Footprinting and Reconnaissance

Module 02

Footprinting a Target Network

Footprinting refers to collecting as much information as possible regarding a target network from publicly accessible sources.

ICON KEY

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

Lab Scenario

Reconnaissance refers to collecting information about a target. It has its roots in military operations where it refers to the missions to collect information about an enemy. Information gathering is the first step in any attack on information systems. It helps attackers to narrow down the scope of their efforts and helps them select the weapons of attack. Attackers use information about the target to create a blueprint or footprint of the organization, which helps them in selecting the most effective strategy to compromise system and network security.

Similarly, the security assessment of a system or network starts with the reconnaissance and footprinting of the target. Ethical hackers and penetration (pen) testers must collect enough information about the target of the evaluation before starting the assessments. The ethical hackers and pen testers should simulate all the steps that an attacker usually follows in order to obtain a fair idea of the security posture of the target organization.

In this scenario, you work as an ethical hacker with a large organization. Your organization is alarmed at the news stories about new attack vectors plaguing large organizations around the world. Your organization was also a target of a major security breach in the past where the personal data of several of its customers were exposed on social networking sites.

You have been asked by top management to perform a proactive security assessment of the company. Before you can start any assessment, you should discuss with the management and define the scope of this assessment. Scope of the assessment identifies the systems, network, policies and procedures, human resources, and any other component of the system that requires security assessment. You should also agree with management on rules of engagement (RoE— the do's and don'ts for assessment. Once you have the necessary approvals to perform ethical hacking for your organization, you should start gathering information about the target organization from public sources. The labs in this module will give you real-time experience in collecting information from various open sources.

Lab Objectives

The objective of the lab is to extract information about the target organization that includes, but is not limited to:

- Internet Protocol (IP) address and IP range associated with the target
- Purpose of organization and why it exists
- Size of the organization

- Class of its IP block
- People and contacts at the target
- Types of operating systems (OS) and network topology in use
- Type of firewall implemented, either hardware or software or combination
- Type of remote access used, either SSH or VPN

Lab Environment

This lab requires:

- Web browsers with Internet connection
- Administrator privileges to run the tools
- The labs in this module will work in the CEH lab environment containing Windows Server 2012, Windows 8.1, Windows Server 2008, Kali Linux and Windows 7 machines.

Lab Duration

Time: 115 Minutes

Overview of Footprinting

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 02 Footprinting and Reconnaissance

Footprinting, the first step in ethical hacking, refers to the process of collecting information about a target network and its environment. Using footprinting, you can find various ways to intrude into the target organization's network.

Once you begin the footprinting process in a methodological manner, you will obtain the blueprint of the security profile of the target organization. The term blueprint refers to the unique system profile of the target organization as the result of footprinting.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to collect information about the target. Recommended labs that will assist you in learning various footprinting techniques include:

- Open Source Information Gathering Using **Windows Command Line Utilities**
- Gathering Personal Information Using Online **People Search Services**
- Collecting Information About a Target Website Using **Firebug**
- Extracting a Company's Data Using **Web Data Extractor**
- Mirroring Website Using **HTTrack Web Site Copier**
- Collecting Information About a Target by **Tracing Emails**

- Gathering IP and Domain Name Information Using **Whois Lookup**
- Advanced Network Route Tracing Using **Path Analyzer Pro**
- Footprinting a Target Using **Maltego**
- Performing Automated **Network Reconnaissance** Using **Recon-ng**
- Using Open-source Reconnaissance Tool **Recon-ng** to Gather **Personnel Information**
- Collecting Information from Social Networking Sites Using **Recon-ng Pushpin**
- Automated Fingerprinting of an Organization Using **FOCA**
- Identifying Vulnerabilities and Information Disclosures in Search Engines Using **SearchDiggity**

Lab Analysis

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

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

Lab 1

Open Source Information Gathering Using Windows Command Line Utilities

Windows offers several powerful command line utilities that help attackers as well as ethical hackers and pen testers to gather open source information about the target of the evaluation.

ICON KEY

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

Lab Scenario

As a professional Ethical Hacker or Pen Tester, your first step will be to check for the reachability of a computer in the target network. Operating systems offer several utilities that you can readily use for primary information-gathering. Windows command-line utilities such as ping, nslookup, and tracert gather important information like IP address, maximum Packet Fame size, etc. about a target network or system that form a base for security assessment and pen test.

Lab Objectives

This lab demonstrates how to use ping, nslookup, and tracert utilities to gather information about a target. The lab teaches how to:

- Use ping utility to find the IP address of a target domain
- Use ping utility to emulate the tracert (traceroute) command
- Find the maximum frame size for the network
- Identify Internet Control Message Protocol (ICMP) type and the code for echo request and echo reply packets

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 02 Footprinting and Reconnaissance

Lab Environment

To carry out this lab, you need:

- Administrator privileges to run the tools
- TCP/IP settings correctly configured, and an accessible DNS server
- Windows Server 2012

HaCkRhInO-TeaM !

Lab Duration

Time: 10 Minutes

Overview of The Lab

Ping is a network administration utility used to test the reachability of a host on an IP network and to measure the round-trip time for messages sent from the originating host to a destination computer. The ping command sends ICMP echo request packets 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 ICMP type and code in the ping reply provide important insight of the network.

The nslookup is a network administration command-line tool generally used for querying the Domain Name System (DNS) to obtain a domain name or IP address mapping or for any other specific DNS record.

The traceroute is a computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an IP network.

Lab Tasks

TASK 1

Finding IP Address of a Target Domain

1. Find the IP address for http://www.certifiedhacker.com.
2. Right-click the **Windows** icon at the lower-left corner of the screen.

FIGURE 1.1: Windows Server 2012 – Desktop view

PING stands for Packet Internet Groper.

Ping command Syntax: ping [-q] [-v] [-R] [-c Count] [-w Wait] [-s PacketSize] Host.

3. Click **Command Prompt** to launch the command prompt program.

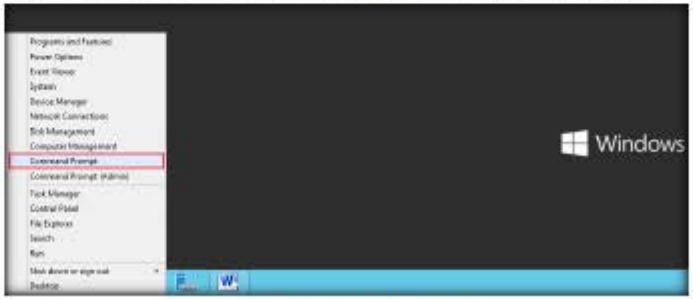


FIGURE 1.2: Windows Server 2012 – Apps

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

4. Type **ping www.certifiedhacker.com** in the command prompt window, and press **Enter** to find its IP address. The displayed response should be similar to the one shown in the following screenshot.

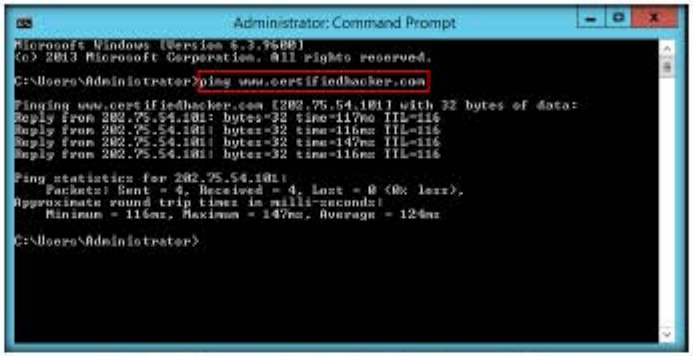


FIGURE 1.3: The ping command to extract the IP address for www.certifiedhacker.com

For the command, ping -c count, specify the number of echo requests to send.

5. Note the target domain's IP address in the result above: **202.75.54.101**. You also get information on Ping Statistics, such as packets sent, packets received, packets lost, and Approximate round-trip time.

6. Now, find the maximum frame size on the network. In the command prompt window, type **ping www.certifiedhacker.com -f -l 1500**

TASK 2

Finding Maximum Frame Size

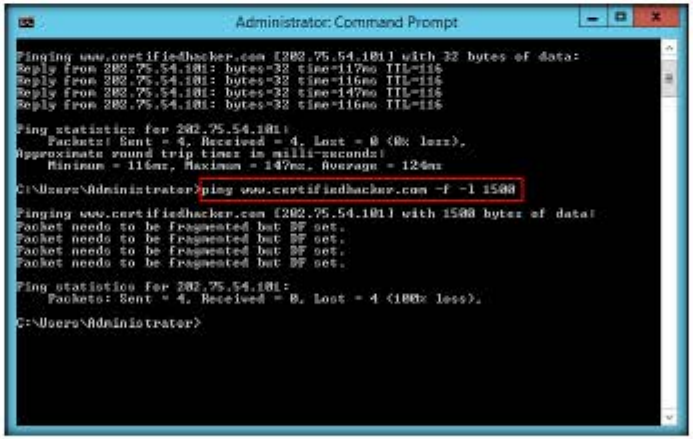


FIGURE 1.4: The ping command for www.certifiedhacker.com with –f –l 1500 options

-f switch sets the Do Not Fragment bit on the ping packet. By default, the ping packet allows fragmentation.

7. 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. Since we used the -f switch with the ping command, the packet was not sent, and the ping command returned this error.

8. Type **ping www.certifiedhacker.com –f –l 1300.**

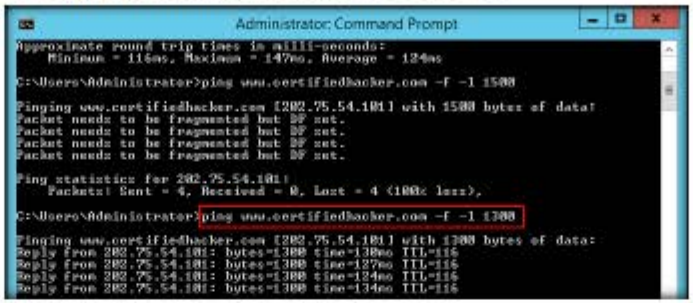


FIGURE 1.5: The ping command for www.certifiedhacker.com with –f –l 1300 options

In the ping command, the –l size option means to send the buffer size.

9. Observe that the maximum packet size is less than 1500 bytes and more than 1300 bytes.
10. 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 is the maximum frame size on this machine's network.

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

In the ping command, "Ping –q," means quiet output, only summary lines at startup and completion.

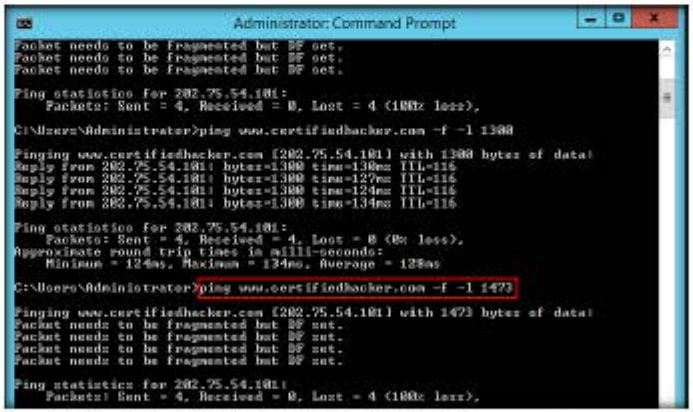


FIGURE 1.6: The ping command for www.certifiedhacker.com with –f –l 1473 options

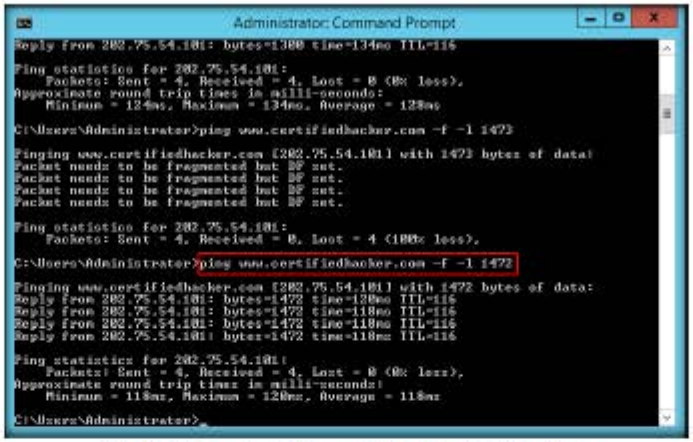


FIGURE 1.7. The ping command for www.certifiedhacker.com with –f –l 1472 options

The ping command, "Ping –R," means record route. It turns on route recording for the Echo Request packets, and displays the route buffer on returned packets (ignored by many routers).

11. Now, find out 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.
12. In the command prompt, type **ping www.certifiedhacker.com -i 3**. This option sets the time to live (**-i**) value as **3**.

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

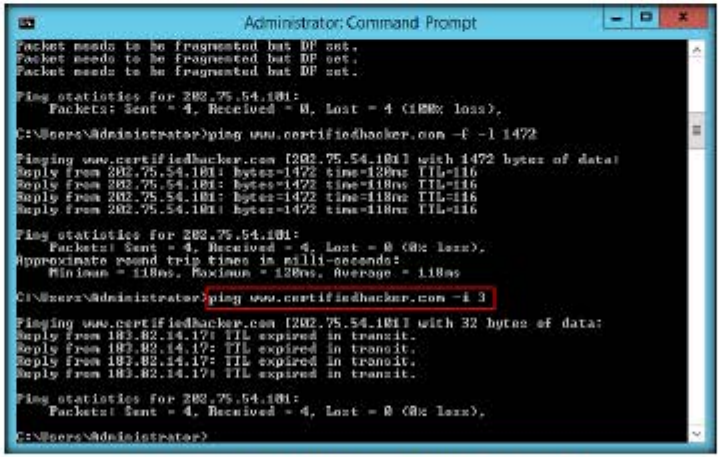


FIGURE 1.8. The ping command for www.certifiedhacker.com with –i 3 options

The ping command, "ping –i wait," means wait time, that is the number of seconds to wait between each ping.

13. Reply from 183.82.14.17: TTL expired in transit means that the router (183.82.14.17, students will have some other IP address) discarded the frame, because its TTL has expired (reached 0).

HaCkRhInO-TeaM !

TASK 3

Emulate Tracert

14. We will use the ping command to emulate a traceroute.
15. Find the traceroute from your PC to www.certifiedhacker.com using the **tracert** command.
16. The results you receive might differ from those in this lab.
17. Launch a new command prompt and type **tracert www.certifiedhacker.com**. This command traceroutes the network configuration information of the target domain.

The router discards packets when TTL reaches 0(Zero) value.

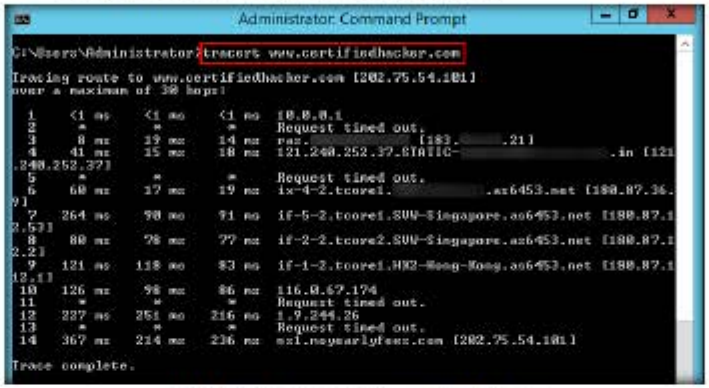


FIGURE 1.9: The tracert command for www.certifiedhacker.com

18. Minimize the command prompt shown above and launch a new command prompt. In the command prompt window, type **ping. www.certifiedhacker.com -i 2 –n 1**. The only difference from the previous ping command is that we are setting the TTL to two in an attempt to check the life span of the packet.

In the ping command, -t means to ping the specified host until stopped.

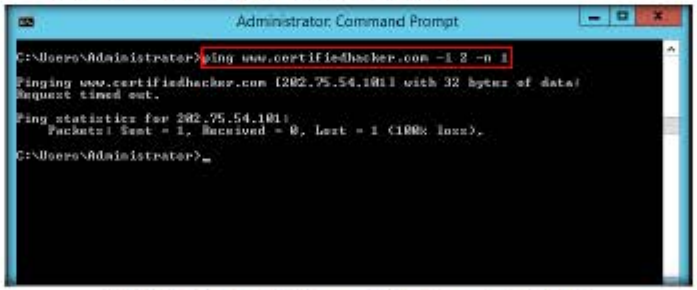


FIGURE 1.10: The ping command for www.certifiedhacker.com with –i 2 –n 1 options

19. In the command prompt window, type **ping www.certifiedhacker.com -i 3 –n 1**. This sets the TTL value to **3**.

In the ping command, the -v option means verbose output, which lists individual ICMP packets, as well as echo responses.

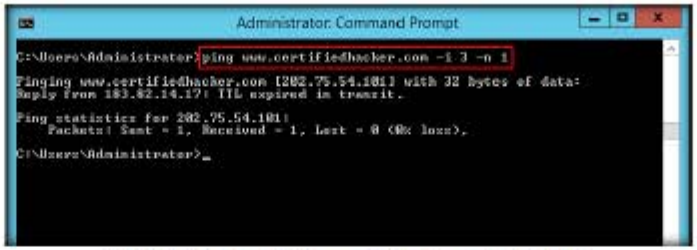


FIGURE 1.11: The ping command for www.certifiedhacker.com with –i 3 –n 1 options

20. Observe that there is a reply coming from the IP address **183.82.14.17** and there is no packet loss.

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

21. In the command prompt, type **ping www.certifiedhacker.com -i 4 -n 1**. This sets the time to live value as **4**.

In the ping command, the -w option represents the timeout in milliseconds to wait for each reply.

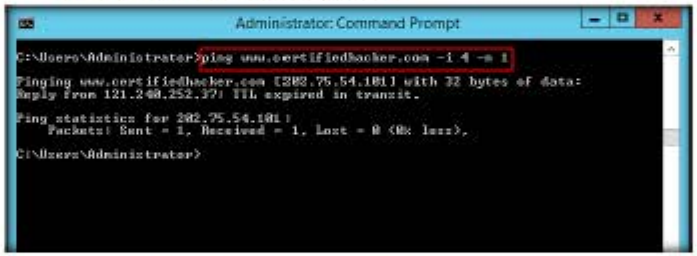


FIGURE 1.12: The ping command for www.certifiedhacker.com with –i 4 –n 1 options

22. Repeat the above step until you reach the IP address for **www.certifiedhacker.com** (in this case, **202.75.54.101**).

Traceroute sends a sequence of Internet Control Message Protocol (ICMP) echo request packets addressed to a destination host.

FIGURE 1.13: The ping command for www.certifiedhacker.com with –i 10 –n 1 options

23. Here the successful ping to reach **www.certifiedhacker.com** is 14 hops. The output will be similar to the trace route results

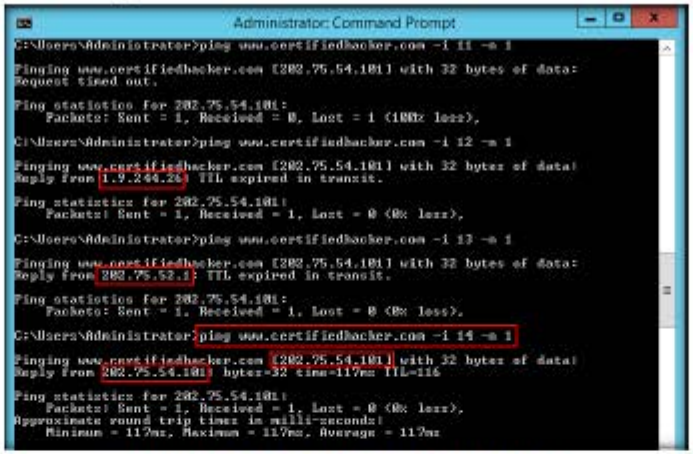


FIGURE 1.14: The ping command for www.certifiedhacker.com with –i 14 –n 1

24. This implies that, at a time to live value of 14, the reply is received from the destination host (202.75.54.101).

Note: This result might vary in your lab environment.

25. Make a note of all the IP addresses from which you receive the reply during the ping to emulate tracert.

TASK 4

Launch nslookup terminal

26. Launch a new command prompt, type **nslookup**, and press **Enter**. This displays the default server and its address assigned to **Windows Server 2012** host machine.

FIGURE 1.15: Command prompt with nslookup command

Note: The DNS server Address (8.8.8.8) may differ in your lab environment

TASK 5

Obtain the IP Address of the Target Domain using nslookup

27. In the nslookup **interactive** mode, type **set type=a** and press **Enter**.

Setting the type as a configures nslookup to query for the IP address of a given domain.

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

28. Type the target domain **www.certifiedhacker.com** and press **Enter**. This resolves the IP address and displays the result shown in the following screenshot:

FIGURE 1.16: In nslookup command, set type=a option

29. The first two lines in the result are:

    google-public-dns-a.google.com and **8.8.8.8**

    This specifies that the result was directed to the default server hosted on the local machine (**Windows Server 2012**) that resolves your requested domain.

Typing "help" or "?" at the command prompt generates a list of available commands.

30. Thus, if the response is coming from your local machine's server (Google), but not the server that legitimately hosts the domain **www.certifiedhacker.com**, it is considered to be a non-authoritative answer.

    www.certifiedhacker.com

    202.75.54.101

31. Since the result returned is non-authoritative, you need to obtain the domain's authoritative name server.

TASK 6

Find Cname

32. Type **set type=cname** and press **Enter**.

    The CNAME lookup is done directly against the domain's authoritative name server and lists the CNAME records for a domain.

33. Type **www.certifiedhacker.com** and press **Enter**.

34. This returns the domain's authoritative name server, along with the mail server address shown in the following screenshot:

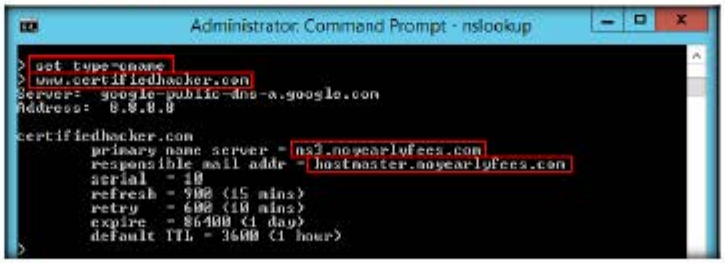


FIGURE 1.17: In nslookup command, set type=cname option

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

TASK 7

Obtain the IP Address of the Primary Name Server

35. Since you have obtained the authoritative name server, you will need to determine the IP address of the name server.
36. Issue the command **set type=a** and press **Enter**.
37. Type **ns3.noyearlyfees.com** (or the primary name server that is displayed in your lab environment) and press **Enter**. This returns the IP address of the server as shown in the following screenshot:

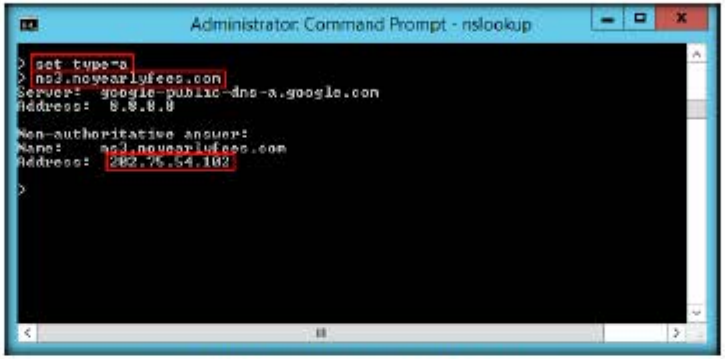


FIGURE 1.18 Screenshot showing returns the IP address of the server

To make querytype of NS a default option for your nslookup commands, place one of the following statements in the user_id.NSLOOKUP.ENV data set: set querytype=ns or querytype=ns.

38. The authoritative name server stores the records associated with the domain. So, if an attacker can determine the authoritative name server (primary name server) and obtain its associated IP address, he/she might attempt to exploit the server to perform attacks which include DoS, DDoS, URL Redirection and so on.

Lab Analysis

Document all the IP addresses, reply request IP addresses, their TTLs, DNS server names, and other DNS information.

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

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

Lab 2

Gathering Personal Information Using Online People Search Services

Online people search services provide real-time information about people. These tools help to perform online footprinting and discover information about people.

ICON KEY

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

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 02 Footprinting and Reconnaissance

Lab Scenario

During information gathering, you need to gather personal information about employees working on critical positions in the target organization such as Network Administrator, Help Desk Employees, Receptionist, etc. The information collected can be useful in performing social engineering. This lab will demonstrate how you can search for personal information using online people search services.

Lab Objectives

The objective of this lab is to gather personal information using pipl, a utility that can be found at https://pipl.com/.

Lab Environment

In the lab, you need:

- A Web browser with an Internet connection
- Administrator privileges to run the tools
- Windows Server 2012

Lab Duration

Time: 5 Minutes

Overview of Pipl

Pipl aggregates vast quantities of public data and organizes the information into easy-to-follow profiles. Information like name, email address, phone number, street address and username can be easily found using this tool.

Lab Tasks

TASK 1

Launch Web Browser

1. Click the **Windows** icon at the lower-left corner of the screen.

FIGURE 2.1: Windows Server 2012 – Desktop view

2. The **Start** screen appears. Click the **down arrow button**.

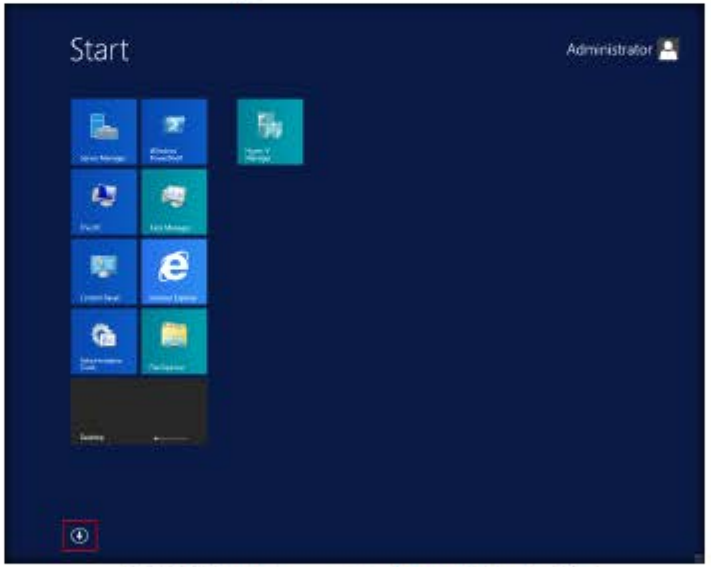


FIGURE 2.2: Click on down arrow to view installed apps in Windows Server 2012

PIPL people search allows you to find old friends, reunite with classmates, teammates and military buddies, or find lost and distant family.

HaCkRhInO-TeaM !

3. The **Apps** screen appears. Click **Google Chrome** to launch the Chrome browser (or launch any other browser of your choice).

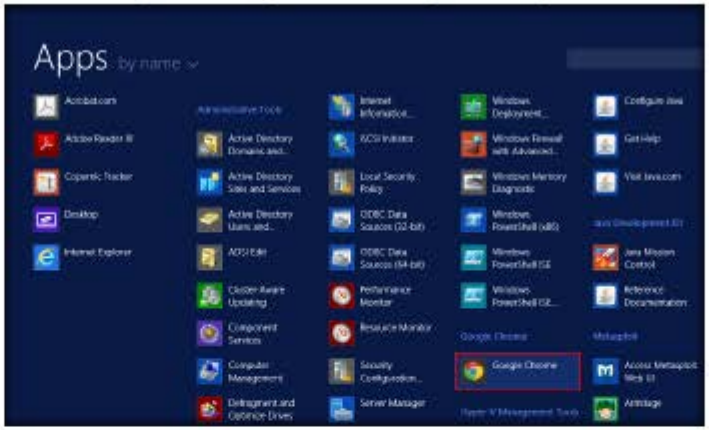


FIGURE 2.3: Installed apps in Windows Server 2012

Usernames in use by the person online. This includes screen names, handles and nicknames from across the web, social media sites, forums and more.

TASK 2

People Search using pipl

4. The Google Chrome browser window appears.
5. In the browser, type **https://pipl.com** in the address bar and press **Enter**.
6. The Pipl home page appears as shown in the following screenshot.

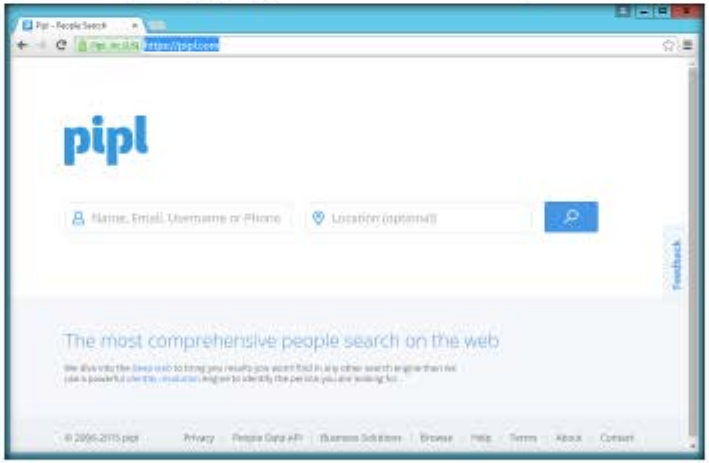


FIGURE 2.4: Pipl home page https://pipl.com/

Apart from Name search, pipl supports four types of search:

- Email Address
- Phone Number
- Username
- Residential Address

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

7. To begin the search, enter the details of the person you want to search for in the **Name, Email, Username or Phone** fields and click the **Search icon**.

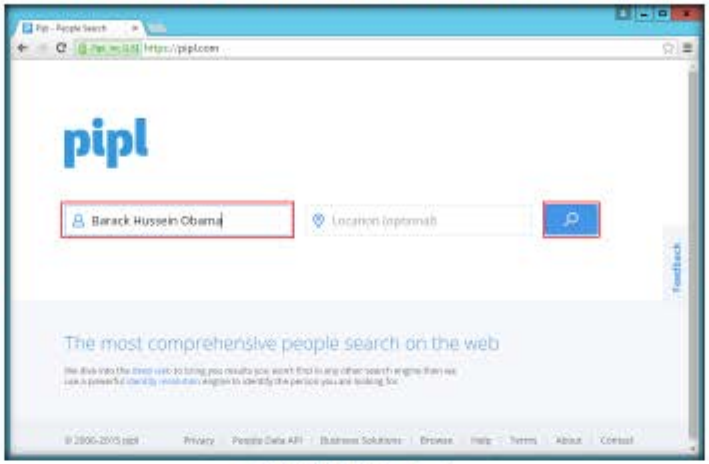


FIGURE 2.5: Pipl - Name Search

Image URL of profile images and other images that are related to the person. Each image includes a thumbnail token for our complementary thumbnail service.

8. Pipl returns search results with the name you have entered.

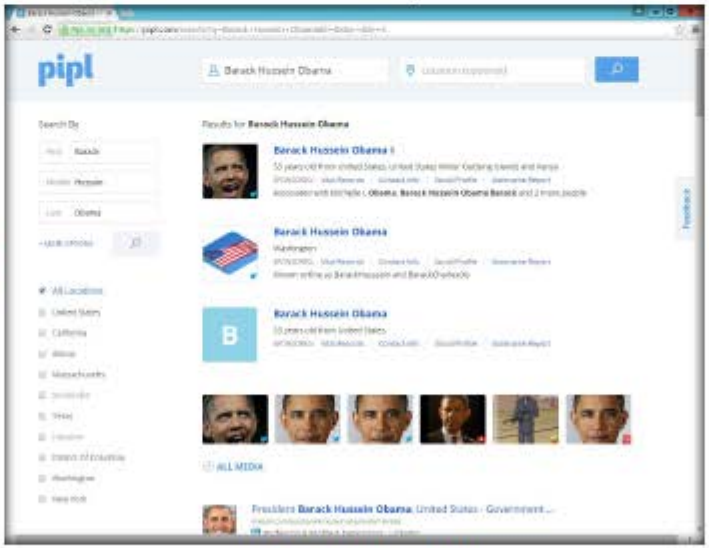


FIGURE 2.6: Pipl People Search Results

Public profiles from social networks are aggregated in pipl and many places, including search engines.

9. Click any of the links for more information on the person.

Date of Birth, might be given as a range if the exact date is unknown.

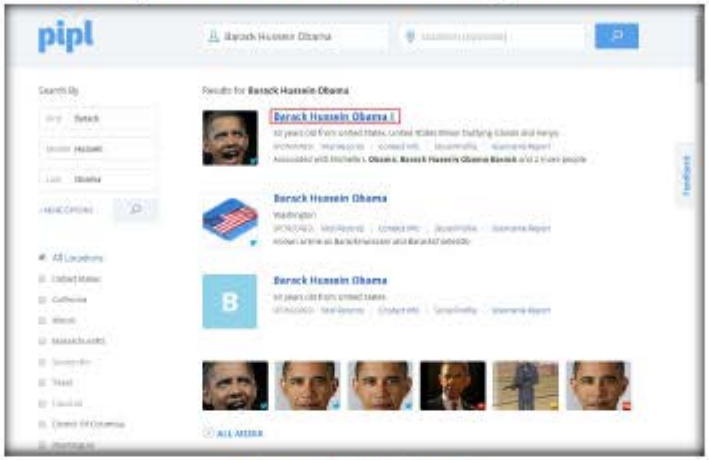


FIGURE 2.7: Pipl People Search Results

10. Pipl displays the complete information as shown in the below screenshot.
11. This will show career, education, usernames, phones, etc. information.

Home and work, current and past addresses associated with the person. Includes house number, street, city, ZIP code, state and country.

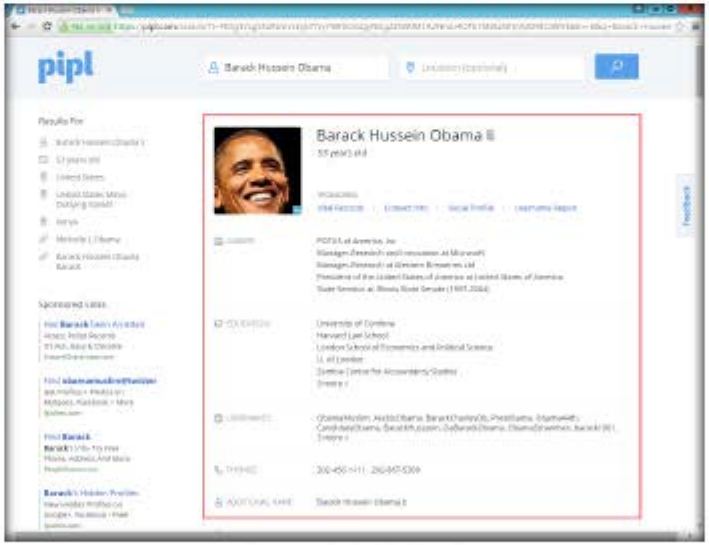


FIGURE 2.8: Pipl People Search Results

12. To learn the places where the person visited, click any link in the **Places** section.

Friends, family, colleagues, social media followers and other people associated with the person.

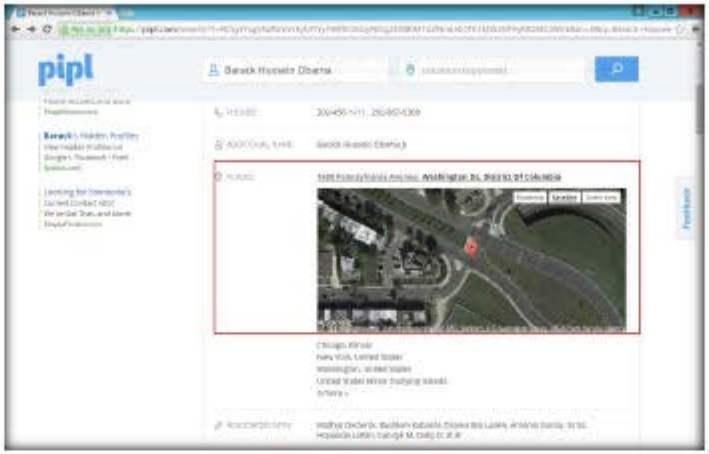


FIGURE 2.9: Pipl Places section

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 3

Collecting Information About a Target Website Using Firebug

Firebug integrates with Firefox providing a lot of development tools to edit, debug, and monitor CSS, HTML, and JavaScript live in any web page.

ICON KEY

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

Lab Scenario

As a part of information gathering activity, you have been asked to collect information on the target website and extract the source code of the web pages built in HMTL, Java Script, CSS script etc. This activity may reveal potential vulnerabilities in the web application that can be exploited later in the security assessment phases. This lab will demonstrate how to reveal source code and collect information about a target website

Lab Objectives

The objective of this lab is to help students learn editing, debugging, and monitoring CSS, HTML and JavaScript, and also obtain server-side technologies and cookies.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 02 Footprinting and Reconnaissance

Lab Environment

In the lab, you need:

- A Web browser with an Internet connection
- Administrator privileges to run the tools
- Windows Server 2012

Lab Duration

Time: 10 Minutes

Overview of Firebug

Firebug is an add-on tool for Mozilla Firefox. Running Firebug displays information like directory structure, internal URLs, cookies, session IDs, etc.

Lab Tasks

TASK 1

Launch Firefox

1. Click the **Windows** icon at the lower left corner of the screen.

FIGURE 3.1: Windows Server 2012 - Desktop view

Firebug includes a lot of features such as debugging, HTML inspecting, profiling and etc. which are very useful for web development.

