ANALISA KEAMANAN JARINGAN SMK 1 MUHAMMADIYAH SUKOHARJO

Makalah

Program Studi Teknik Informatika

Fakultas Komunikasi dan Informatika

Diajukan oleh :

Eti Rohani

Fatah Yasin, S.T.,M.T

Irma Yuliana, ST., M.M

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS KOMUNIKASI DAN INFORMATIKA

UNIVERSITAS MUHAMMADIYAH SURAKARTA

Januari, 2013

HALAMAN PENGESAHAN

Publikasi ilmiah dengan judul

ANALISA KEAMANAN JARINGAN SMK 1 MUHAMMADIYAH SUKOHARJO

Yang dipersiapkan dan disusun oleh :

Eti Rohani

L200080123

Telah disetujui pada :

Hari : .....

Tanggal : .....

Pembimbing I	Pembimbing II
Fatah Yasin, S.T., M.T.	**Irma Yuliana, ST.,M.M.**
NIK: 738	NIP: 200.1476

Publikasi ilmiah ini telah diterima sebagai salah satu persyaratan untuk memperoleh gelar sarjana

Tanggal .....

Mengetahui

Ketua Program Studi

Teknik Informatika

18/2/2013

Dr. Heru Supriyono, M.Sc.

NIK. 930

UNIVERSITAS MUHAMMADIYAH SURAKARTA
PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS KOMUNIKASI DAN INFORMATIKA

ANALISA KEAMANAN JARINGAN

SMK 1 MUHAMMADIYAH SUKOHARJO

(Studi Kasus SMK 1 MUHAMMADIYAH SUKOHARJO)

Eti Rohani, Fatah Yasin, Irma Yuliana

Teknik Informatika, Fakultas Komunikasi dan Informatika

Universitas Muhammadiyah Surakarta

E-Mail : etyrohani@gmail.com

ABSTRACT

Technology development that improve fastly proves that computer has important role in some aspects that is integrated each other with life aspect. Now almost people shifts in *wireless technology*. This *technology* begins to advance in a *network* which connected with *internet*, so it can be a dangerous threats.

The system that is used by SMK 1 Muhammadiyah Sukoharjo has applied *captive portal* which designed by *open authentication* method it is router mechine that doesn't allow the first.

The research includes some experiment which is done, such as : maping the network, *denoal of service, MITM, penetration key, injection proxy.* From experiments above savety analysis experiment is done by testing savety level by *flooding* that is sent at the attacked IP. There is space of savety on the *wireless* system which is still susceptible on threats from inside or outside without using encryption.

Keywords : *Network Topology, Encryption, Wireless*

ABSTRAKSI

Perkembangan teknologi yang terus berkembang pesat membuktikan peranan komputer penting di berbagai bidang yang saling terintegrasi aspek kehidupan. Sebanyak yang beralih dengan teknologi *wireless.* Dalam teknologi ini mulai berkembang di suatu jaringan yang terhubung dengan internet, maka bisa menjadi suatu ancaman yang berbahaya.

Sistem yang digunakan di SMK 1Muhammadiyah Sukoharjo ini sudah menerapkan *captive portal* yang di design dengan metode *Open Authentikasi* yang merukan mesin router yang tidak mengizikan adanya trafik sehingga user melakukan registrasi ketika akses pertama kali.

Penelitian ini meliputi beberapa percobaan yang dilakukan antara lain : Pemetaan Jaringan, *Denial Of Service*, MITM, *penetration key, injection proxy.* Dari percobaan diatas melakukan analisis keamanan yang dilakukan dengan menguji tingkat keamanan dengan cara *flooding* yang dikirim pada IP yang akan diserang. Terdapat celah keamanan pada sistem wireless yang masih rawan terhadap ancaman dari dalam maupun luar tanpa menggunakan enkripsi sama sekali.

Kata Kunci : Topologi Jaringan, *Enkripsi*, *Wireless*,

I. PENDAHULUAN

Perkembangan teknologi yang terus berkembang pesat, tentu saja peranan komputer masih penting di berbagai bidang yang saling terintegrasi disetiap aspek kehidupan. Saat ini lembaga/perusahaan baik pemerintah atau swasta telah menggunakan komputer sebagai alat bantu untuk menyelesaikan tugas pekerjaan. Oleh karena itu komputer merupakan salah satu faktor pendukung yang membantu kita mengerjakan tugas. Adanya jaringan komputer bukanlah sesuatu yang baru saat ini.

