

**APLIKASI NOTIFIKASI ALERT INTRUSION DETECTION SYSTEM
(IDS) PADA EMAIL UNTUK REPORTING KEAMANAN JARINGAN
(Studi Kasus : Wisma Gunung Merah)**

SKRIPSI



disusun oleh
Crishariansyah
16.11.0631

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2020**

**APLIKASI NOTIFIKASI ALERT INTRUSION DETECTION SYSTEM
(IDS) PADA EMAIL UNTUK REPORTING KEAMANAN JARINGAN
(Studi Kasus : Wisma Gunung Merah)**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika



disusun oleh
Crishariansyah
16.11.0631

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2020**

PERSETUJUAN

SKRIPSI

**APLIKASI NOTIFIKASI ALERT INTRUSION DETECTION SYSTEM
(IDS) PADA EMAIL UNTUK REPORTING KEAMANAN JARINGAN
(Studi Kasus : Wisma Gunung Merah)**

yang dipersiapkan dan disusun oleh

Crishariansyah

16.11.0631

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 9 November 2020

Dosen Pembimbing,

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

PENGESAHAN

SKRIPSI

APLIKASI NOTIFIKASI ALERT INTRUSION DETECTION SYSTEM (IDS) PADA EMAIL UNTUK REPORTING KEAMANAN JARINGAN

(Studi Kasus : Wisma Gunung Merah)

yang dipersiapkan dan disusun oleh

Crishariansyah
16.11.0631

telah dipertahankan di depan Dewan Penguji
pada tanggal 19 November 2020

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Melwin Syafrizal, S.Kom., M.Eng

NIK. 190302105

Joko Dwi Santoso, M.Kom

NIK. 190302181

Nila Feby Puspitasari, S.Kom, M.Cs

NIK. 190302161

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 4 Desember 2020

DEKAN FAKULTAS ILMU KOMPUTER

Krisnawati, S.Si, M.T.

NIK. 190302038

PERNYATAAN

Saya yang bertanda tangan 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 ini dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 08 Desember 2020


METERAI
TEMPEL
7DEEBAHF806427641
6000
ENAM RIBU RUPIAH
Crishariansyah
NIM. 16.11.0631

MOTTO

” Bila kaum muda yang telah belajar di sekolah dan menganggap dirinya telalu tinggi dan pintar untuk melebur dengan masyarakat yang berkerja dengan cangkul dan hanya memiliki cita-cita yang sederhana, maka lebih baik pendidikan itu tidak diberikan sama sekali”

(Tan Malaka)

”Semakin aku banyak membaca, semakin aku banyak berpikir, semakin aku banyak belajar, semakin aku sadar bahwa aku tak mengetahui apa pun.”

(Voltaire)

”Belajar tentang pikiran dan ilmu pengetahuan, tanpa belajar untuk memperkaya hati sama dengan tak belajar apa-apa.”

(Aristoteles)

”Menghina tuhan tak perlu dengan umpatan dan membakar kitab sucinya, khawatir besok kamu tidak bisa makan saja itu sudah menghina tuhan”

(Sujiwo Tejo)

”Ijazah itu tanda orang pernah sekolah, bukan tanda orang pernah berfikir”

(Rocky Gerung)

PERSEMBAHAN

Alhamdulillahrabbi`alamin.

Segala puji bagi Allah SWT Tuhan Semesta Alam atas berkah, rahmat dan hidayah-Nya untuk kelancaran penulisan ini dan juga waktu serta kesempatan untuk merasakan indahnya kehidupan. Junjungan besar Nabi Muhammad SAW yang telah menjadi suri tauladan bagi Saya dalam menjalani hidup.

Perjalanan selama lebih dari 4 tahun telah mencapai tahap ini, tahap dimana saya berhasil naik satu tingkat dalam jenjang akademik. Pencapaian ini tidak lepas dari dukungan dan panjatan doa dari orang-orang luar biasa yang berada di sekeliling Saya tentunya. Dengan bangga dan tidak mengurangi rasa hormat serta terimakasih sedalam-dalamnya kepada:

