

## **BAB V**

### **KESIMPULAN DAN SARAN**

#### **5.1. Kesimpulan**

Hasil penelitian ini membuktikan bahwa implementasi SSH secara standart tidak cukup efektif dalam mengamankan transmisi FTP. Teori tentang kelemahan SSH pada brute force root login terbukti benar dengan hasil yang didapat pada fase brute force dengan Hydra. Password dari root dapat ditemukan dalam 49 kali percobaan dari 81 kombinasi.

#### **5.2. Saran**

Berdasarkan dari hasil penelitian di atas kelemahan ssh bisa di cegah dengan:

1. penerapan firewall untuk melindungi port.
2. Menggunakan port knocking
3. Menggunakan password dengan kombinasi unik seperti menyisipkan angka ditengah password dengan minimal panjang 8 atau lebih
4. Memasang captcha sehingga perlu verifikasi untuk login
5. Meperlambat waktu login sehingga serangan *bruteforce* akan bisa diminimalisir.
6. Melakukan verifikasi dengan digital signature pada piranti lunak yang digunakan untuk memastikan keaslian dan mencegah beredarnya malicious program pada sistem sehingga backdoor tidak bisa dipasang.
7. Membuat backup sistem log secara rutin dengan scheduler program.

8. direktori dan dengan nama yang berbeda, untuk menghambat proses covering tracks.

