PENERAPAN KEAMANAN SERVER MENGGUNAKAN SECURITY INFORMATION EVENT AND MANAGEMENT PADA SISTEM OPERASI UBUNTU SERVER

Maulana Alhif Ikhsan; Bana Handaga
Prodi Teknik Informatika, Fakultas Komunikasi dan Informatika, Universitas Muhammadiyah Surakarta

Abstrak

Seiring dengan berkembangnya teknologi yang mengharuskan keamanan pada perangkat server menjadi sebuah kewajiban yang harus diperhatikan. Dalam upaya untuk melindungi sebuah server yang terdapat pada Batalyon Arhanud 14/PWY Cirebon belum cukup jika hanya menggunakan teknik hardening pada perangkat saja. Mengacu pada framework security seperti NIST terdapat 5 hal yang perlu diperhatikan yaitu identify, protect, detect, respond, dan recovery. Pada Batalyon Arhanud 14/PWY Cirebon hanya menerapkan protect saja dengan menggunakan teknik hardening pada perangkat server. Kurangnya monitoring pada perangkat server menyebabkan adanya aktifitas mencurigakan yang disebabkan oleh faktor internal ataupun eksternal. Upaya dalam menangani masalah ini adalah dengan menerapkan teknologi SIEM (Security Information Event and Management) yang terdapat metode IDS (Intrusion Detection System) berfungsi sebagai pendeteksi ancaman secara realtime pada perangkat server dengan sistem operasi Ubuntu Server. Pada penelitian ini menggunakan ELK (Elasticsearch, Logstash, Kibana) dan Auditbeat yaitu perangkat yang dapat melakukan log management dengan visualisasi untuk mempermudah melakukan analisa. Pengujian ini dilakukan dengan berfokus pada penyerangan pada service SSH dan FTP. Proses pengujian tersebut menggunakan metode Brute Force. Metode penelitian ini adalah eksperimental yang meliputi identifikasi, analisa kebutuhan, desain, implementasi, pengujian dan evaluasi. Berdasarkan hasil pengujian dari penerapan penelitian ini, SIEM dapat mendeteksi adanya serangan yang telah dilakukan pada proses pengujian seperti pada service SSH dan FTP melalui log file dan divisualisasikan oleh Kibana secara realtime.

Kata Kunci: SIEM**,** Elasticsearch, Logstash, Kibana, Server, Ubuntu.

Abstract

Along with the development of technology that requires security on server devices is an obligation that must be considered. In an effort to protect a server contained in the Arhanud 14/PWY Cirebon Battalion, it is not enough to only use hardening techniques on the device. Referring to a security framework such as NIST, there are 5 things that need attention: identify, protect, detect, respond, and recover. The Arhanud 14/PWY Cirebon Battalion only applied for protection by using

hardening techniques on server devices. Lack of monitoring on server devices causes suspicious activity caused by internal or external factors. The effort to deal with this problem is to apply SIEM (Security Information Event and Management) technology in which the IDS (Intrusion Detection System) method functions as a real-time threat detector on server devices with the Ubuntu Server operating system. This study uses ELK (Elasticsearch, Logstash, Kibana) and Auditbeat, which are devices that can perform log management with visualization to make analysis easier. This test was carried out by focusing on attacks on SSH and FTP services. The testing process uses the Brute Force method. This experimental research method includes identification, needs analysis, design, implementation, testing, and evaluation. Based on the test results from the application of this study, SIEM can detect attacks that have been carried out in the testing process such as SSH and FTP services through log files and visualized by Kibana in real-time.

Keywords: SIEM, Elasticsearch, Logstash, Kibana, Server, Ubuntu.

1. PENDAHULUAN

Perkembangan teknologi informasi sudah menjadi peran penting dalam kehidupan sehari-hari. Hal ini tentu tidak datang tanpa adanya bahaya, yaitu berbagai kegiatan jahat yang dapat berdampak pada suatu instansi ataupun perusahaan (Jokić et al., 2021). Kebutuhan keamanan jaringan komputer telah menjadi bagian penting untuk menjaga keamanan data dengan memprioritaskan *confidentiality*, *integrity*, dan *availability.* Serangan ke dalam server jaringan komputer bisa terjadi kapan saja dan oleh siapa saja, maka diperlukan adanya pendeteksian serta monitoring terhadap keamanan server jaringan komputer secara realtime untuk mempermudah seorang security analyst untuk menganalisa lalu lintas yang mencurigakan (Alamsyah et al., 2020).

