BAB V

PENUTUP

5.1. Kesimpulan

1. *Authentication windows* terhadap *user* adalah pengenalan *windows* terhadap *user* serta *Sid User* tersebut.
2. *Authorization windows* terhadap *user* adalah *restricted user* terhadap *resource*.
3. *Accounting* dalam *windows security* digunakan untuk melakukan pengubahan terhadap *Authorization user* terhadap *resource*.
4. *Accounting* digunakan untuk melakukan *optimalisasi Windows Security* atau mendefaultkan *Windows security*.
5. *Optimalisasi windows security* dilakukan dengan cara menambah *access rule* atau *permission* terhadap *privilege resource* dan juga dengan melakukan pengubahan nilai data atau *encryption*.
6. Keamanan *windows* bekerja dengan cara *Authentication user* dan menyeleksi hak *user* atau disebut dengan *Authorization*.
7. Kelemahan sistem keamanan *windows* adalah *file* yang digunakan untuk menyimpan informasi keamanan dapat di-*extract*.
8. *Privilege resource* adalah sebuah bentuk *authorization user* terhadap *resource*.
9. *Privilege resource* dapat diubah menggunakan operasi *permission*.

10. *Sid* adalah nilai yang digunakan untuk melakukan operasi *permission* bukan *user name*.

5.2. Saran

Saran bagi teman-teman yang akan mengembangkan hasil analysis yang terdapat pada skripsi ini adalah:

1. Mengetahui cara mendapatkan *Sid* serta dapat mengconvertnya menjadi variable string.
2. Mengetahui fungsi *SACL*, *DACL*.
3. Mengetahui fungsi *Descriptor*.
4. Mengetahui dan bisa menggunakan fungsi *pointer* dengan baik.