BAB V
PENUTUP

Pada bab lima ini menjelaskan kesimpulan hasil penelitian dari rumusan masalah pada bab satu, dengan penjelasan dari bab empat. Serta memberikan penjelasan untuk penelitian selanjutnya sebagai saran.

5.1. Kesimpulan

Kesimpulan pada penelitian ini menjelaskan *Intrusion Detection System Snort* dan *Cowrie* dari poin-poin dari rumusan masalah yaitu:

1. Sistem keamanan *snort* dan *cowrie* dapat melindungi *VPS server*, *snort* dapat mendeteksi serangan dengan membandingkan paket yang melewati jaringan server dengan *ruleset snort* dan tercatat pada log. *Cowrie* menjadi server palsu dengan *default port ssh*, dan *port ssh* pada server asli diubah dan disembunyikan. *Cowrie* akan menjadi server *dummy* dari server asli sehingga semua percobaan serangan dapat tercatat pada log. *Snort* dan *Cowrie* terintegrasi dengan *splunk* sehingga log dapat dibaca dengan mudah untuk melihat bila ada serangan.
2. Hasil pengujian *Snort* dan *Cowrie* dari *serangan port scanning, brute force,* dan *DDoS.* Pengujian serangan *port scanning* pada *snort* dapat mendeteksi dari dua metode *Connect Scan* dan *SYN Scan*, dengan *Connect Scan snort* dapat mendeteksi adanya *port scan* sedangkan *SYN Scan* cuman terdeteksi adanya paket *icmp(ping)* dari *NMAP*. *Cowrie* dalam *mendeteksi port scanning* cuman terdeteksi dari *Connect Scan*, sedangkan *SYN scan* tidak terdeteksi. Pengujian serangan *brute force, Cowrie* dapat mencatat semua percobaan serangan, sedangkan *snort* mendeteksi adanya koneksi ke *ssh*. Pengujian serangan *DDoS*, dilakukan dengan dua pengujian serangan ke *port 22 ssh* dan *port 443 HTTPS*. *Snort* dapat mendeteksi adanya banyak permintaan koneksi ke *port 22* dan *port 443*, sedangkan *Cowrie* cuman mendeteksi serangan ke *port 22*.

3. Hasil pengujian CIA Triad sistem keamanan snort dan cowrie, dapat memenuhi tiga aspek dari Confidentiality, Integrity, dan Availability. Akan tetapi ada beberapa yang harus di evaluasi pada snort dan cowrie, salah satunya ada kekurangan pada Availability. Penggunaan resource cowrie saat di serang dengan serangan yang berat sangat tinggi yang dapat menggagu server, dan penggunaan Splunk untuk monitoring saat mengolah data log lumayan tinggi. Ada beberapa solusi dengan cpulimit dan sistem monitoring SIEM splunk diganti dengan graylog atau yang berbasis cloud.

5.2. Saran

Ada beberapa harapan untuk penelitian selanjutnya, karena ada kekurangan pada penelitian ini sebagai berikut:

1. Menambahkan plugin hyperscan pada Snort3 untuk meningkatkan performa dalam bekerja. Akan tetapi, karena pada penelitian ini menggunakan infrastruktur VPS yang berbasis virtual environtment, tidak dapat menggunakan plugin hyperscan karena harus ada integrasi langsung dari CPU intel.
2. Menggunakan SIEM selain Splunk salah satu graylog atau dengan SIEM yang berbasis Cloud, Karena penggunaan Splunk membutuhkan resource hardware yang tinggi untuk berjalan.
3. Menambahkan otomatis update untuk rule dan ip list, dengan skrip systemD. Supaya rule snort dan ip list mendapat update, sehingga snort dapat mengatasi serangan-serangan terbaru.