BAB II
TINJAUAN PUSTAKA

2.1. Penelitian Sebelumnya

Dalam penelitian yang sudah dilakukan sebelumnya menunjukkan bahwa melakukan sebuah serangan terhadap sebuah jaringan sangat dibutuhkan untuk membantu mengetahui kelemahan sebuah jaringan yang nantinya berguna serta dapat digunakan untuk antisipasi serangan yang sama.

Seperti penelitian sebelumnya yang berjudul Analisis Keamanan Jaringan WLAN Dengan Metode *Penetration testing* yang dilakukan oleh Imam Kreshna Bayu, Muh. Yamin, dan LM Fid Aksara pada tahun 2017 dengan studi kasus: Laboratorium Sistem Informasi Dan Programming Teknik Informatika UHO yang memiliki tujuan untuk menguji tingkat keamanan WLAN yang tersedia menggunakan metode *penetration testing*. Setelah hasil didapat selanjutnya dilakukan analisis untuk mengetahui status keberhasilan terhadap serangan yang telah dilakukan[1].

Seperti penelitian berjudul Evaluasi Keamanan Akses Jaringan Komputer Nirkabel (Kasus: Kantor Pusat Fakultas Teknik Universitas Gadjah Mada) yang dilakukan oleh Ida Bagus Verry Hendrawan, Risnauri Hidayat, dan Sri Suning Kusumawardani memiliki fungsi untuk mengetahui seberapa tingkat keamanan jaringan WLAN yang telah diterapkan oleh Fakultas Teknik Universitas Gadjah Mada. Setelah hasil didapat kemudian dijadikan sebagai penilaian yang nantinya dapat digunakan untuk dapat meningkatkan keamanan akses jaringan komputer yang dimiliki oleh Kantor Pusat Fakultas Teknik Universitas Gadjah Mada[2].

Penelitian lain berjudul Evaluasi Keamanan *Wireless Local Area Network* Menggunakan Metode *Penetration testing* yang dilakukan oleh Bambang Pujiarto, Ema Utami, Sudarmawan pada tahun 2013 ini melakukan pengujian terhadap jaringan WLAN di Universitas Muhammadiyah Magelang yang menghasilkan tingkat *Vulnerability Level* jaringan tersebut. Proses pengujian dilakukan dengan menggunakan metodologi ISSAF sebagai *framework*, untuk evaluasi sistem keamanan dengan menggunakan metode *penetration testing*[3].

Penelitian selanjutnya yang berjudul Analisis dan Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel (*Wireless LAN*); Studi Kasus Di Kampus STMIK Mataram pada tahun 2017 yang dilakukan oleh Lalu Desi Samsumar, Karya Gunawan bertujuan untuk mengetahui celah keamanan yang dimiliki pada jaringan tersebut dan membuat solusi untuk keamanan jaringan dari data penyerangan yang dilakukan. Setelah pengujian dilakukan ditemukan bahwa jaringan nirkabel masih terdapat celah, sehingga dilakukan peningkatan keamanan menggunakan RADIUS server yang dirancang sesuai dengan model AAA (*authentication, authorization, dan accounting*). Hal tersebut menghasilkan peningkatan terhadap keamanan jaringan sehingga apabila dilakukan serangan yang sama akan gagal[4].

Penelitian selanjutnya yang berjudul Analisis Keamanan *Webserver* Menggunakan Metode *Penetration testing* yang dilakukan oleh Yunanri W, Imam Riadi dan Anton Yudhana pada tahun 2016 memiliki tujuan untuk mencari celah kerentanan atau kelemahan pada *webserver* yang dilakukan oleh para *hacker* yang mencoba untuk memanfaatkan hal tersebut demi keuntungan pribadi maupun organisasi yang dijalankannya. Karena dengan melihat kondisi seperti ini seharusnya dapat mengambil langkah cepat untuk mengamankan *web server* yang dimiliki oleh suatu badan institusi baik pemerintah, swasta, maupun perseorangan yang mengalami kerugian yang diakibatkan[5].

