e-ISSN: 2549-7952
p-ISSN: 2580-3336

OPTIMALISASI SISTEM KEAMANAN JARINGAN WIRELESS MENGGUNAKAN FIREWALL FILTERING MAC ADDRESS DI CV. MULTI KARYA

Muhammad Dhiqfan Ranca Putra[1], Mochammad Alfan Rosid[2]
[1,2] Teknik Informatika, Fakultas Sains Dan Teknologi, Universitas Muhammadiyah Sidoarjo
E-mail: [1]*dhiqfanrancaputra@gmail.com*, [2]alfanrosid@umsida.ac.id,

Abstrak – *Jaringan keamanan WLAN merupakan hasil dalam suatu bentuk pengelola jaringan maupun Network administrator agar dapat menegatahui tingkat keamanan dalam sebuah jaringan yang tersedia.. Tujuan Penelitian mengoptimalisasi system jaringan yang berfungsi untuk mendeteksi mac address filtering untuk meminimalisir serangan attacker yang berbahaya maupun dari wireless attack lainnya dengan metode ini dapat membantu sebuah administrator jaringan di instansi maupun organisasi tertentu sehingga mempunyai wadah dalam menanggulangi serangan – serangan cyber dari segi jaringan WLAN maupun jaringan kabel.*. Hasil Penelitian yang dimana Sistem Keamanan jaringan wireles menggunakan filtering Mac Address mampu memblock terhadap attacker menggunakan suatu keamanan pada router dimana dengan ini user yang ingin masuk kedalam Jaringan Wireless selalu terdeteksi keamanan nya. *Sistem keamanan jaringan ini memiliki verifikasi hak akses 2 (kali) dengan menyesuaikan username dan password didalam hotspot lohin dengan physical address dari user tersebut, jadi setiap client yang ingin terhubung ke jaringan internet ini haruslah menggunakan perangkat yang telah didaftarkan Mac Address nya dan sesuai dengan hak akses dan password yang ada di dalam Hotspot login*

Kata Kunci — Jaringan,Sistem Keamanan, WLAN

1. PENDAHULUAN

Jaringan keamanan WLAN merupakan hal yang perlu diketahui oleh pengelola jaringan maupun Network administrator agar dapat menegatahui tingkat keamanan dalam sebuah jaringan yang tersedia. Di gresik kecamatan driyorejo merupakan salah satu daerah yang berlingkup pada instansi perusahaan besar dengan infrastruktur IT yang mempuni jaringan computer di daerah tersebut sudah menerapkan jaringan nirkabel maupun WLAN sebagai media pertukaran data/informasi sebagai sarana dan prasarana yang dibutuhkan oleh masing masing instansi perusahaan di samping itu rentan keamanan jaringan mereka yang terganggu dengan adanya ancaman serangan karena gelombang radio [6]

Menurut Abdul Kadir dalam bukunya(jaringan computer pada tahun (2003) Jaringan Komputer ialah suatu hubungan dua simpul atau beberapa computer atau lebih yang tujuan utamanya yaitu untuk melakukan pertukarab data, dimana masing – masing terhubung melalui media komunikasi dimana media komunikasi ini dapat menghubungkan komouter tidam hanya melalui nirkabel tembaga saja tetapi dapat melalui fiber optic,gelombang radio,infared, maupun satelit kecepatan dalam transfer data dari suatu jaringan dan di dalam kecepatan transfer data mempunyai bandwith satuan yang dimiliki bandwith ini dapat berupa bit per-detik maupun byte per-detik satu byte nya terdiri dari 8 bit data sedangkan 1 kilobyte data terdiri dari 1024 byte perdata.Didukung oleh penelitian [1] pada penelitian yang berjudul "Pengembangan Sistem Pengamanan Jaringan Komputer berdasarkan Analisis Forensic Jaringan" pada penelitian ini dilakukan bertujuan untuk mendeteksi serangan ataupun gangguan dari attacker serta menginvestigasi aktivitas yang dilakukan oleh attacker, alamat ip dari attacker yang masuk ke sebuah port maupun packet data otomatis terdeteksi dalam proses investigasi menggunakan MTI UAD dalam proses investigasi ini perangkat mikrotik dapat

e-ISSN: 2549-7952
p-ISSN: 2580-3336

mendeteksi alamat ip maupun mac attacker yang tidak dikenal masuk kedalam halaman login mikrotik dan proses serangan yang dilakukan dalam investigasi yakni tools MTI UAD serta terbantu nya fitur firewall yang tersedia di mikrotik dapat mencegah serangan terlalu dalam.

Keamanan Jaringan WLAN ada beberapa gangguan ancaman virus yang biasanya sering terjadi yaitu mulai dari masuk nya packet packet data yang ilegal bisa jadi Mac Address ataupun IP Address yang ilegal masuk kedalam jaringan dengan cara menggunakan celah yang terbuka dalam jaringan sebuah intansi atau sebuah organisasi tertentu oleh sebab itu demi terjaganya informasi/data yang bersifat privasi atau orang – orang tertentu yang hanya boleh mengakses data tersebut harus diberikan wadah keamanan jaringan WLAN yang kuat sehingga tidak terjadi kecolongan data ataupun kerusakan data/informasi yang bersifat privasi.

Hal ini dikarenakan serangan yang terjadi menjadi lebih otomatis dan memberikan penyebab jumlah penebakan password, mengetahui password wifi yang sangat besar dan eksploitasi pengetahuan rentan kernetanan dari menonaktifkan audit, pencurian sampai dari pembajakan pada suatu network maupun data/informasi untuk virus yang sering terjadi mulai dari tahun 2000 an yaitu DOS Deniel Of Service sampai berkembang hingga saat ini menjadi DDOS Distributed Deniel of service dan enkripsi biner, sementara pengetahuan mengenai pengetahuan penyusupan semakin menurun [6]. Pada penelitian [6] Penelitian yang berjudul "keamanan jaringan wlan terhadap serangan Wireless Hacking Pada Dinas Komunikasi & Informatika DIY". Penelitian ini dilakukan bertujuan untuk mendeteksi dari serangan attacker yang berbahaya yang nantinya akan menghambat kinerja jaringan dikarenakan rentan serangan dari gelombang radio dan progress yang dilakukan pada penilitian ini yakni menguji serta menginvestigasi serangan dari attacker menggunakan tools netstumber,insider,ettercap tools ini yang nantinya dapat mencegah serangan dari attacker.

CV. Multi Karya merupakan perusahaan dimana dalam operasional nya penggunaan jaringan melalui jaringan via Wlan salah satu proses terselesai nya suatu pekerjaan di perusahaan ini apalagi dengan persaingan Teknologi industry yang semakin hari semakin pesat dalam hal ini permasalahan yang sering terjadi pada CV. Multi Karya adalah rata – rata dari segi terbobol nya password maupun packet data yang masuk melalui celah yang terbuka dari keamanan jaringan dengan itu attacker akan memulai sebuah modifikasi sebuah data maupun merusak data di dalam sebuah perangkat IT dan permasalahan yang sering terjadi yakni Virus Ransomeware dan sejenisnya apalagi yang sering dimodifikasi data itu adalah data data penting pada CV. Multi Karya [3]

Penggunaan dalam jaringan yang dipakai oleh berbagai instansi perusahaan adalah jaringan nirkabel dan dalam sebuah jaringan internet tersebut bukan berarti pengguna aman dari berbagai ancaman virus maupun hacker yang bias mengeksploitasi data peting dari suatu instansi,menyadap data password dan data penggunanya, maka dalam mengimplementasikan jaringan internet bersifat wireless harus memiliki rancangan dengan teliti agar bias meminimalisir segala jenis serangan yang dilakukan dari pihak – pihak yang tidak bertanggung jawab untuk dapat melindungi user.

