BAB II
TINJAUAN PUSTAKA

2.1 Tinjauan Pustaka

Sebuah penelitian yang berjudul "A Study on Security Threats and Dynamic Access Control Technology for BYOD, Smart-work Environment" dibuat oleh Eun Byol Koh, Joohyung Oh, dan Chaete Im pada tahun 2014 yang menjelaskan sebuah istilah BYOD (Bring Your Own Device) yang bearti membawa perangkat anda sendiri untuk memudahkan para karyawan disebuah perusahaan dapat mengakses sebuah data, database dan aplikasi lebih mudah dengan menggunakan perangkat seluler pribadi mereka seperti ponsel pintar, laptop computer dan PC tablet. Tetapi dengan adanya lingkungan teknologi yang baru seperti sistem BYOD dapat membuat sebuah ancaman keamanan meningkat diwaktu yang sama. Untuk menghadapi ancaman itu, para peneliti menerapkan solusi keamanan jaringan seperti NAC (*Network Access Control*). Namun dengan begitu saja tidak cukup untuk menyelesaikan resiko yang terjadi didalam lingkungan BYOD. Para peneliti perlu untuk menetapkan kebijakan keamanan yang fleksibel dengan mempertimbangkan beragam jenis terminal dan beragam keadaan. Akhirnya, makalah ini mengusulkan sistem keamanan terpadu untuk menyelesaikan ini ancaman keamanan. Ini menunjukkan bahwa sistem ini meneliti konteksnya informasi yang melakukan kontrol akses dinamis berdasarkan itu. (Koh, Oh, & Im, 2014)

Penilitian selanjutnya yang berjudul "A Review of Opensource *Network Access Control* (NAC) Toold for Enterprise Educational Networks" yang dibuat oleh Henry Nunoo dan Emmanuel Kofi yang berisikan bahwa dalam sebuah jaringan perusahaan terdapat konsep BYOD (Bring Your Own Devices) untuk bekerja dan juga untuk para tamu yang akan terhubung kedalam jaringan yang dianjurkan. Sebagai factor kebutuhan control akses ke jaringan sangatlah penting dikarenakan akan munculnya potensi ancaman keamanan yang tinggi pada jaringan tersebut. Penilitian ini lebih banyak menjelaskan penggunaan opensource untuk jaringan perusahaan terutama untuk jaringan yang memiliki budget yang rendah. Penelitian ini juga menggunakan opensource seperti Packetfence atau FreeNAC. (Nunoo-mensah & Akowuah, 2014)

Penelitian selanjutnya yaitu sebuah penelitan yang berjudul " Implementasi *Network Access Control* pada Jaringan EEPIS" penelitian ini dibuat oleh mahasiswa jurusan Teknk Informatika di sebuah perguan tinggi Politeknik Elektronika Surabaya yaitu Ali Latiful Aprianto dan Idris Winarno. Penilitian ini menjelaskan bahwa pencurian identitas pribadi melalui media internet semakin memarak. Bebagai cara bias digunakan misalnya seperti phising, email scan ataupun ada yang menggunakan piranti yang dapat melacak gerak-gerik kebiasaan *user* ketika mengakses situs-situs web di internet. Kebocoran informasi ini tidak hanya terjadi secara personal tapi juga bias terjadi secara korporat. Yang mana tidak tertutup kemungkinan kebocoran itu dating dari orang dalam sendiri. Karena itulah dperlukan adanya pengaman jaringan diantaranya dengan menggunakan metode NAC (*Network Access Control*) dengan

menggunakan metode NAC, Seorang administrator jaringan dapat mengontrol dan mengamankan jaringannya dari aksi para *user* yang tidak bertanggung jawab dengan cara mengisolasi computer *user* tersebut dari koneksi jaringan. Pada penelitian ini dijelaskan bahwa NAC dapat dikembangkan lebih lanjut dengan menambah komponen-komponen pendukung lain. Seperti hping, nmap, nessus, ethereal dan masih banyak lagi. Penelitian ini juga mengatakan bahwa peneliti berharap dengan adanya NAC ini dapat membuat keamanan dalam jaringan akan lebih semakin terjamin. (Latiful Aprianto, Ali. Winarno, 2015)

