ANALISIS KEAMANAN JARINGAN WIRELESS LAN (WLAN) DENGAN METODE PENETRATION TESTING PADA PT.PLN (PERSERO) SEKTOR PENGENDALIAN PEMBANGKITAN PEKANBARU

SKRIPSI

Diajukan Untuk Memenuhi Salah Satu Syarat Untuk Memperoleh
Gelar Sarjana Teknik Pada Fakultas Teknik
Universitas Islam Riau Pekanbaru

Oleh:

RIVALDI RACHMAN
173510612

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS ISLAM RIAU

PEKANBARU

2021

KATA PENGANTAR

بسم الله الرحمن الرحيم

Assalamu'alaikum Warahmatullahi Wabarokatuh,

Dengan mengucapkan Alhamdulillah segala puji sedalam syukur penulis haturkan kehadirat ALLAH SWT, karena berkat rahmat serta hidayahnya pada penyusunan skripsi yang berjudul "Analisis Keamanan Jaringan Wireless LAN (WLAN) Dengan Metode Penetration Testing Pada PT. PLN (Persero) Sektor Pengendalian Pembangkitan Pekanbaru". Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Teknik Program strata-1 dijurusan Teknik Informatika, Fakultas Teknik, Universitas Islam Riau.

Penulis menyadari dalam penyusunan skripsi ini tidak akan selesai tanpa bantuan dari berbagai pihak. Karena itu pada kesempatan ini Penulis ingin mengucapkan terimakasih kepada:

1. Bapak Dr. Eng. Muslim, MT selaku Dekan Fakultas Teknik, Universitas Islam Riau.
2. Bapak Dr. Apri Siswanto S.Kom., M.Kom, selaku ketua Program Studi Teknik Informatika, Universitas Islam Riau.
3. Bapak Dr. Apri Siswanto S.Kom., M.Kom, selaku dosen pembimbing yang selalu memberikan dan semangat kepada penulis.

4. Segenap Dosen Program Studi Teknik Informatika, Universitas Islam Riau yang telah memberikan ilmu, pendidikan, dan pengetahuan kepada penulis selama duduk dibangku perkuliahan.
5. Kedua orang tua dan keluarga yang selalu mendoakan dan memberikan semangat baik itu moril ataupun materil dengan ikhlas.
6. Teman-teman kelas A angkatan 2017 Teknik Informatika, Universitas Islam Riau yang selalu memberikan semangat dan motivasi.

Penulis menyadari didalam penulisan skripsi ini tidak luput dari berbagai kekurangan. Penulis mengharapkan saran dan kritik demi kesempurnaan dan perbaikannya sehingga laporan skripsi ini dapat memberikan manfaat bagi bidang pendidikan dan penerapan dilapangan serta bisa dikembangkan lebih lanjut dan lebih baik lagi.

Pekanbaru, 10 November 2021

RIVALDI RACHMAN

ANALISIS KEAMANAN JARINGAN WIRELESS LAN (WLAN) DENGAN METODE PENETRATION TESTING PADA PT. PLN (PERSERO) SEKTOR PENGENDALIAN PEMBANGKITAN PEKANBARU

Rivaldi Rachman

Program Studi Teknik Informatika

Universitas Islam Riau

Email : rivaldirachman03@student.uir.ac.id

ABSTRAK

Teknologi informasi dan komunikasi merupakan hal yang sulit terpisahkan dari kehidupan manusia di era sekarang ini. Salah satu contoh teknologi informasi dan komunikasi tersebut adalah Wireless Local Area Network (WLAN) atau disebut juga teknologi jaringan lokal nirkabel. Penelitian ini menggunakan metode Penetration Testing, yang bertujuan melakukan analisis terhadap sistem keamanan teknologi WLAN yang sudah diterapkan di PT. PLN (Persero) Sektor Pengendalian Pembangkitan Pekanbaru. 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. Hasil penelitian ini menunjukkan keamanan jaringan yang dimiliki oleh jaringan WLAN PT. PLN (Persero) Sektor Pengendalian Pembangkitan Pekanbaru masih memiliki banyak celah untuk dieksploitasi dimana hasil penelitian yang dilakukan bahwa dari tiga jenis serangan, hanya satu yang berstatus gagal yaitu pada jenis serangan *Cracking the Encryption*. Selain itu pada pengujian *Analisa Lalulintas Jaringan (Traffic Network) Menggunakan Wireshark* dan *Man In The Middle*, jaringan WLAN belum memberi keamanan kepada user yang terkoneksi agar tidak mendapatkan gangguan pada saat mengakses layanan internet.

Kata Kunci: Penetration Testing, Wireless LAN, Kali Linux

ANALYSIS OF WIRELESS LAN (WLAN) NETWORK SECURITY WITH PENETRATION TESTING METHOD AT PT. PLN (PERSERO) SEKTOR PENGENDALIAN PEMBANGKITAN PEKANBARU

Rivaldi Rachman

Program Studi Teknik Informatika

Universitas Islam Riau

Email : rivaldirachman03@student.uir.ac.id

ABSTRACT

Information and communication technology is an inseparable part of human life in today's era. One example of information and communication technology is Wireless Local Area Network (WLAN) or also called wireless local network technology. This study uses the Penetration Testing method, which aims to analyze the security system of Wireless LAN technology applied at PT. PLN (Persero) Sektor Pengendalian Pembangkitan Pekanbaru. In analyzing the security of the Wireless LAN network, it is done by the Penetration Testing method where the attack on the network is simulated, one of the operating systems that has the right specifications in this case is Kali Linux. The results of this study indicate the security of the network owned by the Wireless LAN network of PT. PLN (Persero) Sektor Pengendalian Pembangkitan Pekanbaru still has many gaps to be exploited where the results of research conducted show that of the three types of attacks, only one failed, namely the Cracking the Encryption attack type. In addition, in testing Network Traffic Analysis Using Wireshark and Man In The Middle, the Wireless LAN network has not provided security to connected users so as not to get disturbed when accessing internet services.

Keywords: Penetration Testing, Wireless LAN, Kali Linux

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi semakin lama semakin maju dengan pesat mendorong manusia untuk menciptakan teknologi baru yang dapat lebih bermanfaat dan mempermudah pekerjaan manusia. Tentunya perkembangan teknologi tersebut akan membuat laju informasi di dunia ini semakin cepat. Laju informasi yang begitu cepatnya membuat manusia harus mampu mengolah berbagai informasi yang ada untuk memperoleh suatu hasil data yang diinginkan. Perkembangan teknologi komunikasi ini juga didukung dengan semakin meningkatnya kemajuan infrastruktur dan teknologi komunikasi dan informasi ini adalah komunikasi menggunakan wireless. Ini ditandai dengan perkembangan munculnya peralatan nirkabel yang telah menggunakan standar protokol *Wireless Fidelity* (WiFi) yang berbasiskan standar IEEE 802.11. Penggunaan jaringan yang semakin luas di dunia bisnis dan pertumbuhan kebutuhan penggunaan internet online services yang semakin cepat mendorong untuk memperoleh keuntungan dari shared data dan shared resources.

Berbicara tentang jaringan internet, tentu kita sekarang sudah tidak asing lagi mendengar nama itu, semua orang didunia memanfaatkan internet untuk berbagai kepentingan seperti pendidikan, perusahan, perdagangan bahkan seorang anak kecil sekalipun sekarang sudah banyak menggunakanya. Dari sekian banyak manfaat internet, ada sebuah ancaman yang sangat besar mengintai pengunanya seperti Phising, Sniffing, Hacking, Cracking, Denial of Service Attack, Malcios

dan kejahatan lainnya, baik untuk mengetes atau untuk keperluan yang tidak bertanggung jawab, seperti pencurian data, penyalahgunaan hak akses dll. Dengan adanya ancaman-ancaman tersebut tentu kita sebagai pengguna akan merasa tidak aman karena bisa kapan saja ancaman tersebut dapat menyerang sistem, data dan jaringan kita. Oleh sebab itu diperlukan lah sebuah keamanan jaringan (Network Security) yang baik untuk mencegah dan menangani ancaman-ancaman seperti itu.

Penelitian ini menggunakan metode Penetration Testing, yang bertujuan melakukan analisis terhadap sistem keamanan teknologi WLAN yang sudah diterapkan di PT. PLN (Persero) Sektor Pengendalian Pembangkitan Pekanbaru. Tujuan PT. PLN melakukan penetration testing karena masih memiliki banyak celah untuk dieksploitasi dimana hasil penelitian yang dilakukan bahwa dari empat jenis serangan yaitu *Analisa Lalulintas Jaringan (Traffic Network) Menggunakan Wireshark, Cracking The Encryption,* dan *Man In The Middle,* Jaringan WLAN belum memberi keamanan kepada *user* yang terkoneksi agar tidak mendapatkan gangguan pada saat mengakses layanan internet.

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, *software* yang memiliki spesifikasi yang tepat dalam hal ini adalah *Wireshark*. Jaringan wireless merupakan jaringan yang banyak digunakan pada institusi maupun tempat umum.

Walaupun memiliki sitem keamanan, jaringan wireless masih dapat di diserang oleh para-attacker.

Dengan *Wireless Local Area Network* (Wireless LAN) pengguna dapat mengakses informasi tanpa mencari tempat untuk *plug in* dan dapat men*set-up* jaringan tanpa menarik kabel. *Wireless* LAN dapat mengatasi masalah kekurangan wired network, karena mempunyai kelebihan dibandingkan antara lain sebagai berikut: *Mobility, Scalability, Installation Speed and Simplicity, Installation Fleksibility, Reduced cost of ownership.* Teknologi informasi bukan tekonologi *wireless* yang menghasilkan berbagai kemudahan juga membawa dampak bagi para pengguna jasa internet baik industri, pendidikan dan user mandiri. Perkembangan ini juga dapat dirasakan secara langsung oleh kita dengan banyaknya *wireless hotspot* yang tersedia dimana-mana. Selain dapat membantu serta melahirkan berbagai inovasi yang positif tetapi juga melahirkan sisi negatif, dan ini selalu terjadi tidak terkecuali pada perkembangan *wireless.*

Untuk membatasi permasalahan yang meluas, maka permasalahan yang akan dibahas dalam penelitian ini dibatasi pada infrastruktur protokol keamanan *wireless* LAN. Analisis dilakukan melalui beberapa kajian *white paper* yaitu sebuah dokumen yang berisi penjelasan akan sebuah masalah yang ingin diselesaikan suatu projek, serta penjelasan detil project, pembuatannya, dan interaksi dengan pengguna. Dan wacana yang ada serta melakukan eksperimen dengan melakukan serangan (*attack)* terhadap infrastruktur *Wireless* LAN. Metode keamanan *Wireless* LAN yang digunakan dalam penelitian ini yaitu *Penetration Testing,* dimana tindakan pengujian sistem dengan cara

mensimulasikan bentuk-bentuk serangan terhadap sistem tersebut sehingga akan diketahui tingkat kerentanannya, dengan menggunakan *tools* yaitu *Wireshark* dan sistem operasi *Kali linux.*

Tujuan penulisan proposal skripsi ini adalah melakukan analisis terhadap sistem keamanan teknologi WLAN yang sudah diterapkan di PT. PLN (Persero) Sektor Pengendalian Pembangkitan Pekanbaru.

1.2 Identifikasi Masalah

Adapun indentifikasi masalah yang dapat diambil dari latar belakang diatas adalah :

1. Bagaimana melakukan monitoring / memantau lalulintas jaringan ancaman serangan dari luar yang terdeteksi dengan *tools wireshark* dalam jaringan Wireless LAN PT. PLN (Persero) Sektor Pengendalian Pembangkitan Pekanbaru.
2. Keamanan jaringan dengan yang sudah diterapkan belum cukup untuk menjaga keamanan jaringan di PT. PLN (Persero) Sektor Pengendalian Pembangkitan Pekanbaru terhadap ancaman serangan – serangan yang ada.

1.3 Rumusan Masalah

Berdasarkan latar belakang diatas maka penulis merumuskan beberapa masalah yaitu :

1. Bagaimana memformulasikan permasalahan keamanan yang ada dan di identifikasi berdasarkan aspek keamanan *wireless* LAN dengan metode penetration testing?
2. Bagaimana percobaan yang dilakukan terhadap serangan luar terhadap Wireless LAN?

1.4 Tujuan Penelitian

Adapun tujuan penelitian ini untuk menganalisa tingkat kerentanan keamanan jaringan Wireless LAN terhadap serangan luar/dalam dengan menggunakan metode penetration testing pada kantor PT. PLN (Persero) Sektor Pengendalian Pembangkitan Pekanbaru.

1.5 Batasan Masalah

Sehubungan dengan keterbatasan yang dimiliki, dari segi waktu, pemikiran serta biaya, maka batasan masalah pada penelitian ini yaitu :

1. Dalam penelitian keamanan jaringan ini menggunakan *tools* yaitu *Wireshark* dan *kali linux* sebagai alat penguji.
2. Penelitian hanya akan mengevaluasi jaringan WLAN dengan menggunakan metode PENTES (penetration testing) pada PT. PLN (Persero) Sektor Pengendalian Pembangkitan Pekanbaru.

1.6 Manfaat Penelitian

Adapun manfaat penelitian ini adalah :

1. Memberikan solusi terbaik untuk keamanan jaringan.

2. Memperkuat keamanan dan mengoptimalkan jaringan Wireless LAN terhadap kantor PT. PLN (Persero) Sektor Pengendalian Pembangkitan Pekanbaru.
3. Membantu administrator dalam mengontrol dan memantau keamanan jaringan terhadap serangan luar.

BAB II

LANDASAN TEORI

2.1 Studi Kepustakaan

Studi Kepustakaan yang pertama adalah berdasarkan penelitian yang dilakukan oleh Yesi Novaria Kunang, Taqrim Ibadi, Suryayusra (2018) tentang Celah Keamanan Sistem Autentikasi *Wireless* Berbasis *RADIUS*. Dengan latar belakang yaitu Penggunaan teknologi jaringan berbasis *wireless* (tanpa kabel) memiliki resiko yang besar akan bahaya serangan dan pencurian informasi. Salah satu teknik pengamanan yang banyak digunakan pada jaringan *wireless* adalah system autentikasi yang menggunakan *RADIUS*. Untuk itu pada penelitian ini membahas pengujian penetrasi pada system Autentikasi *Wireless* berbasis *RADIUS* dengan tujuan untuk mencari celah keamanan pada sistem autentikasi berbasis *RADIUS*. Hasil yang didapatkan dari penelitian ini memperlihatkan bahwa Sistem autentikasi wireless berbasis *RADIUS* masih memiliki beberapa celah keamanan antara lain kemungkinan serangan *DoS* ke *Access point*, pencurian data *clien*t menggunakan *session hijacking*, dan pemutusan koneksi *client* untuk mengambil alih sesi koneksi. Rekomendasi dari penelitian ini diharapkan bisa menjadi acuan bagi administrator dan pengembang jaringan untuk menutup celah keamanan yang bisa dieksploitasi tersebut.

Persamaan penelitian ini dengan penelitian tersebut yaitu sama-sama membahas Sistem Keamanan yang menjadi perbedaan adalah penelitian terdahulu Mencari celah keamanan menggunakan metode RADIUS.

Studi kepustakaan yang kedua adalah berdasarkan penelitian yang dilakukan oleh Deny Purwanto, Raditya Danar Dana (2015), tentang Sistem Keamanan Jaringan Model Client Server Menggunakan Enksripsi Data (MD5) Pada Dinas Kesehatan Kota Cirebon. Dengan latar belakang yaitu Keamanan data dalam suatu jaringan komputer sangatlah penting sehingga diperlukannya suatu filter keamanan dan sistem yang mampu mengenkripsi data, dengan adanya filter keamanan dan system mengenkripsi data pihak-pihak yang tidak bertanggung jawab tidak dapat mencuri data dengan mudah karena data tersebut sudah diamankan oleh filter keamanan dan system mengenkripsi data. Sehingga dengan adanya sistem ini tidak ada lagi kehilangan atau kebocoran data pada suatu jaringan komputer. Suatu keamanan jaringan yang dibuat agar data tidak mudah dibaca atau dibobol dan tidak terjadinya lagi kebocoran data oleh pihak ketiga dengan cara data pada komputer server diproteksi dengan menggunakan mikrotik dan Password, Username dan data terenkripsi dengan menggunakan md5.

MD5 yang merupakan singkatan dari Message-Digest algortihm 5, adalah fungsi hash (prosedur terdefinisi atau fungsi matematika yang mengubah variabel dari suatu data yang berukuran besar menjadi lebih sederhana) kriptografik yang digunakan secara luas dengan hash value 128-bit.

MD5 dimanfaatkan dalam berbagai aplikasi keamanan, dan umumnya digunakan untuk meguji integritas sebuah file. Sehingga password, username dan data yang terenkripsi. Sehingga tidak mudah dibaca atau dibobol oleh pihak ketiga yang tidak bertanggung jawab. Karena begitu pentingnya keamanan data pada suatu jaringan dalam dunia jaringan komputer.

Persamaan penelitian ini dengan penelitian tersebut yaitu sama-sama membahas Sistem Keamanan yang menjadi perbedaan adalah penelitian terdahulu menjaga kehilangan atau kebocoran data pada suatu jaringan komputer menggunakan metode Message-Digest algortihm 5.

Studi kepustakaan yang ketiga adalah berdasarkan penelitian yang dilakukan oleh Ahmad Herdinal Muttaqin, Adian Fatur Rochim, Eko Didik Widianto (2016) tentang Sistem Autentikasi Hotspot Menggunakan LDAP dan Radius pada Jaringan Internet Wireless Prodi Teknik Sistem Komputer. Dengan latar belakang yaitu Jaringan nirkabel adalah jaringan yang memanfaatkan gelombang radio yang menyebar secara terbuka. Jaringan ini membutuhkan keamanan untuk menyederhanakan proses dengan menggunakan Otentikasi pengguna. Salah satu teknologi yang dapat digunakan untuk membuatnya lebih aman adalah Lightweight Directory Access Protocol (LDAP) dan Remote Authentication Dila In User Service (RADIUS).

Jurusan Teknik Sistem Komputer adalah salah satu program studi di Fakultas Teknik, Universitas Diponegoro yang memesan layanan internet setiap hari untuk kebutuhan mahasiswa. Namun, jaringan nirkabel internet di departemen ini belum cukup aman, untuk itu perlu dibuat sistem keamanan dengan LDAP dan RADIUS. Hasil penelitian ini adalah server otentikasi jaringan menggunakan Open LDAP dan FreeRadius Hotspot yang akan diintegrasikan dengan akun Sistem Informasi Akademik, yang diterapkan pada Prodi Teknik Sistem Komputer Universitas Diponegoro.

Persamaan penelitian ini dengan penelitian tersebut yaitu sama-sama membahas Sistem Keamanan yang menjadi perbedaan adalah penelitian terdahulu Sistem Autentikasi Hotspot menggunakan metode LDAP dan RADIUS.

Dalam penelitian ini, diambil beberapa referensi kepustakaan yang bersumber pada penelitian-penelitian sebelumnya. Hal ini berguna sebagai perbandingan bahan referensi dalam menyelesaikan penelitian ini. Adapun penelitian yang berkaitan dengan masalah yang diteliti yaitu dapat dilihat pada table 2.1.

Tabel 2. 1 Kajian Terdahulu

No.	Judul Penelitian	Tahun	Penulis	Keterangan
1	Celah Keamanan Sistem Autentikasi Wireless Berbasis RADIUS	2017	Yesi Novaria Kunang, Taqrim Ibadi, Suryayusra	Keamanan sistem ini dibangun sebagai pengguna yang mempunyai satu akun terintregasi untuk bisa mendapat fasilitas internet
2	Sistem Keamanan Jaringan Model Client Server Menggunakan Enksripsi Data (MD5) Pada Dinas Kesehatan Kota Cirebon	2015	Deny Purwanto, Raditya Danar Dana	Sistem keamanan ini bertujuan untuk memproteksi kehilangan atau kebocoran data pada suatu jaringan komputer
3	Sistem Autentikasi Hotspot Menggunakan LDAP dan Radius pada Jaringan Internet Wireless Prodi Teknik Sistem Komputer	2016	Ahmad Herdinal Muttaqin, Adian Fatur Rochim, Eko Didik Widianto	Sistem ini dibangun sebagai kemudahan bagi setiap pengguna yang mempunyai satu akun terintregasi untuk bisa

				mendapakan fasilitas internet tanpa mengenyampingkan aspek keamanan yang ada.

2.2 Dasar Teori

2.2.1 Jaringan Komputer.

Jaringan komputer merupakan kumpulan dari dua atau lebih komputer yang saling berhubungan dengan berinteraktif yang dihubungkan dengan media transmisi alat komunikasi dan membentuk suatu kesatuan sehingga tujuan dan sasaran dapat tecapai dan saling berbagi menggunakan sumber daya baik perangkat keras maupun perangkat lunak yang ada dan tehubung pada jaringan komputer (Arifin 2019), Jaringan komputer adalah kumpulan beberapa komputer yang saling berhubungan antara komputer satu dengan yang lain didalam suatu jaringan membentuk satu kesatuan sehingga tujuan dan sasaran dapat tercapai dengan baik.

2.2.2 Jaringan *Wireless Local Area Network* (WLAN).

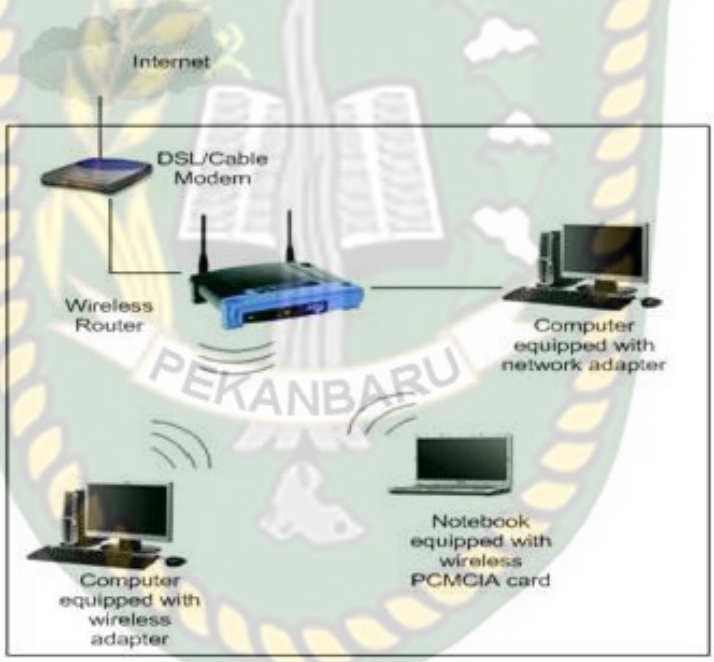
Jaringan *Wireless* merupakan suatu jaringan komputer yang saling terhubung tanpa menggunakan kabel *Local Area Network*dari komputer maupun dari peralatan lainnya dapat dikembangkan lewat sinyal radio atau gelombang cahaya. Teknologi *Wireless* LAN ada yang menggunakan frekuensi radio untuk

mengirim dan menerima data tanpa adanya membutuhkan kabel untuk saling menghubungkan sehingga tidak tergantung pada suatu tempat atau lokasi. *Wireless* LAN atau yang sering disingkat dengan WLAN merupakan sebuah sistem komunikasi data yang fleksibel yang dapat diaplikasikan sebagai ekstensi ataupun sebagai alternatif pengganti untuk jaringan LAN kabel. WLAN menggunakan teknologi frekuensi radio, mengirim dan menerima data melalui media udara, dengan meminimalisasi kebutuhan akan sambungan kabel. Dengan begitu, WLAN telah dapat mengkombinasikan antara konektivitas data dengan mobilitas user. WLAN adalah sebuah alternative dimana untuk alternative LAN kabel sulit atau tidak mungkin dibangun. Tempat-tempat seperti banguan tua atau ruangan kelas (Wongkar dkk., 2015).

Wireless LAN (WLAN) atau *Wireless Fidelity* (Wi-Fi), yaitu teknologi yang digunakan untuk mentranmisikan data yang berjalan pada jaringan komputer lokal tanpa penggunaan kabel dengan menggunakan infrastruktur dan media transmisi yang baru, dalam hal ini adalah gelombang radio. Agar berbagai macam produk *Wireless* LAN yang berasal dari vendor yang berlainan dapat saling bekerja sama/kompatibel pada jaringan, maka dibuatlah suatu standar untuk teknologi ini, yang disebut dengan IEEE (*Institute for Electrical and Electronic Engineers)* 802.11.

Wireless LAN sebenarnya hampir sama dengan jaringan LAN, akan tetapi setiap node pada WLAN menggunakan *Wireless Device* untuk berhubungan dengan jaringan *node* pada WLAN menggunakan kanal frekuensi yang sama dan SSID yang menunjukkan identitas dari *Wireless Device*. Tidak seperti jaringan

kabel, jaringan *Wireless* memiliki dua mode yang dapat digunakan yaitu, *infrastruktur* dan *Ad-Hoc*. Konfigurasi *Infrastruktur* adalah komunikasi antar masing-masing PC melalui sebuah *Access Point* pada WLAN atau LAN. Komunikasi *Ad-Hoc* adalah komunikasi secara langsung antara masing-masing komputer dengan menggunakan piranti *Wireless.* Penggunaan kedua mode ini tergantung dari kebutuhan untuk berbagi data atau kebutuhan yang lain dengan jaringan berkabel.

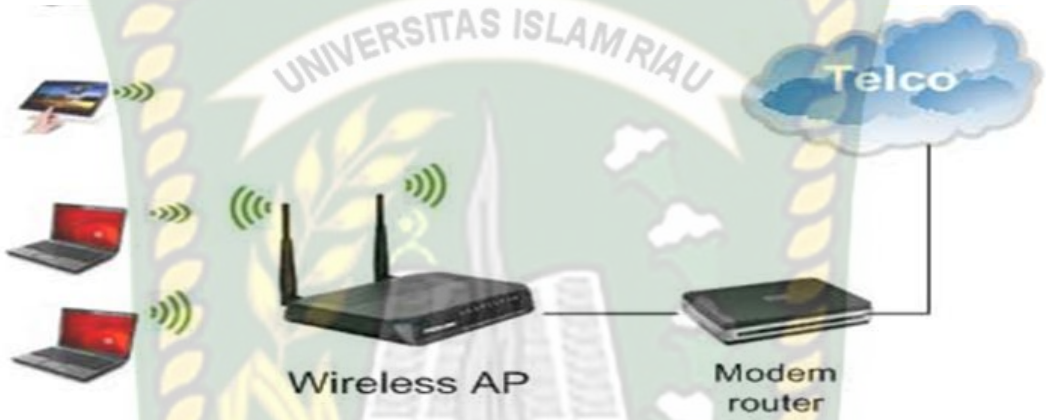


Gambar 2. 1 Konfigurasi WLAN

Jaringan *Wireless* LAN terdiri dari komponen *Wireless User* dan *Access Point* dimana setiap *Wireless User* terhubung ke sebuah *Access Point.* Topologi *Wireless LAN* dapat dibuat sederhana atau rumit dan terdapat dua macam topologi yang biasa digunakan, Arbough (2004) yaitu sebagai berikut:

- **Sistem infrastruktur**

Wireless LAN memiliki SSID *(Service Set Identifier)* sebagai nama jaringan wireless tersebut. Sistem penamaan SSID dapat diberikan maksimal sebesar 32 karakter. Karakter-karakter tersebut juga dibuat case sensitive sehingga SSID dapat lebih bannyak variasinya.

