**ACC PRINT BERSIH, kirimkan lembar pengesahan skripsi.**

**(21-01-2022)**

**IMPLEMENTASI UNTUK MENDETEKSI SERANGAN SERVER MENGGUNAKAN SNORT INTRUSION DETECTION SYSTEM (IDS) DAN KEAMANAN SERVER MENGGUNAKAN PORT KNOCKING DAN IPTABLES FIREWALL**

**(PEMINATAN : NETWORKING)**

**SKRIPSI**

**TEKNIK INFORMATIKA STRATA 1**



**OLEH :**

**ARIE SOEHARYANTO : 17101152630054**

**PROGRAM STUDI TEKNIK INFORMATIKA**

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS PUTRA INDONESIA “YPTK”**

**PADANG**

**2021**

**LEMBAR PERNYATAAN**

**S**aya yang bertanda tangan dibawah ini :

Nama : **ARIE SOEHARYANTO**

NOBP : **17101152630054**

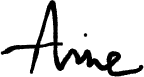
Program Study : **Teknik Informatika**

Fakultas : **Ilmu Komputer**

Menyatakan :

1. Sesungguhnya Skripsi/Tugas Akhir yang saya susun ini merupakan hasil karya tulis saya sendiri. Adapun bagian-bagian tertentu dalam Skripsi/Tugas Akhir yang saya peroleh dari hasil karya tulis orang lain, telah saya tuliskan sembernya dengan jelas, sesuai dengan kaidah penulisan ilmiah.
2. Jika dalam pembuatan Skripsi/Tugas Akhir baik pembuatan program maupun skripsi/Tugas Akhir secara keseluruhan ternyata terbukti dibuatkan oleh orang lain, maka saya bersedia menerima sanksi akademik, berupa pembatalan Skripsi/tugas Akhir dan mengulang penelitian serta mengajukan judul baru.

Demikian surat pernyataan ini saya buat dengan sesungguhnya tanpa ada paksaan dari pihak manapun.

Padang, DD MM 2022

**Arie Soeharyanto**

**LEMBAR PENGESAHAN PENGUJI SIDANG SKRIPSI**

**IMPLEMENTASI UNTUK MENDETEKSI SERANGAN SERVER MENGGUNAKAN SNORT INTRUSION DETECTION SYSTEM (IDS) DAN KEAMANAN SERVER MENGGUNAKAN PORT KNOCKING DAN IPTABLES FIREWALL**

**OLEH :**

**ARIE SOEHARYANTO**

**17101152630054**

**PROGRAM STUDI TEKNIK INFORMATIKA**

**Skripsi ini telah dinyatakan LULUS oleh Penguji Materi Pada Sidang Skripsi**

**Program Studi Strata 1 Ilmu Komputer Program Studi Teknik Informatika**

**Universitas Putra Indonesia “YPTK” Padang**

**Pada Hari/Tgl :............../....../.............. 2022**

**TIM PENGUJI :**

**1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ .................................**

**2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ .................................**

**Padang, 2021**

**Mengetahui,**

**Dekan Fakultas Ilmu Komputer**

**Universitas Putra Indonesia YPTK Padang**

**(Dr. Yuhandri, S.kom, M.kom)**

**NIDN: 1015057301**

**LEMBAR PENGESAHAN LULUS SIDANG SKRIPSI**

**IMPLEMENTASI UNTUK MENDETEKSI SERANGAN SERVER MENGGUNAKAN SNORT INTRUSION DETECTION SYSTEM (IDS) DAN KEAMANAN SERVER MENGGUNAKAN PORT KNOCKING DAN IPTABLES FIREWALL**

**Yang Dipersiapkan Dan Disusun Oleh :**

**ARIE SOEHARYANTO**

**17101152630054**

**Yang Telah Dipertahankan Didepan Dewan Penguji**

**Pada Tanggal/bulan/2022**

**Dan Dinyatakan Telah Lulus**

**Memenuhi Syarat**

**Pembimbing I Pembimbing II**

**(Randy Permana, S.Kom, M.Kom) (Rima Liana Gema, S.Kom, M.Kom)**

**NIDN : 1012128701 NIDN : 1013098901**

**Padang,Tanggal/Bulan/2022**

**Dekan Fakultas Ilmu Komputer**

**Universitas Putra Indonesia “YPTK” Padang**

**Dr. Yuhandri, S.Kom, M.Kom**

**NIDN. 1015057301**

**ABSTRACT**

**Arie Soeharyanto, IMPLEMENTATION TO DETECT SERVER ATTACK USING SNORT INTRUSION DETECTION SYSTEM (IDS) AND SERVER SECURITY USING PORT KNOCKING AND IPTABLES FIREWALL**

The server is a service provider center and data processing center in a network, and a request sent by the client will be processed by the server. Server performance depends on data packets sent by clients on the network. If a threat or attack on the server, it will cause problems on server performance. To overcome this problem, a research was conducted by implementing the snort intrusion detection system (IDS) and port knocking on the server port security and iptables as firewall security. Snort-IDS is able to analyze packets passing through the network and try to determine whether there are data packets that contain suspicious activity or not. Port Knocking gives access to open ports and services only for certain users, and provides login access in the form of authentication, while those who are not authorized cannot access the port information itself. The iptables handling system uses the attacker's ip address to give action, the actions taken are divided into accept actions, reject actions and drop actions. The test was carried out with IP Portscanning attack conditions and slow HTTP DoS attacks. HTTP slow DoS attack is one of the methods of DoS attack targeting HTTP servers. This method hampers the service by flooding it causing a pool of connections with slow and heavy requests to the web server.

***Keyword* *:*** Server*, Network Security, Snort intrusion detection system (IDS), Port Knocking, Iptables, Port Scanning, Dos attack Slow HTTP. Web Servers*.

**ABSTRAK**

**Arie Soeharyanto, IMPLEMENTASI UNTUK MENDETEKSI SERANGAN SERVER MENGGUNAKAN SNORT INTRUSION DETECTION SYSTEM (IDS) DAN KEAMANAN SERVER MENGGUNAKAN PORT KNOCKING DAN IPTABLES FIREWALL**

Server adalah pusat penyedia layanan dan pusat pemrosesan data dalam suatu jaringan, dan sebuah permintaannya yang dikirim oleh *client* akan diproses oleh *server*. Kinerja *server* tergantung pada paket data yang dikirim oleh client pada jaringan. Jika sebuah ancaman atau serangan pada *server*, maka akan menimbulkan masalah pada kinerja *server*. Untuk mengatasi permasalahan tersebut, dilakukan penelitian dengan mengimplementasikan *snort intrusion detection system* (IDS**)** dan *port knocking* pada kemanan port server dan *iptables* sebagai keamanan firewall. Snort-IDS mampu menganalisis paket-paket yang melewati jaringan dan berusaha menentukan apakah terdapat paket-paket data yang berisi aktivitas mencurigakan atau tidak. Port Knocking memberikan akses untuk membuka port dan layanan hanya untuk pengguna tertentu, dan memberi akses masuk berupa otentifikasi, sementara yang tidak diberi kewenangan tidak dapat mengakses informasi port itu sendiri. Sistem penanganan iptables menggunakan alamat ip penyerang untuk diberikan aksi, aksi yang dilakukan terbagi menjadi aksi accept, aksi reject dan aksi drop. Pengujian dilakukan dengan kondisi serangan IP Portscanning dan serangan *DoS slow HTTP.* Serangan DoS slow HTTP adalah salah satu metode serangan DoS yang menargetkan server HTTP. Metode ini menghambat layanan dengan membanjiri sehingga menimbulkan kumpulan koneksi dengan permintaan yang lambat dan banyak menuju web server.

**Kunci*:*** Server*, Network Security, Snort intrusion detection system* (IDS), *Port Knocking, Iptables, Port Scanning, Dos serangan Slow HTTP. Web Server***.**

**KATA PENGANTAR**

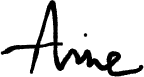
**S**egalapuji kita ucapkan kehadiran Tuhan Yang Maha Esa yang telah memberikan Rahmat dan Hidayahnya sehingga penulis dapat menyusun dan menyelesaikan laporan skripsi denagn judul **“IMPLEMENTASI UNTUK MENDETEKSI SERANGAN SERVER MENGGUNAKAN SNORT INTRUSION DETECTION SYSTEM (IDS) DAN KEAMANAN SERVER MENGGUNAKAN PORT KNOCKING DAN IPTABLES FIREWALL’’**

Penelitian ini adalah tindak lanjut dari ilmu yang telah didapatkan dari proses perkuliahan. Hasil penelitian ini diharapkan dapat membantu pihak pihak yang membutuhkan terutama untuk pengguna sehingga dapat meningkatkan efisien dan efektifitas kerja dalam menjalankan pekerjaan dan menyajikan informasi. Ucapan terima kasih juga tidak lupa penulis ucapkan kepada semua pihak yang juga telah membantu dalam menyelesaikan skripsi ini,terutam kepada :

1. Ibuk Dr.Zerni Melmusi, MM, Ak, selaku ketua Yayasan Perguruan Tinggi Komputer YPTK Padang
2. Bapak Prof. Dr. Sarjon Defit, S.kom, M.Sc, Selaku Rektor Universitas Putra Indonesia YPTK Padang.
3. Bapak Dr.Yuhandri, S.kom, M.kom, Selaku Dekan Fakultas Ilmu Komputer Universitas Putra Indonesia YPTK Padang.
4. Bapak Eka Praja Wiyata Mandala, S.kom, M.kom, M.kom, Selaku ketua Program Study Teknik Informatika Universitas Putra Indonesia YPTK Padang.
5. Bapak Randy Permana, S.kom, M.kom, Selaku Sekretaris I Program Study Teknik Informatika Universitas Putra Indonesia YPTK Padang.
6. Ibu Yesri Elva, S.kom, M.kom, Selaku Sekretaris II Program Study Teknik Informatika Universitas Putra Indonesia YPTK Padang.
7. Bapak Randy Permana, S.kom, M.kom, Selaku Dosen Pembimbing I yang telah memberikan masukan dan bimbingan dalam penyusunan atau penulisan tugas akhir ini.
8. Ibuk Rima Liana Gema, S.kom, M.kom, Selaku Dosen Pembimbing II yang telah memberikan masukan dan bimbingan dalam penyusunan atau penulisan tugas akhir ini.
9. Orang tua penulis yang selalu memberikan semangat dan dukungan kepada penulis dalam penyelesaian tugas akhir ini.
10. Bapak dan ibu dosen serta karyawan dan karyawati Universitas Putra Indonesia YPTK Padang yang telah banyak membantu penulis dalam segi ilmu maupun waktu semasa penulis menjadi mahasiswa disini.
11. Teman-teman penulis yang sama-sama memberikan bantuan, masukan dan sarannya demi penyelesaian tugas akhir ini.

Pada penyelesaian skripsi ini penulis menyadari bahwa hasil dari skripsi ini sangat jauh dari kesempurnaan, namun tetap diharapkan hasil dari penelitian ini dapat memberikan manfaat bagi penulis maupun pembaca dikemudian hari. Semoga skripsi ini dapat memberikan kontribusi terhadap masyarakat dan khususnya terhadap Universitas Putra Indonesia YPTK Padang.

