

SISTEM INFORMASI PENCARIAN JUDUL SKRIPSI DAN TUGAS AKHIR PADA STMIK TIDORE MANDIRI

Edy Waly Rumaf
STMIK Tidore Mandiri
edy.waly.rumaf@stmik-tm.ac.id

ABSTRAK

Seringkali mahasiswa kesulitan dalam pencarian tema judul skripsi dan tugas akhir serta mendapat kendala dengan beberapa kali mengganti judul skripsi dan tugas akhir. Pengajuan judul kadang diterima dan kadang ditolak berdasarkan pertimbangan yang salah satunya adalah judul yang sudah ada. Tujuan dari penelitian ini adalah membuat perangkat lunak yang dapat melakukan pencarian dan pengecekan judul-judul skripsi dan tugas akhir secara cepat dan akurat. Metode yang digunakan dalam penelitian ini adalah metode pengembangan yaitu bagaimana sistem dikembangkan dari sistem yang manual menjadi sistem yang terkomputerisasi. Dengan aplikasi sistem informasi ini diharapkan dapat memudahkan pengecekan, pencarian dan pengelolaan judul-judul skripsi dan tugas akhir mahasiswa serta menghindari indikasi adanya kesamaan judul dan plagiat.

Kata Kunci: Sistem, Informasi, Cari, Judul, Skripsi, Tugas Akhir

I. PENDAHULUAN

Salah satu persoalan yang dihadapi mahasiswa semester akhir adalah memilih judul untuk skripsi atau tugas akhir mereka. Tak sedikit dari judul yang diajukan mahasiswa ditolak oleh bagian program studi karena sama dengan judul-judul skripsi / tugas akhir mahasiswa sebelumnya. Hal tersebut terjadi karena kurangnya informasi yang didapatkan oleh mahasiswa terkait judul-judul skripsi / tugas akhir yang sudah ada tersebut. Dengan belum adanya aplikasi khusus untuk pencarian dan pengecekan judul skripsi dan tugas akhir itulah yang menjadi penyebab hal tersebut bisa terjadi. Selain itu dengan belum adanya sistem pengelolaan judul skripsi dan tugas akhir yang baik, mengakibatkan bagian program studi kesulitan dan membutuhkan banyak waktu untuk memberikan informasi seputar judul skripsi dan tugas akhir kepada mahasiswa.

Proses pencarian dan penyajian informasi judul skripsi dan tugas akhir yang digunakan bagian program studi saat ini masih secara manual, yaitu dengan membuka berkas dan formulir pengajuan judul yang dikumpulkan dibagian program studi. Oleh karena itu pengelolaan judul skripsi dan tugas akhir perlu ditingkatkan agar lebih efektif dan efisien serta tidak ada lagi judul yang sama. Selain itu mempermudah penyajian informasi judul skripsi dan tugas akhir kepada mahasiswa.

Berdasarkan hal tersebut, maka perlu dibuat aplikasi khusus berbasis sistem informasi yaitu aplikasi pencarian judul skripsi dan tugas akhir yang nantinya akan memiliki kemampuan dalam proses pengelolaan dan penyajian informasi yang lebih baik.

II. TINJAUAN PUSTAKA

A. Sistem Informasi

Menurut Jogiyanto (2005 : 34), mengartikan sistem adalah kumpulan dari komponen-komponen yang saling berhubungan satu dengan yang lainnya membentuk satu kesatuan untuk mencapai tujuan tertentu. Contoh sistem yang didefinisikan dengan pendekatan komponen adalah sistem komputer yang didefinisikan sebagai kumpulan dari perangkat keras dan perangkat lunak. Sedangkan informasi menurut Whitten (2004 : 27) adalah data yang telah diproses atau disusun kedalam suatu format sehingga lebih berarti untuk seseorang. Informasi dibentuk dari kombinasi dari data yang dengan penuh harapan dapat mempunyai arti bagi penerimanya. Informasi harus bebas dari kesalahan-kesalahan dan tidak biasa atau menyesatkan serta jelas mencerminkan maksudnya. Ketidakakuratan dapat terjadi karena sumber informasi (data) mengalami gangguan atau kesenjangan sehingga merusak atau merubah data-data asli tersebut.

B. Pencarian Judul

Pengertian pencarian menurut Kamus Besar Bahasa Indonesia *online*, adalah proses, cara atau perbuatan mencari. Sedangkan judul adalah nama yang dipakai untuk buku atau bab dalam buku yang dapat menyiratkan secara pendek isi atau maksud buku atau bab itu.

C. Skripsi / Tugas Akhir

Menurut Kamus Besar Bahasa Indonesia *online*, Skripsi / Tugas Akhir adalah karangan ilmiah yang wajib ditulis mahasiswa sebagai bagian dari persyaratan akhir pendidikan akademisnya. Sedangkan menurut Wikipedia Indonesia Skripsi / Tugas Akhir adalah istilah yang digunakan di Indonesia untuk mengilustrasikan suatu karya tulis ilmiah berupa paparan tulisan hasil penelitian sarjana S1 yang membahas suatu permasalahan atau fenomena dalam bidang ilmu tertentu dengan menggunakan kaidah-kaidah yang berlaku.

