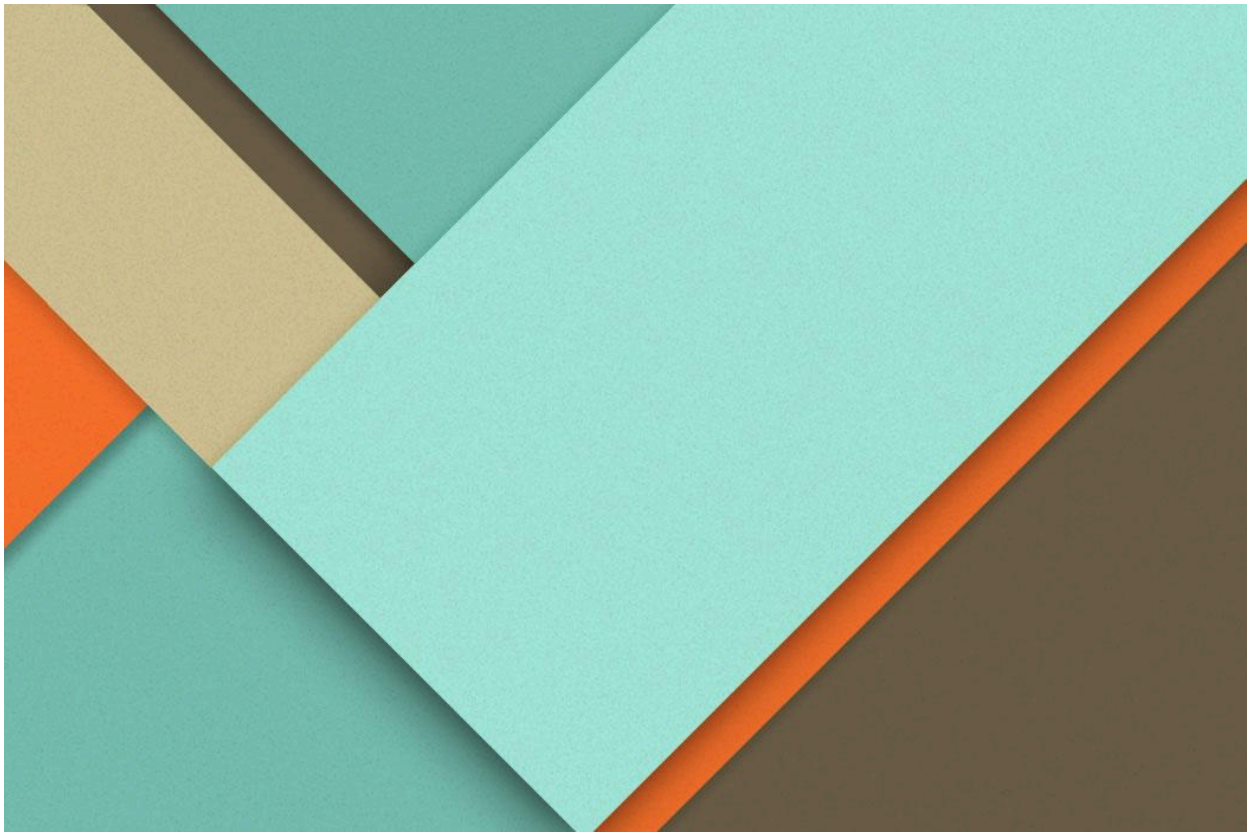

Penetration Testing Report

Detailed Technical Report

09.01.2024

Simeon Hawkins
Artemis, Inc.

Table of Contents

Overview

The cybersecurity assessment conducted for Artemis, Inc. aims to identify and evaluate vulnerabilities within the organization's network infrastructure, web applications, and other critical systems. The assessment includes a detailed analysis of the potential threats and provides actionable recommendations to mitigate the identified risks.

