***Detailed Technical Report***

07/09/2023

ARTEMIS PENTEST 2023

Artemis Gas, Inc.

***Table of Contents***

***Abstract:***

This Detailed Technical Report presents the findings and analysis from the comprehensive penetration testing engagement conducted for Artemis Gas, Inc. The report outlines the scope and approach of the assessment, including the reconnaissance activities, vulnerability identification, and threat analysis. The objective was to assess the security posture of Artemis Gas, Inc. and provide actionable recommendations to mitigate potential risks and vulnerabilities. The report highlights the identified vulnerabilities, their potential impact, and offers strategic guidance to enhance the organization's overall security defenses. By implementing the recommended measures, Artemis Gas, Inc. can strengthen their security infrastructure and safeguard critical assets against potential threats.

***Introduction:***

This Detailed Technical Report provides an in-depth analysis of the penetration testing engagement conducted for Artemis Gas, Inc. The objective of this report is to present the comprehensive findings, vulnerabilities, and threats identified during the assessment, offering valuable insights to the client's IT staff. By examining the security posture of Artemis Gas, Inc., this report aims to assist in strengthening the organization's overall security defenses.

The penetration testing engagement focused on assessing the external network infrastructure and selected web applications of Artemis Gas, Inc. Through a systematic and controlled approach, various reconnaissance techniques were employed to gather critical information about the organization's systems and potential attack surfaces. The

obtained insights were then leveraged to identify vulnerabilities and potential entry points that could be exploited by malicious actors.

The scope of work encompassed multiple phases, including reconnaissance and information gathering, target identification and scans against the external network, vulnerability identification and assessment, threat analysis, and the development of comprehensive recommendations for remediation and risk mitigation. Throughout the engagement, diligent efforts were made to align the assessment with the specific context and environment of Artemis Gas, Inc.

By conducting this penetration test, our goal was to identify potential vulnerabilities and assess the effectiveness of existing security controls within Artemis Gas, Inc. Furthermore, we aimed to evaluate the associated risks and their potential impact on the organization. This report presents the detailed findings and offers strategic recommendations to address the identified vulnerabilities, enhancing the overall security posture of Artemis Gas, Inc.

It is crucial to emphasize that the findings and recommendations presented in this report are based solely on the context of the penetration testing engagement. The objective is to provide Artemis Gas, Inc.'s IT staff with actionable insights that can be utilized to bolster their security infrastructure and safeguard their critical assets.

We strongly encourage the client's IT staff to carefully review the detailed findings, take into consideration the organization's unique requirements and constraints, and implement the recommended measures to mitigate potential risks. By doing so, Artemis Gas, Inc. can proactively strengthen their security defenses, protect sensitive data, and minimize the likelihood of successful cyber-attacks.

In conclusion, this Detailed Technical Report serves as a comprehensive documentation of the penetration testing engagement conducted for Artemis Gas, Inc. It provides a detailed analysis of vulnerabilities, threat vectors, and strategic recommendations to empower the client's IT staff to take appropriate actions to enhance their security posture.

***Scope of Work:***

The scope of the penetration testing engagement conducted for Artemis Gas, Inc. encompasses a comprehensive assessment of the organization's external network infrastructure and selected web applications. The primary objective is to identify potential vulnerabilities and assess the effectiveness of existing security controls within the defined scope. The penetration testing activities will be conducted in a controlled and structured manner, adhering to industry best practices and ethical guidelines.

The assessment will begin with an extensive reconnaissance phase, involving the gathering of publicly available information about Artemis Gas, Inc., its systems, and its digital footprint. This information will provide a foundation for subsequent target identification and scans against the external network. The focus will be on identifying potential entry points, open ports, and services that could be susceptible to exploitation.

In the vulnerability identification and assessment phase, various automated scanning tools and manual techniques will be utilized to identify known vulnerabilities in the identified targets. The assessment will cover a wide range of systems, including network devices, web applications, and databases. The goal is to identify vulnerabilities such as misconfigurations, outdated software, weak authentication mechanisms, and potential avenues for privilege escalation.

The findings will be thoroughly analyzed and categorized based on severity, impact, and exploitability. The threat analysis phase will assess the risks associated with the identified vulnerabilities, taking into consideration the likelihood of exploitation and the potential consequences to Artemis Gas, Inc. This analysis will help prioritize the remediation efforts and guide the development of strategic recommendations.

