INTISARI

ANALISIS KEAMANAN JARINGAN WIFI WPA-2 PERSONAL/PSK TERHADAP SERANGAN PACKET ANALYZER/SNIFFING

Oleh:

Harryson Baringin Samosir

11/314237/PA/13764

Perkembangan penggunaan internet yang semakin lama semakin canggih memungkinkan penggunanya untuk dapat melakukan pertukaran informasi hanya dengan menekan tombol saja. Informasi juga bermacam-macam dan pastinya ada informasi yang bersifat sensitif dan tak ingin orang lain mengetahuinya. Namun melakukan transmisi melalui internet memiliki kelemahan dibagian keamanannya dan merupakan masalah utama. Protokol Kemanan SSL merupakan salah satu usaha yang dilakukan untuk mencegah terjadinya serangan-serangan ilegal yang dapat mengekspos informasi dari pengguna. Ketika Komputer mengirim data melalui jaringan, data tersebut akan ditrasmisi kedalam bentuk paket-paket data. Sniffing adalah satu cara yang dapat digunakan untuk mencuri informasi dari paket-paket data yang mengalir tadi. Informasi yang diperoleh dari paket data tersebut pun macam-macam ada yang berupa password, id username, e-mail, atau informasi sensitif lainnya.

Pada penelitian ini dilakukan 2 tahap uji coba pencurian paket data yang pertama hasilnya berupa *username* dan *password* sebuah akun, uji coba kedua hasilnya berupa gambar. Aplikasi yang digunakan adalah Ettercap untuk data berupa teks dan Driftnet untuk data berupa gambar. Serangan yang dilakukan terhadap protokol keamanan SSL adalah dengan *ARP Poisoning*. *ARP Poisoning* adalah sebuah cara dimana penyerang membangun sebuah koneksi antara *client* dengan *server* dan menjadikan dirinya sebagai jembatan yang membuat penyerang dapat melihat atau memonitor segala aktivitas *client* dengan *server.*

Dari hasil pengujian diperoleh bahwa Protokol Kemanan SSL dalam penelitian ini belum sudah menjamin 100% keamanan pengguna dan website yang menggunakannya. Namun soal kemanan kembali lagi kepada pengguna pada saat mengakses internet karena metode yang digunakan pada penelitian ini bertujuan untuk mengelabui pengguna terbukti bahwa *username*/*password* dan gambar terekam ketika target pengguna mengakses sebuah website dengan menghiraukan *policy* dari sertifikat SSL. Hal ini dapat membahayakan privasi dari pengguna dan kenyamanan mengakses internet, sehingga sangat diperlukan peningkatan sistem keamanan lebih lanjut untuk mencegah serangan ilegal yang dapat mengganggu pengguna.

ABSTRACT

ANALYSIS OF WIFI WPA2 PERSONAL/PSK NETWORK SECURITY AGAINST PACKET ANALYZER/SNIFFING ATTACKS

By:

Harryson Baringin Samosir

11/314237/PA/13764

The use of the Internet at this time is growing rapidly allow user to be able to exchange information by simply pressing buttons. There's many type of information and definitely there's some sensitive information that we need to keep it safe from outsiders. But transmitting data via internet has flaws, the most major problem that we need to face is the security system. Protocol Security SSL is one of many way to keep user safe. When computer sends data over the network, the data is transmitting into parts called packet data. Sniffing is one of many way to steal information inside packet data. Information that can be obtained from Sniffing are password, username, e-mail, or other sensitive information.

This research conducted two phase of trial the first trial yield *username* and *password* for website account, the second trial yield images. Applications that used in the research are Ettercap and Driftnet, Ettercap for text data and driftnet for images data. The attack done by using a technique called ARP Poisoning. ARP Poisoning is a technique where attacker build a connection between the *client* and *server* connections and establish itself as the connection that makes the attacker can view or spy all the activities between the *client* and the *server* which allow attacker to look at the contents inside packet data that flow from client to server.

From the test results showed that the security protocol SSL network is still lacking and can not guarantee 100% that user and website are safe. Proved that *username* / *password* and the image data being recorded when a user accessing a multiple of websites. This may threaten the privacy of users and the convenience of accessing the internet, so it is necessary to increase the security system to prevent further attacks by Packet Sniffer or any other illegal activity. Moreover the level of SSL security depends on the classification of SSL ifself. SSL is divides into 5 level called class. Each class has a different security level and different purposes.