ANALISIS KELEMAHAN KEAMANAN PADA JARINGAN WIRELESS

SKRIPSI

Oleh:
Novia Sitohang
160210215

PROGRAM STUDI TEKNIK INFORMATIKA
UNIVERSITAS PUTERA BATAM
2020

ANALISIS KELEMAHAN KEAMANAN PADA JARINGAN WIRELESS

SKRIPSI
Untuk memenuhi salah satu syarat
memperoleh gelar Sarjana

Oleh:
Novia Sitohang
160210215

PROGRAM STUDI TEKNIK INFORMATIKA
UNIVERSITAS PUTERA BATAM
2020

SURAT PERNYATAAN ORISINALITAS

Yang betanda tangan di bawah ini saya:

Nama : Novia Sitohang

NPM : 160210215

Fakultas : Teknik dan Komputer

Frogram Studi : Teknik Informatika

Menyatakan bahwa " skripsi" yang saya buat dengan judul:

Analisis Kelemahan Keamanan Pada Jaringan Wireless.

Adalah hasil karya sendiri dan buka "duplikasi" dari karya orang lain. Sepengetahuan saya, didalam naskah skripsi ini tidak terdapat karya ilmiah atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali secara tertulis dikutip naskah ini dan disebutkan dalam sumber kutipan dan daftar pustaka.

Apabila ternyata didalam naskah Skripsi ini dapat dibuktikan terdapat unsur- unsur PLAGIAT, saya bersedia naskah Skripsi ini digugurkan dan gelar akademik saya peroleh dibatalkan , serta proses sesuai dengan peraturan perundang-undangan yang berlaku. Demikian pernyataan ini saya buat dengan sebenarnya tanpa ada paksaan dar siapapun.

Batam, 20 Februari 2019

Novia Sitohang
16021021

ANALISIS KELEMAHAN KEAMANAN PADA JARINGAN WIRELESS

SKRIPSI
Untuk memenuhi salah satu syarat
memperoleh gelar Sarjana

Oleh
Novia Sitohang
160210215

Telah disetujui oleh Pembimbing pada tanggal
seperti tertera dibawah ini

Batam, 20 Februari 2020

Cosmas Eko Suharyanto, S.Kom., M.MSI
Pembimbing

ABSTRAK

Tujuan yang ingin dicapai dalam penelitian ini adalah untuk mendapatkan hasil analisis keamanan dan kinerja jaringan pada Kantor PT Codewell Tekindo Jaringan menggunakan Nmap dan Kali Linux, sehingga dapat diketahui kelemahan dan kekurangan sistem kemanan jaringan sehingga dapat diberikan usulan mengenai keamanan jaringan yang lebih kuat dan tidak mudah disadap oleh orang yang tidak bertanggung jawab. Metode penelitian yang digunakan meliputi metode wawancara (terhadap sistem yang sedang berjalan, serta analisis masalah dan kebutuhan) dan metode observasi berupa perancangan desain sistem jaringan, perancangan sistem, peralatan jaringan yang ada digunakan dan konfigurasi pada jaringan. Hasil penelitian adalah Sistem kemanan jaringan yang ada di Kantor PT Codewell Tekindo Cemerlang masih jauh dari kata aman. Hal ini dapat dibuktikan dengan berhasilnya *hacker* masuk ke dalam jaringan dan menghentikan aktivitas jaringan menggunakan kali linux Disisi lain kemanan jaringan setelah dianalisis menggunakan Nmap dengan menggunakan komputer dengan IP 192.168.192.3 dan IP laptop 103.29.184.44 tidak didapatkan *port* yang terbuka sehingga dapat dinyatakan aman hal ini dibuktikan hasil *scanning* tidak menemukan satupun *port* yang terbuka.

Kata kunci: jaringan, *scanning*, mikrotik, *port*, Nmap, Kali Linux, speedtest

ABSTRACT

The aim of this research is to obtain the results of network security and network performance analysis at the Office of Investment and Integrated Services of codewell tekindo cemerlang Nmap and Kali Linux, so that weaknesses and weaknesses in the network security system can be identified so that suggestions can be given regarding network security stronger and not easily infiltrated by irresponsible people. The research methods used include the interview method (of the current system, and analysis of problems and needs) and observation methods in the form of network system design, system design, existing network equipment used and configuration on the network. The results of the study are that the network security system in the PT Codewell Tekindo Cemerlang Officein Regency is far from safe. This can be proven by the successful hackers into the network and stop network activity using kali kali On the other hand network security after being analyzed using Nmap using computers with IP 192.168.192.3 and laptop IP 103.29.184.44 do not get an open port so that it can be declared safe this is proven by scanning results not finding any open ports.

Keywords: Network, scanning, mikrotik, *port, Nmap, Kali Linux, speedtest*

KATA PENGANTAR

Segala puji bagi Tuhan Yang Maha Esa yang telah melimpahkan segala berkat dan karunia-NYA, sehingga penulis dapat menyelesaikan laporan tugas akhir yang merupakan salah satu persyaratan untuk menyelesaikan program studi strata satu (S1) pada Program Studi Teknik Informatika Universitas Putera Batam.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati. Dengan segala keterbatasan, penulis menyadari pula bahwa skripsi ini takkan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Rektor Universitas Putera Batam.
2. Ketua Program Studi Teknik Informatika Universitas Putera Batam, Bapak Andi Maslan, S.T., M.SI.
3. Bapak Cosmas Eko Suharyanto, S.Kom., M.SI. selaku pembimbing Skripsi pada Program Studi Teknik Informatika Universitas Putera Batam.
4. Dosen dan Staff Universitas Putera Batam.
5. Suami saya Lancang Nainggolan yang telah membatu saya dalam materi, semangat dan doa.
6. Orang tua dan keluarga besar OP, Bora yang terus membawa saya dalam doa.
7. Sahabat saya Rahmat Ismail yang membantu saya dalam memberi semangat.
8. Sahabat saya Esra Simanungkalit yang telah memotivasi dan mendukung saya.
9. Bu Deski Liana yang telah membantu dalam penelitian ini.
10. Rekan-rekan mahasiswa/i Universitas Putera Batam yang turut memberikan doa dan dukungannya
11. Mitra kerja yang selalu memberikan masukan yang berguna untuk penelitian ini
12. Serta pihak-pihak lain yang tidak dapat disebutkan satu per satu.

