



**ANALISIS KEAMANAN JARINGAN SISTEM FILTERING
DENGAN KIDSAFE PROXY MENGGUNAKAN
RASPERRY Pi**

Disusun dan Diajukan untuk Memenuhi Persyaratan Ujian Akhir Memperoleh
Gelar Sarjana Komputer pada Fakultas Sains dan Teknologi
Universitas Pembangunan Pancabudi Medan

SKRIPSI

OLEH

**NAMA : SOEDARTA UTAMA
NPM : 1514370574
PROGRAM STUDI : SISTEM KOMPUTER**

**FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2020**

ABSTRAK

SOEDARTA UTAMA

Analisis Keamanan Jaringan Sistem Filtering Dengan Kidsafe Proxy Menggunakan Raspberry Pi 2020

Seiring dengan perkembangan teknologi informasi dan komunikasi, berdampak juga pada gaya hidup manusia. Internet merupakan sarana untuk mencari informasi pada sebuah instansi, perorangan, maupun di dalam kehidupan berkeluarga. Namun tidak dapat di pungkiri banyak dampak buruk dari internet seperti situs terlarang yang tidak boleh di akses. Salah satu metode yang dapat digunakan untuk menjawab masalah tersebut yakni dengan menggunakan *kidsafe proxy*. *Kidsafe* merupakan aplikasi yang di instal pada *server proxy* dengan antamuka berbasis web yang mempermudah pengguna untuk menggunakan dan menjelajahi internet dengan aman. Hasil dari penelitian ini berupa tabel dan gambar yang menunjukkan bahwa sistem dapat melakukan pembatasan hak akses sesuai dengan kategori yang ada.

Kata Kunci: *Kidsafe, Server Proxy, Raspberr Pi.*

DAFTAR ISI

LEMBAR PENGESAHAN	i
SURAT PERNYATAAN	ii
PERNYATAAN ORISINALITAS	iii
ABSTRAK	iv
KATA PENGANTAR	v
DAFTAR ISI	vii
DAFTAR GAMBAR	ix
DAFTAR TABEL	x
DAFTAR LAMPIRAN	xi
BAB I PENDAHULUAN	
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	3
BAB II LANDASAN TEORI	
2.1 Jaringan.....	4
2.1.1 Pengertian Jaringan Komputer	4
2.1.2 Jenis Jenis Jaringan	4
2.1.2.1 <i>Local Area Network (LAN)</i>	4
2.1.2.2 <i>Metropolitan Area Network (MAN)</i>	4
2.1.2.3 <i>Wide Area Network (WAN)</i>	5
2.1.2.4 Internet	5
2.1.2.5 Jaringan Tanpa Kabel.....	5
2.2 Topologi Jaringan.....	5
2.2.1 Topologi Bus	6
2.2.2 Topologi <i>Token Ring</i>	7
2.2.3 Topologi <i>Star</i>	7
2.2.4 Topologi <i>Mesh</i>	9
2.2.5 Topologi <i>Wireless</i>	9
2.3 Fungsi Komputer Dalam Jaringan	10
2.3.1 Jaringan <i>Client Server</i>	10
2.3.2 Jaringan <i>peer-to-peer</i>	10
2.4 Keamanan Jaringan	10
2.5 Jenis Jenis Keamanan Jaringan	11
2.5.1 <i>Physical Security</i>	11
2.5.2 <i>Personal Security</i>	13
2.5.3 Keamanan Data	14
2.5.4 <i>Operating System Security</i>	15
2.6 <i>Protocol TCP/IP</i>	15
2.7 <i>Server</i>	16
2.8 <i>Proxy Server</i>	17

2.9	<i>Web Server</i>	18
2.10	<i>Web Login</i>	19
2.11	<i>Contex Diagram (CD)</i>	19
2.12	<i>Data Flow Diagram (DFD)</i>	19
2.13	<i>Entity Relationship Diagram (ERD)</i>	20
2.14	<i>Flowchart</i>	20
2.15	<i>MySQL</i>	21
2.16	<i>PhpMyAdmin</i>	21
2.17	<i>Kidsafe Proxy</i>	22
2.18	<i>Raspberry Pi</i>	23
2.19	<i>Squid</i>	24

BAB III ANALISIS DAN PERANCANGAN SISTEM

3.1	Tahap Penelitian.....	26
3.2	Metode Pengumpulan Data.....	26
3.3	Analisis Sistem Sedang Berjalan.....	27
3.4	Rancangan Penelitian.....	31
3.4.1	Anggaran Biaya.....	33
3.4.2	<i>Kidsafe Proxy</i> Yang Akan Diterapkan.....	35
3.4.3	<i>Installasi Operating Sistem Raspbian Untuk Raspberry Pi</i>	36
3.4.4	Konfigurasi <i>Remote Connection Raspberry Pi</i>	38
3.4.5	Konfigurasi dan <i>Instalasi Squid Kidsafe Proxy</i>	40
3.4.6	Pengujian Yang Dilakukan Terhadap <i>Kidsafe Proxy</i>	41

BAB IV Hasil Dan Pembahasan

4.1	Kebutuhan <i>Spesifikasi Hardware dan Software</i>	43
4.2	Pengujian dan Pembahasan.....	46
4.2.1	Pembahasan.....	47
4.2.2	Pengujian Dan Analisa.....	54

BAB V PENUTUP

5.1	Kesimpulan.....	59
5.2	Saran.....	60

DAFTAR PUSTAKA

BIOGRAFI PENULIS

LAMPIRAN-LAMPIRAN

BAB I

PENDAHULUAN

1. Latar Belakang

Internet saat ini sangat berperan penting dalam kehidupan bagi masyarakat modern sebagai sumber daya informasi. Hampir seluruh lapisan masyarakat menggunakan internet dan berinteraksi dengan internet sesuai dengan kepentingan mereka masing masing.

Hal yang harus di perhatikan dalam penggunaan internet adalah dampak buruk dari internet, terutama di kalangan anak-anak. Banyak situs situs yang berdampak negatif bagi anak-anak seperti situs *pornography*, perjudian, dan situs situs terlarang yang mengandung virus serta *file-file* berbahaya lainnya. Untuk mengurangi atau mengatasi dampak tersebut, perlu di lakukannya keamanan jaringan untuk membatasi hak hak akses internet pada setiap kalangan pengguna.

Kidsafe merupakan program yang di rancang untuk di instal pada *proxy squid* yang menyediakan kontrol dengan antarmuka *web* untuk membatasi hak akses internet berdasarkan *rule* yang di terapkan dalam jaringan lokal. *Kidsafe* bukan *firewall*, meskipun beberapa fungsi *firewall* turut disertakan. *Kidsafe* bekerja di dalam *proxy*, cara kerjanya yaitu sebelum permintaan data dari *client* sampai ke tujuannya (*web server* lain) di internet, data tersebut terlebih dahulu akan di arahkan ke *server proxy*. *Server Proxy* akan menjalankan beberapa fungsi yakni *sharing*, dalam praktiknya semua *client* bisa bersama sama saling terhubung ke *server proxy* dan dapat melakukan akses internet secara bersamaan melalui *server proxy*. Kemudian fungsi *caching* yakni membuat salinan data konten di dalam

cache proxy, sehingga apabila client ingin mengakses situs atau konten yang sama, *server proxy* tidak perlu lagi menghubungi alamat yang menyediakan konten tersebut [1].

Raspberry Pi, sering disingkat dengan nama *Raspi*, adalah komputer papan tunggal (*single-board circuit; SBC*) yang seukuran dengan kartu kredit yang dapat digunakan untuk menjalankan program perkantoran, permainan komputer, dan sebagai pemutar media hingga video beresolusi tinggi.

Berdasarkan latar belakang diatas, maka dalam penelitian ini penulis mengambil suatu topik penelitian yaitu mengenai “ Analisis Keamanan Jaringan Sistem Filtering Dengan Kidsafe Proxy Menggunakan Raspberry Pi “.

2. Perumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan di atas maka rumusan masalah pada penelitian ini sebagai berikut:

- a. Bagaimana cara mengatasi dampak negatif penggunaan internet khususnya pada anak-anak?
- b. Bagaimana cara membangun keamanan jaringan sistem filtering dengan kidsafe proxy menggunakan raspberry pi?

3. Batasan Masalah

Untuk mendapatkan pembahasan semaksimal mungkin dan agar mudah dipahami serta menghindari pembahasan yang terlalu meluas, maka batasan masalah yang dibahas dalam laporan skripsi ini adalah:

- a. Penulis membuat suatu *login* untuk para pengguna internet agar bisa di batasi hak akses yang akan di gunakan oleh *user*.
- b. Penulis membangun keamanan jaringan dengan *kidsafe proxy* menggunakan *raspberry pi* di dalam sistem operasi *raspbian jessy*.

4. ***Tujuan Penelitian***

Adapun tujuan dari penelitian ini adalah sebagai berikut :

- a. Menbatasi hak akses pada penggunaan internet khususnya kepada anak anak dengan memblok situs situs yang berbahaya buat anak anak..
- b. Membangun suatu *proxy kidsafe* menggunakan *raspberry pi* dengan tujuan membatasi hak akses situs internet..

5. ***Manfaat Penelitian***

Adapun manfaat penulisan skripsi ini adalah sebagai berikut:

- a. Dapat mengurangi dampak negatif dalam penggunaan internet pada anak anak dengan membatasi hak akses situs internet.
- b. Dapat memberikan tambahan ilmu dan pengetahuan *praktis* dari keadaan sebenarnya untuk mengimplementasikan ilmu pengetahuan yang didapat dalam perkuliahan khususnya tentang *proxy server*.

BAB II

LANDASAN TEORI

2.1 Jaringan

2.1.1 Pengertian Jaringan Komputer

Jaringan komputer adalah suatu kumpulan beberapa komputer yang saling terhubung sehingga dapat saling berkomunikasi satu sama lain dengan komputer lainnya. Dengan adanya jaringan komputer, seorang user bisa memperoleh informasi dengan mudah tanpa bertemu secara langsung dengan user lainnya.

2.1.2 Jenis Jenis Jaringan

2.1.2.1 *Local Area Network (LAN)*

Merupakan jaringan *internal* di dalam sebuah gedung atau kampus. *LAN* seringkali digunakan untuk menghubungkan komputer komputer pribadi dan *workstation* dalam kantor suatu organisasi, perusahaan atau pabrik-pabrik untuk memakai bersama sumberdaya (misalnya *printer*, media penyimpanan/*storage*) dan saling bertukar informasi.

2.1.2.2 *Metropolitan Area Network (MAN)*

Merupakan versi *LAN* yang dengan area yang lebih luas dan biasanya menggunakan teknologi yang sama dengan *LAN*. *MAN* dapat mencakup kantor-kantor perusahaan yang letaknya berdekatan atau juga sebuah kota dan dapat dimanfaatkan untuk keperluan pribadi (swasta) atau umum (Lukman.N ,2016).

2.1.2.3 Wide Area Network (WAN)

Jangkauannya mencakup daerah *geografis* yang luas, seringkali mencakup sebuah negara bahkan benua. WAN terdiri dari kumpulan mesin-mesin yang bertujuan untuk menjalankan program-program (aplikasi) pemakai.

2.1.2.4 Internet

Orang yang terhubung ke jaringan sering berharap untuk bisa berkomunikasi dengan orang lain yang terhubung ke jaringan lainnya. Keinginan seperti ini memerlukan hubungan antar jaringan yang seringkali tidak *kompatibel* dan berbeda. Kumpulan jaringan yang saling terhubung (*terinterkoneksi*) inilah yang disebut dengan internet.

2.1.2.5 Jaringan Tanpa Kabel

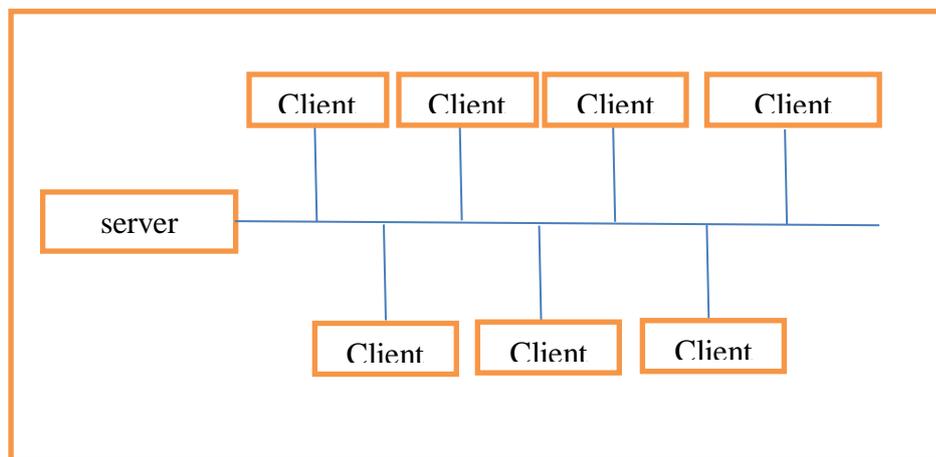
Jaringan ini lebih dikenal dengan *wireless* merupakan suatu solusi terhadap komunikasi yang tidak bias dilakukan dengan jaringan yang menggunakan kabel. Jaringan tanpa kabel lebih leluasa bergerak (*mobile*) dalam melakukan aktifitas komunikasi (Lukman.N ,2016).

2.2 Topologi jaringan .

Topologi jaringan komputer adalah suatu cara menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk jaringan. Cara yang saat ini banyak digunakan adalah bus, token *ring*, dan *star*. Dalam suatu jaringan komputer jenis topologi yang dipilih akan mempengaruhi kecepatan komunikasi. Untuk itu maka perlu dicermati kelebihan/keuntungan dan kekurangan atau kerugian dari masing-masing topologi berdasarkan karakteristiknya.

