BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi sampai saat ini terus berkembang. Perkembangan tersebut berdampak pada keamanan sistem yang ada didalamnya. Sehingga bagi pengguna aplikasi yang terhubung pada jaringan internet perlu lebih waspada terhadap penetrasi yang dilakukan oleh pihak lain yang tidak bertanggung jawab. Tidak sedikit pengguna jaringan (internet) yang telah menjadi korban penetrasi. Salah satu penetrasi yang berhasil dilakukan adalah penetrasi terhadap *website* resmi MUI yang berhasil diretas oleh hacker (Iqbal, 2012). Kewaspadaan ini tentunya tidak cukup hanya dilakukan oleh pengguna jaringan internet saja, melainkan juga perlu dilakukan bagi pengelola jaringan (Administrator Jaringan).

Keamanan jaringan komputer sebagai bagian dari sebuah sistem menjadi sangat penting untuk menjaga *validitas* dan *integritas* data serta menjamin ketersediaan layanan bagi penggunanya. Suatu serangan ke dalam server jaringan komputer dapat terjadi kapan saja. Baik pada saat administrator yang sedang bekerja ataupun tidak. Dengan demikian dibutuhkan sistem keamanan di dalam *server* itu sendiri yang mampu mendeteksi langsung

Amarudin (2018) mengatakan analisis keamanan jaringan merupakan salah satu hal terpenting dalam proses sebelum implementasi jaringan komputer, tidak sedikit jaringan komputer mengalami masalah yang disebabkan oleh kelalaian tersebut sehingga dapat membuka peluang bagi para *hacker* untuk meretas dan merusak jaringan yang akan dibangun Oleh sebab itu, keamanan jaringan saat ini menjadi isu yang sangat penting yang patut di perhitungkan sebagai elemen yang rentan akan penyerangan orang-orang yang tidak bertanggung jawab, selain menimbulkan banyak manfaat juga memiliki banyak sisi buruk Salah satunya adalah serangan terhadap sistem komputer yang terhubung ke internet Sebagai akibat dari serangan itu banyak sistem komputer atau jaringan yang terganggu bahkan menjadi rusak. Untuk menanggulangi hal tesebut, diperlukan sistem keamanan yang dapat menanggulangi dan mencegah kegiatan-kegiatan yang mungkin menyerang sistem jaringan kita.

Kantor Desa Mekar Sari merupakan salah satu dari tujuh desa yang ada pada Kecamatan Kalaena. Kantor Desa Mekar Sari itu sendiri memiliki tugas dalam melayani data kemasyarakatan sepertihalnya pengiriman data atau informasi, oleh karena itu dalam proses menerima dan mentransfer data yang bersifat rahasia pihak desa menggunakan fasilitas jaringan *Wi-Fi* (*Wireless Fidelity*) yang dapat dikoneksikan pada media elektronik sepertihalnya *handphone*, komputer dan laptop. Namun, kondisi saat ini di kantor desa Mekar Sari sudah memiliki akses jaringan tetapi tingkat keamanannya terhadap jaringan *wireless* masih kurang karena terdapat oknum atau warga yang tinggal disekitaran kantor menghack jaringan tersebut yang mengakibatkan koneksi yang lambat, maka dari itu penulis akan melakukan analisis sistem keamanan dengan konsep *Port Knocking* yang diterapkan pada *Mikrotik Router OS* yang dapat meminimalisir terjadinya penyalahgunaan akses router dari pihak yang tidak bertanggung jawab.

Permasalahan yang timbul dalam menangani jaringan komputer di Kantor Desa Mekar Sari yaitu didalam pengaturan, penggunaan dan pemanfaatan fasilitas jaringan yang masih terdapat beberapa kelemahan. Kelemahan tersebut antara lain: 1) Penggunaan Proteksi satu *password* yang mudah dikenali dan tidak terautentifikasi secara benar. 2) Koneksi jaringan masih mudah diretes dan menimbulkan pengaksesan menjadi lambat karna *overload* pengguna. 3) pengguna jaringan bebas mengakses situs-situs negatif yang mengakibatkan tidak optimalnya penggunaan jaringan oleh pegawai. Sehingga admin kantor harus selalu mengganti *password wifi* tersebut dan masih awannya staff kantor yang kurang menguasai jaringan sehinggan internt mudah diakses oleh pihak luar.

