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

Ade Hendri Hendrawan, Foni Agus Setiawan, Arief Sekto Mulyo
Unversitas Ibn Khaldun Bogor
Jln. K.H Sholeh Iskandar Km. 2 Bogor
e-mail: hendri_hendrawan@yahoo.com, masagus@uika-bogor.ac.id, alex_hyker@yahoo.com

***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.**

I. PENDAHULUAN

A. Latar Belakang

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.

B. Tujuan

Menganalisis keamanan jaringan Universitas Ibn Khaldun Bogor menggunakan metode *Security LifeCycle*.

II. METODOLOGI

Penelitian yang dilakukan menggunakan metode SLC dengan variasi sebagai berikut:

Gambar 1. 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.

A. Monitoring

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.

B. 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.

C. 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.

D.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.

E. Evaluasi

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.

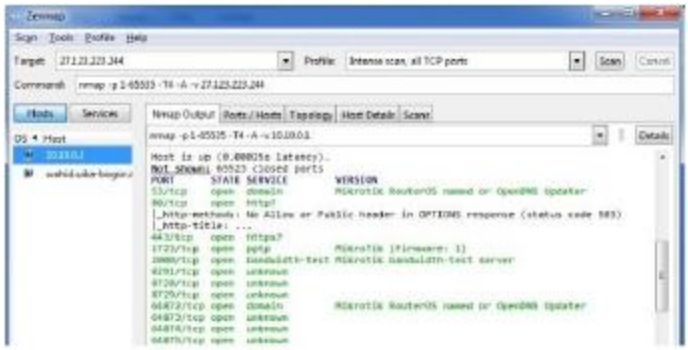
III. HASIL DAN BAHASAN

A. Monitoring

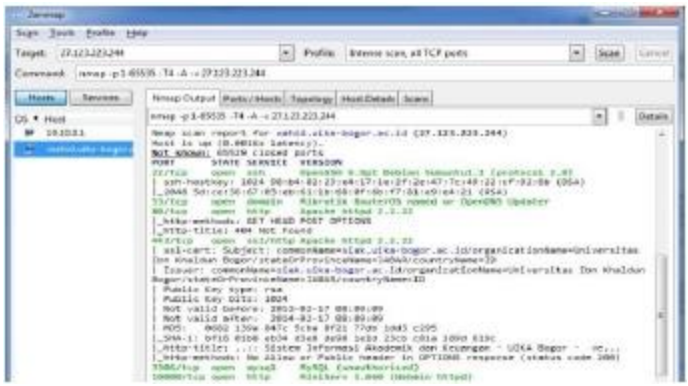
1. Scan jaringan menggunakan Nmap

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 2 dan 3 di bawah ini.

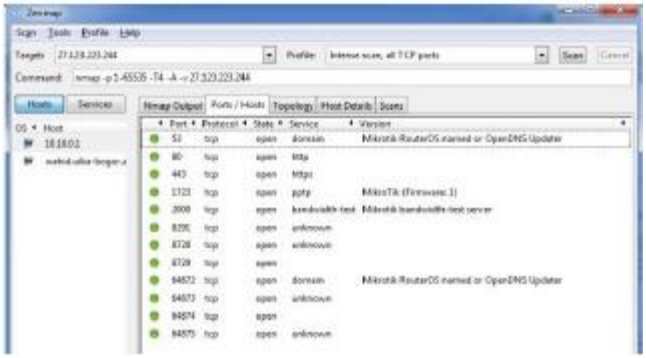


Gambar 2. Hasil *scan* sistem *Hotspot* menggunakan Nmap.



Gambar 3. 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 4. Adapun hasil scan topology terhadap *Server* ditunjukkan pada Gambar 5.

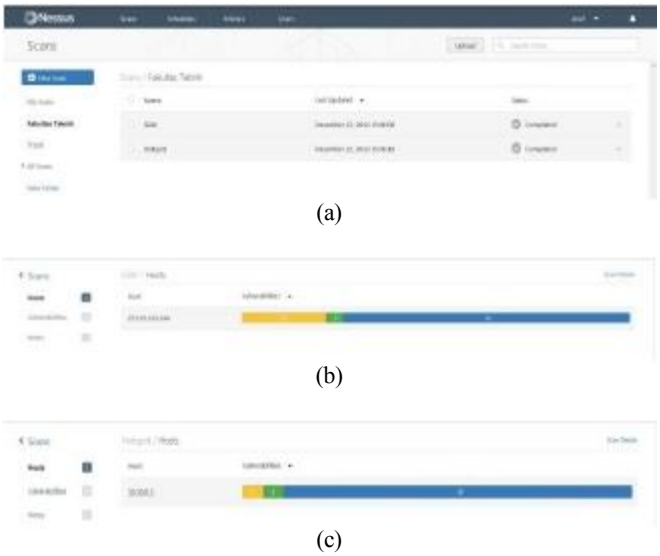


Gambar 4. Hasil *scan ports/hosts Server* menggunakan Nmap.

Gambar 5. 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 6.



(a)

(b)

(c)

Gambar 6. 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 7.

Gambar 7. Detil *kerentanan* sistem *hotspot.*

B. 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.

27.123.223.244

Summary

Critical	High	Medium	Low	Info	Total
0	0	10	4	35	49

Details

Severity	Plugin Id	Name
Medium (6.8)	62101	Apache 2.2 < 2.2.23 Multiple Vulnerabilities
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.1)	68915	Apache 2.2 < 2.2.25 Multiple Vulnerabilities
Medium (5.0)	10539	DNS Server Recursive Query Cache Poisoning Weakness
Medium (5.0)	12217	DNS Server Cache Snooping Remote Information Disclosure
Medium (5.0)	35450	DNS Server Spoofed Request Amplification DDoS
Medium (5.0)	45411	SSL Certificate with Wrong Hostname
Medium (4.3)	42873	SSL Medium Strength Cipher Suites Supported
Medium (4.3)	64912	Apache 2.2 < 2.2.24 Multiple Cross-Site Scripting Vulnerabilities
Low (2.6)	65821	SSL RC4 Cipher Suites Supported
Low (2.6)	70658	SSH Server CBC Mode Ciphers Enabled
Low (2.6)	71049	SSH Weak MAC Algorithms Enabled
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10267	SSH Server Type and Version Information
Info	10287	Traceroute Information
Info	10719	MySQL Server Detection
Info	10737	Webmin Detection
Info	10863	SSL Certificate Information
Info	10881	SSH Protocol Versions Supported
Info	11002	DNS Server Detection
Info	11153	Service Detection (HELP Request)
Info	11219	Nessus SYN scanner
Info	11936	OS Identification

Tabel 2. *Host summary* sistem *Hotspot*.

10.10.0.1

Summary

Critical	High	Medium	Low	Info	Total
0	1	1	1	13	16

Details

Severity	Plugin Id	Name
High (7.5)	41028	SNMP Agent Default Community Name (public)
Medium (5.0)	12217	DNS Server Cache Snooping Remote Information Disclosure
Low (3.3)	10663	DHCP Server Detection
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10287	Traceroute Information
Info	10919	Open Port Re-check
Info	11002	DNS Server Detection
Info	11219	Nessus SYN scanner
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	30212	MikroTik RouterOS Detection
Info	35296	SNMP Protocol Version Detection
Info	40448	SNMP Supported Protocols Detection
Info	71077	MikroTik Neighbor Discovery Protocol Detection

C. 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 membloknya.
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.

IV. 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.

V. DAFTAR PUSTAKA

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

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

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

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

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

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

[7] http://www.nessus.org diakses pada tanggal 05 Desember 2014.