SIMULASI *INTRUSION DETECTION SYSTEM* (IDS) DALAM KEAMANAN WEB SERVER PADA JARINGAN

SKRIPSI

Disusun Oleh :

IRMA MALINI AMIR
NPM. 18020033

PROGRAM STUDI REKAYASA SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS DEHASEN
BENGKULU

2023

SIMULASI *INTRUSION DETECTION SYSTEM* (IDS)
DALAM KEAMANAN WEB SERVER PADA JARINGAN

SKRIPSI

IRMA MALINI AMIR
NPM. 18020033

Diajukan sebagai salah satu syarat untuk memperoleh gelar sarjana Strata I program studi Rekayasa Sistem komputer Universitas Dehasen Bengkulu

PROGRAM STUDI REKAYASA SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS DEHASEN
BENGKULU
2023

SIMULASI *INTRUSION DETECTION SYSTEM* (IDS)
DALAM KEAMANAN WEB SERVER PADA JARINGAN

SKRIPSI

Oleh :

IRMA MALINI AMIR
NPM. 18020033

Disetujui Oleh:

Pembimbing Utama,	Pembimbing Pendamping,
Riska, S.Kom., M.Kom	**Yessi Mardiana, S.Kom., M.Kom**
NIDN: 02.240192.01	NIDN: 02.030288.02

Mengetahui,

Ketua Program Studi
Rekayasa Sistem Komputer

Toibah Umi Kalsum, S.Kom,M.Kom
NIDN. 02.060573.01

SIMULASI *INTRUSION DETECTION SYSTEM* (IDS)
DALAM KEAMANAN WEB SERVER PADA JARINGAN

SKRIPSI

Disusun Oleh :

IRMA MALINI AMIR
NPM. 18020033

Telah dipertahankan di depan TIM penguji
Universitas Dehasen Bengkulu pada:

Hari : Sabtu
Tanggal : 17 Juni 2023

Skripsi ini telah diperiksa dan disetujui oleh TIM Penguji:

Penguji	Nama	NIDN	Tanda Tangan
Ketua	Riska, S.Kom., M.Kom	02.240192.01	
Sekretaris	Yessi Mardiana, S.Kom., M.Kom	02.030288.02	
Penguji I	Toibah Umi Kalsum, S.Kom,M.Kom	02.060573.01	
Penguji II	Hendri Alamsyah, S.Kom., M.Kom	02.110391.02	

Mengetahui,

Dekan
Fakultas Ilmu Komputer

H. Siswanto, S.E., S.Kom., M.Kom
NIDN : 02.240363.01

RIWAYAT HIDUP

Penulis dilahirkan di Bengkulu, pada tanggal 02 November 2000 Anak ketiga dari tiga bersaudara Ayah Faisal Amir dan Ibu Mardiati. Bangku pendidikan yang pernah ditempuh (SMK) N 5 Bengkulu diselesaikan pada tahun 2018, Dan pada 2018 penulis melanjutkan ke Program Studi Rekayasa Sistem Komputer di Universitas Dehasen Bengkulu.

MOTTO DAN PERSEMBAHAN

"It's not always easy, but that's life. Be strong because there are better days ahead."

"Ku rangkai kata, ku baca makna, ku ikat dalam alinea, ku bingkai dalam bab sejumlah lima, jadilah mahakarya gelar sarjana siap kuterima."

Skripsi ini saya persembahkan:

- Untuk diri saya sendiri yang telah berjuang dan bertahan hingga saat ini dapat menyelesaikan perkuliahan.
- Almarhum Bapak tercinta Faisal Amir yang senantiasa memberi dukungan, do'a, serta kasih sayang yang tak terhingga sepanjang masa.
- Ibu yang saya sayangi Mardiati yang takhenti memberi limpahan do'a dan menjadi donatur utama yang tak ternilai harga serta kasih sayang nya.
- Serta Rahmat Hidayat saudara satu satunya yang selalu memberikan dukungan dan motivasi berharga.

ABSTRAK

SIMULASI *INTRUSION DETECTION SYSTEM* (IDS)
DALAM KEAMANAN WEB SERVER PADA JARINGAN

Oleh:

Irma Malini Amir[1]
Riska, S.Kom., M.Kom[2]
Yessi Mardiana, S.Kom., M.Kom[2]

Penelitian ini bertujuan untuk merancang sebuah sistem keamanan jaringan komputer dengan menerapkan Snort Intrusion Detection System (IDS). Sistem keamanan jaringan yang dibangun. Integrasi antara Snort Intrusion Detection System (IDS), Database System, dan Monitoring System. Dalam skema pengujian, sistem terdiri dari dua jenis, yaitu server dan client. Server berfungsi sebagai target serangan dan sekaligus digunakan untuk melakukan pemantauan terhadap jaringan. Sedangkan client berfungsi sebagai intruder (penyusup). Metode pengujian adalah adalah melakukan Port Scanning sehingga di dapat port yang terbuka 22, 80, 10000 dan ping secara nornal serta ping dengan menyertakan paket data sebesar 10000 dan 65000. Dari hasil pengujian yang telah dilakukan, Snort-IDS mampu mendeteksi paket-paket yang melewati jaringan. Dari hasil data deteksi tersebut akan dikirim ke whastapp kemudian diteruskan ke GUI Snort dan di simpan pada log sehingga memudahkan untuk mebaca data tersebut. Linux Ubuntu Server Dalam menjalan Snort Intrusion Detection System (IDS) berjalan dengan baik dan membutuhkan source yang kecil yaitu CPU sebesar Kecil dari 10% and memory kecil dari 50%.

Kata Kunci: **Snort, GUI Snort, Linux Ubuntu**
Keterangan :
1: Peneliti
2: Pembimbing 1 dan Pembimbing 2

ABSTRACT

THE SIMULATION OF INTRUSION DETECTION SYSTEM (IDS) IN WEB SERVER SECURITY ON THE NETWORK

By:
Irma Malini Amir[1]
Riska,S.Kom., M.Kom[2]
Yessi Mardiana, S.Kom., M.Kom[2]

This study aims to design a computer network security system by implementing the Snort Intrusion Detection System (IDS). Built network security system. Integration between Snort Intrusion Detection System (IDS), Database System, and Monitoring System. In the test scheme, the system consists of two types, namely server and client. The server functions as an attack target and is also used to monitor the network. While the client functions as an intruder (intruder). The test method is to do Port Scanning so that you can get open ports 22, 80, 10000 and ping normally and ping by including data packets of 10000 and 65000. From the test results that have been done, Snort-IDS is able to detect packets that pass through network. From the results of the detection data, it will be sent to WhatsApp, then forwarded to the Snort GUI and stored in a log, making it easier to read the data. Linux Ubuntu Server When running the Snort Intrusion Detection System (IDS) it works well and requires a small source, namely a small CPU of 10% and a small memory of 50%.

