

Executive Summary – Kubernetes Penetration Test

Assessment Name:	Pals for Life – Kubernetes Security Assessment
Assessment Type:	External Black-Box Penetration Test
Environment:	Kubernetes-based Infrastructure
Tester:	Toibat Bamigboye

Overview

A penetration test was conducted to evaluate the security posture of a Kubernetes-based environment. The objective was to identify exposed services, misconfigurations, and weaknesses that could be exploited by an external attacker. The assessment simulated real-world attack behavior without prior access or credentials.

Key Findings

- Public exposure of Kubernetes-related services significantly increased the attack surface.
- Security misconfigurations allowed enumeration and discovery of cluster components.
- Weak access controls could enable attackers to escalate privileges and move laterally within the environment.

Business Impact

If exploited in a production environment, the identified weaknesses could lead to unauthorized access to containerized workloads, potential data exposure, service disruption, and full compromise of cloud infrastructure. Such incidents may result in regulatory non-compliance, reputational damage, and operational downtime.

Overall Risk Rating

High – Due to exposed Kubernetes components combined with insecure configurations.

High-Level Recommendations

- Restrict public access to Kubernetes APIs and internal services.
- Enforce strong authentication and least-privilege RBAC policies.
- Harden exposed web services and continuously monitor Kubernetes activity.
- Perform regular security assessments and configuration audits.