BAB II

TINJAUAN PUSTAKA

A. HASIL PENELITIAN DAHULU

Bedasarkan penelitian dari (Haeruddin & Kurniadi, 2021) Jaringan *wireless* adalah sebuah teknologi yang digunakan untuk menerima maupun mengirim di jaringan lokal tanpa menggunakan kabel atau melalui gelombang radio. Kelemahan jaringan wireless adalah orang sekitar bisa melakukan *hacking* menggunakan *tools* yang tersedia di internet untuk mendapatkan password atau mengambil data secara illegal. 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 ini menunjukan bahwa hanya dua dari tiga serangan yang berhasil. Oleh karena itu, harus meningkatkan keamanan pada simulasi yang berhasil dilaksanakan.

Penelitian terdahulu dari (Bayu et al., 2017) yang bertujuan untuk menganalisis terhadap sistem keamanan jaringan WLAN pada Laboratorium Sistem Informasi dan Programming Teknik Informatika Universitas Halu Oleo yang sudah diterapkan. Dalam menganalisis 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. Hasil penelitian ini menunjukan keamanan jaringan yang dimiliki oleh jaringan WLAN Laboratorium Sistem Informasi dan Programming Teknik Informatika UHO masih memiliki banyak celah untuk dieksploitasi dimana hasil penelitian yang dilakukan bahwa dari empat jenis serangan, hanya satu yang berstatus gagal yaitu pada jenis serangan *Cracking the Encryption.* Selain itu pada pengujian *Attacking The Infrastructure* dan *Man In The Middle*, jaringan WLAN belum memberi keamanan kepada user yang terkoneksi agar tidak mendapatkan gangguan pada saat mengakses layanan internet.

Penelitian dari (Wahyudi, 2018) tentang pengujian keamanan jaringan nirkabel merupakan salah satu teknologi yang mengalami pertumbuhan yang pesat dan hampir digunakan disetiap penjuru dunia saat ini. Banyaknya perusahaan maupun individu yang mengimplementasikan jaringan nirkabel ini tak lepas dari permasalahan yang paling sering dijumpai dalam telekmounikasi, yaitu masalah keamanan. Banyak orang yang masih ragu dengan keamanan *wireless*, dan banyak pula yang meyakini bahwa sistem keamanan *wireless* yang menggunakan WPA2-PSK lebih aman dibandingkan dengan sistem keamanan *wireless* yang lain. Namun dari hasil studi pustaka yang dilakukan, sistem keamanan *wireless* yang benar-benar mampu memberikan keamanan yang lebih adalah dengan menggunakan sistem keamanan *Remote Authentication Dial In User Service* (RADIUS) server. Saat ini masih banyak perusahaan yang menggunakan WPA2-PSK sebagai

sistem keamanan wireless mereka untuk menghindari kemungkinan penggunaan akses internet secara ilegal oleh orang yang tidak memiliki hak akses. Penelitian yang dilakukan ini bertujuan untuk menganalisa perbandingan kedua sistem keamanan jaringan wireless diatas dan menyimpulkan hasil pengujiannya untuk mengetahui sistem yang mana yang benar-benar aman untuk jaringan *wireless*. Pengujian dilakukan dengan menggunakan metode *wireless penetration testing* dengan melakukan beberapa kemungkinan serangan seperti *Brute force, MAC Address Spoofing, Sniffing to Eavesdrop, Man in the Middle Attack, Ping of Death,* dan *Deauthentication Attack*.

Penelitian yang dilakukan (Pujiarto et al., 2013) tentang *Wireless Local Area Network* (WLAN) merupakan jaringan yang banyak digunakan pada beberapa institusi untuk menyediakan akses informasi secara bersama. Untuk melihat kualitas keamanan jaringan maka perlu dilakukan evaluasi terhadap sistem keamanan yang ada dalam jaringan tersebut. Salah satu metode yang dapat digunakan untuk mengevaluasi adalah dengan *penetration testing* terhadap jaringan tersebut. Serangan yang dilakukan terhadap sistem dapat merugikan pihak target pengujian dan bagi pelaku tentunya merupakan sebuah tindakan pelanggaran apabila tidak adanya kesepakatan atas tindakan yang akan dilakukan dan konsekuensi terhadap akibat dari tindakan tersebut. Oleh sebab itu untuk menerapkan pada institusi perlu adanya perencanaan dan persiapan yang baik agar tidak merugikan masing-masing pihak. Penelitian ini

menggunakan kasus di Universitas Muhammadiyah Magelang sebagai institusi yang dijadikan objek untuk menerapkan model evaluasi keamanan WLAN dengan *penetration testing*.