2.2.1 Topologi Bus

Topologi bus terlihat pada Gambar 2.1. Media penghantar untuk jenis topologi BUS adalah kabel Koaksial. Topologi BUS menggunakan metode *unicast*, *multicast* dan *broadcast*. *Unicast* adalah komunikasi antara satu pengirim dengan satu penerima di jaringan. *Multicast* adalah komunikasi antara satu pengirim dengan banyak penerima di jaringan. Sedangkan pada *Broadcast*, setiap titik akan menerima dan menyimpan *frame* yang disalurkan/dihantarkan.



Gambar 2.1. Topologi Bus

Keuntungan topologi bus :

1. Hemat kabel
2. *Layout* kabel sederhana
3. Mudah dikembangkan

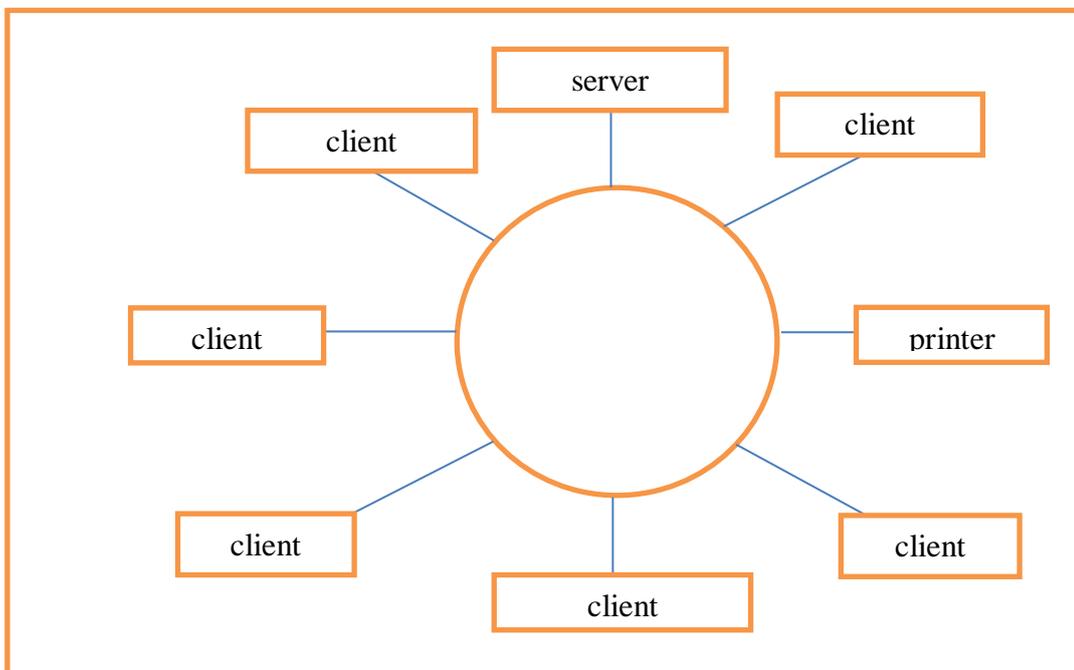
Kerugian topologi bus :

1. *Deteksi* dan isolasi kesalahan sangat kecil
2. Kepadatan lalu lintas

3. Bila salah satu *client* rusak, maka jaringan tidak bisa berfungsi
4. Diperlukan repeater untuk jarak jauh Topologi *Token Ring*

2.2.2 Topologi *Token Ring*

Topologi *token ring* merupakan topologi dengan metode *ring* dimana metode ini menghubungkan satu komputer dengan yang lainnya dalam bentuk lingkaran atau *ring*., dimana setiap simpul mempunyai tingkatan yang sama.

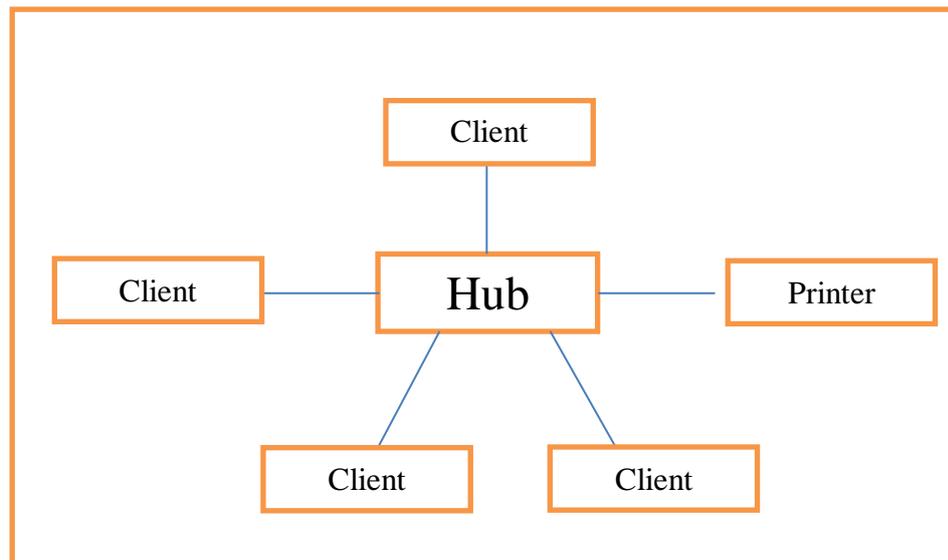


Gambar 2.2 Topologi *Token Ring*

Topologi *token ring* mempunyai keuntungan yaitu hemat dalam penggunaan kabel dan biaya. Tetapi topologi ini juga mempunyai kekurangan yaitu dalam pengembangan jaringan jenis ini sangat kaku.

2.2.3 Topologi *Star*

Topologi *Star* adalah Topologi dimana model topologi ini berbentuk bintang (*Star*) dan pada topologi ini semua client terkontrol di pusat.



Gambar 2.3 Topologi *Star*

Keuntungan topologi *star* :

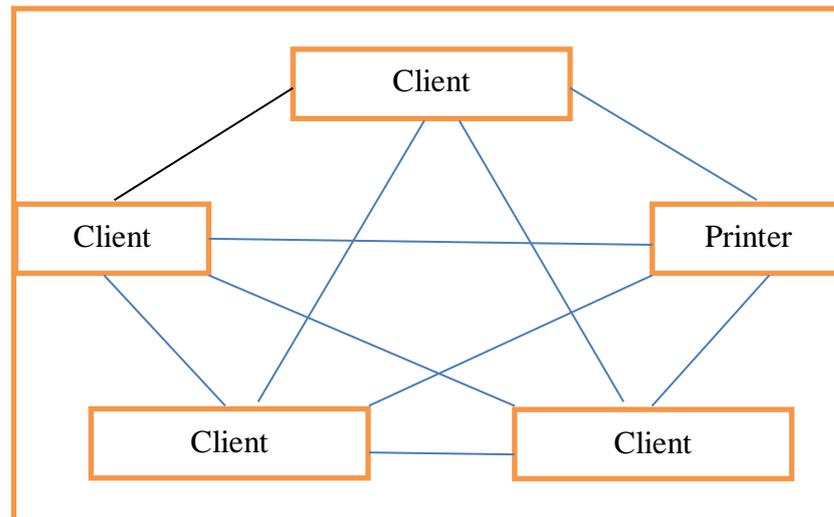
1. Paling *fleksibel*
2. Pemasangan/perubahan stasiun sangat mudah dan tidak mengganggu bagian jaringan lain
3. Kontrol terpusat
4. Kemudahan deteksi dan isolasi kesalahan/kerusakan
5. Kemudahan pengelolaan jaringan

Kerugian topologi *star* :

1. Boros kabel
2. Perlu penanganan khusus
3. Kontrol terpusat (*HUB/Switch*) jadi elemen kritis.

2.2.4 Topologi MESH

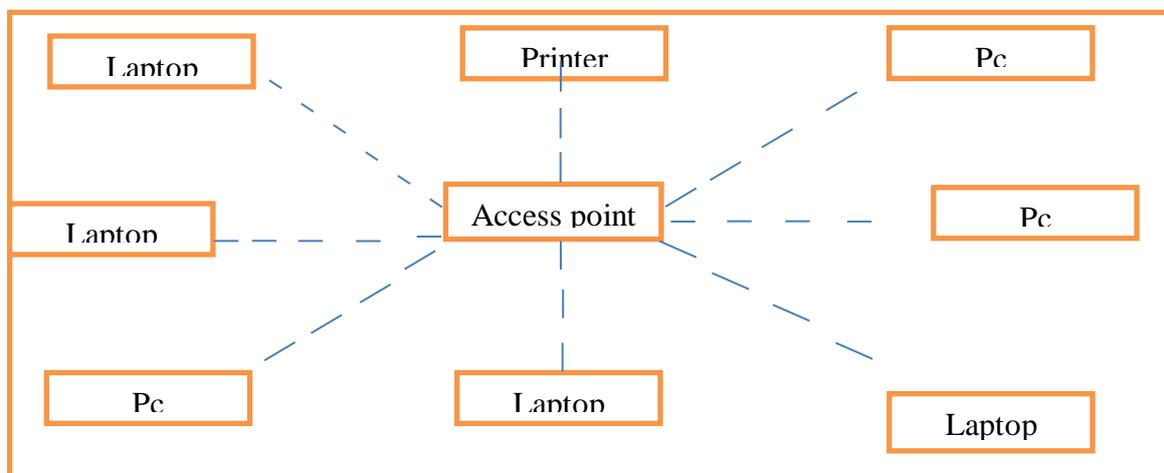
Topologi *Mesh* dibangun dengan banyak *link*, dimana pada setiap komputer menggunakan lebih dari satu *NIC*.



Gambar 2.4 Topologi Mesh

2.2.5 Topologi WIRELESS

Topologi *wireless* adalah jenis topologi dimana satu komputer dan komputer lainnya dapat terhubung dengan gelombang radio..



Gambar 2.5 Topologi wireless

2.3 Fungsi Komputer Dalam Jaringan

2.3.1 Jaringan *Client Server*

Jaringan *Client Server* merupakan jaringan dimana satu komputer bertindak sebagai server murni. Maksudnya Dalam jaringan ini satu komputer berfungsi sebagai pusat pelayanan (*server*) dan komputer yang lain berfungsi meminta pelayanan (*client*). Sesuai dengan namanya, *client-server* berarti adanya pembagian kerja pengolahan data *client* dan *server*.

2.3.2 Jaringan *Peer – to – Peer*

Dalam jaringan ini tidak ada komputer yang berfungsi khusus, dan semua komputer dapat berfungsi sebagai *client* dan *server* dalam satu saat yang bersamaan. Pengguna masing-masing komputer bertanggung jawab terhadap *administrasi resource* komputer (dengan membuat nama *user*, membuat *share*, menandai izin mengakses *share* tersebut) (Yuisar, et al., 2015).

2.4 Keamanan Jaringan

secara umum adalah komputer yang terhubung ke *network*, mempunyai ancaman keamanan lebih besar daripada komputer yang tidak terhubung ke manamana.” Dengan pengendalian yang teliti, resiko tersebut dapat dikurangi, namun *network security* biasanya bertentangan dengan *network access*, di mana bila *network access* semakin mudah, maka *network security* semakin rawan, begitu pula sebaliknya. Keamanan jaringan (*network security*) dalam jaringan komputer sangat penting dilakukan untuk memonitor akses jaringan dan mencegah

penyalahgunaan sumber daya jaringan yang tidak sah. gas keamanan jaringan dikontrol oleh *administrator* jaringan (Sutarti, et all., 2017).

prinsip keamanan jaringan komputer diklasifikasikan menjadi 3 bagian:

1. *Confidentiality* (kerahasiaan)
2. *Integrity* (integritas)
3. *Availability* (ketersediaan)

2.5 Jenis Jenis Keamanan Jaringan

2.5.1 *Physical Security*

Merupakan jenis keamanan jaringan yang bersifat fisik.



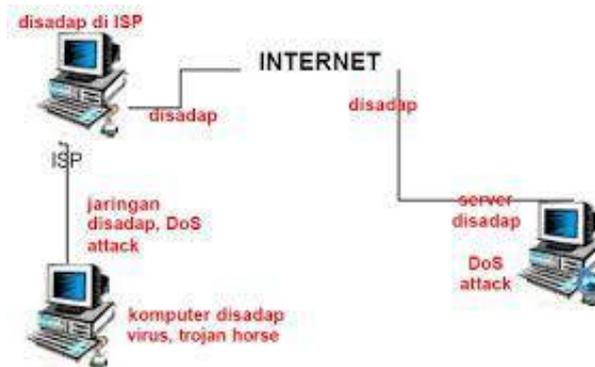
Gambar 2.6 *physical security*

Sumber: <http://kang-saleh.blogspot.com/2016/07/jenis-jenis-keamanan-jaringan-komputer.html>

Physical security menfokuskan pada *strategi* untuk mengamankan pekerja atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran, akses tanpa *otorisasi*, dan bencana alam. Jenis *physical security*

termasuk juga akses orang ke gedung serta peralatan dan media yang digunakan. Contohnya adalah sebagai berikut.

a.) *Wiretapping*, merupakan jenis *Physical security* yang berhubungan dengan akses ke kabel atau komputer yang digunakan, misalnya *scanner* pada bank.