Keywords: Snort, GUI Snort, Linux Ubuntu
Information :
1: Student
2: Supervisors

KATA PENGANTAR

Alhamdulillah penulis panjatkan kehadirat Allah SWT yang melimpahkan rahmat dan karunia-nya sehingga Skripsi yang berjudul "Simulasi *Intrusion Detection System* (IDS) dalam Keamanan Web Server pada Jaringan" ini dapat diselesaikan dalam waktu yang telah ditetapkan.

Pada kesempatan ini penulis ingin menyampaikan ucapan terimakasih kepada pihak-pihak yang telah banyak membantu penulis selama penyusunan Skripsi ini terutama kepada :

1. Bapak Prof. Dr. Husaini. S.E., M.Si., Ak, CA, CRP, selaku Rektor Universitas Dehasen Bengkulu.
2. Bapak Siswanto,S.E., M.Kom selaku Dekan Fakultas Ilmu Komputer Universitas Dehasen Bengkulu.
3. Ibu Toibah Umi Kalsum,S.Kom, M.Kom selaku Ketua Program Studi Rekayasa Sistem Komputer Universitas Dehasen Bengkulu.
4. Bapak Riska, M.Kom selaku Dosen Pembimbing I yang telah banyak memberikan arahan dan bimbingan kepada penulis.
5. Ibu Yessi Mardiana, M.Kom selaku Dosen Pembimbing II yang telah banyak memberikan arahan dan bimbingan kepada penulis.
6. Kedua orang tua penulis yang tercinta, Alm Bapak Faisal Amir dan Ibu Mardiati, yang telah memberikan kasih sayang, do'a, dan pengorbanan yang takterhingga demi masa depan penulis.
7. Abangku Rahmat Hidayat yang telah memberikan dukungan, do'a, serta setia mendampingi penulis baik suka maupun duka.

8. Seluruh member NCT, terutama Na Jaemin yang telah memberikan energi positif dan semangat dalam penyelesaian Skripsi ini.
9. Fifmianti Bibiola selaku teman seperjuangan yang telah memberikan bantuan dan dukungan yang luar biasa dalam menyelesaikan skripsi ini.
10. Seluruh pihak yang telah membatu penulis dalam menyelesaikan Skripsi ini.

Semoga segala bantuan dan bimbingan yang telah diberikan kepada penulis mendapat imbalan yang berlimpah dari Tuhan YME.

Penulis mengharapkan kritik dan saran yang sifatnya membangun dari berbagai pihak. Akhirnya semoga Skripsi ini dapat bermanfaat bagi penulis khususnya, dan bagi pembaca umumnya.

Bengkulu, 2023

Penulis

DAFTAR ISI

Halaman

HALAMAN JUDUL i

HALAMAN PENGESAHAN ii

HALAMAN PERSETUJUAN iii

RIWAYAT HIDUP v

MOTTO DAN PERSEMBAHAN vi

ABSTRAK vii

ABSTRACT viii

KATA PENGANTAR ix

DAFTAR ISI xi

DAFTAR GAMBAR xiii

DAFTAR TABEL xiv

BAB I. PENDAHULUAN

1.1 Latar Belakang 1

1.2 Rumusan Masalah 3

1.3 Batasan Masalah 3

1.4 Tujuan Penelitian 3

1.5 Manfaat Penelitian 4

BAB II. LANDASAN TEORI

2.1 Simulasi 5

2.2 Intrusion Detection System 6

2.3 Keamanan 7

2.4 Web Server 8

2.5 Jaringan Komputer 11

2.6 Snort 12

2.7 Ubuntu Server 13

BAB III. METODOLOGI PENELITIAN

3.1 Subjek Penelitian 16
A. Tempat dan Waktu Penelitian 16
B. Struktur Organisasi 16
C. Tugas dan Wewenang 17
3.2 Metode Penelitian 20
3.3 Instrumen Perangkat Keras dan Perangkat Lunak 21
3.4 Metode Pengumpulan Data 22
3.5 Metode Perancangan Sistem 23
3.5.1 Blok Diagram Sistem Lama 24
3.5.2 Blok Diagram Sistem Baru 24
3.5.3 Prinsip Kerja Sistem 24
3.5.4 Rencana Kerja 25
3.6 Rencana Pengujian 27

BAB IV. HASIL DAN PEMBAHASAN

4.1 Hasil 30
4.1.1 Pengujian ICMP 31
4.1.2 Pengujian Dilakukan Dengan Aplikasi NMAP 37
4.1.3 Pengujian Dengan Menggunakan Perintah TOP 40
4.2 Pembahasan 41
4.2.1 Installasi Linux Ubuntu Server 42
4.2.2 Installasi LAMP (Apache2, MySQL dan PHP) 45
4.2.3 Install Snort 48
4.2.4 Konfigurasi File Snort 49
4.2.5 Konfigurasi Rules Snort 50
4.2.6 Install dan Konfigurasi ACIDBASE 51
4.3 Hasil Pengujian 52
4.3.1 Pengujian ICMP 53
4.3.2 Pengujian Dilakukan Dengan Aplikasi NMAP 56
4.3.3 Pengujian Dengan Menggunakan Perintah TOP 57

BAB V. KESIMPULAN DAN SARAN

5.1 Kesimpulan 59

5.2 Saran 59

DAFTAR PUSTAKA

LAMPIRAN

DAFTAR GAMBAR

Gambar		Halaman
3.1	Blok Diagram Sistem Aktual	23
3.2	Blok Diagram Sistem Yang Diusulkan	24
3.3	Rencana Kerja	25
4.1	Tampilan Status User	30
4.2	Tampilan Pihan Bahasa Install Linux	42
4.3	Tampilan Input Proxy Linux	43
4.4	Tampilan Pilihan Respotary Linux	43
4.5	Tampilan Pilihan HDD Sistem Linux	44
4.6	Tampilan Konfirmasi Pilihan HDD Sistem Linux	44
4.7	Tampilan Proses Install Linux	45
4.8	Tampilan Install Linux Selesai	45
4.9	Tampilan Status Apache2	46
4.10	Tampilan Proses Install MySQL	47
4.11	Tampilan Proses Install PHP	47
4.12	Tampilan IP Address Server Snort	48
4.13	Tampilan Rules Snort	51
4.14	Tampilan Ping Standar ke Server Snort	54
4.15	Tampilan Ping Buffer Size 10000	55
4.16	Tampilan Ping Buffer Size 65000	55

DAFTAR TABEL

Tabel Halaman

3.1 Rencana Pengujian 27

4.1 Hasil Pengujian..... 57

DAFTAR LAMPIRAN

1. Time Schedule
2. Struktur Organisasi
3. Kartu Bimbingan

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pertumbuhan internet dan jaringan komputer yang terjadi pada zaman sekarang ini memberikan keuntungan dan kemudahan kepada pengguna komputer untuk dapat berbagi sumber daya dan informasi antara beberapa komputer yang saling terhubung dalam suatu jaringan yang sifatnya lokal maupun internasional.

