BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi yang begitu pesat telah memberikan berbagai kemudahan dalam penyebaran data dan informasi melalui jaringan internet. Namun, seiring kemudahan tersebut, muncul pula ancaman siber yang semakin kompleks. Laporan *Data Breach Investigations Report (DBIR)* 2021 dari Verizon menyebutkan bahwa terdapat lebih dari 29.000 insiden kebocoran data di seluruh dunia, dengan peningkatan signifikan pada sektor Pendidikan dan layanan publik [1]. Ancaman seperti *SQL Injection, Brute Force*, dan *serangan Denial of service (DoS)* terus berkembang dan menyerang berbagai layanan web yang tidak memiliki sistem keamanan yang memadai [2].

Pada sistem informasi berbasis Web yang dimaksud adalah sistem informasi website Jurusan Teknik Informatika Politeknik Negeri Bengkalis yang dimana digunakan sebagai penyedia informasi akademik yang menjadi pusat komunikasi di ruang lingkup Jurusan Teknik Informatika. Dalam hal ini, website Teknik Informatika Politeknik Negeri Bengkalis berperan dalam menunjang kegiatan Pendidikan dan layanan informasi. Namun, pada website Teknik Informatika belum adanya sistem monitoring keamanan siber secara real-time yang membuat website teknik informatika berisiko menjadi target serangan siber kapan saja.

Sistem deteksi dini serangan siber merupakan pendekatan yang masih digunakan dalam dunia keamanan siber. Salah satu solusi opensource yang digunakan adalah *Wazuh*, yang dimana merupakan pengembangan dari OSSEC dengan kemampuan sebagai *Host-based intrusion Detection System (HIDS)* dan *SIEM (Security information and Event Management)*. *Wazuh* dapat memantau log sistem secara real time untuk mendeteksi aktivitas yang mencurigakan, dan memberikan peringatan kepada administrator [3]. *Wazuh* juga mendukung integrasi dengan telegram atau kustom visualisasi dashboard sistem SIEM, yang

menjadikannya fleksibel dan efisien untuk di implementasikan pada institusi dengan sumber daya terbatas.

Implementasi sistem deteksi dini menggunakan *wazuh* diharapkan mampu memberikan perlindungan terhadap website Teknik Informatika dari berbagai ancaman serangan siber. Melalui pengumpulan log, analisis aktivitas tidak wajar, dan pemberian notifikasi secara real time kepada administrator sehingga dapat segera merespons ancaman yang muncul. Hal ini tidak hanya membantu dalam pencegahan insiden siber, tetapi juga meningkatkan kesadaran keamanan siber dilingkungan kampus secara menyeluruh [1].

Dengan adanya sistem monitoring keamanan ini, diharapkan website jurusan dapat mengidentifikasi berbagai potensi ancaman siber yang dapat mengganggu ketersediaan informasi dan kepercayaan publik terhadap institusi. Penelitian ini menjadi langkah awal untuk meningkatkan ketahanan digital di sektor Pendidikan, khususnya di lingkungan Jurusan Teknik Informatika Politeknik Negeri Bengkalis.

1.2 Rumusan Masalah

Di era digital saat ini, institusi pendidikan semakin mengandalkan sistem informasi berbasis web untuk mendukung aktivitas akademik dan pelayanan informasi. Website Jurusan Teknik Informatika politeknik Negeri Bengkalis, sebagai salah satu sarana utama penyampaian informasi akademik dan komunikasi internal yang memiliki peran vital dalam menunjang kegiatan tridarma perguruan tinggi. Namun, pemanfaatan teknologi ini tidak terlepas dari ancaman serangan siber yang terus berkembang, seperti *SQL Injection*, *Brute Force*, dan *Denial of service (DoS)*. Ancaman tersebut adalah salah satu kerentanan yang dapat mengeksploitasi celah keamanan pada website dan berdampak pada kebocoran data,gangguan layanan, bahkan menurunkan kepercayaan publik terhadap institusi.

