Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)
Vol. 1, No. 1, April 2014, hlm. 14-17

AUDIT DAN INVESTIGASI SISTEM KEAMANAN JARINGAN KOMPUTER DI LINGKUNGAN KAMPUS

Eko Sakti P[1], Ari Kusyanti[2], R. Arief Setyawan[3]

[1,2,3]Program Studi Ilmu Komputer, Universitas Brawijaya
Email: [1]ekosakti@ub.ac.id, [2]ari.kusyanti@ub.ac.id, [3]rarief@ub.ac.id

(Naskah masuk: 2 Desember 2013, diterima untuk diterbitkan: 17 Februari 2014)

Abstrak

Pemanfaatan internet untuk bidang pendidikan telah banyak membantu civitas akademika di lingkungan kampus dalam proses belajar mengajar. Selain memberikan dampak positif, penggunaan internet juga tak lepas dari efek negatif, antara lain issue keamanan jaringan komputer lingkungan kampus. Untuk kepentingan tersebut, penelitian ini ditujukan untuk melakukan audit dan investigasi jaringan kompuer kampus untuk menemukan celah kemanan dan memetakan serangan-serangan yang ada. Untuk proses audit, Indeks KAMI (SNI ISO 27000) digunakan sebagai standar keamanan komputer di Indonesia. Sedangkan untuk proses investigasi menggunakan SNORT yang merupakan pendeteksi serangan pada jaringan komputer. Dari hasil investigasi dengan SNORT didapatkan 80 jenis serangan dengan 315838 kali percobaan serangan selama 30 hari. Jenis serangan paling banyak mengarah ke WEB-PHP Wordpress dengan 99665 kali percobaan. Dari hasil evaluasi Indeks KAMI, tingkat kematangan pengamanan informasi lingkungan kampus adalah pada Tingkat I+, yang artinya bahwa kampus telah secara aktif menerapkan kerangka kerja dasar.

Kata kunci: SNORT, *Indeks* KAMI, *network attack*.

Abstract

Utilization of the Internet for education has helped many academic community on campus in the learning process . In addition to providing a positive impact , the use of the internet is also not free from the negative effects, among other issues the campus computer network security . For this purpose , this study aimed to conduct audits and investigations kompuer campus network to find security holes and map the existing attacks . For the audit process , WE Index (ISO 27000) was used as a standard computer security in Indonesia . As for the investigation process that is using Snort detection of computer network attacks . From the investigation results obtained with Snort 80 type attack with 315 838 times during a 30-day trial attacks . Most types of attacks leading to the WEB - PHP WordPress with 99 665 trials . WE index of evaluation results , the level of maturity of the campus information security is at Level I + , which means that the college has been actively implementing the basic framework.

Keywords: SNORT, KAMI *Indeks*, *Network Attack*.

1. PENDAHULUAN

Pemanfaatan internet dalam kampus diwujudkan dalam jaringan "*interconection*", saling berbagi informasi dan '*interconnect*', sehingga pelajar pengajar, dan staff dapat mengakses internet melalui jaringan kampus. Dengan bertambahnya pengguna internet, ditambah dengan tenaga pengajar dan tenaga pendukung pendidikan. Dengan jumlah pengguna jaringan komputer yang seperti itu perilaku pengguna jasa sulit diatur, bahkan ada yang melanggar. Ancaman pada jaringan kampus bisa datang dalam dua arah, yaitu dari dalam dan dari luar kampus.

Penelitian ini melakukan audit dan investigasi sistem keamanan jaringan komputer yang diterapkan pada jaringan kampus ini bertujuan untuk memperoleh informasi yang berkaitan dengan pola penggunaan internet, ancaman-ancaman yang muncul. Sehingga dapat digunakan sebagai acuan dalam pengembangan jaringan kampus selanjutnya. Untuk audit menggunakan Indeks KAMI, sedangkan untuk investigasi menggunakan SNORT, yaitu sebuah pendeteksi serangan pada jaringan komputer.

