

**IMPLEMENTASI INTRUSION DETECTION PREVENTION
SYSTEM (IDPS) DALAM JARINGAN WIFI MENGGUNAKAN
SURICATA PADA PFSENSE**

SKRIPSI



Oleh :

WAHYU FERDYANTO

NPM. 1234010143

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN"
JAWA TIMUR**

2019

HALAMAN PENGESAHAN

Judul : Implementasi Intrusion Detection Prevention System (IDPS) dalam Jaringan Wifi menggunakan Suricata pada PfSense

Oleh : Wahyu Ferdyanto

NPM : 1234010143

Telah Diseminarkan Dalam Ujian Skripsi Pada :

Hari Jum'at Tanggal 17 Mei 2019

Menyetujui

Dosen Pembimbing 1



Henni Endah Wahanani, S.T., M.Kom.

NPT. 3 7809 13 0348 1

Dosen Pembimbing 2



Wahyu S.J. Saputra, S.Kom., M.Kom.

NPT. 3 8608 10 0295 1

Dosen Penguji 1



Intan Yuniar P., S.Kom., Mc.

NPT. 3 8006 04 0198 1

Dosen Penguji 2



Eva Yulia P., S.Kom., M.Kom.

NPT. 3 8907 13 0346 1

Dosen Penguji 3



Firza Prima Aditiawan, S.Kom., MTI.

NPT. 3 8605 13 0344 1

Mengetahui

Dekan

Fakultas Ilmu Komputer



Dr. Ir. Ni Ketut Sari, MT.

NIP. 19650731 199203 2 001.

Koordinator Program Studi
Teknik Informatika



Budi Nugroho, S.Kom., M.Kom.

NPT. 3 8009 05 0205 1

IMPLEMENTASI INTRUSION DETECTION PREVENTION SYSTEM (IDPS) DALAM JARINGAN WIFI MENGGUNAKAN SURICATA PADA PFSense

Nama Mahasiswa : Wahyu Ferdyanto
NPM : 1234010143
Program Studi : Teknik Informatika
Dosen Pembimbing 1 : Henni Endah Wahanani, ST, M.Kom.
Dosen Pembimbing 2 : Wahyu SJ. Saputra, S.Kom, M.Kom.

ABSTRAK

Keamanan jaringan komputer sebagai bagian dari sebuah sistem menjadi sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunaannya. Dalam beberapa tahun terakhir ini, wifi telah menarik banyak perhatian, terutama untuk para pengguna internet, dikarenakan kemudahan konfigurasi dan kemudahan akses yang disediakan.

Pada penelitian ini dilakukan serangan untuk merusak jaringan WiFi, diantaranya SYN Flood, ICMP Flood. Serangan tersebut dilakukan secara berulang - ulang keseluruh device yang terhubung pada jaringan tersebut. Tools yang digunakan untuk mendeteksi dan mencegah serangan serangan tersebut yaitu Suricata pada PfSense. Suricata merupakan Tools yang dapat berjalan secara Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS). Dan sistem operasi yang digunakan adalah PfSense.

Hasil dari penelitian ini menyatakan bahwa agar celah keamanan pada jaringan wifi bisa diatasi maka dibangunlah suatu sistem terintegrasi yang dapat menangani masalah keamanan pada jaringan wifi, dengan membangun sistem intrusion detection prevention system (IDPS) berbasis Suricata dengan memanfaatkan open source firewall yaitu *pfsense* yang berbasis *freebsd*.

Kata kunci : *Suricata, IDS, IPS, Wifi, SYN Flood, ICMP Flood, PfSense*

SURAT PERNYATAAN ANTI PLAGIAT

Saya, mahasiswa Teknik Informatika UPN "Veteran" Jawa Timur, yang bertandatangan di bawah ini

Nama : WAHYU FERDYANTO

NPM : 1234010143

Menyatakan bahwa Judul Skripsi/ Tugas Akhir yang Saya ajukan dan akan dikerjakan, yang berjudul

**IMPLEMENTASI INTRUSION DETECTION PREVENTION SYSTEM (IDPS) DALAM
JARINGAN WIFI MENGGUNAKAN SURICATA PADA PFSENSE**

Bukan merupakan plagiat dari Skripsi/ Tugas Akhir/ Penelitian orang lain dan juga bukan merupakan produk dan atau *software* yang saya beli dari pihak lain. Saya juga menyatakan bahwa Skripsi/ Tugas Akhir ini adalah pekerjaan Saya sendiri, kecuali yang dinyatakan dalam Daftar Pustaka dan tidak pernah diajukan untuk syarat memperoleh gelar di UPN "Veteran" Jawa Timur maupun di institusi pendidikan lain.

Jika ternyata di kemudian hari pernyataan ini terbukti tidak benar, maka Saya siap menerima segala konsekuensinya.

Surabaya, 27 Mei 2019

Hormat Saya,



WAHYU FERDYANTO

NPM. 1234010143

KATA PENGANTAR

Syukur Alhamdulillah kami panjatkan kehadiran Allah SWT yang telah memberikan rahmat serta hidayah-Nya sehingga penyusunan Laporan Skripsi ini dapat diselesaikan.