Sistem pengawasan dan pengamanan data harus mampu mencegah dan menghentikan potensi penyusupan dari orang yang tidak memiliki otoritas dalam jaringan tersebut. Ada banyak cara yang dapat dilakukan untuk mengatasi masalah keamanan jaringan dan gangguan sistem, Salah satunya yang digunakan adalah IDS *(intrusion detection system)*. Sistem pendeteksi intrusi atau IDS (*Intrusion Detection System*) merupakan salah satu metode untuk melindungi jaringan komputer dengan cara mendeteksi serangan-serangan yang ada dan memberitahukannya kepada administrator sistem jaringan komputer untuk segera mengantisipasi serangan tersebut. Fungsi utama IDS adalah untuk mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan secara *realtime*/berkala terhadap kegiatan-kegiatan yang mencurigakan didalam sebuah sistem jaringan.

Keamanan web, sangat erat kaitannya dengan jaringan karena untuk mengakses sebuah *website* pasti dibutuhkan koneksi jaringan. Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi, namun masalah keamanan ini sering kali kurang diperhatikan oleh para pemilik dan pengelola sistem informasi sehingga memungkinkan terjadinya resiko ya 1 ıp signifikan. Sebagai contoh, dalam suatu

persaingan bisnis dalam dunia maya, dapat memungkinkan terjadinya suatu penyerangan terhadap *web server* yang kemudian akan menimbulkan kerugian bagi pemilik dimana *website* yang diserang menjadi *down* atau tidak dapat diakses oleh *client* sehingga dapat memberikan kontribusi bagi para pesaing bisnis lainnya.

Dibalik kemudahan pengaksesan informasi yang disediakan oleh internet terdapat bahaya besar yang mengintai, yaitu berbagai macam serangan yang berusaha mencari celah dari sistem keamanan jaringan komputer yang digunakan. Serangan – serangan itu dapat mengakibatkan kerusakan data dan bahkan kerusakan pada *hardware*. Karena itulah sistem keamanan terhadap jaringan komputer juga harus semakin ditingkatkan.

Masalah tersebut telah menuntut suatu instansi maupun perusahaan untuk melindungi integritas dan kerahasiaan informasi mereka, dikarenakan tidak semua informasi data bersifat terbuka untuk umum dan tidak semua orang dapat mengaksesnya. Suatu jaringan komputer memerlukan suatu sistem pengawasan dan pengamanan data untuk menjaga agar informasi penting yang ada dalam jaringan tersebut tetap aman.

Maka dari latar belakang diatas penelitian ini akan mengambil judul yaitu ***"Simulasi Intrusion Detection System(IDS) dalam Keamanan Web Server pada Jaringan "***.

1.2 Rumusan Masalah

Berdasarkan uraian masalah pada latar belakang diatas, maka rumusan masalah pada penelitian ini adalah bagaimana simulasi *Intrusion Detection System*(IDS) dalam keamanan *web server* pada jaringan?

1.3 Batasan Masalah

Agar Pembahasan dalam penelitian ini tidak meluas, maka batasan masalah yang akan dibahas pada penelitian ini adalah sebagai berikut :

1. *Server* menggunakan sistem operasi linux ubuntu *server* 20.10
2. Sistem IDS menggunakan Snort dengan jenis HIDS

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini dibedakan menjadi 2 tujuan yaitu, tujuan umum dan tujuan khusus:

A. Tujuan Umum

Tujuan umum pembuatan proposal skripsi ini adalah sebagai salah satu syarat akhir dalam penyelesaian studi pada Fakultas Ilmu Komputer Universitas Dehasen Bengkulu.

B. Tujuan Khusus

1. Membuat sistem keamanan dengan menerapkan metode *Intrusion Detection System*(IDS).
2. Mencegah dan mengatasi permasalahan keamanan jaringan agar dapat memberikan keamanan, kenyamanan bagi pengelola jaringan.

1.5 Manfaat Penelitian

Manfaat yang diharapkan oleh peneliti dalam penelitian ini adalah sebagai berikut:

1. Menerapkan simulasi *intrusion detection system*(IDS) dalam keamanan *web server* pada jaringan.
2. Dapat menerapkan sistem keamanan *web server* pada jaringan menggunakan snort.
3. Hasil dari penelitian ini diharapkan dapat menjadi dasar untuk penelitian berikutnya dan menambah teori-teori baru untuk penelitian yang sejenis.

BAB II

LANDASAN TEORI

2.1 Simulasi

Menurut Ahdan, dkk. (2018:29) Simulasi merupakan alat yang berguna untuk menganalisis sistem yang rumit dimana kita tidak dapat menggunakan metode standar dalam riset operasional, selain itu simulasi dapat diartikan sebagai meniru suatu sistem nyata yang kompleks dengan penuh sifat probabilistik, tanpa harus mengalami keadaan yang sesungguhnya.

Menurut Munifatussangadah dan Sutisna (2021:69) Simulasi adalah proses merancang model dari suatu sistem dan kemudian menjalankannya untuk mendeskripsikan, menjelaskan, dan memprediksi karakteristik dinamis sistem tersebut. Simulasi sebagai metode yang digunakan untuk menyelesaikan berbagai persoalan sebenarnya cukup lama diperkenalkan. Namun baru dirasakan kehadirannya seiring dengan perkembangan dunia komputer yang semakin berkembang saat ini. Tidak jarang banyak persoalan-persoalan rumit di industri dapat diselesaikan lebih cepat dan lebih mudah dengan menggunakan simulasi.

Dari beberapa pendapat di atas, dapat disimpulkan bahwa pengertian simulasi adalah suatu kegiatan merancang atau mendeskripsikan dengan menggunakan situasi tiruan untuk memahami tentang konsep, prinsip, atau keterampilan tertentu.

2.2 *Intrusion Detection System*(IDS)

5

Menurut Wijaya dan Pratama (2020:98) IDS merupakan suatu sistem yang memiliki kemampuan untuk menganalisis data secara realtime dalam mendeteksi, mencatat (log) dan menghentikan penyalahgunaan dan penyerangan. IDS merupakan security tools yang dapat digunakan untuk menghadapi aktivitas hacker. IDS ini mampu

memberikan peringatan kepada administrator apabila terjadi suatu serangan atau penyalahgunaan di dalam jaringan, bahkan peringatan itu dapat pula menunjukkan alamat IP dari sebuah sistem penyerang.

