BAB 5
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan penelitian yang dilakukan, terkait pencegahan eksploitasi pada jaringan network *printer* dengan bantuan *firewall* pfSense dan IDS/IPS Suricata, dapat disimpulkan hasil sebagai berikut:

1. Dampak yang ditimbulkan apabila sebuah *network printer* berhasil diretas adalah hilangnya layanan *print* dari *network printer*, kemudian juga bocornya kerahasiaan informasi baik konfigurasi maupun data yang tersimpan pada *network printer*, serta rusaknya integritas atau keaslian data yang tersimpan pada *network printer*.
2. Peretasan pada *network printer* dapat dicegah dengan menggunakan kombinasi *firewall* berserta *intrusion detection system* dan *intrusion prevention system.* Adapun lengkapnya, dapat dilihat dari poin-poin berikut ini:
    a. Ketersediaan layanan dari *network printer* dapat sedikit ditingkatkan dengan bukti yaitu didapatkan hasil bahwa *firewall* pfSense dengan IDS/IPS Suricata dapat membatasi akses serta perintah paket yang dapat membuat perangkat menjadi *error*. Namun pada penelitian ini, permasalahan untuk memitigasi dampak terhadap ketersediaan layanan *printer* secara menyeluruh masih belum terangkat, terutama untuk serangan *denial-of-service* melalui *packet flooding*. Oleh karena itu, *printer* masih dikatakan rentan terhadap serangan yang berkaitan dengan ketersediaan layanan.
    b. Kerahasiaan informasi dari *network printer* dapat ditingkatkan dengan bukti yaitu didapatkan hasil bahwa *firewall* pfSense dengan IDS/IPS Suricata dapat membatasi akses serta perintah paket yang dapat membocorkan *password printer*. Namun untuk kerahasiaan data yang tersimpan pada *printer* tidak dapat diobservasi, hal ini terlihat pada perintah "*get*" yang tidak memunculkan hasil yang diinginkan.
    c. Integritas data pada *network printer* dapat ditingkatkan dengan bukti yaitu didapatkan hasil bahwa *firewall* pfSense dengan IDS/IPS Suricata dapat

membatasi akses serta perintah paket yang dapat terkirim dari perangkat asing yang seolah-olah berperan sebagai *root*.

5.2 Saran

Adapun saran yang dapat diberikan untuk penelitian selanjutnya adalah sebagai berikut:

1. Menggunakan kombinasi *firewall* yang berbeda serta IDS/IPS yang berbeda.
2. Menggunakan *printer* uji yang berbeda, dan sangat disarankan untuk menggunakan minimal dua perangkat *network printer* sehingga segala perbedaan hasil pada eksploitasi dan pengamanan dapat diperhatikan dengan lebih jelas.
3. Melakukan enkripsi terhadap paket yang terkirim untuk mengetahui apakah paket dapat lolos *firewall* dan IDS/IPS dan apakah printer masih dapat mengetahui isi dari paket terkirim.
4. Mencoba menggunakan sebuah *print server* yang berfungsi untuk menampung *print job* sebelum dikirimkan ke *network printer* atau menggunakan sebuah *load balancer* apabila terdapat dua atau lebih *network printer* untuk membagi *print job* secara merata sehingga permasalahan mengenai serangan *denial-of-service* dapat dimitigasi.