ABSTRAK

Nama	:	Fadhilah Jasman
Program Studi	:	Teknik Informatika
Judul	:	Analisis Keamanan Website Terhadap Packet Sniffing pada Jaringan Wifi Menggunakan Aplikasi Wireshark

Serangan packet sniffing yang mana pada packet sniffing dapat menyadap komunikasi antara web browser dan server tanpa diketahui target. Serta untuk mengetahui bagaimana tingkat keamanan dari protokol-protokol pertukaran data (Hypertext Transfer Protocol) HTTP dan (Hypertext Transfer Protocol Secure) HTTPS.Dari hasil analisis kemanan website terhadap protokol jaringan antara HTTP dan HTTPS terhadap serangan packet sniffing yaitu dapat melakukan monitoring aktifitas yang dilakukan pengguna menggunakan tools pihak ketiga oleh network analyzer dengan tujuan untuk mengontrol pengawasan terhadap pengguna sehingga administrator dapat memantau pertukaran data yang terjadi antara web browser dengan server yang mencurigakan.

Dalam penelitian ini dilakukan dua tahap, yang pertama yaitu mengidentifikasi tingkat keamanan website menggunakan aplikasi Wireshark dan yang kedua yaitu membandingkan tingkat keamanan website dengan Google Account untuk mengetahui kelemahannya. Hasil dari penelitian ini adalah dengan penyerangan packet sniffing pada website, dapat merekam dan menampilkan informasi sensitif seperti username dan password dengan menggunakan aplikasi wireshark. Selain itu website rentan terhadap serangan MITM (man in the middle), karena belum menggunakan sertifikat SSL.

Kata Kunci: Keamanan Website, Packet Sniffing, Protocol HTTP dan HTTPS

ABSTRACK

Name	:	Fadhilah Jasman
Study Program	:	Teknik Informatika
Title	:	Analysis of Website Security Against Packet Sniffing on Wifi Networks Using the Wireshark Application

Packet sniffing attacks in which packet sniffing can intercept communications between web browsers and servers without the target knowing. As well as to find out how the level of security of data exchange protocols (Hypertext Transfer Protocol) HTTP and (Hypertext Transfer Protocol Secure) HTTPS. From the results of website security analysis on network protocols between HTTP and HTTPS against packet sniffing attacks, namely being able to monitor activities carried out users use third-party tools by network analyzer with the aim of controlling surveillance of users so that administrators can monitor the exchange of data that occurs between suspicious web browsers and servers.

In this research two stages were carried out, the first was to identify the level of website security using the Wireshark application and the second was to compare the level of website security with a Google Account to find out its weaknesses. The result of this study is that with packet sniffing attacks on websites, it can record and display sensitive information such as usernames and passwords using the Wireshark application. In addition, the website is vulnerable to MITM (man in the middle) attacks, because it does not use an SSL certificate.

Keywords: *Website Security, Packet Sniffing, HTTP and HTTPS Protocols*