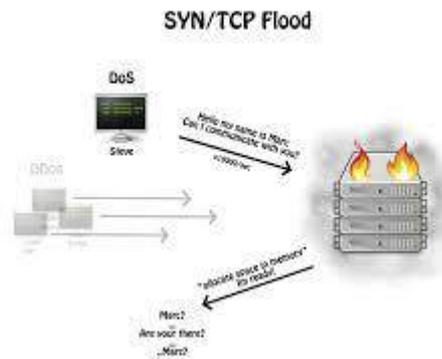


Gambar 2.7 Jenis *Physical Security wiretapping*

Sumber: <http://kang-saleh.blogspot.com/2016/07/jenis-jenis-keamanan-jaringan-komputer.html>

Pada proses *wiretapping*, penyadapa melakukan proses pengambilan data yang ditransmisikan pada saluran kabel komunikasi dengan menggunakan sambungan perangkat keras.

b.) *Denial of service*, merupakan jenis *physical security* dengan cara mematikan peralatan atau membanjiri saluran komunikasi dengan pesan-pesan yang tidak jelas. Akibat yang ditimbulkan oleh *denial of service* adalah layanan (*service*) tidak dapat diterima oleh pemakai karena terlalu banyak jumlah pesan yang diterima atau masuk (1).

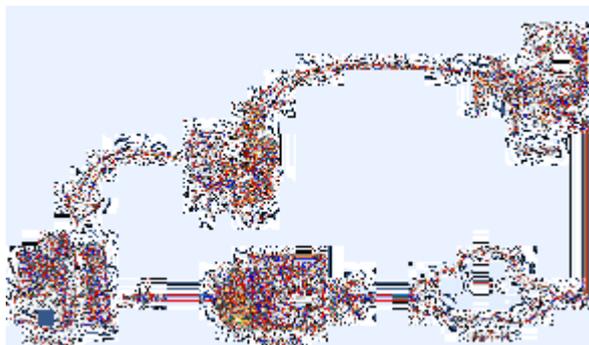


Gambar 2.8 *Syn flood attack*

Sumber: <http://kang-saleh.blogspot.com/2016/07/jenis-jenis-keamanan-jaringan-komputer.html>

2.5.2 *Personal Security*

Keamanan yang berhubungan dengan orang (*personal*). merupakan jenis keamanan yang berhubungan dengan *indeftikasi user* (yaitu *usrname* dan *password*) dari orang yang memilik akses, baik pemakai merupakan pengelola. Artinya, kelemahan dari keamanan sistem seringkali disebabkan oleh pengelola atau *user* yang menggunakan sistem jaringan. Keamanan yang berhubungan dengan orang-orang yang melakukan tindakan kriminal dan seolah-olah sebagai pengguna atau pengases informasi asli sering dikenal dnegan istilah "*social engineering*" (1).



Gambar 2.9 Social engineering

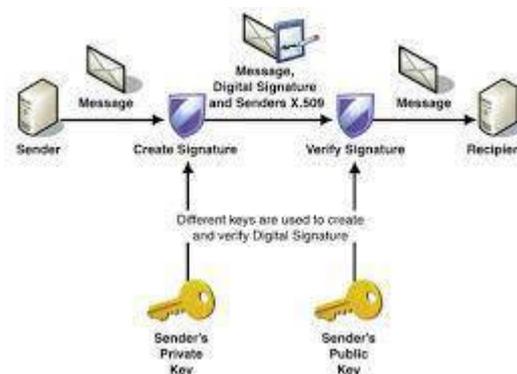
Sumber: <http://kang-saleh.blogspot.com/2016/07/jenis-jenis-keamanan-jaringan-komputer.html>

keterangan gambar di atas:

keamanan yang berhubungan dengan *personal* dikenal dengan istilah *social engineering*. Semakin banyak penyanggah atau proses serangan yang dilakukan secara langsung pada pengguna dengan membocorkan berbagai macam informasi yang sangat *sensitif*, asumsinya pengguna tidak melakukan kesalahan pada sistem tersebut .

2.5.3 Keamanan Data

Keamanan dari data dan media serta tekni komunikasi, merupakan jenis keamanan yang berhubungan dengan kelemahan dari *software* yang digunakan untuk memproses dan mengelola data. Kejahatan dilakukan oleh seorang yang tidak bertanggung jawab dengan memasang dan menyebarkan virus atau *trojan horses* sehingga orang tersebut mendapatkan *password* atau hak akses yang bukan miliknya .

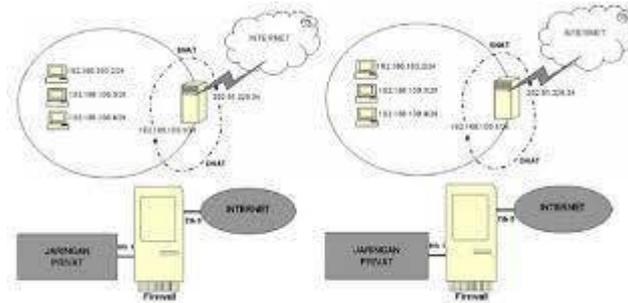


Gambar 2.10 Keamanan Data dan Media

Sumber: <http://kang-saleh.blogspot.com/2016/07/jenis-jenis-keamanan-jaringan-komputer.html>

2.5.4 Operating System Security

Keamanan dalam operasi, merupakan jenis keamanan jaringan berhubungan dengan *prosedur* untuk mengatur dan mengelola sistem keamanan.



Gambar 2.11 Keamanan yang berhubungan dengan prosedur

Sumber: <http://kang-saleh.blogspot.com/2016/07/jenis-jenis-keamanan-jaringan-komputer.html>

2.6 Protokol TCP / IP

TCP / IP adalah salah satu perangkat lunak jaringan komputer (*networking software*) yang terdapat dalam sistem, dan dipergunakan dalam komunikasi data dalam *local area network (LAN)* maupun Internet. *TCP* singkatan dari *Transmission Control Protocol* dan *IP* singkatan dari *Internet Protocol*. *TCP/IP* menjadi satu nama karena fungsinya selalu bergandengan satu sama lain dalam komunikasi data. *TCP/IP* saat ini dipergunakan dalam banyak jaringan komputer lokal (*LAN*) yang terhubung ke Internet, karena memiliki sifat:

- 1) Merupakan *protokol standar* yang terbuka, gratis dan dikembangkan terpisah dari perangkat keras komputer tertentu. Karena itu *protokol* ini banyak didukung oleh *vendor* perangkat keras, sehingga *TCP/IP* merupakan pemersatu perangkat keras komputer yang beragam merek begitu juga sebagai pemersatu berbagai perangkat lunak yang beragam merk sehingga walau memakai

perangkat keras dan perangkat lunak komputer yang berlainan, komputer dan komputer lainnya dapat berkomunikasi data melalui Internet (Yuisar, et all., 2015).

- 2) Berdiri sendiri dari perangkat keras jaringan apapun. Sifat ini memungkinkan *TCP/IP* bergabung dengan banyak jaringan komputer. *TCP/IP* bisa beroperasi melalui sebuah *Ethernet*, sebuah saluran *dial-up*, dan secara *virtual* melalui berbagai media fisik transmisi data.
- 3) Bisa dijadikan alamat umum sehingga tiap perangkat yang memakai *TCP/IP* akan memiliki sebuah alamat unik dalam sebuah jaringan komputer lokal, atau dalam jaringan komputer global seperti Internet (Yuisar, et all., 2015).

2.7 Server

Sebuah *server* (biasanya disebut *server* aplikasi) adalah sebuah program aplikasi yang menerima sambungan untuk permohonan *servis* dan memberikan kembali *respons*. Sebuah *server* aplikasi dapat dijalankan pada komputer yang sama dengan *client* yang menggunakan *server* tersebut, atau dapat tersambung melalui jaringan komputer. *Server* komputer adalah sistem komputer yang dibuat untuk menjalankan aplikasi *server*. Sebuah komputer server yang dialokasikan untuk menjalankan sebuah aplikasi *server* yang *spesifik* seringkali disebut dengan nama aplikasi tersebut. Contoh, jika *software Apache HTTP server* dijalankan di komputer *server* perusahaan, maka biasanya disebut *web server* saja .

Server adalah sebuah sistem komputer yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer. *Server* didukung dengan prosesor yang bersifat *scalable* dan *RAM* yang besar, juga dilengkapi dengan sistem operasi

khusus, yang disebut sebagai sistem operasi jaringan atau *network operating sistem*. *Server* juga menjalankan perangkat lunak *administratif* yang mengontrol akses terhadap jaringan dan sumber daya yang terdapat di dalamnya, seperti halnya berkas atau alat pencetak (*printer*), dan memberikan akses kepada *workstation* anggota jaringan (Yuisar, et all., 2015).

2.8 *Proxy Server*

Proxy server adalah sebuah komputer *server* atau program komputer yang dapat bertindak sebagai komputer lainnya untuk melakukan *request* terhadap *content* dari Internet atau intranet. *Proxy Server* bertindak sebagai *gateway* terhadap dunia ini Internet untuk setiap komputer *client*. *Proxy server* tidak terlihat oleh komputer *client* seorang pengguna yang berinteraksi dengan Internet melalui sebuah *proxy server* tidak akan mengetahui bahwa sebuah *proxy server* sedang menangani *request* yang dilakukannya. *Web server* yang menerima *request* dari *proxy server* akan menginterpretasikan *request - request* tersebut seolah-olah *request* itu datang secara langsung dari komputer *client*, bukan dari *proxy server* .

Proxy server juga dapat digunakan untuk mengamankan jaringan pribadi yang dihubungkan ke sebuah jaringan publik (seperti halnya Internet). *Proxy server* memiliki lebih banyak fungsi daripada *router* yang memiliki fitur *packet filtering* karena memang *proxy server* beroperasi pada *level* yang lebih tinggi dan memiliki kontrol yang lebih menyeluruh terhadap akses jaringan. *Proxy server* yang berfungsi sebagai sebuah "agen keamanan" untuk sebuah jaringan pribadi, umumnya dikenal sebagai *firewall* .

Proxy Server adalah *server* yang diletakkan antara suatu aplikasi *client* dan aplikasi *server* yang dihubungi. Aplikasi *client* dapat berupa *browser web*, *client FTP*, dan sebagainya. Sedangkan aplikasi *server* dapat berupa *server web*, *server FTP* dan sebagainya. *Proxy Server* yang diletakkan di antara aplikasi *client* dan aplikasi *server* tersebut, dapat digunakan untuk mengendalikan maupun *memonitor* lalu-lintas paket data yang melewatinya (Yuisar, et all., 2015).

2.9 Web Server

Web server merupakan suatu perangkat lunak yang berjalan di sisi *server* dan bertugas untuk menerima permintaan dari *web browser*, menerjemahkan permintaan tersebut, dan mengembalikan ke *web browser* hasil dari permintaan. Fungsi utama *Server* atau *Web server* adalah untuk melakukan atau akan *mentransfer* berkas permintaan pengguna melalui *protokol* komunikasi yang telah ditentukan sedemikian rupa. halaman *web* yang diminta terdiri dari berkas teks, video, gambar, *file* dan banyak lagi. Salah satu contoh dari *Web Server* adalah *Apache*. *Apache (Apache Web Server – The HTTP Web Server)* merupakan *web server* yang paling banyak dipergunakan di Internet. Program ini pertama kali didesain untuk sistem operasi lingkungan *UNIX*. *Apache* mempunyai program pendukung yang cukup banyak. Hal ini memberikan layanan yang cukup lengkap bagi penggunaanya .

2.10 *Web Login*

Web login adalah halaman *login* yang ditampilkan pertama kali ketika ada pengguna mengakses internet atau *web server*. Kegunaan dari halaman *web* ini adalah sebagai keamanan sehingga hanya pengguna yang mengetahui *Username* dan *Password* yang benar yang dapat mengakses internet (Aprilianto.P, et all., 2018).

2.11 *Contex Diagram (CD)*

Context diagram merupakan data *flow* diagram yang menggambarkan garis besar *operasional sistem*. Konteks diagram menggambarkan hubungan sistem dengan *entitas-entitas* di luar sistem. *CD* memperlihatkan sistem sebuah proses. Tujuannya adalah memberikan pandangan umum sistem. *CD* memperlihatkan sebuah proses yang berinteraksi dengan lingkungan luarnya. Ada pihak luar yang memberikan masukan dan pihak yang menerima keluaran sistem (Iswandi. E., et all., 2015).

2.12 *Data Flow Diagram (DFD)*

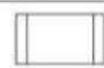
Diagram aliran data sistem disebut juga dengan *Data Flow Diagram (DFD)*. *DFD* sering digunakan untuk menggambarkan suatu sistem yang telah ada atau sistem baru yang akan dikembangkan secara logika tanpa mempertimbangkan lingkungan fisik dimana data tersebut mengalir atau lingkungan fisik dimana data tersebut disimpan. *DFD* menggambarkan arus data didalam sistem dengan terstruktur dan jelas (Iswandi. E., et all., 2015).

2.13 Entity Relationship Diagram (ERD)

Entity Relationship Diagram (ERD) memiliki dua komponen utama yaitu *Entitas (Entity)* dan *Relasi (Relation)*. Kedua komponen ini ,masing-masing dilengkapi dengan sejumlah atribut yang mempresentasikan seluruh fakta yang ada di dunia nyata. *ERD* ini dapat digambarkan secara sistematis dengan menggunakan simbol-simbol .

2.14 Flowchart

Flowchart merupakan urutan-urutan langkah kerja suatu proses yang digambarkan dengan menggunakan simbol-simbol yang disusun secara *sistematis*. Simbol-simbol yang digunakan untuk menggambarkan *flowchart* dapat dilihat pada gambar 2.13 (Iswandi. E., et all., 2015).

SIMBOL-SIMBOL DIAGRAM ALIR			
Simbol	Maksud	Simbol	Maksud
	Terminal (START, END)		Titik sambungan pada halaman yang sama
	Input/Output (READ, WRITE)		Titik konektor yang berada pada halaman lain
	Proses (menyatakan assignment statement)		Call (Memanggil subprogram)
	Decision (YES, NO)		Dokumen
	Display		Stored Data
	Alur proses		Preparation (Pemberian nilai awal suatu variabel)

Tabel 2.1 Simbol flowchart.

