Cyber Security Internship – Task 14

Title: Linux Server Hardening & Secure Configuration
Platform Used: Kali Linux (UTM on macOS – Apple Silicon)

Objective

The objective of this task is to harden a Linux system by reducing its attack surface, securing access controls, configuring firewall rules, and monitoring system activity. Although Kali Linux is primarily designed for offensive security, it was intentionally used to demonstrate how a less-hardened system can be secured following best practices.

Linux Hardening Checklist

- Reviewed existing users, services, and open network ports
- Removed unused user accounts and restricted sudo access
- Disabled root login to prevent brute-force attacks
- Configured SSH with key-based authentication
- Updated all system packages
- Enabled automatic security updates
- Configured UFW firewall to restrict network traffic
- Stopped and disabled unnecessary services
- Secured file permissions for sensitive configuration files
- Reviewed authentication and system logs

Security Configuration Summary

- Root login was disabled to minimize the risk of unauthorized privileged access.
- Least privilege principle was enforced by limiting sudo access to essential users only.
- SSH was hardened by disabling password-based authentication and enforcing key-based access.
- UFW firewall was configured to deny all incoming traffic except SSH.
- Unused services were disabled to reduce the attack surface.
- Automatic security updates were enabled to ensure timely patching of vulnerabilities.
- System logs were reviewed to monitor authentication attempts and system events.

Final Outcome

After completing this task, the Linux system was significantly more secure and resilient against common attacks such as brute-force login attempts, unauthorized access, and service exploitation. This task improved practical understanding of Linux security hardening techniques used in real-world environments.