Analisis Keamanan Jaringan *Wireless Local Area Network* dengan Metode *Extended Access List*

Artikel Ilmiah

Peneliti :
Gilvan Januar Sirait(672014238)
Indrastanti R. Widiasari, M.T.

Program Studi Teknik Informatika
Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Salatiga
2018

Lembar Persetujuan

Analisis Keamanan Jaringan Wireless Local Area Network dengan menggunakan metode Extended Access List

Oleh,

GILVAN JANUAR SIRAIT
672014238

ARTIKEL ILMIAH

Diajukan Kepada Program Studi Teknik Informatika Guna Memenuhi Sebagian Dari Persyaratan Untuk Mencapai Gelar Sarjana S.Kom

Disetujui oleh,

Dr. Indrastanti R. Widiasari, MT.
Pembimbing 1

Diketahui oleh,

Wiwin Sulistyo, ST., M.Kom.
Dekan

Magdalena A. Ineke Pakereng, M.Kom.
Ketua Program Studi

FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN SATYA WACANA
SALATIGA
2018

Lembar Pengesahan

Judul Tugas Akhir	: Analisis Keamanan Jaringan Wireless Local Area Network dengan menggunakan metode Extended Access List
Nama Mahasiswa	: GILVAN JANUAR SIRAIT
NIM	: 672014238
Program Studi	: Teknik Informatika
Fakultas	: Teknologi Informasi

Menyetujui,

Dr. Indrastanti R. Widiasari, MT.
Pembimbing 1

Mengesahkan,

Wiwin Sulistyo, ST., M.Kom.
Dekan

Magdalena A. Ineke Pakereng, M.Kom.
Ketua Program Studi

Dinyatakan Lulus Tanggal: 28 NOVEMBER 2018

Reviewer :

- Dian W. Chandra, S.Kom., M.Cs.

PERPUSTAKAAN UNIVERSITAS
UNIVERSITAS KRISTEN SATYA WACANA
Jl. Diponegoro 52 – 60 Salatiga 50711
Jawa Tengah, Indonesia
Telp. 0298 – 321212, Fax. 0298 321433
Email: library@adm.uksw.edu ; http://library.uksw.edu

PERNYATAAN PERSETUJUAN AKSES

Saya yang bertanda tangan di bawah ini:

Nama	: Gilvan Januar Sirait		
NIM	: 672014238	Email	: gilvanjanuarsirait7@gmail.com
Fakultas	: Teknologi Informasi	Program Studi	: Teknologi Informatika
Judul tugas akhir	: Analisis Keamanan Jaringan Wireless Local Area Network dengan Metode Extended Access List		

Dengan ini saya menyerahkan hak *non-eksklusif** kepada Perpustakaan Universitas – Universitas Kristen Satya Wacana untuk menyimpan, mengatur akses serta melakukan pengelolaan terhadap karya saya ini dengan mengacu pada ketentuan akses tugas akhir elektronik sebagai berikut (beri tanda pada kotak yang sesuai):

☑ a. Saya mengijinkan karya tersebut diunggah ke dalam aplikasi Repositori Perpustakaan Universitas, dan/atau portal GARUDA

☐ b. Saya tidak mengijinkan karya tersebut diunggah ke dalam aplikasi Repositori Perpustakaan Universitas, dan/atau portal GARUDA**

* *Hak yang tidak terbatas hanya bagi satu pihak saja. Pengajar, peneliti, dan mahasiswa yang menyerahkan hak non-ekslusif kepada Repositori Perpustakaan Universitas saat mengumpulkan hasil karya mereka masih memiliki hak copyright atas karya tersebut.*

** *Hanya akan menampilkan halaman judul dan abstrak. Pilihan ini harus dilampiri dengan penjelasan/ alasan tertulis dari pembimbing TA dan diketahui oleh pimpinan fakultas (dekan/kaprodi).*

Demikian pernyataan ini saya buat dengan sebenarnya.

Salatiga, 10 JANUARI 2019

GILVAN JANUAR SIRAIT
Tanda tangan & nama terang mahasiswa

Mengetahui,

Indrastanti R.W.
Tanda tangan & nama terang pembimbing I

Tanda tangan & nama terang pembimbing II

PERPUSTAKAAN UNIVERSITAS
UNIVERSITAS KRISTEN SATYA WACANA
Jl. Diponegoro 52 – 60 Salatiga 50711
Jawa Tengah, Indonesia
Telp. 0298 – 321212, Fax. 0298 321433
Email: library@adm.uksw.edu ; http://library.uksw.edu

PERNYATAAN TIDAK PLAGIAT

Saya yang bertanda tangan di bawah ini:

Nama	:	Gilvan Januar Sirait		
NIM	:	672014238	Email	: gilvanjanuarsirait7@gmail.com
Fakultas	:	Teknologi Informasi	Program Studi	: Teknologi Informatika
Judul tugas akhir	:	Analisis Keamanan Jaringan Wireless Local Area Network dengan Metode Extended Access List		
Pembimbing	:	1. Indrastanti R. W.		

Dengan ini menyatakan bahwa:

1. Hasil karya yang saya serahkan ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar kesarjanaan baik di Universitas Kristen Satya Wacana maupun di institusi pendidikan lainnya.
2. Hasil karya saya ini bukan saduran/terjemahan melainkan merupakan gagasan, rumusan, dan hasil pelaksanaan penelitian/implementasi saya sendiri, tanpa bantuan pihak lain, kecuali arahan pembimbing akademik dan narasumber penelitian.
3. Hasil karya saya ini merupakan hasil revisi terakhir setelah diujikan yang telah diketahui dan disetujui oleh pembimbing.
4. Dalam karya saya ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali yang digunakan sebagai acuan dalam naskah dengan menyebutkan nama pengarang dan dicantumkan dalam daftar pustaka.

Pernyataan ini saya buat dengan sesungguhnya. Apabila di kemudian hari terbukti ada penyimpangan dan ketidakbenaran dalam pernyataan ini maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya saya ini, serta sanksi lain yang sesuai dengan ketentuan yang berlaku di Universitas Kristen Satya Wacana.

Salatiga, 19 JANUARI 2019

GILVAN JANUAR SIRAIT

Tanda tangan & nama terang mahasiswa

FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN SATYA WACANA
Jalan Diponegoro 52 – 60
Phone. (0298) 321212 (Hunting)
Fax. (0298) 321433
E-mail: fti@uksw.edu
Salatiga 50711 – INDONESIA

LEMBAR PERSETUJUAN PUBLISH JURNAL

Dengan mempertimbangkan isi dari jurnal mahasiswa :

Nama Mahasiswa : Gilvan Janvar Grait
NIM : 672014238

Maka jurnal ini dinyatakan :

LAYAK TERBIT / ~~TIDAK LAYAK TERBIT~~

Menyetujui,

Indrastanti R.W.

Pembimbing 1

Pembimbing 2

Mengetahui,

Dian W. Chandra

Reviewer

Analisis Keamanan Jaringan *Wireless Local Area Network* dengan Metode *Extended Access List*

[1)]Gilvan Januar Sirait, [2)]Indrastanti R. Widiasari

Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Jl. Dr. O. Notohamidjojo, Salatiga 50714, Indonesia
Email : [1)]672014238@student.uksw.edu, [2)] indrastanti@uksw.edu

Abstract

The level of use of wireless networking in everyday life are increasingly high. This is because the wireless network is highly modular and flexible making it easy to use. But, the wireless network also has its disadvantages, namely utilizing a high frequency to deliver a communication so that the vulnerability to security is also higher. Tapping on the lines of communication (man-in-the-middle attack) can be done more easily because it does not need to find wiring for intercourse. One way of securing a wireless network is to use the method of Extended Access List. Extended Access List can manage access rights for each host, control whether these packages are skipped or stopped, and can guarantee security for each computer. On the research done in real wireless network creation by using the network device such as a cisco router, wireless Access Point, a laptop computer as well as a striker as a client. In addition, the experiment carried out attacks against wireless networking on protocol tcp and icmp using tools of times linux, wireshark, and websploit. The result is a method used to successfully secure the tcp protocol, whereas the icmp protocol was not successful.

Keywords: Security, Wireless Networking, Exteded Access List

Abstrak

Tingkat penggunaan jaringan *wireless* pada kehidupan sehari-hari semakin tinggi. Hal ini disebabkan karena Jaringan *wireless* sangat modular dan fleksibel sehingga mudah untuk digunakan. Tapi, jaringan *wireless* juga memiliki kelemahan yaitu memanfaatkan frekuensi tinggi untuk menghantarkan sebuah komunikasi sehingga kerentanan terhadap keamanan juga lebih tinggi. Penyadapan pada jalur komunikasi (*man-in-the-middle attack*) dapat dilakukan lebih mudah karena tidak perlu mencari jalur kabel untuk melakukan hubungan. Salah satu cara untuk mengamankan jaringan *wireless* adalah dengan menggunakan metode *Extended Access List*. *Extended Access List* dapat mengatur hak akses tiap *host*, mengontrol apakah paket-paket tersebut dilewatkan atau dihentikan, dan dapat menjamin keamanan untuk setiap komputer. Pada penelitian dilakukan pembuatan jaringan *wireless* secara *real* dengan menggunakan perangkat jaringan seperti *Router Cisco*, *Access Point wireless*, laptop sebagai penyerang serta komputer sebagai *client*. Selain itu, dilakukan percobaan penyerangan terhadap jaringan *wireless* pada *protocol tcp* dan *icmp* dengan menggunakan *tools kali linux, wireshark*, dan *websploit*. Hasilnya metode yang digunakan berhasil mengamankan *protocol tcp*, sedangkan *protocol icmp* tidak berhasil.

