BAB II
TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Penelitian terdahulu ini menjadi satu acuan penulis dalam membuat laporan akhir sehingga dapat memperkaya teori yang digunakan dalam mengkaji penelitian yang dilakukan. Berikut merupakan penelitian terdahulu berupa beberapa jurnal yang terkait dengan judul laporan akhir penulis.

Pada penelitian sebelumnya yang dilakukan (Jamaludin. 2016) dalam jurnal yang berjudul "**Teknik Keamanan Jaringan *Wireless* LAN Pada Warnet Salsabila *Computer***". Permasalahannya ialah jaringan *WiFi* memiliki kelemahan dibanding dengan jaringan kabel diantaranya menyangkut keamanan. Penanganan pada jaringan kabel hanya mencakup pada komputer yang terhubung dengan jaringan tersebut, beda dengan jaringan yang menggunakan teknologi *Wi-Fi* yang jangkauannya lebih luas dan bisa di *access* di mana saja yang memungkinkan orang untuk masuk atau memanfaatkan fasilitas *Wi-Fi* atau bahkan mengambil data-data kita untuk kepentingan tertentu. Oleh karena itu pengamanan pada jaringan yang menggunakan teknologi *Wi-Fi* harus lebih maksimal. Untuk mendapatkan jaringan *wireless* dengan keamanan sempurna, pencegahan tetap harus dilakukan ketika kita merancang jaringan *wireless*. Metode penelitian yang digunakan dalam penelitian ini adalah metode pengamanan *Wireless Access Point*, metode *Wired Equivalent Privacy (*WEP*),* dan metode *Media Access Control (*MAC*) Address*. Maka dapat diperoleh kesimpulan bahwa tingkat keamanan pada *wireless* LAN lebih tinggi dibanding dengan jaringan kabel LAN biasa di mana secara fisik adalah aman sementara jaringan *wireless* LAN tidak hanya bisa dibatasi oleh dinding di dalam gedung namun jaringan *wireless* bisa menembus dinding pembatas gedung dan untuk penanganan keamanan jaringan *wireless* di Salsabila Net menggunakan cara menyembunyikan SSID, memanfaatkan kunci WEP, WPA-PSK dan mengimplementasikan fasilitas MAC *Address*.

Pada penelitian sebelumnya yang dilakukan (Mochamad Gilang Hari Wibowo, Joko Triyono, Edhy Sutanta. 2017) dalam jurnal yg berjudul

"**KEAMANAN JARINGAN WLAN TERHADAP SERANGAN *WIRELESS HACKING* PADA DINAS KOMUNIKASI & INFORMATIKA DIY**". Permasalahannya ialah penggunaan media WLAN tersebut rentan terhadap ancaman serangan karena menggunakan gelombang radio. Penelitian ini dilakukan untuk memperoleh hasil pengujian keamanan jaringan *wireless* pada Dinas Kominfo DIY, sehingga bisa digunakan sebagai masukan bagi pengelola dalam rangka menjaga dan meningkatkan kualitas layanan koneksi jaringan WLAN yang disediakan. Metode penelitian yang dilakukan penulis yaitu menggunakan perangkat keras dan perangkat lunak pendukung yang digunakan sebagai sarana melakukan pengujian dan analisa dan *access point* atau *router* yang digunakan untuk mendapatkan informasi tentang jaringan WLAN, melakukan pengujian serangan ke jaringan WLAN dan konfigurasi keamanan jaringan WLAN. Kesimpulan yang dapat diambil dari penelitian ini yaitu keamanan jaringan WLAN di Dinas Kominfo DIY sudah aman, karena *access point* atau *router* jaringan WLAN yang tersedia sudah menerapkan sistem keamanan setingkat WPA/WPA2-PSK. Celah keamanan pada beberapa jaringan WLAN adalah pengguna yang sedang menggunakan jaringan WLAN masih bisa diserang oleh pengguna lain pada jaringan *wireless* yang sama. Untuk meningkatkan keamanan jaringan WLAN di Dinas Kominfo DIY perlu diaktifkan fitur ARP atau binding pada *access point* atau *router* agar terhindar dari serangan *spoofing* seperti nmap, *netcut*, dan lain-lain, sehingga pengguna menjadi aman dalam menggunakan jaringan WLAN tanpa diganggu oleh pengguna lainnya..