Throughout the engagement, strict adherence to ethical guidelines and professional standards will be maintained. The assessment will be conducted from an external perspective, simulating the actions of a potential attacker without causing any disruption or damage to the production environment. The objective is to provide an accurate assessment of the organization's security posture while minimizing any potential risks to the systems and data.

It is important to note that the penetration testing engagement will not include any exploitation of vulnerabilities beyond proof of concept demonstrations, ensuring that the assessment remains within the predefined scope. The focus is on identifying and documenting vulnerabilities, conducting risk analysis, and providing recommendations for remediation.

Upon completion of the assessment, a detailed technical report will be provided to Artemis Gas, Inc.'s IT staff. The report will include a comprehensive summary of findings, an analysis of the identified vulnerabilities, and actionable recommendations to enhance the organization's security defenses. The scope of work is designed to provide Artemis Gas, Inc. with valuable insights into their security posture, empowering them to make informed decisions regarding risk mitigation and strengthening their overall security resilience.

In summary, the scope of work for the penetration testing engagement covers a thorough assessment of Artemis Gas, Inc.'s external network infrastructure and selected web applications. The focus is on identifying vulnerabilities, analyzing threats, and providing strategic recommendations to enhance the organization's security posture. The assessment will be conducted in a controlled and ethical manner, ensuring minimal disruption while delivering comprehensive insights to the client.

***Project Objectives:***

The primary objectives of the penetration testing engagement for Artemis Gas, Inc. were designed to provide a comprehensive assessment of the organization's security posture. The following project objectives were pursued to fulfill this purpose:

**Identify Vulnerabilities:** The foremost objective of the penetration test was to identify vulnerabilities within Artemis Gas, Inc.'s external network infrastructure and web applications. By leveraging a combination of automated scanning tools and manual techniques, the assessment aimed to uncover potential weaknesses, misconfigurations, and software vulnerabilities that could be exploited by malicious actors. This objective sought to provide a clear understanding of the security gaps within the organization's systems.

**Assess Security Controls:** Another crucial objective was to assess the effectiveness of the existing security controls and measures implemented by Artemis Gas, Inc. This involved examining firewall configurations, access controls, authentication mechanisms, and other security mechanisms deployed to protect the external network infrastructure and web applications. By evaluating the strength and

adequacy of these controls, the assessment aimed to identify any gaps or weaknesses that could undermine the organization's overall security posture.

**Evaluate Risk and Impact:** An essential aspect of the penetration testing engagement was to evaluate the risk associated with identified vulnerabilities and the potential impact they could have on Artemis Gas, Inc. This objective aimed to assess the likelihood of exploitation and the potential consequences in terms of data breaches, unauthorized access, service disruption, and reputational damage. By considering the context of the organization's operations and the sensitivity of its assets, the evaluation of risk and impact provided valuable insights to prioritize remediation efforts.

**Provide Recommendations for Remediation:** To assist Artemis Gas, Inc. in strengthening its security defenses, the penetration test aimed to provide comprehensive recommendations for remediation and risk mitigation. Based on the identified vulnerabilities and their associated risks, the objective was to offer actionable guidance to address the gaps in security controls. The recommendations encompassed measures such as software patching, configuration changes, access control enhancements, and employee awareness training. These recommendations were intended to enable the organization to improve its security posture and reduce the likelihood of successful cyber-attacks.

By pursuing these project objectives, the penetration testing engagement aimed to provide Artemis Gas, Inc. with a thorough understanding of its security strengths and weaknesses. The comprehensive assessment of vulnerabilities, evaluation of security controls, risk analysis, and targeted recommendations were all geared towards empowering the organization to make informed decisions in enhancing its security

defenses. By addressing the identified vulnerabilities and implementing the recommended measures, Artemis Gas, Inc. could significantly improve its resilience against potential cyber threats and mitigate the associated risks.

***Assumptions:***

**Access Permissions:** It was assumed that Artemis Gas, Inc. has granted the necessary access permissions to the consulting firm conducting the assessment. These permissions were assumed to be sufficient to perform the required scanning, vulnerability identification, and testing activities. It was assumed that the provided access would enable the testing team to gather the required information and conduct assessments without any limitations that could hinder the identification of vulnerabilities.