Penelitian selanjutnya yang berjudul Keamanan Jaringan WLAN Terhadap Serangan *Wireless Hacking* Pada Dinas Komunikasi & Informatika DIY yang telah dilakukan oleh Mochamad Gilang Hari Wibowo, Joko Triyono dan Edhy Sutanta pada tahun 2017 memiliki tujuan agar pengelola jaringan di Dinas Komunikasi dan Informatika Daerah Istimewa Yogyakarta (Dinas Kominfo DIY) mengetahui keamanan jaringan yang dimilikinya. Karena salah satu lembaga dalam lingkungan Pemerintahan DIY yang menetapkan jaringan komputer kabel dan WLAN sebagai media pertukaran data dan informasi[6].

Dari penjelasan di atas, ringkasan penelitian yang relevan ditunjukan pada tabel di bawah ini:

Tabel 2.1 Penelitian Terdahulu

No	Judul penelitian	Masalah	Metode	Keluaran
1.	Analisis Keamanan Jaringan WLAN Dengan Metode *Penetration testing* (Studi Kasus: Laboratorium Sistem Informasi Dan Programming Teknik Informatika UHO)	Mencari celah yang dapat di eksploitasi dari jaringan WLAN yang dimiliki Laboratorium Sistem Informasi dan Programming Teknik Informatika UHO	*Penetration testing*	Hasil dari penelitian yang telah dilakukan yaitu masih banyak celah untuk di eksploitasi yang berarti dapat dijadikan sebagai pedoman untuk meningkatkan keamanan jaringan.
2.	Evaluasi Keamanan Akses Jaringan Komputer Nirkabel	Melakukan penilaian ulang terhadap stabilitas jaringan pada Kantor Pusat Fakultas Teknik Universitas Gadjah Mada	*Penetration testing*	Hasil dari penelitian menghasilkan sebuah model sebagai hasil dari penilaian yang dapat digunakan sebagai anjuran berguna untuk meningkatkan keamanan akses jaringan komputer
3.	Evaluasi Keamanan Wireless Local Area Network Menggunakan Metode *Penetration testing*	Melihat kualitas keamanan jaringan dan melakukan evaluasi sehingga mengetahui tingkat kerentanan jaringan Universitas Muhammadiyah Magelang	*Penetration testing*	Hasil keseluruhan yang didapat setelah melakukan pengujian menunjukkan rata-rata memiliki tingkat kerentanan yang cukup tinggi pada keseluruhan jaringan WLAN di Universitas Muhammadiyah Magelang.
4.	Analisis dan Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel (Wireless LAN); Studi Kasus Di Kampus STMIK Mataram	Memelihara dan menjaga stabilias jaringan agar tetap memadai pada jaringan kampus STMIK Mataram	*Vulnerability Assesment* dan *Penetration testing*	Dari hasil yang didapat setelah melakukan pengujian berguna untuk menghasilkan sebuah model yang digunakan sebagai referensi untuk mengembangkan dan meningkatkan

No	Judul penelitian	Masalah	Metode	Keluaran
				keamanan akses jaringan komputer nirkabel pada jaringan kampus STMIK Mataram
5.	Analisis Keamanan Webserver Menggunakan Metode Penetrasi Testing	Banyaknya hacker yang mencoba untuk membobol web server	*Penetration testing*	Mencari kerentanan atau kelemahan dari sebuah Web Server.
6.	Keamanan Jaringan WLAN Terhadap Serangan Wireless Hacking Pada Dinas Komunikasi & Informatika DIY	Keamanan jaringan WLAN merupakan hal penting yang perlu diketahui oleh pengelola jaringan	*Penetration testing*	Hasil dari pengujian keamanan agar bisa digunakan sebagai masukan bagi pengelola dalam rangka menjaga atau meningkatkan kualitas layanan.

Berdasarkan Tabel 2.1 penelitian terdahulu, dapat disimpulkan bahwa metode *penetration testing* sudah tepat digunakan untuk melakukan analisis atau evaluasi dalam sebuah keamanan jaringan ataupun *web server* berdasarkan penelitian sebelumnya. Penelitian sebelumnya yang menjadi acuan utama adalah penelitian nomor 1 pada tabel karena memiliki metode yang serupa. Perbedaan terletak pada studi kasus yang dilakukan dan juga *tools* yang akan digunakan pada penelitian ini.

2.2. Dasar Teori

2.2.1 *Wireless Local Area Network* (WLAN)

Wireless Local Area Network adalah sebuah sistem komunikasi yang cukup fleksibel, pengirim dan penerima data hanya melalui media udara dengan memanfaatkan teknologi frekuensi radio[7]. WLAN dapat digolongkan menjadi dua kategori utama, yaitu:

1. *Wireless* LAN modus *Ad-Hoc*

   Pada model jaringan modus *ad-hoc*, jaringan antara satu perangkat dengan perangkat yang lainnya dilakukan dengan spontan atau langsung tanpa perlu melalui konfigurasi tertentu selama signal dari pemancar yakni

transmitter dapat diterima dengan baik oleh perangkat-perangkat penerima yaitu *receiver*[2].

2. *Wireless* LAN modus Infrastruktur

   Pada model jaringan ini yaitu infrastruktur, model ini memberikan koneksi antara perangkat yang terhubung dengan jaringan WLAN, diperlukan suatu *intermediary device* berupa *Access Point* yang terhubung dalam jaringan komputer kabel, sebelum melakukan transmisi kepada perangkat-perangkat yang akan menjadi penerima dari signal tersebut[4].

Kerentanan pada jaringan nirkabel (*wireless LAN*) terhadap keamanan data pengguna, informasi, dan ketersediaan layanan menjadi topik yang dapat menjadi perhatian dan perbincangan dalam kalangan praktisi. Maka itu, dikemukakan dalam sebuah teori bahwa sebuah jaringan komputer dikatakan aman dan juga handal apabila memenuhi unsur-unsur berikut ini[8]:

1. *Privacy* dan *Confidentiality*

   Suatu mekanisme yang dilakukan dalam upaya untuk melindungi suatu informasi dari pengguna seorang jaringan yang tidak memiliki hak akses, sedangkan *confidentiality* lebih mengarah kepada tujuan dari informasi yang diberikan dan hanya boleh untuk diketahui oleh yang berkepentingan.

2. Integrity

   Aspek *integrity* adalah aspek yang mengutamakan akses informasi yang ditujukan hanya untuk pengguna tertentu, di mana integritas dari informasi tersebut masih sangat terjaga.

3. Authentication

   Pada bagian ini mengutamakan validitas dari *user* yang melakukan akses terhadap suatu data, informasi, atau layanan dari suatu institusi.

4. Availability

   Aspek yang berhubungan dengan ketersediaan data, informasi, atau layanan ketika diperlukan.

5. Access Control

   Aspek ini berhubungan dengan klasifikasi pengguna dan cara pengaksesan informasi yang dilakukan oleh pengguna.

6. Non Repudiation

Aspek yang berkaitan dengan pencatatan pengguna, agar penggunaan data, informasi atau layanan tidak dapat menyangkal bahwa telah melakukan akses terhadap data, informasi, ataupun layanan yang tersedia.

Wireless LAN menggunakan teknologi *Radio Frequency* (RF) untuk mentransmisikan data. Jauh lebih sulit untuk menjamin keamanan dalam jaringan *wireless* daripada jaringan kabel, karena media yang digunakan adalah udara. Dalam jaringan kabel, pengguna harus terhubung langsung melalui kabel ke dalam jaringan LAN. Sedangkan *Wireless* LAN dapat diakses perangkat *wireless* selama masih dalam jangkauan *wireless.* Akses ke dalam suatu jaringan WLAN oleh pengguna yang tidak mempunyai hak dapat mengakibatkan modifikasi data, *Denial Of Service (DOS),* penggunaan data informasi yang ada di dalam Wireless LAN[1].

