

Bài: 6.2 System Hacking - Lab bẻ khóa mật khẩu sử dụng Pwdump7 & Ophcrack, điều khiển NTFS stream, Steganography

Xem bài học trên website để ủng hộ Kteam: [6.2 System Hacking - Lab bẻ khóa mật khẩu sử dụng Pwdump7 & Ophcrack, điều khiển NTFS stream, Steganography](#).

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!

Lab 6-3: Bẻ khóa mật khẩu sử dụng Pwdump7 và Ophcrack

Case Study

Trong thực nghiệm này, chúng ta sử dụng Windows 7 và Windows 10 cùng với Pwdump7 và Ophcrack. Đang có rất nhiều user được thiết lập trên nền tảng Windows 7. Sử dụng quyền truy cập quản lý, chúng ta sẽ tiếp cận các hash đã mã hóa và chuyển tiếp chúng đến nền tảng Windows 10 chứa Ophcrack để bẻ khóa mật khẩu.

Quy trình

1. Vào **Windows 7 machine** và chạy **Command Prompt** với đặc quyền quản lý.

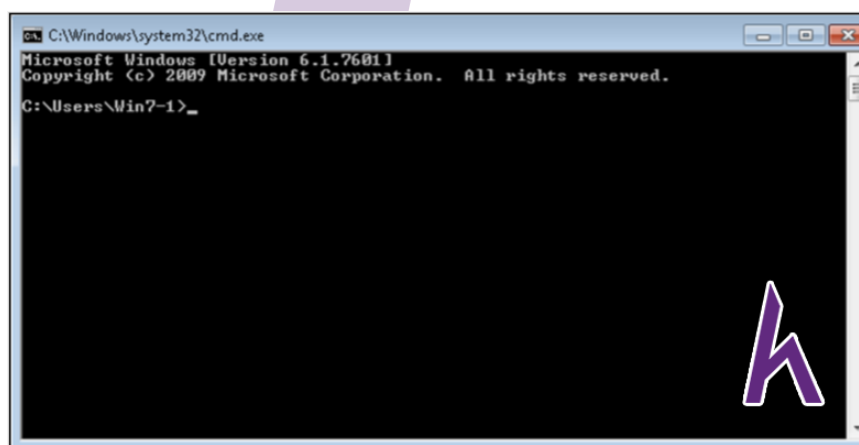
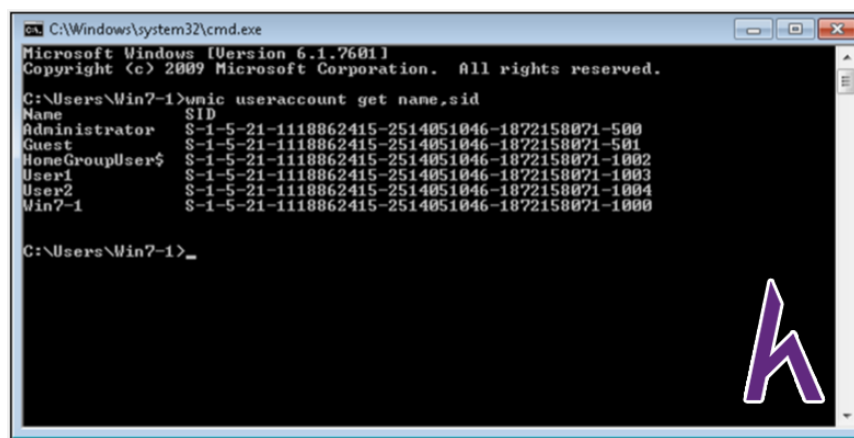


Figure 6-20 Windows Command Line

2. Nhập dòng lệnh sau:

```
C:\Users\Win7-1>wmic useraccount get name,sid
```



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Win7-1>wmic useraccount get name,sid
Name SID
Administrator S-1-5-21-1118862415-2514051046-1872158071-500
Guest S-1-5-21-1118862415-2514051046-1872158071-501
HomeGroupUser$ S-1-5-21-1118862415-2514051046-1872158071-1002
User1 S-1-5-21-1118862415-2514051046-1872158071-1003
User2 S-1-5-21-1118862415-2514051046-1872158071-1004
Win7-1 S-1-5-21-1118862415-2514051046-1872158071-1000

C:\Users\Win7-1>
```

Figure 6-21 Extracting Username and SIDs

Output của dòng lệnh sẽ cho thấy tất cả **tên user** và **mật khẩu hashed** của họ

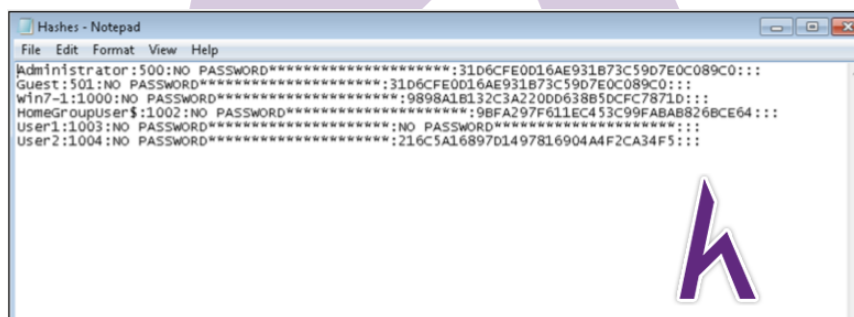
- Đến thư mục chứa pwdump7 và cho chạy ứng dụng. Trong trường hợp chúng tôi thì pwdump7 được đặt ở desktop.

```
C:\Users\Win7-1\Desktop\pwdump7>pwdump7.exe
```

- Copy kết quả vào một tệp văn bản sử dụng lệnh:

