IMPLEMENTASI MAC ADDRESS REGISTER UNTUK MENGATASI PENGGUNA ANONIM DALAM JARINGAN

Pahala Bima Pramudya[1], Djuniadi[2]

[1]Universitas Negeri Semarang, Sekaran, Kec Gn. Pati Kota Semarang
[2]Universitas Negeri Semarang, Sekaran, Kec Gn. Pati Kota Semarang
Email: [1]pahala11@gmail.com, [2]djuniadi@mail.unnes.ac.id

Abstrak. Keamanan adalah faktor penting di era digital saat ini. Di zaman yang sangat modern dengan teknologi yang semakin terkoneksi ini memungkinkan kemunculan banyak metode serangan baru, terutama dalam hal rawan yaitu privasi data. Penerapan sistem keamanan dalam suatu jaringa merupakan fokus utama seorang *developer* jaringan dan administrator jaringan. Salah satu keamanan jaringan yang paling dasar adalah berupa hak akses dengan penerapan MAC *Adress Register* sebagai keamanan dasar yang dapat mencegah pengguna anonim mengakses sistem jaringan, dengan simulasi *Cisco Packet Tracer*. Hasil yang didapatkan dari simulasi adalah sistem yang mampu mencegah pengguna anonim untuk mengakses jaringan, dan mengizinkan pengguna dengan MAC *Address registered* untuk mengakses jaringan. Selanjutnya hasil simulasi bisa diterapkan pada jaringan sebagai keamanan dasar.

Kata kunci: *Keamanan Jaringan; MAC Address Register; Pengguna Anonim; Cisco Packet Tracer.*

1 Pendahuluan

Keamanan jaringan adalah sektor yang sangat penting pada zaman modern ini. Karena semakin banyak ancaman yang datang dalam jaringan, maka semakin kompleks pula suatu jaringan harus dibangun [1]. Serangan (Gangguan) keamanan dapat dikategorikan dalam empat kategori utama, yaitu *Interruption*, suatu aset dari suatu sistem diserang sehingga menjadi tidak tersedia atau tidak dapat dipakai oleh yang berwenang. *Interception*, suatu pihak yang tidak berwenang mendapatkan akses pada suatu aset. Pihak yang dimaksud bisa berupa orang, program, atau sistem yang lain. *Modification*, suatu pihak yang tidak berwenang dapat melakukan perubahan terhadap suatu aset. *Fabrication*, suatu pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem [2]. Serangan jaringan dapat dibagi menjadi empat kategori, serangan penolakan layanan (DoS), serangan pengguna ke *root* (U2R), serangan jarak jauh ke lokal (R2L), dan serangan *probe* jaringan [3].

Data IDSIRTII yang dikutip Aidil menyatakan jumlah total serangan kedalam jaringan 135,6 juta serangan pada tahun 2016 mengalami kenaikan 50% dibandingkan dengan 2015 [4]. Kejahatan dunia maya sebagai profesi semakin

Diterima 08 Januari 2021 Direvisi 30 April 2021 Diterima untuk publikasi 10 Mei 2021

menarik bagi peretas yang cakap, dan pada gilirannya, serangan siber sendiri semakin terorganisir dengan baik [5]. Bahkan beberapa teknologi kriminal lebih tinggi dari level ahli komputer, sehingga jaringan keamanan tidak bisa dijamin [6].

Berdasarkan permasalahan di era digital ini, keamanan jaringan sangat penting diterapkan untuk memungkinkan mencegah tindak kejahatan *cyber-crime.* Misalnya dalam penerapan MAC *Address Register*, administrator bisa memberi hak akses pada pengguna yang dikehendaki saja, dan melarang pengguna Anonim untuk terhubung dalam jaringan. Pengguna Anonim memiliki kemungkinan untuk membobol jaringan atau melakukan bermacam *cyber-crime*. Tindak kejahatan yang umumnya dilakukan pengguna Anonim berupa *Access Attacks*. Serangan akases berupa orang yang tidak berwenang mendapatkan akses ke jaringan atau perangkat yang tidak berhak mereka akses. Ada dua jenis serangan akses: yang pertama adalah akses fisik, di mana penyusup dapat memperoleh akses ke perangkat fisik. Yang kedua adalah akses jarak jauh, yang dilakukan ke perangkat yang terhubung dengan IP [7].