Menurut Sutarti, dkk. (2018:2) *Intrusion Detection System* (IDS) adalah sebuah sistem yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. Jika ditemukan kegiatan-kegiatan yang mencurigakan berhubungan dengan traffic jaringan, maka IDS akan memberikan peringatan kepada sistem atau administrator jaringan. Pada umumnya IDS terbentuk menjadi dua, yaitu:

1. NIDS (*Network - based Intrusion Detection System*)

   Menurut Purba dan Efendi (2020:145) NIDS (*Network - based Intrusion Detection System*) merupakan sebuah perangkat lunak yang bekerja secara otomatis untuk memantau suatu paket data yang masuk ke dalam sistem jaringan. Semua paket data yang berjalan pada sistem jaringan, akan dianalisis untuk melihat apakah ada percobaan serangan atau penyusupan ke dalam sistem jaringan. Jika ada kecocokan dengan *rules* yang telah dibuat, maka hasilnya akan dicatat dalam sebuah file.

2. HIDS (*Host Intrusion Detection System*)

   Menurut Purba dan Efendi (2020:146) HIDS (*Host Intrusion Detection System*) merupakan jenis IDS yang bekerja pada *host* yang individual atau perangkat tertentu pada sistem jaringan komputer secara *real-time*. HIDS akan memantau paket-paket data ketika sedang terjadi penyusupan saja.

Dalam melakukan tugasnya IDS (*intrusion detection system*) berada pada lapisan jaringan OSI (*Open System Interconnection*) model yang terdapat pada lapisan ketiga

yaitu pada lapisan *network* dan sensor jaringan pasif yang secara khusus diposisikan pada *choke point* pada jaringan metode dari lapisan OSI.

Dari pengertian yang telah dikemukakan oleh beberapa para ahli diatas, maka penulis dapat menyimpulkan bahwa *Intrusion Detection System* (IDS) adalah sebuah metode yang dapat digunakan untuk mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan.

2.3 Keamanan

Menurut Noviansyah dan Saiyar (2021:38) Keamanan jaringan adalah salah satu aspek penting dalam dunia internet suatu jaringan internal perusahaan membutuhkan keamanan khusus yang dapat menjaga data dimana berfungsi sebagai keamanan jaringan.

Menurut Wijaya dan Pratama (2020:97) Keamanan jaringan komputer sebagai bagian dari sebuah sistem informasi adalah sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya. Sistem harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan oleh pihak yang tidak berhak

Sedangkan keamanan sendiri adalah sistem dari semua itu yang berarti sesuatu yang membuat kita menjadi aman. Biasanya istilah ini biasa digunakan dengan hubungan dengan kejahatan dan segala bentuk kecelakaan. Keamanan sendiri adalah suatu yang sangat penting karena ini sangat menjaga kestabilan contohnya keamanan nasional yang mencegah dari kriminalitas tingkat tinggi seperti terorisme, cracker atau hacker dan keamanan terhadap ekonomi nasional.

Tujuan utama dengan adanya keaman adalah untuk membatasi akses informasi dan sumber hanya untuk pemakai yang memiliki hak akses.

2.4 Web Server

Menurut Roihan (2018:91) Web Server adalah layanan server yang berfungsi menerima permintaan HTTP atau HTTPS dari klien dengan menggunakan web browser dan mengirimkan kembali hasilnya dalam bentuk halaman-halaman web yang umumnya berbentuk dokumen HTML dan format dokumen web lainnya.

Menurut Ramadhani (2017 : 309) Web server adalah perangkat lunak (*software*) dalam server yang memberikan layanan berbasis data dan berfungsi untuk menerima permintaan (*request*) berupa halaman web melalui protokol HTTP dan atau HTTPS dari klien yang lebih dikenal dengan nama *browser*, kemudian mengirimkan kembali (*respon*) hasil permintaan tersebut kedalam bentuk halaman web yang pada umumnya berbentuk dokumen HTML.

Berdasarkan pengertian diatas dapat disimpulkan bahwa Web Server adalah sebuah *Software* (perangkat lunak) yang memberikan layanan berupa data. Berfungsi untuk menerima permintaan HTTP atau HTTPS dari klien atau kita kenal dengan web browser (*Chrom, Firefox*).

Gambar 2.1 Web Server

Web Server berungsi menerima permintaan HTTP atau HTTPS dariklien atau kitakenal dengan web browser (*Chrom, Firefox*). Ia juga akan mengirimkan respon atas permintaan kepada *client* dalam bentuk halaman web yang umumnya HTML.

Jenis-jenis dari web server adalah sebagai berikut

1. Web Server Apache

   Web server yang populer dan paling banyak digunakan kebanyakan orang, yaitu jenis Apache. Pada awalnya Apache didesain guna mendukung penuh sistem operasi UNIX. Selain cukup mudah dalam implementasinya, Apache juga memiliki beberapa program pendukung sehingga memberikan layanan yang lengkap, seperti PHP, SSI dan control akses. Berikut detailnya:

   a. PHP (*Personal Home Page* atau PHP *Hypertext Processor*)

      Program semacam CGI, berfungsi memproses teks yang bekerja di server. Apache sangat mendukung PHP dengan menempatkannya sebagai salah satu modulnya (*mod php*). Hal tersebut membuat PHP bekerja lebih baik.

   b. SSI (*Server Side Include*)

      Perintah yang bisa disertakan dalam bekas HTML. Kemudian ia dapat diproses oleh web server ketika pengguna mengaksesnya.

   c. Access Control

      Kontrol Akses dapat dijalankan berdasarkan nama *host* atau nomor IP CGI (*Common Gateway Interface*). Lalu yang paling umum untuk digunakan adalah perl (*Practical Extraction and Report Language*), disupport oleh Apache dengan menempatkannya sebagai modul (*mod perl*).

Apache sangat aman dan nyaman untuk digunakan karena memiliki beberapa keuntungan seperti proses instalasi yang mudah, freeware, dan sistem konfigurasi yang masih tergolong mudah. Selain itu ia juga mampu bekerja pada sistem operasi *open* atau *closed source*.

2. Web Server Nginx

   Salah satu pesaing unggul Apache yaitu Nginx. Nginx dikenal mampu melayani segala macam permintaan, seperti request pada dengan tingkat kepadatan lalu lintas atau *taffic* yang sangat padat. Nginx memang lebih unggul dari segi kualitas, kecepatan dan dalam hal performannya. Nginx memiliki banyak kelebihan dalam hal fitur, diantaranya *URL rewriting, virtual host, file serving, reverse proxying, access control*, dan masih banyak lagi.

3. Web Server IIS

   Web Server IIS (*Internet Information Services*) adalah web server yang bekerja pada jenis protokol seperti DNS, TCP/IP, atau beragam *software* lainnya yang berguna untuk merangkai sebuah situs.

