<u>**Phase 5: The Detailed Technical Report**</u>

Springboard

Findings Report

ARTEMIS GAS, INC.

Customer Name: Artemis Gas, Inc.

Project Name: Artemis Gas Pentest

Testing Date: 07-21-2023 - 08-03-2023

Version: 1.0

Creation Date: 07-01-2023

Presented By: Chad Warner

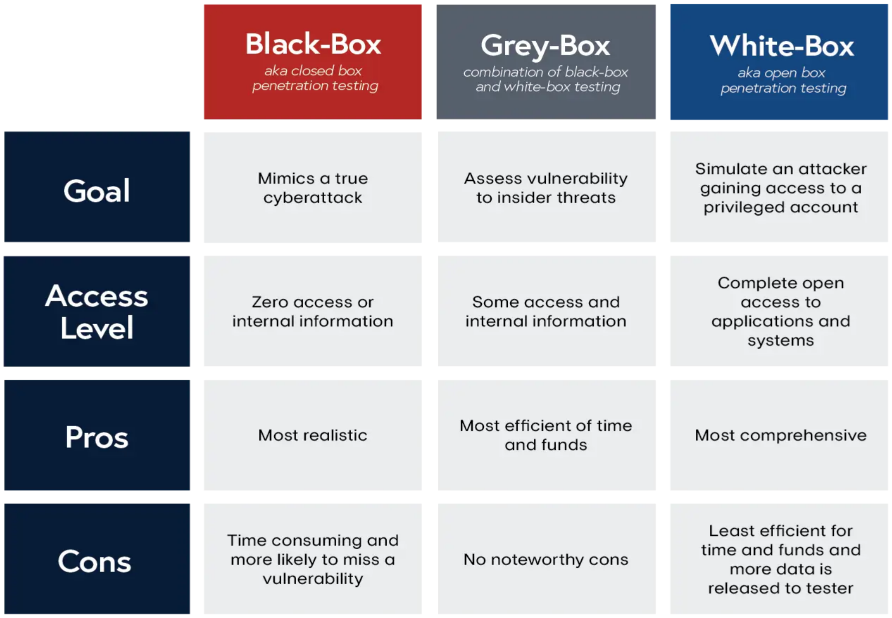
<u>FINAL REPORT</u>

Presented To: Olayemi Agbeleye

C. Table of Contents

D. Scope of Work

The scope of this pentest is to identify the target systems, networks, applications, and data. The perspective of this evaluation is from a Grey-Box tester. After the scope is defined, we will conduct a vulnerability assessment and highlight weaknesses in the system.



	Black-Box *aka closed box penetration testing*	Grey-Box *combination of black-box and white-box testing*	White-Box *aka open box penetration testing*
Goal	Mimics a true cyberattack	Assess vulnerability to insider threats	Simulate an attacker gaining access to a privileged account
Access Level	Zero access or internal information	Some access and internal information	Complete open access to applications and systems
Pros	Most realistic	Most efficient of time and funds	Most comprehensive
Cons	Time consuming and more likely to miss a vulnerability	No noteworthy cons	Least efficient for time and funds and more data is released to tester

A. What are the target organization's biggest security concerns:

a. Disclosure of Sensitive Information
b. Escalation of Privilege
c. Data Breaches
d. Installation of Malware
e. Ransomware
f. Man-in-the-Middle Attacks
g. Data Leakage
h. Destruction of the infrastructure
i. Distributed Denial of Service Attacks
j. Compromising Data Integrity

k. Denial of Service Attacks
l. Compromising System Availability
m. Compromising Data Confidentiality
n. Broken Access Controls
o. Authentication
p. Software Flaws
q. Encryption

B. What specific hosts, network address ranges, or applications should be tested:

A. Company's internet assets
B. Applications on-site and AWS
C. PARS system
D. APOLLO system

C. What specific hosts, network address ranges, or applications should NOT be test:

N/A

D. List any company assets in the systems or networks that are in scope as well as which systems they own :

A. F5
B. Cisco
C. Fortinet
D. Palo Alto
E. Zscaler
F. AWS applications
G. AWS servers
H. SAP
I. Linux
J. Oracle 12c
K. Exchange Online

