TUGAS AKHIR
SKEMA MAGANG

PENGUJIAN WAZUH DALAM MENDETEKSI SERANGAN DOS DAN BRUTE FORCE PADA WINDOWS SERVER

MUHAMMAD NOOR CHOLIS MAJID

NIM : 215610084

PROGRAM STUDI SISTEM INFORMASI

PROGRAM SARJANA

FAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS TEKNOLOGI DIGITAL INDONESIA

YOGYAKARTA

2025

TUGAS AKHIR
SKEMA MAGANG

PENGUJIAN WAZUH DALAM MENDETEKSI SERANGAN DOS DAN BRUTE FORCE PADA WINDOWS SERVER

Diajukan sebagai salah satu syarat untuk menyelesaikan studi pada
Program Sarjana
Program Studi Sistem Informasi
Fakultas Teknologi Informasi
Universitas Teknologi Digital Indonesia

Disusun Oleh

MUHAMMAD NOOR CHOLIS MAJID
NIM : 215610084

PROGRAM STUDI SISTEM INFORMASI
PROGRAM SARJANA
FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS TEKNOLOGI DIGITAL INDONESIA
YOGYAKARTA
2025

HALAMAN PERSETUJUAN UJIAN TUGAS AKHIR

HALAMAN PERSETUJUAN UJIAN TUGAS AKHIR

Judul	:	Pengujian Wazuh dalam Mendeteksi Serangan DoS dan Brute Force pada Windows Server
Nama	:	Muhammad Noor Cholis Majid
NIM	:	215610084
Program Studi	:	Sistem Informasi
Program	:	Sarjana
Semester	:	Ganjil
Tahun Akademik	:	2024/2025

Telah diperiksa dan disetujui untuk diujikan
di hadapan Dewan Penguji Tugas Akhir

Yogyakarta, 17 Desember 2024

Dosen Pembimbing,

Dr. L.N. Harnaningrum, S.Si, M.T.
NIDN : 0513057101

ii

HALAMAN PENGESAHAN

HALAMAN PENGESAHAN

PENGUJIAN WAZUH DALAM MENDETEKSI SERANGAN DOS DAN BRUTE FORCE PADA WINDOWS SERVER

Telah dipertahankan di depan Dewan Penguji dan dinyatakan diterima untuk memenuhi sebagian persyaratan guna memperoleh

Gelar Sarjana

Program Studi Sistem Informasi

Fakultas Teknologi Informasi

Universitas Teknologi Digital Indonesia

Yogyakarta, 8 Januari 2025

Dewan Penguji	NIDN	Tandatangan
1. Deborah Kurniawati, S.Kom., M.Cs. (Ketua)	0511107301	.....
2. Dr. L.N. Harnaningrum, S.Si., M.T. (Sekretaris)	0513057101	.....
3. Adi Kusjani, S.T., M.Eng. (Anggota)	0515067501	.....

Mengetahui

Ketua Program Studi Sistem Informasi

Deborah Kurniawati, S.Kom, M.Cs

NPP : 051149

iii

PERNYATAAN KEASLIAN TUGAS AKHIR

PERNYATAAN KEASLIAN TUGAS AKHIR

Dengan ini saya menyatakan bahwa naskah Tugas Akhir ini belum pernah diajukan untuk memperoleh gelar sarjana di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara sah diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 17 Desember 2024

Muhammad Noor Cholis Majid
NIM: 215610084

HALAMAN PERSEMBAHAN

Dengan penuh rasa syukur dan terima kasih, tugas akhir ini saya persembahkan kepada:

1. Allah SWT, yang senantiasa memberikan petunjuk, rahmat, dan kemudahan dalam setiap langkah hidup ini, sehingga tugas akhir ini dapat terselesaikan dengan baik.
2. Kedua orang tua tercinta, yang tidak pernah lelah memberikan doa, dukungan, dan motivasi tiada henti. Kasih sayang dan pengorbanan kalian adalah sumber kekuatan terbesar yang membawa saya sampai pada titik ini.
3. Ibu Dosen Pembimbing, L.N. Harnaningrum, Dr., S.Si, M.T., yang dengan sabar memberikan bimbingan, arahan, dan nasihat, sehingga tugas akhir ini dapat terselesaikan dengan baik.
4. Teman-teman seperjuangan, yang senantiasa memberikan semangat, dukungan, dan kebersamaan, sehingga saya terus termotivasi untuk menyelesaikan tugas akhir ini.
5. Diri sendiri, terima kasih telah bertahan, bekerja keras, dan tidak menyerah, sehingga mampu menghadapi semua tantangan hingga tugas akhir ini terselesaikan.

PRAKATA

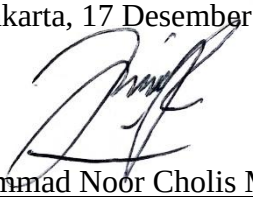
Dengan menyebut nama Allah yang Maha Pengasih lagi Maha Penyayang, segala puji dan syukur penulis panjatkan atas rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan tugas akhir yang berjudul "Pengujian Wazuh dalam Mendeteksi Serangan DoS dan Brute Force pada Windows Server" ini dengan baik.

