IMPLEMENTASI WAZUH UNTUK MENDETEKSI SERANGAN PADA ENDPOINT BERBANTUAN OWASP RISK RATING ASSESSMENT SEBAGAI PENILAIAN RISIKO SERANGAN

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer

disusun oleh

KUMARA PRAYOGA

17.83.0099

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2022

IMPLEMENTASI WAZUH UNTUK MENDETEKSI SERANGAN PADA ENDPOINT BERBANTUAN OWASP RISK RATING ASSESSMENT SEBAGAI PENILAIAN RISIKO SERANGAN

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer

disusun oleh

KUMARA PRAYOGA

17.83.0099

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2022

HALAMAN PERSETUJUAN

SKRIPSI

IMPLEMENTASI WAZUH UNTUK MENDETEKSI SERANGAN PADA ENDPOINT BERBANTUAN OWASP RISK RATING ASSESSMENT SEBAGAI PENILAIAN RISIKO SERANGAN

yang disusun dan diajukan oleh

Kumara Prayoga

17.83.0099

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 23 Agustus 2022

Dosen Pembimbing,

Banu Santoso, S.T., M.Eng
NIK. 190302327

HALAMAN PENGESAHAN

SKRIPSI

IMPLEMENTASI WAZUH UNTUK MENDETEKSI SERANGAN PADA ENDPOINT BERBANTUAN OWASP RISK RATING ASSESSMENT SEBAGAI PENILAIAN RISIKO SERANGAN

yang disusun dan diajukan oleh

Kumara Prayoga

17.83.0099

Telah dipertahankan di depan Dewan Penguji
pada tanggal 23 Agustus 2022

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Andika Agus Slameto, M.Kom **NIK. 190302109**	
Lukman, S.Kom., M.Kom **NIK. 190302151**	
Banu Santoso, S.T., M.Eng **NIK. 190302327**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 23 Agustus 2022

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Kumara Prayoga
NIM : 17.83.0099

Menyatakan bahwa Skripsi dengan judul berikut:

Implementasi Wazuh Untuk Mendeteksi Serangan Pada Endpoint Berbantuan Owasp Risk Rating Assessment Sebagai Penilaian Risiko Serangan

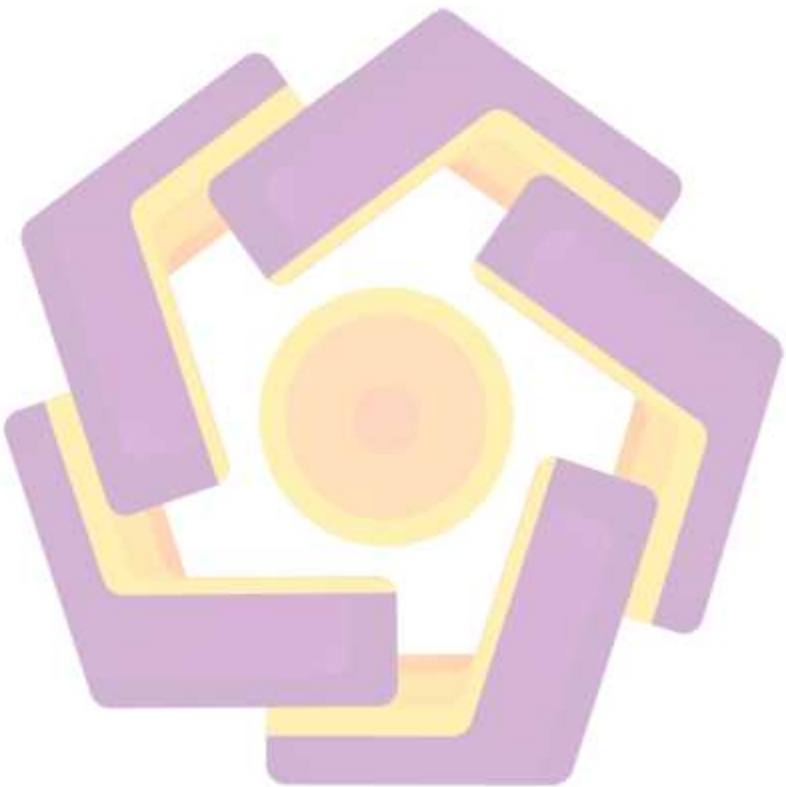
Dosen Pembimbing: Banu Santoso, S.T., M.Eng

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 23 Agustus 2022

Yang Menyatakan,

Kumara Prayoga



HALAMAN PERSEMBAHAN

Dengan segala puji dan syukur kepada Tuhan yang Maha Esa dan atas dukungan dan doa dari orang-orang tercinta, akhirnya skripsi ini dapat diselesaikan dengan baik. Oleh karena itu, dengan rasa bangga dan bahagia saya haturkan rasa syukur dan terima kasih saya kepada:

1. Allah SWT, Tuhan Yang Maha Esa karena hanya atas izin dan karunia-Nyalah, maka skripsi ini dapat dibuat dan selesai pada waktunya. Puji syukur yang tak terhingga pada Tuhan semesta alam yang meridhoi dan mengabulkan segala doa.
2. Orang tua saya, yang tidak pernah lelah memberikan saya dukungan dan doa. Untuk Ibu yang tidak pernah lelah dalam memberikan semangat supaya saya bisa menyelesaikan skripsi ini dan untuk Bapak yang telah banyak memberikan begitu banyak pengorbanan yang tidak bisa saya balaskan. Terimakasih banyak saya ucapkan untuk keduanya.
3. Dosen Pembimbing skripsi bapak Banu Santoso, S.T., M.Eng selaku dosen pembimbing saya, saya sangat berterimakasih atas bimbingannya selama ini yang telah memberikan masukan, kritik dan saran yang membangun agar menjadi lebih baik lagi untuk kedepannya. serta seluruh jajaran dosen Universitas Amikom Yogyakarta yang sudah membagikan ilmunya saya mengucapkan terimakasih, semoga ilmu dari bapak dan ibu dosen bisa saya amalkan ke yang lain juga.
4. Seluruh teman dan sahabat khususnya Misbachul Munir, Ipung Ardiansah, Muhammad Rasyid Maulana, Cadipa Sidiq, Ahmad Ristanto dan Iffatun Nadya.

Terimakasih yang sebesar-besarnya untuk kalian semua, akhir kata saya persembahkan skripsi ini untuk kalian semua, orang-orang yang telah memberikan pengalaman yang sangat berarti dalam hidup saya. Semoga skripsi ini dapat bermanfaat dan berguna untuk kemajuan ilmu pengetahuan di masa yang akan datang.

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT yang selalu melimpahkan rahmat serta hidayah-Nya kepada setiap hamba-Nya. Skripsi ini disusun sebagai salah satu syarat kelulusan Program Strata 1 Program Studi Teknik Komputer, Universitas AMIKOM Yogyakarta dan untuk memperoleh gelar Sarjana Komputer (S.Kom).

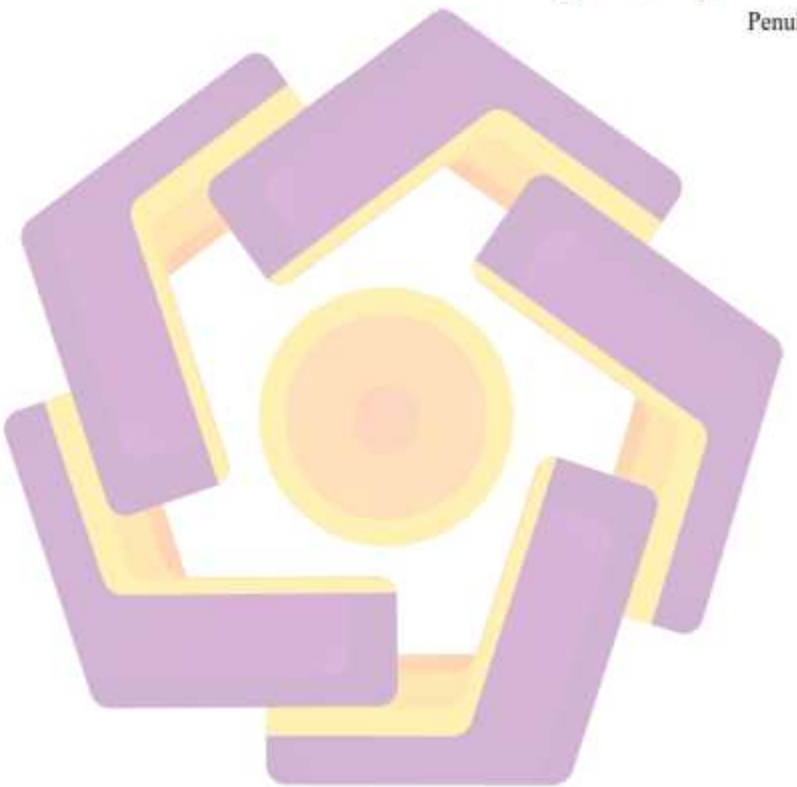
Dengan selesainya skripsi yang berjudul ***"Implementasi Wazuh Untuk Mendeteksi Serangan Pada Endpoint Berbantuan OWASP Risk Rating Assessment Sebagai Penilaian Risiko Serangan"***, dengan ini penyusun ingin mengucapkan terima kasih kepada:

1. Allah SWT atas rahmat, hidayah, serta karunia-Nya yang telah diberikan kepada penulis sehingga skripsi ini dapat terselesaikan.
2. Prof. Dr. M. Suyanto, MM selaku rektor Universitas AMIKOM Yogyakarta
3. Hanif Al Fatta, S.Kom., M.Kom selaku Dekan Fakultas Ilmu Komputer dan Ketua Program Studi S1 Sistem Informasi.
4. Bapak Dony Ariyus, M.Kom selaku Ketua Program Studi S1 Teknik Komputer Universitas AMIKOM Yogyakarta.
5. Kedua orang tua, yang selalu memberikan dukungan baik materi maupun doa.
6. Bapak Banu Santoso, S.T., M.Eng selaku dosen pembimbing yang tidak bosan memberikan arahan, saran dan motivasi agar penulis bisa mengerjakan naskah ini dengan baik dan benar.
7. Bapak dan Ibu dosen Universitas AMIKOM Yogyakarta yang telah memberikan ilmunya selama penulis kuliah.
8. Keluarga besar kelas S1 Teknik Komputer 02 angkatan 2017.

Akhirnya dengan kerendahan hati penulis mengucapkan terimakasih dan semoga skripsi ini dapat bermanfaat bagi penulis maupun pembaca.

Yogyakarta, 23 Agustus 2022

Penulis



DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Semakin pesatnya kemajuan teknologi khususnya dalam dunia siber, semakin banyak pula ancaman serangan siber yang dapat merugikan penggunanya. Sehingga mengancam tiga pilar keamanan informasi yaitu *Confidentiality, Integrity*, dan *Availability* (CIA). *Security Information and Event Management* (SIEM) adalah suatu kontrol keamanan yang dapat mendeteksi serangan, *monitoring* secara *real-time* dan memvisualisasikan serangan, sehingga mudah analisis dan mempercepat penanganan saat terjadinya serangan.

Dengan menggunakan wazuh yang diimplementasikan sebagai SIEM untuk mendeteksi dan mengidentifikasi serangan, dan menganalisis data hasil serangan menggunakan metode OWASP *risk rating assessment* sebagai penilaian risiko secara keseluruhan. Pengujian dilakukan dengan menyerang *endpoint* yang sudah terpasang website yang terintegrasi sebagai wazuh agent.

Hasilnya, wazuh dapat mendeteksi dan mengidentifikasi semua serangan yaitu serangan XSS, directory traversal, SQL injection, brute force, dan DDoS. Sedangkan penilaian serangan menggunakan OWASP *risk rating assessment* mendapatkan 2 kategori, yaitu *High* untuk serangan XSS, directory traversal, SQL injection dan DDoS, sedangkan kategori risiko *Medium* untuk serangan brute force.

Kata kunci: SIEM, Wazuh, CIA, OWASP risk rating assessment, Endpoint

ABSTRACT

The more rapid technological advances, especially in the cyber world, the more threats of cyber attacks that can harm users. This threatens the three pillars of information security, namely Confidentiality, Integrity, and Availability (CIA). Security Information and Event Management (SIEM) is a security control that can detect attacks, monitor real -time and visualize attacks, making it easy to analyze and speed up handling when an attack occurs.

By using wazuh which is implemented as a SIEM to detect and identify attacks, and analyze data resulting from attacks using the OWASP risk rating assessment as an overall risk assessment. The test is carried out by attacking endpoints that have an integrated website installed as a wazuh agent.

As a result, wazuh can detect and identify all attacks, namely XSS attacks, directory traversal, SQL injection, brute force, and DDoS. While the attack assessment using the OWASP risk rating assessment gets 2 categories, namely High for XSS attacks, directory traversal, SQL injection and DDoS, and Medium for brute force attacks.

Keywords: SIEM, Wazuh, CIA, OWASP risk rating assessment