IMPLEMENTASI KEAMANAN DATABASE DARI SERANGAN PACKET SNIFFING PADA DEPARTEMEN TI PT PUPUK SRIWIDJAJA PALEMBANG

[1]Misinem, [2*]M. Agung
[1]Teknik Komputer, Fakultas Vokasi, Universitas Bina Darma Palembang
[2] Teknik Komputer, Fakultas Vokasi, Universitas Bina Darma Palembang
*Misinem@binadarma.ac.id

Abstract *- PT Pupuk Sriwidjaja Palembang is one of the companies engaged in the manufacturing industry in the form of urea fertilizer as raw material, this agency uses a Storage Area Network (SAN) as data storage, the agency uses wired and wireless internet to process data and input it to the website company. Sniffing is the act of capturing data packets that pass through the network. Sniffing is very dangerous if eavesdroppers take action or modify network data packets, because data can be stolen. The theft of the data can have an impact on certain parties. Data is obtained by attackers using sniffing attacks when data is sent via wifi networks, hotspots, servers and others. So that this becomes the background of this research which has the formulation of the problem is How to implement database security from packet sniffing attacks at the Department TI of PT Pupuk Sriwidjaja Palembang. The trick is to use a VPN / IPSec tunnel using a proxy tool. This study uses the Action Research method which includes diagnosis, action plan, action, evaluation, and learning. After implementing security using a VPN in the Department TI of PT Pupuk Sriwidjaja, packet sniffing makes security difficult to penetrate*

Keywords: Sniffing, Database Security, VPN, IPSec, Mikrotik

Abstrak - PT Pupuk Sriwidjaja Palembang merupakan salah satu perusahaan yang bergerak dalam industri manufacture berupa pupuk urea sebagai bahan bakunya, instansi ini menggunakan *Storage Area Network (SAN)* sebagai penyimpanan data-data, instansi tersebut menggunakan internet kabel dan *wireless* untuk mengolah data dan menginput nya ke website perusahaan. *Sniffing* merupakan tindakan menangkap paket data yang melewati jaringan. *Sniffing* sangat berbahaya jika penyadap mengambil tindakan atau memodifikasi paket data jaringan, karena data dapat dicuri. Pencurian data tersebut dapat berdampak pada pihak tertentu. Data didapatkan penyerang dengan menggunakan serangan *sniffing* saat ada data yang dikirim melalui jaringan wifi, *hotspot*, server dan lain-lain. Sehingga hal tersebut menjadi latar belakang penelitian ini yang mempunyai rumusan masalah adalah Bagaimana menerapkan keamanan database dari serangan packet *sniffing* pada Departemen TI PT Pupuk Sriwidjaja Palembang. Caranya adalah menggunakan VPN / IPSec Tunnel dengan menggunakan alat mikrotik. Penelitian ini menggunakan metode *Action Research* yang meliputi diagnosa, rencana tindakan, melakukan tindakan, evaluasi, dan pembelajaran. Setelah adanya penerapan keamanan menggunakan VPN di Departemen TI PT Pupuk Sriwidjaja maka keamanan sulit ditembus oleh packet *sniffing.*

Kata kunci: *Sniffing, Keamanan Database, VPN, IPSec, Mikrotik*

1. Pendahuluan

Perkembangan teknologi informasi semakin pesat khususnya di era modern seperti sekarang ini, seiring dengan berkembangnya teknologi. Dengan berkembangnya teknologi informasi saat ini, kebutuhan akan informasi semakin meningkat. Dimana setiap masyarakat membutuhkan informasi dalam waktu yang cepat, singkat, dan akurat. Namun permasalahan yang sering muncul adalah faktor keamanan saat ini menjadi menjadi perhatian yang sangat penting. Sehingga diperlukan suatu metode untuk dapat memperoleh suatu informasi data , pertukaran data, dilakukan dengan aman dan stabil [5]. Keamanan database harus dikembangkan dan diutamakan agar tidak ada yang membobol sebuah data penting yang ada di

dalam server. Kebutuhan akan keamanan database berasal dari kebutuhan untuk melindungi data. Pertama, kehilangan data dan kerusakan data. Kedua, beberapa pihak tidak berwenang untuk mengakses atau mengubah data. Masalah lain termasuk melindungi data dari penundaan yang tidak semestinya dalam akses atau penggunan data, atau menyelesaikan masalah penolak layanan

