

# Module 08

## System Hacking

## Windows Hacking

# Windows Hacking

Windows hacking, a subset of System hacking, is the science of testing computers and networks for vulnerabilities and plug-ins.

## ICON KEY



Important Information



Quiz



CPTE Labs



Course Review

## Lab Objectives

The objective of this lab is to help students learn to monitor a system remotely and to extract hidden files and other tasks that include:

- Password cracking
- Password attacks
- Identifying various password cracking tools
- Formulating countermeasures for password cracking
- Escalating privileges
- Executing applications
- Keyloggers and Spywares
- Spyware and keylogger countermeasures
- Hiding files and extracting hidden files
- Understanding rootkits
- The use of Steganography
- Covering tracks
- Monitoring a system remotely

## Lab Scenario

Password hacking is one of the easiest and most common ways hackers obtain unauthorized computer or network access. Although strong passwords that are difficult to crack (or guess) are easy to create and maintain, users often neglect this.

Therefore, passwords are one of the weakest links in the information security chain.

Passwords rely on secrecy. After a password is compromised, its original owner isn't the only person who can access the system with it. Hackers have many ways to obtain passwords. Hackers can obtain passwords from local computers by using password-cracking software. To obtain passwords from across a network, hackers can use remote cracking utilities or network analyzers. This lab demonstrates just how easily hackers can gather password information from your network and describes password vulnerabilities that exist in computer networks along with countermeasures to help prevent these vulnerabilities from being exploited on your systems.

## Lab Environment

This lab requires:

- A computer running Windows 7 as host machine
- Windows Server 2008 running in virtual machine as guest machine
- A web browser with Internet access

## Lab Duration

Time: 100 Minutes

## Overview of Windows Hacking

The goal of system hacking is to gain access, escalate privileges, execute applications, and hide files.

## Lab Tasks

Recommended labs to assist you in Windows Hacking:

- **Lab 1: User System Monitoring and Surveillance Needs Using Spytech SpyAgent**
- **Lab 2: Hiding Files Using NTFS Streams**
- **Lab 3: Find Hidden Files Using ADS Spy**
- **Lab 4: Hiding Files Using the Stealth Files Tool**
- **Lab 5: Extracting SAM Hashes Using Pwdump7 Tool**
- **Lab 6: Creating the Rainbow Tables Using Winrtge**
- **Lab 7: Password Cracking Using RainbowCrack**

# System Monitoring and Surveillance Needs Using Spytech SpyAgent

## Spytech SpyAgent Overview

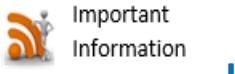
Lab

1

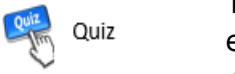
---

### ICON KEY

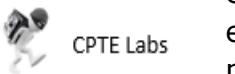
---



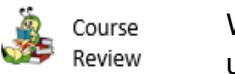
Important Information



Quiz



CPTE Labs



Course Review

SpyAgent also features powerful filtering and access control features, such as Chat Blocking (to restrict access to chat software), Application Blocking (to prevent specific applications from being executed), and Website Filtering.

### Lab Scenario

Today, employees are given access to computer, telephone, and other electronic communication equipment. Email, instant messaging, global positioning systems, telephone systems, and video cameras have given employers new ways to monitor the conduct and performance of their employees. Many employees also are given laptop computer and wireless phones they can take home and use for business outside the workplace.

Whether an employee can claim a reasonable expectation of privacy when using such company-supplied equipment, in large part, depends upon the steps the employer has made to minimize that expectation.

The objective of this lab is to help students use Spytech and the SpyAgent tool.

After completing this lab, students will be able to:

- Install and configure Spytech SpyAgent
- Monitor keystrokes typed, websites visited, and Internet Traffic Data

### Lab Resources

To run this lab, you will need the following:

- SpyTech SpyAgent located at Desktop
- Run this tool on Windows 7
- Administrative privileges to run tools

### Lab Duration

Time: 15 Minutes

## Lab Tasks

1. Navigate to Desktop
2. Double-click **SpyTechSetup.exe**. You will see the following window. Click **Next**.



Figure 1.1 – Installation of Spytech SpyAgent

3. The **Welcome** wizard of the Spytech SpyAgent program appears; read the instructions and click **Next**.

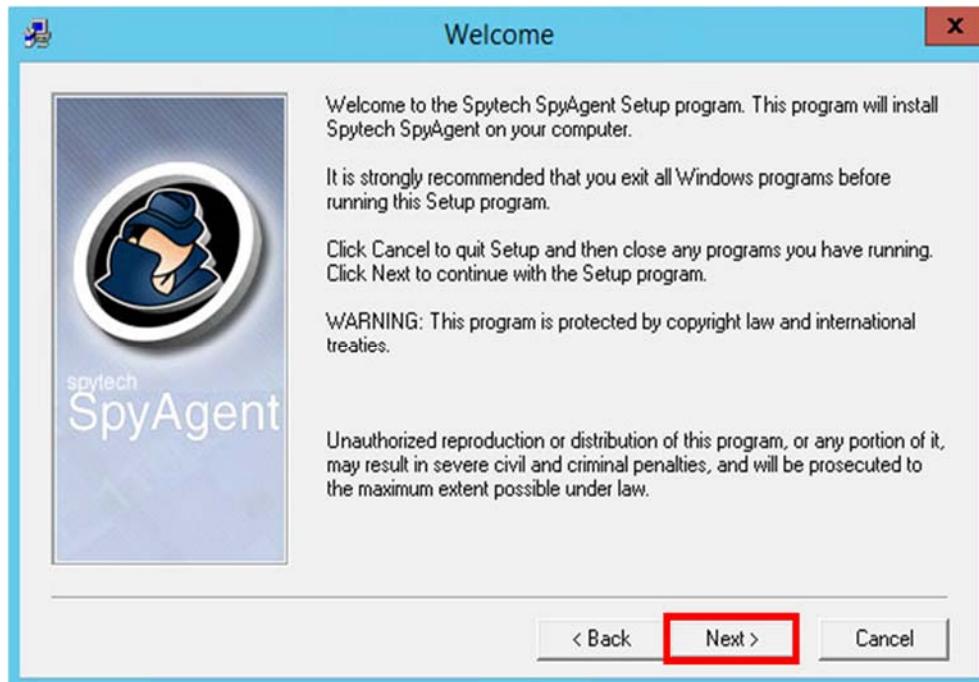


Figure 1.2 – Installation wizard of Spytech SpyAgent

4. The **Important Notes** window appears. Read the note and click **Next**.



Figure 1.3 – Installation wizard

5. The **Software License Agreement** window appears; you must accept the agreement to install Spytech SpyAgent.  
6. Click **Yes** to continue.

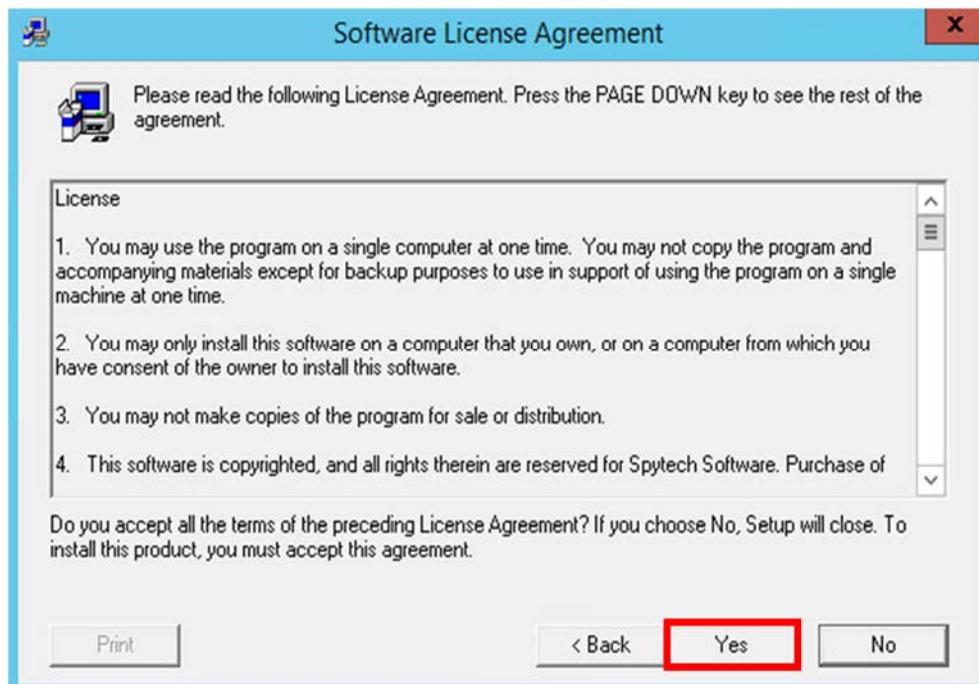


Figure 1.4 – Select the Agreement

**Active Mode:** This option allows SpyAgent to be started in monitoring mode when it is opened -no need for manually starting its monitoring





**Stealth Mode:** This option allows SpyAgent to run in total stealth. Combined with 'Active Mode' the software will load and run in monitoring mode in complete stealth.