**Cooperation and Support:** It was assumed that the IT staff of Artemis Gas, Inc. would provide the necessary cooperation and support throughout the engagement. This includes timely provision of information, assistance in resolving any technical issues that may arise during the assessment, and coordination with relevant stakeholders within the organization. It was assumed that the IT staff would actively engage with the consulting team, promptly address any queries, and facilitate the smooth execution of the penetration testing activities.

**Test Environment Alignment:** It was assumed that the test environment provided by Artemis Gas, Inc. accurately reflects the production environment in terms of systems, configurations, and applications. This assumption was crucial to ensure that the assessment accurately represents the organization's security posture and vulnerabilities. It was assumed that the test environment would closely mirror the

production environment to provide meaningful insights into the actual risks faced by the organization.

These assumptions formed the basis for planning and executing the penetration testing engagement. It was essential to have the necessary access permissions, cooperation, and a test environment that accurately reflects the production environment to ensure the validity and relevance of the findings. By relying on these assumptions, the penetration testing assessment aimed to provide a realistic evaluation of Artemis Gas, Inc.'s security posture and deliver actionable recommendations for enhancing its defenses.

***Timeline:***

The penetration testing engagement for Artemis Gas, Inc. was conducted over a period of 7 weeks, encompassing several key milestones and activities to ensure a comprehensive assessment of the organization's security posture. The timeline was divided into five distinct phases, each serving a specific purpose in the overall testing process.

**Phase 1: Reconnaissance and Information Gathering**

During the initial phase, the cybersecurity team conducted simulated reconnaissance activities to gather vital information about Artemis Gas, Inc. and its network infrastructure. This involved leveraging various open-source intelligence (OSINT) techniques to collect publicly available data, analyzing the organization's online presence, and identifying potential vulnerabilities and entry points for further exploration.

**Phase 2: Target Identification and Scans against External Network**

In this phase, the team focused on identifying the target systems within Artemis Gas, Inc.'s external network. Through a combination of network scanning and enumeration techniques, the team aimed to map out the network architecture, identify active hosts and services, and gather valuable information about the target infrastructure. This phase involved the use of industry-standard tools such as Nmap, OpenVAS, and Nessus to conduct comprehensive scans and identify potential vulnerabilities.

**Phase 3: Vulnerability Identification and Assessment**

During this phase, the team performed in-depth vulnerability assessments on the identified systems and applications. By utilizing automated vulnerability scanning tools and conducting manual analysis, the team aimed to identify and validate potential security flaws, misconfigurations, and weaknesses within the target environment. The assessments covered a range of areas, including network devices, web applications, databases, and operating systems, to provide a holistic view of the vulnerabilities present within the organization's infrastructure.

**Phase 4: Threat Analysis and Risk Evaluation**

In this critical phase, the team analyzed the identified vulnerabilities and assessed the potential threats and risks they posed to Artemis Gas, Inc. By considering the likelihood and impact of exploitation, the team evaluated the potential consequences, such as unauthorized access, data breaches, and service disruptions. The analysis took into account the current threat landscape, industry best practices, and the specific context of Artemis Gas, Inc.'s operations to provide an accurate assessment of the risks associated with the identified vulnerabilities.

### Phase 5: Reporting and Recommendations

The final phase focused on documenting the findings and delivering actionable recommendations to Artemis Gas, Inc. The team compiled a comprehensive report that detailed the vulnerabilities discovered, their potential impact, and the recommended steps for remediation and risk mitigation. The report included an executive summary, a technical overview, prioritized recommendations, and suggested controls to improve the organization's security posture. The aim was to provide the client's IT staff with clear and actionable guidance to address the identified vulnerabilities and enhance their overall security posture.

Throughout the 7-week engagement, the cybersecurity team followed a systematic and thorough approach to ensure the accuracy and reliability of the findings. The timeline was designed to allocate sufficient time for each phase, including planning, execution, analysis, and reporting, while considering the unique characteristics of Artemis Gas, Inc.'s network infrastructure and the complexity of its operations.

## *Summary of Findings*

### Reconnaissance Activities

During the reconnaissance phase of the penetration testing engagement, a variety of activities were conducted to gather information about Artemis Gas, Inc. and its network infrastructure. Open-source intelligence (OSINT) techniques were employed to collect publicly available data, analyze the organization's online presence, and identify potential entry points for further exploration. Methods such as social media analysis, search engine queries, and company research were utilized to gather information on the organization's employees, technologies, and business operations. This phase provided

valuable insights into the organization's online footprint, potential attack vectors, and areas of vulnerability.