PT. Pupuk Sriwidjaja merupakan salah satu perusahaan yang bergerak dalam industri manufacture berupa pupuk urea sebagai bahan bakunya. Departemen TI PT Pupuk Sriwidjaja (PUSRI) yang berada di Jl. Mayor Zen, Kalidoni Palembang adalah instansi milik negara yang menproduksi dan mengelola Pupuk urea Di Indonesia, instansi ini menggunakan *Storage Area Network (SAN)* sebagai penyimpanan data-data, Instansi tersebut menggunakan internet kabel dan *wireless* untuk mengolah data dan menginputnya ke *website* perusahaan. Bahaya yang tidak diharapakan bisa terjadi kapanpun tanpa sepengetahuan Pegawai/Staff ketika menggunakan jaringan *wireless*. Bahkan *Wifi* instansi tersebut bisa saja diretas oleh hacker. Berdasarkan hal tersebut, dengan maraknya kejahatan pada keamanan database salah satunya adalah *website* yang harus dikembangkan dan diutamakan agar tidak ada yang membobol sebuah data penting yang ada di dalam *website* server.

Penelitian ini bertujuan untuk Menerapkan keamanan data informasi yang dilakukan secara *real time* jika *user* menerapkan keamanan jaringan menggunakan VPN IPSec dari beberapa ancaman *packet sniffing* yang ada pada jaringan internet.

2. Tinjauan Pustaka

2.1 Mikrotik Router OS

Mikrotik Router OS adalah sistem operasi dari perangkat lunak Mikrotik Router *Board*. Sistem operasi ini bisa juga di install di komputer biasa dan menjadikannya sebagai router dengan fitur-fitur yang sudah tersedia, seperti : routing , firewall, bandwith management, *Wireless* acces point, dll [9].

2.2 Winbox

Winbox merupakan sebuah *software* yang digunakan untuk proses konfigurasi ke *server* mikrotik. Winbox digunakan dalam konfigurasi mikrotik dalam sebuah *server* yang melalui media komputer, maka di gunakan winbox sebagai pengkonfigurasi mikrotik [1].

2.3 VPN

VPN merupakan sebuah jaringan publik yang menjamin ketersediaan jalur komunikasi untuk suatu perusahaan tetapi tidak dalam bentuk jalur khusus. VPN merupakan sebuah sistem yang dipuji sebagai solusi yang mampu mengatasi semua masalah untuk meningkatnya biaya koneksi WAN dan disisi lain juga telah dikuatirkan bahwa akan menjadi titik lemah pada sebuah sekuriti di perimeter atau perbatasan network [10].

2.4 IPSec (Internal Protocol Security)

IPSec adalah kumpulan protokol untuk mengamankan jaringan melalui proses otentikasi dan enkripsi paket IP. Dengan IPSec , sebuah sistem bisa memilih protokol keamanan [8].

2.5 Penelitian Terdahulu

Adapun penelitian sebelumnya juga telah dilakukan oleh (Hidayat S : 2022) yaitu mengoptimalkan RouterOS yang dimiliki perusahaan agar dapat menjadi jaringan Tunnel yang dapat menjembatani komunikasi data antara jaringan publik (internet) dengan jaringan LAN kantor, sehingga karyawan dapat mengakses *resource* kantor tanpa batasan ruang dan waktu akibat regulasi pemerintah dan kebijakan perusahaan [4] . Penelitian lain juga dilakukan oleh

(M Novriansyah : 2021) juga menerapkan VPN Tunnel untuk mencegah *Packet Sniffing* dengan metode LP2TP/IPSec. Untuk mengamankan paket data yang dikirim digunakan IPSec, sedangkan dengan IPSec VPN proses pengiriman data akan lebih aman tanpa adanya gangguan karena data yang telah dikirim telah dienkripsi dengan baik [6].

