

SISTEM KEAMANAN JARINGAN WIRELESS MENGGUNAKAN PEAP MS CHAP

Elis Septia Wati¹, Dodi Apriansyah²

¹ Mahasiswa Program Studi Manajemen Informatika, AMIK Dian Cipta Cendikia

² Dosen Program Studi Manajemen Informatika, AMIK Master
elisseptia03@gmail.com¹, dodyapriansyah@dcc.ac.id²

ABSTRAK

Pada komunikasi data menggunakan nirkabel, pengamanan data merupakan faktor penting karena data yang melewati jaringan nirkabel dapat dengan mudah dicuri dan disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab. Pada penelitian ini dilakukan pengamanan data pada komunikasi data nirkabel menggunakan protokol PEAP Ms CHAP V2 yang memiliki mekanisme otentikasi berbasis password, challenge response, dan protokol dengan sifat mutual-authentication. Metode otentikasi ini juga menerapkan adanya TLS Channel untuk melindungi pertukaran username dan password dari user yang sah, juga melindungi data dengan cara mengenkripsi dan menjaga integritas data. Pengujian keamanan komunikasi data dengan cara melakukan serangan brute force dan sniffing. Berdasarkan pengujian, penggunaan protokol PEAP MS CHAP V2 pada komunikasi data menggunakan jaringan nirkabel akan terlindungi dari serangan brute force dan sniffing, sehingga proses komunikasi data lebih aman dan terkendali.

Kata kunci: Nirkabel, Komunikasi data, PEAP MS CHAP V2, Otentikasi

1. Pendahuluan

Pada saat ini penggunaan perangkat portable/mobile telah menjadi sarana yang banyak diterapkan dan digunakan hat tersebut dimungkinkan dengan adanya jaringan nirkabel. Namun dengan segala kemudahannya, salah satu masalah utama yang muncul adalah masalah keamanan, karena data yang melewati jaringan nirkabel dapat dengan mudah dicuri dan disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab. Salah satu cara pengamanan pada jaringan nirkabel adalah adanya proses otentikasi dan enkripsi. Proses otentikasi dan enkripsi merupakan proses yang penting karena merupakan proses yang pertama kali dijalankan sebelum pengguna dapat mengakses suatu jaringan nirkabel.

Salah satu protokol yang menyediakan proses otentikasi dan enkripsi adalah PEAP Ms CHAP V2. Protected Extensible Authentication Protokol (PEAP) adalah bagian dari protokol Extensible Authentication Protokol (EAP) yang menggunakan Transport Layer Security (TLS) sebagai media untuk mengenkripsi channel yang digunakan untuk proses otentikasi antar client pada PEAP. Sedangkan Ms

CHAP adalah Protokol yang dikembangkan oleh Microsoft untuk melakukan otentikasi berdasarkan username dan password dan dapat melakukan otentikasi secara dua arah.

Tujuan dan rumusan masalah penelitian ini berdasarkan kepada proses konfigurasi PEAP MS CHAP V2 sebagai metode keamanan jaringan nirkabel untuk mencegah client yang tidak ter-otentikasi dapat mengakses jaringan internet dan pengujian mengamankan jaringan nirkabel terhadap serangan brute force dan sniffing.

Proses konfigurasi dan pengujian dibatasi berdasarkan hal-hal sebagai berikut.

- a. Protokol otentikasi yang dipakai adalah PEAP Ms CHAP V2.
- b. Menggunakan Internet Authentication Service (IAS) sebagai Remote Authentication Dial-In User Service (RADIUS) Server
- c. Implementasi pengujian pengamanan menggunakan serangan brute force dan sniffing
- d. Pengujian menggunakan simulasi jaringan nirkabel LAN
- e. Topologi yang digunakan pada pengujian adalah topologi star
- f. PEAP Ms CHAP V2 ini diterapkan pada Sistem Operasi Windows Server 2003 Enterprise Edition R2
- g. Client menggunakan Sistem Operasi Window XP
- h. Pendistribusian IP Address dilakukan dengan cara DHCP
- i. Software yang digunakan untuk pengujian penyerangan jaringan adalah Wireshark, Cain and Abel, Aircrack, dan Zenmap
- j. Algoritma enkripsi yang dipakai adalah Advance Encryption Standard (AES)