Sumber : <https://bukubiruku.com/simbol-flowchart-dan-fungsinya/>

2.15 *MySQL*

MySQL merupakan *software* yang tergolong *database server* dan bersifat *open source*. *Open Source* menyatakan bahwa *software* ini dilengkapi dengan *source code* (kode yang dipakai untuk membuat *MySQL*), selain tentu saja bentuk *executabel*-nya atau kode yang dapat dijalankan secara langsung dalam *system* operasi, dan bias diperoleh dengan cara mengunduh diinternet secara gratis. Hal menarik lainnya adalah *MySQL* juga bersifat *multiplatform*. *MySQL* dapat dijalankan pada berbagai *system* operasi. Pengaksesan data dalam *database* dapat dilakukan dengan mudah melalui *SQL* (*Structure Query Language*). Data dalam *database* biasa diakses melalui aplikasi non-*web* (misalnya dengan *visual basic*) maupun aplikasi *Web* (misalnya aplikasi *PHP*). *SQL* (*Structured Query Language*) adalah bahasa *standart* yang digunakan untuk mengakses *server database*. Semenjak tahun 70an bahasa ini telah dikembangkan oleh *IBM*, yang kemudian diikuti dengan adanya *Oracle*, *Informix* dan *Sybase*. Dengan menggunakan *SQL*, proses akses *database* menjadi lebih *userfriendly* dibandingkan dengan misalnya *dBase* ataupun *Clipper* yang masih menggunakan perintah – perintah pemrograman murni (Maria.W., et all., 2015).

2.16 *PhpMyAdmin*

PhpMyadmin adalah perangkat lunak bebas yang ditulis dalam bahasa pemrograman *PHP* yang digunakan untuk menangani *administrasi MySQL* melalui

Jejaring Jagat Jembar (*World Wide Web*). *phpMyAdmin* mendukung berbagai operasi *MySQL*, diantaranya (mengelola basis data, tabel tabel, bidang (*fields*), relasi (*relations*), indeks, pengguna (*users*), perijinan (*permissions*), dan lain-lain). Pada dasarnya, mengelola basis data dengan *MySQL* harus dilakukan dengan cara mengetikkan baris-baris perintah yang sesuai (*command line*) untuk setiap maksud tertentu. Jika seseorang ingin membuat basis data (*database*), ketikkan baris perintah yang sesuai untuk membuat basis data. Hal tersebut tentu saja sangat menyulitkan karena seseorang harus hafal dan mengetikkan perintahnya satu per satu. Saat ini banyak sekali perangkat lunak yang dapat dimanfaatkan untuk mengelola basis data dalam *MySQL*, salah satunya adalah *phpMyAdmin*. Dengan *phpMyAdmin*, seseorang dapat membuat *database*, membuat tabel, mengisi data, dan lain-lain dengan mudah, tanpa harus menghafal baris perintahnya. *Php MyAdmin* merupakan bagian untuk mengelola basis data *MySQL* yang ada di komputer (Maria.W., et all., 2015).

2.17 Kidsafe Proxy

Kidsafe merupakan program yang dirancang untuk di install pada proxy squid yang menyediakan kontrol dengan antarmuka web untuk membatasi hak akses internet berdasarkan rule yang diterapkan dalam jaringan lokal. Kidsafe bukan firewall, meskipun beberapa fungsi firewall turut di sertakan. Kidsafe bekerja dalam proxy, cara kerjanya yaitu sebelum permintaan data dari client di sampaikan ketujuannya (web server lain) di internet data tersebut terlebih dahulu akan di arahkan ke server proxy .

Server proxy akan menjalankan beberapa fungsi yakni sharing, dalam praktiknya semua client bisa bersama-sama saling terhubung ke server proxy dan dapat melakukan akses internet secara bersamaan melalui server proxy, kemudian fungsi caching yakni membuat salinan data konten di dalam cache proxy, sehingga apabila client ingin mengakses situs atau konten yang sama, server proxy tidak perlu lagi menghubungi alamat yang menyediakan konten tersebut.

Proses Filtering, Kidsafe proxy dapat diatur untuk melakukan penyaringan terhadap alamat website, kidsafe dalam praktiknya ACL (Access Control List) akan mengizinkan rule yang ditambahkan kedalam rule list, sehingga sistem akan memblokir alamat-alamat yang tidak di tambahkan kedalam rule. Hal ini dikarenakan dalam pembentukan rule tidak murni pada suatu alamat saja, sebab konten dan isi suatu website terkait dengan website lainnya (Radjulan.C.J., et all., 2015).

2.18 *Raspberry PI*

Raspberry Pi merupakan komputer mini yang memiliki ukuran kecil yaitu sebesar kartu *ATM* tetapi mampu menjalankan tugas yang sama dengan komputer *PC*. *Raspberry Pi* dirilis dengan *lisensi Open-Source Hardware* yang berarti rancangan perangkat kerasnya dirilis ke publik agar dapat bebas dipelajari, *dimodifikasi*, *didistribusi*, dirakit, dan dijual sesuai rancangan aslinya. Karena dirilis dengan *lisensi OpenSource Hardware*, *Raspberry pi* telah dipergunakan untuk berbagai keperluan, diantaranya untuk hardware yang menjalankan: *media center*, *Networked komputer*, dan *web server*. Salah satu sistem operasi yang

digunakan oleh *raspberry pi* adalah *raspbian*. *Raspbian* adalah sistem operasi bebas berbasis *Debian GNU/ Linux* dan dioptimalkan untuk perangkat keras *Raspberry Pi* (Aprilianto.P, et all., 2018).



Gambar 2.12 *Raspberry pi3*

Sumber : Aprilianto.P, et all., 2018

2.19 Squid

Squid adalah program proxy server yang tersedia secara open source yang sangat banyak kegunaannya, salah satunya untuk melakukan cache terhadap konten pada dari sebuah website. Squid memiliki banyak jenis penggunaan, mulai dari mempercepat server web dengan melakukan caching permintaan yang berulang-ulang, caching DNS, caching situs web, dan caching pencarian komputer di dalam jaringan untuk sekelompok komputer yang menggunakan sumber daya jaringan yang sama, hingga pada membantu keamanan dengan cara melakukan penyaringan (filter) lalu lintas. Meskipun seringnya digunakan untuk protokol HTTP dan FTP, Squid juga menawarkan dukungan terbatas untuk beberapa protokol lainnya

termasuk Transport Layer Security (TLS), Secure Socket Layer (SSL), Internet Gopher, dan HTTPS (Putra.E., Ariffin., 2019).

BAB III

METODE PENELITIAN

1. Tahap Penelitian

Metode yang digunakan dalam membangun penelitian ini adalah dengan Metode pengumpulan data, pengumpulan data adalah tahapan yang penting dalam berlangsungnya sebuah *riset*, karena demi mendapatkan data yang tepat maka *riset* akan berlangsung sesuai dengan rumusan masalah yang telah ditentukan. Metode pengumpulan data yang digunakan adalah studi pustaka, studi sejenis, wawancara dan *obeservasi*.

2. Metode Pengumpulan Data

a. Studi Pustaka

Studi Pustaka adalah tahap yang mana dengan mempelajari teori-teori yang ada dan berkaitan mengenai penelitian dalam mendukung pemecahan masalah penelitian. Dalam pencarian *referensi* didapati pada perpustakaan, toko buku, jurnal, buku *elektronik*, dan sarana *online* melalui internet. Pustaka yang dijadikan acuan terdapat pada Daftar Pustaka.

b. Studi Sejenis

Pada tahap ini dilakukan *studi* sejenis mengenai analisis keamanan jaringan sistem *filtering* dengan *kidsafe proxy* menggunakan *Raspberry Pi 3+*. *Studi* sejenis yang digunakan dapat berupa skripsi, jurnal, artikel ilmiah, maupun dari studi kasus yang pernah ada.

c. *Wawancara*

Dalam tahap ini penulis melakukan pertemuan dan *wawancara* kepada pihak-pihak yang berhubungan dan berpengalaman dengan penelitian ini

d. *Observasi*

Tahap ini bertujuan untuk memperoleh informasi mengenai perangkat dan data yang dibutuhkan yang berkaitan dengan penelitian ini.

3. Analisis Sistem Sedang Berjalan

Internet bukanlah lagi mainan baru dalam kalangan anak-anak, kebebasan anak-anak dalam mengakses internet tentu kadang tidak selamanya dapat dipantau oleh orang dewasa, dengan kebebasan itu terkadang anak-anak tidak memikirkan dampak buruk dalam mengakses internet seperti halnya dalam mengakses situs yang tidak seharusnya untuk diakses oleh anak-anak seperti *pornografi*, perjudian, situs hiburan, dan lainnya. Dengan begitu orang tua pasti menginginkan anak-anak mereka untuk dapat mengakses internet untuk hal yang aman dan sehat, dengan begitu orang tua membutuhkan pembatasan akses internet untuk anak-anak mereka. dengan menggunakan *kidsafe proxy* setidaknya dapat menjawab kekhawatiran para orang tua dalam membatasi kebebasan anak untuk berinternet dengan mengarahkan mereka kesitus yang aman dan sehat.

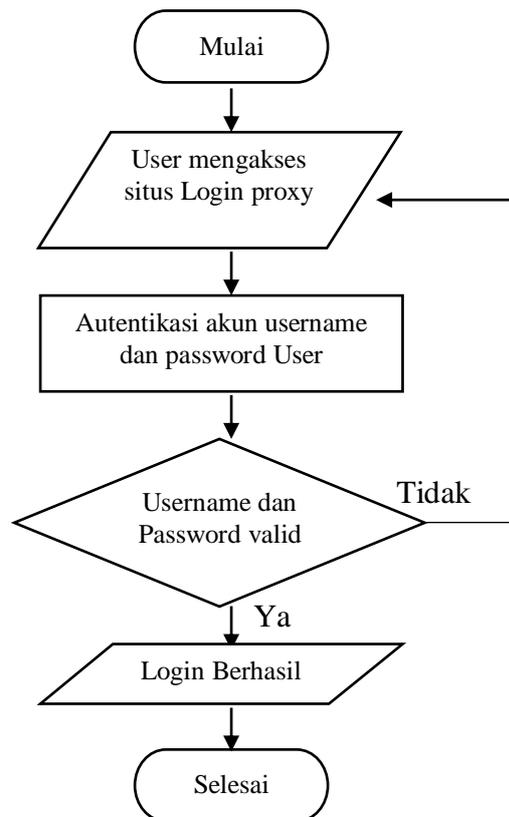
Kidsafe adalah sebuah perangkat lunak yang telah dikembangkan untuk mendukung *Squid proxy* dalam menyediakan kendali dalam bentuk *basis web* dengan fungsi untuk membatasi hak akses internet sesuai dengan *rule* yang

diterapkan. *Kidsafe* bekerja dengan mengalihkan permintaan data dari *client* terlebih dahulu ke *web proxy* server lokal.

Raspberry pi adalah komputer dengan memiliki ukuran kecil yang dilengkapi dengan *processor*, *RAM*, dan beberapa *port* yang dapat kita temukan pada sebuah komputer besar. Dalam penelitian ini *Raspberry pi* akan berfungsi sebagai sebuah *server* kecil yang didalamnya akan diisi oleh *kidsafe proxy* untuk *filtering* akses internet.

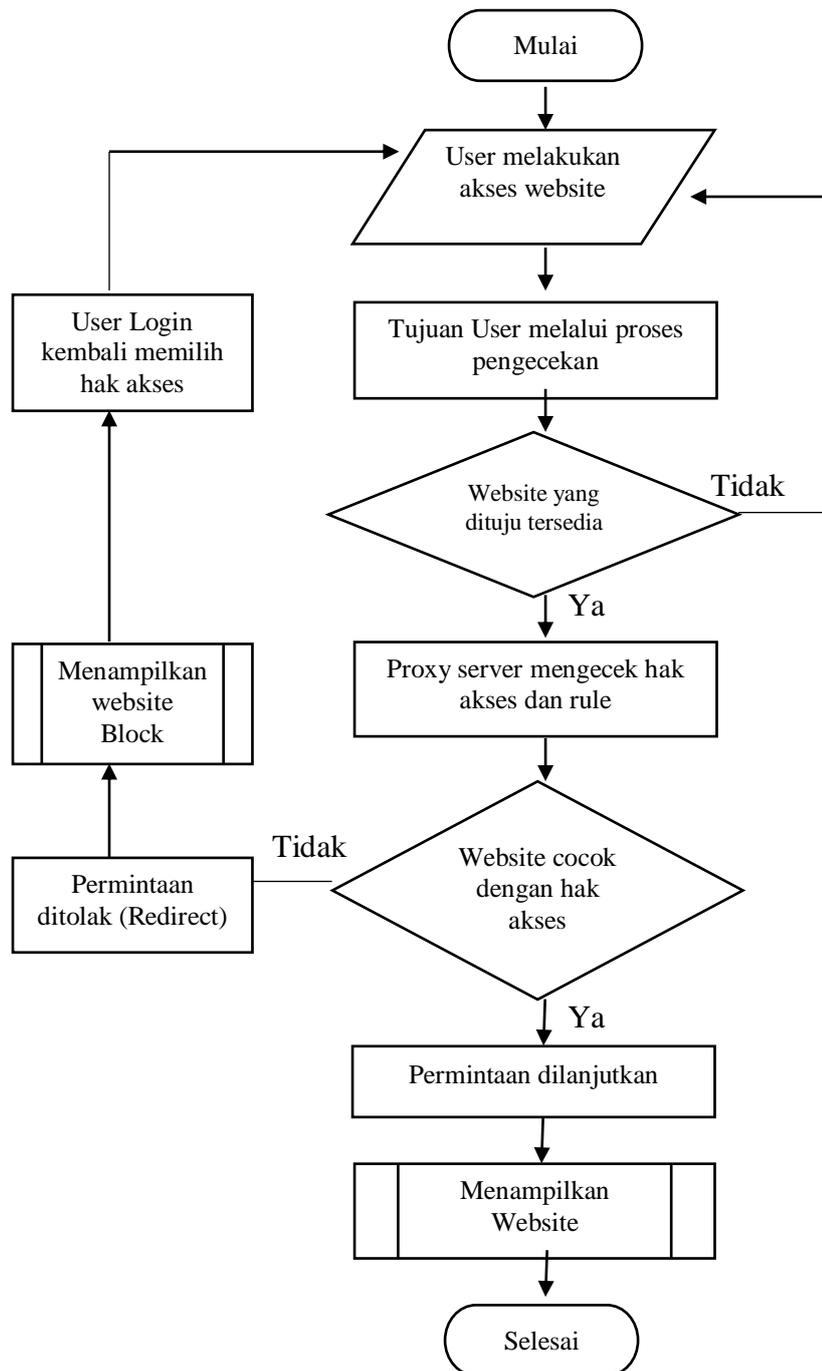
Cara kerja dari sistem *filtering kidsafe proxy* dapat dideskripsikan langkah pengujian yang dilakukan.