7. Choose the **Destination Location** to install Spytech SpyAgent.
8. Click **Next** to continue installation.

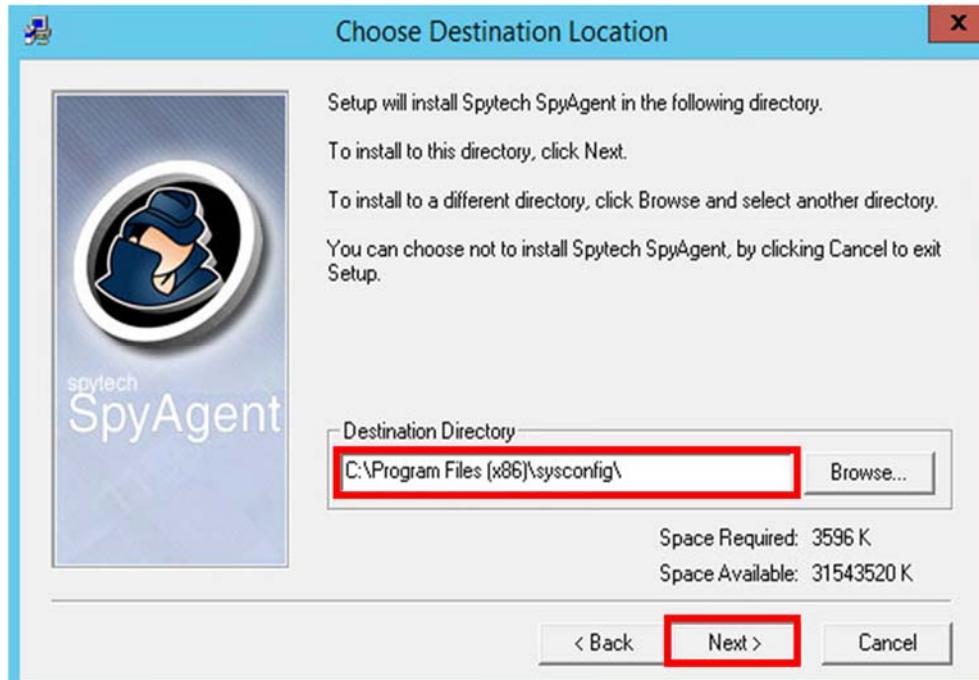


Figure 1.5 – Selecting folder for installation

9. Select SpyAgent installation type, and select **Administrator/Tester** as the setup type.
10. Click **Next**.



Figure 1.6 – Selecting installation type

11. The **Ready to Install** window appears. Click **Next** to start installing Spytech SpyAgent.

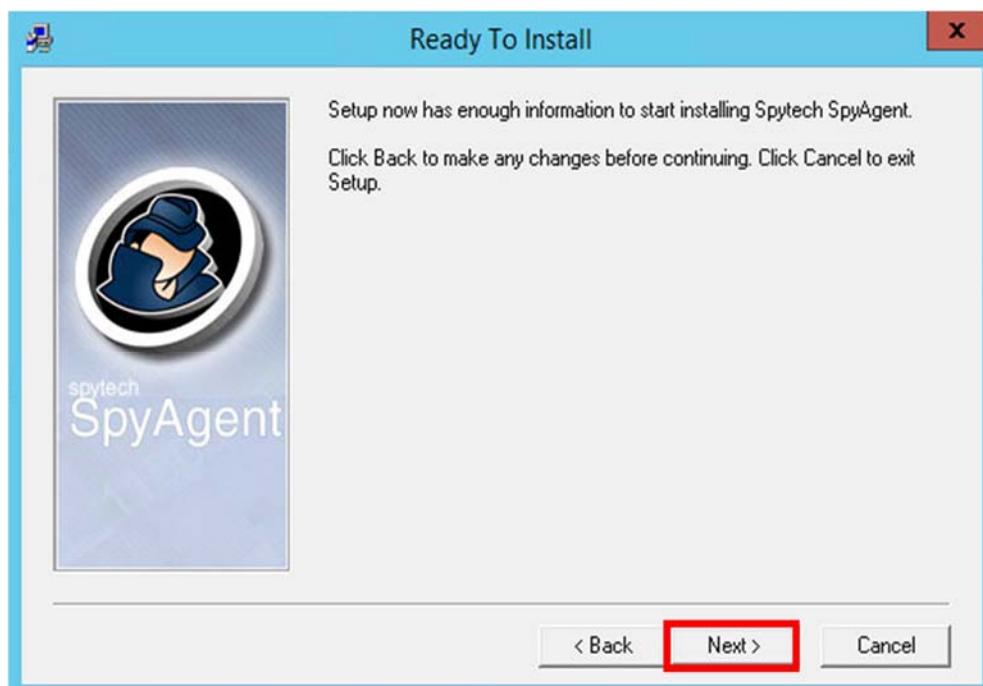


Figure 1.7 – Ready to Install window

12. The prompt will ask: *Would you like to include an uninstaller?* Click **Yes**.

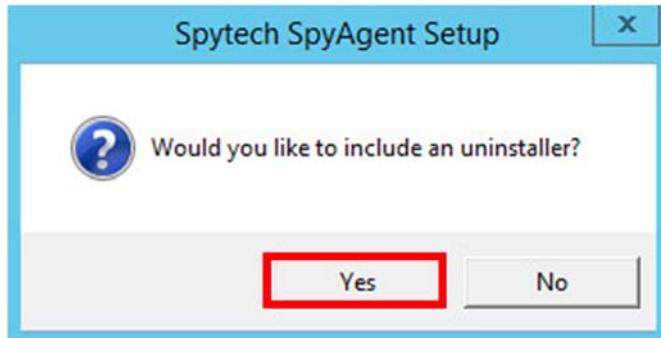


Figure 1.8 – Selecting an uninstaller

13. A **Notice for Antivirus Users** window appears; read the text, click **Next**.



Figure 1.9 – Accept Antivirus notice

14. The **Finished** window appears. Click **Close** to end the setup.

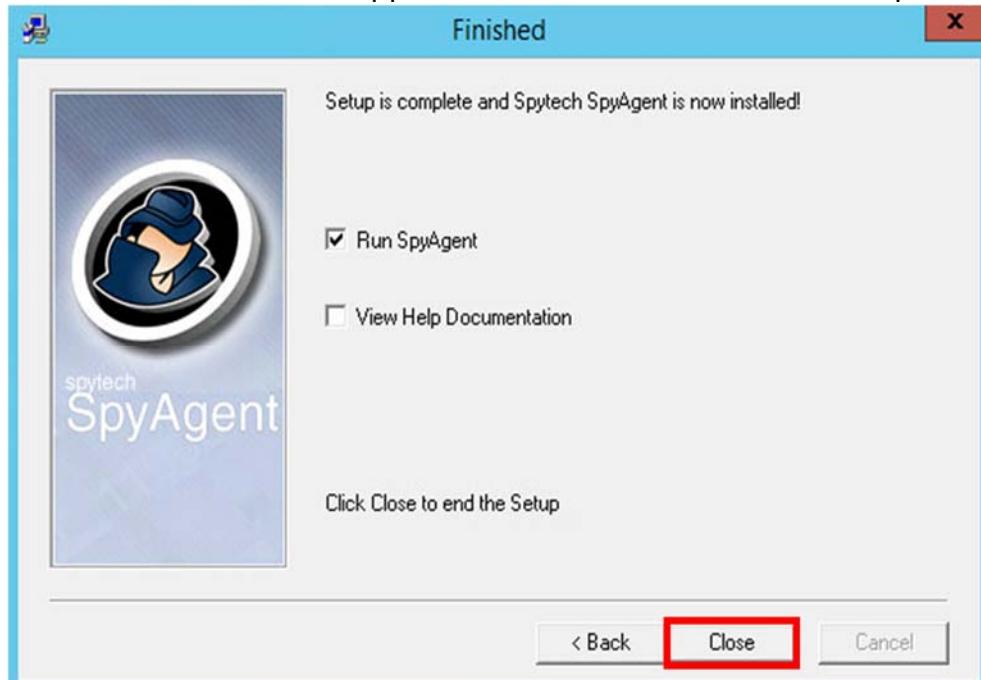


Figure 1.10 – Accept Antivirus notice

15. The following window appears. Click **continue**.



Figure 1.11 – Ordering Info SpyAgent window



Figure 1.12 – Welcome SpyAgent window – Step 1

- 16.The following window appears. Enter the password in **New Password** field, and retype the same password in **Confirm** field.
- 17.Click **OK**.



Figure 1.13 – Selecting New Password

18.The following window appears. Click **click to continue**



Figure 1.14 – Welcome SpyAgent window – Step 2

19.Configuration package wizard appears. Select the **Complete + Stealth Configuration** package.

20.Click **Next**.



Figure 1.15 – Selecting configuration package

21.Choose additional options, and select the **Display Alert on Startup** check box.

22.Click **Next**.



**Internet Traffic**  
 Data: This logs ALL incoming and outgoing internet data transmitted and received by users. All email passwords, FTP passwords, website transmissions, etc. will be logged by this feature



Figure 1.16 – Selecting additional option

23. The **Confirm Settings** wizard appears. To continue click **Next**.



SpyAgent has the unique ability to allow you to have its activity logs delivered to your personal e-mail address or FTP account

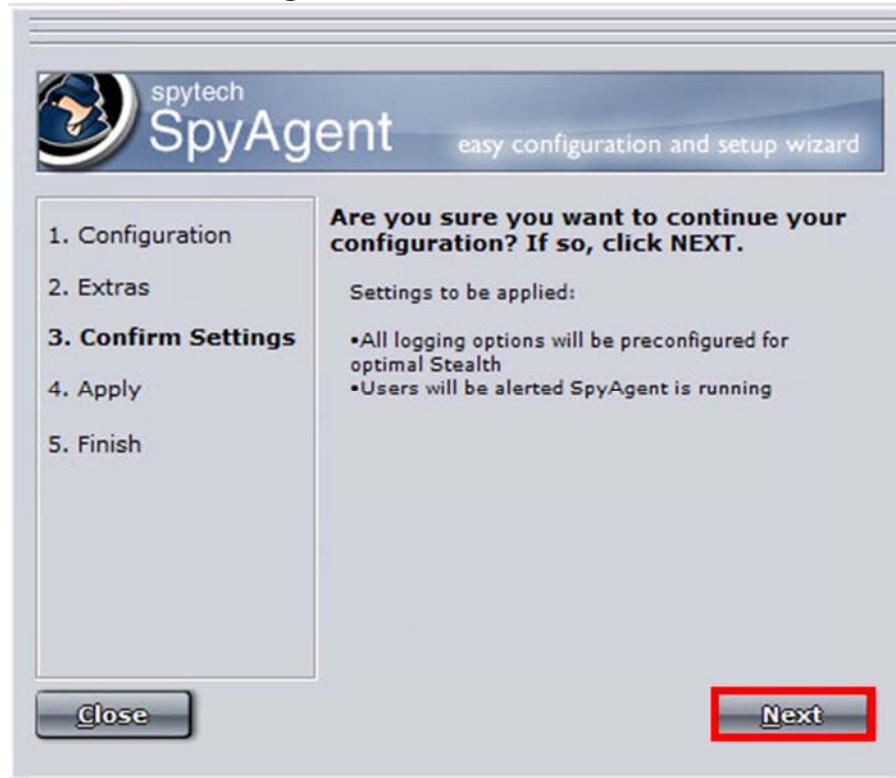


Figure 1.17 – Confirm setting wizard

24.The **Configurations Applied** window appears. Click **Next**.



Figure 1.18 –Configuration applied window

25.The **Configuration Finished** window appears. Click **Finish** to successfully set up SpyAgent.



Figure 1.19 –Configuration finished window

  
SpyAgent has a built in scheduling feature that allows you to configure SpyAgent to log user activities during specific hours of the day, or to lock down your computer at certain times.

26.The main window of Spytech SpyAgent appears, as shown in the following figure. Click **Click to continue...**

27.To check the general user activities, click **Start Monitoring**.



**Task 2**

### Monitoring User Activities



SpyAgent has a feature called SmartLogging that lets you trigger monitoring when certain events arise, instead of constantly logging everything that users do. SmartLogging ties into the keystrokes, websites visited, applications ran, and windows used logging functions.



Figure 1.18 – Start Monitoring

28. When the **Enter Access Password** window appears, enter the **password**.
29. Click **OK**.
30. When the Stealth Notice window appears, read the instructions, click **OK**  
NOTE: To bring SpyAgent out of stealth mode, press **CONTROL+SHIFT+ALT+M** on your keyboard.
31. To check user keystrokes from the keyboard, click **Keyboard & Mouse**, then **View Keystrokes log**.
32. It will show all the resulting keystrokes as shown in the following screenshot.

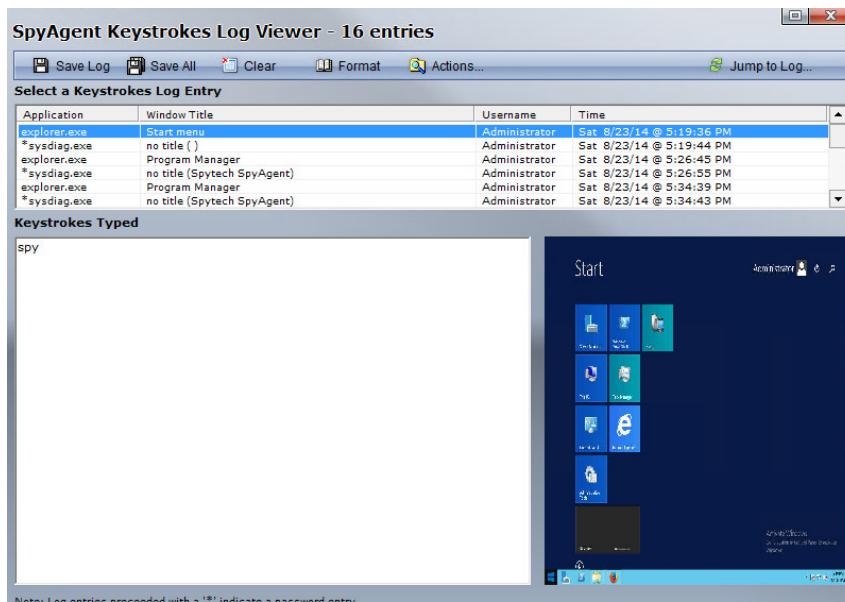
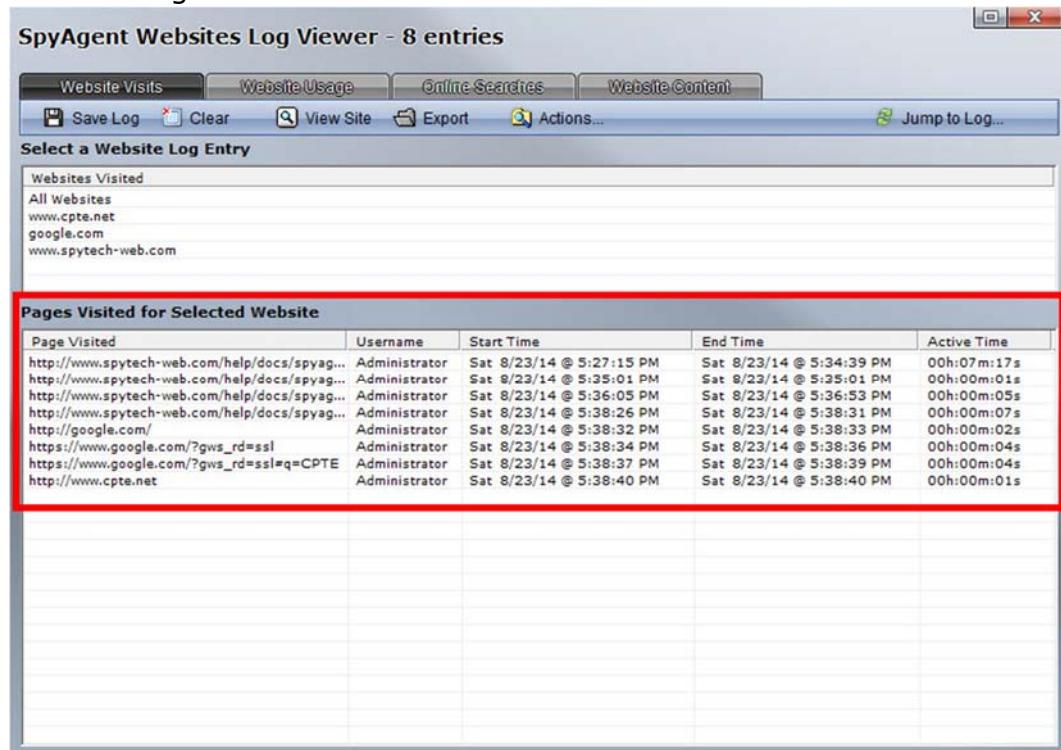


Figure 1.19 – Resulted Keystrokes

33. To check the websites visited by the user, click **Website Usage**, then click **View Websites Logged**.

34. It will show all the user visited website results, as shown in the following screenshot.



The screenshot shows the SpyAgent Websites Log Viewer interface. At the top, there are tabs for Website Visits, Website Usage, Online Searches, and Website Content. The Website Usage tab is selected. Below the tabs is a toolbar with Save Log, Clear, View Site, Export, Actions..., and Jump to Log... buttons. A sub-menu titled 'Select a Website Log Entry' is open, showing options like 'Websites Visited' and 'All Websites'. The main area displays a table titled 'Pages Visited for Selected Website' with the following data:

Page Visited	Username	Start Time	End Time	Active Time
http://www.spytech-web.com/help/docs/spyag...	Administrator	Sat 8/23/14 @ 5:27:15 PM	Sat 8/23/14 @ 5:34:39 PM	00:07m:17s
http://www.spytech-web.com/help/docs/spyag...	Administrator	Sat 8/23/14 @ 5:35:01 PM	Sat 8/23/14 @ 5:35:01 PM	00:00m:01s
http://www.spytech-web.com/help/docs/spyag...	Administrator	Sat 8/23/14 @ 5:36:05 PM	Sat 8/23/14 @ 5:36:53 PM	00:00m:08s
http://www.spytech-web.com/help/docs/spyag...	Administrator	Sat 8/23/14 @ 5:38:26 PM	Sat 8/23/14 @ 5:38:31 PM	00:00m:07s
http://google.com/	Administrator	Sat 8/23/14 @ 5:38:32 PM	Sat 8/23/14 @ 5:38:33 PM	00:00m:02s
https://www.google.com/?gws_rd=ssl	Administrator	Sat 8/23/14 @ 5:38:34 PM	Sat 8/23/14 @ 5:38:36 PM	00:00m:04s
https://www.google.com/?gws_rd=ssl&q=CPTE	Administrator	Sat 8/23/14 @ 5:38:37 PM	Sat 8/23/14 @ 5:38:39 PM	00:00m:04s
http://www.cpte.net	Administrator	Sat 8/23/14 @ 5:38:40 PM	Sat 8/23/14 @ 5:38:40 PM	00:00m:01s

Figure 1.19 – Resulted of visited websites

## Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

Tool/Utility	Information Collected/Objectives Achieved
<b>Spytech SpyAgent</b>	<p>Output:</p> <ul style="list-style-type: none"> <li>Monitoring keystrokes typed</li> <li>Website log entries</li> <li>Pages visited for selected website</li> <li>Internet traffic data</li> </ul>

## Hiding Files Using NTFS Streams

**Lab**

**2**

### NTFS Streams Overview

Alternate Data Streams (ADS) have been around since the introduction of windows NTFS. They were designed to provide compatibility with the old Hierarchical File System (HFS) from Mac which uses something called resource forks. [<http://www.securityfocus.com/infocus/1822>, [http://en.wikipedia.org/wiki/Alternate\\_Data\\_Streams](http://en.wikipedia.org/wiki/Alternate_Data_Streams)]

Access these sites outside of the lab environment for more information.

