Phase 4: Threat Assessment

Objective: This document presents a hypothetical threat assessment for Artemis, Inc., based on nine potential vulnerabilities. Each entry provides an analysis of the vulnerability, affected systems, risks upon exploitation, possible attack vectors, countermeasures, and remediation actions. This assessment will aid in prioritizing remediation efforts and improving Artemis's overall security posture.

Vulnerability Assessment

Scenario 1: Unpatched RDP Exposed to the Internet

- **Description**: Microsoft Remote Desktop Protocol (RDP) is exposed to the internet without patches. Vulnerabilities like CVE-2019-0708 (BlueKeep) enable attackers to execute code remotely.
- **Operating Systems/Versions Affected**: Primarily Windows 7, Windows Server 2008, and some other legacy systems.
- **Exploitation Risks**: High chance of a denial-of-service (DoS) attack or remote code execution (RCE). Could cause system crashes, potentially locking out legitimate users.
- **Risk Upon Exploitation**: An attacker could gain unauthorized access, execute arbitrary code, move laterally across the network, or conduct DoS attacks.
- **Attack Vectors**:
    - Brute-force attacks on RDP credentials.
    - Exploiting known RDP vulnerabilities like BlueKeep for remote code execution.
- **Blocking Mechanisms**:
    - Firewalls, Intrusion Detection Systems (IDS), and antivirus (AV) software may help. These defenses could be bypassed by tunneling RDP traffic through encrypted channels or using obfuscation tools.
- **Remediation Action**:
    - Restrict RDP access to internal IPs only.
    - Apply security patches to ensure systems are protected against vulnerabilities like BlueKeep.
    - Enable network-level authentication (NLA) to reduce RDP attack surfaces.
- **CVSS Score**: 9.8 (Critical)

Scenario 2: Web Application Vulnerable to SQL Injection

- **Description**: SQL Injection allows attackers to execute unauthorized SQL commands against a backend database, potentially exposing or modifying sensitive data.
- **Operating Systems/Versions Affected**: Affects web applications with SQL databases, including MySQL, MSSQL, and Oracle.
- **Exploitation Risks**: High risk of data theft or corruption; possible denial of service if the database is overloaded with malicious queries.
- **Risk Upon Exploitation**: Direct access to sensitive data, including user credentials and PII. Possible modifications to database data or deletion of entire records.
- **Attack Vectors**:
    - Malicious input in vulnerable input fields.
    - HTTP request manipulation using tools like Burp Suite or SQLmap.
- **Blocking Mechanisms**:
    - Web Application Firewalls (WAF) and input validation practices can mitigate SQLi attacks. However, attackers can use obfuscated payloads to bypass basic WAF filtering.
- **Remediation Action**:
    - Implement parameterized queries and prepared statements to prevent SQL Injection.
    - Set WAF rules to monitor and block SQL Injection attempts.
- **CVSS Score**: 9.0 (Critical)

Scenario 3: Default Password on Cisco Admin Portal

- **Description**: The Cisco administration portal is accessible with default or weak passwords, allowing unauthorized access.
- **Operating Systems/Versions Affected**: Affects Cisco routers, switches, and other Cisco-based network devices.
- **Exploitation Risks**: Unauthorized access may lock out legitimate users or cause system disruptions if the device settings are altered.
- **Risk Upon Exploitation**: Full control over the network device configuration, which can lead to network disruptions or man-in-the-middle (MITM) attacks.
- **Attack Vectors**:
    - Brute-force or credential stuffing attacks using common default credentials.
    - Direct access over HTTP/S with known default admin credentials.
- **Blocking Mechanisms**:
    - Two-factor authentication (2FA) and AV software on admin devices. These defenses can be bypassed using credential stuffing or brute-force attacks.
- **Remediation Action**:
    - Enforce strong password policies and remove all default credentials.

    - Enable 2FA on the Cisco admin portal to strengthen authentication.
- **CVSS Score**: 7.5 (High)

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

- **Description**: Privilege escalation vulnerability in Apache HTTP Server allows attackers to gain elevated permissions, potentially leading to full server compromise.
- **Operating Systems/Versions Affected**: Apache HTTP Server versions 2.4.17 to 2.4.38.
- **Exploitation Risks**: Unauthorized elevation of privileges, potential crash of services or host.
- **Risk Upon Exploitation**: Full control over web server, access to sensitive files, and potential for lateral movement within the network.
- **Attack Vectors**:
    - Exploit privilege escalation by executing malicious scripts.
    - Install backdoors for persistent access.
- **Blocking Mechanisms**:
    - AV software, IDS/IPS, though attackers may evade detection using encrypted payloads.
- **Remediation Action**:
    - Update Apache to the latest secure version.
    - Limit privilege access on the web server to reduce the potential for privilege escalation.
- **CVSS Score**: 8.8 (High)

Scenario 5: Web Server Exposing Sensitive Data

- **Description**: Sensitive files (e.g., backup, configuration files) are exposed on a web server due to improper permissions.
- **Operating Systems/Versions Affected**: Web servers across various platforms.
- **Exploitation Risks**: Exposure of sensitive data can lead to PII or credential theft.
- **Risk Upon Exploitation**: Potential data leakage, including credentials or PII, which could enable further targeted attacks.
- **Attack Vectors**:
    - Direct access to directories not configured correctly.
    - Files may also be indexed by search engines, making them publicly accessible.
- **Blocking Mechanisms**:
    - WAF rules and strict file permissions can help prevent access, though attackers may bypass protections by accessing exposed file paths directly.
- **Remediation Action**:
    - Remove public access to sensitive files and apply correct permissions.