```
pwdump7.exe > C:\Users\Win71\Desktop\Hashes.txt
```

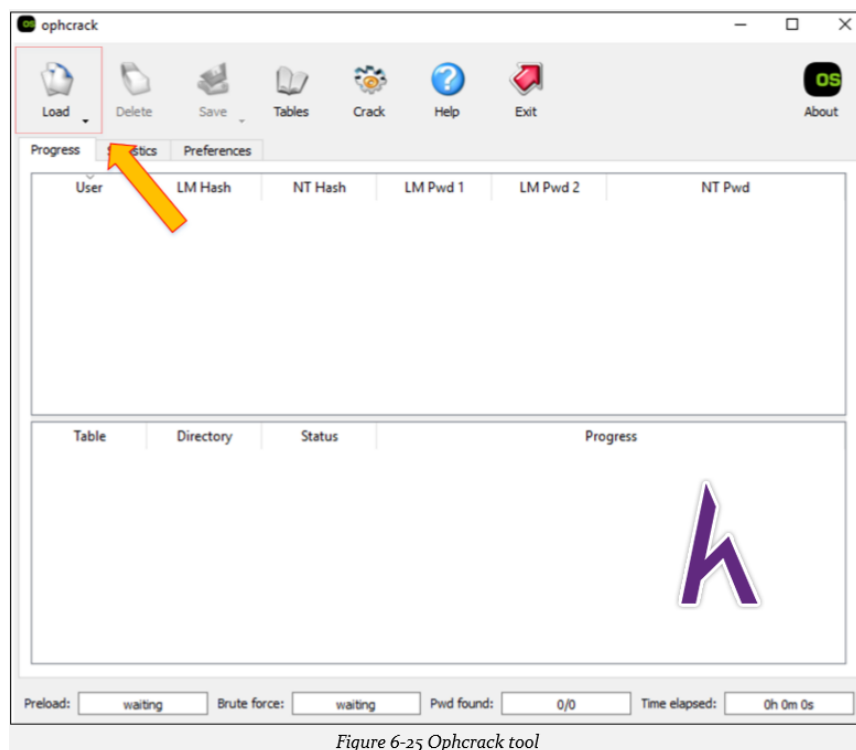
- Kiểm tra tệp **Hashes.txt** ở desktop.



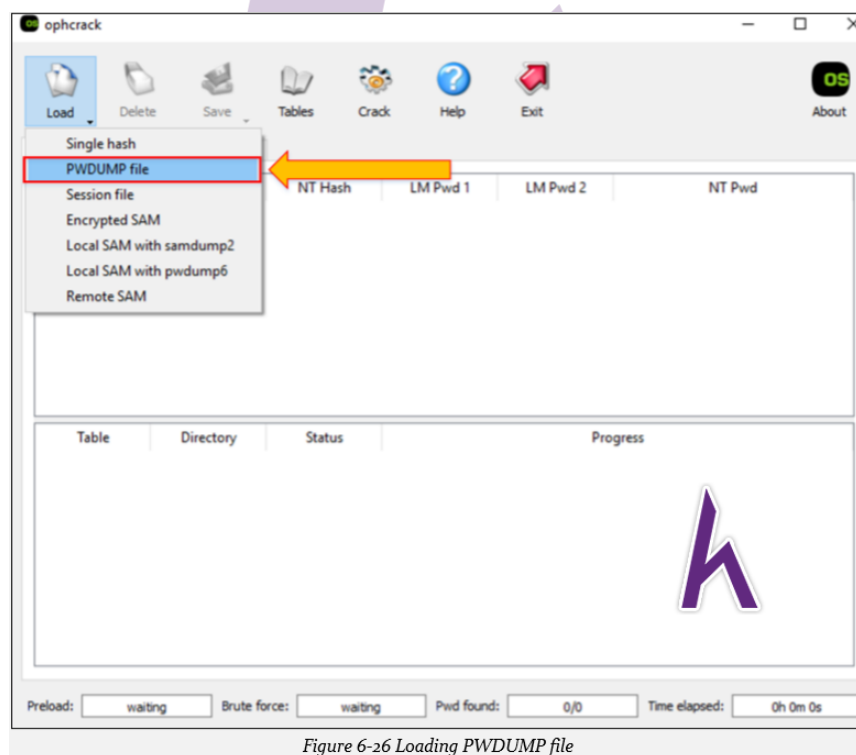
```
Hashes - Notepad
File Edit Format View Help
Administrator:500:NO PASSWORD*****:31D6CFE0D16AE931B73C59D7E0C089C0:::
Guest:501:NO PASSWORD*****:31D6CFE0D16AE931B73C59D7E0C089C0:::
Win7-1:1000:NO PASSWORD*****:9898A1B132C3A2200D638B5DCFC7871D:::
HomeGroupUser$:1002:NO PASSWORD*****:9BFA297F611EC453C99FABAB826BCE64:::
User1:1003:NO PASSWORD*****:NO PASSWORD*****:
User2:1004:NO PASSWORD*****:216C5A16897D1497816904A4F2CA34F5:::
```

Figure 6-24 Extracted hashes in a notepad file

- Chuyển tệp đến một remote machine (Windows 10). Bạn cũng có thể cài đặt Ophrack trên cùng machine.
- Chạy ứng dụng **Ophrack** trên nền tảng Windows 10.



8. Click vào nút **Load**, chọn **PWDUMP File** trong menu thả xuống.



9. **Hashes** đã được tải trong ứng dụng như hình dưới.

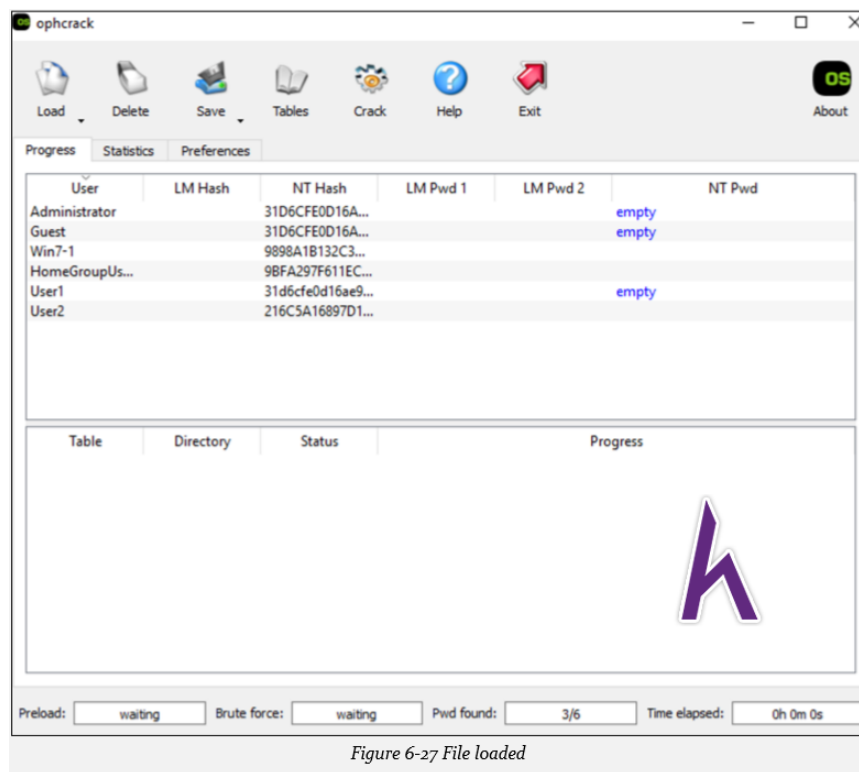


Figure 6-27 File loaded

10. Click vào nút **Table** để tải/chèn bảng.

11. Chọn bảng. Trong trường hợp này, chúng tôi chọn **Vista free table**.

12. Chọn và nhấn **Install**.

13. Chọn vị trí cho folder chứa bảng. Chúng tôi sử dụng bảng mặc định của ứng dụng nên folder ở chung vị trí với ứng dụng.

14. Click **OK**

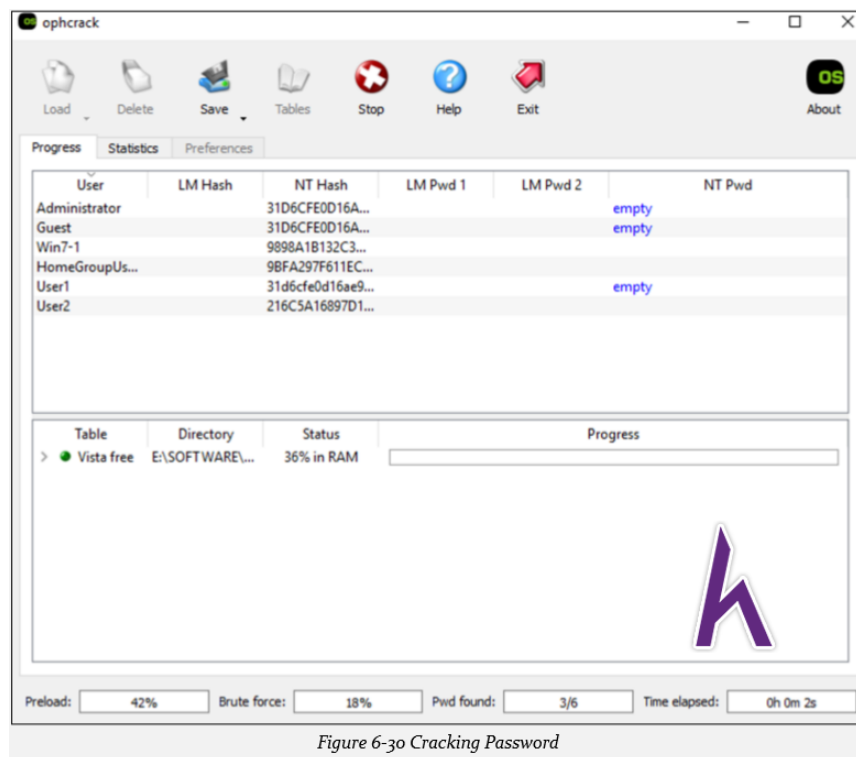


Figure 6-30 Cracking Password

15. Nhấn nút **Crack** để bắt đầu bẻ khóa.

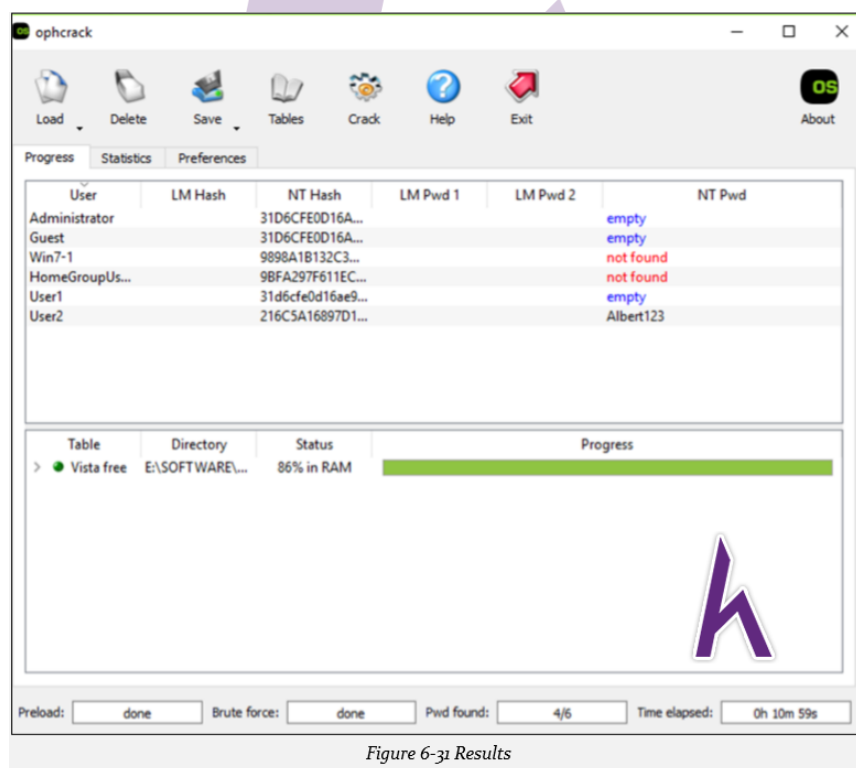


Figure 6-31 Results

- Kết quả cho thấy **user** không thiết lập mật khẩu, user với mật khẩu đã bẻ khóa. Trong kết quả có thể có những mật khẩu chưa được bẻ khóa, bạn có thể thử các bảng khác để bẻ khóa.
- Trong trường hợp của chúng tôi, User2 với mật khẩu **Albert123** đã được bẻ khóa. Bây giờ bạn có thể truy cập Windows 7 Machine bằng User2.

18. Nhập mật khẩu **Albert123** (đã bẻ khóa).

Đăng nhập thành công.

Tăng đặc quyền

Trong mục này, chúng ta sẽ tìm hiểu hành động tiếp theo sau khi truy cập vào mục tiêu. Có khá nhiều nhiệm vụ trong công đoạn này. Không phải lúc nào bạn cũng hack được tài khoản admin, đôi khi bạn chỉ sở hữu tài khoản user ít đặc quyền hơn admin. Sử dụng tài khoản đặc quyền thấp sẽ không giúp bạn hoàn thành mục tiêu. Sau khi truy cập thành công, việc đầu tiên bạn phải làm là tăng đặc quyền để có quyền truy cập cao với ít hoặc hoàn toàn không giới hạn.