2. The **Start** screen appears. Click the down arrow button.

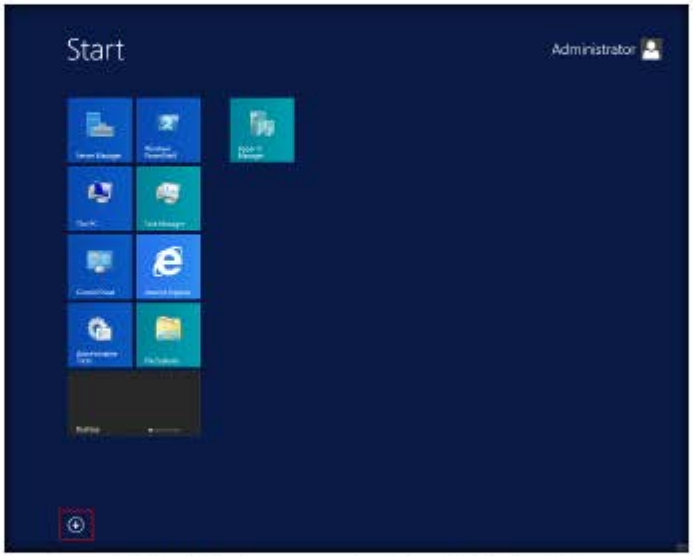


FIGURE 3.2: click on down arrow to view installed apps in Windows Server 2012

The CSS panel manipulates CSS rules. It offers options for adding, editing and removing CSS styles of the different files of a page containing CSS. It also offers an editing mode, in which you can edit the content of the CSS files directly via a text area.

HaCkRhInO-TeaM !

3. The **Apps** screen appears. Click **Mozilla Firefox** to launch the browser.

Firebug features:

- Javascript debugging
- Javascript CommandLine
- Monitor the Javascrit Performance and XmlHttpRequest
- Logging
- Tracing
- Inspect HTML and Edit HTML
- Edit CSS

FIGURE 3.3: Installed apps in Windows Server 2012 – Opening Firefox app

TASK 2

Install Firebug Add-on

4. Launch the Firefox web browser. Type the URL https://addons.mozilla.org/en-US/firefox/addon/firebug in the address bar and press **Enter**.
5. The Firebug add-on webpage appears. Click **Add to Firefox**.

Firebug inspects HTML and modify style and layout in real-time

FIGURE 3.4: Entering URL in Firefox browser window

6. The add-on begins to download.

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

7. On completion of download, a **Software Installation** dialog-box appears. Click **Install Now**.

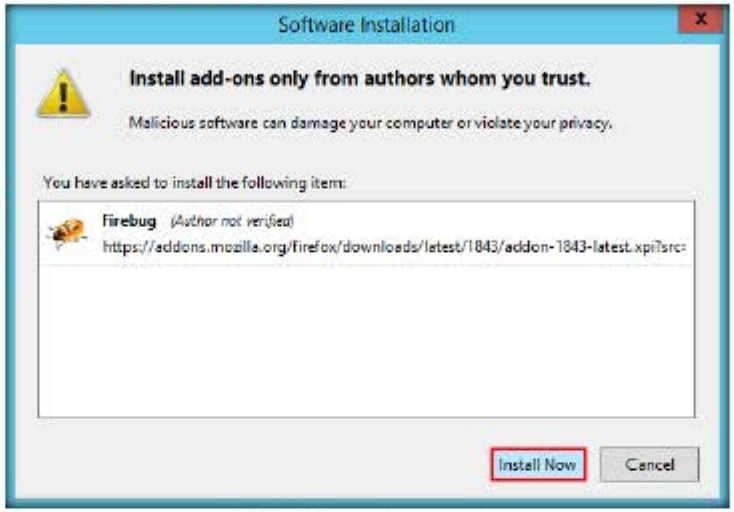


FIGURE 3.5: Software Installation dialog-box

Firebug adds several configuration options to Firefox. Some of these options can be changed through the UI, others can be manipulated only via about:config.

8. On successful installation, an extension pop-up appears stating that firebug has been successfully installed.

FIGURE 3.6: extension pop-up

extensions.firebug.panelTabMinWidth describes minimal width in pixels of the Panel tabs inside the Panel Bar when there is not enough horizontal space.

9. The Firebug add-on appears on the top-right corner of the **Navigation Toolbar** as shown in the following screenshot:

FIGURE 3.7: Firebug add-on

extensions.firebug.showFirstRunPage specifies whether to show the first run page.

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

10. Enter the URL of the target website in the address bar and press **Enter**. In this lab, the target website is moviescope and its URL is http://www.moviescope.com.

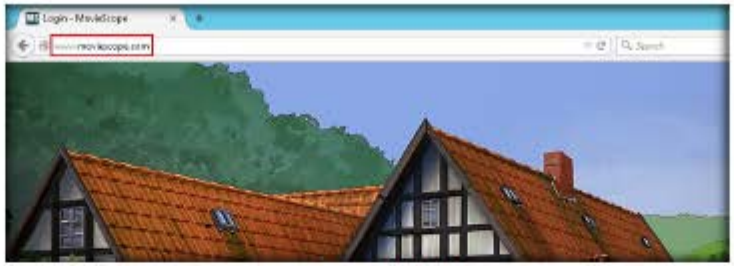


FIGURE 3.8: moviescope home page

The console panel offers a JavaScript command line, lists all kinds of messages and offers a profiler for JavaScript commands.

11. Click the Firebug add-on on the top-right corner of the **Navigation Toolbar** to enable the Firebug control panel.

FIGURE 3.9: Launching Firebug add-on

TASK 3

Examine Console Tab

12. The Firebug panel appears at the lower end of the screen. Click the **Console** tab, and from the Firebug panel's menu bar click **Enable**.

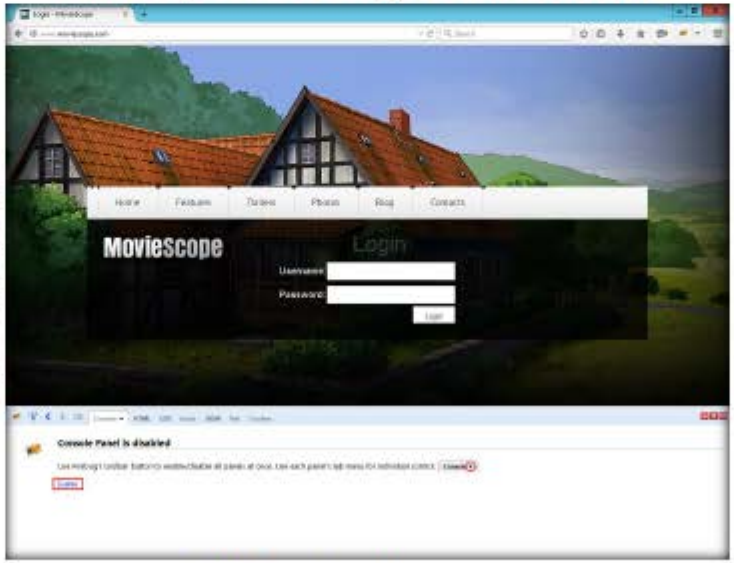


FIGURE 3.10: Selecting Console tab from Firebug panel

The HTML panel displays the generated HTML/XML of the currently opened page. It differs from the normal source code view, because it also displays all manipulations on the DOM tree. On the right side it shows the CSS styles defined for the currently selected tag, the computed styles for it, layout information and the DOM variables assigned to it in different tabs.

13. Press **F5** on the keyboard to refresh the webpage.
14. Click The **Warnings** tab under the **Console** section. Under this tab, Firebug displays all the issues related to the security of the website's architecture, as shown in the following screenshot:

Net Panel's purpose is to monitor HTTP traffic initiated by a web page and present all collected and computed information to the user. Its content is composed of a list of entries where each entry represents one request/response round trip made by the page..

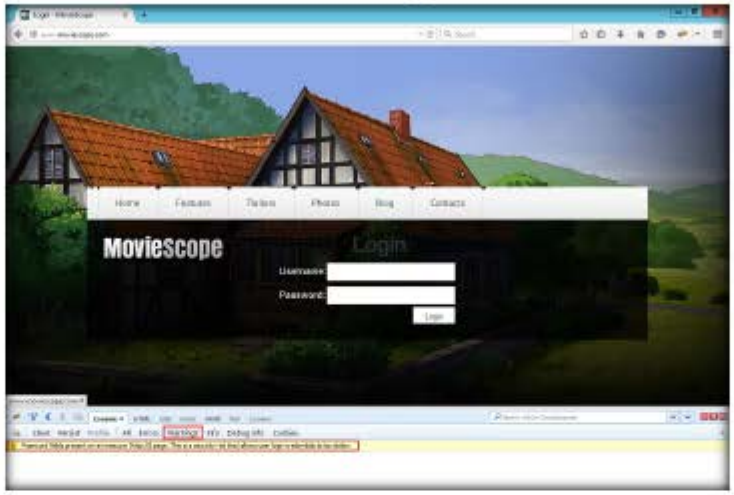


FIGURE 3.11: Firebug Panel Displaying Warning

15. The warning returned in the above screenshot states that the password fields are present on an insecure (http://) page. This vulnerability allows attackers to easily sniff the passwords in plain text.

Note: The warning results may vary depending on the websites you access.

16. You can view the results in all the other tabs under the **Console** section, which might return useful information related to the website/web application.

TASK 4

Examine HTML Tab

17. Click the **HTML** tab in the Firebug UI. The HTML section contains two tags: **head** and **body**, which contain scripts and text that might reveal the build of the website.

Note: If you find this section empty, refresh the webpage.

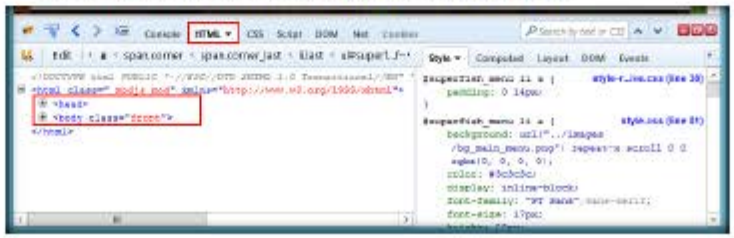


FIGURE 3.12: Firebug HTML tags

Script panel debugs JavaScript code. Therefore the script panel integrates a powerful debugging tool based on features like different kinds of breakpoints, step-by-step execution of scripts, a display for the variable stack, watch expressions and more...

18. The head and body tags contain information related to the authentication of the username and password fields, such as the type of input that is to be given in the fields (numbers or characters, or combination of numbers and characters, etc.) which allows attackers to narrow down their exploitation techniques.

    For example, an attacker who knows that the password field takes only numbers can perform a brute force attack with only combinations of numbers (instead of applying random combinations of numbers, letters, and special characters).

19. Expand these nodes and observe the script written to develop the webpage.

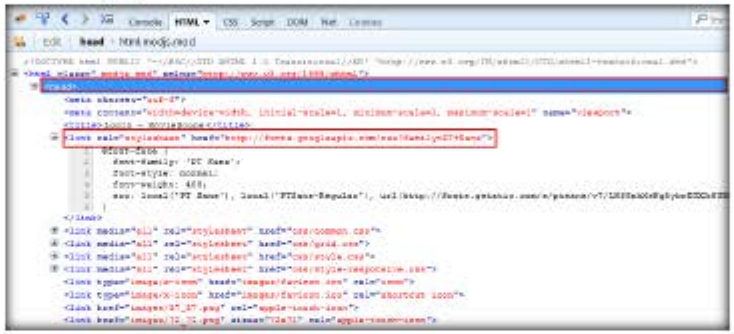


FIGURE 3.13: Firebug HTML tags

20. Refer to tabs such as **Style**, **Computed**, **Layout** and so on in the right pane in order to observe the script used to design the webpage.

Export cookies for this site - exports all cookies of the current website as text file. Therefore the Save as dialog is opened allowing you to select the path and choose a name for the exported file.

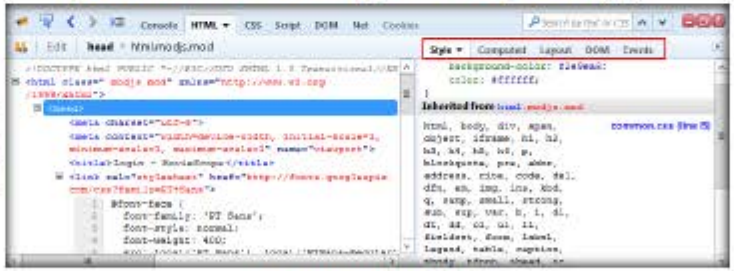


FIGURE 3.14: Firebug additional tabs

TASK 5

Examine CSS and Script Tab

21. The **CSS** and **Script** tabs also display the HTML and Java scripts that were used to design the webpage.

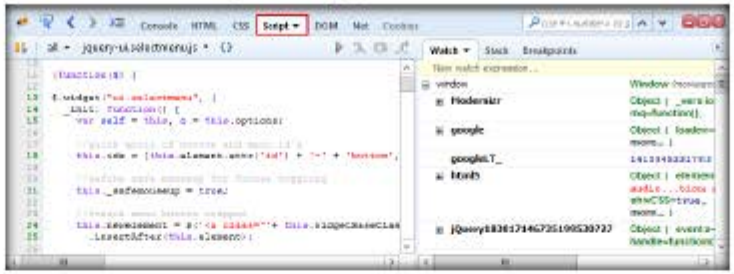


FIGURE 3.15: Firebug Script tab

22. Attackers could use these scripts to build a similar website (cloned website) which could be used to serve malicious purposes such as harvesting the data entered in specific fields.

TASK 6

Examine DOM Tab

23. Click **DOM** (Document Object Model) tab in the Firebug control panel.

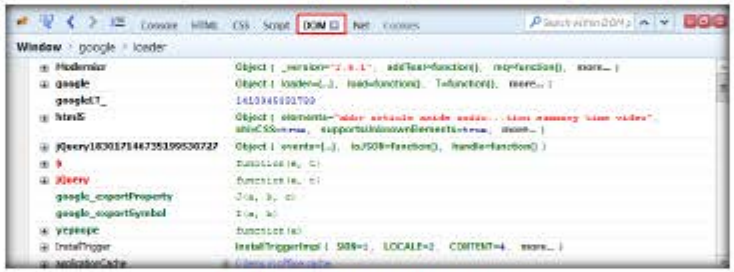


FIGURE 3.16: Firebug Document Object Model tab

24. This tab contains scripts written in various web technologies such as html5, jQuery, etc. This allows attackers to perform exploitation techniques on a specific version of a web application, which leads to expose sensitive information.

TASK 7

Examine NET Tab

25. Now, click the **Net** tab in the Firebug control panel and click **Enable**.

FIGURE 3.17: Firebug Enabling Net tab

26. Select the **All** tab under this section, and then **refresh** the page.
27. This tab displays the GET requests and responses for all the items in the **Net** section such as **HTML**, **CSS**, etc., along with their size, status, timeline, domain and remote IP.

Firebug's CSS tabs tell you everything you need to know about the styles in your web pages, and if you don't like what it's telling you, you can make changes and see them take effect instantly.

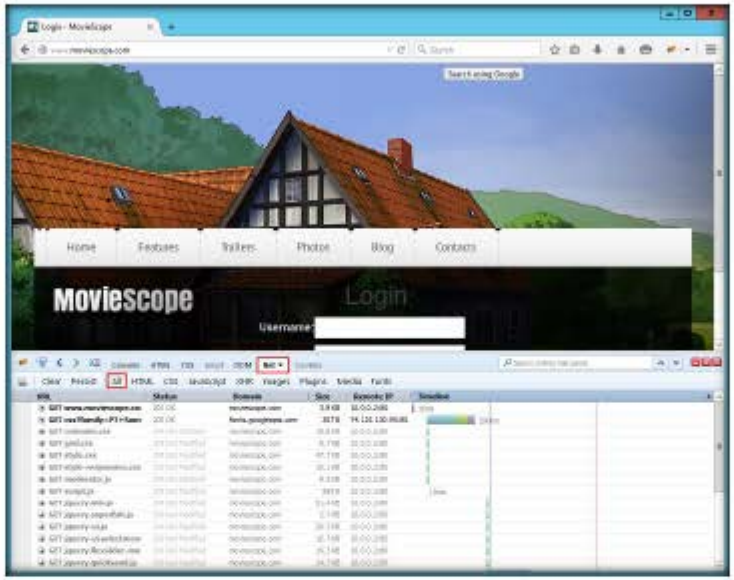


FIGURE 3.18: Firebug Net tab

When your CSS boxes aren't lining up correctly it can be difficult to understand why. Let Firebug be your eyes and it will measure and illustrate all the offsets, margins, borders, padding, and sizes for you.

28. Under this tab, expand a **GET** request node related to **moviescope**.
29. Under the **Headers** tab, expand the **Response Headers** node.

FIGURE 3.19: Firebug All tab

30. Observe the server name (IIS) and its version, along with the web application framework (ASP.NET) used to develop the website and its version. By learning this, attackers can target the vulnerabilities of that specific version in an attempt to exploit the web application.

TASK 8

Examine Cookies Tab

31. Click the **Cookies** tab in the Firebug control panel and click **Enable**.

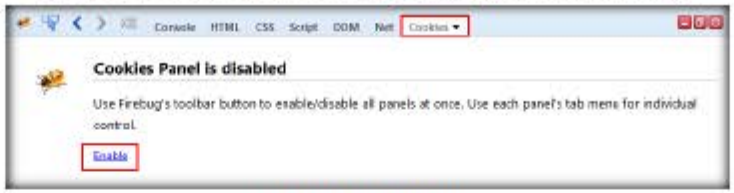


FIGURE 3.20: Firebug Cookies tab

You can also manage cookie permissions for the current site directly from the Firebug's toolbar. The permission button displays the current status as a label and it's automatically updated if the permission is changed (e.g. from the Firefox options dialog).

32. Refresh the webpage. Observe the cookies related to the current session as shown in the following screenshot:

FIGURE 3.21: Firebug Cookies tab

Note: The cookies results might vary in your lab environment.

33. Attackers can use sniffing techniques to steal the cookies and manipulate them, thereby hijacking the session of an authenticated user without the need of entering legitimate credentials.
34. By gaining the information described in the lab, an attacker can obtain the script related to a web page, identify the server-side technologies and manipulate the cookies, which allow them to perform fraudulent activities such as entering the web application, cloning a web page, hijacking a session, stealing database information , etc.

Lab Analysis

Collect information like internal URLs, cookie details, directory structure, session IDs, etc. for different websites using Firebug.

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

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

Lab 4

Extracting a Company's Data Using Web Data Extractor

Web Data Extractor is used to extract a targeted company's contact details or data such as emails, fax, phone through web for responsible b2b communication.

ICON KEY

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

Lab Scenario

In the process of information gathering, your next task will be to extract information from the organization website. You are required to perform web data extraction in order to gain useful information from the website. This lab will show you how to perform web data extraction on the target website.

Lab Objectives

The objective of this lab is to demonstrate how to extract a company's data using Web Data Extractor. Students will learn how to:

- Extract meta tag, email, phone/fax from the web pages

Lab Environment

To carry out the lab, you need:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 02 Footprinting and Reconnaissance

- Web Data Extractor, which can be acquired from at **D:\CEH-Tools\CEHv9 Module 02 Footprinting and Reconnaissance\Web Spiders\Web Data Extractor**. You can also download the latest version of Web Data Extractor from the link http://www.webextractor.com/download.htm. If you decide to download the latest version, then screenshots shown in the lab might differ
- Windows Server 2012

Lab Duration

Time: 5 Minutes

Overview of Web Data Extracting

Web Data Extraction is the process of extracting data from Web pages. It is also referred as Web Scraping or Web Data Mining

Lab Tasks

TASK 1

Install Web Data Extractor

1. Navigate to **D:\CEH-Tools\CEHv9 Module 02 Footprinting and Reconnaissance\Web Spiders\Web Data Extractor** and double-click **wde.exe**.
2. If the **Open File - Security Warning** pop-up appears, click **Run**.
3. Follow the wizard steps to install Web Data Extractor.

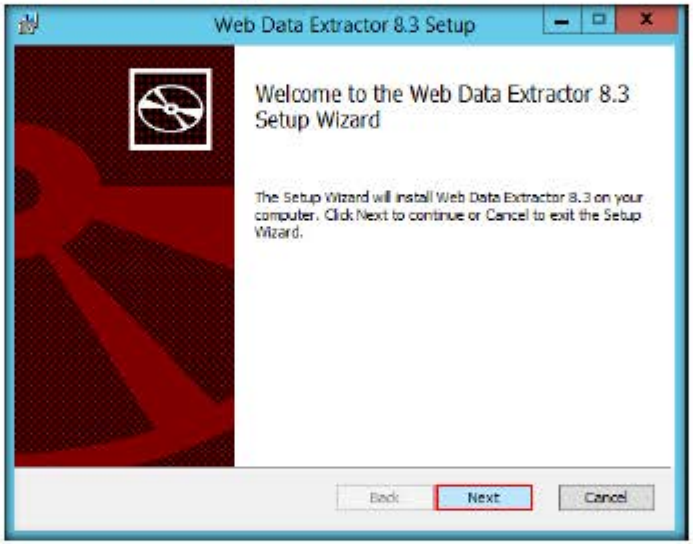


FIGURE 4.1: Web Data Extraction Setup pop-up Wizard

WDE - Phone, Fax Harvester module is designed to spider the web for fresh Tel, FAX numbers targeted to the group that you want to market your product or services

4. On installation, launch **Web Data Extractor** from the **Apps** screen.

FIGURE 4.2: Installed apps in Windows Server 2012– Selecting Web Data Extractor

TASK 2

Configuring Web Data Extractor

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

FIGURE 4.3: The Web Data Extractor main window

It has various limiters of scanning range - url filter, page text filter, domain filter - using which you can extract only the links or data you actually need from web pages, instead of extracting all the links present there, as a result, you create your own custom and targeted data base of urls/links collection

6. Clicking **New** opens the **Session settings** window.
7. Type a URL (http://www.certifiedhacker.com) in the **Starting URL** field. Check all the options as shown in the following screenshot, and click **OK**.

Web Data Extractor automatically get lists of meta-tags, e-mails, phone and fax numbers, etc. and store them in different formats for future use

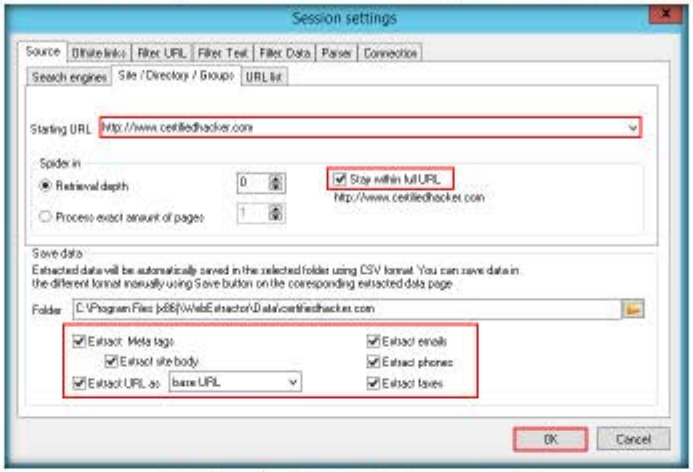


FIGURE 4.4: Web Data Extractor the Session setting window

TASK 3

Extracting Data from Web Data Extractor

8. Click **Start** to initiate the Data Extraction.

FIGURE 4.5: Web Data Extractor initiating the data extraction windows

9. Web Data Extractor will start collecting information (emails, Phones, Faxes, etc.).

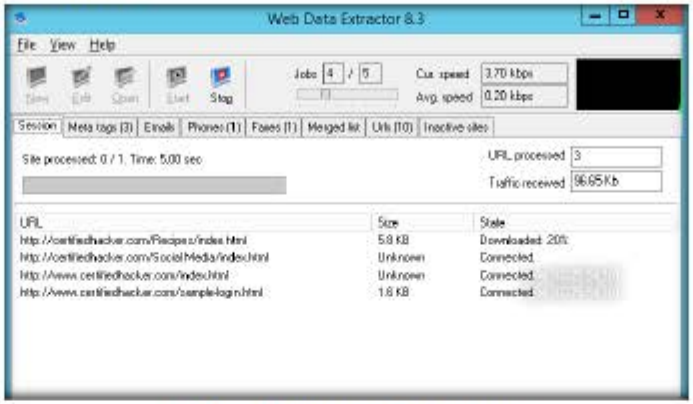


FIGURE 4.6: Web Data Extractor collecting information

It supports operation through proxy-server and works very fast, as it is able of loading several pages simultaneously, and requires very few resources. Powerful, highly targeted email spider harvester

10. Once the data extraction process is completed, an **Information** dialog box appears. Click **OK**.

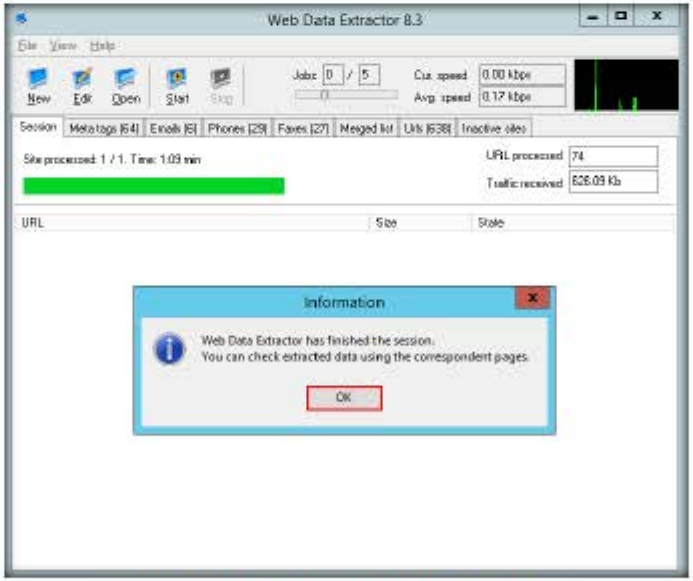


FIGURE 4.7: Web Data Extractor Data Extraction information windows

Fixed "Stay with full url" and "Follow offsite links" options which failed for some sites before

Meta Tag Extractor module is designed to extract URL, meta tag (title, description, keyword) from web-pages, search results, open web directories, list of urls from local file

TASK 4

Examine the Collected Data

11. View the extracted information by clicking the tabs.

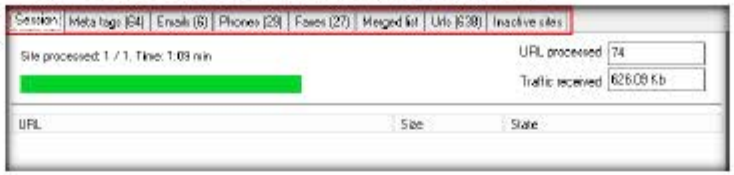
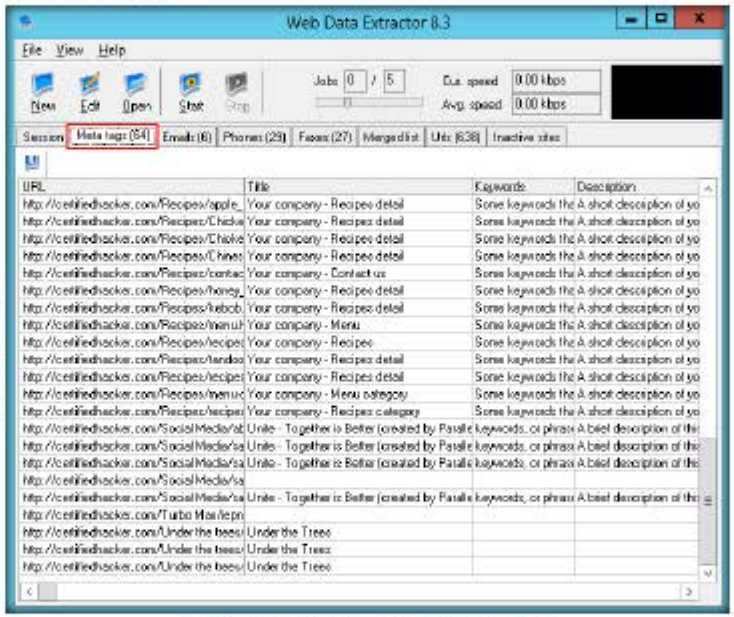


FIGURE 4.8: Web Data Extractor Data Extraction windows

12. Select **Meta tags** tab to view the URL, title, keywords, description, host, domain, etc.



WDE send queries to search engines to get matching website URLs. Next it visits those matching websites for data extraction. How many deep it spiders in the matching websites depends on "Depth" setting of "External Site" tab

FIGURE 4.9: Web Data Extractor Extracted emails windows

13. Select the **Emails** tab to view the email address, name, URL, Title, host, keywords density, etc. information related to emails.

The option "No duplicate domains" is really useful when a list contains e-mails in corporative domains. Using this option you avoid mailing the same message to the same company repeatedly. But at the same time you keep only one e-mail address per a web-based service (domains yahoo, hotmail, msn, etc.), while in fact each address in such domains belongs to a different person.

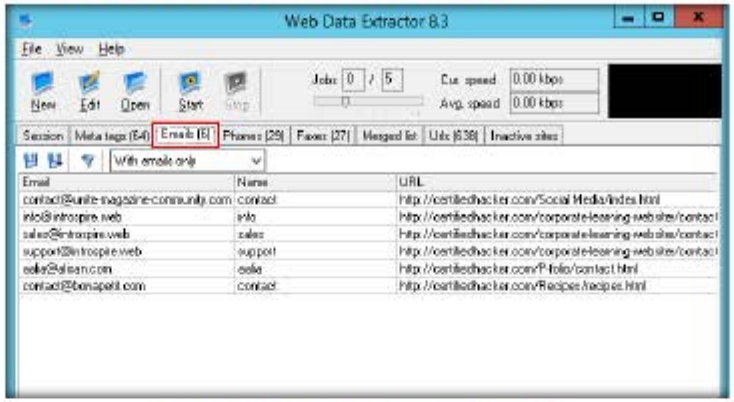


FIGURE 4.10: Web Data Extractor Extracted Phone details window

14. Select **Phones** tab to view the phone number, source, tag, etc.

Save extracted links directly to disk file, so there is no limit in number of link extraction per session. It supports operation through proxy-server and works very fast, as it is able of loading several pages simultaneously, and requires very few resources

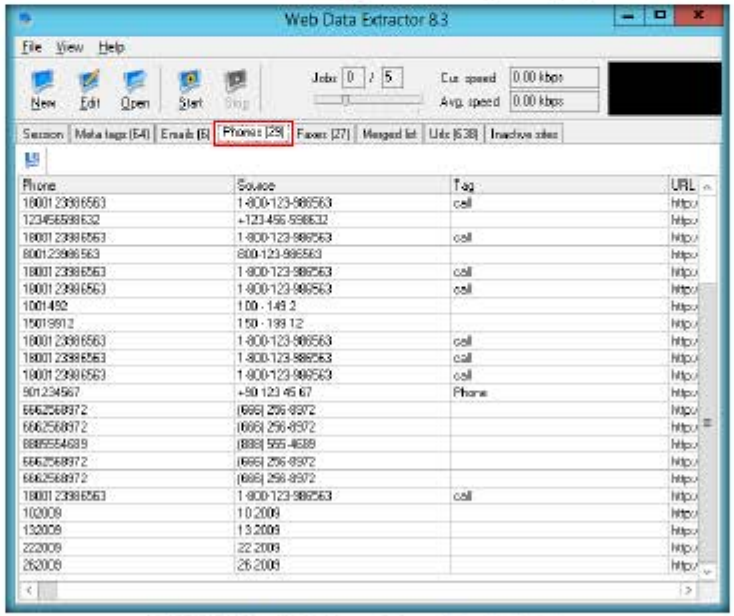


FIGURE 4.11: Web Data Extractor Extracted Phone details window

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

TASK 5

Save a Session

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

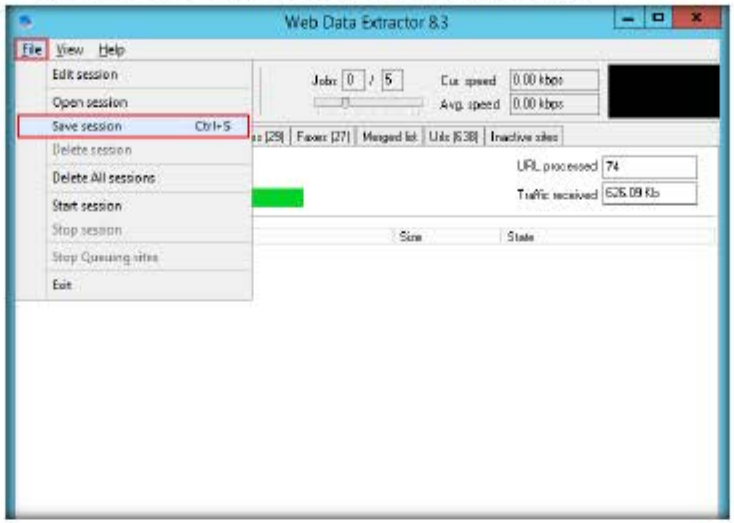


FIGURE 4.12: Web Data Extractor Extracted Phone details window

17. Specify the session name in the **Save session** dialog box and click **OK**.

WDE will query 18+ popular search engines, extract all matching URLs from search results, remove duplicate URLs and finally visits those websites and extract data from there

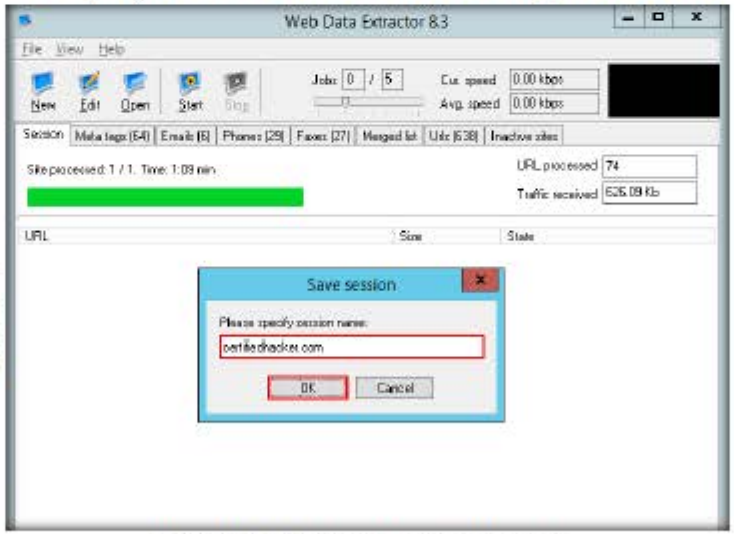
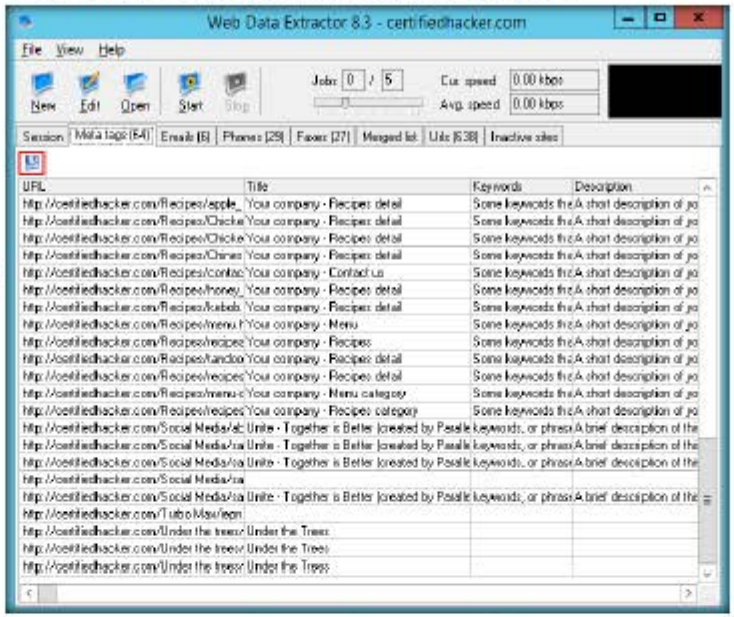


FIGURE 4.13: Web Data Extractor Extracted Phone details window

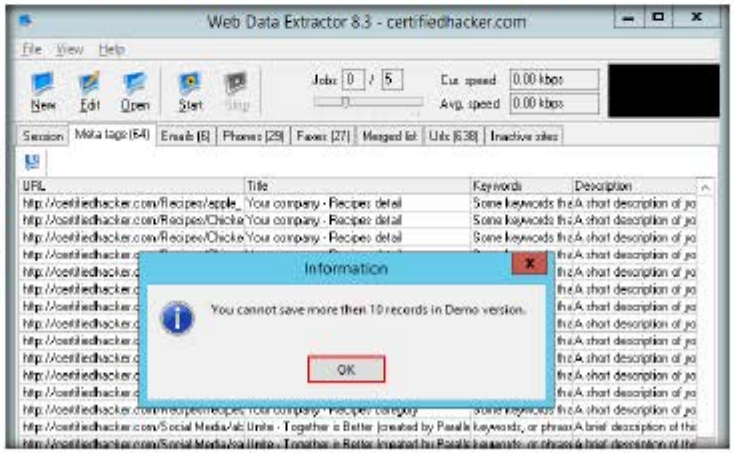
18. Click the **Meta tags** tab and then **click** the **floppy** icon.



WDE send queries to search engines to get matching website URLs

FIGURE 4.14: Web Data Extractor Mega tab

19. An **Information** pop-up may appear with the message, **You cannot save more than 10 records in Demo Version**. Click **OK**.



If you want WDE to stay within first page, just select "Process First Page Only". A setting of "0" will process and look for data in whole website. A setting of "1" will process index or home page with associated files under root dir only.

