

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Keamanan data merupakan salah satu masalah terbesar yang dihadapi oleh dunia usaha, penyedia jasa layanan internet dan pihak pengatur kebijakan serta penegak konsekuensi pelanggaran. Berkembangnya teknologi yang memudahkan manusia dalam melakukan akses terhadap suatu komputer *standalone* maupun jaringan komputer mengharuskan pihak pengelola suatu lembaga mampu untuk menentukan bagaimana kebijakan yang ditetapkan dan mampu memperkirakan tantangan yang akan dihadapi.

Berdasarkan *survey* (Desember 2000), ancaman terbesar dari jaringan komputer adalah 68% karyawan, 17% *hacker*, 9% pesaing, dan 6% pelanggan. Hal ini tentunya dapat dijadikan salah satu pedoman bahwa faktor keamanan harus mencakup bagian dalam maupun luar organisasi agar dapat meminimalisasi ancaman dan gangguan pada sistem.

CV Brainesia sebagai sebuah perusahaan yang bergerak dalam bidang hosting, domain, dan pembuatan web mencoba untuk melakukan pembuatan infrastruktur perusahaan berupa jaringan komputer yang terdiri dari jaringan LAN dan WLAN yang terhubung pada komputer server data. Faktor terpenting yang dihadapi adalah keamanan jaringan agar data informasi dari perusahaan tersebut tidak diakses oleh pihak yang tidak berhak.

Keamanan jaringan sebagai salah satu cabang ilmu yang berkembang pada lingkungan teknologi informasi dapat digunakan sebagai ilmu untuk melakukan penggalan informasi pada sistem komputer. Informasi yang dapat kita peroleh antara lain dapat berupa *log files*, file dokumen, *file archive*, konfigurasi komputer, kelemahan komputer, dan *network traffic*. Analisis terhadap informasi tersebut dapat digunakan untuk mengambil kebijakan lebih lanjut guna pengembangan sistem keamanan jaringan komputer.

Pengujian keamanan jaringan pada CV. Brainesia menjadi salah satu solusi yang penting agar penanggungjawab keamanan maupun pihak manajemen mampu menentukan bagaimana kebijakan yang tepat terhadap sistem yang ditangani, mampu mengenali batas kemampuan sistem, *troubleshoot* jika terjadi permasalahan dan memberikan *response* terhadap anomali yang mungkin terjadi pada sistem.

Berdasarkan latar belakang di atas, maka penulis bermaksud untuk mengambil topik skripsi dengan judul **“Metode Pengujian Keamanan File Server Sebagai Langkah Dalam Menentukan Kebijakan Keamanan Di CV. Brainesia”**.

1.2 Rumusan Masalah

Berdasarkan pemaparan latar belakang masalah diatas maka dapat diidentifikasi permasalahan-permasalahan yang dihadapi dalam penelitian ini :

1. Bagaimanakah langkah-langkah untuk menguji fitur-fitur keamanan yang dapat diterapkan pada jaringan lokal CV. Brainesia?

2. Apa saja saran dan usulan kebijakan yang dapat diberikan kepada CV. Brainesia agar dapat meningkatkan keamanannya ?

1.3 Batasan Masalah

Mengingat banyaknya kemungkinan permasalahan dan agar permasalahan terfokus pada suatu permasalahan yang ingin diuraikan, maka diperlukan adanya batasan masalah, yaitu :

1. Penelitian terbatas pada pengujian metode-metode pengujian fitur-fitur keamanan komputer dan jaringan lokal.
2. Penelitian dilakukan dengan metode simulasi, bukan pada objek sebenarnya karena merupakan mesin produksi yang sedang beroperasi sehingga tidak dimungkinkan untuk implementasi secara langsung.
3. Informasi yang digali merupakan informasi yang bersumber pada keadaan sistem terkoneksi dengan jaringan lokal.
4. Jaringan komputer yang digunakan adalah Local Area Connection (LAN) yang terhubung dengan sebuah Access Point (AP).
5. Penelitian ini menggunakan IPv4.
6. Penelitian ini tidak membahas enkripsi secara mendalam.
7. Komputer server menggunakan sistem operasi Windows Server 2003.
8. Produk antivirus yang digunakan adalah Clamav Windows.
9. Mode keamanan yang digunakan pada perangkat nirkabel adalah Hidden SSID, MAC Filter, WEP (Wired Equivalent Privacy), dan WPA/WPA2 (Wi-Fi Protected Access).