Mỗi hệ điều hành có những cài đặt mặc định và tài khoản user như tài khoản administrator, tài khoản root, tài khoản guest, ... với mật khẩu mặc định. Người tấn công có thể dễ dàng tìm thấy lỗ hổng của những tài khoản thiết lập sẵn để khai thác. Những thiết lập và tài khoản mặc định này phải được đảm bảo an toàn và thay đổi để chống lại những truy cập không chính thống.

Tăng đặc quyền được chia thành hai loại:

1. Tăng đặc quyền ngang
2. Tăng đặc quyền dọc

Tăng đặc quyền ngang

Tăng đặc quyền ngang xảy ra khi kẻ tấn công truy cập vào bộ tài nguyên tương tự của một user nhất định.

Hãy xem xét ví dụ sau đây, trong đó hệ điều hành có vô số user bao gồm administrator, user A, user B và các user khác với đặc quyền thấp (chỉ có thể chạy ứng dụng, không thể cài đặt hay gỡ cài đặt bất cứ ứng dụng nào). Mỗi user nhận được bộ đặc quyền giống nhau. Bằng cách tìm ra điểm yếu hay khai thác lỗ hổng, user A sẽ tiếp cận user B và lấy quyền truy cập. Bây giờ user A sẽ có quyền kiểm soát và truy cập tài khoản user B.

Tăng đặc quyền dọc

Trong loại này, kẻ tấn công cố gắng tăng đặc quyền lên cấp cao hơn. **Tăng đặc quyền dọc** xảy ra khi kẻ tấn công lấy quyền truy cập vào tài khoản admin. Đặc quyền cao hơn giúp kẻ tấn công tiếp xúc những thông tin nhạy cảm, cài đặt, chỉnh sửa, xóa tệp và chương trình như virus, trojans, ...

Tăng đặc quyền sử dụng DLL Hijacking

Ứng dụng cần **Dynamic Link Libraries** (DLL) để chạy các tệp có thể thực thi. Trong hệ điều hành Windows, đa số ứng dụng tìm DLL trong các thư mục thay vì sử dụng các con đường đủ tiêu chuẩn. Một khi DLL ác ý được đặt tên giống như DLL chính thống và thay thế trong thư mục, tệp sẽ load DLL ác ý từ thư mục ứng dụng thay vì DLL thực.

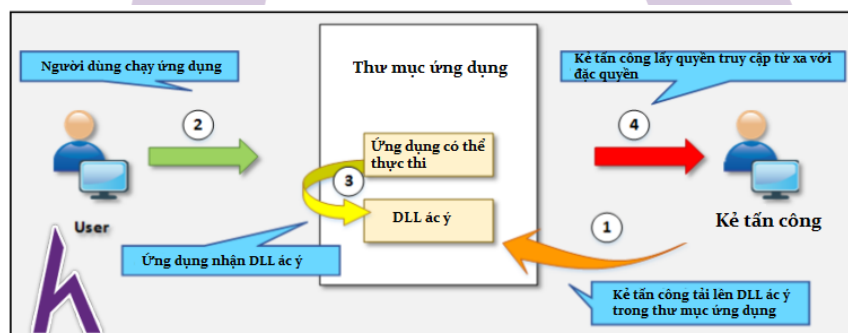
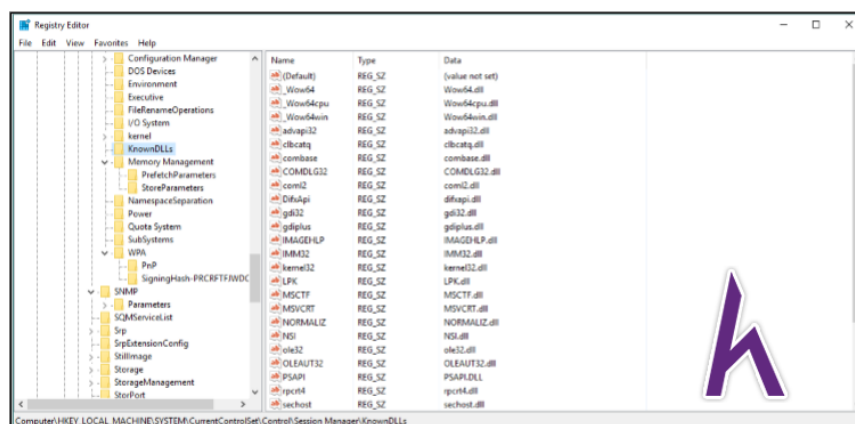


Figure 6-34 Vertical Privilege Escalation

http://HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager



- Thư mục ứng dụng hay thư mục hiện tại
- Thư mục hệ thống, ví dụ: **C:\\Windows\\System32**
- Thư mục Windows

Những dự định cụ thể của kẻ tấn công trong việc chạy ứng dụng ác ý là:

- Cài đặt ứng dụng Malware để thu thập thông tin
- Dừng cửa sau để duy trì truy cập
- Cài đặt Cracker để bẻ khóa mật khẩu và script
- Cài đặt Keylogger để thu thập thông tin từ những thiết bị đầu vào như bàn phím

- Triển khai bộ phần mềm trên hệ thống mục tiêu
- Chạy ứng dụng và script từ xa
- Thực thi ứng dụng theo kế hoạch dựa trên ngày và giờ cụ thể
- Quản lý thiết lập từ xa như chỉnh sửa đăng ký, vô hiệu hóa tài khoản, chỉnh sửa và thao tác trên tệp