Semoga Tuhan Yang Maha Esa membalas kebaikan semua pihak yang mendukung dalam penyelesaian skripsi ini. Akhir kata penulis mengucapkan terimakasih

Batam, Februari 2020

Novia Sitohang

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1

PENDAHULUAN

1.1 Latar Belakang Penelitian

Perkembangan teknologi pada saat ini identik dengan efisiensi dan inovasi, dalam segala aspek kehidupan seperti saat sekarang ini dimana kita bisa melihat dalam kehidupan, sehingga perkembangan teknologi komunikasi dan informasi merupakan suatu keharusan. Sebab teknologi komunikasi dan informasi saat ini merupakan hal yang sulit terpisahkan. Salah satu contoh kemajuan teknologi komunikasi dan informasi tersebut ialah WLAN (*Wireless Area Network*) yang sering disebut sebagai teknologi jaringan tanpa kabel (*nirkabel*) Penggunaan teknologi jaringan *wireless* sering dijumpai pada *café, hotspot komersial*, kampus-kampus, perkantoran dan tempat-tempat umum. Akan tetapi kurangnya kesadaran pengguna untuk memperhatikan keamanan komunikasi data pada jaringan *wireless* tersebut.

Pada saat ini Perkembangan jaringan mempunyai peranan penting dalam berbagai aktivitas dalam pekerjaan. Dalam penggunaannya jaringan lebih cepat dan akurat sehingga dapat menjadikan satu alternatif untuk memecahkan masalah. Perkembangan teknologi komunikasi ini didukung dengan adanya peningkatan pada kemajuan infrastruktur dan teknologi. Komunikasi dan informasi ini merupakan komunikasi yang menggunakan *wireless* pada komunikasinya, hal ini ditandai dengan hadirnya peralatan *wireless* yang saat ini menggunakan

standarisasi peralatan *wireless* ialah IEEE 802.11. Penggunanaan jaringan yang semakin luas ditandai dengan pertumbuhan pada pengunaan internet yang media penghantarannya dapat dikatakan semakin cepat untuk memperoleh informasi dan keuntungan dari *shared* data dan *shared resourse*. Dengan digunakannya *WLAN* dapat mengaksess informasi tanpa mencari tempat untuk menghubungkan menggunakan media kabel. *Wireles Lan* dapat mengatasi masalah dari kekurangan yang dimiliki oleh *wired network,* dikarenakan *wireless lan* mempunyai kelebihan yakni: *Scalability, Mobility, Installation speed*, *Installation Fleksibility, simplicity*, dan *Reduced cost of ownership*. Teknologi *wireless* yang memiliki berbagai kemudahan, tetapi terdapat pula dampak buruk bagi pengguna internet. Pada perkembangan teknologi ini lah dapat dirasakan dengan banyaknya jaringan *wireless hotspot* yang tersedia. Selain itu jaringan *wireleess hotspot* bisa membantu menciptakan berbagai inovasi yang positif. Namun terdapat pula sisi negative.

PT Codewell Tekindo Cemerlang adalah perusahaan yang bergerak dalam bidang aplikasi, jaringan, kontruksi dan *general supplier*. PT Codewell Tekindo Cemerlang terdapat suatu jaringan yang memiliki peran penting dalam kesehariannya. Dengan menggunakan jaringan *wireless* untuk dapat mengakses jaringan tersebut, agar tidak terjadi permasalahan sebaiknya melakukan pengujian kinerja jaringan *wireless.*

Topologi yang digunakan pada PT Codewell Tekindo Cemerlang ialah menggunakan topologi *star*. Wahana (2014) menggunakan topologi *star* dapat mengurangi terjadinya kegagalan jaringan karena semua node jaringan terhubung

ke *hub* dimana *Hub* tersebut melakukan *broadcast* keseluruh *node* yang terhubung. Apabila pada satu *line* terdapat salah satu putus dari *node* sentral maka *node* yang lain tidak terganggu.

Wireless ialah perangkat teknologi yang menghubungkan dua komputer, sehingga dapat bertukar data/ informasi tanpa harus menggunakan jaringan kabel. Adapun keuntungan jaringan *witeless* ialah dapat mengurangi dari penggunaan kabel, yang dirasa cukup mengganggu dalam peroses instalasi yang lebih dari dua perangkat yang dihubungkan dalam suatu jaringan. Akan tetapi dari segi keamanan yang dimiliki jaringan *wireless* masih kurang aman karena mudah terkena serangan para *hacker* (peretas jaringan), sebab jaringan *wireless* masih menggunakan gelombang radio (Andi & Madcoms, 2015).

Perangkat lunak atau aplikasi yang digunakan *hacker* adalah *NMAP* dan *kali linux* dalam menelusuri jaringan karena sistem operasinya yang bersifat *open source* dan digunakan untuk mengetahui kelemahan dari jaringan. *NMAP* dan *Kali Linux* digunakan oleh *attacker* untuk melakukan *scanning* dalam jaringan besar atau kecil dengan menggunakan paket *raw* IP untuk mengetahui *host* yang sedang online dalam jaringan, mengetahui *port* yang terbuka, dan dapat mengetahui *firewall* yang digunakan. Sehingga penulis tertarik untuk menggunakan aplikasi ini untuk melakukan analisis jaringan *wireless*. Penulis mengunakan aplikasi *NMAP* mempunyai alasan yakni, Melakukan penelusuran secara menyeluruh pada jaringan dan mengetahui *Port* yang lebih spesifik pada *service* yang aktif. Nmap merupakan salah satu *tools* aplikasi yang banyak digunakan untuk melakukan proses *scanning* yang dikenal sebagai *tools* dengan *multiplatform*, cepat dan

ringan. *Nmap* berjalan pada semua jenis Sistem Operasi, baik mode *console* maupun grafis. Sedangkan *Kali Linux* Terdapat 300 lebih alat *penetration testing* yang telah di sempurnakan. Karena bersifat (*Open Source*) gratis, pengembang yang aman, dan dapat di modifikasi kapanpun.

Telah disimpulkan dari pembahasan di atas kinerja jaringan *wireless* di PT Codewell Tekindo Cemerlang, harus memiliki format yang baik untuk efisiensi dalam pencegahan bertumpuknya berkas sehingga mengakibatkan koneksi jaringan tidak stabil. Penulis mengkaji ulang untuk diteliti dan mencari tahu kualitas jaringan *wireless* dan keamanan yang ada di PT Codewell Tekindo Cemerlang, pada sebuah aplikasi NMAP dan Sistem operasi Kali Linux dalam menganalisa pengukuran jaringan dan memonitoring kinerja jaringan wireless sehingga penulis mengetahui kinerja jaringan pada infrastruktur dalam mengukur kecepatan unggah (*upload*) dan unduh (d*owndload*), dengan cara menggunakan parameter *bandwidth* dalam mengukur keamanan jaringan pada PT Codewell Tekindo Cemerlang. Setelah melihat uraian diatas penulis berniat mengambil tugas akhir dengan judul "**Analisis Kelemahan Keamanan Pada Jaringan *Wireless***".