3. Metodologi Penelitian

3.1 Metode Penelitian

Metode *Action research* pada hakikatnya merupakan rangkaian yang dilakukan secara sistematik, dalam rangka memecahkan masalah, sampai masalah itu terpecahkan (Tenggono *et al*. 2018). Prasetyo, Hasanah, *and* Wijaya 2022 Membagi *Action Research* dalam 5 langkah yaitu:

1) Melakukan Diagnose (*Diagnosing)*

Pada tahapan ini peneliti akan melakukan identifikasi masalah-masalah yaitu diagnosa sistem keamanan dengan cara melakukan studi literatur , penentuan ruang lingkup serta pengumpulan data dari observasi dan dokumentasi.

2) Membuat Rencana Tindakan (*Action Planing)*

Tahapan ini peneliti melakukan pemahaman pokok masalah yang ada dan menyusun rencana tindakan yang tepat untuk menyelesaikan masalah yang ada.

3) Melakukan Tindakan (*Action Taking)*

Mengimplementasikan rencana tindakan yang telah disusun.

4) Melakukan Evaluasi (*Evaluating)*

Melakukan evaluasi pada hasil dari implementasi sebelumnya dan mulai menyimpulkan hasil dari langkah sebelumnya.

5) Pembelajaran (*Learning)*

Tahap akhir dari penelitian yaitu melakukan review terhadap hasil dari tahapan-tahapan yang telah dilalui.

3.2 Metode Pengumpulan Data

Metode pengumpulan data yang digunakan yaitu terdiri dari beberapa teknik pengumpulan data seperti berikut ini :

1) Metode Pengamatan (Observasition)

Pada tahap ini penulis mencari permasalahan mengenai data, yang ingin penulis amati pada perusahaan tersebut.

2) Diskusi dan Wawancara

Penulis melakukan diskusi langsung kepada pegawai IT, mengenai hal-hal yang berhubungan dengan objek dan penelitian yang ingin di tinjau.

3) Metode Studi Pustaka

Data tersebut penulis dapatkan dan pahami dari teori-teori yang relevan dengan topik yang akan penulis bahas dalam penelitian Karya Akhir. Teori-teori tersebut penulis dapat dari kuliah, buku, jurnal, artikel internet, dan sumber lainnya.

P-ISSN 2654-5438
E-ISSN 2828-4917

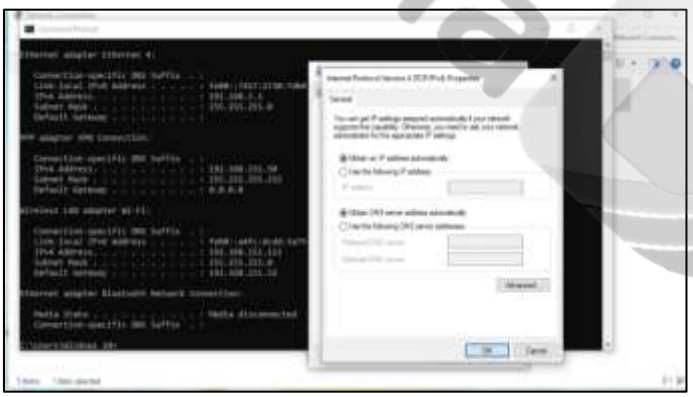
4. Hasil dan Pembahasan

4.1 Hasil Pengujian Firewall

Setelah dilakukannya konfigurasi terhadap *Router* Mikrotik dengan Metode yang digunakan yaitu VPN L2TP/IPSec, kemudian selanjutnya dilakukan pengujian keamanan *firewall* pada jaringan computer dengan hasil sebagai berikut :

