Technical Penetration Testing Report

(Version 1.0)

Client: Artemis Gas Inc.

Prepared by Cyrus Lomibao

July 24.2024

Table of Contents

1.0 Scope of Work

This engagement aimed to perform an external network penetration test for Artemis Gas, Inc. The assessment focused on identifying vulnerabilities in the company's external-facing infrastructure, evaluating potential risks, and providing recommendations for remediation.

The scope of this penetration test includes:

1.1 External network assessment:

We are assessing the security of Artemis' external-facing systems and infrastructure from an attacker's perspective.

KEY COMPONENTS:

- **Passive Reconnaissance-** Gathering information about public, social media, **and** DNS records**.**
- **Active Reconnaissance-** Actively engaging with the system to gather more detailed information using network scanning tools.
- **Enumeration-** Identifying open ports, services, and applications running on the target systems including software versions, configurations**,** and potential entry points**.**
- **Vulnerability Identification-** Using automated tools and manual techniques to identify known vulnerabilities. Assess the security posture of web applications, network services, and any exposed systems.
- **Exploitation-** Using tools like Metasploit to assess and identify known exploits. Demonstrate the potential impact of successful exploitation.
- **Post-Exploitation-** Assessing the extent of access gained, and the potential for lateral movement, data exfiltration, and other activities.
- **Reporting-** Document findings, creating both technical and executive-level reports tailored to different audiences within the organization. Provide recommendations for remediation and improving security posture.
- **Remediation Verification-** verifying that all identified vulnerabilities have been effectively mitigated or resolved. Conduct follow-up assessments as needed.

1.2 Web application testing:

We are focusing on identifying security vulnerabilities and weaknesses in web applications.

KEY COMPONENTS:

1. **INFORMATION GATHERING AND MAPPING:**
   - **Application Mapping-** Understanding the structure of the web application including directories, pages, and functionalities.

- **Technology Identification-** Identifying the frameworks, technologies, and programming languages used by the application.

2. CONFIGURATION AND DEPLOYMENT MANAGEMENT TESTING:

- **Server Configurations-** Check for misconfigurations in web servers, databases, and other related components.
- **SSL/TLS Testing-** Ensuring that secure communication protocols are properly implemented.

3. IDENTITY MANAGEMENT TESTING:

- **User Registration Processes-** Analyzing the security of user registration, password recovery, and account management features.
- **Authentication Mechanisms-** Testing multi-factor authentication and the robustness of login mechanisms.

4. AUTHENTICATION TESTING:

- **Credential Brute Forcing-** Attempting to guess user credentials using automated tools like John the Ripper, Hashcat, Aircrack, etc.
- **Session Management-** Assessing how sessions are managed, including session IDs, cookies, and tokens for timed sessions.

5. AUTHORIZATION TESTING:

- **Access Control-** Ensuring users can only access resources and functionalities based on their authorizations.
- **Horizontal and Vertical Privilege Escalation-** Checking for vulnerabilities that allow users to escalate their privileges.

6. DATA VALIDATION TESTING:

- **Input Validation-** Testing for SQL Injection, cross-site scripting (XSS), and command injection from input vulnerabilities.
- **Output Encoding-** Ensuring all applications properly encode output to prevent attacks like XXS.

7. ERROR HANDLING:

- **Error Messages-** Analyzing error messages for information leakage that could be useful to attackers.
- **Exception Management-** Ensuring that the application handles exceptions securely without revealing sensitive information.

8. BUSINESS LOGIC TESTING:

- **Logic Flaws- I**dentifying application workflow vulnerabilities, such as bypassing intended business rules or exploiting logical inconsistencies.
- **Abusive Functionality-** Testing for unintended uses of legitimate functionalities.

9. CLIENT-SIDE TRAINING:

- **JavaScript Security-** Analyzing client-side scripts for vulnerabilities like DOM-based XSS and client-side validation bypasses.
- **Local Storage-** Ensuring that sensitive data is not stored insecurely on the client side.

10. API TESTING:

- **API Endpoints-** Testing the security of the API endpoints for issues like improper authentication, authorization, and input validation.
- **REST and SOAP Services-** Analyzing web services for vulnerabilities specific to RESTful and SOAP.

11. REPORTING:

- **Detailed Findings-** Documenting vulnerabilities with detailed descriptions, steps to reproduce, and potential impacts.
- **Remediation Recommendations-** Providing actionable recommendations to fix identified vulnerabilities.
- **Risk Assessment-** Prioritizing vulnerabilities based on their severity and organizational impact.

