## Lab 4-01: Information Gathering Using Maltego

### Scenario

You are working with a military organization that deals in cyber operations. You are assigned a task to gather information about a target website using OSINT techniques. The website in question is suspected of hosting malicious content and engaging in illicit activities. Your objective is to conduct thorough reconnaissance using OSINT techniques to uncover relevant information about the website’s infrastructure, associated entities, and potential vulnerabilities.

### Solution

You are assigned a task to gather information about a target. Maltego has proven to be an invaluable tool in your OSINT arsenal for gathering comprehensive information about the target website. Maltego is a powerful OSINT and data visualization tool that allows you to conduct automated reconnaissance and gather intelligence from various publicly available sources.

Using Maltego, you can perform a comprehensive analysis of the target website’s digital footprint, uncovering crucial details such as IP addresses, email addresses, documents, and web technologies utilized

|  |
| --- |
| 1. Open the Maltego installer file and start installing. Click **Next** to continue.    2. Select **Maltego CE (Free)**, which is the Community Edition. You need to register for the free account by clicking on the **Register** button.    3. It shows the Welcome screen. Click on the **Next** button.    4. You registered earlier, so just login with the registered credentials. Click on the **Next** button.    5. Select the **Maltego public servers** option to install Transforms and click **Next**.    6. Select the **Run a machine** option and click the **Finish** button.    7. Once the installation is completed, you will see the Home page displaying the plugins. Click the **New** button to open a new graph.    8. Search for the **web** in the search box on the left pane under the **Entity Palette**. Drag and drop the **Website** Entity into the empty graph. You can edit the domain name and write the target domain name for which you want to gather information. Here, **www.maltego.com** is used.    9. Right-click on the **Entity**, and it will display the **Transforms** list. A Transform is an operation that you want to perform on the target Entity. Click on the **To IP Address [DNS]** Transform to gather the IP Addresses associated with **www.maltego.com**.    10. It shows the IP Addresses associated with **www.maltego.com**. You can also see the output in the **Transform Output** window below.    11. Explore other options, such as running the **Mirror: Email addresses found** Transform.    12. It shows the email addresses associated with the target domain.    13. Run the **To Phone Numbers [within Properties]** Transform to gather the phone numbers.    14. It is not showing any phone number in the graph, and it says **Transform to Phone Numbers [within Properties] done** in the output window, which means there may be some information you will be unable to gather, or that information simply does not exist.    15. Run the **To Web Technologies [BuiltWith]** Transform to gather information about the technologies used by the target domain.    16. It shows information about the technologies used by the target domain.    17. You can delete the Transforms by selecting them and clicking the **Delete** button on the keyboard. Click **Yes** when it asks you to confirm.    18. Try another Transform: **To Snapshots of Files (Extensions) [Wayback Machine]** to gather the old documents that may have been archived, or you are not able to find them on Google.    19. It asks you to enter the file extensions you want to search. Keeping it default here, clicking **Run**.    20. It shows the gathered PDF documents that may have been archived, or you are not able to find them on Google.    21. You can select a document Entity and copy the URL. Open the URL in the browser to open the document. |

## Lab 4-02: Find Metadata and Hidden Information Using FOCA

### Scenario

Your organization’s cybersecurity team has assigned you a critical task to gather comprehensive information about a target website using Open Source Intelligence (OSINT) techniques. The target website, belonging to a potential competitor, has recently emerged as a significant player in the industry, and there is a pressing need to understand its digital footprint, infrastructure, and potential vulnerabilities. As a seasoned OSINT analyst, you recognize the importance of this mission and are determined to leverage the best tools and techniques to uncover valuable insights.

