ISSN : 2407 - 3911

ANALISIS DAN EVALUASI TINGKAT KEAMANAN JARINGAN KOMPUTER NIRKABEL (*WIRELESS LAN*); STUDI KASUS DI KAMPUS STMIK MATARAM

Lalu Delsi Samsumar[1)], Karya Gunawan[2)]
[1)] Dosen Program Studi Manajemen Informatika, [2)] Dosen Program Studi Komputerisasi Akuntansi
Sekolah Tinggi Manajemen Informatika Komputer (STMIK) Mataram
Jl. Pelor Mas III Kampus STMIK-ASM Mataram, Kekalik Kota Mataram NTB
Surel : [1)] lalu.ellsyam@gmail.com

ABSTRAK

Perkembangan teknologi informasi saat ini telah berkembang dengan sangat pesat, terutama dalam hal penggunaan jaringan komputer nirkabel. Penggunaan teknologi internet semakin banyak dan tidak terkontrol, hal ini disebabkan karena banyaknya pengguna internet di dunia, dan hampir semua lapisan masyarakat mengetahui tentang adanya internet dan cara mengaksesnya. Fenomena saat ini, banyak instansi-instansi pemerintah maupun swasta yang telah memanfaatkan teknologi nirkabel untuk mengkoneksikan perangkatnya, sehingga dapat menyelesaikan tugas-tugasnya dengan cepat. Namun hal ini membuat seorang administrator jaringan komputer untuk berfikir dan bekerja keras dalam membangun sebuah koneksi yang bersifat *secure* dan *private.*

Seiring dengan perkembangan teknologi tersebut dibutuhkan kemampuan untuk dapat memecahkan persoalan-persoalan yang semakin kompleks dan rumit seperti persoalan terkait dengan keamanan jaringan komputer khusunya jaringan yang berbasis jaringan nirkabel. Untuk memelihara dan menjaga stabilitas jaringan agar tetap memadai dibutuhkan evaluasi dan analisis penilaian secara berkala. Penelitian ini menghasilkan sebuah model sebagai hasil dari penilaian yang dapat digunakan sebagai referensi untuk mengembangkan dan meningkatkan keamanan akses jaringan komputer nirkabel pada jaringan kampus STMIK Mataram.

Kata kunci : analisis, jaringan nirkabel, keamanan jaringan, wireless LAN.

Abstract

The development of information technology has now grown very rapidly, especially in the case of the use of wireless computer networks. The use of internet technology more and more uncontrolled, this is due to the number of internet users in the world, and almost all levels of society know about the Internet and how to access it. The current phenomenon, many government agencies and private companies that have taken advantage of wireless technology to connect the device, so it can complete the tasks quickly. But this makes a computer network administrator to think and work hard in building a connection that is secure and private.

Along with the development of these technologies required the ability to be able to solve the problems of increasingly complex and complicated such as issues related to the security of computer networks, especially network-based wireless network. To maintain and maintain network stability in order to be adequate, regular evaluation evaluations are required. This study produced a model as a result of the assessment that can be used as a reference to develop and improve the security of wireless computer network access on the campus network STMIK Mataram.

Keywords : analisys, wireless network, network security, wireless local area network

I. PENDAHULUAN

Jaringan komputer telah mengalami perkembangan yang sangat pesat. Seiring dengan meningkatnya kebutuhan pengguna komputer yang terkoneksi ke dalam sebuah jaringan komputer, dibutuhkan juga infrastruktur yang dapat mengakomodir permintaan dari pengguna dan pemberdayaan sumberdaya yang tersedia. STMIK Mataram telah banyak memanfaatkan teknologi jaringan komputer. Penggunaan teknologi jaringan ini dilakukan untuk mendukung kegiatan perkuliahan serta kegiatan yang berhubungan dengan administrasi. Karena itu semua informasi yang dikirmkan melalui jaringan komputer perlu untuk mendapat suatu perhatian.

