# Olakojo Olaoluwa

olakjosh@gmail.com — (234) 813-717-8824 — linkedin.com/in/sci-sec/ — secfortress.com — github.com/sec-fortress

youtube.com/@sec-fortress — sec-fortress.github.io

## SUMMARY

Offensive security engineer/penetration tester with hands-on experience in networking, scripting, Linux administration, Active Directory exploitation, and cloud environments. Skilled in offensive security methodologies with deep familiarity with security frameworks such as OWASP Top 10, Microsoft SDL, MITRE ATT&CK, and the SANS Top 25. Knowledgeable in defensive security practices including SIEM tuning, threat hunting, and blue-red team collaboration. Holds multiple industry recognized certifications, including OSCP (Offensive Security Certified Professional), HTB CPTS (Certified Penetration Testing Specialist), and CRTP (Certified Red Team Professional). Continuously expanding technical depth through real world attack simulations, red team exercises, and adversary emulation labs.

## EXPERIENCE

**Boch Systems Ltd** — Hybrid, Nigeria
*Offensive Security Engineer* — September 2024 – Present

- Executed advanced red team assessments for 12+ organizations in the banking, pension, and fintech sectors, including Trustfund Pensions, Olive Microfinance Bank, DLM, and Gateway Mortgage Bank, simulating real-world adversaries to uncover systemic weaknesses.
- Uncovered critical vulnerabilities that could have resulted in more than 300 million ($250,000 +) in potential financial losses, helping clients avoid data breaches and regulatory penalties.
- Gained domain admin access in multiple internal network assessments via techniques such as Zerologon exploitation, NTLM hash relay, and password spraying targeting weak corporate credentials (e.g. P@ssw0rd123, hyosung).
- Leveraged tools like BloodHound and PingCastle to map domain privilege paths and expose risky Active Directory configurations.
- Successfully bypassed Rublon MFA on Remote Desktop services by extracting browser-saved credentials with LaZagne, simulating adversary-in-the-middle scenarios.
- Discovered vulnerabilities in automated teller machine applications during an internal banking assessment, where I gained access to the Windows host that runs automated teller machine software, manipulated transaction workflows, and demonstrated redirection of internal money transfer operations, all under strict rules of engagement.
- Authored comprehensive reports with executive summaries, technical findings, and prioritized mitigation steps, directly leading to security policy revisions and patch management strategies.
- Strengthened clients' internal security posture, reduced attack surface by 65%, and improved incident response maturity across multiple organizations.

**VibesMeet LLC** — (Contract) Remote, United Kingdom
*Application Security Consultant* — December 2024 – February 2025

- Supported the DevOps team of a UK-based dating platform to embed security into the SDLC and reduce risk exposure across AWS-hosted infrastructure.
- Discovered and reported high-impact API vulnerabilities, including business logic flaws and endpoints that leak user Personally Identifiable Information (PII), such as emails and phone numbers, mitigating potential GDPR violations.
- Conducted SAST using Semgrep, reducing production bugs by 40% and ensuring compliance with the OWASP Top 10 standards.
- Strengthened AWS cloud security by configuring CloudFront, Cloudflare WAF, and IAM policies, blocking more than 10,000 unauthorized requests per week, and preventing asset enumeration.
- Hardened content delivery configurations to prevent unauthorized downloads and hotlinking of premium content.
- Implemented a real-time threat detection stack combining:
  **AWS GuardDuty** : threat intelligence and anomaly detection
  **AWS CloudTrail + CloudWatch** : for event monitoring and alerting
  **Wazuh** : for endpoint threat visibility and log correlation
- Reduced attack surface by 70%, prevented customer data leakage, and helped the company avoid potential fines of £100,000+ under UK data protection laws.

**TechPeak Lab** — Remote, United Kingdom
*Security Specialist* — February 2024 - February 2025

- Conducted comprehensive web application security assessments focusing on common vulnerabilities such as SQL injection, XSS, CSRF, and IDOR, using tools like Burp Suite, OWASP ZAP, and Nessus.
- Specialized in API security testing for RESTful and GraphQL APIs, identifying misconfigurations, insecure data exposure, and access control issues using Postman, FFuF, and custom scripts to ensure robust API security measures.
- Collaborated directly with clients to understand their security needs, tailoring security assessments and remediation plans to align with their specific business objectives and compliance requirements (e.g., GDPR, PCI-DSS, ISO 27001).
- Provided security recommendations based on OWASP Top 10 and SANS Top 25 vulnerabilities, ensuring adherence to best practices in secure software development across the SDLC for web applications and APIs.

- Performed continuous security monitoring of client environments, integrating SIEM tools (e.g., Splunk, Wazuh, Suricata) to detect and respond to security incidents, including unauthorized access attempts on APIs and web platforms.
- Developed and enforced secure API gateway policies and authentication mechanisms, such as OAuth2, JWT, and API key management, ensuring secure client-server communication and access control.
- Maintained and deployed Web Application Firewalls (WAF) and API gateways, ensuring protection from attacks like DDoS, Botnet attacks, and API-specific threats such as GraphQL injections or excessive data exposure
- Applied SAST and DAST tools (e.g., SonarQube, Veracode) to perform static and dynamic analysis of web applications, identifying vulnerabilities in both code and runtime environments, and ensuring that security is integrated throughout the development lifecycle.

**WTCN Solutions** Hybrid, Nigeria
*Network Penetration Tester* February 2022 – August 2023

- Utilized tools like Nmap, LDAP enumeration tools (such as ADExplorer, LDAPSearch), or PowerShell scripts (Powersploit) to gather information about the Active Directory environment, including domain controllers, user accounts, group memberships, etc.
- Perform password spraying or brute-force attacks against user accounts to identify weak passwords.
- Attempts to escalate privileges by exploiting vulnerabilities like Kerberos attacks (Golden Ticket, Silver Ticket), pass-the-hash attacks and ACL exploits.
- Pivoting through the network by exploiting trust relationships, weakly secured services and compromised credentials.
- Attempts to exfiltrate sensitive data from the network to assess the effectiveness of data loss prevention (DLP) controls.
- Conducted thorough security assessments of web applications, identifying vulnerabilities and weaknesses.
- Participated in client penetration tests, utilizing tools such as Burp Suite, OWASP ZAP, and Nessus to identify and remediate security vulnerabilities.
- Played a key role in the creation of Capture The Flag (CTF) labs (Boot2root) whereby utilizing platforms like Hack The Box and TryHackMe to provide hands-on training environments for cybersecurity enthusiasts alongside.
- Collaborated in setting up VMware, UTM and VirtualBox virtualization labs, configuring comprehensive home lab environments with Active Directory, Kali Linux, pfSense, and Snort.
- Led training sessions for internal teams, improving overall awareness of emerging cybersecurity threats and best practices.
- Documented all findings, including vulnerabilities, exploited paths, and recommendations for remediation whereby providing evidence such as screenshots, log excerpts, and command outputs to support my findings.

**SenseLearner PvT Limited** Remote, India
*Web Application Penetration Tester* August 2021 - November 2021

- Gathered information about the target web application using tools like Whois, DNSDumpster, Recon-ng etc.
- Identified subdomains, IP addresses, server information, and any publicly available information about **Senselearner's** application and its infrastructure.
- Used automated scanning tools like Burp Suite, OWASP ZAP, Nessus and Nikto to map out the web application attack surface.
- Perform manual and automated vulnerability assessments to identify common security issues such as SQL injection, cross-site scripting (XSS), CSRF, SSRF, IDOR, RCE and LFI.
- Also tested for data leakage, insecure file uploads, or other avenues for unauthorized access or manipulation.
- Worked with the development team and system administrators to validate the effectiveness of remediation efforts.
- Recommended implementing continuous security monitoring solutions to detect and respond to new vulnerabilities or security incidents e.g snort, wazuh and suricata.
- Generated detailed reports outlining findings, recommendations, and remediation steps, specifying CWE catalog and CVSS for each finding.