Peneliti oleh (Sabdho & Ulfa, 2018) tentang Penelitian ini menggunakan metode *Penetration Testing*, yang bertujuan melakukan analisis terhadap sistem keamanan teknologi WLAN yang sudah diterapkan di PT. Mora Telamatika Indonesia. Uji penetrasi adalah serangkaian kegiatan yang dilakukan untuk mengidentifikasi dan mengeksploitasi kerentanan keamanan. 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. Jaringan *wireless* merupakan jaringan yang banyak digunakan pada institusi maupun tempat umum. Walaupun memiliki sistem keamanan, jaringan *wireless* masih dapat di diserang oleh para *attacker*.

Penelitian dari (Ismail & Pramudita, 2020) Membahas tentang Pemanfaatan jaringan *Wireless*, pengguna dapat menikmati internet tanpa harus tersambung pada sebuah kabel. PT. Puma Makmur Aneka *Engineering* sudah menggunakan *Wireless* sebagai penyedia internet yang dapat digunakan oleh pegawai. *Wardriving* merupakan ancaman bagi PT. Puma Makmur Aneka *Engineering* karena data penting yang diolah

menggunakan jaringan *Wireless* tidak terjamin keamanannya. Untuk mengetahui seberapa kuat keamanan jaringan Wireless pada PT. Puma Makmur Aneka Engineering, maka diperlukan analisis. 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.

Peneliti sebelumnya dari (Miftahul Anwar, Mohammad Iwan Wahyuddin, 2019) tentang *Wireless Local Area Network* (WLAN) merupakan salah satu alternatif dalam mengatasi masalah kabel di jaringan lokal. Seringkali keamanan jaringan nirkabel yang diinstal masih menggunakan pengaturan *default* vendor seperti SSID, *IP Address*, *Remote Management*, DHCP *Enabled*, saluran frekuensi, tanpa enkripsi, bahkan pengguna atau kata sandi untuk administrasi nirkabel. Bagaimana cara kerja sistem keamanan WLAN yang kuat? Sistem keamanan yang paling umum diterapkan pada jaringan nirkabel saat ini dimulai dari pengamanan titik akses dengan menerapkan konsep *MAC Filtering*, menggunakan kunci keamanan WPA / WPA2-PSK, dan otentikasi server RADIUS. Untuk melihat kualitas keamanan jaringan LAN nirkabel, bagaimana Anda menganalisis pengujian sistem keamanan yang ada di jaringan. Metode yang dapat digunakan dalam morgevaluasi jaringan nirkabel adalah dengan menguji sistem dengan melakukan simulasi bentuk serangan pada jaringan nirkabel dengan metode Penetration Testing. Dengan melakukan 4 tahap penelitian dengan

menggunakan metode pengujian penetrasi (*Cracking The Encryption*, *Bypassing MAC Address*, *Attacking The Infrastructure* dan MITM) menggunakan Kali Linux didapatkan hasil dari empat jenis serangan yang dilakukan, hanya satu yang gagal yaitu jenis serangan *cracking* dari enkripsi pada server RADIUS karena menggunakan otentikasi *captive portal.*

Pada penelitian sebelumnya oleh (Hutabarat et al., 2020) tentang Seiring makin berkembangnya teknologi informasi dan komunikasi yang mengglobal membuat setiap orang harus dapat menerima perubahan tersebut. Dengan berkembangnya teknologi maka peningkatan penggunaan teknologi akan meningkat. Sehingga banyak orang yang akan mempelajari teknologi terbaru. Dengan banyaknya orang-orang yang baru mempelajari perkembangan teknologi membuat banyak kasus *cybercrime* yang memanfaatkan orang-orang yang tidak "melek teknologi" yang menganggap bahwa keamanan atau privasi seorang tidaklah cukup penting. Tugas akhir ini bertujuan untuk menganalisa sistem keamanan pada jaringan *end user* dari serangan *Exploit* menggunakan metode *Penetration Testing*. Dalam pengujiannya, penelitian ini melakukan *exploitasi* menggunakan *tool The Fatrat* yang diinstall pada sistem operasi *Parrot OS*. Pada penelitian ini memanfaatkan celah dari *Address Resolution Protocol* (ARP), yaitu *ARP Spoofing*.. Hasil dari penelitian ini merupakan sebuah cara dalam menghadapi masalah keamanan jaringan *end user*, yaitu dengan cara dilakukannya

penambahan pada konfigurasi router mikrotik sehingga membuat jaringan *end user* menjadi aman dari serangan *Exploit* yang memanfaatkan teknik *ARP Spoofing*.