Kata Kunci : Keamanan, Jaringan Wireless, Exteded Access List

1. Pendahuluan

Teknologi *wireless* saat ini berkembang sangat pesat terutama dengan hadirnya perangkat teknologi informasi dan komunikasi. Awalnya teknologi ini hanya didesain untuk aplikasi perkantoran dalam ruangan, namun sekarang *Wireless LAN* dapat digunakan pada jaringan *peer to peer* dalam ruangan dan juga *point to point* di luar ruangan maupun *point to multipoint* pada aplikasi *bridge.* Jaringan *Wireless LAN* di desain sangat modular dan fleksibel sehingga Jaringan ini dapat dioptimalkan pada lingkungan yang berbeda. Jaringan komunikasi *wireless* memberikan kemudahan dan fleksibilitas yang tinggi bagi para pemakainya untuk dapat mengadakan hubungan komunikasi dengan sesama pemakai jaringan *wireless* maupun dengan pemakai lain yang terhubung dengan jaringan yang memakai media transmisi kabel *(wired network)* sehingga sangat banyak digunakan, baik untuk komunikasi suara maupun data[1].

Teknologi *wireless* memanfaatkan frekuensi tinggi untuk menghantarkan sebuah komunikasi, maka kerentanan terhadap keamanan juga lebih tinggi dibanding dengan teknologi komunikasi yang lainnya. Penyadapan pada jalur komunikasi (*man-in-the-middle attack*) dapat dilakukan lebih mudah karena tidak perlu mencari jalur kabel untuk melakukan hubungan. Sistem yang tidak menggunakan pengamanan enkripsi dan otentikasi, atau menggunakan enkripsi yang mudah dipecahkan (*kriptanalisis*), akan sangat mudah ditangkap. Berbagai tindakan keamanan sudah pernah dilakukan, misalnya dengan *WEP (Wired Equivalent Privacy)* yang menjadi standart keamanan wireless sebelumnya, saat ini dapat dengan mudah dipecahkan dengan berbagai tools yang tersedia secara gratis di internet. *WPA-PSK* dan *LEAP* yang dianggap menjadi solusi menggantikan *WEP,* saat ini juga sudah dapat dipecahkan dengan metode *dictionary attack* secara *offline*[2].

Secara garis besar celah pada jaringan *wireless* terbentang di atas empat layer yaitu *Physical Layer, Network Layer, User Layer* dan *Application Layer* di mana keempat layer tersebut sebenarnya merupakan proses dari terjadinya komunikasi data pada media *wireless.* Hal ini membuat para penyerang atau penyusup (*hacker*) menjadi tertarik untuk melakukan berbagai aktifitas yang biasanya ilegal terhadap jaringan *wireless* (*WLAN*)[3].

Oleh karena itu, dilakukan penelitian metode *Extended Access List* yang merupakan salah satu jenis *Access Control List (ACL)* dan diterapkan pada jaringan *Wireless*. Metode ini merupakan metode keamanan yang tepat untuk komunikasi jaringan. *Extended Access List* berperan untuk mengatur hak akses tiap *host* yang ada di dalam simulasi jaringan tersebut. *Extended Access List* dapat menyaring lalu lintas data suatu jaringan dengan mengontrol

apakah paket-paket tersebut dilewatkan atau dihentikan. *Extended Access List* juga dapat menjamin keamanan untuk setiap komputer sehingga jalur komunikasi serta hak akses setiap komputer dapat berjalan dengan baik[4].

Adapun batasan masalah dalam penelitian ini adalah sebagai berikut : a) Keamanan jaringan *WLAN* tidak membahas *WEP, WPA* dan *MAC filtering.* b) pengujian pada keamanan jaringan *WLAN* tidak menggunakan penyerangan jaringan seperti *WEP Attack, DDoS Attack,* dan *Rouge Access point*. c) Tidak membahas penyerangan pada sistem jaringan *WLAN.*

2. Tinjauan Pustaka

Beberapa penelitian sudah pernah dilakukan, salah satunya dilakukan oleh Musril[4]. Dalam penelitian ini dibahas penerapan *Extended Access List* dalam jaringan sehingga dapat melakukan *filter* terhadap paket data yang melewati jaringan. Penerapannya menggunakan *software Packet Tracer* 6.1.1 untuk membuat bentuk jaringan dan mensimulasikannya. Pada penelitian ini *protokol* yang dikonfigurasi antara lain adalah *TCP* (*port* yang diatur adalah *www/http, telnet, ftp,* dan *smtp*), *UDP* (*port* yang diatur adalah *dns*), dan *ICMP* (yang dikonfigurasi adalah *ping*). Hasilnya *Extended Access List* dapat melakukan pengendalian *trafik* jaringan dengan menyaringan paket data yang melewati *router*. *Extended Access List* melakukan pengecekan terhadap beberapa atribut, yaitu alamat sumber, alamat tujuan, *protokol,* dan nama *port*[4].

Penelitian yang lain menganalisis tentang kelemahan keamanan pada jaringan *wireless*[5]. Secara garis besar, penelitian ini menemukan bahwa celah pada jaringan *wireless* terbentang di atas lima *layer* di mana kelima lapis *(layer)* tersebut sebenarnya merupakan proses dari terjadinya komunikasi data pada media *wireless.* Kelima lapis itu adalah *Aplication layer, Transport Layer, Network Layer, Data Link Layer,* dan *Physical Layer.* Selain itu, penelitian ini menganalisis model-model keamanan yang terjadi pada masing-masing lapis pada teknologi *wireless* seperti menyembunyikan *SSID,* memanfaatkan kunci *WEP, WPA-PSK* atau *WPA2-PSK,* implementasi fasilitas *MAC filtering,* serta pemasangan infrastruktur *captive portal.* Jaringan *wireless* menggunakan frekuensi yang sifat lebih terbuka dibanding dengan menggunakan kabel, maka kerentanan keamanan jalur komunikasi akan lebih berbahaya dibanding menggunakan kabel[5].

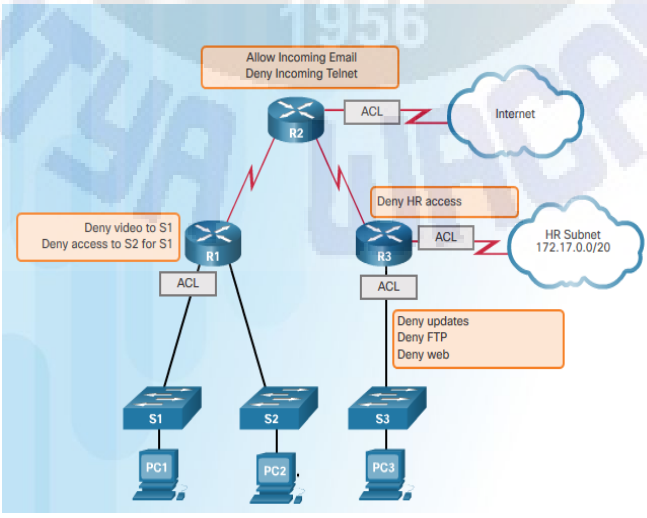
Jaringan *Lokal Nirkabel* atau *wireless local area network* (*Wireless LAN* atau *WLAN*) merupakan teknologi jaringan komputer tanpa kabel, yaitu menggunakan gelombang berfrekuensi tinggi agar komputer-komputer bisa saling terhubung tanpa menggunakan kabel sehingga mengakibatkan pengguna mempunyai fleksibilitas yang tinggi dan tidak tergantung

pada suatu tempat atau lokasi. Teknologi 802.11 yang dikeluarkan oleh IEEE mengatur standar pada dua buah lapisan terbawah dari jaringan komputer[6].

Teknologi *Wireless* terus dikembangkan hingga sekarang. Generasi teknologi *wireless* yang dikembangkan berdasarkan kode IEEE adalah sebagai berikut : a) 802.11b merupakan standar yang paling banyak digunakan di kelas standar 802.11. Standar ini memiliki data *rate* sebesar 11 *Mbps* serta mengunakan frekuensi 2,4 *GHz*. b) 802.11g merupakan standar yang menyediakan jalur komunikasi kecepatan tinggi hingga 54 *Mbps*. Namun, frekuensi yang digunakan pada standar ini sama dengan frekuensi yang digunakan standar 802.11b yaitu frekuensi gelombang 2,4 *GHz*. c) 802.11a standar ini menggunakan frekuensi 5 *GHz Unlicensed National Information Infrastrusture (UNII)* dengan kecepatan transfer 54 *Mbps*. d) 802.11n merupakan standar yang mampu menyediakan kecepatan data lebih dari 100 *Mbps* sampai 500 *Mbps* dengan menggunakan frekuensi 2,4 *GHz* dan 5 *GHz*. e) 802.11ac standar ini merupakan teknologi *wireless* generasi baru. Standar ini memiliki kecepatan jaringan yang mencapai 1300 *Mbps* atau 1,3 *Gbps* serta menggunakan frekuensi 5 *GHz*[6].

