BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Pasca pandemi COVID-19, saat ini penggunaan dan perkembangan teknologi informasi mengalami percepatan yang sangat signifikan, contohnya di institusi pendidikan yang memanfaatkan teknologi informasi untuk bertukar informasi dan data melalui jaringan komputer atau internet. Semakin meningkatnya penggunaan jaringan komputer atau internet tentu resiko atau ancaman akan muncul terhadap pengguna dan penyedia layanan. Keamanan jaringan komputer telah menjadi masalah besar di institusi pendidikan untuk menjaga integritas dan keberlangsungan operasional institusi tersebut. Berdasarkan data dari situs *checkpoint* terdapat 10 juta lebih serangan *cyber* dalam satu hari dimana jenis serangan *Denial of Service Attack* menjadi 8 besar jenis *cyber attack* yang digunakan oleh *Cybercriminals* dan urutan teratas serangan *cyber* tersebut ditunjukkan di institusi pendidikan. Dari data tersebut dapat dikatakan bahwa setiap menit ada serangan *cyber* yang terjadi di seluruh dunia dan institusi pendidikan merupakan target teratas serangan *cyber* tersebut.

Institusi pendidikan menggunakan jaringan komputer atau internet untuk berbagai keperluan operasional seperti menyimpan data sensitif atau administrasi, memberikan akses ke sumber daya digital, dan melakukan proses pembelajaran. Maka dari itu perlindungan keamanan jaringan komputer menjadi aspek penting dalam institusi pendidikan. Keamanan jaringan komputer di institusi pendidikan melibatkan langkah-langkah untuk melindungi data pribadi dosen dan mahasiswa, mencegah akses tidak sah terhadap sumber daya digital dan melindungi kekayaan intelektual yang dimiliki oleh institusi pendidikan tersebut. Dalam operasionalnya institusi pendidikan perlu melakukan pemantauan serta pemeliharaan sistem jaringan komputer dan mengadopsi kebijakan atau standar sistem keamanan jaringan komputer yang diterbitkan oleh pemerintah.

Menurut Peraturan Menteri Komunikasi dan Informatika No. 4 Tahun 2016 yang mengatur Standar Sistem Manajemen Keamanan Informasi (SMKI), disebutkan bahwa setiap penyelenggara sistem elektronik wajib mematuhi SMKI dengan menjunjung nilai-nilai CIA, yaitu Kerahasiaan (*Confidentiality*), Keutuhan (*Integrity*), dan Ketersediaan (*Availability*). Oleh karena itu, keamanan jaringan komputer di lingkungan institusi pendidikan seharusnya dapat secara efektif melindungi data yang bersifat sensitif, mencegah ancaman, dan menjaga integritas jaringan. Untuk memenuhi standar tersebut institusi pendidikan wajib memiliki kebijakan keamanan jaringan yang jelas dan terdokumentasi. Kebijakan tersebut mencakup kebijakan akses yang terbatas, tindakan pencegahan serangan *malware*, dan langkah-langkah lainnya untuk melindungi jaringan komputer. Selain itu Institusi pendidikan juga wajib memiliki sistem pemantauan dan deteksi keamanan yang aktif. Hal ini untuk mendeteksi aktivitas mencurigakan atau serangan, termasuk serangan *DDoS*, serangan *phishing*, atau upaya peretasan. (Rijal Kamal & Andri Setiawan, 2021).

Politeknik Kesehatan Kartini Bali merupakan sebuah institusi pendidikan tinggi di bidang kesehatan. Sebagai lembaga pendidikan, Politeknik Kesehatan Kartini Bali juga menerapkan teknologi informasi dan jaringan komputer untuk menunjang aktivitas operasional dan pembelajaran. Politeknik Kesehatan Kartini Bali menggunakan jaringan komputer untuk mendukung konektivitas, komunikasi, akses informasi di seluruh kampus dan termasuk penyediaan akses internet yang cepat dan stabil bagi mahasiswa, dosen dan staf. Institusi pendidikan ini memiliki tiga buah server yang berfungsi untuk sistem *web server*, sistem informasi terintegrasi (sister) perguruan tinggi, dan sistem Neo Feeder PDDikti.