- Kiểm soát hệ thống mục tiêu từ xa như tắt máy, chế độ ngủ, thức, khởi động lại hay khóa, ...

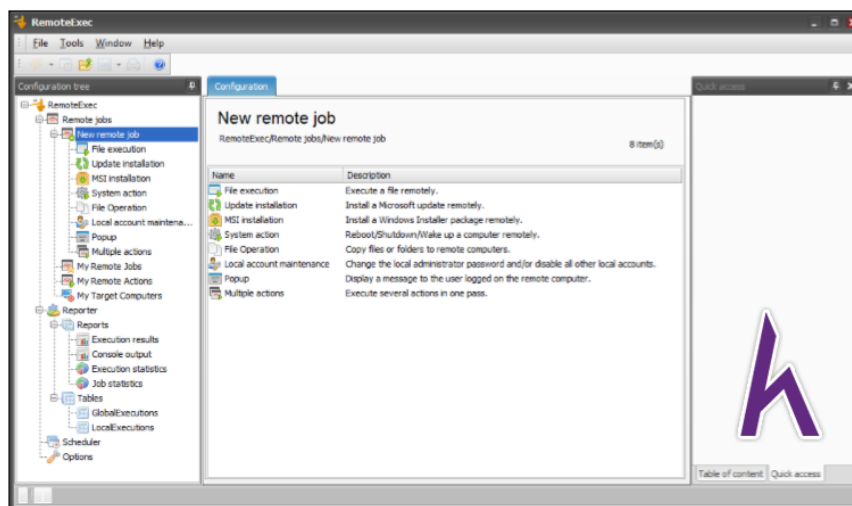


Figure 6-36 RemoteExec Application

PDQ Deploy

PDQ Deploy là một phần mềm sử dụng công cụ admin hệ thống để cài đặt và gửi bản nâng cấp đến hệ thống ở xa một cách âm thầm. **PDQ Deploy** cho phép hay giúp admin cài đặt ứng dụng và phần mềm trên một hệ thống riêng biệt cũng như nhiều hệ thống trong mạng. Phần mềm này có thể bí mật triển khai hầu hết ứng dụng (như .exe hay .msi) đến hệ thống mục tiêu. Sử dụng PDQ Deploy, bạn có thể cài đặt, gỡ cài đặt, copy, chạy và gửi tệp.

Keylogger

Keystroke logging, **Keylogging** và **keyboard capturing** là quá trình sử dụng **Keylogger** quan sát hay quay lại bất cứ hành động nào của user, ví dụ như quan sát user sử dụng bàn phím. Keylogger có thể là phần cứng hoặc phần mềm. Mục đích của việc dùng Keylogger là quan sát dữ liệu được copy vào clipboard, ảnh chụp màn hình, nhật kí màn hình bằng cách chụp màn hình mỗi khi user click.

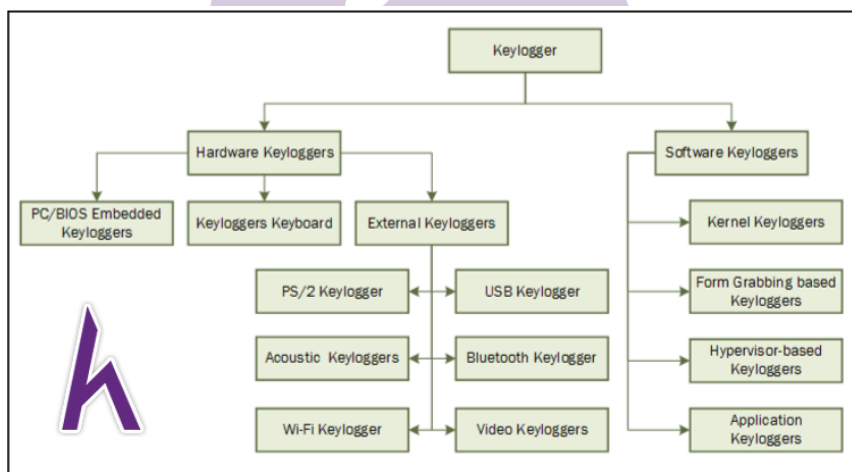


Figure 6-37 Types of Keyloggers

Các loại Keystroke Loggers

Phần mềm keylogger (Software Keylogger)

Phần mềm hoạt động bằng cách ghi lại hoạt động để lấy cắp thông tin từ mục tiêu. **Phần mềm Keylogger** được cài đặt từ xa, hoặc kẻ tấn công sẽ gửi phần mềm cho user và user vô tình thực thi ứng dụng. Phần mềm bao gồm:

- Application Keylogger

- Kernel Keyloggers
- Hypervisor-based Keyloggers
- Form Grabbing based Keyloggers

Phần cứng Keylogger (Hardware Keylogger)

Phần cứng Keylogger thuộc phần cứng hoặc Keylogger cài đặt trên phần cứng bằng cách truy cập vật lí vào thiết bị. **Firmware-based Keyloggers** yêu cầu truy cập vật lí với máy để load phần mềm vào BIOS. Phần cứng bàn phím như key grabber USB là một thiết bị cần được cài đặt song song với bàn phím. Phần cứng Keylogger được chia thành các loại sau:

- PC/BIOS Embedded Keyloggers
- Keyloggers Keyboard
- External Keyloggers

Phần cứng Keylogger

Phần cứng Keylogger	Website
KeyGrabber USB	http://www.keydemon.com/
KeyGrabber PS/2	http://www.keydemon.com/
VideoGhost	http://www.keydemon.com/
KeyGrabber Nano Wi-Fi	http://www.keydemon.com/
KeyGrabber Wi-Fi Premium	http://www.keydemon.com/
KeyGrabber TimeKeeper	http://www.keydemon.com/
KeyGrabber Module	http://www.keydemon.com/
KeyGhost USB Keylogger	http://www.keyghost.com/
KeyCobra Hardware Keylogger (USB and PS2)	http://www.keycobra.com/

Anti-Keyloggers

