KEAMANAN AUTHENTIKASI HOTSPOT MENGGUNAKAN CAPTCHA

Kiki Pradikta Prasetyo, Rahayu Widayanti, Sigit Setyowibowo
Program Studi Teknik Informatika, STMIK PPKIA Pradnya Paramita Malang
Email: kiki_pradikta@yahoo.com

Abstrak

Hotspot networking SMKMuhammadiyah2Malang do not have a good security system that can be used by unauthorized users. With the issue of the security system research and design that has a hotspot network's security level better than before. The purpose of this study is to secure hotspot network of ilegal users by adding a captcha in the authentication process using MikroTik hotspot. Data collection methods used to analyze the data and make the information that will be used to determine the problems faced. System development method using the waterfall method. The use of captcha on the authentication process hotspot login page in SMK Muhammadiyah 2 Malang using Mikrotik has not been able to provide evidence of the power system network security hotspot. This is evidenced by the test using a brute force attack techniques. The testing process using the same time frame with the type of passwords that are very weak and not obtained differences of the results achieved. Hotpsot proxy authentication security system based captive portal using only user and password as the authentication process already has a good level of security even without using captcha.

Keyword:*Networking Security, authentication, hotspot, captcha.*

1. PENDAHULUAN

Hotspot merupakan area publik yang telah dipasangi jaringan *internet* w*ireless* atau nirkabel. Terdapat banyak area *hotspot* yang dapat kita temukan, bahkan banyak yang menyediakan akses *free hotspot* agar semua orang dapat menggunakan layanan ini secara gratis. Isu keamanan juga menjadi salah satu hal yang dipertimbangkan dalam penggunaan fasilitas *hotspot* di area publik karena sifatnya yang terbuka.

SMK Muhammadiyah 2 Malang terdapat jaringan *hotspot* yang biasa sering digunakan oleh guru dan karyawan dalam berselancar di dunia *internet*. Teknik pengamanan jaringan *hotspot* di SMK Muhammadiyah 2 menggunakan *mode WPA PSK*. Sistem keamanan dari jaringan *hotspot* di SMK Muhammadiyah 2 Malang ternyata bisa disusupi oleh pengguna yang tidak berhak karena kerahasian dari kunci pengamanan sistem jaringan *hotspot* sulit dijaga kerasahasiaannya. Sifat kunci keamanan yang hanya satu kunci digunakan untuk banyak *user* menyebabkan sulit untuk menjaga kerahasiaan dari kunci pengamanan tersebut dan hal tersebut menyebabkan pengelola jaringan harus sering mengganti kunci keamanan jaringan *hotspot* tersebut agar jaringan *hotspot* aman dari pengguna yang tidak berhak. Selain hal tersebut, ternyata pada teknik pengamanan *WPA PSK* dapat dengan mudah dipecahkan menggunakan *tools* gratis yang bisa di unduh melalui *internet*. Dengan mudahnya proses *crack* terhadap sistem keamanan jaringan *hotspot* di SMK Muhammadiyah 2 Malang yang menggunakan teknik *WPA PSK*, menyebabkan kerugian yang dialami oleh penyedia layanan jaringan *hotspot* tersebut karena adanya pengguna-pengguna yang tidak berhak yang ikut menggunakan layanan jaringan *hotspot* di SMK Muhammadiyah 2 Malang.

Captive portal menjadi mekanisme populer bagi infrastruktur komunitas WiFi dan operator *hotspot* yang memberikan *authentikasi* bagi penguna infrastruktrur maupun manajemen *flow IP,* seperti, *traffic shaping* dan kontrol *bandwidth,* tanpa perlu menginstalasi aplikasi khusus di komputer pengguna. Proses *authenticatio*n secara aman dapat dilakukan melalui sebuah *web browser* biasa di sisi pengguna. Sistem keamanan authentikasi *Captive portal* pada jaringan *hotspot* saat ini banyak yang hanya menggunakan *user* dan *password* sebagai cara untuk mengamankan jaringan *hotspot* dari pengguna yang tidak diinginkan.

Oleh karena masalah keamanan tersebut, peneliti melakukan penelitian tentang mengamankan *authentikasihotspot* di SMK Muhammadiyah 2 Malang dengan menambahkan *captcha* pada proses authentikasi *hotspot* dengan menggunakan *MikroTik*.

2. KAJIAN ISTILAH

Jaringan Komputer

Jaringan komputer adalah sekumpulan komputer beserta mekanisme dan prosedurnya yang saling terhubung dan berkomunikasi. Komunikasi yang dilakukan oleh computer tersebut dapat berupa transfer berbagai data, instruksi, dan informasi dari satu komputer ke komputer lainnya. (Amir, Zaid. 2012:190)

Menurut S, Sudarma. (2010:2) Jaringan komputer adalah sistem yang terdiri dari komputer-komputer, serta piranti-piranti yang saling terhubung sebagai satu kesatuan. Dengan dihubungkannya piranti-piranti tersebut, alhasil dapat saling berbagi sumber daya antar satu piranti dengan piranti lainnya.

Wireless LAN

Hantoro, D.G. (2009 : 2) menyimpulkan dengan *Wirelless LAN* memungkinkan para penguna komputer terhubung tanpa kabel (*wirellessly*) kedalam jaringan.

