APLIKASI MANAJEMEN DAN MONITORING UNTUK KEAMANAN PADA JARINGAN HOTSPOT

Sadam Husen[1] , Raisul Azhar[2]

[1]Mahasiswa Jurusan Teknik Informatika, STMIK Bumigora Mataram

[2] Staf Pengajar Jurusan Teknik Informatika, STMIK Bumigora Mataram

1sadamibnusalam@gmail.com, 2raisulazhar@yahoo.co.id

Abstract

STMIK Bumigora has five internet hotspot access point which can be used by students. Fifth hotspot wireless access point includes faculty, labs, students, faculty and for management purposes. The use of wireless networks for internet access led to the illegal activities that can not be monitored by the network administrator. Activity is mainly on the use of the router that serves as a proxy router connected directly to the ISP (Internet Service Provider). Illegal activities are often done by the students is trying to log into any network devices using bruteforce method. Techniques used include using remote access such as ssh, telnet and ftp. In addition, the activity of port scanning is often performed by the students to observe the security gaps that are still weak in a hotspot, especially at the p*ort still open on the network.* To overcome this problem, researchers built an application that is capable of managing and monitoring security hotspots making it easier for network administrators to take action against such *illegal activities. Research method used is SDLC, in which the system is intended to develop a system that has existed previously in PUSTIK STMIK Bumigora Mataram*

Keywords*: hotspot, bruteforce, port scanner, spoofing, security, networking*

1. PENDAHULUAN

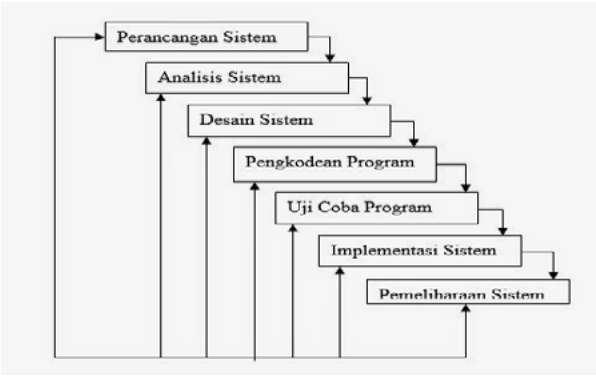
Sekolah Tinggi Manajemen dan Informatika (STMIK) Bumigora Mataram adalah salah satu perguruan tinggi swasta dibidang Teknik Informasi dan Komunikasi (TIK) yang berkedudukan di Provinsi Nusa Tenggara Barat. Pada kampus STMIK Bumigora memiliki lima titik hotspot internet yang dapat digunakan yaitu pada SSID Lab BumigoraNET, Mahasiswa BumigoraNET, Dosen BumigoraNET, Perpustakaan BumigoraNET, dan Open Source BumigoraNET. Dimana kelima titik hotspot tersebut dapat digunakan oleh civitas akademika meliputi dosen, mahasiswa, staf dan manajemen. Kelima titik hotspot tersebut dimanajemen oleh PusTIK, akan tetapi terdapat aktivitas illegal yang dilakukan pengguna terhadap mikrotik. Aktivitas-aktivitas illegal tersebut seperti pengguna yang berusaha login terhadap masing-masing mikrotik jaringan hotspot. Aktifitas login dilakukan menggunakan bruteforce ssh, bruteforce telnet dan bruteforce ftp, serta terdapatnya aktiftas port scanning dan spoofing yang dapat memungkinkan terjadinya serangan dalam bentuk yang berbeda [1]. Port scanning merupakan aktifitas yang dilakukan seseorang untuk melihat port/saluran yang terbuka pada jaringan untuk dipergunakan sebagai tindak kejahatan [2].

Untuk menanggulangi permasalahan yang terjadi tersebut, pihak administrator jaringan biasanyan masih menggunakan fitur IP Fireall Filter pada mikrotik, yaitu dengan menambahkan skrip firewall yang harus disalinkan secara manual ke seluruh Mikrotik yang ada pada STMIK Bumigora Mataram, sehingga tidak efektif dan efisien dalam memonitoring aktivitas yang terjadi pada masing masing titik hotspot.