Jaringan nirkabel saat ini menjadi sorotan mengenai tingkat keamanannya, sehingga perlu mendapatkan perhatian serius, hal ini disebabkan karena jaringan nirkabel memanfaatkan gelombang radio yang dipancarkan secara *broadcast*, dan bergerak bebas di udara yang dapat ditangkap oleh siapapun dan kapanpun. Perancangan dan implementasi suatu topologi jaringan, dalam hal ini jaringan komputer nirkabel, tidak dapat diandalkan begitu saja, diperlukan suatu proses lanjutan untuk melakukan suatu penetrasi terhadap kemampuan jaringan tersebut agar tetap sesuai dengan tujuan perancangan. Oleh karena itu, dibutuhkan evaluasi penilaian terhadap ketersediaan, kerahasiaan, dan integritas pada suatu jaringan komputer, agar performa dari jaringan komputer tersebut dapat diandalkan. Dengan melakukan evaluasi secara rutin dan berkala terhadap jaringan komputer yang ada, karena begitu dinamisnya perkembangan teknologi sehingga vulnerability pun terus berkembang juga, sehingga diharapkan dapat diketahui lubang atau celah keamanan yang ada pada sistem jaringan komputer nirkabel yang sedang berjalan sehingga dapat dibuat suatu model sistem keamanan jaringan komputer nirkabel yang baik dan andal.

Evaluasi ini dilakukan sebagai bentuk untuk meningkatkan kesadaran pengelolaan masalah keamanan atau *intrusion detection* dan seberapa cepat kemampuan respon terhadap adanya ancaman (*threat*), selain itu evaluasi ini juga dilakukan sebagai bahan pertimbangan dalam pengambilan keputusan oleh manajemen yang lebih tinggi pada STMIK Mataram dalam hal kerentanan akan keamanan sistem jaringan, di mana manajemen kampus mungkin tidak ingin atau tidak mampu untuk mengatasi semua kerentanan yang ditemukan dalam penilaian kerentanan, tetapi mungkin ingin untuk mengatasi kelemahan sistem yang ditemukan dianggap paling berbahaya, sehingga disinilah fungsi dari evaluasi ini melalui tes penetrasi.

Selain alasan di atas, perlunya dilakukan evaluasi terhadap keamanan jaringan adalah untuk memenuhi standard atau regulasi yang berlaku, mengacu pada banyaknya standar yang mewajibkan untuk pengelolaan kerentanan *teknis (technical vulnerability management)* seperti yang tertuang dalam ISO27001. Di Indonesia, standar ini telah diadopsi sebagai SNI ISO27001.

II. KAJIAN LITERATUR

Jaringan komputer *(computer networks)* adalah suatu himpunan interkoneksi sejumlah komputer *autonomous*. Jaringan komputer terdiri atas perangkat-perangkat yang saling terhubung satu sama lain melalui media perantara seperti router, switch dan sebagainya. Media perantara ini bisa berupa media kabel ataupun media tanpa kabel (nirkabel).

Wireless (nirkabel) adalah teknologi yang menghubungkan dua piranti untuk bertukar data tanpa media kabel. Adapun *Wireless Fidelity* (WiFi), yaitu perangkat standar yang digunakan untuk komunikasi jaringan lokal tanpa kabel (*Wireless Local Area Network*/WLAN) yang didasari pada spesifikasi IEEE 802.11 (Sofana, 2013).

II.1 WLAN *(wireless local area network)*

Wireless Local Area Network adalah sistem komunikasi yang fleksibel dimana pengirim dan penerimaan datanya melalui media udara dengan menggunakan teknologi frekuensi radio. WLAN dapat digolongkan menjadi dua kategori utama yakni:

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 Infrastuktur

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 (Pratama, 2015, S'to, 2015).

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:

1. *Privacy* dan *Confidentiality:* Suatu mekanisme yang 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.
2. *Integrity:* Aspek yang mengutamakan akses informasi yang ditujukan untuk pengguna tertentu, di mana integritas dari informasi tersebut masih terjaga.
3. *Authentication:* Pada bagian ini mengutamakan validitas dari user yang melakukan akses terhadap suatu data, informasi, atau layanan dari suatu institusi.
4. *Availability:* Aspek yang berhubungan dengan ketersediaan data, informasi, atau layanan, ketika data, informasi atau layanan tersebut diperlukan.
5. *Acces Control:* Aspek ini berhubungan dengan klasifikasi pengguna dan cara pengaksesan informasi yang dilakukan oleh pengguna.
6. *Non Repudiation:* Aspek yang berkaitan dengan pencatatan pengguna, agar pengguna data, informasi atau layanan tidak dapat menyangkal bahwa telah melakukan akses terhadap data, informasi, ataupun layanan yang tersedia (Garfinkel, 2003).