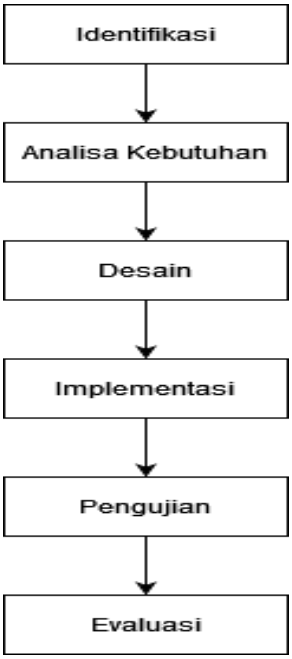
Penerapan keamanan keamanan pada instansi atau perusahaan sebagian besar hanya menggunakan firewall pada endpoint yang digunakan. Namun perlindungan dengan menggunakan firewall tidak cukup, karena firewall hanya melindungi koneksi inbound dan outbound. Selain itu, firewall tidak dapat melakukan deteksi jika terjadi suatu serangan (Ari Setiawan & Tria Putra Abza, 2020). Hal ini dapat dibantu dengan menerapkan SIEM (Security Information Event and Management) sebagai sistem monitoring yang dapat mendeteksi dan merespon serangan dengan melalui analisis log dari event-log seperti IDS, IPS ataupun server secara realtime (ARFANUDIN et al., 2019). Pengujian pada sistem ini yaitu melakukan serangan langsung seperti FTP

Attack dan SSH Attack. Kegagalan saat melakukan login pada FTP dan SSH dapat terdeteksi oleh sistem yang akan disimpan pada log file dan ditampilkan oleh Kibana.

Pada penelitian ini memanfaatkan sebuah software yaitu Elasticsearch, Logstash, Kibana (ELK) sebagai sistem monitoring yang menerapkan sentralisasi pada setiap node. ELK juga merupakan software yang berbasis open source dengan setiap softwarenya terdistribusi satu dengan yang lainnya. Elasticsearch yang merupakan software yang berfungsi sebagai mesin pencari yang terdistribusi. Logstash berfungsi untuk mengumpulkan, mengelola data log yang kemudian dilakukan penyaringan serta memproses data log sesuai dengan kebutuhan. Kibana berfungsi sebagai software visualisasi data log berupa web interface. Dengan menggunakan ELK, suatu instansi atau perusahaan dapat melakukan monitoring pada setiap node (endpoint) serta melakukan deteksi dan respon terhadap segala jenis serangan (Sholihah et al., 2020). Adapun instansi yang ambil dalam penelitian ini adalah Batalyon Arhanud 14/PWY Cirebon. Instansi negara yang bergerak dalam bidang pertahanan ini memiliki divisi cyber dengan nama Cangehgar Cyber Operation Center. Adanya server pada divisi cyber, dapat membuat instansi ini melakukan komunikasi data secara lebih cepat. Pada penelitian ini juga berharap agar divisi cyber dapat selalu memonitoring dan menganalisa server yang sedang berjalan. Pengujian sistem terhadap keamanan menjadi langkah terpenting dalam mengetahui seberapa aman sistem yang sudah menerapkan SIEM. Dalam pengujian ini diharapkan SIEM yang sudah diterapkan mampu mengidentifikasi dan memberikan peringatan tanpa adanya kecacatan.

2. METODE

Metode yang digunakan untuk menyusun penelitian "Penerapan Keamanan Server Menggunakan Security Information Event and Management Pada Sistem Operasi Ubuntu Server" yaitu menggunakan metode eksperimental. Metode eksperimental merupakan metode untuk menguji dan mengetahui keadaan dari suatu sistem yang sedang digunakan dengan pengujian yang berbeda-beda (ROMADHON, WAHYU DWI and , Devi Afriyantari Puspa Putri, S.Kom., 2021). Berikut alur penelitian dapat dilihat pada Gambar 1.