Menurut Siregar, E. (2010:10), *Wireless* LAN tidak memiliki *physical layout*. Hanya dengan menambah *wireless* NIC maka sebuah *workstation* akan mampu mengirim dan menerima data. Secara umum, *workstation* pada *wireless* LAN akan berkomunikasi dengan kecepatan Hingga 20 Mbps. *Workstation* pada *wireless* LAN bisa ditempatkan dimana saja sepanjang masih dalam jangkauan *Access Point* (*Wireless Hub*).

Mode pada Wireless LAN

Menurut Rahman, Hadi (2011:9) *WLAN* sebenarnya memiliki kesamaan dengan jaringan *LAN*, akan tetapi setiap *node* pada *WLAN* menggunakan *wireless device* untuk berhubungan dengan jaringan.

Komponen *Wireless LAN*

Secara umum, komponen *wireless* terdiri dari atas perangkat berikut:

1) *Access Point*

Prinsip kerja *Access Point* pada prinsipnya mirip dengan cara kerja dari *Switch Hub* yang biasa terdapat pada topologi LAN namun memiliki perbedaan pada media koneksinya. Pada *Switch hub* masih menggunakan kabel UTP sedangkan pada *acces point* sudah menggunakan gelombang radio atau lebih dikenal dengan *wireless (nirkabel)*. (Prabawati, A. 2010:8)

2) *Router*

Router adalah sebuah alat yang mengirimkan paket data melalui sebuah jaringan atau *Internet* menuju tujuannya, melalui sebuah proses yang dikenal sebagai *routing*. (Iwan Sofana:2012).

Menurut Prabawati, Arie. (2010:16) *Router* adalah piranti elektronik yang fungsinya mem-*foward* data antara jaringan computer. *Router* adalah piranti dimana *software* dan *hardware* disetting untuk melakukan *routing* dan mem-*forward* informasi.

3) *LAN Card*

Menurut Siregar, (2010:10), *Wireless* LAN tidak memiliki *physical layout*. Hanya dengan menambah *wireless* NIC maka sebuah *workstation* akan mampu mengirim dan menerima data. Secara umum,

workstation pada *wireless* LAN akan berkomunikasi dengan kecepatan Hingga 20 Mbps.(*Wireless Hub*).

Hotspot

Hotspot area adalah sebuah area terbatas yang dilayani oleh satu atau sekumpulan *access point wireless* LAN standar 802.11 a/b/g. Dimana *user* dapat masuk ke dalam *access point* secara bebas maupun terbatas pada *user* tertentu saja (*password protected*) mengakses *internet* menggunakan peralatan *wireless* (*laptop*, PDA, *Smart Phone*). Tenggono, A. 2011:185).

Mikrotik

Mikrotik adalah sebuah piranti lunak *router* dengan sistem *operasi linux* dan *MS Dos* yang dikombinasikan dengan teknologi *Wireless Local Area Network (W-LAN) aeronet* berkecepatan 2Mbps. Linux yang digunakan pertama kali adalah kernel 2.2 dengan membayar biaya lisensi sebesar 45 dollar America pengguna dapat memperoleh paket level 3.. (Utomo, P.S., 2010:30)

Menurut Riadi, I. (2010:376) *Mikrotik* adalah sistem operasi indepeden berbasiskan *Linux* khusus untuk komputer yang difungsikan sebagai *router*.

Mikrotik dikenal dengan istilah *Level* pada lisensinya. Tersedia mulai dari *Level* 0 kemudian 1, 3 hingga 6, untuk *Level* 1 adalah versi *Demo Mikrotik* dapat digunakan secara gratis dengan fungsi-fungsinya yang sangat terbatas. Tentunya tiap *level* memiliki kemampuan yang berbeda-beda sesuai dengan harganya. (Riadi, I. 2010:377)

Menurut Riadi, I. (2010:377) Level-level pada *Mikrotik* secara singkat dapat dijelaskan sebagai berikut:

a) *Level* 0 (gratis); tida membutuhkan lisensi untuk menggunakannya dan penggunaan fitur hanya dibatasi 24 jam setelah instalasi dilakukan.
b) *Level* 1 (*demo*); pada level ini dapat digunakan sebagai fungsi *routing* standar saja dengan 1 pengaturan serta tidak memiliki limitasi waktu untuk menggunakannya.
c) *Level* 3; sudah mencakup *level* 1 ditambah dengan kemampuan untuk manajemen segala perangkat keras yang berbasisikan kartu jaringan atau *Ethernet* dan pengelolaan perangkat keras tipe klien.
d) *Level* 4; sudah mencakup *level* 1 ditambah dengan kemampuan untuk mengelola perangkat *wireless* tipe akses poin.
e) *Level* 5; mencakup *level* 1, 3 dan 4 ditambah dengan kemampuan mengelola jumlah pengguna *hotspot* yang lebih banyak.
f) *Level* 6; mecakup semua *level* dan tidak memiliki limitasi apapun.

Sistem Keamanan Jaringan *Wi-Fi*

Menurut Hantoro, D. G. (2009:73) Sistem keamanan jaringan komputer yang terhubung ke I*nternet* harus direncanakan dan dipahami dengan baik agar dapat melindungi investasi dan sumber daya didalam jaringan komputer tersebut secara efektif.

Menurut Prabawati, Arie. (2010:15) Celah-celah keamanan pada sebuah jaringan *Wi-Fi* dapat mempengaruhi kinerja sebuah jaringan *Wi-Fi*.

Menurut Prabawati, Arie. (2010:15) terdapat beberapa jenis pengaturan keamanan jaringan Wi-Fi, antara lain:

1) WPA Pre-Shared Key
2) WPA RADIUS
3) WPA2 Pre-Shared Key Mixed.
4) WPA2 RADIUS Mixed
5) RADIUS.
6) WEP.

