ANALISIS KEAMANAN JARINGAN PADA FASILITAS INTERNET (WIFI) TERHADAP SERANGAN PACKET SIFFING

Disusun dan Diajukan untuk Memenuhi Persyaratan Ujian Akhir Memperoleh
Gelar Sarjana Komputer pada Fakultas Sains dan Teknologi
Universitas Pembangunan Panca Budi
Medan

SKRIPSI

OLEH

NAMA	**: TAUFIQ ISMAIL SIREGAR**
NPM	**: 1514370436**
PROGRAM STUDI	**: SISTEM KOMPUTER**

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2019

ABSTRAK

TAUFIQ ISMAIL SIREGAR

Analisis Keamanan Jaringan Pada Fasilitas Internet (WIFI) Terhadap Serangan Packet Sniffing

Jaringan komputer mempunyai dua media transmisi data yaitu kabel dan nirkabel PT.(PERSERO) Angkasa Pura II Bandar Udara Internasional Kualanamu Medan merupakan salah satu Badan Usaha Milik Negara (BUMN) yang mempunyai fasilitas jaringan nirkabel (*wifi*). Jaringan *wifi* sangat rentan terhadap ancaman serangan, karena komunikasi yang terjadi berifat terbuka. Diperlukan sistem pengamanan yang baik untuk dapat menjaga keamanan data pengguna agar terhindar dari serangan yang dilakukan oleh orang-orang yang tidak bertanggung jawab. Penelitian ini membahas evaluasi tingkat keamanan fasilitas *wifi* di PT.(PERSERO) Angkasa Pura II Bandar Udara Internasional Kualanamu Medan dengan menggunakan aplikasi *ettercap*. *Ettercap* adalah *tools packet sniffer* yang dipergunakan untuk menganalisa protokol jaringan dan mengaudit keamanan jaringan, yang juga memiliki kemampuan untuk memblokir lalu lintas pada jaringan *LAN*, mencuri *password*, dan melakukan penyadapan aktif terhadap protokol-protokol umum.

Kata Kunci : *Ettercap, LAN , password.*

KATA PENGANTAR

Puji syukur Tuhan yang Maha Esa karena dengan berkat dan kasih anugrah-Nya penulis masih diberikan kesehatan dan keselamatan.

Skripsi disusun berdasarkan hasil penelitian yang dilaksanakan pada PT.(PERSERO) Angkasa Pura II Bandar Udara Internasional Kualanamu Medan dengan judul "ANALISIS KEAMANAN JARINGAN PADA FASILITAS INTERNET (WIFI) TERHADAP SERANGAN PAKET SNIFFING".

Dalam kesempatan ini, penulis mengucapkan terimakasih yang sebesar-besarnya kepada banyak pihak yang telah membantu dalam penyelesaian penyusunan Tugas Akhir ini. Penulis ingin mengucapkan terimakasih kepada :

1. Ibunda penulis tercinta, Hj. Nurleni Purba.
2. Abang penulis tersayang M. Okto Zainuddin Siregar.
3. Kakak penulis tersayang Nuradha Nina Siregar.
4. Abang penulis tersayang Baginda Mulya Hadi Siregar.
5. Pendamping penulis tersayang Giassanistya Fadillah Marpaung.
6. Sahabat dan teman teman yang tidak bisa disebutkan satu persatu.
7. Rektor Universitas Pembangunan Pancabudi, Bapak Dr. H. Muhammad Isa Indrawan, S.E, M.M.
8. Rektor I, Bapak Ir. Bhakti Alamsyah, M.T,Ph.D.
9. Dekan Fakultas Sains dan Teknologi, Ibu Sri Shindi Indira, ST., M.Sc.
10. Ketua Program Studi Sistem Komputer, Bapak Dr. Muhammad Iqbal, S.Kom., M.Kom.
11. Dosen Pembimbing I, Ibu Leni Marlina, S.Kom., M.Kom.
12. Dosen Pembimbing II, Bapak Dian Kurnia, S.Kom., M.Kom.

Penulis juga menyadari bahwa penyusunan skripsi ini belum sempurna baik dalam penulisan maupun isi disebabkan keterbatasan kemampuan penulis. Oleh karena itu, penulis mengharapkan kritik dan saran yang sifatnya membangun dari pembaca untuk penyempurnaan isi skripsi ini.

Medan, 28 Agustus 2019

Penulis

(Taufiq Ismail Siregar)
(1514370436)

DAFTAR GAMBAR

Halaman

DAFTAR ISI

DAFTAR LAMPIRAN

Halaman

DAFTAR TABEL

Halaman

BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Pada saat ini *issue* kemanan jaringan menjadi sangat penting dan patut untuk diperhatikan, jaringan yang terhubung dengan internet pada dasarnya tidak aman dan selalu dapat diekploitasi oleh para hacker, baik jaringan *wired LAN* maupun *wir*eless *LAN*. Pada saat data dikirim akan melewati beberapa terminal untuk sampai tujuan berarti akan memberikan kesempatan kepada pengguna lain yang tidak bertanggung jawab untuk menyadap atau mengubah data tersebut. Dalam pembangunan perancangannya, sistem kemanan jaringan yang terhubung ke internet harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif dan meminimalisir terjadinya serangan oleh para hacker.

Ettercap adalah *tools packet sniffer* yang dipergunakan untuk menganalisa protocol jaringan dan mengaudit kemanan jaringan. Ia memiliki kemampuan untuk memblokir lalu lintas pada *LAN*, mencuri password, dan melakukan penyadapan aktif terhadap protokol-protokol umum.

PT. (Persero) Angkasa Pura II merupakan salah satu Badan Usaha Milik Negara (BUMN) dalam lingkungan Departemen Perhubungan yang bergerak dalam bidang perhubungan udara khususnya penyedia jasa penerbangan udara. Wilayah kerja PT. (Persero) Angkasa Pura II meliputi sebagian besar bandara-bandara di kawasan barat Indonesia, sedangkan kawasan timur Indonesia

pengaturannya ditangani oleh PT. (Persero) Angkasa Pura II. manajemen Banda Udara Internasional Kualanamu Medan berada dalam wilayah kerja PT. (Persero) Angkasa Pura II Bandar Udara Internasional Kualanamu Medan.

Saat ini PT. (Persero) Angkasa Pura II cabang Bandar Udara Internasional Kualanamu Medan telah menerapkan jaringan komputer kabel maupun nirkabel sebagai media petukaran data/informasi pelayanan umum atau komersial, kepegawaian dan informasi penting lainnya. Terdapat dua jaringan yang terpasang dalam lingkup Bandara Internasional Kualanamu Medan yaitu :

1. Terinstal pada gedung baru yang didalamnya terdapat ruang/kantor TU, Kasir, Administrasi dan Pelayanan Umum dengan menerapkan jaringan kabel
2. Terinstal pada kantor Telekomunikasi dan Navigasi (TelNav) yang terhubung dengan terminal bandara dengan menerapkan jaringan kabel dan terdapat dua access point sebagai jaringan kabel.

Menurut Thomas Setiawan (2004), pada penelitian dengan judul Analisis Keamanan jaringan Internet Menggunakan *Hping, Nmap, Nessus,* dan *Ethereal* yang berisi bahwa sistem keamanan jaringan komputer yang terhubung ke internet harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang berada didalam jaringan tersebut secara efektif. Apabila ingin mengamankan suatu jaringan maka harus ditentukan terlebih dahulu tingkat ancaman yang harus diatasi, dan resiko yang harus diambil maupun dihindari.

Berdasarkan penelitian terdahulu yaitu penelitian dari Hendri Noviyanto (2011) dengan judul Analisis Keamanan *Wireless* di Universitas Muhammadiyah Surakarta yang berisi tentang pemakaian pemakaian *access point* yang mudah, bisa disembarang tempat yang terjangkau sinyal *wireless* tanpa harus berada disebuah tempat tertentu untuk dapat mengakses internet. Dalam penerapannya *wireless* menggunakan gelombang radio untuk saling berkomunikasi atau bertukar informasi dari point ke point yang lain, sehingga jaringan tersebut sangat rawan dari serangan para penjahat dunia maya. Kondisi tersebut ditambah para pemula yang memasang *access point* untuk *hotspot* tanpa sepengetahuan yang berwenang. Karena kurangnya pengetahuan, sebuah *access point* tersebut dipasang tanpa pengamanan dan hanya bergantung pada *settingan* dari *vendor*.

Penelitian penulis sekarang memanfaatkan *tools netstumbler* untuk mendeteksi dan mengidentifikasi sinyal *wireless* yang terbuka dan menyusup kedalam jaringan. *Sniffing* adalah tindakan penyadapan yang dilakukan dalam jaringan dengan tujuan untuk dapat mencuri data-data pribadi ataupun *account* lain yang bersifat pribadi. Karena data yang mengalir pada jaringan bersifat bolak-balik, maka dengan proses *sniffing* ini dapat menangkap paket yang dikirimkan dan terkadang menguraikan isi dari RFC (*Request for Comments*).

Berdasarkan uraian di atas, penulis tertarik untuk mempelajari cara mengamankan suatu jaringan. Oleh karena itu, penulis mengambil bahan mengenai “Analisis Keamanan Jaringan Pada Fasilitas Internet (WIFI) Terhadap Serangan Packet Sniffing”.

1.2 Rumusan Masalah

Dengan berdasarkan latar belakang masalah dan hubungannya dengan pemilihan judul tersebut, maka penulis merumuskan pokok permasalahan yaitu Bagaimana menganalisis keamanan fasilitas internet (WIFI) di PT. (Persero) Angkasa Pura II Bandar Udara Internasional Kualanamu Medan untuk mengetahui sejauh mana kualitas keamanan fasilitas internet (WIFI) di PT. (Persero) Angkasa Pura II Bandar Udara Internasional Kualanamu Medan.

1.3 Batasan Masalah

Dalam penelitian ini, penulis membatasi masalah yang akan dianalisis yaitu:

1. Penggunaan aplikasi *Ettercap* untuk menganalisa keamanan jaringan di PT. (Persero) Angkasa Pura II Bandar Udara Internasional Kualanamu Medan.
2. Penulis tidak melakukan implementasi peningkatan kemanan jaringan yang sudah ada dan hanya memberikan solusi yang sebaiknya dilakukan untuk mengantisipasi terjadinya serangan seperti yang dilakukan penulis.
3. Keamanan jaringan yang diamati di PT. (Persero) Angkasa Pura II Bandar Udara Internasional Kualanamu Medan hanya pada jaringan *wireless.*

1.4 Tujuan Penelitian

Tujuan yang hendak dicapai penulis dalam penelitian ini adalah untuk menganalisa tingkat keamanan fasilitas internet (WIFI) di PT. (Persero) Angkasa Pura II Bandar Udara Internasional Kualanamu Medan.

1.5 Manfaat Penelitian

Penelitian ini bermanfaat untuk, antara lain :

1. Sebagai data yang bisa diberikan dan digunakan oleh pihak IT TelNav di PT. (Persero) Angkasa Pura II Bandar Udara Internasional Kualanamu Medan guna mengamankan jaringan computer *LAN* agar lebih baik.
2. Sebagai pengetahuan bagi pengguna layanan / fasilitas internet (WIFI maupun kabel *LAN*) khususnya bagi pengguna yang awam terhadap bahaya jaringan *LAN* tanpa pengamanan.

BAB II
LANDASAN TEORI

Menurut Thomas Setiawan (2004), pada penelitian dengan judul Analisis Keamanan Jaringan Internet Menggunakan *Hping, Nmap, Nessus,* dan *Ethereal*, yang berisi bahwa Sistem keamanan jaringan komputer yang terhubung ke internet harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif. Apabila ingin mengamankan suatu jaringan maka harus ditentukan terlebih dahulu tingkat ancaman yang harus diatasi, dan resiko yang harus diambil maupun yang harus dihindari.

Penelitian lain yang dijadikan acuan adalah penelitian Aji Supriyanto (2006) dengan judul Analisis Kelemahan Keamanan Pada Jaringan *Wireless*, isi dari penelitiannya adalah pemakaian perangkat teknologi berbasis *wireless* pada saat ini sudah begitu banyak, baik digunakan untuk komunikasi suara maupun data. Karena teknologi *wireless* memanfaatkan frekwensi tinggi untuk mengantarkan sebuah komunikasi, maka kerentanan terhadap keamanan juga lebih tinggi disbanding dengan teknologi komunikasi lainnya. Berbagai tindakan pengamanan dapat dilakukan melalui perangkat komunikasi yang digunakan oleh *user* maupun operator yang memberikan layanan komunikasi. Kelamahan jaringan *wireless* secara umum dapat dibagi menjadi 2 jenis, yakni kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang digunakan. Secara garis besar, celah pada jaringan *wireless* terbentang di atas empat *layer* di mana keempat lapis tersebut sebenarnya merupakan proses dari terjadinya komunikasi data pada

media *wireless*. Keempat lapis tersebut adalah lapis fisik, lapis jaringan, lapis *user*, dan lapis aplikasi. Model-model penanganan keamanan yang terjadi pada masing-masing lapis pada teknologi *wireless* tersebut dapat dilakukan antara lain yaitu dengan cara menyembunyikan *SSID,* memanfaatkan kunci *WEP, WPA-PSK* atau *WPA2-PSK*, implementasi fasilitas *MAC filtering*, pemasangan infrastruktur *capative portal*.

Berdasarkan penelitian terdahulu yaitu penelitian dari Hendri Noviyanto (2011) dengan judul Analisis Keamanan Wireless di Universitas Muhammadiyah Surakarta yang berisi tentang pemakaian-pemakaian *acces point* yang mudah, bias disembarang tempat yang terjangkau sinyal *wireless* tanpa harus berada disebuah tempat tertentu untuk dapat mengakses internet. Dalam penerapannya *wireless* menggunakan gelombang radio untuk saling berkomunikasi atau untuk bertukar informasi dari point ke point yang lain, sehingga jaringan tersebut sangat rawan dari serangan para penjahat dunia maya. Kondisi tersebut ditambah para pemula yang memasang *access point* tanpa sepengetahuan yang berwenang, karena kurangnya pengetahuan, sebuah *access point* tersebut dipasang tanpa pengaman dan hanya bergantung pada *settingan* dari vendor.

