

BAB V

PENUTUP

5.1 Kesimpulan

Penelitian ini bertujuan untuk meningkatkan keamanan jaringan di ruangan Sertifikasi Informatika BLPT Yogyakarta dengan mengimplementasikan Intrusion Detection System (IDS) berbasis aplikasi Snort. Dalam penelitian ini metode pengujian yang dilakukan untuk penerapan IDS berbasis Snort ini SLC (Security Life Cycle) dengan tahapan mulai dari merancang topologi, konfigurasi, implementasi, pengujian, evaluasi hasil pengujian. Snort terbukti efektif dalam mendeteksi berbagai jenis serangan intrusi seperti ICMP Ping, Akses SSH, Akses Telnet dan Scanning Nmap dan salah satu jenis serangan Dos yaitu Ping Of Death

Pengujian yang dilakukan juga sejenis dengan rules yang dibuat seperti pengujian melalui Ping dari Client, Akses SSH melalui Putty dan Windows Powershell, Akses Telnet melalui Putty, Scanning Nmap menggunakan aplikasi Zenmap GUI dan Ping Of Death melalui CMD. Dari pengujian tersebut hasilnya menunjukkan Snort dapat mendeteksi dan mencatat semua serangan tersebut dengan akurat baik dari IP, waktu dan jenis serangannya.

Implementasi IDS Snort di ruangan Sertifikasi Informatika memberikan efek yang signifikan dalam meningkatkan keamanan jaringan di ruangan tersebut. Dengan kemampuan Snort yang dapat mendeteksi serangan secara realtime potensi serangan intrusi dalam ruangan tersebut dapat di minimalisir sehingga dapat melindungi PC yang ada pada ruangan tersebut.

5.2 Saran

Berikut merupakan saran yang dapat dipertimbangkan bagi peneliti selanjutnya yang akan membahas tentang Snort.

1. Pengembangan rules Snort sangat disarankan untuk dapat memastikan Snort dapat mendeteksi jenis-jenis serangan yang lebih baru
2. Menerapkan integrasi dengan beberapa software untuk monitoring seperti

Bot Telegram dan Bot Whatsapp

3. Untuk pengembangan penelitian kedepannya bisa menerapkan *block* serangan secara otomatis.