E. Will the test be performed against a live production environment or a test environment:

This penetration test will be conducted in a test environment

F. **Will the penetration test include the following testing techniques:**

  a. **Ping sweep of network ranges:** YES

  b. **Port scan of target hosts:** YES

  c. **Vulnerability scan of targets:** YES

  d. **Penetration into targets:** YES

  e. **Application-level manipulation:** YES

  f. **Physical penetration attempts:** NO

  g. **Social engineering of people:** NO

  h. **Are Denial of Service attacks allowed:** YES

E. Project Objectives

E.1 - Objectives

1. **Objective:** Enumerate the vulnerabilities in the company's assets internally and externally. To provide recommendations to reduce the threat landscape.

Method: Determine and assess the vulnerabilities. Apply controls to remediate vulnerabilities that require immediate attention.

E.2 - Process

This comprehensive pentest will consist of 5 stages.

In **Phase 1**, we conducted and outlined methodologies to perform reconnaissance, active and passive, about Artemis Gas Inc. In Phase 1, we will discuss in detail the tools and resources that we used to perform the reconnaissance.

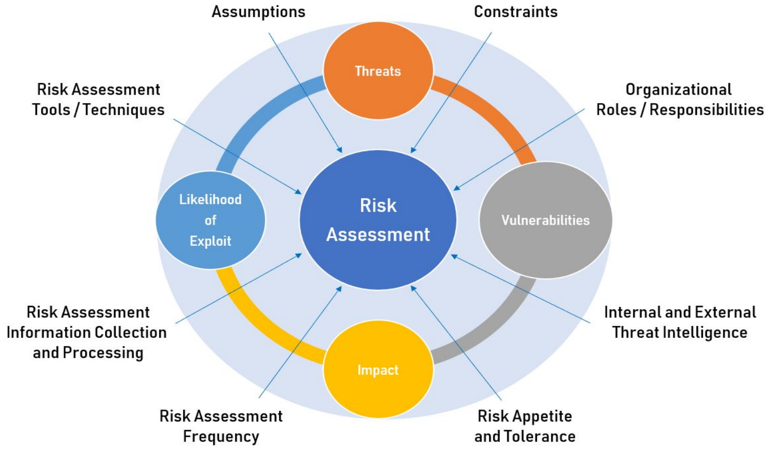
During **Phase 2**, we conducted and ran scans on the target (Artemis Gas Inc). We will discuss in detail the tools and resources that we used to perform the host discovery and enumeration.

During **Phase 3**, we conducted a vulnerability scan of the system. We will discuss in detail the tools and techniques that we used to perform the vulnerability scan.

During **Phase 4**, we conducted a threat assessment based on the client's (Artemis Gas Inc.) network. We will discuss in detail the resources and techniques that we used to conduct the threat assessment.

During **Phase 5**, we researched, implemented, and prepared a report based on the findings that we concluded.

F. Assumptions


Assumptions
Constraints
Threats
Risk Assessment Tools / Techniques
Organizational Roles / Responsibilities
Likelihood of Exploit
Risk Assessment
Vulnerabilities
Risk Assessment Information Collection and Processing
Internal and External Threat Intelligence
Impact
Risk Assessment Frequency
Risk Appetite and Tolerance

Risk Assumptions: How your organization currently perceives risk factors such as threats, weaknesses, loss expediencies, consequences (fines, penalties, loss of confidence), and exploit probability.

For the purpose of this report, we're going to assume that Artemis Gas Inc.,

A. Artemis Gas, Inc.'s network is not safe

    a. **Artemis Gas Inc.’s network is NOT safe because there are many identifiable vulnerabilities.**

B. Artemis Gas Inc.will prioritize the vulnerabilities based on the business impact and the determined severity of the vulnerabilities.