1. Kedua Orang Tua saya ibu (Lily Hermita) dan Bapak (Jamilus) serta Almarhum ayah saya (Jonedi), yang sangat berarti untuk saya. Saya ucapkan ribuan Makasih atas support dan dukungannya sehingga saya dapat menyelesaikan pendidikan Strata I saya. Mungkin hal ini tak sebanding dengan apa yang telah kalian lakukan dan berikan kepada saya.
2. Teruntuk Kakek (Amrin) dan Nenek (Rohana) yang telah mengasuh dan mendidik Saya sejak kecil, Saya ucapkan ribuan makasih untuk semuanya yang telah kalian berikan kepada Saya, mungkin tak banyak kata yang saya tulis karna tak sebanding dengan yang kalian lakukan.
3. Saudara yang Saya sayangi Liza anjelina, Nur Fadilla. Karna kalian adalah penyemangat untuk terus cepat menyelesaikan pendidikan ini.
4. Keluarga besar saya, sepupu-sepupu saya yang selalu memberikan dukungan kepada saya.
5. Dosen Pembimbing Ibu Nila Feby Puspitasari, terimakasih atas bimbingan dan waktu yang telah ibu berikan kepada saya selama ini, sehingga saya

bisa dapat menyelesaikan skripsi ini. Terimakasih juga atas semua kebaikan yang telah ibu berikan kepada saya selama ini dan sabar dalam membimbing saya.

6. Keluarga besar Mayapala, walaupun saya tidak menyelesaikan pendidikan saya sebagai anggota tetap akan tetapi ilmu yang telah kalian berikan sangatlah berarti baik itu bersifat teoritis maupun empiris.
7. Keluarga besar IKPM Sumatra Barat, terimakasih atas pengalaman dan tukar pikiran terkait kampung halaman.
8. Keluarga besar IPPSA, baik yang di cabang (yogyakarta) atau pun yang dipusat, yang tidak dapat disebut satupersatu, terima kasih kerja samanya dan pengalamannya.
9. Keluarga besar Asrama, terimakasih juga atas support yang telah diberikan dan jadi tempat keluh kesah(Ari Polo, Fauzan, Hafiz, Dzaki, Yusri, uda ju, uda addi, uda ul, ilek)
10. Keluarga besar GMI 1930, terimakasih atas ilmu yang telah diberikan ketika diskusi setiap malam minggu (direktur utama: uda Addi arrahman, auliah rahmat, uda juharmen dan, yang lain-lain) semoga menjadi amal jariyah dan ilmu yang diberikan dapat bermanfaat bagi kehidupan saya selanjutnya.
11. Keluarga Besar Rose House Squad dan 16IF10 terima kasih untuk semuanya.(abed prayoga, vicky, bagus, dan lain-lain yang tak dapat ditulis satu-persatu).
12. Dosen-dosen Amikom yang telah memberikan ilmu dalam 4 tahun terakhir ini, semoga menjadi amal jariyah dan ilmu yang diberikan dapat bermanfaat bagi kehidupan saya selanjutnya.
13. terimakasih banyak kepada 3 orang ini (Andi Mashar/pahe, Muhammad ilham/ilek) yang banyak jasanya dalam perjalanan hidup saya hingga dapat menyelesaikan perkuliahan ini.
14. Dan terima kasih untuk semua yang tak dapat dituliskan satu persatu.

KATA PENGANTAR

Puji syukur saya ucapkan kehadirat Tuhan Yang Maha Kuasa atas limpahan berkah-Nya sehingga penulis dapat menyelesaikan laporan Penelitian Skripsi berjudul “Aplikasi *Notifikasi Alert Intrusion Detection System (IDS)* Pada Email Untuk *Reporting* Keamanan Jaringan (Studi Kasus : Wisma Gunung Merah)“.

Pengajuan skripsi ini ditujukan sebagai pemenuhan kelulusan pada jenjang perkuliahan Strata I Universitas Amikom Yogyakarta. Melewati penyusunan skripsi ini tentunya tidak terlepas dari hambatan, tantangan serta kesulitan, namun karena binaan dan dukungan dari semua pihak, akhirnya semua hambatan tersebut dapat teratasi.

Dalam penulisan skripsi ini tentunya penulis sadar akan banyak ditemukan kekurangan pada laporan ini, baik itu dari segi kualitas maupun dari segi kuantitas bahan observasi yang penulis tampilkan. Selanjutnya penulis mengucapkan terimakasih yang sebanyak-banyaknya kepada segenap pihak yang telah memberikan dukungan, baik itu berupa bantuan, doa maupun dorongan dan beragam pengalaman selama proses penyelesaian penulisan skripsi ini.

Akhir kata, semoga semua bantuan yang telah diberikan oleh segenap pihak dapat menjadi ladang kebaikan. Dan semoga skripsi ini dapat memberikan manfaat.

