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

(Anita Muliawati, S.Kom., MTI.)
Penguji II

(Henki Bayu Seta, S.kom, MTI.)
Dosen Pembimbing

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

(Dr. Widya 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 Pembagunan 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

DAFTAR GAMBAR

DAFTAR TABEL