Red Team Report

Red Team vs Blue Team event

Ibrahim Durmus, Rene van Vliet and Rens van der Linden

2020-10-26

Contents

1 Red Team Report

1.1 Introduction

The Red Team report contains all efforts that were conducted in order to test the security of the systems. The purpose of this report is to transfer our findings to the system owner, so he can take action upon this.

1.2 Objective

The objective of this assessment is to perform an internal penetration test against systems developed by the security engineers.

2 Red Team Report - High-Level Summary

We were tasked with performing an internal penetration test towards the systems that have been developed by the security engineers. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate these systems. our overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to the security engineers.

When performing the attacks, we found several misconfiguraitons, and we were able to access a Portainer application which gave us full access to the database, api, etc. due to poor password reusal. These systems as well as a brief description on how access was obtained are listed below:

3 Red Team Report - Findings

- Uses HTTP, so MITM is possible
- When send directly to microservice, no authorization (Happens throug Gateway)
- Password reusal for Portainer

3.0.1 Informational

- JWT doesn't work when scaling because of random signing credentials.
- Latest submit is broken
- After registration no success message

4 Recommendations

- Use https instead of http
- Fix the authorization so it can be bypassed
- Use strong and unique passwords for each service
- Implement a valid solution for the JWT signing credentials so the application is scalable