IMPLEMENTASI SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) PADA LINGKUNGAN ITSEC ASIA MENGGUNAKAN ELASTIC SIEM

INDONESIA

Fazrin Alfiansyah
Jurusan Teknik Informatika dan Komputer
Politeknik Negeri Jakarta
Bogor, Indonesia
Fazrin.alfiansyah.tik16@mhsw.pnj.ac.id

Fachroni Arbi Murad, Skom., Mkom.
Jurusan Teknik Informatik dan Komputer
Politeknik Negeri Jakarta
Depok, Indonesia
fachroni.murad@tik.pnj.ac.id

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*

I. PENDAHULUAN

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.

A. Elastic Stack

ELK stack adalah platform manajemen dan analisis log yang komplet. analisis log mempunyai peran penting dalam mengelola keamanan pada sistem. Analisis log membantu dalam mendeteksi pelanggaran keamanan, penyalahgunaan aplikasi, serangan berbahaya, dan sebagainya.

ELK stack terdiri dari elasticsearch, logstash, dan kibana. Masing-masing membuat pencarian dan analisis data menjadi lebih mudah. Berikut penjelasan dari tiga perangkat tersebut.

Gambar 1. Alur Kerja Elastic Stack

1. Elasticsearch

Elasticsearch merupakan mesin pencari berbasis full-text yang handal dan menyediakan kemampuan untuk melakukan pencarian dokumen berbeda dengan cepat dan realtime. Elasticsearch bersifat open source dan menggunakan platform Java. Elasticsearch merupakan upgrade dari Apache Lucene yang mana membawa beberapa kelebihan dibanding Lucene seperti API yang lebih sederhana, kemudahan dalam penggunaan operasional dan terdapat fitur cluster dan replica[1]

2. Kibana

Kibana memvisualisasikan data yang tersimpan pada cluster elasticsearch. Kibana menyediakan antarmuka berbasis browser yang memudahkankan dalam membuat dashboard dengan cepat. Kibana menyajikan data dalam bentuk histogram, geomaps, diagram lingkaran, grafik, tabel, dan lain-lain.

3. Filebeat

Filebeat adalah bagian dari Beats, yaitu log collector open source yang memforward log dari server ke server pusat. Filebeat merupakan sebuah upgrade dari Logstash Forwarder. Tujuan filebeat yaitu untuk memonitor setiap file log dan mengirimkan pesan log tersebut ke target yang diinginkan [2]

4. Logstash

Logstash membantu dalam membangun jaringan pipeline yang dapat memusatkan pengolahan data. Menggunakan berbagai plugin input dan output untuk memudahkan dalam parsing dan memproses format yang berbeda dalam skala besar. Logstash berfungsi untuk memproses log, peristiwa, dan data tidakterstruktur. Data yang telah diproses dikirim ke elasticsearch menggunakan plug in output pada logstash.

B. Winlogbeat

Winlogbeat membaca dari satu atau lebih event log menggunakan API Windows, memfilter event berdasarkan kriteria yang dikonfigurasi pengguna, lalu mengirimkan data peristiwa ke output yang dikonfigurasi (Elasticsearch atau Logstash). Winlogbeat mengawasi event log sehingga event data baru dikirim tepat waktu. Winlogbeat dapat menangkap data peristiwa dari event log apa pun yang berjalan di system