2. Kajian Pustaka

2.1 Jaringan Nirkabel

Jaringan Nirkabel atau dikenal dengan nama Wireless, merupakan salah satu media transmisi yang menggunakan gelombang radio. Data-data digital yang dikirim melalui wireless akan dimodulasikan ke dalam gelombang elektromagnetik tersebut. Wireless Fidelity (Wi-Fi) adalah nama yang diberikan oleh Wi-Fi Alliance untuk mendeskripsikan produk Wireless Local Area Network (WLAN) yang berdasarkan standar Institute of Electrical and Electronics Engineers (IEEE) 802.11. Tidak seperti jaringan kabel, jaringan wireless memiliki dua mode yang dapat digunakan: infrastruktur dan Ad-Hoc. Konfigurasi infrastruktur adalah komunikasi antar masing-masing PC melalui sebuah access point pada WLAN atau LAN. Komunikasi Ad-Hoc adalah komunikasi secara langsung antara masing-masing komputer dengan menggunakan piranti wireless. Penggunaan kedua mode ini tergantung dari kebutuhan untuk berbagi data atau kebutuhan yang lain dengan jaringan berkabel.

Teknologi wifi memiliki standar yang ditetapkan oleh sebuah instusi internasional yang bernama institute of electrical and electronic engineers (IEEE), yang secara umum sebagai berikut : [1]

- a. Standar IEEE 802.11a yaitu wifi dengan frekuensi 5 Ghz yang memiliki kecepatan 54 Mbps dan jangkauan jaringan 300 m
- b. Standar IEEE 802.11b yaitu wifi dengan frekuensi 2,4 Ghz yang memiliki kecepatan 11 mbps dan jangkauan jaringan 100 m
- c. Standar IEEE 802.11g yaitu wifi dengan frekuensi 2,4 GHz yang memiliki kecepatan 54 mbps dan jangkauan jaringan 300 m
- d. Standar IEEE 802.11 n, yaitu wifi yang memiliki kecepatan 108 – 120 Mbps

2.2 Keamanan Jaringan Nirkabel

Aspek-aspek dasar keamanan jaringan komputer melingkupi hal-hal sebagai berikut: [2]

- a. Privacy atau ConfidentialityInti utama dari aspek ini adalah usaha untuk menjaga informasi dari orang tidak berhak mengakses. Privacy lebih kearah data-data yang sifatnya pribadi, sedangkan confidentiality biasanya berhubungan dengan data yang diberikan kepihak lain untuk keperluan tertentu.

- b. Integrity adalah menekankan bahwa informasi tidak boleh diubah tanpa ijin pemilik informasi. Contoh Sebuah email dapat saja ditangkap (intercept) di tengah jalan, diubah isinya (altered, tampered, modified) kemudian diteruskan ke alamat yang dituju.
- c. Authentication metode untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud, atau server yang kita tuju adalah benar-benar server asli. Dalam hal ini pengguna harus menunjukkan bukti bahwa memang dia adalah pengguna yang sah, misalnya dengan menggunakan password, keamanan biometric dan sejenisnya.
- d. Availability atau ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang dapat menghambat akses ke informasi. Contoh hambatan adalah serangan yang sering disebut dengan denial of service attack di mana server mendapatkan permintaan palsu yang bertubi-tubi sehingga tidak dapat melayani permintaan lain dan bahkan sampai down, hang serta crash.
- e. Access Control pengaturan akses kepada informasi. Hal ini biasanya berhubungan dengan klasifikasi data (public, private, confidential, top secret) dan user (guest, admin, top manager, dan lain sebagainya). Mekanisme Authentication, privacy, dan Access Control seringkali dilakukan dengan menggunakan kombinasi user id, password atau dengan menggunakan biometric.
- f. Non Repudiation Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan transaksi. Sebagai contoh, seseorang mengirimkan email untuk memesan barang tidak dapat menyangkal bahwa dia telah mengirimkan email tersebut. Aspek ini sangat penting dalam hal electronic commerce. Penggunaan digital signature, certificates dan teknologi cryptography secara umum dapat menjaga aspek ini.

Jenis pengamanan jaringan nirkabel dapat dibagi menjadi beberapa kategori sebagai berikut [2].

- a. Access Control, dilakukan dengan menggunakan mekanisme filtering (penyaringan). Penyaringan dapat dilakukan berdasarkan SSID, MAC Address atau IP Address ataupun protokol
- b. Authentication, sebuah proses dimana Access Point melakukan penerimaan atau penolakan terhadap sebuah permintaan koneksi. Contoh otentikasi yang dapat dilakukan seperti open sistem atau shared key, WPA, WPA-PSK.
- c. Encryption, sebuah proses untuk melindungi informasi dengan cara melakukan penyandian terhadap informasi tersebut. Beberapa teknologi enkripsi yang dapat digunakan pada jaringan wireless antara lain WEP, TKIP, atau AES.