Proses kerja dari *kidsafe proxy* sebelum masuk dalam proses *filtering* diawali ketika *user* melakukan *login* dengan mengunjungi situs *kidsafe*, sebab sebelum *user* dapat menikmati internet tanpa *terblokir*, *user* harus melakukan *login* terlebih dahulu yang nantinya apakah *user* itu anak-anak, remaja atau orang dewasa.



Gambar 3.1 Proses *login Kidsafe Proxy*

Pada gambar 3.1 menjelaskan proses login nantinya melalui dari proses *autentikasi* dengan mencocokkan apakah *username* dan *password valid* dengan yang ada didalam *database*. Bila proses *autentikasi* tersebut memeriksa *username* dan *password* cocok dengan *database* yang ada maka proses *login* dikatakan berhasil dan bila proses *autentikasi username* dan *password* tidak cocok dengan *database* maka akan menginformasikan bahwa *username* dan *password* salah



Gambar 3.2 Proses kerja *filtering Kidsafe Proxy*

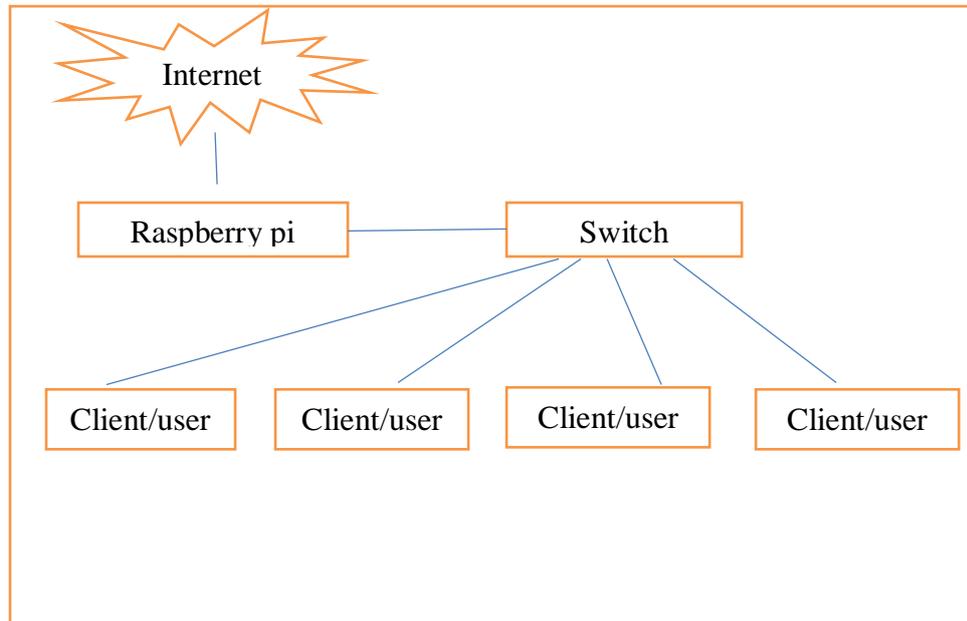
Pada gambar 3.2 dapat dijelaskan setelah dilakukannya proses *login*, kemudian tahap kerja dari *kidsafe proxy* sendiri yaitu dapat dijelaskan seperti berikut:

- a. Diawali dengan *user* melakukan pencarian sebuah *website*.
- b. *Website* diproses apakah *website* tersebut ada atau tidak, bila *website* tersebut tidak tersedia maka *user* diarahkan kembali untuk melakukan pencarian *website* dan bila *website* tersedia maka data akan diarahkan pada proses *filtering*.
- c. Proses *filtering* ini nantinya akan menyeleksi dengan mengecek komponen dari *website* tujuan baik dari alamat, *level user*, izin *user* sesuai dengan *rule* yang nantinya akan diseleksi apakah alamat *website* yang dituju sesuai dengan hak akses *user*.
- d. Bila *website* melewati penyeleksian dan menghasilkan hak akses sesuai maka *user* diizinkan mengakses *website* dan bila hak akses *user* di tolak (*redirect*) maka *user* dialihkan pada sebuah *website Block user* dan *user* disuruh untuk melakukan *login* ulang untuk memilih hak *user* yang cocok dengan izin mengakses *website* tersebut.

4. Rancangan Penelitian

Dalam tugas akhir ini akan menerapkan sebuah keamanan jaringan sistem *filtering* dengan *kidsafe proxy* menggunakan *Raspberry pi* .

Sistem yang akan di bangun dapat digambarkan dengan topologi berikut:



Gambar 3.3 Topologi keamanan jaringan dengan *Kidsafe proxy*

Dalam gambar 3.3 Diatas dapat dijelaskan dengan pengalamatan *IP* pada tabel berikut ini:

Tabel 3.1 Daftar Alamat IP

NO	<i>Hardware/Software Network</i>	<i>Port Ethernet</i>	<i>Alamat IP / IP Address</i>
1	Internet	-	<i>Address 192.168.43.1</i>
2	<i>Raspberry Pi</i>	<i>Eth 0</i>	<i>Address 192.168.43.5</i> <i>Netmask 255.255.255.0</i> <i>Gateway 192.168.43.1</i>

		<i>Eth 1</i>	<i>Address</i> 192.168.10.1 <i>Netmask</i> 255.255.255.0
4	<i>Client</i> Terhubung Jaringan Lokal	<i>Port</i> <i>switch</i>	<i>Address</i> 192.168.10.2- 192.168.10.254 <i>Gateway</i> 192.168.10.1

Dalam tabel 3.1 Pengalamatan alamat *Ip* dapat dejalaskan bahwa:

1. Sistem akan memproses semua data dari *client* yang menuju ke akses internet, pada sisi *Raspberry pi* akan terjadinya proses *kidsafe proxy filtering*.
2. *Client/User* akan menikmati koneksi internet melalui *Raspberry Pi*.
3. *Raspberry pi* berisikan *kidsafe proxy* yang bekerja untuk memfilter situs-situs *web* sesuai dengan kategori yang ditentukan.

3.4.1 Anggaran Biaya

Untuk memenuhi dalam penelitian ini penulis melakukan pengumpulan biaya yang dikeluarkan untuk penelitian mengenai analisis keamanan jaringan sistem *filtering* dengan *kidsafe proxy* menggunakan *raspberry pi*, sebagai berikut:

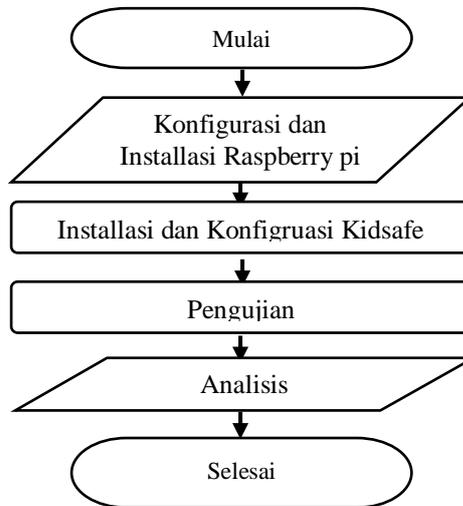
Tabel 3.2 Biaya Keseluruhan

NO	Hardware/Software	Spesifikasi	Harga
1	<i>Raspberry pi 3 +</i>	SoC: <i>Broadcom BCM2837</i> CPU: 4x <i>ARM Cortex-A53</i> , 1.2GHz GPU: <i>Broadcom VideoCore IV</i> RAM: 1GB <i>LPDDR2 (900 MHz)</i> Networking: 10/100 <i>Ethernet</i> , 2.4GHz <i>802.11n wireless</i> <i>Bluetooth: Bluetooth 4.1 Classic</i> , <i>Bluetooth Low Energy</i> Storage: <i>microSD</i> GPIO: 40-pin <i>header, populated</i> Ports: <i>HDMI, 3.5mm analogue</i> <i>audio-video jack, 4x USB 2.0</i> , <i>Ethernet, Camera Serial Interface</i> <i>(CSI), Display Serial Interface</i> <i>(DSI)</i>	Rp. 800.000
2	<i>MicroSDHC Sandisk</i>	<i>Sandisk Ultra 32GB Class 10</i>	
	<i>Adaptor</i>	<i>High Quality Adaptor 5V3A</i>	
	<i>Fan</i>	<i>Fan 5V</i>	
	<i>Heatsink</i>	-	
3	<i>Cable UTP 1.5 Meter</i> <i>+ 2 RJ45</i>	Cat 5	Kabel Rp. 3000/Meter RJ45 Rp. 500
5	3 Laptop untuk <i>Client</i>	<i>Client 1:</i>	<i>Client 1:</i> Rp.

	Intel® Core™ i3 generasi ke-4	5.300.000
	Ram 4 GB	<i>Client 2:</i> Rp. 3.400.000
	HDD 500 GB	<i>Client 3:</i> Rp. 3.100.000
	Intel Celeron B877	
	Ram 4Gb	
	HDD 320 Gb	
	<i>Client 3:</i>	
	Processor AMD A6-6310	
	Ram 2 Gb	
	HDD 500 Gb	

3.4.2 *Kidsafe Proxy* yang akan diterapkan

Dalam membangun penelitian agar berjalan sesuai dengan apa yang diinginkan dengan baik, dibutuhkannya proses yang akan dibuat dalam bentuk diagram alir berikut :



Gambar 3.4 Flowchart langkah penerapan *kidsafe proxy*

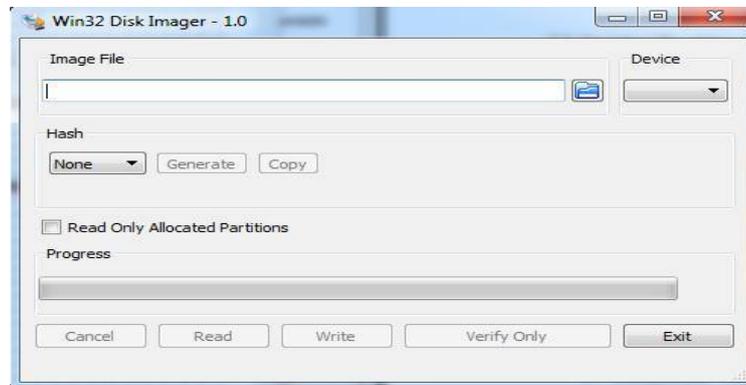
Untuk penjelasan pada gambar diatas sebagai berikut :

1. Diawali dengan menginstallasi dan konfigurasi apa-apa saja yang di butuhkan *raspberry pi* sehingga nantinya *raspberry pi* dapat bekerja menjadi sebuah *server* mini dalam menampung *kidsafe proxy*.
2. Setelah itu lakukan instalasi kebutuhan paket dan konfigurasi *squid proxy* dengan *kidsafe proxy filter*.
3. Setelah itu lakukan pengujian terhadap *kidsafe proxy* yang telah dibangun.
4. Bila semua tahap telah berhasil, lakukan tahap akhir yaitu lakukan pengumpulan data dan menganalisa.

3.4.3 Instalasi operating sistem Raspbian untuk *raspberry pi*

Pada penelitian ini jenis sistem operasi yang akan digunakan yaitu menggunakan *raspbian Jessie* tahapnya yaitu :

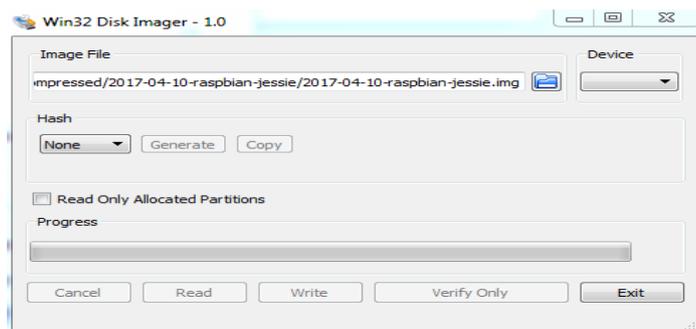
- a. Sebelum menginstall *raspbian* ke dalam *SDcard*, jalankan terlebih dahulu program *Win32DiskImager*.



Gambar 3.5 Tampilan Awal *Win32 Disk 2*.

- b. Selanjutnya, masukkan *SDcard* ke laptop *card reader* sampai *SDcard* sudah terdeteksi oleh laptop.

