Rancang bangun dan implementasi IDS (intrusion detection system) server dan sistem monitoring berbasis web pada network admission control (NAC) untuk meningkatkan keamanan jaringan = Design and implementation of Intrusion Detection System (IDS) server and web based monitoring system on Network Admission Control (NAC) for improving the network security

Taufik Wicaksono, author

Abstrak

Kebutuhan akan akses internet dewasa ini sangat tinggi, hal ini mengakibatkan peningkatan permintaan akses ke jaringan yang aman semakin tinggi. Keadaan ini menuntut admin jaringan agar lebih selektif dalam memperbolehkan user melakukan akses ke jaringan. Setelah proses seleksi awal pada user admin jaringan juga bertugas untuk memproteksi user dari gangguan yang dilakukan user lain atau dari akses luar jaringan. Konsep jaringan seperti ini menjadi dasar munculnya konsep jaringan NAC. Network Admission Control (NAC) adalah teknologi keamanan jaringan komputer dimana client komputer harus melakukan autentifikasi sebelum diperbolehkan mengakses jaringan. Salah satu teknologi NAC yang terkenal adalah Cisco NAC (C-AC).
Terdapat dua fasilitas utama yang dimiliki oleh NAC server yaitu policy server dan IDS server. Policy server bertugas untuk melakukan authentifikasi terhadap user yang akan mengakses ke network devices jaringan. IDS server bertugas untuk melakukan deteksi terhadap serangan yang terjadi terhadap server, sehingga server dapat memberikan peringatan dan kemudian dapat menghentikan serangan. IDS server juga memiliki kemampuan untuk memberikan peringatan melalui SMS dan memiliki fasilitas monitoring serangan melalui web. IDS Server dibuat menggunakan operating system Linux. Sistem ini dibagi menjadi beberapa modul yaitu IDS software yaitu snort, report modul yaitu BASE, dan client - server modul yang bertugas mengirimkan alerting kepada policy server . Sementara network devices yang digunakan pada arsitektur jaringan ini adalah sebuah switch dan router.
Pengujian sistem dilakukan dengan melakukan beberapa variasi serangan terhadap server yaitu denial of service (DOS), port scanning, dan ICMP flood. Dari server akan diambil parameter response time dan action time. Pengujian juga membandingkan nilai response time apabila menggunakan 1 client dan 5 client. Apabila penyerangan menggunakan 5 client menyebabkan adanya penuruan response time sebesar 64.81% apabila dilakukan penyerangan menggunakan DoS dan 92.65% apabila 5 client melakukan penyerangan menggunakan port scanning.
<hr><i>Requirement for accessing internet at the moment is very high, this matter an improvement of request access to secure network. This situation make network administrator to be more selective for give user to access network, so requirement for some system that can perform authentication to user for accessing network is important. This network concept becomes the appearance of base conception of Network Admission Control (NAC). Network Admission Control (NAC) is computer network security technology where computer client have to establish authentication before allowing to access the network. One of NAC technology most popular is Cisco NAC (C-NAC).
There are two main features of NAC server that is policy server and Intrusion Detection System (IDS)

server. Policy server undertakes to do authentication to user to access to network devices network. IDS server function to probe attacks or intrusion against the server, so IDS server can give alerting and then be able to stop the intrusion. IDS server also be able to reporting to administrator through SMS and monitoring through web when intrusion detected. IDS server build use operating system Linux. This system divided becomes three modules that are IDS software use SNORT, report module use Basic Analysis Security Engine (BASE) and client ' server module to communicate between IDS server and policy server. NAC network design will be use router and switch.

Examination of system to carry out some variation of attacks against the server. The variation of attack is denial of service (DOS), port scanning, and ICMP flood. Parameters are taken from the server is response time and action time. Examination also use comparison response time if use 1 client and 5 clients. Attack against IDS server show decreasing response time when server attacked by 5 client. IDS sever attacked use denial of service (DoS) response time decreasing 64.81% if attacked by 5 clients and 92.65% when 5 clients attacked use port scanning.</i>