ANALISIS KEAMANAN JARINGAN PADA FASILITAS *WIFI* TERHADAP SERANGAN *SNIFFING*

SKRIPSI

Oleh:

Putri Rosayanti Silalahi
180210034

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN KOMPUTER
UNIVERSITAS PUTERA BATAM
2024

ANALISIS KEAMANAN JARINGAN PADA FASILITAS *WIFI* TERHADAP SERANGAN *SNIFFING*

SKRIPSI

Untuk memenuhi salah satu syarat

memperoleh gelar sarjana

Oleh:

Putri Rosayanti Silalahi
180210034

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN KOMPUTER
UNIVERSITAS PUTERA BATAM
2024

SURAT PERNYATAAN ORISINALITAS

Yang bertanda tangan di bawah ini saya:

Nama	: Putri Rosayanti Silalahi
NPM	: 180210034
Fakultas	: Teknik dan Komputer
Program Studi	: Teknik Informatika

Menyatakan bahwa **"Skripsi"** yang saya buat dengan judul:

"ANALISIS KEAMANAN JARINGAN WIFI TERHADAP SERANGAN SNIFFING"

Ini bukan "duplikasi" karya orang lain; itu sepenuhnya ciptaanmu sendiri. Sepanjang pengetahuan saya, karya ilmiah atau pendapat yang dimuat dalam naskah skripsi ini hanyalah yang dikutip secara tertulis dan dicantumkan dalam daftar pustaka dan sumber kutipan. Semua karya dan opini lainnya telah ditulis atau diterbitkan oleh orang lain.

Apabila terbukti naskah tesis saya mengandung unsur PLAGIASI, maka saya setuju untuk dibatalkan dan gelar akademik saya dicabut, sesuai dengan peraturan perundang-undangan yang berlaku.

Oleh karena itu saya sungguh-sungguh membuat pernyataan ini bebas dari segala tekanan pihak luar.

Batam, 23 Februari 2024

Putri Rosayanti Silalahi

180210034

ANALISIS KEAMANAN JARINGAN PADA FASILITAS *WIFI* TERHADAP SERANGAN *SNIFFING*

SKRIPSI

Untuk memenuhi salah satu syarat
guna memperoleh gelar Sarjana

Oleh
Putri Rosayanti Silalahi
180210034

Telah disetujui oleh Pembimbing pada tanggal
Seperti tertera di bawah ini

Batam,23 Februari 2024

Sunarsan Sitohang, S.Kom., M.TI.
Pembimbing

ABSTRAK

Perkembangan teknologi dan ketergantungan pada jaringan *WiFi* memberikan manfaat besar dalam dunia bisnis, termasuk di YAMAHA, PT ALFA SCORPII Tembesi. Namun, kekhawatiran terhadap keamanan jaringan semakin meningkat, terutama dengan serangan cyber yang semakin kompleks. Salah satu ancaman yang muncul adalah serangan *sniffing*, di mana penyerang berusaha mencuri data sensitif melalui jaringan *WiFi*. Wireshark, sebagai alat peretasan *WiFi*, memainkan peran krusial dalam mengidentifikasi dan mengatasi potensi ancaman keamanan jaringan. Alat ini memiliki kemampuan untuk mendeteksi sinyal nirkabel terbuka, menganalisis protokol jaringan, dan mengaudit keamanan jaringan. Selain itu, Wireshark dapat melakukan tindakan lebih lanjut seperti memblokir lalu lintas di jaringan *LAN*, mencuri kata sandi, dan melakukan penyadapan aktif pada protokol umum. Penelitian ini dilakukan dalam dua tahap. Tahap pertama adalah mengidentifikasi keberadaan dan keamanan jaringan *WiFi* di YAMAHA, PT ALFA SCORPII Tembesi. Sementara itu, tahap kedua melibatkan serangan paket *sniffing* menggunakan perangkat lunak Wireshark. Penelitian ini bertujuan untuk melakukan analisis mendalam terhadap keamanan jaringan *WiFi* di perusahaan tersebut terhadap serangan *sniffing*. Hasil penelitian ini memberikan wawasan lebih mendalam tentang tingkat keamanan jaringan *WiFi* di YAMAHA, PT ALFA SCORPII Tembesi. Selain itu, diharapkan penelitian ini membantu perusahaan mengidentifikasi dan mengatasi potensi kerentanan keamanan yang dapat dieksploitasi oleh serangan *sniffing*. Dengan meningkatkan keamanan jaringan, YAMAHA, PT ALFA SCORPII Tembesi dapat memastikan bahwa data sensitif pelanggan dan informasi perusahaan tetap aman dari ancaman serangan *sniffing*.