Padang, 4 Juni 2021



Penulis

**DAFTAR ISI**

**HALAMAN JUDUL** i

**LEMBARAN PERNYATAAN** ii

**LEMBARAN PENGESAHAAN SKRIPSI iii**

**LEMBARAN PENGESAHAN LULUS SIDANG SKRIPSI iv**

**ABSTRACT** v

**ABSTRAK** vi

**KATA PENGANTAR** vii

**DAFTAR ISI** ix

**DAFTAR TABEL**

**DAFTAR GAMBAR**

**DAFTAR LAMPIRAN**

**BAB I PENDAHULUAN** 1

1.1 Latar Belakang Masalah 1

1.2 Perumusan Masalah 3

1.3 Hipotesa 3

1.4 Batasan Masalah 4

1.5 Tujuan Penelitian 4

1.6 Manfaat Penelitian 4

1.7 Gambaran Umum Object Penelitian 5

1.7.1 LLDIKTI 5

1.7.2 PENILAIAN ANGKA KREDIT (PAK) 6

17.3 Struktur Organisasi Dan Pembagian Tugas Serta Wewenang 8

**BAB II LANDASAN TEORI** 13

2.1 Jaringan Komputer 13

2.1.1 Pengertian Jaringan Komputer 13

2.1.2 Perangkat Jaringan Komputer 14

2.2 Topologi Jaringan 15

2.2.1 Topologi Bus 15

2.2.2 Topologi Ring (Cincin) 16

2.2.3 Topologi Star (Bintang) 17

2.2.4 Topologi Tree (Pohon) 18

2.2.5 Topologi Mesh (Tidak Beraturan) 19

2.3 Komponen Utama Jaringan Komputer 20

2.3.1 Lan Card 20

2.3.2 Hub 20

2.3.3 Switch 21

2.3.4 Router 22

2.3.5 Kabel jaringan dan Teknik Pengkabelan 22

2.4 Ancaman Jaringan Komputer 24

2.4.1 *Scanning* 24

2.4.2 *WEB Vulnerability Scanning* 24

2.4.3 *Reconnaissance* 25

2.4.4 Spam Email Dan Spyware 25

2.4.5 Implantasi Virus 25

2.5 *Denial of service* (DoS) 26

2.6 *Slow HTTP DoS Attack* 27

2.7 *Intrusion Detection System*  dan *Intrusion Prevention System* 27

2.7.1 *Intrusion Detection System* (IDS) 27

2.7.2 Signature Based IDS 29

2.7.3 Anomaly-Based IDS 30

2.7.4 *Intrusion Prevention System* (IPS) 30

2.8 Snort 30

2.9 Firewall dan IPTABLES 31

2.9.1 Firewall 31

2.9.2 IPTABLES 32

2.10 Port-Knocking 32

2.10.1 Metode Port Knocking 33

2.10.2 Cara Kerja Port Knocking 34

**BAB III METODOLOGI PENELITIAN** 16

3.1 Kerangka Penelitian 37

3.2 Tahapan Penelitian 38

3.2.1 Penelitian Pendahuluan 38

3.2.2 Pengumpulan Data 38

3.2.3 Analisa 40

3.2.4 Instalasi dan Konfigurasi 41

3.2.5 Implementasi 42

3.2.6 Hasil Pengujian 43

**BAB IV ANALISA DAN PERANCANGAN** 44

4.1 Analisa Network 44

4.2 Perancangan Mekanisme 45

4.2.1 Perancangan Mekanisme Snort 45

4.2.2 Perancangan Mekanisme IPTABLES 47

4.3 Rancangan Penujian Serangan 48

4.3.1 *Slow Headers* (Slowloris) 48

4.3.2 Serangan *port scanning* 49

4.3.3 Akses Port Secara langsung 49

4.4 Perancangan Network Topologi 50

**BAB V IMPLEMENTASI DAN PENGUJIAN 51**

5.1 Implementasi Sistem 51

5.1.1 Lingkungan Implementasi 51

5.1.2 Perangkat Keras 51

5.1.1.2 Perangkat Lunak 51

5.2 Pengujian 52

5.2.1 Pengujian mendeteksi aplikasi snort 52

5.2.2 Pengujian Port Scanning 54

5.2.3 *Slow HTTP DDOS Attack* 55

5.2.4 Port Knocking 58

5.3 Tabel Hasil Pengujian 60

**BAB VI PENUTUP 61**

6.1 Kesimpulan 61

6.2 Keterbatasan Sistem 61

6.3 Saran 62

**DAFTAR PUSTAKA**

**DAFTAR LAMPIRAN**

**DAFTAR GAMBAR**

Gambar 1.1 Struktur Organisasi LLDIKTI WILAYAH X 8

Gambar 2.1 Topologi Bus 15

Gambar 2.2 Topologi Ring 16

Gambar 2.3 Topologi Star (Bintang) 17

Gambar 2.4 Topologi Tree (Pohon) 18

Gambar 2.5 Topologi Mesh (Tidak Beraturan 19

Gambar 2.6 Network Interface Card 20

Gambar 2.7 Hub 20

Gambar 2.8 Switch 21

Gambar 2.9 Router 22

Gambar 2.10 Klasifikasi DoS 26

Gambar 2.11 Metode Port Knocking 34

Gambar 2.12 Block dari firewall input 34

Gambar 2.13 Ketukan open knock 7000 8000 dan 9000 35

Gambar 2.14 Membuka port ssh 35

Gambar 2.15 Membuka ssh port 22 agar masuk ke server 36

Gambar 2.16 Close Knock 36

Gambar 3.1 Kerangka Penelitian 37

Gambar 4.1 Topologi Jaringan LLDIKTI 45

Gambar 4.2 Gambaran Mekanisme snort 46

Gambar 4.3 Gambaran Mekanisme IPTABLES 47

Gambar 4.4 Ilustrasi gambaran serangan 48

Gambar 4.5 Ilustrasi gambaran port knocking 49

Gambar 4.6 Gambaran Perancangan Network 50

Gambar 5.1 Tampilan Proses mendeteksi snort 52

Gambar 5.2 Tampilan Log pada more alert 53

Gambar 5.3 Hasil ip scanning tanpa iptables 54

Gambar 5.4 Hasil ip scanning dengan iptables 55

Gambar 5.5 Tampilan serangan Slowloris tanpa iptables 55

Gambar 5.6 Tampilan web server yang terkna slowloris 56

Gambar 5.7 Tampilan Slowloris dengan iptables 56

Gambar 5.8 Tampilan webserver tidak terkena slowloris 57

Gambar 5.9 Tampilan PortKnocking di aktifkan 58

Gambar 5.10 Tampilan tidak terhubung SSH 58

Gambar 5.11 Tampilan knocking 59

Gambar 5.12 Tampilan SSH yang dapat di akses 59

**DAFTAR TABEL**

Tabel 2.1 Jenis Kabel Jaringan 23

Tabel 2.2 Tipe Kabel 23

Tabel 3.1 Jadwal Penelitian 22

Tabel 5.1 Tabel Black Box Hasil Pengujian 60

**BAB I**

**PENDAHULUAN**

* 1. **Latar Belakang Masalah**

Lembaga Layanan Pendidikan Tinggi atau disingkat LLDIKTI X sebelumnya bernama Koordinasi Perguruan Tinggi Swasta atau Kopertis yang merupakan salah satu unit kerja di lingkungan Kementerian Pendidikan dan Kebudayaan (Kemdikbud). Dan sistem pada LLDIKTI X terdapat PAK Online yaitu Penilaian Angka Kredit untuk kenaikan jabatan dosen sistem ini harus dilindungi dan diamankan agar data-data Dosen dapat terjaga dengan aman.

Kemajuan teknologi di bidang jaringan mengharuskan untuk terkoneksi komputer dengan komputer lainnya. Suatu jaringan komputer biasanya terdiri dari server dan client. Server dan Client diartikan sebagai suatu perancangan jaringan komputer yang mana perangkat client melakukan proses meminta data, dan server yang bertugas untuk memberikan respon dari feedback yang berupa data. Menurut (Refflan, 2012) Client adalah perorangan yang menghubungkan dengan server untuk meminta data atau layanan ke server sedangkan server adalah, perorangan yang menyediakan data atau layanan yang di diharapkan oleh client. Client-Server adalah pembagian tugas antara server dan client yang mempunyai akses menuju server di dalam suatu satu jaringan. Jadi arsitektur client-server ialah desain aplikasi yang berisi client dan server yang saling berkomunikasi ketika hendak mengakses server untuk suatu jaringan,

Kinerja server berpegang terhadap paket data yang digunakan oleh client pada jaringan.

Pertukaran data melalui jaringan internet yang paling awal dikembangkan dan masih digunakan hingga saat ini adalah FTP (file transfer protocol), dimana dengan protocol ini user dapat melakukan pertukaran data baik pengunduhan (download) dan pengunggahan (upload). FTP merupakan protokol level aplikasi dalam standarisasi protokol OSI yang digunakan untuk standar proses file transfer. Dalam menjalankan fungsinya, inisialisasi transfer FTP yaitu pada port nomor 21 yang menggunakan port TCP (transmission control protocol) sebagai komunikasi data komputer client dan server. Dalam suatu jaringan Administrator bertindak untuk memonitoring dan meremot suatu server dan Administrator haruslah orang yang berhak agar mengakses server tersebut.

Maka dari itu, keamanan data pada komputer server PAK Online LLDIKTI harus diperhatikan dan di jaga sehingga Data-Data yang ada didalamnya menjadi confidentialitas, availibilitas, integritas menjadi aman dan terjaga.

Metode-metode pencegahan dan keamanan terhadap serangan pada sistem informasi harus terus dikembangkan. Beberapa aplikasi atau sistem telah dikembangkan dan diterapkan untuk mengatasi serangan yang terjadi. Contohnya teknik pengamatan dengan firewall atau Intrusion Prevention System (IPS) untuk mencegah serangan, atau pendeteksian pada saat mulai terjadi serangan dengan Intrusion Detection System (IDS). Snort merupakan salah satu aplikasi yang dapat berfungsi sebagai IDS ataupun IPS. Snort merupakan suatu perangkat lunak untuk mendeteksi penyusup dan mampu menganalisis paket yang melintasi jaringan secara real time. Traffic dan logging ke dalam database serta mampu mendeteksi berbagai serangan.

Tindakan pencegahan yang bisa di lakukan untuk mencegah keamanan yaitu pencegahan yang dilakukan dengan penjagaan di sistem operasi, aplikasi, infrastuktur jaringan dan komputer server, penerapan sistem pencegahaan penyusupan dan lain sebainya. Maka dari itu, dibangun Firewall dengan *Intrusion Detection system* (IDS) dan IPTABLES sehingga dapat melakukan mendeteksi dan proteksi pada komputer server. IDS mampu memantau trafik jaringan yang melewati komputer server dan mampu bekerja dengna membangun sebuah engine yang membaca IP asal penyerang kemudian IPTables digunakan untuk memberikan penanganan terhadap serangan sesuai dengan aksi yang dilakukan oleh administrator dan rancang sebuah rules Firewall untuk memblok akses dari IP penyerang tersebut dan dikombinasikan dengan Port Knocking dapat menjaga dalam meremot komputer server dan juga port-port penting dalam komputer server. Beradasarkan pada informasi diatas penulis mengangkat judul “IMPLEMENTASI UNTUK MENDETEKSI SERANGAN SERVER MENGGUNAKAN SNORT INTRUSION DETECTION SYSTEM (IDS) DAN KEAMANAN SERVER MENGGUNAKAN PORT KNOCKING DAN IPTABLES FIREWALL PADA LLDIKTI WILAYAH X BAGIAN PAK ”

* 1. **Perumusan Masalah**

Rumusan masalah yang dibuat dapat dirumuskan berdasarkan latar belakang diatas adalah:

1. Bagaimana Snort intrusion detection system dapat mendeteksi serangan terhadap komputer server PAK online LLDIKTI X?
2. Bagaimana cara mengkonfigurasi IPTABLES agar dapat menangkal dan meningkatkan sistem pada komputer server PAK online LLDIKTI X?
3. Bagaimana Port Knocking dapat menangkal dan meningkatkan keamanan sistem terhadap komputer server PAK online LLDIKTI X?
   1. **Hipotesa**

Berdasarkan perumusan di atas, maka penulis juga dapat menarik hipotesa-hipotesa yang dapat memberikan kesimpulan sementara sebagai acuan penulis dalam menyelesaian penelitian ini, antara lain:

1. Dengan menggunakan SNORT INTRUSION DETECTION SYSTEM (IDS) diharapkan dapat mendeteksi aktivitas yang masuk ke server PAK online LLDIKTI X.
2. Dengan menggunakan Firewall IPTABLES diharapkan dapat mengamankan server dari Serangan jaringan pada server PAK online LLDIKTI X.
3. Dengan Menggunakan Port Knocking diharapkan dapat mengamankan Port pada server PAK online LLDIKTI X.
   1. **Batasan Masalah**

Menghindari terlalu luasnya permasalahan dan pemecahan masalah yang dilakukan, maka perlu dibatasi sistem yang dirancang. Batasan-batasan yang diberikan adalah :

1. Untuk menganalisa serangan yang masuk ke server PAK online LLDIKTI X.
2. Mengetahui jenis kemanan yang dirancang.
3. Mengetahui jenis Port yang akan di amankan pada server PAK online LLDIKTI X.
   1. **Tujuan Penelitian**

Tujuan dari mengembangkan sistm pendukung keputusan penerimaan karyawan yaitu sebagai berikut:

1. Untuk menerapkan sistem keamanan Firwall pada Server PAK online LLDIKTI.
2. Untuk menerapkan sistem pantuan atau monitoring agar mengetahui aktivitas yang masuk pada Server PAK online LLDIKTI.
3. Untuk menerapkan sistem kemanan pada Port pada PAK online LLDIKTI.
   1. **Manfaat Penelitian**

Manfaat yang didapaat dalam penggunaan pendukung keputusan penerimaan karyawan adalah:

1. Sistem yang dibangun dapat mempermudah dalam pemantuan pada server PAK online LLDIKTI X.
2. Sistem yang dibangun dapat mempertahankan dalam serangan jaringan pada server PAK online LLDIKTI X.
3. Menjaga keamanan Port server dalam akses port tertentu pada server PAK online LLDIKTI X.
   1. **Gambaran Umum Object Penelitian**

**1.7.1 LLDIKTI**

Lembaga Layanan Pendidikan Tinggi disingkat LLDIKTI, sebelumnya bernama Koordinasi Perguruan Tinggi Swasta atau Kopertis yang merupakan salah satu unit kerja di lingkungan Kementerian Pendidikan dan Kebudayaan (Kemdikbud). Undang-Undang Nomor 12 Tahun 2012 tentang Pendidikan Tinggi mengamanatkan bahwa Pemerintah perlu membentuk Lembaga Layanan Pendidikan Tinggi (LLDIKTI). Hal ini menjadi dasar dari perubahan nama Kopertis Wilayah X menjadi Lembaga Layanan Pendidikan Tinggi (LLDIKTI) Wilayah X. Berdasarkan Peraturan Menteri Pendidikan dan Kebudayaan Nomor 34 Tahun 2020 tentang Organisasi Tata Kerja Lembaga Layanan Pendidikan Tinggi, LLDIKTI Wilayah X mempunyai tugas dan fungsi di bidang fasilitasi peningkatan mutu penyelenggaraan pendidikan tinggi di wilayah kerjanya (Sumatera Barat, Riau, Jambi, dan Kepulauan Riau) yang dipimpin oleh seorang Kepala dan bertanggung jawab kepada Menteri Pendidikan dan Kebudayaan. Dalam peraturan tersebut, susunan organisasi Lembaga Layanan Pendidikan Tinggi terdiri atas Kepala, Sekretariat, dan dan Kelompok Tenaga Ahli. Sekretariat LLDIKTI Wilayah X dipimpin oleh sekretaris dan terdiri atas bagian tata usaha dan kelompok jabatan fungsional. LLDIKTI Wilayah X berfungsi melaksanakan pemetaan mutu pendidikan tinggi, fasilitasi peningkatan mutu penyelenggaraan pendidikan tinggi, fasilitasi peningkatan mutu pengelolaan perguruan tinggi, fasilitasi kesiapan perguruan tinggi dalam penjaminan mutu eksternal, evaluasi dan pelaporan pelaksanaan fasilitasi peningkatan mutu perguruan tinggi, pengelolaan data dan informasi di bidang mutu pendidikan tinggi, dan pelaksanaan administrasi LLDIKTI Wilayah X. Dalam melaksanakan tugasnya, LLDIKTI dibantu oleh kelompok tenaga ahli. Kelompok tenaga ahli diangkat dan diberhentikan oleh Kepala atas persetujuan Menteri Pendidikan dan Kebudayaan. Tugasnya, membantu Kepala untuk melaksanakan kegiatan sesuai dengan bidang keahlian masing-masing dalam peningkatan mutu penyelenggaraan perguruan tinggi yang ditentukan berdasarkan kebutuhan dan beban kerja LLDIKTI.

**1.7.2 PENILAIAN ANGKA KREDIT (PAK)**

Penilaian Angka Kredit Kenaikan jabatan Akademik/Pangkat Dosen (PO 2019) ini merupakan penyempurnaan dari PO 2014, yang dikembangkan dengan merujuk pada perubahan peraturan perundangan terkait serta dalam konteks menguatkan upaya peningkatan mutu dosen perguruan tinggi melalui publikasi karya ilmiahnya, termasuk karya ilmiah prestisius dan luar biasa. Standar, tata cara dan prosedur penilaian angka kredit dosen untuk kepentingan pengusulan jabatan akademik/pangkat dosen memerlukan penyempurnaan yang bersifat mendasar dan menyeluruh, dengan mengacu pada Undang-undang Nomor 20 tahun 2003 tentang sistem Pendidikan Nasional, Undang-Undang Nomor 14 tahun 2005 tentang Guru dan Dosen Peraturan Pemerintah Nomor 37 tahun 2009 tentang Dosen dan Undang-Undang Nomor 12 tahun 2012 tentang Pendidikan Tinggi.

