BAB I

PENDAHULUAN

1.1. Latar Belakang

Pada saat ini perangkat mobile ada di semua tempat di lingkungan sekitar kita dan sekarang mempengaruhi segala sesuatu yang kita lakukan dalam kehidupan sehari-hari. Jika kita melompat mundur 10 atau 12 tahun silam, kita akan di tempatkan di era di mana mayoritas komputer atau perangkat teknologi masih di transfer ke jaringan dengan menggunakan kabel Ethernet yang lama, dan telpon seluler adalah perangkat yang praktis untuk menelpon dan saling bertukar pesan.

Namun perkembangan dalam era globalisasi ini dimana perangkat komputer dan seluler pada saat ini sangat berkembang hampir semua perangkat mobile sekarang telah mendukung jaringan nirkabel untuk menyesuaikan kemudahan dalam bertukar data tanpa menggunakan bantuan kabel atau sinyal seluler dengan kecepatan yang mumpuni serta mempunyai mobilitas yang tinggi yang akan mempermudah dalam mengurus berbagai kegiatan sehari-hari. Keamanan data pada komputer dan perangkat *mobile* yang terhubung dalam sebuah jaringan sangat penting untuk dijaga validitas dan integritasnya serta dijamin ketersediaannya bagi pengguna. Sistem harus dapat dilindung dari pengguna yang tidak berhak mengaksesnya (*unauthorized user*).

Jenis serangan yang penulis uji yaitu menggunakan *Deauthentication Attack* dan *Evil Twin Attack* menggunakan Fluxion. Dikarenakan evil twin attack cukup banyak melakukan kerusakan dibeberapa tempat seperti Bandara, Mall, dan Hotel. Penelitian serupa dilakukan oleh Sharma et al., (2016). Pada penelitiannya membahas tentang serangan evil twin attack banyak terjadi di area umum yang memiliki banyak lalu lintas wireless[1].

Penelitian serupa dilakukan oleh Ahmad et al., (2017). Pada penelitian ini melakukan pendekatan metode live forensik dan pendekatan dari sisi user, untuk mendeteksi aktivitas ilegal yang terjadi di dalam jaringan wifi, proses investigasi *MITM Based Evil* di fokuskan pada dua proses penelitian yaitu proses analisa wifi scanning dan analisa network traffik untuk proses penemuan barang bukti digital berupa informasi traffik data dari serangan *mitm based evil twin.* [2].

Alasan penulis membuat penelitian menggunakan wifislax sebagai operasi sistem dan menggunakan fluxion untuk menggabungkan rule serangan untuk menciptakan evil twin attack yaitu untuk meningkatkan mobilitas dalam proses penyerangan terhadap lalu lintas jaringan nirkabel.

Dari latar belakang permasalahan tersebut, penulis termotifasi untuk membuat suatu penelitian dengan judul **"Analisis Dan Implementasi Bentuk Serangan Pada Jaringan Dengan Wifislax Dan Fluxion Menggunakan Metode Evil Twin Attack".**

1.2. Rumusan Masalah

Dari uraian latar belakang diatas maka dapat dirumuskan beberapa pertanyaan sebagai berikut:

a. Bagaimana Menggunakan serangan *evil twin attack* dengan menggunakan Wifislax sebagai sistem operasi?

b. Apakah Wifislax dapat berjalan dengan lancar menggunakan *bootable* usb?

c. Bagaimana dampak yang di hasilkan *evil twin attack* terhadap klien yang menggunakan jaringan nirkabel?

d. Apakah analisa menggunakan Snort sebagai *Wireless Intrusion Detection System* mampu mendeteksi jenis serangan?

e. Bagaimana skema penyerangan dan analisis yang akan dilakukan berdasarkan data yang ada?

1.3. Batasan Masalah

Penerapan analisis dan implementasi jenis serangan wireless memiliki beberapa batasan masalah, yaitu:

a. Menggunakan Wifislax sebagai sistem operasi dari serangan.

b. Menggunakan fluxion sebagai media penggabungan dari jenis serangan *evil twin attack.*

c. Serangan *evil twin attack* hanya mampu berhasil dalam jarak yang sudah ditentukan.

d. Serangan *evil twin attack* tidak bisa di cegah secara otomatis.

e. Perangkat harus terkoneksi dengan akses point untuk menghubungan satu sama lain dan harus memiliki kekuatan sinyal sesuai standar penyerangan.

f. Menjalankan semua *rule* serangan untuk menyerangan *client* yang terhubung menggunakan *wireless*.

g. Menganalisa jenis serangan menggunakan WIDS untuk menentukan jenis serangan.