Hampir di setiap perusahaan/lembaga yang terdapat jaringan komputer untuk memperlancar arus informasi. Internet yang mulai berkembang saat ini adalah suatu jaringan jaringan komputer yang terhubung dengan internet bisa menjadi suatu ancaman yangberbahaya,banyak serangan yang dapat terjadi baik dari dalam maupun luar seperti *virus, Trojan*, maupun *hacker*. Pada akhirnya keamana jaringan sangat berperan penting dalam kasus ini.

Sistem keamanan jaringan komputer ini yang terhubung ke internet harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif dan efisien. SMK 1 Muhammadiyah Sukoharjo telah merancang dan menerapkan sistem jaringan dengan kondisi gedung bertingkat yang sudah terpasang banyak *access point*. Semua ini harus diperhatikan untuk segi keamanan jaringannya.

Segala ancaman dari dunia maya,

mulai dari serangan virus, *Trojan, phishing* hingga *cracker* yang bisa memanipulasi keamanan sistem komputer. Oleh sebab itu administrator harus meningkatkan keamanan dalam jaringan di SMK 1 Muhammadiyah Sukoharjo. Namun semua ini dapat diatasi dengan adanya *intruder* yang berguna untuk menjaga data / file baik dalam komputer maupun pada jalur komunikasi dari pemakaian yang tidak dikehendaki, *intruder* ini juga memerlukan untuk mmenjaga kerahasiaan data agar data tidak mudah disalah gunakan oleh *hacker*. Suatu konfigurasi firewall yang baik dapat mengurangiancaman-ancaman tersebut.

II. TINJAUAN PUSTAKA

2.1 Telaah Pustaka

Dalam penelitian ini penulis mengacu pada beberapa penelitian terdahulu sebagai panduan dalam melakukan penelitian ini, diantaranya :

Penelitian sebelumnya Riadi (2011) dalam skripsinya "*Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik*" membahas tentang pengguna jaringan komputer yang sangat memberikan pengaruh besar pada penyebaran informasi. Semakin banyak yang mengakses data melalui internet dapat diatasi menggunakan mikrotik sebagai lalu lintas data internet sekaligus melakukan pemfiteran. Pemfilteran ini dapat dilakukan melalui beberapa tahap yaitu yang pertama adalah analisa proses untuk menentukan alur lalu lintas yang melewati proses dengan menggunakan *firewall*, desain untuk mendapatkan cara yang efektif dan efisien dalam implementasi *router*, serta pengujian yang dilakukan dengan metode *Stress Test*..

Ciptadi David, Yonatan, (2011) dalam skripsinya "*Analisis dan Perancangan Sistem Keamanan Jaringan Menggunakan Router Firewall dan Software Monitoring pada PT. ARWANA CITRAMULIA"* membahas tentang penentuan solusi yang dapat memberikan

penyelesaian permasalahan dalam sistem keamanan jaringan. Metode dilakukan dengan wawancara terhadap IT manager dan analisis kondisi sistem jaringan komputer yang berjalan. Setelah melakukan analisis hasil yang dapat ditarik adalah penggunaan *Router Firewall* dapat meningkatkan keamanan jaringan serta kinerja jaringan yang lebih efisien dan optimal.

2.2 Landasan teori

2.2.1Jaringan Komputer

Jaringan komputer adalah sekumpulan komputer, printer dan peralatan lainnya yang terhubung. Informasi data bergerak melalui kabel-kabel sehingga memungkinkan pengguna jaringan komputer dapat saling bertukar dokumen dan data mencetak pada printer yang sama dan bersama-sama menngunakan *hardware* atau *software* yang terhubung dengan jaringan. Sistem keamanan jaringan komputer yang terhubung ke internet harus direncanakan dan dipahami dengan baik agar melindungi sumber daya yang berada dalam jaringan tersebut secara efektif (Melwin Syahfrizal, 2005).

2.2.2 Captive Portal

Captive Portal merupakan mesin router atau gateway yang memproteksi atau tidak mengizinkan adanya trafik hingga user melakukan registrasi atau authentikasi pengguna managemen IP, mwlakukan bandwith control dan mengatur traffic tanpa aplikasi apapun di sisi client (M. Sinambrela, 2007).

