



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

SKRIPSI

FAJAR SUBKHI SULAIMAN

1710511036

**PROGRAM STUDI INFORMATIKA, PROGRAM SARJANA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA
2021**



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

SKRIPSI

**Diajukan Sebagai Salah Satu Syarat untuk Memperoleh Gelar Sarjana
Komputer**

FAJAR SUBKHI SULAIMAN

1710511036

**PROGRAM STUDI INFORMATIKA, PROGRAM SARJANA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA
2021**

PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri, dan semua sumber yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : Fajar Subkhi Sulaiman

NIM : 1710511036

Tanggal : 28 Juni 2021

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 28 Juni 2021

Yang Menyatakan,



(Fajar Subkhi Sulaiman)

LEMBAR PENGESAHAN

Dengan ini dinyatakan bahwa Skripsi berikut:

Nama : Fajar Subkhi Sulaiman
NIM : 1710511036
Program Studi : Informatika
Judul Skripsi : Pencegahan Eksplorasi Pada Jaringan Network Printer
Dengan Signature Based IDS/IPS Suricata Pada Pfsense

Telah berhasil dipertahankan di hadapan Tim Pengaji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi S1 Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.

Iin Ernawati, S.Kom., M.Si.

Pengaji I

I Wayan Widi P, S.Kom., MTI.

Pengaji II

Henki Bayu Seta, S.Kom., MTI.

Pembimbing I

Noor Falih, S.Kom., M.T.

Pembimbing II



Dr. Ernatita, M.Kom.

Dekan

Yuni Widiastiwi, S.Kom., Msi.

Ketua Program Studi

Ditetapkan di : Jakarta

Tanggal Pengesahan : 14 Juli 2021



PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademik Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertanda tangan dibawah ini:

Nama : Fajar Subkhi Sulaiman
NIM : 1710511036
Fakultas : Ilmu Komputer
Program Studi : Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti NonEkslusif (Non-Exclusive Royalty Free Right) atas karya ilmiah saya yang berjudul:

Pencegahan Eksplorasi Pada Jaringan Network Printer Dengan Signature Based IDS/IPS Suricata Pada PfSense

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan Skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta
Pada Tanggal : 28 Juni 2021
Yang Menyatakan,



(Fajar Subkhi Sulaiman)

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*

KATA PENGANTAR

Penulis ucapkan rasa puji dan syukur kehadirat Allah S.W.T karena atas berkat rahmat dan hidayah-Nya, penulis dapat menyelesaikan skripsi di pertengahan masa pandemi COVID-19 ini. Adapun judul untuk skripsi ini adalah:

Pencegahan Eksplorasi Pada Jaringan Network Printer Dengan Signature Based IDS/IPS Suricata Pada PfSense

Selanjutnya ucapan terima kasih yang sebesar-besarnya juga ingin penulis berikan kepada pihak-pihak yang selalu sabar untuk menemani, membimbing, serta memberi saran terbaik yang mana tanpa kehadiran mereka, penulisan naskah skripsi ini tidak akan pernah selesai seperti sekarang ini. Adapun pihak terkait antara lain:

1. Kedua orang tua yang telah memberi dukungan dan semangat serta mendoakan penulis agar dapat menyelesaikan naskah skripsi ini tanpa kendala.
2. Bapak Henki Bayu Seta, S.Kom., MTI selaku dosen pembimbing satu yang membimbing penulis dalam menyusun naskah skripsi ini.
3. Bapak Noor Falih, S.Kom., M.T. selaku dosen pembimbing dua yang juga telah membimbing dalam penulisan naskah skripsi ini.
4. Bapak I Wayan Widi P., S.Kom., MTI selaku dosen penguji yang telah memberi arahan dan saran komprehensif.
5. Ibu Iin Ernawati, S.Kom., M.Si selaku dosen penguji yang telah memberi arahan dan saran komprehensif.
6. Bapak/Ibu dosen Informatika Universitas Pembangunan Nasional Veteran Jakarta yang telah memberi ilmu yang banyak dan bermanfaat.
7. Teman-teman semua di Tim NaQoS yang telah memberi dukungan moral serta menyediakan waktu untuk melakukan diskusi tentang tugas akhir.

Kemudian penulis juga menyadari bahwa penyusunan skripsi ini masih jauh dari kata sempurna, namun penulis berharap agar pihak yang membaca naskah ini

mendapatkan ilmu yang dapat digunakan kelak. Dan penulis juga berharap atas kritik dan saran yang konstruktif dari pembaca.

Akhir kata, semoga Allah S.W.T memberi balasan yang berlipat ganda atas kebaikan dan jasa kepada semua pihak yang turut membantu penyelesaian naskah skripsi ini. Semoga tujuan daripada penulisan skripsi ini dapat tercapai sesuai dengan harapan.

DAFTAR ISI

PERNYATAAN ORISINALITAS.....	ii
LEMBAR PENGESAHAN	iii
PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI.....	iv
ABSTRAK.....	v
ABSTRACT.....	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	ix
DAFTAR GAMBAR.....	xii
DAFTAR TABEL	xiv
DAFTAR LAMPIRAN	xv
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah	2
1.3 Tujuan Penelitian.....	2
1.4 Manfaat Penelitian.....	2
1.5 Ruang Lingkup.....	3
1.6 Luaran Yang Diharapkan	3
1.7 Sistematika Penulisan	3
BAB 2 LANDASAN TEORI	5
2.1 Jaringan Komputer	5
2.1.1 Jaringan <i>Local Area Network (LAN)</i>	5
2.1.2 Internet.....	5
2.2 <i>Network Protocol</i>.....	5
2.2.1. Open System Interconnection (OSI) Model	5
2.2.2. Simple Network Management Protocol (SNMP).....	8
2.3 MAC Address	8
2.4 IP Address	9
2.5 Port	9
2.6 Multifunctional Device	9
2.7 Printer	9

2.7.1	<i>Printer Job Language (PDL)</i>	10
2.7.2	<i>Page Description Language (PDL)</i>	10
2.7.3	<i>Port RAW 9100</i>	10
2.8.	Keamanan Jaringan	10
2.8.1	<i>Confidentiality</i>	10
2.8.2	<i>Integrity</i>	11
2.8.3	<i>Availability</i>	11
2.9.	Serangan pada Network Printer	11
2.9.1	<i>Denial of Service</i>	11
2.9.2	<i>Privilege Escalation</i>	11
2.9.3	<i>Print Job Manipulation</i>	11
2.9.4	<i>Information Disclosure</i>	12
2.9.5	<i>Remote Code Execution</i>	13
2.10.	Firewall	13
2.11.	Access Control List (ACL)	14
2.12.	PfSense	14
2.13.	Suricata	14
2.14.	Wireshark	15
2.15.	Metasploit Framework	15
2.16.	Nmap	16
2.17.	VirtualBox	17
2.18.	Printer Exploitation Toolkit (PRET)	17
2.19.	Penelitian Terkait	18
BAB 3 METODOLOGI PENELITIAN	21
3.1.	Kerangka Pikir	21
3.1.1	Identifikasi Masalah	21
3.1.2	Studi Literatur	22
3.1.3	Konfigurasi Sistem	22
3.1.4	Pengujian Sistem	24
3.1.5	Dokumentasi	25
3.2.	Alat Bantu Penelitian	25
3.2.1.	Alat bantu perangkat keras meliputi:	25
3.2.2.	Alat bantu perangkat lunak meliputi:	25

3.3. Jadwal Penelitian	26
BAB 4 HASIL DAN PEMBAHASAN.....	27
 4.1 Identifikasi Masalah	27
4.1.1 Common Vulnerabilities and Exposures (CVE)	28
4.1.2 Uji Port Scanning Nmap.....	28
4.1.3 Uji Coba PostScript Interpreter	30
4.1.4 Uji Coba Printer Job Language (PJV)	31
4.1.5 Uji Coba Printer Command Language (PCL)	33
4.1.6 Printer Uji, Interpreter, dan PRET.....	37
4.1.8 Uji Coba LPD	39
4.1.9 Password Extraction Pada port 8000	40
 4.2 Konfigurasi Sistem.....	41
4.2.1 Cara Kerja pfSense.....	42
4.2.2 Konfigurasi PfSense	44
4.2.3 Cara Kerja Suricata.....	45
4.2.4 Konfigurasi Suricata.....	45
 4.3 Pengujian Sistem.....	51
4.3.1 Uji Pengiriman Paket.....	52
4.3.2 Konfigurasi Ulang dan Uji Pengiriman Paket.....	54
4.3.3 Drop Paket Terkirim	57
4.3.4 Uji Internet	59
BAB 5 KESIMPULAN DAN SARAN.....	61
 5.1 Kesimpulan.....	61
 5.2 Saran	62
DAFTAR PUSTAKA.....	63
DAFTAR RIWAYAT HIDUP	66
LAMPIRAN.....	67