### Solution

To accomplish the task of gathering information about the target website, one effective OSINT technique is to utilize Fingerprinting Organizations with Collected Archives (FOCA). FOCA is a powerful reconnaissance tool specifically designed to extract metadata and hidden information from various search engines, such as Google, Bing, and DuckDuckGo. By leveraging FOCA, you can conduct a comprehensive analysis of the target domain to uncover valuable insights such as metadata associated with web pages, hidden files, and directory structures.

|  |
| --- |
| 1. Download FOCA from this website: **https://softradar.com/foca/**. Open the file **FOCA** after you have downloaded it.    2. It shows an error **Database not found**, so you have to download and install the SQL database first, then try opening the **FOCA** application file again. Download the SQL database server from here: **https://www.microsoft.com/en-us/sql-server/sql-server-downloads**.    3. Once the application is open, you will see a display like this. It shows the project details on the left-hand pane, and the new project configuration on the right-hand pane.    4. Create a new project by entering the **Project name**, **Domain website**, and the destination **file location** where you want to save the project file. Click on the **Create** button to create the project.    5. The project is saved successfully.    6. Click on the **Settings** button below.    7. Uncheck every **Module filter** except FOCA to use it.    8. You can select all the **Search Engines** and **Extensions** to find all these files using the checked search engines. Click on the **Search All** button to start searching.    9. It shows the URLs of the PDF files found.    10. Right-click on the **Download** column and click **Download All** to download all the files.    11. It indicates that the files are successfully downloaded with the **green** dots in the **Download** column.    12. Right-click on the **Download** column again and click the **Extract All Metadata** option to extract all the metadata of the files.    13. Right-click on the **Download** column again and select the **Analyze All Metadata** option to analyze the metadata of the files.    14. Expand the **Metadata Summary** object on the left-hand pane to see the metadata organized in different categories.    15. Select the **Users** object under the **Metadata Summary** object to see the users who may have contributed to the gathered documents.    16. You can select a particular document under **Document Analysis > Files > PDF** objects. It shows all the metadata related to the selected document in the right-hand pane.    17. Right-click the document and click **Open document** to open the document in the browser. |

## Lab 4-03: Information Gathering Using Fsociety

### Scenario

As a cybersecurity analyst assigned by your organization's threat intelligence team, you are tasked with conducting an Open Source Intelligence (OSINT) assessment of a competitor’s public-facing website and associated digital infrastructure. The objective is to produce a lawful, non-intrusive intelligence brief that characterizes the target’s external attack surface, public misconfigurations, exposed services, and indicators of risk that could affect your sector. Before beginning, obtain written authorization from your management and ensure the engagement adheres to legal, ethical, and corporate policies. OSINT activities must be strictly passive and must not attempt unauthorized access or disruption.

### Solution

One effective OSINT technique to gather information about open ports and associated services regarding the target domain is to utilize Fsociety. Fsociety is a versatile OSINT tool known for its capabilities in reconnaissance and information gathering. By leveraging Fsociety, you can conduct a thorough scan of the target domain to identify open ports and the services running on them.

|  |
| --- |
| 1. Use the **git clone https://github.com/Manisso/fsociety.git** command to download Fsociety. Use the **cd fsociety** command to move into the **fsociety** folder.    2. Use the **./fsociety.sh** command to install Fsociety.    3. Use the **./fsociety.py** command to run Fsociety.  4. You can see that it shows the **zsh: permission denied: ./fsociety.py** error message, which means you do not have permission to **execute** the file or script.  5. Use the **ls –l** command to list all the files in the **fsociety** folder with details, where you can see the read, write, and execute permissions of the files. **Fsociety.py** has only read and write permissions.    6. Use the **chmod +x fsociety.py** command to add executepermission to this script.  7. Now, if you see the details using the **ls –la** command, you can see that it has read, write, and execute (rwx) permissions.    8. Use the **./fsociety.py** command to run the Fsociety script. It runs this time. Type **1** to select **Information Gathering** among the other options and hit **Enter**.    9. Type **1** to select **Nmap – Network Mapper** as your tool for information gathering. Press **Enter**.    10. Enter the target domain, **certifiedhacker.com,** in this case. Type **2** to select the scan type **Port Scan [-Pn]** and hit **Enter**.    11. It starts scanning and shows the result that lists the open ports with their service names. Press **Enter** to continue.    12. Type **3** to select the **Host To IP** tooland hit **Enter**.    13. It gives you the IP Address associated with the target domain. |

## Lab 4-04: DoS Attack with PENTMENU

### Scenario

As a cybersecurity analyst, you have been assigned a challenging task by your organization’s security team: to launch a Denial of Service (DoS) attack against a target website. The target website belongs to a competitor in the e-commerce sector, and disrupting its online operations could provide a strategic advantage to your organization. The success of this operation relies on your expertise in performing such attacks while ensuring minimal risk of detection and legal ramifications.

**Solution**

To carry out the DoS attack against the target website, you can utilize a powerful tool known as Pentmenu, a Linux-based tool specifically designed for conducting penetration tests and network attacks. Pentmenu offers a suite of attack options, including various DoS techniques such as SYN flooding, ICMP flooding, and UDP flooding. Leveraging the capabilities of Pentmenu, you can launch a sophisticated and targeted attack against the target website, saturating its network bandwidth and exhausting its server resources to disrupt its availability.

|  |
| --- |
| **Download and Install Pentmenu**  1. Use the **git clone https://github.com/GinjaChris/pentmenu.git** command to download Pentmenu. Move into the Pentmenu directory using the **cd pentmenu** command.    2. Use the **ls –la** command to see the execution permission for the **pentmenu** file. Use the **./pentmenu** command to run the file.    **Using Pentmenu**  1. After running the script, type **2** to select **DOS**.    2. Type **1** to select **ICMP Echo Flood**. You can select any othertypeof DoS attack.    3. Enter the target website: **testphp.vulnweb.com** in this case.    4. Enter **r** to select a random IP Address as the source IP Address.    5. It has started the DoS attack, and it says **hping in flood mode, no replies will be shown**. |

## Lab 4-05: Perform Whois Lookup using DomainTools

### Scenario

You are an ethical hacker hired by InfoSec Dynamics, a technology firm specializing in secure application development. The company recently discovered that an unknown entity registered a domain with a similar name, “infosecdynamics-security.com,” potentially targeting their clients with phishing attacks. Concerned about the risk of domain spoofing and intellectual property misuse, the company’s management has asked you to investigate the suspicious domain and assess its origin and ownership details.

### Solution

Using DomainTools, a powerful Whois lookup and domain intelligence platform, your task is to gather as much information as possible about the target domain. This includes identifying its registrar, registration details, name servers, administrative and technical contacts, and other associated metadata. The goal is to analyze whether the domain is linked to malicious activities and to provide recommendations for mitigating potential risks.

By completing this lab, you will gain hands-on experience performing Whois footprinting and leveraging domain intelligence platforms like DomainTools. Your findings will help InfoSec Dynamics take appropriate actions, such as reporting the malicious domain to the registrar, implementing stronger client education on phishing threats, and monitoring for similar domain registrations in the future. This exercise highlights the critical role of Whois footprinting in proactive cybersecurity measures.

|  |
| --- |
| 1. Turn on the **Windows 11** virtual machine. Open any browser and go to [**http://whois.domaintools.com**](http://whois.domaintools.com).    2. The screenshot displays the Whois Lookup website. Now, type **www.certifiedhacker.com** into the search bar.    3. As shown in the screenshots, this search result displays the information related to the entered URL, **www.certifiedhacker.com**, including organizational details like IP address, location, name servers, and registration information.    4. Scroll down to see more information about the target website. This brings the example of using DomainTools to perform a Whois lookup to obtain information about a target organization to a conclusion.    6. An attacker can use this information to map the organization’s network, deceive domain owners through social engineering, and gather internal network information.  7. To obtain more target Whois information, use other Whois lookup tools like Batch IP Converter (http://www.sabsoft.com), SmartWhois (https://www.tamos.com), etc. |

## Lab 4-06: Gather DNS Information using nslookup Command Line Utility and Online Tool

### Scenario

A company has hired you to test its network infrastructure penetration. You must gather information about the company’s Domain Name System (DNS) configuration as part of your assessment. You must use a command-line tool and a web app to perform the task. You need to gather the target domain’s IP address and DNS information.

### Solution

A company has hired you to test its network infrastructure penetration. You are required to gather a target domain’s IP address and DNS information. To perform the task, you will use a Windows command-line tool known as nslookup and a web application. You may not have access to specific command-line tools on their network. In this case, you could use an online web app tool to perform nslookup instead.

|  |
| --- |
| 1. Open **Command Prompt** in your Windows machine and type the **nslookup** command. You will enter the **nslookup interactive mode** to type commands.    2. Enter the **set type=a** command and enter the target domain **certifiedhacker.com**. It will give you the corresponding IP address.    There are two servers; one is the default server on your local Windows machine, and the other is the server that hosts the target domain **certifiedhacker.com**. When the response comes from the local server, it is considered a **Non-authoritative** answer. When the response comes from the server that hosts the target, it is considered the **Authoritative** answer.  In this case, the answer is **Non-authoritative**. Certifiedhacker.com has the IP address **162.241.216.11**.  3. Use the commands  **set type=cname**  **certifiedhacker.com**    It lists the CNAME records for a domain because CNAME lookup is performed directly against the **Authoritative** name server of the target domain.  It gives two domain names: **ns1.bluehost.com** and **dnsadmin.box5331.bluehost.com**.  4. Enter the following commands to find the IP address of the name server.  **set type=a**  **ns1.bluehost.com**    It gives the IP address of the name server **162.159.24.80**.  Authoritative name servers have domain information. If the attacker finds the server name, he can also find its corresponding IP address. Hackers can perform DoS, DDoS, and other URL Redirection attacks if the IP address is found.  5. Perform the same tasks through the web application. Open any web browser and go to the website [**http://kloth.net/services/nslookup.php**](http://kloth.net/services/nslookup.php).    6. Enter the **target domain** in the domain field and select Query type **A (IPv4 address)**. Click **Look it up**.    7. You can see the IPv4 information. You can also select the **AAAA (IPv6 address)** Query type, as there are some attacks for IPv6, too.    8. It shows the DNS information related to IPv6. |

## Lab 4-07: Perform Network Tracerouting in Windows and Linux Machines

### Scenario

A company has hired you to test its network infrastructure penetration. As part of your assessment, you need to identify any potential vulnerabilities. You have to use the traceroute tool, which can be used to trace the route that network packets take from one location to another. Perform the task on both Windows and Linux machines.

### Solution

A company has hired you to test its network infrastructure penetration. As part of your assessment, you need to identify any potential vulnerabilities. Depending on the company’s network infrastructure, you may need to use Windows and Linux machines to assess. The Windows and Linux versions of the traceroute tool may implement the traceroute function differently, which means that the results obtained from the two tools may differ.

|  |
| --- |
| 1. Open **Command Prompt** on your Windows machine and type the **tracert certifiedhacker.com** command to trace the route or to see the hops in the path. It shows the IP addresses of the routers a packet goes through.    2. Use the **tracert /?** command to see the available options.    3. You must do the same process on Linux. Open your **Mate terminal** on your ParrotOS, type the **traceroute certifiedhacker.com** command, and press **Enter**.    4. It shows the IP addresses of the routers in the path to the destination.    You can also use tools like **Traceroute NG** ([**https://www.solarwinds.com**](https://www.solarwinds.com)) and **Visual Route** (<http://visualroute.com>). |

## Lab 4-08: Gather Information about a Target by Tracing Emails using eMailTrackerPro

### Scenario

You are an ethical hacker hired by SecureNova Solutions, a cybersecurity consulting firm, to investigate a recent spear-phishing attempt targeting their employees. The phishing email, disguised as a message from the company’s HR department, attempted to harvest login credentials by directing recipients to a malicious website. To analyze the origin and intent of the phishing campaign, you have been tasked with tracing the email and gathering detailed information about its sender using eMailTrackerPro, an email analysis tool.

### Solution

Your objective is to extract and analyze metadata from the email header, identify the sender’s IP address, trace the geolocation of the origin, and uncover details about the mail servers and infrastructure used. By tracing the email, you aim to map the attacker’s digital footprint, providing actionable insights to SecureNova’s incident response team.

Email headers can be extracted and examined to determine the sender’s information. Use eMailTrackerPro to determine the origin of the email and gather information such as IP address, mail servers, and geolocation. Cross-reference suspicious URLs or email addresses to understand the scope of the attack.

An essential email component is the header, which is also regarded as a valuable information source for ethical hackers planning an attack on a target. The sender, recipient, date, subject, routing information, and addressing scheme are all included in the email header. Additionally, ethical hackers can more easily trace an email’s path before it reaches its recipient due to the email header.

