

HALAMAN JUDUL

IMPLEMENTASI *INTRUSION PREVENTION SYSTEM* SURICATA PADA RASPBERRY PI 4

Diajukan sebagai syarat memperoleh gelar Sarjana Strata Satu (S-1)

Program Studi Teknik Elektro Fakultas Teknik

Universitas Muhammadiyah Yogyakarta



Disusun Oleh:

KHALID RAHMAT PRIYOTAMA

NIM: 20160120131

PROGRAM STUDI TEKNIK ELEKTRO

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH YOGYAKARTA

2020

HALAMAN PERNYATAAN

Yang Bertanda Tangan Dibawah ini:

Nama : Khalid Rahmat Priyotama
NIM : 20160120131
Jurusan : Teknik Elektro
Fakultas : Teknik
Universitas : Universitas Muhammadiyah Yogyakarta

Saya menyatakan dengan sesungguhnya bahwa tugas akhir ini dengan judul “IMPLEMENTASI *INTRUSION PREVENTION SYSTEM* SURICATA PADA RASPBERRY PI 4” merupakan hasil karya tulis saya sendiri dan tidak terdapat karya yang pernah diajukan untuk memperoleh gelar sarjana di Perguruan Tinggi dan sepanjang pengetahuan penulis juga tidak terdapat karya yang telah dipublikasikan oleh orang lain, kecuali secara tertulis disebutkan sumbernya dalam naskah dan daftar pustaka dengan mengikuti tata cara dan etika karya ilmiah yang lazim.

Yogyakarta, 22 Juni 2020


**METERAI
TEMPEL**
REGTADAHF459932820
6000
ENAM RIBU RUPIAH

Khalid Rahmat Priyotama

HALAMAN PERSEMBAHAN

Assalamualaikum Wr. Wb.

Alhamdulillahirabbil'alamin, puji syukur atas kehadiran Allah SWT atas segala limpahan kenikmatan kesehatan, Iman, Islam dan Karunia-nya sehingga Penulis dapat menyelesaikan Tugas Akhir. Dengan penuh rasa syukur, tugas akhir ini Penulis persembahkan untuk:

1. Orang tua, Ayah Heri Setiono dan Ibu Susilawati yang selalu memberikan dukungan, semangat, membiayai kebutuhan penulis dan tidak lupa selalu berdo'a semoga Allah SWT membalas seluruh kebaikan kepada mereka.
2. Adikku Abaz, Arby dan Fadli serta keluarga besar Penulis yang selalu mendukung dan memberikan semangat kepada Penulis sehingga menyelesaikan Tugas Akhir ini dengan selesai.
3. Seluruh Dosen Teknik Elektro yang sudah memberikan ilmunya selama masa perkuliahan. Semoga ilmu yang disampaikan dapat bermanfaat dan menjadi amal ibadah.
4. Teman daerah Bandar Lampung yang selalu mendukung dan memberikan masukan.
5. Teman-teman kelas D 2016 yang menjadi teman selama masa perkuliahan dan seperjuangan. Semoga selalu diberikan kemudahan dan kelancaran.
6. Teman-teman anggota grup "POKOKNYA WISUDA" yang selalu melancarkan dalam setiap hal dan hiburan dengan spam sticker-stickernya.
7. Teruntuk Angestia Belgis yang selalu mendukung, mendo'akan, memberikan semangat, masukan saran selama pengerjaan Tugas Akhir dan seterusnya.

MOTTO

فَبِأَيِّ آلَاءِ رَبِّكُمَا تُكَذِّبِينَ

“Maka nikmat Tuhan kamu yang manakah yang kamu dustakan?”

(Q.S AR-RAHMAN : 55)

“IF YOU MESS UP IT'S NOT YOUR PARENT'S FAULT, SO DON'T WHINE ABOUT YOUR MISTAKES; LEARN FROM THEM.”

(BILL GATES)

“THE PURPOSE OF TECHNOLOGY IS NOT TO CONFUSE THE BRAIN BUT TO SERVER THE BODY.”

(WILLIAM S. BURROUGHS)

“SUCCESSFUL PEOPLE ONLY HAVE TWO THINGS ON THEIR LIPS: SILENCE AND SMILE.”

(MARK ZUCKERBERG)

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Assalamualaikum Wr. Wb.

Puji syukur atas kehadiran Allah SWT karena telah melimpahkan segala rahmat, karunia serta hidayah-Nya memberikan Penulis segala nikmat kemudahan sehingga dapat menyelesaikan tugas akhir ini dengan baik dan dengan baik dan selesai pada waktunya yang berjudul “**IMPLEMENTASI *INTRUSION PREVENTION SYSTEM* SURICATA PADA RASPBERRY PI 4**”. Tugas akhir ini diajukan guna untuk memenuhi salah satu syarat untuk menyelesaikan pendidikan Program Studi S-1 Teknik Elektro Universitas Muhammadiyah Yogyakarta.

