BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Dinas Kesehatan Provinsi Jawa Barat merupakan salah satu dinas yang berada di Provinsi Jawa Barat. Dinas Kesehatan Provinsi Jawa Barat saat ini memiliki 3 lantai, lantai 1 memiliki 4 ruangan, lantai 2 memiliki 8 ruangan, lantai 3 memiliki 4 ruangan. Masing-masing lantai memiliki 2 akses point sebagai jaringan *wireless* yang mencangkup seluruh ruangan pada setiap lantai. Penerapan jaringan kabel LAN belum menyeluruh pada setiap lantai mengakibatkan 60 persen komputer Dinas Kesehatan Provinsi Jawa Barat menggunakan jaringan *wireless.*

Jaringan *wireless* yang digunakan untuk memenuhi kebutuhan jaringan teridiri dari 6 perangkat wireless untuk mencakup seluruh lantai di Dinas Kesehatan Provinsi Jawa Barat. Perangkat *wireless* yang ada menggunakan keamanan yang berbeda diantaranya 4 perangakat terbuka (*open)* dan dua perangkat dengan jenis keamanan WPA2-PSK. Penggunaan *wireless* yang dominan ini memiliki ancaman penyerangan jaringan yang lebih rentan daripada penggunan jaringan LAN. Hal ini memaksa Divisi TIK untuk melakukan penganalisaan lebih terhadap jaringan wireless yang ada di Dinas Kesehatan Provinsi Jawa Barat.

Jaringan *wifi* memiliki lebih banyak kelemahan dibanding dengan jaringan kabel [15]. seperti pada wawancara dengan Bapak Agung Aditia selaku Divisi Teknologi Informasi Komunikasi. Bahwa Dinas Kesehatan Jawa Barat sering terjadi gangguan seperti *flooding, illegal access*. pada tahun yang sama pada bulan Desember, Januari, dan Februari tahun 2017 telah terjadi serangan flooding terhadap perangkat *wifi* yang berimbas pada 12 PC dan mengakibatkan keduabelas PC tersebut tidak dapat mengakses internet, serta Dinas Kesehatan Provinsi Jawa barat memiliki empat *wifi* yang terbuka dan siapapun dapat mengakses perangkat tersebut. Maka dari itu dinas kesehatan membutuhkan analisis dan audit sistem keamanan jaringan agar dapat memastikan bahwa Dinas Kesehatan Provinsi Jawa Barat baik dalam segi sistem keamanan jaringannya terutama jaringan *wireless*.

Divisi Teknologi Informasi Komunikasi dalam melakukan analisis dan audit membutuhkan sebuah tools yang akan menjadi sebuah standar dalam menganalisa sistem keamanan jariangan Dinas Kesehatan Provinsi Jawa barat. Maka dari itu dibutuhkan sebuah tools standar dalam analisis dengan menggunakan *Penetration Testing Execution Standard* yang merupakan salah satu *tools* yang dikembangkan oleh *pentest organitation* untuk menjadi standar dalam menganalisis atau mengaudit sistem keamanan jaringan pada sebuah perusahaan dalam kasus ini yaitu menganalsis dan mengaudit sistem keamanan jaringan *wireless* Dinas Kesehatan Provinsi Jawa barat.

1.2 Identifikasi Masalah

Berdasarkan latar belakang tersebut, maka dapat diidentifikasi masalah-masalah yang ada adalah sebagai berikut.

1. Bagaimana Divisi Teknologi Informasi mengetahui seberapa baik sistem keamanan jaringan wireless yang dimiliki Dinas Kesehatan Provinsi Jawa Barat.
2. Bagaimana *Penetration Testing Execution Standard* di terapkan dalam menganalisa sistem keamanan jaringan *wireless* Dinas kesehatan Provinsi Jawa Barat.

1.3 Maksud dan Tujuan

Maksud dari penelitian ini adalah menganalisa sistem keamanan jaringan Dinas Kesehatan Provinsi Jawa Barat dengan menggunakan metode *penetration testing execution standard*, sehingga Divisi Teknologi Informasi Komunikasi mengetahui baik atau tidaknya sistem keamanan jaringan *wireless* di Dinas Kesehatan Provinsi Jawa Barat. Sedangkan tujuan dari penelitian ini adalah sebagai berikut.