Pada penelitian sebelumnya yang dilakukan (Muhammad Ivan Susanto, Andi Hasad, M. Amin Bakri. 2019) dalam jurnal yg berjudul "**Sistem Proteksi Jaringan Wlan Terhadap Serangan *Wireless Hacking***". Permasalahannya ialah bagaimana melakukan pengujian keamanan jaringan *Wireless* pada CV Kernias Bekasi dan bagaimana meningkatkan keamanan jaringan WLAN agar terhindar dari serangan WPS aktif, *bypassing* MAC *Address*, ARP Spoofing dan Cracking. Tujuan dalam penelitian ini adalah mengetahui hasil pengujian keamanan jaringan *wireless* pada CV Kernias Bekasi dan mengetahui cara pencegahan serangan *wireless hacking* pada jaringan WLAN dan mengantisipasi serangan *wireless*

hacking pada keamanan jaringan WLAN di CV Kernias Bekasi dan penerapan pengaktifan fitur ARP atau binding pada *access point* atau *router* agar terhindar dari serangan WPS Aktif, *bypassing* MAC *Address*, ARP *Spoofing* dan *Cracking*. Hasil penelitian ini adalah memperoleh hasil implementasi pengujian keamanan jaringan *wireless* pada CV Kernias Bekasi, sehingga bisa dijadikan sebagai masukan bagi *staff* IT dalam rangka menjaga dan meningkatkan kualitas layanan koneksi jaringan.

Dari penelitian-penelitian terdahulu berupa beberapa jurnal yang terkait dengan judul laporan akhir penulis. Pada judul laporan akhir penulis disini melakukan *monitoring* terhadap *Wireless Hacking* agar mengetahui siapa saja yang *login* ke dalam jaringan seperti (Jamaludin. 2016). Akan tetapi, Penulis melakukan *monitoring* tersebut melalui *hotspot,* dengan dilakukannya *monitoring hotspot* dapat diketahui siapa saja yang masuk ke dalam jaringan yang sudah terbangun. Untuk keamanan *internet* penulis menggunakan *firewall* sistem pada mikrotik. Dengan terbangunnya keamanan *internet* menggunakan *firewall* yaitu melakukan *setting* pada *filter rules* dan NAT membantu pengguna untuk meminimalisir terjadinya serangan dari luar. Untuk melakukan pengujian ini penulis menggunakan aplikasi Technitium MAC *Address Changer* seperti pada penelitian (Muhammad Ivan Susanto, Andi Hasad, M. Amin Bakri. 2019) dan (Mochamad Gilang Hari Wibowo, Joko Triyono, Edhy Sutanta. 2017). Dengan Menggunakan aplikasi tersebut, dapat dengan mudah mengubah MAC *Address* agar bisa masuk ke jaringan WLAN. Untuk pengembangan baru yang akan dilakukan terkait laporan akhir penulis ialah penanganan serangan mac *clone* pada *hotspot* mikrotik. Dengan dilakukannya pemblokan pada MAC-*Address Cloning*, user *illegal* tidak dapat dengan mudah untuk mengambil alih hak akses pemilik user asli.

2.2 Jaringan Komputer

Jaringan komputer adalah sebuah sistem yang terdiri atas beberapa unit komputer yang didesain sedemikian rupa sebagaimana tujuan utamanya yakni untuk dapat berbagi sumber daya (CPU, *printer*, *scanner, plotter*, *hardisk*, dan

sebagainya), berkomunikasi (pesan instan, surel), dan dapat mengakses informasi (situs web). Menurut pembagiannya, jaringan komputer dapat dibedakan menjadi dua jenis, yakni jaringan terdistribusi dan jaringan tersentral (Madcoms, 2015:2).

