CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 2, No. 1, Mei 2019, hlm. 1-7

ANALISIS SERANGAN ROUTER DENGAN *SECURITY INFORMATION AND EVENT MANAGEMENT* (SIEM) DAN IMPLIKASINYA PADA INDEKS KEAMANAN INFORMASI

Studi Kasus : Dinas Komunikasi dan Informatika Kota Tegal

Citra Arfanudin[1], Bambang Sugiantoro[2], Yudi Prayudi[3]

[1]Magister Teknik Informatika, Fakultas Teknologi Industri,Universitas Islam Indonesia
[2]Magister Teknik Informatika, UIN Sunan Kalijaga, Yogyakarta
[3]Magister Teknik Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia
Email: [1]12917116@students.uii.ac.id, [2]bambang.sugiantoro@uin-suka.ac.id, [3]prayudi@uii.ac.id

Abstrak

Keamanan informasi menjadi kebutuhan untuk mengamankan aset informasi organisasi. Pemerintah sebagai regulator menerbitkan Sistem Manajemen Keamanan Informasi (SMKI) dan Indeks Keamanan Informasi (KAMI) sebagai pengukur keamanan informasi di instansi suatu daerah. *Security Information and Event Management (SIEM)* merupakan teknologi keamanan untuk mengamankan aset informasi. *SIEM* diharapkan dapat memberikan informasi serangan yang terjadi di jaringan *router* dan menaikan nilai Indeks KAMI instansi pemerintah. Akan tetapi penggunaan *SIEM* masih dipertanyakan apakah dapat mengenali serangan pada *router* dan dampaknya terhadap nilai Indeks KAMI. Penelitian ini mengsimulasi serangan terhadap *router* dengan 8 serangan yaitu *Mac Flooding, ARP-Poisoning, CDP Flooding, DHCP Starvation, DHCP Rogue, SYN Flooding SSH Bruteforce* dan *FTP Bruteforce.* 8 tipe serangan dilanjutkan dengan Analisis digital forensik dengan metode OSCAR untuk melihat dampaknya terhadap *router* maupun *SIEM*. Diukur juga indeks KAMI sebelum dan sesudah adanya SIEM untuk dapat mengukur pengaruh pemasangan *SIEM* terhadap nilai indeks KAMI. Didapatkan bahwa penggunaan *SIEM* untuk melakukan *monitoring* keamanan terbukti berhasil mengenali serangan, tetapi tidak semua dikenali *SIEM*. *SIEM* hanya mengenali *DHCP Starvation, DHCP Rogue, SSH Bruteforce* dan *FTP Bruteforce*. Serangan *Mac Flooding, ARP-Poisoning, CDP Flooding, SYN Flooding* tidak dikenali *SIEM* karena *router* tidak memproduksi *log*. Didadapatkan juga pengunaan *SIEM* terbukti menaikan indeks KAMI dari aspek Teknologi.

Kata kunci: *SIEM, Network Security, Forensic, KAMI*

ANALYSIS OF ROUTER ATTACK WITH SECURITY INFORMATION AND EVENT MANAGEMENT AND IMPLICATIONS (SIEM) IN INFORMATION SECURITY INDEX