Penulis sangat menyadari bahwa dalam penyusunan tugas akhir ini tidak lepas dari berbagai hambatan dan permasalahan. Namun berkat bantuan, bimbingan, masukan dan semangat secara langsung ataupun tidak langsung dari berbagai pihak sehingga Penulis mampu menyelesaikan tugas akhir ini. Dalam kesempatan ini, Penulis mengucapkan sangat terima kasih kepada:

1. Bapak Dr. Ir. Gunawan Budiyo, MP. selaku Rektor Universitas Muhammadiyah Yogyakarta.
2. Bapak Jaza'ul Ikhsan, S.T., M.T, Ph.D. selaku Dekan Fakultas Teknik Universitas Muhammadiyah Yogyakarta.
3. Bapak Dr. Ramadoni Syahputra, S.T., M.T. selaku Ketua Program Studi Teknik Elektro Universitas Muhammadiyah Yogyakarta.
4. Bapak Yudhi Ardiyanto, S.T., M.Eng. selaku Dosen Pembimbing I dan Ibu Anna Nur Nazilah Chamim, S.T., M.Eng. selaku Dosen pembimbing II , yang meluangkan waktunya untuk membimbing, memberikan saran, masukan dan pengalaman yang sangat berharga dalam penulisan tugas akhir ini. Semoga Allah SWT membalas seluruh kebaikan mereka.
5. Bapak Kunnu Purwanto, S.T., M.Eng. selaku Dosen penguji yang telah

memberikan masukan dan saran dalam Tugas Akhir ini.

6. Para seluruh Dosen Jurusan Teknik Elektro UMY yang telah memberikan ilmu yang bermanfaat selama Penulis menempuh pendidikan di Teknik Elektro UMY. Semoga Ilmu yang diberikan menjadi amal ibadah.
7. Seluruh staff labaratorium Teknik Elektro UMY yang telah memberi arahan dalam melaksanakan praktikum selama menempuh pendidikan.
8. Seluruh jajaran staff tata usaha dan referensi Teknik UMY yang telah membantu kemudahan Penulis selama menempuh Pendidikan.
9. Semua teman-teman yang terlibat secara langsung maupun tidak langsung dalam membantu penyusunan tugas akhir ini.
10. Penulis sangat menyadari bahwa tugas akhir ini masih banyak kekurangan. Oleh karena itu, kritik dan saran maupun masukan yang sifatnya membangun dari pembaca sangat Penulis harapkan, sehingga tugas akhir ini lebih baik kedepannya. Akhir kata, semoga tugas akhir ini dapat bermanfaat bagi semua pihak dan dapat dijadikan sumber referensi pada penelitian selanjutnya.

Yogyakarta, 22 Juni 2020

Penulis

Khalid Rahmat Priyotama

DAFTAR ISI

HALAMAN JUDUL.....	i
LEMBAR PENGESAHAN I.....	ii
LEMBAR PENGESAHAN II.....	iii
HALAMAN PERNYATAAN.....	iv
HALAMAN PERSEMBAHAN.....	v
MOTTO.....	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	ix
DAFTAR GAMBAR.....	xii
DAFTAR TABEL.....	xiv
INTISARI.....	xv
<i>ABSTRACT</i>	xvi
BAB I.....	1
PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah.....	2
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	3
1.6 Sistematika Penulisan.....	3
BAB II.....	5
LANDASAN TEORI.....	5
2.1 Tinjauan Pustaka.....	5
2.2 Dasar Teori.....	9
2.2.1 Jaringan Komputer.....	9
2.2.1.1 Jenis- Jenis Jaringan Komputer.....	10
2.2.1.2 Berdasarkan Konfigurasi Jaringan Komputer.....	10
2.2.2 Keamanan Jaringan Komputer.....	11
2.2.3 Ancaman Jaringan Komputer.....	12
2.2.4 <i>Internet of Things</i> (IoT).....	13
2.2.5 Ancaman Serangan IoT (<i>Internet of Things</i>).....	13