Berdasarkan latar belakang diatas, maka penulis termotivasi untuk melakukan penelitian dengan mengangkat judul penelitian "Analisis Sistem Keamanan Jaringan Kantor Desa Mekar Sari Menggunakan Mikrotik Dikabupaten Luwu Timur". Sistem ini dibangun dengan tujuan menjaga keamanan data-data yang bersifat rahasia.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dipaparkan diatas, maka penulis dapat merumuskan permasalahan pada penelitian ini adalah Bagaimana

menganalisis sistem keamanan jaringan Kantor Desa Mekar Sari menggunakan Mikrotik Dikabupaten Luwu Timur?

1.3 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah untuk menganalisis sistem keamanan jaringan Kantor Desa Mekar Sari menggunakan Mikrotik Dikabupaten Luwu Timur

1.4 Manfaat Penelitian

Manfaat penelitian ini antara lain adalah:

1. Bagi Penulis

Meningkatkan wawasan dan kompetensi di dalam memahami tentang Analisis Keamanan Jaringan Menggunakan Mikrotik, yang nantinya penulis buat. Selain itu merupakan syarat untuk melakukan penyusunan tugas akhir pada Program Studi Teknik Informatika di Universitas Cokroaminoto Palopo.

2. Bagi Instansi

Dapat memberikan solusi dalam meningkatkan sistem keamanan jaringan dengan *mikrotik* agar lebih nyaman dan aman dalam penggunaan jaringan internet didalam lingkugan kantor desa bagi penggunanya.

3. Bagi Akademik

Sebagai bahan acuan dan referensi penelitian dalam upaya pengembangan dan peningkatan keamanan jaringan.

BAB II
KAJIAN TEORI

2.1 Kajian Teori

Kajian teori merupakan teori yang dikumpulkan oleh penulis dari berbagai sumber terkait dengan penelitian yang dilakukan oleh penulis, yang bertujuan untuk memberikan pemahaman tentang penelitian yang sedang dikerjakan oleh penulis.

1. Analisis

Menurut Kamus Besar Bahasa Indonesia (2008), analisis merupakan penguraian suatu pokok atas berbagai bagiannya dan penelaahan bagian itu sendiri serta hubungan antarbagian untuk memperoleh pengertian yang tepat dan pemahaman arti keseluruhan. Analisis juga merpakan penyelidikan terhadap suatu peristiwa (karangan, perbuatan, dan sebagainya) untuk mengetahui keadaan yang sebenarnya.

Menurut Rifki (2016), analisis adalah aktivitas yang memuat sejumlah kegiatan seperti mengurai, membedakan memilih sesuatu untuk digolongkan dan dikelompokkan kembali menurut kriteria tertentu kemudian dicari kaitannya dan ditafsirksn maknanya. Dalam pengertian lainnya, analisis adalah sikap atau perhatian terhadap sesuatu (benda, fakta, fenomena) sampai mampu menguraikan menjadi bagian-bagian, serta mengenal kaitan antarbagian tersebut dalam keseluruhan.

2. Keamanan Jaringan

Menurut Sadikin (2012), keamanan jaringan komputer adalah kumpulan piranti yang dirancang untuk melindungi data ketika *transmisi* terhadap ancaman pengaksesan, pengubahan dan penghalangan oleh pihak yang tidak berwenang. Perkembangan teknologi jaringan komputer menyebabkan terkaitnya satu komputer dengan komputer lainnya. Hal ini membuka peluang dalam pengembangan aplikasi komputer tetapi juga membuat peluang adanya ancaman terhadap pengubahan dan pencurian data. Sebuah aplikasi yang melintasi jaringan *public* seperti internet diansusmsikan dapat diakses oleh siapapun termasuk orang-orang atau pihak-pihak yang memang berniat untuk mencuri atau mengubah data. Oleh karena itu, untuk melindungi data terhadap akses, pengubahan dan

penghalangan yang tidak dilakukan oleh pihak yang berwenang, peranti keamanan data yang melintas di jaringan komputer harus disediakan.

