OSINT (OPEN SOURCE INTELLIGENCE) TOOLS (SCENARIO & STEP TO USE)

Commonly used OSINT (Open Source Intelligence) tools that are often utilized in Security Operations Centres (SOCs) or by cybersecurity professionals for gathering information:

Censys: Censys is a search engine that allows researchers to query large datasets for host and network information.

Creepy: A geolocation OSINT tool that allows users to gather geolocation information about a target.

Google Dorks: Techniques to use Google's search engine more effectively for specific information gathering.

Hunchly: A tool that captures and organizes web-based evidence for online investigations and OSINT gathering.

Maltego: A versatile tool for open-source intelligence and forensics, offering data mining and visualization capabilities.

Metagoofil: A tool for extracting metadata from public documents (PDF, DOC, XLS, PPT, etc.) available on the internet.

Nmap: An open source Linux command-line tool used for network exploration, host discovery, and security auditing.

OSINT Framework: A collection of various tools for gathering OSINT information, including both online and offline resources.

Photon: A fast OSINT tool for extracting URLs, web directories, and metadata from target websites.

Recon-ng: An open-source reconnaissance framework written in Python, useful for conducting reconnaissance of targets.

Shodan: A search engine for internet-connected devices, it allows for reconnaissance of devices, services, and more.

SpiderFoot: A reconnaissance tool that automatically queries over 100 public data sources to gather intelligence on IP addresses, domain names, e-mail addresses, names, and more.

theHarvester: A tool for gathering email addresses, subdomains, hosts, employee names, open ports, and banners from different public sources like search engines and PGP key servers.

Wireshark: Though primarily a network protocol analyser, Wireshark can be used to gather information about network traffic and potential security threats.

Scenario & Step To Use

1. Censys

Scenario: Suppose you want to investigate the SSL/TLS certificates used by the domain "izzmier.com" to identify potential security vulnerabilities or misconfigurations within your SOC.

Steps to use:

1. **Access Censys Website**:
   - Go to Censys and sign in to your account. If you don't have an account, you may need to create one.
2. **Perform a Certificate Search**:
   - In the search bar, enter the domain you want to investigate. For example, enter parsed.names: izzmier.com to search for SSL certificates associated with "izzmier.com".
3. **Review the Certificate Details**:
   - Censys will display a list of SSL certificates used by "izzmier.com". This includes information such as:
     - Common Name (CN)
     - Subject Alternative Names (SANs)
     - Issuer
     - Validity period
     - Key size
     - Cipher suites used
     - Associated domains and subdomains
4. **Analyse the Results**:
   - Evaluate the SSL/TLS configuration details to identify potential weaknesses or vulnerabilities, such as expired certificates, weak ciphers, or misconfigured domains.
5. **Additional Features**:
   - Censys also provides insights into other aspects of internet infrastructure, such as open ports, protocols, and vulnerabilities associated with the target domain.

Example Output:

After performing the search on Censys for "izzmier.com", you might see results similar to the following:

```
Certificate Details:
- Common Name (CN): izzmier.com
- Subject Alternative Names (SANs): www.izzmier.com, mail.izzmier.com
- Issuer: Let's Encrypt
- Validity Period: Valid until 2030-03-30
- Key Size: 2048 bits
```

- Cipher Suites: TLS_RSA_WITH_AES_256_GCM_SHA384, TLS_RSA_WITH_AES_128_GCM_SHA256
- Associated Domains: subdomain1.izzmier.com, subdomain2.izzmier.com

2. Creepy

Scenario: Suppose you want to investigate a specific geographical area or event where social media users have posted geotagged content. You aim to gather information about these users and their activities for intelligence gathering within your SOC environment.

Steps to use:

1. **Install and Configure Creepy**:
   - Creepy is typically available for Linux systems and can be installed using Git. Ensure you have Python installed as well.