Yogyakarta, 08 Desember 2020

Penulis



Crishariansyah

Daftar Isi

PERSETUJUAN	I
PENGESAHAN	II
PERNYATAAN.....	III
MOTTO	IV
PERSEMBAHAN.....	V
KATA PENGANTAR	VII
DAFTAR ISI.....	VIII
DAFTAR TABEL.....	XII
DAFTAR GAMBAR	XIII
INTISARI.....	XVI
ABSTRACT.....	XVII
BAB I PENDAHULUAN.....	1
1.1 LATAR BELAKANG	1
1.2 RUMUSAN MASALAH	2
1.3 BATASAN MASALAH	3
1.4 MAKSUD DAN TUJUAN PENELITIAN	3
1.4.1 Maksud.....	3
1.4.2 Tujuan.....	4
1.5 MANFAAT PENELITIAN.....	4
1.6 METODE PENELITIAN	5
1.6.1 Metode Pengumpulan Data	5
1.6.2 Metodologi Pengembangan Jaringan	5
1.7 SISTEMATIKA PENULISAN	6
BAB II LANDASAN TEORI.....	8

2.1	KAJIAN PUSTAKA.....	8
2.2	DASAR TEORI.....	10
2.2.1	Definisi Jaringan Komputer	10
2.2.2	Jenis Jaringan Komputer	10
2.2.3	Jenis Koneksi Jaringan Komputer.....	11
2.2.4	Intrusion Detection System	12
2.2.5	Tipe Intrusion Detection System.....	13
2.2.6	Pendekatan Intrusion Detection System.....	13
2.2.7	Passive Intrusion Detection System.....	14
2.2.8	Reactive Intrusion Detection System	14
2.2.9	Arsitektur Intrusion Detection System.....	15
2.2.10	Pengendalian Intrusion System	15
2.2.11	Waktu	16
2.2.12	Mikrotik.....	16
2.2.13	Firewall.....	17
2.3	PENGERTIAN DESAIN	19
2.4	INTERNET	19
2.5	ETHERNET 802.3	19
2.6	PROTOKOL	20
2.7	REFRENSI MODEL OSI.....	20
2.8	REFRENSI MODEL DOD (TCPIP).....	21
2.8.1	Layar 4 Application.....	21
2.8.2	Layar 3 Transport.....	21
2.8.3	Layar 2 Internet	21
2.8.4	Layar 1 Network Interface	22
2.9	IP ADDRESS	22
2.10	KEAMANAN KOMPUTER.....	23
2.11	KEBIJAKAN KEAMANAN JARINGAN.....	24
2.12	ASPEK-ASPEK KEAMANAN JARINGAN	25
2.12.1	Interupsion.....	25
2.12.2	Intercaption.....	25

2.12.3 Medification	25
2.12.4 Febrication.....	25
2.13 PORT	26
2.14 NETWORK DEVELOPMENT LIFE CYCLE (NDLC)	26
BAB III ANALISIS DAN PERANCANGAN	29
3.1 TINJAUAN UMUM.....	29
3.2 TAHAPAN ANALISIS	29
3.2.1 Pengumpulan Data	30
3.2.2 Indentifikasi Masalah	33
3.2.3 Analisis Masalah	34
3.2.4 Hipotesis Solusi.....	35
3.3 TAHAPAN/METODOLOGI PENGEMBANGAN JARINGAN	36
3.3.1 Analisis Kebutuhan	36
3.3.2 Kebutuhan Fungsional.....	36
3.3.3 Kebutuhan Non-Fungsional	37
3.4 DESIGN DAN PERANCANGAN SISTEM (DESIGN)	41
3.4.1 Rancangan Intrusion Detection System	41
3.4.2 Gambaran Umum Sistem	42
3.4.3 Rancangan Alur Kerja IDS	43
3.4.4 Topologi Implementasi IDS	44
3.4.5 Prosedur Implementasi IDS	45
3.4.6 Proses Pendeteksian Serangan	46
3.4.7 Proses Sistem Keseluruhan	46
3.4.8 Prosedur Penjadwalan	47
3.4.9 Perancangan Penempatan Pada Jaringan.....	48
3.4.10 Perancangan Rule Firewall.....	48
BAB IV IMPLEMENTASI DAN PEMBAHASAN	50
4.1 IMPLEMENTASI (IMPLEMENT).....	50
4.2 IMPLEMENTASI TOPOLOGI SISTEM	50
4.3 INSTALASI	51