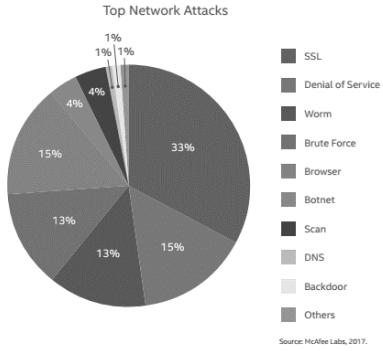
Abstract

Information security is a need to secure organizational information assets. The government as the regulator issues an Information Security Management System (ISMS) and Information Security Index (US) as a measure of information security in the agency of a region. Security Information and Event Management (SIEM) is a security technology to secure information assets. SIEM is expected to provide information on attacks that occur on the router network and increase the value of the Indeks KAMI of government agencies. However, the use of SIEM is still questionable whether it can recognize a router attack and its impact on the value of our index. This research simulates attacks on routers with 8 attacks namely Mac Flooding, ARP-Poisoning, CDP Flooding, DHCP Starvation, DHCP Rogue, SYN Flooding SSH Bruteforce and FTP Bruteforce. 8 types of attacks followed by digital forensic analysis using the OSCAR method to see the impact on routers and SIEM. Also measured is index KAMI before and after the SIEM to be able to measure the effect of SIEM installation on the value of index KAMI. It was found that the use of SIEM to conduct security monitoring proved successful in identifying attacks, but not all were recognized by SIEM. SIEM only recognizes DHCP Starvation, DHCP Rogue, SSH Bruteforce and FTP Bruteforce. Mac Flooding, ARP-Poisoning, CDP Flooding, SYN Flooding attacks are not recognized by SIEM because routers do not produce logs. Also obtained is the use of SIEM proven to increase our index from the aspect of technology.

Keywords: *SIEM, Network Security, Forensic, KAMI*

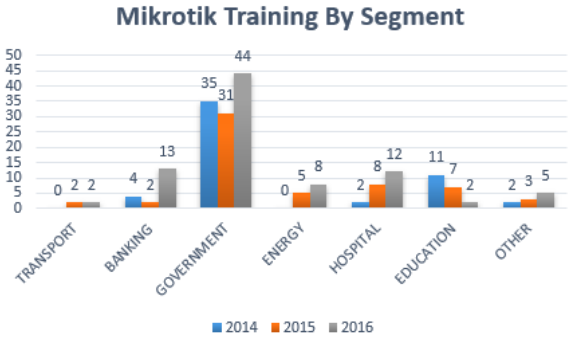
1. PENDAHULUAN

McAfee Labs Threat Security Report 2017 melaporkan, mayoritas serangan terhadap aset infrastruktur yang ada pada instansi adalah *SSL, DOS, Worm, Brute Force* dan serangan lainnya (McAfee et al., 2017), seperti ditunjukan pada gambar 1 dibawah ini.



Gambar 1. Top Network Security Attack

Router adalah perangkat yang penting di jaringan. Pada segmen jaringan skala kecil dan menengah banyak yang masih menggunakan *router mikrotik* sebagai alat untuk mengamankan jaringan seperti diperlihatkan gambar 2 di bawah ini.



Gambar 2: Mikrotik Training 2014-2016 (Source:Inixindo Jogja Internal Data)

Security Information and Event Management (SIEM) adalah Sistem *monitoring* yang dapat mendeteksi serangan dan respon suatu sistem keamanan terhadap serangan melalui analisis *log* dari berbagai *event-log* yang berasal dari berbagai sumber data seperti *(IPS, IDS, UTM, Router, Server*) secara *real-time* (Gartner, 2016).

Di pemerintahan tuntutan untuk dapat menerapkan Standar Manajemen Keamanan Informasi sesuai dengan SMKI (Sistem Manajemen Keamanan informasi) dan Kebutuhan *monitoring* terhadap *network* menjadi pilihan yang mutlak agar *security officer* dapat dengan jelas melihat apa yang terjadi dengan jaringannya yang akan berimbas pada nilai indeks KAMI di instansi tersebut. Akan tetapi, yang menjadi pertanyaan adalah apakah penggunaan *SIEM* benar-benar mendeteksi semua serangan yang ada pada jaringan terutama untuk asset *router* dan efektif mengamankan jaringan dari serangan-serangan yang ada.

Saat ini banyak yang menggunakan *IPS/IDS* dan *Syslog* untuk melihat serangan yang terjadi dijaringan. Dan tidak menganalisa *log* yang ada dan hanya disimpan saja dalam *syslog server.*

Penelitian tentang implementasi penggunaan *SIEM* untuk *Server, IPS/IDS, UTM* atau korelasi *SIEM* dengan *system audit* dan disiplin ilmu lain seperti *forensic* terutama *network forensic* menggunakan metode penelitian *OSCAR* (*Obtain Information -> Strategize -> Collect Evidence -> Analyze -> Report)* agar didapat hasil yang valid dalam pengujian serangan dan hasil serangan.