Pola keamanan jaringan yang sudah banyak diketahui dengan itu akan menjadi masalah tentu nya pada pihak administrator oleh sebab itu Dalam mengatasi permasalahan di perusahaan CV.Multi Karya ulasan yang akan di lakukan dalam penelitian ini yakni menguji keamanan jaringan serta pengembangan dengan metode keamanan jaringan forensic untuk mekanisme dalam menangani kejadian ini dengan memanfaatkan aktivitas lalu lintas data dengan investigasi yang terjadi oleh sebab itu sebuah penyimpanan dapat dilihat dari investigasi yang lakukan dari metode jaringan forensic itu sendiri peristiwa ini tentunya sudah tersimpan dalam file log system, dengan itu berbagai proses dalam

e-ISSN: 2549-7952
p-ISSN: 2580-3336

menjalankan forensic jaringan seperti, monitoring, koleksi data maupun analisa data source tracebak yang akan menjadikan kemanan itu agar dapat membantu meminimalisir administrator jaringan dari serangan attacker[6].

Salah satu metode yang dilakukan dalam penelitian ini adalah mengimplementasi serta mengoptimalkan keamanan jaringan WLAN menggunakan firewall filtering mac address yang tersedia, tipe keamanan yang digunakan yaitu mikrotik router serta router yang digunakan oleh instansi perusahaan.

Menurut David icove, melihat dari lubang sebuah keamana yang ada pada suatu system keamanan dapat diklarifikasikan menjadi berbagai macam salah satu nya firewall, merupakan Keamanan Jaringan Firewall merupakan fitur keamanan yang ada di dalam sebuah jaringan dimana aktifitas keseluruhan bisa diatur oleh firewall itu sendiri, jaringan firewall ini merupakan bentuk antisipasi dari bentuk peretasan system maupun aktivitas yang bisa dimanipulasi yang biasa disebut attacker yakni seorang peretas system ada beberaapa tahap dalam memberikan keamanan jaringan maupun system gunanya agar aktivitas yang sedang berjalan tidak dapat diganggu oleh virus maupun serangan – serangan yang merugikan suatu organisasi tahapan yang sering digunakan yakni keamanan pada (physical security), keamanan dat dan media,keamanan dari pihak luar, keamanan dalam operasi dimana tahapan itu adalah bentuk dari penyerangan oleh attacker.

Mikrotik Router ini sudah memiliki teknologi keamanan firewall yang kuat sehingga mikrotik router juga bisa dijadikan sebagai security keamnan pada jaringan kabel maupun nirkabel karena dengan fitur ini jika ada sebuah alamat ip maupun mac address yang tidak dikenal bisa langsung di block dalam konfigurasi firewall yang ada pada mikrotik ini manfaat dari keamanan yang ada pada mikrotik ini sangat membantu bagi security analis maupun administrator jaringan yang mengelola jaringan maupun keamanan jaringan dalam segi perangkat mikrotik router ini memiliki perangkat dari segi router hingga hub/switch mikrotik router sudah menyediakan dengan berbagai tipe dan fitur yang berbeda – beda dan mikrotik router juga sudah menyediakan HTB untuk pengelolaan jaringan fiber optic [7].

Harapan dalam pengujian serta Implemenetasi keamanan jaringan wireless dari serangan wireless attack di CV. Multi Karya ini bisa membantu kepada pihak administrator jaringan di perusahaan CV. Multi Karya dari serangan yang berbahaya termasuk serangan DDOS maupun serangan yang berbahaya lainnya serta menghindari dari kebocoran data maupun rusaknya data dengan penelitian ini dapat membantu pihak perusahaan dari kerugian yang besar atas serangan yang dilakukan oleh attacker.

2. METODE PENELITIAN

Dalam memimpin eksplorasi ini, jenis pemeriksaan yang digunakan adalah pemeriksaan kuantitatif dengan strategi uji coba. Jenis pengujian ini dipilih karena pembuatnya percaya bahwa jenis ini benar-benar masuk akal dengan penelitian yang diajukan oleh pembuatnya karena memainkan strategi untuk meningkatkan sistem keamanan organisasi jarak jauh dan mengarahkan penelitian pada peningkatan firewall penyaringan macintosh. alamat.

Strategi pengumpulan informasi adalah persepsi, wawancara, studi penulisan dari berbagai sumber, misalnya buku harian, buku, laporan, dan lain-lain yang terkait dengan eksplorasi ini. Sumber informasi yang dilakukan dalam eksplorasi ini adalah memanfaatkan Library Research yang merupakan suatu pendekatan untuk mengumpulkan informasi dari beberapa buku, diari, proposal, postulat, dan tulisan lainnya yang dapat dimanfaatkan sebagai sumber perspektif pembicaraan dalam masalah ini.