Berdasarkan permasalan yang ada pada PUSTIK STMIK Bumigora tersebut, maka dibutuhkan sebuah solusi yakni dengan membangun sebuah aplikasi manajemen dan monitoring keamanan hotspot. Aplikasi yang dibangun nantinya memiliki kemampuan mendeteksi aktivitas-aktivitas illegal dalam jaringan hotspot, serta dapat membantu menangani permasalahan keamanan jaringan yang sering terjadi terutama akfitas illegal seperti bruteforce dengan telnet,ssh,ftp dan aktifitas scanning port dan spooing, sehingga dapat mempermudah administrator dalam memanajemen dan memonitor aktivitas yang berlangsung secara terpusat. Aplikasi dalam penelitian ini dibangun menggunakan antarmuka berbasis web dan menggunakan PHP Framework Laravel sehingga mudah diakses dari lokasi manapun juga.

II. METODOLOGI

Metode penelitian yang digunakan adalah Pengembangan Piranti Lunak System Development Life Cycle (SDLC) Model Waterfall. Model ini sebenarnya adalah "Linear Sequential Model". Model ini sering disebut dengan "classic life cycle" atau model waterfall.



Gambar.1 Medel Waterfall

Model ini adalah model yang muncul pertama kali yaitu sekitar tahun 1970 sehingga sering dianggap dianggap metode klasik untuk pengembangan sistem. Metode ini merupakan model yang paling banyak dipakai didalam softwareeEngineering[3].

Untuk melengkapi metode penelitian yang digunakan, diperlukan analis-analis sistem yang dilakukan oleh peneliti mencakup:

1. Analisis kebutuhan untuk menghasilkan spesifikasi terhadap system yang akan dibangun
2. Analis proses dan analisis data-data yang meliputi:
   a. Rancangan topologi jaringa n hotspot yang dipergunakakan dalam bentuk prototype.
   b. Penggunaan UML (Unified Modeling Language) untuk menghasilkan alur proses Object Oriented Analysis And Design (OOAD).
   c. Penggunaan pemetaan database menggunakan Object Relational Maping (ORM).
   d. Pembuatan beberapa diagram proses seperti Use Case Diagram, Activity Diagram, Class Diagram, Sequence Diagram dan Component Diagram.
   e. Design interface dari aplikasi program
3. Dalam pengumpulan data dilakukan dengan beberapa cara antara lain:
   a. Wawancara terhadap pihak yang berkepentingan dalam hal ini bagian administrator jaringan
   b. Dokumentasi dengan melakukan dengan mengambil capture tehadap aktifitas illegal yang pernah dilakukan terhadap jaringan hotspot, terutama difokuskan terhadap brute force dan port scanning.
   c. Memberikan penyebaran Quisioner terhadap pengguna hotspot.
4. Melakukan Analisis hasil pengujian

   Analisis hasil pengujian dilakukan dengan menyusun scenario pengujian dengan melakukan beberapa tahap scenario pengujian seperti melakukan simulasi teknik serangan dan dilakukan menitoring terhadap aktifitas tersebut, serta membandingkan penggunaan aplikasi yang dihasilkan berdasarkan kecepatan akses notifikasi,efisiensi waktu dengan aplikasi winbox yang telah terintegrasi dengan router mikrotik.