Penelitian tentang penggunaan *SIEM* pada *router* mengungkap bagaimana *SIEM* dapat membantu mengamankan jaringan berbasis *router Mikrotik.* Apakah *SIEM* dapat memberikan *monitoring* keamanan terhadap semua serangan terhadap router atau tidak secara *real time* sehingga hasil penelitian dapat memberikan gambaran implementasi *SIEM* di jaringan dan pengaruh penggunaan *SIEM* terhadap nilai indeks Keamanan Informasi (KAMI) terutama dari aspek Teknologi di instansi pemerintahan.

Dalam penelitian ini *SIEM* yang digunakan adalah *LogSign SIEM dengan* Tipe serangan yang akan disimulasikan adalah *Mac Flooding, ARP-Poisoning, CDP Flooding, DHCP Starvation, DHCP Rogue, Syn flooding, SSH Bruteforce* dan *FTP Bruteforce. Device Mikrotik* sebagai *router*-nya dan *Kalilinux OS* sebagai Penyerangnya, penelitian ini dilakukan di instansi Dinas Komunikasi dan Informastika Kota Tegal

Dengan analisa yang ada maka dalam penelitian ini diharapkan mampu mendapatkan informasi mengenai serangan apa saja yang bisa di kenali oleh *SIEM*, serta rekomendasi apakah memang perlu adanya *SIEM* dalam menjaga keamanan di *network environment* yang dimiliki oleh suatu instansi, dalam penelitian ini juga diharapkan mampu menjawab apakah penggunaan *SIEM* dapat menaikan indeks Keamanan Informasi

2. PENELITIAN TERKAIT

SIEM merupakan sistem monitoring yang dapat mendeteksi serangan suatu sistem melalui analisis *log* dari berbagai event yang berasal dari berbagai sumber *log*.

Rigal dan Purnamasari dalam penelitiannya melakukan implementasi dan analisis keamanan di perusahaan menggunakan *Open Source Security Information Management (OSSIM) AlientVault* dengan mengintegrasikan *OSSIM AlientVault* dengan perangkat keamanan jaringan *IDS* dan *firewall (Juniper)* dan memantau trafik yang lewat selama satu minggu, dengan melakukan simulasi serangan *ICMP Flooding*, hasilnya menunjukan bahwa *OSSIM*

AlientVault dapat mendeteksi serangan *ICMP Flooding* di jaringan mereka (Rihal & Purnamasari, 2010).

Arsyam dalam penelitiannya membangun sistem manajemen keamanan jaringan menggunakan *OSSIM* untuk membantu *security officer* menangani dan mengamankan sebuah jaringan. *OSSIM* diintegrasikan dengan modul *OSSEC* agen *HIDS* sebagai pendeteksi serangan (*Intrusion Detection System)* dan melakukan simulasi serangan *DDos, Sniffing* maupun *Exploit* ke target. Dan hasilnya *SIEM*-pun dapat mengenali serangan tersebut (ARSYAM, 2016).

Vendy, Rifqy & Roestam meneliti dan menggunakan *OSSIM AlientVault* sebagai *NMS (Network Monitoring System)* di perusahaan, peneliti menganalisa dan mengimplementasikan *OSSIM AlientVault* dengan metode *Top Down* dan mengsimulasikan serangan *Bruteforce* ke *Zimbra Email Server*, hasil penelitiannya *OSSIM AlientVault* dapat melihat serangan terhadap *E-mail Server Zimbra* dan memberikan notifikasi *e-mail* kepada *administrator*. Penelitipun menganjurkan untuk membuat *backup server* dan penambahan notifikasi keamanan berbasis *sms* (Vendy Djunaidi, rifqy & Roestam, 2014).

Pratama dan Wijaya dalam penelitian menggunakan *OSSIM Alientvault* untuk memonitoring *server* Universitas Bina Darma Palembang dari sisi keamanan, penggunaan *OSSIM Alientvault* dapat melaporkan ancaman seperti virus, ancaman *malware* terhadap jaringan secara *realtime* (Pratama, Wijaya, & D, 2016)).

Bachane dan Adsi dalam penelitiannya menggunakan *SIEM* sebagai alat *forensic* di lingkungan *cloud*, didalam *cloud* dengan berbagai service serta kombinasi berbagai layanan yang ada didalam lingkungan *cloud*, penulis melihat perlunya penggunaan *SIEM* untuk lingkungan *cloud* secara *realtime* agar proses penanganan masalah keamanan dalam lingkungan *cloud* dapat di proses dengan lebih cepat, dan hasil penelitian mengganggap penggunaan *SIEM* lebih efektif dibandingkan menggunakan *syslog server* (Bachane, Adsi, & Adsi, 2017).

