

**IMPLEMENTASI KEAMANAN JARINGAN MENGGUNAKAN INTRUSION
PREVENTION SYSTEM (IPS) DAN PORT KNOCKING DI SMK YADIKA
BANDAR LAMPUNG**

SKRIPSI



disusun oleh

Dominggus Abednegho Hurupatu

16.11.0807

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2021

**IMPLEMENTASI KEAMANAN JARINGAN MENGGUNAKAN INTRUSION
PREVENTION SYSTEM (IPS) DAN PORT KNOCKING DI SMK YADIKA
BANDAR LAMPUNG**

SKRIPSI



disusun oleh

Dominggus Abednegho Hurupatu

16.11.0807

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2021

PERSETUJUAN

SKRIPSI

IMPLEMENTASI KEAMANAN JARINGAN MENGGUNAKAN INTRUSION PREVENTION SYSTEM (IPS) DAN PORT KNOCKING DI SMK YADIKA BANDAR LAMPUNG

yang dipersiapkan dan disusun oleh

Dominggus Abednegho Hurupatu

16.11.0807

telah disetujui oleh Dosen Pembimbing
Skripsi pada tanggal 9 Agustus 2021

Dosen Pembimbing,

Mulia Sulistivono, M.Kom

NIK. 190302248

PENGESAHAN
SKRIPSI
IMPLEMENTASI KEAMANAN JARINGAN
MENGGUNAKAN INTRUSION PREVENTION SYSTEM
(IPS) DAN PORT KNOCKING DI SMK YADIKA BANDAR

yang dipersiapkan dan disusun oleh
Dominggus Abednegho Hurupatu

16.11.0807

telah dipertahankan di depan Dewan Penguji
pada tanggal 24 Agustus 2021

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Yoga Pristyanto.S.Kom.. M.Eng
NIK. 190302412

Mulia Sulistiyono.M.kom
NIK. 190302248

Nila Feby Puspitasari. S.Kom. M.Cs
NIK. 190302161

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 12 Oktober 2021

DEKAN FAKULTAS ILMU KOMPUTER

Hanif AlFatta. S.Kom.. M.Kom
NIK. 190302096

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka. Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 18 Oktober 2021