Seiring dengan berkembangnya penggunaan jaringan *wireless* LAN saat ini, aspek keamanan menjadi pusat perhatian utama. Banyak serangan yang dapat terjadi pada jaringan *wireless*. Serangan-serangan yang paling sering muncul pada jaringan *wireless* ini adalah sebagai berikut: (Manuaba, 2012)

1. *Reveal SSID*: Usaha serangan yang dilakukan dengan menyingkap SSID dari *access point* yang sengaja disembunyikan oleh administrator jaringan komputer.
2. *MAC Address Spoofing:* Usaha yang dilakukan oleh seorang peretas untuk menembus keamanan *MAC address filtering* dengan melakukan *spoofing MAC address* pada jaringan komputer, dengan menggunakan MAC address pengguna yang sah untuk mendapatkan layanan jaringan komputer.
3. *Authentication Attack:* Serangan terhadap *authentication user* yang sah, sehingga menyebabkan kelumpuhan atau terputusnya pengguna sah. Penyerang memanfaatkan serangan ini agar mendapatkan sumberdaya yang lebih dalam menggunakan layanan jaringan.
4. *Eavesdropping:* Serangan yang dilakukan dengan cara mendengarkan semua paket-paket yang ditransmisikan oleh pengguna yang berada dalam jaringan komputer yang tidak terenkripsi menggunakan teknik enkripsi apapun.
5. *Session Hijacking:* Suatu serangan yang menyerang suatu sesi seorang pengguna untuk dimanfaatkan sebagai ajang untuk mendapatkan suatu hak akses ke layanan yang sedang diakses oleh pengguna sah.
6. *Man In The Middle Attack:* Serangan yang dilakukan dengan melakukan *spoofing* terhadap pengguna sah sehingga transmisi yang dilakukan target adalah menuju penyerang, sehingga penyerang mendapatkan semua informasi yang ditransmisikan oleh target.
7. *Denial of Service:* Serangan yang menyerang ketersedian sumber daya sehingga menyebabkan pengguna sah mengalami koneksi terputus dari jaringan komputer.
8. *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*.

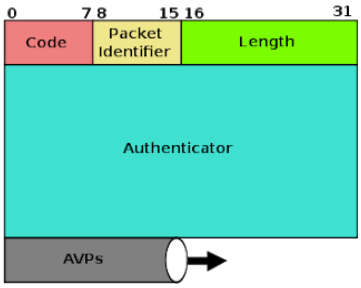
II.2 RADIUS *(Remote Authentication Dial-In User Service)*

Radius adalah sebuah protokol keamanan komputer yang digunakan unutk 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 merupakan proses pengesahan identitas pengguna *(end-user)* untuk mengakses jaringan. *Authorization* merupakan merupakan proses pengecekan wewenang yang dimiliki oleh pelanggan pengguna jaringan komputer. Sedangkan *accounting* merupakan proses penghitungan yang dilakukan oleh sistem yang kemudian melakukan pencatatan sumberdaya yang telah dipakai oleh pengguna jaringan komputer nirkabel.

RADIUS memiliki suatu format paket yang digunakan dalam melakukan transmisi data (Prihanto, 2014).



Gambar 1. Protokol RADIUS

1. *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. Kode pada Protokol RADIUS

Kode	Deskripsi
1	Access – Request
2	Access – Accept
3	Access – Reject
4	Accounting – Request
5	Accounting – Respond
11	Access Challenge
12	Status – Server
13	Status - Client
255	Reserved

2. *Packet Identifier:* memiliki panjang satu oktet (8 bit) dan bertujuan untuk mencocokkan permintaan client dan paket respon yang diberikan oleh server RADIUS.
3. *Length:* memiliki panjang dua oktet (16 bit), memberikan informasi mengenai panjang paket, termasuk didalamnya adalah *code, identifier, length, authenticator, atribut.*
4. *Authenticator:* memiliki panjang 16 oktet (128 bit), digunakan untuk membuktikan balasan dari RADIUS server, selain itu digunakan juga untuk algoritma *password*.
5. *Atributs:* 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 detil konfigurasi spesifik yang diperlukan untuk permintaan dari client RADIUS ataupun NAS.