III. METODE PENELITIAN

Adapun metode penelitian yang digunakan adalah metode pengembangan, yaitu bagaimana sistem dikembangkan dari sistem yang manual menjadi sistem yang terkomputerisasi pada bagian program studi Sistem Informasi STMIK Tidore Mandiri.

A. Waktu dan Lokasi Penelitian

Waktu pelaksanaan penelitian ini dilakukan mulai dari bulan Desember 2018 sampai dengan bulan Januari 2019 dan berlokasi di kampus STMIK Tidore Mandiri.

B. Jenis Penelitian

Jenis penelitian yang digunakan dalam penelitian ini adalah penelitian deskriptif analitis, yaitu mengumpulkan data-data sebenarnya kemudian disusun, diolah dan dianalisis untuk mendapatkan gambaran dan kejelasan persoalan yang akan diselesaikan. Setelah mendapatkan kerangka kerja yang tepat maka selanjutnya dilakukan proses pembuatan aplikasi dengan metode pengembangan, yaitu mengembangkan sistem manual yang sedang berjalan menjadi sistem yang terkomputerisasi.

C. Instrumen Penelitian

Instrumen atau alat yang digunakan dalam penelitian ini terdiri dari perangkat keras komputer yaitu *laptop* dan untuk pembuatan aplikasi menggunakan perangkat lunak yang terdiri dari bahasa pemrograman PHP dan aplikasi manajemen database MySQL. Sedangkan untuk mengolah data dan pembuatan laporan menggunakan aplikasi Microsoft Office.

D. Tahapan Penelitian

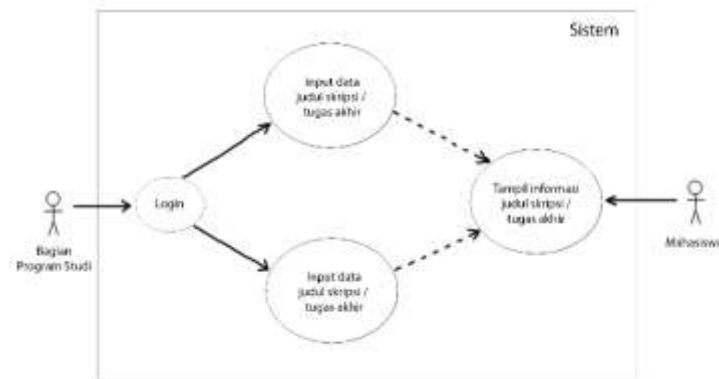
Secara garis besarnya, tahapan-tahapan penelitian yang dilakukan dalam perancangan dan pembuatan aplikasi sistem informasi ini adalah sebagai berikut.

1. Analisis Kebutuhan Sistem.
2. Rancangan Model Sistem.
3. Rancangan Sistem Aplikasi.

E. Analisis Kebutuhan Sistem

Pada tahap ini dilakukan analisis terhadap kebutuhan sistem dan *use case diagram* serta spesifikasi yang dibutuhkan oleh sistem. Fungsi-fungsi yang dibutuhkan dalam aplikasi ini adalah sebagai berikut.

1. Fungsi untuk Bagian Program Studi yaitu input data judul skripsi / tugas akhir dan data dosen pembimbing.
2. Fungsi untuk Mahasiswa yaitu melihat informasi judul skripsi / tugas akhir.



Gambar 1. Use Case Diagram Aplikasi Pencarian Judul Skripsi dan Tugas Akhir

IV. HASIL DAN PEMBAHASAN

Hasil dari penelitian ini adalah berupa sebuah aplikasi pencarian judul skripsi dan tugas akhir mahasiswa berbasis web pada kampus STMIK Tidore Mandiri. Aplikasi ini terdiri dari 2 tampilan, yaitu tampilan untuk bagian program studi dan tampilan untuk mahasiswa.

A. Aplikasi untuk Bagian Program Studi

Aplikasi untuk bagian program studi digunakan untuk mengelola data informasi judul skripsi dan tugas akhir serta data dosen pembimbing judul tersebut. Tampilan aplikasi untuk Bagian Program Studi dapat dilihat pada gambar berikut ini.



