BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dari tahun ke tahun mengalami kemajuan yang pesat, selalu saja ada teknologi terbaru yang lebih baik. Salah satu teknologi yang mengalami perkembangan inovasi yaitu teknologi jaringan. Jaringan yang semakin rumit berdampak pada rumitnya pemantauan dan me-manage yang dilakukan oleh administrator jaringan. Seorang administrator dituntut untuk selalu bekerja cepat, tepat, teliti, dan professional dalam menangani permasalahan infrastruktur jaringan (Sarah, 2019).

Teknologi jaringan komputer semakin memudahkan masyarakat dalam memenuhi kebutuhan informasi. Salah satu teknologi yang dikembangkan adalah teknologi media transmisi nirkabel atau *wireless*. Mudahnya pengguna umum terhubung dengan jaringan *wireless* tentunya masalah keamanan perlu diperhatikan, apalagi didalam sebuah korporasi atau sebuah lembaga yang peduli dengan keamanan data. Jaringan *wireless* menggunakan gelombang radio sebagai media transmisi sehingga jaringan akan lebih mudah dimasuki oleh penyusup dan serangan yang berasal dari semua arah (Sabdho dkk., 2018).

Perkembangan tersebut membuat keamanan suatu jaringan semakin rentan mengalami serangan dari oknum-oknum yang tidak bertanggung jawab. Keamanan jaringan sangat vital bagi sebuah jaringan komputer. Kelemahan - kelemahan yang terdapat pada jaringan komputer jika tidak dilindungi dan dijaga dengan baik akan menyebabkan kerugian berupa kehilangan data, kerusakan sistem server, tidak maksimal dalam melayani user atau bahkan kehilangan aset - aset berharga di suatu organisasi (Hasibuan dkk., 2022).

Media transmisi yang digunakan *wireless* adalah gelombang radio yang dipancarkan ke semua area yang bisa dijangkau oleh gelombang radio tersebut. Beberapa vendor menyediakan fitur-fitur yang memudahkan pengguna maupun administrator jaringan untuk menggunakannya, sehingga sering dijumpai masih menggunakan konfigurasi *default* dari vendor. Oleh karena itu, para *hacker* sering melakukan aksinya untuk menguji kemampuan yang telah dipelajari sebelumnya.

Kemudian terhubung dalam satu jaringan yang sama dan mengambil data pengguna lainnya secara ilegal (Wahyudi, 2018).

Di era saat ini kebutuhan akan jaringan komputer semakin bertambah penting baik dalam pendidikan maupun dalam sebuah pekerjaan dan salah satu hal penting dalam mengelola jaringan komputer yaitu keamanan dari jaringan itu sendiri, dengan banyaknya akses ke jaringan tersebut maka akan banyak pula peluang kejahatan yang terjadi didalam jaringan tersebut, misalkan adanya pencurian data yang terjadi dijaringan tersebut ataupun adanya peretas yang mematikan sumber daya jaringan tersebut. Banyak teknik yang dapat diupayakan dalam memperkecil tingkat kejahatan dalam jaringan ini, salah satu teknik yang banyak digunakan untuk pengamanan jaringan lokal adalah dengan menggunakan *security port* dimana ini merupakan teknik yang akan mengizinkan siapa saja yang berhak menggunakan akses jaringan melalui *port* yang tersedia di *switch* (Nitra dan Ryansyah, 2019).

Dikarenakan lebih rentan diserang oleh *hacker*, maka dibutuhkan sebuah metode untuk melakukan ujicoba apakah jaringan *wireless* yang telah terpasang sudah aman atau sesuai dengan standard operasional. Metode ini biasa disebut dengan metode *penetration testing*. Metode *Penetration Testing* adalah proses simulasi serangan pada sistem yang memerlukan sertifikasi keamanan jaringan untuk mencegah peretas atau penyerang jaringan yang menyebabkan kehilangan data pribadi dan data perusahaan. Orang yang melakukan metode ini juga disebut sebagai *pentester* (Mushlih dkk., 2019).

Ada banyak cara yang bisa digunakan untuk menghindari serangan terhadap keamanan komputer, salah satunya yaitu dengan memperkuat sistem keamanan jaringan komputer tersebut, namun sebelum memperkuat keamanan suatu jaringan maka perlu dilakukan monitoring jaringan komputer terlebih dahulu untuk mengetahui celah-celah yang dapat terkena serangan, melakukan penetrasi testing dapat membantu kita untuk mengetahui celah-celah yang dapat terkena serangan pada suatu jaringan.

Penetration testing adalah alat penilaian jaminan bernilai yang menguntungkan baik bisnis dan operasinya. Dari segi operasional, *penetration testing* membantu membentuk strategi keamanan informasi melalui identifikasi

kerentanan yang cepat dan akurat. *Penetration testing* membagikan informasi rinci tentang ancamanan keamanan secara aktual, yang dapat dieksploitasi jika tercakup dalam aliran dan proses keamanan organisasi, hal ini akan membantu organisasi untuk mengidentifikasi dengan cepat dan akurat, potensi kerentanan yang nyata (Hasibuan dkk., 2022).