2.1 Keamanan Jaringan Komputer

2.1.1 Keamanan Komputer

Menurut Gollmann (1999) keamanan komputer adalah berhubungan dengan pencegahan diri dan deteksi terhadap tindakan pengganggu yang tidak dikenali dalam sistem komputer. Sedangkan

menurut John D. Howard (1997) keamanan komputer adalah tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab. Jaringan komputer adalah sebuah sistem yang terdiri atas komputer-komputer yang didesain untuk dapat berbagai sumber daya (printer, CPU), berkomunikasi (surel, pesan instan), dan dapat mengakses informasi (peramban web). Setiap bagian dari jaringan komputer dapat meminta dan memberikan layanan (*service*). Menurut David Icove (1997) berdasarkan lubang kemanan, keamanan komputer dapat dibagi menjadi 4 macam, yaitu :

a. Keamanan Fisik (*Physical Security*)

   Termasuk akses orang ke gedung, peralatan, dan media yang digunakan. Contoh : *Wiretapping* atau hal-hal yang ber-hubungan dengan akses ke label atau komputer yang digunakan juga dapat dimasukkan ke dalam kelas ini.

b. *Denial Of Service*

   Dilakukan misalnya dengan mematikan peralatan atau membanjiri saluran komunikasi dengan pesan-pesan (yang dapat berisi apa saja karena yang diutamakan adalah banyaknya jumlah pesan)

c. *Syn Flood Attack*

   Dimana sistem (*host*) yang dituju dibanjiri oleh permintaan sehingga dia menjadi terlalu sibuk dan bahkan dapat berakibat macetnya sistem (*hang*).

d. Keamanan yang berhubungan dengan orang

Contoh : Identifikasi *user* (*username* dan *password*), profil resiko dari orang yang mempunyai akses (pemakai dan pengelola).

2.1.2 Jaringan Komputer

Pihak yang meminta/menerima layanan disebut peladen (server), desain ini disebut dengan sistem Iclient-server, dan digunakan pada hamper seluruh aplikasi jaringan komputer Jafar Noor Yudianto (2013). Sedangkan menurut Abdul Kadir (2003) Jaringan komputer adalah hubungan dua buah simpul (umumnya berupa komputer) atau lebih yang tujuan utamanya adalah untuk melakukan pertukaran data. Yudianto (2007) mengatakan pula bahwa pada dasarnya, jaringan komputer merupakan suatu bentuk interkoneksi atau hubungan antar komputer, yang pada dasarnya memiliki beberapa jenis, ditinjau dari 4 aspek atau bagian. Berikut ini adalah beberapa jenis dari jaringan komputer

a. Berdasarkan jangkauan geografis

Apabila dibedakan menurut jangkauan geografisnya, maka jaringan komputer dapat dibagi dan dibedakan menjadi 3 jenis jaringan, yaitu :

1. Jaringan local (*LAN*) atau *Local Area Network*.
2. Jaringan perkotaan (*MAN*) atau *Metropolitan Area Network*.
3. Jaringan Luas (*WAN*) *Wide Area Network*.

b. Berdasarkan distribusi data atau sumber informasi

Aspek berikutnya dalam pembagian jenis jaringan adalah berdasarkan distribusi data. Apabila dilihat berdasarkan distribusi data, maka, jaringan komputer dapat dibedakan menjadi 2 jenis, yaitu :

1. Jaringan terpusat.
2. Jaringan terdistribusi.

c. Berdasarkan media transmisi dari jaringan komputer

Jaringan komputer membutuhkan media untuk dapat mentransmisikan paket data yang akan dibagikan antar komputer. Karena itu, jaringan komputer juga dapat dibedakan menjadi 2 jenis jaringan apabila dilihat dari media transmisi jaringannya :

1. Jaringan kabel (*Wired Network*)
2. Jaringan nirkabel (*Wireless Network*)

d. Berdasarkan peran komputer dalam proses transmisi data

Dengan adanya banyak komputer yang saling terhubung satu sama lain di dalam sebuah jaringan, maka ada 2 jenis jaringan yang dibedakan menurut peranan komputer sebagai perangkat kertas jaringan komputer. Berikut ini adalah jenisnya :

1. *Client-to-server connection*.
2. *Peer to peer connection*.

2.1.3 Keamanan jaringan komputer

Menurut Ri2M (2010) keamanan jaringan dapat digambarkan secara umum yaitu apabila komputer yang terhubung dengan jaringan yang lebih banyak mempunyai ancaman keamanan dari pada komputer yang tidak terhubung ke mana – mana. Namun dengan adanya pengendalian maka resiko yang tidak diinginkan dapat dikurangi. Adanya keamanan jaringan maka para pemakai berharap bahwa pesan yang dikirim dapat sampai dengan baik ke tempat yang dituju tanpa mengalami adanya kecacatan yang diterima oleh si penerima, misalnya saja adanya perubahan pesan. Biasanya jaringan yang aksesnya semangkin mudah, maka keamanan jaringannya semangkin rawan, namun apabila keamanan jaringan semangkin baik maka pengaksesan jaringan juga semangkin tidak nyaman.

Didalam keamanan jaringan terdapat pula resiko jaringan komputer yang merupakan segala bentuk ancaman baik fisik maupun logik yang langsung atau tidak langsung mengganggu kegiatan yang sedang berlangsung dalam jaringan. Resiko dalam jaringan komputer disebabkan oleh beberapa factor yaitu :

1. Kelemahan manusia.
2. Kelemahan perangkat keras komputer.
3. Kelemahan sistem operasi jaringan.
4. Kelemahan sistem jaringan komunikasi.

Selain itu, keamanan jaringan juga mempunyai tujuan yang dapat membuat keamanan jaringan lebih ditingkatkan lagi, yaitu :

a. Confidentiality

Adanya data – data yang paling penting yang biasanya tidak boleh diakses oleh seseorang, maka dilakukan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Biasanya *confidentialy* ini berhubungan dengan informasi yang diberikan ke pihak lain.

b. *Integrity*

Bahwa pesan yang disampaikan tetap orisinil yang tidak diragukan keasliannya, tidak dimodifikasi selama dalam perjalanan dari sumber ke penerimanya.

c. *Avaibility*

Dimana user yang mempunyai hak akses diberi akses tepat pada waktunya, biasanya ini berhubungan dengan ketersediaan informasi atau data ketika dibutuhkan. Apabila sistem informasi ini diserang maka akan menghambat bahkan menyebabkan tidak dapat mengakses informasi tersebut.

Tujuan keamanan jaringan dapat dicapai dengan suatu metode keamanan jaringan yang dapat melindungi sistem baik dari dalam maupun dari luar jaringan, namun bukan hanya melindungi tetapi harus dapat bertindak apabila terjadi serangan yang ada didalam jaringan. Salah satu metode tersebut yaitu *Intrusion Detection System* (*IDS*) dan *Intrusion*

Prevention System (*IPS*). Namun, selain metode tersebut dibutuhkan juga suatu pemahaman tentang menentukan kebijakan keamanan (*security policy*) dalam keamanan jaringan. Jika ingin menentukan apa saja yang harus dilindungi maka harus mempunyai perencanaan keamanan yang matang dan baik berdasarkan pada peosedur dan kebijakan keamanan jaringan, karena apabila tidak direncanakan maka tidak akan sesuai dengan yang diharapkan dalam perindungan jaringan.

2.2 Konsep Keamanan Jaringan Komputer

Pada saat ini *issue* kemanan jaringan komputer menjadi sangat penting dan patut untuk diperhatikan, jaringan yang terhubung dengan internet pada dasarnya tidak aman dan selalu dapat dieksploitasi oleh para *hacker*, baik jaringan *LAN* maupun *wireless*. Pada saat data dikirim akan melewati beberapa terminal untuk sampai tujuan berarti akan memberikan kesempatan kepada pengguna lain yang tidak bertanggung jawab untuk menyadap dan mengubah data tersebut. Dalam pembangunan perancangannya, sistem keamanan jaringan yang terhubung ke internet harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan tersrbut secara efektif dan meminimalisir terjadinya serangan oleh para *hacker*.

Apabila ingin mengamankan suatu jaringan maka harus ditentukan terlebih dahulu tingkat ancaman yang harus diatasi, dan resiko yang harus diambil maupun yang harus dihindari. Berikut ini akan dibahas mengenai ancaman, kelemahan, dan *policy* keamanan jaringan.

2.2.1 Ancaman

Pada dasarnya, ancaman datang dari seseorang yang mempunyai keinginan memperoleh akses ilegal kedalam suatu jaringan computer. Oleh karena itu, harus ditentukan siapa saja yang diperbolehkan mempunyai akses legal kedalam sistem, dan ancaman-ancaman yang dapat mereka timbulkan. Ada beberapa tujuan yang ingin dicapai oleh para penyusup dan sangat berguna apabila dapat membedakan tujuan-tujuan tersebut pada saat merencanakan sistem keamanan jaringan computer. Beberapa tujuan para penyusup adalah :

a. Pada dasarnya hanya ingin tahu sistem dan data yang ada pada suatu jaringan computer yang dijadikan sasaran. Penyusup yang bertujuan seperti ini sering disebut dengan *the curius.*
b. Membuat sistem jaringan menjadi down, atau mengubah tampilan situs web. Penyusup yang mempunyai tujuan seperti ini sering disebut sebagai *the malicious*.
c. Berusaha untuk menggunakan sumber daya didalam sistem jaringan komputer untuk memperoleh popularitas. Penyusup seperti ini sering disebut sebagai *the high-profile intruder*.
d. Ingin tahu data apa saja yang ada didalam jaringan komputer untuk selanjutnya dimanfaatkan untuk mendapatkan uang. Penyusup seperti ini sering disebut sebagai *the competition.*

2.2.2 Kelemahan

Kelemahan menggambarkan seberapa kuat sistem keamanan suatu jaringan komputer terhadap jaringan komputer yang lain dan kemungkinan bagi seseorang untuk mendapat akses ilegal kedalamnya.

2.3 Jenis-Jenis Ancaman Keamanan Jaringan

Jenis-jenis ancaman jaringan komputer adalah sebagai berikut.

2.3.1 Packet Sniffer

Packet *Sniffer* adalah sebuah metode serangan dengan cara mendengarkan seluruh paket yang lewat pada sebuah media komunikasi baik itu media kabel ataupun nirkabel. Setelah paket-paket yang lewat itu didapatkan, paket-paket tersebut kemudian disusun ulang sehingaa data yang dikirimkan oleh sebuah pihak dapat dicuri oleh pihak yang tidak berwenang. Hal ini dapat dilakukan karena pada dasarnya sebuah koneksi *Ethernet* adalah koneksi yang bersifat *broadcast*, dimana semua host dalam sebuah kelompok jaringana akan menerima paket yang dikirimkan oleh sebuah host. Cukup sulit untuk melindungi diri dari gangguan ini karena sifat dari *packet sniffing* yang merupakan metode pasif (pihak penyerang tidak perlu melakukan apapun, hanya perlu mendengar saja).

2.3.2 ARP spoofing / ARP poisoning

ARP (Address Resolution Protocol) poisoning ini adalah suatu teknik menyerang pada jaringan komputer lokal baik dengan media kabel atau *wireless*, yang memungkinkan penyerang bisa mengendus *frames*

data pada jaringan lokal dan melakukan modifikasi *traffic* atau bahkan menghentikan *traffic. ARP spoofing* merupakan konsep dari serangan penyadapan diantara dua mesin yang sedang berkomunikasi atau disebut dengan *MITM* (*Man in The Middle Attack*). Prinsip serangan *ARP poisoning* ini memanfaatkan kelemahan pada teknologi jaringan komputer itu sendiri yang menggunakan *ARP broadcast. ARP* berada pada layer 2, dimana alamat dari layer 2 adalah *MAC address*. Misalnya pada host (contoh : PC) yang terhubung pada sebuah *LAN* ingin menghubungi host lain pada *LAN* tersebut, maka dia membutuhkan informasi *MAC address* dari *host* tujuan.

2.3.3 Probe

Sebuah *probe* dapat dikenali dari adanya usaha-usaha yang tidak lazim untuk memperoleh akses kedalam suatu sistem atau untuk menemukan informasi tentang sistem tersebut. Salah satu contohnya adalah usaha untuk login kedalam sebuah akun yang tidak digunakan. *Probing* ini dapat dianalogikan sebagai usaha untuk memasuki sebuah ruangan dengan mencoba-coba apakah pintunya terkunci apa tidak.

2.3.4 Scan

Scan adalah kegiatan *probe* dalam jumlah besar dan menggunakan *tool* secara otomatis. *Tool* tersebut secara otomatis dapat mengetahui port-port yang terbuka pada *host local* maupun *host remote, IP address* yang aktif, bahkan bisa untuk mengetahui sistem operasi yang digunakan pada host yang dituju.

2.3.5 Account Compromise

Account Compromise adalah penggunaan akun sebuah komputer secara ilegal oleh seseorang yang bukan pemilik akun tersebut, *account compromise* dapat mengakibatkan korban mengalami kehilangan atau kerusakan data. Sebuah insiden *account compromise* dapat berakibat lebih lanjut, yaitu terjadinya insiden *root compromise*, yang dapat menyebabkan kerusakan lebih besar.

2.3.6 Root Compromise

Root Compromise mirip dengan *account compromise*, dengan perbedaan *account* yang digunakan secara ilegal adalah *account* yang mempunyai *privilege* sebagai administrator sistem. Isitilah *root* diturunkan dari sebuah *account* pada sistem berbasis UNIX yang mempunyai *previlage* tidak terbatas. Penyusup yang berhasil melakukan *root compromise* dapat melakukan apa saja pada sistem yang menjadi korban, termasuk menjalankan program, mengubah kinerja sistemn dan menyembunyikan jejak penyusupan.

2.3.7 Denial Of Service (DOS)

Sumber daya jaringan yang berharga antara lain komputer dan database, serta layanan-layanan (service) yang disediakan oleh organisasi pemilik jaringan. Kebanyakan user jaringan memanfaatkan layanan-layanan tersebut agar pekerjaan mereka jadi efisien. Bila pelayanan ini tidak dapat dipergunakan karna sebab sebab tertentu, maka tentu saja akan menyebabkan kehilangan produktivitas. Sulit untuk memperkirakan

penyebab *denial of service*. Berikut adalah contoh penyebab terjadinya *denial of service* :

a. Kemungkinan jaringan menjadi tidak berfungsi karena kebanjiran traffic.
b. Kemungkinan ada virus yang menyebar dan menyebabkan sistem komputer menjadi lamban atau bahkan lumpuh.
c. Kemungkinan device yang melindungi jaringan dirusak.