Permasalahan utama yang dihadapi saat ini adalah belum adanya sistem deteksi dan monitoring keamanan siber secara real time pada website jurusan. Yang menjadikan website rentan terhadap serangan yang dapat terjadi kapan saja tanpa terdeteksi secara cepat dan tepat. Ketiadaan sistem deteksi dini juga menyebabkan keterlambatan dalam penanganan insiden keamanan, sehingga potensi kerusakaan

bisa menjadi lebih besar. Sebagai solusi, penggunaan sistem keamanan berbasis open source seperti *Wazuh* menjadi pilihan yang relevan dan efisien.

Wazuh memiliki kapabilitas sebagai *Host based Intrusion Detection System (HIDS)* dan *SIEM (Security Information and Event Management)* yang mampu mendeteksi aktivitas mencurigakan, menganalisis log secara real time, serta memberikan notifikasi kepada administrator. Namun demikian, efektivitas dari implementasi sistem ini pada skala institusi pendidikan, khususnya dalam konteks website jurusan, masih perlu dianalisis secara mendalam.

Oleh karena itu, permasalahan yang akan diteliti yaitu bagaimana merancang dan menerapkan sistem deteksi dini serangan siber menggunakan *Wazuh* pada website melalui deteksi dan respon terhadap ancaman secara real-time. Permasalahan ini dianggap mendesak untuk diselesaikan mengingat urgensinya dalam menjaga kontinuitas layanan informasi dan membangun ketahanan digital institusi.

1.3 Batasan Masalah

Pada penelitian ini terdapat beberapa batasan yaitu antara lain:

1. Objek penelitian difokuskan pada Website Jurusan Teknik Informatika Politeknik Negeri Bengkalis sebagai target pengujian keamanan.
2. Sistem deteksi dini yang diterapkan menggunakan *Wazuh* sebagai *Security Information and Event Management* (SIEM) berbasis open-source
3. Lingkungan pengujian dilakukan pada server berbasis Ubuntu Server dengan arsitektur *Wazuh* Manager dan *Wazuh* Agent.
4. Jenis serangan yang dilakukan pada penelitian ini seperti:
    a. Serangan Denial of service (DoS)
    b. Serangan brute force pada layanan autentikasi
    c. Serangan SQL injection pada form input website
5. Penelitian hanya berfokus pada proses deteksi dan notifikasi serangan, bukan pada tahap pencegahan atau hardening sistem.
6. Visualisasi hasil deteksi dilakukan melalui:
    a. Dashboard *Wazuh*

b. Dashboard kustom berbasis web

7. Sistem notifikasi dibatasi pada integrasi Telegram sebagai media peringatan serangan real-time
8. Penelitian tidak membahas aspek forensik digital lanjutan, pemulihan sistem, maupun analisis malware secara mendalam.

1.4 Tujuan

Penelitian ini bertujuan untuk :

1. Menerapkan sistem deteksi dini serangan siber berbasis *wazuh* pada website Jurusan Teknik Informatika.
2. Menganalisis kemampuan *wazuh* dalam mendeteksi dini serangan siber terhadap website Teknik Informatika.

1.5 Manfaat

Manfaat dari penelitian ini :

1. Penelitian ini diharapkan dapat memberikan peningkatkan keamanan website Jurusan Teknik Informatika. Dengan menerapkan sistem deteksi dini menggunakan *wazuh*, sehingga website dapat beroperasi dengan lebih aman dan efisien.
2. Penelitian ini diharapkan dapat mendorong adopsi solusi keamanan informasi berbasis open source yang berkelanjutan dilingkungan pendidikan tinggi vokasi yang tercipta ekosistem keamanan informasi yang adaptif dan sadar risiko dalam menghadapi ancaman digital di era transformasi digital
3. Penelitian ini diharapkan bisa memberikan gambaran konkret mengenai penerapan sistem IDS dan Siem berbasis open source, sehingga dapat menjadi studi kasus atau bahan praktikum dalam mata kuliah keamanan jaringan, sistem informasi, dan administrasi server.
4. Penelitian ini menjadi referensi dalam mengintergrasikan sistem keamanan ke dalam siklus pengembangan website. Pengembang dapat memahami pentingnya sistem monitoring log dan respons otomatis terhadap potensi ancaman keamanan.