MANAJEMEN LOG SERANGAN DEAUTHENTICATION PADA JARINGAN NIRKABEL MENGGUNAKAN ELK STACK (ELASTICSEARCH LOGSTASH DAN KIBANA)

SKRIPSI

Disusun oleh:

Ero Wahyu Pratomo

17.83.0068

PROGRAM SARJANA

PROGRAM STUDI TEKNIK KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

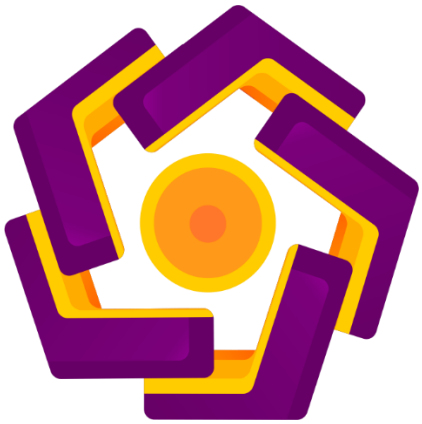
YOGYAKARTA

2021

MANAJEMEN LOG SERANGAN DEAUTHENTICATION PADA JARINGAN NIRKABEL MENGGUNAKAN ELK STACK (ELASTICSEARCH LOGSTASH DAN KIBANA)

SKRIPSI

Diajukan kepada Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta
untuk memenuhi salah satu syarat memperoleh gelar Sarjana Komputer
Pada Jenjang Program Sarjana – Program Studi Teknik Komputer



Disusun oleh:

Ero Wahyu Pratomo

17.83.0068

PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2021

HALAMAN PERSETUJUAN

SKRIPSI

MANAJEMEN LOG SERANGAN DEAUTHENTICATION PADA JARINGAN NIRKABEL MENGGUNAKAN ELK STACK (ELASTICSEARCH LOGSTASH DAN KIBANA)

yang dipersiapkan dan disusun oleh

Ero Wahyu Pratomo

17.83.0068

Telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal 18 Desember 2020

Dosen Pembimbing,

Joko Dwi Santoso, M.Kom

NIK. 190302181

HALAMAN PENGESAHAN

SKRIPSI

MANAJEMEN LOG SERANGAN DEAUTHENTICATION PADA JARINGAN NIRKABEL MENGGUNAKAN ELK STACK (ELASTICSEARCH, LOGSTASH DAN KIBANA)

yang dipersiapkan dan disusun oleh

Ero Wahyu Pratomo

17.83.0068

Telah dipertahankan di depan Dewan Penguji
pada tanggal 18 Desember 2020

Susunan Dewan Penguji

Nama Penguji	**Tanda Tangan**
Ferry Wahyu Wibowo, S.Si., M.Cs	
NIK. 190302235	
Sumarni Adi, S.Kom, M.Cs	
NIK. 190302256	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 18 Desember 2021

DEKAN FAKULTAS ILMU KOMPUTER

Krisnawati, S.Si, M.T.

NIK. 190302038

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Ero Wahyu Pratomo
NIM : 17.83.0068

Menyatakan bahwa Skripsi dengan judul berikut:

Manajemen Log Serangan Deauthentication Pada Jaringan Nirkabel Menggunakan ELK Stack (Elasticsearch, Logstash dan Kibana)

Dosen Pembimbing : Joko Dwi Santoso, M.Kom

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 18 Desember 2020

Yang Menyatakan,

Ero Wahyu Pratomo

HALAMAN MOTTO

"HIDUPMU ADALAH TEMPATMU DI DUNIA. PERGI DAN LAKUKAN APA YANG BISA KAMU LAKUKAN. BUATLAH HIDUPMU INI SEPERTI YANG KAMU INGINKAN." -MAE JEMISON

"TINGGALKAN PIKIRAN YANG MEMBUATMU LEMAH, DAN PEGANGLAH PIKIRAN YANG MEMBERI KEKUATAN BAGIMU" - MARTIN LUTHER KING JR.