C. Wazuh

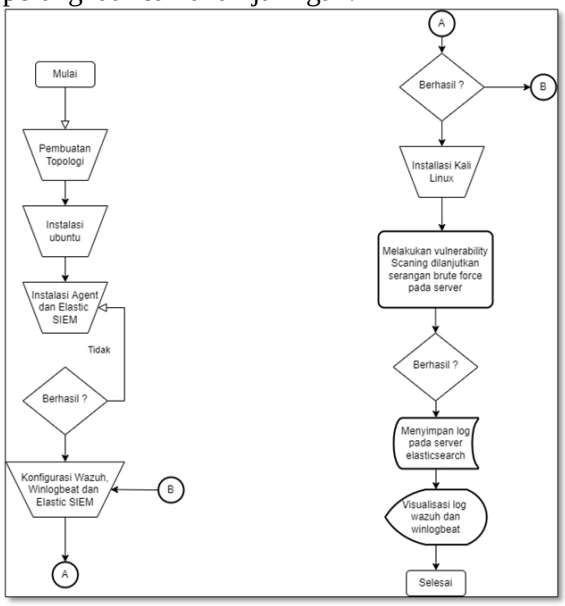
Wazuh merupakan perangkat berbasis OpenSource yang berfungsi sebagai sistem deteksi intrusi berbasis host (endpoint). Wazuh melakukan analisis log, pemeriksaan integritas, pemantauan registry Windows, deteksi rootkit, peringatan berbasis waktu dan respon. Wazuh merupakan perangkat yang menyediakan fitur visibilitas keamanan yang lebih dalam ke sebuah infrastruktur dengan memantau host pada sistem operasi dan juga pada tingkat aplikasi. Wazuh terdiri dari 2 (dua) bagian yaitu Wazuh-Server dan Wazuh-Agent. Wazuh server merupakan perangkat yang digunakan sebagai manajemen agen dan dashboard sistem monitoring baik file integrity, intrusion, maupun log. Sedangkan Wazuh agent merupakan perangkat yang diinstall pada perangkat endpoint untuk melakukan pembacaan sistem, pengumpulan log serta mengirimkan ke Wazuh server.

D. *Basic Attack*

Basic Attack merupakan serangan yang dilakukan untuk menguji suatu system keamanan yang bertujuan untuk mengetahui apakah *rule* atau parameter yang telah ditetapkan bisa berjalan dengan baik atau tidak, pada pengujian kali ini *basic attack* yang akan di gunakan yaitu *vulnerability scanning* dan *bruteforce attack.*

II. METODE

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.



Gambar 2. *Flowchart* Pengerjaan dan Pengujian Sistem

Gambar 2 diatas merupakan Flowchart untuk pengerjaan dan pengujian terhadap sistem yang telah dibuat pada sistem operasi Linux distro ubuntu dan kali linux menggunakan Virtual Machine. Elastic SIEM dan wazuh di pasang pada server ubuntu, kemudian winlogbeat dipasang pada computer berbasis OS windows. Pada tahapan awal dalam merancang sistem penulis membuat topologi jarangan agar memudahkan penulis dalam melakukan implementasi, setiap computer yang terhubung pada jaringan di divisi SOC akan di install agent wazuh dan winlogbeat untuk memudahkan dalam melakukan monitoring terhadap aktivitas yang terjadi pada computer tersebut, penulis mencoba untuk melakukan serangan pada server menggunakan OS kali linux dengan Teknik serangan vulnerability scanning dilanjutkan dengan melakukan bruteforce, selain itu penulis juga akan melakukan penambahan dan penghapusan user pada salah satu komuputer untuk menguji apakah agent winlogbeat berjalan dengan baik atau tidak. Agent yang telah di install pada server dan computer client bertindak untuk menyimpan log serangan yang telah dilakukan untuk kemudian di simpan pada elasticsearch dan ditampilkan pada visualisasi kibana.

Beberapa perangkat keras yang dibutuhkan dalam melakukan implementasi penelitian adalah sebagai berikut:

A. 1 buah Laptop sebagai virtualisasi.
   - Processor: Intel(R) Core (TM) i7
   - Memory: 20 GB
   - Hardisk Drive: 1 TB
   - NIC: Fast Ethernet

B. 1 buah laptop sebagai client(tester)
   - *Prosesor*: Intel(R) Core (TM) i3
   - Memory: 8 GB
   - Hardisk Drive: 256 GB
   - NIC: Fast Ethernet

