BAB 1
PENDAHULUAN

1.1 Latar Belakang

Pada tahun 1966, sebuah proyek bernama *Advanced Research Projects Agency Network* (ARPANET) dimulai. ARPANET adalah proyek yang dimaksudkan untuk memungkinkan komputer agar dapat diakses dari jarak jauh dan agar komputer dapat saling berkomunikasi. Proyek inilah yang menjadi cikal bakal internet yang sering digunakan saat ini. Keberadaan internet sendiri selain untuk akses komputer jarak jauh, juga membuka kemungkinan untuk melakukan pembagian sumber daya, salah satu sumber daya yang sering dibagi-bagi adalah printer.

Printer pada dasarnya adalah sebuah alat yang berfungsi untuk mencetak *file*. Karena fungsi yang mudah ini, printer sering dipandang sebelah mata oleh masyarakat. Seiring berjalannya waktu, printer-printer terbaru dibuat agar dapat mengakses sebuah jaringan dengan alasan untuk berbagi sumber daya pada satu jaringan kecil yang disebut *Local Area Network* (LAN). Printer yang terkoneksi ke dalam sebuah jaringan ini yang akan disebut sebagai *network printer*. Selain memudahkan organisasi untuk berbagi sumber daya, dikarenakan terkoneksi ke dalam jaringan, maka keamanan dari sebuah *network printer* perlu dipertimbangkan.

Pada masa pandemik COVID-19 ini, bisnis *digital print* akan semakin marak sehingga penggunaan *printer* semakin bertambah banyak (Andriansyah, 2020, h.1). Karena hal tersebut, tentu ketersediaan serta keamanan dari *network printer* sangatlah penting karena alat itu sendiri akan sangat sering digunakan.

Pada akhir tahun 2018, lebih dari 50.000 *printer* terkena serangan siber yang memaksa printer mencetak pesan yang merupakan *spam* yang berisi ajakan untuk melakukan *subscribe to PewDiePie* (Brewster, 2018, h.1). Hal ini terjadi dikarenakan pihak yang tidak memiliki wewenang mendapatkan akses ke sebuah *network printer*. Jika misalkan pesan *spam* tersebut berubah menjadi pesan untuk kegiatan politik dan dalam skala besar, maka dapat menimbulkan masalah

tingkat nasional. Oleh karenanya perlu adanya sebuah sistem berfungsi untuk melakukan kendali terhadap akses-akses yang masuk pada sebuah *network printer*.

Berdasarkan latar belakang di atas, Penulis ingin membuat sebuah sistem yang dapat membatasi akses, atau biasa disebut *access control* yang digunakan untuk mencegah akses tidak berwenang ke sebuah *network printer* dengan cara memisahkan jaringan antara komputer dengan *network printer* serta mengimplementasikan *firewall* dengan teknologi *intrusion detection system* dan *intrusion prevention system* dengan harapan kedua teknologi tersebut akan dapat melakukan *filter* terhadap paket yang saling terkomunikasi antara komputer dengan *printer* sehingga akses ke *printer* beserta isi dari paket yang diperbolehkan untuk komunikasi menjadi sangat terbatas. Karena hal tersebut, penulis akan memberi judul "Pencegahan Eksploitasi Pada Jaringan Network Printer Dengan Signature Based IDS/IPS Suricata Pada Pfsense."

1.2 Rumusan Masalah

Rumusan masalah yang dapat dituliskan dari uraian di atas antara lain:

a. Apakah dampak yang ditimbulkan apabila perangkat *network printer* berhasil diretas oleh pihak tidak bertanggung jawab?
b. Apakah tindak peretasan dari *network printer* dapat dicegah dengan menggunakan kombinasi *firewall* dan *intrusion detection system* bersamaan dengan *intrusion prevention system*?

1.3 Tujuan Penelitian

Tujuan yang diharapkan dari penjabaran rumusan masalah adalah:

a. Memastikan adanya ketersediaan layanan, kerahasiaan data dan informasi, serta integritas dari data pada sebuah *network printer* kemudian juga membatasi perangkat dari akses pihak yang tidak berwenang.

1.4 Manfaat Penelitian

Merujuk kepada paparan rumusan masalah dan tujuan penelitian di atas, manfaat yang diperoleh dari penelitian ini antara lain:

a. Meningkatkan adanya ketersediaan layanan, kerahasiaan data dan informasi, serta integritas data dari sebuah *printer* yang terkoneksi ke sebuah jaringan komputer.
b. Menjadi tulisan rujukan untuk penelitian yang terkait dengan topik pembahasan yang sama seperti penelitian ini.

1.5 Ruang Lingkup

Ruang lingkup dari penelitian ini adalah:

a. Penelitian hanya menangkap dan menganalisis paket yang bersifat TCP yang terkirim menuju port pada *network printer* yang terbuka.
b. Penelitian hanya melakukan pembatasan akses dengan menggunakan *firewall* pfSense.
c. *Printer* yang digunakan adalah *printer* Canon imageRunner ADV 4035.

1.6 Luaran Yang Diharapkan

Luaran yang diharapkan adalah sistem dapat membatasi akses dari komputer dalam jaringan berbeda ke sebuah *printer*.

1.7 Sistematika Penulisan

Penulisan laporan ini berdasarkan sistematika sebagai berikut:

a. BAB 1 Pendahuluan

Bab ini akan membahas tentang latar belakang dalam penulisan ini, serta rumusan masalah, tujuan yang ingin dicapai, manfaat penelitian, ruang lingkup, serta luaran yang diharapkan dari adanya penelitian ini.

b. BAB 2 Landasan Teori

Bab ini akan memaparkan teori-teori terkait yang mendasari penelitian ini.

c. BAB 3 Metodologi Penelitian

Bab ini akan membahas tentang metode serta kerangka berpikir dan jadwal kegiatan yang dilakukan selama penelitian.

d. BAB 4 Hasil dan Pembahasan

Bab ini membahas tentang isi dari kegiatan penelitian yang dilakukan. Hal ini termasuk konfigurasi sistem serta pengujian sistem begitupula dengan hasil yang didapatkan dari penelitian.

e. BAB 5 Kesimpulan dan Saran

Bab ini memaparkan kesimpulan yang didapat dari penelitian yang dilakukan, baik temuan yang diharapkan maupun yang termasuk temuan baru bagi penulis. Bab ini juga berisikan saran dari penulis untuk penelitian serupa yang akan datang.

f. Daftar Pustaka