System Hacking

Module 05

System Hacking

System hacking is the science of testing computers and network for vulnerabilities and plug-ins.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

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 chapter demonstrates just how easily hackers can gather password information from your network and describes password vulnerabilities that exit in computer networks and countermeasures to help prevent these vulnerabilities from being exploited on your systems.

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:

- Extracting administrative passwords
- Hiding files and extracting hidden files
- Recovering passwords
- Monitoring a system remotely

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

Lab Environment

To carry out the lab you need:

- A computer running **Windows Server 2012**
- A web browser with an **Internet** connection
- Administrative privileges to run tools

Lab Duration

Time: 100 Minutes

Overview of System Hacking

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

TASK 1

Overview

Lab Tasks

Recommended labs to assist you in system hacking:

- Extracting Administrator Passwords Using **LCP**
- Hiding Files Using **NTFS Streams**
- Find Hidden Files Using **ADS Spy**
- Hiding Files Using the **Stealth Files Tool**
- Extracting SAM Hashes Using **PWdump7** Tool
- Creating the Rainbow Tables Using **Winrtge**
- Password Cracking Using **RainbowCrack**
- Extracting Administrator Passwords Using **L0phtCrack**
- Password Cracking Using **Ophcrack**
- System Monitoring Using **RemoteExec**
- Hiding Data Using **Snow** Steganography
- Viewing, Enabling and Clearing the Audit Policies Using **Auditpol**
- Password Recovery Using **CHNTPW.ISO**
- User System Monitoring and Surveillance Needs Using **Spytech SpyAgent**
- Web Activity Monitoring and Recording using **Power Spy 2013**
- Image Steganography Using **QuickStego**

Lab Analysis

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

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab 1

Extracting Administrator Passwords Using LCP

Link Control Protocol (LCP) is part of the Point-to-Point (PPP) protocol. In PPP communications, both the sending and receiving devices send out LCP packets to determine specific information required for data transmission.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Hackers can break weak password storage mechanisms by using cracking methods that outline in this chapter. Many vendors and developers believe that passwords are safe from hackers if they don't publish the source code for their encryption algorithms. After the code is cracked, it is soon distributed across the Internet and becomes public knowledge. Password-cracking utilities take advantage of weak password encryption. These utilities do the grunt work and can crack any password, given enough time and computing power. In order to be an expert ethical hacker and penetration tester, you must understand how to crack administrator passwords.

Lab Objectives

The objective of this lab is to help students learn how to crack administrator passwords for ethical purposes.

In this lab you will learn how to:

- Use an LCP tool
- Crack administrator passwords

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

Lab Environment

To carry out the lab you need:

- LCP located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Password Cracking Tools\LCP**
- You can also download the latest version of **LCP** from the link http://www.lcpsoft.com/english/index.htm

- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- Follow the wizard driven installation instructions
- Run this tool in **Windows Server 2012**
- Administrative privileges to run tools
- **TCP/IP** settings correctly configured and an accessible DNS server

Lab Duration

Time: 10 Minutes

Overview of LCP

LCP program mainly audits **user account passwords** and **recovers** them in Windows 2008 and 2003. General features of this protocol are **password recovery**, **brute force** session distribution, account information importing, and **hashing.** It can be used to test password security, or to recover lost passwords. The program can import from the local (or remote) computer, or by loading a SAM, LC, LCS, PwDump or Sniff file. LCP supports dictionary attack, brute force attack, as well as a hybrid of dictionary and brute force attacks.

Lab Tasks

TASK 1

Cracking Administrator Password

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

FIGURE 1.1: Windows Server 2012 – Desktop view

2. Click the **LCP** app to launch **LCP**.

You can also download LCP from http://www.lcpsoft.com.

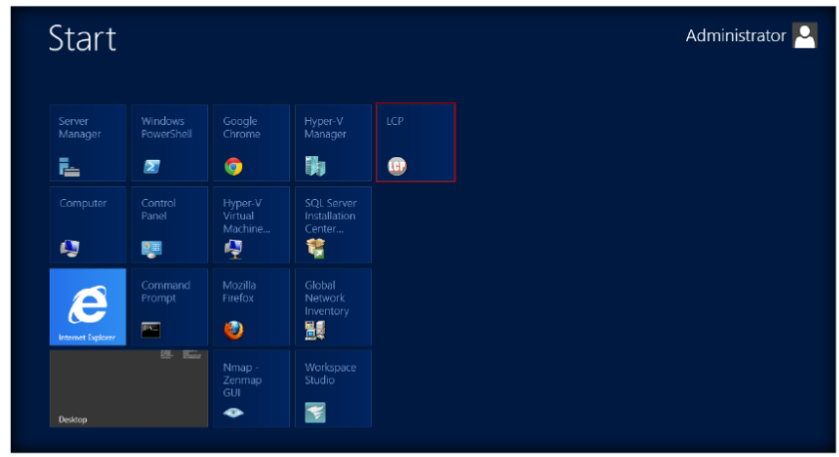


FIGURE 1.2: Windows Server 2012 – Apps

3. The **LCP** main window appears.

LCP supports additional encryption of accounts by SYSKEY at import from registry and export from SAM file.

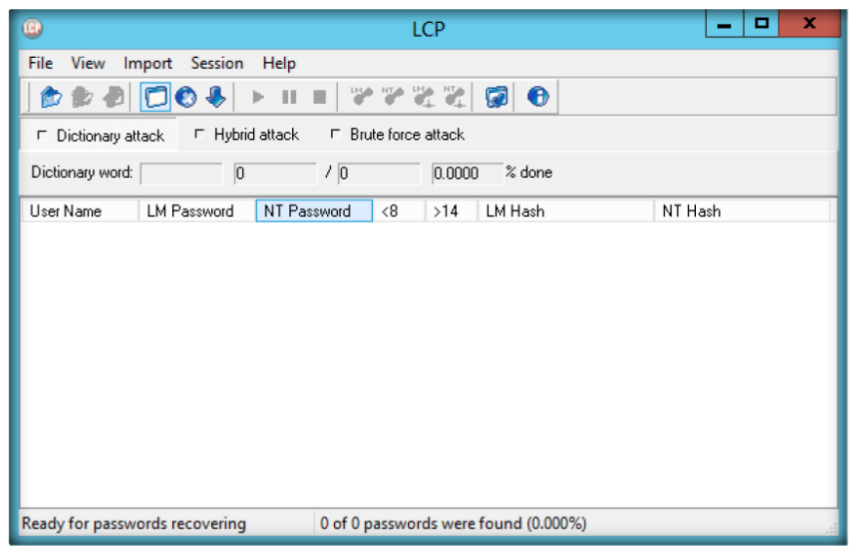


FIGURE 1.3: LCP main window

4. From the menu bar, select **Import** and then **Import from remote computer**.

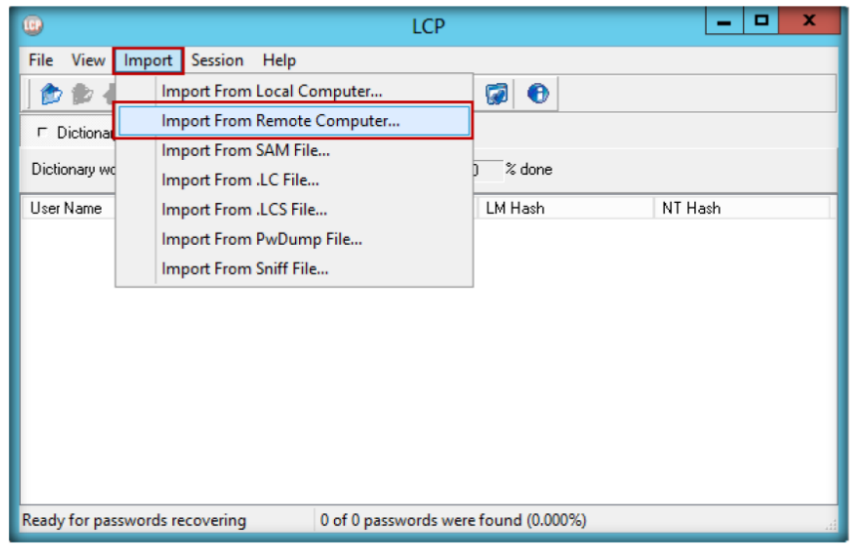


FIGURE 1.4: Import the remote computer

LCP is logically a transport layer protocol according to the OSI model.

5. Select **Computer name or IP address**, select the **Import type** as **Import from registry**, and click **OK**.

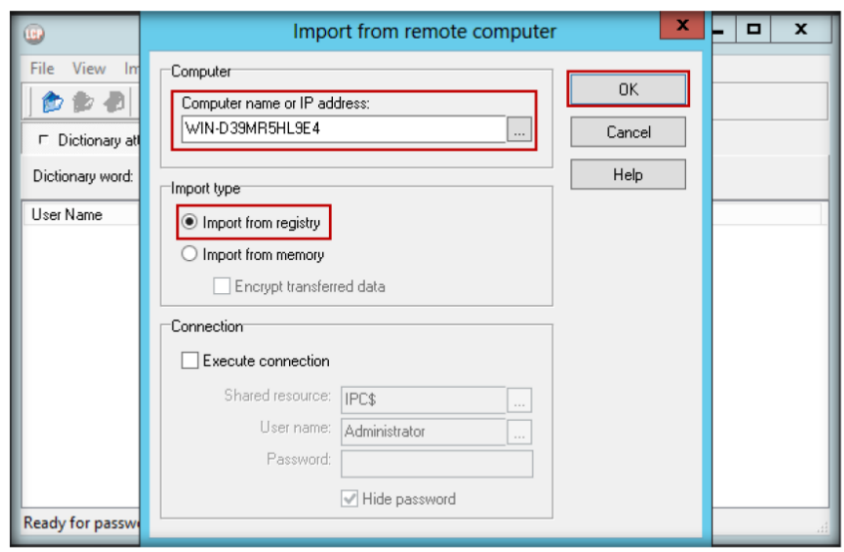
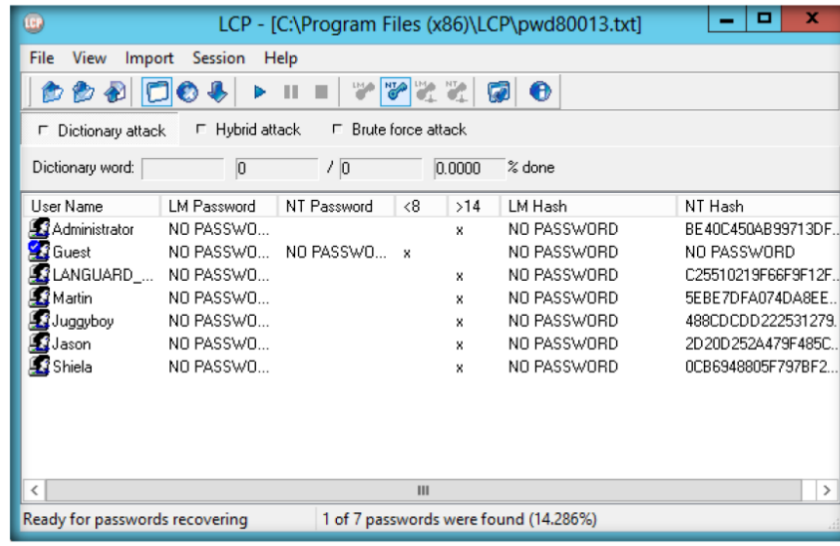


FIGURE 1.5: Import from remote computer window

LCP checks the identity of the linked device and either accepts or rejects the peer device, then determines the acceptable packet size for transmission.

6. The **output** window appears.



Main purpose of LCP program is user account passwords auditing and recovery in Windows

FIGURE 1.6: Importing the User Names

7. Now select any **User Name** and click the **Play** button.
8. This action generates passwords.

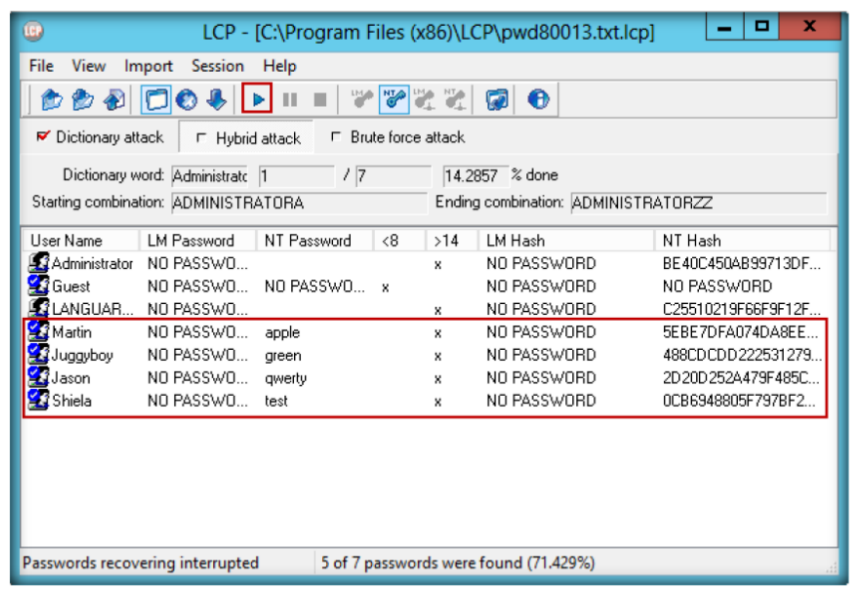


FIGURE 1.7: LCP generates the password for the selected username

Lab Analysis

Document all the IP addresses and passwords extracted for respective IP addresses. Use this tool only for training purposes.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
LCP	**Remote Computer Name:** WIN-D39MR5HL9E4
	Output: User Name - NT Password ▪ Martin - apple ▪ Juggyboy - green ▪ Jason - qwerty ▪ Shiela - test

Questions

1. What is the main purpose of LCP?
2. How do you continue recovering passwords with LCP?

Internet Connection Required	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Lab 2

Hiding Files Using NTFS Streams

A stream consists of data associated with a main file or directory (known as the main unnamed stream). Each file and directory in NTFS can have multiple data streams that are generally hidden from the user.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

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.

Lab Objectives

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

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

It will teach you how to:

- Use NTFS streams
- Hide files

Lab Environment

To carry out the lab you need:

- A computer running **Windows Server 2008** as virtual machine
- Formatted **C:** drive NTFS

Lab Duration

Time: 15 Minutes

Overview of NTFS Streams

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

NTFS supersedes the FAT file system as the preferred **file system** for Microsoft Windows operating systems. **NTFS** has several **improvements** over FAT and **HPFS** (High Performance File System), such as improved support for **metadata** and the use of advanced **data structures**.

Lab Tasks

TASK 1

NTFS Streams

1. Run this lab in Windows Server 2008 virtual machine
2. Make sure the **C:\ drive** is formatted for **NTFS**.
3. Create a folder called **magic** on the **C:** drive and copy **calc.exe** from **C:\windows\system32** to **C:\magic**.
4. Open a command prompt and go to **C:\magic** and type **notepad readme.txt** in command prompt and press **Enter**.
5. **readme.txt** in Notepad appears. (Click **Yes** button if prompted to create a new **readme.txt** file.)
6. Type **Hello World!** and **Save** the file.

NTFS stream runs on Windows Server 2008

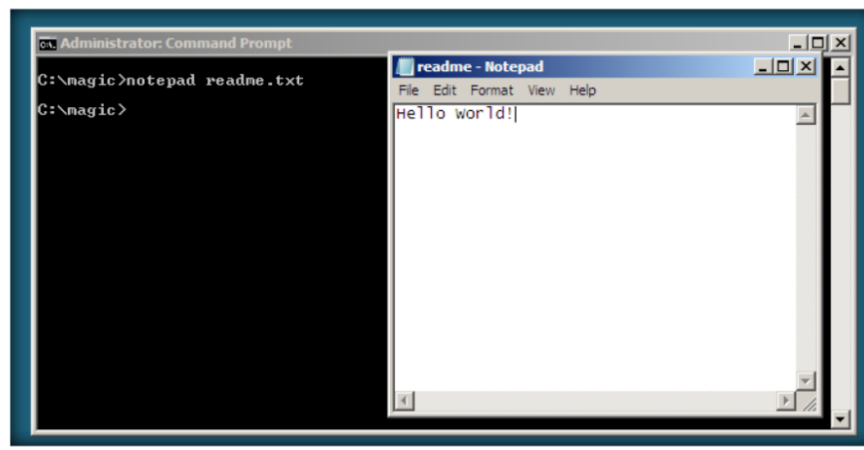


FIGURE 2.1: Command prompt with "notepad readme.txt" command

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

   type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe

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

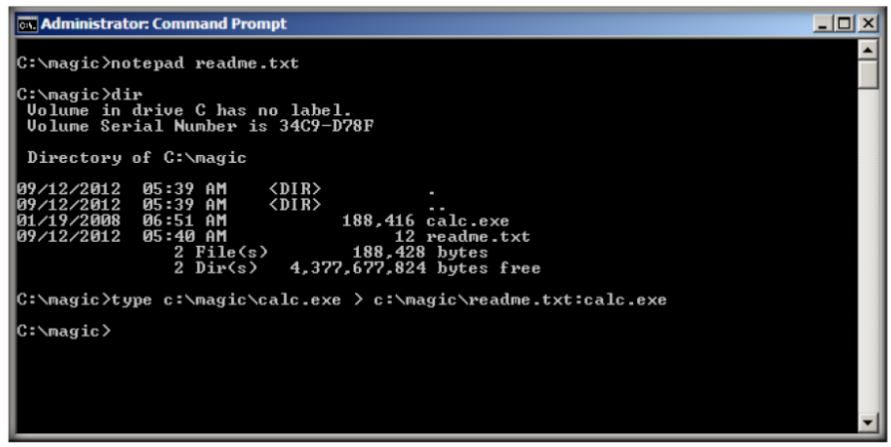


FIGURE 2.2: Command prompt with hiding calc.exe command

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

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

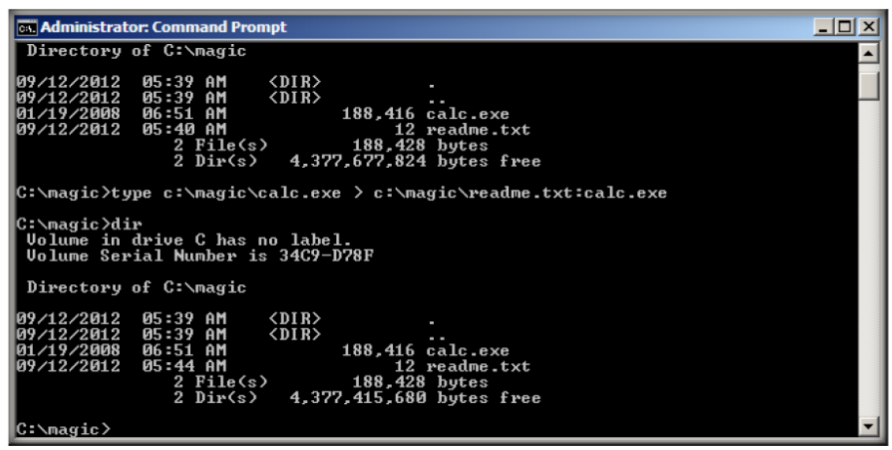


FIGURE 2.3: Command prompt with executing hidden calc.exe command

10. The file **size** of the readme.txt **should not change**. Now navigate to the directory **c:\magic** and **delete calc.exe**.
11. Return to the command prompt and type command:

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

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

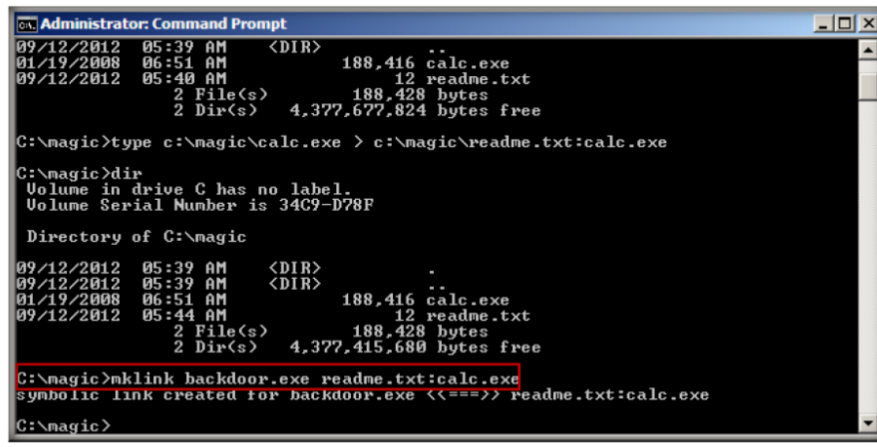


FIGURE 2.4: Command prompt linking the executed hidden calc.exe

12. Type **backdoor**, press **Enter**, and the the calculator program will be **executed**.

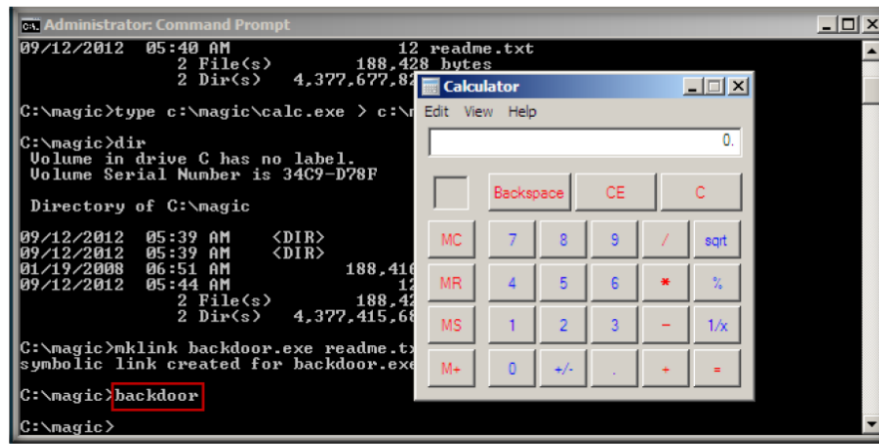


FIGURE 2.5: Command prompt with executed hidden calc.exe

Lab Analysis

Document all the results discovered during the lab.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

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

Questions

1. Evaluate alternative methods to hide the other exe files (like calc.exe).

Internet Connection Required	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Lab 3

Find Hidden Files Using ADS Spy

Ads Spy is a tool used to list, view, or delete Alternate Data Streams (ADS) on Windows Server 2008 with NTFS file systems.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

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 exit in computer networks and countermeasures to help prevent these vulnerabilities from being exploited on your systems. In order to be an expert ethical hacker and penetration tester, you must understand how to find hidden files using ADS Spy.

Lab Objectives

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

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

Lab Environment

To carry out the lab you need:

- ADS Spy located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\NTFS Stream Detector Tools\ADS Spy**
- You can also download the latest version of **ADS Spy** from the link http://www.merijn.nu/programs.php#adsspy
- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- Run this tool in **Windows Server 2012**

Lab Duration

Time: 10 Minutes

Overview of ADS Spy

An ADS (Alternate Data Stream) is a technique used to store meta-info on files.

ADS Spy is a tool used to list, view, or delete Alternate Data Streams (ADS) on **Windows Server 2008** with NTFS file systems. ADS Spy is a method of storing **meta-information** of files, without actually storing the information inside the file it belongs to.

Lab Tasks

TASK 1

Alternative Data Streams

1. Navigate to the CEH-Tools directory **D:\CEH-Tools\CEHv8 Module 05 System Hacking\NTFS Stream Detector Tools\ADS Spy**
2. Double-click and launch **ADS Spy**.

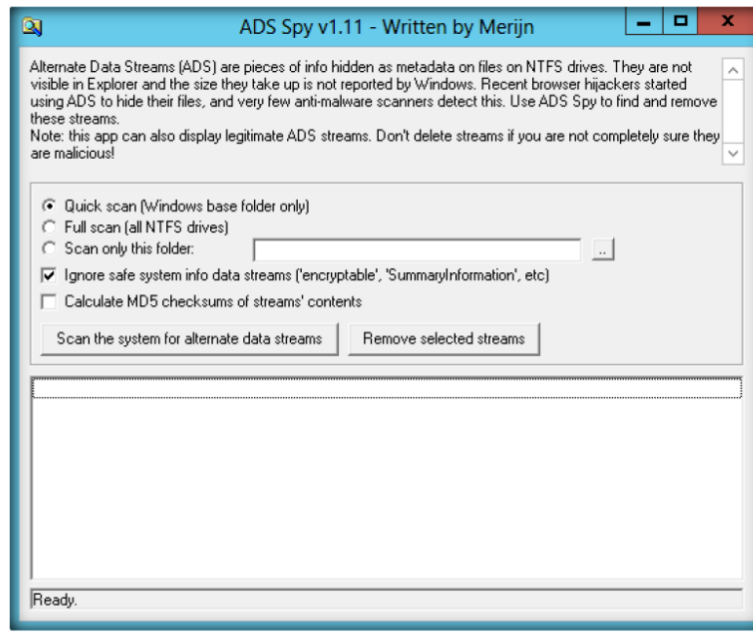


FIGURE 3.1 Welcome screen of ADS Spy

ADS Spy is a small tool to list, view, or delete Alternate Data Streams (ADS) on Windows 2012 with NTFS file systems.

3. Start an **appropriate scan** that you need.
4. Click **Scan the system for alternate data streams**.

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

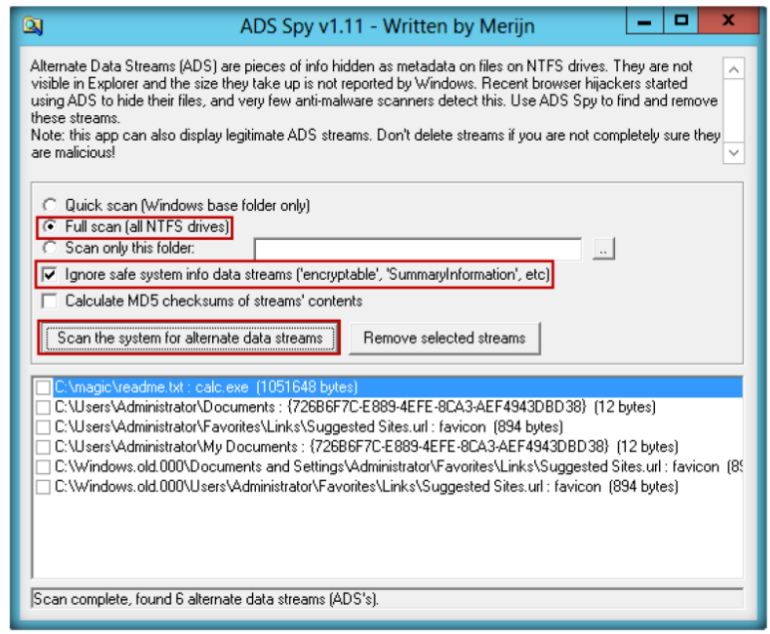


FIGURE 3.2 ADS Spy window with Full Scan selected

5. Find the **ADS hidden info file** while you scan the system for alternative data streams.
6. To remove the Alternate Data Stream, click **Remove selected streams**.

Compatible with: Windows Server 2012, 20008

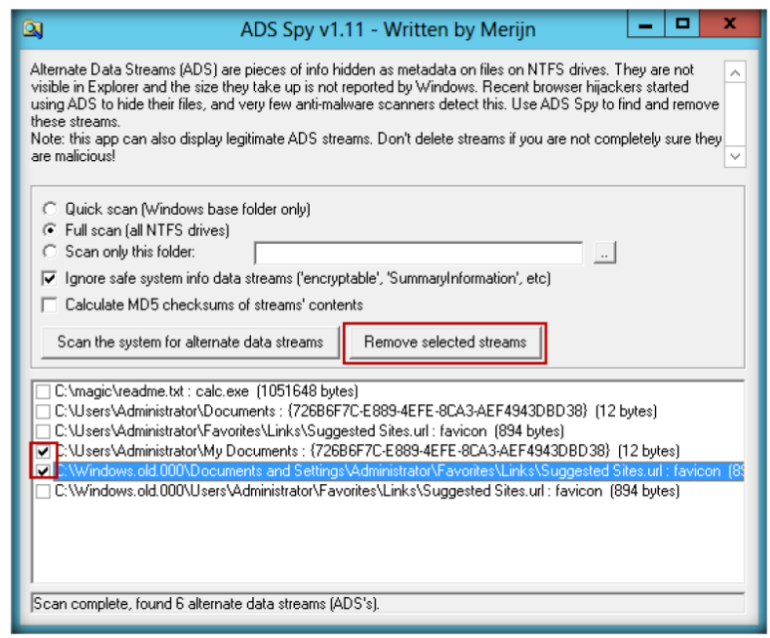


FIGURE 3.3: Find the hidden stream file

Lab Analysis

Document all the results and reports gathered during the lab.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
ADS Spy	**Scan Option:** Full Scan (all NTFS drives)
	Output: ▪ Hidden files with its location ▪ Hidden files size

Questions

1. Analyze how ADS Spy detects NTFS streams.

Internet Connection Required	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Lab 4

Hiding Files Using the Stealth Files Tool

Stealth Files use a process called steganography to hide any files inside of another file. It is an alternative to encryption of files.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

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 an expert ethical hacker and penetration tester, 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.

Lab Objectives

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

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

Lab Environment

To carry out this lab you need:

- **Stealth Files** tool located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Steganography\Audio Steganography\Stealth Files**
- A computer running **Window Server 2012** (host machine)
- You can also download the latest version of **Stealth Files** from the link http://www.froebis.com/english/sf40.shtml

- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- Administrative privileges to run the **Stealth files** tool
- Run this tool in Windows Server 2012 (Host Machine)

Lab Duration

Time: 15 Minutes

Overview of Stealth Files Tool

Stenography is the art and science of writing hidden messages.

Stealth files use a process called **steganography** to hide any files inside of another file. It is an alternative to encryption of files because no one can decrypt the encrypted information or data from the files unless they know that the hidden files exist.

Lab Tasks

TASK 1

Stenography

1. Follow the wizard-driven installation instructions to install **Stealth Files Tool**.
2. Launch **Notepad** and write **Hello World** and save the file as **Readme.txt** on the desktop.

Stealth Files uses a process called steganography to hide any file or files inside of another file

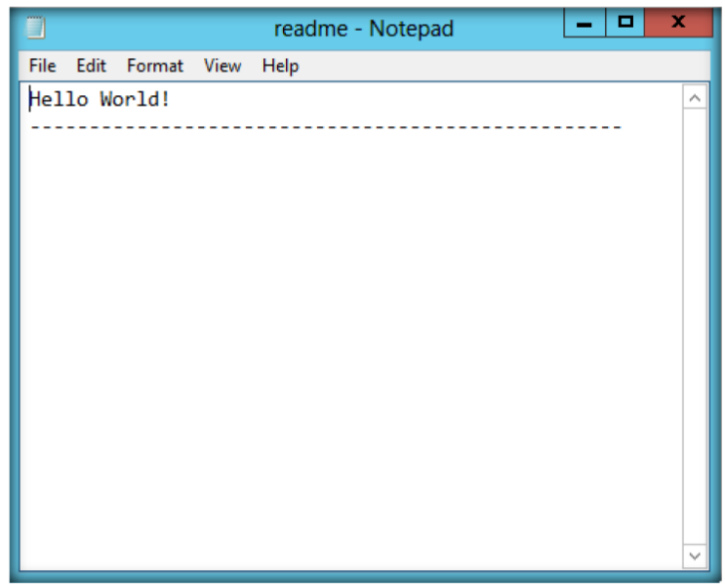


FIGURE 4.1: Hello world in readme.txt

3. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

FIGURE 4.2: Windows Server 2012 – Desktop view

4. Click the **Stealth Files 4.0** app to open the **Stealth File** window.

You can also download Stealth File from http://www.froebis.com.