Scope of Work

The scope of this assessment includes, but is not limited to, the following areas:

1. **External Network Infrastructure:**
    - Perimeter devices (firewalls, routers, etc.)
    - Publicly accessible services (e.g., RDP, web servers)
    - DNS and email servers
2. **Internal Network Infrastructure:**
    - Internal servers and workstations
    - Network segmentation and access controls
    - SNMP-enabled devices
3. **Web Applications:**
    - Publicly accessible web applications (e.g, RFQ/RFP system)
    - Internal web applications used by employees
4. **Cloud Services:**
    - Cloud Storage configurations (e.g., AWS S3 buckets)
    - Cloud-based applications and services
5. **Authentication and Access Control:**
    - Single Sign-On (SSO) mechanisms
    - User authentication methods and policies

Project Objectives

The primary objectives of this cybersecurity assessment are to:

1. **Identify vulnerabilities in the external and internal network infrastructure:**
    - Conduct a thorough examination of both external and internal network infrastructure to uncover potential security weaknesses.
    - Evaluate the configuration and security of perimeter devices, including firewalls, routers, and publicly accessible servers.
2. **Assess the security posture of web applications and cloud services:**
    - Perform a comprehensive security assessment of publicly accessible web applications, including the RFQ/RFP system, to identify vulnerabilities such as SQL injection, cross-site scripting (XSS), and broken access controls.
    - Evaluate internal web applications used by employees for potential security weaknesses.
3. **Evaluate Cloud Services:**
    - Assess the security configurations of cloud storage services, particularly those hosted on AWS, to identify misconfigurations and potential data exposure risks.
    - Examine cloud-based applications and services for vulnerabilities that could be exploited by attackers.
4. **Review Authentication and Access Controls:**
    - Analyze the existing Single Sign-On (SSO) mechanisms and user authentication methods to ensure they are robust and secure.
    - Evaluate access control policies and practices to ensure they effectively restrict unauthorized access to sensitive resources.
5. **Perform Threat Analysis:**
    - Conduct a detailed threat analysis based on identified vulnerabilities to understand the potential impact and attack vectors.
    - Prioritize vulnerabilities based on their severity and the potential risk they pose to the organization.
6. **Provide Actionable Recommendations:**
    - Develop practical and actionable recommendations to mitigate identified vulnerabilities and strengthen the overall security posture.
    - Offer best practices and security controls that can be implemented to prevent future security breaches.
7. **Enhance Security Awareness:**

- Raise awareness among Artemis, Inc. staff about potential security threats and best practices for maintaining a secure environment.
- Provide guidance on developing a culture of security within the organization, promoting continuous vigilance and proactive security measures.

8. **Ensure Compliance:**
   - Ensure that the security assessment and subsequent recommendations align with relevant regulatory and compliance requirements.
   - Provide guidance on maintaining compliance with industry standards and best practices.
9. **Document Findings and Recommendations:**
   - Compile all findings, threat analyses, and recommendations into a comprehensive Detailed Technical Report for the IT staff.
   - Create an Executive Summary for senior management, highlighting the key findings and business risks in a concise and clear manner.

Assumptions

The Cybersecurity assessment for Artemis, Inc. is based on several key assumptions to ensure the effectiveness and accuracy of the findings and recommendations.

1. **Access to Systems and Personnel:**
   - Artemis, Inc. will provide full access to necessary systems, networks, and applications required for the assessment.
   - Key personnel, including IT staff and system administrators, will be available for interviews and to provide necessary information.
2. **Up-to-date System Documentation:**
   - Artemis, Inc. will provide accurate and up-to-date documentation of the network architecture, system configurations, and security policies.
   - Any changes to the network or systems during the assessment period will be promptly communicated to the assessment team.
3. **Stable Network Environment:**
   - The network environment will remain stable and consistent throughout the assessment period to ensure accurate and reliable results.
   - No significant network changes or upgrades will be implemented during assessment without prior notice.
4. **No Interference with Normal Operations:**
   - The assessment activities will be conducted in a manner that minimizes disruption to normal business operations.
   - Any potential disruptive activities, such as network scans, will be scheduled during off-peak hours or coordinated with Artemis, Inc. staff.
5. **Security Controls in Place:**

- Basic security controls, such as firewalls and antivirus software, are already in place and operational within the Artemis, Inc. network.
- The assessment will focus on identifying gaps and weaknesses in the existing security controls.