2.3 *MAC-Clone (MAC Address Clone)*

Mac *Address (Media Access Control*) adalah sebuah alamat jaringan yang diimplementasikan dalam tujuh lapisan OSI yang mempresentasikan sebuah node tertentu dalam jaringan. Mac *Address* merupakan alamat yang unik yang memiliki panjang 48 bit, dimana 24 bit dibuat untuk siapa pembuat kartu tersebut sementara sisanya mempresentasikan nomor kartu tersebut. Karakteristik yang dimiliki Mac *Address* adalah kumpulan angka dan huruf unik yang terdiri dari 48 bit dimana setiap komputer atau PC memiliki Mac *Address* yang berbeda beda. Ciri fisik tersebut sengaja dibedakan untuk membedakan masing-masing komputer yang satu dengan komputer yang lain. Mac yang sering digunakan dalam jaringan *local* yaitu bekerja pada osi layer lapis ke 2 layer network. MAC (*Media Access Control) address* adalah alamat sebuah *hardware* atau alamat fisik yang secara unik mengidentifikasi setiap komputer atau alat yang terhubung dalam jaringan, MAC *address* juga sering disebut *physical/hardware address*. (Jubilee Enterprise, 2009:86). Berikut adalah beberapa fungsi dari MAC *address* :

a. Memberikan kontrol terhadap alat apa saja yang bisa terkoneksi dengan *router*.
b. Membatasi akses berdasarkan MAC *access lists* (ACLs) yang tersimpan dan didistribusikan dalam hampir setiap jenis *router*.
c. Memiliki kemampuan penyaringan akses ke dalam sebuah komputer menggunakan daftar perijinan (permissions list) yang dibuatkan berdasarkan MAC *address*. MAC-*Clone* merupakan suatu tindakan pembobolan, duplikasi (*cloning*) pada alamat sebuah *hardware* atau alamat fisik pada komputer agar memiliki MAC *address* yang sama tujuannya agar dapat dengan mudah masuk ke dalam jaringan tanpa

melakukan perijinan dari administrator terlebih dahulu. (Jubilee Enterprise, 2009:86).

2.4 *Hotspot*

Menurut Iwan Sofana (2008:355), *hotspot* adalah tempat khusus yang disediakan untuk mengakses *internet* mengunakan peralatan Wi-fi. Umumnya layanan *hotspot* bersifat gratis. Dengan berbekal laptop atau PDA maka koneksi *internet* dapat dilakukan secara cuma-cuma. Biasanya pengguna terlebih dulu harus melakukan registrasi kepenyedia layanan *hotspot* untuk mendapatkan login dan password. Kemudian pengguna dapat mencari area *hotspot*, seperti pusat perbelanjaan, kafe, hotel, kampus, sekolahan, bandara udara, dan tempat-tempat umum lainnya. Proses otentikasi dilakukan ketika browser diaktifkan. Untuk membuat *hotspot* dibutuhkan alat seperti *access point* (AP). *Access point* bisa dianalogikan dengan hub dan repiter pada (wired LAN). *Access point* dapat menerima dan meneruskan sinyal dari berbagai peralatan WIFI. *Access point* juga dapat menggabangkan jaringan *wireless* dengan wired dan dapat memperbesar jangkauan WLAN. Ada beberapa kelebihan *hotspot* diantaranya :

a. Banyaknya disediakannya koneksi di tempat umum, seperti café, lobi hotel, restoran, executive lounge bandara dll.
b. User bisa bekerja secara mobile tanpa harus mencari plug koneksi.
c. Membuang kerumitan kabel dan membuat perusahaan bisa konsentrasi ke business processnya
d. Transfer data bisa mencapai 11 mbps dengan *troughput* yang besar dan tergantung standar yang digunakan.
e. Kompabilitas dengan banyak *devices* yang sudah terdapat Wi-Fi *enabled*.
f. *Trend* dan *branding*.

