# Detailed Technical Report

For Artemis Gas, Inc.

August 14th, 2024

By: Humayun Ahmed

## Table of Contents:

## Scope of the Project

The security assessment focuses on conducting a comprehensive penetration test on the client's network infrastructure, specifically targeting two accessible servers locate at IP addresses 192.168.1.75 and 196.1681.76. The assessment was performed from a black box perspective, meaning no prior knowledge about the internal network structure, configurations, or application running on the servers was provided to the penetration testing team. The only information was the IP addresses of the servers under test.

The testing process included the following activities:

- Reconnaissance: Gathering as much information as possible about the target servers without triggering any alerts.
- Scanning: Using various tools to identify open ports, services, and potential vulnerabilities.
- Exploitation: Attempting to exploit identified vulnerabilities to gain access or escalate privileges within the target systems.
- Post-ExploitationL Assessing the potential impact of successful exploitation, such as data extraction or further lateral movement within the network.

The scope of the assessment was strictly confined to the specified IP addresses, ensuring the no other systems o network segments were targeted or affected during the testing process. All activities were conducted ethically and in a controlled manner, with minimal disruption to the client's operations.

## Project Objectives

The primary objective of this security assessment is to evaluate the security posture of Artemis Gas, Inc.'s internet-facing servers. The goal is to identify and analyze potential vulnerabilities within the specified IP addresses and to assess their susceptibility to exploitation by malicious actors. This assessment aims to provide actionable insights into the most critical security weaknesses that could be leveraged in real-world attacks. Given the scope and time constraints of this engagement, the assessment focused primarily on identifying and testing vulnerabilities that are immediately exploitable. These include, but are not limited to, weaknesses in open ports, running services, outdated software, and common misconfigurations. The vulnerabilities discovered during the assessment were assigned risk ratings based on three key factors:

1. Threat Level: The likelihood of an attacker targeting the identified vulnerability.
2. Vulnerability Severity: The potential impact of exploiting the vulnerability.
3. Business Impact: The potential consequences of a successful attack on the organization's operations, reputation, and data security.

The results of this assessment are intended to assist Artemis Gas, Inc. in prioritizing remediation efforts and enhancing their overall security posture.

## Assumptions

Several assumption were made during the preparation and execution of this penetration testing report to ensure clarity and accuracy in the findings:

1. Public IP Addresses: It is assumed that both IP addresses are publicly ;accessible and exposed to the internet. This assumption underpins the focus on external threats and the potential for remote attacks.
2. Non-Disclosure Agreement (NDA): It is assumeed that a Non-Disclosure Agreement (NDA) and Rules of Engagement (RoE) were signed prior to the commencement of the assessment. These documents outline the legal and ethical boundaries of the testing activites, ensuing that all parties understand the scope, limitations, and responsibilities involved.
3. Company Information: Based on the initial information gathering phase, it is assumed that the target organization is Artemis Gas, Inc. This assumption guided the context and focus of the assessment, particularly in evaluating the business impact of potential security breaches.
4. System Configuration: It is assumed that the systems being tested are configured as they would be in a production environment, meaning no special adjustments were made to harden or alter the system configuration specifically for the purpose of this test.
5. TIme Constraints: The assessment was conducted under a limited timeframe, which influenced the decision to focus on the most critical and exploitable vulnerabilities. It is assumed that the time constraints did not allow for exhaustive testing of all possible attack vectors.