**Vulnerabilities Identified**

The assessment uncovered several vulnerabilities within Artemis Gas, Inc.'s network infrastructure and web applications. These vulnerabilities pose varying degrees of risk and potential impact to the organization's security posture. Notable vulnerabilities include unpatched Remote Desktop Protocol (RDP) exposed to the internet, a web application susceptible to SQL injection, default passwords on Cisco admin portals, a vulnerable Apache web server (CVE-2019-0211), and sensitive data exposure on a web server. Each vulnerability was assessed based on its severity, affected systems, and potential impact. It is important to address these vulnerabilities promptly to prevent unauthorized access, data breaches, and potential disruption of critical systems.

**Threat Analysis**

Based on the identified vulnerabilities and the current threat landscape, an analysis was conducted to assess the threats that Artemis Gas, Inc. faces. This analysis considered the likelihood and potential consequences of exploitation. The vulnerabilities identified could expose the organization to various threats, including unauthorized access, data manipulation, information disclosure, and service disruptions. Threat actors could leverage these vulnerabilities to launch attacks on internal systems, gain privileged access, move laterally within the network, and compromise sensitive information. The organization's reliance on outdated network hardware, misconfigurations, and non-compliance with security policies further exacerbate the

threat landscape. It is imperative that appropriate measures are taken to mitigate these threats and enhance the organization's overall security posture.

By identifying these vulnerabilities and assessing the associated threats, Artemis Gas, Inc. can gain a deeper understanding of its security risks and take proactive steps to address them. The organization should prioritize the remediation of critical vulnerabilities, implement robust security controls, and enforce strong access management practices. Regular vulnerability assessments, patch management, and security awareness training should be integrated into the organization's security program to reduce the risk of exploitation and enhance the protection of critical assets. By addressing these findings and adopting a proactive security approach, Artemis Gas, Inc. can significantly improve its overall security posture and safeguard its valuable assets and sensitive data.

***Recommendations***

Based on the findings and threat analysis conducted during the penetration testing engagement, the following recommendations are provided to enhance the security posture of Artemis Gas, Inc. These recommendations are categorized by priority and impact, aiming to address the identified vulnerabilities and mitigate the associated threats effectively. Each recommendation includes a clear description and justification, providing a roadmap for improving the organization's security resilience.

**Patch and Update Vulnerable Systems:**

To begin with, it is crucial to prioritize regular patching and updating of all systems and applications. Unpatched systems are easy targets for attackers, leaving them susceptible to exploitation and unauthorized access. By ensuring that all software

and firmware are up to date, Artemis Gas can significantly reduce the risk of known vulnerabilities being exploited.

**Strengthen Network Perimeter Security:**

Furthermore, enhancing network perimeter security is of utmost importance. This can be achieved by implementing robust firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS). These measures provide a strong defense against external threats and unauthorized access attempts, safeguarding the organization's critical assets.

**Implement Secure Configuration Practices:**

Another critical recommendation is to establish secure configuration standards for all systems and devices. Misconfigured systems can introduce vulnerabilities and weaken the overall security posture. By adhering to industry best practices and ensuring secure configurations, Artemis Gas can reduce the attack surface and minimize the risk of exploitation.

**Conduct Regular Vulnerability Assessments:**

In addition to proactive measures, conducting regular vulnerability assessments is vital for maintaining an up-to-date understanding of the organization's security posture. By identifying vulnerabilities and promptly remediating them, Artemis Gas can stay ahead of potential threats and mitigate risks effectively.

**Implement Web Application Security Measures:**

Web application security should also be a priority. Employing secure coding practices, regularly updating web applications, and conducting thorough penetration testing can help identify and remediate vulnerabilities. Common web application

vulnerabilities, such as SQL injection and sensitive data exposure, can be mitigated through these measures.

**Strengthen Authentication and Access Control:**

Strengthening authentication and access control mechanisms is essential for protecting sensitive data and preventing unauthorized access. Enforcing strong password policies, implementing multi-factor authentication (MFA), and regularly reviewing user access privileges will significantly reduce the likelihood of compromised credentials leading to security breaches.