Tugas akhir ini disusun sebagai syarat kelulusan program Sarjana Sistem Informasi di Universitas. Penulis menyadari bahwa tanpa dukungan dan bantuan dari berbagai pihak, tugas akhir ini tidak akan terselesaikan. Oleh karena itu, dengan segala hormat, penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Allah SWT: Terima kasih atas kesehatan dan petunjuk-Nya. Dengan rahmat dan hidayah-Nya, saya dapat menyelesaikan laporan ini tepat waktu.
2. Keluarga: Terima kasih kepada ayah, ibu, dan kakak yang memberikan kasih sayang, semangat, doa, dan dukungan tanpa henti.
3. Pembimbing Akademik: Terima kasih kepada Ibu L.N. Harnaningrum, Dr., S.Si., M.T., selaku Pembimbing Akademik MBKM Mandiri. Bimbingan dan arahan beliau sangat membantu dalam menyelesaikan laporan ini.
4. Mentor PT. Dua Empat Tujuh: Terima kasih kepada Kak Risma Diyah Pramesti, selaku mentor PT. Dua Empat Tujuh, yang selalu memberikan pengetahuan tambahan dan bimbingan.
5. Rekan-rekan dan teman-teman mahasiswa yang telah memberikan bantuan serta dukungan selama proses penulisan tugas akhir ini.

Semoga segala bantuan dan dukungan yang diberikan mendapatkan balasan dari Allah SWT. Akhir kata, penulis berharap semoga tugas akhir ini dapat memberikan manfaat dan kontribusi positif bagi para pembaca.

Yogyakarta, 17 Desember 2024



Muhammad Noor Cholis Majid

NIM: 215610084

DAFTAR ISI

Hal

DAFTAR GAMBAR

Hal

DAFTAR TABEL

Hal

INTISARI

Keamanan siber menjadi aspek yang sangat penting dalam menghadapi ancaman terhadap infrastruktur teknologi informasi. Penelitian ini bertujuan untuk menguji efektivitas Wazuh, sebuah platform *open-source* untuk *security information and event management* (SIEM), dalam mendeteksi serangan siber seperti *Denial of Service (DoS)* dan *Brute Force*. Uji coba dilakukan pada Windows Server 2019 sebagai *endpoint*, menggunakan integrasi Wazuh dengan Suricata untuk memperkuat deteksi ancaman berbasis jaringan serta bot Telegram untuk notifikasi real-time.

Penelitian dimulai dengan instalasi dan konfigurasi Wazuh di server utama, diikuti dengan simulasi serangan DoS menggunakan *hping3* dan serangan *Brute Force* menggunakan Hydra. Proses pengujian ini dilakukan di lingkungan virtual yang terdiri dari Ubuntu 20.04 LTS sebagai Wazuh Server, Ubuntu 20.04 LTS lainnya sebagai mesin penyerang dan Windows Server 2019 sebagai target serangan. Selama pengujian, data aktivitas jaringan dianalisis menggunakan WireShark untuk memvalidasi keberhasilan serangan, sementara log dan *alert* dari Wazuh dievaluasi melalui dashboard dan bot Telegram.

Hasil pengujian menunjukkan bahwa Wazuh berhasil mendeteksi pola serangan dengan baik. Serangan DoS terdeteksi melalui integrasi dengan Suricata, sedangkan serangan *Brute Force* berhasil diidentifikasi berdasarkan *log authentication failure* yang tercatat di dashboard Wazuh. Notifikasi real-time melalui Telegram memungkinkan administrator segera mengambil tindakan mitigasi. Penelitian ini membuktikan bahwa Wazuh memiliki kemampuan deteksi yang efektif, meskipun masih membutuhkan optimalisasi pada aturan deteksi dan integrasi sistem untuk meningkatkan respons terhadap ancaman yang lebih kompleks.

Kata kunci: *Brute Force*, DoS, Suricata, Wazuh, keamanan siber

ABSTRACT

Cybersecurity is a critical aspect in addressing threats to information technology infrastructure. This study aims to evaluate the effectiveness of Wazuh, an open-source platform for Security Information and Event Management (SIEM), in detecting cyberattacks such as Denial of Service (DoS) and Brute Force. The testing was conducted on Windows Server 2019 as an endpoint, utilizing Wazuh's integration with Suricata to enhance network-based threat detection and a Telegram bot for real-time notifications.

The research began with the installation and configuration of Wazuh on the main server, followed by simulating DoS attacks using hping3 and Brute Force attacks using Hydra. The testing was performed in a virtual environment consisting of Ubuntu 20.04 LTS as the Wazuh server, another Ubuntu 20.04 LTS machine as the attacking machine, and Windows Server 2019 as the target. During the tests, network activity data was analyzed using WireShark to validate the success of the attacks, while Wazuh logs and alerts were evaluated through its dashboard and Telegram bot notifications.

The results showed that Wazuh effectively detected attack patterns. DoS attacks were identified through Suricata integration, while Brute Force attacks were detected based on authentication failure logs recorded on the Wazuh dashboard. Real-time notifications via Telegram enabled administrators to take immediate mitigation actions. This study demonstrates that Wazuh possesses effective detection capabilities, though optimization of detection rules and system integration is still needed to enhance responsiveness to more complex threats.

***Keywords**: Brute Force, DoS, cybersecurity, Suricata, Wazuh*