# BAB 1
# PENDAHULUAN

## 1.1 Latar Belakang

Keamanan pada sebuah jaringan internet merupakan hal yang sangat penting untuk menjaga jaringan tersebut dari aktivitas yang bertujuan untuk menyerang dan menyusup ke dalam jaringan tersebut. Serangan yang masuk pada sebuah jaringan bisa menyebabkan jaringan tersebut lumpuh, atau menurunnya performa jaringan tersebut jika tidak ditangani dengan cepat dan tepat. Oleh karena itu, butuh adanya pengolahan keamanan yang sistemik serta komprehensif. Aspek kebutuhan pengelolaan keamanan harus memuat 3 unsur penting yang biasa disebut CIA, yaitu *confidentiality* (kerahasiaan), *integrity* (integritas) dan *availability* (ketersediaan). Adapun dari sisi layer dimana dapat melihat mekanisme aliran *log* secara *realtime* yaitu menggunakan layer 4 dan 5, dikarenakan layer tersebut berfungsi sebagai *transport* yang bertugas untuk komunikasi data melalui koneksi seperti TCP (Transmission Control Protocol ) dan UDP (User Data Protocol).

Saat ini pada laboratorium jaringan komputer yang ada di kampus mempunyai jaringan infrastruktur yang dapat mengakses internet. Sehingga dipastikan adanya potensi indikasi ancaman dari dalam untuk menginstalasi sebuah *software* berbahaya.

Dikarenakan saat ini pihak laboratorium jaringan komputer belum ada mengimplementasikan *log monitoring* di laboratorium tersebut. Maka penulis mengajukan untuk implementasikan sistem *log monitoring* pada laboratorium jaringan komputer.

| Serverfault | |
|---|---|
| Topics | Words |
| log in network | TCP, UDP, log, port, lo, accept |
| syslog in messaging | syslogng, log, destination, source, get, messages |
| **Superuser** | |
| Topics | Words |
| syslog in message server | syslog, server, log, syslogd, mesaages, information |
| log in opengl file | system, opengl, log, logs, file, extension |
| log in file using command line | file, log, command, log, commands, output |
| **Software Engineering** | |
| Topics | Words |
| Java | public, void, static, try, catch, throw, class, exception |
| log in client server | log, client, server, clients, logger,request |
| log in user application | log, user, application, logging, logged, data |
| log in files | log, files, appender, file, tests, application |
| log in applications | logs, log, message, loglevel, application, information |
| log in systems | system, logging, libraries, log, developer, exception |

:

Gambar 1. 1 Data topic logging populer

*Sumber :* (Gujral *et al.*, 2019)

Berdasarkan gambar 1.1 data bersumber dari topik *logging* populer yang teridentifikasi, ada 3 hal yang dijadikan penulis sebagai data, yaitu berdasarkan *logging serverfault, superuser* dan *software engineering.*

Maka salah satu solusi yang dapat digunakan adalah SIEM (*Security Infromation and Event Management*). SIEM adalah sistem *monitoring* yang dapat mendeteksi serangan dan respon disuatu sistem keamanan terhadap serangan melalui *log* dari berbagai *event-log* yang berasal dari sumber data serta dapat pemeriksaan integritas, deteksi *rootkit,* dan mempunyai respon aktif untuk menemukan kesamaan pada pola yang apabila sama akan dianggap sebagai ancaman secara *real-time*. Adapun *software* yang menggunakan teknologi SIEM ini seperti Logstash, Graylog, Splunk, serta Solarwinds.

