



**ANALISIS LOG SISTEM PADA SECURITY INFORMATION AND
EVENT MANAGEMENT UNTUK MENDETEKSI SERANGAN DDOS**

SKRIPSI

GEDE ANGGA WIDYA PUTRA

1910511063

INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

JAKARTA

2022

LEMBAR PENGESAHAN

LEMBAR PENGESAHAN

Dengan ini dinyatakan bahwa Tugas Akhir berikut:

Nama : Gede Angga Widya Putra
NIM : 1910511063
Program Studi : S1 Informatika
Judul : Analisis Log Sistem Pada Security Information And Event Management Untuk Mendeteksi Serangan DDOS


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. Widva Cholil, M.I.T)
Penguji I


(Anita Muliawati, S.Kom., M.TI.)
Penguji II


(Henki Bayu Seta, S.kom, M.TI.)
Dosen Pembimbing


(Dr. Ermatita, M.Kom.)
Dekan Fakultas Ilmu Komputer


(Dr. Widva Cholil, M.I.T)
Ketua Program Studi

Ditetapkan di : Jakarta
Tanggal Persetujuan : 11 Juli 2023



PERNYATAAN ORISINALITAS

PERNYATAAN ORISINALITAS

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

Nama : Gede Angga Widya Putra

NIM : 1910511063

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, 05 Juni 2023

Yang Menyatakan,



(Gede Angga Widya Putra)

ABSTRAK

Salah satu bidang teknologi yang berkembang pesat saat ini adalah Teknologi Informasi dan Komunikasi. Bentuk kemajuan teknologi informasi dan komunikasi yang seringkali kita jumpai dalam kehidupan sehari-hari adalah Internet (Interconnected Network). Melalui internet berbagai individu maupun organisasi dapat saling bertukar informasi. Namun, peningkatan tersebut juga berbanding lurus dengan munculnya berbagai macam celah keamanan yang seringkali dimanfaatkan oleh para penjahat elektronik untuk mendapatkan keuntungan finansial. Hal ini dapat dilihat dari banyaknya kasus serangan DDoS pada organisasi. Serangan Distributed Denial of Service dilakukan dengan membanjiri server atau host yang mengakibatkan host korban kehabisan sumber daya untuk melayani pengguna lain. Untuk mengatasi hal tersebut, penulis menggunakan Security Information and Event Management (SIEM). SIEM merupakan sebuah metode untuk melakukan monitoring, analisa, memberikan peringatan serta automasi respon terhadap suatu insiden. Penelitian ini diharapkan mampu menjelaskan hasil pengujian, analisis serta solusi mengenai masalah serangan DDoS pada SIEM.

Kata kunci : Log, Security Information and Event Management, DDoS

ASBTRACT

One area of technology that is growing rapidly today is information and communication technology. The form of advances in information and communication technology that we often encounter in everyday life is the Internet (Interconnected Network). Through the internet, various individuals and organizations can exchange information with each other. However, this increase is also directly proportional to the emergence of various kinds of security holes that are often exploited by electronic criminals to gain financial gain. This can be seen from the number of cases of DDoS attacks on organizations. Distributed Denial of Service attacks are carried out by flooding a server or host, causing the victim host to run out of resources to serve other users. To overcome this, the author uses Security Information and Event Management (SIEM). SIEM is a method for monitoring, analyzing, giving warnings and automating responses to incidents. This research is expected to be able to explain the results of testing, analysis, and solutions regarding the problem of DDoS attacks on SIEM.

Keyword : Log, Security Information and Event Management, DDoS

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas segala karunia-Nya Penulis dapat menyelesaikan pengerjaan Skripsi ini. Dengan ini penulis menyadari bahwa banyak pihak yang telah memberi dukungan serta bantuan selama proses pengerjaan Skripsi ini, oleh sebab itu dengan penuh rasa hormat Penulis ingin mengucapkan terima kasih kepada :

1. Tuhan Yang Maha Esa, yang sudah memberikan kesehatan, kekuatan, serta kemudahan kepada penulis dalam menyelesaikan skripsi ini.
2. Kedua Orang Tua penulis dan seluruh keluarga besar penulis yang selalu memberikan dukungan, doa, serta semangat untuk menyelesaikan Skripsi.
3. Bapak Henki Bayu Seta, S.Kom, MTI. Selaku dosen pembimbing yang selama ini telah membantu dan memberikan saran, semangat, dan masukan yang sangat bermanfaat dalam pengerjaan Skripsi ini.
4. Ibu Dr. Ermatita, M.Kom. Selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta.
5. Bapak Hamonangan Kinantan Prabu, M.T. dan Bapak Ing. Artambo Benjamin Pangaribuan, M. Eng Selaku dosen pembimbing akademik.
6. Bapak/Ibu seluruh dosen Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta yang telah memberikan ilmu-ilmu yang bermanfaat dan dapat digunakan di masa yang akan datang oleh Penulis.
7. Seluruh rekan rekan penulis atas dukungan yang telah diberikan kepada penulis yang tidak dapat disebutkan satu per satu.

Akhir kata, semoga skripsi ini dapat bermanfaat bagi para pembacanya.