Untuk mengamankan jaringan wireless menurut Stiawan, D. dan Rini, D.P. (2009:2) dapat menggunakan beberapa model strategi, diantaranya adalah Pemfilteran *MAC Address*, Kunci *Enkripsi WEP* dan *WPA*, *SSID Filtering*, dan penggunaan *Protocol Filtering*.

Enkripsi digunakan untuk mengubah bit setiap data paket untuk melindungi dari para

penyusup, atau pengguna yang tidak berhak. (Stiawan, D. dan Rini, D.P., 2009:2)

Menurut Stiawan, D. dan Rini, D.P., (2009:2) dalam pengimplementasian berbabagi cara macam enkripsi yang digunakan untuk mengamankan suatu jaringan *wireless* diantaranya adalah:

1) *WEP* (*Wired Equivalent Pivacy*)
2) *WPA, Wi-Fi Protected Access (WPA)*

Menurut Stiawan, D. dan Rini, D.P., (2009:2) *RADIUS* merupakan sebuah *protocol* yang memungkinkan perubahan utuk melakukan *Authentication* (otentikasi/pembuktian keaslian), *Authorize* (otoritas/pemberian hak), dan *Accounting* (akuntansi) atau yang bisa disebut AAA.

Authentikasi

Salah satu aspek keamanan komputer adalah aspek *authentication. Aspek authentication* berhubungan dengan identitas atau jati diri atau kepemilikan yang sah. Ada dua masalah yang terkait dengan aspek ini, yang pertama pembuktian keaslian informasi dan yang kedua adalah *access control*. *User authentication* dilakukan untuk memastikan siapa pengguna jaringan sebenarnya. Hal ini untuk mencegah seseorang yang tidak diharapkan dapat mengakses suatu jaringan. *User authentication* mengidentifikasi pengguna jaringan dengan menggunakan *username* dan *password* yang dimasukkan oleh pengguna. (Tenggono, A. 2011:185).

User* dan *Password

Menurut Arief, M. Rudyanto (2008:2) Metode otentikasi konvensional yang selama ini familiar di gunakan adalah menggunakan kombinasi "*username*" dan "*password*" atau biasa juga disebut dengan *metode "single factor authentication*". *Username* adalah sebuah penanda unik yang dapat digunakan untuk mengidentif ikasi seorang *user* yang mencoba masuk (*log on*) kedalam sebuah sistem komputer. *Password* adalah sebuah kombinasi rahasia yang terdiri dari kombinasi huruf, angka, dan karakter khusus.

Captcha

Menurut Setiawan, E. B. (2012:19) *Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA)* dapat dikatakan sebagai suatu teknik yang dilakukan untuk membedakan antara manusia dengan komputer di internet.

CAPTCHA (*Completely Automated Public Turing test to tell Computers and Humans Apart*), juga dikenal sebagai*Human Interactive Proof (HIP)*, adalah tes Turing otomatis di mana kedua generasi tantangan dan tanggapan yang dilakukan oleh program komputer.

Istilah"*CAPTCHA*" pertama kali diperkenalkan pada tahun 2000 olehVon dan kawan-kawannya, Menggambarkan tes yang dapat membedakan manusia dari komputer. Di bawah syarat umum, tes harus:

1) Mudah dipecahkan oleh manusia
2) Mudah dihasilkan dan dievaluasi,
3) Tapi, tidak mudah diselesaikan oleh komputer

Selama beberapa dekade terakhir, sejumlah teknik yang berbeda untuk menghasilkan *CAPTCHA* telah dikembangkan, masing-masing memenuhi sifat yang dijelaskan di atas untuk berbagai derajat. Yang paling umum ditemukan *CAPTCHA* dengan tantangan visual yang membutuhkan pengguna untuk mengidentifikasi karakter *alfa numerik* yang hadir dalam gambar *Obfuscated* dengan beberapa kombinasi kebisingan dan distorsi (Azad, Silky & Jain, Kiran. 2013:15).

Kelebihan dan Fungsidari*CAPTCHA*

Menurut Azad, Silky & Jain, Kiran (2013:15) *CAPTCHA* digunakan dalam upaya untuk mencegah perangkat lunak otomatis dari melakukan tindakan yang menurunkan kualitas pelayanan sistem tertentu. *CAPTCHA* juga digunakan untuk meminimalkan posting otomatis ke berbagai situs.

1) Mencegah Komentar *Spam* di *Blog*.
2) Melindungi Pendaftaran *website*.
3) Melindungi Alamat *Email*.

4) Pencegahan dari Pengikis.
5) Alamat *online Polls.*
6) Mencegah Serangan Kamus.
7) *BotSearch Engine*.
8) Mencegah*Worms* dan *Spam.*

Kelemahan CAPTCHA

Penggunaan *CAPTCHA* selain dapat mengamankan *website* dari serangan *bots*, juga terkadang terlalu menyulitkan untuk diselesaikan sehingga dapat menyita waktu untuk menjawab pertanyaan yang ditampilkan. Tidak jarang bahkan harus sampai beberapa kali untuk mengulang pertanyaan yang berbeda. Dari segi keamanan *CAPTCHA* itu sendiri, para analis keamanan mengkonfirmasi bahwa serangan otomatis terhadap *Captchatext-based* telah berhasil dilakukan sebesar 20% terhadap Google's *CAPTCHA* , 30-35% berhasil dilakukan terhadap *Microsoft's CAPTCHA*, 35% terhadap *Yahoo! CAPTCHA*. Sedangkan serangan terhadap *audio-based CAPTCHA* miliknya *Google* bahkan sekitar 90% berhasil dipecahkan. (Setiawan, E. B., 2012:20)

