CONFIDENTIAL

Artemis Gas Inc.

Penetration Test Conducted by Vinay

EXECUTIVE SUMMARY

Artemis Gas Inc. is a company that focuses on producing natural gas. They worked with me to do a vulnerability assessment. This helped us figure out how likely it is for our security to be at risk from either people inside the company or outside threats. In August 2024 I checked for weaknesses in Artemis's network security. I did this by testing from outside the network using a security analyst's computer connected to the internet and from inside the network using the analyst's laptop connected to Artemis's internal network. This report gives a summary of all the main findings and shows charts with numbers for all the problems found. Suggestions will be given for important and risky weaknesses. The assessment results indicate that Artemis Gas Inc. will be vulnerable to attacks from both external and internal threat actors unless it addresses the following:

- Improve patch management procedures for critical updates to the operating system and services
- Put proper security controls in place for new network devices
- Make sure to put security measures in place while developing software to prevent code injection risks.
- Configure IAM permissions to remediate insecure cloud services
    - I identified 3 critical and 2 high risk vulnerabilities on the external network and 1 high risk vulnerability on the internal network. I recommend remediation of the critical and high-risk vulnerabilities within the next 30 days to reduce the risk of exposing the networks to attacks.

Key Summary Findings and Recommendations:

VENDOR RECOMMENDATIONS:

1. An unprotected Windows web server and exchange server that can be accessed by the public were discovered. Not updating these hosts and services puts the internal network at risk of being attacked which could lead to a data breach or compromise the entire internal IT system.

2. The SQL statements and PHP scripts are vulnerable to malicious attacks. Input validation and dynamic code testing has to be performed throughout the software development life cycle.

VENDOR RECOMMENDATIONS:

Management needs to incorporate secure code at the very beginning of the software development process by using an agile framework.

3. Weak configurations on Cisco router and overly permissive IAM policies on AWS.