Vol.2 No. 2 (Desember 2014)

ANALISIS KEAMANAN JARINGAN DENGAN METODE *SECURITY LIFECYCLE* DI UNIVERSITAS IBN KHALDUN BOGOR

Ade Hendri Hendrawan[1], Foni Agus Setiawan[2], Arief Sekto Mulyo[3]
Program Studi Teknik Informatika, Fakultas Teknik, Universitas Ibn Khaldun Bogor
hendri_hendrawan@yahoo.com[1], masagus@uika-bogor.ac.id[2], alex_hyker@yahoo.com[2]

Abstract. Computer network located in the building of Faculty of Engineering, Universitas Ibn Khaldun Bogor (FT UIKA) is currently the center of internet facility provider and Academic and Financial Information System (SIAK) which is connected directly to the Rectorat building. All services either internet connection and applications accessed by the faculties of UIKA have to go through this pathway. This strategic role of the network in FT UIKA need reliable security that are not easily damaged. One method of analyzing network security is Security Lifecycle (SLC). This method has stages ranging from data analysis of potential threats that may occur, the policy on what is allowed and not allowed to run a system, and specification of the desired system functionality, as well as the results of implementation of the security system tested. This study conducted a security analysis of UIKA network using SLC, build fortifications against attacks, perform a series of tests, and recommend matters related to network security and services in the FT UIKA. Implementation of these recommendations on computer network in UIKA will secure the system from various types of attacks to keep the continuity of operations.

Keywords: Analisis Keamanan Jaringan, *Security Life Cycle*, Nmap, Nessus.

1 PENDAHULUAN

Jaringan komputer yang berada di gedung Fakultas Teknik Universitas Ibn Khaldun Bogor (FT UIKA) saat ini menjadi pusat penyedia fasilitas internet dan Sistem Informasi Akademik dan Keuangan (SIAK) yang terhubung langsung ke gedung Rektorat. Segala layanan baik berupa koneksi internet maupun aplikasi yang diakses oleh sivitas akademik UIKA harus melalui jalur ini. Peran yang strategis tersebut membuat jaringan komputer di FT UIKA membutuhkan

pengamanan yang handal agar tidak mudah dirusak.

Perkembangan teknologi dan aplikasi internet yang semakin pesat menuntut adanya pengamanan jaringan dan layanannya dari kemungkinan adanya serangan. Berbagai cara dapat digunakan untuk mendeteksi serangan atau penyusupan, seperti packet sniffing, network scanning, dan monitoring layanan. Dengan teknik-teknik tersebut kita dapat menolak, memperbolehkan, atau menyaring paket yang mencoba masuk ke dalam jaringan atau ingin mengakses sumberdaya atau layanan tertentu.

Salah satu metode dalam menganalisis keamanan jaringan adalah *Security Lifecycle (SLC)*. Metode ini memiliki tahapan mulai dari analisis data potensi ancaman yang mungkin terjadi, kebijakan atas apa yang diperbolehkan dan tidak diperbolehkan dalam menjalankan sebuah sistem, dan spesifikasi mengenai fungsi sistem yang diinginkan, serta hasil implementasi dari sistem keamanan yang diuji.

Serangan yang ditujukan kepada jaringan komputer UIKA dilakukan baik oleh pihak luar maupun sivitas akademik UIKA sendiri. Serangan yang dilakukan oleh pihak luar misalnya berusaha melakukan *Denial of Service (DoS)* terhadap server web yang ada atau berusaha menembus masuk ke dalam Sistem Informasi Akademik dan Keuangan UIKA. Serangan yang dilakukan oleh mahasiswa seperti mencuri password hostspot dan SIAK. Kebijakan yang diberikan oleh FT berupa layanan internet yang sebelumnya 24 jam non-stop sekarang hanya 18 jam saja menjadi hambatan untuk para mahasiswa yang ingin sekedar mencari referensi tugas di malam hari. Hal ini juga menjadi salah satu pemicu bagi mahasiswa untuk mencoba merusak sistem keamanan jaringan yang ada.