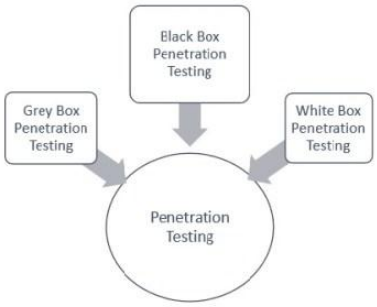
Dalam penerapanya, RADIUS server dipadukan dengan *captive portal* yang merupakan suatu teknik *routing traffic* untuk melakukan autentikasi dan pengamanan data yang melewat jaringan internal ke jaringan eksternal dengan membelokan traffic pengguna ke sebuah halaman login (Wiliyana, 2014).

II.3 *Penetration Test (Pentest)*

Pentest adalah sebuah metode untuk melakukan evaluasi terhadap keamanan dari sebuah sistem dan jaringan komputer. Evaluasi dilakukan dengan cara melakukan sebuah simulasi serangan *(attack).* Hasil dari pentest ini sangat penting sebagai umpan balik bagi administrator sistem dan jaringan untuk memperbaikai tingkat keamanan dari sistem komputernya, selain itu juga akan memberikan masukan terhadap kondisi vulnerabilitas sistem sehingga memudahkan dalam melaksanakan evaluasi dari sistem keamanan komputer yang sedang berjalan. Aktifitas pentest juga dikenal dengna istilah *"ethical hacking"*.

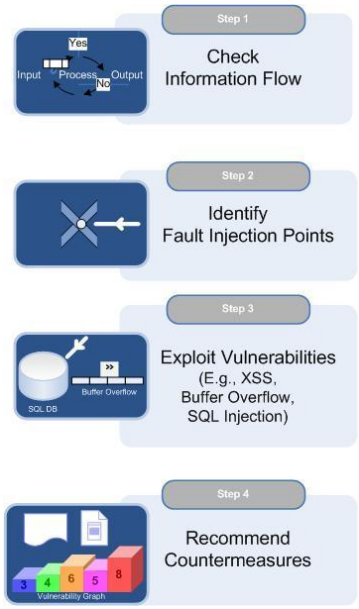
Ada beberapa teknik dan metode yang digunakan dalam melakukan Pintest, diantaranya adalah dengan *black box, white box* dan *grey box*. *Black box* testing adalah metode Pentest di mana diasumsikan tester tidak mengetahui sama sekali infrastruktur dari target pentest. Dengan demikian pada black box test ini tester harus mencoba untuk 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 *gray box* adalah kombinasi dari kondisi black box dan white box. Pengertian lain dari white

box adalah full disclosure, grey box adalah partial disclosure dan black box adalah blind disclosure.

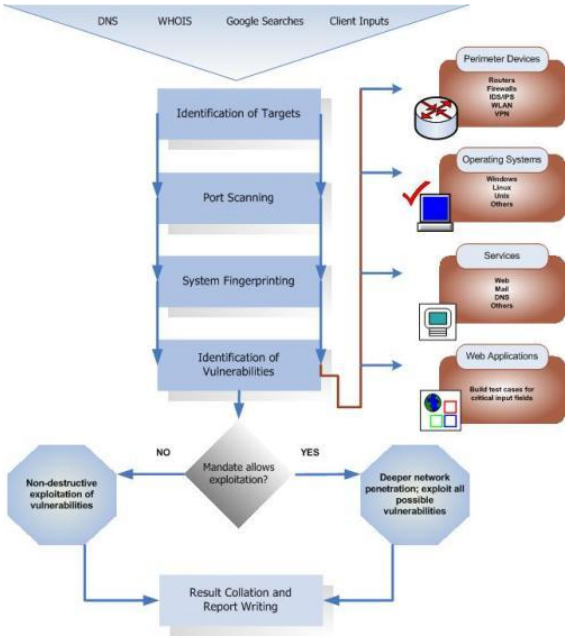


Gambar 2. Metode Pentest

Secara umum ada 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 (Anonimus, 2013).