Karakteristik CAPTCHA

Menurut Setiawan, E. B. (2012:20) karakteristik dari penggunaan *CAPTCHA* harus bersifat :

1. *Automated*, tantangan yang dilakukan harus dihasilkan secara otomatis dan dapat ditingkatkan *level* kesulitannya dengan mudah oleh komputer.
2. *Open*, database dan algoritma dari tantangan yang dilakukan harus bersifat publik.
3. *Usable*, tantangan harus mudah untuk diselesaikan oleh manusia dalam waktu yang wajar.
4. *Secure*, tantangan yang dilakukan harus sulit bagi komputer untuk memecahkan algoritmanya.

3. METODE PENELITIAN

Metode yang digunakan dalam penelitian ini menggunakan dua metode penelitian, yakni metode pengumpulan data dan metode pengembangan sistem.

Metode Pengumpulan data

Metode pengumpulan data yang digunakan peneliti untuk melakukan analisis data dan menjadikannya informasi yang akan digunakan untuk mengetahui permasalah yang dihadapi.

1) Studi Lapangan/Observasi

Metode pengumpulan data dengan cara melakukan observasi dan melakukan wawancara di lokasi penelitian untuk memperoleh keterangan yang berkaitan dengan permasalah jaringan yang ada di SMK Muhammadiyah 2 Malang.

2) Studi Pustaka dan Literatur

Metode studi pustaka dan literatur digunakan untuk menghimpun informasi yang relevan dengan topik atau masalah dalam penelitian.

Metode Pengembangan Sistem

Metode pengembangan sistem yang dilakukan dalam penelitian ini menggunakan metode waterfall yang terdiri dari beberapa tahapan, yaitu:

1) Analisis

Tahap analisis dilakukan dengan menelaah setiap data yang didapat dari data-data sebelumnya, mulai dari konfigurasi jaringan, media yang digunakan, user/pengguna jaringan, dan sistem keamanan jaringan.

2) Desain

Tahap desain bertujuan membuat gambar rancangan topologi jaringan hotspot dan rancangan dari proses sistem keamanan authentikasi yang akan digunakan. Diharapkan dengan gambar ini akan memberikan gambaran seutuhnya kebutuhan yang ada.

3) Simulasi Prototipe

Tahapan simulasi prototipe bertujuan untuk mencoba skrip kode captcha yang digunakan dalam pengamanan sistem authentikasi hotspot

4) Implementasi (Penerapan)

Tahapan implementasi adalah tahapan proses penerapan dari proses sebelumnya. Pada proses implementasi yang dilakukan

adalah instalasi dan konfigurasi rancangan topologi jaringan, serta penerapan kode captcha untuk system keamanan jaringan pada proses authententikasi.

5) Pengujian

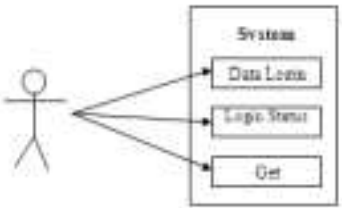
Tahapan pengujian yaitu suatu kegiatan dimana suatu sistem atau komponen dijalankan dalam kondisi tertentu, yang mana hasilnya diamati atau direkam untuk kemudian dilakukan evaluasi. Dalam penelitian ini akan dilakukan pengujian terhadap sistem yang digunakan dalam authentikasi halaman *login hotspot* dengan menambahkan *captcha*. Pengujian akan dilakukan terhadap proses klient ketika *login* pada hotspot serta melakukan pengujian mencoba melakukan serangan terhadap keamanan proses authentikasi jaringan *hotspo*t.

4. HASIL DAN PEMBAHASAN

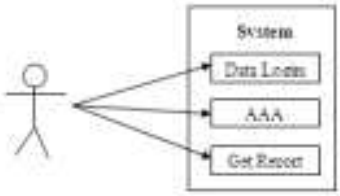
Perancangan Logik

Perancangan logik merupakan perancangan yang lebih menekankan kepada desain yang konseptual. Peneliti akan menggunakan *use case* diagram dan *flowchard* untuk menggmbarkan proses dan logika sistem authentikasi *hotspot* di SMK Muhammadiyah 2 Malang.