Berdasarkan masalah tersebut, untuk membantu menjaga keamanan jaringan dan layanannya di FT UIKA, penelitian ini mencoba melakukan analisis keamanan jaringan komputer menggunakan metode SLC, membangun benteng-benteng pertahanan terhadap serangan, melakukan serangkaian pengujian, dan merekomendasikan hal-hal terkait pengamanan jaringan dan layanannya di FT UIKA. Diharapkan dengan penelitian ini, jaringan FT UIKA dapat aman terjaga dari berbagai jenis serangan untuk menjaga kesinambungan operasionalnya.

2 TINJAUAN PUSTAKA

2.1 Konsep Keamanan Jaringan

Menurut Bishop [1], konsep keamanan komputer mencakup tiga aspek utama, yaitu kerahasian (*confidentiality*), integritas

(*integrity*) dan ketersediaan (*availability*). Interpretasi dari setiap aspek pada lingkungan suatu organisasi ditentukan oleh kebutuhan dari individu yang terlibat, kebiasaan dan hukum yang berlaku dalam organisasi tersebut.

Kerahasiaan (*Confidentiality*). Ada beberapa jenis informasi yang tersedia di dalam sebuah jaringan komputer. Setiap data yang berbeda pasti mempunyai grup pengguna yang berbeda pula dan data dapat dikelompokkan sehingga beberapa pembatasan kepada pengunaan data harus ditentukan. Pada umumnya data yang terdapat di dalam suatu institusi bersifat rahasia dan tidak boleh diketahui oleh pihak ketiga yang bertujuan untuk menjaga rahasia dan strategi institusi. *Backdoor*, sebagai contoh, melanggar kebijakan dikarenakan menyediakan akses yang tidak diinginkan ke dalam jaringan komputer. Kerahasiaan dapat ditingkatkan dengan pengenkripsian data atau menggunakan VPN.

Akses kontrol adalah cara yang lazim digunakan untuk membatasi akses ke dalam sebuah jaringan komputer. Sebuah cara yang mudah tetapi mampu untuk membatasi akses adalah menggunakan kombinasi dari username dan password untuk proses otentifikasi pengguna dan memberikan akses kepada pengguna yang telah dikenali.

Keutuhan (Integrity) Jaringan komputer yang dapat diandalkan juga berdasarkan pada fakta bahwa data yang tersedia merupakan data yang sudah seharusnya. Jaringan komputer mau tidak mau harus terlindungi dari serangan (attacks) yang dapat merubah data selama dalam proses persinggahan (transmit). *Man-in-the-Middle* merupakan jenis serangan yang dapat merubah integritas dari sebuah data yang mana penyerang (attacker) dapat membajak "session" atau memanipulasi data yang terkirim. Didalam jaringan komputer yang aman, partisipan dari sebuah transaksi data harus nyata bahwa orang yang terlibat dalam komunikasi data dapat diandalkan dan dapat dipercaya. Keamanan dari sebuah komunikasi data sangat diperlukan pada sebuah tingkatan yang dipastikan data tidak berubah selama proses pengiriman dan penerimaan pada saat komunikasi data. Ini tidak harus selalu berarti bahwa traffic perlu di enkripsi, tapi juga tidak tertutup kemungkinan serangan *Man-in-the-Middle* dapat terjadi.

Ketersedian (*Availability*) Ketersediaan data atau layanan dapat dengan mudah dipantau oleh pengguna dari sebuah layanan, dimana ketidaktersediaan dari sebuah layanan (*service*) dapat menjadi

sebuah halangan bagi sebuah perusahaan maju dan bahkan dapat berdampak lebih buruk lagi, yaitu penghentian proses produksi sehingga untuk semua aktifitas jaringan, ketersediaan data sangat penting untuk sebuah sistem agar dapat terus berjalan dengan benar.

2.2 Insiden Keamanan Jaringan

Terdapat berbagai jenis insiden yang mungkin terjadi terhadap keamanan suatu jaringan. Beberapa yang umum terjadi, diantaranya [2]:

Probe Sebuah *probe* dapat dikenali dari adanya usaha-usaha yang tidak lazim untuk memperoleh akses ke dalam suatu sistem atau untuk menemukan informasi tentang sistem tersebut. Salah satu contohnya adalah usaha untuk login menggunakan sebuah akun yang tidak digunakan. *Probing* ini dapat dianalogikan sebagai usaha untuk memasuki sebuah ruangan yang dengan mencoba-coba apakah pintunya terkunci atau tidak.