Through this lab, you will gain hands-on experience tracing emails and analyzing metadata to uncover critical information about the sender. Your findings will enable SecureNova Solutions to take immediate actions, such as:

* Reporting the open relay server to the hosting provider.
* Blacklisting the malicious domain.
* Educating employees on recognizing phishing emails to prevent similar attacks.

This exercise demonstrates the importance of email footprinting in understanding and mitigating phishing threats.

|  |
| --- |
| 1. Turn on the **Windows 11** virtual machine. Open any browser and go to the following link: **https://www.java.com/en/download/manual.jsp** to download the Java Runtime Environment (JRE). Click on the **Windows Offline** link to download JRE. After downloading the executable file of JRE, go to the **Downloads** folder. Double-click on the **jre-8u431-windows-i586.exe**. Click the **Yes** button if the **User Account Control** pop-up appears.    2. Click on the **Install** button.    3. After the installation is completed, click on the **Close** button.    4. Navigate to the browser and go to the following link: [**https://emailtrackerpro.software.informer.com/download/#downloading**](https://emailtrackerpro.software.informer.com/download/#downloading) to download eMailTrackerPro. After downloading the executable file of eMailTrackerPro, go to the **Downloads** folder. Double-click on the **emt.exe**. Click the **Yes** button if the **User Account Control** pop-up appears.    5. The **eMailTrackerPro Setup** window appears. Install eMailTrackerPro by following the wizard’s instructions and selecting the default settings. Click on the **Next** > button.    6. Click on the **I Agree** button.    7. Click on the **Next >** button.    8. Leave the default destination folder click on the **Next >** button.    9. Click on the **Install** button.    10. Once the installation is finished, uncheck the **Show Readme** checkbox in the **Completing the eMailTrackerPro Setup Wizard**. To start eMailTrackerPro, click the **Finish** button.    11. The **eMailTrackerPro’s** main window opens. In that the **Edition Selection** pop-up appears**.** Click on the **OK** button.    12. Hence, we successfully installed **eMailTrackerPro** in Windows 11. The **eMailTrackerPro** main window appears, as shown in the screenshot below.    13. Email headers can be traced by selecting the **My Trace Reports** icon from the **View** section. The output report for the traced email header can be found here.    14. Click on the **Trace Headers** icon from the **New Email Trace** section to start the trace.    15. A pop-up window will appear; select **Trace an email I have received**. In the **Email headers** field under the **Enter Details** section, copy the email header from the questionable email you want to track down.    16. Open any web browser and sign in to your preferred email account. Then, from the inbox, select the message you want to view the headers. To locate the email header in **Gmail**, take the following actions:   * Open an email; click on the dots (**More**) icon arrow next to the **Reply** icon at the top-right corner of the message pane. * Select **Show original** from the list.     19. The **Original Message** window appears in a new browser tab with all the details about the email, including the email header. Click on the **Copy to clipboard** button.    20. To locate the email header in Outlook, take the following actions:   * The email can be opened in a new window by double-clicking it. * Click the ... **(More actions)** icon present at the right of the message pane to open message options * From the options, click on **View**. * The **view message source** window appears with all the details about the email, including the email header.     21. The **Message source** window appears.    22. Paste the entire email header text into the **Email headers** field in eMailTrackerPro. Click on the **Trace** button.  **Note:** We are examining the Gmail account’s email header in this case.    23. The **My Trace Reports** window opens.   * The location of the email will be shown on a **Map** (world map GUI). You can also see the summary by choosing **Email Summary** from the menu on the right side of the window. The route’s complete hops and IP and suspected locations for each are displayed in the **Table** section directly beneath the Map. * To examine the Network Whois data. Click on the **Network Whois** button below the **Email Summary** to view the Network Whois data.     24. This concludes the demonstration of gathering information through analysis of the email header using eMailTrackerPro.  25. You can also use email tracking tools such as **MxToolbox** (https://mxtoolbox.com/), **Social Catfish** (https://socialcatfish.com/), **IP2Location Email Header Tracer** (https://www.ip2location.com/), etc., to monitor an email and retrieve target data, including the sender’s IP address, mail server, location, and other details.  26. Close all open windows and record the data you have collected. |

## Lab 4-09 Gather Information using Advanced Google Hacking Techniques

### Scenario

You are an ethical hacker hired by TechSecure Inc., a mid-sized technology company specializing in software development and IT solutions. Recently, TechSecure experienced a surge in phishing attempts and unauthorized access attempts on its web application. A security audit revealed that attackers might have used publicly accessible pages and misconfigured directories on the company’s website to gather sensitive information. This data potentially includes internal employee directories, customer service logs, and development files mistakenly exposed online. These files contained sensitive information, such as internal project details and credentials embedded in older scripts.

