Phase 1

Perform Reconnaissance

Phase 1: Perform Reconnaissance

Tool/Resource 1: Google/Bing search engines (Google Dorking)

Description: Search engines such as Google and Bing are powerful tools needed to conduct a passive reconnaissance that could help gather information about Artemis's profile. The information that Artemis posts can also provide information that is about their network. It is also possible to search for information or files that were leaked or not intended to be on the internet.

Usage: Search Artemis Gas INC and look up information that can be found and look up their website. Can use Google Dorking, such as search site:Artemis Gas INC ext:(pdf | CSV | xls| txt) (https://www.google.com/ or https://www.bing.com/)

Tool/Resource 2: OSINT Framework

Description: Another search engine that was originally created focused on IT security. OSINT framework can integrate data, processes, methods, tools, and techniques to help identify the information we need on Artemis.

Usage: Search Artemis Gas INC on all the framework sections and see what I can find that Google/Bing can't be found. Can try to check its IP addresses and domain name. (https://osintframework.com/)

Tool/Resource 3: nslookup

Description: Nslookup is a name server lookup that can be used on the Kali Linux command line to find DNS, IP address, or other records for DNS.

Usage: Using the Kali Linux command line, type in "nslookup (Artemis's website)," and it will show the IP address in IPv4 and IPv6. We can also type in "nslookup" on the command line, then "set type=ns," then "Artemis's website" this will give all the various name service and their IP addresses associated with Artemis. Or you can use the website (https://www.nslookup.io/)

Tool/Resource 4: WhoIs Lookup

Description: A query and response protocol that provides registration information for internet properties. We can gather the company's email address, phone number, and owner's name if there is no whoisguard protection.

Usage: Using the Kali Linux command line, type in "whois (Artemis's website)," and it will show information such as the creation date, updated date, and expiration date of the website as well as a registrant email that can be contacted with. If Artemis didn't use whoisguard protection, it is good to inform them. Or you can use the website (https://www.whois.com/)

Tool/Resource 5: Hurricane Electric Internet Services

Description: It is a global Internet service provider that offers internet transit, tools, and network application. We can find Artemis Gas INC's IP address range and the Autonomous system number.

Usage: Search Artemis Gas INC on the search bar and view the ASN and IP results range. (https://bgp.he.net/)

Tool/Resource 6: Maltego

Description: It is an OSINT and graphical link analysis tool that gathers and connects information for investigative tasks. We can use Maltego to passively gather information and build an understanding of how Artemis is structured.

Usage: Using the Paterva CTAS CE on Maltego, create a domain and put Artemis Gas INC's website as the domain. Then we can create a graph of other domains and sub-domain and the mail services that tell us where the mail is being handled. We can find out all the top-level domain associated with Artemis. We can also convert the domain into IP address sources, and with the email address, we can use them to find out the email addresses associated with those IP addresses. (https://www.maltego.com/)

Tool/Resource 7: DNSDumpster

Description: DNSDumpster is a trusted open-source security vulnerability scanner and network intelligence tool. This tool can discover the hard-to-find sub-domains and web hosts. We can use it to find Artemis's hidden domains.

Usage: Search Artemis Gas INC's website on the search bar, view all the IP addresses, and export it into a CSV file. Then maybe put all the IP addresses into a mass scanner and scan all the IP addresses. (https://dnsdumpster.com/)

Tool/Resource 8: Shodan

Description: A search engine for internet-connected devices. It's an internet scanner that may be able to find devices within the IP address range belonging to a company. It can scan for open ports, services, and autonomous system numbers. And identifying one or more on the network may give attackers a good starting point for attacking the company.

Usage: Search org: "Artemis Gas INC" port:21,445,3389,5900 on Shodan. Port 21 for FTP, 445 for SMB, 3389 for RDP, and 5900 for VNC. To scan if there is any of those port open. (https://www.shodan.io/)

Tool/Resource 9: theHarvester to find Employee names using LinkedIn

Description: A command line tool included in Kali Linux that can provide email accounts, subdomain names, virtual hosts, open ports/ banners, and employee names.

Usage: Using the Kali Linux command line, type in "theHarvester -d (Artemis's website) -l 1000 -b LinkedIn". -d = domain, -l = limit search, and -b = source. It will search for employees working in Artemis and their position on LinkedIn.

Tool/Resource 10: Censys

Description: A search engine that provides hosts and creates aggregate reports on how the website and certificates are configured and deployed. We can use Censys to find all the IP addresses containing Artemis company and the certificates containing Artemis.

Usage: Search Artemis Gas INC's website on the search bar, and view IPv4 and Certificates. (https://search.censys.io/)

Tool/Resource 11: Recon-ng on Kali Linux

Description: An OSINT reconnaissance framework that is written in Python. It can provide functions such as information-gathering techniques using various open sources. Using Recon-ng, information such as Geo-IP lookup, banner grabbing, DNS lookup, port scanning, sub-domain, and reverse IP lookup.

Usage: Using the Kali Linux command line, type in "recon-ng" and then "add domains (Artemis website)." After booting recon-ng on Linux, we have to add the workspace and domain of (Artemis website). Then we can type in "use recon/domains-hosts/google_domain_web and run it. And then, using google as a search engine, we can type in "use recon/domains-hosts/brute_hosts" and run it. This will help us check the different subdomains within the Artemis website.

We can type in "use recon/domains-contacts/pgp_search" and run it. This will search for all the email addresses associated with the domains. Typing "use recon/contacts-credentials/hibp_paste" and run it will check all the email accounts that we gathered on the Artemis website and put in all the potential passwords that we might be able to use against the email address users. Lastly, we can type in "use reporting/html" and run it to have a report.

Tool/Resource 12: BuiltWith

Description: A tool that targets the domain API and live domain API. BuiltWith can use it to scan the website and see what tech stack they got and see if there are any vulnerabilities.

Usage: Search Artemis Gas INC's website on the search bar and look at the detailed Technology profile, we will have an understanding of what the tech stack of Artemis will be and can maybe find some vulnerabilities within the tech stack. (https://builtwith.com/)

Tool/Resource 13: Hunter

Description: An email finder tool that can search for the company and its employees' email addresses.

Usage: Search Artemis Gas INC's website on the search bar and look for email addresses. Using email addresses attackers can use them for phishing attacks. (https://hunter.io/)

Tool/Resource 14: URL Fuzzer

Description: A tool that can discover any hidden, sensitive, or vulnerable files and routes in a web application and servers.

Usage: Search Artemis Gas INC's website on the search bar. We will be able to find any hidden files that search engines wouldn't be able to find easily. (https://pentest-tools.com/website-vulnerability-scanning/discover-hidden-directories-and-files)

Tool/Resource 15: Nmmapper

Description: A tool with multiple tools such as Sublister, DNScan, Lepus, and Amass to search for subdomains. It can provide the sub-domain, IP address, and ASN.

Usage: Search Artemis Gas INC's website on the search bar. Another tool that can help find and check the domain, sub-domain, and IP addresses for Artemis. (https://www.nmmapper.com/sys/tools/subdomainfinder/)