Serangan pada sistem keamanan jaringan dapat dikategorikan menjadi dua jenis sebagai berikut:

a. Serangan Pasif

Pada serangan pasif, penyerang hanya mengumpulkan data yang melintas pada jaringan *public* (jaringan yang bisa diakses oleh penyerang). Serangan pasif tidak melakukan modifikasi data yang melintas atau merusak sistem, penyerang hanya punya kemampuan membaca saja (*read only).* Lalu berdasarkan data yang dikumpulkan, penyerang melakukan analisis untuk menggagalkan tujuan layanan keamanan jaringan. Oleh karena itu, penekanan untuk mengatasi serangan pasif lebih pada pecegahan dari pada pendeteksian. Berikut ini beberapa jenis serangan yang digolongkan sebagai serangan pasif :

1) *Snooping*
2) *Traficc Analysis*

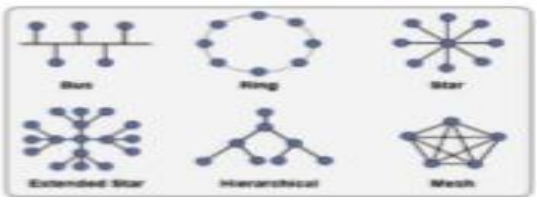
b. Serangan Aktif

Serangan aktif (*active attack*) dapat mengakibatkan perubahan data yang terkirim dan jalannya sistem terganggu. Pada serangan aktif seakan-akan penyerang memperoleh kemampuan untuk mengubah data pada lalu lintas data selain kemampuan baca. Jenis-jenis serangan aktif adalah sebagai berikut:

1) *Masquerade*
2) *Modification*
3) *Replay*
4) *Denial of Service*

3. Topologi Jaringan

Menurut Muhamad dan Hasan (2016), topologi jaringan komputer secara umum terbagi dalam 6 bentuk sebagai berikut.



Gambar 1. Topologi Jaringan (Sumber: Muhamad dan Hasan, 2016)

Masing-masing topologi diatas dijelaskan sebagai berikut:

a. Topologi *Bus*

Topologi Bus, adalah topologi jaringan yang menggunakan sebuah kabel utama sebagai tulang punggung (*backbone*). Keuntungan topologi ini adalah hemat kabel, layout kabel sederhana, serta mudah dikembangkan. Kerugiannya adalah *deteksi* dan *isolasi* kesalahan sangat kecil, padatnya lalu lintas atau bila salah satu *client* rusak maka jaringan tidak berfungsi, dan diperlukan *repeater* untuk menguatkan sinyal untuk jarak jauh.

b. Topologi *Ring*

Adalah topologi jaringan berupa lingkaran tertutup yang berisi node-node. Semua komputer tersambung membentuk lingkaran. Setiap simpul memiliki tingkat yang sama. Jaringan ini disebut *loop*. Data dikirim ke setiap simpul dan simpul memeriksa alamat informasi yang diterima, apakah untuknya atau tidak. Keuntungan topologi ini adalah pemeliharaan mudah, jarak jangkauan lebih luas daripada topologi bus, laju data (*transfer rate*) tinggi, dapat melayani lalu lintas data yang padat, tidak diperlukan pengendali pusat (*hub/switch*), dan komunikasi antar terminal yang mudah. Kerugiannya adalah penambahan/ pengurangan terminal sangat sulit, tidak kondusif untuk pengiriman suara dan gambar, dan kerusakan pada media pengirim akan menghentikan kerja seluruh jaringan.