Dalam penelitian Irfan, abbas dan Iqbal menguji kelayakan penggunaan *SIEM* untuk *forensic* di lingkungan *cloud*, mereka menggunaan *USM AlientVault* sebagai pilihan *SIEM*-nya dan menggunaakan beberapa aset seperti *Windows 8.1, Windows 7, Windows Xp, Windows Server 2008*, dan *Solarwinds* sebagai pilihan *NMS*-nya, Peneliti melakukan simulasi serangan *Bruteforce* dan *Dos* dengan menggunakan *KaliLinux*, dan hasil implementasi tersebut didapakan bahwa serangan dan analisis yang dikumpulkan dalam *SIEM* dapat menujukan kelayakan penggunaan *SIEM* di lingkungan *cloud* (Irfan, Abbas, & Iqbal, 2015).

Anastasov dan Davcec mengusulkan penggunaan model dan arsitektur baru dalam implementasi *SIEM* dengan menggunakan *Hierarchical SIEM Manager*, mekanisme yang memang diperuntukkan untuk tipe perusahaan dengan organisasi yang terdistribusi. Peneliti berhasil menggunakan *ArchSight* dalam implementasi keamanan jaringan yang besar dan terdistibusi (Anastasov & Davcev, 2014).

Hadiansyah dan Iskandar Ikbal melakukan penelitian implementasi penggunaan *SIEM* untuk mengamankan jaringan di Dinas Komunikasi dan Informatika Provinsi Jawa Barat. Peneliti memasang OSSIM di jaringan Provinsi Jawa Barat dengan aset berupa *Windows Server 2003*, *Linux Redhat* dan *Email Server*. Mereka menggunakan *OSSIM AlientVault* dan mensimulasikan serangan menggunakan *ICMP flooding*. *SIEM* dapat mengenali serangan dan menujukan *top attacker*, *top source* dan *top destination* (Hadiansyah & Iskandar Ikbal, 2017).

Vianello menggunakan *SIEM* untuk infrastruktur yang komplek dan dengan jumlah aset yang banyak dan dengan sistem *SIEM* yang tidak terdistribusi membuat *SIEM* kekurangan *resource* untuk memproses semua *event* yang ada dan mengkorelasikan dengan kemungkianan adanya serangan. Peneliti mencoba untuk melakukan pengetesan *SIEM* di sistem *Olympic Games* dengan pendekatan *distributed correlation* dan *query parallelization* dalam menyerang. Dan menggunakan *Dos* dan menggunakan *Worm* sebagai alat serangan, hasil *monitoring* berupa notifikasi ke *admininistrator*. Peneliti menggunakan *OSSIM AlientVault* dan mensimulasikan serangan menggunakan *Worm* dan *Bruteforce* (Vianello et al., 2013).

Dairinram, Wongsawang dan Pengsart melihat bahwa banyaknya jumlah *event* yang semakin meningkat di infrastruktur yang komplek membuat identifikasi terhadap ancaman yang ada dari *event* yang terkumpul menjadi salah satu masalah yang di hadapi administrator. Peneliti menggunakan The *Latent Semantic Analysis (LSA)* untuk menganalisa korelasi serangan dari *event-event* yang di kumpulkan oleh *SIEM* (Dairinram, Wongsawang, & Pengsart, 2013).