Teknologi Sistem dan Jaringan adalah teknologi kunci untuk berbagai macam aplikasi. Ini adalah persyaratan penting dalam jaringan situasi saat ini, ada kekurangan metode keamanan yang signifikan yang dapat dengan mudah diterapkan [8]. Dengan meningkatnya permintaan layanan jaringan (misalnya, *e-commerce*), arsitektur jaringan menjadi semakin rumit. Misalnya, jaringan kampus perlu mencakup berbagai departemen yang memiliki kepentingan jaringan dan persyaratan / kebijakan perlindungan keamanan yang berbeda, dan hal ini menyebabkan konfigurasi / manajemen jaringan yang kompleks dan penggunaan sumber daya keamanan jaringan yang tidak efisien (misalnya, perangkat keamanan yang telah dipasang sebelumnya di departemen tertentu tidak dapat digunakan untuk departemen lain) [9].

Keamanan berdasar pada serangan. Keamanan pada jaringan yang dibangun berdasar ancaman serangan yang akan datang, dan serangan yang sedang dilakukan [1]. Perusahaan biasanya menggunakan berbagai produk keamanan konvensional yang secara sempit berfokus pada aspek jaringan tertentu [10]. Sedangkan pemantauan jaringan untuk manajemen keamanan bertujuan untuk melindungi informasi sensitif pada perangkat yang terhubung ke jaringan data dengan mengontrol titik akses ke informasi tersebut [11]. Pengamanan pada *port* komputer nantinya akan membuat serangan pada komputer tidak mempunyai hak akses maupun yang tidak berkepentingan dapat dengan mudah mengandalikan *port–port* yang telah ia masuki [12].

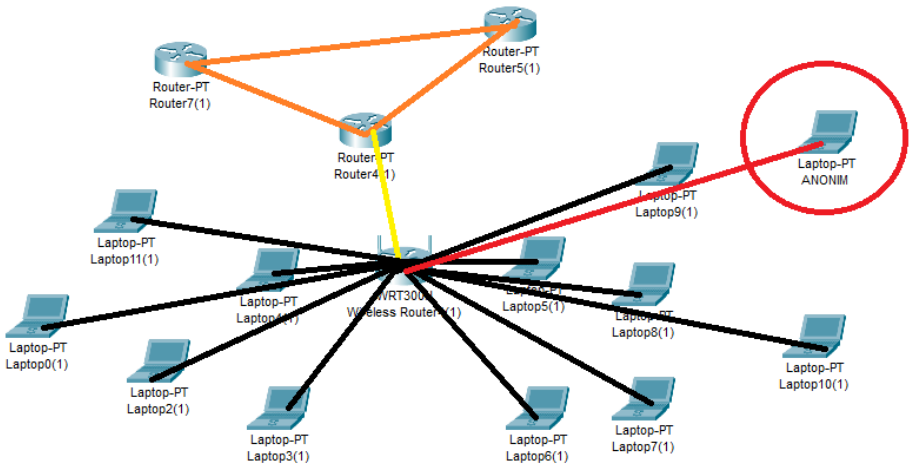
2 Metode Penelitian

Perkembangan teknologi pada jaringan komputer semakin menuntut keamanan pada sistem yang dibangun. Keamanan juga membutuhkan fleksibilitas, efisiensi, dan efektivitas. Pertukaran informasi melalui koneksi internet menjadi hal yang normal dilakukan pada saat ini. Namun, cara ini bisa memicu pencurian data atau kejahatan dunia maya yang merugikan kedua belah pihak

[13]. Penyaringan IP dan MAC adalah cara untuk melindungi jaringan nirkabel agar tidak digunakan dan disalahgunakan oleh sembarang orang. Teknik ini sangat berguna untuk mengamankan data di komputer jika bergabung dengan jaringan publik. Dengan mendaftarkan IP dan MAC di *Router*, ini akan menjaga informasi tidak digunakan dan dicuri. Sistem ini hanya beberapa komputer yang dapat dihubungkan ke hotspot nirkabel dengan alamat IP dan MAC yang terdaftar [13]. *Authenticity*: *Authenticity* mengacu pada konfirmasi identitas sebenarnya dari node jaringan untuk membedakan pengguna yang sah dari pengguna yang tidak sah. Dalam jaringan nirkabel, sepasang node yang berkomunikasi harus terlebih dahulu melakukan otentikasi timbal balik sebelum membuat tautan komunikasi untuk transmisi data [14]. Pada jaringan nirkabel, penyusup yang telah disusupi dapat dideteksi melalui MAC *Address* yang terhubung, tetapi kelemahan keberadaan seseorang tidak dapat ditemukan semudah yang dibayangkan. Itulah alasan mengapa keamanan jaringan nirkabel diperlukan [13].