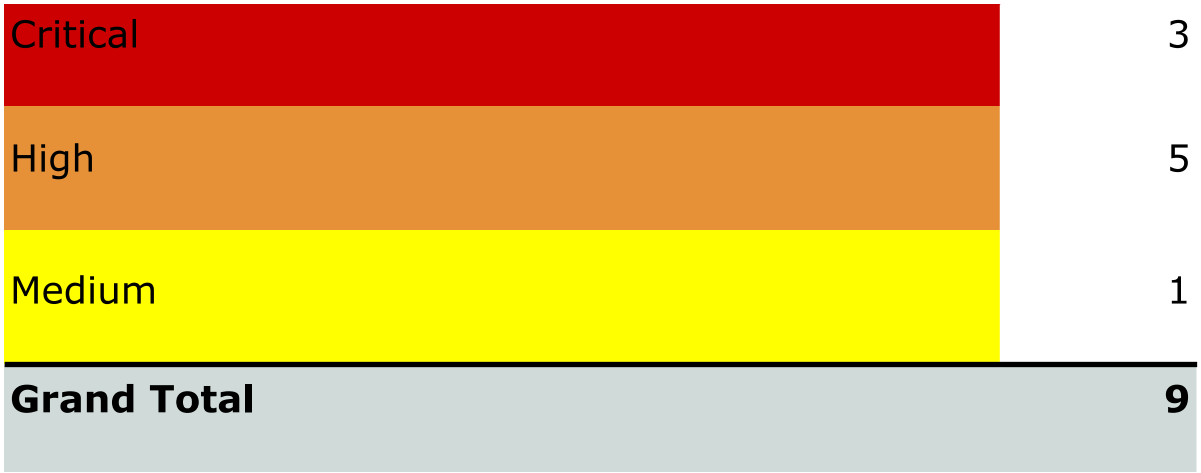
These assumptions were necessary to frame the scope of the assessment and ensure that the findings are relevant and actionable for Artemis Gas, Inc.

## Timeline

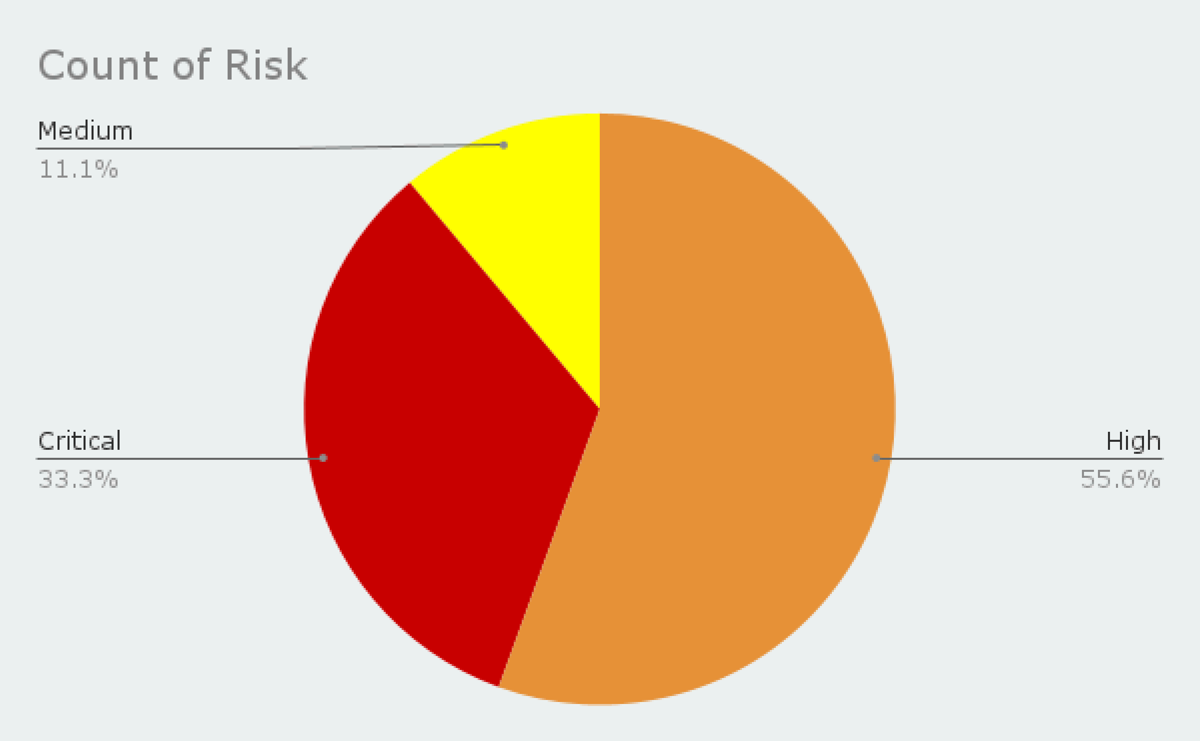
The timeline of the test is as below:

