# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang

Universitas Islam Negeri Sultan Syarif Kasim Riau (UIN SUSKA) merupakan salah satu universitas negeri yang berbasis Islami. UIN SUSKA pada saat ini merupakan lembaga pendidikan dengan semboyan menuju "*world class university*" dimana untuk mencapai tujuan tersebut dibutuhkan seluruh sumberdaya-sumberdaya pendukung. Salah satu sumberdaya pendukung untuk mencapai tujuan tersebut adalah jaringan internet yang akan digunakan oleh staff, pengajar, dan mahasiswa sehingga dalam proses administrasi dan akademik yang terjadi di UIN SUSKA RIAU efektif dan efisien.

Salah satu dari fasilitas yang dimiliki UIN SUSKA RIAU adalah jaringan kampus. Jaringan ini dikelola oleh salah satu Unit Pelayanan Teknis (UPT) kampus yaitu Departemen Pusat Teknologi Informasi dan Pangkalan Data (PTIPD). PTIPD merupakan UPT yang bertanggung jawab berjalannya segala unit yang berhubungan teknologi informasi dan pangkalan data di UIN SUSKA RIAU salah satunya berjalannya sistem informasi kampus. Sistem Informasi memiliki peranan sangat besar dalam perkembangan teknologi di UIN SUSKA RIAU, sehingga web server dan aplikasi berbasis web merupakan salah satu target penyerangan yang sering dilakukan oleh peretas (hacker). Selain bisa di akses dengan mudah, ketersediaan resource konten aplikasi melalui jaringan (internet) membuat peretas (hacker) memiliki kebebasan untuk melakukan analisis dan serangan terhadap resource target serangan.

Menurut Direktorat Keamanan Informasi, Direktorat Jenderal Aplikasi Informatika dan Kementerian Komunikasi dan Informatika tahun 2011. Saat ini situs web merupakan salah satu layanan informasi yang banyak diakses oleh

pengguna internet di dunia. Data setiap pengunjung ketika mengakses aplikasi berbasis web akan tersimpan pada file yang dinamakan log yang terdapat pada web server. Data pengunjung pada log web server sangat diperlukan untuk melakukan pencarian data ketika terjadi penyerangan terhadap web server. Data log file yang bisa di ambil salah satunya adalah alamat IP yang dipakai untuk mengakses web server. Namun data alamat IP yang tersimpan dalam log berisi seluruh data pengunjung yang mengakses web server sehingga menjadi tidak efisien karena harus diperiksa satu per satu alamat IP. Berdasarkan permasalahan tersebut, ada beberapa perangkat lunak yang dapat digunakan untuk melakukan identifikasi pelaku terkait dengan serangan ke log web server diantaranya IDS (Intrusion Detection System). Aplikasi IDS yang populer saat ini adalah Snort.

Snort merupakan aplikasi linux yang dapat digunakan untuk meningkatkan keamanan komputer. Ada beberapa software pihak ketiga yang memberikan GUI untuk snort yang berbasis PHP sehingga bisa diakses melalui web browser. Dengan membuat berbagai rules untuk mendeteksi ciri-ciri khas (signature) dari berbagai macam serangan, maka Snort dapat mendeteksi dan melakukan logging terhadap serangan-serangan tersebut. Menurut penelitian ( Kharulanam, 2011) yang menggunakan snort untuk pendeteksi serangan pada jaringan komputer, menurutnya kelemahan mesin snort harus mengupdate rule-rule dikarenakan usaha para peretas (hacker) terus berkembang, sehingga sistem pendeteksi ini harus selalu diperbarui apabila terdeteksi pola penyerangan baru.Snort dapat melakukan deteksi adanya penyusupan terhadap log web server dengan cara menganalisis data log dan menyesuaikan dengan signature yang dimiliki oleh Snort tersebut. Dalam melakukan identifikasi, snort hanya dapat melakukan analisis log. Sebagai contoh, berkas-berkas yang sensitif (seperti program untuk melakukan login, authetikasi) dimonitor dengan ketat. Jika terjadi perubahan yang tidak direncanakan maka ada kemungkinan penerobos sudah masuk dan mengganti (mengubah) berkas tersebut. Demikian pula berkas log dimonitor untuk mengetahui adanya penerobosan.