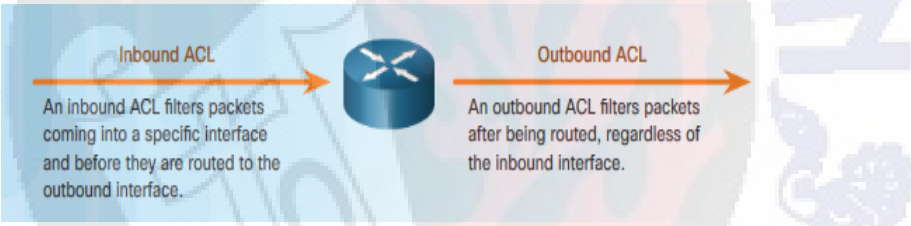
Tindakan keamanan pada jaringan wireless telah dilakukan, misalnya dengan cara *WEP*, *WPA-PSK* serta penyembuyian *SSID*. Namun tindakan keamanan tersebut sangat mudah untuk dipecahkan oleh *hacker*.

Mekanisme dasar *ACL* yakni menyaring paket yang tidak diinginkan ketika komunikasi data berlangsung sehingga menghindari permintaan akses maupun paket data yang mencurigakan dalam keamanan sebuah jaringan. Apabila ditemukan akses yang tidak diizinkan maka *router* akan langsung memblok alamat perangkat jaringan tersebut. Mekanisme *ACL* dapat dilihat pada Gambar 1 berikut[7].



Gambar 1 Mekanisme *ACL* [7]

Pada Gambar 1 menunjukkan router *R2* dengan *link WAN serial* ke Internet. *Router* memiliki *ACL* ditempatkan pada *interface* serial. Pada *router R2 ACL* memungkinkan email masuk, tetapi memblokir permintaan telnet yang masuk. Ada dua lagi *link WAN serial* aktif pada *router*, dan masing-masing dari dua *link WAN serial* ini terhubung ke *router R1* dan *R3*. *R1* dan *R3* memiliki *interface LAN* yang terhubung ke *switch*. Ada *ACL* yang dikonfigurasi pada *interface LAN*. *ACL* pada *router R1* menyangkal lalu lintas video menuju *switch* yang terhubung dan menolak *switch* untuk membuat koneksi ke *switch* pada *interface LAN* lainnya. *R3* memiliki dua *interface LAN*. Satu *interface LAN* terhubung ke *switch*, dan *link WAN serial* dilampirkan ke *subnet internal*. *ACL* pada tautan *subnet internal* yang menolak semua lalu lintas yang berasal dari *router* yang diarahkan ke *subnet*. Oleh karena itu, hanya data yang berasal dari dalam *subnet* yang diizinkan meninggalkan jaringan. *Interface LAN* pada *router R3* memiliki *ACL* yang menolak pembaruan apa pun, *FTP*, atau lalu lintas *web*[5]. *ACL* mendefinisikan aturan yang memberikan kontrol tambahan untuk paket yang masuk ke *router*, dan paket yang keluar dari *router*. Aturan dapat diterapkan pada lalu lintas masuk dan lalu lintas keluar seperti yang ditunjukkan pada Gambar 2 berikut[7].



Gambar 2 *Inbound* & *Outbound ACL* [7]

Pada Gambar 2 menunjukkan paket yang masuk diproses terlebih dahulu sebelum diarahkan ke *interface* keluar. Lalu setelah itu, paket akan filter setelah dialihkan dari interface masuk[7].

ACL Standar menyaring alamat IP sumber dalam paket IP. Ini juga digunakan untuk membatasi akses telnet ke router. Nomor ACL untuk rentang ACL standar mulai 1 hingga 99 dan 1300 hingga 1999. Entri dapat dibuat dalam IP ACL dengan nomor standar dengan menggunakan perintah daftar-akses. *Standar access list* dalam melakukan penyaringan paket data hanya memperhatikan alamat sumber (alamat asal) dari paket yang dikirimkan[8].

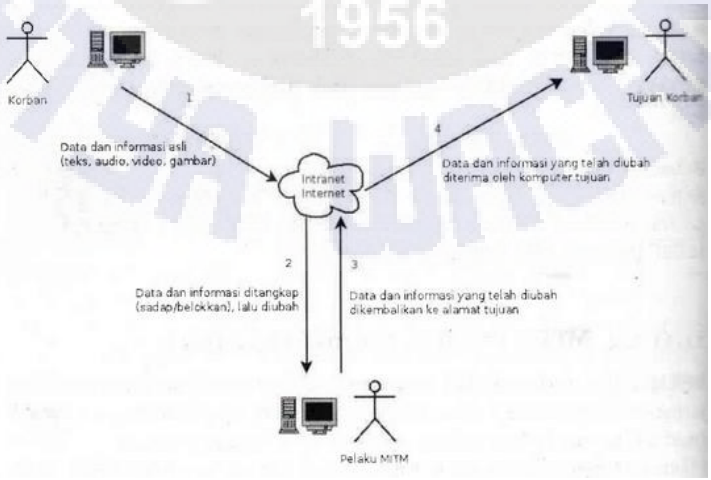
Extended Access List merupakan sebuah metode yang berfungsi untuk menyeleksi paket-paket yang keluar masuk *network*. *Extended access list* memungkinkan penyaringan berdasarkan sumber atau alamat tujuan, *protocol* yang dipilih, *port* yang digunakan, dan apakah koneksi sudah ditetapkan sehingga dapat secara efektif mengizinkan akses pengguna ke *LAN* fisik dan menghentikan mereka dari mengakses *host* tertentu atau hanya layanan

tertentu saja dari *host* tersebut. Nomor daftar akses *IP extended* adalah 100 hingga 199 dan dua perintah yang digunakan pada konfigurasi *Extended Access List* adalah *permit* dan *deny*[8].

Pada umumnya, kelemahan jaringan wireless berada pada kelima layer yaitu : *Aplication layer*, *Transport Layer*, *Network Layer*, *Data Link Layer*, dan *Physical Layer*. Hal ini menyebabkan para penyusup dapat dengan mudah untuk menyerang jaringan *wireless* tersebut. Selain itu, penyadapan jalur komunikasi atau biasa disebut *Man In The Middle Attack* sangat mudah dilakukan karena tidak perlu mencari kabel.

MITMA (*Man In The Middle Attack)* merupakan bentuk serangan di dalam jaringan komputer, di mana penyerang *(attacker)* berada di tengah-tengah *(middle)* antara korban dengan tujuan korban. Bentuk serangan dari *MITMA* dapat berupa adanya penyadapan komunikasi suara dan teks, perusakan privasi, dan hilangkan keaslian suatu data akibat diubah oleh pelaku *(attacker)*. Sejumlah aplikasi dan layanan pada *application layer* yang rentan terhadap jenis serangan *Man In The Middle (MITMA)* antara lain pada jenis layanan surat elektronik *(e-mail)*, layanan komunikasi berbasis *web*, *Domain Name System (DNS)*, dan telepon berbasis *Internet Protocol (Voice Over Internet Protocol/VOIP)*[9].

Gambar 3 mengilustrasikan penjelasan untuk suatu studi kasus *MITMA (Man In The Middle Attack)*, sebagai salah satu bentuk ancaman keamanan jaringan komputer. Bentuk penyerangan dimulai dari seorang pelaku *(Attacker)* melakukan pembelokan, penyadapan, pencurian paket data berupa audio, video, gambar, dan dokumen untuk kemudian diubah *(modifikasi)* lalu dikembalikan ke komputer tujuan, kemudian diterima oleh komputer tujuan tersebut. Pelaku berada di tengah-tengah antara korban dan tujuan korban pada jaringan komputer baik intranet maupun internet[9].

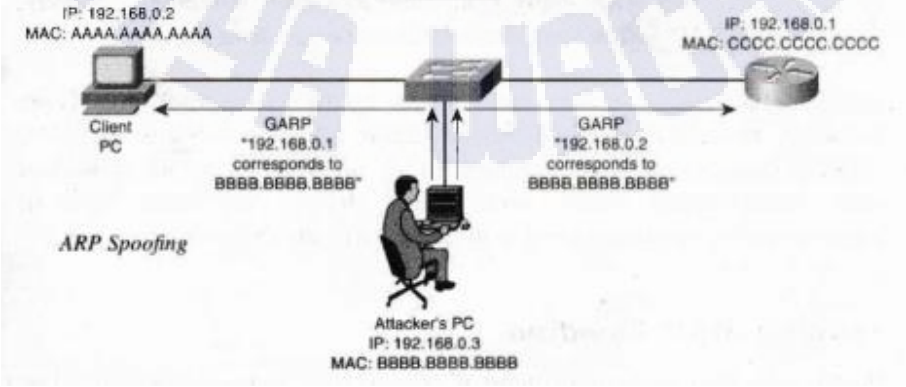


Gambar 3 Ilustrasi *MITMA* [9]

ARP Attack atau *ARP Spoofing* atau juga disebut juga dengan *ARP Poisoning*, merupakan bentuk serangan terhadap *protocol ARP (Address Resolution Protocol)* pada jaringan komputer. Peranan *ARP* adalah untuk menterjemahkan alamat jaringan berbasiskan *Internet Protocol (IP Address)* pada suatu komputer dengan alamat fisik berdasarkan perangkat keras *(Hardware)* penghubung yang dimiliki oleh komputer bersangkutan dengan menggunakan bantuan *Meda Access Control (MAC Address)*.