2.3 Certification Authority

Certification Authority adalah suatu entitas yang dipercaya untuk mengeluarkan sertifikat kepada individu, komputer, atau organisasi yang menegaskan identitas dan atribut dari subjek sertifikat ke entitas lain. Berikut adalah beberapa jenis Certificate authority [3].

- a. Stand Alone Root CA, jenis ini digunakan dalam keadaan offline. Stand Alone root CA tidak terintegrasi dengan active directory. Namun informasi dari CA masih bisa dipublikasikan ke active directory.
- b. Enterprise root CA, server akan bertindak sebagai server yang akan menyediakan sertifikat untuk client dibawahnya. Enterprise root CA ini terintegrasi dengan active directory.

- c. Stand Alone subordinate CA berarti bahwa server CA adalah server CA bawahan dan telah mendapat sertifikat yang ditandatangani oleh CA server lain CA.
- d. Enterprise subordinate CA adalah anggota dari sebuah domain active directory dan terintegrasi dengan active directory. Pengguna dan komputer account dapat mendaftarkan diri atau autoenroll untuk sertifikat dari CA ini. Server CA menyediakan fungsi yang sama sebagai server enterprise root CA, namun Enterprise root CA adalah server CA bawahan.

2.4 PEAP Ms CHAP Versi 2

Protected Extensible Authentication Protokol (PEAP) adalah jenis baru dari Extensible Authentication Protokol (EAP). PEAP menggunakan Transport Layer Security (TLS) untuk membuat saluran terenkripsi antara client dengan PEAP otentikasi. PEAP tidak menentukan metode otentikasi, tetapi menyediakan keamanan tambahan lain untuk protokol otentikasi EAP, seperti EAP-MS CHAP v2, yang dapat beroperasi melalui saluran terenkripsi TLS yang disediakan oleh PEAP. PEAP adalah skema yang lebih fleksibel daripada EAP- TLS, PEAP menciptakan saluran SSL/TLS terenkripsi antara client dan server otentikasi, dan saluran 16 kemudian melindungi pertukaran otentikasi pengguna berikutnya [4].

2.5 Protokol AAA

Authentication, Authorization, and Accounting(AAA) adalah sebuah model keamanan jaringan komputer yang berfungsi untuk memverifikasi, memeriksa, dan memantau keabsahan suatu entitas yang terdiri atas tiga fitur utama, yaitu [2].

- a. Authentication adalah proses dimana identitas sebuah entitas/pengguna diperiksa.
- b. Authorization adalah proses yang berfungsi untuk memeriksa apakah pengguna yang telah di otentikasi berhak mengakses suatu layanan atau tidak.
- c. Accounting adalah proses pencatatan aktivitas pengguna selama mengakses jaringan.

2.6 Komponen Otentikasi

Komponen otentikasi pada 802.1x terdiri atas tiga entitas, yaitu : [2]

- a. Supplicant, sering juga disebut peer, adalah peralatan client, seperti PC, notebook atau smartphone, yang ingin tersambung ke LAN/WLAN. Supplicant mengirimrequest berupa otentikasi ke authenticator untuk bisa mengakses jaringan melewati authenticator.
- b. Authenticator,sering juga disebut Network Access Server (NAS), berfungsi sebagai filter antara supplicant dan jaringan yang diproteksi. Supplicant tidak diperbolehkan mengakses jaringan melewati authenticator sebelum identitas supplicant telah diperiksa dan divalidasi. Ketika supplicant mengirimkan request otentikasi ke authenticator, selanjutnya authenticator meneruskannya ke authentication server untuk menentukan apakah otentikasi tersebut valid atau tidak. Authenticator dalam jaringan nirkabel umumnya adalah sebuah wireless access point.
- c. Authentication Server bertugas untuk memeriksa identitas entitas yang dikirimkan oleh supplicant melalui authenticator. Authentication Server umumnya adalah server yang mendukung protokol RADIUS dan EAP.