## SKILLS

- **Secure Software Development Framework(SSDF):** OWASP Top 10, SANS Top 25, Microsoft SDL, MITRE ATT&CK Framework.
- **Identity Provider:** Active directory.
- **Scripting Languages:** Bash, Python, Powershell.
- **Networking Protocols:** OSI Model, TCP/IP, FTP, SMB, SSH, VoIP, Telnet, Web.
- **Encryption:** Symmetric, Asymmetric, OpenSSL.
- **Endpoint Monitoring:** Snort, Wazuh, Suricata.
- **SDLC Security Practices:** Threat Modeling, SAST, DAST, SCA, OSSTMM, PTES.
- **Operating Systems:** Linux(Debian, Kali, Ubuntu, ParrotSec), Microsoft Windows 10/11, Windows Server 2019/2022.
- **Security Tools:** Nessus, Semgrep, Metasploit, Powersploit, Hydra, Hashcat, PingCastle, Havoc, Bloodhound, Burp Suite, Impacket, Mimikatz, Nmap, FFuF, SysInternals, Ligolo-ng, Lazagne.
- **Container:** Docker Security, Vagrant.
- **Hypervisors:** VM Ware, Virtual Box, Qemu.
- **Networking:** Wireshark, TCPdump, VLANs, Routing, Switching, proxies, Tcp/Ip, OSI Model.
- **Database Management Systems:** SQLite, PostgreSQL, MongoDB, Redis.

- **Reporting:** MS Word, PDFTeX, Sysreptor, Libre Office.
- **Microsoft Office Suite:** Word, Excel, PowerPoint, Outlook.
- **Communication:** Fluent in English (UK).

## ACHIEVEMENTS & CERTIFICATIONS

| | | |
|---|---|---|
| 2025 | **OSCP+**, OffSec Certified Professional+ | portal.offsec.com |
| 2025 | **OSCP**, OffSec Certified Professional | portal.offsec.com |
| 2024 | **CVE-2024-55341**, Stored Cross Site Scripting(XSS) | MITRE-Corp |
| 2024 | **CVE-2024-55342**, Authenticated Remote Code Execution(RCE) | MITRE-Corp |
| 2024 | **CVE-2024-44871**, Authenticated Remote Code Execution(RCE) | MITRE-Corp |
| 2024 | **CVE-2024-44872**, Reflected Cross Site Scripting(XSS) | MITRE-Corp |
| 2024 | **Prolabs:** | |
| | – **Dante**, Penetration Tester Level II lab | Hackthebox.com |
| | – **Zephyr**, Red Team Operator Level I | Hackthebox.com |
| 2024 | **CPTS**, Certified Penetration Testing Specialist | Hackthebox.com |
| 2024 | **CRTP**, Certified Red Team Professional | AlteredSecurity.com |
| 2024 | **OffSec**, Offensive Pentester Path | Tryhackme.com |
| 2024 | **Jr Pentester**, Junior Penetration Tester Path | Tryhackme.com |
| 2023 | **PEH**, Practical Junior Penetration Tester | Academy.tcm-sec.com |

## EDUCATION

**Air Force Secondary School**, Lagos, Nigeria — Enrolled: February 2018 — Finished: September 2022
High-School **Art** — Threads: literature, visual arts, music.

**National Open University**, Nigeria — Enrolled: January 2024 — Expected: January 2027
BSc **Criminology** — Threads: Criminal Behavior Analysis

**Team 5h4d0wbr0k3r5 — Hackthebox** — Remote, India
*CTF Player* — December 2023 – Ongoing

- Actively engage in penetration testing activities on the HTB platform, practicing machines to exploit the latest CVEs and enhance my skills,
- Completed various challenges and achieved a ranking of **pro-hacker** on the HTB platform.
- Collaborated closely with team members to develop exploits for the latest CVEs (Common Vulnerabilities and Exposures) and tools aimed at simplifying Capture The Flag (CTF) challenges for all team members.
- HTB-Profile -: 5h4d0wbr0k3r5