     ```
     git clone https://github.com/ilektrojohn/creepy.git
     cd creepy
     pip install -r requirements.txt
     ```

2. **Launch Creepy**:
   - Start Creepy by running the following command in your terminal:

     ```
     python creepy.py
     ```

3. **Configure Search Parameters**:
   - In the Creepy interface, specify the search criteria such as geographical coordinates, radius, and social media platforms (Twitter or Instagram).
   - For example, set the location to search near a specific latitude and longitude coordinates:

     ```
     location: 2.9198, 101.7809
     radius: 5km
     ```

4. **Start the Search**:
   - Initiate the search within Creepy to collect data from social media platforms based on the specified location and radius.
   - Creepy will retrieve publicly available posts that match the search criteria, focusing on geotagged content.
5. **Analyse Results**:
   - Creepy will display information about social media users who have posted content within the specified area, including their usernames, posts, and geotag locations.
   - Review the collected data to identify patterns, behaviours, or potential security risks associated with the users or events.
6. **Export and Document Findings**:
   - Export the gathered information from Creepy for further analysis or reporting within your SOC environment. This may include user profiles, posts, timestamps, and geolocation data.

Example Output:

After using Creepy to search near Bangi (latitude 2.9198, longitude 101.7809), you might see output similar to this:

```
[+] Found 10 tweets within 5km of Bangi:
- User: @Iffah
  - Location: Bangi,Selangor
  - Tweet: "Makan sedap! #Bangi"
- User: @Nadzirah
  - Location: Taman Tasik Cempaka
  - Tweet: "Beautiful day at the park! #TamanTasikCempaka"
...
```

3. Google Dorks

Scenario: Suppose you want to identify publicly accessible documents (e.g., PDF files) related to a target organization "izzmier.com". You aim to find potentially sensitive information that may have been inadvertently exposed on the web.

Steps to use:

1. **Choose a Google Dork Query**:
   - Use an appropriate Google Dork query to target PDF files on the domain "izzmier.com". For example:

     ```
     site:izzmier.com filetype:pdf
     ```

     - site:izzmier.com: Limits the search results to the domain "izzmier.com".
     - filetype:pdf: Filters the results to include only PDF files.
2. **Run the Google Dork Query**:
   - Enter the Google Dork query directly into Google's search engine (or use specialized tools that facilitate Dork queries).
   - Press Enter to execute the search.
3. **Review Search Results**:
   - Google will return a list of PDF files hosted on "izzmier.com" that are publicly accessible. These files may include reports, manuals, presentations, or other documents.
4. **Analyse Document Contents**:
   - Click on the search results to access and analyse the contents of the PDF documents. Look for sensitive information such as:
     - Internal company policies or procedures.
     - Financial reports.
     - Technical specifications.
     - Employee directories.
5. **Extract and Document Findings**:
   - Extract relevant information from the discovered documents for further analysis or reporting within your SOC environment.
   - Document any findings that may indicate security risks or potential exposures.

Example Output:

After running the Google Dork query site:izzmier.com filetype:pdf, you might see search results listing PDF documents hosted on "izzmier.com":

```
[+] Found 10 PDF documents on izzmier.com:
- Report on Financial Performance 2024.pdf
- Employee Handbook.pdf
- Technical Specifications.pdf
```

4. **Hunchly**:

Scenario: Suppose you are investigating a potential security incident involving a suspicious website that might be hosting phishing content targeting your organization. You want to use Hunchly to capture and document evidence from this website for further analysis and reporting.