Konsekuensi yang disebabkan oleh penyerang dalam proses resolusi alamat adalah serius. Misalnya, serangan *man-in-the-middle* mencegat dan merusak data, yang dapat menyebabkan gangguan komunikasi jaringan dan konsekuensi serius lainnya [15]. MAC *Filtering* memungkinkan akses hanya untuk perangkat yang diinginkan [16]. Penerapan MAC *Filtering* atau MAC *Address Register* ini dilakukan melalui simulasi *Cisco Packet Tracer*. Hampir semua spesialis jaringan memiliki simulator jaringan yang membantu mereka. Karena tidak selalu memungkinkan untuk bekerja di laboratorium. Dan program simulasi ini sangat baik untuk praktek konfigurasi jaringan dan setelah itu dengan mudah dapat mengkonfigurasi jaringan di area nyata, simulator ini seperti NS (*Network simulator*) *Cisco Packet Tracer* dan eNSP [17]. Program *Cisco Packet Tracer* dan eNSP adalah program simulasi yang menyediakan lingkungan lab jaringan bagi pengguna untuk melakukan operasi atau aplikasi Cisco tanpa memerlukan penggunaan mesin fisik atau kendaraan apa pun [17]. *Cisco Packet Tracer* adalah alat perangkat lunak jaringan komputer visualisasi dan simulasi yang dapat diakses secara gratis oleh siswa yang terdaftar di program *Cisco Network Academy*. Di sisi lain, alat tersebut masih bisa digunakan oleh mereka yang berada di luar akademi sebatas untuk tujuan pendidikan saja [18].

A. Desain Simulasi



Gambar 1. *Desain Jaringan*

Desain Jaringan seperti pada Gambar 1 berupa jaringan nirkabel atau *wireless* yang merupakan simulasi jaringan perkantoran dan memungkinkan terhubung ke kantor yang lain yang dalam satu perusahaan. Dalam jaringan kantor terdapat *Router* yang berfungsi untuk menghubungkan ke kantor yang lainnya, dan terdapat WiFi juga dalam kantor tersebut. WiFi ini yang akan disimulasikan sebagai tempat pengamanan jaringan dalam kantor, yang menghubungkan beberapa *device* dari karyawan kantor. Dan ada 1 *device* yang diibaratkan Laptop Anonim yang mencoba terhubung ke dalam jaringan, maka peran keamanan jaringan *MAC Address Register* membuat Laptop Anonim seharusnya tidak dapat terhubung ke dalam jaringan.

Pelaksanaan Simulasi.

Simulasi dilakukan menggunakan *software* aplikasi *Cisco Packet Tracer*, replika *device* dan fitur keamanan konfigurasi juga menggunakan yang sudah tersedia di aplikasi tersebut.

Alat dalam *Cisco Packet Tracer* yang digunakan:

-*Network Devices (Routers)* – PT *Router* (3 *devices*)

-*Network Devices (Wireless Devices)* – WRT300N (1 *devices*)

-*End Devices* – Laptop (12 *devices*)

Koneksi antar *devices* menggunakan *Components* lalu pilih *Automatically Choose Connection Type*, dan hubungkan setiap *device*s seperti dalam Desain Jaringan.

Konfigurasi setiap *devices*:

Hubungkan *Router* dengan connector Serial DCE. Lalu lakukan pengaturan *Router* dengan CLI.

1.***Router* 2 (setting 2 serial)** , seperti Sintak 1:

```
Router>en// enable
Router #conf t//configure terminal
Router (config)#int s2/0//setting interface dari router ke router
Router (config-if)#ip add 172.16.1.2 255.255.0.0//setting IP dan subnet
mask
Router (config-if)#no shut//mengaktifkan port status
Router (config-if)#ex//exit
Router (config)#
Router (config)#int s3/0//setting interface serial di Router
Router (config-if)#ip add 10.10.10.2 255.0.0.0
Router (config-if)#no shut//mengaktifkan port status
Router (config-if)#ex//exit
```

