PENCEGAHAN EKSPLOITASI PADA JARINGAN *NETWORK PRINTER* DENGAN *SIGNATURE BASED* IDS/IPS SURICATA PADA PFSENSE

Fajar Subkhi Sulaiman

ABSTRAK

Pada akhir tahun 2018, lebih dari 50.000 printer terkena serangan siber yang memaksa printer mencetak pesan yang merupakan *spam*. Jika misalkan pesan *spam* tersebut berubah menjadi pesan untuk kegiatan politik dan dalam skala besar, maka dapat menimbulkan masalah tingkat nasional. Berdasarkan hal tersebut, muncul sebuah masalah yaitu apakah dampak yang terjadi apabila *network printer* berhasil diretas dan apakah tindak peretasan dapat dicegah dengan kombinasi *firewall* dengan IDS/IPS Suricata. Penelitian hanya membahas paket komunikasi TCP, pembatasan akses dengan menggunakan *firewall* pfSense bersamaan dengan IDS/IPS Suricata dan *printer* uji yang digunakan adalah printer model Canon imageRunner ADV 4035. Solusi yang ditawarkan adalah dengan memisahkan jaringan kedalam dua *network* yang berbeda dan meletakkan *firewall* di antara jaringan pertama dengan jaringan kedua dan melakukan konfigurasi terhadap *firewall* tersebut, setelah itu akan dilakukan konfigurasi pada IDS/IPS agar dapat mendeteksi paket yang berbahaya. Luaran yang didapatkan dari penelitian ini adalah sistem dapat membatasi akses dan melakukan filter paket dari komputer dalam jaringan berbeda ke *network printer* yang mana dapat meningkatkan ketersediaan layanan, kerahasiaan informasi, serta integritas data pada *network printer*.

Kata Kunci: *Firewall, Network Printer, Packet Filter, IDS, IPS*

EXPLOITATION PREVENTION ON NETWORK PRINTER WITH SIGNATURE BASED IDS/IPS SURICATA ON PFSENSE

Fajar Subkhi Sulaiman

ABSTRACT

In late 2018, more than 50,000 printers were exposed to a cyberattack that forced them to print spam messages. Were the spam message turned into a message for large-scale political activities, it can cause problems at the national level. Based on this, two problem arises, namely what is the impact of hacked printers. In addition, whether a combination of a firewall with Suricata IDS/IPS can prevent hacking on printers. The research only discusses TCP communication packets, access restrictions using the pfSense firewall along with Suricata IDS/IPS, and Canon imageRunner ADV 4035 as the test printer. The solution offered is to separate the network into two different networks, put a firewall between the networks and configure the firewall, and then the IDS/IPS configuration will be carried out so that it can detect malicious packets. The output obtained from this research is a system that can limit access and perform packet filters from computers on different networks to network printers, which can increase service availability, information confidentiality, and data integrity on network printers.

Keywords: *Firewall, Network Printer, Packet Filter, IDS, IPS*