C. 1 buah router
D. 1 buah kabel RJ45
E. 1 buah access point

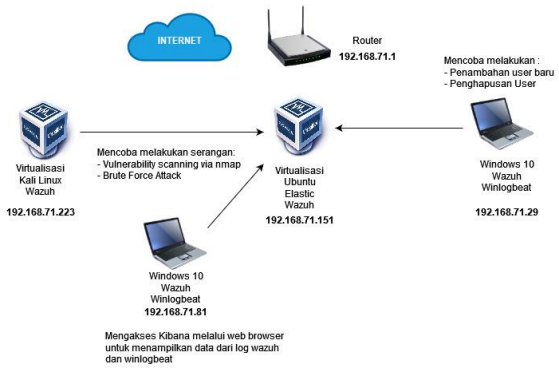
Beberapa perangkat lunak yang dibutuhkan dalam melakukan implementasi penelitian adalah sebagai berikut:

a. VMWare: Mesin Virtual
b. Ubuntu 20.04: Distro linux
c. Windows 10: Sistem operasi
d. Kali linux: Distro linux
e. Metasploit: untuk melakukan vulnerability scan dan bruteforce.
f. Wazuh : Endpoint Protection
g. Winlogbeat : Endpoint Protection
h. Filebeat 7.13: Dibutuhkan pada SIEM untuk mengirim log
i. Logstash 7.13: Dibutuhkan pada SIEM untuk parsing data
j. Elasticsearch 7.13: Dibutuhkan pada SIEM untuk penyimpanan data

k. Kibana 7.13: Dibutuhkan pada SIEM untuk visualisasi data

III. HASIL DAN PEMBAHASAN

Pada bab ini akan dijelaskan pengujian dari sistem keamanan yang telah dirancang. Dalam melakukan pengujian pada sistem keamanannya digunakan beberapa keadaan pengujian yang berbeda. Kemudian hasil pengujian dari masing-masing pengujian tersebut dianalisa serta dibandingkan bagaimana hasilnya dengan pengujian yang sebelumnya telah dilakukan.



Gambar 3. Prosedur pengujian

pengujian yang dilakukan adalah dengan melakukan vulnerability scanning terhadap server melalui salah satu computer yang sudah terinstall OS kali linux, proses ini bertujuan untuk mengetahui port mana saja yang terbuka pada server untuk kemudian dilakukan serangan, serangan yang akan dilakukan yaitu serangan bruteforce yang bertujuan untuk mendapatkan akses login pada server. Serangan tersebut juga bertujuan untuk menguji agent wazuh apakah dapat menangkap log serangan tersebut atau tidak.

Selain itu, penulis juga melakukan penambahan user pada salah satu komputer yang terhubung pada jaringan yang sama dan telah di install agent winlogbeat, hal ini bertujuan untuk menguji agent winlogbeat apakah dapat menangkap log aktivitas yang dilakukan tersebut atau tidak..

A. Pengujian Menggunakan nmap

Pengujian yang dilakukan pertama kali yaitu melakukan vulnerability scanning menggunakan tool nmap.

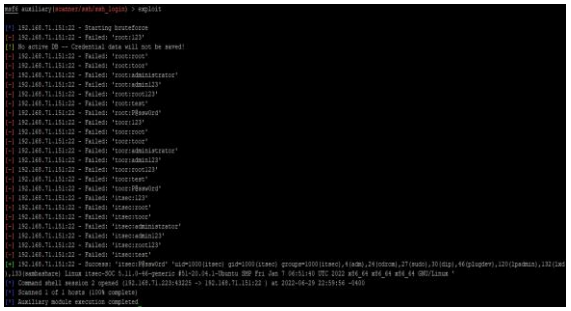
```
┌──(root💀kali)-[/home/kali]
└─# nmap 192.168.71.151
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-30 00:49 EDT
Nmap scan report for 192.168.71.151
Host is up (0.00012s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
3389/tcp open  ms-wbt-server
5900/tcp open  vnc
9200/tcp open  wap-wsp
MAC Address: 08:00:27:B4:9C:18 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.32 seconds
```

Gambar 4. Vulnerability scanning

B. Pengujian Menggunakan tool metasploit

Pada pengujian menggunakan Metasploit, modul yang digunakan yaitu modul auxiliary untuk melakukan serangan bruteforce pada server.



