BAB I

PENDAHULUAN

1.1 Latar Belakang

Dengan majunya teknologi informasi sekarang ini, *internet* merupakan sarana komunikasi dan informasi yang sangat dibutuhkan manusia karena pemakaian *internet* sangat besar manfaatnya dan bersifat global, dengan adanya *internet* informasi yang didapat lebih mudah dan lebih cepat daripada sarana komunikasi yang lainnya.

Perkembangan *internet* tak pernah lepas dari penggunaan *domain name system (dns)*. Pengetahuan dan pengertian tentang *domain name system (dns)* merupakan hal yang mutlak dimiliki oleh operator *internet* sebab dengan adanya *domain name system (dns)* pengguna *internet* tidak perlu lagi menghafal nomor *IP (Internet Protokol)* yang menjadi penghubung antar komputer dan jaringan. Selain itu, *domain name system (dns)* juga menyediakan layanan *mail routing*, informasi mengenai *hardware*, sistem operasi yang dijalankan, dan aplikasi jaringan yang ditangani oleh *host* tersebut. Dengan adanya *domain name system (dns)* juga tidak menutup kemungkinan terdapatnya resiko celah keamanan *domain name system (dns)* yang mungkin dapat dimasuki oleh penyusup *(intruder)* pada umumnya seperti berikut ini:

1. *Domain name system (dns) spoofing* atau *cache poisoning* adalah teknik untuk memasukkan atau meracuni *cache* pada suatu *server domain name*

system (dns) dengan data atau informasi yang salah. Jika sebuah *server domain name system (dns)* terkena *domain name system (dns) spoofing* atau *cache poisoning* maka data atau informasi yang diberikan *server domain name system (dns)* tersebut tidak *valid* lagi karena telah di-*spoof* atau diracuni oleh sang penyerang[1].

2. *Denial of Service Attack (DoS)* adalah tipe penyerangan kepada suatu layanan dalam hal ini yang kita bicarakan adalah layanan *domain name system (dns)*. Akibatnya orang lain yang akan menggunakan layanan server *domain name system (dns)* ini tidak akan dapat menggunakannya[2].
3. Pengeksploitasian terhadap beberapa software *domain name system (dns)* dimana seringkali terjadi penyerangan terhadap komputer-komputer yang menjalankan aplikasi *domain name system (dns) server* untuk melayani permintaan *domain name system (dns)* pada *internet*. Umumnya serangan-serangan tersebut terjadi karena faktor cacat aplikasi *(bug)* pada software *domain name system (dns) server* serta kesalahan konfigurasi yang menyebabkan komputer tersebut dapat diambil oleh penyerang *(hacker/ cracker)*.

Berdasarkan pada hal-hal tersebut diatas dan kebutuhan informasi pada PT. NOK Indonesia, maka penulis akan menganalisa dan membuat sebuah perancangan yang dapat digunakan oleh PT. NOK Indonesia dengan

---

[1] http://pl.duniasemu.org/network/bind_dns/bind_dns-4.html
[2] Ibid, hal.1

judul **"PERANCANGAN SISTEM KEAMANAN DOMAIN NAME SYSTEM (DNS) SERVER DENGAN BIND PADA PT. NOK INDONESIA".**

1.2 Rumusan Masalah

Berdasarkan pada latar belakang diatas, maka perumusan masalahnya adalah bagaimana merancang sistem keamanan *domain name system (dns) server dengan bind* pada PT. NOK Indonesia yang aman dari sabotase user asing.

1.3 Batasan Masalah

Dalam tugas akhir ini penulis membatasi pembahasan perancangan sistem keamanan *domain name system (dns) server dengan bind* pada PT. NOK Indonesia. Pembatasan masalah yang dilakukan dalam tugas akhir ini adalah sebagai berikut:

1. Penggunaan sistem operasi berbasis linux dengan distribusi CentOS 5.4 sebagai sistem operasi *server.*
2. Untuk merancang sistem keamanan *domain name sistem (dns) server* dengan menggunakan *bind,* digunakan paket program *bind 9* dengan versi terbaru, yang mana saat tugas akhir ini dibuat versi terbaru dari bind adalah bind-9.7.1-P1.tar.gz, dimana paket program tersebut dapat berjalan dengan baik di sistem operasi linux CentOS 5.4.