Basically, ADS can be used to hide the presence of a secret or malicious file inside the file record of an innocent file. That is, when Windows shows you a file, say "readme.txt", the metadata that tells your system where to get "readme.txt" may also contain information for "EvilSpyware.exe". Thus, malicious files may be on your system and you cannot see them using normal means.

### Lab Scenario

Once the hacker has fully hacked the local system, installed their backdoors and port redirectors, and obtained all the information available to them, they will proceed to hack other systems on the network. Most often there are matching service, administrator, or support accounts residing on each system that make it easy for the attacker to compromise each system in a short amount of time. As each new system is hacked, the attacker performs the steps outlined above to gather additional system and password information. Attackers continue to leverage information on each system until they identify passwords for accounts that reside on highly prized systems including payroll, root domain controllers, and web servers. In order to be an expert ethical hacker and penetration tester, you must understand how to hide files using NTFS streams.

The objective of this lab is to help students learn how to hide files using NTFS streams.

It will teach you how to:

- Use NTFS streams
- Hide files

### Lab Resources

To run this lab, you will need the following:

- A computer running on Windows 7 Virtual Machine
- NTFS drive
- Administrative privileges to run tools

### Lab Duration

Time: 15 Minutes

## Lab Tasks



### Task 1

#### NTFS Stereams



NTFS (New Technology File System) is the standard file system of Windows.

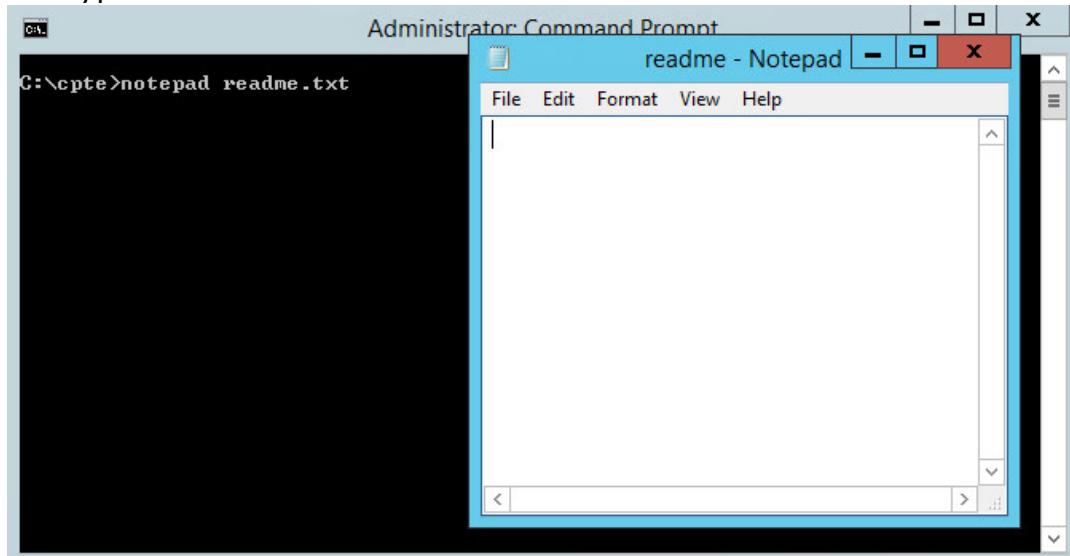


Figure 3.1 – Command prompt with “notepad readme.txt”

6. Note the file **size** of the **readme.txt** by typing **dir** in the command prompt.
7. Now hide **calc.exe** inside the **readme.txt** by typing the following in the command prompt:

```
type c:\cpte\calc.exe > c:\cpte\readme.txt:calc.exe
```

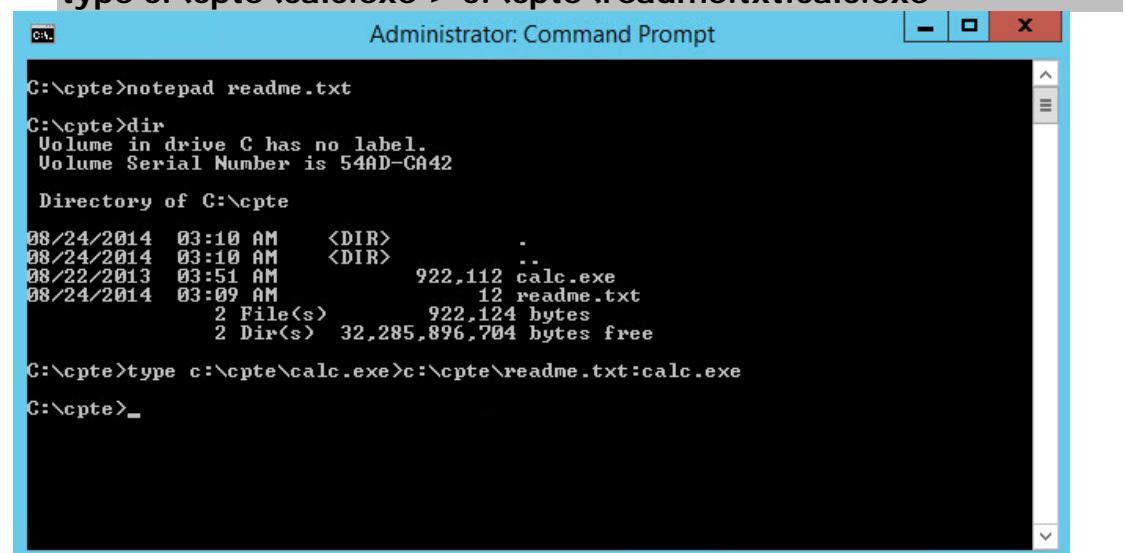


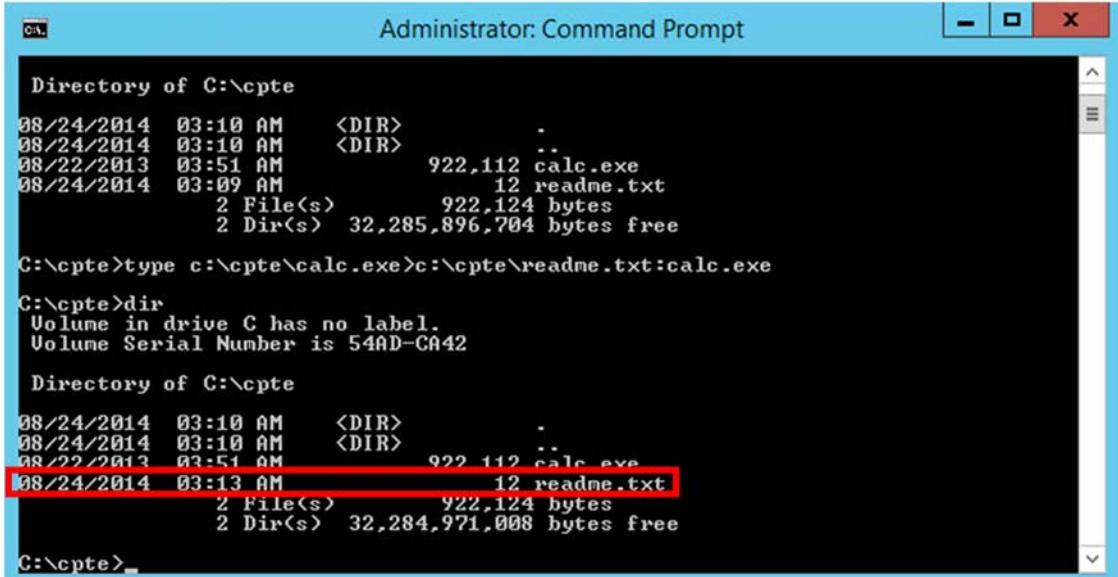
Figure 3.2 – Command prompt with hiding calc.exe

A stream consists of data associated with a main file or directory (known as the main unnamed stream).

8. Type **dir** in the command prompt and note the file size of **readme.txt**.



NTFS (New Technology File System) is the standard file system of Windows.



```

Administrator: Command Prompt

Directory of C:\cpte
08/24/2014  03:10 AM      <DIR>    .
08/24/2014  03:10 AM      <DIR>    ..
08/22/2013  03:51 AM          922,112 calc.exe
08/24/2014  03:09 AM          12 readme.txt
              2 File(s)       922,124 bytes
              2 Dir(s)   32,285,896,704 bytes free

C:\cpte>type c:\cpte\calc.exe>c:\cpte\readme.txt:calc.exe

C:\cpte>dir
Volume in drive C has no label.
Volume Serial Number is 54AD-CA42

Directory of C:\cpte
08/24/2014  03:10 AM      <DIR>    .
08/24/2014  03:10 AM      <DIR>    ..
08/22/2013  03:51 AM          922,112 calc.exe
08/24/2014  03:13 AM          12 readme.txt
              2 File(s)       922,124 bytes
              2 Dir(s)   32,284,971,008 bytes free

C:\cpte>_

```

Figure 3.3 – Command prompt with executing hidden calc.exe command

9. The file **size** of the **readme.txt** **should not change**. Now navigate to the directory **c:\cpte** and **delete calc.exe**.

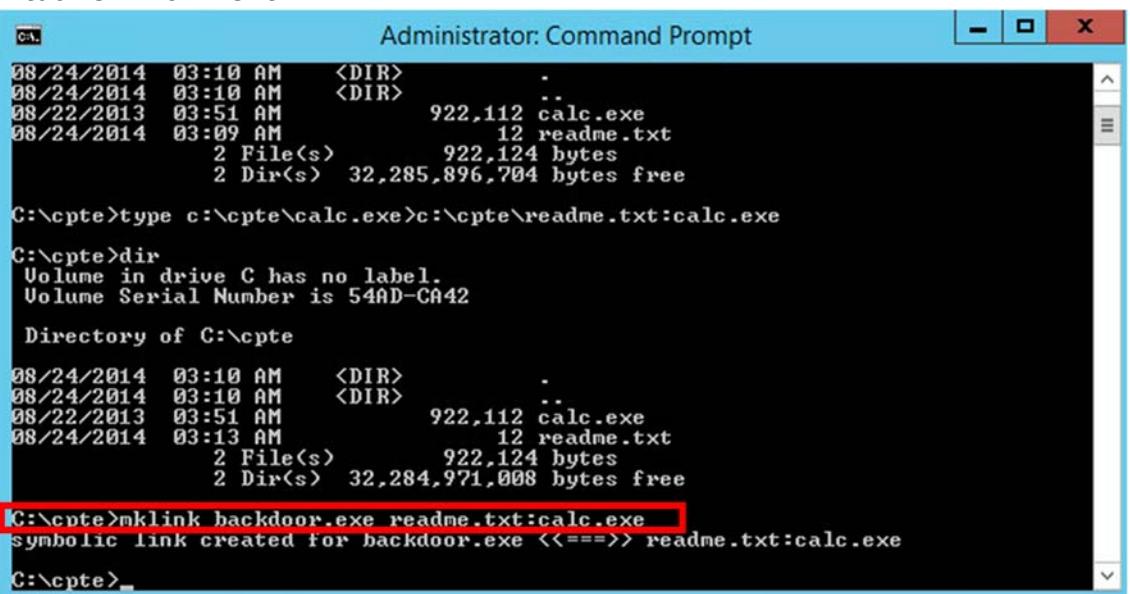
10. Return to the command prompt and type command:

**mklink backdoor.exe readme.txt:calc.exe and press Enter**

Note: outside of this lab environment you would now be able to type backdoor.exe to open calculator. Unfortunately this part doesn't work in the virtual environment.



NTFS supersedes the FAT file system as the preferred file system for Microsoft's Windows operating systems.



```

Administrator: Command Prompt

08/24/2014  03:10 AM      <DIR>    .
08/24/2014  03:10 AM      <DIR>    ..
08/22/2013  03:51 AM          922,112 calc.exe
08/24/2014  03:09 AM          12 readme.txt
              2 File(s)       922,124 bytes
              2 Dir(s)   32,285,896,704 bytes free

C:\cpte>type c:\cpte\calc.exe>c:\cpte\readme.txt:calc.exe

C:\cpte>dir
Volume in drive C has no label.
Volume Serial Number is 54AD-CA42

Directory of C:\cpte
08/24/2014  03:10 AM      <DIR>    .
08/24/2014  03:10 AM      <DIR>    ..
08/22/2013  03:51 AM          922,112 calc.exe
08/24/2014  03:13 AM          12 readme.txt
              2 File(s)       922,124 bytes
              2 Dir(s)   32,284,971,008 bytes free

C:\cpte>mklink backdoor.exe readme.txt:calc.exe
symbolic link created for backdoor.exe <>> readme.txt:calc.exe

C:\cpte>_

```

Figure 3.4 – Command prompt linking the hidden calc.exe

If the **mklink** fails, another option is:

**start .\readme.txt:calc.exe or start \cpte\readme.txt:calc.exe**

FYI, typing in **backdoor.exe** starts the calc.exe program on physical devices yet this typically fails on virtual machine systems.



A stream is a hidden file that is linked to a normal (visible) file.

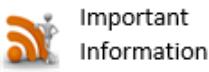
## Lab Analysis

Document all the results discovered during the lab.

