Тема за проект : Систем за детекција на Bruteforce напад

Константина Сарваноска 201519

Системот ќе собира логови за успешни и неуспешни сесии и логирање кон некој сервер. Ова е налик на систем на кој се логираат вработени на една компанија секојдневно, но наместо само на една апликација, ќе се симулираат сите обиди за логирање на повеќе апликации.

За зачувување на интегритетот на лозинките, тие нема да се содржат во логовите, само портата низ која е направен обидот за логирање, timestamp, и статус на логирањето - успешно или безуспешно. Тука постои можност за додавање дополнителни информации во логот, како на пример типот на систем од кој се логира корисник, корисничкото име, IP адреса, производител на уред и слично, за да се прецизира обидот или можниот напад.

Сакам да имплементирам систем кој ќе ги брои овие обиди и сите оние кои се безуспешни и ќе надминат одреден број (на пример 5 безуспешни обиди за логирање по ред) ќе бидат маркирани како обид за упад на систем.

Ова е систем кој ќе собира податоци како lastlog датотеката во Linux дистрибуциите, но од повеќе машини.

Овој систем би се состоел од клиенти (Producers) кои ќе користат класа LogGenerator за креирање на многубројни логови кои ќе се испраќаат преку RabbitMQ до еден Consumer каде тие логови ќе се анализираат и класификуваат како напади доколку има одреден број последователни бесуспешни обиди за логирање.

Декември 2023