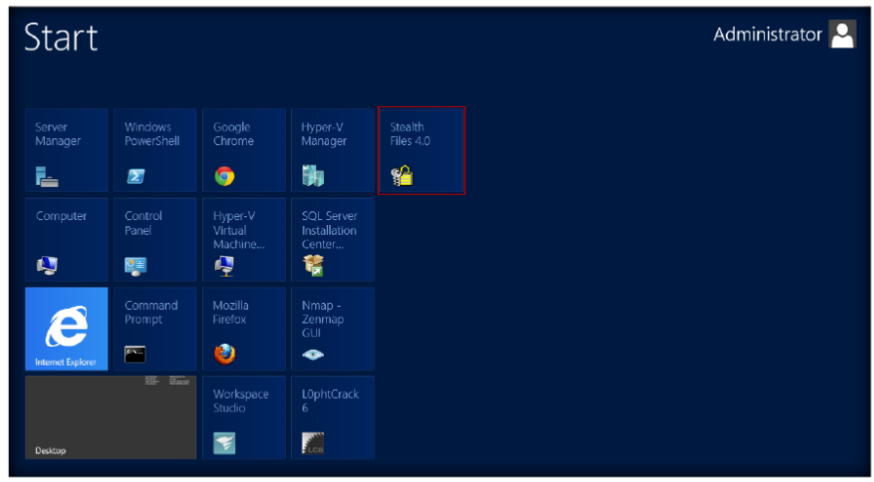


FIGURE 4.3: Windows Server 2012 – Apps

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

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

FIGURE 4.4: Control panel of Stealth Files

6. Click **Hide Files** to start the process of hiding the files.
7. Click **Add files**.

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

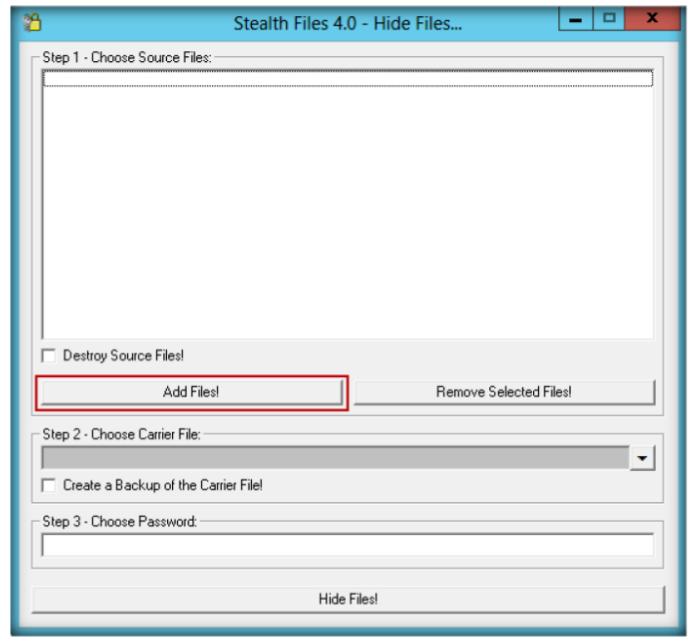


FIGURE 4.5: Add files Window

8. **In Step1,** add the **Calc.exe** from **c:\windows\system32\calc.exe**.
9. **In Step 2,** choose the carrier file and add the file **Readme.txt** from the **desktop**.
10. **In Step 3,** choose a password such as **magic** (you can type any desired password).

Stealth Files 4.0 can be downloaded from the link: http://www.froebis.com/english/sf40.shtml

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

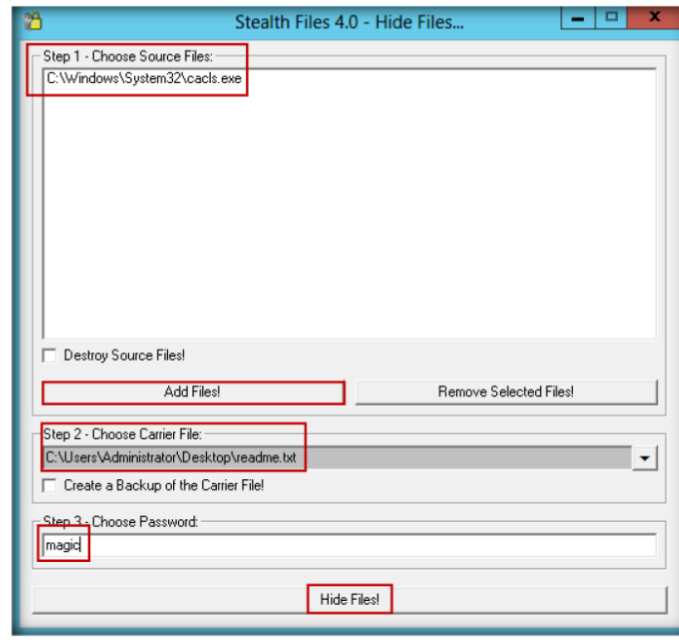


FIGURE 4.6: Step 1-3 Window

11. Click **Hide Files**.
12. It will hide the file **calc.exe** inside the **readme.txt** located on the desktop.
13. 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 prompted to enter it again to recover the hidden files

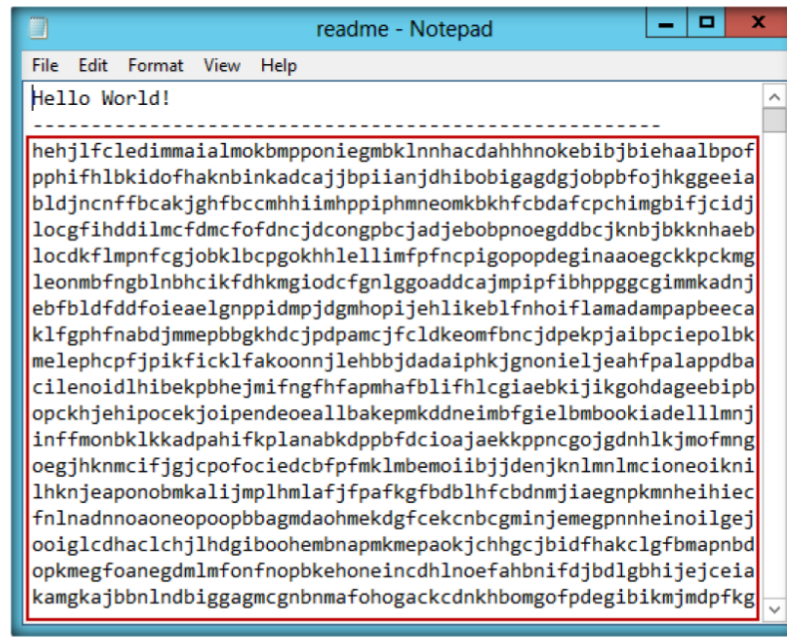


FIGURE 4.7: Calc.exe copied inside notepad.txt

14. 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

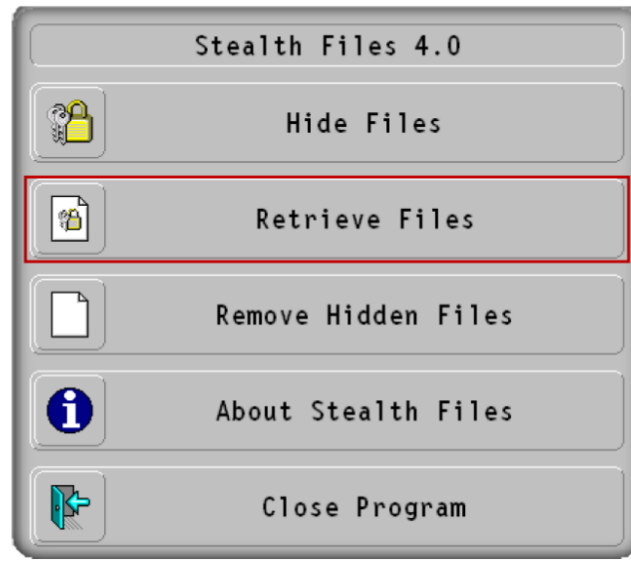


FIGURE 4.8: Stealth files main window

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

This carrier file can be any of these file types: **EXE, DLL, OCX, COM, JPG, GIF, ART, MP3, AVI,** WAV, DOC, BMP, and WMF. Most audio, video, and executable files can also be carrier files

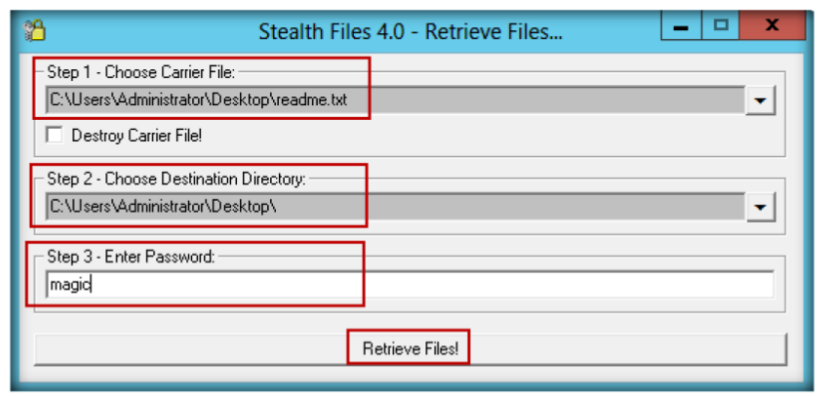


FIGURE 4.9: Retrieve files main window

18. The retrieved file is stored on the **desktop**.

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

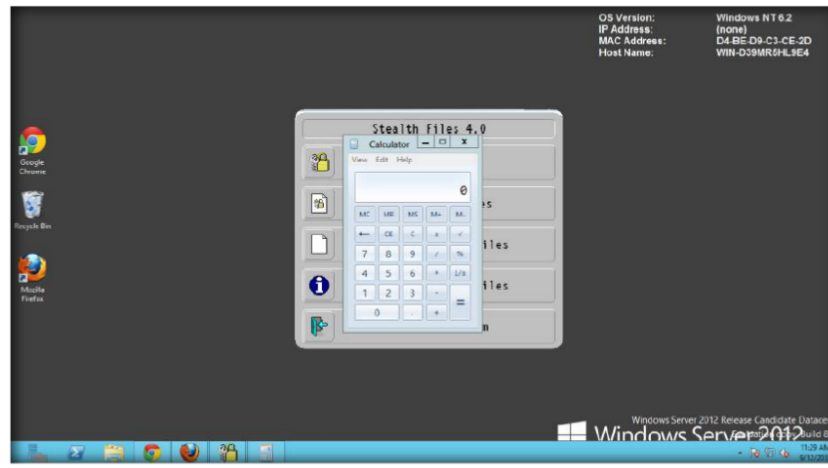


FIGURE 4.10: Calc.exe running on desktop with the retrieved file

Lab Analysis

Document all the results and reports gathered during the lab.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

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

Questions

1. Evaluate other alternative parameters for hiding files.

Internet Connection Required	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Lab 5

Extracting SAM Hashes Using PWdump7 Tool

Pwdump7 can also be used to dump protected files. You can always copy a used file by just executing: pwdump7.exe -d c:\lockedfile.dat backup-lockedfile.dat. Icon key.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook 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 worry, this chink in the armour can come to your rescue. By using password cracking tools or password cracking technologies that allows hackers to steal password can be used to recover them legitimately. In order to be an expert ethical hacker and 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.

Lab Objectives

This lab teaches you how to:

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

Lab Environment

To carry out the lab you need:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

- **Pwdump7** located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Password Cracking Tools\pwdump7**
- Run this tool on **Windows Server 2012**
- You can also download the latest version of **pwdump7** from the link http://www.tarasco.org/security/pwdump_7/index.html
- Administrative privileges to run tools

- **TCP/IP** settings correctly configured and an accessible DNS server
- Run this lab in **Windows Server 2012** (host machine)

Lab Duration

Time: 10 Minutes

Overview of Pwdump7

Pwdump7 can be used to dump protected files. You can always copy a used file just by executing: pwdump7.exe -d c:\lockedfile.dat backup-lockedfile.dat. Icon key

Lab Tasks

TASK 1

Generating Hashes

1. Open the command prompt and navigate to **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Password Cracking Tools\pwdump7**.
2. Alternatively, you can also navigate to **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Password Cracking Tools\pwdump7**and right-click the **pwdump7** folder and select **CMD prompt here** to open the command prompt.

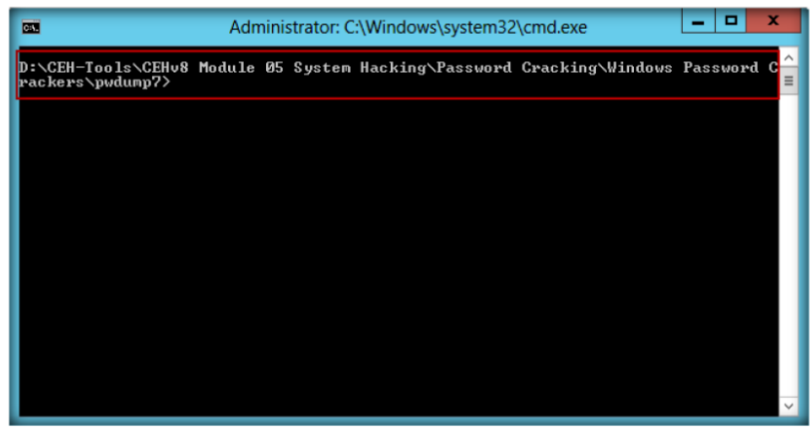


FIGURE 5.1: Command prompt at pwdump7 directory

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

3. Now type **pwdump7.exe** and press **Enter**, which will display all the password hashes.

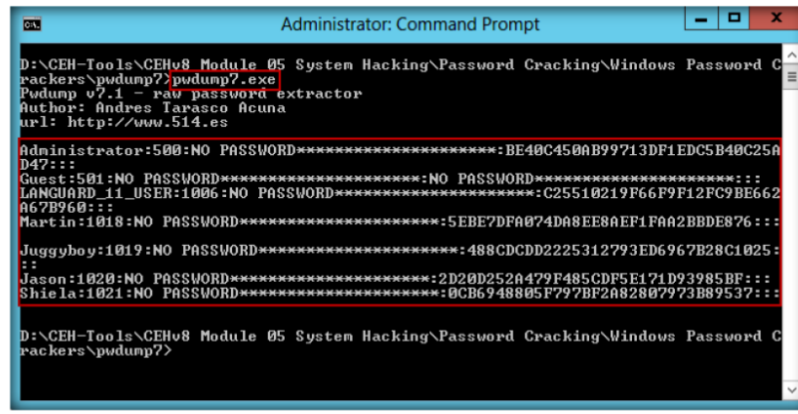


FIGURE 5.2: pwdump7.exe result window

Always copy a used file just executing: pwdump7.exe -d c:\lockedfile.dat backup-lockedfile.dat.

4. Now type **pwdump7.exe > c:\hashes.txt** in the command prompt, and press **Enter**.
5. 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.)

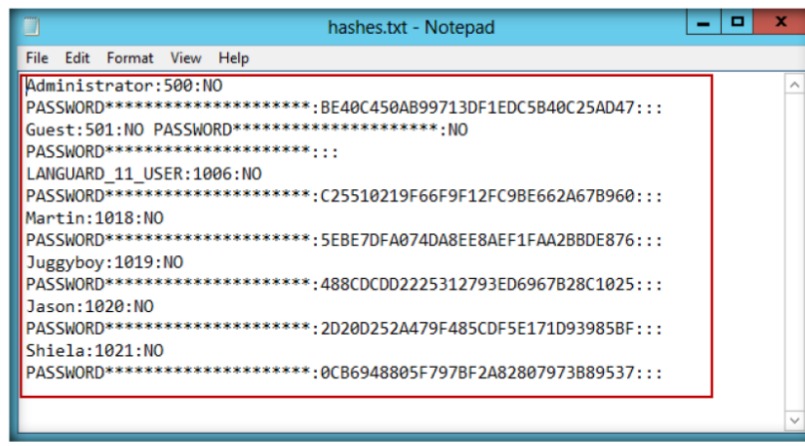


FIGURE 5.3: hashes.txt window

Lab Analysis

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

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
PWdump7	**Output:** List of User and Password Hashes ▪ Administrator ▪ Guest ▪ Lauguard ▪ Martin ▪ Juggyboy ▪ Jason ▪ shiela

Questions

1. What is pwdump7.exe command used for?
2. How do you copy the result of a command to a file?

Internet Connection Required	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Lab 6

Creating the Rainbow Tables Using Winrtgen

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.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In computer and information security, the use of password is essential for users to protect their data to ensure a secured 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 system users' passwords. In order to be an expert ethical hacker and penetration tester, you must understand how to create rainbow tables to crack the administrator password.

Lab Objectives

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

Lab Environment

To carry out the lab, you need:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

- **Winrtgen** Tool located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Rainbow Table Creation Tools\Winrtgen**
- A computer running **Window Server 2012**
- You can also download the latest version of **Winrtgen** from the link http://www.oxid.it/projects.html
- If you decide to download the latest version, then screenshots shown in the lab might differ

- Run this tool on **Windows Server 2012**
- Administrative privileges to run this program

Lab Duration

Time: 10 Minutes

You can also download Winrtge from http://www.oxid.it/projects.html

Overview of Rainbow Table

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.

Lab Task

TASK 1

Generating Rainbow Table

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

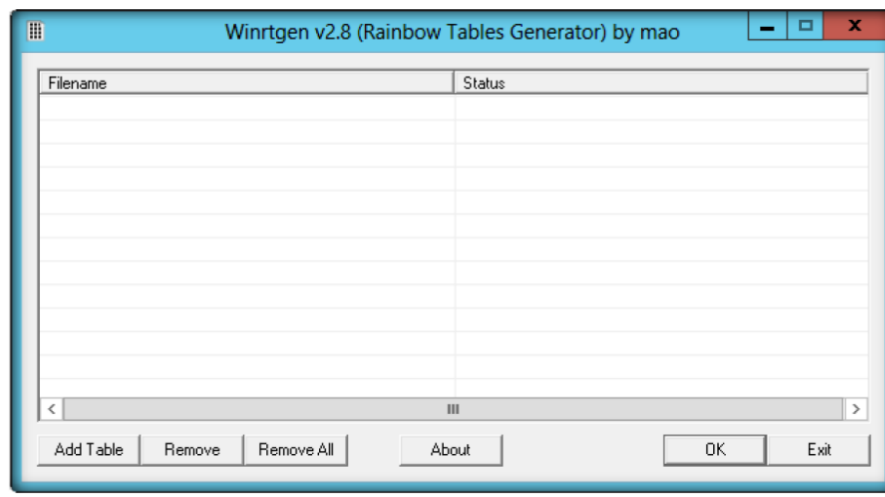


FIGURE 6.1: winrtgen main window

Rainbow tables usually used to crack a lot of hash types such as NTLM, MD5, SHA1

2. Click the **Add Table** button.

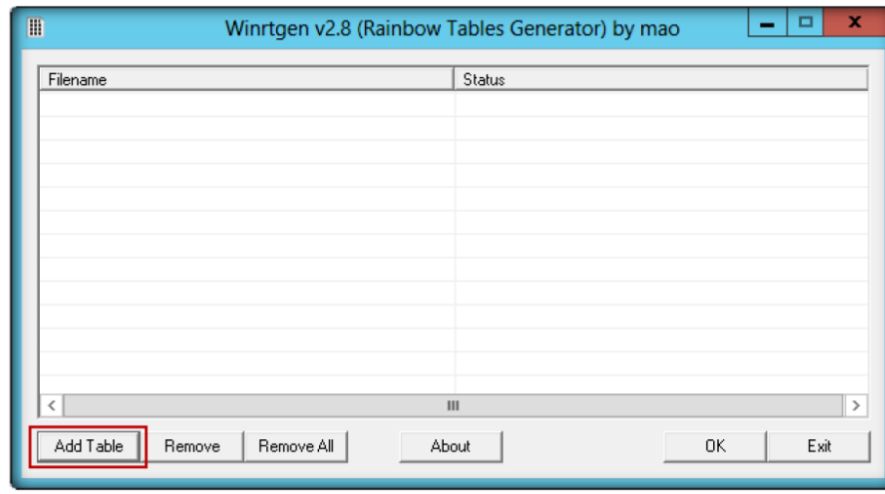


FIGURE 6.2: creating the rainbow table

3. **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 **4000000**.
   iii. Select **loweralpha** from the **Charset** drop-down list (this depends on the password).
4. Click **OK**.

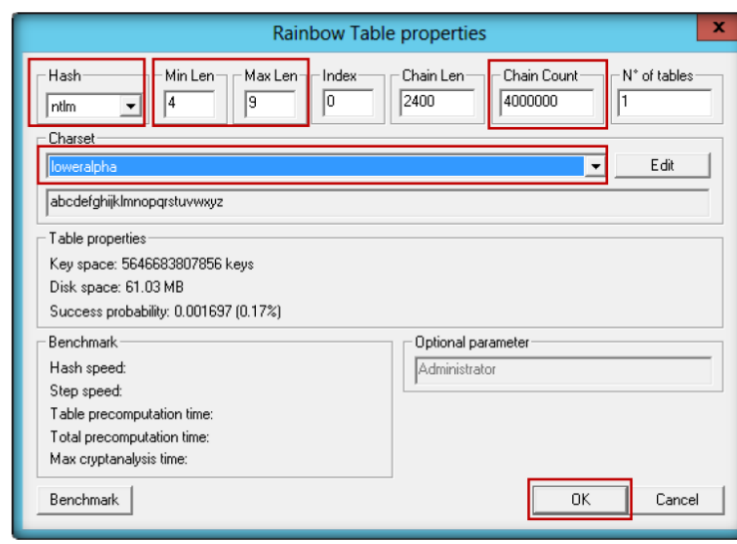


FIGURE 6.3: selecting the Rainbow table properties

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

You can also download Winrtge from http://www.oxid.it/projects.html.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

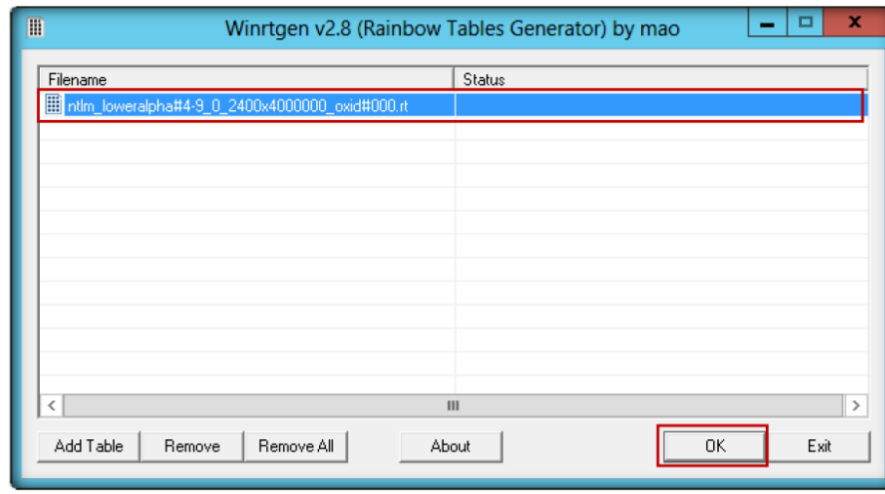


FIGURE 6.4: Alchemy Remote Executor progress tab window

6. Creating the hash table will take some time, depending on the selected hash and charset.

   Note: To save the time for the lab demonstration, the generated hash table is kept in the following folder: **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Rainbow Table Creation Tools\Winrtgen**

You must be careful of your harddisk space. Simple rainbow table for 1 – 5 alphanumeric and it costs about 613MB of your harddisk.

7. Created a hash table saved automatically in the folder containing **winrtgen.exe**.

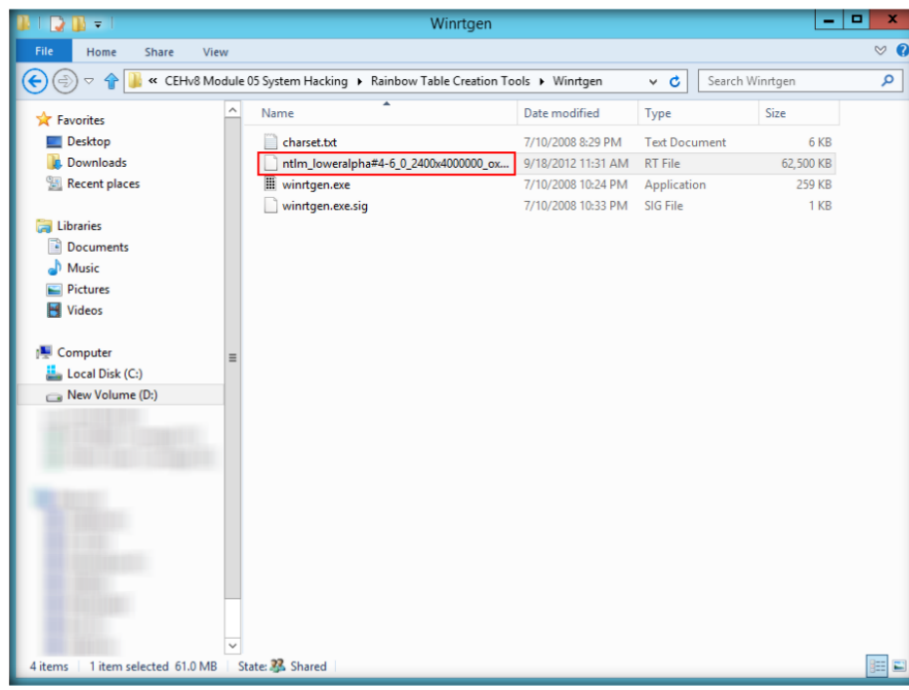


FIGURE 6.5: Generated Rainbow table file

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
Winrtge	**Purpose:** Creating Rainbow table with lower alpha
	Output: Created Rainbow table: ntlm_loweralpha#4-6_0_2400X4000000_ox…

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 7

Password Cracking Using RainbowCrack

RainbowCrack is a computer program that generates rainbow tables to be used in password cracking.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

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, no laborious tasks, only simple words or programs. In order to be an ethical hacker and penetration tester, you must understand how to crack administrator password. In this lab we discuss how to crack guest users or administrator passwords using RainbowCrack.

Lab Objectives

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

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

Lab Environment

To carry out the lab, you need:

- **RainbowCrack** Tool located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Rainbow Table Creation Tools\RainbowCrack**
- A computer running **Window Server 2012**
- You can also download the latest version of **RainbowCrack** from the link http://project-rainbowcrack.com/

You can also download Winrtge from http://www.oxid.it/projects.html

- If you decide to download the latest version, then screenshots shown in the lab might differ
- Run this tool on **Windows Server 2012**
- Administrative privileges to run this program

Lab Duration

Time: 10 Minutes

Overview of RainbowCrack

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.

Lab Task

TASK 1

Generating the Rainbow Table

1. Double-click the **rcrack_gui.exe** file. The main window of RainbowCrack is shown in the following figure.

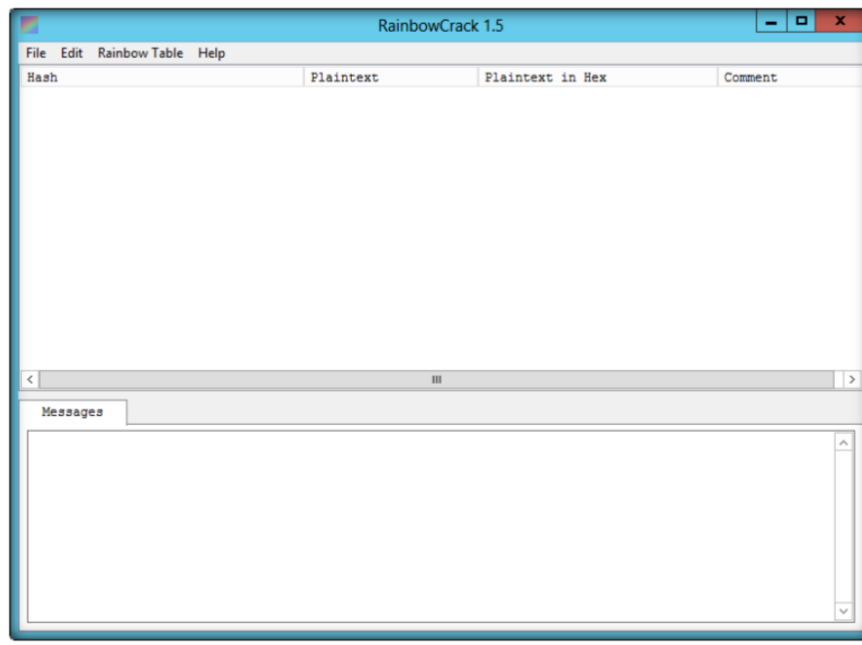


FIGURE 7.1: RainbowCrack main window

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

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

RainbowCrack for GPU is significantly faster than any non-GPU accelerated rainbow table lookup program and any straight GPU brute forcing cracker

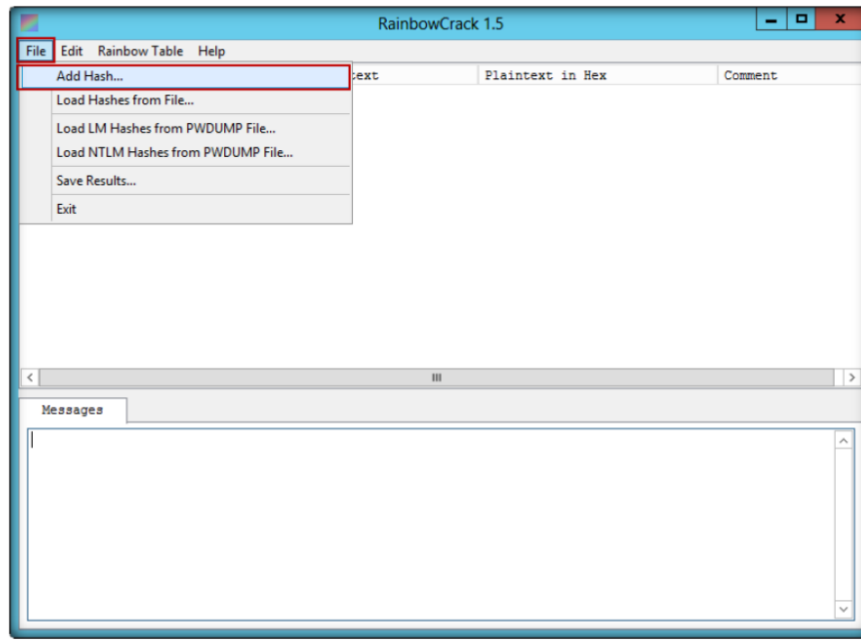


FIGURE 7.2: Adding Hash values

3. The **Add Hash** window appears:
   i. Navigate to **c:\hashes**, and open the **hashes.txt** file (which is already generated using Pwdump7 located at **c:\hashes.txt** in the previous **Lab no:5**) .
   ii. Right-click, copy the hashes from **hashes.txt** file.
   iii. Paste into the **Hash** field, and give the comment (optional).
   iv. Click **OK**.

