Bài: 6.1 System Hacking - Hệ phương pháp của system hacking và bẻ khóa mật khẩu

Xem bài học trên website để ủng hộ Kteam: 6.1 System Hacking - Hệ phương pháp của system hacking và bẻ khóa mật khẩu

Mọi vấn đề về lỗi website làm ảnh hưởng đến bạn hoặc thắc mắc, mong muốn khóa học mới, nhằm hỗ trợ cải thiện Website. Các bạn vui lòng phản hồi đến Fanpage How Kteam nhé!

Tóm tắt

Với thông tin thu thập được từ các công đoạn xâm nhập trước như thăm dò, quét, liệt kê, bây giờ bạn có thể chuyển qua level tiếp theo: **system hacking**. Sử dụng tất cả những thông tin về mục tiêu trước đó, chúng ta sẽ đi tiếp đến bước truy cập hệ thống.

Hãy tóm tắt tất cả những thông tin thu thập được, ví dụ như danh sách tên user, địa chỉ mail, mật khẩu, nhóm, dải IP, hệ điều hành, phiên bản phần cứng và phần mềm, chia sẻ, giao thức, thông tin dịch vụ và những chi tiết khác. Dựa vào những thông tin này, người tấn công sẽ có một bức tranh rõ ràng hơn về mục tiêu.

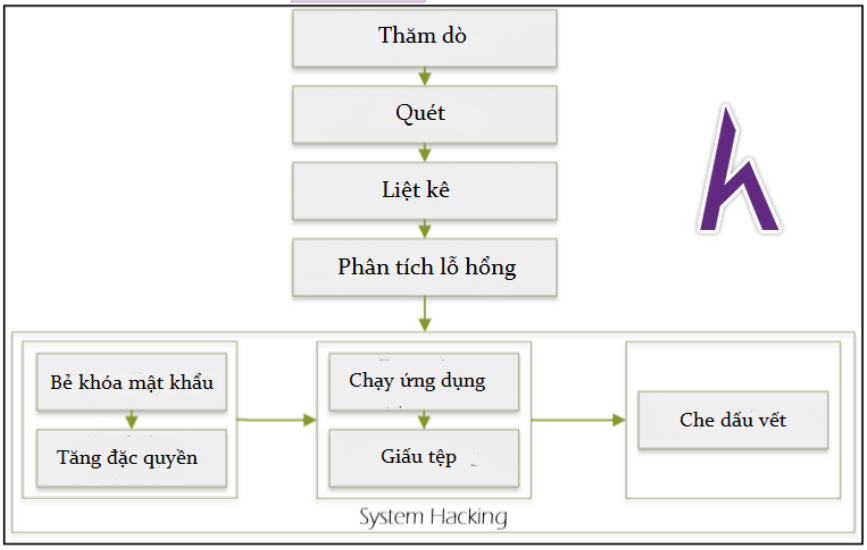

Figure 6-01 System Hacking

System hacking

Sau khi có được thông tin cần thiết thì chuyển qua công đoạn **system hacking**. Quy trình hacking ở đây khó khăn và phức tạp hơn những công đoạn trước.

Trước khi bắt đầu, một hacker "**mũ trắng**" hay một **pentester** (người kiểm thử xâm nhập) phải ghi nhớ rằng việc truy cập vào hệ thống ngay khi mới thử là bất khả thi. Bạn phải quan sát kĩ càng, kiên nhẫn chờ đợi và cố gắng vì mục tiêu thì mới có kết quả.

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 bao gồm:

1. Bẻ khóa mật khẩu
2. Tăng đặc quyền
3. Chạy ứng dụng
4. Giấu tệp

5. Che dấu vết

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 kĩ 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 kí truy cập (logs).

