ISSN: 2503-054X
Vol. 7 No: 1, April 2022

Proteksi Akses Jaringan WIFI berbasis MAC Address (Studi Kasus : Jaringan WIFI Indihome)

Wahyudi
STMIK Horizon Karawang, Sistem Informasi
Jl. Pangkal Perjuangan Km.1, Karawang Barat, Jawa Barat
wahyudi008@gmail.com

Abstract - Perkembangan teknologi jaringan khusus jaringan yang berbasis wireless begitu pesat, terutama terkait dengan teknologi perangkat jaringan itu sendiri . Interkoneksi yang begitu komplek menuntut setiap perangkat WIFI memiliki kemampuan untuk memproteksi agar hanya pengguna yang memiliki otorisasi yang dapat terkoneksi keperangkat WIFI tersebut , salah satu fitur keamanan akses jaringan WIFI yang saat ini ada adalah dengan menggunakan MAC Address. Keamanan akses pada jaringan WIFI sangat diperlukan untuk menghindar terjadi pengaksesan internet oleh pihak yang tidak memiliki otorisasi, untuk menghindari penyalahgunaan itu maka diperlukan proteksi terhadap jaringan yang dimiliki. Dengan melakukan *mac address filtering* diharapkan hanya perangkat yang terdaftar saja yang hanya dapat terhubung ke perangkat WIFI tersebut.

Kata Kunci : Koneksi Jaringan, WIFI, Keamanan Jaringan, MAC Address.

I. PENDAHULUAN

Seiring dengan perkembangan teknologi informasi, kebutuhan koneksi setiap tahunnya terus meningkat hal tersebut terlihat dari data yang dikeluarkan oleh Asosiasi Penyelengggara Jasa Internet Indonesia yang menunjukan kenaikan pengguna internet tiap tahunnya.

PT. Telekomunikasi Indonesia (Telkom) selaku perusahaan yang penyedia jasa telekomunikasi dengan nama produknya indihome (Indonesia Digital Home), yang tersebar hampir diseluruh Indonesia. PT. TELKOM dalam produk indihome nya menyediakan tiga layanan langsung dengan koneksi menggunakan Fiber Optic, yaitu Internet (*Internet on Fiber* atau *High Speed Internet*) , layanan televisi interaktif (IPTV) dan Telepon rumah digital (VoIP).[5]

Permasalahan yang sering kali terjadi pada jaringan WIFI adalah aspek keamanan. Cakupan area WIFI dapat dijangkau sampai keluar rumah yang memungkinkan pengguna lain pun dapat pula mengaksesnya, yang dapat memungkinkan penurunan performansi akses ke internet. Ada beberapa cara pencegahan yang dapat dilakukan salah satunya adalah melakukan proses *filtering MAC Address* dengan cara melakukan pendataan terhadap perangkat untuk didaftarkan pada perangkat WIFI Indihome. Sehingga setiap mac address yang terdaftar diperangkat WIFI dapat diberikan wewenang untuk dapat terkoneksi keperangkat WIFI indihome atau tidak.

II. TINJAUAN PUSTAKA

II.1. WLAN

Wireless Local Area Networks menggunakan infrared atau gelombang radio yang menyediakan koneksi jaringan untuk perangkat wireless dan mengijinkan pengguna untuk mengirim data satu dengan yang lainnya dalam area yang terjangkau tanpa terkendala dengan kabel. WLANs memiliki perbedaan protocol seperti IEEE802.11, *Bluetooth, HomeRF* dan *HiperLAN*. Banyak perangkat *wireless* mendukung

ISSN: 2503-054X
Vol. 7 No: 1, April 2022

WLAN termasuk *mobile phones, game consoles*, beberapa kamera, *tablets* dan juga *GPS system*. WLAN berisikan dua perangkat atau lebih hingga ratusan . [1]

II.2. Standar WLAN

Jaringan *wireless* adalah sistem komunikasi data yang fleksibel yang menggunakan teknologi *infrared* atau frekuensi radio untuk mengirim dan menerima informasi melalui udara. Tahun 1997, IEEE 802.11 mengimplementasikan WLAN untuk pertama kalinya menggunakan teknologi radio [7]. Sampai hari ini standard WLAN telah berkembang seperti table berikut ini : [1]