Keterkaitan antara *IP Address* dan *MAC Address* pada suatu komputer, akan menjadi identitas dari komputer bersangkutan di dalam jaringan komputer, sehingga dapat dikenali oleh komputer-komputer lainnya di dalam jaringan dan dapat melakukan koneksi dengan baik termasuk juga melakukan komunikasi dan pertukaran data di dalamnya[9].

Di dalam menjalankan fungsinya, *ARP* memiliki empat buah komponen yang saling bekerja sama untuk dapat mengetahui komputer mana yang memiliki *MAC Address* dan *IP Address* yang dimaksud. Keempat komponen tersebut yaitu : a) ARP Request, berfungsi untuk meminta informasi mengenai komputer mana yang memiliki *IP Address* yang dimaksud. Komputer pengirim atau komputer asal akan mengirimkan ke semua komputer di dalam jaringan *(Broadcast)* mengenai informasi suatu *IP Address* yang ingin ditujunya. b) ARP Reply, berfungsi untuk membantu komputer asal atau komputer pengirim di dalam memperoleh jawaban atas pertanyaan Broadcast yang diajuakannya kepada komputer-komputer lain di dalam satu jaringan. Jawaban diberikan langsung oleh komputer penerima atau komputer tujuan. c) *RARP (Reverse ARP Request)*, sama dengan *ARP Request*, namun informasi yang ditanyakan adalah *MAC Address*. d) *RARP (Reverse ARP Reply)*, sama dengan *ARP Reply*, namun informasi yang diberikan atau dijawab adalah *MAC Address*[9].



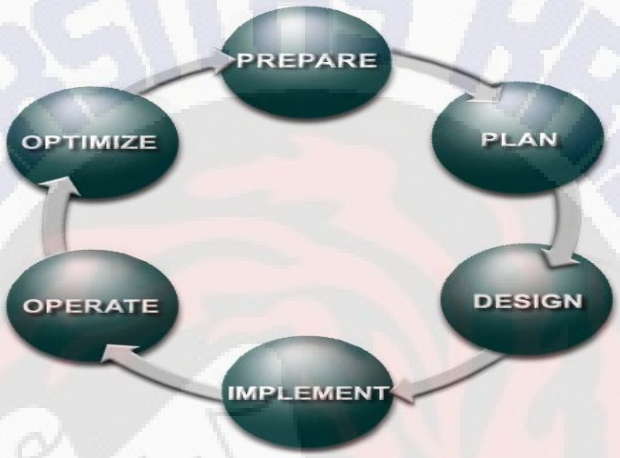
Gambar 4 Bentuk *ARP Attack (ARP Spoofing/Poisoning)* [9]

Pada Gambar 4 *attacker* melakukan penipuan untuk informasi yang diterima pada komunikasi jaringan dengan melakukan perubahan data di dalam jaringan komputer berupa *IP*

Address dan *MAC Address* dari komputer *client* dan *router* sesuai dengan *IP Address* dan *MAC Address* yang dimiliki, sehingga *attacker* dapat berpura-pura sebagai komputer yang sesungguhnya[9].

3. Metode dan Perancangan

Metode yang digunakan dalam penelitian ini merupakan metode pengembangan jaringan *PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize).* Metode ini merupakan formula khusus yang telah dihasilkan oleh Cisco seperti yang dapat digambarkan pada Gambar 5[10].



Gambar 5 Metode PPDIOO [10]

Pada Gambar 5 dapat dijelaskan sebagai berikut :

a. Fase *Prepare* (Persiapan) merupakan fase untuk menetapkan kebutuhan apa saja yang dibutuhkan dalam perancangan suatu jaringan, yaitu :
   - Router *cisco*
   - *Access Point (AP)*
   - Satu *PC Client*
   - Laptop untuk Menyerang & monitoring

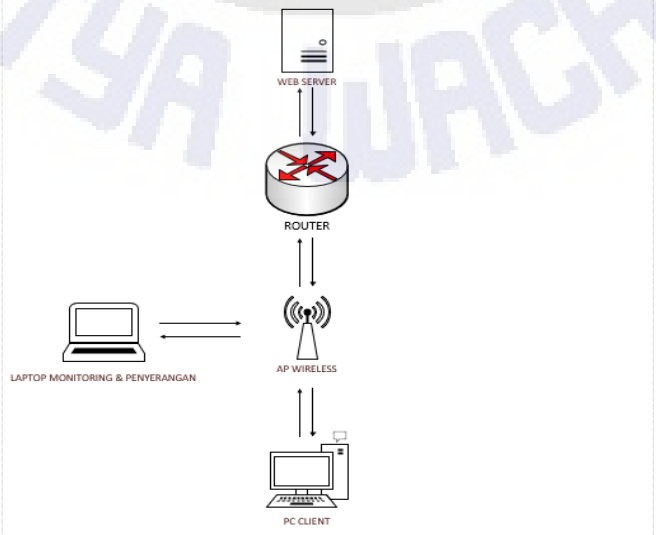
b. Fase *Plan* (Perencanaan) merupakan fase dimana mengidentifikasi persyaratan jaringan berdasarkan tujuan dan kebutuhan. Dalam fase ini akan dilakukan konsep dan desain jaringan secara abstrak sesuai dengan kebutuhan. Hal ini akan berupa sketsa gambar suatu jaringan.

c. Fase *Design* (Desain) merupakan fase untuk merancang suatu jaringan fisik berdasarkan kebutuhan dan tujuan yang didapatkan. Pada bagian ini akan dilakukan perancangan suatu jaringan dan disertai dengan konfigurasinya.

d. Fase *Implement* (Implementasi) pada fase ini akan dilakukan percobaan pada sistem jaringan yang telah dikonfigurasi. Pengujiannya akan menggunakan *PC* monitoring yang terkoneksi dengan jaringan *wireless*. Penyerangan yang dilakukan adalah penyerangan *Man in the middle attack.*
e. Fase *Operate* (operasional) pada fase ini akan dilakukan pengujian kembali dengan melakukan penyerangan secara terus-menerus pada sistem jaringan dan akan dilakukan pengecekan apakah metode yang digunakan berjalan dengan baik atau tidak.
f. Fase *Optimize* (Optimilisasi) pada fase ini akan diperbaharui jika ada sistem jaringan yang tidak berjalan dengan baik sewaktu menerima penyerangan.

Pada tahap persiapan dilakukan dengan cara menetapkan perangkat jaringan yang dibutuhkan dalam perancangan sistem keamanan jaringan. Perangkat yang digunakan pada penelitian ini meliputi perangkat lunak dan perangkat keras. Perangkat lunak yang digunakan meliputi *PuTTY, Cisco Packet Tracer, Virtual Box, Wireshark, Kalli Linux, Ubuntu Server 14.04, Visio.* Sedangkan perangkat keras yang digunakan meliputi *Router cisco 1840, TP-LINK MR3220, Laptop Asus A456U, PC Acer H81M-DS2, Cable Serial, Cable Console, Cable Cross-over.*

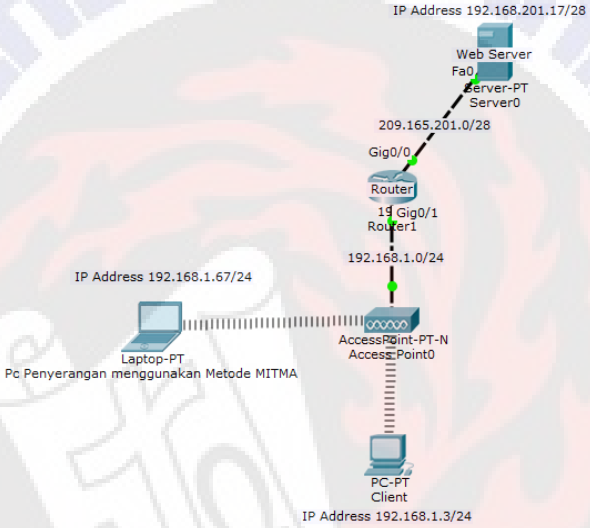
Pada tahap *plan* dilakukan pembuatan arsitektur jaringan pada sistem keamanan jaringan yang meliputi : *Web Server, Router, AP Wireless, Pc Client,* Laptop Penyerangan dan monitoring. Arsitektur jaringan sangat diperlukan karena merupakan rancangan arus komunikasi dalam jaringan seperti dapat dilihat pada Gambar 6 berikut.