Laporan Skripsi ini disusun untuk memenuhi syarat dalam memperoleh gelar sarjana komputer, program studi Teknik Informatika. Judul yang diambil dalam penulisan Skripsi ini adalah :

“IMPLEMENTASI INTRUSION DETECTION PREVENTION SYSTEM (IDPS) DALAM JARINGAN WIFI MENGGUNAKAN SURICATA PADA PFSense”

Penulis menyadari bahwa penulisan Laporan Skripsi ini masih belum sempurna. Oleh karena itu, saran dan kritik yang membangun akan penulis terima dengan senang hati.

Akhir kata semoga Laporan Skripsi ini dapat memberikan manfaat bagi para mahasiswa khususnya dan pengetahuan pada umumnya.

Surabaya, 17 Mei 2019

Penulis

DAFTAR ISI

ABSTRAK	i
KATA PENGANTAR	ii
UCAPAN TERIMA KASIH	ii
DAFTAR ISI	v
DAFTAR GAMBAR	ix
BAB I PENDAHULUAN	1
1.1. Latar Belakang.....	1
1.2. Perumusan Masalah	4
1.3. Batasan Masalah	4
1.4. Tujuan	5
1.5. Manfaat	5
1.6. Sistematika Penulisan	6
BAB II TINJAUAN PUSTAKA	8
2.1. Penelitian Terdahulu	8
2.2. Dasar Teori.....	9
2.2.1. Intrusion Detection System (IDS)	9
2.2.2. Intrusion Prevention System (IPS).....	12
2.2.2.1. Signature Based Intrusion Detection System.....	14
2.2.2.2. Anomaly Based Intrusion Detection System	14

2.2.2.3. Host Based Intrusion Prevention System (HIPS).....	15
2.2.2.4. Network Based Intrusion Prevention System (NIPS)	15
2.2.3. WiFi Network.....	15
2.2.4. Suricata.....	17
2.2.5. PfSense	19
2.2.6. SYN Flood.....	21
2.2.7. Ping Attack.....	25
2.2.8. Mikrotik RouterBoard	26
2.2.9. WinBox	26
BAB III METODOLOGI PENELITIAN.....	27
3.1. Alur Penelitian	27
3.1.1. Studi Pustaka	28
3.1.2. Perancangan Sistem.....	28
3.1.3. Pengujian Sistem	28
3.1.4. Analisa Serangan	29
3.1.5. Kesimpulan.....	29
3.2. Rancangan Penelitian.....	29
3.2.1. Definisi Kebutuhan Sistem.....	29
3.2.2. Rancangan Jaringan.....	30
3.3. Skenario Uji Coba.....	31
3.3.1. Skenario Serangan SYN Flood.....	32

3.3.2.	Skenario Serangan ICMP Flood	33
3.4.	Analisa dan Pembuktian Serangan.....	34
BAB IV HASIL DAN PEMBAHASAN		38
4.1.	Instalasi Sistem	38
4.1.1.	Instalasi Pfsense.....	38
4.1.2.	Instalasi Suricata.....	46
4.2.	Konfigurasi Sistem.....	48
4.2.1.	Konfigurasi Mikrotik.....	48
4.2.2.	Konfigurasi Suricata	55
4.3.	Implementasi Serangan.....	58
4.3.1.	Serangan ICMP Flood.	59
4.3.2.	Serangan SYN Flood.	61
4.4.	Implementasi Pendeteksi dan Pencegahan.....	63
4.4.1.	Pendeteksi dan Pencegahan Serangan ICMP Flood.	63
4.4.2.	Pendeteksi dan Pencegahan Serangan SYN Flood.....	65
4.5.	Perbandingan Kinerja PfSense RouterOS dan Router PfSense	67
4.5.1.	PfSense RouterOS	67
4.5.2.	Router PfSense	69
BAB V KESIMPULAN DAN SARAN.....		71
5.1.	Kesimpulan	71
5.2.	Saran	71

DAFTAR PUSTAKA 73

DAFTAR GAMBAR

Gambar 2.1. Intrusion Detection System (IDS)	10
Gambar 2.2. Perancangan Sistem Wireless Intrusion Detection System (IDPS)..	13
Gambar 2.3. Wireless Network	17
Gambar 2.4. Desain Intrusion Prevention System (IPS) pada Suricata.....	18
Gambar 2.5. PfSense	21
Gambar 2.6. Alur Three – Way Handshake	22
Gambar 2.7. Skenario Syn Flood Attack.....	23
Gambar 3.1. Alur Rancangan Penelitian	27
Gambar 3.2. Skenario Topologi Jaringan.....	31
Gambar 3.3. Alur Serangan SYN Flood.....	32
Gambar 3.4. Alur Serangan ICMP Flood.....	33
Gambar 3.5. Alur Kerja Suricata	34
Gambar 3.6. Daftar Rules Pada Suricata	35
Gambar 3.7. Contoh Log Pada Suricata	36
Gambar 4.1. Proses Membuat guest baru pada VirtualBox	38
Gambar 4.2. Proses Mengatur memori RAM.....	39
Gambar 4.3. Proses Virtual Hard Disk	39
Gambar 4.4. Proses Mengatur memori Hardware	40
Gambar 4.5. Adapter 1 menggunakan Bridged (WAN).....	41
Gambar 4.6. Adapter 2 menggunakan Jaringan Area Network.....	41
Gambar 4.7. Proses Memasukkan Virtual Optical Disk File	42
Gambar 4.8. Tampilan layar IP Pfsense pada VirtualBox.....	43