Umumnya serangan yang terjadi menimbulkan kesan negatif, merugikan atau ketidaknyamanan (seperti *defacing*), seperti situs www.presidensby.info pada rabu 1 september 2012 sempat di *deface* peretas. Pelaku meninggalkan jejak dengan menuliskan diri sebagai *Jember Hacker Team*.Namun tidak tertutup kemungkinan penyerang dapat membuat masalah yang lebih serius atau bahkan sangat merugikan. Permasalahan yang ditimbulkan adalah bagaimana cara mengidentifikasi pola kecenderungan penyerangan yang dilakukan para peretas (hacker), pada penelitian sebelumnya (Chayanto, Adi, 2014), mereka menginvestigasi forensika data log web server untuk mencari bukti digital terkait adanya serangan menggunakan hidden markov models. Pada penelitian ini mereka membahas data log pada web server ketika terjadi penyerangan (hacker) yang di alami web server sehingga penelitian ini bukan mencegah atau mencari adanya tanda penyerangan tetapi hanya mencari bukti apabila web server sudah terserang oleh peretas (hacker).

Selanjutnya (Halvey.M, dkk, 2005) melakukan penelitian hubungan antara waktu akses pengguna dengan segmentasi log dengan menggunakan markov model mereka berhasil mendapatkan kunci untuk mengetahui pola perilaku pengguna dengan melihat dari pola waktu pengaksesan web mobile. Namun pada penelitian tersebut terdapat beberapa kriteria yang digunakan untuk prediksi perilaku pengguna hanya berdasarkan Time (waktu pengaksesan dan berapa lama mereka mengakses web mobile), Hits (klik, analisa akan dilakukan ketika pengguna mulai mengklik situs web), dan IP Address sehingga kurang efektif karena tidak bisa menganalisa apa yang dilakukan pengguna pada saat mengakses web mobile tersebut. Pada penelitian lain yang menggunakan HIDS (Host Based Intrusion Detection System) dengan melakukan *quick report* pada system pendeteksi penyusupan berbasis host (HIDS), penelitian ini menjadi alternatif notifikasi kepada administrator untuk mengambil tindakan terhadap intrusi yang ada. (Abdillah, R, 2014: Vol. 11). Pada penelitian ini dibangun menggunakan konsep SMS Gateway, namun proses tindak lanjut akan cepat terlaksana apabila administrator cepat menanggapi notifikasi yang dikirim oleh

sistem. Jadi efektif tidaknya sistem ini apabila respon cepat yang dilakukan administrator.

Pada juni 2014 salah satu dari peserta Seminar nasional aplikasi teknologi informasi (SNATI) di jogjakarta menemukan cara mencari atau menginvestigasi data log ketika terjadi penyerangan. (Triawan, Adi, 2014). Pada penelitian tersebut mereka mencari file log yang sudah terjadi penyerangan dengan cara identifikasi berdasarkan ip dan respon code error. Pada peleitian tersebut yang menggunakan algoritma Hidden Markov Model mendapatkan hasil rincian data log penyerangan serta menampilkan dalam bentuk ip geolocation, penelitian tersebut belum membahas secara rinci waktu penyerangan dan tingkat keakuratan penyerangan pada log tidak ada beliau hanya menampilkan posisi ip penyerangan.