1.4. Tujuan Penelitian

Penelitian ini bertujuan untuk menambah wawasan tentang tren keamanan jaringan (*cryber security*) untuk menimalisir dampak dari serangan antara lain sebagai berikut:

1. Untuk mengetahui pola cara penyerang *evil twin attack* dan apa dampak negatif yang di dapatkan setelah terkena serangan tersebut.
2. Menganalisis pola serangan yang berbahaya bagi pengguna jaringan wireless dan memberikan rasa aman dalam menjalakan aktifitas.
3. Masyarakat yang awam terhadap teknologi bisa melakukan investigasi secara mandiri dengan menggunakan Snort sebagai WIDS (*wireless intrusion detection sytem*).
4. Penelitian ini dirancang dengan mendasarkan Windows sebagai sistem operasi agar masyarakat dapat mengetahui dan menggunakan dengan mudah.

1.5. Manfaat Penelitian

Penelitian yang dilakukan memiliki manfaat bagi berbagai pihak antara lain sebagai berikut:

1. Sebagai referensi penelitian yang berkaitan dengan keamanan jaringan nirkabel.
2. Mengetahui konsep dari serangan berbasis *evil twin attack* dan *deauthentication attack.*
3. Mencegah terjadinya jenis serangan dari *evil twin attack* dan *deauthentication attack.*
4. Meningkatkan mobilitas sistem keamanan jaringan.
5. Mengetahui sistem analisis WIDS menggunakan Snort.

1.6. Metode Penelitian

Metode penelitian yang digunakan dalam penulisan skripsi **"Analisis Dan Implementasi Bentuk Serangan Pada Jaringan Dengan Wifislax Dan Fluxion Menggunakan Metode Evil Twin Attack"** ini adalah sebagai berikut:

1.6.1 Metode Pengumpulan Data

Dalam penelitian ini data-data yang digunakan didapat dari beberapa metode, antara lain:

1.6.1.1 Metode Kepustakaan

Data-data dikumpulkan dengan cara mempelajari, meneliti dan memahami berbagai literature baik dalam buku, jurnal ilmiah dan berbagai bacaan lain yang berkaitan dengan topic penelitian yang dapat dijadikan referensi.

1.6.1.2 Metode Observasi

Penulis terjun langsung ke objek yaitu meninjau langsung dan melalukan implentasi serta analisis singkat dilokasi objek penelitian yang nantinya digunakan untuk pengujian sistemnya. Dimana alasan penulis terjun langsung ke

objeknya agar penulis tahu bahwa ragam device yang memiliki karakteristik yang berbeda-beda dan meninjau langsung reaksi masyarakat yang terkena dampak serangan *evil twin attack*.

1.6.2 Metode dan Perancangan Sistem

Network Development Life Cycle (NDLC) merupakan suatu metode yang digunakan dalam mengembangkan atau merancang jaringan infrastruktur yang memungkinkan terjadinya pemantauan jaringan untuk mengetahui statistik dan kinerja jaringan. [3] Metode ini bersifat continous improvement dimana hasil dari analisis akan terus dijadikan sebagian bahan pertimbangan untuk melakukan perbaikan terus-menerus. Metode NDLC memiliki tahapan sebagai berikut:

1. Analisis Kebutuhuan

Tahapan awal dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa pengguna, dan analisa topologi jaringan yang sudah ada saat ini.

2. Design

Dari data-data yang didapatkan sebelumnya, tahap design ini akan membuat gambar desain topologi jaringan interkoneksi yang akan dibangun. Diharapkan dengan gambar ini akan memberikan gambaran seutuhnya dari kebutuhan yang ada. Desain bisa berupa desain struktur topologi, desain akses data, desain layout perkabelan, dan sebagainya yang akan memberikan gambaran jelas tentang proyek yang akan dibangun. Biasanya hasil dari design berupa:

a) Gambar-gambar topologi (server farm, firewall, datacenter, storages, lastmiles, perkabelan, titik akses dan sebagainya).

b) Gambar-gambar detail estimasi kebutuhan yang ada.

