

- Tấn công phi kỹ thuật.
- Tấn công online chủ động.
- Tấn công online thụ động.
- Mật khẩu mặc định.
- Tấn công offline.
- Đoán mật khẩu.
- USB drive.

a) Tấn công phi kỹ thuật:

- Tấn công phi kỹ thuật là loại tấn công không đòi hỏi bất kỳ kiến thức chuyên môn nào. Loại tấn công này được thực hiện bằng **shoulder surfing**, **social engineering** và **dumpster diving**.

- Ví dụ: lấy cắp tên user và mật khẩu bằng cách đứng sau lưng mục tiêu khi người ấy đang đăng nhập (shoulder surfing), hoặc tiếp xúc với các thông tin nhạy cảm, ... Số tài khoản, mật khẩu hay các thông tin bí mật khác có thể bị đánh cắp thông qua shoulder surfing do sự bất cẩn của mục tiêu.

b) Tấn công online chủ động:

Tấn công online chủ động bao gồm nhiều kỹ thuật tiếp cận trực tiếp với mục tiêu để bẻ khóa mật khẩu:

- Dictionary attack: Trong loại tấn công này, một ứng dụng bẻ khóa mật khẩu được chạy song song với một tệp từ điển. Tệp từ điển này chứa toàn bộ các từ thông thường để trích rút mật khẩu. Đây là loại tấn công mật khẩu đơn giản nhất. Nếu hệ thống sử dụng mật khẩu mạnh, độc đáo, gồm ký tự chữ - số thì thường không bị ảnh hưởng bởi dictionary attack.

- Brute force attack: Tấn công này sẽ lấy mật khẩu bằng cách thử tất cả các kết hợp ký tự đến khi một mật khẩu được chấp nhận. Đây là cách tấn công mật khẩu thông thường và cơ bản.

- Hash injection: Kiểu tấn công này đòi hỏi kiến thức về hashing (hàm băm) và cryptography (mật mã học). Trong tấn công này:

- Kẻ tấn công cần trích rút nhật ký của user trong hashes và stores trong tệp Security Account Manager (SAM).

- Bằng cách lợi dụng những lỗ hổng, kẻ tấn công sẽ xâm nhập vào máy chủ hay workstation, từ đó nhận quyền truy cập vào hệ thống máy.

- Một khi truy cập vào hệ thống máy thành công, kẻ tấn công sẽ trích rút log-on hashes của những user và admin quan trọng.

- Nhờ những hashes đã được trích rút này, kẻ tấn công sẽ đăng nhập vào máy chủ như người kiểm soát để khai thác thêm nhiều tài khoản.

c) Tấn công online thụ động:

Kiểu tấn công này không can thiệp vào mục tiêu. Điểm mấu chốt của tấn công là việc trích rút mật khẩu mà không làm lộ thông tin. Kiểu tấn công online thụ động thường thấy nhất là:

- Wire sniffing: Đây là quá trình nghe trộm gói tin bằng các công cụ nghe trộm trong mạng nội bộ (LAN). Việc thăm dò gói tin mục tiêu có thể giúp lấy được những thông tin nhạy cảm và mật khẩu, ví dụ như Telnet, FTP, SMTP, rlogin credentials. Hiện nay có nhiều công cụ nghe trộm phục vụ thu thập gói tin truyền qua mạng LAN bất kể loại thông tin. Bên cạnh đó, một số công cụ cho phép người sử dụng lọc dữ liệu để thu thập một số gói tin nhất định.

- Man-in-the-middle attack: Đây là kiểu tấn công mà người tấn công tham gia vào cuộc giao tiếp của các nodes khác. MITM có thể được hiểu là một user truyền tin với một user hoặc serve khác, và người tấn công sẽ tham gia vào đoạn hội thoại bằng cách nghe trộm gói tin và tạo ra tấn công MITM hay Replay traffic. Dưới đây là các tài nguyên sẵn có để tổ chức tấn công MITM:

- SSL Strip
- Burp Suite
- Browser Exploitation Framework (BeEF)

- Replay attack: Trong tấn công này, kẻ tấn công lấy gói tin bằng các công cụ nghe trộm gói tin. Khi nhận được gói tin, kẻ tấn công sẽ trích rút được thông tin quan trọng như mật khẩu. Từ đó, kẻ tấn công sẽ có quyền truy cập hệ thống nếu họ tạo ra replay traffic với các thông tin đã trích rút.

d) Mật khẩu mặc định:

- Mỗi thiết bị mới đều được nhà sản xuất thiết lập một mật khẩu mặc định. Người dùng nên đổi mật khẩu này thành một mật khẩu bí mật và độc nhất khác. Kẻ tấn công sử dụng mật khẩu mặc định này bằng cách tìm kiếm thông qua trang web của nhà sản xuất hoặc công cụ tìm mật khẩu mặc định online.

- Một số công cụ sẵn có để tìm mật khẩu mặc định:

- <https://cirt.net/>
- <https://default-password.info/>
- <https://passwordsdatabase.com/>

e) Tấn công offline:

Pre-Computed hashes and Rainbow Table (hàm băm tính toán trước và bảng cầu vòng)

- Một ví dụ của tấn công offline là dùng bảng cầu vòng để so sánh mật khẩu. Một bảng cầu vòng là danh sách chứa các giá trị hash đã được tính toán cho mọi kết hợp ký tự. Bạn có thể lấy giá trị hash được trích rút từ máy tính mục tiêu và so sánh nó với giá trị trong bảng cầu vòng. Ưu điểm của bảng cầu vòng là tiết kiệm thời gian lấy mật khẩu, bởi vì tất cả các giá trị hash đã được tính toán trước. Tuy nhiên nhược điểm là tốn nhiều thời gian để tạo ra bảng cầu vòng ban đầu.

- Để tạo bảng cầu vòng, bạn có thể sử dụng các tài nguyên sau: winrtgen, GUI-based generator, và rtgen, một công cụ dòng lệnh. Dưới đây là các format hashing được hỗ trợ:

- MD2
- MD4
- MD5
- SHA1
- SHA-256
- SHA-384
- SHA-512 và các format hashing khác

Network Attack (DNA)

- DNA là một kiểu tấn công nâng cao để bẻ khóa mật khẩu. DNA lấy mật khẩu bằng cách trích rút các hashes nhờ công cụ xử lý của các máy móc trong hệ thống mạng. Trong tấn công Distributed Network cần có một Manager và Client. DNA Manager được đặt ở trung tâm mạng, xung quanh là các Clients. DNA Manager sẽ phân phối các nhiệm vụ nhỏ cho toàn hệ thống mạng. Từ đó mạng sẽ tính toán ở nền, sử dụng những tài nguyên chưa khai thác để bẻ khóa mật khẩu.

f) Đoán mật khẩu:

- Đây chỉ là quy trình đoán mật khẩu lặp đi lặp lại. Kẻ tấn công sử dụng những thông tin trích rút từ những công đoạn trước để làm cơ sở đoán mật khẩu thủ công. Kiểu tấn công này không phổ biến và tỉ lệ thất bại cao do yêu cầu của chính sách mật khẩu. Thông thường, các thông tin thu được từ tấn công phi kỹ thuật có thể có ích cho kiểu tấn công này.

g) USB Drive:

- Kẻ tấn công có thể sử dụng USB Drive trong tấn công online chủ động bằng cách cắm USB chứa công cụ hacking như “Passview”. Sau khi cắm, đặc tính Window Autorun sẽ chạy ứng dụng tự động nếu đặc tính này được kích hoạt. Một khi ứng dụng được phép thực thi, ứng dụng sẽ trích rút mật khẩu từ mục tiêu.

Công cụ bẻ khóa mật khẩu:

- Pwdump7.
- Fgdump.
- L0phtCrack.
- Ophcrack.
- RainbowCrack.
- Cain and Abel.
- John the Ripper và nhiều công cụ khác.
- FlexiSpy dành cho điện thoại.

2. Tăng đặc quyền:

- Tăng đặc quyền (Privilege Escalation) là một kỹ thuật quan trọng trong System Hacking, cho phép hacker nâng cao quyền truy cập của họ trong hệ thống mục tiêu. Mục tiêu của việc tăng đặc quyền là để đạt được quyền truy cập root hoặc quyền quản trị viên, từ đó hacker có thể thực hiện bất kỳ hành động nào trong hệ thống.

- Có rất nhiều phương pháp khác nhau để tăng đặc quyền, và phương pháp phù hợp sẽ phụ thuộc vào hệ điều hành, cấu hình hệ thống và lỗ hổng bảo mật cụ thể được khai thác. Dưới đây là một số phương pháp phổ biến:

a) Khai thác lỗ hổng phần mềm:

- Lỗ hổng phần mềm có thể cho phép hacker thực thi mã độc với quyền hạn cao hơn bình thường.

- Ví dụ: hacker có thể khai thác lỗ hổng trong ứng dụng web để thực thi mã độc trên máy chủ web và sau đó sử dụng mã độc này để tăng đặc quyền trên hệ điều hành.

b) Lợi dụng cấu hình sai lầm:

- Cấu hình sai lầm trong hệ thống có thể cho phép hacker truy cập vào tài khoản có quyền hạn cao hơn.

- Ví dụ: hacker có thể tìm thấy tài khoản người dùng có mật khẩu mặc định hoặc tài khoản có quyền truy cập quản trị viên không được sử dụng.

c) Sử dụng các công cụ tăng đặc quyền:

- Có rất nhiều công cụ tăng đặc quyền có sẵn trên mạng, có thể được sử dụng để tự động tìm kiếm và khai thác lỗ hổng trong hệ thống.