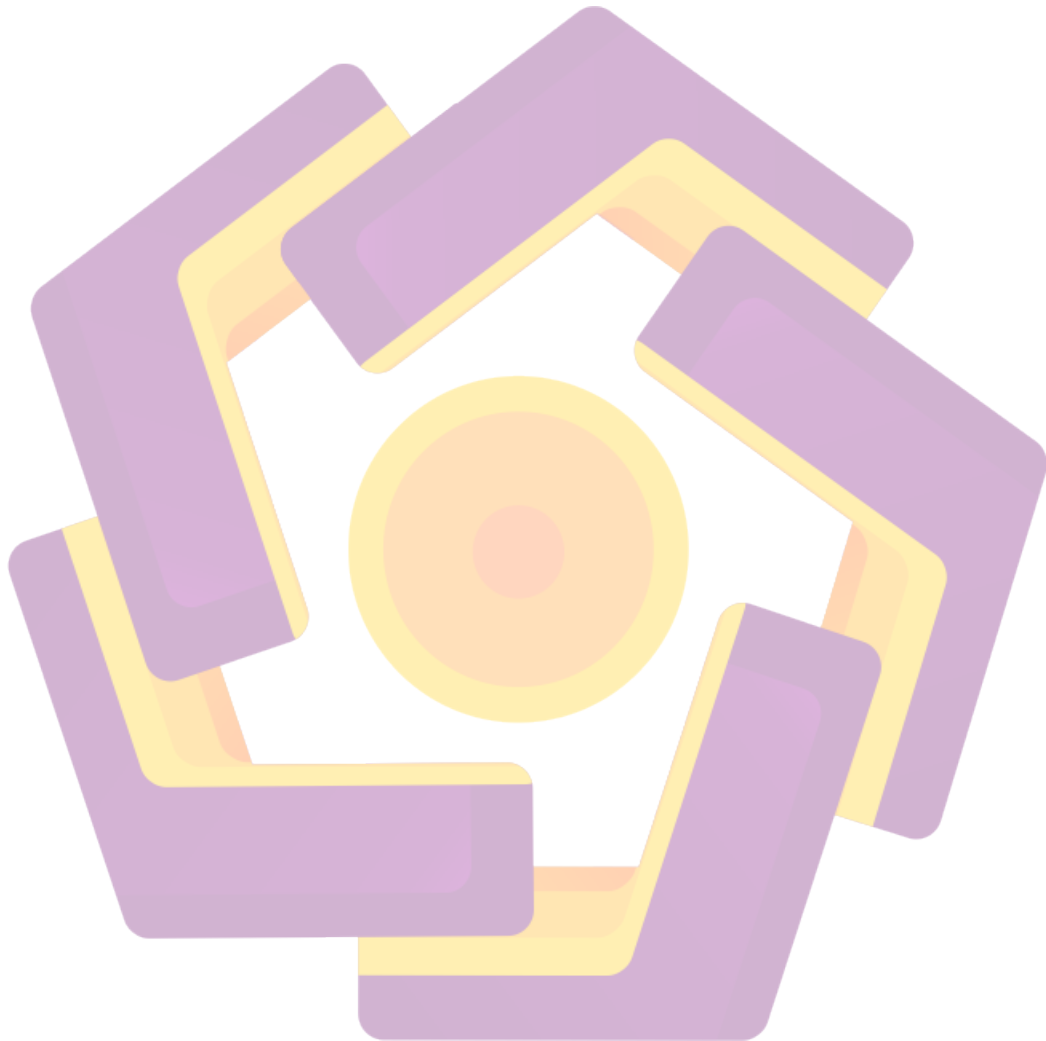
Dominggus Abednegho Hurupatu

NIM. 16.11.0807

MOTTO

“Everything will be okay in the end. If it’s not okay, it’s not the end.”

Jhon Lennon



PERSEMBAHAN

Mengucapkan puji syukur kepada Tuhan Yesus Kristus, dan mengucapkan terima kasih atas dukungan dan do'a dari orang-orang tercinta atas bantuan dan dukungan, sehingga skripsi ini dapat diselesaikan dengan baik. Untuk itu penulis mengucapkan banyak terimakasih kepada :

1. Tuhan Yesus Kristus atas segala pertolongannya, sehingga penulis bisa menyelesaikan skripsi ini.
2. Keluarga besar, Bapak, Mamak, Kakak dan Adik, terimakasih atas do'a, semangat, kasih sayang, dan pengorbanan yang tulus dalam mendampingi penulis.
3. Dosen pembimbing yang senantiasa memberikan masukan dan bimbingan sehingga penulis bisa menyelesaikan skripsi dengan baik.
4. Guru SMK Yadika Bandar Lampung, seluruh karyawan yang sudah membantu penulis dalam penyelesaian skripsi. Teman-teman IF13, BARBEL, dan kontrakan ijo terimakasih banyak atas semangat, keceriaan dan ketulusannya dalam mendampingi penulis.

Akhir kata diucapkan terima kasih sebesar-besarnya semoga skripsi ini bisa bermanfaat bagi penulis dan pembaca.