2.2.6	<i>Intrusion Detection System (IDS)</i>	14
2.2.7	<i>Intrusion Prevention System (IPS)</i>	15
2.2.7.1	Jenis-Jenis IPS	16
2.2.7.2	Cara Kerja IPS	16
2.2.8	<i>Software Suricata</i>	17
2.2.8.1	Penjelasan <i>Software Suricata</i>	17
2.2.8.2	Panduan <i>Suricata</i>	17
2.2.9	<i>Firewall</i>	25
2.2.9.1	Teknik <i>Firewall</i>	26
2.2.9.2	Tipe-Tipe <i>Firewall</i>	26
2.2.10	OS Ubuntu	27
2.2.11	<i>Software Kali Linux</i>	28
2.2.12	<i>Software Nmap</i>	29
2.2.13	<i>Software Nikto</i>	31
2.2.14	<i>Software WPScan</i>	31
2.2.15	<i>Software Red Hawk</i>	32
2.2.16	<i>Software WPHunter</i>	34
2.2.17	<i>Software WAScan</i>	34
2.2.18	Raspberry Pi	36
2.2.18.1	Web Server pada Raspberry Pi 4	36
2.2.18.2	Raspberry Pi 4 Model B RAM 4GB	38
BAB III		40
METODE PENELITIAN		40
3.1	Tahapan Jalannya Penelitian Tugas Akhir	40
3.2	Studi Literatur	41
3.3	Identifikasi dan Perumusan Masalah	41
3.4	Analisa Kebutuhan <i>Suricata</i> di Raspberry Pi 4	41
3.5	Alat dan Bahan Penelitian	41
3.7	Install OS Ubuntu 19.10 pada Raspberry Pi 4	42
3.8	Install <i>Suricata</i> dan <i>Iptables</i> pada OS Ubuntu di Raspberry Pi 4	43
3.9	Implementasi dan Tahapan Pengujian Sistem	49
3.10	Pengukuran <i>performance</i> Raspberry Pi 4	51
3.11	Laporan Penelitian dan Hasil Pengujian	52
BAB IV		53

HASIL DAN PEMBAHASAN.....	53
4.1 Implementasi Topologi Suricata pada Raspberry Pi 4	53
4.2 <i>Running</i> Suricata pada Raspberry Pi 4	54
4.3 Pengujian Suricata pada Raspberry Pi 4.....	55
4.3.1 Serangan pada Raspberry Pi 4 dengan Zenmap.....	55
4.3.2 Mendeteksi Serangan Zenmap pada Suricata	56
4.3.3 Hasil Pengujian Serangan Zenmap pada Raspberry Pi 4.....	57
4.4 Implementasi <i>Intrusion Prevention System</i> pada Raspberry Pi 4.....	57
4.4.1 <i>Running</i> Iptables Mode NFQUEUE Suricata	58
4.4.2 Pengujian Iptables Mode NFQUEUE dengan Zenmap	59
4.5 Perbandingan Hasil Zenmap Penerapan IPS Suricata.....	59
4.6 Implementasi Raspberry Pi 4 sebagai Web Server.....	s60
4.6.1 Pengujian Akses Web Server Raspberry Pi 4	61
4.6.2 Pengujian Suricata pada Web Server Raspberry Pi 4	63
4.6.3 Serangan Web Server pada WordPress dengan Nikto	63
4.6.4 Mendeteksi Serangan Nikto pada Suricata	64
4.6.5 Serangan Web Server pada WordPress dengan WPScan	65
4.6.6 Serangan Web Server pada WordPress dengan Red Hawk	66
4.6.7 Serangan Web Server pada WordPress dengan WPHunter	69
4.6.8 Serangan Web Server pada WordPress dengan WAScan.....	69
4.6.9 Hasil Pengujian Serangan pada Web Server WordPress	71
4.7 Mengukur <i>Performance</i> Suricata pada Raspberry Pi 4	72
4.8 Mengukur <i>Performance</i> Raspberry Pi 4.....	75
4.8 Waktu dan Uraian Penerapan Suricata pada Raspberry Pi 4.....	77
BAB V.....	80
PENUTUP.....	80
5.1 Kesimpulan.....	80
5.2 Saran	80
DAFTAR PUSTAKA	81

DAFTAR GAMBAR

Gambar 2.1 Topologi Jaringan Peer-to-Peer.....	11
Gambar 2.2 Topologi Jaringan Client atau Server.....	11
Gambar 2.3 Grafik IoT Penetration	14
Gambar 2.4 Topologi Intrusion Detection System (IDS)	14
Gambar 2.5 Topologi Intrusion Prevention System (IPS)	15
Gambar 2.6 Logo Software Suricata.....	17
Gambar 2.7 Topologi Firewall.....	26
Gambar 2.8 Logo OS Ubuntu	27
Gambar 2.9 Logo Software Kali Linux	29
Gambar 2.10 Logo Software Nmap	30
Gambar 2.11 Tampilan GUI Software Zenmap.....	30
Gambar 2.12 Logo Software Nikto.....	31
Gambar 2.13 Logo Software WPScan	32
Gambar 2.14 Tampilan Software Red Hawk	34
Gambar 2.15 Tampilan Software WPHunter	34
Gambar 2.16 Tampilan Software WAScan.....	35
Gambar 2.17 Logo Software Raspbian	36
Gambar 2.18 Desain Perangkat Raspberry Pi 4 Model B RAM 4GB	38
Gambar 3.1 Flowchart Metodologi Penelitian.....	40
Gambar 3.2 Raspbian Running di OS Ubuntu 19.10	43
Gambar 3.3 Flowchart Tahapan Install Suricata dan Iptables pada OS Ubuntu....	43
Gambar 3.4 Paket Kompilasi Suricata	44
Gambar 3.5 Hasil Ekstrak Rules	45
Gambar 3.6 Letak Default Rules Suricata.....	45
Gambar 3.7 Memperbarui Sumber Suricata	46
Gambar 3.8 Memperbarui Daftar Sumber Suricata	46
Gambar 3.9 Memperbarui dan Mengaktifkan Sumber OISF/Trafficid	47
Gambar 3.10 Penambahan Repository OISF Suricata	47
Gambar 3.11 Install Suricata.....	48