2.2.2 Jaringan Komputer

Konsep jaringan komputer telah lahir pada tahun 1940-an di Amerika dari sebuah proyek pengembangan mesin komputer yang bernama MODEL I di laboratorium milik Bell dan grup riset milik Harvard University yang pada saat itu dipimpin oleh profesor H. Aiken. Pada awal mulanya proyek tersebut memiliki tujuan hanya ingin memanfaatkan sebuah mesin perangkat komputer agar dapat di pakai secara bersamaan. Bertujuan untuk mengerjakan beberapa proses tanpa perlu banyak membuang waktu yang kosong maka dibuatlah model proses beruntun (*Batch Processing*), sehingga beberapa program dapat dijalankan dalam sebuah komputer dengan menggunakan kaidah antrian. Pada tahun 1950-an ketika beberapa jenis komputer mulai terkenal sampai dengan terciptanya sebuah super komputer, maka sebuah komputer harus dapat melayani satu ataupun beberapa terminal. Oleh karena ditemukanlah sebuah konsep distribusi proses yang berdasarkan dengan waktu yang dikenal dengan sebuah nama yaitu *Time Sharing Syste*m (TTS), oleh karena itu untuk saat pertama kalinya bentuk jaringan komputer dapat diaplikasikan pada saat itu juga. Pada sebuah sistem *Time Sharing System (TSS*) beberapa terminal yang terhubung secara seri dengan sebuah *host* komputer. Dalam proses *Time Sharing System* (TSS) sudah mulai nampak perpaduan antara teknologi komputer dan juga teknologi telekomunikasi yang pada awalannya berkembang secara sendiri-sendiri[1].

Jaringan komputer merupakan sebuah kumpulan ataupun beberapa komputer yang dihubungkan sehingga dapat berkomunikasi dengan yang lainnya, termasuk juga dengan *printer* dan peralatan lainnya yang saling terhubung dalam sebuah jaringan. Data ataupun informasi yang ditransfer melalui kabel ataupun *wireless* sehingga orang yang menggunakan komputer dalam jaringan yang sama dapat saling bertukar dokumen dan juga data, mencetak dengan menggunakan *printer* yang sama dan juga dapat bersama-sama menggunakan *hardware* yang terhubung dengan jaringan yang sama[9].

2.2.3 OSI *Layer*

OSI *Layer* merupakan salah satu dari arsitektur jaringan. OSI *layer* sendiri sering digunakan untuk menjelaskan cara kerja jaringan komputer secara logika. Secara umum model OSI membagi berbagai fungsi *network* menjadi 7 lapisan sedangkan lembaga yang mempublikasikan model OSI adalah *International Organization for Standardization* (ISO). Model OSI diperkenalkan pada tahun 1984. Model OSI terdiri atas *layer-layer* atau lapisan-lapisan berjumlah 7 buah. Ketujuh *layer* tersebut dapat dilihat pada Gambar 2.1[10]:

1. *Layer Aplikasi (Application Layer)*

   Pada *layer* ini berurusan dengan program komputer yang digunakan oleh *user*. Program komputer yang berhubungan hanya program yang melakukan akses jaringan, tetapi bila yang tidak berarti tidak berhubungan dengan OSI.
   Contoh: Aplikasi *Word Processing*, aplikasi ini digunakan untuk pengolahan teks sehingga program ini tidak berhubungan dengan OSI. Tetapi bila program tersebut ditambahkan fungsi jaringan misal pengiriman *email*, maka aplikasi *layer* baru berhubungan di sini.

2. *Layer Presentasi (Presentation Layer)*

   Pada *layer* ini bertugas untuk mengurusi format data yang dapat dipahami oleh berbagai macam media. Selain itu *layer* ini juga dapat mengkonversi *format data*, sehingga *layer* berikutnya dapat memahami format yang diperlukan untuk komunikasi.
   Contoh format data yang didukung oleh *layer* presentasi antara lain :*Text, Data, Graphic, Visual Image, Sound, Video.*