2.4 Topologi Jaringan Komputer

Menurut Jaffar Noor Yudianto (2002) topologi jaringan komputer adalah suatu sistem yang terdiri atas sebuah beberapa komputer yang didesain untuk bisa saling berbagi sumber daya (printer, CPU), berkomunukasi (surel, pesan instan), dan bisa mengakses informasi (peramban web). Sedangkan menurut Abdul kadil (2006) definisi topologi jaringan komputer adalah suatu hubungan dua buah simpul (umumnya berupa komputer) atau lebih yang tujuan utamanya yaitu untuk melakukan pertukaran data.

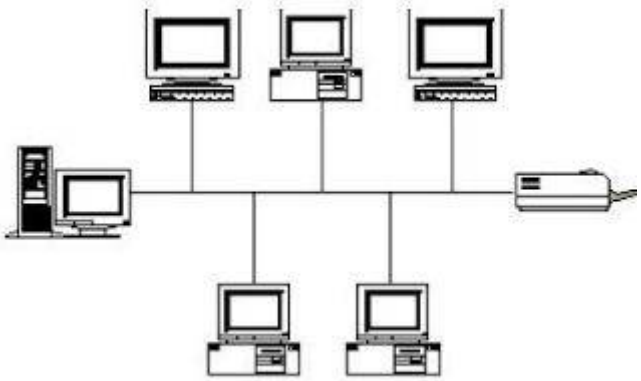
Dalam instalasi jaringan, kita perlu memperhatikan kategori, kelebihan & kekurangan masing-masing topologi jaringan yang dapat kita pakai.

Berikut jenis-jenis topologi jaringan beserta kelebihan dan kekurangannya :

1. Topologi BUS

   Topologi bus adalah topologi yang cukup sederhana jika dibandingkan dengan topologi lainnya. Topologi bus umumnya digunakan pada

instalasi jaringan berbasis *fiber optic*, selanjutnya digabungkan dengan topologi *star/*topologi bintang untuk menghubungkan *client* atau *node*. Topologi bus hanya menggunakan satu kabel *type coaxial* disepanjang *node client*. Biasanya, ujung kabel *coaxial* tersebut diberikan T konektor yang merupakan kabel *end to end*.



Gambar 2.1 Topologi Bus

Kelebihan dari topologi bus adalah sebagai berikut :

a. Biaya instalasi yang dapat dibilang amat sangat murah lantaran hanya menggunakan sedikit kabel.
b. Tambahan *Client* / *workstation* baru akan dilakukan dengan mudah.
c. Topologi yang amat sangat sederhana dan gampang diaplikasikan.

Kekurangan dari topologi bus adalah sebagai berikut :

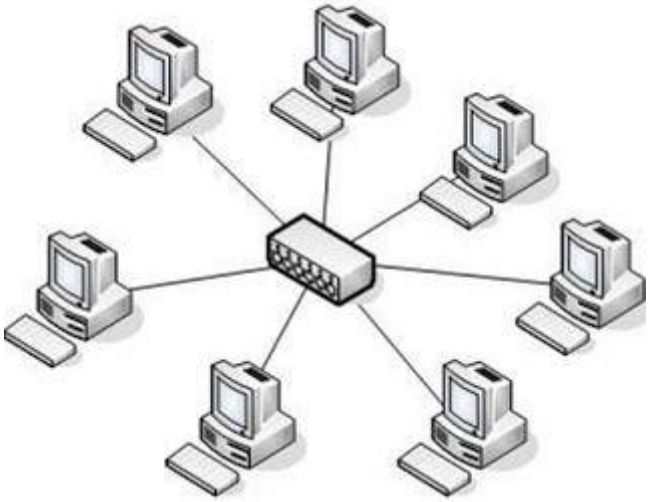
a. Apabila salah satu kabel pada topologi jaringan bus putus atau bermasalah, faktor tersebut akan mengganggu komputer *workstation* / *client* lainnya.

b. Proses *sending* (mengirim) dan *receiving* (menerima) data kurang efisien, bahkan sering terjadi tabrakan data pada topologi ini.

c. Topologi yang teramat jadul dan susah dikembangkan.

2. Topologi Star

Topologi star atau topologi bintang adalah salah satu bentuk topologi jaringan yang umumnya memakai *switch* / *hub* untuk menghubungkan *client* satu dengan *client* lainnya.



Gambar 2.2 Topologi Star

Kelebihan dari topologi star adalah sebagai berikut :

a. Jika salah satu komputer mengalami masalah, jaringan pada topologi ini masih dapat berjalan dan tidak akan mempengaruhi komputer/pc lainnya.

b. Tingkat keamanan dapat dibilang cukup baik daripada topologi bus.

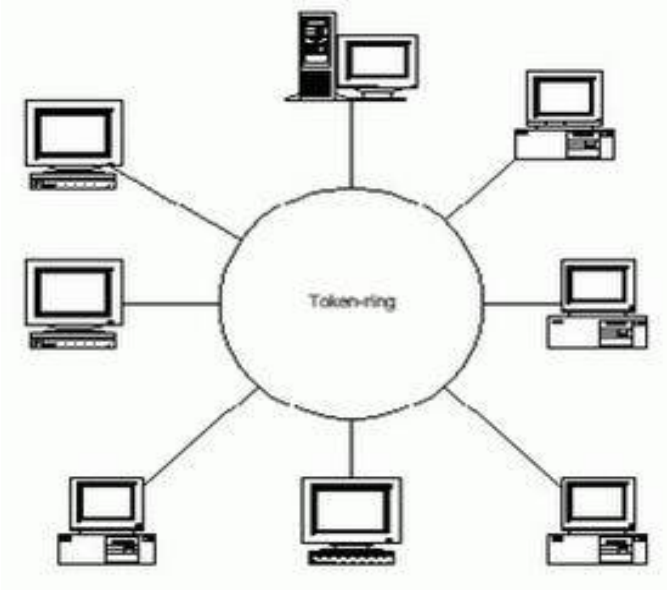
c. Kemudahan deteksi masalah cukup mudah bila terjadi kerusakan pada jaringan. Selain itu, setiap node memiliki akses ke *bandwith* penuh dari *LAN*, setidaknya dilingkungan *LAN switch*.

Kekurangan dari topologi star adalah sebagai berikut :

a. Apabila *switch* / *hub* yang notabenenya sebagai titik pusat mengalami masalah, maka semua komputer yang mengakses pada topologi ini pun mengalami masalah.
b. Membutuhkan banyak kabel, sehingga biaya atau anggaran yang dikeluarkan dapat dibilang cukup mahal.
c. Jaringan sangat tergantung pada terminal pusat.

3. Topologi Ring

Topologi ring atau cincin adalah salah satu topologi jaringan yang menghubungkan satu pc / komputer dengan pc / komputer yang lain dalam satu buah rangkaian melingkar, serupa dengan cincin. Kebanyakan topologi ini cuma memanfaatkan kartu *LAN* untuk menghubungkan komputer satu pc / komputer yang lain.



Gambar 2.3 Topologi Ring

Kelebihan dari topologi ring adalah sebagai berikut :

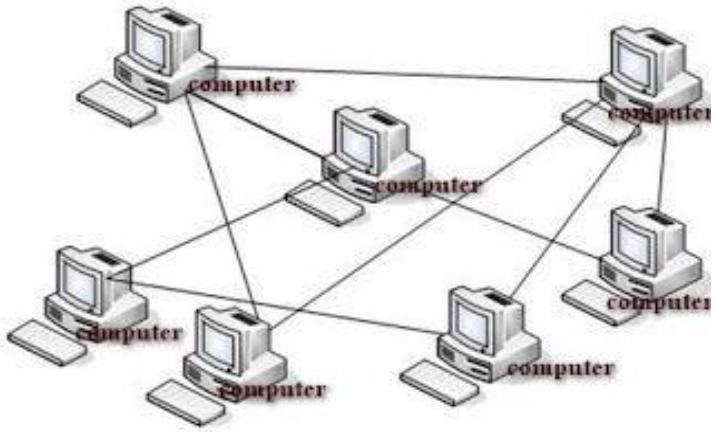
a. Mempunyai performa yang tambah baik daripada topologi bus.
b. Mudah diimplementasikan.
c. Konfigurasi ulang dan instalasi perangkat baru dapat dibilang cukup mudah.
d. Anggaran instalasi lumayan murah.

Kekuranga dari topologi ring adalah sebagai berikut :

a. Kinerja komunikasi dalam topologi ini dinilai dari jumlah / sejumlah titik atau node.
b. *Troubleshooting* lumayan rumit.
c. Apabila salah satu koneksi putus, sehingga koneksi lainnya pun ikut terputus.
d. Pada topologi ini biasanya berjalan *collison* (tabrakan data).

4. Topologi Mesh

Topologi mesh yakni bentuk topologi yang sangat tepat dalam aspek pemilihan rute yang banyak. Faktor tersebut berfungsi sebagai jalur *backup* pada waktu jalur lain mengalami masalah.



Gambar 2.4 Topologi Mesh

Kelebihan dari topologi mesh adalah sebagai berikut :

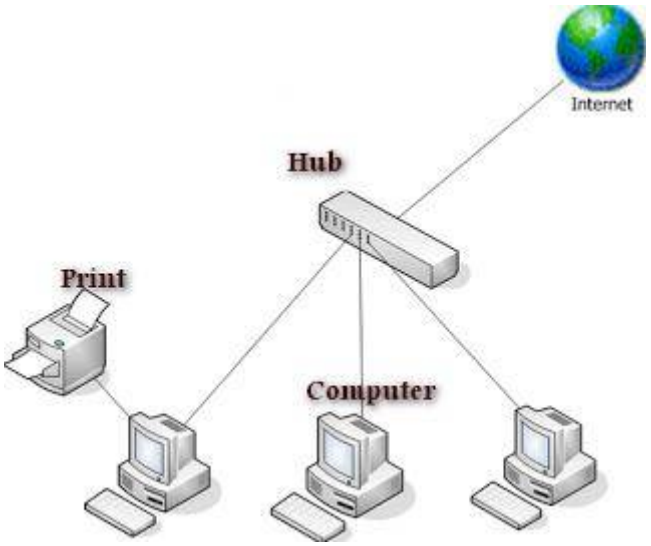
a. Jalur pengiriman data yang diperlukan sangat banyak, jadi tidak perlu khawatir akan adanya tabrakan data (*collison*).
b. *Bandwith* yang lumayan lebar.
c. Keamanan kepada topologi ini dapat dibilang amat sangat baik.

Kekurangan dari topologi mesh adalah sebagai berikut :

a. Proses instalasi jaringan pada topologi ini sangatlah rumit.
b. Membutuhkan banyak label.
c. Memakan anggaran instalasi yang amat mahal, lantaran membutuhkan tidak sedikit kabel.

5. Topologi Peer to Peer

Topologi peer to peer adalah topologi yang amat sangat sederhana sebab hanya memanfaatkan 2 buah komputer / pc untuk saling membuka. Pada topologi ini kebanyakan memakai satu kabel yang menghubungkan antar pc / komputer untuk memproses pertukaran data.



Gambar 2.5 Topologi Peer to Peer

Kelebihan dari topologi peer to peer adalah sebagai berikut :

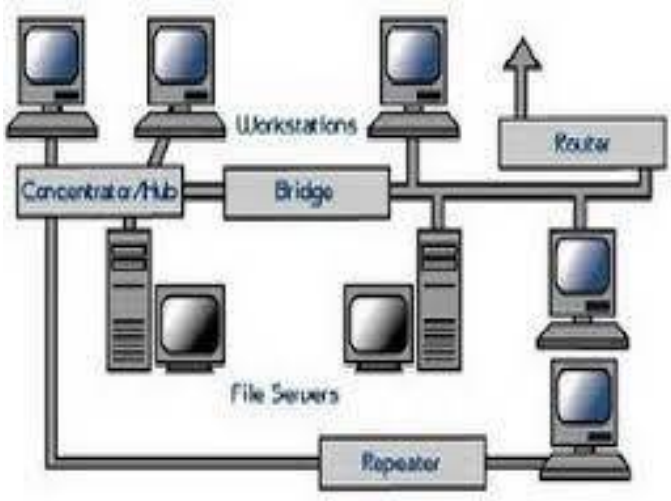
a. Anggaran yang dibutuhkan cukup murah.
b. Masing-masing pc / komputer akan berperan juga sebagai client ataupun server.
c. Instalasi jaringan yang lumayan mudah.

Kekurangan dari topologi peer to peer adalah sebagai berikut :

a. Keamanan pada topologi type ini bisa dibilang amat sangat rentan.
b. Susah dikembangkan.
c. Sistem keamanan dikonfigurasi oleh masing-masing pengguna.
d. *Troubleshooting* jaringan rumit.

6. Topologi Linier

Topologi linier atau biasanya dinamakan topologi bus beruntut. Pada topologi ini umumnya memakai satu kabel utama guna menghubungkan tiap titik sambungan pada tiap-tiap komputer.



Gambar 2.6 Topologi Linier

Kelebihan dari topologi linier adalah sebagai berikut :

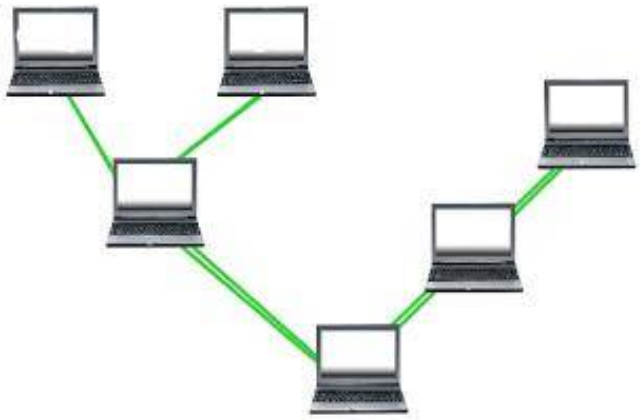
a. Mudah dikembangkan.
b. Membutuhkan sedikit kabel.
c. Tidak membutuhkan kendali pusat.
d. Tata letak terhadap rangkaian topologi ini dapat dibilang cukup sederhana.

Kekurangan dari topologi linier adalah sebagai berikut :

a. Mempunyai kepadatan lalu lintas.
b. Keamanan data kurang baik.

7. Topologi Tree

Topologi tree atau pohon ialah topologi gabungan antara topologi star dan topologi bus. Topologi jaringan ini umumnya difungsikan untuk interkoneksi antar sentral dengan hirarki yang berbeda-beda.