- Một số công cụ phổ biến bao gồm Metasploit, Nmap và Mimikatz.

d) Tấn công lừa đảo (Social Engineering):

- Hacker có thể lừa người dùng tiết lộ thông tin đăng nhập hoặc thực hiện hành động cho phép họ tăng đặc quyền.

- Ví dụ: hacker có thể gửi email giả mạo cho người dùng yêu cầu họ nhập mật khẩu hoặc nhấp vào liên kết độc hại.

e) Khai thác các tính năng hợp pháp:

- Một số tính năng hợp pháp trong hệ thống có thể được sử dụng để tăng đặc quyền.

- Ví dụ: hacker có thể sử dụng lệnh “sudo” để thực thi các lệnh với quyền hạn root.

f) Sử dụng mật khẩu yếu và mặc định:

- Hacker có thể tìm thấy hoặc đoán được mật khẩu yếu hoặc mật khẩu mặc định và sử dụng chúng để đăng nhập với quyền admin.

g) Lạm dụng dịch vụ và tiến trình:

- Một số dịch vụ hoặc tiến trình hệ thống chạy với quyền cao có thể bị lạm dụng để thực thi lệnh với quyền admin.

- Ví dụ: sử dụng các dịch vụ có quyền ghi vào tập tin thực thi hoặc dịch vụ có thể bị chen mã độc.

h) Khai thác các dịch vụ mạng:

- Các dịch vụ mạng, chẳng hạn như SMB hoặc RDP, có thể chứa các lỗ hổng hoặc cấu hình sai cho phép tăng đặc quyền.

Để bảo vệ hệ thống khỏi các phương pháp tấn công này, quản trị viên cần liên tục cập nhật phần mềm và hệ điều hành, kiểm tra cấu hình bảo mật, sử dụng mật khẩu mạnh và kiểm tra định kỳ các lỗ hổng bảo mật trong hệ thống.

3. Chạy ứng dụng:

- Hệ phương pháp chạy ứng dụng (Application Execution Methodology - AEM) là một phần quan trọng trong quá trình System Hacking, tập trung vào việc thực thi các chương trình độc hại trên hệ thống mục tiêu sau khi đã xâm nhập.

thành công. Mục đích của AEM là duy trì truy cập trái phép, thu thập thông tin nhạy cảm, hoặc gây ra thiệt hại cho hệ thống.

a) Quy trình AEM thường bao gồm các bước sau:

- Lựa chọn ứng dụng: Kẻ tấn công sẽ lựa chọn ứng dụng phù hợp với mục tiêu tấn công và hệ điều hành mục tiêu. Ứng dụng có thể là mã độc hại được viết riêng, hoặc các công cụ hacking sẵn có.

- Truyền tải ứng dụng: Ứng dụng độc hại cần được truyền tải lên hệ thống mục tiêu bằng các phương pháp như tải xuống tệp tin, khai thác lỗ hổng, hoặc sử dụng các kỹ thuật tấn công phi kỹ thuật (social engineering).

- Thực thi ứng dụng: Kẻ tấn công sẽ sử dụng các kỹ thuật khác nhau để thực thi ứng dụng độc hại, ví dụ như sử dụng các lỗ hổng trong hệ điều hành, leo thang đặc quyền, hoặc che giấu ứng dụng dưới dạng tệp tin hợp pháp.

- Ẩn dấu ứng dụng: Sau khi thực thi, kẻ tấn công sẽ sử dụng các kỹ thuật để che giấu sự hiện diện của ứng dụng độc hại. Ví dụ: xóa dấu vết trong nhật ký hệ thống, hoặc sử dụng rootkit.

- Duy trì truy cập: Kẻ tấn công có thể sử dụng ứng dụng độc hại để thiết lập backdoor, cho phép truy cập từ xa vào hệ thống mục tiêu trong tương lai.

b) Một số kỹ thuật phổ biến được sử dụng trong AEM:

- Kỹ thuật Shellcode: Shellcode là một đoạn mã ngắn được thực thi trực tiếp trong bộ nhớ, cho phép kẻ tấn công thực hiện các hành động tùy ý trên hệ thống mục tiêu.

- Kỹ thuật DDL Hijacking: Kỹ thuật này liên quan đến việc thay thế một DLL hợp pháp bằng một DLL độc hại sẽ được thực thi khi tải ứng dụng.

- Kỹ thuật Hooking: Kỹ thuật này liên quan đến việc sửa đổi bảng địa chỉ của quy trình để chuyển hướng các lệnh gọi hàm sang mã độc.

- Kỹ thuật Metasploit: Metasploit là một bộ khung phần mềm mã nguồn mở cung cấp nhiều công cụ và khai thác để thực hiện các cuộc tấn công mạng, bao gồm cả việc chạy ứng dụng độc hại.

4. Giấu tệp:

- Hệ phương pháp giấu tệp (File Hiding Methodology - FHM) là một kỹ thuật quan trọng trong System Hacking, tập trung vào việc che giấu sự tồn tại của tệp tin hoặc thư mục trên hệ thống mục tiêu. Mục đích của FHM là để bảo vệ thông tin nhạy cảm, tránh sự phát hiện của phần mềm chống virus hoặc quản trị viên hệ thống, hoặc duy trì truy cập trái phép vào hệ thống.

- Có nhiều phương pháp khác nhau để giấu tệp tin, có thể được phân loại thành hai nhóm chính:

a) Kỹ thuật dựa trên ứng dụng:

- Thay đổi thuộc tính tệp: Kẻ tấn công có thể thay đổi thuộc tính tệp tin để ẩn tệp khỏi các công cụ tìm kiếm thông thường. Ví dụ: thuộc tính "hidden" có thể được đặt để ẩn tệp khỏi Windows Explorer.

- Sử dụng NTFS Alternate Data Streams (ADS): ADS là một tính năng của hệ thống tệp NTFS cho phép lưu trữ dữ liệu bổ sung bên cạnh tệp tin chính. Kẻ tấn công có thể sử dụng ADS để lưu trữ tệp tin ẩn mà không bị phát hiện bởi các công cụ tìm kiếm thông thường.

- Sử dụng thư mục ẩn: Một số hệ điều hành có các thư mục ẩn được thiết kế để lưu trữ tệp hệ thống. Kẻ tấn công có thể sử dụng các thư mục này để lưu trữ tệp tin ẩn.

- Mã hóa tệp: Kẻ tấn công có thể mã hóa tệp tin bằng thuật toán mật mã để khiến tệp không thể đọc được.

b) Kỹ thuật dựa trên ứng dụng:

- Sử dụng phần mềm giấu tệp: Có nhiều phần mềm miễn phí và trả phí có thể được sử dụng để giấu tệp tin trên hệ thống. Phần mềm này thường sử dụng các kỹ thuật khác nhau như thay đổi thuộc tính tệp, mã hóa tệp hoặc tạo các thư mục ẩn.

- Sử dụng steganography: Steganography là kỹ thuật ẩn dữ liệu bí mật trong các tệp tin bình thường, chẳng hạn như hình ảnh hoặc tệp âm thanh. Kẻ tấn công có thể sử dụng steganography để ẩn tệp tin trong các tệp tin khác mà không bị phát hiện.

- Tạo các phân vùng ẩn: Kẻ tấn công có thể tạo các phân vùng ẩn trên ổ cứng để lưu trữ tệp tin. Các phân vùng này không được hiển thị trong hệ điều hành thông thường và chỉ có thể được truy cập bằng các công cụ đặc biệt.

5. Che dấu vết:

- Hệ phương pháp che dấu vết (Covering Tracks Methodology - CTM) là một phần quan trọng trong quá trình System Hacking, tập trung vào việc xóa bỏ các bằng chứng về hoạt động xâm nhập và duy trì tính ẩn danh của kẻ tấn công. Mục đích của CTM là để ngăn chặn việc phát hiện xâm nhập, bảo vệ danh tính của kẻ tấn công và tránh bị truy tố.

- Có nhiều kỹ thuật khác nhau để che dấu vết, có thể được phân loại thành hai nhóm chính:

a) Kỹ thuật trước khi xâm nhập:

- Sử dụng hệ thống ẩn danh: Kẻ tấn công có thể sử dụng các hệ thống ẩn danh như Tor hoặc I2P để che giấu địa chỉ IP thực của họ.

- Sử dụng phần mềm độc hại không dấu vết: Một số phần mềm độc hại được thiết kế để tự động xóa dấu vết sau khi thực thi.

- Sử dụng các công cụ dọn dẹp: Kẻ tấn công có thể sử dụng các công cụ dọn dẹp để xóa nhật ký hệ thống, tệp tin tạm thời và các bằng chứng khác về hoạt động của họ.

b) Kỹ thuật sau khi xâm nhập:

- Xóa nhật ký hệ thống: Kẻ tấn công có thể xóa nhật ký hệ thống để che giấu dấu vết về hoạt động của họ.

- Xóa tệp tin tạm thời: Kẻ tấn công có thể xóa tệp tin tạm thời có thể chứa thông tin nhạy cảm.

- Sửa đổi nhật ký hệ thống: Kẻ tấn công có thể sửa đổi nhật ký hệ thống để che giấu dấu vết về hoạt động của họ.

- Sử dụng rootkit: Rootkit là một loại phần mềm độc hại được cài đặt vào hệ điều hành để che giấu sự hiện diện của kẻ tấn công và các tệp tin độc hại.

- Gỡ cài đặt phần mềm độc hại: Kẻ tấn công có thể gỡ cài đặt phần mềm độc hại sau khi sử dụng để xóa dấu vết.

