**INTERNSHIP REPORT**

**Name:** Stephen Mwaniki Mleghwa  
**Institution:** Redynox  
**Department:** Cybersecurity  
**Internship Duration:** June 21, 2025 – July 20, 2025

**Task 1: Introduction to Network Security Basics**

**Objective:**  
To understand foundational network security concepts, identify common network threats, and implement basic protection measures in a lab environment.

**Summary:**  
I set up a virtual lab consisting of pfSense (as the firewall/router), Kali Linux, Ubuntu, and Windows machines. The objective was to explore and understand network threats and apply defensive techniques in real-time.

**Activities Performed:**

* Studied common network threats: viruses, worms, trojans, phishing, ransomware.
* Configured pfSense for LAN/WAN segmentation.
* Enabled firewall rules to filter inbound and outbound traffic.
* Configured Windows Defender Firewall.
* Applied security measures including changing default passwords and enabling WPA2 encryption.

**Threats Identified:**

* **Viruses:** Malicious programs that replicate and spread.
* **Worms:** Self-replicating malware that spreads without user interaction.
* **Trojans:** Malicious software disguised as legitimate programs.
* **Phishing:** Social engineering attacks aimed at stealing sensitive data.

**Security Measures Implemented:**

* Setup and hardened pfSense firewall rules.
* Enabled Windows Defender Firewall with custom rules.
* Used WPA2 encryption on wireless settings.
* Disabled unused services and changed default credentials.

**Monitoring:**  
Used **Wireshark** on Kali Linux to capture and analyze network traffic. Identified various protocols like HTTP, DNS, and ICMP. Observed normal versus suspicious behavior.

**Screenshot Placeholder:**  
[Insert Wireshark capture screenshot showing traffic types here]

**Reflection:**  
Basic network security involves more than firewalls; it's about layered defense. I now understand how important it is to analyze traffic and apply minimum privilege policies.

**Task 2: Web Application Vulnerability Testing Using OWASP ZAP**

**Objective:**  
To learn how to identify and exploit web application vulnerabilities using ZAP and DVWA (Damn Vulnerable Web Application).

**Summary:**  
I set up DVWA in my Kali Linux VM and used OWASP ZAP to capture traffic and detect vulnerabilities. I changed DVWA security settings to "Low" for easier identification and practiced ethical hacking methods.

**Tools Used:**

* OWASP ZAP (Zed Attack Proxy)
* Firefox (configured through proxy)
* DVWA (hosted locally)
* Kali Linux

**Steps Taken:**

1. Installed and configured DVWA and its database.
2. Set up OWASP ZAP to intercept and scan traffic from Firefox.
3. Explored DVWA sections like SQL Injection, XSS, Command Injection.
4. Used ZAP Spider and Active Scan to identify vulnerabilities.

**Vulnerabilities Identified:**

* **SQL Injection:** Found on vulnerabilities/sqli/ page.
  + Risk: High
  + Fix: Use prepared statements.
  + [Insert screenshot of SQLi alert in ZAP]
* **Reflected XSS:** Found on vulnerabilities/xss\_r/ page.
  + Risk: Medium
  + Fix: Encode user input.
  + [Insert screenshot of XSS alert in ZAP]
* **Command Injection:** Found on vulnerabilities/exec/ page.
  + Risk: High
  + Fix: Validate shell commands strictly.
  + [Insert screenshot of Command Injection alert in ZAP]

**Reflection:**  
This task helped me understand how attackers interact with vulnerable web apps. OWASP ZAP provided practical insight into how security scanners identify threats.

**Task 3: Cybersecurity Branding via LinkedIn**

**Objective:**  
To develop a professional cybersecurity identity and begin building a digital footprint.

**Summary:**  
I created a LinkedIn profile tailored to my cybersecurity career. I included skills, added the internship experience, and posted about my progress. I also connected with cybersecurity communities.

**Profile Highlights:**

* Headline: Cybersecurity Intern | Ethical Hacker in Training
* Experience: Added Redynox internship with description of tasks
* Skills: Wireshark, OWASP ZAP, Network Security, Kali Linux

**LinkedIn Post:**

Started my cybersecurity internship with Redynox! I've set up pfSense, tested DVWA using OWASP ZAP, and explored vulnerabilities like SQLi and XSS. Learning so much in real-time. #Cybersecurity #OWASPZAP #Internship

**Screenshot Placeholder:**  
[Insert screenshot of LinkedIn profile here]  
[Insert screenshot of internship progress post]

**Reflection:**  
This task made me appreciate how personal branding is essential in cybersecurity. Sharing my learning publicly not only documents growth but also connects me with mentors and job opportunities.

**Conclusion**

This internship has provided me with foundational and practical skills in cybersecurity. From building a secure network to finding web app flaws and establishing a personal brand, I’ve taken my first solid step toward a professional career in cybersecurity.

**Next Steps:**

* Continue learning ethical hacking techniques.
* Pursue certifications like CompTIA Security+ or OSCP.
* Build and document more home lab projects.

**[End of Report]**