The Reconnaissance phase for this project requires that we gather publicly available information to build our detailed profile target Artemis. I will be conducting a collection of information that identifies the possible vulnerabilities, the very understanding of the target's technological infrastructure, and gaining insight into their operations. Using readily available Open Source Intelligence (OSINT) techniques to gather details about Artemis. This is a company that truly mixes cloud and on-premise infrastructure. The following tools and methods will be launched and used to gather a range of publicly available data.

1. Google Querying and Dorking (Search Engine)

This method will help me to use advanced search operators to extract specific information from search engines. Through quotation and specific search querying.

The way I will do this for this project is to search for specific queries like "Artemis Contact Information" or "Artemis Resume site:linkedin.com", that way we can uncover email addresses, job listings, and employee profiles. The goal will ultimately help us to find employee contact information, social media, technologies, documents, and other sensitive information that search engines like Google can index from the query.

1. LinkedIn surveillance and Platform use (Social media)

LinkedIn is an incredibly powerful platform that can identify employees, job titles, and professional networks, groups, technologies, etc. The various we can use for this is the use of LinkedIn search and a specific scraping tool that can be used for LinkedIn through PhantomBuster. My goal is to be able to gather the OSINT of employee details, being role, skill, and other connections they may prove to be useful for. I will be able to uncover the potential technologies and tools that are used by Artemis in this way.

1. Bing Search (Search Engine)

Bing Search will do the same thing as Google Dorking when surfing on Google but through a different search engine that can have items that are not indexed by Google or any other search engine. To gain information about company details and employee intel.

1. Glassdoor (Job Board)

Glassdoor provides practically most details about company details, from salaries, roles, reviews at working at any company. This will work for our reconnaissance phase to gather information about Artemis' work environment, culture, and technologies, and types of employees employed to work there.

1. Indeed (Job Board)

Indeed is a standard but widely used job board. They post jobs all year round and include a lot of information similar to Glassdoor. This works for our investigation and plan.

1. Zoominfo (Company Research)

Zoominfo is a great source to extract information about company profiles, the heads and decision-makers, job title, contact information, and the “About” in the company. This will help bring the information we need.

1. Crunchbase (Company Research)

Crunchbase does a lot of the same that zoominfo does but highlights really important sensitive information and detail for gaining business details, funding history, and investment companies are a part of.

1. WHOIS Lookup (Domain and IP Research)

A searching tool that utilizes domain registrations to reveal registrars, owners, and in charge of admin information and contact. This will reveal all information regarding the domain of Artemis.

1. Pastebin (Pastebins)

A site that can paste and share text. Can be often used to steal sensitive information like credentials, code, and personally identifiable information (PII). Any information regarding Artemis can search, steal, and exploit the information that regards to the company’s credentials.

1. Shodan (Domain and IP Research)

Shodan is a large surveillance of all things regarding the Internet of Things (IoT). These can be servers, services that are exposed and unprotected, ports, etc. This would be a great way to obtain all the details regarding the Artemis domain and IP Research.

1. Ghostbin (Pastebins)

It is similar to pastebin, it allows the pasting and sharing of text. This text can pertain to data that is sensitive and is exposed. This data ranges from company-related leaks, tasks, and technical intel gathered from the company publicly.

1. Company Website (Company Research)

The company website is publicly available for everyone to view their information. Through here we can find out about employee information, contact details, and technical descriptions that the company uses and works with.

1. Monster (Job Board)

Contains detail and information about Artemis, this site works like any other job board like LinkedIn or Indeed. But this tool is much more extensive and provides much more about the details that are involved regarding an employer and tools, technologies, that are interviewed.

1. Twitter (Social Media)

This social media tool is incredibly vital to gathering information about most things. News, trends, and other important information can be posted there. Twitter has a lot of information regarding activities, updates, and other intel that can be sensitive in some nature. Tracking and utilizing Twitter API is another technique that can be huge for data reconnaissance.

1. Facebook (Social Media)

This works like other social platforms but with this social media it has the tool of Social Searcher or manual search. Data on employees (Professional or Personal) is all available. The tagging feature to mention or linked to their information is a tool that can be vital to reconnaissance and can be a way to exploit if human error occurs.