Gambar 6 Arsitektur Jaringan Keamanan Jaringan *Wireless LAN*

Pada Gambar 6 menunjukkan perancangan arsitektur keamanan jaringan *Wireless LAN*. *Router* berperan sebagai jembatan komunikasi antara *client* dan *Web Server* dan sebagai pengaman dalam komunikasi. *Client* akan mengakses data yang berada di *Web server*, sementara laptop penyerangan akan mencoba menyerang informasi tersebut. Pada tahap penyerangan informasi, laptop penyerang akan menggunakan *ARP attack* untuk menduplikasi *IP Address* dan *MAC Address* sehingga *PC Client* tidak dapat mengakses *web server.*

Pada fase design dilakukan perancangan jaringan menggunakan topologi bus karena menggunakan kabel tunggal atau kabel pusat tempat yang menghubungkan client dan web server seperti dapat dilihat pada Gambar 7 berikut.



Gambar 7 Topologi Bus

Pada Gambar 7 dapat dijelaskan bahwa *client* dan laptop penyerangan akan mendapatkan *IP Address* secara *dhcp* dari *router*. Selain itu, laptop penyerangan dan *client* terkoneksi dengan router menggunakan *Access Point wireless* untuk dapat berkomunikasi dengan *web server*.

Selain itu juga, dilakukan pembagian *IP Address* kepada setiap *device* yang terkoneksi dalam jaringan. Hal ini dilakukan agar setiap *device* yang terkoneksi dalam jaringan, dapat saling berkomunikasi dengan baik.

Tabel 1 *IP Address*

Perangkat Jaringan	***IP Address***
Web Server	192.168.201.17/28
Router	192.168.201.18/28 192.168.1.1/24
AP	192.168.1.2/24
Client	192.168.1.3/24
PC Penyerang & Monitoring	192.168.1.67/24

Pada Tabel 1 pembagian *IP Address* menggunakan kelas C. Hal ini dilakukan karena kelas C pada pengalamatan berbasiskan *Internet Protocol (IP Address)* khususnya pada *IPV₄*, merupakan kelas yang sesuai dengan jaringan berskala kecil. Kelas C hanya memiliki jangkauan *(range)* untuk pengalamatan dalam bentuk *IPV₄* dimulai dari 192.0.0.0 hingga 223.255.255.255. Jumlah jangkauan tersebut hanya mampu membentuk 2.097.152 buah jaringan, dimana setiap jaringan tersebut hanya mampu menampung hingga 254 buah komputer perangkat yang terhubung. Selain itu juga, Pada Tabel 3.1 perhatikan angka 24 dan 28 yang diawali dengan tanda /. Angka tersebut menyatakan *Prefix Length* atau jumlah *bit* yang ditandai pada jaringan komputer yang bersangkutan. Dalam kelas C jumlah *bit* dimulai dari angka 24 yang dapat menampung *host* sebanyak 256 sehingga jumlah *bit* tersebut mampu untuk menampung *host* dalam jaringan. Semakin besar jumlah *bit* tersebut, semakin kecil pula jumlah *host* yang dapat ditampung.

Setelah dilakukan pembuatan *design* jaringan dan pembagian *IP Address* kepada setiap perangkat yang terkoneksi, lalu dilakukan konfigurasi *ACL Extended*. Konfigurasi *ACL Extended* dilakukan pada *Router* karena *Router* yang akan menjadi jalur berjalannya informasi antara *client* dan *Web Server* serta menjadi tempat yang mengamankan informasi tersebut seperti pada gambar 8 berikut.

```
ip classless
!
no ip http server
!
access-list 100 permit icmp host 192.168.1.3 host 192.168.201.17
access-list 100 permit tcp host 192.168.1.3 host 192.168.201.17 eq www
access-list 100 deny   ip any any
!
control-plane
!
!
```

Gambar 8 *ACL Extended*

Pada Gambar 8 merupakan hasil *Konfigurasi ACL Extended* yang mengatur *client* atau *host* 192.168.1.3 dapat mengakses *web server* melalui *protocol icmp* dan *tcp* sedangkan *client* yang tidak mendapatkan *IP* 192.168.1.3 tidak dapat mengakses *web server* melalui *protocol icmp* dan *tcp*. Selain konfigurasi ini, ACL Extended juga memiliki konfigurasi yang lain. Konfigurasinya dapat dilihat pada Gambar 9 berikut.

```
interface FastEthernet0/0
 ip address 192.168.201.18 255.255.255.248
 ip access-group 100 out
 duplex auto
 speed auto
```

Gambar 9 *ip access-group 100 out*

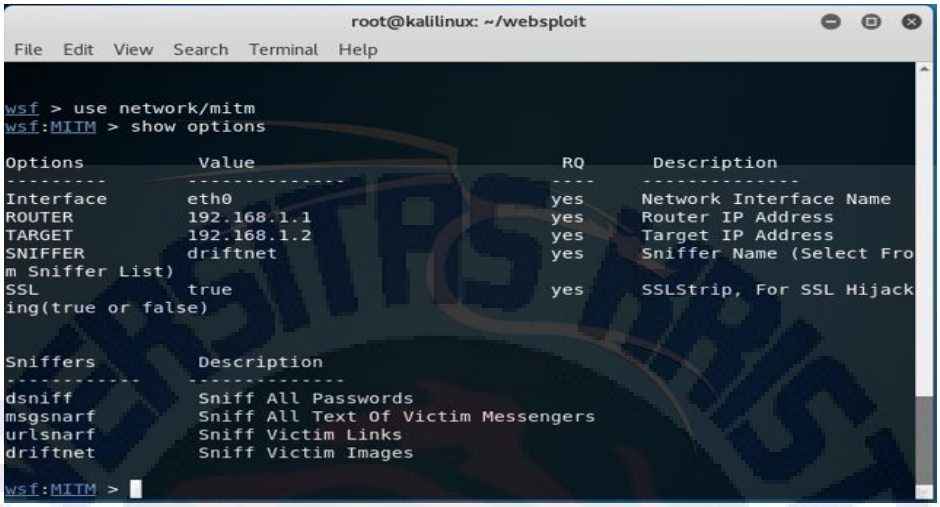
Gambar 9 menunjukkan bahwa setiap data yang menuju web server akan di filter terlebih dahulu karena *ip access-group 100 out berada pada interface Fa0/0* yang menjadi jalur komunikasi antara *client* dan *web server*. Setelah *konfigurasi* ini dilakukan cisco juga menyediakan *konfigurasi* untuk mengetahui apakah *konfigurasinya* berjalan atau tidak. *Konfigurasinya* dapat dilihat pada Gambar 10 berikut.

```
Router#show access-lists 100
Extended IP access list 100
    10 permit icmp host 192.168.1.3 host 192.168.201.17 (4 matches)
    20 permit tcp host 192.168.1.3 host 192.168.201.17 eq www (6 matches)
    30 deny ip any any (3205 matches)
Router#show access-lists 100
Extended IP access list 100
    10 permit icmp host 192.168.1.3 host 192.168.201.17 (8 matches)
    20 permit tcp host 192.168.1.3 host 192.168.201.17 eq www (6 matches)
    30 deny ip any any (3264 matches)
Router#show access-lists 100
Extended IP access list 100
    10 permit icmp host 192.168.1.3 host 192.168.201.17 (12 matches)
    20 permit tcp host 192.168.1.3 host 192.168.201.17 eq www (6 matches)
    30 deny ip any any (3381 matches)
Router#show access-lists 100
Extended IP access list 100
    10 permit icmp host 192.168.1.3 host 192.168.201.17 (12 matches)
    20 permit tcp host 192.168.1.3 host 192.168.201.17 eq www (11 matches)
    30 deny ip any any (3440 matches)
```

Gambar 10 *ACL Extended* Berjalan

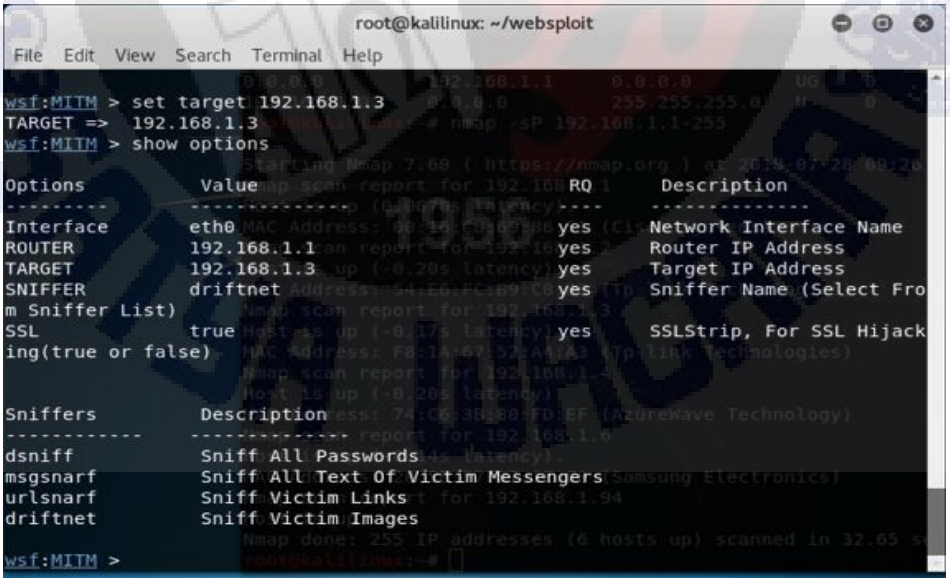
Pada Gambar 10 menunjukkan bahwa *ACL Extended* berjalan dengan baik sehingga muncul keterangan berupa 4 *matches* dan 6 *matches* bahwa *client* 192.168.1.3 dapat mengakses *web server* melalui *protocol icmp* dan *tcp*. Selain itu juga, *client* 192.168.1.3 lebih sering mengakses *icmp* atau *ping* sehingga keterangan dalam mengakses lebih besar dan terjadi berulang-ulang dari pada mengakses *tcp* atau *http*. Pemblokiran *client* yang tidak mendapatkan *IP* 192.168.1.3 juga berhasil karena keterangan pemblokirannya sangat besar.