1.2 Identifikasi Masalah

Berdasarkan uraian diatas, dapat disimpukan masalah dari peneletian ini ialah bagaimana caranya menganalisa jaringan *wireless* menggunakan aplikasi *NMAP* dan *kali linux* pada PT Codewell Tekindo Cemerlang.

I.3 Pembatasan Masalah

Dalam penelitian ini peneliti berusaha menghindari pembahasan yang terlalu luas, sehingga peneliti membuat batasan-batasan masalah sebagai berikut:

1. Keamanan yang diuji hanya pada *acces point*.
2. Penelitian dilakukan pada PT Codewell Tekindo Cemerlang.
3. Analisa yang dilakukan pada celah keamanan jaringan nirkabel (802.11 a/b/g).
4. Melakukan analisis kecepatan *bandwith* jaringan di PT Codewell Tekindo Cemerlang.

I.4 Perumusan Masalah

Berdasarkan batasan masalah tersebut, penulis merumuskan masalah syakni: Bagaimana cara menganalisa jaringan *wireless* menggunakan aplikasi *NMAP* dan sistem operasi *Kali Linux* dengan menggunakan indikator port?

I.5 Tujuan Penelitian

Penelitian mempunyai tujuan yang ingin dicapai yakni untuk memperoleh hasil analisa keamanan jaringan *wireless* pada PT Codewell Tekindo Cemerlang dengan menggunakan aplikasi NMAP dan sistem operasi Kali Linux.

I.6 Manfaat Penelitian

Secara spesifik, penelitian ini diharapkan mampu memberikan manfaat baik dari aspek teoritis maupun aspek praktis. Manfaat yang didapatkan dari penelitian ini antara lain:

1.6.1 Teoritis

Penelitian ini dapat di simpulkan secara teoritis sebagai berikut:

1. Pada penelitian menggunakan aplikasi *NMAP* dan sistem operasi *Kali Linux* diharapkan bisa untuk menambah ilmu pengetahuan tentang konsep keamanan jaringan, sehingga memperoleh pengetahuan bagi pembacanya dan menambah wawasan
2. Penelitian ini diharapkan dapat dijadikan sebagai keamanan jaringan.

1.6.2. Teoritis

Penelitian ini dapat di simpulkan secara teoritis sebagai berikut:

1. Bagi masyarakat, sebagai media edukasi keamanan jaringan *wireles*
2. Bagi peneliti selanjutnya, dapat menambah pengetahuan dan wawasan serta dapat menjadi acuan bagi penelitian selanjutnya.

BAB II

TINJAUAN PUSTAKA

2.1 Teori Dasar

2.1.1 Pengertian Jaringan Komputer

Komputer dapat dihubungkan dengan komputer lain supaya dapat bertukar data dan informasi fungsi dari jaringan komputer. Setiap instansi atau perusahaan menggunakannya dengan tujuan untuk memperlancar arus informasi. Beberapa Banyak komputer, printer dan perangkat lainnya yang saling terhubung dalam satu ruangan berdasarkan penelian Saputra dan Basten. Menggunakan kabel atau tanpa kabel dapat membuat *user* atau pengguna saling bertukar data dengan menggunakan perangkat keras (*hardware*), perangkat lunak dan *software* yang terhubung dalam suatu jaringan. Jaringan komputer dapat memiliki dua puluhan, ribuan atau bahkan jutaan *node* karena *node* adalah komputer, printer, *periferal* dan perangkat lainnya yang terhubung dalam jaringan. (Ardianto & Akbar, 2017).

2.1.2 Konsep Hubungan Jaringan Komputer

Hubungan jaringan komputer terdiri dari dua konsep antara lain sebagai berikut:

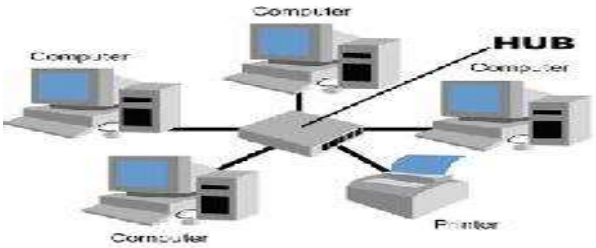
1. *Peer to Peer*

Bebepara perangkat komputer terhubung pada satu sistem jaringan tanpa perantara hingga bisa dibuat menjadi satu kesatuan fungsi dan berbagi jaringan atau dapat disebut dengan *peer to peer*.

Gambar 2.1 *Peer to Peer*
(Sumber: Zunaidi et al., 2014)

2. Client-Server

Komputer yang berfungsi sebagai *server* adalah menjadi syarat mutlak yang harus dipenuhi dalam sebuah kesatuan fungsi *client-server*. Dimana server bertugas untuk malayani *request* data dari komputer *client*. (Zunaidi et al., 2014)



Gambar 2.2 *Client-Server*
(Sumber: Zunaidi et al., 2014)

2.1.3 Jenis-jenis Jaringan Komputer

Dibawah ini beberapa jenis jaringan dan fungsi yang berbeda-beda yakni sebagai berikut:

1. LAN *(Local Area Network)*

LAN merupakan jaringan yang kerap ditemukan. Menghubungkan komputer satu dengan yang lain di ruang lingkup kecil fungsi dari jaringan LAN.

Gambar 2.3 *Wide Area Network*
(Sumber : Wongkar et al., 2015)

2. MAN *(Metropolitan Area Network)*

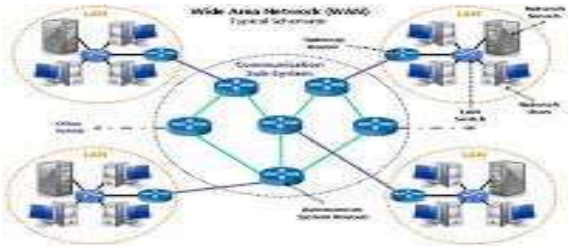
Jaringan komputer yang mempunyai jaringan komputer LAN dalam satu Kota sehingga dapat dihubungkan antara yang satu dengan lain adalah jenis jaringan MAN. Sebuah lokasi sekolah yang terhubung ke kampus dan perkantoran sehingga terbentuk sebuah WAN.