Gambar 2. Tampilan Halaman Login Untuk Bagian Program Studi



Gambar 3. Tampilan Menu Admin Bagian Program Studi

 STMIK TIDORE MANDIRI St. Tidar Jalan Widyadarmas No. 33, Mt. Gunungrejo, Kota Tidore Kepulauan				
Daftar Judul Skripsi dan Tugas Akhir				
Kembali		Tambah Judul		Cari Judul atau Nama
No.	NPM	Nama	Judul	Setting
1.	6001114000	Ahmad Fauzi Hutan	Sistem Informasi Perpustakaan Motor Sepeda Kiroki Pada Dealer Soudara	Detail Ubah Hapus
2.	6001114000	Sukartika Arson	Sistem Informasi Akutansi Desa Berbasis Web Di Kecamatan Oba Utara Kota Tidore Kepulauan	Detail Ubah Hapus
3.	6001114000	Hermani Taki	Sistem Informasi Pengawasan Pemeliharaan Daerah pada Satuan Kecamatan Sat Penanahan Mndol Provda Maluku Utara	Detail Ubah Hapus
4.	6001114000	Ayu Dwiatika Wihari	Sistem Informasi Akutansi Perawatan Ruang Dengan Konsep Perpustakaan Menggunakan Metode HOTSUPD	Detail Ubah Hapus
5.	6001114000	Erhan Yusuf	Penerangan Sistem Informasi RSM STMIK Tidore Mandiri	Detail Ubah Hapus
6.	6001114000	M Rudi Hakim	Analisa Anggaran Berbasis Energi Daerah Kota Tidore Kepulauan Berbasis Visual Basic	Detail Ubah Hapus
7.	6001114000	Roswanti Lufri	Penerangan Aplikasi Promosi dan Pembelian Jajanan Motor pada Diler Honda di Kota Tidore Kepulauan	Detail Ubah Hapus
8.	6001114000	Ahrii Anan	Aplikasi Pengiriman Data dan Auditasi pada Sistem Jaringan Internet Kota Tidore Kepulauan Berbasis Web	Detail Ubah Hapus
9.	6001114000	Alexis Anissa	Penerangan Sistem Informasi Pendaftaran Peserta Ujian Nasional Taghat Sekolah Dasar Pada Kantor Dinas Pendidikan Pemuda dan Olahraga Kota Tidore Kepulauan	Detail Ubah Hapus
10.	6001114000	Marta Isara	Penerangan Aplikasi Berbasis Multimedia Flash Dalam Proses Pendidikan Kalsidaryan Indonesia Untuk	Detail Ubah Hapus

Gambar 4. Tampilan Daftar Judul Skripsi dan Tugas Akhir

 STMIK TIDORE MANDIRI St. Tidar Jalan Widyadarmas No. 33, Mt. Gunungrejo, Kota Tidore Kepulauan	
Tambah Judul Skripsi dan Tugas Akhir	
Kembali	
NPM	
Nama	
Judul	
Daftar Pendaftaran 1	+
Daftar Pendaftaran 2	+
Tampilkan Data Kembali	

Gambar 5. Halaman Tambah Judul Skripsi dan Tugas Akhir

 STMIK TIDORE MANDIRI St. Tidar Jalan Widyadarmas No. 33, Mt. Gunungrejo, Kota Tidore Kepulauan	
Ubah Judul Skripsi dan Tugas Akhir	
Kembali	
NPM	6001114000
Nama	Ahmad Fauzi Hutan
Judul	Sistem Informasi Perpustakaan Motor Sepeda Kiroki Pada Dealer Soudara
Daftar Pendaftaran 1	Ahmad Fauzi, S.P., M.Ang
Daftar Pendaftaran 2	Randi Salsos, S.Pd., M.Pd
Tampilkan Data Kembali	

Gambar 6. Halaman Ubah Judul Skripsi dan Tugas Akhir

dan Tugas Akhir - Mozilla Firefox

Page 11 of 24

Print Landscape

Close

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
STMIK TIDORE MANDIRI
 Jln. Sultan Zainal Abidin Syah No. 25 Kel. Gamtuffange

Daftar Judul Skripsi dan Tugas Akhir

No.	NPM	Nama Lengkap	Judul	Pembimbing I	Pembimbing II
1	6301114005	AHMAD FAUZI HASAN	Sistem Informasi Penjualan Motor Secara Kredit Pada Dealer Soodara	Amal Khairan, ST., M.Eng	Ramli Selasa, S.Pd., M.Pd
2	6301113006	HAMDAN TULUJI	Sistem Informasi Pengawasan Perusahaan Daerah pada Badan Koordinasi dan Penanaman Modal Provinsi Maluku Utara	Prof. Dr. Ir. H. M. Tola, M.Eng	Dr. Mashur Razak, SE, MM
3	6301113005	AYU DINATIKA IDHAM	Sistem Informasi Akuntansi Persediaan Barang Dengan Konsep Penjualan Menggunakan Metode FIFO/LIFO	Dr. Mashur Razak, SE., MM	Separudin, S.Kom., M.Kom
4	6301113001	ERKAN YUSUF	Perancangan Sistem Informasi BEM STMIK Tidore Mandiri	Dr. Mashur Razak, SE., MM	Sri Damayanti, S.Si., M.Sc
5	6301112007	M RIZAL HAKIM	Analisis Anggaran Berbasis Kinerja Daerah Kota Tidore Kepulauan Berbasis Visual Basic	-	-
6	6301112006	RISWANTO SAFAR	Perancangan Aplikasi Promosi dan Pembeban Sepeda Motor pada Dealer Honda di Kota Tidore Kepulauan	-	-
7	6301112004	FAHRI AMIN	Aplikasi Pengolahan Data Iklan Usaha Jasa Konstruksi Pada Dinas pekerjaan Umum Kota Tidore Kepulauan Berbasis Web	-	-
8	6301112003	ARWIS AMMA	Perancangan Sistem Informasi Pendaftaran Peserta Ujian Nasional Tingkat Sekolah Dasar Pada Kantor Dinas Pendidikan Pemuda dan Olahraga Kota Tidore Kepulauan	-	-
9	6301112001	MUTIA KRAM	Perancangan Aplikasi Berbasis Multimedia Flash Dalam Proses Pembelajaran Kebulayaan Indonesia Untuk Stowit Tingkat Sekolah Dasar	-	-

Gambar 7. Tampilan Laporan Judul Skripsi dan Tugas Akhir

B. Aplikasi untuk Mahasiswa

Aplikasi untuk mahasiswa digunakan untuk mencari informasi judul skripsi / tugas akhir. Tampilan aplikasi untuk mahasiswa dapat dilihat pada gambar 3.