Pada tahap *Implement & operate* dilakukan percobaan penyerangan kepada sistem keamanan jaringan. Metode penyerangan yang dilakukan dengan metode *Man in the middle attack* seperti dapat dilihat pada gambar 11 berikut.



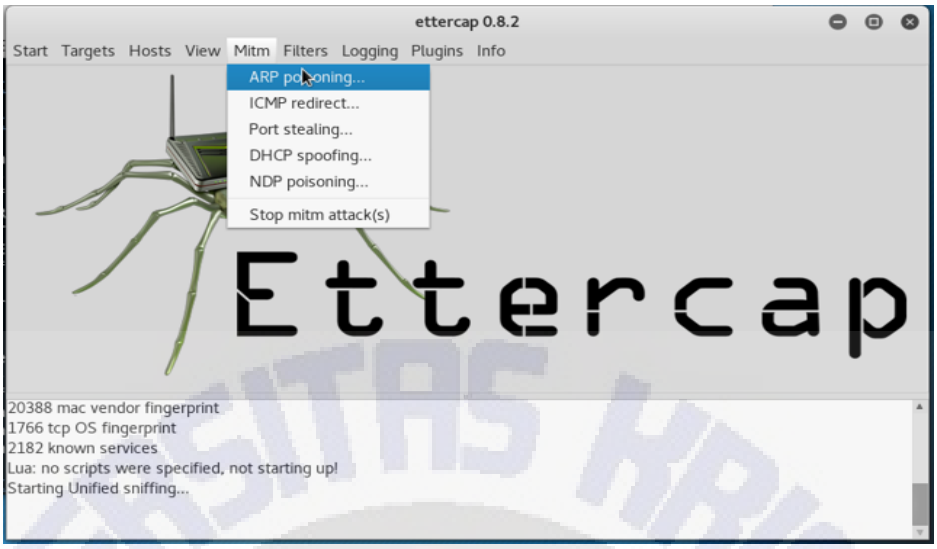
Gambar 11 *Network Man In The Middle Attack*

Pada Gambar 11 merupakan bagian jaringan dari metode *MITMA.* Bagian ini sangat penting karena bagian ini dilakukan pengaturan *Interface*, *IP Router*, *IP* Target, dan *Sniffer* yang digunakan dalam penyerangan. Hal ini harus disesuaikan dengan konsep penyerangan yang akan dilakukan.



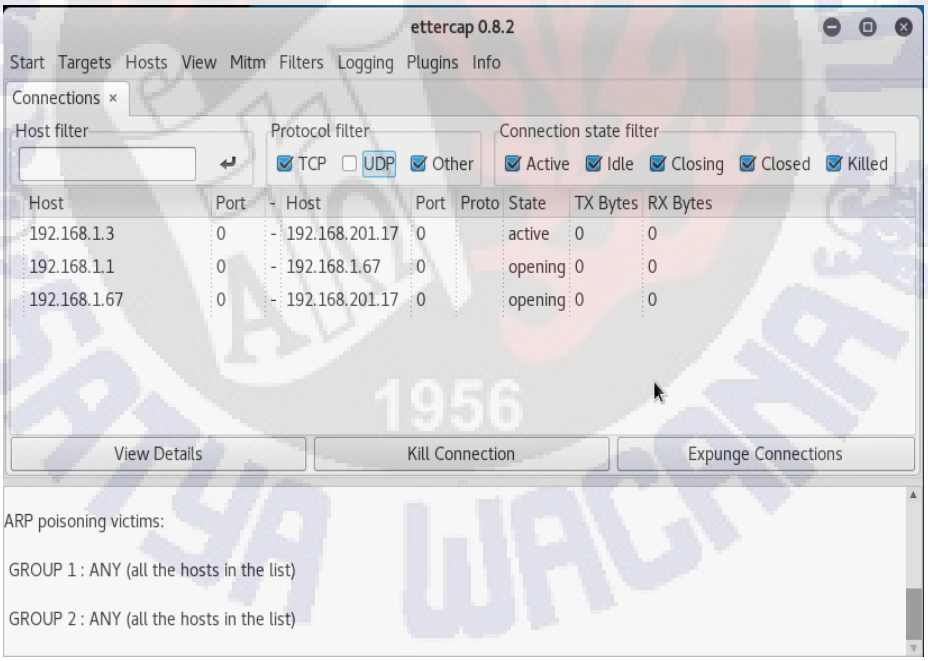
Gambar 12 *IP* Target

Pada Gambar 12 merupakan pengubahan *IP* TARGET sesuai dengan yang dimilki oleh client, sehingga penyerangan yang dilakukan akan tepat sasaran. Pada bagian ini hanya dilakukan perubahan pada bagian TARGET karena ROUTER dan Interface sudah sesuai.



Gambar 13 Metode *Mitm*

Gambar 13 merupakan metode-metode penyerangan *Man In The Middle Attack*. Penyerangan dilakukan dengan metode *ARP Poisoning*.



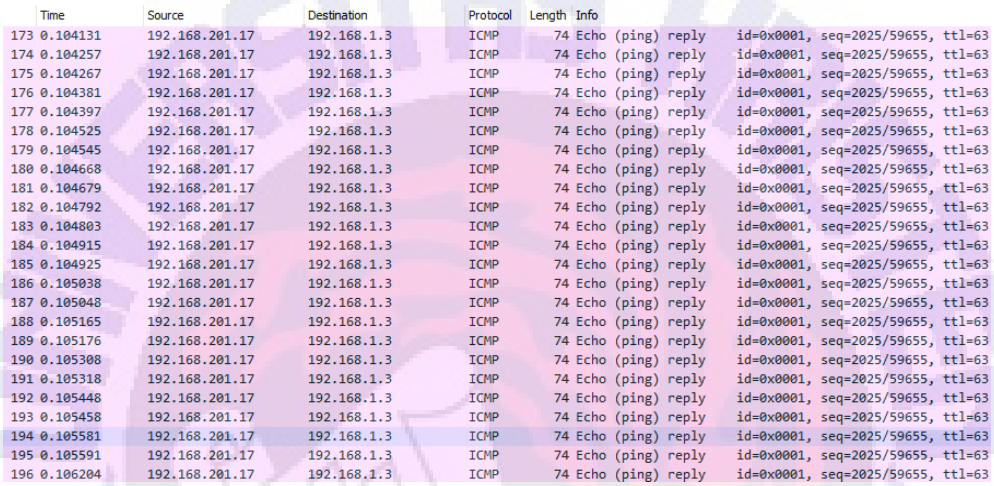
Gambar 14 Mengakses *Web server*

Pada Gambar 14 dapat dilihat bahwa IP Client yang menjadi target terbaca pada bagian connections. Hal ini menunjukan bahwa penyerangan berhasil dilakukan. Percobaan penyerangan ini dilakukan secara terus-menerus agar dapat memastikan apakah metode keamanan serta metode penyerangan berjalan dengan baik.

Pada tahap *Optimize* sudah dilakukan perbaruan sistem keamanan karena didapati beberapa hal yang tidak berjalan dengan baik. Akan tetapi, perbaruan sistem tersebut belum maksimal karena keterbatasan waktu dan pengunaan perangkat jaringan.

4. Hasil dan Pembahasan

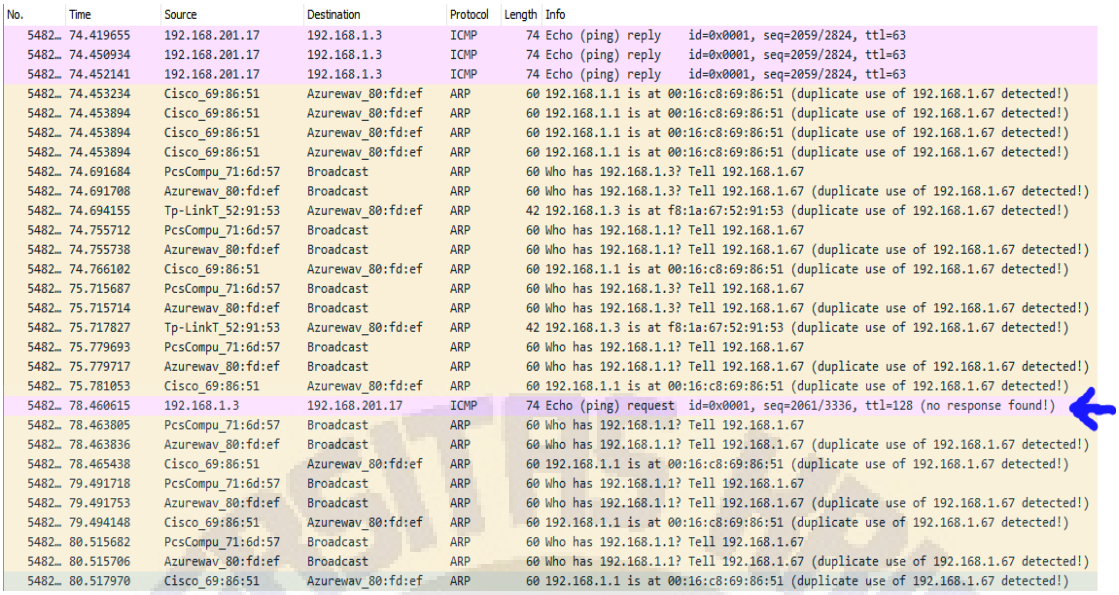
Pada bagian ini dilakukan analisis hasil penyerangan terhadap sistem keamanan jaringan. Analisis tersebut menggunakan *software wireshark* seperti pada Gambar 15 berikut.