c. Topologi *Star*

Adalah topologi jaringan yang menggunakan *concentrator* (*hub/switch*) untuk mengatur paket data. Topologi ini memiliki kontrol terpusat. Semua link harus melewati pusat yang menyalurkan data ke semua simpul (*client*). Simpul pusat disebut stasiun primer (*server),* simpul lain disebut stasiun sekunder (*client server).* Setelah hubungan dimulai oleh *server*, setiap *client server* dapat menggunakan jaringan tanpa menunggu perintah *server.* Topologi ini adalah paling fleksibel. Pemasangan/perubahan stasiun sangat mudah dan tidak mengganggu bagian jaringan lain. Juga memiliki kemudahan dalam pengelolaan jaringan. Kerugiannya antara lain adalah boros kabel, dan *hub/switch* menjadi suatu elemen yang kritis.

d. Topologi *Tree*

Adalah kombinasi/gabungan topologi *Bus* dan topologi *Star*. Dalam topologi ini tidak semua node memiliki kedudukan yang sama. Node berkedudukan tinggi menguasai node dibawahnya sehingga node terbawah sangat tergantung pada node diatasnya. Penerapan teknologi ini biasa digunakan pada infrastruktur jaringan *LAN* antar gedung.

e. Topologi *Mesh*

Adalah topologi jaringan yang semua komputernya saling terkoneksi satu sama lain. Penerapannya pada jaringan *WAN*.

f. Topologi *Wireless.*

Terdapat 2 jenis topologi jaringan *wireless*, yaitu *peer-to-peer* dan clientserver. Pada topologi *wireless peer-to-peer*, jaringan terhubung pada setiap komputer dalam jaringan dengan lebih mudah dan langsung. Sedangkan pada topologi *wireless client-server*, harus ada access point untuk memungkinkan komputer menerima/mengirim data.

4. Komponen Jaringan Komputer

a. *Wireless Router*

Menurut Madcoms (2015), pada dasanya *wireless router* berfungsi hampir sama seperti *wireless access point*, sebagai penghubung *wireless client*, hanya saja *wireless router* dilengkapi kemampuan untuk melakukan *routing*, sedangkan untuk *wireless access point* tidak memiliki kemampuan tersebut.

Wireless router adalah sebuah *device* yang berfungsi untuk meneruskan paket-paket dari sebuah *network* ke *network* yang lainnya sehingga *host* yang ada pada sebuah *network* bisa berkomunikasi dengan *host* yang ada pada *network* lain.

Gambar 2. Komponen *wireless router* (Sumber: Madcoms, 2015)

Wireless router memeiliki berbagai jenis koneksi internet yang berbeda-beda antara lain, koneksi internet melalui modem 3G biasanya *wireless router*

sudah suport dengann modem 3G GSM dan juga CDMA yang menggunakan port USB. Koneksi untuk menghubungkan ke modem ADSL. *Wireless router* jenis ini tidak bisa dipakai menggunakan modem 3G, hanya untuk modem ADSL. (Madco

b. *Switch*

Menurut Zaki (2010), *switch* adalah piranti jaringan yang digunaka untuk mengatur *bandwidth* dijaringan yang berukuran besar. Walaupun demikian karena harganya yang semakin murah, *switch* mulai digunakan pada jaringan rumahan dengan skala kecil. *Switch* lebih canggih dibandingkan dengan *hub* karena *switch* sering digunakan sebagai pengganti *hub*. *Switch* memiliki kemampuan dalam menggendalikan jumlah penguna *bandwidth* dijaringan.

