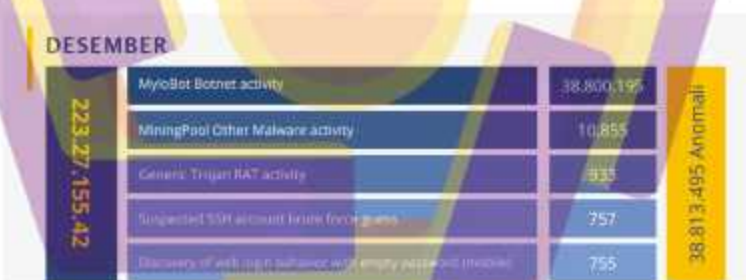
BAB I
PENDAHULUAN

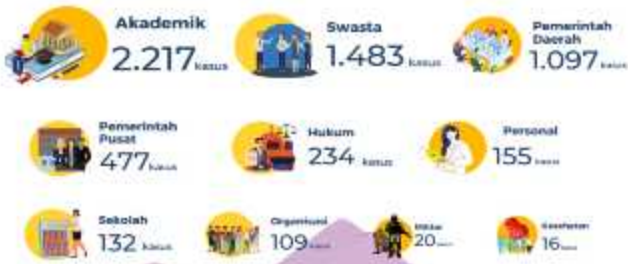
1.1 Latar Belakang

Teknologi dalam dunia siber terus berkembang dengan pesat. Hal ini diikuti dengan semakin besarnya ancaman siber seperti serangan malware yang dapat menyerang penggunanya. Dari data hasil konferensi pers BSSN pada senin tanggal 7 Maret 2022, Letjen TNI (Purn) Hinsa Siburian menyatakan bahwa hasil dari monitoring BSSN tercatat lebih dari 1,6 miliar anomali trafik/serangan siber[1]. Anomali terbanyak yang dicatat oleh BSSN yaitu Mylobot Botnet, PROTOCOL-SCADA Moxa, MiningPool, Win Trojan Zeroaccess, Discover Using Socks Agent, CVE-2017-0147, Win Trojan Allaple, Rdp Brute Force, Generic Trojan Rat, dan ISC Bind Dos[2]. Pada laporan monitoring tahunan BSSN 2021 dibulan desember tercatat anomali terbanyak yaitu anomali MyloBot Botnet activity yang mencapai 38.813.495 anomali per bulan sesuai Gambar 1.1.



Gambar 1. 1 Anomali Pada Desember 2021[2]

Selain serangan malware, serangan phising dan web defacement juga termasuk serangan terbanyak yang terjadi pada tahun 2021 menurut laporan tahunan *monitoring* dari BSSN[2]. Dampak yang dihasilkan serangan tersebut cukup besar khususnya pada lembaga akademik yang mencapai 2.217 kasus, sedangkan kasus terbanyak lainya berdampak pada lembaga swasta 1.483 kasus sesuai Gambar 1.2.



Gambar 1. 2 Kasus Web Defacement[2]

Sementara itu diberitakan dari bleepingcomputer.com ransomware conti berhasil membobol Bank Indonesia dan membocorkan datanya[3]. Dari berita diatas disimpulkan pentingnya untuk menjaga kemanan sebuah sistem dan website. Salah satu solusi yaitu dengan menganalisis log untuk mengetahui serangan dan peristiwa yang terjadi didalam sistem. Namun hal tersebut akan memakan banyak waktu jika membaca log satu-persatu sehingga cara tersebut tidak efisien dan memperlambat penanganan saat insiden keamanan terjadi. *Security Information and Event Management* (SIEM) adalah salah satu solusi keamanan yang dapat mendeteksi serangan dan memvisualisasikan data hasil serangan agar mudah dianalisis[4]. Karena sistem SIEM memiliki *intrusion detection system* (IDS) yang mampu mendeteksi dan memonitoring serangan, hal tersebut dapat mempercepat penanganan pada sistem yang menerapkan SIEM.

SIEM terdiri dari dua komponen diantaranya adalah SIM (*Security Information Management*) dan SEM (*Security Event Management*) yaitu SIM bekerja untuk mengumpulkan seperti log aktivitas dan juga serangan, dan SEM bekerja untuk pemantauan peristiwa secara *real-time*[5]. SIEM bekerja mengumpulkan, mengatur, dan menganalisis aktivitas terkait keamanan dari berbagai sumber perangkat keras *(hardware)* dan perangkat lunak *(software)* di seluruh sistem. Tujuan utama SIEM adalah keamanan, namun banyak perusahaan menggunakan SIEM untuk *compliance* (kepatuhan) terhadap undang-undang dan standar perlindungan data seperti NIST, GDPR, HIPAA, PCI-DSS, dan SOX[6].

Wazuh adalah salah satu tool atau aplikasi dari sumber terbuka (*open source*) yang bekerja layaknya sebuah SIEM dan sudah dilengkapi oleh IT compliance yang berguna sebagai data bukti kepatuhan yang didapat dari hasil analisis log aktivitas di sebuah sistem[7]. Cara kerja Wazuh yaitu memantau *endpoint* seperti komputer desktop, server, sampai virtual machine yang terkoneksi pada host Wazuh. OSSEC adalah IDS/IPS yang di gunakan Wazuh sebagai alat memantau dan deteksi juga sebagai pencegahan saat adanya serangan yang masuk ke sistem.

