BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil pembahasan pada konfigurasi dan pengujian yang telah dipaparkan pada BAB IV, dapat ditarik beberapa kesimpulan penting terkait keamanan server Ubuntu menggunakan metode Port Knocking dan Intrusion Detection System berbasis PortSentry:

1. Meningkatkan keamanan akses terhadap server Ubuntu menggunakan port knocking: Implementasi port knocking telah terbukti efektif dalam meningkatkan keamanan akses ke server Ubuntu. Dengan menyembunyikan port 22 dan 80 dari pemindaian, akses hanya diberikan setelah pengguna memasukkan urutan knocking yang benar. Ini mencegah serangan brute force dan otomatis yang mengincar port terbuka, sehingga memberikan lapisan keamanan tambahan yang signifikan.

2. Peran IDS dalam mendeteksi aktivitas mencurigakan: Intrusion Detection System (IDS) seperti Snort atau Suricata dapat memantau lalu lintas jaringan secara real-time untuk mendeteksi aktivitas mencurigakan, seperti port scanning atau usaha eksploitasi. Dengan mendeteksi dan mencatat alamat IP pelaku, IDS memberikan peringatan dini dan dapat secara otomatis memblokir ancaman yang teridentifikasi, sehingga menambah perlindungan bagi server.

3. Dampak implementasi terhadap kinerja server: Kombinasi port knocking dan IDS tidak memengaruhi kinerja operasional server secara signifikan. Sistem tetap efisien dengan pengaturan firewall dan knocking sequence yang terintegrasi dengan baik, memastikan pengalaman pengguna yang lancar tanpa mengorbankan keamanan.

4.

Secara keseluruhan, kombinasi Port Knocking dan Intrusion Detection System berbasis PortSentry terbukti menjadi solusi yang efektif dalam meningkatkan keamanan server Ubuntu. Implementasi ini memberikan perlindungan berlapis terhadap akses tidak sah dan serangan jaringan tanpa

mengorbankan kinerja server, menjadikannya strategi yang relevan untuk melindungi server dari ancaman siber yang semakin kompleks.

5.2 Saran

Berdasarkan kesimpulan implementasi *port knocking* dan penggunaan *firewall* untuk meningkatkan keamanan *server*, ada beberapa saran yang dapat penulis sampaikan, yaitu :

1. Melakukan pemantauan teratur terhadap aktivitas *port scanning* dan konfigurasi *firewall* untuk mengidentifikasi potensi ancaman keamanan baru.
2. Memperbaharui secara berkala kebijakan keamanan yang mengatur penggunaan *port knocking* dan manajemen *firewall* sesuai dengan perkembangan teknologi dan serangan keamanan terbaru.
3. Memberikan pelatihan intensif kepada *administrator* dan pengguna mengenai penggunaan yang benar dari teknik *port knocking* dan pentingnya keamanan jaringan untuk meningkatkan kesadaran dan responsibilitas terhadap keamanan informasi.