2.7 Internet Authentication Service

Internet Authentication Service (IAS) merupakan salah satu tool snap in yang terdapat pada sistem operasi berbasis windows. IAS dapat digunakan sebagai server RADIUS untuk melakukan proses otentikasi, otorisasi, dan akunting terhadap client RADIUS. [2]

2.8 TLS/SSL

Transport Layer Security (TLS) dan pendahulunya Secure Socket Layer (SSL) adalah protokol kriptografi yang menyediakan keamanan dalam berkomunikasi melalui jaringan. TLS menyediakan keamanan dalam tiga hal : [2]

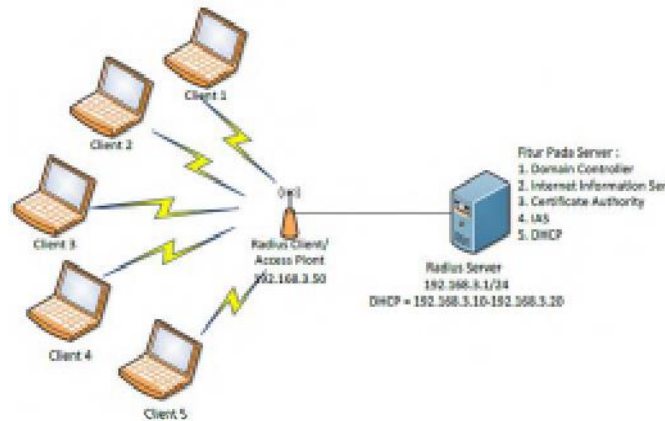
- a. Mutual Authentication antara client dan server dengan public key cryptography berdasarkan digital signatures. Dengan ini identitas client/server dapat dibuktikan dan pemalsuan pesan dapat dihindari. Algoritma kriptografi kunci publik yang sering digunakan adalah Rivest, Shamir, Adleman (RSA) dan Digital Signature Algorithm (DSA).
- b. Menjaga kerahasiaan data dengan fungsi kriptografi simetrik untuk melakukan enkripsi/dekripsi data sehingga mencegah pihak ketiga untuk melakukan eavesdropping. Algoritma kunci simetrik yang sering digunakan adalah AES (Advanced Encryption Standard) dan 3DES (Triple DES).
- c. Menghasilkan Message Authentication Code (MAC) melalui fungsi hash untuk mendeteksi adanya gangguan dan menjaga integritas data. Algoritma hash 25 yang sering digunakan adalah Message-Digest Algorithm (MD5) dan Secure Hash Algorithm (SHA-1)

Penelitian ini tidak terlepas dari penelitian-penelitian sebelumnya, adapun penelitian sebelumnya yang berkaitan dengan penelitian ini adalah:

- a. Implementasi Dan Analisis Jaringan Menggunakan Wireshark, Cain And Abels, Network Minner. [5] Dari hasil penelitian ini dapat disimpulkan, bahwa penggunaan wifi belum dapat dikontrol dengan baik sehingga mahasiswa belum secara penuh memanfaatkan internet.
- b. Mengamankan Wireless Dengan Menggunakan Two Factor, Password Dan Mac Address Filtering. [6] Hasil dari penelitian ini adalah: Dua faktor keamanan dalam penelitian ini menggunakan keamanan WPA-PSK dan dengan menggunakan Mac Address Filtering, yang berarti jika ada seseorang yang ingin mengakses wifi harus mempunyai dua otentikasi, karena apabila hanya memiliki password WPA-PSK-nya saja maka tetap tidak akan bisa terkoneksi karena mac address pada perangkatnya tidak terdaftar. Dengan menggunakan keamanan two factor, password dan Mac Address Filtering lebih memiliki beberapa kelebihan dibandingkan dengan menggunakan keamanan pada WPA-nya saja, karena dengan menggunakan dua otentikasi ini jika ada seseorang yang ingin mengakses ke hotspot harus memiliki password WPA-PSK dan mendaftarkan Mac Address perangkatnya ke Administrator, karena jika tidak memenuhi persyaratan keduanya atau salah satunya tidak akan bisa terkoneksi

3. Metode Penelitian

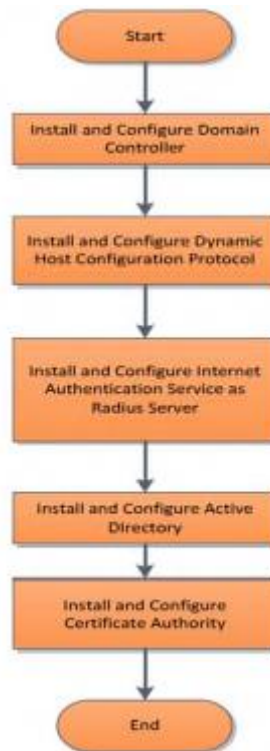
Dalam membangun “Pengamanan Jaringan Wireless Menggunakan PEAP Ms CHAP V2” menggunakan topologi star sebagai berikut:



Gambar 1. Topologi Simulasi Jaringan

Konfigurasi jaringan

Tahapan proses konfigurasi sistem seperti diperlihatkan flowchart yang ditunjukkan pada Gambar 2.