4. Web Server Lighttpd

   Programmer asal Jerman telah menciptakan web server berbasis *open source*guna mendukung sistem *Linux* dan *Unix*. Bila dilihat dari segi keunggulan, web server yang satu ini memiliki beberapa keunggulan berdasarkan fitur tambahan yang tersedia. Seperti *FastCGI, Output-Compression, FastCGI, dan URL writing*. Jika kamu menggunakan web server Lighttpd, kamu akan merasakan performa yang lebih cepat dan efektif.

2.5 Jaringan Komputer

Menurut Rahmatulloh dan Firmansyah (2017:242) Jaringan Komputer adalah suatu sistem telekomunikasi yang didalamnya terdiri dari dua atau lebih perangkat komputer yang dirancang untuk dapat berkerja secara bersama-sama dengan tujuan dapat berkomunikasi, mengakses informasi, meminta serta memberikan layanan atau service antara komputer satu dengan yang lainnya.

Menurut Noviansyah dan Saiyar (2021:37) Jaringan komputer merupakan kumpulan dari beberapa komputer dan peralatan penunjang lainnya yang terhubung dalam satu kesatuan dan saling terkoneksi.

Berdasarkan pengertian diatas dapat disimpulkan bahwa jaringan komputer adalah suatu sistem telekomunikasi yang didalamnya terdiri dari dua atau lebih perangkat komputer yang terhubung dalam satu kesatuan dan saling terkoneksi.

Jaringan komputer pada umum nya di kelompokkan menjadi 5 kategori, yaitu berdasarkan jangkauan geografis, media tranmisi data, distribusi sumber informasi/data, peranan dan hubungan tiap komputer dapam memproses data, dan berdasarkan jenis topologi yang digunakan. Jenis jaringan komputer berdasarkan jangkauan geografis yaitu:

1. Local Area Network :

   Local area network atau disingkat LAN merupakan jaringan yang mencakup wilayah kecil. salah satu contoh adalah jaringan komputer yang berada dilingkup sekolah, kampus atau kantor. Biasanya jaringan LAN menggunakan teknologi IEEE 802.3 ethernet dengan kecepatan transfer data sekitar 10 MB/s, 100 MB/p dan 1 GB/s. selain menggunakan teknologi ethernet jaringan LAN bisa menggunakan teknologi nirkabel seperti wi-fi.

2. Metropolitan Area Network :

Metropolitan area network atau disingkat WAN merupakan sebuah jaringan yang berada di dalam satu kota dengan kecepatan transfer data tinggi yang menghubungkan beberapa tempat tetapi masih dalam satu wilayah kota. jaringan MAN merupakan gabungan dari beberapa jaringan LAN

3. Wide Area Network :

   Wide area network atau disingkat WAN merupakan jaringan yang jangkauannya mencakup daerah geografis yang luas, semisal antar wilayah, daerah, kota, negara bahkan benua.

2.6 Snort

Menurut Dewi (2017:74) Snort adalah perangkat lunak IDS dan NIDS berbasis opensource dan banyak digunakan untuk untuk mengamankan sebuah jaringan dari aktifitas yang berbahaya. Cara kerja Snort mirip dengan TcpDump, tetapi fokus sebagai security packet sniffing. Fitur utama Snort yang membedakan dengan TcpDump adalah payload inspection, dimana Snort melakukan analisis payload rule set yang disediakan.

Menurut Sutarti, dkk. (2018:2) Snort adalah suatu perangkat lunak untuk mendeteksi penyusup dan mampu menganalisi paket yang melintasi jaringan secara *real time traffic* dan *logging* ke dalam database serta mampu mengidentifikasi berbagai serangan yang berasal dari luar jaringan.

2.7 Ubuntu Server

Menurut Husen dan Surbakti (2020:21) Ubuntu adalah salah satu distribusi Linux yang berbasis Debian dan didistribusikan menjadi perangkat lunak sistem operasi yang bebas. Secara singkat dan jelasnya yaitu Ubuntu adalah sejenis sistem operasi yang

berbasiskan Linux Debian. Adapun versi Ubuntu yang telah dirilis 5 tahun terakhir adalah sebagai berikut :

a. Versi 16.04 LTS (Xenial Xerus).

b. Versi 16.10 (Yakkety Yak).

c. Versi 17.04 (Zesty Zapus).

d. Versi 17.10 (Artful Aardvark).

e. Versi 18.04 LTS (Bionic Beaver).

f. Versi 18.10 (Cosmic Cuttlefish).

g. Versi 19.04 (Disco Dingo).

h. Versi 19.10 (Eoan Ermine)

i. Versi 20.04 LTS (Focal Fossa)

j. Versi 20.10 (Groovy Gorilla)

Menurut Sampurno (2019:2) Linux adalah sistem operasi yang bersifat *open source* dan bebas (*free*) di bawah lisensi GNU (GNU *is not Unix*) GPL (*General Public License*).

Adapun kelebihan Linux yaitu:

1. Bersifat *open source*, bebas dan terbuka. Sehingga tidak perlu biaya untuk mendapatkannya.
2. Linux sekarang sudah mudah untuk dioperasikan.
3. Hampir semua aplikasi yang digunakan di *windows* sudah ada aplikasi linuxnya yang dikembangkan oleh komunitas linux atau bisa juga menggunakan *software emulator*.
4. Memiliki keamanan yang lebih unggul karna didesain *multiuser* sehingga apabila *virus* menyerang *user* tertentu, akan sangat sulit untuk menyebar ke *user* yang lain.

5. Cocok untuk PC yang memiliki *spesifikasi* minimum karna linux membutuhkan *resource* yang lebih kecil dibandingkkan dengan windows.

BAB III

METODOLOGI PENELITIAN

3.1 Subjek Penelitian

A. Tempat dan Waktu Penelitian

1. Tempat Penelitian

   Penelitian dilaksanakan di laboratorium komputer UPT. Puskom Universitas Dehasen Bengkulu yang beralamatkan di Jl. Meranti Raya No. 32 Sawah Lebar Bengkulu.

2. Waktu Penelitian

   Penelitian ini dilakukan dengan dua tahap yaitu:

   a. Pra - Penelitian

      Pra – penelitian ini dilakukan dari bulan Maret 2022 sampai dengan bulan Mei 2022.