III. HASIL DAN PEMBAHASAN

a. Hasil Rancangan

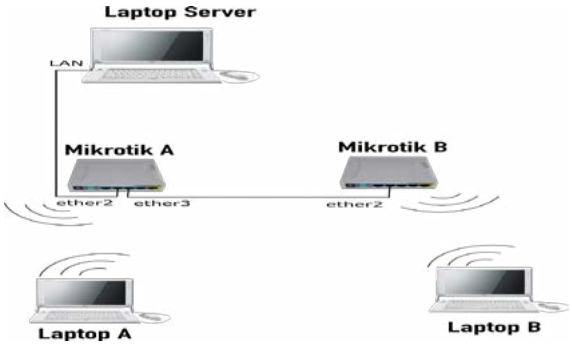
Dalam membangun rancangan, peneliti membagi menjadi 2 (dua) bagian rancangan, yaitu perancangan jaringan dan perancangan aplikasi. Perancangan jaringan dimaksudkan untuk membangun lingkungan uji coba secara local, sedangkan perancangan aplikasi dimaksudkan untuk menangkap artefak proses Object Oriented Analysis dan Design yang sering disebut dengan OOAD [4] menggunakan Unifield Modelling Language (UML).

b. Rancangan Jaringan

Untuk mendapatkan hasil sesuai dengan kebutuhan pihak administrator jaringan STMIK Bumigora Mataram, terlebih dahulu dilakukan perancangan jaringan dengan membangun tipologi jaringan prototype yang sesuai dengan keadaan sesungghunya pada lokasi penelitian.

1. Topologi Jaringan Pengujian

Adapun rancangan topologi jaringan yang akan digunakan untuk uji coba aplikasi dapat di lihat pada gambar berikut ini:



Gambar 2. Topologi Jaringan Uji Coba

Pada gambar di atas terdapat satu komputer server, 2 (dua) buah perangkat router mikrotik, 2 (dua) komputer klien dan masing-masing perangkat memiliki fungsi yang berbeda diantranya:

a. Pada Laptop Server digunakan untuk menjalankan Aplikasi Manajemen Dan Manajemen Dan Monitoring Keamanan Hotspot, dan installasi paket-paket

pendukung untuk menjalankan aplikasi.

b. MikroTik Router BOARD 951 difungsikan sebagai routing terhadap jaringan hotspot.

c. Komputer Laptop A dan Laptop B sebagai klient yang akan melakukan simulasi serangan ke jaringan hotspot yang didalamnya terdapat paket-paket pendukung untuk melakukan bruteforce, spoofing dan scanning port.

2. Pengalamatan Jaringan HotSpot

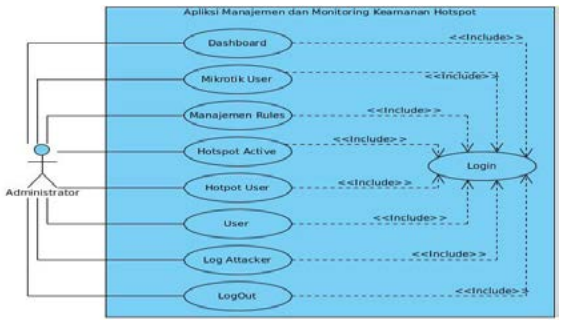
Pada aplikasi, menggunakan alamat jaringan yang telah ditentukan, mikrotik menggunakan 2 port ethernet untuk mikrotik A, kemudian 1 port ethernet untuk mikrotik B. Sedangkan komputer server menggunakan LAN, kemudian untuk komputer klient menggunakan IP DHCP dari perangkat router Mikrotik.

c. Rancangan Aplikasi

Rancangan aplikasi ini menggunakan Unified Modeling Language (UML) untuk menghasilkan alur proses Object Oriented Analysis And Design (OOAD) dan pemetaan database menggunakan Object Relational Maping (ORM). Adapun diagram-diagram UML yang dirancang dalam aplikasi ini adalah Use Case Diagram, Activity Diagram, Class Diagram, Sequence Diagram, Component Diagram.