DAFTAR GAMBAR

Gambar 1 Format <i>Header</i> saat Komunikasi TCP	6
Gambar 2 Format <i>Header</i> saat Komunikasi UDP	7
Gambar 3 Komponen <i>Printer</i>	10
Gambar 4 PostScript <i>Dictionary Stack</i>	12
Gambar 5 Cara Kerja <i>Filter Paket</i> pada <i>Firewall</i>	14
Gambar 6 Cara Kerja Metasploit	15
Gambar 7 Cara Kerja Nmap	16
Gambar 8 Arsitektur dan Cara Kerja PRET	17
Gambar 9 Kerangka pikir.....	21
Gambar 10 Topologi saat ini.....	23
Gambar 11 Rancangan topologi	23
Gambar 12 Alur Konfigurasi Sistem	24
Gambar 13 Alur Pengujian Sistem.....	24
Gambar 14 Komponen <i>Printer</i>	27
Gambar 15 Perintah Port Scanning dengan Nmap	29
Gambar 16 Hasil Scan Nmap – Terminal.....	29
Gambar 17 Hasil Scan Nmap – HTML	30
Gambar 18 Uji Postscript.....	31
Gambar 19 Uji Coba PJL.....	31
Gambar 20 Uji PJL PrintEnv Awal	32
Gambar 21 Uji PJL Ubah Konfigurasi.....	32
Gambar 22 Uji PJL PrintEnv Setelah Ubah Konfigurasi.....	32
Gambar 23 Uji PJL Put.....	33
Gambar 24 Uji PCL.....	33
Gambar 25 Uji PCL Informasi dan Ubah Konfigurasi.....	34
Gambar 26 Uji PCL Put	35
Gambar 27 Uji PCL Get	35
Gambar 28 Uji PCL Delete	36
Gambar 29 Uji Print	38
Gambar 30 Hasil Uji Print pada <i>Printer</i> Uji	38
Gambar 31 Pesan <i>Error</i> pada <i>Printer</i>	39
Gambar 32 Uji LPD	40
Gambar 33 Hasil Uji LPD	40
Gambar 34 Password Extract	41
Gambar 35 Topologi Pengujian.....	42
Gambar 36 Cara Kerja pfSense	43
Gambar 37 Konfigurasi interface pada pfSense	44
Gambar 38 Instalasi Suricata pada pfSense.....	44
Gambar 39 Ruleset pada Suricata	46
Gambar 40 Port Terbuka pada <i>Printer</i> Uji.....	46

Gambar 41 <i>Rules</i> ETOOpen - Exploit	47
Gambar 42 Beberapa <i>Rules</i> ETOOpen Exploit yang Diaktifkan.....	47
Gambar 43 <i>Rules</i> ETOOpen - Malware.....	48
Gambar 44 <i>Rules</i> ETOOpen - Policy	48
Gambar 45 Beberapa <i>Rules</i> ETOOpen Policy yang Diaktifkan.....	48
Gambar 46 <i>Rules</i> ETOOpen - Scan.....	49
Gambar 47 <i>Rules</i> Scan yang Diaktifkan.....	49
Gambar 48 <i>Rules</i> ETOOpen - WebServer dan <i>Rules</i> GPLv2 Community	50
Gambar 49 Pengaktifan Suricata	50
Gambar 50 Alur Pengujian Sistem.....	51
Gambar 51 Uji Kirim Paket RAW 1.....	52
Gambar 52 Uji Kirim Paket RAW 2.....	52
Gambar 53 Uji Kirim Paket LPD.....	53
Gambar 54 Uji Kirim Paket <i>Malicious</i> dengan Metasploit.....	53
Gambar 55 Uji Kirim Paket <i>Malicious</i> dengan NMAP.....	54
Gambar 56 Isi Paket RAW yang Terkirim	55
Gambar 57 Isi Paket LPD	55
Gambar 58 Mendefinisikan <i>Rules</i> Baru Sesuai Isi Paket.....	56
Gambar 59 Hasil Uji dengan <i>Custom Rules</i>	57
Gambar 60 <i>Drop</i> Paket RAW.....	57
Gambar 61 <i>Drop</i> Paket LPD.....	58
Gambar 62 <i>Drop</i> Paket Metasploit.....	58
Gambar 63 <i>Drop</i> Paket NMAP.....	59
Gambar 64 <i>Blocked IP List</i>	59
Gambar 65 Uji Internet – Ping Situs.....	60
Gambar 66 Traceroute untuk Membuktikan Bahwa Paket Melewati <i>Firewall</i>	60

DAFTAR TABEL

Tabel 1 Tipe Protokol SNMP	8
Tabel 2 Penelitian Terkait.....	19
Tabel 3 Jadwal Kegiatan Penelitian	26
Tabel 4 Uji <i>Interpreter Printer</i> Uji dengan PRET	37

DAFTAR LAMPIRAN

Lampiran 1 Skor Turnitin	68
---------------------------------------	-----------