4.3.1 Instalasi Winbox.....	51
4.4 KONFIGURASI.....	51
4.4.1 Konfigurasi System Tool	51
4.4.2 Konfigurasi IDS	57
4.5 TAHAP PENGUJIAN	69
4.5.1 Fungsionalitas Test.....	70
4.5.2 Respon Time	85
4.6 ANALISA HASIL PENGUJIAN.....	90
4.7 ANALISIS MASALAH	91
4.7.1 Masalah Teknis	91
4.7.2 Masalah Non Teknis.....	92
BAB V PENUTUP.....	93
5.1 KESIMPULAN.....	93
5.2 SARAN.....	94
DAFTAR PUSTAKA	95
LAMPIRAN.....	96

Daftar Tabel

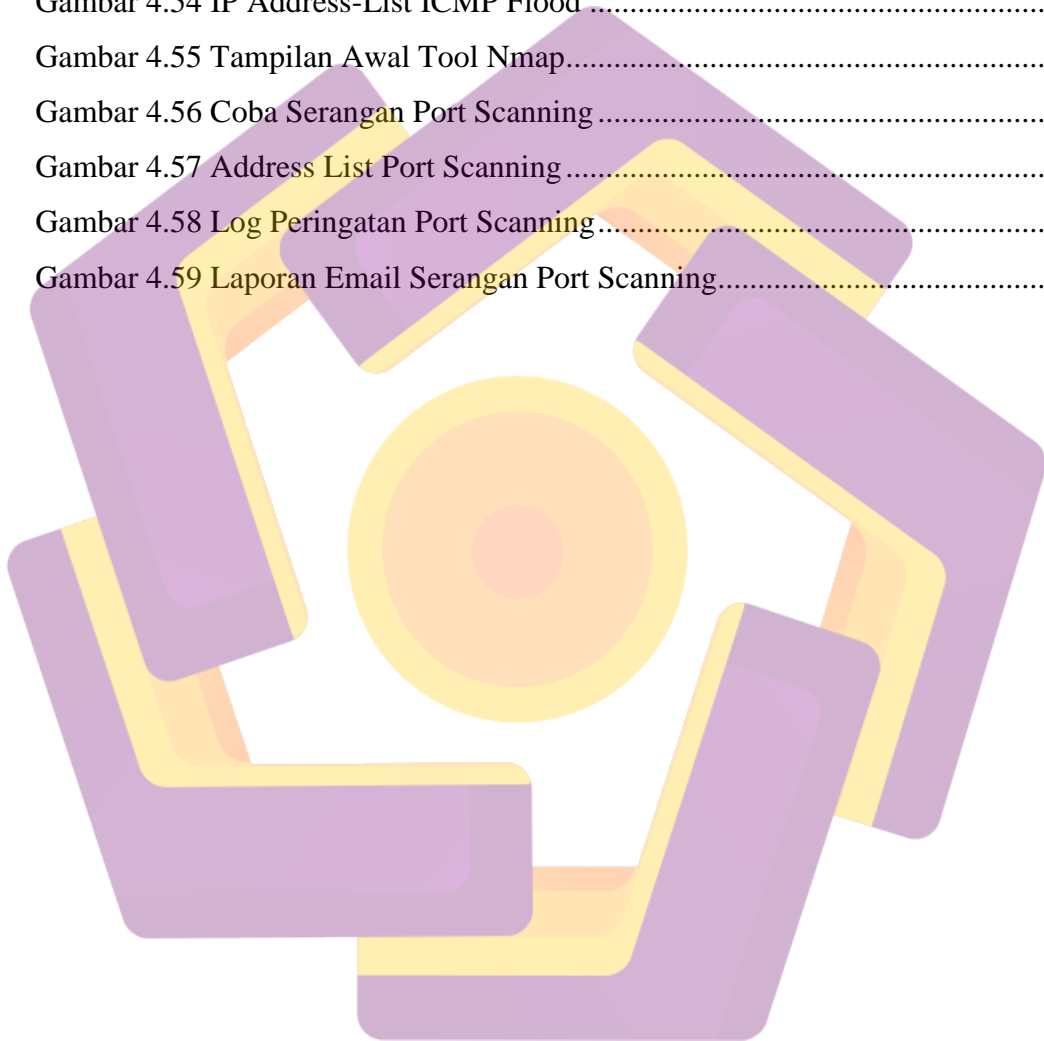
Tabel 2.1 Contoh IP address	22
Tabel 2.2 bagian kelas IP address	23
Tabel 3.1 IP Address Pada Modem ADSL	31
Tabel 3.2 Hasil Observasi Sistem Berjalan.....	32
Tabel 3.3 Spesifikasi Laptop yang dibutuhkan.....	38
Tabel 3. 4 Spesifikasi Routerboard Mikrotik RB941-2nD-TC.....	38
Tabel 4.1 Respon Time Serangan Berurutan FTP Bruteforce	85
Tabel 4.2 Respon Time Serangan Bersamaan FTP Bruteforce.....	86
Tabel 4.3 Respon Time Serangan Berurutan SSH Bruteforce.....	87
Tabel 4.4 Respon Time Serangan Bersamaan SSH Bruteforce	87
Tabel 4.5 Respon Time Serangan Berurutan ICMP Flood	88
Tabel 4.6 Respon Time Serangan Bersamaan ICMP Flood	88
Tabel 4.7 Respon Time Serangan Berurutan Port Scanning.....	89
Tabel 4.8 Respon Time Serangan Bersamaan Port Scanning.....	89
Tabel 4.9 Konfigurasi Sistem.....	90
Tabel 4.10 Pengujian Sistem.....	91