PHÂN LOẠI

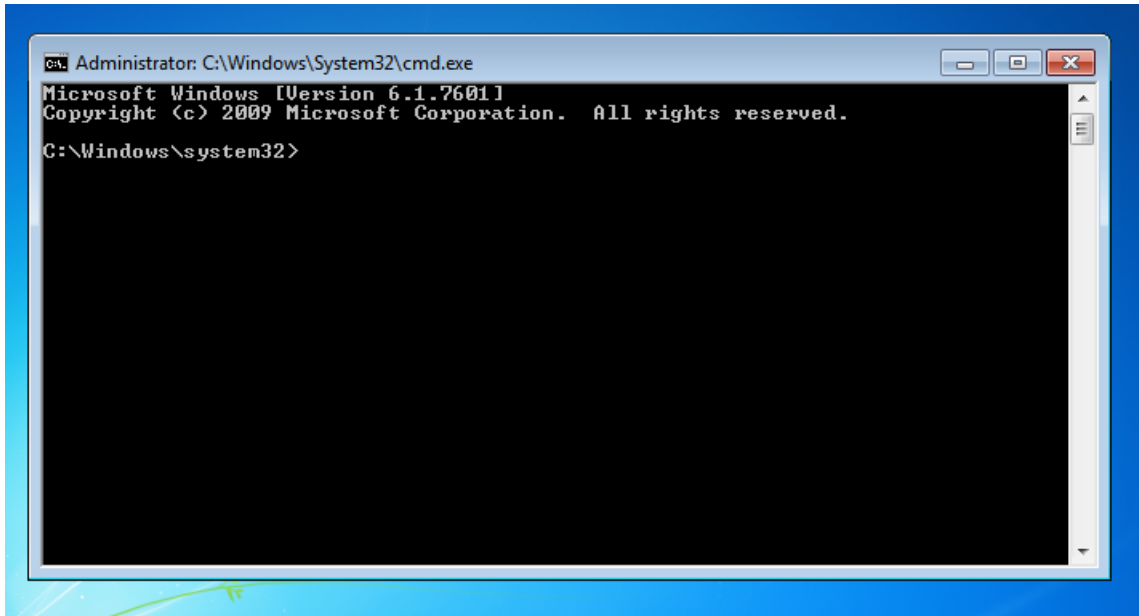
- White Hat Hacker (Hacker Mũ Trắng):
 - + Sử dụng kỹ năng hacking của họ để tìm kiếm và vá các lỗ hổng bảo mật cho hệ thống, giúp bảo vệ dữ liệu và hệ thống.
 - + Làm việc với các tổ chức để cải thiện an toàn và phòng thủ chống lại các mối đe dọa.
 - Đạo đức và hợp pháp, với mục tiêu làm cho thế giới kỹ thuật số an toàn hơn.
- Black Hat Hacker (Hacker Mũ Đen)
 - + Sử dụng kỹ năng hacking của họ để xâm nhập hệ thống, đánh cắp dữ liệu, phá hoại hệ thống hoặc chiếm quyền kiểm soát.
 - + Động cơ bởi lợi ích cá nhân, ác ý hoặc các lý do khác.
 - + Bất hợp pháp và vô đạo đức, với mục tiêu gây hại hoặc khai thác hệ thống cho lợi ích cá nhân.

II. TRIỂN KHAI HỆ THỐNG

1. Hướng dẫn lấy mật khẩu của máy Windows 7

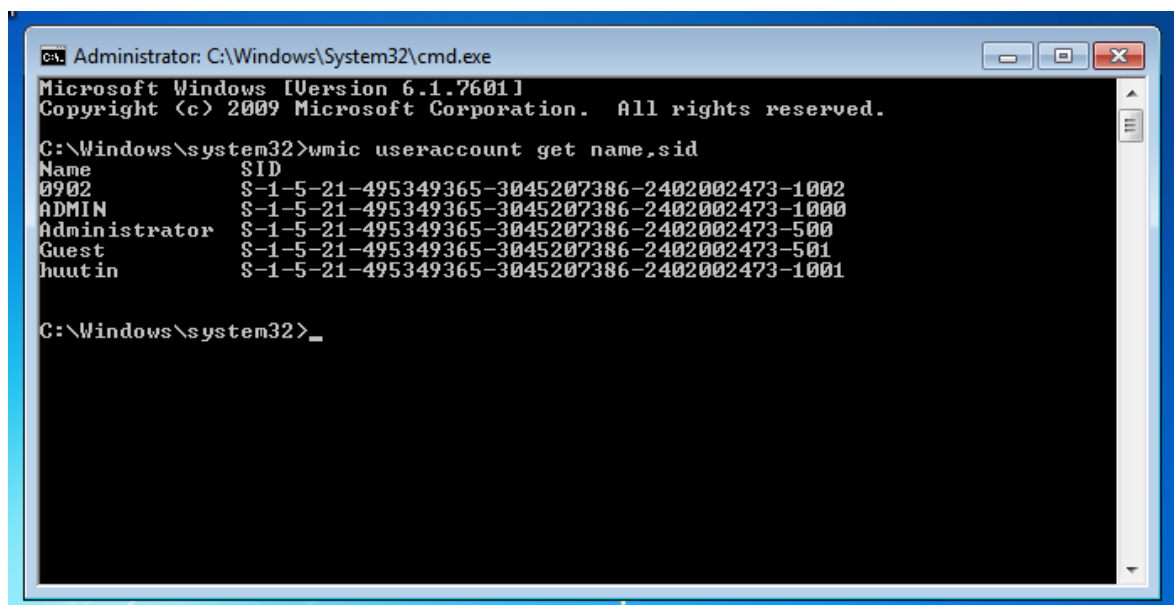
Sử dụng Windows 7 và Windows 10 với công cụ Pwdump7 và Ophcrack. Máy Windows 7 có nhiều user được cấu hình trên đó. Sử dụng quyền truy cập quản trị viên, chúng ta sẽ truy cập các mã băm được mã hóa và chuyển nó sang máy Windows 10 đã cài đặt công cụ Ophcrack để giải mã mật khẩu.

Bước 1: Khởi động máy ảo Windows 7 và mở cmd dưới quyền administrator



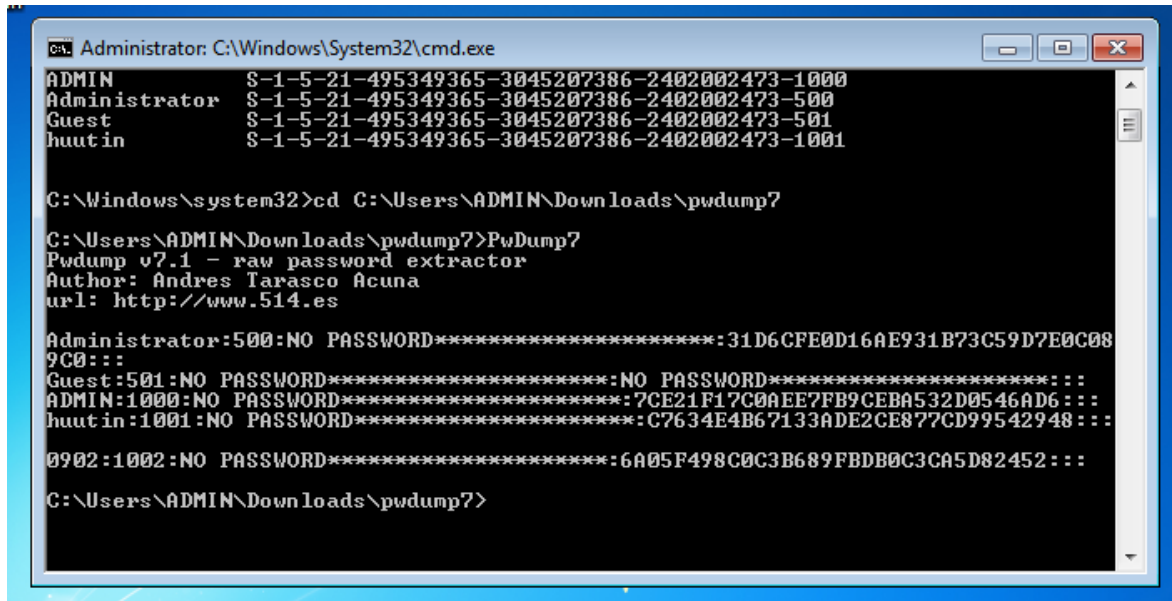
Hình 1. Mở cmd dưới quyền administrative

