Phase 4: Threat Assessment

Executive Summary:

The vulnerability assessment conducted on Artemis Gas, Inc.'s network revealed several critical and high-risk vulnerabilities. Firstly, unpatched RDP exposed to the internet poses a high risk, potentially leading to unauthorized access and data breaches. Secondly, a web application vulnerable to SQL Injection presents a high risk of unauthorized data access and manipulation. Additionally, a default password on the Cisco admin portal raises concerns of unauthorized network access and configuration tampering. Another high risk vulnerability involves an Apache web server susceptible to remote code execution. Lastly, a web server misconfigured to expose sensitive data poses a medium risk of data breaches and compromised confidentiality. Immediate remediation actions are necessary to address these vulnerabilities and mitigate potential threats to Artemis' network security.

Threat Assessment:

1. ***Vulnerability: Unpatched RDP exposed to the internet***
    - Description: The presence of unpatched Remote Desktop Protocol (RDP) services exposed to the internet poses a significant security risk. Unpatched RDP services may contain known vulnerabilities that can be exploited by threat actors to gain unauthorized access to systems. This could result in potential data breaches, unauthorized lateral movement within the network, and potential disruption of critical services.

- Operating Systems/Versions Affected: Windows operating systems running unpatched RDP services.
- Risks of Exploitation: Unauthorized access to systems, potential data theft, privilege escalation, unauthorized control over critical systems.
- Potential Attack Vectors: Launch attacks on internal systems, steal sensitive information, execute arbitrary commands, manipulate or delete data, disrupt services.
- Blocking Mechanisms: Network firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), regular patching and updates, strong password policies.
- Password Cracking: Tools such as John the Ripper, Hashcat, and CrackStation can be utilized to crack weak or default RDP passwords.
- Remediation: Patch RDP services with the latest security updates, enforce strong password policies, restrict access to RDP services via firewall rules, implement multi factor authentication (MFA).
- CVSS Score: 8.0 (High)

2. ***Vulnerability: Web application vulnerable to SQL Injection***
    - Description: A web application vulnerable to SQL Injection attacks allows unauthorized access and manipulation of the underlying database. This vulnerability arises from inadequate input validation and sanitization, enabling malicious actors to inject malicious SQL code into web application inputs. Exploitation of this vulnerability can lead to unauthorized disclosure of sensitive data, data corruption, privilege

escalation, and potentially complete compromise of the web application and underlying systems.

- Operating Systems/Versions Affected: Web applications with insecure database query handling.
- Risks of Exploitation: Unauthorized access to sensitive data, potential data loss or corruption, privilege escalation, potential compromise of the web application and associated systems.
- Potential Attack Vectors: Extract sensitive data, modify or delete data, execute arbitrary commands, bypass authentication mechanisms, gain unauthorized administrative access.
- Blocking Mechanisms: Implement secure coding practices, employ parameterized queries and prepared statements, perform input validation and sanitization, employ web application firewalls (WAF) to detect and block SQL Injection attempts.
- Password Cracking: Not applicable to this specific vulnerability.
- Remediation: Implement secure coding practices, employ input validation and parameterized queries, sanitize user input, regularly update and patch web application frameworks, and perform regular security assessments.
- CVSS Score: 7.5 (High)

3. ***Vulnerability: Default password on Cisco admin portal***

- Description: The use of default or weak passwords on the Cisco admin portal exposes network devices to unauthorized access and control. These devices play a critical role in network infrastructure, and

unauthorized access to them can lead to network disruptions, configuration manipulation, interception of sensitive data, and potential compromise of the entire network.

- Operating Systems/Versions Affected: Cisco network devices with default or weak admin passwords.
- Risks of Exploitation: Unauthorized access to network infrastructure, potential data interception, configuration tampering, network disruption, unauthorized control over critical systems.
- Potential Attack Vectors: Alter network configurations, intercept sensitive data, launch further attacks against internal systems, gain unauthorized control over critical network devices.
- Blocking Mechanisms: Implement strong password policies, enforce password rotation, use complex passwords, employ multi-factor authentication (MFA), regularly audit and monitor administrative access to network devices.
- Password Cracking: Tools such as John the Ripper, Hashcat, and Crackstation can be utilized to crack weak or default passwords.
- Remediation: Change default passwords to strong, unique passwords, enforce password policies, implement multi-factor authentication (MFA) for administrative access to network devices, regularly update and patch firmware/software on network devices.
- CVSS Score: 9.0 (Critical)

4. ***Vulnerability: Apache web server vulnerable to CVE-2019-0211***

- Description: A vulnerability in the Apache web server, specifically versions prior to a specific patch, can allow for remote code execution. Exploitation of this vulnerability can lead to potential compromise of the web server, unauthorized access to sensitive data, and potential disruption of services.
- Operating Systems/Versions Affected: Apache web servers with the vulnerable version.
- Risks of Exploitation: Remote code execution, unauthorized access to sensitive data, potential disruption of services, potential compromise of the web server.
- Potential Attack Vectors: Exploit the vulnerability to execute arbitrary commands, upload malicious files, gain unauthorized access to the server, disrupt services.
- Blocking Mechanisms: Regular patching and updates for the Apache web server, employ web application firewalls (WAF), employ intrusion detection/prevention systems (IDS/IPS).
- Password Cracking: Not applicable to this specific vulnerability.
- Remediation: Apply the latest patches and updates for Apache web server, monitor for security advisories, employ web application firewalls (WAF) to detect and block malicious requests, regularly perform security assessments and penetration testing.
- CVSS Score: 8.5 (High)

