

KEAMANAN JARINGAN KOMPUTER NIRKABEL DENGAN CAPTIVE PORTAL DAN WPA/WPA2 DI POLITEKNIK GANESHA GURU

Gede Arna Jude Saskara¹⁾, I Putu Oktap Indrawan²⁾, Putu Maha Putra³⁾

^{1,3} Program Studi D3 Teknik Komputer, Politeknik Ganesha Guru

² Program Studi D3 Manajemen Informatika, Politeknik Ganesha Guru

Email: arna@poltekbanesha.ac.id, oktap@poltekbanesha.ac.id, maha@poltekbanesha.ac.id

ABSTRAK

Pada Revolusi Industri 4.0 saat ini perkembangan jaringan komputer sudah semakin pesat. Dilihat dari media penghubung antara komputer satu dengan komputer satunya yang sebelumnya masih menggunakan kabel, sekarang ini sudah berubah menjadi tanpa menggunakan perantara kabel atau istilahnya nirkabel atau *wireless*. Salah satu instansi swasta yaitu Politeknik Ganesha Guru banyak memanfaatkan teknologi jaringan komputer yang bersifat nirkabel atau *wireless*. Penggunaan jaringan komputer nirkabel di instansi dibangun untuk mendukung kegiatan administrasi hingga kegiatan perkuliahan di Politeknik Ganesha Guru. Perkembangan jaringan tersebut berjalan lurus dengan keamanan jaringan. Pada jaringan nirkabel banyak *user* dapat terhubung ke dalam jaringan sehingga dibutuhkan lapisan keamanan agar sistem maupun server yang terdapat di instansi aman. Untuk mengamankan jaringan nirkabel terdapat beberapa teknologi yang dapat digunakan untuk mengamankan jaringan beberapa diantaranya adalah menambahkan *Captive Portal*, *RADIUS* hingga *Authentication* dengan kriptografi seperti *WPA* dan *WPA2*. Keamanan jaringan di Politeknik Ganesha Guru sudah menerapkan lapisan keamanan *Captive Portal*, *RADIUS* dan juga *Authentication* dengan *WPA*. Untuk menguji keamanan jaringan di instansi menggunakan pengujian dengan *Vulnerability Assessment* dan juga *Penetration Test*. Dari hasil pengujian didapatkan jaringan nirkabel di Politeknik Ganesha Guru yang hanya menggunakan *Captive Portal* dan *RADIUS*, *user* masih dapat melakukan penyerangan terhadap jaringan, sedangkan setelah ditambahkan *authentication* dengan *WPA*, *user* tidak dapat melakukan serangan.

Kata kunci: Jaringan, Nirkabel, *Captive Portal*, *RADIUS*, Keamanan

ABSTRACT

At the time of the Industrial Revolution 4.0, the development of computer networks was increasing rapidly. Judging from the media link between one computer and the other computer that was previously still using a cable, now it has changed to without using a cable intermediary or the term wireless. One of the institutions, namely the Ganesha Guru Polytechnic, uses many wireless computer network technologies. The use of wireless computer networks in institutions was built to support administrative activities until lecture activities at The Ganesha Guru Polytechnic. The development of the network goes straight with network security. In wireless networks, many users can connect to the network so that a security layer is needed so that the systems and servers in the institution are safe. To secure wireless networks there are several technologies that can be used to secure networks, some of which are adding Captive Portal, RADIUS and cryptographic Authentication such as WPA and WPA2. Network security at the Ganesha Guru Polytechnic has applied the security layer of Captive Portal, Radius and Authentication with WPA. To test network security, institution use Vulnerability Assessment and Penetration Test. From the results of the testing, there is a wireless network in the Ganesha Guru Polytechnic, who only use the Captive Portal and Radius can still attack the network, whereas after adding authentication with WPA the user cannot attack.

Keywords : Network, Wireless, *Captive Portal*, Radius, Security

1. PENDAHULUAN

Jaringan komputer merupakan sebuah sistem yang menghubungkan dua atau lebih komputer [1]. Pada Revolusi Industri 4.0 sekarang ini perkembangan jaringan komputer itu sendiri sudah semakin pesat. Dilihat dari media penghubung antara komputer satu dengan komputer yang satunya yang sebelumnya masih menggunakan kabel, sekarang ini sudah berubah tanpa menggunakan kabel atau istilahnya adalah *Wireless*. Hampir semua instansi swasta maupun negeri berlomba-lomba untuk mengembangkan sistem yang dapat diakses oleh orang banyak. Seiring dengan peningkatan kebutuhan dari sistem tersebut, infrastruktur yang dapat mengakomodir permintaan dari pengguna dan penyimpanan sistem tersebut harus ditingkatkan juga.

Salah satu instansi swasta yaitu Politeknik Ganesha Guru banyak memanfaatkan teknologi jaringan komputer yang bersifat nirkabel atau *wireless*. Penggunaan jaringan komputer nirkabel di instansi tersebut dilakukan untuk mendukung kegiatan administrasi hingga kegiatan perkuliahan yang terjadi di Politeknik Ganesha Guru. Dengan penggunaan jaringan komputer secara nirkabel juga bertujuan untuk memudahkan perangkat untuk terhubung tanpa menggunakan kabel. Karena segala kegiatan di instansi menggunakan jaringan komputer nirkabel perlu diperhatikan keamanan data yang terdapat di jaringan agar tidak dicuri oleh orang. Penggunaan jaringan nirkabel akan dengan mudah ditangkap oleh siapapun dikarenakan jaringan nirkabel menggunakan gelombang radio yang dipancarkan secara bersamaan dan bergerak bebas di udara.

Pembangunan jaringan nirkabel di sebuah instansi diperlukan perencanaan, perancangan dan implementasi suatu topologi jaringan, setelah implementasi suatu jaringan nirkabel tidak begitu saja dapat digunakan. Diperlukan suatu tahapan lanjutan yaitu melakukan proses penetrasi terhadap jaringan komputer nirkabel tersebut agar dapat berjalan sesuai dengan tujuan pembangunan jaringan tersebut. Selain dilakukan proses penetrasi perlu juga dilakukan evaluasi terhadap ketersediaan, kerahasiaan, dan integrasi pada jaringan, agar performa dari jaringan nirkabel yang dibangun mencapai titik maksimal, selain mengevaluasi performa perlu juga dilakukan evaluasi keamanan dari jaringan nirkabel yang dibuat sehingga diketahui celah-celah keamanan yang terdapat pada sistem sehingga dapat dibuat suatu model sistem keamanan yang baik.

