PERTEMUAN 15
MIKTROTIK HOTSPOT SYSTEM DAN RADIUS SERVER

A. TUJUAN PEMBELAJARAN

Pada bab ini akan dijelaskan mengenai Mikrotik Hotspot System dan Radius Server.

B. URAIAN MATERI

1. Hotspot Sistem

Gambar 6.3 Topologi Hotspot System

Hotspot digunakan untuk melakukan autentikasi pada jaringan local. Autentikasi yang digunakan berdasarkan pada HTTP atau HTTPS protocol dan dapat diakses dengan menggunakan Web Browser. Hotspot sendiri adalah sebuah system yang mengkombinasikan beberapa macam features dari MikroTik RouterOS yang sangat mudah dikonfigurasi. Hotspot System adalah sebuah teknologi autentikasi yang biasa digunakan ketika kita akan menyediakan akses internet pada areal publik, seperti : Hotel, café, airport, taman, mall dll. Teknologi akses internet ini biasanya menggunakan jaringan wireless atau wired. Kita bisa menyediakan akses internet gratis dengan menggunakan hotspot atau bisa juga menggunakan Voucer untuk autentikasinya.

a. Cara Kerja Hotspot Sistem

Ketika kita memcoba membuka sebuah web page maka router yang sudah memiliki hotspot system, akan men cek apakah user sudah di autentikasi pada system hotspot tersebut. Jika belum melakukan autentikasi, maka user akan di arahkan pada hotspot login page yang harus di isikan berupa usernama dan password. Jika informasi login yang dimasukkan sudah benar, maka router akan memasukkan user tersebut kedalam hotspot sytem dan client sudah bisa mengakses halaman web. Selain itu akan muncul popup windows berisi status ip address, byte rate dan time live. Dari urutan proses diatas, maka user sudah bisa mengakses halaman internet melalui hotspot gateway.

b. Keunggulan Hotspot Sistem

Hotpost system digunakan untuk autentikasi user, penggunaan akses internet dapat dihitung berdasarkan waktu dan data yang di download / upload. Selain itu dapat juga dilakukan limitasi bandwidth berdasarkan data rate, total data upload/download atau bisa juga di limit berdasarkan lama pemakaian. Hotspot system juga mendukung system Radius.

Terdapat beberapa metode autentikasi yang berbeda dalam profile setting, jenis autentikasi tersebut adalah:

1. HTTP PAP - Metode yang paling sederhana, yang menunjukkan halaman login HotSpot dan mengharapkan untuk mendapatkan info otentikasi (username dan password yaitu) dalam teks biasa. Perhatikan bahwa password yang tidak dienkripsi saat ditransfer melalui jaringan. Penggunaan lain dari metode ini adalah kemungkinan informasi otentikasi keras-kode di halaman login servlet hanya menciptakan link yang sesuai.
2. HTTP CHAP - metode standar, yang meliputi tantangan CHAP di halaman login. Tantangan CHAP MD5 hash akan digunakan bersama-sama dengan password user untuk menghitung string yang akan dikirim ke gateway HotSpot. Hasil hash (sebagai password) bersama dengan username yang dikirim melalui jaringan ke layanan Hotspot (sehingga, sandi tidak pernah dikirim dalam teks biasa melalui IP jaringan). Pada sisi klien, MD5 algoritma diimplementasikan dalam applet JavaScript, jadi jika browser tidak mendukung JavaScript (seperti, misalnya, Internet Explorer 2.0 atau beberapa browser PDA), tidak akan dapat mengotentikasi pengguna. Hal ini dimungkinkan untuk memungkinkan password yang tidak terenkripsi dapat diterima dengan menghidupkan metode otentikasi HTTP PAP, tetapi tidak direkomendasikan (karena pertimbangan keamanan) untuk menggunakan fitur itu.
3. HTTPS - protokol SSL ini hampir sama seperti HTTP PAP, tetapi menggunakan untuk mengenkripsi transmisi. HotSpot pengguna hanya mengirim passwordnya tanpa tambahan hashing (catatan bahwa tidak ada perlu khawatir tentang paparan plain-text password melalui jaringan, sebagai transmisi itu sendiri dienkripsi). Dalam kedua

kasus, metode HTTP POST (jika tidak memungkinkan, maka - HTTP GET method) digunakan untuk mengirim data ke gateway HotSpot.