Gambar 1. Alur Penelitian Eksperimental

2.1 Identifikasi

Pada tahap ini terdapat sistem yang sedang berjalan pada server Batalyon Arhanud 14/PWY yaitu FTP Server. FTP digunakan untuk melakukan komunikasi data atau pertukaran file dengan mudah antar divisi. Penggunaan FTP server hanya digunakan oleh dua divisi saja yaitu Divisi Cyber dan Divisi Intelijen. Permasalahan pada server ini terdapat kekurangan pada sisi keamanan seperti firewall, antivirus dan tidak ada log management (monitoring). Namun penelitian ini akan berfokus pada monitoring log menggunakan teknologi SIEM dengan tools ELK Stack. Pada FTP, dapat terjadi penyerangan berupa FTP dengan memanfaatkan credential "*anonymous/anonymous"*. Hal tersebut dapat terjadi apabila mengaktifkan fitur mengizinkan mengakses melalui akun anonymous. Permasalahan tersebut akan dijelaskan pada tahap selanjutnya dengan menerapkan SIEM atau Security Information Event and Management dengan menggunakan Elasticsearch, Logstash, Kibana (ELK Stack) yang dapat berjalan pada server yang ada dengan spesifikasi processor 2 CPU, memory 4GB, disk 80GB, dan sistem operasi Ubuntu Server 20.04 dengan menggunakan layanan cloud computing.

2.2 Analisa Kebutuhan

Pada penelitian ini akan berfokus pada penerapan dan pengembangan sistem monitoring yang mengadaptasikan teknologi SIEM atau Security Information Event and Management menggunakan tools berupa ELK Stack (Elasticsearch, Logstash,

Kibana) dengan penambahan file berupa Beats dan dibantu oleh agent yang telah dipasang pada server (node). Penggunaan ELK diharapkan mampu menjalankan *system monitoring log* saat terjadinya suatu serangan seperti serangan *FTP attack* dan *SSH attack* (Agrawal et al., 2018). Dengan memanfaatkan IDS dan log management untuk meminimalisir adanya kecacatan alert berupa *false-positive* ataupun *false-negative.* Berikut analisa kebutuhan yang akan digunakan pada penelitian ini.

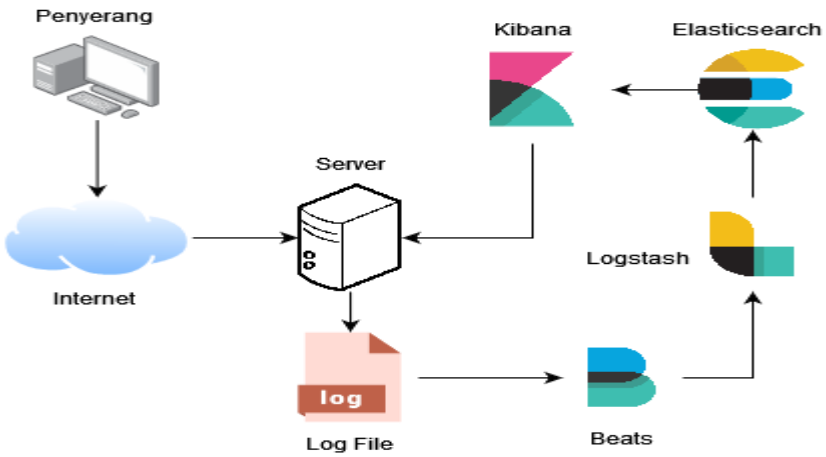
Tabel 1. Analisa Kebutuhan

No.	Perangkat Lunak	Keterangan
1.	Ubuntu Server 20.04	Komputer server yang digunakan sebagai server
2.	ELK	Tools yang digunakan untuk mendistribusikan, mengolah dan memvisualisasikan log
3.	Hydra	Tools yang dapat melakukan brute force terhadap layanan FTP dan SSH

Perangkat lunak yang dibutuhkan untuk implementasi SIEM dan proses pengujian tersebut dijelaskan pada Tabel 1. Proses instalasi, konfigurasi untuk ELK akan dijelaskan pada Tabel 2 dan proses penggunaan Hydra untuk proses pengujian akan dijelaskan pada Bab 3.