Gambar 2.7 Topologi Tree

Kelebihan dari topologi tree adalah sebagai berikut :

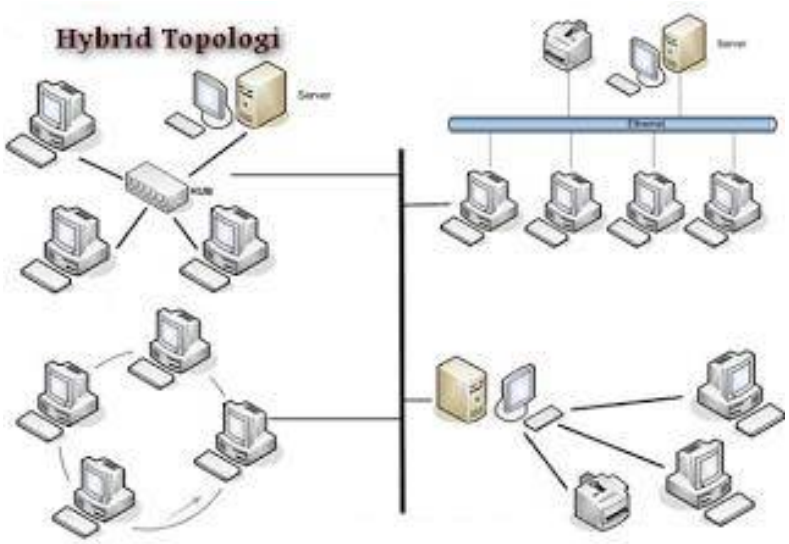
a. Susunan data terpusat dengan cara hirarki, faktor tersebut menciptakan manajemen data tambah baik dan mudah.
b. Mudah dikembangkan jadi jaringan yang lebih luas lagi.

Kekurangan dari topologi tree adalah sebagai berikut :

a. Seandainya komputer yang menduduki tingkatan paling atas mengalami masalah, sehingga komputer yang terdapat dibawahnya pun ikut bermasalah.
b. Kinerja jaringan pada topologi ini terbilang lambat.
c. Memanfaatkan banyak kabel dan kabel terbawah (backbone) yakni pusat dari teknologi ini.

8. Topologi Hybrid

Topologi *hybrid* yaitu topologi gabungan antara sekian banyak topologi yang tidak serupa. Terhadap dikala dua atau lebih topologi yang tidak sama membuka satu sama lain, dikala itulah gabungan topologi tersebut menempa topologi *hybrid*.



Gambar 2.8 Topologi Hybrid

Kelebihan dari topologi *hybrid* ini adalah sebagai berikut :

a. Fleksibel.
b. Tambahan koneksi yang lain benar-benar mudah.

Kekurangan dari topologi *hybrid* adalah sebagai berikut :

a. Pengelolahan pada jaringan *hybrid* benar-benar sulit.
b. Anggaran pembangunan yang mahal.
c. Instalasi dan konfigurasi jaringan pada topologi ini dapat dibilang cukup rumit, dikarenakan terdapat topologi yang berbeda-beda.

BAB III
METODE PENELITIAN

3.1 Tahapan Penelitian

Tahapan-tahapan penelitian adalah sebagai berikut.

3.1.1 Waktu dan Tempat Penelitan

Penelitian dilaksanakan pada bulan maret 2019 bertempat di PT. (PERSERO) Angkasa Pura II cabang Bandar Udara Internasional Kualanamu Medan.

3.1.2 Profil Secara Umum

PT. (Persero) Angkasa Pura II merupakan salah satu Badan Usaha Milik Negara (BUMN) dalam lingkungan Departemen Perhubungan yang bergerak dalam bidang perhubungan udara khususnya penyedia jasa penerbangan udara. Wilayah kerja PT. (Persero) Angkasa Pura II meliputi sebagian besar bandara-bandara di kawasan barat Indonesia, sedangkan kawasan timur Indonesia pengaturannya ditangani oleh PT. (Persero) Angkasa Pura I. manajemen Banda Udara Internasional Kualanamu Medan berada dalam wilayah kerja PT. (Persero) Angkasa Pura II Bandar Udara Internasional Kualanamu Medan.

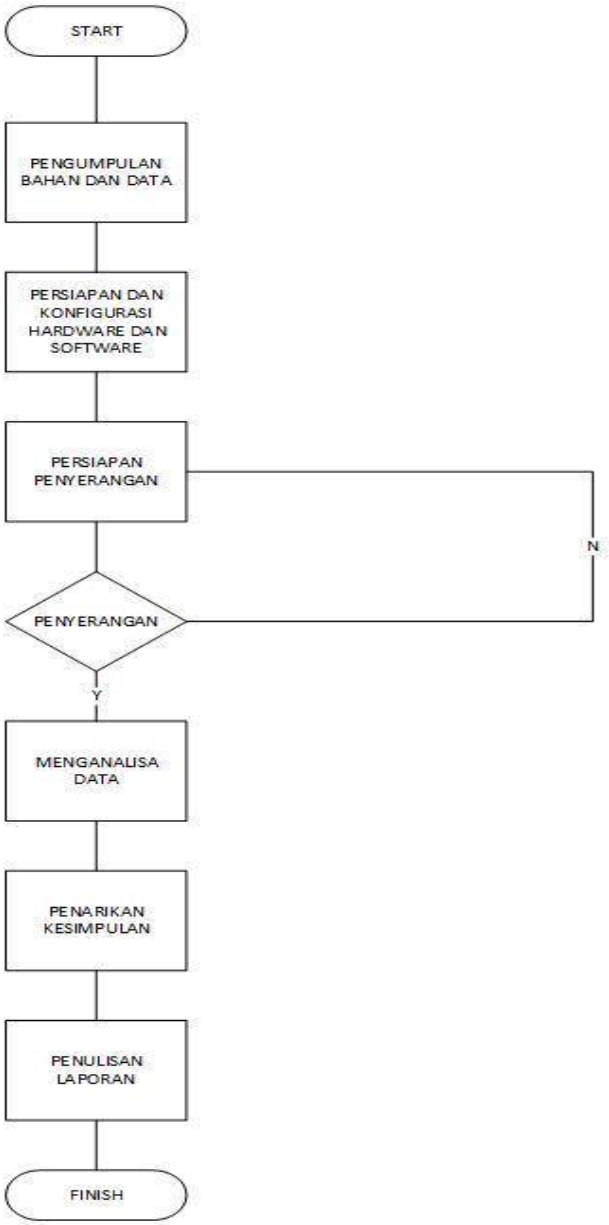
Saat ini PT. (Persero) Angkasa Pura II cabang Bandar Udara Internasional Kualanamu Medan telah menerapkan jaringan komputer kabel maupun nirkabel sebagai media petukaran data/informasi pelayanan umum atau komersial, kepegawaian dan informasi penting lainnya.

Terdapat dua jaringan yang terpasang dalam lingkup Bandara Internasional Kualanamu Medan yaitu :

1. Terinstal pada gedung baru yang didalamnya terdapat ruang/kantor TU, Kasir, Administrasi dan Pelayanan Umum dengan menerapkan jaringan kabel
2. Terinstal pada kantor Telekomunikasi dan Navigasi (TelNav) yang terhubung dengan terminal bandara dengan menerapkan jaringan kabel dan terdapat dua access point sebagai jaringan kabel.

3.1.3 Kerangka Pemikiran dan Flowchart

Dalam menjelaskan sebuah permasalahan kerangka pemikiran atau alur penelitian disajikan untuk mempermudah pemahaman dalam penelitian tersebut. Metode tersebut tersaji dalam diagram alir penelitian.



Gambar 3.1 Diagram Alir Penelitian

Sesuai dengan diagram alir penelitian diatas penelitian ini dilakukan dalam beberapa tahapan.

a. Menyiapkan *literature*, buku-buku, *ebook* dan artikel untuk menunjang penelitian.
b. Memenuhi persyaratan / prosedur perizinan penelitian yang diberikan oleh pihak KesKam (keselamatan dan keamanan) di PT. (PERSERO) Angkasa Pura II cabang Bandar Udara Internasional Kualanamu Medan, karena tidak semua tempat / lokasi boleh masuk kecuali karyawan tertentu yang berhak.
c. Mencari informasi data-data yang ada, konfigurasi jaringan kabel *LAN* dan *wifi* yang terpasang diseluruh lingkup Bandar Udara Internasional Kualanamu meliputi tempat, SSID, BSSID, enkripsi yang digunakan, channel.
d. Menyiapkan *hardware* dan *software* yang dibutuhkan untuk menunjang pelaksanaan penelitian.
e. Melangkah untuk melakukan sebuah percobaan penyerangan kepada jaringan kabel *LAN* dan *wifi* untuk mendapatkan informasi tentang keamanannya.
f. Menarik kesimpulan untuk memutuskan sebuah saran yang bisa digunakan untuk mengamankan jaringan kabel *LAN* dan *wifi* melihat dari sisi pengguna.

3.2 Metode Pengumpulan Data

Metode pengumpulan data yang digunakan oleh penulis disini adalah metode penelitian lapangan (*field research*), yaitu mengumpulkan data tentang obyek penelitian di lapangan atau di lokasi objek penelitian berkedudukan.

3.3 Analisis Sistem Sedang Berjalan

3.3.1 Instalasi dan konfigurasi software

Dalam penelitian ini penulis menggunakan applikasi *Ettercap.* Tahapan-tahapan instalasi dan konfigurasi *software* tersebut adalah sebagai berikut.

1. Instalasi *software Ettercap* pada *Ubuntu* 18.04
    a. Pertama update *index package* terlebih dahulu melalui terminal dengan perintah *command* :

       # sudo apt-get update

    b. Kemudian install *Ettercap-gtk deb package* dengan perintah :

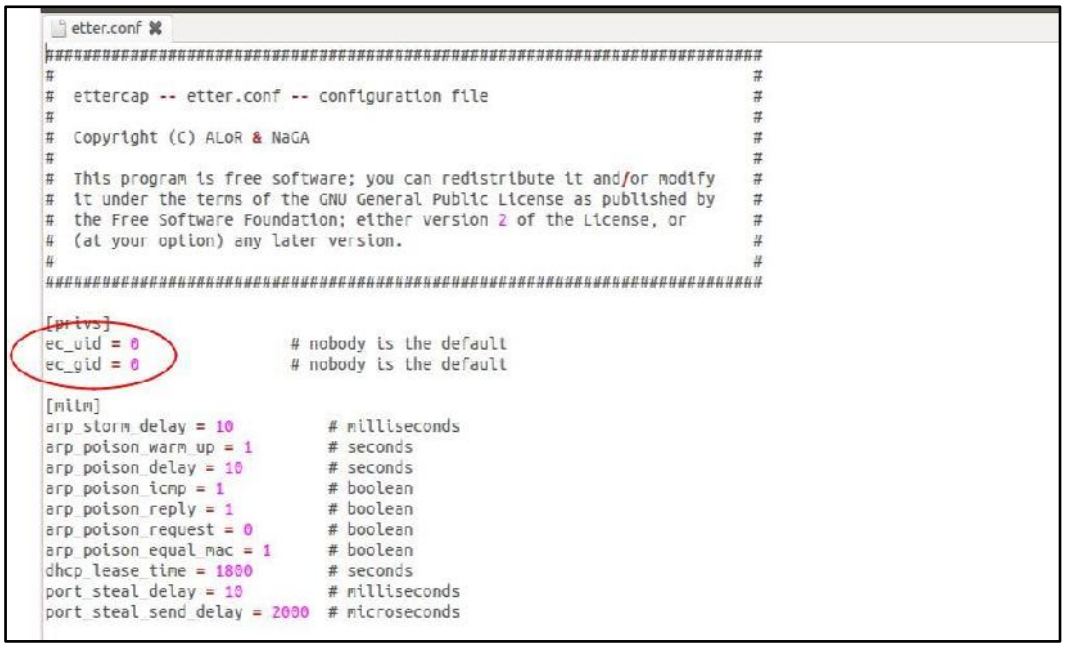
       # sudo apt-get install Ettercap-gtk

Gambar 3.2 Tampilan *software Ettercap* pada *Ubuntu* 18.04.

c. Langkah berikutnya setting file *etter.conf* dengan perintah :

 # nano /etc/ettercap/etter.conf

d. Kemudian ubah isi dari file *etter.conf* untuk mengkonfigurasi *software Ettercap* agar dapat berjalan dengan baik pada koneksi aman *ssl*.



Gambar 3.3 Tampilan konfigurasi file *etter.conf.*

Gambar 3.3 di atas merupakan konfigurasi *Ettercap* yang bertujuan agar dapat menjalankan tugas sebagai software penyerang dengan bersih atau tidak diketahui user lain, dengan mengubah pada bagian privs menjadi 0.

 # if you see iptables

Redir_command_on = "iptables-t nat-A PREROUTING –I %iface –p tcp --dport %port –j REDIRECT –to-port %rport"

Redir_command_on = "iptables-t nat-D PREROUTING –I %iface –p tcp --dport %port –j REDIRECT –to-port %rport"

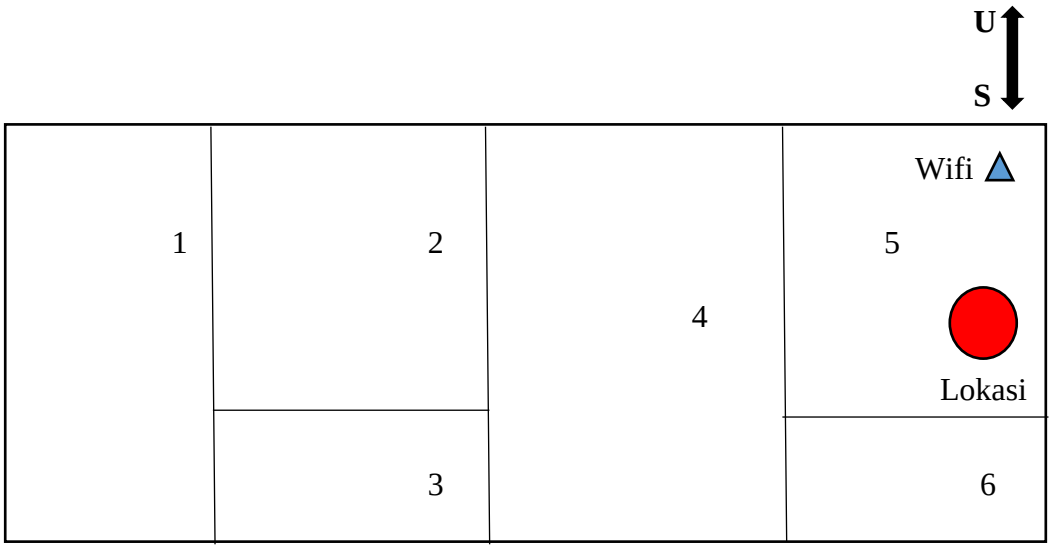
Perintah di atas merupakan konfigurasi *Ettercap* yang bertujuan untuk menjalankan penyerangan agar dapat berjalan dengan baik pada koneksi jaringan aman *ssl* dan *https* maka penulis harus memastikan bahwa *script redir_command_on* pada *etter.conf* aktif.

