Lab 4

Perform Website Footprinting

Website footprinting refers to monitoring and analyzing the target organization's website for information.

Lab Scenario

ICON KEY

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

As a professional ethical hacker, you should be able to extract a variety of information about the target organization from its website; by performing website footprinting, you can extract important information related to the target organization's website such as the software used and the version, operating system details, filenames, paths, database field names, contact details, CMS details, the technology used to build the website, scripting platform, etc. Using this information, you can further plan to launch advanced attacks on the target organization.

Lab Objectives

- Gather information about a target website using ping command line utility
- Gather information about a target website using Website Informer
- Extract a company's data using Web Data Extractor
- Mirror the target website using HTTrack Web Site Copier
- Gather a wordlist from the target website using CeWL

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Web Data Extractor located at **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Web Spiders\Web Data Extractor**

- HTTrack Web Site Copier located at **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Website Mirroring Tools\HTTrack Web Site Copier**
- You can also download the latest versions of **Web Data Extractor** and **HTTrack Web Site Copier** from their official websites. If you decide to download the latest versions, the screenshots shown in the lab might differ.

Lab Duration

Time: 35 Minutes

Overview of Website Footprinting

Website footprinting is a technique used to collect information regarding the target organization's website. Website footprinting can provide sensitive information associated with the website such as registered names and addresses of the domain owner, domain names, host of the sites, OS details, IP details, registrar details, emails, filenames, etc.

Lab Tasks

TASK 1

Gather Information About a Target Website using Ping Command Line Utility

1. Turn on the **Windows 10** virtual machine.
2. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.

TASK 1.1

Finding the IP Address of a Target Domain

3. Open the **Command Prompt** window. Type **ping www.certifiedhacker.com** and press **Enter** to find its IP address. The displayed response should be similar to the one shown in the screenshot.

Ping is a network administration utility used to test the reachability of a host on an IP network and measure the round-trip time for messages sent from the originating host to a destination computer

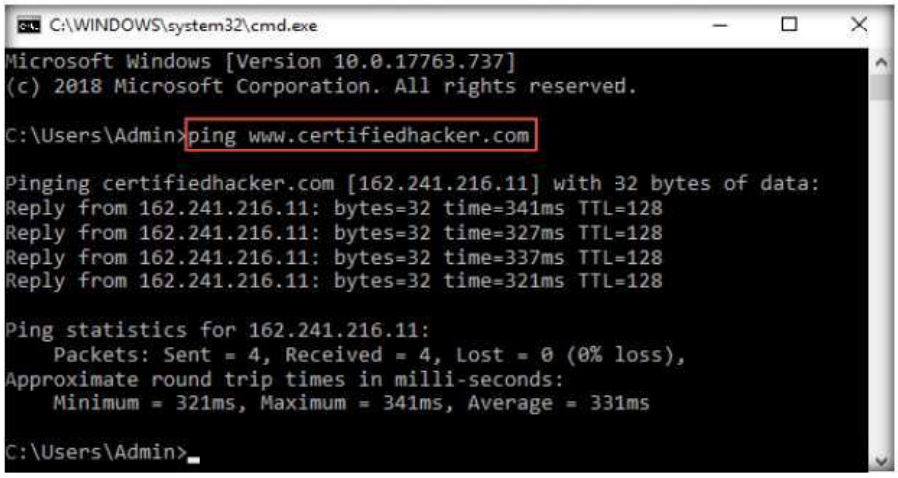

Figure 4.1.1: The ping command to extract the IP address for www.certifiedhacker.com

4. Note the target domain's IP address in the result above (here, **162.241.216.11**). You also obtain information on Ping Statistics such as packets sent, packets received, packets lost, and approximate round-trip time.

Note: The IP address of the target website may differ in your lab environment.

TASK 1.2

Finding Maximum Frame Size

5. In the **Command Prompt** window, type **ping www.certifiedhacker.com -f -l 1500** and press **Enter**.

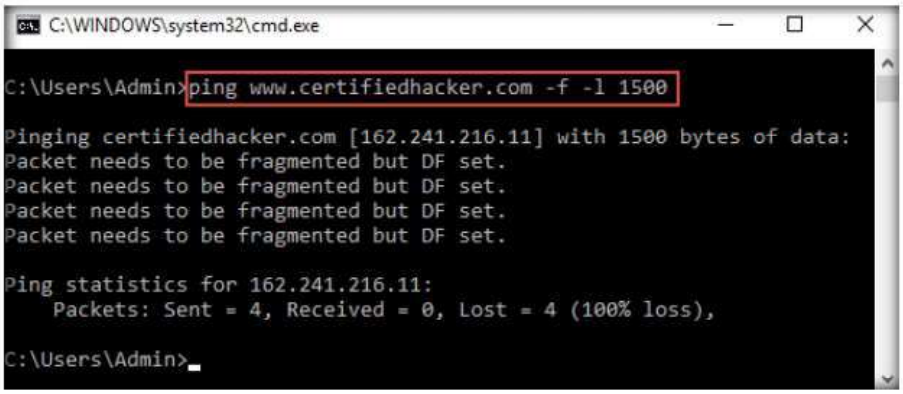

Figure 4.1.2: The ping command for www.certifiedhacker.com with -f -l 1500 options

The ping command sends an ICMP echo request to the target host and waits for an ICMP response. During this request-response process, ping measures the time from transmission to reception, known as round-trip time, and records any loss of packets. The ping command assists in obtaining domain information and the IP address of the target website.

6. The response, **Packet needs to be fragmented but DF set**, means that the frame is too large to be on the network and needs to be fragmented. The packet was not sent as we used the **-f** switch with the ping command, and the ping command returned this error.
7. In the **Command Prompt** window, type **ping www.certifiedhacker.com -f -l 1300** and press **Enter**.

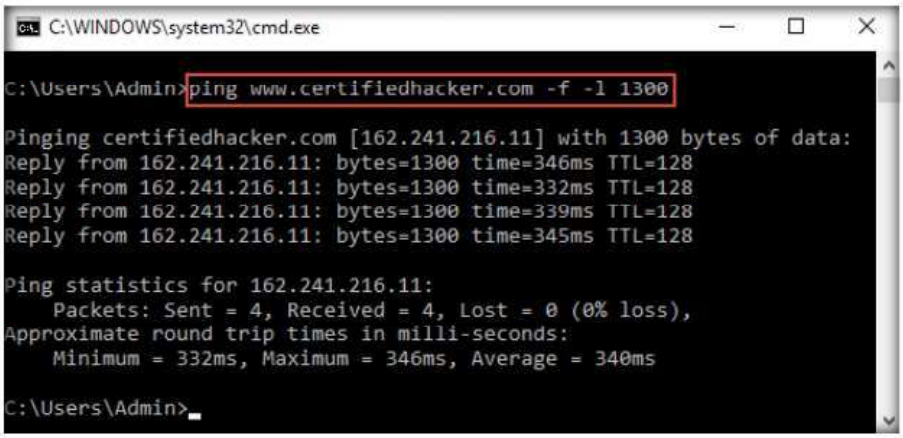

Figure 4.1.3: The ping command for www.certifiedhacker.com with -f -l 1300 options

8. Observe that the maximum packet size is less than **1500** bytes and more than **1300** bytes.

9. Now, try different values until you find the maximum frame size. For instance, **ping www.certifiedhacker.com -f -l 1473** replies with **Packet needs to be fragmented but DF set**, and **ping www.certifiedhacker.com -f -l 1472** replies with a successful ping. It indicates that **1472** bytes are the maximum frame size on this machine's network.

Note: The maximum frame size will differ depending upon the target network.

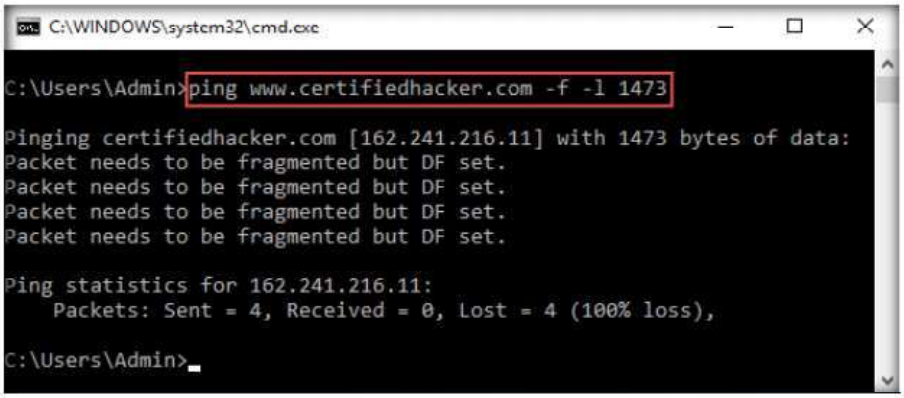

Figure 4.1.4: The ping command for www.certifiedhacker.com with -f -l 1473 options

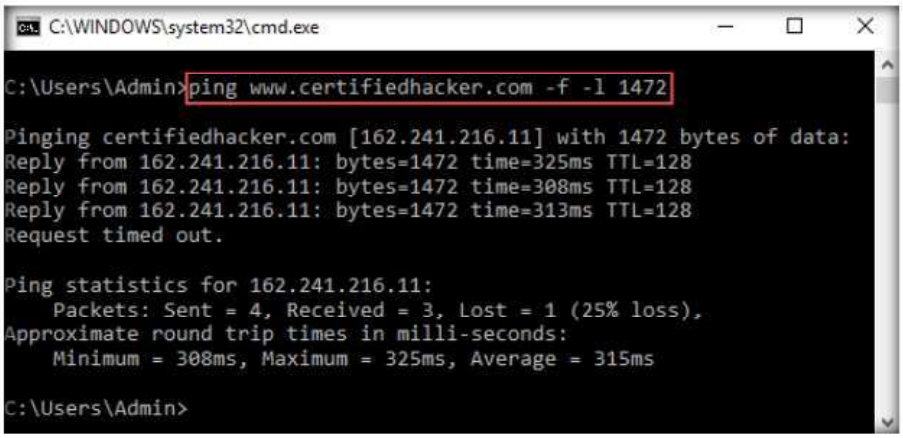

Figure 4.1.5: The ping command for www.certifiedhacker.com with -f -l 1472 options

10. Now, discover what happens when TTL (Time to Live) expires. Every frame on the network has TTL defined. If TTL reaches 0, the router discards the packet. This mechanism prevents the loss of packets.

TASK 1.3

Finding Hop Count using TTL Value

11. In **Command Prompt**, type **ping www.certifiedhacker.com -i 3** and press **Enter**. This option sets the time to live (**-i**) value as **3**.

Note: The maximum value you can set for TTL is 255.

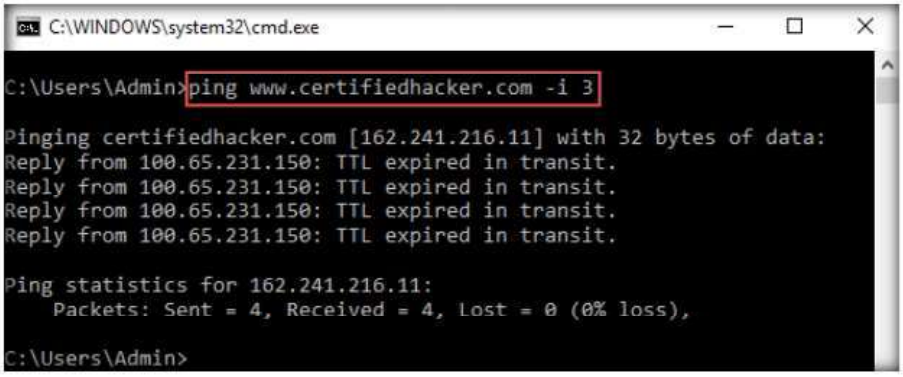

Figure 4.1.6: The ping command for www.certifiedhacker.com with –i 3 options

12. **Reply from 100.65.231.150: TTL expired in transit** means that the router (100.65.231.150, students will have some other IP address) discarded the frame because its TTL has expired (reached 0).

Note: The IP address 100.65.231.150 may vary in your lab environment.

Note: If you get the **Request timed out** reply for the above query, then use **Command Prompt of your host machine** instead of the Windows 10 virtual machine to run the query.

13. Minimize the command prompt shown above and launch a new **command prompt**. Type **ping www.certifiedhacker.com -i 2 -n 1** and press **Enter**. Here, we set the TTL value to **2** and the **-n** value to 1 to check the life span of the packet.

Note: **-n** specifies the number of echo requests to be sent to the target.

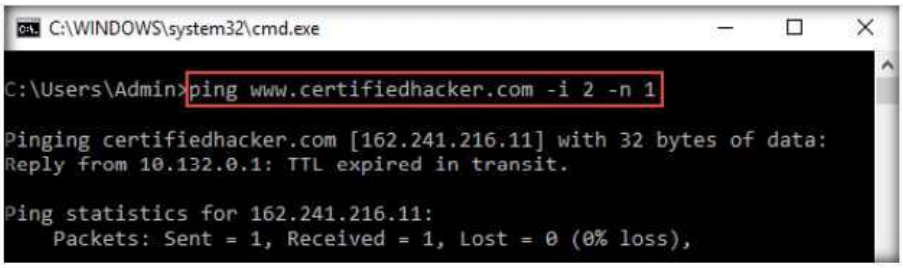

Figure 4.1.7: The ping command for www.certifiedhacker.com with –i 2 –n 1 options

14. Type **ping www.certifiedhacker.com -i 3 -n 1**. This sets the TTL value to **3**.

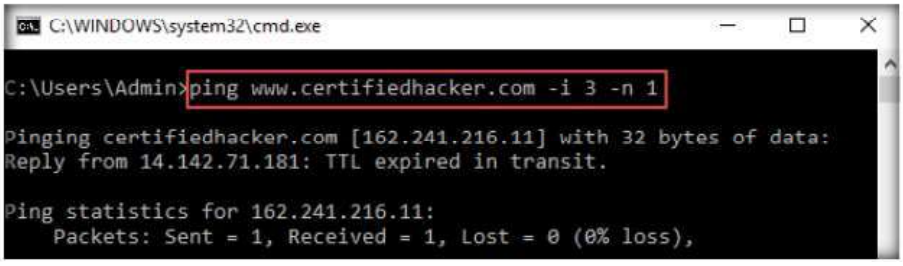

Figure 4.1.8: The ping command for www.certifiedhacker.com with –i 3 –n 1 options

15. Observe that there is a reply coming from the IP address **162.241.216.11**, and there is no packet loss.

Note: The result displayed in the above step might differ in your lab environment.