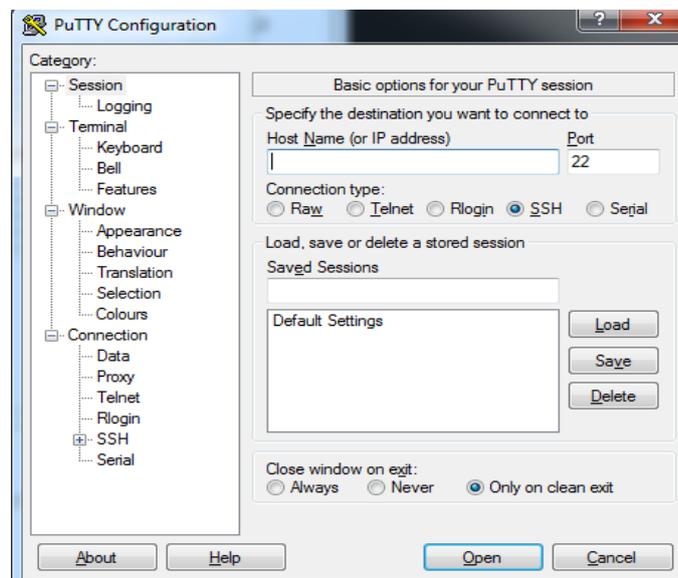
Setelah itu, pilih *Device* pada *Win32Disk Imager* dengan *drive letter* *SDcard*nya dan sorot *Image File* dengan *Image Raspbian* yang dapat di *download* gratis di website <http://www.raspberrypi.org/downloads/>.



Gambar 3.6 *Insert Raspbian OS image 3*.

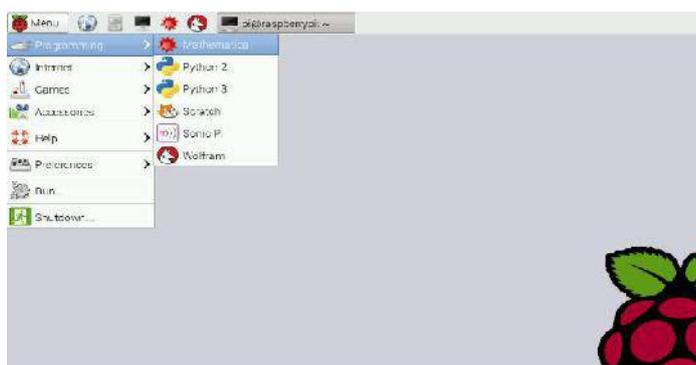
- c. Lalu, pilih *Write* dan tunggu hingga proses penulisan *file image Raspbian* selesai.
- d. Apabila proses pembuatan *OS Raspbian* selesai, maka pada *drive letter* *SDcard* akan seperti gambar 3.7.

- c. Setelah semuanya tersambung, jalankan *software Putty*, konfigurasi *IP Address*nya yaitu 192.168.43.5 kolom *port* tidak perlu diubah karena *default port remote connection* adalah 22. Lalu pilih *Open*.



Gambar 3.8 Pengaturan pada *Putty 2*.

- d. Tampilan berikut pada *Putty* adalah masukan *user* dan *password default user* dan *password* adalah *user = pi*, *password = raspberry*.
- e. Apabila sudah berhasil *login*, maka artinya sudah sukses meremote *Raspberry Pi* melalui Laptop. Karena masih berbasis teks, untuk pindah ke basis *Graphical User Interface (GUI)* gunakan perintah *lxsession*.
- f. Jika berhasil maka akan muncul tampilan *GUI OS Raspbian*.



Gambar 3.9 Tampilan GUI OS Raspbian

3.4.5 Konfigurasi dan Instalasi Squid Kidsafe Proxy

Dengan dilakukannya *installasi* dan *konfigurasi* terhadap *raspberry pi* maka beralih pada *installasi* dan *konfigurasi Squid kidsafe proxy* itu sendiri dengan cara:

- a. Lakukan *update* dan *upgrade repository* operasi sistem serta *installasi* beberapa paket yang dibutuhkan dengan perintah berikut:

```
Apt-get install update  
  
Apt-get upgrade  
  
Apt-get install squid3  
  
Apt-get install lighttpd  
  
Apt-get install mysql-server  
  
Apt-get install php5-common php5-cgi php5 php5-mysql
```

- b. Setelah paket yang dibutuhkan terinstall maka download dan *ekstrak file* yang dibutuhkan yaitu *squidapp* dan *webapp* agar *kidsafe proxy* dapat dioperasikan dalam bentuk *web* nantinya. Dengan perintah berikut:

```
Wget http://www.penguintutor.com/software/squid-kidsafe/0.2.0/kidsafe-squidapp-0.2.0.tgz  
  
Wget http://www.penguintutor.com/software/squid-kidsafe/0.2.0/kidsafe-webapp-0.2.0.tgz  
  
Dan ekstrak dengan perintah:
```

Tar -xvzf kidsafe-squidapp-0.2.0.tgz kedalam folder /opt

Tar -xvzf kidsafe-webapp-0.2.0.tgz kedalam folder /var/www

3.4.6 Pengujian yang dilakukan terhadap *kidsafe proxy*

Pengujian yang dilakukan yaitu dengan melihat apakah sistem mampu memfilter hak akses terhadap suatu *website* sesuai dengan kategori yang ada baik untuk anak-anak, remaja, dan dewasa dengan berupa tabel seperti berikut:

Tabel 3.3 Contoh Presentasi Pengujian

No	Alamat website	Kategori					
		<i>Child</i>		<i>Teen</i>		<i>Adult</i>	
		Akses	Block	Akses	Block	Akses	Block
1	www.learninggamesforkids.com/						
2	www.Kid.nationalgeographic.com						
3	www.funbarin.com						
4	www.starfall.com						

5	www.nick-asia.com						
6	www.facebook.com						
7	www.youtube.com						
8	www.detik.com						
9	www.instagram.com						
10	www.google.com						

Untuk pengujian lainnya nanti menggunakan *wireshark* dalam memantau lalulintas akses *website* dan menampilkan hasil dari pengujian *kidsafe* itu sendiri.

BAB IV

HASIL DAN PEMBAHASAN

4.1 Kebutuhan *Spesifikasi Hardware dan Software*

Sebagaimana dalam mendukung keberlangsungan penelitian ini agar penelitian ini berjalan dengan baik maka dibutuhkan beberapa perangkat keras dan lunak.

a. Kebutuhan *Hardware*

Hardware yang dibutuhkan untuk mendukung penelitian analisis keamanan jaringan sistem *filtering* dengan *kidsafe proxy* menggunakan raspberry pi dapat di lihat dengan tabel sebagai berikut:

Tabel 4.1 Komponen Perangkat Keras

NO	Perangkat Keras	Keterangan	Jumlah
1	Raspberry pi 3 Model B	SoC: Broadcom BCM2837 CPU: 4x ARM Cortex- A53, 1.2GHz GPU: Broadcom VideoCore IV RAM: 1GB LPDDR2 (900 MHz) Networking: 10/100 Ethernet, 2.4GHz 802.11n wireless Bluetooth: Bluetooth 4.1	1 unit

		<p>Classic, Bluetooth Low Energy</p> <p>Storage: microSD</p> <p>GPIO: 40-pin header, populated</p> <p>Ports: HDMI, 3.5mm analogue audio-video jack, 4x USB 2.0, Ethernet, Camera Serial Interface (CSI), Display Serial Interface (DSI)</p>	
2	Laptop	<p>Intel Celeron B877</p> <p>Ram 4Gb</p> <p>HDD 320 Gb</p> <p>Client 3:</p> <p>Processor AMD A6-6310</p> <p>Ram 2 Gb</p> <p>HDD 500 Gb</p>	1 unit
3	Cable UTP dan RJ45	Cable UTP Cat 5	<p>1 Meter Cable</p> <p>2 RJ45</p>
4	1 paket Raspberry pi	<p>MicroSD Sandisk 16GB</p> <p>Adaptor</p> <p>Heatsink</p>	1 unit

b. *Kebutuhan Software*

Untuk mendukung penelitian analisis keamanan *FTP Server* dengan protokol SSL dari serangan *Brute Force* dibutuhkan beberapa perangkat lunak agar sistem bekerja dengan apa yang diinginkan, adapun perangkat lunak yang dibutuhkan dapat dilihat dengan tabel berikut:

Tabel 4.2 Komponen Perangkat Lunak

NO	Perangkat Lunak	Keterangan
1	Sistem Operasi	Raspbian Jessie dipergunakan untuk sistem operasi dari raspberry pi
2	<i>Squid3</i>	Dipergunakan untuk <i>Web Proxy</i>
4	AngryIP	<i>Tool</i> untuk mencari alamat IP <i>default</i> raspberry pi
5	Putty	<i>Tool</i> untuk <i>monitoring</i> raspberry pi melalui ssh
6	<i>VNC Viewer</i>	<i>Tool</i> untuk <i>monitoring</i>

		raspberry pi dalam bentuk <i>Graphic User Interface</i> (GUI)
7	Kidsafe	Tool basis web yang bekerja dengan squid untuk <i>filtering</i>
8	Phpmyadmin	Tool dalam mempermudah admin dalam mengelola <i>database</i>
9	<i>MySql</i>	<i>Tool</i> penyedia layanan database
9	Mozilla	<i>Tool web browser</i> untuk mengakses <i>website</i>

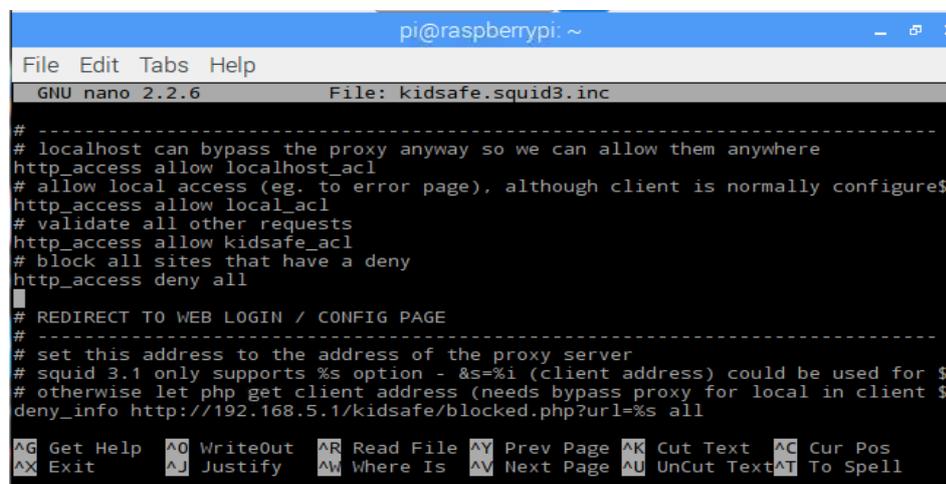
4.2 Pengujian dan Pembahasan

Dalam hal ini sistem yang telah dibahas dan diterapkan dengan cara sistem dioperasikan dan melakukan pengujian untuk melihat hingga sampai mana sistem yang dibangun dapat berjalan dengan baik, kemudian dianalisa agar sesuai dari apa yang ada pada rumusan masalah dan tujuannya.

4.4.1 Pembahasan

Pada bagian sebelumnya dapat dibahas mengenai penerapan dari keamanan jaringan sistem *filtering* dengan *kidsafe proxy*. Kemudian dalam pembahasan ini akan dibahas mengenai bagian-bagian dari *filtering kidsafe proxy*.

Untuk bagian pengkodean dari *kidsafe* sendiri yaitu ada pada direktori `/opt/kidsafe/kidsafe.squid3.inc` yang berisikan seperti berikut:



```

pi@raspberrypi: ~
File Edit Tabs Help
GNU nano 2.2.6 File: kidsafe.squid3.inc
# -----
# localhost can bypass the proxy anyway so we can allow them anywhere
http_access allow localhost_acl
# allow local access (eg. to error page), although client is normally configured
http_access allow local_acl
# validate all other requests
http_access allow kidsafe_acl
# block all sites that have a deny
http_access deny all
#
# REDIRECT TO WEB LOGIN / CONFIG PAGE
# -----
# set this address to the address of the proxy server
# squid 3.1 only supports %s option - %s=%i (client address) could be used for %s
# otherwise let php get client address (needs bypass proxy for local in client %s)
deny_info http://192.168.5.1/kidsafe/blocked.php?url=%s all
AG Get Help  AO WriteOut  AR Read File  AY Prev Page  AK Cut Text  AC Cur Pos
AX Exit      AJ Justify   AW Where Is AV Next Page  AU UnCut Text AT To Spell

```

Gambar 4.1 isi dari file *kidsafe.squid3.inc*

Pada gambar 4.1 menunjukkan isi dari file penghubung antara *kidsafe* dengan *squid proxy*, file *kidsafe.squid3.inc* berisikan rules akses dari *kidsafe* itu sendiri untuk baris ACL `local_ACL` dst dan `localhost_ACL` ini menunjukkan agar ACL diizinkan akses melalui alamat `192.168.5.1/24` dan jaringan local `127.0.0.1/32::1`. Kemudian pada baris dengan perintah `http_access deny all` ini bekerja untuk memblok seluruh akses yang diminta dan untuk baris dengan perintah `deny info http://192.168.5.1/kidsafe/blocked.php`? Menunjukkan bahwa pengarahannya akses yang diblok diarahkan pada *website admin*.

Kemudian untuk menghubungkan *kidsafe* dengan *squid proxy* yaitu mengikut sertakan *file kidsafe.squid3.inc* yang ada pada folder *kidsafe* kedalam file *squid* dengan mengedit *file squid* itu sendiri yang ada pada */etc/squid3/squid.conf* seperti berikut:

```
# TAG: url_rewrite_concurrency
#   Remove this line. Set the 'concurrency=' option of url_rewrite_children$
#Default:
# none
include /opt/kidsafe/kidsafe.squid3.inc
# TAG: dns_testnames
#   Remove this line. DNS is no longer tested on startup.
#Default:
# none
```

Gambar 4.2 isi *file squid.conf*

Pada gambar 4.2 dapat dilihat bahwa ada penambahan perintah didalam *file squid.conf* dengan menambahkan perintah *include /opt/kidsafe/kidsafe.squid3.inc* dimana nantinya *squid* akan mengikutsertakan *kidsafe* dalam melakoni *squid proxy* itu sendiri.