3. METODE PENELITIAN

Penelitian *SIEM* banyak membahas pengunaannya untuk asset berupa *server*, dan penelitian ini mencoba untuk menggunakan *SIEM* untuk asset infrastruktur jaringan untuk melihat apakah penggunaan *SIEM* dapat mengenali serangan yang ada dijaringan. Proses digital forensic dilakukan dengan menggunakan Analisis *Network Forensic*

Dalam penelitian ini disusun langkah-langkah penelitian untuk menjaga penelitian ini terarah dan fokus, dan Berikut tahapan penelitian yang dilakukan

a. Studi Literatur

Peneliti melakukan studi literatur untuk mencari referensi dan landasan teori sebagai dasar melakukan

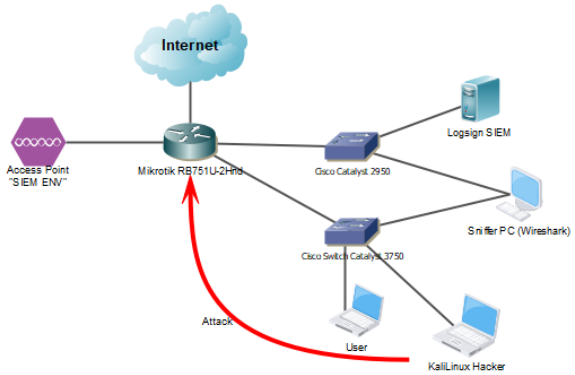
penelitian. Serta peneliti melakukan *review* terhadap jurnal sejenis, membaca berbagai sumber pustaka yang terkait dan *paper* dengan bahasan yang sejenis.

b. *Pre-Assesment* Indeks KAMI

Peneliti mengukur nilai indeks Keamanan Informasi (KAMI) pada Dinas Komunikasi dan Informatika Kota Tegal sebagai tahapan awal assesment. Dalam pengukuran nilai indeks KAMI Diskominfo Kota Tegal, metode yang digunakan adalah metode kuisioner kepada staf pranata komputer di lingkungan Diskominfo Kota Tegal. Hasil dari kuisioner tersebut dihitung sesuai dengan format aplikasi yang dimiliki oleh Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika Indonesia.

c. Pembuatan *Network Environment*

Ditahap ini peneliti membuat *network environtment* yang bisa digunakan dalam melakukan pengujian serangan sebagai *trigger* untuk melihat apakah *SIEM* dapat melihat serangan yang disimulasikan. Dalam penelitian ini digunakan perangkat seperti router *Mikrotik, Switch Manageable* dan *software* pendukung. Berikut merupakan topologi *network environment* yang akan dibuat, sesuai dengan gambar 3.



Gambar 3: Topologi *Network Environment*

Sepeti ditunjukan pada gambar 3 Peneliti menyediakan 2 jaringan yang terdiri dari jaringan *user* dimana *hacker* akan masuk dan menyerang aset *router Mikrotik*, serta jaringan dimana *SIEM Logsign* berada untuk menganalisa *log* yang dikirimkan oleh *router Mikrotik* kepada *SIEM Logsign*. *Switch manageable*-pun dipersiapakan untuk dapat menangkap semua trafik agar dapat dianalisa di proses *network forensic*.

d. Penyerangan *Network Environment*

Peneliti melakukan penyerangan terhadap infrastruktur jaringan yang telah dibuat sesuai dengan gambar 3. Peneliti melakukan penyerangan terhadap *router Mikrotik* dari Jaringan Internal *(Private Network).* Dengan beberapa serangan dan *software* Kalilinux.

e. Network Forensic

Setelah simulasi serangan dilakukan pada saat bersamaan dilakukan penyadapan terhadap semua aktifitas yang berjalan dan menangkap semua traffic dari *SWITCH A* dan *SWITCH B.* Dalam penelitian ini dilakukan penyadapan trafik komunikasi antara *hacker* dan *router Mikrotik* serta *router Mikrotik* ke *SIEM* dengan menggunakan *Wireshark*.

Dalam proses analisa dipenelitian ini mengikuti metodelogi yang ada dengan menggunakan metode *OSCAR* yang diseuaikan dengan kebutuhan peneliti,, Dari metodologi yang *OSCAR* yang digunakan, peneliti mencoba untuk lebih mendetailkan 3 proses terakhir yaitu *collect evidence, analyze* dan *reporting*

Dari hasil *capture* serangan yang dilakukan ditahap sebelumnya seperti ditunjukan pada gambar 4, dilakukan analisa pada *Log Sign SIEM* dan mendata apakah serangan tersebut memberikan dampak pada jaringan dan melihat apakah *Log Sign SIEM* dapat memdeteksi serangan tersebut.