2.5 *Firewall*

Firewall atau dinding api adalah sistem perangkat lunak yang mengizinkan lalu lintas jaringan yang dianggap aman untuk dapat melaluinya dan mencegah lalu lintas jaringan yang dianggap tidak aman. Pada dasarnya sebuah *firewall* dipasang pada sebuah *router* yang berjalan pada *gateway* antara jaringan lokal dengan jaringan *Internet* (Wahana Komputer, 2014:72).

2.5.1 Fungsi *Firewall*

Menurut Wahana Komputer (2014:72), *Firewall* berperan dalam melindungi jaringan dari serangan yang berasal dari jaringan luar. *Firewall* mengimplementasikan paket *filtering*. Dengan demikian, *firewall* menyediakan fungsi kemanan yang digunakan untuk mengelola aliran data ke, dari, dan melalui *router*. Berikut fungsi – fungsi firewall secara umum:

1. Mengontrol dan mengawasi paket data yang mengalir di jaringan.
   Firewall harus dapat mengatur, memfilter dan mengontrol lalu lintas data yang diizin untuk mengakses jaringan *private* yang dilindungi *firewall*. *Firewall* harus dapat melakukan pemeriksaan terhadap paket data yang akan melewati jaringan *private*. Beberapa kriteria yang dilakukan *firewall* apakah memperbolehkan paket data lewati atau tidak, antara lain:
   a. Alamat IP dari komputer sumber
   b. Port TCP/UDP sumber dari sumber
   c. Alamat IP dari komputer tujuan
   d. Port TCP/UDP tujuan data pada komputer tujuan
   e. Informasi dari *header* yang disimpan dalam paket data
2. Melakukan autentifikasi terhadap akses.
3. Aplikasi Proxy
   Firewall mampu memeriksa lebih dari sekedar *header* dari paket data, kemampuan ini menuntut *firewall* untuk mampu mendeteksi protokol aplikasi tertentu yang spesifikasi.

4. Mencatat semua kejadian di jaringan.

   Mencatat setiap transaksi kejadian yang terjadi di *firewall*. Ini memungkinkan membantu sebagai pendeteksian dini akan kemungkinan penjebolan jaringan.

2.6 Mikrotik

` Mikrotik merupakan sebuah perusahaan yang bergerak di bidang produksi perangkat keras (Hardware) dan perangkat lunak (Sofware) yang berhubungan dengan sistem jaringan komputer yang berkantor pusat di Latvia, bersebelahan di Rusia. Mikrotik didirikan pada tahun 1995 untuk mengembangkan *router* dan sistem ISP (*Internet Service Provider*) nirkabel. Mikrotik adalah *router* yang dibangun dari sistem operasi Linux, hanya saja dimodifikasi sedemikian rupa sehingga fungsinya spesifik ke arah *routing* dan fungsi jaringan. Alat ini dapat digunakan untuk *routing static, routing dinamic, hotspot, firewall*, VPN, DHCP *Server*, DNS *cache*, dan *web* proxy (Hardana & Ino Irvantino, 2011).

2.7 *Router*

Menurut Iwan Sofana (2008:69) Pengertian *Router* adalah peralatan jaringan yang dapat menghubungkan satu jaringan dengan jaringan yang lain. *Router* bekerja menggunakan *routing table* yang disimpan di *memory*-nya untuk membuat keputusan tentang kemana dan bagaimana paket dikirimkan. *Router* merupakan perangkat yang dikhususkan untuk menangani koneksi antara dua atau lebih jaringan yang terhubung melalui *packet switching*. *Router* bekerja dengan melihat alamat asal dan alamat tujuan dari paket yang melewatinya dan memutuskan rute yang akan dilewati paket tersebut untuk sampai ketujuan. *Router* mengetahui alamat masing-masing komputer dilingkungan jaringan lokalnya, mengetahui alamat *bridge*, dan *router* lainnya. Sebuah *router* mampu mengirimkan data atau informasi dari satu jaringan lain yang berbeda, *router* hampir sama dengan *bridge*, meski tidak lebih pintar dibandingkan *bridge*, namun pengembangan