Use Case Diagram



Gambar 1*Use Case* Diagram *User*

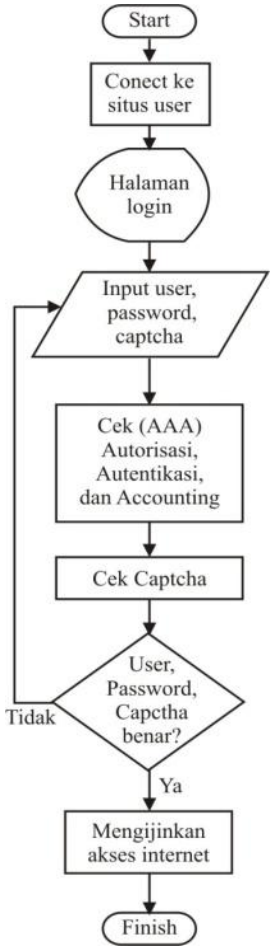


Gambar 2*Use Case* Diagram *Administrator*

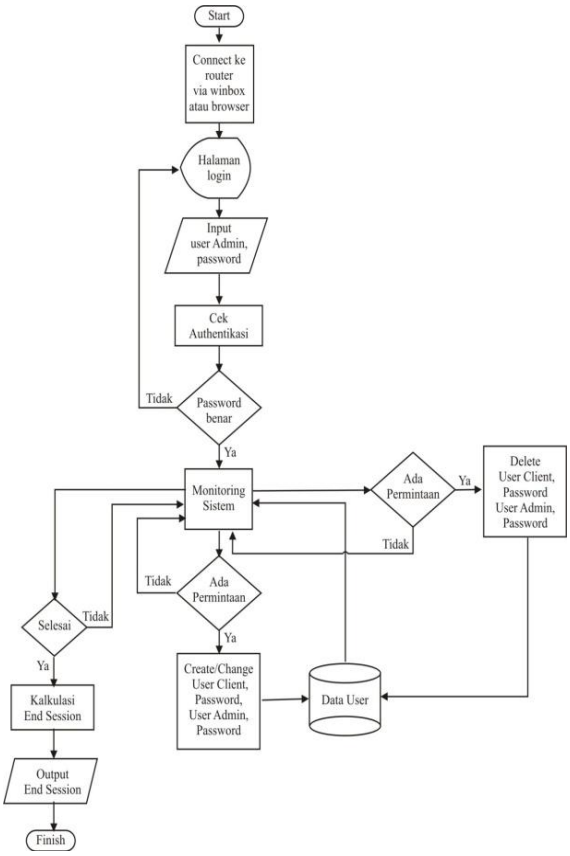
Keterangan:

1. *User*/pengguna adalah guru dan karyawan SMK Muhammadiyah 2 Malang yang menggunakan layanan jaringan *hotspot* di lingkungan SMK Muhammadiyah 2 Malang.
2. *Administrator* adalah orang yang mengelola, memonitor dan mengontrol kinerja jaringan *hotspot* di SMK Muhammadiyah 2 Malang.

Flowchard



Gambar 3 *Flowchard login user*



Gambar 4*Flowchard login administrator*

Rancangan tampilan login

Tampilan standar halaman authentikasi *hotspotmikrotik* masih terlihat sederhana, pada *form login* tersebut hanya terdapat isian untuk *user* dan *password* saja. Dalam penelitian ini akan ditambahkan *captcha* beserta isiannya dibawah isian *user* dan *password*. Rancangan dari halaman authentikasi *hotspot* di SMK Muhammadiyah 2 Malang dengan *captcha* adalah seperti pada Gambar 1 Rancangan tampilan autentikasi *hotspot* dengan *captcha*.

Gambar 5 Rancangan tampilan authentikasi *hotspot* dengan *captcha*.

Algoritma Captcha

Algoritma digunakan dalam dalam pembuatan *captcha* pada proses authentikasi *login hotspot* di SMK Muhammadiyah 2 Malang adalah sebagai berikut:

1) Membuat *random text* yang akan dijadikan sebagai kode verifikasi.
2) Menampilkan *random text* kepada *user*.
3) Menampilkan *button* untuk *refresh captcha*
4) Mencocokkan *input* dari *user* dengan *random text*.

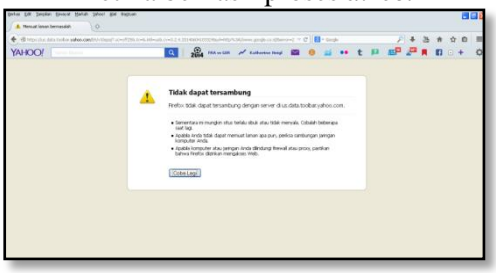
PENGUJIAN

Uji coba hasil dari penelitan dilakukan melalui dua tahapan pengujian, yakni tahapan uji coba pada konfigurasi jaringan *hotspot* dan tahapan uji coba pada proses autentikasi dan keamanan proses authentikasi *hotspot*.

Uji Coba Konfigurasi Jaringan *Hotspot*

Pengujian konfigurasi jaringan *hotspot* dilakukan dengan cara menguji koneksi antara perangkat client dengan jaringan *hotspot Mikrotik* yang sudah dibangun. Pengujian dilakukan dengan cara membuka sebuah alamat *website* melalui *web browser* menggunakan perangkat *client* yang sudah tersambung dengan jaringan *hotspot.* Pada saat proses membuka halaman *web* tersebut *client*akan diarahkan menuju ke halaman *login hotspot.* Apabila perangkat *client* dapat menampilkan halaman *login hotspot* maka jaringan dianggap tersambung. Apabila perangkat*client* tidak dapat menampilkan halaman *login hotspot* maka jaringan dianggap belum tersambung.

Gambar 6 Tampilan halaman *login hotspot* ketika berhasil proses *direct*



Gambar 7 Tampilan halaman *login hotspot* ketika gagal proses *direct*

Dari hasil pegujian konfigurasi jaringan hotpsot yang dilakukan melalui perangkat *client* menggunakan *web browser*, didapatkan hasil perangkat *client* bisa terhubung dengan *hotpsot gateway*. Hal tersebut dapat dibuktikan dengan tampilnya halaman proses authentikasi *hotspot* pada *web browser* perangkat *client* ketika mencoba membuka sebuah halaman *website*.