3.3.2 Teknis Pengujian Kemanan

Pengujian kemanan bertujuan untuk memperoleh kesadaran akan permasalahan kemanan pada jaringan kabel dan nirkabel (*wireless LAN*).

a. Penulis mengidentifikasi keberadaan dan kemanan yang digunakan *wifi* target.
b. Setelah mengetahui keberadaan dan keamanan yang digunakan *wifi* target, penulis masuk untuk mendapatkan koneksi dengan *wifi* target.
c. Langkah pengujian keamanan, setelah mendapatkan koneksi dengan *wifi* target, penulis mencoba melakukan serangan *packet sniffing* terhadap *wifi* dan jaringan kabel dengan menggunakan *software Ettercap*, serangan akan berhasil jika transfer data tidak dilindungi oleh keamanan seperti *SSL*, *IPSec, WEP, WPA,* dan *WPA2*. Karena data yang didapat terenkripsi.

3.3.3 Posisi tempat penyerangan



Gambar 3.4 Posisi tempat/ lokasi penyerangan

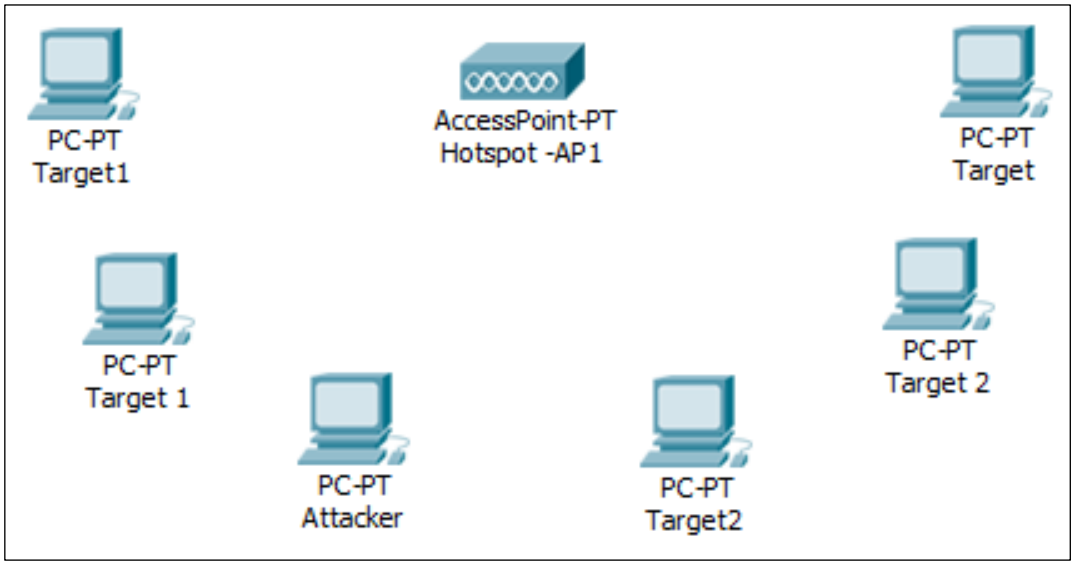
Gambar 3.4 adalah denah lokasi dimana penulis melakukan penelitian pada gedung telekomunikasi dan navigasi di PT. (PERSERO) Angkasa Pura II Bandar Udara Internasional Kualanamu Medan, angka-angka yang tertulis diatas merupakan perwakilan dari beberapa ruangan, berikut penjelasannya :

a. Ruang 1 adalah server.
b. Ruang 2 adalah ruang karyawan elektronika dan listrik.
c. Ruang 3 adalah ruang asisten manager elektronika dan listrik.
d. Ruang 4 adalah ruang server.
e. Ruang 5 adalah ruang monitoring jaringan komputer yang penulis gunakan sebagai tempat penelitian.
f. Ruang 6 adalah gedung.

3.4 Rancangan Penelitian

3.4.1 *Layout* Jaringan Komputer

Layout jaringan adalah tata letak komponen halaman yang digunakan dalam jaringan. Adapun gambar *layout* jaringan dapat dilihat sebagai berikut :



Gambar 3.5 *Layout* Jaringan

Gambar diatas merupakan gambar dari *layout* jaringan saat penyerangan. Dimana pengaturan *IP address* pada PC-PT Target yaitu 192.168.0.4, kemudian pengaturan *IP address* pada PC-PT 192.168.0.2 Target 2, kemudian pengaturan *IP address* pada PC-PT Target 2 192.168.0.88, kemudian pengaturan *IP address* pada PC-PT Target 1 192.168.0.100/101, dan pengaturan *IP address* pada PC-PT Attacker adalah 192.168.0.132.

3.4.2 Manajemen Jaringan

Jaringan komputer pada PT. (Persero) Angkasa Pura II Bandar Udara Internasional Kualanamu Medan dimanfaatkan untuk beberapa hal, antara lain : Keuangan, Vicon, Internal Server, *LAN*, *Hotspot*, dan *CCTV*. Keenam bagian ini memiliki masing-masing *IP Pool* dan *Interface* yang berbeda-beda. Pada *LAN*, *IP address*nya adalah 192.168.0.1/24 dan menggunakan *interface ether* 6. Subnet/24 ini berarti bahwa pada *LAN* terdapat 254 alamat *IP* yang bisa digunakan dan 1 alamat untuk *broadcast*. Alamat *IP LAN* yang ada akan dipakai oleh komputer di PT. (Persero) Angkasa Pura II Bandar Udara Internasional Kualanamu Medan. Komputer mendapatkan alamat secara manual maupun secara otomatis (*DHCP*). Alamat *IP* yang telah dipakai akan diproses oleh *address resolution protocol* sehingga didapat *MAC address* dari komputer. Fungsi dari *address resolution protocol* adalah mengubah alamat *IP* menjadi *MAC address* sehingga mudah dalam transmisi data. Jika komputer berada diluar jaringan, maka *ARP* akan melacak *MAC address* dari router yang terkoneksi dengan komputer.

3.4.3 Keamanan Jaringan

Firewall adalah mekanisme perlindungan terhadap terhadap suatu jaringan komputer. Pada jaringan komputer PT. (Persero) Angkasa Pura II Bandar Udara Internasional Kualanamu Medan, metode *firewall* yang diberikan antara lain *jump*, *redirect*, dan *masquarde*. *Jump* berarti menempatkan suatu paket kekeadaan selanjutnya. Contohnya adalah pada

aksi 0 dan 1 paket data akan ditempatkan ke *dstnat* (*destination NAT*) dan *hotspot*. *Redirect* adalah mengalihkan paket ke *port* tujuan tertentu. Paket yang masuk akan dialihkan ke port 53(*DNS*), 80(*http*), 443(*https*), 3128(*proxy*), dan 8080(*http*). Pada *firewall* jaringan komputer PT. (Persero) Angkasa Pura II Bandar Udara Internasional Kualanamu Medan, terdapat mekanisme pengarahan pengguna *hotspot* yang mengharuskan pengguna untuk *login* sehingga dapat menggunakan internet yang disediakan PT. (Persero) Angkasa Pura II Bandar Udara Internasional Kualanamu Medan. Mekanisme tersebut dapat terlihat pada *chain hotspot, hs-unauth,* dan *hs-auth*.

Selain mekanisme pada *hotspot*, terdapat juga *firewall NAT* berupa *masquerade*. *NAT* (*Network Adress Translation*) berfungsi untuk menyamarkan alamat *IP* saat paket memasuki perangkat jaringan seperti *router*. *Masquerade* berfungsi untuk menyamarkan alamat *IP* yang sedang dipakai di PT. (Persero) Angkasa Pura II Bandar Udara Internasional Kualanamu Medan, yaitu alamat *IP* local, sehingga tidak diketahui pihak luar dan yang diketahui hanya alamat *IP* public yang digunakan jaringan komputer PT. (Persero) Angkasa Pura II Bandar Udara Internasional Kualanamu Medan. Terdapat 4 *NAT masquerade* dijaringan komputer PT. (Persero) Angkasa Pura II Bandar Udara Internasional Kualanamu Medan, yaitu *NAT* lokal angkasa pura, *NAT* admin data utama, *NAT CCTV* angkasa pura, dan *NAT hotspot network*. Sementara utuk keamanan jaringan hotspot sendiri PT. (Persero) Angkasa Pura II Bandar Udara

Internasional Kualanamu Medan digunakan untuk fasilitas publik tidak untuk dikomersilkan jadi tidak diberi pengaman seperti *WEP, WPA, WPA*2 dan lain-lain agar para pengguna jasa layanan penerbangan dapat dengan mudah dan cepat untuk terkoneksi dengan internet.

BAB IV
HASIL DAN PEMBAHASAN

4.1 Kebutuhan Spesifikasi Minimum *Hardware* dan *Software*

Dalam penelitian ini bahan penelitian berdasarkan dari teori dasar kemanan jaringan komputer yang diambil dari berbagai *literature* seperti buku, artikel berbentuk *softcopy* dan *hardcopy*. Untuk spesifikasi alat yang digunakan penelitian adalah sebagai berikut:

1. Kebutuhan perangkat keras dan sistem operasi.
    a. Laptop Compaq CQ40, Processor dual-core 2.10 Ghz, Memori 2GB.
    b. *LAN Card* 10/100BASE-T *Ethernet LAN*.
    c. *Wireless network card Broadcom* 802.11 b/g *WLAN*.
    d. Sistem operasi *linux Ubuntu* 18.04.
2. Kebutuhan perangkat lunak.
    a. *Software Ettercap 0.8.2* (untuk serangan *packet sniffing*).

4.2 Pengujian Aplikasi dan Pembahasan

4.2.1 *Packet sniffing* menggunakan *software Ettercap* pada *wifi* dan jaringan kabel.

Langkah-langkah yang dilakukan yaitu :

a. Langkah pertama penulis menghidupkan *software etercap* melalui terminal dengan perintah

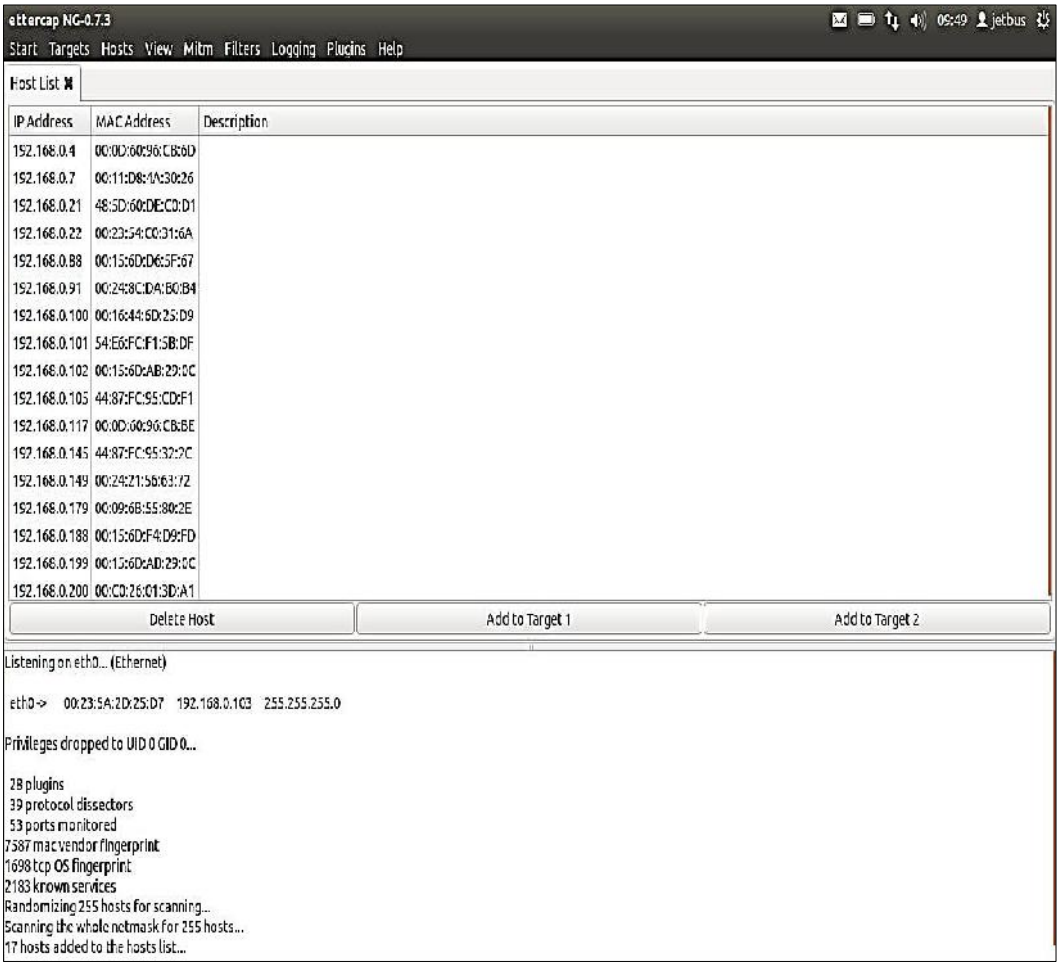
   # sudo Ettercap –gtk (tampilan dapat dilihat pada gambar 4.1.)

b. Kemudian langkah kedua klik pada *toolbar* menu *sniff* pilih *unified sniffing*, lalu pilih *device elo/wlo LAN card* agar dapat berjalan pada jaringan kabel.

