Arnold Mavhezha

New York, NY | (917) 449-0928 | arnoemavhezha@gmail.com | linkedin.com/in/arnold-mavhezha/ | github.com/mavhezha | mavhezha.com/

SUMMARY

Offensive security-focused graduate student pursuing an M.S. in Cybersecurity at Yeshiva University, with 5+ years of hands-on experience in penetration testing, vulnerability assessment, and adversarial simulation. Proficient with Burp Suite, Metasploit, Nmap, and Wireshark, with real-world application across web and network engagements. Currently pursuing OSCP; active HackTheBox (Premium) practitioner with documented writeups on GitHub. Brings professional experience translating offensive findings into actionable remediation roadmaps and client-ready reports.

EDUCATION

Master of Science in Cybersecurity | GPA 4.0 August 2025 - May 2027
Yeshiva University, Katz School of Science and Health New York, NY
Relevant Coursework: Architecture Of Secure Operating Systems, Applications and Devices, E-Discovery and Digital Forensics, Cloud Security, Network Security

Bachelor of Technology in Computer Science and Engineering | GPA: 3.8 July 2016 – July 2020
Parul University Gujarat, India
Relevant Coursework: Design and Analysis of Algorithms, Python Programming, Network Security, Problem Diagnosis and Practices, Theory of Computation, Parallel and Distributed Computing

CERTIFICATIONS

OSCP (Offensive Security Certified Professional) | In Progress June 2026
CompTIA Security+
ISC2 Certified in Cybersecurity (CC)
ISO/IEC 27001:2022 Lead Auditor

PROJECTS

Web Application Penetration Test – OWASP Juice Shop February 2026
Tools: OWASP Top 10, Burp Suite, CVSS, Vulnerability Testing

- Executed a full black-box penetration test against OWASP Juice Shop, identifying 9 vulnerabilities across 7 OWASP Top 10 (2021) categories - 2 Critical, 3 High, and 4 Medium severity
- Pinpointed an Insecure Direct Object Reference (IDOR) vulnerability enabling sequential enumeration of all users' basket data via unauthenticated API requests
- Exploited the absence of rate limiting on the login endpoint to brute-force admin credentials on attempt 3, demonstrating a complete Broken Authentication (CVSS 7.5) attack chain
- Bypassed client-side file upload restrictions using Burp Suite request interception, confirming the absence of server-side validation across 3 upload endpoints
- Produced a 33-page professional penetration test report with executive summary, CVSS-scored findings, 45 evidence screenshots, Proof of Concept (PoC) steps, and a prioritized remediation roadmap

PROFESSIONAL EXPERIENCE

Security Engineer April 2022 - July 2025

Exceedingly Great Technologies Harare, ZW

- Engineered threat detection logic across 1,000+ endpoints using Splunk Security Information and Event Management (SIEM), cutting mean time to detect (MTTD) by 35% through custom correlation rules and behavioral analytics mapped to MITRE ATT&CK tactics, techniques, and procedures
- Led vulnerability assessment and penetration testing exercises using Nessus and Nmap, mapping findings to Common Vulnerability Scoring System (CVSS) attack vectors and eliminating 45% of critical CVEs within 30- day remediation cycles
- Conducted adversarial simulation and firewall rule-set analysis, stress-testing network perimeter defenses and identifying blind spots, reducing threat-blocking failures by 20% and cutting false positives by 30%
- Hardened AWS cloud environment by enforcing IAM least-privilege access, MFA, Security Groups, and CloudTrail logging, eliminating 40% of unauthorized access vectors
- Spearheaded end-to-end incident response operations, leading triage, containment, and forensic root-cause analysis, successfully neutralizing 50+ security incidents with zero business disruption
- Executed controlled exploitation of 15+ web and network vulnerabilities (SQL injection, XSS, IDOR, privilege escalation) using Burp Suite and Metasploit to validate impact and guide remediation

Junior Security Analyst February 2021 - March 2022

Exceedingly Great Technologies Harare, ZW

- Escalated an average of 15 high-priority incidents per week, ensuring timely containment of malware, phishing, and unauthorized access attempts
- Performed vulnerability assessments across 250+ endpoints and 10 servers, remediating 95% of critical vulnerabilities within SLA targets with findings mapped to real-world attack vectors
- Executed targeted phishing simulation campaigns against 80+ staff members, analyzing click rates and credential harvesting susceptibility, achieving a 60% improvement in phishing awareness scores
- Partnered with network teams to enforce security controls including Multi-Factor Authentication (MFA) rollout and password policy hardening, reducing account lockout incidents by 40%
- Documented forensic incident reports and root-cause analyses, improving team knowledge base and cutting average response time by 20%

Junior Developer August 2020 - January 2021

Exceedingly Great Technologies Harare, ZW

- Designed 10+ secure APIs with integrated authentication controls, developing expertise in application security and vulnerability identification techniques
- Implemented security-by-design principles across 5+ applications establishing foundational cybersecurity best practices for enterprise IT systems
- Deployed automated systems using Python and process automation, contributing to secure development lifecycle and risk mitigation measures

SKILLS

Offensive Security: Penetration Testing, Vulnerability Testing, OWASP Top 10, SQL Injection, XSS, Authentication Bypass, Privilege Escalation

Security Tools: Splunk, SIEM, Burp Suite, Nessus, Nmap, Wireshark, OWASP ZAP, Metasploit, IDS/IPS

Programming: Python, JavaScript, SQL, Bash, PowerShell

Cloud & Systems: AWS, Linux, Windows, Active Directory, TCP/IP, HTTP/S, DNS

Frameworks: NIST, MITRE ATT&CK, CIS Benchmarks, ISO/IEC 27001, CVSS

MEMBERSHIPS

ISC2 New Jersey Chapter | Member

OWASP New York Chapter | Member