Technical Report: A Detailed Technical Report for Artemis IT Staff.

Vincent Kiweesi

Capstone

May 26th, 2023

[**Appendices 3**](#_b6blimbat0a6)

[Appendix A 4](#_j5owvz9xhr0w)

[**Scope of work 5**](#_ew07bxfpm5gp)

[**Project Objectives 5**](#_linl00iv1s0q)

[**Assumption 5**](#_smty1gwhbqce)

[**Timeline 5**](#_vqcrenruz47m)

[**Summary of Finding 6**](#_l70j5tlr3m47)

[**Summary of Recommendation 7**](#_e0zl9sui6q97)

[Vulnerability Management: 8](#_6fp6k5wxmj7s)

[Access Management: 8](#_oytoom8n7qtf)

[Security Awareness Training: 8](#_y5d0onaxb6q)

# Appendices

## 

## Appendix A

Black Box Penetration Testing

For Artemis

05/26/2023

By: Vincent Kiweesi

# Scope of work

Three accessible servers are subjected to an external penetration testing as part of this security assessment. With no awareness of the data being assessed, the evaluation was conducted in a "black box" method.

# Project Objectives

The objective of this security assessment was to identify and evaluate potential vulnerabilities and risks within Artemis' network infrastructure and web applications. The assessment focused on various areas, including remote access vulnerabilities, web application security, default credentials, and misconfigurations.

# Assumption

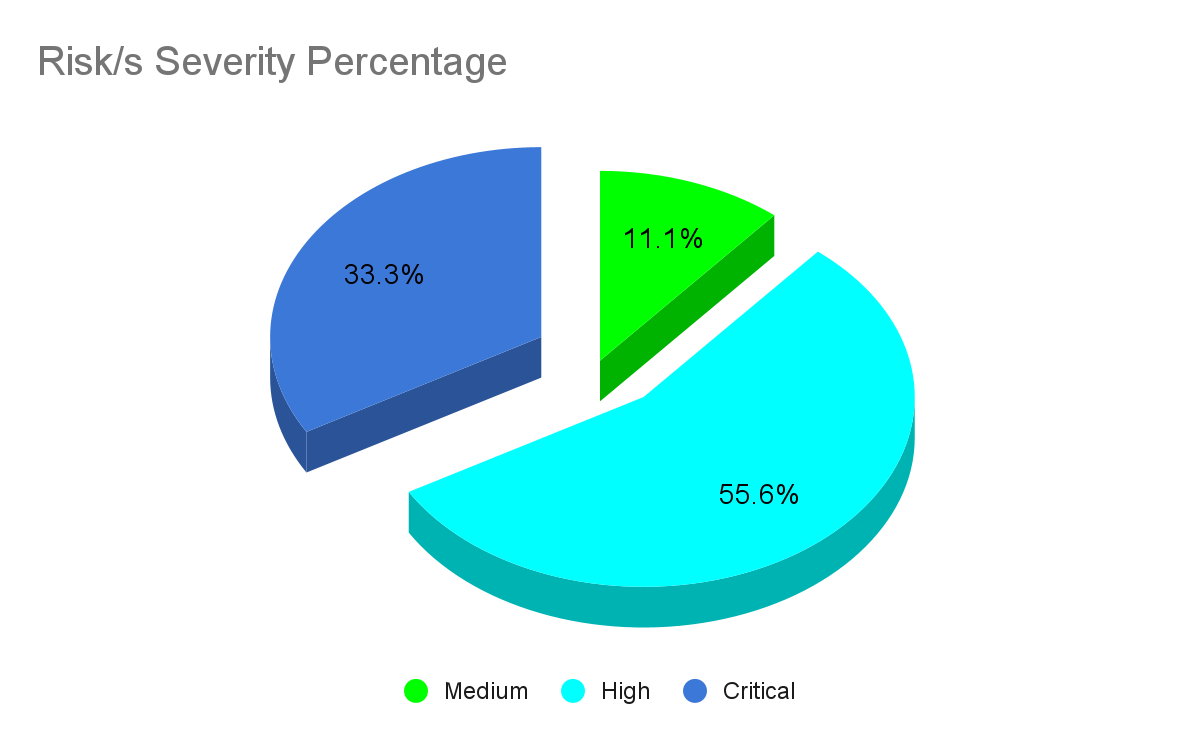
Its presume that both IP addresses are regarded as public IP addresses, that an NDA and terms of engagement have been signed, and that the name of the company is Artemis based on the reconnaissance phase.

