IMPLEMENTASI KEAMANAN JARINGAN DENGAN METODE WHITELIST PADA SERVER JURUSAN ELEKTRO DI POLITEKNIK NEGERI MALANG

Januar Ariq Pratama[1)], Yoyok Heru[2)], Mochammad Junus[3)]
[1,2,3)] Program Studi Jaringan Telekomunikasi Digital, Teknik Elektro, Politeknik Negeri Malang
Email: januar.ariq@gmail.com

Abstract

Politeknik Negeri Malang adalah seuatu lembaga pendidikan yan berbasis Teknik dimana database sangat diperlukan disini, database itu sendiri adalah sebuah data-data penting yang harus di simpan dan tidak boleh dilihat oleh orang lain. Keamanan database lah harus dikembangkan dan diutamakan agar tidak ada yang membobol sebuah data penting yang ada di dalam server.

Metode whitelist ini memanfaatkan sebuah port yang bisa memblok akses port kepada jaringan luar yang rentan terhadap tindakan kejahatan, metode ini menggunakan ssh sebagai media untuk mengatur pengontrolan dari sebuah alamat ip. Alamat ip akan ditambahkan sebuah port dibelakangnya. Penggunaan block ip dengan os linux dan diuji melalui web dan laptop menggunakan akses point local.

Hasil pengujian menunjukan bahwa kualitas yang digunakan untuk keamanan yaitu whitelist, diaman metode ini digunakan untuk keamanan ip yang digunakan. Proses block dan unblock IP dapat dilakukan dengan baik. Proses penambahan dan penghapusan port dapat dilakukan dengan baik. Sehingga secara umum, keseluruhan sistem berjalan dengan baik dan akses yang mudah.

Keywords: *whitelist,* SSH*,* Port*,* IP*,*Linux*,*

I. PENDAHULUAN

Keperluan keamanan database timbul dari kebutuhan untuk melindungi data. Pertama, dari kehilangan dan kerusakan data. Kedua, adanya pihak yang tidak diijinkan hendak mengakses atau mengubah data. Permasalahan lainnya mencakup perlindungan data dari delay yang berlebihan dalam mengakses atau menggunakan data, atau mengatasi gangguan denial of service.

Kontrol akses terhadap terhadap informasi yang sensitif merupakan perhatian terutama oleh manajer, pekerja di bidang informasi, application developer, dan DBA. Kontrol akses selektif berdasarkan authorisasi keamanan dari level user dapat menjamin kerahasiaan tanpa batasan yang terlalu luas. Level dari kontrol akses ini menjamin rahasia informasi sensitif yang tidak akan tersedia untuk orang yang tidak diberi ijin (authorisasi) bahkan terhadap user umum yang memiliki akses terhadap informasi yang dibutuhkan, kadang-kadang pada tabel yang sama.

Mengijinkan informasi dapat dilihat atau digunakan oleh orang yang tidak tepat dapat menyulitkan, merusak, atau membahayakan individu, karir, organisasi, agensi, pemerintah, atau negara. Namun untuk data tertentu seringkali bercampur dengan data lainnya, informasi yang kurang sensitif yang secara legal dibutuhkan oleh berbagai user. Membatasi akses terhadap semua table atau memisahkan data sensitive ke database terpisah dapat menciptakan lingkungan kerja yang tidak nyaman yang membutuhkan biaya besar pada hardware, software, waktu user, dan administrasi.

Ketersediaan informasi terus mengalami peningkatan pesat, metoda untuk penyandian dan penyimpanan informasi juga mengalami peningkatan. Perkembangan jumlah sumber informasi ini membawa beberapa permasalahan, diantaranya tentang bagaimana mengkombinasikan tempat penyimpanan data yang terdistribusi dan berbeda. Informasi pada suatu organisasi atau perusahaan biasanya disimpan di lokasi yang terpisah dan berbedabeda format. Ketika terjadi peningkatan kapasitas tempat penyimpanan dan besarnya biaya pencarian informasi perusahaan dihadapkan pada masalah melimpahnya jumlah data.

Basis data terdistribusi adalah basis data dimana data ditempatkan di beberapa lokasi, tetapi menerapkan suatu mekanisme tertentu untuk membuatnya menjadi satu kesatuan basis data (Fathansyah, 2004). Sebuah system

basis data terdistribusi hanya mungkin dibangun dalam sebuah sistem jaringan komputer. Berbeda dengan basis data terpusat yang datanya ditempatkan di beberapa lokasi tetapi tidak saling berhubungan.