Uji Coba Proses Autentikasi *Hotspot*

Pengujian authentikasi dilakukan dengan beberapa tahapan pengujian, diantaranya adalah pengujian tampilan halaman *login* proses authentikasi, pengujian proses authentikasi, pengujian *login* menggunakan *user-user* yang sudah terdaftar dan pengujian keamanan proses authentikasi *hotspot*.

Uji Halaman Login Proses Authentikasi

Pengujian halaman authentikasi dilakukan dengan cara menampilkan halaman *login* proses authentikasi *hotspot* melalui *web browser* perangkat *client* dengan kondisi perangkat*client* sudah terhubung dengan jaringan hotspot. Pengujian dilakukan menggunakan 3 macam *web browser* yakni: *Mozilla Firefox, Internet Explorer,* dan *Google Chrome*. Pada *web browser,* perangkat *client* dilakukan percobaan membuka sebuah halaman *website*, pada kondisi tersebut *web browser* tidak akan langsung merespon permintaan untuk membuka halaman *website* tersebut. *Web browser*akan mengarahkan pengguna ke halaman authentkasi *hotspot* untuk melakukan *login* ke jaringan *hotspot* terlebih dahulu, setelah proses *login* berhasil pengguna dapat kembali membuka halaman *website* yang dituju.

Dari hasil pengujian tampilan halaman *login* proses authentikasi *hotspot* menggunakan 3 macam jenis *web browser* yang berbeda didapatkan hasil halaman authentikasi *hotspot* menggunakan *captcha* bisa ditampilan pada *web browser Mozilla Firefox, Google Chrome* dan *Internet Explorer*. Pada pengujian ini dapat diambil analisa bahwa tampilan halaman authentikasi melalui *Mozilla Firefox* dan *Google Chrome* terlihat tertata rapi, sedangkan melalui *Internet Explorer* tampilan halaman *login* proses authentikasi *hotspot* tidak tertata rapi.

Tabel 1 Hasil uji halaman *login hotspot*

No	Web Browser	Hasil	Keterangan
1.	Mozilla Firefox	Dapat ditampilkan	Tertata rapi
2.	Google Chrome	Dapat ditampilkan	Tertata rapi
3.	Internet Explorer	Dapat ditampilkan	Tidak tertata rapi

Uji Proses Authentikasi

Pengujian proses authentikasi dilakukan melalui perangkat *client*. Pada tahapan pengujian proses authentikasi ini dilakukan

pengujian terhadap *form login* proses authentikasi *hotspot*. Cara kerja dari pengujian ini dilakukan dengan menguji dari fungsi masing-masing inputan yang ada pada *form login*, yang terdiri dari inputan *username*, inputan *password* dan inputan kode *captcha*. Pengujian pada proses authentikasi tersebut dilakukan dengan mencoba memasukkan inputan-inputan dengan berbagai macam variasi data masukan ke dalam form inputan yang ada pada halaman *login*.

Dari hasil keseluruhan pengujian proses authentikasi *hotspot* dapat diambil kesimpulan semua inputan *User, Password* dan *Captcha* yang dimasukkan harus bernilai benar agar akses *login* ke jaringan *hotspot* bisa diterima. Namun, akses *login*akan ditolak jika inputan yang dimasukkan ada yang bernilai salah atau dikosongkan, hal tersebut dibuktikan dengan pesan validasi yang ditampilkan ketika setelah menekan *button OK* yang ada pada *form login*.

Tabel 2 Hasil Uji Proses Authentikasi H*otspot* di SMK Muhammadiyah 2 Malang

No	Inputan			Hasil	Keterangan
	User	Password	Captcha		
1	Benar	Benar	Benar	Diterima	Tampil halaman infromasi IP
2	Benar	Benar	Salah	Ditolak	Tampil pesan captcha salah
3	Benar	Salah	Benar	Ditolak	Tampil pesan user & password salah
4	Benar	Salah	Salah	Ditolak	Tampil pesan user & password salah
5	Salah	Benar	Benar	Ditolak	Tampil pesan user & password salah
6	Salah	Benar	Salah	Ditolak	Tampil pesan user & password salah
7	Salah	Salah	Benar	Ditolak	Tampil pesan user & password salah
8	Salah	Salah	Salah	Ditolak	Tampil pesan user & password salah
9	Kosong	Benar	Benar	Ditolak	Tampil pesan user kosong
10	Benar	Kosong	Benar	Ditolak	Tampil pesan password kosong
11	Benar	Benar	Kosong	Ditolak	Tampil pesan captcha kosong

Uji *Login User*

Pengujian *login user* dilakukan untuk menguji masing-masing *user* yang sudah terdaftar bisa atau tidaknya digunakan untuk *login* pada authentikasi *hotspot*. Selain untuk menguji masing-masing *user* juga dilakukan pengujian untuk mengetahui bisa atau tidaknya jika sebuah *data user* digunakan untuk *login* secara bersamaan. Proses pengujian dilakukan dengan cara mencoba melakukan *login* terhadap proses authentikasi jaringan *hotspot* menggunakan masing-masing *user* dan *password* yang sudah terdaftar pada jaringan *hotspot* di SMK Muhammadiyah 2 Malang.

Dari hasil pengujian *login User* dapat diambil sebuah kesimpulan bahwa sebuah *User* dan *Password* hanya bisa digunakan oleh satu orang pengguna dan tidak bisa digunakan *login* secara bersamaan, hal tersebut dibuktikan dengan adanya pesan yang tampil pada halaman authentikasi ketika pengguna melakukan proses *login* .

Uji Keamanan Authentikasi *Hotspot*

Pengujian keamanan authentikasi *hotspot* dilakukan dengan cara melakukan serangan/hacking dari proses authentikasi *hotspot* tersebut. Dalam pengujian ini, peneliti akan melakukan pengujian terhadap halaman *login* authentikasi *hotspo*t sebelum menggunakan *captcha* dan setelah menggunakan captcha dengan menggunakan teknik *brute force attack*.

Serangan *brute force* adalah sebuah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci yang memungkinkan. Di dalam pengujian *brute force* terhadap keamanan authentikasi *hotspot* ini menggunakan *tool aircrack* dan *reaver* yang sudah terinstall di perangkat *client* dengan menggunakan sistem operasi *Linux Ubuntu*.

Proses pengujian keamanan authentikasi *hotspot* dengan teknik *brute force attack* dilakukan secara dua tahap. Tahap pertama dilakukan serangan terhadap jaringan *hotspot*

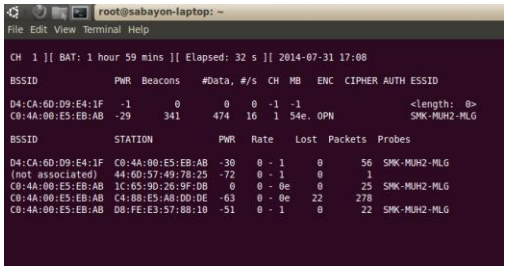
dengan kondisi halaman *login* proses authentikasi *hotspot* belum terdapat *captcha*, tahap kedua dilakukan serangan dengan kondisi halaman *login* sudah terdapat *captcha*. Di dalam pengujian ini, *password* yang digunakan untuk *admin* dibuat sangat lemah dengan hanya menggunakan tiga buah karakter huruf kecil (*lowercase*).

Tabel 3 Hasil *brute force attack* sistem keamanan jaringan *hotspot*

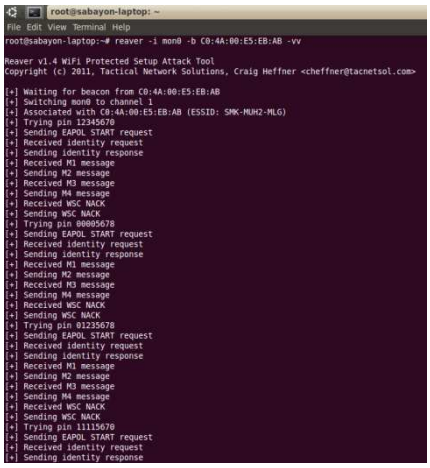
No.	Pengujian	Waktu	Hasil	Keterangan
1.	Authentikasi tanpa captcha	8 jam	Belum terpecahkan	
2.	Authentikasi menggunakan captcha	10 jam	Belum terpecahkan	

Hasil dari pengujian terhadap sistem keamanan jaringan *hotspot* di SMK Muhammadiyah 2 Malang menggunakan teknik *brute force attack* adalah kode kunci sistem keamanan authentikasi *hotspot* berbasis *captive portal* menggunakan *mikrotik* tidak dapat dipecahkan menggunakan serangan *brute force*. Pengujian tersebut dilakukan terhadap dua model halaman *login* proses authentikasi dan lama waktu yang digunakan di dalam proses penyerangan menggunakan waktu selama 8 sampai 10 jam setiap satu model halaman *login* proses authentikasi.

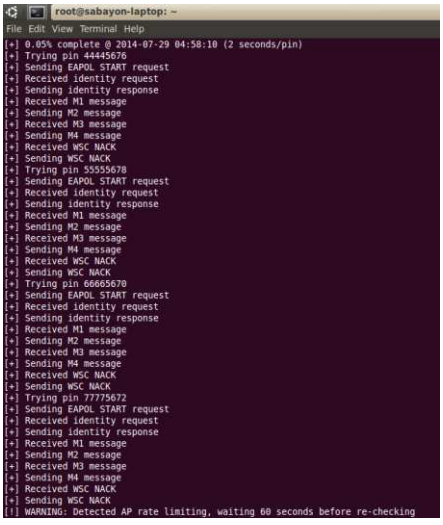
Dari hasil pengujian terhadap dua model sistem keamanan jaringan *hotspot* di SMK Muhammadiyah 2 Malang menggunakan teknik *brute force attack*,dapat diambil kesimpulan bahwa dengan teknik *brute force attack* belum dapat membongkar kunci keamanan jaringan *hotspotmikrotik.*



Gambar 8 Data jaringan *wifi* yang akan diserang

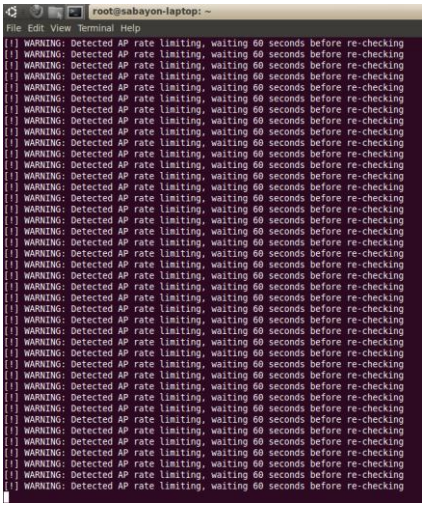


Gambar 9 Informasi data tentang jaringan *wifi* (bagian pertama)



Gambar 10 Informasi data tentang jaringan *wifi* (bagian kedua)