B. LANDASAN TEORI

1. Keamanan Jaringan (*Network Security*)

Network Security pada awalnya konsep ini menjelaskan lebih banyak mengenai keterjaminan (*security*) dari sebuah sistem jaringan komputer yang terhubung ke internet terhadap ancaman dan gangguan yang ditunjukan kepada sistem tersebut. *Network Security* hanyalah menjelaskan kemungkinan-kemungkinan yang akan timbul dari konektifitas jaringan komputer local kita dengan *wide-area network.* Secara umum, terdapat 3 (tiga) kata kunci dalam konsep *network security*, yaitu: resiko / tingkat bahaya, ancaman, dan kerapuhan sistem (*vulnerability*).

a. Resiko atau Tingkat Bahaya

Resiko dalam hal ini berarti berapa besar kemungkinan keberhasilan para penyusup dalam rangka memperoleh akses ke dalam jaringan komputer local yang dimiliki melalui konektivitas jaringan lokal ke *wide-area network.* Secara umum, akses-akses yang diinginkan adalah :

1) *Read Access:* mampu mengetahui keseluruhan sistem jaringan informasi.
2) *Write Accsess:* mampu melakukan proses menulis ataupun menghancurkan data yang terdapat di sistem tersebut.
3) *Denial of Service:* menutup penggunaan utilitas-utilitas jaringan normal dengan cara menghabiskan jatah CPU, bandwidth maupun memori.

b. Ancaman

Ancaman dalam hal ini berarti orang yang berusaha memperoleh akses-akses illegal terhadap jaringan komputer yang dimiliki seolah-olah memiliki otoritas terhadap akses ke jaringan komputer.

c. Kerapuhan Sistem (*Vulnerability*)

Kerapuhan sistem lebih memiliki arti seberapa jauh proteksi yang bisa diterapkan kepada *network* yang dimiliki dari seseorang dari luar sistem yang berusaha memperoleh akses illegal terhadap jaringan komputer tersebut dan kemungkinan orang-orang dari dalam sistem memberikan akses kepada dunia luar yang bersifat merusak sistem jaringan.

2. Aspek - aspek Keamanan Jaringan

Menurut dari Garfinkel (1995), bahwa aspek-aspek keamanan komputer dapat dibedakan menjadi, antara lain:

a. ***Privacy atau confidentiality***

Privacy mencakup kerahasian informasi. Inti aspek privacy adalah bagaimana menjaga informasi agar tidak dilihat atau diakses oleh orang yang tidak berhak. Sebagai contoh, e-mail seorang pemakai tidak boleh dibaca orang lain bahkan administrator. Salah satu usaha yang dapat dilakukan yaitu penggunaan enkripsi. Kita dapat menggunakan enkripsi untuk setiap dokumen atau informasi lainnya yang dianggap rahasia dan hanya kita sendiri yang dapat membukanya menggunakan kunci yang tepat.

b. ***Integrity***

Integrity atau integritas mencakup keutuhan informasi. Inti aspek integrity ini adalah bagaimana menjaga informasia agar tetap utuh. Informasi tidak boleh diubah, baik ditambah atau pun dikurangi, kecuali jika mendapat izin dari pemilik informasi. Virus, Trojan horse, atau pemakai lain yang mengubah informasi tanpa izin pemiliknya merupakan contoh masalah yang mengganggu aspek ini. Penggunaan anti virus, enkripsi, dan digital signature, merupakan contoh usaha untuk mengatasi masalah ini.

c. ***Authentication***

Authentication atau otentikasi berkaitan dengan keabsahan pemilik informasi. Harus ada cara untuk mengetahui bahwa informasi benar-benar asli, kemudian yang mengakses informasi adalah orang-

orang yang berhak, dan hanya yang berhak saja yang boleh memberikan informasi tersebut kepada orang lain. Penggunaan *access* control seperti login dan password merupakan usaha yang dilakukan untuk memenuhi aspek ini. Digital signature dan watermarking juga merupakan salah satu usaha untuk melindungi intellectual property yang sesuai dengan aspek *authentication*.