Mengenali kebutuhan ujian Merupakan tahapan dalam membuat pengaturan yang harus dipenuhi agar suatu siklus ujian dapat berjalan, baik sebagai kebutuhan perlengkapan (equipment) maupun kebutuhan pemrograman (programming), sebagai media untuk membantu

e-ISSN: 2549-7952
p-ISSN: 2580-3336

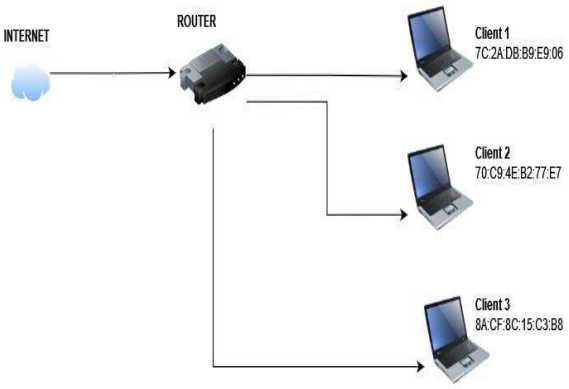
siklus ujian agar berjalan dengan baik. create dan testing dipartisi menjadi beberapa bagian, antara lain:

1. Media Penghubung
a. Kabel LAN Cat 5
b. Conector RJ45
2. Perangkat Hardware
a. Mikrotik OS RB 951 UI-2HND
b. Modem ISP
3. Laptop HP dengan spesifikasi:
a. Prosesor intel® Core™ i5-10210U - @ 1.60GHz (8 CPUs), ~2.1GHz
b. Memory 8Gb
c. Hard Disk 1000 Gb

3. HASIL DAN PEMBAHASAN

3.1 Hasil

Dalam pengujian serta implementasi dari Optimalisasi Keamanan Jaringan wireless menggunakan Filtering Mac Address dalam penelitian ini penulis menggunakan skema jaringan yang sudah terlihat pada gambar 4.1 dengan IP Address yang sudah tertera pada sebuah Tabel 1.



Gambar 1. Skema Jaringan

Gambar 1 diatas merupakan gambaran jaringan yang akan dilakukan dalam penelitian ini, client 1 menggunakan Mac Address 7C:2A:DB:B9:E9:06, sedangkan client 2 mengguanakan MAC Address 70:C9:4E:B2:77:E7, dan client 3 pun juga mengguanakan MAC Address 8A:CF:8C:15:C3:B8, dimana nantinya setiap masing masing client mendapatkan hak akses kedalam jaringan melakukan verifikasi didalam hotspot login dengan meggunakan akses user dan password yang berbeda diantara client.

Tabel 1. List Alamat IP Dan Mac Address

NO	Interface	IP Address	Network
1.	Ether 1 (to ISP)	192.168.100.2	192.168.100.0
2.	Ether 2 (to Local)	192.168.10.1	192.168.10.0
3.	Wlan 1 (to Local)	192.168.20.1	192.168.20.0
4.	Client 1	DHCP Client	192.168.20.0
5.	Client 2	DHCP Client	192.168.20.0
6.	Client 3	DHCP Client	192.168.20.0

Pada Tabel 1 terdapat Interface Ether 1 yaitu dengan alamat IP Address 192.168.100.2, digunakan sebagai IP Address yang akan terhubung ke Alamat IP ISP, sedangkan interface ether 2 dengan alamat IP Address 192.168.10.1, digunakan sebagai gateway untuk jaringan lokal yang nantinya akan terhubung menggunakan media kabel LAN serta interface Wlan1 dengan Alamat IP Address 192.168.20.1, digunakan sebagai gateway pada jaringan lokal wireless.