Dengan menyebut nama Tuhan Yesus Kristus Puji syukur atas hadiratnya yang telah melimpahkan kasih karunia-Nya. Sehingga skripsi dengan judul "Implementasi Intrusion Prevention System (IPS) dan Port Knocking di SMK Yadika Bandar Lampung" dapat terselesaikan.

Penulis menyadari bahwa dalam pelaksanaan dan penyusunan skripsi ini tidak lepas dari bantuan dan dukungan dari berbagai pihak. Untuk itu perkenankan penulis mengucapkan terima kasih kepada :

1. Prof. Dr. M. Suyanto, M.M selaku Rektor Universitas AMIKOM Yogyakarta.
2. Ibu Windha Mega PD, M.Kom selaku ketua program studi Informatika.
3. Bapak Mulia Sulistiyono, M.kom selaku pembimbing yang senantiasa memberikan masukan dan bimbingan dalam skripsi ini.
4. Bapak Yoga Pristyanto, S.Kom., M.Eng., dan Ibu Nila Feby Puspitasari, S.Kom., M.Cs. selaku penguji yang telah memberikan masukan dan saran.
5. Dosen dan seluruh staf Universitas Amikom Yogyakarta, yang telah memberikan ilmu selama menjalani Pendidikan di Universitas Amikom Yogyakarta.
6. Orang tua tercinta Bapak Martin Luther Hurupatu, Ibu Titik Puji Lestari dan kakak saya Yohanes Alex Fernando Hurupatu, D a n a d i k - a d i k s a y a Yohanes Erik Ferdinan Hurupatu, Mona Olivya Hurupatu, terimakasih tak

terhingga atas do'a, semangat, kasih sayang, dan pengorbanan yang tulus selama ini.