1. Menganalisa dan mengaudit sistem keamanan jaringan *wireless* yang telah diterapkan oleh Dinas Kesehatan Provinsi Jawa Barat.
2. Menerapkan *Penetration Testing Execution Standard* dalam menganalisa sistem keamanan jariangan *wireless* Dinas Keseahatan Provinsi Jawa Barat.

1.4 Batasan Masalah

Pembatasan suatu masalah di gunakan untuk menghindari adanya penyimpangan maupun pelebaran pokok masalah supaya penelitian tersebut lebih terarah dan memudahkan dalam pembahasan sehingga tujuan penelitian akan tercapai. Dalam penelitian ini penulis membatasi masalah yang akan di analisa yaitu:

1. Pengujian dapat dilakukan diatas pukul 5 sore atau setelah jam kantor pada hari kerja.
2. Sistem oprasi yang digunakan merupakan sistem operasi *open source*.
3. Penelitian hanya mencangkup perangkat *wifi.*
4. Pengujian hanya dilakukan pada perangkat *wifi* Dinas Kesehatan dan AP-KESDIS dengan type keamanan Dinas Kesehatan terbuka (OPN) dan AP-KESDIS (WPA2_PSK).
5. Divisi Teknologi Informasi Komunikasi tidak memiliki berita acara mengenai setiap kasus serangan yang terjadi pada komputer *user* Dinas Kesehatan Provinsi Jawa barat.
6. Alamat ip tidak dipublikasikan demi keamanan Dinas Kesehatan provinsi Jawa Barat.

1.5 Metodologi Penelitian

Metodologi penelitian merupakan suatu proses yang digunakan untuk memecahkan suatu masalah yang logis, di mana memerlukan data-data untuk mendukung terlaksananya suatu penelitian. Metodologi penelitian yang digunakan adalah metode analisis deskriptif. Metode analisis deskriptif merupakan metode yang menggambarkan fakta-fakta dan informasi dalam situasi atau kejadian sekarang secara sistematis, faktual dan akurat. Metode penelitian ini memiliki dua tahapan, yaitu tahap pengumpulan data dan analisis keamanan jaringan.

1.6 Metode Pengumpulan Data

Metode pengumpulan yang digunakan dalam penelitian ini sebagai berikut

1. Studi Literatur.

   Pengumpulan data dengan cara mengupulkan literatur, jurnal, *paper,* dan bacaan-bacaan yang kaitanya dengan judul penelitian.

2. *Observasi*

   Teknik pengumpulan data dengan mengadakan penelitian dan peninjuan secara langsung terhadap permasalahan yang di ambil.

3. *Interview*

   Teknik pengumpulan data dengan mengadakan tanya jawab secara langsung yang ada kaitanya dengan topik yang diambil.

1.7 Metode Penetrasi Jaringan

Metode penetrasi yang digunakan pada penelitian ini adalah PTES (*Penetration Testing Execution Standard*). PTES merupakan metode yang



Gambar 1. 1 Metode *Penetration Testing Execution Standard* (PTES)

mencangkup segala uji penetrasi. Metode ini memiliki tujuh tahap pengujian yaitu. *Pre-engagement, Interlligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post-Exploitation, Reporting.* Gambar metode *penetration testing execution standart* dapat dilihat pada gambar 1.1.

