ANALISIS DAN PERANCANGAN KEAMANAN DAN MANAJEMEN JARINGAN WIRELESS PADA PT. SEMEN BATURAJA (PERSERO)

Beni Andesta[1], Ahmad Luthfi[2], Suryayusra[3],.
Dosen Universitas Bina Darma [1], Mahasiswa Universitas Bina Darma[2]
Jalan Jenderal Ahmad Yani No.12 Palembang
Pos-el : beni.andesta@ymail.com[1], suryayusra@yahoo.co.id[2]

ABSTRACT: PT**.** Semen Baturaja (Persero) *is a State Owned Enterprise (SOE) is engaged in the cement industry. Currently* PT. Semen Baturaja (Persero) *had assets of Communications Information technology has (ICT) in the form of information systems, database systems, and computer network infrastructure. .* Semen Baturaja (Persero) *also have used technology as a media-based wireless LAN supporting business operations, and as a liaison employees and guests who use mobile devices (laptops, tablets, smartphones, etc.) to the local network (Intranet) or public (Internet).*
To improve WLAN security and network management in this study the authors designed WLAN security and network management available today. The need for this design is to take advantage of features usermanager mikrotik, wireless router using dd-wrt firmware and the dude as monitoring client.

Key word: Wireless LAN, mikrotik, *user manager, dd-wrt, the dude*

ABSTRAK: PT. Semen Baturaja (Persero) adalah Badan Usaha Milik Negara (BUMN) yang bergerak di bidang industri semen. Saat ini PT. Semen Baturaja (Persero) telah memiliki aset *Information Comunication Teknology (ICT)* berupa sistem informasi, sistem basis data, dan infrastruktur jaringan komputer. PT. Semen Baturaja juga telah memanfaatkan teknologi berbasis *Wireless LAN* sebagai media pendukung operasi bisnis dan sebagai penghubung karyawan maupun tamu yang menggunakan perangkat *mobile (Laptop, tablet, smartphone, dll)* ke jaringan lokal (Intranet) maupun publik (Internet).
Untuk meningkatkan kemanan dan manajemen jaringan *WLAN* maka pada penelitian ini penulis merancang keamanan dan manajemen jaringan *WLAN* yang ada saat ini. Adapun kebutuhan untuk perancangan ini yaitu mikrotik dengan memanfaatkan fitur *usermanager*, *wireless router* menggunakan *firmware dd-wrt* dan the dude sebagai *monitoring* klien.

Kata kunci: *Wireless LAN*, mikrotik, *user manager*, *dd-wrt*, *the dude*

I. PENDAHULUAN

1.1 Latar Belakang

Penggunaan jaringan komputer selama beberapa dekade telah digunakan untuk saling berhubungan pada proses bisnis di perusahaan, perguruan tinggi, antar kota, ataupun antar wilayah. Pada awalnya jaringan komputer menggunakan kabel untuk saling berhubungan, namun perlahan hal ini berubah menuju ke arah pemakaian jaringan nirkabel. Aplikasi jaringan nirkabel ini memberikan dampak perubahan yang cukup signifikan yang memungkinkan orang-orang bisa memperluas ruang kerja mereka karena tidak terikat pada penggunaan kabel. M. Setiawan Hidayat (2009) menjelaskan bahwa banyak *benefit* yang nyata dari penggunaan jaringan wireless, terutama yang berkaitan dengan masalah yang terdapat pada jaringan kabel. Salah satu *benefit* dari penggunaan jaringan *wireless* adalah relatif tidak adanya batasan jarak. Biasanya kabel harus dipasang mengikuti bentuk dinding, melintasi lantai dan lain-lain. Jaringan *wireless* meniadakan hal ini karena bersifat *line of sight.*

Saat ini jaringan komputer nirkabel atau sering disebut *Wireless Local Area Network (WLAN)* sudah menjadi *trend* dalam jaringan komputer, karena memungkinkan efesiensi dalam implementasi dan pengembangan jaringan komputer sehinga dapat meningkatkan mobilitas *user* dan mengingat keterbatasan dari teknologi jaringan kabel. Jemis Pangaribuan (2011) memberikan fakta dan hasil riset dari berbagai lembaga riset internasional seperti Gartner, ABI *Research*, WiFi *Aliance* tentang *market trend* di bidang *wireless*:

1. Sebanyak 43% pekerja *enterprise* sudah menggunakan *wireless LAN* pada tahun 2010, dan akan mengalami pertumbuhan 58% di tahun 2014;
2. Sebanyak 580 Juta peralatan *WiFi* pada tahun 2009, diantaranya *handset (Mobility);*
3. Dua tahun lalu 20% *handset* sudah menggunakan *Wifi* 80.11n;
4. Pertama kalinya, *Laptop* sudah melampaui penjualan *Desktop* pada tahun 2009.

Artinya, kebutuhan akan akses layanan jaringan *Enterprise Wireless* mutlak diterapkan, karena teknologi ini bersifat fleksibel, lebih *secure*, mudah dikelola, murah investasinya dan mendukung program *Green Technology*.

Sedangkan Kemudahan yang di tawarkan oleh teknologi *WLAN* (Gunadi 2009) antara lain:

1. **Mobilitas,** *User* dapat terhubung kedalam jaringan untuk mengakses file, mengambil data serta melakukan koneksi ke internet tanpa perlu menggunakan kabel;
2. **Kemudahan Instalasi,** Jaringan nirkabel lebih mudah untuk diimplementasikan karena tidak membutuhkan pemasangan kabel yang kompleks sehingga dapat menghemat waktu.

PT. Semen Baturaja (Persero) adalah Badan Usaha Milik Negara (BUMN) yang bergerak di bidang industri semen. Saat ini PT. Semen Baturaja (Persero) telah memiliki aset *Information Comunication Teknology (ICT)* berupa sistem informasi, sistem basis data, dan infrastruktur jaringan komputer. Aset *ICT* yang telah berjalan saat ini sebagai media pendukung operasi bisnis, baik itu terhubung melalui kabel atau nirkabel. Hampir 80% (k.a Biro *ICT*) karyawan berhubungan dengan jaringan komputer setiap harinya untuk melakukan pekerjaan masing-masing.

Dalam operasi bisnis yang telah terintegrasi dengan komputer, saat ini PT. Semen Baturaja telah memanfaatkan teknologi berbasis *Wireless LAN* sebagai media pendukung operasi bisnis dan sebagai penghubung karyawan maupun tamu yang menggunakan perangkat *mobile* (*Laptop, tablet, smartphone,* dll) ke jaringan lokal (Intranet) maupun publik (Internet). Namun jaringan *WLAN* yang sedang berjalan saat ini belum termanajemen dengan baik. Sebagai

salah satu contoh adalah masalah topologi, topologi saat ini dinilai kurang baik, karena akan menyulitkan *Administrator* jaringan dalam melakukan *monitoring*, karena harus mengakses satu-persatu *Access Point (AP)* untuk melakukan pengawasan terhadap pengguna jaringan *WLAN*. Masalah yang kedua yaitu masalah keamanan, keamanan yang di gunakan saat ini adalah *WEP* yang sudah terbukti tidak aman.

Dengan kondisi di atas maka dibutuhkan manajemen yang baik dan peningkatan kemanan untuk melindungi data pada lalu lintas jaringan *WLAN*.

1.2 Perumusan Masalah

Berdasarkan latar belakang diatas, maka penulis merumuskan permasalahan dalam penelitian ini yaitu:

1. Bagaimana merancang topologi jaringan *wireless* yang aman?
2. Bagaimana merancang kebijakan keamanan jaringan *WLAN* pada PT. Semen Baturaja (Persero) ?

1.3 Batasan Masalah

Agar penelitian lebih terarah dan tidak menyimpang dari permasalahaan yang ada, maka perlu adanya batasan masalah. Adapun batasan masalah dalam penelitian ini adalah :

1. Jaringan yang di analisis adalah jaringan *WLAN* yang sedang berjalan pada kantor pusat PT. Semen Baturaja (Persero) Palembang;
2. Konfigurasi Mikrotik RouterBoard dan konfigurasi *Wireless* Router;
3. Konfigurasi portal *login hotspot*.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Penelitian ini bertujuan untuk mendesain ulang jaringan *WLAN* dan merancang kebijakkan kemanan yang tepat untuk meningkatkan keamanan pada jaringan *WLAN* PT. Semen Baturaja (Persero).

1.4.2 Manfaat

Adapun manfaat dari penelitian ini adalah :

1. Dengan adanya *server* jaringan *WLAN* terpusat maka *administrator* jaringan dapat memonitor aktifitas *client* yang terhubung ke jaringan *WLAN* dan mendapatkan informasi yang menggambarkan keadaan jaringannya;
2. Dengan peningkatan keamanan jaringan *WLAN*, maka mengurangi kemungkinan pengguna yang tidak berhak untuk mengakses jaringan *WLAN* yang ada di PT. Semen Baturaja (Persero).

II. METODOLOGI PENELITIAN

2.1 Metode Pengumpulan Data

Dalam melakukan pengumpulan data, penulis menggunakan beberapa cara yaitu :

1. Studi Pustaka

   Untuk mendapatkan data yang sifatnya teoritis, yaitu dengan cara membaca literatur yang relevan dengan penelitian yang penulis lakukan.

2. Metode Observasi

   Data dikumpulkan dengan melihat secara langsung dari objek yang diteliti pada Kantor Pusat PT. Semen Baturaja (Persero), yaitu dengan mengamati infrastruktur jaringan *WLAN* dan Keamanan yang digunakan.

3. Wawancara

   Data dikumpulkan dengan cara melakukan wawancara secara langsung kepada pihak yang terkait dengan aset *ICT* yang ada di Kantor Pusat PT. Semen Baturaja (Persero) Palembang.

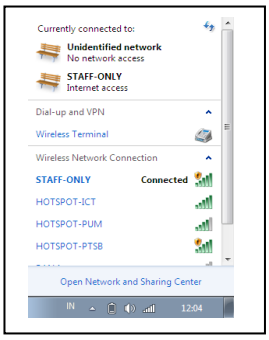
2.2 Metode Penelitian

Pada penelitian ini penulis menggunakan metode *Action Research*. Adapun tahapan-tahapan yang akan penulis lakukan sesuai dengan judul yang penulis angkat yaitu tentang Analisis dan Perancangan Keamanan dan Manajemen Jaringan Wireless , adalah sebagai berikut :

1. Melakukan diagnosa (*diagnosing*)
2. Membuat rencana tindakan (*action planning*)
3. Melakukan tindakan (*action taking*)
4. Melakukan evaluasi (*evaluating*)
5. Pembelajaran (*learning*)

III. HASIL

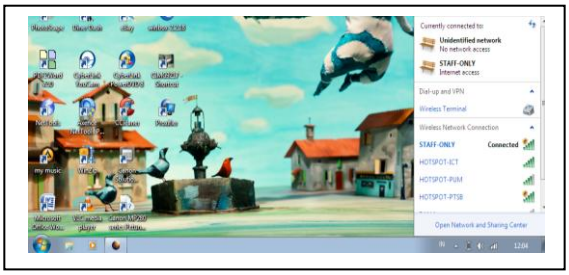
Setelah tahap demi tahap sudah peneliti lakukan dalam merancang keamanan dan manajemen jaringan *wireless* dengan *multiple SSID, STAFF-ONLY* dan *HOTSPOT*-PTSB, sebuah peralatan *WLAN* dapat mendeteksi kedua buah *SSID*. Kedua *SSID* tersebutpun dapat diakses sesuai dengan *username* dan *password* yang telah dibuat pada *usermanager* mikrotik. Pengguna jaringan *WLAN* baik dari *SSID STAFF-ONLY* maupun *SSID HOTSPOT*-PTSB, juga mendapat IP *Address* secara otomatis dari sebuah *DHCP server*. Berikut merupakan hasil pendeteksian pengguna jaringan nirkabel:



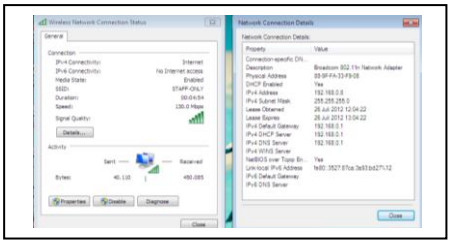
Gambar 4.1 Hasil *scan* dua buah *SSID*

3.1 *Testing* koneksi *SSID STAFF-ONLY*

Berikut ini *testing* dari klien yang terkoneksi ke *SSID STAFF-ONLY*, *SSID* ini hanya untuk karyawan PT. Semen Baturaja saja. Pertama klien akan menemukan dua buah *SSID* dari perangkatnya kemudian mengkoneksikan sesuai dengan hak aksesnya. Jika user hanya ingin internet saja *user* karyawan dapat memilih *SSID HOTSPOT*-PTSB, namun jika user karywan ingin mengakses internet dan aplikasi yang terdapat di server lokal , user dapat memilih *SSID STAFF-ONLY*. ini adalah hasil dari koneksi *user* karyawan dengan *SSID STAFF-ONLY*:



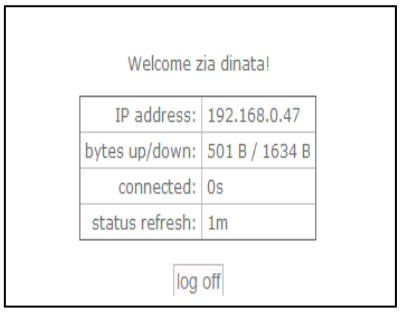
Gambar 4.1 Testing koneksi SSID STAFF-ONLY



Gambar 4.2 IP Address user karyawan yang terkoneksi ke STAFF-ONLY

Setelah user terkoneksi ke SSID STAFF-ONLY dan mendapat IP Address DHCP dari mikrotik, kemudian dilanjutkan dengan membuka web browser, pada penelitian ini peneliti menggunakan browser Google Crome. Jika user mengakses www.google.com atau halaman lainnya, maka akan di di*direct* ke halaman login hotspot PT. Semen Baturaja. Berikut ini adalah tampilan halam login yang sudah peneliti rubah dari tampilah default dari mikrotik:

Gambar 4.3 Halaman login untuk user STAFF-ONLY

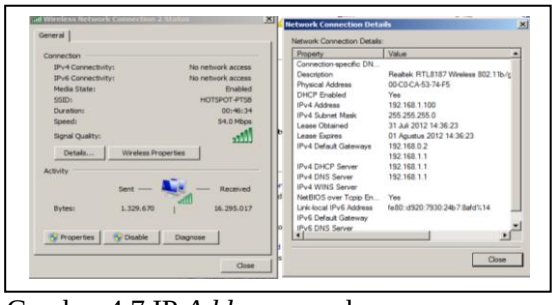


Gambar 4.4 Informasi user karyawan setelah melakukan login

3.2 Testing koneksi SSID HOTSPOT-PTSB

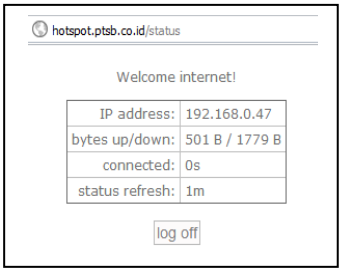
Berikut adalah *testing* dari klien yang terkoneksi ke SSID HOTSPOT-PTSB, SSID ini diperuntukan untuk umum baik karyawan maupun tamu. Sama halnya seperti sekenario diatas pertama klien akan menemukan dua buah SSID dari perangkatnya kemudian mengkoneksikan sesuai dengan hak aksesnya.

Gambar 4.6 Testing koneksi SSID HOTSPOT-PTSB



Gambar 4.7 IP *Address user* karyawan yang terkoneksi ke HOTSPOT-PTSB

Gambar 4.8 Halaman login untuk *user* STAFF-ONLY

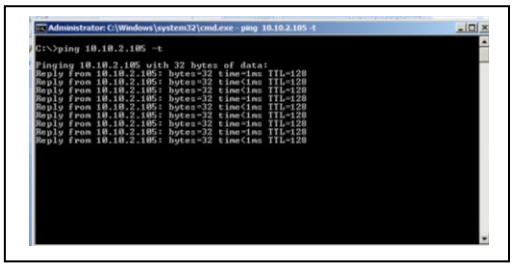


Gambar 4.9 Informasi *user* tamu setelah melakukan login

3.3 Testing Akses user staff ke server intranet dan internet

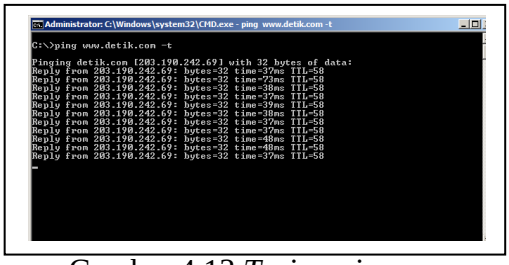
Dari konfigurasi yang telah peneliti lakukan bahwa hak akses untuk user karyawan setelah melakukan koneksi ke SSID STAFF-ONLY user dapat mengakses server intranet dan internet. Berikut adalah hasil pengujian koneksi user SSID STAFF-ONLY:

Gambar 4.10 *User* karywan mengakses *server intranet*



Gambar 4.11 *Teting ping user* kryawan ke *server* intranet

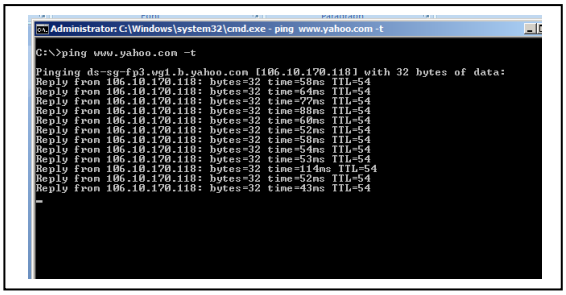
Gambar 4.12 *User* karywan mengakses *server* internet



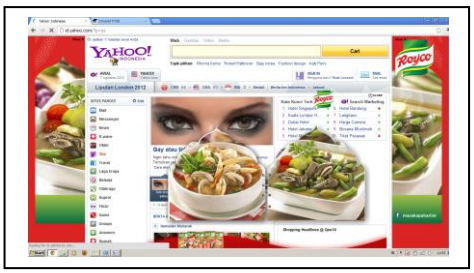
Gambar 4.13 *Tesing ping user* karyawan ke www.detik.com

3.4 *Testing* Akses *user* tamu hanya ke internet

Dari konfigurasi yang telah peneliti lakukan bahwa pembatasan hak akses untuk *user* tamu tidak diperbolehkan untuk mengakses *server* lokal namun hanya mendapat akses internet saja. Berikut adalah hasil *testing* klien tamu dengan *login username* internet dan *password* semenbaturaja:

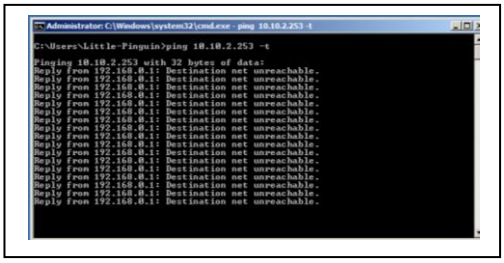


Gambar 4.14 *Testing user* tamu mengakses internet

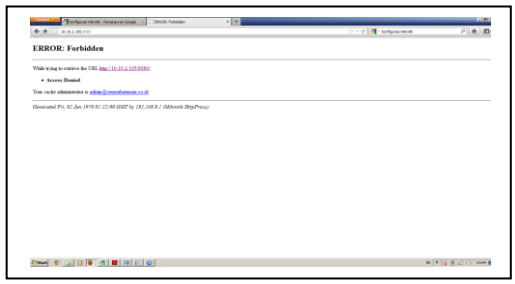


Gambar 4.15 *Testing user* tamu mengakses www.yahoo.com

Gambar diatas adalah *user* tamu yang mengakses internet, namun apabila *user* tamu mencoba mengakses *server* lokal , sesuai dengan *firewall* yang sudah peneliti konfigurasi pada bab sebelumnya maka akan diblokir. Berikut adalah hasil *testing user* tamu yang mencoba mengakses *server* lokal.



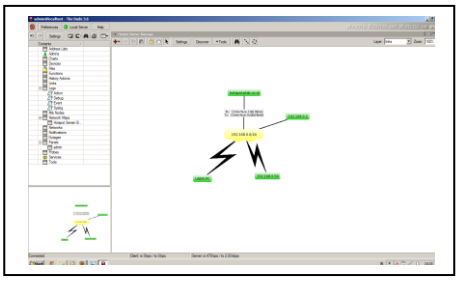
Gambar 4.16 *Testing ping user* tamu ke *server* lokal



Gambar 4.17 *Testing user* tamu mengakses *server* lokal

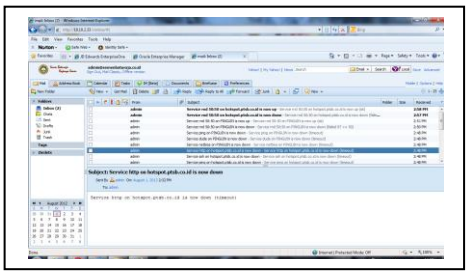
3.5 Hasil *Monitoring The Dude*

Setelah peneliti melakukan konfigurasi terhadap *tool monitoring the dude* menghasilkan sebuah tampilan *grafis* yang menunjukkan keadaan jarngan secara *realtime*. Berikut ini merupakan hasil *monitoring* terhadap dua klien yang terhubung ke jaringan dan *routerboard* mikrotik dengan informasi yang diberikan oleh fitur *SNMP* yaitu informasi *TX/RX* yang sedang berjalan dan *wireless router*.

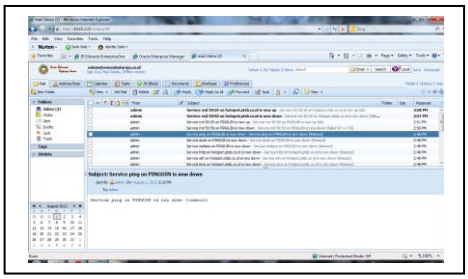


Gambar 4.18 Hasil monitoring the dude

Seperti yang telah peneliti uraikan pada bab sebelumnya bahwa *the dude* akan memberi sebuah *notifikasi* terhadap keadaan jaringan yang di*monitor*. Berikut adalah hasil *notifikasi* melalui *email*:



Gambar 4.19 *Notifikasi email, service on http* hotspot.ptsb.co.id *down*



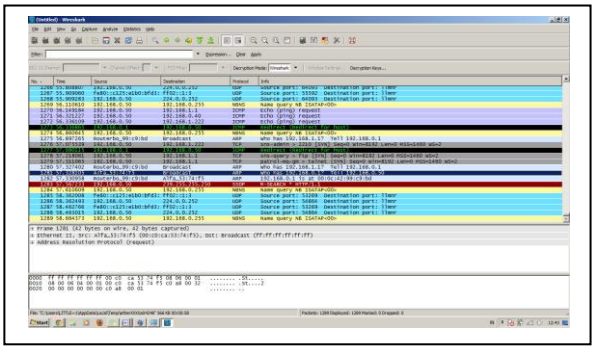
Gambar 4.20 *Notifikasi email, service ping on* PINGUIN *down*

Pada gambar gambar 4.11 *the dude* memberi informasi bahwa *service http* pada hotspot.ptsb.co.id sedang *down*, artinya klien tidak dapat melakukan *login* untuk menggunakan layanan *hotspot*. Dengan pemberitahuan ini maka *administrator* dapat langsung melakukan perbaikan terhadap masalah yang dihadapi. Kemudian pada gambar 4.12 *the dude* memberitahukan bahwa *service ping* ke *host* PINGUIN (nama komputer klien) *down*, ini artinya klien telah melakukan *log off* dari jaringan *hotspot*.

3.6 Pembahasan

Keamanan yang telah peneliti rancang menggunakan autentikasi captive portal yang terintegrasi dengan *radius server*, maka pada tahap ini peneliti melakukan sebuah uji coba untuk menguji sejauh mana tingkat keamanan fitur *hotspot* pada mikrotik. Sekenario pengujian ini, peneliti bertindak sebagai *user* yang tidak mempunyai *username* dan *password* kemudian mencoba mendapatkan *username* dan *password* klien yang sah. *Tools* yang digunakan yaitu *wireshark* yang dijalankan di sistem operasi windows 7. Berikut ini adalah tahapan dalam melakukan pengujian ini.

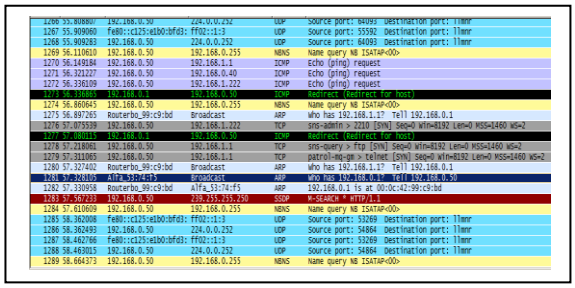
Pertama peneliti melakukan koneksi ke *SSID STAFF-ONLY*, setelah terkoneksi dilanjutkan dengan membuka aplikasi *wireshark* dan memulai untuk melakukan serangan *sniffing*. Berikut adalah hasil *sniffing* menggunakan aplikasi *wireshark:*



Gambar 4.21 Hasil paket-paket yang berhasil ditangkap *wireshark*

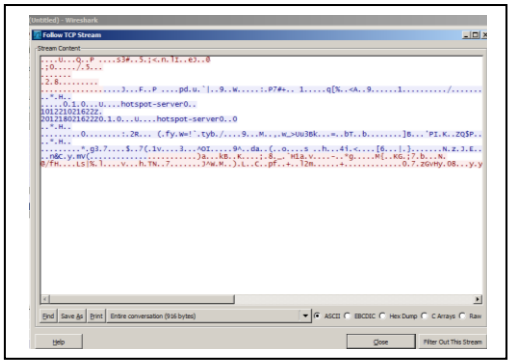
Gambar 4.21 adalah hasil dari serangan *sniffing* yang berhasil di tangkap oleh *wireshark*. peneliti akan mencoba menganalisis informasi apa saja yang di dapat selama *wireshark* melakukan *scanning*. Perlu di ketahui bahwa pada saat *wireshark* berjalan peneliti mengakses portal *login hotspot* kemudian memasukan akun karyawan dan *logoff*, setelah *log off* penelti mengulang memasukan kembali akun karyawan dan mengakses aplikasi yang disediakan di *server* lokal. Hal ini peneliti lakukan untuk melihat

informasi apa yang terekam pada aplikasi *wireshark*.