Akses basis data terdistribusi merupakan proses untuk mencampur dan mencocokkan, query, memanipulasi, dan menggabungkan data dalam suatu basis data terdistribusi. Akses basis data akan menampilkan hasil query yang diinginkan pemakai. Akses basis data tidak melakukan pelacakan terjadinya perubahan pada basis data pada tiap-tiap host.

II. TINJAUAN PUSTAKA

A. Web Server

Sebuah software yang memberikan layanan berbasis data dan berfungsi menerima permintaan dari HTTP atau HTTPS pada klien yang dikenal dan biasanya kita kenal dengan nama web browser dan untuk mengirimkan kembali yang hasilnya dalam bentuk beberapa halaman web dan pada umumnya akan berbentuk dokumen HTML. itulah pengertian web server sebenarnya. dalam bentuk sederhana web server akan mengirim data HTML kepada permintaan web Browser sehingga akan terlihat seperti pada umumnya yaitu sebuah tampilan website.

B. Linux

Software sistem operasi open source yang gratis untuk disebarluaskan di bawah lisensi GNU. Linux merupakan turunan dari unix dan dapat bekerja pada berbagai macam perangkat keras koputer mulai dari inter x86 sampai dengan RISC. Dengan lisensi GNU (Gnu Not Unix) Anda dapat memperoleh program, lengkap dengan kode sumbernya (source code). Tidak hanya itu, Anda diberikan hak untuk mengkopi sebanyak Anda mau, atau bahkan mengubah kode sumbernya.Dan itu semua legal dibawah lisensi. Meskipun gratis, lisensi GNU memperbolehkan pihak yang ingin menarik biaya untuk penggandaan maupun pengiriman program.

C. Whitelist_from

Begitu juga sebaliknya, sebuah fitur yang disediakan oleh SpamAssassin untuk memperbolehkan alamat email tertentu untuk masuk ke dalam kotak email anda / inbox anda walaupun email tersebut di kategorikan SPAM oleh SpamAssassin anda.

F. Database

Penggunaan teknologi dalam sebuah perusahaan, institusi ataupun organisasi mempunyai peranan penting guna mencapai tujuan. Suatu perusahaan dituntut untuk bekerja se-efisien mungkin supaya bisa bertahan di atas kerasnya persaingan. Salah satu teknologi yang harus dimiliki oleh sebuah perusahaan, institusi maupun organisasi adalah teknologi dalam memproses data sehingga menjadi informasi yang beguna, teknologi yang dimaksud adalah sistem pengolahan basis data atau database. Penggunaan database yang baik pada perusahaan retail misalnya, mampu membantu seorang kasir bekerja lebih cepat ketika mencari jumlah barang atau harga barang yang akan dijual. Begitupun dengan admin, database mempermudah ketika pencarian stok persediaan, barang paling laku dan banyak lagi yang lainnya.sekumpulan data yang sudah disusun sedemikan rupa dengan ketentuan atau aturan tertentu yang saling berelasi sehingga memudahkan pengguna dalam mengelolanya juga memudahkan memperoleh informasi. Selain itu adapula yang mendefinisikan database sebagai kumpulan file, tabel, atau arsip yang saling terhubung yang disimpan dalam media elektronik.

III. METODE PENELITIAN

A. Perencanaan System

Berikut adalah keterangan blok diagram perencanaan sistem yang ditampilkan:

1. Install linux sebagai os yang akan digunakan, linux ini hanya untuk jembatan yang akan dilakukan untuk mengakses sebuah server.
2. Setelah linux sudah terinstall maka langkah selanjutnya yaitu meinstall apa saja yang diperlukan dalam keamaan server dalam linux tersebut.
3. Pada bagian keamanan port whitelist yaitu dimana memperbolehkan port yang hanya dipakai saja sementara yang lain diblock.
4. Database yang sudah tersedia akan dibuatkan port sendiri dimana port tersebut sudah terdaftar pada white list dan dapat diakses dengan aman.

5. Command yang dilakukan hanya menggunakan Terminal linux saja.

B. Variabel Penelitian Definisi Operasional

Didalam penelitian ini diperoleh bahwa laptop lain tidak bisa atau tidak dapat mengakses ip dimana port yang sudah ada pada white list tersebut jadi keamanan akan terjaga pada database yang sudah di list.

C. Teknik Pengumpulan Data

Pada teknik pengumpulan data dilakukan mencoba dengan ping ip pada server dan pada port yang sudah disediakan sebelumnya untuk mengakses melalui browser, jika ip sudah di block maka tidak dapat diakses.