16. Now, change the time to live value to **4** by typing, **ping www.certifiedhacker.com -i 4 -n 1** and press **Enter**.

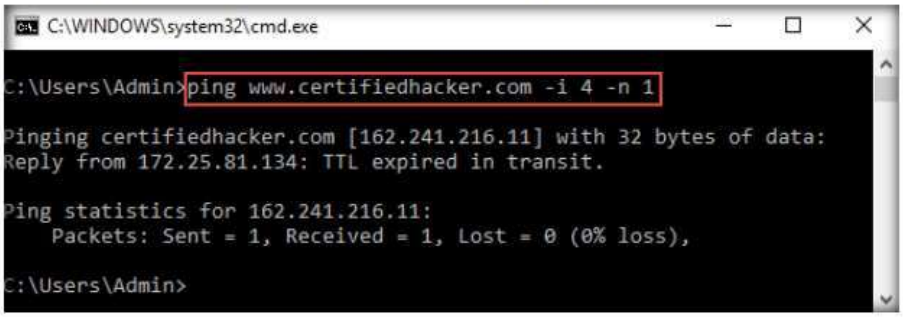

Figure 4.1.9: The ping command for www.certifiedhacker.com with –i 4 –n 1 options

17. Repeat the above step until you reach the IP address for **www.certifiedhacker.com** (in this case, **162.241.216.11**).

18. Here, the successful ping to reach **www.certifiedhacker.com** is **27** hops.

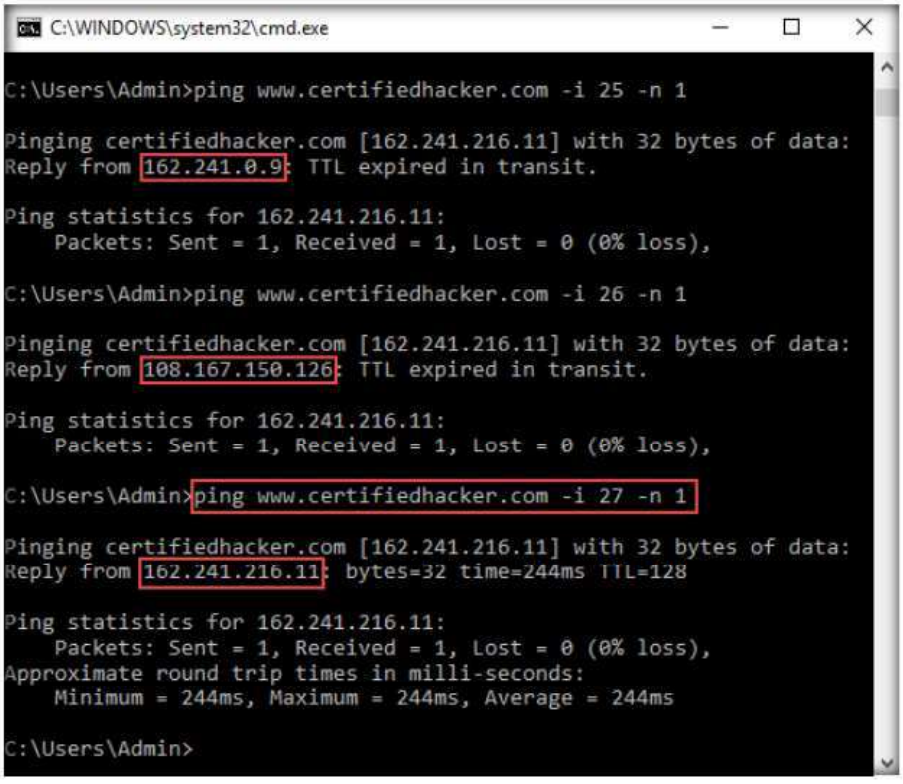

Figure 4.1.10: The ping command for www.certifiedhacker.com with –i 27 –n 1

19. This implies that, at a time to live value of **27**, the reply is received from the destination host (**162.241.216.11**).

Note: The result might vary in your lab environment.

20. This concludes the demonstration of gathering information about a target website using Ping command-line utility (such as the IP address of the target website, hop count to the target, and value of maximum frame size allowed on the target network).

21. Close all open windows and document all the acquired information.

TASK 2 Gather Information about a Target Website using Website Informer

Website Informer is an online tool that gathers detailed information on a website such as a website's traffic rank, daily visitors rate, page views, etc. Website Informer discovers the main competitors of the website, reveals DNS servers used by the website, and also obtains the Whois record of the target website.

1. In the **Windows 10** virtual machine, open a web browser (here, **Mozilla Firefox**), type **https://website.informer.com** in the address bar, and press **Enter**. The Website Informer website appears, as shown in the screenshot.

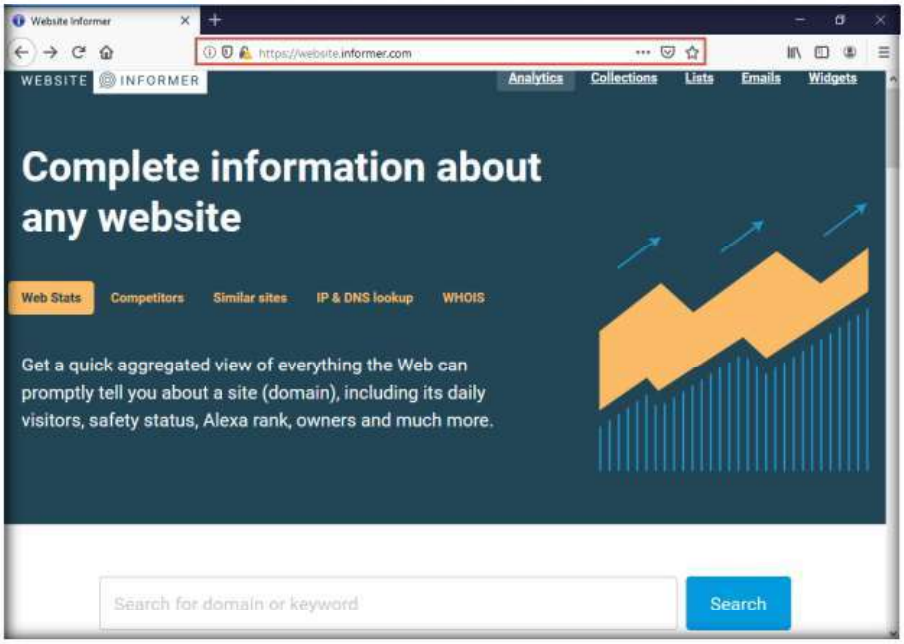

Figure 4.2.1: Website Informer website

2. To extract information associated with the target organization website, type the target website's URL (here, **www.certifiedhacker.com**) in the text field, and then click on the **Search** button, as shown in the screenshot below.

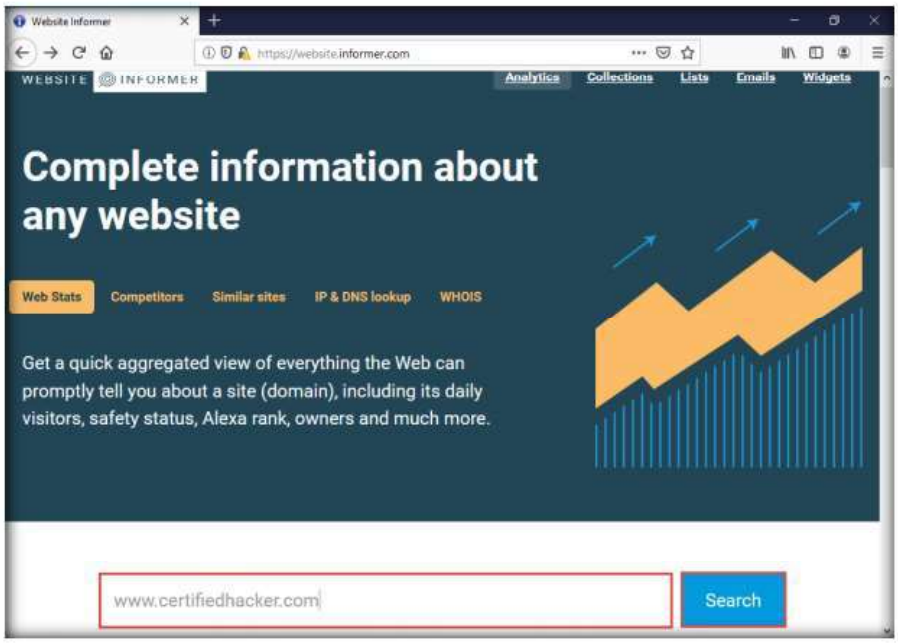

Figure 4.2.2: Enter the target website

3. A search result for **WWW.CERTIFIEDHACKER.COM** containing information such as **General Info**, **Stats & Details**, **Whois**, and **IP Whois** is displayed, as shown in the screenshot.

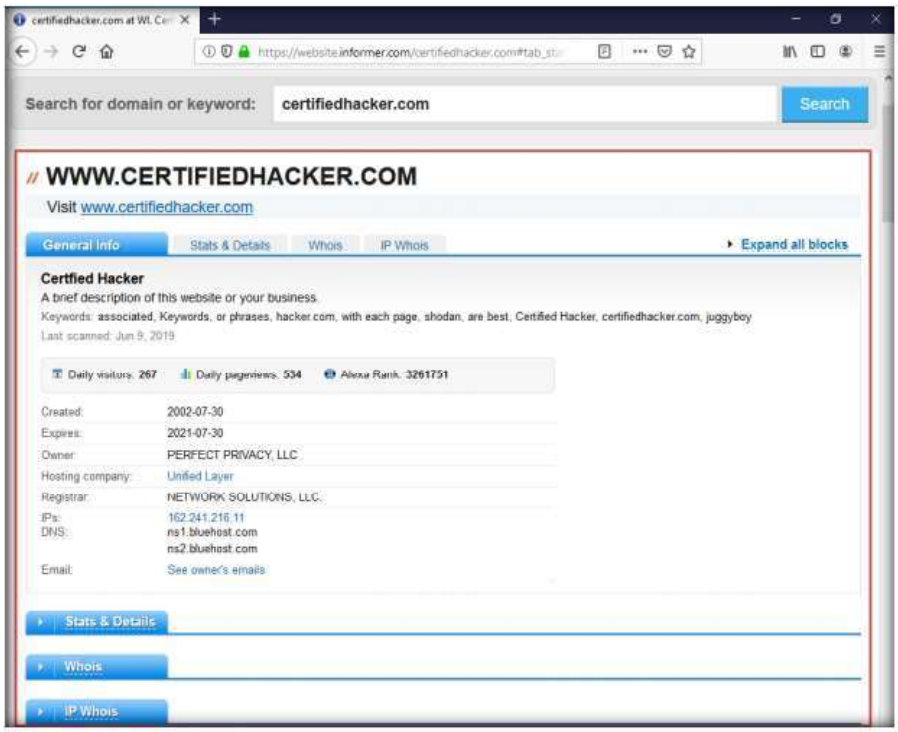

Figure 4.2.3: Search result generated by Website Informer

4. In the **General Info** tab, information such as **Created**, **Expires**, **Owner**, **Hosting company**, **Registrar**, **IPs**, **DNS**, and **Email** associated with the target website is displayed as shown in the screenshot.

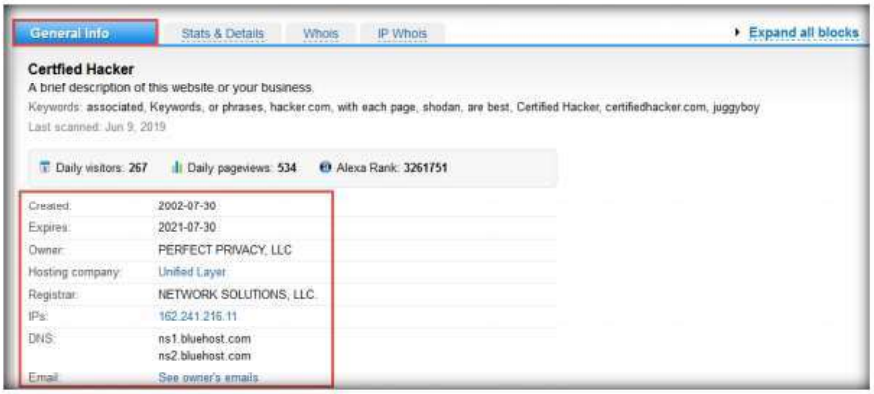

Figure 4.2.4: Website Informer General Info

5. Click on the **Whois** tab to view detailed Whois information about the target website, as shown in the screenshot.

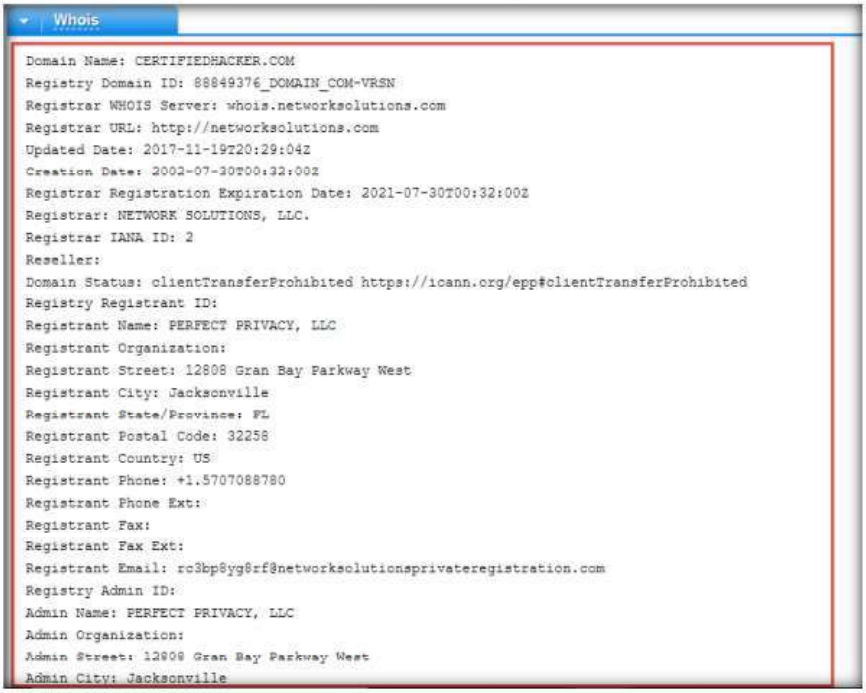

Figure 4.2.5: Website Informer Whois information

You can also use tools such as **Burp Suite** (https://portswigger.net), **Zaproxy** (https://www.owasp.org), etc. to perform website footprinting on a target website.