Bước 2: Nhập câu lệnh wmic useraccount get name,sid



Hình 2. Màn hình hiển thị toàn bộ user và mật khẩu được mã hóa

Bước 3: Đến thư mục chứa file pwdump7.exe



```
Administrator: C:\Windows\System32\cmd.exe

ADMIN          S-1-5-21-495349365-3045207386-2402002473-1000
Administrator  S-1-5-21-495349365-3045207386-2402002473-500
Guest          S-1-5-21-495349365-3045207386-2402002473-501
huutin         S-1-5-21-495349365-3045207386-2402002473-1001

C:\Windows\system32>cd C:\Users\ADMIN\Downloads\pwdump7

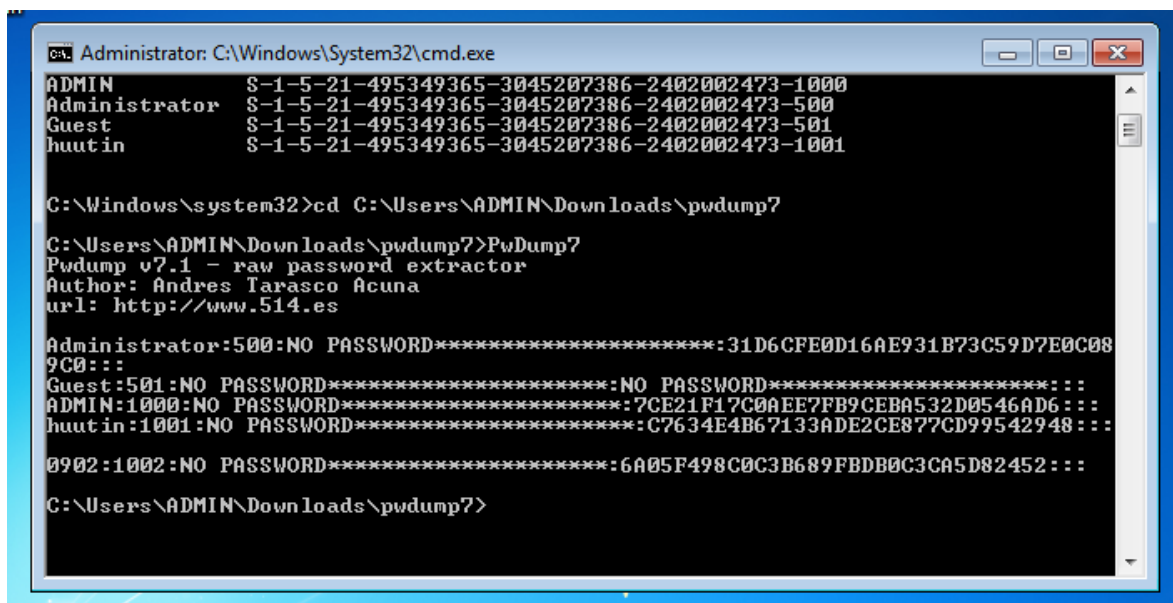
C:\Users\ADMIN\Downloads\pwdump7>PwDump7
PwDump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:NO PASSWORD*****:31D6CFE0D16AE931B73C59D7E0C08
9C0:::
Guest:501:NO PASSWORD*****:NO PASSWORD*****:
ADMIN:1000:NO PASSWORD*****:7CE21F17C0AEE7FB9CEBA532D0546AD6:::
huutin:1001:NO PASSWORD*****:C7634E4B67133ADE2CE877CD99542948:::
0902:1002:NO PASSWORD*****:6A05F498C0C3B689FBD80C3CA5D82452:::

C:\Users\ADMIN\Downloads\pwdump7>
```

Hình 3. Tên user và mã hash của mật khẩu

Bước 4: Copy toàn bộ vào file Hash.txt



```
Administrator: C:\Windows\System32\cmd.exe

ADMIN          S-1-5-21-495349365-3045207386-2402002473-1000
Administrator  S-1-5-21-495349365-3045207386-2402002473-500
Guest          S-1-5-21-495349365-3045207386-2402002473-501
huutin         S-1-5-21-495349365-3045207386-2402002473-1001

C:\Windows\system32>cd C:\Users\ADMIN\Downloads\pwdump7

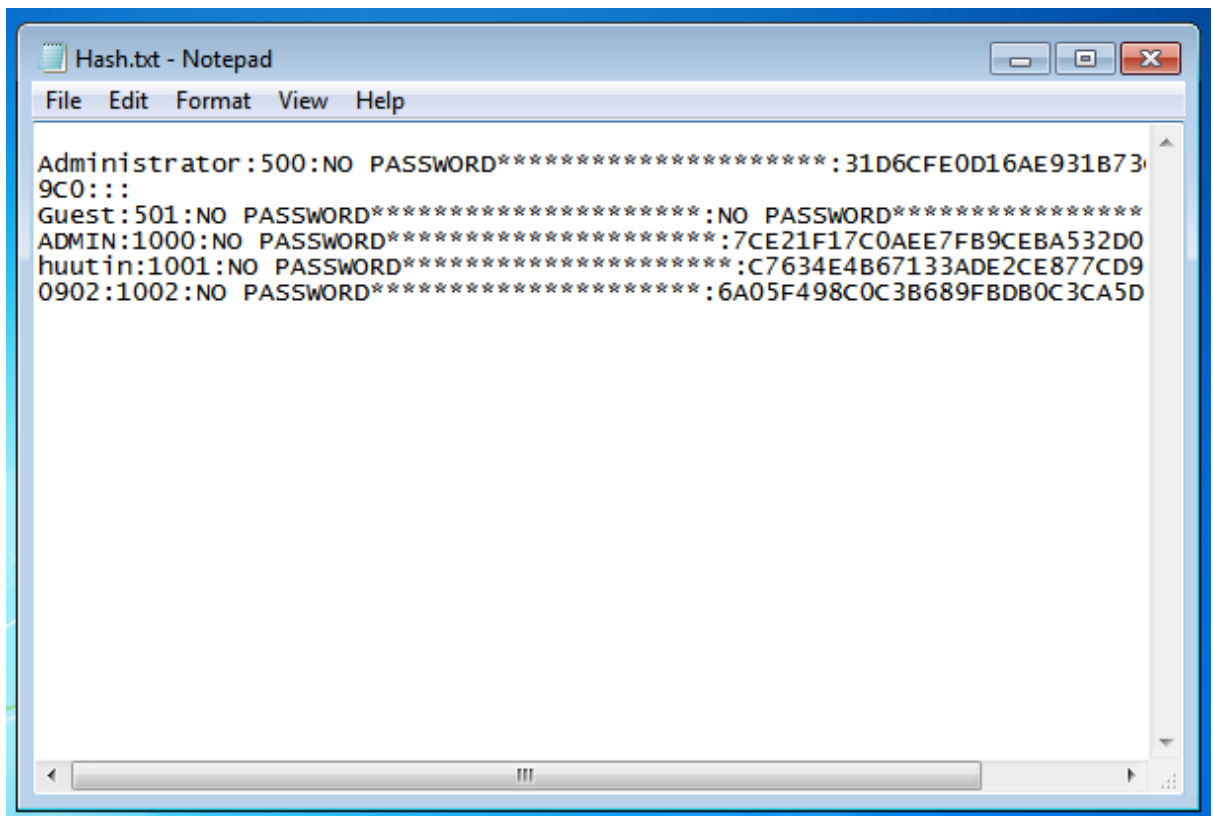
C:\Users\ADMIN\Downloads\pwdump7>PwDump7
PwDump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:NO PASSWORD*****:31D6CFE0D16AE931B73C59D7E0C08
9C0:::
Guest:501:NO PASSWORD*****:NO PASSWORD*****:
ADMIN:1000:NO PASSWORD*****:7CE21F17C0AEE7FB9CEBA532D0546AD6:::
huutin:1001:NO PASSWORD*****:C7634E4B67133ADE2CE877CD99542948:::
0902:1002:NO PASSWORD*****:6A05F498C0C3B689FBD80C3CA5D82452:::

C:\Users\ADMIN\Downloads\pwdump7>
```

