TONY TABWA

PENETRATION TESTING ASSISTANT

174 Bay Leaf Street,
Chantelle, GP, South Africa

(+27) 64-393-9152

tabwatony7@gmail.com

LinkedIn
Projects Portfolio

CORE SKILLS

- Penetration Testing & Exploitation
- Vulnerability Scanning & Enumeration
- Metasploit Framework, Burp Suite, Aircrack-ng
- Reverse Engineering (PE Explorer)
- Brute-force & Credential Capture Techniques
- Kali Linux & Bash Scripting
- Python for Automation

EDUCATION

NATIONAL DIPLOMA IN I.T
Damelin College
2020 - 2023

NATIONAL CERTIFICATE IN I.T
C.C.O.S.A
2017 - 2018

CERTIFICATES

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

PROFESSIONAL PROFILE

I'm a highly motivated and technically skilled aspiring Penetration Tester with hands-on experience in identifying and exploiting security flaws in web applications and networked environments. Proficient in using industry-standard tools such as **Metasploit, Burp Suite**, **SQLMap, Wireshark, Nmap, and Gobuster** to perform full-scope offensive security assessments. Demonstrated capability in executing brute-force directory enumeration, SQL Injection, Cross-Site Scripting (XSS), and remote exploitation of outdated services. Adept at crafting custom payloads, establishing reverse shells, and maintaining persistence through post-exploitation tactics. Passionate about simulating real-world attack vectors in lab environments to assess and improve system resilience.

PROFESSIONAL EXPERIENCE

CYBERSECURITY RED TEAM INTERN — **APR 2025 – MAY 2025**
Hack Secure

- Performed comprehensive vulnerability assessments and web application penetration testing on target environments.
- Discovered exposed directories (/admin/, /secured/) using Dirb/Gobuster and conducted brute-force enumeration.
- Executed SQL Injection and XSS attacks to exploit web application vulnerabilities and extract database information.
- Captured network traffic via Wireshark to retrieve plaintext credentials during insecure login transmissions.
- Leveraged Metasploit to identify and exploit services (e.g., Samba) and gain reverse shell access to Metasploitable VMs.
- Implemented post-exploitation techniques using Meterpreter, including persistence mechanisms (scheduled tasks, registry edits).
- Cracked WPA2 Wi-Fi handshakes obtained via de-authentication attacks in a controlled lab setup.
- Developed custom Metasploit payloads to simulate real-world attacker scenarios.
- Practiced binary analysis and reverse engineering on executables using PE Explorer to extract key insights.

FREELANCE DEVELOPER (SECURITY FOCUS) — **AUG 2020 – PRESENT**
Remote

- Built secure authentication systems for clients using Node.js and PHP.
- Leveraged python libraries to automate open-source intelligence tools to gather data and insights on potential security threats against client networks, improving incident response strategies.
- Applied secure coding practices and input sanitization.
- Secured RESTful APIs by integrating authentication and encryption strategies, ensuring data integrity and confidentiality.
- Worked on developing automation tools for security-focused tasks, reducing manual efforts and increasing overall efficiency in vulnerability detection.

Available for onsite testing, remote engagements, and red team support roles