Gambar 3. Komponen *Switch* (Sumber: Zaki, 2010)

Switch dapat mengontrol aliaran data menggunakan alamat MAC *address* yang diletakkan ditiap paket data. *Switch* membagi jaringan ke semua entitas yang disebut dengan *Virtual LAN (VLAN).*

5. *Mikrotik*

Menurut Madcoms (2014), mejelaskan bahwa, *MikroTik* pertama kali digagas pembuatnya pada tahun 1996 oleh John dan Arnis, kedua orang ini berasal dari Negara Moldova tepatnya kota Roga, sebuah negara pecahan Uni Sofiet, Kedua orang tersebut memulai sejarah *MikroTik* dengan membangun sebuah perangkat hasil dari perpaduan antara dua buah sistem operasi (*Linux* dan *DOS*) dan teknologi *wireless LAN* atau *WLAN Aeronet* yang memiliki kecepatan 2 Mbps. Gambar dari mikrotik dapat dilihat pada gambar 4.

Gambar 4. *Mikrotik* (Sumber Madcoms, 2014)

Berdasarkan jenisnya mikrotik dibagi menjadi 2 yaitu mikrotik *router OS* dan mikrotik *routerboard*, yang akan dijelaskan sebagai berikut.

a. Mikrotik OS

Mikrotik Router OS merupakan sistem operasi yang diperuntukkan sebagai *network router*. Mikrotik *Router OS* sendiri adalah sistem operasi dan perangkat lunak yang yang dapat digunakan untuk membuat komputer biasa menjadi *router network* yang handal, mencakup berbagai fitur yang dibuat untuk IP *network* dan jaringan *wireless*.

b. Mikrotik *RouterBoard*

Mikrotik *RouterBoard* adalah *router embedded* produk dari Mikrotik. *Router Board* seperti sebuah *PC* mini yang terintegrasi karena dalam suatu *board* tertanam proses, *RAM, ROM*, dan memori *flash*. *RouterBoard* menggunakan *OS Router OS* yang berfungi sebagai router jaringan, *bandwidth*, management, *proxy server*, *DHCP, DNS* server dan bisa juga berfungsi sebagai *hotspot server*.

6. *Cisco Packet Tracer*

Menurut Ahmad (2013), *Cisco Packet Tracer* adalah sebuah program *graphical network simulator* simulasi jaringan komputer berbasis *GUI* yang mirip dengan yang dapat mensimulasikn *topologi* yang lebih kompleks karena menggunakan *operating system* asli dari perangkat jaringan.

7. *Winbox*

Pamungkas (2016), mendefinisikan bahwa *Winbox* adalah sebuah *software* atau *utility* yang di gunakan untuk meremote sebuah *server MikroTik* ke dalam mode GUI (*Graphical User Interface*) melalui *operating system windows.*

Aplikasi *winbox* mempunyai sebuah kelebihan dapat digunakan malakukan konfigurasi IP *address* secara besar pada *PC* maupun pada *MikroTik* sendiri. *Winbox* dapat berjalan dengan mengandalakan MAC *address*, tentu hanya bisa dilakukan jika *PC* mengandalkan *winbox* terhubung satu dengan *router MikroTik.* Ini dapat memudahkan jika anda lupa akan IP *address* telah dikonfigurasi sebelumnya pada *router MikroTik.*

8. *Wireshark*

Menurut Suhervan (2014), *Wireshark* merupakan salah satu tools atau aplikasi *Network Analyzer* atau Penganalisa Jaringan. Penganalisaan Kinerja Jaringan itu dapat melingkupi berbagai hal, mulai dari proses menangkap paket-paket data atau informasi dalam jaringan, sampai pada digunakan pula untuk *sniffing* (memperoleh informasi penting seperti *password* email). *Wireshark* sendiri merupakan *free tools* untuk *Network Analyzer* yang ada saat ini. Dan tampilan dari *Wireshark* ini sendiri terbilang sangat bersahabat dengan *user* karena menggunakan tampilan grafis atau GUI (*Graphical User Interface*).