6. **Confidentiality and Data Protection:**
   - All information and data provided by Artemis, Inc. will be treated with the utmost confidentiality and used solely for the purpose of the assessment.
   - Sensitive data will be handled and stored securely, adhering to best practices for data protection.
7. **Current Threat Landscape:**
   - The assessment will be based on the current threat landscape and known vulnerabilities at the time of the assessment.
8. **Timely Remediation:**
   - Artemis, Inc. will take timely action to remediate identified vulnerabilities and implement recommended security controls.
9. **Regulatory Compliance:**
   - Artemis, Inc. will provide information on applicable regulatory and compliance requirements relevant to the assessment.
   - The assessment will consider these requirements when making recommendations to ensure compliance.
10. **Commitment to Security:**
    - Artemis, Inc. is committed to improving its security posture and will allocate the necessary resources to complement the recommended changes.
    - Ongoing security training and awareness programs will be supported to maintain a high level of security vigilance.

Timeline

The following timeline outlines the schedule of the cybersecurity assessment project for Artemis, Inc. it includes key milestones and deliverables to ensure the project is completed efficiently and effectively.

Phase 1: Planning

Duration: 2 days

Activities:

- Conduct initial meetings with key stakeholders
- Define the scope of work and project objectives
- Allocate necessary resources and finalize project plan.

Phase 2: Reconnaissance

Duration: 4 Days

Activities:

- Gather publicly available information about Artemis, Inc.
- Map network infrastructure and identify potential targets.

Phase 3: Scanning

Duration: 5 Days

Activities:

- Perform network scanning using tools like Nmap and Masscan.
- Conduct vulnerability scanning using Tenable Nessus, OpenVAS, and Burp Suite.

Phase 4: Analysis

Duration: 3 Days

Activities:

- Analyze identified vulnerabilities and assess associated threats.
- Prioritize vulnerabilities based on risk and potential impact.

Phase 5: Reporting

Duration: 4 Days

Activities:

- Draft the Detailed Technical Report, including findings and recommendations.
- Prepare the Executive Summary for senior management.

Phase 6: Review

Duration: 3 Days

Activities:

- Conduct an internal review of the reports.
- Present draft reports to Artemis, Inc for feedback.
- Make final revisions based on client input.

Phase 7: Presentation

Duration: 1 Day

Activities:

- Present the final findings and recommendations to Artemis, Inc. senior management and IT staff.

Phase 8: Remediation

Duration: 5 Days (if required)

Activities:

- Provide support and guidance for implementing recommended security measures.

Phase 9: Follow-Up

Duration: 2 Days

Activities:

- Conduct a post-remediation review to ensure all recommendations have been implemented.
- Submit the final report, including verification of remediation efforts.

Summary of Findings

The cybersecurity assessment of Artemis, Inc. revealed several critical vulnerabilities across the organization's network infrastructure, web applications, and cloud services. This summary highlights the key findings and provides an overview of the identified risks and their potential impact on the organization.

Key Findings

1. **Unpatched RDP Exposed to the Internet**
    - **Description:** Several RDP (Remote Desktop Protocol) servers are exposed to the internet without the latest security patches.
    - **Risk Level:** High
    - **Impact:** Potential unauthorized access and control over internal systems, leading to data breaches or system compromise.
2. **Web Application Vulnerable to SQL Injection**
    - **Description:** The RFQ/RFP web application does not properly sanitize user inputs, making it susceptible to SQL Injection attacks.
    - **Risk Level:** High
    - **Impact:** Unauthorized access to sensitive data, database manipulation, and potential data loss.

3. **Default Password on Cisco Admin Portal**
    - **Description:** Several Cisco devices are using default administrative passwords.
    - **Risk Level:** High
    - **Impact:** Unauthorized administrative access to network devices, leading to configuration changes or network compromise.
4. **Apache Web Server Vulnerable to CVE-2019-0211**
    - **Description:** An Apache HTTP Server is running a version vulnerable to privilege escalation (CVE-2019-0211).
    - **Risk Level:** Medium
    - **Impact:** Local attackers could gain root privileges, compromising the server and potentially other connected systems.
5. **Web Server Exposing Sensitive Data**
    - **Description:** An Apache HTTP Server is running a version vulnerable to privilege escalation (CVE-2019-0211)
    - **Risk Level:** Medium
    - **Impact:** Exposure of sensitive information to unauthorized parties, which could be used for further attacks.
6. **Web Application with Broken Access Control**
    - **Description:** The web application allows users to access resources and perform actions outside their intended permissions.
    - **Risk Level:** Medium
    - **Impact:** Unauthorized access to restricted areas, leading to data leakage or misuse of administrative functions.
7. **Oracle WebLogic Server Vulnerable to CVE-2020-14882**
    - **Description:** The Oracle WebLogic Server has a remote code execution vulnerability (CVE-2020-14882).
    - **Risk Level:** High
    - **Impact:** Remote attackers could execute arbitrary code, leading to full server control and potential data breaches.
8. **Misconfigured Cloud Storage**
    - **Description:** Cloud storage services, particularly AWS S3 buckets, are misconfigured, leading to potential data exposure
    - **Risk Level:** Medium
    - **Impact:** Unauthorized access to sensitive data stored in the cloud, leading to data breaches.
9. **Microsoft Exchange Server Vulnerable to CVE-2021-26855**
    - **Description:** The Microsoft Exchange Server has a remote code execution vulnerability (CVE-2021-26855).
    - **Risk Level:** High