Penelitian sebelumnya menyatakan bahwa dengan jaringan yang menggunakan nirkabel dimana implementasinya menggunakan frekuensi yang sifatnya terbuka dibandingkan dengan menggunakan kabel, maka kerentanan keamanan jalur komunikasi akan lebih berbahaya dibandingkan dengan menggunakan kabel. Kerentanan tersebut terjadi pada seluruh lapisan *protocol* yang dimiliki pada jaringan komunikasi nirkabel [2]. Selain itu juga seperti yang sudah diteliti pada jaringan komputer nirkabel pada KPFT-UGM dengan melakukan *penetration test* berupa *Mac Address spoofing, authentication attack, DoS, MITM, Eavesdropping, WEP cracking*. Sistem otentikasi digunakan untuk perpaduan *Captive Portal* dengan *Server Otentikasi* belum cukup dipercaya untuk melawan *MAC Address spoofing, authentication attack, dan denial of service attack*. Implementasi kombinasi model keamanan otentikasi *server, captive portal, firewall*, serta *WPA/WPA2* pada penelitian tersebut dapat meningkatkan tingkat keamanan dari celah-celah kebocoran dan mekanisme keamanan jaringan nirkabel pun meningkat [3].

Berdasarkan analisis kelemahan celah lapisan keamanan pada jaringan nirkabel adapun beberapa upaya pengamanan jaringan nirkabel dapat dilakukan dengan menyembunyikan SSID, menggunakan kunci WEP, kunci WPA-PSK atau WPA2-PSK, memanfaatkan MAC Filtering, menggunakan *Captive Portal*, Ganti Password Admin secara berkala, matikan SSID broadcasting, dan Matikan WAP saat tidak digunakan [4]. Berdasarkan kelemahan tersebut yang mempengaruhi penelitian analisis dan evaluasi tingkat keamanan jaringan nirkabel yang menjelaskan bahwa analisis dan evaluasi keamanan terhadap tingkat keamanan jaringan komputer nirkabel pada STMIK Mataram dapat dilakukan dengan metode *penetration testing* seperti *spoofing Mac Address, authentication attack, denial of service, Man In The Middle Attack, dan Eavesdropping* [5].

Berdasarkan penelitian-penelitian sebelumnya diatas, untuk itu di instansi Politeknik Ganesha Guru perlu melakukan analisis dan evaluasi terhadap jaringan komputer nirkabel dikarenakan jaringan nirkabel sendiri sangat rentan terhadap serangan selain itu juga pada instansi sendiri juga terdapat beberapa sistem yang harus dijaga keamanannya agar tidak terjadi kerusakan. Sehingga dengan dilakukannya penelitian ini Keamanan pada jaringan komputer nirkabel di Instansi Politeknik Ganesha Guru dapat ditingkatkan.

2. KAJIAN TEORI

Jaringan komputer adalah himpunan *interkoneksi* antara dua komputer *autonomous* atau lebih yang terhubung. Untuk menghubungkan dua buah komputer *autonomous* diperlukan beberapa

perangkat yang menjadi perantara dari kedua komputer tersebut seperti *switch*, *router*, akses point, dan juga media perantara untuk mengirim data antar dua buah komputer tersebut dapat menggunakan kabel maupun tanpa menggunakan kabel atau dikenal dengan istilahnya adalah *wireless* (nirkabel). Jenis kabel yang biasa digunakan untuk perantara dua buah komputer adalah kabel *Unshielded Twisted Pair* [1].

Wireless (nirkabel) merupakan sebuah teknologi yang dapat digunakan untuk menghubungkan 2 buah piranti yang berupa komputer, laptop maupun *mobile phonet* tanpa menggunakan kabel untuk bertukar data maupun informasi. Salah satu perangkat umum yang digunakan berkomunikasi dalam jaringan lokal nirkabel (*Wireless Local Area Network/WLAN*) adalah *Wireless Fidelity (WiFi)* berdasarkan spesifikasi *IEEE 802.11*. Hal tersebut merupakan standar yang umum digunakan pada komunikasi nirkabel secara internasional. [6].

A. WLAN (Wireless Local Area Network)

Wireless Local Area Network merupakan sistem komunikasi dengan cakupan yang kecil atau biasa dikenal dengan *Local Area Network* yang sifatnya fleksibel dimana pengirim dan penerima datanya melalui media udara dengan menggunakan teknologi frekuensi radio. Sehingga perangkat dapat bergerak dengan mudah dikarenakan tidak terikat dengan kabel. WLAN sendiri dapat digolongkan menjadi 2 kategori utama yaitu :

a) *Wireless LAN modus Ad-Hoc*

Pada model jaringan modus *ad-hoc*, jaringan antara satu perangkat dengan perangkat yang lain dilakukan secara spontan/langsung tanpa melalui konfigurasi tertentu selama signal dari pemancar yakni *transmitter* dapat diterima dengan baik oleh perangkat- perangkat penerima yakni *receiver*.

b) *Wireless LAN modus Infrastruktur*

Pada model jaringan modus *infrastruktur*, model ini memberikan koneksi antara perangkat yang terhubung ke dalam jaringan WLAN, diperlukan suatu *intermediary device* berupa *access point* yang terhubung dalam jaringan komputer kabel, sebelum melakukan *transmisi* kepada perangkat-perangkat penerima *signal* [7][8].

Kerentanan jaringan nirkabel (*Wireless LAN*) terhadap keamanan data, informasi, dan ketersediaan layanan menjadi topik yang menjadi perhatian dan perbincangan dikalangan praktisi. Untuk itu, dikemukakan dalam suatu teori bahwa suatu jaringan komputer dikatakan aman dan andal apabila memenuhi unsur-unsur berikut:

a) *Privacy dan Confidentiality:*

Suatu mekanisme yang dilakukan untuk melindungi suatu informasi dari pengguna jaringan yang tidak memiliki hak, sedangkan *confidentiality* lebih mengarah kepada tujuan dari informasi yang diberikan dan hanya boleh untuk tujuan tersebut saja.

b) *Integrity:*

Aspek yang mengutamakan akses informasi yang ditujukan untuk pengguna tertentu, di mana integritas dari informasi tersebut masih terjaga.

c) *Authentication:*

Pada bagian ini mengutamakan validitas dari user yang melakukan akses terhadap suatu data, informasi, atau layanan dari suatu institusi.

d) *Availability:*

Aspek yang berhubungan dengan ketersediaan data, informasi, atau layanan, ketika data, informasi atau layanan tersebut diperlukan.

e) *Access Control:*

Aspek ini berhubungan dengan klasifikasi pengguna dan cara pengaksesan informasi yang dilakukan oleh pengguna.

f) *Non Repudiation:*

Aspek yang berkaitan dengan pencatatan pengguna, yang bertujuan untuk menghindari penyangkalan pengguna yang pernah merambah layanan, data maupun informasi yang tersedia [9].

Jaringan wireless LAN saat ini sudah dipergunakan banyak instansi maupun perorangan. Hal tersebut menyebabkan pentingnya aspek keamanan diperhatikan karena banyaknya celah serangan yang dapat terjadi pada jaringan wireless. Berbagai serangan yang umumnya muncul pada jaringan wireless adalah sebagai berikut :

a) *Reveal SSID:*

Usaha serangan yang dilakukan dengan menyingkap SSID dari *access point* yang sengaja disembunyikan oleh administrator jaringan komputer.

b) MAC Address Spoofing:

Usaha seorang peretas menembus keamanan MAC Address filtering dengan memanfaatkan proses spoofing MAC Address, kemudian MAC Address pengguna yang sah dimanfaatkan untuk terhubung kedalam jaringan komputer dan menggunakan sesuai keinginan.

c) Authentication Attack:

Dilakukan penyerangan terhadap authentication user yang sah. Hal tersebut menyebabkan pengguna yang sah tidak dapat mengakses layanan menggunakan autentikasi yang dimilikinya, hal tersebut memutus hal pengguna masuk ke dalam jaringan nir kabel. Penyerang dimanfaatkan biasanya untuk mendapatkan sumberdaya yang lebih dalam menggunakan layanan jaringan.

d) Eavesdropping:

Serangan ini menyerang pengguna yang berada dalam jaringan komputer yang tidak terenkripsi menggunakan teknik enkripsi apapun. Penyerang melakukan aksinya dengan dengan semua paket yang ditransmisikan oleh pengguna didengarkan dan dimanfaatkan untuk tujuan tertentu.

e) Session Hijacking:

Serangan dilakukan dalam suatu sesi disaat seorang pengguna menggunakan hak aksesnya. Hal tersebut dimanfaatkan untuk mendapatkan suatu hak akses ke layanan yang sedang diakses oleh pengguna sah tersebut.

f) Man In The Middle Attack:

Serangan yang dilakukan dengan cara spoofing terhadap pengguna sah. Spoofing menyebabkan transmisi yang dilakukan target malah menuju penyerang, sehingga penyerang mendapatkan semua informasi yang ditransmisikan oleh target.

g) Denial of Service:

Serangan yang menyerang ketersediaan sumber daya sehingga menyebabkan pengguna sah mengalami koneksi terputus dari jaringan komputer.

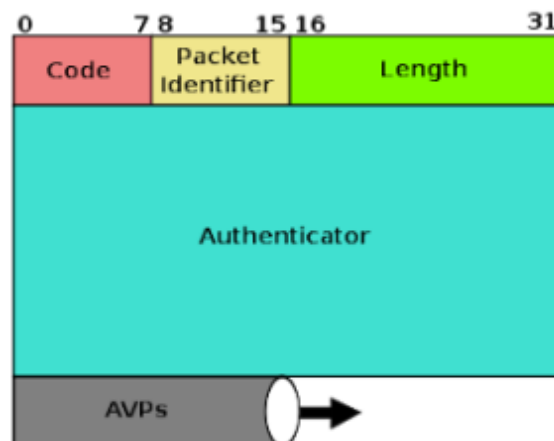
h) Rogue Access Point:

Serangan yang menggunakan suatu perangkat access point yang dibuat sama dengan access point yang berada pada suatu institusi. Sehingga ketika pengguna sah melakukan akses ke *access point* [3].

B. RADIUS (Remote Authentication Dial-In User Service)

RADIUS adalah sebuah protokol keamanan komputer yang digunakan untuk melakukan autentikasi, otorisasi dan pendaftaran akun pengguna secara terpusat untuk mengakses jaringan. Server Autentikasi merupakan perangkat keamanan pada suatu jaringan komputer yang menerapkan proses autentikasi untuk melayani permintaan autentikasi dari pengguna layanan jaringan. *Server autentikasi* ini menerapkan model AAA (*authentication, authorization, dan accounting*).

Authentication adalah proses pengesahan identitas pengguna (end-user) dalam mengakses jaringan. Sedangkan accounting adalah proses komputasi yang dilakukan oleh sistem dengan pencatatan sumberdaya yang telah dipakai oleh pengguna jaringan komputer nirkabel. *RADIUS* memiliki suatu format paket yang digunakan dalam melakukan transmisi data [10].



Gambar 1. Protokol (Format Paket) RADIUS
(Sumber : Prihanto, 2014 [10])

a) Code :

memiliki panjang satu oktet (8 bit) dan digunakan untuk membedakan tipe pesan RADIUS yang dikirimkan pada paket. Berikut adalah kode-kode tersebut (dalam desimal) antara lain.

Tabel 1. Code pada Protokol RADIUS

Kode	Deskripsi
1	<i>Access – Request</i>
2	<i>Access – Accept</i>
3	<i>Access – Reject</i>
4	<i>Accounting – Request</i>
5	<i>Accounting – Respond</i>
11	<i>Access Challenge</i>
12	<i>Status – Server</i>
13	<i>Status – Client</i>
255	<i>Reserver</i>

b) Packet Identifier :

memiliki panjang satu oktet (8 bit) dan bertujuan untuk mencocokkan permintaan client dan paket respon yang diberikan oleh server RADIUS.

c) Length :

memiliki panjang dua oktet (16 bit), memberikan informasi mengenai panjang paket, termasuk didalamnya adalah code, identifier, length, authenticator, atribut.

d) Authenticator :

memiliki panjang 16 oktet (128 bit), digunakan untuk membuktikan balasan dari RADIUS server, selain itu digunakan juga untuk algoritma password.

e) Atributs :

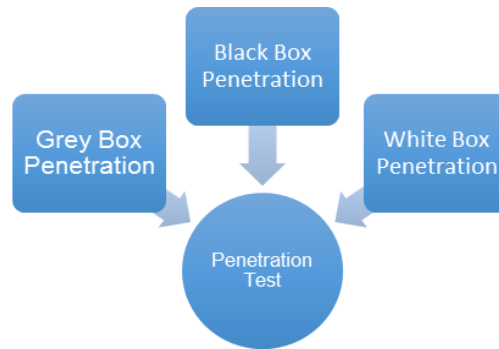
Atribut berisi informasi yang dibawa pesan RADIUS. Setiap pesan dapat membawa satu atau lebih atribut. Contoh atribut RADIUS: nama pengguna, password, CHAP-password, alamat IP access point (AP), pesan balasan. Bagian paket ini berisi autentikasi, otorisasi, informasi dan detail konfigurasi spesifik yang diperlukan untuk permintaan dari client RADIUS ataupun NAS.

Dalam penerapannya, RADIUS server dipadukan dengan *captive portal* yang merupakan suatu teknik routing traffic untuk melakukan autentikasi dan pengamanan data yang melewati jaringan internal ke jaringan eksternal dengan membelokkan traffic pengguna ke sebuah halaman login [11].

C. Penetration Test

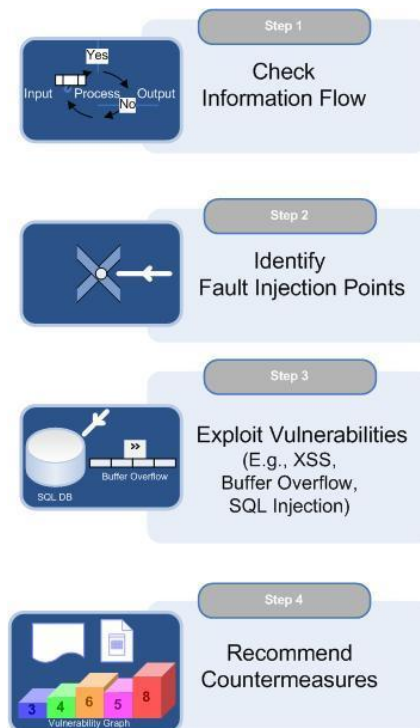
Penetration test atau biasa disebut dengan Pentest merupakan sebuah metode yang digunakan untuk mengevaluasi keamanan dari sebuah sistem maupun keamanan pada jaringan komputer. Evaluasi tersebut dilakukan dengan cara melakukan sebuah simulasi serangan (*attack*). Hasil dari pentest tersebut sangat penting bagi administrator sebagai umpan balik dari sistem atau jaringan komputernya, yang kemudian diperbaiki tingkat keamanan dari sistem komputernya, selain itu juga akan diberikan masukan terhadap kondisi *vulnerabilitas* sistem sehingga memudahkan dalam melaksanakan evaluasi dari sistem keamanan komputer yang sedang berjalan. Aktifitas pentes juga dikenal dengan istilah “ethical hacking”.

Berbagai metode pentest yang dapat digunakan antara lain: *black box*, *white box* dan *grey box*. *Black box testing* adalah metode pentest yang mengasumsikan tester tidak mengetahui sama sekali infrastruktur dari target pentest. Sehingga, tester dengan metode ini harus mencoba menggali dari awal semua informasi yang diperlukan kemudian melakukan analisis serta menentukan jenis serangan yang akan dilakukan. Pada *White box testing* terjadi sebaliknya, tester telah mengetahui semua informasi yang diperlukan untuk melakukan pentest. Sementara *grey box* mengkombinasikan dari kondisi *black box* dan *white box*. Istilah lain dari *white box* adalah *full disclosure*, *grey box* adalah *partial disclosure* dan *black box* adalah *blind disclosure*.



Gambar 2. Metode *Penetration Test*

Secara umum terdapat empat langkah dasar yang dilakukan untuk aktivitas pentest yaitu 1) mengumpulkan sejumlah informasi penting dari sistem, 2) Melakukan analisis untuk menentukan jenis serangan yang akan dilakukan, 3) Melakukan aktivitas serangan untuk mengeksploitasi *vulnerabilitas* sistem, dan 4) Melakukan laporan serta rekomendasi untuk perbaikan sistem [5].



Gambar 3. Langkah dasar dalam aktivitas *Penetration Test*
(Sumber : Samsunar, 2017 [5])

3. METODE EVALUASI JARINGAN

Mekanisme evaluasi keamanan jaringan komputer nirkabel pada Politeknik Ganesha Guru dilakukan dengan cara membangun jaringan simulasi jaringan komputer nirkabel Politeknik Ganesha Guru dengan mensimulasikan substansi – substansi keamanan jaringan yang terdapat pada Politeknik Ganesha Guru. Pengujian dilakukan pada jaringan simulasi, dilakukan dengan melakukan *Vulnerability Assesment (VA)* dan *penetration test* dengan menyerang jaringan simulasi dengan menggunakan serangan-serangan yang mungkin muncul pada jaringan komputer nirkabel yang sesuai pada studi kasus. Serangan sesuai untuk jaringan simulasi tersebut adalah MAC address spoofing, authentication attack, denial of service, eavesdropping, man in the middle attack, dan WEP cracking.

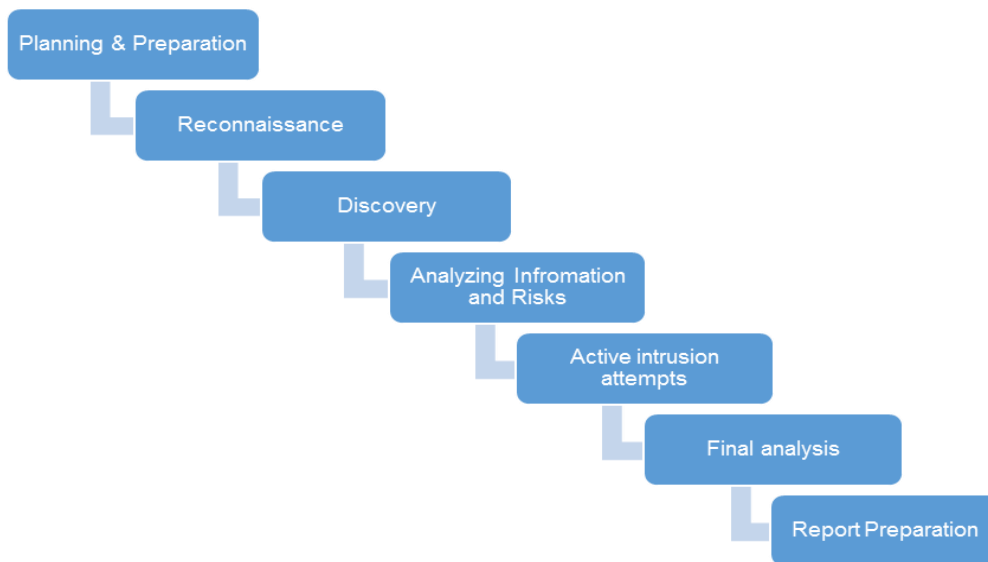
A. Vulnerability Assesment (VA)

Adapun tujuan melakukan VA adalah sebagai upaya untuk mengetahui apa yang perlu diperbaiki dari sistemnya agar sistemnya cukup tangguh dari potensi kegagalan ataupun potensi

dibobol *hacker/cracker*. Hasil dari VA adalah daftar kelemahan yang dimiliki oleh sistem dan penyebabnya serta rekomendasi untuk memperbaiki kelemahan ataupun menutup lubang keamanan yang masih ada. uji *vulnerability assessment* (VA) meliputi : 1) Katalog aset-aset dan resources pada sebuah sistem , 2) Menetapkan nilai ukur dan tingkat kepentingan resources , 3) Identifikasi kerentanan keamanan atau potensial ancaman pada setiap resource, dan 4) Mengurangi atau menghilangkan kerentanan yang sangat serius untuk resource yang sangat berharga [5].

B. Penetration Test (Pentest)

Penetration test dilakukan untuk mengetahui lubang atau celah keamanan yang terdapat pada jaringan komputer nirkabel Politeknik Ganesha Guru. *Penetration test* meliputi 1) Penentuan lingkup, 2) Mengumpulkan informasi target dan atau pengintaian, 3) Upaya eksploitasi untuk mendapat akses dan eskalasi, 4) Uji data sensitif yang terkumpul, dan 5) Membersihkan jejak pengintaian dan melakukan pelaporan. Secara umum langkah-langkah yang dilakukan dalam Pentest adalah sebagai berikut [5]:



Gambar 4. Tahapan metode Pentest

a) **Planning and Preparation :**

Menentukan tujuan dan sasaran yang akan dicapai dalam proses *penetration testing* assessment. Langkah pertama *planning and preparation* ditujukan agar selama proses testing dari tahap ke tahap bisa di-runtut secara mudah dan jelas, secara umum *planning and preparation* berfokus pada langkah identifikasi *vulnerabilities* dan peningkatan dari segi keamanan.

b) **Reconnaissance :**

Reconnaissance bisa disebut dengan pengumpulan data bisa dikategorikan sebagai *passive penetration testing* karena dalam langkah *reconnaissance* pengumpulan data dilakukan secara manual, bisa lewat dokumentasi pihak terkait ataupun informasi terbuka yang ditanyakan langsung pada pihak yang terkait dengan sistem.

c) **Discovery :**

Discovery merupakan langkah di mana dilakukan pengumpulan informasi dengan menggunakan *automated tool* untuk memindai *vulnerabilities* (kerentanan) pada sistem termasuk didalamnya pemindaian terhadap jaringan, server, perangkat, maupun data.

d) **Analyzing information and risk :**

merupakan tahap di mana dilakukan analisa terperinci terhadap informasi yang telah didapatkan sebelumnya (tahap *reconnaissance* dan *discovery*) untuk menemukan resiko dan celah keamanan yang bisa ditimbulkan dari kerentanan sistem yang terpasang.

e) **Active intrusion attempts :**

merupakan tahap di mana diberikan semacam instruksi (petunjuk, arahan) secara aktif dari segi keamanan sistem sehingga kerentanan yang ditemukan bisa diperbaiki/ disempurnakan keamanannya.

f) Final analysis :

Analisa akhir secara keseluruhan memberikan pernyataan terhadap segala temuan dan petunjuk teknis perbaikan sisi keamanan setelah adanya skema sistematis analisa.

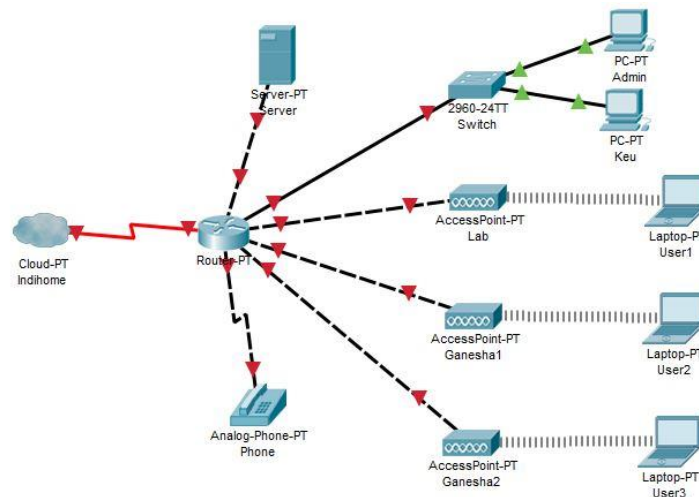
g) Report preparation :

Tahap akhir dari kegiatan pentest adalah memberikan laporan hasil investigasi dan rekomendasi terhadap pihak yang terkait dan bertanggungjawab dengan sistem untuk dijadikan acuan pembenahan dari segi keamanan sistem.

Hasil dari *Vulnerable* dan *penetration testing* mendapatkan suatu hasil yang dapat dianalisis dan dievaluasi untuk mendapatkan suatu model keamanan jaringan komputer nirkabel yang digunakan untuk menutup lubang atau celah keamanan jaringan komputer nirkabel di Politeknik Ganesha Guru, yang dilanjutkan dengan melakukan pengujian terhadap model yang telah dibuat untuk memastikan model yang digunakan sudah benar dan tepat.

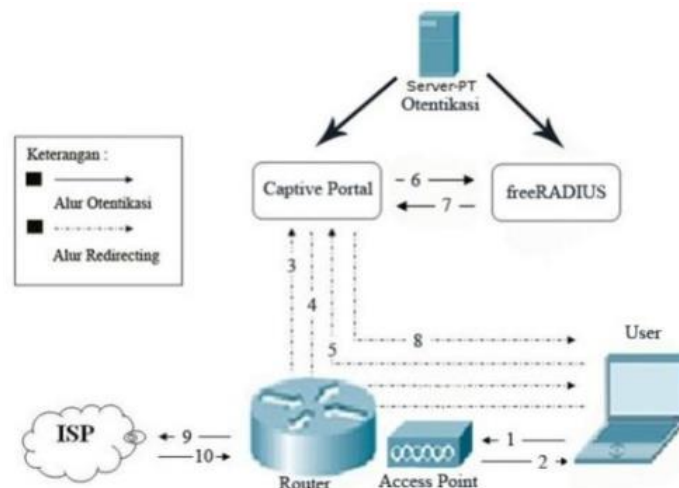
4. SIMULASI

Untuk melakukan simulasi terhadap jaringan komputer nirkabel Politeknik ganesha guru, dibutuhkan topologi jaringan yang sesuai untuk menggambarkan keadaan jaringan pada studi kasus.



Gambar 5. Topologi Jaringan Komputer Nirkabel di Politeknik Ganesha Guru

Pada gambar 5 di atas, merupakan topologi jaringan komputer nirkabel di Politeknik Ganesha Guru. Dalam topologi tersebut hanya menggunakan satu buah model keamanan. Model keamanan menggunakan mekanisme keamanan dengan server autentikasi RADIUS dengan menggunakan *captive portal* untuk meredirect pengguna ke halaman autentikasi.



Gambar 6. Model Keamanan Akses Jaringan Nirkabel Politeknik Ganesha Guru

Pada gambar 6 diatas, terdapat mekanisme autentikasi yang diwakilkan oleh penomoran yang tertera pada gambar untuk menunjukkan mekanisme autentikasi yang diberlakukan pada setiap bagian yang ada di kampus Politeknik Ganesha Guru. Setelah mendapatkan informasi mengenai mekanisme keamanan jaringan komputer nirkabel yang digunakan, berikutnya adalah merancang konfigurasi untuk server RADIUS yang dipadukan dengan *captive portal*. Konfigurasi *captive portal* dan RADIUS yang dibangun menampilkan tampilan seperti yang ditunjukkan pada gambar 7.



Gambar 7. *Captive Portal* Politeknik Ganesha Guru

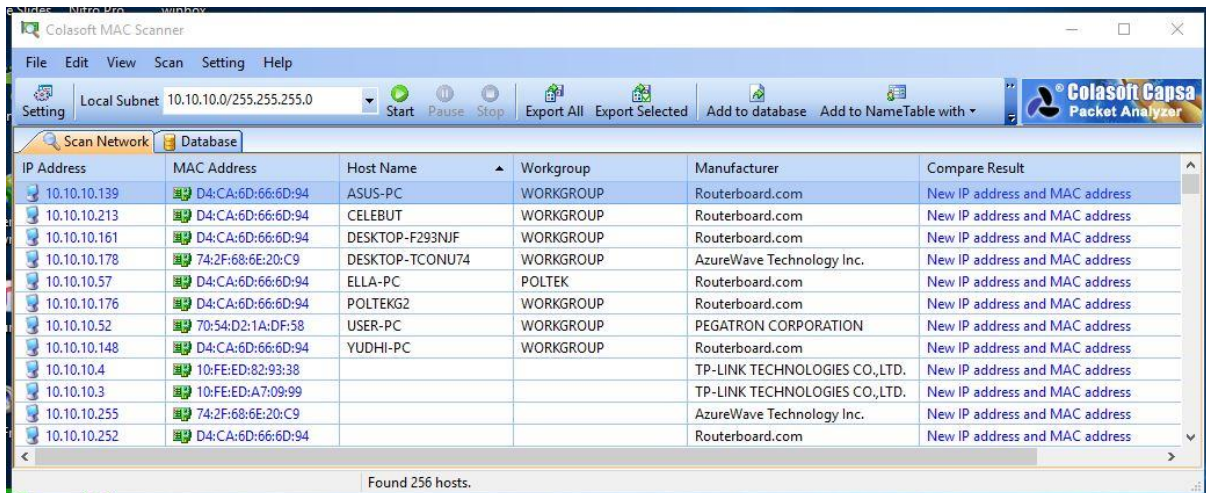
5. PENGUJIAN DAN ANALISIS

Seperti yang sudah dijelaskan pada bab sebelumnya, untuk mengetahui rentan atau tidaknya jaringan nirkabel di Politeknik Ganesha Guru dilakukan pengujian dengan *Vulnerability Assessment* dan juga *Penetration Test*. Melakukan *Vulnerability Assessment* bertujuan untuk mengetahui nilai kerentanan dari jaringan nirkabel yang dibuat, sedangkan dengan *Penetration Test* dilakukan untuk mengetahui celah keamanan yang terdapat di jaringan nirkabel Politeknik Ganesha Guru. Tabel 2 berikut merupakan *Penetration Test* yang dilakukan di jaringan nirkabel politeknik ganesha guru.

Tabel 2. *Penetration Testing* di Politeknik Ganesha Guru

Jenis Serangan	Informasi yang diperlukan	Status Serangan
<i>Man In The Middle Attack</i>	Port yang terbuka di server, IP address user yang terhubung dalam jaringan Nirkabel	Gagal
<i>Eavesdropping</i>	Penyerang harus ada di dalam jaringan komputer nirkabel	Gagal
<i>Denial of Service</i>	Daftar IP address dari user yang terhubung dalam jaringan nirkabel	Berhasil
<i>Authentication Attack Tunggal</i>	Daftar Mac Address User yang terhubung dalam jaringan nirkabel	Berhasil
<i>Mac Address Spoofing</i>	Daftar Mac Address yang terhubung dalam jaringan nirkabel	Berhasil

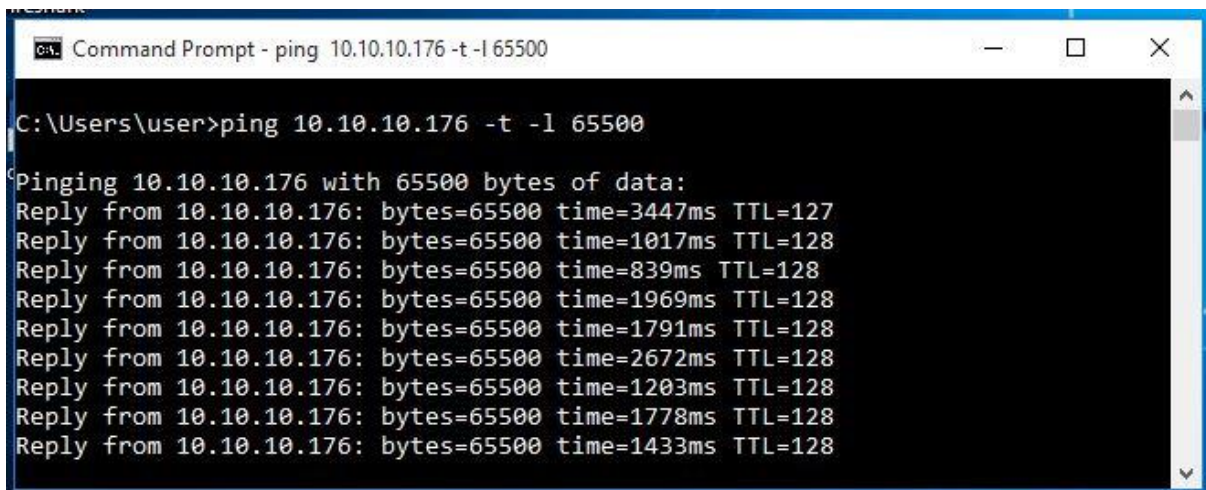
Dari hasil pentest tersebut didapatkan bahwa dengan menggunakan *captive portal* dengan RADIUS authentication server serangan *Man In The Middle Attack* dan *Eavesdropping* gagal terjadi. Namun beberapa serangan seperti *Denial of Service*, *Authentication Attack Tunggal* dan *Mac Address Spoofing* masih dapat dilakukan pada jaringan nirkabel dengan tambahan *captive portal* dengan Radius Authentication. Sebagai dasar dalam melakukan penyerangan adalah dengan melakukan pengumpulan informasi terkait IP Address dan Mac Address komputer user maupun server yang terhubung ke jaringan. Untuk melakukan pengumpulan informasi tersebut diperlukan sebuah aplikasi. Gambar 8 berikut merupakan hasil scanning/pengumpulan informasi IP Address dan Mac Address di jaringan nirkabel Politeknik Ganesha Guru.