9. *Port Knocking*

a. Pengertian *Port Knocking*

Menurut Sel, Totakura, dan Carle (2016), menyatakan bahwa *port-knocking* adalah sebuah konsep menyembunyikan layanan jarak jauh di dalam sebuah *firewall* yang memungkinkan akses ke port tersebut hanya untuk mengetahui *service* setelah clien berhasil diautentikasi ke *firewall.* Hal ini dapat membantu untuk mencegah pemindai untuk mengetahui *service* apa saja yang saat ini tersedia di host dan juga berfungsi sebagai pertahanan terhadap serangan *zero-day*. *Port Knocking* adalah metode yang dilakukan untuk membuka akses ke port tertentu yang telah diblock oleh *Firewall* pada perangkat jaringan dengan cara mengirimkan paket atau koneksi tertentu. Koneksi bisa berupa protocol TCP, UDP maupuan ICMP. Jika koneksi yang dikirimkan oleh host tersebut sudah sesuai dengan *rule knocking* yang diterapkan, maka secara dinamis *firewall* akan memberikan akses ke port yang sudah diblock.

b. Konsep Penggunaan *Port Knocking*

Membuat rule *port knocking* yang hanya akan mengijinkan *user* mengakses *router* menggunakan *winbox* (tcp 8291) jika *user* tersebut sudah melakukan ping dan *telnet* ke ip *router.* Jika *user* belum melakukan ping lalu kemudian *telnet* ke ip *router*, maka *user* tersebut tidak akan bisa meremote *router* menggunakan *winbox*. Jadi kuncinya *user* harus ping dulu ke ip *router,* lalu setelah ping, kemudian akses ip router dengan *telnet* barulah user tersebut akan diijinkan oleh *firewall* router untuk mengakses *winbox.*

c. Cara Kerja *Port Knocking*

Memasukkan setiap ip *address user* yang melakukan ping dan *telnet* ke ip *router* ke dalam *address-list* setelah itu ip user akan diijinkan untuk mengakses *router* melalui aplikasi *winbox*. Perlu diketahui, rangkaian proses *knocking* harus sesuai dengan urutan *rule port knocking* yang dikonfigurasi jika proses *knocking* tidak sesuai urutan maka akan tetap diblock oleh *firewall* pada *router.*

10. *Research And Development* (RND)

Menurut Mahfud dan Eko Bagus dalam (Borg & Gall 1983), Riset dan pengembangan bidang pendidikan (*R & D*), adalah suatu proses yang digunakan untuk mengembangkan dan mengesahkan produk bidang pendidikan.

11. *Network Development Life Cycle* (NDLC)

Menurut Goldman dan Rawles (2004), Metode *Network Development Life Cycle (NDLC)* yaitu mendefinisikan siklus proses perancangan atau pengembangan suatu sistem jaringan komputer. *NDLC* mempunyai elemen yang mendefinisikan fase, tahapan, langkah atau mekanisme proses spesifik. *NDLC* dijadikan metode yang digunakan sebagai acuan (secara keseluruhan atau secara garis besar) pada proses pengembangan dan perancangan sistem jaringan komputer.