2.2 Landasan Teori

Dalam landasan teori sebuah *Network Access Control*, penulis mengumpulkan beberapa teori – teori yang akan digunakan untuk menguatkan teori yang ada didalam penelitian ini. Teori yang akan digunakan didalam penelitian ini ialah sebagai berikut:

2.2.1 Jaringan Komputer

Jaringan komputer atau yang biasa kita sebut secara singkat jaringan adalah kumpulan *computer* dan perangkat - perangkat lain yang saling terhubung menggunakan media komunikasi. *Computer* dalam jaringan dapt saling berhubungan melalui kabel, jaringan telepon, gelombang radio, satelit ataupun sinar infra merah(Khairul, 2014).Jika dilihat berdasarkan luas area yang dapat dijangkau jaringan *computer* dibagi menjadi 3 jenis, yaitu:

1. *Local Area Network* (LAN)

   LAN merupakan jaringan milik pribadi di dalam sebuah gedung atau kampus yang berukuran sampai beberapa kilometer. LAN seringkali

digunakan untuk menghubungkan komputer-komputer pribadi dan *workstation* dalam kantor suatu perusahaan atau pabrik untuk pemakaian bersama sumber daya dan saling bertukar informasi.

2. *Metropolitan Area Network* (MAN)

   MAN adalah versi LAN yang berskala lebih besar dan biasanya MAN menggunakan teknologi yang sama seperti LAN. MAN dapat menjangkau area kurang lebih berjarak 5-50km. MAN digunakan untuk mendukung layanan yang membutuhkan bandwidth terpercaya dan limit waktu yang terbatas, sebagai tambahan untuk layanan-layanan data.

3. *Wide Area Network* (WAN)

   WAN adalah jaringan yang lingkup areanya dapat dijangkau menggunkana sarana satelit ataupun kabel bawah laut. Pengelolaan WAN kerap lebih rumit dan kompleks, karena WAN menggunakan banyak sarana untuk menghubungkan antara LAN dan WAN ke dalam komunikasi global seperti internet (Eko, 2015).

2.2.2 *Server*

Server adalah sebuah fasilitas yang menyediakan beberapa jenis layanan dalam sebuah jaringan komputer. *Server* dapat didukung dengan prosesor yang kuat atau bersifat *Random access memory* dan *scalable,* juga dilengkapi dengan *operation sistem* khusus, yang bisa disebut juga sebagai OS jaringan atau *Network operating sistem*(Fitriastuti & Utomo, 2014).

Server juga dapat menjalankan beberapa perangkat lunak yang mengontrok akses jaringan sumber daya yang ada terdapat didalamnya, contoh seperti berkas ata alat pencetak dan dapat memberikan akses kepada anggota jaringan yang lainnya(Yasin, 2017).

2.2.3 Topologi

Topologi jaringan komputer atau arsitektur jaringan komputer adalah pola hubungan antar terminal dalam suatu *sistem* jaringan komputer yang dapat mempengaruhi tingkat efektivitas kinerja jaringan(Eko, 2015). Ada empat bentuk dasar jaringan, yaitu:

1. Topologi *Bus*

   Topologi *bus* ialahn topologi yang semua host terhubung secara langsung pada kabel *backbone* dan *T-Connector* (dengan terminator 50ohm pada ujung network), maka komputer atau perangkat jaringan lainnya bias dengan mudah dihubungkan satu sama lain. Beberapa sulitan yang sangat sering dihadapi adalah kemungkinan terjadinya bentrokan data karena adanya jaringan relatif sederhana jika salah satu *node* putus maka akan mengganggu kinerja dan trafik seluruh jaringan lainya.

2. Topologi *Star*

   Topologi *star* merupakan bentuk topologi jaringan yang menghubungkan semua komputer atau *note* pada sentral atau konsentrator. Biasanya konsentrator adalah sebuah hub atau *switch*.