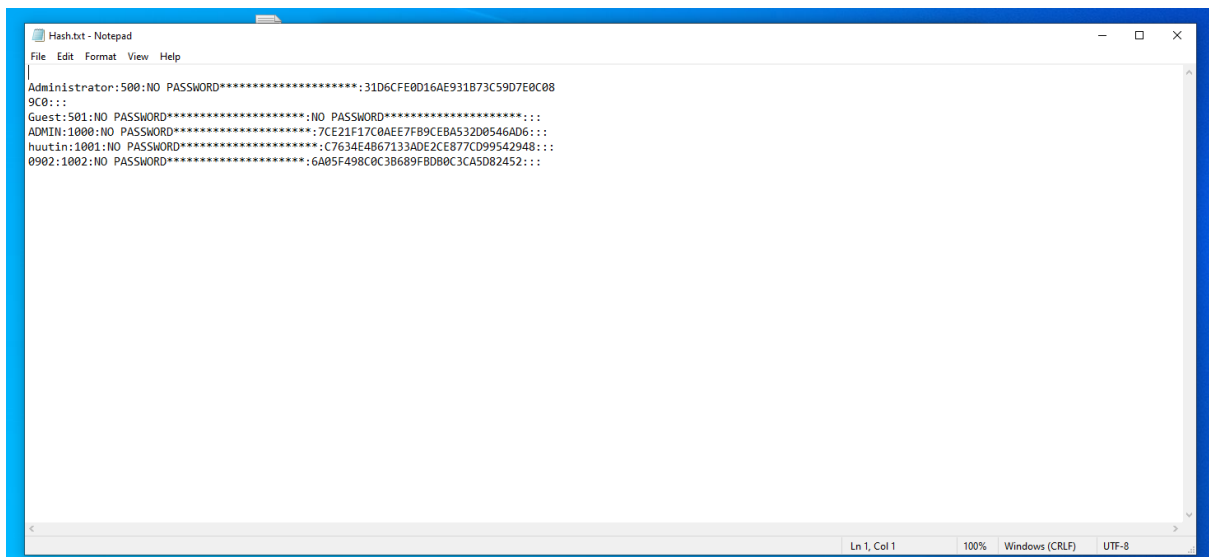
Hình 4. Copy toàn bộ vào file Hash.txt

Bước 5: Kiểm tra file Hash.txt trong thư mục pwdump7 ở Desktop



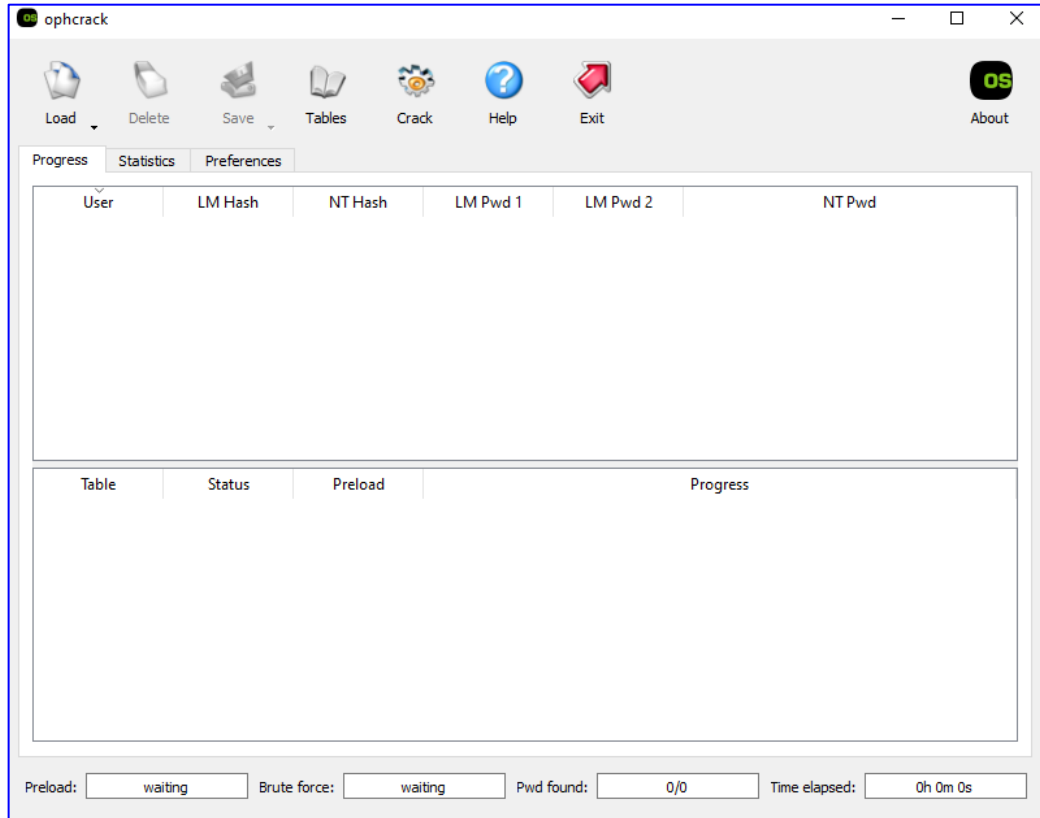
Hình 5. File Hash.txt trong thư mục pwdump7

Bước 6: Chuyển file Hash.txt vào máy ảo Windows 10



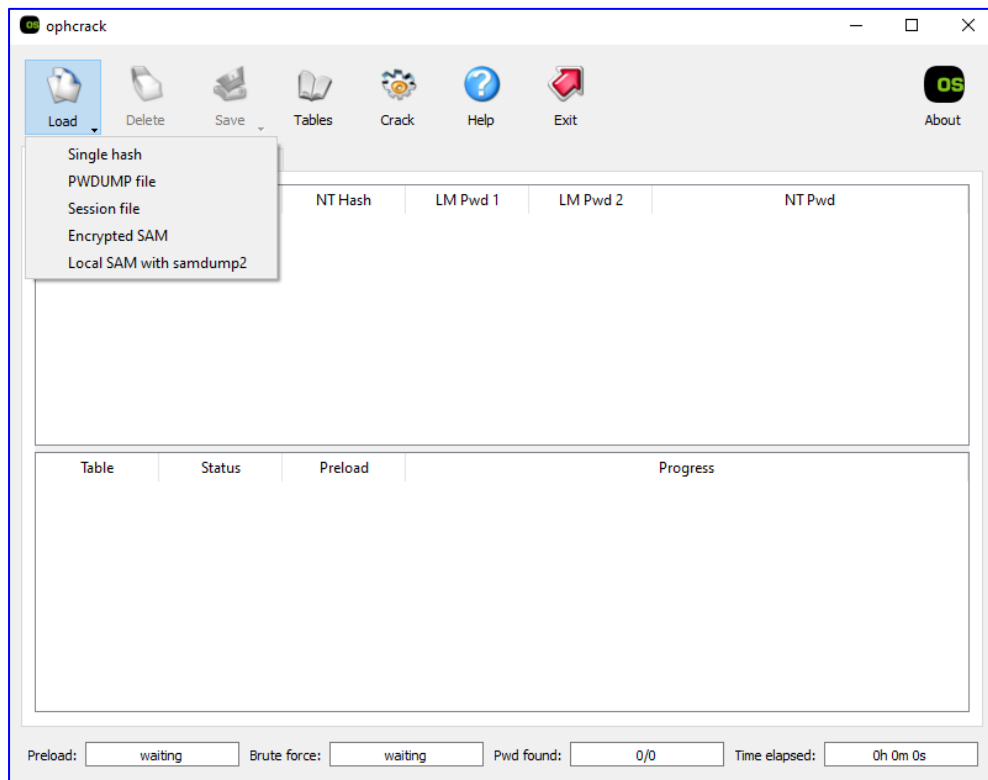
Hình 6. Chuyển file Hash.txt vào máy ảo Windows 10

Bước 7: Khởi động Ophcrack trên máy ảo Windows 10



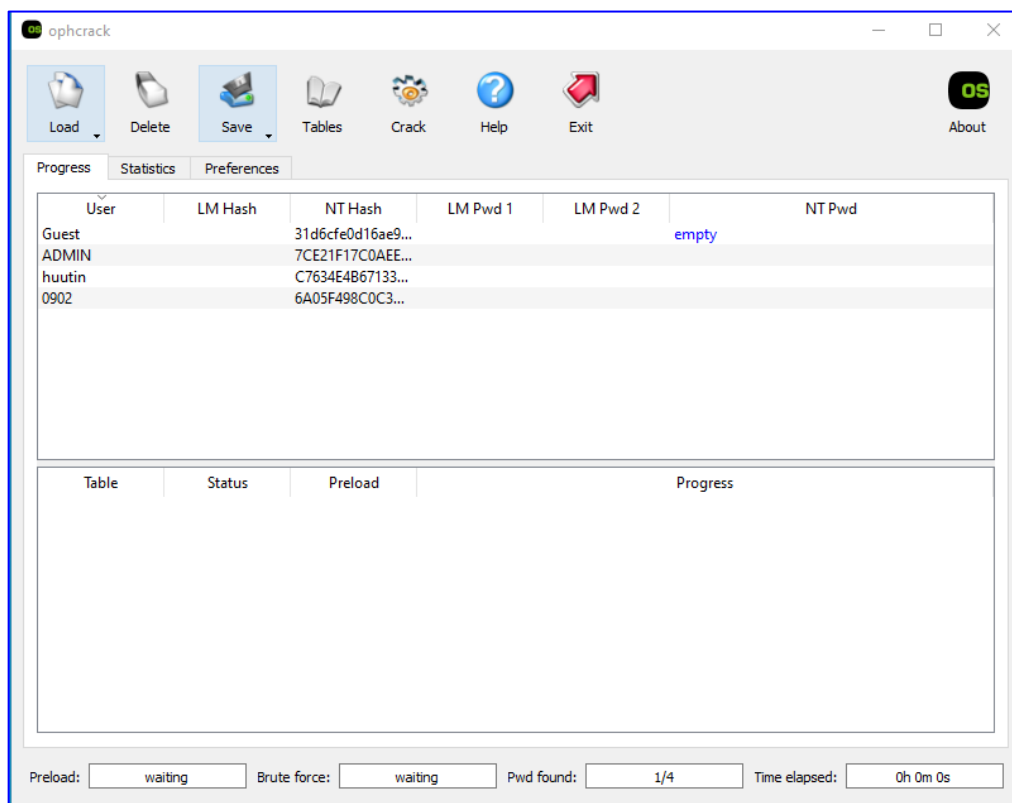
Hình 7. Khởi động Ophcrack trên máy ảo Windows 10

Bước 8: Nhấn vào nút Load, chọn PWDUMP File



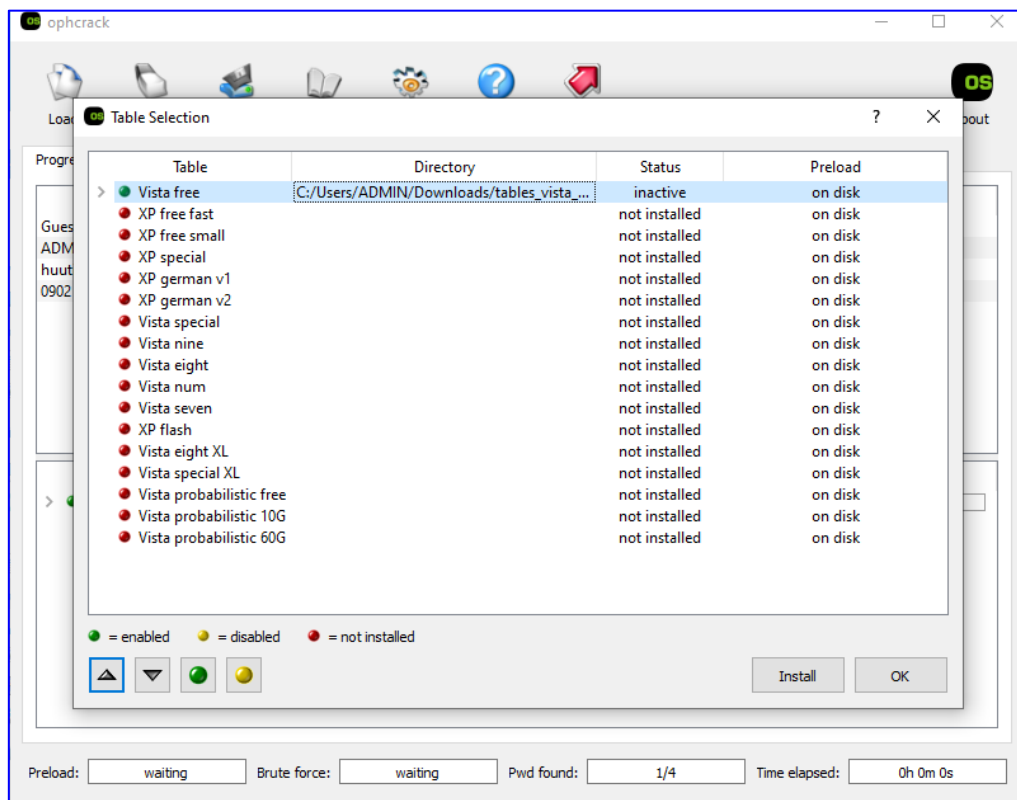
Hình 8. Nhấn vào nút Load, chọn PWDUMP File