Anti-Keyloggers là những phần mềm ứng dụng chống lại **keylogging**. Phần mềm này loại bỏ những nguy cơ keylogging bằng việc cung cấp bảo vệ SSL, bảo vệ khỏi keylogging, bảo vệ khỏi **clipboard logging** và chống lại **screen logging**. Một vài phần mềm **Anti-Keylogger** được liệt kê dưới đây:

- Zemana Anti-Keylogger (<https://www.zemana.com>)
- Spyshester Anti-Keylogger software (<https://www.spyshester.com>)
- Anti-Keylogger (<http://anti-keyloggers.com>)

Mindmap



Spyware

Spyware là phần mềm thiết kế để thu thập thông tin user tương tác với một hệ thống ví dụ như địa chỉ email, chứng thư đăng nhập và các chi tiết khác mà không thông báo cho user của hệ thống mục tiêu. Spyware hầu hết được sử dụng để theo dõi tương tác trên mạng của user. Những thông tin thu thập được sẽ gửi đến một địa điểm từ xa. Spyware giấu tệp và quy trình của mình để tránh bị phát hiện. Những loại Spyware thông thường là:

- Adware
- System Monitors
- Tracking Cookies
- Trojans

Chức năng của Spyware

Hiện nay có nhiều công cụ spyware trên internet, cung cấp các chức năng nâng cao như sau:

- Theo dõi user như Keylogging
- Quan sát hoạt động user như việc vào website nào
- Ghi chép cuộc trò chuyện
- Chặn ứng dụng và dịch vụ
- Gửi nhật kí đến những địa chỉ xa
- Theo dõi giao tiếp email
- Ghi chép những phương tiện giao tiếp có thể dời đi như USB
- Thu âm giọng
- Quay video
- Dò địa chỉ
- Theo dõi điện thoại

Giấu tệp

Rootkits

Rootkits là bộ phần mềm cung cấp quyền truy cập đặc quyền với một hệ thống mục tiêu cho một user ở xa. **Rootkits** thường là bộ phần mềm ác ý được kẻ tấn công triển khai sau khi hắn đã dành được quyền truy cập quản lí vào mục tiêu, dùng để duy trì truy cập đặc quyền trong tương lai. Nó tạo ra một cửa sau cho tấn công. **Rootkits** thường nguy hại vì sự tồn tại của nó để tránh bị phát hiện.

Các loại Rootkits

- Rootkits cấp ứng dụng
- Rootkits này điều khiển những tệp ứng dụng tiêu chuẩn, chỉnh sửa hành vi ứng dụng hiện tại bằng việc đưa vào những codes.
- Rootkits cấp Kernel
- Kernel là trung tâm của một hệ điều hành. Rootkits cấp Kernel thêm vào những code ác ý, thay thế chuỗi codes gốc của kernel hệ điều hành.
- Rootkits cấp hardware/ firmware

- Loại rootkits này ẩn nấp ở phần cứng như ổ cứng, card giao tiếp mạng, hệ điều hành BIOS, những nơi không bị kiểm tra tính chính thống. Những rootkits này được gắn vào chipset để phục hồi máy tính đã mất, dữ liệu đã xóa, hoặc làm chúng trở nên vô hiệu. Bên cạnh đó, rootkits có những điều khoản an ninh và bảo mật việc không bị phát hiện.