d. ***Avaibility***

Aspek ini berhubungan dengan ketersediaan informasi. Informasi harus tersedia manakala dibutuhkan. Contoh serangan terhadap aspek ini yaitu "*Denial of Service attack*" atau DoS *attack*. Misalkan, server dikirim request palsu sacara bertubi-tubi sehingga tidak dapat melayani permintaan lain atau bahkan sampai *down, hang, crash.*

3. Jenis-Jenis Ancaman

Jenis-jenis serangan yang dapat digunakan untuk melakukan pengujian keamanan pada jaringan WLAN adaah sebagai berikut:

a. *Cracking The Encryption*

Cracking The Encryption adalah pelanggaran enkripsi jaringan (misalnya WEP, WPA, dll),biasanya melalui penggunaan perangkat lunak peretas enkripsi khusus. Serangan ini dapat dilakukan melalui berbagai serangan (aktif dan pasif). Tujuan dari serangan ini adalah

untuk mengetahui apakah semua access point dilindungi dengan sistem keamanan enkripsi seperti WEP, WPA ataupun WPA2.

b. *Man In The Middle Attack (MITM)*

Man in The Middle attack atau MITM merupakan istilah yang digunakan ketika *hacker* memposisikan dirinya di antara percakapan dua belah pihak seperti user dan website. Serangan ini dilakukan secara diam-diam sehingga korban tidak menyadari bahwa percakapan atau komunikasi yang dilakukan sedang diamati oleh *hacker*. Agar lebih mudah dipahami, *Man in The Middle* juga dapat digambarkan seperti seorang pekerja pos jahat yang dapat membaca dan mengubah surat sebelum diteruskan kepada penerima sah.

4. *Penetration Testing*

Berdasarkan definisi dalam modul CEH, *Penetration Testing* merupakan metode evaluasi keamanan sistem komputer atau jaringan dengan mensimulasikan serangan dari sumber yang berbahaya dan merupakan bagian dari *security* audit. Simulasi serangan yang dilakukan dibuat seperti kasus yang bisa dibuat oleh *black hat hacker*, *cracker*, dan sebagainya. Tujuannya adalah menentukan dan mengetahui macam – macam serangan yang mungkin dilakukan pada sistem beserta akibat yang bisa terjadi karena kelemahan sistem. Dalam melakukan *penetration testing*, diperlukan analisa intensif untuk setiap kerentanan yang diakibatkan oleh kelemahan sistem. Nantinya setelah seluruh analisa

selesai dilakukan, akan didokumentasikan dan diberikan kepada pemilik beserta solusi dan dampak yang dapat diakibatkan dari celah keamanan yang ada.

5. WLAN atau Wi-Fi

Menurut Sofana, (2012:428) pada dasarnya jaringan wireless local area network sama dengan jaringan LAN biasa, hanya saja proses transmisinya tidak memakai kabel tetapi memakai gelombang elektromagnetik atau infrared. Tetapi belakangan ini gelombang elektromagnetik lebih dominan digunakan. Jaringan wireless menggunakan *electromagnetic airwaves* untuk bertukar data ataupun informasi yang dibutuhkan. Gelombang radio biasa digunakan sebagai pembawa karena dapat dengan mudah mengirimkan daya ke penerima. Data ditransmisikan dengan cara ditumpangkan pada gelombang pembawa sehingga bisa diekstrak pada ujung penerima. Data ini umumnya digunakan sebagai pemodulasi dari pembawa oleh sinyal informasi yang sedang ditransmisikan. Dalam konfigurasi biasa, pemancar dengan antena, yang disebut titik akses nirkabel atau *access point* (AP), terhubung ke LAN kabel dari lokasi tetap atau piring satelit yang menyediakan koneksi internet (ISP). AP menyediakan layanan internet untuk sejumlah client pada ruang lingkup geografis kecil (kisaran ratusan kaki / meter) itulah yang kita kenal dengan "*Hotspot Zone*" atau Hotspot. (untuk memperluas jangkauan perlu menambah jumlah AP yang ada).