Mendeteksi serangan dan menemukan kerentanan adalah hal penting, namun memperkirakan risiko dari serangan yang dideteksi adalah hal yang sama pentingnya. OWASP *risk rating assessment* adalah sebuah metode untuk menilai risiko serangan secara keseluruhan. Hasil yang akan didapat dengan menggunakan metode OWASP *risk rating assessment* yaitu dengan cara mengkalikan faktor kemungkinan dan faktor dampak untuk mendapatkan hasil risiko keseluruhan[8].

Berdasarkan permasalahan diatas maka peneliti membuat sebuah topik penelitian yang berjudul ***"Implementasi Wazuh Untuk Mendeteksi Serangan Pada Endpoint Berbantuan OWASP Risk Rating Assessment Sebagai Penilaian Risiko Serangan"***. Judul tersebut dipilih karena keamanan pada *endpoint* termasuk bagian penting dalam suatu sistem untuk menjaga tiga pilar yaitu CIA (*confidentiality, integrity, and availability*). Memilih metode OWASP *risk rating assessment* sebagai penilaian tingkat risiko dikarenakan OWASP adalah standar keamanan sebuah web app dunia dan sudah memiliki metode untuk menilai log serangan untuk memperkirakan dampak risiko dari serangan.

1.2 Rumusan Masalah

Untuk memperjelas dan mengarahkan penelitian ini agar hasil yang di dapat sesuai dengan yang diharapkan, maka masalah yang ada dapat dirumuskan adalah:

1. Bagaimana cara mengidentifikasi serangan cross site scripting (XSS), directory traversal, SQL injection, brute force dan DDoS pada waazuh?
2. Termasuk dalam kategori apa saja risiko serangan yang terdeteksi oleh

wazuh yang dinilai menggunakan metode OWASP *risk rating assessment*?

1.3 Batasan Masalah

Adapun batasan masalah yang bertujuan untuk memfokuskan pembahasan dalam penelitian ini adalah:

a. Penelitian ini hanya dilakukan menggunakan *virtual environment*.
b. Penelitian ini menggunakan sistem operasi ubuntu sebagai wazuh server.
c. Penelitian ini menggunakan sistem operasi fedora sebagai *vulnerable machine* dan berperan sebagai objek penelitian.
d. Penlitian ini menggunakan sistem operasi kali linux yang berperan sebagai penyerang.
e. Penelitian ini hanya menggunakan wazuh untuk mendeteksi anomali serangan yang diujikan pada objek penelitian yang sudah terintegrasi menjadi wazuh agent.
f. Penelitian ini hanya melakukan serangan XSS, SQL injection, directory traversal, DDoS, dan brute force.
g. Penelitian ini hanya melakukan penambahan rule jika diperlukan atau wazuh server tidak dapat mengidentifikasi serangan.
h. Penelitian ini menggunakan metode OWASP *risk rating assessment* hanya untuk melakukan penilaian tingkat risiko pada serangan yang dianalisis tidak sampai pada tahap menentukan perbaikan dan faktor pembobotan.
i. Penelitian ini hanya melakukan simulasi serangan tanpa adanya recovery sistem yang dilakukan penyerangan.

1.4 Tujuan Penelitian

Tujuan yang ingin diraih pada penelitian ini yaitu:

1. Mengidentifikasi serangan cross site scripting (XSS), directory traversal, SQL injection, brute force dan DDoS yang terdeteksi wazuh.
2. Mengetahui kategori tingkat risiko serangan yang terdeteksi oleh wazuh menggunakan metode OWASP *risk rating assessment*.

1.5 Manfaat Penelitian

Manfaat penelitian ini yaitu sebagai salah satu *security solution* untuk mendeteksi dan memanajemen serangan dengan memvisualisasikan data agar lebih mudah dianalisis.

1.6 Sistematika Penulisan

Dalam penelitian ini, penulis disajikan dalam lima bab dengan sistematika pembahasan sebagai berikut:

Bab I Pendahuluan

Bab ini berisi tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

Bab II Landasan Teori

Bab ini berisi tentang teori-teori pemecahan masalah yang berhubungan dan digunakan untuk mendukung penulisan penelitian ini.

Bab III Metodologi Penelitian

Bab ini berisi alur penelitian, metode penelitian, objek penelitian, serta alat dan bahan yang digunakan untuk penelitian.

Bab IV Pembahasan

Bab ini berisi tentang pembuatan environment virtual untuk membuat sistem SIEM dari wazuh, implementasi SIEM, pengujian sistem, dan berisi penilaian log serangan menggunakan OWASP *risk rating Assessment*.

Bab V Penutup

Bab ini berisi tentang kesimpulan dari pembahasan penelitian, hasil akhir penelitian dan saran.

DAFTAR PUSTAKA

Pada bagian ini akan dipaparkan tentang sumber-sumber yang digunakan dalam penulisan penelitian ini.