7. Terima kasih untuk wanita yang saya sayang selalu menemani dan juga memberi semangat, dukungan, amarah, tawa serta kecewa yang memberi motivasi untuk segera menyelesaikan skripsi ini
8. Untuk sahabat saya M. Yoga Haidil Akbar, dan Isnandar Septiawan. Serta keluarga besar BARBEL dan teman-teman IF 13 yang selalu menjaga dan mengingatkan saya selama di perantauan.
9. Semua teman-teman yang ikut terlibat dalam kelancaran skripsi ini.

Akhir kata dalam penyusunan skripsi ini penulis menyadari masih belum sempurna oleh karena itu penulis mengharapkan kritik dan saran untuk perbaikan dimasa yang akan datang. Semoga skripsi ini bermanfaat bagi penulis dan pembaca.

Yogyakarta,

Dominggus Abednegho Hurupatu

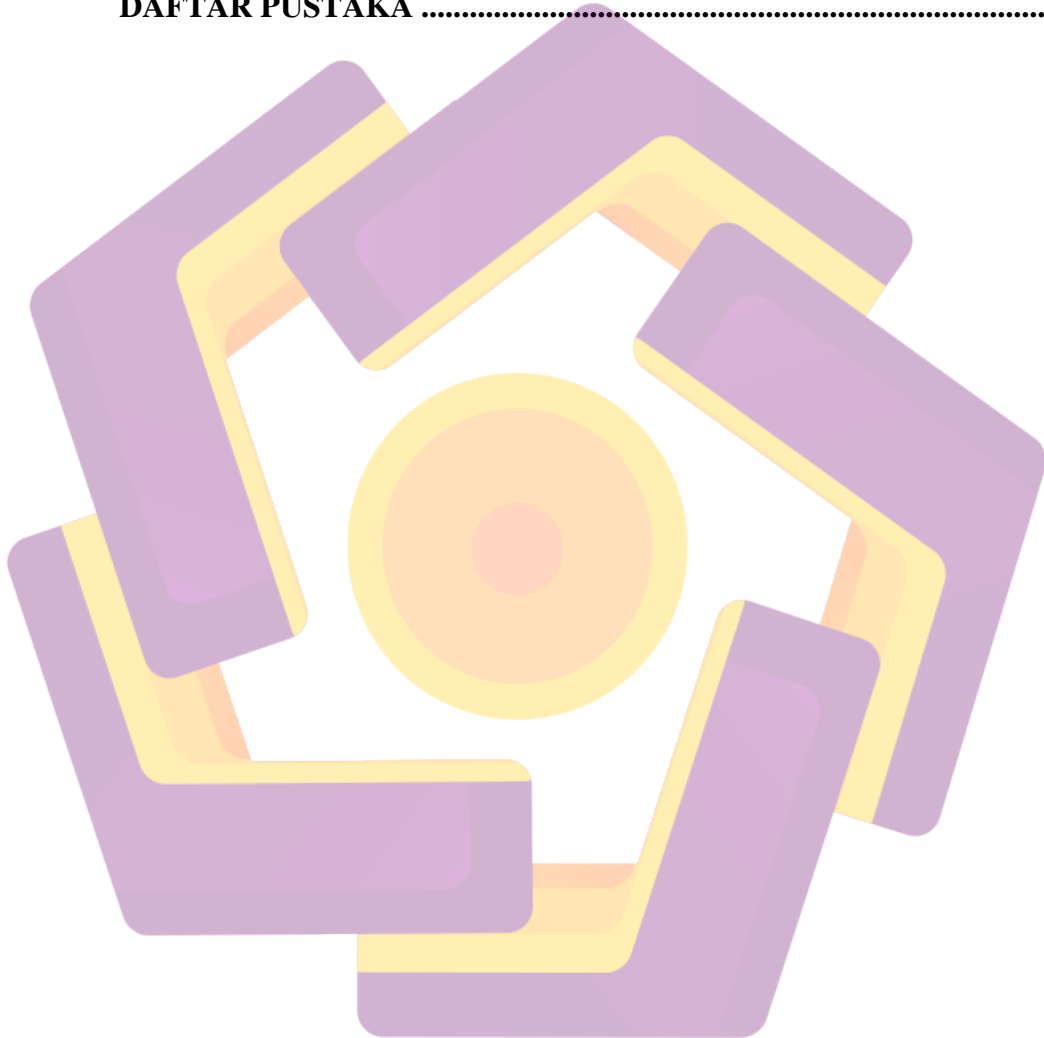
DAFTAR ISI

JUDUL	i
LEMBAR PERSETUJUAN	ii
LEMBAR PENGESAHAN	iii
PERNYATAAN	iv
MOTTO	v
PERSEMBAHAN	vi
DAFTAR ISI	ix
DAFTAR TABEL	xiii
DAFTAR GAMBAR	xiv
INTISARI	xvii
ABSTRACT	xviii
BAB I Pendahuluan	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	3
1.5 Metode Penelitian	4
1.5.1 Metode Pengumpulan Data	4
1.5.2 Metode Analisis dan Perancangan	4
1.6 Sistematika Penulisan	4
BAB II Landasan Teori	6
2.1 Tinjauan Pustaka	6
2.2 Intrusion Prevention System (IPS)	11

2.2.1	Tujuan Penggunaan Intrusion Prevetion System (IPS)	12
2.2.2	Host Based Intrusion Prevention System (HIPS).....	13
2.2.3	Network Based Intrusion Prevention System (NIPS)	13
2.3	Port Knocking	14
2.4	Keamanan Jaringan	14
2.5	Snort.....	16
2.6	Definisi Jaringan Komputer	19
2.7	Jenis Jaringan Komputer.....	21
2.8	Topologi Jaringan	23
2.8.2	Topologi Ring	24
2.8.3	Topologi Star	24
2.8.4	Topologi Mesh	25
2.9	Router	25
2.11	TCP dan UDP	26
2.11.1	Transmission Control Protocol (TCP).....	27
2.11.2	User Datagram Protocol (UDP).....	27
2.12	Mikrotik Router.....	27
2.13	Perangkat Lunak yang Digunakan	28
2.13.1	Mikrotik RouterOS.....	28
2.13.2	Winbox.....	30
2.13.3	Wireshark	31
2.13.4	Putty	31
2.13.5	VMware Workstation.....	32
2.13.6	Zenmap	32
2.13.7	Kali Linux.....	33
2.14	Action Research (Penelitian Tindakan).....	33
2.15	Metode Simulasi.....	35
BAB III METODE PENELITIAN.....		36