Berikut adalah tahapan-tahapan yang dilakukan dalam penelitian ini.

a. Pre-Engagement

Pre-engagement adalah tahap dimana seorang *pentester* menjelaskan kegiatan *pentest* yang akan dilakukan kepada *client (*perusahaan*).* Hal yang

perlu dijelaskan dalam *pre-engagement* ini adalah *Questionnaires*, rentan ip, Aturan pengujian *Danial Of Service*.

b. Intelligence Gathering

Interlligence Gathering adalah 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 *Covert Gathering, Footprinting,* Identifikasi mekanisme perlindungan.

c. Theart Modeling

Threat Modeling merupakan pendefinisian dari pendekatan permodelan ancaman. *Threat Modeling* diperlukan untuk pelaksanaan pengujian penetrasi yang benar. Pendekatan permodelan yang di maksud adalah pengamatan terhadap target yang bertujuan untuk mengetahui proses bisnis target agar lebih mudah dalam menentukan serangan. Hal yang perlu dijadikan dasar *threat modeling* adalah analisis tujuan bisnis.

d. Vulnerability Analysis

Vulnerability Analisis adalah dimana tahap untuk mencari celah keamanan berdasarkan informasi yang telah didapatkan sebelumnya. *Vulnerability analisis* bertujuan untuk menemukan kekurangan didalam sistem jaringan yang dapat dimanfaatkan oleh penyerang. Hal yang akan menjadi dasar pengujian *vulnerability analisis* adalah pengujian aktif dan pasif.

e. Exploitation

Expolition adalah tahap dimana seorangan *pentester* melakukan serangan pada target. Walaupun demikian tahap ini kebanyakan dilakukan dengan metode *brute force* tanpa memiliki unsut presisi. Seseorang *pentester* hanya akan melakukan *exploitation* ketika dia sudah mengetahui secara pasti apakah serangan yang dilakukan berhasil atau tidak, namun tentu saja ada kemungkinan tidak terduga dalam sistem keamanan target. Walaupun begitu, sebelum melakukan serangan, *pentester* harus tahu kalau target mempunyai celah keamanan yang bisa di gunakan. Melakukan serangan secara membabi-buta dan

berharap sukses bukanlah metode yang produktif. Seorangan *pentester* selalu menyempurnakan analisisnya terlebih dahulu sebelum melakukan serangan yang efektif

f. Post-Exploitation

Post Exploitation adalah tahap dimana seorangan *pentester* masuk kedalam sistem jaringan target dan kemudian melakukan analisis infrastuktur yang ada. Pada tahap ini seorang *pentester* mempelajari bagian-bagian di dalam sistem dan menentukan bagian yang paling *critical* bagi target (perusahaan). Disini seorang *pentester* harus bisa menghubungkan semua bagianbagian sistem yang ada untuk menjelaskan dampak serangan atau kerugian yang paling besar yang bisa terjasi pada target (perusahaan).

g. 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 di lakuakan, bagaimana cara melakukannya, resiko yang bisa terjadi dan yang paling utama adalah cara untuk memperbaiki sistemnya.

1.6 Sistematika Penulisan

Dalam penulisan tugas akhir, penulis mambaginya menjadi lima bab pembahasan. rincian pembahasan setiap bab yaitu sebagai berikut :

BAB I PENDAHULUAN

Menjelaskan latar belakang penelitian, ruang lingkup penelitian, tujuan dan manfaat penelitian, metologi yang di gunakan dan sistematika penulisan laporan

BAB II LANDASAN TEORI

Pada bab ini berisi tentang teori – teori yang berkaitan dengan pokok bahasan penulisan serta teori-teori pendukungnya dari hasil studi literatur yang akan menjadi landasan dalam proses penelitian .

BAB III ANALISIS DAN PENGUJIAN

Menjelaskan proses analisis dan pengujian sistem . pertama-tama di lakuakan analisis pre-engagement, setelah itu pengambilan informasi dengan *Intelligence Gathering,* serta menganalisa dengan *Vulnerability Analisis.*

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Menjaelaskan proses penetrasi dan pelaporan . pertamama-tama dilakukan *exploitation,* setelah *exploitation* maka dilakukan *post-exploitation,* serta untuk bagian akhir dalam implementasi yaitu pelaporan pada setia kegiatan yang telah dilakukan.

BAB V KESIMPULAN DAN SARAN

Pada bab ini, merupakan penutup yang berisi kesipulan dan hasil kegiatan penelitian dan pembuatan skripsi ini, serta saran untuk pengembangan lebih lanjut.