1. Use Case Diagram

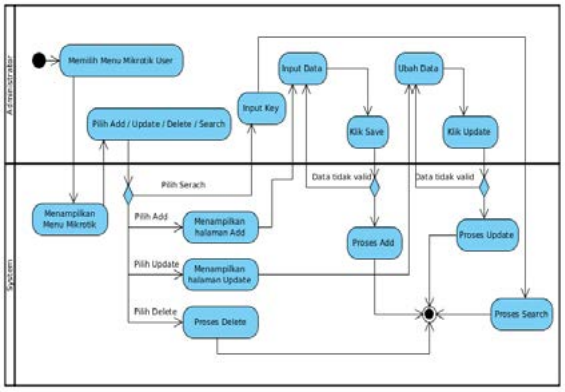
Gambar 3 merupakan Use Case Diagram yang menjelasknan tentang fitur-fitur yang tersedia dalam Aplikasi Manajemen dan Monitoring Keamanan Hotspot



Gambar 3. Use Case Diagram

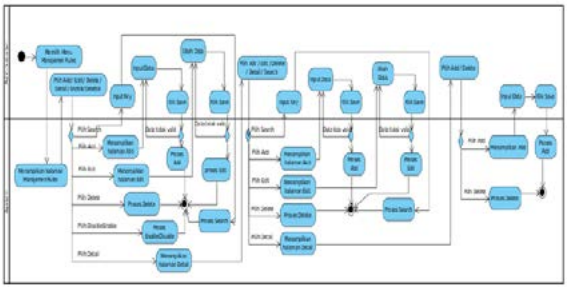
2. Activity Diagram

Pada Gambar 4. merupakan Activity Diagram mikrotik user menggambarkan proses penambahan, pengubahan, penghapusan, dan pencarian data.



Gambar 4. Aktivity Diagram User

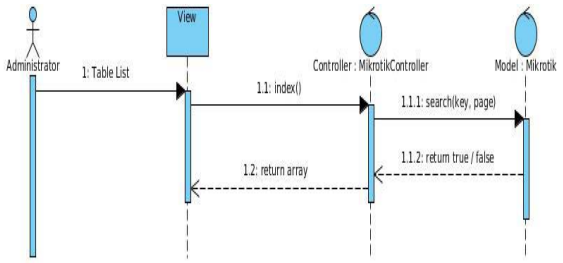
Pada Gambar 4 merupakan Activity Diagram manajemen rules yang menggambarkan proses penambahan, pengubahan, penghapusan, disable, enable, dan pencarian rules yang telah tersimpan pada database aplikasi:



Gambar 5. Aktivity Diagram Rules

3. Sequence Diagram

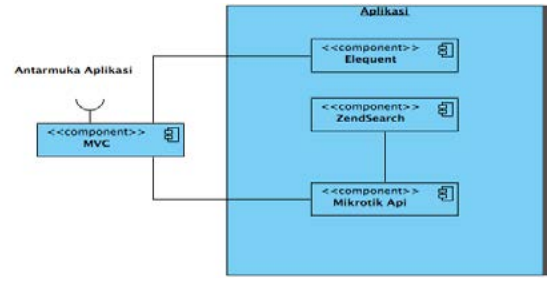
Sequence Diagram Mikrotik User menggambarkan interaksi antar objek untuk menampilkan mikrotik yang telah ditambahkan pada database aplikasi,



Gambar 6. Class Diagram User

4. Component Diagram

Pada Gambar 7 merupakan Componen Diagram digunakan untuk menggambarkan hubungan sistem dengan komponen-komponen yang digunakan.



Gambar 7. Componen Diagram

d. Hasil Aplikasi Program

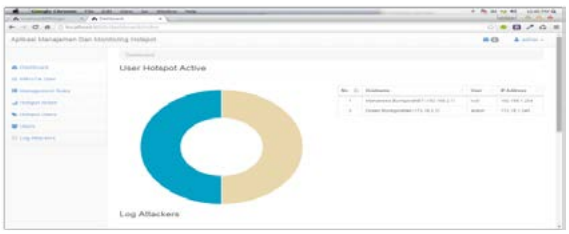
Tampilan Halaman Login

Menu login, seperti yang ditunjukkan pada gambar 7. merupaka tampilan utama pada saat administrator mengakses aplikasi. Untuk dapat masuk kedalam aplikasi, administrator diharuskan melakukan login terlebih dahulu dengan memasukkan username dan password yang telah didaftarkan didalam database aplikasi.

