BAB II

TINJAUAN PUSTAKA

2.1 Teori Dasar

2.1.1 Pengertian Jaringan Komputer

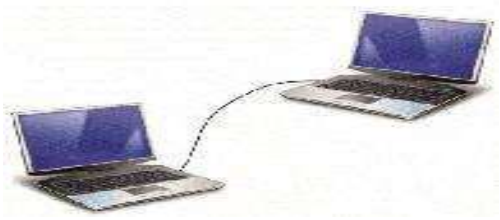
Komputer dapat dihubungkan dengan komputer lain supaya dapat bertukar data dan informasi fungsi dari jaringan komputer. Setiap instansi atau perusahaan menggunakannya dengan tujuan untuk memperlancar arus informasi. Beberapa Banyak komputer, printer dan perangkat lainnya yang saling terhubung dalam satu 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*

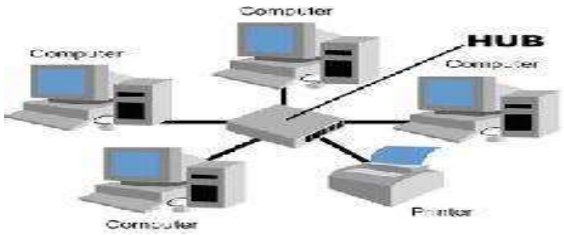
Bebepara perangkat komputer terhubung pada satu sistem jaringan tanpa perantara hingga bisa dibuat menjadi satu kesatuan fungsi dan berbagi jaringan atau dapat disebut dengan *peer to peer.*



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)*

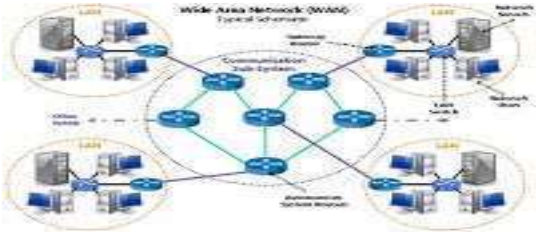
Jaringan komputer yang mempunyai jaringan komputer LAN dalam satu Kota sehingga dapat dihubungkan antara yang satu dengan lain adalah jenis jaringan MAN. Sebuah lokasi sekolah yang terhubung ke kampus dan perkantoran sehingga terbentuk sebuah WAN.

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)



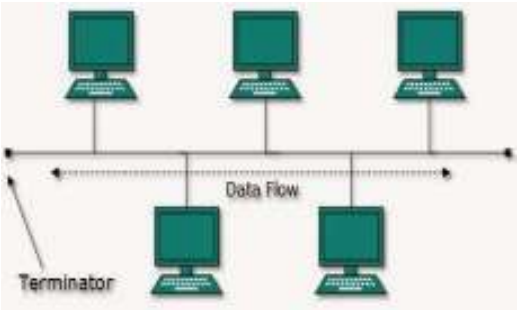
Gambar 2.5 *Wide Area Network*
(Sumber : Wongkar et al., 2015)

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*

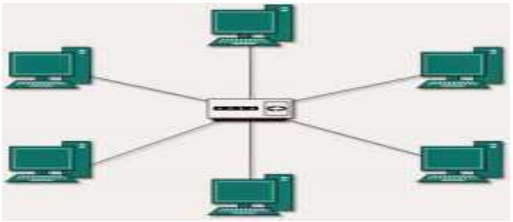
   Topologi ini cukup mudah untuk menghungkan komputer dengan kabel komunikasi antar komputer. Kabel yang digunakan topologi ini adalah *coaxial* sebagai penghubung. (Masse & Iyan, 2016).



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

2. Topologi *Star*

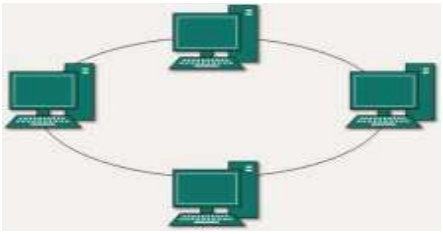
Beberapa komputer yang dihubungkan dengan satu pusat komputer dengan komputer lainnya sehingga *control* terpusat berbagi sumber daya. Topologi ini menggunakan switch. (Masse & Iyan, 2016)



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

3. Topologi *Ring*

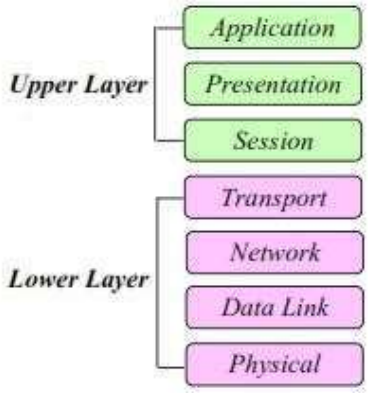
Untuk menghubungkan komputer dengan kabel tunggal dan berbentuk bagan seperti dalam rangkaian melingkar menggunakan LAN *card* jenis topologi ini. (Masse & Iyan, 2016)



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)

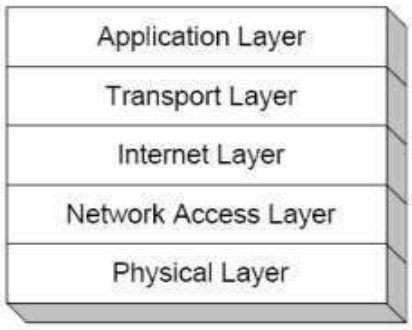
7. *Physical Layer*

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"

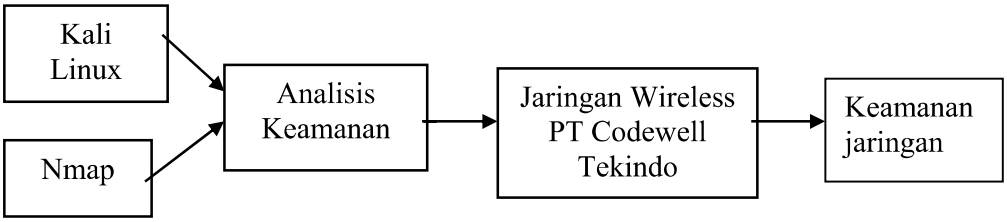
(ISSN: 1907-6738) menyimpulkan bahwa perangkat teknologi berbasis nirkabel banyak digunakan dalam jaringan nirkabel suara maupun data. Teknologi nirkabel mengunakan frekuensi tinggi untuk menghantar komunikasi sehingga kerentanan terhadap keamanan juga tinggi dibandingkan dengan yang lain.

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)