HALAMAN PERSEMBAHAN

Segala puji dan syukur kupersembahkan kepada Allah SWT terimakasih atas rasa syukur, nikmat, dan karunia yang telah Engkau berikan. Terimakasih Engkau telah memberiku pertolongan, kekuatan, kesabaran, ilmu, serta memberiku orang-orang baik di sekelilingku sehingga skripsi ini bisa terselesaikan. Untuk itu kuucapkan rasa terimakasihku juga kepada :

1. Kedua orang tuaku dan adiku yang telah memberikan do'a, sabar dalam mendidik, serta memberikan segala dukungan dan motivasi dalam menempuh studi yang telah penulis lakukan dan menyelesaikan skripsi ini.
2. Dosen pembimbingku, Joko Dwi Santoso, M.Kom yang telah membimbing dan membantu dalam pengerjaan skripsi ini.
3. Nabila Roro Ayu Hapsari yang memberikan pembelajaran luar biasa serta dukungan agar saya menjadi yang lebih baik lagi sebelumnya.
4. Edo, Yuga dan teman-teman satu kelas 17S1TK02 terima kaisih yang telah memberikan dukungan, arahan, serta motivasi atas terselesaikannya skripsi ini.

KATA PENGANTAR

Puji syukur penulis panjatkan kepas Tuhan Yang Maha Esa atas berkat, rahmat serta karunia-Nya, Penulis dapat menyelesaikan skripsi berjudul : "MANAJEMEN LOG SERANGAN DEAUTHENTICATION PADA JARINGAN WIRELESS MENGGUNAKAN ELK (ELASTICSEARCH LOGSTASH DAN KIBANA".

Penulis menyadari dalam penulisan skripsi ini masih jauh dari kata sempurna dan banyak kekurangan baik dalam metode penulisan maupun dalam pembahasan materi. Sehingga penulis mengharapkan saran dan kritik yang bersifat membangun, sehingga dikemudian hari dapat memperbaiki segala kekurangannya.

Dalam penulisan skripsi ini, penulis selalu mendapat bimbingan dan dorongan serta semangat dari banyak pihak. Oleh karena itu penulis mengucapkan terima kasih kepada :

1. Bapak Prof. Dr. M. Suyanto,MM. selaku Rektor Universitas AMIKOM Yogyakarta.
2. Ibu Krisnawati, S.Si, M.T. selaku Dekan Fakultas Imu Komputer Unviersitas AMIKOM Yogyakarta.
3. Bapak Joko Dwi Santoso, M.Kom selaku Dosen Pembimbing yang telah membantu, mendukung dan mendoakan saya sampai saat ini.
4. Segenap Dosen Program Studi Sistem Informasi, Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta yang telah memberikan ilmu dan pengetahuan dan wawasan selama perkuliahan berlangsung.
5. Sahabatku Edo Maland dan Yuga yang telah membantu dalam proses penelitian.
6. Kedua orang tua sekaligus adik ku tercinta.

7. Keluarga S1- TK02 terima kasih untuk membantu berjalan selama 7 semester ini. Suka duka 3,5 tahun telah kita lalui. Semoga segera menyusul.
8. Terakhir untuk Nabila Roro Ayu yang selalu memberikan doa dan bantuan.