Gambar 3. Langkah dasar aktivitas Pentest



Gambar 4. Ilustrasi aktivitas detail dari Pintest

III. ANALISIS DAN PERANCANGAN

III.1 Metode

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 assesment* (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.

B. Penetration Test (Pentest)

Penetration test dilakukan untuk mengetahui lubang atau celah keamanan yang terdapat pada jaringan komputer STMIK Mataram. *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) Membersikan jejak pengintaian dan melakukan pelaporan. Secara umum langkah-langkah yang dilakukan dalam Pentest adalah sebagai berikut :

Gambar 5. Tahapan metode Pentest

1. *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.
2. *Reconnaissance* : *Reconnaissance* bisa disebut dengan pengumpulan data bisa dikategorikan sebagai *passive pentetration testing* karena dalam langkah *reconnaissance* pengumpulan data dilakukan secara manual, bisa lewat dokumentasi pihat terkait ataupun informasi terbuka yang ditanyakan langsung pada pihak yang terkait dengan sistem.
3. *Discovery* : *Discovery* merupakan langkah di mana dilakukan pengumpulan informasi dengan menggunakan *automated tool* untuk memindai *vulnerbilities* (kerentanan) pada sistem termasuk didalamnya pemindaian terhadap jaringan, server, perangkat, maupun data.
4. *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 kemanan yang bisa ditimbulkan dari kerentanan sistem yang terpasang.
5. *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
6. *Final analysis* : Analisa akhir secara keseluruhan memberikan pernyataan terhadapa segala temuan dan petunjuk teknis perbaikan sisi keamanan setelah adanya skema sistematis analisa
7. *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 pemebnahan dari segi keamanan sistem

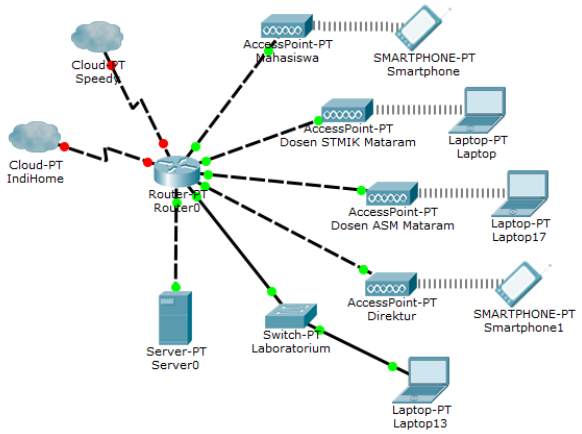
Metode analisis tingkat keamanan jaringan nirkabel dilakukan dengan cara membangun jaringan simulasi pada substansi-substansi keamanan jaringan yang terdapat pada jaringan nirkabel kampus STMIK Mataram.

Pengujian yang dilakukan pada jaringan simulasi, adalah dengan menyerang jaringan simulasi menggunakan serangan-serangan yang mungkin muncul pada jaringan komputer nirkabel yang sesuai dengan studi kasus. Serangan untuk jaringan simulasi tersebut diantaranya adalah *Spoofing MAC address, authentication attack, denial of service, eavesdropping,* dan *man in the middle attack.*

Hasil dari *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 STMIK Mataram, yang dilanjutkan dengan melakukan pengujian terhadap model yang telah dibuat untuk memastikan model yang digunakan sudah benar dan tepat.

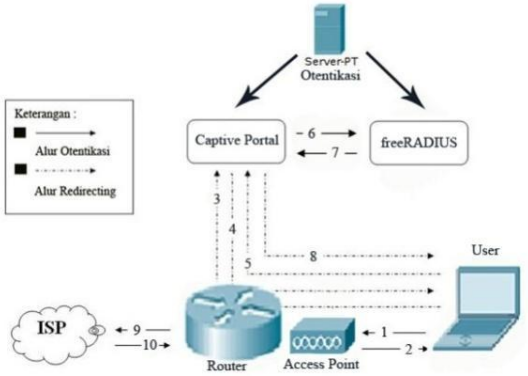
III.2 Simulasi Jaringan Komputer STMIK Mataram

Untuk melakukan simulasi terhadap jaringan komputer nirkabel STMIK Mataram, dibutuhkan topologi jaringan yang sesuai untuk menggambarkan keadaan jaringan pada studi kasus.



Gambar 6. Topologi Jaringan Komputer STMIK Mataram

Pada gambar 6 di atas, merupakan topologi jaringan komputer pada STMIK Mataram. 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.



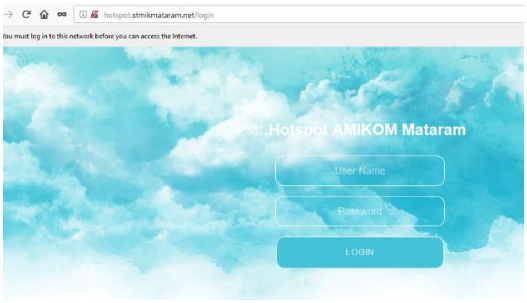
Gambar 7. Model Keamanan Akses Jaringan STMIK Mataram

Pada gambar 7 di atas, terdapat mekansime autentikasi yang diwakilkan oleh penomoran yang tertera pada gambar untuk menunjukan mekanisme autentikasi yang diberlakukan pada setiap bagian yang ada di kampus STMIK Mataram.

Setelah mendapatkan informasi mengenai mekanisme keamanan jaringan komputer nirkabel yang digunakan, berikutnya adalah merancang konfigurasi untuk server RADIUS yang dipadukan dengan *captive portal*. Konfigurasi yang dijalankan dapat dilihat pada file `/etc/chilli/main.conf`

```
domain lan
dns1 202.3.208.11
uamhomepage http://10.1.0.1/coova_json/splash.php
wisprllogin https://coova.org/app/uam/auth
wwwdir /etc/chilli/www
wwbin /etc/chilli/wwwsh
locationname "STMIK-Mataram"
RADIUSlocationname STMIK_Mataram
RADIUSlocationid isocc=,cc=,ac=,network=STMIKMataram
```

Konfigurasi *captive portal* dan RADIUS ketika dijalankan akan menampilkan tampilan seperti gambar berikut.



Gambar 8. *Captive portal* STMIK Mataram

III.3 Pengujian dan Analisis

Untuk menilai kerentanan pada jaringan komputer nirkabel yang dilakukan oleh pengguna, maka dilakukan uji *vulnerability assesment* (VA), untuk menilai dan mengukur tingkat keamanan yang digunakan pada suatu jaringan. Metode yang digunakan dalam tes yang dilakukan pada jaringan simulasi ini adalah metode *penetration test*, hal ini dilakukan untuk mengetahui lubang atau celah keamanan yang terdapat pada jaringan komputer STMIK Mataram. Berikut adalah hasil tes yang dilakukan pada jaringan.

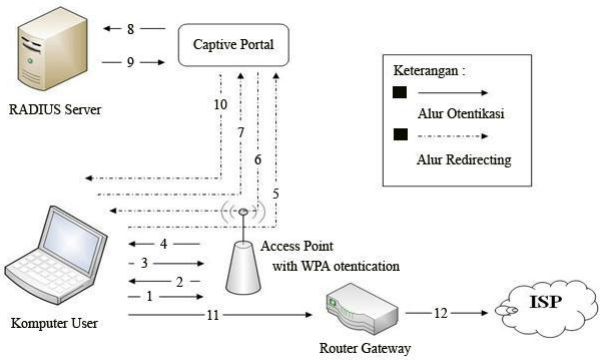
Tabel 2. *Penetration Testing* pada Jaringan

Jenis Serangan	Informasi yang dibutuhkan	Status serangan
Spoofing MAC Address	List MAC Address pengguna yang terkoneksi ke dalam jaringan	Berhasil
Eavesdropping	Penyerang harus berada dalam jaringan intranet	Gagal
Denial of Service (DoS)	List IP address pengguna yang	Berhasil

	terkoneksi ke dalam jaringan	
Man in The Midle Attack	Port yang terbuka pada server dan IP address dari user yang terkoneksi	Gagal
Authentication Attack Tunggal	List MAC *Address user* yang terkoneksi ke dalam jaringan, channel yang digunakan oleh *Access point*	Berhasil

Pada Tabel 2 di atas, menunjukan bahwa serangan *eavesdropping* dan *Man In the Middle Attack* gagal terjadi pada jaringan yang menggunakan *RADIUS authtentication server*.

