OLAKOJO OLAOLUWA

CONTACT INFORMATION

Phone: +234 8137178824
Email: olakjosh@gmail.com
LinkedIn: linkedin.com/in/sci-sec
Portfolio: sec-fortress.github.io
Github: github.com/sec-fortress
Youtube: youtube.com/@sec-fortress

SUMMARY

An **experienced** and results-driven Penetration Tester with over **1 year of experience** and a proven track record in identifying and **mitigating cybersecurity vulnerabilities**. Expertise in comprehensive penetration testing across networks, web applications, and systems. Proficient in **Linux**, Experience with programming languages like **Bash and Python scripting**, Possessing a robust understanding of IT technologies, including **IPS/IDS, TCP/IP, OSI model, Firewalls, Active Directory, Threat hunting**. Currently preparing for the **Certified Red Team Professional** exam, demonstrating a commitment to staying at the forefront of offensive security practices. Seeking a challenging role to leverage technical acumen, strategic thinking, and exceptional **report writing skills** in enhancing organizational cybersecurity.

WORK EXPERIENCE

SenseLearnerPvt.Limited, Internship, India — Remote + September 2023 - November 2023

- Conducted penetration tests on web applications, networks, and systems to identify vulnerabilities and assess the overall security posture.
- Collaborated remotely with cross-functional teams to develop and implement effective remediation plans for identified security issues.
- Provided detailed and actionable reports to clients, outlining vulnerabilities, potential exploits, and recommended mitigation strategies.

WTCN Solutions, Instructor, Nigeria — Remote + April 2023 - Present

- Delivering engaging and effective penetration testing courses to students, imparting practical skills and theoretical knowledge.
- Developing curriculum content, practical labs, and assessments to ensure a well-rounded and impactful learning experience.
- Providing mentorship and guidance to students, preparing them for real-world challenges in the field of cybersecurity.

TryHackMe, CTF Player, UK — Remote + October 2022 - Present

- Practice vulnerable machines and labs based on Linux / Windows OS for online penetration testing.
- Solved variety of challenges, showcasing proficiency in exploiting vulnerabilities, Privilege Escalation, and cryptographic analysis.
- THM-Profile – h4x0rOJ

Hackthebox, CTF Player, UK — Remote + October 2022 - Present

- Actively engage in penetration testing activities on the HTB platform, practicing machines to exploit the latest CVEs and enhance my skills.
- Authored walkthroughs and write-ups for completed HTB challenges, contributing to the cybersecurity community's knowledge base.
- HTB-Profile – 0l40luw4

HackMyVM, CTF Player, EU — Remote + September 2023 - Present

- Participated in various jeopardy challenges including pwn, web, crypto, osint, prog and misc to boost problem solving skills.
- Engaged in live Boot2Root VM hacking on both Windows and Linux platforms, encompassing enumeration, privilege Escalation, pivoting and persistence
- Authored standard walkthroughs and writeups for completed machines
- HMV-Profile – 0xpwn

MINOR PROJECTS

1. Damn Vulnerable Web App (DVWA Owasp-Top10).
   - **Project Link** -: DVWA Walkthrough
   - Installed and configured DVWA on a web server.
   - Explored a range of common web vulnerabilities, including SQL injection, cross-site scripting (XSS), file inclusion, and command injection.
   - Demonstrated the ability to manipulate and exploit vulnerabilities in a controlled setting.
2. Active Directory Domain Controller Setup.
   - **Project Link** -: AD Lab DC Setup
   - Setup one Domain controller on a Windows Server
   - Configuration of Active Directory Domain Services (AD DS) role on the server.
   - Setting Up Certificate Services
3. Nebula Privilege Escalation lab
   - **Project Link** -: Nebula Privilege Escalation
   - In depth understanding of linux through various privilege escalation methods
   - Explored and tackled a wide range of vulnerabilities in Linux systems, including SUID files, permissions, race conditions, and scripting language vulnerabilities.
4. Ping Sweeper/Port Mapper(Automation
   - **Project Link** -: Ping Sweeper/Port Mapper
   - Bash script to perform ICMP Echo request on a /24 network
   - Run a Network mapper and discover open ports including service versions and basic reconnaissance on each host

EDUCATION // ACHIEVEMENTS

2022 – Completed the **Comptia Security+ SY0-601**, covering diverse cybersecurity domains from **ITPRO.TV** such as threat identification, access management, risk assessment, cryptography, incident response, and governance, providing a foundational understanding of IT security principles and best practices.
2023 – Completed **INE's eLearnSecurity Junior Penetration Tester (eJPT)** course, acquiring skills in penetration testing, ethical hacking, and security analysis, emphasizing hands-on experience in various security domains
2023 – Played my first ever live **ECOWAS CTF** with team, **hackstreetboys**, Made Top 20 in leaderboards and you can find my writeup from here
2023 – Completed the **Practical Junior Penetration Tester (PJPT)** course from **TCM Security**, honing my skills in web and Active Directory penetration testing, with a focus on Linux and scripting proficiency, You can find the course note from here. aiming to obtain certification, currently preparing for the exam.
Expected Exam Date: January 1, 2024, Actively preparing for the **Certified Red Team Professional**CRTP exam, focusing on advanced skills in **Active directory penetration testing with powershell**. You can monitor my progress from here

SKILLS

- **Technical Skills:**
  - Penetration Testing (Web and Network)
  - Vulnerability Assessment
  - Firewall and IDS Implementation
  - Cryptography
  - Secure Coding Practices
- **Tools:**
  - Metasploit, Burp Suite, Nmap, Wireshark
  - Kali Linux, OWASP Zap, Nessus
- **Programming Languages:**
  - Bash, Python, SQLite
- **Operating Systems:**
  - Linux, Ubuntu, ParrotSecurity, Windows
- **Soft Skills:**
  - Strong Analytical and Problem-Solving Skills.
  - Excellent Communication and Presentation Skills.
  - Team Collaboration and Leadership.
  - Client-Focused Approach.
  - Time management.
  - Anger management.
  - Self-confidence.
  - Stress management.
  - Work-Life Balance.
- **Miscellaneous:**

- Docker, Git, Markdown, Vim, Debian