

TONY TABWA

Penetration Testing Assistant | Offensive Security | Red Team Support

174 Bay Leaf Street, Chantelle, GP, South Africa

(+27) 64-393-9152 | [Email](#)

[LinkedIn](#) | [Projects Portfolio](#)

PROFESSIONAL SUMMARY

Detail-driven and technically adept Penetration Testing Assistant with hands-on experience executing offensive security operations, vulnerability assessments, and exploitation techniques in simulated and real-world environments. Skilled in using industry-standard tools such as **Metasploit**, **Burp Suite**, **SQLMap**, **Nmap**, and **Wireshark** for full-scope red team exercises. Proven ability to uncover misconfigurations, craft custom payloads, exploit web app and network flaws, and implement post-exploitation persistence mechanisms. Eager to support dynamic security teams in remote, hybrid, or onsite roles focused on red teaming, vulnerability research, or penetration testing.

CORE COMPETENCIES

Web & Network Penetration Testing (**Kali Linux**, **Burp Suite**) | Vulnerability Scanning & Enumeration (**Nmap**, **Gobuster**) | Exploitation Frameworks (**Metasploit**, **SQLMap**, **XSS**, **RCE**) | Post-Exploitation & Persistence (**Meterpreter**, **Reg Hacks**) | Wireless Network Attacks (**WPA2**, **Aircrack-ng**) | **Python & Bash** for Security Automation | Secure Coding & Input Sanitization | OSINT Automation (**Python Libraries**) | Traffic Analysis (**Wireshark**, **Credential Capture**) | Reverse Engineering (**PE Explorer**)

PROFESSIONAL EXPERIENCE

CYBERSECURITY RED TEAM INTERN

Hack Secure – Remote | APR 2025 – MAY 2025

- Conducted in-depth vulnerability assessments and web application penetration testing across lab targets using **Burp Suite**.
- Discovered exposed directories using **Dirb/Gobuster**; executed brute-force enumeration on hidden endpoints.
- Exploited SQL Injection and Cross-Site Scripting (XSS) flaws to extract sensitive data.
- Captured unencrypted credentials using **Wireshark** and identified insecure login mechanisms.

- Gained reverse shell access through **Metasploit** exploitation of vulnerable services (e.g., Samba).
- Applied post-exploitation techniques with **Meterpreter** (scheduled tasks, registry modifications) to maintain persistence.
- Executed WPA2 de-authentication attacks in lab environments and cracked Wi-Fi handshakes with **Airgeddon**.
- Designed custom payloads to simulate attacker behavior and validate defense mechanisms.
- Used **PE Explorer** for binary reverse engineering, analyzing disassembled code and API calls.

FREELANCE DEVELOPER (SECURITY FOCUS)

Remote | AUG 2020 – Present

- Built secure authentication systems for clients using **Node.js, PHP, and RESTful API encryption**.
- Developed **Python scripts** to automate OSINT gathering and vulnerability discovery.
- Applied secure coding principles including **validation, sanitization, and token-based authentication**.
- Created **security automation tools** that reduced manual penetration testing overhead.
- Supported incident response readiness by identifying external threat intelligence trends and internal weak points.

EDUCATION


National Diploma in Information Technology

Damelin College | 2020 – 2023


National Certificate in Information Technology

CCOSA | 2017 – 2018

CERTIFICATIONS

 Blue Team Junior Analyst Pathway – Security Blue Team (Nov 2024)

✕ Ethical Hacker – Cisco Networking Academy (Aug 2024)

 Junior Cybersecurity Analyst Pathway – Cisco Networking Academy (Nov 2024)

 Cyber Threat Management – Cisco Networking Academy (Nov 2024)

○ Network Defense – Cisco Networking Academy (Nov 2024)

AVAILABILITY

Available Immediately / Open to Red Team Support, Offensive Security, and Remote Penetration Testing Roles