To prevent further reputational damage and ensure compliance with data protection regulations, the company’s senior management has requested a proactive security assessment to identify exposed data accessible through search engines like Google. The goal is to identify sensitive pages indexed by Google Search, such as administrator login portals, internal documentation directories, and forgotten subdomains. They want you to simulate an attacker’s perspective using Advanced Google Hacking Techniques—leveraging Google search operators to locate exposed information.

### Solution

Your task begins with reconnaissance and footprinting the TechSecure Inc. website, aiming to identify all sensitive data that might be inadvertently exposed. You will use advanced search operators such as site, intitle, inurl, filetype, and combinations of Boolean logic to locate pages containing sensitive information.

Advanced Google hacking is the practice of crafting intricate search engine queries using advanced Google operators in order to retrieve confidential or obscured data about a target business from the Google search results. Information about websites that are susceptible to exploitation may be obtained from this.

Through this exercise, you will provide a detailed report highlighting the exposed assets and recommend strategies to prevent future exposure, such as implementing a robots.txt file, restricting directory browsing, and removing sensitive files from the public domain. By understanding how attackers leverage Google Dorking techniques during reconnaissance, you will help TechSecure Inc. strengthen its defenses and protect its reputation.

**Note:** In this lab, we will use the **EC-Council** as a target organization. However, you are free to choose the target organization.

|  |
| --- |
| 1. Turn on your Windows 11 virtual machine. Open any browser and go to **https://www.google.com** (here, we use Google Chrome).    2. In the search bar, copy and paste this search command **intitle:login site:eccouncil.org**. The intitle and site Google advanced operators used in this search command limit the results to pages on the eccouncil.org website that have the login pages. Attackers and pen testers can extract login pages from the target organization's website with the help of this Advanced Google Search operator. Attackers can subject login pages to various attacks, such as credential brute-forcing, injection attacks, and other web application attacks. Analyzing the login pages for different types of attacks is also essential for penetration testing.    3. Similarly, copy and paste the following command **EC-Council filetype:pdf ceh** in the search bar to search your results based on the file extension and the keyword (here, ceh). Click on any link from the results here, and click on **CEH-brochure.pdf** to view the PDF file. Here, the target organization, EC-Council, is found by searching for the file type PDF. When you do this activity, the outcome may be different. Sensitive information about the target's goods and services may be included in PDFs and other documents downloaded from the target website. They might assist attackers in identifying a way to attack the victim.    4. The page appears to display the PDF file, as shown in the screenshot.    5. In the search field, enter the following command: **allinurl: EC-Council career.** The **allinurl** operator restricts results to pages containing all the query terms specified in the URL. Only sites with the terms "EC-Council" and "career" in the URL are returned by the **allinurl: EC-Council career** query**.**    6. Copy and paste the following command: **inurl: copy site:www.eccouncil.org** in the search bar. The **inurl** operator restricts the results to pages containing the word specified in the URL. **inurl: copy site:www.eccouncil.org** query returns only pages in the EC-Council site where the URL has the word “copy.”    7. Copy and paste the following command: **allintitle: detect malware** in the search bar. Results are restricted to pages that include every query phrase listed in the title using the **allintitle** operator. Only pages that include every query phrase listed in the title are returned by the **allintitle** operator**.** Only sites with the terms "detect" and "malware" in the title are returned by the **allintitle: detect malware** query**.**    8. Copy and paste the **Anti-virus inanchor:Norton** command in the search bar. The **inanchor** operator restricts results to pages containing the query terms specified in the anchor text on links to the page. **Anti-virus inanchor:Norton** query returns only pages with anchor text on links to the pages containing the word “Norton” and the page containing the word “Anti-virus.”    9. Copy and paste the following command: **allinanchor: best cloud service provider** in the search bar. The **allinanchor** operator restricts results to pages containing all query terms specified in the anchor text on links to the page. Only sites that include the terms "best," "cloud," "service," and "provider" in the anchor text of links to those pages are returned by the **allinanchor: best cloud service provider** query.    10. Copy and paste the following command: **link:www.eccouncil.org** in the search bar. The **link** operator looks for webpages or websites that have links pointing to the designated webpage or website. **link:www.eccouncil.org** discovers links pointing to the main website of the EC-Council.    11. Copy and paste the following command: **related:www.eccouncil.org** in the search bar. The **Related** operator displays websites that are similar or related to the URL specified. The Google search engine results page containing websites that are similar to eccouncil.org is displayed when you enter **related:www.eccouncil.org.**    12. Copy and paste the following command: **info:eccouncil.org** in the search bar. The **info** operator finds information for the specified web page. The query **info:eccouncil.org** returns details about the homepage of www.eccouncil.org.    13. Copy and paste the following command: **location: EC-Council** in the search bar. Information about a particular site is found by the **location** operator. **location: EC-Council** query gives you results based on the term EC-Council.    14. This concludes the demonstration of gathering information using advanced Google hacking techniques. With the help of these sophisticated Google operators, you can do many queries and obtain pertinent data about the intended company. |