6. Similarly, you can click on the **Stats & Details** and **IP Whois** tabs to view the detailed information of the target website.
7. This concludes the demonstration of gathering information about a target website using the Website Informer online tool.
8. Close all open windows and document all the acquired information.

TASK 3 Extract a Company's Data using Web Data Extractor

Here, we will gather the target company's data using the Web Data Extractor tool.

TASK 3.1

Install Web Data Extractor

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Web Spiders\Web Data Extractor** and double-click **wde.exe**.
2. If the **User Account Control** pop-up appears, click **Yes**.

Note: If the **Open File - Security Warning** pop-up appears, click **Run**.

3. Follow the wizard steps to install Web Data Extractor and click **Finish**.

Web data extraction is the process of extracting data from web pages available on the company's website. A company's data such as contact details (email, phone, and fax), URLs, meta tags (title, description, keyword) for website promotion, directories, web research, etc. are important sources of information for an ethical hacker.

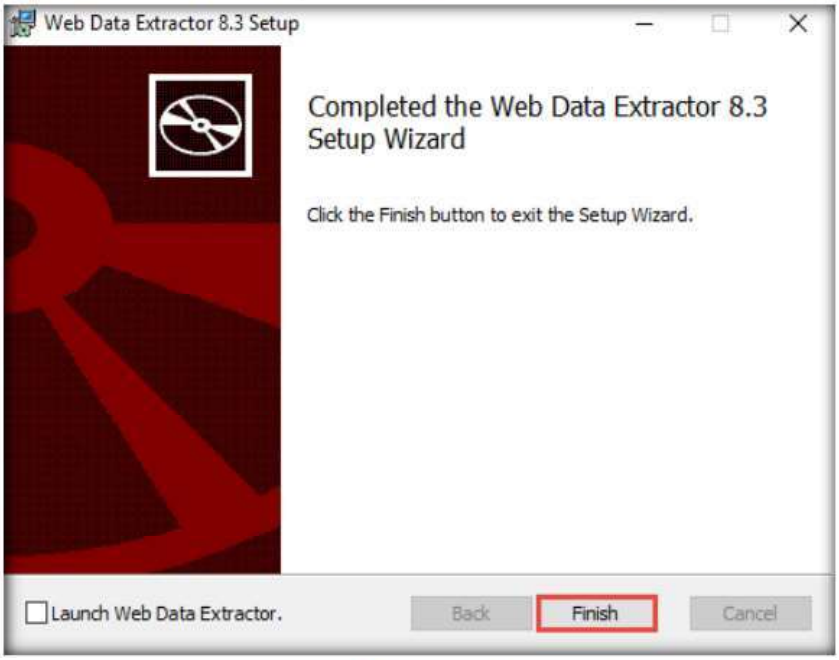

Figure 4.3.1: Web Data Extractor Setup Pop-up Wizard

Web spiders (also known as a web crawler or web robot) such as Web Data Extractor perform automated searches on the target website and extract specified information from the target website.

4. After installation, launch **Web Data Extractor** from **Desktop**.

Figure 4.3.2: Installed apps in Windows 10 - Selecting Web Data Extractor

TASK 3.2

Configure Web Data Extractor

5. The **Web Data Extractor** main window appears. Click **New** to start a new session.

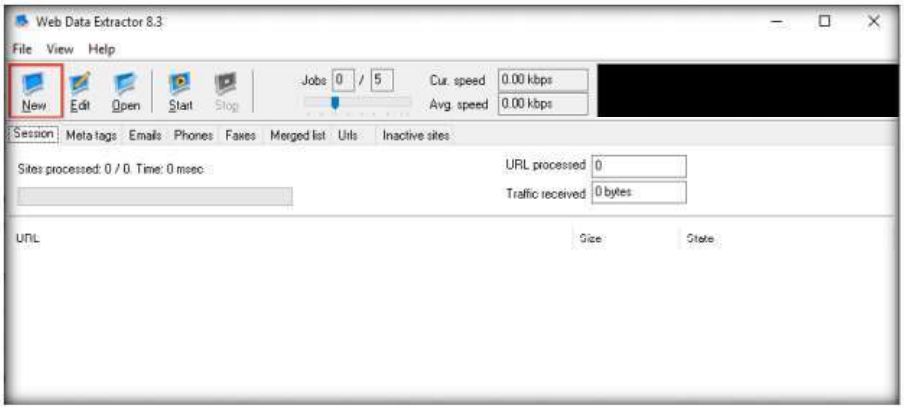

Figure 4.3.3: The Web Data Extractor main window

6. The **Session settings** window appears; type a URL (here, **http://www.certifiedhacker.com**) in the **Starting URL** field. Check all the options, as shown in the screenshot, and click **OK**.

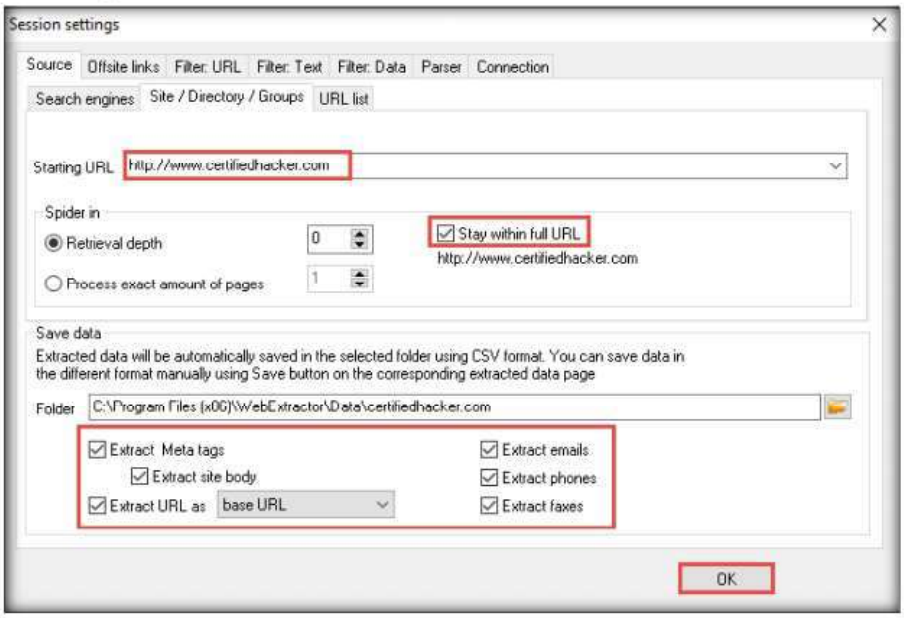

Figure 4.3.4: Web Data Extractor - Session settings window

TASK 3.3

Extract Target Website Data

7. Click **Start** to initiate the data extraction.

Figure 4.3.5: Web Data Extractor initiating the data extraction

8. Web Data Extractor will start collecting information (**Session**, **Meta tags**, **Emails**, **Phones**, **Faxes**, **Merged list**, **URLs**, and **Inactive sites**).