Peraturan turunan dari Undang-Undang tersebut memberikan arahan yang lebih spesifik tentang kenaikan jabatan/pangkat dosen, termasuk Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 17 Tahun 2013 tentang jabatan Fungsional Dosen dan Angka Kreditnya juncto Nomor 46 Tahun 2013 tentang Perubahan atas Peraturan Menteri Pendayagunaan Aparatur Negara dan reformasi Birokrasi Nomor 17 Tahun 2013 tentang jabatan Fungsional Dosen dan Angka Kreditnya, Peraturan Bersama Menteri Pendidikan dan Kebudayaan dan Kepala Badan Kepegawaian Negara Nomor 4/VIII/PB/2014 dan Nomor 24 Tahun 2014 tentang Ketentuan Pelaksanaan Jabatan Fungsional Dosen dan Angka Kreditnya, dan Peraturan Menteri Pendidikan dan Kebudayaan Nomor 92 Tahun 2014 tentang Petunjuk Teknis Pelaksanaan Penilaian Angka Kredit Jabatan fungsional Dosen dan Angka Kreditnya, dan Peraturan Menteri Riset, Teknologi dan Pendidikan tinggi Nomor 26 Tahun 2015 Juncto Nomor 2 Tahun 2016 tentang Registrasi Pendidik pada Perguruan Tinggi. Peraturan yang terakhir ini secara spesifik memerinci kategori pendidik di perguruan tinggi dengan Nomor Induk Dosen Nasional (NIDN), Nomor Induk Dosen Khusus (NIDK) dan Nomor Urut Pendidik (NUP). Untuk itu diperlukan penyesuaian pengaturan berkenaan dosen di perguruan tinggi sekaitan dengan kenaikan jabatan akademik/pangkat. Dalam rangka dinamika untuk menghargai prestasi karya ilmiah dan keluarbiasaan kinerja dosen maka proses penilaian akan mengakomodasi kombinasi sekuensial antara jabatan akademik dan pangkat.

Selain itu, terlihat pesat adanya perkembangan ragam karya tulis dan jenis tempat pemuatan karya tulis tersebut. Pedoman ini diharapkan mampu mendorong produktivitas karya ilmiah dan penerbitannya. Disadari bahwa jabatan akademik dosen pada dasarnya merupakan pengakuan, penghargaan dan kepercayaan atas kompetensi, kinerja, integritas dan tanggung jawab dalam pelaksanaan tugas, serta tata krama dosen dalam melaksanakan tugas tridharmanya. Selain itu diharapkan pula bahwa jabatan ini dapat berfungsi sebagai insentif non-menteri bagi dosen untuk berkerja lebih giat, lebih kreatif, dan lebih baik lagi. Oleh karenanya, maka standar, tata cara dan prosedur penilaian seyogyanya sejalan dan bersifat kondusif bagi terciptanya tujuan dimaksud.

**1.7.3 Struktur Organisasi Dan Pembagian Tugas Serta Wewenang**



**Gambar 1.1** **Struktur Organisasi LLDIKTI WILAYAH X**

1. **Kepala LLDIKTI Wilayah X Prof. Dr. Herri, MBA**

LLDIKTI diminta Kemdikbud untuk meningkatkan kualitas perguruan tinggi, bersama-sama bekerja sama dan berkontribusi untuk pendidikan tinggi yang berkualitas melalui pelayanan yang berkualitas.

Untuk optimalisasi layanan kepada stakeholders, LLDIKTI Wilayah X mengembangkan beberapa aplikasi, seperti:

• e-office (Layanan Persuratan)

• Penilaian Angka Kredit (PAK) online

• Gugus Layanan Mutu (Gulamu)

* Pendampingan dan Audit Sistem Penjaminan Mutu (SPMI)
* Pelatihan, Pendampingan, Pre Asesmen Dokumen Akreditasi Program Studi dan Akreditasi Perguruan Tinggi

• Sistem Informasi Manajemen Dosen (Simdos)

• LAPOR (Pengaduan Masyarakat)

1. **Sekretaris LLDIKTI Wilayah X Yandri. A, SH, MH**

Untuk layanan tatap muka, di LLDIKTI Wilayah X terpusat pada Unit Layanan Terpadu (ULT). Layanan satu pintu ini berfungsi sebagai wadah dalam efisiensi dan efektivitas layanan kepada masyarakat sebagai perwujudan reformasi birokrasi.

1. **Kepala Bagian Tata Usaha LLDIKTI Wilayah X Ir. Yuniati**

Mempunyai tugas melaksanakan urusan perencanaan, keuangan, kepegawaian, barang milik negara, hukum, organisasi dan ketatalaksanaan, hubungan masyarakat, persuratan, kearsipan, dan kerumahtanggaan.

Bagian Tata Usaha menyelenggarakan fungsi:

a. penyusunan bahan rencana, program, dan anggaran;

b. pengelolaan keuangan;

c. pengelolaan kepegawaian;

d. pengelolaan barang milik negara;

e. pelaksanaan urusan hukum;

f. pelaksanaan urusan organisasi dan ketatalaksanaan;

g. pelaksanaan urusan hubungan masyarakat;

h. pelaksanaan urusan persuratan, kearsipan, dan kerumahtanggaan; dan

i. penyusunan laporan.

Dalam upaya meningkatkan mutu perguruan tinggi, LLDIKTI Wilayah X juga menyelenggarakan program-program seperti:

1.      Workshop Pemantapan Program PDDIKTI Feeder, PIN (Penomoran Ijazah Nasional) dan Sistem Verifikasi Ijazah Secara Elektronik (SIVIL)

2.      *Training Of Trainer* (ToT) Pengembangan Kurikulum Perguruan Tinggi

3.      Pelatihan Penyusunan BKD LKD

4.      Pelatihan Pembekalan Program Sertifikasi Dosen

5.      Bimtek Penyususnan Dokumen Mutu Sistem Penjaminan Mutu Internal (SPMI), Audit Mutu Internal (AMI)

6.      Workshop Akreditasi Program Studi dan Akreditasi Perguruan Tinggi

7.      Bimtek Akreditasi Unggul Perguruan Tinggi

8.      Manajemen Perguruan Tinggi dan Kepemimpinan

9.      Peningkatan Kerja Sama Perguruan Tinggi

10.  Bimtek Pembuatan Proposal Program Pengembangan Perguruan Tinggi Swasta (PP PTS)

11.  Entrepreneurship Award

12.  Olimpiade Nasional Matematika dan Ilmu Pengetahuan Alam (ON-MIPA)

13.  Kompetisi Debat Mahasiswa Indonesia (KDMI)

14.  *National University Debate Championship* (NUDC)

15.  Pemilihan Mahasiswa Berprestasi

16.  Pemilihan Diktendik Berprestasi

**BAB II**

**LANDASAN TEORI**

**2.1 Jaringan Komputer**

**2.1.1 Pengertian Jaringan Komputer**

Jaringan Komputer merupakan media telekomunikasi yang menghubungkan antar komputer untuk saling terkoneksi dan juga bertukar data. Jaringan komputer dirancang dengan kombinasi hardware dan software. Saat dua komputer atau lebih komputer yang saling terhubung satu sama lain dan digunakan untuk berukar data, ada bagian-bagian dari jaringan komputer yang menjadi pihak yang menerima layanan yang disebut dengan client, dan yang mengirimkan disebut dengan server. Cara seperti ini disebut dengan Sistem Client- Server (Putri et al., 2016).

Ada beberapa jenis-jenis jaringan komputer yang dapat dibagi pada cangkupan areanya, yaitu:

1. LAN (Local Area Network)

LAN atau​​ Local Area Network​​ meruapa konsep yang menghubungkan suatau perangkat jaringan dalam jarak yang relatif dekat atau pendek. Biasanya dapat di gunakan untuk rumah, sekolah, kantor atau perusahaan, dan lain-lain. Jaringan LAN biasanya cenderung menggunakan konektivitas tertentu, terutapa Token Ring dan Ethernet.

Terdapat juga jaringan LAN yang memakai teknologi jaringan​​ Wireless​​ atau nirkabel dengan WI-FI yang dikenal dengan nama​​ Wireless Local Area Network (WLAN) (Putri et al., 2016).

1. MAN (Metropolitan Area Network)

MAN atau​​ Metropolitan Area Network​​ meruapakan konsep yang menghubungkan perangkat jaringan dari satu Kota ke Kota, atau perusahan ke perusahan lainnya. Jika jarak cangkupan LAN sudah tidak memungkinkan untuk membangun jaringan, maka jaringan MAN yang lebih tepat di gunakan, dikarenakan jarak cangkupannya yang lebih besar dari LAN, maka MAN memerulukan perangkat khusus dan memerlukan​​ operator​​ telekomunikasi yang bekerja sebagai penguhubung antar jaringan komputer (Putri et al., 2016).

1. WAN (Wide Area Network)

WAN atau​​ Wide Area Network​​ merupakan konsep yang menghubungkan perangkat jaringan dari satu pulau, negara, dan juga benua. Komputer yang mencangkup wilayah super luas dan umumnya WAN dihubgkan dengan jaringan telepon digital dan juga menggunakan peralatan yang super canggih apabila di bandingkan dengan MAN dan LAN (Putri et al., 2016).

1. Internet

Internet merupakan interkoneksi jaringan-jaringan komputer yang berada di dunia. Yang jangkauannya sudah menggapai satu dunia, lalu tidak menutup kemungkinan jangkauannya antar planet. Koneksi yang ada pada jaringan komputer dapat dijalankan berkat adanya bantuan protokol yang khusus yaitu Internet Protocol (IP) (Putri et al., 2016).

**2.1.2 Perangkat Jaringan Komputer**

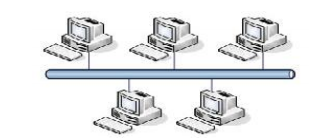
Perangkat keras (Hardware) Merupakan bentuk fisik komputer yang dibedakan dengan data yang berpengaruh didalamnya atau beroperasi di dalamnya, yang dibedakan dengan perangkat lunak (software) dan menyedikan informasi untuk perangkat keras dalam menjalankan tugasnya. Secara umum, perangkat keras/hadwareyang yang butuhkan agar membangun sebuah jaringan komputer yaitu: Network Interface Card (NIC), Swicth, dan semua yang bersangkutan dengan koneksi jaringan seperti : Bridges, Router dan lainnya untuk proses transformasi data di dalam jaringan (Putri et al., 2016).

**2.2 Topologi Jaringan**

Topologi jaringan merupakan struktur yang dibuat pada suatu jaringan komputer atau suatu metode untuk mengkoneksikan komputer satu dengan komputer yang lain sehingga bisa membangun suatu jaringan komputer, Secara definisi topologi terbagi dua, yaitu topologi fisik (physical topology) dan topologi logik (logical topology) (Yulianeu & Wahab, 2017).

Berikut topologi yang dimaksud :

**2.2.1. Topologi Bus**



**Gambar 2.1** **Topologi Bus (Sumber : Yulianeu & Wahab, 2017).**

**Sumber :**

Topologi Bus adalah topologi yang disebut topologi Backbone, dikarnakan pada massa penggunaan kabel coaxial menjamur, pada topologi ini setiap komputer akan terhubung ke satu kabel Panjang dengan beberapa terminal, dan pada ujung dari kabel harus di akhiri dengan satu terminator.

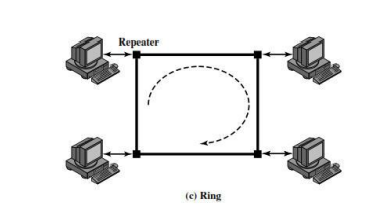
Kelebihan Topologi Bus :

1. Biaya yang lebih murah
2. Tidak memerlukan sumber daya kabel yang banyak
3. Kerusakan satu komputer client tidak akan mempengaruhi komunikasi antar client yang lain.

Kekurangan Topologi Bus :

1. Jika kabel backbone putus maka koneksi gagal.
2. Jika kabel utama sangat Panjang maka sulit untuk melakukan troubleshoot dan akan terjadi tabarkan data (data collision) (Yulianeu & Wahab, 2017).

**2.2.2 Topologi Ring (Cincin)**



**Gambar** **2.2 Topologi Ring (Sumber : Santoso, 2016).**

Topologi Ring dapat disebut dengan topologi cincin karena bentuknya sama seperti cincing yang melingkar. Metode ini menghubungkan setiap komputer dengan cara membentuk sebuah cincin. Terdapat ciri-ciri khsusu topologi ring yaitu menggunakan kabel UTP dan Patch Cable yang membentuk jaringan menyerupai lingkaran sederhana dan teridiri dari node disusun secara seri. Fungsi yang diperlukan dalam topologi ring :

1. Penyelipan data

Penyelipan data merupakan sebuah proses yang diamna saat data dikirim kedalam saluran transmisi oleh terminal pengiriman setelah diberi alamat dan bit-bit tamabahan lainnya.

1. Penerimaan data

Penerimaan data merupakan proses yang dimana saat alamat yang dituju telah menerima data dari pengirim data, terdapat cara membandingkan alamat yang berada pada paket data dengan alamat terminal itu sendiri. Dan ketika alamat tersebut dikirim kembali ke alamat yang sama maka data yang dikirim akan disalin.

1. Pemindahan data

Pemindahan data merupakan proses pada saat kiriman data diambil Kembali oleh terminal pengiriman dikarenakan tidak ada terminal yang menerima data tersebut atau kemungkinan salah alamat pada penerimaan data. Dan jika data tersebut tidak diambil kembali oleh pengirim maka data yang dikirim tadi akan terus berputar-putar dalam saluran.

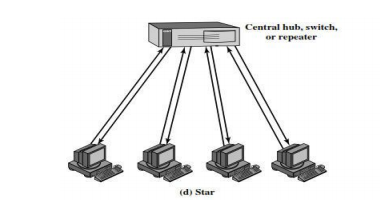
Kelebihan Topologi Ring :

1. Stabilitas koneksi cukup baik.
2. Proses pemasangan dan konfigurasi lebih mudah.
3. Biaya pemasangan lebih murah.

Kekurangan Topologi Ring :

1. Jika terdapat masalah koneksi, maka untuk troubleshooting jaringan akan rumit.
2. Sangat rentan akan terjadinya tabrakan arus data.
3. Jika terdapat salah satu koneksi client bermasalah maka koneksi pada jaringan akan terputus (Yulianeu & Wahab, 2017).

**2.2.3 Topologi Star (Bintang)**



**Gambar** **2.3 Topologi Star (Bintang) (Sumber : Santoso, 2016).**

Disebut topologi star karena bentuknya seperti bintang, Jaringan yang dihubungkan dari beberapa komputer yang memiliki koneksi dengan concentrator bisa beruapa hub atau switch. Pada topologi Star (Bintang) terdapat terminal pusat yang menjadi pengatur dan pengendali semua komunikasi yang terjadi. Segala aktivitas pertukaran data yang dilakukan akan melewati jaringan di pusat.

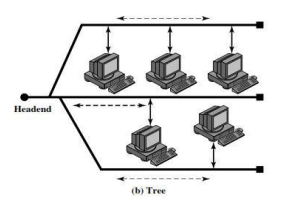
Kelebihan Topologi Star (Bintang) :

1. Untuk kegagalan pada satu terminal tidak akan mempengaruhi komunikasi pada terminal lain.
2. Untuk menambah jumlah client atau komputer maka tidak perlu mengganggu aktivitas jaringan yang lain.

Kekurangan Topologi Star (Bintang) :

1. Bila kegagalan terdapat pada pusat kontrol maka semua koneksi akan terputus.
2. Aktivitas data yang padat dapat membuat koneksi jaringan bekerja lebih lambat (Yulianeu & Wahab, 2017).