Sintak 1. *Konfigurasi Router 2*

2. *Router*-ISP (setting 2 serial) , seperti Sintak 2:

```
Router >en// enable
Router #conf t        //configure terminal
Router (config)#ints2/0//setting interface dari router kerouter
Router (config-if)#ip add 192.168.1.2 255.255.255.0//setting IP dan
subnet mask
Router (config-if)#no shut//mengaktifkan port status
Router (config-if)#ex//exit
Router (config)#
Router (config)#int s3/0//setting interface dari router kerouter
Router (config-if)#ip add 10.10.10.1 255.0.0.0
Router (config-if)#no shut//mengaktifkan port status
Router (config-if)#ex//exit
```

Sintak 2. *Konfigurasi Router ISP*

3. *Router* 1(setting 2 Se, 1 FastEthernet 0/0) , seperti Sintak 3:

```
Router >en// enable
Router #conf t//configure terminal
Router (config)#ints2/0//setting interface dari router kerouter
Router (config-if)#ip add 172.16.1.1 255.255.0.0 //setting IP dan subnet mask
Router (config-if)#no shut//mengaktifkan port status
Router (config-if)#ex//exit
Router (config)#
Router (config)#int s3/0//setting interface dari router kerouter
Router (config-if)#ip add 192.168.1.1 255.255.255.0//setting IP dan subnet mask
Router (config-if)#no shut//mengaktifkan port status
Router (config-if)#ex//exit
Router (config)#
Router (config)#intfa 0/0//setting interface dari router keRouter-Wi-Fi
Router (config-if)#ip add 192.168.3.2255.255.255.0//setting IP dan subnet mask
Router (config-if)#no shut//mengaktifkan port status
Router (config-if)#ex//exit
```

Sintak 3. *Konfigurasi Router 1*

Lalu lakukan *Static Routing* pada setiap *Router* dengan jaringan yang tidak terhubung secara langsung, seperti Sintak 4:

1. **Router 2:**

```
Router (config)#ip route 192.168.1.0 255.255.255.0 10.10.10.1
Router (config)#ip route 192.168.1.0 255.255.255.0 172.16.1.1
Router (config)#ip route 192.168.0.0 255.255.255.0 172.16.1.1
Router (config)#ip route 192.168.3.0 255.255.255.0 10.10.10.1
```

2. **Router 1:**

```
Router (config)#ip route 172.16.0.0 255.255.0.0 10.10.10.2
Router (config)#ip route 172.16.0.0 255.255.0.0 192.168.1.1
Router (config)#ip route 192.168.0.0 255.255.255.0 192.168.1.1
Router (config)#ip route 192.168.3.0 255.255.255.0 10.10.10.2
```

3. **Router-ISP:**

```
Router (config)#ip route 10.0.0.0 255.0.0.0 172.16.1.2
Router (config)#ip route 10.0.0.0 255.0.0.0 192.168.1.2
```

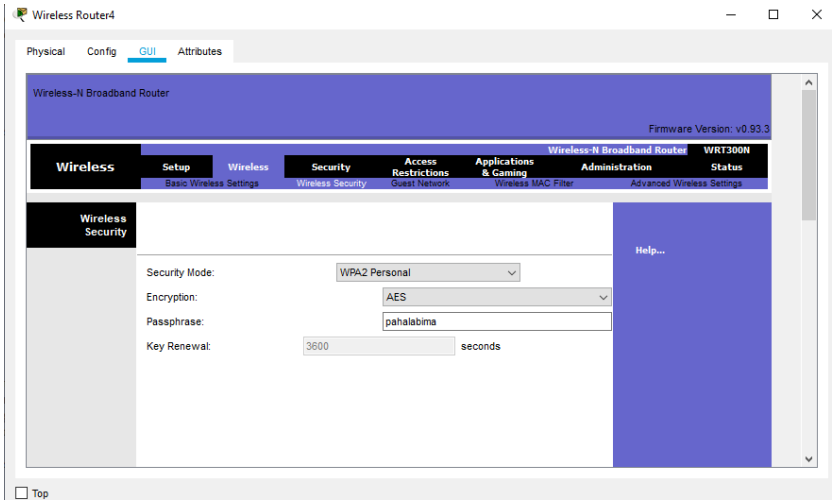
Sintak 4. *Konfigurasi Static Routing*

Melakukan pengaturan terhadap jaringan internet yaitu antara *Route*r *Wi-Fi* dihubungkan ke *Router* 1. Dengan menggunakan IP *Static* 192.168.3.1 dan *SubnetMask* 255.255.255.0 pada *Router Wi-Fi*, 192.168.3.2 dan *SubnetMask* 255.255.255.0 pada *Router* 1 atau sebagai *gateway* antara *Router-Wi-Fi* dengan ISP. Lalu melakukan pengaturan terhadap IP Address dan *SubnetMask* para pengguna dengan menggunakan DHCP agar memudahkan pengguna dalam mendapat IP *Address*.Untuk membatasi pengguna dilakukan dengan membatasi jumlah IP *Address* yang diberikan. Pada jaringan ini digunakan IP *Private* kelas C yaitu 192.168.20.10 sampai 192.168.20.24 dan *SubnetMask* 255.255.255.0. Sehingga jumlah penggunanya ada 15 pengguna.