Sekolah Menengah Kejuruan Negeri (SMKN) 4 Luwu, adalah salah satu sekolah yang ada di luwu yang ber alamatkan Jl. Poros, Jl. Palopo-Masamba No.Km 16, Kalibamamase, Kec. Walenrang, Kabupaten Luwu, Sulawesi Selatan 91951, dimana lokasi tersebut memiliki jaringan *wireless* yang sering terjadi kebocoran password hal ini terjadi karena banyak user baru dari *wireless* yang berhasil menebak password atau kata sandi jaringan *wireless* tersebut, sehingga peluang terjadinya serangan masih sangat rentan.

Setelah melihat permasalahan di atas, maka penulis berkeinginan melakukan penelitian di SMK Negeri 4 Luwu dengan judul "Implementasi Keamanan Jaringan *Wireless* Menggunakan *System Penetration* Testing pada SMK Negeri 4 Luwu".

1.1 Rumusan Masalah

Berdasarkan latar belakang yang dikemukakan di atas, maka rumusan masalah pada penelitian ini adalah "bagaimana cara mengimplementasikan keamanan jaringan *wireless* menggunakan *system penetration testing*?".

1.2 Tujuan Penelitian

Berdasarkan rumusan masalah di atas maka penelitian ini bertujuan untuk mengimplementasikan keamanan jaringan baru sebagai solusi dari pemasalahan yang ditemukan.

1.3 Manfaat Penelitian

Diharapkan penelitian ini nantinya dapat bermanfaat bagi beberapa pihak yang akan menggunakannya antara lain:

1. Manfaat Bagi Penulis

Manfaat bagi penulis adalah sebagai pengaplikasian ilmu atau menerapkan ilmu yang diperoleh selama duduk dibangku pendidikan kuliah, serta penambah wawasan dalam pengaplikasian teknologi dan mengetahui bagaimana analisis keamanan jaringan *wireless* dengan melakukan penetrasi testing.

2. Manfaat Terhadap Dunia Akademik

Manfaat penelitian ini terhadap dunia akademik adalah menambah wawasan para mahasiswa untuk melanjutkan penelitian ini dikemudian hari serta dapat menjadi referensi dalam analisis sistem keamanan jaringan *wireless* dengan melakukan penetrasi testing dan sebagai literatur bagi pembuatan laporan sejenis dalam lingkungan Universitas Cokroaminoto Palopo.

3. Manfaat Bagi SMK Negeri 4 Luwu

Dengan penelitian ini dapat memberikan informasi dan solusi mengenai permasalahan jaringan yang sedang terjadi.

1.4 Batasan Penelitian

Batasan pada penelitian ini adalah sebagai berikut:

1. Analisis keamanan ini dilakukan dengan mengikuti permasalahan yang ada pada SMK Negeri 4 Luwu
2. Implementasi dilakukan sebagai bentuk solusi dari perrmasalahan yang ditemukan.
3. Metode pengujian menggunakan metode penetrasi testing.
4. Hasil yang ditampilkan berupa keamanan jaringan yang ada di SMK Negeri 4 Luwu

BAB II
TINJAUAN PUSTAKA

2.1 Kajian Teori

Kajian teori berisi topik-topik yang akan dibahas dalam penelitian ini. Kajian teori mempunyai peranan penting dalam hal melakukan penelitian. Dengan Kajian teori, Penulis dapat menjustikasi adanya masalah penelitian dan mengidentifikasi arah penelitian.

1. Implementasi

Menurut Asiah (2022) Implementasi adalah tindakan menyediakan alat-alat yang diperlukan untuk menjalankan suatu kebijakan dan dapat /berdampak pada objek tertentu. Implementasi adalah suatu proses dinamis dimana suatu kebijakan di wujudkan dalam tindakan untuk melaksanakan suatu kegiatan atau tindakan yang pada akhirnya akan menghasilkan suatu hasil yang sejalan dengan maksud atau tujuan kebijakan tersebut.

Saepulloh (2019) Implementasi menargetkan aktivitas, operasi, atau mekanisme sistem tertentu. Implementasi bukan hanya tindakan; itu adalah kegiatan dengan strategi yang bertujuan untuk mencapai tujuan kegiatan itu.

Menurut definisi implementasi yang dikemukakan oleh beberapa ahli tersebut di atas, dapat dikatakan bahwa implementasi mengacu pada pelaksanaan suatu proses yang melibatkan berbagai sumber daya, seperti personel, sumber daya keuangan, dan kemampuan organisasi, yang dilakukan oleh publik. dan sektor swasta untuk menghasilkan hasil yang konsisten dengan maksud atau tujuan kebijakan 2488 itu sendiri.

