

## BAB V PENUTUP

### 5.1. Kesimpulan

Dari pengujian penelitian yang telah dilakukan untuk pengamanan *server* pada layanan *secure shell* (ssh) dapat disimpulkan hasil sebagai berikut:

1. Keamanan *secure shell* (ssh) tanpa pengamanan *port knocking* dan *key authentication* dapat ditembus oleh perentas dengan metode *brute force* dengan mendapatkan *username* dan *password* yang digunakan administrator *server*.
2. Keamanan *secure shell* (ssh) dengan pengamanan *port knocking* dan *key authentication* tidak dapat ditembus oleh perentas dengan metode *brute force* dan metode *sniffing*.
3. Hasil pengujian pada penelitian ini adalah pengamanan *secure shell* (ssh) dengan *port knocking* dan *key authentication* lebih baik daripada tanpa pengamanan lebih. Serangan *sniffing* dapat melihat pola *port knocking* dan data yang dikirim *secure shell* (ssh). Serangan *brute force* efektif untuk menyerang *secure shell* (ssh) tanpa keamanan dengan metode *port knocking* dan *key authentication*.

### 5.2. Saran

Berdasarkan penelitian yang dilakukan terdapat saran untuk perkembangan penelitian selanjutnya:

1. Menambahkan pembuatan pola *port knocking* secara manual dan dikirim kepada administrator secara otomatis.
2. Menambahkan enkripsi pada pola *port knocking* untuk menghindari serangan *sniffing*.
3. Jika administrator lebih dari satu, tambahkan aplikasi untuk para administrator dapat melihat pola port knocking yang dapat digunakan.