FIGURE 4.15: Web Data Extractor saving information window

20. Select the **Location** and **File format** and click **Save**.

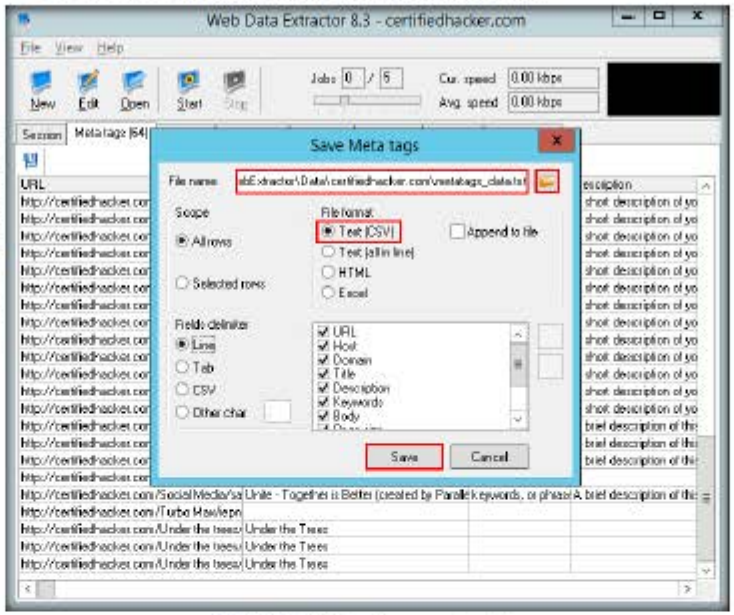


FIGURE 4.16: Web Data Extractor saving window

> If you access the Internet via a dial-up, xDSL, cable modem or LAN that DOES NOT use a firewall or proxy server, then select the Direct connection to the internet option. However, if you connection is through a firewall or proxy server, you will have to choose the Connect through proxy option and supply the required data.

21. By default, the session will be saved at **C:\Program Files (x86)\WebExtractor\Data\certifiedhacker.com**.
22. You can save information from the Emails, Phones, Faxes, Merged list, Urls and Inactive sites tabs.

Lab Analysis

Document all the Meta Tags, Emails, and Phone/Fax.

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

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

HaCkRhInO-TeaM !

Lab 5

Mirroring Website Using HTTrack Web Site Copier

HTTrack Web Site Copier is an offline browser utility that downloads a Web site to a local directory.

ICON KEY

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

Lab Scenario

It can be difficult to perform footprinting on a live website. In that case, you may need to mirror the target website. This mirroring of the website helps you to footprint the web site thoroughly on your local system. As a professional ethical hacker or pen tester, you should be able to mirror the website of the target organization. This lab will demonstrate how to mirror a target website.

Lab Objectives

The objective of this lab is to help students learn mirroring websites using HTTrack Web Site Copier.

Lab Environment

To carry out the lab, you need:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 02 Footprinting and Reconnaissance

- Web Data Extractor, located at **D:\CEH-Tools\CEHv9 Module 02 Footprinting and Reconnaissance\Website Mirroring Tools\HTTrack Web Site Copier**. You can also download the latest version of HTTrack Web Site Copier from the link http://www.httrack.com/page/2/en index.html. If you decide to download the latest version, then **screenshots** shown in the lab might differ
- Windows Server 2012
- Administrator privileges

Lab Duration

Time: 10 Minutes

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

Overview of Web Site Mirroring

Web site mirroring creates a replica of an existing site. It 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.

Lab Tasks

TASK 1

Install and configure HTTTrack Website Copier

1. Navigate to **D:\CEH-Tools\CEHv9 Module 02 Footprinting and Reconnaissance\Website Mirroring Tools\HTTrack Web Site Copier** and double-click **httrack_x64-3.47.27.exe**.
2. 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 **View history.txt file** options and click **Finish**.
5. The **WinHTTrack Website Copier** main window appears. Click **OK** and then click **Next** to create a **New Project**.

Note: If the application doesn't launch, you can launch it manually from the **Apps** screen.

WinHTTrack arranges the original site's relative link-structure.

Quickly updates downloaded sites and **resumes** interrupted downloads (due to connection break, crash, etc.)

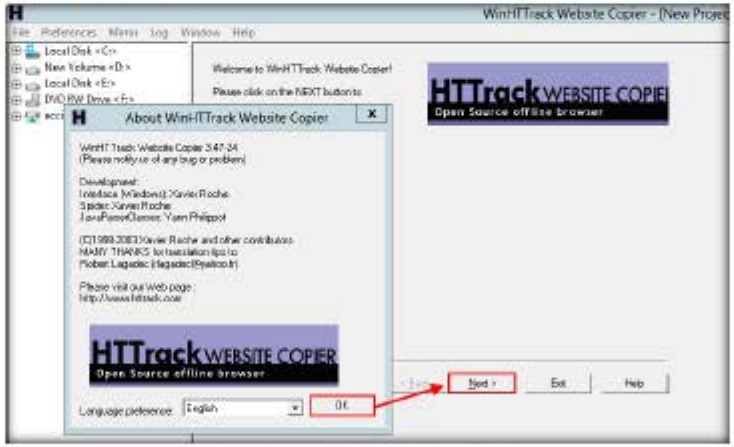
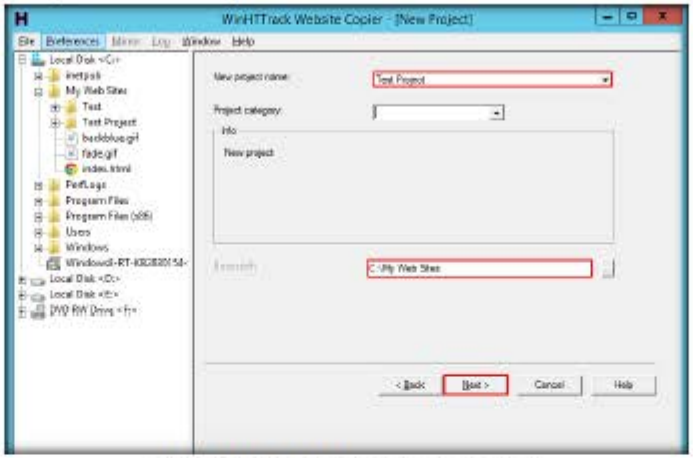


FIGURE 5.1: HTTrack Website Copier main window

6. Enter the name of the project in the **Project name** field. Select the Base path to store the copied files. Click **Next**.

Wizard to specify which links must be loaded (accept/refuse: link, all domain, all directory)



File names with original structure kept or splitted mode (one html folder, and one image folder), dos 8-3 filenames option and user-defined structure

FIGURE 5.2: HTTrack Website Copier selecting a New Project

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

Timeout and minimum transfer rate manager to abandon slowest sites

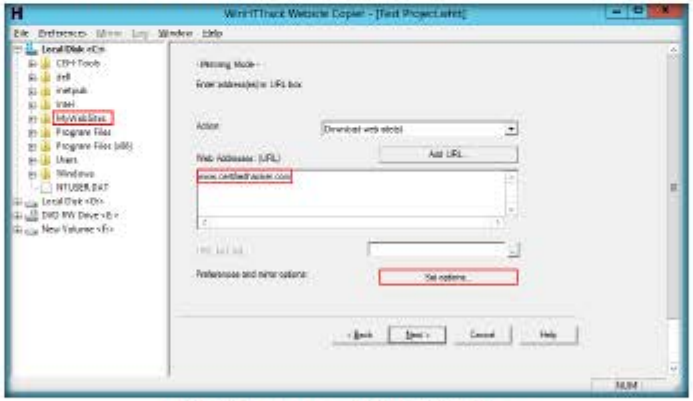


FIGURE 5.3: Setting options in HTTrack Website Copier

8. Click the **Set options** button to launch the **WinHTTrack** window.

9. Click the **Scan Rules** tab and select the check boxes for the file types as shown in the following screenshot, then click **OK**.

WinHTTrack works as a command-line program or through a shell for both private (capture) and professional (on-line web mirror) use.

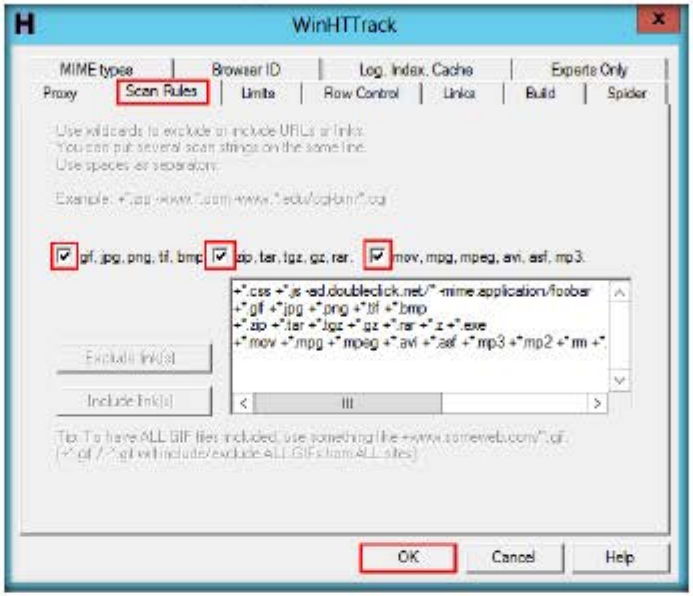
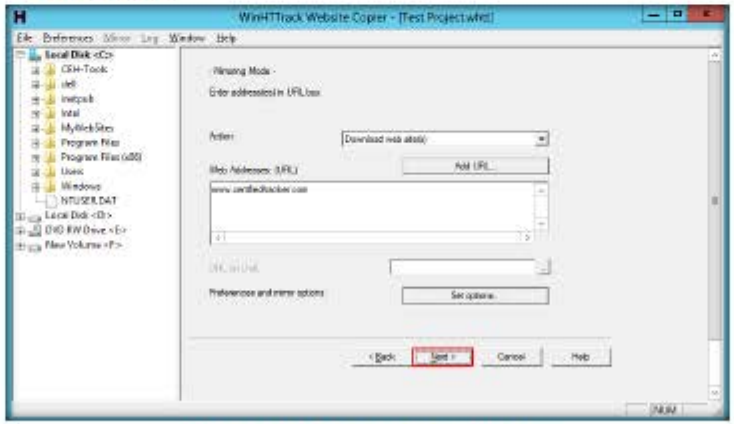


FIGURE 5.4: Scan Rules tab in HTTrack Website Copier

HTML parsing and tag analysis, including javaScript code/embedded HTML code

10. Click **Next**.



Proxy support to maximize speed, with optional authentication

FIGURE 5.5: HTTrack Website Copier Select a project window

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

The tool has integrated DNS cache and native https and ipv6 support

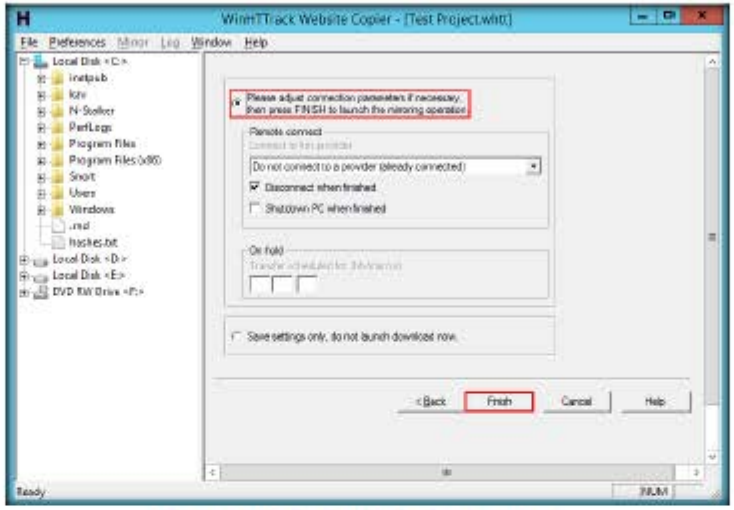


FIGURE 5.6: HTTrack Website Copier launching mirroring operation

13. Site mirroring progress will be displayed as in the following screenshot:

HTTrack can also update an existing mirrored site and resume interrupted downloads. HTTrack is fully configurable by options and by filters

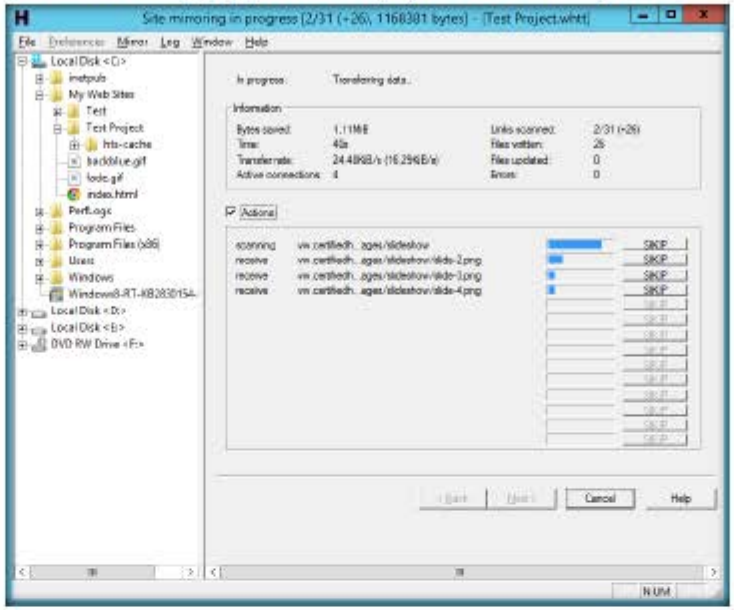


FIGURE 5.7: HTTrack Website Copier displaying site mirroring progress

14. WinHTTrack displays the message **Mirroring operation complete** once the site mirroring is completed. Click **Browse Mirrored Website**.

Filter by file type, link location, structure depth, file size, site size, accepted or refused sites or filename (with advanced wild cards).

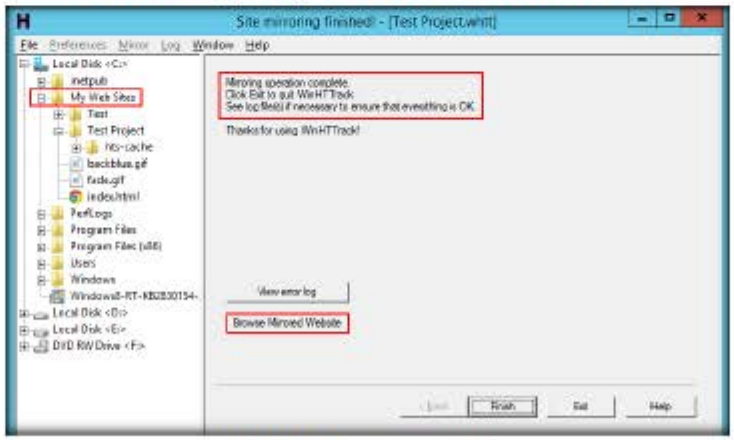


FIGURE 5.8: Browsing a mirrored website

TASK 2

Browse the Mirrored Website

15. 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.

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

Use bandwidth limits, connection limits, size limits and time limits

Optional log file with error-log and comments-log

FIGURE 5.9: HTTrack Website Copier Mirrored Website Image

Do not download too large websites: use filters, try not to download during working hours

16. Some websites are very large and it might take a long time to mirror the complete site.
17. If you wish to stop the mirroring in progress, Click **Cancel** on the Site mirroring progress window.
18. The site will work like a **live hosted website**.

Lab Analysis

Document the mirrored websites directories, getting HTML, images, and other files.

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

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

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

Lab 6

Collecting Information About a Target by Tracing Emails

Tracing emails involves analyzing the email header to discover details about the sender.

ICON KEY

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

Lab Scenario

An attacker may send malicious emails to a victim (employee) in order to carry out an attack on a target organization. As a professional ethical hacker, you should be able to trace out information about such malicious email. It involves analyzing the email headers of suspicious email to extract information such as the date that an email was received or opened, geographical information, etc.

Lab Objectives

The objective of this lab is to demonstrate email tracing using eMailTrackerPro. Students will learn how to:

- Trace an email to its true geographical source
- Collect Network (ISP) and domain Whois information for any email traced

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 02 Footprinting and Reconnaissance

Lab Environment

In the lab, you will need :

- eMailTrackerPro, which is located at **D:\CEH-Tools\CEHv9 Module 02 Footprinting and Reconnaissance\Email Tracking Tools\eMailTrackerPro**. You can also download the latest version of eMailTrackerPro from the link http://www.emailtrackerpro.com/download.html. If you decide to download the latest version, then screenshots shown in the lab might differ. This tool installs Java runtime.
- Windows Server 2012
- Administrator privileges

- A valid email account (Hotmail, Gmail, yahoo, etc.). We suggest you to sign up with any of these services to obtain a new email account for this lab. *Do not* use your real email account and password in this exercise.

Lab Duration

Time: 5 Minutes

eMailTrackerPro helps identify the true source of emails to help track suspects, verify the sender of a message, trace and report email abusers.

Overview of Email Tracing/Tracking

E-mail tracking is a method to monitor or spy on email delivered to the intended recipient. It reveals information such as:

- When an email message was received and read
- If a destructive email was sent
- The GPS coordinates and map location of the recipient
- 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

Install eMailTrackerPro

1. Navigate to **D:\CEH-Tools\CEHv9 Module 02 Footprinting and Reconnaissance\Email Tracking Tools\eMailTrackerPro** and double-click **emt.exe**.
2. If the **Open File - Security Policy** pop-up appears, click **Run**.
3. Follow the wizard steps (by selecting default options) to install eMailTrackerPro.
4. In the last step of installation, uncheck Show Readme option and click **Finish**.
5. Launch the **eMailTrackerPro** application from the **Apps** screen.

6. The main window of eMailTrackerPro appears along with the **Edition Selection** pop-up. Click **OK**.

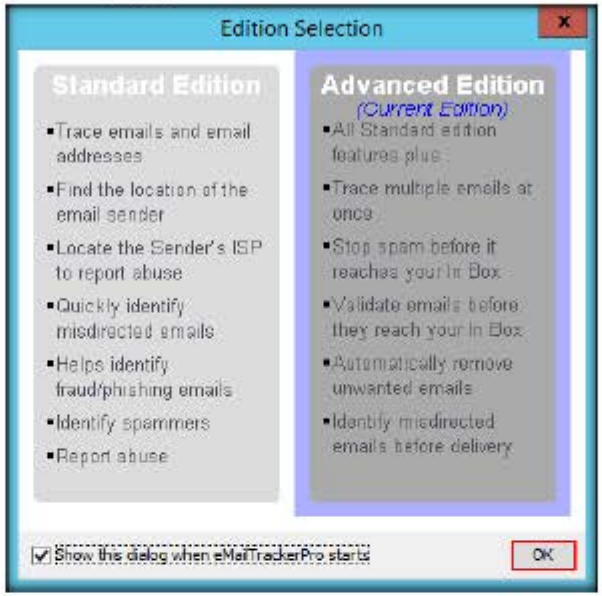


FIGURE 6.1: eMailTrackerPro edition Selection pop-up window

eMailTrackerPro Advanced Edition includes an online mail checker which allows you to view all your emails on the server before delivery to your computer.

7. The **eMailTrackerPro** main window appears as shown in the following screenshot:

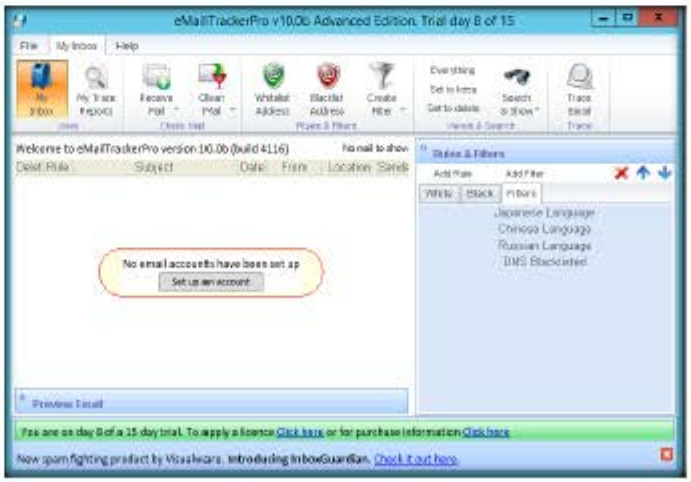


FIGURE 6.2: eMailTrackerPro main window

This tool also uncovers common SPAM tactics.

TASK 2

Trace Email headers

8. Click **My Trace Reports**.

FIGURE 6.3: The eMailTrackerPro Main window

9. Click **Trace Headers** to start the trace.
10. Select **Trace an email I have received**. Copy the email header from the email you wish to trace and paste it in the **Email headers** field under **Enter Details**.

The filter system in eMailTrackerPro allows you to create custom filters to match your incoming mail.

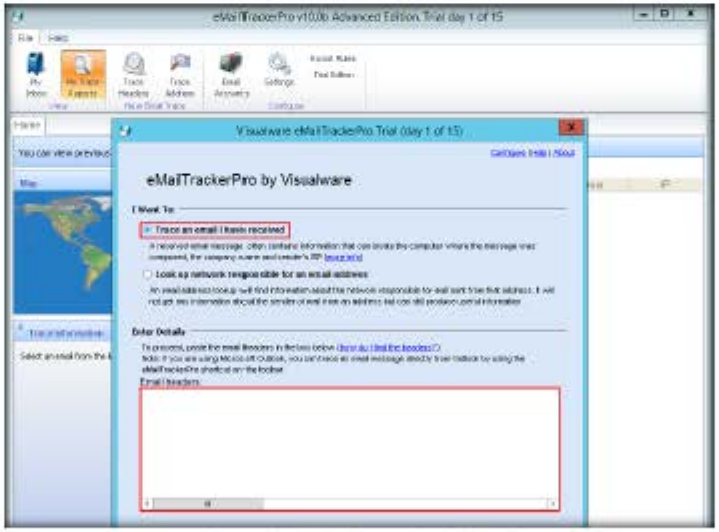


FIGURE 6.4: The eMailTrackerPro entering details window

TASK 3

Finding Email Header

11. Log in to an email account and open the message you'd like to view headers for.
12. Click the down arrow next to **Reply**, at the top of the message pane.
13. Select **Show Original** from the drop-down list.

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

- Double-click the email to open it in a new window.
- Click the small arrow in the lower right corner of the **Tags** toolbar box to open **Message Options** information box.
- Under **Internet headers**, you will find the **Email header**.

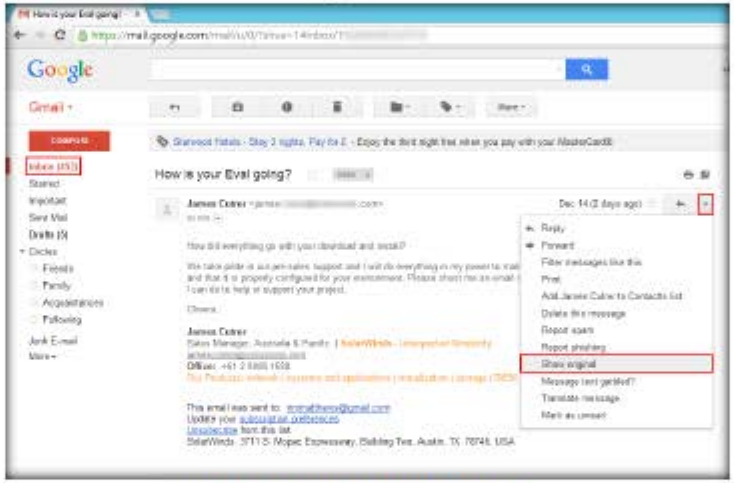


FIGURE 6.5: Finding Email Header in Outlook 2010

The abuse report option from the **My Trace Reports** window automatically launches a browser window with the abuse report included.

14. The header appears in a new tab as shown in the following screenshot:

FIGURE 6.6: header appearing tab in browser

✉ Each email message includes an Internet header with valuable information, eMailTrackerPro analyzes the message header and reports the IP address of the computer where the message originated, its estimated location, the individual or organization the IP address is registered to, the network provider, and additional information as available

15. Copy the entire text and paste it in the **Email headers** field, and click **Trace**.

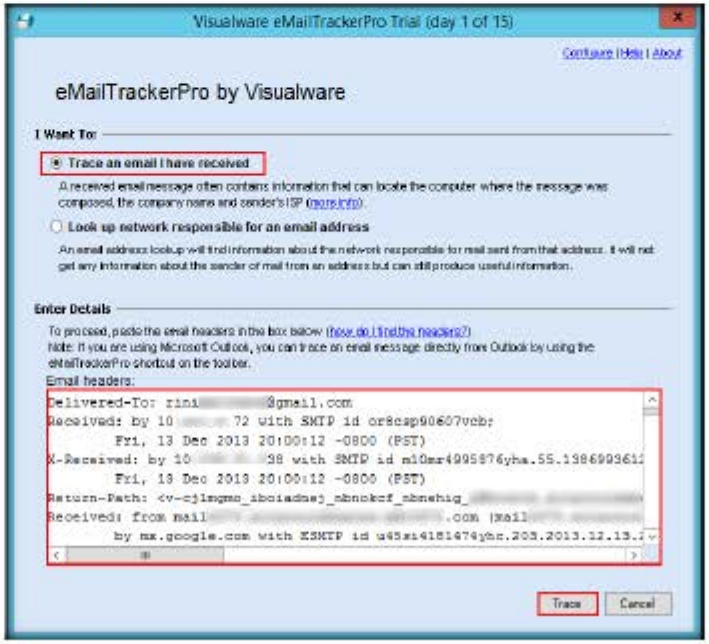


FIGURE 6.7: Email headers and Tracing emails

emailTrackerPro can detect abnormalities in the email header and warn you that the email may be spam

16. The **My Trace Reports** window opens.
17. The email location is traced in a GUI world map. The location and IP addresses may vary. You can also view the summary by selecting **Email Summary** on the right side of the window.
18. The **Table** section right below the Map shows the entire hop in the route, with the **IP** and suspected locations for each hop.

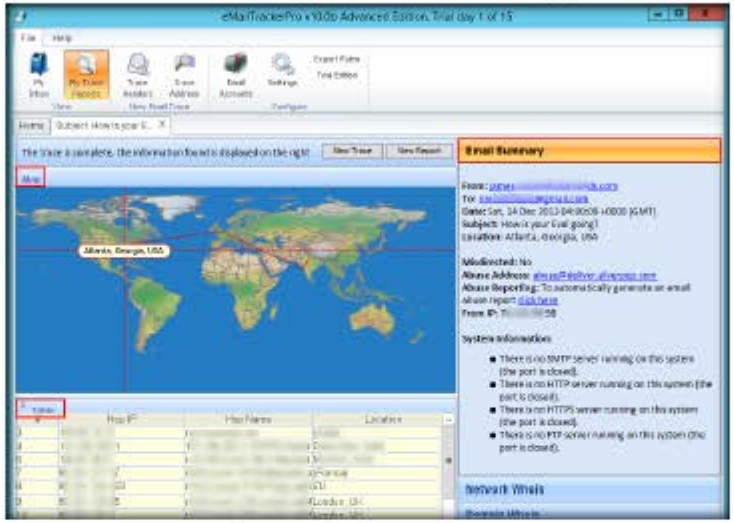


FIGURE 6.8: eMailTrackerPro – Email Trace Report

TASK 4

Examine the Report

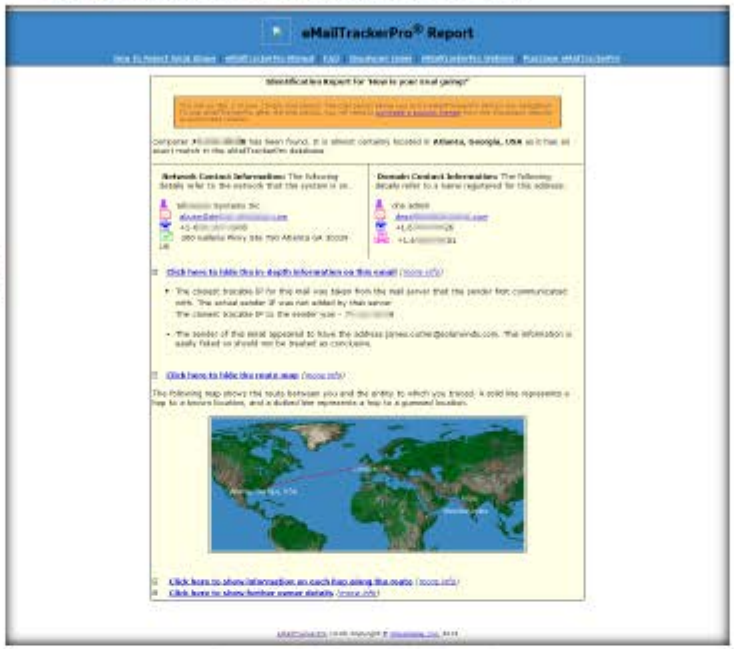
19. Click **View Report** to view the complete trace report.

FIGURE 6.9: The eMailTrackerPro - My Trace Reports tab

20. The complete report appears in the default browser.

HaCkRhInO-TeaM !

21. Expand each section to view detailed information.



Tracking an email is useful for identifying the company and network providing service for the address.

FIGURE 6.10: eMailTrackerPro – detailed information Report

Lab Analysis

Document all the live emails discovered during the lab with all additional information.

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

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

Lab 7

Gathering IP and Domain Name Information Using Whois Lookup

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 information gathering process, you will be asked to perform WHOIS foot printing on the target domain name or IP addresses. It involves gathering information on the target IP and domain obtained during previous information gathering steps. As a professional ethical hacker or pen tester, you should be able to perform WHOIS foot printing on the target. With this kind of footprinting, you can extract information such as the IP addresses or host names of the company's DNS servers and contact information usually containing the address and phone number.

Lab Objectives

The objective of this lab is to help students analyze domain and IP address queries. This lab helps you to get information including hostname, IP address, and domain.

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 02 Footprinting and Reconnaissance

In the lab you need:

- A computer running any version of Windows with Internet access
- Administrator privileges to run SmartWhois
- The **SmartWhois** tool, available in **D:\CEH-Tools\CEHv9 Module 02 Footprinting and Reconnaissance\WHOIS Lookup Tools\SmartWhois** or downloadable from http://www.tamos.com. If you decide to download the latest version, then screenshots shown in the lab might differ.

Lab Duration

http://www.tamos.com

Time: 5 Minutes

Overview of Whois Lookup

The WHOIS database is a searchable list of every domain currently registered. Whois Lookup reveals who owns a particular domain name.

Lab Tasks

TASK 1

Lookup IP

1. Navigate to **D:\CEH-Tools\CEHv9 Module 02 Footprinting and Reconnaissance\WHOIS Lookup Tools\SmartWhois** and double-click **setup.exe**.
2. If the **Open File - Security Warning** pop-up appears, click **Run**.
3. The **Welcome** wizard; click **Next**.
4. Follow the wizard steps (by choosing default options) to install SmartWhois.
5. In the **Optional Components** window, uncheck all options and click **Next**.
6. The **SmartWhois Setup** dialog box appears. Click **Yes**.
7. Launch **SmartWhois** from the **Apps** screen.
8. The **SmartWhois** application updates pop-up appears. Click **No**.

SmartWhois can save obtained information to an archive file. Users can load this archive the next time the program is launched and add more information to it. This feature allows you to build and maintain your own database of IP addresses and host names.

SmartWhois can be configured to work from behind a firewall by using HTTP/HTTPS proxy servers. Different SOCKS versions are also supported.

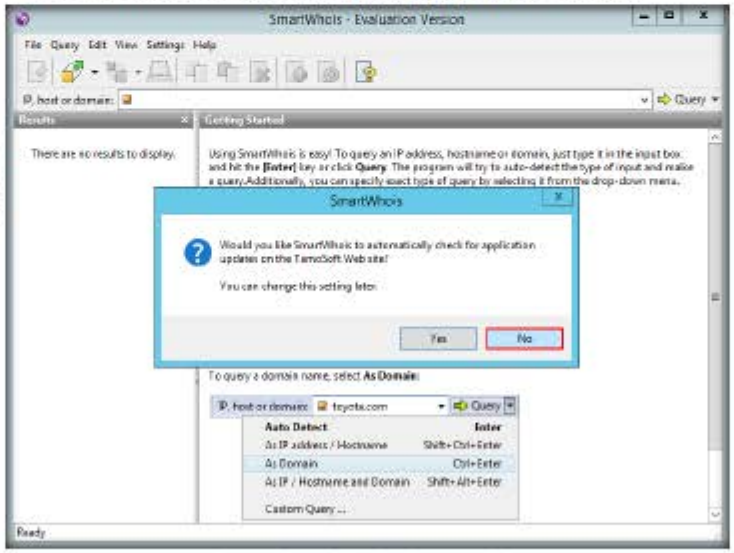


FIGURE 7.1: SmartWhois main settings pop-up windows

TASK 2

Perform Domain Lookup

9. The **SmartWhois** main window appears. Type an IP address, hostname, or domain name in the **IP, host or domain** text field. An example of a Domain name query is shown below for www.google.com.

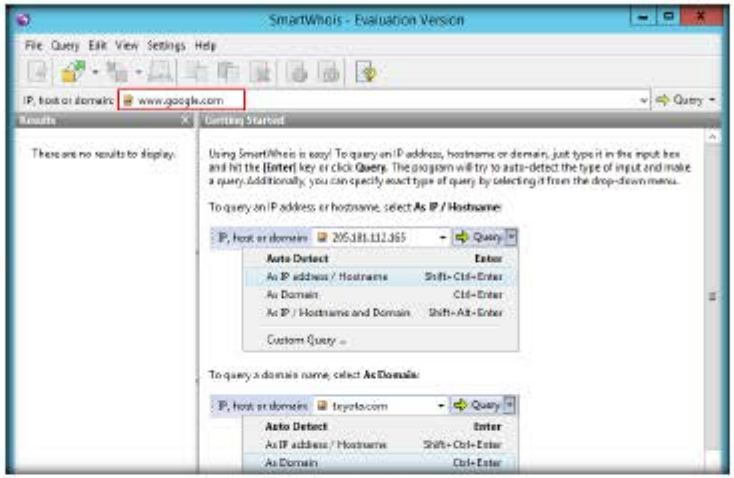


FIGURE 7.2: A SmartWhois domain search

If you need to query a non-default whois server or make a special query click View → Whois Console from the menu or click the Query button and select Custom Query.

10. Click the **Query** drop-down list and select **As Domain**.

Note: To query an **IP address** or **hostname**, select **As IP / Hostname.** To query a **domain** name, select **As Domain**.

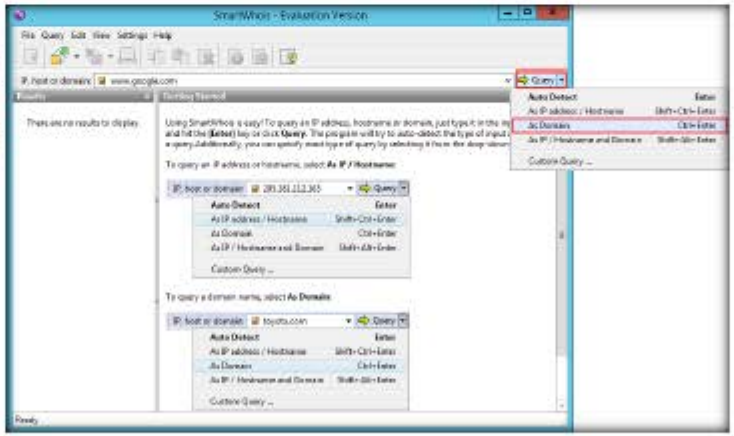


FIGURE 7.3: The SmartWhois – Selecting Query type

SmartWhois is capable of caching query results, which reduces the time needed to query an address; if the information is in the cache file it is immediately displayed and no connections to the whois servers are required.

11. The domain displays in the left pane and the result of the query displays in the right pane, as shown in the following screenshot:

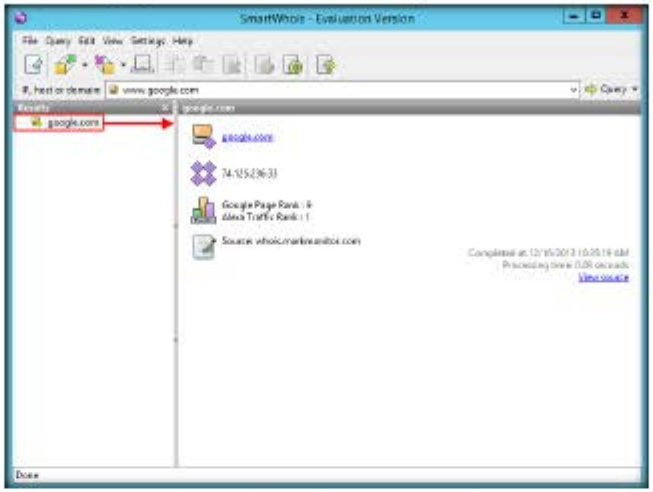


FIGURE 7.4: The SmartWhois – Domain query result

SmartWhois can process lists of IP addresses, hostnames, or domain names saved as plain text (ASCII) or Unicode files. The valid format for such batch files is simple. Each line must begin with an IP address, hostname, or domain. If you want to process domain names, they must be located in a separate file from IP addresses and hostnames.

Note: The IP address displayed in the result may vary in your lab environment.

12. Click the **Clear** icon in the toolbar to clear the history.

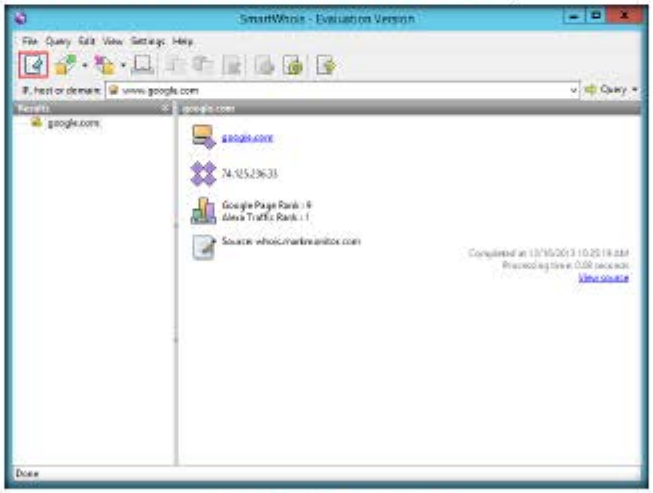


FIGURE 7.5: A SmartWhois toolbar

HaCkRhInO-TeaM !