**2.2.4 Topologi Tree (Pohon)**

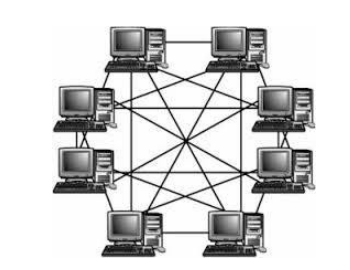


**Gambar** **2.4 Topologi Tree (Pohon) (Sumber : Santoso, 2016).**

Topologi pohon meruapakan gabungan topologi bus dan star. Media transmisi merupakan satu kabel yang bercabang namun loop tidak tertutup. Yang dimana topologi bus menjadi konektor utama dari menghubungkan topologi star.Beberapa kesulitan pada topologi tree (pohon) :

1. Sulit mengetahui kemana data yang dikirim, dikarenakan banyak cabang yang begitu banyak pada cabang pada topologi.
2. Perlu suatu proses untuk mengatur pengiriman dari terminal-terminal dalam jaringan (Yulianeu & Wahab, 2017).

**2.2.5 Topolgi Mesh (Tidak Beraturan)**



**Gambar** **2.5 Topologi Mesh (Tidak Beraturan) (Sumber : Santoso, 2016).**

Topologi Mesh merupakan topologi yang terbentuk dengan ketidak sengajaan atau tidak memiliki perencanaan awal ketika membangun suatu jaringan dan tidak mempunyai aturan dalam koneksi. Karena terbentuk dengan ketidak sengajaan dan tidak teratur maka sulit untuk menemukan kegagalan komunikasi, dan ada kemungkinan boros dalam pemakaian media transmisi. Tetapi topologi ini dapat meningkatkan proses transfer data dikarenakan langsung dikirim langsung ke komputer yang dituju tanpa perantara (Yulianeu & Wahab, 2017).

**2.3** **Komponen Utama Jaringan Komputer**

**2.3.1 Lan Card**



**Gambar** **2.6 Network Interface Card** (Sumber : Aini, 2019)**.**

Lan Card atau Network Interface Card (NIC) adalah sebuah komponen yang tepenting saat membangun sebuah jaringan, perancangan jaringan dalam sekala besar maupun sekala kecil, Lan Card berguna untuk menghubungkan jaringan internet dengan komputer yang menggunakan kabel LAN (Aini, 2019).

**2.3.2 Hub**



**Gambar** **2.7 Hub (Sumber : Aini, 2019).**

Hub merupakan sebuah komponen yang berfungsi untuk mengambil daya listrik dari stop kontak pada dinding biasa, dan hub berfungsi menghubungkan beberapa komputer satu dengan kompter lainnya dalam satu koneksi jaringan (Aini, 2019).

**2.3.3 Switch**



**Gambar** **2.8 Switch (Sumber : Aini, 2019).**

Switch sekilas hampir sama dengan hub tetapi memiliki fungsi yang berbeda yaitu bridge (menghubungkan dua buah LAN). Switch memiliki beberapa port sehingga switch disebut multiport bridge. Jika salah satu port yang terdapat pada switch mengalami lalu lintas jaringan yang padat (sibuk) maka port-port lainnya akan tetap berfungsi. Tetapi, bridge dan switch tidak dapat melanjutkan paket yang akan dikirim ke alamat IP yang tertuju ke komputer lain yang secara Logika tidak dalam satu network atau berbeda jaringan (Aini, 2019).

**2.3.4 Router**



**Gambar** **2.9 Router (Sumber : Aini, 2019).**

Router merupakan perangkat yang berfungsi untuk menghubungkan beberapa jaringan, baik itu jaringan yang sama atau juga jaringan yang berbeda yang memiliki lapisan OSI I, II dan III, contoh sebuah LAN dengan Netware yang akan dikoneksikan dengan jaringan yang menggunakan UNIX (Aini, 2019) (Aini, 2019).

**2.3.5 Kabel Jaringan dan Teknik Pengkabelan**

Sebuah komponen jaringan komputer yang mejadi alat untuk menghubungkan suatu sisi dengan sisi yang lainnya disebut kabel. Tetapi bukan berarti bagian kurva yang tertutup dan bisa jadi merupakan bagian kurva terbuka ( dengan terbuka dengan terminator di ujungnya). Perkembangan teknologi dalam alat penghubung atau perkabelan mulai mengalami perubahan. Contoh kabel fiber optik yang menjadi salah satu perkembangan jaringan komputer. Bentuk dan fungsi jaringan komputer dapat menentukan pemilihan jenis kabel untuk melihat ketersediaan kabel dan juga harga menjadi peninjauan utama untuk membangun sebuah jaringan (Aini, 2019).

**Tabel** **2.1 Jenis Kabel Jaringan (Sumber : Aini, 2019).**

|  |  |  |
| --- | --- | --- |
| Physical Topology | Common Cable | Common Protocol |
| Ring | Fiber Twisted Pair | Token Ring |
| Linear Bus | Twisted Pair Coaxial Fiber | Ethernet LocalTalk |
| Star | Twisted Pair Fiber | Ethernet LocalTalk |

**Tabel** **2.2 Tipe Kabel (Sumber : Aini, 2019).**

|  |  |  |
| --- | --- | --- |
| Cable | Type | Feature |
| Type CAT 1 | UTP | Analog (biasanya digunakan di perangkat telephon pada umumnya dan pada jalur ISDN – integrated service digital network. Juga untuk menghubungkan modem dengan line telepon) |
| Type CAT 2 | UTP | Up to 1 Mbits (sering digunakan pada topologi *token ring*) |
| Type CAT 3 | UTP/STP | 16 Mbits data transfer (sering digunakan pada topologi *token ring* atau 10Baset) |
| Type CAT 4 | UTP STP | 20 Mbits data transfer (biasanya digunakan pada topologi token ring) |
| Type CAT 5 | UTP,STP – up to 100 MHz | 100 Mbits data transfer / 22 db |
| Type CAT 5 enhanced | UTP,STP – up to 100 MHz | 1 gigabit Ethernet up to meters- 4 copper pairs (kedua jenis CAT5 sering digunakan pada topologi token ring *16Mbps* atau pada *fastEthernet* 100*Mbps*) |
| Type CAT 6 | Up to 155 MHz or 250 MHz | 2,5 Gigabit Ethernet up to 100 meter or 10Gbit/s up to 25 meter / 20,2 db (Gigabit Ethernet) |
| Type CAT 7 | Up to 200 MHz or 700 MHz | Giga – Ethernet / 20.8 db (Gigabit Ethernet) |

**2.4 Ancaman Jaringan Komputer**

Vulnerability merupakan sebuah aktivitas yang berjalan pada sebuah komputer yang dapat secara langsung atau tidak langsung maka akan memicu kebocoran kerahasiaan, integritas, ketersediaan informasi atau data pada jaringan (Utomo et al., 2017).

**2.4.1 *Scanning***

*Scanning* merupakan awal dimulainya serangan *hacker*. Yang dimana *hacker* akan mencari tau hal-hal apa saja yang dapat memungkinkan untuk mengambil alih komputer korban. Dengan informasi yang didapat pada komputer korban yang di *scanning*, *hacker* dapat mencari tau jalan untuk mengambil alih komputer korban karnah lemahnya sistem keamanan pada komputer tersebut. DenganBermacam-macam *tool* yang biasanya digunakan oleh *hacker* dalam membantu proses *scanning* (Utomo et al., 2017)*.*

**2.4.2 *Web Vulnerability Scanning***

*Vulnerability scanning* adalah *scanning* yang bertujuan untuk mencari tau kelemahan dari sebuah sistem. Beberapa *software* *vulnerability scanning* yang biasanya digunakan yaitu, Saint, Nessus, Nmap, Nikto, SQLmap, Scrawlr (*SQL Injection Scanner),* WPScan, Wikto dan lain-lain (Utomo et al., 2017).

**2.4.3 *Reconnaissance***

*Reconnaissance* merupakan tahapan untuk mengumpulkan data yang diamana saat *hacker* akan mengumpulkan semua data sebanyak mungkin mengenai target. Reconnaissance terbagi menjadi dua, yaitu : (Utomo et al., 2017).

1. *Active reconnaissance*

*Reconnaissance* yang dilakukan secara aktif, saat hacker melakukan aktivitas kepada korban agar mendapatkan data tersebut (Utomo et al., 2017).

1. *Pasive reconnaissance*

*Reconnaissance* yang dilakukan tanpa berhubungan secara langsung kepada korban, yang dimana orang yang melakukan *reconnaissance* tidak terdetaksi oleh korban(Utomo et al., 2017) .

**2.4.4 Spam Email Dan Spyware**

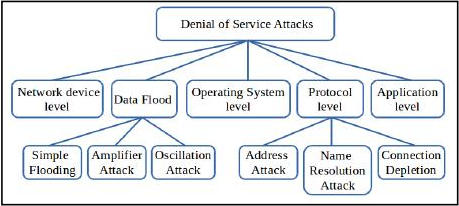
Dalam bentuk komunikasi yang biasa, berkirim email merupakan sebuah kebiasaan yang lebih umum digunakan di zaman sekarang. Terutama di semua jenis pekerjaan sering kali untuk berkirim email, email merupakan peran penting dalam kegiatan pekerjaan. Karena itu banyak *hacker* yang memanfaatkan kesempatan tersebut, dengan menggunakan email untuk mengambil data privasi pengguna atau tujuan lain. Mereka terutama memaksa pengguna lain untuk menerima pesan spam yang mereka kirim agar jika pengguna lain mengklik atau mengunduh perangkat lunak khusus yang mereka masukkan, maka pengguna lain akan kehilangan informasi yang dimiliki (Munawar, Zen and Putri, 2020).

**2.4.5 Implantasi Virus**

Dalam menggunakan komputer semua orang takut terhadap virus komputer, dikarenakan virus dapat disisipkan ke bermacam-macam jenis aplikasi program, pengguna dengan tidak sengaja akan menjalankan virus tersebut, kemudian virus tersebut dengan cepat akan menyebar ke seluruh bagian sistem komputer. Selanjutnya sistem pada bagian inti akan terinfeksi oleh virus, virus tersebut akan mempengaruhi kerja normal pengguna dalam waktu singkat, sehingga menyebabkan kerugian bagi pengguna (Munawar, Zen and Putri, 2020).

**2.5 *Denial of Service* (DoS)**

Serangan DoS merupakan sebuah ancaman keamanan yang dimana penyerang mengirimkan sejumlah permintaan palsu ke *host* atau *server*, akibatnya host terget menolak akses dari pengguna yang berhak sehingga layanan dari *host* menjadi tidak dapat diakes, oleh karna itu serangan tersebut dapat mengganggu ketersediaan sistem. Serangan *denial of service* (DoS) paling umum digunakan adalah serangan DDoS, serangan DDoS merupakan serangan yang terjadi ketika sejumlah host terinfeksi dengan *malware* yang memungkinkan *host* diambil alih oleh *hacker*, lalu program penyerang akan memerintahkan pengguna untuk mengakses situs *web hacker.* Umumnya, host yang menjadi target serangan DoS adalah sistem berbasis *web* atau *server web.* Biasanya program *server web,* seperti *Apache,* IIS memiliki keahlian untuk menangani atau menerima sejumlah koneksi dari pengguna. Penyerang meraih keuntungan dari kejadian tersebut (Arman, 2020).



**Gambar** **2.10 Klasifikasi DoS (Sumber : Arman, 2020).**

**2.6 *Slow HTTP DoS Attack***

*Slow HTTP Denial of Service* (DoS) meruapakan serangan lapisan aplikasi yang dimana sejumlah besar *request HTTP* tidak lengkap yang dikirim. Merupakan layer 7 DoS. Serangan aplikasi DoS merupakan kelas yang baru dalam serangan DoS untuk mencari kelemahan sistem dalam desain aplikasi atau implementasinya. Serangan ini sangat sulit untuk dilacak dibandingkan dengan serangan DoS biasanya dikarenakan, sebagai berikut:

1. Serangan ini tidak mengambil banyak *bandwidth.*
2. Target ini untuk membuat kemacetan dan sumber daya pembatasan dalam sistem dengan befokus pada tautan terlemah dalam aplikasi.
3. Serangan ini biasanya menggunakan https sebagai alat bantu mereka untuk menyembunyikan asal mereka yang sebenrnya (Arman, 2020).

**2.7 *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS)**

**2.7.1** ***Intrusion Detection System* (IDS)**

Intrusion Detection System (IDS) merupakan sebuah aplikasi software atau hardware yang berfungsi untuk mendeteksi aktivitas yang mencurigakan dan mengancam dalam sebuah sistem atau jaringan. IDS dapat melakukan pemantuan terhadap lalu lintas yang masuk dan lalu lintas yang keluar dalam sebuah sistem atau jaringan, melakukan analisis dan mencari bukti dari percobaan intrusi (penyusupan) (Fachri & Harahap, 2020). Jika terindikasi adanya aktifitas yang mencurigakan terhadap aliran (traffic) paket-paket yang keluar dan masuk pada sistem, maka IDS akan merekam aktifitas tersebut. IDS merupakan software atau hardware yang melakukan otomatisasi proses monitoring kejadian yang muncul di sistem komputer atau jaringan, menganalisanya untuk menemukan permasalahan keamanan (Wijaya & Pratama, 2020). Kelebihan yang akan di dapatkan dengan menggunakan IDS (*Intrusion Detection System*) sebagai metode Keamanan:

1. Memiliki ketepatan keamanan yang baik IDS (*Intrusion Detection System*) haruslah memiliki ketepatan atau ketelitian, jadi IDS (*Intrusion Detection System*) yang baik adalah IDS (Intrusion Detection System) yang mempunyai ketelitian yang baik untuk mengetahui ancaman dan serangan yang datang. Pada saat sekrarang ini IDS (*Intrusion Detection System*) mampu mendeteksi secara tepat waktu dan melakukan blocking terhadap tindakan yang mencurigakan. Selain itu IDS (*Intrusion Detection System*) juga mampu mendeteksi dan menganalisa trafik paket secara menyeluruh seperti paket – paket data baik Header Paket maupun Payload yang dipergunakan serta membedakan paket data yang keluar masuk dalam lalu lintas jaringan sehingga dapat mengenal benar karateristik trafic.

2. IDS memiliki kemampuan untuk Mengetahui ancaman yang ada dan Mencegah Serangan. IDS (*Intrusion Detection System*) yang mempunyai karateristik:

1. Dapat beroperasi secara in-line.

2. Memiliki kehandalan dan ketersediaan.

3. Deliver high performance.

4. Kebijakan policy pada IDS (*Intrusion Detection System*) yang dapat diatus sesuai dengan yang dibutuhkan.

3. IDS Memiliki skala yang luas dalam mengetahui proses ancaman IDS (*Intrusion Detection System*) haruslah memiliki kamampuan yang luas, dapat mengetahui serangan apa yang belum dikenalnya, seperti contoh IDS(*Intrusion Detection System*) dapat mengetahui serangan *DoS* dengan menggunakan metode analisis signature dan dapat mendeteksi semua tindakan yang mencurigakan. IDS (*Intrusion Detection System*) yang baik dalam mengetahui attacking adalah IDS (Intrusion Detection System) yang memiliki karateristik:

1. Memiliki AI () sehingga IDS (*Intrusion Detection System*) tersebut dapat memonitoring sendiri serangan – serangan yang datang.

