SIMULASI KEAMANAN SERVER MENGGUNAKAN OPENVPN

Sandre Handoyo[1], Mochammad Fahru Rizal[2], Setia Juli Irzal Ismail[3]

[1,2,3] Fakultas Ilmu Terapan - Telkom University
sandre.nobunaga@gmail.com[1], mfrizal@tass.telkomuniversity.ac.id[2], jul@tass.telkomuniversity.ac.id [3]

Abstrak

Seiring perkembangan yang cepat pada bidang teknologi terutama pada sektor jaringan, telah memungkinkan terjadinya sebuah transaksi data dari dua tempat yang berjauhan. Transaksi data yang terjadi tersebut melewati jaringan publik yang merupakan jaringan yang dipakai oleh semua orang. Data yang melewati jaringan publik secara otomatis data tersebut dapat disadap oleh pihak yang tidak berwenang atau sering disebut sniffing, maka diperlukan sebuah sistem keamanan untuk mencegah hal tersebut. Pada proyek akhir ini disimulasikan sebuah sistem keamanan yang mencegah tindakan sniffing dengan menggunakan Virtual Private Network (VPN). Dengan menggunakan VPN seluruh paket data yang terkirim dienkripsi sebelum dikirimkan agar isi data tersebut tidak dapat langsung dibaca oleh orang lain yang tidak memiliki wewenang. OpenVPN merupakan VPN yang disimulasikan dalam proyek akhir ini.

Kata kunci: *sniffing*, VPN, OpenVPN

Abstract

With the rapidly development of technology esespecially on network technology, it is possible to do a transaction data to or from far away server. As a data that cross over network that used by everyone its mean there are possiblity the data can be stealed by the others or usually called sniffing, because of that the server indeed need a security system to avoid this happen. This final proyek focused on simulation a security system to avoid sniffing using a virtual private network (VPN). With VPN all packet data will be encrypted before it transmitted, so it can't be read easily. OpenVPN will be the VPN that used in this final project.

Keywords: *sniffing*, VPN, OpenVPN

1. Latar Belakang

Server dalam sebuah jaringan komputer merupakan bagian yang sangat penting karena menyimpan dan melakukan transaksi data yang penting. Dengan adanya data penting maka rawan terjadinya pencurian data pada server yang sering disebut sebagai *sniffing*.

Maka dari itu diperlukan sebuah sistem keamanan yang dapat mengurangi pencurian data tersebut. Banyak cara yang dapat dilakukan untuk mencegah dan mengurangi pencurian data, dalam simulasi proyek akhir ini digunakan Virtual Private Network (VPN) dengan menggunakan tools berupa OpenVPN.

2. Dasar Teori

a. Server

"Serve" yang berarti melayani merupakan kata asal dari server, adalah sebuah sistem atau perangkat yang mempunyai fungsi khusus dalam suatu jaringan sebagai penyedia layanan kepada klien. Setiap server secara khusus memungkinkan memiliki fungsi yang berbeda antara satu dengan yang lainnya, serta tidak menutup kemungkinan satu komputer dapat berfungsi sebagai beberapa server sekaligus [6].

b. sniffing

sniffing atau *packet sniffing* merupakan sebuah teknik monitoring setiap paket yang terjadi dalam sebuah jaringan. *packet sniffer* adalah sebuah *software* atau *hardware* untuk memonitoring seluruh trafik dalam jaringan. *Sniffer* atau pihak yang melakukan sniffing merupakan ancaman dalam keamanan dalam keahlian mereka dalam menangkap dan membaca trafik masuk maupun keluar [5].

c. VPN

Virtual Private Network (VPN) merupakan sebuah ekstensi dari intranet privat yang melewati jaringan public seperti internet, untuk membuat sebuah koneksi jaringan privat baru yang aman melalui sebuah lorong [1].

walaupun tidak memiliki fisik, sebuah VPN harus diperlakukan sebagai sebuah ekstensi dari suatu infrastruktur jaringan, yang berarti harus tersedia layanannya ke seluruh klien dan aplikasi yang terdapat pada topologi utama jaringan tersebut [3].

d. OpenVPN

OpenVPN merupakan sebuah alat yang digunakan untuk membuat layanan VPN yang mendukung keamanan SSL/TLS, Ethernet bridging, TCP atau UDP tunneling melalui proxy atau NAT, mendukung DHCP hingga ribuan klien dan dapat dijalankan hamper di setiap sistem operasi [2].

OpenVPN mendukung enkripsi konvensional yang menggunakan *pre-shared secret key* (Static Key Mode) atau *public key security* (SSL/TLS mode) menggunakan sertifikasi klien dan server. OpenVPN juga mendukung non-enkripsi TCP/UDP tunneling. OpenVPN bekerja dengan menggunakan antarmuka virtual TUN/TAP [4].