4. HTTP cookie - setelah setiap login berhasil, ada cookie yang dikirim ke browser web dan sama cookie akan ditambahkan ke daftar cookie HTTP aktif. Lain kali pengguna yang sama akan mencoba untuk log in, web browser akan mengirimkan cookie http. Cookie ini akan dibandingkan dengan yang disimpan pada gateway HotSpot dan hanya jika sumber alamat MAC dan ID secara acak yang dihasilkan sesuai dengan yang tersimpan pada gateway, pengguna akan secara otomatis login menggunakan informasi login (Username dan pasangan password) digunakan bila ada cookie yang pertama kali dihasilkan. Jika tidak, user akan diminta untuk login, dan di otentikasi kasus berhasil, cookie lama akan dihapus dari lokal HotSpot daftar cookie aktif dan yang baru dengan ID acak yang berbeda dan waktu kedaluwarsa akan ditambahkan ke daftar dan dikirim ke web browser. Hal ini juga memungkinkan untuk menghapus cookie di logoff user manual (tidak di halaman server default). Metode ini hanya dapat digunakan bersama dengan HTTP PAP, HTTP CHAP atau metode HTTPS karena akan ada apa-apa untuk menghasilkan cookie di tempat pertama sebaliknya.

5. MAC address - mencoba untuk mengotentikasi klien segera setelah mereka muncul di daftar host (yaitu, segera setelah mereka telah mengirim paket apapun ke server HotSpot), klien menggunakan alamat MAC sebagai username.

2. Radius Server

Adalah server Remote Authentikasi Dial-in Service (RADIUS), sebuah protocol keamanan jaringan komputer berbasis server yang sering digunakan untuk melakukan authentikasi dan otorisasi serta pendaftaran akun (account) pengguna secara terpusat untuk mengakses jaringan yang aman. Server Radius menyediakan mekanisme keamanan dengan menangani otentikasi dan otorisasi koneksi yang dilakukan user. Pada saat komputer client akan menghubungkan diri dengan jaringan maka server Radius akan meminta identitas user (username dan password) untuk kemudian dicocokkan dengan data yang ada dalam database server Radius untuk kemudian ditentukan apakah user diijinkan untuk menggunakan layanan dalam jaringan komputer. Jika proses otentikasi dan otorisasi berhasil maka proses pelaporan dilakukan, yakni dengan mencatat semua aktifitas koneksi user, menghitung durasi waktu dan jumlah transfer data dilakukan oleh user. Proses pelaporan yang dilakukan server Radius bisa dalam bentuk waktu (detik, menit, jam, dll) maupun dalam bentuk besar transfer data (Byte, KByte, Mbyte) (Anonim-B, 2006). Software server Radius yang digunakan dalam penelitian ini adalah Freeradius yang bersifat modular dan memiliki banyak fitur. Freeradius merupakan software server yang berbasis pada open source dan berlisensi GPL.

a. Konsep Cara Kerja secara singkatnya adalah sebagai beikut

Gateway router akan mengarahkan user pada halaman login dan memaksa untuk melakukan otentifikasi atau payment terlebih dahulu (jika diimplementasikan system akunting) sebelum user mengakses external network, otentifikasi yang dilakukan user pada form login yg disebut captive portal, lalu user dan password yang diisikan kedalam form tersebut akan disingkronkan dengan user yang ada pada server radius.

Kelebihan dan Kelemahan RADIUS

Beberapa kelebihan yang diberikan oleh protokol RADIUS yaitu :

1) Menjalankan sistem administrasi terpusat,
2) Protokol connectionless berbasis UDP yang tidak menggunakan koneksi langsung,
3) Mendukung autentikasi Password Authentication Protocol (PAP) dan Challenge Handshake Authentication Protocol (CHAP) Password melalui PPP.

