Group 2: Phase 1 Report

Lockwood Topping, Eric Chapman, Tre Germany, Joseph Daher, & Manasa Mutpur
Department of Cybersecurity, Kennesaw State University
CYBR 7910: Capstone in Cybersecurity Practicum
Dr. Zhigang Li
November 4, 2024

Project Status Update

Since the project plan submission, members of Group 2 have made significant strides in familiarizing themselves with the Akwaaba virtual machine (VM) environment. Each member has successfully connected to the VM, allowing for group-wide engagement and exploration of the project during our bi-weekly meetings. Following concerted collaborative efforts, Group 2 has constructed a comprehensive information security policy for Akwaaba, conducted a thorough risk assessment to identify potential threats, and drafted a technical plan to outline the security measures that will implement on the Akwaaba VM. To further prepare for future phases of the project, the team has also diligently researched and tested known exploits relevant to the system and vulnerabilities that may be present within the Red Hat server, Apache service, WordPress platform, MariaDB, and SSH services.

In terms of project management, Group 2 has made some adjustments to the project plan to accommodate challenges uncovered during our research. Specifically, we have allocated additional time for the vulnerability testing and subsequent hardening of the VM that are needed to enhance Akwaaba's overall security posture, as the initial allotment of time given to those areas looks to be insufficient. However, due to the efficient teamwork used in creating the information security and risk assessment documents, Group 2 has been able to reallocate time from the document-writing tasks to cover the additional time needed for the penetration testing tasks. Additionally, smaller group chats and separate Microsoft Teams meetings have been utilized as needed to facilitate effective collaboration between team members working on a specific task or subtask together. And finally, due to the number of tasks required of the team in the final two weeks of the project, the Group 2 presentation lead has begun work on proactively creating the structure for the final presentation to alleviate strain on the group during the final two weeks of the project.

Information Security Policy

1. Purpose & Scope

This policy establishes guidelines for protecting Akwaaba's sensitive information, systems, and resources. It applies to all employees, contractors, vendors, and third parties accessing Akwaaba's systems, networks, and data, ensuring confidentiality, integrity, and availability of information assets while guarding against unauthorized access, breaches, and threats.

2. Information Classification

Akwaaba's data is categorized based on sensitivity:

- **Confidential**: Highly sensitive information (e.g., payment details, HR records) requiring restricted access and encryption.
- **Internal Use Only**: Business-critical data requiring role-based access control (RBAC) and encryption when transmitted externally.
- **Public**: Non-sensitive information that may be shared after review.

Handling Procedures:

- **Confidential**: Encrypted at rest and in transit; access limited to authorized personnel.
- **Internal Use Only**: RBAC controls access, and external transmissions are encrypted.
- **Public**: Reviewed before release; no special handling required.

3. Access Control

- **User Authentication**: Access requires strong passwords, biometrics, and/or multi-factor authentication (MFA) on approved devices.
- **RBAC**: Access is role-based, limited to the data and systems necessary for job functions. Periodic audits ensure adherence to the least-privilege principle.
- **Conditional Access Policies**: Only pre-approved devices may access systems, and untrusted connections are blocked.

4. Access Management Policy

Access permissions are role-specific to maintain security across Akwaaba's two restaurant locations and headquarters. Defined access includes:

- **Hosts, Waitstaff, Cooks, and Bartenders**
  - *Resource Access*: Point-of-Sale (POS) systems for order processing, limited to shift hours.
  - *Restrictions*: No access to sensitive financial, HR, or managerial systems.
- **General Managers**
  - *Resource Access*: POS systems, employee scheduling software, and inventory management. Limited financial reporting access for daily reconciliation.
  - *Restrictions*: No access to sensitive HR or payroll information.
- **Accountant**
  - *Resource Access*: Full access to financial records, payroll, and vendor payment systems.
  - *Restrictions*: No access to HR records, employee scheduling data, POS, or operational systems.
- **Owner**

    - *Resource Access*: Access to all systems, including financials, HR records, POS data, and inventory management for oversight and audit purposes.
    - *Restrictions*: None.
- **HR Personnel**
    - *Resource Access*: Full access to employee records, payroll systems, and HR management systems.
    - *Restrictions*: No access to financial systems or POS data.
- **Web Developer**
    - *Resource Access*: Full access to website infrastructure, e-commerce data, and content management systems.
    - *Restrictions*: No access to POS systems, HR, or payroll data.

5. Remote Access
All remote access occurs through a secure Virtual Private Network (VPN). Mobile Device Management (MDM) policies require up-to-date antivirus, firewalls, and encryption. Public Wi-Fi is prohibited without VPN.

6. Password Management

- **Requirements**: Passwords are at least ten characters with varied complexity.
- **Two-Factor Authentication**: Required for critical systems.
- **Change Policy**: Password changes occur only after known compromise or risk assessment.

7. Acceptable Use of Office Computing Technology

- **Device Use**: Only company-provided devices access sensitive systems.
- **Software**: Installation of unauthorized software or external storage access is prohibited.
- **Email Use**: Official communication occurs via company-approved systems; personal email use for business matters is disallowed.
- **Social Media and Malware Prevention**: Access to social media and sites known for malware is restricted; suspicious activity must be reported to IT.

