BAB 1

PENDAHULUAN

1.1 Latar Belakang

Teknologi komputer seperti perangkat lunak, jaringan, maupun perangkat keras semakin berkembang untuk menjawab kebutuhan konsumen yang semakin kompleks. Pada pengembangannya, masing-masing mendapat porsi dan proses perkembangan yang berbeda.

Salah satu perkembangan teknologi komputer adalah *Internet*. *Internet* merupakan hasil teknologi komputer yang diciptakan agar *user* dapat berinteraksi dengan dunia luar (informasi). Oleh karena itu, dapat dilihat bahwa informasi merupakan kebutuhan yang penting untuk sebagian besar masyarakat. Berbagai informasi dapat diakses dengan mudah melalui *Internet*. Sumber-sumber informasi dapat diakses secara bebas ketika ter*hub*ung dengan jaringan *Internet*. Namun, untuk mengakses *Internet*, dibutuhkan koneksi yang baik dan cepat. Koneksi seperti ini akan menentukan kemudahan yang dapat diberikan kepada *user*.

Berbagai informasi seperti musik, *file, film,* data, dan lainnya dapat dicari ketika mengakses *Internet*. Apalagi jika bergerak pada badan instansi tertentu seperti universitas ataupun perusahaan, kebutuhan untuk mengakses *Internet* untuk mendapatkan informasi yang sesuai kebutuhan akan sering dilakukan, jenis kebutuhan ini ada yang bersifat umum, namun ada juga yang bersifat pribadi maupun rahasia untuk kepentingan instansi tersebut. Dalam pemakaian *Internet*,

user dapat secara bebas mengakses dan masuk ke dalam jaringan *Internet* yang ada karena bersifat *shared* dan *public*. Oleh karena itu, dikhawatirkan timbul permasalahan pada jaringan *Internet* yang ada, sehingga dibutuhkan keamanan yang baik dalam pemakaian *Internet* agar tidak merugikan pihak instansi ataupun pemakai yang ada. Keamanan dalam mengakses data menjadi hal yang patut dipertimbangkan ketika *Internet* digunakan untuk mendapatkan informasi penting dari dalam perusahaan atau instansi seperti sekolah dan universitas. Hal ini tentu saja akan sangat merugikan ketika akses *Internet* yang bebas itu dapat dimasuki oleh pihak lain dan digunakan untuk kepentingan yang tidak baik.

Untuk itu perlu suatu solusi dalam menanggulangi masalah yang ada dalam meningkatkan QoS (*Quality Of Service*) yang diberikan pihak instansi kepada *user*. Solusi ini diharapkan mampu menyelesaikan masalah keamanan jaringan *Internet* seperti adanya *server* yang mengatur pembatasan dan otentikasi pengaksesan pada *client* yang ingin menggunakan layanan *Internet* di UPH, salah satunya adalah dengan menggunakan *captive portal*.

1.2 Perumusan Masalah

Penggunaan jaringan *Internet* yang terus berkembang serta maraknya koneksi *wireless* yang digunakan, maka dibutuhkan suatu aplikasi yang dapat meningkatkan keamanan dari jaringan *Internet* yang digunakan. Setiap orang yang mau mengakses *Internet* dapat secara bebas memakai *Internet* di UPH jika telah terdaftar MAC *address*-nya dan pihak luar juga dimungkinkan dapat mengakses *Internet* dengan memakai MAC *address user* lain dikarenakan tidak adanya *security* yang jelas. Hal seperti ini disebut MAC *spoofing*, yaitu peniruan

atau penduplikasian MAC oleh orang lain sehingga dapat menjadi masalah ketika akan digunakan oleh pihak yang memiliki MAC *address* tersebut. Hal ini menyebabkan ketidaknyamanan dari sisi *user* yang ingin menggunakan layanan tersebut serta *service* yang diberikan pun menjadi tidak maksimal. Untuk mengatasi permasalahan tersebut, diperlukan adanya aplikasi *server* yang dapat melakukan beberapa *action* seperti aplikasi yang mengatur bagaimana proses seorang *user* sebelum mengakses *Internet*. Proses ini dapat diatur dengan menggunakan aplikasi *captive portal. Captive portal* merupakan suatu sistem yang mengatur informasi yang dapat diakses oleh *client* setelah melalui proses otentikasi. Untuk memeriksa hak akses dari *user* menggunakan proses *login* dan *password* yang terhubung dengan *database* sehingga proses sinkronisasi pun terjadi. Pembentukan *captive portal* yang dibangun harus dapat memenuhi standar-standar yang biasa diimplementasikan pada instansi tertentu, misalnya dapat melakukan proses otentikasi *user*, dapat melakukan proteksi kepada *user* untuk menghindari aktivitas-aktivitas *wireless* yang tidak diinginkan, serta melakukan *manage* yang lebih baik dalam mengatur aktivitas *wireless* dan *user*.

Jadi permasalahan yang akan dibahas pada laporan tugas akhir ini adalah gambaran umum sistem koneksi *wireless* dan *wireline* pada saat menggunakan *captive portal* beserta keterangan dan informasi yang ada. Lalu, akan dibahas juga aplikasi dan prinsip kerja *captive portal*, sehingga dipahami proses kerja aplikasi secara lengkap dan jelas. Pada saat implementasi akan diterangkan proses instalasi, proses pengerjaan aplikasi pfSense serta tampilan aplikasi yang dibangun, sehingga diketahui proses-proses serta hal-hal yang diatur pada

aplikasi. Hasil implementasi diuji coba, sehingga dapat dilihat hasil yang diinginkan apakah sesuai dengan kebutuhan pemakai layanan *Internet* di kampus atau tidak.

1.3 Ruang Lingkup dan Batasan Permasalahan

Ruang lingkup dan batasan masalah yang terkait dengan pokok permasalahan di atas adalah *User* yang ingin menggunakan *Internet* dapat melakukan *login* satu kali setiap kali akan memakai layanan internet tersebut pada jangka waktu tertentu; melalui *login* ini, *user* mendapatkan tingkat *security* yang lebih aman dengan adanya proses otentikasi. Kemudian mengimplementasikan *Captive portal*, yaitu sebuah aplikasi *web server* yang berfungsi sebagai protokol yang memberikan ijin pengaksesan *Internet* kepada *user* yang ingin mengakses layanan tersebut. Ijin ini diberikan kepada *user* setelah melalui proses-proses otentikasi yang ada, setelah itu kebijakan diberikan untuk disetujui sebelum *user* benar-benar mengakses ke *Internet*. Hal ini dilakukan agar *provider* tidak bertanggung jawab lagi jika *user* yang telah menyetujui *policy* melakukan aksi kriminal pada *network*. *Captive portal* biasa digunakan pada instansi tertentu yang memakai *wireless connection* dalam mengakses *Internet*. Biasanya berupa *login* dan *password* sebelum masuk dan mengakses *network*. Kebanyakan *Captive portal* juga berisi anti *virus* dan *firewall* untuk membantu melindungi dan mencegah kerusakan pada komputer *client* dari *Internet* dan pihak lainnya.

Captive portal yang akan dibangun harus dapat memenuhi kebutuhan pemakaian jaringan *Internet* di UPH, sehingga kondisi permasalahan di UPH dapat diselesaikan dengan adanya aplikasi ini. Sesuai dengan kondisi

permasalahan di atas, maka batasan masalah yang dirumuskan dalam membangun *captive portal* adalah aplikasi *captive portal* ini harus dapat melakukan proses otentikasi kepada *user* yang ingin menggunakan layanan *Internet* di UPH. Aplikasi *captive portal* juga harus dapat diimplementasikan ke semua tipe koneksi jaringan *Internet*, misalnya *wireless* dan *wireline* di UPH.

1.4 Tujuan Magang

Berdasarkan rumusan masalah yang telah dijelaskan sebelumnya, hasil akhir yang diharapkan adalah bahwa dengan menerapkan aplikasi *captive portal* pada sistem koneksi jaringan *wireless* dan *wireline* di UPH, dapat dihasilkan kualitas sistem keamanan yang lebih optimal pada jaringan internet.

1.5 Alokasi waktu & Tempat Magang

Pada tabel 1.1 akan ditampilkan kegiatan dan hasil kerja penulis selama magang di ICT UPH. Magang dimulai dari tanggal 1 Maret 2007 sampai dengan 31 Agustus 2007. Tempat magang berlangsung di Universitas Pelita Harapan bagian ICT lantai 5 Gedung B selama 6 bulan dan mengerjakan aplikasi *captive portal* serta pekerjaan rutin lainnya.

Tabel 1.1 Alokasi waktu & Tempat magang

Tanggal	Kegiatan	Tempat Magang	Hasil Kegiatan
1/3/2007 - 15/3/2007	Mencari informasi yang berhubungan dengan aplikasi *captive portal*	ICT UPH ruang 540	Mendapatkan beberapa sumber data seperti definisi dan karakteristik aplikasi *captive portal* (en.wikipedia.org/wiki/captive_portal) dan informasi awal mengenai aplikasi
16/3/2007 31/3/2007	Melakukan kegiatan rutin (menarik kabel, *troubleshooting* , dan *request* lainnya) serta memilah informasi mengenai aplikasi yang ada	ICT UPH ruang 540	Menemukan langkah awal dalam mengerjakan aplikasi Captive portal dan membuat laporan bab 1
1/4/2007 - 30/4/2007	Melakukan kegiatan rutin dan mencoba mengerjakan aplikasi	ICT UPH ruang 540	Mendapatkan beberapa hal dari kegiatan rutin dan sedang mengalami kebuntuan dalam pengerjaan aplikasi dan mengerjakan bab 2
1/5/2007 - 31/5/2007	Melakukan kegiatan rutin dan mendapatkan informasi baru mengenai pengerjaan aplikasi	ICT UPH ruang 540	Mencoba memahami informasi baru dari www.pfsense.com serta perencanaan pengerjaan aplikasi dari dan membuat bab 3
1/6/2007 - 30/6/2007	Melakukan kegiatan rutin dan melakukan percobaan terhadap aplikasi yang dibangun dengan menggunakan pfSense	ICT UPH ruang 540	Mendapatkan hasil awal pada pengerjaan aplikasi *captive portal* berupa uji coba dengan 1 komputer dan mengerjakan bab 4
1/7/2007 - 31/7/2007	Melakukan kegiatan rutin dan melakukan percobaan aplikasi dengan ruang lingkup yang lebih besar melalui banyak komputer	ICT UPH ruang 540	berhasil mencapai tujuan yang diinginkan pada pengerjaan aplikasi dan menyelesaikan bab 4
1/8/2007 - 31/8/2007	Melakukan penyelesaian Laporan dan pengerjaan aplikasi	ICT UPH ruang 540	menyelesaikan laporan dan pengerjaan aplikasi *captive portal*

1.6 Sistematika Penulisan

Laporan Magang ini terbagi menjadi lima bab yaitu:

BAB 1 PENDAHULUAN

Bab ini membahas latar belakang sistem pengajuan *captive portal* yang terdapat di UPH yang mendorong dikembangkannya komputerisasi dari sistem yang ada.

BAB 2 LANDASAN TEORI

Bab ini berisi konsep dan teori yang dipakai untuk menunjang pengembangan aplikasi dan *hub*ungannya dengan bidang-bidang terkait pada sistem.

BAB 3 GAMBARAN UMUM ICT

Bab ini menjelaskan profil umum ICT serta topologi jaringan tempat magang penulis. Dijelaskan pula sistem pengajuan dan kondisi sistem yang telah dan sedang digunakan oleh UPH, mencakup batasan dan permasalahan yang dihadapi.

BAB 4 ANALISIS DAN PERANCANGAN

Bab ini menjabarkan analisis dan perancangan dari aplikasi *Captive portal* sebagai solusi dari masalah-masalah pada sistem lama.

BAB 5 KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan secara keseluruhan dari laporan tugas akhir. Saran untuk penelitian lebih lanjut maupun saran perbaikan untuk perusahaan juga dituliskan pada bab ini