- Rootkits cấp máy ảo (hypervisor)
- Rootkits này khai thác những chức năng của phần cứng như AMD-V (công nghệ ảo hóa) hay Intel VT, hai chức năng này sẽ biến hệ điều hành thành máy ảo.
- Rootkits cấp bootloader (Bootkits)
- Bootkits sẽ thay thế bootloader gốc với bootloader ác ý, từ đó cho phép Rootkits hoạt động trước khi hệ điều hành hoạt động. Bootkits là nguy cơ nghiêm trọng đối với an ninh hệ thống bởi vì nó có thể làm các startup codes nhiễm độc như Master Boot Record (MBR), Volume Boot Record (VBR) hay boot sector. Bootkits được sử dụng để tấn công hệ thống mã hóa ổ đĩa, hack khóa mã hóa và mật khẩu.

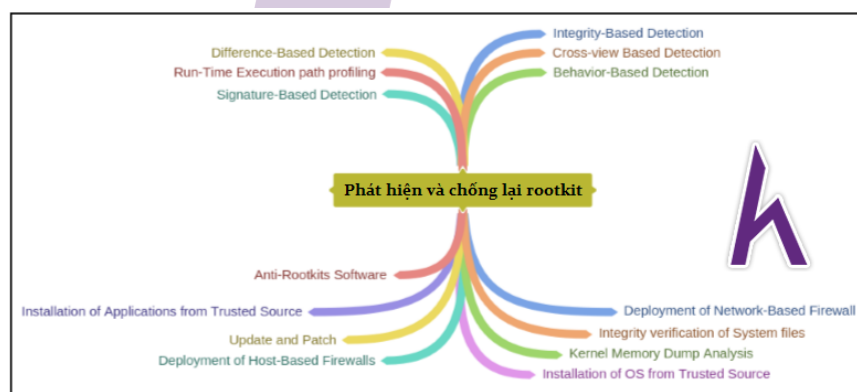
Những công cụ Rootkit

- Avatar
- Necurs
- Azazel
- ZeroAccess

Phát hiện & chống lại Rootkit

Có thể sử dụng nhiều cách tiếp cận để phát hiện Rootkit như phát hiện dựa trên tính chính thống, chữ kí số, phát hiện dựa trên điểm khác biệt, phát hiện hành động, kết xuất bộ nhớ (memory dump). Trên nền tảng Unix, các công cụ phát hiện Rootkit bao gồm Zeppoo, chrootkit và các công cụ khác. Trên nền tảng Windows có **Microsoft Sysinternals RootkitRevealer** và **Avast and Sophos anti-Rootkit**.

Mindmap



NTFS Stream

NTFS là viết tắt của **New Technology File System** (hệ thống tệp công nghệ mới), là một hệ thống tệp độc quyền sản xuất của Windows. NTFS là hệ thống tệp mặc định của Windows NT 3.1. Nó cũng là hệ thống tệp cơ bản của Windows 10, Windows 8, Windows 7, Windows Vista, Windows XP, Windows 2000, và các hệ điều hành Windows NT.

Dòng dữ liệu xen kẽ (ADS)

ADS là một thuộc tính tệp trong NTFS. Đặc tính này của NTFS chứa **metadata** để định vị trí một tệp nhất định. ADS được ra mắt dành cho **Macintosh Hierarchical File System** (HFS). ADS có thể giấu dữ liệu tệp vào một tệp hiện hành mà không gây ra thay đổi nào đáng chú ý. Trong môi trường thực tế, ADS là một nguy cơ đối với hệ thống an ninh bởi vì kẻ tấn công có thể sử dụng ADS để giấu tệp ác ý và thực thi ứng dụng.

Lab 6-4: Điều khiển NTFS stream

Điều khiển NTFS stream

Ở dòng lệnh, nhập " **notepad Testfile.txt** ". Nó sẽ mở ra một notepad với một tệp văn bản mang tên Test.

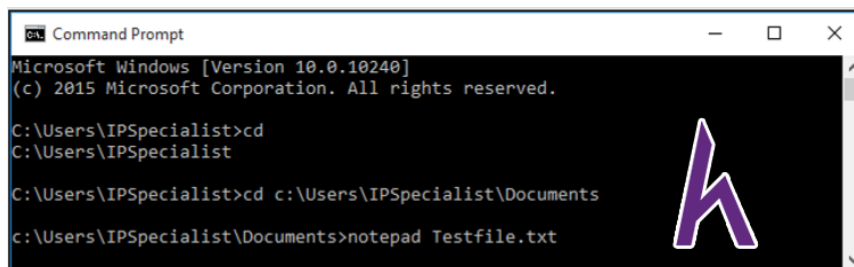


Figure 6-38 Creating Cover File (Text File)

Nhập dữ liệu vào tệp.

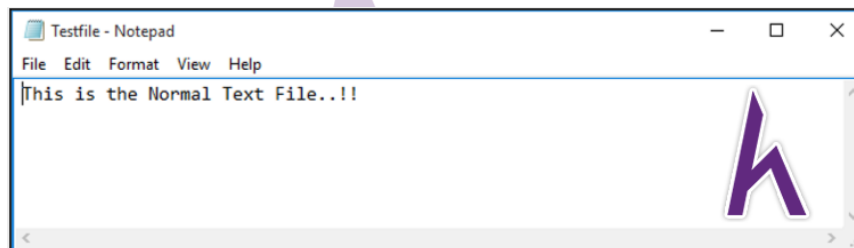


Figure 6-39 Cover File(Text File)

Lưu tệp và đóng Notepad.

Kiểm tra kích thước tệp.

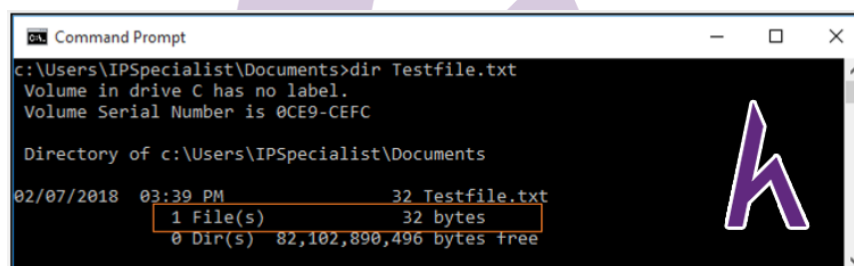


Figure 6-40 Determining File Size

Ở dòng lệnh, nhập " **notepad Testfile.txt:hidden.txt** "