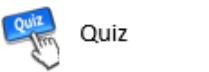
Tool/Utility	Information Collected/Objectives Achieved
<b>NTFS Streams</b>	<b>Output:</b> Calculator (calc.exe) file executed

## Quiz

1. Evaluate alternative methods to hide the other exe files (like calc.exe).
2. Does ADS (Alternate Data Streams) lose hidden streams when copied across the network?
3. Can \*Nix handle NTFS ADS data streams?
4. Enumerate Alternate Data Streams with LADS tool.

**Lab****3****ICON KEY**

Important Information



Quiz



CPTE Labs



Course Review

# Find Hidden Files Using ADS Spy

## ADS Spy Overview

**ADS Spy:** A small tool to list, view or delete Alternate Data Streams (ADS) on Windows systems with NTFS file systems. ADS are a way of storing meta-information about files, without actually storing the information in the file it belongs to, carried over from early MacOS compatibility from Windows NT4. This meta-information is not visible in Windows Explorer.

Recently, browser hijackers began using this technique to store hidden information on the system, and even store Trojan executable files in ADS streams of random files on the system. Use with caution, Windows and several antivirus programs also store (temporary) information in ADS.

## Lab Scenario

Hackers have many ways to obtain passwords. Hackers can obtain passwords from local computers by using password-cracking software. To obtain passwords from across a network, hackers can use remote cracking utilities or network analyzers. This chapter demonstrates just how easily hackers can gather password information from your network and describes password vulnerabilities that exist in computer networks and countermeasures to help prevent these vulnerabilities from being exploited on your systems. In order to be an expert penetration tester, you must understand how to find hidden files using ADS Spy.

The objective of this lab is to help students learn how to list, view, or delete Alternate Data Streams and how to use them.

It will teach you how to:

- Use ADS Spy
- Find hidden files

## Lab Resources

To run this lab, you need the following:

- ADS Spy is located at Desktop
- Run this tool in Windows 7

## Lab Duration

Time: 10 Minutes

## Lab Tasks

- Double-click and launch **ADS Spy** from Desktop.

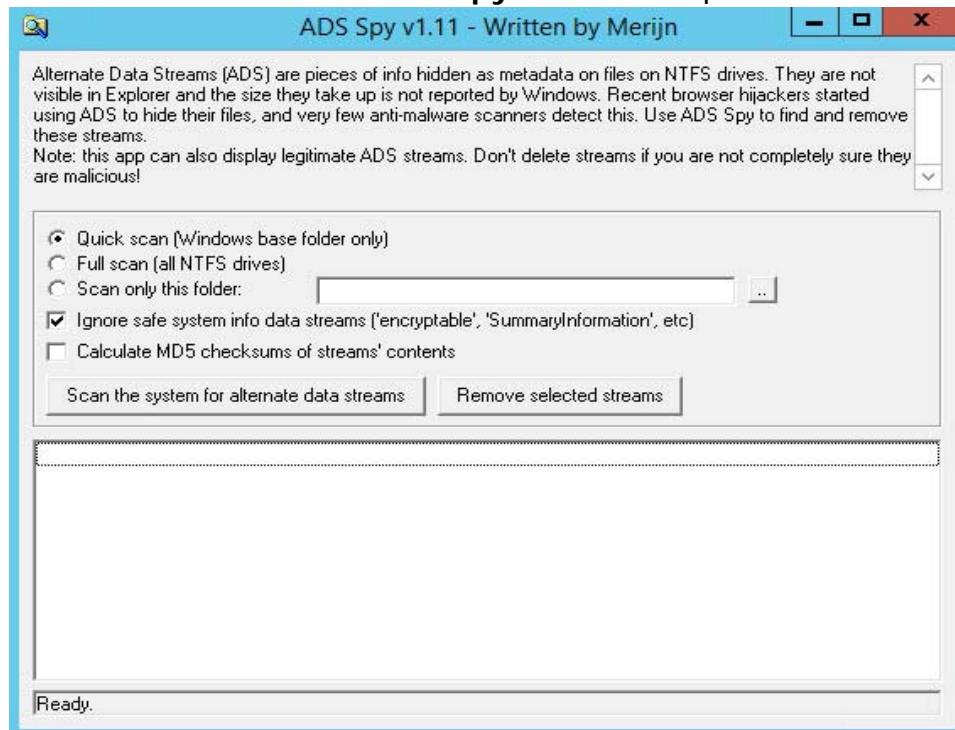
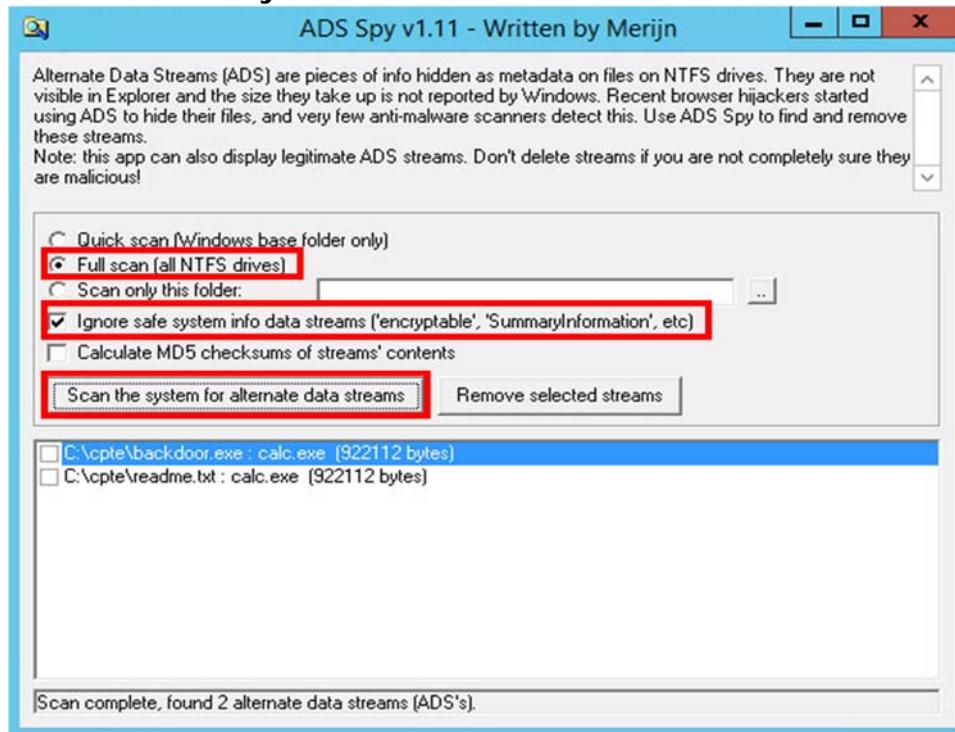


Figure: 4.1- Welcome screen of ADS Spy

- Start an appropriate scan.
- Click **Scan the system for alternate data streams**.



ADS Spy is a small tool to list, view, or delete Alternate Data Streams (ADS) on Windows Operating Systems with NTFS file systems.

- 
- ADS are a way of storing meta-information regarding files, without actually storing the information in the file it belongs to, carried over from early MacOS compatibility**
4. Find the **ADS hidden info file** while you scan the system for alternative data streams
  5. To remove the Alternate Data Streams, click **Remove Selected streams**

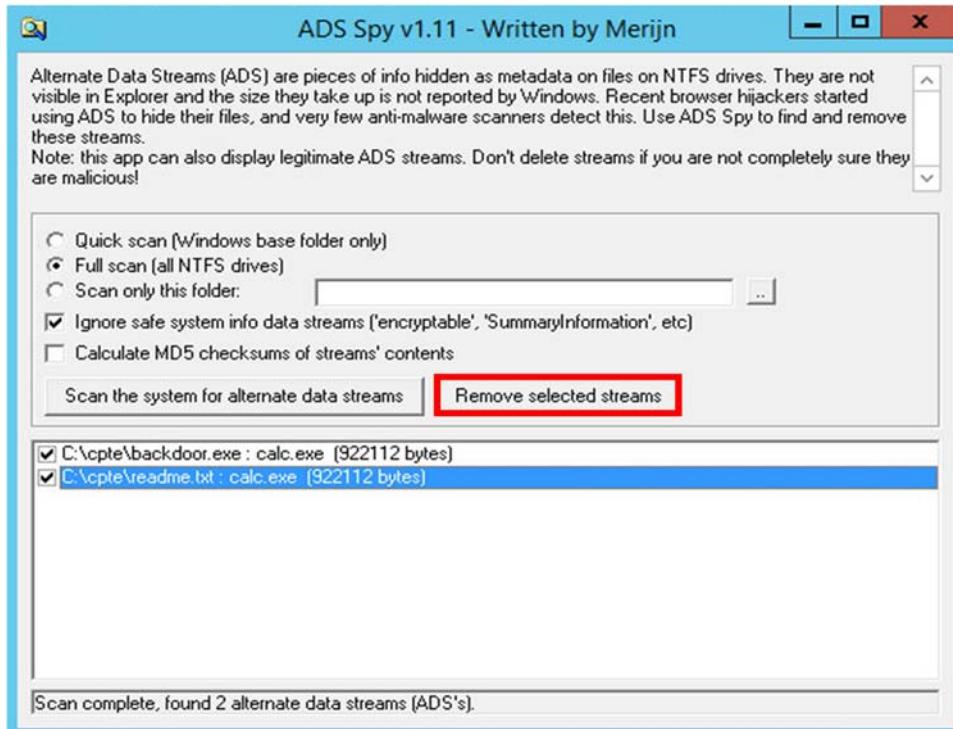


Figure: 4.3- Find the hidden streams file

## Lab Analysis

Document all the results discovered during the lab.

Tool/Utility	Information Collected/Objectives Achieved
<b>ADS Spy</b>	<p><b>Scan Option:</b> Full Scan (all NTFS drives)</p> <p><b>Output:</b></p> <ul style="list-style-type: none"> <li>• Hidden files with its location</li> <li>• Hidden files size</li> </ul>

## Quiz

1. Analyze how ADS Spy detects NTFS streams.

# Lab

## 4

**ICON KEY**
 Important Information

 Quiz

 CPTE Labs

 Course Review

# Hiding Files Using the Stealth Files Tool

## Stealth Files Overview

**Stealth Files:** Stealth Files hides any type of file in almost any other type of file. This is called steganography. This is a way of encrypting data so that it is hard to find. You can not decrypt something unless you know what to decrypt. Using steganography, Stealth Files compresses, encrypts, and then hides any type of file inside many other types of files, including EXE, DLL, OCX, COM, JPG, GIF, ART, MP3, AVI, WAV, DOC, BMP, and most other types of video, image, and executable files. You will still be able to view, open, and run these files without any problems. If you want to, you can also use a password to encrypt the hidden files.

## Lab Scenario

The Windows NT NTFS file system has a feature that is not well documented and is unknown to many NT developers and most users. A stream is a hidden file that is linked to a normal (visible) file. A stream is not limited in size and there can be more than one stream linked to a normal file. Streams can have any name that complies with NTFS naming conventions. In order to be a penetration tester engineer, you must understand how to hide files using the Stealth Files tool. In this lab, discuss how to find hidden files inside of other files using the Stealth Files Tool.

The objective of this lab is to teach students how to hide files using the Stealth Files tool.

It will teach you how to:

- Use the Stealth Files Tool
- Hide files

## Lab Resources

To run this lab, you need the following:

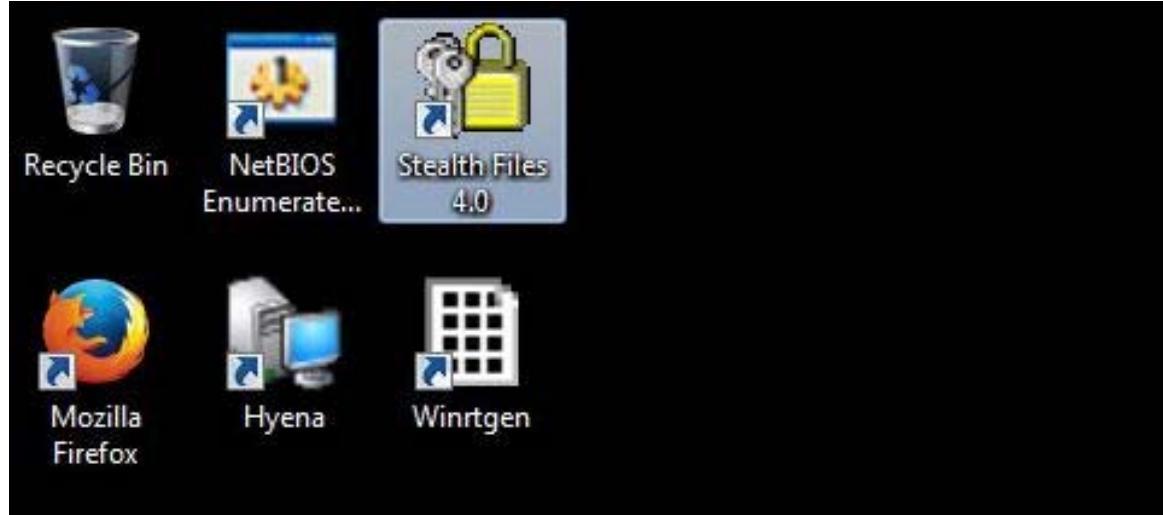
- Stealth files tool located on Desktop
- Run this tool in Windows 7
- Administrative privileges to run the **Stealth files tool**