Pengaturan IP Address untuk Laptop.

Sambungkan terlebih dahulu WPC 300N untuk masing-masing laptop. Lalu sambungkan setiap Laptop dengan *Router-Wi-Fi* dengan masuk ke *Dekstop* → PC *Wireless* → *Connect* → Pilih *Wireless Network Name* yang ada → tekan *Connect* → masukkan *Pre-shared Key* → Pilih *Connect*. Maka IP *Address* akan terisi dengan sendirinya. Lakukan langkah berikut sampai 11 Laptop yang lain. Penggantian SSID sebaiknya dilakukan berkala agar menyulitkan bagi pengguna ilegal untuk dapat mengakses data pada jaringan *Wi-Fi*. Karena apabila dapat SSID jarang diganti, dapat menjadikan jaringan *Wi-Fi* menjadi rawan akan tertembusnya jaringan oleh pengguna ilegal. Untuk SSID *Broadcast* sebagai bentuk keamanan lebih lanjut dapat dinon-aktifkan setelah semua pengguna telah masuk ke jaringan *Wi-Fi* tersebut.

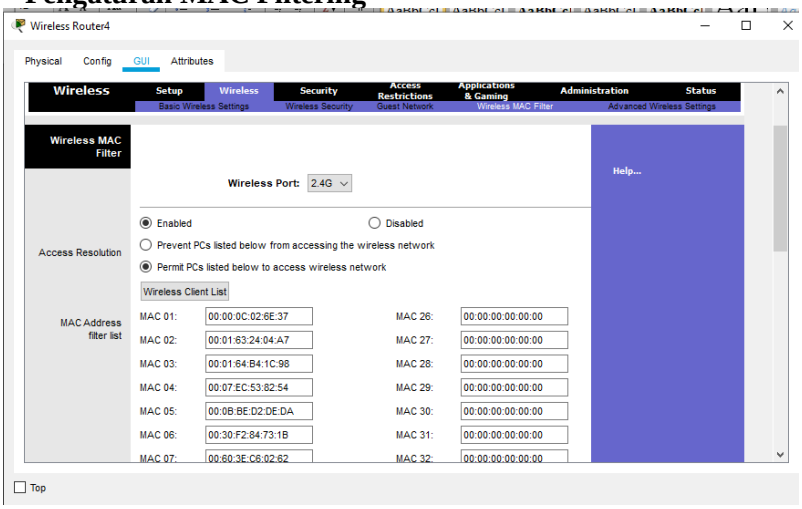
Pengaturan WPA



Gambar 2. *Tampilan Jendela GUI pada Wireless Security*

Security Mode seperti pada Gambar 2 menyajikan pilihan dalam mode pengamanan untuk *Router-Wi-Fi* . Peneliti menggunakan mode WPA2 *Personal* sebagai *Security mode* karena lebih aman dan terstandard dibandingkan WEP. Dengan melakukan pergantian secara berkala terhadap *PassPhrase* akan memberikan keamanan sehingga menyulitkan para pengguna ilegal untuk masuk dengan mudah ke dalam jaringan *Wi-Fi.*

Pengaturan MAC Filtering

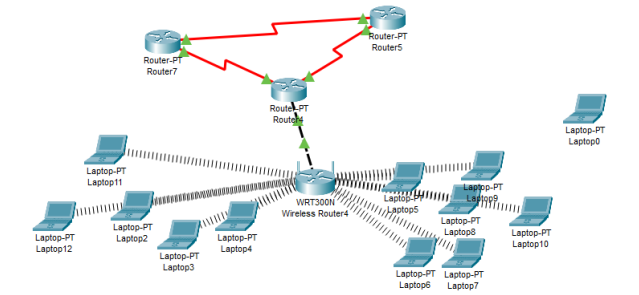


Gambar 3. *Tampilan Jendela GUI pada Wireless MAC Filter*

Seperti pada Gambar 3, MAC *Filtering* ditujukan untuk memberikan akses jaringan *Wi-Fi* kepada para pengguna yang telah terdaftar secara resmi. Maka jika ada pengguna yang tidak terdaftar dalam *Wireless Client List* maka tidak dapat mengakses jaringan *Wi-Fi* tersebut. Laptop Anonim tetap dibiarkan saja dan jangan didaftarkan dalam MAC *Filter*, agar dianggap pengguna anonim tidak dapat terhubung ke dalam jaringan.

3 Hasil dan Pembahasan

B. Hasil



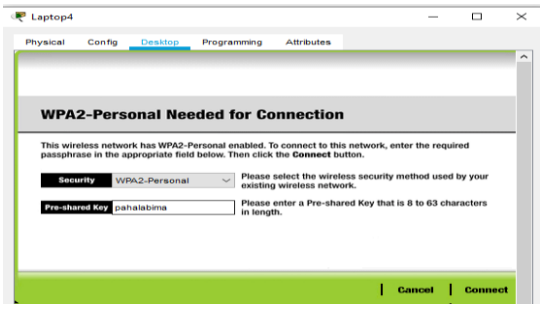
Gambar 4. *Hasil Desain Keamanan Jaringan*

Dalam Gambar 4 merupakan percobaan yang telah dilakukan, dapat juga menggunakan hanya 1 *Router* untuk penerapan jaringan, akan tetapi pada Gambar 4 tersebut mensimulasikan jaringan kantor dan kantor cabang. Laptop yang terhubung dan memiliki MAC *Address* terdaftar akan memiliki simbol garis-garis, dan bisa mengakses WiFi. Sedangkan laptop Anonim atau yang MAC *Address* belum terdaftar tidak memiliki simbol dan tidak bisa mengakses jaringan.

Router dapat saling terhubung seperti pada Gambar 4 yang berarti setiap kantor dapat terhubung ke kantor cabang yang lainnya, dan dalam jaringan kantor juga terdapat keamanan berupa *MAC Address Filter* dalam *Wireless Device*. Laptop yang *MAC Address* nya didaftarkan dalam WiFi dapat terhubung ke dalam jaringan sebagai pengguna yang diketahui, sedangkan pengguna yang tidak diketahui(Anonim) tidak dapat terhubung ke jaringan dikarenakan *MAC Address* nya tidak didaftarkan.

C. Pembahasan

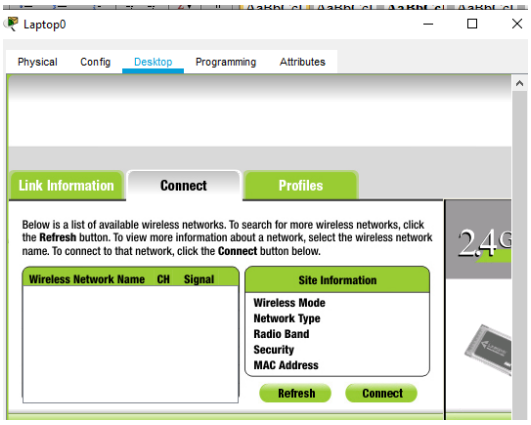
Setelah membuat dan melakukan pengaturan terhadap jaringan pada sistem jaringan, maka peneliti melakukan Pengujian dan analisis mengenai keamanan pada jaringan *Wi-Fi* yang telah dibuat dengan menggunakan *Cisco Packet Tracer*.



Gambar 5. *Tampilan jendela PC Wireless*

Pada Gambar 5, Laptop 4 ketika melakukan koneksi untuk mengakses jaringan setelah menemukan SSID maka dituntut untuk memberikan *Pre-shared key* yang berfungsi sebagai kunci untuk membuka pintu akses terhadap jarigan *Wi-Fi* tersebut.

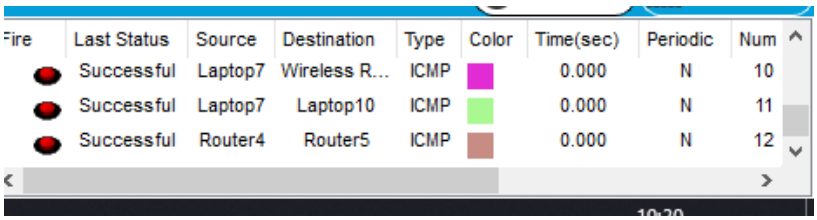
Setelah melakukan pengaturan, maka uji konektivitas dilakukan untuk membandingkan antara pengguna resmi dan pengguna ilegal. Dengan melihat pada lembar kerja *Cisco Packet Tracer* dapat diketahui Laptop mana saja yang telah tersambung dengan jaringan tersebut seperti pada Gambar 6.