2.3 Desain

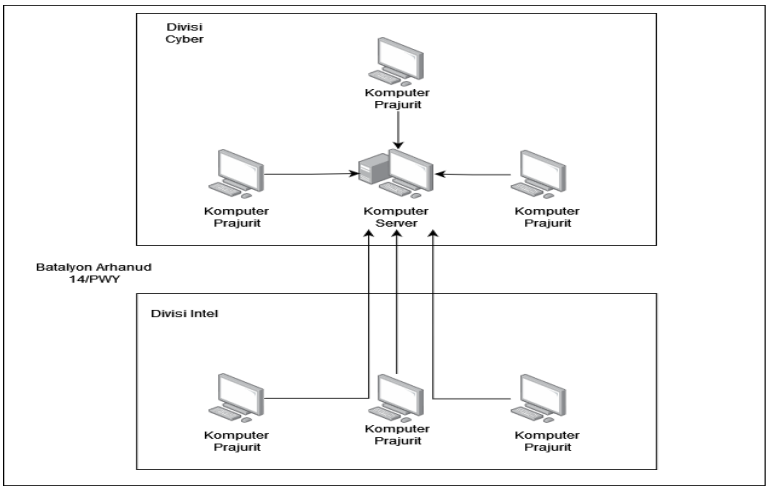
Tahapan desain adalah tahapan yang menggambarkan bagaimana langkah-langkah dari sistem yang akan dibuat. Berikut skema sistem yang dibuat pada Gambar 2.



Gambar 2. Skema sistem

Skema pada Gambar 2, menggambarkan bagaimana sistem ini bekerja. Sistem monitoring yang digunakan pada penelitian ini adalah ELK Stack (Elasticsearch, Logstash, Kibana) dan Auditbeat yang dipasang pada komputer server dengan sistem operasi Ubuntu Server untuk monitoring lalu lintas jaringan (*Host*). Pengujian sistem deteksi yang sudah dipasang akan dilakukan dengan metode bruteforce yang berfokus pada FTP Attack dan SSH Attack. Pemilihan metode tersebut berdasarkan pengujian serangan yang telah dilakukan pada Batalyon Arhanud 14/PWY Cirebon sebelumnya dan terdapat kesalahan dalam konfigurasi FTP yang menyebabkan penyerang dapat masuk ke dalam system (FTP) dengan menggunakan kredensial “anonymous” dan log tersebut tersimpan pada file /var/log/vstfpd.log (Putra & Alghozy, 2022). Permasalahan ini muncul karena log pada server hanya berupa command line dan itu menyulitkan untuk melakukan monitoring. Setelah dilakukan pemasangan SIEM, serangan tersebut dapat dibaca oleh administrator karena sudah tervisualisasikan untuk setiap serangan yang masuk. Menganalisa log dapat meminimalisir adanya potensi peretasan karena sudah mengetahui apa yang sedang dilakukan oleh penyerang dengan memanfaatkan log file yang sudah tervisualisasikan pada dashboard Kibana. Namun sebelum tervisualisasi, log akan dikirim oleh Beats (Auditbeat) ke Logstash untuk dilakukan pengumpulan dan parsing data sebelum dilakukan indexing oleh Elasticsearch dan visualisasi oleh Kibana untuk dilakukan monitoring oleh administrator (Irma Anggraeni, 2022).

2.4 Implementasi



Gambar 3. Arsitektur Jaringan

Penjelasan pada Gambar 3. yang merupakan artisektur jaringan yang digunakan pada Batalyon Arhanud 14/PWY dengan Komputer Server yang menjadi pusat dari pengiriman data yang keluar dan masuk antar divisi. Pada Komputer Server terdapat service FTP dan SSH yang berjalan dengan sistem operasi Ubuntu Server. Komunikasi ini terjalin karena adanya pertukaran dokumen yang penting melalui FTP antara client (komputer prajurit) ke server (komputer server) agar memudahkan prajurit dalam mengirimkan data antar divisi tanpa harus melakukan kontak fisik seperti memberikan *flash drive* atau *harddisk*. Setiap prajurit yang akan mengakses ke komputer server hanya perlu menggunakan kredensial yang sudah diberikan yaitu dengan username "cyber" dan password "cangehgar14". Namun pada saat melakukan *penetration testing* yang telah dilakukan sebelumnya,s terdapat adanya celah keamanan yang dapat dimanfaatkan dengan menggunakan kredensial "*anonymous*" pada *username* dan *password*. Kredensial tersebut merupakan kredensial dasar yang sudah ada pada service FTP termasuk pada *VSFTPD* ataupun *ProFTP*. Modul tersebut seharusnya tertutup, namun terbuka karena administrator hanya mengikuti tutorial yang terdapat pada internet tanpa mengetahui maksud yang disampaikan oleh tutorial tersebut.

2.5 Instalasi ELK

Instalasi dan konfigurasi ELK beserta agent yang digunakan dapat dilihat pada Tabel 2.

Tabel 2. Instalasi ELK Stack

Software	Instalasi	Tempat File Konfigurasi
Elasticsearch	*sudo apt install elasticsearch*	*vim /etc/elasticsearch/elasticsearch.yml*
Kibana	*sudo apt install kibana*	*vim /etc/kibana/kibana.yml*
Logstash	*sudo apt install logstash*	*vim /etc/logstash/logstash.yml*
Beats/Auditbeat	*sudo apt install auditbeat*	*vim /etc/auditbeat/auditbeat.yml*

Hasil instalasi dan konfigurasi yang telah dilakukan pada Tabel 2, akan dijelaskan pada Bab 3 beserta hasil implementasi dan proses pengujiannya.

2.6 Pengujian Sistem

Menguji sistem dilakukan untuk mengetahui kinerja sistem IDS yang terdapat pada SIEM dalam mendeteksi adanya serangan. Dengan memastikan kinerja IDS, seorang administrator dapat menganalisa jalannya traffic yang masuk dan keluar melalui log.

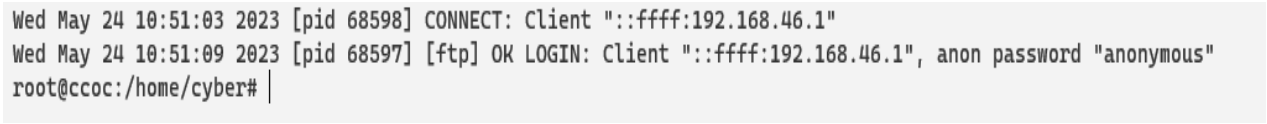
Administrator harus memastikan IDS harus berjalan dan meminimalisir adanya kecacatan seperti *false-positive* ataupun *false-negative*. Maka pada pengujian kali ini, akan dilakukan beberapa pengujian seperti *SSH Attack* dan *FTP Attack.* Penelitian ini akan berfokus pada sisi pendeteksi serta monitoring log yang akan divisualisasikan oleh Kibana pada web interface. Berikut jenis-jenis serangan yang dilakukan:

2.6.1 FTP Attack

FTP merupakan protocol yang digunakan untuk melakukan transfer file antar client-server. Proses pengujian pada FTP attack akan dilakukan dengan 2 metode yaitu dengan kredensial "anonymous" dan *bruteforce* dengan *wordlist* yang sudah disediakan diantaranya "*cyber, admin, superadmin, toor, root, cangehgar, Cangehgar2122, TNIJuara, Arhanud12345*"(Komang et al., 2020).

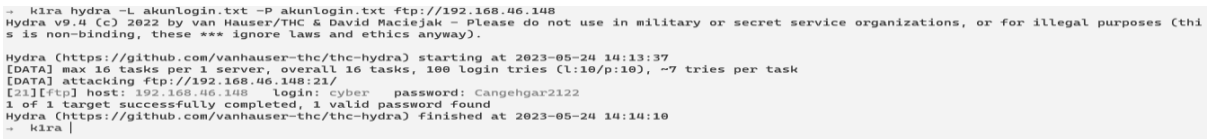
Gambar 4. Anonymous Attack

Gambar 4. merupakan salah satu langkah exploitasi yang dapat dilakukan untuk menguji service FTP dengan memanfaatkan kesalahan konfigurasi yang dilakukan oleh administrator yang tidak melakukan blocking untuk akun "*anonymous*". Dapat dilihat bahwa *exploitasi* tersebut berhasil dan masuk ke dalam *server* dengan menggunakan kredensial "*anonymous*".



Gambar 5. Log Kredensial Anonymous

Pengujian yang telah dilakukan dengan menggunakan kredensial "anonymous" tercatat pada log file /var/log/vsftpd.log seperti pada Gambar 5. Log file tersebut mencatat seluruh aktifitas yang masuk melalui service FTP secara realtime.



Gambar 6. Brute Force Attack FTP

Pada Gambar 6. terdapat command untuk melakukan *Brute Force* dengan menggunakan *tools Hydra*. *Command* tersebut adalah "*hydra -L akunlogin.txt -P akunlogin.txt ftp://192.168.46.148*". Opsi pada *command* tersebut adalah -L untuk *login (username)* dengan menggunakan *wordlist* dan -P untuk *password* dengan menggunakan *wordlist*, sedangkan untuk *ftp://192.168.46.148* merupakan *service* yang dituju beserta *host*. Proses pengujian ini dilakukan dengan memanfaatkan celah pada hardening yang tidak diterapkan dengan mengaktifkan fitur *firewall* atau fitur yang dapat melakukan *blocking* apabila terjadi kesalahan sebanyak 3x. Maka penyerang dapat melakukan serangannya terus menerus hingga menemukan kredensial yang sesuai.

```
Wed May 24 14:13:42 2023 [pid 91037] CONNECT: Client "::ffff:192.168.46.1"
Wed May 24 14:13:42 2023 [pid 91038] CONNECT: Client "::ffff:192.168.46.1"
Wed May 24 14:13:42 2023 [pid 91016] [cyber] OK LOGIN: Client "::ffff:192.168.46.1"
Wed May 24 14:13:43 2023 [pid 91040] CONNECT: Client "::ffff:192.168.46.1"
Wed May 24 14:13:43 2023 [pid 91015] [cyber] FAIL LOGIN: Client "::ffff:192.168.46.1"
Wed May 24 14:13:44 2023 [pid 91041] CONNECT: Client "::ffff:192.168.46.1"
Wed May 24 14:13:44 2023 [pid 91042] CONNECT: Client "::ffff:192.168.46.1"
```

Gambar 7. Log Brute Force FTP

Gambar 7. menunjukkan kredensial apa saja yang dicoba dalam melakukan pengujian serangan menggunakan metode *Brute Force* pada service FTP. *Log file* tersebut mencatat semua upaya *Brute Force* dengan hasil *fail* ataupun *success*. Hal ini menunjukkan bahwa setiap aktivitas akan direkam atau dicatat ke dalam log file sebagai jejak yang harus diperhatikan oleh seorang *Attacker* atau *Hacker* dalam melakukan suatu tindakan yang melanggar etika.

2.6.2 SSH Attack

SSH menjadi salah satu protokol yang dapat melakukan kontrol dan modifikasi terhadap *server* dari jarak jauh. Pengujian ini diperlukan untuk mengetahui seberapa banyak upaya untuk masuk ke dalam *server* dengan menggunakan metode *Brute Force*. Pada pengujian ini akan dilakukan dengan menggunakan *tools* bernama *Hydra* dengan *wordlist "cyber, admin, superadmin, toor, root, cangehgar, Cangehgar2122, TNIJuara, Arhanud12345"* (Park et al., n.d.).

```
→  k1ra hydra -L akunlogin.txt -P akunlogin.txt ssh://192.168.46.148
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (thi
s is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-24 14:28:41
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (l:10/p:10), ~7 tries per task
[DATA] attacking ssh://192.168.46.148:22/
[22][ssh] host: 192.168.46.148   login: cyber   password: Cangehgar2122
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-05-24 14:29:16
→  k1ra
```

Gambar 8. Brute Force Attack SSH

Pengujian pada Gambar 7. terlihat proses exploitasi tersebut berhasil dan mendapatkan kredensial untuk melakukan login melalui service SSH yaitu dengan username “cyber” dan *password “Cangehgar2122”*. Kedua proses pengujian SSH dan FTP hingga mendapatkan kredensial yaitu dikarenakan *wordlist* yang digunakan terdapat potensi

```
May 24 14:28:45 ccoc sshd[91760]: Invalid user admin from 192.168.46.1 port 29084
May 24 14:28:45 ccoc sshd[91757]: pam_unix(sshd:auth): check pass; user unknown
May 24 14:28:45 ccoc sshd[91757]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.46.1
May 24 14:28:45 ccoc systemd-logind[1001]: New session 43 of user cyber.
May 24 14:28:45 ccoc sshd[91765]: Invalid user admin from 192.168.46.1 port 29092
May 24 14:28:45 ccoc sshd[91760]: pam_unix(sshd:auth): check pass; user unknown
May 24 14:28:45 ccoc sshd[91760]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.46.1
May 24 14:28:45 ccoc sshd[91765]: pam_unix(sshd:auth): check pass; user unknown
May 24 14:28:45 ccoc sshd[91765]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.46.1
May 24 14:28:45 ccoc sshd[91734]: Failed password for cyber from 192.168.46.1 port 29046 ssh2
May 24 14:28:46 ccoc sshd[91741]: Failed password for cyber from 192.168.46.1 port 29008 ssh2
May 24 14:28:46 ccoc sshd[91737]: Failed password for cyber from 192.168.46.1 port 29070 ssh2
```