## Lab Duration

Time: 15 Minutes

## Lab Tasks

1. Navigate to Desktop
2. Click the **Stealth Files 4.0** icon to open the **Stealth File** window.



### Task 1

#### Steganography



3. The main window of **Stealth Files 4.0** is shown in the following figure.

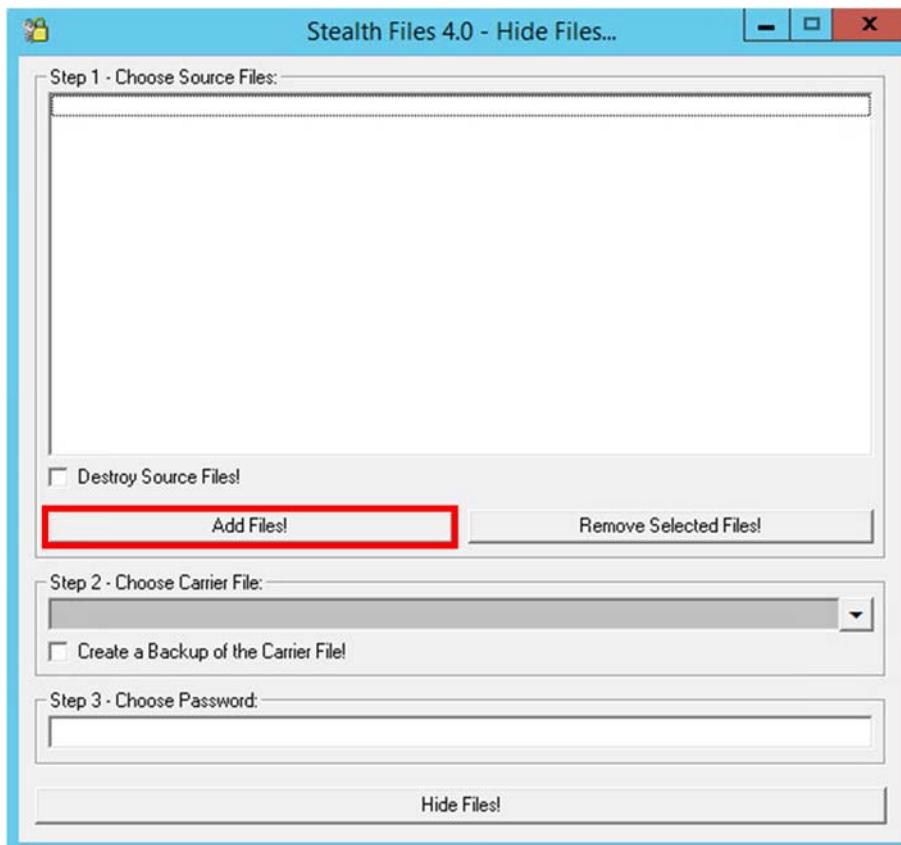


Steganography is the art and science of writing hidden messages

4. Click **Hide Files** to start the process of hiding the files.
5. Click **Add files**.



**This is an alternative to encryption because no one can decrypt encrypted information or files unless they know that the hidden files exist.**

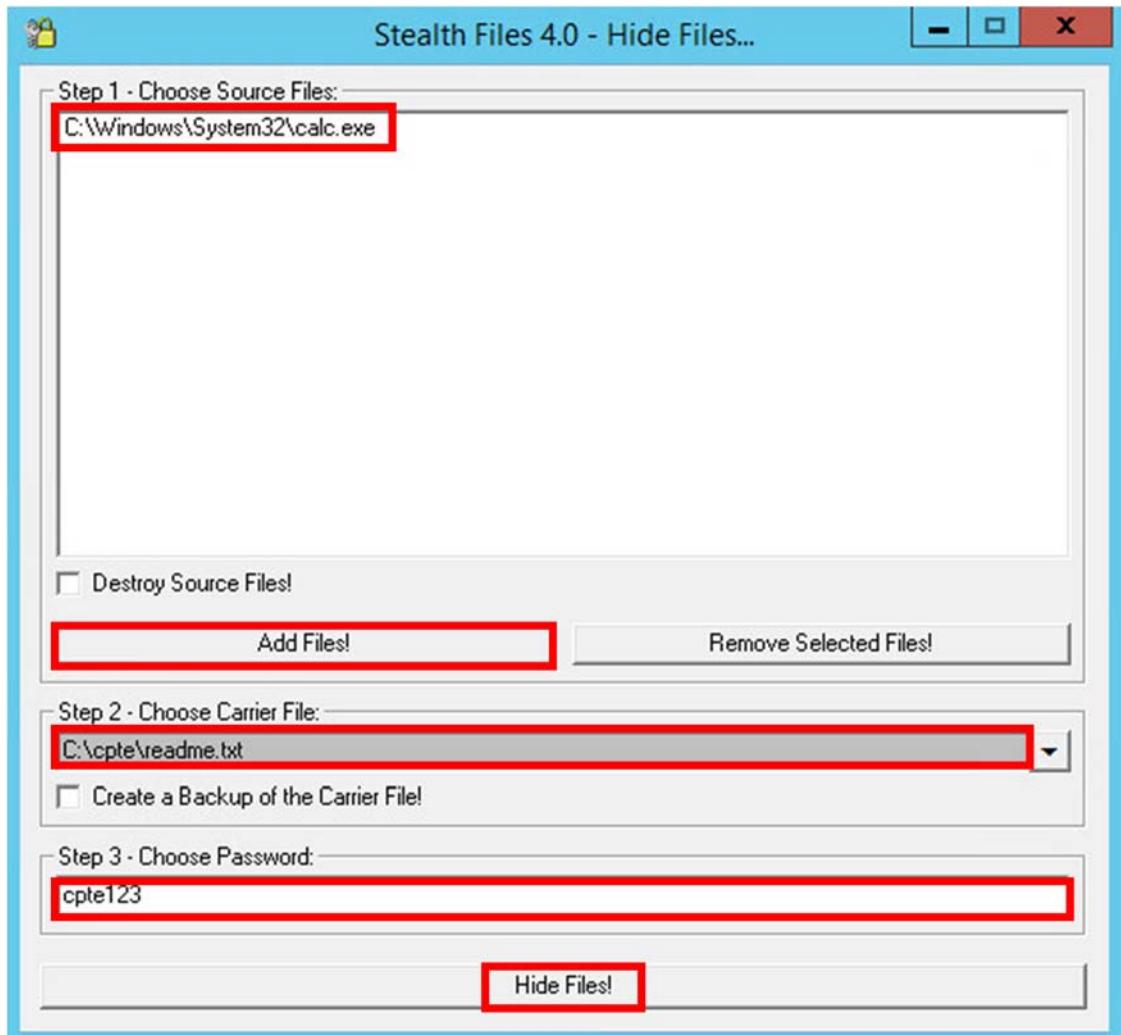


Before Stealth Files hides a file, it compresses it and encrypts it with a password. Then you must select a carrier file, which is a file that contains the hidden files

6. In **Step 1**, add the Calc.exe from c:\windows\system32\calc.exe.
7. In **Step 2**, choose the carrier file and add the file **Readme.txt** from the c:\cptc
8. In **Step 3**, choose a password such as cptc123 (you can type any desired password).

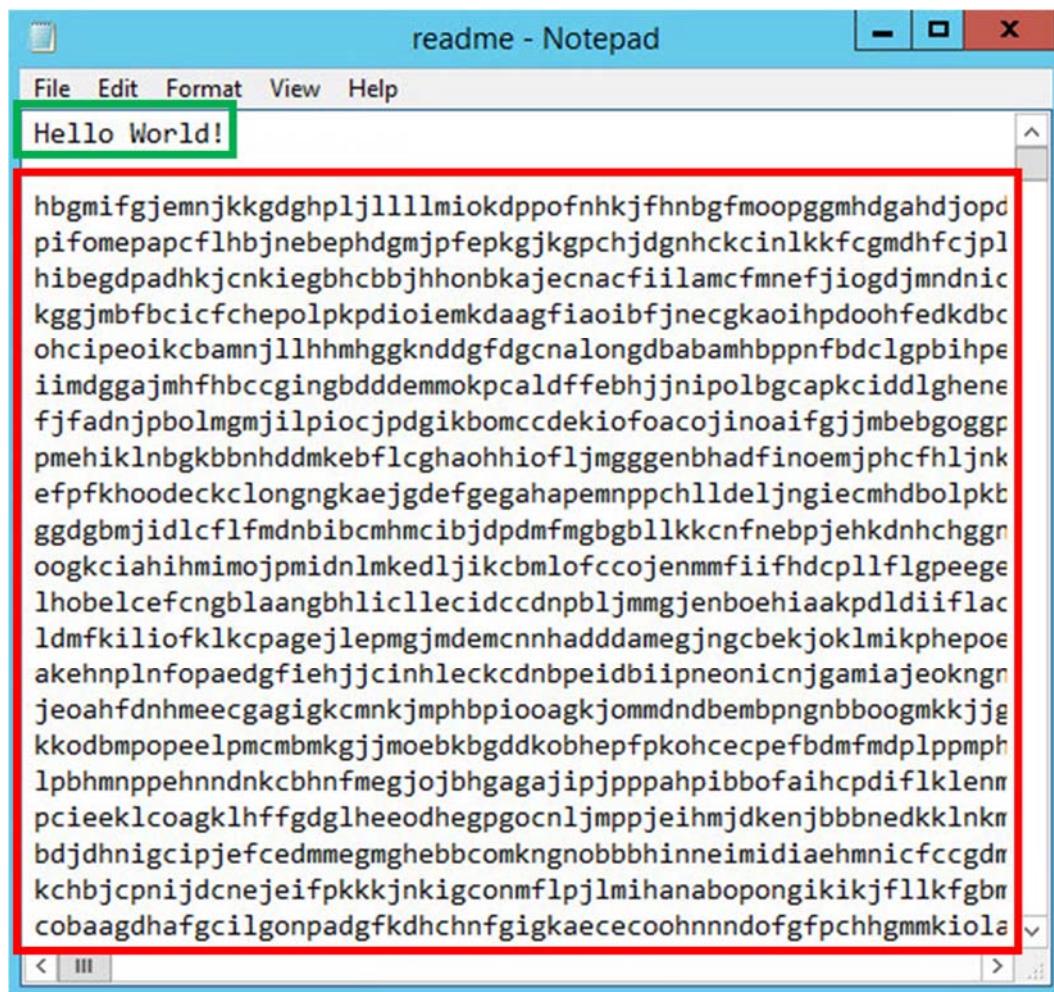


You can also remove the hidden files from the carrier file by going to Remove Hidden Files and following the instructions



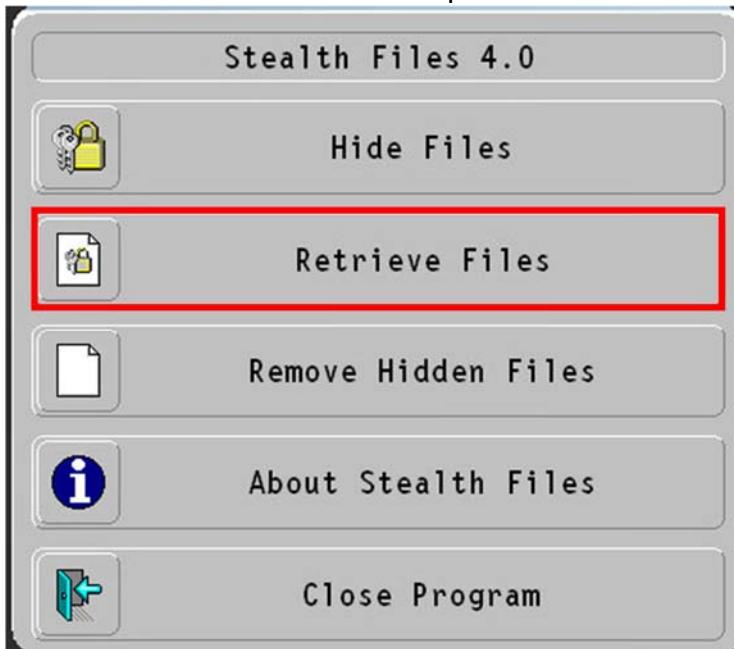
Step 1 to 3 screen

9. Click **Hide Files!**
10. It will hide the file **calc.exe** inside the **readme.txt** located on the desktop.
11. Open the notepad and check the file; **calc.exe** is copied inside it.



When you are ready to recover your hidden files, simply open them up with Stealth Files, and if you gave the carrier file a password, you will be prompted to enter it again to recover the hidden files

Figure: 5.5- Calc.exe copied inside Readme.txt  
12. Now open the **Stealth files Control** panel and click **Retrieve Files**.



Pictures will still look the same, sound file will still sound the same, and programs will still work fine

These carrier files will still work perfectly even with the hidden data in them

Figure: 5.6- Stealth Files main Window

13. In **Step 1**, choose the file (Readme.txt) from the Desktop where you have saved the **calc.exe** file.
14. In **Step 2**, choose the path to store the retrieved hidden file. In the lab, the path is Desktop.
15. Enter the password magic (the password that is entered to hide the file) and click on **Retrieve Files!**



You can transfer the carrier file through the Internet, and the hidden files inside will transfer simultaneously.

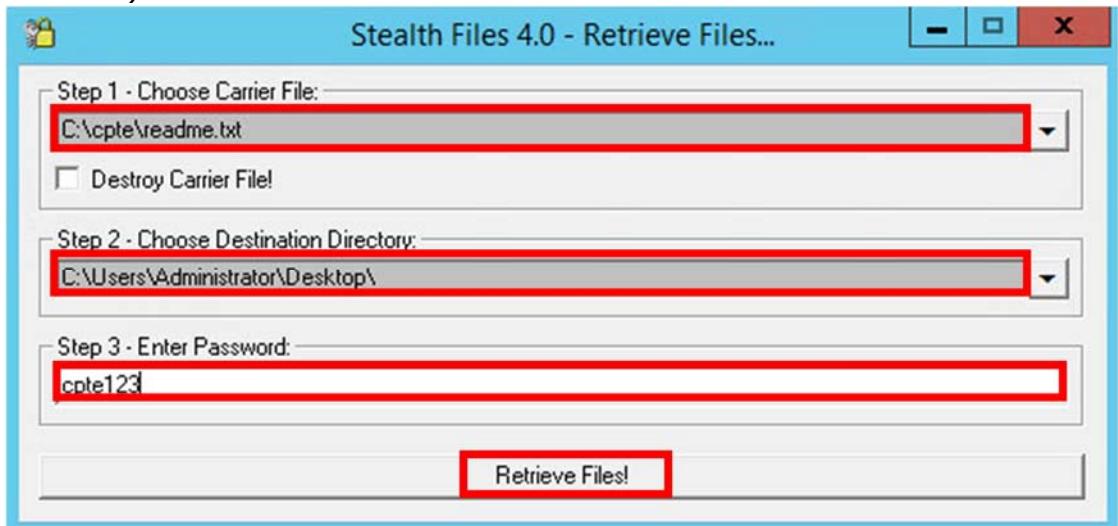


Figure: 5.7- Retrieve files main Window

16. The retrieved file is stored on the Desktop

## Lab Analysis

Document all the results discovered during the lab.

