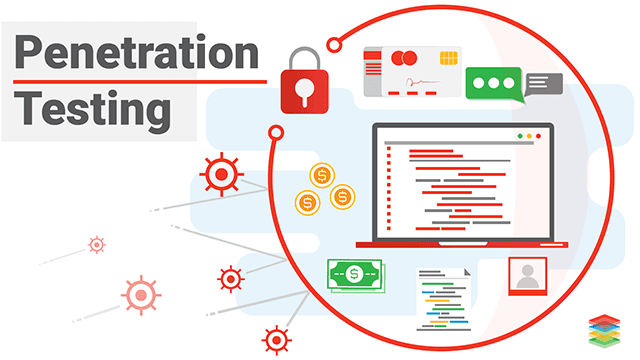
**Artemis Penetration Testing**

**By: Long Trang Corp.**



**Table of content**

[**Scope of Work 3**](#_mlyn3nxax0mk)

[**Project Objectives 4**](#_t53l2lu00pjg)

[**Assumptions 5**](#_d037yt3vrkb4)

[**Timeline: 5**](#_kk498o50qs2c)

[**Summary of Findings: 6**](#_cssdvu8v6vqy)

[**Recommendations: 8**](#_fbcu8j7wyafm)

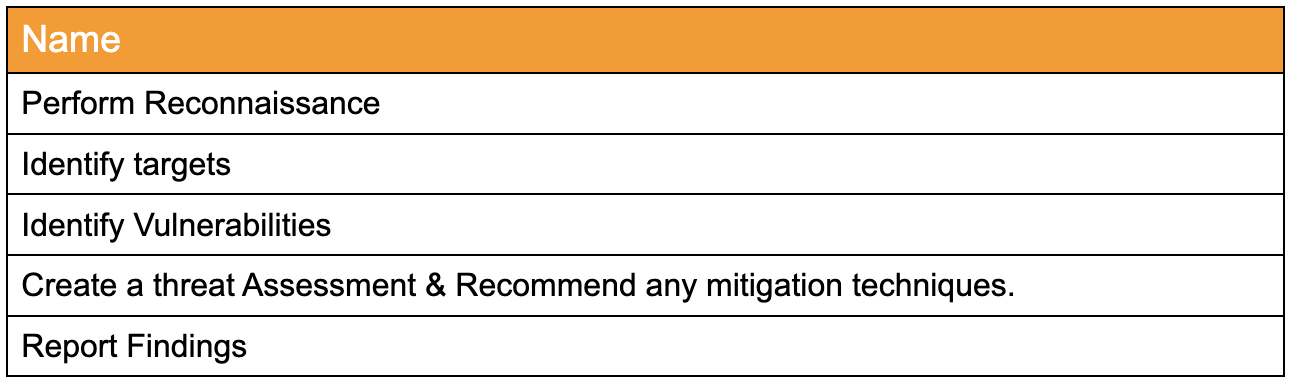
[**Executive Summary 11**](#_u666pqjrgkot)

# **Scope of Work**

Long Trang Corp. has been tasked with conducting a comprehensive penetration testing process to identify both internal and external vulnerabilities of the organization. The testing will be conducted in five phases: Reconnaissance, Target Identification, Vulnerability Identification, and Risk Assessment. Long Trang Corp. is expected to create a detailed report that outlines the network architecture of Artemis, including servers, databases, cloud environments, and configurations. The report must also prioritize the risks facing the organization and provide a threat assessment that ranks the vulnerabilities by severity. In addition, technical remediation steps for the IT department must be included in the report. An Executive Summary for Senior Management should also be provided.

# **Project Objectives**

Artemis employs a range of security vendors and technologies, such as Cisco, Fortinet, and Palo Alto for firewall, F5 Big IP for load balancing, and Zscaler for secure remote application access. The organization operates a combination of on-premise and cloud (AWS) assets that are distributed across four data centers situated in Houston, Paris, Cairo, and Singapore. While the network is currently being transitioned to SD-WAN, some MPLS links are still in use, particularly in remote locations. To reduce costs, outdated Cisco equipment is being replaced with Fortinet's Fortigate devices, which may also result in the elimination of remaining Cisco gear. The primary objective of the penetration test is to identify security weaknesses in the network, system, or software. Once the vulnerabilities are identified, they can be remediated or mitigated to reduce the chances of threat actors discovering them, which ultimately enhances the security posture of the company.