2. LANDASAN TEORI

Proses investigasi dan audit pada penelitian ini adalah dengan menggunakan SNORT dan Indeks KAMI yang akan dibahas pada bagian ini.

2.1. SNORT

SNORT merupakan *network intrusion detection system* (NIDS) yang mempunyai kemampuan untuk paket *sniffing* dan perekaman paket selain sebagai pendeteksi serangan. Kemampuan ini bermanfaat untuk mendapatkan pemberitahuan secara *real time,* dari pada harus terus menerus memonitor sistem SNORT yang sedang berjalan.

Dalam bentuk paling sederhana SNORT mirip dengan penyortir koin mekanis (Beale 2003).

1. Mengambil semua koin yang ada (mengambil paket pada jaringan utama).
2. Kemudian mengirimkan koin melalui saluran untuk menentukan apakah mereka adalah koin dan bagaimana mereka harus menggulung (preprocessor).
3. Selanjutnya, mengurutkan koin berdasarkan tipe. Merupakan tempat untuk menyimpan koin ratusan, puluhan, sen. (pada IDS ini adalah mesin deteksi).
4. Akhirnya, tugas administrator untuk memutuskan apa yang akan dilakukan dengan koin itu. Menyimpan atau membuangnya (perekaman dan disimpan dalam database).

2.2. Indeks KAMI

Pada tahun 2008 Kementrian Departement Komunikasi dan Informasi Indonesia telah mengeluarkan standar keamanan yang diadopsi dari ISO/IEC 27000 mengenai *Information Security Management System* (ISMS), yaitu SNI ISO 27000 yang dikenal dengan nama Indeks KAMI (Depkominfo, 2011). Oleh karena itu, untuk mengetahui tingkat pengamanan dan kelengkapan yang dimiliki oleh Indeks KAMI adalah alat evaluasi untuk menganalisa tingkat kesiapan pengamanan informasi.

Alat evaluasi ini memberikan gambaran kondisi kesiapan kerangka kerja keamanan system dan dilakukan terhapad area yang memenuhi semua aspek keamanan yang didefinisikan oleh standar ISO/IEC 27001:2005.

Proses evaluasi Indeks KAMI ini dilakukan dengan 2 metode:

1. Jumlah kelengkapan bentuk pengamanan
2. Tingkat Kematangan proses pengolaan pengamanan informasi

Area yang akan diaudit meliputi:

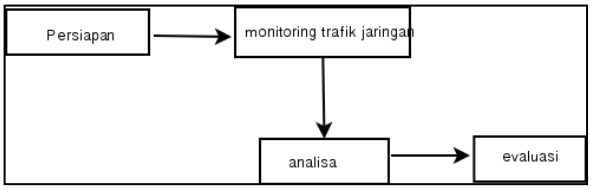
1. Peran TIK di dalam Instansi
2. Tata Kelola Keamanan Informasi
3. Pengelolaan Risiko Keamanan Informasi
4. Kerangka Kerja Keamanan Informasi
5. Pengelolaan Aset Informasi
6. Teknologi dan Keamanan Informasi

3. PERANCANGAN SISTEM

Ada 2 hal yang dilakuan pada penelitian ini, yang pertama melakukan investigasi dengan snort dan yang kedua melakukan audit dengan KAMI. Untuk mempermudah pembahasan kedua hal ini akan dijelaskan terpisah dimulai dengan investigasi kemudian audit.

3.1. Investigasi

Proses investigasi yang dilakukan dapat dilihat pada Gambar 1 yang terdapat beberapa proses. Pertama tahap persiapan meliputi kontruksi, pengaturan rencana. Kedua monitoring trafik jaringan meliputi, mengoleksi data trafik, penyimpanan data. Ketiga analisa meliputi pemeriksaan, hipotesis, pelaporan. Dan keempat tahap evaluasi meliputi penyajian, pembenaran dan peninjauan. Model investigasi tersebut digunakan untuk mendapatkan data-data yang berupa serangan apa saja yang terjadi selama proses investigasi.