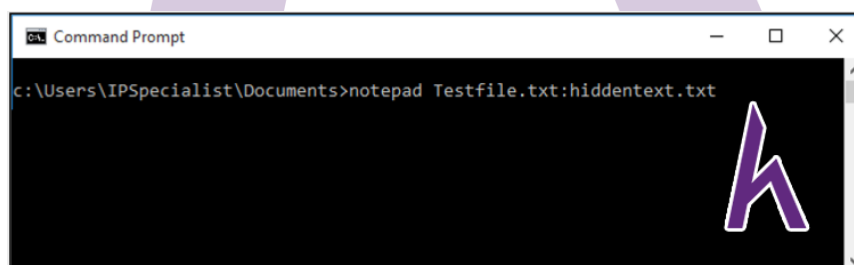


Figure 6-41 Creating Hidden File

Nhập một số đoạn văn bản vào Notepad.

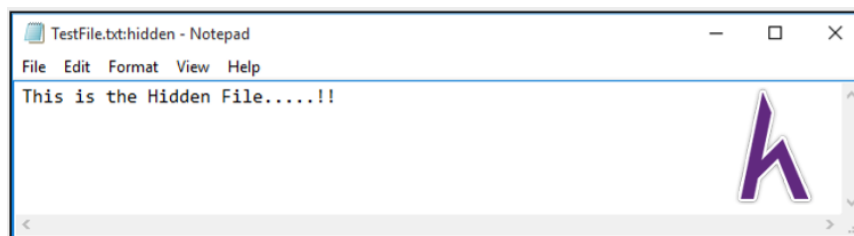


Figure 6-42 Hidden File (ADS)

Lưu tệp và đóng lại.

Kiểm tra kích thước tệp lần nữa (giống với kích thước ban đầu)

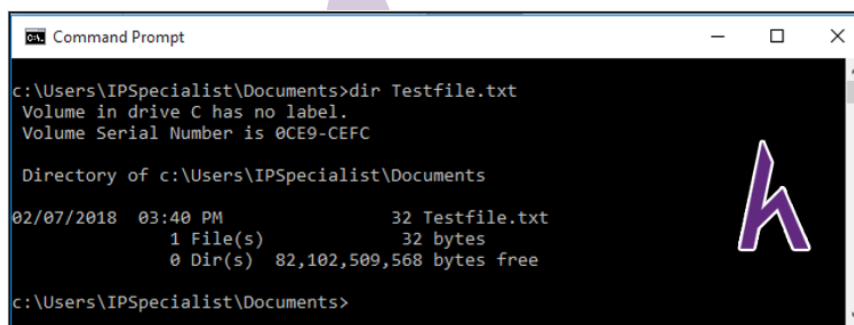


Figure 6-43 Comparing File Size

Mở **Test.txt**. Bạn sẽ chỉ thấy dữ liệu gốc.

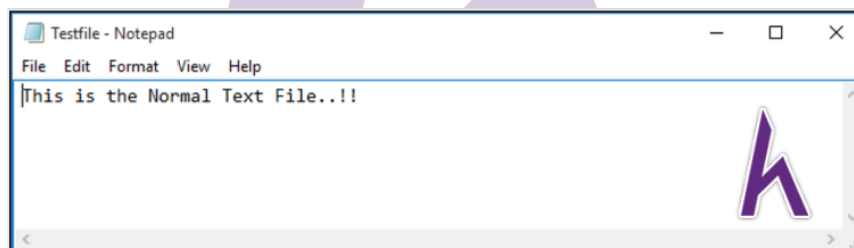


Figure 6-44 Comparing File

Nhập "**type Testfile.txt:hidden.txt**" ở dòng lệnh. Một tin nhắn **syntax error** sẽ xuất hiện.

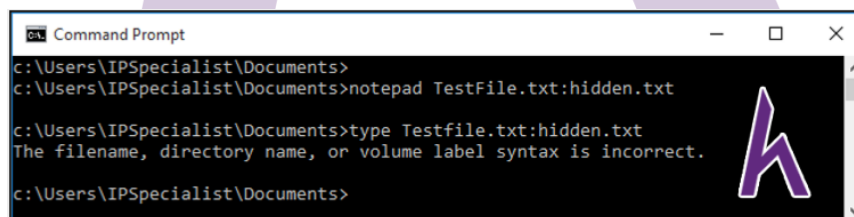


Figure 6-45 Accessing Hidden File

Nếu bạn kiểm tra thư mục, bạn sẽ thấy không có tệp nào được tạo mới.

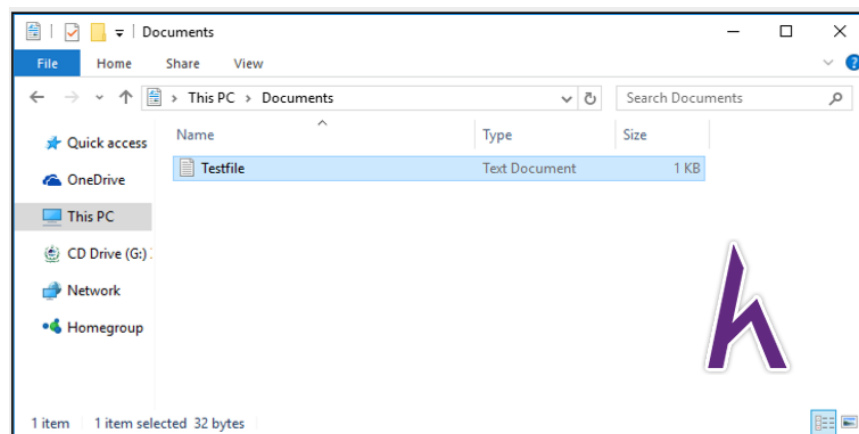


Figure 6-46 File directory

Bây giờ bạn có thể sử dụng tài nguyên như **Makestrm.exe** để trích rút thông tin ẩn từ dòng dữ liệu ADS.

Phát hiện NTFS stream

Bởi vì tệp này không cho thấy bất cứ chỉnh sửa nào nên không thể xác định được đây là tệp thường hay tệp chứa tệp ẩn. Để phát hiện ADS, cần có một công cụ như **ADS Spy**. Mở ứng dụng **ADS Spy** và chọn phương án bạn muốn:

- Quét nhanh
- Quét toàn bộ
- Quét một số folder nhất định

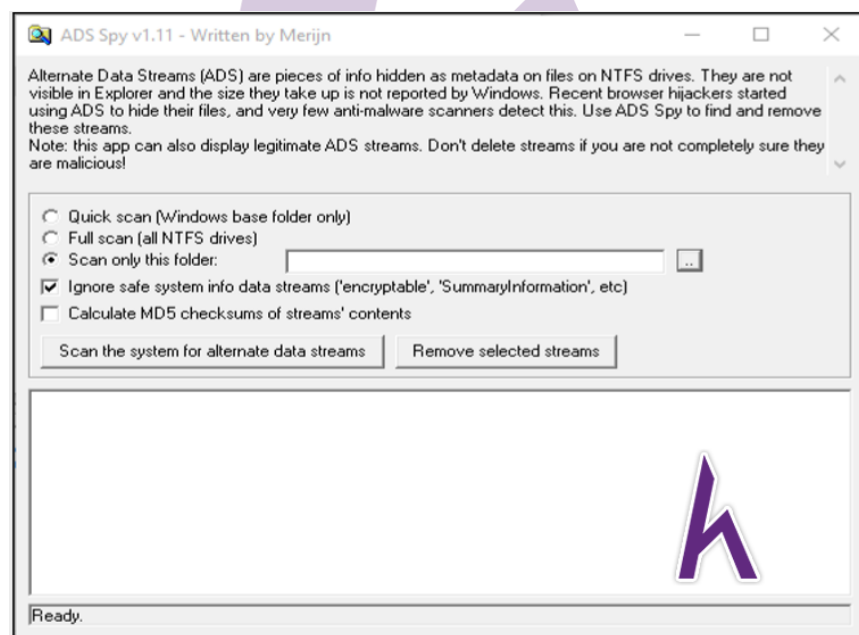


Figure 6-47 ADS Spy Application

Vì chúng ta lưu tệp trong **Document folder**, chọn Document folder để quét.

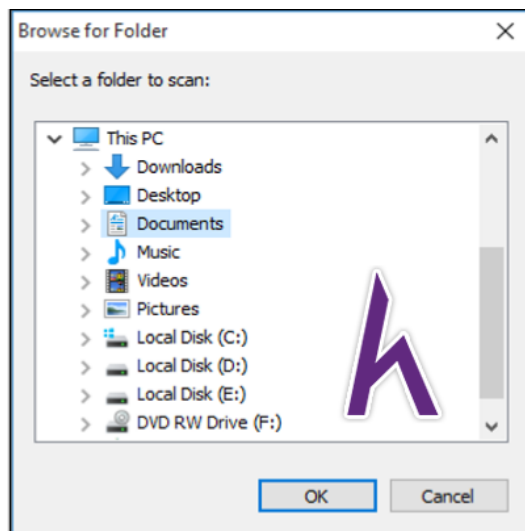


Figure 6-48 Browsing Directory

Chọn một phương án. Nếu bạn muốn quét tìm ADS, chọn "**Scan the system for ADS**" / hoặc chọn nút **removes** để xóa tệp.

Như trong hình dưới đây, ADS Spy đã phát hiện tệp ẩn **Testfile.txt:hidden.txt** từ thư mục.

Đối phó NTFS stream

Sử dụng công cụ và công nghệ từ bên thứ ba có thể chống lại **NTFS stream**. Phương pháp đơn giản nhất để ngăn chặn NTFS là chuyển tệp đáng nghi đến FAT. FAT không hỗ trợ dòng dữ liệu xen kẽ (ADS). Chuyển ADS từ NTFS đến FAT sẽ làm hỏng tệp. Có nhiều công cụ khác như ADS Spy, ADS Tools, LADS, Stream Armor có thể phát hiện và xóa tệp hoàn toàn.

Steganography

Steganography cơ bản là một công nghệ ẩn những thông tin nhạy cảm vào một tin nhắn thông thường để bảo mật. Thông tin ẩn sẽ được người nhận chính thống trích rút ở điểm đến. **Steganography** sử dụng mã hóa để duy trì tính bảo mật và nguyên vẹn. Bên cạnh đó, nó sẽ ẩn những dữ liệu mã hóa để che giấu.

Mục tiêu sử dụng **Steganography** là để che giấu thông tin từ bên thứ ba. Kẻ tấn công dùng công nghệ này để giấu thông tin như tài nguyên codes, kế hoạch, và các thông tin nhạy cảm khác để chuyển tiếp không bị phát hiện.

