7/19/2025

KENYA POWER INDUSTRIAL ATTACHMENT GROUP REPORT

ICT SECURITY DEPARTMENT – ELECTRICITY HOUSE

REPORTING PERIOD: MAY – JULY 2025

GROUP: E-HOUSE ICT SECURITY ATTACHEES

Introduction

This report summarizes the skills and knowledge gained by the group of student attachés stationed at **Electricity House** under the **ICT Security Department** during our industrial attachment at Kenya Power and Lighting Company (KPLC). The attachment program provided immersive, hands-on exposure to modern cybersecurity tools, enterprise infrastructure, and real-world ICT operations, enabling us to grow both technically and professionally.

Departmental Placement

We were placed within the **ICT Security Department** headquartered at **Electricity House, Nairobi**, with cross-functional experiences involving the **Network Operations Center (NOC)**, the **Security Operations Center (SOC)**, and KPLC's **Data Centers**. The department specializes in protecting digital assets, managing secure IT infrastructure, and responding to threats in real-time.

Members:

FULL NAME	NATIONAL ID NUMBER	COURSE	LEVEL	TRAINING INSTITUTION	PHONE NUMBER	EMAIL
Okumu Christopher Wasonga	41399371	Applied Computer Science	Undergraduate	Daystar University	254 707390793	kokumuchris@gmail.com
Wycliff Arasa	41632546	Computer Technology	Undergraduate	Jomo Kenyatta University of Agriculture and Technology	254 743987138	arasaw88@gmail.com
Felisters Mumo	41900213	ICT	Diploma	Kabete Technical	254 748222058	felistersmumo015@gmail.com
Grace Favour	40029430	Information Security and Forensics	Undergraduate	KCA University	254 726760178	neemakibali97@gmail.com

Collective Skills and Experiences Gained

Cybersecurity Operations

- **SIEM (Security Information and Event Management):**
  - ❖ Onboarded Windows and Linux devices to FortiSIEM.
  - ❖ Analyzed logs and detected incidents like UDP port scans.
  - ❖ Gained experience using read-only SIEM dashboards for safe monitoring.
  - ❖ Learned incident escalation workflows in a tiered SOC environment.
- **Penetration Testing & Vulnerability Assessment:**
  - ❖ Conducted penetration testing on FacilityApp, MyPower App, and the Project Tracking Tool.
  - ❖ Exploited and documented XSS, CSRF, SQL injection, command injection, and broken authentication issues.
  - ❖ Used tools like Burp Suite, Postman, APKTool, and ADB for testing both web and mobile applications.
- **Threat Detection and Threat Hunting:**
  - ❖ Practiced using platforms like CyberDefenders and VirusTotal.
  - ❖ Developed incident response playbooks.
  - ❖ Understood how FortiAnalyzer detects and blocks malicious external traffic.
- **Privileged Access Management (PAM):**
  - ❖ Gained exposure to PAM controls used to manage access to critical resources.
  - ❖ Understood session tracking and access revocation mechanisms.
- **Network Access Control (NAC):**
  - ❖ Explored FortiNAC to detect rogue devices on the LAN and enforce reauthorization of IPs.
- **Firewall & IDS/IPS Exposure:**
  - ❖ Observed firewall rule configuration and the role of intrusion detection/prevention systems.
  - ❖ Studied their placement across the OSI model and impact on enterprise security posture.

Systems & Infrastructure Management

- **Data Management and Backups:**
  - ❖ Used CommVault and CommCell platforms for enterprise backup operations.
  - ❖ Learned about full, incremental, synthetic, and differential backup strategies.
  - ❖ Understood encryption, secure storage, and peer-reviewed command execution.
- **System and Network Administration:**
  - ❖ Performed user account setup and management.
  - ❖ Activated Windows OS licenses via PowerShell.
  - ❖ Installed enterprise applications like SAP, antivirus, DCF, IMS, and Outlook.
- **Data Center and Server Room Exposure:**
  - ❖ Gained access to and observed HVAC systems, UPS setups, precision cooling units, fire suppression systems, and structured cabling in live server rooms.
  - ❖ Understood the infrastructure that powers KPLC's Data Centers and disaster recovery strategies.

Project Work

- **Smart IT Resource Management System (SIRMS):**
  - ❖ Participated in both frontend and backend development of a full-stack system for asset and resource tracking.
  - ❖ Built RESTful APIs with CRUD functionality for Users, Organizations, Departments, and Assets.
  - ❖ Integrated authentication, logic validation, and multi-tenant structures in backend architecture.

Professional and Soft Skills

- **Team Collaboration:**
  - o Worked collaboratively in both technical assignments and documentation tasks.
  - o Participated in joint sessions and department-wide workshops.
- **Technical Documentation & Reporting:**
  - o Authored and submitted penetration testing reports with evidence.
  - o Practiced security report generation and documentation best practices.

- **Communication Skills:**
    - Strengthened our ability to present findings professionally and clearly.
    - Attended and participated in department meetings and presentations.
- **Time Management & Workplace Discipline:**
    - Adhered to daily responsibilities, managed time across assignments, and remained disciplined in all tasks.

Challenges Faced

- Limited access to some systems and configurations due to security restrictions.
- Adapting to the complexity of enterprise-level tools (SIEM, PAM, NAC) in a short span of time.
- Adjusting to live infrastructure environments and the scale of operations.

Recommendations

- Allow access to sandbox environments or virtual labs for deeper tool interaction.
- Encourage weekly mentorship sessions or guided walkthroughs for complex tools.
- Promote cross-team learning opportunities (e.g., DevSecOps, Governance Risk & Compliance).

Conclusion

Our attachment at **Electricity House – ICT Security Department** has been a transformative experience. We have acquired critical skills in cybersecurity operations, infrastructure management, incident response, and application security. The opportunity to interact with enterprise-grade tools and systems has sharpened both our technical and professional abilities.

We are grateful to the entire KPLC ICT Security team for the mentorship, support, and exposure. We leave this program better equipped for the challenges of modern-day cybersecurity roles and IT system development.