BAB I

PENDAHULUAN

1.1. Latar Belakang

Network forensics (forensik jaringan) adalah kegiatan menangkap, mencatat dan menganalisis kejadian pada jaringan untuk menemukan sumber serangan keamanan atau masalah kejadian lainnya. Kekuatan dari forensik adalah memungkinkan analisis dan mendapatkan kembali fakta dan kejadian dari lingkungan, karena fakta mungkin saja tersembunyi. Berbeda dari forensik pada umumnya, forensik komputer adalah kegiatan mengumpulkan dan menganalisis data dari berbagai sumber daya komputer.

Pada era saat ini, web server dan aplikasi berbasis web merupakan target serangan yang popular bagi kalangan peretas. Selain kemudahan dalam mengakses, ketersediaan resource konten aplikasi melalui jaringan (internet) membuat peretas memiliki banyak waktu untuk melakukan analisis dan serangan terhadap resource target serangan. Web server merupakan sebuah aplikasi yang terdapat pada server yang melayani permintaan HTTP atau HTTPS dari browser dan mengirimkannya kembali dalam bentuk halaman-halaman web.

Data setiap pengunjung yang mengirimkan permintaan atau ketika mengakses aplikasi berbasis web akan disimpan pada suatu file yang dinamakan log dalam hal ini yang terdapat pada web server. Data pengunjung yang terdapat

pada log web server akan sangat bermanfaat apabila nantinya terdapat suatu permasalahan yang terjadi terhadap web server tersebut, misalnya kasus peretasan aplikasi web (deface). Dengan memeriksa satu per satu setiap catatan yang tersimpan pada log, maka data-data seorang peretas akan diketahui. Data peretas tersebut, dapat diketahui salah satu caranya adalah dengan melihat dari alamat IP yang dipakai untuk mengakses web server.

Log yang berasal dari komputer (forensik komputer) adalah log antivirus, log database atau log dari aplikasi yang digunakan. Forensik jaringan merupakan bagian dari forensik digital, dimana bukti ditangkap dari jaringan dan di interpretasikan berdasarkan pengetahuan dari serangan jaringan. Hal ini bertujuan untuk menemukan penyerang dan merekonstruksi tindakan serangan penyerang melalui analisis bukti penyusupan. Kasus SQL Injection terjadi ketika seorang penyerang dapat memasukkan serangkaian pernyataan SQL ke query dengan memanipulasi data input ke aplikasi. SQL Injection adalah sebuah metodologi serangan yang menargetkan data yang berada dalam database melalui firewall yang melindungi data tersebut. Forensik jaringan berakar dari keamanan jaringan dan deteksi penyusupan. Forensik jaringan berkaitan dengan perubahan data dari milidetik ke milidetik. Investigasi serangan cyber atau penyusupan adalah investigasi forensik jaringan. Tantangan utama yang dihadapi dari forensik jaringan adalah bagaimana caranya mempertahankan bukti kemudian digunakan di pengadilan.

Website Kabar Indonesia dengan domain www.kabarindonesia.com merupakan situs kabar berita yang memiliki banyak artikel. Namun website ini memiliki kerentanan terhadap serangan *SQL Injection* dimana pernah terjadi serangan *SQL Injection* pada *web server*, celah tersebut didapatkan dari salah satu artikel dimana di artikel tersebut *vuln* terhadap serangan *SQL Injection* hal ini tentu sangat merugikan karena penyerang bisa masuk langsung ke *database.*

Maka dari itu di diperlukan sebuah investigasi dan penyidikan dengan menggunakan *Network Forensics* (forensik jaringan) pada penelitian ini dan data yang di teliti adalah data dari log serangan *SQL Injection* yang menuju ke server.

Berdasarkan latar belakang yang telah diuraikan diatas maka peneliti mengangkat judul "**Penerapan Teknik Komputer Forensik Basis Data Untuk Menelusuri Serangan Pada Web Server"**

1.2. Rumusan Masalah

Adapun rumusan masalah ini adalah "Bagaimana cara mencari bukti adanya serangan pada web server berdasarkan log serangan yang ada"

1.3. Batasan Masalah

penelitian ini dibatasi hanya pada:

1. Mengumpulkan dan membaca *log* serangan terhadap web server yang ada di snort.

1.4. Tujuan Dan Manfaat

1.4.1 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Menerapkan metode teknik komputer forensik dalam proses identifikasi barang bukti berupa log aktivitas dan mengumpulkan bukti digital.
2. Mencari tahu jenis serangan yang dilakukan.