Implementasi adalah proses melaksanakan pilihan mendasar pada tataran praktis. Ada beberapa langkah untuk proses, termasuk:

1. Proses pengesahan hukum dan peraturan
2. Bagaimana lembaga pelaksana melaksanakan keputusan
3. Kesiapan kelompok sasaran untuk mengimplementasikan pilihan.
4. Apakah pilihan memiliki efek yang diinginkan atau tidak, mereka selalu memiliki pengaruh.

5. Dampak keputusan sesuai dengan yang diantisipasi oleh badan pelaksana.
6. Upaya penguatan hukum, kebijakan, dan regulasi

Setidaknya ada beberapa hal penting yang terlibat dalam tahap persiapan implementasi, yaitu:

1. Menyiapkan sumber daya, unit, dan teknik
2. Membuat rencana dan arahan berdasarkan kebijakan yang dapat dianut dan dijalankan.
3. Secara teratur memberikan layanan, melakukan pembayaran, dan mengurus hal-hal lain
4. Maka dari defenisi di atas dapat di jabarkan bahwa ketika sebuah organisasi menerapkan strategi, ia mengukur kemampuannya untuk memobilisasi orang dan sumber daya dalam unit organisasinya secara terkordinasi dan menginspirasi mereka untuk menemukan solusi kreatif untuk mencapai tujuan yang telah ditentukan sebelumnya.

2. Keamanan Jaringan

Keamanan jaringan komputer adalah suatu bagian dari sebuah sistem yang sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunaannya (Mulyanto, dkk., 2022).

Pentingnya suatu keamanan jaringan membuat banyak pengguna jaringan yang berusaha untuk selalu mengupdate keamanan mereka, karena pada masa ini segala bentuk serangan bisa meyerang sistem keamanan kita, jadi memperkuat keamanan jaringan adalah solusi yang sangat tepat untuk menghindari hal tersebut. Keamanan jaringan biasanya terdiri dari tiga kontrol yang berbeda yaitu:

a. Fisik

Keamanan jaringan fisik didesain untuk mencegah *personel* yang tidak berwenang untuk mendapat akses fisik ke jaringan seperti *router*, lemari kabel, atau yang lain.

b. Teknis

Kontrol keamanan jaringan teknik diperlukan untuk melindungi data yang disimpan jaringan atau data yang transit melintasi.

c. Administratif

Kontrol keamanan jaringan administratif terdiri dari kebijakan yang mengatur perilaku *user*, seperti langkah autentikasi, tingkat akses *user*, serta bagaimana *staff IT* ketika menerapkan perubahan pada infrastruktur jaringan.

Keamanan Jaringan komputer menjadi hal mutlak untuk di perhatikan oleh perusahaan ketika melihat segudang manfaat dari perencanaan pembangunan jaringan komputer yang akan di dapat (Sudirman, dkk., 2021), pada umumnya konsep keamanan jaringan diantaranya sebagai berikut:

a. *Risk* atau resiko

Merupakan tingkat gangguan yang mungkin saja dapat terjadi, dan mampu memberikan dampak pada ketersediaan dari jaringan komputer secara keseluruhan.

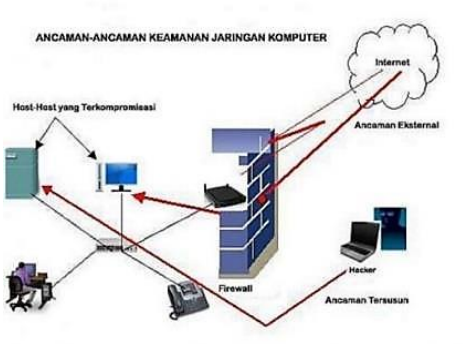
b. *Threat* atau ancaman

Adanya kemungkinanan serangan yang dapat menghambat lalu lintas jaringan yang aktif bahkan beberapa peluang ancaman dapat membuat sumber utama mati total.

c. *Vurnability* atau kerentanan

Celah keamanan pada sistem yang dapat di kategorikan pada beberapa level, misalnya rendah, menengah sampai tinggi dan menjadi kelemahan yang dapat mengancam ekosistem jaringan utama secara keseluruhan.

Keamanan jaringan merupakan suatu aspek paling penting yang harus selalu diperhatikan untuk melindungi seluruh pengguna yang menggunakan suatu jaringan, karena keamanan jaringan akan menjadi gerbang utama yang harus dilewati oleh setiap gangguan atau serangan yang akan merusak atau mengambil data-data dari pengguna jaringan tersebut.



Gambar 1. Ancaman Keamanan jaringan
Sumber: https://kakangramdani.blogspot.com/2018/01/tugas-isp.html

3. Jaringan Komputer

Menurut Al Fauzan dkk (2021), jaringan komputer merupakan sebuah jaringan telekomunikasi yang membolehkan node-node untuk saling berbagi sumber daya (*resources*).