D. Teknik Analisis Data

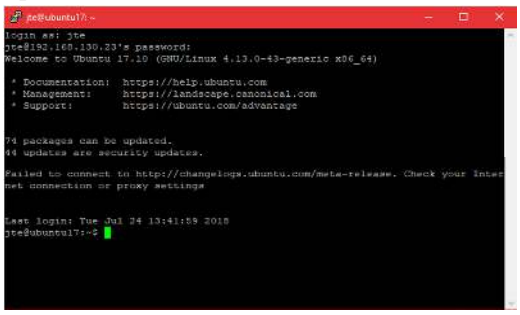
Dari proses pengumpulan data maka dapat dilakukan analisa tingkat keamanan database pada saat mengakses bagaimana ip pada browser.

IV. HASIL DAN PEMBAHASAN

4.1 Hasil Keamanan Server

1. Ubuntu Server

Pada gambar yang akan di tampilkan yaitu ubuntu server yang sudah di remote menggunakan putty, lalu masukkan username dan password terlebih dahulu agar server bisa di setting. Pengaturan ini dilakukan dengan memasukkan script ubuntu *Open SSH* dan apache2.



Gambar 4.1 *Server* login berhasil
Sumber : Hasil Pengujian

2. Setting Open SSH

Ketikan script untuk membuka open ssh. Setelah masuk pada menu tersebut lalu ketik port yang di tentukan dimana port, jika port sudah di tentukan makan akses untuk pengremote an tidak bisa di gunakan dengan bebas hanya super user saja yang tau port tersebut.

3. Setting apache2

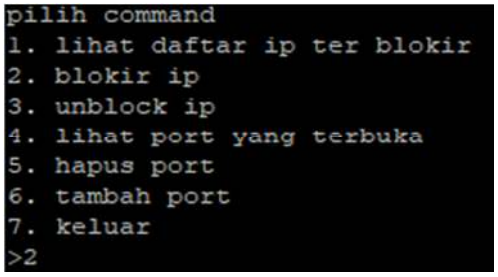
Script apache2 Script ini di perlukan untuk mengakses Listen port dimana bagian ini akan di akses oleh web untuk penempatan database yang sudah tersedian di port ini, maka di apache2 kita dapat menulisa listen apa saja yang dapat dimasukkan dan dapat menghapus untuk keamanan didalamnya.

4. Iptables

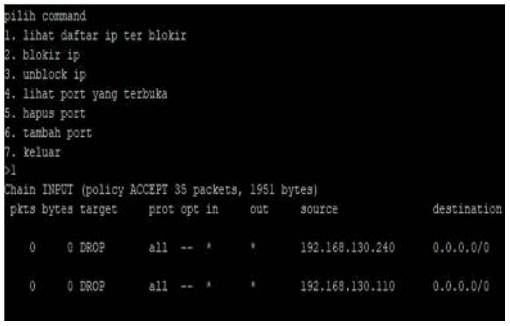
Pemasangan perintah iptables yaitu untuk pemblock atau unblock ip. Script ini digunakan agar ip lain tidak bisa mengakses server dan tidak dapat mengeping.

5. Commanad Prompt Admin

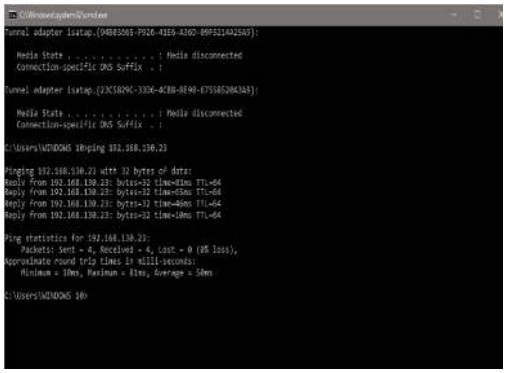
a. Block IP pada pilihan nomor 2, dan Unblock IP pada pilihan nomor 3



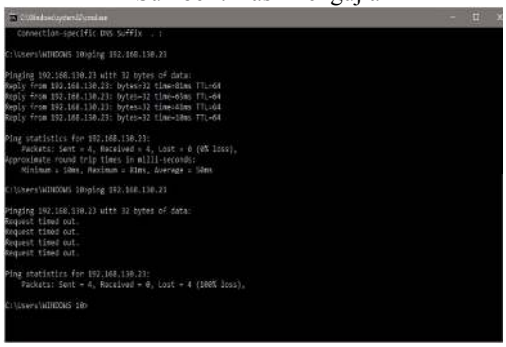
Lalu setelah memasukkan ip yang akan di block. Pilih no 1 untuk melihat daftar ip yang terblock



