**Name: Tanvir Ahmed**

**Date: June 9 2025**

**Phase 1. Perform Reconnaissance**

**Intro:**

Artemis is a natural gas corporation headquartered in Paris, France operating 1,000 miles of industrial gas pipelines across the U.S. The company uses hybrid security infrastructure incorporating technologies like Cisco, Fortinet, and Palo Alto. To perform reconnaissance and profile Artemis, OSINT, a open source intelligence framework will be used to gather useful information.

**Reconnaissance:**

**Goal:** The target is Artemis and through reconnaissance a profile should be created that includes email addresses, phone numbers, and other details.

**Procedure:**

**Social Media:**

Social Media is a perfect place to gather info regarding company culture, employees and their behavior along with threats and leaked information.

1. **Linkedin**

Using tools like ScrapedIn, employee data from Artemis can be scraped. With simple input of the target name, the tool can find the Linkedin Id that will help to perform employee search with a maximum search result of 1,000 contacts. The dataset of the result includes, firstname, last name, occupation, location, industry and profile url. In addition, Scrapedln can provide pictures of employees.

1. **Instagram**

With Osintgram, we can analyze Artemi’s post, stories, photos, hashtags, comments, tagged content and emails. These insights will help identify workplace environment, exposed emails in user buis, staff events, and comments.

1. **Twitter**

Twint allows scraping Twitter data based on specific hashtags, specific hashtags, usernames, and keywords. It can expose sensitive information like emails and phone numbers. Very useful to gather info on company culture and their internal behaviors, indicating company operations and vulnerabilities.

1. **Facebook**

Facebook provides more informal insights. Corporate pages and public posts by employees may reveal office images, social gatherings and events. The network of the company can be analyzed to map employee connections.

**Search Engines:**

Search engines are ideal to gather past history and information that are accidental or intentionally published on the internet.

1. **Google Advanced Search** is a tool that can be next in the procedure to get more curated info with specific phrase, region and site to obtain any file or document of Artemis. Google operators like site:, intitle:, filetype:, help locate specific documents related to Artemis. Documents may include public reports, manuals and employee lists.
2. **Bing** is another tool that can be used as an alternative to gather information on Artemis which has not been captured by Google. It can reveal new documents, archived pages revealing Artemis’s online footprint.

**Job Boards:**

1. **Linkedin**

Through linkedin we can scrape job listing and hiring trends of Artemis. It will give insight on the technologies they are using, and ongoing projects.

1. **Indeed / Other Job Portals**

Scraping Indeed and other job portals can identify the required roles in Artemis. It will also provide a glimpse of the company’s internal working.

**Company Research:**

1. **Maltego**

With the help of maltego many things can be obtained that will help to analyze the relationship between Artemis, its employees, infrastructure, and public entities. Maltego helps visualize connections that may be otherwise difficult to detect.

1. **AnnualReport.com**

In order to find more internal information on Artemis, [AnnualReports.com](http://annualreports.com) tool can be used to gather info on past projects involvements, and operations, key financial data, performance highlights, and overall health of the company.

1. **CrunchBase**

Crunchbase provides information on company funding rounds, investors, acquisition, and tech stack. It can show Artemis’s growth business model, and technological investments over time.

**Domain and IP Research:**

1. **Wireshark**

Wiresharkis a tool that operates in active recon for capturing, analyzing, and visualizing the traffics of Artemis. It helps to understand protocols such as HTTP, TCP, FTP. Wireshark is used by the red team to analyze the data coming from source to destination traffic.

1. **DNS History**

This tool contains the history of over 3.2 billion domains and 47 billion DNS which can easily benefit the recon of Artemis domain and ip research. It can give info about the owners of the company, registration dates, change in ip address, subdomain enumeration, DNS events and website traffic statistics.

**Pastebins**

1. **HaveIbeenPwned**

In this tool, it showcases all the data from data leaks of any person or company. Through this tool info like, email, phone number, and other sensitive information can be gathered and researched. With a database of large leakeddata finding information on Artemis can be beneficial from this tool.

1. **IntelX**

This is a search engine with data archives from various sources including the dark web, data leaks, and document sharing platforms. Hence it can help discover Artemis related leaks including accounts, names, IP address, passwords, date of birth, and email addresses.

**Conclusion**

The reconnaissance of Artemis Corporation involves strategic procedure with various tools. With the help of social media, breach databases, domain research tools, a comprehensive profile of Artemis can be created. Each OSINT tool has unique insights and will help to get as much information as possible within the legal boundaries.