2. Dapat melakukan proses deteksi trafic paket yang ada dan pembersihan terhadap host ( Layer-Layer 7 ).

3. Mampu melakukan deteksi terhadap TCP dan UDP.

4. Mampu memeriksa keberadaan backdoor.

4. Dapat menyimpulkan dan memberikan informasi dari ancaman-ancaman yang pernah terjadi dan menjadikan file logging untuk disimpan.

5. Memiliki kamampuan Forensik yang canggih dan mampu menghasilkan reporing yang baik. Memiliki sensor yang dapat dipercaya untuk memastikan pendeteksian dan pencegahan (Navirgo & Habibbullah, 2019).

**2.7.2 Signature Based IDS**

Cara kerja IDS signature yaitu akan melakukan pengamatan dan mendeteksi terhadap paket-paket di dalam lalu lintas jaringan dan melakukan analisa terhadap paket-paket tersebut dengan basis data signature yang dimiliki oleh sistem IDS ini atau bentuk serangan yang pernah diketahui kemudian data tersebut pernah disimpan oleh pemeriksaan (data ancaman yang sudah ada). Cara ini hampir sama dengan sistem kerja aplikasi antivirus dalam melakukan monitoring aktivitas terhadap malware. Saat mencoba mendeteksi sebuah ancaman terbaru di internet dengan menggunakan signature untuk melakukan deteksi yang diterapkan didalam basis data IDS yang digunakan. Dikarenakan sebuah pengujian serangan terhadap jaringan, sistem IDS ini tidak mampu untuk mendeteksi jenis serangan terbaru, karena informasi jenis serangan terbaru tidak dikenali di dalam basis data signature sistem IDS ini. Jenis serangan terbaru pada sistem IDS ini tidak mampu untuk mendeteksi serangan tersebut dikarenakan ketelmbatan waktu untuk mengetahui jenis serangan baru tersebut (Dar & Harahap, 2018).

**2.7.3 Anomaly-based IDS**

Anomaly-based techniques, dapat dikenal sebagai profile-based atau anomaly detection didasarkan pada pembuatan baseline profile yang mewakili aktivitas jaringan yang normal / diharapkan, dan bahwa setiap anomali yang diamati dari current activity dibandingkan dengan profil ini dianggap anomali. Profil ini sebagian besar dihasilkan melalui statistical dan historical network traffic data. Contoh klasik dari jenis deteksi ini adalah ketika pengguna tertentu selalu menggunakan Internet untuk jangka waktu tertentu, selama jam kerja. Bahwa user ini adalah seorang manajer di sebuah perusahaan yang dipantau oleh IDS berbasis anomali. IDS ini menghabiskan satu minggu penuh untuk membuat profil normal pengguna ini, dan sejak hari terakhir minggu itu, IDS menggunakan profil ini sebagai kewajiban untuk waktu yang diizinkan untuk menggunakan Internet. Sementara deteksi aktif, manajer ingin menggunakan Internet pada malam hari untuk mengirimkan laporan menit terakhir, yang merupakan sesuatu yang tidak biasa untuk penggunaan reguler. Respons IDS berbasis anomali terhadap perilaku tidak biasa ini adalah membatasi akses Internet ke pengguna tersebut, yang akan valid jika ini bukan pengecualian; Namun, ini sebenarnya akan dianggap sebagai false positive (Imam et al., 2019).

**2.7.4 *Intrusion Prevention System* (IPS)**

*Intrusion Prevention System* (IPS) merupakan sistem yang memiliki fungsi dalam mendeteksi dan memberikan pencegahan serangan. Dengan kata lain, IPS adalah peningkatan dari IDS dengan menambahkan beberapa komponen seperti firewall dan beberapa komponen lain untuk bekerja sama dalam mengamankan dan menghentikan terjadinya penyusupan dari client (Arman, 2020).

**2.8 Snort**

Snort adalah sebuah aplikasi monitoring dan pengamanan yang berfungsi untuk menemukan intrusi-intrusi jaringan (Scanning, penyusupan, penyerangan dan segala bentuk ancaman yang membahayakan). Snort sangat ahli dalam menciptakan sebuah paket *logging* paket-paket yang terdeteksi kedalam Snort yang menciptakan sebuah history, dan analisis trafik yang masuk akan terdeteksi secara *real-time* dalam jaringan-jaringan berbasis TCP/IP (Dar & Harahap, 2018). Secara prinsip dapat dibagi dalam tiga mode :

1. *Packet sniffer*: untuk memonitoring paket-paket yang masuk di jaringan.
2. *Packet logger*: untuk mencatat semua paket-paket yang masuk di jaringan dan untuk dipriksa di kemudian hari.
3. NIDS, deteksi penyusup network: pada mode ini snort akan berguna sebagai pendeteksi serangan yang dilakukan melalui jaringan komputer. Untuk menggunakan mode IDS dibutuhkan pengaturan yang akan membedakan sebuah paket biasa dengan paket yang membawa serangan (Dar & Harahap, 2018).

**2.9 Firewall dan IPTABLES**

**2.9.1 *Firewall***

Firewall adalah teknik pengamanan untuk melindungi keamanan komputer dan akan mencegah kegagalan komputer, juga terdapat jenis tindakan keamanan komputer yang paling umum digunakan. *Firewall* dapat berupa perangkat keras, perangkat lunak, atau antara dua komputer atau lebih. *Firewall* juga menjadikan peran yang lebih untuk melindungi komputer, karena semua aktivitas perlu disaring melalui firewall (Munawar, Zen and Putri, 2020). Secara umum *firewall* memiliki fungsi sebagai berikut :

1. *Firewall* depat mencegah orang lain yang tidak memiliki izin untuk memasuki komputer pengguna yang berhak.
2. *Firewall* jika seseorang dari luar ingin memasuki sistem, maka *firewall* dapat mencegahnya untuk mendekati sistem tersebut.
3. *firewall* dapat mencegah untuk mengunjungi situs khusus / tertentu karena kemampuannya untuk memfilter alamat yang tidak dikenal dan pada akhirnya, firewall dapat mencegah mengunjungi situs tertentu. Pada intinya komputer harus memiliki pemantauan keamanan (Munawar, Zen and Putri, 2020).

**2.9.2 IPTABLES**

Iptables adalah bagian dari proyek Netfilter. Netfilter merupakan gabungan kait kernel Linux yang berkomunikasi dengan jaringan. Iptables merupakan perintah dan struktur tabel yang berisi aturan-aturan yang mengontrol pemfilteran paket. Ada tiga table di iptables. Aturan atau rantai khusus yang akan dibuat lalu dimasukkan ke salah satu table tersebut. Filter table adalah default, dan salah satu yang sangat banyak digunakan. Tabel filter berisi rantai built-in: INPUT: Proses paket masuk MAJU: Proses paket yang dirutekan melalui host, OUTPUTP: Proses paket yang keluar (Amien, 2020).

**2.10 Port-Knocking**

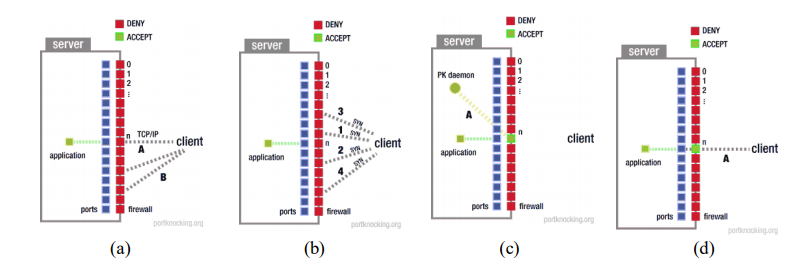
Port-Knocking merupakan sebuah metode untuk memblokir sementara layanan jarak jauh di dalam sebuah firewall yang memungkinkan untuk di akses ke port tersebut hanya untuk mengetahui service setelah klien berhasil diverifikasi ke firewall. Hal ini dapat berguna untuk menghindari pemindai yang bertujuan untuk mengetahui service apa saja yang saat ini dapat di akses pada host dan juga berfungsi sebagai pertahanan terhadap serangan zero-day (Amarudin, 2018).

Port knocking sebenarnya tidak terlalu banyak pengaruhnya dan tidak terlalu utama. bagi user jaringan local biasa. Dikarenakan fungsinya hanya melakukan buka tutup port komunikasi saja tentu tidaklah terlalu banyak gunanya, Namun bagi para pekerja telekomputer, para user komputer yang sering bekerja di luar kantor atau para administrator jaringan dan server yang harus memonitoring server-server mereka dari mana saja dan saat waktu penting. Port knocking memiliki metode yang yang dimana berfungsi sebagai penghubung sebuah koneksi ke perangkat-perangkat komputer tersebut (Riska et al., 2018).

Port Knocking merupakan metode sistem autentikasi yang secara khusus dibuat untuk jaringan. Ide dasar dari sistem autentikasi ini telah lama digunakan namun baru pada tahun 2003. Pada dasarnya port knocking dapat diartikan sebagai suatu metode komunikasi antara dua komputer atau lebih, yang dimana informasi yang dikirimkan di-encode dalam bentuk usaha koneksi ke port–port dalam urutan tertentu. Usaha membangun koneksi ini bisa disebut juga ketukan. Mekanisme port knocking akan menggunakan file log yang dibuat oleh firewall untuk mengetahui apakah suatu usaha koneksi telah dibuat oleh suatu host atau tidak (Mulyanto et al., 2021).

**2.10.1 Metode Port Knocking**

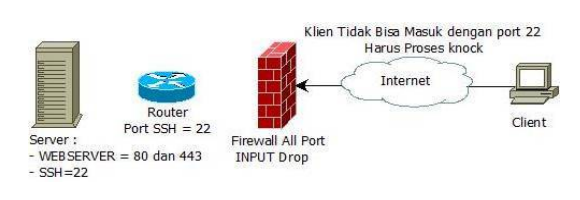
Metode port knocking memiliki sistem authentication yang dapat dirancang untuk sebuah koneksi client dan server. Pada metode port knocking ini dapat digunakan untuk autenifikasi pengiriman informasi atau data, yang dimana sebuah informasi dan data tersebut akan dikirimkan atau dikodekan (mungkin juga dienkripsi) ke dalam urutan nomor-nomor port. Urutan ini disebut dengan knock (ketukan). Cara kerja metode dari port knocking yang dapat diuraikan sesuai dari urutan-urutan pada gambar 3. Secara biasanya komputer server tidak pernah mengizinkan port untuk terbuka kepada public network dan server juga memonitoring semua upaya koneksi yang masuk ke dalamnya (gambar 3.a). Untuk mengawali koneksi client, akan dimulai dengan cara mengkoneksi ke sebuah server dengan serangkaian urutan ke well-defined set of ports, yang juga memberikan paket SYN atau synchronus ke port yang dipilih sebelumnya dalam ketetapan atau disebut dengan knock. Proses sebuah knock inilah yang memicu port untuk mengetuk nomornya (gambar 3.b). Selama tahapan knock yang terjadi pada server, server tidak memberikan respons atau izin terlebih dahulu kepada client, namun dari sisi server menafsirkan yaitu decodes dan decryptes pada urutan port-port untuk diperiksa otentifikasinya. Sehingga server akan menerima dan mengartikan sebuah ketukan well-defined set of ports yang valid, kemudian server tersebut akan memicu untuk membuat koneksi antara client dan server melalui proses transfer data (gambar 3.d) (Khadafi et al., 2019).



**Gambar** **2.11 Metode Port Knocking (Sumber : Khadafi et al., 2019).**

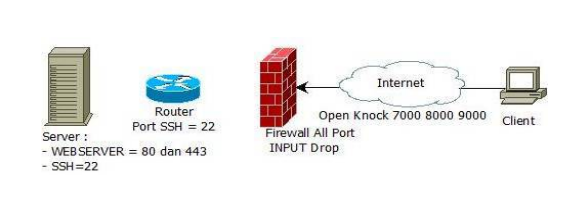
**2.10.2 Cara Kerja Port Knocking**

1. Pada gambar 2.12 menjelaskan tentang user tidak dapat masuk atau mengakses aplikasi SSH karena port ssh(22) sudah di block dari firewall input.



**Gambar** **2.12 *Block* dari *firewall* *input* (Sumber : Amien, 2020).**

2. Pada gambar 2.13 menejlaskan dalam proses ini user akan mengetuk terlebih dahulu dengan tahapan yaitu 7000, 8000, dan 9000 dalam waktu bersamaan, pengetukan ini sudah di atur dan dikonfigurasi di dalam firewall agar bisa membuka port 22.



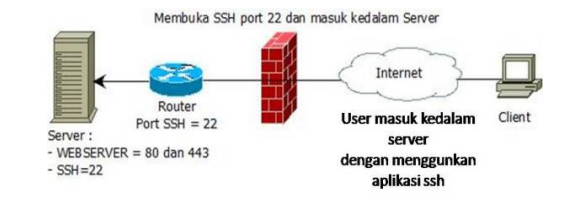
**Gambar** **2.13 Ketukan *open knock* 7000 8000 dan 9000 (Sumber : Amien, 2020).**

3. Proses oupot di firewall (port Knocking daemon) mencegah upaya koneksi dan meinterpretasikan (akan meuraikan sandi dan membaca sandi) terdiri dari otentik Port Knocking Firewall melakukan tugas tertentu berdasarkan isi dari port knocking, firewall sudah mengizinkan user untuk mengakses dan melakukan monitoring berdasarkan IP User dan melakukan pencatatan berupa log di dalam firewall, Langkah disni user dapat menggunakan aplikasi SSH untuk melakukan remot terhadap server.



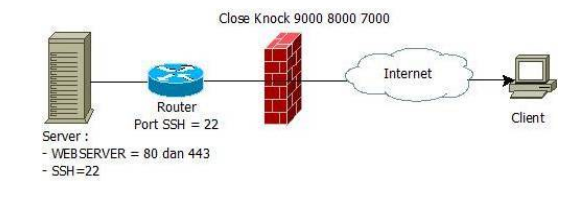
**Gambar** **2.14 Membuka port ssh (Sumber : Amien, 2020).**

4. Proses user membuka aplikasi SSH dengan meremot port 22 kedalam server user bebas mengakses di dalam server.



**Gambar** **2.15 Membuka ssh port 22 agar masuk ke server (Sumber : Amien, 2020).**

5. Closing, sedangkan jika user/admin ingin menutup port 22, exit terlebih dahulu dari Aplikasi SSH maka ketukan yang akan digunakan adalah 9000 8000 7000, seluruh aktifitas user akan di tutup kembali, dan Firewall melakukan proses dimana seluruh port akan tertutup kembali (Amien, 2020).



**Gambar** **2.16 Close Knock (Sumber : Amien, 2020).**

**BAB III**

**METODOLOGI PENELITIAN**

**3.1 Kerangka Penelitian**

Kerangka penelitian adalah konsep atau tahap-tahap yang akan dilakukan dalam penelitian yang akan diuraikan pada Gambar 3.1 di bawah ini.