- **Impact:** Remote attackers could execute arbitrary code, leading to data breaches and unauthorized access to email communications.

Recommendations

Key Recommendations

1. **Patch Management**
   - **Action:** Ensure that all systems and applications are up-to-date with the latest security patches and updates.
   - **Details:**
     i. Prioritize patching high-risk vulnerabilities, such as those affecting RDP servers, web applications, Oracle WebLogic Server, and Microsoft Exchange Server.
     ii. Implement an automated patch management process to regularly update software and systems.
   - **Benefit:** Reduces the risk of exploitation by known vulnerabilities and strengthens the overall security posture.
2. **Access Controls**
   - **Action:** Implement strong access control measures to restrict unauthorized access to critical systems and data.
   - **Details:**
     i. Change default passwords on all administrative accounts and enforce the use of strong, unique passwords.
     ii. Implement multi-factor authentication (MFA) for accessing sensitive systems and applications.
     iii. Regularly review and update access control policies to ensure compliance with best practices.
   - **Benefit:** Minimizes the risk of unauthorized access and protects sensitive data from potential breaches.
3. **Web Application Security**
   - **Action:** Enhance the security of web applications to protect against common vulnerabilities such as SQL Injection and broken access controls.
   - **Details:**
     i. Implement input validation and parameterized queries to prevent SQL Injection attacks.
     ii. Conduct regular security testing and code reviews to identify and remediate vulnerabilities.

iii. Utilize web applications firewalls (WAF) to detect and block malicious traffic.

- **Benefit:** Reduces the risk of data breaches and unauthorized access through web applications.

4. **Cloud Security**
   - **Action:** Strengthen the security of cloud storage and services to prevent data exposure and unauthorized access.
   - **DetailsL**
     i. Review and update cloud storage configurations, ensuring proper access restrictions and permissions.
     ii. Implement encryption for data at rest and in transit to protect sensitive information.
     iii. Conduct regular audits of cloud services to ensure compliance with security policies.
   - **Benefit:** Protects sensitive data stored in the cloud from unauthorized access and potential breaches.
5. **Continuous Monitoring and Incident Response**
   - **Action:** Establish continuous monitoring and incident response capabilities to detect and respond to security threats in real-time.
   - **Details:**
     i. Implement a Security Information and Event Management (SIEM) system to monitor network activity and detect anomalies.
     ii. Develop and maintain an incident response plan to ensure a rapid and effective response to security incidents.
     iii. Conduct regular security assessments and vulnerability scans to identify and remediate new risks.
   - **Benefit:** Enhance the organization's ability to detect, respond to, and recover from security incidents.
6. **Security Awareness Training**
   - **Action:** Conduct regular security awareness training for employees to promote a culture of security within the organization.
   - **Details:**
     i. Provide training on best practices for cybersecurity, including recognizing phishing attacks and handling sensitive data.
     ii. Encouraging employees to report suspicious activity and potential security incidents.
     iii. Evaluate the effectiveness of training programs through regular assessments and updates.
   - **Benefit:** Reduces the risk of human-related security incidents and fosters a proactive security mindset among employees.

Conclusion

Implementing these recommendations will help Artemis, Inc. address the identified vulnerabilities and strengthen its defenses against cyber threats. By prioritizing patch management, enhancing access controls, securing web applications and cloud services, and investing in continuous monitoring and security awareness training, Artemis, Inc. can significantly improve its security posture and protect its critical assets from potential attacks.