Scan adalah kegiatan *probe* dalam jumlah yang besar dengan menggunakan *tool* secara otomatis. *Tool* tersebut secara otomatis dapat mengetahui port-port yang terbuka pada host lokal maupun host *remote*, IP address yang aktif, bahkan bisa untuk mengetahui sistem operasi yang digunakan pada host yang dituju. Contoh tool *scanner* adalah Nmap yang akan dibahas pada poin alat penguji jaringan.

Account compromise adalah penggunaan akun sebuah komputer secara ilegal oleh seseorang yang bukan pemilik akun tersebut. *Account compromise* dapat mengakibatkan korban mengalami kehilangan atau kerusakan data. Sebuah insiden *account compromise* dapat berakibat lebih lanjut, yaitu terjadinya insiden *root compromise* yang dapat menyebabkan kerusakan lebih besar.

Root compromise mirip dengan *account compromise*, dengan perbedaan akun yang digunakan secara ilegal adalah akun yang mempunyai *privilege* sebagai administrator sistem. Istilah root diturunkan dari sebuah akun pada sistem berbasis UNIX yang mempunyai *privilege* tidak terbatas. Penyusup yang berhasil melakukan *root compromise* dapat melakukan apa saja pada sistem yang menjadi korban, termasuk menjalankan program, mengubah kinerja sistem, dan menyembunyikan jejak penyusupan.

Packet Sniffer adalah suatu device, baik perangkat lunak maupun perangkat keras yang digunakan untuk memperoleh informasi yang melewati jaringan komputer. Cara kerja dari *packet sniffer* adalah dengan membuat NIC (*Network Interface Card*), contohnya

Ethernet, dalam mode *promiscuous* sehingga dapat menangkap semua *traffic* dalam jaringan. Mode *promiscuous* adalah mode di mana semua *workstation* pada jaringan komputer "mendengar" semua *traffic*, tidak hanya *traffic* yang dialamatkan ke *workstation* itu sendiri. Jadi *workstation* pada mode *promiscuous* dapat "mendengarkan" *traffic* dalam jaringan yang dialamatkan kepada *workstation* lain. Sebuah *sniffer* dapat berupa kombinasi dari perangkat lunak dan perangkat keras. Keberadaan *sniffer* di dalam jaringan sangat sulit untuk dideteksi karena sniffer adalah program aplikasi yang sangat pasif dan tidak membangkitkan apa-apa, dengan kata lain tidak meninggalkan jejak pada sistem.

Denial of Service (DoS) Sumber daya jaringan yang berharga antara lain komputer dan database, serta pelayanan-pelayanan (*service*) yang disediakan oleh organisasi pemilik jaringan. Kebanyakan pengguna jaringan memanfaatkan layanan tersebut agar pekerjaan mereka menjadi efisien. Bila layanan ini tidak dapat digunakan karena sebab-sebab tertentu, maka tentu saja akann menyebabkan kehilangan produktivitas. Sulit untuk memperkirakan penyebab DoS.

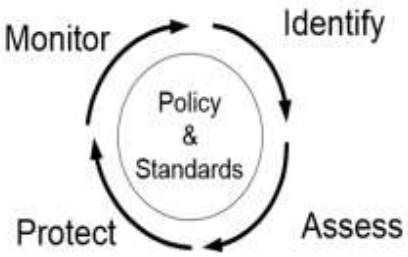
2.3 *Security Lifecycle (SLC)*

Seperti proses TI lainnya, keamanan pun dapat mengikuti model siklus hidup. Model siklus hidup keamanan atau SLC mengikuti langkah-langkah dasar yang terdiri dari [3]: IDENTIFY - ASSESS - PROTECT - MONITOR. Siklus ini memberikan dasar yang baik untuk setiap program keamanan. Model siklus ini memberikan panduan untuk memastikan bahwa keamanan terus ditingkatkan.