Jakarta, 5 Juni 2023

Penulis

DAFTAR ISI

LEMBAR PENGESAHAN	ii
PERNYATAAN ORISINALITAS	iii
ABSTRAK	iv
ASBTRACT	v
KATA PENGANTAR	vi
DAFTAR ISI.....	vii
DAFTAR GAMBAR	ix
DAFTAR TABEL	x
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Identifikasi Masalah	4
1.3 Rumusan Masalah	4
1.4 Batasan Masalah.....	5
1.5 Tujuan Penelitian.....	5
1.6 Manfaat Penelitian.....	5
1.7 Sistematika Penulisan.....	6
BAB 2 TINJAUAN PUSTAKA	8
2.1 <i>Distributed Denial of Service</i>	8
2.2 Log.....	9
2.3 Syslog	10
2.4 Security Information and Event Management.....	12
2.5 Log Management.....	14
2.6 Wazuh.....	14
2.7 Suricata	14
2.8 Penelitian Terkait	16
BAB 3 METODELOGI PENELITIAN	19
3.1 Tahapan Penelitian	19
3.1.1 Identifikasi Masalah.....	20
3.1.2 Studi Literatur	20
3.1.3 Perancangan Topologi.....	20

3.1.4	Implementasi	23
3.1.5	Hasil	24
3.2	Perangkat Penelitian	24
3.3	Jadwal Penelitian	25
BAB IV PEMBAHASAN.....		26
4.1	Penyajian Data.....	26
4.1.1	Perancangan Topologi.....	26
4.2	Pengujian Data	32
4.3	Analisis Data	37
BAB V PENUTUP.....		42
5.1	KESIMPULAN	42
5.2	SARAN	43
DAFTAR PUSTAKA		44
DAFTAR RIWAYAT HIDUP.....		47
LAMPIRAN.....		48

DAFTAR GAMBAR

Gambar 1. 1 Perbandingan jumlah serangan DDoS: Q2 2022 dan Q2 2021 serta Q1 2022 dikutip dari sumber : (DDoS Attacks in Q2 2022 Securelist, n.d.).....	2
Gambar 1. 2 Perbandingan durasi serangan DDoS: Q2 2022 dan Q2 2021 serta Q1 2022 dikutip dari sumber : (DDoS Attacks in Q2 2022 Securelist, n.d.).....	3
Gambar 2. 1 Contoh log serangan SYN Flood dikutip dari sumber : (Fitri Nova et al., 2022).....	9
Gambar 2. 2 Contoh log serangan UDP Flood dikutip dari sumber : (Fitri Nova et al., 2022).....	9
Gambar 2. 3 Contoh log serangan ICMP Flood dikutip dari sumber : (Fitri Nova et al., 2022).....	9
Gambar 2. 4 Format pesan syslog diadaptasi dari sumber : (What Is Syslog Server and Its Working ? - GeeksforGeeks, n.d.).....	10
Gambar 2. 5 Arsitektur SIEM diadaptasi dari sumber : (Georgeta Catescu, 2018).....	13
Gambar 2. 6 Contoh Eve.JSON dari suricata.....	15
Gambar 3. 1 Kerangka Berpikir.....	19
Gambar 3. 2 Rancangan Serangan DDoS.....	21
Gambar 3. 3 Topologi Penyerangan.....	22
Gambar 3. 4 Rancangan Topologi Pemantauan.....	23
Gambar 3. 5 Skema Pengujian.....	24
Gambar 4. 1 Tampilan wazuh manager.....	27
Gambar 4. 2 Tampilan Dashboard Wazuh.....	28
Gambar 4. 3 Security Alert.....	29
Gambar 4. 4 Instalasi Agent Wazuh.....	30
Gambar 4. 5 Wazuh Agent Berhasil Terinstall.....	30
Gambar 4. 6 Perintah untuk menginstall Suricata.....	31
Gambar 4. 7 perintah untuk ekstraksi aturan Emerging Threats Suricata.....	31
Gambar 4. 8 Penambahan Konfigurasi Suricata pada Agent Wazuh.....	31
Gambar 4. 9 Suricata sudah berhasil berjalan.....	31
Gambar 4. 10 Konfigurasi IP Komputer Target.....	32
Gambar 4. 11 Perintah SYN Flooding.....	32
Gambar 4. 12 Perintah ICMP Flooding.....	33
Gambar 4. 13 Perintah UDP Flooding.....	33
Gambar 4. 14 Peningkatan penggunaan resource pada saat SYN Flooding.....	34
Gambar 4. 15 Peningkatan penggunaan resource pada saat ICMP Flooding.....	35
Gambar 4. 16 Peningkatan penggunaan resource pada saat UDP Flooding.....	36
Gambar 4. 17 Alarm terkait SYN Flooding.....	37
Gambar 4. 18 Alarm terkait ICMP Flooding.....	38
Gambar 4. 19 Alarm terkait UDP Flooding.....	38
Gambar 4.20 3 IP teratas dari penyerang.....	39
Gambar 4.21 Informasi lengkap tentang IP penyerang.....	39

DAFTAR TABEL

Tabel 2. 1 Facility Code diadaptasi dari sumber :(What Is Syslog Server and Its Working ? - GeeksforGeeks, n.d.)	11
Tabel 2. 2 Severity Level diadaptasi dari sumber : (What Is Syslog Server and Its Working ? - GeeksforGeeks, n.d.)	11
Tabel 3. 1 Jadwal Pelaksanaan.....	25
Table 4. 1 Hasil Percobaan	40