Steps to use:

1. **Start a New Case**:
    - Launch Hunchly on your browser (Hunchly is a browser extension available for Chrome and Firefox).
    - Start a new case for your investigation. Give it a descriptive name related to the incident or website you are investigating.
2. **Navigate to the Suspicious Website**:
    - Enter the URL of the suspicious website in your browser's address bar and visit the site.
3. **Capture Web Pages**:
    - Hunchly will automatically start capturing web pages visited during your browsing session. It records the HTML content, screenshots, and metadata (such as timestamps) for each page visited.
4. **Document Findings**:
    - As you browse through the website, Hunchly captures each page transition and interaction, creating a timeline of your investigation. You can add notes and tags to document specific observations or findings.
5. **Review and Analyse Captured Data**:
    - After completing your investigation session, review the captured data in Hunchly. This includes:
        - Screenshots of each visited page.
        - URLs and HTML content.
        - Timestamps of each interaction.
        - Metadata such as server headers and response codes.
6. **Export Reports**:
    - Generate and export reports from Hunchly to share findings with your team or stakeholders. Reports can include detailed logs of browsing activity, screenshots, and annotated notes.

Example Output:

After using Hunchly to investigate the suspicious website, your findings might include:

- Timeline of visited pages and interactions.
- Screenshots showing the website layout and content.
- Metadata indicating server information and HTTP response headers.

5. **Maltego**

Scenario: Suppose you need to gather information about a target organization, "Izzmier Enterprise," for threat intelligence purposes. You want to gather details such as domain names, email addresses, related social media profiles, and any associated entities that might be relevant to your investigation.

Steps to use:

1. **Launch Maltego**:
   - Open Maltego on your computer. It's available for various platforms including Windows, macOS, and Linux.
2. **Choose a Transform**:
   - Maltego uses "transforms" to query different data sources. Select appropriate transforms based on the information you want to gather (e.g., Domain to DNS Name, Person to Email Address, etc.).
3. **Add Entity (e.g., Domain)**:
   - Start by adding an entity related to the target organization. For example, add a "Domain" entity and enter izzmierenterprise.com.
4. **Run Transforms**:
   - Right-click on the domain entity and select "Run Transforms" or "Run All" to execute transforms associated with that entity. This action queries various OSINT data sources.
5. **Review Results**:
   - Maltego will display a graph showing relationships between entities (e.g., domain names, email addresses, social media profiles) associated with the target organization. You can explore these connections visually.
6. **Export and Analyse**:
   - Export the results or save the graph for further analysis. Analyse the gathered information to identify potential security risks, connections to threat actors, or vulnerabilities.

Example Output:

After running transforms in Maltego, you might see a graph with nodes representing various entities connected to "Izzmier Enterprise," such as:

- Domain names (e.g., izzmierenterprise.com, izzmierenterprise.net)
- Email addresses (e.g., iffah@izzmierenterprise.com, info@izzmierenterprise.com)
- Social media profiles (e.g., LinkedIn, Twitter)
- Related organizations or subsidiaries

The graph visualization in Maltego helps SOC teams to understand the organizational structure, potential attack vectors, and relationships between different entities associated with the target organization.

6. **Metagoofil**:

Scenario: Suppose you need to gather metadata from documents associated with a domain "izzmier.com" to extract information that might reveal details about internal systems, technologies used, or potentially sensitive data.

Steps to use:

1. **Install Metagoofil** (if not already installed):
   - Metagoofil is typically included in security-focused Linux distributions like Kali Linux. Ensure you have it installed, or you can download it from its GitHub repository.
2. **Run Metagoofil** with the desired options:
   - Open your terminal or command prompt.
   - Use the following command to search for documents associated with izzmier.com and extract metadata:

     ```
     metagoofil -d izzmier.com -t pdf,doc,docx,xls,xlsx,ppt,pptx -l 100 -n 50 -o output_folder
     ```

     - -d izzmier.com: Specifies the domain you want to target.
     - -t pdf,doc,docx,xls,xlsx,ppt,pptx: Specifies the file types to search for (PDF, Word documents, Excel spreadsheets, PowerPoint presentations).
     - -l 100: Limits the number of results to 100 files.
     - -n 50: Limits the number of files to download per search engine query.
     - -o output_folder: Specifies the output folder where extracted files will be saved.
3. **Review the Extracted Metadata**:
   - Metagoofil will search for documents matching the specified criteria (file types and domain) and extract metadata such as author names, software versions, timestamps, and potentially sensitive information.
4. **Analyse the Output**:
   - Explore the extracted metadata to identify potentially sensitive information or details about the organization's internal systems and technologies.