TASK 3

Perform IP/Hostname Lookup

13. To perform a sample **host name query**, type www.facebook.com in the **IP, host or domain** text field.
14. Click the **Query** drop-down list and choose **As IP address/ Hostname**.

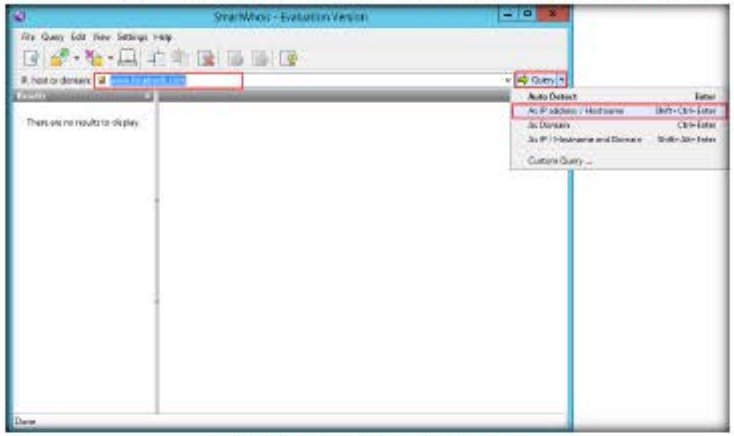


FIGURE 7.6: A SmartWhois host name query

15. In the left pane, the resultant query displays, and the right pane displays the results of your query, as shown in the following screenshot:

Note: This result may vary in your lab environment.

If you want to query a domain registration database, enter a domain name and hit the Enter key while holding the Ctrl key, or just select As Domain from the Query dropdown menu.

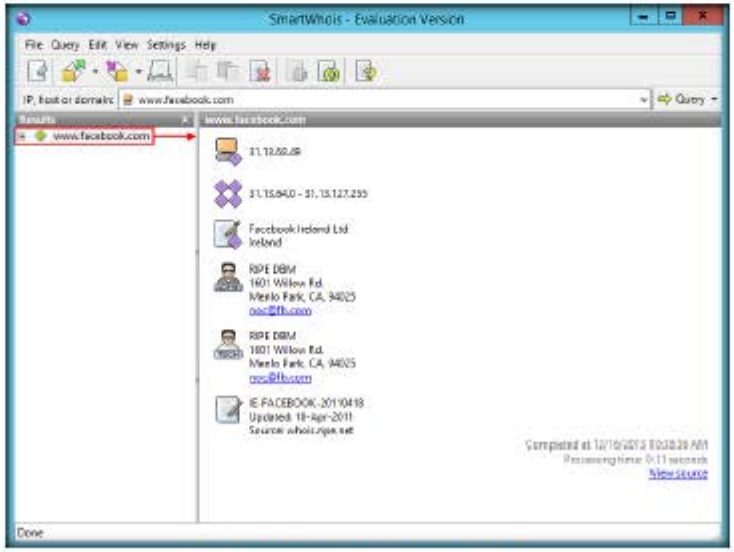


FIGURE 7.7: A SmartWhois host name query result

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

16. Click the **Clear** icon in the toolbar to clear the history.

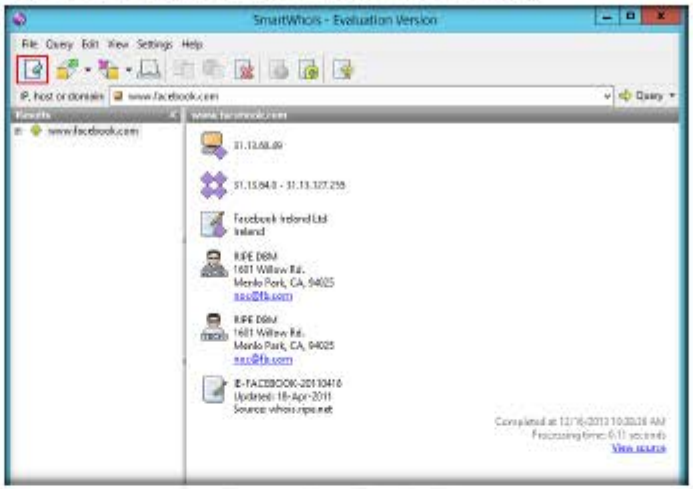


FIGURE 7.8: A SmartWhois clearing history

If you're saving results as a text file, you can specify the data fields to be saved. For example, you can exclude name servers or billing contacts from the output file. Click Settings→Options→Text & XML to configure the options.

17. To perform a sample IP Address query, enter the IP address of the **Windows 8.1** virtual machine, i.e., **10.0.0.10** in the **IP** field and click **Query**.

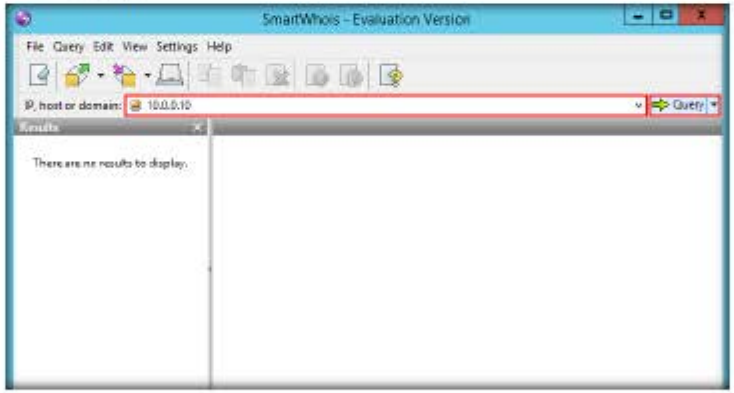


FIGURE 7.9: A SmartWhois IP address query

SmartWhois supports command line parameters specifying IP address/hostname/domain, as well as files to be opened/saved.

Note: 10.0.0.10 is the IP address of **Windows 8.1** virtual machine. The IP address of this machine may differ in your lab environment.

HaCkRhInO-TeaM !

18. The IP address displays in the left pane and the result of your query displays in the right pane, as shown in the following screenshot:

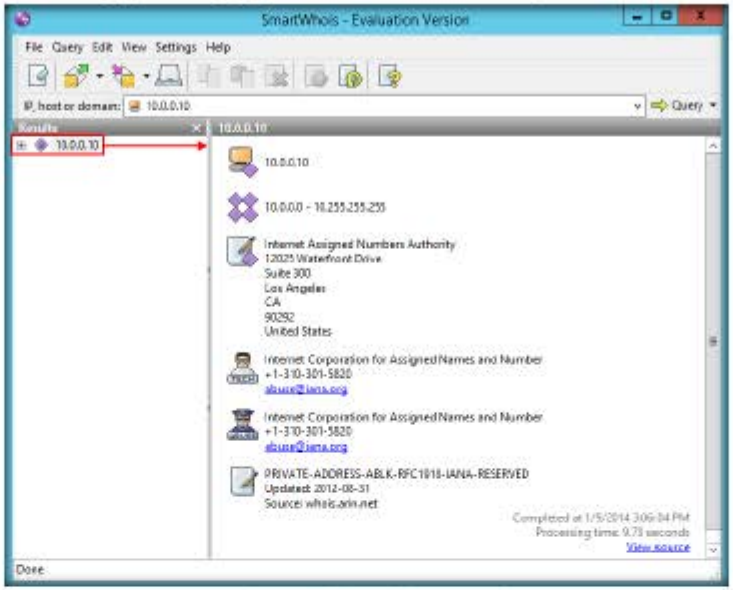


FIGURE 7.10: The SmartWhois IP query result

Lab Analysis

Document all the IP addresses/Hostnames for the Lab for further information.

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

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

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

Lab 8

Advanced Network Route Tracing Using Path Analyzer Pro

Path Analyzer Pro delivers advanced network route tracing with performance tests, DNS, whois, and network resolution to investigate network issues.

ICON KEY

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

Lab Scenario

With the IP address, hostname, and domain obtained in the previous information gathering steps, your next task will be to trace the route of the target network in order to detect the trusted routers, firewall, and network topology used in the network. This lab will demonstrate how to perform route tracing on the target network.

Lab Objectives

The objective of this lab is to help students trace out network paths along with IP addresses of intermediate nodes.

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 02 Footprinting and Reconnaissance

In the lab, you will need:

- Path Analyzer pro, which is available at **D:\CEH-Tools\CEHv9 Module 02 Footprinting and Reconnaissance\Traceroute Tools\Path Analyzer Pro**. You can also download the latest version of Path Analyzer Pro from the link http://www.pathanalyzer.com/download.opp. If you decide to download the latest version, then **screenshots** shown in the lab might differ
- Windows Server 2012
- Administrator privileges

Lab Duration

Time: 5 Minutes

Overview of Network Route Tracing

Network route tracing can determine the intermediate nodes traversed towards the destination and can detect the complete route (path) from source to destination.

Lab Tasks

TASK 1

Install Path Analyzer Pro

1. Navigate to **D:\CEH-Tools\CEHv9 Module 02 Footprinting and Reconnaissance\Traceroute Tools\Path Analyzer Pro** and double-click **PAPro27.msi**.
2. If the **Open File - Security Warning** pop-up appears, click **Run**.
3. Follow the wizard steps (by selecting default options) to install Path Analyzer Pro.
4. Launch **Path Analyzer Pro** from the **Apps** screen.

FIGURE 8.1: Installed apps in windows Server 2012 - Selecting Path Analyzer Pro 2.7

Path Analyzer Pro summarizes a given trace within seconds by generating a simple report with all the important information on the target--we call this the Synopsis.

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

5. The Path Analyzer Pro window appears along with a **Registration Form** pop-up. Click **Evaluate** in the pop-up.

Path Analyzer Pro summarizes all the relevant background information on its target, be it an IP address, a hostname, or an email address.

FIGURE 8.2: Path Analyzer Pro 2.7 Registration Form window

6. The Main window of **Path Analyzer Pro** appears as shown in the screenshot
7. In the **Standard Options** and **Advanced Probe Details** sections, a few options are set to default.
8. Ensure that the **ICMP** radio button under the **Protocol** field is selected.
9. In the **Advanced Probe Details** section, ensure that the **Smart** option is checked under the **Length of packet** field.

Note: If you have a firewall it must be disabled for appropriate output.

TASK 2

Trace a Target Network

FIN Packets Only- generates only TCP packets with the FIN flag set in order to solicit an RST or TCP reset packet as a response from the target. This option may get beyond a firewall at the target, thus giving the user more trace data, but it could be misconstrued as a malicious attack.

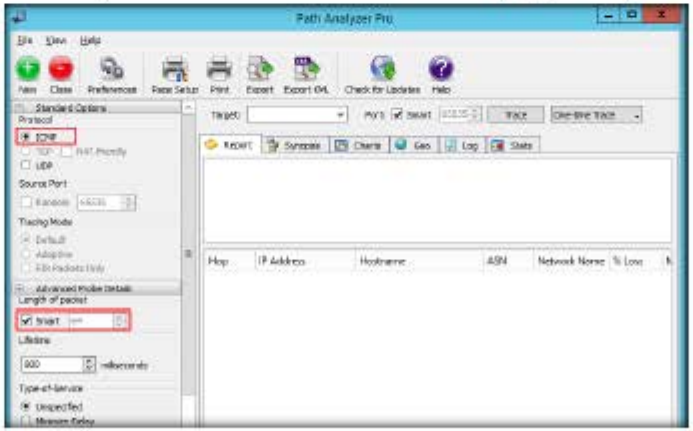


FIGURE 8.3: The Path Analyzer Pro Advanced Probe Details window

10. In the **Advanced Tracing Details** section, a few options are set to default.
11. Ensure that the **Stop on control messages (ICMP)** option is checked in the **Advanced Tracing Details** section.

Note: Path Analyzer Pro is not designed to be used as an attack tool.

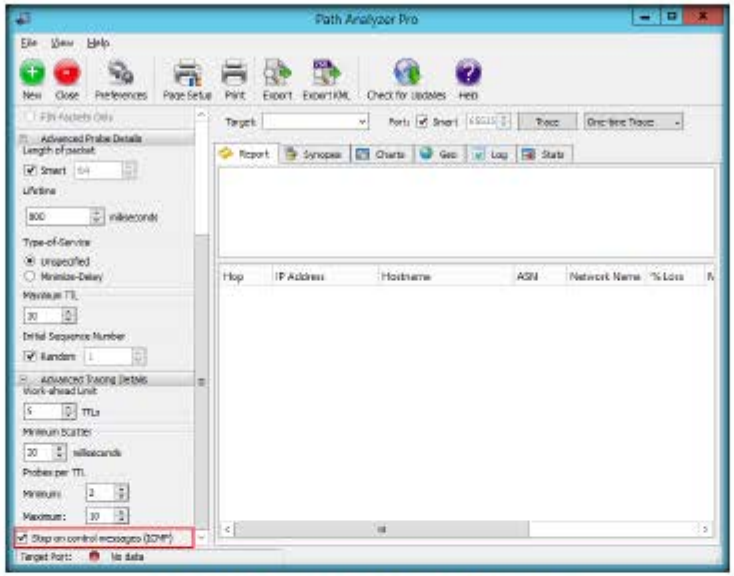


FIGURE 8.4: The Path Analyzer Pro Advanced Tracing Details window

12. To perform the trace, enter the host name in the Target field (for instance www.google.com), and check **Smart** under the **Port** field as default (**65535**).
13. From the drop-down menu, choose **Timed Trace** and click **Trace**.

Traceroute is a system administration utility to trace the route IP packets take from a source system to some destination system.

FIGURE 8.5: A Path Analyzer Pro Advance Tracing Details option

14. The **Type time of trace** dialog box appears. Specify the time of trace in HH: MM: SS format and click **Accept**.

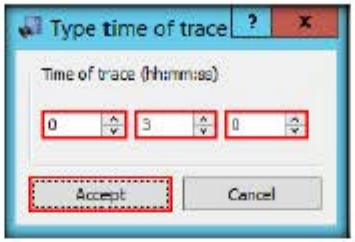


FIGURE 8.6: The Path Analyzer Pro Type time of trace option

The Advanced Probe Details settings determine how probes are generated to perform the trace. These include the Length of packet, Lifetime, Type of Service, Maximum TTL, and Initial Sequence Number.

15. While Path Analyzer Pro performs this trace, the **Trace** tab changes automatically to **Stop**.

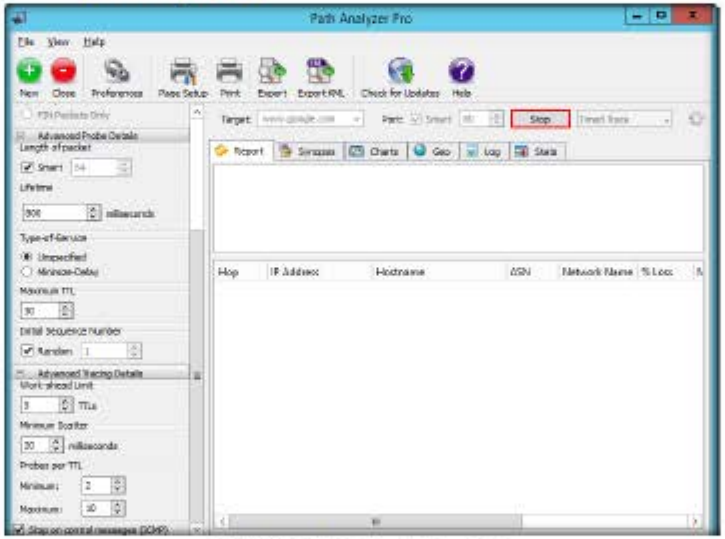


FIGURE 8.7: A Path Analyzer Pro Target Option

TASK 3

Examine the Results

16. The trace results display under the **Report** tab in the form of a linear **chart depicting** the number of hops between you and the target.

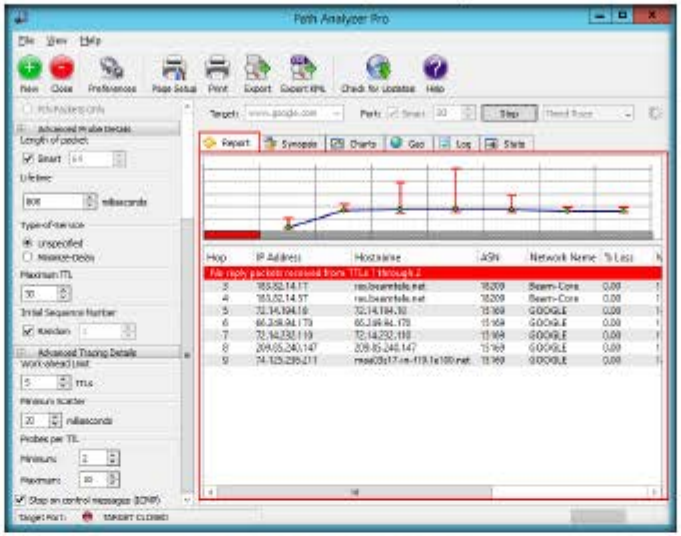


FIGURE 8.8: A Path Analyzer Pro Target option

17. Click the **Synopsis** tab, which displays a one-page summary of trace results.

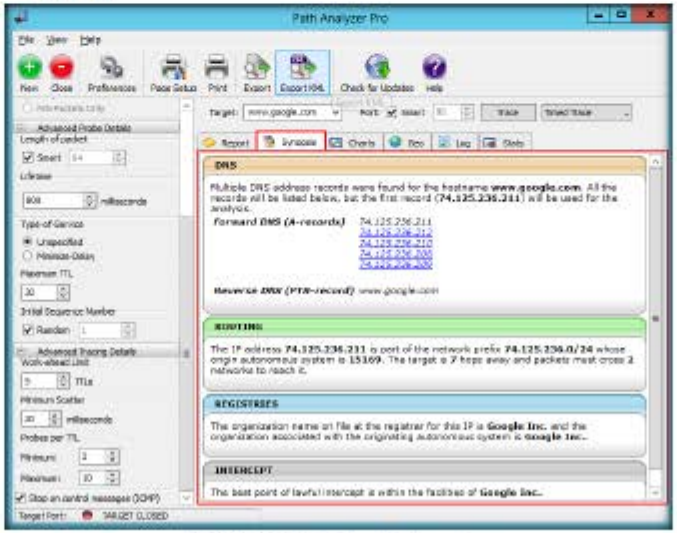


FIGURE 8.9: A Path Analyzer Pro Target option

Length of packet: This option allows you to set the length of the packet for a trace. The minimum size of a packet, as a general rule, is approximately 64 bytes, depending on the protocol used. The maximum size of a packet depends on the physical network but is generally 1500 bytes for a regular Ethernet network or 9000 bytes using Gigabit Ethernet networking with jumbo frames.

TASK 4

View Charts

18. Click the **Charts** tab to view the results of the trace.

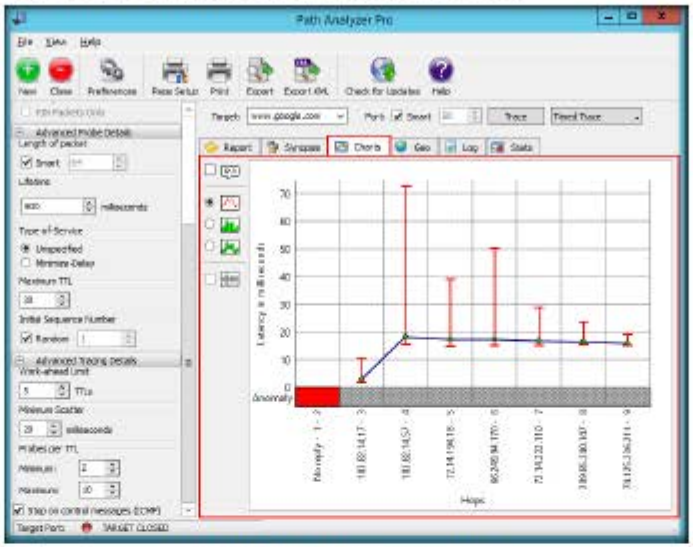


FIGURE 8.10: The Path Analyzer Pro Chart Window

TASK 5

Inspect the Geographical Location

19. Click **Geo**, which displays a world map of the trace route.

FIGURE 8.11: The Path Analyzer Pro chart window

Path Analyzer Pro uses Smart as the default Length of packet. When the Smart option is checked, the software automatically selects the minimum size of packets based on the protocol selected under Standard Options.

TASK 6

Examine the Logs

20. Click the **Log** tab to view the **Current Trace Log** and **Session Log**.

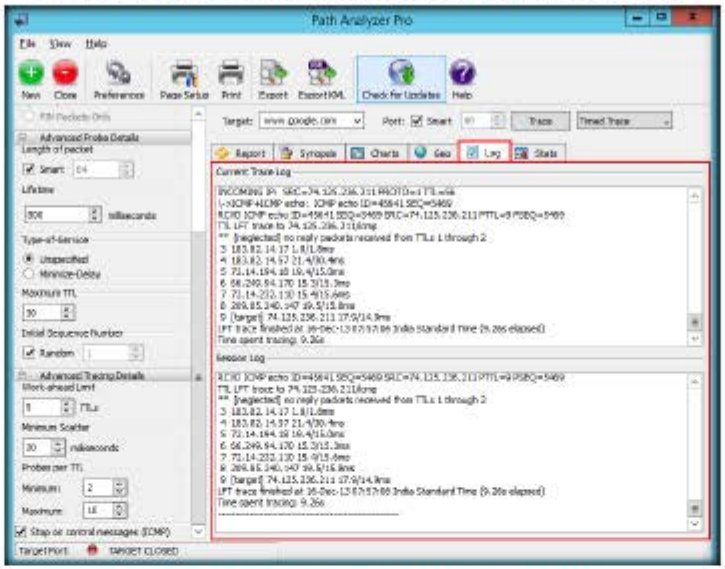


FIGURE 8.12: The Path Analyzer Pro Current trace Log and Session Log window

TASK 7

Observe the Statistics

21. Click the **Stats** tab, which features the **Vital Statistics** of the current trace.

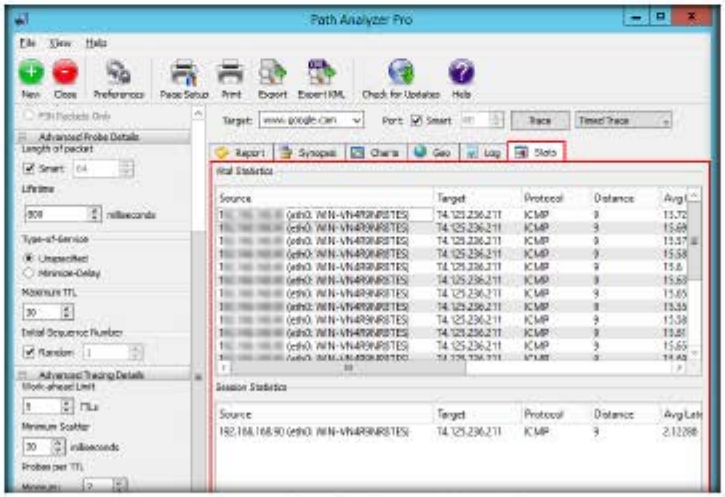


FIGURE 8.13: The Path Analyzer Pro Statistics window

Maximum TTL: The maximum Time to Live (TTL) is the maximum number of hops to probe in an attempt to reach the target. The default number of hops is set to 30. The Maximum TTL that can be used is 255.

TASK 8

Export Results

22. Click **Export** in the toolbar to export the report.

FIGURE 8.14: The Path Analyzer Pro Save Report As window

23. By default, the Report will be saved at **C:\Program Files (x86)\Path Analyzer Pro 2.7**. However, you may change it to a preferred location.
24. Specify the name of the file in **File name** field and click **Save**.

The Initial Sequence Number is set as a counting mechanism within the packet between the source and the target. It is set to Random as the default, but you can choose another starting number by unchecking the Random button and filling in another number. Please Note: The Initial Sequence Number applies only to TCP connections.

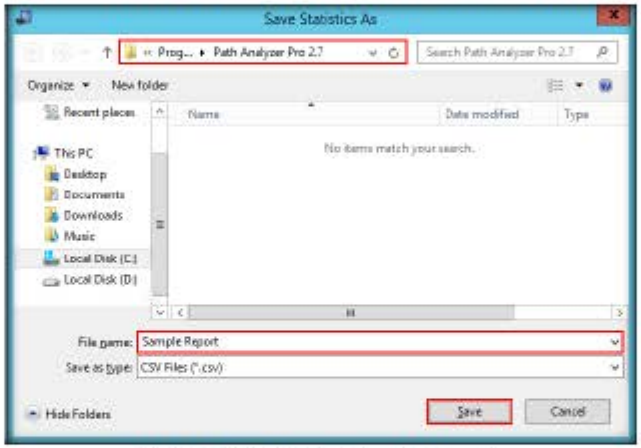


FIGURE 8.15: The Path Analyzer Pro Save Report As window

Lab Analysis

Document the IP addresses that are traced for the lab for further information.

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

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

Lab 9

Footprinting a Target Using Maltego

Maltego is an open source intelligence and forensics application. It gathers information about a target and represents this information in an easily-understandable format.

ICON KEY

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

Lab Scenario

The information gathered in the previous steps might not be sufficient to reveal potential vulnerabilities of the target. There could be more information available that could help in finding loopholes in the target. As an ethical hacker, you should look for as much information as possible about the target. This lab will demonstrate what other information you can extract from the target.

Lab Objectives

The objective of this lab is to help students gather as much information as possible about the target. With this lab student can:

- Identify the Server Side Technology
- Identify the Domain
- Identify the Domain Name Schema
- Identify the Service Oriented Architecture (SOA) Information
- Identify the Mail Exchanger
- Identify the Name Server
- Identify the IP Address
- Identify the Geographical Location
- Identify the Entities
- Find out the Email Addresses
- Find out the Phone Numbers

Lab Environment

In this lab, you will need:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 02 Footprinting and Reconnaissance

- Maltego, which can be found at **D:\CEH-Tools\CEHv9 Module 02 Footprinting and Reconnaissance\Footprinting Tools\Maltego**. You can also download the latest version of **Maltego** from the link https://www.paterva.com/web6/products/download2.php. If you download the latest version, then screenshots shown in the lab might differ. This tool installs Java runtime.
- **Windows Server 2012**
- Administrator privileges
- A valid email account (Hotmail, Gmail, yahoo, etc.). We suggest you sign up with any of these services to obtain a new email account for this lab. Do not use your real email accounts and passwords in these exercises.

Lab Duration

Time: 15 Minutes

Overview of Maltego

Maltego is a Footprinting tool, used to gather maximum information for the purpose of ethical hacking, and forensic and pen testing. It provides a library of transforms for discovery of data from open sources, and visualizing that information in a graph format, suitable for link analysis and data mining.

Lab Tasks

TASK 1

Obtain the Target's Website URL

1. Launch a web browser, type the URL (www.google.com) in the address bar, and press **Enter**.

FIGURE 9.1: Google Webpage

2. Type the target in the Search field and press **Enter**. The URL of the target displays as shown in the following screenshot:

Maltego takes various bits of information (referred to as Entities within the application), and converts these (via code known as transforms) to other Entities.

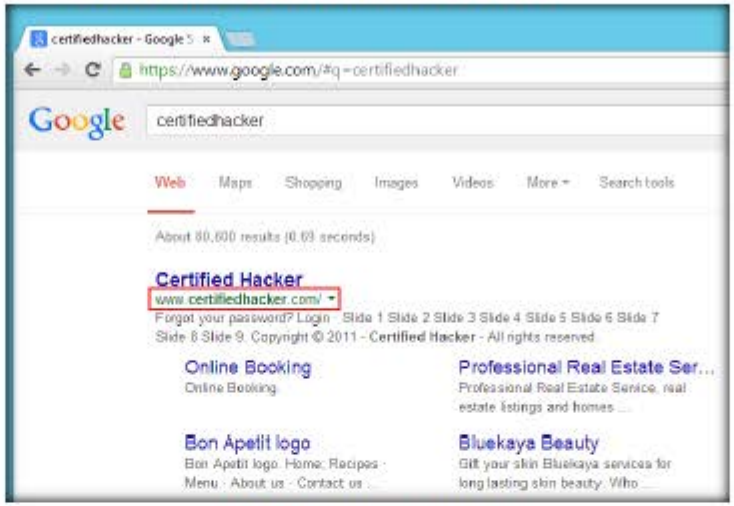


FIGURE 9.2: Google's Search Engine Result Page

TASK 2

Configure Maltego

3. Note down the URL and close the web browser. Launch **Maltego** from the **Apps** screen of **Windows Server 2012**.
4. A **Welcome** wizard appears on the Maltego GUI. Click **Next**.

Maltego provides you with a graphical interface that makes seeing these relationships, instant and accurate and even making it possible to see hidden connections.

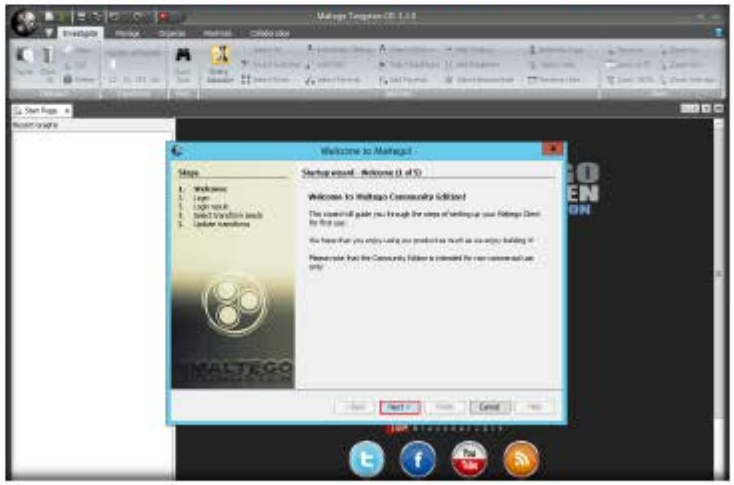


FIGURE 9.3: Maltego Welcome wizard

5. You will be redirected to the **Login** section. Click **register here**.

Using the graphical user interface (GUI) you can see relationships easily - even if they are three or four degrees of separation away.

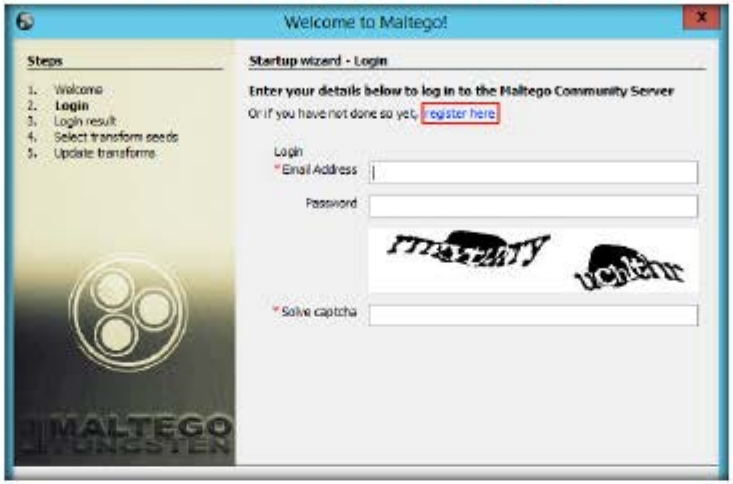


FIGURE 9.4: Maltego Login section

6. Register your account and activate it.

Maltego is unique because it uses a powerful, flexible framework that makes customizing possible, where Maltego can be adapted to your own, unique requirements.

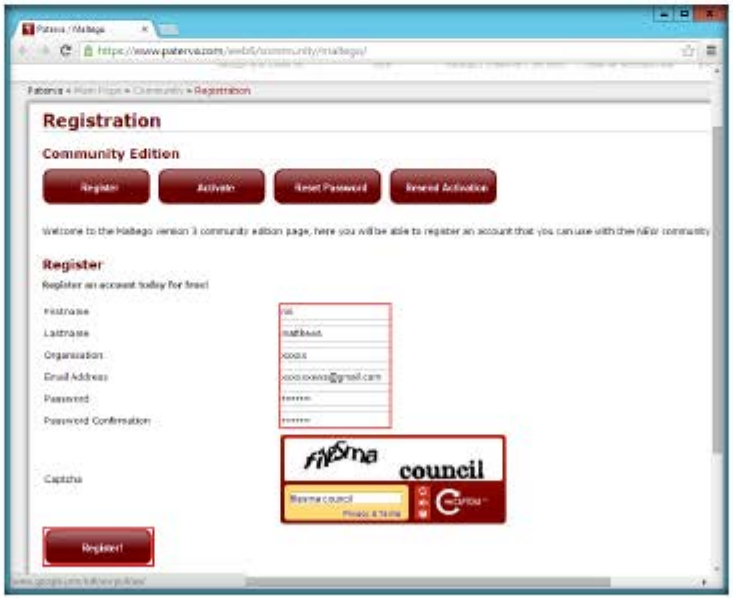


FIGURE 9.5: Registration Section

7. Go back to the setup wizard and enter the **Email Address** and **Password** specified at the time of registration, solve the **captcha,** and click **Next**.

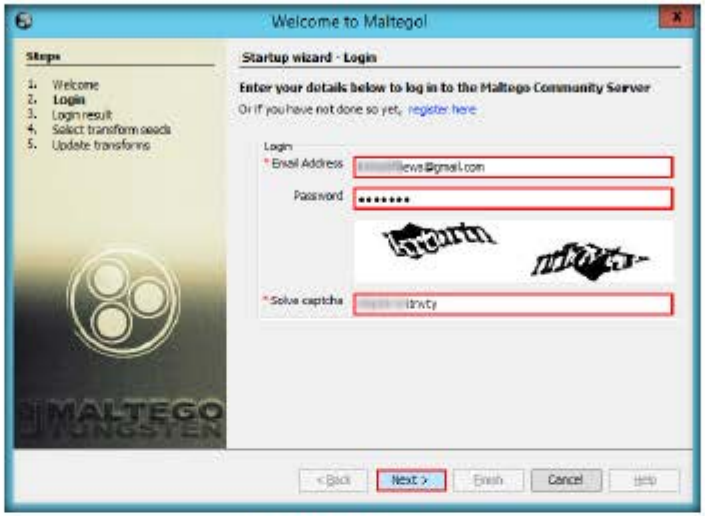


FIGURE 9.6: Maltego Login Section

The mapping of a network and understanding how everything fits together is an important step in getting to know a target. The process can be labour intensive and only some aspects can be automated successfully.

8. The Login result section displays your personal details. Click **Next**.

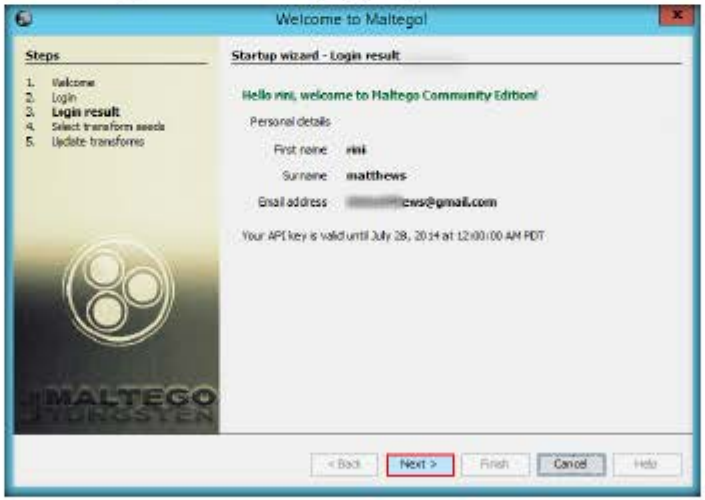


FIGURE 9.7: Maltego Login result section

Maltego tries to consolidate some of the required functions easily and accurately. Maltego provides accurate results that will also have been obtained when utilising other available tools and commands manually.

9. The **Select transform seeds** section appears. Leave the settings to default and click **Next**.

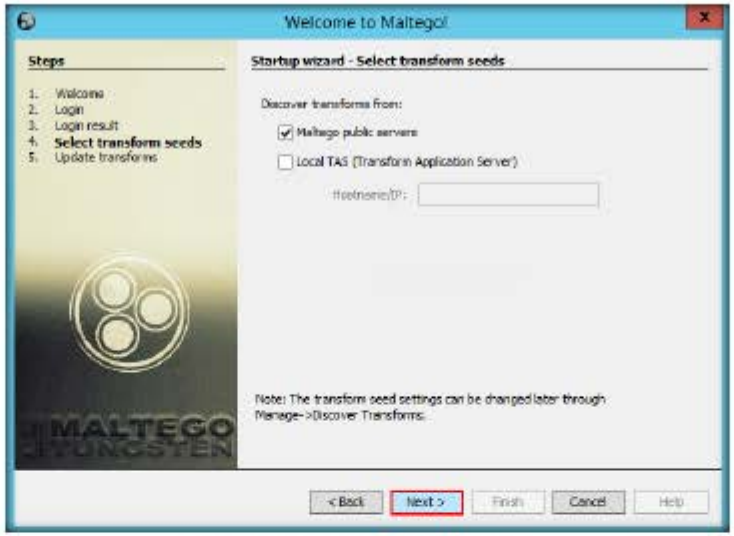


FIGURE 9.8: Maltego Select transform seeds section

10. The **Update transforms** section appears. Leave the options set to default and click **Finish**.

FIGURE 9.9: Maltego Update transforms section

Assuming a certain level of knowledge and experience, Maltego is easy to understand and utilise.

Maltego uses Java version 6 (1.6 - at least update 10) which is available for most popular operating systems. Maltego will not function correctly with version 5 (1.5). The Maltego installer will not install or upgrade your system to Java 1.6, but this should be a painless procedure.

11. The **Start a Machine** wizard appears. Click **Cancel** in order to perform footprinting manually.

Maltego loves memory and raw CPU power. Rendering views take a lot of computing power and the slower your computer, the longer it will take.