Kemudian mengenal cara kerja dari *rules* yang ada pada *kidsafe* yaitu dapat dilihat dengan membuka *file kidsafe.rules* didalam folder *kidsafe rule* yang telah dibuat dapat dilihat seperti berikut:

```

pi@raspberrypi: ~
File Edit Tabs Help
GNU nano 2.2.6 File: kidsafe.rules
# This is a system generated file
# Do not edit it manually - instead use the PHP web page to configure the rules
# See http://www.penguintutor.com/kidsafe for more information
* 2 9 9+ 0 0
www.kids.nationalgeographic.com 3 9 1+ 1563817361 1
www.brainly.co.id 4 9 1+ 1563817379 1
www.brainly.co.id 5 9 1+ 1563817396 1
www.komik.pendidikan.id 6 9 1+ 1563813815 1
www.starfall.com 7 9 1+ 1563813846 1
www.nick-asia.com 8 9 1+ 1563813859 1
www.facebook.com 9 9 5+ 1563813883 1
www.youtube.com 10 9 5+ 1563817498 1
www.hidayatullah.com 11 9 5+ 1563810922 1
www.instagram.com 12 9 8+ 0 1
www.twitter.com 13 9 8+ 0 1
* 1 0 * 0 1
[ Read 16 lines ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell

```

Gambar 4.3 isi dari *rule kidsafe*

Pada gambar 4.3 dapat dipelajari bahwa terdapat komponen-komponen yang ada pada *rule kidsafe* itu sendiri yang dapat dijelaskan seperti berikut:

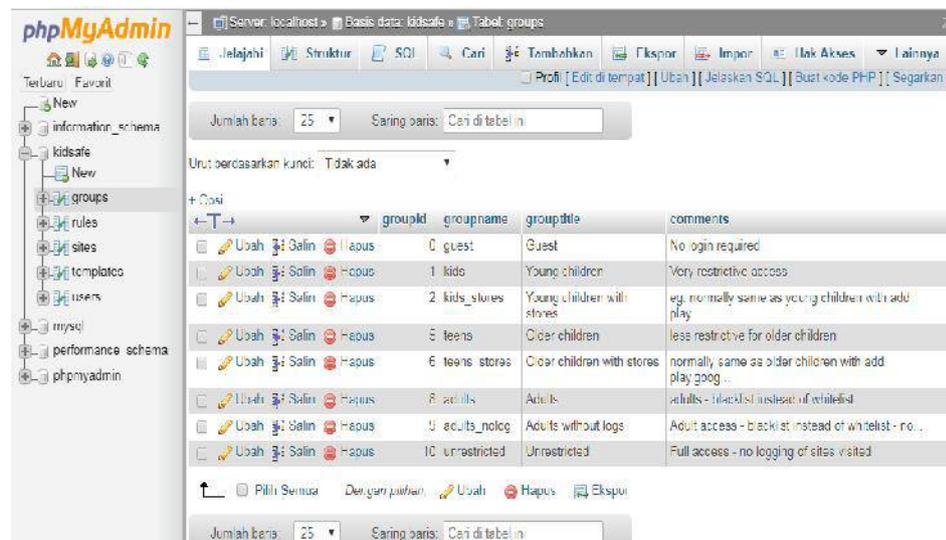
Contoh komponen yaitu : * 2 9 9+ 0 0

- Untuk komponen * berfungsi untuk menunjukkan alamat *website*.
- Untuk komponen 2 merupakan *ID Rule* yang menunjukkan identitas dari nomor urut *rule*.
- Untuk komponen 9 merupakan permission yang menunjukkan perintah untuk mengizinkan atau tidaknya suatu *website* untuk diakses, defaultnya 0 untuk deny dan 9 untuk allow.
- Untuk komponen 9+ berfungsi untuk mewakili level dari penggunaan dalam sistem yang secara *defaultnya* dengan nilai 0 untuk guest, 1+ untuk child, 5+ untuk teen, 9+ untuk adult, dan 10 untuk *owner*

- Untuk komponen 0 berfungsi sebagai *template* yang secara *default* bernilai 0.
- Untuk komponen 0 dapat disebut *log* yang berisikan nilai *default* yang ada 0 untuk *no logging*, 1 untuk *critical only*, 2 untuk *significant (warning)*, 3 untuk *disable all logging of accepts/deny*, 4 untuk *log entries where log=yes is set on rule*, 5 untuk *includes denies*, 6 untuk *include accept*, 7 untuk *include sessions tests*, 8 untuk *detailed session log*, 9 untuk *debug*, dan 10 untuk *full debug*.

Kemudian untuk komponen *rule* yang telah ada atau yang telah ditambahkan dapat dilakukan perubahan baik itu ditambah dan dikurangi namun hal ini dapat mempengaruhi kinerja dari *kidsafe* hingga *database* tidak dapat *sinkron* dengan *rule* yang ada pada *file kidsafe.rules*.

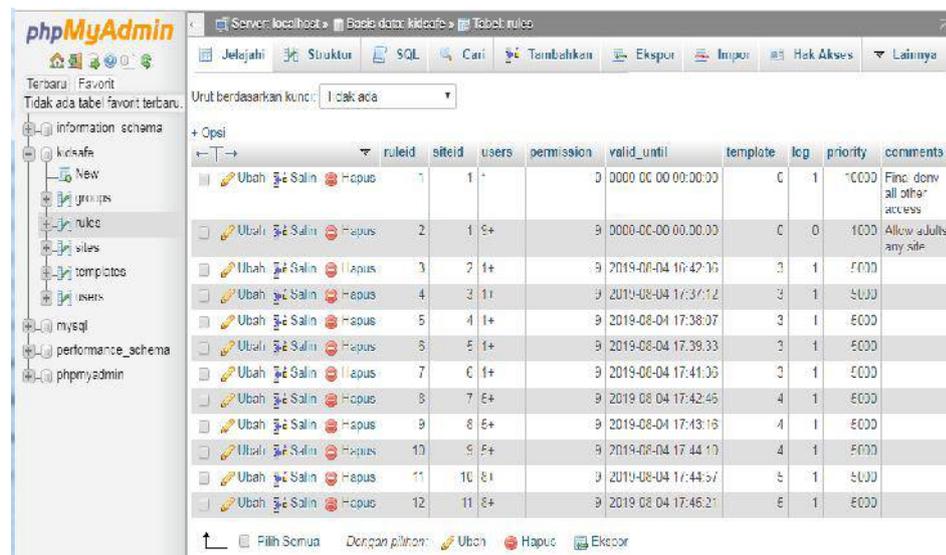
Kemudian pada *website kidsafe* yang disediakan oleh pengembang *kidsafe* tentu membutuhkan *database* untuk menyimpan perintah dan data lainnya dan agar *website* dapat bekerja dengan lancar untuk melihat bagaimana isi dari *database kidsafe* yang terhubung pada *website kidsafe* itu sendiri terdapat beberapa *table* yang ada didalam *database kidsafe* yaitu *table groups*, *table rules*, *table sites*, *table templates*, *table users*. Dapat ditampilkan seperti berikut:



groupid	groupname	groupitle	comments
0	guest	Guest	No login required
1	kids	Young children	Very restrictive access
2	kids_stores	Young children with stores	eg. normally same as young children with add play
3	teens	Older children	less restrictive for older children
4	teens_stores	Older children with stores	normally, same as older children with add play goog...
5	adults	Adults	adults - blacklist instead of whitelist
6	adults_nolog	Adults without logs	Adult access - blacklist instead of whitelist - no...
7	unrestricted	Unrestricted	Full access - no logging of sites visited

Gambar 4.4 Tampilan *table groups*

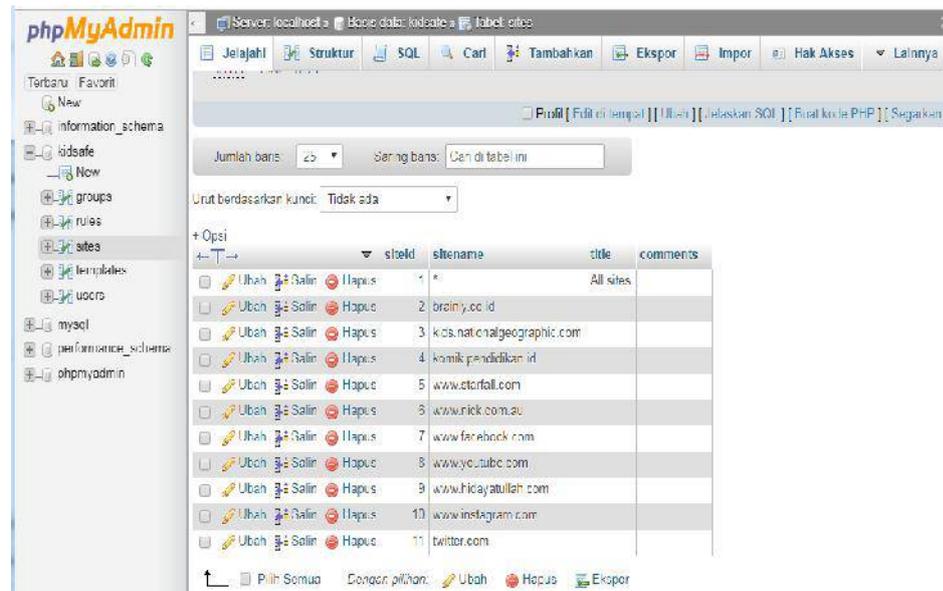
Pada gambar 4.4 menunjukkan kolom yang ada pada *table groups* yang fungsinya nantinya *table* ini terhubung pada menu pemilihan hak akses sesuai dari aturan yang admin berikan apakah pengguna itu *kids* (anak), *teen* (remaja), *adult* (dewasa) dan lainnya.



ruleid	siteid	users	permission	valid_until	template	log	priority	comments
1	1	*		0 0000-00-00 00:00:00	0	1	1000	Find domw all other access
2	1	9+		9 0000-00-00 00:00:00	0	0	1000	Allow adults any site
3	2	1+		9 2019-08-04 16:42:35	3	1	5000	
4	3	1+		9 2019-08-04 17:37:12	3	1	5000	
5	4	1+		9 2019-08-04 17:38:07	3	1	5000	
6	5	1+		9 2019-08-04 17:39:33	3	1	5000	
7	6	1+		9 2019-08-04 17:41:05	3	1	5000	
8	7	1+		9 2019-08-04 17:42:45	4	1	5000	
9	8	1+		9 2019-08-04 17:43:18	4	1	5000	
10	9	1+		9 2019-08-04 17:44:10	4	1	5000	
11	10	1+		9 2019-08-04 17:44:57	5	1	5000	
12	11	1+		9 2019-08-04 17:46:21	6	1	5000	

Gambar 4.5 Tampilan *Table rules*

Pada gambar 4.5 dapat diketahui bahwa terdapat *table rules* yang mana isinya berupa kode yang terhubung pada *groups* yang disesuaikan dengan alamat *website* yang telah di tambahkan untuk tiap-tiap *group*, sesuai dari yang telah dijelaskan diatas bagaimana membaca *rules* pada *kidsafe*.



sited	sitemame	title	comments
1	*	All sites	
2	brainy.co.id		
3	kids.nationalgeographic.com		
4	komik.pendidikan.id		
5	www.stcfull.com		
6	www.nick.com.au		
7	www.facebook.com		
8	www.youtube.com		
9	www.hidayatullah.com		
10	www.instagram.com		
11	twitter.com		

Gambar 4.6 Tampilan *Table Sites*

Pada tampilan 4.6 berisikan dari alamat *domain* yang telah ditetapkan oleh *admin* bahwa terdapat 10 *website* yang hanya bisa diakses oleh pengguna dari *kidsafe* itu sendiri.

templateid	templatename	description	users	permission
1	allow-everyone	Allow all users including guests	*	9
2	deny-everyone	Deny all users	*	0
3	allow-kids	Allow all logged in users (kids upwards)	1+	9
4	allow-teens	Allow teens upwards	13+	9
5	allow-adults	Allow only adults	18+	9
6	allow-stores	Stores - adults allowed, kids / teens need approval	2,5,8+	0
7	deny-kids	Deny kids / guests - including store level	3	0
8	deny-teens	Deny teens / less - including store level	13-	0
9	deny-guests	Deny not logged in	0	0
10	deny-store	Deny children not logged in as store level and guests	0,1,3,4,6,7	0

Gambar 4.7 Tampilan *Table Templates*

Pada tampilan 4.7 dapat dijelaskan bahwa terdapat beberapa kolom yang menunjukkan hak akses *user* dalam mengakses sebuah *website* yang telah ditetapkan *admin*, apakah *user* tersebut dapat mengakses *website* tersebut atau tidak, contoh baik itu seluruh anak-anak diizinkan mengakses atau seluruh anak-anak tidak diizinkan untuk mengakses.

Menampilkan baris 0 - 3 (total 4). Pencarian dilakukan dalam 0.0003 detik.

SELECT * FROM `users`

Jumlah baris: 25 | Sering baris: Cari di tabel ini

Urut berdasarkan kunci: Tidak ada

	user_id	username	accesslevel	fullname	password	status	loginexpiry	supervisor	admin
Ubah	1	admin	10	Admin user	bf6273e3611d53fe30a1asab7a01ec	1	0	1	1
Ubah	2	child	1	Child user	1b7d97200030a020a070000fe06e4f5	1	3600	0	0
Ubah	3	teen	6	Teenager	6a3a6f633217afa9373d906e2a9a00	1	3600	0	0
Ubah	4	adult	9	Adult user	b0374900ce1448024adfe0ea0c194aa	1	3600	1	0

Pilih Semua | Sembunyikan | Usah | Hapus | Ekspor

Jumlah baris: 25 | Sering baris: Cari di tabel ini

Operasi hasil kueri

Gambar 4.8 Tampilan *Table Users*

Pada tampilan 4.8 dapat dijelaskan bahwa terdapat beberapa kolom yang menunjukkan beberapa *user* lengkap dengan *user* dan *password* dari tiap-tiap penggunaannya. Penyimpanan dari akun ini yang nantinya dipergunakan pengguna untuk dapat *login* atau masuk hingga dapat mengakses *website* yang telah ditentukan.