Example Output:

After running Metagoofil on "izzmier.com", you might find output such as:

```
[INFO] Searching in Bing...
[INFO] Searching in Google...
[INFO] Searching in DuckDuckGo...
[INFO] Downloading files...
[INFO] Downloading file: document1.pdf
[INFO] Downloading file: presentation.pptx
```

```
[INFO] Downloading file: report.docx
...
[INFO] Extracting metadata from downloaded files...
[INFO] Metadata extracted from document1.pdf:
  - Author: Izzmier
  - Software: Adobe Acrobat 10.1.3
  - Creation Date: 2024-06-26
  - Keywords: Report, Finance, Quarterly
...
```

7. **Nmap**

Scenario: Suppose you want to perform a network scan on a target domain "izzmier.com" to identify open ports, services running on those ports, and potentially vulnerable systems within your SOC environment.

Steps to use:

1. **Install and Configure Nmap**:
   - Nmap is available for various operating systems. Install Nmap on your system from the official website or your package manager.
2. **Perform a Basic Scan**:
   - Open your terminal or command prompt.
   - Use the following command to perform a basic TCP port scan on the target domain "izzmier.com":

     ```
     nmap izzmier.com
     ```

     This command will scan the most common 1,000 ports by default.
3. **Review Scan Results**:
   - Nmap will output information about open ports, services running on those ports, and potentially the operating system of the target system(s).
4. **Perform a More Detailed Scan**:
   - To gather more detailed information, you can perform a more comprehensive scan with additional options. For example, to perform a more detailed scan and detect operating system versions:

     ```
     nmap -A izzmier.com
     ```

     - -A: Enables OS detection, version detection, script scanning, and traceroute.
5. **Analyze Scan Output**:
   - Analyze the scan output to identify:
     - Open ports and associated services (e.g., HTTP, FTP, SSH).
     - Versions of services running on open ports.
     - Potential vulnerabilities or misconfigurations that could be exploited.
6. **Export and Document Findings**:
   - Export Nmap scan results for documentation and further analysis. You can save the scan results to a file for reporting and sharing with your team.

Example Output:

After running Nmap on "izzmier.com", you might see output similar to this:

```
PORT    STATE   SERVICE     VERSION
```

```
80/tcp   open     http        Apache HTTP Server 2.4.38
443/tcp  open     ssl/http    Apache httpd
22/tcp   closed   ssh
```

8. **OSINT Framework**

Scenario: Suppose you need to gather OSINT information about an individual named "Izzmier" for a security investigation within your SOC. You want to find details like social media accounts, email addresses, and other online footprints associated with this person.

Steps to use:

1. **Access OSINT Framework**:
   - Visit the OSINT Framework website to access the categorized list of OSINT tools and resources.
2. **Navigate to Relevant Sections**:
   - Explore sections related to people, social media, email addresses, and any other relevant categories where you might find information about "Izzmier".
3. **Select and Use Tools**:
   - Choose specific tools or resources listed under each category to conduct your investigation. For example:
     - **Social Media**: Tools like Intel Techniques or SpiderFoot (mentioned earlier) for gathering social media profiles.
     - **Email Addresses**: Tools like theHarvester or Maltego (mentioned earlier) for extracting email addresses associated with the target.
4. **Run Queries and Gather Information**:
   - Use the selected tools to run queries based on the available information about "Izzmier". This might include searching for usernames, real names, or other identifiers associated with the individual.
5. **Analyse and Document Results**:
   - Review the gathered information to compile a comprehensive profile of "Izzmier". Document findings such as social media accounts, email addresses, online activities, and any potential connections.