Gambar 2.4 *Metropolitan Area Network*
(Sumber : Wongkar et al., 2015)

3. WAN *(Wide Area Network)*

Jaringan WAN merupakan jaringan komputer mencakup area yang lebih luas dimana jaringan ini menghubungkan jaringan yang satu dengan

jaringan yang lebih banyak lagi adalah jenis jaringan WAN. (Wongkar et al., 2015)



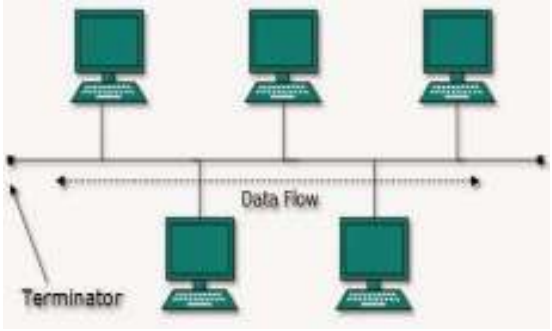
Gambar 2.5 *Wide Area Network*
(Sumber : Wongkar et al., 2015)

2.1.4 Topologi Jaringan

Sebuah struktur atau gambaran dalam menghubungkan sebuah komputer dengan yang lain secara fisik dan hubungan antara komponen-komponen yang saling berkaitan dengan perangkat jaringan seperti, *server* dan *switch* disebut dengan topologi jaringan. Adapun jenis topologi jaringan adalah topologi *bus*, topologi *star* dan topologi *ring*. (Widodo et al., 2018).

1. Topologi *Bus*

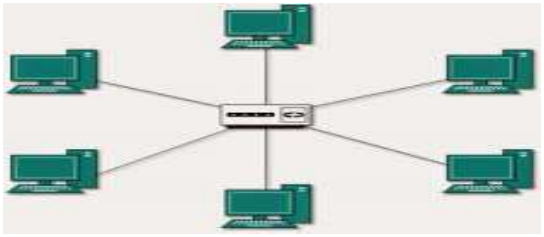
   Topologi ini cukup mudah untuk menghungkan komputer dengan kabel komunikasi antar komputer. Kabel yang digunakan topologi ini adalah *coaxial* sebagai penghubung. (Masse & Iyan, 2016).



Gambar 2.6 Topologi *Bus*
(Sumber : Masse & Iyan, 2016)

2. Topologi *Star*

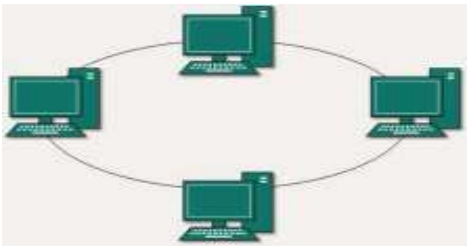
Beberapa komputer yang dihubungkan dengan satu pusat komputer dengan komputer lainnya sehingga *control* terpusat berbagi sumber daya. Topologi ini menggunakan switch. (Masse & Iyan, 2016)



Gambar 2.7 Topologi *Star*
(Sumber : Masse & Iyan, 2016)

3. Topologi *Ring*

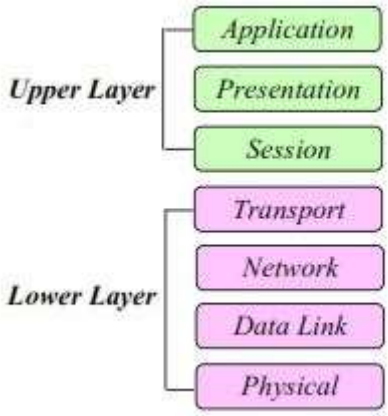
Untuk menghubungkan komputer dengan kabel tunggal dan berbentuk bagan seperti dalam rangkaian melingkar menggunakan LAN *card* jenis topologi ini. (Masse & Iyan, 2016)



Gambar 2.8 Topologi *Ring*
(Sumber : Masse & Iyan, 2016)

2.1.5 Model OSI *Layer*

Model Osi *Layer* yang dikembangkan oleh badan ISO *(International Organization for Standardization)* di Eropa pada tahun 1977 menyatakan bahwa model ini referensi jaringan terbuka dari arsitektural jaringan. Model ini terdiri dari tujuh lapis atau *OSI seven layer model* sebab mempunyai tujuh bagan, setiap lapisan memiliki data protokol. Dimana Model Osi ini dibagi menjadi 7 standar *laye*r atau lapisan antara lain adalah *Physical Layer*, *Data Link Layer*, *Network Layer*, *Transport Layer*, *Session Layer*, *Presentation Layer*, dan *Application Layer*. (Sondakh et al., 2014)



Gambar 2.9 Model OSI Layer
(Sumber : Masse & Iyan, 2016)

1. *Application Layer*

Layer ini berfungsi mengatur aplikasi dalam menggunakan jaringan. HTTP, FTP, SMTP, DNS, TELNET, NFS, dan POP3 adalah protokol yang ada dalam layer. (Masse & Iyan, 2016)

2. *Presentation Layer*

Layer ini berfungsi mentranslasikan data yang ditransmisikan aplikasi ke format jaringan yang dikenal. (Masse & Iyan, 2016)

3. *Session Layer*

Layer berfungsi untuk membuat koneksi, menjaga koneksi, dan menghilangkan. Protokol RPC dan AppleTalk DSP ada pada lapisan *session layer*. (Masse & Iyan, 2016)

4. *Transport Layer*

Layer ini berfungsi memecahkan data dalam paket-paket data serta memberikan *nomor urut* ke paket-paket sehingga dapat disusun kembali pada tujuan yang diterima. Protokol UDP, TCP, dan SPX terdapat pada *transport layer*. (Masse & Iyan, 2016)

5. *Network Layer*

Layer ini bertujuan membuat IP *address*, membuat *hacker* paket data dan menjalankan *routing* pada *internetworking* dengan *router* dan switch. Protokol DDP, Net BEUI, ARP, dan RARP terdapat pada *network layer*. (Masse& Iyan, 2016)

6. *Data Link Layer*

Layer ini berfungsi mengelompokkan *bit-bit* data menjadi format dapat disebut dengan *frame.* Melakukan koreksi kesalahan, *flow control* dalam menentukan perangkat jaringan yang beroperasi dan pengamatan perangkat keras terdapat pada layer ini. Standar IEEE 802 membagi *layer* menjadi dua, yaitu *layer logical link control* dan *layer media access control*. (Masse & Iyan, 2016)

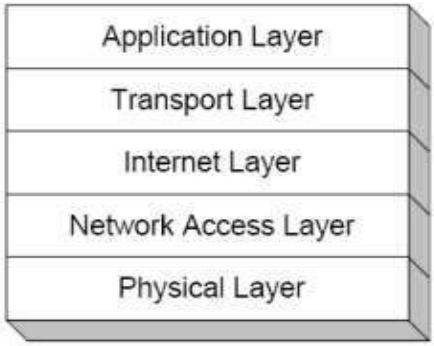
7. *Physical Layer*

Layer berfungsi sebagai media transmisi, pensinyalan, sinkronisasi *bit* data, arsitektur jaringan dan topologi jaringan. *Ethernet*, FDDI, ISDI, dan ATM protokol yang terdapat pada *layer*. (Masse & Iyan, 2016)

2.1.6 TCP/IP *(Transmission Control Protocol/Internet Protocol)*

Kumpulan *protokol* komunikasi yang dipakai dalam komunitas global jaringan komputer disebut dengan *Transmission Control Protocol/Internet Protocol* (TCP/IP). Protokol standar yang dipakai komputer-komputer dalam lingkungan sistem operasi UNIX adalah TCP/IP yang berfungsi untuk menghubungkan jaringan komputer dan jalannya jaringan.