IP Address	MAC Address	Host Name	Workgroup	Manufacturer	Compare Result
10.10.10.139	D4:CA:6D:66:6D:94	ASUS-PC	WORKGROUP	Routerboard.com	New IP address and MAC address
10.10.10.213	D4:CA:6D:66:6D:94	CELEBUT	WORKGROUP	Routerboard.com	New IP address and MAC address
10.10.10.161	D4:CA:6D:66:6D:94	DESKTOP-F293NJF	WORKGROUP	Routerboard.com	New IP address and MAC address
10.10.10.178	74:2F:68:6E:20:C9	DESKTOP-TCONU74	WORKGROUP	AzureWave Technology Inc.	New IP address and MAC address
10.10.10.57	D4:CA:6D:66:6D:94	ELLA-PC	POLTEK	Routerboard.com	New IP address and MAC address
10.10.10.176	D4:CA:6D:66:6D:94	POLTEKG2	WORKGROUP	Routerboard.com	New IP address and MAC address
10.10.10.52	70:54:D2:1A:DF:58	USER-PC	WORKGROUP	PEGATRON CORPORATION	New IP address and MAC address
10.10.10.148	D4:CA:6D:66:6D:94	YUDHI-PC	WORKGROUP	Routerboard.com	New IP address and MAC address
10.10.10.4	10:FE:ED:82:93:38			TP-LINK TECHNOLOGIES CO.,LTD.	New IP address and MAC address
10.10.10.3	10:FE:ED:A7:09:99			TP-LINK TECHNOLOGIES CO.,LTD.	New IP address and MAC address
10.10.10.255	74:2F:68:6E:20:C9			AzureWave Technology Inc.	New IP address and MAC address
10.10.10.252	D4:CA:6D:66:6D:94			Routerboard.com	New IP address and MAC address

Gambar 8. Hasil Scanning IP Address dan Mac Address

Dari hasil scanning tersebut dapat dilakukan tindakan selanjutnya seperti melakukan Denial of Service, Autenticatin Tunggal, dan Mac Address Spoofing. Salah satu contoh serangan yang dilakukan pada pengujian kali ini adalah dengan menggunakan serangan Denial of Service atau biasa di kenal dengan DoS Attack. DoS attack merupakan serangan dengan membanjiri jaringan korban dengan paket UDP. Jenis serangan DoS adalah Syn Attack, Ping of Death, Buffer overflow, Teardrop, dan Smurf. Pada pengujian kali ini menggunakan serangan Ping of Death, yang merupakan menyerang komputer target dengan mengirimkan Ping melalui Terminal namun dengan paket yang cukup besar. Dalam sekali melakukan Ping dapat mengirimkan paket sebesar 65500 bytes. Gambar 9 merupakan contoh dalam melakukan Ping of Death.



```
Command Prompt - ping 10.10.10.176 -t -l 65500

C:\Users\user>ping 10.10.10.176 -t -l 65500

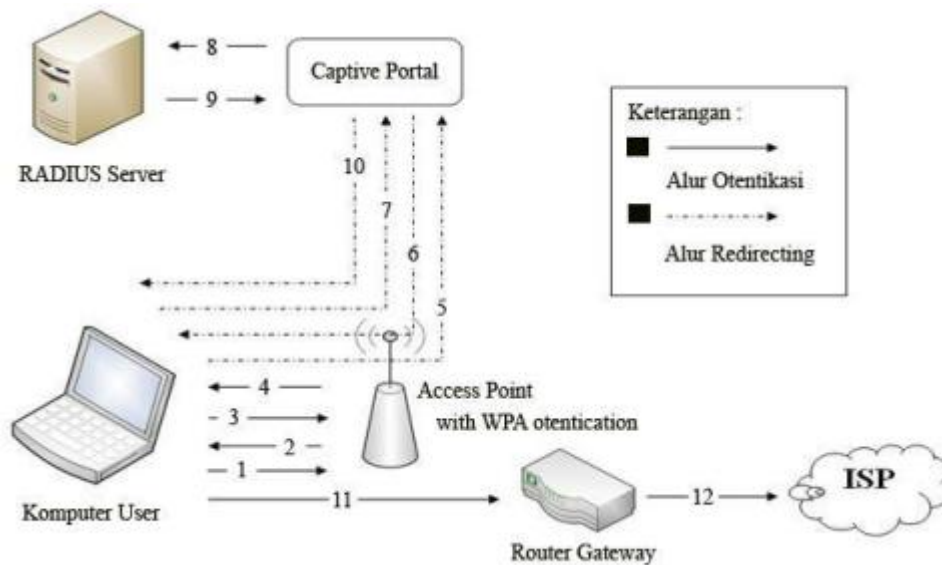
Pinging 10.10.10.176 with 65500 bytes of data:
Reply from 10.10.10.176: bytes=65500 time=3447ms TTL=127
Reply from 10.10.10.176: bytes=65500 time=1017ms TTL=128
Reply from 10.10.10.176: bytes=65500 time=839ms TTL=128
Reply from 10.10.10.176: bytes=65500 time=1969ms TTL=128
Reply from 10.10.10.176: bytes=65500 time=1791ms TTL=128
Reply from 10.10.10.176: bytes=65500 time=2672ms TTL=128
Reply from 10.10.10.176: bytes=65500 time=1203ms TTL=128
Reply from 10.10.10.176: bytes=65500 time=1778ms TTL=128
Reply from 10.10.10.176: bytes=65500 time=1433ms TTL=128
```