Gambar 8. Tampilan Halaman Login

Tampilan Halaman Dashboard

Pada menu Dashboard terdapat informasi jumlah presentase hotspot user yang aktif dari masing masing hotspot dan informasi serangan yang terjadi



Gambar 9. Halaman Dashboard

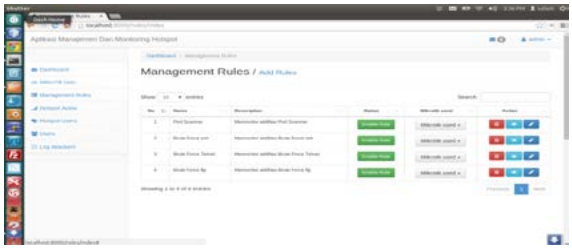
Tampilan Halaman Mikrotik User

Digunakan untuk mendaftarkan mikrotik yang akan dimasukkan dalam aplikasi.

Gambar 10. Tampilan Pengguna

Tampilan Halaman Rules

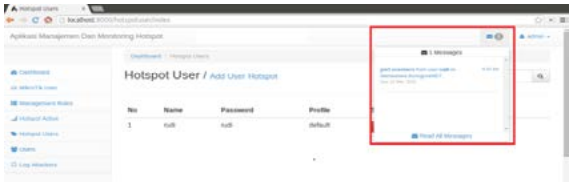
Menu Manajemen Rules merupakan tempat melihat dan menerapkan daftar-daftar rules yang telah dibuat dan tersimpan dalam database aplikasi



Gambar 11. Tampilan halaman Rules

Tampilan Halaman Notification

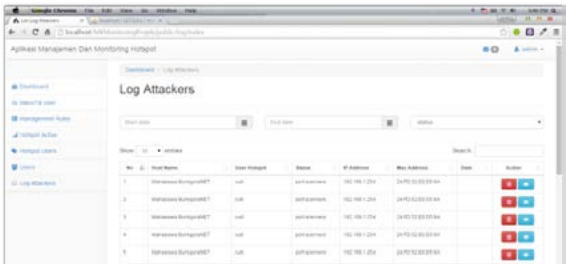
Setiap serangan yang dilakukan pengguna terhadap mikrotik, maka akan tampil pada menu notification yang berfungsi menampilkan jenis serangan, dan dari mana serangan berasal.



Gambar 12. Halaman Notification

Halaman Log Attacker

Menu Log Attacker adalah menu yang menampilkan daftar-dafar penyerang yeng telah dilakukan pengguna user hotspot, Berikut tampilan menu Log Attacker



Gambar 13. Halaman Log Attacker

e. Analisis Hasil Pengujian

Hasil pengujian dibawah ini merupakan hasil penerapan aplikasi yang dibangun berdasarkan scenario pengujian yang dilakukan antara lain dengan:

1. Melakukan serangan/attack dari computer client hotspot dengan menggunakan aplikasi port scanning dan spoofing yang bersifat freeware, dan pada aplikasi dilakukan penerapan aturan/rule security.

2. Melakukan serangan dari komputer client hotspot dari signal wireless connection/SSID yang ditujukan keperangkat router yang membentuk SSID dan melakukan pembentukan parameter-parameter/rule security yang bervariasi pada aplikasi, dan melakukan pengamatan terhadap hasil yang diperoleh.

3. Melakukan serangan dari komputer client dengan metode bruteforce, dengan mencoba akses login beberapa kali dengan kombinasi seperti teks,angka, hurf besar/kecil dan symbol, dengan cara remote access ssh,telnet dan FTP client, terhadap router jaringan hotspot.

Dari scenario simulasi tersebut, berikut ini merupakan sebagian rule-rule security yang dibuat pada aplikasi dan rule yang dibuat melalui aplikasi winbox pada router mikrotik yang dapat tergenerate langsung ke perangakat router, jika terjadi aktfitas penyerangan.