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 tên user và mật khẩu.
- Thứ tôi là, ví dụ như sinh trắc học (dấu vân tay).
- Thứ tôi sở hữu, ví dụ như thiết bị đã đăng ký/ được cấp phép

Bẻ khóa mật khẩu là quá trình trích rút mật khẩu để nhận quyền truy cập vào mục tiêu như một 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 kĩ 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 tốt tiêu biểu sẽ chứa:

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

Các kiểu tấn công mật khẩu

Tấn công phi kĩ thuật

Tấn công phi kĩ thuật là loại tấn công không đòi hỏi bất cứ kiến thức chuyên môn nào. Loại tấn công này có thể 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, v.v. 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

Tấn công online chủ động

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

a. 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 kí tự chữ-số thì thường không bị ảnh hưởng bởi dictionary attack.

b. Brute force attack

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

c. Hash injection

Kiểu tấn công này đòi hỏi kiến thức về **hashing** (hàm băm) và **cryptograhy** (mật mã học). Trong tấn công này:

- Kẻ tấn công cần trích rút nhật kí của user trong hashes và stores trong tệp **Security Account Manager** (SAM).
- Bằng cách lợi dụng những lổ 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.

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:

a. 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.

b. 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)

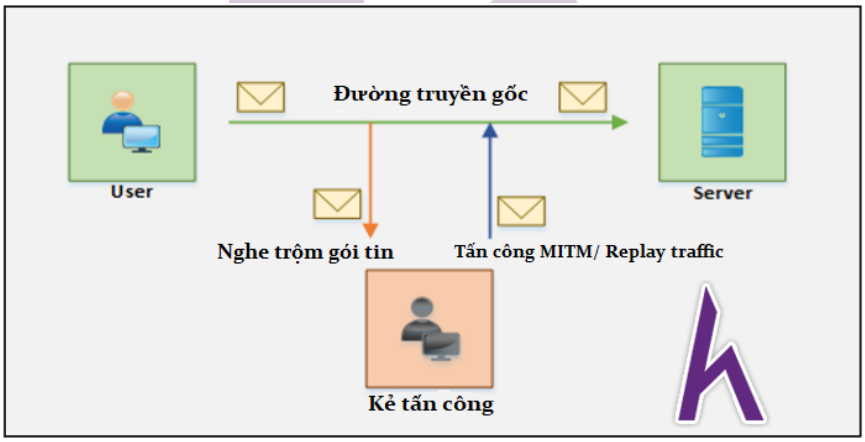

Figure 6-02 MITM Attack

c. 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 anh ta tạo ra replay traffic với các thông tin đã trích rút.

Mật khẩu mặc định (Default Password)

Mỗi thiết bị mới đều được nhà sản xuất thiết lập một **mật khẩu mặc định**. Mặc dù user được khuyến cáo đổi mật khẩu sẵn có này sang một mật khẩu độc nhất và bí mật khác, nhiều người vẫn giữa nguyên mật khẩu mặc định, tạo điều kiện cho tấn công. Tấn công này phù hợp với đối tượng muốn sử dụng mật khẩu mặc định bằng cách tìm trong website của nhà sản xuất hoặc nhờ công cụ tìm mật khẩu mặc định online. Dưới đây là danh sách các công cụ sẵn có để tìm mật khẩu mặc định.

- https://cirt.net/

- https://default-password.info/
- http://www.passwordsdatabase.com/

Lab 6-1: Sử dụng công cụ online để tìm mật khẩu mặc định

Bài tập

Mở trình duyệt internet. Đến bất cứ website tìm mật khẩu mặc định nào bạn thích. Ví dụ, vào website

> https://cirt.net/

Sau đó, chọn nhà sản xuất thiết bị của bạn.

Sau khi chọn, web sẽ cho thấy mật khẩu tất cả thiết bị của nhà sản xuất này.

Tấn công offline

a. **Pre-Computed hashes** and **Rainbow Table** (hàm băm tính toán trước và bảng cầu vồng)

Một ví dụ của tấn công offline là dùng bảng cầu vồng để so sánh mật khẩu. Một bảng cầu vồng là danh sách chứa các giá trị hash đã được tính toán cho mọi kết hợp kí 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 vồng. Ưu điểm của bảng cầu vồng 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 vồng ban đầu.

Để tạo bảng cầu vồng, 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

b. Distributed 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 lí 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.

Lab 6-2: Tạo bảng cầu vồng bằng công cụ Winrtgen

Bài tập

Mở ứng dụng Winrtgen. Click vào nút **Add Table** để tạo Bảng cầu vồng mới.

