Structured Walkthrough
For
Artemis Gas Inc.

Capstone Project by Cyrus Lomibao

Introduction

This capstone project is a structured walkthrough penetration test of a fictional company, Artemis Incorporated. A structured walkthrough is an organized procedure ofor a group of peers to review and discuss the technical aspectos of various IT, IT Security, and IT Audit work products. The major objectives of a structured walkthroughtare to find errors and improve the quality of the product or service to be delivered.

This document provides a comprehensive overview of the project and the expected deliverables.

Client Overview

ARTEMIS GAS INC. ("Artemis"), based in Paris, France, is present in 40 countries with approximately 30,000 employees and serves more than 1.7 million customers and patients. Oxygen, nitrogen, and hydrogen have been at the core of its activities since its creation in 1922. They own and operate over 1,000 miles of industrial gas pipelines in the U.S., supplying mainly oxygen, nitrogen, hydrogen, and syngas in large quantities from multiple production sources to major customers in the chemicals, petrochemicals, refining, and steel industries. Their pipeline operations and industrial gas production facilities are closely monitored 24/7 within their leading-edge operations control center located in Houston, TX. Their operations control group monitors over 49,000 data points and assists with product supply and coordination. They are constantly optimizing their supply network to provide high reliability and energy efficiencies, allowing Artemis to adjust supply needs more quickly and effectively, thus enabling growth for their customers.

Artemis quickly grew over the past few years, and the need to "make things work" has outpaced the need to "make things work securely." Some security solutions are fairly mature and effective; some are less so. Among the company's concerns are:

- Some older network hardware, in the process of being phased out, is unsupported and may have unpatched vulnerabilities.
- Some newer network hardware may not have been configured properly.
- Some business units do not always follow company policy regarding storing data in the cloud, creating websites, or conducting file transfers.
- Some IT admins like to do their own thing because "that's the way they've always done it." This could be exposing the network to unknown risks.

Technology Overview

Artemis utilizes a mix of security vendors and technologies. The firewall landscape consists of Cisco, Fortinet, and Palo Alto. They use F5 (Big IP) for load balancing, and for secure remote application access, they use Zscaler. Roughly half of their servers and applications are in the cloud (AWS), and the rest are on-prem. These on-prem assets are spread out among four major data centers located in Houston, Paris, Cairo, and Singapore.

The network is currently transitioning to SD_WAN so there are still several MPLS links, especially in the smaller, more remote locations. The old Cisco equipment is being phased out in favor of the Fortigate devices from Fortinet. Additionally, since the Forigates can also act as firewalls, the company is considering eliminating the rest of its Cisco gear to cut costs. They are unable to supply a current network diagram. The ones they have are severely out of date and would not be of any use to you.

Internally, Artemis utilizes a Single Sign-On (SSD) solution that leverages Microsoft Active Directory to authenticate users to other applications. SAP is the company's primary ERP system and runs on Linux and Oracle 12c servers. Prem Microsoft Exchange servers. The only other applications of note are the PARS system and the APOLLO system.

PARS allows engineers to submit technical information regarding potential patents. If the submission passes legal and technical review, it is forwarded to the Intellectual Property group for submission to either the US Patent Office, the National Institue of Industrial Property (INPI) in France, or both. APOLLO is the repository for trade secrets, primarily around manufacturing processes.

Phase 1: Perform Reconnaissance of the Client and the Perimeter Network

Goal: Build a robust profile on Artemis Gas Inc. The profile should include the technology stack, email addresses, phone numbers, resumes, etc…

Step 1: Identify Tools and Techniques for OSINT

Tools:

1. **Maltego**: A graphical link analysis tool to visualize relationships and find hidden connections between pieces of information (e.g., people, emails, users, web addresses). This tool will help find public information about the company and help make decisions on removing any information that should not be available. Additional features are available at a cost.

2. **Recon-ng**: A full-featured web reconnaissance framework written in Python, Recon-ng is a reconnaissance / OSINT tool with an interface similar to Metasploit. Running recon-ng from the command line speeds up the recon process as it automates gathering information from open sources. Recon essentially offers the same features as Maltego without the image graph.

3. **theHarvester**: A command line tool for gathering emails, subdomains, hosts, employee names, open ports, and banners from different public sources that acts as a wrapper for

various search engines. However, theHarvester’s passive approach is stealthier, because it only extracts email addresses from the Google search. The active mode is more comprehensive. The stealth vs quantity decision is dependent on the pen tester.

4. **Shodan**: A search engine for Internet-connected devices to find vulnerable devices and systems. Instead of indexing websites, it scans the web for devices and provides information about them such as operating systems, open ports, and services running.

5. **Google Dorks**: Advanced search techniques using specific queries to uncover hidden information. Using specific search queries for certain phrases, or topics using operators, this technique refines the search for pinpoint results. For example:
   Filetype: This operator searches for specific file types. (eg., `filetype:pdf` would return PDF files.)

6. **FOCA (FIngerprint Organizations with Collected Archives)**: A tool to find metadata and hidden information in documents and is capable of analyzing a wide variety of documents, with the most common being Microsoft Office, Open Office, or PDF files.

7. **SpiderFoot**: An automated OSINT tool that scans the web for information about an IP address, domain, or other targets and can be defensively used to gather information on what the organization might have accidentally exposed over the internet.

8. **WHOIS Lookup**: Provides domain registration information using a query and response protocol for querying databases that store internet registration information on users or assignees within the organization.

9. **DNS Enumeration**: Identifies DNS records to understand the domain’s structure. This process discovers all DNS records for a domain, hostnames, IP addresses, and services running which may reveal potential vulnerabilities.

10. **Subdomain Enumeration**: Find subdomains that could lead to entry points. By enumerating all subdomains, you may find subdomains that are less protected than the root domain of the organization, making them more vulnerable to attack.

11. **Social Media Profiling**: Analyze the social media presence of Artemis and its employees. This process may reveal information that can be used as an attack vector for malicious hackers, such as company emails, vendor affiliations, or trade secrets.

12. **Website Mirroring**: Downloads a website for offline analysis. Creating an exact copy of a website’s content and structure for various purposes such as offline browsing, archiving, testing, and backup in case availability gets compromised. Tools include HTTrack, Wget , and SiteSucker.

13. **LinkedIn**: Gathers information about employees and their roles. This can help to understand the company’s structure, key personnel, technologies used, and potential vulnerabilities. Article postings by employees or key company officials may unintentionally give out trade secrets as public information.

14. **Pastebin**: Searches for potentially leaked information. Pastebin is a web application where users can store plain text, often used to share snippets of code. However, it can also inadvertently be a source of sensitive information leaks, such as credentials, configuration files, and other sensitive data.

15. **Public Code Repositories**: (e.g., GitHub, GitLab, and Bitbucket) Searches for exposed code or credentials. These repositories are where developers often host, share, and collaborate on code. Sensitive information like credentials, API keys, or proprietary code is sometimes accidentally exposed. Examples of Search Queries include:

    GitHub:

    ```
    org:Artemis “AWS_SECRET_ACCESS_KEY”
    org:Artemis “db_password”
    org:Artemis “private key”
    ```

    GitLab:

    ```
    in:Artemis “token”
    in:Artemis “secret”
    ```

---

2. Techniques:

- **Social Media Profiling**: Analyzing the company’s and employees’ social media presence to gather insights.
- **WHOIS Lookup**: Obtaining domain registration information.
- **DNS Enumeration**: Identifying DNS records to understand the domain’s structure.
- **Subdomain Enumeration**: Finding subdomains that could lead to entry points.
- **Metadata Analysis**: Extracting metadata from publicly available documents.
- **Network Footprinting**: Mapping the network's architecture and identifying potential entry points.
- **Website Mirroring**: Downloading a website for offline analysis.

Step 2: Documentation and Organization

Documentation:

- **Reconnaissance Report Template**: A structured document that includes sections for each type of information gathered.
- **Introduction**: Overview of the reconnaissance phase.
- **Tools and Techniques Used**: Detailed list of tools and techniques.
- **Findings**:
  - **Domain and IP Information**: Details from WHOIS and DNS records.
  - **Subdomains**: List of discovered subdomains.
  - **Social Media Insights**: Information from social media profiles.
  - **Metadata Findings**: Extracted metadata from documents.
  - **Network Architecture**: Overview of the network structure.
- **Potential Vulnerabilities**: Initial analysis of potential weak points.
- **Conclusion**: Summary of findings and next steps.

Organization:

- **Digital Filing System**: Use a digital filing system with clear naming conventions for easy access.
  - **Folder Structure**:
    - /Reconnaissance/Domain_Information/
    - /Reconnaissance/Subdomains/
    - /Reconnaissance/Social_Media/
    - /Reconnaissance/Metadata/
    - /Reconnaissance/Network_Architecture/
- **Collaboration Tools**: Utilize collaboration tools such like SharePoint or Confluence for team access and version control.

Step 3: Utilize Gathered Information

---

1. Correlate Findings:

Cross-reference information from different sources to find patterns and potential vulnerabilities.
Identify key assets and points of interest to be targeted in later phases.

---

2. Prioritize Targets:

Focus on high-value targets identified during reconnaissance.
Develop a target list based on the impact and likelihood of vulnerabilities.

---

3. Plan Subsequent Phases:

Use the gathered information to refine the scope of vulnerability scanning and exploitation. Based on the findings, develop a detailed timeline and task list for the next phases.

Deliverable for Phase 1:

Reconnaissance Report: A comprehensive document detailing all findings from the OSINT process, organized and presented clearly and professionally.

This outlines the plan for Phase 1 of the structured walkthrough penetration test for Artemis. Ensure that your team is familiar with the tools and methods detailed here as they will be crucial for success in executing this phase.

Next Steps:

Prepare for Phase 2, which will involve vulnerability scanning based on the reconnaissance information gathered.