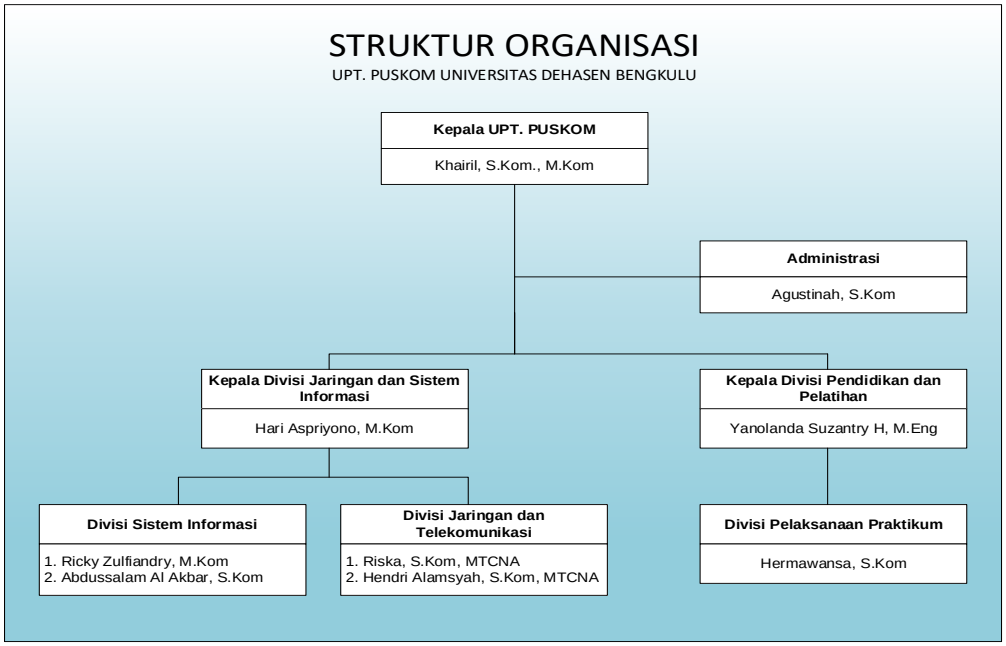
   b. Penelitian

      Penelitian ini dilakukan dari bulan Mei 2022 sampai dengan bulan Juli 2022.

B. Struktur Organisasi

Struktur Organisasi merupakan kerangka kerja dimana didalamnya menggambarkan hubungan dan tanggung jawab setiap tingkat yang berada dalam

Organisasi tersebut untuk melaksanakan demi tercapainya tujuan yang telah ditetapkan. Dengan demikian orang-orang tersebut mempunyai tugas, wewenang, dan tanggung jawab sesuai tugas masing-masing. Struktur Organisasi sangatlah penting dalam suatu perusahaan atau instansi pemerintah. Karena dengan adanya struktur organisasi akan memperlihatkan dengan jelas kedudukan seseorang, sehingga setiap karyawan atau pegawai perusahaan atau instansi yang bersangkutan dapat mengetahui aktifitas dari perusahaan atau instansi dan dapat bekerja secara baik dari segi pembagian tugas maupun hal pelimpahan wewenang yang telah ditetapkan dalam struktur. Adapun struktur organisasi UPT. Puskom Universitas Dehasen Bengkulu terlampir pada gambar 3.1



C. Tugas dan Wewenang

1. Kepala Pusat Komputer (Puskom)

a. Menyusun Rencana Induk Teknologi Informasi Unived.

b. Menyelenggarakan perkuliahan dan praktikum komputer.

c. Melakukan perencanaan standar peralatan Teknologi Informasi, pengoperasian, pendayagunaan, dan pemeliharaan jaringan dilingkungan Unived.

d. Memasyarakatkan layanan Teknologi Informasi kepada pengguna dan calon pengguna.

e. Melakukan pengendalian keamanan dan keandalan kinerja jaringan baik dari sisi hardware maupun software sesuai dengan kemajuan teknologi.

f. Melaksanakan pengelolaan layanan Teknologi Informasi yang antisipatif terhadap kebutuhan Universitas dan responsif terhadap keluhan pengguna.

g. Menetapkan kualifikasi dan memberikan pertimbangan dalam rekruitmen dan penerimaan teknisi Teknologi Informasi pada semua unit di lingkungan Unived.

h. Melakukan koordinasi dan memberikan konsultasi teknis jaringan secara berkala kepada para teknisi Teknologi Informasi di lingkungan Unived.

i. Mengelola dan menjamin kelancaran akses informasi ke jaringan lokal Universitas dan jaringan global bagi semua pengguna.

Membuat laporan secara periodik kepada pimpinan Unived.

2. Administrasi

a. Membantu menyusun RKAT Pusat Komputer.

b. Mewakili tugas Kepala Pusat Komputer.

c. Melaksanakan urusan keuangan.

d. Melakukan tatalaksana dan kepegawaian.

e. Melaksanakan urusan rumah tangga.

f. Melaksanakan sosialisasi layanan Puskom.

g. Melaksanakan administrasi layanan Puskom.

h. Membina kelompok tenaga ahli.

i. Membuat laporan pelaksanaan kegiatan Puskom.

j. Melaksanakan tugas lain yang diberikan oleh pimpinan.

3. Divisi Pendidikan dan Pelatihan

a. Menyusun rencana dan program kerja.

b. Mengkoordinasikan penyusunan Rencana Kerja dan Anggaran.

c. Mengkoordinasikan pelaksanaan praktikum.

d. Melaksanakan kebijakan umum dan teknis pendidikan dan pelatihan bagi dosen dan mahasiswa.

e. Menyampaikan saran dan pertimbangan kepada kepala UPT. Puskom guna kelancaran pelaksanaan kegiatan.

4. Divisi Pelakasana Praktikum

a. Mengkoordinasikan *hardware* dan *software* praktikum dengan dosen pengasuh.

b. Mengkoordinasikan jadwal praktikum dengan administrasi.

c. Menyiapkan fasilitas perkuliahan dan/atau praktikum komputer.

5. Divisi Jaringan Telekomunikasi

a. Menyusun RKAT di lingkungan seksi Layanan Jaringan Komputer.

b. Memelihara hardware, software, dan sistem operasi komputer;

c. *Cabling* dan *switching*.

d. *Routing*, *Bandwidth* management, dan *firewall*.

e. Penataan/pemetaan (topologi) jaringan.

f. Melakukan pelatihan pengoperasian jaringan di lingkungan Unived.

6. Divisi Sistem Informasi

a. Menyusun RKAT di lingkungan Seksi Layanan Teknologi Informasi.

b. Layanan e-mail dan web *server*.

c. Layanan aplikasi teknologi informasi.

d. Bantuan teknis operasional sistem informasi manajemen.

e. Sistem pencadangan data (*backup system*).

f. Layanan instalasi *software* aplikasi.

g. Mengembangkan *software* teknologi informasi.

h. Melaksanakan pelatihan operasional *software* manajemen informasi di lingkungan Unived.