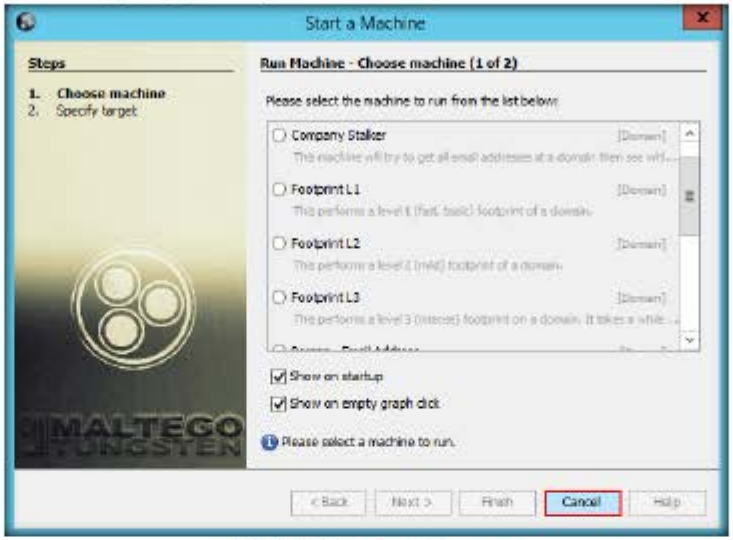


FIGURE 9.10: Maltego Start a Machine wizard

12. If a **Results limited** pop-up appears, click **OK**.

As this is a Community edition, the application displays only 12 entities of a result

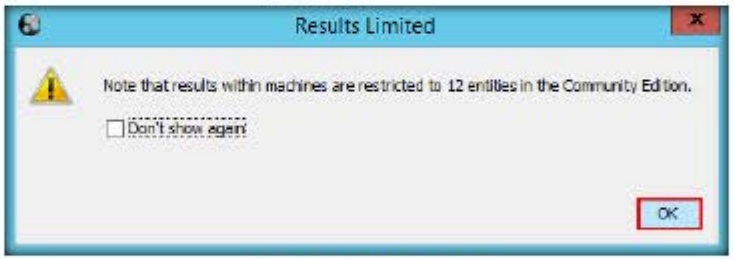


FIGURE 9.11: Results limited pop-up

13. The Maltego GUI appears as shown in the following screenshot:

If your computer is under-powered this can become frustrating. If you plan to work on large graphs you'll also need some memory.

FIGURE 9.12: Maltego GUI

TASK 3

Adding a Domain Entity

14. Click the icon located at the top-left corner of the GUI (in the toolbar) to start a new graph.

FIGURE 9.13: Maltego Toolbar

15. The **New graph (1)** window appears along with a **Palette** in the left pane. It contains a list of default built-in transforms.
16. Expand the **Infrastructure** node under **Palette**.

Maltego server is delivered as a VMWare image allowing you to run your Maltego server on practically anything that supports VMWare or a virtual machine system that can 'play' VMWare images. As such any operating system capable of running a virtual machine system can be used.

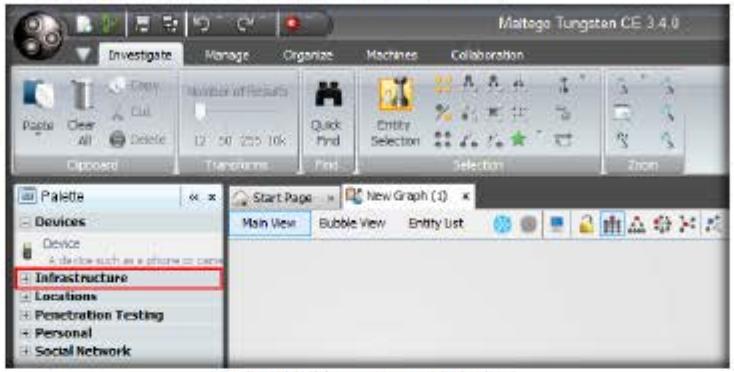


FIGURE 9.14: Maltego New graph (1) window

17. Expand the node and observe a list of entities such as AS, DNS Name, Domain, etc.
18. Drag the **Website** entity onto the **New Graph (1)** section.

Maltego requires the sun-java JDK and it is important that you install this version rather than the openjdk that comes with a lot of the operating systems.

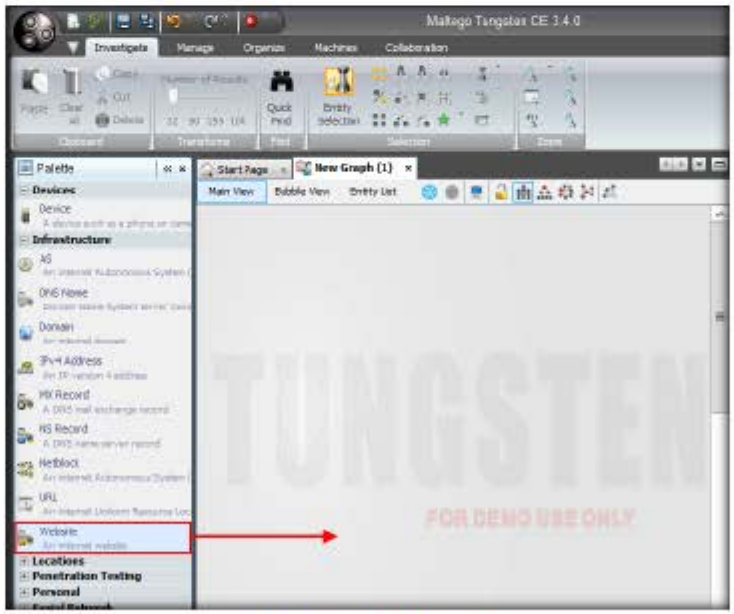


FIGURE 9.15: Selecting a Website Entity

19. The entity appears on the new graph, with the **www.paterva.com** URL selected by default.

Make 100% sure that you can read and write in the directory where you've installed the application – for instance - when you've installed the application as root and you run it under a normal user you might find that reading and writing your configuration files fails. This might cause problems.

FIGURE 9.16: Website Entity in New Graph (1) Section

20. Double-click paterva.com and rename the domain name to **www.certifiedhacker.com**. Press **Enter**.

You can create new graph at any time by clicking on this button. The keyboard shortcut for creating a new graph is Control T (new tab). Once you open your first graph it becomes available to add entities and to r change those entities to new entities.

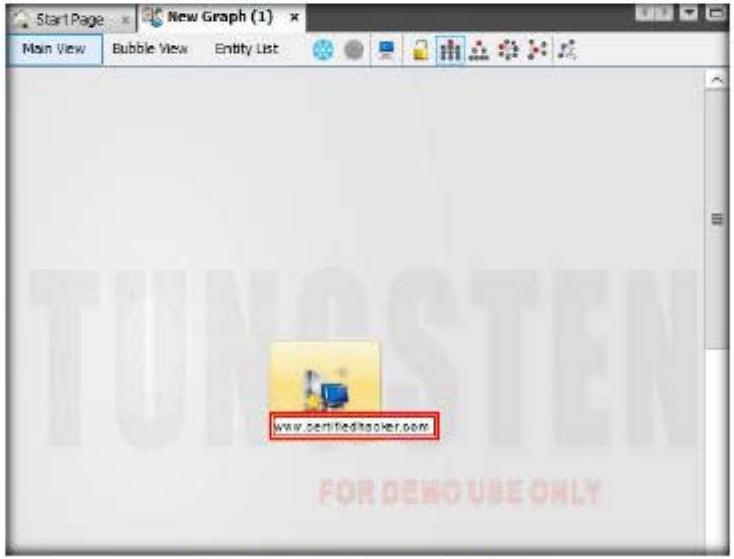


FIGURE 9.17: Website Entity in New Graph (1) Section

TASK 4

Identify the Server Side Technology

21. Right-click the entity and select **Run Transform → All Transforms → ToServerTechnologiesWebsite**.

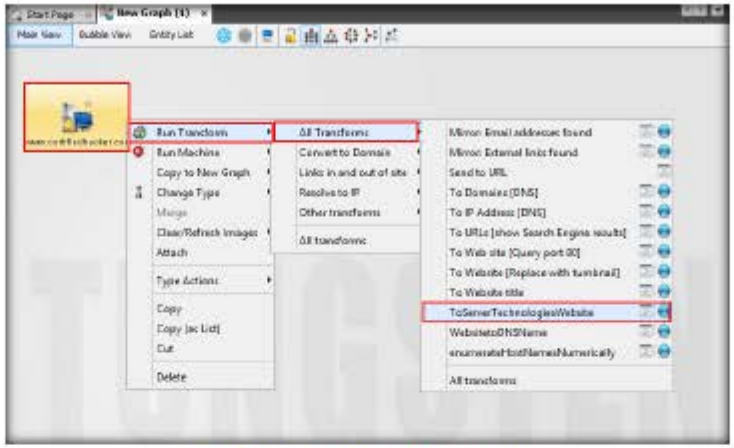


FIGURE 9.18: Selecting ToServerTechnologiesWebsite

22. The Required inputs pop-up appears. Check **I accept the above disclaimer** and **Remember these settings**. Click **Run!**

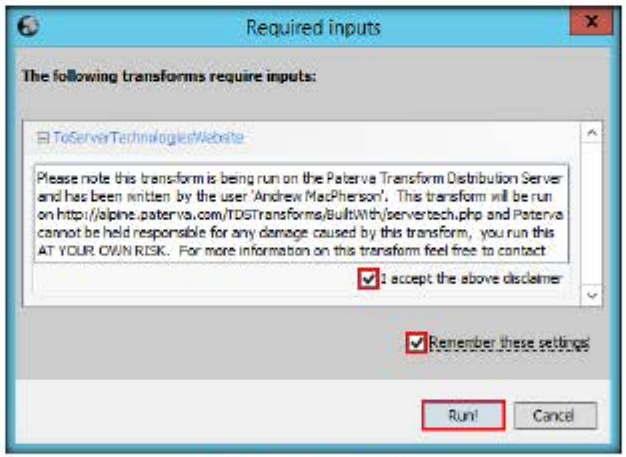


FIGURE 9.19: Required inputs pop-up

The 'add path' selection shortcut is most useful. It selects the nodes in the path between multiple is disabled unless multiple nodes are selected.

23. Maltego starts running the transform ToServerTechnologiesWebsite entity. Observe the status in the progress bar.

"Zoom to selection" was introduced in Maltego 3.0.3. This allows the user to select a portion of the graph using normal selection techniques and then quickly zoom to the area.

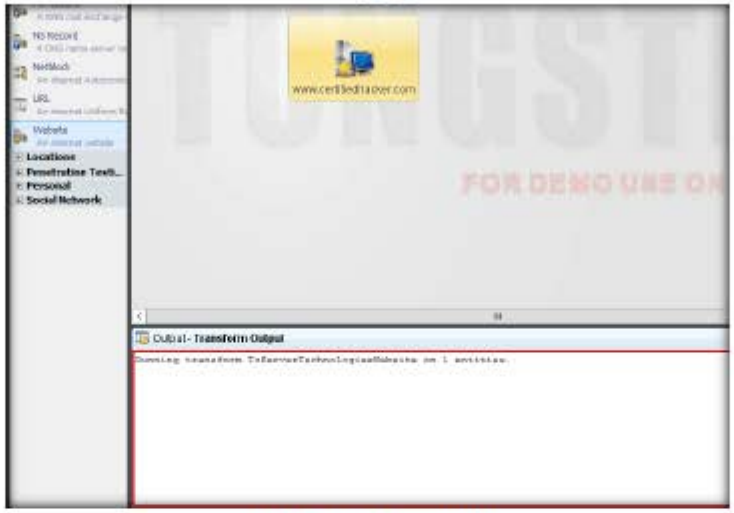


FIGURE 9.20: Required inputs pop-up

24. Once Maltego completes the Transforming Server Side Technologies, it displays the technology implemented on the server that hosts the website, as shown in the following screenshot:

Maltego can be used for the information gathering phase of all security related work. It will save you time and will allow you to work more accurately and smarter.

FIGURE 9.21: Server Side Technologies in www.certifiedhacker.com

25. After obtaining the built-in technologies of the server, attackers might search for vulnerabilities related to any of them and simulate exploitation techniques to hack them.

Hackers use this information and perform research on these technologies in order to find any vulnerabilities that could be used to exploit them.

26. To start a new transform, select all the entities by pressing **Ctrl+A** on the keyboard and press **Delete**.
27. A **Delete** pop-up appears. Click **Yes**.

FIGURE 9.22: Delete pop-up

28. Follow steps **18-20** to create a website entity with the URL www.certifiedhacker.com.

TASK 5

Identify the Domain

29. Right-click the entity and select **Run Transform → All Transforms → To Domains [DNS]**.

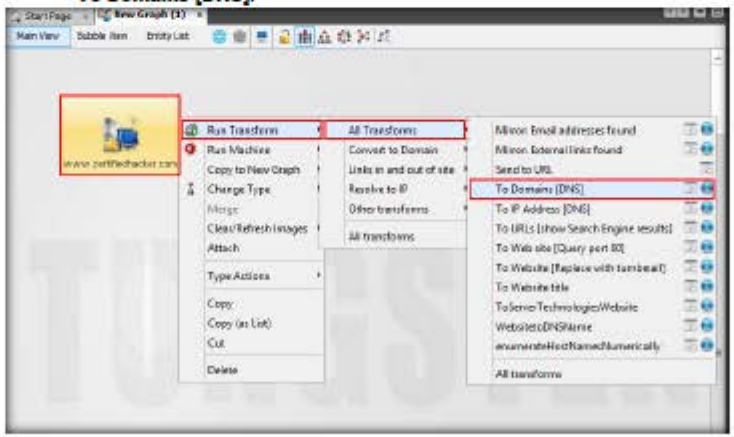


FIGURE 9.23: Selecting To Domains [DNS]

Maltego aids you in your thinking process by visually demonstrating interconnected links between searched items.

30. The domain corresponding to the website displays, as shown in the following screenshot:

FIGURE 9.24: Domain Name of the Corresponding Website

TASK 6

Identify the Domain Name Schema

31. Right-click the entity and select **Run Transform → All Transforms → DomainToDNSNameSchema**.

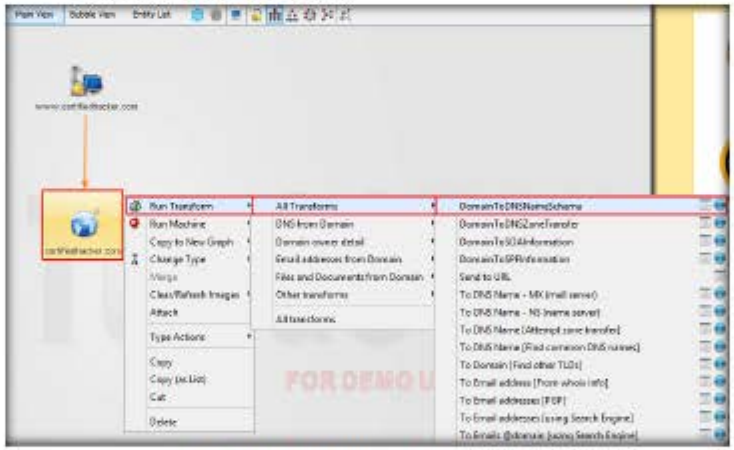


FIGURE 9.25: Selecting DomainToDNSNameSchema

32. The **Required inputs** pop-up appears. Check **I accept the above disclaimer** and **Remember these settings.** Click Run!

If access to "hidden" information determines your success, Maltego can help you discover it.

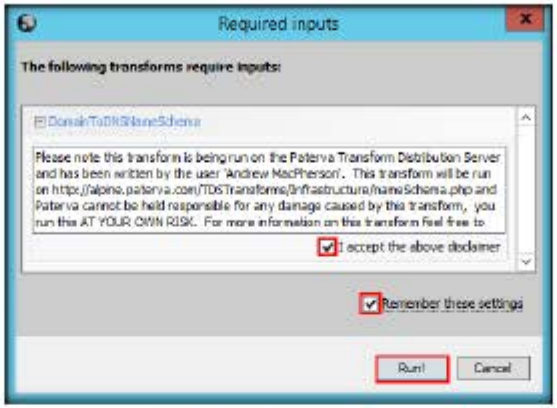


FIGURE 9.26: Required inputs pop-up

33. This transform will attempt to test various name schemas against a domain and try to identify a specific name schema for the domain as shown in the following screenshot:

Maltego is unique because it uses a powerful, flexible framework that makes customizing possible. As such, Maltego can be adapted to your own, unique requirements.

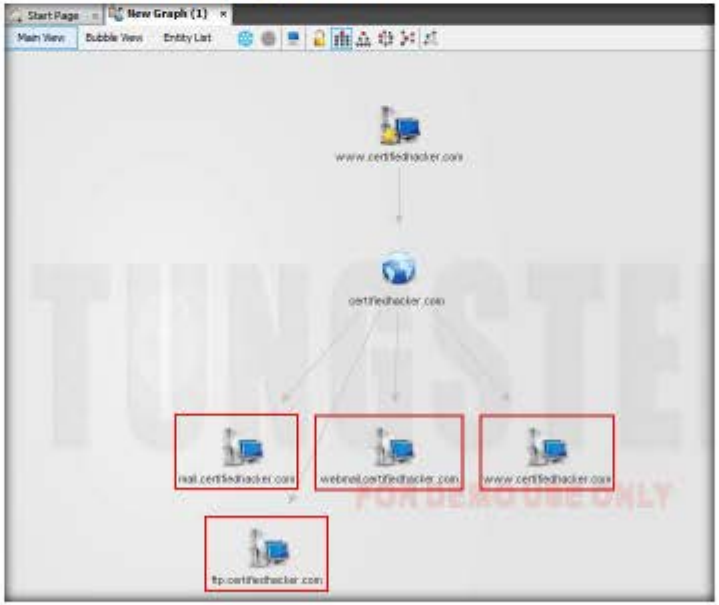


FIGURE 9.27: DNSNameSchema of certifiedhacker.com

34. After identifying the name schema, attackers attempt to simulate various exploitation techniques to gain sensitive information related to the resultant name schemas. For example, an attacker may implement a brute force or dictionary attack to log in to ftp.certifiedhacker.com and gain confidential information.
35. Select only the name schemas by dragging and deleting them.

Using the graphical user interface (GUI) you can see relationships easily - even if they are three or four degrees of separation away.

FIGURE 9.28: Deleting the Name Schemas

36. Right-click the entity and select **Run Transform → All Transforms → DomainToSOAInformation.**

TASK 7

Identify the Service Oriented Architecture (SOA) Information

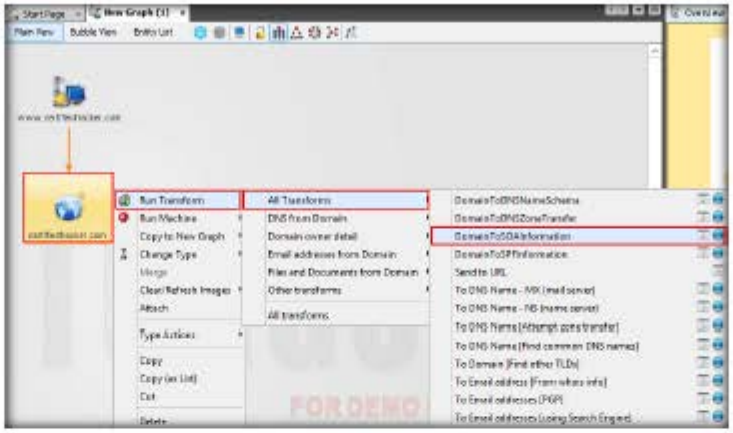


FIGURE 9.29: Deleting the Name Schemas

37. This returns the primary name server and the email of the domain administrator, as shown in the following screenshot:

Maltego provides you with a graphical interface that makes seeing these relationships instant and accurate - making it possible to see hidden connections.

FIGURE 9.30: Primary Name Server and the Email of the Domain

38. By extracting the SOA related information, attackers attempt to find vulnerabilities in their services and architectures, and exploit them.

39. Select both the name server and the email by dragging and deleting them.

Maltego is easy and quick to install - it uses Java, so it runs on Windows, Mac and Linux.

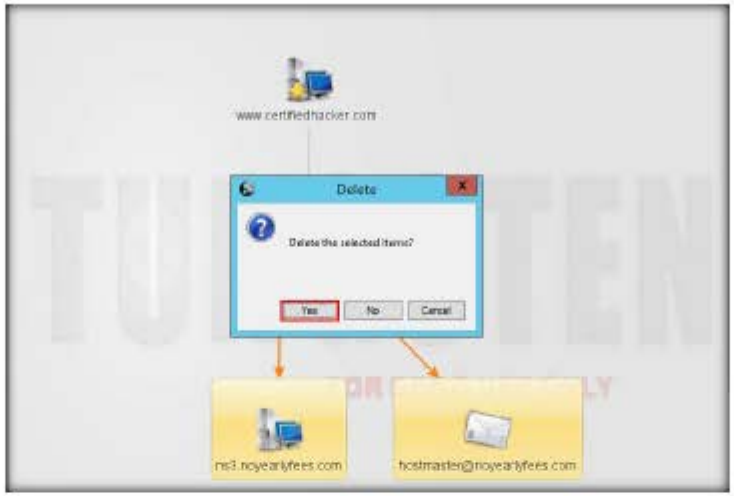


FIGURE 9.31: Deleting the Primary Name Server and the Email of the Domain

TASK 8

Identify the Mail Exchanger

40. Right-click the entity and select **Run Transform → All Transforms → To DNS Name - MX (mail server).**

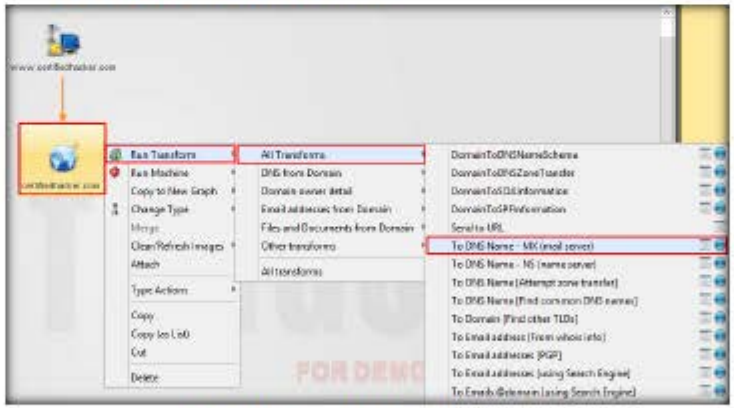


FIGURE 9.32: Selecting To DNS Name - MX (mail server)

41. This transform returns the mail server associated with the certifiedhacker.com domain, as shown in the following screenshot:

Maltego offers the user with unprecedented information. Information is leverage. Information is power. Information is Maltego.

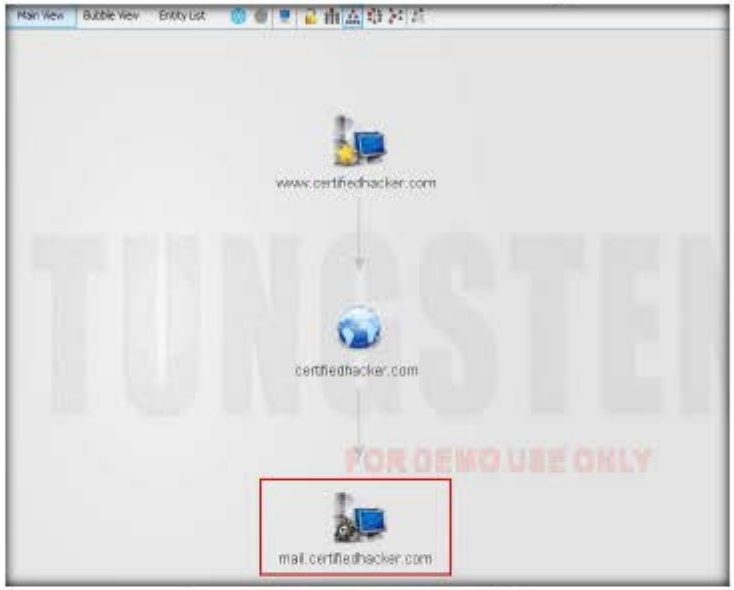


FIGURE 9.33: Mail Server Associated with the certifiedhacker.com

42. By identifying the mail exchanger server, attackers attempt to exploit the vulnerabilities in the server and thereby use it to perform malicious activities such as sending spam e-mails.

43. Select only the mail server by dragging and deleting it.

The unique perspective that Maltego offers to both network and resource based entities is the aggregation of information posted all over the internet - whether it's the current configuration of a router poised on the edge of your network or the current whereabouts of your Vice President on his international visits, Maltego can locate, aggregate and visualize this information.

FIGURE 9.34: Deleting the Mail Server Entity

TASK 9

Identify the Name Server

44. Right-click the entity and select **Run Transform → All Transforms → To DNS Name - NS (name server)**.

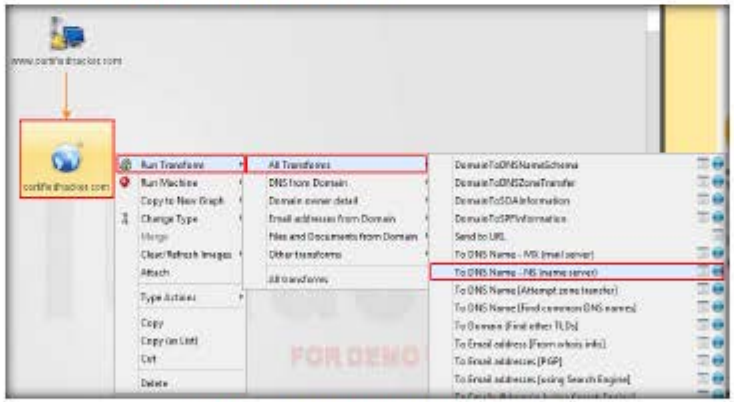


FIGURE 9.35: Selecting To DNS Name - NS (name server)

45. This returns the name servers associated with the domain, as shown in the following screenshot:

Maltego is a unique platform developed to deliver a clear threat picture to the environment that an organization owns and operates.

FIGURE 9.36: Name Server Associated with the Domain

46. By identifying the primary name server, an attacker can implement various techniques to exploit the server and thereby perform malicious activities such as DNS Hijacking, and URL redirection.

47. Select both the domain and the name server by dragging and deleting them.

TASK 10

Identify the IP Address

48. Right-click the entity and select **Run Transform → All Transforms → To IP Address [DNS]**.

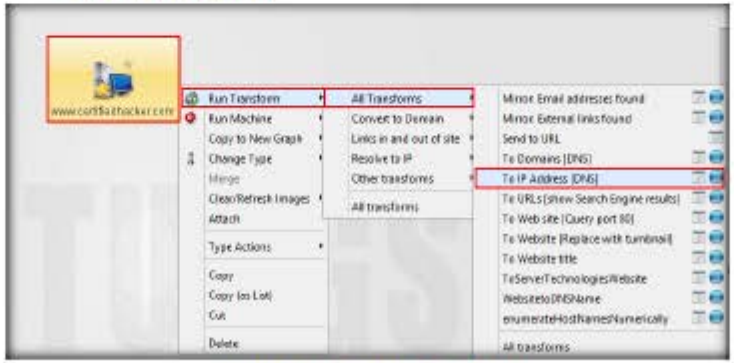


FIGURE 9.37: Selecting To IP Address [DNS]

Maltego's unique advantage is to demonstrate the complexity and severity of single points of failure as well as trust relationships that exist currently within the scope of your infrastructure.

49. This displays the IP address of the website, as shown in the following screenshot:

FIGURE 9.38: IP address of the website

50. By obtaining the IP address of the website, an attacker can simulate various scanning techniques to find open ports and vulnerabilities, and thereby attempt to intrude in the network and exploit them.

TASK 11

Identify the Geographical Location

51. Right-click the entity and select **Run Transform → All Transforms → To Geo location [whoisAPI]**.

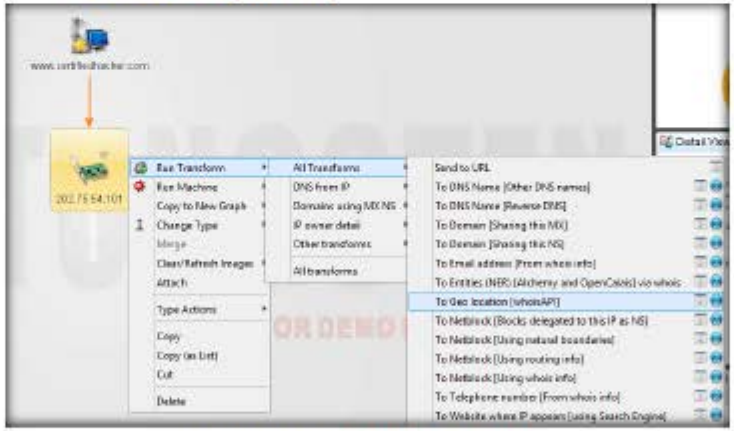


FIGURE 9.39: Selecting To Geo location [whoisAPI]

52. This transform identifies the geographical location where the IP address is located, as shown in the following location:

Custom entities can easily be shared between users by exporting and importing them. It's also possible to share entities by simply saving a graph containing custom entities and loading it in another (clean) Maltego.

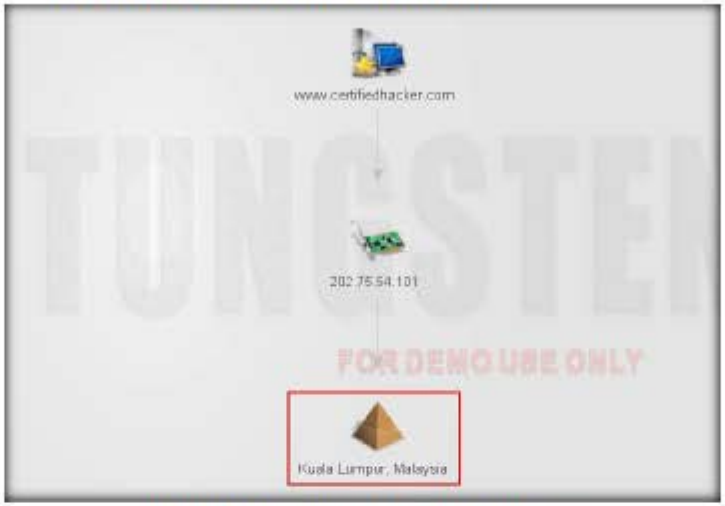


FIGURE 9.40: Geographical Location where the IP Address is Located

53. By obtaining the information related to geographical location, attackers can perform social engineering attacks by making voice calls (vishing) to an individual in an attempt to leverage sensitive information.

54. Follow **Step 27** to resolve the domain name of the website.

By putting an exclamation mark in front of a phrase you can invert the selection - e.g. if you want to that do not match the word 'linode' you need to search for '!linode'.

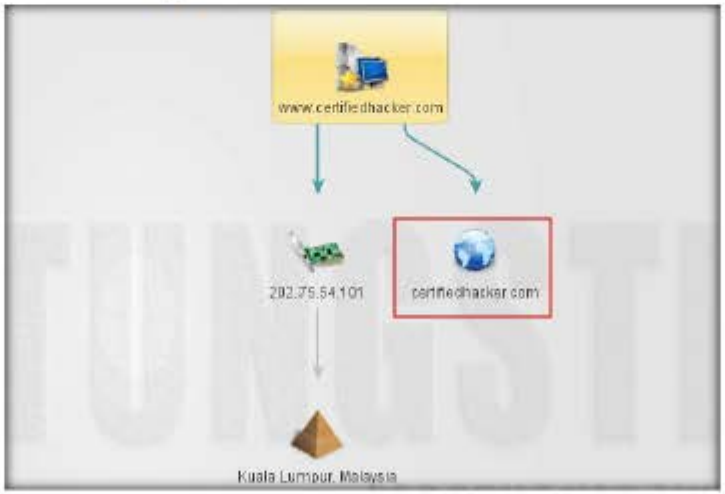


FIGURE 9.41: Domain Name Corresponding to the Website

TASK 12

Identify the Entities

55. Right-click the domain entity (certifiedhacker.com) and select **Run Transform → Domain owner detail → To Entities (NER) [Alchemy and OpenCalais] via whois.**

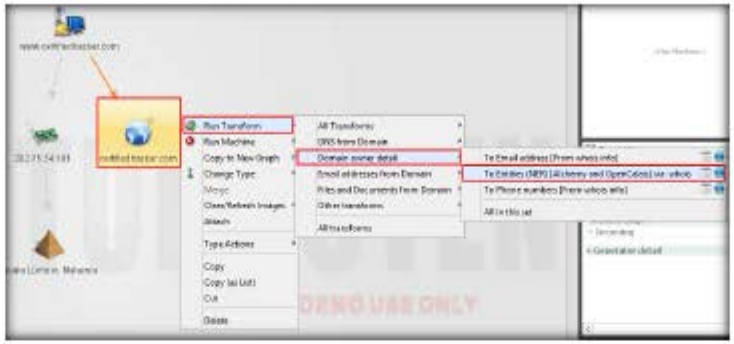


FIGURE 9.42: Selecting o Entities (NER) [Alchemy and OpenCalais] via whois

56. This transform returns the entities pertaining to the owner of the domain, as shown in the following screenshot:

FIGURE 9.43: Entities Pertaining to the Owner of the Domain

The Find (Control F) functionality with the secondary search in the Detail View gives a lot a flexibility and power.

57. By obtaining this information, an attacker can exploit the servers displayed in the result or simulate a brute force attack or any other technique to hack in to the admin mail account and send phishing mails to the contacts in that account.

TASK 13

Identify the Email Address

58. Perform Footprinting on a target person to obtain the email address and phone number.
59. Click the icon located at the top-left corner of the GUI (in the toolbar) to start a new graph

FIGURE 9.44: Creating a New Graph

60. A new graph (**New Graph (2)**) appears in Maltego. Expand the **Personal** tab in the left pane and drag the **Person** entity to the **New Graph (2)** section.
61. The name of the entity is set as **John Doe** by default.

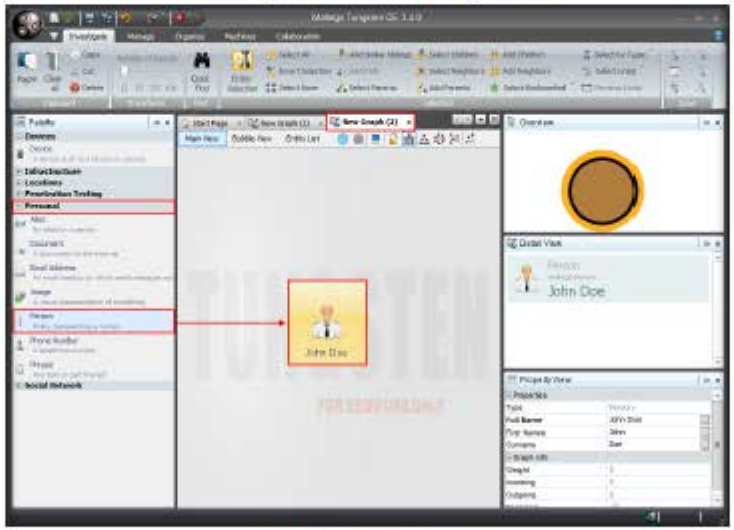


FIGURE 9.45: Adding a Person Entity

The detail view contains information about the entity that cannot be displayed in the main graph window. These are things that the transform author wants you to see about the entity.

62. To assign a target person name, double-click **John Doe** and type the name of the person (here, **rini matthews**).

As the mouse is moved over entities both the entity properties and detail view is updated.

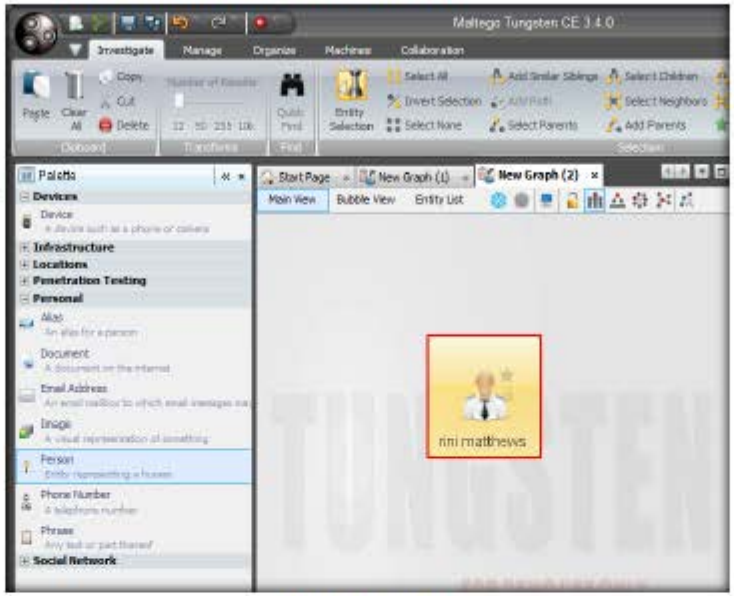


FIGURE 9.46: Renaming the Entity

63. Right-click the entity and select **Run Transform → All Transforms → To Email Address [Verify common]**.

Each entity has a number of properties and may have a detailed view. Most of the pro while the detailed view is read-only.

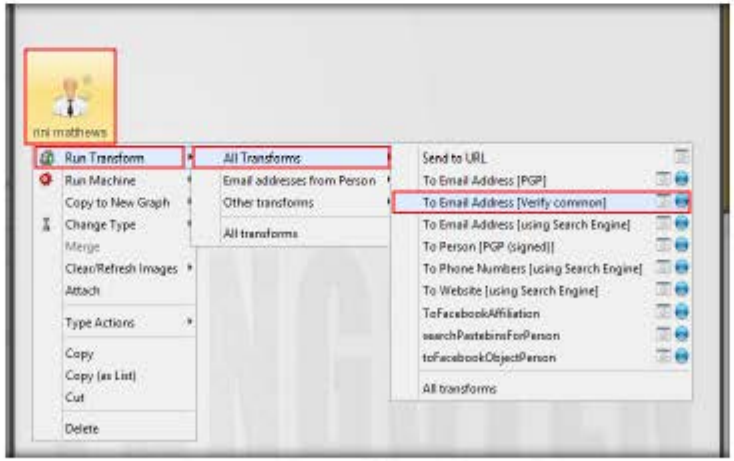


FIGURE 9.47: Setting To Email Address [Verify common] Option

64. Maltego displays all the valid email addresses (which have the name in common) corresponding to the given name, as shown in the following screenshot:

The properties of an entity are used by transforms and are passed along with the entity's value to the transform. Detailed view information is not passed to the transform.