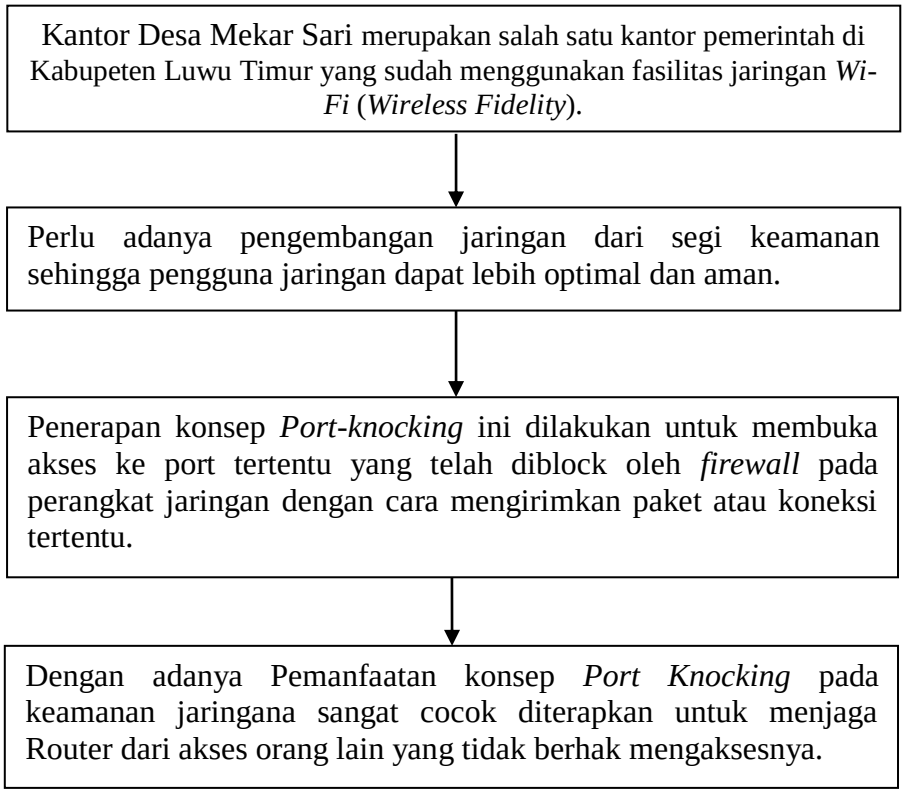
2.2 Hasil Penelitian yang Relavan

1. Arif Hidayat Dan Ismail Puji Saputra, 2018 Dengan Judul “Analisa Dan Problem Solving Keamanan Router Mikrotik Rb750ra Dan Rb750gr3 Dengan Metode *Penetration Testing*”. Hasil penelitian ini menunjukkan keamanan jaringan yang dimiliki oleh jaringan warnet Aulia.net masih memiliki banyak celah untuk dieksploitasi. Adapun hasil beberapa serangan menunjukkan hal yang serius dalam hal eksploitasi mikrotik seperti luaran mendapatakan *username* dan *password router mikrotik*. Hal ini sangat crusial dan berbahaya apabila juga terjadi pada jaringan instansi yang bersekala besar seperti perusahaan dan pendidikan. Penelitian ini juga memberikan solusi bagaimana agar *router mikrotik* terhindar dari jenis exploitasi tersebut.

2. Arandha Aryton Astari, 2018 Dengan Judul “Implementasi Keamanan Jaringan Dengan Metode *Firewall Filtering* Menggunakan Mikrotik”. Hasil penelitian yaitu Sistem diterapkan menggunakan Metode *firewall filtering* menggunakan *MikroTik* yang dihasilkan adalah link yang berbau fornografi atau media sosial berhasil di block dan link yang tidak berbau *fornografi* atau media sosial tidak di block dan berhasil masuk ke link yang dituju. Tabel pengujian menunjukkan bahwa *Mikrotik* behasil *block keyword* yang sudah ditentukan.
3. Ari Muzakir dan Maria Ulfa, 2019 Dengan judul “Analisis Kinerja Packet Filtering Berbasis Mikrotik Routerboard Pada Sistem Keamanan Jaringan”. Hasil penelitian ini adalah untuk mengetahui kemampuan *packet filtering* dalam melakukan bloking terhadap suatu situs web, kemudian hasilnya adalah metode ini dapat diterapkan untuk sistem keamanan jaringan. Dalam menganalisis *kinerja packet filtering* menggunakan *tool network packet anayzer wireshark* dengan cara melakukan capture paket yang lewat didalam jaringan dan menampilkan semua informasi secara detil dan dengan melakukan konfigurasi dan ujicoba sistem keamanan jaringan ini membuktikan bahwa kinerja dari *filtering rule* cukup baik dalam memblok akses web protocol http dan https.

2.3 Kerangka Pikir

Untuk lebih memperjelas permasalahan yang disajikan, maka berikut akan ditunjukkan kerangka pikir seperti pada gambar dibawah.



Gambar 5. Kerangka Pikir