Mojetioluwa Daniel Bolaji-Busola

princeheritage1@gmail.com | 0x5h4q.github.io | github.com/0x5h4q | linkedin.com/in/daniel-bolaji-busola
Lagos, Nigeria +234 704 266 5679

Summary

Penetration tester and security researcher with hands-on experience across Active Directory exploitation, web application security, ICS/OT security research, and IoT hardware hacking. **Pro Hacker** on HackTheBox (**#2 in Nigeria**; **6th**, Season 11, team RanswomWeare), **Top 6%** on TryHackMe, **103rd/6,734** in Cyber Apocalypse CTF 2026. PJPT & CRTA certified. I break things, document the kill chain, and help organizations fix what matters.

Education

Covenant University SECOND CLASS UPPER
B.Sc. Computer Science *Ota, Nigeria*

Experience

Cybersecurity Intern June 2026 – Present
Ubuntu Bridge Initiative — Cyber Core Associate (Simulated SOC Engagement) *Remote*
- Reconstructed a 4-stage attacker kill chain for a fintech breach investigation — initial access (SQLi, SSRF) through persistence (sudoers abuse, shell profile backdoor) to exfiltration and C2 beaconing, then identified an insider threat obscuring the incident from the board.
- Delivered a board-ready remediation package: risk register, regulatory breach notification, **30/60/90**-day roadmap, and confirmed-vs-exposed data control mapping.
- Exploited an AWS IAM privilege-escalation path (unrestricted `iam:PassRole` → Lambda execution role assumption → crown-jewel data access) in a cloud attack-path assessment, then remediated it with a scoped `iam:PassedToService` condition while preserving the authorized workflow.

Security Researcher Jul 2025 – Present
HackerOne / BugCrowd / YesWeHack *Remote*
- Hunt web application vulnerabilities specializing in authentication flaws, IDOR, and API security; acknowledged in program hall of fame for disclosed findings.

Security Engineer Apprentice Apr 2024 – Present
Covenant University *Ota, Nigeria*
- Perform authorized penetration tests against university infrastructure and build Python automation for security audit workflows aligned with NIST and ISO 27001.

Leadership

Cybersecurity/Networking Lead Present
Google Developers Group (GDG) — University Chapter *Ota, Nigeria*
- Built and maintain gdg-cyber-quiz.web.app, a weekly cybersecurity quiz platform combining multiple-choice questions and hands-on practical challenges for group members.

Projects

sh4q | *Python* — safety-first reconnaissance control plane
- Designing a scope-enforced recon orchestrator with scoped DNS/HTTP resolution, redirect and DNS-rebinding validation, request-budget limiting, and an event-sourced SQLite evidence store with tool-version provenance.

SafeCO | *Python, SQLite, Modbus* — ICSC 2026 submission
- Building a local-first, explainable monitor that flags protocol-valid-but-unsafe commands against a simulated water treatment plant and advises a human operator, backed by a tamper-evident hash-chained event store.

VulnBank Pentest Series | *Burp Suite, OWASP WSTG/API Top 10*
- Ran a full black-box pentest of a vulnerable fintech app, chaining SQLi auth bypass, JWT forgery, BOLA, and negative-amount transfer theft into full account and financial compromise; 8 findings (4 critical) published with PoCs and remediations.

HTB Pro Labs & Fortresses | *Active Directory, Cloud, Web*
- Completed Pro Lab **Puppet** and Fortresses **Context** and **Akerva**. Pwned Hard-rated machines (Pirate, Logging, TombWatcher) chaining Pre2k, gMSA abuse, RBCD, SPN jacking, and ADCS ESC15.

ESP32 Marauder, **BadUSB/Rubber Ducky** & **PSRecon** | *KiCad, CircuitPython, Python/Impacket*
- Built a custom PCB (ESP32, CC1101, GPS) for deauth detection, BLE scanning, and evil-portal deployment; built a Pico HID device for credential harvesting; and developed a post-exploitation tool extracting PSReadline history over SMB with Pass-the-Hash support.

Security Blog | *Jekyll* — 0x5h4q.github.io
- Authored **20+** technical write-ups in under two months spanning Active Directory attacks, web application vulnerabilities, and ICS/OT research, including the two-part VulnBank pentest series and CVE-2026-54121 (Certighost) research.

Research

AI-Driven Network Anomaly Detection for Healthcare IoT July 2026 – Present
Lead Researcher

- Developing a real-time threat monitoring system for IoT medical devices, EHRs, and hospital networks targeted by ransomware and data breaches.

Certifications

Certified: PJPT (TCM Security), CRTA (CyberWarfare Labs), AWS Cloud Practitioner, Associate of $(ISC)^2$, Jr. Penetration Tester (THM), Puppet, Akerva, Context (HTB)
Pursuing: CPENT|AI, CPTS (HTB)

Technical Skills

Web & API Security: Burp Suite, OWASP WSTG, OWASP API Top 10
Active Directory & Windows: BloodHound, Impacket, Evil-WinRM, NetExec, Certipy
Recon, Exploitation & Analysis: Nmap, Metasploit, Wireshark, Ghidra
Cloud Security: AWS IAM, Terraform, AWS CLI, CloudTrail analysis
Hardware & Embedded: KiCad, ESP32, CircuitPython
Languages: Python, PowerShell, Bash, C++
Frameworks & Standards: MITRE ATT&CK, NIST, ISO 27001