Menurut Parusa (2021), jaringan komputer adalah kumpulan beberapa komputer (dan perangkat lain seperti *router*, *switch*, dan sebagainya) yang saling terhubung satu sama lain melalui media kabel ataupun media tanpa kabel (nirkabel).

Menurut Fasehan (2021), jaringan komputer adalah kumpulan komputer dan alat-alat lain yang saling terhubung bersama menggunakan media komunikasi tertentu. Tujuan dari jaringan komputer ialah agar setiap bagian dari jaringan komputer dapat saling berkomunikasi dan berbagi atau sharing informasi.

Jaringan komputer terbagi beberapa jenis jaringan, yang memisahkan berdasarkan area atau skala dan terbagi menjadi tiga bagian, yaitu:

a. Local area network (LAN)

LAN merupakan jaringan komputer yang terbatas dalam satu area, biasanya dioperasikan oleh satu administrasi. Umumnya, *LAN* berada di gedung perkantoran dan sekolah. *LAN* biasanya digunakan untuk memudahkan proses berbagi sumber daya, misalnya printer dan dapat saling bertukar informasi (Vera, 2022).

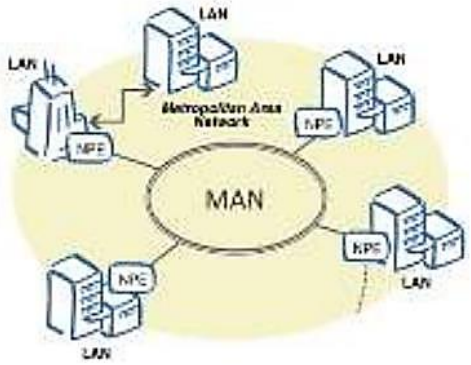


Sumber : Vera (2022)

Menurut Winarno dan Isnaini (2019), beberapa keuntungan yang didapat jika menggunakan jaringan *LAN* adalah proses sharing data lebih mudah dilakukan dan pelayanan publik bisa dilakukan dengan beberapa komputer secara bersama-sama karena jaringan *LAN* memiliki kecepatan pengiriman datanya yang relatif tinggi.

b. Metropolitan Area Network (MAN)

MAN adalah jaringan komputer yang mencakup area yang lebih luas dari pada *LAN*, biasanya antar provinsi. Jaringan *MAN* menggabungkan banyak jaringan kecil bersama- sama untuk membentuk jaringan yang lebih besar. Jaringan *MAN* terbentuk ketika sebuah instansi atau perusahaan memiliki cabang di kota atau provinsi yang dipisahkan oleh 10-50 km dan setiap cabang jaringan untuk berbagi data dan informasi.



Gambar 3. MAN (*Metropolitan Area Network*)
Sumber: Vera (2022)

MAN merupakan jaringan komputer dalam lingkup yang lebih luas, misalnya dalam satu kota. *MAN* berkerja di antara *LAN* dan *WAN* serta menjembatani *LAN* untuk terhubung dengan *WAN* atau internet. Jaringan *MAN* dapat berupa jaringan tunggal, jaringan televisi kabel, jaringan telepon seluler, dan juga dapat berbentuk dari gabungan sejumlah *LAN*. Selain itu jaringan *MAN* mampu menunjang pemindahan data dan suara.

c. Wide Area Network (WAN)

Menurut Vera (2022), *WAN* memiliki lingkup jaringan yang lebih luas dibandingkan dengan *MAN*. Jaringan dalam *WAN* dapat mencakup beberapa provinsi, bahkan satu negara. Contoh penerapan *WAN* adalah jaringan yang terdapat di suatu perusahaan yang terletak di luar negeri, misalnya di jepang. Perusahaan tersebut dapat berhubungan secara cepat dengan kantor cabang yang terdapat di Jakarta. Jenis jaringan ini biasanya memanfaatkan jaringan internet dan jaringan telepon.



Gambar 4. *WAN (Wide Area Network)*
Sumber: Vera (2022)

WAN merupakan suatu jaringan yang meliputi area geografis yang lebih luas lagi, yang mencakup suatu negara atau dunia. Umumnya jaringan ditempatkan pada banyak lokasi yang berbeda. *WAN* digunakan untuk menghubungkan banyak *LAN* menggunakan layanan seperti *leased line*, *dial-up*, satelit atau layanan paket *carrier*. Menurut Leriana (2019), adapun manfaat-manfaat jaringan komputer adalah sebagai berikut:

a. Jaringan komputer dapat memproses pengiriman data dengan cepat.
b. Komputer dapat mengsharing *hardware* antar *client*-nya.
c. Jaringan komputer bisa menghubungkan seseorang dengan orang lain di berbagai negara dengan berkomunikasi via teks, gambar, audio dan video.