Standard	Data rate	Frequency	Modulation	Range	Date of Release
802.11.a	54 MBps	5 GHz	OFDM	35-120 m	Sep 1999
802.11.b	11 MBps	2.4 GHz	DSSS	35-120 m	Sep 1999
802.11.g	54 MBps	2.4 GHz	OFDM, DSSS	35-120 m	Jun 2003
802.11.n	150 MBps	2.4 – 5 GHz	OFDM	35-120 m	Oct 2009
802.11.ac	867 MBps	5 GHz	OFDM	35 - .. m	Dec 2013
802.11 ax	2,2 GBps	2.4/5/6	MIMO-OFDM	30-120 m	Sept 2019

Tabel 1. Standard WLAN

II.3. Komponen WLAN

Ada dua komponen dasar dari WLAN : [6] [7]

1. *Access Point*
   Hub dari jaringan area local nirkaberl (AP) membantu dalam pertukaran informasi dengan perangkat nirkabel lainnya melalui antenna. Dengan menggunakan teknik modulasi 802.11 dengan spectrum frekuensi tertentu.
2. *Network Interface Cards / Client Adapters*
   NIC memindai spectrum frekuensi yang tersedia untuk konektivitas dan menghubungkannya ke titik akses atau klien nirkabel lain.

Gambar 1. Komponen WLAN

II.4 Keuntungan dari Wireless Local Area Networks

Wireless Local Area Network memiliki beberapa keuntungan. Pertama, *wireless local area network* lebih *flexible* dan *mobile* dibandingkan dengan kabel dan WLAN tidak terbatasi oleh kabel. Pengguna memiliki akses ke atau menerima informasi dalam area yang terjangkau secara real time. Kedua, WLAN memiliki scalabilitas yang bagus. Pengguna dapat menambahkan lebih banyak Access Point (AP) untuk memperluas jaringan secara efektif untuk memenuhi kebutuhan aplikasi dan instalasi

tertentu. Ketiga, WLANs tidak membutuhkan kabel, ini akan mengurangi beban dari jaringan kabel. Terakhir adalah WLAN lebih mudah di-*setup* dibandingan dengan kabel dan tidak mudah terpengaruh oleh bencana alam [4].

II.5 Kekurangan Wireless Local Area Networks

Ada beberapa kekurangan dari WLANs. Pertama, WLAN bekerja berdasarkan frekuensi radio untuk melakukan transmisi data. Dinding dan gedung akan memcegah transmisi dari frekuensi radio, mengurangi signal dan mengganggu kelancaran performansi dari WLAN. Kedua, beberapa perangkat WLAN memiliki frekuensi yang sama yaitu seri 802.11 dan mengakibatkan terjadinya interferensi / gangguan gelombang radio. Ketiga, Wireless LAN kurang aman dibandingkan dengan LAN berbasis kabel. Ketika sebuah jaringan melalui udara, ini dapat menyebabkan terjadinya *intercepted*/pencegahan pesan dalam waktu yang bersamaan. Keempat, jangkauan area WLAN terbatas, dengan meningkatnya area jangkauan yang dibutuhkan akan menambah biaya yang lebih besar. [4].

II.6 Media Transmisi Wireless LAN

Ada beberapa jenis media transmisi yang terdapat pada *Wireless* LAN, Jenis media transmisi nirkabel yang digunakan dalam komunikasi adalah .[4]

- *Infrared*
- *Broadcast Radio*
- *Cellular Radio*
- *Microwave*
- *Communication Satellite*

II.7 Ancaman WLAN

Sebuah serangan adalah suatu tindakan yang dilakukan oleh penyusup untuk mengkompromikan informasi dalam suatu organisasi. Tidak seperti jaringan kabel, WLAN menggunakan teknologi transmisi frekuensi radio atau inframerah untuk komunikasi, yang membuat WLAN rentan terhadap serangan. Serangan-serangan ini bertujuan untuk mencuri kerahasian dan integritas informasi dan ketersediaan jaringan. [2]

Serangan diklasifikasikan menjadi dua :

- Serangan pasif
- Serangan aktif

Serangan pasif adalah tipe serangan dimana penyerangan berusaha untuk mencoba memperoleh informasi pada saat mengirim dan menerima pada sebuah jaringan. Jenis serangan ini sulit untuk di deteksi karena tidak ada perubahan isi dari informasi yang dilakukan oleh penyerang.[2]. Ada dua tipe dari serangan pasif, ada analisis traffik dan *eaves dropping*.

Serangan aktif adalah tipe serangan dimana penyerang tidak hanya memperoleh informasi dalam jaringan tetapi juga merubah isi dari informasi atau memberikan informasi yang tidak benar dalam jariangan. Jenis serangan ini akan menimbulkan kerugian yang besar bagi organisasi [2]. Berikut merupakan jenis serangan aktif dalan teknologi WLAN :

- *Unauthorized Access*
- *Rogue Access Point*
- *Man in the Middle Attach (MITM)*
- *Denial-of-Service*
- *Reply Attach*
- *Session High Jackin*g

ISSN: 2503-054X
Vol. 7 No: 1, April 2022

Menurut *CIA triad* [3], keamanan informasi terdiri dari 3 aspek yaitu *Confidentiality, Integrity* dan *Availability*. Ketiga aspek tersebut diperlukan sampai pada tahap tertentu untuk mencapai keamanan yang sesungguhnya. Jika tidak jaringan akan rentan terhadap suatu serangan. Berikut adalah dua aspek lainya yaitu akses control dan otentikasi.

- *Confidentiality* adalah mencegah dari mengungkapkan data secara sengaja / tidak sengaja
- *Integrity* adalah mengendalikan perubahan data baik secara sengaja / tidak sengaja
- *Availability* adalah control atas penyediaan sumber daya system sesuai dengan permintaan untuk diotorisasi pengguna/system/proses.
- *Access Control* adalah control akses ke sumber daya oleh pengguna yang sah
- *Authenticatio*n adalah proses dimana system memverifikasi identitas pengguna yang ingin mengaksesnya [8].

Dari berbagai tipe serangan/ancaman WLAN yang telah dibahas diatas dan akan dilaksanakan pada penelitian ini adalah *Unauthorized Access* dengan menggunakan salah satu fitur AP Indihome yaitu *WIFI MAC Filtering.* Berikut beberapa fitur keamanan yang tersedia dalam *Access Point* Indihome (HG8245H5) :

1. *IPv4 Filtering*
2. *MAC Filtering*
3. *Wi-Fi MAC Filtering*
4. *Parent Control*
5. *Device Access Control*

III. METODOLOGI PENELITIAN

Seperti pada umumnya keamanan suatu jaringan memiliki siklus model tersendiri dimana langkah-langkah yang perlu dilakukan pada metodologi penelitian ini adalah : *IDENTIFY – ASSESS – PROTECT – MONITOR* [10] [11] seperti diperlihatkan gambar berikut dibawah ini.

Gambar 2. *Security Life Cycle*

III.1. *IDENTIFY*

Langkah pertama dalam membangun sebuah keamanan adalah mengetahui apa yang akan di proteksi. Yang dilakukan pada fase ini adalah melakukan pemetaan terhadap jaringan, mengidentifikasi perangkat dan memahami aplikasi apa saja yang sedang berjalan. Pada kasus ini adalah melindungi akses koneksi PC atau laptop ke perangkat *Access Point* untuk terhubung ke internet, cara kerjanya adalah dengan memastikan hanya komputer/PC yang *MAC Address* nya terdaftar di *Access Point* Indihome (HG8245H5) yang dapat terhubung ke internet.

III.2. *ASSESS*

Pada phase ini berupa identifikasi terhadap asset yang dilakukan melalui *security assessment* berupa *scanning* terhadap perangkat yang berpotensi dapat menimbulkan kelemahan terhadap sistem yang

ISSN: 2503-054X
Vol. 7 No: 1, April 2022

sedang berjalan. Langkah awal yang dilakukan pada phase ini adalah melakukan pembicaraan dengan teknikal yang menangani perangkat tersebut, seperti administrator sistem, administrator jaringan dan pengembang aplikasi. Cari informasi sebanyak mungkin terkait dengan konfigurasi dan topologi keamanan sistem yang ada, berupa :

- Aturan *password* dan *user account*
- *Review UserIDs* dan *Group*
- *Review of Administrator or Root Account*
- *Review* apa dan siapa saja yang dapat masuk dan akses terhadap *logs*.

