**ASHIDI, JOY SESI**

(+234)8165391713 [|ashidioy52@gmail.com](mailto:|ashidioy52@gmail.com) | <https://www.linkedin.com/ashidi-joy|> <https://github.com/joyashidi>

**PROFILE**

Results-driven penetration tester with hands-on experience in identifying and mitigating security vulnerabilities. Proficient in penetration testing techniques, vulnerability assessments, and security tools such as Metasploit, Burp Suite, and Nmap. Completed extensive coursework and practical labs in cybersecurity, gaining real-world experience in ethical hacking, network security, and adversary emulation. Strong analytical mindset, attention to detail, and a passion for continuous learning. Eager to apply skills in a professional setting to enhance system and network security.

**SKILLS**

* **Vulnerability Assessment**: Basic proficiency in vulnerability scanning tools to identify and report security weaknesses in networks, applications, and systems.
* **Penetration testing**: Skilled in performing full lifecycle penetration testing and simulating attack techniques to evaluate security defences.
* **Active Directory Security**: Proficient in performing advanced Active Directory penetration tests, including hash capturing, cracking, NTLM hash dumping, and Kerberos exploitation.
* **Adversary Emulation**: Knowledge of adversary tactics, techniques, and procedures (TTPs), with hands-on experience in emulating real-world attack scenarios.
* **Scripting and Automation**: Experienced with Python and Bash scripting to automate scanning, exploit generation, and reporting tasks.
* **Operating Systems**: Familiarity with Linux, Kali Linux and Windows.
* **Network Security**: Solid understanding of network protocols (TCP/IP, HTTP, DNS) and basic network security principles, such as firewalls, segmentation, and VPNs.
* **Security Frameworks**: Awareness of OWASP Top 10 and familiarity with basic concepts in the MITRE ATT&CK framework.

**TECHNICAL TOOLS**

* **Vulnerability Assessment**: Nessus, OpenVAS, Nikto, Wireshark, Nmap, OWASP ZAP
* **Penetration testing**: Metasploit Framework, Burp Suite, Hydra, SQLmap, Netcat, John the Ripper, Hashcat, Gobuster, Dirb, Social-Engineer Toolkit (SET), Aircrack-ng,
* **Active Directory Penetration Testing**: Responder, Python3 (GetNPUsers, secretsdump.py, smbexec.py), Mimikatz
* **Programming/Scripting/Automation**: Python, Java, Bash, PowerShell, Windows task scheduler
* **Adversary Emulation tools**: MITRE frameworks, Mimikatz, Metasploit framework, AdFind, Net User
* **Frameworks**: Kubernetes, OWASP ZAP, ITIL Framework
* **Technical report writing:** Proficient in technical report writing

**CERTIFICATIONS AND TRAINING**

* eLearnSecurity Junior Penetration Tester (eJPT) - *April 2025*
* CompTIA Security+ (INFOSEC) - *October 2024*
* Blockchain Security (INFOSEC) - *October 2024*
* Machine Learning for Red Team Hackers (INFOSEC) - *October 2024*
* Cybersecurity Leadership and Management (INFOSEC) *- October 2024*
* Cybersecurity Soft Skills (INFOSEC) *- October 2024*
* ISC2 Certified in Cybersecurity (CC) - *September 2024*
* Adversary Emulation Methodology – *September 2024*
* CompTIA Linux+ (INFOSEC) - *May 2024*
* Junior Cybersecurity Analyst (Cisco) - *February 2024*

**EXPERIENCE**

**Cybersecurity Analyst Trainee – Vulnerability Assessment and Penetration testing**

**CyberSafe Foundation, CyberGirls Training Programme – Remote**

March 2024 – December 2024

* Mastered foundational principles of vulnerability assessment and penetration testing through the completion of the Junior Penetration Tester (eJPT) course, gaining hands-on experience in identifying and exploiting security weaknesses.
* Automated critical security tasks and exploit development by leveraging scripting languages such as Bash and Python, significantly enhancing the effectiveness of red team operations.
* Explored cutting-edge machine learning techniques for red team hacking, enabling the identification and exploitation of vulnerabilities in complex environments with increased precision.
* Developed strong soft skills in collaboration and leadership, effectively contributing to cybersecurity teams and navigating both the technical and strategic aspects of security testing.
* Gained expertise in blockchain security, assessing and mitigating vulnerabilities in decentralized systems and applying this knowledge to safeguard advanced technological environments.
* Collaborated with teammates on projects and presentations, demonstrating strong teamwork and communication in cybersecurity topics.

**Mastercard Cybersecurity Virtual Experience Program**

**Forage – Remote**

August 2024

* Identified and mitigated phishing threats as part of a job simulation, creating an educational campaign using real-fake emails to enhance security awareness across the organization.
* Analyzed and pinpointed key areas within the business requiring enhanced security training, leading to the development and implementation of targeted training programs.

**EDUCATION**

* **Bachelor of Science (BSc.) in Computer Science**

University of Lagos | Lagos, Nigeria | (In View)

**PROJECT**

* **Automating Windows Server Hardening** | PowerShell, Windows Task schedular August 2024

Played a key role in automating Windows server hardening, leading to enhanced system defences by implementing security policies through Windows Task Scheduler and PowerShell. Achieved 2nd place for this project, showcasing effective collaboration and technical execution.

* **Active Directory Penetration testing** November, 2024  
  Conducted an in-depth penetration test of an Active Directory environment, identifying privilege escalation paths and misconfigurations, and suggesting mitigations.

**VOLUNTEER EXPERIENCE**

**SheCodeAfrica (SCA Unilag chapter) - Non-Profit Organization**

Community Manager | 2025 - Present

* Initiated efforts on expanding and creating a thriving community for collaboration, building skills and sharing knowledge.

**Professor Ayodele Awojobi Design Competition (P.A.A.D.C) - Non-Profit Organization**

Deputy team lead, Protocol team | 2023 - Present

* Analyzed, reached out to potential guests/judges and invited them to different stages of the competition process e.g review stage, nexus, pre-event, masterclass and grand finale.
* Collaborated with a fellow team mate to produce a handbook for the team for present and future protocol teams

**REFEREES**

Available upon request