Gambar 11 Informasi data tentang jaringan *wifi* (bagian ketiga)



Gambar 12 Proses brute *force attack* selama 10 jam

5. KESIMPULAN

Penggunaan *captcha* pada halaman *login* proses authentikasi *hotspot* menggunakan *Mikrotik* belum dapat memberikan bukti kekuatan sistem keamanan jaringan *hotspot*. Hal tersebut dibuktikan dengan pengujian melakukan serangan terhadap dua model halaman *login* proses authentikasi tanpa *captcha* dan menggunakan *captcha* menggunakan teknik *brute forcé attack*. Di dalam proses pengujian tersebut menggunakan rentang waktu yang sama dan tipe *password* yang sangat lemah tidak didapatkan perbedaan dari hasil yang dicapai, karena *capthca* yang digunakan bersifat *client side* dan tidak tersimpan di *server hotspot mikrotik*. Sehingga sistem keamanan authentikasi *hotpsot mikrotik* berbasis *captive portal* yang hanya menggunakan *user* dan *password* sebagai proses authentikasi sudah memiliki tingkat keamanan yang baik walaupun tanpa menggunakan *captcha*.

Kode *captcha* yang ditampilkan pada proses authentikasi ditampilkan secara *random*, sehingga kode *captcha* akan selalu berubah ketika halaman *login* proses authentikasi di *refresh*. Dengan ditambahkannya validasi pada proses authentikasi *hotspot* di SMK Muhammadiyah 2 Malang juga memberikan kemudahan bagi pengguna/*user* untuk mengetahui letak kesalahan ketika melakukan *login* pada jaringan *hotspot*.

6. DAFTAR PUSTAKA

1. Amir, Zaid. 2012. *Analisis Vulnerabilitas Host Pada Keamanan Jaringan Komputer Di PT. Sumeks Tivi Palembang (PALTV) Menggunakan Router Berbasis Unix*. (http://news.palcomtech.com/wp-content/uploads/2013/03/ZAID_TE0203 2012.pdf tanggal 21 Juli 2014 Jam 11.15)
2. Anhar, 2010. *Panduan Menguasai PHP & MySQL Secara Otodidak*. Jakarta: Mediakita
3. Arief, M. Rudyanto. 2008. *Otentikasi Multi Faktor Untuk Meningkatkan Keamanan Komputer*.(http://p3m.amikom.ac.id/p3m/dasi/des06/08%20-%20STMIK%20AMIKOM%20Yogyakarta%20Makalah%20M%20RUDYANTO%20ARIEF.pdf Tanggal 21 Juli 2014 Jam 21.45)

4. Azad, Silky & Jain, Kiran. 2013. *CAPTCHA: Attacks and Weaknesses against OCR Technology*. (https://globaljournals.org/GJCST_Volume13/3-CAPTCHA-Attacks-and-Weaknesses.pdf tanggal 21 Juli 2014 Jam 11.30)
5. Hantoro, Dwi, Gunadi, 2009, *WIFI (Wireless LAN) Jaringan Komputer Tanpa Kabel*, Bandung:INFORMATIKA
6. Kustiyahningsih, Yeni. 2011. *Pemrograman Basis Data Berbasis Web Menggunakan PHP & MySQL*. Jakarta: Graha Ilmu.
7. Prabawati, Arie. 2010. *Tips Jitu Optimasi Jaringan Wi-Fi*. Yogyakarta: ANDI
8. Pratama, Antonius, N. W., 2010. *Codelgniter: Cara Mudah Membangun Aplikasi PHP*. Jakarta: Mediakita
9. Riadi, Imam. 2010. *Optimasi Bandwidth Menggunakan Traffic Shapping*. (http://jifo.uad.ac.id/upload/makalah/optimasi_bandwith_menggunakan_traffic_shapping.pdf tanggal 16 Mei 2014 Jam 8.50)
10. S, Sudarma. 2010. *Membangun Jaringan Komputer & Internet*. Jakarta: Mediakita
11. Setiawan, Eko, B., 2012. *Optimalisasi Keamanan Website Menggunakan Captcha – Ad Video* **.**Bandung : Komputa
12. Sibero,Alexander F.K. 2012. *Kitab Suci Web Programing*. Jakarta: Mediakom.
13. Siregar, Edison. 2010. *Langsung Praktik Mengelola Jaringan Lebih Efektif Dan Lebih Efisien*. Yogyakarta : Andi
14. Sofana, Iwan. 2012. *CISCO CCNA & Jaringan Komputer*. Bandung: Informatika
15. Stiawan, D. dan Rini, D.P. 2009. *Analisis Perbandingan Sistem Keamanan WEP/WPA/RADIUS Pada Jaringan Publik Wireless Hotspot*. (http://elektro.um.ac.id/sneie/files/B1.%20IT/01_ANALISIS%20PERBANDINGAN%20SISTEM%20KEAMANAN%20WEP_WPA_RADIUS.pdf Tanggal 18 Mei 2014 Jam 19.30)
16. Sutarman. 2012. *Pengantar Teknologi Informasi*. Jakarta: Bumi Aksara
17. Utomo, Puputro, S. 2010. *Analisis Kinerja VPN Berbasis Mikrotik Pada Proses Kompresi-Dekompresi dan Enkripsi-Dekripsi Di Bandingkan VPN Berbasis Open Source*. Skripsi tidak diterbitkan. Jakarta: Fakultas Sains dan Teknologi Universitas Islam Negeri Syarif Hidayatullah.