

Hardening Kubernetes Clusters

Reducing Attack Surface in Kubernetes by means of Rootless Containers, Network Policies and Role Based Access Control

Bachelor Thesis

Submitted in partial fulfillment of the requirements for the degree of

Bachelor of Science in Engineering

to the University of Applied Sciences FH Campus Wien

Bachelor Degree Program: Computer Science and Digital Communications

Author:

Guntram Björn Klaus

Student identification number:

c2110475170

Supervisor:

BSc. MSc. Bernhard Taufner

Date:

dd.mm.yyyy

Declaration of authorship:

I declare that this Bachelor Thesis has been written by myself. I have not used any other than the listed sources, nor have I received any unauthorized help.

I hereby certify that I have not submitted this Bachelor Thesis in any form (to a reviewer for assessment) either in Austria or abroad.

Furthermore, I assure that the (printed and electronic) copies I have submitted are identical.

Date:

Signature:

Abstract

(E.g. “This thesis investigates...”)

Kurzfassung

(Z.B. "Diese Arbeit untersucht...")

List of Abbreviations

ARP	Address Resolution Protocol
GPRS	General Packet Radio Service
GSM	Global System for Mobile communication
WLAN	Wireless Local Area Network

Key Terms

GSM

Mobilfunk

Zugriffsverfahren

Contents

1	Introduction	1
1.1	Background: Enterprises and Cloud	2
1.2	Research Objectives	2
1.3	Methodology	3
1.4	Structure	3
2	Concepts	4
2.1	Containervirtualization	4
2.1.1	Linux Kernel	5
2.1.2	Container Images	6
2.1.3	Container Runtimes	7
2.2	Kubernetes	8
2.2.1	Components	8
2.2.2	Cluster Architecture	9
2.2.3	Cluster Objects	10
3	Literature Review	11
3.1	State of the Art	11
3.2	CVE Numbers	12
3.3	Incident Reports	13
4	Hardening Measures	14
4.1	Securing Containers	14
4.1.1	Linux File Permissions	14
4.1.2	Root versus Rootless	15
4.1.3	Rootless Policy Enforcement	16
4.2	Securing the Network	17
4.2.1	Network Policies	17
4.2.2	Service Mesh	18
4.3	Authentication and Authorization	19
4.3.1	Role Based Access Control	19
4.3.2	Kubeconfig Keys and Certificates	20
4.3.3	Service Accounts	21
5	Discussion	22
5.1	Implications for businesses	22
5.2	Tradeoffs and Difficulties	23
5.3	Complexity	23
6	Conclusion	24
7	Outlook / Future work	25
	Bibliography	26

List of Figures	27
List of Tables	28
Appendix	29

1 Introduction

1 Introduction

1.1 Background: Enterprises and Cloud

1.2 Research Objectives

1.3 Methodology

1.4 Structure

2 Concepts

2.1 Containervirtualization

2 Concepts

2.1.1 Linux Kernel

2 Concepts

2.1.2 Container Images

2 Concepts

2.1.3 Container Runtimes

2.2 Kubernetes

2.2.1 Components

2.2.2 Cluster Architecture

2.2.3 Cluster Objects

3 Literature Review

The purpose of this literature review is to explore the scope of vulnerabilities found in Kubernetes environments. Specifically, recurring concepts and common denominators across vulnerabilities shall be identified and discussed. For this, the database of Common Vulnerabilities and Exposures (CVE), the IEEE database, the ACM digital library and the official Kubernetes feed of CVEs are queried using keywords pertaining to Container and Kubernetes Security. The acquired papers, articles and CVE descriptions are skimmed through. the most relevant results are narrowed down and selected for closer inspection. It shall be noted that Kubernetes vulnerabilities do not only entail standard Kubernetes components, but also add-ons deployed on top of 'plain' Kubernetes. Such can be the Nginx Ingress-Controller, a Service-Mesh, CI/CD tools closely embedded into Kubernetes and more. Generally, this can be anything that extends the Kubernetes API through Custom Resource Definitions (CRDs).

According to RedHat's report on the state of Kubernetes security in 2022, yes hello

3.1 State of the Art

3.2 CVE Numbers

3.3 Incident Reports

4 Hardening Measures

4.1 Securing Containers

4.1.1 Linux File Permissions

4 Hardening Measures

4.1.2 Root versus Rootless

4 Hardening Measures

4.1.3 Rootless Policy Enforcement

4.2 Securing the Network

4.2.1 Network Policies

4 Hardening Measures

4.2.2 Service Mesh

4.3 Authentication and Authorization

4.3.1 Role Based Access Control

4.3.2 Kubeconfig Keys and Certificates

4 Hardening Measures

4.3.3 Service Accounts

5 Discussion

5.1 Implications for businesses

5.2 Tradeoffs and Difficulties

5.3 Complexity

6 Conclusion

7 Outlook / Future work

Bibliography

List of Figures

List of Tables

Appendix

(Hier können Schaltpläne, Programme usw. eingefügt werden.)