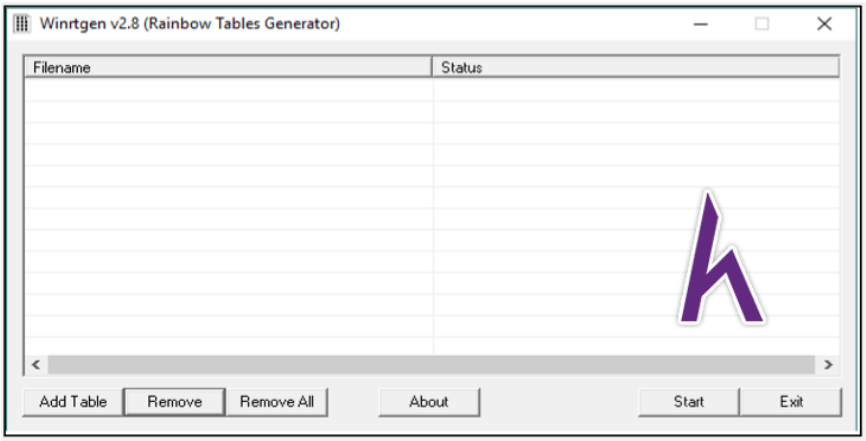

Figure 6-05 Winrtgen tool for Rainbow Table

Chọn Hash, độ dài tối thiểu, độ dài tối đa và các thuộc tính khác theo yêu cầu.

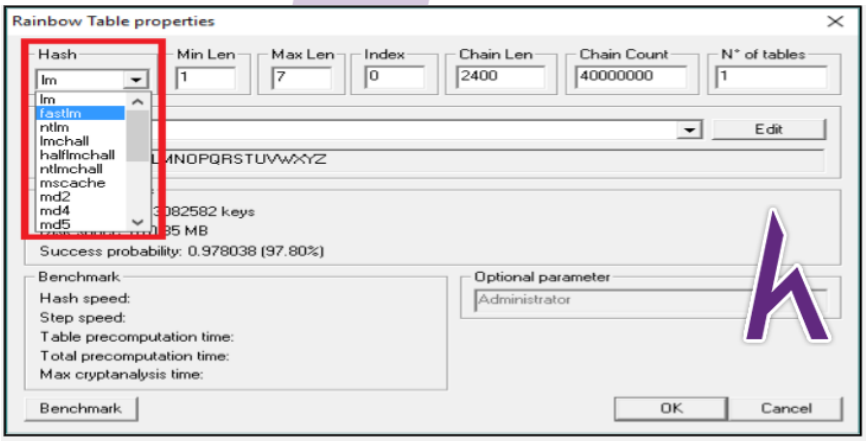

Figure 6-06 Winrtgen tool for Rainbow Table

Chọn giá trị **Charset**. Có thể chọn bảng chữ cái, kí tự chữ số hoặc các kết hợp kí tự có sẵn khác như trong hình dưới đây.

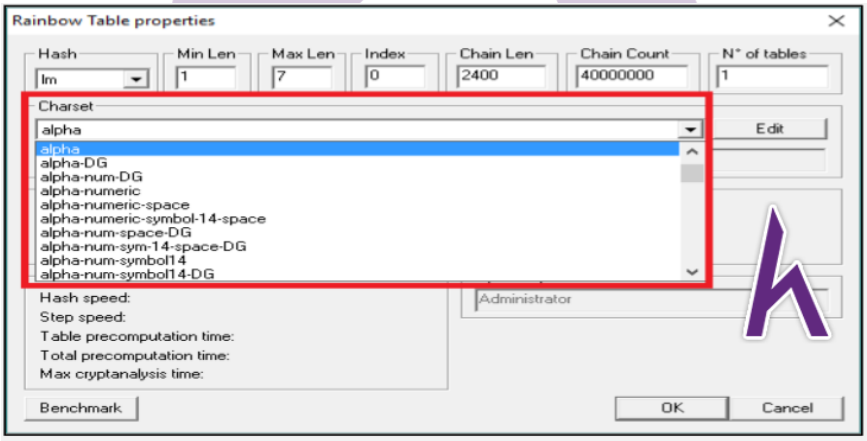

Figure 6-07 Winrtgen tool for Rainbow Table

Click vào nút **Benchmark** để ước lượng tốc độ **Hash**, tốc độ **Step**, thời gian tính toán và các thông số khác.

Click **OK** để tiếp tục.