Our security firm has been engaged by ARTEMIS INC to conduct an external penetration test on their organization. The test will be conducted in five distinct phases to ensure that the final report provided to ARTEMIS is comprehensive and accurate. These five phases are outlined as follows:

Upon completion of the aforementioned phases, our firm will have a comprehensive understanding of the potential threats facing the organization and the level of risk they may pose. We will be able to accurately identify all vulnerabilities present within the system and provide recommended solutions that the organization can implement to effectively mitigate these threats.

In order to identify potential threats within the infrastructure of ARTEMIS INC, our firm will be conducting tests on the following components within the organization:

* Internal Network
* Internal Web Application
* Internal Systems i.e (WorkStations, Servers, Databases)
* Devices

# **Assumptions**

In the context of a penetration test, the existence of a security boundary is presupposed as the objective of such a test is to overcome it. The security boundary serves to separate the internal components of the security target from external entities, including the outside world, through the implementation of various security measures. Long Trang Corp. has posited the following scenarios as part of their penetration testing methodology:

* Scenario 1: Unpatched RDP is exposed to the internet
* Scenario 2: Web application is vulnerable to SQL Injection
* Scenario 3: Default password on Cisco admin portal
* Scenario 4: Apache web server vulnerable to CVE-2019-0211
* Scenario 5: Web server is exposing sensitive data
* Scenario 6: Web application has broken access control
* Scenario 7: Oracle WebLogic Server vulnerable to CVE-2020-14882
* Scenario 8: Misconfigured cloud storage (AWS security group misconfiguration, lack of
* access restrictions)
* Scenario 9: Microsoft Exchange Server vulnerable to CVE-2021-26855

# **Timeline**

The testing phase is scheduled to last for a duration of two months, commencing from March 22, 2023, and concluding on May 23, 2023. Throughout this period, the organization will be subjected to a simulated attack, with the aim of uncovering potential vulnerabilities within its network infrastructure. Please note that our firm cannot be held accountable for any incidents that occur outside the aforementioned time frame.

# **Summary of Findings**

Here is an overview of the vulnerabilities detected, classified according to their impact severity as Critical, High, Medium, or Low. A total of four Critical and five High severity vulnerabilities have been identified, and immediate remedial action is required within the next 30 days. These vulnerabilities have helped to uncover shortcomings in the organization's controls and in the implementation of measures such as Patch Management, Secure Access Configuration, and the Identity/Classification and Protection of Sensitive Data. A Technical Threat Assessment containing details such as CVSS scores, vulnerability definitions, and associated risks has been included in the Threat Assessment Table on page 27 for the reference of IT personnel. We recommend that IT and security personnel review all the 'Defense in Depth' comments provided for each vulnerability to obtain a comprehensive understanding of the optimal security posture.

1. Unpatched RDP is exposed to the internet - Critical

A system that has not been updated with the latest Remote Desktop Protocol (RDP) patches presents a significant security risk. Furthermore, if users have a tendency to reuse passwords, the risk factor increases as it increases the probability of cyber attackers gaining access to the password in the event that they manage to breach another website and obtain a password list.

1. Web application is vulnerable to SQL Injection - Critical

SQL injection vulnerabilities are primarily caused by a combination of code and data in a dynamic SQL statement, improper input validation, and the disclosure of error information. These weaknesses expose an organization's sensitive information to unauthorized access and pose a significant risk of severe damage to the system by malicious actors.

1. Default password on Cisco admin portal - Medium

When the default password for a device is persistently utilized on the Cisco admin portal without being updated, both the device and its data are susceptible to security breaches. This presents an opportunity for hackers to infiltrate the device and access its data. If the device is linked to a company network, the security risk becomes more significant, affecting the entire organization. This vulnerability is frequently caused by employee negligence, such as falling prey to phishing emails or having inadequate security awareness.

