Lembar Pengesahan Pembimbing

REAL TIME ANALISIS KEAMANAN ROUTER JARINGAN DENGAN *SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)* DAN IMPLIKASINYA PADA INDEKS KEAMANAN INFORMASI (KAMI)

Studi Kasus : Dinas Komunikasi dan Informatika Kota Tegal

Citra Arfanudin, S.Kom
12917116

Yogyakarta, Desember, 2017

Pembimbing I	Pembimbing II
Dr. Bambang Sugiantoro, S.Si., M.T.	Yudi Prayudi, S.Si.,M.Kom.

Lembar Pengesahan Penguji

REAL TIME ANALISIS KEAMANAN ROUTER JARINGAN DENGAN _SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)_ DAN IMPLIKASINYA PADA INDEKS KEAMANAN INFORMASI (KAMI)

Studi Kasus : Dinas Komunikasi dan Informatika Kota Tegal

Citra Arfanudin, S.Kom.

12917116

Tim Penguji,

Dr. Bambang Sugiantoro, S.Si., M.T.

Ketua

Yudi Prayudi, S.Si. ,M.Kom.

Anggota I

Dr. Imam Riadi, M.Kom.

Anggota II

Mengetahui,

Ketua Program Studi Teknik Informatika Program Magister

Fakultas Teknologi Industri

Universitas Islam Indonesia

Izzati Muhimmah, ST., M.Sc., Ph.D.

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

Pernyataan keaslian tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Untuk material yang membutuhkan izin, saya juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan material tersebut dalam tesis ini.

Yogyakarta, Desember. 2017

Citra Arfahudin

Publikasi selama masa studi

Publikasi yang menjadi bagian dari tesis

Kontributor	Jenis Kontribusi
Citra Arfanudin	Mendesain eksperimen (70%) Menulis *paper* (70%)
Dr. Bambang Sugiantoro, S.Si., M.T.	Mendesain eksperimen (10 %) Menulis dan mengedit *paper* (15%)
Yudi Prayudi, S.Si.,M.Kom	Mendesain eksperimen (20%) Menulis dan mengedit *paper* (15%)

Kontribusi yang diberikan oleh pihak lain dalam tesis ini

Terima Kasih kepada Kepala Dinas Komunikasi dan Informatika Kota Tegal beserta Jajaran

Halaman Persembahan

BISMILLAHIRRAHMANIRRAHIM...

Kupersembahkan karyaku ini kepada orang-orang yang telah membimbingku memaknai hidup.

- Emak yang Tercinta
- Emak yang Kusayang yang Pekerja Keras
- Emak yang terkasih dan memberikan contoh semangat dan motivasi agar tidak menyerah.
- Abah yang memberikan support untuk setiap pilihan anaknya. Dan untuk semua pengorbanan yang Abah lakukan.
- Kakak-kakakku yang menjadi motivasiku untuk menjadi orang yang lebih baik agar kelak bisa menjadi contoh yang layak.
- Yang selalu memberikan motivasi dan memberi nasehat seperti Shincan
- Yang mengajarkan untuk selalu mendekat dengan Allah My Hunny :**

Dengan segala ketulusan hati,

Citra Arfanudin

Kata Pengantar

Assalamualaikum, Wr, Wb

Alhamdulillah, puji syukur kehadirat Allah SWT atas segala nikmat, karunianya sehingga tesis yang berjudul "***REAL TIME* ANALISIS KEAMANAN ROUTER JARINGAN DENGAN *SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)* DAN IMPLIKASINYA PADA INDEKS KEAMANAN INFORMASI (KAMI) Studi Kasus : Dinas Komunikasi dan Informatika Kota Tegal**" dapat diselesaikan. Tesis ini disusun sebagai salah satu syarat untuk meraih gelar Magister Komputer pada program studi Magister Teknik informatika, Program Pascasarjana Fakultas Teknologi Industri, Universitas Islam Indonesia, disusun sebagai sarana untuk menerapkan ilmu yang telah didapatkan selama masa perkuliahan dengan konsentrasi Forensik Digital. Dalam penyusunan laporan ini tidak lepas dari dukungan pihak terkait, oleh karena itu pada kesempatan ini penulis dengan kerendahan hati ingin menyampaikan rasa terima kasihnya kepada:

- Allah SWT, tiada Tuhan selain Allah, Muhammad utusan-Nya.
- Emak & Abah atas doa dan restunya.
- Kakak-Kakakku, Yu Risa, Mas Shofi, Mas Wanto (Bapak Kost), Yu Henie, Yu Hetty
- Bapak Dr. Bambang Sugiantoro, S. Si., M.T. selaku Dosen Pembimbing I.
- Bapak Yudi Prayudi, S. Si, M. Kom selaku Dosen Pembimbing II.
- Ketua Program Pascasarjana FTI UII & seluruh jajaran formasinya.
- Dosen Magister Teknik Informatika khususnya untuk konsentrasi forensik digital.
- Jajaran Dinas Komunikasi dan Informatika Kota Tegal
- Teman-teman Forensik Digital angkatan 6
- Teman-teman Inixindo Jogja atas dukungan selama proses pembuatan tesis ini
- Pihak-pihak anonim yang langsung maupun tidak langsung memberikan dukungan.

Akhir kata semoga laporan ini dapat berguna bagi kemajuan bidang ilmu forensik digital. Aamiin.

Wassalamualaikum, Wr. Wb

Yogyakarta, Desember 2017

Citra Arfanudin