Sebagian besar WLAN saat ini berjalan pada standar yang dikenal sebagai 802.11b. standar ini juga dikenal sebagai Wi-Fi (*Wireless Fidelity*). WLAN menggunakan standar ini untuk melakukan komunikasi dengan kecepatan 11 Mbps. Sementara jaringan berkabel mempunyai kecepatan 100 Mbps. Tetapi standar baru dari Wi-Fi seperti 802.11a dan 802.11g, sudah mampu mentransmisi data dengan kecepatan 54Mbps. (Turban et all., 2005 :173)

6. Kali Linux

Definisi Kali Linux adalah sistem operasi komputer bertipe Unix yang dikembangkan oleh para pecinta komputer di seluruh dunia. Linux merupakan sebuah sistem operasi berbasis *open source* yang bebas digunakan, dikembangkan, dan didistribusikan oleh siapa saja. Linux pertama kali dikenalkan oleh Linus Torvalds pada Tahun 1991. Pada waktu itu, sistem operasi Linux memanfaatkan sistem operasi GNU buatan Richard Stallman yang sudah dikembangkan oleh Linus Torvalds. Sejak pertama kali dikenalkan hingga saat ini , Linux telah dikenal sebagai salah satu sistem operasi server terbaik yang pernah ada di dunia. Pengembangan Linux sebagai sistem operasi server bahkan didukung oleh perusahaan-perusahaan besar yang ada di dunia teknologi seperti Dell, IBM, Red Hat, dll.

Beberapa fitur yang dimiliki oleh Kali Linux, yaitu:

a. Lebih dari 300 *tools Penetration Testing*

b. Gratis

c. *Open SourceGit Tree*

d. Mengikuti FHS *compliant*

e. Dukungan perangkat *wireless* yang luas

f. Modifikasi *kernel* yang sudah di *patch* untuk *injection*

g. Lingkungan pengembangan yang aman

h. GPG menandai beberapa paket dan repository

i. Banyak bahasa

j. Dapat dirubah sepenuhnya

k. Mendukung ARMEL dan ARMHF

7. Aircrack

Aircrak-ng adalah alat untuk menilai keamanan network WiFi. Banyak cara yang bisa dilakukan dengan menggunakan *tools* bawaan aircrack, misalnya memonitor wifi yang berada di sekitar kita, menangkap paket data yang lalu lalang, memutuskan koneksi wifi perangkat lain, menemukan SSID yang tersembunyi, menebak password wifi, dan lainnya. Sistem operasi yang mendukung Aircrack-ng adalah Linux, tapi bisa juga berjalan di Windows, OS X, FreeBSD, OpenBSD, dll. Sebelum mulai menggunakan *tools* ini, ada baiknya cek dulu WiFi interface yang Anda gunakan, apakah mendukung atau tidak. Berikut beberapa Fitur-fitur Aircrack-ng:

a. Aircrack-ng = untuk Crack WEP dan WPA dengan menggunakan Dictionary attack keys.
b. Airdecap-ng = untuk Mendeskripsi WEP atau WPA yang terenkripsi dengan kunci yang ada.
c. Airmon-ng = menempatkan jaringan WiFi pada monitoring mode.
d. Aireplay-ng = packet Injector
e. Airodump-ng = untuk sniffing paket. Ditempatkan pada lalu lintas data PCAP atau IVS files dan menunjukkan informasi tentang jaringan.
f. Packetforge-ng = mengenkripsi paket untuk injeksi.
g. Airdriver-ng = alat untuk mengatur driver WiFi.
h. Tkiptun-ng = untuk WPA/TKIP attack.

8. Ettercap

Ettercap adalah *tools* packet sniffer yang dipergunakan untuk menganalisa protokol jaringan dan mengaudit keamanan jaringan, yang juga memiliki kemampuan untuk memblokir lalu lintas pada jaringan LAN, mencuri password, dan melakukan penyadapan aktif terhadap protokol-protokol umum. Untuk mereka yang tidak menyukai perintah berbaris (CLI), alat bentu ini disediakan dengan antar muka grafis yang mudah. Ettercap memungkinkan membentuk serangan melawan protokol ARP dengan memposisikan diri sebagai "penengah, orang yang ditengah"

dan, jika sudah berada pada posisi tersebut, maka akan memungkinkan untuk:

a. Menginfeksi, mengganti, menghapus data dalam sebuah koneksi
b. Melihat password pada protokol-protokol seperti FTP, HTTP, POP, SSH1,dll
c. Menyediakan SSL sertifikasi palsu dalam bagian HTTPS pada korban.