f. *Post-Assesment* Indeks KAMI

Setelah melakukan proses *network forensic* terhadap simulasi serangan, dilakukan paparan mengenai hasil simulasi serangan dan *network forensic* kepada responden yang dalam hal ini adalah Staff Pranata Komputer Diskominfo Kota Tegal. Dan memberikan *post-assesment* KAMI untuk mengukur nilai indeks KAMI instansi tersebut setelah *SIEM* ada, penulis menggunakan metode kuisioner kepada Hasil dari kuisioner tersebut dihitung sesuai dengan format aplikasi yang dimiliki oleh Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika Indonesia.

g. Analisa Serangan

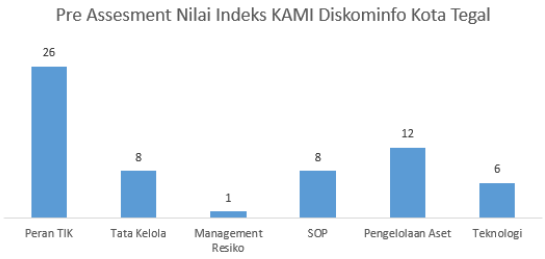
Dari hasil *network forensic* yang didapatkan dari tahap sebelumnya, dirangkumlah dan dianalisa 8 macam serangan yang ada dan dianalisa dan disimpulkan apakah *Log Sign SIEM* mengenali serangan tersebut atau tidak.dan dampak pemasangan *SIEM* terhadap indeks KAMI dengan cara membandingkan nilai indeks KAMI sebelum dan setelah dipasang *SIEM*

4. ANALISIS

Analisis implementasi *SIEM* ini dilakukan dalam beberapa tahapan, dengan tujuan untuk dapat menganalisa serangan dan proses *network forensic* dengan baik. Analisis *network forensic* juga digunakan sebagai salah satu acuan untuk dapat mengukur apakah indeks KAMI di Dinas Komunikasi dan Informatika Kota Tegal dapat dipengaruhi dengan ketersediaan *SIEM*. Dan berikut adalah hasil penelitian yang dilakukan.

a. Pre-Assesment Indeks KAMI

Dari hasil kuisioner yang diberikan, peneliti memasukan data kuisioner yang ada kedalam aplikasi dan didapatkan nilai indeks KAMI seperti ditunjukan pada gambar 5 dibawah.



Gambar 5: Indeks Kami Tegal Sebelum di Pasang SIEM

Dari grafik diatas dapat dilihat bahwa Diskominfo Kota Tegal mempunyai ketergantungan dan peran kepentingan IT yang tinggi yaitu dengan nilai poin 26, akan tetapi tidak ditindak lanjuti dengan nilai Indeks KAMI yang tinggi, hasil evaluasi dari indeks KAMI menunjukan nilai dari Diskominfo Kota Tegal adalah 35 yang mencakup 5 aspek (Tata Kelola, Managemen Resiko, SOP, Pengelolaan Aset dan Teknologi). Dan khusus untuk Aspek Teknologi mendapat nilai 6 poin.

b. Pembuatan *Network Environment*

Setelah pembuatan *environment* jaringan dilakukan, selanjutnya proses penyerangan aset *router Mikrotik* dengan menggunakan *Kalilinux OS*. Dalam proses penyerangan ini digunakan beberapa *software* yang ada di *Kalilinux* yaitu:

1. *MacOF*
2. *Etterchap*
3. *Hping3*
4. *Yersinia*
5. *Hydra*

c. Penyerangan *Network Environment*

Peneliti melakukan penyerangan terhadap infrastruktur jaringan yang telah dibuat dengan beberapa tipe serangan dan beberapa *tools.* Peneliti melakukan penyerangan terhadap *router Mikrotik* dari Jaringan Internal *(Private Network).* Dan berikut merupakan daftar serangan dan *tool* yang digunakan dalam simulasi serangan,