WPA (Wifi Protected Access)

Merupakan teknologi keamanan yang diciptakan untuk menggantikan kunci WEP. Ada 2 jenis WPA personal (WPA-PSK) dan WPA-RADIUS. Saat ini yang sudah dicrack adalah WPA-PSK dengan menggunakan metode brute force attack secara offline. Serangan ini akan berhasil jika passphrase yang digunakan wireless tepat pada kamus yang digunakan oleh hacker (M. Sinambrela, 2007).

2.2.3 Topologi Jaringan

Topologi yang berada di SMK 1 Muhammadiyah Sukoharjo diantaranya adalah.

a. Topologi bus adalah topologi masing-masing workstation dan servernya dihubungkan denga sebuah kabel menggunakan konektor T dengan kabel pada umumnya adalah tipe coaxial (Kurniawan Wiharsono, 2007)

b. Topologi star adalah topologi yang menghubungkan suatu workstation dengan server menggunakan suatu konsentrator.

c. Topologi tree adalah topologi yang memiliki sistem rangkaian seperti topologi star dan topologi bus dimana setiap jaringan dihubungkan dalam topologi jaringan bus yang berperan sebagai tulang punggung jaringan (backbone).

2.2.4 Serangan pada wireless

Pada jaringan wireless lebih cenderung rawan terhadappenyerangan, karena jaringan tersebut memakai gelombang radio untuk saling berkomunikasi, maka dari itu gelomang ini mengetahui bahwa siapa saja yang dapat mengintip gelombang tersebut. Semua dapat dibutuhkan mekanisme keamanan untuk mengatasi masalah yang ada (Sarjanoko, 2007).

2.2.5 Handshaking pada jaringan wireless

TCP handshaking atau mudah dikenal dengan jabat tangan digital secara wireless yang terjadi antara 2 device atau lebih. Handshake dibagi menjadi 3 tahap proses yang dilakukan oleh mesin tersebut ketika berkenalan untuk menyambung koneksi satu sama lain. Sederhananya ketika mesin hendak berkenalan mereka akan berjabat tangan (handshake) terlebih dahulu (Stevens,1944).

2.2.6 Serangan yang terjadi pada wireless

Dalam serangan ini dapat dikategorikan dalam 9 jenis serangan (Sarjanoko, 2007)

1. Session hijacking attack

Serangan ini dapat dilakukan untuk mencuri *session* dari seorang *wireless user* yang sudah terontentikasi dengan *access point. Wireless user* akan mengira bahwa koneksi *access point* telah terputus, namun *access point* tetap beranggapan bahwa *wireless user* masih terkoneksi.

2. Man-in-the-middle attack

Proses *authentikasi* satu arah ini ternyata memungkinkan terjadinya *man-in-the-middle attack* yaitu penyerang bertindak seolah-olah sebagai *access point* di hadapan *wireless user* dan bertindak seolah-olah sebagai *wireless user* digadapan *access point.*

3. Insertion attack

Serangan ini terjadi jika terdapat pihak-pihak yang sebenarnya tidak mempunyai hak akses ke dalam jaringan, namun masuk ke dalam jaringan tanpa proses keamanan dan *authentikasi* yang sebenarnya

4. *Interception dan montoring attack*

Serangan yang dilakukan dengan menangkap lalu lintas jaringan.

5. Serangan terhadap enkripsi

Serangan terhadap *wireless* LAN yang menggunakan *wireless Equivalent Privacy* (WEP). Tidak banyak peralatan siap tersedia untuk mengatasi masalah ini, tetapi perlu di ingat bahwa penyerang selalu dapat merancang alat yang dapat mengimbangi sistem keamanan yang baru.

6. Denial of service attack (Dos)

Serangan ini biasanya dilakukan untuk melumpuhkan ketersediaan jaringan sehingga *wireless user* tidak dapat mengakses jaringan dengan mudah untuk diterapkan ke dalam *wireless* LAN, yaitu dengan mengirimkan paket-paket yang membanjiri lalu lintas jaringan *(flooding).*

7. *Brute force attack* terhadap *password* pengguna

Serangan ini melakukan uji coba terhadap kunci akses dengan memasukkan beberapa kemungkinan dimana sebagian besar *access point* menggunakan suatu kunci tunggal atau password yang dimiliki oleh *wireless user* pada *wireless* LAN.

