FACULTY OF COMPUTER SCIENCE
PUTRA INDONESIA UNIVERSITY "YPTK"
Thesis, August 2024

MHD HANAFI AKBAR

EVALUATION OF NETWORK (WI-FI) SECURITY AGAINST PACKET SNIFFING ATTACKS ON HTTP AND HTTPS PROTOCOLS AT PT PELABUHAN INDONESIA (PERSERO) REGIONAL 2 TELUK BAYUR

ABSTRACT

Computer networks are not something new nowadays, almost every place there is a computer network to facilitate the flow of information in that place. In a computer network, there are lots of data packets passing by on network cables or wirelessly, both data packets containing important personal information, namely usernames and passwords, site addresses, user IP addresses and so on. In general, every network connected via the internet has a low level of security so it can still be exploited by hackers. Given this problem, researchers carried out a network security evaluation (wi-fi) against packet sniffing attacks on the http and https protocols at PT. Indonesian Harbor II Padang branch office.This research analyzes the effectiveness of security protocols, especially the use of Secure Socket Layer (SSL) on Wi-Fi networks, in protecting data from sniffing attacks. This research uses attack simulations using the Burpsuite and Wireshark applications to compare the level of security between websites that use the HTTPS protocol and those that only use HTTP. The research results show that there is a significant difference in the level of security between the HTTP and HTTPS protocols. The HTTPS protocol is proven to be better able to protect sniffing attacks data from compared to HTTP. The HTTP protocol is very vulnerable to packet sniffing attacks due to the lack of data encryption. The transmitted data can easily be stolen and misused by attackers. It is recommended that PT. Pelabuhan Indonesia II Padang organizes routine cyber security training programs and simulates social engineering attacks for employees and implements a security monitoring and analysis system to detect and respond quickly to threats.

Keywords: Network security, WI-FI, HTTP AND HTTPS, Packet Snifing

FAKULTAS ILMU KOMPUTER
UNIVERSITAS PUTRA INDONESIA "YPTK"
Skripsi, Agustus 2024

MHD HANAFI AKBAR

EVALUASI KEAMANAN JARINGAN (*Wi-Fi)* TERHADAP SERANGAN PACKET SNIFFING PADA PROTOCOL HTTP DAN HTTPS DI PT. PELABUHAN INDONESIA (PERSERO) REGIONAL 2 TELUK BAYUR

ABSTRAK

Jaringan komputer bukanlah sesuatu yang baru saat ini, hampir disetiap tempat terdapat jaringan komputer untuk memperlancar arus informasi pada tempat tersebut. Di dalam jaringan komputer banyak sekali paket data yang berlalu lalang pada kabel jaringan maupun nirkabel, baik itu paket data yang mangandung informasi- informasi penting yang bersifat pribadi yaitu *username* dan *password*, alamat dari sebuah situs, *ip address user* dan sebagainya. Pada umumnya s+etiap jaringan yang terhubung melalui internet tingkat keamanannya masih rendah sehingga masih dapat diekploitasi oleh para *hacker.* Dengan adanya masalah tersebut maka peneliti melakukan evaluasi keamanan jaringan (*wi-fi*) terhadap serangan *packet sniffing* pada protocol *http* dan *https* di PT. Pelabuhan Indonesia II kantor cabang padang. Penelitian ini menganalisis efektivitas protokol keamanan, khususnya penggunaan *Secure Socket Layer (SSL*) pada jaringan *Wi-Fi*, dalam melindungi data dari serangan *sniffing*. Penelitian ini menggunakan simulasi serangan menggunakan *aplikasi Burpsuite* dan *Wireshark* untuk membandingkan tingkat keamanan antara situs *web* yang menggunakan protokol *HTTPS* dengan yang hanya menggunakan *HTTP*.Hasil penelitian menunjukkan adanya perbedaan signifikan dalam tingkat keamanan antara protokol *HTTP* dan *HTTPS*. Protokol *HTTPS* terbukti lebih mampu melindungi data dari serangan sniffing dibandingkan dengan *HTTP*. Protokol *HTTP* sangat rentan terhadap serangan *packet sniffing* karena tidak adanya enkripsi data. Data yang ditransmisikan dapat dengan mudah dicuri dan disalahgunakan oleh penyerang. Disarankan, pihak PT. Pelabuhan Indonesia II Padang menyelenggarakan program pelatihan keamanan *cyber* yang rutin dan mengadakan simulasi serangan *social engineering* kepada pegawai serta mengimplementasikan sistem pemantauan dan analisis keamanan untuk mendeteksi dan merespons ancaman dengan cepat

Kata Kunci : Keamanan jaringan, *WI-FI, HTTP* DAN *HTTPS, Packet Snifing*