	OSI Layer	TCP/IP	Datagrams are called
Software	Layer 7 Application	HTTP, SMTP, IMAP, SNMP, POP3, FTP	Upper Layer Data
	Layer 6 Presentation	ASCII Characters, MPEG, SSL, TSL, Compression (Encryption & Decryption)	
	Layer 5 Session	NetBIOS, SAP, Handshaking connection	
	Layer 4 Transport	TCP, UDP	Segment
	Layer 3 Network	IPv4, IPv6, ICMP, IPSec, MPLS, ARP	Packet
Hardware	Layer 2 Data Link	Ethernet, 802.1x, PPP, ATM, Fiber Channel, MPLS, FDDI, MAC Addresses	Frame
	Layer 1 Physical	Cables, Connectors, Hubs (DLS, RS232, 10BaseT, 100BaseTX, ISDN, T1)	Bits

Gambar 2.1 OSI *Layer*

3. *Layer Sesi (Session Layer)*

Sesi *layer* mendefinisikan bagaimana memulai, mengontrol dan mengakhiri suatu percakapan (biasa disebut *session*).

Contoh *layer session* : NFS, SQL, RPC, ASP, SCP

4. *Layer Transport*

Transport Layer bertanggung jawab untuk mengirimkan pesan antara dua atau lebih host yang berada di dalam jaringan. *Transport Layer* juga menangani pemecahan dan penggabungan pesan lalu mengontrol jalur koneksi yang akan diberikan. Protokol TCP merupakan contoh yang paling sering digunakan pada *Transport Layer*.

5. *Layer Network*

Fungsi utama dari *layer network* adalah pengalamatan dan *routing*. Pengalamatan pada *layer network* merupakan pengalamatan secara *logical*, Contoh penggunaan alamat *IP*.

6. *Layer Data Link*

Fungsi yang diberikan pada layer data link antara lain:

a. *Arbitration*, pemilihan media fisik.
b. *Addressing*, pengalamatan fisik.
c. *Error detection*, menentukan apakah data telah berhasil terkirim.
d. *Identify Data Encapsulation*, menentukan pola *header* pada suatu data.

7. *Physical Layer*

Layer ini mengatur tentang bentuk *interface* yang berbeda-beda dari sebuah media transmisi. Spesifikasi yang berbeda misal konektor, *pin*, penggunaan *pin*, arus listrik yang lewat, *encoding*, dan sumber cahaya.

2.2.4 *Penetration testing*

Pentest adalah sebuah metode untuk melakukan evaluasi terhadap keamanan dari sebuah sistem dan jaringan komputer. Evaluasi dilakukan dengan cara melakukan sebuah simulasi serangan *(attack)*. Hasil dari *pentest* ini sangat penting sebagai umpan balik bagi *administrator* sistem dan jaringan untuk memperbaiki tingkat keamanan dari sistem komputernya, selain itu juga akan memberikan masukan terhadap kondisi *vulnerability* sistem sehingga memudahkan dalam melaksanakan evaluasi dari sistem keamanan komputer yang sedang berjalan. Aktifitas *pentest* juga dikenal dengan istilah *"ethical hacking"*[4].

Ada beberapa teknik dan metode yang digunakan dalam melakukan *Pentest*, diantaranya adalah dengan *black box, white box* dan *grey box. Black box testing* adalah metode *Pentest* di mana diasumsikan *tester* tidak mengetahui sama sekali infrastruktur dari target *pentest.* Dengan demikian pada *black box test* ini *tester* harus mencoba untuk menggali dari awal semua informasi yang diperlukan kemudian melakukan analisis serta menentukan jenis serangan yang akan dilakukan. Pada *White box testing* terjadi sebaliknya, *tester* telah mengetahui semua informasi yang diperlukan untuk melakukan pentest. Sementara *gray box* adalah kombinasi dari kondisi *black box* dan *white box*. Pengertian lain dari *white box* adalah *full disclosure, grey box* adalah *partial disclosure* dan *black box* adalah *blind disclosure*.

Secara umum langkah-langkah *penetration testing* dapat dibagi menjadi 7 langkah yaitu[7]:

1. *Planning and Preparation*

Langkah pertama pada *penetration testing* adalah menentukan tujuan dan juga sasaran yang akan dicapai dalam proses keseluruhan dalam *penetration testing*. Tahap ini berfokus pada langkah indentifikasi *vulnerabilities* dan juga peningkatan dari segi keamanan.