**Penelitian Pendahuluan**

**Pengumpulan Data**

**Analisa**

**Analisa Sistem**

**Analisa Data**

**Analisa Proses**

**Instalasi dan Konfigurasi**

**Implementasi**

**Port Knocking**

**IPTABLES**

**Snort**

**Hasil Pengujian**

**Gambar** **3.1 Kerangka Penelitian**

**3.2 Tahapan Penelitian**

Pada tahapan penelitian ini, terdapat beberapa tahapan yang akan dijelaskan dengan melakukan pengumpulan beberapa laporan yang diperlukan dan akan rangkum seperti dibawah ini.

**3.2.1 Penelitian Pendahuluan**

Penelitian Pendahuluan dilakukan dengan melakukan pendekatan terhadap objek penelitian. Tujuan dari tahap ini adalah untuk mengetahui permasalahan yang terjadi secara tepat, sehingga diharapkan penelitian dapat memberikan solusi yang paling optimal terhadap pemecahan permasalahan tersebut.

Permasalahan yang telah berhasil di identifikasi pada PAK online LLDIKTI X adalah bagaimana cara mengamankan keamanan jaringan pada server PAK online LLDIKTI X dan juga untuk mengetahui bagaimana cara mengkonfigurasi sistem keamanan pada jaringan server tersebut agar nantinya dapat menangkal serangan yang masuk.

**3.2.2 Pengumpulan Data**

Pada tahap ini membahas tentang pengumpulan data dan informasi. Dalam melakukan penelitian untuk mendapatkan data dan informasi maka metode yang dilakukan dalam proses pengumpulan data dilakukan dengan tahapan, yaitu :

1. **Waktu Penelitian**

Pengumpulan data serta informasi pada tahap ini dilakukan untuk mengetahui mengenai objek yang diteliti. Adapun waktu penelitian yang dilakukan pada bulan April 2021 sampai selesesai.

**Tabel 3.1 Jadwal Penelitian**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Kegiatan | Bulan Ke 1 | | | | Bulan Ke 2 | | | | Bulan Ke 3 | | | | Bulan Ke 4 | | | |
| 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| Pendahuluan |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Pengumpulan Data |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Analisa |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Perancangan |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Implementasi |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Pengujian |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

1. **Tempat Penelitian**

Dalam malakukan penelitian ini penulis langsung mengamati dan melakukan tanya jawab secara langsung kepada Kepala Administrator PAK Online LLDIKTI X. Adapun objek dan tempat penelitian ini yaitu di Kantor LLDIKTI X bagian PAK Online yang beralamat di Jl. Khatib Sulaiman Gunung Pangilun, Alai Parak Kopi, Kec. Padang Utara, Kota Padang, Sumatera Barat 25173.

1. **Metode Penelitian**

Adapun metode penelitian yang dilakukan oleh penulis dalam menyelesaikan penelitian adalah sebagai berikut:

1. Penelitian Lapangan

Pada penelitian lapangan ini dilakukan wawancara Kepala Administrator PAK Online LLDIKTI X, untuk menganalisis masalah, serta memperoleh informasi yang dibutuhkan. Serta mengetahui bagaimana cara kerja sistem yang ada di PAK Online LLDIKTI X.

1. Penelitian Kepustakaan

Penelitian kepustakaan ini dilakukan dengan cara membaca, membahas, meringkas dan membuat kesimpulan dari buku,jurnal dan internet yang berkaitan dengan Snort,Iptables dan Port Knocking untuk mendapatkan bahan-bahan yang secara ilmiah dapat dijadikan landasan dalam menyusun laporan penelitian ini.

1. Penelitian Laboratorium

Penelitian Laboratorium merupakan suatu metode penelitian yang dilakukan dengan menggunakan alat bantu personal komputer (PC). Dalam hal ini penelitian dilakukan dengan merancang sistem yang sesuai dengan topik permasalah yang dihadapi dan juga dalam hal penyususnan laporan secara keseluruhan. Gunanya adalah memenuhi kreteria sebuah penelitian dan menguji keakuran sistem yang akan dirancang.

**3.2.3 Analisa**

Dalam tahap ini dapat dilakukan dengan tiga tahap analisa sebagai berikut:

1. Analisa Data

Data-data yang diperoleh dari berbagai sumber seperti hasil wawancara dan website resmi LLDIKTI X. Data tersebut berupa penjelasan skema jaringan atau Topologi jaringan yang ada pada PAK Online LLDIKTI X dan sistem keamanan yang berada pada PAK Online LLDIKTI.

1. Analisa Proses

Pada tahap Analisa proses ini, penulis menggunakan Analisa terhadap sistem jaringan dan keamanan yang berada pada PAK Online LLDIKTI X.

1. Analisa Sistem

Analisa sistem merupakan suatau cara menganalisis permasalahan yang sedang berjalan saat ini. Bagaimana sistem yang berada pada PAK Online LLDIKTI X dapat mengamankan data pada komputer server tersebut.

Analisa sistem dilakukan agar penulis dapat mendeskripsikan dan mengimplementasikan sistem yang akan dirancang. Dengan adanya Analisa sistem diharapkan dapat mempermudah dalam mengisi kekurangan sistem dan tidak merusak sistem yang ada.

Berdasarkan identifikasi masalah di atas, maka dibutuhkan analisa sistem keamanan pada LLDIKTI X PAK Online terlebih dahulu. Hal ini bertujuan agar sistem yang di rancang menjadi sebuah metode baru untuk membangun sebuah sistem keamanan.

**3.2.4 Instalasi dan Konfigurasi**

Pada tahap Instalasi dan Konfigurasi penulis akan membuat sebuah perancangan sistem yang akan dijalankan, mulai dari menganalisa program yang berjalan, dan mengkonfigurasi program yang akan dijalankan tersebut. Pada tahap ini peneliti menggunakan beberapa *software* dan *hardware* diantaranya:

1. *Software*
   1. Sistem Operasi Linux Ubuntu 20.04.1 Desktop.
   2. Snort 2.9.7.0-5build1.
   3. IPTABLES 1.8.4-3ubuntu2.
   4. PORT KNOCKING/Knockd 0.7.
   5. Apache.
   6. PHP.
2. *Hardware*
   1. Komputer Server.
   2. Leptop sebagai client dan penyerang.
   3. Mouse.
   4. Keyboard.

**3.2.5 Implementasi**

Tahapan ini dilakukan Instalasi dan Konfigurasi pada sistem PAK Online LLDIKTI X. dan selanjutnya akan diimplementasikan pada komputer server untuk merancang sebuah Sistem keamanan tersebut dan Laptop sebagai user untuk mengakses serta sebagai penyerangan sistem tersebut. Implementasi yang dilakukan dengan pada penelitian ini yaitu :

1. Snort

Pada implementasi ini Snort adalah hal yang utama yaitu mendeteksi sistem jaringan pada PAK Online LLDIKTI X.

1. Port Knocking

Pada implementasi ini Port Knocking akan di ujicobakan dengan membuka tutup port yang akan digunakan seperti penggunaan FTP port 21 dan SSH port 22.

1. Iptables

Pada implementasi ini Iptables akan di ujicobakan dengan memblock ancaman-ancaman yang ada seperti uji coba iptables untuk memblokir IP Scaning dan DDOS webserver.

Apabila sistem yang dibangun telah seperti yang diharapkan. Maka penulis dapat menarik kesimpulan dalam pengujian ini.

**3.2.6 Hasil Pengujian**

Hasil dan pengujian sistem ini merupakan proses selanjutnya setelah implementasi perangkat lunak selesai dilakukan. Pengujian ini dilakukan untuk menguji sistem yang telah dirancang pada PAK Online LLDIKTI X, sistem yang telah dirancang apakah sudah berjalan dengan benar dan sesuai dengan percancangan yang dinginkan. Pengujian yang dilakukan dengan melakukan:

1. Pengujian Mendeteksi pada aplikasi Snort.
2. Pengujian PORTKNOCKING untuk pengamanan port.
3. Pengujian IPTABLES dalam mencegah serangan.

**BAB IV**

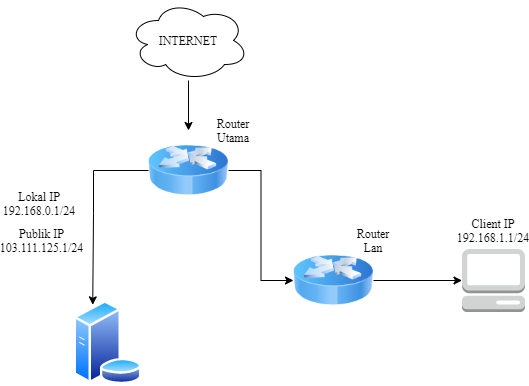
**ANALISA DAN PERANCANGAN**

**4.1 Analisa Network**

Keamanan jaringan saat ini merupakan kewajiban dari suatu mekanisme yang harus dimiliki dan sangat penting untuk menjaga validitas dan integritas data bagi setiap penggunanya. Sistem harus dilindungi dari segala macam serangan dan usaha- usaha peyusupan oleh pihak – pihak yang tidak berhak atau tidak memiliki otoritas.

Proses Analisa Network pada jaringan sangat diperlukan untuk mensimulasikan tingkat keamanan pada suatu jaringan. Karena dengan analisa yang baik , diharapkan mampu mengidentifkasi celah keamanan sebaik mungkin. Hal ini yang mendasari Snort sebagai sebuah *software* untuk mendeteksi sebuah serangan.

Suatu perangkat **Intrusion Detection Sistem** (IDS) digunakan sebagai pendeteksian dari sebuah ancaman, Portknocking disini berfungsi untuk menjaga port-port yang dalam keadaan terbuka dengan begitu *port* tersebut juga menjadi salah satu ancaman dan Iptables meruapakan mekanisme yang berfungsi untuk menjaga sistem keamanan seperti *firewall*. IDS akan bertindak sebagai alarm dengan memberikan suatu respon (pasif maupun aktif) yang dapat dijadikan acuan oleh seorang pengelola jaringan untuk memperbaiki konfigurasi dari sistem keamanan tersebut. Penelitian ini dilakukan dengan menggunakan sistem operasi Linux Ubuntu, Snort yang memiliki kemampuan untuk mendeteksi adanya penyusupan terhadap jaringan dan memberikan *alert* serta sebagai *monitoring* jaringan, Portknocking memiliki kemanan untuk menjaga keamanan port dan Iptables sebagai keamanan *firewall*.

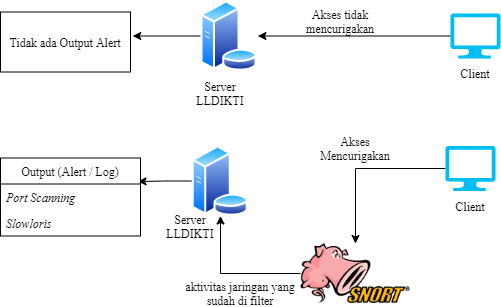


**Gambar** **4.1 Topologi Jaringan LLDIKTI**

**4.2 Perancangan Mekanisme**

**4.2.1 Perancangan Mekanisme Snort**

Perancangan mekanisme snort pada penelitian berguna sebagai sistem pengumplan dari setiap data serangan. Agar mekanisme dapat sesuai yang diharapkan dan berjalan sesuai dengan yang dirancang maka diperlukan alur mekanisme seperti pada Gambar 4.2

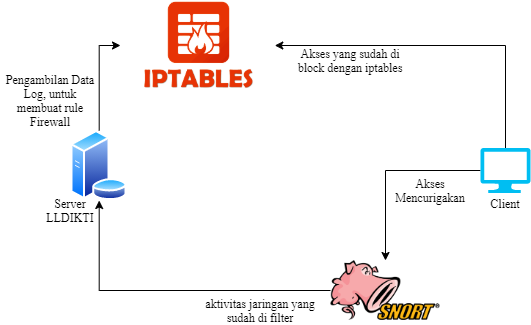


**Gambar** **4.2 Gambaran Mekanisme snort**

Pada Gambar diatas merupakan mekanisme snort yang akan dirancang, pada saat sistem snort dinyalakan maka paket yang masuk akan di filter kedalam kemudian snort akan mendeteksi paket tersebut apakah ada ancaman, jika ancaman tersebut ada maka ancaman tesebut akan masuk kedalam *alert console* dan memberikan informasi jenis ancaman dan dari mana asal ancaman tersebut berasal kemudian sistem akan menghasilkan *monitoring* dalam bentuk hasil Log.

**4.2.2 Perancangan Mekanisme IPTABLES**

Pada gambar 4.3 perancangan pada mekanisme IPTABLES. Sistem dimulai ketika mendapatkan data terbaru, jika rule IPTABLES tersebut dapat diketahui untuk menahan serangan, maka IPTABLES akan mengambil tindakan untuk menahan dan memblock ancaman tersebut dan jika tidak maka akan dirancang rule yang baru untuk menahan serangan yang baru.



**Gambar** **4.3 Gambaran Mekanisme IPTABLES**

Pada gambar diatas merupakan rancangan mekanisme IPTABLES yang mana pada saat pengambilan data dari log maka akan diberikan keamanan rule untuk sistem pertahanan jika rule bekerja maka ancaman tersebut tidak akan bahaya dan jika rule tidak bekerja maka akan dibuatkan sebuah rule terbaru agar nantinya akan melakukan aksi pada serangan.

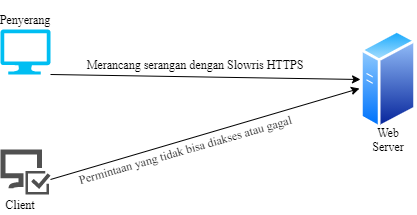
**4.3 Rancangan Pengujian Serangan**

Pengujian dilakukan bertujuan untuk mengetahui seberapa suskes sitem dapat membuat rules IDS dan mendeteksi beberapa serangan yang dilakukan. Untuk memudahkan penjelasan dibagi dengan beberapa bagian diantaranya.

terbagi menjadi dua *Slow HTTP DoS Attack* dan Serangan port scanning.

**4.3.1 *Slow Headers* (Slowloris)**

Dalam serangan *Slow Header*, seorang penyerang meluncurkan aksinya dengan bantuan alat yang disebut Slowloris atau sejenisnya. Alat ini membuka koneksi, kemudian mengirim *header HTTP*, menambah tetapi tidak pernah menyelesaikan permintaan. Ribuan koneksi *HTTP POST* dibuat dan mengirimkan *HTTP Header* dengan sangat lambat untuk memaksa serverweb target untuk menjaga koneksi tetap terbuka. Koneksi ini akan tetap hidup, tidak terputus dari server target. Slowloris akan mengambil semua sumber daya dari *server web* target, sehingga memblokir permintaan dari klien yang sah atau klien yang ingin mengakses *server web* tersebut.