## Lab 4-10: Information Gathering Using theHarvester

### Scenario

While working as a Certified Penetration Tester in a cybersecurity company, you are assigned to perform the reconnaissance phase of a penetration test for a client. The goal is to gather as much Open-Source Intelligence (OSINT) as possible about the client’s public-facing infrastructure. Using the Parrot Security virtual machine, you decide to run theHarvester, a powerful OSINT tool, to collect information such as emails, subdomains, and IP addresses linked to the client’s domain. This information will help build a clear picture of the target’s digital footprint and potential attack surface.

### Solution

TheHarvester provides an effective way to perform footprinting by automating the collection of publicly available information about a target domain. Running on the Parrot Security virtual machine, it can query multiple search engines and data sources to gather emails, subdomains, IP addresses, and hostnames linked to the target. This data is crucial in the reconnaissance phase of penetration testing, as it helps build a clear picture of the organization’s external exposure. To make the results easier to analyze, theHarvester also allows exporting findings into a structured HTML report, which simplifies review and documentation.

|  |
| --- |
| 1. Turn on the Parrot Security virtual machine and log in with your credentials. Before starting this lab, integrate ShellGPT in the Parrot Security machine.  2. Open the terminal and write the command **theHarvester -v** to ensure Harvester is installed and working.    3. To launch an information gathering campaign on a target, type the command **theHarvester -d hackaday.com -l 300 -b bing,duckduckgo.** This will start theHarvester. It will begin searching Bing and DuckDuckGo for the top 300 results related to hackaday.com. For this target, we found only one email using two search engines, and no additional information was available.    4. If we want to gather even more information about our target, we can specify the following command: **theHarvester -d hackaday.com -l 300 -b all.** The **-b all** tag will search all available search engines through the Harvester for information regarding hackaday.com. As you can see, it is an extremely useful tool for discovering email addresses, some other URLs, Hosts, and IP addresses.        5. If we wanted to display this information in an easier-to-read format, we could add the **-f** tag at the end of the command **theHarvester -d hackaday.com -l 300 -b all -f hackaday.com.results.**    6. In Parrot OS, this saves the information gathered into **JSON** and **XML** files (e.g., **hackaday.com.results.json** and **hackaday.com.results.xml**). These files can then be opened with tools like **jq** (for JSON) or any XML viewer, allowing the results to be read in a structured and clearer way.    7. You can also use ShellGPT for gathering information using theHarvester. As you have already incorporated SHellGPT in your Parros OS machine, run **sgpt --chat footprint --shell “Use theHarvester to gather email accounts associated with 'microsoft.com', limiting results to 200, and leveraging 'baidu' as a data source”** command to a target organization for harvesting emails. You can write the script according to your requirements.      10. This concludes the demonstration of this lab. |