Berkaitan dengan hal tersebut, melalui penelitian ini diharapkan dapat melakukan analisa pola kecenderungan penyerangan terhadap log file berdasarkan segmentasi waktu yang tersimpan pada web server di UIN SUSKA sehingga dapat mengantisipasi apabila ada pengunjung yang mencoba melakukan penyerangan (anomaly detection). Banyaknya data log tersebut, akan menyebabkan record yang terdapat pada log file menjadi semakin banyak. Dengan semakin banyaknya data log, terdapat record pada log yang tidak terkait dengan proses serangan, record tersebut disebut dengan false alarm. Untuk mengurangi false alarm yang disebabkan banyaknya data log, maka akan dilakukan filtering dan statistik terhadap log menggunakan metode hidden markov models. Maka akan dilakukan penelitian yang berjudul **"**PREDIKSI POLA KECENDERUNGAN PENYERANGAN WEB SERVER**".**

## 1.2 Rumusan Masalah

Berdasarkan dari latar belakang yang telah disebutkan di atas, maka dibuatlah rumusan masalah yaitu bagaimana memprediksi pola kecenderungan penyerangan

web server berdasarkan segmentasi waktu berbasis log data pada web server yang ada di UIN SUSKA RIAU.

## 1.3 Batasan Masalah

Berikut beberapa hal yang menjadi batasan masalah dalam penelitian tugas akhir yang dilakukan adalah sebagai berikut:

1. Penelitian tugas akhir ini hanya memprediksi pola kecenderungan penyerangan pada web server yang difokuskan pada aktifitas log data.
2. Aktifitas log data yang akan dianalisa yaitu data log aktifitas dimulai dari tanggal 25 januari 2016 sampai dengan tanggal 3 agustus 2016 yang diperoleh dari web server tif.uin-suska.ac.id.
3. Kriteria untuk analisa pola penyerangan dalam penelitian ini yaitu user Identification (Ip Address), session identification (user yang merequest GET), dan transaction identification ( user yang menimbulkan error).
4. Untuk memprediksi kecenderungan penyerangan web server dalam penelitian tugas akhir ini menggunakan metode Hidden Markov Model.

## 1.4 Tujuan Penelitian

Tujuan dalam penelitian ini yaitu untuk mengetahui pola kecenderungan penyerangan pada suatu situs web sehingga membantu meningkatkan keamanan pada suatu situs web tif.uin-suska.ac.id.

## 1.5 Sistematika Penulisan

Pada penyusunan Tugas Akhir, sistematika penulisan diatur dan disusun dalam 5 (lima) bab, dan tiap-tiap bab terdiri dari sub-sub bab. Untuk memberikan gambaran yang lebih jelas, maka diuraikan secara singkat mengenai materi dari bab-bab dalam penulisan Tugas Akhir ini sebagai berikut :

## Bab I. Pendahuluan

Menjelaskan tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian dan sistematika penulisan.

## Bab II. Landasan Teori

Pada bab ini akan dijelaskan tentang teori-teori umum dan khusus yang berhubungan dengan konsep *Metode Hidden Markov Model* (HMM), *Error Log*. Teori yang didapatkan berasal dari buku – buku dan jurnal – jurnal *online* mengenai penelitian sejenis yang di akses melalui *internet*.

## Bab III. Metodologi Penelitian

Bab ini membahas langkah-langkah yang dilakukan dalam proses penelitian tugas akhir ini, yaitu mulai dari identifikasi masalah, rumusan masalah, studi literature, analisa (preprocessing, identifkasi log web server, fase training, fase testing, dan fase analisis), dokumentasi, kesimpulan dan saran.

## Bab IV. Analisa

Berisi tentang tahapan analisa iaitu data preprocessing, identifkasi log web server, fase training, fase testing, dan fase analisis. Dengan menggunakan teknik dari fase training dan testing yang nantinya digunakan untuk mengukur dan mengevaluasi serangan yang terdeteksi apakah berhasil atau gagal, kemudian kedua klasifikasi sesi dan kuantifikasi serangan akan membantu untuk menyusun dokumentasi.

## Bab V. Penutup

Dalam bab ini akan dijelaskan mengenai kesimpulan dari hasil penelitian yang telah dilakukan dan saran terhadap penelitian kedepannya.