4.4.2 Pengujian dan Analisa

Setelah dilaluinya proses penerapan dan pembahasan yang telah dilakukan kemudian menghasilkan beberapa *user* yang ada pada *kidsafe* dengan *level user* yang berbeda-beda untuk antarmuka dari *user admin* sendiri memiliki hak akses penuh sehingga tampilan antarmuka dari *admin* berbeda dengan *user* dimana *admin* memiliki otoritas tinggi dalam mengelola *user* dan *rule*, kemudian untuk kinerja

dari sistem *kidsafe filter* ini bergantung pada *database* agar *rule website* yang ditambahkan dapat dipergunakan, untuk menambah *rule* seperti berikut:



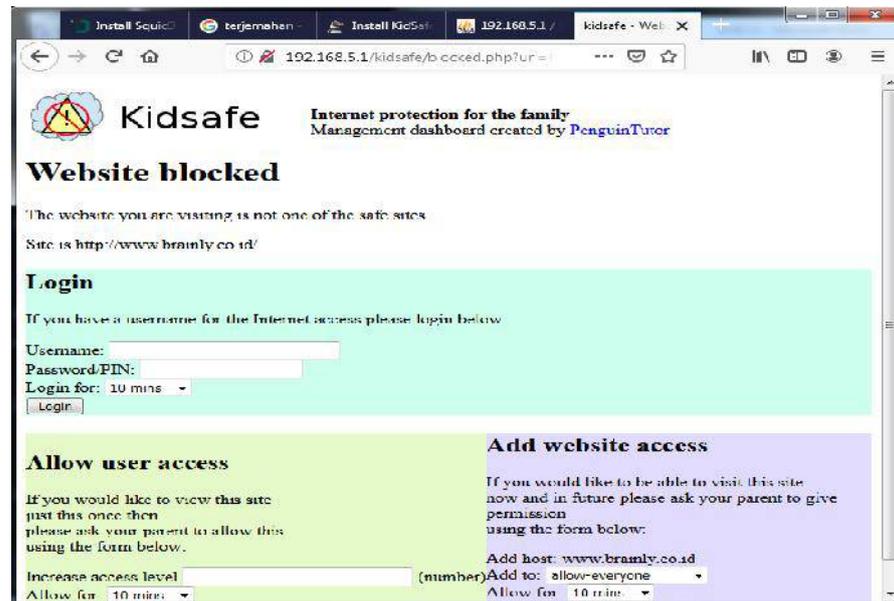
The screenshot shows the Kidsafe management dashboard. At the top right, it says "Welcome: admin - [Manage account](#) - [Logout](#)". The Kidsafe logo is on the left, with the text "Internet protection for the family" and "Management dashboard created by [PenguinTutor](#)". Below the logo is a navigation menu with "Home", "Rules", "Users", and "Log viewer". The main heading is "Add new rule to kidsafe". The form includes the following fields: "Add host:" with a text input; "Add to:" with a dropdown menu set to "allow-everyone"; "or:" with a text input and the note "(only if 'Add individual group' selected)"; "Allow for:" with a dropdown menu set to "10 mins"; and "Comments:" with a text input. At the bottom of the form is an "Add rule" button.

Gambar 4.9 antarmuka menambahkan *rule situs*

Pada gambar 4.9 menunjukkan antarmuka dari menu *Rules* untuk menambahkan *rules website* agar *website* tersebut dapat diakses oleh *user* yang memperbolehkan si *user* untuk mengaksesnya.

Analisis keamana jaringan *sistem filtering* dengan *kidsafe proxy* dilakukan beberapa pengujian dengan menggunakan *tools* untuk mengujinya baik itu menggunakan *web browser* mozilla.

Kemudian untuk antarmuka yang ditampilkan bila *website* yang diakses *user child* tersebut diarahkan ke *website blokir* seperti berikut:



Gambar 4.10 tampilan antarmuka dari *website blokir*

Gambar 4.10 menampilkan *website blokir* yang disediakan *server* untuk *user* melakukan pengaksesan *website* yang memang bukan *rule* untuk *user* itu sendiri. Dimana *user* yang *login* kedalam *kidsafe* itu sendiri *user child* (anak) kemudian *user* ingin mengakses *website youtube.com rules* yang diperuntukkan *teen* (remaja) atau *adult* (dewasa).

Kemudian pengujian yang telah dilakukan yaitu membuktikan apakah sistem dari *kidasfe proxy* dapat mampu melakukan pembatasan hak akses terhadap *website* sesuai dengan *rules* yang telah ada maka pengujian tersebut dapat dilihat pada table berikut:

Tabel 4.3 Presentasi Pengujian

No	Alamat <i>website</i>	Kategori					
		<i>Child</i>		<i>Teen</i>		<i>Adult</i>	
		Akses	Block	Akses	Block	Akses	Block
1	www.kids.nationalgeographic.com	Akses		Akses		Akses	
2	www.brainly.co.id	Akses		Akses		Akses	
3	www.komik.pendidikan.id	Akses		Akses		Akses	
4	www.starfall.com	Akses		Akses		Akses	
5	www.nick-asia.com	Akses		Akses		Akses	
6	www.facebook.com		Block	Akses		Akses	
7	www.youtube.com		Block	Akses		Akses	
8	www.hidayatullah.com		Block	Akses		Akses	

9	www.instagram.com		Block		Block	Akses	
10	www.twitter.com		Block		Block	Akses	

Tabel 4.3 menampilkan 10 *website* dengan alamat *website* yang berbeda-beda menunjukkan bahwa sistem dapat melakukan batas akses bagi *user* sesuai dengan *rule* yang ada dengan keterangan bahwa *user child* (anak) dapat mengakses *website* deri nomor 1 hingga 5 dimana memang *website* tersebut diperuntukkan untuk *user child* dari kelima *website* tersebut memang masih aman untuk diakses bagi anak-anak, kemudian pada nomor 6 sampai 8 diperuntukkan bagi *user Teen* (remaja) dalam mengaksesnya dan nomor 8,9 diperuntukkan bagi *user adult* (dewasa). Dari tabel pun dapat dilihat bahwa pengujian menunjukkan bahwa *user* yang tidak terkena oleh hak akses *blok website* yaitu *user adult* (dewasa) saja dikarenakan komponen yang digunakan oleh *user adult* (dewasa) komponen yang dapat mengakses segala *website*, berbeda dengan *user child* (anak) yang dibatasi hak aksesnya dalam mengakses sebuah *website*.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan pembahasan yang telah dibahas dalam penelitian tersebut, maka penulis mengambil kesimpulan sebagai berikut :

1. Internet sangat berdampak bagi pengguna, baik berdampak *positif* maupun *negatif*. Tetapi banyak masyarakat yang salah menggunakan internet sehingga banyak menimbulkan dampak *negatif* terutama pada anak-anak. Untuk mengurangi dampak tersebut maka perlu membangun sebuah pengamanan hak akses, yaitu dengan membuat suatu *proxy kidsafe* menggunakan *raspberry pi*. Dimana dengan *kidsafe proxy*, *admin* bisa membagi hak akses *website* yang bisa dikunjungi oleh setiap pengguna.
2. Untuk membangun suatu keamanan jaringan pembatasan hak akses dengan *kidsafe proxy*, perlu membuat suatu *database login* yang dapat membagi hak akses. Dalam penelitian ini menggunakan beberapa perangkat lunak dan perangkat keras yang dapat mendukung sistem, diantaranya adalah *raspberry pi3 Model B*, Laptop, *Cable UTP* dan *RJ45* selaku perangkat keras serta *Raspbian jessy* (sistem operasi), *Squid3* (*web proxy*), *wireshark* (*tool network analyzer*), *angry ip* (mencari alamat ip *raspberry*), *putty* (*monitoring raspberry* melalui *ssh*), *vnc viewer* (*monitoring* dalam bentuk *GUI*), *kidsafe* (*tool basis web* dengan *squid* untuk *filtering*), *phpmyadmin* (mempermudah *admin* mengelola *database*), *mysql* (*tool penyedia layanan*), dan *Mozilla* (*web browser* untuk pengaksesan *website*)

5.2 Saran

Berdasarkan kesimpulan di atas, dan juga sebagai pertimbangan bagi pembaca atau peneliti, penulis mempunyai beberapa saran-saran yang dapat dipertimbangkan, antara lain :

1. Penelitian ini hanya dilakukan pada jaringan lokal, selanjutnya bisa dikembangkan pada jaringan besar.
2. Diharapkan juga adanya pengembangan terhadap proxy kidsafe sehingga dapat mempermudah dalam pengamanan jaringan.

DAFTAR PUSTAKA

- Aprilianto, T., Samsul, A.(2018). Perancangan dan *implementasi hotspot* cerdas berbasis mikrotik *OS* dan *web server mini pc raspberry pi*. Jurnal sistem dan teknologi informasi. 4, No.2, 2018, pp.125-144.
- Carlo, J. R., Dian, W. C., Radius,T.(2015). *Implementasi kidsafe proxy* sebagai pembatas hak akses dan *filtering* menggunakan raspberry pi.
- Fachri, barany, agus perdana windarto, and ikhsan parinduri. "penerapan backpropagation dan analisis sensitivitas pada prediksi indikator terpenting perusahaan listrik." jepin (jurnal edukasi dan penelitian informatika) 5.2 (2019): 202-208.
- Fachri, b., windarto, a. P., & parinduri, i. (2019). Penerapan backpropagation dan analisis sensitivitas pada prediksi indikator terpenting perusahaan listrik. Jepin (jurnal edukasi dan penelitian informatika), 5(2), 202-208.
- Fachri, barany; windarto, agus perdana; parinduri, ikhsan. Penerapan backpropagation dan analisis sensitivitas pada prediksi indikator terpenting perusahaan listrik. Jepin (jurnal edukasi dan penelitian informatika), 2019, 5.2: 202-208.
- Hamdi, nurul. "model penyiraman otomatis pada tanaman cabe rawit berbasis programmable logic control." jurnal ilmiah core it: community research information technology 7.2 (2019).
- Iswandi, E.(2015). Sistem penunjang keputusan untuk menentukan penerimaan dana santunan sosial anak nagari dan penyalurannya bagi mahasiswa dan pelajar kurang mampu di Kenagarian Barung-Barung Balantai Timur. 3, No.2.
- Khuluq, H., Makinun, A., Mohamad, H., Muhammad, A. E.(2016). *Implementasi VOIP (Voice Over Internet Protocol) server* berbasis *raspberry pi* sebagai media komunikasi. Jurnal ilmiah *edutic*. 3,No.1.
- Maria, W. H. B., Arie, S. M. L., Anneke, W.(2015).Perancangan aplikasi *sms gateway* untuk pembuatan kartu perpustakaan di Fakultas Teknik Unsrat.Jurnal teknik elektro dan komputer.
- Permana, aminuddin indra. "kombinasi algoritma kriptografi one time pad dengan generate random keys dan vigenere cipher dengan kunci em2b." (2019).

- Putra, randi rian. "sistem informasi web pariwisata hutan mangrove di kelurahan belawan sicanang kecamatan medan belawan sebagai media promosi." jurnal ilmiah core it: community research information technology 7.2 (2019).
- Putra, randi rian, et al. "decision support system in selecting additional employees using multi-factor evaluation process method." (2019).
- Putra, randi rian. "implementasi metode backpropagation jaringan saraf tiruan dalam memprediksi pola pengunjung terhadap transaksi." jurti (jurnal teknologi informasi) 3.1 (2019): 16-20.
- Putra, E., Ariffin.(2018). *Web proxy server linux* debian 8 jessie untuk blokir situs pada SMK Al-Washliyah pasar senen Kota Medan Provinsi Sumatra Utara. Jurnal ilmiah *Core IT*. E-issn : 2548-3528.
- Saputra, muhammad juanda, and nurul hamdi. "rancang bangun aplikasi sejarah kebudayaan aceh berbasis android studi kasus dinas kebudayaan dan pariwisata aceh." journal of informatics and computer science 5.2 (2019): 147-157
- Sidik, a. P., efendi, s., & suherman, s. (2019, june). Improving one-time pad algorithm on shamir's three-pass protocol scheme by using rsa and elgamal algorithms. In journal of physics: conference series (vol. 1235, no. 1, p. 012007). Iop publishing.
- Sitepu, n. B., zarlis, m., efendi, s., & dhany, h. W. (2019, august). Analysis of decision tree and smooth support vector machine methods on data mining. In journal of physics: conference series (vol. 1255, no. 1, p. 012067). Iop publishing.
- Sutarti, Khairunnisa.(2017). Perancangan dan analisis keamanan jaringan *nirkabel* dari serangan *DDOS (Distributed Denial Of Service)* berbasis *Honeypot*. Jurnal prosisko. 4, N0.2.
- Tasril, v., wijaya, r. F., & widya, r. (2019). Aplikasi pintar belajar bimbingan dan konseling untuk siswa sma berbasis macromedia flash. Jurnal informasi komputer logika, 1(3).
- Utama, S.(2020). Analisis keamanan jaringan sistem *filtering* dengan *kidsafe proxy* menggunakan raspberry pi.
- Yuisar, Liza,Y., Yanolanda, Suzantry, H.(2015). Analisa pemanfaatan *proxy server* sebagai media *filtering* dan *caching* pada jaringan komputer.Jurnal media infotama. 11, No.1.