Gambar 6. *Wireless PC Anonim*

Pada jendela *PC Wireless*, Pengguna Ilegal tidak menemukan SSID pada *Router-Wi-Fi* seperti pada Gambar 6. Hal yang pertama yaitu karena SSID Broadcast dinon-aktifkan. Yang kedua karena MAC *Address* dari Pengguna Ilegal tidak masuk ke dalam daftar MAC *Address* yang diijinkan. Maka dari itu penggantian berkala SSID dan *PassPhrase* dapat meminimalisir dari kegagalan MAC *Address*.

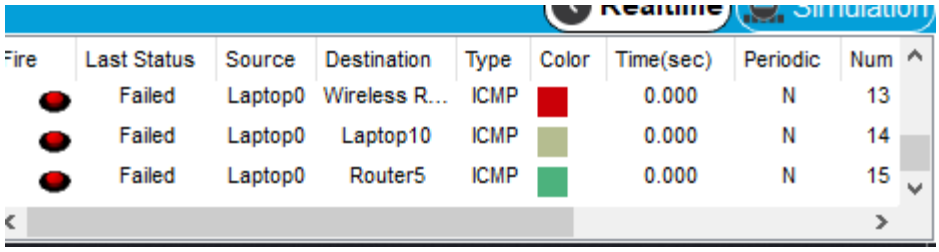
Pengujian Jaringan dengan PING dan PDU



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	Laptop7	Wireless R...	ICMP		0.000	N	10
	Successful	Laptop7	Laptop10	ICMP		0.000	N	11
	Successful	Router4	Router5	ICMP		0.000	N	12

Gambar 7. *Konektivitas Laptop Terdaftar*

Pengujian konektivitas antar Laptop yang terhubung seperti pada Gambar 7. Sebagai contoh di atas Laptop7 melakukan perintah PING terhadap Laptop10. Dapat dilihat perintah PING sukses. Laptop7 terhadap *Router*-ISP dan *Router*1 ketika melakukan perintah PING, sukses.
Pengujian konektivitas antar *Router* dengan menggunakan PDU berlangsung dengan "*Successful*" yang berarti antar ketiga *Router* terhubung.



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Failed	Laptop0	Wireless R...	ICMP		0.000	N	13
	Failed	Laptop0	Laptop10	ICMP		0.000	N	14
	Failed	Laptop0	Router5	ICMP		0.000	N	15

Gambar 8. *Konektivitas Laptop-Pengguna Ilegal*

Pada Gambar 8 diketahui Laptop-Anonim ketika dilakukan uji konektivitas dengan PING dan PDU, tidak berhasil. Pada perintah PING packet tidak terkirim kembali atau 100% *Lost* dan *Request Timed Out*. Dan pengiriman PDU berstatus akhir "*Failed*" sehingga Laptop-Anonim tidak terhubung ke dalam jaringan tersebut.

Dengan pengujian yang telah dilakukan dan mendapatkan hasil yang efektif, makan metode MAC *Address Register* mampu menjadi model keamanan dasar pada jaringan *Wireless* untuk mencegah pengguna Anonim.

4 Kesimpulan

Sistem kemanan jaringan berbasis *MAC Address Register* untuk mencegah Pengguna Anonim dapat berfungsi sesuai seperti apa yang diharapkan. Sistem keamanan ini mampu berperan sebagai keamanan tingkat dasar dalam sebuah jaringan. Keamanan ini hanya memberikan akses kepada *devices* yang sudah terdaftar dalam *MAC Address Filter*, sehingga pengguna dengan *devices* yang belum terdaftar tidak dapat

menemukan dan terhubung ke dalam jaringan. Hal ini meminimalisir tindakan pembobolan jaringan. Simulasi Keamanan jaringan *Wi-Fi* dilakukan dengan menggunakan software *Cisco Packet Tracer*. *Static Routing* dapat mengantisipasi jaringan dari terputusnya koneksi jika terjadi masalah pada salah satu jalur jaringan. Keamanan jaringan *Wi-Fi* dapat berjalan maksimal jika penggantian SSID dan *PassPhrase* dilakukan berkala dan MAC *filtering* dijalankan dengan baik.