Agar memastikan pelayanan dan operasional institusi berjalan dengan baik, perlindungan atau pengamanan yang efektif menjadi suatu keharusan. Politeknik Kesehatan Kartini Bali menggunakan sistem *Intrusion Detection System* (IDS) Snort sebagai pendeteksi aktifitas mencurigakan pada jaringan komputer dan firewall sederhana yang terdapat di router mikrotik sebagai

sistem pengamanan jaringan komputer. Sistem snort dan *firewall* membantu menentukan paket jaringan komputer yang boleh lewat dan yang diblokir berdasarkan *rule* yang ditentukan oleh administrator jaringan. Apabila terdeteksi aktivitas yang mencurigakan atau anomali dan aktivitas tersebut merupakan serangan, namun tidak tercatat dalam rule keamanan yang telah ditentukan atau terjadi kesalahan dalam mendefinisikan suatu rule, maka hal tersebut dapat menjadi ancaman serius bagi keamanan jaringan komputer. Dari data dan fakta yang ada dilapangan untuk mengoptimasi sistem keamanan jaringan komputer di Politeknik Kesehatan Kartini Bali peneliti mengusulkan untuk memanfaatkan *Framework Streamlit* sebagai *Live Analysis* berbasis *website* untuk memberikan hasil analisis *event* dan *log* paket jaringan komputer. Penelitian ini menggunakan *One-Class Support Vector Machine (OCSVM)* sebagai *Algoritma Machine Learning* pada *Intrusion Detection System* (IDS) untuk melakukan analisis dan menemukan anomali data pada jaringan komputer Politeknik Kesehatan Kartini Bali, penggunaan algoritma tersebut didasarkan pada penelitian Sudhanshu Sekhar Tripathy, (2023) yang berdasarkan pengujian Nilai akurasi *algoritma One-Class Support Vector Machine (OCSVM)* sebesar 98.08%. Pada penelitian ini mengimplementasikan sistem *Intrusion Detection System* Suricata untuk menggantikan sistem lama yaitu Snort. Penggunaan sistem *Intrusion Detection System* Suricata didasarkan pada penelitian Adam Dwi Ralianto & Cahyono, (2021) yang berdasarkan pengujian nilai akurasi suricata didapat 61% dibanding snort yang hanya 31%. Dari sisi penggunaan memory Suricata lebih stabil daripada Snort dikarenakan menggunakan fitur multithreading yang dimilikinya.

Berdasarkan hal tersebut ditemukan bahwa sistem keamanan jaringan komputer yang ada di Politeknik Kesehatan Kartini Bali saat ini perlu dioptimalkan ke sistem yang baru. Maka penelitian ini akan mengimplementasi dan melakukan analisis penggunaan *Framework Streamlit* sebagai *Live Analysis* berbasis *website*, penerapan *One-Class Support Vector Machine (OCSVM)* sebagai *Algoritma Machine Learning* pada *Intrusion*

Detection System (IDS) dan mengimplementasi sistem *Intrusion Detection System* (IDS) Suricata untuk memecahkan masalah yang ada di sistem keamanan jaringan komputer Politeknik Kesehatan Kartini Bali, Maka peneliti akan mengangkat penelitian ini dengan judul "Optimasi Keamanan Jaringan Komputer Berbasis *Live Analysis* dan *Algoritma Machine Learning* Pada *Intrusion Detection System* (IDS) Studi Kasus Poltekkes Kartini Bali". Dengan dilakukan penelitian ini diharapkan dapat melakukan optimasi keamanan jaringan komputer di Politeknik Kesehatan Kartini Bali.

1.2 Identifikasi Masalah

Berdasarkan uraian latar belakang masalah diatas, maka dapat dibuat suatu identifikasi masalah yaitu:

1. Sistem keamanan jaringan komputer yang ada saat ini di Politeknik Kesehatan Kartini Bali dinilai dari sisi akurasi monitoring belum dilakukan optimasi.
2. Belum optimalnya sistem yang dapat melakukan analisis dan memberikan laporan mengenai kejadian dan log jaringan komputer secara visual.
3. Belum adanya suatu sistem yang mampu melakukan korelasi dan analisis terhadap *event* atau *log* dari berbagai sumber, serta menentukan apakah kejadian tersebut dapat dikategorikan sebagai anomali atau tidak.