Tabel 2. Hak Akses User

NO	MAC Address	User	Password
1.	7C:2A:DB:B9:E9:06	Owner	Owner 1
2.	70:C9:4E:B2:77:E7	Manager	Manager 2
3.	8A:CF:8C:15:C3:B8	Administrasi	Administrasi 3

Dalam tabel 2 merupakan sebuah hak akses untuk client untuk melakukan koneksi kedalam jaringan wireless. Untuk hak akses User Owner, dengan password Owner1 dimana nantinya hanya dapat dilakukan oleh client dengan MAC Address 7C:2A:DB:B9:E9:06, saja dan User Manager, dengan Password Manager2, hanya dapat digunakan untuk client dengan MAC Address 70:C9:4E:B2:77:E7, saja dengan ini dapat terlihat bahwa terdapat 2 model konsep

e-ISSN: 2549-7952
p-ISSN: 2580-3336

pengujian untuk melakukan hal optimalisasi keamanan wireless menggunakan filtering MAC Address dimana nantinya. Skenario pertama semua akses client dapat mengakses kedalam jaringan dengan menggunakan user dan password untuk skenario pengujian kedua yaitu menggunakan pembatasan akses berdasarkan user, password dan MAC address nya

3.2 Pembahasan

Untuk melakukan pengujian dalam tahap ini harus melakukan penginstalan software winbox untuk router mikrotik dimana konfigurasi alamat IP serta MAC Address ada didalam software ini serta pengujian jaringan ini nanti akan dilakuakn menggunakan software ini.

Setelah melakukan perancangan dan pengujian terhadap sistem meliputi koneksi sistem / alat dengan aplikasi blynk maka selanjutnya yang harus dilakukan adalah mengimplementasikan aplikasi blynk.

Implementasi koneksi dan keamanan jaringan

Implementasi ini merupakan langkah – langkah terhubung nya koneksi jaringan dalam segi perangkat router maupun dari router internet (ISP) dalam sebuah koneksi ini media kabel juga mempunyai hak akses port yang terhubung ke router Mikrotik. Langka-langka Implementasi koneksi dan keamanan jaringan dalam segi perangkat sebagai berikut yang dimana hal pertama Implementasi pertama yaitu koneksi pada port 2 di router isp terhubung ke Router mikrotik Sebagai koneksi internet pada router mikrotik setalah Implementasi kedua yaitu port 1 (Ether 1) pada mikrotik media kabel yang terhubung ke router isp sebagai media koneksi internet pada router Mikrotik

Gambar 2. Implementasi Koneksi Router ISP

Percakapan pemeriksaan dan hasil eksperimen yang didapat disajikan sebagai penggambaran hipotetis, baik secara subjektif maupun kuantitatif. Hasil percobaan harus ditampilkan sebagai grafik atau tabel. Untuk grafik bisa mengikuti konfigurasi untuk outline dan gambar.

Dalam pengujian jaringan rencana 1, pengujian ini akan memimpin pengujian dalam fase asosiasi keamanan jarak jauh dengan menggunakan kebebasan akses Login Hotspot. Harus terlihat pada Gambar 4.6 ADALAH Hotspot PENGGUNA yang terkait dengan organisasi jarak jauh. Dimana terdapat 3 (tiga) klien yang mendapatkan hak akses masuk dari setiap klien untuk berinteraksi dengan jaringan login remote area of interest.

Dengan pelaksanaan keamanan organisasi jarak jauh dengan menggunakan keamanan organisasi jarak jauh menggunakan login area of interest, dapat membatasi administrasi klien dalam melihat klien dan frase rahasia yang telah diberikan oleh ketua organisasi dalam organisasi ini. Namun keamanan jaringan yang melibatkan model login area of interest masih mengalami kelemahan seperti yang ditampilkan pada Gambar 4.7, ada client yang menggunakan MAC Address 7C:2A:DB:B9:E9:06 siap untuk login menggunakan client Owner dan Manager, Alamat MAC mana yang harus digunakan. oleh klien Administrasi.