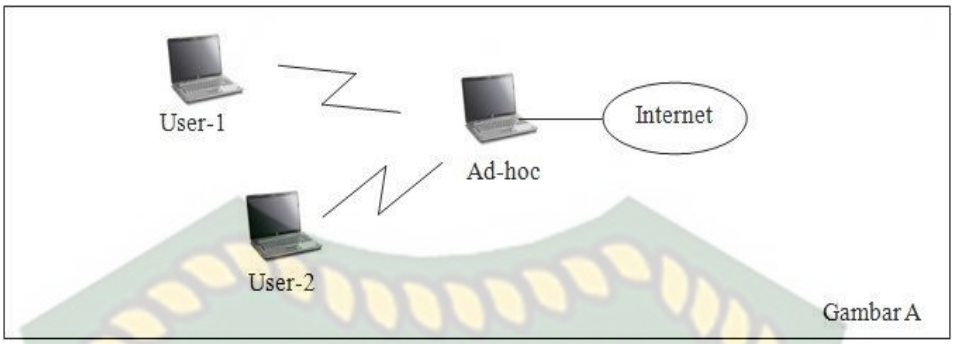


Gambar 2. 2 Jaringan Infrastruktur

Dengan adanya SSID maka wireless lan itu dapat dikenali. Pada saat beberapa komputer terhubung dengan SSID yang sama, maka terbentuklah sebuah jaringan infrastruktur.

- **Sistem Ad Hoc**

Ad Hoc mode digambarkan sebagai jaringan peer-to-peer atau juga disebut dengan *Independent Basic Service Set* (IBSS) yang digunakan bila sesama pengguna dengan saling mengenal *Service Set Identifier* (SSID), dimana jaringannya terdiri dari beberapa komputer yang masing-masing dilengkapi dengan *Wireless Network Interface Card* (*Wireless NIC*).



Gambar 2. 3 Jaringan Ad Hoc

2.2.3 Keamanan Wireless LAN

Jaringan *Wireless* memiliki lebih banyak kelemahan dibanding dengan jaringan kabel (*wired*). Kelemahan jaringan *Wireless* secara umum dapat dibagi menjadi 2 jenis, yakni kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang digunakan. Salah satu contoh penyebab kelemahan pada konfigurasi karena saat ini untuk membangun sebuah jaringan wireless cukup mudah (Pervaiz, 2014). Banyak vendor yang menyediakan fasilitas yang memudahkan pengguna atau admin jaringan sehingga sering ditemukan wireless yang masih menggunakan konfigurasi wireless default bawaan vendor (Glending, 2003). Secara umum, terdapat tiga kata kunci dalam konsep keamanan seperti terlihat pada Tabel 2.2.

Tabel 2. 2 Konsep Keamanan Jaringan

No.	KONSEP	KETERANGAN
1	Resiko atau tingkat bahaya	Resiko berarti beberapa kemungkinan keberhasilan para penyusup dalam mengakses ke dalam jaringan kaomputer lokal yang dimiliki melalui konektivitas jaringan lokal ke Wide Area Network (WAN) antara lain sebagai berikut:
	– Denial of Service	Menutup penggunaan utilitas jaringan normal dengan cara menghabiskan jatah Central Processing Unit (CPU), memory maupun bandwidth.
	– Write Access	Mampu melakukan proses menulis atau menghancurkan data dalam sistem.
2	Ancaman	Orang yang berusaha memperoleh akses secara ilegal ke dalam jaringan.
3	Kerapuhan Sistem	Seberapa jauh perlindungan yang bisa diterapkan kepada network dari seseorang dari luar sistem yang berusaha memperoleh akses ilegal terhadap jaringan dan kemungkinan orang dari dalam sistem

		memberikan akses kepada dunia luar yang bersifat merusak sistem jaringan tersebut.

Keamanan Wireless LAN, terdapat beberapa faktor yang menentukan sejauh mana keamanan ingin didapatkan yaitu penyerang (*attacker*), ancaman (*threats*), potensi kelemahan (*potential vulnerabilities*), aset yang beresiko (*asset at risk*), perlindungan yang ada (*existing safeguard*) dan perlindungan tambahan (*additional control*). Mekanisme keamanan dalam Wireless LAN adalah hal penting dalam menjaga kerahasiaan data. Proses enkripsi didalam mekanisme keamanan merupakan proses pengkodean pesan untuk menyembunyikan isi. Algoritma enkripsi modern menggunakan kunci kriptografi dimana hasil enkripsi tidak dapat didekripsi tanpa kunci yang sesuai (Stallings, 2003). Terlihat pada Tabel 2.3 Layanan Perlindungan Keamanan dibawah ini.

Tabel 2. 3 Layanan Perlindungan Keamanan

No.	KONSEP	KETERANGAN
1	Kerahasiaan (*Confidentiality)*	Yaitu mencegah pihak yang tidak berhak mengakses membaca informasi yang bersifat rahasia dan harus aman dari pengcopyan / penyalinan.
2	Integritas (*Integrity*)	Yaitu menjamin data yang diterima tidak mengalami perubahan selama dikirimkan, baik itu dimodifikasi, dipublikasi, dicopy atau dikembalikan.
3	Otentikasi (*Authentication*)	Yaitu suatu layanan keamanan yang diberikan untuk meyakinkan bahwa identitas pengguna yang melakukan komunikasi di jaringan yang benar.
4	Tidak Terjadi Penyangkalan (*Non Repudiation)*	Yaitu mencegah baik penerima maupun pengirim menyangkal pesan yang dikirim atau diterimanya.
5	Ketersediaan (*Availability*)	Yaitu menjamin ketersediaan suatu sistem untuk dapat selalu digunakan setiap ada

		permintaan dari pengguna.
6	Akses Kendali (*Access Control*)	Yaitu membatasi dan mengontrol akses setiap pengguna.

2.2.4 Serangan Wireless LAN

Jaringan wireless sangatlah rentan terhadap serangan, hal ini dikarenakan jaringan wireless tidak dapat dibatasi oleh sebuah gedung seperti yang diterapkan pada jaringan berbasis kabel. Sinyal radio yang dipancarkan oleh perangkat wireless dalam melakukan proses transmisi data didalam sebuah jaringan dapat dengan mudah diterima / ditangkap oleh pengguna komputer lain selain pengguna dalam satu jaringan hanya dengan menggunakan perangkat yang kompatibel dengan jaringan wireless seperti kartu jaringan wireless.

2.2.5 Protokol Wireless Protected Access (WPA)

Wireless Protected Access (WPA) ditawarkan sebagai solusi keamanan yang lebih baik dari pada *Wired Equivalent Privacy* (WEP). WPA merupakan bagian dari standar yang dikembangkan oleh *Robust Security Network* (RSN) WPA dirancang untuk dapat berjalan dengan beberapa sistem perangkat keras yang ada saat ini, namun dibutuhkan dukungan peningkatan kemampuan perangkat lunak (*Software Upgrade*).

Pada perkembangan selanjutnya, dimana algoritma RC4digantikan oleh algoritma enkripsi baru yaitu *Advance Encryption System* (AES) dengan panjang kunci sepanjang 256 bit. Dukungan peningkatan keamanan Wireless LAN yang disediakan WPA adalah meliputi otentikasi dan kendali Akses, Enkripsi dan

Integritas Data. Standar tersebut ternyata masih mempunyai banyak titik kelemahan dalam keamanan, karena itulah dikembangkan pembagian lapisan keamanan yang sudah ada menjadi tiga yaitu:

1. Lapisan Wireless LAN adalah lapisan yang berhubungan dengan proses transmisi data termasuk juga untuk melakukan enkripsi dan deskripsi.
2. Lapisan Otentikasi, adalah lapisan dimana terjadi proses pengambilan keputusan mengenai pemberian otentikasi kepada pengguna berdasarkan informasi identitas yang diberikan. Dengan kata lain adalah untuk membuktikan apakah identitas yang diberikan sudah benar.
3. Lapisan Kendali Akses, adalah lapisan tengah yang mengatur pemberian akses kepada pengguna berdasarkan informasi dari lapisan otentikasi.

2.2.6 Otentikasi dan Kendali Akses dalam WPA

Otentikasi yang didukung oleh WPA adalah otentikasi dengan menggunakan *Preshared Key* dan otentikasi dengan menggunakan *server based key*. Otentikasi dengan *Preshared Key* adalah model otentikasi dengan menggunakan WEP. Sedangkan otentikasi dengan *server based key* adalah model otentikasi dengan menggunakan akses kontrol.

WPA mendefinisikan dua macam kunci rahasia, yaitu *pairwise key* dan *group key*. *Pairwise key* adalah kunci yang digunakan antara *wireless user* dengan *access point*, kunci ini hanya dapat digunakan dalam tranmisi data di antara kedua belah pihak tersebut (*unicast*). *Pairwise key* maupun *group key* mempunyai manajemen kunci tersendiri yang disebut dengan *pairwise key hierarchy* dan *group key hierarchy*.

2.2.7 Enkripsi dalam WPA

WPA menggunakan protokol enkripsi yang disebut dengan *Temporary Key Integrity Protocol* (TKIP). TKIP mendukung pengubahan kunci (*rekeying*) untuk *pairwise key* dan *group key*. Fitur-fitur keamanan yang disediakan oleh TKIP adalah:

1. Penambahan besar ukuran *initialization vector* untuk mencegah terjadinya pengulangan nilai *initialization vector*.
2. Pengubahan cara pemilihan *initialization vector* untuk mencegah terjadinya *weak key*, juga mencegah terjadinya kemungkinan *replay attack*.
3. Pengubahan kunci enkripsi untuk setiap paket yang dikirimkan (*per packet key mixing*).
4. Penggunaan *message integrity protocol* yang lebih baik untuk mencegah terjadinya modifikasi pesan.
5. Penggunaan mekanisme untuk melakukan distribusi maupun perubahan terhadap kunci rahasia yang digunakan.

2.2.8 Router

Router adalah salah satu komponen pada jaringan komputer yang mampu melewatkan data melalui sebuah jaringan atau internet menuju sasarannya, melalui sebuah proses yang dikenal sebagai *routing*. Proses *routing* dapat dilakukan dengan memasukkan informasi suatu alamat jaringan secara manual kedalam tabel *routing* ataupun dengan bantuan protokol *routing*. Sebuah *router* mampu mengirimkan data/informasi dari satu jaringan kejaringan lain yang

berbeda, *router* hampir sama dengan *bridge*, namun *router* lebih pintar dibandingkan dengan *bridge*. Karena *router* mampu menghubungkan dua atau lebih jaringan yang berbeda, sedangkan *bridge* hanya mampu menghubungkan jaringan yang sama. Dalam pengembangan perangkat *router* dewasa ini sudah mulai mencapai atau bahkan melampaui batas tuntutan teknologi yang diharapkan.

Router akan mencari jalur terbaik untuk mengirimkan sebuah pesan yang berdasarkan atau alamat tujuan dan alamat asal. *Router* mengetahui alamat secara keseluruhan dari masing-masing komputer dilingkungan jaringan lokalnya, dan *router* lainnya (Sumarianta, 2011).

2.2.9 Web Proxy

Web Proxy adalah suatu program yang diletakkan di antara suatu komputer/jaringan komputer dengan Internet. Web Proxy bertindak sebagai perantara (middleman) bagi web browser dan web server. Web Proxy bertindak sebagai server bagi web browser dan proxy bertindak sebagai client bagi web server.

Proxy merupakan jenis serverdan client sekaligus, yaitu proxy sebagai server bagi web-browser dan proxy sebagai client bagi web-server. Urutan pengerjaan proxy dilakukan sebagai berikut:

1. Membuat/menulis server yang akan menangani permintaan dari web-browser. Server inilah yang mengembalikan halaman-halaman HTML ke web-browser.
2. Menulis/membuat program bagi sisi client, yang melakukan koneksi ke web-server.

3. Mengkombinasi kedua sisi diatas untuk membentuk suatu web-proxy sederhana.

Server merupakan program yang menunggu permintaan koneksi pada suatu port tertentu. Untuk membuat server ini dibutuhkan sistem pemanggilan antara lain: *socket, bind, listen, accept, read, write,* dan *close*.

Client melihat alamat IP server kemudian membuat socket dan memanggil *connect* untuk membangun koneksi, setelah koneksi terbentuk, barulah proses pertukaran data dilakukan dengan menggunakan fungsi-fungsi *read* dan *write* pada *socket*. Sistem pemanggilan yang ada untuk client adalah: *socket, connect, read, write,* dan *close*. Gabungan kedua sisi diatas akan membentuk suatu web-proxy.

2.2.10 Virtual Private Network (VPN)

Virtual Private Network atau VPN adalah suatu jaringan pribadi yang dibuat dengan menggunakan jaringan publik, atau dengan kata lain menciptakan suatu WAN yang sebenarnya terpisah baik secara fisikal maupun geografis sehingga secara logikal membentuk satu netwok tunggal, paket data yang mengalir antar site maupun dari user yang melakukan remote akses akan mengalami enkripsi dan authentikasi sehingga menjamin keamanan, integritas dan validitas data.

Lebih jelasnya, VPN adalah sebuah koneksi Virtual yang bersifat private mengapa disebut demikian karena pada dasarnya jaringan ini tidak ada secara fisik hanya berupa jaringan virtual dan mengapa disebut private karena jaringan ini merupakan jaringan yang sifatnya private yang tidak semua orang bisa

mengaksesnya. VPN Menghubungkan PC dengan jaringan public atau internet namun sifatnya private, karena bersifat private maka tidak semua orang bisa terkoneksi ke jaringan ini dan mengaksesnya.

2.2.11 Penetration Testing

Penetration Testing (pentest) merupakan kegiatan yang dilakukan untuk melakukan pengujian terhadap keamanan sebuah sistem. Pengujian ini dilakukan untuk menemukan celah keamanan yang terdapat pada sistem tersebut. Hasil pengujian ini digunakan untuk memperbaiki sisi keamanan dari sistem. Yang dicari dari pentest ini adalah apakah terdapat celah keamanan yang dapat disalah gunakan (*exploitable vulnerability*).

Pentest melibatkan simulasi serangan nyata untuk menilai risiko yang terkait dengan pelanggaran keamanan potensial. Pada pentest (sebagai lawan dari penilaian kerentanan), penguji tidak hanya menemukan kerentanan yang dapat digunakan oleh penyerang tetapi juga mengeksploitasi kerentanan, dimana memungkinkan untuk menilai apa yang penyerang dapat peroleh setelah eksploitasi sukses.

Tujuan pentest diantaranya adalah untuk menentukan dan mengetahui serangan-serangan yang bisa terjadi terhadap kerentanan yang ada pada sistem, mengetahui dampak bisnis yang diakibatkan dari hasil ekpoitasi yang dilakukan oleh penyerang.

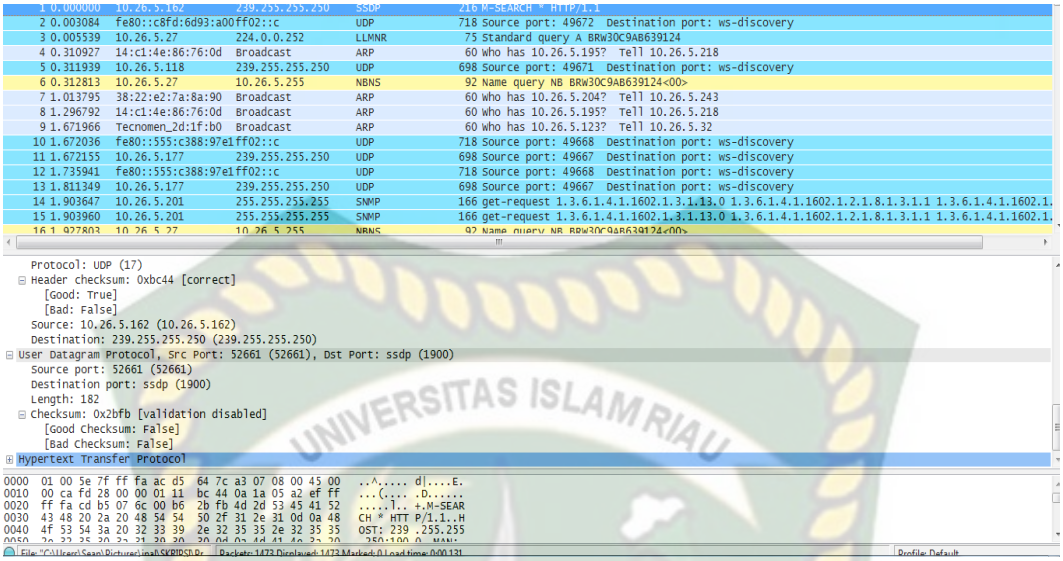
2.2.12 Wireshark

Wireshark adalah program Network Protocol Analyzer alias penganalisa protokol jaringan yang lengkap. Aplikasi ini awalnya bernama Ethereal, dan pada

Mei 2006 proyek ini berganti nama menjadi WIreshark karena masalah merek dagang.

Gambar 2. 4 Icon Wireshark

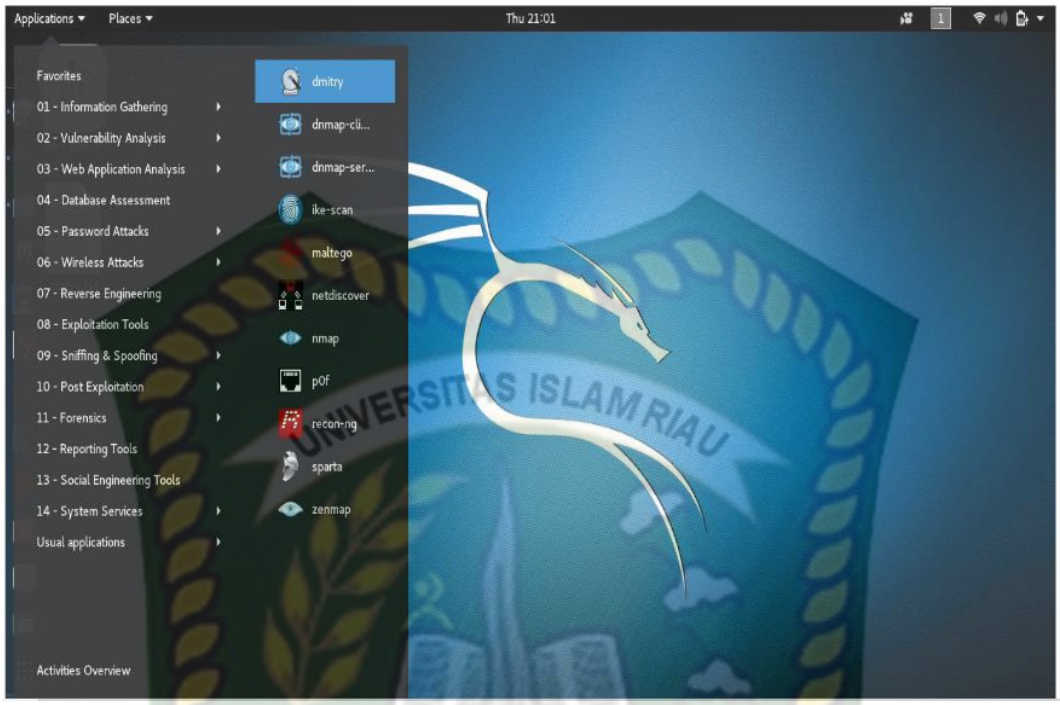
Bahasa Pemrograman yang digunakan adalah bahasa C dengan lisensi public umum GNU. Wireshark banyak disukai karena interfacenya yang menggunakan Graphical User Interface (GUI) atau tampilan grafis. Program ini dapat merakam semua paket yang lewat serta menyeleksi dan menampilkan data tersebut sedetail mungkin, misalnya postingan komentar kamu di blog atau bahkan Username dan Password. Kamu harus bisa menggunakannya dengan bijak. Sebenarnya Wireshark tidak di desain untuk peretasan/hacker. Fungsi aplikasi wireshark utamanya tidak diperuntukkan untuk hacking. Fungsi aplikasi Wireshark yang utama adalah sebagai Administrator Jaringan untuk dapat melacak apa yang terjadi didalam jaringan miliknya atau untuk memastikan jaringannya bekerja dengan baik, serta tidak ada yang melakukan hal-hal buruk pada jaringan itu.



Gambar 2. 5 Contoh monitoring dari tools Wireshark.

2.2.13 Kali Linux

Kali Linux (Kali) adalah sistem distribusi Linux yang di kembangan dengan fokus pada tugas penetration testing. Sebelumnya, Kali Linux dikenal sebagai Back Track, yang mana merupakan penggabungan antara tiga distro penetration testing Linux yang berbeda: IWHAX, WHOPPIX, dan Auditor. Back Track adalah salah satu sistem distribusi yang paling terkenal Linux, seperti dapat dibuktikan dengan jumlah download yang mencapai lebih dari empat juta pada Back Track Linux 4.0 prafinal. Kali Linux Versi 1.0 dirilis pada 12 Maret 2013. Lima hari kemudian, Versi 1.0.1 dirilis, yang telah memperbaiki masalah keyboard USB. Dalam lima hari, Kali telah diunduh lebih dari 90.000 kali.



Gambar 2. 6 Tampilan kali linux

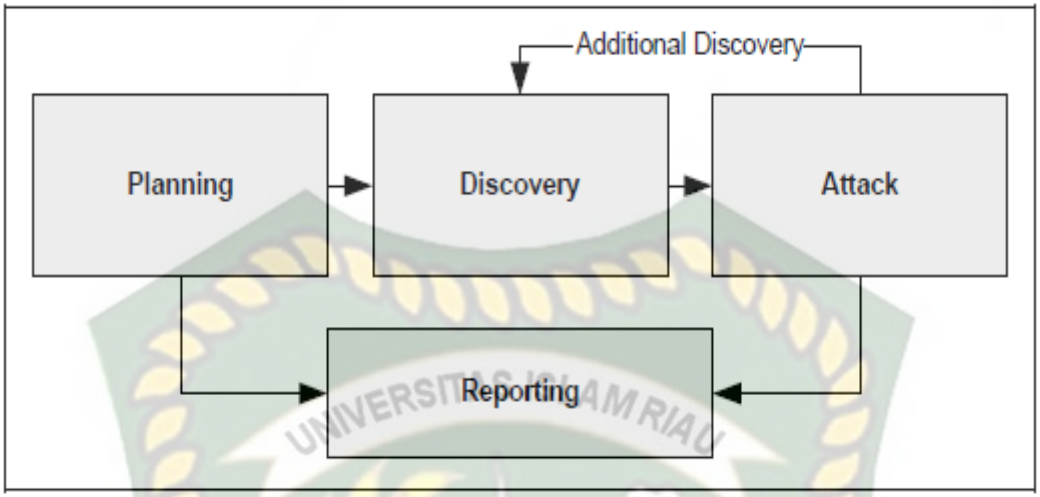
BAB III

METODOLOGI PENELITIAN

3.1 Metode Penelitian

Penetration Testing atau disebut juga *pentest* adalah pengujian keamanan informasi dimana seorang asesor meniru serangan yang biasa sering terjadi untuk mengidentifikasi metode peretasan fitur keamanan aplikasi, sistem, atau jaringan. Pengujian ini dilakukan oleh asesor menggunakan serangan yang nyata, sistem yang nyata, dan data yang nyata menggunakan alat dan teknik yang sering dipakai oleh seorang *hacker*. *Penetration Testing* biasanya dilakukan bersamaan dengan *Vulnerability Assessment* (VA). *Vulnerability Assessment* adalah sebuah proses untuk mengidentifikasi risiko dan celah kerentanan pada aplikasi, sistem, ataupun jaringan. Sebagian besar pentest mencari kombinasi kerentanan pada satu atau lebih sistem untuk mendapatkan akses lebih dalam pada sistem yang menjadi target dibandingkan dengan hanya mengetahui satu macam kerentanan.

Dalam menjalankan pengujian, terdapat 4 tahapan yang dijalankan dalam *Penetration Testing* yaitu tahap *Planning* (Perencanaan), *Discovery* (Penemuan), *Attack* (Serangan), dan *Reporting* (Pelaporan) seperti yang dijelaskan pada Gambar 3.1.



Gambar 3. 1 Tahapan Metodologi Penetration Testing

- **National Institute of Standards and Technology SP 800-42**

Departemen Perdagangan AS menerbitkan rekomendasi tentang Pengujian Keamanan Jaringan sebagaimana ditetapkan di Institut Nasional Standar dan Publikasi Khusus Teknologi 800-42 (NIST SP 800-42). Metodologi dasar untuk penetration testing menurut NIST SP 800-42 terdiri dari empat fase yaitu Planning, Discovery, Attack, dan Reporting, lihat Gambar 3.1. Pada tahap awal Discovery, pentester dapat mengidentifikasi dan mengumpulkan informasi yang berpotensi terkait dengan target. Pengumpulan informasi dapat dilakukan dengan berbagai teknik termasuk interogasi Sistem Nama Domain, InterNIC queries, Pencarian informasi dari server web organisasi target, Pencarian server Protokol Akses Direktori Ringan *Lightweight Directory Access Protocol* (LDAP) organisasi untuk informasi, Pengambilan paket, enumerasi NetBIOS, Sistem Informasi Jaringan, dan Banner grabbing (Rizdqi Akbar Ramadhan et al, 2020 *IOP Conf. Ser.: Mater. Sci. Eng.* **771** 012019).

3.1.1 Manfaat *Penetration Testing*

Dalam implementasinya, *pentest* dapat berguna antara lain untuk menentukan seberapa baik sebuah sistem dapat menangani serangan dunia nyata. Selain itu dapat menentukan penanggulangan yang dapat mengurangi ancaman terhadap sistem, dan untuk mengingkatkan keamanan pada aplikasi, sistem, atau jaringan yang dimiliki. *Pentest* juga digunakan untuk mendeteksi serangan dan merespon dengan cepat dan tepat. Sehingga secara garis besar pentest bertujuan untuk menganalisis risiko yang akan timbul dengan adanya kerentanan yang telah diindentifikasi pada tahap *Vulnerability Assessment* dan memberikan rekomendasi tindakan yang perlu dilakukan apabila sistem yang diuji dapat lolos dari serangan *hacker*.

3.1.2 Penetration Testing

Adapun 3 Tahapan Jenis Serangan Penetration Testing yang akan diuji/dilakukan Pada Kantor PT. PLN (Persero) Sektor Pengendalian Pembangkitan Pekanbaru:

1. Analisa Lalulintas Jaringan (Traffic Network) Menggunakan Wireshark.

   Hasil capture packet yang telah didapatkan dari packet list / daftar paket dapat dianalisa berbagai macam informasi yang didapatkan dari setiap alamat IP sumber (IP Source) dan IP Tujuan (IP Destination). Selain itu didapatkan juga informasi akses dari setiap IP berupa *time, source, destination, protocol, length,* dan *info.*

2. Cracking The Encryption.

   Tahapan yang kedua, dimana tujuan dari serangan ini adalah untuk mengetahui apakah semua access point dilindungi dengan sistem keamanan enkripsi seperti WEP, WPA, ataupun WPA2.

3. Mitm (Man In The Middle Attack).

   Dalam tahap terakhir ini, dilakukan serangan terhadap *user* lain jaringan WLAN yang sama dengan melakukan penyadapan paket data. Pengujian ini menggunakan aplikasi *Ettercap* sebagai alat uji.

Dalam menjalankan pentest, pada umumnya asesor menggunakan *tools* untuk mempermudah pengujian. *Tools* pentest yang sering digunakan antara lain Kali Linux, nmap, Metasploit, Wireshark, Hashcat, Burpsuite, Acunetix Web Vulnerability Scanner, Nessus, dan lain sebagainya.

3.2 Waktu dan Tempat Penelitian

Penelitian ini dilakukan pada bulan Juni 2021 sampai Agustus 2021 dengan melakukan penelitian pada PT. PLN (Persero) Sektor Pengendalian Pembangkitan Pekanbaru.

3.3 Metode Pengumpulan Data

Metode pengumpulan data yang digunakan dalam penelitian ini adalah :

1. Pengumpulan Data Primer

   Observasi atau pengamatan yaitu dengan cara mengamati dan mencatat secara sistematik gejala-gejala yang sedang diselidiki.

2. Pengumpulan Data Sekunder

Studi Pustaka (literatur), data diperoleh melalui studi kepustakaan yaitu dengan mencari bahan dari internet, jurnal, dan perpustakaan serta buku referensi pada penelitian-penelitian terdahulu yang sejenis.

3. Wawancara

   Wawancara merupakan pertanya langsung yang di tanyakan oleh pihak terkait khsusnya Tim jaringan / pengguna jaringan, yang di lakukan adalah dengan Tim jaringan / pengguna jaringan tersebut menanyakan jaringan yang sedang berjalan untuk menunjang penelitian yang di buat.

3.4 Alat Dan Bahan Penelitian

1. Spesifikasi perangkat keras *(Hardware)* pada penelitian ini sebagai berikut:

Tabel 3. 1 Spesifikasi Hardware

No.	Spesifikasi	Keterangan
1	Sistem Operasi	Windows 10
2	Processor	Intel ® i5
3	RAM	8 GB
4	System Type	64-bit operating system

2. Spesifikasi perangkat Lunak *(Software)* pada penelitian ini sebagai berikut:

Tabel 3. 2 Spesifikasi Software

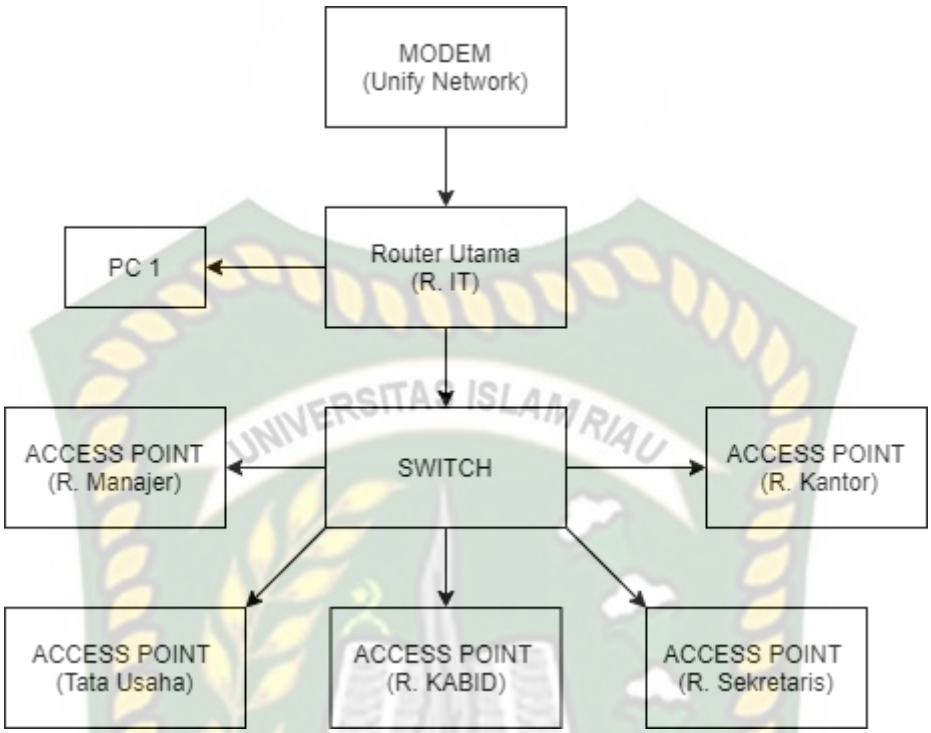
No.	Kebutuhan	Keterangan	Fungsi
1	Sistem Operasi	Window 10, 64 bit	Mengontrol operasi-operasi dasar sistem, termasuk menjalankan perangkat lunak Aplikasi.
2	Aplikasi	Wireshark	Digunakan untuk melakukan analisis dan pemecah masalah jaringan.
3	Aplikasi	Virtual box (Kali Linux)	Digunakan untuk Percobaan Penetrasi pada Jaringan.

3.5 Analisa Sistem

Pada tahap ini akan dijelaskan tentang analisa sistem yang akan dikembangkan.

3.5.1 Analisa Blok Diagram Jaringan

Analisa blok diagram jaringan pada PT. PLN (Persero) Pekanbaru dapat dilihat pada gambar 3.2 di bawah ini.



Gambar 3. 2 Blok Diagram Jaringan

Penjelasan Blok Diagram Jaringan yang digunakan pada Kantor PT. PLN (Persero) Pekanbaru adalah sebagai berikut :

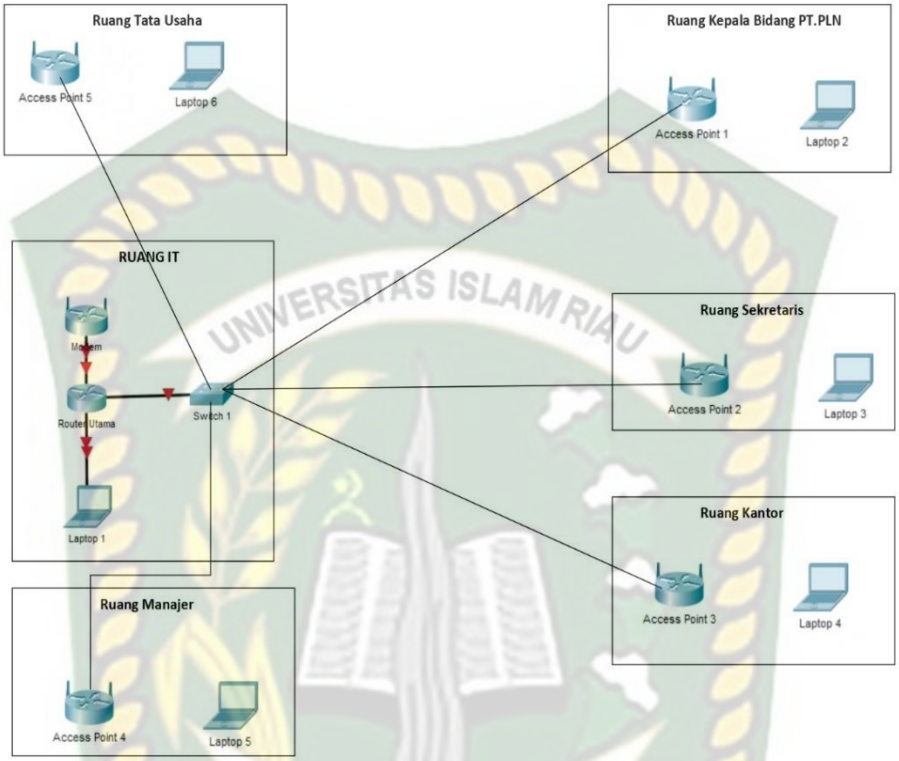
1. PT. PLN (Persero) Pekanbaru menggunakan access point Unifi Ubiquiti dengan internet indihome kapasitas 100 Mbps.
2. Mengunakan Modem Unifi Ubiquiti sebagai alat perantara untuk terhubung ke jaringan internet.
3. Topologi yang digunakan pada Kantor PT. PLN (Persero) Pekanbaru adalah topologi star dan IP Address yang digunakan yaitu IP Address kelas A.
4. Switch sebagai terminal (penghubung) semua komponen data yang terdapat pada jaringan.

5. Mengunakan 1 buah PC yaitu sebagai pengatur Server, untuk mengontrol node pada sebuah jaringan. Dan 10 PC yang terhubung ke Router utama dengan kabel LAN.
6. Mengunakan Router sebagai penghubung antar dua atau lebih jaringan untuk meneruskan data dari satu jaringan ke jaringan lainnya.
7. Access Point sebagai pintu gerbang pengguna wireless di area untuk dapat masuk ke dalam jaringan lokal.

3.5.2 Analisa Sistem Jaringan Kantor PT. PLN (Persero) Pekanbaru

Sistem jaringan yang ada di Kantor PT. PLN (Persero) Pekanbaru yang menggunakan sistem keamanan wi-fi protected access (WPA) dan menggunkanakan OS Windows 10.

Dalam perancangan topologi, Kantor PT. PLN (Persero) Pekanbaru menggunakan jaringan kabel yang terhubung dan dapat diakses jika terhubung ke internet. Topologi yang digunakan adalah topologi star. Prosesnya dapat dilihat pada gambar 3.3.



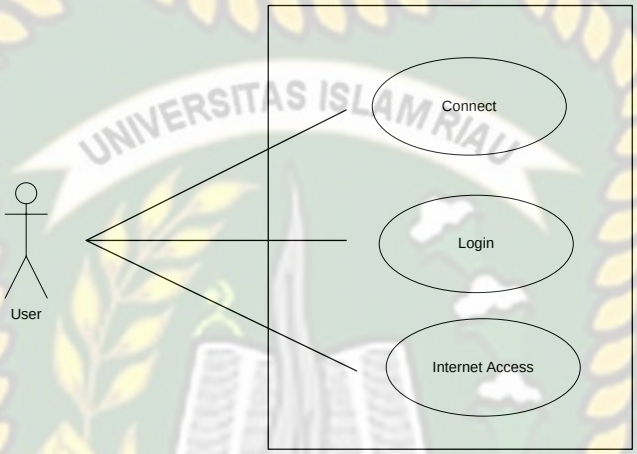
Gambar 3. 3 Topologi Jaringan Fisik PLN

Topologi Logic Jaringan pada Kantor PT. PLN (Persero) Sektor Pengendalian Pembangkitan Pekanbaru:

Tabel 3. 3 Topologi Logic Jaringan PLN

Nama Ruangan	IP Address	Prefix	Netmask
Ruang IT			
-Router Utama	-192.168.100.1	/24	255.255.255.0
-Switch	-DHCP	/24	255.255.255.0
-Modem	-10.26.5.157	/24	255.255.255.0
-PC	-DHCP	/24	255.255.255.0
-Ruang Kepala Bidang PT. PLN			
-Access Point 1	-10.26.5.214	/24	255.255.255.0
-PC/Laptop	-DHCP	/24	255.255.255.0
-Ruang Sekretaris			
-Access Point 2	-10.26.5.24	/24	255.255.255.0
-PC/Laptop	-DHCP	/24	255.255.255.0
-Ruang Kantor			
-Access Point 3	-fe80::2a33::34ff:fec7:fc38	/24	255.255.255.0
-PC/Laptop	-DHCP	/24	255.255.255.0
-Ruang Manejer			
-Access Point 4	-10.26.5.240	/24	255.255.255.0
-PC/Laptop	-DHCP	/24	255.255.255.0
-Ruang Tata Usaha			
-Access Point 5	-10.26.5.277	/24	255.255.255.0
-PC/Laptop	-DHCP	/24	255.255.255.0

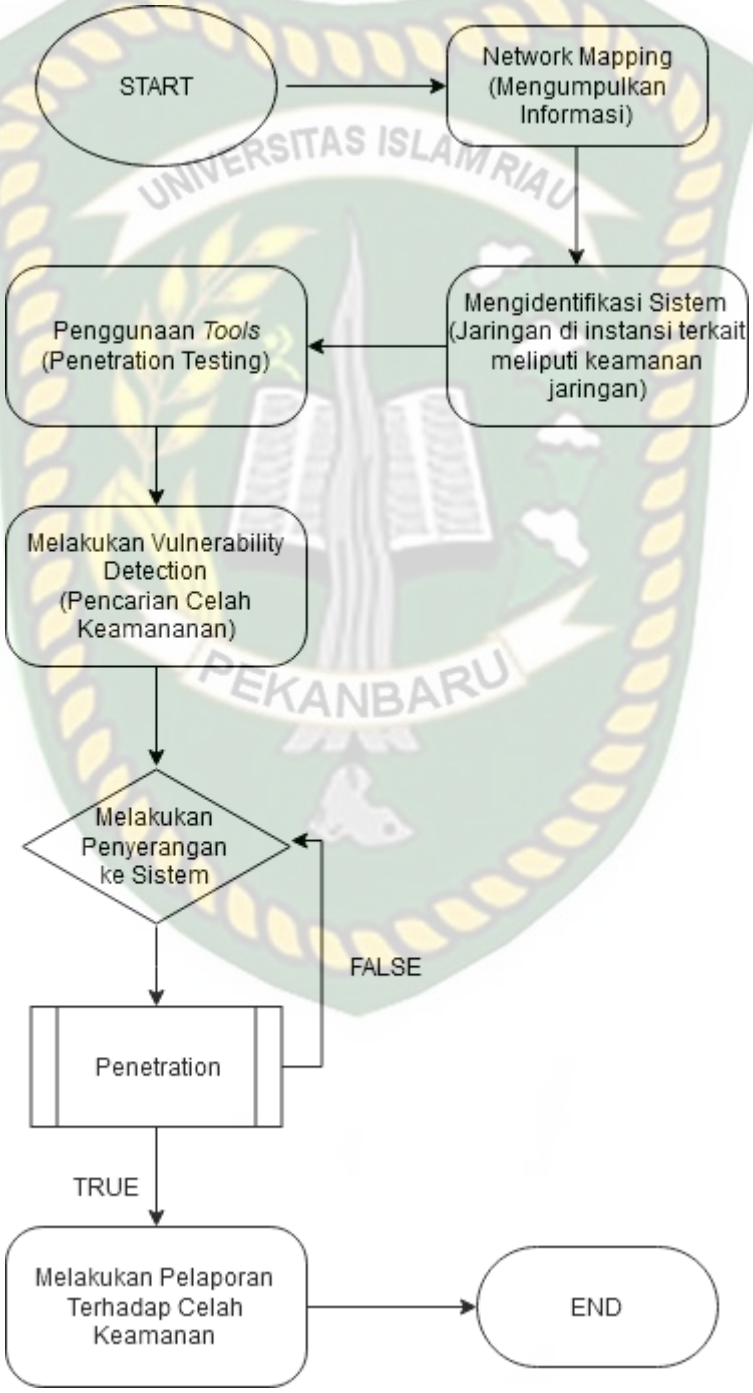
Sistem wi-fi protected access yang ada di Kantor PT. PLN (Persero) Pekanbaru yaitu jika ingin mengakses internet harus memasukkan *Login* atau memasukkan kata sandi pada *internet access*. Proses sistem yang sedang berjalan dapat dilihat pada gambar 3.4.



Gambar 3. 4 Sistem yang sedang berjalan

3.6 Flowchart Alur Penelitian

Pada gambar 3.5 dijelaskan bahwa penelitian ini terbagi menjadi beberapa tahapan alur penelitian beserta penjelasannya, seperti gambar di bawah ini.



Gambar 3. 5 Alur Flowchart Penelitian

Tahapan alur penelitian sebagai berikut:

1. Sebelum penulis melakukan tahap awal penelitian, penulis melakukan Network Mapping mengumpulkan semua ketersediaan referensi sebagai literatur seperti jurnal, buku, artikel dengan tujuan sebagai penunjang pelaksaan penelitian.
2. Penulis Mengidentifikasi Sistem jaringan di instansi terkait meliputi keamanan jaringan.
3. Penulis akan menggunakan tools sebagai percobaan penetration testing.
4. Penulis Melakukan Vulnerabality Detection untuk pencarian celah keamanan.
5. Melakukan penyerangan ke sistem, jika benar maka percobaan penetrasi berhasil dan apabila gagal maka tahap penetrasi akan di uji Kembali.
6. Penulis akan melakukan pelaporan terhadap celah keamanan dan membuat kesimpulan.

BAB IV

HASIL DAN PEMBAHASAN

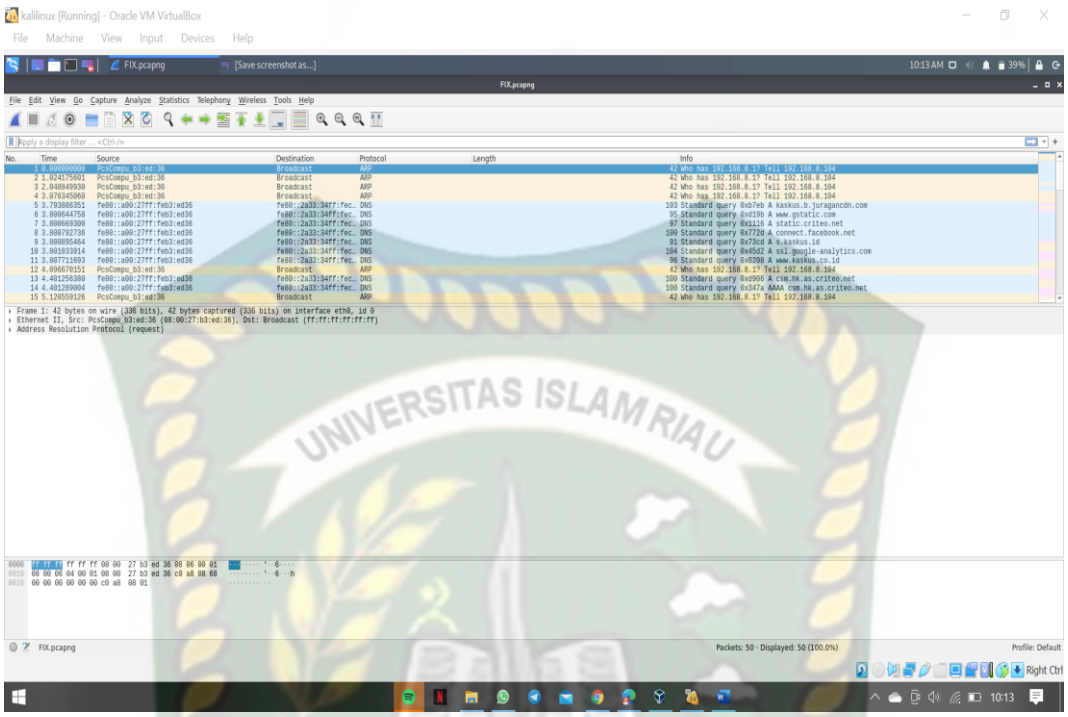
4.1 Hasil dan Pembahasan

Analisis ini perlu dilakukan agar dapat mengetahui seberapa aman tingkat keamanan yang ada dalam sebuah jaringan *wireless lan* pada Kantor PT. PLN (Persero) Pekanbaru. Seperti umumnya tingkat keamanan bukan berasal dari *hardware* dan *software* yang sudah ada namun terdapat peran penting dari manusia / pengguna jaringan yang melakukan kontak atau koneksi dari perancangan jaringan itu sendiri.

Hasil dan pembahasan dari penelitian ini akan dilakukan penetration testing pada sistem *Analisa Lalulintas Jaringan (Traffic Network) Menggunakan Wireshark, Cracking The Encryption,* dan *Man In The Middle* terhadap Access Point.

4.1.1 Analisa Lalulintas Jaringan Menggunakan Wireshark

Pada tahap ini akan dilakukan monitoring packet list (Daftar Paket) dimana sumber ip (Source Ip) dan tujuan ip (Ip Destination) dengan merekam dan memonitoring aktifitas jaringan pada interface wireless di modem Ruang IT (10.26.5.157) menggunakan wireshark. Dengan *capture packet* ini kita dapat mengetahui informasi-informasi seperti *time, source, destination, protocol, length,* dan *info.* Hasil *capture packet* dapat dilihat pada Gambar 4.1 dibawah ini.



Gambar 4. 1 Hasil Capture Packet

Terlihat pada Gambar 4.1, bahwa penulis mengambil sampel sebanyak 10 packet data untuk mengetahui time, source, destination, protocol, length, dan info pada setiap masing-masing ip adress. Berikut penulis akan menyajikannya dalam bentuk hasil tabel, bisa dilihat pada tabel 4.1.

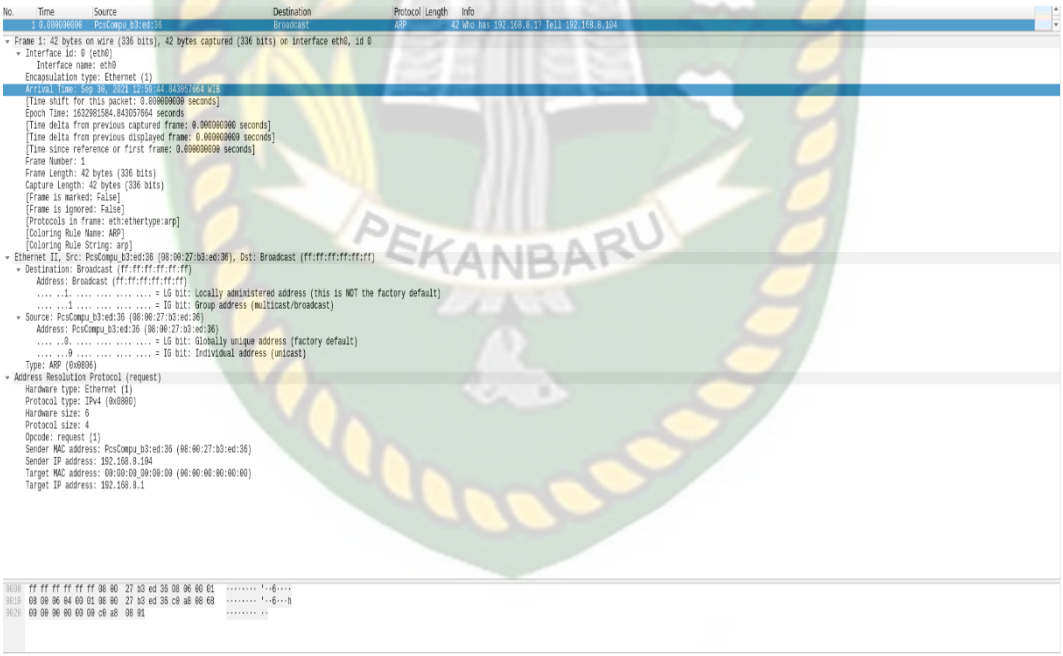
Tabel 4. 1 Hasil Capture Packet

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	PcsCompu_b3:ed:36	Broadcast	ARP	42	Who has 192.168.8.1? Tell 192.168.8.104
2	1.024175601	PcsCompu_b3:ed:36	Broadcast	ARP	42	Who has 192.168.8.1? Tell 192.168.8.104
3	2.048849930	PcsCompu_b3:ed:36	Broadcast	ARP	42	Who has 192.168.8.1? Tell 192.168.8.104
4	3.076345060	PcsCompu_b3:ed:36	Broadcast	ARP	42	Who has 192.168.8.1? Tell 192.168.8.104
5	3.793886351	Fe80::a00:27ff:feb3:ed36	Fe80::2a33:34ff:fec7:fc38	DNS	103	Standard query 0xb7eb A kaskus.b.juragancdn.com
6	3.800644758	Fe80::a00:27ff:feb3:ed36	Fe80::2a33:34ff:fec7:fc38	DNS	95	Standard query 0xd19b A www.Gstatic.com
7	3.800669300	Fe80::a00:27ff:feb3:ed36	Fe80::2a33:34ff:fec7:fc38	DNS	97	Standard query 0x1116 A static.criteo.net
8	3.800792736	Fe80::a00:27ff:feb3:ed36	Fe80::2a33:34ff:fec7:fc38	DNS	100	Standard query 0x772d A Connect.Facebook.net
9	3.800895464	Fe80::a00:27ff:feb3:ed36	Fe80::2a33:34ff:fec7:fc38	DNS	91	Standard query 0x73cd A s.kaskus.id
10	3.801033914	Fe80::a00:27ff:feb3:ed36	Fe80::2a33:34ff:fec7:fc38	DNS	104	Standard query 0x45d2 A ssl.google-analytics.com

Dari tabel diatas dapat diketahui bahwa terdapat 2 protocol yang berbeda yaitu ARP dan DNS, penulis akan menganalisanya untuk mengetahui infomasi secara detail apa saja yang terjadi didalam lalulintas jaringan sebagai berikut:

- **Analisis Protocol ARP**

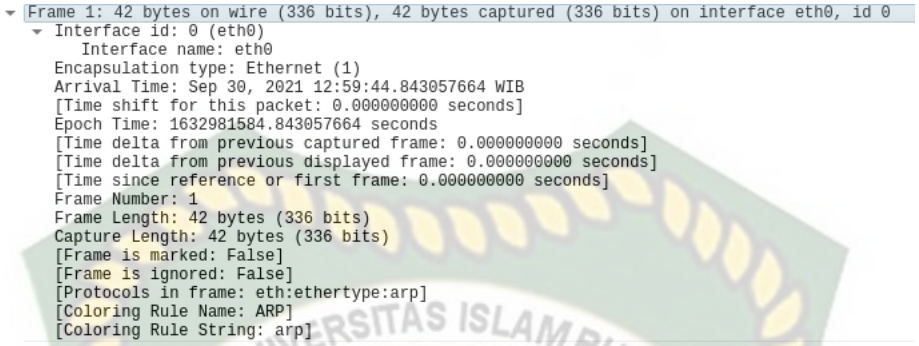
Untuk analisa pertama yaitu dengan melihat informasi lalulintas jaringan pada protocol ARP, penulis akan mengambil sampel dari urutan no 1 dengan Ip sumber (*Source*) PcsCompu_b3:ed:36 dan tujuan (*Destination*) Broadcast, untuk mengetahui informasi secara detail dapat dilihat pada Detail Packet yang terdapat pada gambar 4.2 dibawah ini.



Gambar 4. 2 Detail Paket ARP

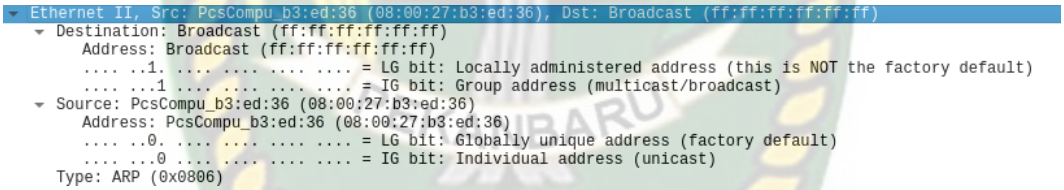
Dari gambar 4.2 diatas ini, akan dijelaskan secara detail tentang Analisa lalulintas jaringan dengan menggunakan wireshark untuk mengetahui informasi dan kesimpulan apa saja yang didapatkan, berikut hasilnya akan dijelaskan pada bagian dibawah ini.

- Didalam box Frame 1 terdapat hal sebagai berikut:



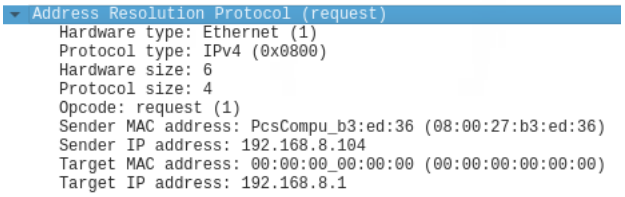
1. Interface name: eth0.
2. Encapsulation type: Ethernet 1.
3. Waktu kedatangan (Arrival Time) 30 September, 2021 pada jam 12:59.44 WIB.

- Didalam box Ethernet II terdapat hal sebagai berikut:



1. Tujuan (Destination): Broadcast (ff:ff:ff:ff:ff:ff).
2. Sumber (Source): PcsCompu_b3:ed:36 (08:00:27:b3:ed:36).
3. Type: ARP (0x0806).

- Didalam box ARP (Address Resolution) terdapat hal sebagai berikut:



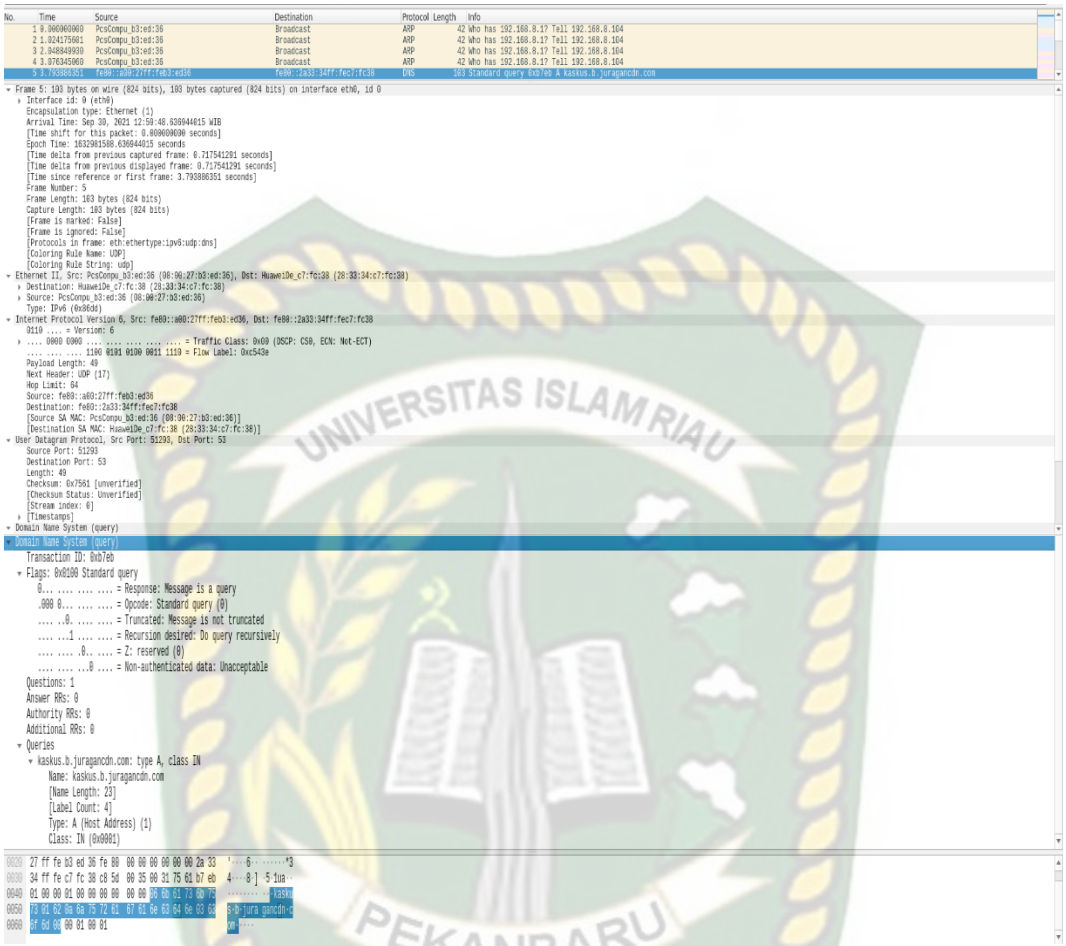
1. Hardware type: Ethernet (1).
2. Protocol type: IPv4 (0x0800).

3. Sender Mac address: PcsCompu_b3:ed:36 (08:00:27:b3:ed:36).
4. Sender IP address: 192.168.8.104.
5. Target Mac address: 00:00:00_ 00:00:00 (00:00:00:00:00:00).
6. Target IP address: 192.168.8.1.

Kesimpulan dari data yang didapat pada gambar diatas dapat diketahui bahwa ARP yang digunakan jenis Ethernet 1 sebagai tipe enkapsulasi dan eth0 sebagai nama interface. Waktu kedatangan (*Arrival Time*) 30 September 2021 pada jam 12:59.44 WIB, yang menunjukkan waktu pengiriman data. ARP request untuk sender dan target dapat diketahui berdasarkan ip address dan juga mac address dari protocol tersebut.

- **Analisis Protocol DNS**

Untuk analisa kedua yaitu dengan melihat informasi lalulintas jaringan pada protocol DNS, penulis akan mengambil sampel dari urutan no 5 dengan Ip sumber (*Source*) fe80::a00:27ff:feb3:ed36 dan tujuan (*Destination*) fe80::2a33:34ff:fec7:fc38, untuk mengetahui informasi secara detail dapat dilihat pada Detail Packet yang terdapat pada gambar 4.3 dibawah ini.



Gambar 4. 3 Detail Paket DNS

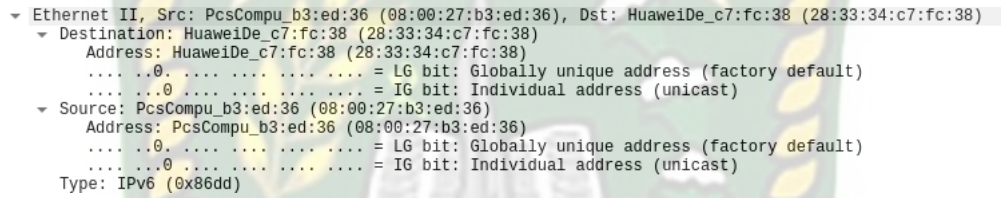
Dari gambar 4.3 diatas ini, akan dijelaskan secara detail tentang Analisa lalulintas jaringan dengan menggunakan wireshark untuk mengetahui informasi dan kesimpulan apa saja yang didapatkan, berikut hasilnya akan dijelaskan pada bagian dibawah ini.

- Didalam box Frame 5 terdapat hal sebagai berikut:

```
Frame 5: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface eth0, id 0
  Interface id: 0 (eth0)
  Encapsulation type: Ethernet (1)
  Arrival Time: Sep 30, 2021 12:59:48.636944015 WIB
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1632981588.636944015 seconds
  [Time delta from previous captured frame: 0.717541291 seconds]
  [Time delta from previous displayed frame: 0.717541291 seconds]
  [Time since reference or first frame: 3.793886351 seconds]
  Frame Number: 5
  Frame Length: 103 bytes (824 bits)
  Capture Length: 103 bytes (824 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ipv6:udp:dns]
  [Coloring Rule Name: UDP]
  [Coloring Rule String: udp]
```

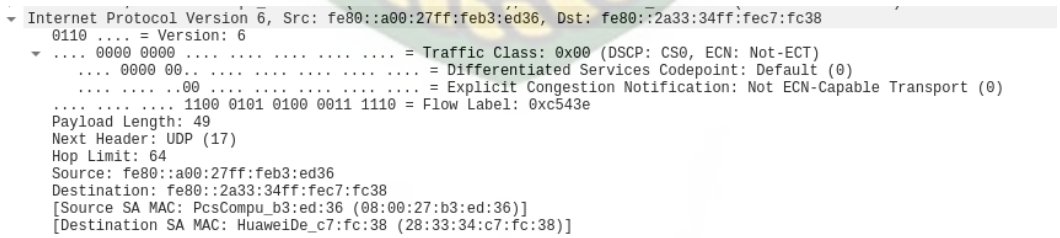
1. Interface id: 0 (eth0), dengan tipe enkapsulasi ethernet 1.
2. Waktu kedatangan (Arrival Time): September 30, 2021. Jam 12:59:48 WIB.
3. Frame & Capture length: 103 bytes (824 bits) jika dikonversikan. Ini merupakan panjang isi paket jika diasumsikan paket sebagai *array of char*.

- Didalam box Ethernet II terdapat hal sebagai berikut:



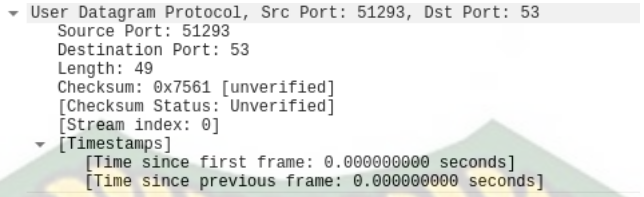
1. Destination (tujuan): HuaweiDe_c7:fc:38 dengan mac address 28:33:34:c7:fc:38.
2. Sorce (sumber): PcsCompu_b3:ed:36 dengan mac address 08:00:27:b3:ed:36.
3. Tipe: IPv6 (0x86dd).

- Didalam box IPv6 terdapat hal sebagai berikut:



1. Source (sumber): fe80::a00:27ff:feb3:ed36.
2. Destination (tujuan): fe80::a00:27ff:feb3:fc38.
3. Payload length: 49, hop limit: 64.

- Didalam box UDP (User Data Protocol) terdapat hal sebagai berikut:



1. Source Port: 51293.
2. Destination Port: 53.
3. Length: 49, Checksum: 0x7561 [unverified] untuk memeriksa kesalahan data.

- Didalam box DNS (Domain Name System) terdapat hal sebagai berikut:

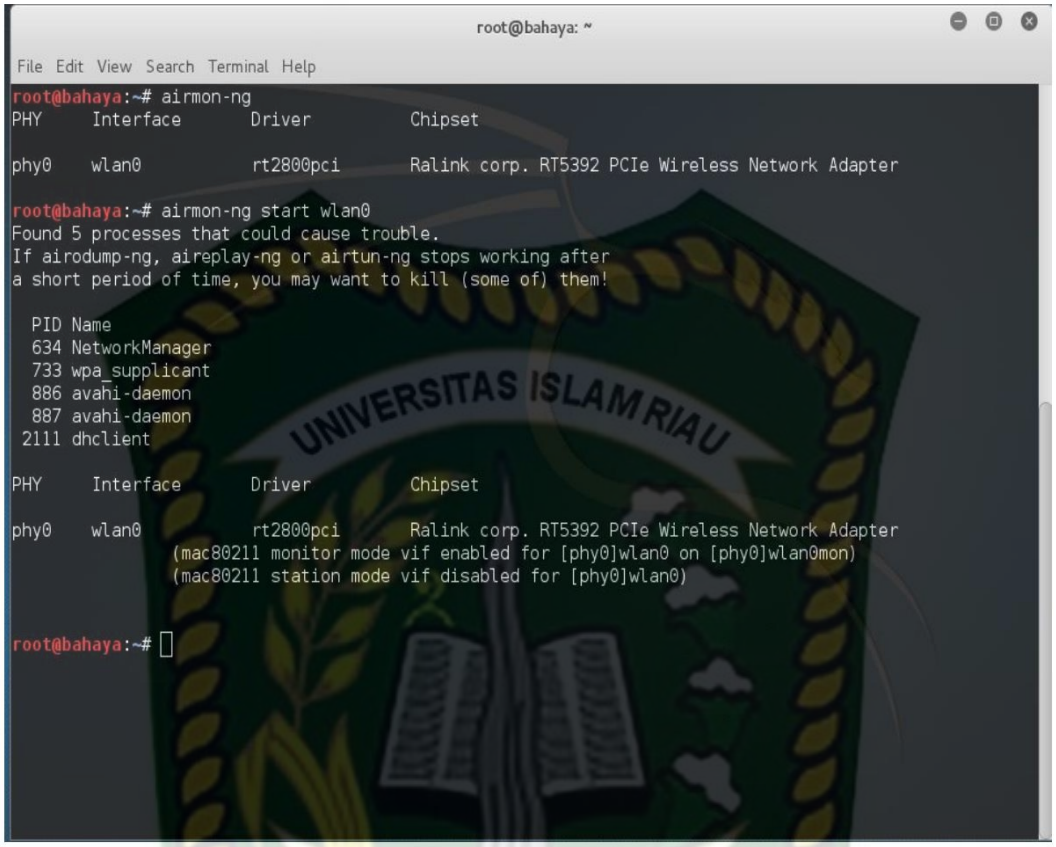
1. ID transaksi: 0xb7eb.
2. Queries: kaskus.b.juragancdn.com: type A, class IN.
3. Name: kaskus.b.juragancdn.com, Name length: 23, Label Count: 4, Type A (host address) dan Class: IN (0x0001).

Kesimpulan dari data yang didapat pada gambar diatas dapat diketahui bahwa DNS yang digunakan jenis Ethernet 1 sebagai tipe enkapsulasi dan eth0 sebagai nama interface. Waktu kedatangan (*Arrival Time*) 30 September 2021 pada jam 12:59.48 WIB, yang menunjukkan waktu pengiriman data. DNS (Domain Name System) dapat diketahui info yang sedang dibuka atau ditelusuri

merupakan situs dari kaskus.b.juragancdn.com. Berhasil mendapatkan informasi berupa Gambar dan Tabel diatas. Informasi ini dinilai krusial karena menyangkut IP dari pengirim dan tujuan, IP ini dapat dimanfaatkan oleh pihak ketiga untuk mendapatkan informasi lebih lanjut yang ada pada komputer yang memiliki IP tersebut. Untuk meningkatkan keamanan jaringan komputer dapat menerapkan mirror server menggunakan Honeypot, agar penyerang tertipu dengan server palsu dengan IP yang sama akan tetapi tidak memiliki folder apapun didalamnya. Cara ini dapat mencegah penyerang yang telah mengetahui IP dari server, yang didapatkan dari teknik Sniffing.

4.1.2 Cracking The Encryption

Tahapan yang pertama, dimana tujuan dari serangan ini adalah untuk mengetahui apakah semua Access Point dilindungi dengan sistem keamanan enkripsi seperti WEP, WPA ataupun WPA2. Penguji melakukan scanning terhadap Access Point Ruang Kantor (fe80::2a33::34ff:fec7:fc38) kemudian menentukan target untuk dilakukan cracking terhadap key yang digunakan sebagai pengamanan yang ditunjukkan pada Gambar 4.4.



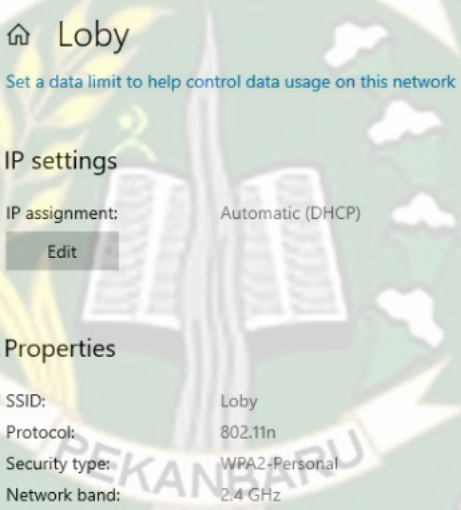
Gambar 4. 4 Perintah Airmon-ng

Dari percobaan Cracking the Encryption dapat ditarik kesimpulan bahwa untuk meningkatkan ketahanan dari password terhadap upaya cracking, maka ada beberapa hal yang harus dilakukan, diantaranya:

1. Menggunakan jenis keamanan enkripsi WPA, WPA2, WPA-PSK, atau WPA2 - PSK (Pre Shared Key) / Personal yang memiliki tingkat keamanan di atas WEP.
2. Menggunakan kombinasi dari huruf besar, huruf kecil, angka dan simbol dalam membuat password, untuk mempersulit serangan baik dengan jenis brute-force attack maupun dictionary.

3. Membuat password dengan panjang di atas 15 karakter, untuk mempersulit serangan baik dengan metode *brute-force attack* maupun *dictionary*.

Dalam percobaan Cracking The Encryption hasil pengujiannya gagal, untuk mengetahui tipe keamanan pada *access point,* penulis akan mengcapture pada bagian properties *access point* seperti pada gambar 4.5.

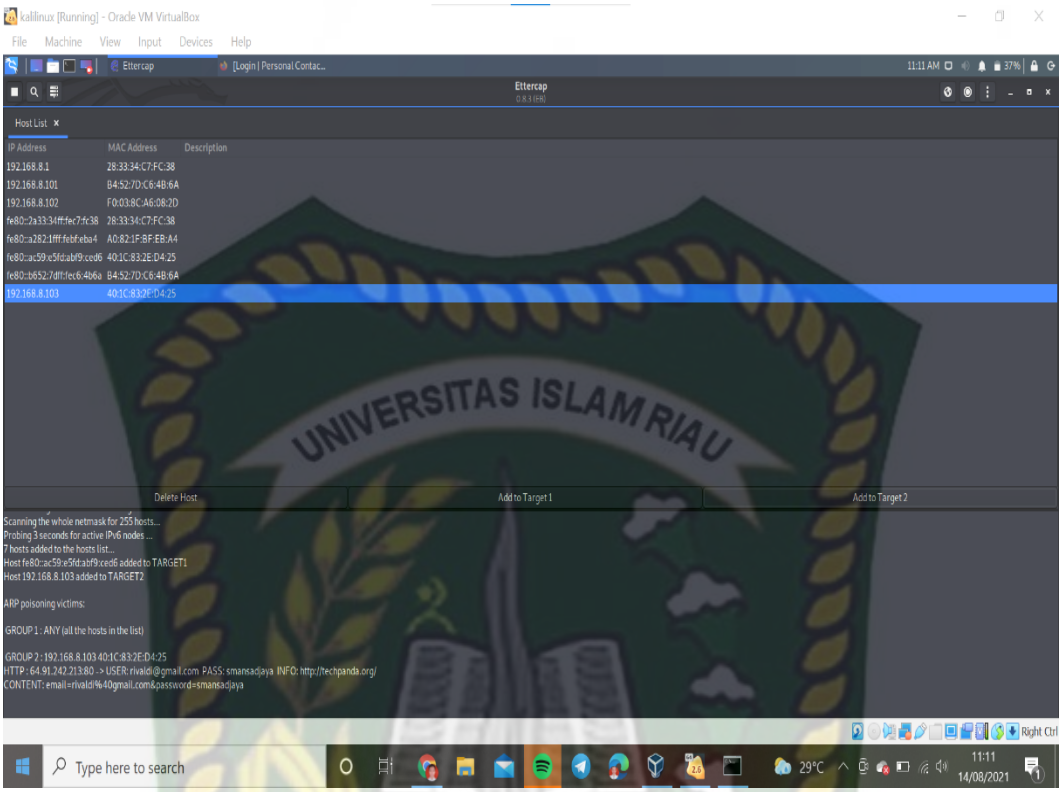


Gambar 4. 5 Tipe Keamanan Access Point

Terlihat dimana type keamanan *access point* yaitu WPA2 - Personal, dimana WPA2 - Personal menggunakan satu kata sandi untuk semua penggunanya.

4.1.3 Man In The Middle (MITM) Attack

Dalam tahap ini dilakukan serangan terhadap *user* lain jaringan Wireless LAN yang sama dengan melakukan penyadapan paket data. Pengujian ini menggunakan aplikasi *Ettercap* sebagai alat uji. Tampilan *Ettercap* ditunjukkan pada Gambar 4.6.



Gambar 4. 6 Hasil Ettercap

Pada tahapan *Man In The Middle Attack*, kondisi awal yang dibutuhkan adalah komputer user dan komputer target harus terhubung di jaringan *wireless Access Point* 'ruang kantor'. Disini komputer tester berperan sebagai pihak ketiga diantara target dan *access point* yang menghubungkan antara target dan layanan internet. Dalam hal ini, pada konfigurasi Ettercap yang menjadi target pertama adalah *gateway* dari *access point* yaitu fe80::2a33::34ff:fec7:fc38 dan yang menjadi target kedua adalah IP dari komputer target yaitu 192.168.8.103.

Tahap selanjutnya adalah melakukan ARP *Poisoning.* Address Resolution Protocol (ARP) adalah sebuah protocol dalam TCP/IP Protocol Suite yang bertanggung jawab dalam melakukan resolusi alamat IP ke dalam alamat Media Access Control (*MAC Address).* ARP Poisoning adalah suatu teknik menyerang pada jaringan komputer local baik dengan media kabel maupun wireless, yang

memungkinkan penyerang bisa mengetahui frames data pada jaringan local atau melakukan modifikasi *traffic* atau bahkan menghentikan traffic. Pada Prinsipnya ARP poisoning ini memanfaatkan kelemahan pada teknologi jaringan komputer sendiri yang menggunakan ARP *broadcast.*

Setelah itu proses *sniffing* dijalankan, untuk kemudian semacam merekam aktifitas komputer target pada saat menggunakan layanan internet. Penulis menyajikannya dalam bentuk Tabel 4.2 dibawah ini.

Tabel 4. 2 Hasil Ettercap

Target 1	**Target 2**	**Informasi**
access point (ip : fe80::2a33::34ff:fec7:fc38)	komputer target (ip:192.168.8.103)	HTTP: 64.91.242.213:80 .> USER: rivaldi@gmail.com PASS: smansadjaya INFO:http://techpanda.org/

Dari percobaan proses sniffing tersebut kemudian berhasil diperoleh informasi bahwa komputer target mengakses situs http://techpanda.org/ dan memasukkan *user* rivaldi@gmail.com serta *passwordnya* smansadjaya. Namun pada saat komputer tester berusaha untuk merekam, pada saat komputer target membuka situs https://www.gmail.com/ ataupun https://www.facebook.com/ aplikasi Ettercap mengalami kegagalan. Setelah dianalisis ditemukan kegagalan dalam proses *sniffing* berasal dari protocol yang digunakan oleh *web server*, yaitu https. Perbedaan antara http dan htpps adalah https bekerja melalui system terenkripsi, sehingga dalam teori, informasi tidak dapat diakses oleh pihak selain klien dan server akhir. Ada dua jenis umum lapisan enkripsi: TLS (Transport

Layer Security) dan SSL (secure Socket Layer), yang keduanya menyandikan catatan data yang dipertukarkan.

Setelah itu kemudian pada komputer target dicoba untuk megakses situs *facebook* dengan cara mengetikkan manual http://www.facebook.com/ pada kolom *url* dari *web browser* yang digunakan yaitu *Mozilla Firefox.* Namun hasilnya pada saat proses berjalan pada kolom *url* Kembali lagi menjadi https. Setelah dilakukan analisis kemudian ditemukan bahwa *website* www.facebook.com ternyata telah menggunakan mekanisme keamanan HSTS. HSTS merupakan singkatan dari (*HTTP Strict Transport Security*) yaitu mekanisme keamanan website yang memaksa *web browser* untuk mengakses *website* hanya via HTTPS.

Jadi faktor kegagalan bukan disebabkan karena konfigurasi keamanan yang dimiliki oleh jaringan WLAN yang ada di 'Ruang kantor', namun lebih kepada konfigurasi keamanan yang dimiliki oleh web server dari situs yang di akses.

4.2 Hasil Penetration Testing

Dari hasil Secara keseluruhan, implementasi dari pengujian keamanan jaringan wireless local area network (WLAN) dengan metode penetration testing dapat dilihat pada Tabel 4.3.

Tabel 4. 3 Hasil Penetration Testing

No.	Jenis Serangan	Informasi yang Dibutuhkan	Status Serangan
1	Analisa Lalulintas Jaringan (Traffic Network) Menggunakan Wireshark	Ip Source dan IP Destination.	Berhasil
2	Cracking The Encryption	Dictionary Word, handshake user lain, Channel yang digunakan dan BSSID dari access point.	Gagal
3	MITM	Attacker harus berada dalam jaringan WLAN, IP address dari user yang terkoneksi.	Berhasil

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan pengujian yang dilakukan Analisis Sistem Keamanan Jaringan Wireless Local Area Network dengan Metode Penetration Testing (Analisa Lalulintas Jaringan (Traffic Network) Menggunakan Wireshark, Cracking The Encryption, Man In The Middle) menggunakan kali linux Pada PT. PLN (Persero) Sektor Pengendalian Pembangkitan Pekanbaru dapat disimpulkan sebagai berikut:

1. Dengan Analisa Lalulintas Jaringan (Traffic Network) Menggunakan Wireshark, dapat ditangkap komunikasi data dari protokol ARP & DNS, sehingga mampu didapatkan informasi yang berupa IP address, time, source, destination, protocol, length, dan info.
2. Keamanan yang dimiliki oleh jaringan WLAN 'PT.PLN (Persero)' masih memiliki banyak celah untuk dieksploitasi. Hal ini dibuktikan dengan hasil penelitian yang dilakukan bahwa dari tiga jenis serangan yang dilakukan, hanya satu yang berstatus gagal yaitu pada jenis serangan cracking the encryption.
3. Pengujian Man In The Middle (MITM), jaringan WLAN belum bisa memberi keamanan kepada user yang terkoneksi agar tidak mendapatkan gangguan maupun penyadapan dari user lain pada saat mengakses layanan internet yang sama.

5.2 Saran

Dengan segala keterbatasan tentang Analisis Sistem Keamanan Jaringan Wireless Local Area Network dengan Metode Penetration Testing Pada PT. PLN (Persero) Sektor Pengendalian Pembangkitan Pekanbaru, Saran terhadap tahap pengembangan sistem keamanan jaringan ini kedepannya agar lebih baik lagi yaitu:

Penetration Testing merupakan tindakan yang membahayakan bagi sistem, maka perlu dipertimbangkan resiko dari tindakan ini. Nilai yang di hasilkan dari pengujian dapat dijadikan acuan dalam meningkatkan kualitas sistem keamanan jaringan WLAN. Diharapkan dapat dikembangkan dengan menggunakan aplikasi dan teknik serangan penetration testing yang lain untuk dapat menjadi bahan evaluasi bagi pengembangan keamanan jaringan WLAN.

DAFTAR PUSTAKA

Alfurqon,D., Assegaff,S, 2018, Analisa Perancangan Jaringan Local Area Network Pada Laboratorium SMK Negeri 1 Kota Jambi, Jurnal Manajemen Sistem Informasi, Vol 3, No 3, ISSN: 2528-0082.

Basten, 2019, Analisa Manejemen Hotspot dengan Captive Portal, *Skripsi*, Program Pasca Sarjana Universitas Negeri Semarang, Unpublished

Jonathan, 2012, Manejemen Jaringan Wireless Menggunakan server Radius, Vol. 20 Nomor 1, ISSN 0853 – 6732

Muttaqin,A.H., Rochim,A.F., dan Widianto,E.D., 2016, Sistem Outentikasi Hotspot Menggunakan LDAP Dan Radius Pada Jaringan Internet Wireless Prodi Teknik Sistem Komputer, *Jurnal Teknologi dan Sistem Komputer*, Vol. 4 Nomor 2, hal Jtsiskom 282 – 288, E-ISSN:2338-0304

Najoan, 2019, Analisis Dan Implementasi Sistem Redundant hot Standby Network Security Menggunakan Metode Intrusion Preventi Sistem (IPS), *Bianglala Informatika,*Vol. 2 No 2, Hal. 112-119

Purwanto,D., dan Dana,RD., 2015, Sistem Keamana Jaringan Model Client Server Menggunakan Enksripsi Data (MD5) Pada Dinas Kesehatan Kota Cirebone, *Jurnal Online ICT STMIK IKM*, Vol. 13 Nomor 1

Riyasa,S., Mulyadi,A., dan Purwanto,Y., 2018, Analisa Dan Implementasi Sistem Redundasi Hot Standby Network Security Menggunakan Metode Intrusion Prevention System (IPS) Dan Captive Portal Pada Jaringan Nirkabel, *Jurnal Teknik Komputer*, No. 1 Vol.10

Setiawan,H, 2018, Rancangan Bangun Captive Portal Untuk Jaringan Wireless Berbasi open Source pada CV. Gempar production Palembang, *Jurnal Teknologi Informasi*, Vol. 7 No. 1, Hal. 36-44.

Sumarianta, 2011, Instalasi dan Konfigurasi Jaringan Komputer, Pustaka Setia, Bandung.

Suprianto,A., Riadi,I., 2013, Rancang Bangun Sistem Hotspot Menggunakan Captive Portal, *Jurnal Sarjana Teknik Informatika*, Vol. 1 Nomor 1, hal 172-180, E-ISSN: 2338-5197.

Wijaya,I.H., 2015, Analisis Dan Implementasi Proxy Server Sebagai Web Caching, Blocking Situs, Dan Monitoring Menggunakan Centos 6 Di Smkn Ganesha Tama Boyolali, *Jurnal Teknologi Informasi & Pendidikan*, Vol. 3 No 1.