ANÁLISE DE SEGURANÇA EM CONTÊINERES DOCKER ORIENTADA A INFRAESTRUTURA[1]

Nikolas Jensen[2], Charles Christian Miers[3].

[1] Vinculado ao projeto "Análise de segurança de recursos virtualizados em nuvens computacionais IaaS baseadas em OpenStack usando honeypots de baixa interatividade"
[2] Acadêmico (a) do Curso de Ciências da Computação – CCT – Bolsista PROBITI
[3] Orientador, Departamento de Ciências da Computação – CCT – charles.miers@udesc.br

O uso sistemas virtualizados vem crescendo desde sua criação. Neste contexto, surgem os contêineres como uma alternativa mais leve às já consagradas máquinas virtuais. O uso de contêineres começou a aumentar rapidamente desde a sua primeira utilização em 2015 com o Docker, sendo que as empresas rapidamente reconheceram a importância de contêineres em novos modelos de aplicações nativas para nuvem baseadas em microsserviços. O uso de contêineres traz diversos benefícios aos sistemas computacionais, uma vez que, utilizam menos recursos que uma máquina virtual, e, consequentemente, são tendem a ter mais eficiência. Os contêineres propiciam uma portabilidade aos sistemas, sendo que a imagem do contêiner por si só já contém o necessário para a execução da aplicação. Com diversas empresas adotando o uso de contêineres e, com isso, sistemas cada vez mais complexos, torna-se demasiadamente difícil coordenar todos os componentes do sistema utilizando somente o ser humano. Neste contexto, surgem os orquestradores de contêineres auxiliando a administrar sistemas de forma eficiente e dinâmica, e oferecendo diversos recursos para auxiliar os desenvolvedores/administradores. Porém, os orquestradores podem aumentar a superfície de ataque, uma vez que adicionam mais recursos e estes podem ser explorados por atacantes. O orquestrador de contêineres mais popular atualmente é o Kubernetes, seguido pelo Docker Swarm e Apache Mesos. Todos estes orquestradores citados possuem vulnerabilidades conhecidas. Assim, caso se encontrem desatualizados, é mais fácil para um atacante explorá-las. Por outra perspectiva, a existência de uma rede interna no orquestrador destinada ao gerenciamento dos nós pode representar um perigo, visto que um atacante pode conseguir atacar outras partes do sistema por meio de um movimento lateral, explorando vulnerabilidades na rede, ou até mesmo, nos contêineres. Por meio da identificação das três partes da superfície de ataque dos orquestradores, sendo estas: *Application Programming Interface* (API), contêiner e aplicação, é possível identificar pontos de falha do sistema para aprimorar sua segurança contra possíveis invasores ou atacantes. A Tabela 1 foi elaborada durante as pesquisas com a lista as principais falhas dos três orquestradores pesquisados e que foram reportadas a principal base, a *Common Vulnerabilities Exposure* (CVE), mantida pelo MITRE. Por outro lado, há a necessidade de organizar e compreender os principais aspectos de segurança e com esse intuito foi elaborada uma nova taxonomia voltada para contêineres (Figura 1).

Palavras-chave: Orquestradores de contêineres. Vulnerabilidades. Análise de segurança.

	Kubernetes	Docker Swarm	Apache Mesos
Negação de serviço	CVE-2019-11248, CVE-2019-11253, CVE-2020-8557, CVE-2020-8552, CVE-2020-8551, CVE-2019-11254,	CVE-2016-6595 CVE-2017-14992 CVE-2019-16884 CVE-2021-21285	CVE-2017-7687 CVE-2017-9790 CVE-2018-1330
Acesso a dados sensíveis	CVE-2019-11248, CVE-2015-7528, CVE-2018-1002100, CVE-2019-11250, CVE-2019-11243, CVE-2020-8566, CVE-2020-8564, CVE-2019-11252	CVE-2014-5277 CVE-2015-3630 CVE-2019-5736 CVE-2018-15664	CVE-2018-8023
Acesso não autorizado	CVE-2016-7075, CVE-2019-11248, CVE-2016-1905, CVE-2017-1002102, CVE-2019-11245, CVE-2020-8559, CVE-2020-8558, CVE-2020-8555, CVE-2019-11251, CVE-2020-8554	CVE-2014-5277 CVE-2016-9962 CVE-2018-15514 CVE-2014-5282 CVE-2019-5736	CVE-2018-1000420, CVE-2019-0204
Execução de código arbitrário	CVE-2016-1906, CVE-2018-1002101, CVE-2019-1002101	CVE-2014-5282 CVE-2019-5736 CVE-2014-0048	CVE-2019-0204
Executar ações não autorizadas	CVE-2019-11247	CVE-2014-5278	não identificado

Tabela 1. CVEs de cada orquestrador, identificadas até 26/07/2021.

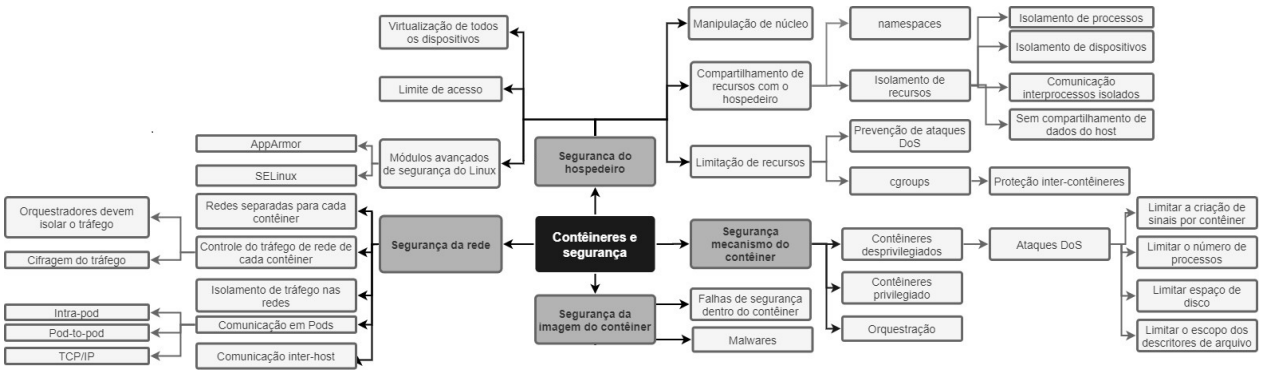

Figura 1. Taxonomia da segurança de contêineres.