Tool/Utility	Information Collected/Objectives Achieved
<b>Stealth Files Tool</b>	<b>Hidden Files:</b> Calc.exe (calculator)
	<b>Retrieve File:</b> readme.txt (Notepad)
	<b>Output:</b> Hidden calculator executed

## Quiz

1. Evaluate other alternative parameters for hiding files.

# Lab

## 5

# Extracting SAM Hashes Using PWDump7 Tool

## PWDump7 Overview

**Pwdump7** runs by extracting the binary SAM and SYSTEM File from the Filesystem and then the hashes are extracted. For that task Rkdetector NTFS and FAT32 filesystem drivers are used.

Pwdump7 is also able to extract passwords offline by selecting the target files.

### ICON KEY



Important Information



Quiz



CPTE Labs



Course Review

## Lab Scenario

Passwords are a big part of this modern generation. You can use the password for your system to protect the business or secret information and you may choose to limit access to your PC with a Windows password. These passwords are an important security layer, but many passwords can be cracked and while that is worrisome, this can come to your rescue. In order to be an expert penetration tester, you must understand how to crack administrator passwords. In this lab, we discuss extracting the user login password hashes to crack the password.

It will teach you how to:

- Use the **pwdump7** tool
- Crack administrator passwords

## Lab Resources

To run this lab you need the following:

- **Pwdump7** located on C:\Drive
- Run this tool in Windows 7

## Lab Duration

Time: 10 Minutes

## Lab Tasks

1. Open the command prompt and type cd\ and press Enter
2. Now type **pwdump7.exe** and press **Enter**, which will display all the password hashes

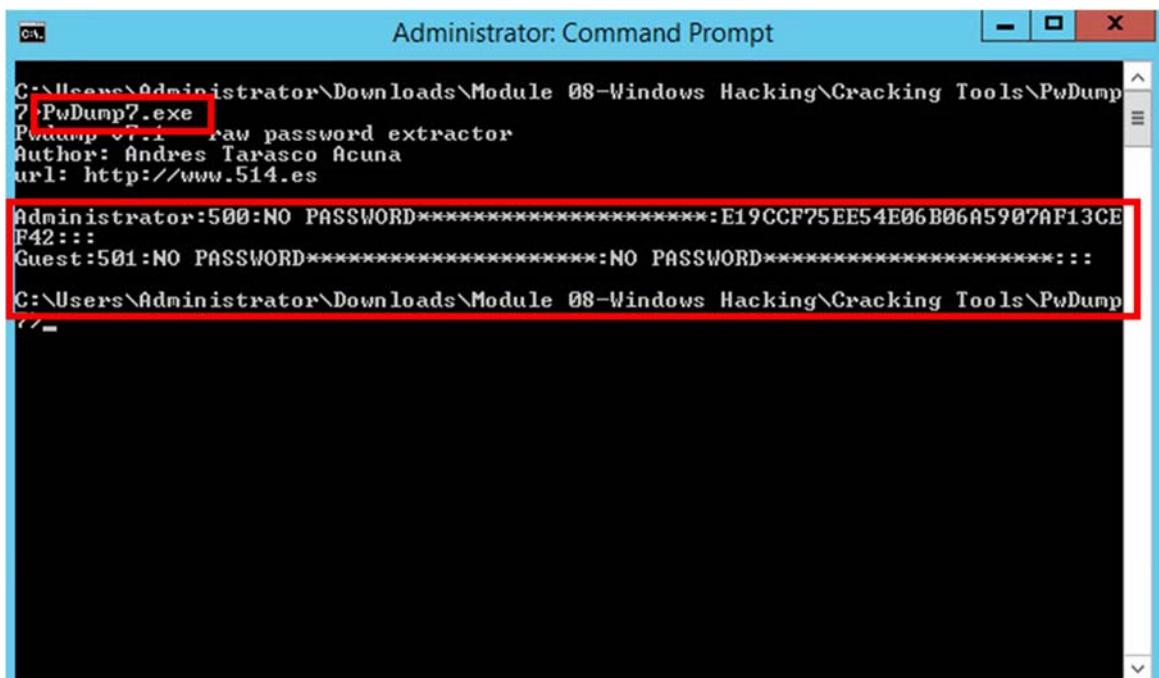


**Task 1**

**Generating Hashes**



Active directory  
passwords are stored  
in the ntds.dit file  
and currently the  
stored structure



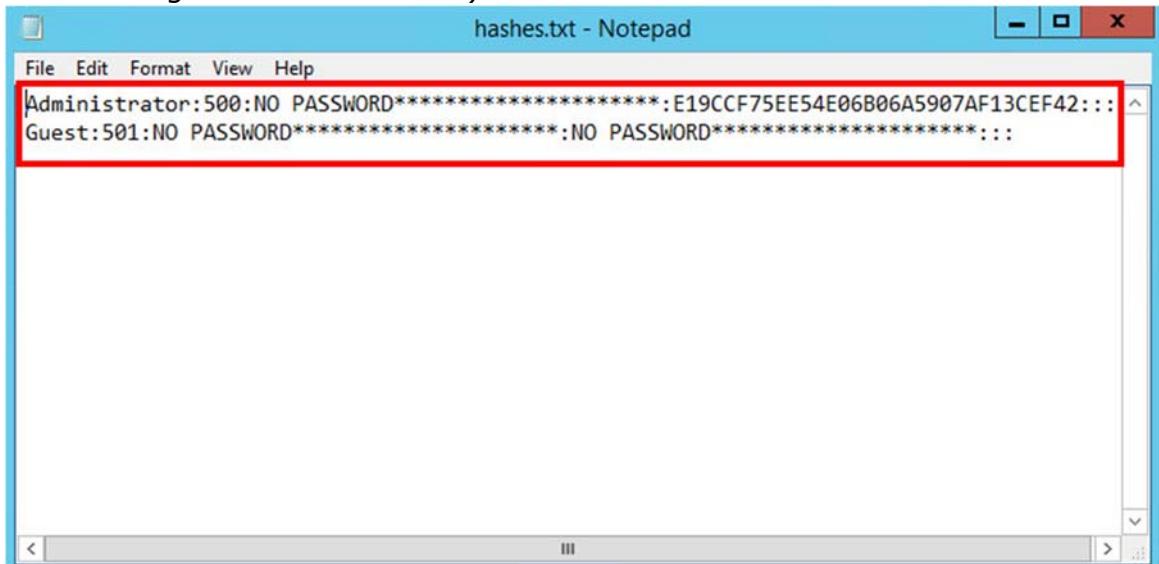
```
C:\Users\Administrator\Downloads\Module 08-Windows Hacking\Cracking Tools\PwDump7\PwDump v7.1 Raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:NO PASSWORD*****:E19CCF75EE54E06B06A5907AF13CE
F42:::
Guest:501:NO PASSWORD*****:NO PASSWORD*****:::

C:\Users\Administrator\Downloads\Module 08-Windows Hacking\Cracking Tools\PwDump7\
```

Figure: 6.1- Pwdump7.exe result window

3. Now type **pwdump7.exe > c:\hashes.txt** in the command prompt, and press **Enter**.
4. This command will copy all the data of **pwdump7.exe** to the **c:\hashes.txt** file. (To check the generated hashes you need to navigate to the C: drive.)



```
hashes.txt - Notepad
File Edit Format View Help
Administrator:500:NO PASSWORD*****:E19CCF75EE54E06B06A5907AF13CE
F42:::
Guest:501:NO PASSWORD*****:NO PASSWORD*****:::
```

Figure: 6.2- hashes.txt contents

## Lab Analysis

Analyze all the password hashes gathered during the lab and figure out what the password was.

Tool/Utility	Information Collected/Objectives Achieved
PWdump7	<b>Output:</b> List of User and Password Hashes <ul style="list-style-type: none"><li>• Administrator</li><li>• Guest</li></ul>

## Quiz

1. What is pwdump7.exe command used for?
2. How do you copy the result of a command to a file?
3. Dump password from SAM files.

# Lab

## 6

### ICON KEY

 Important Information

 Quiz

 CPTE Labs

 Course Review

# Creating the Rainbow Tables Using Winrtgen

## Winrtgen Overview

A rainbow table is a precomputed table for reversing cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering plaintext passwords, up to a certain length, consisting of a limited set of characters.

Rainbow tables reduce the difficulty in brute force cracking a single password by creating a large pre-generated data set of hashes from nearly every possible password.

**Winrtgen** is a graphical Rainbow Tables Generator that supports LM, FastLM, NTLM, LMCHALL, HalfLMCHALL, NTLMCHALL, MSCACHE, MD2, MD4, MD5, SHA1, RIPEMD160, MySQL323, MySQLSHA1, CiscoPIX, ORACLE, SHA-2 (256), SHA-2 (384) and SHA-2 (512) hashes.

## Lab Scenario

In computer and information security, the use of a password is essential for users to protect their data to ensure a seamless access to their system or machine. As users become increasingly aware of the need to adopt strong passwords, it also brings challenges to protection of potential data. In this lab, we will discuss creating the rainbow table to crack the user's system passwords. In order to be an expert penetration tester, you must understand how to create rainbow tables to crack the administrator password.

The objective of this lab is to help students create and use rainbow tables to perform system password hacking.

## Lab Resources

To run this lab, you will need the following:

- **Winrtgen** located on Desktop
- Run this tool in Windows 7
- Administrative privileges to run the **Winrtgen**

## Lab Duration

Time: 10 Minutes

## Lab Tasks

1. Double-click the **winrtgen.exe** file located on the Desktop. The main window of **Winrtgen** is shown in the following figure.

**Task 1**

**Generating Hashes**

Active directory  
passwords are stored  
in the ntds.dit file

Rainbow tables are  
typically used to crack a  
lot of hash types, such  
as  
NTLM, MD 5, SHA1

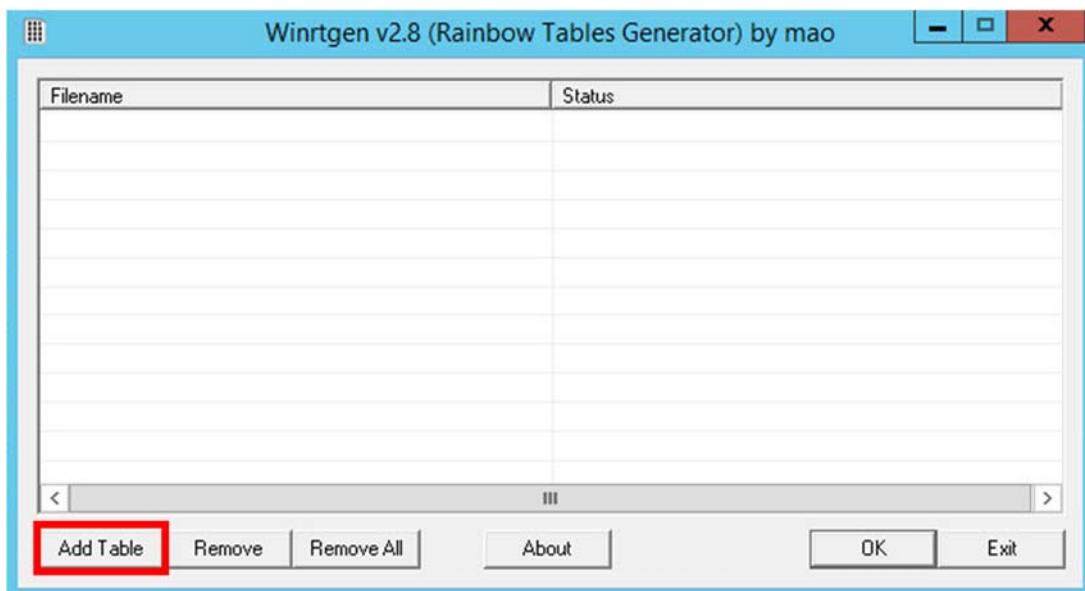


Figure: 7.1- Winrtgen main window

2. Click the **Add Table** button
3. The **Rainbow Table properties** window appears:
  - i. Select **ntlm** from the **Hash** drop-down list
  - ii. Set the **Min Len** as **4**, the **Max Len** as **9**, and the **Chain Count** of **40000000**
  - iii. Select **loweralpha** from the **Charset** drop-down list (this depends on the password).
4. Click **OK**.

