

Ministerul Educației, Culturii și Cercetării al Republicii Moldova

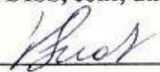
Universitatea Tehnică a Moldovei

Facultatea Calculatoare, Informatică și Microelectronică

Departamentul Informatică și Ingineria Sistemelor

Admis la susținere

Șef de DISS, conf. univ., dr.





“09” 01 2019

**Managementul vulnerabilităților într-un
sistem bazat pe containere Docker**

TEZĂ DE MASTER ÎN

Calculatoare și Rețele Informaționale

Masterand: Igor Toșpan 

Conducător: Mariana Vichre 

Chișinău – 2019

CUPRINS

INTODUCERE.....	5
1.TEHNOLOGIA DOCKER SI RISCURILE INFORMAȚIONALE	6
1.1 Microservicii și virtualizarea bazată pe containere	6
1.1.1Chroot și jail	6
1.1.2.Namespace	8
1.1.3.Control groups	9
1.1.4.Virtualizarea în mediul informațional	10
1.1.5.Diferența între containerele Docker și mașină virtuală	12
1.2.Riscurile informaționale într-un mediu virtualizat	13
1.3. Vulnerabilitățile infrastructurilor cibernetice	15
1.4.Vulnerabilitatile aplicatiilor web rulate in containerul Docker	16
2. RISCURILE INFORMAȚIONALE ÎN MEDIUL DOCKER	20
2.1. Riscurile în imaginile de bază	20
2.2. Riscurile registrelor de imagini	22
2.3. Riscurile sistemului de orchestrare	23
2.4. Riscurile containerelor	24
2.5. Riscurile sistemului de operare gazdă	26
2.6. Remedierea vulnerabilităților	28
3. MANAGEMENT VULNERABILITĂȚILOR ÎN MEDIUL DOCKER	31
3.1. Managementul vulnerabilităților la nivel de cluster Kubernetes	35
3.2. Managementul vulnerabilităților la nivelde container.....	38
3.3 Managementul vulnerabilităților la nivel de registre de imagini Docker	43
3.4. Semnarea digitală a imaginilor Docker	46
3.5 Managementul vulnerabilităților la nivel de aplicație	48
CONCLUZII GENERALE ȘI RECOMANDĂRI.....	61
BIBLIOGRAFIE.....	62
ANEXE.....	67

ADNOTARE

**La teza de master: „Managementul vulnerabilităților într-un sistem bazat pe containere Docker”,
elaborat de Igor Tarpan, Chișinău, 2018.**

Cuvinte cheie: vulnerabilitate, virtualizare, test de penetrare, securitate, riscuri informaționale, Docker.

Lucrarea de față are drept scop studierea procesului de managementul vulnerabilităților și altor riscuri informaționale în mediu virtualizat, unde aplicațiile și/sau servicii sunt rulate cu ajutorul tehnologiei de containerizare Docker.

Tehnologiile utilizate sunt: Docker, care oferă virtualizarea și separarea resurselor mai eficientă a unui sistem de operare pe bază de Linux, posibilitatea de creare a mediilor independente fără utilizarea ”stratului” adăugător de tip hypervisor, utilizând doar componentele nucleului Linux.

Kubernetes ce este un instrument de gestionare și orchestrare a containerelor Docker într-un cluster de servere. Kubernetes realizează o separare între serverele pe care este instalat un sistem de operare pe bază de Linux și aplicațiile care gestionează intercomunicarea ntr servere. De asemenea pentru analiza vulnerabilităților și asigurarea securității informaționale la toate nivele sistemului sunt folosite următoarele:

- Clair – instrument pentru scanarea vulnerabilităților unui container Docker din baza unica CVE;
- Anchore – serviciu de scanare a vulnerabilităților în registre de imagini Docker;
- Notary – semnarea digitală a imaginilor Docker pentru asigurarea integrității și excluderea modificării neautorizate a imaginilor;
- OWASP Zap Proxy – instrument de detectare riscurilor și vulnerabilităților în aplicațiile web.

Memoriul explicativ conține: Introducere, 3 capitole, concluzii, bibliografie cu 42 titluri, dintre care 65 pagini text de bază, 31 figuri.

Capitolul 1 descrie tehnologiile de virtualizare în containere, principiul de microservicii și riscurile informaționale ce persistă în mediul cibernetic.

Capitolul 2 definește riscurile informaționale ce sunt prezente în componentele și serviciile folosite în mediul Docker, cum ar fi: imaginile de bază, sistemele de orchestrare, registrele de imagini și sistemele de operare gazdă.

Capitolul 3 prezintă managementul vulnerabilităților și riscurilor informaționale cu ajutorul tehnologiilor și serviciilor descrise, ce oferă mitigarea riscurilor descrise în Capitolul 2 și oferirea securității informaționale la toate etapele de dezvoltare și mediile de rulare a aplicațiilor pe bază de Docker.

ANNOTATION

**In the master thesis " Vulnerability Management in a Docker Container System ",
elaborated by Igor Tarpan, Chisinau, 2018.**

Keywords: vulnerability, virtualization, penetration test, security, information risks, Docker..

This paper aims to study the process of managing vulnerabilities and other informational risks in a virtualized environment, where applications and / or services are run with Docker container technology.

The technologies used are: Docker, which provides virtualization and resource separation of a Linux-based operating system, the ability to create independent media without the use of the hypervisor-type "layer" using only the Linux kernel constraints.

Kubernetes is a tool for managing and orchestrating Docker containers in a cluster of servers. Kubernetes makes a separation between the Linux-based servers which have installed the applications that manage the intercommunication between the servers. Also for vulnerability scanning and ensuring information security at all levels of the system, the following tools are used:

- Clair - a tool for scanning the vulnerabilities of a Docker container from the CVE base;
- Anchor - Docker image vulnerability scanning service;
- Notary - digital signing service of Docker images for integrity checking and exclusion of unauthorized access to the images;
- OWASP Zap Proxy - a tool for detecting risks and vulnerabilities in web applications.

The explanatory memo contains: Introduction, 3 chapters, conclusions, bibliography with 52 titles, of which 81 basic text pages, 20 figures, 6 tables.

Chapter 1 describes container virtualization technologies, the principle of microservices, and the cybernetic information risks that persist in them.

Chapter 2 defines the information risks that are present in components and services used in the Docker environment, such as: basic images, orchestration systems, image registers, and host operating systems.

Chapter 3 presents information vulnerability and risk management with the technologies and services described, which provides the risk mitigation described in Chapter 2 and provides information security at all development stages and Docker-based environments.