Artemis Inc
Security Assessment Findings Report

Business Confidential

Date: March 18th, 2023
Version: 1.0

Table of Contents

Confidentiality Statement

This document is the exclusive property of Artemis Inc.(AI) and Cyber Cube (CC). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both AI and CC.

CC may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. CC prioritized the assessment to identify the weakest security controls an attacker would exploit. CC recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

Name	Title	Contact Info
Artemis Inc.		
Peter Quill	VP, Information Security (CISO)	111-685-7960
Wade Wilson	IT Manager	222-573-3868
Bruce Banner	Network Engineer	333-583-3858
Cyber Cube		
Pepper pots	Lead Penetration Tester	444-583-5864
Jack Sparrow	Penetration Tester	555-685-6958
Howard Stark	Account Manager	666-104-2968

Assessment Overview

From February 2nd, 2023 to February 27th , 2023, Artemis Inc (AI) engaged CyberCube (CC) to evaluate the security posture of its infrastructure compared to current industry best practices that included an external penetration test. All testing performed is based on the NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks.

Phases of penetration testing activities include the following:
· Planning – Customer goals are gathered and rules of engagement obtained.
· Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
· Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
· Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.

Executive Summary

Find errors within Artemis Inc. which includes Network hardware being configured correctly, Filters sorting through file and data uploads, and 3rd party companies and employees following company policy. Anything not explicitly mentioned in scope can be treated as out of scope during this engagement.

Artemis Inc. allows Cyber Cube to go through their system to find problems within their network which could jeopardize their company due to security not being up to date. By allowing Cyber Cube to go through their network and report their findings it would save Artemis Inc. money, if they were to get a breach it would cost millions. By starting to fix the problem it allows them to fix their walls to prevent an attack. The vulnerability assessment will take place through February 2nd,2023 through February 26th, 2023

Objectives

Before the vulnerability test took place Artemis Inc. tasked Cyber Cube with finding a solution to their filters to uploading data. Artemis also had other concerns that they notified CC about which includes network hardware, IT Administrators not complying to company policy, and 3rd party companies not being compliant with data storage. These were all tested due to possible vulnerabilities that could be exploited such as an APT going up the ladder due to non configured network hardware.

Methodology
During the vulnerability test CC likes their employees to use these tools because from trial and error of using different selection of tools, we prefer this selection:

- Nmap- Network scanner
- OSINT Framework- Search engine query
- OpenVAS- Vulnerability scanner
- Google Dorks- Google query
- Zenmap- Network scanner with GUI

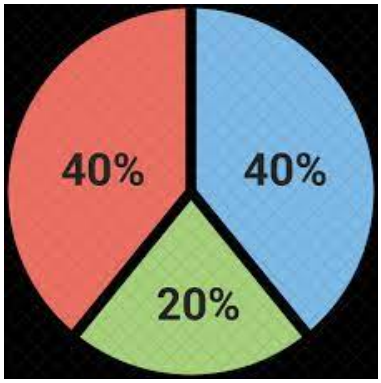
- Nslookup- Name server lookup
- Nessus- Vulnerability Scanner
- Burp Suite- Vulnerability Scanner

Summary of findings and key recommendations

CC found a badly configured Network due to having a mix of old and new network. The Old network hardware was out of date and has known exploits. The newer network hardware was not configured correctly which means an attacker could bypass as a user and won't look suspicious.
Recommendation:
Upgrade to Newer equipment making sure there are no older models. After obtaining the new models configure the network firewalls so there are no attacks like man in the middle.

Conclusion

With a newly evolving environment in cyberspace everyone needs to be careful and guarded up with security. By having security in your company you are able to protect the company, their assets, and customers



Color code:
- High risk = blue
- Moderate risk = red
- Critical risk = green

Scope of work:

This security assessment covers the remote penetration of Artemis Inc. with a possible vulnerability including Artemis' RFQ/RFP web application does not restrict or filter user uploads by file type. Which could lead to allowing threat actors to connect remotely, execute arbitrary code, and then elevate their privileges within the application. Configuration of old and new network hardware,and compliance to company policy. Anything not explicitly mentioned in scope can be treated as out of scope during this engagement

Project Objectives

The major objectives of this structured walkthrough are to find errors within filters to restrict user uploads, within old hardware and new hardware to improve the quality of the product or service to be delivered, by performing an external penetration test.