DAFTAR GAMBAR

Gambar 2.1 Logo Mikrotik	17
Gambar 2.2 Generic Firewall dan Hardware Firewall	18
Gambar 2.3 Referensi Model OSI.....	20
Gambar 2.4 Model DOD.....	22
Gambar 2.5 Metode NDLC.....	26
Gambar 3.1 Topologi Jaringan Lama.....	31
Gambar 3.2 Routerboard Mikrotik RB941-2nD-TC.....	38
Gambar 3.3 Gambaran Umum Sistem IDS.....	42
Gambar 3.4 Alur Kerja IDS	43
Gambar 3.5 Topologi Implementasi Jaringan IDS	45
Gambar 3.6 Flowchart Proses Sistem Keseluruhan	47
Gambar 3.7 Prosedur Penjadwalan	48
Gambar 4.1 Konfigurasi System Identity	52
Gambar 4.2 Konfigurasi NTP Client	52
Gambar 4.3 Script Konfigurasi Tools Email.....	53
Gambar 4.4 Konfigurasi Tool Email.....	53
Gambar 4.5 Script Percobaan Pengiriman Email.....	53
Gambar 4.6 Uji Coba Pengiriman Pesan Email	54
Gambar 4.7 Kata Perintah Logging Local	54
Gambar 4.8 Script Menampilkan Log.....	55
Gambar 4.9 Tampilan Logging Local.....	55
Gambar 4.10 Script Intruksi Pengiriman Email.....	56
Gambar 4.11 Konfigurasi Schedule Pengiriman Email	56
Gambar 4.12 Konfigurasi FTP Bruteforce.....	58
Gambar 4.13 Check Rule Firewall FTP.....	58
Gambar 4.14 Hasil Check Rule Firewall FTP	59
Gambar 4.15 Konfigurasi Pengiriman Email FTP_Bruteforce.....	59
Gambar 4.16 Konfigurasi Schedule FTP Bruteforce	60
Gambar 4.17 Konfigurasi SSH Bruteforce	61

Gambar 4.18 check rule firewall SSH.....	61
Gambar 4.19 Hasil Check rule Firewall SSH	62
Gambar 4.20 Script Pengiriman Email SSH Bruteforce	62
Gambar 4.21 schedule SSH Bruteforce	63
Gambar 4.22 Konfigurasi ICMP_Flood.....	64
Gambar 4.23 check rule firewall ICMP Flood.....	64
Gambar 4.24 Hasil Check rule Firewall ICMP Flood	64
Gambar 4.25 Script Pengiriman ICMP_Flood.....	65
Gambar 4.26 Schedule ICMP Flood	66
Gambar 4.27 Konfigurasi Port Scanning	67
Gambar 4.28 check rule firewall Port Scanning	67
Gambar 4.29 Hasil Check rule Firewall Port Scanning	67
Gambar 4.30 Script Pengiriman PortScanning	68
Gambar 4.31 Schedule Port scanning	68
Gambar 4.32 Skenario Pengujian Serangan.....	69
Gambar 4.33 Rule Firewall FTP Bruteforce	71
Gambar 4.34 Tampilan Aplikasi BrutusAET-2	71
Gambar 4.35 Rule Firewall FTP disable.....	71
Gambar 4.36 Uji Coba Serangan FTP Bruteforce	72
Gambar 4.37 Log FTP Bruteforce pada Router	73
Gambar 4.38 Serangan FTP Bruteforce Gagal	73
Gambar 4.39 Email Report FTP Bruteforce	74
Gambar 4.40 Address-List FTP Bruteforce	74
Gambar 4.41 Tampilan Awal Aplikasi Putty	75
Gambar 4.42 Tampilan Rule Firewall SSH	76
Gambar 4.43 IP Target Pennyserangan SSH.....	76
Gambar 4.44 SSH Bruteforce Berhasil	76
Gambar 4.45 Log SSH Bruteforce Pada Router	77
Gambar 4.46 SSH Bruteforce Gagal.....	77
Gambar 4.47 Email Report SSH Bruteforce	78
Gambar 4.48 Address-list SSH Bruteforce	78