3. Perancangan *domain name sistem (dns) server* dengan menggunakan sistem operasi linux CentOS 5.4.
4. Konfigurasi sistem keamanan *domain name sistem (dns) server* dengan menggunakan *bind.*

1.4 Maksud dan Tujuan

1.4.1 Maksud

Untuk menanggulangi berbagai jenis serangan terhadap celah keamanan *domain name system (dns).* Selain itu maksud dari penyusunan tugas akhir ini adalah sebagai salah satu syarat dalam pencapaian gelar Strata Satu (S1) pada Fakultas Teknik Universitas Bhayangkara Jakarta Raya.

1.4.2 Tujuan

Untuk merancang sistem kemanan *domain name system (dns) server dengan bind* pada PT. NOK Indonesia yang aman dari sabotase user asing.

1.5 Metode Penelitian

Dalam penyusunan tugas akhir ini dilakukan beberapa metode penelitian untuk melengkapi data-data yang dibutuhkan selama penulisan. Metode penelitian yang dilakukan yaitu:

1.5.1 Metode Observasi

Pengertian dari metode observasi adalah pengamatan dan pencatatan secara sistimatik terhadap unsur-unsur yang tampak dalam suatu gejala atau gejala-gejala dalam objek penelitian.

1.5.2 Metode Pustaka

Metode pustaka adalah metode penelitian yang digunakan dengan cara mengumpulkan buku-buku referensi dan informasi-informasi melalui *internet* yang berhubungan dengan tugas akhir.

1.6 Sistematika Penulisan

Adapun sistematika penulisan tugas akhir yang berjudul perancangan sistem keamanan *domain name system (dns) server* dengan *bind* pada PT. NOK Indonesia ini adalah sebagai berikut:

BAB I Pendahuluan

Bab ini berisi tentang uraian singkat mengenai:

a. Latar Belakang.

b. Maksud dan Tujuan.

c. Rumusan Masalah.

d. Batasan Masalah.

e. Metode Penelitian.

f. Sistematika Penulisan.

BAB II Landasan Teori

Bab ini berisi tentang uraian materi atau teori yang berhubungan dengan perancangan sistem keamanan *domain name system (dns) server* dengan *bind* pada PT. NOK Indonesia, yang di peroleh dari rujukan buku-buku atau media informasi yang terdapat pada *internet*.

BAB III Analisa Sistem Yang Sedang Berjalan

Bab ini menjelaskan tentang sejarah, struktur organisasi PT. NOK Indonesia, arsitektur jaringan, spesifikasi perangkat keras, analisa sistem yang sedang berjalan serta permasalahan dan pemecahannya.

BAB IV Perancangan Sistem Keamanan Domain Name System (DNS) Server Dengan BIND Pada PT. NOK Indonesia

Bab ini berisi tentang proses installasi linux CentOS 5.4, perancangan sistem keamanan *domain name system (dns) server* dengan *bind* pada PT. NOK Indonesia.

BAB V Kesimpulan dan Saran

Bab ini berisi tentang kesimpulan dari proses perancangan sistem keamanan *domain name system (dns) server* dengan *bind* pada PT. NOK Indonesia., serta saran dalam pengaplikasian agar sistem berjalan dengan aman dan optimal.

Daftar Pustaka

Dalam daftar pustaka ini berisi beberapa referensi tentang sumber-sumber materi maupun buku-buku yang dijadikan sebagai acuan dalam penulisan tugas akhir ini, selain itu ada juga beberapa referensi yang bersumber dari media *internet* yang dilengkapi dengan alamat situsnya.

Lampiran

Berisi lampiran-lampiran yang berhubungan dengan proses perancangan sistem keamanan *domain name system (dns) server* dengan *bind* pada PT. NOK Indonesia.