**Artemis Penetration Testing Report**

Tanvir Ahmed

**Table of Content**

[**1. Introduction 3**](#_8x5h3qqwstla)

[**2. Scope of Work 3**](#_r1tk80obq8bg)

[**3. Project Objectives 3**](#_x8q4gf8u8782)

[**4. Assumptions 3**](#_ntso3mymz43b)

[**5. Timeline 4**](#_9xd4uz9ro1jm)

[5.2 Phase 2 : Target Scanning 4](#_g9eamd5l9cq4)

[5.3 Phase 3 : Vulnerability Scanning 4](#_yc2h0tomty5y)

[5.4 Phase 4: Vulnerability Assessment 5](#_h6p61f7t65mb)

[**6. Summary of Findings 5**](#_l5ebd6i5v2pp)

[**7. Recommendations 6**](#_h5z4q76c66m5)

[**8. Methodology 6**](#_354x1uvlhygv)

[**9. References 7**](#_7pgp6r4njzzk)

## **1. Introduction**

Penetration testing is what helps an organization operate efficiently and strengths their security posture by identifying vulnerabilities within the network. Artemis, a natural gas company serving 1.7 million customers, has an obligation to safeguard both its internal and external network while ensuring the protection of customer information. In order to maintain network integrity and comply with industry standard security practices, regular penetration testing is essential. For this purpose, Artemis comminsed a cybersecurity firm to conduct a comprehensive assessment. The focus was to evaluate the current state of network identity, risk, and provide actionable recommendations.

The assessment was carried out in multiple stages using standard tools and techniques to uncover weaknesses in the network. This report provides an in-depth analysis of each phase, including reconnaissance, target scanning, vulnerability scanning, threat assessment and recommendations to mitigate threat vectors and exposure.

## **2. Scope of Work**

Artemis is a large enterprise operating across several technological domains including web applications, internal network, and cloud infrastructures. The penetration testing focused on evaluating the organization’s network security, including employee and customer facing web applications. Cloud storage and API endpoints were included as part of the cloud infrastructure assessment.

Excluded from the testing were physical security components and personal devices of employees and customers not connected to the Artemis network. With Artemis permission all the testing was completed successfully. The assessment spanned two weeks and employed tools aligned with industry standards such as Security Methodology Testing Manual (OSSTMM) with OWASP testing guide. The testing type was grey box testing, incorporating prior knowledge of Artemis systems such as outdated softwares, unpatches services, SD WAN transition details, tools and repository system.

## **3. Project Objectives**

The objective was to explore Artemis network and apply cybersecurity methodologies to identify vulnerabilities that could be exploitable by attackers. Each vulnerability was assessed based on severity, risk and potential and remediation strategies. Recommendations were designed to be practical for future maintenance goals and enhancement of security.

## **4. Assumptions**

All the testing was performed keeping real world seniors in the production environment. Artemis provided valid credentials and services needed to assess the environment. The testing did not hinder the workflow, business operation continued without disruption. Testing tools were chosen by the firm, following industry standard penetration strategy and procedure. Artemis were in the transition phase to certain services hence they already maintained full backups, enabling safe testing and assessment without worrying about data loss.

## **5. Timeline**

The penetration testing was completed in four structured phases:

### **5.1 Phase 1 : Reconnaissance**

The goal was to gather intelligence from open sources (OSINT) and create a profile on Artemis including email addresses, phone numbers and other details.

Tools used in this recon included:

* **Scrapedln**: Linkedin data scraping including name, occupation location, industry and profile url.
* **Osintgram**: Analyze posts, hashtags, and tagged emails
* **Twint** to scrape Twitter for work culture behavior, hashtags and keywords specific searches on anything that indicates the company’s operations and vulnerabilities.
* **Facebook** for more behavior insights.
* **Search Engines**: Public reports and press releases
* **Maltego:** Infrastructure mapping with other public entities
* [**AnnualReport.com**](http://annualreport.com) **and Crunchbase**: Company structure and financial data including business growth model, and investments time
* **Wireshark**: Capture HTTP, TCP, FTP traffic
* **DNS History**: Subdomain enumeration and DNS records
* **HaveIBeenPawned & IntelX**: Identified leaked data including DOB, emails, passwords

Initial recon helped to profile Artemis with a variety of information and knowledge to drive forward for the next phase. It also gave insight on the company's culture and data exposed because of a lack of security in the Artemis network.

### **5.2 Phase 2 : Target Scanning**

In this phase the object was to scan the target, identify open ports, services, and version details.

Tool used:

* **Nmap**: It is a command line scanning tool with command “nmap -sV -sC [www.artmeis.com](http://www.artmeis.com) -p 21” is incorporated to check for open ports.
* **Zenmap**: GUI environment for customizable scanning that enhances nmap command allowing for better optimizing for TCP, UDP and port ranges. Required a great amount of time for multiple scanning.
* **Armitage**: GUI environment that utilizes metasploit with command “db\_nmap” is used.
* **Telent:** A command line interface used to connect host computers mimicking physical files.

### **5.3 Phase 3 : Vulnerability Scanning**

The purpose of this phase was to do more in depth scanning to Identify flaws and match to known CVEs.

* OpenVAS, Zenmap Metasploit, Wapiti and Burp Suite was used to detect vulnerability including XSS, SQLi and CSRF and command line injections.
* **Zenmap and Metasploit** both were used to do manual checking of CVEs.
* **OpenVAS**: GUI interface in web application environment that was customized for many scanning and shows CPE inventory and showcases areas of vulnerability like OS fingerprinting.
* **Nessus:** Tenable Nessus detected CVEs and weaknesses in the system with links to remediating such vulnerability.
* **Burp Suite**: It detected CVEs and vulnerability by intercepting HTTP traffic for inspection through its browser. With automation detection it was easy to detect the CVEs.
* **Wapiti:** Can detect open redirect, XSS, XRF, SQL injection, by intercepting HTTP traffic.

