



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,

A handwritten signature in black ink is written over a yellow and blue postage stamp. The stamp features the Garuda Pancasila emblem and the text 'METERAI TEMPEL' and 'B0AKX595910280'. The signature is written in a cursive style.

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 Nasional Veteran 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 Nurhaili Isnainiyah, S.Kom., M.Sc.
Penguji II



Henki Bayu Seta, S.Kom., M.TI.
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

LEMBAR PERNYATAAN ORISINALITAS	i
LEMBAR PERNYATAAN PERSETUJUAN	ii
LEMBAR PENGESAHAN	iii
KATA PENGANTAR	iv
ABSTRAK	v
ABSTRACT	vi
DAFTAR ISI	vii
DAFTAR TABEL	x
DAFTAR GAMBAR	xi
DAFTAR KODE	xii
BAB I	1
PENDAHULUAN	1
1.1 Latar Belakang Permasalahan	1
1.2 Rumusan Masalah	4
1.3 Batasan Masalah	5
1.4 Tujuan Penelitian	5
1.5 Manfaat Penelitian.....	5
1.6 Sistematika Penulisan	6
BAB II	8
TINJAUAN PUSTAKA	8
2.1 Port Scanning.....	8
2.2 Brute Force Attack	8
2.3 RDP	9
2.4 SSH.....	10
2.5 Operating system	10
2.6 Log.....	11
2.7 Syslog	11
2.8 Security Information and Event Management.....	13
2.9 Log Management	14
2.10 Wazuh.....	14
2.11 Hydra.....	14
2.12 Penelitian Terkait.....	15
BAB III	19

METODOLOGI PENELITIAN	19
3.1 Tahapan Penelitian	19
3.1.1 Identifikasi Masalah	19
3.1.2 Studi Literatur	20
3.1.3 Perancangan Topologi.....	20
3.1.4 Implementasi	22
3.1.5 Hasil	23
3.2 Perangkat Penelitian	23
3.3 Jadwal Penelitian	23
BAB IV	25
HASIL DAN PEMBAHASAN	25
4.1 Topologi	25
4.2 Topologi Pemantauan	26
4.2.1 Wazuh Indexer.....	26
4.2.2 Wazuh Server	31
4.2.3 Wazuh Dashboard	32
4.2.4 Wazuh Agent.....	35
4.3 Konfigurasi Target.....	37
4.3.1 Target Pertama (Windows 10).....	37
4.3.2 Target Kedua (CentOS 8)	38
4.4 Topologi Penyerangan	38
4.5 Penyerangan <i>Brute-Force</i>	39
4.6 Fitur dan Hasil Pemantauan.....	44
4.6.1 Fitur-Fitur Wazuh	44
□ Manajemen dan Analisis <i>Log</i>	45
□ Pemantauan Integritas File (FIM)	46
□ Manajemen Kerentanan (<i>Vulnerability</i>)	46
□ Deteksi Ancaman dan Respon Insiden.....	47
□ Dukungan Kepatuhan dan Regulasi	48
□ <i>Container Security</i>	49
4.6.2 Hasil Pemantauan - <i>Vulnerability</i>	50
4.6.3 Hasil Pemantauan - Manajemen dan Analisis Log Serangan <i>Brute-Force</i> RDP (Windows 10).....	54
4.6.4 Hasil Pemantauan - Manajemen dan Analisis Log Serangan <i>Brute-Force</i> SSH (CentOS 8).....	56
4.6.5 Hasil Pemantauan – Kinerja Manajemen dan Analisis <i>Log</i>	57

BAB V	61
KESIMPULAN	61
5.1 KESIMPULAN	61
5.2 SARAN	62
DAFTAR PUSTAKA	64
LAMPIRAN	67
RIWAYAT HIDUP	79

DAFTAR TABEL

Tabel 2.1 Facility Code diadaptasi dari sumber :(What Is Syslog Server and Its Working ? - GeeksforGeeks, n.d.).....	12
Tabel 2.2 Severity Level diadaptasi dari sumber : (What Is Syslog Server and Its Working ? - GeeksforGeeks, n.d.).....	12
Tabel 3.1 Jadwal Pelaksanaan Maret 2023 - Juli 2023	23
Tabel 3.2 Jadwal Pelaksanaan Agustus 2023 - Desember 2023	24

DAFTAR GAMBAR

Gambar 1.1 Jumlah serangan RDP brute-force sepanjang H1 2022.....	2
Gambar 1.2 Statistik serangan brute-force terhadap protokol SSH.....	3
Gambar 2.1 Format pesan syslog diadaptasi dari sumber : (What Is Syslog Server and Its Working ? - GeeksforGeeks, n.d.).....	11
Gambar 2.2 Arsitektur SIEM.....	14
Gambar 3.1 Kerangka Berpikir.....	19
Gambar 3.2 Rancangan Serangan Brute Force.....	21
Gambar 3.3 Rancangan Topologi Pemantauan.....	22
Gambar 4.1 Topologi Pengujian.....	25
Gambar 4.2 Config .yaml.....	27
Gambar 4.3 Username dan Password Wazuh Dashboard.....	29
Gambar 4.4 Alamat IP Wazuh Server.....	30
Gambar 4.5 Halaman Login Wazuh Dashboard.....	34
Gambar 4.6 Halaman Utama Wazuh Dashboard.....	34
Gambar 4.7 Halaman Agents Wazuh Dashboard.....	35
Gambar 4.8 Deploy Agent (1).....	36
Gambar 4.9 Deploy Agent (2).....	36
Gambar 4.10 Deploy Agent (3).....	37
Gambar 4.11 Bukti Agent aktif.....	37
Gambar 4.12 Gambar Username dan Password Win.10.....	38
Gambar 4.13 Perincian Versi Ubuntu Server.....	38
Gambar 4.14 Manajemen dan Analisis Log.....	45
Gambar 4.15 Pemantauan Integritas File (FIM).....	46
Gambar 4.16 Manajemen Kerentanan (Vulnerability).....	47
Gambar 4.17 Deteksi Ancaman dan Respon Insiden.....	48
Gambar 4.18 Dukungan Kepatuhan dan Regulasi.....	49
Gambar 4.19 Container Security.....	50
Gambar 4.20 Tampilan Halaman Vulnerabilities.....	51
Gambar 4.21 Laporan Serangan Brute-Force RDP (1).....	54
Gambar 4.22 Laporan Serangan Brute-Force RDP (2).....	54
Gambar 4.23 Laporan Serangan Brute-Force SSH (1).....	56
Gambar 4.24 Laporan Serangan Brute-Force SSH (2).....	56
Gambar 4.25 Log dalam bentuk user-friendly interface.....	57

DAFTAR KODE

Kode 4.1 Pengunduhan Komponen Pemasangan Wazuh	26
Kode 4.2 Generate Cluster Key.....	28
Kode 4.3 Pemasangan Wazuh Indexer.....	28
Kode 4.4 Menunjukkan Password Admin Wazuh	29
Kode 4.5 Template Perintah Test Wazuh Indexer	29
Kode 4.6 Melakukan Tes Wazuh Indexer.....	30
Kode 4.7 Pemasangan Wazuh Server	31
Kode 4.8 Pemasangan Wazuh Dashboard.....	32
Kode 4.9 Pemeriksaan Komponen Wazuh.....	32
Kode 4.10 Script Blokade IP Penyerang.....	35
Kode 4.11 Pemasangan Hydra	38
Kode 4.12 Perintah Brute-Force SSH	40
Kode 4.13 Perintah Brute-Force RDP.....	42