Detailed Technical Report of Artemis Inc. Penetration Test

Ronald Rodriguez Reyes

University of South Florida (USF)

03/13/25

Table of Contents

Scope of Work

Testing scope

Client	Artemis Inc.
Penetration Testing Provider	CyberHack Inc.
Engagement Start Date	March 3, 2025
Engagement End Date	March 11, 2025

Assets to Be Tested	
External Network	**Internal Network**
Web Application	Routers
Cloud Storage	On-Prem Servers
Firewalls	Endpoints

Exclusions
Social Engineering Attacks
Physical Penetration Testing

Type of testing technique

- Black box testing is a type of testing for which we know nothing about the company, just its name.
- Grey Box is a type of testing in which the tester knows some company details.

Methodology

The penetration test will follow industry-recognized frameworks and methodologies, including:

- OSINT: For gathering information.
- OWASP 10: For Web Application vulnerability test
- Network Scanning: For discovering and enumerating host
- Privilege escalation: Attempt to escalate privilege to compromise system
- Exploitation: Attempt to exploit identified vulnerabilities to compromise the system.
- Post Exploitation: Testing the impact of successful breach and lateral movements.

Tools

- Burp Suite
- OWASP ZAP
- Nmap
- Nessus
- OpenVAS
- Wireshark
- Metasploit
- John the Ripper
- SamDump2

Project Objectives

- Reveal vulnerabilities within Artemis Inc.'s internal and external network infrastructure and web applications.
- Assess the effectiveness of network appliances in detecting and thwarting attacks.
- Assess the impact of exploiting those vulnerabilities
- Provide recommendations to improve security posture and risk management.
- Verify that the system or network meets regulatory compliance requirements and security best practices.

Assumptions

- The right individuals within the organization approve the penetration test.
- The penetration testing will be performed to minimize disturbances to normal business operations.
- The penetration testing team will use a standard set of tools, techniques, and methodologies for testing mentioned in the scope.
- The penetration testing team will adhere to strict confidentiality and data protection protocols during and after the engagement, including handling sensitive data.
- The penetration test will be completed within the time frame selected in the scope.

Timeline

Reconnaissance Stage: March 3, 2025 - March 4, 2025

Discovering and Enumerating Stage: March 5, 2025 - March 5, 2025

Vulnerability Assessment Stage: March 6, 2025 - March 7, 2025

Threat Assessment Stage: March 10, 2025 - March 11, 2025

Reporting Stage: March 12, 2025 - March 13, 2025

Summary Findings

The penetration process on Artemis Inc.'s internal and external networks revealed three critical, five high, and one medium vulnerabilities.

Vulnerabilities

- One of the Cisco appliances was added to the internal network without changing the default password.
- The Oracle WebLogic Server contains a vulnerability that allows intruders to compromise it through the HTTP protocol.
- One Microsoft Exchange Server presents a vulnerability that allows unauthenticated users to send random HTTP requests and authenticate.
- CVE-2019-0211 is an Apache web server vulnerability that allows the attacker to execute random code with the privileges of the parent process by controlling the scoreboard.
- A web server with a security hole that exposes sensitive data to unauthorized network users can lead to identity theft and financial fraud.
- An unpatched endpoint using Remote Desktop Protocol (RDP) was facing the Internet.
- The web application was helpless against SQL injection.
- A web application with a broken access control allows the hacker to penetrate the system by parameter tampering or force browsing.
- A misconfigured Cloud Storage in AWS providing more permission than the user needs

Impacts

If these vulnerabilities are exploited, the intruder could exfiltrate the information and use it for identity theft, financial fraud, impersonation of the victims, sell it, or launch a social engineering attack to compromise more victims. He could also escalate the privileges in the system to find and crack the passwords using the John the Ripper tool. After that, he could compromise the endpoint and move it horizontally using worms. He could also create a botnet using the technique previously described and launch a DoS attack. He could also redirect or block network traffic if he compromises a network device such a router.

Recommendations

The company must implement the following suggestions to enhance its security stance while complying with cybersecurity best practices.

Immediate Recommendations

- The administrator must change this device's default password as soon as possible and adhere to the standard for safe passwords to make it difficult to crack.
- The administrator should filter or block Port 700 to prevent harm during the patching.
- The administrator should employ a web application firewall (WAF) to reduce the attack surface.
- The administrator should install antivirus software in the endpoints to detect and protect against malware.
- The administrator should patch several applications to prevent attackers from exploiting the identified vulnerabilities.

Short-Term Recommendations

- The administrators should enforce the principle of least privilege for users with access to servers to reduce damage in case of a breach.
- The developers should validate all the input fields to prevent injection attacks.
- The data should also be encrypted while traveling through the network using SSL/TLS and SSH protocols.
- Forced to establish a connection with secure protocols.
- Data should be encrypted with symmetric algorithms at rest, and the key should be on a different device.

- The developers should implement access control once and reuse it throughout the application.
- The administrator should change the policy of web application access to deny access by default unless it is a public resource, alert the administrator when a login fails, and follow the OAuth standard.

Long-Term Recommendations

- The provisioning network process should be reviewed and updated to prevent these issues.
- Audit the provisioning process and evaluate which permissions should be added to which roles to ensure the least privilege principle and remove unused users and roles.
- The administrator should review and improve the update and patching process to prevent future issues.