Oshunsan Samuel Ifeoluwa *Junior Penetration Tester*

✉ samuel.oshunsan@protonmail.com　　📞 07072188495

📅 2003/12/08　　🔗 https://samuelifeoluwa.github.io/

Profile

Dedicated Computer Science graduate with hands-on experience in penetration testing, ethical hacking, and vulnerability assessment. Transitioned from mobile development exposure to cybersecurity after discovering a strong passion for offensive security during university. Actively preparing for eJPT certification while building a practical portfolio covering network exploitation, web testing, payload evasion, cloud misconfigurations, and wireless attacks. Foundational knowledge of Python with ongoing self-study to deepen practical skills for automation and exploit development. quick learner, and eager to contribute to mission-driven cybersecurity teams in Nigeria and Africa.

Languages

- English

Professional Experience

2025/04 – 2026/04 Abuja, Nigeria	**Procurement** *Liviasoft Technologies ltd.* (*NYSC*)
2024/03 – 2024/12 Lagos, Nigeria	**mobile app developer** *UNEE*

Education

illishan-remo, Nigeria	**BSc. Computer Science** *Babcock University*

Certificates

- NASS BDL Training
- Ejpt -in progress

Skills

Penetration Testing
Network scanning & enumeration
Web reconnaissance
Password attacks
Wireless testing fundamentals
Vulnerability identification
Basic exploitation techniques

Projects

Windows Exploitation Labs (VM Environment)
- *Exploited Windows 7 VM via EternalBlue (Metasploit) for remote code execution.*

Web Vulnerability Assessment
- *Performed reconnaissance and scanning on family WordPress site (with explicit permission).　- Identified vulnerable RioVizual plugin and PHP version information disclosure.　- Recommended remediation: plugin update/removal, server header suppression.*

Credential Harvesting Simulation (MITM)

Used Responder (-vdwF) on Windows 10 VM to capture NTLMv2 hashes via protocol poisoning

Payload Obfuscation & Evasion

Built reverse shell with Villain → obfuscated (backticks, variable renaming) → converted/hidden via bat2exe & image embedding.

Wireless Security Lab

- Wireless Captured/cracked WPA2 handshakes using Aircrack-ng suite in controlled environment