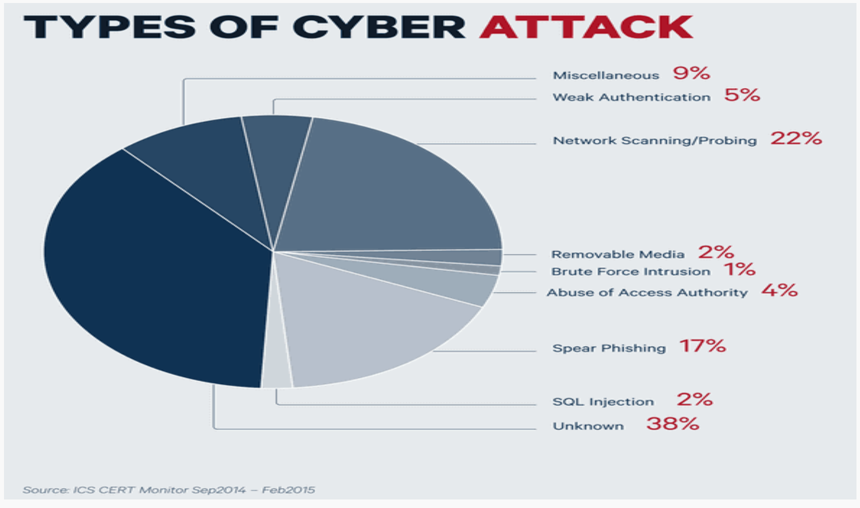
    a. Artemis Gas Inc.’s internal policy threat assessment will include a methodology to prioritize threats.

C. The client would like to be in compliance in accordance with laws and regulations.

    a. Artemis Gas Inc.’s policies and procedures should be aligned with the current laws and regulations

D. Artemis Gas Inc. has a risk strategy of “Mitigation” - Risk is reduced through the application of controls, enhanced safety features, implementation of technical safeguards, or use of countermeasures.

    a. The vulnerability assessment’s objective will incorporate remediation tactics and Artemis Gas Inc. will likely mitigate the found vulnerabilities.



Source: ICS CERT Monitor Sep2014 – Feb2015

G. Timeline

Vulnerability	Week 1	Week 2	Week 3	Week 4
Microsoft Exchange Server vulnerable to CVE-2021-26855	🟩	🟩	🟩	🟩
Oracle WebLogic Server vulnerable to CVE-2020-14882	🟧	🟧	🟧	🟧
Default password on Cisco admin portal	🟧			
Web server is exposing sensitive data	🟦	🟦	🟦	🟦
Web Application is vulnerable to SQL injection	🟦	🟦	🟦	🟦
Apache web server vulnerable to CVE-2019-0211	🟨	🟨		
Unpatched RDP is exposed to the internet	🟩	🟩	🟩	
Web application has broken access control	🟥	🟥	🟥	🟥
Misconfigured cloud storage	🟪	🟪		

H. Vulnerabilities Identified

Internal Vulnerabilities

During the internal phase of the assessment, Springboard identified a total of **9** vulnerabilities. This includes a total of **four (4)** critical findings, **four (4)** high findings, and **one (1)** low findings.

Internal Critical Findings

Most of the security issues identified and discussed throughout this document relate to unpatched systems and insecure system or application configurations that could allow an attacker to gain unauthorized access to restricted or sensitive data, or to directly compromise **Artemis Gas Inc.** assets. **Springboard** has analyzed these findings and provided details of each, along with mitigation strategy recommendations, below. Efforts to implement such changes would eliminate risk in several areas and greatly reduce the attack surface of the organization.

The vulnerabilities identified in this document introduce critical risk to **Artemis Gas Inc**. Implementing the changes recommended in this document would resolve many of the technical findings, significantly reduce risk to **Artemis Gas Inc**, and greatly increase the organizational security posture.

Definition of Severities

Springboard has categorized the findings into four categories of severity. These ratings were determined based upon variables such as impact, likelihood, and ease of a successful attack.

- CRITICAL – These issues can pose a very significant security threat. The issues that have a critical impact are typically those that would allow an attacker to gain full administrative access to service, device, or network resources. Often, these vulnerabilities can be exploited with little or no user interaction. There were four (4) critical findings identified during the application/server assessment.

- HIGH – These issues pose a significant threat to security but have some limitations on the extent to which they can be leveraged. User-level access to a device and a denial of service (DoS) vulnerability in a critical service would fall into this category. These findings typically will result in unauthorized access to restricted assets and may require user interaction to exploit. There were four (4) high-rated findings identified during the network assessment.