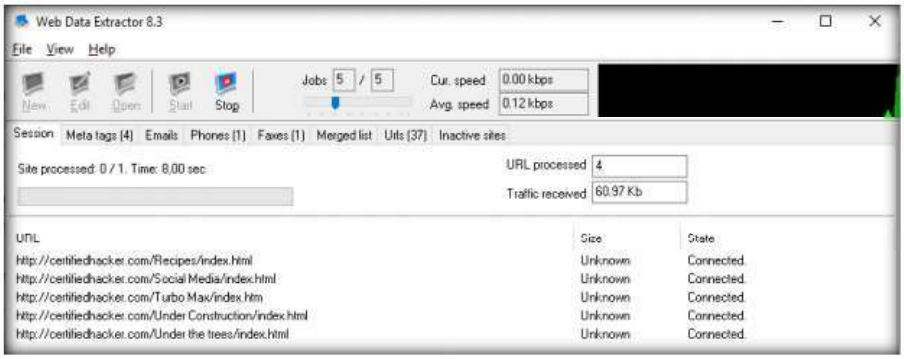

Figure 4.3.6: Web Data Extractor collecting information

9. Once the data extraction process is completed, an **Information** dialog box appears; click **OK**.

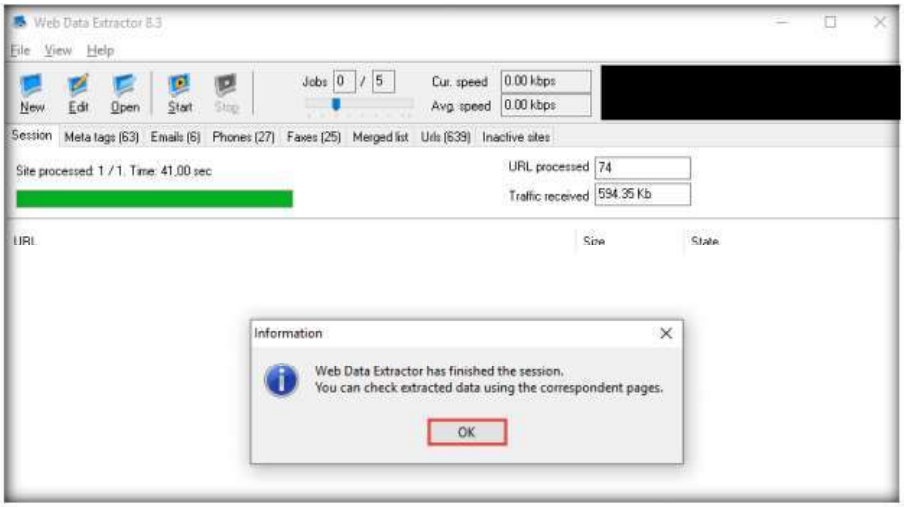

Figure 4.3.7: Web Data Extractor Data Extraction information window

10. View the extracted information by clicking the tabs.

TASK 3.4

Examine the Collected Data

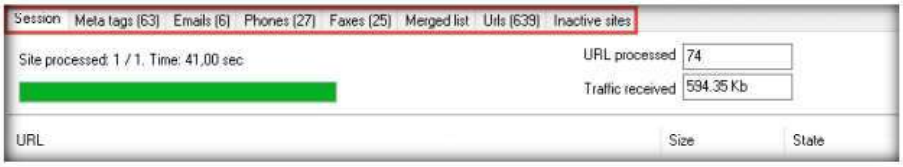

Figure 4.3.8: Web Data Extractor Data Extraction window

11. Select the **Meta tags** tab to view the URL, Title, Keywords, Description, Host, Domain, page size, etc.

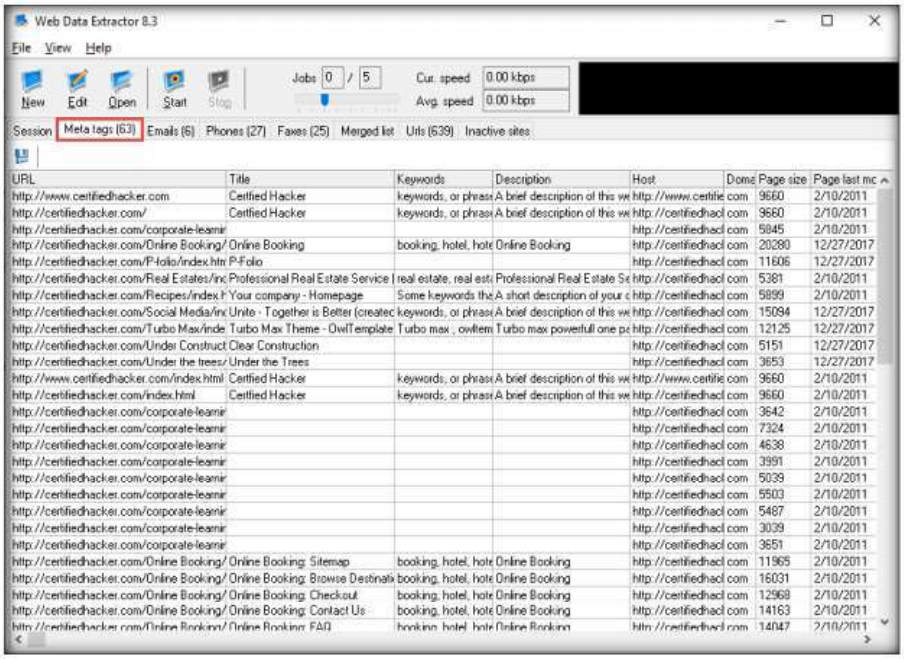

Figure 4.3.9: Web Data Extractor- Meta tags tab

12. Select the **Emails** tab to view information related to emails such as Email address, Name, URL, Title, etc.

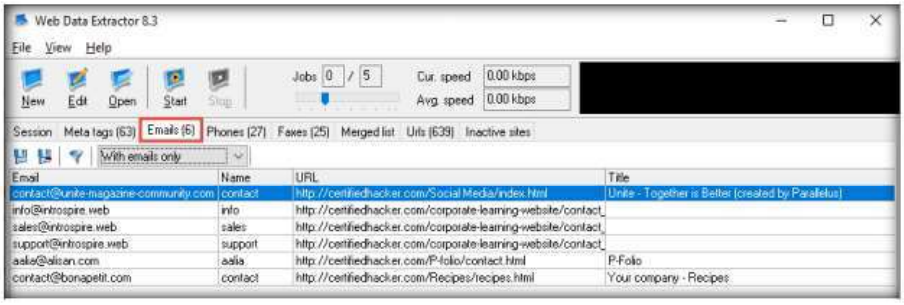

Figure 4.3.10: Web Data Extractor- Emails tab

13. Select the **Phones** tab to view the Phone, Source, Tag, URL, etc.

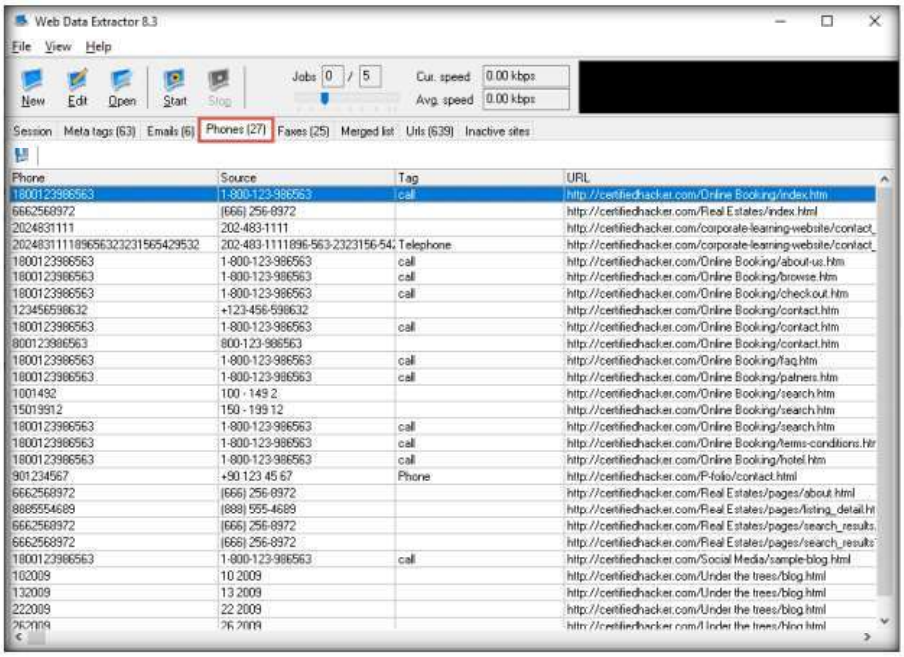

Figure 4.3.11: Web Data Extractor- Phones tab

14. Check for more information under the **Faxes**, **Merged list**, **URLs**, and **Inactive sites** tabs.

TASK 3.5

Save a Session

15. To save the session, choose **File** and click **Save session**.

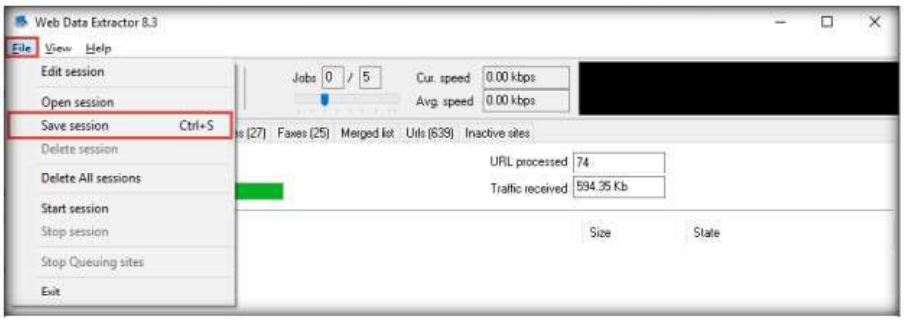

Figure 4.3.12: Web Data Extractor session saving window

16. Specify the session name (here, **certifiedhacker.com**) in the **Save session** dialog box and click **OK**.

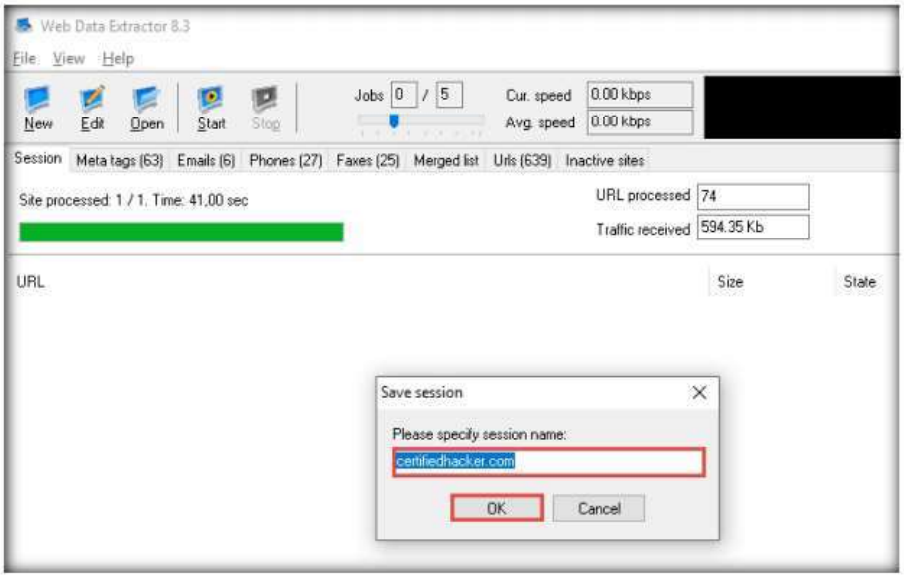

Figure 4.3.13: Web Data Extractor specifying the session name

17. Click the **Meta tags** tab, and then click the **floppy** icon.

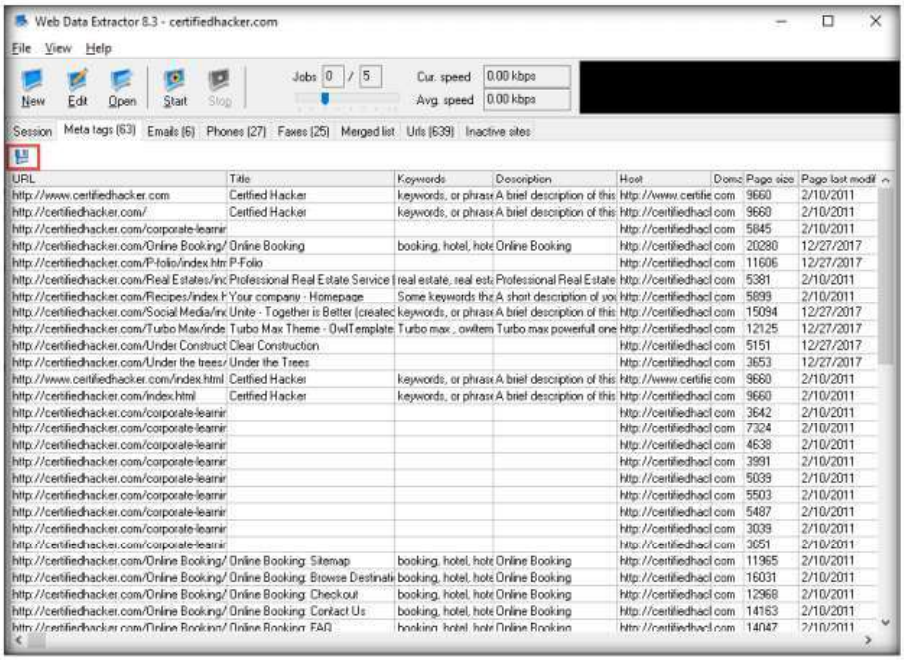

Figure 4.3.14: Web Data Extractor - Meta tags tab

18. An **Information** pop-up may appear with the message **You cannot save more than 10 records in Demo Version**; click **OK**.

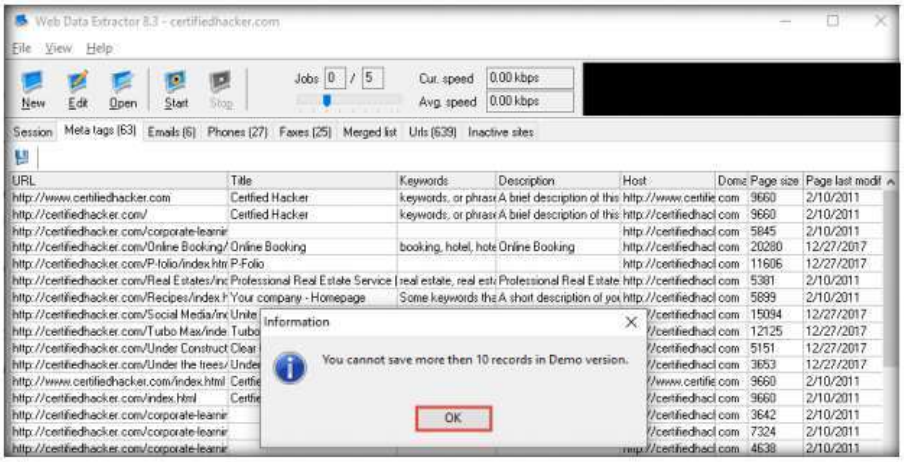

Figure 4.3.15: Web Data Extractor saving information window

19. The **Save Meta tags** window appears. In the **File name** field, click on the **folder icon**, select the location where you want to save the file, choose **File format**, and click **Save**.

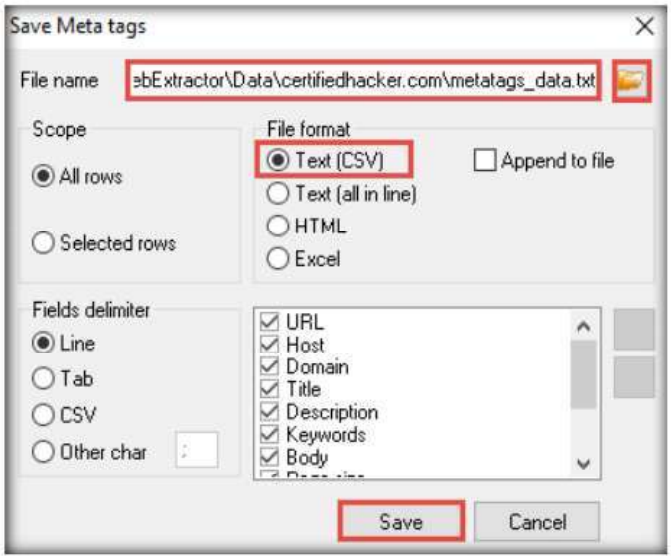

Figure 4.3.16: Web Data Extractor saving window

You can also use other web spiders such as **ParseHub** (https://www.parsehub.com), **SpiderFoot** (https://www.spiderfoot.net), etc. to extract the target organization's data.

20. By default, the session will be saved at **C:\Program Files (x86)\WebExtractor\Data\certifiedhacker.com**. You can choose your desired location to save the file.
21. This concludes the demonstration of extracting a company's data using the Web Data Extractor tool.
22. Close all open windows and document all the acquired information.

TASK 4

Mirror a Target Website using HTTrack Web Site Copier

Here, we will use the HTTrack Web Site Copier tool to mirror the entire website of the target organization, store it in the local system drive, and browse the local website to identify possible exploits and vulnerabilities.

TASK 4.1

Install HTTrack Web Site Copier

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Website Mirroring Tools\HTTrack Web Site Copier** and double-click **httrack-3.49.2.exe**.
2. If the **User Account Control** pop-up appears, click **Yes**.

Note: If the **Open File - Security Warning** pop-up appears, click **Run**.

3. Follow the wizard steps to install **HTTrack Web Site Copier**.
4. In the last step of the installation wizard, uncheck the **View history.txt file** option and click **Finish**.

Website mirroring is the process of creating a replica or clone of the original website; this mirroring of the website helps you to footprint the web site thoroughly on your local system, and allows you to download a website to a local directory, analyze all directories, HTML, images, flash, videos, and other files from the server on your computer.

Figure 4.4.1: HTTrack Website Copier Setup Pop-up Wizard

TASK 4.2

Mirror the Target Website

5. The **WinHTTrack Website Copier** window appears. Click **OK** in the pop-up window, and then click **Next >** to create a **New Project**.

Note: If the application does not launch, you can launch it manually from the **Apps** screen.

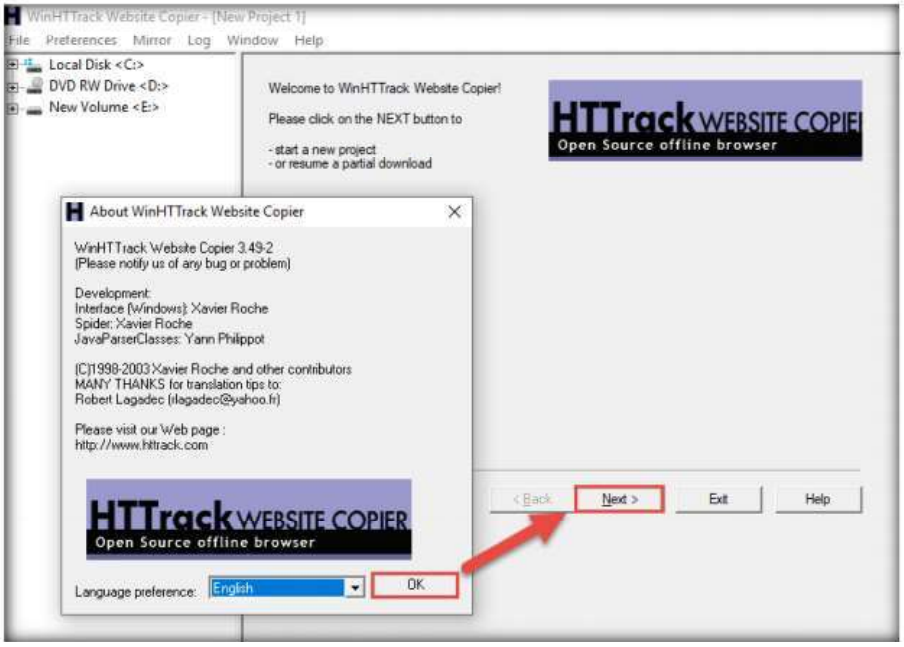

Figure 4.4.2: HTTrack Website Copier main window

You can duplicate websites by using website mirroring tools such as HTTrack Web Site Copier. HTTrack is an offline browser utility that downloads a website from the Internet to a local directory, builds all directories recursively, and transfers HTML, images, and other files from the webserver to another computer.

6. Enter the name of the project (here, **Test Project**) in the **New project name:** field. Select the **Base path:** to store the copied files; click **Next >**.