8. Bring Your Own Device (BYOD)
Personal devices may not access Akwaaba's network unless enrolled in the BYOD program, which includes MDM compliance for antivirus and encryption.

9. Data Protection & Encryption

- **Encryption Policy**: Sensitive data is encrypted at rest and in transit; encryption keys are managed centrally.
- **Email Encryption**: External communications of sensitive data are encrypted with company-approved tools.
- **Backup and Disaster Recovery**: Secure, encrypted backups support quick restoration.

Risk Assessment

1. Overall Evaluation of the Server Infrastructure

Akwaaba's e-commerce platform operates within a structured server infrastructure with Apache 2.4.37 as the web server, MariaDB 10.6.4 for database management, and WordPress as the website interface, all running on Red Hat OS 8.4. While this infrastructure supports robust operations, each component must be monitored, maintained, and regularly updated to mitigate evolving security threats. Comprehensive configuration management is essential to ensure each service remains secure and functional.

2. Important Assets to Protect

Akwaaba's assets comprise both digital and human components critical to business continuity and data protection.

- **Digital Assets**:
  - **Linux Server (Red Hat OS)**: Centralized control for the web server, database server, and web content management system.
  - **Web Server (Apache)**: The outward-facing server for Akwaaba's online presence, essential for customer interaction and business transactions.
  - **Database Server (MariaDB)**: Provides WordPress with data storage and retrieval, query handling, and security and role-based access control
  - **Web Content Management System (WordPress)**: a web content management system (CMS) that is responsible for the creation and management of the Akwaaba web site.
  - **Customer Data**: Personally identifiable information (PII) and payment data require secure storage and access control policies.
  - **Employee Data**: Sensitive HR and payroll data necessitate restricted access to prevent identity theft or internal fraud.
- **Human Assets**:
  - **Web Developer**: Responsible for platform security and functionality.
  - **IT Staff**: Tasked with maintenance, updates, and implementation of security protocols.
  - **General Employees**: General staff who handle customer data and follow organizational security policies to protect information.

3. Potential Threats and Vulnerabilities

Assets	Threats/Risks	Possibility of Successful Compromise	Damage if Asset Compromised
Linux Server (Red Hat OS)	Exploitation of unpatched vulnerabilities, unauthorized root access, SSH attack	Medium	Loss of server control, potential malware spread, data and credential theft, impact on other network assets

Assets	Threats/Risks	Possibility of Successful Compromise	Damage if Asset Compromised
Web Server (Apache)	Denial of Service (DoS), misconfigurations	Medium	Loss of website access, revenue loss, damage to company reputation
Database (MariaDB)	SQL injection, unauthorized access	High	Data breach affecting customer/employee and web site data, financial and legal repercussions
Web Content Management System (WP)	Exploitation of outdated plugins, admin credentials	High	Website defacement, data breach, operational downtime, revenue loss
Customer Data	Data theft, misuse of sensitive information	High	Identity theft, fraud, loss of customer trust, potential lawsuits
Employee Data	Unauthorized access to payroll and HR information	Medium	Financial and identity theft, risk of lawsuits from employees
Human Assets (IT, Web Dev)	Social engineering, insider threats	Low	Potential leaks of sensitive data, impact on system security

4. Probability of Major Attacks Happening

Each asset's probability of compromise varies based on inherent risks and current security posture.

- **Linux Server (Red Hat OS)**: Moderate risk if critical patches are delayed or root access is insufficiently protected.
- **Web Server (Apache)**: Moderate likelihood, as misconfigurations or exposure to DoS attacks could lead to disruptions.
- **Database (MariaDB)**: High likelihood due to the potential for SQL injection vulnerabilities if input sanitization is lacking.
- **Web Content Management System (WordPress)**: High likelihood, due to potential exploitation of outdated plugins and admin account vulnerabilities.
- **Customer Data**: High risk, particularly if database controls are weak or system vulnerabilities are exploited.
- **Employee Data**: Medium risk of unauthorized access, particularly through weak internal controls.
- **Web Developer**: Moderate likelihood of social engineering attacks targeting code access or improper permissions.
- **IT Staff**: Moderate risk of insider threats, especially if security procedures are not strictly enforced.
- **General Employees**: Low risk, with social engineering or phishing posing the main threats if security awareness training is inadequate.

Technical Plan

1. Overview of the Technical Infrastructure

Akwaaba is a Caribbean-inspired steakhouse with locations in New York City, Atlanta, and Los Angeles. The restaurant is operational during lunch and dinner, with a staff of approximately 60 employees spread across multiple roles such as cooks, waiters, bartenders, managers, and administrative staff. Akwaaba's server infrastructure supports these operations through:

- **Server**: A Red Hat OS 8.4 environment hosting Apache 2.4.37 as the web server, MariaDB 10.6.4 for database management, and WordPress 5.8.1 as the content management system (CMS).
- **Access and Ports**: Ports 22 (SSH), 80 (HTTP), and 443 (HTTPS) are open and used for secure remote management, forwarding to HTTPS, and providing secure web services respectively.
- **Database**: The MariaDB instance provides WordPress with data storage and retrieval, query handling, and security and role-based access control.