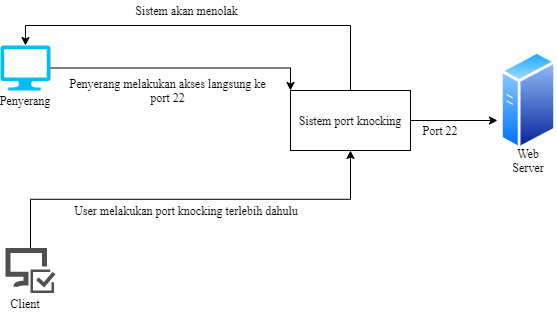
**Gambar** **4.4 Ilustrasi gambaran serangan**

**4.3.2 Serangan *port scanning***

*port scanning* adalah serangan untuk memperoleh informasi target. Tujuan serangan adalah membanjiri *request* ke port icmp, tcp dan udp, hingga mendapat informasi melalui port tersebut.

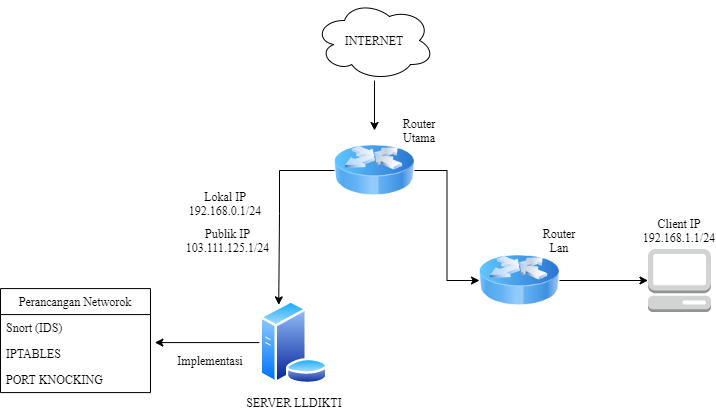
**4.3.3 Akses Port secara langsung**

Pada pengujian ini akan digunakan akses port 22 untuk pengujian ini yang dimana nantinya seorang user yang sudah mengetahui akan adanya ip dan port yang harus di masukkan sebelum mengakses port 22 dan juga pengujian pada penyerang yang dimana akan langsung mengakses port 22 tanpa adanya akses port knocking terlebih dahulu hasilnya penyerang tidak dapat mengakses port 22 tersebut dikarnakan adanya port knocking yang sudah dirancang.



**Gambar** **4.5 Ilustrasi gambaran port knocking**

**4.4 Perancangan Network Topologi**



**Gambar** **4.6 Gambaran Perancangan Network**

Pada Gambaran 4.6 dijelaskan bahwa penambahan network pada LLDIKTI, dijelaskan bahwa Network yang akan di rancang pada implementasi ini berupa Snort, IPTABLES, dan Portknocking. Gambaran perancangan ini memiliki satu client yang saling terhubung melalui router Router Lan, kemudian di sambungkan ke Router utama, lalu terhubung ke server LLDIKTI.Perancangan ini di implementasikan secara langsung pada network server LLDIKTI dan di harapkan agar dapat menjalankan fungsi dengan baik.

**BAB V**

**IMPLEMENTASI DAN PENGUJIAN**

**5.1 Implementasi Sistem**

Implementasi sistem merupakan bagian dari pengembangan sistem, untuk melakukan sebuah implementasi maka diperlukan program komputer dengan perancangan *installasi program* dan penulisan kode program untuk konfigurasi sesuai dengan sistem yang dirancang.

**5.1.1 Lingkungan Implementasi**

Sebelum melakukan implementasi, maka dibutuhkan spesifikasi perangkat keras (*hardware*) dan perangkat lunak (*software*) serta langkah-langkah yang dilakukan untuk menjalankan sistem agar dapat berjalan sebagaimana mestinya.

**5.1.2 Perangkat Keras**

Perangkat keras yang dibutuhkan dalam perancangan ini adalah sebagai berikut:

1. Komputer Server (LLDIKTI)
2. Laptop ASUS Notebook X453m (Client dan penyerangan)

**5.1.3 Perangkat Lunak**

Perangkat lunak yang dibutuhkan dalam percangan system ini adalah sebagai berikut:

1. Sistem Operasi Ubuntu (Server)
2. Sistem Operasi Windows 7/8/10 dan Kali Linux (Client)
3. Snort IDS (**Intrusion Detection System**)
4. IPTABLES
5. PORTKNOCKING
6. Apache
7. SSH
8. Slowloris

**5.2 Pengujian**

Pengujian adalah proses menjalankan sistem yang telah di konfigurasi dan dirancang untuk melihat proses ketika sistem yang sudah di implementasikan berjalan.

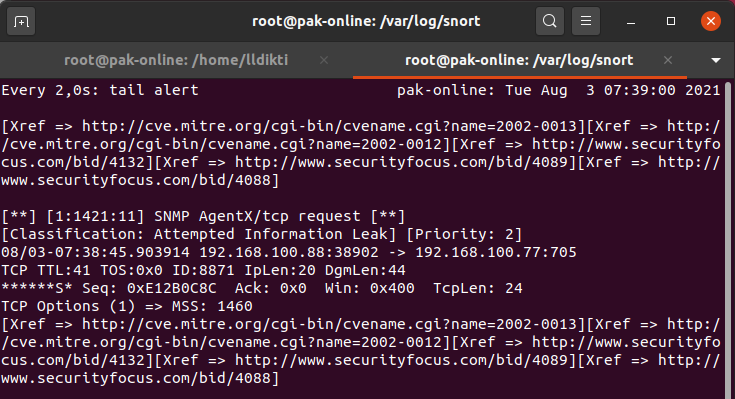
**5.2.1 Pengujian mendeteksi aplikasi snort.**

Pada pengujian yang menggunakan snort, yang berfungsi untuk mendeteksi aktifitas jaringan serta paket yang mengarah langsung ke arah komputer server dengan rules yang sudah di rancang. Proses penangkapan tersebut dapat dilakukan dengan perintah berikut :

$ sudo su

$ snort -c /etc/snort/snort.conf -l /var/log/snort/ -K ascii -D

$ watch -n 2 tail alert



**Gambar** **5.1 Tampilan Proses mendeteksi snort**

Tampilan pada Gambar 5.1 merupakan proses mendeteksi snort yang telah di jalankan pada komputer server LLDIKTI, yang dimana proses ini dapat menampilkan proses aktivitas yang berlangsung mengarah IP komputer server dan mengetahui IP yang sedang mengakses server pada LLDIKTI.

Untuk melihat log pada proses snort dapat dilihat pada folder dengan mengetikan perintah berikut :

$ cd /var/log/snort

$ more alert



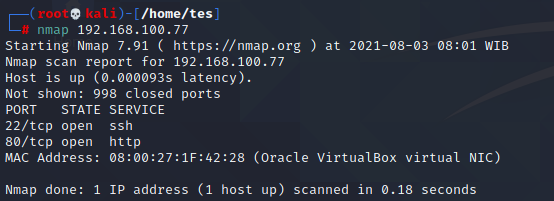
**Gambar** **5.2 Tampilan Log pada more alert**

Tampilan pada Gambar 5.2 merupakan sebuah file log pada snort yang mampu melihat aktifitas yang masuk ke dalam server dan snort juga mengetahui dari mana aktifitas tersebut berasal seperti IP dan bentuk ancaman yang dilakukan.

**5.2.2 Pengujian Port Scanning**

Pada pengujian serangan port scanning dengan menggunakan software NMAP. Pengujian ini dilakukan dengan 2 metode :

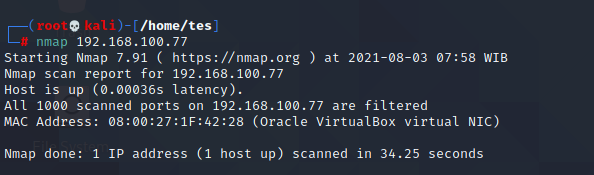
1.Pengujian port scanning tanpa iptables



Gambar 5.3 Hasil ip scanning tanpa iptables

Tampilan pada gambar 5.3 merupakan hasil IP scanning tanpa iptables. Pada saat iptables belum dijalankan makai ip scanning dapat melihat port yang terbuka pada sebuah komputer tersebut. Kemudian di pengujian selanjutnya akan dilakukan pengujian port scanning dengan iptables.

2.Pengujian port scanning dengan iptables



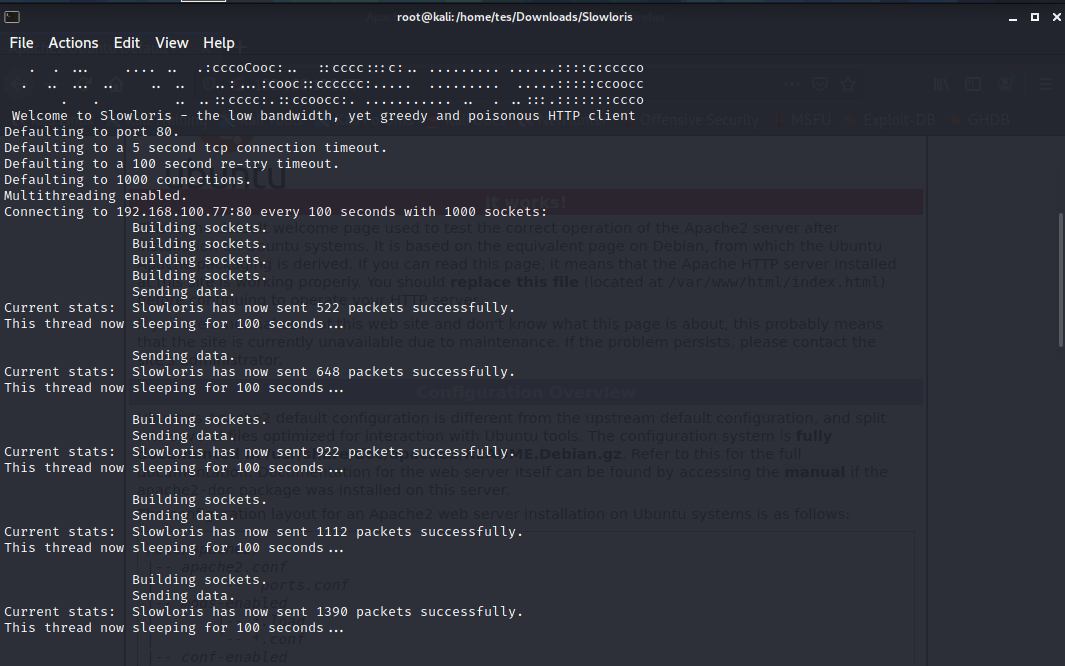
**Gambar 5.4 Hasil ip scanning dengan iptables**

Tampilan pada gambar 5.4 merupakan hasil dari IP scanning yang dilakukan, dikarenakan iptables yang sudah di jalankan dan yang sudah di setting mampu menahan serangan ip scanning yang berfungsi menyembunyikan port pada komputer.

**5.2.3 *Slow HTTP DDOS Attack***

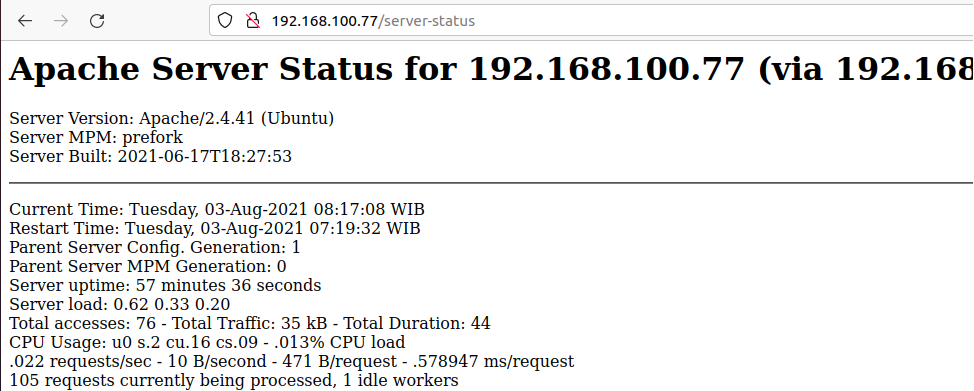
Pada pengujian serangan *Slow HTTP DDOS* dengan menggunakan *Slowloris*. Pengujian ini dilakukan dengan 2 metode :

1.Pengujian *Slow HTTP DDOS Attack* tanpa iptables



**Gambar 5.5 Tampilan serangan Slowloris tanpa iptables**

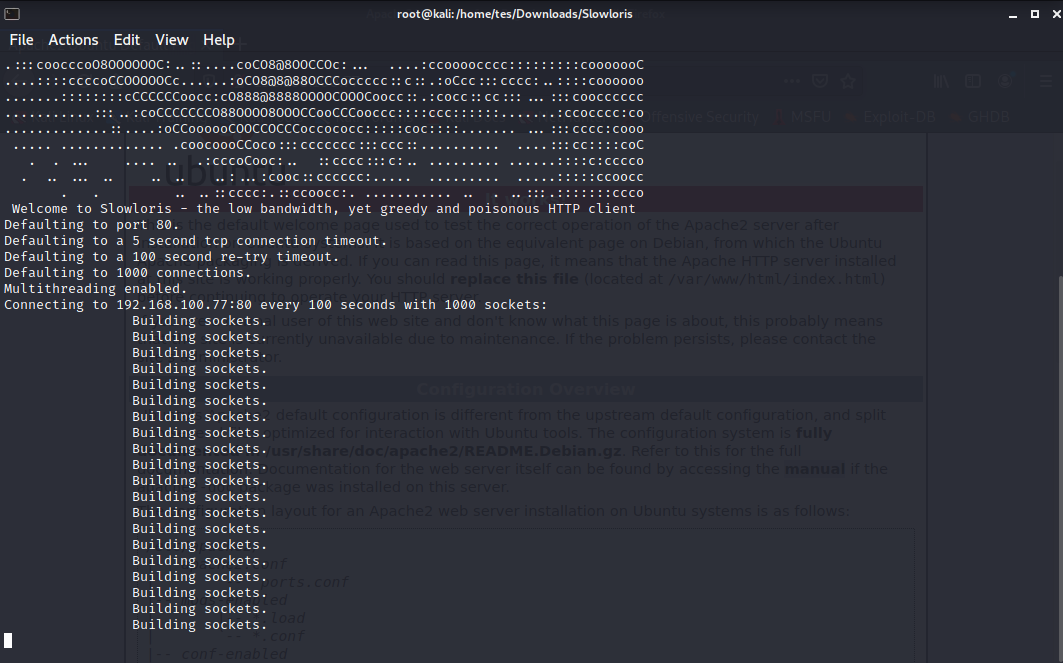
Tampilan Pada gambar 5.5 menjelaskan bahwa serangan slowloris dapat di lancarkan ke web server dikarenakan belum dijalankannya iptables, slowloris dapat menimbulkan kelambatan pada web server dikarnakan paket request yang banyak.