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

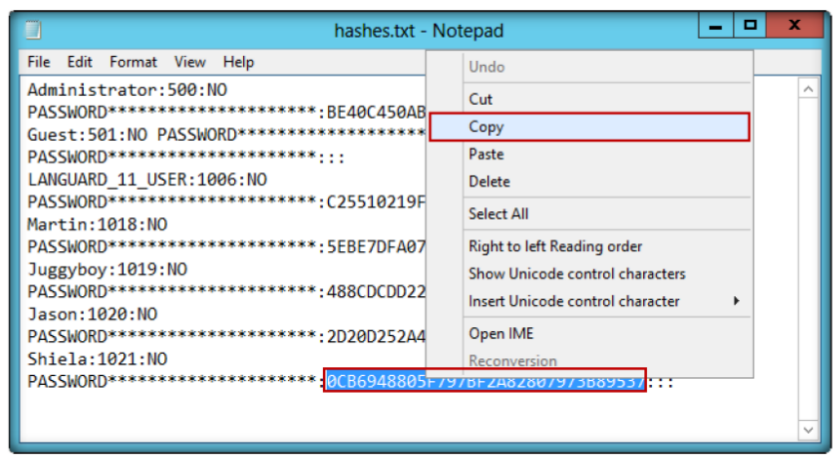


FIGURE 7.3: Selecting the hashes

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

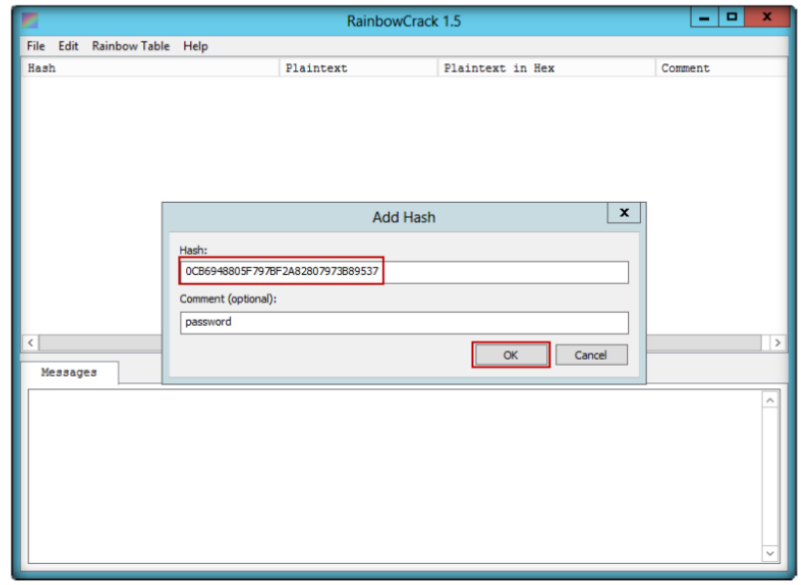


FIGURE 7.4: Adding Hashes

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

Full time-memory tradeoff tool suites, including rainbow table generation, sort, conversion and lookup

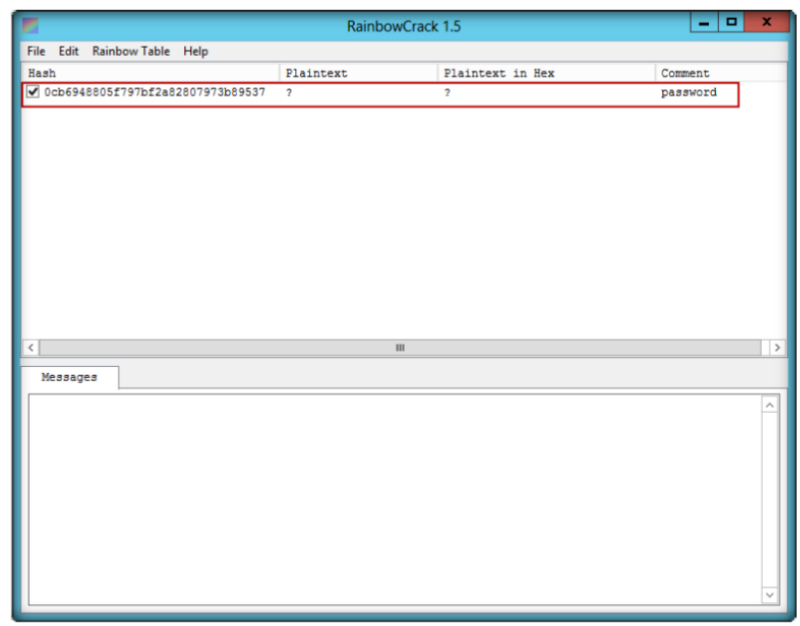


FIGURE 7.5: Added hash show in window

5. To add more hashes, repeat steps **2 & 3 (i,ii,iii,iv)**.
6. Added hashes are shown in the following figure.

RainbowCrack's purpose is to generate rainbow tables and not to crack passwords per-se, some organizations have endeavored to make RainbowCrack's rainbow tables available free over the internet.

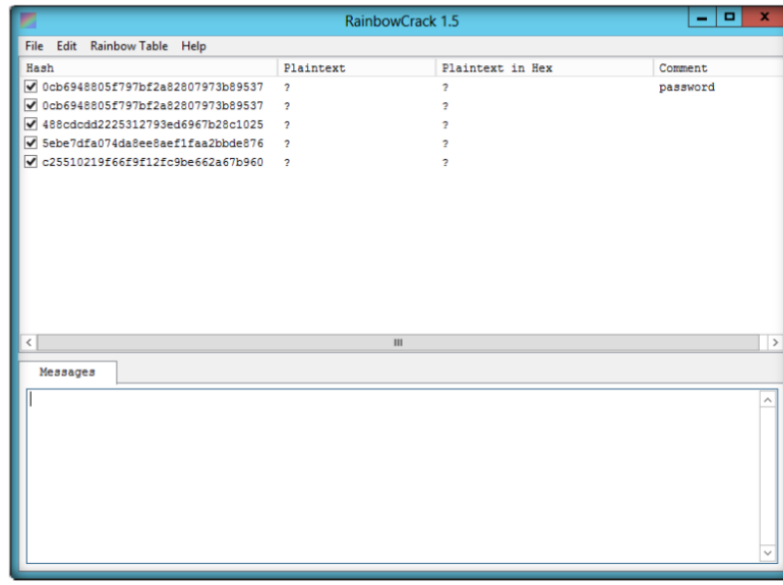


FIGURE 7.6: Added Hashes in the window

7. Click the **Rainbow Table** from the menu bar, and click **Search Rainbow Table...**

RainbowCrack for GPU software uses GPU from NVIDIA for computing, instead of CPU. By offloading computation task to GPU, the RainbowCrack for GPU software can be tens of times faster than non-GPU version.

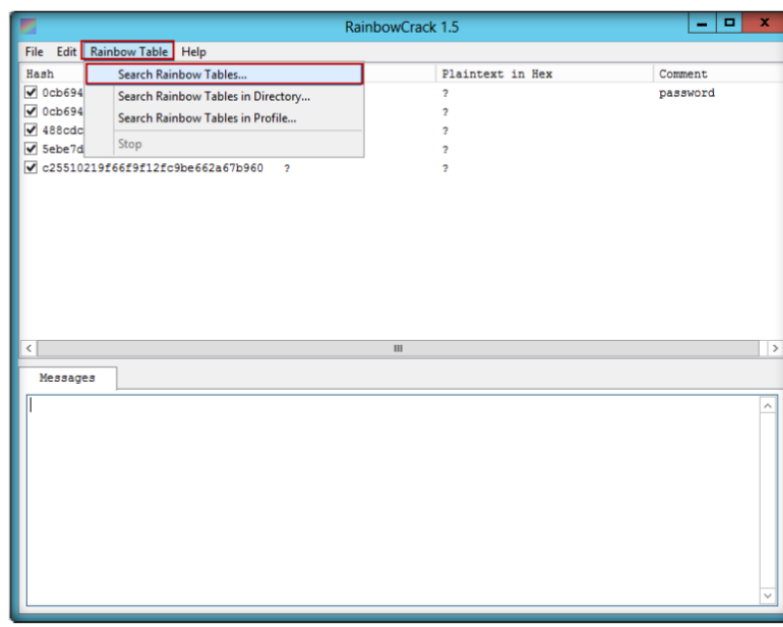


FIGURE 7.7: Added Hashes in the window

8. Browse the **Rainbow Table** that is already generated in the previous lab, which is located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Rainbow Table Creation Tools\Winrtgen**.
9. Click **Open**.

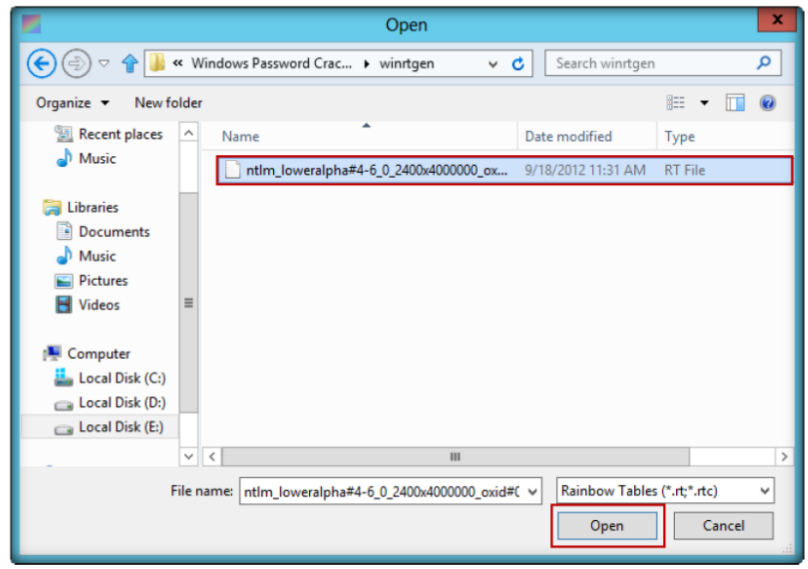
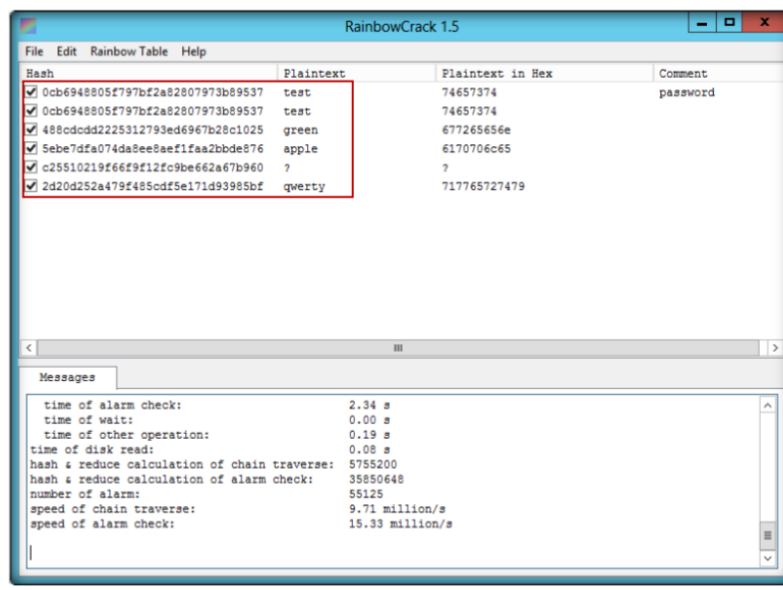


FIGURE 7.8: Added Hashes in the window

A time-memory tradeoff hash cracker need a pre-computation stage, at the time all plaintext/hash pairs within the selected hash algorithm, charset, plaintext length are computed and results are stored in files called rainbow table

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



RainbowCrack focus on the development of optimized time-memory tradeoff implementation, and generation of large rainbow tables.

FIGURE 7.9: Added Hashes in the window

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
RainbowCrack	**Hashes:** ▪ Administrator ▪ Guest ▪ Languard ▪ Martin ▪ Juggyboy ▪ Jason ▪ Shiela
	Password Cracked: ▪ test ▪ test ▪ green ▪ apple ▪ qwerty

Questions

1. What kind of hashes does RainbowCrack support?

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 8

Extracting Administrator Passwords Using L0phtCrack

L0phtCrack is packed with powerful features, such as scheduling, hash extraction from 64-bit Windows versions, multiprocessor algorithms, and network monitoring and decoding. It can import and crack UNIX password files and remote Windows machines.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Since security and compliance are high priorities for most organizations, attacks on a company or organization's computer systems take many different forms, such as spoofing, smurfing, and other types of denial-of-service (DoS) attacks. These attacks are designed to harm or interrupt the use of your operational systems.

Password cracking is a term used to describe the penetration of a network, system, or resource with or without the use of tools to unlock a resource that has been secured with a password. In this lab we will look at what password cracking is, why attackers do it, how they achieve their goals, and what you can do to do to protect yourself. Through an examination of several scenarios, in this lab we describe some of the techniques they deploy and the tools that aid them in their assaults and how password crackers work both internally and externally to violate a company's infrastructure.

In order to be an expert ethical hacker and penetration tester, you must understand how to crack administrator passwords. In this lab we crack the system user accounts using LOphtCrack.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

Lab Objectives

The lab teaches you how to:

- Use the **L0phtCrack** tool
- Crack **administrator** passwords

Lab Environment

To carry out the lab you need:

- **L0phtCrack** tool located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Password Cracking Tools\L0phtCrack**
- Run this tool on **Windows Server 2012** (host machine)
- You can also download the latest version of **L0phtCrack** from the link http://www.l0phtcrack.com
- Administrative privileges to run tools
- Follow wizard driven installation instructions
- **TCP/IP** settings correctly configured and an accessible DNS server
- This tool requires the **user** to register or you can also use the evaluation version for a limited period of time

Lab Duration

Time: 10 Minutes

Overview of L0phtCrack

L0phtCrack provides a scoring metric to quickly assess **password quality**. Passwords are measured against current industry **best practices** and are rated as **Strong, Medium, Weak**, or **Fail.**

Lab Tasks

TASK 1

Cracking Administrator Password

1. Launch the **Start** menu by hovering the mouse cursor to the lower left most corner of the desktop.

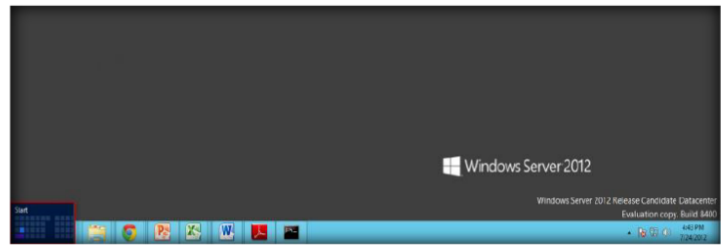


FIGURE 8.1: Windows Server 2012 – Desktop view

2. Click the **LOphtCrack6** app to open the **LOphtCrack6** window.

You can also download the L0phtCrack from http://www.l0phtcrack.com.

L0phtCrack supports pre-computed password hashes.

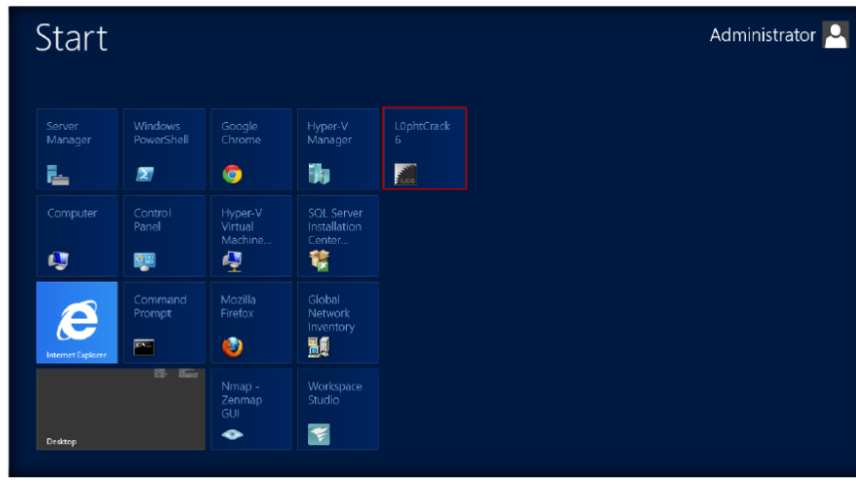


FIGURE 8.2: Windows Server 2012 – Apps

3. Launch **L0phtCrack,** and in the **L0phtCrack Wizard**, click **Next**.

L0phtCrack can also cracks UNIX password files.

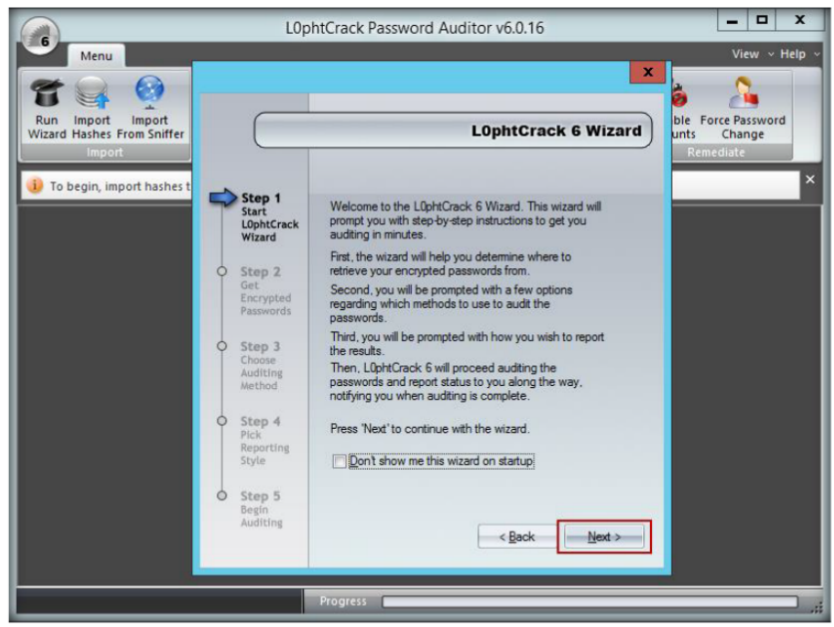


FIGURE 8.3: Welcome screen of the L0phtCrack Wizard

4. Choose **Retrieve from the local machine** in the **Get Encrypted Passwords** wizard and click **Next**.

FIGURE 8.4: Selecting the password from the local machine

L0phtCrack has a built-in ability to import passwords from remote Windows, including 64-bit versions of Vista, Windows 7, and UNIX machines, without requiring a third-party utility.

5. Choose **Strong Password Audit** from the **Choose Auditing Method** wizard and click **Next**.

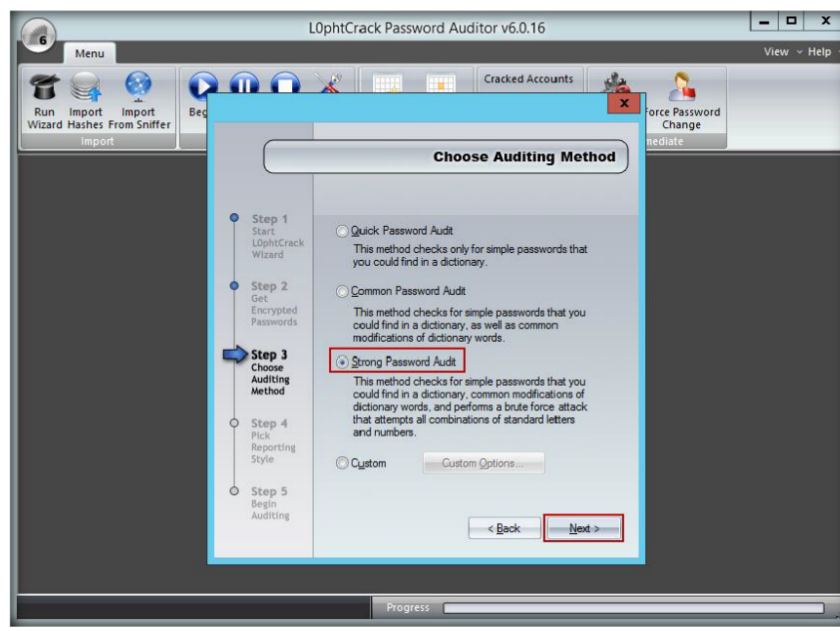


FIGURE 8.5: Choose a strong password audit

6. In **Pick Reporting Style**, select all **Display encrypted password hashes**.
7. Click **Next**.

L0phtCrack offers remediation assistance to system administrators.

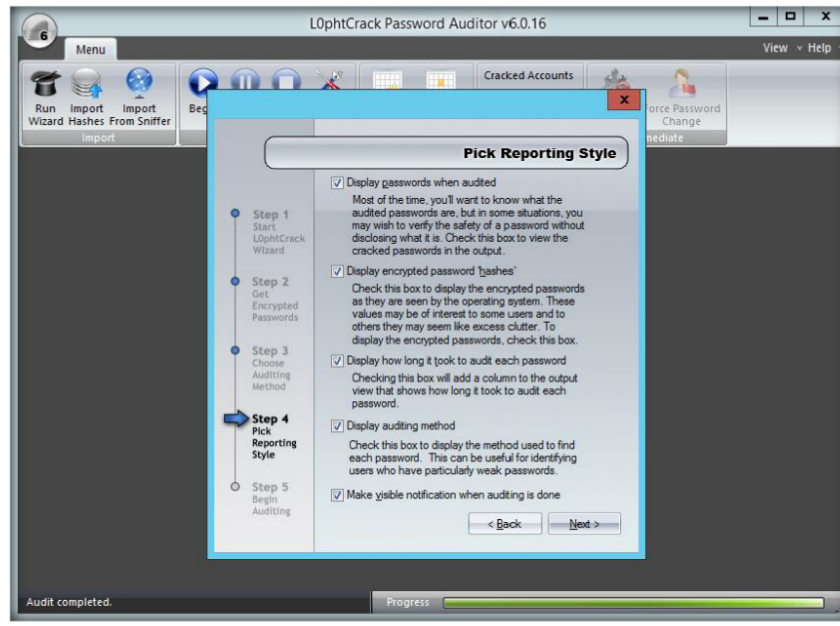


FIGURE 8.6: Pick Reporting Style

8. Click **Finish**.

L0phtCrack has real-time reporting that is displayed in a separate, tabbed interface.

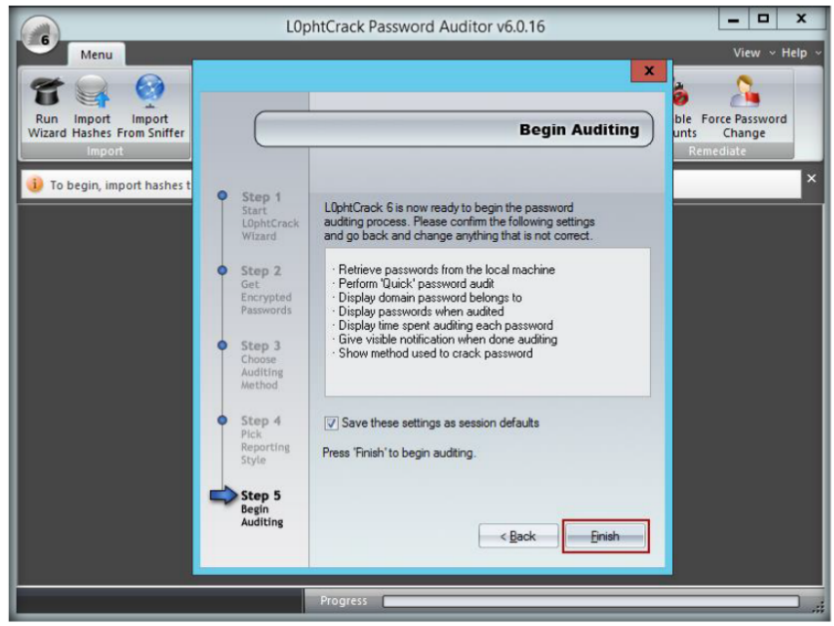


FIGURE 8.7: Begin Auditing

9. LOpntcrack6 shows an **Audit Completed** message, Click **OK**.
10. Click **Session options** from the menu bar.

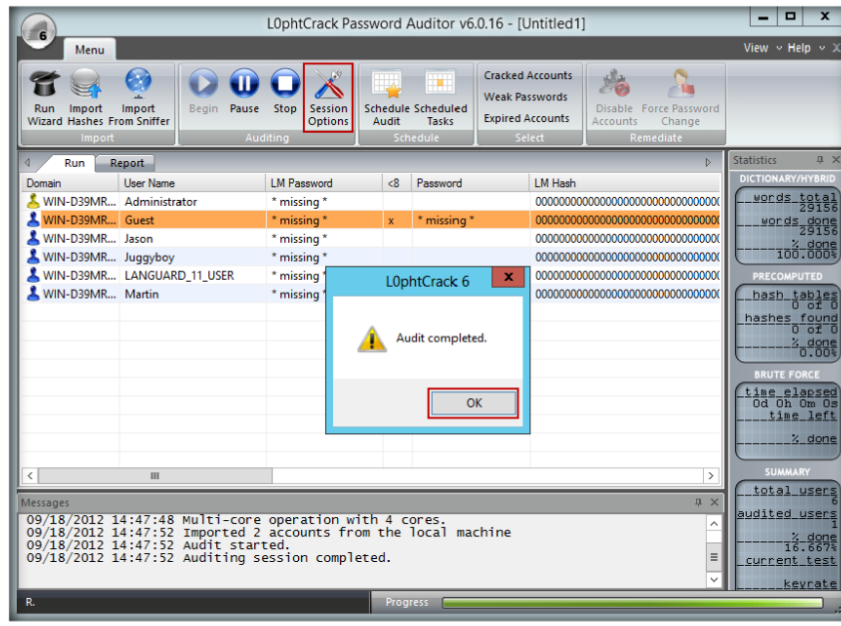


FIGURE 8.8: Selecting Session options

L0phtCrack uses Dictionary, Hybrid, Recomputed, and Brute Force Password auditing methods.

11. **Auditing options For This Session** window appears:
    i. Select the **Enabled**, **Crack NTLM Passwords** check boxes in **Dictionary Crack**.
    ii. Select the **Enabled**, **Crack NTLM Passwords** check boxes in **Dictionary/Brute Hybrid Crack**.
    iii. Select the **Enabled**, **Crack NTLM Passwords** check boxes in **Brute Force Crack**.
    iv. Select the **Enable Brute Force Minimum Character Count** check box.
    v. Select the **Enable Brute Force Maximum Character Count** check box.
12. Click **OK**.

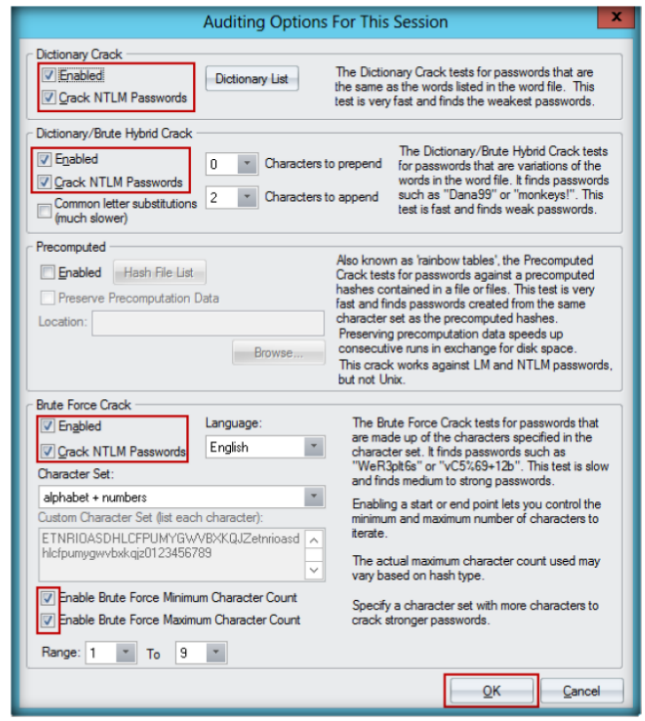


FIGURE 8.9: Selecting the auditing options

13. Click **Begin** from the menu bar. L0phtCrack cracks the **administrator password**.

14. A **report** is generated with the cracked passwords.

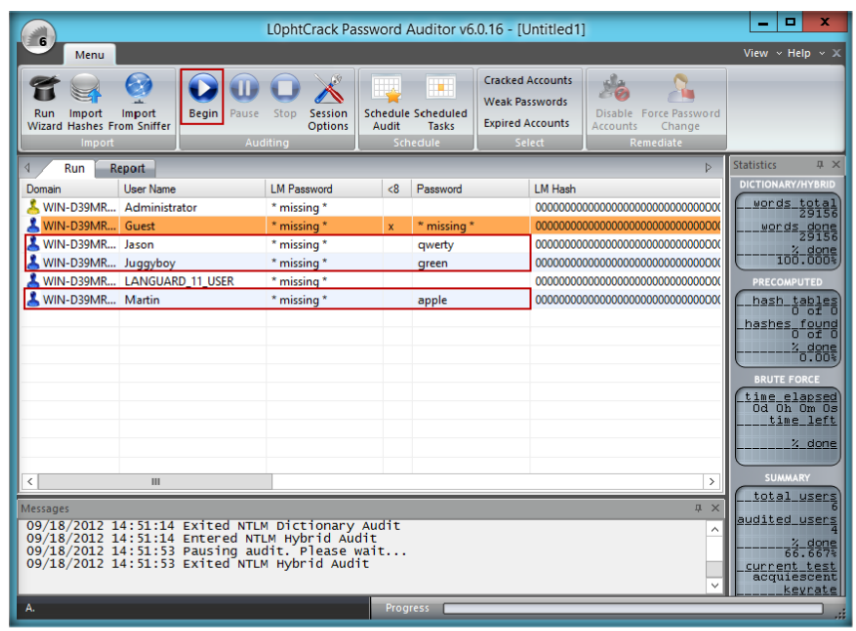


FIGURE 8.10: Generated cracked Password

Lab Analysis

Document all the results and reports gathered during the lab.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
LOphtCrack	**User Names:** ▪ Administrator ▪ Guest ▪ Jason ▪ Juggyboy ▪ LANGUARD_11_USER ▪ Martin
	Password Found: ▪ qwerty ▪ green ▪ apple

Questions

1. What are the alternatives to crack administrator passwords?
2. Why is a brute force attack used in the L0phtCrack tool?

Internet Connection Required	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Lab 9

Password Cracking Using Ophcrack

Ophcrack is a free open source (GPL licensed) program that cracks Windows passwords by using LM hashes through rainbow tables.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In a security system that allows people to choose their own passwords, those people tend to choose passwords that can be easily guessed. This weakness exists in practically all widely used systems instead of forcing users to choose well-chosen secrets that are likely to be difficult to remember. The basic idea is to ensure that data available to the attacker is sufficiently unpredictable to prevent an off-line verification of whether a guess is successful or not; we examine common forms of guessing attacks, password cracking utilities to develop examples of cryptographic protocols that are immune to such attacks. Poorly chosen passwords are vulnerable to attacks based upon copying information. In order to be an expert ethical hacker and penetration tester, you must understand how to crack the weak administrator or system user account password using password cracking tools. In this lab we show you how to crack system user accounts using Ophcrack.

Lab Objectives

The objective of this lab is to help students learn:

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

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

Lab Environment

To carry out the lab, you need:

- **OphCrack** tool located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Password Cracking Tools\Ophcrack**
- Run this tool on **Windows Server 2012** (Host Machine)
- You can also download the latest version of **L0phtCrack** from the link http://ophcrack.sourceforge.net/

- Administrative privileges to run tools
- Follow the wizard-driven installation instructions

Lab Duration

Time: 15 Minutes

Overview of OphCrack

Rainbow tables for LM hashes of alphanumeric passwords are provided for free by developers. By default, OphCrack is bundled with tables that allow it to crack passwords no longer than 14 characters using only alphanumeric characters.