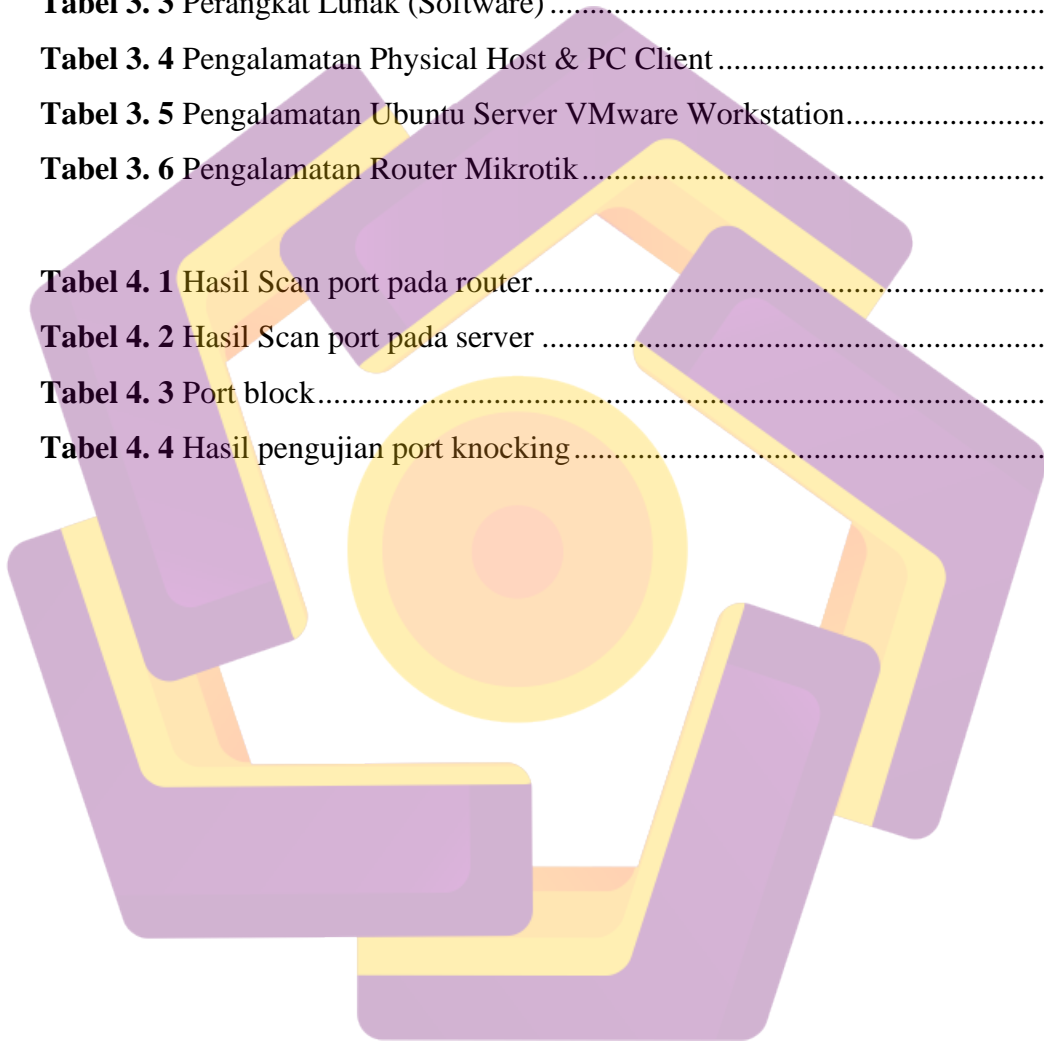
3.1	Identifikasi Masalah	36
3.1.1	Alur Penelitian.....	37
3.2	Pengumpulan Data	38
3.2.1	Observasi.....	38
3.3	Alat dan Bahan	40
3.3.1	Perangkat Keras (Hardware).....	40
3.3.2	Perangkat Lunak (Software).....	41
3.4	Perancangan Metode	42
3.4.1	Topologi Lama.....	42
3.4.2	Rancangan Topologi Jaringan.....	43
3.4.3	Simulasi	44
3.4.4	Pengalamatan jaringan.....	45
BAB IV IMPLEMENTASI DAN PEMBAHASAN Implementasi		47
4.1	Implementasi	47
4.1.1	Konfigurasi awal Mikrotik RouterBoard	47
4.1.2	Pengujian Awal Sistem	53
4.2	Konfigurasi Snort Intrusion Prevention System (IPS).....	55
4.2.1	Pengaturan zona waktu pada server	55
4.2.2	Install snort di ubuntu	56
4.2.3	Memasang data aquisition (DAQ)	58
4.2.4	Konfigurasi Snort.....	59
4.3	Pengujian Intrusion Prevention System (IPS)	61
4.3.1	Pengujian brute force	62
4.3.2	Pengujian jaringan.....	63
4.3.3	Analisis Traffic	64
4.4	Konfigurasi Port Knocking.....	65
4.4.1	Membuat filter rules knock.....	66
4.4.2	Membuat filter rule safe IP	67
4.4.3	Membuat filter rule penyusup	69
4.4.4	Membuat filter rule drop.....	70

4.4.5	Pengujian Port Knocking	72
4.5	Hasil pengujian port knocking	77
BAB v PENUTUP		79
5.2	Kesimpulan.....	79
5.3	Saran	79
DAFTAR PUSTAKA		81



DAFTAR TABEL

Tabel 2. 1 Tinjauan Pustaka.....	8
Tabel 2. 2 Pemicu Port Knocking.....	14
Tabel 3. 1 Hasil pengamatan jaringan.....	40
Tabel 3. 2 Perangkat Keras (Hardware).....	40
Tabel 3. 3 Perangkat Lunak (Software).....	41
Tabel 3. 4 Pengalamatan Physical Host & PC Client.....	46
Tabel 3. 5 Pengalamatan Ubuntu Server VMware Workstation.....	46
Tabel 3. 6 Pengalamatan Router Mikrotik.....	46
Tabel 4. 1 Hasil Scan port pada router.....	54
Tabel 4. 2 Hasil Scan port pada server.....	55
Tabel 4. 3 Port block.....	66
Tabel 4. 4 Hasil pengujian port knocking.....	77



