BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kesimpulan yang dapat diambil dari penelitian dengan judul Analisis dan Perancangan *Reactive Intrusion Detection System* Menggunakan Mikrotik Berbasis Log dan Mail Report (Studi Kasus: PT. Wahana Lintas Nusa Persada) adalah sebagai berikut :

1. Administrator Jaringan PT.Wahana Lintas Nusa Persada dapat melakukan quick respon terhadap adanya serangan jaringan berupa serangan *FTP Bruteforce, SSH Bruteforce* dan *ICMP Flood (ping of death)* dengan memantau log melaui *syslog server The Dude* yang diiringi dengan suara dan popup untuk memudahkan penangkapan informasi oleh admin ketika serangan terjadi. (Lampiran IV)
2. Administrator yang *mobile* dapat mengetahui jenis serangan *FTP Bruteforce, SSH Bruteforce* dan *ICMP Flood (ping of death)* yang terjadi pada jaringan client dengan memlihat setiap email yang dikirim sebagai respon sistem terhadap adanya serangan. (Gambar 4.44, 4.56, 4.69)
3. Administrator pada jaringan client PT. Wahana Lintas Nusa Persada dapat memantau log router miliknya melalui *syslog server mikrotik syslog* yang dikirim oleh *reactive intrusion detection system* .(Lampiran IV)
4. Dengan adanya laporan mingguan administrator PT. Wahana dapat mengetahui *IP address* penyerang *FTP Bruteforce, SSH Bruteforce* dan *ICMP Flood (ping of death)* selama satu minggu terakhir yang dikirim

5. melalui email, untuk memudahkan dalam dokumentasi serangan dan dapat dipantau melalui *syslog server the dude*. (Gambar 4.44, 4.58, 4.70, Lampiran IV)
6. Seluruh kendali *reactive IDS* dapat dilakukan secara terpusat menggunakan *syslog server The Dude*.
7. Pada *fungsional test reactive intrusion detection system* menggunakan mikrotik versi 5.20 dapat mendeteksi adanya serangan baik berupa *FTP Bruteforce, SSH Bruteforce* dan *ICMP Flood (ping of death)* dan menghalau serangan tersebut serta melakukan respon dengan mengirimkan email dan log.
8. Berdasarkan pengujian yang telah dilakukan, *reactive intrusion detection system* menggunakan mikrotik versi 5.20 yang telah dibangun adalah jenis *interval based (batch mode)* dimana Informasi dikumpulkan terlebih dahulu dan kemudian dievaluasi menurut interval waktu yang telah ditentukan (Gambar 4.74, 4.75), atau dengan jenis *realtime* dimana informasi dapat langsung dikirim. (Tabel 4.13,4.14)
9. Berdasarkan percobaan yang telah dilakukan dengan melakukan serangan secara berurutan *(Sekuensial)* dan Serentak *(simultan) respon time* sistem yang dihasilkan adalah tidak tentu *(fluktuasi)*. (Sub-bab Respon Time Test)
10. Berdasarkan pengujian yang telah dilakukan, perbedaan interval penjdwalan script dengan *timeout* sebuah *address-list* dapat menimbulkan respon sistem berupa *false positive* dalam mode interval. (Tabel 4.12)

5.2 Saran

Dari perancangan *reactive intrusion detection system* menggunakan mikrotik versi 5.20 ini, Ada beberapa saran yang dapat dikembangkan untuk penelitian selanjutnya. Adapun sebagai berikut :

1. *Reactive Intrusion detection system* menggunakan mikrotik versi 5.20 ini dapat di integrasikan dengan *sms gateway*, agar respon sistem dapat berupa pengiriman sms.
2. *Reactive Intrusion detection system* menggunakan mikrotik versi 5.20 ini dikembangkan menjadi *Anomaly Detection System*.
3. *Reactive Intrusion detection system* menggunakan mikrotik versi 5.20 ini akan lebih baik dikembangkan mengggunakan *application Programmable Interface* (API) untuk membuat perangkat lunak yang dapat dimodifikasi untuk berkomunikasi dengan *RouterOS* untuk mengumpulkan informasi.
4. Dikembangkan dengan menambah fitur update otomatis.
5. Pengujian serangan lebih bervariasi lagi.
6. Perlunya pengujian *false negative* dan *false positive* secara lebih mendalam, untuk mengetahui tingkat *anomaly false negative* dan *positive*