Gambar 3.12 Install Mode IPS NFQUEUE	48
Gambar 3.13 Konfigurasi Mode IPS NFQUEUE	49
Gambar 3.14 Blok Diagram Pengujian Sistem Suricata	50
Gambar 4.1 Topologi Jaringan Suricata pada Raspberry Pi 4	53
Gambar 4.2 Running Suricata pada eth0 Raspberry Pi 4.....	54
Gambar 4.3 Serangan Port Scanning pada Raspberry Pi 4 dengan Zenmap	56
Gambar 4.4 Log serangan Attacker terhadap Raspberry Pi 4.....	56
Gambar 4.5 Mengaktifkan Iptables Mode NFQUEUE.....	58
Gambar 4.6 Running Iptables Mode NFQUEUE Suricata	58
Gambar 4.7 Serangan Port Scanning Attacker dicegah	59
Gambar 4.8 Hasil Web Server WordPress pada Raspberry Pi 4.....	61
Gambar 4.9 Hasil akses Web Server Raspberry Pi 4 pada Laptop ASUS.....	62
Gambar 4.10 Hasil akses Web Server Raspberry Pi 4 pada Iphone 7+	62
Gambar 4.11 Serangan Scanning Web Server WordPress dengan Nikto.....	64
Gambar 4.12 Log serangan Web Server WordPress dengan Nikto	65
Gambar 4.13 Serangan Scanning Web Server WordPress dengan WPScan	66
Gambar 4.14 Serangan ke IP Web Server dengan Red Hawk	66
Gambar 4.15 Serangan Red Hawk Scanner Web Server dengan Basic Recon	67
Gambar 4.16 Serangan Red Hawk Scanner Web Server dengan WordPress Scan	68
Gambar 4.17 Hasil serangan Tools WordPress Scan pada Red Hawk	68
Gambar 4.18 Serangan Scanning Web Server WordPress dengan WPHunter.....	69
Gambar 4.19 Tampilan Tools pada WAScan	70
Gambar 4.20 Serangan Scanning Web Server pada WordPress dengan WAScan	71
Gambar 4.21 Perintah Top PID Suricata pada Raspberry Pi 4	73
Gambar 4.22 Grafik Performance Suricata pada Raspberry Pi 4.....	75
Gambar 4.23 Hasil Top <i>Performance</i> Raspberry Pi 4 saat tidak terjadi serangan.....	76
Gambar 4.24 Hasil Top <i>Performance</i> Raspberry Pi 4 dengan serangan Zenmap	76
Gambar 4.25 Hasil Top <i>Performance</i> Raspberry Pi 4 dengan serangan Nikto	77

DAFTAR TABEL

Tabel 2.1 Susunan Daftar Tinjauan Pustaka	5
Tabel 2.2 Suricata CLO (Command Line Options)	18
Tabel 2.3 Kombinasi Simbol Operator pada Source dan Destination	21
Tabel 2.4 Contoh dan Penjelasan Rule-Vars	21
Tabel 2.5 Kombinasi Simbol Operator pada Port	22
Tabel 2.6 Contoh Penggunaan Simbol Operator pada Port	22
Tabel 2.7 Tools dan fungsi pada Red Hawk	32
Tabel 3.1 Hardware dan Software Penelitian.....	41
Tabel 4.1 Device dan Alamat pada Topologi Jaringan Host-Based IPS.....	54
Tabel 4.2 Hasil log serangan dan dampak pada Raspberry Pi 4	57
Tabel 4.3 Perbandingan Hasil Penerapan IPS Suricata.....	60
Tabel 4.4 Hasil log serangan dan dampak pada Web Server Raspberry Pi 4	71
Tabel 4.5 Ringkasan Performance PID Suricata pada Raspberry Pi 4	73
Tabel 4.6 Waktu Penerapan Suricata pada Raspberry Pi 4 di Jaringan	77