UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

ANALISIS LOG SISTEM PADA SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) UNTUK MENDETEKSI SERANGAN BRUTE FORCE

SKRIPSI

CALEB SEBASTIAN
1910511116

INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

2023

LEMBAR PERNYATAAN ORISINALITAS

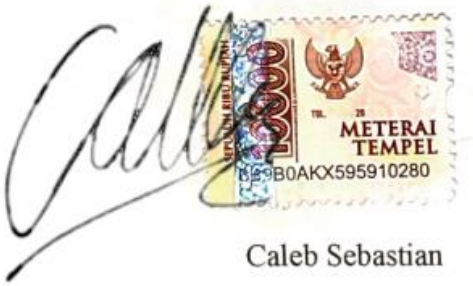
Skripsi ini adalah hasil karya sendiri dan semua sumber yang dikutip maupun ditujuk telah saya nyatakan dengan benar.

Nama	: Caleb Sebastian
NIM	: 1910511116
Program Studi	: S1 – Informatika

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 22 Januari 2024

Yang Menyatakan,



Caleb Sebastian

LEMBAR PERNYATAAN PERSETUJUAN

Yang bertanda tangan di bawah ini, saya:

Nama	: Caleb sebastian
NIM	: 1910511116
Program Studi	: S1 – Informatika
Perguruan Tinggi	: Universitas Pembangunan Nasional Veteran Jakarta
Jenis Karya Ilmiah	: Skripsi/Tugas Akhir

Dengan ini menyetujui untuk memberikan izin kepada pihak **Universitas Pembangunan NasionalVeteran Jakarta. Hak Bebas Royalti Non-Eksklusif (*Non-exclusive Royalti-Free Right*)** atas karya ilmiah kami yang berjudul:

ANALISIS LOG SISTEM PADA SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) UNTUK MENDETEKSI SERANGAN BRUTE FORCE

Dengan **Hak Bebas Royalti Non-Eksklusif** ini, **Universitas Pembangunan Nasional "Veteran"Jakarta** berhak menyimpan, mengalih-media atau *format*-kan, mengelolanya dalam *database*, mendistribusikan-nya, dan menampilkan atau mempublikasikannya di *internet* atau media lain untuk kepentingan akademis tanpa perlu meminta izin selama tetap mencantumkan nama penulis/pencipta karya ilmiah tersebut.

Demikian pernyataan ini dibuat dengan sebenarnya.

Dibuat di : Jakarta
Pada Tanggal : 22 Januari 2024
Yang menyatakan,

Caleb Sebastian

LEMBAR PENGESAHAN

Dengan ini dinyatakan bahwa Tugas Akhir berikut:

Nama : Caleb Sebastian

NIM. : 1910511116

Program Studi : S1 Informatika

Judul Skripsi/TA. : ANALISIS LOG SISTEM PADA SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) UNTUK MENDETEKSI SERANGAN BRUTE FORCE

Telah berhasil dipertahankan dihadapan Tim Penguji dan diterima sebagai bagian dari persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi S1 Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional "Veteran" Jakarta.

Dr. Widya Cholil, S.Kom., M.I.T
Penguji I

Ika Nurlaili Isnainiyah, S.Kom., M.Sc.
Penguji II

Henki Bayu Seta, S.Kom., MTI.
Dosen Pembimbing

Prof. Dr. Ir. Supriyanto, ST., M.Sc., IPM
Dekan

Dr. Widya Cholil, S.Kom., M.I.T
Ketua Program Studi

Ditetapkan ini : Jakarta

Tanggal Ujian : Rabu, 10 Januari 2024

KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Tuhan yang Mahakuasa atas segala karunianya, sehingga skripsi dengan judul "Analisis Log Sistem Pada *Security Information And Event Management* (SIEM) Untuk Mendeteksi Serangan *Brute Force*" ini berhasil diselesaikan. Skripsi ini disusun sebagai syarat kelulusan Studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta. Penulis mengakui bahwa penyusunan skripsi ini tidak akan terselesaikan tanpa dukungan dari berbagai pihak. Oleh karena itu, penulis ingin menggunakan kesempatan ini untuk mengungkapkan rasa terima kasih kepada:

1. Ibu Dr. Ermatita, M.Kom., selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta.
2. Ibu Dr. Widya Cholil, M.I.T., selaku Ketua Program Studi Sarjana Jurusan S1 Informatika.
3. Bapak Henki Bayu Seta, S.Kom., MTI., selaku Dosen Pembimbing yang telah memberikan kritik beserta saran selama penulisan skripsi ini.
4. Orang tua yang telah memberikan dukungan secara penuh secara material dan moral kepada penulis.
5. Teman – teman seperjuangan yang sudah turut membantu dan memberikan dukungan kepada penulis.

Meskipun penulis telah berupaya sebaik mungkin untuk menyelesaikan skripsi ini, penulis menyadari bahwa masih terdapat kekurangan. Oleh karena itu, penulis mengharapkan kritik dan saran yang membangun. Terakhir, penulis berharap skripsi ini dapat memberikan manfaat bagi pembaca dan pihak-pihak terkait yang memiliki kepentingan.

Jakarta, 30 November 2023

Caleb Sebastian

ABSTRAK

Serangan brute-force adalah serangan siber yang sering menargetkan protokol SSH dan RDP. Serangan ini dapat menyebabkan kerugian yang signifikan bagi organisasi. Salah satu solusi untuk mendeteksi serangan brute-force adalah dengan menggunakan Security Information and Event Management (SIEM). SIEM dapat memantau aktivitas login dan mengidentifikasi pola yang mencurigakan. Penelitian ini menggunakan Wazuh, salah satu platform SIEM open-source yang populer, untuk mendeteksi serangan brute-force yang menargetkan protokol SSH dan RDP. Hasil penelitian menunjukkan bahwa Wazuh dapat mendeteksi serangan brute-force dengan baik. Wazuh dapat memblokir alamat IP yang mencoba login dengan kata sandi yang salah berulang kali. Penelitian ini memberikan informasi yang bermanfaat bagi organisasi dalam upaya meningkatkan keamanannya dari serangan brute-force. Organisasi dapat menggunakan SIEM, seperti Wazuh, untuk mendeteksi serangan brute-force dan memberikan respons yang cepat dan tepat.

Kata Kunci: Serangan brute-force, SIEM, Wazuh, SSH, RDP

ABSTRACT

Brute-force attacks are a common type of cyber attack that target SSH and RDP protocols. These attacks can cause significant damage to organizations. One solution for detecting brute-force attacks is to use Security Information and Event Management (SIEM). SIEM can monitor login activity and identify suspicious patterns. This study uses Wazuh, a popular open-source SIEM platform, to detect brute-force attacks targeting SSH and RDP protocols. The results of the study show that Wazuh can detect brute-force attacks effectively. Wazuh can block IP addresses that attempt to log in with the wrong password repeatedly. This study provides valuable information for organizations in their efforts to improve their security against brute-force attacks. Organizations can use SIEM, such as Wazuh, to detect brute-force attacks and provide a timely response.

Keyword: Brute-force attack, SIEM, Wazuh, SSH, RDP

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR KODE