Tabel 1. Rules Port Scanner Menggunakan Aplikasi

No	Item	Parameter	waktu
1	-	Login	11.4
2	-	Add Rules	31.2
3	Drop	Add Rules Detail	13.6
4	-	Add Rules Detail Param	35
5	to address list	Add Rules Detail	13.6
6	-	Add Rules Detail Param	64.8
	penerapan rules	untuk 2 mikrotik	8
		Jumlah	177.6

Tabel 2 Rules Port Scanner Menggunakan Winbox

No	Item	Parameter	Waktu (s)
1	-	Login	15.8
2	Drop	Add Firewall Filter	42.6
3	to address list	Add Firewall Filter	69.8
	Jumlah Waktu Penerapan Per 1 (Satu) Mikrotik		128.2
	Jumlah Waktu Penerapan Per 2 (dua) Mikrotik		256.4

Tabel 3 Rules Brute Force Menggunakan Aplikasi

No	Item	Parameter	Waktu
1	-	Login	11.4
2	-	Add Rules	31.2
3	Drop	Add Rules Detail	13.6
4		Add Rules Detail Param	61
5	Blacklist	Add Rules Detail	13.6
6		Add Rules Detail Param	82.6
7	Stage3	Add Rules Detail	13.6
8		Add Rules Detail Param	70.8
9	Stage2	Add Rules Detail	13.6
10		Add Rules Detail Param	69.6
11	Stage1	Add Rules Detail	13.6
12		Add Rules Detail Param	57.2
	Penerapan rules	untuk 2 mikrotik	8
		Jumlah	459.8

Tabel 4. Rules Brute Force Winbox

No	Item	Parameter	Waktu
1	-	Login	15.8
2	Drop	Add Firewall Filter	67
3	Blacklist	Add Firewall Filter	98
4	Stage3	Add Firewall Filter	102.4
5	Stage2	Add Firewall Filter	98
6	Stage1	Add Firewall Filter	74.2
	Jumlah Waktu Penerapan Per1(Satu) Mikrotik		455.4
	Jumlah Waktu Penerapan Per2(Dua) Mikrotik		910.8

Pada tabel diatas, terlihat pula waktu/kecepatan akses yang diperlukan untuk menambah rules baru untuk memanajemen keamanan hotspot. Waktu tersebut menyatakan kecepatan yang dibutuhkan antara aplikasi yang dibangun untuk menambah rule terhadap aplikasi winbox pada router. Rule ini dapat berupa filtering pada firewall seperti pembungan paket yang datang dari client (drop) dan melakukan filtering blacklist.

Dibawah ini adalah hasil perbandingan pengamatan dari monitoring notifikasi penyerangan yang telah dijalankan:

Tabel 2 Monitoring penyerangan pada aplikasi dan winbox

Percobaan ke	Notifikasi penyerangan Menggunakan Aplikasi Manajemen dan Mnitoring Keamanan	Notifikasi penyerangan Menggunakan Aplikasi Winbox
1	45	14
2	50	16
3	48	14
4	60	14
5	50	13
Rata-Rata	**50.6**	**14.2**

Dari tabel 5 dan 6 terlihat bahwa dalam memonitoring aktifitas illegal akan membutuhkan kecepatan akses yang lebih lama dengan menggunakan aplikasi, hal ini apabila dibandingkan dengan notifikasi waktu menggunakan winbox, Berkurangnya kecepatan dikarenakan lokasi fiture yang berbeda yang terdapat pada mikrotik.