1.3 Cloud Storage Configuration Review:

A cloud storage configuration review involves examining the settings and practices used to manage and secure data stored in cloud environments. Here are the main steps and components involved in conducting a cloud storage configuration review:

1. ACCESS CONTROL:

- **User and Group Permissions:** Reviewing permissions assigned to users and groups to ensure the principle of least privilege is followed.
- **Role-Based Access Control (RBAC):** Ensuring roles are appropriately defined and assigned.
- **Access Keys and Secrets:** Check the management of access keys and secrets, including their rotation policies.

2. AUTHENTICATION AND AUTHORIZATION:

- **Multi-factor Authentication (MFA):** Ensuring MFA is enabled for all accounts, especially those with privileged access.
- **Identity and Access Management (IAM) Policies:** Reviewing IAM policies to ensure they are correctly configured and not overly permissive.

3. DATA ENCRYPTION:

- **Encryption at Rest:** Verifying that data stored in the cloud is encrypted using strong encryption algorithms.
- **Encryption in Transit:** Ensuring that data is encrypted while being transmitted to and from the cloud storage.
- **Key Management:** Assessing the use and management of encryption keys, including the use of Key Management Services (KMS).

4. DATA BACKUP AND RECOVERY:

- **Backup Policies:** Reviewing backup policies and ensuring that they are properly implemented.

- **Disaster Recovery**: Verifying the existence and effectiveness of disaster recovery plans.

5. LOGGING AND MONITORING:

- **Activity Logs:** Ensuring that all access and modification activities are logged.
- **Security and Event Management (SIEM)**: Using SIEM tools to monitor and analyze logs for suspicious activities.

- **6. NETWORK SECURITY:**

  - **Firewall and Security Groups:** Review the configuration of virtual firewalls and security groups to ensure that only necessary ports are open.
  - **Private vs. Public Access**: Ensuring that sensitive data is stored in private buckets or containers and that public access is only granted when necessary.

- **7. DATA LIFECYCLE MANAGEMENT:**

  - **Activity Logs**: Ensuring that all access and modification activities are logged.
  - **Security Information and Event Management (SIEM):** Using SIEM tools to monitor and analyze logs for suspicious activities.

- **8. COMPLIANCE AND GOVERNANCE:**

  - **Regulatory Compliance**: Ensuring that cloud storage configurations comply with relevant regulations and standards (e.g., GDPR, HIPAA, PCI-DSS).
  - **Policy Enforcement**: Verifying that organizational policies are enforced across all cloud storage environments.

- **9. SECURITY BEST PRACTICES:**

  - **Vendor-Specific Best Practices:** Review and implement best practices provided by the cloud storage vendor (e.g., AWS, Azure, Google, Cloud).
  - **Data Deletion**: Ensuring that data is securely deleted when no longer needed.

- **10. INCIDENT RESPONSE:**

  - **Response Plans:** Ensuring that incident response plans are in place and that staff are trained to handle security incidents.
  - **Forensic Readiness**: Preparing for forensic investigations by ensuring that necessary logs and data are available and securely stored.

By conducting a thorough cloud storage configuration review, organizations can identify and mitigate risks, ensure compliance with regulations, and enhance the overall security of their cloud-stored data.

1.4 Vulnerability analysis on specific systems:

Vulnerability analysis on specific systems involves a detailed examination of the system's security posture to identify, assess, and prioritize vulnerabilities. Here's a step-by-step approach to conducting vulnerability analysis on specific systems:

1. SCOPE DEFINITION

- **Identify Systems:** Determine which systems will be analyzed (e.g., servers, workstations, network devices, applications).
- **Define Boundaries: c**learly define the boundaries of the assessment, including network segments, subnets, and specific assets.

2. INFORMATION GATHERING

- **System Inventory:** Compile a list of all components, including hardware, software, and network configurations.
- **Documentation Review:** Examine existing documentation, including network diagrams, system configurations, and security policies.

3. RECONNAISSANCE

- **Network Scanning:** Use tools like Map to discover active systems, open ports, and services.
- **Service Enumeration:** Identify running services and their versions using tools like Nessus and OpenVAS.

4. VULNERABILITY IDENTIFICATION

- **Automated Scanning:** Employ automated vulnerability scanners to identify known vulnerabilities (e.g., Nessus, Qualys, Rapid7).
- **Manual Analysis:** Perform manual checks to identify vulnerabilities not covered by automated tools, such as configuration issues and business logic flaws.

5. VULNERABILITY VALIDATION

- **Verification:** Confirm the existence of identified vulnerabilities by attempting to replicate the conditions under which they were found.
- **False Positives:** Filter out false positives to ensure accurate reporting.

