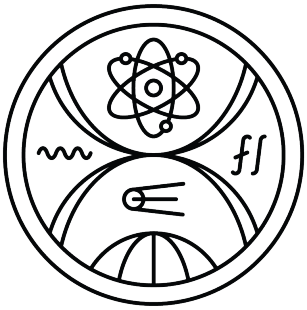
COMENIUS UNIVERSITY IN BRATISLAVA
FACULTY OF MATHEMATICS PHYSICS AND INFORMATICS

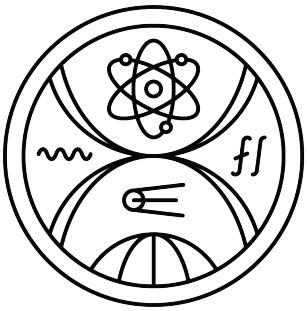


KUBERNETES SECURITY ASSESSMENT

Master thesis

2023 Bc. Pavel Semenov

COMENIUS UNIVERSITY IN BRATISLAVA
FACULTY OF MATHEMATICS PHYSICS AND INFORMATICS



KUBERNETES SECURITY ASSESSMENT

Master thesis

Study program:	Applied informatics
Branch of study:	Applied informatics
Department:	Department of Applied Informatics
Supervisor:	RNDr. Richard Ostertág, PhD.

Bratislava, 2023 Bc. Pavel Semenov

Comenius University Bratislava
Faculty of Mathematics, Physics and Informatics

THESIS ASSIGNMENT

Name and Surname: Bc. Pavel Semenov
Study programme: Applied Computer Science (Single degree study, master II. deg., full time form)
Field of Study: Computer Science
Type of Thesis: Diploma Thesis
Language of Thesis: English
Secondary language: Slovak

Title: Kubernetes security assessment

Annotation: Kubernetes has been gaining popularity rapidly in recent years as more and more enterprise solutions are subjected to cloud transformation and more companies are looking for the ways to increase development efficiency and reduce development costs. This brings new concerns from clients and stakeholders about the security of Kubernetes and its exposure to cyber-attacks.

Aim:

This thesis studies, compares and evaluates the state-of-the-art tools designed to discover vulnerabilities concerning the cluster configuration, running pods or cluster itself. Assessment is carried out in both local cluster setup predisposed with multiple vulnerabilities and real-world enterprise cloud infrastructure. Based on the assessment results we intend either to improve one of the existing tools or develop a Kubernetes security framework of our own, which will be able to provide better results in addressing the cluster security.

Literature:

V. B. Mahajan and S. B. Mane, "Detection, Analysis and Countermeasures for Container based Misconfiguration using Docker and Kubernetes", 2022 International Conference on Computing, Communication, Security and Intelligent Systems (IC3SIS), 2022, pp. 1-6, doi: 10.1109/IC3SIS54991.2022.9885293. https://ieeexplore.ieee.org/document/9885293

D. B. Bose, A. Rahman and S. I. Shamim, "'Under-reported' Security Defects in Kubernetes Manifests", 2021 IEEE/ACM 2nd International Workshop on Engineering and Cybersecurity of Critical Systems (EnCyCriS), 2021, pp. 9-12, doi: 10.1109/EnCyCriS52570.2021.00009. https://ieeexplore.ieee.org/document/9476056

Castillo Rivas, D.A., Guamán, D. (2021). "Performance and Security Evaluation in Microservices Architecture Using Open Source Containers". In: Botto-Tobar, M., Montes León, S., Camacho, O., Chávez, D., Torres-Carrión, P., Zambrano Vizuete, M. (eds) Applied Technologies. ICAT 2020. Communications in Computer and Information Science, vol 1388. Springer, Cham. https://doi.org/10.1007/978-3-030-71503-8_37

Clinton Cao, Agathe Blaise, Sicco Verwer, and Filippo Rebecchi (2022). "Learning State Machines to Monitor and Detect Anomalies on a Kubernetes Cluster". In Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES '22). Association for Computing Machinery, New York, NY, USA, Article 117, 1–9. https://doi.org/10.1145/3538969.3543810

Comenius University Bratislava
Faculty of Mathematics, Physics and Informatics

Supervisor:	RNDr. Richard Ostertág, PhD.
Department:	FMFI.KI - Department of Computer Science
Head of department:	prof. RNDr. Martin Škoviera, PhD.
Assigned:	07.12.2022
Approved:	07.12.2022

prof. RNDr. Roman Ďurikovič, PhD.
Guarantor of Study Programme

.....
Student

.....
Supervisor

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta: Bc. Pavel Semenov
Študijný program: aplikovaná informatika (Jednoodborové štúdium, magisterský II. st., denná forma)
Študijný odbor: informatika
Typ záverečnej práce: diplomová
Jazyk záverečnej práce: anglický
Sekundárny jazyk: slovenský

Názov: Kubernetes security assessment
Testovanie bezpečnosti Kubernetes

Anotácia: Kubernetes v posledných rokoch rýchlo získava na popularite, pretože čoraz viac spoločností hľadá spôsoby, ako zvýšiť efektivitu vývoja a znížiť náklady na vývoj. Táto zvýšená popularita so sebou prináša väčšie vystavenie kybernetickým útokom a zvýšené obavy zainteresovaných strán o bezpečnosť Kubernetes.

