OSCAR OPEMBA

> RED TEAMER // CYBERSECURITY ARCHITECT

oscaropemba@gmail.com | github: Oscar-Opemba | THM: 0xgh0stx | HTB: @0100M | Nairobi, Kenya

$ whoami && cat identity.txt

// CORE SKILLS

- [+] Kali Linux
- [+] Burp Suite
- [+] Wireshark
- [+] Sliver C2
- [+] Volatility3
- [+] YARA
- [+] Splunk
- [+] Python
- [+] Metasploit
- [+] Nmap
- [+] Cobalt Strike
- [+] BloodHound
- [+] Ghidra
- [+] Zeek
- [+] Docker
- [+] Bash

// CERTIFICATIONS

> eJPT — eLearnSecurity
> Google Cybersecurity Cert
> TryHackMe Top 5%

// PLATFORMS

TryHackMe
0xgh0stx

HackTheBox
@0100M

GitHub
Oscar-Opemba

// LANGUAGES

Python
Bash
JavaScript
Java

// PROFILE

Red Teamer and Cybersecurity Architect specializing in adversary simulation, threat intelligence, and offensive security operations. Experienced in full-scope penetration testing, red team engagements, and building automated threat intel pipelines. Operates from Nairobi with global client engagements across finance, government, and tech sectors across East Africa and beyond.

// EXPERIENCE

Red Teamer & Security Analyst
2023 — Present
Freelance / Remote

- [+] Lead red team engagements for financial and tech orgs across East Africa
- [+] Conduct full-scope web app and network penetration tests (OWASP/PTES)
- [+] Build automated threat intelligence pipelines using Python and STIX/TAXII
- [+] Deliver executive and technical pentest reports with remediation guidance

Penetration Tester
2022
Security Consultancy

- [+] Performed grey-box and black-box network penetration tests
- [+] Identified critical vulnerabilities in enterprise web applications
- [+] Automated recon and vulnerability scanning workflows with Python

SOC Analyst L1
2021
Managed Security Services

- [+] Monitored SIEM alerts and triaged security incidents
- [+] Performed initial malware analysis and threat hunting
- [+] Documented incident response procedures and runbooks

// NOTABLE PROJECTS

Threat Intelligence Pipeline
Python · Splunk · STIX/TAXII · Docker
Real-time IOC aggregation reducing analyst triage time by 60%

Web App Pentest Framework
Python · Burp Suite · OWASP
OWASP-aligned automated recon and vuln scanning toolkit

Network Anomaly Detector
Python · Scikit-learn · Zeek
ML model detecting C2 beaconing and lateral movement

OSINT Recon Toolkit
Python · Shodan API · DNS
Pre-engagement attack surface mapping automation

$ echo "Available for red team engagements globally" // oscaropemba@gmail.com github.com/Oscar-Opemba