Annotated Bibliography

Feasibility Demo - Project Artefact

Finlay Reid

CMP400: Honours Project

BSc Ethical Hacking Year 4

2021/22

Note that Information contained in this document is for educational purposes.

.

Contents

.

1.1 INTRODUCTION

THIS DOCUMENT INCLUDES SEVEN PAPERS WHICH HAVE BEEN CRITICALLY APPRAISED IN THE FORMAT OF AN ANNOTATED BIBLIOGRAPHY. HOW THEY ARE RELEVANT TO MY PROJECT AND THE LIMITATIONS OF THE PAPER ARE DISCUSSED, ONE SECTION CONTAINS ALL THE NEW PAPERS AND ANOTHER HAS THE PAPERS THAT WERE INCLUDED IN THE PROJECT PROPOSAL.

.

2 NEW PAPERS

2.1 CLOUD COMPUTING SECURITY ISSUES AND CHALLENGES

Full reference : Kuyoro, S.O., Ibikunle, F. and Awodele, O., 2011. Cloud computing security issues and challenges. *International Journal of Computer Networks (IJCN)*, *3*(5), pp.247-255.

Source : International Journal of Computer Networks

Content : Research article

Summary : The researchers at Babcock university, use data gathered from the IDC enterprise panel to describe the main issues related with cloud computing. The study results highlight how security is the principal concern of users when discussing the cloud model. Undertaken by the IDC, a leading market research company, the study was conducted in 2008 at the IDC enterprise panel. The sample size and composition of the study are unknown, limitations of the study also include its date as cloud computing technology has significantly progressed since the study. The authors make the point that on the one hand security in cloud computing could improve due to its heavy concentration of data and security-focused resources. Overall, the paper confidently highlights the security risks posed to this rapidly developing technology known as cloud computing.

Relevance to project: The paper is relevant to the project as cloud computing is hugely important in containerization and its deployment. They share a lot of the same potential security weaknesses and this paper helped expand my knowledge concerning the issues within cloud computing.

2.2 UNDERSTANDING CONTAINER ISOLATION MECHANISMS FOR BUILDING SECURITY-SENSITIVE PRIVATE CLOUD

Full reference: Babar, M.A. and Ramsey, B., 2017. Understanding container isolation mechanisms for building security-sensitive private cloud. *The University of Adelaide, Australia*.

Source: Report

Content: Technical report

Summary: Researchers at the Centre for Research on Engineering Software Technologies, University of Adelaide published a report analysing the isolation mechanisms found in container technologies: namely Docker, LXD, and rkt. The report was undertaken to ensure security practitioners and researchers had a foundation of knowledge when attempting to secure container environments. In order to make sure the evaluation was carried out sufficiently a 3-step process was applied, identification of isolation mechanism, analysis of isolation mechanism, and improvement of isolation mechanism. Results of the experiment concluded that when looking at isolation from the host’s point of view there is a lot of improvement needed to secure this technology. The report documents the weakness of processes being viewable on particular containers through the ‘systemd init’ system. The report fails to look at other

.

security mechanisms, solely focusing on isolation devices, which would give users a more complete overview of container security.

Relevance to project: The information contained within this report will assist in the creation of the hardening script and security plan. Due to the requirement of an intimate understanding of a container's inner workings and the report provides this by detailing isolation mechanisms.

2.3 VIRTUAL MACHINE ISOLATION

Full reference: Jithin, R. and Chandran, P., 2014, March. Virtual machine isolation. In *International Conference on Security in Computer Networks and Distributed Systems* (pp. 91-102). Springer, Berlin, Heidelberg.

Source: Textbook

Content: Survey paper

Summary: A paper detailing virtual machine isolation was presented at the Second International Conference on Security in Computer Networks and Distributed Systems held in Trivandrum, India, during March 13–14, 2014. The paper at its core studies the main concerns with virtualization technology, including an exanimation of different exploits and attack vectors. The study was undertaken to shed light on the main security vulnerabilities within virtualization and the steps necessary to mitigate the risks posed by these weaknesses. A strength of the paper is the level of detail the authors cover each architectural limitation and its helpful categorization of each of the potential methods of security compromisation. One small drawback of the report is in its failure to include many diagrams, relying on large blocks of text to explain its concepts and the overall readability could be improved. However, this report is exceedingly well researched and versed in virtual machine security.

Relevance to project: The aforementioned report discussing virtual machine security is pertinent to my project as virtual machines are closely linked with containers. Furthermore, the creation of the clean Kubernetes cluster was completed on a virtual machine. Ultimately both are forms of virtualization.

2.4 'UNDER-REPORTED 'SECURITY DEFECTS IN KUBERNETES MANIFESTS

Full reference: Bose, D.B., Rahman, A. and Shamim, S.I., 2021, June. 'Under-reported'Security Defects in Kubernetes Manifests. In *2021 IEEE/ACM 2nd International Workshop on Engineering and Cybersecurity of Critical Systems (EnCyCriS)* (pp. 9-12). IEEE.