3.2 Metode Penelitian

Metode penelitian yang di gunakan adalah penelitian tindakan atau *action research*. Penelitian tindakan atau *action research* yaitu mendeskripsikan, menginterpretasi dan menjelaskan suatu situasi atau keadaan pada jaringan dan melakukan analisis terhadap implementasi *Intrusion Detection System*. Pada implementasi *Intrusion Detection System* yaitu dengan menggunakan beberapa komponen *Intrusion Detection System* yang terdiri dari *snort engine, php, apache, dan sql server* dengan menggunakan *software* atau modul tambahan seperti program BASE (*Basic Analysis and Security Engine*) serta sistem operasi linux ubuntu 20.10 server.

3.3 Instrumen Perangkat Lunak dan Perangkat Keras

Dalam melakukan penelitian ini, alat dan bahan yang digunakan meliputi perangkat lunak dan perangkat keras.

1. Perangkat Lunak (*Software*)

   Adapun perangkat lunak (*software*) yang digunakan dalam penelitian ini dapat dilihat seperti berikut.

   a. Sistem Operasi Linux Ubuntu *Server* 20.10

   b. Snort

   c. Php

   d. Apache

2. Perangkat Keras (*Hardware*)

No	Kebutuhan	Perangkat	Spesifikasi
1	2 unit PC *Server*	Processor	Intel(R) Pentium(R) CPU G620 @ 2.60GHz
		Memory	2 GB
		Harddisk	250 GB
		NIC	Fast Ethernet Card 10/100 MBps
2	Laptop	3 unit	
3	Switch	1 Unit	Merk: TP-LINK8 Port Kecepatan: 10/100Mbps Tipe: Desktop Switch TL-SF1008D

3.4 Metode Pengumpulan Data

Untuk memperoleh data yang diperlukan dalam penyusunan skripsi nanti penulis menggunakan beberapa metode dalam pengumpulan data yaitu:

A. Observasi

Merupakan metode pengumpulan data yang digunakan dengan cara melakukan pengamatan langsung pada jaringan yang ada di Lab Jaringan Universitas Dehasen Bengkulu.

B. Studi Pustaka

Merupakan metode pengumpulan data yang dilakukan dengan cara membaca buku-buku di perpustakaan kampus maupun perpustakaan daerah dan artikel di *internet* yang ada hubungannya dengan masalah yang dibahas dalam penelitian ini.

C. Studi Laboratorium

Data penelitian dikumpulkan dengan melakukan percobaan di laboratorium komputer UPT. Puskom Universitas Dehasen Bengkulu yang berhubungan dengan kemananan jaringan komputer dengan *Network Intrusion Detection System* (NIDS).

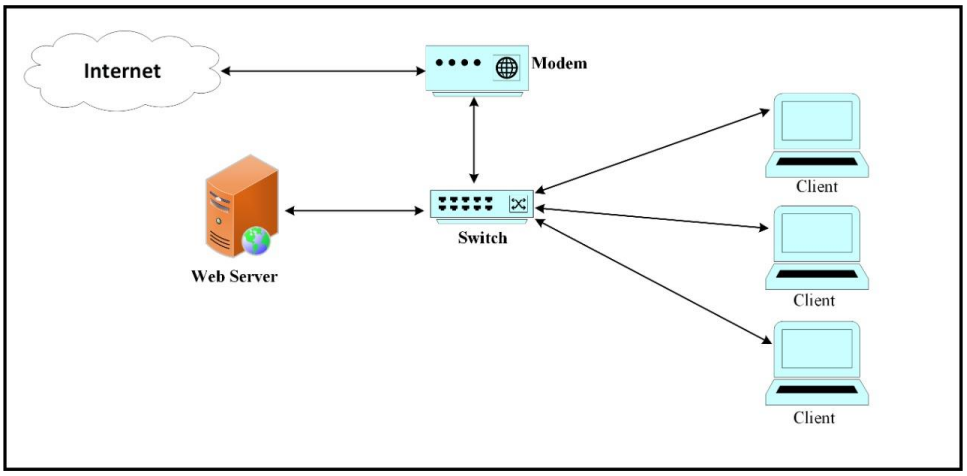
D. Studi Dokumentasi

Studi dokumentasi dilakukan dengan cara mengumpulkan, menganalisis dokumen-dokumen, catatan-catatan yang penting dan berhubungan serta dapat memberikan data-data untuk memecahkan permasalahan dalam penelitian.

3.5 Metode Perancangan Sistem

3.5.1 Diagram Blok Sistem Lama

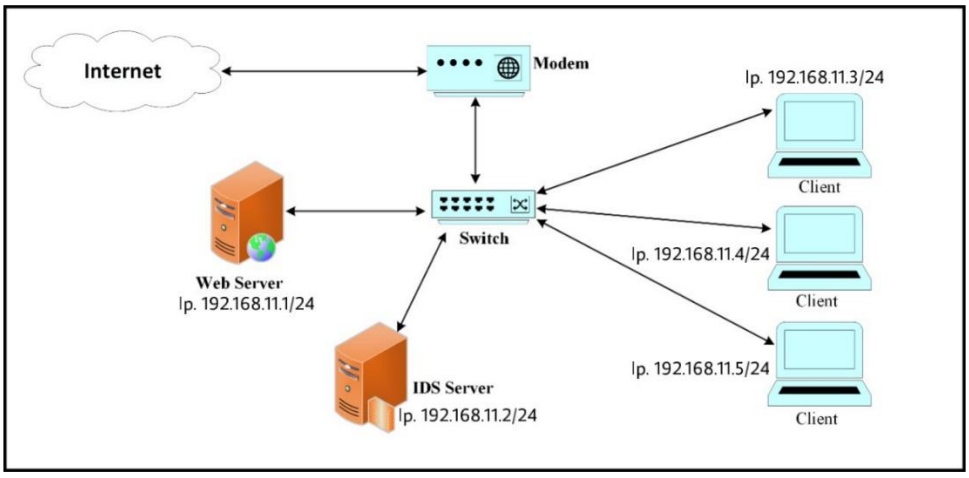
Berdasarkan dari data yang penulis peroleh dari studi observasi yang dilakukan, saat ini tidak ada sistem yang digunakan secara khusus untuk melakukan pengawasan. Adapun skema diagram blok sistem yang ada saat ini adalah sebagai berikut.



Gambar 3.2 Diagram Blok Sistem Lama

3.5.2 Diagram Blok Sistem Baru

Pada penelitian ini akan dilakukan pengembangan terhadap jaringan yang sudah ada dengan menerapkan *Intrusion Detection System* (IDS) dalam keamanan web server pada jaringan serta notifikasi menggunakan aplikasi *Whatsapp*. Adapun topologi yang akan digunakan adalah sebagai berikut.