Dari uji coba serangan-serangan yang telah dilakukan, dapat dianalisis bahwa dalam jaringan komputer nirkabel dibutuhkan suatu lapisan keamanan untuk mencegah user yang tidak memiliki hak agar tidak dapat bergabung dengan jaringan. Lapisan keamanan yang dibutuhkan berupa autentikasi pada layer 2, yang terdapat pada *access point* berupa suatu lapisan yang menggunakan teknologi enkripsi. Sejauh ini, teknik autentikasi ini ada beberapa macam, seperti WPA (*Wi-Fi Protected Access*), dan WPA2 (*Wi-Fi Protected Access2*). Dalam membangun sistem keamanan jaringan nirkabel, dianjurkan menggunakan mekanisme autentikasi yang lebih baik, dengan menggunakan WPA/WPA2. Rekomendasi yang disarankan tersebut dipadukan dengan server autentikasi RADIUS untuk memberikan mekanisme keamanan jaringan komputer nirkabel yang berlapis.



Gambar 9. Model Keamanan Jaringan Komputer Nirkabel STMIK Mataram

Model keamanan jaringan komputer nirkabel menggunakan dua lapisan keamanan yaitu dengan menggunakan WPA dan server autentikasi RADIUS yang dikombinasikan dengan menggunakan *captive portal*. *Captive portal* akan melakukan *redirecting* pengguna ke halaman autentikasi ketika pengguna melakukan akses ke jaringan internet dengan menggunakan web browser. *Captive portal* akan berasosiasi dengan server RADIUS untuk melakukan validasi dari pengguna dan kata kunci yang dikirimkan oleh pengguna.

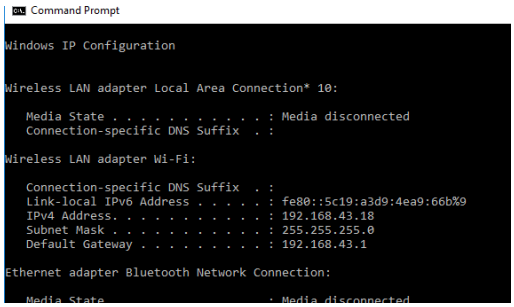
Selain memberikan tingkat keamanan yang lebih baik dan andal, penggunaan RADIUS server yang dirancang sesuai model AAA (*authentication, authorization,* dan *accounting*) memberikan kemudahan dalam melakukan pencatatan aktivitas pengguna. Untuk menguji model keamanan jaringan komputer nirkabel ini, dilakukan dengan teknik yang sama yakni serangan-serangan yang mungkin terjadi pada jaringan komputer nirkabel, seperti:

Tabel 3. Pengujian model keamanan jaringan komputer nirkabel STMIK Mataram

Jenis Serangan	Informasi yang dibutuhkan	Status serangan
Spoofign MAC Address	List MAC Address pengguna yang terkoneksi ke dalam jaringan	Gagal
Eavesdroping	Penyerang harus berada dalam jaringan intranet	Gagal
Denial of Service (DoS)	List IP address pengguna yang terkoneksi ke dalam jaringan	Gagal
Man in The Midle Attack	Port yang terbuka pada server dan IP address dari user yang terkoneksi	Gagal
Cracking WPA	Dictionary word, handshake user lain, BSSID AP	Gagal

Sebagai contoh serangan yang dilakukan pada pengujian ini adalah menggunakan jenis serangan DoS, di mana jenis serangan ini berupa ping of death, smurf, buffer overflow, teardop dan syn attack. Sebelum melakukan serangan ada beberapa alat yang digunakan, diantaranya adalah nemsey (menghasilkan paket acak), LaTierra (spoofing IP dan membuka koneksi TCP), Panther (membanjiri jaringan korban dengan paket UDP), Bootnet dan lainnya. Berikut adalah hacking dengan menggunakan ping of death. Langkah pertama adalah

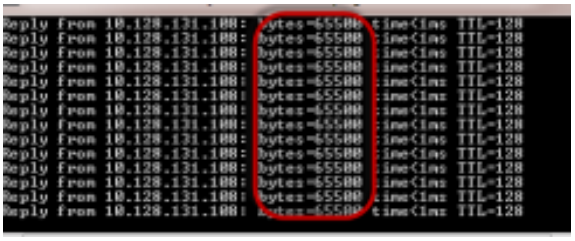
dengan membuka command prompt dan memasukkan perintah ipconfig, dan hasilnya seperti



di bawah ini:

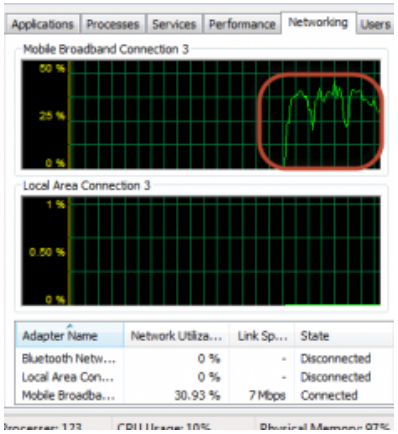
Gambar 10. Windows IP Configuration

Selanjutnya, masukkan perintah berikut : 10.128.131.108 -t -65500, di mana 10.128.131.108 adalah alamat IP korban, -t = paket data harus dikirim sampai program berhenti



Gambar 11. Membanjiri komputer dengan paket data

Untuk melihat efek serangan pada komputer target, dapat dilihat melalui *task manager* dan melihat aktifitas jaringan.



Gambar 12. Aktifitas Network

Jika serangannya berhasil maka akan terlihat peningkatan aktivitas jaringan, jika gagal maka akan terlihat sebaliknya.

IV. KESIMPULAN DAN SARAN

Dari hasil penelitian, dapat disimpulkan bahwa analisis dan evaluasi terhadap tingkat keamanan jaringan komputer nirkabel pada STMIK Mataram dapat dilakukan dengan menggunakan metode *penetration test* seperti *Spoofing MAC address, authentication attack, Denial of Service, Man In The Midle Attack*, dan *Eavesdropping*. Adapun saran yang dapat diberikan adalah penggunaan sistem autentikasi dengan menggunakan server autentikasi yang dipadukan dengan *captive portal* belum cukup kuat untuk menangani serangan-serangan seperti *enial of service, authentication attack*, dan *MAC address spoofing.* Model keamanan yang menggunakan kombinasi antara server autentikasi, *captive portal, firewall*, serta WPA/WPA2 yang dihasilkan pada penelitian ini dapat menutup lubang atau celah keamanan dan meningkatkan mekanisme keamanan jaringan nirkabel. Penggunaan kata kunci autentikasi disarankan untuk menggunakan kata kunci dengan kombinasi angka, huruf dan karakter untuk meningkatkan keamanan dari kata kunci yang digunakan.

REFERENSI

Anonimus, 2013. *Penetration Test (Pentest)*. www.niiconsulting.com

Garfinkel, S; Spafford, G; Schwartz, A. 2003. *Practical UNIX and Internet Security (Third Edition)*. O'Reilly & Associate Inc. Sebastopol, CA.

Manuaba, I.B.V.H., Hidayat, R., Kusumawardani, S.S., 2012. Evaluasi Keamanan Akses Jaringan Nirkabel (Kasus: Kantor Fakultas Teknik Universitas Gadjah Mada). JNTETI, Vol. 1, No. 1, Mei 2012. UGM. Yogyakarta.

Pratama, Romadhon Pearl. 2015. Analisis Kinerja Jaringan Wireless LAN Menggunakan Metode QOS dan RMA Pada PT. Pertamina Ep Ubep Ramba (Persero). Palembang: Program Pascasarjana Univ. Bina Darma.

Prihanto, Agus. 2010. Membangun *RADIUS Server* untuk Keamanan Wifi Kampus. Jurnal

SimanteC Vol. 1, Vo. 3 Desember 2010. Surabaya.

Sofana, I., 2013. Membangun Jaringan Komputer. Bandung. Informatika.

S'to, (2015). *Wireless* Kung Fu : *Networking & Hacking.* Jasakom. Jakarta. http://jasakom.com/sto

Wiliyana, Dian. 2014. Perancangan Jaringan LAN dan Keamanan *Wireless* Internet Hotspot Berbasis Mikrotik Router Pada Pomdam IV Sriwijaya. Palembang: Program Pascasarjana Univ. Bina Darma.