Simeon Hawkins
Capstone Project: Phase 1 Perform Reconnaissance

Phase 1. Performance Reconnaissance

Reconnaissance Report for Artemis, Inc.

Objective:

To gather as much publicly available information about Artemis, Inc. to build a robust profile for the penetration test.

Tools and Methods:

1. **Google Dorking**

   Tool: Google search engine
   Method: Using advanced search operators to find specific information about Artemis, Inc. such as file types, login pages, and employee information.
   Commands:

   - site:artemis.com filetype:pdf
   - site:artemis.com inurl:login
   - Intitle:"index of" site:artemis.com

   Findings:

- Found several PDF documents containing technical specifications and internal reports
- Discovered login pages for internal applications, including potential admin portals for the RFQ/RFP system.
- Identified directory listings exposing sensitive files, such as configuration files and internal documentation.

2. **WHOIS Lookup**

   Tool: whois command, Whois.com (WHOIS is a protocol used to query databases that store information about the ownership, registration, and administrative details of domain names and IP address blocks)
   Method: Identifying domain registration details and contact information
   Example Commands:

- whois command, Whois.com
- Using Whois.com to search for Artemis domain details

Findings:

- Domain registered to Artemis, Inc., providing contact details for domain administrators.
- Identified registration and expiration dates, as well as name servers associated with the domain.

3. **Wayback Machine**

Tool: archive.org (Known as the Internet Archive, is a non-profit digital library that offers free access to a vast collection of digital content, including websites, books, audio recordings, videos, images, and software.
Method: Viewing historical snapshots of the Artemis website to understand its evolution and possible vulnerabilities.
Example Usage:

- Access Wayback Machine and enter artemis.com to examine different snapshots of the website to identify changes in content, structure, and technology.

Findings:

- Historical versions of the website revealed older content management systems and unpatched vulnerabilities that might still be relevant.
- Changes in website structure and content provided insights into the company's growth and technological advancements.

4. **DNS Information**

Tool: nslookup, dig, host
Method: Gathering DNS records to understand the network infrastructure.
Example Commands:

- nslookup artemis.com (Maps a domain to its corresponding IPv4 address)
- dig artemis.com any (is a more powerful and flexible DNS query tool that provides detailed information about DNS records
- host -a artemis.com (a simple utility to perform DNS lookups. It is straightforward and can be used to query different DNS records

Findings:

- Identified multiple subdomains, including mail servers and development environments
- Discovered DNS records indicating the use of various cloud services (AWS) and on-premises solutions (located in Houston, Paris, Cairo, and Singapore).

5. Metadata Extraction

Tool: exiftool (command-line application for reading, writing, and editing metadata in a wide variety of file formats. Developed by Phil Harvey, ExifTool is widely used for managing metadata in images, videos, audio files, PDFs, and more.
Method: Extracting metadata from public documents to find sensitive information
Example Commands:

- exiftool document.pdf
- exiftool -r /path/to/documents

Findings:

- Metadata from documents revealed usernames, software versions, and document creation/modification date.
- Identified potential internal network paths and directory structures, including references to SAP and Oracle 12c systems.

6. Network Scanning

Tool: Nmap (Network Mapper) is a powerful open-source tool used for network discovery and security auditing.
Method: Identifying live hosts, open ports, and running services on the network
Commands:

- nmap -sP 192.168.1.0/24
- Nmap -sV -p 80, 443 artemis.com

Findings:

- Discovered several live hosts within the target IP range, including servers potentially related to the operations control center in Houston.
- Identified open ports and services, including HTTP, HTTPS, and SSH, on these hosts.

7. **Subdomain Enumeration**

   Tool: Sublist3r (open-source tool used for subdomain enumeration. It helps in discovering subdomains for a given domain through various public sources and APIs), **Amass** (known for its capabilities in subdomain enumeration, but it also provides other features for gathering information about an organization's external attack surface. Amass integrates data from various public sources, APIs, and scraping techniques to provide a comprehensive view of an organization's online presence.
   Method: Identifying subdomains associated with Artemis, Inc.
   Commands:

   - Sublist3r -d artemis.com
   - Amass enum -d artemis.com

   Findings:

- Found subdomains such as dev.artemis.com, mail.artemis.com, and vpn.artemis.com
- Subdomains indicated the presence of development, email, and remote access systems.

8. **Web Crawling**

   Tool: Burp Suite (provides a suite of tools that work together to support the entire testing process, from initial mapping and analysis of an application's attack surface to finding and exploiting security vulnerabilities), **OWASP ZAP** (web application security scanner and testing tool. ZAP provides an easy-to-use interface and a rich set of features, making it suitable for both beginners and experienced security testers).
   Method: Crawling and mapping the Artemis web application to identify potential vulnerabilities.
   Usage:

- Use Burp Suite to intercept and analyze web traffic while browsing the Artemis website.
- Use OWASP ZAP to perform an automated crawl of the site.

   Findings:

- Identified hidden pages and parameters susceptible to injection attacks
- Detected outdated libraries and plugins used in the web application.

9. **Social Media Analysis**

   Tool: LinkedIn, Twitter
   Method: Gathering information about employees and their roles
   Searches:

- Collected information on key personnel, including job titles, departments, and contact details.
- Identified public discussions related to Artemis's projects and partnerships.

10. **Email Harvesting**

   Tool: theHarvester (can query multiple public data sources to gather information about a target)
   Method: Collecting email addresses from public sources.
   Commands:

- theHarvester -d artemis.com -b google
- theHarvester -d artemis.com -b linkedin

   Findings:

- Harvested numerous email addresses of employees, useful for social engineering attacks.
- Identified email patterns used by the organization.

11. **SNMP Enumeration**

   Tool: snmpwalk (this tool is commonly used by network administrators and security professionals to monitor and manage network devices, such as routers, switches, and servers)
   Method: Gathering information from SNMP-enabled devices
   Commands:

- snmpwalk -v 2c -c public artemis.com

   Findings:

- Retrieved information on network devices, including configurations and firmware versions.
- Identified potential misconfigurations and outdated firmware.

12. **Public Documents Search**

Tool: Google, Bing
Method: Searching for publicly available documents containing sensitive information.
Commands:

- site:artemis.com filetype:doc
- site:artemis.com “confidential”

Findings:

- Found documents containing internal reports and project details
- Documents exposed sensitive information such as strategic plans and technical specifications.

13. **Phone Calls**

Method: Calling employees to gather information (ethical considerations apply).
Example:

- Contacting helpdesk to inquire about security policies

Findings:

- Gained insights into internal processes and potential weak points in security policies.
- Discovered information on IT support procedures and common issues faced by employees.

14. **Pastebins**

Tool: Pastebins.com, other paste sites
Purpose: To find potentially leaked information related to Artemis, Inc.

Method: Search paste sites for mentions of Artemis, Inc. or related keywords

15. **Job Boards**

Tool: Indeed, Glassdoor, LinkedIn Jobs
Purpose: To gather information from job postings that might reveal technology stack details and other internal information.
Method: Search for job postings by Artemis, Inc. to find information about technologies used, job roles, and organizational structure.

Conclusion:

The reconnaissance phase has yielded a comprehensive overview of the publicly available information about Artemis, Inc. This data will inform the subsequent stages of the penetration test, ensuring all team members are familiar with the tools and techniques to be utilized. This approach will optimize the testing process and help meet the client's expectations.