| Penetration Testing Stage | Start Date | End date |
|---|---|---|
| Initial reconnaissance, vulnerability scanning, and cloud security assessment. | July 24th, 2024 | July 28st, 2024 |
| Detailed analysis of findings, exploitation simulations, and risk assessment. | July 29th, 2024 | August 2nd, 2024 |
| Drafting of the Detailed Technical Report, including vulnerability details, risk analysis, and recommended remediation actions. | August 3rd, 2024 | August 8th, 2024 |
| Final review with the IT team, refinement of the report, and submission to senior management. | August 9th, 2024 | August 14th, 2024 |

## Summary of Findings:



| | |
|---|---|
| Critical | 3 |
| High | 5 |
| Medium | 1 |
| **Grand Total** | **9** |



Artemis Gas, Inc. needs to significantly improve its information security practices. During our assessment, we were able to access a critical server in under a very short time, highlighting serious vulnerabilities. Strengthening processes, personnel training, and system hardening is essential.

Key findings from the penetration test include:

- Unpached RDP Exposed to the internet: Windows server 2019 had exposed and unpatched RDP services, posing risks as unauthorized access, data theft, and ransomware attacks. Immediate firewall policy updates are needed.
- Web Application Vunlenarbilities: Several web applications were found vulnerable to SQL injection and broken access control, risking unauthorized data access. Secure coding practices and proper access controls should be enforced.

- Default Password on CIsco Admin Portal: A default password was found on the Cisco admin portal, increasing the risk of unauthorized access. Strong unique passwords should be implemented.
- Outdated software and misconfiguration: Servers, including Apache, Oracle WebLogic, and Microsoft Exchange, were found vulnerable due to outdated software and misconfigurations. Immediate patching and proper configuration are essential.
- Misconfigured CLoud Storage: AWS security groups were misconfigured, exposing cloud storage to unauthorized access. Proper configuration and access restrictions are necessary.

These vulnerabilities expose Artemis Gas, Inc. to significant risks. Immediate remediation, improved patch management, and secure configurations are critical to protecting the company's assets.

## Recommendations

Based on the identified vulnerabilities and risk analysis, the following recommendations are made to improve the security posture of Artemis Gas, Inc.:

1. Patch Management:
   - Implement a regular pach management cycle to ensure all the systems are up-to-date with security patches.
   - Prioritize the patching of critical vulnerabilities, especially those exposed to the internet.
2. Access Controls:

   - Enforce strong access controls, including the use of multi-factor authentication and least privilege principles.
   - Review and update default passwords on all the network devices and applications.
3. Web Application Security:
   - Secure web applications by implementing input validation, WAFs, and secure coding practices.
   - Conduct regular web application security testing to identify and fix vulnerabilities.
4. Network Security:
   - Regularly audit network devices for default credentials and insecure configurations.
   - Implement network segmentation to limit the impact of a compromised device.
5. Cloud Security:
   - Review and correct cloud storage configuration to ensure no unauthorized access is possible.
   - Implement AWS Config for continuous monitoring of security compliance.
   - Enable encryption for sensitive data stored in the cloud.
6. Employee Training:
   - Provide regular cybersecurity training to employees to raise awareness about phishing, social engineering, and other attack vectors.

   - Encourage reporting of suspicious activities and provide clear guidelines for responding to potential security incidents.
7. Incident Response Planning:
   - Develop and regularly update an incident response plan to quickly and effectively respond to security breaches.
   - Conduct regular exercises to test the effectiveness of the incident response plan.

## Conclusion

The vulnerability assessment conducted for Artemis Gas, Inc. has identified several critical risks that could significantly impact the organization's IT infrastructure and overall business operations. By addressing these vulnerabilities and implementing the recommended security measures, Artemis Gas, Inc. can enhance its security posture, protect its assets, and reduce the likelihood of a successful cyber attack.

It is crucial that the IT department prioritizes the remediation of the identified high-risk vulnerabilities and continuously monitors the environment for new threats. The support of senior management is essential in allocating the necessary resources and ensuring the implementation of a robust security framework.