Lab Task

TASK 1

Cracking the Password

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

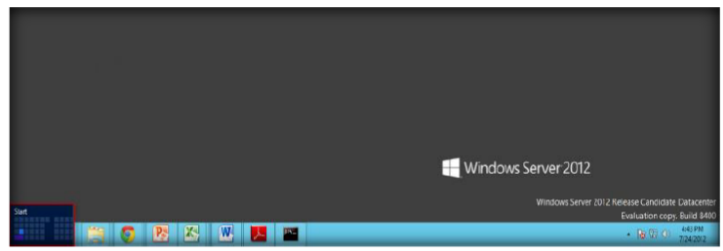


FIGURE 9.1: Windows Server 2012 – Desktop view

2. Click the **OphCrack** app to open the **OphCrack** window.

You can also download the 0phCrack from http://ophcrack.sourceforge.net.

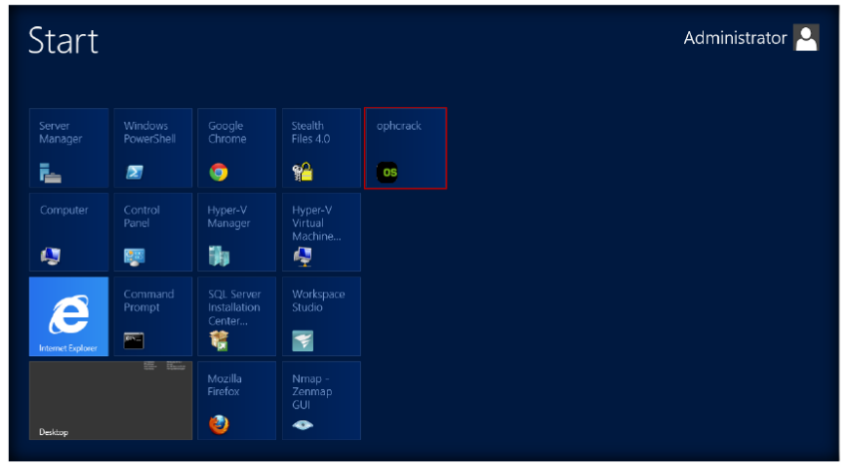


FIGURE 9.2: Windows Server 2012 – Apps

3. The **OphCrack** main window appears.

Rainbow tables for LM hashes of alphanumeric passwords are provided for free by the developers

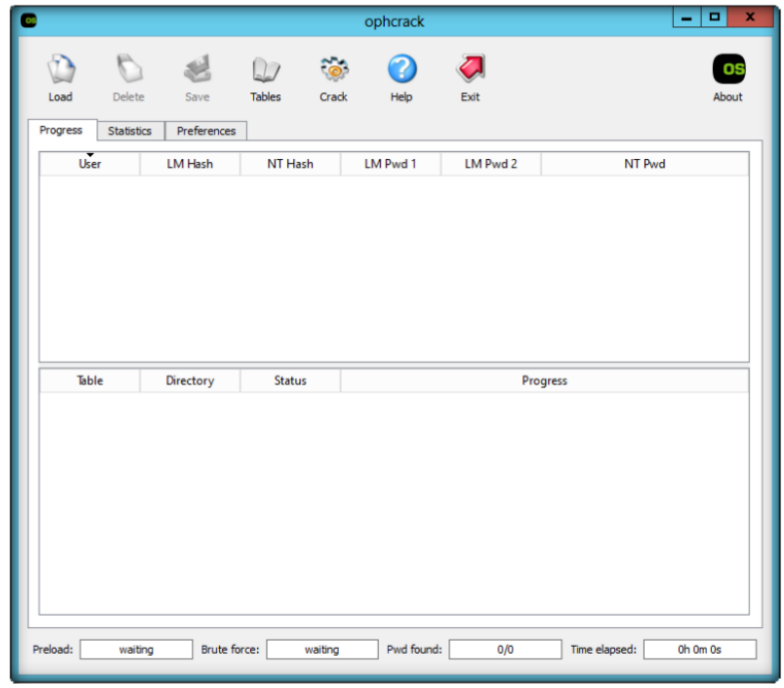


FIGURE 9.3: OphCrack Main window

4. Click **Load**, and then click **PWDUMP file**.

Ophcrack is bundled with tables that allows it to crack passwords no longer than 14 characters using only alphanumeric characters

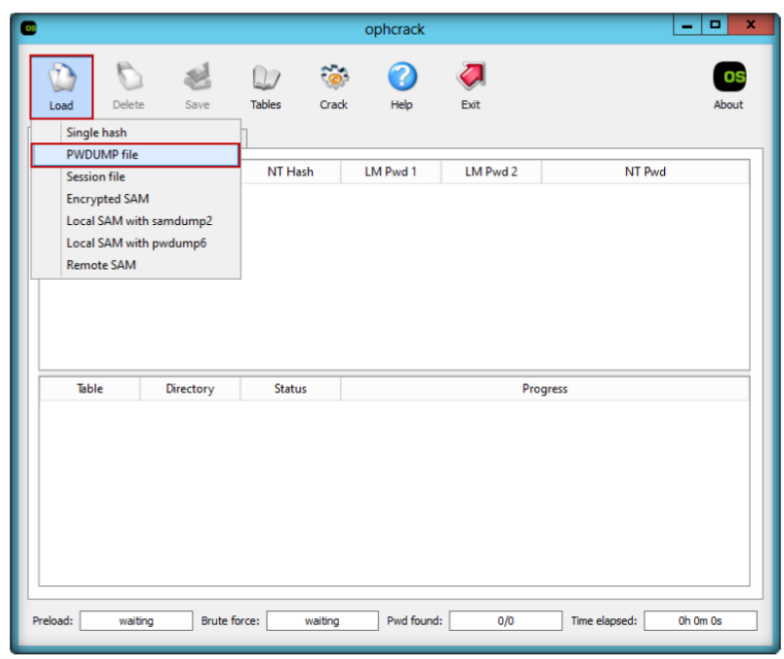


Fig 9.4: Selecting PWDUMP file

5. Browse the PWDUMP file that is already generated by using PWDUMP7 in the previous lab no:5 (located at **c:\hashes.txt**).
6. Click **Open**.

Ophcrack is also available as Live CD distributions which automate the retrieval, decryption, and cracking of passwords from a Windows system.

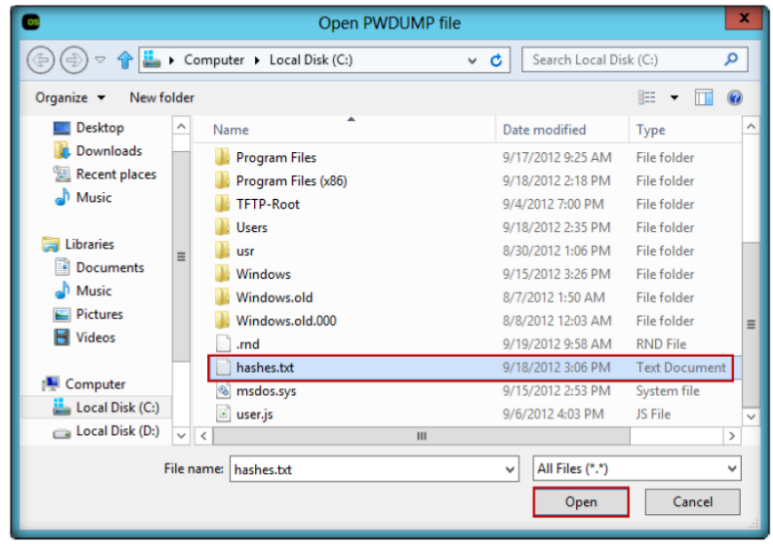


FIGURE 9.5 import the hashes from PWDUMP file

7. Loaded hashes are shown in the following figure.

Ophcrack Cracks LM and NTLM Windows hashes

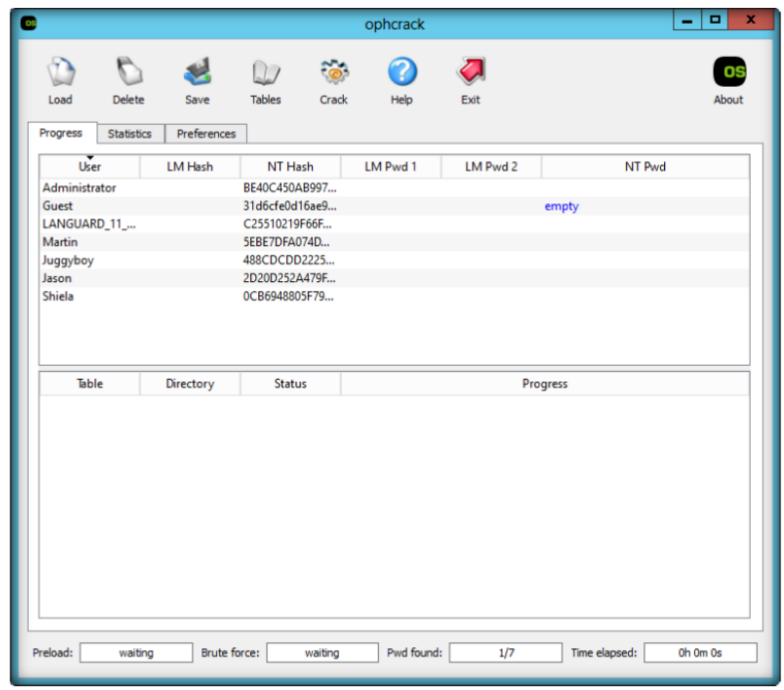


FIGURE 9.6 Hashes are added

8. Click **Table**. The **Table Selection** window will appear as shown in the following figure.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

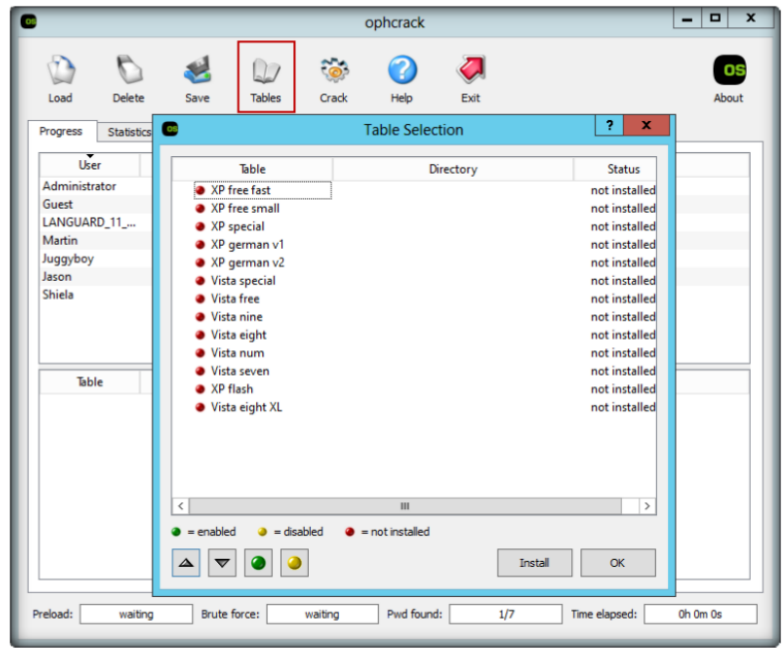


FIGURE 9.7: selecting the Rainbow table

Note: You can download the free XP Rainbow Table, Vista Rainbow Tables from http://ophcrack.sourceforge.net/tables.php

9. Select **Vista free**, and click **Install**.

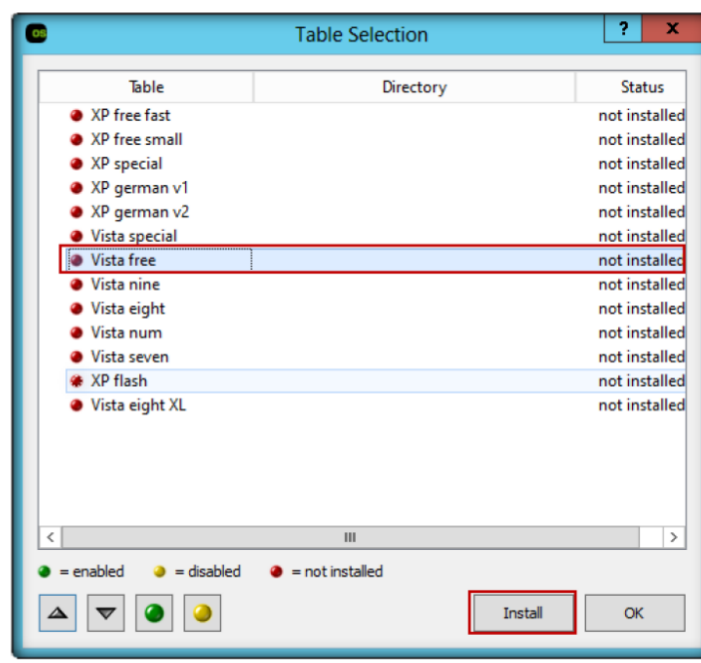
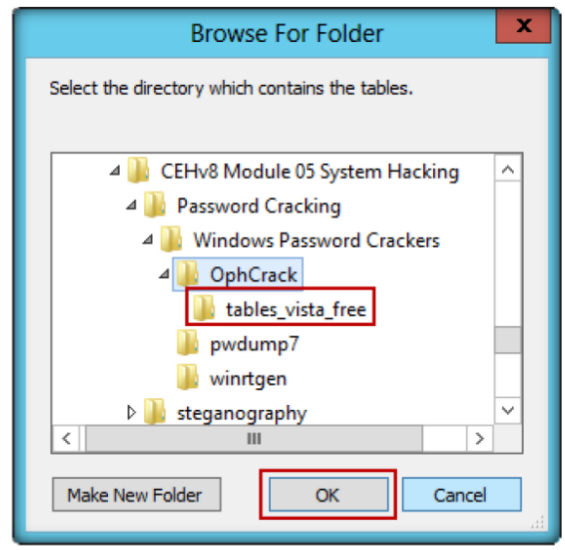


FIGURE 9.8: Installing vista free rainbow table

10. The **Browse For Folder** window appears; select the **the table_vista_free** folder **(which is already download and kept at D:\CEH-Tools\CEHv8 Module 05 System Hacking\Password Cracking Tools\Ophcrack)**
11. Click **OK**.

🗁 Ophcrack Free tables available for Windows XP, Vista and 7



12. The selected **table_vista_free** is installed,; it shows a **green** color ball which means it is enabled. Click **OK**.

🗁 **Loads hashes from encrypted SAM recovered from a Windows partition**

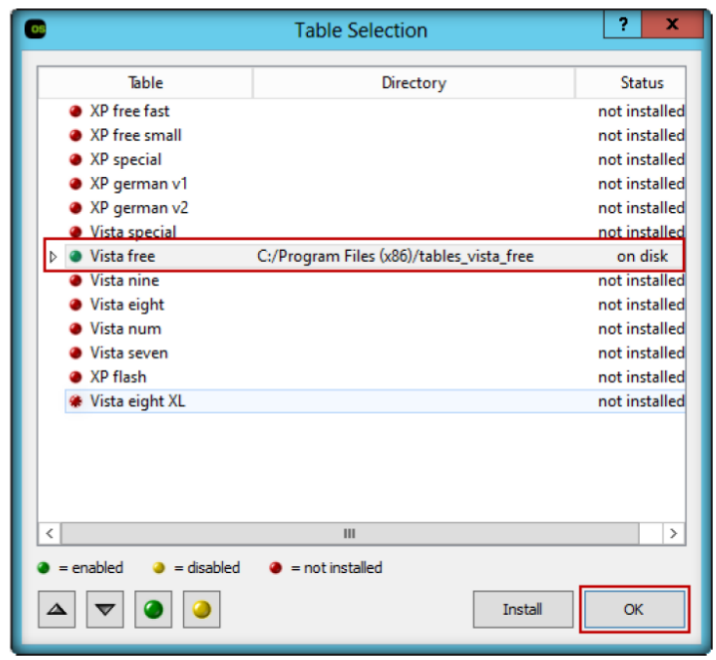


FIGURE 9.9: vista free rainbow table installed successfully

13. Click **Crack**; it will crack the password as shown in the following figure.

This is necessary if the generation of the LM hash is disabled (this is default for Windows Vista), or if the password is longer than 14 characters (in which case the LM hash is not stored).

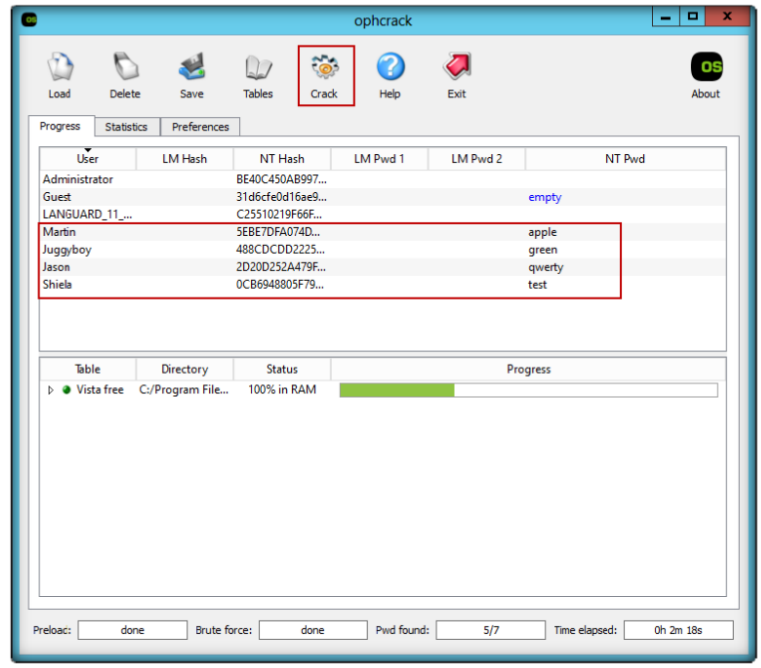


FIGURE 9.10: passwords are cracked

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
OphCrack	**User Names:** ▪ Administrator ▪ Guest ▪ LANGUARD_11_USER ▪ Martin ▪ Juggyboy ▪ Jason ▪ Sheiela
	Rainbow Table Used: Vista free
	Password Found: ▪ apple ▪ green ▪ qwerty ▪ test

Questions

1. What are the alternatives to cracking administrator passwords?

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 10

System Monitoring Using RemoteExec

System hacking is the science of testing computers and networks for vulnerabilities and plugging.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

To be an expert ethical hacker and penetration tester, you must have sound knowledge of footprinting, scanning, and enumeration. This process requires an active connection to the machine being attacked. A hacker enumerates applications and banners in addition to identifying user accounts and shared resources.

You should also have knowledge of gaining access, escalating privileges, executing applications, hiding files, and covering tracks.

Lab Objectives

The objective of this lab is to help students to learn how to:

- **Modify**/**Add**/**Delete** registry keys and or values
- Install service packs, patches, and hotfixes
- Copy folders and files
- Run programs, scripts, and applications
- Deploy Windows Installer packages in silent mode

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

Lab Environment

To carry out the lab, you need:

- **Remote Exec** Tool located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Executing Applications Tools\RemoteExec**
- **Windows Server 2008** running on the Virtual machine
- Follow the Wizard Driven Installation steps

- You can also download the latest version of **RemoteExec** from the link http://www.isdecisions.com/en
- If you decide to download the latest version, then screenshots shown in the lab might differ
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of RemoteExec

RemoteExec, the universal deployer for Microsoft Windows systems, allows network administrators to run tasks remotely.

Lab Task

TASK 1

Monitoring System

System Requirements:

Target computers can have any of these operating systems: Microsoft Windows 2003/2008 (No Service Pack is required); an administration console with Microsoft Windows 2003/2008 Service Pack 6, IE5 or more.

1. Install and launch **RemoteExec**.

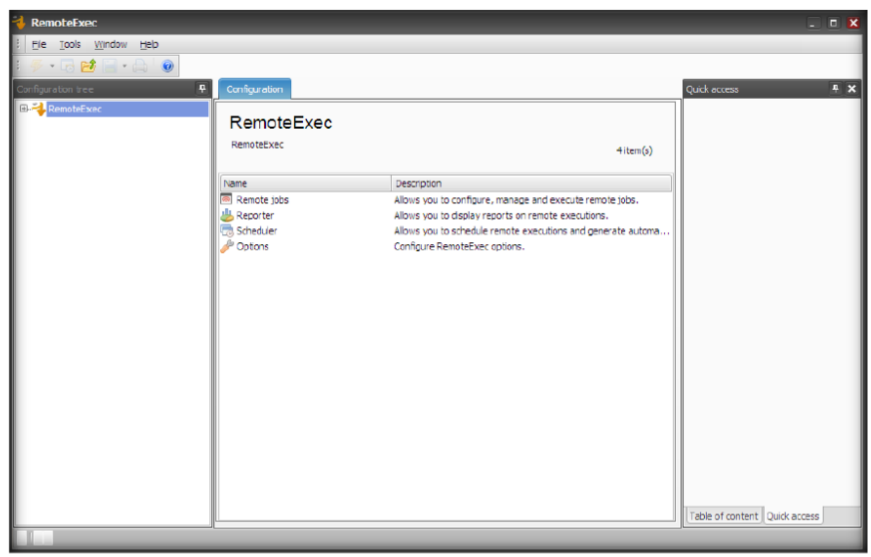


FIGURE 10.1: RemoteExec main window

2. To configure executing a file, double-click **Remote jobs**.

RemoteExec considerably simplifies and accelerates all install and update tasks on a local or wide area network (WAN) as well as on remote machines.

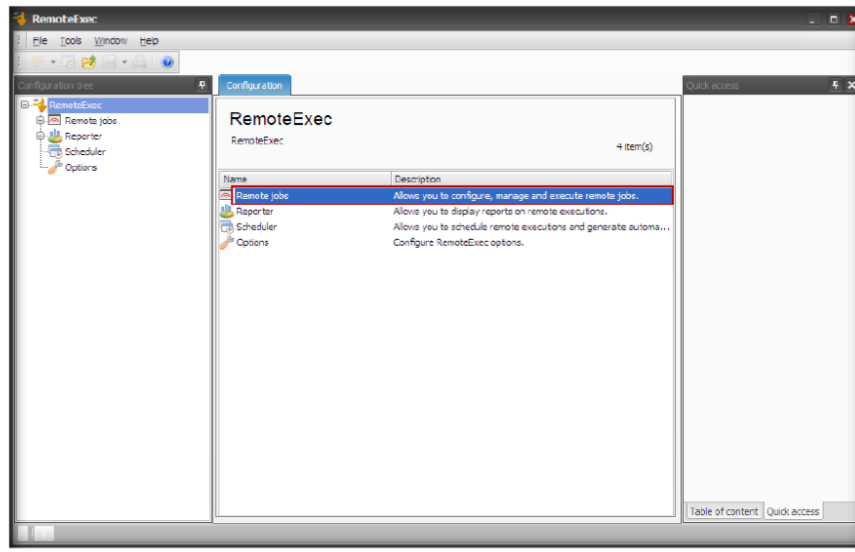


FIGURE 10.2: RemoteExec configuring Remote jobs

Remote execution requirements: The account running RemoteExec needs administrative rights on target computers. Microsoft file and printer sharing (SMB TCP 445) and ICMP (ping) should be enabled. These protocols also need to be allowed in any firewall between the administration console and target computers.

3. To execute a **New Remote job,** double-click the **New Remote job** option that **configures** and **executes** a new remote job.

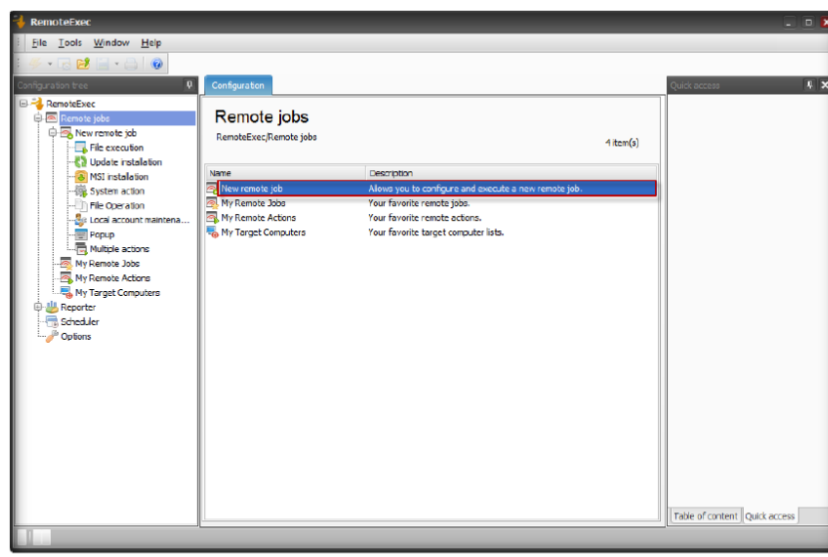


FIGURE 10.3: RemoteExec configuring New Remote job

Configure files to be generated: You see that the report has been added after the installation of Acrobat Reader in the scheduled tasks. A new section, "Document generation," is available to specify the output files. Select a PDF file to be generated in an existing folder. Make sure that the account running the task has write access to this folder.

4. In a **New Remote job** configuration you can view different categories to work remotely.
5. Here as an example: we are executing the file execution option. To execute double-click **File Execution**.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

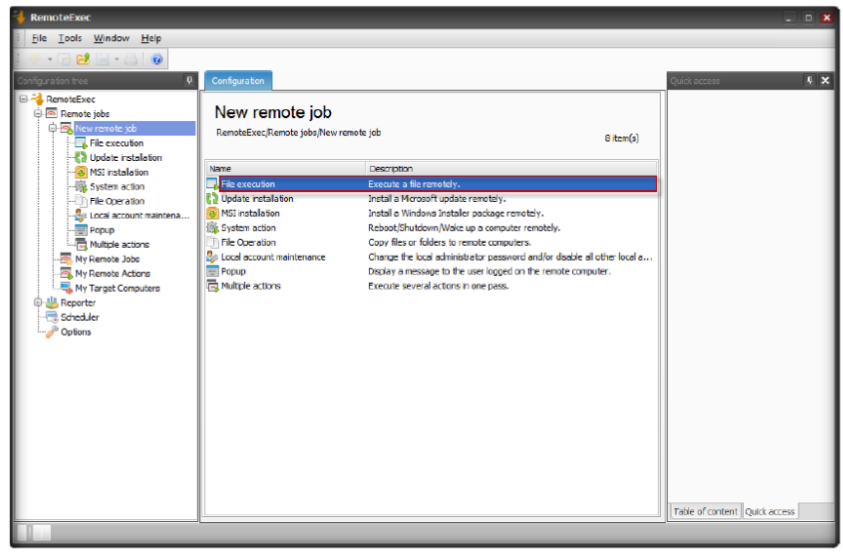


FIGURE 10.4: RemoteExec configuring File Execution

6. In the **File execution** settings, browse the **executable** file, select **Interactive** from drop-down list of **Context**, and check the **Auto** option.

Note: Using RemoteExec, you can:
Install patches, service packs, and hotfixes
Deploy Windows Installer packages in silent mode
Run applications, programs, and scripts
Copy files and folders

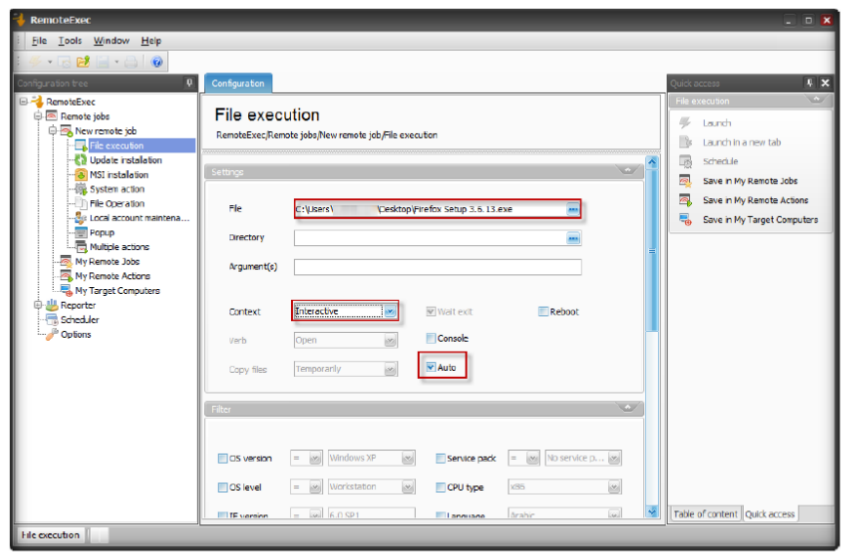


FIGURE 10.5: RemoteExec File execution settings

Automated reports: You may want to get all these reports automatically by email each time a scheduled attempt has been done. To do this, follow the steps below

7. Configuring the **Filter Section**:
   a. For the **OS version**, select **=** from the drop-down menu and specify the operating system.
   b. For the **OS level**, select **=** from the drop-down menu and select **Workstation**.
   c. For the **IE version**, select **>=** from the drop-down menu and specify the IE version.

d. For the **Service Pack**, select **=** from the drop-down menu and specify the service pack version.

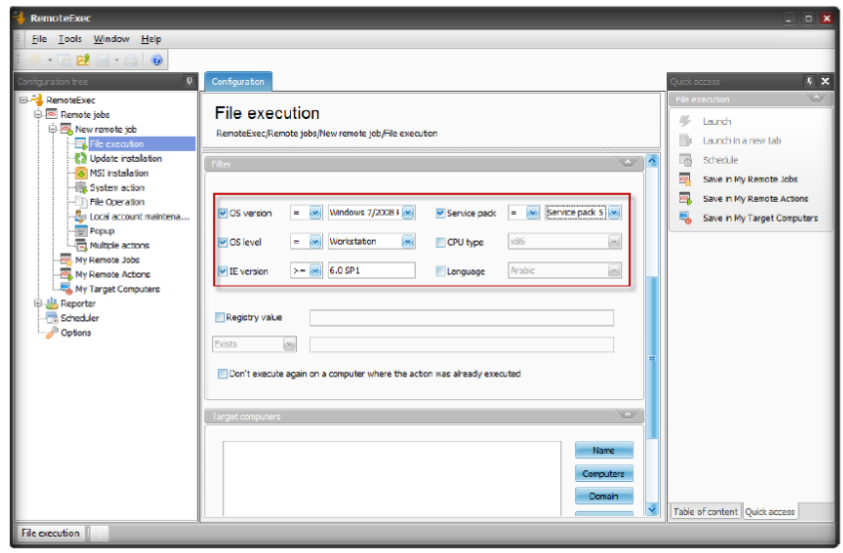


FIGURE 10.6: RemoteExec Filter tab

Once installed, RemoteExec and its documentation are accessible through the Windows Start menu. By default, RemoteExec is installed in evaluation mode.

8. Selecting a **Target Computer:** Enter the target computer name manually by selecting **Name** from the drop-down list and clicking **OK**.

The remote job was automatically set with the filter option, "Don't execute again on a computer where the action was already executed." So, even if several execution attempts have been scheduled, the installation of Acrobat Reader is executed only once on each computer.