Tabel 1. Teknik Serangan

***Layer* Serangan**	**Teknik Serangan**	***Tools***
Link Attack	*Mac Flooding*	*MacOF*
	Arp Poisioning	*Ettercap*
	CDP Flooding	*Yersinia*
Internet Attack	*DHCP Starvation*	*Yersinia*
	DHCP Rogue	*Yersinia*
Transport Attack	*Syn Flooding*	*Hping3*
Application Attack	*SSH Bruteforce*	*Hydra*
	FTP Bruteforce	*Hydra*

d. Network Forensik

Setiap serangan yang disimulasikan oleh *hacker* di *capture* oleh *sniffer* untuk tujuan analisa. Dengan adanya analisa terhadap semua simulai serangan yang *hacker* lakukan berguna untuk mengvalidasi apakah serangan memang benar-benar terjadi dan menjawab bagaimana komunikasi dan trafik apa saja yang lewat dalam jaringan tersebut. Tabel 2 menunjukan hubungan antara serangan dan outputnya pada Mikrotik dan SIEM.

Tabel 2. Teknik Serangan dan Output Siem

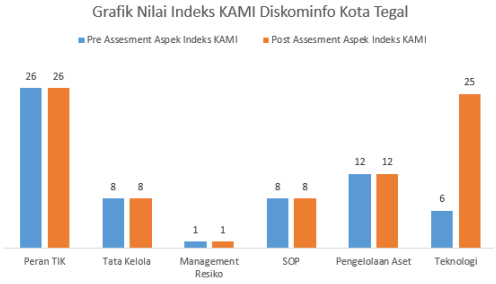
No	**Serangan**	**Hasil Mikrotik**	**Hasil *SIEM***	**Output *SIEM***
1	*Mac Flooding*	*router* tidak memproduksi *log*	Tidak ada aktifitas	*SIEM* tidak mendeteksi serangan
2	*Arp Poisioning*	*router* tidak memproduksi *log*	Tidak ada aktifitas	*SIEM* tidak mendeteksi serangan
3	*CDP Flooding*	*router* tidak memproduksi *log*	Tidak ada aktifitas	*SIEM* tidak mendeteksi serangan
4	*DHCP Starvation*	*router* memproduksi *log*	Ada aktifitas	*SIEM* mendeteksi serangan
5	*DHCP Rogue*	*router* memproduksi *log*	Ada aktifitas	*SIEM* mendeteksi serangan
6	*Syn Flooding*	*router* tidak memproduksi *log*	Tidak ada aktifitas	*SIEM* tidak mendeteksi serangan
7	*SSH Bruteforce*	*router* memproduksi *log*	Ada aktifitas	*SIEM* mendeteksi serangan
8	*FTP Bruteforce*	*router* memproduksi *log*	Ada aktifitas	*SIEM* mendeteksi serangan

e. Post-Assesment Indeks KAMI

Setelah melakukan analisis dan simulasi, dilakukan paparan terhadap hasil analisis forensik kepada Diskominfo Tegal dan melakukan kuisioner ulang sebagai bentuk perbandingan, apa yang terjadi jika *SIEM* di Implementasikan didalam Infrastruktur Pemerintahan Kota Tegal. Peneliti melakukan *post-assesment* terhadap Diskominfo Kota Tegal dengan kuisioner indeks KAMI untuk dapat mengukur nilai indeks KAMI yang dimiliki oleh Diskominfo Tegal.

Dengan ketergantungan dan peran kepentingan IT yang tinggi, dan dari hasil analisis serangan dan korelasinya dengan *SIEM* yang dilakukan. Terlihat

pada gambar 6 menunjukan bahwa nilai dari Dinas Komunikasi dan Informatika Kota Tegal adalah 54, yang menunjukan tingkat kematangan keamanan informasi masih tetap dan masih di level yang sama pada saat *pre-assesment* dilakukan, akan tetapi dari aspek teknologi menunjukan adanya kenaikan poin nilai dari 35 menuju ke 54 dikarnakan ada aspek teknologi yang naik dari 6 menuju 25 poin, naik 19 poin seperti ditunjukan pada gambar 5 dibawah ini.



