Abstrak

Teknologi *containerization* menjadi salah satu alternatif dalam virtualisasi. Docker membutuhkan *docker daemon* untuk membangun, mendistribusikan, dan menjalankan *container* sehingga membuat docker tidak aman karena *docker daemon* rentan terserang oleh serangan permukaan (*Docker Daemon Attack Surface*). Serangan tersebut ialah serangan terhadap *docker daemon* yang mengambil alih akses (*root*). Pencegahan serangan dilakukan menggunakan *rootless mode*. Dalam tugas akhir ini, dilakukan pencegahan serangan *docker daemon attack surface* dengan membuat dan menjalankan *docker container* lalu mencegah serangan tersebut menggunakan *docker* dalam *rootless mode* sehingga seragan gagal dilakukan. Pembuktian bahwa serangan berhasil ialah pengguna dapat mengakses file /etc/shadow yang seharusnya file tersebut hanya dapat diakses oleh *user* yang mempunyai hak akses *root*. Didapatkan pernyataan bahwa file tersebut tidak dapat diakses jika docker dijalankan dengan *rootless mode*. Untuk mengukur apakah penggunaan *rootless mode* pada docker ini menambah beban CPU *usage* dan seberapa besar peningkatannya, maka dilakukan pengukuran CPU usage saat serangan dilakukan dengan docker yang dijalankan melalui hak akses root dan *rootless mode*. Didapatkan hasil penggunaan CPU sebesar 39% saat menggunakan docker dengan *rootless mode*. Sedangkan menggunakan docker dengan hak akses root hanya sebesar 0%. Peningkatan yang terjadi sebesar 39% merupakan peningkatan yang sepadan dengan keuntungannya yang dapat mencegah serangan *docker daemon attack surface*.

Kata kunci : docker, *container*, *daemon*, *rootless*, *root*, *privilege*.