5 Daftar Istilah

PDU : *Protocol Data Unit*

SSID : *Service set identifier*

WPA : *Wifi Protected Access*

Wi-Fi : *Wireless Fidelity*

MAC : *Media Access Control*

ISP : *Internet Service Provider*

6 Referensi

[1] A. S. Li, X. C. Li, P. YiCheng, And Z. Wei, *Strategies for Network Security*, Science China Information Science, 2015, vol.58, 012107:1-012107:14. https://doi.org/10.1007/s11432-014-5182-9

[2] R. Mentang, A. E. Sinsuw, And X. B. Najoan, *Perancangan Dan Analisis Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System*, E-Journal Teknik Elektro dan Komputer, 2016, vol.5, no.7, 2301-8402. https://doi.org/10.35793/jtek.4.7.2015.10592

[3] N. Khamphakdee, N. Benjamas, And S. Saiyod, *Improving Intrusion Detection System Based on SNORT Rules for Network Probe Attacks Detection with Association Rules Technique of Data Mining*, Journal of ICT Research and Applications, 2015, vol.8, no.3, 234-250. https://dx.doi.org/10.5614%2Fitbj.ict.res.appl.2015.8.3.4

[4] J. Fahana, R. Umar, And F. Ridho, *Pemanfaatan Telegram Sebagai Notifikasi Serangan untuk Keperluan Forensik Jaringan*, Jurnal Sistem Informasi, 2017, vol.1, no.2, 6-14.

[5] K. Huang, M. Siegel, And S. Madnick, *Systematically Understanding the Cyber Attack Business: A Survey*. *ACM Computing Surveys*, 2018, vol.51, no.4, 70. https://doi.org/10.1145/3199674

[6] M. Zen, And I. P. Novianti, *Keamanan Jaringan Komputer Pada Era Big Data*, Jurnal Sistem Informasi-J-SIKA, 2020, vol.2, no.1.

[7] A. Mohamed, And M. K. Geir, *Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks, Journal of Cyber Security*, 2015.

[8] M. V. Pawar, And J. Anuradha, *Network Security and Types of Attacks in Network*, Procedia Computer Science, 2015, vol.48, 503-506. https://doi.org/10.1016/l.procs.2015.04.126

[9] S. Seungwon, W. Haopei, And Guofei Gu, *A First Step Toward Network Security Virtualization From Concept To Prototype, Automatic Control and Computer Sciences*, IEEE Transactions on Information Forensics and Security, 2015.

[10] R. S. Michael, And S. P. Scott, *Systems and methods of network security and threat management*, United States Patent, 2018.

[11] G. Ibrahim, P. Vaclav, S. Jakub, and H. Mohammad, *A Survey on Network Security Monitoring Systems*, 4th International Conference on Future Internet of Things and Cloud Workshops, 2016.

[12] R. Putu, S. Putu, And W. Ichsan, *Sistem Keamanan Jaringan Komputer dan Data Dengan Menggunakan Metode Port Knocking*, Jurnal Sistem Informasi dan Komputer Terapan Indonesia (JSIKTI), 2018, vol.2, no.2, doi: https://doi.org/100.33173/jsikti.12

[13] D. S. Ressy, Supiyandi, P. U. S Andysah, M. Muhammad, And B. G. Raheliya, *A Review of IP and MAC Address Filtering in Wireless Network Security*, Science and Technology. IJSRST, 2017.

[14] Z. Yulong, Z. Jia, W. Xianbin, And H. Lajos, *A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends*, Proceedings of the IEEE, 2016, vol. 104, no.9.

[15] S. Guang-jia, And J. Zhen-zhou, *Anonymous-address-resolution model*, *Frontiers of Information Technology & Electronic Engineering*, Springer, 2016.

[16] G. Minela, P. Drazen, P. Srdan, And K. Vladimir, *Provided security measures of enabling technologies in Internet of Things (IOT): A survey*, Zooming Innovation in Consumer Electronics International Conference (ZINC), 2016.

[17] M. H. Sayed, And G. Ali, *Performance Evaluation of a Network Using Simulation Tools or Packet Tracer*, Journal of Computer Engineering. IOSRJournals, 2017.

[18] Nazre, Z. Muhammad, Rasyidi, And F. Salman, *Cisco Packet Tracer Simulation as Effective Pedagogy in Computer Networking Course*, Universiti Pendidikan Sultan Idris, Perak, Malaysia, iJIM, 2019, vol.13, no.10, https://doi.org/10/3991/ijim.v13i10.11283