Bước 9: Chọn file Hash.txt đã được nhận từ máy Windows 7



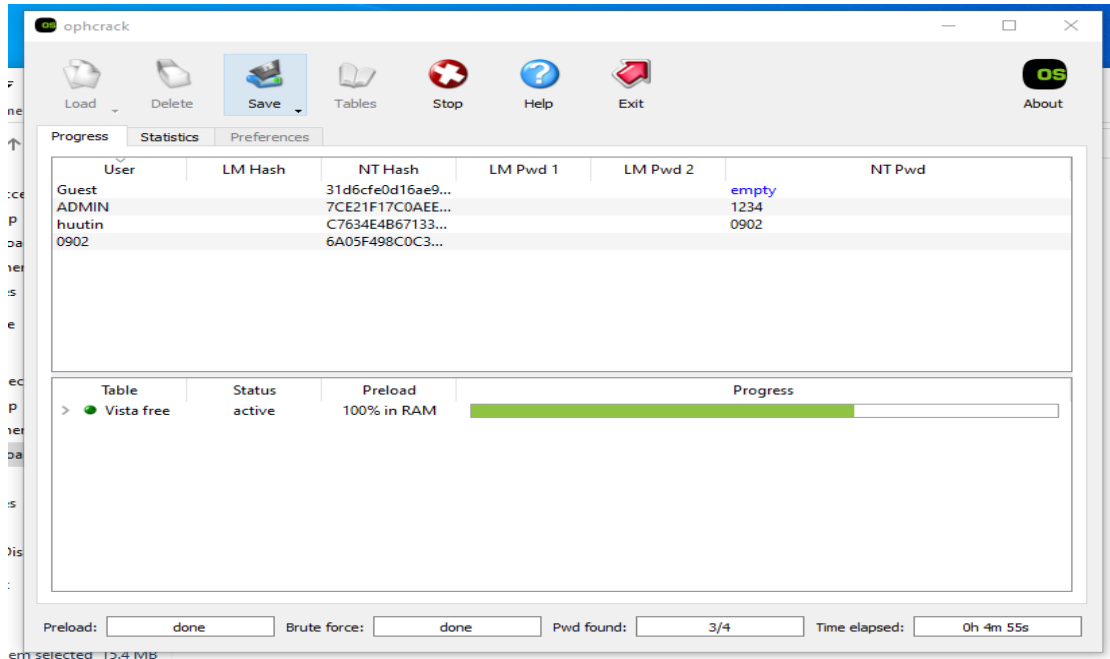
Hình 9. Chọn file Hash.txt

Bước 10: Chọn Tables để hiện mật khẩu (cài đặt Vista free)



Hình 10. Cài đặt Vista free

Bước 11: Chọn Crack để bắt đầu mã hóa dữ liệu



Hình 11. Mật khẩu của các user

2. Sử dụng tool hashcat trên kali để dò mật khẩu win 7

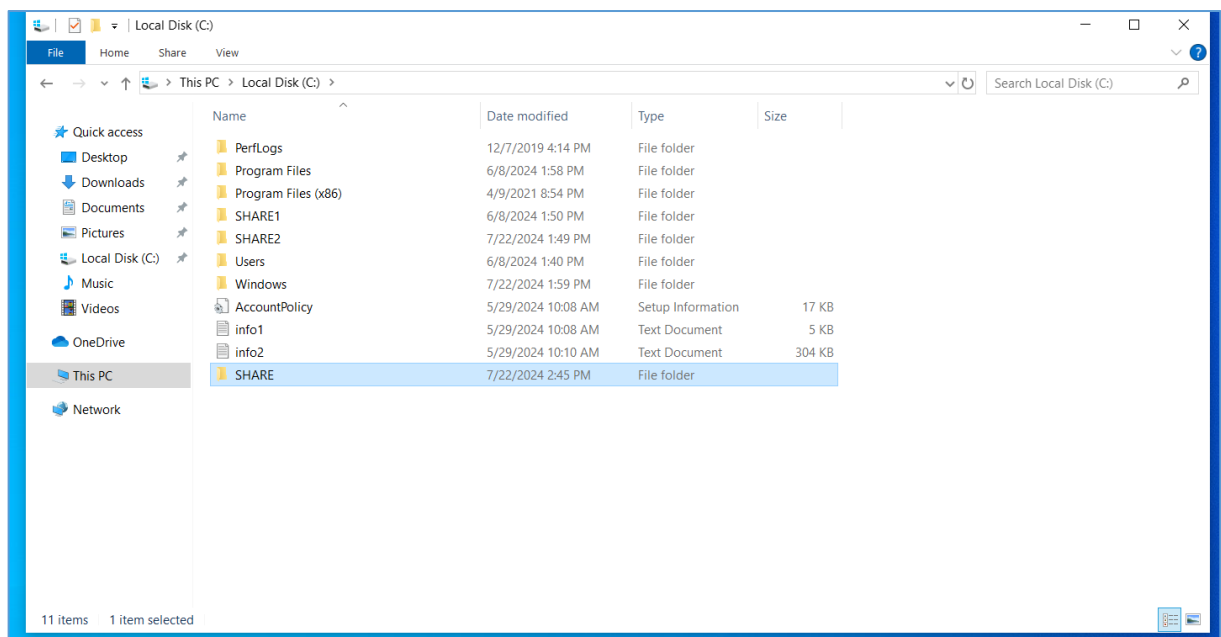
Chuẩn bị 3 máy kali win 10 win 7

Máy bị tấn công win 7

Win 10 lấy thông tin win 7

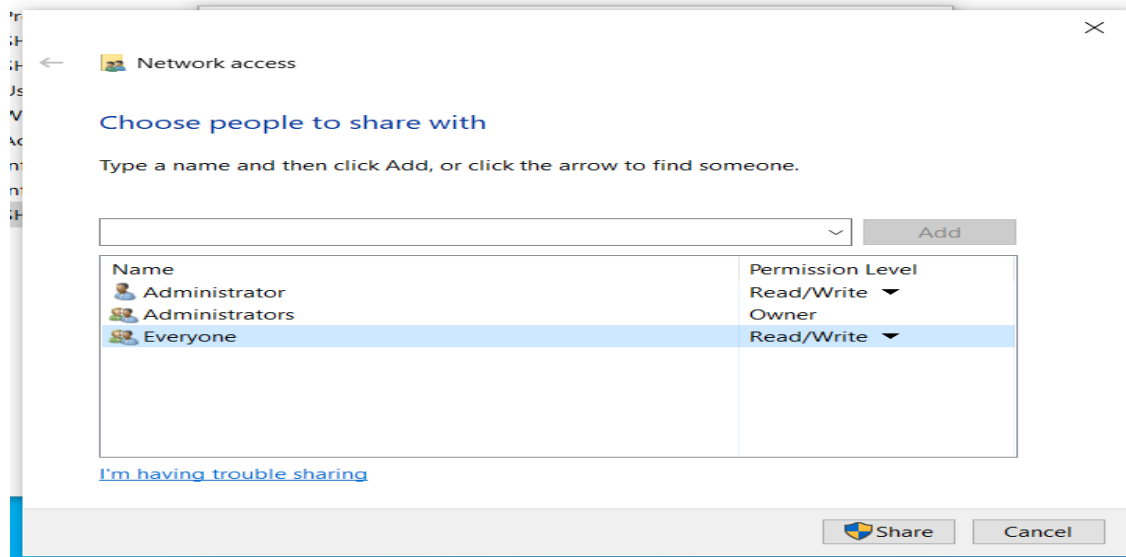
Sử dụng tool hashcat trên kali để dò mật khẩu win 7