2. *Reconnaisance*

Tahap pengumpulan data yang biasa dikategorikan sebagai *passive penetration testing*, karena pada tahap ini pengumpulan data dilakukan secara manual bisa lewat dokumentasi dari pihak yang terkait ataupun informasi yang bersifat terbuka pada pihak terkait dengan sistem yang akan diuji.

3. *Discovery*

Merupakan tahap berupa dilakukannya pengumpulan informasi bisa dengan menggunakan *automated tools* untuk memindai *vulnerabilities* (kerentanan) pada sistem termasuk didalamnya ada pemindaian terhadap jaringan, *server*, perangkat, maupun data.

4. *Analyzing information and risk*

Merupakan tahap melakukan analisis yang rinci terhadap informasi yang telah didapatkan pada tahap sebelumnya *(Reconnaisance* dan *discovery*).

5. *Active intrusion attempts*

Merupakan tahap percobaan serangan yang dilakukan secara aktif dari segi keamanan sistem sehingga dapat menemukan kerentanan yang nantinya bisa diperbaiki atupun disempurnakan keamanannya.

6. *Final analysis*

Merupakan analisis akhir secara keseluruhan kemudian memberikan pernyataan terhadap segala temuan dan juga petunjuk teknis untuk perbaikan sisi dan keamanan.

7. *Report preparation*

Merupakan tahap terakhir dari kegiatan *penetration testing* yaitu memberikan laporan hasil dari investigasi dan rekomendasi terhadap pihak yang terkait ataupun yang bertanggung jawab dengan sistem untuk dapat dijadikan acuan untuk melakukan pembenahan dari segi keamanan dari sistem yang diuji.

2.2.5 Kali Linux

Kali Linux adalah sebuah distribusi Linux berbasis Debian yang ditujukan untuk Pengujian Penetrasi dan Audit Keamanan tingkat lanjut. Kali Linux berisikan beberapa ratus alat yang ditujukan untuk berbagai tugas tentang keamanan informasi, seperti *Penetration Testing*, *Security Research*, *Computer Forensics*, dan

Reverse Engineering. Kali Linux dirilis pada 13 Maret 2013 sebagai pembangunan kembali dari BackTrack Linux, dari atas ke bawah sepenuhnya mengikuti standar pengembangan Debian. Di bawah ini merupakan fitur yang dimiliki oleh Kali Linux:

1. Lebih dari 600 alat *penetration testing*

   Peninjauan setiap alat yang termasuk di dalam BackTrack, lalu menghilangkan sejumlah besar *tools* yang tidak berfungsi atau digandakan oleh *tools* lain yang menyediakan fungsi yang sama atau serupa.

2. Gratis

   Kali Linux seperti BackTrack, yaitu sepenuhnya gratis dan akan selalu seperti itu, tidak perlu membayar untuk menggunakan Kali Linux.

3. *Open Source*

   Kali Linux telah berkomitmen pada pengembangan *open source* sehingga tersedia untuk dilihat semua orang. Semua *source code* yang masuk ke Kali Linux tersedia untuk siapa saja yang ingin merubah ataupun membangun kembali sesuai dengan kebutuhan yang spesifik.

4. Sesuai dengan FHS

   Kali Linux mematuhi *Filesystem Hierarchy Standard* (FHS), yaitu memungkinkan pengguna Kali Linux untuk dengan mudah menemukan *locate binaries, support files, libraries*, dan lainnya.

5. Dukungan perangkat *wireless* yang luas

   Kali Linux telah dibangun untuk mendukung sebanyak mungkin perangkat *wireless,* memungkinkannya untuk berjalan baik pada berbagai *hardware* dan membuatnya kompatibel dengan banyak USB dan perangkat *wireless* lainnya.

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

   Sebagai penguji penetrasi, pengembangan sering perlu dilakukan penilaian, sehingga kernel Kali Linux memiliki tambalan dari injeksi terbaru.

7. Dikembangkan dalam lingkungan yang aman

   Tim Kali Linux terdiri dari sekelompok kecil individu yang dapat dipercaya untuk *commit packages* dan berinteraksi dengan repositori, yang semuanya dilakukan dengan menggunakan protokol yang aman.