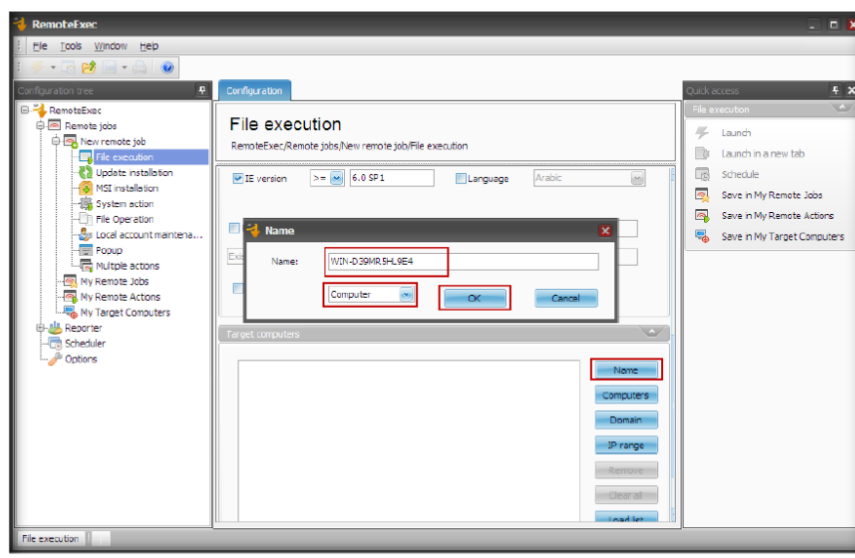


FIGURE 10.7: RemoteExec Add/Edit a computer

Configure the report you want to generate automatically as if you wanted to display it. When you schedule a report, if you select the latest execution, the report is always generated for the latest execution.

9. To execute the defined action on the remote computer, click the **Launch** option in the right pane of the window.

Schedule the report: To configure schedule report, click on Schedule in the toolbar and, when prompted select the task that has been created previously to install Acrobat Reader.

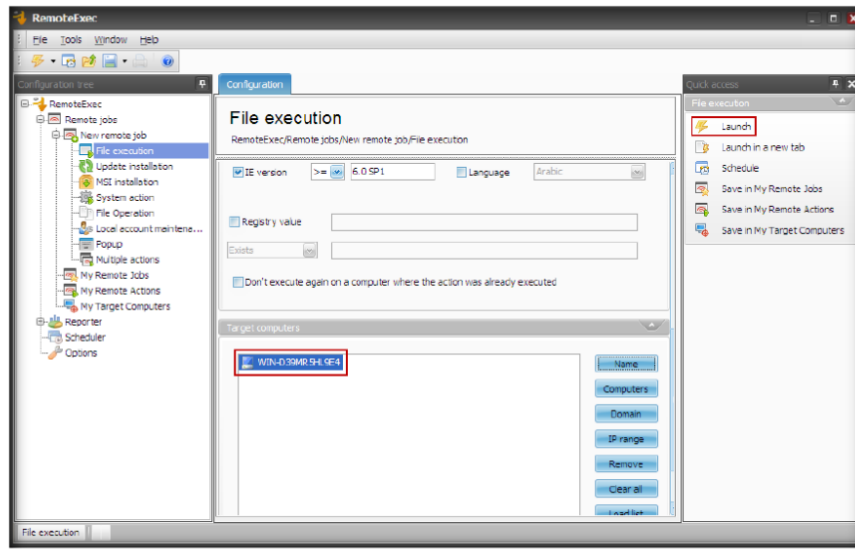


FIGURE 10.8: RemoteExec executing the defined action

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
RemoteExec	**File to Execute:** Firefox setup 3.6.13.exe
	Computer Name: WIN-D39MRSHL9E4

Internet Connection Required	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Lab 11

Hiding Data Using Snow Steganography

Snow is used to conceal messages in ASCII text by appending whitespace to the end of lines. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers. And if the built-in encryption is used, the message cannot be read even if it is detected.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Network steganography describes all the methods used for transmitting data over a network without it being detected. Several methods for hiding data in a network have been proposed, but the main drawback of most of them is that they do not offer a secondary layer of protection. If steganography is detected, the data is in plaintext. To be an expert ethical hacker and penetration tester, you must have sound knowledge of footprinting, scanning, and enumeration. This process requires an active connection to the machine being attacked.

Lab Objectives

The objective of this lab is to help students learn:

- Using Snow steganography to hide files and data
- Hiding files using spaces and tabs

Lab Environment

To carry out the lab, you need:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

- Snow located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Steganography\Whitespace Steganography\SNOW**
- Run this tool on **Windows Server 2012**
- You can also download the latest version of **Snow** from the link http://www.darkside.com.au/snow/
- If you decide to download the **latest version,** then screenshots shown in the lab might differ

Lab Duration

Time: 10 Minutes

Overview of Snow

Snow exploits the steganographic nature of whitespace. Locating trailing whitespace in text is like finding a polar bear in a snowstorm. It uses the ICE encryption algorithm, so the name is thematically consistent.

Lab Task

1. Open a command prompt and navigate to **D:\CEH-Tool\CEHv8 module 05 system hacking\steganography\white space steganography\snow**
2. Open Notepad and type **Hello World!** and then press enter and press the Hyphen key to draw a line below it.
3. Save the file as **readme.txt**.

The encryption algorithm built in to **snow** is ICE, a 64-bit block cipher also designed by the author of **snow**. It runs in 1-bit cipher-feedback (CFB) mode, which although inefficient (requiring a full 64-bit encryption for each bit of output),

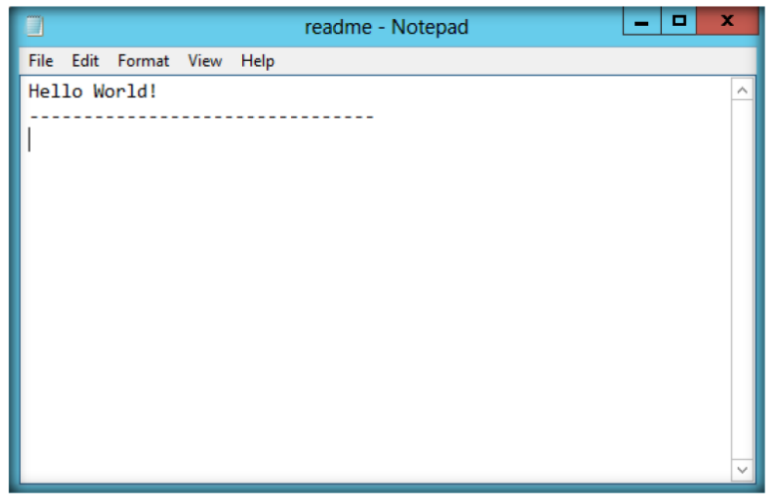


FIGURE 11.1: Contents of readme.txt

4. Type this command in the command shell: **readme2.txt**. It is the name of another that will be created automatically.

   snow -C -m "My swiss bank account number is 45656684512263" -p "magic" readme.txt readme2.txt(magic is the password, you can type your desired password also)

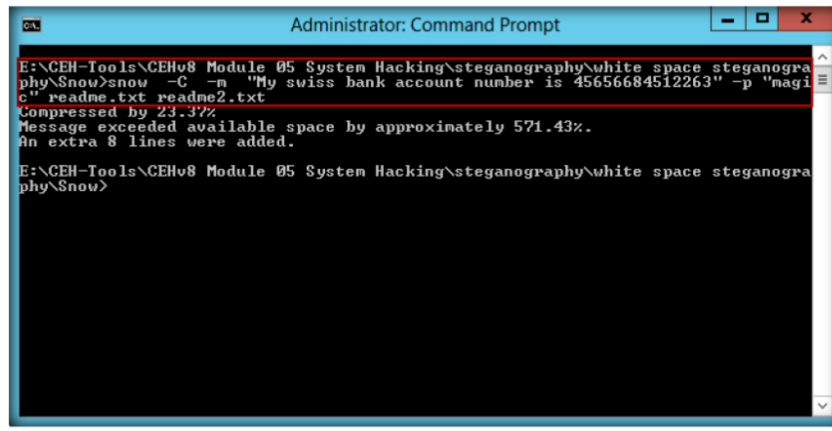


FIGURE 11.2: Hiding Contents of readme.txt and the text in the readme2.txt file

5. Now the data ("**My Swiss bank account number is 45656684512263**") is hidden inside the **readme2.txt** file with the contents of **readme.txt**.

If you want to compress a long message, or one not containing standard text, you would be better off compressing the message externally with a specialized compression program, and bypassing **snow**'s optional compression step. This usually results in a better compression ratio.

6. The contents of **readme2.txt** are **readme.txt** + **My Swiss bank account number is 45656684512263**.
7. Now type **snow -C -p "magic" Readme2.txt**; this will show the contents of readme.txt.(magic is the password which was entered while hiding the data).

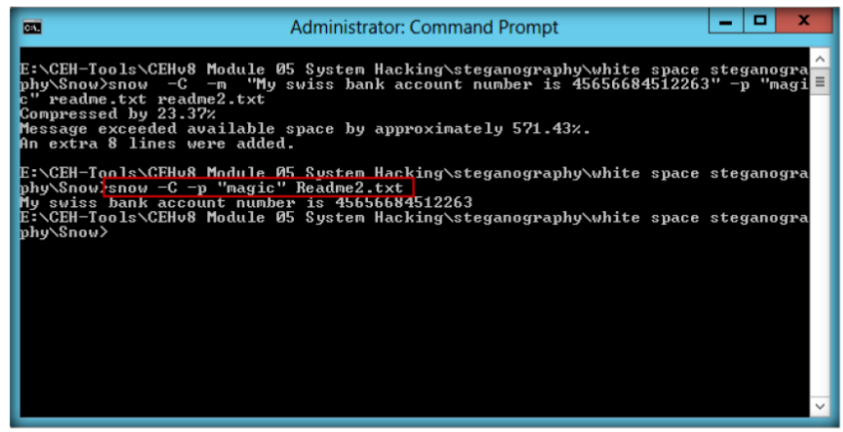


FIGURE 11.3: Revealing the hidden data of readme2.txt

8. To check the file in a GUI , open the **readme2.txt** in Notepad and select **Edit→Select all**. You will see the hidden data inside readme2.txt in the form of spaces and tabs.

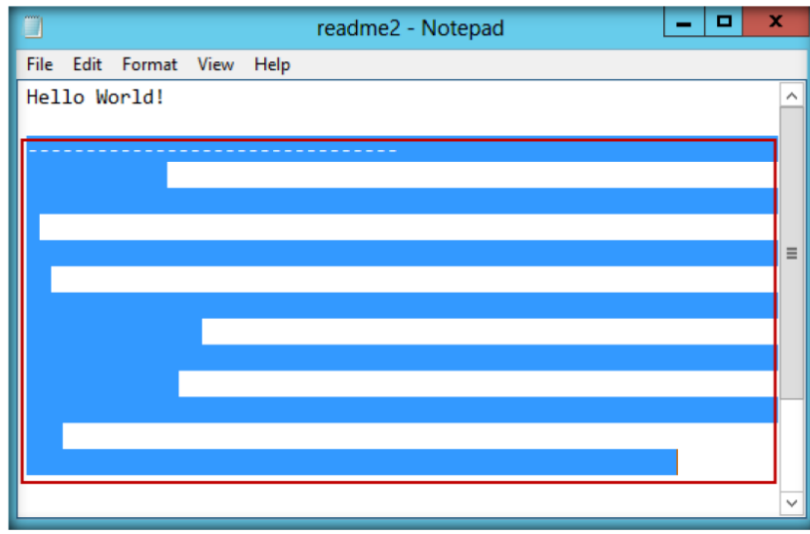


FIGURE 11.4: Contents of readme2.txt revealed with select all option

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Snow Steganography	**Output:** You will see the hidden data inside Notepad

Lab Questions

1. How would you hide the data of files with secret data in other files?
2. Which encryption is used in Snow?

Internet Connection Required	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Lab 12

Viewing, Enabling, and Clearing the Audit Policies Using Auditpol

Auditpol is a command in Windows Server 2012, Windows Server 2008, and Windows Server 2003 and is required for querying or configuring an audit policy at the subcategory level.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

To be an expert ethical hacker and penetration tester, you must have sound knowledge of footprinting, scanning, and enumeration. This process requires an active connection to the machine being attacked. A hacker enumerates applications and banners in addition to identifying user accounts and shared resources.

You should also have knowledge on gaining access, escalating privileges, executing applications, hiding files, and covering tracks.

Lab Objectives

The objective of this lab is to help students learn:

- How to set audit policies

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

To carry out the lab, you need:

- **Auditpol is a built-in command in Windows Server 2012**
- You can see the more audit commands from the following link: http://technet.microsoft.com/en-us/library/cc731451%28v=ws.10%29.aspx for **Windows Server 2012**
- Run this on **Windows Server 2012**

Lab Duration

Time: 10 Minutes

Overview of Auditpol

Auditpol displays information on performance and functions to **manipulate** audit policies.

Lab Task

/get
Displays the current audit policy.

1. Select **Start → Command Prompt**.
2. **Administrator:** A command prompt will appears as shown in the following figure.

/set
Sets the audit policy.

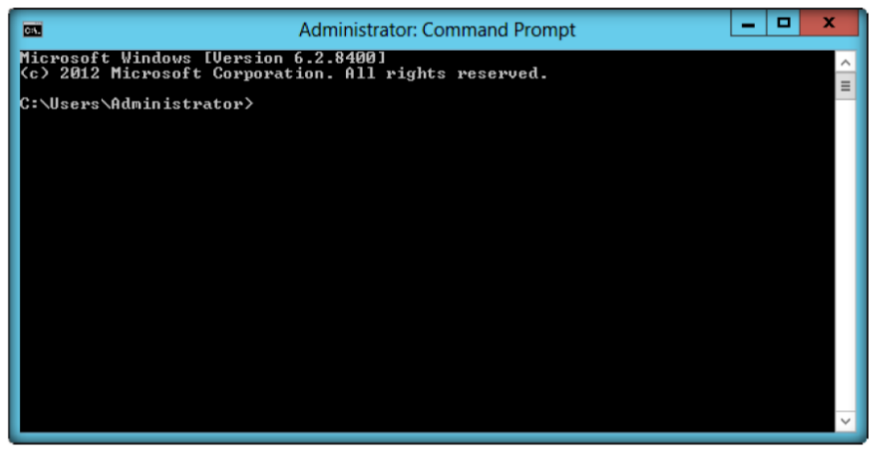


FIGURE 12.1: Administrator: Command Prompt in windows server 2012

/list
Displays selectable policy elements.

3. To **view** all the audit policies, type the following command in the command prompt:

   auditpol /get /category:*

/backup
Saves the audit policy to a file.

4. Press **Enter**.

/restore
Restores the audit policy from a file that was previously created by using auditpol /backup.

/clear
Clears the audit policy.

/remove
Removes all per-user audit policy settings and disables all system audit policy settings.

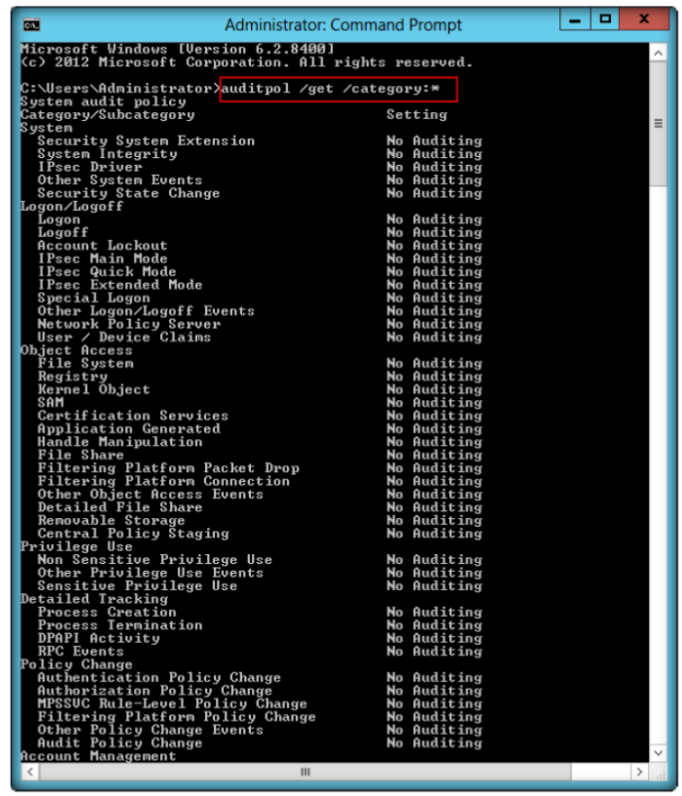


FIGURE 12.2: Auditpol viewing the policies

5. To **enable** the audit policies, type the following command in the command prompt:

   auditpol /set /category:"system","account logon" /success:enable /failure:enable

6. Press **Enter**.

/resourceSACL
Configures global resource system access control lists (SACLs).

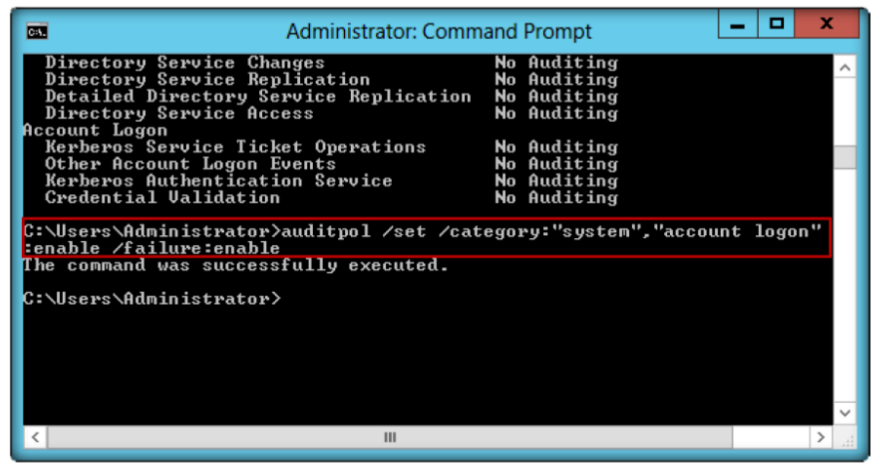


FIGURE 12.3: Auditpol Local Security Policies in Windows Server 2012

7. To check if audit policies are enabled, type the following command in the command prompt **auditpol /get /category:***
8. Press **Enter**.

Auditpol /get
[/user[:<username>|<{sid}>]]
[/category:*|<name>|<{guid}>[,:<name|<{guid}>…]]
[/subcategory:*|<name>|<{guid}>[,:<name|<{guid}>…]]
[/option:<option name>]
[/sd]
[/r]

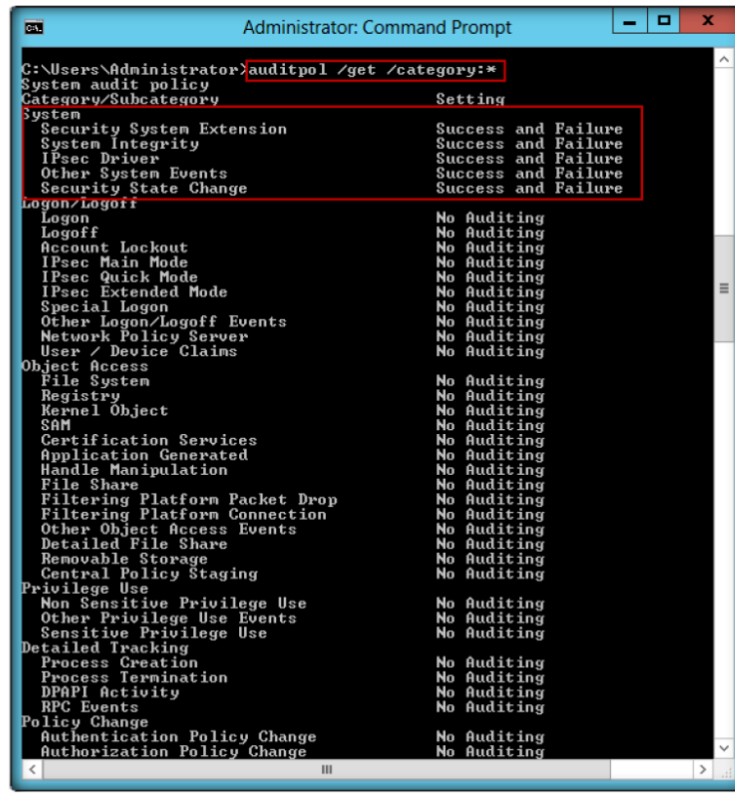


FIGURE 12.4: Auditpol enabling system and account logon policies

9. To **clear** the audit policies, type the following command in the command prompt:

   auditpol /clear /y

10. Press **Enter**.

Auditpol /set
[/user[:<username>|<{sid}>][/include][/exclude]]
[/category:<name>|<{guid}>[,:<name|<{guid}>…]]
[/success:<enable>|<disable>][/failure:<enable>|<disable>]
[/subcategory:<name>|<{guid}>[,:<name|<{guid}>…]]
[/success:<enable>|<disable>][/failure:<enable>|<disable>]
[/option:<option name>
/value:
<enable>|<disable>]

auditpol /list
[/user|/category|subcategory[:<categoryname>|<{guid}>|*]]
[/v] [/r]

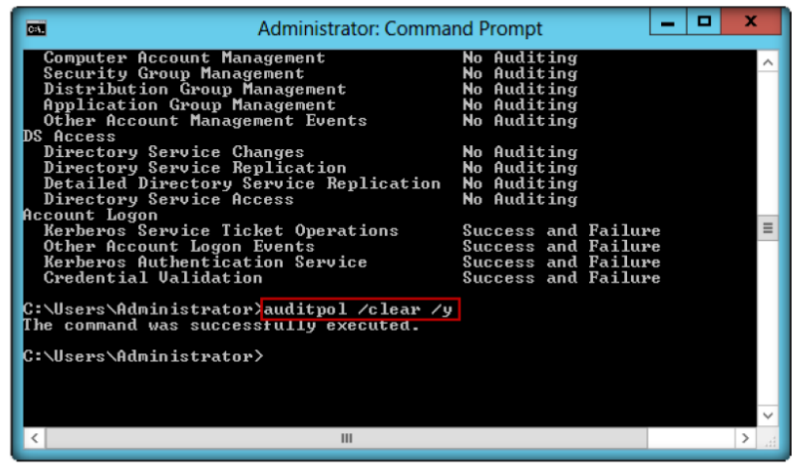


FIGURE 12.5: Auditpol clearing the policies

11. To check if the audit policies are cleared, type the following command in the command prompt:

    auditpol /get /category:*

12. Press **Enter**.

Auditpol /set
[/user[:<username>|<{sid}>][/include][/exclude]]
[/category:<name>|<{guid}>[,:<name|<{guid}>…]]
[/success:<enable>|<disable>][/failure:<enable>|<disable>]
[/subcategory:<name>|<{guid}>[,:<name|<{guid}>…]]
[/success:<enable>|<disable>][/failure:<enable>|<disable>]
[/option:<option name>
/value:
<enable>|<disable>]

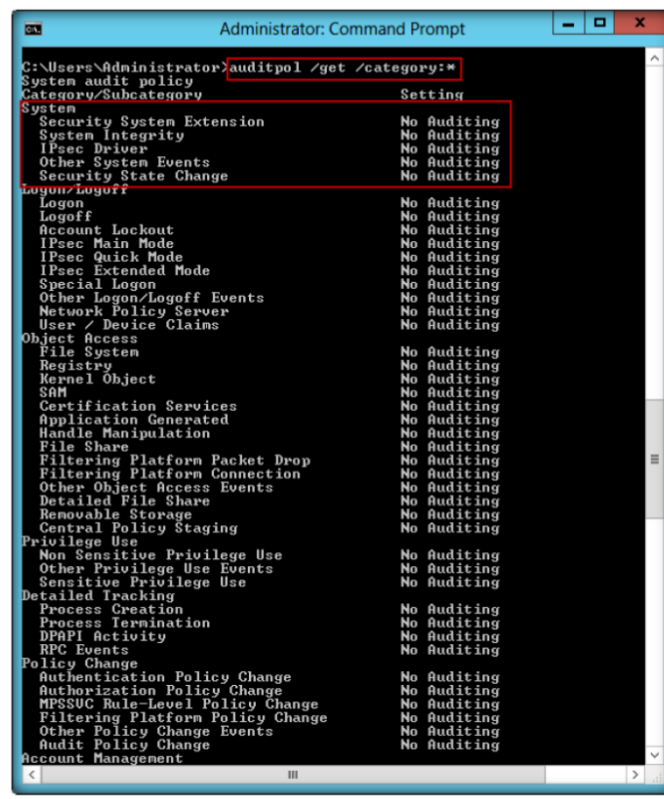


FIGURE 12.6: Auditpol clearing the audit policies

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
AuditPol	**Result open Auditpol Category:** ▪ System ▪ Account Logon

Questions

1. How do you configure global resource SACLs using Auditpol?
2. Evaluate a report or backup an audit policy to a comma separated value (CSV) text file.

Internet Connection Required	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Lab 13

Password Recovery Using CHNTPW.ISO

CHNTPW.ISO is a password recovery tool that runs on Windows Server 2003, Windows Server 2008, and Windows 7 Virtual Machine.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Nowadays, attacking the password is one of the most straightforward hacking attacks. Passwords are the most common access control method used by system administers to manage the usage of network resources and applications. There are numerous feasible methods to crack passwords. To be an expert ethical hacker and penetration tester, you must have sound knowledge of footprinting, scanning, and enumeration. This process requires an active connection to the machine being attacked. A hacker enumerates applications and banners in addition to identifying user accounts and shared resources.

In this lab, we show you how to erase or recover an admin password using CHNTPW.ISO.

Lab Objectives

The objective of this lab is to help students learn:

- **Recovering the Password of Windows Server 2008**

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

Lab Environment

To carry out the lab, you need:

- CHNTPW.ISO located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Password Recovery Tools\CHNTPW.ISO\cd110511**
- CHNTPW.ISO is tool to recover/erase the administrator passwords for Windows Server 2008
- A computer running with Windows Server 2008 as Virtual Machine

Lab Duration

Time: 15 Minutes

Overview of CHNTPW.ISO

CHNTPW.ISO is an offline NT password and registry editor, boot disk/CD.

Lab Task

1. Start Hyper-V Manager by selecting **Start →Hyper-V Manager**.
2. Before starting this lab make sure that **Windows Server 2008** Virtual Machine is shut down.

📖 Offline NT Password & Registry Editor can delete any password from nearly any installation of Windows almost instantly.

3. Now select **Windows Server 2008** Virtual Machine and click **Settings** in the right pane of Hyper-V..

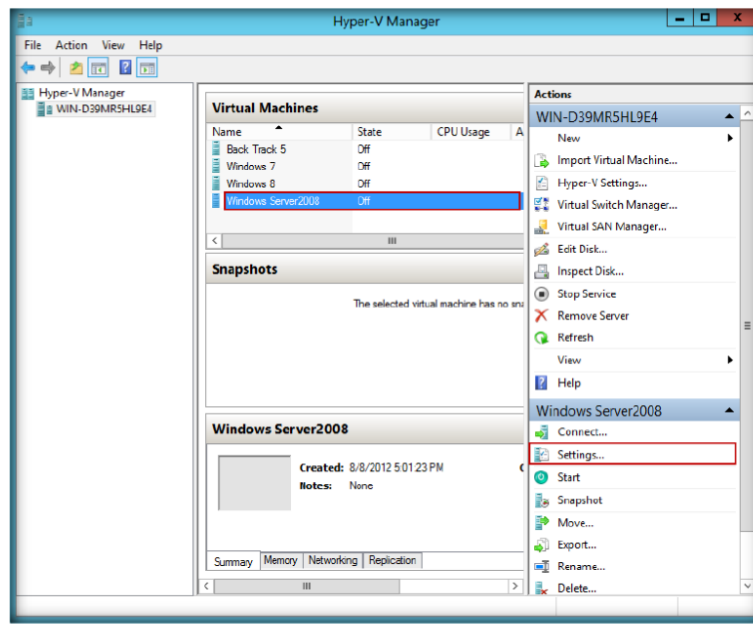


FIGURE 13.1: CHNTPW.ISO Windows Server 2008 settings

🗁 Offline NT Password & Registry Editor simply deletes passwords instead of displaying them making it fast and easy to use.

4. Select **DVD drive** from **IDE controller in** the left pane of **Settings** for Windows Server 2008.
5. Check the **Image file** option and browse for the location of **CHNTPW.ISO,** and select **Apply→OK**.

📖 No installation in Windows is required making this program an easy alternative to many other password recovery tools.

Offline NT Password & Registry Editor is completely free to download and use.

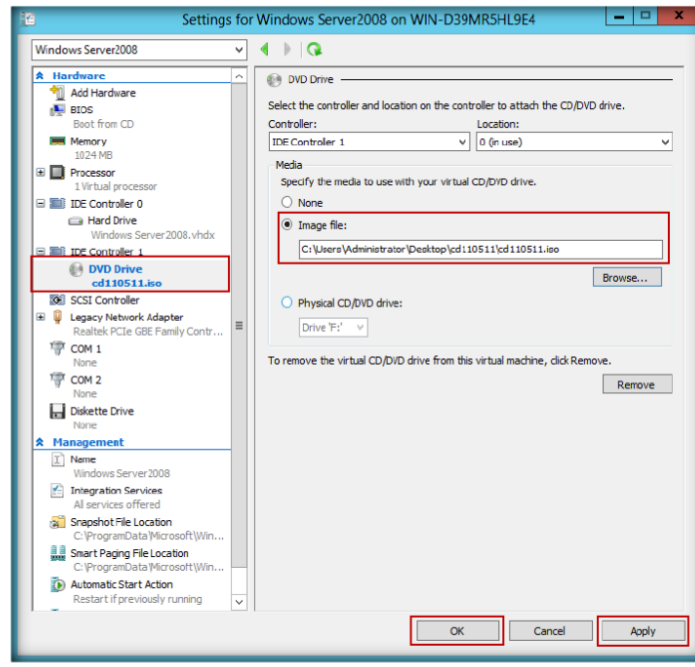


FIGURE 13.2: CHNTPW.ISO Windows Server 2008 settings

Tool will also remove passwords from 64-bit versions of Windows Operating Systems.

6. Now go to Hyper-V Manager and right-click **Windows Server 2008**, and select **Connect** to start Windows Server 2008 Virtual Machine.

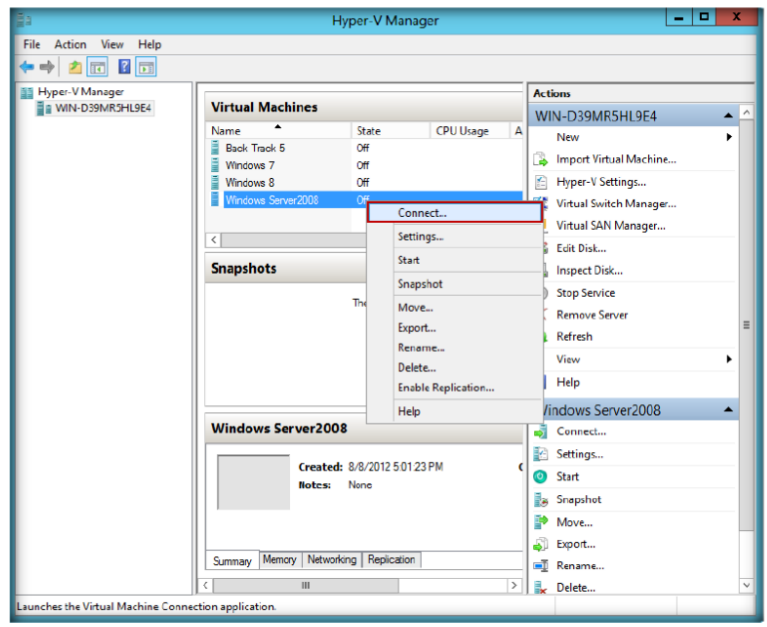


FIGURE 13.3: CHNTPW.ISO Connecting to Windows Server 2008

Offline NT Password & Registry Editor works with all popular Windows versions including Windows 7 and more.

7. Click the **Start** button; **Windows Server 2008** will start.

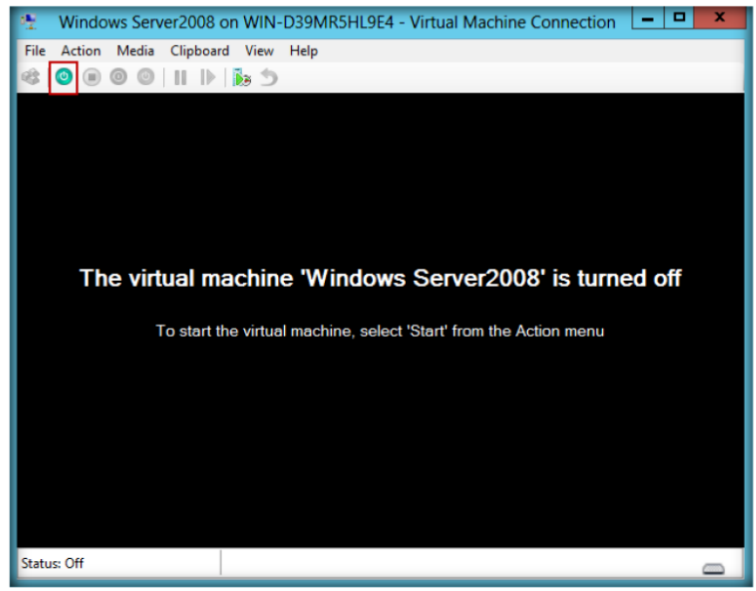


FIGURE 13.4: starting windows server 2008 O/S

8. After booting, Window will prompt you with: **Step one: Select disk where the Windows installation is**
9. Press **Enter**.

📖 It works offline, that is, you have to shut down your computer and boot off a floppydisk or CD or another system.

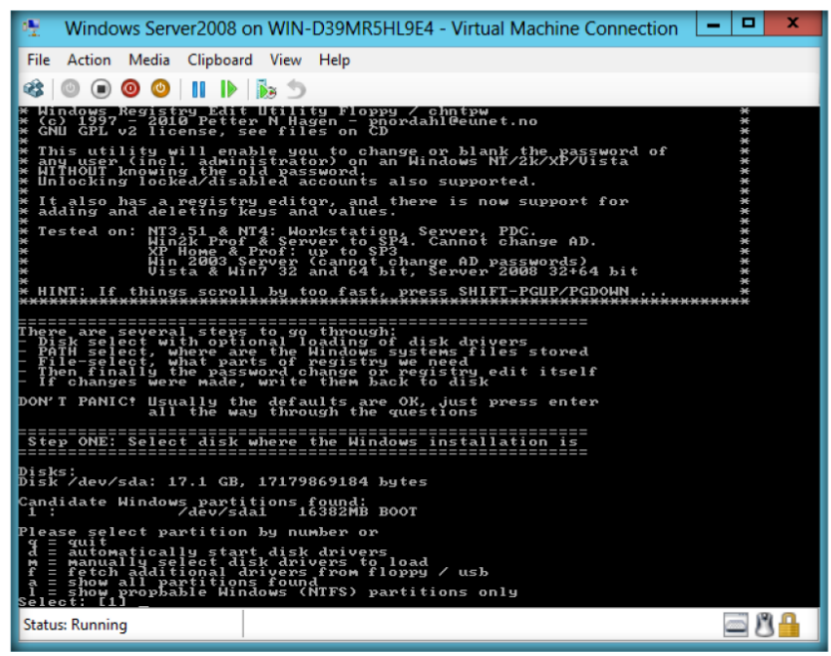


FIGURE 13.5: CHNTPW.ISO Step One

10. Now you will see: **Step TWO: Select PATH and registry files**; press **Enter**.

This is a utility to (re)set the password of any user that has a valid (local) account on your NT system.

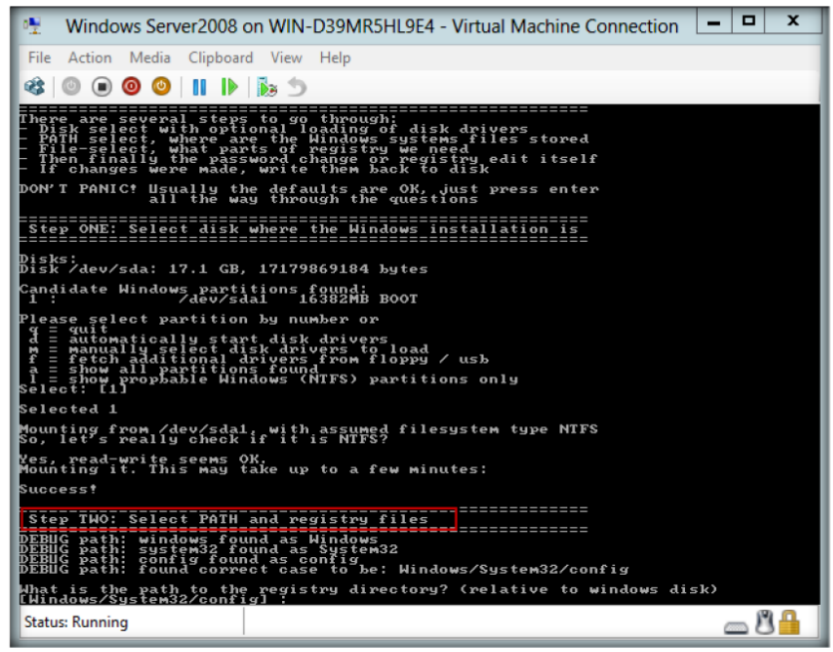


FIGURE 13.6: CHNTPW.ISO Step Two

11. Select which part of the registry to load, use predefined choices, or list the files with space as delimiter, and then press **Enter**.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

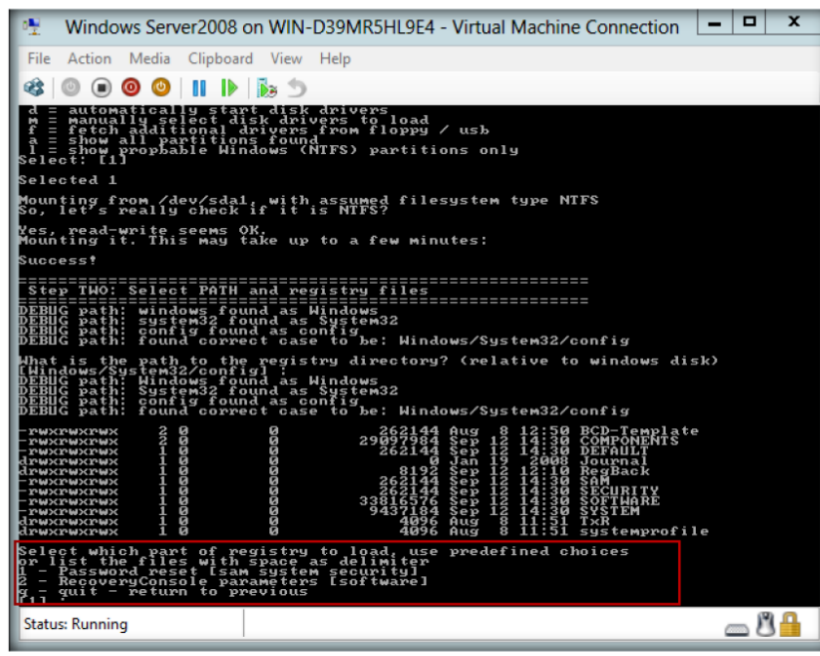


FIGURE 13.7: CHNTPW.ISO loading registry request

12. When you see: **Step THREE: Password or registry edit**, type yes (**y**), and press **Enter**.

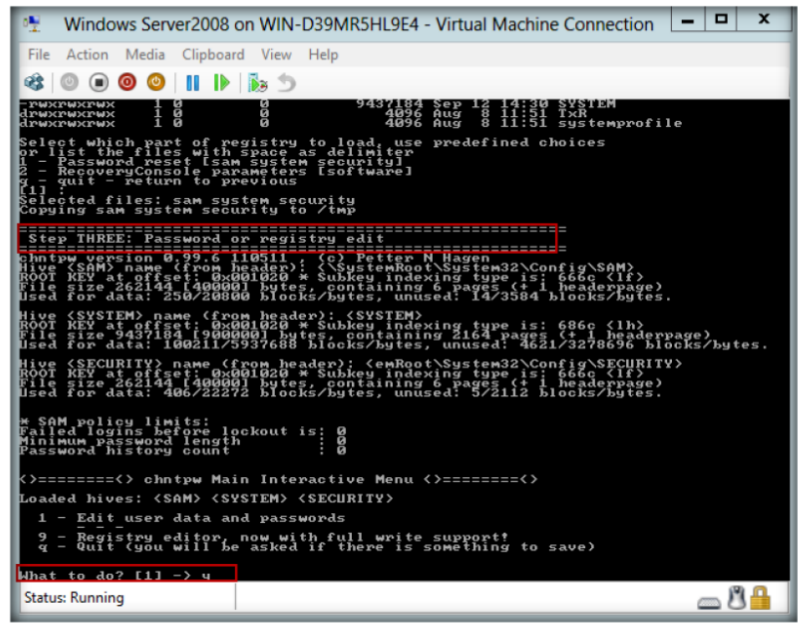


FIGURE 13.8: CHNTPW.ISO Step Three

13. **Loaded hives**: <SAM><system><SECURITY>

    1 – Edit user data and passwords

    9 – Registry editor, now with full write support!

    Q – Quit (you will be asked if there is something to save)

    In **What to do**? the default selected option will be [1]. Press **Enter**.

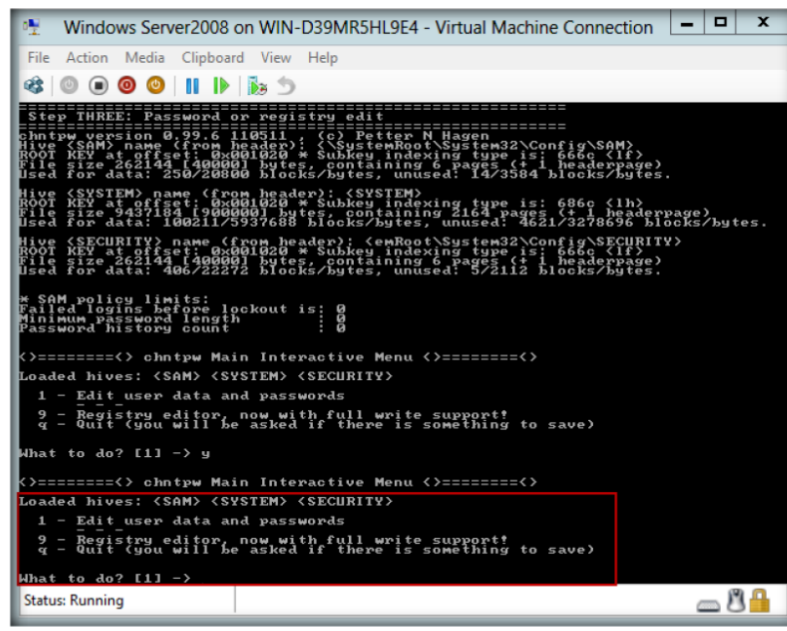


FIGURE 13.9: CHNTPW.ISO loading hives

📖 It works offline, that is, you have to shutdown your computer and boot off a floppydisk or CD. The bootdisk includes stuff to access NTFS and FAT/FAT32 partitions and scripts to glue the whole thing together.

📖 **CEH-Tools is also Mapped in Virtual Machine as Network Drive Z:**

14. In **chntpw Edit User Info & Passwords**, press **Enter** to enter the user name to change

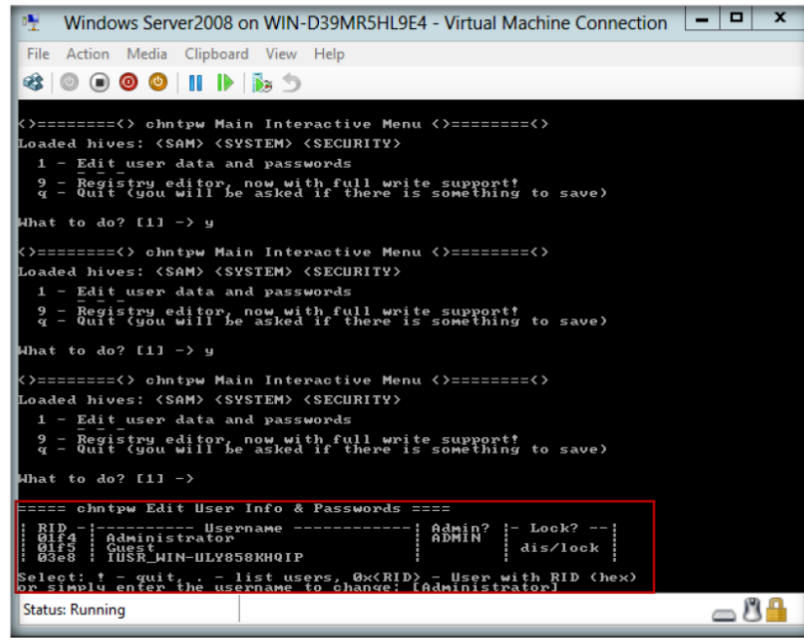


FIGURE 13.10: CHNTPW.ISO chntpw Edit User Info & Passwords

15. In the **User Edit Menu**:

    1 – Clear (blank) user password

    2 – Edit (set new) user password (careful with this on XP or Vista)

    3 – Promote user (make user an administrator)

    4 – Unlock and enable user account [seems unlocked already]

    q – Quit editing user, back to user select

    The default option, Quit [**q**], is selected. Type **1** and press **Enter**.

NT stores its user information, including crypted versions of the passwords, in a file called 'sam', usually found in \winnt\system32\config. This file is a part of the registry, in a binary format previously undocumented, and not easily accessible.

Disable your software firewall (Norton Internet Security is often the culprit).

Disable all "download accelerator" programs; they will more than likely corrupt your download.

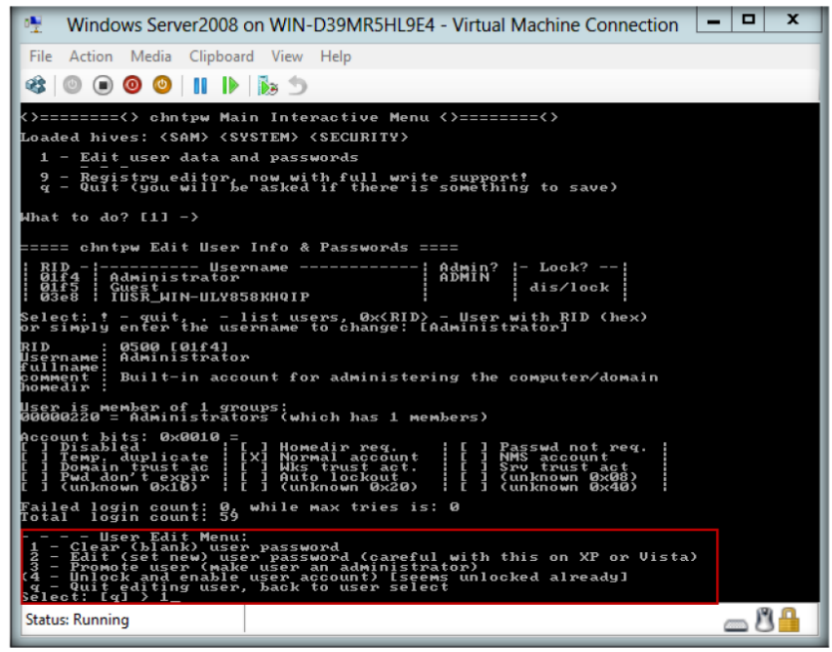


FIGURE 13.11: CHNTPW.ISO User Edit Menu

16. Type **!** after clearing the password of the user account, and press **Enter**.

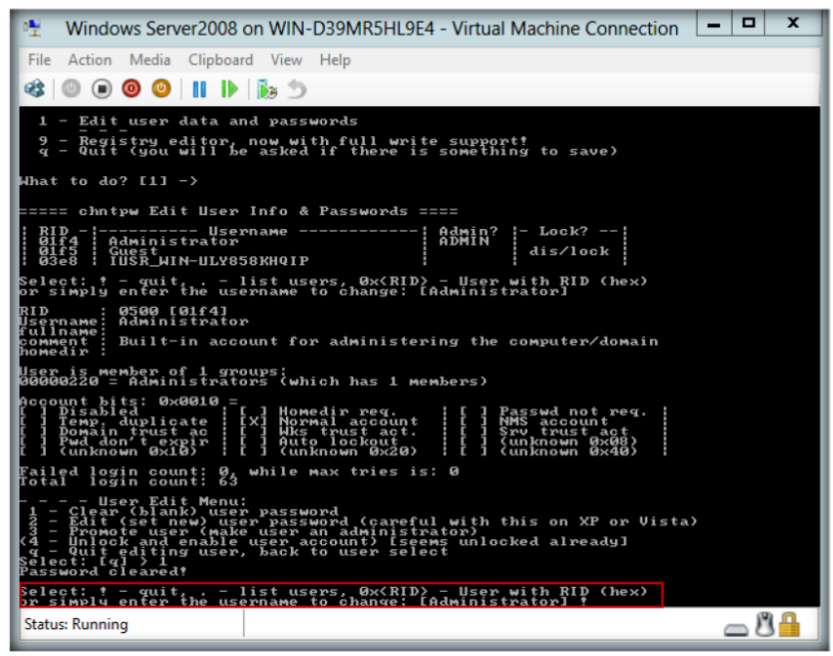


FIGURE 13.12: CHNTPW.ISO Password Cleared

17. **Load hives**: <SAM><system><SECURITY>

    1 – Edit user data and passwords

    9 – Registry editor, now with full write support!

Q – Quit (you will be asked if there is something to save)

In **What to do?**, the default selected option will be [1]. Type quit (**q**), and press **Enter**.

CEH-Tools is also Mapped in Virtual Machine as Network Drive Z:

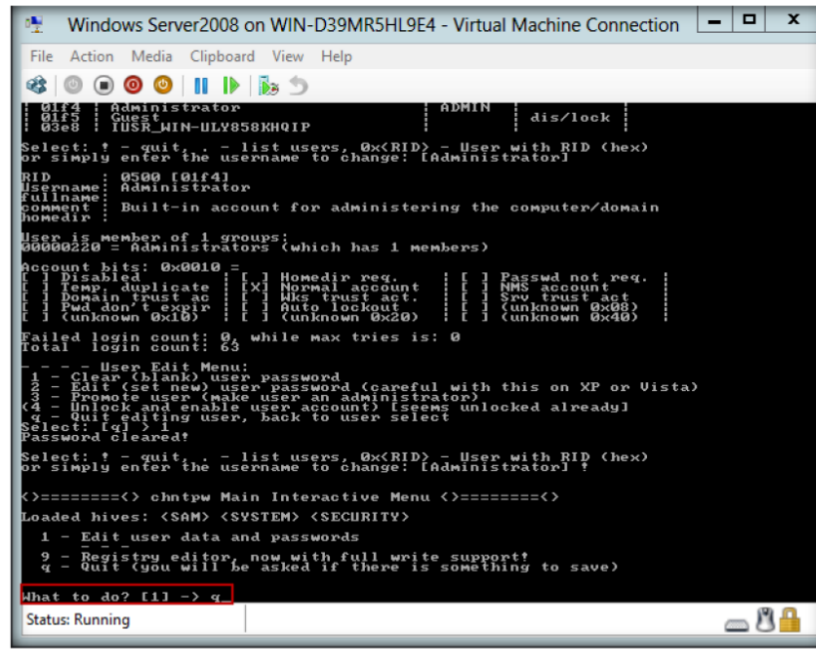


FIGURE 13.13: CHNTPW.ISO loading hives Quit option

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

18. In **Step FOUR: Writing back Changes, About to write file(s) back! Do it?**, here the default option will be [**n**]. Type yes [**y**] and press **Enter**.

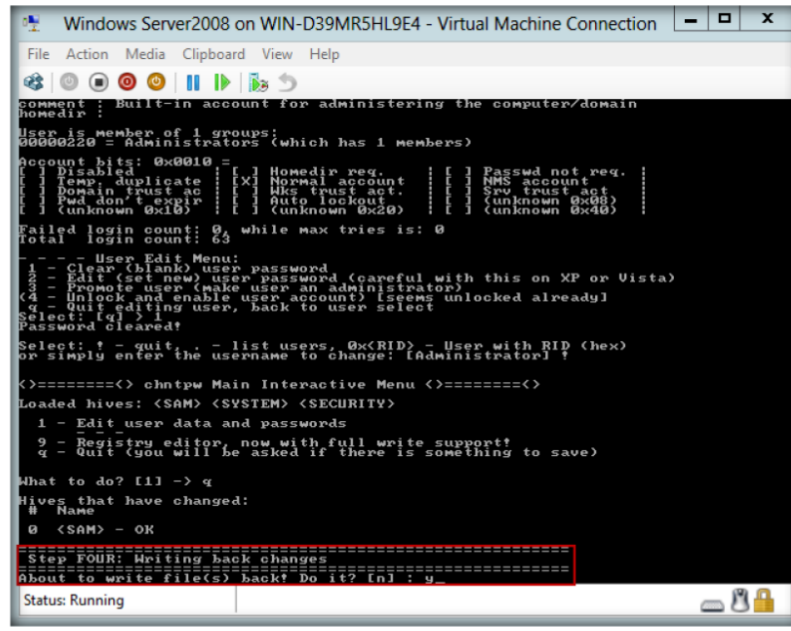


FIGURE 13.14: CHNTPW.ISO Step Four

19. The edit is completed.

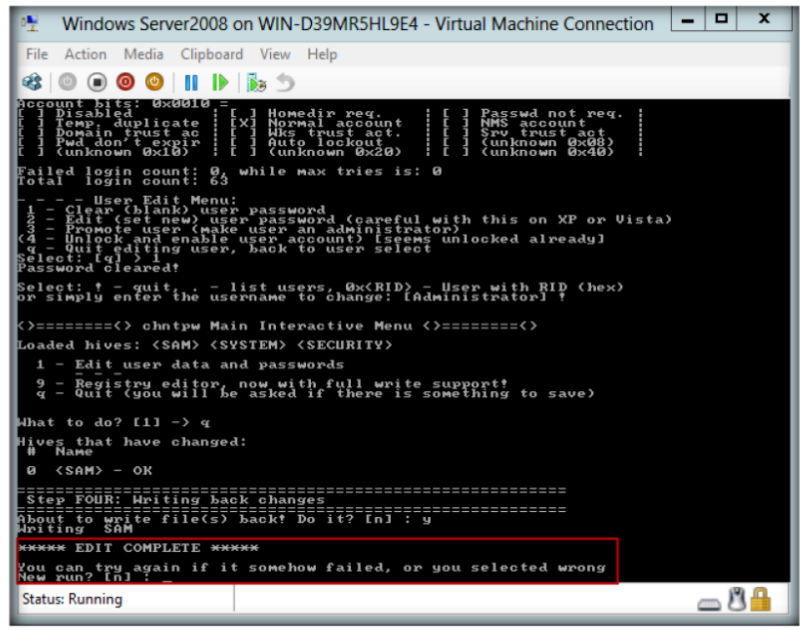


FIGURE 13.15: CHNTPW.ISO Edit Completed

20. Now **turn off** the **Windows Server 2008** Virtual Machine.

21. Open Hyper-V Manager settings of Windows Server 2008 and change the **DVD drive** option to **None** from **IDE Controller 1** and then select click **→Apply →OK**.

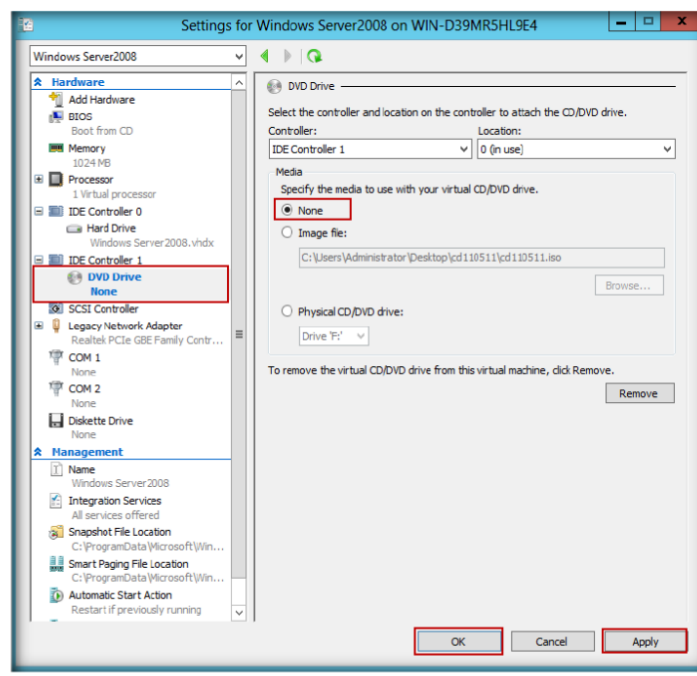


FIGURE 13.16: CHNTPW.ISO Windows Server 2008 Settings

It works offline, that is, you have to shutdown your computer and boot off a floppydisk or CD or another system.

CEH-Tools is also Mapped in Virtual Machine as Network Drive Z:

22. Go to **Windows Server 2008** Virtual Machine, and click the **Start** button.

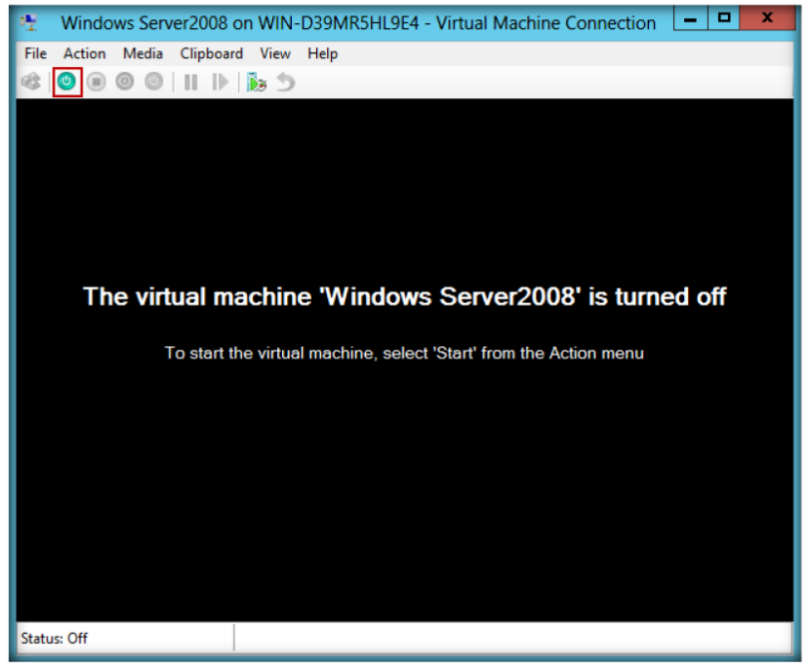


FIGURE 13.17: starting windows server 2008

23. Windows server 2008 boots without requiring any password.

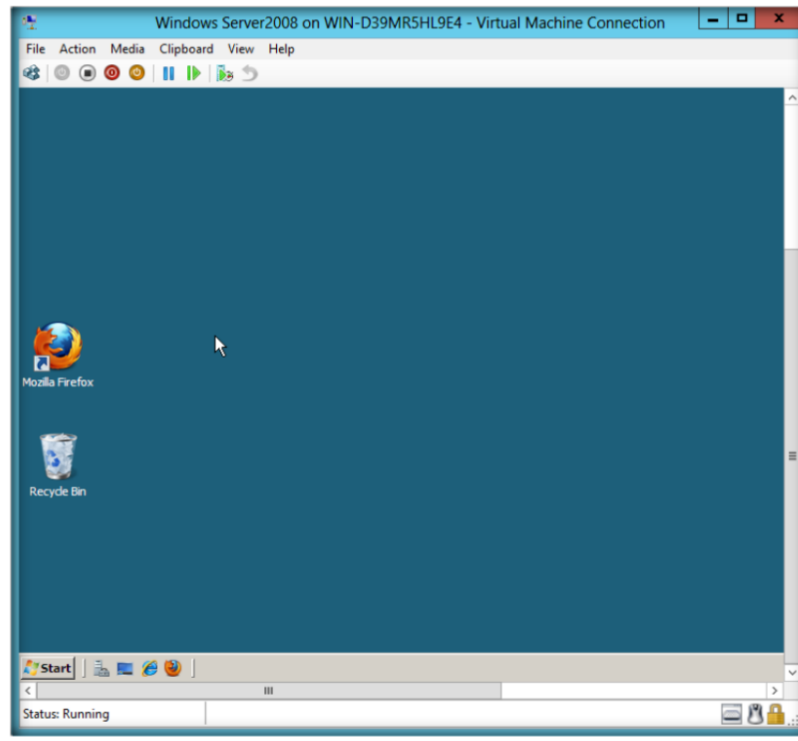


FIGURE 13.18: Windows Server 2008 Window

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
CHNTPW.ISO	**Machine Name:** Windows server 2008
	Output: Log into Windows Server 2008 without entering the user name and password

Questions

1. How do you configure **CHNTPW.ISO** in **Windows Server 2008 Virtual Machine Settings**?

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab

14

User System Monitoring and Surveillance Needs Using Spytech SpyAgent

Spytech SpyAgent is powerful computer spy software that allows you to monitor everything users do on your computer, in total stealth. SpyAgent provides a large array of essential computer monitoring features, as well as website, application, and chat client blocking, lockdown scheduling, and remote delivery of logs via email or FTP.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

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.

In this lab, we explain monitoring employee or student activity using Spytech SpyAgent .

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

Lab Objectives

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 Environment

To perform the lab, you need:

- A computer running **Windows Server 2012**
- Administrative privileges to install and run tools
- Run this tool in Windows Server 2012
- You can also download Spytech SpyAgent from http://www.spytech-web.com/spyagent.shtml
- If you decided to download the latest version, screenshots may differ

Lab Duration

Time: 15 Minutes

Overview of Spytech SpyAgent

SpyAgent is a powerful solution that can log all keystrokes, emails, windows, websites, applications, Internet connections, chat conversations, passwords, print jobs, documents viewed, and even screenshots. SpyAgent runs in complete stealth with optional email delivery and logging and lockdown scheduling. 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 Tasks

The basic idea in this section is to:

TASK 1

Installation of Spytech SpyAgent

1. Navigate to **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Keyloggers\Spytech SpyAgent**
2. Double-click **Setup.exe**. You will see the following window. Click **Next**.

