Judul:

Implementasi *Security Information and Event Management* (SIEM) pada lingkungan ITSEC Asia Menggunakan Elastic SIEM

SKRIPSI

Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan untuk Memperoleh Diploma Empat Politeknik

Fazrin Alfiansyah

4816050122

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

DEPOK

2022

HALAMAN PERNYATAAN ORISINALITAS

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

Nama : Fazrin Alfiansyah

NIM : 4816050122

Tanggal : 08 Juli 2022

Tanda Tangan :

KATA PENGANTAR

Skripsi diajukan oleh:

Nama	: Fazrin Alfiansyah
NIM	4816050122
Program Studi	: Teknik Multimedia dan Jaringan
Judul Skripsi	: Implementasi *Security Information and Event Management* (SIEM) pada lingkungan ITSEC Asia Menggunakan Elastic SIEM

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Jum'at Tanggal 8 bulan Juli Tahun 2022 dan dinyatakan **LULUS.**

Disahkan oleh

Pembimbing I	:	Fachroni Arbi Murad, S.Kom., M.Kom.	( )
Penguji I	:	Defiana Arnaldy, S.Tp., M.Si.	( )
Penguji II	:	Ayu Rosida Zain, S.ST, M.T.	( )
Penguji III	:	Ariawan Andi Suhandana, S.Kom., M.T.I.	( )

Mengetahui:

Jurusan Teknik Informatika dan Komputer

Ketua

Mauldy Laya, S. Kom, M. Kom.

NIP. 19780211 200912 1 003

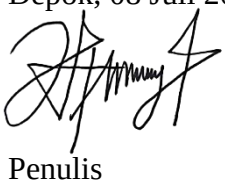
KATA PENGANTAR

Alhamdulillah. Puji syukur saya panjatkan kepada Allah SWT, karena atas berkat dan rahmat-Nya, penulis dapat menyelesaikan laporan Skripsi ini. Penulisan laporan Skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Terapan Politeknik. Penulis menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan laporan Skripsi, sangatlah sulit bagi penulis untuk menyelesaikan laporan Skripsi ini. Oleh karena itu, penulis mengucapkan terima kasih kepada:

a. Bapak Mauldy Laya, S. Kom., M. Kom. selaku ketua jurusan Teknik Informatika dan Komputer Politeknik Negeri Jakarta;
b. Bapak Defiana Arnaldy, S. Tp., M. Si. selaku ketua program studi Teknik Multimedia dan Jaringan Jurusan Teknik Informatika dan Komputer Politeknik Negeri Jakarta;
c. Bapak Fachroni Arbi Murad S.Kom, M.Kom., selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan penulis dalam penyusunan laporan Skripsi ini;
d. Pihak Civitas Jurusan TIK yang telah banyak membantu dalam usaha memperoleh data yang penulis perlukan;
e. Orang tua dan keluarga penulis yang telah memberikan bantuan dukungan moral dan material;
f. Sahabat dan Dosen yang telah banyak membantu penulis dalam menyelesaikan laporan Skripsi ini.

Akhir kata, penulis berharap Allah SWT, berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga laporan Skripsi ini membawa manfaat bagi pengembangan ilmu.

Depok, 08 Juli 2022



Penulis

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI

SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya yang bertanda tangan di bawah ini:

Nama : Fazrin Alfiansyah

NIM 4816050122

Program Studi : Teknik Multimedia dan Jaringan

Jurusan : Teknik Informatika dan Komputer

Jenis karya : Skripsi/~~Tesis/Disertasi/ Karya Ilmiah~~ Lainnya*: .....

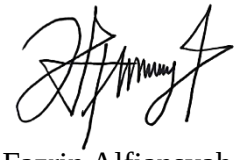
demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta **Hak Bebas Royalti Noneksklusif (Non-exclusive Royalty- Free Right)** atas karya ilmiah saya yang berjudul:

"Implementasi Security Information and Event Management (SIEM) pada lingkungan ITSEC Asia Menggunakan Elastic SIEM" beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Politeknik Negeri Jakarta berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan memublikasikan skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok, Pada tanggal: 08 Juli 2022

Yang menyatakan



Fazrin Alfiansyah

Implementasi Security Information and Event Management (SIEM) pada lingkungan ITSEC Asia Menggunakan Elastic SIEM