1.3 Batasan Masalah

Agar penelitian tidak menyimpang dari maksud dan tujuan, maka peneliti membuat batasan masalah yaitu:

1. Implementasi sistem yang dibangun hanya untuk optimasi *monitoring*, menganalisis dan mendeteksi aktivitas mencurigakan di jaringan komputer Poltekkes Kartini Bali.
2. Sistem pendeteksi aktivitas yang mencurigakan di jaringan komputer menggunakan *Intrusion Detection System* (IDS) Suricata.
3. Pengumpulan dan pelaporan informasi dari aktivitas mencurigakan di jaringan komputer secara visual menggunakan *Framework Streamlit*

sebagai *Live Analysis* berbasis *website*.

4. *One-Class Support Vector Machine (OCSVM)* sebagai *Algoritma Machine Learning* digunakan untuk meningkatkan nilai akurasi sistem *Intrusion Detection System* (IDS) Suricata.
5. Pengujian untuk mengukur nilai optimasi sistem baru keamanan jaringan komputer dilakukan dalam satu jaringan yang sama dengan menggunakan Komputer *Attacker*.
6. Target yang menjadi serangan untuk pengujian sistem adalah komputer *server*.
7. Pengujian rules suricata menggunakan tiga jenis metode serangan yaitu *Port Scanning, Ddos Attack,* dan *Brute Force Attack.*
8. Parameter pengujian adalah kecepatan dalam membaca dan menganalisis *log* yang masuk ke dalam sistem keamanan.

1.4 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan di atas terdapat beberapa rumusan masalah yaitu:

1. Bagaimana implementasi *Framework Streamlit* sebagai *Live Analysis* berbasis *website* dan *Intrusion Detection System* (IDS) Suricata pada jaringan komputer Politeknik Kesehatan Kartini Bali?
2. Bagaimana melakukan analisis aktifitas yang merupakan anomali berdasarkan *log* yang didapat dari sistem keamanan jaringan komputer?
3. Bagaimana hasil optimasi keamanan jaringan komputer Politeknik Kesehatan Kartini Bali menggunakan *Framework Streamlit* sebagai *Live Analysis* berbasis *website* dan *One-Class Support Vector Machine (OCSVM)* sebagai *Algoritma Machine Learning* pada *Intrusion Detection System (IDS)?*

1.5 Tujuan Penelitian

Tujuan yang ingin dicapai dari penulisan dan pembuatan proposal tesis ini yaitu:

1. Melakukan implementasi *Framework Streamlit* sebagai *Live Analysis* berbasis *website* dan *One-Class Support Vector Machine (OCSVM)* sebagai *Algoritma Machine Learning* pada *Intrusion Detection System (IDS) Suricata* di sistem keamanan jaringan komputer Politeknik Kesehatan Kartini Bali.
2. Menguji *Framework Streamlit* sebagai *Live Analysis* berbasis *website* dan *One-Class Support Vector Machine (OCSVM)* sebagai *Algoritma Machine Learning* pada *Intrusion Detection System (IDS)* untuk mendeteksi penyerangan jaringan komputer dan menganalisis *log* penyerangan jaringan komputer Politeknik Kesehatan Kartini Bali.
3. Melakukan analisis hasil optimasi *Intrusion Detection System* (IDS) menggunakan *One-Class Support Vector Machine (OCSVM)* dan *Framework Streamlit* pada keamanan jaringan komputer Politeknik Kesehatan Kartini Bali untuk melakukan pendeteksian terhadap tiga metode serangan seperti *Port Scanning, Brute Force Attack* dan *Ddos Attack* sehingga memudahkan *administrator* jaringan komputer melakukan tindakan pengamanan jaringan komputer dengan cepat.

1.6 Manfaat Penelitian

Manfaat yang didapat dari penelitian ini adalah sebagai berikut:

1. Membantu *administrator* jaringan komputer Politeknik Kesehatan Kartini Bali dalam memonitoring keamanan jaringan komputer dan melakukan tindakan terhadap aktivitas yang mencurigakan.
2. Membantu optimasi sistem keamanan jaringan komputer Politeknik Kesehatan Kartini Bali dengan menggunakan *Framework Streamlit* sebagai *Live Analysis* berbasis *website* dan *Intrusion Detection System* (IDS).

1.7 Rencana Publikasi

Pada penelitian ini rencana publikasi atau jurnal yang dituju untuk tempat publish hasil penelitian adalah Jurnal Teknik Informatika (JUTIF)

yang dikelola oleh Jurusan Informatika Universitas Jenderal Soedirman Pada bulan Februari (No 2) yang sudah memiliki sertifikasi akreditasi SINTA 3.