You can download the spytech SpyAgent from *http://www.spytech-web.com*

FIGURE 14.1: Installation of Spytech SpyAgent

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

FIGURE 14.2: Installation wizard of Spytech SpyAgent

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

FIGURE 14.3: Installation wizard

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

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

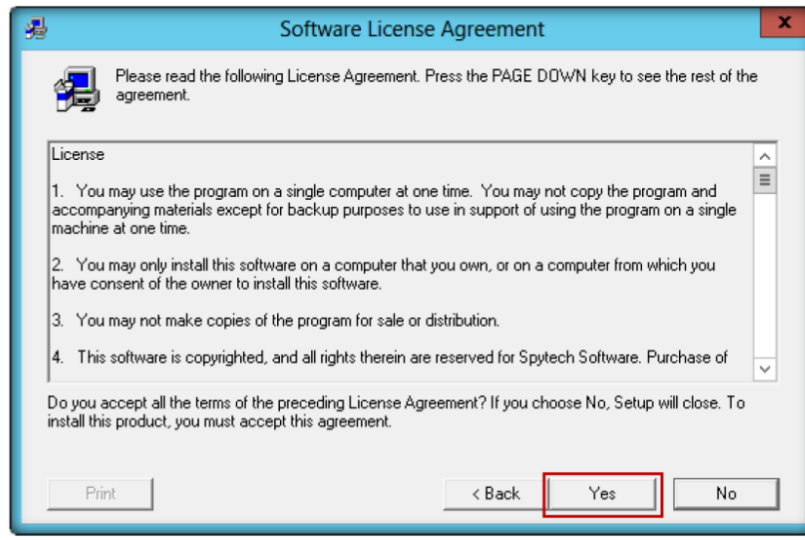


FIGURE 14.4: Select the Agreement

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

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

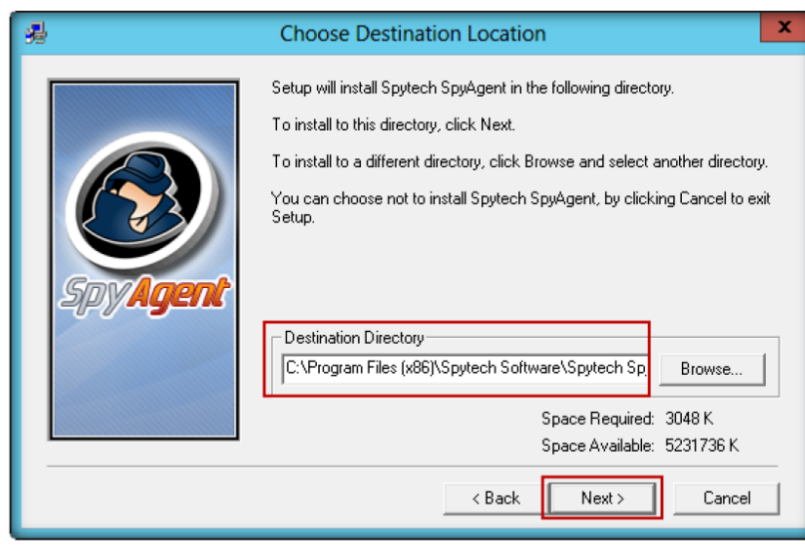


FIGURE 14.5: Selecting folder for installation

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

FIGURE 14.6: selecting installation type

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

Splash Warning: This option allows you to display a message to the user when SpyAgent is started. This message can be configured in the Advanced Settings→ Splash Screen window

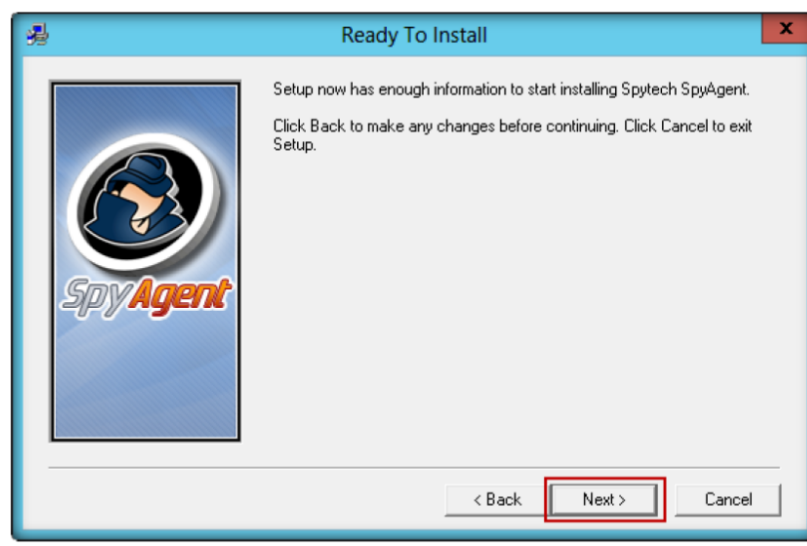


FIGURE 14.7: Ready to install window

12. It will prompt for include an **uninstaller**. Click **Yes**.

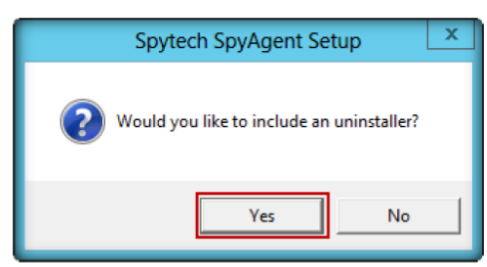


FIGURE 14.8: Selecting an uninstaller

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

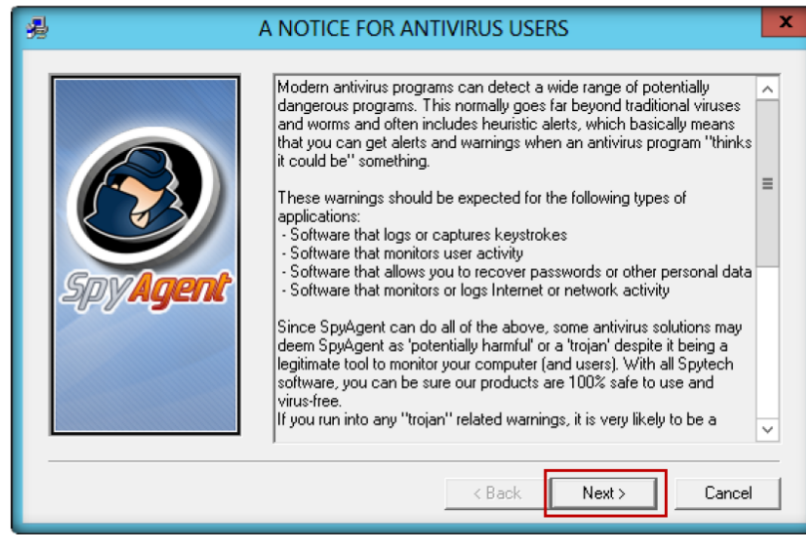


FIGURE 14.9: Accept Antivirus notice

Log Location: this allows you to specify where you want SpyAgent to store its activity logs. For Windows NT/2000/XP systems monitoring ALL users it is recommended that the log location be set to x:\documents and settings\all users

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

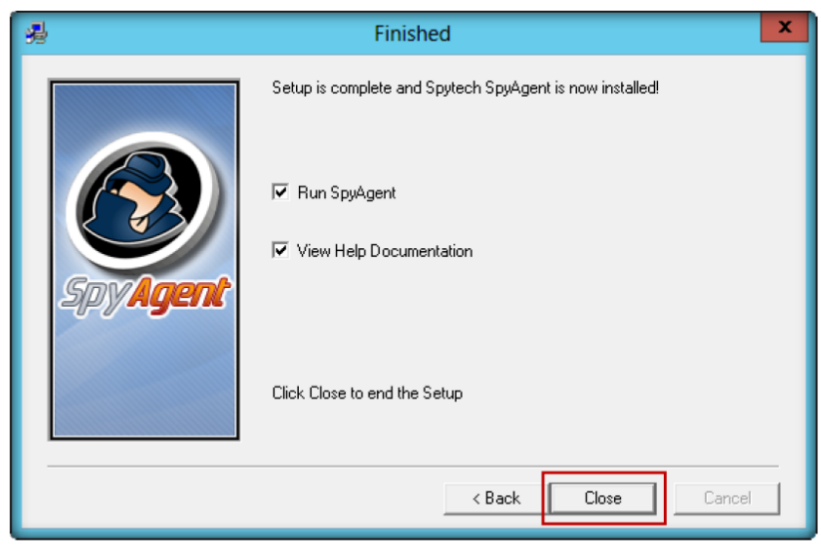


FIGURE 14.10: Finish window

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

FIGURE 14.11: Welcome SpyAgent window

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

SpyAgent can deliver its activity logs in secret to your own personal email or FTP account

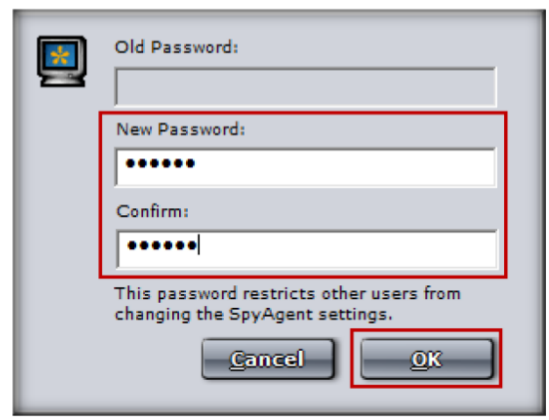


FIGURE 14.12: Selecting New Password

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

FIGURE 14.13: Welcome SpyAgent window

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

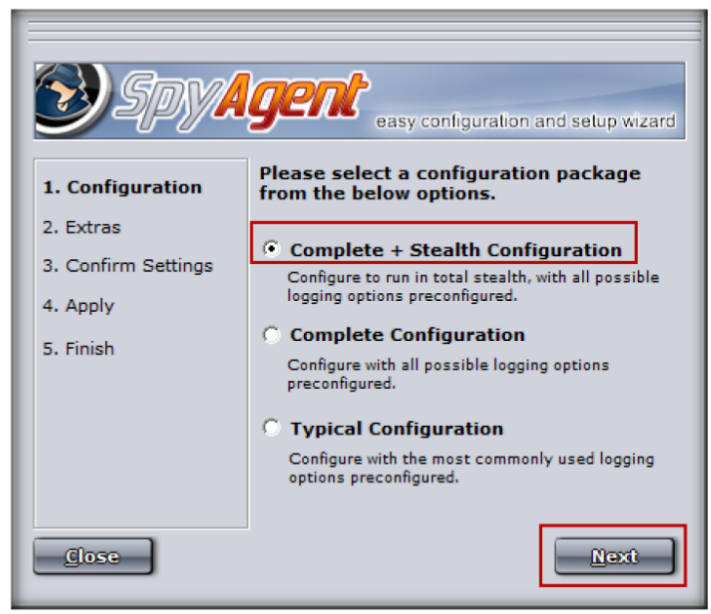


FIGURE 14.14: Selecting configuration package

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

Internet Traffic Data: This log 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

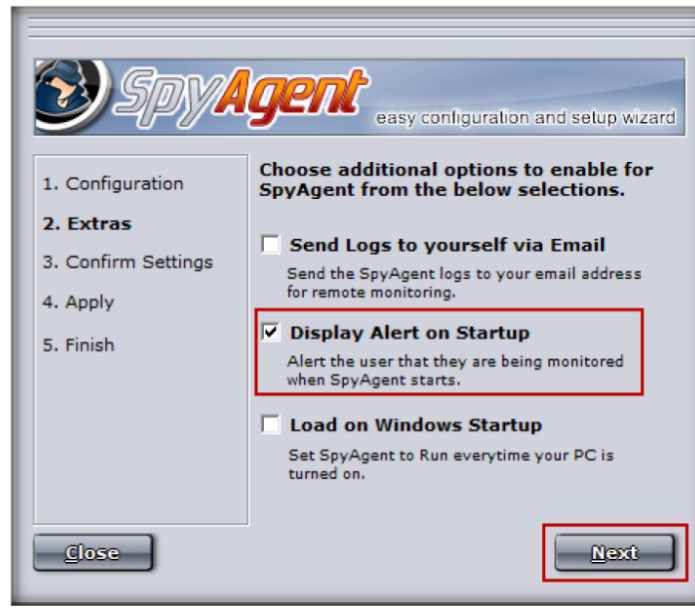


FIGURE 14.15: Selecting additional option

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

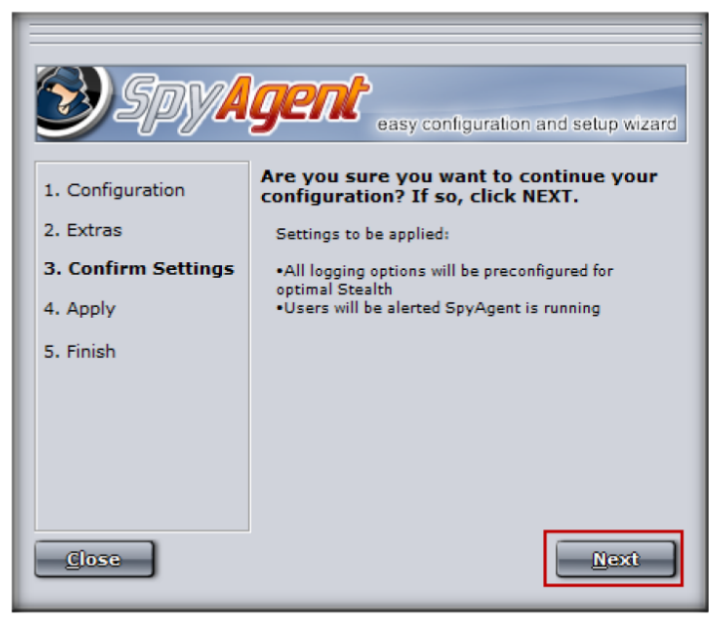


FIGURE 14.16: Confirm setting wizard

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

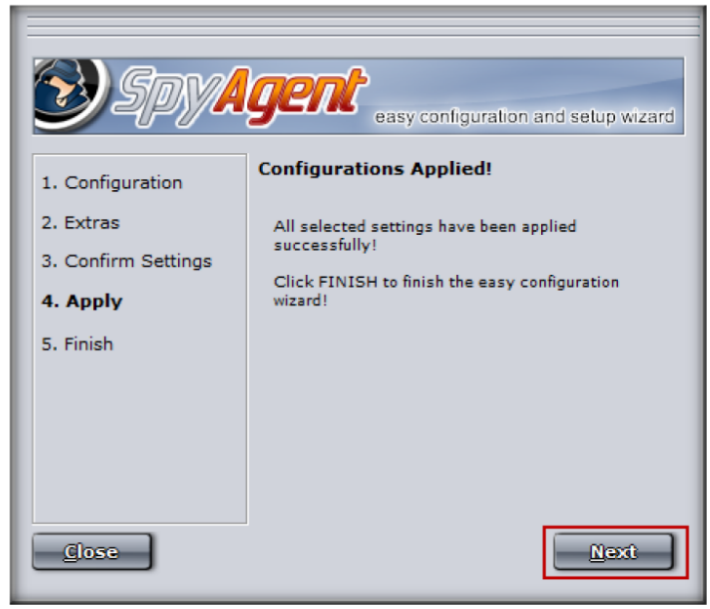


FIGURE 14.17: Configuration applied window

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

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

FIGURE 14.18: Configuration finished window

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

FIGURE 14.19: Main window of SpyAgent

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

TASK 2

Monitoring User Activities

FIGURE 14.20: Start monitoing

28. When the **Enter Access Password** window appears, enter the **password**.
29. Click **OK**.

FIGURE 14.21: Entering the password

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

30. 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.

FIGURE 14.22: Stealth mode notice

SpyAgent allows you to save all of SpyAgent's keystrokes, websites, windows, applications, connections, clipboard, activity, print jobs, file usage, and documents logs to a specified directory at once - for easier viewing later on - or so you can clear your logs without losing data.

31. It will show the following window, with the options select **Do not show this Help Tip** again and select **Do not show Related Help Tips like this again**. Click **click to continue...**

FIGURE 14.23: Start monitoing

SpyAgent features a large set of reporting tools that allow you to save and prepare log data for later viewing, documentation, and printing. All reports are formatted in HTML format for viewing with your web-browser.

32. Now browse the Internet (anything). To bring spyAgent out of stealth mode press **CONTROL+SHIFT+ALT+M** on your keyboard.
33. It will ask for the Access Password; enter the password and click **OK**.

FIGURE 14.24: Entering the password

34. To check user keystrokes from the keyboard, click **Keystrokes Typed** from **General User Activities**.
35. It will show all the resulting keystrokes as shown in the following screenshot.

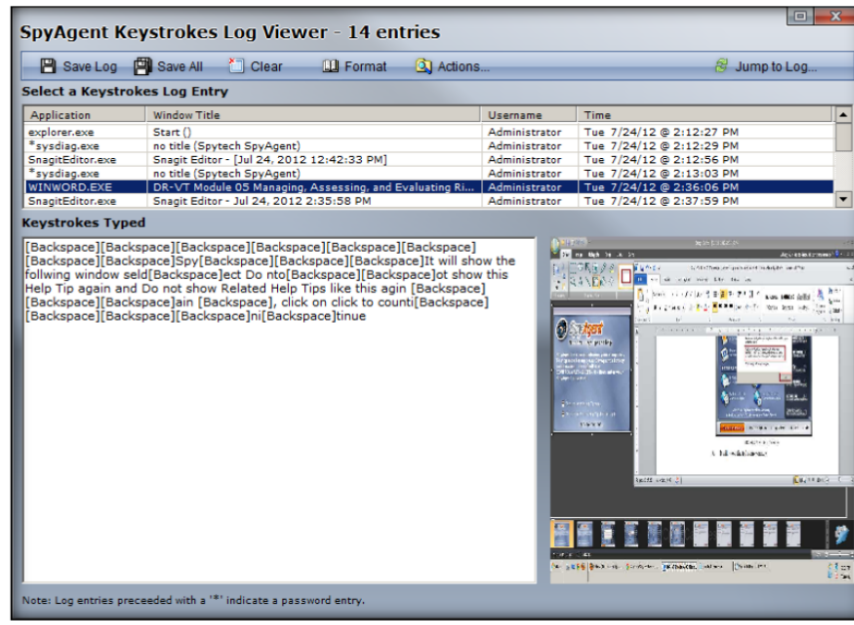


FIGURE 14.25: Resulted keystrokes

36. To check the websites visited by the user, click **Website Visited** from **Internet Activities**.

37. It will show all the user visited websites results, as shown in the following screenshot .

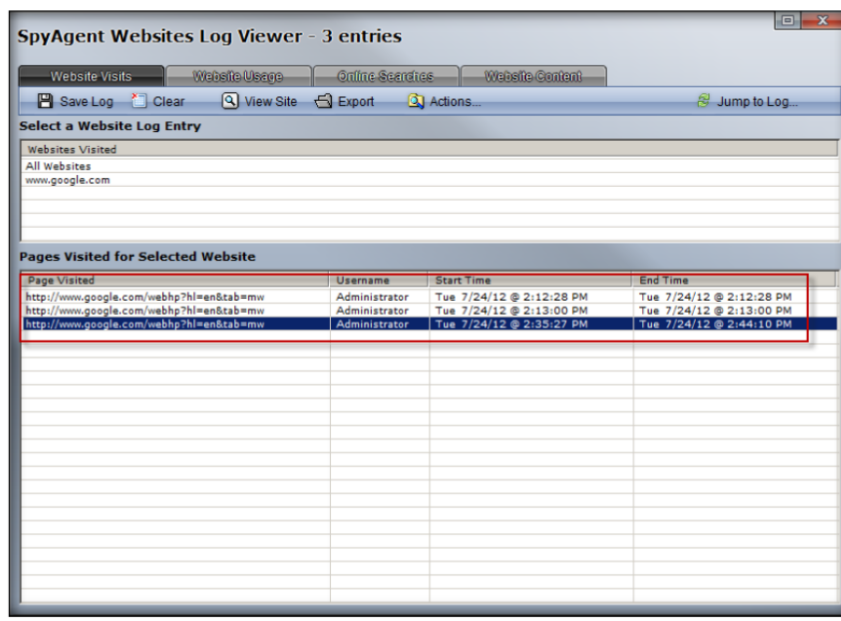


FIGURE 14.26: Result of visited websites

Lab Analysis

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

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Spytech SpyAgent	**Output:** ▪ Monitoring keystrokes typed ▪ Website log entries ▪ Pages visited for selected website ▪ Internet traffic data

Internet Connection Required	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Lab

15

Web Activity Monitoring and Recording Using Power Spy 2013

Power Spy 2013 software allows you to secretly monitor and record all activities on your computer, and this is completely legal.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Today, employees are given access to computers, telephones, 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 computers and wireless telephones 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.

In this lab, we explain monitoring employee or student activity using Power Spy 2013.

Lab Objectives

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

The objective of this lab is to help students use the Activity Monitor tool. After completing this lab, students will be able to:

- Install and configure **Power Spy 2013**
- Monitor keystrokes typed, websites visited, and Internet Traffic Data

Lab Environment

To perform the lab, you need:

- A computer running **Windows Server 2012**
- Administrative privileges to install and run tools
- You can also download Power Spy tool from http://ematrixsoft.com/download-power-spy-software.php

- If you decided to download latest version screenshots may differ
- Run this tool in Windows Server 2012

Lab Duration

Time: 15 Minutes

Overview of Power Spy 2013

Power Spy software records Facebook use and all keystrokes typed, and captures all chats and IMs in Windows Live Messenger (MSN Messenger) , Skype, Yahoo Messenger, Tencent QQ, Google Talk, GADU-GADU, ICQ, AOL Instant Messenger (AIM), and others. It records all websites visited, emails read, documents opened, windows opened, clipboard activities, passwords typed, and applications executed.

Lab Tasks

The basic idea in this section is to:

TASK 1

Installation of Power Spy 2013

1. Navigate to **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Spywares\Email and Internet Spyware\Power Spy**.
2. Double-click **pcspy.exe**. The **Software License Agreement** window appears. You must accept the agreement to install Power Spy.
3. Click **Next** in the **License Agreement** wizard.

You can download the Power Spy 2013 from *http://ematrixsoft.com/index.php*

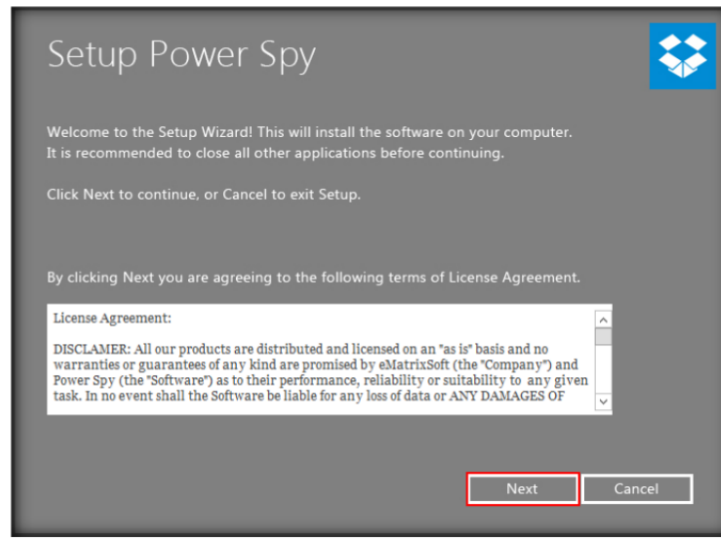


FIGURE 15.1: Installation of Spytech SpyAgent

4. Setup has finished the installation on the system. Click **Finish**.

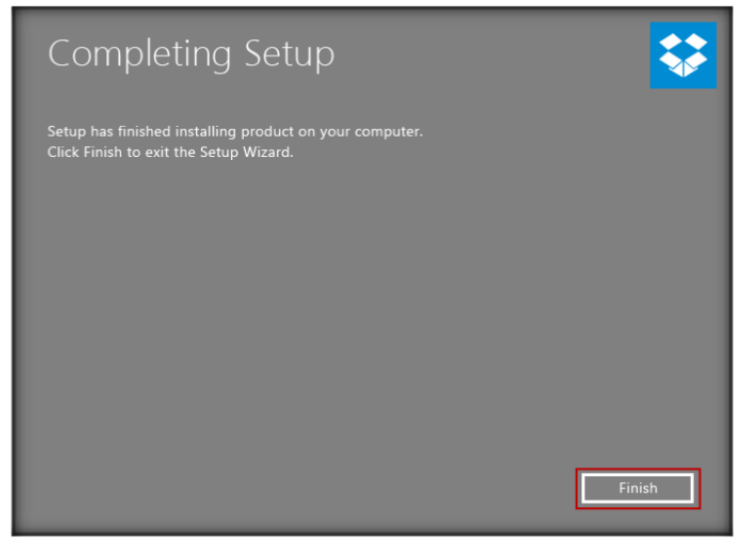


FIGURE 15.2: Select the Agreement

Keystrokes Typed – log all keystrokes, including optional non-alphanumerical keys, typed with time, Windows username, application name and window caption

5. The **Run as administrator** window appears. Click **Run**.

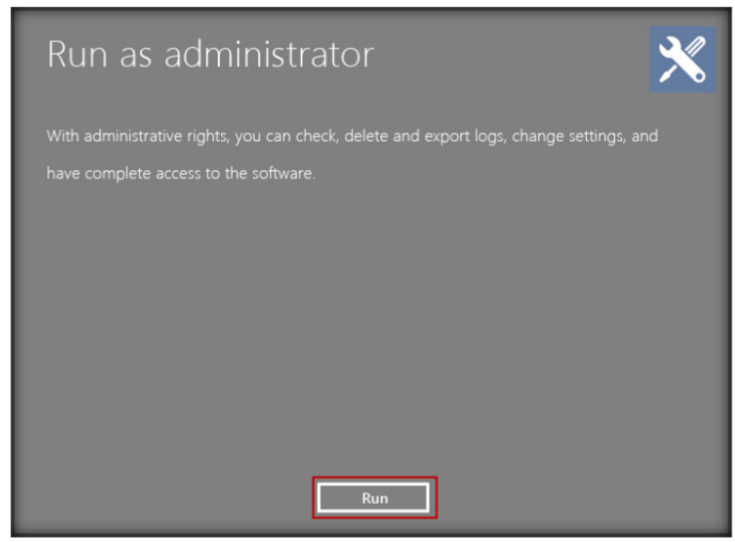


FIGURE 15.3: Selecting folder for installation

Net Chatting Conversations – monitor and record all latest version Windows Live Messenger / Skype / MSN Messenger / ICQ / AIM / Yahoo! Messenger's BOTH SIDES chatting conversations with time, chat users, and all coming/outgoing messages

6. The **Setup login password** window appears. Enter the password in the **New password** field, and retype the same password in the **Confirm password** field.
7. Click **Submit**.

Screen Snapshots – automatically captures screenshots of entire desktop or active windows at set intervals. Save screenshots as JPEG format images on your computer harddisk. Automatically stop screenshot when user is inactive

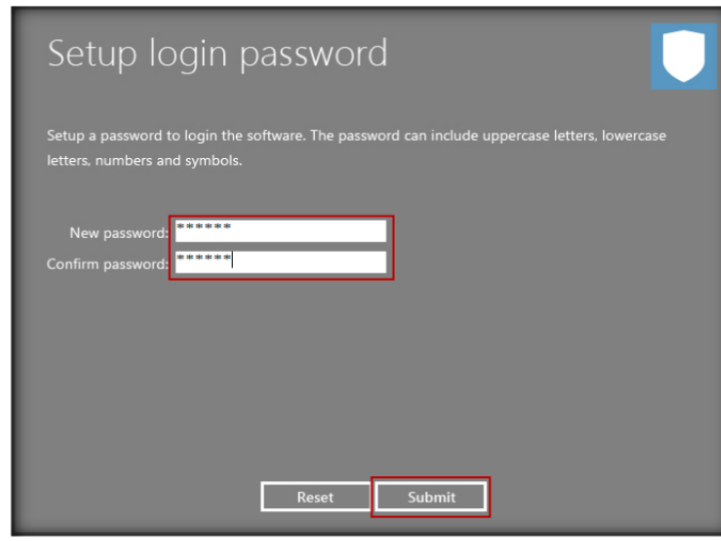


FIGURE 15.4: Selecting New Password

8. The **Information** dialog box appears. Click **OK**.

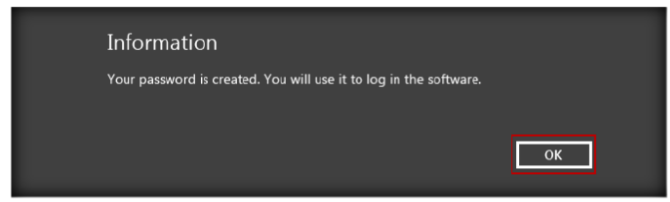


FIGURE 15.5: password confirmation window

9. The **Enter login Password** window appears. Enter the password (which is already set).
10. Click **Submit**

Self-Actions – record Power Spy administrator operations, like start or stop monitoring

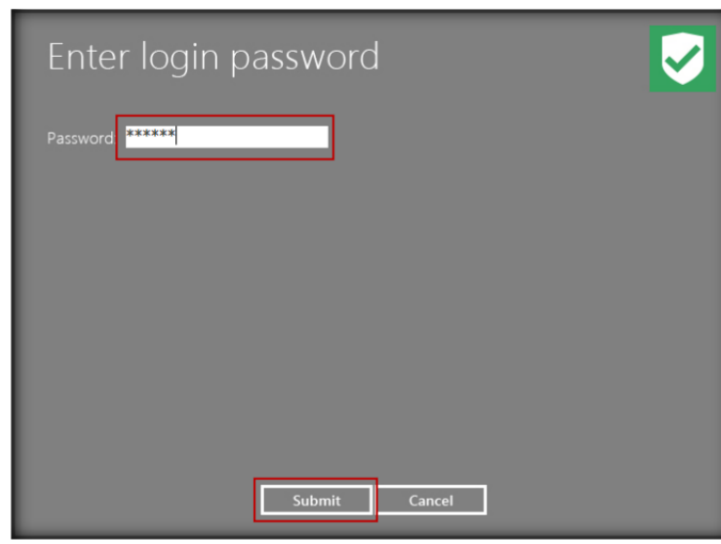


FIGURE 15.6: Enter the password

11. The **Register product** window appears. Click **Later** to continue.

Stealth Mode: Power Spy run absolutely invisibly under Windows systems and does not show in Windows task list. None will know it's running unless you tell them! You can also choose to hide or unhide Power Spy icon and its uninstall entry

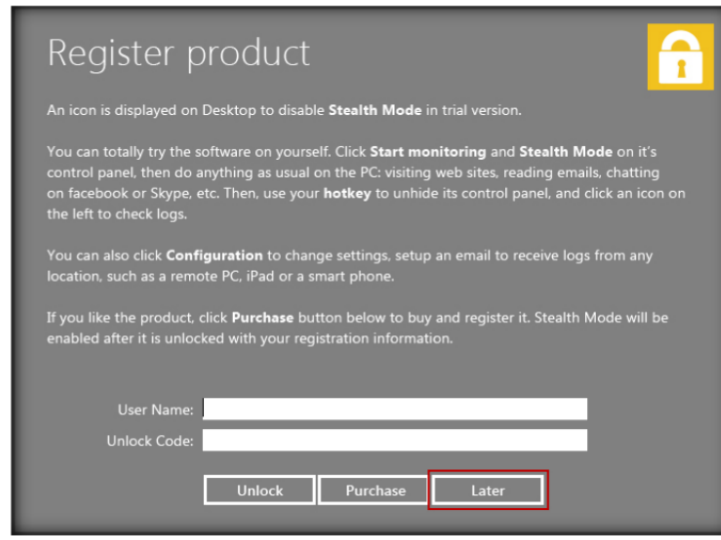


FIGURE 15.7: Register product window

12. The main window of **Power Spy** appears, as displayed in the following figure.

Task Schedule: You can set starting and ending time for each task to automatically start and stop the monitoring job.