Mengatur kegiatan *internet* dan menfasilitasi dalam memyelesaikan pekerjaan WWW *(World Wide Web)* adalah *internet protocol*. (Hasrul & Lawani, 2017)



Gambar 2.9 Layer TCP/IP
(Sumber : Sondakh et al., 2014)

2.1.7 Pembagian Kelas IP *Address*

Kelas IP *Address* dibagi berdasarkan jumlah *host* yang dimiliki. IP *Adress* mendapat pembagian jaringan, sebagai berikut:

1. IP *Address* Kelas A diberikan *host* sepanjang 24 bit dengan total *host* 16 juta *host*.
2. IP *Address* Kelas B di berikan *host* sepanjang 16 bit dengan total *host* 65.000 *host*.
3. IP *Address* Kelas C di berikan *host* sepanjang 8 bit dengan total *host* 256 *host*. (Sari et al., 2013)

2.2 Teori Khusus

Dalam pembahasan teori khusus dalam penelitian ini, penulis memberikan penjelasan mengenai pengertian dari beberapa istilah jaringan sesuai dengan judul penelitan ini dan menggunakan referensi dari jurnal yang memiliki ISSN.

2.2.1 Pengertian Analisis

Menurut, Mardi (dalam Neni, 2017) analisis adalah pengujian informasi yang ada dengan yang lain untuk mendapat petunjuk perbaikan dalam meningkatkan kemampuan sistem. Analisis adalah uraian satu pokok yang tepat dan pemahaman secara keseluruhan dapat kita lihat dalam kamus Bahasa Indonesia. Sugiyono (dalam Neni, 2017) penelitian kuantitatif menggunakan teknik *statistic* dalam menganalisis data. Teknik statistik deskriptif digunakan pada penelitian ini. Statistik deskriptif adalah menganalisa data atau menggambarkan sebenarnya tanpa membuat kesimpulan.

Ika (Tumino, 2017) analisis adalah sejumlah kegiatan yang dibuat seperti mengurai, membedakan dan mencari kelompok yang ada kaitanya. Analisis adalah merangkum data menjadi informasi yang dapat dipresentasikan. Analasis adalah uraian satu pokok dalam penelaan hubungan sehingga memperoleh

pengertian yang tepat dan membedakan komponen-komponen atau bagian-bagian yang relevan dari seluruh data sehingga membuat data mudah diatur. Analisis menjelaskan pola-pola secara konsisten agar dapat dipelajari dan mempunyai arti.

Cara membandingkan dua atau lebih kelompok sampel menggunakan analisis perbandingan. Pengertian Analisis perbandingan adalah perbandingan data variabel yang dilakukan. Metode perbandingan ini dapat dilakukan dengan mengumpulkan data (sampel) dan melakukan pengukuran kuantitatif yang beskala interval (Bimo dan Neni, 2017).

2.2.2 Jaringan Komputer

Menurut Andi & Madcoms (2015:2). Jaringan komputer merupakan sejumlah komputer yang dirancang sedemikian rupa dengan tujuan dapat membuat aplikasi *software* ke komputer lain. Model referensi OSI terbagi 7 lapisan dimana fitur lapisan memiliki funsi yang berbeda.

Jaringan komputer (*computer network*) ada ketika adanya pengiriman data dari komputer satu ke komputer lain atau yang disebut dengan internet, tahun 1969 memutuskan mengadakan riset untuk memenghubungkan beberapa komputer dalam bentuk *organic* pada Departemen Pertahanan Amerika, U.S. *Defense Advanced Research Projects Agency* (DARPA). Program ini disebut dengan ARPANET.

2.2.3 Standar Wireless

Pada saat ini *wireless* menggunakan sfesifikasi 802.11a, 802.11b, dan 802.11g. Sebuah lembaga *Institute of Electrical and Ecectronics Engineer* (IEEE) membuat fitur. Andi (2012: 34).

2.2.4 Standar Keamanan Wireless

Didalam sebuah jaringan terdapat beberapa keamanan yang perlu di ketahui sebagai berikut:

a. WEP

WEP adalah salah satu jenis *key* yang gampang di*crack* atau di sadap. WEP memeliki 64bit sampai 128bit, untuk login ke kunci WEP menggunakan set atau *generate* melalui *passphrase*. Ketika megetik abjab *passphrase generate* otomatis dan memasukkan 0-9 dan A-F (hexadecimal) maka kita dapat melihatnya. Kunci WEP tidak boleh lebih atau kurang, Jika 64bit bisa 10key maka untuk 128bit gunakan 26key. Pengguna hanya dapat memasukkan kunci ke *client* maupun *access point*. Untuk autentikasi ke *access poin* memakai kunci saat megakses ke *acces poin*. Andi (2012: 13)

b. WPA-PSK

Model WPA-PSK digunakan pada saat tidak ada *authentikasi server*. Model WPA dapat digunakan dengan bantuan komputer lain sehingga *acces poin* dapat dijalankan karena mengkonfigurasi seadanya saja. Cara kerja *access point* berbeda dalam mendapatkan *Shared-Key* Karena *acces point* sebagian memiliki fasilitas yang berbeda karena WPA-PSK lebih cepat update dari WEP. WPA-PSK dan WEP memiliki *decryption* sehingga bisa di*crack* atau disadap dan WEP memerlukan waktu lebih lama. Kunci paling banyak 8-63 dan megimput 64 *hexadecimal* atau ASCII. Andi (2012: 13)

c. WPA2-PSK

WPA2 menggunakan sfesifikasi IEEE 802.11i. WPA2 menggantikan *wired equivalent privacy* (WEP) dimana fitur keamanan asli dengan sfesifikasi IEEE 802.11. Standar IEEE 802.11i tidak dukung produk WPA walaupun WPA2 bertujuan mendukung. WPA2-PSK kunci terbaru *wireless* yang lebih baik dari WEP dan WPA-PSK, kedua kunci ini bisa di*crack* atau disadap dengan membutuhkan waktu yang lebih lama lagi. WPA2-PSK mempunyai dua jenis *decryption* antara lain *Advanced Encryption Standard* (AES) dan *Temporal Key Integrity Protocol* (TKIP) dimana TKIP memiliki lebih banyak dari pada AES. Kunci paling banyak 8-63, mampu menampung 64 *hexadecimal* atau ASCII. Adapun solusi pencegahan dengan menduplikasi MAC address dapat dibuat dengan memasang *Mikrotik Router* sebagai kemanan tambahan. Ini dilakukan pada *Mikrotik* karena memilki pengaturan yang dapat membatasin *MAC address* kembar dalam jaringan WLAN. Sehingga, teknik pengamanan memakai *MAC Address Filtering* bisa berjalan secara optimal. Pada penelitian ini, pengujian dilakukan menggunakan PC tester yang terdapat di dalam Laboratorium Sistem Informasi dan *Programming*. Pengujian dilakukan dengan 4 tahapan berbeda yaitu:

a. *Cracking The Encryption*

Adapun tujuan dari serangan ini adalah untuk mengetahui Access Point dilindungi dengan sistem keamanan enkripsi seperti WEP, WPA ataupun WPA2. Penguji dapat membuat *scanning* terhadap *Access Point* dan

menentukan tujuan untuk melakukan *cracking* terhadap *key* yang digunakan sebagai penguji.