Source: Workshop

Content: Research paper

Summary: In this paper, the authors investigate how security weaknesses routinely appear within Kubernetes implementations and develop the best security practices for Kubernetes from this acquired knowledge. Researchers at the Tennessee Technological University performed a qualitative analysis

.

utilizing 5,193 commits, that were coalesced through 38 open source repositories to demonstrate that weaknesses related to security are wholly under discussed and researched. A drawback of the paper includes the bias of the methods used to obtain the results, due to the open source repositories being not only the authors but the subjects of the experiment. The research conducted, however, is effective in demonstrating how under-researched Kubernetes security remains even today.

Relevance to project: The research carried out inside this paper is beneficial to researchers and the project, as it describes the Under-reported' Security Defects in Kubernetes through scientific analysis. Providing data that will assist in writing the Kubernetes hardening guide

.

3 PROJECT PROPOSAL PAPERS

3.1 ELIMINATING PRIVILEGE ESCALATION TO ROOT IN CONTAINERS RUNNING ON KUBERNETES

Full reference: Artem, L., Tetiana, B., Larysa, M. and Vira, V., 2020. Eliminating privilage escalation to root in containers running on Kubernetes. *Scientific and practical cyber security journal*.

Source: Journal

Content: Research paper

Summary: The following paper undertakes a study into container privilege escalation attacks and develops a mitigation plan derived from the results of the study. Researchers at the University of Kyiv describe the steps taken to escalate privileges on a Kubernetes container running a kubelet version of v1.13.6 and v1.14.2, further describing the measures taken to ensure the security vulnerability is negligible. Furthermore, the paper describes the individual Kubernetes components in depth during its 'kubernetes basics' section. The main limitation present, is the failure to walkthrough any additional methods of privilege escalation, at most describing a technique that exploits a vulnerability when running a process as a mem cache user. To a certain extent this paper describes container escalation attacks effectively, however, it fails to cover the exploits as thoroughly as the preceding papers.

Relevance to project: Research contained within the background, escalation method and mitigation sections discuss important information which will assist in the development of the in-depth security plan and the analysation of container-based exploits. This paper particularly was useful when constructing the Kubernetes diagrams in the other artifact.

3.2 A MEASUREMENT STUDY ON LINUX CONTAINER SECURITY: ATTACKS AND COUNTERMEASURES

Full reference: Lin, X., Lei, L., Wang, Y., Jing, J., Sun, K. and Zhou, Q., 2018, December. A measurement study on linux container security: Attacks and countermeasures. In *Proceedings of the 34th Annual Computer Security Applications Conference* (pp. 418-429).

Source: Conference

Content: Study paper

.

Summary: In this paper, a measurement study is conducted on Linux container security through the use of exploits. Researchers at several educational bodies including the George Mason University, University of Chinese Academy of Science, and the CAS Institute of Information Engineering classify 223 container exploits into specific categories through the use of a two-dimensional attack taxonomy. A limitation of the paper is in the provided method to mitigate privilege escalation attacks, as the measures can be easily circumvented through other types of attacks such as container breakout. Another limitation of the paper is the failure to analyze other attack vectors, as privilege escalation is solely examined and discussed. This study completes a thorough analysis of privilege escalation attacks and effectively classifies relevant container exploits.

Relevance to project: The paper provides a list of successful and failed exploits which will assist in the development of the hardening script. It also describes the internal Linux security mechanisms and how docker interacts with these, providing good knowledge that will assist when utilizing the container runtime software docker.

3.3 XI Commandments of Kubernetes Security: A Systematization of Knowledge Related to Kubernetes Security Practices

Full reference: Shamim, M.S.I., Bhuiyan, F.A. and Rahman, A., 2020, September. XI Commandments of Kubernetes Security: A Systematization of Knowledge Related to Kubernetes Security Practices. In 2020 IEEE Secure Development (SecDev) (pp. 58-64). IEEE.

Source: Journal

Content: Technical paper

Summary: The following paper aims to provide security practitioners with a systemization of knowledge to assist in securing Kubernetes containers. Researchers at the Dept. of Computer Science Tennessee Technological University use data gathered from 104 Internet artifacts to systemize Kubernetes security knowledge through analysation. This includes blog posts and video presentations rather than academic forums. A limitation of the paper involves the possibility of bias from one of the authors due to his previous experience using Kubernetes, as he has his own assumptions and beliefs pertaining to Kubernetes security. Another limitation is related to the presumption that security information will be missed, on blog posts, presentations, and textbooks. Overall, this paper excellently coalesces the most critical information and security practices related to Kubernetes.

Relevance to project: The research contained within this document is useful to my project as it collates all the important security practices which will assist in the creation of the in-depth security plan. Furthermore, it includes a host of effective security measures that mitigate the risk posed by container exploitation

.