Gambar 4.49 ICMP Flood saat firewall disable.....	79
Gambar 4.50 Statistik ICMP Flood Bruffer Size 60000	80
Gambar 4.51 ICMP Flood Gagal	80
Gambar 4.52 Total Size Ping 32 Byte.....	81
Gambar 4.53 Laporan Email ICMP Flood.....	82
Gambar 4.54 IP Address-List ICMP Flood	82
Gambar 4.55 Tampilan Awal Tool Nmap.....	83
Gambar 4.56 Coba Serangan Port Scanning.....	83
Gambar 4.57 Address List Port Scanning.....	84
Gambar 4.58 Log Peringatan Port Scanning.....	84
Gambar 4.59 Laporan Email Serangan Port Scanning.....	84



INTISARI

Perkembangan teknologi dimasa Revolusi industri 4.0 mengalami kemajuan yang sangat pesat, terutama di bagian keamanan data dan jaringan komputer. Seorang administrator jaringan bertugas untuk memastikan jaringan komputer selalu aman dari tindakan penyusupan atau serangan dan memastikan ketersediaan layanan bagi para pengguna, dengan cara melakukan monitoring. Sistem monitoring jaringan pada Wisma Gunung Merah belum ada, sehingga permasalahan yang terjadi pada *server* seperti *FTP server* menjadi lambat untuk ditangani oleh administrator jaringan. Sebab Wisma Gunung Merah masih melakukan pemantauan dan pendeteksian dengan cara manual, oleh karna itu jaringan pada Wisma Gunung Merah masih sangat rentan terhadap intrusi (penyusupan) dari pihak yang tidak bertanggung jawab.

Penelitian ini mengimplementasikan sistem keamanan jaringan menggunakan *Intrusion Detection System (IDS)* dan *firewall* dengan Router Mikrotik serta memanfaatkan aplikasi E-mail sebagai media notifikasi alert pada Wisma Gunung Merah, sehingga Mikrotik akan difungsikan sebagai *IDS* tipe *Network-Based Intrusion Detection System (NIDS)* dan akan dikombinasikan dengan *firewall*. Adapun Email sebagai media pemberitahuan *alert* apabila terjadi serangan yang terdeteksi.

Pengujian sistem dilakukan dengan menggunakan beberapa jenis serangan ke jaringan untuk dapat mengetahui fungsi sistem ini bekerja, dengan memberikan laporan dalam bentuk pesan teks yang dikirim pada Email administrator yang berisi informasi, yaitu alamat IP penyerang, waktu, tanggal dan jenis serangan.

Kata Kunci: Keamanan Jaringan, IDS, Firewall, Mikrotik, Monitoring, Email

ABSTRACT

The development of technology during the Industrial Revolution 4.0 has progressed very rapidly, especially in the section of data security and computer networks. A network administrator is tasked with ensuring the computer network is always safe from intrusions or attacks and ensuring the availability of services for users, by monitoring. The network monitoring system at Wisma Gunung Merah does not exist yet, so the problems that occur in servers such as FTP servers are slow to be handled by network administrators. Because Wisma Gunung Merah still conducts monitoring and detection by manual, therefore the network at Wisma Gunung Merah is still very vulnerable to intrusion from irresponsible parties.

This research implements network security system using Intrusion Detection System (IDS) and firewall with Mikrotik Router and utilizes E-mail application as alert notification media at Wisma Gunung Merah, so mikrotik will function as NETWORK-Based Intrusion Detection System (NIDS) type IDS and will be combined with firewall. The Email as a media alert notification in case of an attack is detected.

System testing is carried out by using several types of attacks to the network to be able to know the function of this system works, by providing a report in the form of a text message sent in the administrator's Email containing information, namely the attacker's IP address, time, date and type of attack.

Keyword: *Network Security, IDS, Firewall, Mikrotik, Monitoring, Email*