Perancangan dan Analisis Aplikasi Smart Penetration Tester dengan Metode Sniffing dalam Network Security

Fernando Alexsandro Siregar[1], Satria Mandala[2]

[1,2]Fakultas Informatika, Universitas Telkom, Bandung

[1]fernandoalex@students.telkomuniversity.ac.id, [2]pembimbing1@telkomuniversity.ac.id,

Abstrak

Saat ini perkembangan teknologi informasi dari waktu ke waktu telah berkembang sangat pesat begitu juga keamanan informasi yang terdapat dalam teknologi tersebut menjadi sangat penting, sehingga proses melakukan pencurian data maupun informasi menggunakan (*Packet Sniffer*) akan sangat biasa di lakukan apabila kemanan informasi tesebut tidak di enkripsi dengan baik, proses *sniffing* yang saya lakukan bersifat *Penetration Tester* yaitu keadaan dimana seseorang menguji keamanan data informasi yang dikirimkan dari sebuah client ke server sehingga pihak server akan mengetahui bagaimanan data informasi tersebut dapat di curi dengan hanya memonitoring paket data yang keluar dan masuk pada jaringan LAN. Proses *packet sniffing* yang dilakukan menggunakan Bahasa pemograman python yang di modifikasi untuk memonitoring packet data yang masuk dan keluar pada jaringan network berbasis LAN, pada aplikasi yang saya buat terdapat 3 skenario protokol yang dapat di jalankan, yakni UDP, TCP, dan ICMP. Skenario protokol ini dibuat untuk mengetahui seberapa baik *packet sniffer* bekerja pada lapisan tersebut dikarena fungsi dari ketiga protokol tersebut berbeda-beda, karena itu saya ingin mengetahui seberapa baik aplikasi ini bekerja pada lapisan UDP, TCP, dan ICMP pada jaringan LAN(*Local Area Network).* Berdasarkan implementasi dan analisis yang telah dilakukan hasil yang didapat berdasarkan kalkulasi packet yang telah dimonitoring dengan menggunakan aplikasi sehingga di dapatkan bahwa lapisan UDP yang paling mudah di monitoring pada posisi pertama, dan lapisan TCP pada posisi kedua dan terakhir adalah ICMP dan ini tidak selamanya pada posisi tersebut dikarenakan tergantung pada keadaan komunikasi pada jaringan dan keadaan stabil pada internet.

Kata kunci : penetration tester, UDP, TCP, ICMP, LAN, packet sniffer.

Abstract

At present the development of information technology from time to time has developed very quickly so that the information in the technology becomes very important, and the process of using data or information (Sniffer Package) will be very common in security information is not encrypted. Well, the sniffing process that I do as Penetration Tester is the location where someone uses information data sent from a client to the server. The party server will provide information such as information data that can be stolen by only selecting data packets that come out and enter the LAN network. The packet sniffing process is carried out using a modified python programming language to monitor incoming and outgoing packet data on a LAN network, in the application I created there are 3 protocol scenarios that can be run, namely UDP, TCP, and ICMP. This protocol scenario is made to determine whether the packet sniffer works on a different function than the different, because it will be very easy to use on UDP, TCP, and ICMP on LAN (Local Area Network) networks. Through the implementation and analysis of the results that have been done with packages that have been monitored using the application that is most easily monitored in the first position, and the TCP layer in the second and final position is ICMP and does not turn on the position depending on the state of communication on network and stable state on the internet.

Keywords: penetration tester, UDP, TCP, ICMP, LAN, packet sniffer.