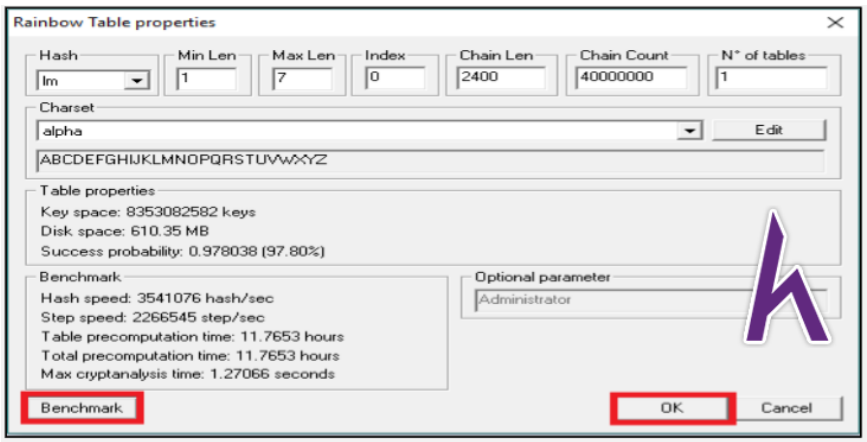

Figure 6-08 Winrtgen tool for Rainbow Table

Click **Start** để bắt đầu tính toán.

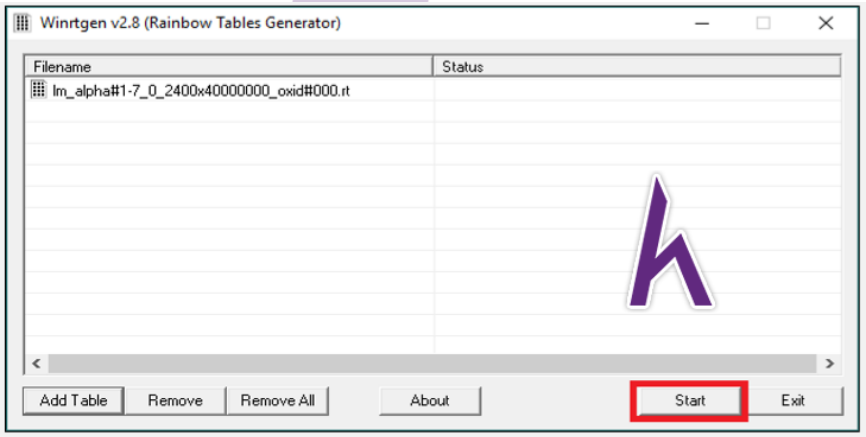

Figure 6-09 Winrtgen tool for Rainbow Table

Tính toán tất cả các giá trị hashes sẽ tốn một khoảng thời gian khá lâu.

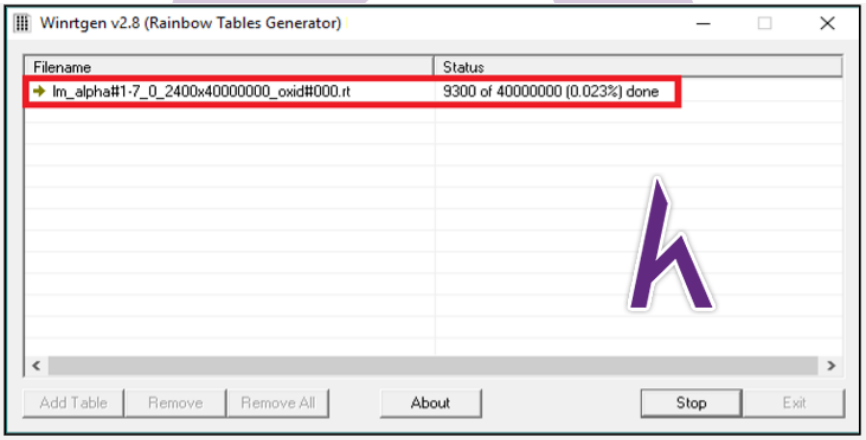

Figure 6-10 Winrtgen tool for Rainbow Table

Khi bảng hoàn thành, bạn có thể tìm được **Window Table** ở trong thư mục (directory).

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 kĩ thuật có thể có ích cho kiểu tấn công này.

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.