    - Regularly audit file permissions on the server.
- **CVSS Score**: 7.3 (High)

Scenario 6: Web Application with Broken Access Control

- **Description**: Inadequate access control mechanisms allow unauthorized access to restricted areas or actions.
- **Operating Systems/Versions Affected**: Commonly affects custom web applications, CMS platforms.
- **Exploitation Risks**: Unintended privilege escalation, unauthorized data modification or access.
- **Risk Upon Exploitation**: Unauthorized data access, including admin panels and sensitive functions; potential for data theft or unauthorized actions.
- **Attack Vectors**:
    - Bypass controls by directly accessing URL endpoints or exploiting unprotected API endpoints.
- **Blocking Mechanisms**:
    - Role-based access controls (RBAC) and WAF rules. Attackers may bypass by navigating directly to vulnerable URLs.
- **Remediation Action**:
    - Implement RBAC, apply token validation, and enforce authentication on sensitive endpoints.
- **CVSS Score**: 8.0 (High)

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

- **Description**: A remote code execution vulnerability allows unauthorized access to WebLogic servers.
- **Operating Systems/Versions Affected**: Oracle WebLogic versions before the October 2020 patch.
- **Exploitation Risks**: May crash server, affecting availability and user access.
- **Risk Upon Exploitation**: Full server control, remote execution, lateral movement, and data access.
- **Attack Vectors**:
    - Exploit through specially crafted HTTP requests for RCE.
- **Blocking Mechanisms**:
    - WAF, AV software; attackers may bypass using encrypted or obfuscated payloads.
- **Remediation Action**:
    - Patch WebLogic to the latest version; limit access through network segmentation.
- **CVSS Score**: 9.8 (Critical)

Scenario 8: Misconfigured Cloud Storage (AWS S3)

- **Description**: AWS S3 bucket misconfiguration allows unrestricted access, enabling data leakage.
- **Operating Systems/Versions Affected**: AWS S3 storage.
- **Exploitation Risks**: Data tampering, deletion, or exposure; reputational harm if sensitive data is exposed.
- **Risk Upon Exploitation**: Direct access to sensitive data, with potential for data manipulation or deletion.
- **Attack Vectors**:
    - Direct access through AWS URLs; tools like `awscli` can be used to list bucket contents.
- **Blocking Mechanisms**:
    - AWS Identity and Access Management (IAM) policies; attackers may bypass through public API endpoints.
- **Remediation Action**:
    - Enforce “least privilege” IAM policies, disable public access, and use bucket policies for strict access control.
- **CVSS Score**: 8.5 (High)

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

- **Description**: A server-side request forgery (SSRF) vulnerability in Microsoft Exchange allows remote attackers to bypass authentication.
- **Operating Systems/Versions Affected**: Microsoft Exchange Server 2013, 2016, and 2019.
- **Exploitation Risks**: Exploitation may lock out users, and server may crash under heavy load.
- **Risk Upon Exploitation**: Full compromise of the Exchange server, privilege escalation, and

Summary of Threat Assessment

This threat assessment has analyzed nine potential vulnerabilities within Artemis, Inc.’s network infrastructure and applications, identifying the risks and possible attack vectors associated with each one. These vulnerabilities range from common misconfigurations, like an exposed RDP service and default passwords, to specific high-risk vulnerabilities affecting Oracle WebLogic, Apache, and Microsoft Exchange. Key findings include:

1. **High-Risk External Access Points**: Vulnerabilities such as exposed RDP, SQL Injection, and web application access control issues could provide attackers with initial access points to the network. Remote access vulnerabilities, such as unpatched RDP

and SQL Injection, scored high in risk due to the potential for unauthorized entry and lateral movement within the network.
2. **Application-Level Threats**: Vulnerabilities in web applications, particularly SQL Injection, broken access control, and sensitive data exposure, indicate a need for enhanced application security practices, such as implementing Web Application Firewalls (WAF), input validation, and stricter access control policies.
3. **Critical System Vulnerabilities**: Notable vulnerabilities affecting core services, including the Microsoft Exchange Server (CVE-2021-26855) and Oracle WebLogic Server (CVE-2020-14882), highlight the importance of regular patch management and system updates to prevent exploitation. The CVSS scores reflect the high risk of exploitation, data exposure, and remote code execution that these vulnerabilities present.
4. **Cloud Configuration and Data Exposure Risks**: Misconfigured AWS S3 storage exposes sensitive data and creates a risk of data loss or tampering, underscoring the need for strict IAM policies, secure bucket configurations, and regular audits of cloud assets.

Key Recommendations

1. **Implement Strong Patch Management**: Ensure timely application of patches for critical systems like Microsoft Exchange, Oracle WebLogic, Apache, and network devices.
2. **Strengthen Access Controls and Authentication**: Enforce multi-factor authentication (MFA), eliminate default credentials, and implement role-based access control (RBAC) to protect administrative portals and applications.
3. **Enhance Application Security**: Apply secure coding practices, use parameterized queries to prevent SQL Injection, and implement a WAF to mitigate risks associated with web applications.
4. **Regular Configuration and Security Audits**: Conduct routine audits of cloud storage configurations, file permissions, and network device settings to identify and rectify misconfigurations.
5. **Continuous Monitoring and Threat Detection**: Deploy intrusion detection systems (IDS), intrusion prevention systems (IPS), and endpoint security tools to detect and mitigate suspicious activities quickly.

Artemis, Inc. can significantly improve its security posture by addressing these vulnerabilities based on their criticality and the CVSS scores provided, reducing the risk of unauthorized access, data breaches, and system compromise. This threat assessment provides a prioritized list of actions that should be implemented to safeguard the organization against potential security incidents.