Gambar 9. Serangan Ping Of Death

Perintah yang dimasukkan untuk melakukan Ping of Death adalah Ping <ip target> -t -l 65500. Yang harus diketahui terlebih dahulu adalah alamat IP target, dapat menggunakan tools pada Gambar 8. Kemudian -t merupakan perintah untuk mengirimkan paket data secara terus menerus, dan -l adalah perintah untuk mengirimkan paket dengan besaran yang sudah ditentukan yaitu 65500. Dengan membebani komputer target akan menyebabkan aktifitas jaringan akan semakin besar dan komputer akan semakin lambat dalam pembacaan packet data yang diterima maupun dikirim.

Agar dapat menghalau segala jenis serangan pada jaringan nirkabel tersebut diperlukan suatu lapisan keamanan sehingga dengan cepat mencegah user yang tidak memiliki hak tidak dapat terhubung dengan jaringan yang dimiliki. Pada jaringan nirkabel sendiri terdapat lapisan keamanan tambahan yang dapat digunakan berupa autentikasi pada layer 2, berupa lapisan yang menggunakan teknologi enkripsi. Teknologi autentikasi dengan enkripsi ini ada beberapa macam, seperti WPA (Wi-Fi Protected Access) dan WPA2 (Wi-Fi Protected Access2). Dengan perkembangan teknologi saat ini, dalam membangun jaringan komputer nirkabel diperlukan autentikasi keamanan yang lebih baik, yaitu

dengan menggunakan autentikasi WPA/WPA2. Dengan menambahkan lapisan autentikasi WPA/WPA2 dipadukan dengan server autentikasi RADIUS memberikan mekanisme keamanan jaringan komputer nirkabel yang berlapis. Pada gambar 8 berikut merupakan gambaran keamanan jaringan nirkabel yang memadukan *Captive Portal*, Server Radius dan juga penambahan WPA/WPA2.



Gambar 10. Model Keamanan Jaringan Komputer Nirkabel dengan WPA Authentication dan RADIUS
(Sumber : Manuaba, 2013 [3])

Jaringan komputer nirkabel dengan menggunakan dua lapisan keamanan WPA/WPA2 dan server autentikasi RADIUS yang dikombinasikan dengan menggunakan *captive portal*. User akan diredirect ke halaman autentikasi ke *Captive Portal* ketika melakukan akses jaringan melalui web browser. Server RADIUS akan berasosiasi dengan *Captive Portal* di dalam proses validasi username dan kata kunci yang dikirimkan oleh pengguna. Dari hasil pengujian didapatkan apabila penyerang tidak mengetahui kata kunci WPA authentication maka serangan seperti Man In The Middle Attack, Eavesdropping, Denial of Service, Authentication Attack Tunggal, dan juga Mac Address Spoofing tidak akan dapat dilakukan, atau status serangannya menjadi gagal.

6. KESIMPULAN DAN SARAN

Berdasarkan hasil pengujian jaringan komputer nirkabel sebelum menggunakan dan setelah menggunakan WPA/WPA2 jaringan komputer nirkabel di Politeknik Ganesha Guru dapat di analisis dan evaluasi dengan menggunakan *Vulnerability Assesment* dan *Penetration Test* Seperti *Man In The Middle Attack*, *Eavesdropping*, *Denial of Service*, *Authentication Attack* Tunggal, dan *Mac Address Spoofing*. Dari pengujian didapatkan jaringan nirkabel yang menggunakan *Captive Portal* dan RADIUS Server dapat menangkal *Man In The Middle Attack* dan *Eavesdropping* namun tidak dapat menghalau *Denial of Service*, *Authentication Attack* Tunggal dan *Mac Address Spoofing*. Sedangkan dengan ditamhkannya lapisan autentikasi dengan enkripsi seperti WPA atau WPA2 segala jenis serangan *Penetration Test* dapat digagalkan. Saran kedepannya kemaan jaringan nirkabel dapat menggunakan autentikasi selain WPA/WPA2. Selain dengan autentikasi untuk menjaga keamanan server perlu juga ditambahkan *firewall* sehingga segala jenis serangan ke server dapat dihalau, atau juga bisa menambahkan *honeypot*.

DAFTAR PUSTAKA

- [1] M Syafrizal, *Pengantar Jaringan Komputer*. Yogyakarta: Andi, 2005.
- [2] Aji Supriyanto, "Analisis Kelemahan Keamanan pada Jaringan Wireless," *J. Teknol. Infromasi Din.*, 2006.
- [3] S. S. K. Ida Bagus Verry Hendrawan Manuaba, Risanuri Hidayat, "Evaluasi Keamanan Akses Jaringan Komputer Nirkabel (Kasus : Kantor Pusat Fakultas Teknik Universitas Gadjah mada)," *JNTETI*, 2013.
- [4] Rico, "Analisis Kelemahan Celah Lapisan Keamanan Pada Jaringan Nirkabel," vol. 9, no. 1, pp. 8–20, 2012.

- [5] L. D. Samsumar, K. Gunawan, D. Program, S. Manajemen, D. Program, and S. Komputerisasi, "Analisis Dan Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel (Wireless Lan); Studi Kasus Di Kampus Stmik Mataram," vol. IV, no. 1, pp. 73–82, 2017.
- [6] I Sofana, *Membangun Jaringan Komputer*. Bandung: Informatika, 2013.
- [7] P. P. ROMADHON, "Skripsi ini diajukan sebagai syarat memperoleh gelar Sarjana Komputer di Universitas Bina Darma," Palembang, 2014.
- [8] S'to, *Wireless Kung FU : Networking & Hacking*. Jakarta: Jasakom, 2015.
- [9] S. Garfinkel, G. Spafford, and A. Schwartz, "Practical UNIX and Internet Security," *Computer (Long. Beach. Calif)*., 2003.
- [10] A. Prihanto, "Membangun Radius Server Untuk Keamanan Wifi Kampus," *J. simanteC*, 2010.
- [11] D. Wiliyana, "Perancangan Jaringan LAN dan Keamanan Wireless Internet Hotspot Berbasis Mikrotik Router Pada Pomdam IV Sriwijaya," Palembang, 2013.