Dalam penulisan skripsi ini, penulis akan meneliti tentang *log* dari layanan yang terdapat pada server seperti Akses Root dan Nmap. Berdasarkan uraian diatas, saya sebagai penulis tertarik dalam menggunakan laporan skripsi yang berjudul **"Studi Kasus Perancangan Sistem Log Monitoring Keamanan Jaringan Untuk Local Area Network (LAN) Pada Laboratorium Jaringan Universitas Bhayangkara Jakarta Raya"**

## 1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah diuraikan sebelumnya, maka dapat diidentifikasikan masalah sebagai berikut:

1. Belum ada sistem untuk mengetahui pemantauan aktivitas *log* terhadap ancaman dari penyusup
2. Belum ada informasi mengenai ancaman serta pola serangan yang berada dalam jaringan LAN
3. Tidak tersedianya sistem yang dapat mendeteksi penyusup pada LAN

## 1.3 Batasan Masalah

Berdasarkan masalah yang ditemukan, maka batasan masalah dari skripsi ini sebagai berikut:

1. Sistem yang berjalan berfokus pada informasi mengenai ancaman serta pola serangan.
2. *Monitoring* yang dilakukan yaitu pemantauan aktivitas *log.*
3. Perancangan khusus untuk LAN pada laboratorium jaringan komputer.

## 1.4 Rumusan Masalah

Berdasarkan dari latar belakang dan identifikasi masalah, maka perumusan masalah dalam skripsi ini sebagai berikut adalah bagaimana cara membangun sistem dan mengimplementasikannya untuk keamanan pada jaringan terhadap serangan dari penyusup?

## 1.5 Tujuan Penelitian

Adapun tujuan dalam penelitian skripsi ini adalah untuk membangun sistem *monitoring* jaringan untuk aktivitas yang mencurigakan didalam jaringan.

## 1.6 Manfaat Penelitian

Adapun manfaat dalam penelitian skripsi ini adalah memudahkan dalam mengidentifikasi penyusup yang berada di dalam jaringan serta mengetahui informasi mengenai ancaman dari penyusup.

## 1.7 Metode Penelitian

Metodologi yang digunakan pada penelitian ini adalah dengan menggunakan:

a) Observasi

Melakukan pengamatan secara langsung atau tinjauan langsung ke perusahaan, melakukan pengamatan langsung terhadap objek permasalahan yang diteliti.

b) Metode Wawancara

Dilakukan dengan mengajukan pertanyaan-pertanyaan atau tanya jawab secara langsung kepada pihak yang menangani permasalahan tersebut untuk mengetahui cara mengatasinya.

c) Studi Literatur

Mengkaji dan mempelajari berbagai jenis buku serta artikel-artikel dan jurnal dari internet yang berhubungan dengan permasalahan yang diteliti, dimana teori-teori yang dipergunakan untuk dijadikan sebagai refrensi dalam penyusunan skripsi.

## 1.8 Sistematika Penulisan

Berdasarkan skripsi ini sistematika yang dibuat oleh penulis sebagai berikut:

**BAB I: PENDAHULUAN**

Pada bab ini penulis akan menguraikan mengenai latar belakang masalah, identifikasi masalah, batasan masalah, rumusan masalah, tujuan dan manfaat penelitian yang digunakan dalam pengumpulan data serta sistematika penulisan.

**BAB II: LANDASAN TEORI**

Pada pembahasan bab ini menjelaskan mengenai tinjauan pustaka dan landasan-landasan teori yang saling berkaitan dengan topik pembahasan.

**BAB III: METODOLOGI PENELITIAN**

Bab ini penulis berisikan tentang objek penelitian, kerangka penelitian, sistem berjalan, analisis sistem berjalan, permasalahan, analisis usulan sistem, analisis kebutuhan sistem, dan metode penelitian serta alat penelitian yang diperlukan.

**BAB IV: PERANCANGAN SISTEM DAN IMPLEMENTASI**

Pada bab ini menjelaskan tentang perancangan sistem yang diusulkan dan menjelaskan mengenai usulan tersebut yang akan di gambarkan dengan perancangan sistem prototipe, spesifikasi usulan dan evaluasi terhadap implementasi tersebut.

## BAB V: PENUTUP

Bab ini berisikan mengenai kesimpulan dan saran dari penulisan skripsi yang telah dibuat.