Opeyemi Ariyo

the.opemi.aa@gmail.com — (234) 916-145-4820 — linkedin.com/in/opeyemi-ariyo — opemi-aa.github.io

youtube.com/@the.opemi$_{a}a$ — github.com/opemi-aa

SUMMARY

Security researcher/penetration tester with extensive networking, scripting, linux administration, active directory and cloud experience. Familiarity with security frameworks including OWASP Top 10, Microsoft SDL, MITRE ATT&CK Framework and SANS Top 25. Knowledgeable on defensive security concepts including SIEM and threat hunting. Actively pursuing the **CEH** certification to further validate proficiency and skill set.

EXPERIENCE

Boch Systems Hybrid, Nigeria
Ethical Hacker February 2024 - Present

- 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.

Virtually Testing Foundation Remote, Nigeria
Cloud Security Engineer Intern November 2023 – January 2024

- Completed guided labs on Whizlabs, mastering core concepts like IAM policies, data encryption, secure network configurations, and threat detection in cloud environments.
- Practiced identifying and remediating common cloud misconfigurations (e.g., excessive permissions, unencrypted storage, open ports) through Whizlabs' simulated attack scenarios.
- Conducted penetration testing exercises, including brute-force attacks, privilege escalation, and lateral movement, to understand attacker techniques and defensive best practices.
- Gained proficiency with Whizlabs-integrated tools for log analysis, intrusion detection, and compliance auditing.
- Summarized lab findings with screenshots, command outputs, and step-by-step remediation notes to reinforce learning and track progress.
- Engaged in group lab challenges and discussions to troubleshoot security scenarios and share solutions with peers.

Virtually Testing Foundation Remote, Nigeria
Red Team Engineer Intern July 2023 - September 2023

- Executed advanced attack scenarios using CALDERA (MITRE ATTCK framework) and Covenant C2 to emulate real-world threats, including lateral movement, privilege escalation, and exfiltration.
- Configured and secured a pfSense firewall in VMware to segment lab networks, test rule effectiveness, and block malicious traffic during red team exercises.
- Completed TryHackMe offensive security rooms, practicing exploits, post-exploitation tactics, and evasion techniques.
- Designed and deployed custom payloads (e.g., PowerShell Empire, Metasploit modules) to test detection capabilities and endpoint security controls.
- Detailed attack methodologies, including screenshots, command logs (Terminal, Covenant GUI), and mitigation recommendations for blue team review.
- Participated in capture-the-flag (CTF) challenges and shared findings with peers to improve collective red/blue team strategies.

Pearlsoft Incorporated Hybrid, Nigeria
Industrial Training December 2022 - May 2023

- Assisted in designing, coding, and debugging software solutions, ensuring optimal performance and reliability across applications.
- Updated and maintained MySQL PostgreSQL databases, optimizing queries and ensuring data integrity for seamless operations.
- Conducted testing (unit, integration) and troubleshooting to identify and resolve bugs, improving application stability.
- Researched and implemented latest tech trends into projects, staying ahead of industry advancements through workshops and training.
- Proposed and implemented efficiency enhancements, reducing runtime by 15% in key workflows.
- Taught Scratch programming and robotics to students, fostering problem-solving skills and creativity in 20+ learners.

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, 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	**ACP**, APIsec Certified Practitioner	🔗 APIsec
2025	**CASA**, Certified API Security Analyst	🔗 APIsec
2023	**Pentest+**, CompTIA PenTest+ Learning Path	🔗 Tryhackme.com
2023	**Jr Pentester**, Junior Penetration Tester Path	🔗 Tryhackme.com
2023	**ES**, Endpoint Security	🔗 Cisco.com

EDUCATION

Olabisi Onabanjo University, Nigeria — Enrolled: September 2018 — Finished: December 2023
Threads: BSc **Bachelor Of Engineering** — Threads: Computer Engineering

Ingressive For Good, Nigeria — Enrolled: April 2023 — Finished: July 2023
Threads: Cybersecurity Scholarship

HNG Tech, Nigeria — Enrolled: Jun 2024 — Finished: August 2024
Threads: Devops Engineering

Team opemi — 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 -: opemi