1.4.2 Manfaat Penelitian

Adapun manfaat dari penelitan ini adalah sebagai berikut:

1. Meningkatkan keamanan *web server.*
2. Memberikan pengenalan dan pemahaman terhadap metode penanganan kasus serangan terhadap web server dengan model investigasi teknik komputer forensik.

1.5. Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah metode *action research* menurut masyhiri dan zainudin (2009) *Action Research* adalah metode untuk mengembangkan keterampilan – keterampilan baru atau cara

pendekatan baru untuk memecahkan masalah di dunia kerja atau dunia terapan lain.

Adapun tahapan yang merupakan siklus dari *Action Research* ini yaitu :

1. Melakukan diagnose *(diagnosting)*
2. Melakukan rencana tindakan *(action planning)*
3. Melakukan tindakan *(action taking)*
4. Melakukan evaluasi *(evaluating)*
5. Pembelajaran *(learning)*

Dari tahapan diatas maka yang akan penulis lakukan pada setiap tahap sesuai dengan judul yang penulis angkat yaitu sebagai berikut :

1. Melakukan Diagnosa *(Diagnosting)*, melakukan identifikasi masalah – masalah pokok yang ada guna menjadi dasar dalam penelitian. Pada tahap ini peneliti melakukan diagnose terhadap parameter yaitu terdapat sebuah serangan pada *web server*.
2. Membuat Rencana Tindakan *(action planning)*, Peneliti mempelajari masalah yang ada lalu dilanjutkan dengan menyusun rencana tindakan yang akan dilakukan dalam menyelesaikan masalah-masalah pada *web server* sehingga diharapkan mampu untuk menutupi kerentanan yang ada pada *web server.*
3. Melakukan Tindakan *(action taking)*, Peneliti melakukan tindakan disertai implementasi rencana yang telah di buat dengan melakukan pengamanan

pada *web server* sehingga dapat menutupi kerentanan terhadap celah – celah pada web server tersebut.

4. Melakukan Evaluasi *(evaluating),* Peneliti melakukan evaluasi hasil dari tindakan yang dilakukan pada *web server* dalam bentuk laporan.

5. Pembelajaran *(Learning),* Setelah melakukan analisis yang sudah dianggap cukup, kemudian peneliti mendapatkan rapot tentang kelemahan – kelemahan pada *web server* tersebut.

1.5.1 Metode pengumpulan data

Metode Pengumpulan Data yang digunakan dalam penelitian ini adalah :

1. Kepustakaan

   Mengumpulkan data dengan cara mencari dan mempelajari data-data dari buku-buku ataupun dari referensi lain yang berhubungan dengan penulisan laporan penelitian proposal. Buku yang digunakan penulis sebagai referensi, adapun metode yang digunakan penulis dalam merancang dan mengembangkan dapat dilihat pada daftar pustaka.

2. Pengamatan

   Pengamatan (observation), data dikumpulkan dengan melihat secara langsung dari objek yang di teliti pada Web server.

1.6 Sistematika Penulisan

Untuk mendapatkan gambaran secara garis besar dalam penulisan laporan penelitian ini, maka penulisan dibagi menjadi 5 bab, yaitu :

BAB I PENDAHULUAN

Pada bab ini dijelaskan mengenai latar belakang penulisan, perumusan masalah, batasan masalah, tujuan dan manfaat penelitian, metodologi penelitian, waktu dan tempat penelitian, alat dan bahan yang digunakan, metode penelitian, metode pengumpulan data, dan sistematika penulisan.

BAB II LANDASAN TEORI

Pada bab ini menjelaskan tentang tinjauan objek dan landasan dari teori-teori dasar yang mendukung materi dalam penelitian ini.

BAB III PERANCANGAN

Pada bab ini membahas mengenai rancangan pengembangan yang berpedoman dari metode *action research* yang meliputi, *Diagnosting, action planning, action taking, evaluating, learning*

BAB IV HASIL DAN PEMBAHASAN

Dalam bab ini penulis akan menjelaskan mengenai hasil dan langkah-langkah pembahasan mengenai tahap investigasi forensik

BAB V KESIMPULAN DAN SARAN

Dalam bab ini penulis menjelaskan secara garis besar mengenai kesimpulan dan saran dari hasil peneliti