6. RISK ASSESSMENT

- **Impact Analysis:** Assess the potential impact of each vulnerability on the system, considering factors like data sensitivity and criticality.

- **Likelihood Analysis:** Evaluate the likelihood of exploitation based on factors like ease of exploitation and presence of mitigations.

7. PRIORITIZATION

- **Severity Rating:** Assign severity ratings to vulnerabilities based on their risk using CVSS scores.
- **Business Impact:** Consider the business impact and prioritize vulnerabilities that pose the greatest risk to the organization.

8. REPORTING

- **Detailed Findings:** Document each identified vulnerability, including a description, risk assessment, and evidence.
- **Recommendations:** Provide actionable recommendations for remediation or mitigation.
- **Executive Summary:** Create a high-level summary for stakeholders, highlighting key findings and strategic recommendations.

9. REMEDIATION

- **Action Plan:** Develop a remediation plan with specific steps, responsible parties, and timelines.
- **Patch Management:** Apply patches and updates to address verified vulnerabilities.
- **Configuration Changes:** Implement necessary configuration changes to strengthen and enhance security posture.

10. FOLLOW-UP

- **Verification:** Verify that remediation efforts have been successfully implemented.
- **False Positives:** Establish ongoing monitoring to detect new vulnerabilities and ensure continued security.

TOOLS AND TECHNIQUES

- **Network Scanners:** Nmap, Masscan
- **Vulnerability Scanners:** Nessus OpenVAS, Nikto, Rapid7
- **Configuration Tools:** CIS-CAT, Lynis
- **Manual Testing:** Penetration testing techniques, custom scripts
- **Compliance Checkers:** SCAP tools, cloud security poster management (CSPM) tools

BEST PRACTICES

- **Regular Scans:** Conduct regular vulnerability scans to stay ahead of emerging threats.
- **Patch Management:** Apply patches and updates to address identified vulnerabilities.
- **Security Training:** Implement necessary configuration changes to enhance security.

- **Incident Response:** Prepare an incident response plan to address security breaches promptly.

1.5 The test covers the following components:

- **External-facing IP addresses**
- **Web application and portals**
- **Cloud storage services (AWS)**
- **Specific critical servers (e.g., RDP, Exchange)**

2.0 Project Objectives

2.1 The primary objectives:

- Identify and evaluate potential vulnerabilities in the client's network and systems.
- Assess the effectiveness of current security measures and controls.
- Provide actionable recommendations to improve the overall security posture.

3.0 Assumptions

3.1 This assessment is based on the following assumptions:

- All necessary permissions and authorizations have been granted.
- The network and systems will remain operational during testing.
- No significant changes will be made to the network during the testing period.

4.0 Timeline

Timeline Table

Task	Duration
Planning and Scoping	1 week

Task	Duration
Reconnaissance	1 week
Vulnerability Analysis	2 weeks
Exploitation and Validation	1 week
Reporting	1 week

5.0 Summary of Findings

5.1 Threat Assessment

1. **Scenario 1: Unpatched RDP Exposed to the Internet**

   Description: Remote Desktop Protocol (RDP) is exposed to the Internet on an unpatched system.
   Operating System Affected: Windows Server 2016, 2019**.**
   Risks of Exploitation: Potential for unauthorized remote access, and lateral movement within the network.
   Remediation: Patch the RDP service and implement network-level authentication.

2. **Scenario 2: Web Application Vulnerable to SQL Injection**

   Description: The web application allows for SQL Injection attacks.
   Operating Systems Affected: All operating systems running the web application.
   Risks of Exploitation: Unauthorized data access, and database manipulation.
   Remediation: Implement parameterized queries and input validation.

3. **Scenario 3: Default Password on Cisco Admin Portal**

   Description: The Cisco admin portal is accessible with default credentials.
   Operating Systems Affected: Cisco devices.
   Risks of Exploitation: Complete control over network devices**.**
   Remediation: Change default passwords and implement strong password policies.

   1. **Scenario 4: Apache Web Server Vulnerable to CVE-2019-0211**

Description: Apache web server is vulnerable to privilege escalation.

In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.

Operating Systems Affected: Unix-based systems running Apache 2.4.17-2.4.38.
Risks of Exploitation: Local users could gain elevated privileges.
Remediation: Update Apache to the latest version. More information can be found on the NIST website.