Bước 1: Tạo một thư mục share trên win 10



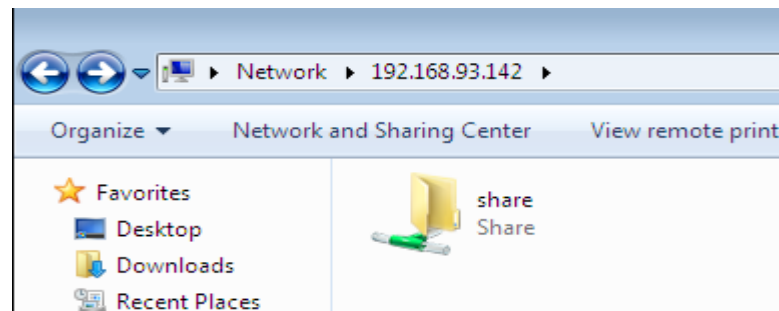
Hình 12. Tạo thư mục Share trên win 10

Bước 2: Cấp quyền truy cập thư mục



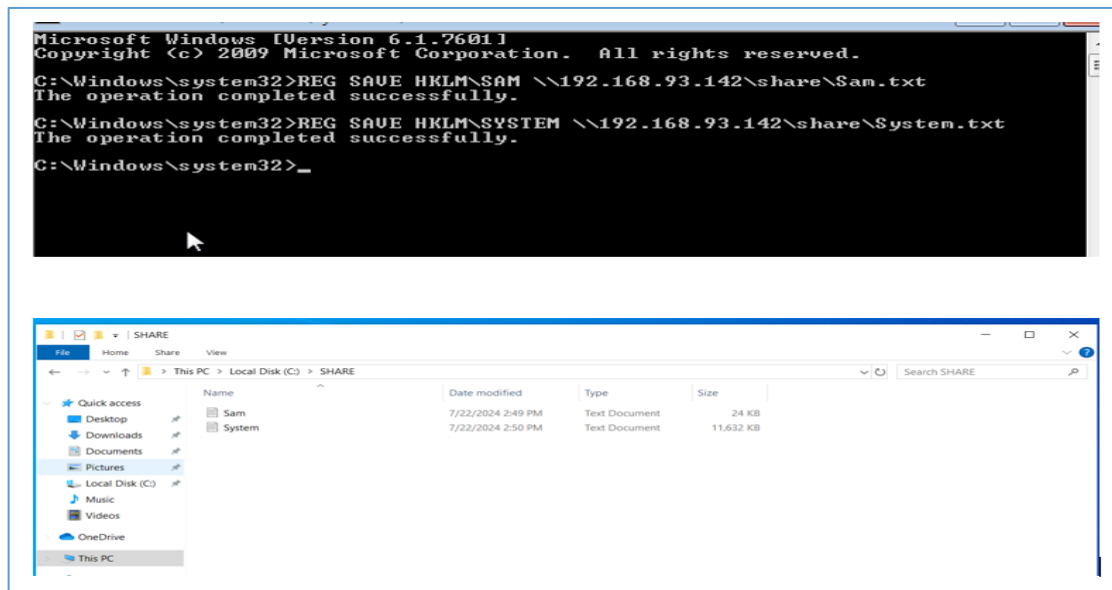
Hình 13. Cấp quyền everyone

Bước 3: win 7 truy cập dữ liệu share win 10



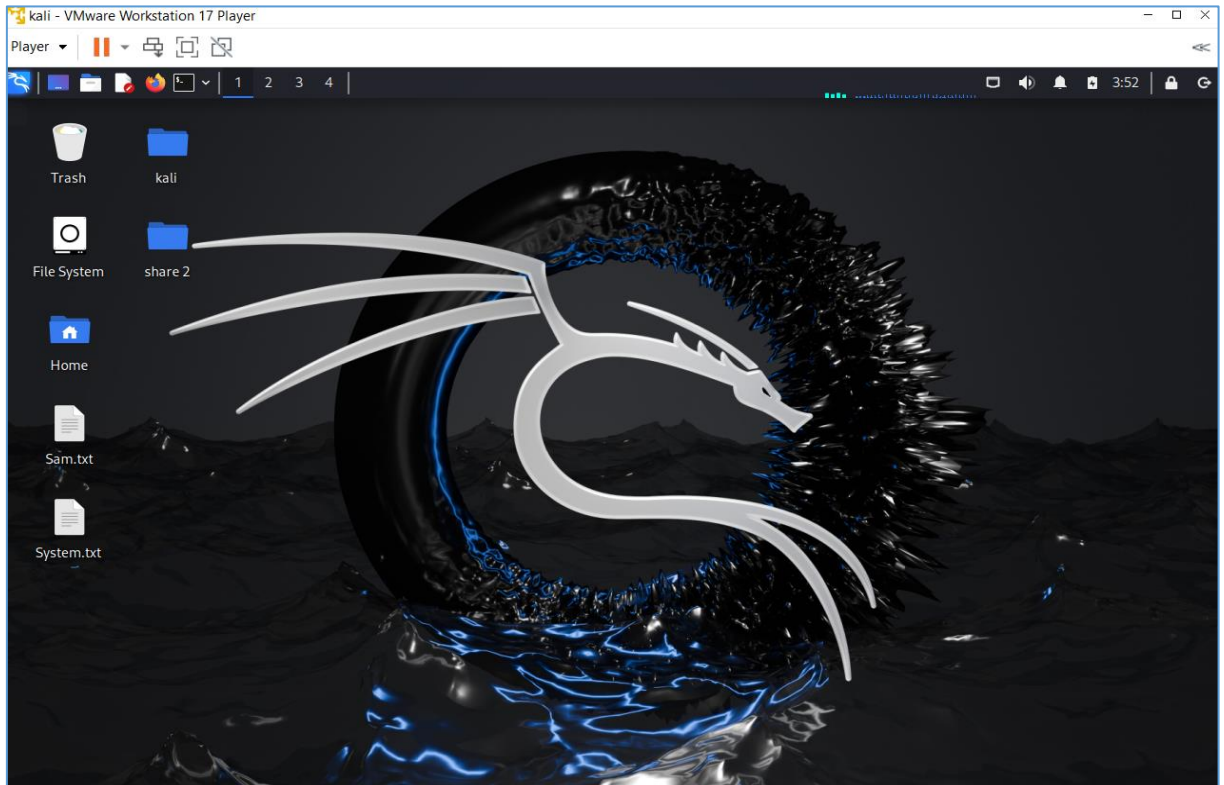
Hình 14. Win 7 truy xuất share win 10

Bước 4: Lưu 2 file sam và system của máy win 7 vào dữ liệu share win 10



Hình 15. Lưu 2 file sam và system của win 7 cho máy win 10

Bước 5: Lấy 2 file system và sam qua máy kali



Hình 16. Lấy file sam và system từ máy win 10 qua kali

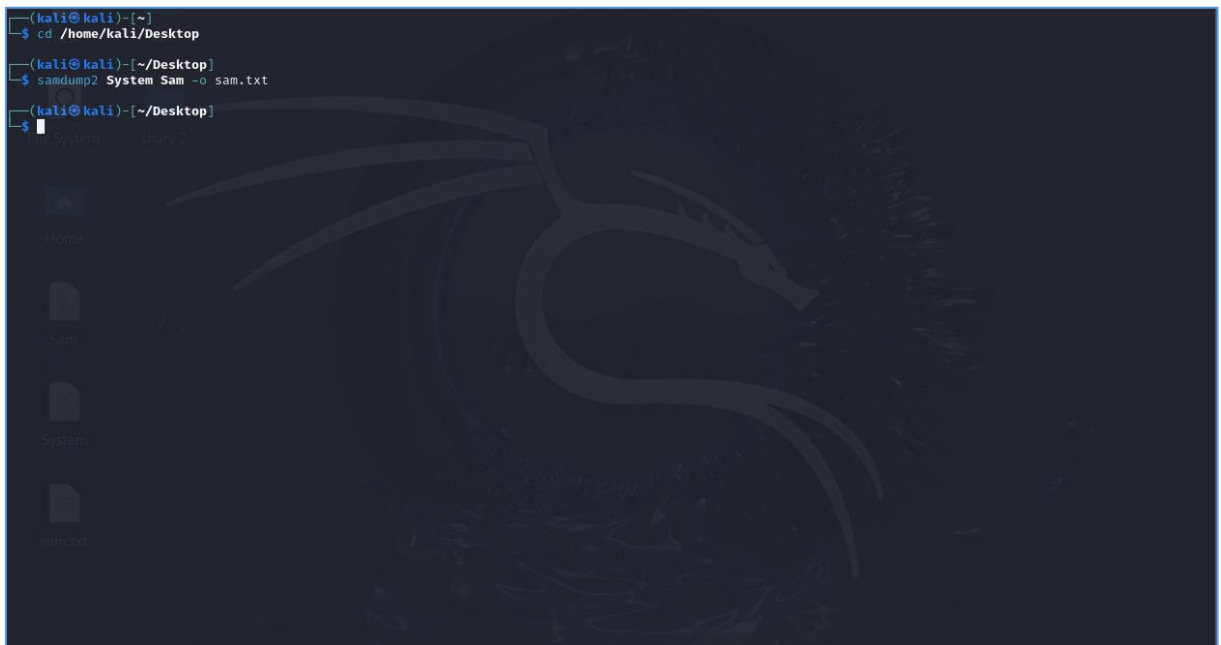
Bước 6: samdump2 được sử dụng để trích xuất các hashes mật khẩu từ các file registry SYSTEM và SAM của Windows.