Gambar 1. Model investigasi pada jaringan komputer

Perangkat lunak dalam investigasi menggunakan SNORT yang dikonfigurasi kedalam jaringan dalam mode *port mirroring,* yaitu metode untuk mengirimkan salinan paket jaringan pada suatu kanal *switch* ke sebuah jaringan pemantau di kanal *switch* yang lain. Sehingga penggunaan SNORT tidak mengganggu kinerja sistem jaringan komputer di lingkungan kampus yang sudah berjalan.

3.2 Audit

Berdasarkan standar Indeks KAMI langkah-langkah audit sistem keamanan diantarnya :

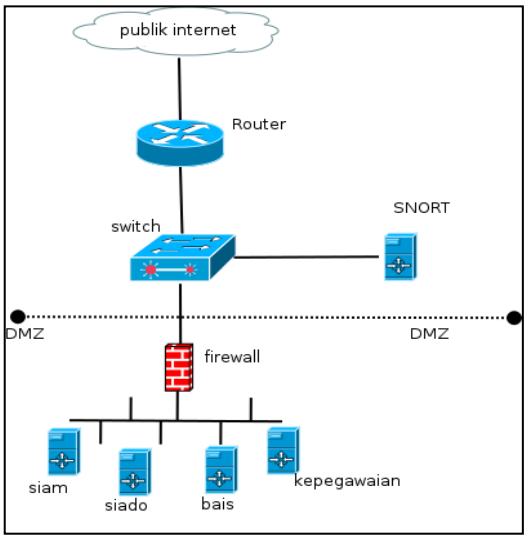
1. Mendefiniskan Ruang Lingkup
   Ruang lingkup yang dapat dievaluasi ini harus didefinisikan sesuai kepentingan instansi, dalam hal ini adalah lingkungan kampus.
2. Menetapkan Peran TIK
   Bagian ini memberi tingkatan peran dan kepentingan TIK dengan meninjau bahan evaluasi pada bagian 1.
3. Menilai Kelengkapan Pengamanan 5 Area
   Dari 5 area pengelompokan tersebut, maka pada tahap ini pertanyaan-pertanyaan evaluasi akan dikelompokkan berdasarkan 3 kategori, yaitu:
   a. Kerangka Kerja Pengamanan Informasi
   b. Efektivitas dan Konsistensi Pengamanan Informasi
   c. Kemampuan untuk meningkatkan kinerja

   Dengan penilaian : Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh.
4. Mengkaji Hasil Indeks KAMI dan Menetapkan Langkah Perbaikan Penetapan Prioritas

5. Mengkaji Ulang Tingkat Kelengkapan dan Kematangan Indeks KAMI
   Disarankan untuk menerapkan proses evaluasi Indeks KAMI sebanyak dua kali per tahun.

4. HASIL UJI COBA DAN ANALISA

Bagian ini bertujuan untuk mendapatkan data serangan-serangan yang masuk atau berada di lingkungan jaringan kampus khususnya terhadap service-service yang sering digunakan, misalnya SIAM, SIADO, dll. Alat yang digunakan adalah SNORT versi 2.9.3 dengan rule *snortrules-snapshot*-2930 diletakkan pada (*demilitarized zone*) DMZ seperti pada Gambar 2. Penempatan pada DMZ dipilih karena lalu lintas yang paling padat ada dijalur ini dan mempermudah pengambilan trafik dan analisa oleh SNORT supaya tidak mengganggu kinerja jaringan.



Gambar 2. Penempatan SNORT pada DMZ

Dengan metode *port mirroring*, lalu lintas jaringan yang menuju ke DMZ dikopi dan kopiannya akandialirkan oleh *switch* ke mesin SNORT. Teknik ini sangat bermanfaat untuk mendapatkan lalulintas yang asli tetapi tidak mengganggu lalu lintas yang akan menuju ke alamat atau tujuan sebenarnya. Selama SNORT dijalankan, dimulai hasilnya terdapat 80 jenis aktifitas yang dianggap berbahaya oleh SNORT dan terdapat 315838 peringatan serangan.