3. Topologi *Ring*

   Topologi *ring* ialah topologi jaringan yang berbentuk rangkaian titik yang masing-masing terhubung ke dua titik lainnya sehingga membentuk jalur melingkar yang membentuk cincin. Pada topologi *ring,* komunikasi data dapat terganggu jika slaah satu titik mengalami gangguan.

4. Topologi *Tree*

   Topologi *Tree* adalah kombinasi karakteristik antara topologi *star* dan topologi *bus.* Topologi ini terdiri atas kumpulan topologi *star* yang dihubungkan dalam satu topologi *bus* sebagai jalus *backbone.* Komputer-komputer dihubungkan kehub, sedangkan hub lain di hubungkan sebagai jalur tulang *backbone*.

2.2.4 IP *Address*

IP Address ialah singkatan dari *Internet Protocol Address* yang merupakan identitas numerik unik yang diberikan kepada suatu perangkat seperti komputer, *Router*, printer ataupun perangkat lainnya yang terdapat dalam suatu jaringan komputer yang menggunakan *internet protocol* sebagai sarana komunikasi. Berdasarkan tipe dan fungsinya, *IP Address* dalam sebuah jaringan komputer dibagi menjadi beberapa jenis, yaitu :

1. *Static IP* adalah *IP Address* yang diisi secara manual oleh pengguna komputer ataupun administrator.

2. *Dynamic IP* adalah *IP Address* yang didapatkan secara otomatis melalui *DHCP Server* ketika perangkat terhubung ke jaringan yang memiliki layanan tersebut.
3. *Public IP* adalah *IP Address* yang digunakan ketika komputer atau perangakat jaringan lainnya terhubung ke jaringan Internet.
4. *Private IP* adalah *IP Address* yang hanya bisa digunakan pada jaringan local pada sesama komputer untuk dapat saling terkoneksi.

Untuk mempermudah pembagian dan pendistribusiannya, alamat IP dikelompokkan dalam beberapa kelas berdasarkan jangkauan jaringan dan jumlah ip yang dapat ditampung dalam jaringan tersebut. *IP Address* dibagi menjadi kelas A, kelas B, dan kelas C.

1. IP kelas A terdiri dari atas 8 bit untuk *network ID* dan sisanya 24 bit digunakan untuk *host ID,* sehingga *IP Address* kelas A yang digunakan dengan jumlah host sangat besar. Karakteristik IP kelas A:

Format	:0nnnnnnn.hhhhhh.hhhhhhh.hhhhhhh
Bit pertama	: 0
NetworkID	: 8 bit
HostID	: 24 bit
Oktat pertama	: 0 - 129
Jumlah *network*	: 126
Rentang IP	: 1.xxx.xxx.xxx – 126.xxx.xxx.xxx
Jumlah IP	: 16.777.214

2. IP kelas B terdiri atas 16 bit untuk network ID dan sisanya 16 bit digunakan untuk *host ID*, sehingga *IP Address* kelas B digunakan untuk jaringan dengan jumlah *host* sedang. Pada 2 bit pertama diset dengan angka 10 sehingga bernilai 128 sampai 191.

   Karakteristik IP kelas B:

   Format : 10nnnnn.nnnnnnn.hhhhhhh.hhhhhhh

   Bit pertama : 10

   NetworkID : 16 bit

   HostID : 16 bit

   Oktat pertama : 138 - 191

   Jumlah *network* : 16.384

   Rentang IP : 128.0.xxx.xxx – 191.255.xxx.xxx

   Jumlah IP : 65.534

3. Kelas C terdiri atas 24 bit untuk *network ID* dan sisanya 8 bit digunakan untuk host ID, sehingga *IP Address* kelas C digunakan untuk jaringan berukuran kecil seperti LAN. Pada 3 bit pertama, berisi angka 110. Karakteristik IP kelas C:

   Format : 110nnnn.nnnnnnn.nnnnnnn.hhhhhhh

   Bit pertama : 110

   NetworkID : 24 bit

   HostID : 8 bit

   Oktat pertama : 192 - 223

Jumlah *network* : 2.097.152

Rentang IP : 192.0.0.xxx – 223.255.255.xxx

Jumlah IP : 254

2.2.5 *Router*

Router merupakan perangkat yang melewatkan paket IP dari satu jaringan ke jaringan lainnya dengan menggunakan metode *Addressing* dan *protocol* tertentu. *Router* yang terkoneksi dalam suatu jaringan tergabung dalam suatu algoritma *routing* untuk menentukan jalur yang terbaik untuk dilalui oleh paket IP (Eko, 2015). Proses *routing* dilakukan dengan cara *hop by hop*. IP tidak mengetahui semua jalur untuk menuju tujual setiap paket. IP hanya mencarikan jalur terdekat dengan memberitahukan *IP Address* dari *Router* selanjutnya.(Farouk, Ramdhani, & Wibowo, 2012)

Gambar 2.1 Salah satu contoh *Router*.

2.2.6 Switch

Switch adalah perangkat penghubung untuk beberapa perangkat untuk membentuk sebuah Local Area Network. Perbandingannya dengan *Router*, *Switch* merupakan sebuah jalanan sedangkan *Router* merupakan penghubung antar jalanan. Masing – masing berada di jalan yang mempunyai alamat yang berurutan. Dengan cara yang sama, *switch* menghubungkan berbagai jenis alat, yang masing – masing mempunyai alamet IP tersendiri. (Abdullah, Tamam Asrori, 2014)

Gambar 2.2 salah satu contoh *switch*

2.2.7 Mikrotik

Mikrotik merupakan salah satu dari beberapa perusahaan it yang bergerak dalam memproduksi sebuah aplikasi dan peralatan jaringan *computer*. “Mikrotik *Router* OS adalah *sistem* operasi dan perangkat lunak yang dapat digunakan untuk

menjadikan *computer* menjadi *Router* network yang sangat handal, mencakup berbagai fitur yang dibuat untuk ip network dan jaringan *wireless*, cocok untuk digunakan oleh ISP dan provider *hotspot*". Pada dasarnya *Router* OS berjalan pada *sistem* operasi Linux sehingga seluruh perintah didasarkan pada perintah Linux.

Salah satu produk utama Mikrotik adalah *RouterBoard* yang merupakan perangkat keras yang berfungsi utama sebagai *Router*. *RouterBoard* biasanya dilengkapi dengan *Router operating sistem* (*Router* OS) yang membuat *RouterBoard* memiliki fungsi yang lebih lengkap dalam mendukung manajemen jaringan *computer* itu sendiri(Abdullah, Tamam Asrori, 2014).

Konfigurasi yang dapat dilakukan *RouterBoard* bisa melalui mode GUI *(Graphic User Interface)* atau mode text/terminal. Dengan aplikasi kecil yang diberi nama Winbox, pengguna dapat mengkonfigurasi *RouterBoard* tanpa perlu menghafalkan berbagai perintah. Oleh Karena penggunaannya yang sangat sederhana, *RouterBoard* banyak digunakan di Universitas, ISP, bahkan di warnet.

Beberapa fitur utama yang menjadikan *RouterBoard* sebgai *Router* popular adalah *Hotspot* dan RADIUS *Server*. Keduanya berfungsi sebagai modul AAA dimana *Hotspot* sifatnya lebih sederhana sedangkan RADIUS *Server* untuk implementasi yang lebih kompleks.(Alex, 2016)

