🔒 Security Measures Implemented

1. Network Layer Security

- Enforced a **default deny firewall policy** to block all inbound traffic except explicitly allowed ports.
- Restricted open ports to **80 (HTTP), 443 (HTTPS), and a limited use of 22 (SSH)** with strict access controls.
- Implemented **protection against SYN flood attacks** to mitigate Denial of Service (DoS) risks.

2. Application Layer Security

- Configured **Role-Based Access Control (RBAC)** with distinct Admin and User privileges to limit access.
- Used **password hashing with MD5** for stored credentials *(Note: MD5 is insecure for production; bcrypt or Argon2 are recommended for better security)*.
- Used **prepared statement** to prevent **SQL Injection and force browsing**
- Applied **secure file permissions** (`chmod 755 /var/www/mysite`) to restrict unauthorized file access.

3. Monitoring

- Enabled **real-time monitoring** of Apache services to detect availability issues promptly.
- Set up **email alerts** for service interruptions to ensure immediate response.
- Established **performance baseline tracking** for identifying anomalies and optimizing system health.

□ Lessons Learned

- The critical need for **persistent and correctly configured firewall rules** to maintain security posture.
- The **value of proactive monitoring** in identifying issues before they escalate into incidents.
- The ongoing **challenge of balancing security measures with usability**, ensuring security does not hinder legitimate access or user experience.