Yogyakarta, Desember 2020

Penulis,

Ero Wahyu Pratomo

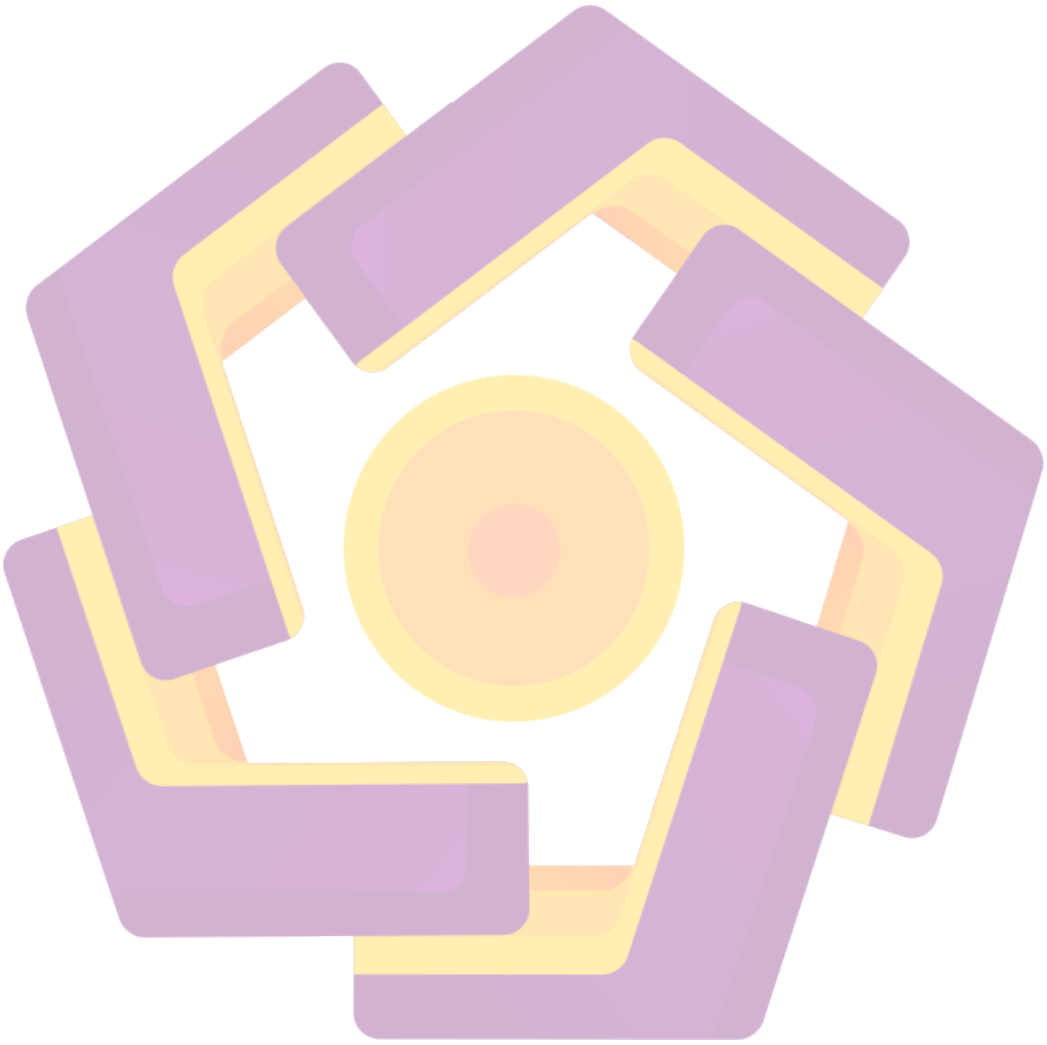
17.83.0068

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR ISTILAH



INTISARI

Dalam menyusun komponen agar dapat lebih informatif, teknologi saat ini menggunakan fasilitas yang umum. Selain menyediakan konektivitas yang mudah serta jangkauan yang cukup luas, jaringan tersebut juga menawarkan keamanan kepada penggunanya dimana hanya orang yang mempunyai autentikasi password yang dapat menggunakan fasilitas tersebut atau biasa disebut dengan WiFi.

Salah satu serangan terhadap access point sehingga user client ataupun admin akan mengalami disconnecting (Deauthentication Attack) atau membuat kecepatan internet melambat. Oleh karena itu, salah satu solusi log management yang bisa digunakan adalah ELK Stack, sebuah solusi berbasis open source yang dapat mencatat log dari seluruh perangkat yang ada di infrastruktur IT secara real-time. Dengan 4 komponen seperti Beats, s*hipping agent* yang berfungsi untuk mengirimkan data *log* ke dalam Logstash.

Logstash, *tool* yang digunakan untuk mengumpulkan dan mem-*parsing log* data, serta membuat indeks *log* yang disimpan pada Elasticsearch. Elasticsearch, *search* dan *analytics engine* berbasis Apache Lucene yang bersifat *open source.* Kibana, *web interface* yang dapat memvisualisasikan data dari Elasticsearch dalam beragam bentuk grafik, sehingga keempat komponen saling bekerjasama untuk memonitor dan mengamankan infrastruktur IT secara *real-time.*

***Kata kunci** : Deauthentication Attack, ELK Stack, Log Management*

ABSTRACT

Inorder to arrange a components to be more informative, technology currently uses public facilities. In addition to providing easy connectivity and wide coverage, the network also offers security to its users where only people who have password authentication can use these facilities or commonly known as WiFi.

One of the attacks on the access point is that the client or admin user will be disconnected (Deauthentication Attack) or make the internet speed slow down. Therefore, one of the log management solutions that can be used is the ELK Stack, is an open source based solution that can log real-time logs of all devices in the IT infrastructure. With 4 components such as Beats, a shipping agent whose function is to send log data into Logstash.

Logstash, a tool used to collect and parse log data, as well as index logs stored on Elasticsearch. Elasticsearch, an open source Apache Lucene based search and analytics engine. Kibana, a web interface that can visualize data from Elasticsearch in various graphical forms, so that the four components work together to monitor and secure the IT infrastructure in real-time.

Keyword: *Deauthentication Attack, ELK Stack, Log Management*