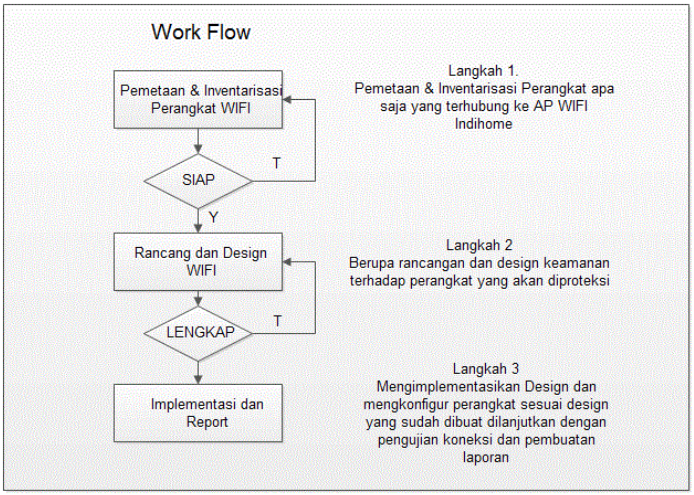
III.3. *PROTECT*

Berdasarkan pemetaan jaringan, sistem dan mengidentifikasi kelemahan sistem. fase berikutnya adalah melakukan perlindungan terhadap asset dengan tujuan mengurangi resiko yang mungkin terjadi. Yang dilakukan pada fase ini untuk memproteksi jaringan WIFI indihome adalah dengan mendaftarkan seluruh *MAC Address* PC/Komputer yang akan terhubung ke *Access Point* Indihome. Tujuan nya adalah hanya *MAC Address* PC/Komputer yang terdaftar di *Access Point* Indihome yang dapat terhubung atau ditolak untuk akses ke perangkat WIFI tersebut.

III.4. *MONITOR*

Fase terakhir ini adalah melakukan *monitoring* terhadap sesuatu yang telah dilakukan pada fase *protected* untuk memastikan bahwa setiap perubahan yang dilakukan untuk proses keamanan berjalan sesuai dengan yang diharapkan.

III.5. *WORKFLOW*



Gambar 3 : Work Flow

IV. HASIL DAN PEMBAHASAN

TOPOLOGI JARINGAN INDIHOME

Gambar 4. : Topologi Jaringan Indihome

KONFIGURASI PERANGKAT

Langkah-langkah proteksi di perangkat WIFI Indihome :

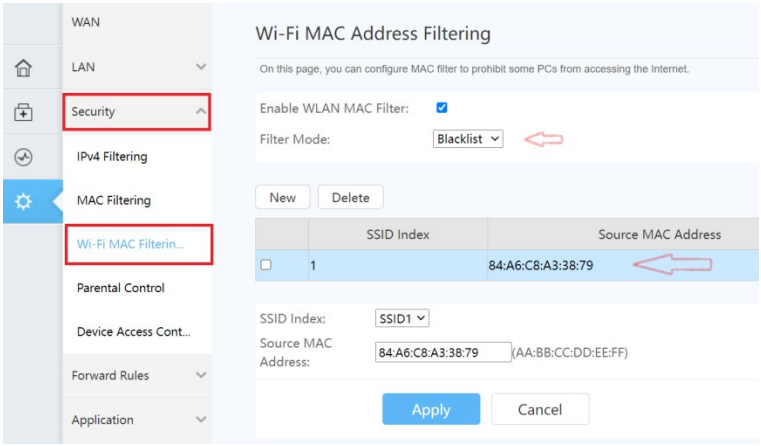
1. Login ke perangkat WIFI (HG8245H5)
2. Lakukan *list MAC Address* untuk mengetahui perangkat apa saja yang terhubung ke WIFI Indihome. (table 2)
3. Masukan Mac Address yang akan di *filter*/*blacklist* seperti Gambar 5
4. *Apply*
5. Test koneksi dari perangkat yang sudah di *filter Mac Address* nya

WIFI Devices			
No	Device Name	Port ID	Device Info
1	-	SSID1	[redacted].e3.45
2	XiaoMiRepeater	SSID1	[redacted]:93:04

ISSN: 2503-054X
Vol. 7 No: 1, April 2022

3	Galaxy-A7	SSID1	[redacted]:cc:e5
4	Galaxy-A30	SSID1	[redacted]:5e:8d
5	M2103K19G	SSID1	[redacted]:2f:28
6	-	SSID1	[redacted]:fb:50
7	Desktop-M177S6C	SSID1	84:a6:c8:a3:38:79