DAFTAR GAMBAR

Gambar 2. 1 Contoh Rule Snort.....	16
Gambar 2. 2 Jaringan Client-Server.....	20
Gambar 2. 3 Jaringan Peer to Peer.....	21
Gambar 2. 4 Topologi LAN.....	22
Gambar 2. 5 Topologi MAN.....	22
Gambar 2. 6 Topologi WAN.....	23
Gambar 2. 7 Topologi Bus.....	24
Gambar 2. 8 Topologi Ring.....	24
Gambar 2. 9 Topologi Star.....	25
Gambar 2. 10 Topologi Mesh.....	25
Gambar 2. 11 TCP Header.....	27
Gambar 2. 12 UDP Header.....	27
Gambar 2. 13 Mikrotik RB941-2nD-TC.....	28
Gambar 2. 14 Mikrotik RB800.....	28
Gambar 2. 15 Logo Mikrotik.....	30
Gambar 2. 16 Logo Winbox.....	31
Gambar 2. 17 Logo Wireshark.....	31
Gambar 2. 18 Logo Putty.....	32
Gambar 2. 19 Logo VMware.....	32
Gambar 2. 20 Logo Zenmap.....	33
Gambar 2. 21 Logo kali linux.....	33
Gambar 2. 22 Tahapan Action Research.....	34
Gambar 3. 1 Diagram Alur Penelitian.....	37
Gambar 3. 2 Hasil rekam 1.....	38
Gambar 3. 3 Hasil rekam 2.....	39
Gambar 3. 4 Hasil rekam 3.....	39
Gambar 3. 5 Topologi jaringan lama.....	43
Gambar 3. 6 Racangan Topologi jaringan.....	44
Gambar 3. 7 Topologi Simulasi.....	45

Gambar 4. 1 Mengganti Password Router	47
Gambar 4. 2 Merubah tanggal dan waktu	48
Gambar 4. 3 Konfigurasi IP Address	48
Gambar 4. 4 Konfigurasi Routes	49
Gambar 4. 5 Konfigurasi NAT	49
Gambar 4. 6 Perintah untuk mengatur IP server	50
Gambar 4. 7 Konfigurasi IP pada Server	50
Gambar 4. 8 Konfigurasi IP pada Client.....	51
Gambar 4. 9 Ping dari router ke client	51
Gambar 4. 10 Ping dari router ke server	52
Gambar 4. 11 Ping dari server ke router	52
Gambar 4. 12 Ping dari server ke client.....	52
Gambar 4. 13 Ping dari client ke router	53
Gambar 4. 14 Ping dari client ke server.....	53
Gambar 4. 15 Hasil scan port pada router.....	54
Gambar 4. 16 Hasil scan port pada server	55
Gambar 4. 17 List zona waktu	56
Gambar 4. 18 Perintah mengubah zona waktu	56
Gambar 4. 19 Hasil zona waktu diperbarui	56
Gambar 4. 20 Perintah install snort di ubuntu	56
Gambar 4. 21 Memilih Interface snort.....	57
Gambar 4. 22 Memberikan IP untuk local network.....	57
Gambar 4. 23 Memilih Interface snort.....	58
Gambar 4. 24 Perintah memasang DAQ.....	58
Gambar 4. 25 Snort membaca modul DAQ.....	58
Gambar 4. 26 Perintah konfigurasi snort.conf	59
Gambar 4. 27 Konfigurasi di file snort.conf	59
Gambar 4. 28 Perintah konfigurasi local.rules.....	60
Gambar 4. 29 Rules baru untuk snort	60
Gambar 4. 30 Perintah untuk menjalankan snort.....	61
Gambar 4. 31 serangan brute force sebelum implementasi	62