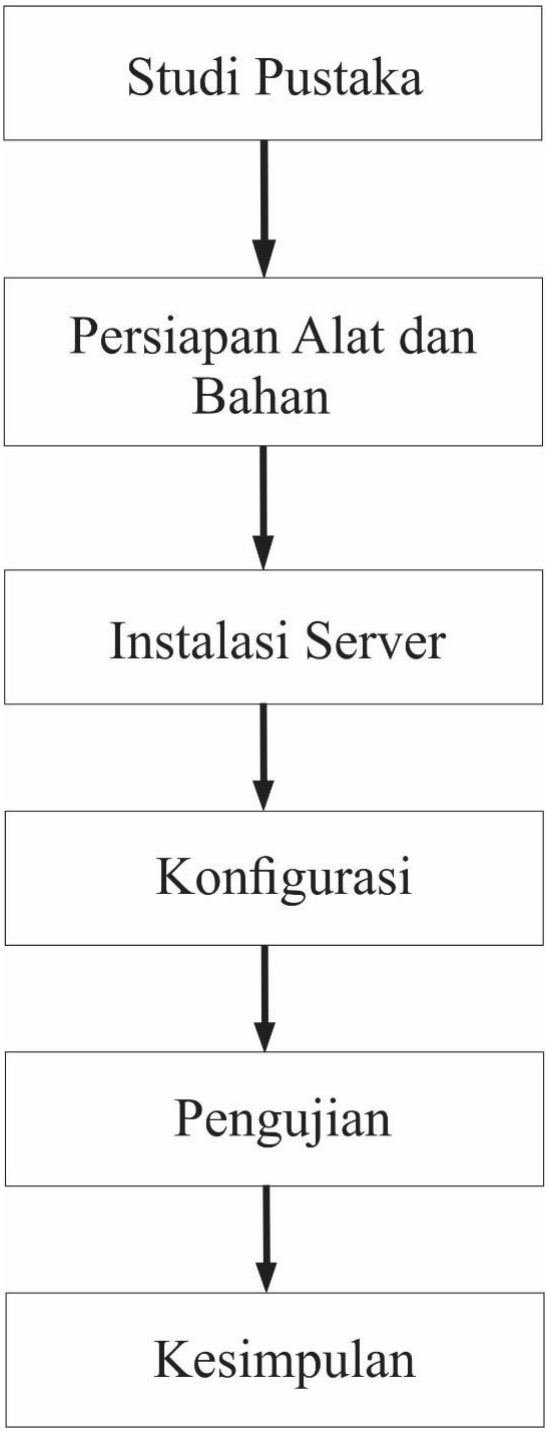
Gambar 3.3 Diagram Blok Sistem Baru

3.5.3 Prinsip Kerja Sistem

Prinsip kerja dari *Intrusion Detection System* (IDS) adalah dengan mendeteksi serangan dan menghentikannya. Pada gambar 3.3 terdapat 3 unit laptop, yang mana pada *client* pertama melakukan pengujian ICMP *Flooding*. *Client* kedua melakukan pengujian *Port Scan* yang dilakukan dengan aplikasi NMAP. Pada *client* ketiga melakukan pengujian penggunaan sumberdaya, yang mana pada *client* ketiga ini akan menunjukkan IP dari penyerang dan menghasilkan *alert* peringatan "WARNING!!! ICMP large ICMP packet". Secara otomatis pengguna yang mengakses suatu akses yang tidak diizinkan akan *ter-block*.

3.5.4 Rencana Kerja

Rencana kerja dari implementasi *Intrusion Detection System* (IDS) dalam Keamanan *Web Server* pada Jaringan adalah sebagai berikut.



Gambar 3.4 Rencana Kerja Sistem

Keterangan :

1. Studi Pustaka

   Studi pustaka dilakukan dengan cara membaca buku-buku di perpustakaan kampus maupun perpustakaan daerah dan artikel di *internet* yang ada hubungannya dengan masalah yang dibahas dalam penelitian ini.

2. Persiapan Alat dan Bahan

   Adapun alat dan bahan yang harus disiapkan, antara lain sebagai berikut:

   a. 3 Unit Laptop
   b. 2 Unit PC Server
   c. 1 Unit Switch
   d. Sistem Operasi Linux Ubuntu Server 20.10
   e. Snort
   f. Php
   g. Apache

3. Instalasi Server

   Melakukan Instalasi sistem operasi linux ubuntu 20.10 agar dapat digunakan untuk sistem IDS.

4. Konfigurasi.

   Konfigurasi dapat dilakukan sehingga antara sistem operasi *server* dan *client* dapat saling berkomunikasi.

5. Pengujian

Tahapan ini dilakukan untuk menguji sistem yang sudah diterapkan atau diimplementasikan pada jaringan. Apakah berjalan dengan baik ataupun sebaliknya.

6. Kesimpulan

Pada tahapan ini adalah tahapan untuk menyimpulkan hasil dari penelitian yang telah dilakukan.

3.6 Rancangan Pengujian

Pengujian ini dilakukan dengan metode *blackbox*, yaitu sebuah metode yang digunakan untuk menemukan kesalahan dan mendemonstrasikan fungsional sistem saat dioperasikan, apakah *input* diterima dengan benar dan *output* yang dihasilkan telah sesuai dengan yang diharapkan, sehingga dapat membuktikan kebenarannya. Adapun rancangan pengujian dapat dilihat seperti Tabel 3.1 berikut.

Tabel 3.1 Pengujian dan Analisa

No	Jenis Pengujian	Kriteria Pengujian	Hasil Pengujian	Keterangan
1.	Pengujian ICMP Flooding	Pengujian dengan PING dengan buffer size standar		
		Pengujian dengan PING dengan buffer size 10000		
		Pengujian dengan PING dengan buffer		

No	Jenis Pengujian	Kriteria Pengujian	Hasil Pengujian	Keterangan
		size 65000		
2.	Pengujian Port Scan	Pengujian dilakukan dengan aplikasi NMAP		
3.	Pengujian Penggunaan Sumberdaya	Pengujian dilakukan dengan menggunakan perintah TOP pada terminal linux untuk melihat penggunaan sumber daya server IDS. Sumberdaya yang diuji seperti prosesor, memori.		

No	Kebutuhan	Perangkat	Spesifikasi
1	2 unit PC *Server*	Processor	Intel(R) Pentium(R) CPU G620 @ 2.60GHz
		Memory	2 GB
		Harddisk	250 GB
		NIC	Fast Ethernet Card 10/100 MBps
2	Laptop	3 unit	
3	Switch	Tp-Link SF1008D Switch HUB 8Port	a. Interface : 8 10/100Mbps Ports, Auto-Negotiation, Auto-MDI/MDIX b. Buffer Size : 2Mb c. LED Indicator : Yes d. Power Supply : Output: 5.0VDC / 0.6A e. Adaptor : Yes, 220V, 50Hz D f. Data Rates : 10/100Mbps at Half Duplex, 20/200Mbps at Full Duplex Standards & g. Protocols : IEEE 802.3, IEEE 802.3u, IEEE 802.3x CSMA/CD