Phase 1. Perform Reconnaissance

Goal: Build as robust a profile on the target (Artemis) as possible. The profile should include the target's technology stack, email addresses, phone numbers, resumes, and so on.
Procedure: Detail the activities you plan to use to obtain as much publicly available information as you can.
Deliverable: Provide a minimum two-page description of all the tools and methods you will use to accomplish this task. Deliverable should cover at least 15 tools/resources

- ## WHOIS

  Whois is a tool that is commonly used to find information on a domain. I use Whois to find the company's domains, company number.

- ## Shodan

  We can rely on Shodan to feed us with detailed information. Like Google, Shodan is a search engine. It searches the invisible parts of the internet for information on internet-connected devices. This tool was helpful in finding what kind of servers that the company uses and what servers are in the same location as the control center and also finding ports.

- ## Linkedin

  Linkedin is an online platform that connects professionals. But sometimes those professionals add their emails and personal/work numbers onto their profiles. So, I can scrape all of this data in case I want to use the emails for brute force attacks or the phone numbers can be used for social engineering attacks.

- ## Google Hacking

  Google was used to find passwords, hidden files, metadata. People often use a resource called the google hacking database, which is a free online tool that stores useful google search queries that have been known to return interesting results.

- ## Maltego

  Maltego is an open-source intelligence (OSINT) and graphical link analysis tool for gathering and connecting information for investigative tasks.This can be useful in finding publicly available information on the target like emails, phone numbers, and mutual contacts.

- ## Nmap

  This tool gives me a list of open ports.

- ## Nessus

  After finding available ports, I will use Nessus to find vulnerabilities in the server.

- ## Pastebin

  I can use this to find pages that document passwords, database leaks and other sensitive information.

- ## Facebook

  I can find phone numbers and sometimes emails.

- ## Pipl

  This is great for gathering information about people and provide access to phone numbers, email addresses, addresses (past and present).

- ## PeekYou

  I could use this to find the target's public records.

- ## Job Sites

  Sites like indeed and glassdoor valuable resources for identifying technologies in use by the target organization. I would use Google Dorks to search <Artemis> site:indeed.com

- Netcraft

  Netcraft can be used to gather information about websites which are run by the target information and returns information such as its IP address, hosting provider, technology in use etc.

- theHarvester

  This tool searches through a range of data sources on the internet to collect information on a given person, system, company, or event.

- SpiderFoot

  A free tool that performs fingerprinting on a topic by linking together different discoveries about a given target.

- OSINT Framework

  Gives me a variety of tools to use for gathering information.