STMIK TIDORE MANDIRI
 Jln. Sultan Zainal Abidin Syah No. 25, Kel. Gamtuffange, Kota Tidore Kepulauan

Sistem Informasi Pencarian Judul Skripsi dan Tugas Akhir

(Silahkan pilih kata kunci (contoh : Sistem, gis, pengolahan data))

Masukkan kata kunci

CARI JUDUL

Gambar 8. Tampilan Aplikasi Pencarian Judul Skripsi / Tugas Akhir Untuk Mahasiswa



Gambar 9. Tampilan Hasil Pencarian Judul Skripsi / Tugas Akhir Untuk Mahasiswa

V. KESIMPULAN

Berdasarkan hasil penelitian maka dapat disimpulkan bahwa aplikasi sistem informasi ini dapat berjalan dengan baik dan diharapkan dapat memudahkan pengecekan, pencarian dan pengelolaan judul-judul skripsi dan tugas akhir mahasiswa, serta menghindari indikasi adanya kesamaan judul dan plagiat.

REFERENSI:

- [1] Eko R, 2000. **Manajemen Sistem Informasi dan Teknologi Informasi**. Jakarta: PT Elex Media Komputindo.
- [2] Jogiyanto H. M, 2003. **Sistem Teknologi Informasi**. Yogyakarta: Andi Offset.
- [3] Sutanta E, 2003. **Sistem Informasi Manajemen**. Edisi pertama, Yogyakarta: Graha Ilmu.
- [4] Sutedjo B, 2002. **Perencanaan dan Pembangunan Sistem Informasi**. Yogyakarta: Andi Offset.
- [5] Anonymous, 2019. **Skripsi** (Online). (<https://kbbi.web.id/skripsi>). Diakses 18 Januari 2019
- [6] Anonymous, 2019. **Skripsi** (Online). (<https://id.wikipedia.org/wiki/Skripsi>). Diakses 18 Januari 2019
- [7] Anonymous, 2019. **Judul** (Online). (<https://kbbi.web.id/judul>). Diakses 18 Januari 2019

SISTEM PENCEGAHAN GANGGUAN JARINGAN KOMPUTER BERBASIS DETEKSI POLA SNORT

Said D. Bahta

STMIK Tidore Mandiri

said.baht4@gmail.com

ABSTRAK

Karena keterbatasan firewall dan sistem pendeteksi gangguan jaringan, kami membahas dalam makalah ini tentang sistem pencegahan gangguan jaringan, yang merupakan pendekatan baru di bidang keamanan jaringan. Kami membuat sebuah daemon yang bertindak sebagai sistem pencegahan yang berjalan di GNU/Linux. Sistem pencegahan ini telah diuji terhadap serangan XSS (Cross Side Scripting), scanning dan serangan DDOS . Hasilnya, ketiga jenis serangan tersebut berhasil dicegah.

Kata kunci : sistem pencegahan gangguan jaringan, snort, firewall

I. PENDAHULUAN

Gangguan jaringan sering terjadi dalam jaringan. Ketika firewall digunakan untuk melindungi jaringan, rule firewall sangat mudah diakali, menyebabkan kerentanan jaringan yang dilindungi masih tetap tinggi. Alasan utama masalah ini adalah karena keterbatasan firewall untuk mendeteksi dan membedakan antara paket normal dengan paket gangguan jaringan. Firewall hanya dapat membuat keputusan berdasarkan aturan statis yang diatur oleh administrator jaringan.

Selain firewall, sistem pendeteksi gangguan jaringan juga merupakan salah satu alat yang sering digunakan untuk melindungi jaringan terhadap gangguan jaringan. Sayangnya, sistem pendeteksi gangguan jaringan juga memiliki keterbatasan untuk memblokir paket yang dideteksi sebagai paket gangguan. Dengan kata lain, sistem pendeteksi gangguan jaringan sama seperti kamera. Kamera hanya bisa merekam, tapi tidak dapat melakukan pencegahan.

Masalah di atas, membawa kami pada pertanyaan. Yang mana, salah satu dari dua sistem tersebut yang harus digunakan untuk melindungi jaringan terhadap paket gangguan jaringan?

Kita bisa saja memilih firewall atau sistem pendeteksi gangguan jaringan berdasarkan kebutuhan jaringan. Jika kebutuhan jaringan adalah untuk meminimalkan gangguan jaringan, firewall mungkin menjadi pilihan terbaik. Di sisi lain, sistem pendeteksi gangguan baiknya digunakan ketika kebutuhan jaringan adalah untuk pemantauan dan pencatatan gangguan. Namun, kedua pilihan tersebut bukan merupakan pilihan yang ideal, karena itu kami mengusulkan sistem pencegahan gangguan yang mampu memantau juga memiliki mekanisme pencegahan. Kontribusi kami dalam penelitian ini adalah sebagai berikut:

1. Kami membuat sebuah daemon pada sistem operasi GNU/Linux yang berfungsi sebagai sistem pencegahan gangguan jaringan. (Halaman 2)
2. Kami melakukan pengujian deteksi gangguan jaringan menggunakan tiga jenis gangguan, scanning (nmap), XSS (Cross Side Scripting), dan DDOS (hping). (Halaman)

3. Kami melakukan tes pencegahan serangan dengan membandingkan aktivitas koneksi saat server berjalan dengan sistem pencegahan dibandingkan dengan saat server berjalan tanpa sistem pencegahan. (Halaman 4)

II. PENELITIAN TERKAIT

Penelitian ini, termotivasi oleh beberapa penelitian yang dilakukan oleh peneliti sebelumnya. Beberapa penelitian terkait sebagai berikut :

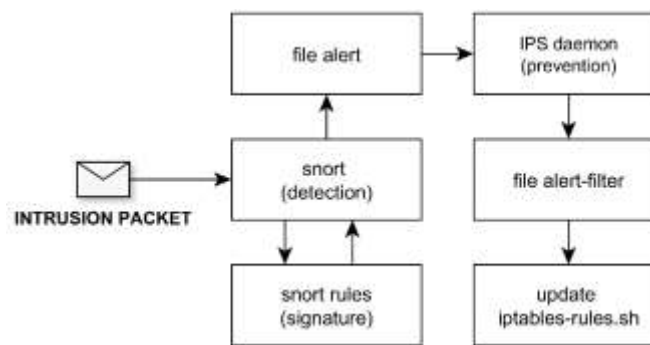
1. Sistem Pemantauan & Pengaturan Firewall Jaringan Komputer berbasis IDS - 2013 [1]
Dalam penelitian ini, peneliti membuat pendeteksi gangguan jaringan yang menyimpan peringatan ke dalam sistem basis data menggunakan snortbase. Selain itu, peneliti juga membuat antarmuka untuk menambahkan aturan firewall secara manual.
2. Penelitian pada sistem pencegahan gangguan jaringan berbasis Snort - 2011 [2]
Dalam penelitian ini, peneliti membuat sistem pencegahan gangguan jaringan dengan menggabungkan snort dan IPSec, yang berjalan pada sistem operasi keluarga Windows.
3. Real Time Analisis Performa Sistem Pendeteksi dan Pencegahan menggunakan Snort - 2012 [3]
Dalam penelitian ini, peneliti menganalisis kinerja snort sebagai sistem pendeteksi gangguan jaringan. Pada akhir jurnal peneliti menyimpulkan dengan saran untuk meletakkan fitur iptables pada snort.
4. Membuat Platform Sebuah Standar untuk Semua Sistem Pendeteksi/Pencegahan - 2010 [4]
Dalam penelitian ini, peneliti mengembangkan dan mengusulkan platform sebagai standar untuk sistem pendeteksi gangguan jaringan dan sistem pencegahan gangguan jaringan.
5. Sistem Pencegahan gangguan Cerdas berbasis Snort - 2010 [5]
Dalam penelitian ini, peneliti mengembangkan sistem pencegahan gangguan yang dikombinasikan dengan SVM (Support Vector Machine) untuk meningkatkan akurasi deteksi.

III. PERANCANGAN DAN PENGUJIAN

Sistem pencegahan gangguan jaringan dalam penelitian ini adalah penggabungan firewall (iptables) dengan sistem pendeteksi gangguan (snort).

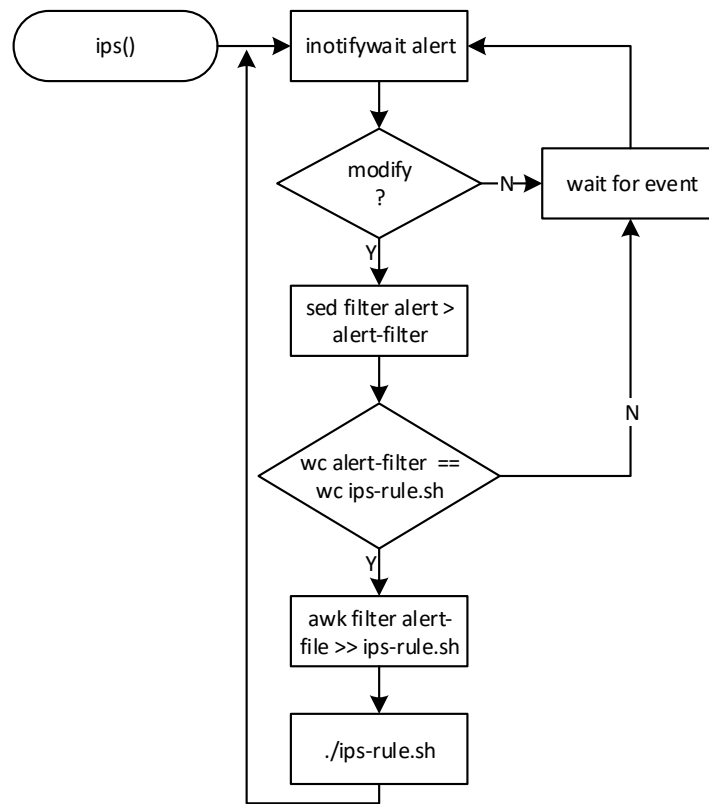
A. Sistem Pencegahan Gangguan Jaringan (daemon)