Keuntungan yang didapat didalam menggunakan jaringan komputer adalah sebagai berikut:

a. Jaringan komputer dapat mengakses data di komputer lain dari komputer yang kita gunakan.
b. Data di jaringan komputer dapat kita simpan atau kita copy ke beberapa komputer lainnya, sehingga bila salah satu komputer rusak, maka salinan di komputer yang lain masih dapat kita gunakan.
c. Penghematan biaya, karena sebuah perangkat dapat digunakan secara bersama-sama.

4. Jaringan *Wireless*

Jaringan *wireless* merupakan suatu jaringan yang tidak menggunakan media kabel tapi menggunakan pancaran gelombang radio untuk interaksi atau komunikasi antar perangkat yang mendukung koneksi *wireless*. Bekerja pada

frekuensi 2,4 GHz (802.11 b/g/n/ac) atau 5 GHz (802.11 a/n/ac). *Backbone* jaringan *wireless* biasanya menggunakan kabel, dengan satu atau lebih titik akses.

Jaringan *wireless* saat ini menjadi salah satu fasilitas standar yang diberikan kepada pengguna yang dapat diakses melalui laptop, smartphone, tablet, dan perangkat lainnya yang mendukung jaringan *wireless*. Fasilitas tersebut banyak membantu pengguna dalam proses pencarian informasi. Jaringan *wireless* yang ada pada umumnya masih mempergunakan kabel *unshielded twisted pair* (UTP) sebagai *backbone* dari *access point*. Penggunaan kabel UTP sebagai *backbone* dari *access point* menjadi salah satu kendala yang dihadapi jika area cakupan yang harus terlayani akses jaringan *wireless* sangat luas, karena dengan *backbone* yang menggunakan kabel UTP memiliki keterbatasan jarak, semakin jauh jarak yang ditempuh maka semakin banyak kabel UTP yang harus digunakan dan akan sangat berpengaruh pada pengiriman dan penerimaan arus data (Rusdan dan Sabar 2020).

6. Penetrasi Testing

Penetration Testing adalah metode Pengujian penetrasi, atau pentesting (jangan dikelirukan dengan pengujian *ballpoint* atau pulpen), melibatkan simulasi serangan nyata untuk menilai risiko yang terkait dengan potensi pelanggaran keamanan. Pada pentest (sebagai lawan dari penilaian kerentanan), penguji tidak hanya menemukan kerentanan yang dapat digunakan oleh penyerang tetapi juga mengeksploitasi kerentanan, jika memungkinkan, untuk menilai apa yang mungkin diperoleh penyerang setelah eksploitasi yang berhasil (Mulyanto, dkk, 2022).



Gambar 2.1 Penetration Testing
Sumber : Santoso NA, Ainurohman M, Kurniawan RD (2022)

Uji penetrasi adalah serangan jaringan yang disimulasikan pada sistem komputer untuk mengungkap kerentanan, ancaman, dan risiko dalam aplikasi

perangkat lunak, jaringan, atau aplikasi web yang dapat digunakan penyerang (Haeruddin dan Kurniadi, 2021). Dalam melakukan *penetration testing* menggunakan 7 metode yaitu:

a. Planning and Preparation

Mendefinisikan ruang lingkup dan tujuan pengujian, termasuk sistem yang ditangani dan metodologi pengujian yang akan digunakan mengumpulkan data (nama domain jaringan dan server e-mail). Untuk lebih memahami cara kerja target dan potensi kerentanan. Langkah pertama adalah pada saat proses pengujian rencana awal dan pekerjaan persiapan berfokus pada mengidentifikasi kerentanan dan secara bertahap meningkatkan keamanan.

b. Reconnaissance

Atau yang biasa disebut dengan pengumpulan data, tergolong uji intrusi data pasif karena pengumpulan data dilakukan secara manual, melalui dokumentasi atau informasi publik yang relevan, atau dengan bertanya langsung kepada pemangku kepentingan yang terlibat dalam sistem.

c. Discovery

Adalah langkah mengumpulkan informasi menggunakan alat otomatis dari sistem pemindaian untuk menemukan kerentanan, termasuk pemindaian jaringan, server, perangkat, dan data. Langkah selanjutnya adalah memahami bagaimana target merespons berbagai upaya penyusupan.

d. Analyzing information and risk

Ini adalah fase di mana anda menganalisis informasi terperinci yang diperoleh sebelumnya tentang risiko (fase pengintaian dan deteksi) dan kerentanan keamanan. Dari jumlah tersebut,dapat disebabkan oleh kerentanan dalam sistem yang diinstal.

e. Active intrusion attempts

Ini adalah fase, yang secara aktif memberikan beberapa instruksi dari perspektif keamanan sistem sehingga kerentanan yang terdeteksi dapat diperbaiki atau diperbarui.

f. Final analysis

Analisis keseluruhan akhir memberikan pedoman teknis untuk meningkatkan keamanan berdasarkan semua temuan dan rencana analisis sistematis.

g. Report preparation

Langkah terakhir dalam kegiatan pengujian penetrasi ini adalah memberikan laporan temuan. Laporan ini diberikan kepada semua pihak yang terlibat dan bertanggung jawab terhadap sistem dan digunakan sebagai acuan untuk meningkatkan keamanan sistem.