10. Program aplikasi yang digunakan komputer penguji (tester) merupakan program aplikasi yang sudah terinstall pada Linux Backtrack 5 diantaranya Aircrack-ng Suite, Nmap, Nessus, Armitage.

1.4 Maksud dan Tujuan Penelitian

Maksud dan tujuan yang ingin dicapai dari penelitian ini adalah :

1. Memenuhi salah satu syarat dalam rangka menyelesaikan program studi Strata 1 Jurusan Teknik Informatika di Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta.
2. Membangun komputer server dengan pertimbangan fungsional dan keamanan.
3. Membangun infrastruktur jaringan yang handal dan dapat memberikan jaminan keamanan.
4. Memperkenalkan perangkat lunak seperti Aircrack-ng suite, Nmap, Nessus, Armitage, dan Wireshark sebagai perangkat lunak bantu guna menemukan celah keamanan jaringan kemudian digunakan sebagai acuan dalam proses pengamanan jaringan.

1.5 Manfaat Penelitian

Manfaat yang dapat diambil dari penelitian yang dilakukan adalah :

1. Memberikan solusi alternatif kepada CV. Brainesia dalam melakukan konfigurasi perangkat jaringan.

2. Memberikan jaminan keamanan terhadap penggunaan infrastruktur jaringan pada CV. Brainesia.
3. Sebagai referensi belajar bagi mahasiswa untuk meningkatkan pemahaman tentang keamanan jaringan.
4. Sebagai acuan bagi mahasiswa lain dalam melakukan penelitian skripsi dengan tema yang sama.

1.6 Metode Penelitian

Beberapa metode yang digunakan dalam penelitian ini, yaitu:

1. Kepustakaan

Metode ini diterapkan dengan membaca dan memahami literatur-literatur yang berhubungan dengan objek penelitian. Literatur yang ada menjadi landasan tentang teori-teori seputar objek yang diteliti.

2. Interview

Metode ini diterapkan dengan cara melakukan komunikasi langsung dengan beberapa orang yang lebih menguasai bidang yang sedang diteliti. Selain itu dilakukan juga komunikasi langsung dengan elemen-elemen terkait dengan objek penelitian.

3. Eksperimental dan Observasi Komputer

Metode ini diterapkan dengan cara membangun objek penelitian, yaitu dengan membangun infrastruktur LAN, WLAN, serta komputer server secara simulasi guna mengurangi resiko kerusakan dan efisiensi

waktu. Pengujian yang dilakukan kemudian dianalisis dan diambil kesimpulan.

1.7 Sistematika Penelitian

Sistematika penulisan laporan ini agar dapat lebih terstruktur serta mudah dipahami maka dibagi dalam beberapa bagian yaitu :

1. Bab I : PENDAHULUAN

Bab ini menguraikan tentang latar belakang, batasan masalah, maksud, tujuan, dan sistematika penulisan.

2. Bab II : LANDASAN TEORI

Bab ini menguraikan tentang tinjauan pustaka mengenai konsep dan prinsip dasar yang diperlukan untuk memecahkan masalah penelitian. Disamping itu juga memuat uraian tentang hasil penelitian yang pernah dilakukan sebelumnya oleh peneliti lain yang ada hubungannya dengan penelitian yang dilakukan.

3. Bab III : METODE PENELITIAN

Bab ini menguraikan tinjauan mengenai identifikasi permasalahan dan langkah dalam membangun simulasi infrastruktur jaringan LAN dan WLAN serta metode pengujian yang akan dilakukan pada infrastruktur yang dibangun.

4. Bab IV : HASIL DAN PEMBAHASAN

Bab ini menguraikan tentang proses dan hasil pengujian keamanan pada komputer server dan jaringan yang telah dibangun. Pada bab ini

pula dilakukan pembahasan proses yang dilakukan dan berdasarkan hasil tersebut dilakukan penyusunan usulan kebijakan keamanan yang dapat diberikan guna menjamin keamanan sistem yang dibangun.

5. Bab V : PENUTUP

Bab ini menguraikan pemaparan singkat berupa kesimpulan dan saran yang direkomendasikan bagi CV. Brainesia maupun untuk pengembangan penelitian selanjutnya.

