Abstrak

Keamanan informasi menjadi salah satu kebutuhan dan upaya organisasi untuk dapat mengamankan aset informasi organisasi. Pemerintah sebagai regulator mengeluarkan Sistem Managemen Keamanan Informasi (SMKI) dan Indeks Keamanan Informasi (KAMI) sebagai pengukur tingkat kematangan keamanan informasi. Dalam proses penerapannya berbagai macam teknologi keamanan akan digunakan untuk dapat mengamankan aset informasi tersebut, salah satunya *Security Information and Event Management (SIEM)*. *SIEM* diekpektasikan dapat memberikan informasi terhadap serangan yang terjadi di jaringan, terutama *router* sebagai penghubung jaringan. Beberapa penelitian sebelumnya tentang *SIEM* telah menunjukan keberhasilan untuk serangan di server dan aset informasi lainnya. Adapun penggunaan *SIEM* masih dipertanyakan implikasinya terhadap nilai Indeks KAMI. Dalam penelitian ini dilakukan simulasi serangan terhadap *router* dengan 8 tipe serangan yaitu (*Mac Flooding, ARP-Poisoning, CDP Flooding, DHCP Starvation, DHCP Rogue, SYN Flooding SSH Bruteforce* dan *FTP Bruteforce)* dilanjutkan dengan proses digital forensik untuk setiap serangan untuk melihat dampaknya terhadap *router* maupun *SIEM*, selain itu juga dilakukan *pre-assessment* indeks KAMI dan *post-assessment* KAMI untuk mengukur pengaruh pemasangan SIEM terhadap KAMI. Dalam penelitian ini didapatkan informasi bahwa penggunaan *SIEM* untuk melakukan *monitoring* keamanan terbukti berhasil memberikan informasi serangan. Akan tetapi tidak semua serangan dapat di kenali oleh *SIEM*. Hanya serangan *DHCP Starvation, DHCP Rogue, SSH Bruteforce* dan *FTP Bruteforce* dikenali oleh *SIEM*. Sedangkan untuk serangan *Mac Flooding, ARP-Poisoning, CDP Flooding, SYN Flooding* tidak dikenali *SIEM* karena *router* tidak memproduksi *log*. Dalam hubungannya dengan indeks KAMI pengunaan *SIEM* terbukti menaikan indeks KAMI dari aspek Teknologi.

Kata kunci

SIEM, Keamanan Jaringan, Forensik, KAMI

Abstract

Information security becomes one of the organization's needs and efforts to secure information assets owned by the organization. The government as regulator issues Sistem Managemen Keamanan Informasi (SMKI) and information security index (KAMI) as a measure of information security maturity level. In the process of application of various security technologies will be used to secure the information assets, one of them is Security Information and Event Management (SIEM). SIEM is expected to provide information against attacks that occur in the network, especially the router as a network connector. Several previous studies on SIEM have shown success for attacks on servers and other information assets. The use of SIEM is still questionable implication to the value of information security index (KAMI). In this research, simulation of attack on router with 7 types of attacks (Mac Flooding, ARP-Poisoning, CDP Flooding, SYN Flooding, DHCP Starvation, DHCP Rogue, SSH Bruteforce and FTP Bruteforce) followed by digital forensic process for each attack to see the impact on router and SIEM, in addition to the pre-assessment of information security index (KAMI) and post-assessment information security index (KAMI)to measure the effect of SIEM's installation on information security index (KAMI)

In this study obtained information that the use of SIEM to conduct security monitoring proved successful in providing information attacks. However, not all attacks can be recognized by SIEM. Only DHCP Starvation, DHCP Rogue, SSH Bruteforce and FTP Bruteforce recognized by SIEM. As for Mac Flooding attacks, ARP-Poisoning, CDP Flooding and SYN Flooding, can not be recognized by SIEM because the router does not produce logs. In conjunction with the information security index (KAMI) the use of SIEM technology has proven to increase the value of information security index (KAMI) from the aspect of Technology.

Keywords

SIEM, Network Security, Forensic, KAMI