Grafik berikut merupakan siklus bagaimana sistem pencegahan gangguan jaringan bekerja:



Gambar III - 1 siklus sistem pencegahan gangguan

1. Paket masuk
2. Ketika snort mendeteksi paket yang masuk sebagai paket gangguan, alarm (alert) akan secara otomatis menghasilkan peringatan dalam bentuk teks ascii disimpan dalam file peringatan. Daemon kemudian mengekstrak alamat IP sumber dari paket yang dianggap sebagai paket gangguan.
3. Setelah mendapatkan alamat sumber paket gangguan, daemon juga akan secara otomatis membuat rule firewall pada CHAIN iptables untuk mencegah semua paket datang dari alamat yang dianggap sebagai alamat paket gangguan tersebut.



Gambar III-2 sistem pencegahan gangguan

Masalahnya sebelumnya, berupa rule statis firewall, sekarang dapat berubah secara real time bergantung pada hasil deteksi snort.

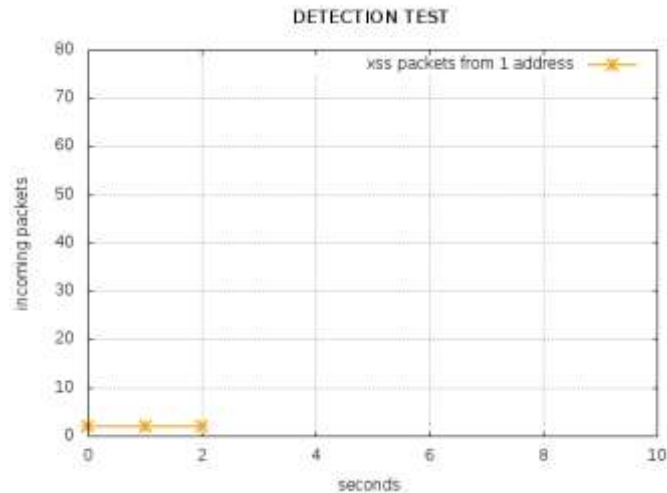
B. Pengujian Sistem Pencegahan Gangguan Jaringan

Sementara pengiriman paket data gangguan dikirimkan, sistem pencegahan mendeteksi paket gangguan dan memberikan peringatan berdasarkan rule bawaan snort.

Pengujian pertama, kami mengirim serangan XSS ke server. Proses pengiriman membutuhkan waktu 3 detik, Pada detik ke 0, snort mendeteksi 2 paket bersumber dari 192.168.137.4 ke alamat tujuan 192.168.137.3. Paket dikirimkan menggunakan protokol TCP. Selanjutnya, pada detik ke 1 snort mendeteksi dua paket lagi yang berasal dari alamat yang sama 192.168.137.4 menuju ke tujuan yang sama 192.168.137.3, juga menggunakan protokol TCP. Pada detik ke 3, snort mendeteksi dua paket yang berasal dari sumber yang sama ke tujuan yang sama. Tabel dan grafik di bawah ini menggambarkan paket gangguan serangan XSS.

Tabel III-1 hasil pantauan paket XSS

Alamat Sumber	Alamat Tujuan	Port	Protokol	Total Packet
192.168.137.4	192.168.137.3	80	TCP	6 packet

