SAMSON OBIE

+234 904 267 1764 samsonobie475@gmail.com https://samsonobie.github.io
https://ng.linkedin.com/in/samson-obie-a0a181259

PROFESSIONAL SUMMARY

Dedicated Cybersecurity Analyst, Ethical Hacker, and Penetration Tester with years of hands-on experience identifying, exploiting, and validating security weaknesses across web applications and network environments. Experienced in OWASP Top 10 vulnerabilities, exploit verification, and practical remediation guidance, using tools such as Kali Linux, Metasploit, and Wireshark to help organizations reduce risk and strengthen their security posture.

TECHNICAL SKILLS

- Security Assessment: Penetration Testing, Vulnerability Scanning, Ethical Hacking, Threat Analysis, Social Engineering, Risk Assessment.
- Tools & Platforms: Kali Linux, Metasploit Framework, Burp Suite (Community), Nmap, Wireshark, Nessus, John the Ripper, Hydra, VirtualBox/VMware.
- Web Application Security: OWASP Top 10, SQL Injection (SQLi), Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Session Hijacking, Input Validation.
- Network Security: Cisco IOS, Firewall Configuration, VLAN Segmentation, Access Control Lists (ACLs), TCP/IP, OSI Model, Port Security, IDS/IPS Concepts.
- Physical Security & ICS: Biometric Access Control Systems, IP Surveillance/CCTV Networking, RFID Technology, Automated Security Systems, Industrial IoT (IIoT) Security.
- Operating Systems: Linux (Kali, Ubuntu, Debian), Windows Server, Windows 10/11.

PROFESSIONAL EXPERIENCE

Ethical Hacker / Penetration Tester
Commonwealth Bank| October 2024 - Present

- Performed ethical hacking engagements across web applications and Windows-based environments using structured penetration testing methodologies.
- Discovered and Validated 30+ security vulnerabilites including broken authentication, access control flaws, insecure configuration, exposed services, and injection-related weakness.
- Simulated real-world attack paths using tools such as Burp Suite, Nmap, Metasploit, Wireshark, Nessus, SQLmap, BloodHound, Impacket, Responder, John the Ripper, Hashcat, FFUF, Nikto, OWASP ZAP, Evil-WinRM.

- Produced professional penetration testing reports with severity ratings, proof-of-concept evidence, attack reproduction .

- Provide guidance for these teams, making remediations and delivering recommendations to ensure any vulnerabilities found are adequately addressed.

- Ensure all processes used by the team are documented thoroughly and adhere to the necessary security standards particularly highly confidential processes.

CYBERSECURITY PROJECTS & LABS

- Advanced Penetration Testing & Vulnerability Assessment (Home Lab) Designed and deployed an isolated virtualization environment using VMware to simulate a corporate network, hosting attacker machines (Kali Linux) and vulnerable targets (Metasploitable 2, Windows 10).

- Executed comprehensive network enumeration using Nmap to map attack surfaces and identify open ports. Successfully exploited legacy services (e.g., vsftpd, Samba) using the Metasploit Framework, demonstrating the ability to compromise systems and escalate privileges to root.
- Created detailed technical reports documenting attack vectors, exploitation steps, and remediationrecommendations, simulating professional penetration testing deliverables.

Web Application Security Assessment (OWASP Juice Shop & DVWA)

- Exploitation: Utilized Burp Suite to intercept and manipulate HTTP/HTTPS traffic. Successfully executed SQL Injection (SQLi) attacks to bypass authentication mechanisms and exfiltrate database information. Demonstrated Reflected and Stored XSS attacks to validate client-side risks.

Enterprise Network Hardening (Cisco Packet Tracer)

- Configured secure network topologies simulating enterprise environments. Implemented VLANs to segment traffic and reduce lateral movement opportunities.

- Applied granular Access Control Lists (ACLs) to restrict unauthorized access to critical network segments and management interfaces.

- Configured Port Security to mitigate Layer 2 attacks such as MAC address flooding and DHCP snooping, ensuring the integrity of the network edge.

EDUCATION

Secondary Education
Ibru College | 2018

- Continuing professional development through industry certifications

CERTIFICATIONS

- Cisco introduction to Cybersecurity Certificate | 2024

- Cisco Networking Basics Certificate | 2024

- Cisco Ethical hacker Certificate | 2024