### **5.4 Phase 4: Vulnerability Assessment**

Assessed risk based on severity, exploitability, and impact. Applied OWASP and CVSS scoring for vulnerabilities scenarios. Key finding includes:

* Unpatched RDP
* SQL Injection weakness
* Cisco default credentials
* Apache CVE-2019-0211
* Broken Access Control
* Web server exposed data
* Oracle WebLogic RCE (CVE-2020-14882)
* Misconfigured AWS cloud storage
* Microsoft Exchange Server CVE-2021-26855

## **6. Summary of Findings**

The penetration testing revealed 5 critical and 4 high risk vulnerabilities in the Artemis network. Notable issue:

* **Outdated RDP**: Risk of lateral movement by brute force attack and unauthorized access to sensitive systems like the Apollo repository. Potential risk of man in the middle attack and deployment of malware, compromising the system.
* **SQL Injection**: Risk of attacker gaining read / write access and manipulating records, even exfiltrating Apollo systems revealing business critical data.
* **Default Cisco Credentials**: Easy brute force access into the network leading to stealing sensitive data.
* **Apache Web Server CVE-2019-0211:** Risk of root privilege and gaining full control over the system and Apollo system.
* **Web server exposed data:** Leakage of customer and employee data allowing attackers to misuse services using leaked data.
* **Broke access control:** Unauthorized manipulation of resources by easily accessing admin url. Attackers can post, delete and alter claims without validation from the server.
* **Oracle WebLogic RCE:** Risk of ransomware deployment, giving attackers access to the server to exfiltrate data.
* **AWS Misconfiguration:** Possible exposure of customer bank credentials SSN, phone number, and email, that can later be sold in black market for money or illegal activity. The data breach can impact CIA triad and eventually losing PCI DSS and GDPR compliances.
* **Microsoft Exchange Server:** Access to full mailbox with user IP addresses and privilege escalation. Ability to run arbitrary code to gain administrator access.

## **7. Recommendations**

To mitigate the vulnerabilities found in the assessment:

* Immediately patch all outdated services, especially for RDP and Apache
* Implementing network segmentation to limit lateral movement to prevent attackers from getting full control over the network.
* Hardening IAM policies to apply least privilege principles.
* Restrict public access to cloud storage
* Not storing sensitive data in web root
* Enable MFA on all admin panels to restrict other users from gaining administrator privilege
* Implementing VPN access for internal tools and for secure connection
* Better policy for continuous monitoring for vulnerabilities and maintaining logs for changes in cloud services and failed attempt alert to admin.
* Train developers on secure coding practices
* Regular vulnerability scans and penetration testing.
* Separate Exchange Server from internet facing system

## **8. Methodology**

For CVSS Score CVSS score metric was used with 3 categories, basic, temporal and environmental.

## 

## **9. References**

Acunetix. (n.d.). *What is SQL injection (SQLi) and how to prevent it*.<https://www.acunetix.com/websitesecurity/sql-injection/>

Apache Software Foundation. (2024). *Apache HTTP Server 2.4 vulnerabilities*.<https://httpd.apache.org/security/vulnerabilities_24.html#:~:text=(CVE-2024-38475),execution%20or%20source%20code%20disclosure>

Cisco. (2011, June 1). *Cisco Network Registrar Denial of Service Vulnerability*. Cisco Security Advisories.<https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-20110601-cnr.html>

Cloudflare. (n.d.). *RDP security risks*.<https://www.cloudflare.com/learning/access-management/rdp-security-risks/>

Cybersecurity & Infrastructure Security Agency. (2021, March 3). *AA21-062A: Mitigate Microsoft Exchange Server vulnerabilities*. CISA.<https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-062a>

Fortect. (n.d.). *Remote Desktop Protocol (RDP): Risks and how to protect your Windows PC*.<https://www.fortect.com/how-to-guides/remote-desktop-protocol-risks-and-how-to-protect-your-windows-pc/#:~:text=Risks%20of%20Remote%20Desktop%20Protocol,unauthorized%20access%20to%20your%20system>

Imperva. (2020, November 4). *Bug hunting for a quick buck using WebLogic vulnerability CVE-2020-14882*.<https://www.imperva.com/blog/bug-hunting-for-a-quick-buck-using-weblogic-vulnerability-cve-2020-14882/>

Red Hat. (2019). *CVE-2019-0211 - Apache HTTP Server privilege escalation vulnerability*. Red Hat Customer Portal.<https://access.redhat.com/security/cve/cve-2019-0211>

Tenable. (2020, November 2). *CVE-2020-14882: Oracle WebLogic remote code execution vulnerability exploited in the wild*.<https://www.tenable.com/blog/cve-2020-14882-oracle-weblogic-remote-code-execution-vulnerability-exploited-in-the-wild>

Tenable. (n.d.). *Apache HTTP Server < 2.0.55 mod\_imap Arbitrary File Disclosure*.<https://www.tenable.com/plugins/nessus/23938>

Trend Micro. (2019, April 4). *CVE-2019-0211 patched: Apache HTTP Server root privilege escalation flaw a priority for web hosting providers*.<https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/cve-2019-0211-patched-apache-http-server-root-privilege-escalation-flaw-a-priority-for-web-hosting-providers>