7. Kali Linux

Kali linux adalah salah satu sistem operasi dari distribusi Linux tingkat lanjut untuk *Penetration Testing* dan audit keamanan. Kali linux merpakan pengembangan kembali *backtrack* Linux secara sempurna, mengikuti sepenuhnya kepada standar pengembangan Debian (Rusdi dan Prasti, 2019).

Semua infrastruktur baru telah dimasukkan ke dalam satu tempat, semua tools telah direview dan dikemas, dan kami menggunakan Git untuk VCS nya.

Fitur-fitur Kali Linux adalah sebagai berikut:

1. Lebih dari 300 tools *penetration testing*
2. Gratis dan akan selalu gratis
3. Mengikuti *FHS compliant*
4. Dukungan perangkat *wireless* yang luas
5. Lingkungan pengembangan yang aman
6. Dukungan banyak Bahasa



Gambar 6. Contoh Tampilan Kali Linux
Sumber: https://www.kali.org/blog/kali-linux-2020-2-release/

8. Perangkat Jaringan Komputer

Menurut Sundari (2021) jaringan komputer adalah sekumpulan peralatan atau komputer yang saling dihubungkan untuk berbagi sumber daya. perangkat jaringan

yang dapat dilalui oleh protokol adalah *TCP/IP*, begitu juga dengan media transmisi yang digunakan hingga perangkat penyalurnya. Peralatan jaringan yang umum di pakai adalah sebagai berikut:

a. Modem

modem adalah jaringan komputer yang menggunakan perangkat lain supaya komputer bisa berhubungan dengan penyedia layanan internet atau disebut dengan (*ISP*). *modem* berasal dari singkatan modulator demodulator, modulator merupakan bagian yang mengubah sinyal informasi kedalam sinyal pembawa (*carrier*) dan siap untuk dikirimkan, sedangkan demodulator adalah bagian yang memisahkan sinyal informasi (yang berisi data atau pesan) dari sinyal pembawa yang diterima sehingga informasi tersebut dapat diterima dengan baik.

Berdasarkan definisi di atas penulis dapat menyimpulkan bahwa modem adalah sesuatu yang dapat mengalihkan sinyal dan mengubah sinyal informasi yang terkirim.



Gambar 7. *Modem*
Sumber: Sundari, (2021).

b. Hub

hub merupakan suatu *device* pada jaringan yang secara konseptual beroperasi pada layer 1 (*physical layer*). Maksudnya, *hub* tidak menyaring menerjemahkan sesuatu, hanya mengetahui kecepatan transfer data dan susunan pin pada kabel. Cara kerja alat ini adalah dengan cara mengirimkan sinyal paket data keseluruh *port* pada *hub* sehingga paket data tersebut diterima oleh seluruh komputer yang berhubungan dengan *hub* tersebut kecuali komputer yang mengirimkan. Sinyal yang dikirimkan tersebut diulang-ulang walaupun paket data telah diterima oleh komputer.

Berdasarkan definisi di atas penulis dapat menyimpulkan bahwa *hub* merupakan sesuatu yang dapat mengetahui kecepatan suatu data dan susunan pin kabel yang dikirim.



Gambar 8. *Hub*
Sumber: Sundari, (2021).

c. Switch

switch merupakan suatu device pada jaringan yang secara konseptual berada pada layer 2 (Datalink Layer) dan ada yang layer 3 13 (*network layer*). Maksudnya, switch pada saat pengiriman data mengikuti Mac address pada NIC (*network interface card*) sehingga switch mengetahui kepada siapa paket ini akan diterima.

Berdasarkan uraian di atas penulis dapat menyimpulkan bahwa perangkat jaringan itu suatu alat yang dapat menghubungkan komputer seperti *modem*, *hub*, dan *switch*.



Gambar 9. *Switch*
Sumber: Sundari, (2021).

d. Router

Menurut Kuswanto & Rahman (2019), menyatakan bahwa *router* merupakan perangkat yang sangat penting penggunaannya dalam sebuah jaringan. Fungsi *router* selain sebagai penghubung antar jaringan yang berbeda jga sekaligus sebagai pintu gerbang atau *gateway* dari jaringan lokal ke jaringan internet. Seperti halnya pada koneksi internet dan *link* internet tetap terjaga penggunaan *router* pada jaringan yang besar juga perlu adanya *link backup* untuk menjaga ketersediaan koneksi.