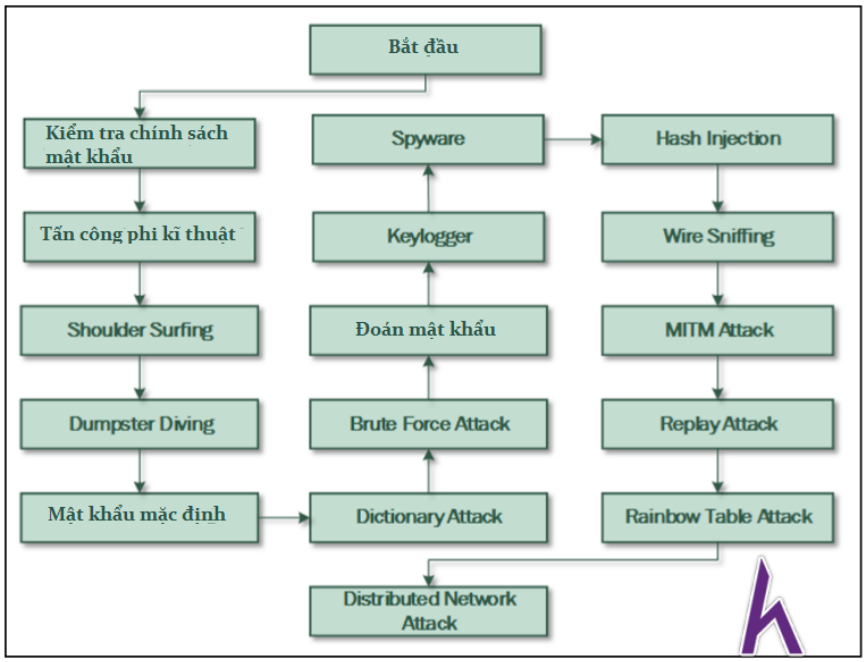

Figure 6-11 Password Cracking Flow Chart

Xác thực Microsoft

Trong hệ thống mạng máy tính, xác thực là quá trình xác nhận danh tính của user hay thiết bị. Khi bạn xác thực một thực thể, mục tiêu là xác thực tính chính thống của thiết bị. Tương tự, khi bạn xác thực một user, mục tiêu là xác thực user đó có phải kẻ mạo danh hay không.

Trong nền tảng Microsoft, hệ điều hành cài đặt một bộ giao thức xác thực mặc định bao gồm Kerberos, Security Account Manager (SAM), NT LAN Manager (NTLM), LM, và các cơ chế xác thực khác. Những giao thức này đảm bảo quá trình xác thực user, máy tính và dịch vụ diễn ra thành công.

Security Account Manager (SAM) (Quản lí bảo mật tài khoản)

SAM là một cơ sở dữ liệu chứa dữ liệu xác minh và các thông số khác như mật khẩu để phục vụ quá trình xác thực trong hệ điều hành Windows. Trong nền tảng Microsoft, SAM chứa mật khẩu dưới dạng hashed và các thông tin tài khoản khác.

Khi hệ điều hành đang hoạt động, cơ sở dữ liệu này bị khóa lại để tránh tiếp cận từ dịch vụ. Có nhiều thuật toán bảo mật khác được sử dụng để bảo đảm tính toàn vẹn của dữ liệu.

Microsoft Windows lưu trữ mật khẩu dưới dạng hashing LM/ NTLM. Windows XP và các phiên bản mới hơn của Windows không chứa giá trị LM hash, hoặc khi giá trị LM hash vượt quá 14 kí tự, máy sẽ chứa giá trị trống hoặc mô hình giả (dummy).

> **Username: user ID: LM Hash: NTLM Hash:::**

Mật khẩu dưới dạng hashed được lưu trữ như hình dưới:

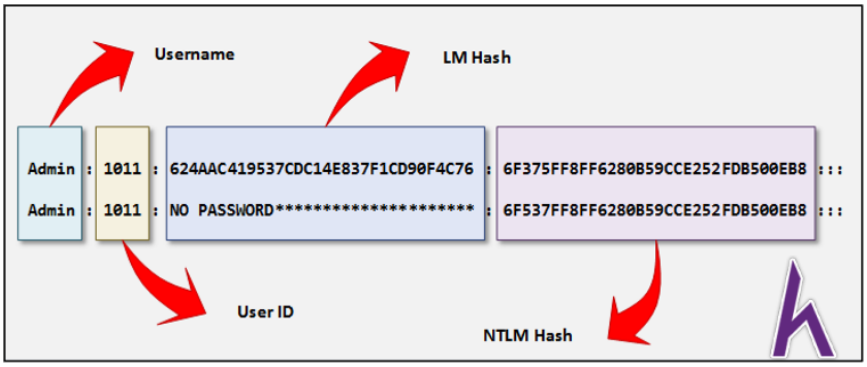

Figure 6-12 Stored hashed password in SAM File

Tệp SAM ở trong thư mục

> c:\windows\system32\config\SAM.

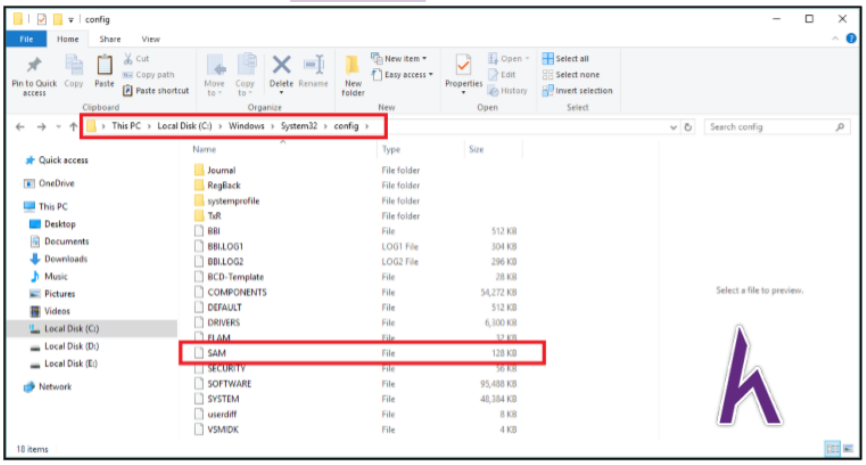

Figure 6-13 SAM File Directory

Xác thực NTLM

NT Lan Manager (NTLM) là giao thức xác thực sở hữu độc quyền của Microsoft. Trong quy trình xác thực NTLM, user gửi dữ liệu xác minh đăng nhập cho bộ kiểm soát miền (domain controller).

Bộ kiểm soát miền sẽ tạo ra "thử thách": đó là "nonce" được mã hóa bằng hash của mật khẩu. Nonce này là một mã số ngẫu nhiên 16-byte mà bộ kiểm soát miền tạo ra. Bộ kiểm soát sẽ so sánh phản hồi nhận được với dữ liệu, từ đó quyết định cho phép hay từ chối việc đăng nhập. Microsoft đã nâng cấp cơ chế xác thực mặc định từ NTLM sang Kerberos.

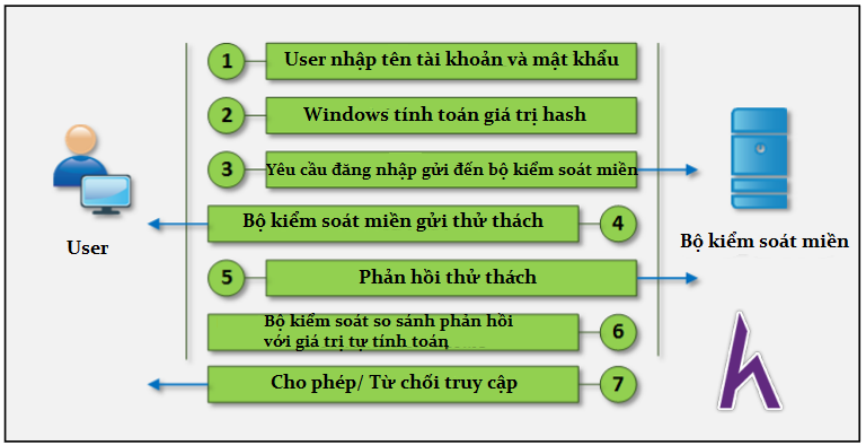

Figure 6-14 NTLM Authentication Process

Xác thực NTLM có hai phiên bản:

1. NTLMv1 (phiên bản cũ)
2. NTLMv2 (phiên bản nâng cấp)

NTLM hoạt động song song với một tầng bảo mật khác: **Security Support Provider** (SSP) (Hỗ trợ bảo mật)

Dưới đây là một số hệ điều hành mà tệp của chúng chứa các mật khẩu mã hóa.