Table 2 : *List Mac Address WIFI Device*



Gambar 5 : *Setting WIFI Mac Filtering*

HASIL PENGETESAN SEBELUM DAN SESUDAH *MAC FILTERING*

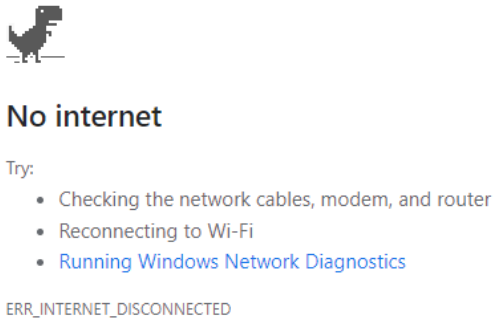
Filtering dilakukan pada perangkat yang memiliki *MAC Address* 84:A6:C8:A3:38:79 dimana pengetesan yang dilakukan dengan melakukan *browsing* ke alamat http://www.horizon.ac.id dengan hasil sebagai berikut :

Sebelum dilakukan *filtering wifi mac address* :

Gambar 6 : Web site STMIK/STIKES HORIZON

Hasil koneksi setelah dilakukan *filtering wifi mac address* :

ISSN: 2503-054X
Vol. 7 No: 1, April 2022



Gambar 7 : Koneksi Gagal

V. KESIMPULAN

KESIMPULAN :
Dari hasil pengetesan yang dilakukan sebelum dan sesudah *mac filtering* dengan *MAC Address* 84:A6:C8:A3:38:79 maka dapat disimpulkan bahwa proses *filtering* terhadap *MAC Address* tersebut berjalan dengan baik, hal tersebut dapat dilihat dari hasil pengujian yang terdapat pada gambar 6 dan 7.

SARAN :
Penggunaan *MAC Address* bukan merupakan satu-satunya yang dapat digunakan untuk memproteksi jaringan WIFI Indihome, banyak fitur lainnya yang tersedia pada perangkat *Access Point* Indihome seperti *filtering IP Address, parent control* dan *Access Control* yang dapat digunakan dan dikembangkan untuk melindungi jaringan WIFI yang dilakukan oleh pihak-pihak yang tidak memiliki hak akses kejaringan WIFI.

DAFTAR PUSTAKA

[1] Bradley, M. 2020. Wireless Standards 802.11a, 802.11b/g/n, and 802.11ac. WWW document. Available at: https://www.lifewire.com/wireless-standards802-11a-802-11b-g-n-and-802-11ac-816553 [Accessed Oct 10, 2021].
[2] B. Forouzan, Data Communications & Networking. 4th edition. New York: McGraw-Hill, 2008
[3] Chai Wesley., 2021, " Confidentiality, Integrity and availability (CIA triad) "WWW document. Available at : https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA., [Accessed Nov 12, 2021]
[4] Geeksforgeeks., Apr 2020. " Advantages and Disadvantages of Wireless Communication". WWW document Availabel at : "https://www.geeksforgeeks.org/advantages-and-disadvantages-of-wireless-communication/ [Accessed Nov 2021].
[5] Kompas.com – Juni 2021., "Daftar Harga Paket Internet Indihome". WWW document Available at : https://tekno.kompas.com/read/2021/06/06/12050097/daftar-harga-paket-internet-indihome-mulai-dari-rp-275000-per-bulan., [Accessed Dec 2021].
[6] P. Feng,Wireless LAN security issues and solutions,*IEEE Symposium on the Robotics and Applications (ISRA)*, 2012.
[7] R.A. Hamid, *Wireless LAN: Security Issues and Solutions* [Press release], 2003.
[8] Search Security, (2011) Information security tutorials [Online], Available at: http://searchsecurity.techtarget.com/tutorial/Informationsecurity-tutorials, [Accessed on: 14/11/2021].

ISSN: 2503-054X
Vol. 7 No: 1, April 2022

[9] Teaching Computer Network – Lesson 9 Wireless Transmission Media https://sites.google.com/site/pnutpck11/lesson-9---wireless-transmission-media diaskes 27 October 2021
[10] Global Information Assurance Certification Paper., Author Retains Full Right,. SANS Institute diakses 31 Oktober 2021
[11] The Information Security Lifecycle., 'Identify, Assess, Protect, and Monitoring .,' https://plextrac.com/the-information-security-lifecycle/ [Accessed on : 11/10/2021]