ANALISA KEAMANAN JARINGAN WIFI TERHADAP SERANGAN PACKET SNIFFING

Turkhamun Adi Kurniawan
t.adikurniawan@usni.ac.id
Fakultas Teknik Informatika
Universitas Satya Negara Indonesia, Jakarta

ABSTRAK

Jaringan komputer mempunyai dua media transmisi data yaitu kabel dan nirkabel. PT. XYZ merupakan sebuah perusahaan yang mempunyai fasilitas jaringan nirkabel (wifi). Jaringan wifi sangat rentan terhadap ancaman serangan, karena komunikasi yang terjadi bersifat terbuka. Diperlukan system pengamanan yang baik untuk dapat menjaga keamanan data pengguna agar dapat terhindar dari berbagai serangan yang dilakukan oleh orang–orang yang tidak bertanggung jawab. Penelitian ini membahas evaluasi tingkat keamanan fasilitas wifi di PT. XYZ dengan menggunakan Aplikasi Ettercap. Ettercap adalah tools packet sniffer yang dipergunakan untuk menganalisa protokol jaringan dan mengaudit keamanan jaringan, yang juga memiliki kemampuan untuk memblokir lalu lintas pada jaringan LAN, mencuri password, dan melakukan penyadapan aktif terhadap protokol-protokol umum. Dalam penelitian ini dilakukan serangan packet sniffing menggunakan software ettercap sebagai langkah pengujian keamanan di PT. XYZ. Hasil dari penelitian ini adalah dengan terdeteksinya keberadaan dan keamanan wifi yang terbuka atau tanpa pengamanan dan terekamnya username dan password. Hal ini dapat membahayakan keamanan lalulintas data para pengguna jaringan wifi maupun LAN kabel khususnya para karyawan/i, sehingga diperlukan peningkatan keamanan yang baik untuk dapat mencegah/menangani serangan packet sniffing dan yang lebih lanjut.

Kata Kunci*:* Ettercap, Sniffing, Keamanan Jaringan, Netstumbler

ABSTRACT

Computer networks have two data transmission media, namely wired and wireless. PT. XYZ is a company that has wireless network facilities (wifi). Wifi networks are very vulnerable to the threat of attack, because the communication that occurs is open. A good security system is needed to be able to maintain the security of user data in order to avoid various attacks by irresponsible people. This study discusses the evaluation of the security level of wifi facilities at PT. XYZ by using the Ettercap Application. Ettercap is a packet sniffer tool used to analyze network protocols and audit network security, which also has the ability to block traffic on a LAN network, steal passwords, and perform active wiretapping of common protocols. In this study, packet sniffing attacks were carried out using ettercap software as a security testing step at PT. XYZ. The results of this study are the detection of the presence and security of open or unsecured wifi and the recording of the username and password. This can jeopardize the data traffic security of users of wifi networks and wired LANs, especially employees, so that a good security enhancement is needed to prevent / handle packet sniffing attacks and more.

Keywords: Ettercap, Sniffing, Network Security, Netstumbler

.

.

PENDAHULUAN

Berbagai Issu keamanan jaringan saat ini menjadi sangat penting dan patut untuk diperhatikan. Sebuah jaringan yang terhubung dengan internet pada dasarnya tidak aman dan selalu dapat diekploitasi oleh para hacker, baik jaringan wired LAN maupun wireless LAN. Pada saat proses pengiriman data akan melewati beberapa terminal untuk sampai tujuan berarti akan memberikan kesempatan kepada pengguna lain yang tidak bertanggung jawab untuk menyadap atau mengubah data tersebut.

Dalam perancangan sebuah system keamanan jaringan yang handal maka perlu dipahami dengan baik melalui prosess analisa yang tepat sehingga system keamanan jaringan yang terhubung ke internet nantinya dapat berjalan efektif dan meminimalisir terjadinya serangan-serangan oleh para hacker. Ettercap adalah tools packet sniffer yang dipergunakan untuk menganalisa protokol jaringan dan mengaudit keamanan jaringan. Ia memiliki kemampuan untuk memblokir lalu lintas pada jaringan LAN, mencuri password, dan melakukan penyadapan aktif. Ia memiliki kemampuan untuk mencuri password, dan melakukan penyadapan aktif terhadap protokol-protokol umum. Sedangkan Netstumbler adalah tools wifi hacking yang digunakan untuk mendeteksi dan mengidentifikasi sinyal wireless yang terbuka dan menyusup ke dalam jaringan

DASAR TEORI

Studi Literatur

Menurut Thomas Setiawan (2004), pada penelitian dengan judul Analisis Keamanan Jaringan Internet Menggunakan Hping, Nmap, Nessus, dan Ethereal, yang berisi bahwa Sistem keamanan jaringan komputer yang terhubung ke Internet harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif. Apabila ingin mengamankan suatu jaringan maka harus ditentukan terlebih dahulu tingkat ancaman yang harus diatasi, dan resiko yang harus diambil maupun yang harus dihindari.

Penelitian lain yang dijadikan acuan adalah penelitian Aji Supriyanto (2006) dengan judul Analisis Kelemahan Keamanan Pada Jaringan Wireless, isi dari penelitiannya adalah Pemakaian perangkat teknologi berbasis wireless pada saat ini sudah begitu banyak, baik digunakan untuk komunikasi suara maupun data. Karena teknologi wireless memanfaatkan frekwensi tinggi untuk menghantarkan sebuah komunikasi, maka kerentanan terhadap keamanan juga lebih tinggi dibanding dengan teknologi komunikasi yang lainnya. Berbagai tindakan pengamanan dapat dilakukan melalui perangkat komunikasi yang digunakan oleh user maupun oleh operator yang memberikan layanan komunikasi. Kelemahan jaringan wireless secara umum dapat dibagi menjadi 2 jenis, yakni kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang digunakan. Secara garis besar, celah pada jaringan wireless terbentang di atas empat layer di mana keempat lapis tersebut sebenarnya merupakan proses dari terjadinya komunikasi data pada media wireless. Keempat lapis tersebut adalah lapis fisik, lapis jaringan, lapis user, dan lapis aplikasi. Model-model penanganan keamanan yang terjadi pada masing-masing lapis pada teknologi wireless tersebut dapat dilakukan antara lain yaitu dengan cara menyembunyikan SSID, memanfaatkan kunci WEP, WPA-PSK atau WPA2-PSK, implementasi fasilitas MAC filtering, pemasangan infrastruktur captive portal.

A. Konsep keamanan jaringan

Jaringan komputer adalah sebuah sistem yang terdiri atas sebuah komputer dan perangkat jaringan lainnya yang bekerja bersama-sama untuk mencapai suatu tujuan yang sama. Komputer dapat berhubungan satu dengan yang lainnya secara tidak terbatas baik dengan menggunakan kabel tembaga, fiber optik, infrared, gelombang microwave, bahkan bisa juga menggunakan satellite

B. Sniffing

Pembacaan data yang bukan tujuannya ini dikenal sebagai sniff. Program Sniffer yang digunakan adalah Network Monitor dari Distinct Corporation. Program ini merupakan versi trial yang berumur 10 hari. Di dalam komunikasi TCP/IP atau yang menggunakan model komunikasi 7 layer OSI, sebuah komputer akan mengirim data dengan alamat komputer tujuan. Pada sebuah LAN dengan topologi

bus atau star dengan menggunakan hub yang tidak dapat melakukan switch (hub tersebut melakukan broadcast), setiap komputer dalam jaringan tersebut menerima data tersebut. Standarnya hanya komputer dengan alamat yang bersesuaian dengan alamat tujuanlah yang akan mengambil data tersebut. Tetapi pada saat snif, komputer dengan alamat bukan alamat tujuan tetap mengambil data tersebut. Dengan adanya sniffer ini, maka usaha untuk melakukan kriptografi dalam database (dalam hal ini login user dan password) akan sia- sia saja