Abstrak

Risiko keamanan pada perusahaan yang tidak terkontrol dapat meningkatkan jumlah serangan keamanan yang dapat menjadi kerugian finansial yang besar. Risiko ini dapat meningkatkan vulnerability dalam sistem. Vulnerability adalah kelemahan besar dalam keamanan sistem dan jaminan informasi. Penyerang menggunakan vulnerability ini untuk mengeksploitasi sistem dan mendapatkan akses dan informasi yang tidak sah. Untuk itu, dibutuhkan suatu alat atau sistem yang mampu mendeteksi serangan yang masuk pada suatu jaringan di perusahaan, namun kebanyakan tools yang digunakan terinstall terpisah sehingga menyulitkan admin untuk memonitoring log yang masuk, dengan menggunakan elastic SIEM kita dapat mengumpulkan berbagai log dari tools yang terinstal sepeti log dari surciata, wazuh, dan winlogbeat. Untuk memastikan tools berjalan dengan baik maka diperlukan adanya uji coba pada tools yang telah diimplementasikan dengan cara melakukan basic attack seperti vulnerability scanning dan *bruteforce.*

Kata Kunci: *Vulnerability scanning*, elastic SIEM, *Bruteforce*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

ITSEC merupakan sebuah perusahaan Stonetree Group, telah menjadi perusahaan yang terdepan dalam industri keamanan informasi sejak didirikan pada tahun 2004. ITSEC berkantor pusat di Singapura dan memiliki kantor regional di Asia-Pasifik, Asia Selatan, Timur Tengah, Australia dan Eropa. ITSEC memberdayakan klien dengan mengamankan bisnis mereka dan bertujuan untuk membantu dunia menjalankan perusahaan yang aman.

Pada era berkembangan teknologi seperti sekarang ini, hampir di setiap perusahaan menggunakan jaringan komputer untuk memperlancar arus informasi di dalam perusahaan tersebut. Salah satu contohnya adalah internet yang merupakan jaringan komputer yang terhubung dan saling dapat berinteraksi. Kebutuhan akan informasi dan akses data pada saat ini sangat tinggi, maka dari itu peran internet sangatlah penting, akan tetapi dalam dunia internet banyak sekali hal – hal negatif yang dapat membahayakan dan merugikan bagi perseorangan maupun suatu perusahaan.

Divisi *Security Operation Center* (SOC) PT. ITSEC ASIA memiliki sebuah jaringan internet yang terhubung dengan berbagai *client* di Indonesia maupun di luar negri, dengan jaringan yang luas tersebut tidak menutup kemungkinan akan banyak *attacker* yang mencoba untuk menyerang jaringan tersebut. Oleh karena itu, diperlukan suatu sistem yang dapat mencegah atau meminimalisir hal tersebut. SIEM merupakan suatu sistem yang dapat membantu perusahaan dalam memonitor jaringan, SIEM dapat mengumpulkan berbagai log aktivitas dari *agent* yang telah di *install* pada *server* yaitu wazuh dan winlogbeat yang kemudian dapat dianalisa oleh seorang analis supaya suatu serangan dapat di cegah lebih awal dan meminimalisir kerugian. Untuk menguji sistem tersebut penulis akan melakukan beberapa *basic attack* yang di tujukan langsung pada server.

1.2 Perumusan Masalah

Berdasarkan hal-hal yang telah diuraikan dalam latar belakang, maka rumusan masalah dalam skripsi ini adalah

- Bagaimana *agent* wazuh dan winlogbeat dapat terintall pada *server*.

- Bagaimana mengumpulkan log dari *agent* untuk kemudian di *monitor* melalui elastic SIEM.
- Apakah penambahan agent pada server dapat membuat server lebih aman dan lebih termonitor?

1.3 Batasan Masalah

Berdasarkan latar belakang tersebut, dapat diuraikan perumusan masalah untuk dibahas dalam penelitian ini yaitu:

a. Ruang lingkup penelitian hanya meliputi jaringan di ITSEC Asia.
b. Log yang masuk pada Elastic SIEM berasal dari *agent* yang telah di *install* pada server.
c. Agent yang di *install* pada perangkat yaitu winlogbeat dan wazuh.
d. *Basic attack* yang di implementasikan yaitu *vulnerability scanning* dan *bruteforce*, serta melakukan penambahan user baru.
e. Serangan dilakukan pada jaringan internal yang sama dengan server.
f. Pengujian dilakukan untuk memastikan *agent* yang terinstall dapat mendeteksi serangan yang terjadi pada server.
g. Penambahan metric beat untuk monitoring server

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Tujuan dari penelitian ini yaitu :

1. Mendeteksi serangan bruteforce pada server yang telah di install agent wazuh.
2. Mendeteksi penambahan dan penghapusan user pada komputer yang terlah di install agent winlogbeat
3. Melakukan transfer data dari agent wazuh dan winlogbeat pada server elasticsearch.
4. Memonitoring serangan yang masuk pada perangan keamanan jaringan menggunakan elastic SIEM
5. Mempermudah memonitoring serangan yang masuk pada perangkat keamanan jaringan menggunakan Elastic SIEM.