Untuk percobaan atau serangan yang paling sering dilakukan yang terjadi pada rentang 30 hari di lingkungan jaringan kampus antara lain :

- *WEB-PHP Wordpress timthumb.php theme remote file include attack attempt*, Serangan ini paling banyak terjadi, karena website yang ada di kamus hampir semuanya dibuat dari CMS tersebut. Serangan ini memanfaatkan celah untuk penggunaan *timthum.php*.Iika sebuah website yang dibangun dari wordpress dan konfigurasi *$allowedsites* pada *timthum.php* dibiarkan *default* maka mendapat serangan dengan teknik *remote file,* yang artinya website tersebut mempunyai celah keamanan. Contoh serangan *remote file*dengan perangkat lunak *shell* seperti Alucar shell.
- *WEB-MISC Microsoft Windows ASP.NET information disclosure attempt t*adalah celah keamanan yang terdapat pada ASP.NET, yang mengizinkan keterbukaan informasi. Penyeragan yang berhasil mengeksploitasi kelemahan ini dapat membaca data. Solusinya hanya memperbarui vesi dari *framework*ASP.NET yang dipakai.
- *WEB-MISC Multiple Products excessive HTTP 304 Not Modified responses exploit attempt* muncul karena pengguna internet explorer di kampus tidak melakukan *update* versi terbaru terutama yang memakai sistem operasi windows vista kebawah.
- *SQL MySQL/MariaDB client authentication bypass attempt*, sql / password.c di Oracle MySQL 5.1.x sebelum 5.1.63, 5.5.x sebelum 5.5.24, dan 5.6.x sebelum 5.6.6, dan MariaDB 5.1.x sebelum 5.1.62, 5.2.x sebelum 5.2.12 , 5.3.x sebelum 5.3.6, dan 5.5.x sebelum 5.5.23, ketika berjalan di lingkungan tertentu dengan implementasi tertentu dari fungsi *memcmp*,memungkinkan melakukan serangan *remote* untuk memotong otentikasi dengan berulang kali memasukkan sandi yang salah, yang pada akhirnya menyebabkan nilai kembalian Token perbandingan tidak jelas.
- SPECIFIC-*THREATS Havij advanced SQL injection tool user-agent string*. Havij adalah alat otomatis yang membantu menguji penetrasi, untuk menemukan, dan mengeksploitasi kerentanan SQL injection pada halaman web. Hal ini biasa dilakukan oleh pengelolah web kampus untuk menguji sistem yang dibuat atau sengaja dilakukan oleh penyerang. SQL injection ancaman yang serius jika pembuat website tidak mengantisipasinya. Celah ini bisa ada dari kelalaian pembuat aplikasi.

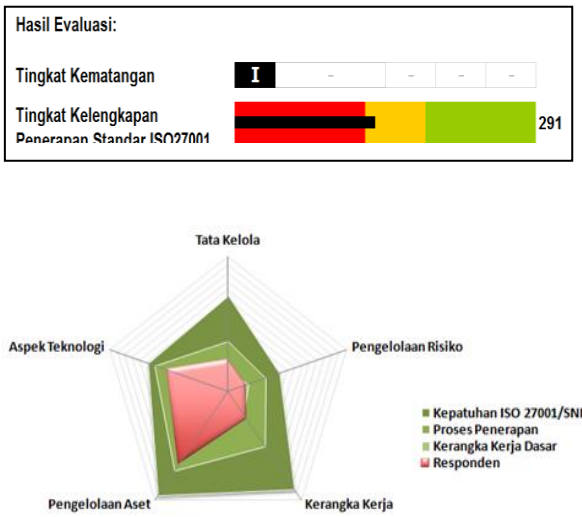
Hasil evaluasi pada lingkungan kampus adalah bahwa peran dan tingkat kepentingan TIK di lingkungan kampus memiliki skor 29 yang termasuk kedalam Kategori Tinggi. Hasil ini menunjukkan bahwa peran TIK di lingkungan kampus merupakan bagian yang tidak terpisahkan dari proses kerja yang berjalan.