Giải thích các thành phần của lệnh:

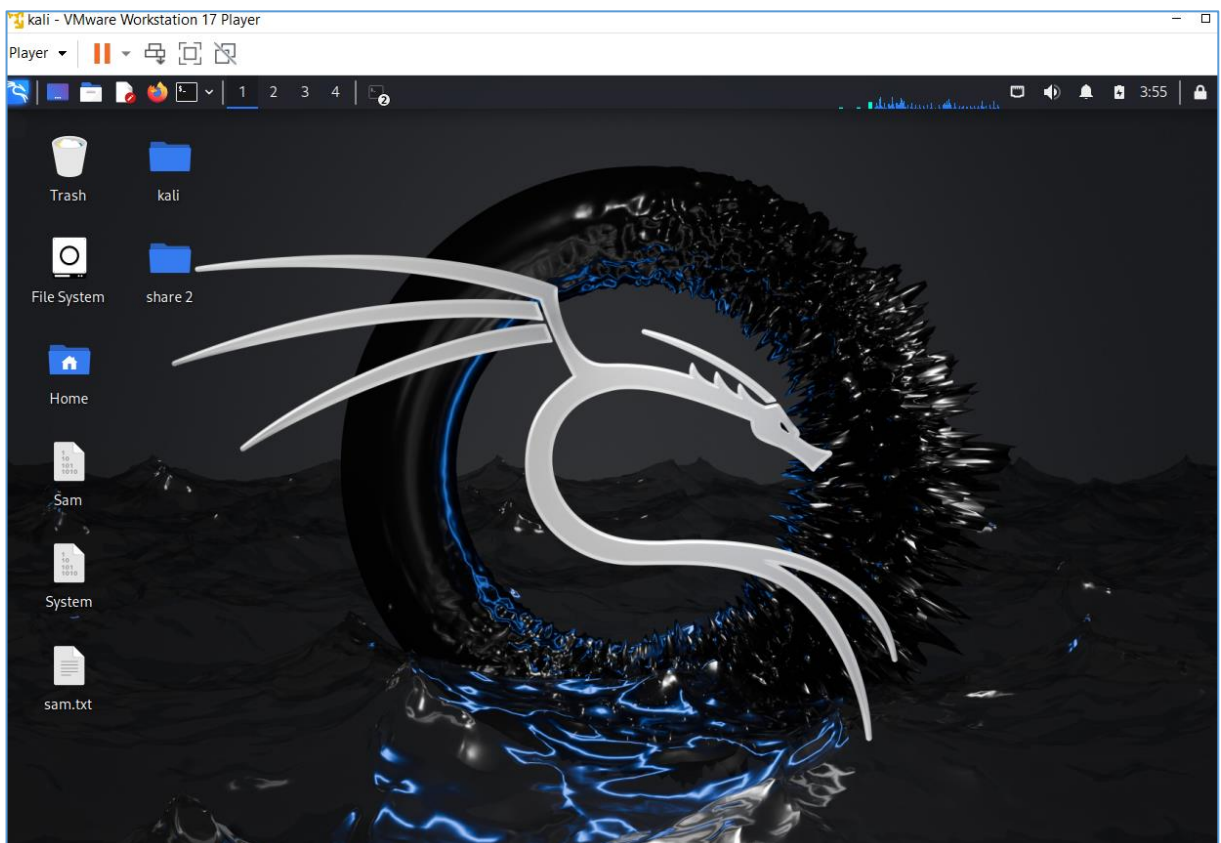
- samdump2: Là công cụ để trích xuất hashes mật khẩu từ các file registry của Windows.
- SYSTEM: Là file registry SYSTEM của Windows. File này chứa thông tin về cấu hình hệ thống và thường được tìm thấy trong thư mục C:\Windows\System32\config.
- SAM: Là file registry SAM của Windows. File này chứa thông tin về tài khoản người dùng và hashes mật khẩu và cũng thường được tìm thấy trong thư mục C:\Windows\System32\config.
- -o sam.txt: Tùy chọn -o chỉ định file đầu ra nơi lưu trữ các hashes mật khẩu đã trích xuất.

Chức năng của lệnh:

- Lệnh samdump2 System Sam -o sam.txt sẽ làm các bước sau:
 - + Trích xuất các hashes mật khẩu: samdump2 sẽ trích xuất các hashes mật khẩu từ file SAM bằng cách sử dụng thông tin từ file SYSTEM.
 - + Lưu trữ các hashes mật khẩu: Các hashes mật khẩu trích xuất được sẽ được lưu vào file đầu ra sam.txt.



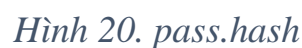
Hình 17. Lệnh



Hình 18. Sam.txt

Bước 7: Copy đoạn mật khẩu chưa được mã hóa của user mà bạn muốn tìm mật khẩu vào file pass.hash

Giải thích chi tiết:



Bước 8: Hashcat nhằm thực hiện một cuộc tấn công brute-force trên các hashes mật khẩu được lưu trong file pass.hash

- hashcat: Đây là chương trình Hashcat, một công cụ mạnh mẽ để bẻ khóa các hashes mật khẩu bằng nhiều phương pháp khác nhau, bao gồm brute-force, dictionary attacks, và nhiều phương pháp khác.

- pass.hash: Đây là file chứa các hashes mật khẩu mà bạn muốn bẻ khóa. Bạn có thể có một hoặc nhiều hashes trong file này.

- -d 1: Chỉ định thiết bị (device) mà Hashcat sẽ sử dụng để thực hiện tấn công. -d 1 có nghĩa là sử dụng thiết bị thứ nhất (thường là GPU đầu tiên). Nếu bạn có nhiều GPU, bạn có thể chỉ định các GPU cụ thể bằng các chỉ số khác nhau.

- -a 3: Chọn chế độ tấn công. -a 3 chỉ định chế độ brute-force attack.

- -m 1000: Chỉ định loại hash mà bạn đang tấn công. -m 1000 là NTLM hash (mật khẩu Windows).

- -i: Bật chế độ tăng dần (incremental mode). Điều này cho phép Hashcat bắt đầu với mật khẩu ngắn hơn và dần dần tăng độ dài cho đến khi đạt độ dài tối đa được chỉ định.

- --increment-min=3: Đặt độ dài tối thiểu của mật khẩu là 3 ký tự. Chỉ áp dụng khi -i được bật.

- --increment-max=3: Đặt độ dài tối đa của mật khẩu là 3 ký tự. Chỉ áp dụng khi -i được bật.

- ?d?d?d: Đây là mặt nạ (mask) cho brute-force attack. ?d đại diện cho bất kỳ chữ số nào (0-9). ?d?d?d có nghĩa là thử tất cả các mật khẩu có 3 chữ số từ 000 đến 999.

```
The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keypace - workload adjusted.

Session.....: hashcat
Status.....: Exhausted
Hash.Mode.....: 1000 (NTLM)
Hash.Target.....: aad3b435b51404eeaad3b435b51404ee
Time.Started.....: Mon Jul 22 04:00:20 2024 (0 secs)
Time.Estimated...: Mon Jul 22 04:00:20 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.....: ?d?d?d [3]
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 83059 H/s (1.34ms) @ Accel:1024 Loops:10 Thr:1 Vec:8
Recovered.....: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.....: 1000/1000 (100.00%)
Rejected.....: 0/1000 (0.00%)
Restore.Point....: 100/100 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-10 Iteration:0-10
Candidate.Engine.: Device Generator
Candidates.#1....: 123 → 676
Hardware.Mon.#1..: Util: 21%

Started: Mon Jul 22 04:00:12 2024
Stopped: Mon Jul 22 04:00:22 2024
```

```
(kali@kali)~[~/Desktop]
$
```

Hình 21. Kết Quả

III. ĐÁNH GIÁ

1. Chúng tôi làm được những gì?

- Nắm vững kiến thức cơ bản về system hacking: Hiểu rõ các hình thức tấn công system hacking phổ biến, cách thức hoạt động và tác động của chúng.
- Có khả năng áp dụng các biện pháp phòng chống cơ bản: Biết cách triển khai các biện pháp bảo vệ như Prepared Statements và ORM để giảm thiểu rủi ro SQL Injection.
- Có kỹ năng thực hành: Thực hành thành công việc triển khai các biện pháp phòng chống trên các ứng dụng mẫu.

2. Chưa làm được những gì?

- Kinh nghiệm thực tế: Chưa có cơ hội áp dụng kiến thức và kỹ năng trên các hệ thống thực tế phức tạp.
- Áp dụng toàn diện: Do hạn chế về thời gian và nguồn lực, chưa thể áp dụng đầy đủ các biện pháp phòng chống trong một dự án thực tế.
- Kỹ thuật nâng cao: Chưa có đủ thời gian để nghiên cứu và áp dụng các kỹ thuật bảo mật tiên tiến

3. Điểm hạn chế:

- Hạn chế về kinh nghiệm thực tiễn trong việc phát hiện và ngăn chặn các cuộc tấn công hệ thống trên các hệ thống thực tế. Chưa có đủ thời gian để nghiên cứu và áp dụng các kỹ thuật bảo mật tiên tiến hơn như Machine Learning trong phát hiện và ngăn chặn các cuộc tấn công hệ thống.

4. Hướng phát triển trong tương lai:

- Tiếp tục học tập và rèn luyện: Trau dồi kiến thức và kỹ năng về system hacking thông qua các khóa học, tài liệu chuyên ngành và dự án thực tế.
- Tăng cường thực hành: Áp dụng kiến thức đã học vào thực tế để nâng cao khả năng phát hiện và xử lý các lỗ hổng system hacking.
- Nghiên cứu kỹ thuật tiên tiến: Tìm hiểu và áp dụng các kỹ thuật bảo mật tiên tiến như Machine Learning để nâng cao hiệu quả phòng chống system hacking.
- Mở rộng kiến thức: Mở rộng kiến thức về an ninh mạng nói chung để có thể đánh giá và bảo vệ hệ thống một cách toàn diện.

IV. KẾT LUẬN

System Hacking là một mối đe dọa phổ biến và tinh vi, gây ra rủi ro lớn về an toàn và toàn vẹn của hệ thống máy tính và mạng. Việc cảnh giác và chủ động phòng thủ chống lại các mối đe dọa này là rất quan trọng bằng cách liên tục cập nhật kiến thức và kỹ năng để đối phó với các cuộc tấn công ngày càng phức tạp và tinh vi. Bằng cách đó, chúng ta có thể đảm bảo bí mật, toàn vẹn và sẵn sàng

của thông tin nhạy cảm và bảo vệ chống lại các hậu quả thảm khốc của hack hệ thống.

V. TÀI LIỆU THAM KHẢO

- Chat GPT
- CEH V10 EC-COUNCIL CERTIFIED MODULE 6