Cieľ: Cieľom práce je porovnať a zhodnotiť moderné nástroje určené na odhaľovanie zraniteľností týkajúcich sa konfigurácie klastra, bežiacich podov alebo aj samotného klastra. Posúdenie bude prebiehať na lokálnom klastri s prednasadenými viacerými zraniteľnosťami, ako aj v reálnej podnikovej cloudovej infraštruktúre. Na základe výsledkov hodnotenia máme v úmysle buď vylepšiť niektorý z existujúcich nástrojov, alebo vyvinúť vlastný bezpečnostný rámec pre Kubernetes, ktorý bude schopný poskytnúť lepšie výsledky pri riešení klastrovej bezpečnosti.

Literatúra:
V. B. Mahajan and S. B. Mane, "Detection, Analysis and Countermeasures for Container based Misconfiguration using Docker and Kubernetes", 2022 International Conference on Computing, Communication, Security and Intelligent Systems (IC3SIS), 2022, pp. 1-6, doi: 10.1109/IC3SIS54991.2022.9885293. https://ieeexplore.ieee.org/document/9885293

D. B. Bose, A. Rahman and S. I. Shamim, "'Under-reported' Security Defects in Kubernetes Manifests", 2021 IEEE/ACM 2nd International Workshop on Engineering and Cybersecurity of Critical Systems (EnCyCriS), 2021, pp. 9-12, doi: 10.1109/EnCyCriS52570.2021.00009. https://ieeexplore.ieee.org/document/9476056

Castillo Rivas, D.A., Guamán, D. (2021). "Performance and Security Evaluation in Microservices Architecture Using Open Source Containers". In: Botto-Tobar, M., Montes León, S., Camacho, O., Chávez, D., Torres-Carrión, P., Zambrano Vizuete, M. (eds) Applied Technologies. ICAT 2020. Communications in Computer and Information Science, vol 1388. Springer, Cham. https://doi.org/10.1007/978-3-030-71503-8_37

Clinton Cao, Agathe Blaise, Sicco Verwer, and Filippo Rebecchi (2022). "Learning State Machines to Monitor and Detect Anomalies on a Kubernetes Cluster". In Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES '22). Association for

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

Computing Machinery, New York, NY, USA, Article 117, 1–9. https://doi.org/10.1145/3538969.3543810

Vedúci: RNDr. Richard Ostertág, PhD.
Katedra: FMFI.KI - Katedra informatiky
Vedúci katedry: prof. RNDr. Martin Škoviera, PhD.

Spôsob sprístupnenia elektronickej verzie práce:
bez obmedzenia

Dátum zadania: 07.12.2022

Dátum schválenia: 07.12.2022 prof. RNDr. Roman Ďurikovič, PhD.
garant študijného programu

.....
študent

.....
vedúci práce

I hereby declare that I have written this thesis by myself, only with help of referenced literature, under the careful supervision of my thesis advisor.

.....

Bratislava, 2023 Bc. Pavel Semenov

Acknowledgement

Abstract

Kubernetes has been gaining popularity rapidly in recent years as more and more enterprise solutions are subjected to cloud transformation and more companies are looking for the ways to increase development efficiency and reduce development costs. This brings new concerns from clients and stakeholders about the security of Kubernetes and its exposure to cyber-attacks. This thesis studies, compares and evaluates the state-of-the-art tools designed to discover vulnerabilities concerning the cluster configuration, running pods or cluster itself. Assessment is carried out in both local cluster setup predisposed with multiple vulnerabilities and real-world enterprise cloud infrastructure. Based on the assessment results we intend either to improve one of the existing tools or develop a Kubernetes security framework of our own, which will be able to provide better results in addressing the cluster security.

Keywords: space debris, machine learning, space object classification

Abstrakt

Zvýšený záujem o vesmírne aktivity spôsobil vznik vesmírneho odpadu obiehajúceho okolo Zeme. V posledných rokoch však vesmírny odpad predstavuje veľmi nebezpečný problém, ktorý môže ľahko ohroziť budúce vesmírne misie. Aby sa predišlo tomuto problému, je nevyhnutné pravidelné sledovanie a detekcia vesmírneho odpadu. Snímky získané z astronomických pozorovaní vesmírneho odpadu je potrebné spracovať a analyzovať, aby sme identifikovali astronomické objekty. Snímky zachytávajú signály z rôznych zdrojov. Od šumu spôsobeného nedokonalosťami CCD čipu, cez defekty spôsobené vonkajšími zdrojmi, alebo pozadím oblohy až po skutočné astronomické objekty, ako sú hviezdy, galaxie alebo objekty slnečnej sústavy (vesmírny odpad, satelity, kométy atď.) Na správnu identifikáciu objektov, je potrebné obrázky najskôr očistiť od nežiadúcich efektov alebo navrhovaný algoritmus musí byť dostatočne robustný, aby sa zameral iba na signály zo skutočných astronomických objektov.

Na základe rozsiahleho výskumu analyzujúceho rôzne existujúce riešenia sme sa rozhodli použiť konvolučnú neurónovú sieť na vyriešenie úlohy klasifikácie vesmírnych objektov. V našej práci sme navrhli architektúru siete a prešli rozsiahlym procesom ladenia hyperparametrov. Aby sme sieť natrénovali a zároveň zabezpečili, že dáta sú robustné a vyvážené, generujeme syntetické snímky pomocou nášho vlastného generátora dát - starGen. Výkonnosť nášho modelu je vyhodnotená na reálnych dátach získaných z Astronomického a Geofyzikálneho observatória v Modre. Na zlepšenie výkonu tiež používame malé množstvo reálnych dát v kombinácii s technikami augmentácie na doladenie nášho modelu. V záverečnej časti porovnávame výkon nášho modelu s najmodernejšou sieťou ResNet-18.

Kľúčové slová: vesmírny odpad, strojové učenie, klasifikácia vesmírnych objektov

Contents

List of Figures

List of Tables