perangkat *router* dewasa ini sudah mulai mencapai bahkan melampaui batas tuntunan teknologi yang diharapkan. *Router* akan mencari jalur terbaik untuk mengirimkan sebuah pesan yang berdasarkan atas alamat tujuan dan alamat asal. *Router* mengetahui alamat masing-masing komputer dilingkungan jaringan lokalnya, *bridge* dan *router* lainya. *Router* juga dapat mengetahui keseluruhan jaringan dengan melihat sisi nama yang paling sibuk dan bisa menarik data dari sisi yang sibuk tersebut sampai sisi tersebut bersih.

Menurut (Cartealy, 2013) *Router* adalah salah satu komponen pada jaringan Komputer yang mampu melewatkan data melalui sebuah jaringan atau *internet* menuju sasarannya melalui sebuah proses yang dikenal sebagai routing. Router berfungsi sebagai penghubung antar dua atau lebih jaringan untuk meneruskan data dari satu jaringan kejaringan lainnya. *Router* bertugas untuk menyampaikan paket data dari satu jaringan ke jaringan lainnya, jaringan pengirim hanya tahu bahwa tujuan jauh dari *router*. Selain itu, *router* juga memilih jalur untuk mencapai tujuan. Menurut (Cartealy, 2013) *Router* dipasaran terbagi menjadi tiga yaitu:

a. *Router* PC merupakan komputer dengan sistem operasi yang memiliki fasilitas untuk membagi dan men-*sharing* IP address, dimana perangkat (PC) yang terhubung ke komputer tersebut akan dapat menikmati IP Address atau koneksi yang disebarkan oleh sistem operasi tersebut.
b. *Router* Aplikasi merupakan suatu aplikasi yang dapat diinstal pada sistem operasi dimana memiliki kemampuan seperti *router*.
c. *Router Hardware* merupakan *hardware* yang memiliki kemampuan seperti *router* dari berbagai *hardware* yang memancarkan atau membagi IP *address* dan men-*sharing* IP *address*.

Gambar 2. 1 Mikrotik *Router* RB941-2ND.

2.8 *Access Point*

Access Point adalah sebuah perangkat jaringan yang berisi sebuah transceiver dan antena untuk transmisi dan menerima sinyal ke dan dari *clients remote*. Dengan *access points* (AP) *clients wireless* bisa dengan cepat dan mudah untuk terhubung kepada jaringan LAN kabel secara *wireless*. Atau agar kita lebih mudah untuk memahaminya maka bisa dibilang sebuah alat yang digunakan untuk menghubungkan alat-alat dalam suatu jaringan, dari dan ke jaringan *wireless.* (Firdana, 2012).

Gambar 2. 2 Mikrotik Access Point RB951UI-2ND

Secara garis besar, *access point* berfungsi sebagai pengatur lalu lintas data, sehingga memungkinkan banyak *Client* dapat saling terhubung melalui jaringan (*Network*). Atau jika ingin diperinci lebih jelas lagi fungsi *access point* adalah sebagai berikut (Purwanto, 2013) :

1) Mengatur supaya AP dapat berfungsi sebagai DHCP *server.*
2) Mencoba fitur *Wired Equivalent Privacy* (WEP) dan Wi-Fi *Protected Access* (WPA).
3) Mengatur akses berdasarkan MAC *Address device* pengakses.
4) Sebagai *Hub/Switch* yang bertindak untuk menghubungkan jaringan lokal dengan jaringan *wireless*/nirkabel.