Gambar 1. Network Connection configured VPN L2TP/ IPSec

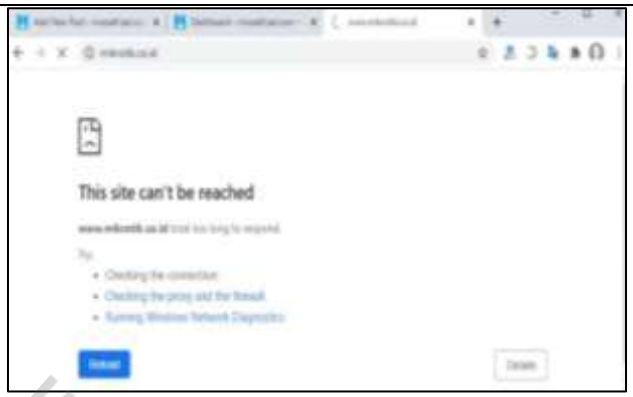
Pada Gambar 1. Merupakan *user* sedang dalam pengaktifan Vpn, dan Vpn telah tersambung. Selanjutnya pada pengujian DHCP *Server computer client* akan diberikan IP *Address* secara otomatis.



Gambar 2. Pengujian DHCP Server

Pada Gambar 2. Merupakan pengujian pada keamanan *firewall filtering* yang akan menolak akses kepada *website-website* yang tidak diinginkan atau tidak diizinkan untuk diakses oleh *user*.

P-ISSN 2654-5438
E-ISSN 2828-4917

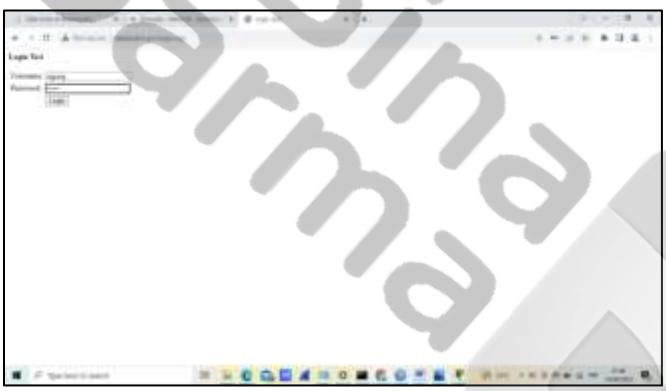


Gambar 3. Firewall Filtering

Pada Gambar 3. Merupakan situs www.mikrotik.co.id telah berhasil diblokir dan tidak dapat diakses dengan memasukkan *domain name server* situs tersebut pada *web browser*.

4.2 Uji Coba Simulasi Tools Wireshark Pada Serangan Packet Sniffing

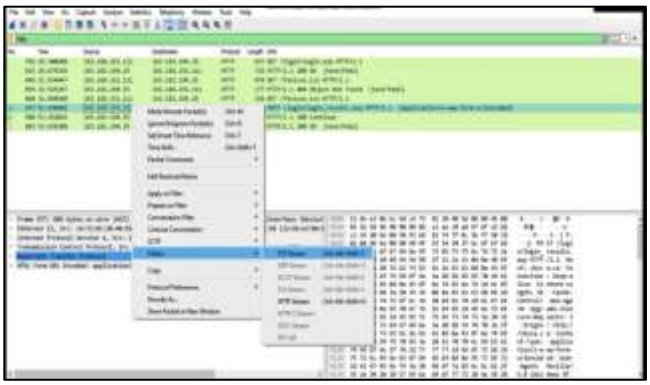
1. Langkah pertama masuk ke aplikasi Wireshark. Selanjutnya masuk ke web *logintest.*



Gambar 4. Ketik Username dan Password

Pada Gambar 3.24 merupakan pemberian identitas dengan memasukkan *name* (Agung) dan *password* (12345).

2. Cari IP internet yang dipakai lalu klik kanan > Follow > TCP *Stream.*



Gambar 5. Pencarian IP Internet

Pada Gambar 5. Merupakan langkah awal masuk ke *Wireshark* menggunakan koneksi yang digunakan lalu cari IP nya , kemudian klik kanan > Follow > TCP *Stream*.

3. Tampilan Penyerangan Packet Sniffing.

P-ISSN 2654-5438
E-ISSN 2828-4917

Gambar 6. Username dan Password Diketahui

Pada Gambar 6. Merupakan tampilan hasil penyerangan *Packet Sniffing*, dimana *username* dan *password* yang telah dimasukkan pada *website* sebelumnya telah diketahui.