Gambar 2. Proses Konfigurasi Sistem

Secara ringkas tahapan proses konfigurasi sistem dapat diuraikan sebagai berikut [2].

- a. Instalasi dan Konfigurasi Domain Name Sistem (DNS) digunakan untuk menangani penerjemahan dari alamat IP ke nama domain atau sebaliknya.
- b. Konfigurasi IAS Sebagai Radius Server diperlukan untuk menyediakan server yang melakukan proses otentikasi, otorisasi, dan akunting.

- c. Konfigurasi Active Directory, Active Directory adalah sebuah directori service yang menyediakan informasi tentang objek-objek pada jaringan (user, group, domain, dll.) yang dapat dimanfaatkan oleh user anggota jaringan atau oleh administrator jaringan.
- d. Konfigurasi Certificate Authority digunakan sebagai Enterprise Root CA, yaitu issuer atau penerbit resmi dari certificate yang akan diberikan kepada client.
- e. Pemasangan Sertifikat Root Pada Server langkah ini berfungsi untuk memverifikasi apakah root CA sudah terpasang pada server.
 - f. Membuat Policy pada Sertifikat Root dengan cara mengatur Encrypting File System dan Automatic Certificate Request Setting pada Public Key Policies yang terdapat pada Windows Setting (Group Policy Object Editor)
- g. Konfigurasi Access Point, dipilih mode keamanan WPA2 atau WPA2 Enterprise dengan cipher type AES dan Pre Shared Key- nya EAP untuk mendukung metode pengamanan PEAP Ms CHAP V2, sedangkan pada port diisikan dengan 1812 sebagai port otentikasi pada radius server.

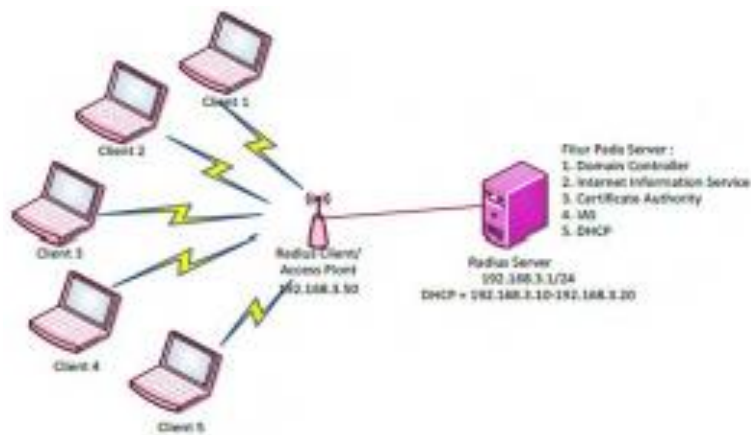
4. Hasil dan Pembahasan

Pengujian Otentikasi Client

Pengujian akan dilakukan dengan tujuan yang akan dicapai adalah:

- a. Konfigurasi WPA Network Key, Username, dan Password telah sesuai dengan rancangan
- b. Client terotentikasi dan dapat terhubung ke internet dengan menggunakan metode PEAP Ms CHAP V2

Topologi pengujian yang dilakukan untuk client terkoneksi ke internet ditunjukkan pada Gambar 3.



Gambar 3. Topologi Pengujian Otentikasi Client

Pengujian Serangan

Pengujian keamanan dengan serangan sniffing dan bruteforce untuk mendapatkan beberapa hal berikut.

- a. Tujuan Pengujian yang akan dicapai adalah:
 - 1) Untuk menguji tingkat keamanan jaringan wireless dengan mendapatkan WPA Network Key, username, dan password client
 - 2) Mendapatkan capture paket hasil otentikasi antara client dengan access point

- b. Parameter pengujian yang ingin dicapai adalah
 - 1) Mendapatkan WPA Network Key
 - 2) Mendapatkan username dan password
 - 3) Capture paket otentikasi
- c. Cara Pengukuran Parameter
 - 1) Dilakukan dengan software Cain and abel, Wireshark, dan Zenmap
 - 2) Menggunakan aircrack dan backtrack
 - 3) Pengujian 1 adalah keadaan dimana jaringan tidak menggunakan PEAP MS CHAP V2
 - 4) Pengujian 2 adalah keadaan dimana jaringan menggunakan PEAP MS CHAP V2.