Example Output:

After using OSINT Framework tools to gather information about "Izzmier", you might compile results such as:

- **Social Media Profiles**:
  - Facebook: Izzmier
  - Twitter: @izzmier
  - LinkedIn: Izzmier
- **Email Addresses**:
  - izzmier@gmail.com

9. **Photon**

Scenario: Suppose you want to conduct OSINT on a target domain "izzmier.com" to identify subdomains, directories, and files that may be publicly accessible. You aim to gather information that could reveal potential security risks or expose sensitive information.

Steps to use:

1. **Install and Configure Photon**:
   - Photon can be installed via Python's package manager pip. Ensure you have Python installed first. You can install Photon by running:

     ```
     pip install photon
     ```

2. **Run Photon with Target Domain**:
   - Open your terminal or command prompt.
   - Use the following command to run Photon and specify the target domain:

     ```
     photon -u izzmier.com
     ```

     - -u izzmier.com: Specifies the target URL or domain to crawl and gather information from.
3. **Crawl and Gather Information**:
   - Photon will start crawling the target domain "izzmier.com" and its subdomains. It will discover URLs, directories, files, and other resources accessible from the web server.
4. **Collect Results**:
   - Photon will output discovered URLs, directories, and files to the terminal. It categorizes and organizes findings based on the discovered paths and resources.
5. **Review and Analyse Findings**:
   - Review the output from Photon to identify:
     - Subdomains associated with "izzmier.com".
     - Directories and paths that may contain sensitive or publicly accessible information.
     - Files such as configuration files (robots.txt), documents, or other resources.
6. **Export Results**:
   - Optionally, export the results from Photon to further analyse or share with your team. Photon provides options to export findings in various formats for documentation and reporting purposes.

Example Output:

After running Photon on "izzmier.com", you might see output similar to this:

```
Discovered URLs:
```

- https://izzmier.com/
- https://www.izzmier.com/
- https://subdomain.izzmier.com/
- https://izzmier.com/page1.html
- https://izzmier.com/page2.html

Discovered Files:
- https://izzmier.com/robots.txt
- https://izzmier.com/config.php
- https://izzmier.com/report.pdf

10. **Recon-ng**

Scenario 1: Suppose you want to gather OSINT information about the domain "izzmier.com" to assess its digital footprint and potential security risks within your SOC.

Steps to use:

1. **Launch Recon-ng**:
   - Recon-ng is a Python-based tool that you can install and run from your terminal. Make sure you have it installed, typically using:

     ```
     git clone https://github.com/lanmaster53/recon-ng.git
     cd recon-ng
     pip install -r REQUIREMENTS
     ./recon-ng
     ```

2. **Start a New Workspace**:
   - Begin by creating a new workspace for your investigation. This isolates your findings and allows you to organize results efficiently within Recon-ng.
3. **Set Up the Environment**:
   - Configure Recon-ng with the necessary modules and APIs for your investigation. This might involve setting API keys or configuring specific modules related to domain reconnaissance.
4. **Run Modules**:
   - Use Recon-ng modules to gather information about the target domain "izzmier.com". For example, you can run the following commands within Recon-ng:

     ```
     use recon/domains-hosts/google_site_web
     set source izzmier.com
     run
     ```

     This command sequence uses Google as a data source to gather information about websites related to "izzmier.com".

5. **Explore Results**:
   - Recon-ng will display results such as subdomains, IP addresses, email addresses, and potentially other relevant information associated with "izzmier.com". Review and analyse these results to understand the domain's digital footprint.
6. **Export and Analyse**:
   - Export the results obtained from Recon-ng for further analysis and reporting within your SOC. Use this information to identify potential security weaknesses, exposed assets, or areas requiring further investigation.