3. Simulation Prototype

Beberapa pekerja jaringan akan membuat dalam bentuk simulasi dengan bantuan tools khusus di bidang network seperti Boson, Packet Tracert, Netsim, dan sebagainya. Hal ini dimaksudkan untuk melihat kinerja awal dari jaringan yang akan dibangun dan sebagai bahan presentasi dan sharing dengan team work lainnya. Namun karena keterbatasan perangkat lunak simulasi ini, banyak para pekerja jaringan yang hanya menggunakan alat bantu tools Visio untuk membangun topologi yang akan di-design.

4. Implementation

Pada tahapan ini akan memakan waktu lebih lama dari tahapan sebelumnya. Dalam implementasi pekerja jaringan akan menerapkan semua yang telah direncanakan dan didesain sebelumnya. Implementasi merupakan tahapan yang sangat menentukan dari berhasil/gagalnya proyek yang akan dibangun dan ditahap inilah team work akan diuji dilapangan untuk menyelesaikan masalah teknis dan non teknis. Ada beberapa Masalah-masalah yang sering muncul pada tahapan ini, diantaranya:

a) Jadwal yang tidak tepat karena faktor-faktor penghambat.

b) Masalah dana/anggaran dan perubahan kebijakan.

c) Team work yang tidak solid.

d) Peralatan pendukung dari vendor makanya dibutuhkan manajemen proyek dan manajemen resiko untuk menimalkan sekecil mungkin hambatan-hambatan yang ada.

5. Monitoring

Setelah implementasi tahapan monitoring merupakan tahapan yang penting, agar jaringan komputer dan komunikasi dapat berjalan sesuai dengan keinginan dan tujuan awal dari user pada tahap awal analisis, maka perlu dilakukan kegiatan monitoring. Monitoring bisa berupa melakukan pengamatan pada:

a) Infrastruktur hardware: dengan mengamati kondisi reliability/kehandalan sistem yang telah dibangun.
b) Memperhatikan jalannya paket data di jaringan (pewaktuan, latency, peektime, troughput).
c) Metode yang digunakan untuk mengamati kondisi jaringan dan komunikasi secara umum secara terpusat atau tersebar.
d) Pendekatan yang paling sering dilakukan adalah pendekatan Network Management. Dengan pendekatan ini banyak perangkat baik yang lokal dan tersebar dapat dimonitor secara utuh.

6. Management

Pada level manajemen atau pengaturan, salah satu yang menjadi perhatian khusus adalah masalah kebijakan (policy). Kebijakan perlu dibuat untuk membuat/mengatur agar sistem yang telah dibangun dan berjalan dengan baik dapat berlangsung lama dan unsur reliability terjaga. Policy akan sangat

tergantung dengan kebijakan level management dan strategi bisnis perusahaan tersebut. IT sebisa mungkin harus dapat mendukung atau alignment dengan strategi bisnis perusahaan.

1.7. Sistematika Penullisan

Pada penulisan skripsi ini, akan dipergunakan sistematika penulisan sebagai berikut:

BAB I – Pendahuluan

Bagian ini berisikan informasi mengenai latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian. Metode yang digunakan dan sistematika penulisan.

BAB II – Landasan Teori

Bagian ini berisi mengenai teori dan penjelasan lainya yang relevan mengenai analisis dan implementasi bentuk serangan dan permasalahan lain yang akan dibahas dalam penulisan skripsi ini diantaranya Wifislax, Fluxion, Snort dan lain sebagainya.

BAB III – Metode Penelitian.

Bagian ini berisi tentang analisis dan implementasi dari metode yang digunakan dalam penelitian ini serta rule dan data – data yang dibutuhkan dalam perancangan suatu system serangan yang terdiri dari tampilan interface dari jenis serangan dan analisis yang digunakan.

BAB IV – Hasil dan Pembahasan

Pada bab ini berisi tentang implementasi serangan dan analisis yang sudah di terapkan pada perangakat yang menggunakan jaringan *wireless* dan evaluasi mengenai *rule* dan data dari serangan.

BAB V – Penutup

Bagian ini berisi mengenai kesimpulan yang dapat diambil dari penyusunan tugas akhir, serta saran – saran penulis yang diharapkan dapat bermanfaat bagi pihak – pihak yang berkepentingan.