Gambar 4.9. Proses Setting interface IP address	43
Gambar 4.10. Proses Konfigurasi LAN.....	44
Gambar 4.11. Proses Set New LAN IP Address	44
Gambar 4.12. Proses Set Subnet IP Address LAN.....	44
Gambar 4.13. Proses Set Gateway IP Address LAN.....	45
Gambar 4.14. Proses Set DHCP Server LAN	45
Gambar 4.15. Proses Set IP Range LAN.....	45
Gambar 4.16. Setting IP Address LAN	45
Gambar 4.17. Tampilan Awal PfSense	46
Gambar 4.18. Proses Instalasi Paket Suricata pada Pfsense.....	47
Gambar 4.19. Proses Download Suricata	47
Gambar 4.20. Proses Setting interface pada Mikrotik.....	48
Gambar4.21. Proses Setting IP Address LAN.....	49
Gambar 4.22. Proses Setting IP Pool LAN	50
Gambar 4.23. Proses Setting DHCP Server LAN	51
Gambar 4.24. Proses Setting IP Address Wifi.....	52
Gambar 4.25. Proses Setting IP Pool Wifi	53
Gambar 4.26. Proses Setting DHCP Server Wifi	54
Gambar 4.27. Proses Konfigurasi Global Setting.....	55
Gambar 4.28. Proses Konfigurasi General Settnng.....	55
Gambar 4.29. Proses Update Install Rule.....	56
Gambar 4.30. Proses Konfigurasi WAN Setting.....	56
Gambar 4.31. Proses Konfigurasi Alert dan Block	57
Gambar 4.32. Daftar Rules Pada Suricata	58

Gambar 4.33. Performa CPU sebelum terjadi serangan.....	59
Gambar 4.34. Perintah Serangan ICMP Flood	60
Gambar 4.35. Performa CPU setelah terjadi serangan ICMP Flood	60
Gambar 4.36. Perintah Serangan SYN Flood.....	61
Gambar 4.37. Performa CPU setelah terjadi serangan SYN Flood.....	62
Gambar 4.38. Log serangan ICMP Flood.....	64
Gambar 4.39. Log serangan SYN Flood	66
Gambar 4.40. Alert pada Suricata	68
Gambar 4.41. Perangkat keras Router PfSense	69
Gambar 4.42. Alert pada Suricata	69

UCAPAN TERIMA KASIH

Selama melaksanakan pengerjaan tugas akhir dan dalam menyelesaikan laporan skripsi ini, penulis telah banyak menerima bimbingan, pengarahan, petunjuk dan saran, serta fasilitas yang membantu hingga akhir dari penulisan laporan ini. Untuk itu penulis menyampaikan ucapan terimakasih yang sebesar-besarnya kepada :

1. Allah SWT, karena atas rahmat dan limpahan beliau penulis dapat menyelesaikan penulisa laporan tugas akhir.
2. Kedua orang tua dan keluarga yang telah memberikan doa, kasih sayang, serta semangat.
3. Ibu Dr. Ir. Ni Ketut Sari, MT selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jawa Timur.
4. Ibu Budi Nugroho ,S.Kom ,M.Kom selaku Ketua Jurusan Teknik Informatika Universitas Pembangunan Nasional “Veteran” Jawa Timur.
5. Ibu Henni Endah Wahanani, ST, M.Kom selaku Dosen Pembimbing pertama skripsi yang telah membimbing penulis selama pelaksanaan dan penyusunan laporan skripsi.
6. Bapak Wahyu SJ. Saputra, S.Kom, M.Kom selaku Dosen Pembimbing kedua skripsi yang telah membimbing penulis selama pelaksanaan dan penyusunan laporan skripsi.
7. Bapak Hendra Maulana, S.Kom selaku Koordinator Tugas Akhir / PIA Universitas Pembangunan Nasional “Veteran” Jawa Timur.

8. Bapak dan Ibu dosen Teknik Informatika yang tidak dapat disebutkan satu persatu. Terima kasih banyak, berkat beliau semua penulis mendapat banyak ilmu dan wawasan yang berguna pada kemudian hari
9. Bapak dan Ibu Staff Universitas Pembangunan Nasional “Veteran” Jawa Timur yang membantu penulis dalam proses tugas akhir.
10. Teman - teman Teknik Informatika UPN “Veteran” Jawa Timur tidak bisa penulis sebutkan satu persatu.