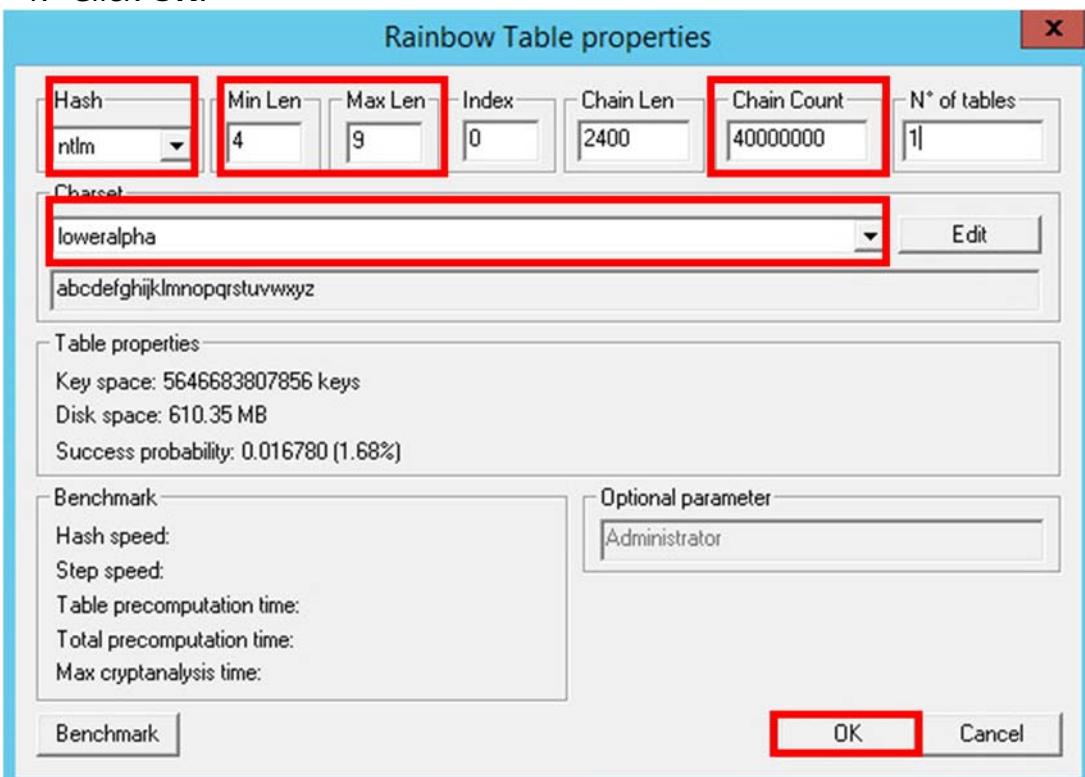


Figure: 7.2- Selecting the Rainbow table properties

5. A file will be created; click **OK**.

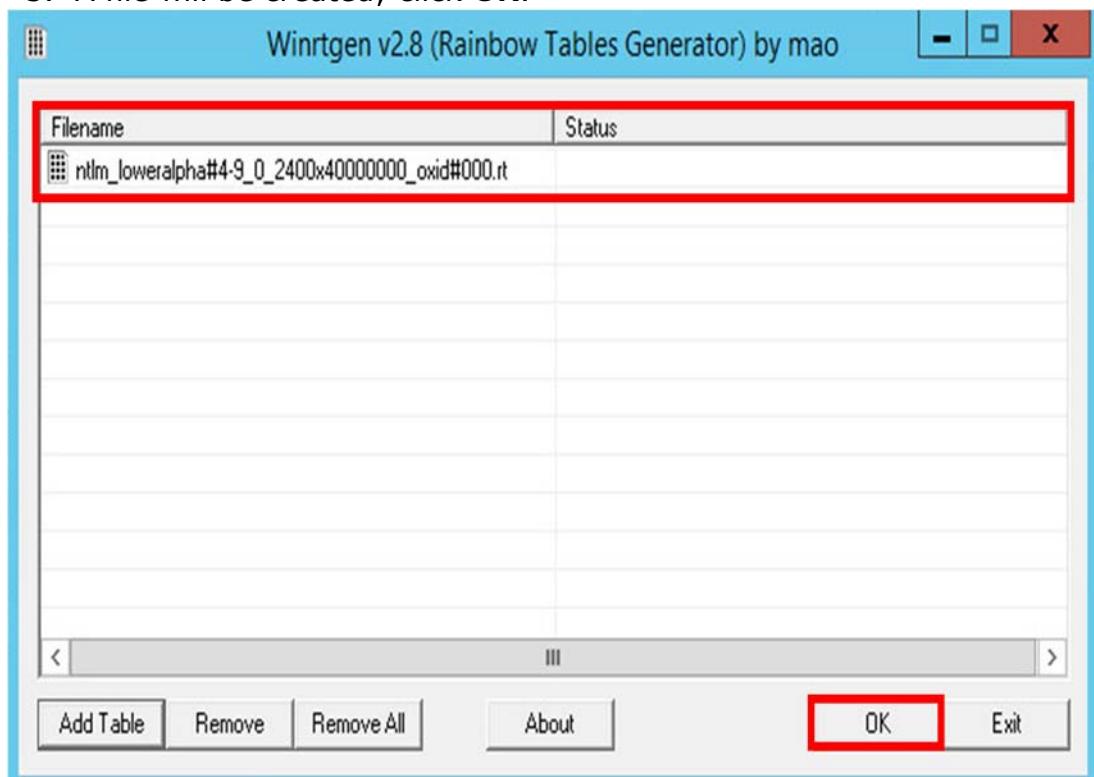


Figure: 7.3- Rainbow Table name to be generated

6. Creating the hash table will take some time, depending on the selected hash and charset. With the recommended settings this rainbow table will take 40 minutes to an hour to generate. Move on to the next module and come back to lab 7 once the rainbow table has finished.
7. The created hash table saved automatically in the folder containing **winrtgen.exe**.

## Lab Analysis

Analyze all the password hashes gathered during the lab and figure out what the password was.

Tool/Utility	Information Collected/Objectives Achieved
Winrtgen	<b>Purpose:</b> Creating Rainbow table with lower alpha <b>Output:</b> Created Rainbow table: ntlm_lowe1-alpha#4-6_0_2400X40000000_ox...

# Lab

## 7

### ICON KEY

 Important Information

 Quiz

 CPTE Labs

 Course Review

# Password Cracking Using RainbowCrack

## RainbowCrack Overview

RainbowCrack is a computer program that generates rainbow tables to be used in password cracking. RainbowCrack differs from "conventional" brute force crackers in that it uses large pre-computed tables called rainbow tables to reduce the length of time needed to crack a password.

A brute force hash cracker generates all possible plaintexts and computes the corresponding hashes on the fly, then compares the hashes with the hash to be cracked. Once a match is found, the plaintext is found. If all possible plaintexts are tested and no match is found, the plaintext is not found. With this type of hash cracking, all intermediate computation results are discarded. A time-memory tradeoff hash cracker needs a pre-computation stage, at that time all plaintext/hash pairs within the selected hash algorithm, charset, plaintext length are computed and results are stored in files called rainbow tables. It is time consuming to do this kind of computation. But once the one time pre-computation is finished, hashes stored in the table can be cracked with much better performance than a brute force cracker.

## Lab Scenario

Computer passwords are like locks on doors; they keep honest people honest. If someone wishes to gain access to your laptop or computer, a simple login password will not stop them. Most computer users do not realize how simple it is to access the login password for a computer, and end up leaving vulnerable data on their computer, unencrypted and easy to access. Are you curious how easy it is for someone to gain access to your computer? Windows is still the most popular operating system, and the method used to discover the login password is the easiest.

A hacker uses password cracking utilities and cracks your system. That is how simple it is for someone to hack your password. It requires no technical skills, in laborious tasks, only simple words or programs. In order to be an expert penetration tester, you must understand how to crack administrator passwords. In this lab, we discuss how to crack guest users or administrator passwords using RainbowCrack.

The objective of this lab is to help students **crack passwords** to perform system password hacking.

## Lab Resources

To run this lab, you need the following:

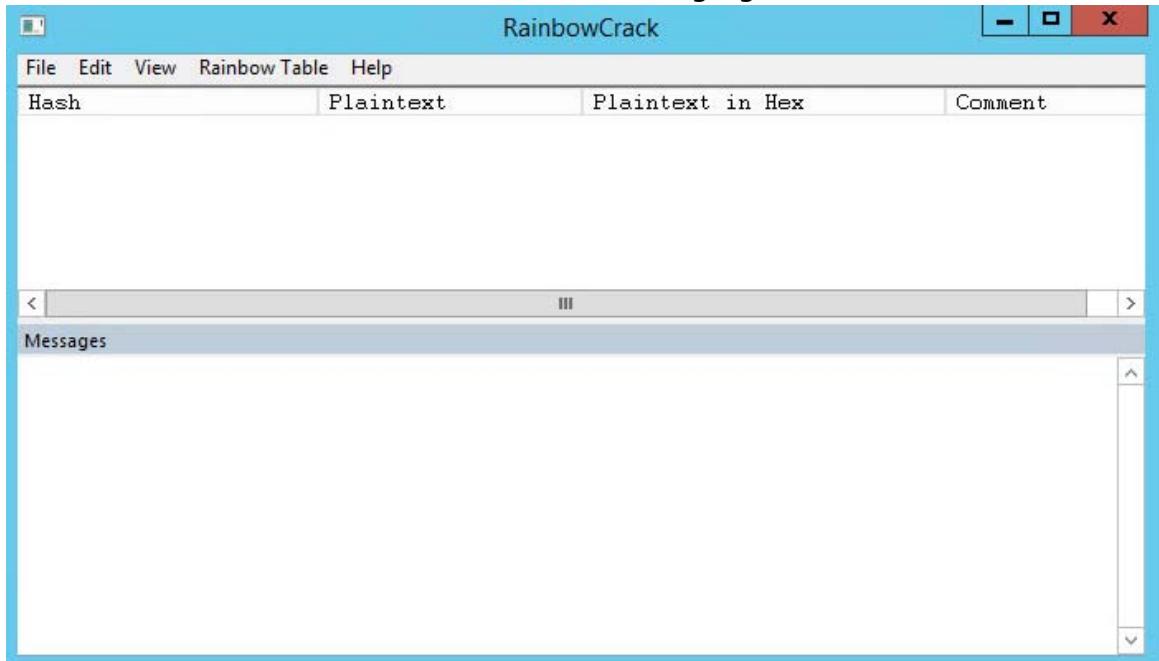
- **RainbowCrack** located on Desktop
- Run this tool in Windows 7
- Administrative privileges to run the **RainbowCrack**

## Lab Duration

Time: 10 Minutes

### Lab Tasks

- Double-click the **rcrack\_gui.exe** file on Desktop. The main window of **Rainbowcrack** is shown in the following figure.



#### Task 1

##### Generating the Rainbow Tables



RainbowCrack for GPU is the hash cracking program in RainbowCrack hash cracking utilities.

Figure: 8.1- RainbowCrack main window

- Click **File**, and then click **Add Hash...**

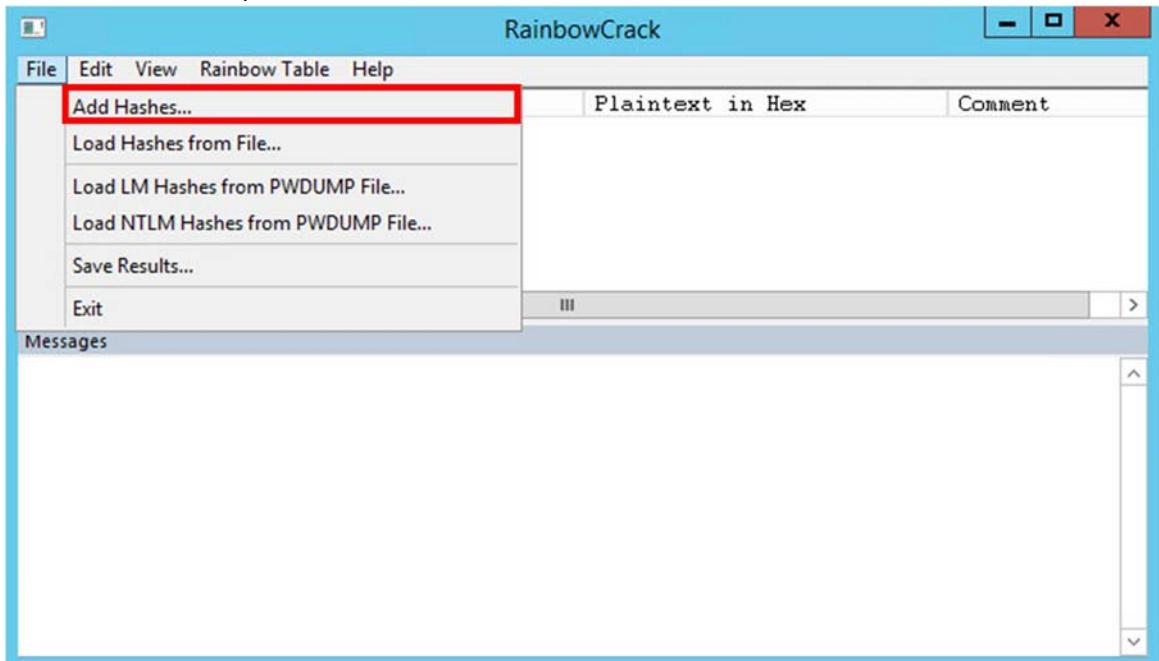


Figure: 8.2- Add Hash Values

3. The Add Hash window appears:
  - a. Navigate to **c:\cpte**, and open the **hashes.txt** file (which is already generated using **Pwdump7** located at **c:\cpte\hashes.txt** in the previous **Lab 5**).
  - b. Right-click, copy the hashes from hashes.txt file.
  - c. Paste into the **Hash** field.
  - d. Click **OK**.