- MEDIUM – These issues have significant limitations on the direct impact they can cause. Typically, medium-rated findings would include significant information leakage issues, DoS on non-critical services, or those that provide significantly limited access to resources or data. Medium findings may not result in compromise but provide information that may be used in further attacks which might. There were eighty-seven (1) medium-rated findings identified during the network assessment.

Vulnerability	Severity	CVSS Score	Description	Risk
Microsoft Exchange Server vulnerable to CVE-2021-26855	Critical	9.8	This is a server-side request forgery (SSRF) vulnerability in Exchange which allows the attacker to send arbitrary HTTP requests and authenticate as the Exchange Server.	By exploiting this vulnerability chain, threat actors could achieve remote code execution and potentially compromise the entire Exchange Server environment.

Oracle WebLogic Server vulnerable to CVE-2020-14882	Critical	9.8	Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server.	It allows unauthenticated attackers to take full control of vulnerable systems, posing risks such as data theft, malware installation, and operational disruption.
Default password on Cisco admin portal	Critical	9.8	An intact passcode provides opportunistic hackers with an attack vector to gain unwarranted access to your device and data.	An attacker could use this knowledge to authenticate with administrative privileges and arbitrarily change the configuration of Cisco Network Registrar
Web server is exposing sensitive data	Critical	9.4	Sensitive data exposure occurs as a result of not adequately protecting a database where information is stored.	This might be a result of a multitude of things such as weak encryption, no encryption, software flaws, or when someone mistakenly uploads data to an incorrect database.
Web Application is vulnerable to SQL injection	High	8.6	When a cybercriminal inserts a malicious SQL injection, a line of code is added that can interfere with the queries the application itself makes sends to its database.	Depending on the data stored on the SQL server, an attack can expose private user data, such as credit numbers.
Apache web server vulnerable to CVE-2019-0211	High	7.8	Lets an attacker execute unprivileged scripts, usually run by Apache with lowered privileges to take over the main Apache process. This can also lead to an attacker gaining root access to the server by simply running a script.	CVE-2019-0211 vulnerability poses severe risks when the web server is used for running shared hosting instances, in this scenario, users with limited permissions could exploit the flaw to get root privileges, allow them to gain complete control of the machine, using scripts and run commands on vulnerable Apache web servers.

Unpatched RDP is exposed to the internet	High	7.5	Cyber actors can infiltrate the connection between the machines and inject malware or ransomware into the remote system.	The possible threats from someone accessing a computer on your network via RDP include data and financial theft. Malware and ransomware can be installed and activated to send infected e-mails to your contacts, vendors or customers.
Web application has broken access control	High	7.1	Broken access control vulnerability is a type of security flaw that allows an unauthorized user access to restricted resources.	If an attacker is able to gain access to sensitive data, they may be able to use this information for malicious purposes, such as identity theft or fraud. Additionally, data breaches can damage an organization's reputation and lead to financial losses.
Misconfigured cloud storage	Medium	5.3	Cloud misconfiguration refers to any glitches, gaps, or errors that could expose your environment to risk during cloud adoption.	These cyber threats come in the form of security breaches, external hackers, ransomware, malware, or insider threats that use vulnerabilities to access your network. Cloud misconfigurations result in companies exposing unencrypted or sensitive data to the public internet.

I. Recommendations

This section will include recommendations for remediations for the 9 vulnerabilities found in the vulnerability assessment.

1. **Microsoft Exchange Server vulnerable to CVE-2021-26855 -** CRITICAL
    a. Patching: Applying the available security updates and patches provided by Microsoft is critical to remediate ProxyLogon and protect Exchange Server environments from potential exploitation. This should be done immediately to prevent unauthorized access.

   b. Incident Response: Organizations must initiate an incident response plan to identify any signs of compromise, investigate the extent of the breach, and contain the impact. This includes conducting thorough system audits, monitoring network traffic, and analyzing log data to detect any unauthorized activities.
   c. Enhanced Monitoring: Implementing robust network monitoring and intrusion detection systems can help identify and respond to any suspicious activities related to ProxyLogon or potential follow-up attacks.
   d. User Awareness and Training: Educating users about the risks of phishing attacks, suspicious emails, and social engineering techniques helps mitigate the likelihood of falling victim to such attacks. Users should be vigilant and report any unusual or suspicious emails or activities to the appropriate security teams.