Gambar 5: Indeks Kami Tegal Sebelum dan sesudah adanya SIEM

5. KESIMPULAN

Penggunaan *SIEM* untuk melakukan *monitoring* keamanan terbukti dapat memberikan informasi mengenai serangan yang terjadi pada *router* kepada *security officer*. 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* dan *Syn Flooding* tidak dapat dikenali oleh *SIEM* karena *router* tidak mengirim *log* ke *SIEM.*

Dalam hubungannya dengan indeks keamanan informasi (KAMI) pengunaan teknologi *SIEM* terbukti menaikan nilai indeks Keamanan Informasi (KAMI) Dinas Komunikasi dan Informatka Kota Tegal di aspek Teknologi, dari 35 poin ke 54 poin adapun kenaikan ini karena kemampuan *SIEM* dalam menganalisa kelemahan dan perubahan konfigurasi aset informasi di Dinas Komunikasi dan Informatka Kota Tegal, kemampuan *SIEM* untuk dapat memonitor dan melakukan proses analisa dan audit terhadap aset yang dimiliki Dinas Komunikasi dan Informatka Kota Tegal secara rutin dan sistematis. Penggunaan *SIEM* di Dinas Komunikasi dan Informatka Kota Tegal meningkatkan kemampuan Monitoring dan Audit semua aset di Lingkunagn Dinas Komunikasi dan Informatika Kota Tegal

DAFTAR PUSTAKA

Anastasov, I., & Davcev, D. (2014). SIEM implementation for global and distributed environments. In *2014 World Congress on Computer Applications and Information Systems, WCCAIS 2014*. https://doi.org/10.1109/WCCAIS.2014.6916651

Arsyam, K. (2016). Implementasi Manajemen Keamanan Jaringan Menggunakan Open Source Security Information Management (OSSIM). Retrieved from https://repository.telkomuniversity.ac.id/pustaka/121650/implementasi-manajemen-keamanan-jaringan-menggunakan-open-source-security-information-management-ossim-.html

Bachane, I., Adsi, Y. I. K., & Adsi, H. C. (2017). Real time monitoring of security events for forensic purposes in Cloud environments using SIEM. In *Proceedings - 2016 3rd International Conference on Systems of Collaboration, SysCo 2016*. https://doi.org/10.1109/SYSCO.2016.7831327

Dairinram, P., Wongsawang, D., & Pengsart, P. (2013). SIEM with LSA technique for Threat identification. In *2013 19th IEEE International Conference on Networks (ICON)* (pp. 1–6). https://doi.org/10.1109/ICON.2013.6781951

Gartner. (2016). Security Information and Event Management (SIEM) - Gartner IT Glossary. Retrieved from http://www.gartner.com/it-glossary/security-information-and-event-management-siem/

Hadiansyah, C., & Iskandar Ikbal. (2017). Pembangunan Server Security Information Management Untuk Monitoring Keamanan Di Server Diskominfo Provinsi Jawa Barat.

Irfan, M., Abbas, H., & Iqbal, W. (2015). Feasibility analysis for incorporating/deploying SIEM for forensics evidence collection in cloud environment. In *2015 IEEE/ACIS 14th International Conference on Computer and Information Science, ICIS 2015 - Proceedings* (pp. 15–21). https://doi.org/10.1109/ICIS.2015.7166563

McAfee, Beek, C., Frosst, D., Greve, P., Gund, Y., Moreno, F., … Weafer, V. (2017). *McAfee Labs Threats Report April 2017*. Santa Clara.

Pratama, A., Wijaya, A., & D, R. N. H. (2016). Penerapan Network Monitoring Menggunakan Security Information And Event Management (Siem) Berbasis Open Source Di Universitas Bina Darma Palembang.

Rihal, M., & Purnamasari, P. D. (2010). *Implementasi dan Analisa Security Information Management Menggunakan OSSIM Pada Sebuah Perusahaan*. universitas

indonesia. Retrieved from http://lib.ui.ac.id/file?file=digital/20249100-R031079.pdf

Vendy Djunaidi, rifqy, supriomanto W., & Roestam, R. (2014). Analisis Dan Perancangan Sistem Monitoring Jaringan Dengan Memanfaatkan Ossim Alientvault Pada Pt.Metalogix Infolink Persada.

Vianello, V., Gulisano, V., Jimenez-Peris, R., Patiño-Martínez, M., Torres, R., Díaz, R., & Prieto, E. (2013). A scalable SIEM correlation engine and its application to the olympic games it infrastructure. In *Proceedings - 2013 International Conference on Availability, Reliability and Security, ARES 2013* (pp. 625–629). https://doi.org/10.1109/ARES.2013.82