Pada tabel 3 diberikan penjelasan terdapat sebuah celah keamanan dari iplemenetasi keamanan jaringan wireless yang hanya menggunakan hotspot login. Dalam artian client tersebut dapat menggunakan user dan user dan password client lain untuk melakukan konektifitas kedalam jaringan Wi-Fi. Dijelaskan pada tabel 3, client 1 dengan MAC Address 7C:2A:DB:B9:E9:06 mampu melakukan Login baik menggunakan user Owner, Manager dan Administrasi sedangkan client 2 dengan MAC Address 70:C9:4E:B2:77:E7 pun mampu melakukan hal yang sama untuk login dengan user Owner, Manager dan Administrasi serta

e-ISSN: 2549-7952
p-ISSN: 2580-3336

client 3 menggunakan MAC Address 8A:CF:8C:15:C3:B8 yang seharusnya digunakan untuk user Administrator dapat melakukan konektifitas kedalam jaringan wireless menggunaan user Owner serta user Manager

Tabel 3. Security Hotspot Login.

NO	MAC Address	User	Password	konektifitas
1.	7C:2A:DB:B9:E9:06	Owner	Owner 1	OK
		Manager	Manager 2	OK
		Administrasi	Administrasi 3	OK
2.	70:C9:4E:B2:77:E7	Owner	Owner 1	OK
		Manager	Manager 2	OK
		Administrasi	Administrasi 3	OK
3.	8A:CF:8C:15:C3:B8	Owner	Owner 1	OK
		Manager	Manager 2	OK
		Administrasi	Administrasi 3	OK

Celah keamanan yang terdapat didalama hotspot login dapat dimanfaatkan oleh client yang tidak mempunyai akses untuk mengganggu kestabilan infrastruktur sebuah jaringan bahkan sampai keamanan privasi client yang sedang digunakan dengan hak aksesnya.

Dalam pengujian skema yang ke 2 pada penelitian yang dilakukan yaitu pengujian dalam segi keamanan jaringan wireless dimana dalam memfilter mac address pengguna dimana pada tahapan ini bisa mengurangi terjadinya serangan wireless attack karena banyak sekali mac address yang tidak di kenal masuk aabila tidak di filter menggunakan login user password 3 akses di dalam perusahaan CV. Multi Karya yaitu user Owner, manager, Administrasi dimana setiap masing masing mac address memiliki hak akases user login password untuk memfilter mac address yang masuk.

hak akses hotsopot login dari beberapa user yang sudah disediakan oleh adminstrator antara Owner, Manager, Administrator diamana jika dilakukan hak akses oleh user tersebut dapat terkoneksi kealam jaringan begitupun sebaliknya apabila yang mengakses tidak mempunyai hak akses tidak bisa mengakses jaringan dan dalam keamanan ini mengantisipasi serta meminimalisir attacker untuk mengakses karena setiap user yang terhubung akan melalui lalu lintas data dengan fitur filetring mac address.

Sebuah percobaan akses user dimana terdapat user yang mengakses dan terhubung kedalam jaringan sementara ada juga yang mengakses berbeda mac address dan tidak dapat terhubung dikarenakan tidak sesuai dengan Mac Address yang ada di halaman login hotspot dimana Mac Address yang dapat terhubung yaitu MAC Address User Owner, Manager, Administrator selain itu tidak dapat diakses karena semua itu melalui lalu lintas data yang ada di fitur firewall.

Tabel 4. Uji Koenektifitas Jaringan

Mac Address	User	Password	Konektifitas	
			Sebelum	Sesudah
7C:2A:DB:B9:E9:06	Owner	Owner	OK	OK
	Manager	Manager	OK	Block
	Administrasi	Administrasi	OK	Block
70:C9:4E:B2:77:E7	Owner	Owner	OK	Block
	Manager	Manager	OK	OK
	Administrasi	Administrasi	OK	Block
8A:CF:8C:15:C3:B8	Owner	Owner	OK	Block
	Manager	Manager	OK	Block
	Administrasi	Administrasi	OK	OK

Tabel 4 diatas merupakan pengujian Konektifitas jaringan Wireless menggunakan filtering Mac Address. Jika sebelumnya, client dapat memgakses user dan password siapapun. Ketika mengimplementasikan filtering Mac Address, user Owner hanya dapat digunakan oleh perangkat dengan Mac Address 7C:2A:DB:B9:E9:06 saja, dan user Manager Hanya dapat diakses oleh perangkat dengan Mac Address 70:C9:4E:B2:77:E7 saja, oleh sebab itu bisa meminimalisir user yang tidak dikenal dapat masuk kedalam jaringan wireless di CV. Multi Karya

e-ISSN: 2549-7952
p-ISSN: 2580-3336

4. SIMPULAN

Kesimpulan dari pembahasan dari Optimalisasi Sistem Keamanan jaringan wireless menggunakan Filtering Mac Address di CV. Multi Karya Yaitu :