1.4.2 Manfaat

1. Dapat mendeteksi serangan bruteforce dan penambahan user serta penghapusan user menggunakan agent wazuh dan winlogbeat.
2. Dapat memonitoring serangan yang masuk pada perangkat keamanan jaringan yang di visualisasikan pada Elastic SIEM.

3. Mempermudah dalam pembacaan serangan menggunakan Elastic SIEM.

1.5 Metode Pelaksanaan Skripsi

Untuk menyeselaikan masalah ini, metode yang digunakan yaitu bersifat eksperimental dengan membuat sebuah sistem untuk menguji perangkat keamanan jaringan bisa membaca serangan *vulnerability scanning* dan *bruteforce* serangan dilakukan menggunakan *tools* pada kali linux. Serta log dari agent yang telah di *install* bisa di visualisasikan pada Kibana. Menggunakan Elastic SIEM diharapkan bisa mempermudah dalam memonitor serangan yang masuk pada perangkat keamanan jaringan.

BAB V

KESIMPULAN

5.1 Kesimpulan

Berdasarkan hasil dari penelitian yang telah dilakukan oleh penulis, maka dapat ditarik kesimpulan sebagai berikut:

1. Serangan *brute force* yang dilakukan pada *server* dengan IP server 192.168.71.151 melalui port 22 (SSH) berhasil di deteksi oleh agent wazuh dan dapat di tampilkan pada elastic SIEM.
2. Aktifitas penambahan dan penghapusan user dengan nama *user* skripsi pada salah satu *computer* yang sudah di *install agent* winlogbeat dan terhubung pada jaringan yang sama dapat terdeteksi oleh *agent* winlogbeat dan dapat ditampilkan pada elastic SIEM.
3. Semua log yang masuk pada *agent* winlogbeat dan wazuh dapat di visualisasikan oleh elastic SIEM.
4. Elastic SIEM mempermudah dalam melakukan monitoring terhadap perangkat keamanan jaringan

5.2 Saran

Saran yang dapat diusulkan pada penelitian ini adalah :

1. Menggunakan berbagai macam tipe serangan pada setiap *agent* untuk agar dapat mengetahui serangan mana saja yang dapat terdeteksi dan tidak dapat terdeteksi oleh *agent* wazuh dan winlogbeat.
2. Menggunakan lebih dari 2 *agent* untuk memperkuat sistem keamanan pada *server*.

DAFTAR PUSTAKA

ITSEC ASIA. *About US, https://www.itsec.asia/ (*Diakses 5 Februari 2021)

Elasticsearch. *SIEM Guide,* https://www.elastic.co/guide/en/siem/guide/7.8/index.html (Diakses 7 Februari 2021)

Alpuji, Aldi. 2021, Implementasi *Security Information And Event Management* Menggunakan Tools Elastic Serta Suricata Sebagai Sistem Pendeteksi Intrusi Pada Sistem Operasi Linux Ubuntu Di Perusahaan PT. ITSEC ASIA.

WAZUH. *Abous US, https://wazuh.com/* (Diakses 17 Juni 2022)

Adrian, Admi. 2020, Penerapan Elastic Stack sebagai *Tools* Alternatif Pemantauan *Traffic* Jaringan dan *Host* pada Instansi Pemerintah untuk Memperkuat Keamanan dan Ketahanan Siber Indonesia.

Dinata, Rangga. 2020, Implementasi Sistem Pendeteksi Serangan *SQL Injection* dengan Menggunakan *Algoritme K-Nearest Neighbor.*

Napoleon, Putu. 2020, Implementasi *Server Log Monitoring System* menggunakan Elastic Stack.

Huda, Nurul. & Najoan. 2016, Analisa dan Implementasi *Network Intrusion Prevention* Sistem di Jaringan Universitas Sam Ratulangi.

Nur, Siti. & Jamu, Sandra. 2019. Rancangan Virtualisasi Server Menggunakan VMWare Vsphare.

Admi, A., & Maulana, A. H. N. 2020. Penerapan Elastic Stack sebagai Tools Alternatif Pemantauan Traffic Jaringan dan Host pada Instansi Pemerintah untuk Memperkuat Keamanan dan Ketahanan Siber Indonesia. JUSTINDO (Jurnal Sistem dan Teknologi Informasi Indonesia), 5(2), 69-77.

Agrawal, Kavita, and Hemant Makwana. 2015. "Review of Different Log Management Tools Used for Data Analysis." Data Mining and Knowledge Engineering 7.4. 161-163.