Σχεδιασμός και ανάπτυξη πλατφόρμας Capture The Flag σε περιβάλλον Kubernetes

Η διπλωματική εργασία αφορά τον σχεδιασμό και την ανάπτυξη μιας πλατφόρμας Capture The Flag (CTF) για την εκπαίδευση και την πρακτική εξάσκηση σε θέματα κυβερνοασφάλειας. Η πλατφόρμα θα αξιοποιεί το Kubernetes για τη δυναμική δημιουργία, διαχείριση και απομόνωση των περιβαλλόντων εκτέλεσης των προκλήσεων, προσφέροντας επεκτασιμότητα, ευελιξία και ασφάλεια. Στόχος είναι η δημιουργία ενός ολοκληρωμένου συστήματος που θα υποστηρίζει τη διεξαγωγή διαγωνισμών CTF και την εξάσκηση σε τεχνικές εντοπισμού και εκμετάλλευσης ευπαθειών σε ελεγχόμενο περιβάλλον.

Συνοπτικά το σύστημα θα διαθέτει τα ακόλουθα:

Frontend: θα παρέχει το περιβάλλον χρήστη για εγγραφή, σύνδεση, υποβολή/προβολή προκλήσεων, υποβολή flags και παρακολούθηση βαθμολογίας. Πιθανές λύσεις:

- React + FastAPI
- HTML + CSS + JavaScript
- PHP

Backend: υλοποιεί το REST API με το frontend, την επικοινωνία με τη βάση για την αυθεντικοποίηση χρηστών, την επαλήθευση των flags, τη διαχείριση διαγωνισμών και την επικοινωνία με το Kubernetes API[1]. Μέσω του Kubernetes API δημιουργεί ένα Pod ή ένα Deployment, Service και, όπου απαιτείται, προσωρινό δικτυακό endpoint. Κάθε περιβάλλον αποκτά όρια πόρων και χρονικό όριο ζωής.

Βάση δεδομένων: αποθηκεύει τους χρήστες, τις ομάδες, τις προκλήσεις, τα metadata των deployments, τις υποβολές, τη βαθμολογία. Π.χ. PostgreSQL

Kubernetes cluster: τοπικό με Kind[2] ή πολλαπλά VMs με Kubeadm[3]

Docker[4] image για κάθε πρόκληση. Ενδεικτικές προκλήσεις:

- Web πρόκληση SQL Injection ή authentication bypass.
- Linux πρόκληση μέσω SSH ή terminal
- Kubernetes misconfiguration challenge

Ενδεικτικό use case: ο χρήστης πατά «Έναρξη Πρόκλησης»

1. Το frontend στέλνει αίτημα POST /api/challenges/1/start.
2. Το backend ελέγχει τον χρήστη και διαβάζει από τη βάση ποιο image αντιστοιχεί στην πρόκληση.
3. Δημιουργεί τους απαιτούμενους Kubernetes πόρους.
4. Καταχωρίζει στη βάση τη συνεδρία και το αναγνωριστικό των πόρων.
5. Επιστρέφει την κατάσταση εκκίνησης και, όταν είναι διαθέσιμο, το URL του στόχου.

[1] https://kubernetes.io/docs/reference/using-api/
[2] https://kind.sigs.k8s.io/docs/user/quick-start/
[3] https://kubernetes.io/docs/setup/production-environment/tools/kubeadm/create-cluster-kubeadm/
[4] https://docs.docker.com/