# Timeline

|  |  |  |
| --- | --- | --- |
| **Penetration Testing** | **Start Date/Time** | **End Date/Time** |
| Pen Test 1 | 05/10/2023 | 05/23/2023 |

# Summary of Finding

|  |  |
| --- | --- |
| **Value** | **Number of risks** |
| Low | 0 |
| Medium | 1 |
| High | 5 |
| Critical | 3 |

****

Artemis faces multiple high-risk vulnerabilities across its network infrastructure and web applications. It is crucial to address these vulnerabilities promptly to mitigate the risk of unauthorized access, data breaches, and potential system compromise. We strongly recommend applying the recommended patches, implementing proper access controls, and regularly reviewing and updating security configurations.

# 

# Summary of Recommendation

Implement a defense-in-depth strategy in which Artemis uses a range of security tools, systems, and procedures to safeguard its assets and data. like some of these:

* To prevent an attacker from exploiting the vulnerability, it should be patched as soon as possible.
* To prevent an attacker from exploiting Vulnerabilities, default passwords should be changed as soon as possible.
* To prevent an attack from exploiting Vulnerabilities, they should be patched as soon as possible.
* Access to the data should be limited and should be encrypted as soon as possible to prevent an attacker from exploiting it.
* To prevent an attacker from exploiting Vulnerabilities the access control should be fixed as soon as possible.
* To prevent an attacker from exploiting Vulnerabilities they should be patched as soon as possible.
* To prevent an attacker from exploiting Vulnerabilities, misconfiguration should be fixed as soon as possible.

## Vulnerability Management:

* Put in place a reliable patch management system to guarantee timely updates and fix known vulnerabilities.
* Run regular penetration tests and vulnerability assessments to proactively find and fix vulnerabilities.

## Access Management:

* Implement multi-factor authentication (MFA) and the least privilege principles to strengthen access controls.
* To reduce the danger of unauthorized access, periodically review and update user access privileges.

## Security Awareness Training:

* To reduce the risk of social engineering assaults, give all workers thorough security awareness training.
* Encourage reporting of suspicious activity or occurrences and build a culture of cybersecurity awareness.
* Target the training depending on requirements of employees, such as IT staff, executives, or non-technical personnel, the training materials may change. It is easier to make sure that everyone receives the right information and direction regarding their obligations by tailoring the training to diverse audiences.
* Run simulated phishing exercises to determine the employees' sensitivity to phishing assaults, these exercises involve sending simulated phishing emails to them. The findings highlight the value of maintaining vigilance against such threats and point out areas that need more training.
* Use of multi-factor authentication (MFA) increases security by asking users to submit additional verification in addition to their standard login information, such as a one-time password or biometric information. People can understand the value of MFA in securing their accounts and sensitive data by being encouraged to utilize it.
* Secure Remote Work Practices, train people about secure procedures for gaining access to company resources from locations other than the typical office setting. This includes safeguarding home networks and devices, avoiding unsecured Wi-Fi networks, and employing secure VPN connections.
* Emphasize the importance of rapidly applying updates and patches to safeguard against potential vulnerabilities.
* People need to be aware of the dangers to physical security, including shoulder surfing, tailgating, and handling important documents and equipment correctly.
* Best practices must be emphasized and continuously communicated like utilizing a variety of tools to keep security awareness top of mind for staff, including internal blogs, posters, and recurring reminders.
* Encourage teamwork among participants who actively seek out and report potential security incidents. Security breaches can be prevented and mitigated by promoting open communication and developing a culture where people feel comfortable reporting irregularities or weaknesses.
* Cover data protection rules, privacy legislation, and their roles in protecting sensitive data.
* Stay informed of new threats and developing best practices, security awareness programs should be frequently evaluated and updated and take into account employee feedback, incident trends, and industry advancements.
* Mobile device security: As smartphones and tablets become more common, People receive instruction on how to protect their mobile devices with secure passcodes, enable encryption, and exercise caution when downloading apps or connecting to unsecured Wi-Fi networks.
* People must be aware of the proper handling and protection of sensitive data like data privacy laws, safe data handling procedures, and the potential repercussions of data breaches or unauthorized disclosure.
* Promoting a culture of immediately reporting security incidents or suspicious activity is part of security awareness. To guarantee a prompt and efficient response, people should be aware of who to contact and how to report issues.
* For the protection of online accounts and systems, strong passwords are important. using strong, one-of-a-kind passwords, changing them frequently, and not using the same password for several accounts.
* Social engineering is the practice of deceiving others in order to obtain sensitive information or unlawful access. Inform people about social engineering attack techniques including impersonation, pretexting, and baiting so they can see and prevent such tries.