Package List:

```
 - openSUSE Leap 42.3 (i586 x86_64):

    apache2-2.4.23-45.1
    apache2-debuginfo-2.4.23-45.1
    apache2-debugsource-2.4.23-45.1
    apache2-devel-2.4.23-45.1
    apache2-event-2.4.23-45.1
    apache2-event-debuginfo-2.4.23-45.1
    apache2-example-pages-2.4.23-45.1
    apache2-prefork-2.4.23-45.1
    apache2-prefork-debuginfo-2.4.23-45.1
    apache2-utils-2.4.23-45.1
    apache2-utils-debuginfo-2.4.23-45.1
    apache2-worker-2.4.23-45.1
    apache2-worker-debuginfo-2.4.23-45.1

 - openSUSE Leap 42.3 (noarch):

    apache2-doc-2.4.23-45.1
```

4. Scenario 5: Web Server Exposing Sensitive Data

Description: The web server is misconfigured, exposing sensitive data.
Operating Systems Affected: All operating systems running the web server.
Risks of Exploitation: Unauthorized access to sensitive information.
Remediation: Review and secure web server configuration, and restrict access.

5. **Scenario 6: Web Application Has Broken Access Control**

   Description: Web application lacks proper access controls.
   Operating Systems Affected: All operating systems running the web application.
   Risks of Exploitation: Unauthorized access to restricted areas.
   Remediation: Implement appropriate access control mechanisms.

6. **Scenario 7: Oracle WebLogic Server Vulnerable to CVE-2020-14882**

   Description: Oracle WebLogic Server is vulnerable to remote code execution.

   Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. 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. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

   Risks of Exploitation: Complete control over the affected server.

   36 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials.

   Remediation: Apply the latest security patches from Oracle. More information and patch updates are available on Oracle's website.

   Oracle recommends that customers apply the Critical Patch Update October 2020 to the Oracle Database components of Oracle Fusion Middleware products.

   Product releases that are not under Premier Support or Extended Support are not tested for the presence of vulnerabilities addressed by this Critical Patch Update. However, likely, earlier versions of affected releases are also affected by these vulnerabilities. As a result, Oracle recommends that customers upgrade to supported versions.

7. **Scenario 6: Misconfigured Cloud Storage**

   Description: AWS security group misconfigurations, and lack of access restrictions.
   Operating Systems Affected: AWS cloud environments.
   Risks of Exploitation: Unauthorized access to stored data.

Remediation: Review and apply proper access restrictions, and use encryption.

8. **Scenario 9: Microsoft Exchange Server Vulnerable to CVE-2021-26855**

   Description: Microsoft Exchange Server vulnerable to remote code execution.

   This vulnerability is part of an attack chain. The initial attack requires the ability to make an untrusted connection to Exchange server port 443.

   Operating Systems Affected: Exchange Server 2013, 2016, 2019
   Risks of Exploitation: Unauthorized access and control over the email server.
   Remediation: Apply security updates from Microsoft immediately. The following recommendations are suggested by Microsoft:

   This can be protected against by restricting untrusted connections, or by setting up a VPN to separate the Exchange server from external access. Using this mitigation will only protect against the initial portion of the attack. Other portions of the chain can be triggered if an attacker already has access or can convince an administrator to open a malicious file.

   We recommend prioritizing installing updates on Exchange Servers that are externally facing.

9. **Windows MSHTML Platform Security Feature Bypass Vulnerability**

   Description: MSHTML Platform Vulnerable to **CVE-2024-30040**
   Operating Systems Affected: Windows MSHTML
   Risks of Exploitation: Altered control flow, arbitrary control of a resource, or arbitrary code execution.
   Remediation: Apply security patches, monitor input validation.

6.0 Recommendations

6.1 Scenarios

1. Unpatched RDP Exposed to the Internet

- **Recommendation:** Apply the latest security patches, and restrict RDP access to internal networks only.

2. Web Application Vulnerable to SQL Injection

- **Recommendation:** Implement prepared statements, input validation, and WAF rules to block SQL Injection.

3. Default Password on Cisco Admin Portal

- **Recommendation:** Change default passwords immediately, and enforce strong password policies.

4. Apache Web Server Vulnerable to CVE-2019-0211

- **Recommendation:** Update Apache to the latest version, and apply relevant security patches.

5. Web Server Exposing Sensitive Data

- **Recommendation:** Restrict access to sensitive data, review and implement proper access controls.

6. Web Application with Broken Access Control

- **Recommendation:** Implement proper access controls, and regularly review access policies.

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

- **Recommendation:** Apply security patches, and update the WebLogic server.

8. Misconfigured Cloud Storage (AWS Security Group Misconfiguration)

- **Recommendation:** Review and correct security group configurations, and implement least privilege.

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

- **Recommendation:** Apply security patches, and update the Exchange server.