b. Bypassing MAC Authentication

Tahapan yang kedua, tujuan dari percobaan ini adalah untuk mengetahui apakah sistem keamanan menggunakan metode pembatasan hak akses dengan *MAC filtering* atau tidak. Setelah dilakukan percobaan menghubungkan antara perangkat pengujian dan *access point* ditemukan bahwa sistem keamanan dari jaringan *wireless* tidak menggunakan *MAC filtering*, sehingga semua perangkat yang dapat terhubung dengan Wi-fi bisa mengakses jaringan *wireless* ini asal mengetahui *encryption key*-nya.

c. Attacking The Infrastructure

Dalam tahap ini dilakukan serangan pada layanan *wireless* untuk *client* sehingga dapat mempengaruhi kinerja jaringan. Bentuk serangan ini adalah *DoS attack* yang bertujuan melumpuhkan koneksi *user* lain di dalam jaringan. Informasi awal yang dibutuhkan adalah *password* dari jaringan *wireless* yang diuji, agar komputer *tester* dapat terhubung dengan layanan *wireless*.

d. Man In the Middle (MITM) Attack

Dalam tahap ini melakukan serangan terhadap user lain dengan jaringan WLAN yang dapat melakukan penyadapan paket data. Pengujian ini menggunakan aplikasi *ettercap* sebagai alat uji. Kondisi awal yang dibutuhkan adalah komputer *tester* dan komputer target harus terhubung di jaringan *wireless* ‘LAB SIM dan *Programming*. Disini komputer *tester*

berperan sebagai pihak ketiga diantara target dan *access point* yang menghubungkan antara target dan layanan internet.

2.3 TOOLS

2.3.1 *NMAP*

NMAP adalah *tool* yang bagus untuk melakukan *Port Scanning*. NMAP tidak hanya diperlukan untuk melakukan *Port scannin*g tetapi berfungsi mencari kerentanan sistem secara otomatis. Untuk mencari celah SQL *Injection* pada suatu *website*, XSS *scanning*, SMTP *Relay Attack, Ddos Attack install* dan masih banyak lagi menggunakan NMAP, *toolOpen Source* yang dapat di*install* baik di sistem operasi *windows* maupun *linux* (Doel dalam Neni, 2017).

NMAP dapat digunakan sebagai *tool* dalam mencari kerentanan pada suatu *server* jaringan oleh *hacke*r. NMAP berguna untuk memantau kerentanan *server* yang dikelolanya, Mencari kelemahannya sebelum celahnya diketahui oleh orang lain.

Neni (2017) mengaudit keamanan dan mengeksplorasi jaringan menggunakan *Nmap*, komputer yang tidak terhubung dengan jaringan dapat juga digunakan. *Scanning* menggunakan jaringan besar atau kecil pada paket *raw* IP untuk melihat *host* yang *up* dalam jaringan desain oleh *Nmap*. *Service* yang diproses menggunakan nomor *port*, yang terbuka dapat di *filter*/ *firewall* yang digunakan berbagai karakteristiknya. NMAP melakukan *fingerprinting* dan memberikan estimasi sistem yang digunakan target. NMAP mempunyai kelebihan memanipulasi *scanning.*

2.3.2 Kali Linux

S’to (2014) Offensive Security menyatakan *Kali Linux* adalah *Backtrack* versi 6 sebab tidak dijelaskan secara detail karena sistem operasi yang dipakai sangat mendasar karena *backtrack* dibuat tergantung sistem operasi buntu, sistem operasi dasarnya Debian menggunakan *kali linux.*

Kali linux mendapatkan penyempurnaan karena mengganti sistem operasi dasar dari awal dan pertama kali direlease pada tanggal 13 maret 2013. Kali linux merupakan penerus *BackTrack* dimana sistemnya kinerjanya masih fleksibel. Sistem ini bisa jalankan sesuai kebutuhan. *Kali linux* dapat digunakan dengan, (a) *Live* CD/ DVD, (b) *Harddisk*. Metode ini mempunyai keunggulan dan kelemahannya maka pilihlah yang terbaik buat kamu.

2.3.3*Test Speed Internet (Speed Test)*

Speed Test adalah pengujian kecepatan jaringan internet. Kebanyakan orang mengartikan dengan paket internet, contohnya kecepatan internet 386, 512, 1 Mbps pada saat berlangganan *speedy.* Yang bertujuan untuk mengecek kecepatan internet dan kecepatan koneksi adalah *Speed test* disediakan oleh perusahaan kalispel. Adil (2017: 28). Dapat disimpulkan bahwa *speed test* adalah pengujian kecepatan internet.

2.4 Penelitian Terdahulu

Ada beberapa jurnal yang di buat oleh beberapa peneliti sebelumnya, yang cukup relevan dan berkaitan dengan tema yang diteliti dan dikembangkan oleh penulis. Penulis menjadikan beberapa jurnal (hasil penelitian) dari peneliti tersebut sebagai referensi dan sekaligus memperbandingkan dengan hasil

penelitian yang ditemukan penulis. Dibawah ini beberapa jurnal hasil penelitian terdahulu yang ingin digunakan oleh peneliti sebagai referensi yaitu:

1. Menurut jurnal Ida Bagus Verry Hendrawan Manuaba dkk, tahun 2012 dengan judul"Keamanan Akses Jaringan Komputer" (ISSN: 2301-4156) memyimpulkan bahwa keamanan sangat dibutuhkan untuk memilihara stabilitas jaringan agar tetap memadai, jurnal ini dapat digunakan sebagai pedoman dan berguna untuk meningkatkan keamanan jaringan sehingga mempengaruhi kinerja jaringan *compute*r.
2. Berdasarkan jurnal yang dibuat oleh Nazwita dkk, tahun 2017 dengan judul "Analisis Sistem Keamanan *Web Server* Dan *Database Server* Menggunakan *Suridata*" (ISSN: 2579-5406). Menyimpulkan bahwa keamanan sistem jaringan sangat penting dalam menjaga validitas, *integritas* data serta menjamin tersedianya layanan bagi pengguna.
3. Berdasarkan jurnal yang dibuat oleh Bagus Mardiyanto dkk, tahun 2016 dalam judul "Analisis dna implementasi *Honeypot* Dalam Mendeteksi Serangan *Distributed Denial- Of- Service*" (DDOS) Pada Jaringan Wireless (ISSN 32-42) menyimpulkan bahwa perkembangan jaringan teknologi yang paling utama sistem keamanan jaringan semakin berkembang dan menuntut agar sistem keamanannya meningkat. *Honeyd* adalah *honeypot* dengan jenis *low Interaction* karena mempunyai resiko lebih kecil dan tidak secara langsung melibatkan sistem secara seluruhan.
4. Berdasarkan jurnal yang dibuat oleh Riko tahun 2014 dengan judul "Analisis Kelemahan Celah Lapisan Keamanan pada Jaringan Nirkabel"

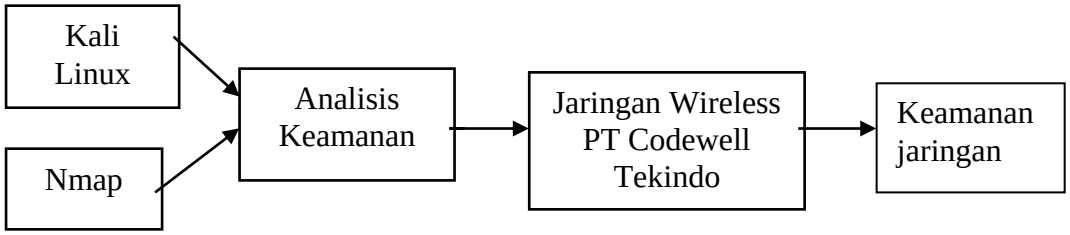
(ISSN: 1907-6738) menyimpulkan bahwa perangkat teknologi berbasis nirkabel banyak digunakan dalam jaringan nirkabel suara maupun data. Teknologi nirkabel mengunakan frekuensi tinggi untuk menghantar komunikasi sehingga kerentanan terhadap keamanan juga tinggi dibandingkan dengan yang lain.

5. Berdasarkan jurnal yang dibuat oleh Nugroho, B.A. Tahun 2012 yang berjudul Analis Keamanan Jaringan Pada Fasilitas Internet (WIFI) pada serangan *Packet Sniffing* menyimpulkan bahwa media *wireless* merupakan salah satu fasilitas penunjang pekerjaan diman media *wireless* memanfaatkan gelombang radio sehingga rentan terhadap ancaman serangan, sehingga perlu diuji keamanannya. Pengujian dilakukan berdasarkan konsep *wireless hacking*, meliputi ARP *spooting* dan serangan wps aktif.
6. Berdasarkan jurnal yang dibuat oleh Bangkit Kurnia Ari Setyawa dkk, tahun 2012 dengan judul Analisis Keamanan Jaringan Wireless Yang Menggunakan *Captive Portal* (ISSN: 1411-3201). Jaringan *wireless* yang digunakan untuk melihat keadaan dan kondisi *wireless* serta mengambil data yang digunakan untuk menganalisa data dan simulasi analisis keadaan dan kondisi *wireless.*
7. Berdasrkan jurnal yang dibuat oleh Yudi Herdiana tahun 2014 dengan judul Kemanan Pada Jaringan *Wireless* (ISSN: 1979-4819). Dimana *wireless* semakin meningkat dimana teknologi *wireless* semakin meningkat memanfaatan frekuensi untuk menghantarkan semua komunikasi.

Kelemahan jaringan *wireless* terbagi 2 antara lain kelemahan konfigurasi dan kelemahan jenis enkripsi.

2.5 Kerangka Pemikiran

Agar topik yang dibahas tetap berada dalam konteks yang diinginkan, maka berikut ini dibuat kerangka pemikiran, seperti pada gambar berikut:



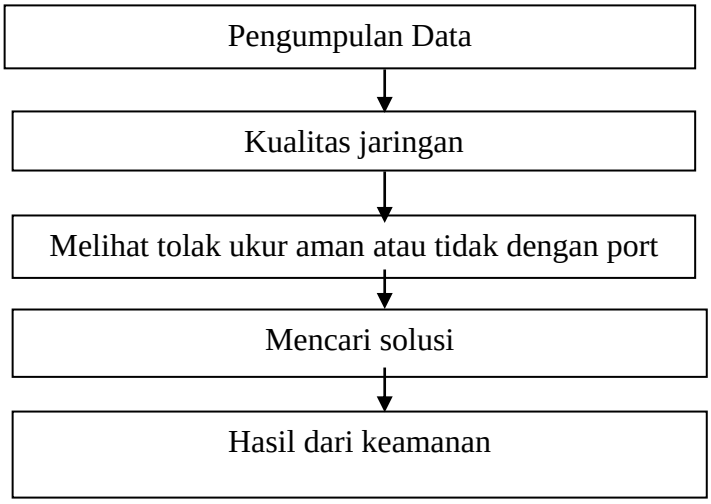
Gambar 2.10 Kerangka Pemikiran (Sumber: Data Penelitian: 2019)

BAB III

METODE PENELITIAN

3.1 Desain Penelitian

Sebelum sampai tahap penelitian ini, peneliti seharusnya merancang sebuah struktur/ tahapan agar dapat menjabarkan jalannya sebuah penelitian dengan membuat berbagai bentuk bagan atau skema. Menurut (Martono, 2010: 131). Tahapan dan skema yang menjadi panduan dalam penelitian adalah sebagai berikut:



Gambar 3.1 Desain Penelitian

(Sumber: Data Penelitian, 2019)

1. Pada tahap ini pertama peneliti melakukan pengumpulan data. Pada proses ini peneliti melakukan pengumpulan data yang ada di Kantor PT Codewell Tekindo Cemerlang. Data yang dikumpulkan adalah data yang dibutuhan

peneliti antara lain, *bandwith* atau kecepatan akses jaringan, masalah pada jaringan dan alat-alat jaringan yang dibutuhkan seperti komputer/laptop.

2. Adapun tahap berikutnya adalah pengamatan terhadap jaringan nirkabel. Dalam proses ini peneliti menggunakan peralatan (tools) Nmap dan sistem operasi *kali linux*. Pengunaan *Nmap* bertujuan untuk melihat celah keamanan jaringan pada sistem yang sedang berjalan, serta bertujuan untuk mengeksplorasi dan mengaudit keamanan jaringan yang berjalan. Menggunakan *tools Nmap* dapat mencari *port-port* yang terbuka dimana sistem operasi *Kali Linux* digunakan untuk melakukan penyusupan pada sistem jaringan melalui celah keamanan yang terbuka.

a. Dari penggunaan alat atau *tools Nmap* terlihat masalah-masalah yang timbul pada jaringan dan celah pada sistem keamanan jaringan.

b. Setelah proses deteksi terhadap masalah yang timbul maka langkah selanjutnya adalah mencari solusi dengan melakukan beberapa esperimen.