**Gambar 5.6 Tampilan web server yang terkna slowloris**

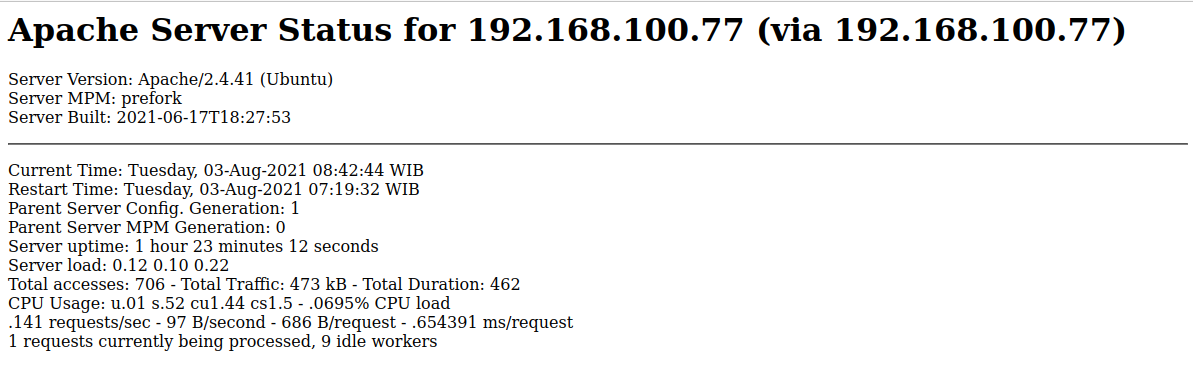
Tampilan pada gambar 5.6 menjelaskan bahwa terdapat 105 reqest pada web server. Hal ini disebabkan oleh serangan *Slow HTTP DDOS Attack* yang menimbulkan kelambatan dalam mengakses server. Kemudian pada pengujian selanjutnya akan dilakukan pengujian *Slow HTTP DDOS Attack* dengan iptables.

2.Pengujian *Slow HTTP DDOS Attack* dengan iptables



**Gambar 5.7 Tampilan Slowloris dengan iptables**

Tampilan pada gambar 5.7 menjelaskan bahwa Slowris tidak berhasil dilakukan, dikarnakan adanya iptables yang sudah di jalankan sehingga mampu menahan serangan *Slow HTTP DDOS Attack* pada komputer.



**Gambar 5.8 Tampilan webserver tidak terkena slowloris**

Tampilan pada gambar 5.8 menjelaskan bahwa web server yang tidak terkena serangan *Slow HTTP DDOS Attack* dikarenakan sudah dijalankannya iptables untuk menahan *Slow HTTP DDOS Attack* tersebut.

+

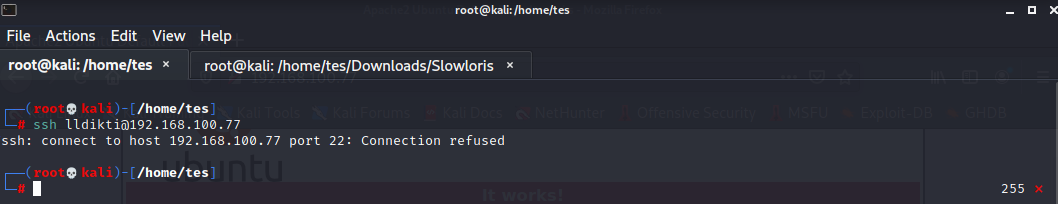
**5.2.4 Port knocking**



**Gambar 5.9 Tampilan PortKnocking di aktifkan**

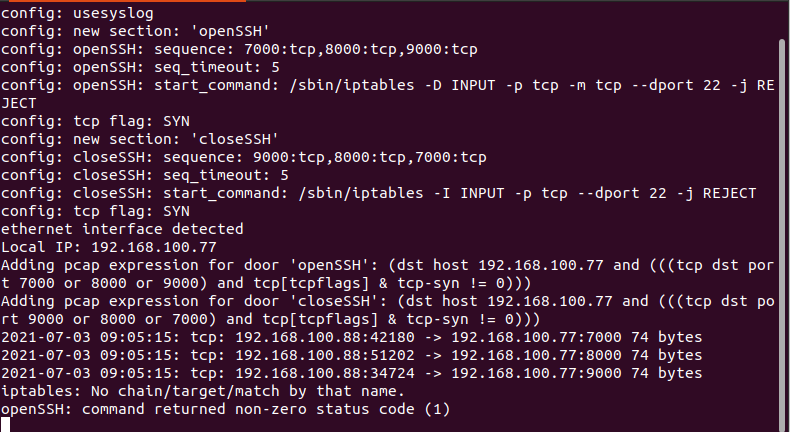
Tampilan pada gambar 5.9 menjelaskan bahawa mengaktifkan dan memonitoring portknocking, tampilan ini dapat dijalankan dengan mengetikkan perintah berikut :

$ sudo knockd -D -i nama\_ethernet



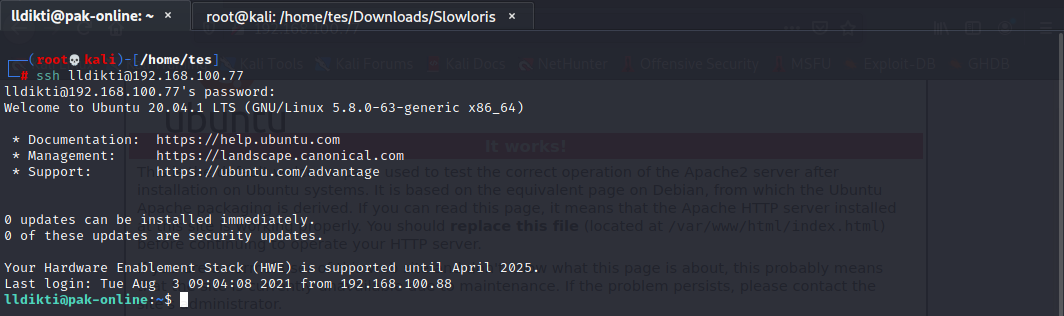
**Gambar 5.10 Tampilan tidak terhubung SSH**

Tampilan pada gambar 5.10 menjelaskan bahwa penolakan untuk mengakses SSH, hal ini dikarenakan belum mengakses portknocking terlebih dahulu sehingga sistem menolak untuk mengakses SSH.



**Gambar 5.11 Tampilan knocking**

Tampilan pada gambar 5.11 mejelaskan bahawa proses portknocking baru saja dilakukan dengan mengakses port 7000 8000 9000 maka port 22 akan terbuka dan dapat di akses.



**Gambar 5.12 Tampilan SSH yang dapat di akses**

Tampilan pada Gambar 5.12 menjelaskan bahwa kita dapat mengakses SSH dikarenakan sudah melakukan portknocking terlebih dahulu, proses akses dengan menggunakan aplikasi SSH untuk meremot server LLDIKTI yang akan di akses.

**5.3 Tabel Hasil Pengujian**

Tabel 5.1 Tabel Black Box Hasil Pengujian

|  |  |  |  |
| --- | --- | --- | --- |
| NO | Aktivitas Pengujian | Hasil yang diharapkan | Hasil pengujian |
| 1 | Pengujian Snort | Mampu mendeteksi atau memantau aktvitas jaringan yang menuju pada komputer server | Sesuai harapan |
| 2 | Pengujian serangan ip scanning tanpa iptables | Memmpu memberikan serangan pada komputer server yang menimbulkan terbukanya port pada komputer server | Sesuai harapan |
| 3 | Pengujian serangan ip scanning dengan iptables | Mampu menahan ip scanning dan menyembunyikan port pada komputer server | Sesuai harapan |
| 4 | Pengujian serangan *Slow HTTP DDOS Attack* tanpa iptables | Memmpu memberikan serangan pada komputer server yang menimbulkan kelambatan dalam mengakses webserver | Sesuai harapan |
| 5 | Pengujian serangan *Slow HTTP DDOS Attack* dengan iptables | Mampu menahan serangan *Slow HTTP DDOS Attack* pada komputer server | Sesuai harapan |
| 6 | Pengujian Portknokcing | Mampu menerapkan sistem kemanan akses port pada komputer server | Sesuai harapan |

**BAB VI**

**PENUTUP**

**6.1 Kesimpulan**

Dari hasil penelitian yang telah di implementasikan, maka dapat disimpulkan beberapa hal sebagai berikut:

1. Konfigurasi dan Installasi Snort pada PAK Online LLDIKTI X dapat dijalankan dengan baik dan dapat memonitoring ancaman dan memfilter paket yang masuk langsung ke dalam server.
2. Konfigurasi pada IPTABLES pada PAK Online LLDIKTI X dapat menangkal serangan *IP Scanning* dan *Slow HTTP DDOS Attack* (**Slowloris)**
3. Konfigurasi pada Portknocking pada PAK Online LLDIKTI X dapat menangkal terjadinya penyalahgunaan sistem pada SSH, maka dari itu pengamanan port 22 dapat berjalan dengan baik.

**6.2 Keterbatasan Sistem**

Dalam penelitian ini, ada beberapa keterbatasan dari sistem yang dibuat, yaitu:

1. Sistem yang dirancang merupakan penyerangan pada saat ini, kita tidak tau virus atau serangan baru akan update dan muncul sehingga snort tidak dapat menangkal dengan baik karna virus atau ancaman baru tersebut.
2. Sistem Portknocking wajib ditutup dikarnakan port knocking memiliki akses buka dengan cara manual maka untuk menutup kembali port 22 tersebut harus di tutup dengan manual dengan mengetuk port yang sudah di setting 9000 8000 dan 7000 maka port 22 akan tertutup kembali

**6.3 Saran**

Mengigat berbagai keterbatasan yang dialami penulis terutama masalah pemikiran dan waktu, maka dari itu penyusun memberikan saran yang dapat dipertimbangkan, sebagai berikut:

1. Untuk selalu mengupdate snort versi terbaru, dikarnakan jika Snort mendapatkan update terbaru maka rules tersebut juga ikut terupdate maka tidak perlu khawatir akan adanya ancaman yang baru.
2. Pada aplikasi iptables agar selalu melakukan update rules iptables yang terbaru dalam mengupayakan menangkal serangan yang terbaru.
3. Perlu dibangunnya sebuah sistem khusus untuk pengujian serangan terbaru didalam server, dalam melakukan pengamaman server dengan menggunakan metode snort dan iptables tersebut.

**DAFTAR PUSTAKA**

Aini, N. (2019). *Analisis Jaringan Local Area Network*. *5*(1). https://doi.org/10.31219/osf.io/htxwe

Amarudin, A. (2018). Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking. *Jurnal Teknoinfo*, *12*(2), 72. https://doi.org/10.33365/jti.v12i2.121

Amien, J. Al. (2020). Implementasi Keamanan Jaringan Dengan Iptables Sebagai Firewall Menggunakan Metode Port Knocking. *Jurnal Fasilkom*, *10*(2), 159–165.

Arman, M. (2020). Metode Pertahanan Web Server Terhadap Distributed Slow HTTP DoS Attack. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, *7*(1), 56–70. https://doi.org/10.35957/jatisi.v7i1.284

Dar, M. H., & Harahap, S. Z. (2018). Implementasi Snort Intrusion Detection System (Ids) Pada Sistem Jaringan Komputer. *Jurnal Informatika*, *6*(3), 14–23. https://doi.org/10.36987/informatika.v6i3.1619

Fachri, B., & Harahap, F. H. (2020). Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan dan Komputer. *Jurnal Media Informatika Budidarma*, *4*(2), 413. https://doi.org/10.30865/mib.v4i2.2037

Imam, R. M., Sukarno, P., & Nugroho, M. A. (2019). Deteksi Anomali Jaringan Menggunakan Hybrid Algorithm. *E-Proceeding of Engineering*, *6*(2), 8766–8787.

Khadafi, S., Nurmuslimah, S., & Anggakusuma, F. K. (2019). Implementasi Firewall Dan Port Knocking Sebagai Keamanan Data Transfer Pada Ftp Server Berbasiskan Linux Ubuntu Server. *Nero*, *4*(3), 181–188.

Mulyanto, Y., Julkarnain, M. ;, & Jabi Afahar, A. (2021). *IMPLEMENTASI PORT KNOCKING UNTUK KEAMANAN JARINGANSMKN 1 SUMBAWA BESAR*. *3*(2), 326–335.

Munawar, Zen and Putri, N. I. (2020). Keamanan Jaringan Komputer Pada Era Big Data. *J-SIKA| Jurnal Sistem Informasi Karya Anak Bangsa*, *02*(01), 14–20.

Navirgo, A., & Habibbullah, A. (2019). Implementasi Data Mining Dengan Algoritma Berbasis Tree Untuk Klasifikasi Serangan Pada Intrusion Detection System (Ids). *Jurnal Simada*, *02*(02), 91–181.

Putri, A., Fatoni, & Solikin, I. (2016). Analisa Kinerja Koneksi Jaringan Komputer Pada Smk Teknologi Bistek Palembang. *Universitas Bina Darma*, *12*, 1–11. https://ejournal.unsrat.ac.id/index.php/elekdankom/article/view/10400/9986

Riska, P., Sugiartawan, P., & Wiratama, I. (2018). Sistem Keamanan Jaringan Komputer Dan Data Dengan Menggunakan Metode Port Knocking. *Jurnal Sistem Informasi Dan Komputer Terapan Indonesia (JSIKTI)*, *1*(2), 53–64. https://doi.org/10.33173/jsikti.12

Santoso, K. (2016). Konfigurasi dan Analisis Performansi Routing OSPF pada Jaringan LAN dengan Simulator Cisco Packet Tracer Versi 6.2. *Jurnal Kajian Teknik Elektro*, *1*(1), 67–78.

Utomo, D., Sholeh, M., & Avorizano, A. (2017). Membangun Sistem Mobile Monitoring Keamanan Web Aplikasi Menggunakan Suricata dan Bot Telegram Channel. *Seminar Nasional Teknoka*, *2*(2502), 82-I 87.

Wijaya, B., & Pratama, A. (2020). Deteksi Penyusupan Pada Server Menggunakan Metode Intrusion Detection System (Ids) Berbasis Snort. *Jurnal Sisfokom (Sistem Informasi Dan Komputer)*, *9*(1), 97. https://doi.org/10.32736/sisfokom.v9i1.770

Yulianeu, A., & Wahab, A. (2017). Simulasi Alat Bantu Pembelajaran Topologi Jaringan Secara Visual. *Jurnal Teknik Informatik*, *4*(1), 32–38.

Daftar Riwayat Hidup

**Data Pribadi** / *Personal Details*

Nama / *Name* : ARIE SOEHARYANTO

NOBP : 17101152630054

Tanggal Lahir / *Date of Birth* : 13 Agustus 1999

Jenis Kelamin / *Gender* : Laki – laki

Warga Negara / *Nationality* : Indonesia

Agama / *Religion* : Islam

Alamat / *Address* : Perumahan Hariguna Permain Blok A No.06,

RT.04 RW.11 Kel.Sidomulyo Barat,

Kec.Tampan, Pekanbaru, Riau

Kode Pos / *Postal Code* : 28294

Nomor Telepon / *Phone* : 081275342334

*Email* : ariesoeharyanto@gmail.com

**DAFTAR LAMPIRAN**