Gambar 4.9 Daftar IP Terblock
Sumber : Hasil Pengujian

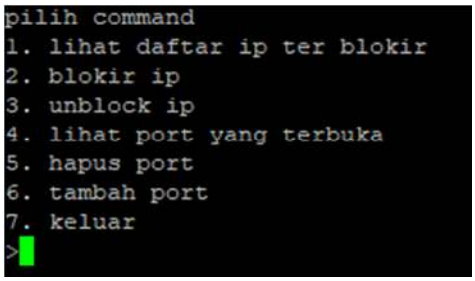


Gambar 4.10 Ping ke Server Sebelum Blocking
Sumber : Hasil Pengujian



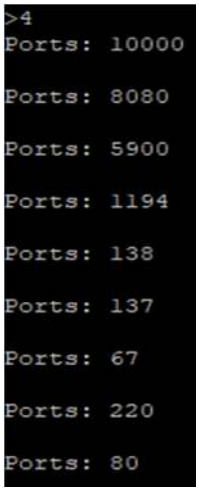
Gambar 4.11 Ping ke server Setelah blocking
Sumber : Hasil Pengujian

Berisi pilihan-pilihan tindakan yang dapat diakses oleh admin dengan cara memasukan kode angka sesuai urutan pada menu.



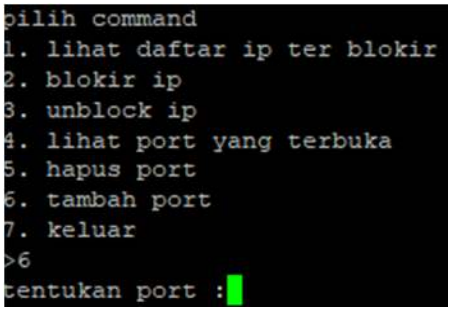
Gambar 4.2 Tampilan Command Prompt Admin
Sumber : Hasil Pengujian

b. Lihat pilhan 4 untuk melihat port yang sudah terdaftar



Gambar 4.3 Daftar Port yang Sudah Terdaftar
Sumber : Hasil Pengujian

c. Penambahan port pada pilihan nomor 6.

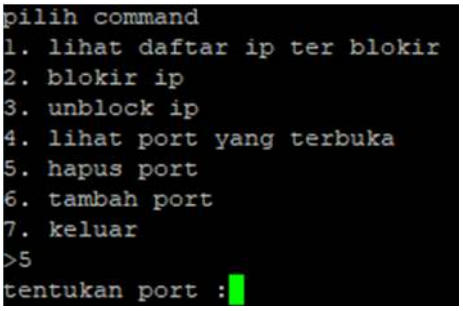


Gambar 4.4 Tampilan Command Prompt
Sumber : Hasil Pengujian

Hasil ketika port yang sudah di masukkan

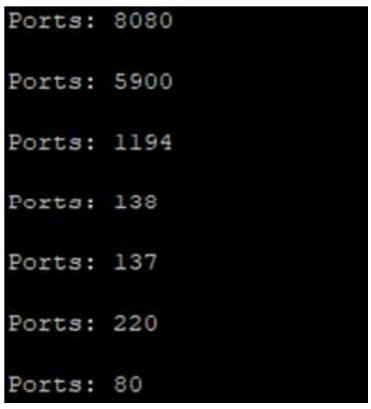
Gambar 4.5 Tampilan Browser untuk akses Port
Sumber : Hasil Pengujian

d. Hapus port pada pilihan pilih nomor 5.



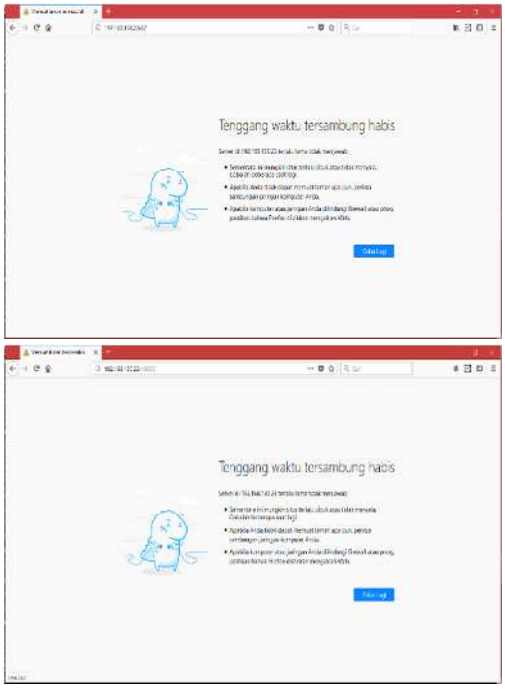
Gambar 4.6 Tampilan Command Prompt
Sumber : Hasil Pengujian