1. Sistem Keamanan jaringan wireles menggunakan filtering Mac Address mampu memblock terhadap attacker atau user yang ingin masuk kedalam Jaringan Wireless.
2. Sistem Keamanan jaringan ini memiliki model keamanan jaringan wireless ini menggunakan model berlapis dengan adanya hotspot halaman login dan kombinasi filtering Mac Address dapat mengoptimalkan baik infrastruktur jaringan dalam skala perusahaan maupun skala pribadi dengan itu user dapat menggunakan layanan jaringan dengan efisien dan nyaman.
3. Penelitian ini merupakan pengembangan dari penelitian sebelumnnyadimana masih menggunakan Konsep jaringan dalam lingkup yang kecil dan versi router yang masih lama
4. Sistem keamanan jaringan ini memiliki verifikasi hak akses 2 (kali) dengan menyesuaikan username dan password didalam hotspot lohin dengan physical address dari user tersebut, jadi setiap client yang ingin terhubung e jaringan internet ini haruslah menggunakan perangkat yang telah didaftarkan Mac Address nya dan sesuai dengan ham akses dan password yang ada di dalam Hotspot login.

5. SARAN

Adapun dari penyusun skripsi diharapkan penelitian berikutnya dapat melakukan pengembangan selanjutnya sehingga penelitian ini bisa sempurna dan aman dalam peretasan dengan melakukan beberapa proses pengujian lainnya diantaranya :

1. Teknik analisa permasalahan terkait attacker yang mencoba masuk kedalam jaringan bertujuan untuk mengidentifikasi seberapa dalam percobaan attacker dalam mengontrol aktivitas jaringan melakukan perubahan atau smapai merusak jika teknik itu sudah dilakukan maka harus memalui tahapan Block akses menggunakan Mac Address Dan Alamat IP.
2. Melakukan keamanan jaringan lainnya dengan menggunakan metode metode terbaru agar dalam suatu jaringan dapat dikontrol oleh administrator dimana administrator akan selalu memonitoring jalur lalu lintas jaringan termasuk hak akses dan lain - lain
3. Membuat konsep terbaru dengan berbagai segmen jaringan dalam segi alamat ip dan Mac Address perangkat yang di gunakan serta teknologi dalam perangkat jaringan sudah diwadahi dengan keamanan yang layak untuk digunakan karena dengan itu jaringan dapat berjalan dengan baik dan normal

DAFTAR PUSTAKA

[1] Abdul Fadlil, Imam Riadi, & Sukma Aji. (2017). Analisis Jaringan Forensik. Pengembangan Sistem Pengamanan Jaringan Komputer berdasarkan Forensik Jaringan, 12-13.

[2] Faidzin Ridho,dkk. (2016). Analisis forensik router. Analisis forensik router mendeteksi serangan DDOS secara real time, 111-112.

[3] Firmansyah,Rusydi Umar,dkk. (2021). Identifikasi forensik jaringan. Identifikasi Bukti Forensik Jaringan Virtual Router Menggunakan Metode NIST, 91-98.

[4] Gilvan januar sirait. (2018). keamanan jaringan wireless. analisis keamanan jaringan wireless LAN Menggunakan metode Extended Acess List, 3-5.

e-ISSN: 2549-7952
p-ISSN: 2580-3336

[5] Joko Dwi Santoso. (2016). Keamanan jaringan nirkabel. Keamanan Jaringan Menggunakan wireless Intrusion Detection System, 44-50.

[6] Mochammad Gilang Ari wibowo,dkk. (2016). keamanan jaringan wireless. keamanan jaringan wireless dari serangan wlan, 2-3.

[7] Tashia. (2017). Keamanan Jaringan Internet dan Firewall. Dirjen Aplikasi Informatika Kemkominfo Republik Indonesia.