2. High-Level Security Strategies

To improve the overall security and management of Akwaaba's technical infrastructure, the following strategies will be implemented:

2.1. Restrict Administrative Privileges

One key issue with the current setup is the overuse of administrative accounts. Reducing the use of root and admin-level accounts across the infrastructure will lower the risk of privilege escalation during an attack. We will:

- Disable root SSH access and enforce the principle of least privilege.
- Assign non-admin accounts to MariaDB and WordPress for day-to-day operations.

2.2. Upgrade System and Software

Outdated software can expose vulnerabilities. To protect the system from known exploits, we will:

- Regularly update Red Hat OS, Apache, MariaDB, and WordPress to the latest stable versions.
- Install security patches as they are released, tested, and stable.

2.3. Strengthen Access and Authentication

SSH access should be secured by disabling password-based login and requiring key-based authentication. Access should be restricted to trusted IP addresses, and two-factor authentication (2FA) will be required for sensitive accounts.

2.4. Enhance Network Security

To reduce the attack surface, we will enhance the firewall configuration and enforce strict access control. Additionally, implementing an Intrusion Detection System (IDS) will help monitor network activity and detect potential security breaches early.

2.5. Backup and Disaster Recovery

To ensure that Akwaaba's infrastructure can quickly recover from failures or attacks, we will implement an automated backup system that stores regular snapshots of server configurations, databases, and website content. These backups will be tested regularly for integrity.

2.6. Logging and Monitoring

Centralized logging and monitoring will be implemented to track server activities, detect suspicious behavior, and provide forensic data in the event of a breach. Logs will be retained and reviewed regularly to maintain compliance and security.

3. Specific Technologies to Support the Strategies

3.1. Reducing Administrative Privileges

MariaDB Role-Based Access Control (RBAC)

MariaDB's built-in role-based access control (RBAC) features will be used to assign specific permissions to users based on their roles. For WordPress, we will create a dedicated non-admin database user with only the necessary privileges to manage database queries without accessing system-level settings.

- Why this technology? MariaDB's RBAC is a native feature that simplifies the creation and management of different privilege levels for users. It enhances security by limiting access to sensitive functions.

3.2. Software and System Updates

Cockpit for Automated Updates

To manage software and system updates, we will use Cockpit, a free and user-friendly, web-based interface included with Red Hat Enterprise Linux. Cockpit allows for streamlined system administration, including package updates, monitoring, and troubleshooting, all from a browser-based dashboard.

- Why this technology? Cockpit is ideal for small to medium-sized environments like Akwaaba's, where centralized management tools like Red Hat Satellite may be unnecessary. It is lightweight, requires minimal configuration, and allows administrators to easily monitor and apply updates to the system without needing complex scripting or external tools.

3.3. SSH Hardening and Access Control

Fail2Ban for SSH Security

To harden SSH access and protect against brute force attacks, we will implement Fail2Ban, a lightweight intrusion prevention tool that enhances SSH security by monitoring log files and banning IP addresses that show suspicious behavior, such as repeated failed login attempts. This approach is straightforward and avoids the complexity of managing SSH key-based authentication while still significantly improving security.

- Why this technology? Fail2Ban is easy to set up and does not require major changes to the existing authentication process. It works by dynamically blocking malicious IP addresses at the firewall level, preventing repeated login attempts without affecting legitimate users.

3.4. Network Security and Intrusion Detection

firewalld and Snort (IDS)

The built-in firewalld tool on Red Hat will be used to enhance firewall rules, allowing only necessary traffic on specific ports. We will also deploy Snort, a powerful open-source IDS, to monitor incoming and outgoing traffic for suspicious activity and alert administrators in case of potential intrusions.

- Why this technology? firewalld is native to Red Hat and provides fine-grained control over network traffic. Snort is a robust, industry-standard IDS that can detect network anomalies, helping to prevent attacks before they escalate.

3.5. Backup and Disaster Recovery

Automated Backups using rsync and cron

To ensure the integrity and availability of Akwaaba's data, we will implement an automated backup strategy utilizing rsync combined with cron jobs. This approach allows for efficient file synchronization and backup of critical data from our server to a secure location, ensuring minimal downtime and quick recovery in the event of data loss or system failure.

- Why this technology? rsync is the most simple and efficient backup solution for single servers or small environments. And although there is no built-in scheduling feature with rsync, the native cron tool in Linux will allow for automated backups without the overhead required for other backup solutions.

3.6. Centralized Logging and Monitoring

OSSEC for Centralized Logging and Monitoring

For centralized logging and real-time monitoring, we will deploy OSSEC, an open-source Security Information and Event Management (SIEM) solutions. This tool aggregates logs from Apache, MariaDB, SSH, and other services, providing comprehensive visibility into server activities and alerting administrators when suspicious behavior is detected.

- Why this technology? OSSEC provides a robust, lightweight monitoring solution that integrates well with Red Hat servers. It allows for real-time analysis and automated alerting, which is essential for identifying and responding to security incidents