2. **Oracle WebLogic Server vulnerable to CVE-2020-14882 - CRITICAL**
   a. Oracle strongly recommends that customers apply the updates provided by this Security Alert as soon as possible after applying the October 2020 Critical Patch Update.
3. **Default password on Cisco admin portal - CRITICAL**
   a. Default passwords are nothing more than, hence should be treated as, placeholders. They should only be used for the first setup or just after a factory reset of your device. Users are typically prompted to change the default password after entering it for the first time. Some companies enforce a change of default password upon first use, such that the setup process cannot proceed otherwise. However, the safest and easiest way to get around this issue is to change it using a good password manager.
4. **Web server is exposing sensitive data - CRITICAL**
   a. Use SSL
   b. Use HTTPS security
   c. Use strong cryptographic algorithms or keys
   d. Using salt with passwords
   e. Encryption All Sensitive Data
   f. Classifying Data
   g. Use Security Testing Tools
   h. Don't hold on to Sensitive Data
5. **Web Application is vulnerable to SQL injection - HIGH**
   a. Using SQL injection, attackers can retrieve and alter data, which risks explaining sensitive company data.
   b. Depending on the data stored on the SQL server, an attack can expose private user data, such as credit numbers.
   c. Bypassing Authentication
   d. Install malicious code
   e. Identifying Injectable Parameters
   f. Executing Remote Commands
   g. Denial of Service
   h. Database Fingerprinting
   i. Spoof identity
   j. Cause repudiation issues (such as voiding transactions or changing balances)

    k. Destroy the data or make it otherwise unavailable
    l. Execute administration operations on the DB.

6. **Apache web server vulnerable to CVE-2019-0211 - HIGH**
    a. System administrators can patch the flaw by updating their servers to Apache httpd version 2.4.39. Developers, programmers, and system admins that use Apache should also employ the principle of least privilege to prevent threats that may exploit related vulnerabilities.
7. **Unpatched RDP is exposed to the internet - HIGH**
    a. Use group policies to specify application allow lists and block lists
    b. Use the regedit tool to prevent the built-in Windows Help feature from being opened
    c. If not using RDP, close TCP port 3389 on the computers and routers
    d. Make sure all security patches have been located on your computers
    e. Make sure all security patches have been loaded
    f. Use 2MFA authentication
    g. Enable event logging and review logs on a regular, at least weekly, basis
    h. Never have RDP active on a critical network device, such as a server
    i. Use VPN connections whenever possible to encrypt RDP traffic
    j. Make sure any public cloud-based systems are not using RDP
    k. Implement Network Level Authentication
    l. Implement an RDP Gateway
    m. Enable RBAC restrictions
    n. Enable Automatic Updates
8. **Web application has broken access control - HIGH**
    a. Enforce Record Ownership
    b. Enable RBAC
    c. Constant Testing and Auditing of Access Controls
    d. Deny by Default
9. **Misconfigured cloud storage - MEDIUM**
    a. Implement logging practices
    b. Enable encryption
    c. The rule of Least Privilege
    d. Perform consistent misconfiguration audits
    e. Create, apply, and communicate strong security policies

J. REFERENCES

https://sansorg.egnyte.com/dl/rsRNIHnrNU
https://sansorg.egnyte.com/dl/yNfjHOQix8
https://redteamsecurity.com/blog/the-purpose-of-penetration-testing
https://www.alpinesecurity.com/blog/cybersecurity-risk-assessment-guide/
https://www.redlegg.com/hubfs/RedLegg_ExternalInternalPenetrationAssessment-SampleReport.pdf?utm_campaign=Pen%20Testing%20Sample%20Reports&utm_

medium=email&_hsmi=78168829&_hsenc=p2ANqtz-8fQCLr8QokcDH-wv7QQUNvZ1dkX8NmU087MMvTg2qHCKGKuy47Q9F1QDrzVv_rNeK35tijupujmKkQDOdELOYCxFYktQ&utm_content=78168829&utm_source=hs_automation