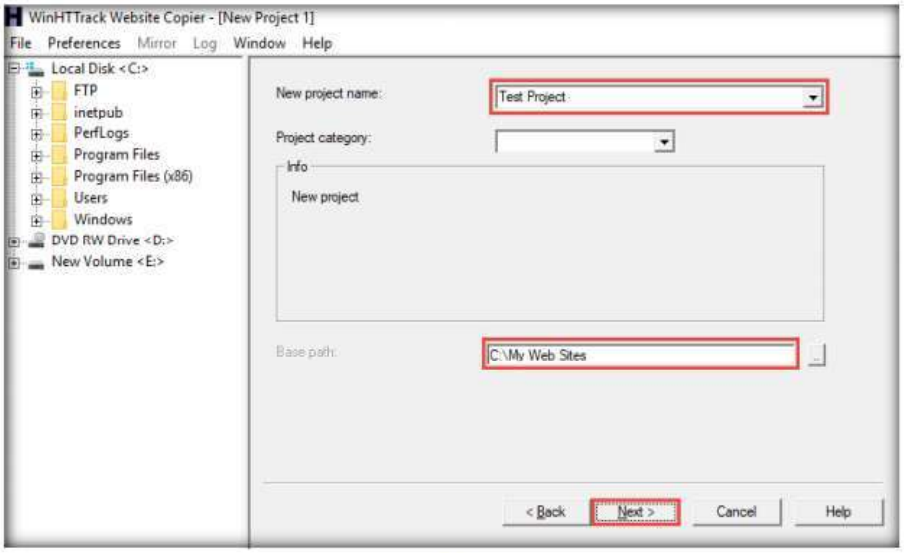

Figure 4.4.3: HTTrack Website Copier selecting a New Project

7. Enter a target URL (here, **www.certifiedhacker.com**) in the **Web Addresses: (URL)** field and click **Set options...**

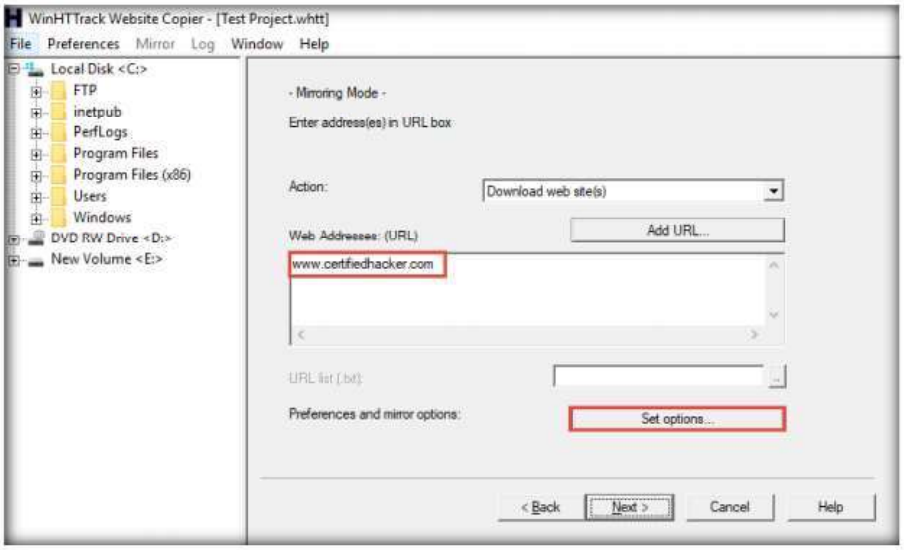

Figure 4.4.4: Setting options in HTTrack Website Copier

8. **WinHTTrack** window appears, click the **Scan Rules** tab and select the checkboxes for the file types as shown in the following screenshot; click **OK**.

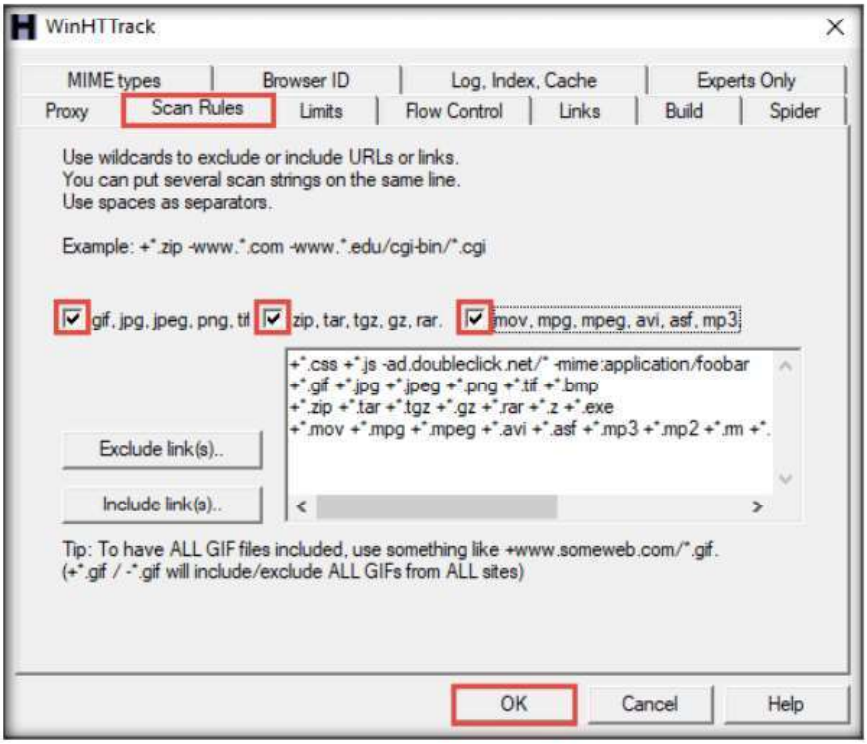

Figure 4.4.5: Scan Rules tab in HTTrack Website Copier

9. Click the **Next >** button.

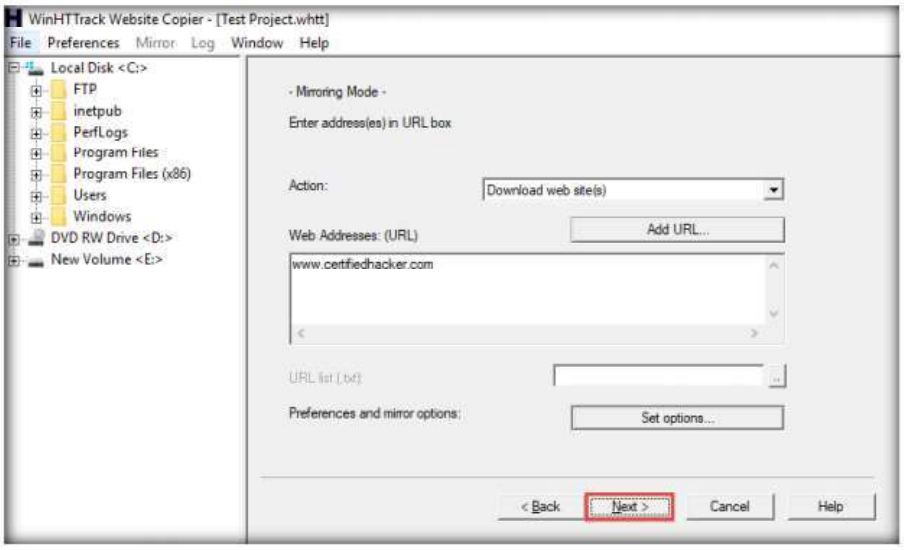

Figure 4.4.6: HTTrack Website Copier Select a project window

10. By default, the radio button will be selected for **Please adjust connection parameters if necessary, then press FINISH to launch the mirroring operation**. Check **Disconnect when finished** and click **Finish** to start mirroring the website.

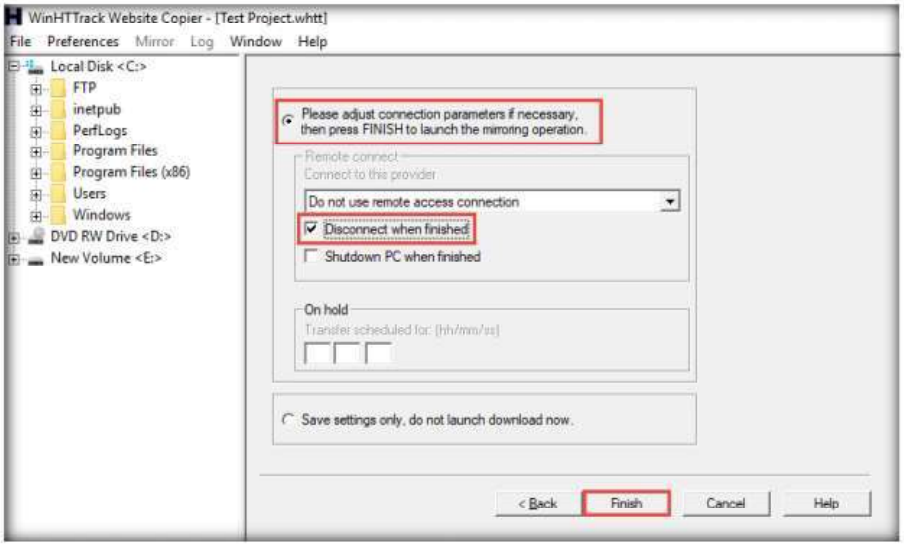

Figure 4.4.7: HTTrack Website Copier launching mirroring operation

11. Site mirroring progress will be displayed, as shown in the screenshot.

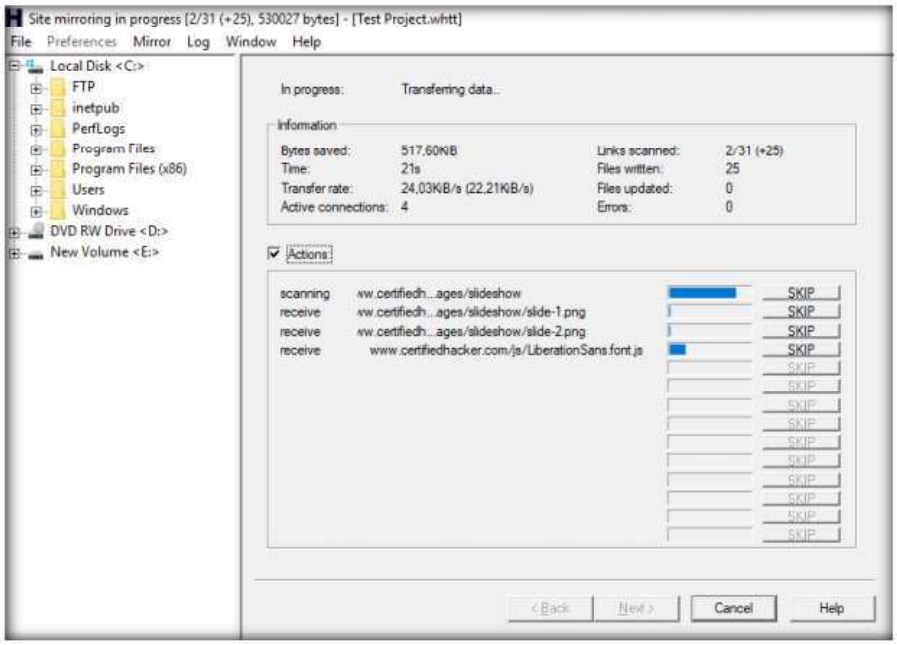

Figure 4.4.8: HTTrack Website Copier displaying site mirroring progress

12. Once the site mirroring is completed, WinHTTrack displays the message **Mirroring operation complete**; click on **Browse Mirrored Website**.

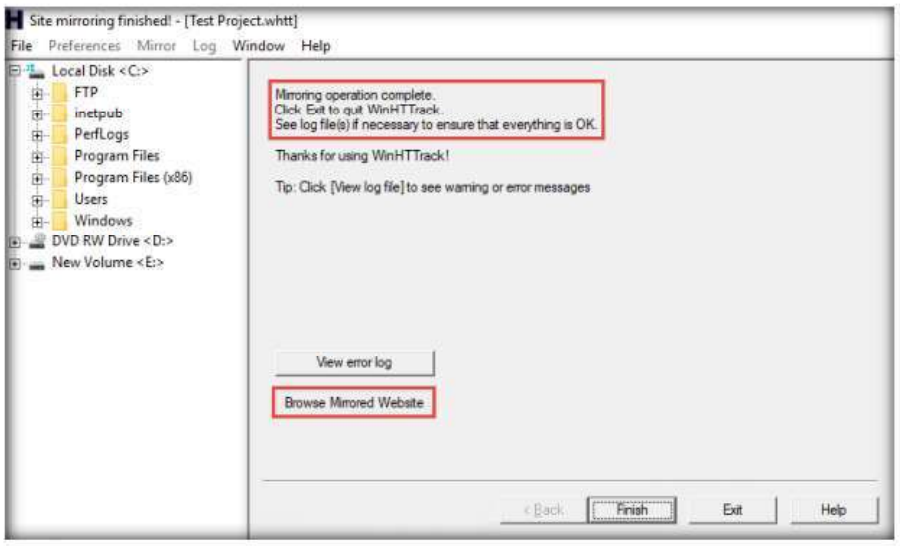

Figure 4.4.9: HTTrack Website Copier displaying site mirroring is complete

TASK 4.3

Browse the Mirrored Website

13. If the **How do you want to open this file?** pop up appears, select any web browser (here, **Mozilla Firefox**) and click **OK**.

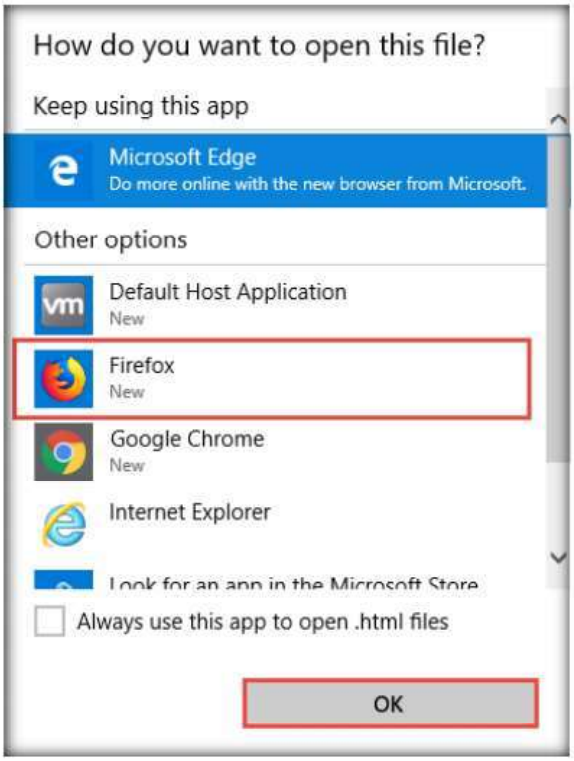

Figure 4.4.10: Selecting Mozilla Firefox

14. The mirrored website for **www.certifiedhacker.com** launches. The URL displayed in the address bar indicates that the website's image is stored on the local machine.