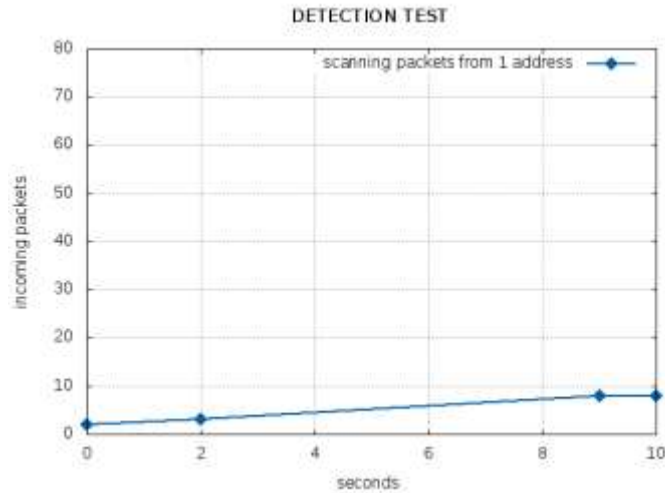


Gambar III-1 hasil pantauan paket XSS

Pengujian kedua, kami mengirimkan serangan pemindaian menggunakan nmap ke server. Proses pengiriman paket memakan waktu 10 detik . Paket pengiriman yang berasal dari alamat 192.168.137.4 ke 192.168.137.3 sebagai alamat server. Dalam detik ke 0, snort mendeteksi 2 paket TCP mencoba mengakses port 3128 dan 8080. Pada detik ke 2, snort mendeteksi 3 paket TCP mencoba mengakses port 1080, 705 dan 161. Pada detik ke 9 juga ke 10, snort mendeteksi empat paket ICMP dan empat paket TCP yang mencoba mengakses port 22, 8, 5, dan 1. Tabel dan grafik berikut adalah karakteristik dari paket scanning menggunakan nmap.

Tabel III-2 hasil pantauan paket scanning

Source address	Destination address	Port	Protocol	Total Packet
192.168.137.4	192.168.137.3	1, 5, 8, 22, 161, 705, 1080, 3128, 8080	TCP ICMP	21 packet

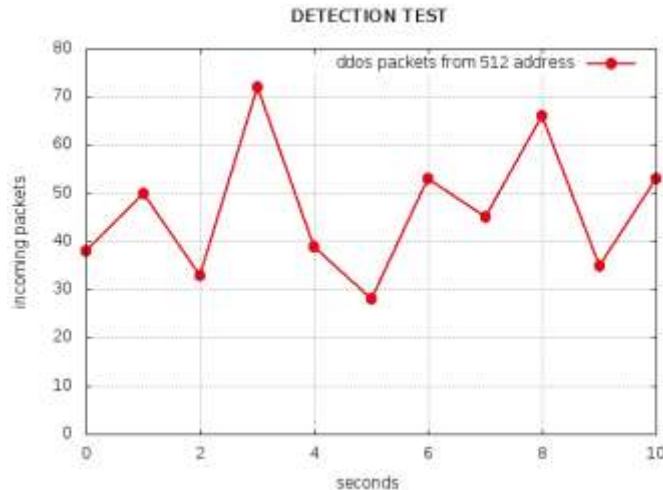


Gambar III-2 hasil pantauan paket scanning

Pengujian ketiga kami mengirimkan paket serangan DDOS ke server menggunakan hping3. Pengiriman paket dilakukan selama 10 detik dari 512 alamat sumber ke alamat tujuan 192.168.137.3. Pada 0 detik, snort mendeteksi 38 paket TCP menargetkan port 80. Pada detik ke 1, snort mendeteksi 50 paket TCP menargetkan port 80. Pada detik 2, snort mendeteksi 33 paket TCP menargetkan port 80. Pada detik 3, snort mendeteksi 72 paket TCP juga menargetkan port 80. Pada detik ke 3, snort mendeteksi 39 paket TCP menargetkan port 80. Pada detik ke 5, snort mendeteksi 28 paket TCP menargetkan port 80. Pada detik ke 6, snort mendeteksi 53 paket TCP menargetkan port 80. Pada detik ke 7, snort mendeteksi 45 paket TCP menargetkan port 80. Pada detik ke 8, Snort mendeteksi 66 paket TCP menargetkan port 80. Pada detik ke 9, snort mendeteksi 35 paket TCP menargetkan port 80. Akhirnya, pada detik 10, snort mendeteksi 53 paket TCP menargetkan port 80. Tabel dan grafik di bawah ini adalah paket intrusi serangan DDOS, pemantauan selama pengujian.

Tabel III-3 hasil pantauan paket DDOS

Alamat Sumber	Alamat Tujuan	Port	Proto kol	Total Packet
111.212.228.89 and 511 another address	192.168.137.3	80	TCP	512 packet



Gambar III-3 hasil pantauan paket DDOS

C. Pencegahan

Kami juga melakukan uji coba pencegahan. Pada saat pengiriman paket, kami secara bersamaan mengirimkan permintaan ICMP untuk memverifikasi koneksi yang telah terjadi antara server dan komputer yang mengirim paket gangguan. Pengujian pencegahan dilakukan dalam dua kondisi. Pertama, ketika server dijalankan dengan menggunakan daemon sistem pencegahan dan kondisi saat server berjalan tanpa sistem pencegahan. Tujuannya adalah untuk melihat keberhasilan pencegahan.

Pada detik ke 0, 9 permintaan paket ICMP dikirim dari server ke pengirim paket gangguan. Reply atau balasan dari komputer pengirim paket gangguan adalah 9 paket ICMP. Ini terjadi pada kedua kondisi, yang berarti koneksi antara server dan penyusup masih terhubung.

Pada detik ke 1, 1 permintaan paket ICMP dikirim, dan 1 balasan paket ICMP dikembalikan, juga terjadi pada kedua kondisi (ketika server berjalan dengan sistem pencegahan dan tanpa sistem pencegahan).

Pada detik ke 2, 7 permintaan paket ICMP dikirim, dan 7 paket balasan ICMP juga dikembalikan seperti sebelumnya.