Phân loại Steganography

Steganography được chia thành hai loại, **Steganography** ngôn ngữ và **Steganography** kỹ thuật. **Steganography** kỹ thuật bao gồm che giấu thông tin sử dụng các phương pháp như mực tàng hình, microdots và các phương pháp khác. **Steganography** ngôn ngữ sử dụng văn bản như phương tiện che giấu thông tin như Ciphers và code.

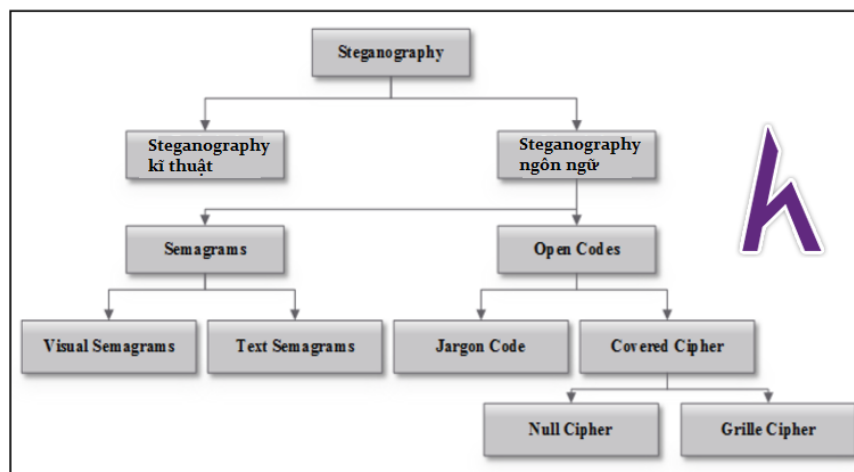


Figure 6-51 Classification of Steganography

Các loại Steganography

Có rất nhiều loại Steganography phổ biến, một số được liệt kê dưới đây:

- Whitespace Steganography
- Image Steganography
- Document Steganography
- Video Steganography
- Audio Steganography
- Folder Steganography
- Spam/Email Steganography

Mindmap

White Space Steganography

White Space Steganography là một phương pháp ẩn thông tin trong một tệp văn bản sử dụng thêm những khoảng trắng giữa những từ. Tin nhắn mật sẽ được thêm dưới dạng khoảng trắng, sử dụng **LZW** và **Huffman compression** sẽ làm giảm kích thước tin nhắn.

Lab 6-5: Steganography

Bài tập

Tạo một tệp văn bản với dữ liệu trong cùng thư mục với **Snow Tool**.



Figure 6-52 Text File (Cover)

Đến **Command Prompt**.

Đổi thư mục để chạy **Snow Tool**.

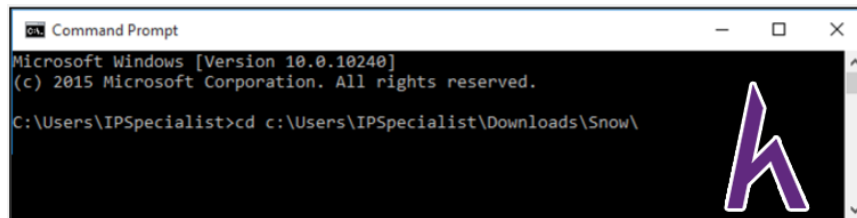


Figure 6-53 Changing Directory

Nhập dòng lệnh **Snow -C -m "text to be hide" -p "password" <Sourcefile> <Destinationfile>**

Tệp nguồn là tệp **Hello.txt** như trên. Tệp đến sẽ là copy của tệp nguồn chứa thông tin đã ẩn.

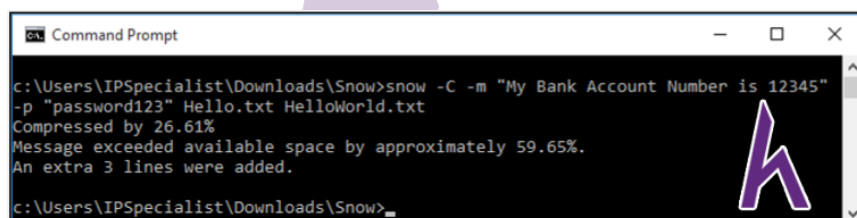


Figure 6-54 White Space Steganography using Snow tool

Đến thư mục, bạn sẽ thấy một tệp mới **HelloWorld.txt**. Mở tệp.

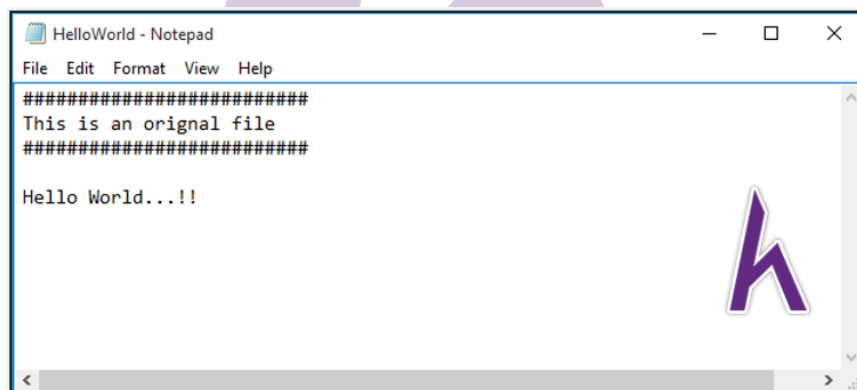


Figure 6-55 File Containing Hidden Encrypted information

Tệp mới chứa văn bản như tệp gốc, không có thông tin ẩn nào. Có thể gửi tệp này cho mục tiêu.

Image Steganography

Trong **Image Steganography**, thông tin ẩn có thể chứa trong các format hình ảnh khác nhau như PNG, JPG, BMP, etc. Phương pháp cơ bản đằng sau **image steganography** là công cụ trong phần mềm này sẽ thay thế những bit thừa của hình ảnh trong tin nhắn. Những thay đổi này không thể được phát hiện bằng mắt thường. Bạn có thể thực hiện **Image Steganography** bằng những kĩ thuật khác nhau như:

- Chèn bit ít đáng kể nhất
- Ngụy trang và lọc
- Thuật toán và biến đổi

Công cụ cho **Image Steganography**:

- OpenStego
- QuickStego