Figure 4.4.11: HTTrack Website Copier Mirrored Website Image

15. Analyze all directories, HTML, images, flash, videos, and other files available on the mirrored target website. You can also check for possible exploits and vulnerabilities. The site will work like a live hosted website.

Note: If the webpage does not open, navigate to the directory where you mirrored the website and open **index.html** with any browser.

16. Once done with your analysis, close the **Firefox** window and click **Finish** on the **WinHTTrack** window to complete the process

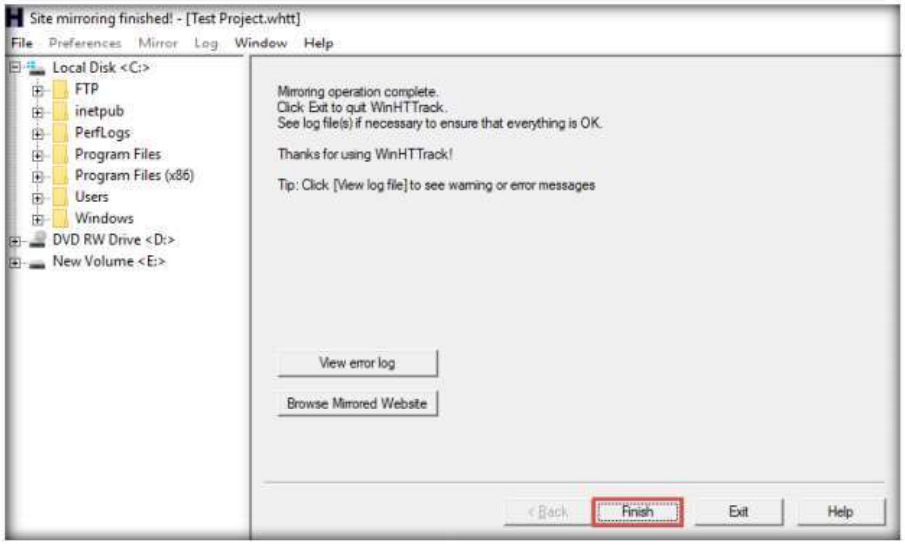

Figure 4.4.12: HTTrack Website Copier displaying site mirroring is complete

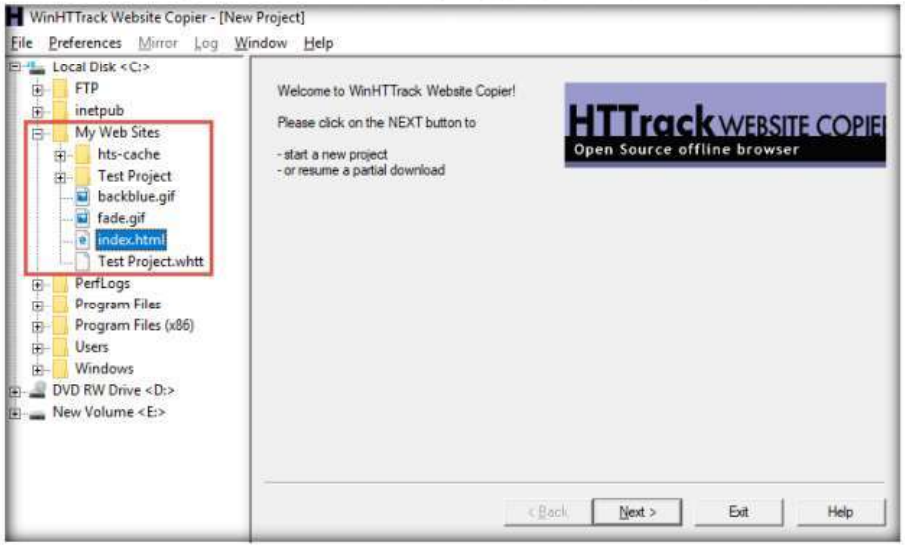

Figure 4.4.13: HTTrack Website Copier displaying mirrored website location

You can also use other mirroring tools such as **NCollector Studio** (http://www.calluna-software.com), **Cyotek WebCopy** (https://www.cyotek.com), etc. to mirror a target website.

17. Some websites are very large, and it might take a long time to mirror the complete site.

18. This concludes the demonstration of mirroring a target website using HTTrack Web Site Copier.
19. Close all open windows and document all the acquired information.
20. Turn off the **Windows 10** virtual machine.

TASK 5 Gather a Wordlist from the Target Website using CeWL

The words available on the target website may reveal critical information that can assist in performing further exploitation. CeWL is a ruby app that is used to spider a given target URL to a specified depth, optionally following external links, and returns a list of unique words that can be used for cracking passwords.

1. Turn on **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

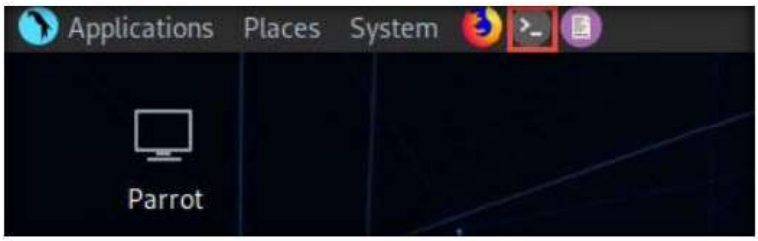

Figure 4.5.1: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

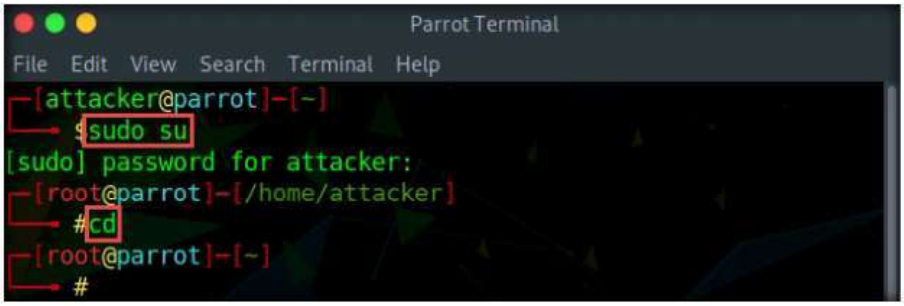

Figure 4.5.2: Running the programs as a root user

7. In the **Parrot Terminal** window, type **cewl -d 2 -m 5 www.certifiedhacker.com** and press **Enter**.

Note: **-d** represents the depth to spider the website (here, **2**) and **-m** represents minimum word length (here, **5**).

Figure 4.5.3: Gathering wordlist

8. A unique wordlist from the target website is gathered, as shown in the screenshot.

Note: The minimum word length is 5, and the depth to spider the target website is 2.

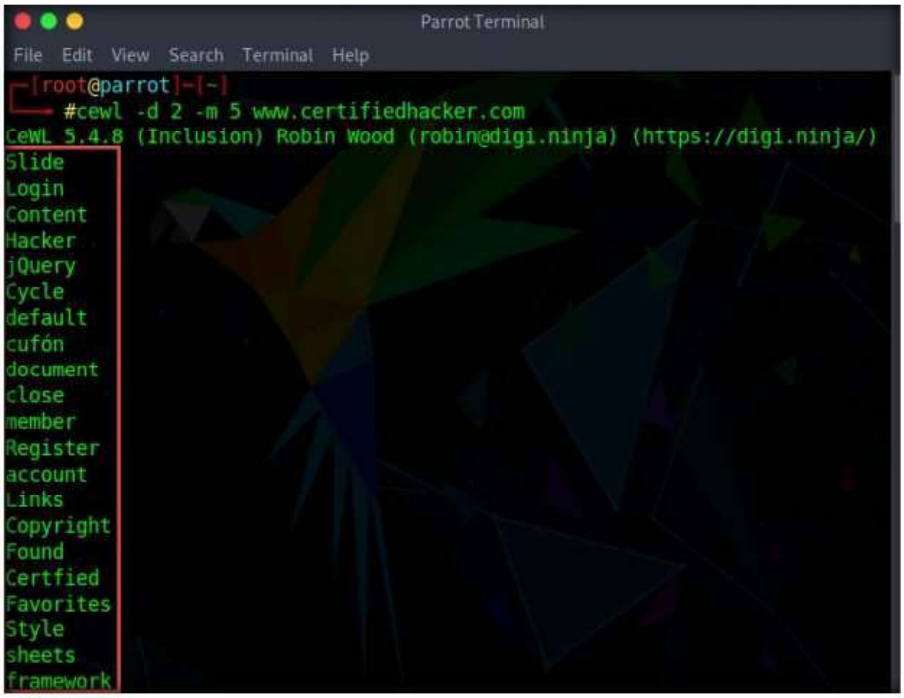

Figure 4.5.4: Wordlist gathered from the target website

9. Alternatively, this unique wordlist can be written directly to a text file by typing **cewl -w wordlist.txt -d 2 -m 5 www.certifiedhacker.com**.

Note: **-w** - Write the output to the file (here, **wordlist.txt**)

Figure 4.5.5: Wordlist written to wordlist.txt file

10. By default, the wordlist file gets saved in the **root** directory. Type **pluma wordlist.txt** and press **Enter** to view the extracted wordlist.

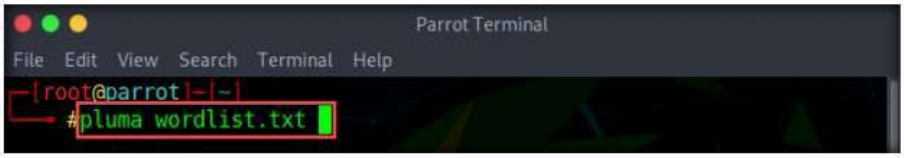

Figure 4.5.6: Open wordlist.txt file

11. The file containing a unique wordlist extracted from the target website opens, as shown in the screenshot.

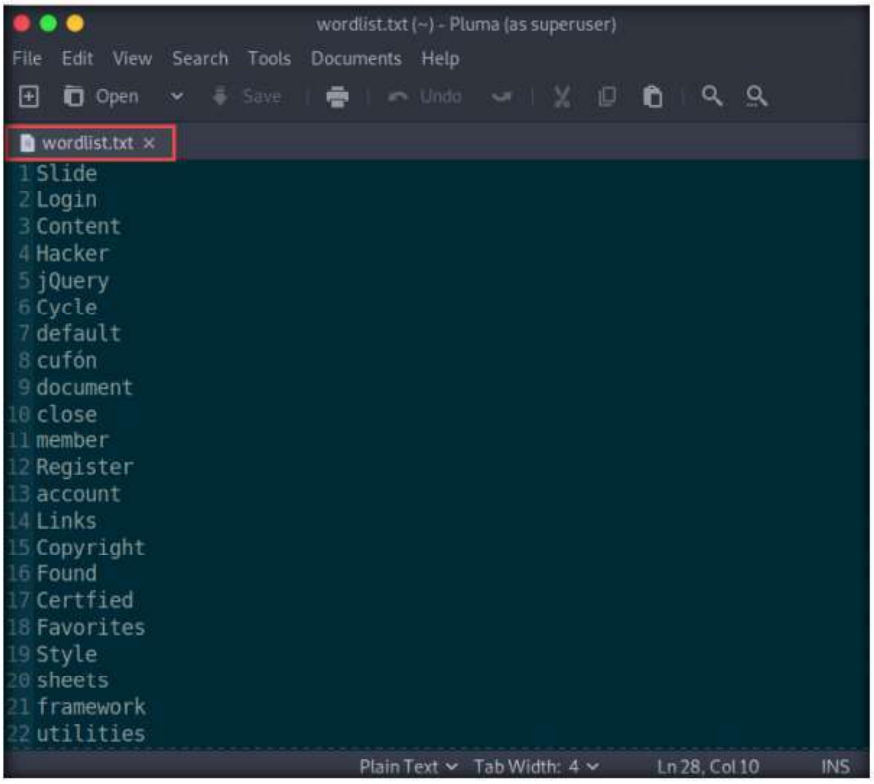

Figure 4.5.7: wordlist.txt file

12. This wordlist can be used further to perform brute-force attacks against the previously obtained emails of the target organization's employees.
13. This concludes the demonstration of gathering wordlist from the target website using CeWL.
14. Close all open windows and document all the acquired information.
15. Turn off the **Parrot Security** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

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

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

Lab 5

Perform Email Footprinting

Email footprinting or tracing emails involves analyzing the email header to discover details about the sender.

Lab Scenario

ICON KEY

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

As a professional ethical hacker, you need to be able to track emails of individuals (employees) from a target organization for gathering critical information that can help in building an effective hacking strategy. Email tracking allows you to collect information such as IP addresses, mail servers, OS details, geolocation, information about service providers involved in sending the mail etc. By using this information, you can perform social engineering and other advanced attacks.

Lab Objectives

- Gather information about a target by tracing emails using eMailTrackerPro

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

To carry out this lab, you need:

- Windows 10 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- eMailTrackerPro located at **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Email Tracking Tools\eMailTrackerPro**
- You can also download the latest version of eMailTrackerPro from its official website. If you decide to download the latest version, the screenshots shown in the lab might differ.

Lab Duration

Time: 10 Minutes

Overview of Email Footprinting

E-mail footprinting, or tracking, is a method to monitor or spy on email delivered to the intended recipient. This kind of tracking is possible through digitally time-stamped records that reveal the time and date when the target receives and opens a specific email.

Email footprinting reveals information such as:

- Recipient's system IP address
- The GPS coordinates and map location of the recipient
- When an email message was received and read
- Type of server used by the recipient
- Operating system and browser information
- If a destructive email was sent
- The time spent reading the email
- Whether or not the recipient visited any links sent in the email
- PDFs and other types of attachments
- If messages were set to expire after a specified time

Lab Tasks

TASK 1 — Gather Information about a Target by Tracing Emails using eMailTrackerPro

Here, we will gather information by analyzing the email header using eMailTrackerPro.