Sebuah program keamanan bukan merupakan penilaian statis atau produk jadi, melainkan membutuhkan perhatian konstan dan perbaikan secara terus-menerus. Seperti aspek lain dari program keamanan, menerapkan siklus hidup keamanan mengharuskan adanya standar kebijakan dan dilaksanakan terlebih dahulu. Kebijakan keamanan dan standar merupakan dasar untuk setiap komponen rencana keamanan. Dua hal ini merupakan komponen yang sangat penting baik dalam tahap penilaian maupun perlindungan siklus hidup.

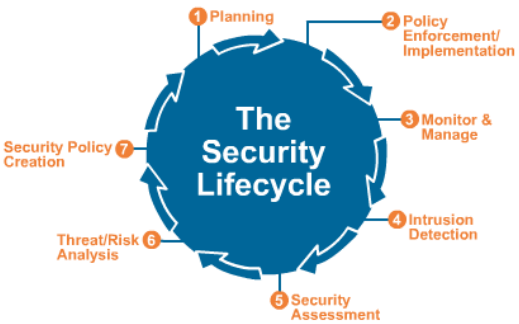
Tahap penilaian akan menggunakan standar dan kebijakan sebagai dasar melakukan penilaian. Sumber daya akan dievaluasi terhadap kebijakan keamanan. Selama fase perlindungan, sumber daya akan dikonfigurasi untuk memenuhi standar kebijakan. Gambar 1 menggambarkan siklus

hidup keamanan. Gambar ini menunjukkan bahwa siklus hidup keamanan dibangun di sekitar kebijakan keamanan dan standar.



Gambar 1 Siklus hidup keamanan menurut versi Robert Pfau (*Sumber*: Pfau, 2003)

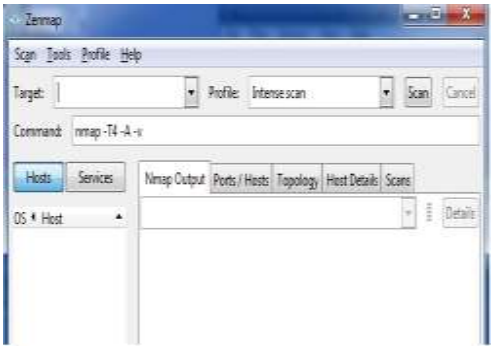
Variasi lain berupa pengembangan dari SLC versi Pfau diusulkan oleh Paranet – *IT Security Consulting* – dengan memodifikasi tahapan menjadi 7, yaitu [4]: PLANNING – IMPLEMENTATION – MONITOR – DETECTION – ASSESSMENT – ANALYSIS – POLICY. Gambar 2 di bawah ini menunjukkan tahapan SLC menurut versi Paranet.



Gambar 2 Siklus hidup keamanan menurut versi Paranet (*Sumber*: Paranet, 2014).

2.4 Alat Penguji Keamanan Jaringan

Nmap (*Network Mapper*) adalah sebuah program *open source* yang berguna untuk mengesksplorasi jaringan. Nmap didesain untuk dapat melakukan *scan* jaringan yang besar, juga dapat digunakan untuk melakukan *scan host* tunggal. Nmap menggunakan paket IP untuk menentukan *host-host* yang aktif dalam suatu jaringan, port-port yang terbuka, sistem operasi yang dipakai, tipe firewall yang dipakai, dll. [5]. Tampilan aplikasi Nmap dapat dilihat pada Gambar 3.



Gambar 3 Tampilan aplikasi Nmap

Keunggulan-keunggulan yang dimiliki oleh Nmap adalah [6]: a) *Powerful*: Nmap dapat digunakan untuk men-scan jaringan yang besar; b) *Portable*: Nmap dapat berjalan di berbagai macam sistem operasi seperti Linux, Windows, FreeBSD, OpenBSD, Solaris, dll.; c) Mudah untuk digunakan; d)

Free; dan e) Mempunyai dokumentasi yang baik.

Nessus adalah sebuah program yang berfungsi sebagai *security scanner* yang akan mengaudit jaringan yang dituju lalu menentukan kelemahan-kelemahan dari jaringan yang dituju [5]. Tampilan aplikasi Nessus dapat dilihat pada Gambar 4.