Gambar 4.1 Tampilan langkah petama untuk *device elo.*

Gambar 4.1 adalah tampilan *software Ettercap* yang sudah berjalan/masuk pada jaringan *wifi*, terdapat beberapa informasi yaitu *IP*

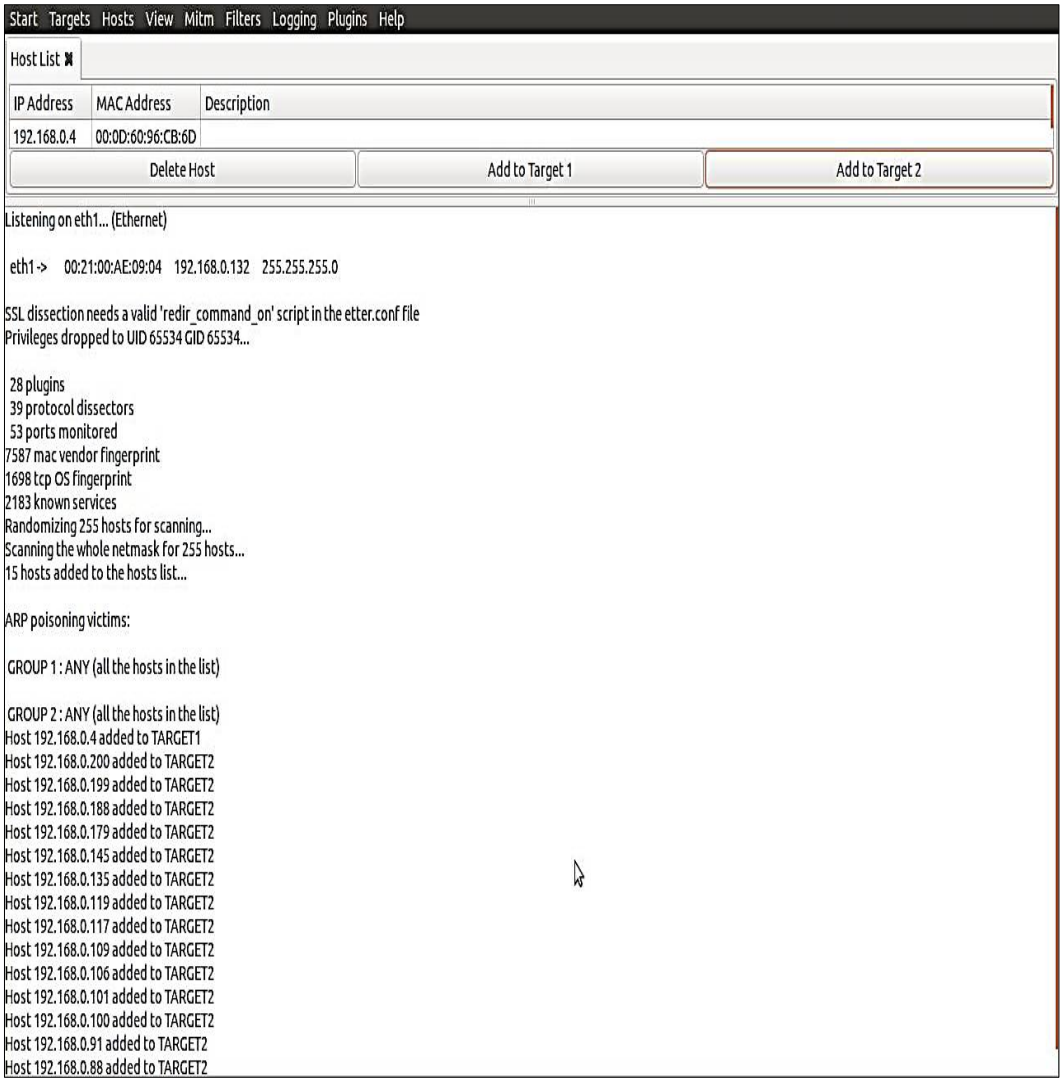
address penyerang yang terdaftar pada jaringan *wifi*, jika terjadi kesalahan konfogirasi juga akan ditampilkan seperti gambar diatas terdapat tulisan ”*SSL dissection needs a valid “redir_command_on”script in the etter.conf”*.



Gambar 4.2 Tampilan langkah pertama untuk *device wlo*.

Gambar 4.2 adalah tampilan *software Ettercap* yang sudah berjalan/masuk pada jaringan kabel *LAN*.

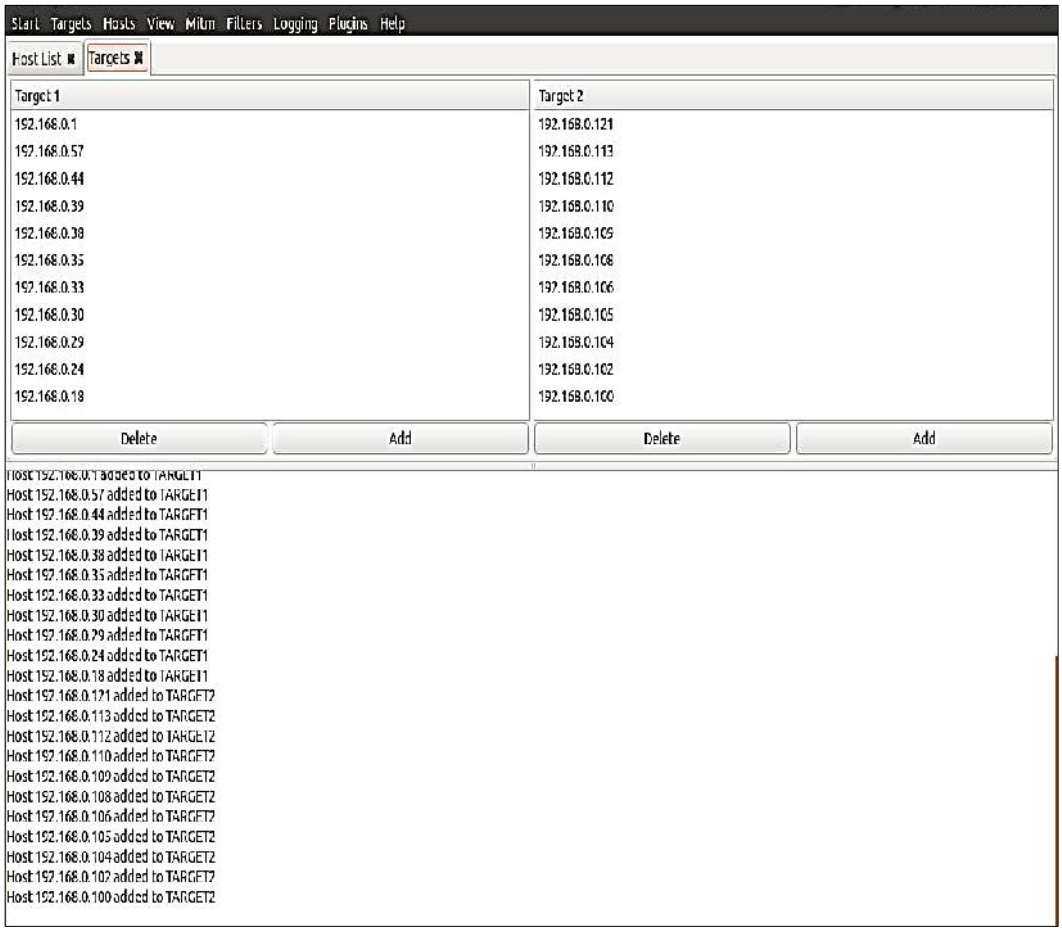
c. Langkah ketiga klik *host* untuk mencari *host* target pilih *scan host.*



Gambar 4.3 Tampilan langkah ketiga *scan host* target.

Gambar 4.3 adalah tampilan *software Ettercap* ketika melakukan *scan host*, didalamnya terdapat informasi *IP address host* yang tersambung pada jaringan *wifi* dan jaringan nirkabel.

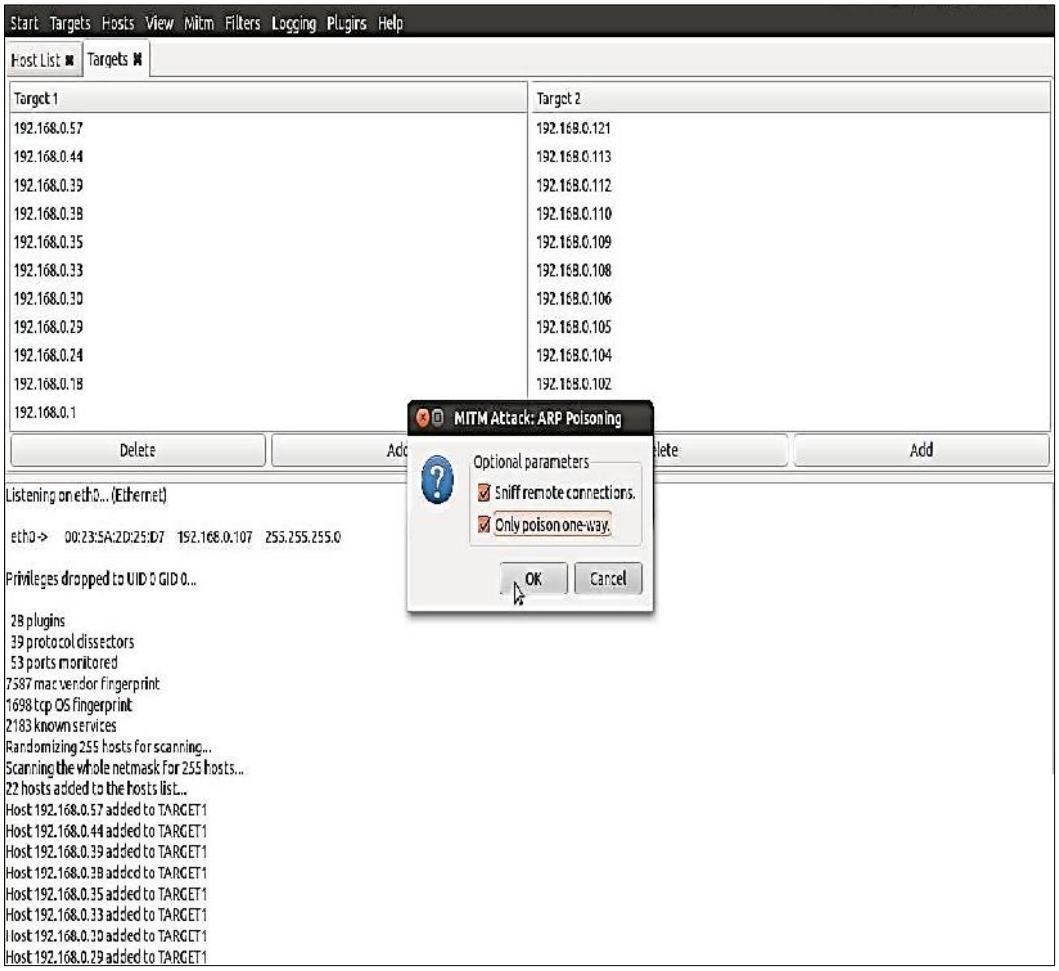
d. Langkah keempat pilih *host* target.



Gambar 4.4 Tampilan langkah keempat memilih *host* target.

Gambar 4.4 adalah langkah untuk memilih *host* yang akan dijadikan target penyerangan, terdapat dua klasifikasi target yaitu target 1 adalah target utama yang akan diserang, target 2 adalah target alternatife jika target 1 tidak mendapat hasil.

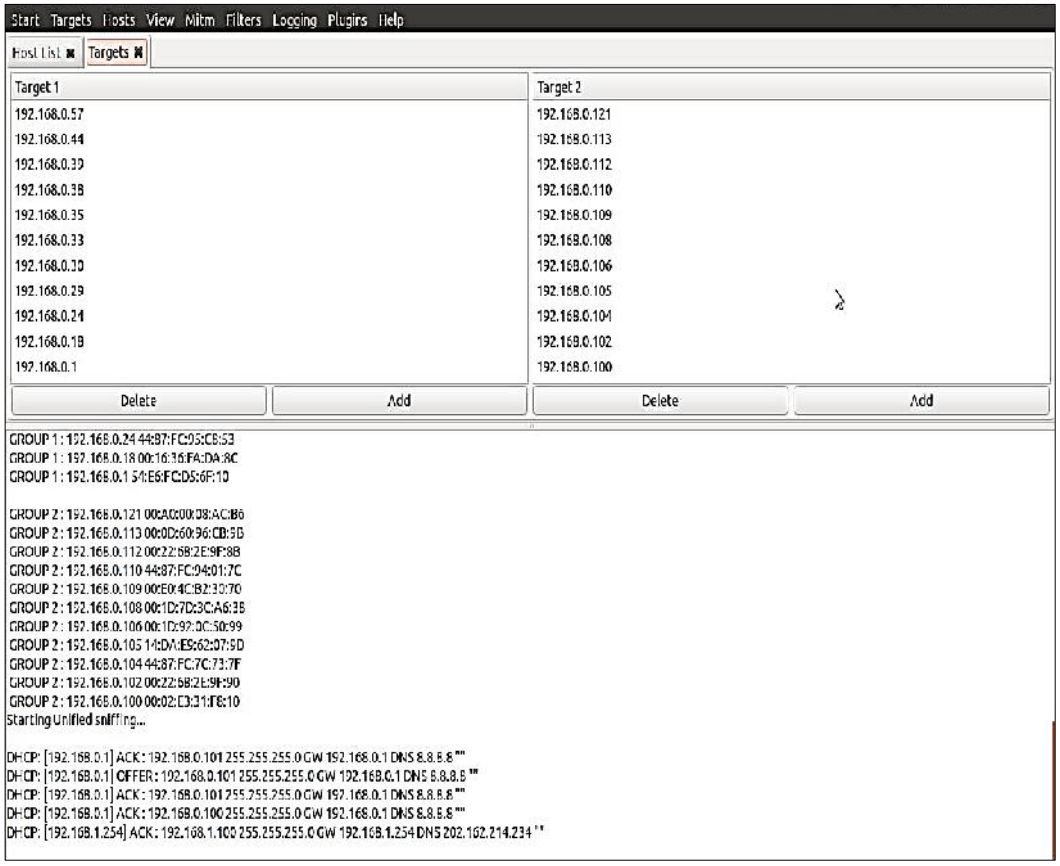
e. Melanjut ke langkah kelima klik *MITM Attack* untuk menyerang pilih *ARP poisoning* melakuka *ARP poisoning* ke *host* yang telah penulis daftarkan ke target 1 dan 2 tadi.



Gambar 4.5 Tampilan langkah kelima melakukan serangan *packet sniffing*.

Gambar 4.5 adalah tampilan langkah untuk melakukan serangan *packet sniffing* , penulis memilih *ARP poisoning* dan mencentang *sniff remote connections* dan *only poison one-way* agar dapat merekam user dan password akun email dan *dns* yang dituju oleh target.

f. Kemudian langkah keenam klik *start*, pilih *start sniffing*.



Gambar 4.6 Tampilan serangan *packet sniffing*.

Gambar 4.6 adalah contoh tampilan hasil serangan *packet sniffing* pada *software Ettercap* yang telah merekam host target yang mengakses *dns* dari google.