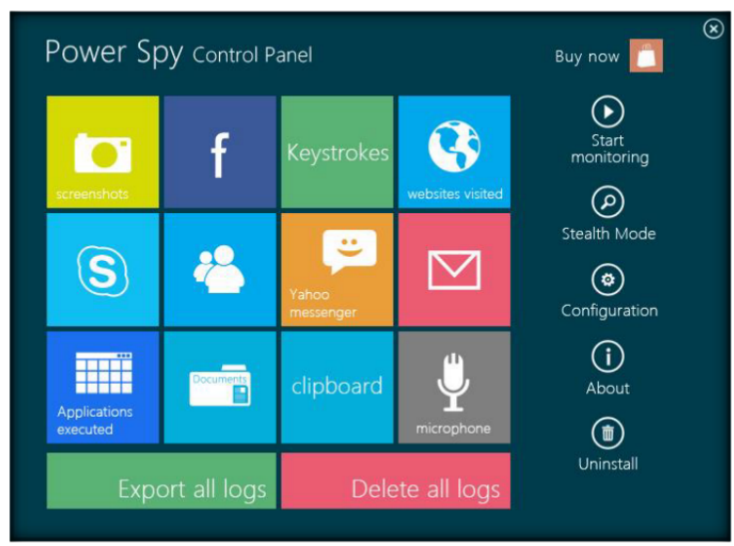


FIGURE 15.8: Main window of Power Spy

13. Click **Start monitoring**.

TASK 2

Monitoring and Recording User Activities

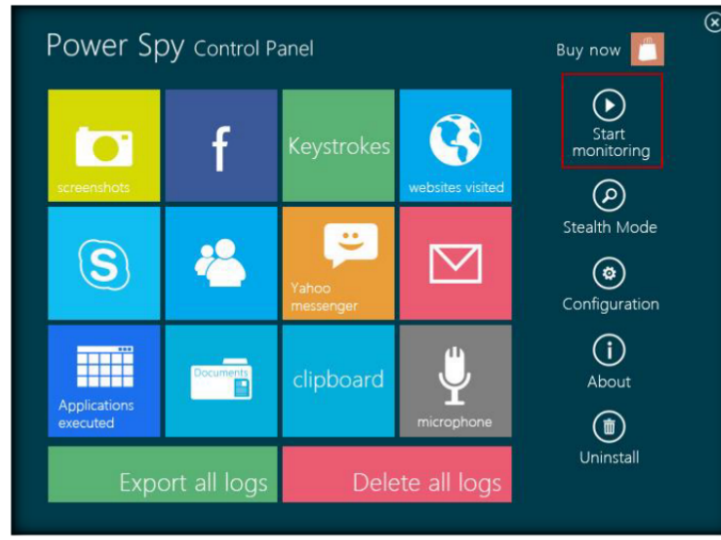


FIGURE 15.9: Start monitoring

Logs View: choose to view different type of logs from program main interface. You can delete selected logs or clear all logs, search logs or export logging reports in HTML format

14. The **System Reboot Recommended** window appears. Click **OK**.

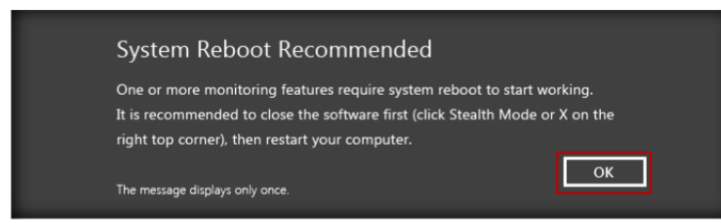


FIGURE 15.10: System Reboot Recommended window

15. Click **Stealth Mode** (stealth mode runs the Power Spy completely invisibly on the computer) .
16. The **Hotkey reminder** window appears. Click **OK** (to unhide Power Spy, use the **Ctrl+Alt+X** keys together on your PC keyboard).

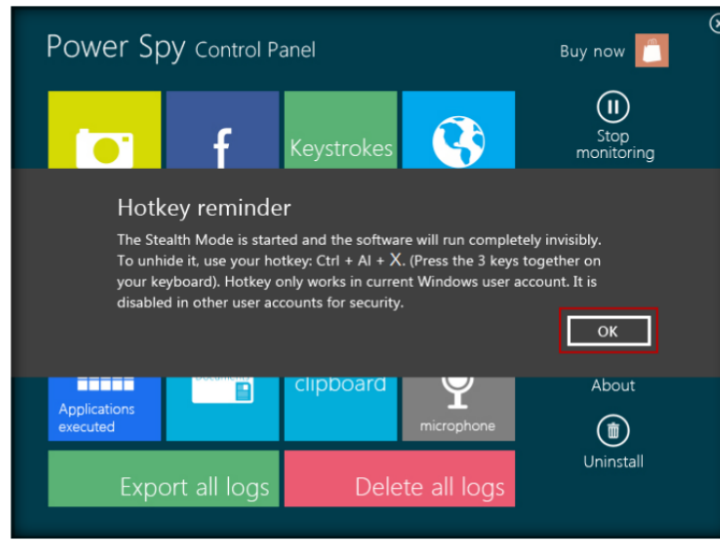


FIGURE 15.11: Stealth mode window

Easy-to-use Interface: config Power Spy with either Wizard for common users or control panel for advanced users. User-friendly graphical program interface makes it easy for beginngers.

17. The **Confirm** window appears Click **Yes**.

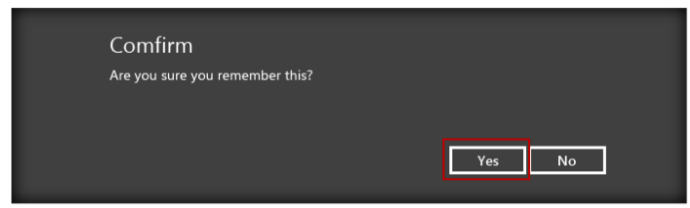


FIGURE 15.12: Stealth mode notice

18. Now browse the Internet (anything). To bring Power Spy out of stealth mode, press **CONTROL+ALT+X** on your keyboard.
19. The **Run as administrator** window appears. Click **Run**.

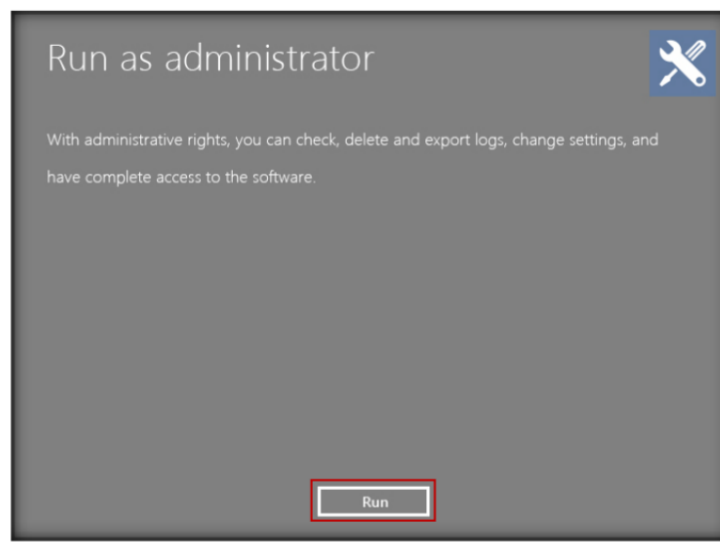


FIGURE 15.13: Run as administrator

20. The **Enter login password** window appears. Enter the password (which is already set) .
21. Click **Submit**.

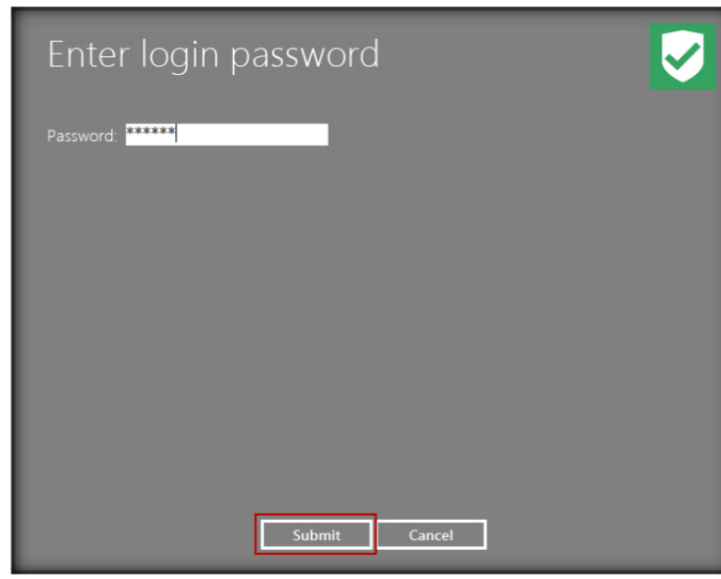


FIGURE 15.14: Enter the password

22. Click **Later** in the **Register product** window to continue if it appears.
23. Click **Stop monitoring** to stop the monitoring.

FIGURE 15.15: Stop the monitoring

24. To check user keystrokes from the keyboard, click **Keystrokes** in **Power Spy Control Panel**.

Program Executed – log all programs including application, executable file, documents and directories navigated with time, Windows username, application/document/directory name and file paths..

FIGURE 15.16: Selecting keystrokes from Power spy control panel

25. It will show all the resulted **keystrokes** as shown in the following screenshot.
26. Click the **Close** button.

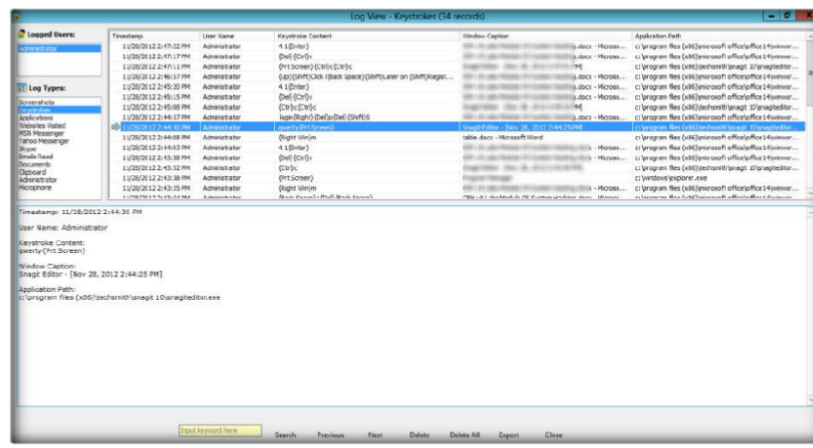


FIGURE 15.17: Resulted keystrokes

Documents Opened – log all text contents of documents opened in MS Word and NotePad.

27. To check the websites visited by the user, click **Website visited** in the **Power Spy Control Panel**.
28. It will show all the **visited websites**, as shown in the following screenshot.

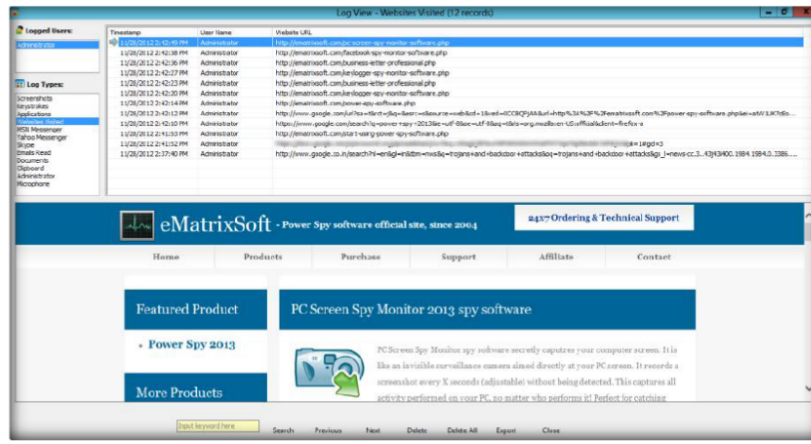


FIGURE 15.18: Result of visited websites

Lab Analysis

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

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
PowerSpy 2013	**Output:** ▪ Monitoring keystrokes typed ▪ Website log entries ▪ Pages visited for selected website ▪ Internet traffic data

Internet Connection Required	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Lab

16

Image Steganography Using QuickStego

QuickStego hides text in pictures so that only other users of QuickStego can retrieve and read the hidden secret messages.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Porn sites are filled with images that sometimes change multiple times each day, require authentication in some cases to access their "better" areas of content, and by using stenographic techniques, would allow an agent to retrieve messages from their home bases and send back updates, all in porn trading. Thumbnails could be scanned to find out if there are any new messages for the day; once decrypted, these messages would point to links on the same site with the remaining information encrypted.

Terrorists know that so many different types of files can hold all sorts of hidden information, and tracking or finding these files can be an almost impossible task. These messages can be placed in plain sight, and the servers that supply these files will never know it. Finding these messages is like finding the proverbial "needle" in the World Wide Web haystack.

In order to be an expert an ethical hacker and penetration tester, you must understand how to hide the text inside the image. In this lab, we show how text is hidden inside an image using the QuickStego tool.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

Lab Objectives

The objective of this lab is to help the students learn how to **hide secret text messages** in an **image**.

Lab Environment

To perform the lab, you need:

- A computer running **Windows Server 2012**
- Administrative privileges to install and run tools

- **QuickStego** is located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Steganography\Image Steganography\QuickStego**
- You can also download Quick Stego tool from http://quickcrypto.com/free-steganography-software.html
- If you decided to download latest version screenshots may differ
- Run this tool in Windows Server 2012

Lab Duration

Time: 10 Minutes

Overview of Steganography

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include stenographic coding inside of a transport layer, such as a document file, image file, program, or protocol.

Lab Tasks

The basic idea in this section is to:

1. Follow the wizard-driven installation steps to install Quick Stego
2. Launch **Quick Stego** from Start menu apps

TASK 1

Hide the text inside the image

You can download the QuickStego from *http://quickcrypto.com*

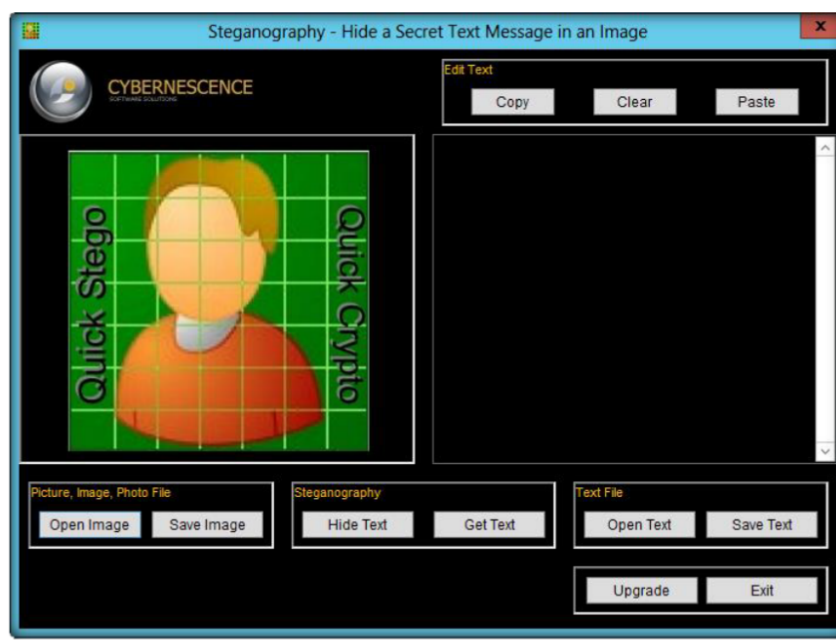


FIGURE 16.1: Main window of the QuickStego

3. Click **Open Image** in the **Picture, Image, Photo File** dialog box.

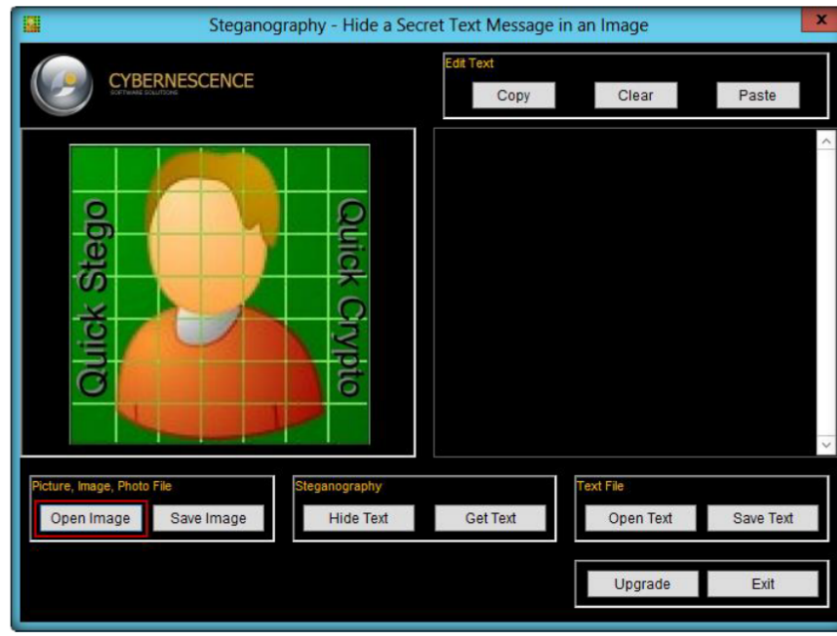


FIGURE 16.2: Opening the image

Image Types that can be opened - .jpg/.jpeg, .gif, or .bmp formats

4. Browse the image from **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Steganography\Image Steganography\QuickStego**.
5. Select **lamborgini_5.jpg**, and then click the **Open** button.

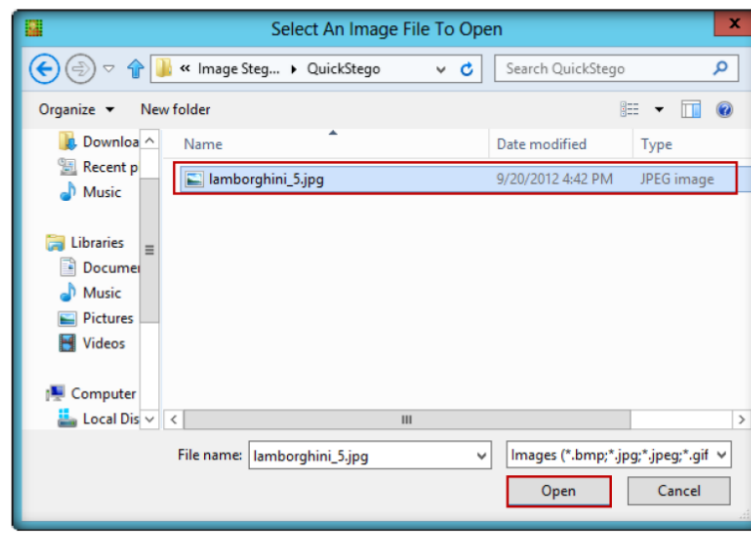


FIGURE 16.3: Selecting the image

Saved Hidden Text Images - .bmp format only

6. The selected image is added; it will show a message that reads: **THIS IMAGE DOES NOT HAVE A QUICK STEGO SECRET TEXT MESSAGE**.

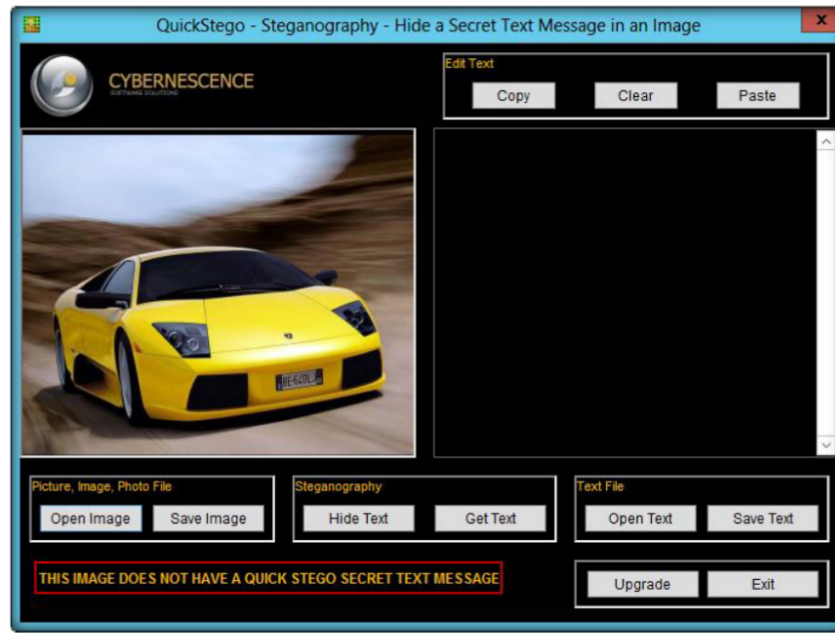


FIGURE 16.4: Selected image is displayed

QuickStego does not ENCRYPT the secret text message though it is well hidden in the image. QuickCrypto includes the functions of QuickStego but also allows you to securely encrypt text and files and even hide files on your computer.

7. To add the text to the image, click **Open Text** from the **Text File** dialog box.

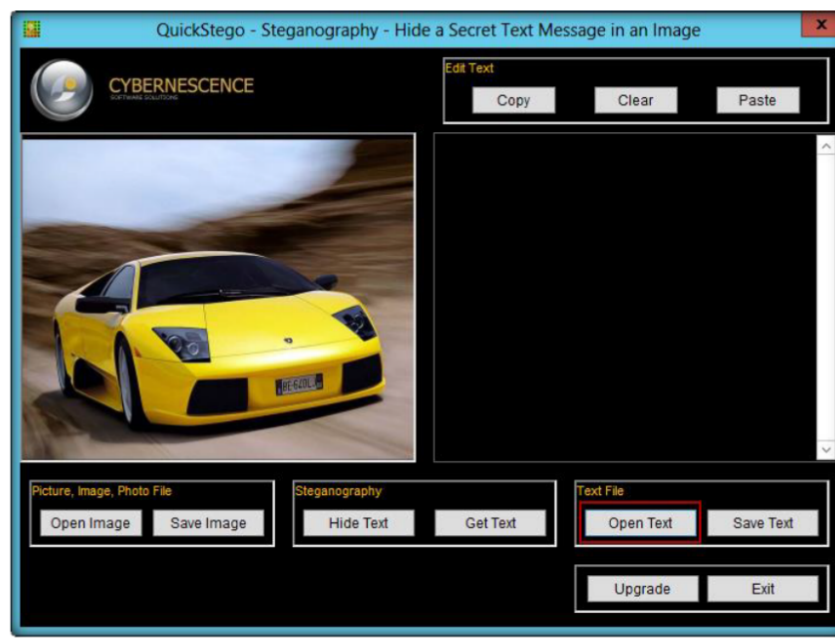
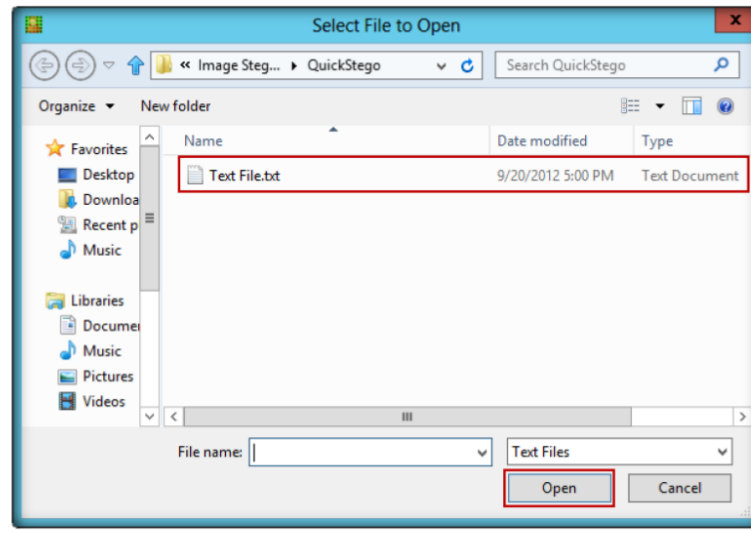


FIGURE 16.5: Selected text file

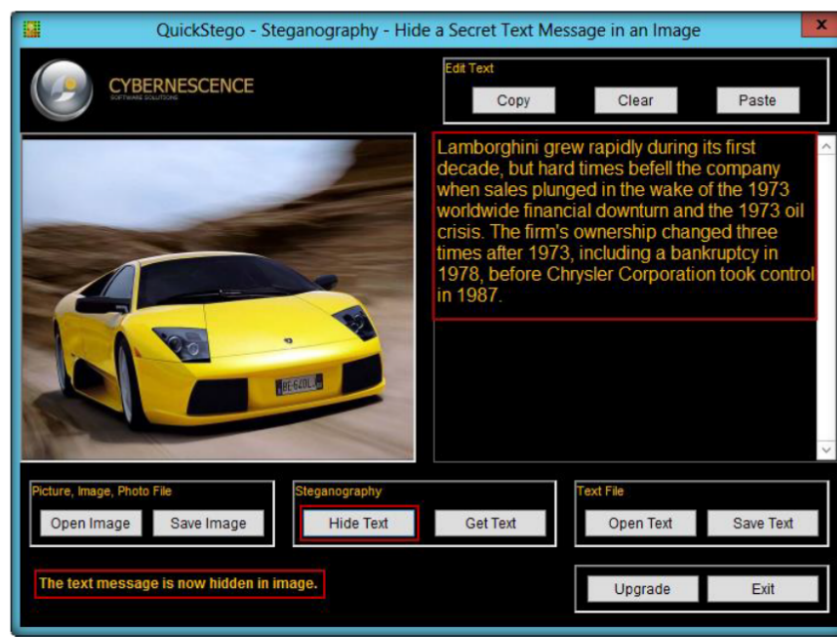
8. Browse the text file from **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Steganography\Image Steganography\QuickStego**.
9. Select Text File.txt file, and then click the **Open** button.



The core functions of QuickStego are also part of QuickCrypto, therefore the product will be supported for the foreseeable future. Functionality on its way is the ability to hide messages inside audio files, e.g. mp3 and wav.

FIGURE 16.6: Selecting the text file

10. The selected text will be added; click **Hide Text** in the **Steganography** dialog box.
11. It shows the following message: **The text message is now hidden in image**.



The larger the image, the more text that can be concealed within. QuickStego will tell you how many characters of text you must lose if you go over this limit per picture. In practice a lot of secret text can be hidden in even a small image.

FIGURE 16.7: Hiding the text

12. To save the image (where the text is hidden inside the image) click **Save Image** in the **Picture, Image, Photo File** dialog box.

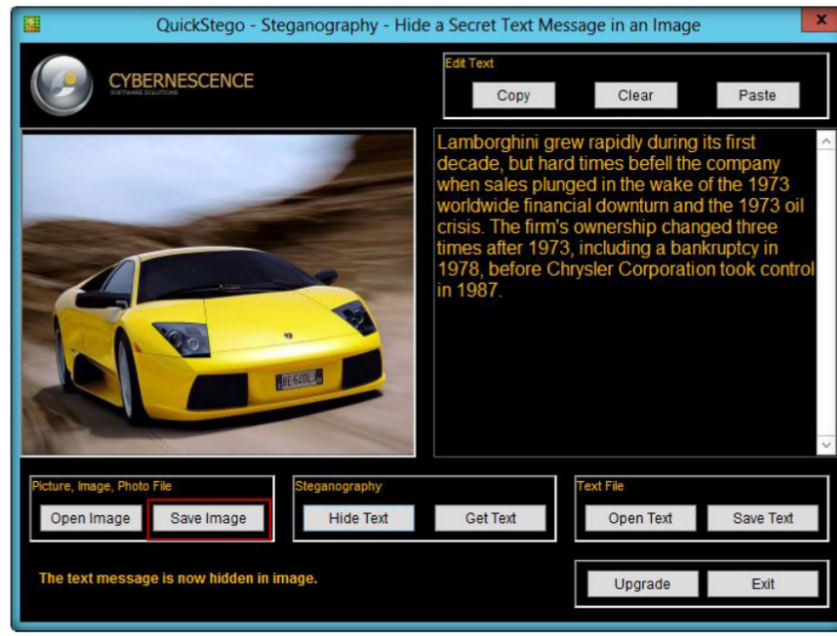


FIGURE 16.8: Save the steganography image

QuickStego imperceptibly alters the pixels (individual picture elements) of the image, encoding the secret text by adding small variations in color to the image. In practice, to the human eye, these small differences do not appear to change the image

13. Provide the file name as **stego**, and click **Save** (to save this file on the desktop).

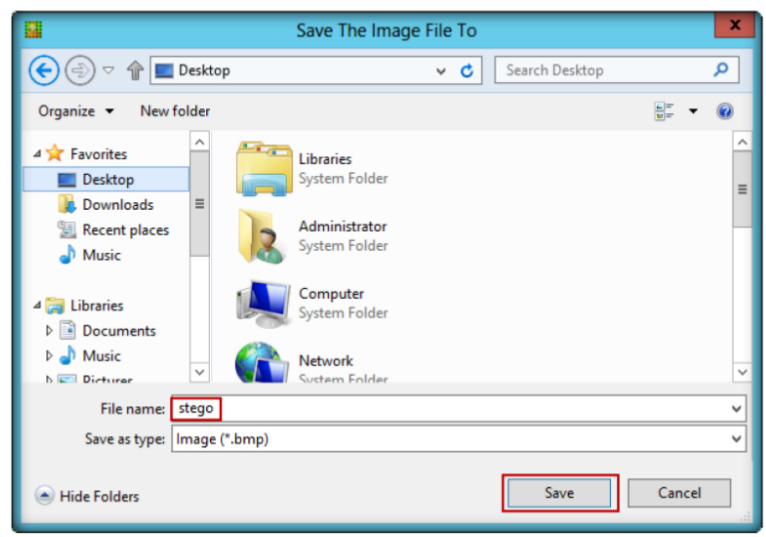


FIGURE 16.9: Browse for saved file

14. **Exit** from the **QuickStego** window. Again open QuickStego, and click **Open Image** in the **Picture, Image, Photo File** dialog box.
15. Browse the **Stego** file (which is saved on desktop).
16. The hidden text inside the image will appear as displayed in the following figure.

Approximately 2MB of free hard disk space (plus extra space for any images)

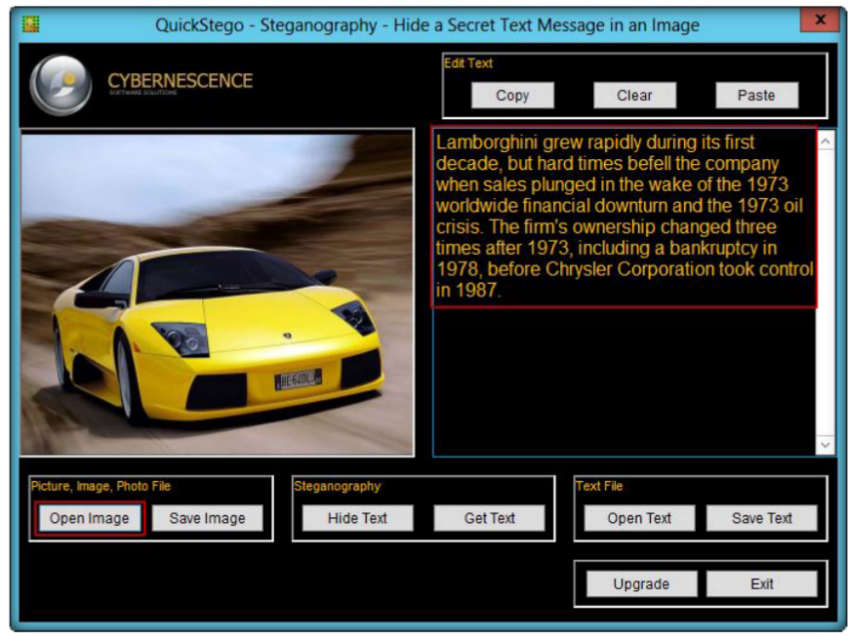


FIGURE 16.10: Hidden text is showed

Lab Analysis

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

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
QuickStego	**Image Used:** Lamborghini_5.jpg
	Output: The hidden text inside the image will be shown

Internet Connection Required	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs