ABSTRAK

IMPLEMENTASI *INTRUSION DETECTION AND PREVENTION SYSTEM* MENGGUNAKAN SURICATA, BARNYARD2 DAN SNORBY PADA LINUX UBUNTU DI DISKOMINFO KAB. GARUT

Oleh :

HARLIN CAHYA TELAUMBANUA
10115165

Keamanan jaringan adalah aktivitas mencegah dan melindungi data dan informasi di dalam sistem jaringan. yang biasanya ada dalam sebuah korporasi, dari gangguan yang tidak sah atau bukan bagian dari pengakses info atau data yang sah. Mencakup teknologi, piranti, dan proses untuk mengamankan semua yang ada di dalam sistem jaringan. Penelitian ini menggunakan Suricata, Barnyard2 dan Snorby pada sistem yang dibangun, bentuk sistem yang dibangun berupa IDPS *(Intrusion Detection And Prevention System)* yang mana dapat mendeteksi dan mencegah terjadinya serangan yang ditujukan kepada server jaringan. Suricata, Barnyard2 dan Snorby pada dasarnya adalah *tools open source* yang dapat digunakan secara bebas antar pengguna komunitas yang mempunyai tujuan untuk melindungi server jaringan. Pada penelitian sebelumya yang membahas mengenai Implementasi *Network Intrusion Detection Systen* suricata dapat mendeteksi setiap serangan yang ditujukan kepada server dengan pengecekan kepada setiap *rules*. Tujuan dari penelitian ini sendiri adalah untuk mendeteksi serangan yang ditujukan kepada server jaringan yang telah dibangun serta memblok serangan yang ditujukan kepada server. Pada penelitian ini terdapat beberapa tahapan, yaitu *planning* yang meliputi pengumpulan informasi perusahaan yang menjadi target, *discovery* yang meliputi pengamatan terhadap perusahaan yang menjadi target, *attack* yang meliputi pencarian celah keamanan yang telah dilakukan pada *planning* dan *discovery* dan *reporting* yang meliputi informasi yang telah didapat pada tahap sebelumnya. Adapun proses pengujian sistem yang telah dibangun meliputi pengujian DOS *(Denial Of Service)* dan *arp spoofing*. Berdasarkan hasil pengujian dengan menggunakan metode *DOS* dan *arp spoofing* didapat suricata dapat mendeteksi serangan yang telah dilakukan, barnyard2 dapat menerjemahkan *log* dari suricara dan memberikan data tersebut kepada snorby. Dan snorby dapat menampilkan serangan yang telah dilakukan di antarmuka *interface*.

Kata Kunci: IDPS, Suricata, Barnyard2, Snorby.