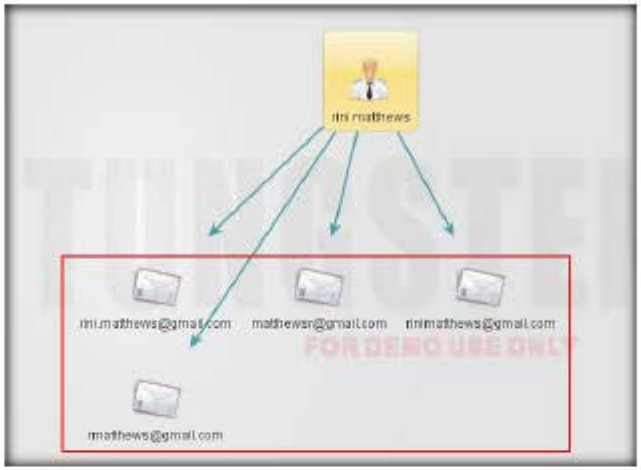


FIGURE 9.48: Setting To Email Address [Verify common] Option

65. Assess the Email addresses and determine which one belongs to the target person.
66. Select all the Email addresses and delete them.

TASK 14

Identify the Phone Number

67. Right-click the **person** entity (rini matthews) and select **Run Transform → All Transforms → To Phone number [using Search Engine]**.

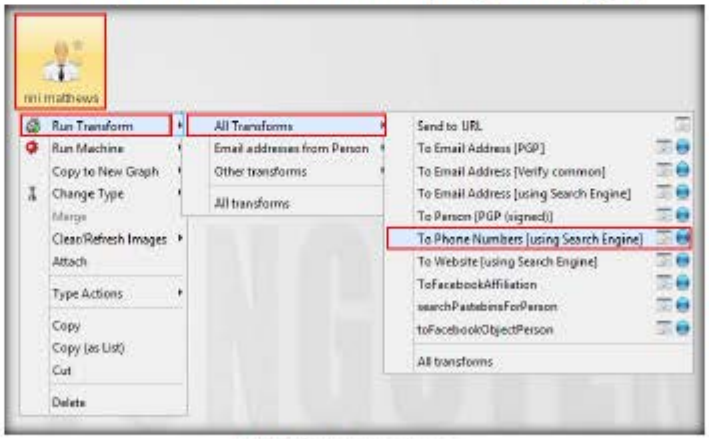


FIGURE 9.49: Selecting a Transform

68. A **Required inputs** pop-up appears. Press **Space** in both the fields and click **Run!**.

The windows can also be ragged around to snap into place in different configurations.

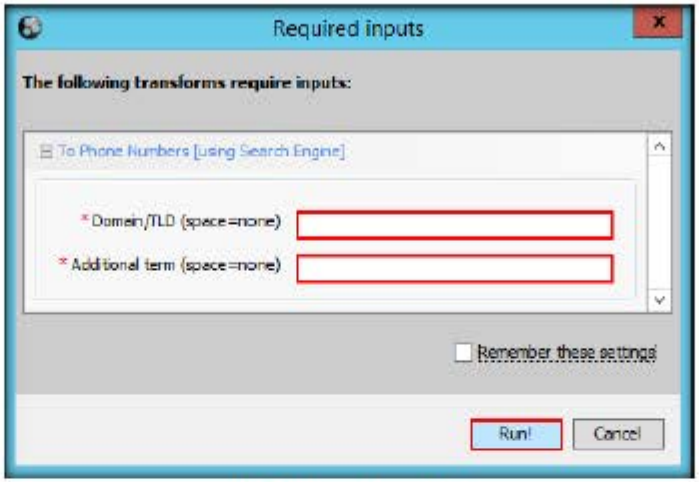


FIGURE 9.50: Required inputs pop-up

69. Maltego displays a list of phone numbers associated to a person, as shown in the following screenshot:

The show opened documents list button that are open. Graphs that have not been saved yet will be displayed as "New Graph (number)".

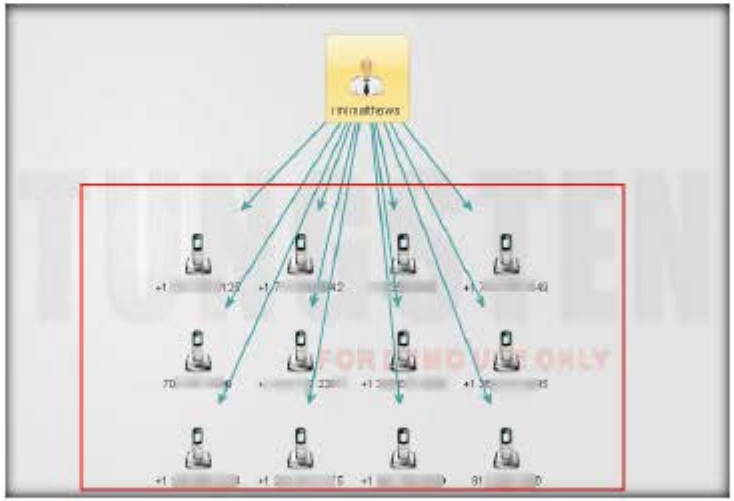


FIGURE 9.51: Phone Numbers Identified

70. Check each number with online people search tools such as yellow pages in order to confirm that a particular phone number belongs to the target person.
71. Select all the entities in the section and delete them.
72. By extracting all this information, an attacker can simulate actions such as enumeration, web application hacking, social engineering, etc. which may allow access to a system or network, gain credentials, etc..
73. Apart from the transforms mentioned above, there are also transforms that can track accounts and conversations of individuals who are registered in social networking sites such as Facebook and Twitter.

Lab Analysis

Collect and document the Information obtained in this lab.

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

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

Lab

10

Performing Automated Network Reconnaissance Using Recon-ng

Recon-ng is a web-based open-source reconnaissance tool used to extract information from a target organization and its personnel.

ICON KEY

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

Lab Scenario

As an ethical hacker or pen tester, you should also perform host discovery on the target to get information about additional domains. This activity will enable you to find all the hosts present on the target. This lab will demonstrate how to discover additional hosts from the target.

Lab Objectives

The objective of this lab is to help students learn how to perform network reconnaissance of a target and:

- Gather hosts related to a domain
- Reverse lookup the IP address obtained during the network reconnaissance

Lab Environment

To carry out the lab, you need:

- **Windows Server 2012** running as a host machine
- **Kali Linux** running as a virtual machine
- A web browser with internet access

Lab Duration

Time: 10 Minutes

Overview of Recon-ng

Recon-ng is a full-featured Web Reconnaissance framework written in Python. Complete with independent modules, database interaction, built in convenience functions, interactive help, and command completion.

Recon-ng is a Web Reconnaissance framework consisting of modules that perform host discovery on the target. It includes these modules that can be used for host discovery

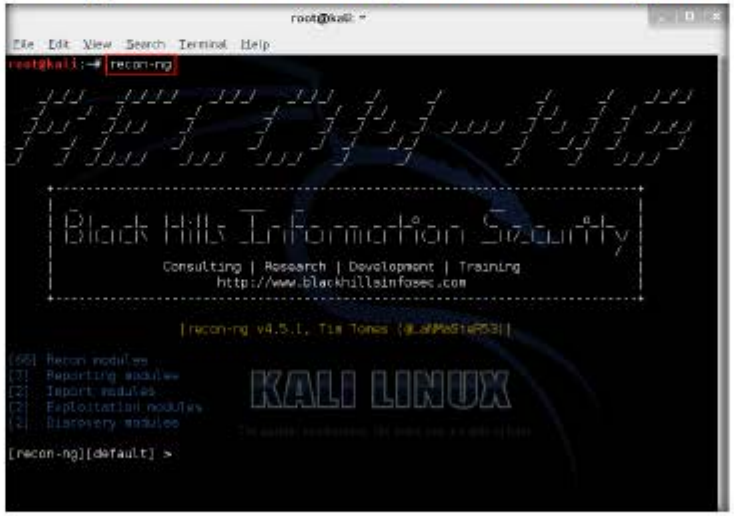
- hosts_baidu – Baidu Hostname Enumerator
- hosts_bing – Bing Hostname Enumerator
- hosts_brute_force – DNS Hostname Brute Forcer
- hosts_google – Google Hostname Enumerator
- hosts_netcraft – Netcraft Hostname Enumerator
- hosts_shodan – Shodan Hostname Enumerator
- hosts_yahoo – Yahoo Hostname Enumerator

Lab Tasks

TASK 1

Launch recon-ng

1. Launch the Kali Linux virtual machine from Hyper-V manager, and log in to it using the credentials: **root**/**toor.**
2. Launch a command line terminal.
3. Type the command **recon-ng** and press **Enter** to launch the application.



Recon-ng provides a powerful environment in which open source web-based reconnaissance can be conducted quickly and thoroughly.

FIGURE 10.1: Launching recon-ng

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

4. Type **show modules** command and press **Enter** to view all the modules contained in recon-ng.
5. You will be able to perform network discovery, exploitation, reconnaissance, etc. by loading the required modules.

Recon-ng has a look and feel similar to the Metasploit Framework, reducing the learning curve for leveraging the framework.

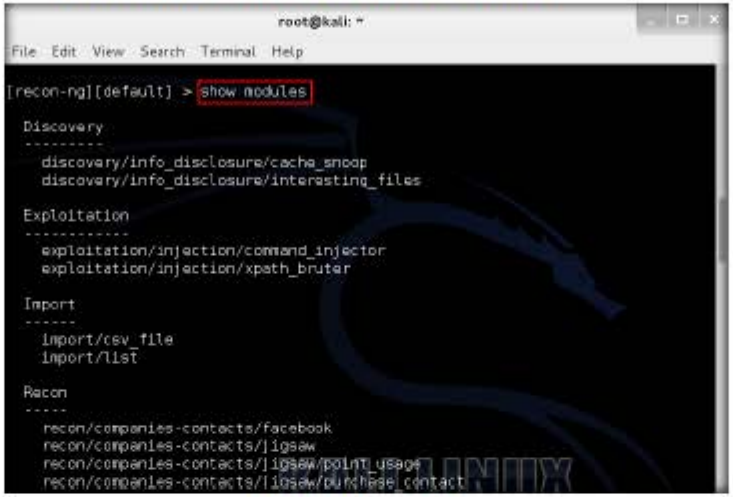


FIGURE 10.2: Viewing Modules

6. Type **help** and press **Enter** to view all the commands that allow you to add/delete records to a database, query a database, etc.

However, it is quite different. Recon-ng is not intended to compete with existing frameworks, as it is designed exclusively for web-based open source reconnaissance.

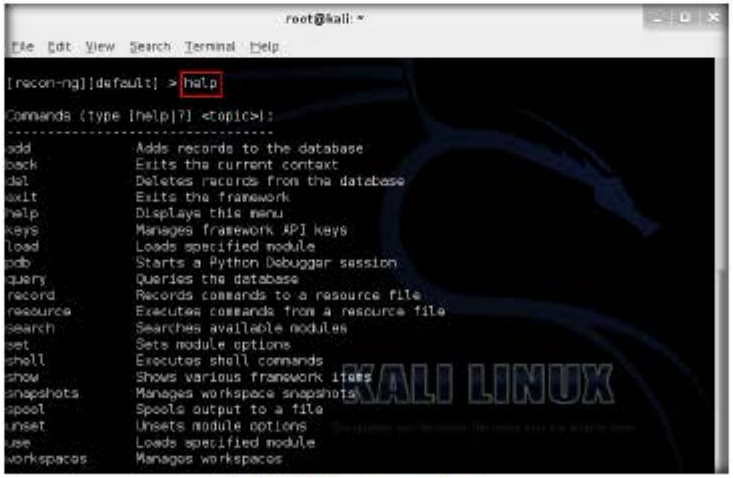


FIGURE 10.3: Viewing recon-ng Commands

TASK 2

Add a workspace

7. Type **workspaces** command and press **Enter**. This displays the usage commands related to the workspaces.

FIGURE 10.4: Viewing Workspaces Related Commands

8. Add a workspace in which to perform network reconnaissance. In this lab, we shall be adding a workspace named **CEH**.
9. To add the workspace, type the command **workspaces add CEH** and press **Enter**. This creates a workspace named CEH as shown in the following screenshot:

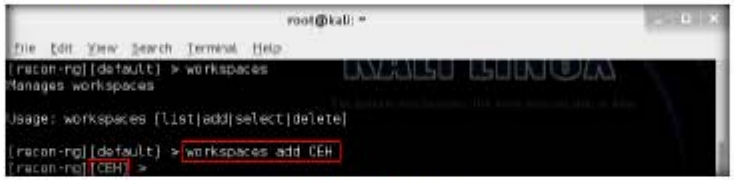


FIGURE 10.5: Adding a Workspace

Note: You can alternatively issue the command **workspaces select CEH** to create a workspace named CEH

10. Enter **workspaces list**. This displays a list of workspaces (along with the workspace added in the previous step) that are present with in the Workspaces databases.

If you want to exploit, use the Metasploit Framework. If you want to social engineer, use the Social-Engineer Toolkit.

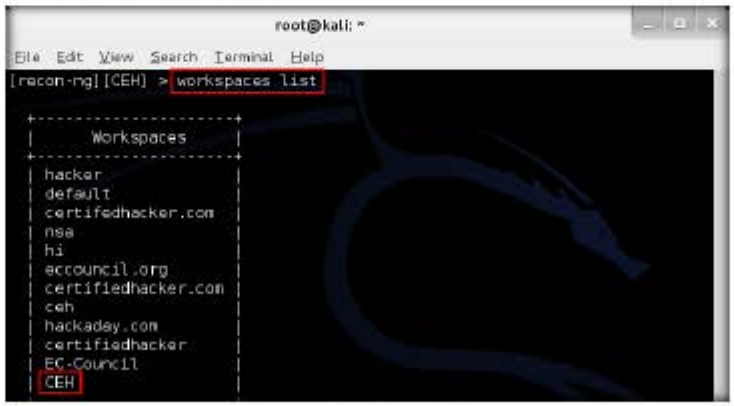


FIGURE 10.6: Viewing the Added Workspaces

TASK 3

Add a Domain

11. Add a domain in which to perform network reconnaissance
12. So, type the command **add domains microsoft.com** and press **Enter**. This adds microsoft.com to the present workspace.

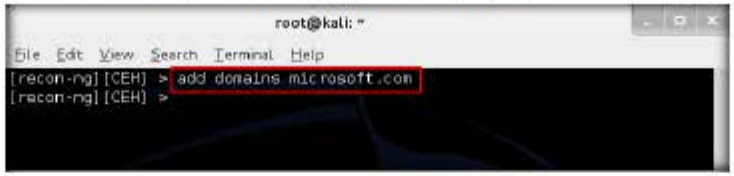


FIGURE 10.7: Adding a Domain

13. You can view the added domain by issuing the **show domains** command as shown in the following screenshot:

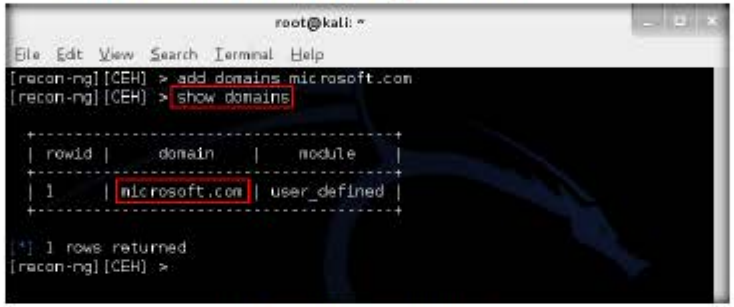


FIGURE 10.8: Viewing the Added Domain

TASK 4

Resolve Hosts Using Netcraft Module

14. Harvest the hosts-related information associated with microsoft.com by loading network reconnaissance modules such as netcraft, bing and brute_hosts.
15. Type the command **search netcraft** and press **Enter** to view the modules related to netcraft

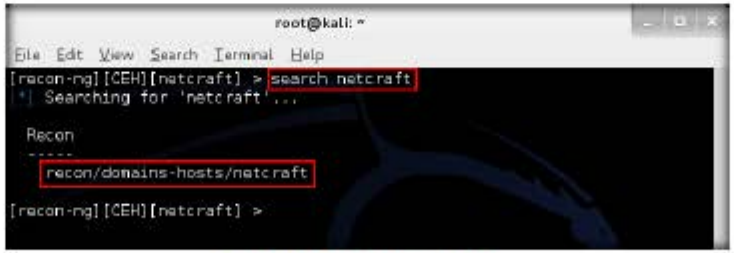


FIGURE 10.9: Searching netcraft Module

16. Load the **recon/domains-hosts/netcraft** module to harvest the hosts. To load this module, enter **load recon/domains-hosts/netcraft**.

Recon-ng is a completely modular framework and makes it easy for even the newest of Python developers to contribute.

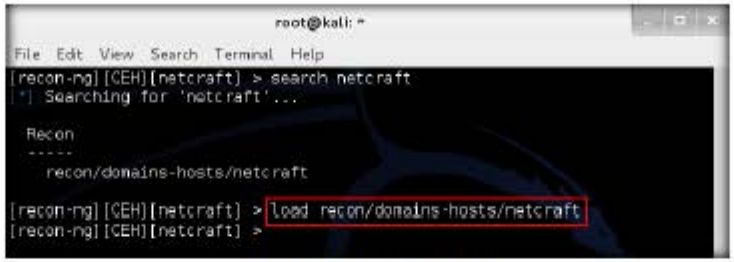


FIGURE 10.10: Loaded netcraft Module

17. Type **run** and press **Enter**. This executes the module and begins to harvest the hosts as shown in the following screenshot:

Each module is a subclass of the "module" class. The "module" class is a customized "cmd" interpreter equipped with built-in functionality that provides simple interfaces to common tasks such as standardizing output, interacting with the database, making web requests, and managing API keys.

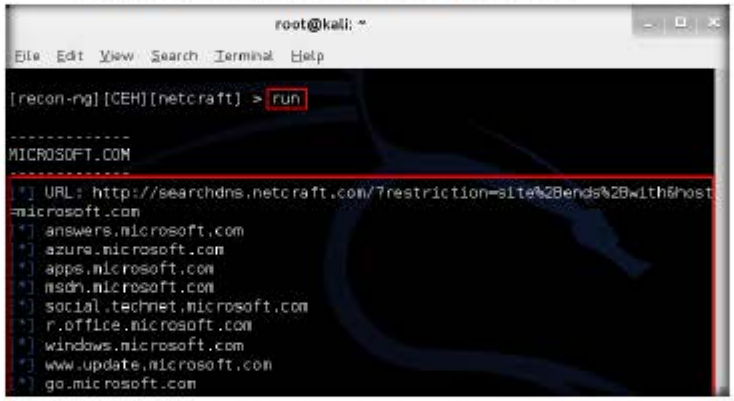


FIGURE 10.11: Running netcraft Module

18. You have harvested the hosts related to microsoft.com using the netcraft module. You can use other modules such as Bing to harvest more hosts.

TASK 5

Resolve Hosts Using Bing Module

19. Type **load bing** (or **search bing**) command and press **Enter** to view all the modules related to Bing. In this lab, you will be using **recon/domains-hosts/bing_domain_web** module to harvest hosts.

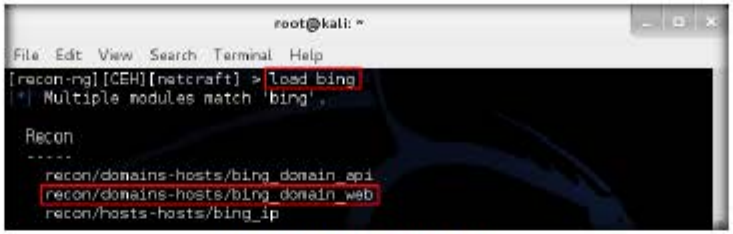


FIGURE 10.12: Searching for bing Module

20. To load the **recon/domains-hosts/bing_domain_web** module, type load **recon/domains-hosts/bing_domain_web** command and press **Enter**

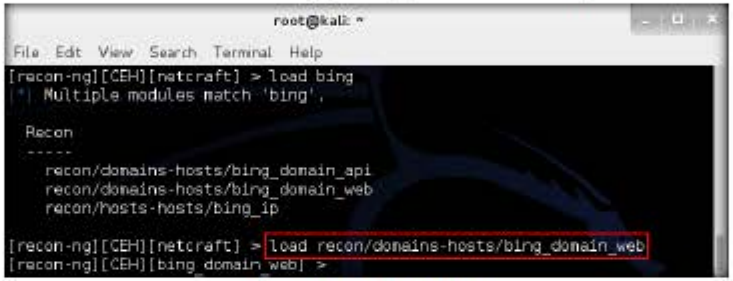


FIGURE 10.13: Loading bing Module

21. Type **run** and press **Enter**. This begins to harvest the hosts as shown in the following screenshot:

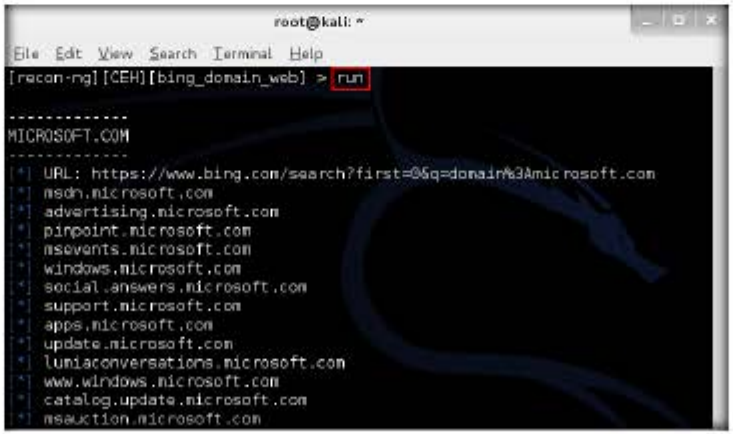


FIGURE 10.14: Running the bing Module

Therefore, all the hard work has been done. Building modules is simple and takes little more than a few minutes.

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

22. Observe that a few more hosts have been harvested. You can use other modules such as **brute_hosts** to harvest more hosts.

TASK 6

Resolve Hosts Using brute_hosts Module

23. Type **load brute** (or **search brute**) command and press **Enter** to view all the modules related to brute forcing. In this lab, you will be using the **recon/domains-hosts/brute_hosts** module to harvest hosts.

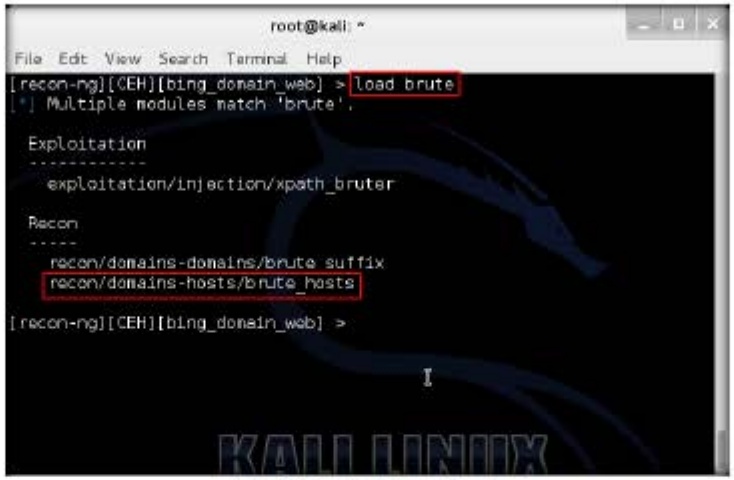


FIGURE 10.15: Searching for brute Module

The "libs" folder is for small 3rd party dependancies not available through the Python Package Index (PIP). The "libs" folder is added to the Python path at runtime. Place modules here and import as normal into modules.

24. To load the **recon/domains-hosts/brute_hosts** module, type load **recon/domains-hosts/brute_hosts** command and press **Enter**

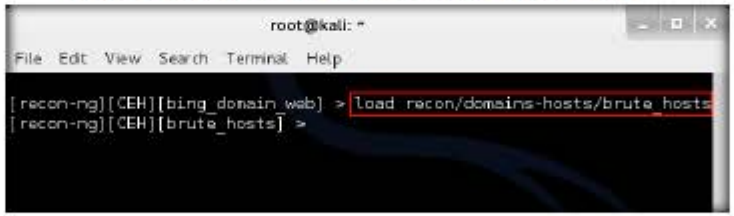


FIGURE 10.16: Loading brute Module

25. Type **run** and press **Enter**. This begins to harvest the hosts as shown in the following screenshot:

The "modules" folder is crawled at runtime to establish the module tree from which all modules are loaded. Place new modules where it makes logical sense, or create a new folder to expand the module tree.

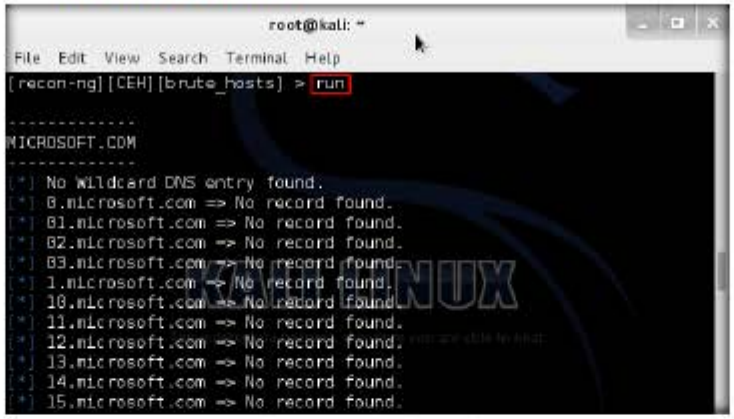


FIGURE 10.17: Running brute Module

26. Observe that a few more hosts have been added by running the **recon/domains-hosts/brute_hosts** module.

FIGURE 10.18: Newly Added Hosts

Modules are loaded on-demand, giving developers the ability to reload modules without restarting the framework by hacking into the global context and reloading the module.

27. Perform a reverse lookup for each IP address (the IP address that is obtained during the reconnaissance process) to resolve to respective hostnames

TASK 7

Perform Reverse Lookup Using reverse_resolve module

28. Type load **reverse_resolve** command and press **Enter** to view all the modules associated with the reverse_resolve keyword. In this lab, we are using **recon/hosts-hosts/reverse_resolve** module.
29. So, type **load recon/hosts-hosts/reverse_resolve** command and press Enter to load the module

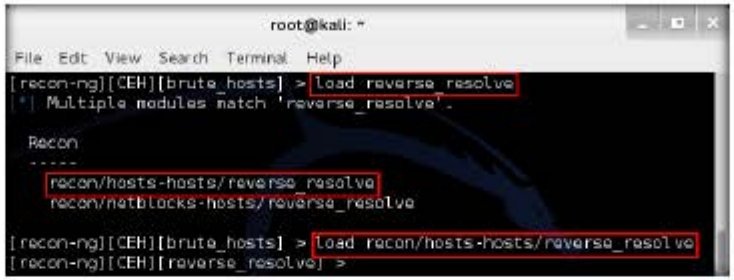


FIGURE 10.19: Search for reverse_resolve Module

30. Issue the **run** command to begin reverse lookup

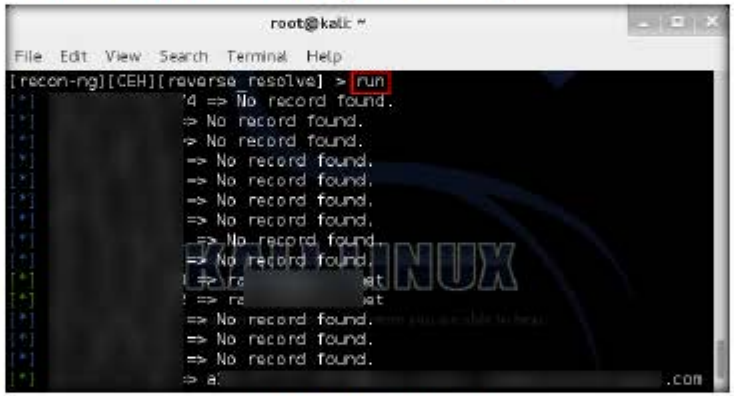


FIGURE 10.20: Running the Module

During module development, developers will need to repeatedly reload framework modules to test code changes. On-demand reloading provides the capability to reload modules while maintaining command history and global options settings.

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

31. Once done with the reverse lookup process, type **show hosts** command and press **Enter**. This displays all the hosts that are harvested so far, as shown in the following screenshot:

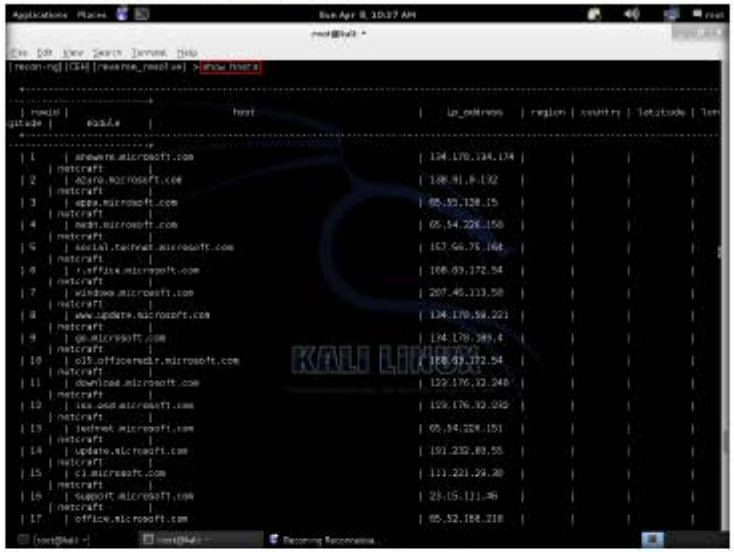


FIGURE 10.21: Viewing the Harvested Hosts

32. Now, type **back** command and press **Enter** to go back to the CEH attributes terminal

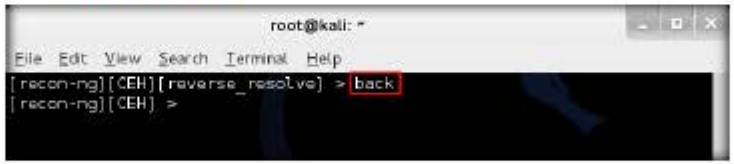


FIGURE 10.22: Going back to the Attributes Section

Squash all commits into a single commit before submitting pull requests. This can be done from the command line by checking out the source fork with the git checkout <fork> command and issuing the git rebase -i command.

TASK 8

Generate a Report

33. Now that you have harvested a number of hosts, you will prepare a report containing all the hosts

34. Type **load reporting** command and press **Enter** to view all the modules associated with the reporting keyword. In this lab, we shall be saving the report in html format. So the module used is **reporting/html**.

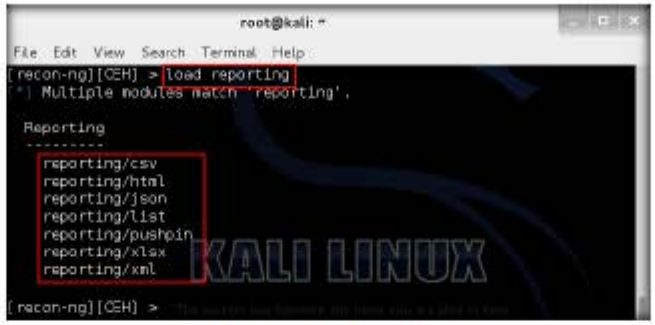


FIGURE 10.23: Searching for reporting Module

35. Type **load reporting/html** command and press **Enter**. Now, you need to know which options are to be configured to generate the html report. To know this, type **show options** command and press Enter.

36. Observe that you need to assign values for **CREATOR** and **CUSTOMER** options, while the **FILENAME** value is already set and you may change the value if required. Leave the SANITIZE option's value set to default.

37. Type:

    a. **set FILENAME /root/Desktop/CEH_results.html** and press **Enter**. By issuing this command, you are setting the report name as **CEH_results** and the path to store the file as **Desktop**.

    b. **set CREATOR [your name]** (here, **Jason**) and press **Enter**

    c. **set CUSTOMER Microsoft Networks** (since, you have performed network reconnaissance on **microsoft.com** domain) and press **Enter**

Choose "squash" for all of your commits, except the first one, and consolidate the commit messages to a single message that summarizes the pull request.

Push the modified fork to the remote repository with the git push -f command.

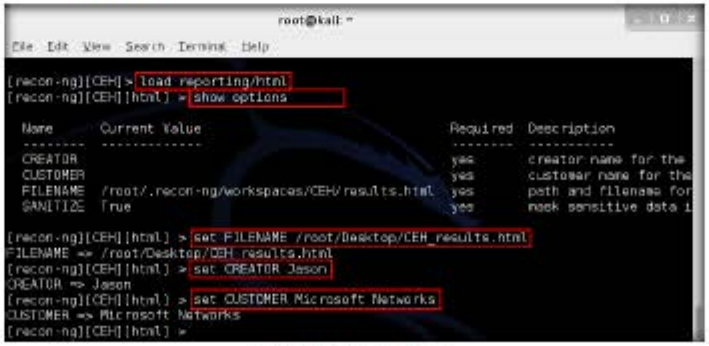


FIGURE 10.24: Saving a Report

38. Type **run** command and press **Enter** to create a report for all the hosts that have been harvested.

FIGURE 10.25: Running the Module

39. The generated report is saved to the **Desktop**. Double-click the **CEH_reults.html** file.

This technique will automatically update existing pull requests from the affected source fork.

FIGURE 10.26: Viewing the Report

40. The generated report appears in the Iceweasel web browser displaying the summary of the harvested hosts. Expand the **Hosts** node to view all the harvested hosts and analyze them.

There is not much in this report, but when you start running multiple modules and add in geolocation reports can get pretty complex, and recon-ng does a great job keeping track of everything.

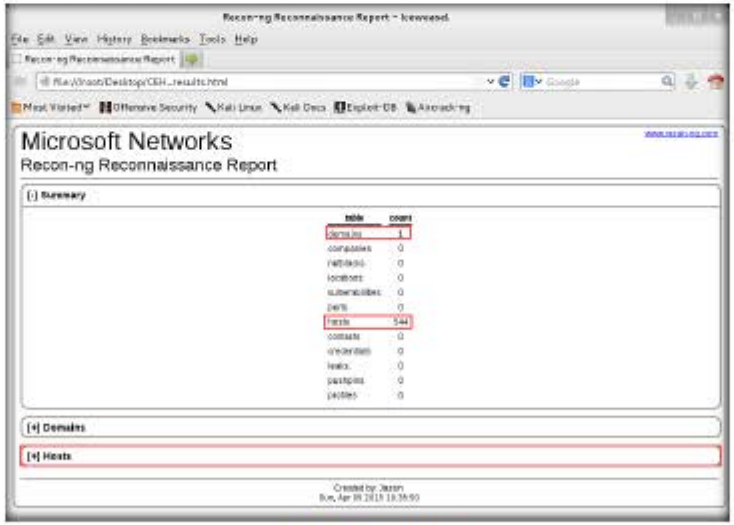


FIGURE 10.27: Viewing the Report

41. Recon-ng performs network reconnaissance on a target domain.

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 ABOUT THIS LAB.

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

Lab 11

Using the Open-source Reconnaissance Tool Recon-ng to Gather Personnel Information

Recon-ng is a web-based open-source reconnaissance tool that extracts information about the target organization and its personnel

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

Lab Scenario

During information gathering, you are required to discover personal information on the target. This personal information can be used later to perform other attacks such as social engineering attacks. So as a professional ethical hacker or pen tester, you should be able to discover the personal information of a target company. This lab will demonstrate how to discover personal information about the target organization.

Lab Objectives

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

- Obtain contacts of personnel working in an organization
- Validate the existence of usernames on specific websites
- Find the existence of user profiles on various websites

Lab Environment

To carry out the lab, you need:

- Windows Server 2012 running as a host machine
- Kali Linux running as a virtual machine
- Web browser with internet access

Lab Duration

Time: 10 Minutes

Overview of Personal Information Gathering

Gathering personal information involves discovering contact details such as email address, address, etc. present on the target organization's web site. The Recon-ng contains various modules for harvesting and discovering contact information about a certain company. Some of the Recon-ng modules for discovering personal information are:

- recon/domain-contacts
- recon/companies-contacts
- recon/domain-contacts/namechk

Lab Tasks

TASK 1

Launch recon-ng

1. Launch Kali Linux virtual machine from Hyper-V manager and log in to it using the credentials: **root**/**toor**.
2. Launch a command line terminal.
3. Type the command **recon-ng** and press **Enter** in order to launch the application.