1. Turn on the **Windows 10** virtual machine.
2. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.

TASK 1.1

Install eMailTrackerPro

3. Open **File Explorer** and navigate to **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Email Tracking Tools\eMailTrackerPro** and double-click **emt.exe**.
4. If the **User Account Control** pop-up appears, click **Yes**.
5. The **eMailTrackerPro Setup** window appears. Follow the wizard steps (by selecting default options) to install eMailTrackerPro.

The email header is a crucial part of any email and it is considered a great source of information for any ethical hacker launching attacks against a target. An email header contains the details of the sender, routing information, addressing scheme, date, subject, recipient, etc. Additionally, the email header helps ethical hackers to trace the routing path taken by an email before delivering it to the recipient.

6. After the installation is complete, in the **Completing the eMailTrackerPro Setup Wizard**, uncheck the **Show Readme** check-box and click the **Finish** button to launch the eMailTrackerPro.

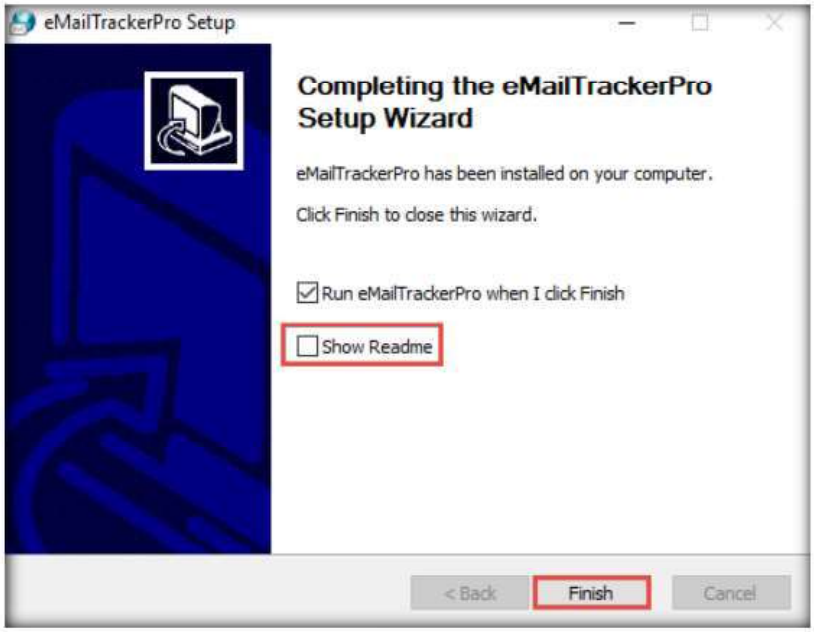

Figure 5.1.1: eMailTrackerPro installation Complete

7. The main window of **eMailTrackerPro** appears along with the **Edition Selection** pop-up; click **OK**.

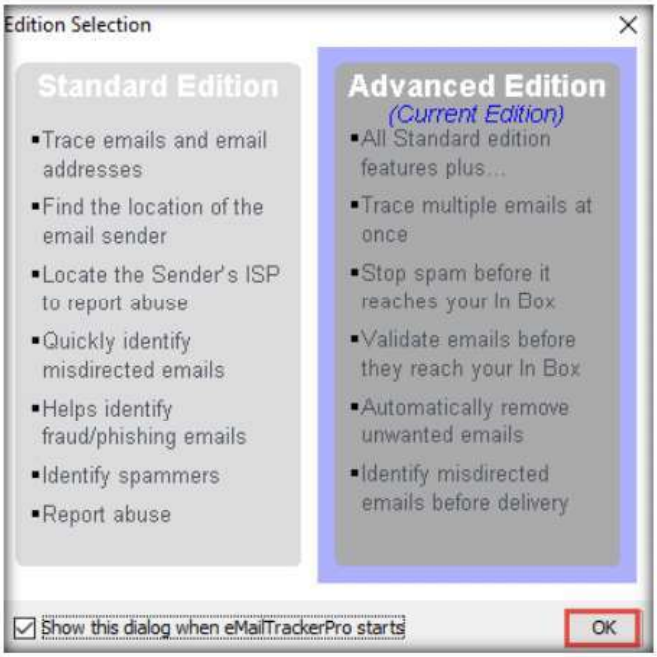

Figure 5.1.2: eMailTrackerPro - Edition Selection pop-up window

8. The **eMailTrackerPro** main window appears, as shown in the screenshot.

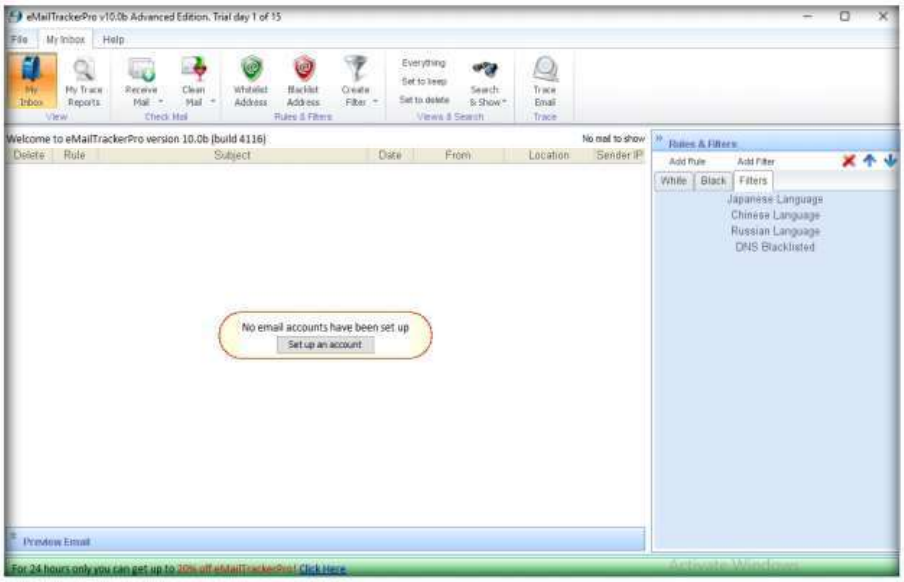

Figure 5.1.3: eMailTrackerPro main window

TASK 1.2

Trace Email Header

9. To trace email headers, click the **My Trace Reports** icon from the **View** section. (here, you will see the output report of the traced email header)
10. Click the **Trace Headers** icon from the **New Email Trace** section to start the trace.

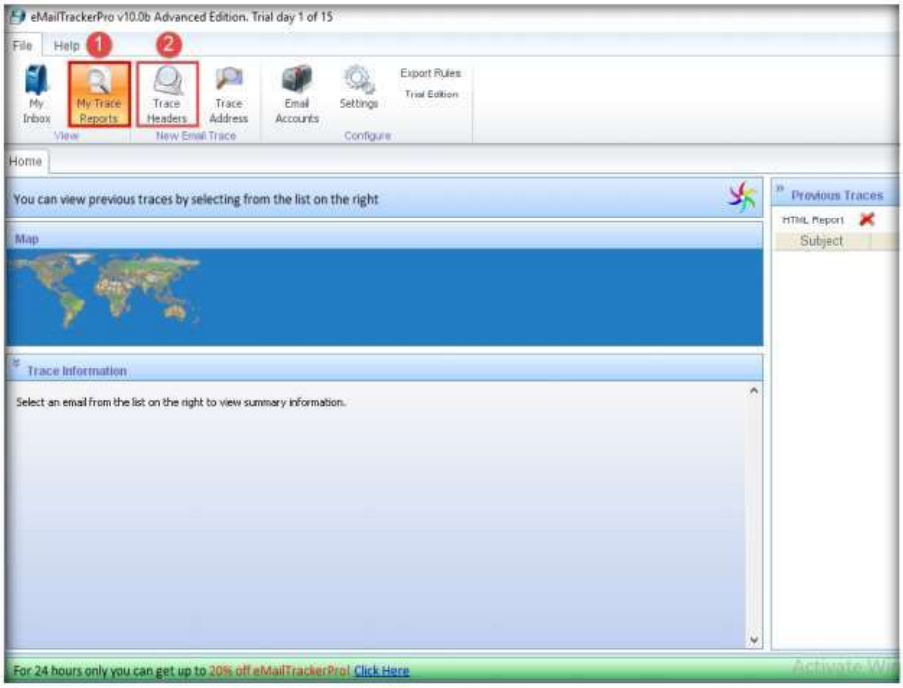

Figure 5.1.4: The eMailTrackerPro main window

11. A pop-up window will appear; select **Trace an email I have received**. Copy the email header from the suspicious email you wish to trace and paste it in the **Email headers:** field under **Enter Details** section.

Figure 5.1.5: The eMailTrackerPro entering details window

12. For finding email headers, open any web browser and log in to any email account of your choice; from the email inbox, open the message you would like to view headers for.

Note: In **Gmail**, find the email header by following the steps:

- Open an email; click the dots (**More**) icon arrow next to the **Reply** icon at the top-right corner of the message pane.
- Select **Show original** from the list.
- The **Original Message** window appears in a new browser tab with all the details about the email, including the email header.

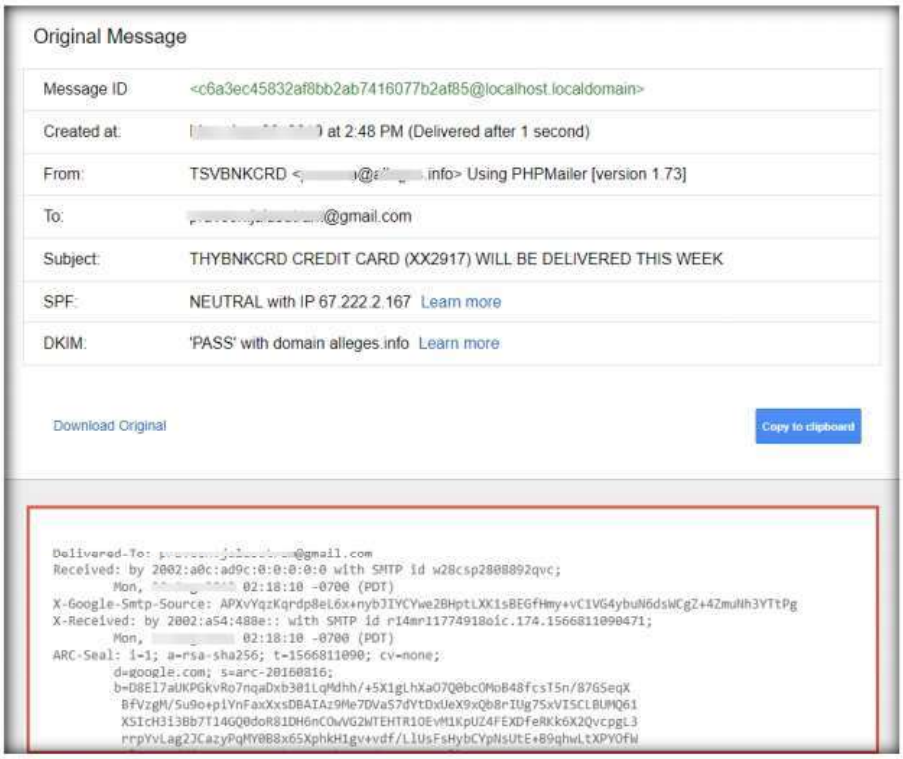

Figure 5.1.6: Sample Email Header in Gmail

Note: In **Outlook**, find the email header by following the steps:

- Double-click the email to open it in a new window
- Click the **...** (**More actions**) icon present at the right of the message-pane to open message options
- From the options, click **View message details**
- The **message details** window appears with all the details about the email, including the email header

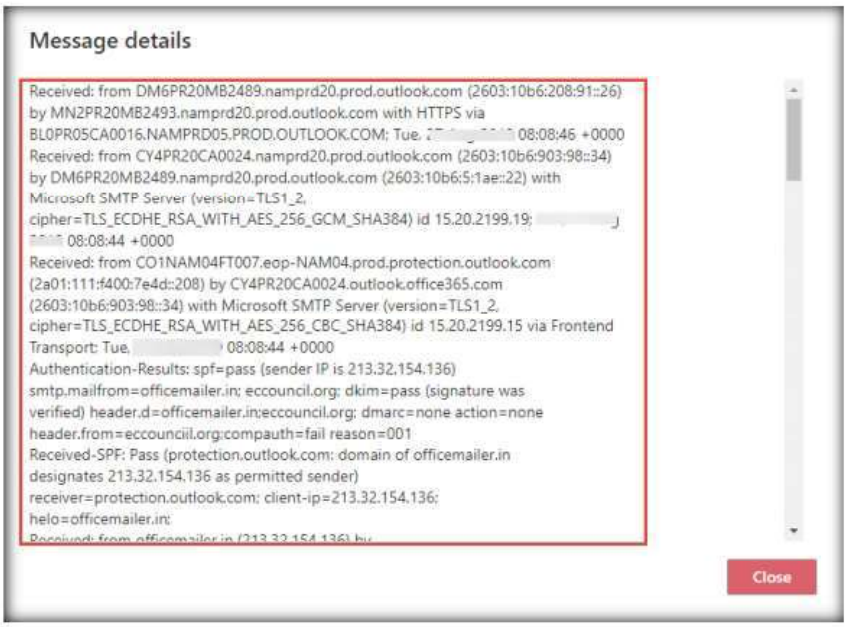

Figure 5.1.7: Sample Email Header in Outlook

13. Copy the entire email header text and paste it into the **Email headers:** field of eMailTrackerPro, and click **Trace**.

