Container Security

Chih-Hsuan Yang

2020-12-15

National Sun-Yet-San University
Bachelor's degree graduation project
Advisor: Chun-I Fan

Contents

1 Abstract

A research of container's modern cyber security issue. Many companies use container to run their services.
// FIXME

2 Motivation

Container is a virtualization technique to package applications and dependencies to run in an isolated environment. Containers are faster to start up, lighter in memory/storage usage at run time and easier to build up than virtual machines. Because the container share the kernel with the host OS and other containers. I often used to run a docker container to host my services. For example: my homeworks, servers and some services in Information security club at NSYSU. But there are some vulnerabilities about container technique. Like "Dirty CoW[1]" and "Escape vulnerabilities". Hence there is a big problem about: "How to make sure my services are isolated and secure ?" I am the leader of Information security club, I should maintain all the services working perfectly. Moreover we are information security club. Hence the security and performance issue are the top priority requirements.

3 Papers Review

4 Methods

5 Expected Outcome

The PoC code and the solution of a container cyber attack.

6 References

References

[1] Dirty CoW. *Dirty CoW CVE-2016-5195*. URL: https://dirtycow.ninja/.