	Time	Source	Destination	Protocol	Length	Info	
173	0.104131	192.168.201.17	192.168.1.3	ICMP	74	Echo (ping) reply	id=0x0001, seq=2025/59655, ttl=63
174	0.104257	192.168.201.17	192.168.1.3	ICMP	74	Echo (ping) reply	id=0x0001, seq=2025/59655, ttl=63
175	0.104267	192.168.201.17	192.168.1.3	ICMP	74	Echo (ping) reply	id=0x0001, seq=2025/59655, ttl=63
176	0.104381	192.168.201.17	192.168.1.3	ICMP	74	Echo (ping) reply	id=0x0001, seq=2025/59655, ttl=63
177	0.104397	192.168.201.17	192.168.1.3	ICMP	74	Echo (ping) reply	id=0x0001, seq=2025/59655, ttl=63
178	0.104525	192.168.201.17	192.168.1.3	ICMP	74	Echo (ping) reply	id=0x0001, seq=2025/59655, ttl=63
179	0.104545	192.168.201.17	192.168.1.3	ICMP	74	Echo (ping) reply	id=0x0001, seq=2025/59655, ttl=63
180	0.104668	192.168.201.17	192.168.1.3	ICMP	74	Echo (ping) reply	id=0x0001, seq=2025/59655, ttl=63
181	0.104679	192.168.201.17	192.168.1.3	ICMP	74	Echo (ping) reply	id=0x0001, seq=2025/59655, ttl=63
182	0.104792	192.168.201.17	192.168.1.3	ICMP	74	Echo (ping) reply	id=0x0001, seq=2025/59655, ttl=63
183	0.104803	192.168.201.17	192.168.1.3	ICMP	74	Echo (ping) reply	id=0x0001, seq=2025/59655, ttl=63
184	0.104915	192.168.201.17	192.168.1.3	ICMP	74	Echo (ping) reply	id=0x0001, seq=2025/59655, ttl=63
185	0.104925	192.168.201.17	192.168.1.3	ICMP	74	Echo (ping) reply	id=0x0001, seq=2025/59655, ttl=63
186	0.105038	192.168.201.17	192.168.1.3	ICMP	74	Echo (ping) reply	id=0x0001, seq=2025/59655, ttl=63
187	0.105048	192.168.201.17	192.168.1.3	ICMP	74	Echo (ping) reply	id=0x0001, seq=2025/59655, ttl=63
188	0.105165	192.168.201.17	192.168.1.3	ICMP	74	Echo (ping) reply	id=0x0001, seq=2025/59655, ttl=63
189	0.105176	192.168.201.17	192.168.1.3	ICMP	74	Echo (ping) reply	id=0x0001, seq=2025/59655, ttl=63
190	0.105308	192.168.201.17	192.168.1.3	ICMP	74	Echo (ping) reply	id=0x0001, seq=2025/59655, ttl=63
191	0.105318	192.168.201.17	192.168.1.3	ICMP	74	Echo (ping) reply	id=0x0001, seq=2025/59655, ttl=63
192	0.105448	192.168.201.17	192.168.1.3	ICMP	74	Echo (ping) reply	id=0x0001, seq=2025/59655, ttl=63
193	0.105458	192.168.201.17	192.168.1.3	ICMP	74	Echo (ping) reply	id=0x0001, seq=2025/59655, ttl=63
194	0.105581	192.168.201.17	192.168.1.3	ICMP	74	Echo (ping) reply	id=0x0001, seq=2025/59655, ttl=63
195	0.105591	192.168.201.17	192.168.1.3	ICMP	74	Echo (ping) reply	id=0x0001, seq=2025/59655, ttl=63
196	0.106204	192.168.201.17	192.168.1.3	ICMP	74	Echo (ping) reply	id=0x0001, seq=2025/59655, ttl=63

Gambar 15 Protocol ICMP

Pada Gambar 15 menunjukkan bahwa *client* mengakses web server melalui protocol *icmp* tidak mengalami gangguan sewaktu belum mangalami serangan. Kemudian dilakukan penyerangan dan hasil dari penyerangan tersebut dapat dilihat pada Gambar 16 berikut.



No.	Time	Source	Destination	Protocol	Length	Info
5482…	74.419655	192.168.201.17	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=2059/2824, ttl=63
5482…	74.450934	192.168.201.17	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=2059/2824, ttl=63
5482…	74.452141	192.168.201.17	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=2059/2824, ttl=63
5482…	74.453234	Cisco_69:86:51	Azurewav_80:fd:ef	ARP	60	192.168.1.1 is at 00:16:c8:69:86:51 (duplicate use of 192.168.1.67 detected!)
5482…	74.453894	Cisco_69:86:51	Azurewav_80:fd:ef	ARP	60	192.168.1.1 is at 00:16:c8:69:86:51 (duplicate use of 192.168.1.67 detected!)
5482…	74.453894	Cisco_69:86:51	Azurewav_80:fd:ef	ARP	60	192.168.1.1 is at 00:16:c8:69:86:51 (duplicate use of 192.168.1.67 detected!)
5482…	74.453894	Cisco_69:86:51	Azurewav_80:fd:ef	ARP	60	192.168.1.1 is at 00:16:c8:69:86:51 (duplicate use of 192.168.1.67 detected!)
5482…	74.691684	PcsCompu_71:6d:57	Broadcast	ARP	60	Who has 192.168.1.3? Tell 192.168.1.67
5482…	74.691708	Azurewav_80:fd:ef	Broadcast	ARP	60	Who has 192.168.1.3? Tell 192.168.1.67 (duplicate use of 192.168.1.67 detected!)
5482…	74.694155	Tp-LinkT_52:91:53	Azurewav_80:fd:ef	ARP	42	192.168.1.3 is at f8:1a:67:52:91:53 (duplicate use of 192.168.1.67 detected!)
5482…	74.755712	PcsCompu_71:6d:57	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.67
5482…	74.755738	Azurewav_80:fd:ef	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.67 (duplicate use of 192.168.1.67 detected!)
5482…	74.766102	Cisco_69:86:51	Azurewav_80:fd:ef	ARP	60	192.168.1.1 is at 00:16:c8:69:86:51 (duplicate use of 192.168.1.67 detected!)
5482…	75.715687	PcsCompu_71:6d:57	Broadcast	ARP	60	Who has 192.168.1.3? Tell 192.168.1.67
5482…	75.715714	Azurewav_80:fd:ef	Broadcast	ARP	60	Who has 192.168.1.3? Tell 192.168.1.67 (duplicate use of 192.168.1.67 detected!)
5482…	75.717827	Tp-LinkT_52:91:53	Azurewav_80:fd:ef	ARP	42	192.168.1.3 is at f8:1a:67:52:91:53 (duplicate use of 192.168.1.67 detected!)
5482…	75.779693	PcsCompu_71:6d:57	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.67
5482…	75.779717	Azurewav_80:fd:ef	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.67 (duplicate use of 192.168.1.67 detected!)
5482…	75.781053	Cisco_69:86:51	Azurewav_80:fd:ef	ARP	60	192.168.1.1 is at 00:16:c8:69:86:51 (duplicate use of 192.168.1.67 detected!)
5482…	78.460615	192.168.1.3	192.168.201.17	ICMP	74	Echo (ping) request id=0x0001, seq=2061/3336, ttl=128 (no response found!)
5482…	78.463805	PcsCompu_71:6d:57	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.67
5482…	78.463836	Azurewav_80:fd:ef	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.67 (duplicate use of 192.168.1.67 detected!)
5482…	78.465438	Cisco_69:86:51	Azurewav_80:fd:ef	ARP	60	192.168.1.1 is at 00:16:c8:69:86:51 (duplicate use of 192.168.1.67 detected!)
5482…	79.491718	PcsCompu_71:6d:57	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.67
5482…	79.491753	Azurewav_80:fd:ef	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.67 (duplicate use of 192.168.1.67 detected!)
5482…	79.494148	Cisco_69:86:51	Azurewav_80:fd:ef	ARP	60	192.168.1.1 is at 00:16:c8:69:86:51 (duplicate use of 192.168.1.67 detected!)
5482…	80.515682	PcsCompu_71:6d:57	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.67
5482…	80.515706	Azurewav_80:fd:ef	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.67 (duplicate use of 192.168.1.67 detected!)
5482…	80.517970	Cisco_69:86:51	Azurewav_80:fd:ef	ARP	60	192.168.1.1 is at 00:16:c8:69:86:51 (duplicate use of 192.168.1.67 detected!)

