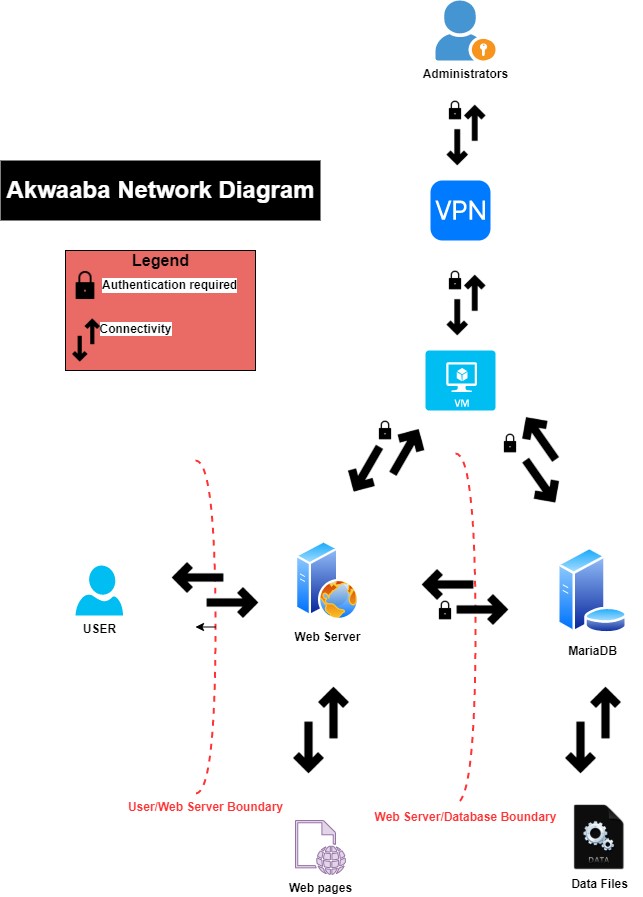
**Server Infrastructure Evaluation (Felton)**



# Infrastructure Evaluation

* The public-facing Apache web server and database are located on the same network/subnet. These two entities should be separated to prevent attacks from external threats.
* Password to web server and database is too weak; therefore, a strong password policy should be implemented.
* Web server can be potentially exploited from user/web server boundary.
* Servers, particularly the web server, are susceptible to denial-of-service (DoS) attacks.
* Data stored in database is unencrypted.
* There are vulnerabilities associated with servers and VM (Virtual Machine) operating systems that need to be addressed.
* Unsecure ports such as HTTP and telnet along with other ports are open.

## Important digital assets to protect

* Administrator account – Admin has access to all data in the Akwaaba infrastructure.
* Apache Web Server - Important asset that hosts the Akwaaba ecommerce website.
* Ecommerce website – Asset that brings revenue from customer purchases.
* MariaDB database – Contains important data from customers and employees of Akwaaba.
* Data stores on database – contains PSI of both customers and employees of Akwaaba.

## Potential known threats and vulnerabilities to each asset

* In today's world we are experiencing so many possible risks to our system in general.

This is the majority part of threats and vulnerabilities to Akwaaba company.

* Physical security violation and intrusion
* Social engineering attacks
* DoS- denial of service attacks
* Attack from insider threat

## Probability of Major Attacks per Asset

* Administrator account - Moderate probability. If the admin is properly educated and keeps all passwords secure, then they can reduce that probability. However, people are normally the weakest link in security, mistakes happen, and the account can be taken by means of physicality. This account is highly targeted because it can access the highest levels of security.
* Apache Web Server - Moderate probability. Web server is currently vulnerable to attacks from users and can lead to access to the ecommerce website, this would be valuable to attackers and should be looked at as a point of interest for security.
* Ecommerce website – High probability. If attackers can get into the web server there would be nothing stopping them from attacking the ecommerce website which grabs valuable customer data and payments.
* MariaDB database - Moderate probability. Weak passwords make it simpler for hackers to break into and whit data in the database not being encrypted it would make a great target.
* Data stored in Database – High probability, data is very valuable especially with customer information and payments. Having this data unencrypted makes it very vulnerable to attack and theft if the attackers can get access to the database.

## Damage to each asset when attacked

The risks identified have a significant impact on the direction of the business and the cause of

operation disruption, financial loss, reputation loss, and safety. The amount of damage on the digital asset determines the exposure factor (EF), which is the percentage of loss the business Akwaaba will allow as a single loss expectancy (SLE); therefore, we quantify the damage posed on each asset of the business monetary each time the attack occurred.

SLE = EF \* AV (Asset Value)

Then, we will determine the business annual loss expectancy based on the attack rate occurrence (ARO) each year.

ALE = SLE \* ARO