1. Apache web server vulnerable to CVE-2019-0211 - High

The vulnerability detected in Apache poses a substantial risk to both the device and data as it facilitates several attacks, including lateral movement and escalation of privileges. The flaw permits a worker process to modify its privileges during server resets, thereby enabling a person with a local account to execute commands with root clearance. Consequently, rogue server scripts can run arbitrary code with root privileges, thereby granting complete control of the target machine to the attacker. The vulnerability was discovered due to a flaw in the system that allowed code running on a child process with lower privileges to execute arbitrary code with the authority of the parent process. This vulnerability could enable a cyber attacker with web server access to execute arbitrary scripts, such as PHP or CGI, with root privileges.

1. Web server is exposing sensitive data - High

Failure to protect sensitive data hosted on a web server can result in grave repercussions for a company, including damage to its reputation and financial standing. The potential loss of confidential information, such as healthcare records, personal data, login credentials, and financial details, can also lead to legal implications. Such vulnerability may arise due to online application weaknesses that allow unauthorized data access or from phishing scams, wherein cybercriminals deceive unsuspecting individuals into disclosing sensitive information.

1. Web application has broken access control - High

Attackers can exploit vulnerabilities to circumvent regular security protocols, gaining unauthorized access to sensitive information or systems. The consequences of such breaches include the potential for criminals to exploit sensitive data for fraudulent purposes or identity theft, damage to an organization's reputation, and financial losses. Additionally, organizations may face fines or other penalties if their access controls are inadequate and fail to meet regulatory requirements. Furthermore, insufficient access controls can also cause operational disruptions, with critical systems being damaged or disabled by attackers, leading to prolonged downtime and further financial losses. Other security concerns include injection flaws, cross-site scripting vulnerabilities, and flawed authentication and session management.

1. Oracle WebLogic Server vulnerable to CVE-2020-14882 - Critical

The identified exploit enables an attacker to execute Remote Code Execution (RCE) on a susceptible Oracle WebLogic Server through an HTTP GET request. The vulnerability lies in the Oracle Fusion Middleware Console subcomponent, thereby affecting the installed version of the Oracle WebLogic Server on the target system.

1. Misconfigured cloud storage (AWS security group misconfiguration, lack of access restrictions) - Critical

Misconfiguration of cloud storage can result in security breaches, as external hackers and internal threats can exploit vulnerabilities to gain access to the network. Such risks include cyberattacks, ransomware, and malware. The underlying causes of misconfiguration are diverse, including a limited comprehension of cloud security and policies, inadequate controls and oversight, negligent behavior by insiders, and the complexity of managing multiple cloud Application Programming Interfaces (APIs) and interfaces.

1. Microsoft Exchange Server vulnerable to CVE-2021-26855 - High

By sending a meticulously constructed HTTP request, the attacker can impersonate the Exchange server, leading to unauthorized access. The resulting exploit creates a web shell, which acts as a backdoor, facilitating remote access to the system. This access allows the attacker to execute malicious commands, obtain user credentials, and launch ransomware attacks, resulting in substantial harm.

# **Recommendations**

The findings we have uncovered have the potential to cause significant harm to the organization's information technology infrastructure and overall operations. To address this, we have suggested a range of mitigation solutions that the ARTEMIS security team can swiftly implement. Below are the following recommendations for Artemis’ threat assessments:

1. To mitigate the risk associated with the vulnerability of unpatched Remote Desktop Protocol (RDP) that is exposed to the internet, the company is taking several measures to bolster its network security. These measures include the implementation of a Single Sign-On (SSO) system, which will simplify access to multiple applications while guaranteeing secure authentication. Moreover, the company is adopting password management and enforcement policies to enhance the security of access to sensitive data. Stringent firewall rules are also being enforced to restrict unauthorized network access, and port 3389 is being locked down to avert any unauthorized remote access.
2. The following recommendations are proposed to address the vulnerability of web applications susceptible to SQL injection. Firstly, staff training should continue and be reinforced to maintain awareness of the associated risks and encourage the adoption of best practices. Secondly, the company's approach of treating all user input as untrusted and implementing strict whitelists to filter and verify it is effective and should be maintained. Thirdly, prioritizing regular system updates and adoption of the latest technologies is critical to preempting potential security threats. Fourthly, using parameterized queries or stored procedures instead of developing SQL injection protection from scratch is recommended. Lastly, regular scans of web applications using a web vulnerability scanner like Acunetix should be performed to identify and mitigate any potential security vulnerabilities. By implementing these measures, the company can demonstrate its commitment to safeguarding its systems and data.
3. To mitigate the vulnerability associated with having a default password on the Cisco admin portal, the following steps are advised. Firstly, employee education should focus on implementing password guidelines that mandate the use of unique and alpha-numeric passwords, with a minimum length of 24 characters. Secondly, Multi Factor Authentication (MFA) should be added to existing password-based security systems. Lastly, periodic updates to password setups and checks to verify their proper operation should be performed. Through the implementation of these proactive measures, the organization can reinforce the security and safeguarding of its sensitive information.
4. To mitigate the vulnerability of the Apache web server, which is susceptible to CVE-2019-0211, we suggest updating to Apache httpd version 2.4.39 or a more recent version, a task that falls under the purview of server administrators. Additionally, we propose implementing the principle of "least privilege" by Apache developers, programmers, and system administrators. These measures will effectively address the vulnerability and prevent any malicious actors from exploiting any associated weaknesses.
5. To mitigate the vulnerability of sensitive data being exposed by web servers, it is recommended to implement the following measures: encryption of all sensitive data during usage and storage, avoiding the storage of private information, utilization of strong standard algorithms, keys, and effective key management, password-specific protection algorithm for storing passwords, and disabling the autocomplete feature for forms that collect sensitive information while also disabling caching for pages that contain sensitive data. By adhering to these guidelines, sensitive information can be effectively secured.
6. To address the vulnerability of a web application that has broken access control, it is recommended to implement the following measures: conducting regular inspections and tests to detect any anomalies, adopting a policy of denying access by default to all users, providing role-based access control to allow access only to authorized personnel, implementing permission-based access control to regulate access to specific resources, and enabling mandatory access control to enhance the security of access control systems. By adhering to these best practices, the web application can maintain robust access control systems and prevent unauthorized access.
7. To mitigate the vulnerability of Oracle WebLogic Server susceptible to CVE-2020-14882, it is recommended to implement the following measures: restrict access to the admin portal from the public internet, monitor network traffic for any unusual HTTP requests, and monitor the application for any suspicious processes, such as cmd.exe or /bin/sh. Moreover, as an interim measure, it is advisable to block access to the admin portal (default TCP port 7001) until the vulnerability is adequately addressed. By adopting these actions, we can minimize the probability of security breaches and safeguard sensitive data.
8. To mitigate the vulnerability associated with misconfigured cloud storage, such as AWS security group misconfiguration and lack of access restrictions, the following recommendations should be implemented: establish comprehensive logging practices, enable encryption to secure sensitive data, regularly check permissions to ensure they are properly configured, conduct frequent audits to identify misconfigurations, establish strong security policies and communicate them effectively, and finally, adopt an automated remediation solution to monitor and promptly alert for any misconfiguration issues. These measures will effectively address the vulnerability and ensure the security and protection of sensitive data in cloud storage.
9. To address the vulnerability of Microsoft Exchange Server exposed to CVE-2021-26855, the following measures are recommended: implementing an IIS Re-Write Rule to filter fraudulent HTTPS requests, deactivating Offline Address Book, VDir, Exchange Control Panel (ECP), and Unified Messaging (UM) through the execution of the ExchangeMitigation.ps1 script, and implementing backend cookie mitigation to filter out harmful X-AnonResource-Backend and X-BEResource cookies from HTTPS requests, which can prevent SSRF attacks. By following these recommendations, we can effectively address the vulnerability and safeguard sensitive information.