5. ***Vulnerability: Web server exposing sensitive data***

- Description: A misconfigured web server that exposes sensitive data allows unauthorized access to files or directories containing confidential information. This vulnerability can result from improper access control configurations, permissions, or directory listings, potentially leading to unauthorized data access and breaches of confidentiality.
- Operating Systems/Versions Affected: Web servers with misconfigured access controls.
- Risks of Exploitation: Exposure of sensitive data, potential data breaches, compromise of confidential information, violation of data privacy regulations.
- Potential Attack Vectors: Access sensitive files or directories, extract sensitive data, identify additional attack vectors through exposed information.
- Blocking Mechanisms: Properly configure access controls and permissions, implement secure file permissions, disable directory listings, regularly audit and review web server configurations.
- Password Cracking: Not applicable to this specific vulnerability.
- Remediation: Review and adjust web server configurations to ensure proper access controls and permissions are in place, regularly audit and review access logs, monitor for unauthorized access attempts.
- CVSS Score: 6.5 (Medium)

6: Web application has broken access control

- Description: The web application lacks proper access control mechanisms, allowing unauthorized users to access sensitive functionalities or data.
- Operating systems/versions affected: Any operating system hosting the vulnerable web application.
- Risks of Exploitation: Unauthorized users can gain access to sensitive data, modify user privileges, perform unauthorized actions, and compromise the confidentiality and integrity of the application.
- Potential Attack vectors: Unauthorized access, privilege escalation, data theft, unauthorized modifications, and potential lateral movement.
- Blocking mechanisms: Access control mechanisms, user authentication, secure session management, and secure coding practices can mitigate the risk.
- Password Cracking: Popular password cracking tools like John the Ripper, Hashcat, or Hydra can be utilized to perform password cracking attempts against the compromised accounts.
- Remediation: Implement proper access controls, role-based access management, session management, and regular security code reviews.
- CVSS score: 7.5 (Medium)

7. Oracle WebLogic Server vulnerable to CVE-2020-14882

- Description: The Oracle WebLogic Server is vulnerable to CVE-2020-14882, which allows remote code execution by an unauthenticated attacker.

- Operating systems/versions affected: Oracle WebLogic Server versions susceptible to CVE-2020-14882.
- Risks of Exploitation: Unauthorized users can gain access to sensitive data, modify user privileges, perform unauthorized actions, and compromise the confidentiality and integrity of the application.
- Attack vectors: Unauthorized access, privilege escalation, data theft, unauthorized modifications, and potential lateral movement.
- Blocking mechanisms: Access control mechanisms, user authentication, secure session management, and secure coding practices can mitigate the risk.
- Password Cracking: Not applicable to this specific vulnerability, however, if unauthorized access to user accounts or administrative privileges is obtained through the exploitation of this vulnerability, password cracking techniques such as John the Ripper, Hashcat, or Hydra, can be utilized for password cracking attempts against the compromised accounts can be employed to crack weak or compromised passwords associated with those accounts.
- Remediation: Apply the latest patches and security updates provided by Oracle, configure secure server configurations, and regularly update and monitor the WebLogic Server.
- CVSS score: 9.8 (High)

8. Misconfigured cloud storage (AWS security group misconfiguration, lack of access restrictions)

- Description: The client's cloud storage, specifically AWS, is misconfigured, leading to security group misconfigurations and inadequate access restrictions.
- Operating systems/versions affected: AWS cloud storage and associated services.
- Risks of Exploitation: Attackers can gain unauthorized access to cloud resources, extract sensitive data, disrupt services, or even perform unauthorized actions on the compromised resources.
- Attack vectors: Inadequate access controls, misconfigured security groups, insecure cloud storage configurations.
- Blocking mechanisms: Properly configuring security groups, implementing access restrictions, adopting the principle of least privilege, and conducting regular security assessments.
- Password Cracking: Not applicable to this specific vulnerability.
- Remediation: Review and update cloud storage configurations, implement proper access controls, regularly review security group settings, and monitor cloud environments for unauthorized access.
- CVSS score: 6.8 (Medium)

9. Microsoft Exchange Server vulnerable to CVE-2021-26855

- Description: The Microsoft Exchange Server is vulnerable to CVE-2021-26855, which allows remote code execution through server-side request forgery (SSRF).

- Operating systems/versions affected: Microsoft Exchange Server versions susceptible to CVE-2021-26855.
- Risks of Exploitation: Attackers can execute arbitrary code remotely, potentially leading to complete compromise of the Exchange Server, unauthorized access to sensitive data, and manipulation of server resources.
- Attack vectors: Remote code execution, email account hijacking, unauthorized access to sensitive data, server manipulation, and potential lateral movement.
- Blocking mechanisms: Applying security patches and updates, implementing network-level controls, utilizing intrusion detection and prevention systems, and conducting regular vulnerability scans.
- If unauthorized access to user accounts or administrative privileges is gained through the exploitation of this vulnerability, password cracking tools, including John the Ripper, Hashcat, or Hydra, can be utilized for password cracking attempts against the compromised accounts.
- Remediation: Apply the latest security updates and patches provided by Microsoft, monitor for suspicious activity, and ensure email server configurations follow best practices.
- CVSS score: 9.1 (High)