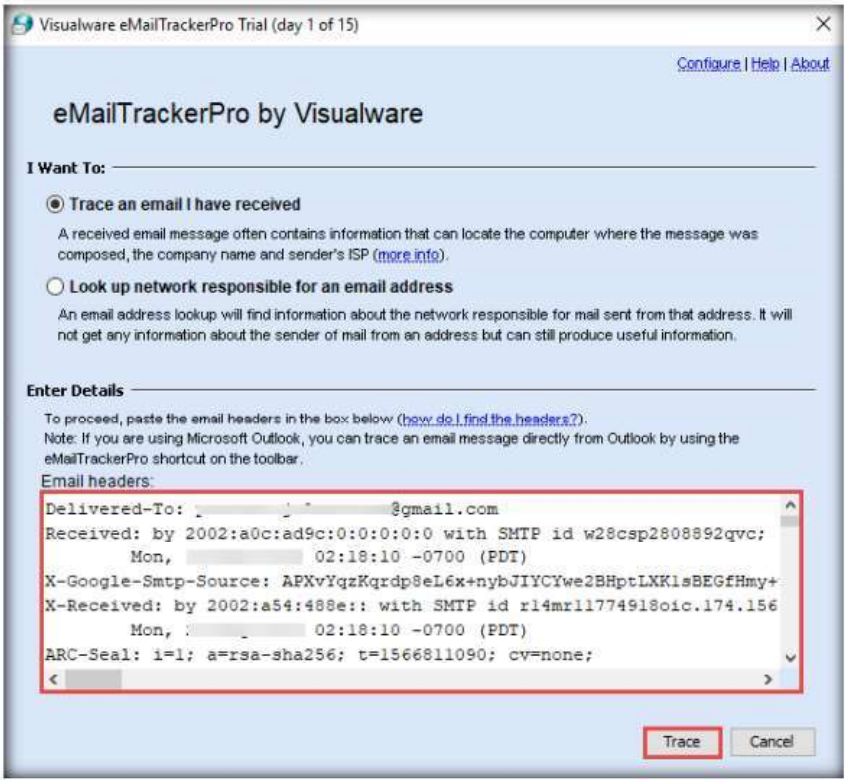

Figure 5.1.8: Email headers and Tracing emails

14. The **My Trace Reports** window opens.

15. The email location will be traced in a **Map** (world map GUI). You can also view the summary by selecting **Email Summary** on the right-hand side of the window. The **Table** section right below the Map shows the entire hop in the route, with the **IP** and suspected locations for each hop.

Note: The location and IP addresses may vary according to your email header.

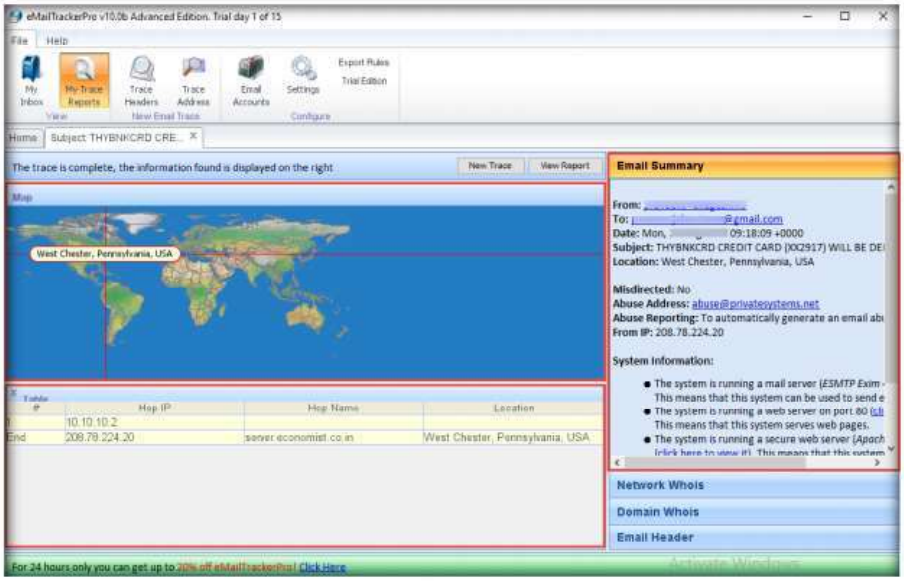

Figure 5.1.9: eMailTrackerPro – Email Trace Report

TASK 1.3

Examine the Report

16. To examine the report, click the **View Report** button above **Map** to view the complete trace report.

Figure 5.1.10: The eMailTrackerPro – My Trace Reports tab

17. The complete report appears in the default browser.

Note: If a pop-up window appears asking for a browser to be selected, select **Firefox** and click **OK**.

18. Expand each section to view detailed information.

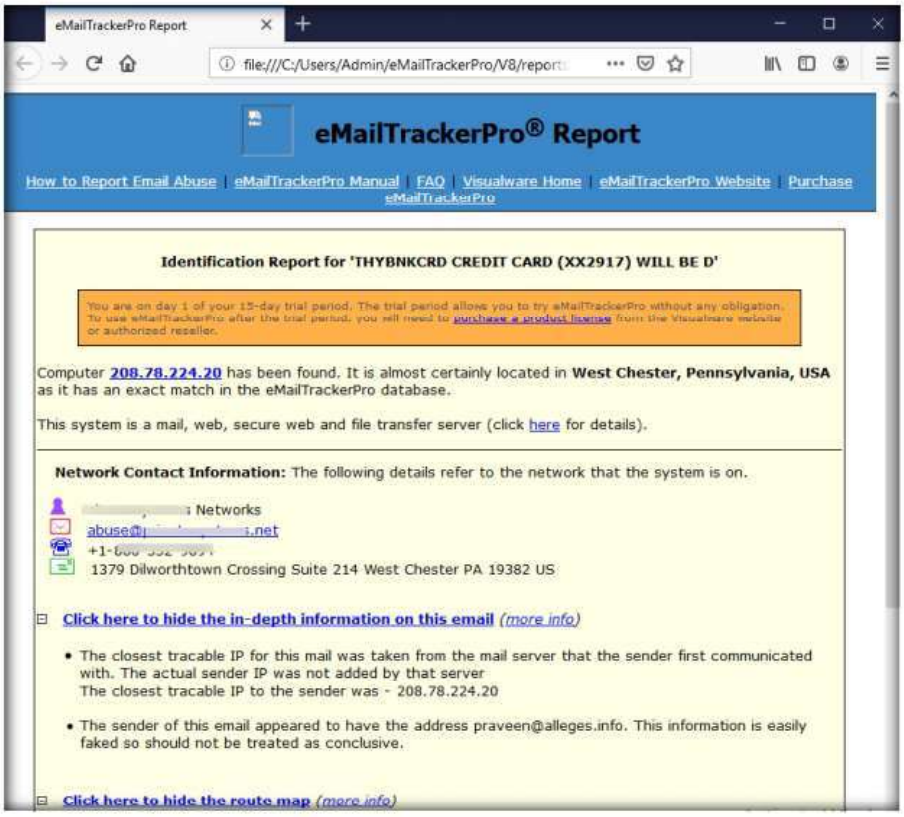

Figure 5.1.11: eMailTrackerPro – detailed information Report

You can also use email tracking tools such as **Infoga** (https://github.com), **Mailtrack** (https://mailtrack.io), etc. to track an email and extract target information such as sender identity, mail server, sender's IP address, location, etc.

19. This concludes the demonstration of gathering information through analysis of the email header using eMailTrackerPro.
20. Close all open windows and document all the acquired information.
21. Turn off the **Windows 10** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

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

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

Lab 6

Perform Whois Footprinting

Whois lookup reveals available information on a hostname, IP address, or domain

ICON KEY

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

Lab Scenario

During the footprinting process, gathering information on the target IP address and domain obtained during previous information gathering steps is important. As a professional ethical hacker or penetration tester, you should be able to perform Whois footprinting on the target; this method provides target domain information such as the owner, its registrar, registration details, name server, contact information, etc. Using this information, you can create a map of the organization's network, perform social engineering attacks, and obtain internal details of the network.

Lab Objectives

- Perform Whois lookup using DomainTools

Lab Environment

To carry out this lab, you need:

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

- Windows 10 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 5 Minutes

Overview of Whois Footprinting

This lab focuses on how to perform a Whois lookup and analyze the results. Whois is a query and response protocol used for querying databases that store the registered users or assignees of an Internet resource such as a domain name, an IP address block, or an autonomous system. This protocol listens to requests on port 43 (TCP). Regional Internet Registries (RIRs) maintain Whois databases, and contains the personal information of domain owners. For each resource, the Whois database

provides text records with information about the resource itself and relevant information of assignees, registrants, and administrative information (creation and expiration dates).

Lab Tasks

TASK 1 Perform Whois Lookup using DomainTools

Here, we will gather target information by performing Whois lookup using DomainTools.

1. Turn on the **Windows 10** virtual machine.
2. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.
3. Open any web browser (here, **Mozilla Firefox**) and navigate to **http://whois.domaintools.com**. In the **Enter a domain or IP address...** search bar, type **www.certifiedhacker.com** and click **Search**.

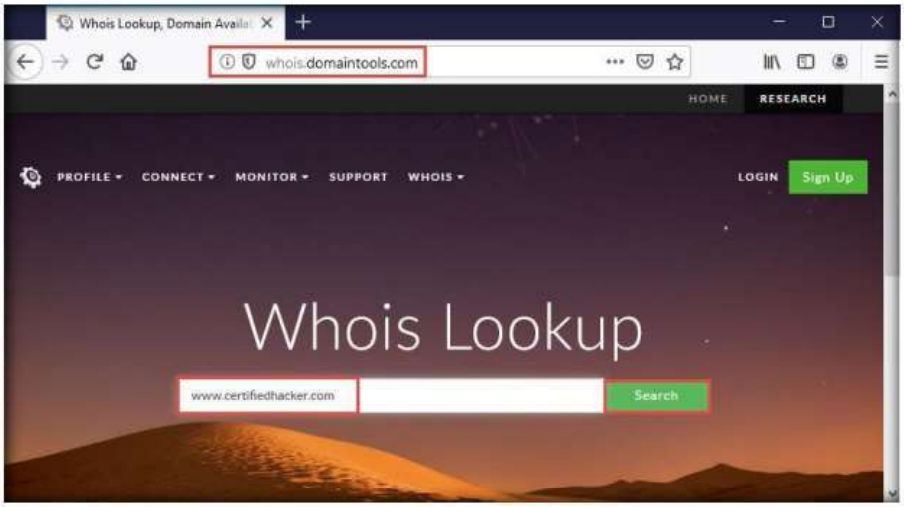

Figure 6.1.1: Whois Domain website

4. This search result reveals the details associated with the URL entered, **www.certifiedhacker.com**, which includes organizational details such as registration details, name servers, IP address, location, etc., as shown in the screenshots.

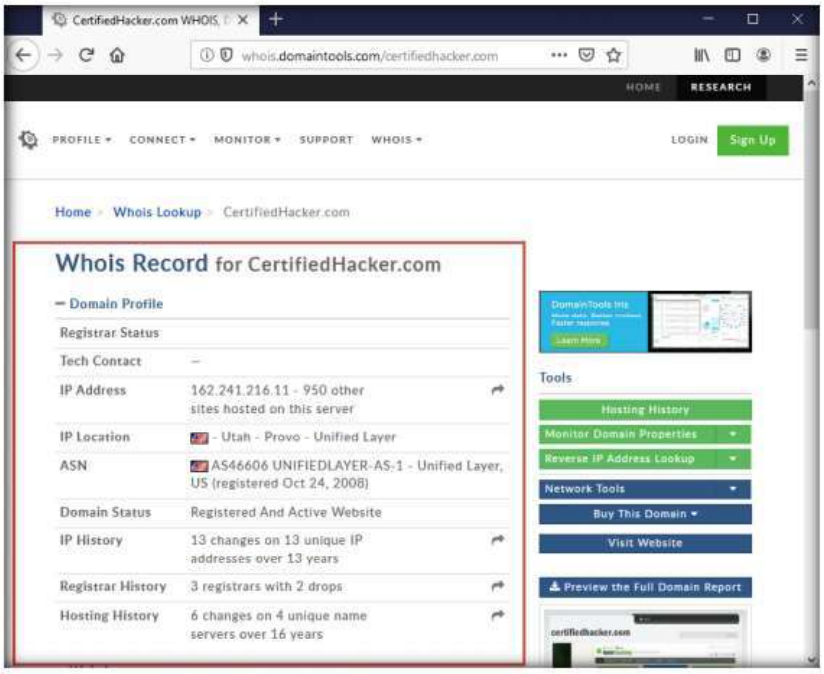

Figure 6.1.2: whois.domaintools.com search results

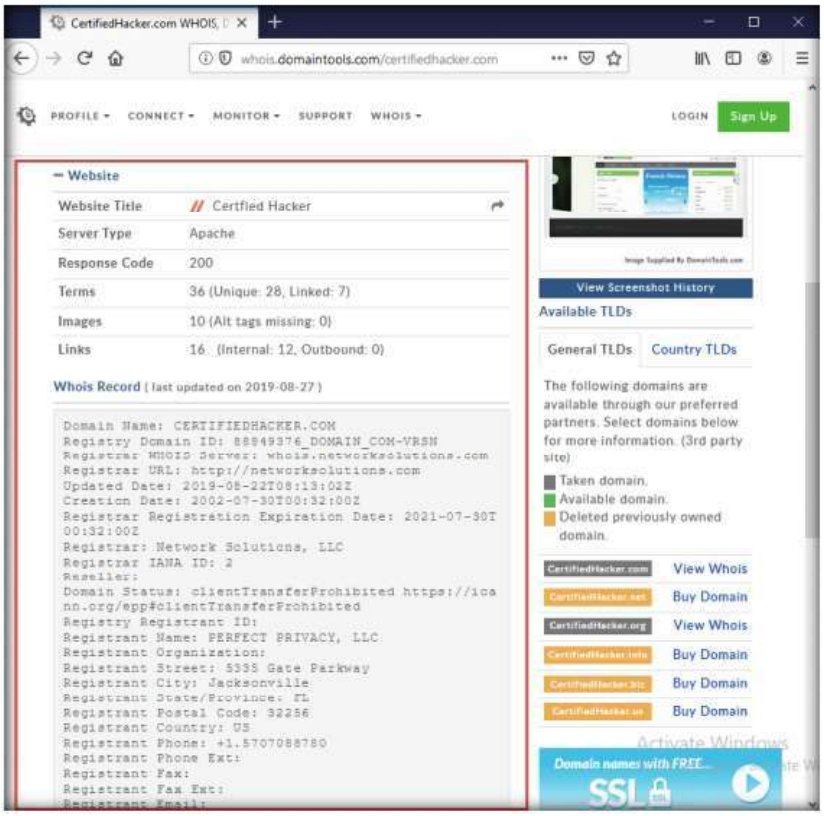

Figure 6.1.3: whois.domaintools.com search results

You can also use other Whois lookup tools such as **SmartWhois** (https://www.tamos.com), **Batch IP Converter** (http://www.sabsoft.com), etc. to extract additional target Whois information.

5. This concludes the demonstration of gathering information about a target organization by performing the Whois lookup using DomainTools.
6. Close all open windows and document all the acquired information.
7. Turn off the **Windows 10** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

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

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