4.2.3 Analisis Hasil Penelitian

Analisis perlu dilakukan untuk mengetahui seberapa aman tingkat keamanan yang telah diterapkan dalam sebuah jaringan kabel maupun *wireless* (nirkabel). Seperti yang kita ketahui tingkat keamanan bukan hanya berasal dari hardware dan software yang sudah ada namun peran

penting dari manusia/pengguna yang melakukan konfigurasi dan dari perancangan jaringan itu sendiri.

Keamanan jaringan yang terinstal di lingkup PT. (Persero) Angkasa Pura II Bandar Udara Internasional Kualanamu Medan pada umumnya masih perlu peningkatan yang terbukti pada *wifi* tidak menggunakan keamanan atau *open* (terbuka). Disamping itu juga masih banyak pegawai yang masih awam dengan yang namanya keamanan jaringan komputer. Adapun kelebihan dan kekurangan dari sistem kemanan jaringan adalah sebagi berikut :

a. Kelebihan
    1. Kecepatan akses lebih tinggi karena penyedia fasilitas jaringan dan pengelolaannya dilakukan secara khusus oleh satu komputer (server) yang tidak dibebani tugas lain sebagai workstation.
    2. Sistem keamanan dan administrasi jaringan lebih baik, karena terdapat seseorang pemakai yang bertugas sebagai administrator jaringan, yang mengelola administrasi dan sistem keamanan jaringan.
    3. Sistem *backup* data lebih baik, karena pada jaringan *client-server backup* dilakukan terpusat di server, yang akan mem*backup* seluruh data yang digunakan di dalam jaringan.

b. Kelemahan

1. Biaya operasional relatif lebih mahal.
2. Diperlukan adanya satu komputer khusus yang berkemampuan lebih ditugaskan sebagai server.
3. Kelangsungan jaringan sangat tergantung pada server. Bila server mengalami gangguan maka secara keseluruhan jaringan akan terganggu.

4.2.4 Mengidentifikasi Wifi

Percobaan ini dilakukan untuk mengidentifikasi keberadaan *wifi* dalam bentuk informasi lengkap dengan nama *SSID*, *mac address*, *RSSI*, *vendor*, *channel* yang dipakai, *network type* dan *security* atau keamanan yang digunakan. Hal ini dilakukan untuk memudahkan penyerangan untuk mendapatkan koneksi dengan jaringan *wifi* yang ada. Dalam percobaan ini penulis mendapatkan *wifi* yang berada di area bandara tidak berpengaman/open.

Adapun topologi jaringan yang digunakan pada penelitian ini adalah topologi jaringan Infrastruktur.

Gambar 4.7 Topologi Infrastruktur

Gambar diatas adalah gambar topologi infrastruktur yang merupakan topologi pada jaringan *wifi*. Dimana komputer komputer maupun *mobile station* yang hendak berhubungan harus melewati *AP*. Jadi, setiap komputer maupun *mobile station* yang hendak berhubungan harus melewati *AP* terlebih dahulu. Baru kemudian dapat menggunakan sumber daya yang ada mpada jaringan.

Kemudian *attacker* melakukan penyerangan dengan mengelompok-kan target menjadi dua yaitu target 1 dan 2 yang dimana berfungsi ketika target 1 tidak melakukan aktifitas maka penyerangan akan berpindah pada target 2 begitu pula sebaliknya hingga *attacker* dapat merekam semua aktifitas yang berjalan.

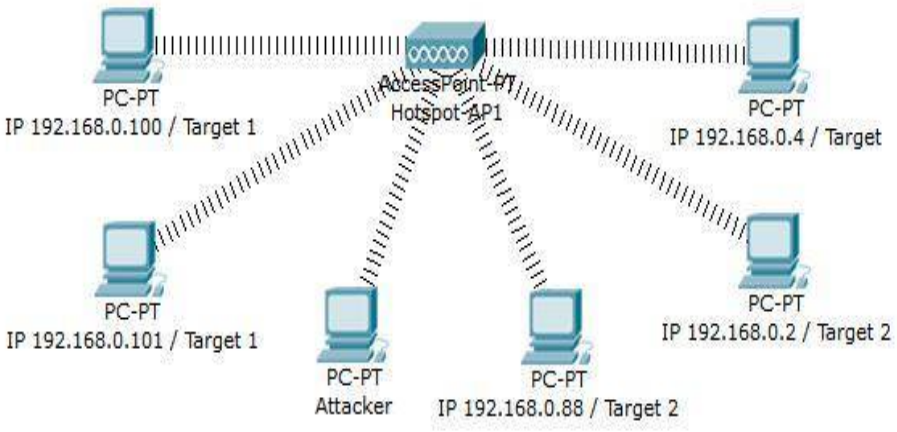
Dimana pengaturan *IP address* pada PC target1 yaitu 192.168.0.4 dan 192.168.0.2 kemudian pengaturan *IP address* pada PC target2 yaitu 192.168.0.88 dan 192.168.0.100/101 dan pengaturan *IP address* pada PC *attacker* yaitu 192.168.0.132.

Tabel 4.1 Target *attacker*

No.	Target Perangkat	Target IP Host	Mac Address	Situs
1.	PC HP	192.168.0.101	00:15:6D:AB:29:0C	accounts.google.com
2.	PC HP	192.168.0.88	00:16:44:6D:25:D9	accounts.google.com
3.	PC HP	192.168.0.88	00:16:44:6D:25:D9	mlogin.yahoo.com

4.2.5 Packet Sniffing

Percobaan ini dilakukan untuk mendapatkan informasi penting mengenai *account username, password,* akses *DNS* yang dituju dan informasi lain. Hal ini dimaksudkan agar penyerang dapat melakukan pengaksesan internet secara tidak sah demi keuntungan pribadi yang dapat mengakibatkan kerugian pada pengguna yang berada dalam jaringan. Pada percobaan ini, berhasil diperoleh informasi mengenai akses *DNS* yang dituju dan penulis juga mendapatkan *username* dan *password email* dari salah satu target. Dengan demikian, penulis dapat menyatakan tidak aman karena semua kegiatan dapat dengan mudah terekam dan mudah dicari.



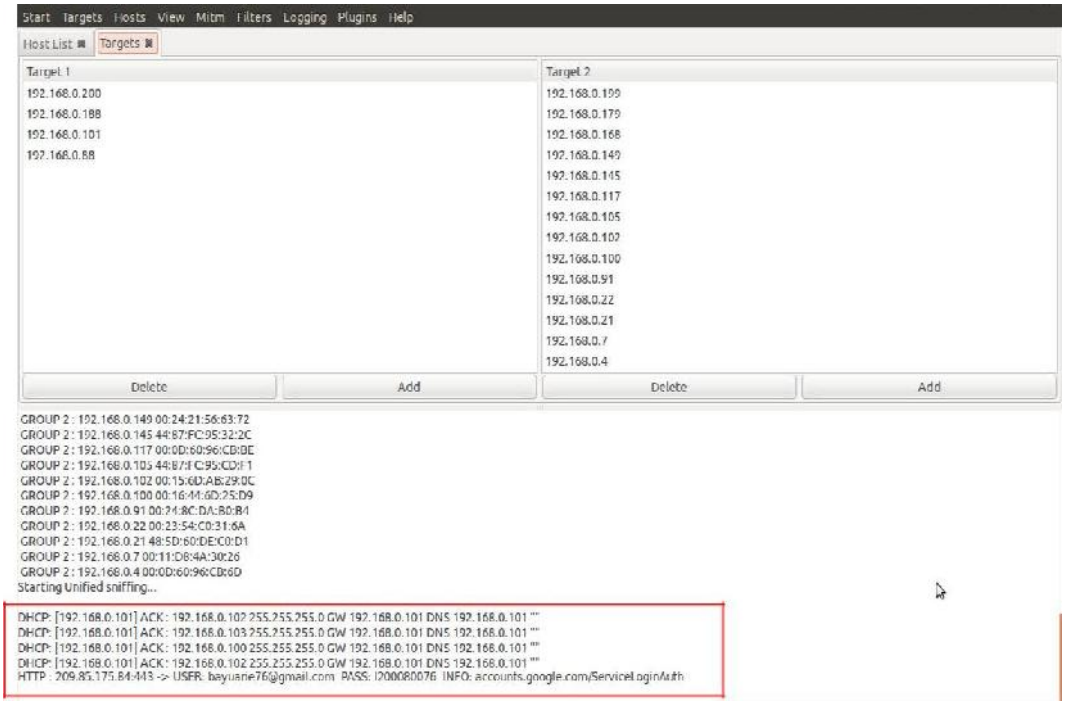
Gambar 4.8 Tampilan Simulasi Penyerangan

Gambar diatas adalah gambaran skenario dimana attacker melakukan penyerangan dengan mengelompokkan target menjadi dua kelompok yaitu target 1 dan target 2 yang dimana berfungsi ketika target utama atau target 1 tidak melakukan aktifitas maka penyerangan akan berpindah pada target 2 begitu pula sebaliknya hingga *attacker* dapat merekam semua aktifitas yang berjalan.

Karena dalam penelitian selama beberapa kali dalam jam kerja penulis tidak menemukan aktifitas yang mengakses akun dan *password*, penulis melakukan dua scenario yaitu :

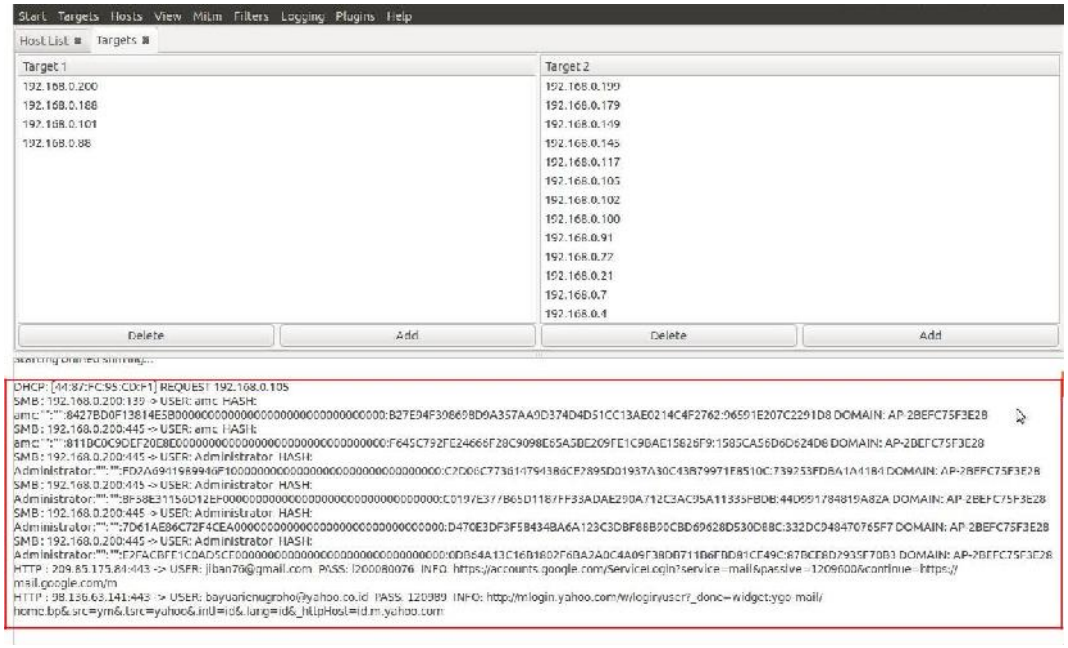
1. Skenario pertama dengan langkah sebagai berikut :
    a. Penulis membuat beberapa akun dan *password* baru.
    b. Akun dicoba *login* menggunakan komputer kantor.

c. Penulis merekam aktifitas yang terjadi menggunakan *software Ettercap*.



Gambar 4.9 Hasil penyerangan *packet sniffing* pada *wifi*

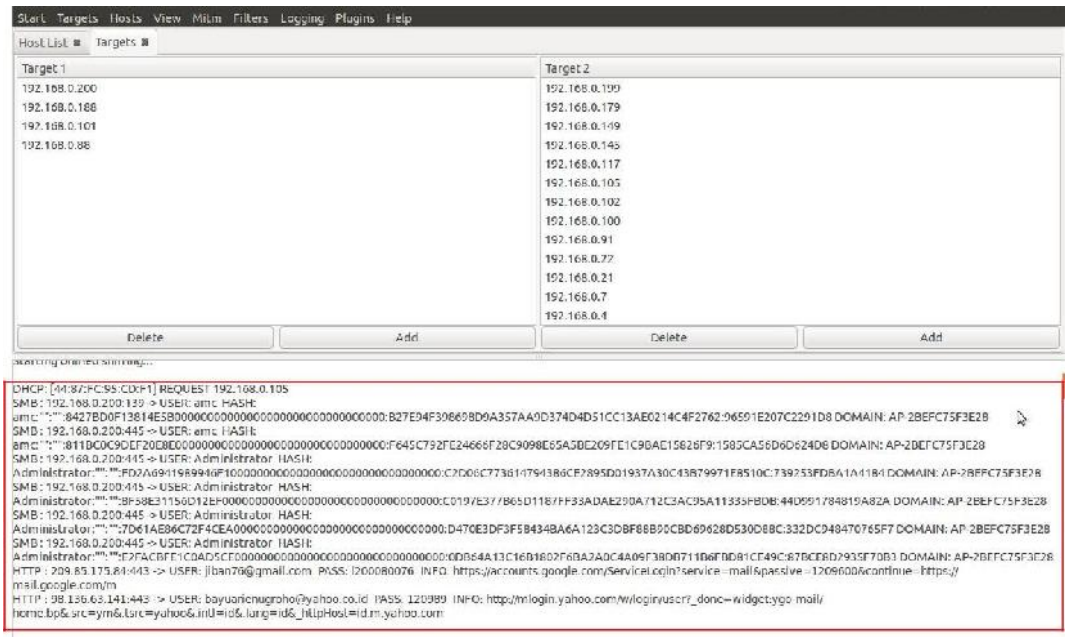
Gambar diatas menerangkan bahwa software dapat merekam beberapa aktifitas yang diberi tanda persegi panjang merah, yaitu pada baris 1 s/d 4 sedang terjadi komunikasi pesan antar komputer dengan komputer dalam satu jaringan untuk memastikan bahwa masih terhubung dalam satu jaringan namun tidak terkait oleh pengguna komputer yang artinya pengguna tidak melakukan komunikasi namun secara otomatis mesin komputer mengirim sendiri pesan tersebut yang disebut *ACK* (*Acknowledgement*). Kemudian pada baris terakhir menerangkan bahwa ada salah satu komputer *client* mengakses akun google *mail* terekam dengan *username bayuarie76@gmail.com* dan *password*-nya *1200080076*



Gambar 4.10 Hasil penyerangan *packet sniffing* pada jaringan kabel dikantor

Gambar diatas dapat menerangkan bahwa pada baris 1 s/d 13 dalam persegi panjang merah sedang terjadi *file sharing* antar *server* dan *client* namun pesan yang terekam terenkripsi sehingga penulis tidak dapat mendeskripsikannya. Sedangkan pada baris 14 s/d 17 terdapat dua komputer *client* yang sedang melakukan *login* akun google *mail* dengan *username* "jiban76@gmail.com dan *password*-nya 120989".