Gambar 10. *Router*
Sumber: *https://www.officeworks.com.au/shop/officeworks/p/d-link-3g-and-4grouter-n300-dldwr116 (2019)*

e. Acces Point

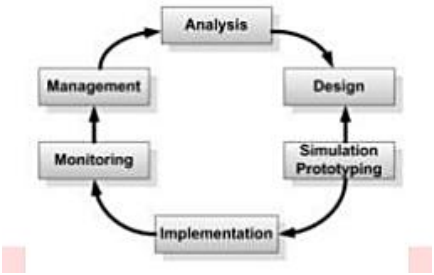
Menurut Ardiansyah & Agustina, (2021) menyatakan bahwa *acces point* merupakan sebuah perangkat jaringan komputer yang dapat menciptakan jaringan lokal *nirkabel* atau WLAN (*Wireless Local Area Nework*). *Acces point* akan dihubungkan dengan *router* atau *hub* atau *switch* melalui kabel *ethernet* dan memancarkan sinyal *Wi-Fi* diarea tertentu, untuk dapat terhubung dengan jaringan lokal yang telah dikonfigurasikan tersebut, perangkat harus melalui *acces point*.



Gambar 11. *Acces Point*
Sumber : Salamadian (2018)

9. *Network Development Life Cycle* (NDLC)

Model *Network Development Life Cycle* (NDLC) dapat digambarkan dalam diagram berikut:

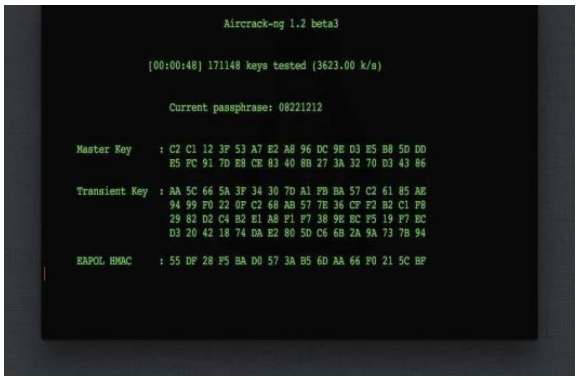


Gambar 12. *Network Development Life Cycle (NDLC)*
Sumber: Ahmad (2021)

Network Development Life Cycle (NDLC) merupakan metode untuk mengembangkan atau merancang sistem jaringan komputer dan memungkinkan pemantauan terhadap sistem yang sedang dirancang atau dikembangkan agar dapat diketahui kinerjanya. NDLC juga merupakan metode yang bergantung pada proses pembangunan sebelumnya seperti perencaan strategi bisnis, daur hidup pengembangan aplikasi dan analisa pedistribusian data. (Ahmad, Saputra & Pangestu, 2021).

1. Aircrack-ng

Aircracrk-ng adalah sebuah *tools* yang digunakan untuk menganalisa atau memonitoring sebuah jaringan, *tools* ini bisa digunakan untuk menebak kata sandi dari sebuah jaringan *wifi*. Melalui *Aircrack-ng* kita dapat mengetahui seberapa kuat pengaman dari sebuah jaringan.



Gambar 13. Contoh hasil dari perintah *Aircrack-ng*
Sumber: kennyvn.com, diakses pada tanggal 17 maret 2023

Tools ini banyak digunakan oleh para *hacker* untuk meretas kata sandi sebuah jaringn Wifi, selain itu aircrack-ng ini juga digunakan untuk menyerang jaringan dan memantau *access point*. Oleh karena itu *tools* ini sangat berguna untuk menguji keamanan suatu jaringan dengan cara kita seolah-olah meretas jaringan tersebut