Gambar 4. 32	serangan brute force sebelum implementasi	63
Gambar 4. 33	serangan brute force sesudah implementasi.....	63
Gambar 4. 34	Uji coba jaringan sebelum serangan	64
Gambar 4. 35	Uji coba jaringan saat terjadi serangan	64
Gambar 4. 36	Grafik perbandingan traffic.....	65
Gambar 4. 37	Tampilan hasil penanganan pada server	65
Gambar 4. 38	Menu general rule knock.....	66
Gambar 4. 39	Menu Action rule knock	67
Gambar 4. 40	Menu general rule safe IP	68
Gambar 4. 41	Menu action rule safe IP	68
Gambar 4. 42	Menu action rule safe IP	69
Gambar 4. 43	Menu general rule penyusup	69
Gambar 4. 44	Menu action rule penyusup	70
Gambar 4. 45	Menu action rule penyusup	70
Gambar 4. 46	Menu general rule drop	71
Gambar 4. 47	Menu action rule drop	71
Gambar 4. 48	Menu action rule drop	72
Gambar 4. 49	Mengakses router melalui port 1000.....	73
Gambar 4. 50	Command dari putty.....	73
Gambar 4. 51	Router membaca list knock-1000.....	74
Gambar 4. 52	Mengakses router melalui port 22.....	74
Gambar 4. 53	Putty dapat mengakses router	75
Gambar 4. 54	Router membaca list SAFE-IP	75
Gambar 4. 55	Koneksi www sebelum di block	76
Gambar 4. 56	Koneksi www sesudah di block	76
Gambar 4. 57	Router membaca list PENYUSUP	76
Gambar 4. 58	Akses winbox sebelum di block.....	77
Gambar 4. 59	Akses winbox setelah di block.....	77

INTISARI

Perkembangan teknologi yang pesat pada saat ini berdampak pada keamanan jaringan yang ada. Upaya serangan dari luar terhadap jaringan menjadi masalah dalam keamanan jaringan yang terus terjadi, bagi instansi instansi terkait yang menggunakan layanan internet, termasuk juga jaringan yang ada di SMK YADIKA BANDAR LAMPUNG layanan internet digunakan sebagai media pembelajaran oleh siswa/siswi rentan terhadap gangguan serangannya oleh pihak pihak yang tidak bertanggung jawab, Gangguan dari dalam sering terjadi pada suatu institusi, menyerang *server*, data, atau *service*. *Server* sebagai pusat penyedia layanan dan pengolahan data dalam suatu jaringan, permintaan yang dikirim oleh *client* akan diolah *server*. Kinerja *server* bergantung terhadap paket yang dikirim oleh *client* pada jaringan, sehingga jika terjadi gangguan pada server akan mengganggu jalannya proses belajar mengajar.

Oleh karena itu diperlukan sistem yang mampu menjaga keamanan pada jaringan, *Intrusion Prevention System (IPS)* yang dijalankan menggunakan snort mode inline dapat melakukan *drop* terhadap paket yang mencurigakan yang bertujuan menyerang server tanpa harus memberikan notifikasi kepada administrator, dan *Port Knocking* digunakan untuk menjaga hak akses perangkat router dari pengguna yang tidak berwenang untuk mengaksesnya. dengan cara kerja yaitu dapat membuka atau menutup akses *port* tertentu melalui *firewall* pada router sesuai dengan *rules* yang dibangun.

Dari penelitian yang dilakukan didapatkan hasil bahwa *Intrusion Prevention System (IPS)* dan *Port Knocking* yang sudah diterapkan dapat melakukan *drop packet* yang menyerang *server*, sehingga kinerja *server* dapat berjalan dengan baik dan mengurangi gangguan saat kegiatan belajar mengajar yang dilakukan oleh siswa dan guru di SMK Yadika Bandar lampung.

Kata kunci: Intursion Prevention system, Port Knocking, Keamanan

Jaringan

ABSTRACT

Rapid technological developments at this time the hedge is on the security of an existing network. Attack attempts from the outside to the network to be a problem in network security continues to occur, for the agency related agencies who use internet services, including network at SMK YADIKA BANDAR LAMPUNG service the internet is used as a medium of learning by the students susceptible to interference serangan by parties who are not responsible, a Distraction from the often occur in an institution, the attacking server, data, or service. Server as a service providers and processing data in a network, a request sent by the client will be processed server. The performance of the server depends on the package that is sent by the client on the network, so if interference occurs on the server will interfere with the course of the process of teaching and learning.

Therefore a system is needed that is able to maintain security on the network, Intrusion Prevention System (IPS) that is run using the snort inline mode can do drop to a suspicious package that aims to attack a server without having to give a notification to the administrator, and Port Knocking is used to maintain the right of access your router from users who are not authorized to access it. by way of working which can open or close access to a specific port through the firewall on the router in accordance with the rules that are built.

From the research conducted showed that the Intrusion Prevention System (IPS) and Port Knocking is already applied can do drop packet that attack the server, so that the performance of the server can be run with better and reduces interference when the teaching and learning activities undertaken by students and teachers in SMK Yadika Bandar lampung.

Keywords: Intursion Prevention system, Port Knocking, Network Security