Gambar 2.3 Mikrotik RB850

2.2.8 Winbox

Winbox merupakan sebuah aplikasi untuk melakukan proses pengendalian jarak jauh ke *Router* mikrotik dengan berbasis digital atau GUI *(Graphical User Interface).* Dengan winbox, pengaturan dapat dilakukan melalui kompuuter *client.* Pengaturan *Router* mikrotik melalui winbox lebih umum digunakan, karena penggunaanya yang mudah serta tidak perlu lagi mengingat perintah – perintah untuk mengkonfigurasi *Router* mikrotik (Fitriastuti & Utomo, 2014). Namun, beberapa *network administrator* lebih memilih mengkonfigurasi *Router* mikrotik dengan berbasis CLI *(Command line Interface)* karena tampilannya yang lebih sederhana, di winbox juga menyediakan opsi untuk pengaturan berbasis CLI(Dwiyatno, Putra, & Krisnaningsih, 2015)

2.2.9 *Access point*

Access point adalah sebuah perangkat yang berfungsi untuk mentransmisikan data dalam sebuah WLAN. *Access point* terhubung dengan jaringan Local melalui media kabel. *Access point* berfungsi untuk memberi jalan *transfer* data antara WLAN dan Wired LAN, melakukan konversi sinyal frekuensi radio (RF) menjadi sebuah *signal* digital yang dapat disalurkan melalui kabel atau sebaliknya disalurkan ke perangkat WLAN yang lainnya dengan merubah kembali menjadi sebuah sinyal *frequensy* radio. (Yessi Alfrida Syahputri, Muh. Yamin, 2017)

2.2.10 *Network Access Control*

Network Access Control (NAC) merupakan sebuah pendekatan dalam keamanan jaringan komputer yang berusaha untuk memadukan beberapa teknologi pengamanan jaringan, seperti antivirus, host intrusion prevention, dan otentikasi pada sistem serta keamanan jaringan lainnya. *Network Access Control* (NAC) adalah sebuah solusi dalam keamanan jaringan komputer yang menggunakan beberapa protokol untuk mendefinisikan dan mengimplementasikan sebuah aturan yang mendeskripsikan cara untuk mengamankan sebuah akses ke dalam sebuah jaringan ketika sebuah alat mencoba untuk tersambung dalam suatu jaringan. Sesuai dengan namanya NAC bertujuan untuk mengontrol akses dalam suatu jaringan dengan aturanaturan tertentu yang telah diatur sebelumnya. Dimana seorang administrator dapat menentukan perangkat mana saja yang dapat mengakses suatu jaringan, dan apa yang dapat dilakukan perangkat tersebut dalam suatu jaringan. Sehingga jaringan tersebut terhindar dari serangan virus, host intrusion, dan network worm.

2.2.11 Radius

Radius adalah singkatan *dari Remote Authentication Dial-in User Service* yang berguna untuk menyediakan sebuah mekanisme keamanan dan *management user* pada sebuah network. *Radius* diterapkan dalam jaringan dengan model *client-Server*.

Server Radius menangani otentikasi dan otorisasi koneksi yang dilakukan *user*, pada saat komputer client akan menghubungkan diri dengan jaringan maka *Server* Radius akan meminta identitas *user* untuk kemudian akan dicocokan dengan data-data yang ada didalam database *Server* Radius itu sendiri.(Gesit Singgih Febyatmoko, Taufiq Hidayat, 2016)

2.2.12 VLAN

VLAN atau dengan nama lain *Virtual Local Area Network* merupakan sebuah jenis jaringan yang tidak dibatasi oleh lokasi fisik semisal LAN. Maka dari itu, menyebabkan jaringan *VLAN* mampu dikonfigurasi secara virtual tanpa menuntut lokasi fisik perangkat keras. Agar *VLAN* bisa digunakan, diperlukan switch yang bisa dikonfigurasi dan memastikan seluruh switch yang berada dalam satu jaringan memiliki konfigurasi yang sama. *VLAN* secara fisik memang terlihat seperti satu jaringan, namun secara logika, *VLAN* merupakan jaringan yang berbeda. Dengan adanya *VLAN* maka kemungkinan seluruh jaringan terganggu akan sangat rendah karena *VLAN* membagi satu jaringan menjadi beberapa jaringan secara logika, sehingga apabila satu vlan terganggu tidak akan terpengaruh *VLAN* yang lain (Putra & Wiwin Sulistyo, S.T., 2014).