Reconnaissance Report on Artemis Gas, Inc.

Objective

The primary objective of reconnaissance is to collect data and construct a robust image of Artemis Gas, Inc. Publicly accessible data, such as personnel profiles, contact information, email addresses, technological stacks, and other details, may be included in this profile.

Procedure and Tools

1. Social Media: Social media platforms can be a great resource for collecting information about Artemis Gas employees, Inc.

- LinkedIn: Professional networking site LinkedIn can be used to identify key employees, roles, technical skills, and expertise. Job descriptions posted on LinkedIn can be useful to understand the technologies used by the company.
- X (formerly Twitter) or Facebook: Individual profiles of employees (especially higher-level employees) in these social media can be a great source of information. Information gathered from here can be used in social engineering, guessing passwords, or answering security questions.

2. Job Boards: Job postings on job boards such as Indeed, ZipRecruiter, Glassdoor, and LinkedIn can reveal information like types of software and technology, web servers, and cloud technologies.

3. Google Hacking: Google hacking or dorking involves advanced queries to reveal hidden information. Search queries such as “site: artemis.com filetype: pdf OR filetype:docx” will search the website for any PDF or DOCX files. Google Dorking can also help find hidden subdomains or directories that might contain sensitive information.

4. Wayback Machine (https://web.archive.org/): The older version of the company website archived in the Wayback Machine can reveal useful information, hidden directories, or documents.

5. Company website: The official company website can be a rich source of information. By analyzing the website, one can gather contact details, press releases, investor information, and insights into company operations. Information about services, technology stack, and organizational structure can also be obtained.

6. Public Code Repositories: Code repositories such as Github, Bitbucket, and CloudForge are used for code sharing and collaboration. A company’s open-source code can be a great resource for finding information such as credentials, IP addresses, or even private files that are accidentally uploaded to the public repository.

7. WHOIS Lookup: WHOIS databases provide information about the ownership and registration details of a domain. Using tools like whois.domaintools.com or whois.net, one can gather details on domain ownership, registration dates, and administrative contacts.

8. Metagoofil: Metagoofil can search metadata from documents that are available on the company's website. It can extract information such as author, company, title, and subject from PDF, doc, XLS, and other file types.

9. FOCA (Fingerprinting Organizations with Collected Archives): FOCA is a similar tool as Metagoofil. However, it can reveal additional information such as software and OS version information, printer information, username, plaintext password, internal network paths, and more.

10. TheHarvester: TheHarvester is an information-gathering tool. It can collect employee information from public data sources or social media. It can also collect information such as subdomain names, open ports, and service banners using Shodan.

11. Recon-ng: Recon-ng can be used to automate the collection of data from sources like search engines, social media, and other public records.

12. Maltego: Maltego can be used to visualize the gathered information. It creates a graph and shows connections between people, companies, email addresses, and all other information.

13. Shodan: Shodan is a search engine for IoT devices. It can be used to gather feeds from security cameras or other types of equipment. It can also be used as a part of physical penetration testing.

14. HaveIBennPawned: HaveIBeenPawned can be used to find out if any email addresses associated with the company have been part of known breaches, which can provide insights into potential security weaknesses.

15. Dark Web: The dark web can be a valuable resource for finding information on potential breaches, previously collected data dumps, and credentials related to Artemis Gas, Inc.

Conclusion

This reconnaissance phase utilizes a variety of tools and methods to gather comprehensive information on Artemis Gas, Inc. Information gathered in this stage provides a solid foundation for further security analysis and subsequent phases of the project.