Gambar 4 Tampilan aplikasi Nessus

Berikut ini adalah fitur-fitur yang dimiliki oleh Nessus [7]:

Plug-in architecture. Setiap security test ditulis sebagai external plugin. Dengan fitur seperti ini, kita dapat dengan mudah menambah tes yang kita inginkan tanpa harus membaca kode dari Nessus engine. *NASL (Nessus Attack Scripting Language)*. NASL adalah sebuah bahasa yang didesain untuk menulis program security test dengan mudah dan cepat. Selain dengan NASL, bahasa C juga dapat digunakan untuk menulis program security test. Nessus security scanner terdiri dari dua bagian, yaitu: sebuah server yang berfungsi sebagai pelaku serangan, dan sebuah client yang berfungsi sebagai frontend. Client dan server dapat berjalan pada sistem yang berbeda. Arti dari fitur ini adalah bahwa keseluruhan jaringan dapat diaudit melalui sebuah PC dengan server yang melakukan serangan ke jaringan yang dituju. *Multi-host testing.* Dapat melakukan tes kepada beberapa host sekaligus dalam waktu yang bersamaan.

3 METODE PENELITIAN

Penelitian yang dilakukan menggunakan metode SLC dengan variasi sebagai berikut:

Gambar 5 Model siklus hidup sistem yang diusulkan.

SLC yang diusulkan untuk implementasi sistem keamanan jaringan di UIKA Bogor meliputi 5 tahap, yaitu: 1) Monitoring; 2) Analisis; 3) Rekomendasi; 4)

Implementasi; dan 5) Evaluasi. Aktivitas yang dilakukan dalam setiap tahapan adalah sebagai berikut.

Monitoring data dilakukan pada jaringan FT UIKA menggunakan tool Nmap dan Nessus selama dua bulan. Hasil *scan* menggunakan Nmap akan memperlihatkan port-port IP SIAK dan Hotspot sebagai IP Target. Adapun hasil *scan* menggunakan Nessus akan memperlihatkan banyaknya kategori kerentanan yang ada di dalam sistem keamanan jaringan FT UIKA.

Analisis pada tahap ini dilakukan proses analisis berupa pengolahan data yang didapatkan dari hasil monitoring dan *scan* yang dilakukan pada tahap sebelumnya dengan *tool* Nmap dan Nessus. Hasil *scan* dengan tool tersebut menampilkan data kerentanan dan *port-port* yang terbuka di server SIAK UIKA Bogor. Data kerentanan yang didapat selanjutnya akan diolah sebagai bahan rekomendasi untuk mengurangi kerentanan yang terdapat di jaringan FT UIKA.

Rekomendasi pada tahap ini dibahas mengenai rekomendasi yang disarankan untuk mengatasi kerentanan yang didapat dari hasil *scan*. Setiap poin kerentanan akan diberikan solusi atau rekomendasi masing-masing mengenai bagaimana cara menutupi lubang keamanan tersebut.

Implementasi pada tahap ini dibahas proses penerapan sistem keamanan yang akan dibangun di FT UIKA. Pada server baru yang direkomendasikan akan diinstal beberapa tool sebagai sistem monitoring keamanan jaringan, seperti *firewall*, *proxy*, *snort*, termasuk Nmap dan Nessus.

Tahap evaluasi akan membahas hasil analisis data yang didapat selama masa penelitian berlangsung. Data hasil evaluasi digunakan untuk mengetahui perbandingan sistem keamanan yang ada dengan sistem keamanan yang akan dibangun. Jika pada pertengahan penelitian sudah diketahui hal-hal yang negatif, saat itu keputusan atau tindakan akan dapat dilakukan untuk penelitian lebih lanjut. Evaluasi dilakukan setelah program sudah betul-betul selesai diimplementasikan. Evaluasi dilakukan untuk menentukan sejauh mana sebuah program mempunyai nilai kemanfaatan, terutama jika dibandingkan dengan sistem keamanan yang lain.

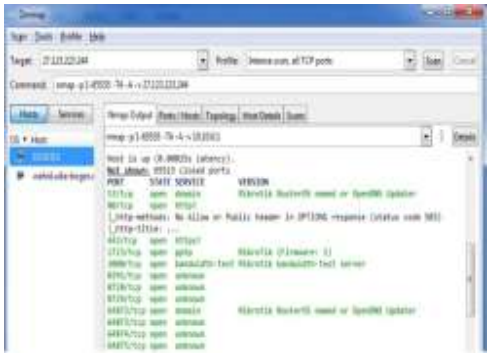
Penelitian ini hanya dibatasi sampai proses rekomendasi dikarenakan terbatasnya waktu untuk melakukan implementasi dan evaluasi. Juga karena tahap ini membutuhkan waktu yang cukup lama untuk membandingkan sistem yang dibangun dengan sistem yang telah ada sebelumnya.

4 HASIL DAN BAHASAN

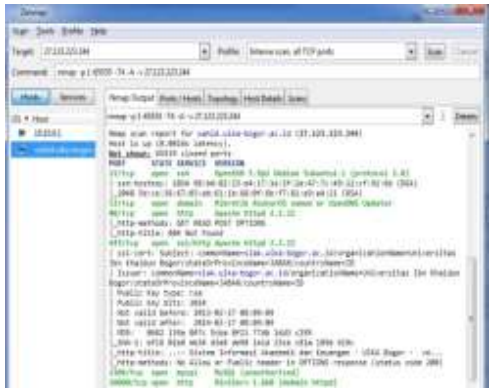
4.1 Monitoring

1. *Scan* jaringan menggunakan Nmap

Scan jaringan menggunakan Nmap menampilkan *host-host* dan port yang terbuka serta detail dari port yang di-*scan.* Selain itu, akan terlihat pula topologi dari IP target yang di-*scan*. Sistem yang di-*scan* adalah *Hotspot* dengan alamat IP 10.10.0.1 dan *Server* web SIAK dengan alamat IP 27.123.223.224. Hasil *scan* yang dilakukan oleh Nmap terhadap *Hotspot* dan *Server* menunjukkan port, state, service dan version seperti ditunjukkan pada Gambar 6 dan 7 di bawah ini.

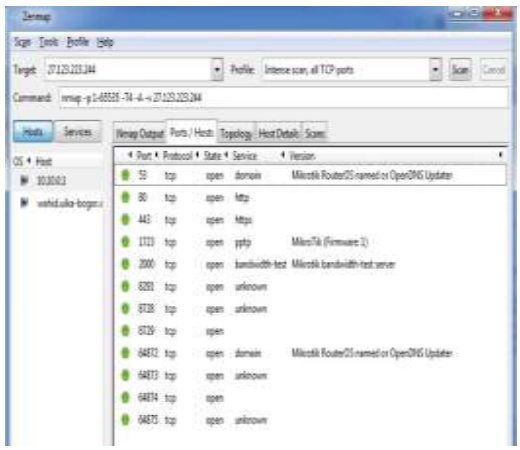


Gambar 6 Hasil *scan* sistem *Hotspot* menggunakan Nmap.



Gambar 7 Hasil *scan* sistem Server web *SIAK* menggunakan Nmap

Hasil *scan ports/hosts* terhadap *Server* menunjukkan secara detil port yang terbuka, mulai dari *protocol*, *state*, *service* hingga versi dari layanan yang berjalan di port tersebut ditunjukkan pada Gambar 8. Adapun hasil scan topology terhadap *Server* ditunjukkan pada Gambar 8.



Gambar 8 Hasil *scan ports/hosts Server* menggunakan Nmap

Gambar 9 Hasil *scan topology Server* menggunakan Nmap

2. Scan jaringan menggunakan Nessus

Scan jaringan menggunakan Nessus menampilkan kerentanan dari IP target yang di scan. Selain daftar kerentanan, Nessus juga menampilkan detil dari kerentanan IP yang di scan beserta solusi untuk mengatasi kerentanan tersebut. Hasil *scan* sistem *Hotspot* dan *Server* web SIAK menggunakan Nessus ditunjukkan pada Gambar 10.

Gambar 10 Hasil *scan* sistem *Server* SIAK dan *Hotspot* menggunakan Nessus: (a) Status scan; (b) Ringkasan untuk sistem *Server* SIAK; dan (c) Ringkasan untuk sistem *Hotspot*

Hasil *scan* menggunakan Nessus menunjukkan jumlah kerentanan dari sistem *Server* SIAK dan *Hotspot*. Bar yang berwarna menunjukkan tingkat kerentanan yang terdapat di masing-masing sistem. Bar berwarna biru menunjukkan informasi; hijau berarti tingkat kerentanan rendah (*low*), kuning berarti menengah (*medium*), oranye berarti tinggi (*high*), dan merah menunjukkan tingkat kerentanan kritis (*critical*). Jika dilihat secara detil kerentanan dari sistem hotspot, hasilnya ditunjukkan seperti pada Gambar 11.

Gambar 11 Detil *kerentanan* sistem *hotspot*

4.2 Analisis

Proses *scanning* yang dilakukan menggunakan Nmap menghasilkan daftar port yang terbuka serta topologi yang digunakan. Hasil *scan ports/hosts* pada Gambar 8 memperlihatkan bahwa di *Server* web SIAK beberapa port yang dikenal (*recognized*) terbuka, seperti port 53 dan

64872-64875 yang digunakan untuk DNS *updater* MikroTik; port 80 untuk HTTP; port 443 untuk HTTPS; port 1723 untuk pptp MikroTik; dan port 2000 untuk tes *bandwidth* oleh MikroTik. Adapun 3 port sisanya yaitu 8291, 8728, dan 8729 belum diketahui kegunaannya.

Hasil *scan topology* pada Gambar 9 menunjukkan bahwa untuk terkoneksi ke *Server* dari jaringan intranet/internet di UIKA, pengguna diharuskan melalui *Hotspot* terlebih dahulu untuk melakukan otentikasi sebagai bagian dari mekanisme keamanan jaringan.

Scanning menggunakan Nessus menghasilkan *output* berupa daftar kerentanan yang terdapat pada sistem yang di-*scan*. Hasil *scan* tersebut menampilkan lima kategori kerentanan, yaitu: *info, low, medium, high* dan *critical*.

Hasil *scan* Nessus pada sistem *Server* SIAK menunjukkan terdapat 49 kerentanan yang terbagi ke dalam 3 kategori yang cukup membahayakan sistem keamanan jaringan FT UIKA seperti terlihat pada Tabel 1. Ketiga kategori tersebut yaitu 10 kategori medium, 4 kategori low, dan 35 kategori info. Hasil *scan* Nessus pada sistem *Hotspot* menunjukkan terdapat 16 kerentanan yang terdiri dari 1 kategori high, 1 kategori medium, 1 kategori low, dan 13 kategori info seperti terlihat pada Tabel 2.

Hasil scan yang dilakukan oleh Nessus ini selanjutnya dapat disimpan dalam format HTML yang akan mempermudah dalam proses pengolahan data lebih lanjut.

Tabel 1. *Host summary* sistem *Server* SIAK

4.3 Rekomendasi

Analisis dari hasil *scan* menggunakan *tool* Nmap memperlihatkan port-port yang terbuka di Server SIAK maupun Hotspot di FT UIKA. Port-port yang terbuka tersebut memungkinkan menjadi celah yang menguntungkan bagi pihak yang tidak

bertanggung jawab untuk masuk dan merusak sistem keamanan jaringan komputer di UIKA. Analisis dari hasil *scan* menggunakan *tool* Nessus memperlihatkan daftar kerentanan yang terdapat pada sistem. Poin-poin kerentanan tersebut harus diselesaikan dengan cara menutup celah-celah keamanan yang memungkinkan terjadinya serangan kepada sistem. Hasil analisis dari kedua *tool* tersebut selanjutnya digabung lalu dibuat daftar rekomendasi untuk menutup celah-celah keamanan seperti tersaji pada Tabel 3 di bawah ini. Poin-poin keamanan yang direkomendasikan hanya untuk tingkat kerentanan *Medium* dan *High*.