Gambar 5. Bruteforce Metasploit

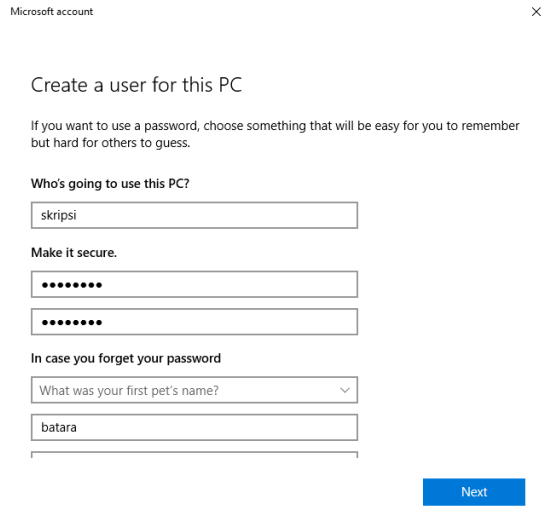
melakukan serangan bruteforce menggunakan module auxiliary, opsi yang diisi adalah pada bagian RHOST yaitu target dari serangan bruteforce, pada bagian RHOST di isi IP server yaitu 192.168.71.151, USER_FILE adalah kumpulan dari user yang akan di coba pada serangan bruteforce, USER_FILE di isi dengan fileuser.txt, PASS_FILE adalah kumpulan dari password yang akan di coba pada serangan bruteforce, PASS_FILE di isi dengan filepass.txt, STOP_ON_SSUCCESS di setting true, hal ini bertujuan ketika ada username dan password yang match maka seragan akan dihentikan, VERBOSE di setting true, hal ini bertujuan untuk menampilkan serangan bruteforce..

Gambar 6. Kibana discover dari brutefoce

Diatas adalah tampilan discover pada kibana, dapat dilihat adanya percobaaan gagal login dari IP 192.168.71.223, IP tersebut merupakan IP kali linux yang tadi digunakan untuk melakukan serangan bruteforce, wazuh agent berhasil mendeteksi serangan yang telah dilakukan.

C. Pengujian dengan menambahkan user

Pada pengujian ini, akan dilakukan penambahan user pada salah satu computer yang sudah terinstall agent winlogbeat dan terhubung dengan jaringan yang sama.



Gambar 7. Penambahan user

Melakukan penambahan *user* dengan nama skripsi pada salah satu *computer*, hal ini dilakukan untuk menguji agent winlogbeat apakah dapat mendeteksi aktifitas penambahan user tersebut atau tidak. Untuk melihat apakah winlogbeat dapat mendeteksi aktifitas penambahan *user* tersebut dapat dilihat pada index winlogbeat pada elastic SIEM.

Gambar 8. Discover winlogbeat

agent winlogbeat dapat mendeteksi penambahan *user* dengan nama user skripsi, hal ini mengindikasikan bahwa *agent* winlogbeat dapat mendeteksi semua aktifitas yang terjadi pada *computer*.

D. Tabel Hasil Pengujian

Tabel 1. Hasil pengujian

Aplikasi	Transport Protocol	Port	Wazuh Mendeteksi Serangan	Winlogbeat Mendeteksi Serangan	Log dikirim pada SIEM
Bruteforce Metasploit	TCP	22	√	-	√
Bruteforce Hydra	TCP	22	√	-	√
Add User	-	-	-	√	√
Detele User	-	-	-	√	√

Pada pengujian serangan bruteforce, penambahan user dan penghapusan user. Semua serangan bisa di deteksi oleh agent wazuh dan winlogbeat. Semua serangan tersebut juga dapat di tampilkan pada elastic SIEM.

BAB IV SIMPULAN DAN SARAN

A. 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

B. 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.

Puji Syukur saya panjatkan kepada Tuhan Yang Maha Esa, 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 skripsi ini. Oleh karena itu, penulis mengucapkan terima kasih kepada:

a. 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;
b. Orang tua dan keluarga penulis yang telah memberikan bantuan dukungan moral dan material; dan
c. Sahabat dan teman-teman 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.

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. [5] Malhotra, Aman. Rawat, Lakshya. Kumar, Lokesh. 2020. MINI SECURITY OPERATIONS CENTER USING ELK.