Daftar port setelah penghapusan port 67 dan 10000



Gambar 4.7 Daftar Port Setelah Dilakukan Penghapusan
Sumber : Hasil Pengujian

Hasil ketika port terhapus



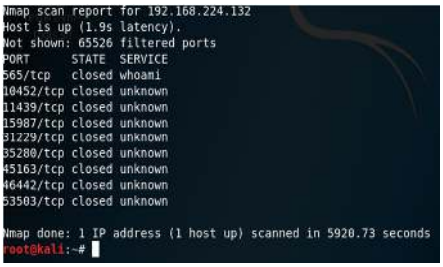
Gambar 4.8 Port 67 dan 10000 Setelah Dilakukan Penghapusan
Sumber : Hasil Pengujian

4.1 Metode Penetrasi Kali linux

Penggunakan kali linux dengan melakukan port scanning terlebih dahulu, kali linux menyediakan scan port dengan menggunakan aplikasi nmap yang ada pada server dengan menggunakan ip palsu lalu masukkan kali linux yng sudah terkoneksi access point. Port akan terscanning secara otomatis dan akan menampilkan port secara acak setelah port yang terbuka akan dilakukan pengaksesan melalui web dengan memassukan ip palsu beserta port yang sudah tersedia.

4.2 Hasil Scanning Port

Cara Scanning port pada gambar 4.4 ini menggunakan os Kali Linux yang otomatis menyediakan nmap untuk melakukan scan secara acak dan hanya mengambil port terbuka saja, port selain pada gambar sudah ada penggunaan pada status service.



Gambar 4.4 Kali Linux scanning port dengan nmap

V. KESIMPULAN & SARAN

Kesimpulan

Dari hasil pengujian dan pembahasan dapat diperoleh simpulan sebagai berikut:

1. Proses pembuatan keamanan ip diawali dengan studi pustaka mengenai perintah linux , open ssh server dan Lamp. Proses selanjutnya yaitu instal yang diperlukan di dalam linux dengan menggunakan cmd terminal linux, jika sudah semua maka percobaan dengan menggunakan alamat ip dan port untuk mencoba apakah perintah pada terminal bisa digunakan dengan baik atau tidak.
2. Pada sisi server, terdapat tujuh menu yang dapat diakses oleh admin, yaitu lihat daftar ip terblokir, Blok IP, Unblock IP, Lihat port yang terbuka, Tambah Port, Hapus port, dan Keluar.
3. Pada percobaan penambahan port, penambahan port dapat dilakukan dengan baik.
4. Pada percobaan penghapusan port, port yang telah dihapus tidak dapat diakses oleh server, yang menandakan sistem dapat berjalan dengan baik
5. Pada percobaan block IP, setelah dilakukan blocking, perangkat dengan IP terblock tidak dapat melakukan akses ke server. Setelah dilakukan unblocking, perangkat dengan IP yang terblock dapat melakukan akses kembali dengan server.
6. Secara keseluruhan, pada sisi server tidak ditemukan kendala teknis karena semua sistem dapat berjalan dengan baik.

SARAN

1. Penginstalan linux pada vmware harus benar, perhatikan spec os linux terlebih dahulu
2. Instal semua keperluan pada linux untuk dapat konfigurasi
3. Atur penyediaan port dan ip untuk mendapatkan hak akses

VI. REFERENSI

Sugiantoro, B., & Istiyanto, J. E. (2015, July). Analisa Keamanan database Server Menggunakan Teknologi Virtual Private Database dan Notifikasi Database Server Menggunakan Agent Bergerak. In *Seminar Nasional Informatika (SEMNASIF)* (Vol. 1, No. 3).

Sirait, E. R. E. (2016). RESPON MASYARAKAT TERHADAP SISTEM WHITELIST: ALTERNATIF UNTUK AKSES INTERNET YANG LEBIH AMAN PUBLIC RESPOND TO WHITELISTING: ALTERNATIVE FOR MORE SECURE INTERNET ACCESS. *Jurnal Penelitian Komunikasi dan Pembangunan*, *17*(2).

Riyanto, K. N. P. (2013). R.,"Membangun Webserver Intranet Dengan Linux,". *Jurnal Media Informatika*,vol. *9*, no 3-5.

Herdiana, Y. (2014). KEAMANAN PADA JARINGAN WIRELESS. *Jurnal Online Sekolah Tinggi Teknologi Mandala*, vol. *7*(1), no 26-37.

Sholeh, M. (2009). Analisis Pencegahan Akses Website Kategori Dilarang. *Jurnal Teknologi IST AKPRIND*, vol. *2*.