Tabel 6. Perbandingan antara aplikasi dengan winbox

No	Item		Waktu (s)			Waktu (m)			Efisiensi Aplikasi (%)	
			Winbox	Aplikasi	Selisih	Winbox	Aplikasi	Selisih	Detail	Total
1	Manajemen	Port Scanner	256.4	177.6	78.8	4.27	2.96	1.31	30.73	45.91
2		Brute Force SSH	910.8	459.8	451	15.18	7.66	7.52	49.52	
3		Brute Force Telnet	910.8	459.8	451	15.18	7.66	7.52	49.52	
4		Brute Force TFTP	406.8	233.6	173.2	6.78	3.89	2.89	42.58	
5		User Hotspot	31.6	30.4	1.2	0.53	0.51	0.02	3.8	
6	Monitoring	Deteksi Serangan	134	50.6	83.4	2.23	0.84	1.39	62.24	62.24
		Jumlah Keseluruhan	2650.4	1361.2	1289.2	44.17	22.68	21.49	48.64	

Dari tabel 6, untuk mendapatkan nilai efisiensi atas perbedaan waktu akses antara aplikasi dan winbox, diperoleh dengan menghitung jumlah selisih waktu yang dipergunakan yakni:

Jumlah selisih / jumlah winbox * 100

= 1155.2 /2516.4 x 100 = 45.91 %

Sedangkan untuk efisiensi dari monitoring diperoleh:

Selisih / winbox * 100 = 83.4 / 134 x 100

= 62.24 %

Dari sisi penangkapan paket menggunakan aplikasi wireshark diperoleh bahwa aktifitas illegal menggunakan telnet dan FTP terhadap user yang mecoba akses login, aktifitas ini tidak membutuhkan inkripsi hal ini sangat rentan jika diaktifkan pada router. Namun sebaliknya apabila menggunakan secure shell (SSH) aktifitas remote akses membutuhkan inkripsi, sehingga hal ini sangat disarankan untuk dipergunakan untuk mengamankan router yang bertindak sebagai hotspot. Aktifitas port scanning dan spoofing dapat dihindari dengan memutup port port yang terbuka pada router dengan melakukan konfigurasi dan memasang aturan firewall yang ketat berdasarkan kebiasaan pengguna.

IV. SIMPULAN DAN SARAN

4.1. Simpulan

Simpulan yang dihasilkan oleh penelitian ini sebagai berikut:

1. Dengan menggunakan Aplikasi Manajemen dan Monitoing Keamanan Hotspot, administrator dapat lebih efektif dan efisien dalam mendeteksi serangan pada hotspot terutama dari akases hotspot yang berbeda, namun dapat mengelola rules atau firewall secara terpusat terhadap aktfitas serangan.
2. Pihak administator jaringan dapat melakukan pemutusan koneksi hotspot terhadap client yang melakukan serangan menggunakan bruteforce ssh, telnet, ftp dan port scanner, secara otomatis pada aplikasi jika ditemukan aktifitas serangan bruteforce.
3. Penggunaan fiture Log pada aplikasi dapat dipergunakan untuk menyimpan aktiftas penyerangan yang dilakukan client sehingga dapat digunakan untuk pengambilan keputusan terhadap client pengguna internet melalui hotspot.

4.2 Saran-Saran

Aplikasi yang dikembangkan pada penelitian ini belum mampu melakukan manajemen dan monitoring aktifitas-aktifitas illegal yang lain selain bruteforce. Oleh karena itu bagi peneliti yang berminat mengembangkan penelitian ini diharapkan mempu menambah fiture-fiture aplikasi untuk jenis jenis serangan yang berbeda terutama pada jaringan hotspot.

DAFTAR PUSTAKA

[1]. Lilis. (2013, july 22). *Weblog Tips & Tutorial Internet Gratis by Neng Lilis. Retrieved from Pengertian Brute-Force Attack*: http://www.potter.web.id/pengertian-brute-force-attack/

[2] Arrifien, A. K. (2011, Oktober 24). *Port Scanning. Retrieved from Deteksi PortScanning*:http://akuarika.blogspot.com/2011/10/deteksi-port-scanning.html

[3] Pressman, R. S. (2010). *Sofware Enginering : A Practitioner's Approach*. University Level : Person Accociates, Inc

[4]. Booch, G., Maksimchuk, R. A., Engle, M. W., Young, B. J., Conallen, J., & Houston, K. A. (2007). *Object-Oriented Analysis and Design with Applications Third Edition.* United State of America: Pearson Education, Inc.