Abstract

Containerization technology is an alternative in virtualization. Docker requires a docker daemon to build, distribute, and run containers so it makes the docker unsafe because the docker daemon is vulnerable to attack by the surface attacks (Docker Daemon Attack Surface). The attack is an attack on the docker daemon which takes over access (root). Prevention of attacks is done using by rootless mode. In this final project, docker daemon attack surface is prevented by creating and running a docker image and then preventing the attack using the docker in a rootless mode so the attack fails. Proof that the attack was successful is that the user can access the /etc/shadow file, which should only be accessible by users who have root privileges. Obtained a statement that the file cannot be accessed if the docker is running in rootless mode. To measure whether the use of the rootless mode on this docker adds to the burden of CPU usage and how much it increased, the CPU usage is measured when an attack is carried out with a docker that is run through root and rootless mode permissions. Obtained CPU usage results of 39% when using the docker with rootless mode. Whereas using a docker with root privileges is only 0%. The increase that occurred by 39% is an increase commensurate with its benefits that can prevent docker daemon attack surface.

Keywords: docker, container, daemon, rootless, root, privilege.