8. Brute force dan dictionary attack

Dictionary attack adalah serrangan dengan mencoba semua kombinasi *password* yang berasal dari dictionary yang berisikan daftar kemungkinan *password* yang biasanya sering digunakan.

9. Kesalahan konfigurasi

Dimana banyak *access point* bekerja dalam suatu konfigurasi yang tidak aman kecuali para administrator yang mengerti resiko penggunaan keamanan *wireless* LAN dan konfigurasi masing-masing unit sebelum digunakan.

2.2.7 Peningkatan keamanan jaringan

Beberapa cara yang dapat meningkatkan keamanan jaringan yang mengenai authentikasi dan enkripsi antara lain (Thomas, 2004)

a. Authentikasi

b. Enkripsi

III. METODE PENELITIAN

Dalam penelitian ini penulis menggunakan beberapa peralatan dan pendukung untuk menunjang dalam penelitian. Peralayan yang digunakan dalam penelitian ini yaitu

3.1. perangkat keras

a. Laptop Toshiba L310, *Processor* dual core 2.00 Ghz, memori 1024 MB.

b. Sistem operasi *windows* 7 ultimate

c. Sistem operasi *linux Ubuntu 10.04*

3.2 perangkat lunak

1. *Software* kismet (Mengidentifikasi jaringan).

2.*Software aircrack-ng* (memecahkan *network key* atau *password*).

3. *Software Wireshark* (memonitoring jaringan).

4. *Software ettercap* (Serangan MITM)

IV HASIL DAN PEMBAHASAN

Hasil penelitian ini dapat dianalisa bahwa jeringan wireless sangat penting karena kemajuan sesuatu diawali oleh sebuah analisa yang akan menemukan sebuah kekurangan dan kelebihan. Serta apa yang harus dilakukan untuk menutup celah keamanan di SMK 1 Muhammadiyah Sukoharjo yang telah menerapkan jaringan wireless.

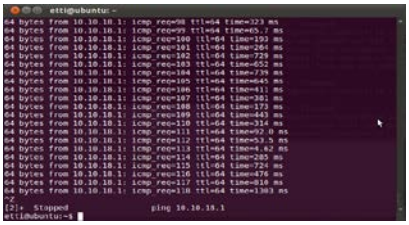
2.3 Analisa hasil penelitian

a. Pemetaan access point

Pemetaan jaringan yang dilakukan untuk mengetahui infrastruktur jaringan yang di pakai di SMK Muhammadiyah 1 sukoharjo dengan menggambarkan topologi yang dipakai serta penempatan hardware jaringan, hasil pemetaan tersebut penulis memfungsikan melihat kesalahan dan menangani kesalahan dengan baik tanpa harus memeriksa satu per satu lokasi yang sebaiknya diganti atau diberikan keamanan yang khusus.

b. Denial of Service

Access point dan server yang diserang menggunakan serangan DoS terbukti terbebani oleh data yang dikirimkan dari pembuktian bahwa ping alamat tujuan penulis mendapatkan respon yang selalu bertambah besar nilainya.



Gambar 1. Hasil ping yang di Dos

c. Cracking Wireless

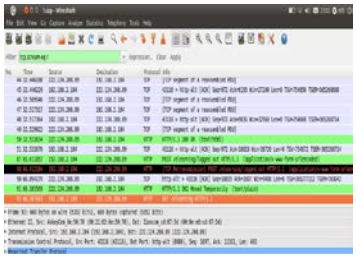
Percobaan ini dilakukan untuk mendapatkan paket data yang terdeteksi di SMK 1 Muhammadiyah Sukoharjo dengan menggunakan keamanan yang ada dalam sistem tersebut. Cracking wireless ini memberikan informati tentang BBSID , jumlah data yang dipakai, CH, MB, ENC / security jaringan wireless yang terdeteksi. Pada percobaan ini penulis kesulitan untuk proses mencari password, karena sudah menerapkan open

system authentication yang disertai enkripsinsupaya hacker tidak mendaoatkan plaintetext dan chipertext.