8. Paket dan repositori yang ditandatangani GPG

Setiap *package* di Kali Linux telah ditandatangani oleh masing-masing pengembang yang telah membangun dan berkomitmen.

9. Dukungan multi -bahasa

Kali Linux menyertakan dukungan multibahasa yang memungkinkan lebih banyak pengguna untuk beroperasi dalam bahasa asli dan menemukan *tools* yang dibutuhkan untuk pekerjaan tersebut.

10. Sepenuhnya dapat dikostumisasi

Kali Linux dapat disesuaikan dengan keinginan penggunanya sampai ke kernel.

11. Dukungan ARMEL dan ARMHF

Saat ini sistem operasi Kali Linux sudah dapat dijalankan pada prosesor berbasis ARMEL dan ARMHF seperti Raspberry Pi dan BeagleBone Black, dengan ketersediaan *tools* yang sama seperti versi Kali Linux Desktop.

2.2.6 *Remote Authentication Dial-In User Service* (RADIUS)

RADIUS adalah sebuah protokol keamanan komputer yang digunakan untuk melakukan autentikasi, otorisasi dan pendaftaran akun pengguna secara terpusat untuk mengakses jaringan. Server autentikasi merupakan perangkat keamanan pada sebuah jaringan komputer yang menerapkan proses autentikasi untuk melayani permintaan autentikasi dari pengguna yang ingin mendapatkan layanan jaringan. Server autentikasi ini menerapkan model AAA (*authentication, authorization*, dan *accounting*).

Authentication merupakan sebuah proses pengesahan identitas *user* untuk mengakses jaringan. *Authorization* merupakan proses pengecekan wewenang yang dimiliki oleh *user* dari pengguna jaringan komputer. Sedangkan *accounting* merupakan proses perhitungan yang dilakukan oleh sistem lalu melakukan pencatatan sumberdaya yang telah digunakan oleh pengguna jaringan komputer nirkabel. RADIUS memiliki suatu format paket yang digunakan dalam melakukan transmisi data yaitu[4]:

1. *Code*

Memiliki panjang satu oktet (8 bit) dan digunakan untuk membedakan tipe pesan RADIUS yang dikirimkan pada paket. Berikut adalah kode-kode tersebut (dalam desimal) dapat dilihat pada Tabel di bawah ini.

Tabel 2.2 Kode Protokol RADIUS

Kode	Deskripsi
1	*Access - Request*
2	*Access - Accept*
3	*Access - Reject*
4	*Accounting - Request*
5	*Accounting - Resond*
11	*Access Challenge*
12	*Status - Server*
13	*Status - Client*
255	*Reserved*

2. *Packet Identifier*

Packet Identifier memiliki panjang satu oktet (8 bit) dan bertujuan untuk mencocokkan permintaan *user* dan paket respon yang diberikan oleh *server* RADIUS.

3. *Length*

Length memiliki panjang dua oktet (16 bit), memberikan informasi mengenai panjang paket, termasuk didalamnya *adalah code, identifier, length, authenticator,* dan *atribut.*

4. *Authenticator*

Authenticator memiliki panjang 16 okter (128 bit), digunakan untuk membuktikan balasan dari RADIUS server.

5. *Atributs*

Atributs berisi informasi yang dibawa pesan RADIUS. Setiap pesan dapat membawa satu atau lebih atribut. Contoh atribut RADIUS yaitu nama pengguna, *password*, CHAP-*password*, alamat *IP Acccess Point* (AP), pesan balasan. Bagian paket ini berisi autentikasi, otorisasi, informasi dan detail konfigurasi spesifik yang diperlukan untuk permintaan dari *user* RADIUS.

2.2.7 *Wordlist*

Wordlist adalah kumpulan kata-kata atau *password* yang biasanya susunan katanya berasal dari data-data target yang telah dikumpulkan sehingga menjadi susunan atau kombinasi *password* dengan berbagai kemungkinan kombinasi angka maupun simbol. *Wordlist* tidak harus selalu dibuat tetapi bisa juga di*download* di internet dan dapat diunduh secara gratis.