Pada protokol RADIUS juga masih ditemukan beberapa kelemahan seperti :

1) Tidak adanya autentikasi dan verifikasi terhadap access request,
2) Tidak sesuai digunakan pada jaringan dengan skala yang besar,
3) MD5 dan shared secret; metode shared secret sudah berisiko untuk diterapkan, hal ini dikarenakan lemahnya MD5 hash yang menyimpan tanggapan autentikator sehingga Hacker / penyusup dapat dengan mudah mengetahui paket access-request beserta tanggapannya dengan cara melakukan penghitungan awal terhadap perhitungan MD5,
4) Pemecahan password ; skema proteksi password yang dipakai adalah stream-chiper, dimana MD5 digunakan sebagai sebuah ad hoc pseudorandom number generator (PRNG). 16 oktet pertama bertindak sebagai sebuah synchronous stream chiper dan yang menjadi masalah adalah keamanan dari cipher ini

3. User Manager

UserManager merupakan fitur AAA server yang dimiliki oleh Mikrotik. Sesuai kepanjangan AAA (Authentication, Authorization dan Accounting), UserManager memiliki DataBase yang bisa digunakan untuk melakukan autentikasi user yang login kedalam network kita, memberikan kebijakan terhadap user tersebut misalnya limitasi transfer rate, dan juga perhitungan serta pembatasan quota yang dilakukan user kita nantinya.

UserManager ini akan memudahkan kita yang ingin membuat layanan internet publik secara luas, misalnya hotspot-hotspot di cafe, mall, hotel dan sebagainya, karena dengan menggunakan UserManager ini kita cukup membuat 1 account user, dan account user tersebut bisa digunakan atau diakses dari router-router Hotspot yang sudah kita pasang.

Informasi service yang bisa kita simpan dalam database UserManager meliputi:

HotSpot users.

PPP (PPtP/PPPoE) users.

DHCP Lease.

Wireless AccessList.

RouterOS users.

4. Tipe Autentikasi pada Sequrity Profile

1. WEP

WEP adalah security untuk wireless yang agak lama. Tipe security ini mudah untuk dicrack atau di sadap orang luar. WEP menggunakan 64bit dan 128bit. Ada dua cara untuk memasukkan WEP key, apakah Anda setkan sendiri atau generate menggunakan passphrase.Passphrase akan generate otomatis WEP key untuk Anda bila Anda masukkan abjad dan tekan generate. Untuk pengatahuan Anda, ia hanya bisa memasukkan 0-9 dan AF (hexadecimal).Panjang key tergantung jenis securiy Anda, jika 64bit, Anda masukkan 10key, dan untuk 128key Anda kena masukkan 26key. Tak bisa kurang dan lebih.

2. WPA-PSK

WPA-PSK adalah security yang lebih update dari WEP. WPA-PSK memiliki decryption yang ada pada WEP. Bahkan ia menambahkan security yang lebih pada wireless Anda. WPA-PSK masih bisa dicrack atau disadap, tetapi memakan waktu lebih lama dari WEP. Panjang key adalah 8-63, Anda bisa memasukkan apakah 64 hexadecimal atau ASCII (seperti biasa).

3. WPA2-PSK

WPA2-PSK adalah security terbaru untuk wireless, dan lebih bagus dari WEP dan WPA-PSK, tetapi masih bisa untuk dicrack atau disadap tetapi sangat memakan banyak waktu. Dalam WPA2-PSK ada dua jenis decryption, Advanced Encryption Standard (AES) dan Temporal Key Integrity Protocol (TKIP). TKIP banyak kelemahan sehingga lebih baik Anda menggunakan AES. Panjang key adalah 8-63, Anda bisa memasukkan apakah 64 hexadecimal atau ASCII (seperti biasa)

C. SOAL LATIHAN/TUGAS

D. DAFTAR PUSTAKA

Buku

Link and Sites: