UJICOBA PENETRASI JARINGAN PADA JARINGAN LAYANAN WIFI DI KEMETERIAN AGAMA KANTOR WILAYAH SUMATERA SELATAN

Wayan suarte[1], Alex Wijaya[2], Suyanto[3]
[1)]Mahasiswa Teknik Informatika Universitas Bina Darma
[2)]Dosen Ilmu Komputer [3)]Dosen Ilmu Komputer. Jl Jend A.Yani No.12 Plaju, Palembang 30264

Email: wayan_suarte@yahoo.com[1)] alexwijaya@ binadarma.ac.id[2)], suyanto@binadarma.ac.id [3)]

Abstrak, Dalam dunia jaringan Wi-Fi , Wi-Fi diperlukan untuk melakukan koneksi internet. Memiliki kemampuan jaringan internet tanpa kabel. Jadi, pengguna di jaringan merasa akses yang lebih cepat . Dari sisi pengguna, itu adalah tindakan yang mungkin pengguna melakukan percobaan menyusup atau merusak sistem dengan memanfaatkan lubang keamanan. Administrator jaringan, dalam hal ini, telah menyadari pihak yang berniat untuk menghancurkan sistem jaringan Wi-fi. Skripsi ini membahas keamanan jaringan Wi-fi. Pemindaian kerentanan dilakukan untuk menentukan kerentanan sistem. Kemudian lakukan hasil verifikasi analisis kerentanan dengan cara uji penetrasi. Kesimpulannya, rekomendasi akan menindaklanjuti hasil yang disajikan bukti .

Kata Kunci : *Pentration Test, Security Network* ,Wi-Fi

Pendahuluan

1. Latar Belakang

Jaringan internet yang digunakan oleh Kementerian Agama Kantor Wilayah Provinsi Sumatera Selatan di bagian Bimbingan Masyarakat (Bimas) yaitu terbagi menjadi 2 *switch* jaringan yaitu, *hotspot* Budha dan *hotspot* Kristen. Sementara kecepatan akses yang diberikan oleh pihak Kementerian Agama Kantor Wilayah Provinsi Sumatra Selatan adalah mencapai 100 Mbps/*second* dan jumlah pengguna yang biasa terhubung koneksi ke internet ±25 *user* per Wi-Fi/ hari. Kantor Wilayah Kementerian Agama Sumatera Selatan menerapkan sistem keamanan WEP, WAP, dan WPA2, sampai saat ini belum pernah di ujicoba apakah itu sudah aman atau belum dari adanya attacker. Pengujian keamanan secara periodik terhadap sistem sangat penting. Tanpa pengujian secara periodik, tidak ada jaminan terhadap tindakan protektif yang dilakukan atau *pacth* pengamanan yang diterapkan oleh administrator berfungsi sebagaimana yang mana mestinya.
Salah satu kegiatan teknologi yang dilakukan oleh karyawan yang bekerja di Kementerian Agama Sumatera Selatan adalah mengirim data ke pusat untuk *update* data terbaru perkembangan masyarakat di Sumatera Selatan. Sebagian besar karyawan juga memanfaatkan fasilitas Wi-Fi yang ada Kementerian Agama Kantor Wilayah Provinsi Sumatera Selatan untuk mengakses media sosial atau *update* berita di *website* Kementerian Agama Kantor Wilayah Provinsi Sumatera Selatan.
Dibalik pesatnya perkembangan dunia internet saat ini banyak *user* yang menyalahgunakan informasi, misalnya merubah password wifi dengan cara melakukan sniffing. Tentunya semua ini tergantung pada sumber daya manusia dalam menggunakan komputer dan internet yang mereka pakai, sehingga perlu untuk berhati-hati pada saat menggunakannya. Agar dapat menghasilkan data yang akurat dan

dapat melindungi informasi dari segala serangan – serangan jahat seperti *linked* yang berisi virus, mereka harus melakukan *instalisasi* beberapa aplikasi ke dalam komputer.
Dalam faktor keamanan ini biasanya perusahaan menempatkan administrator untuk menjaga, namun fungsi administrator tentunya memilki keterbatasan waktu yakni, hanya dapat melakukan fungsi monitoring pada saat jam kerja saja. Sedangkan suatu serangan terhadap sistem keamanan bisa terjadi kapan saja.adapun batasan masalah penelitian ini adalah

a. melakukan ujicoba penetrasi pada bagian bimas budha dan bimas Kristen.

2. Metode dan Perancangan

2.1 Metode Penelitian

Dalam penelitian ini penulis menggunakan metode *Action Research* atau penelitian tindakan merupakan salah satu bentuk rancangan penelitian yang mengutamakan tindakan secara langsung ke lapangan guna untuk mengetahui masalah apa yang sedang dihadapi dan upaya apa yang akan dilakukan dalam pemecahan masalah tersebut.
Tahapan yang dilakukan dalam *Action research* yaitu :

1. Melakukan diagnosa (*diagnosing*), dalam tahapan ini yang dilakukan adalah mengidentifikasi masalah keamanan jaringan terhadap ancaman data *flooding* pada instansi tersebut.
2. Membuat rancangan tindakan (*action planning),* dalam tahapan ini penulis mencoba memahami pokok permasalahan dan kemudian menyusun rencana untuk melakukan penelitian.
3. Melakukan tindakan (*action taking),* dalam tahapan ini penulis melakukan penelitian langsung pada pokok permasalahan yang sudah di diagnosa.
4. Pembelajaran (*learning*), pembelajaran atau *learning* ini adalah tahapan terakhir yang dilakukan penulis. Dalam tahapan ini penulis menganalisa data yang telah diperoleh dari penelitian tersebut.

Metode Pengujian

Didalam penelitian ini yaitu menggunakan metode penetrasi testing. Metode penetrasi adalah suatu metode yang dilakukan guna mengevaluasi keamanan dari sebuah sistem komputer atau jaringan. Tujuan pengujian penetrasi ini adalah untuk menemukan semua titik kerentanan didalam sistem jaringan komputer dengan cara melakukan simulasi serangan dari luar maupun internal sistem jaringan. (Thomas, 2005: 419)
Berikut tahapan-tahapan melakukan penetrasi testing :

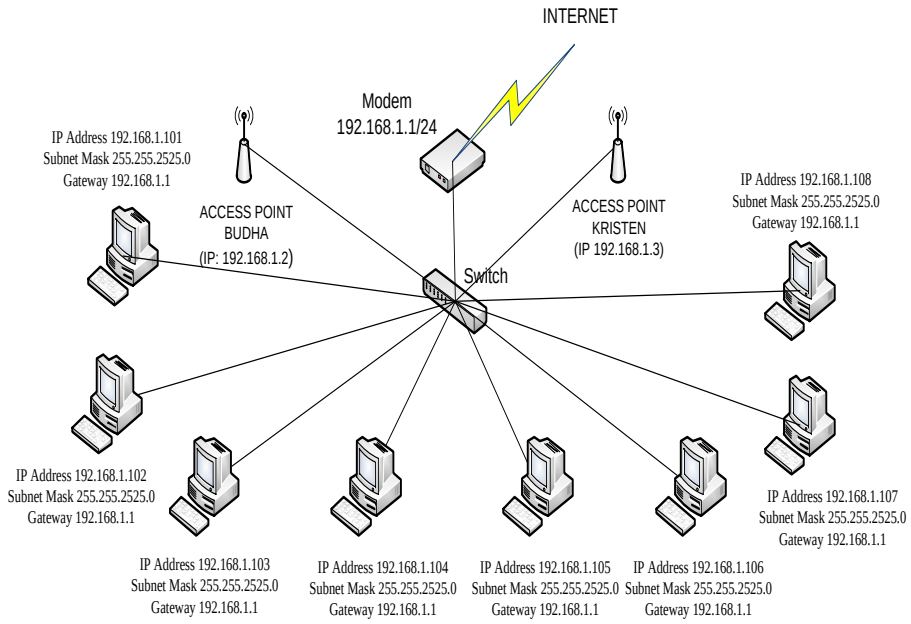
1. *Pre-engagement Interactions*
   Tahap dimana seorang *pentester* menjelaskan kegiatan *pentest* yang akan dilakukan kepada *client* (perusahaan). Disini seorang *pentester* harus bisa menjelaskan kegiatan-kegiatan yang akan dilakukan dan tujuan akhir yang akan dicapai.
2. *Intelligence Gathering*
   Tahap dimana seorang *pentester* berusaha mengumpulkan sebanyak mungkin informasi mengenai perusahaan target yang bisa didapatkan dengan berbagai metode dan berbagai media. Hal yang perlu dijadikan dasar dalam pengumpulan informasi adalah karakteristik sistem jaringan, cara kerja sistem jaringan, dan metode serangan yang bisa digunakan.
3. *Threat Modeling*
   Tahap dimana seorang *pentester* mencari celah keamanan (*vulnerabilities*) berdasarkan informasi yang berhasil dikumpulkan pada tahap sebelumnya.
4. *Vulnerability Analysis*
   Tahap dimana seorang *pentester* mengkombinasikan informasi mengenai celah keamanan yang ada dengan metode serangan yang bisa dilakukan untuk melakukan serangan yang paling efektif.

5. *Reporting*

Reporting adalah bagian paling penting dalam kegiatan *pentest*. Seorang *pentester* menggunakan *report* (laporan) untuk menjelaskan pada perusahaan mengenai *pentesting* yang dilakukan seperti apa yang dilakukan,

2.2 Perancangan

Kepala bagian IT Kementerian Agama Kantor Wilayah Provinsi Sumatera Selatan telah menyetujui rencana proyek *penetration testing* layanan jaringan Wifi di kantor Kementerian Agama Kantor Wilayah Provinsi Sumatera Selatan. Tujuan akhir dalam kegitan adalah untuk mencari kelemahan keamanan jaringan wifi, agar bisa dievaluasi kemananya. Berdasarkan hasil wawancara, penulis medapatkan informasi yaitu arsitektur jaringan di Kementerian Agama Kantor Wilayah Provinsi Sumatera Selatan menggunakan topologi *star* dan topologi *infrastruktur*. Pada topologi *star*, masing-masing komputer atau *client* terhubung secara langsung ke jaringan melalui *switch hub.* Keunggulan dari topologi tipe *star* ini adalah banyak sekali diantaranya memudahkan *admin* dalam mengelola jaringan, memudahkan dalam penambahan komputer atau *client* , kemudahan mendeteksi kerusakan dan kesalahan pada jaringan. Sedang topologi jaringan *wireless* menggunakan topologi infrastruktur dimana menggunakan *access point* sebagai pusat jaringan *wireless* atau *hotspot* yang terhubung langsung pada perangkat *switch hub.* Adapun gambar topologi jaringan yang sedang berjalan yang seperti pada Gambar 3.2



Gambar 3.2 Rancangan Topologi Jaringan komputer

3 Hasil dan Pembahasan

3.1 Hasil

Hasil dari penetrasi yang dilakukan di dua hotspot yaitu hotspot budha dan hotspot Kristen yang dijelaskan tabel 4.1

No	Parameter	*Security layanan Wifi (Tampil / Tidak Tampil)*	
		Bimas Budha	***Bimas Kristen***
1	***User Login AP***	**Tampil**	**Tampil**
2	***Password AP***	**Tampil**	**Tampil**
3	***IP Address AP***	**Tampil**	**Tampil**
4	***Mac Address AP***	**Tampil**	**Tampil**
5	***Password Wifi***	**Tidak Tampil**	**Tidak Tampil**

Tabel 4 .1 Hasil penetrasi layanan Wifi *WPA2*

3.2 Pembahasan

Hasil dari pengujian keamanan layanan Wifi di Kementerian Agama Kantor Wilayah Provinsi Sumatera Selatan yang menggunakan sistem keamanan jaringan *wireless* dengan menggunakan *security internal* perangkat *access point* yaitu *Wireless Protected Access* (*WPA2) Personal* diperoleh hasil dimana *tools ettercap* dapat mengetahui *user* dan *password login* perangkat *access point* yang diakses melalui *web browser* dan informasi lainnya seperti *ip address* dan *mac address client wireless* dan perangkat *access point* sedangkan 2 aplikasi atau *tools sniffing wifi* yaitu *airodump-ng* dan *Elcomsoft Wireless Security* dimana hasil yang diperoleh tidak dapat menampilkan *password* atau *security* pada saat pengujian yang dilakukan antara 3-4 jam , hal ini menunjukan bahwa sistem enkripsi yang digunakan pada metode WPA2 sangat baik hal ini dikarenakan metode tersebut menggunakan teknologi algoritama enkripsi *Advanced Encryption Standard* (AES) dan dalam hal sistem otentikasi, *WPA2 Personal* menggunakan tombol *Preshared Security* (PSK) atau hanya menggunakan sistem *password. Security* atau *password* yang digunakan minimal 8 digit dengan menggunakan character ASCII.

Akan tetapi penyusup atau *hacker* dapat mengamati *user login* beserta *password* atau *security* pada perangkat *access point* yang digunakan *Client Wireless* saat melakukan *remote* atau konfigurasi *access point* hal ini membuktikan bahwa sistem autentikasi yang digunakan pada perangkat access point tersebut kurang baik dikarenakan sangat rentan terhadap penyusup, jika penyusup bisa mendapatkan *user login* dan *password access point* maka penyusup dapat melakukan konfigurasi secara langsung pada perangkat *access point* tersebut

4 Kesimpulan

1. Hasil dari pengujian keamanan layanan Wifi di Kementerian Agama Kantor Wilayah Provinsi Sumatera Selatan yang menggunakan sistem keamanan jaringan *wireless* dengan menggunakan *security internal* perangkat *access point* yaitu *Wireless Protected Access* (*WPA2) Personal* diperoleh hasil dimana *tools ettercap* dapat mengetahui *user* dan *password login* perangkat *access point* yang diakses melalui web browser dan informasi lainnya seperti *ip address* dan *mac address client wireless* dan perangkat *access point*
2. Pengujian dengan menggunakan tools *sniffing wifi* yaitu *airodump-ng* dan *Elcomsoft Wireless Security* dimana hasil yang diperoleh tidak dapat menampilkan *password* atau *security* pada saat pengujian yang dilakukan dari pukul 11.00 – 16.00 pm , hal ini menunjukan bahwa sistem enkripsi yang digunakan pada metode WPA2 sangat baik hal ini dikarenakan metode tersebut menggunakan teknologi algoritama enkripsi *Advanced Encryption Standard* (AES) dalam hal sistem otentikasi.

Referensi

Agusaputra, Ashadi Soki. 2010. *Implementasi Sitem Pencegahan Data Flooding Pada jaringan Komputer.* http://eprints.binadarma.ac.id/24/1/08142223_journal.pdf. Diakses pada 24 November 2015

Madcoms. 2010 . *Sistem Jaringan Komputer untuk Pemula.* Andi, Yogyakarta.

Priyambod. 2005. *Definisi dan pengertian Wi-fi*. http://fatih-io.biz/definisi-pengertian-wifi-menurut-para-ahli.html. Diakses pada 24 November 2015

Ri2m. 2010. *Jaringan and keamanan*. http://ftp.labkom.bI.ac.id. Diakses pada 24 November 2015

S.Nurwenda. 2012. *Analisis Kelakuan Denial-of-Service attack (DoS attack) pada Jaringan Komputer dengan Pendekatan pada Level Sekuritas. http://elib.unikom.ac.id/files/disk1/16/jbptunikompp-gdl-s1-2004-syoninurwe-766-jurnal+D-S.pdf. Diakses* pada tanggal 26 januari 2016

Supriyanto, Aji. 2006. *Analisis Kelemahan Kemanan pada Jaringan Wireless*. (http://www.unisbank.ac.id/ojs/index.php/fti1/article/view/33/28)

Thomas, T. 2005. *Network Security First Step*. Penerbit ANDI, Yogyakarta.

Utomo. 2011. *Implementasi Sistem Pencegahan Data Flooding Pada Jaringan Komputer*. http://eprints.binadarma.ac.id/24/1/08142223_journal.pdf Diakses pada 23 November 2015

Wikipedia, 2011. *Mengenal Wireless Acces Point*. Diakses pada 25 januari 2016

Yusra, Surya. 2010. Penetrasi Jaringan *Wireless* Radius. Diakses pada 23 januari 2016