Gambar 16 Hasil Penyerangan 1

Pada Gambar 16 dapat dilihat bahwa *client* yang mengakses *web server* dengan *protocol icmp* mengalami ganggugan karena laptop penyerangan mengirim *ARP* palsu untuk menggantikan atau menduplicate *IP Address* dan *MAC Address* yang dimiliki oleh *client*. Laptop penyerangan memiliki IP Address 192.168.1.67 sedangkan Client memiliki IP Address 192.168.1.3. Akhirnya seperti yang ditunjukan oleh panah biru, *client* 192.168.1.3 tidak dapat mengkses *web server*. *Client* juga mengakses *web server* dengan *protocol* yang lain seperti pada Gambar 17 berikut.

No.	Time	Source	Destination	Protocol	Length	Info
5484…	101.612817	Azurewav_80:fd:ef	Cisco_69:86:51	ARP	60	192.168.1.3 is at 74:c6:3b:80:fd:ef (duplicate use of 192.168.1.1 detected!)
5484…	101.612891	PcsCompu_71:6d:57	Tp-LinkT_52:91:53	ARP	60	192.168.1.1 is at 08:00:27:71:6d:57 (duplicate use of 192.168.1.3 detected!)
5484…	101.612900	Azurewav_80:fd:ef	Tp-LinkT_52:91:53	ARP	60	192.168.1.1 is at 74:c6:3b:80:fd:ef (duplicate use of 192.168.1.3 detected!)
5484…	101.622915	PcsCompu_71:6d:57	Cisco_69:86:51	ARP	60	192.168.1.2 is at 08:00:27:71:6d:57 (duplicate use of 192.168.1.1 detected!)
5484…	101.622937	Azurewav_80:fd:ef	Cisco_69:86:51	ARP	60	192.168.1.2 is at 74:c6:3b:80:fd:ef (duplicate use of 192.168.1.1 detected!)
5484…	101.623008	PcsCompu_71:6d:57	Tp-LinkT_b9:c8:d8	ARP	60	192.168.1.1 is at 08:00:27:71:6d:57 (duplicate use of 192.168.1.2 detected!)
5484…	101.623021	Azurewav_80:fd:ef	Tp-LinkT_b9:c8:d8	ARP	60	192.168.1.1 is at 74:c6:3b:80:fd:ef (duplicate use of 192.168.1.2 detected!)
5484…	102.563695	PcsCompu_71:6d:57	Broadcast	ARP	60	Who has 192.168.1.3? Tell 192.168.1.67
5484…	102.563729	Azurewav_80:fd:ef	Broadcast	ARP	60	Who has 192.168.1.3? Tell 192.168.1.67 (duplicate use of 192.168.1.67 detected!)
5484…	102.566464	Tp-LinkT_52:91:53	Azurewav_80:fd:ef	ARP	42	192.168.1.3 is at f8:1a:67:52:91:53 (duplicate use of 192.168.1.67 detected!)
5484…	103.132075	192.168.1.3	5.149.254.170	TCP	66	49988 → 2223 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5484…	103.457637	192.168.1.3	192.168.201.17	ICMP	74	Echo (ping) request id=0x0001, seq=2066/4616, ttl=128 (no response found!)
5484…	103.459799	PcsCompu_71:6d:57	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.67
5484…	103.459814	Azurewav_80:fd:ef	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.67 (duplicate use of 192.168.1.67 detected!)
5484…	103.461310	Cisco_69:86:51	Azurewav_80:fd:ef	ARP	60	192.168.1.1 is at 00:16:c8:69:86:51 (duplicate use of 192.168.1.67 detected!)
5484…	103.587704	PcsCompu_71:6d:57	Broadcast	ARP	60	Who has 192.168.1.3? Tell 192.168.1.67
5484…	103.587734	Azurewav_80:fd:ef	Broadcast	ARP	60	Who has 192.168.1.3? Tell 192.168.1.67 (duplicate use of 192.168.1.67 detected!)
5484…	103.590788	Tp-LinkT_52:91:53	Azurewav_80:fd:ef	ARP	42	192.168.1.3 is at f8:1a:67:52:91:53 (duplicate use of 192.168.1.67 detected!)
5484…	104.483713	PcsCompu_71:6d:57	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.67
5484…	104.483748	Azurewav_80:fd:ef	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.67 (duplicate use of 192.168.1.67 detected!)
5484…	104.485730	Cisco_69:86:51	Azurewav_80:fd:ef	ARP	60	192.168.1.1 is at 00:16:c8:69:86:51 (duplicate use of 192.168.1.67 detected!)

Gambar 17 Hasil Penyerangan 2

Pada Gambar 17 menunjukkan bahwa meskipun *protocol icmp* terganggu dengan penyerangan *ARP, protocol tcp* yang diakses oleh *client* tetap berjalan dengan baik karena data sampai kepada *web server* seperti yang ditunjukan pada bagian warna biru pada Gambar 16.

Pada *protocol icmp* metode *Extended Access List* tidak berhasil untuk mengamankan jaringan tersebut. Hal ini terjadi karena metode tersebut menggunakan *permit IP client*, sedangkan penyerangan yang dilakukan untuk mengirim dan mengubah *ARP* yang dimiliki *client*. Dalam metode tersebut sudah ditambahkan beberapa cara salah satunya yaitu dengan teknik *filtering* pada *interface* yang terhubung dengan *client* dengan *command "ip use ACL On Arp 100"*, namun tetap tidak berhasil.

5. Simpulan

Berdasarkan penelitian dan pengujian terhadap keamanan jaringan yang dilakukan, maka dapat disimpulkan bahwa keamanan jaringan menggunakan metode *ACL Extended* dapat menjaga keamanan jaringan *wireless* pada *protocol tcp* atau *http* sedangkan pada *protocol icmp* metode tersebut tidak berhasil. Selain itu, bagi penyerangan (*attacker*) dapat disimpulkan bahwa metode penyerangan terhadap jaringan adalah dengan cara mengumpulkan paket *Address Resolution Protocol (ARP)* yang dimiliki oleh komputer korban lalu ditukarkan dengan *ARP* yang dimiliki oleh *attacker*.

Kelemahan dari hasil analisis jaringan yang dimonitoring pada jaringan *wireless* area tersebut, tidak menjelaskan lebih jauh lagi tentang cara kerja penyerang *(attacker)* terhadap sumber daya sistem jaringan *wireless* serta tidak diterapkan pada jaringan *wireless* yang terkoneksi pada *internet*. Oleh sebab itu, saran untuk pengembangan selanjutnya adalah :

1. Pembuatan jaringan *wireless* secara *real* dan berskala besar serta terintegrasi dengan *internet*.
2. Memperbaharui kembali sistem keamanan *ACL Extended*.
3. Menggunakan metode *ACL Extended* yang lebih kompleks.
4. Mengembangkan ruang lingkup untuk *me-monitoring* tidak hanya *protokol-protokol* analisis lalu lintas jaringan *wireless*, tetapi juga dapat menganalisis *service protokol-protokol* pada jaringan *wireless*.

6. Daftar Pustaka

[1] Arianto, Tri. 2009. *Implementasi Wireless Local Area Network dalam RT/RW Net*. Semarang: Jurnal Teknologi Informasi DINAMIK. Vol. XIV, No.2:152-157

[2] Nugroho, Agung. 2012. *Analisa Keamanan Jaringan Wireless Local Area Network dengan Access Point TP-Link WA500G*. Surakarta:Universitas Muhammadiyah Surakarta

[3] Rumalutur, Sonny. 2014. *Analisis Keamanan Jaringan Wireless LAN (WLAN) Pada PT. PLN (Persero) Wilayah P2B Area Sorong.* Jakarta: Jurnal Teknologi dan Rekayasa. Vol. 19, No.3:48-60

[4] Musril, A.H. 2016. *Extended Access List untuk Mengendalikan Trafik Jaringan*. Medan:Jurnal Edukasi dan Penelitian Informatika (JEPIN). Vol.2, No.2:129-135

[5] Supriyanto, Aji. 2006. *Analisis Kelemahan Keamanan pada Jaringan Wireless*. Semarang: Jurnal Teknologi Informasi DINAMIK. Vol. XI, No.1:38-46

[6] Witono, Timotius. 2006. *Linux-Based Access Point Dalam Wireless LAN*. Bandung: Jurnal Informatika. Vol. 2, No.2:93-107

[7] Cisco Networking Academy, 2017. *Routing and Switching Essentials*. https://static-course-assets.s3.amazonaws.com/RSE6/en/index.html#7.1. Diakses 17 September 2018

[8] Agrawal dkk. 2016. *Ip Trafic Management with Access Control List Using Cisco Packet Treacer*. IJSETR:International Journal of Science, Engineering and Technology Research. Vol 5, No.5:1557

[9] Pratama, Eka Agus Putu I. 2015. *Handbook Jaringan Komputer*. Bandung: Informatika Bandung

[10] Solikin, I. 2017. *Penerapan Metode PPDIOO dalam Pengembangan LAN dan WLAN*. Palembang:Jurnal TEKNOMATIKA. Vol 07, No.01:65-73