Hệ điều hành	Tệp chứa mật khẩu mã hóa
Windows	SAM File
Linux	SHADOW
Domain Controller (Windows)	NTDS:DIT

Kerberos

Microsoft Kerberos là một giao thức xác thực nâng cao. Trong Kerberos, user sẽ nhận được vé (tickets) từ **Key Distribution Center Kerberos** (KDC). KDC hoạt động phụ thuộc vào các thành tố dưới đây:

1. Server xác thực (AS)
2. Serve cấp vé (TGS)

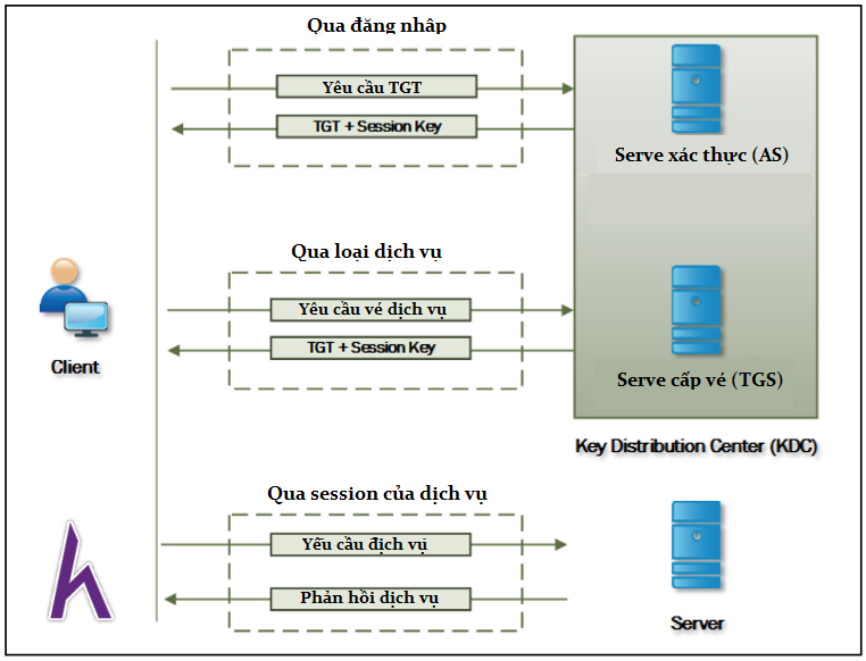

Figure 6-15 Kerberos Authentication Process

Để xác thực, client phải gửi yêu cầu tới server xác thực để được cấp vé **Tick-granting-ticket** (TGT). Serve xác thực client bằng cách so sánh nhân dạng user và mật khẩu với dữ liệu, từ đó gửi đi TGT và một session key. Session key sử dụng cho một session giữa client và serve cấp vé. Bây giờ, client đã được xác thực và có thể giao tiếp với TGS. Client sẽ gửi TGT cho TGS và yêu cầu vé để giao tiếp với các user khác. TGS sẽ tiếp tục gửi vé và session key. Vé và session key sử dụng cho mục đích giao tiếp trong một miền đáng tin cậy.

Password Salting

Password Salting là quá trình thêm kí tự vào mật khẩu để hoạt động một chiều. Các kí tự thêm vào gây khó khăn cho việc đảo ngược hash. Ưu điểm lớn hay chức năng cơ bản của **password salting** là để chống lại **dictionary attack**s và **pre-computed attacks**.

Hãy xem xét ví dụ dưới đây, trong đó một giá trị hash là của mật khẩu không salting và giá trị hash còn lại là mật khẩu trên đã được salting.

> **Không Salting: 23d42f5f3f66498b2c8ff4c20b8c5ac826e47146**
>
> **Salting: 87dd36bc4056720bd4c94e9e2bd165c299446287**

Việc thêm vào mật khẩu nhiều kí tự ngẫu nhiên làm cho nó trở nên phức tạp và khó đảo ngược.

