L4SER SECURITY LABS
BE AWARE ...

# PENETRATION TESTING SYLLABUS FOR LINUX LAGOS COHORT 1

## Module 1 - Introduction:

- Introduction to Penetration testing
- Why penetration testing is important
- Laws and Ethics

## Module 2 – Setting up your Penetration Testing Lab:

- Personal Lab setup
- Corporate Lab setup
- Security Operation Center

## Module 3 – Information Gathering:

- Passive information Gathering
- Active Information Gathering

## Module 4 – Vulnerability Identification & Exploitation :

- Vulnerability Scanning
- Port scanning
- Intrusion Detection System Evasion
- System Identification/Fingerprinting
- Services Identification
- Finding Exploits
- Network Sniffing

- MITM & Session Hijacking
- Buffer Overflows
- Password Attacks
- Web Hacking
- Social Engineering
- Wireless Attacks

## Module 5 – Post Exploitation& Exfiltration:

- Anonymity
- Backdoors
- Reverse Shell
- Encrypted Tunnels
- Privilege escalation
- Data Exfiltration

## Module 6 – Frameworks and Toolkits:

- Pentest Frameworks such as Metasploit, SEToolkit, MSF Venom, etc.
- Operating Systems

## Module 7 - Scripting:

- Bash Scripting
- Python
- Golang
- etc.

## Module 8 – Writing Professional Penetration Testing Reports:

- Technical Reports
- Executive Summary
- Proof Of Concepts

## Module 9 – Hands on Capture The Flag:

- Linux Lagos CTF