K. EXECUTIVE SUMMARY

CONFIDENTIAL

Artemis Inc.
Vulnerability Assessment

EXECUTIVE SUMMARY

Artemis Gas Inc., engaged SPRINGBOARD to conduct a vulnerability assessment ("Assessment") to determine the risk appetite regarding internal or external threats. The assessment was conducted in January of 2023. SPRINGBOARD performed an external network-layer vulnerability assessment from a SPRINGBOARD host on the internet and an internal network-layer vulnerability assessment from an SPRINGBOARD laptop connected inside Artemis Gas Inc.'s internal corporate network. This report provides a summary of the overall findings and the CVSS score of all found vulnerabilities, as well as the detailed findings and recommendations for critical, high-risk, and medium-risk vulnerabilities.

The assessment results indicate that Artemis Gas Inc. may have process gaps in its patch and vulnerability management processes, which could leave the organization vulnerable to attacks from both internal and external sources. SPRINGBOARD identified 4 critical- and 4 high-risk vulnerabilities on the internal network and 1 Medium-risk vulnerabilities on the external networks. **SPRINGBOARD recommends remediation of the critical, high-risk, and medium-risk vulnerabilities within the next 30 days to reduce the risk of exposing the network to attacks.**

Key Summary Findings and Recommendations:

1. 5 servers/RDP protocol vulnerabilities have been identified on the internal network, along with several unpatched systems. Leaving these hosts and services in place opens the larger Artemis Gas Inc. network up to potential vulnerabilities ranging from information disclosure to full system compromise.

SPRINGBOARD RECOMMENDATIONS Patch these vulnerabilities in accordance with their risk level and reevaluate current patch management tools and practices. Artemis Gas Inc. should implement a comprehensive patch management tool and program if one does not already exist. Management should provide oversight to confirm the vulnerability and patch management programs continue to be maintained.

2. Insecure configurations were identified within the cloud infrastructure resulting in weak SSL encryption and increased risk of sensitive information disclosure. This finding indicates a gap in configuration hardening and management processes.

SPRINGBOARD RECOMMENDATIONS Artemis Gas Inc. should develop or revise system configuration hardening standards for all applicable technologies. Conclusion The Assessment has shown that while Artemis Gas Inc. has the ability to patch and remediate vulnerabilities affecting its environment, these processes may not be comprehensive or sufficiently effective to mitigate risk. These unmitigated vulnerabilities, if exploited by an attacker, can be used to potentially compromise the full Artemis Gas Inc. network. Artemis Gas Inc. should investigate opportunities to further improve its vulnerability and patch management to ensure that all critical- and high-risk vulnerabilities are remediated within 30 days or less.

3. Insecure configurations were identified within the Cisco router infrastructure resulting in weak configurations and increased risk of sensitive information disclosure. This finding indicates a gap in configuration hardening and management processes. The default password is a vulnerability.

SPRINGBOARD RECOMMENDATIONS: An attacker could use this knowledge to authenticate with administrative privileges and arbitrarily change the configuration of Cisco Network Registrar. Artemis Gas should change the default password or use a good password manager.

4. The vulnerability assessment identified 2 applications that have vulnerabilities. One web application is susceptible to SQL injection and the other application has a broken access control. For the broken access control, if an attacker is able to gain access to sensitive data, they may be able to use this information for malicious purposes, such as identity theft or fraud. Additionally, data breaches can damage an organization’s reputation and lead to financial losses. Organizations subject to regulatory requirements, such as HIPAA or PCI DSS, must ensure access controls comply with these regulations. For the SQL injection vulnerability, a successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system

SPRINGBOARD RECOMMENDATIONS: For the application that is vulnerable to a SQL injection, Artemis should employ employee training and the developers should use Input validation and the use of whitelists. For the broken access control, the system administrator(s) should enable Role-Based Access Controls.

The full list of vulnerabilities identified in the assessment, with the associated comprehensive details and recommendations, can be found in the Technical Report.

REFERENCES

https://www.springboard.com/archeio/download/ccdcf0619d71421ba66a4bac8e5efc18/