**Enhance Security Awareness and Training:**

A comprehensive security awareness and training program should be implemented to educate employees about cybersecurity best practices and potential threats. Human error and lack of awareness can lead to security breaches. By fostering a culture of security consciousness, Artemis Gas can empower its employees to identify and respond to potential threats effectively.

**Develop an Incident Response Plan:**

Additionally, developing a well-defined incident response plan is crucial for handling security incidents efficiently. This plan should include procedures for detecting, responding to, and recovering from incidents. By having a clear roadmap and predefined actions, Artemis Gas can minimize the impact of security incidents and ensure a swift and coordinated response.

These recommendations should be prioritized based on their impact and the organization's specific context. Regular monitoring, continuous updates, and periodic reassessments of the security posture will enable Artemis Gas to stay resilient to

evolving threats and maintain a proactive security stance. By implementing these recommendations, Artemis Gas, Inc. can enhance its overall security posture, reduce the risk of exploitation, and protect its valuable assets and sensitive data. These measures will contribute to building a robust cybersecurity framework that aligns with the organization's business objectives and mitigates potential risks effectively.

***Conclusion***

In conclusion, the detailed technical report highlights significant vulnerabilities and risks discovered during the penetration testing engagement conducted for Artemis Gas, Inc. The assessment encompassed a thorough analysis of the organization's network infrastructure and web applications, shedding light on critical areas that require immediate attention to enhance the overall security posture.

The reconnaissance activities carried out as part of the engagement provided valuable insights into the client's network architecture and potential attack vectors. Notably, our findings revealed the presence of unpatched Remote Desktop Protocol (RDP) exposed to the internet, a vulnerable web application susceptible to SQL injection, default passwords on the Cisco admin portal, and an Apache web server vulnerable to CVE-2019-0211. These vulnerabilities, if left unaddressed, pose significant risks to the confidentiality, integrity, and availability of Artemis Gas, Inc.'s systems and sensitive data.

Considering the current threat landscape and the identified vulnerabilities, it is crucial for Artemis Gas, Inc. to take immediate action to remediate these risks. Exploitation of the identified vulnerabilities could lead to unauthorized access, data breaches, service disruptions, and potential financial and reputational damage. To

mitigate these risks effectively, the organization should prioritize the following recommendations:

Firstly, prompt application of patches and updates is crucial to address the vulnerabilities identified, particularly in relation to the unpatched RDP, web application security, and the Cisco admin portal. By staying up to date with security patches, the organization can significantly reduce the likelihood of exploitation and protect against potential threats.

Furthermore, the implementation of strong password policies and regular password changes across all systems and applications is essential. This will mitigate the risks associated with default passwords and improve the overall security posture of Artemis Gas, Inc.

Conducting thorough security testing, such as code reviews and penetration testing, is also recommended. This will help identify and address any additional vulnerabilities within the web applications and further strengthen the organization's defense against potential cyber threats.

To bolster the overall network security, it is imperative to enhance network segmentation and access controls. Implementing stringent access restrictions will help prevent unauthorized access and limit the potential impact of a successful breach.

Enhancing monitoring and log management capabilities is crucial for detecting and responding to security incidents in a timely manner. By investing in robust monitoring systems and establishing effective incident response protocols, Artemis Gas, Inc. can detect and mitigate threats promptly, minimizing potential damage.

Lastly, comprehensive security awareness training for all employees is vital. Educating staff about security best practices, including safe data handling, phishing awareness, and adherence to security policies, will create a strong security culture within the organization and significantly reduce the risk of successful attacks.

In conclusion, by implementing these recommendations, Artemis Gas, Inc. can significantly strengthen its security defenses, reduce the risk of exploitation, and safeguard its critical assets and sensitive information. The organization must prioritize the allocation of resources to address the identified vulnerabilities and actively promote a proactive security culture. Through regular vulnerability assessments, continuous monitoring, and proactive security measures, Artemis Gas, Inc. will be better equipped to defend against current and emerging threats, ensuring the confidentiality, integrity, and availability of their systems and data.

This detailed technical report serves as a roadmap for Artemis Gas, Inc. to enhance their cybersecurity posture and mitigate the identified risks. By following the recommendations and investing in robust security practices, the organization can fortify its defenses, protect critical operations, and maintain the trust of customers and stakeholders.