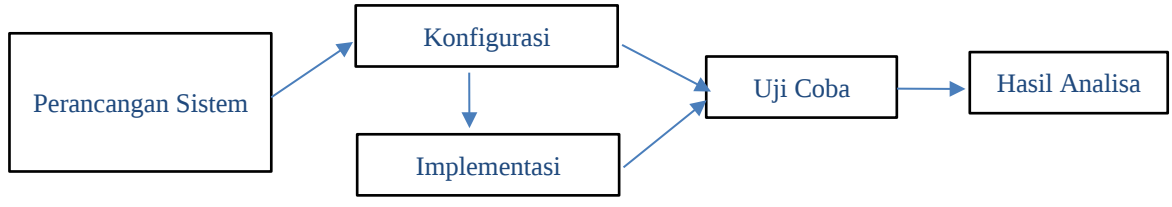
C. Etercap

Ettercap adalah alat untuk analisis protokol jaringan dan audit keamanan. Ia memiliki kemampuan untuk mencegat lalu lintas pada jaringan, menangkap password, dan melakukan menguping aktif terhadap protokol umum. Untuk latihan ini saya akan menggunakan ARP untuk mengendus Keracunan LAN untuk password yang menggunakan SSL (Hotmail, Gmail, dll). ARP adalah sebuah protokol jaringan komputer link layer untuk menentukan host jaringan atau alamat hardware saat hanya Internet layer nya (IP) atau alamat Network Layer dikenal. Fungsi ini sangat penting dalam jaringan area lokal serta untuk lalu lintas internetworking routing yang di gateway (router) berdasarkan alamat IP ketika router hop berikutnya harus ditentukan. Jadi dalam hal yang normal ARP adalah cara kita mendapatkan alamat MAC dari Host atau Node dari alamat IP. ARP Spoofing adalah teknik yang akan kita gunakan untuk menyerang sebuah kabel atau jaringan nirkabel. ARP Spoofing memungkinkan penyerang untuk mengendus frame data dari LAN, kemudian memberi Anda kemampuan untuk memodifikasi lalu lintas (baik untuk mengarahkan ke komputer anda sendiri untuk men-download mengeksploitasi korban), atau menghentikan lalu lintas dari memasuki jaringan, atau yang spesifik komputer

METODE PENELITIAN

Perancangan Sistem

Penjelasan masing-masing desain sistem dalam metode penelitian ini adalah sebagai berikut. 1. Perancangan Sistem Tahap ini merupakan tahap awal yang akan dilakukan untuk melakukan penelitian tentang keamanan jaringan pada fasilitas internet wifi terhadap serangan packet sniffing dengan menggunakan ids. 2. Konfigurasi & Implementasi Install aplikasi Ettercap pada linux yang digunakan untuk melakukan serangan packet sniffing, setelah melakukan instalasi peneliti melakukan konfigurasi terhadap aplikasi Ettercap dan install juga aplikasi / tools ids yang digunakan untuk melakukan pendeteksi adanya serangan packet sniffing, dan juga peneliti juga membuat rule-rule tertentu agar dapat mendeteksi serangan packet sniffing dengan indikasi arp spoofing. 3. Uji Coba Pertama user akan terhubung ke access point yang sudah tersedia, lalu PC penyerang akan melakukan serangan packet sniffing terhadap access point, maka PC pendeteksi akan mendeteksi adanya serangan packet sniffing dengan indikasi arp spoofing. 4. Hasil Analisa Peneliti akan menganalisa hasil uji coba serangan packet sniffing dan mendeteksi serangan dengan menggunakan ids.



Gambar 1. Proses Perancangan Sistem

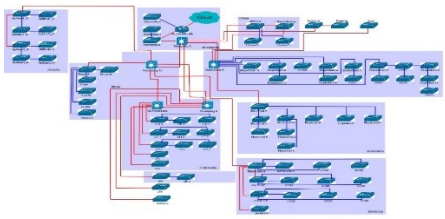
ANALISA DAN IMPLEENTASI SISTEM

Analisa system berjalan.

Analisis perlu dilakukan untuk mengetahui seberapa aman tingkat keamanan yang telah diterapkan dalam sebuah jaringan kabel maupun wireless/nirkabel. Seperti yang kita ketahui

tingkat keamanan bukan hanya berasal dari hardware dan software yang sudah ada namun peran penting dari manusia/pengguna yang melakukan konfigurasi dan dari perancangan jaringan itu sendiri.

Keamanan Jaringan yang terinstall di PT.XYZ pada umumnya masih perlu peningkatan yang terbukti pada wifi tidak menggunakan keamanan atau open (terbuka). Di samping itu juga masih banyak karyawan yang masih awam dengan yang amanya keamanan jaringan computer.

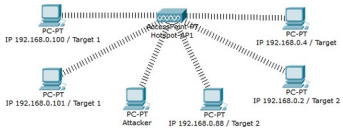


Gambar 2. Jaringan Komputer

Implementasi Sistem

Tahap pertama Mengidentifikasi Wifi Percobaan ini dilakukan untuk mengidentifikasi keberadaan wifi dalam bentuk informasi lengkap dengan nama SSID, mac address, RSSI, vendor, channel yang dipakai, network type dan security atau keamanan yang digunakan. Hal ini dilakukan untuk memudahkan penyerangan untuk mendapatkan koneksi dengan jaringan wifi yang ada. Dalam percobaan ini peneliti mendapatkan wifi yang tidak berpengaman / open.

Tahap kedua Packet Sniffing Percobaan ini dilakukan untuk mendapatkan informasi penting mengenai account username, password, akses DNS yang dituju dan informasi lain. Hal ini dimaksudkan agar penyerang dapat melakukan pengaksesan internet secara tidak sah demi keuntungan pribadi yang dapat mengakibatkan kerugian pada pengguna yang berada dalam jaringan. Dengan demikian, peneliti dapat menyatakan tidak aman karena semua kegiatan dapat dengan mudah terekam dan mudah dicuri.



