ABSTRAK

Salah satu bidang teknologi yang berkembang pesat saat ini adalah Teknologi Informasi dan Komunikasi. Bentuk kemajuan teknologi informasi dan komunikasi yang seringkali kita jumpai dalam kehidupan sehari-hari adalah Internet (Interconnected Network). Melalui internet berbagai individu maupun organisasi dapat saling bertukar informasi. Namun, peningkatan tersebut juga berbanding lurus dengan munculnya berbagai macam celah keamanan yang seringkali dimanfaatkan oleh para penjahat elektronik untuk mendapatkan keuntungan finansial. Hal ini dapat dilihat dari banyaknya kasus serangan DDoS pada organisasi. Serangan Distributed Denial of Service dilakukan dengan membanjiri server atau host yang mengakibatkan host korban kehabisan sumber daya untuk melayani pengguna lain. Untuk mengatasi hal tersebut, penulis menggunakan Security Information and Event Management (SIEM). SIEM merupakan sebuah metode untuk melakukan monitoring, analisa, memberikan peringatan serta automasi respon terhadap suatu insiden. Penelitian ini diharapkan mampu menjelaskan hasil pengujian, analisis serta solusi mengenai masalah serangan DDoS pada SIEM.

Kata kunci : Log, Security Information and Event Management, DDoS

ASBTRACT

One area of technology that is growing rapidly today is information and communication technology. The form of advances in information and communication technology that we often encounter in everyday life is the Internet (Interconnected Network). Through the internet, various individuals and organizations can exchange information with each other. However, this increase is also directly proportional to the emergence of various kinds of security holes that are often exploited by electronic criminals to gain financial gain. This can be seen from the number of cases of DDoS attacks on organizations. Distributed Denial of Service attacks are carried out by flooding a server or host, causing the victim host to run out of resources to serve other users. To overcome this, the author uses Security Information and Event Management (SIEM). SIEM is a method for monitoring, analyzing, giving warnings and automating responses to incidents. This research is expected to be able to explain the results of testing, analysis, and solutions regarding the problem of DDoS attacks on SIEM.

Keyword : Log, Security Information and Event Management, DDoS