RainbowCrack uses a Time-memory tradeoff algorithm to crack hashes. It differs from the hash crackers that use brute force algorithm

	File	Edit	Format	View	Help
Adm		Undo	Ctrl+Z	ORD*****	A87E3A337D73085C45F9416BF5787D86:::
Gue		Cut	Ctrl+X	*****	:NO PASSWORD*****:::
cpt		Copy	Ctrl+C	*****	:C13087D3705DE1F43D80380AD7BB4B1B:::
		Paste	Ctrl+V		

Figure: 8.3- Selecting the Hashes

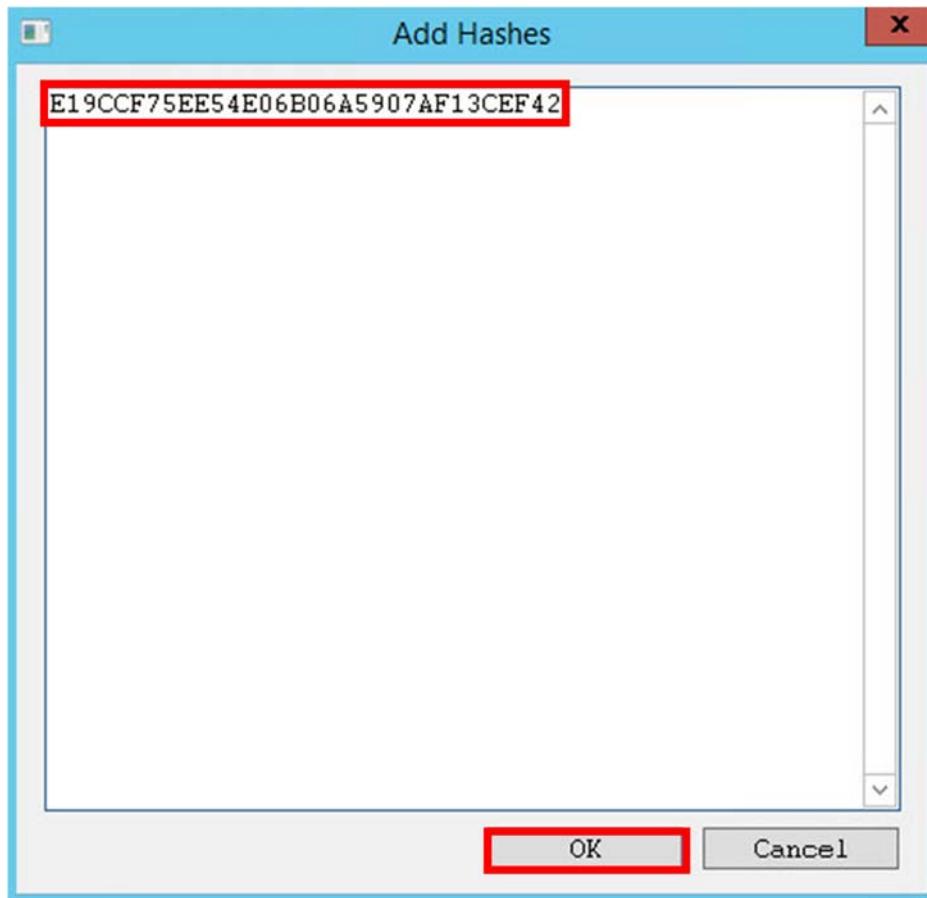


Figure: 8.4- Adding Hashes

4. The selected hash is added, as shown in the following figure.

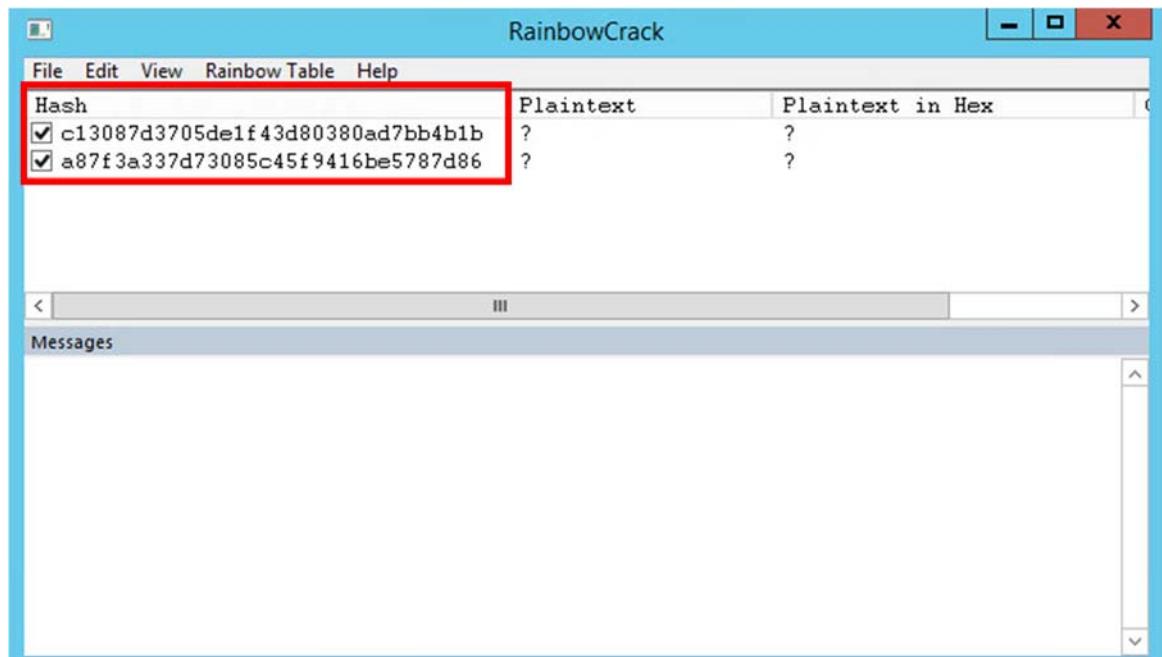


Figure: 8.5- Added Hash show in RainbowCrack main window

5. To add more hashes, repeat steps 2 & 3 (a,b,c,d)
6. Click the **Rainbow Table** from the menu bar, and click Search **Rainbow Table...**

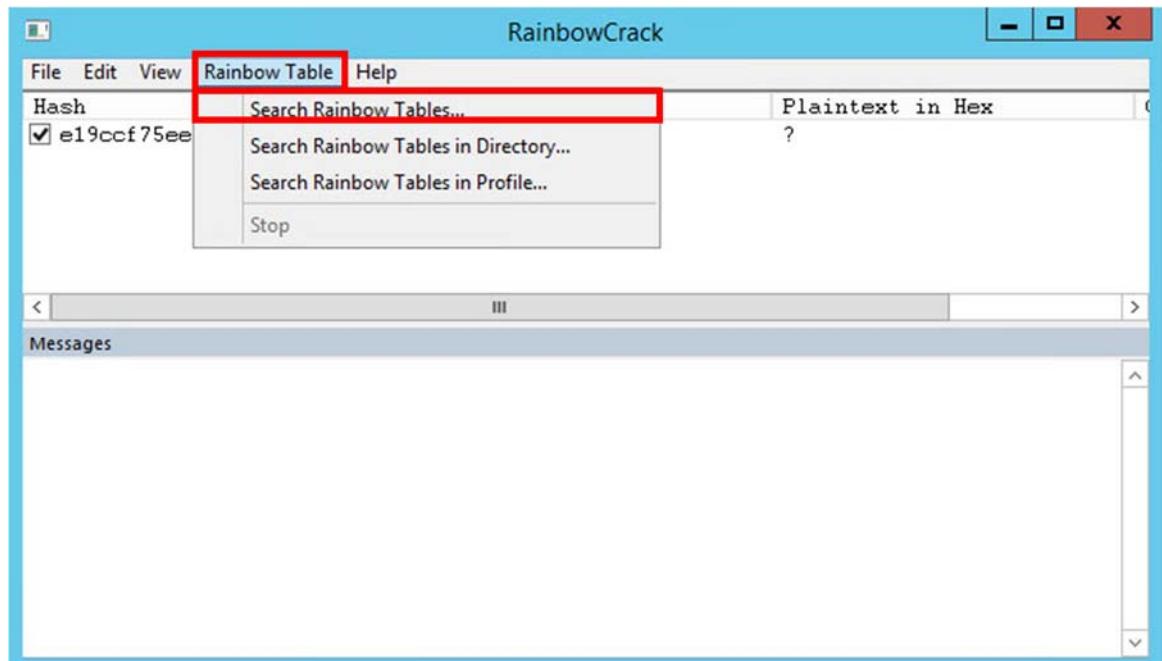


Figure: 8.6- Adding RainbowCrack table

7. Browse the **Rainbow Table** that is already generated in the previous lab, which is located on Desktop
8. Click **Open**.

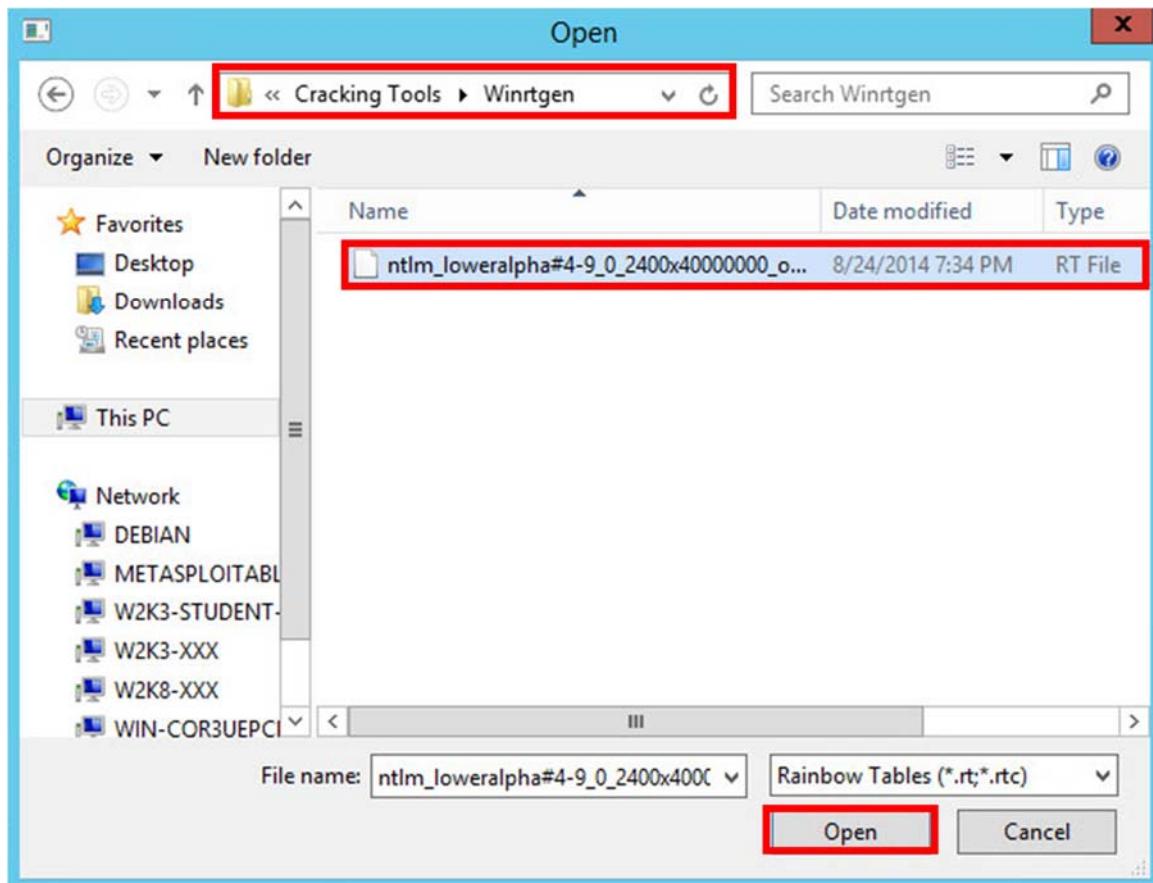


Figure: 8.5- Select Rainbow Table generated in the Winrtgen lab

9. It will crack the password, as shown in the following figure.

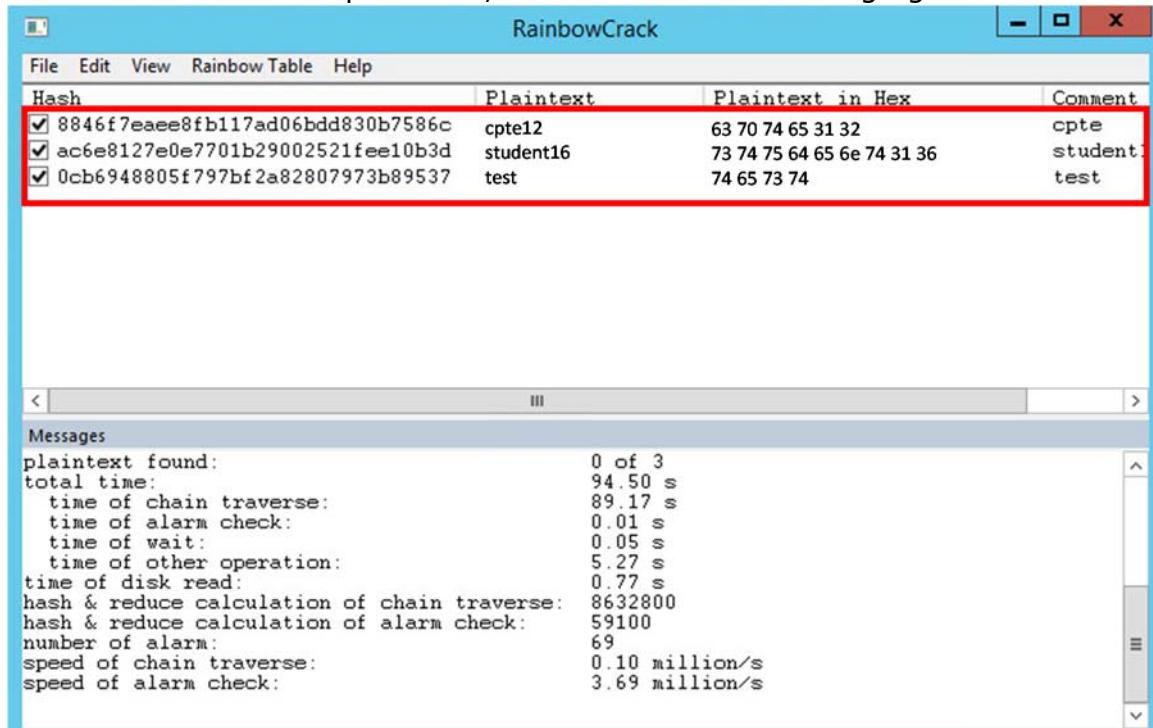


Figure: 8.6- Password cracked with Rainbow Table generated in the Winrtgen lab

## Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
RainbowCrack	<p><b>Hashes:</b></p> <ul style="list-style-type: none"> <li>• Administrator</li> <li>• Guest</li> <li>• Test</li> <li>• CPTE</li> <li>• STUDENT16</li> </ul> <hr/> <p><b>Password Cracked:</b></p> <ul style="list-style-type: none"> <li>• P@ssw0rd</li> <li>• test</li> <li>• test</li> <li>• cppte12</li> <li>• student16</li> </ul>

## Quiz

1. What kind of hashes does RainbowCrack support?