Công cụ bẻ khóa mật khẩu

Có rất nhiều công cụ sẵn có trên internet phục vụ bẻ khóa mật khẩu. Một vài công cụ được liệt kê dưới đây:

- pwdump7
- fgdump
- L0phtCrack
- Ophcrack
- RainbowCrack
- Cain and Abel
- John the Ripper và nhiều công cụ khác.

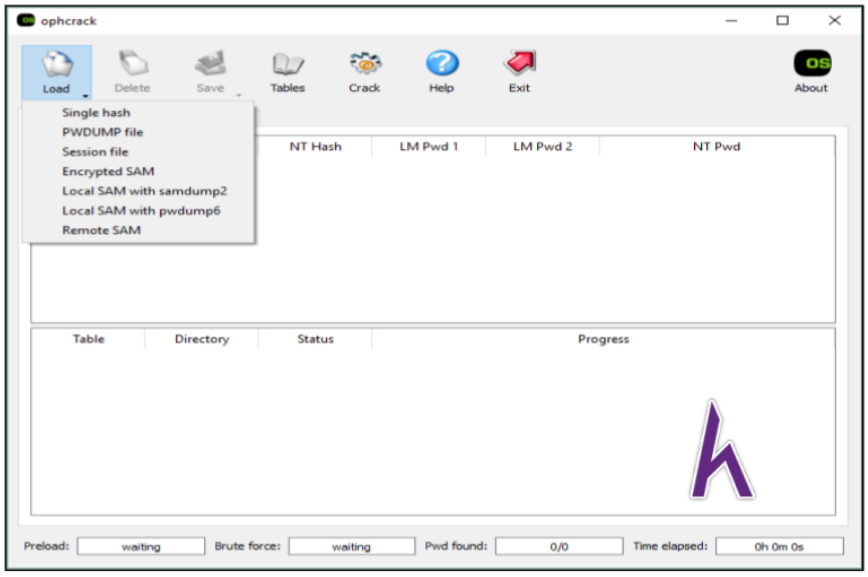

Figure 6-16 Ophcrack Software

Công cụ bẻ khóa mật khẩu dành cho điện thoại

FlexySpy là một trong những công cụ quan sát và thăm dò mạnh nhất dành cho điện thoại. Nó tương thích với các dòng điện thoại Android, iPad, iPhone, Blackberry và Symbian. Để sử dụng, bạn phải cài đặt ứng dụng trên điện thoại. Vào website https://www.flexispy.com để tìm hiểu thêm thông tin.

Sau khi đăng nhập vào **Dashboard**, bạn sẽ thấy mọi mục trong điện thoại của bạn bao gồm tin nhắn, emails, nhật kí cuộc gọi, danh bạ, thu âm, video, thư viện ảnh, vị trí, mật khẩu và các mục khác.

Trong mục **Password**, bạn sẽ nhận được mật khẩu của các tài khoản cùng với tên user và những chi tiết mới nhất.

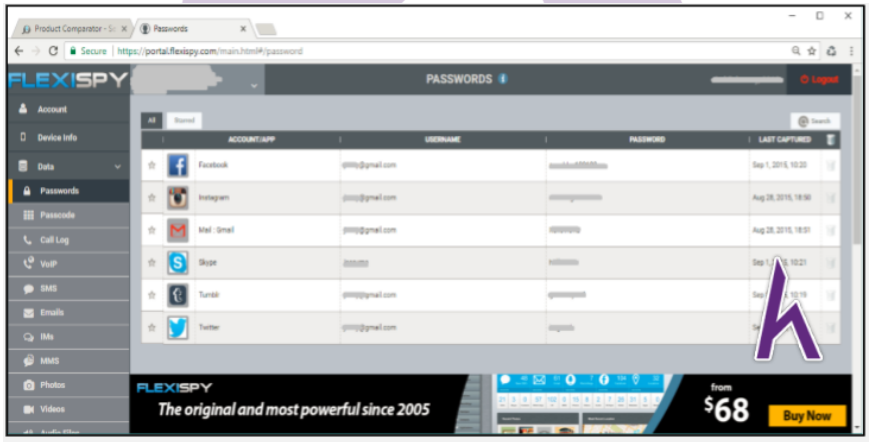

Figure 6-19 FlexySpy

Biện pháp chống lại bẻ khóa mật khẩu