Gambar 2. Monitor jaringan

d. Man In The Middle

Percobaan ini dilakukan untuk mendapatkan informasi mengenai username dan password, agar penyerang dapat bertindak seolah-olah sebagai layanan penyedia dan bertindak sebagai user terhadap access point. Man In The Middle dapat dianalisa bahwa serangan yang dilakukan dengan cara mengintai lalu lalang data dalam jaringan wireless untuk melakukan serangan, namun serangan ini hanya berhasil jika data yang lewat tidak menggunakan enkripsi sama sekali, jadi data terenkripsi maka data tidak akan terlihat oleh attacker.

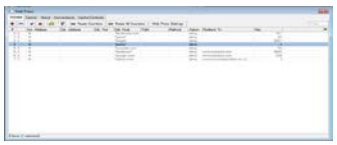


Gambar 3. Pengelompokan Protokol http

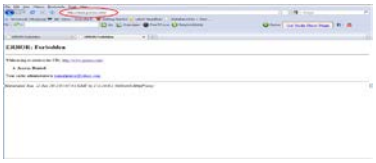
Gambar 4. Hasil Sniffing Username dan Password

e. Hacking Proxy

Percobaan ini dilakukan untuk melewati block dari proxy, serangan yang dilakukan di SMK 1 Muhammadiyah Sukoharjo ini mendapatkan alamat yang diblock dari proxy. Penulis mendapatkan informasi mengenai : dst. Address, dst. Host dan action.



Gambar 5. Web proxy yang diblock



Gambar 6. Alamat web yang diblock proxy

IV. KESIMPULAN

Kesimpulan

Dari penelitian yang telah penulis lakukan penulis telah mencapai target dari yang sudah ditargetkan dalam menyusun laporan.

1. Penelitian yang penulis lakukan meliputi pemetaan jaringan yang berada di SMK 1 Muhammadiyah Sukoharjo dengan hasil bahwa infrastruktur jaringan sudah terbilang cukup baik, mulai dari penggunaan topologi, perancangan hardware yang sudah tergolong rapi.
2. Mendapatkan celah keamanan yang masih dapat ditembus dengan mudah oleh attacker.
3. Pada jaringan wireless dan server proxy yang belum cukup tangguh sehingga penulis masih bisa melakukan serangan terhadap jaringan tersebut.

DAFTAR PUSTAKA

Ciptadi David, Yonatan, dkk. 2011. *Analisa dan Perancangan sistem Keamanan Jaringan Menggunakan Router Firewall dan Software Monitoring Pada PT ARWANA CITRAMULIA*. Skripsi. Jakarta:Universitas Bina Nusantara

Kaeo, Merike. 2004. *Designing Network ecurity*. Singapore :Pearson Education

Kurniawan, wiharsono. 2007. *Jaringan Komputer*. Semarang :Penerbit Andi

Melwin Syafrizal. 2005. *Pengantar Jaringan Komputer*. Yogyakarta: Penerbit Andi

Riadi, iman. 2011. *Optimalisasi Keamanan Jaringan Komputer WAN dengan VPN menggunakan Point to point Tuneling Protocol Serta Pengujian SSH Secure pada PT Kiyonuki Indonesi Bekasi*. Skripsi. Jakarta : Universitas Mercubuana

S'to. 2007. Wireless Kung Fu Networking dan Hacking. Jakarta: JASAKOM

Sarjanoko, R. Joko, 2007. *Analisis Keamanan Jaringan Wireless Local Area Network Standar 802.11: PT Master Data Jakarta.* Bogor: Tesis Institut Pertanian Bogor

Sinambrela, Josh. 2005. "Wireless LAN (Jaringan Nirkabel)" (online), (*josh.staff.ugm.ac.id/seminar/Presentation%20Wireless%20Network.ppt, diakses pada tanggal 29 Desember 2011)*

Tim Penerbit MADCOMS. 2010. *Sistem Jaringan Komputer untuk Pemula.* Yogyakarta : ANDI

BIODATA PENULIS

Nama	: Eti Rohani
Tempat dan Tanggal Lahir	: Sukoharjo. 4 Mei 1988
Jenis Kelamin	: Perempuan
Agama	: Islam
Perguruan Tinggi	: Universitas Muhammadiyah Surakarta
Alamat	: Jl, A. Yani Tromol Pos I Pabelan, Kartasura
Telp / Fax	: (0271) 717417
Alamat Rumah	: Malangan RT 01/03 Tiyaran, Bulu, Sukoharjo 57563
No. HP	: 085786255559
Alamat e-mail	: etyrohani@gmail.com