Example Output:

After running Recon-ng on "izzmier.com", you might obtain results such as:

- **Subdomains**: blog.izzmier.com, shop.izzmier.com
- **IP Addresses**: 192.0.2.1, 198.51.100.1
- **Email Addresses**: info@izzmier.com, support@izzmier.com
- **Employees**: Izzmier (CEO), Iffah (CTO)

Scenario 2: Suppose you want to gather OSINT information about a domain "izzmier.com" to identify subdomains, email addresses, and related information that could provide insights into potential security risks or vulnerabilities.

Steps to use:

1. **Launch Recon-ng**:
   - Open your terminal or command prompt.
   - Start Recon-ng by running:

     ```
     recon-ng
     ```

2. **Initialize and Configure Modules**:
   - Inside Recon-ng, initialize the framework and configure modules for gathering information about the target domain "izzmier.com":

     ```
     [recon-ng] marketplace search domains
     [recon-ng] marketplace install recon/domains-contacts/pgp_search
     [recon-ng] marketplace install recon/domains-contacts/whois_pocs
     ```

3. **Set Up the Workspace**:
   - Create a new workspace and set the source to "izzmier.com":

     ```
     [recon-ng] workspace add izzmier_com
     [recon-ng] options set SOURCE izzmier.com
     ```

4. **Run Modules**:
   - Execute modules to gather information. For example, run modules to discover subdomains and contact information associated with "izzmier.com":

     ```
     [recon-ng] modules load recon/domains-hosts/brute_hosts
     [recon-ng] run
     [recon-ng] modules load recon/domains-contacts/whois_pocs
     [recon-ng] run
     ```

5. **Review and Export Results**:

    - Recon-ng will gather and display information such as discovered subdomains, email addresses, WHOIS details, and potentially other relevant data.
    - Review the gathered information within Recon-ng's interface and export results if needed for further analysis or reporting.

6. **Additional Modules and Customization**:
    - Explore other Recon-ng modules and APIs to further customize your OSINT gathering. Modules can be loaded and executed based on specific information needs or targets.

Example Output:

After running Recon-ng on "izzmier.com", you might see output similar to this:

```
[+] Domains discovered:
  - www.izzmier.com
  - mail.izzmier.com

[+] Email addresses found:
  - admin@izzmier.com
  - support@izzmier.com

[+] WHOIS information:
  - Registrar: Izzmier Registrar
  - Registrant Name: Iffah
  - Registrant Email: iffah@izzmier.com
  - ...

[+] PGP keys found:
  - Key ID: ABC123DEF456
  - Owner: Izzmier <iffah@izzmier.com>
  - ...
```

11. **Shodan**

Scenario 1: Suppose you want to identify open ports and services exposed by devices within a specific IP address range belonging to your organization (192.168.1.0/24). This can help in identifying potential vulnerabilities and assessing the security posture of devices within your network.

Steps to use:

1. **Access Shodan Website**:
   - Go to Shodan and sign in to your account. If you don't have an account, you may need to create one.
2. **Perform a Search**:
   - In the search bar, enter the IP address range you want to scan. For example, enter net:192.168.1.0/24 to search for devices within the 192.168.1.0/24 subnet.
3. **Review the Results**:
   - Shodan will display a list of devices that match the specified IP address range.
   - It will also show information such as open ports, services running on those ports, operating systems, and sometimes even specific vulnerabilities detected.
4. **Analyse the Data**:
   - Review the open ports and services listed for each device. Pay attention to any services that should not be exposed or any devices with outdated software versions that may pose security risks.

Example Output:

After performing the search, you might see results similar to this:

```
IP: 192.168.1.1
Ports: 22 (SSH)
Hostname: router.izzmier.com
Organization: Izzmier Enterprise
Operating System: Linux

IP: 192.168.1.10
Ports: 80 (HTTP), 443 (HTTPS)
Hostname: webserver.izzmier.com
Organization: Izzmier Enterprise
Operating System: Windows Server 2016

...
```

Scenario 2: Imagine you want to assess the security posture of devices within a specific IP address range (192.168.1.0/24) to identify potential vulnerabilities and exposure risks within your SOC.