Gambar 4.22 Analisis paket data yang berhasil ditangkap

Jika diamanti pada hasil *scanning wireshark*, terdapat informasi mengenai *ip arp* yang di *broadcast*, seperti pada kolom yang peneliti lingkari, laporan memberi tahu bahwa *device* Alfa_53:74:f5 mencoba melakukan koneksi ke *ip* 192.168.0.1, terlihat pada kolom *info who has* 192.168.01? tell 192.168.0.50. Namun tujuan dari serang ini dilakukan untuk mendapatkan *username* dan *password* akun karyawan. Untuk itu peneliti memfilter hasil dari paket-paket yang ditangkap *wireshark* sehingga hanya protokol *TCP* saja yang di tampilkan. Kemudian kelik kanan pada salah satu hasil dari paket *TCP/HTTP* pilih *Folow TCP Stream* untuk melihat informasi autentikasi yang telah dilakukan. Berikut adalah hasilnya:



Gambar 4.23 Hasil paket yang di enkripsi

Dari gambar 4.23 dapat dilihat bahwa hasil dari rekaman *ip* klien yang mencoba melakukan autentikasi pada halaman *login* mikrotik sudah di enkripsi.

Kesimpulan dari pengujian ini adalah dengan memanfaatkan portal *login hotspot* masih tergolong aman, karena data yang di lewatkan sudah di enkripsi jadi *user* jahat tidak dapat melihat *username* dan *password* klien *WLAN* ketika melakukan *login.*

V. SIMPULAN

1. Dengan memanfaatkan user manager mikrotik, administrator dapat dengan mudah memanajemen user, baik menambahkan user baru atau menghapus user yang sudah tidak aktif lagi dan ini dilakukan secara terpusat;
2. Dengan adanya wireless router yang membroadcast dua SSID maka karyawan maupun tamu dapat mengkoneksikan jaringan wireless sesuai dengan hak aksesnya, dengan cara seperti ini otomatis user tamu tidak dapat melihat *share folder*

milik karyawan karena masing-masing IP *address* karyawan dan tamu berbeda *network*, selain itu juga user tamu tidak dapat mengakses server-server lokal yang terdapat di PT. Semen Baturaja. Hal ini dapat mengurangi resiko pencurian data dan meminimalisir dari serangan user jahat yang ingin mengekploitasi jaringan di PT. Semen Baturaja;

3. Dengan memanfaatkan the dude sebagai server monitoring, administrator jaringan dapat melihat kondisi jaringannya secara *realtime*, bahkan jika administrator sedang keluar kantor masih dapat mengetahui keadaan jaringaannya menggunakan notification SMS atau email.

VI. DAFTAR PUSTAKA

Geier, E. (2009), *Better Wi-Fi Network Security*. Diakses 2 Mei 2012, dari http://www.datamation.com/features/article.php/3852096/Better-Wi-Fi-Network-Security-Advanced-Techniques.htm

Geier, E. (2011), *The 6 Biggest Wi-Fi Security Mistakes*. Diakses 2 Mei 2012, dari http://www.wi-fiplanet.com/tutorials/the-6-biggest-wi-fi-security-mistakes.html

Hantoro, D.G. (2009), *WiFi (Wireless LAN) Jaringan Komputer Tanpa Kabel*. Bandung:Informatika

Herlambang, L.M & Catur, A. (2008), *Panduan Lengkap Menguasai Router Masa Depan Menggunakan Mikrotik RouterOS.* Yogyakarta:Andi.

Hidaya, S.M. (2009). *Wireless Infrastucture and Centralized Networok Management.* Jakarta :PT. Auto Jaya Idtech & PT. Solusi Preferal

Sunggiardi, M ., *Wawancara dengan CTO Mikrotik Arnis Riekstins*. Diakses 5 Mei 2012, dari http://www.mikrotik.co.id/artikel_lihat.php?id=6

Pangaribuan, J. (2011), *Wireless LAN is real, Wired LAN is History*. Jakarta:PT. Auto Jaya Idtech & PT. Solusi Preferal

Purbo, W.O & Tanuhandaru, P & Noertam, N & Djajadikara, R.M. (2007), *Jaringan Wireless di Dunia Berkembang.* Yogyakarta:Andi

Widiyasono, N. *Implementasi Mikrotik The Dude Network Monitoring Sebagai Alat Bantu Pengawasan Sistem Dan Network Infrastruktur Pada Perusahaan Penyelenggara Jasa Internet (ISP – pesat.net.id PT.Pasifik Satelit Nusantara)*. Fakultas Teknik Universitas Siliwangi Tasikmalaya