Cybersecurity Reconnaissance Report – mgas.ke

1. Objective & Scope

This report documents a full passive and semi-active reconnaissance campaign conducted against the public-facing infrastructure of mgas.ke (M-Gas Kenya). The key goals were to: - Identify live subdomains and backend infrastructure. - Discover exposed services, ports, or misconfigurations. - Detect known vulnerabilities using CVE templates and passive intelligence. - Document the external threat surface for review and remediation planning.

2. Environment & Setup

The work was conducted on a Windows machine using WSL2 (Windows Subsystem for Linux) with Ubuntu. Tools installed: Python3, Sublist3r, Go 1.22.2, httpx, Nmap, WhatWeb, Nuclei, Shodan (Web UI).

3. Subdomain Discovery

Tool: Sublist3r Command: python3 sublist3r.py -d mgas.ke Discovered 15 subdomains, including www.mgas.ke, ameyo.mgas.ke, careers.mgas.ke, etc.

4. Live Host Probing

Tool: httpx Command: cat subdomains.txt | httpx -silent -o live-subdomains.txt Confirmed live subdomains were reachable via HTTP(S).

5. Technology Fingerprinting

Tool: WhatWeb Command: whatweb -i live-subdomains.txt --log=whatweb-results.txt Identified Apache servers, WordPress footprints, and exposed server headers.

6. Port & Service Scanning

Tool: Nmap Command: nmap -iL live-subdomains.txt -T4 -oA nmap-results Open ports: 22 (SSH), 80, 443. Data saved in nmap-summary.csv.

7. Vulnerability Scanning

Tool: Nuclei Templates: CVEs, Misconfigurations, Tech Detection Command: cat live-subdomains.txt | nuclei -t cves/ -o nuclei-results.txt Findings include open redirect, outdated jQuery, CORS misconfig, and exposed debug page.

8. Passive Intelligence via Shodan

Tool: Shodan Web Interface Investigated IPs: 3.249.4.230, 34.249.218.154, etc. Findings: OpenSSH 7.4, Apache servers, Cloudflare/Geo info.

9. Security Risk Summary

- SSH exposure across multiple IPs. - Outdated software (e.g., jQuery, OpenSSH). - Publicly available dev/test subdomains. - Fingerprinted tech stacks via headers.

10. Recommendations

- Update OpenSSH versions. - Whitelist SSH access or restrict to VPN. - Limit CORS policies to trusted origins. - Remove or protect dev/test subdomains. - Replace vulnerable JavaScript libraries.

11. Attachments & References

- nmap-summary.csv - mgas-security-report.docx - Mgas_KE_CyberRecon_Report.docx - nuclei-results.txt (raw output)

12. Status & Completion

All planned recon phases are complete. Ready for presentation or integration into threat modeling exercises.

13. Suggested Next Steps

- Patch identified vulnerabilities. - Remove public access to sensitive subdomains. - Perform red-team testing or phishing simulations. - Establish ongoing monitoring or alerts.