To accomplish the penetration test, CC will implement the following four phases:

1. Perform simulated reconnaissance of the client.
2. Simulate target identification and scans against the external network.
3. Simulate the identification of vulnerabilities.
4. Based on the above, assess the threats and make recommendations.

By implementing these phases in the test CC is able to check the security of Artemis Inc. while staying in scope.

Approach

CC performed a penetration test under a “black box” approach February 2nd, 2023, to February 27th , 2023 without credentials or any advance knowledge of Artemis’ internally facing environment with the goal of identifying unknown weaknesses. Testing was performed from a non-evasive standpoint with the goal of uncovering as many misconfigurations and vulnerabilities as possible.

Testing was performed remotely via a host that was provisioned specifically for this assessment. Each weakness identified was documented and manually investigated to determine exploitation possibilities and escalation potential.

CC sought to demonstrate the full impact of every vulnerability, up to and including internal domain compromise. If CC were able to gain a foothold in the internal network, allowing for further testing including lateral movement and horizontal/vertical privilege escalation to demonstrate the impact of an internal network compromise.

Assumptions

Sean has been given permission to go through Artemis Inc. network to make sure filters and other possible vulnerabilities in the network are patched and fixed.

Timeline

Event	Date(s)
Project Scope Definition Meeting	02.02.2023
Project Scope Review Meeting	02.03.2023
Project Initiated	02.06.2023
Project planning meeting	02.09.2023
External Penetration Testing	02.10.2023 – 02.21.2023
Report Issued	02.22.2023
Summary Letter Issues	02.23.2023
Status Meeting	02.26.2023
Project Closed	02.26.2023

Summary of Findings Table

9.0-10	7.0-8.9	4.0-6.9	0.1-3.9	N/A
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Restriction of user uploads	Critical	Restrict the filter to only allowing certain files or data uploaded depending on what the company only wants to be uploaded
Attackers can exploit older hardware	High	Upgrade all older network hardware and get new hardware
Attackers can bypass firewalls when network isn't configured	High	After getting new hardware configure the network to make sure everything is compliant with policies
Units not following company policy	Moderate	Business units need to upload all data to the cloud
Employees not following policies	Moderate	Make sure that IT admins follow company policies so they aren't jeopardizing the security of the company

Detailed Findings

Inline are the expanded findings outlined above, for more information on the scope of testing that was performed, please refer to above sections on scope, methodology, and context of the engagement kickoff.

Description	Some of the older network hardware that is being phased out is unsupported and may have unpatched vulnerabilities.
Risk	Attackers can exploit older hardware
Remediation	Upgrade all older network hardware and get new hardware
References	A06 Vulnerable and Outdated Components - OWASP Top 10:2021

Description	Some of the newer network hardware may not have been configured properly
Risk	Attackers can bypass firewalls when network isn't configured
Remediation	After getting new hardware configure the network to make sure everything is compliant with policies

Description	Some business units do not always follow company policy regarding storing data in the cloud, creating websites, or conducting file transfers.
Risk	Could create problems with file data being used by unauthorized people
Remediation	Business units need to upload all data to the cloud

Description	Some IT admins like to do their own thing because “that’s the way they’ve always done it.” This could be exposing the network to unknown risks.
Risk	This could cause chaos since no one is following rules and no communication
Remediation	Make sure that IT admins follow company policies so they aren't jeopardizing the security of the company

Description	Artemis’ RFQ/RFP web application does not restrict or filter user uploads by file type.
Risk	This is a vulnerability that could allow threat actors to connect remotely, execute arbitrary code, and then elevate their privileges within the application. In this instance, the threat actors would be able to view or download sensitive information regarding bids and even gain admin rights within the application.
Remediation	Restrict the filter to only allowing certain files or data uploaded depending on what the company only wants to be uploaded

Final Recommendations

- Upgrade all older network hardware and get new hardware
- After getting new hardware configure the network to make sure everything is compliant with policies
- Restrict the filter to only allowing certain files or data uploaded depending on what the company only wants to be uploaded
- Make sure that IT admins follow company policies so they aren't jeopardizing the security of the company
- Business units need to upload all data to the cloud

Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact:

Severity	CVSS Score	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.