Kata kunci: Analisis Keamanan, *Sniffing*, *Wireshark*

ABSTRACT

The integration of technology and reliance on WiFi networks has yielded substantial advantages in the business domain, including at YAMAHA, PT ALFA SCORPII Tembesi. Nevertheless, concerns over network security are escalating, particularly in the face of growing cyber threats. One such potential menace is sniffing attacks, where perpetrators seek to pilfer sensitive data transmitted across WiFi networks. Wireshark, functioning as a WiFi hacking tool, assumes a pivotal role in pinpointing and mitigating potential security risks to the network. This tool possesses the capability to identify open wireless signals, scrutinize network protocols, and audit network security. Moreover, Wireshark can execute actions like obstructing traffic on LAN networks, pilfering passwords, and actively eavesdropping on common protocols. The research unfolds in two phases – the initial phase encompasses recognizing the existence and security of WiFi networks at YAMAHA, PT ALFA SCORPII Tembesi. Simultaneously, the second phase involves executing packet sniffing attacks using Wireshark software. The primary objective of this research is to undertake a thorough analysis of WiFi network security at the company concerning sniffing attacks. The results of this research provide deeper insight into the security level of the WiFi network at YAMAHA, PT ALFA SCORPII Tembesi. Furthermore, the research is poised to aid the company in detecting and rectifying potential security vulnerabilities susceptible to exploitation via sniffing attacks. Through fortifying network security, YAMAHA, PT ALFA SCORPII Tembesi can ensure the safeguarding of customer-sensitive data and company information from the looming threat of sniffing attacks.

Keyword: Security Analysis ,Sniffing,Wireshark

KATA PENGANTAR

Puji syukur kehadirat Tuhan Yang Maha Esa , atas segala limpahan nikmat dan karunia-Nya yang tak terhingga, sehingga penulis dapat melakukan dan menyelesaikan penelitian di YAMAHA, PT ALFA SCORPII Tembesi serta dapat menyelesaikan skripsi yang merupakan salah satu persyaratan untuk menyelesaikan jenjang strata satu (S1) pada Program Studi Teknik Informatika Universitas putera batam.

selanjutnya penulis mengucapkan terimakasih kepada pihak-pihak yang telah mendukung secara langsung maupun tidak langsung dalam kelancaran skripsi ini, antara lain:

1. Rektor Universitas Putera Batam, Ibu Nur Elfi Husda, S.Kom.,M.SI.
2. Dekan Fakultas Teknik dan Komputer, Bapak Welly Sugianto, S.T.,M.Mm.
3. Ketua Program Studi Teknik Informatika Universitas Putera Batam, Bapak Andi Maslan,.S.T.,M.SI.
4. Bapak Sunarsan Sitohang, S.Kom., M.TI. selaku pembimbing skripsi, yang telah bersedia memberikan masukan, nasehat dan dukungannya kepada penulis. Terima kasih, Pak.
5. Bapak Elbert Hutabri, S.Kom., M.Kom. Selaku dosen pembimbing akademik.
6. Dosen dan Staff Universitas Putera Batam.
7. Orang Tua Tercinta, Yang selalu memberikan kasih sayang, dukungan, semangat, moril dan materil yang tak terhingga serta doa. Terima kasih atas jasa yang tak terhingga.
8. Teman, Kakak, Abang, sahabat penulis yang selalu memberi semangat dan dukungan kepada penulis untuk menyelesaikan sripsi.
9. Teman-teman sekelas Teknik Informatika Kelas *Shift*, Teman-teman Teknik Informatika Angkatan 2018 Universitas Putera Batam. Terima kasih untuk segala dukungan dan doa.
10. Kepada pihak-pihak yang telah banyak membantu, mohon maaf apabila tak disebut nama, dan mohon maaf apabila tak disebut gelar. Terima kasih.

Semoga Allah membalas segala kebaikan, memudahkan segala urusan serta mencurahkan rahmat-Nya. Aamiin.

Batam, 23 Februari 2024

Putri Rosayanti Silalahi

DAFTAR ISI

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman