



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



**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 : 

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :

a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.  
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta

2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta





Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :

a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.

b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta

2. Dilarang mengumumkannya dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

## 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





**Hak Cipta :**

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :

a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.

b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta

2. Dilarang mengummumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

## 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\*: .....

demikian 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

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :

a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritis atau tinjauan suatu masalah.

b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta

2. Dilarang mengummumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta





## 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 seperti 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*

POLITEKNIK  
NEGERI  
JAKARTA

#### Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :

a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.

b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta

2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun

tanpa izin Politeknik Negeri Jakarta



## DAFTAR ISI

<b>HALAMAN PERNYATAAN ORISINALITAS .....</b>	<b>ii</b>
<b>LEMBAR PENGESAHAN .....</b>	<b>iii</b>
<b>KATA PENGANTAR.....</b>	<b>iv</b>
<b>PERNYATAAN PERSETUJUAN PUBLIKASI.....</b>	<b>v</b>
<b>ABSTRAK .....</b>	<b>vi</b>
<b>DAFTAR ISI.....</b>	<b>vii</b>
<b>DAFTAR GAMBAR.....</b>	<b>x</b>
<b>DAFTAR TABEL.....</b>	<b>xii</b>
<b>BAB I.....</b>	<b>13</b>
<b>PENDAHULUAN.....</b>	<b>13</b>
1.1 Latar Belakang .....	13
1.2 Perumusan Masalah .....	13
1.3 Batasan Masalah.....	14
1.4 Tujuan dan Manfaat .....	14
1.5 Metode Pelaksanaan Skripsi .....	15
<b>BAB II .....</b>	<b>16</b>
<b>TINJAUAN PUSTAKA .....</b>	<b>16</b>
2.1 Tinjauan Pustaka .....	16
2.1.1 Vulnerability Scanning.....	16
2.1.2 Wazuh .....	16
2.1.3 Winlogbeat.....	17
2.1.4 Jaringan Komputer .....	17
2.1.5 Monitoring Jaringan .....	18
2.1.6 Brute Force.....	18
2.1.7 Vmware .....	18
2.1.8 Linux .....	19
2.1.9 Kali Linux .....	19
2.1.10 SIEM .....	19
2.1.11 Elastic SIEM .....	20
2.2 Penelitian Sejenis .....	23
2.2.1 Alpauji, Aldi (2021).....	23
2.2.2 Admi, A., & Maulana, A. H. N. (2020) .....	24

### Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta





Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

2.2.3 Handika, Vian (2020).....	24
<b>BAB III.....</b>	<b>25</b>
<b>PERANCANGAN DAN REALISASI .....</b>	<b>25</b>
3.1 Perancangan Program.....	25
3.1.1 Flowchart Pengerjaan Penelitian .....	25
3.1.2 Topology Jaringan .....	26
3.2 Skenario Pengujian.....	27
3.3 Tahap Pengujian.....	27
3.3.1 Basic Attack .....	27
3.3.2 Deteksi Agent.....	27
3.3.3 Mengirim Log Wazuh .....	27
3.3.4 Mengirim Log Winlogbeat.....	28
3.3.5 Visualisasi Log Wazuh Dan Winlogbeat .....	28
3.4 Realisasi Sistem .....	28
3.4.1 SIEM.....	28
3.4.2 Instalasi dan konfigurasi Elasticsearch.....	29
3.4.3 Instalasi dan konfigurasi Logstash .....	32
3.4.4 Instalasi dan konfigurasi Kibana .....	33
3.4.5 Instalasi Wazuh.....	35
3.4.6 Instalasi Winlogbeat .....	36
<b>BAB IV .....</b>	<b>38</b>
<b>PEMBAHASAN .....</b>	<b>38</b>
4.1 Skema Pengujian.....	38
4.2 Pengujian.....	39
4.2.1 Vulnerability Scanning menggunakan tool Nmap.....	39
4.2.2 Pengujian menggunakan tool Metasploit.....	40
4.2.3 Pengujian menggunakan tool Hydra.....	43
4.2.4 Pengujian dengan menambahkan user.....	45
4.2.5 Pengujian dengan menghapus user .....	46
4.3 Hasil Pengujian .....	47
<b>BAB V.....</b>	<b>48</b>
<b>PENUTUP.....</b>	<b>48</b>
5.1 Kesimpulan .....	48
5.2 Saran.....	48



DAFTAR PUSTAKA .....	49
DAFTAR RIWAYAT HIDUP PENULIS .....	50



© Hak Cipta milik Politeknik Negeri Jakarta

**Hak Cipta :**

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta





## DAFTAR GAMBAR

Gambar 2.1 Wazuh.....	16
Gambar 2.2 Alur kerja Elastic Stack.....	20
Gambar 2.3 Cluster Elasticsearch .....	21
Gambar 2.4 Prospector.....	23
Gambar 3.1 Flowchart Pengerjaan dan Pengujian Sistem.....	25
Gambar 3.2 Topologi Jaringan.....	26
Gambar 3.3 Instalasi Elasticsearch .....	29
Gambar 3.4 Konfigurasi IP Elasticsearch .....	29
Gambar 3.5 Service Elasticsearch.....	30
Gambar 3.6 Proses Verifikasi .....	31
Gambar 3.7 Otomatisasi Service.....	31
Gambar 3.8 Instalasi Logstash .....	32
Gambar 3.9 Service Logstash .....	32
Gambar 3.10 Instalasi Kibana.....	33
Gambar 3.11 Konfigurasi IP Kibana.....	33
Gambar 3.12 Service Kibana .....	34
Gambar 3.13 Web Kibana.....	34
Gambar 3.14 Proses instalasi wazuh.....	35
Gambar 3.15 Proses menjalankan service wazuh .....	35
Gambar 3.16 Proses intallasi winlogbeat .....	36
Gambar 3.17 Konfigurasi output winlogbeat.....	36
Gambar 3.18 Start service winlogbeat .....	37
Gambar 4.1 Skema pengujian .....	38
Gambar 4.2 Nmap.....	40
Gambar 4.3 Auxiliary module.....	40
Gambar 4.4 Konfigurasi module auxiliary.....	41
Gambar 4.5 Proses serangan bruteforce .....	41
Gambar 4.6 Discover wazuh .....	42
Gambar 4.7 Dashboard wazuh .....	42
Gambar 4.8 Wordlist Username and Password.....	43
Gambar 4.9 Hydra Attack .....	43
Gambar 4.10 Discover Wazuh Detected Hydra Attack .....	44

### Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Gambar 4.11 Dashboard Wazuh Detected Hydra Attack .....	44
Gambar 4.12 create user.....	45
Gambar 4.13 Discover winlogbeat.....	45
Gambar 4.14 Delete user.....	46
Gambar 4.15 Discover winlogbeat.....	46



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan Laporan, penulisan kritik atau tinjauan satu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



## DAFTAR TABEL

Tabel 1 Hasil Pengujian ..... 47



**Hak Cipta :**

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta





## 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 berkembang 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 negeri, 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 terinstall pada *server*.

#### Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :

a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.

b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta

2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun

tanpa izin Politeknik Negeri Jakarta



**Hak Cipta :**

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkannya dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

- 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 telah 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 menyelesaikan 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.



© Hak Cipta milik Politeknik Negeri Jakarta

#### Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkannya dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

## 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. *About 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. & Najoran. 2016, Analisa dan Implementasi *Network Intrusion Prevention* Sistem di Jaringan Universitas Sam Ratulangi.
- Nur, Siti. & Jamu, Sandra. 2019. Rancangan Virtualisasi Server Menggunakan VMWare Vsphere.
- 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.

### Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkannya dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



## © Hak Cipta milik Politeknik Negeri Jakarta

### Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

