

Dynamic Pentest Lab Generator

Building a standardized Azure Pentest Deployment Framework

Graduate



Janosch Bühler



Samuel Maissen



Dante Suwanda

Initial Situation: Hacking-Lab is a platform that provides ethical hacking for educational purposes. The overall goal is to promote awareness in the field of hacking and security. The corresponding challenges are developed in the format of a capture the flag scenario. As it stands, Hacking-Lab leverages Terraform deployments to establish pentest labs in Azure. Each lab, consists of a static Terraform deployment, which is manually developed to suit a specific use-case. This approach, involves a time-intensive process that necessitates manual interventions and several procedures. It also calls for time dedicated to debugging the Terraform deployment. Additionally, it expects the lab creator to possess knowledge of cloud deployments.

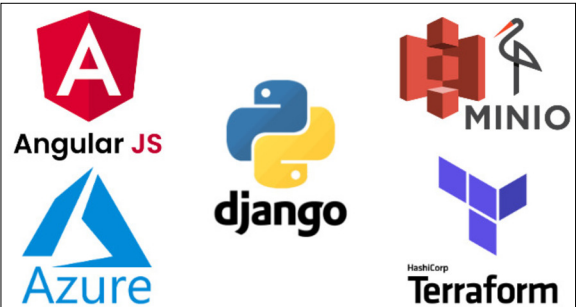
Objective: The objective of this bachelor's thesis is to develop a web application that automates the deployment and configuration of custom pentest lab environments, integrating it into the existing Hacking-Lab infrastructure. The project aims to implement a Visio-like tool that defines the basic infrastructure of a corporate IT network, generating configurations for deployment via Terraform. The solution should simplify the creation of network setups with multiple subnets, deployment of virtual machines and container services. It should include VPN access for students, the possibility to manage communication between resources like a firewall, and DNS resolution for these resources. The tool should offer the ability to use existing Hacking-Lab Docker images and allow virtual machines to be customized. It should also provide options for distributing dynamic flags and setting static or dynamic passwords, enhancing the uniqueness of the labs.

Result: The project successfully established a solid framework for generating pentest labs. This was

achieved using Django for backend operations and Angular for the frontend, ensuring a scalable and maintainable solution. For the deployment part Terraform was used, which dynamically configures and deploys the necessary resources based on the configuration applied in the frontend. The framework integrates seamlessly with Hacking-Lab using SSO authentication.

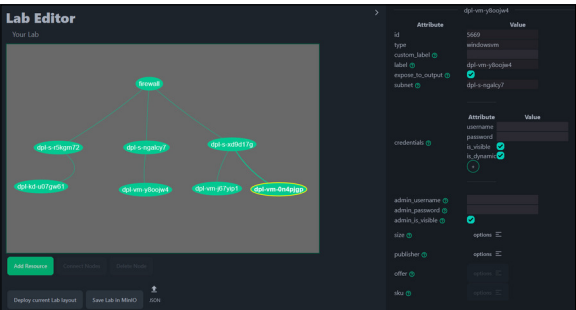
Core Technologies

Microsoft, Angular, Django, HashiCorp, MinIO



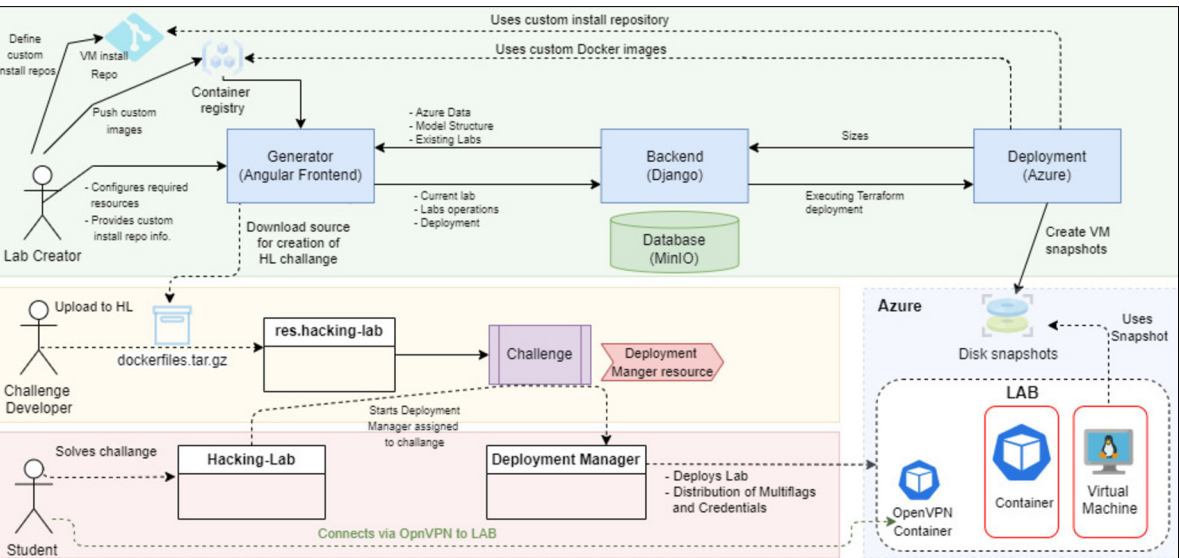
Dynamic Pentest Generator Frontend

Own presentation



Dynamic Pentest Generator System-context

Own presentation



Advisor

Ivan Bütler

Co-Examiner

Daniel Frei, Swiss Reinsurance Company Ltd, Zürich, ZH

Subject Area

Security, Networks, Security & Cloud Infrastructure, Software

Project Partner

Hacking-Lab AG, Jona, SG