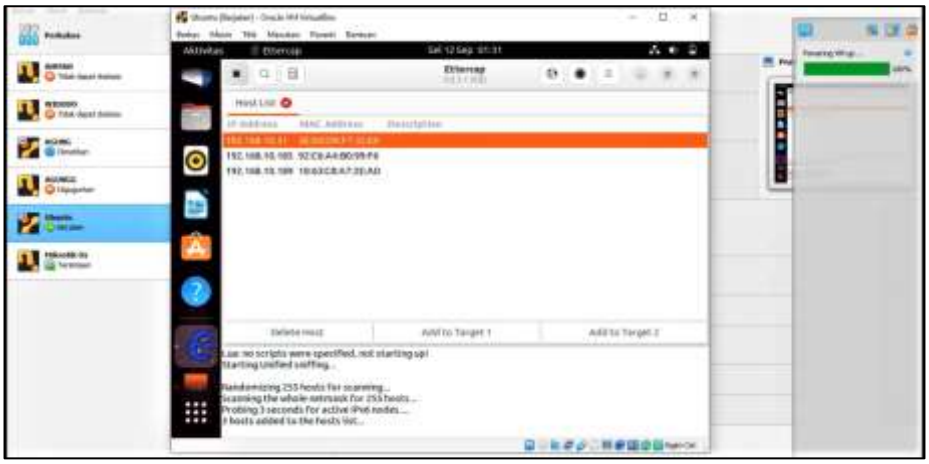
4.3 Uji Coba Simulasi Tools Ettercap Pada Serangan Packet Sniffing

1. Langkah pertama masuk ke aplikasi Virtualbox Ubuntu.

Gambar 7. Tampilan Awal Ubuntu

Pada Gambar 7. Merupakan tampilan awal Ubuntu, kemudian masuk ke Tools Ettercap.

2. Tampilan alamat IP Addres.



Gambar 8. Pemunculan Daftar IP Address

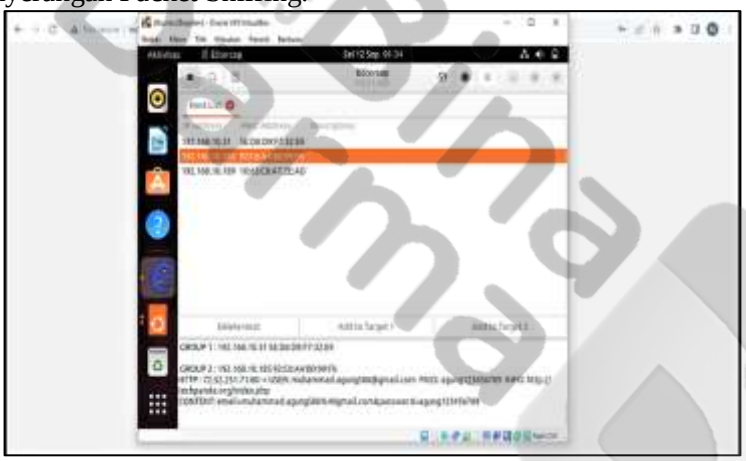
Pada Gambar 8. Merupakan Pemilihan IP Address yang ingin di *sniffing* kemudian add to target.

3. Masuk ke Website Techpanda.

Gambar 9. Pemberian Email dan Password

Pada Gambar 9. Merupakan pemberian identitas dengan memasukkan *email* (muhammad.agung586@gmail.com) dan *password* (agung123456789).

4. Tampilan penyerangan Packet Sniffing.



Gambar 10. Email dan Password Diketahui

Pada Gambar 10. Merupakan tampilan hasil penyerangan *Packet Sniffing*, dimana *email* dan *password* yang telah dimasukkan pada *website* sebelumnya telah diketahui.