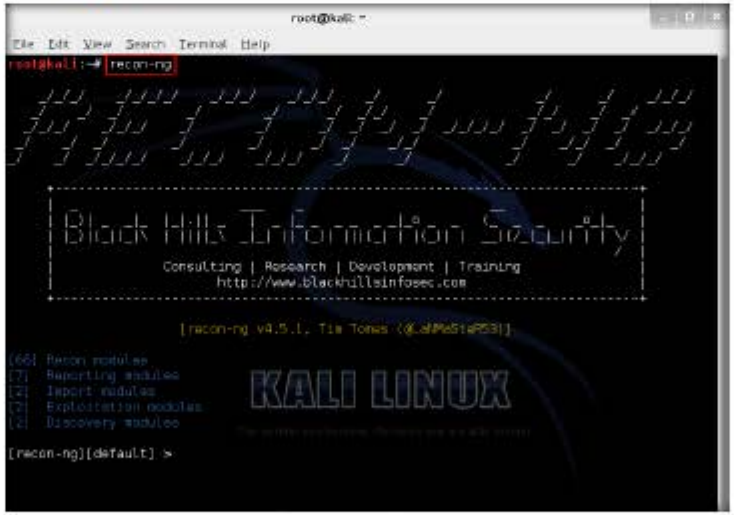


FIGURE 11.1: Launching recon-ng

Some Recon-ng modules require the use of an API key, OAuth Token, etc. To prevent users from having to continually input keys and regenerate tokens, Recon-ng provides methods which assist in storing, managing and accessing these items.

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

TASK 2

Gather Contacts Associated with a Domain

4. Add a workspace in which to perform information gathering. In this lab, we are adding a workspace named **reconnaissance**.
5. To add the workspace, type the command **workspaces add reconnaissance** and press **Enter**. This creates a workspace named reconnaissance.
6. Set a domain and perform footprinting on it to extract contacts available in the domain.
7. Type **load recon/domains-contacts/whois_pocs** and press **Enter**. This module uses the ARIN Whois RWS to harvest POC data from whois queries for the given domain.
8. Type **show info/show options** command and press **Enter** to view the options required to run this module.
9. Type **set SOURCE facebook.com** and press **Enter** to add facebook.com domain.

Some Recon-ng modules may require the use of popular search engines and social media sites with complex OAuth authentication schemes.

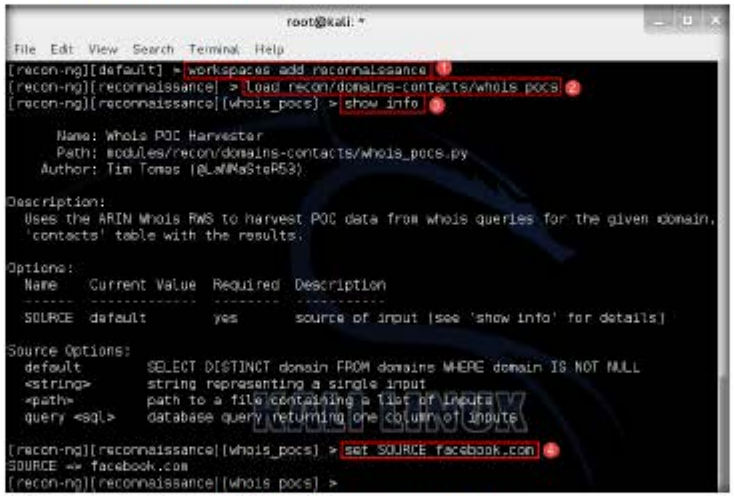


FIGURE 11.2: Harvesting Contacts from Domain

10. Type **run** command and press **Enter**. The **load recon/domains-contacts/whois_pocs** module extracts the contacts associated with the domain, and displays them as shown in the following screenshot:

Recon-ng provides developers with an easy way to create OAuth tokens for the LinkedIn and Twitter APIs, and interface with the Google, Bing, and Shodan search APIs.

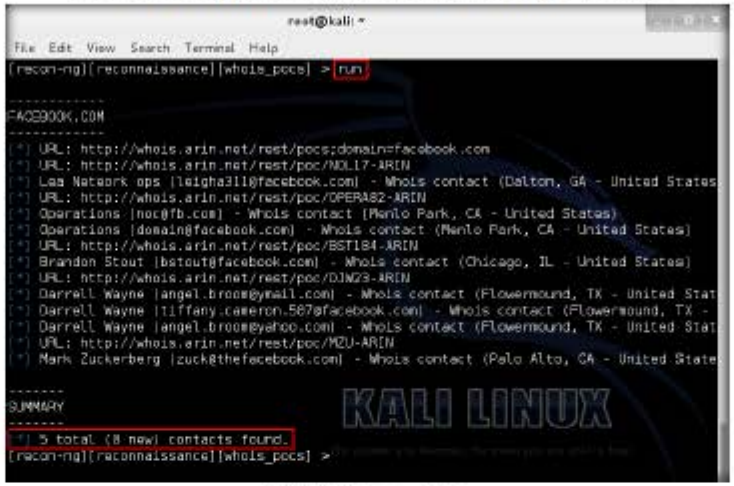


FIGURE 11.3: Running Module

The most important capability of a tool which specializes in web based reconnaissance is the ability to make web requests. Recon-ng relieves the burden of complicated request building logic by providing a custom method for handling web requests.

11. Type **back** and press **Enter** to go back to the workspaces (**reconnaissance**) terminal

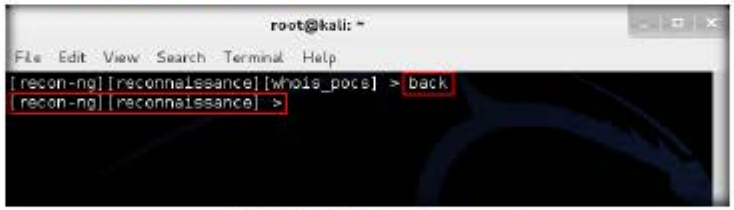


FIGURE 11.4: Going back to workspaces terminal

TASK 3

Check for User Existence

12. Now that you obtained contacts related to the domains, note down these contacts' names and validate the existence of their names (usernames) on specific websites.
13. The **recon/profiles-profiles/namechk** module validates the username existence of a specified contact. The contact we are going to use in this lab is **Mark Zuckerberg**.
14. Type **load recon/profiles-profiles/namechk** command and press **Enter** to load this module
15. Type **set SOURCE MarkZuckerberg** and press **Enter**. This command sets MarkZuckerberg as the source, for which you want to find the user existence on specific websites.

16. Type **run** and press **Enter**. This begins the search for the keyword MarkZuckerberg on various websites.
17. Recon-ng begins to search the internet for the presence of the username on websites and, if found, it returns the result stating "**User Exists!**" as shown in the following screenshot:

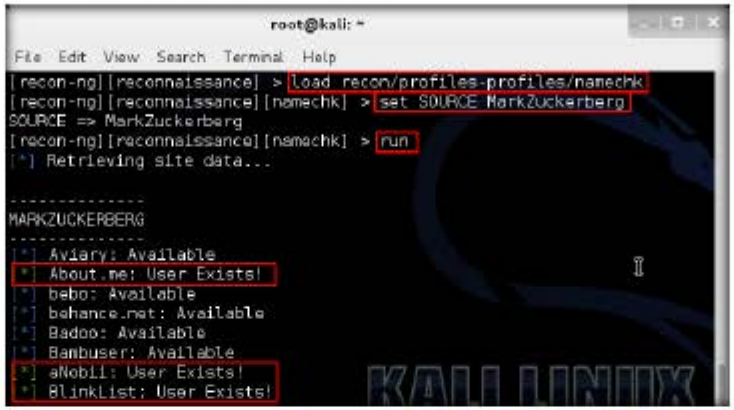


FIGURE 11.5: Running a Module

timeout (optional) is an integer representing the socket timeout for the request. If not set, the socket timeout defaults to the global option setting.

18. Type **back** command and press **Enter** to go back to the workspaces (reconnaissance) terminal.

payload (optional) is a dictionary of name-value pairs to be encoded as request parameters. payload should be used for "GET" and "POST" methods as the request method will encode and build the request as needed for the given method.

19. Find the existence of user profiles in various websites, for which you need to load the recon/profiles-profiles/profiler module.
20. Type **load recon/profiles-profiles/profiler** command and press **Enter**
21. Type **set SOURCE MarkZuckerberg** command and press **Enter**.

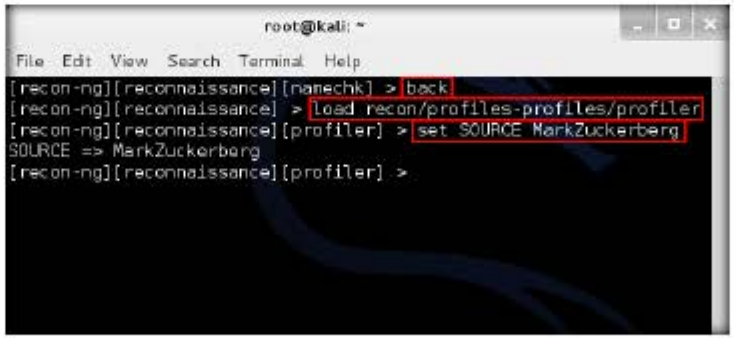


FIGURE 11.6: Configuring Module

TASK 4

Check for Profile Existence

22. Type **run** command and press **Enter**. The recon/profiles-profiles/profiler module searches for this username and returns the URL of the profile (found with the matching username), as shown in the following screenshot:

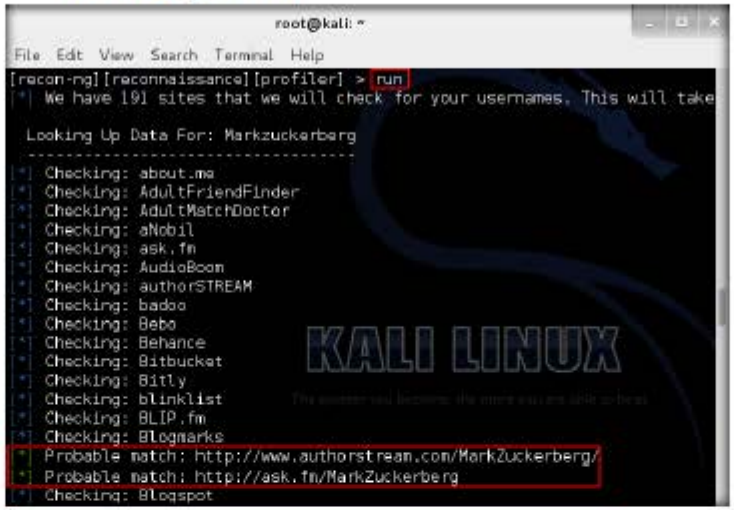


FIGURE 11.7: Running Module

content (optional) is a string indicating the content subtype of the POST payload. By default, the standard for a URL encoded POST payload is applied. Currently, only the default and "JSON" subtypes are available. Submitting a content subtype for any method other than a POST request raises a RequestException.

TASK 5

Generate Report

23. Type **back** and press **Enter** to go back to the workspaces terminal.
24. Now that you have verified the user existence and obtained the profile URL, you will prepare a report containing the result.
25. Type **load reporting** command and press **Enter** to view all the modules associated with the reporting keyword. In this lab, we shall be saving the report in html format. So the module used is **reporting/html**.
26. Type **load reporting/html** command and press **Enter**. Assign values for **CREATOR**, **CUSTOMER**, and **FILENAME**.

27. Type:

   a. **set FILENAME /root/Desktop/Reconnaissance.html** and press **Enter**. By issuing this command, you are setting the report name as **Reconnaissance** and path to store the file as **Desktop**.

   b. **set CREATOR [your name]** (here, **Jason**) and press **Enter**

   c. **set CUSTOMER Mark Zuckerberg** (since, you have performed information gathering on the name of **Mark Zuckerberg**) and press **Enter**

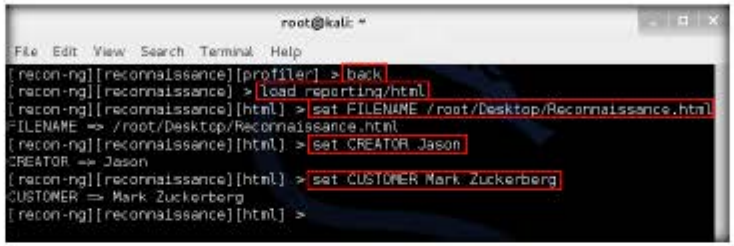


FIGURE 11.8: Configuring a Report

28. Type **run** command and press **Enter** to create a report for all the hosts that have been harvested.

method (optional) is the method of the request. Currently, only "GET" or "POST" are available.

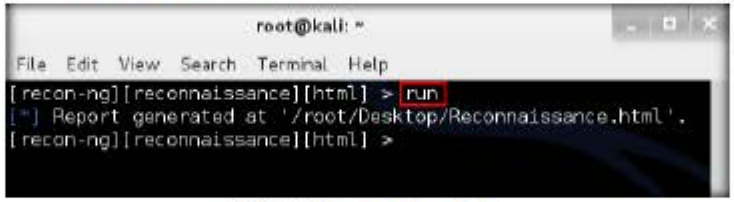


FIGURE 11.9: Running the Report Module

29. The generated report is saved to **Desktop**. Double-click the **Reconnaissance.html** file.

Recon-ng comes equipped with an RPC interface, ./recon-rpc.py, to provide 3rd party tools with a standardized protocol for accessing the data gathered and stored by the framework.

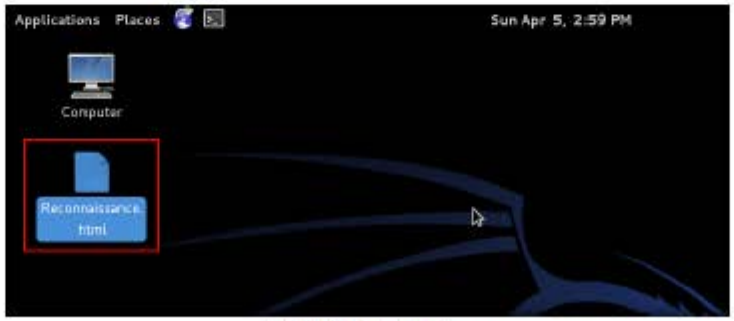


FIGURE 11.10: Viewing the Report

30. The generated report appears in the Iceweasel web browser displaying the summary of the result. You can expand the **Contacts** and **Profiles** nodes to view all the obtained results.

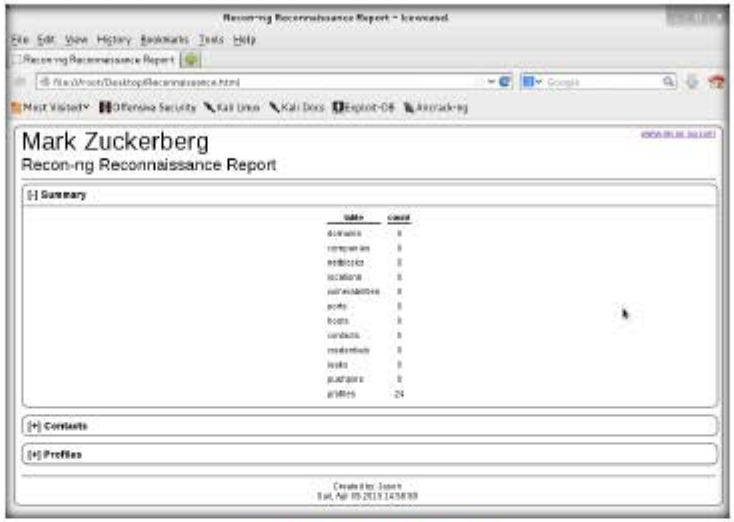


FIGURE 11.11: Viewing the Report

Both JSONRPC and XMLRPC protocols are supported, as well as MultiCall objects, and session IDs are used to provide a multi-user environment. Use ./recon-rpc.py -h for information on runtime options.

31. You have now gathered information on the personnel working in an organization.

Lab Analysis

Analyze and document the results related to 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 12

Collecting Information from Social Networking Sites Using Recon-ng Pushpin

ICON KEY

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

Pushpin is a small Python script that identifies every tweet, flicker pic, and Youtube video within an area of a specific Geo address.

Lab Scenario

For a security assessment, you can gather information about social networking data such as tweets, profiles, pictures, etc. at a specified location. As a professional ethical hacker you should be able to extract such social networking information from a specified geographical location. This lab will demonstrate how to collect information from social networking sites from a specific geographical location.

Lab Objectives

The objective of this lab is to demonstrate how to collect social networking media files and map file using Recon-ng Pushpin module.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 02 Footprinting and Reconnaissance

Lab Environment

To carry out the lab, you need:

- Windows Server 2012 running as host machine
- Kali Linux running as virtual machine
- Web browser with internet access

Lab Duration

Time: 10 Minutes

Overview of Recon-ng Pushpin

Pushpin's integration into the Recon-ng enables pen testers to collect information on social networking sites such as the profile name, latitude, longitude, time, profile URL, screen name, etc.

Lab Tasks

TASK 1

Launch recon-ng

1. Launch **Kali Linux** virtual machine from your Hyper-V Manager.
2. Launch new terminal window, now type **recon-ng** and press **Enter**.
3. The Recon-ng console opens, as shown in the screenshot below.

FIGURE 12.1: Launching recon-ng

TASK 2

Add a Workspace

4. Now select workspaces, type **workspaces select <Workspace name>** and press **Enter**.

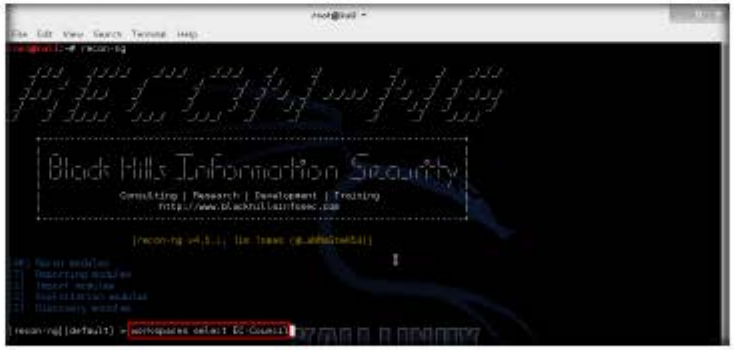


FIGURE 12.2: Adding a Workspace

TASK 3

Configure Location

5. Type **show schema** and press **Enter** to view default schemas.

FIGURE 12.3: Viewing the Schema

6. This command displays the list of schemas in Recon. Now choose **street_address** from the **locations** schema.

Pushpin – Awesome little Python script that will identify every tweet, flicker pic and Youtube video within an area of a specific Geo address.

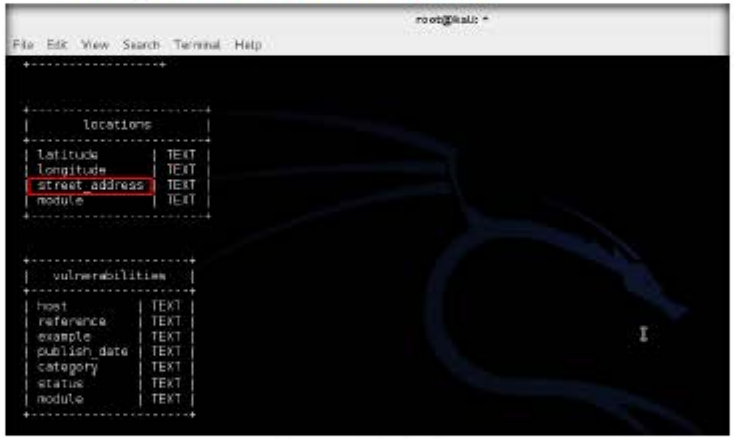


FIGURE 12.4: Viewing the Schema

7. Now type **add locations** and press **Enter**.

8. Press **Enter** twice to get the **street_address (Text):** field, as shown in the below screenshot.

Recon-ng persists module options between sessions. If upgrading to >= 3.3.0, it is recommended that all old configuration files be purged (rm ~/.recon-ng/workspaces/*/config.dat). Failure to remove old configuration files will result in a failure to load saved option values.

FIGURE 12.5: Adding Location

9. Open a web browser and Google the target's organization address.
10. **Copy** the address as shown in the screenshot below.

Install Recon-ng apt-get update && apt-get install recon-ng

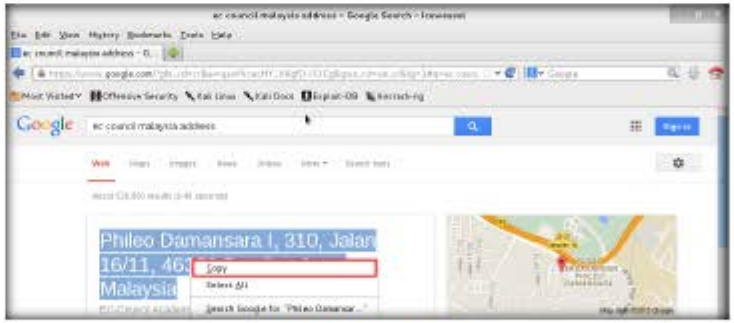


FIGURE 12.6: Adding Location

11. Paste the address in the **street_address (Text):** field, and press **Enter**.

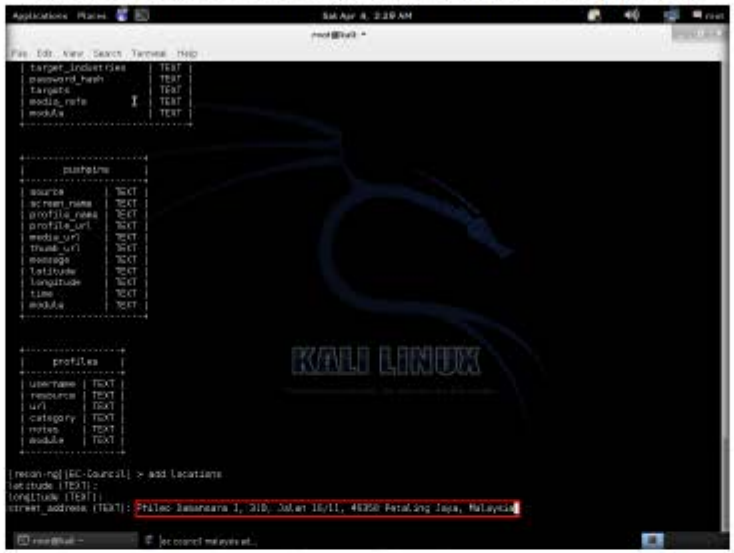


FIGURE 12.7: Adding Location

The Recon-ng project consists of a one-man development team in terms of sustaining the framework. When things break, as they often do when dealing with evolving web technologies, users don't go to the module developer, they go to the Recon-ng Issue Tracker or directly to me.

12. Now type **show locations** and press **Enter**, this command displays the entered address.

As the framework grows, module issues become more and more frequent. I needed a way to "trim the fat" in the framework and determine the best approach to maintaining broken modules.

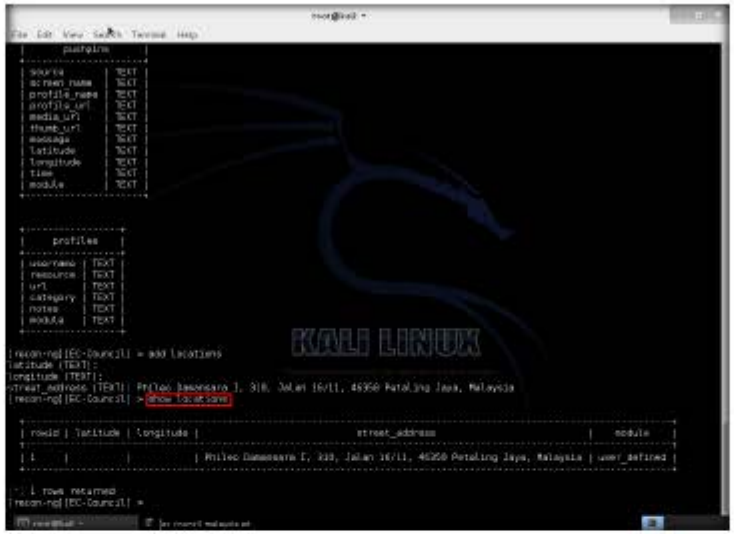


FIGURE 12.8: Viewing the Added Location

13. Now type **load geocode** command and press **Enter** to list out the geocode available exploits.

Therefore, I decided to add an analytics element (eab6307) which would allow me to track the most commonly used modules.

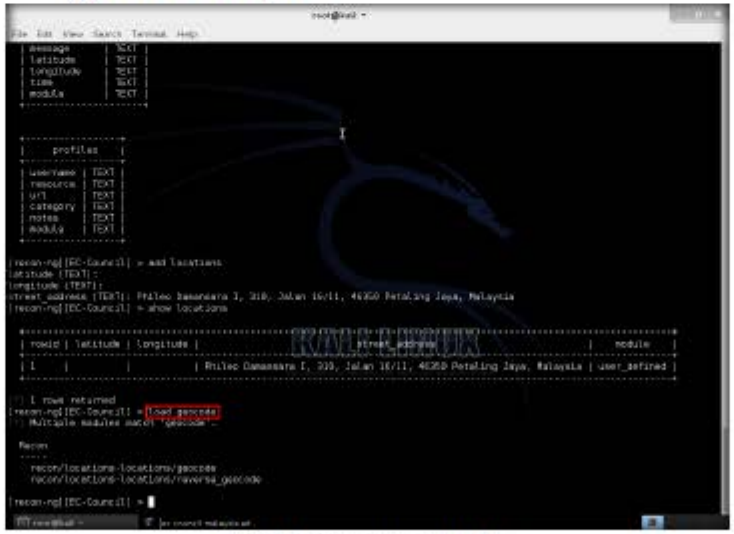


FIGURE 12.9: Searching for geocode Module

14. Now type **load recon/locations-locations/geocode** and press **Enter**

That way, when a user comes to me and says, "There is a problem with module X." I can look at my analytics and determine whether or not it is worth the effort to fix myself, ask them to fix, or remove from the framework all together.

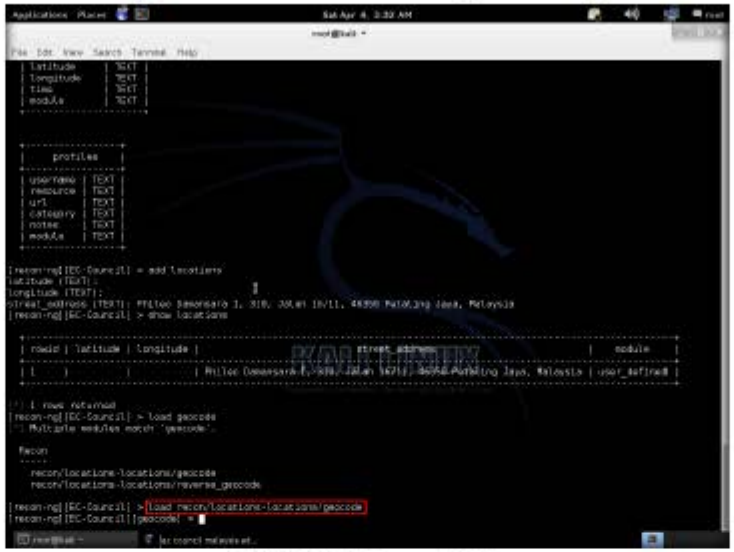


FIGURE 12.10: Loading geocode Module

15. Now type **run** command and press **Enter** to get **Latitude** and **Longitude** information of the provided address.

People use the Internet every day to visit web pages and logically attribute themselves to shady places.

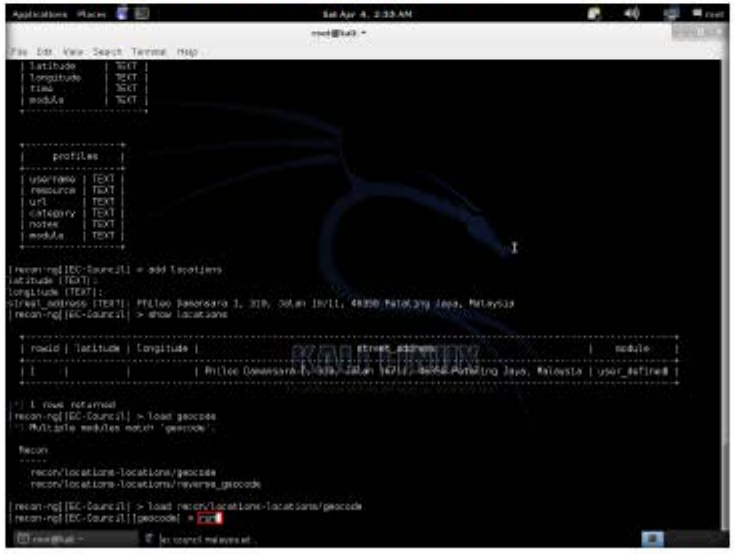


FIGURE 12.11: Running the Module

16. The screenshot below shows the latitude and longitude information for the provided address.

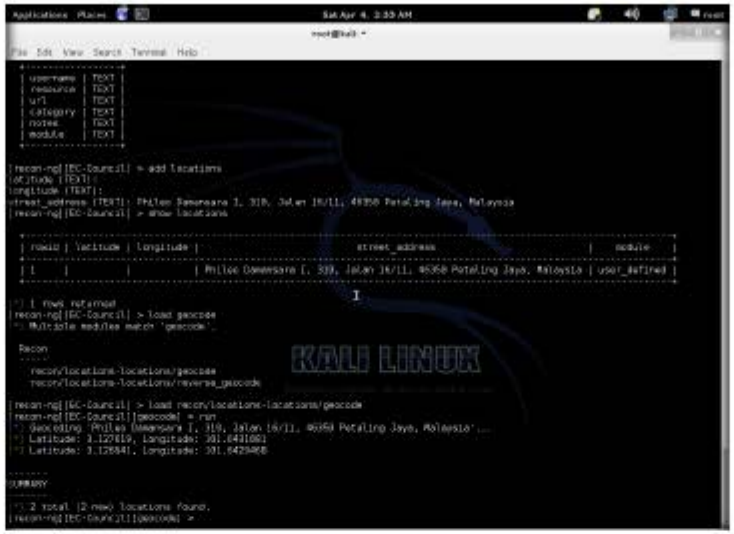


FIGURE 12.12: Viewing the Location

There is no such thing as "leaking" an external IP address. It is a part of layer 3 communication and the way the Internet works.

17. Now type **show locations** and press **Enter** to view the updated location information.

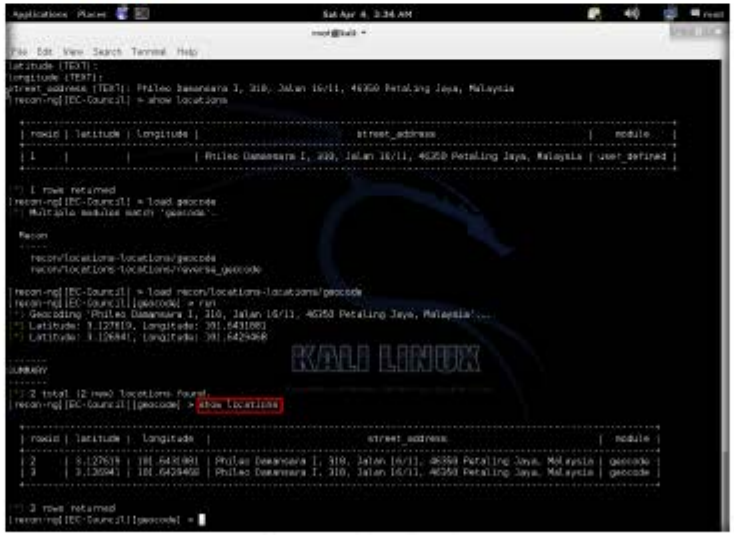


FIGURE 12.13: Viewing the Locations

If you don't want your IP leaked, don't use the Internet, or use an anonymizing service. There is no targeting or harvested information included in the analytics. I encourage users to watch the traffic and validate for themselves.

TASK 4

Obtain Information

18. Type **search locations-** and press **Enter** to list out the information gathering options.

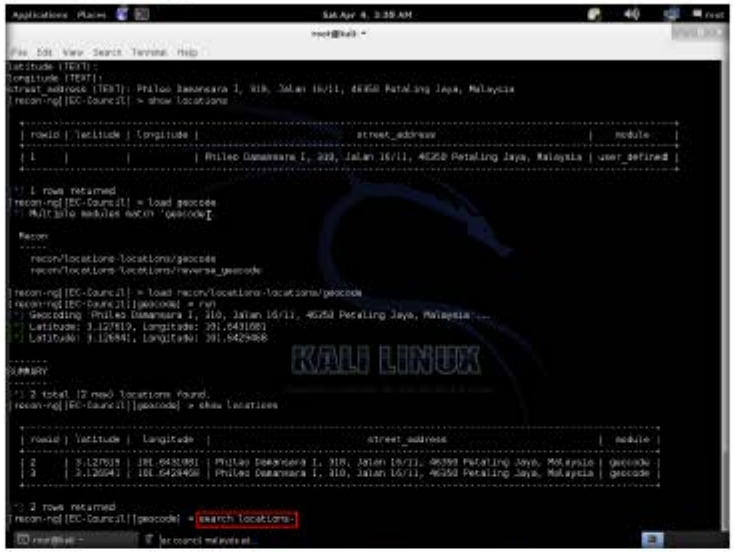


FIGURE 12.14: Searching for Locations Modules

19. The screenshots below show the Recon modules from which to gather information.

20. Type **load picasa** and press **Enter**.

The first time Recon-ng runs, it creates a file in the user's home ~/.recon-ng directory called .cid.

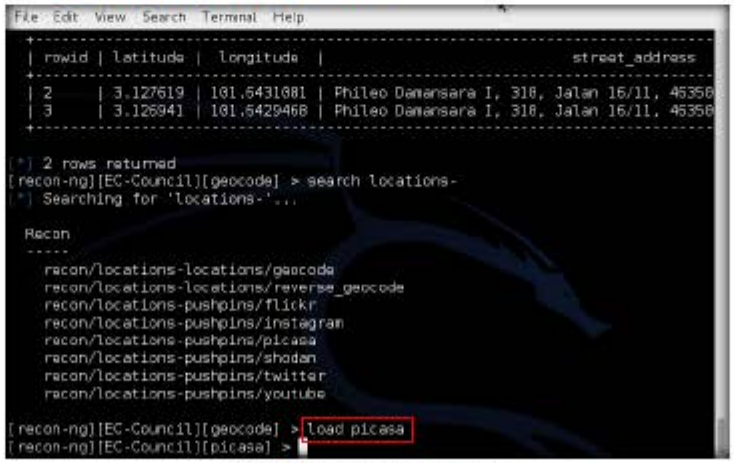


FIGURE 12.15: Loading a Location Module

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

21. Type **show options** and press **Enter** to view **picasa** values and details.

Analytics requests are sent each time a module is loaded using the load or use command.

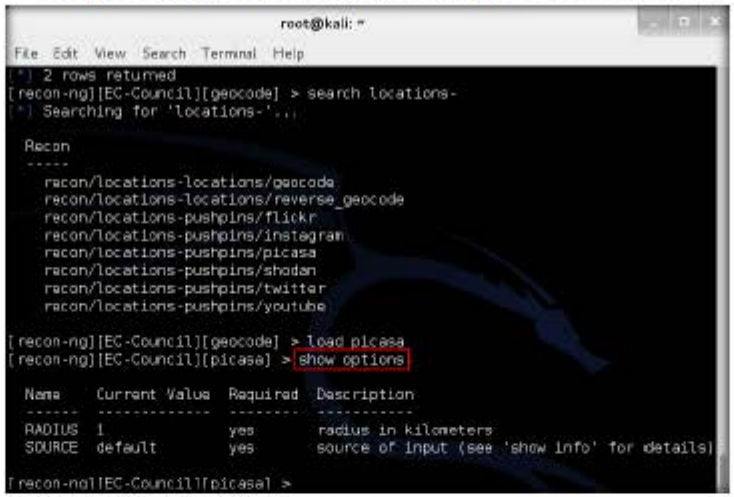


FIGURE 12.16: Viewing Options

22. Type **show info** and press **Enter**. This displays the information related to the location of Picasa as shown in the following screenshot:

The analytics request includes the UUID, the module name, and the version of Recon-ng. No analytics requests are made when loading custom modules (modules that reside in the users home ~/.recon-ng/modules/ directory), and the entire system can be disabled by running Recon-ng with the --no-analytics flag.

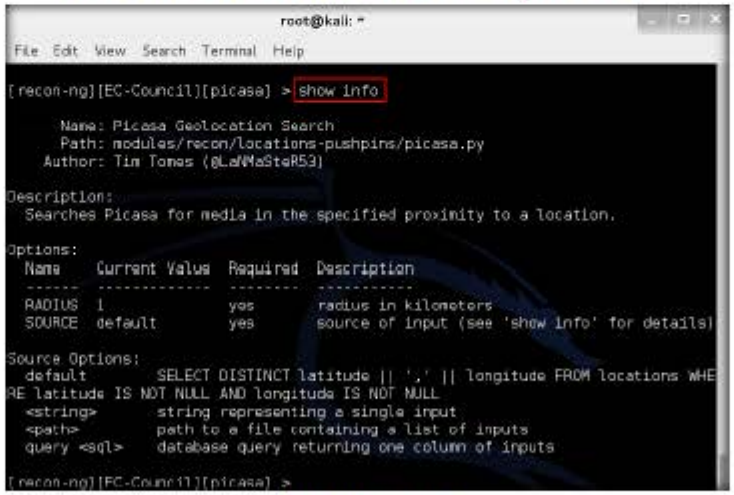


FIGURE 12.17: Viewing Info

23. Type **run** and press **Enter**. The pushpin plugin initiates and begins to collect data associated with Picasa in the default location (because no location was specified), as shown in the following screenshot:

If external shell scripting is preferred, the framework includes a tool called ./recon-cli.py which makes all of the functionality of the Recon-ng framework accessible from the command line. Use ./recon-cli.py -h for information on runtime options.

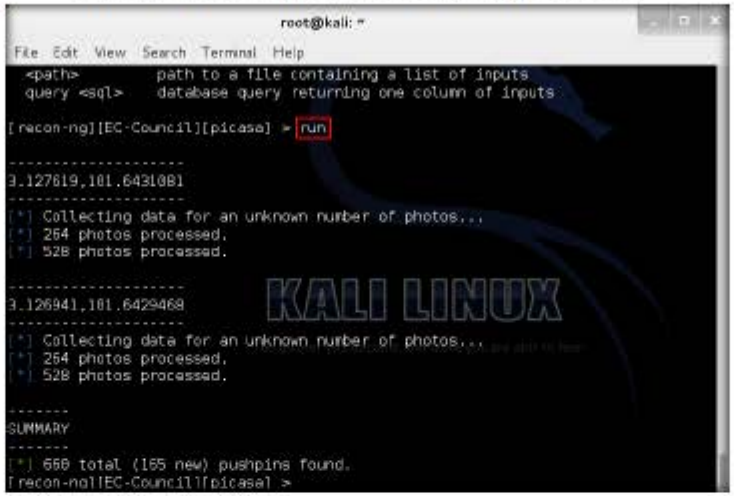


FIGURE 12.18: Running the Module

24. Type **dashboard** and press **Enter** to view the results summary.

To make it easy to create resource files, the framework is equipped with the ability to record commands. The "record" command gives users the ability to start and stop command recording, or check the current recording status.

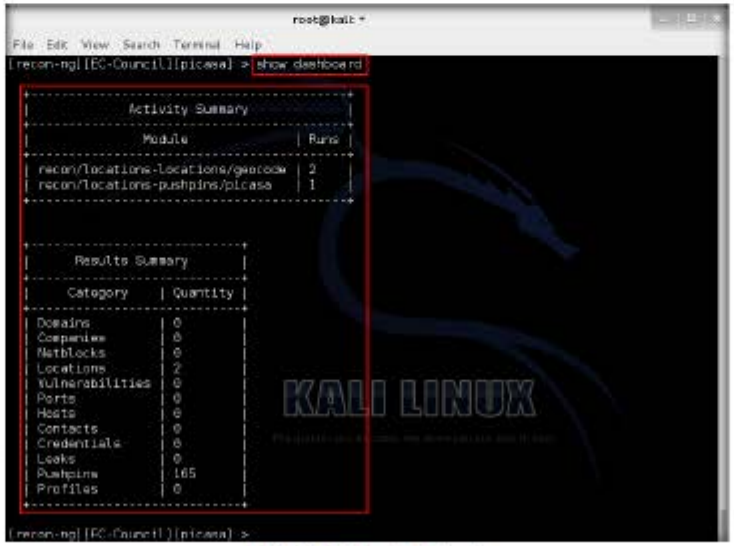


FIGURE 12.19: Viewing Dashboard

25. Type the command **load reporting/pushpin** and press **Enter**.

The destination file for the recorded commands is set as a parameter of the "record start" command, record start <filename>. Use help record for more information on the "record" command.

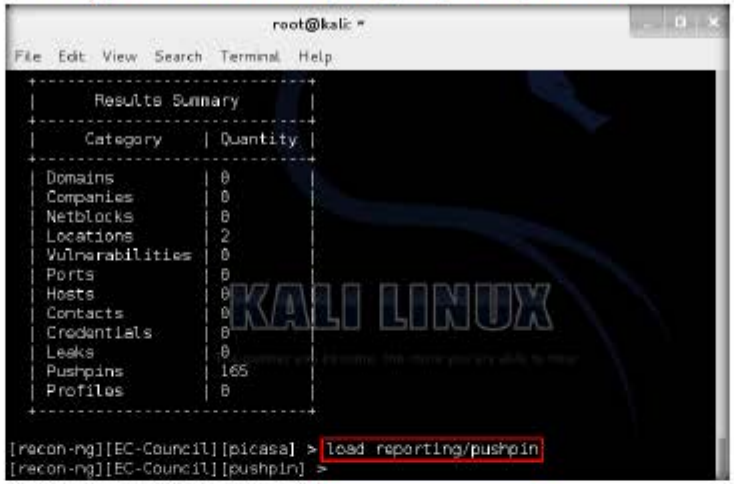


FIGURE 12.20: Loading a Reporting Module

26. Type the command **show options** and press **Enter** to view the options required to run pushpin on Picasa.

The entire framework is scriptable through the use of a resource file. A resource file is a plain text file containing a list of commands for the framework.

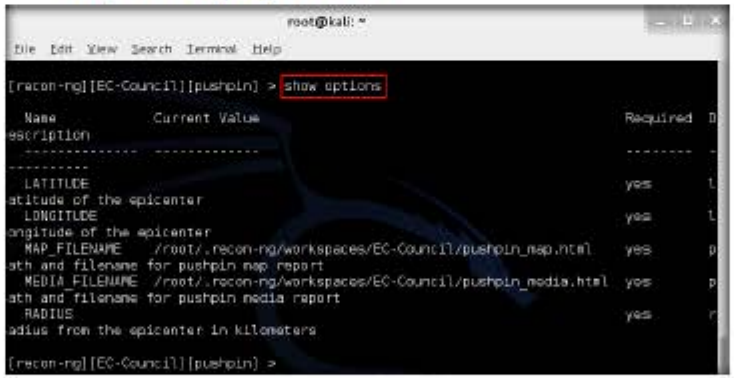


FIGURE 12.21: Viewing Options

27. Type the command **show locations** and press **Enter** to view the location that you have added in the previous steps.

28. Make a note of the latitude and longitude.

Bing API Key (bing_api) - Sign up for the free subscription to the Bing Search API here. Sign in to the Windows Azure Marketplace and go to the "My Account" tab. The API key will be available under the "Account Keys" page.

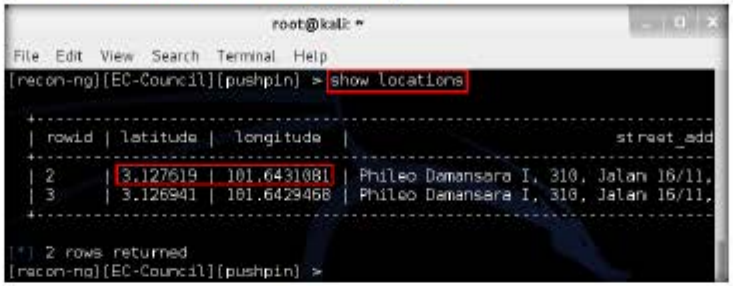


FIGURE 12.22: Viewing Locations

TASK 5

Generate a Report

29. Issue the following commands:

    a. **set LATITUDE [latitude obtained in your lab]**

    b. **set LONGITUDE [longitude obtained in your lab]**

    c. **set RADIUS 1**

    d. **set MAP_FILENAME /root/Desktop/picasa_map.html** (By issuing this command, the file named **picasa_map.html** will be saved to **Desktop.**)

    e. **set MEDIA_FILENAME /root/Desktop/picasa_media.html** (By issuing this command, the file named **picasa_map.html** will be saved to **Desktop.**)

A recorded session of all activity is essential for many penetration testers, but builtin OS tools like "tee" and "script" break needed functionality, like tab completion, and muck with output formatting.

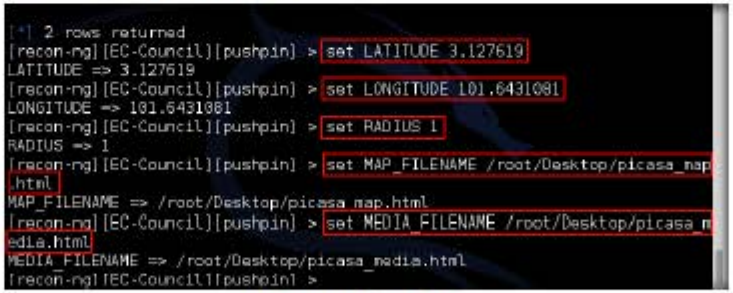


FIGURE 12.23: Configuring Options

30. Now, type **run** and press **Enter**. This extracts the media and map information related to Picasa in the specified location and stores the files on the Desktop.

The destination file for the spooled data is set as a parameter of the "spool start" command, spool start <filename>. Use help spool for more information on the "spool" command.

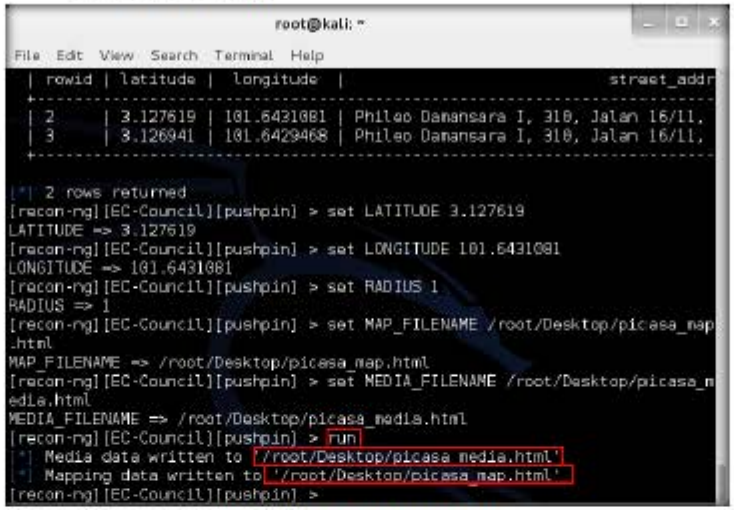


FIGURE 12.24: Running the Reporting Module

31. The resulting files open automatically in the Iceweasel web browser, as shown in the following screenshot:

Every piece of information stored in the Recon-ng database is a potential input "seed" from which new information can be harvested. The "add" command allows users to add initial records to the database which will become input for modules.

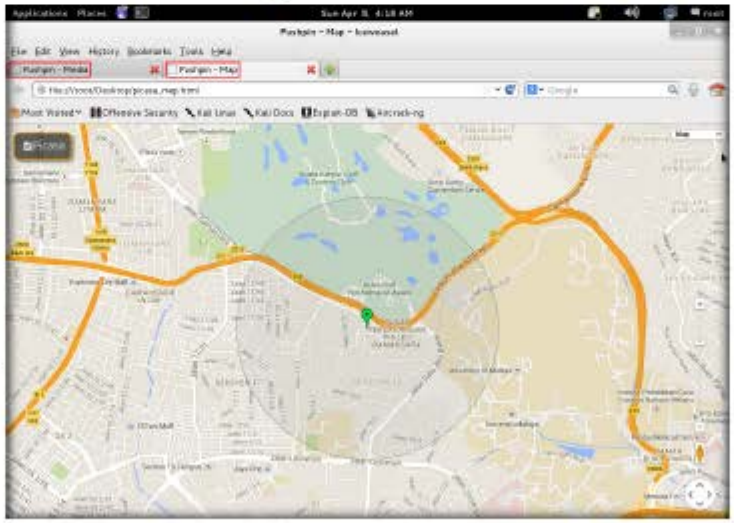


FIGURE 12.25: Viewing the Report

32. Use both the tabs to examine the information that was obtained.
33. Follow Steps 20-32 to extract information associated with Flickr, Instagram, etc. in a specified location.

Note: Some recon modules may require Google API keys, without which you cannot extract information. Google/Bing search engines flag multiple continuous search queries as bot activity and display errors such as "Auto-resuming in 15 minutes." You need to purchase and use Google/Bing Search APIs to avoid this.

Lab Analysis

Analyze and document the results related to 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

13

Automated Fingerprinting of an Organization Using FOCA

ICON KEY

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

FOCA (Fingerprinting Organizations with Collected Archives) is a tool that reveals metadata and shrouded data. These archives may be on site pages, and can be downloaded and dissected with FOCA.

Lab Scenario

Useful information may reside on the target organization's website in the form of pdf documents, Microsoft Word files, etc. As an ethical hacker, you should be able to extract valuable data including metadata and hidden information from such documents. This lab will demonstrate how to extract valuable information from website archives.

Lab Objectives

The objective of this lab is to demonstrate how to extract documents and domain information using FOCA. Students will learn how to perform:

- Metadata Extraction
- Network Analysis
- DNS Snooping
- Search for common files
- Juicy Files
- Proxies Search
- Technologies Identification
- Fingerprinting
- Leaks
- Backups Search
- Error Forcing
- Open Directories Search

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 02 Footprinting and Reconnaissance

Lab Environment

To carry out the lab you need:

- FOCA, which is located at **D:\CEH-Tools\CEHv9 Module 02 Footprinting and Reconnaissance\Footprinting Tools\Foca\bin**. You can also download the latest version of FOCA from the link https://www.elevenpaths.com/labstools/foca/index.htm. If you decide to download the latest version, then **screenshots** shown in the lab might differ.
- Windows Server 2012

Lab Duration

Time: 10 Minutes

Overview of FOCA

FOCA examines a wide mixture of records, with the most widely recognized being Microsoft Office, Open Office, or PDF documents. It may also work with Adobe InDesign or SVG files.

Lab Tasks

TASK 1

Launch FOCA

1. To launch **FOCA,** navigate to **D:\CEH-Tools\CEHv9 Module 02 Footprinting and Reconnaissance\Footprinting Tools\Foca\bin** and double-click **FOCA.exe**.
2. If the **Open File - Security Warning** pop-up appears, click **Run**.
3. The **FOCA** main window appears, as shown in the figure below.

FOCA began as a metadata analysis tool to draw a network based on said metadata.

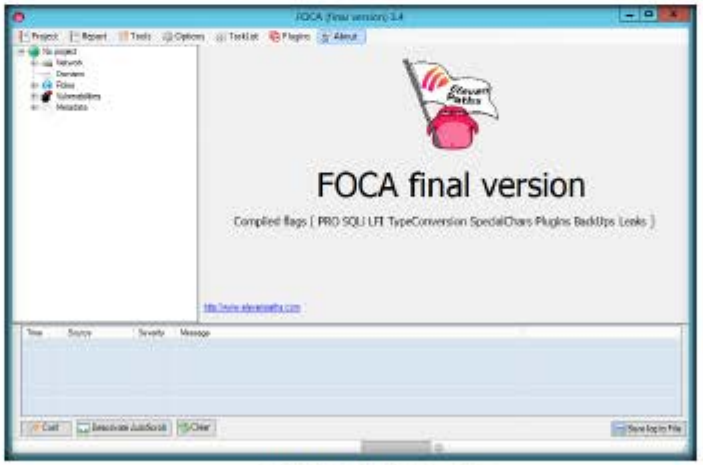


FIGURE 13.1: FOCA main window

TASK 2

Creating New Project

4. Create a new project by navigating to **Project,** and click **New project** on the menu bar.

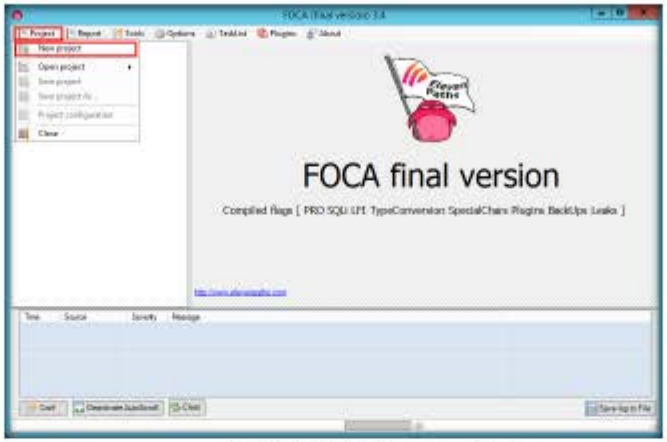


FIGURE 13.2: FOCA creating a new project

FOCA includes a server discovery module, whose purpose is to automate the servers search process using recursively interconnected routines.

5. The FOCA new project wizard appears as shown in the figure below:
   a. Enter a Project name in **Project name** field.
   b. Enter domain website in **Domain website** field.
   c. You can leave the optional Alternative domains field empty.

Web Search

Searches for hosts and domain names through URLs associated to the main domain. Each link is analyzed to extract from it new host and domain names.

6. Click **Folder** to save the document that is extracted by FOCA in the **Folder where save documents** field, leave the other settings to default, and click **Create**.

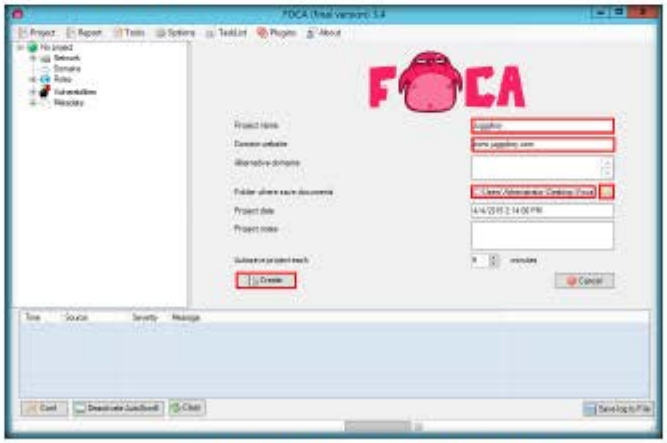


FIGURE 13.3: FOCA providing details for new project

DNS Search

Each domain is checked to ascertain which are the host names configured in NS, MX, and SPF servers to discover new host and domain names.

7. Save project as window appears provide desired location to save the FOCA project and type file a name in **File name** field and click **Save**.

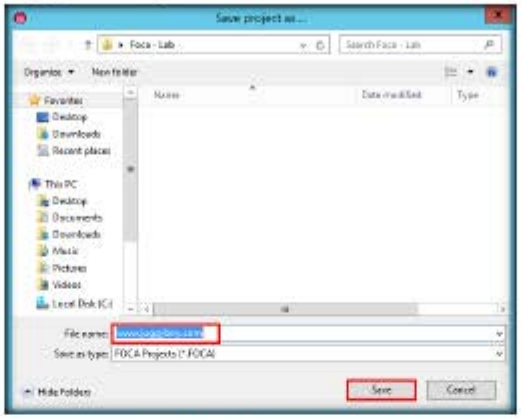


FIGURE 13.4: FOCA Save project as window

PTR Scanning

To find more servers in the same segment of a determined address, IP FOCA executes a PTR logs scan.

8. Project Save successfully pop-up appears click **OK**.

IP resolution

Each host name is resolved by comparison to the DNS to obtain the IP address associated to this server name. To perform this task as accurately as possible, the analysis is carried out against a DNS that is internal to the organization.

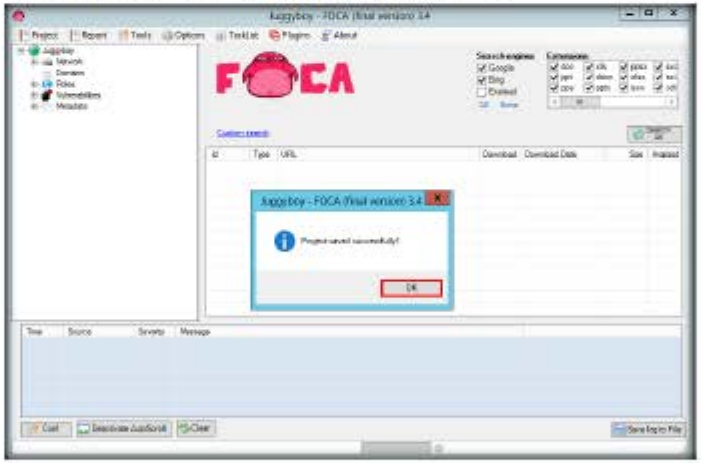


FIGURE 13.5: FOCA Project Saved

TASK 3

Extracting Domain Information

9. To extract the information of the targeted domain, click **Search All**.

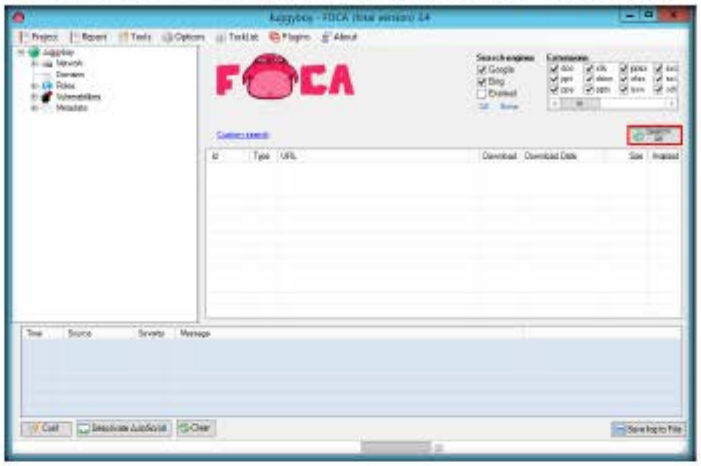


FIGURE 13.6: FOCA Extracting Information

Bing IP

For each IP address discovered, a search process is launched for new domain names associated to that IP address.

10. The **Search All** button automatically toggles the **Stop** button and you can see the result in the lower panes.

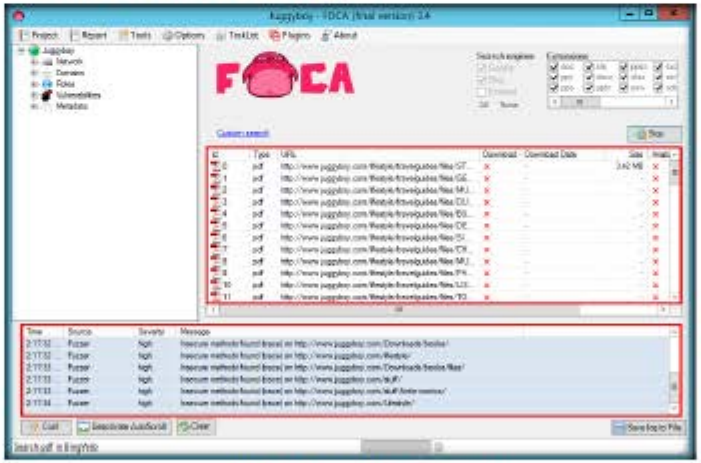


FIGURE 13.7: FOCA Extracted Information

Common names

This module is designed to carry out dictionary attacks against the DNS. It uses a text file containing a list of common host names such as ftp, pc01, pc02, intranet, extranet, internal, test, etc.

DNS Prediction

Used for those environments where a machine name has been discovered that is reason to suspect that a pattern is used in the naming system.

11. Now that the file information is stored in the domain, you can view it. To view the information, right-click the file and click **Link → Open in browser** from the context menu.

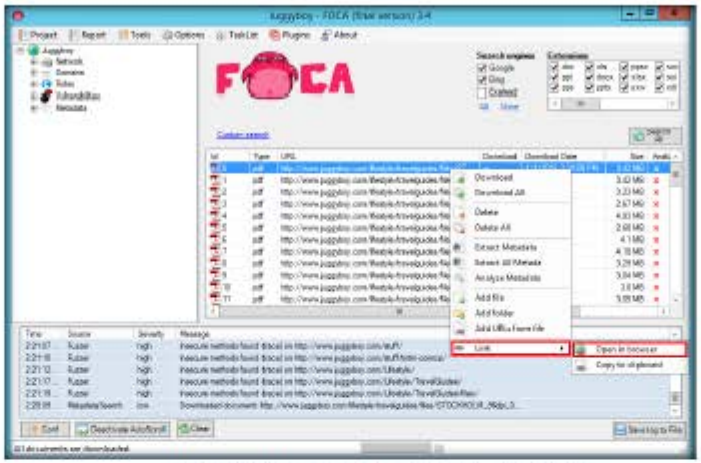


FIGURE 13.8: FOCA examining the extracted information of the file

Robtex

The Robtex service is one of many services available on the Internet to analyze IP addresses and domain names. FOCA uses it in its attempt to discover new domains by searching the information available in Robtext on the latter.

12. You have now extracted the files from the domain by using **FOCA**.

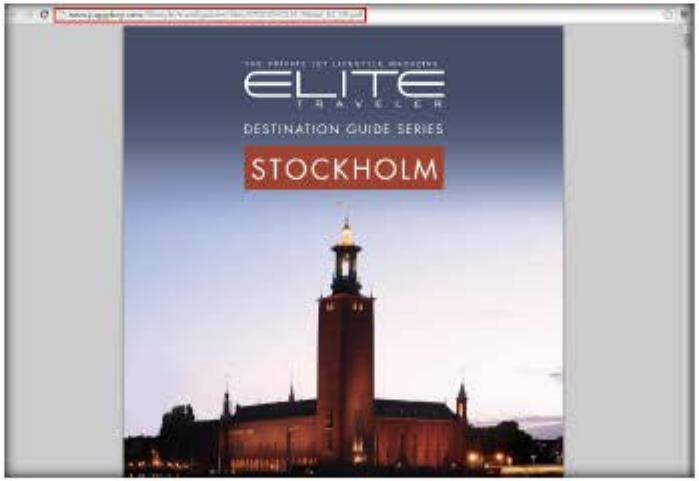


FIGURE 13.9: FOCA Extracted file

The documents are searched for using three possible search engines: Google, Bing, and Exalead. The sum of the results from the three engines amounts to a lot of documents. It is also possible to add local files to extract the EXIF information from graphic files, and a complete analysis of the information discovered through the URL is conducted even before downloading the file.

TASK 4

Network Structure Information

13. Click **Network node** node in the left pane of the window to view the network structure.
14. If the domain has any of the associated **Clients** or **Servers** it displays the related information.

Note: In this lab the domain we used doesn't have associated clients or servers.

All the data extracted from all files, FOCA matches information in an attempt to identify which documents have been created by the same team and what servers and clients may be inferred from them.

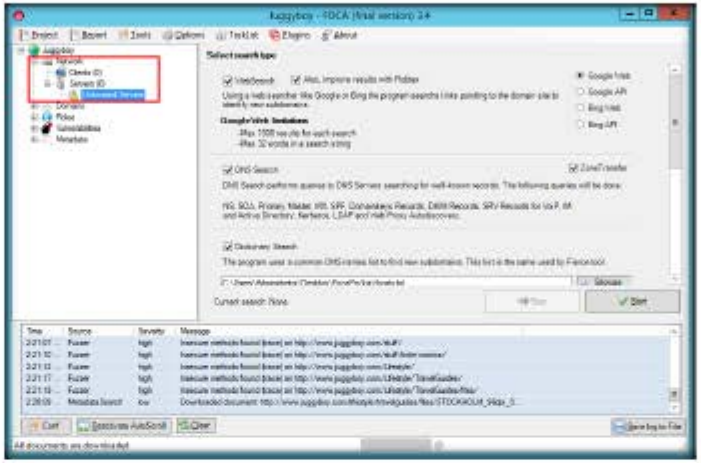


FIGURE 13.10: FOCA Network Information

TASK 5

Domain Information

15. Expand the **Domains** node and it displays the **Domain IP Address**.

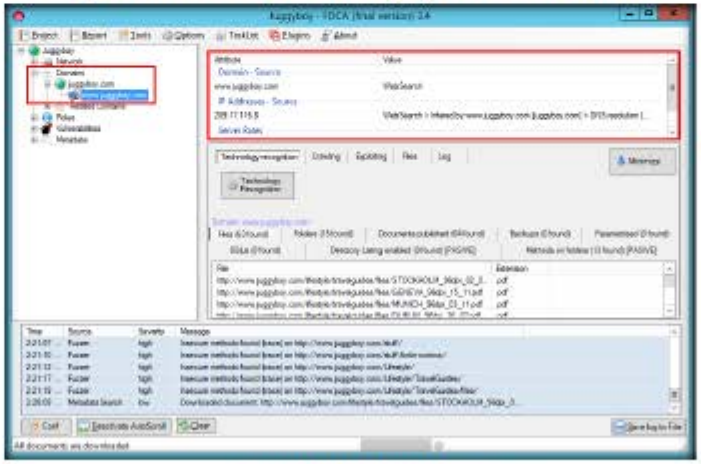


FIGURE 13.11: FOCA Domain Information

TASK 6

HTTP(s) Fingerprinting

16. Expand the **Roles** node, right-click on **Http**, and click **HTTP(s) Fingerprinting** from the context menu to fingerprint the site or domain.

FIGURE 13.12: FOCA HTTP(s) Finger Printing

17. Expand the **Https** node and click Domain to see the **IIS version** installed in the server in the right pane.

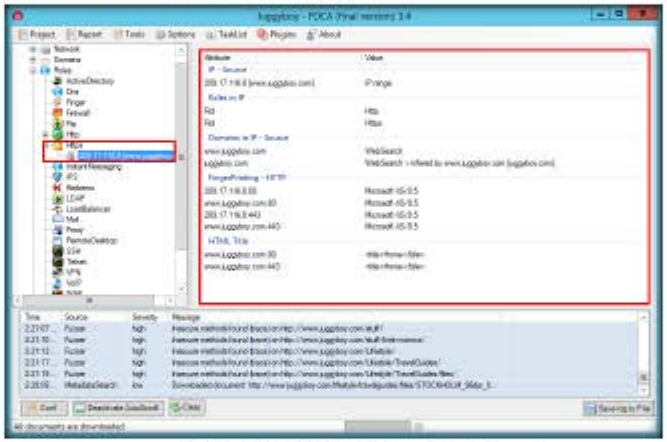


FIGURE 13.13: FOCA HTTP(s) Finger Printing Information

FOCA has a series of plugins to increase the functionality or number of attacks that can be carried out to elements obtained during the analysis.

Lab Analysis

Analyze and document the results related to 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 14

Identifying Vulnerabilities and Information Disclosures in Search Engines Using SearchDiggity

Search Diggity has a predefined query database that runs against the website to scan the related queries.

Lab Scenario

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

As a professional ethical hacker, you should be able to extract information on the target using an automated tool such as SearchDiggity. It uses Google to extract valuable information from the target domain. This lab will demonstrate extracting information using SearchDiggity

Lab Objectives

The objective of this lab is to demonstrate how to identify vulnerabilities and information disclosures in search engines using Search Diggity. Students will learn how to:

- Extract Meta Tag, Email, Phone/Fax from the web pages

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 02 Footprinting and Reconnaissance

To carry out the lab you need:

- Search Diggity is located at **D:\CEH-Tools\CEHv9 Module 02 Footprinting and Reconnaissance\Footprinting Tools\SearchDiggity**. You can also download the latest version of Search Diggity from the link http://www.bishopfox.com/resources/tools/google-hacking-diggity/attack-tools/. If you decide to download the latest version, then screenshots shown in the lab might differ.
- Windows Server 2012

Lab Duration

Time: 5 Minutes

Overview of SearchDiggity

Search Diggity is a primary attack tool of the Google Hacking Diggity Project. It is a MS Windows GUI application that serves as a front end to the latest versions of Diggity tools: GoogleDiggity, BingDiggity, Bing LinkFromDomainDiggity, CodeSearchDiggity, DLPDiggity, FlashDiggity, MalwareDiggity, PortScanDiggity, SHODANDiggity, BingBinaryMalwareSearch, and NotInMyBackYard Diggity.

Lab Tasks

TASK 1

Install Search Diggity

1. Navigate to **D:\CEH-Tools\CEHv9 Module 02 Footprinting and Reconnaissance\Footprinting Tools\SearchDiggity** and double-click **setup.exe**.
2. If the **Open File - Security Warning** pop-up appears, click **Run**.
3. If the **SearchDiggity Setup** window appears, click **Accept**.

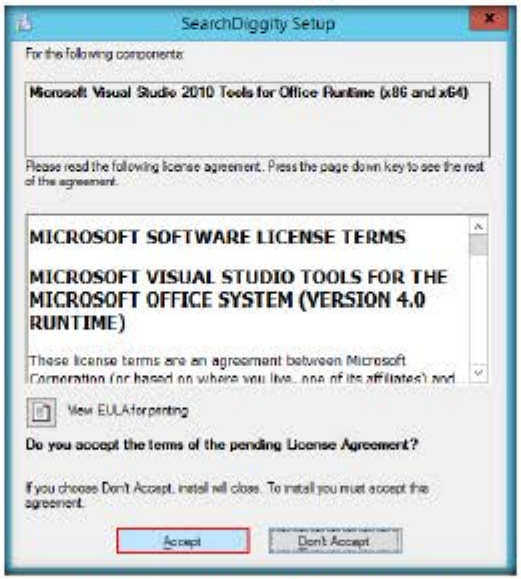


FIGURE 14.1: SearchDiggity Setup Wizard pop-up window

4. Search Diggity starts downloading the required applications and installs them.

GoogleDiggity is the primary Google hacking tool, utilizing the Google JSON/ATOM Custom Search API to identify vulnerabilities and information disclosures via Google searching.

5. Follow the wizard steps to install Search Diggity.

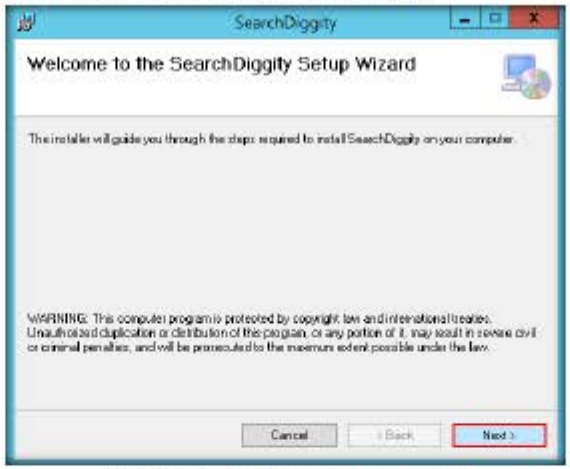


FIGURE 14.2: SearchDiggity Setup Wizard pop-up window

TASK 2

Add Proxies to Search Diggity

6. Launch **SearchDiggity** from the **Apps** screen.

FIGURE 14.3: Installed apps in Windows Server 2012 – Selecting Search Diggity

7. The Search Diggity main window appears with **Google Diggity** selected by default.

Queries – Select Google dorks (search queries) you wish to use in scan by checking appropriate boxes.

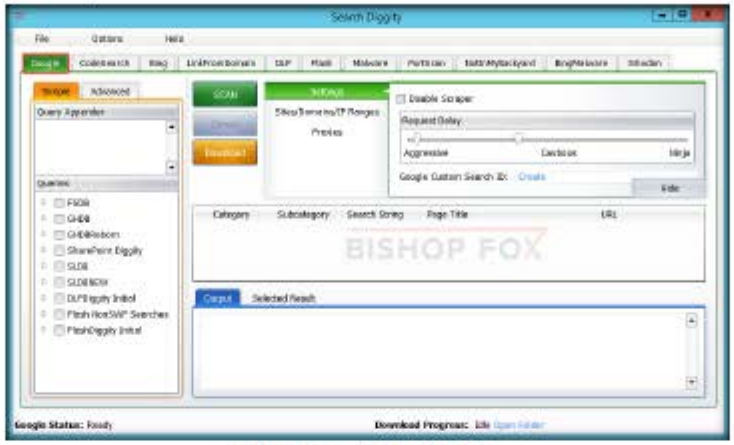


FIGURE 14.4: Search Diggity - Main window

Output – General output describing the progress of the scan and parameters used..

8. Select **Sites/Domains/IP Ranges** and type the domain name (here, **microsoft.com**) in the domain field. Click **Add**.

Import Button – Import a text file list of domains/IP ranges to scan. Each query will be run against Google with `site:yourdomainname.com` appended to it.

FIGURE 14.5: Adding a Domain

9. The added domain name appears in the box under the domain field, as shown in the following screenshot:

FIGURE 14.6: Search Diggity - Domain added

10. Select a **Query** from left pane that you wish to run against the website that you have added to the list, and click **Scan**.

Note: In this lab, we have selected the query **SWF Finding Generic** under **FlashDiggity Initial**. You can select other queries to run against the added website.

TASK 3

Run Query against a website

When scanning is kicked off, the selected query is run against the complete website.

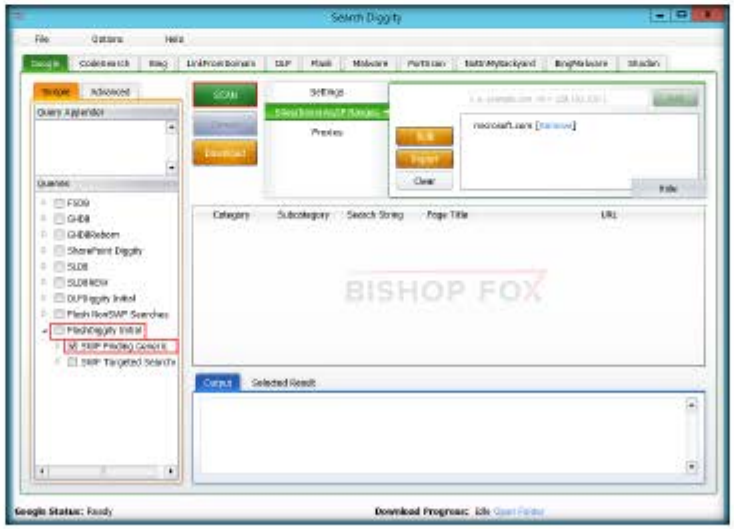


FIGURE 14.7: Search Diggity – Selecting query and Scanning

11. On completion of the scan, all the URLs that contain the SWF extensions are listed and the Output has the query results

Results Pane - As scan runs, results found will begin populating in this window pane.

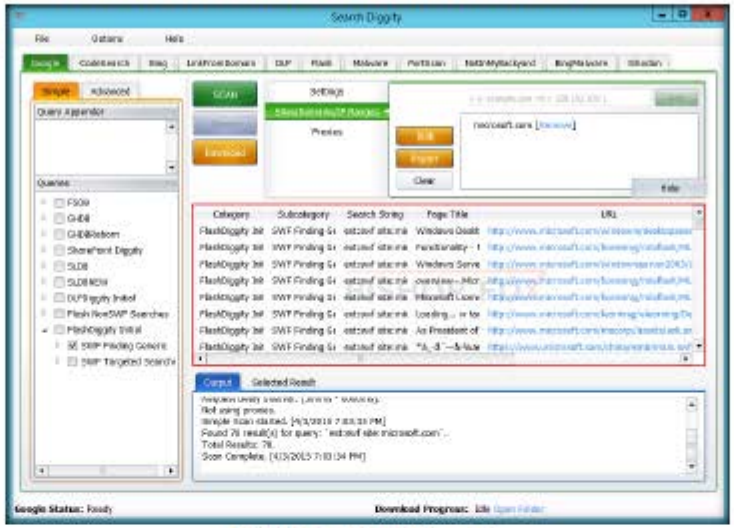


FIGURE 14.8 Search Diggity - Output window

Lab Analysis

Collect different error messages to learn the vulnerabilities, and note the information disclosed about the website.

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

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