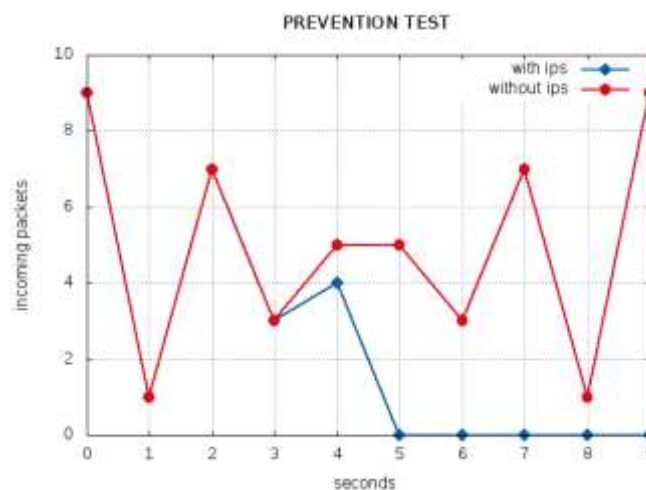
Perubahan terjadi dalam detik ke 4; server mengirimkan 5 paket ICMP request tetapi hanya 4 paket ICMP reply dikembalikan. Ini terjadi ketika server berjalan dengan sistem pencegahan. Di sisi lain, 5 paket balasan ICMP dikembalikan ketika server berjalan tanpa sistem pencegahan intrusi. Perubahan juga terjadi dalam 5 detik, 5 permintaan paket ICMP dikirim tetapi tidak ada balasan paket ICMP yang dikembalikan. Menandakan bahwa hubungan antara server dan penyusup tidak lagi terhubung. Ini hanya terjadi ketika server berjalan dengan sistem pencegahan intrusi, karena sistem pencegahan intrusi sudah menambahkan alamat penyusup ke daftar aturan firewall untuk di DROP semua paket yang berasal dari alamat tersebut. Hasil yang sama terus terjadi pada detik berikutnya (koneksi antara server dan penyusup masih terputus).

Ketika server berjalan tanpa sistem pencegahan, koneksi masih terhubung, yang membuat paket gangguan yang dikirim ke server masih tetap diterima oleh server.

Berikut tabel dan grafik hasil dari tes pencegahan yang kita lakukan:

Tabel III-4 perbedaan ketika menggunakan IPS dan tanpa IPS

Detik	Tanpa IPS		Menggunakan IPS	
	Request packet	Reply packet	Request packet	Reply packet
0	9 packet	9 packet	9 packet	9 packet
1	1 packet	1 packet	1 packet	1 packet
2	7 packet	7 packet	7 packet	7 packet
3	3 packet	3 packet	3 packet	3 packet
4	5 packet	5 packet	5 packet	4 packet
5	5 packet	5 packet	5 packet	0 packet
6	3 packet	3 packet	3 packet	0 packet
7	7 packet	7 packet	7 packet	0 packet
8	1 packet	1 packet	1 packet	0 packet
9	9 packet	9 packet	9 packet	0 packet



Gambar III-4 perbedaan ketika menggunakan IPS dan tanpa IPS

IV. KESIMPULAN

Berdasarkan tes deteksi dan pencegahan di atas, beberapa menyimpulkan adalah sebagai berikut:

1. Jumlah paket gangguan yang dikirim oleh masing-masing jenis serangan berbeda satu sama lain. Untuk jenis serangan XSS , 6 paket dideteksi , 12 paket untuk SCANNING dan 512 paket untuk DDOS, menunjukkan karakteristik masing-masing jenis gangguan.
2. Serangan DDOS memiliki karakteristiknya sendiri. Alamat sumber pengiriman paket gangguan oleh serangan DDOS berasal dari alamat 512 hanya dalam waktu 10 detik .
3. Ketika server berjalan dengan sistem pencegahan intrusi, reply dari 25 Paket ICMP request dikirim untuk mengecek koneksi tidak kembali, berarti bahwa daemon atau sistem pencegahan intrusi telah bekerja. Hal ini berbeda ketika server berjalan tanpa sistem pencegahan intrusi, reply dari 25 Permintaan paket ICMP masih kembali, artinya koneksi masih terhubung.

DAFTAR PUSTAKA

- [1] S. D. Bahta, "Sistem Pemantauan Jaringan Komputer Berbasis IDS," *1. J.*, pp. 1–12, 2013.
- [2] J. Zhai and Y. Xie, "Research on Network Intrusion Prevention System Based on Snort," *1. J.*, vol. 2, pp. 1133–1136, 2011.
- [3] M. Sharma, A. Kaushik, A. Sangwan, and M. Scholor, "Performance Analysis of Real Time Intrusion Detection and Prevention System using Snort," *1. J.*, vol. 1, no. 5, pp. 1–6, 2012.
- [4] L. Rikhtechi and A. R. Roozbahani, "Creating a standard platform for all intrusion detection/prevention systems," *1. J.*, vol. 3, pp. 41–44, 2010.
- [5] H. Li and D. Liu, "Research on intelligent intrusion prevention system based on Snort," *1. J.*, vol. 1, pp. 251–253, 2010.