5. Kesimpulan

Berdasarkan hasil pembahasan terhadap Implementasi Keamanan Database Terhadap Serangan *Packet Sniffing* Pada Departemen TI PT Pupuk Sriwidjaja Palembang maka hasil penelitian ini dapat disimpulkan sebagai berikut :

1. Dengan diterapkannya jaringan *Virtual Private Network* (VPN) L2TP/IPSec pada Departemen TI PT Pupuk Sriwidjaja Palembang, maka keamanan jaringan akan menjadi lebih aman dan lancar.
2. Pada penerapan DHCP *Server* penugasan alamat IP bekerja secara otomatis kepada perangkat yang terhubung ke jaringan, serta dapat mengurasu resiko IP *Address Conflict.*
3. Untuk mengarahkan ke salah satu situs *website* yang akan diblokir maka perlu mengisi "*Regexp" (Regular Expresion)* pada menu *Layer 7 Protocols.* Dengan diberlakukan pemblokiran situs web (*Layer 7 Protocol*s), *user* tidak bisa lagi mengakses situs yang tidak diizinkan.

Referensi

[1] A. Mikola and A. C. Nurcahyo, "Analisis Load Balancing Berbasis Mikrotik Dalam Meningkatkan Kemampuan Server di Institut Shanti Bhuana," *J. Inf. Technol.*, vol. 2, no. 2, pp. 17–20, 2022, doi: 10.46229/jifotech.v2i2.481.

[2] Ariyadi, T., & Maulana, A. T. (2021). Penerapan Web Proxy Dan Management Bandwidth Menggunakan Mikrotik Routerboard Pada Kantor Pos Palembang 30000. *Jurnal Ilmiah Informatika*, *9*(02), 116–122. https://doi.org/10.33884/jif.v9i02.4444

[3] Ariyadi, T., & Prabowo, M. A. (2021). Perbandingan Kinerja Virtual Private Network Antara Vpn Tunnel Dan Internet Protocols Security. *INOVTEK Polbeng - Seri Informatika*, *6*(1), 80. https://doi.org/10.35314/isi.v6i1.1698

[4] Hidayat, S., Budiman, T., & Rini, A. S. (2022). Optimalisasi jaringan tunnel menggunakan routeros untuk mendukung kelangsungan operasional PT. KLK Agriservindo di masa pandemik Covid-19. Jurnal Sains dan Teknologi Widyaloka, 1(1), 1-14. https://doi.org/10.54593/jstekwid.v1i1.44

[5] Normah, Bakhtiar Rifai, Satrio Vambudi, And Rifki Maulana. 2022. "Analisa Sentimen Perkembangan Vtuber Dengan Metode Support Vector Machine Berbasis Smote." Jurnal TeknikKomputerAmikBsi8(2):174–80.

[6] Noviansyah, M., & Saiyar, H. (2021). Pencegahan Packet Sniffing Menggunakan Metode VPN Tunnel Untuk Keamanan Jaringan Komputer Berbasis Mikrotik. Jurnal Akrab Juara, 6(4), 36-46.

[7] Nur Riyansyah, Ariyadi, T., A., Agung, M., & Ikrar, M. A. (2023). Analisis Serangan Dhcp Starvation Attack Pada Router Os Mikrotik. *Jurnal Ilmiah Informatika*, *11*(01), 85–93. https://doi.org/10.33884/jif.v11i01.7162

[8] Prayogi Wicaksana, Hadi, F., & Aulia Fitrul Hadi. (2021). Perancangan Implementasi VPN Server Menggunakan Protokol L2TP dan IPSec Sebagai Keamanan Jaringan. *Jurnal KomtekInfo*, *8*(3), 169–175. https://doi.org/10.35134/komtekinfo.v8i3.128

[9] Syahputra, Hadi, And Romi Wijaya. 2022. "Pembangunan Jaringan Hotspot Berbasis Mikrotik Pada Kampung Tematik Di Kecamatan Padang Utara." 29(1).

[10] Umaroh, Lia, And Machsun Rifauddin. 2020. "Implementasi Virtual Private Network (Vpn) Di Perpustakaan Universitas Islam Malang." 9008(21): 193–201.