Research Proposal Thesis: Container Security Pentesting

Joren Vrancken (s4593847)

04 September 2019

1 Introduction

Secura, a company specializing in digital security, wants to research the security of Docker to improve their infrastructure investigations. Because Docker is widely used software, misconfigured or vulnerable instances are a very interesting attack surface. I have experience with both Docker and penetration testing. That makes this a great topic for me to combine both subjects into a research project.

2 Supervision

At Secura Dave Wurtz and Geert Smelt will be my supervisors. Geert will be the main contact for the Radboud and Dave will be my expert supervisor. Erik Poll will be my supervisor at the Radboud.

3 Research Questions

My main research question will be:

> **What is a good methodology to test the security of Docker?**

3.1 Sub-questions

To answer this question I have split the research question into four sub-questions.

- **What are known vulnerabilities in Docker?**
  I will research vulnerabilities and misconfigurations in Docker that might be of interest during a penetration test. Additionally, I will investigate orchestration software (e.g. Kubernetes) that is used to manage Docker clusters.

- **Is it possible to automate vulnerability detection?**
  I will research the automation of vulnerability and misconfiguration detection of Docker and orchestration software.
- **How can Docker penetration testing be incorporated into the existing methodologies at Secura?**
  I will gather requirements from consultants at Secura about their existing methodologies used in penetration testing. I will use the gathered requirements to develop a new methodology on penetration testing of Docker infrastructure.
- **How does the methodology on penetration testing of Docker map to the corresponding Cis baselines?**
  I will map the methodology to relevant Cis baselines.

4 Results

The goal of my research will be to give Secura insight into how they can improve their infrastructure investigations with regards to Docker.