Steps to use:

1. **Access Shodan Website**:
    - Go to Shodan and sign in to your account. If you don't have an account, you may need to create one.
2. **Perform a Search**:
    - In the search bar, enter the IP address range you want to scan. For example, enter net:192.168.1.0/24 to search for devices within the 192.168.1.0/24 subnet.
3. **Review Device Details**:
    - Shodan will display a list of devices within the specified IP address range, along with details such as open ports, services running on those ports, operating systems, and sometimes even specific vulnerabilities detected.
4. **Analyse Vulnerabilities**:
    - Identify devices with open ports or services that may pose security risks. Look for devices running outdated software versions, known vulnerable services, or misconfigurations.
5. **Explore Additional Features**:
    - Shodan offers filters and sorting options to refine your search results. You can focus on specific types of devices, locations, or other criteria to tailor your assessment.

Example Output:

After performing the search on Shodan for net:192.168.1.0/24, you might see results similar to the following:

```
IP: 192.168.1.1
Ports: 22 (SSH), 80 (HTTP), 443 (HTTPS)
Hostname: router.izzmier.com
Organization: Izzmier Enterprise
Operating System: Linux
```

12. **SpiderFoot**

Scenario: Imagine you need to investigate the domain "izzmier.com" to gather comprehensive OSINT information for security analysis and threat intelligence purposes within your SOC.

Steps to use:

1. **Launch SpiderFoot**:
   - SpiderFoot can be installed on various platforms (Windows, Linux, macOS) and is available as both a command-line tool and a graphical interface. You can download it from the official SpiderFoot website.
2. **Start a New Scan**:
   - Open SpiderFoot and start a new scan. You can initiate this through the command line or using the graphical interface.
3. **Configure the Scan**:
   - Enter the domain "izzmier.com" as the target for your scan. You can specify other parameters such as the depth of the scan (how deep into linked resources SpiderFoot should explore).
4. **Run the Scan**:
   - Execute the scan to let SpiderFoot gather information from various OSINT sources. This may include DNS records, WHOIS information, subdomains, IP addresses, email addresses, and more.
5. **Review Results**:
   - SpiderFoot will present the results in a structured format, showing connections between different entities related to "izzmier.com". You can explore these results to identify potential security risks or areas of concern.
6. **Export and Analyse**:
   - Export the results for further analysis and reporting within your SOC. Analyse the gathered information to understand the digital footprint of the target domain and assess potential security implications.

Example Output:

After running SpiderFoot on "izzmier.com", you might obtain results similar to the following:

- **Domain Information**:
  - Primary domain: izzmier.com
  - Subdomains: blog.izzmier.com, shop.izzmier.com
- **IP Addresses**:
  - Associated IP addresses: 192.0.2.1, 198.51.100.1
- **Email Addresses**:
  - Contact emails: info@izzmier.com, support@izzmier.com
- **Related Entities**:
  - Social media profiles linked to the domain
  - Associated organizations or subsidiaries

13. **theHarvester**

Scenario 1: Imagine you need to gather email addresses associated with a specific domain "izzmier.com" for intelligence gathering within your SOC. You want to identify potential targets or gain insights into the organizational structure and contacts.

Steps to use:

1. **Install theHarvester** (if not already installed):
   - theHarvester can be installed via Python's package manager pip. Ensure you have Python installed first. You can install theHarvester by running:

     ```
     pip install theHarvester
     ```

2. **Run theHarvester** with the desired options:
   - Open your terminal or command prompt.
   - Use the following command to search for email addresses related to the domain izzmier.com:

     ```
     theharvester -d izzmier.com -b google
     ```

     - -d izzmier.com: Specifies the domain you want to target.
     - -b google: Specifies Google as the data source to query.
3. **Review the Results**:
   - theHarvester will start querying Google and other specified sources for email addresses associated with izzmier.com.
   - It will output the results directly in your terminal/command prompt window.
4. **Analyse the Output**:
   - The tool will provide a list of email addresses found associated with izzmier.com. It may also include subdomains, hosts, or other relevant information depending on the sources queried.

