BAB V

PENUTUP

5.1 Kesimpulan

Dari hasil pengujian skripsi ini, dapat diambil kesimpulan agar dapat menjawab pertanyaan-pertanyaan yang terdapat pada rumusan masalah:

1. *Administrator* jaringan dalam mengelola obyek-obyek yang ada dijaringan yaitu berupa data, user, komputer, dapat dimanajemen secara terpusat dengan cara menjadikan komputer workgroup menjadi satu domain dengan satu domain dengan server *Domain Controller Active Directory* (Gambar 4.35, 4.40 dan 4.42)
2. Dengan menggunakan pengaturan kebijakan *Group Policy* , akan memberikan kemudahan bagi *Administrator* jaringan dalam mengelola *resource* jaringan secara terpusat. Sehingga dapat menghindari konfigurasi manual pada setiap *user* atau karyawan. Seperti:
    a) Maping drive tiap departemen (Subab 4.8).
    b) Menerapkan *security policy* kesemua karyawan pada folder Data Asset2, COJ, Asset (Tabel 4.7 Domain Users (MSV\Domain users)).
    c) Tidak diizinkan pengguaan USB atau CD atau DVD (Gambar 4.69 dan 4.70).
    d) Install Aplikasi untuk client AD dapat dilakukan terpusat di server AD (Gambar 4.72).

3. *Group policy Active Directory Domain Services* dapat dimanfaatkan untuk mengoptimalkan *security policy* terhadap hak akses data berdasarkan departemen masing-masing, dan memberikan otoritas tinggi tiap *Lead Departement.* Yaitu dengan menetapkan *Share Permission* (Tabel 4.3 dan Gambar 4.46) dan *security permission* (Tabel 4.6, 4.7 dan Gambar 4.48, 4.51, 4.52). Jadi dapat menciptakan *convidentiality, availability, integrity* data di server.
4. *Active Directory* dapat mengontrol karyawan atau user menggunakan *account* dan mengakses data ke server dengan menggunakan *logon hours*, dengan batasan jam yang telah ditentukan (Gambar 4.71). Hal ini dapat mendorong terciptanya prosedural jika menghendaki penggunaan *account* dan akses data di server sesuai dengan alur bagan *connection policy* (Sub-bab 3.7.5 Gambar 3.13).
5. Fitur *Group Policy Menagement* pada *Domain Controller Active Directory* dapat membantu mencegah tindakan *Attacker* dari menerka-nerka *password* pengguna dan mengurangi keberhasilan serangan dalam jaringan. Hal ini dibuktikan setingan teknis sub-bab 4.6 pada gambar 4.58 dengan hasil Gambar 4.59.
6. *Domain Controller* server *Active Directory* dapat mengontrol aktifitas karyawan atau *user* ketika menggunakan komputer. Hal ini dibuktikan dengan segala *service* yang membutuhkan *run Administrator*. Jadi, terkontrol dengan adanya otentikasi seperti contoh penambahan plugin

maya, install mapun un-*install* aplikasi, perubahan IP *address* (Gambar 4.60)

7. Fitur *Group Policy Menagement* pada *Domain Controller Active Directory* dapat membantu mencegah bocornya aset data melalui USB Flashdisk atau CD atau DVD dari Departmen yang telah ditetapkan kebijakan *Disable* Eksternal *Storage* atau dari user yang *unauthorized.* (Gambar 4.69 dan Gambar 4.70). Hasil dari tersebut, terciptalah prosedur *copy file* yang terdapat pada alur bagan Gambar 3.14.
8. Pengaturan *Audit Policy* untuk menentukan kejadian-kejadian keamanan yang dilaporkan oleh sistem (Gambar 4.66).

5.2 Saran

Dari perancangan sistem *Domain Controller Active Directory* ini, ada beberapa saran yang dapat dikembangkan untuk penelitian berikutnya. Adapun sarannya seperti berikut:

1. Server *Domain Controller Active Directory* yang saat ini masih menyatu dengan server *Data Center* perlu dipisah agar dapat lebih mengoptimalkan proses kerja masing-masing server, dan menempatkan server *Data Center* di area intranet untuk menghindari serangan dari luar.
2. Penaganan *track record* cetak document melalui printer perlu diketahui agar mengetahui siapa, dimana dan kapan ketika cetak document. Penerapan ini dengan memanfaatkan *Group Policy Menagement* dengan *service audit.*

3. Sistem Domain Controller *Active Directory* akan lebih baik jika dilakukan penambahan server backup atau replikasi main server active directory, untuk menjaga kestabilan proses otentikasi user dan ketersediaan *database server Active Directory*.
4. Protokol apa yang digunakan *Operating system* Macingtosh, Linux, Unix ketika ingin join ke Domain Control Active Directory, sehingga semua aset OS yang dimiliki PT. MSV Pictures dapat menjadi member server *Active Directory* Windowserver.
5. Perlu dibuat *Standard operating procedure* kepada user atau karyawan ketika menjalankan tugas atau bekerja, untuk mendukung sistem *security policy* dan fungsi *Domain Controller Active Directory*.
6. Perlu dipertimbangkan Koneksi *client Active Directory* ke *server Active Directory* menggunakan media transmisi *Wireless Fidelity*, karena sering terjadi kegagalan sistem.