Tabel 3. Rekomendasi perbaikan sistem keamanan jaringan UIKA

No	Kerentanan	Sumber	Rekomendasi
1	Port-port yang tidak diperlukan masih terbuka di *Server* SIAK, yaitu port 8291, 8728, dan 8729.	Nmap *port scanning*	Menutup port-port dengan nomor tersebut.
2	Server Web SIAK, Apache 2.2.23, 2.2.24 dan 2.2.25 *multiple vulnerabilities*	Nessus Plugin Id 62101, 64912, dan 68915	Melakukan upgrade Apache ke versi yang lebih tinggi atau versi terbaru.
3	Sertifikat SSL di *Server* SIAK bermasalah	Nessus Plugin Id 45411, 42873, 51192 dan 57582	Me-*register* sertifikat SSL ke sebuah *public Certificate Authority (CA)* sehingga dapat dipercaya (*trusted*).
4	Layanan DNS rentan baik di *Server* SIAK maupun di *Hotspot*	Nessus Plugin Id 10539, 12217, dan 35450	Konfigurasikan DNS agar mampu melakukan hal-hal berikut: o Memvalidasi alamat IP sumber pemohon informasi DNS. Jika bukan dari daftar yang dipercaya, permohonan dapat ditolak. o Memastikan apakah benar terjadi peracunan DNS (DNS *spoofing*) oleh alamat IP tertentu. Jika Ya, dapat dilakukan tindakan pencegahan seperti memblok seluruh paket dari IP tersebut. Jika Tidak, IP tersebut dapat dikeluarkan dari daftar hitam Firewall/IDS yang memblokn ya.
5	Nama dan *password* SNMP Agent di sistem *Hotspot* masih menggunakan konfigurasi *default*	Nessus Plugin Id 41028	SNMP masih menggunakan nama *default* ("*public*") sehingga mudah ditemukan dan dipergunakan sebagai password untuk koneksi antar peralatan. Ubah nama SNMP dan *password*-nya sehingga lebih bersifat konfidensial.

Demikian lima rekomendasi utama yang harus diimplementasikan untuk memperbaiki celah keamanan yang ada di sistem *Server* SIAK dan *Hotspot* di UIKA.

5 PENUTUP

Hasil monitoring keamanan jaringan UIKA yang telah dilakukan mendapati beberapa kerentanan, yaitu: a) pada sistem *Server* SIAK sebanyak 3 untuk kategori *low* dan 15 untuk kategori *medium*; b) pada sistem Hotspot sebanyak 1 untuk kategori *medium* dan 1 untuk kategori *low* pada bulan pertama penelitian pada tanggal 22 November 2014. Hasil analisis yang dilakukan selama 2 bulan menunjukkan peningkatan jumlah kerentanan. Bahkan pada bulan ke-2 terdapat kerentanan dengan kategori *high* pada sistem *Hotspot*.

Hasil rekomendasi yang disarankan untuk mengatasi kerentanan di sistem *Server* SIAK maupun *Hotspot* hendaknya diimplementasikan dan dievaluasi untuk menutup celah keamanan yang ada. Penggunaan SLC yang berkesinambungan dalam proses penanganan keamanan jaringan di UIKA sangat disarankan untuk menjaga agar jaringan dan sistem komputer di UIKA senantiasa dalam keadaan aman.

6. DAFTAR PUSTAKA

Bishop, Matt. *Computer Security*: *Art and Science*, Addison-Wesley, 2003.

Wiharjito, Tony. *Keamanan Jaringan Internet*, PT Gramedia, Jakarta, 2002.

Pfau, Robert. *The Security Lifecycle,* SANS Institute, USA, 2003.

Paranet. *IT Security Risk Management: Managing across the IT Security Lifecycle*, http://www.paranet.com/it-security-risk-management/ diakses tanggal 18 Desember 2014.

Setiawan, Thomas. *Analisis Keamanan Jaringan Internet Menggunakan Hping, Nmap, Nessus, dan Ethereal*, Departemen Teknik Elektro, Fakultas Teknologi Industri, Institut Teknologi Bandung, Bandung, 2004.

http://www.znmap.org diakses pada tanggal 05 Desember 2014.

http://www.nessus.org diakses pada tanggal 05 Desem