Example Output:

After running theHarvester on "izzmier.com", you might see output similar to this:

```
====================
[+] Emails found:
====================
iffah@izzmier.com
rooney@izzmier.com
info@izzmier.com
support@izzmier.com
...
```

Scenario 2: Suppose you're tasked with gathering email addresses associated with a specific domain for a security assessment within your SOC. Let's use theHarvester to search for email addresses associated with the domain izzmier.com.

Steps to use:

1. **Run theHarvester** with the desired options:
   - Open your terminal or command prompt.
   - Use the following command to search for email addresses related to izzmier.com:

     ```
     theHarvester -d izzmier.com -l 100 -b google
     ```

     - -d izzmier.com: Specifies the domain you want to target.
     - -l 100: Limits the number of results to 100 (adjust as needed).
     - -b google: Specifies the data source to use (in this case, Google).
2. **Review the Results**:
   - theHarvester will start querying Google (or other specified sources) for information related to email addresses associated with izzmier.com.
   - It will output the results directly in your terminal/command prompt window.
3. **Analyse the Output**:
   - The tool will provide a list of email addresses found associated with izzmier.com. It may also include subdomains, hosts, or other relevant information depending on the parameters used.

Example Output:

After running the command, you might see output similar to this:

```
[+] Searching in Google...
[+] Searching in Baidu...
[+] Searching in Bing...
[+] Searching in Dogpile...
[+] Searching in Virustotal...
[+] Searching in Netcraft...
[+] Searching in Certspotter...
[+] Searching in Crtsh...
[+] Searching in Bufferover...
[+] Searching in Pgp...
[+] Searching in Linkedin...
[+] Emails found:
iffah@izzmier.com
rooney@izzmier.com
info@izzmier.com
support@izzmier.com
...
```

14. **Wireshark**:

Scenario: Suppose you are investigating suspicious network activity related to a potential cyber-attack targeting your organization. You suspect that malicious traffic is originating from a specific IP address and want to use Wireshark to capture and analyse this traffic for further investigation.

Steps to use:

1. **Capture Network Traffic**:
   - Launch Wireshark on your computer. Wireshark is available for various platforms including Windows, macOS, and Linux.
   - Select the network interface (e.g., Ethernet, Wi-Fi) through which you want to capture traffic.
2. **Apply Filters**:
   - To focus on traffic related to the suspicious IP address, apply a display filter in Wireshark. For example, to capture traffic from IP address 192.168.1.100, you can use the filter:

     ```
     ip.addr == 192.168.1.100
     ```

   - Adjust the filter based on the specific IP address or network range you are investigating.
3. **Capture and Analyse Traffic**:
   - Start capturing traffic by clicking on the "Start" button in Wireshark. It will begin capturing packets flowing through the selected network interface.
4. **Monitor and Identify Suspicious Activity**:
   - As Wireshark captures packets, monitor the traffic for any suspicious patterns or anomalies. Look for:
     - Unusual communication patterns.
     - Unexpected connections or protocols.
     - Large volumes of data transfer.
     - Signs of malware communication (e.g., command and control traffic).
5. **Extract and Analyse Packets**:
   - Analyse captured packets in Wireshark to extract information such as source and destination IP addresses, protocols used, payload contents, and timestamps.
6. **Generate Reports**:
   - Generate reports or export packet captures from Wireshark for further analysis and sharing with your team or stakeholders. Reports can include detailed packet logs, analysis findings, and recommendations.

Example Output:

After capturing and analysing traffic using Wireshark, you might identify:

- Suspicious connections originating from or going to the suspicious IP address.

- Protocols and ports used in the communication.
- Payload contents that may indicate malicious activity (e.g., encoded commands, suspicious URLs).