Gambar 4.1 Tampilan Simulasi Serangan

Gambar diatas adalah gambaran skenario dimana attacker melakukan penyerangan dengan mengelompokkan target menjadi dua kelompok yaitu target 1 dan target 2 yang dimana berfungsi ketika target utama atau target 1 tidak melakukan aktifitas maka penyeangan akan berpindah pada target 2 begitu pula sebaliknya hingga attacker dapat merekam semua aktifitas yang berjalan

Solusi Untuk Mencegah Serangan Packet Sniffing

Setelah menganalisis peneliti telah menyiapkan beberapa rekomendasi solusi untuk meningkatkan keamanan jaringan dari suatu serangan seperti yang dilakukan peneliti untuk menganalisis keamanan jaringan yang dapat diterapkan oleh pihak PT.XYZ, seperti : membedakan jaringan antara jaringan wifi/LAN kantor dengan wifi untuk fasilitas pengguna, agar ketika seorang attacker menyerang menggunakan teknik Packet Sniffing tidak dapat menembus jaringan pada wifi/LAN kantor. Secara teknis solusi diatas dapat diterapkan dengan menyeting ulang subnetting, untuk wifi/LAN kantor, misal dengan IP 192.168.2.1/25 untuk 128 host untuk switch LAN karyawan1, IP 192.168.2.129/25 untuk 128 host untuk switch LAN karyawan2 dan untuk wifi umum dengan IP 192.168.3.1/26 untuk 64 host

Konfigurasi Device Network

Tahapan-tahapan Instalasi dan Konfigurasi Software :

1. Instalasi software Netstumbler pada windows 7
2. Klik 2x pada file netstumblerinstaller_0_4_0.exe untuk instalasi, kemudian ikuti perintah selanjutnya dengan klik i agree, next dan install sampai selesai.
3. Konfigurasi device network yang terhubung dengan laptop pada netstumbler dengan cara meng-klik pilihan device:

Gambar 3.2. konfigurasi *device network adaptor* pada *software netstumbler*

Setelah melihat gambar 3.2. ternyata *device network adaptor* yang terhubung dengan laptop peneliti tidak *support*, karena *software netstumbler* hanya dapat berjalan sempurna pada *windows XP* dan tidak dapat berjalan sempurna pada *windows 7*. Kemudian peneliti menggantinya dengan software *inSSIDer* sebagai alternatif *software netstumbler* untuk *windows 7*

Gambar 3.3. Tampilan *software inSSIDer* pada *windows 7*

Penutup

Kesimpulan

Berdasarkan dari analisis data maka dapat diambil kesimpulan, bahwa sistem keamanan jaringan LAN yang mencakup jaringan kabel dan nirkabel pada *PT.XYZ* masih perlu peningkatan, hal ini dibuktikan dengan : Penyerangan packet sniffing yang dapat merekam dan menampilkan username dan password dengan menggunakan aplikasi Ettercap.

Saran

Berdasarkan uraian dari kesimpulan, maka kelebihan dan kekurangan di atas dapat menjadi pelajaran serta referensi untuk ke depannya. Saran – saran yang dapat dipertimbangkan untuk ke depan antara lain : Diperlukan keamanan WPA2-PSK sebagai keamanan awal wifi untuk dapat meminimalisir sebelum terjadinya serangan packet sniffing.

Daftar Pustaka

Handriyanto, Dwi Febrian. 2009. Kajian Penggunaan Mikrotik Router OS Sebagai Router Pada Jaringan Komputer. Palembang. Universitas Sriwijaya

Handriyanto, Dwi Febrian. 2009. Kajian Penggunaan Mikrotik Router OS Sebagai Router Pada Jaringan Komputer. Palembang. Universitas Sriwijaya

Noviyanto, Hendri. 2011. Analisis Keamanan Wireless di Universitas Muhammadiyah Surakarta. Surakarta : Tugas Akhir Universitas Muhammadiyah Surakarta

Netstumbler Home Page. 2012. " Software Netstumbler ", (http://www.netstumbler.com, diakses pada tanggal 9 Maret 2012)

Oktavianto, Digit. 2012. " Mencegah ARP Spoofing Dan ARP Poisoning Di Linux ", (http://digitoktavianto.web.id/mencegah-arp-spoofing-dan-arppoisoning-di-linux.html, diakses pada tanggal 19 April 2012)