Tabel masing-masing area setelah proses evaluasi di lingkungan kampus dapat terlihat pada

Tabel 1 berikut. Pada tabel ini, dapat dilihat seberapa besar tingkat kelengkapan masing-masing area yang telah dicapai.

Tabel 1. Hasil Indeks KAMI

Peran/Tingkat Kepentingan TIK	29	Tingkat Ketergantungan	Tinggi
Tata Kelola	37	Tingkat Kematangan	I+
Pengelolaan Resiko	24	Tingkat Kematangan	I
Kerangka Kerja Keamanan Informasi	41	Tingkat Kematangan	I+
Pengeloaan Aset	107	Tingkat Kematangan	II
Teknologi dan Keamanan Informasi	82	Tingkat Kematangan	II



Gambar 3. Radar Chart KAMI

Dalam diagram radar pada Gambar 3 latar belakang area menunjukkan ambang batas nilai kelengkapan kategori 1-3. Nilai dari masing-masing area ditampilkan dalam area merah. Dalam diagram ini bisa dilihat perbandingan antara kondisi kesiapan sebagai hasil dari proses evaluasi dengan acuan tingkat kelengkapan yang ada.

Berdasarkan kriteria Depkominfo, hasil evaluasi di lingkungan kampus menunjukkan bahwa:

- Pengamanan sudah diterapkan walaupun sebagian besar masih di area teknis dan belum adanya keterkaitan langkah pengamanan untuk mendapatkan strategi yang efektif.
- Proses pengamanan berjalan tanpa dokumentasi atau rekaman resmi.
- Langkah pengamanan operasional yang diterapkan bergantung kepada pengetahuan dan motivasi individu pelaksana.
- Bentuk pengamanan secara keseluruhan belum dapat dibuktikan efektivitasnya.
- Kelemahan dalam manajemen pengamanan masih banyak ditemukan dan tidak dapat diselesaiakan dengan tuntas oleh pelaksana maupun pimpinan sehingga menyebabkan dampak yang sangat signifikan.
- Manajemen pengamanan belum mendapatkan prioritas dan tidak berjalan secaa konsisten.
- Pihak yang terlibat kemungkinan besar masih belum memahami tanggung jawab mereka.

Dari hasil penelitian investigasi dan audit pada jaringan kampus ini dapat disimpulkan bahwa:

1. Terdapat 315838 serangan dalam 30 hari yang mengarah ke DMZ, dengan 30 % nya mengarah ke web wordpress. Sebagian besar website yang ada dilingkungan kampus menggunakan wordpress, ini ancaman yang serius.
2. Dari hasil audit Indeks KAMI, tingkat ketergantungan terhadap TIK, lingkungan kampus memiliki ketergantungan dengan skor 29 yang menunjukkan bahwa tingkat ketergantungan terhadap TIK adalah sangat besar.
3. Tingkat kematangan pengamanan informasi di lingkungan kampus adalah pada Tingkat I+, yang artinya bahwa kerangka kerja dasar telah secara aktif diterapkan.

5. DAFTAR PUSTAKA

BEALE, et al. 2003. *Snort 2.0 Intrusion Detection*. Syngress Publishing, Inc. 800 Hingham Street Rockland, MA 02370

DEPKOMINFO. 2011. *Tata Kelola Keamanan Informasi*. Direktorat Keamanan Informasi, Kementrian Kominuikasi dan Informatika RI.

GUOCHUN, J. & DENGGUO, F. 2009. *The detection principle and technique of Network Intrusion* [M]. National Defense Industry Press.

JIANZHONG WANG & LV LI. 2008. Based on Campus Net's Security Policy Discussion. *International Symposium on Knowledge Acquisition and Modeling*. kam, pp.366-370.

XINYU, G., BING, L., & XIAOYAN, H. 2009. "Investigation on Security System for SNORT-Based Campus Network," icise, pp.1756-1758, 2009 First International Conference on Information Science and Engineering.