2. Skenario kedua penulis mengganti *password* dan mengacak beberapa akun dan *password* baru



Gambar 4.11 Hasil penyerangan *packet sniffing* pada jaringan kabel di gedung baru

Gambar diatas menerangkan bahwa akun yang diganti *password*-nya dan beberapa akun dan *password* yang diacak dapat direkam.

Dari analisis hasil yang didapat penulis mendapatkan pembahasan pihak pengelola jaringan komputer PT. (Persero) Angkasa Pura II Bandar Udara Internasional Kualanamu medan dan mendapatkan beberapa alasan mengapa *wifi* pada kantor TelNav dan terminal bandara tidak diberi keamanan atau diopen, berikut alasannya :

1. *Wifi* yang terinstal di terminal bandara merupakan fasilitas bagi pengunjung atau pengguna layanan penerbangan, selagi menunggu jadwal penerbangan atau penjemputan dapat mengakses internet secara mudah dan gratis.

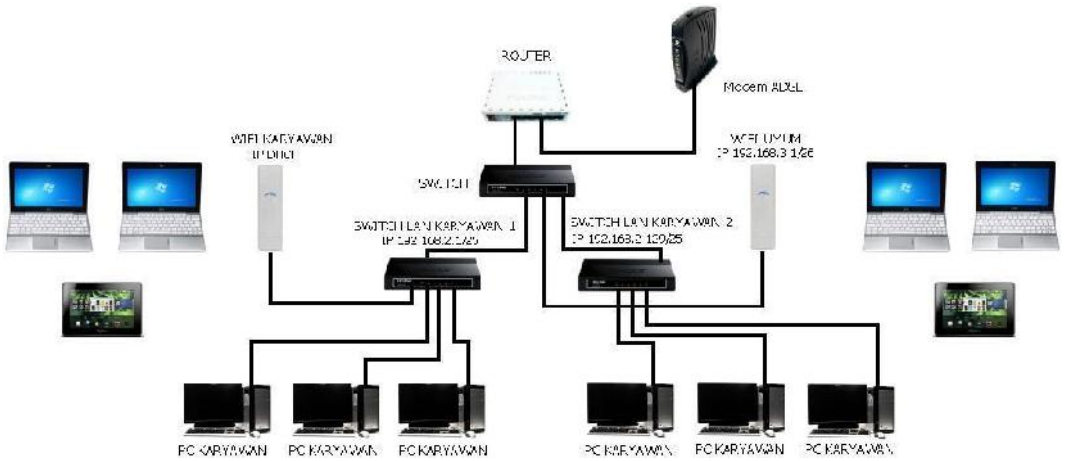
2. *Wifi* yang terinstal di kantor TelNav merupakan *wifi* utama, ketika suatu saat akan menambahkan *wifi* lagi tidak sulit untuk mengkonfigurasinya.

Inti dari kedua pembahasan tersebut diatas adalah *wifi* yang terinstal pada PT. (Persero) Angkasa Pura II Bandar Udara Internasional Kualanamu Medan digunakan untuk fasilitas publik tidak untuk dikomersilkan jadi tidak diberi pengaman seperti *WEP, WPA, WPA*2 dan lain-lain agar para pengguna jasa layanan penerbangan dapat dengan mudah dan cepat untuk terkoneksi dengan internet.

4.2.6 Solusi Untuk Mencegah Serangan Packet Sniffing

Setelah melakukan penelitian penulis telah menyiapkan beberapa rekomendasi solusi untuk meningkatkan keamanan jaringan dari suatu serangan seperti yang dilakukan penulis untuk menganalisis keamanan jaringan yang dapat diterapkan oleh pihak PT. (Persero) Angkasa Pura II Bandar Udara Internasional Kualanamu Medan, seperti :

1. Bedakan jaringan antara jaringan *wifi/LAN* kantor, misal dengan *IP* 192.168.2.1/25 untuk 128 *host* untuk *switch LAN* karyawan1, *IP* 192.168.2.129/25 untuk 128 *host* untuk *switch LAN* karyawan2, dan untuk *wifi* umum dengan *IP* 192.168.3.1/26 untuk 64 *host*.



Gambar 4.12 Perbedaan jaringan internet untuk kantor dan umum.

Gambar diatas menjelaskan bahwa dengan membedakan *IP* jaringan, serangan *packet sniffing* tidak dapat masuk kedalam jaringan yang lain untuk menyadap lalu lintas data yang berjalan, karena secara sistem *packet sniffing* berjalan pada *layer* 2.

2. Binding *IP* dan *MAC Adress*

   Salah satu metode yang dapat digunakan untuk mengatasi *ARP spoofing* pada jaringan adalah dengan binding *IP* dan *MAC Adress*nya sehingga *gateway* tidak akan salah mengirimkan paket kepada user. Dengan menggunakan metode ini, maka *ARP spoofing* dapat ditangkal.

3. Gunakan keamanan *enkripsi WPA2-PSK* dan radius dalam area ruangan untuk mengamankan jaringan *wifi* kantor agar sinyal tidak terlampu jauh dan hanya karyawan yang mengetahui.

4.2.7 Solusi Alternative Untuk Mencegah Serangan Packet Sniffing Bagi Pengguna Linux (Sebagai Client dan Server)

Sebenarnya dapat dengan mudah mencegah *ARP spoofing* dengan cara merubah *ARP table* dari *dynamic* menjadi *static.* Namun tidak cukup hanya membuat *static ARP table* antara *MAC address* dan *IP* saja, karena teknik membuat *static ARP table* hanya dapat mencegah scenario seperti *ARP spoofing*. Jika *attacker* melakukan *spoofing* pada *gateway*, tentu saja antara *ARP table client* dan *ARP table gateway* harus dibuat *static* juga, dengan bantuan *ARPOn* ini kita dapat mencegah *attacker* melakukan *spoofing* menggunakan mode tersebut.

Proses instalasi *ARPOn* :

1. Masuk ke terminal dan jalankan *command* berikut :

   $ sudo apt-get install arpon

Konfigurasi *ARPOn* :

1. Sebelum diaktifkan, *ARPOn* harus dikonfigurasi dulu. File konfigurasi *ARPO nada* di/etc/default/arpon. Edit menggunakan *teks editor* anda :

   $ sudo nano/etc/default/arpon
2. Jika menggunakan *IP static*, maka hilangkan tanda pagar pada baris berikut :

   DAEMON_OPTS=”-d-f/var/log/arpon/arpon.log-g-s”

3. Jika menggunakan *IP dynamic* (*DHCP*), maka hilangkanlah tanda pagar pada baris berikut :

   DAEMON-OPTS=”-d-f/var/log/arpon/arpon.log-g-y”

4. Lalu ubah *no* menjadi *yes* pada bagian *RUN* :

   RUN=”yes”

5. Save file tersebut dengan cara tekan *CTRL+O* dan untuk *exit* tekan *CTRL+X*.

6. Silahkan *restart service ARPOn* :

   $ sudo etc/init.d/arpon restart

7. Untuk menjalankan *ARPOn* bisa dengan perintah berikut :

   $ sudo arpon -y

BAB V
PENUTUP

5.1. Simpulan

Berdasarkan dari analisis data dan percobaan serangan yang dilakukan, maka dapat diambil kesimpulan, bahwa sistem keamanan jaringan *LAN* yang mencakup jaringan kabel dan nirkabel pada PT. (PERSERO) Angkasa Pura II Bandar Udara Internasional Kualanamu Medan masih perlu peningkatan, hal ini dibuktikan dengan :

1. Penyerangan *packet sniffing* yang dapat merekam dan menampilkan *username* dan *password* dengan menggunakan aplikasi e*ttercap*.

5.2. Saran

Berdasarkan uraian dari kesimpulan, maka kelebihan dan kekurangan diatas dapat menjadi pelajaran serta refrensi untuk kedepannya. Saran-saran yang dapat dipertimbangkan untuk kedepan antara lain :

1. Diperlukan pembagian jaringan untuk membedakan jaringan untuk umum dan jaringan untuk karyawan agar tidak terjadi serangan yang dilakukan melalui jaringan wifi umum oleh pihak tidak bertanggung jawab untuk mendapatkan informasi penting yang berlalu lintas dalam jaringan komputer karyawan.
2. Diperlukannya keamanan WPA2-PSK sebagai keamanan awal untuk *wifi* untuk dapat meminimalisir sebelum terjadinya serangan *packet sniffing*.

3. Sebaiknya dilakukan penggantian *password* secara berkala untuk *login system* untuk menghindari terjadinya penyusupan oleh pihak-pihak yang tidak bertanggung jawab.
4. Pengecekan jaringan secara berkala diperlukan untuk menghidari terjadinya permasalahan/*error* pada jaringan yang dapat menyebabkan kinerja jaringan menjadi lambat.

DAFTAR PUSTAKA

Gollmann, Dieter. (1999). *Computer Security Jhon Willey & Son Inc*. Canada.

Howard, John D. (1997). *An Analysis of Security incidents on the internet.* Software Engineering Institute.

Icove, David. (1997). *An Analysis Of Security Incidents On The Internet 1989-1995*. PhD Thesis, Engineering and Public Policy. Carnegie Mellon University.

Kadir, Abdul. (2014). *Pengantar Sistem Informasi Bisnis*. P.T.ELEX Media Komputindo. Jakarta.

Noviyanto, Hendri. (2011). *Analisis Keamanan Wireless di Universitas Muhammadiyah Surakarta*. Surakarta : Tugas Akhir Universitas Muhammadiyah Surakarta.

Perwitasari, I. D. (2018). Teknik Marker Based Tracking Augmented Reality untuk Visualisasi Anatomi Organ Tubuh Manusia Berbasis Android. INTECOMS: Journal of Information Technology and Computer Science, 1(1), 8-18.

Puspita, Khairani, and Purwa Hasan Putra. "Penerapan Metode Simple Additive Weighting (SAW) Dalam Menentukan Pendirian Lokasi Gramedia Di Sumatera Utara." Seminar Nasional Teknologi Informasi Dan Multimedia, ISSN. 2015.

Putera, A., Siahaan, U., & Rahim, R. (2016). Dynamic key matrix of hill cipher using genetic algorithm. Int. J. Secur. Its Appl, 10(8), 173-180.

Putra, Randi Rian, and Cendra Wadisman. "Implementasi Data Mining Pemilihan Pelanggan Potensial Menggunakan Algoritma K Means." INTECOMS: Journal of Information Technology and Computer Science 1.1 (2018): 72-77.

Putri, R. E., & Siahaan, A. (2017). Examination of document similarity using Rabin-Karp algorithm. International Journal of Recent Trends in Engineering & Research, 3(8), 196-201.

Rahim, R. (2018, October). A Novelty Once Methode Power System Policies Based On SCS (Solar Cell System). In International Conference of ASEAN Prespective and Policy (ICAP) (Vol. 1, No. 1, pp. 195-198).

Rizal, Chairul. "Pengaruh Varietas dan Pupuk Petroganik Terhadap Pertumbuhan, Produksi dan Viabilitas Benih Jagung (Zea mays L.)." ETD Unsyiah (2013).

Ruwaida, D., & Kurnia, D. (2018). Rancang Bangun File Transfer Protocol (FTP) dengan Pengamanan Open SSL pada Jaringan VPN Mikrotik di SMK Dwiwarna. CESS (Journal of Computer Engineering, System and Science), 3(1), 45-49.kbar, A. (2018). Pembangunan Model Electronic Government Pemerintahan Desa Menuju Smart Desa. Jurnal Teknik dan Informatika, 5(1), 1-5.

Ri2M. (2010). *Network and Security*. (*http://ftp.labkom.bl.ac.id/*)

Setiawan, Thomas. (2004). *Analisis Keamanan Jaringan Internet Menggunakan Hping, Nmap, Nessus, dab Ethereal*. Bandung : Tugas Akhir Institut Teknologi Bandung. (http://budi.insan.co.id/courses/ec5010/projects/thomas-report.pdf)

Supriyanto, Aji. (2006). *Analisis Kelemahan Keamanan Pada Jaringan Wireless*. Semarang : Tugas Akhir Universitas Stikubank Semarang. (http://www.unisbank.ac.id/ojs/index.php/fti1/article/download/33/28)

Sari, R. D., Supiyandi, A. P. U., Siahaan, M. M., & Ginting, R. B. (2017). A Review of IP and MAC Address Filtering in Wireless Network Security. Int. J. Sci. Res. Sci. Technol, 3(6), 470-473.

Sarif, M. I. (2017). Penemuan Aturan yang Berkaitan dengan Pola dalam Deret Berkala (Time Series).

Siahaan, MD Lesmana, Melva Sari Panjaitan, and Andysah Putera Utama Siahaan. "MikroTik bandwidth management to gain the users prosperity prevalent." Int. J. Eng. Trends Technol 42.5 (2016): 218-222.

Sidik, A. P. (2018). Algoritma RSA dan Elgamal sebagai Algoritma Tambahan untuk Mengatasi Kelemahan Algoritma One Time Pad pada Skema Three Pass Protocol.

Sitorus, Z. (2018). Kebutuhan Web Service untuk Sinkronisasi Data Antar Sistem Informasi dalam Universitas. Jurnal Teknik dan Informatika, 5(2), 87-90.

Sumartono, I., Siahaan, A. P. U., & Mayasari, N. (2016). An overview of the RC4 algorithm. IOSR J. Comput. Eng, 18(6), 67-73.

Supiyandi, S., Hermansyah, H., & Sembiring, K. A. (2020). Implementasi dan Penggunaan Algoritma Base64 dalam Pengamanan File Video. JURNAL MEDIA INFORMATIKA BUDIDARMA, 4(2), 340-346.

Yudianto, M Jafar Noor. (2013). *Jaringan Komputer dan Pengertiannya*. (*http://ilmukomputer.org*)