BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil Skripsi maka dapat diambil kesimpulan sebagai berikut:

1. Sistem Monitoring dan Pencegahan dengan Rules Penanganan Spesifik Serangan Scanning, Dos, Exploit pada Komputer Server menggunakan Suricata telah sesuai dengan apa yang diharapkan di perancangan awal hal tersebut dibuktikan berdasarkan hasil pengujian.

2. Suricata yang berperan sebagai monitoring dan pencegah serangan mampu mengatasi beberapa tipe serangan yang ditujukan langsung kepada server mulai dari serangan *basic* meliputi *scanning TCP/UDP*, serangan level *Intermediate* meliputi *Flooding*, dan level *hardest* yaitu Exploit yang menggunakan *Metasploit* sebagai alat eksploitasi.

3. Suricata memiliki dua mode *inline* untuk mengatasi serangan yang ditujukan kepada server yaitu inline *NFQUEUE* dan *AF_PACKET*. Skripsi ini menggunakan mode inline *AF_PACKET* dalam pengoperasiannya. AF_PACKET pada awalnya hanya mampu dalam mendeteksi tanpa melakukan aksi pencegahan berupa *Drop packet* dan *Reject connection*, namun perkembangan teknologi yang begitu cepat,

developer Suricata memastikan teknologi terbaru AF_PACKET mampu mengadopsi kemampuan NFQUEUE dalam melakukan aksi pencegahan serangan.

5.2 Saran

Beberapa saran yang dapat diberikan antara lain :

1. Sistem Monitoring dan Pencegahan dengan Rules Penanganan Spesifik Serangan Scanning, Dos, Exploit pada Komputer Server menggunakan Suricata dapat di kembangkan arsitekturnya dengan kombinasikan Suricata IDPS dan NSM dengan PFSense menggunakan mode inline NFQUEUE dan IPTables

2. Sistem Monitoring dan Pencegahan dengan Rules Penanganan Spesifik Serangan Scanning, Dos, Exploit pada Komputer Server menggunakan Suricata dapat dikembangkan dengan cangkupan luas seperti pencegahan serangan yang ditujukan langsung pada komputer server dan atau komputer client dalam satu lingkup dengan penggunaan mode NFQUEUE, IPTables dan rules terbaru sesuai perkembangan tipe serangan didunia teknologi informasi.

4. Sistem monitoring yang telah dibangun masih memiliki kekurangan yaitu tidak memiliki web based sebagai control panel berbasis *GUI*, sehingga dalam melakukan pendeteksian serangan terdapat serangkaian data

informasi yang bercampuran tanpa terpisah antara serangan yang telah terjadi dan serangan yang masih berlangsung. Saat melakukan pengujian terpisah menggunakan web based ELK sebagai kontrol panel, web based tidak dapat memberikan informasi tindakan pencegahan yang telah dilakukan Suricata dan hanya menampilkan informasi pendeteksian. Sehingga pada bagian saran, diharapkan pengembang berikutnya dari Skripsi ini menemukan web based yang cocok dengan Suricata sebagai IDS, IPS dan NSM