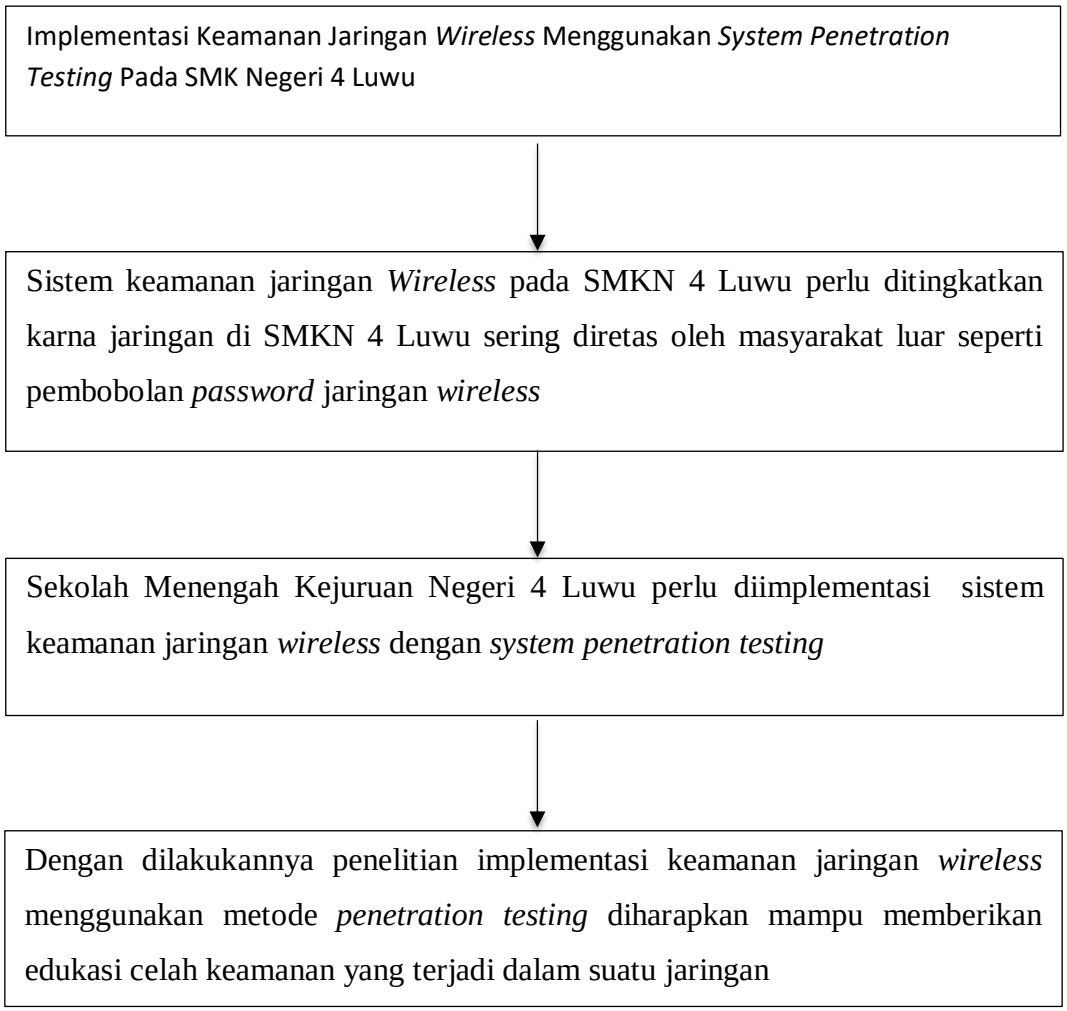
dengan menebak kata sandinya demi mengetahui seberapa kuat keamanan dari jaringan tersbut.

2.2 Hasil Penelitian yang Relavan

1. Haeruddin dan Kurniadi (2021), yang berjudul "Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode *Penetration Testing*" penelitian ini menggunakan metode *penetration testing* untuk menganalisis sistem keamanan jaringan *WLAN* ditempat umum, hotspot, dan kafe. Tujuannya untuk mensimulasikan bentuk serangan jaringan menggunakan tools yang tersedia di kali linux. Hasil dari penelitian menunjukan bahwa hanya dua dari tiga serangan yang berhasil. Oleh karena itu, harus meningkatkan keamanan pada simulasi yang berhasil dilaksanakan.
2. Ismail dan Pramudita (2020), yang berjudul "Metode *Penetration Testing* pada Keamanan Jaringan *Wireless Wardriving*" dari hasil analisis yang telah dilakukan, didapatlah kesimpulan bahwa jaringan *wireless* pada PT. Puma Makmur Aneka Engineering tidak aman karena masih ada titik hotspot yang dapat dilakukan *crack*.
3. Hasil penelitian Yusnanto, Muin dan Wahyudiono (2022), yang berjudul " Analisa Infrastruktur Jaringan *Wireless* dan *Local Area Network* (WLAN) Meggunakan *Wireshark* Serta Metode *Penetration Testing* Kali Linux" Pengujian dilakukan dengan beberapa kegiatan yang diantaranya dengan cara mengidentifikasi serta mengeksploitasi kerentanan pada keamanan jaringan komputer. Dalam menganalisa keamanan jaringan WLAN dilakukan dengan metode *Penetration* Testing dimana bentuk serangan terhadap jaringan disimulasikan, salah satu sistem operasi yang memiliki spesifikasi yang tepat dalam hal tersebut adalah Kali Linux.
4. Hasil penelitian Martin dan Jasri (2021), yang berjudul "Analisa Dan Implementasi Penetration Testing pada Jaringan Wi-Fi" penelitian ini menggunakan metode *penetration testing*, yang bertujuan agar dapat diterapkan untuk menganalisa terhadap keamanan jaringan *Wireless* yang telah sudah diterapkan, dalam penerapan metode *penetration testing* ini dimana bentuk serangan terhadap jaringan disimulasikan, salah satu sistem operasi yang memiliki spesifikasi yang tepat dalam hal tersebut adalah Kali Linux.

2.3 Kerangka Pikir

Berdasarkan penelitian yang telah diuraikan diatas, dapat diketahui bahwa kerangka pikir didasarkan pada pengalaman peneliti dalam menyelesain permasalahan pada objek penelitian ini, yaitu :



Gambar 14. Kerangka Pikir
Sumber: Penulis 2023