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.

"03" 01 2019

Managementul vulnerabilităților într-un sistem bazat pe containere Docker

TEZĂ DE MASTER ÎN

Calculatoare și Rețele Informaționale

Masterand: Igor Toropov

Conducător: Moraru Viorel

Chișinău – 2019

CUPRINS

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 managemetul 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” adaugător de tip hypervisor, utilizind doar conponentele 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 vulnerablităților unui container Docker din baza unica CVE;
- Anchore – servicu de scanare a vulnerabilităților în registre de imagini Docker;
- Notary – semnarea digitală a imaginelor Docker pentru asigurarea integrității și excluderea modificării neautorizate a imaginelor;
- OWASP Zap Proxy – instrument de detectare riscurilor și vulnerabilităților în aplicașiile web.

Memoriul explicativ conţine: 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: imaginele de bază, sistemele de orchestrare, registrele de imagini și sistemele de operare gazdă.

Capitolul 3 prezintă managementul vulnerabilităților și riscurilor informaționale cu ajutorul tehnologielor 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.