3. Analisis dan Perancangan

Dalam proyek akhir ini dibutuhkan beberapa perangkat lunak dan perngakt keras. Tabel 1 berikut menjelaskan kebutuhan perangkat keras.

Tabel 1 Kebutuhan perangkat keras

Jenis	Jumlah	Keterangan
Laptop	1	HDD 500GB, RAM 4GB, Processor core i3

dan Tabel 2 menjelaskan kebutuhan perangkat lunak yang digunakan.

Tabel 2 Kebutuhan perangkat lunak

Nama Perangkat lunak	Versi	Pengembang
OpenVPN	2.3.6	OpenVPN Technologies, Inc
Webmin	1.750	webmin
OpenVPN GUI	2.3.8	OpenVPN Technologies, Inc
Oracle VM VirtualBox	4.3	Oracle corp.

3.1 Langkah Pengerjaan

Berikut merupakan langkah pengerjaan proyek akhir :

a. Implementasi Webmin pada server
b. Instalasi OpenVPN pada server
c. Instalasi modul OpenVPN pada Webmin
d. Konfigurasi OpenVPN
e. Distribusi *keys* untuk klien OpenVPN
f. Melakukan pengujian terhadap data yang terjadi antara server dengan klien.

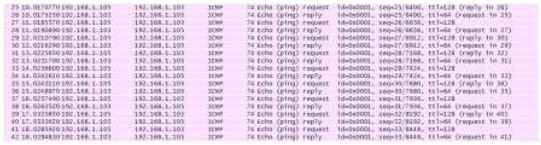
Pada gambar 1 merupakan topologi dari simulasi proyek akhir ini

Gambar 1 Topologi Simulasi

4. Pengujian

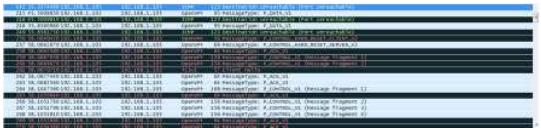
Skenario Pengujian untuk simulasi ini adalah sebagai berikut :

a. Klien terhubung dengan server tanpa menggunakanOpenVPN.
b. Dengan menggunakan aplikasi wireshark, dapat dilihat paket data yang terjadi pada jaringan tersebut.



Gambar 2 hasil rekaman paket data yang terjadi sebelum menggunakan OpenVPN

c. Klien mencoba terhubung dengan server menggunakan OpenVPN.
d. Dengan menggunakan aplikasi wireshark, dapat dilihat paket data yang terjadi pada jaringan tersebut.



Gambar 3 hasil rekaman paket data yang terjadi sebelum menggunakan OpenVPN

e. Melihat catatan l*ogs* pada OpenVPN server dan *logs* pada klien.

5. Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan hasil pengujian dan implementasi Proyek akhir ini, dapat diambil kesimpulan bahwa :

a. Terjadi konektifitas antara klien dan server dengan menggunakan OpenVPN.
b. Berdasarkan hasil pengujian yang dilakukan keamanan akses baik dari maupun ke server terenkripsi paket datanya sehingga mencegah terjadinya *sniffing*.

5.2 Saran

Berdasarkan hasil pengerjaan proyek akhir, dapat diambil saran bahwa OpenVPN yang merupakan aplikasi berbasis open-source sehingga dapat dikombinasikan dengan berbagai alat keamanan lain, seperti firewall. Sehingga dapat menambahkan fungsi yang lebih baik.

Daftar Pustaka

[1] F. Markus, OpenVPN Building and Integrating Virtual Private Networks, Brimingham: Packt Publishing Ltd,2006.
[2] OpenVPN23ManPage - OpenVPN Community. Februari 08, 2015. Diakses Maret 05, 2015 dari Web site : https://community.OpenVPN.net/OpenVPN/wiki/OpenVPN23ManPage
[3] R. Venkateswaran, Virtual Private Networks, IEEE Potentials, Vol: 20, 2001
[4] OpenVPN. OpenVPN Technologies inc. Diakses Maret 03, 2015 dari OpenVPN Web site : https://OpenVPN.net/index.php/open-source/333-what-is-OpenVPN.html
[5] Asrodia Pallavi & Patel Helata, "Analysis of various packet sniffing tools for network monitoring and analysis". International journal of electrical, electronic and computer engineering, Khargome, India, 05 May 2012.
[6] Yadav, S. C, & Singh, S. K. (2009). An Indrodution to CLIENT/SERVER COMPUTING. New Delhi: New Age Internation.