Artemis Gas, Inc. - Penetration Test Report

Executive Summary

This fictional penetration test for Artemis Gas, Inc. identified several critical vulnerabilities in the company's IT infrastructure. Key findings include exposed RDP access, misconfigured AWS environments, unpatched Oracle and Exchange servers, and web application SQL injection risks. These exposures present a high risk of data breaches, operational disruption, and lateral movement across critical infrastructure components.

Key Findings

- Exposed RDP access without patching (CVE-2019-0708)
- SQL injection in customer-facing web application
- Default credentials on Cisco admin portals
- Misconfigured AWS security groups
- Unpatched Oracle WebLogic (CVE-2020-14882) and Microsoft Exchange (CVE-2021-26855)
- Sensitive data exposure and lateral movement risk into SCADA-adjacent systems

Recommendations

- Immediate patching of remote access points
- Harden web applications with input validation and WAFs
- Remove default passwords and enforce strong credential policies
- Restrict cloud access with least privilege IAM policies
- Implement network segmentation and IDS/IPS tools
- Develop and routinely test an incident response plan

Note

This report is a fictional case study derived from a cybersecurity training simulation. It is included in the Cyber Exposure Database to represent high-risk infrastructure clients for underwriting analysis.