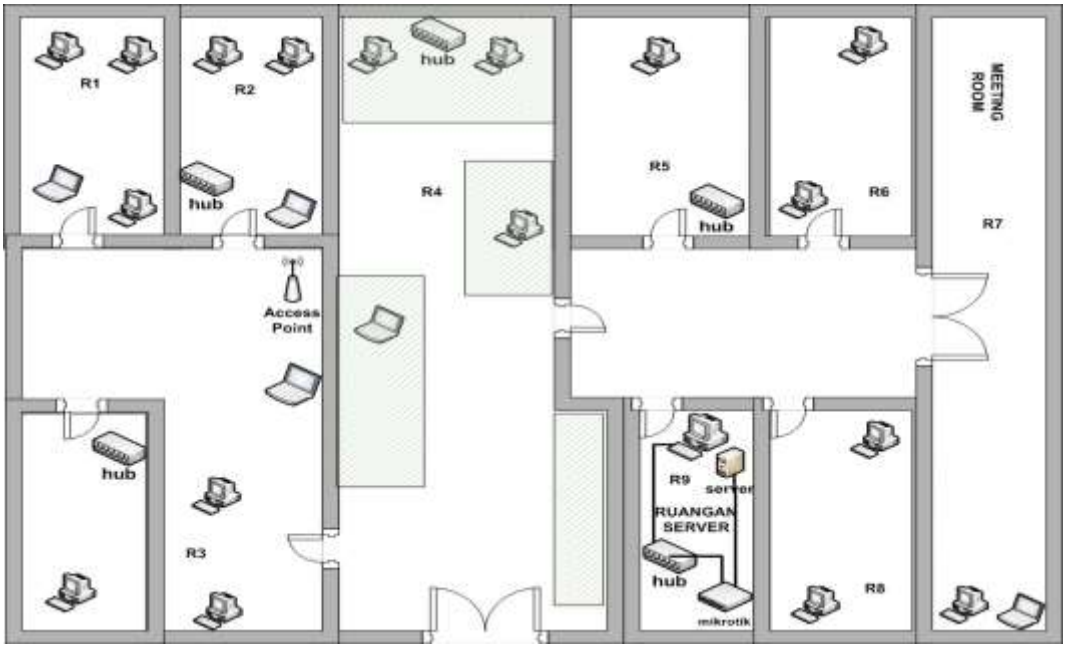
c. Dari berbagai esperimen tersebut diketahui cara / metode yang lebih berpotensi dalam mengatasi masalah pada sitem jaringan.

3.2 Analisa Jaringan Yang Sedang Berjalan

Dalam pengamatan peneliti, model yang dipakai saat ini di PT Codewell Tekindo masih tergolong kurang baik karena kurang megimplementasikan terobosan- terobosan dalam perkembangan teknologi khususnya teknologi jaringan. Sebagai contoh, jaringan *Wireless* LAN yang diterapkan masih menggunakan jaringan perangkat keras *mikrotik* dan *hub*. Perusahaan tersebut menggunakan 5 *hub* untuk menghubungkan komputer dengan *server* maupun

perangkat komputer lainnya. Perangkat mikrotik ini berada pada *serve*r, pengguna dapat menggunakan fasilitas jaringan ini dalam lingkup yang terbatas. Jaringan ini dapat di akses di beberapa ruangan sepanjang jarak antar ruangan tidak jauh. Sebagai contoh jaringan dapat di akses di ruangan HRD dan *Accounting* PT Codewell tekindo secara bersamaan.

Kapasitas *bandwidth* yang didapati tergolong rendah, yakni 4 Mbps. Standar keamanan jaringan yang dipakai adalah WPA2/PSK. Di PT Codewell Tekindo Cemerlang terdapat jaringan *Wireless LAN* seperti dibawah ini:



Gambar 3.2 Model Jaringan *Wireless LAN* Pada Kantor PT Codewell Tekindo Cemerlang
(Sumber: Data Penelitian, 2019)

Kantor PT Codewell Tekindo Cemerlang melakukan test kinerja jaringan *Wireless* untuk menjaga tidak terjadinya masalah sehingga menimbulkan resiko pada saat mengakses internet sehingga penginputan dan pengambilan data perusahaan terlambat yang ada di PT Codewell Tekindo Cemerlang.

PT Codewell Tekindo Cemerlang memiliki 18 komputer dan 5 laptop. PT Codewell Tekindo Cemerlang menggunakan topologi *star* karena Topologi *star* dapat mengalami kegagalan pada saat akses karena node jaringan masih terhubung ke *hub*. Melakukan *broadcast* ke semua *node* yang tersambung jaringan, termasuk *node* aslinya. Peripheral berkomunikasi karena adanya *node* sentral. *Line* yang putus dari *node* sentral tidak berpengaruh pada komputer lain hanya komputer yang terputus.

PT Codewell Tekindo Cemerlang menggunakan jaringan kabel dan jaringan nirkabel. Teknologi yang terhubung antara dua piranti untuk saling bertukar data dan suara tanpa menggunakan media kabel disebut *wireless*. Penggunaan kabel yang mengganggu dapat mengeleminasi dua piranti secara bersamaan. Jaringan nirkabel menggunakan gelombang radio yang berada pada jaringan yang bersamaan sehingga sering diserang oleh para *attacker* atau peretas jaringan.

3.3.1 Objek dan Jadwal Penelitian

3.2.1 Objek Penelitian

Penulis membuat penelitian di PT Codewell Tekindo Cemerlang yang beralamat di Ruko Citra Indah Blok A no 01 Kota Batam. Penulis memilih perusahaan ini sebagai objek penelitian karena berbagai faktor, antara lain:

1. Keterbukaan perusahaan
2. Jenis data yang dibutuhkan relevan dengan penelitian
3. Efisiensi waktu dan biaya

3.3.2 Jadwal Penelitian

Kegiatan peneliti perlu dibuatkan jadwal. Jadwal ini berisi tentang kegiatan yang dilakukan selama membuat penelitian (Sugiyono, 2014). Berikut ini tabel jadwal kegiatan berlangsungnya penelitian.

No	Kegiatan	Tahun 2019																
		Sep 2019				Nov 2019				Des 2019				Jan 2020				Feb 2020
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1
1	Pengajuan Judul																	
2	Penyusunan Bab I																	
3	Penyusunan Bab II																	
4	Penyusunan Bab III																	
5	Penyusunan Bab IV																	
6	Penyusunan Bab V, Daftar Pustaka, Lampiran																	

Jadwal penelitian 2019