Tabel 1. Skenario Pengujian

No	Pengujian 1 Kondisi Sebelum PEAP MS Chap V2	Pengujian 2 Kondisi Sesudah PEAP MS CHAP V2
1	Security Wireless Mode WPA Personal	Security Wireless Mode WPA Enterprise
2	Client Terhubung ke Jaringan	Client Terhubung ke Jaringan
3	Pengujian dengan Zenmap	Pengujian dengan Zenmap
4	Pengujian dengan Cain and Abel dan Wireshark	Pengujian dengan Cain and Abel dan Wireshark
5	Pengujian dengan Aircrack	Pengujian dengan Aircrack

Tabel 2. Hasil Pengujian Peap Ms Chap V2

Tujuan	Parameter	Tools	Hasil Yang Diharapkan	Hasil Pengujian	
				Uji 1	Uji 2
Capture password WPA network key	WPA network key	Aircrack	WPA Key tidak ditemukan	V	V
Scanning port yang terbuka	Port yang terbuka	Zenmap	Port tidak ter-rscan	V	V
Capture user name dan password	User name dan password	Cain and Abel, Wireshark	User name dan password tidak ditemukan	V	V
Eksplorasi port 445	Port 445	Zenmap	Eksplorasi port gagal	V	V

5. Kesimpulan dan Keterbatasan

Setelah melalui tahapan-tahapan proses pengujian, mekanisme otentikasi menggunakan metode pengamanan PEAP Ms CHAP V2, maka didapatkan kesimpulan sebagai berikut :

- a. PEAP MS CHAP V2 adalah salah satu metode pengamanan jaringan wireless untuk mencegah client yang tidak ter-otentikasi untuk dapat mengakses jaringan internet dengan mekanisme otentikasi yang berbasis username dan password, serta adanya mutual authentication antara client dan server.

- b. Metode pengamanan PEAP MS CHAP V2 dapat mengamankan data dan pertukaran username serta password dari serangan sniffing dan bruteforce.

Adapun keterbatasan dari penelitian ini adalah data yang di dapatkan masih terbatas terutama dalam pengujian dan perlu penambahan tool dalam membandingkan hasil dari data yang didapatkan. Bagi peneliti selanjutnya dalam pengumpulan data perlu memperhatikan lama waktu yang digunakan, sehingga data-data yang dikumpulkan lebih banyak dan hasilnya akan lebih baik lagi.

Referensi

- [1] Alan N. Aditya, *Mahir Membuat Jaringan, Dunia Komputer*, Indonesia. 2011
- [2] Efy Zamidra Zam, *Cara Mudah Membuat Jaringan Wireless*, Elex Media Komputindo, 2014
- [3] Eko Priyo Utomo, *Wireless Networking : Panduan Lengkap Membangun Jaringan Wireless Tanpa Teknisi*, Andi Publisher, 2012
- [4] Jubilee Enterprise, *Trik Membuat Jaringan Komputer dan Wi-fi*, Elex Media Komputindo, 2014
- [5] Susianto, D., & Rachmawati, A. (2018). *Implementasi Dan Analisis Jaringan Menggunakan Wireshark, Cain And Abels*, Network Minner. *Jurnal Cendikia*, 16(1 Oktober), 120-125.
- [6] Susianto, D., & Yulianti, I. (2015). *Mengamankan Wireless dengan Menggunakan Two Factor, Password dan Mac Address Filtering*. *EXPERT*, 5(2).
- [7] Lingga Wardhana & Nuraksa Makodian, *Teknologi Wireless Communication Dan Wireless Broadband*, Andi Publisher, 2010
- [8] Technet Microsoft. [Online]. (2011, October) [technet.microsoft.com/en-us/library/cc728188\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc728188(v=ws.10).aspx)
- [9] Patrick Ogenstad. (2010, May) *Certification Authority Types in Windows Certificate Services*. [Online]. <http://networklore.com/Certification-authority-types-in-windows-certificate-services/>
- [10] Pratama. I Putu Agus, *Handbook Jaringan Komputer Teori dan Praktik Berbasiskan Open Source*, 1st ed, Bandung: BI-Obses, 2014.
- [11] Sonny Rumlatur (2014). *Analisis Keamanan Jaringan WirelessLAN (WLAN) Pada PT. PLN (Persero) Wilayah P2B Area Sorong*. *Jurnal Teknologi dan Rekayasa*