Gambar 9. Log File Brute Force SSH

Log file pada /var/log/auth.log yang mencatat segala aktifitas pada SSH telah menyimpan catatan dari aktivitas Brute Force yang telah dilakukan pada pengujian SSH Attack dan terdapat log yang menjelaskan bahwa proses pengujian tersebut gagal menggunakan kombinasi kredensial yang ada pada wordlist. Log file juga mencatat yang berhasil masuk ke service SSH dengan menggunakan kombinasi dari wordlist yang sudah dibuat dengan menambahkan session baru untuk membuktikan hasil kombinasi tersebut benar atau tidak seperti pada Gambar 8.

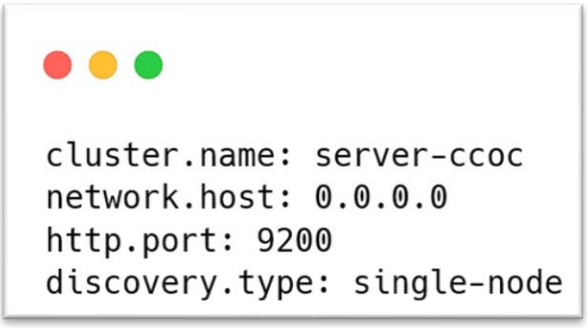
3. HASIL DAN PEMBAHASAN

3.1 Hasil Implementasi

Berdasarkan proses pengujian sistem yang telah dilakukan pada bab sebelumnya dengan menggunakan menyerang service FTP dan SSH dengan metode pengujian menggunakan Brute Force diketahui bahwa setiap serangan ataupun aktivitas lainnya akan tercatat oleh sistem dan disimpan pada log file masing-masing service seperti SSH *(/var/log/auth.log)* dan FTP *(/var/log/vsftpd.log)* dengan catatan waktu secara realtime. Kedua log file tersebut akan terbaca oleh sistem monitoring atau SIEM yang telah dirancang sebelumnya. Pembahasan pada bab ini akan berfokus pada sistem monitoring tersebut dengan membahas mengenai konfigurasi dan tampilan dari deteksi menggunakan Kibana yang telah dilakukan pada proses pengujian.

3.1.1 Konfigurasi Elasticsearch

Sebelum menyimpan, menampilkan, mengolah suatu log diperlukan konfigurasi yang dapat digunakan untuk mengatur jalannya Elasticsearch dalam menjalankan tugasnya. Berikut konfigurasi Elasticsearch :



Gambar 10. Konfigurasi Elasticsearch

Elasticsearch membutuhkan konfigurasi agar dapat berjalan dengan baik dan terhubung antar aplikasi lain (Kibana, Auditbeat, dan Logstash). Seperti pada Gambar 9. terdapat beberapa *environment* penting yang perlu diperhatikan yaitu *cluster.name* (tempat berkumpulnya node-node yang terdapat pada Elasticsearch), *network.host* (digunakan untuk menentukan alamat IP atau host), *http.port* (port yang digunakan untuk menjalankan Elasticsearch), *discovery.type* (pengaturan untuk menentukan mekanisme discovery).

3.1.2 Konfigurasi Kibana

Agar Kibana dapat berjalan dengan baik, maka diperlukan konfigurasi yang dapat terintegrasi dengan Elasticsearch seperti elasticsearch.hosts.

Gambar 11. Konfigurasi Kibana

Konfigurasi yang terdapat pada Kibana digunakan untuk integrasi antara Kibana dengan Elasticsearch untuk visualisasi yang telah dilakukan oleh Elasticsearch seperti yang telah dijelaskan pada arsitektur yang terdapat pada Gambar 2, namun pada Gambar 10.

terdapat *environment* yang perlu diperhatikan seperti *server.port* (port untuk menjalankan Kibana), *server.host* (alamat IP atau host yang digunakan), *elasticsearch.hosts* (host yang digunakan Elasticsearch), *elasticsearch.username* (username pada Elasticsearch), *elasticsearch.password* (password pada Elasticsearch).

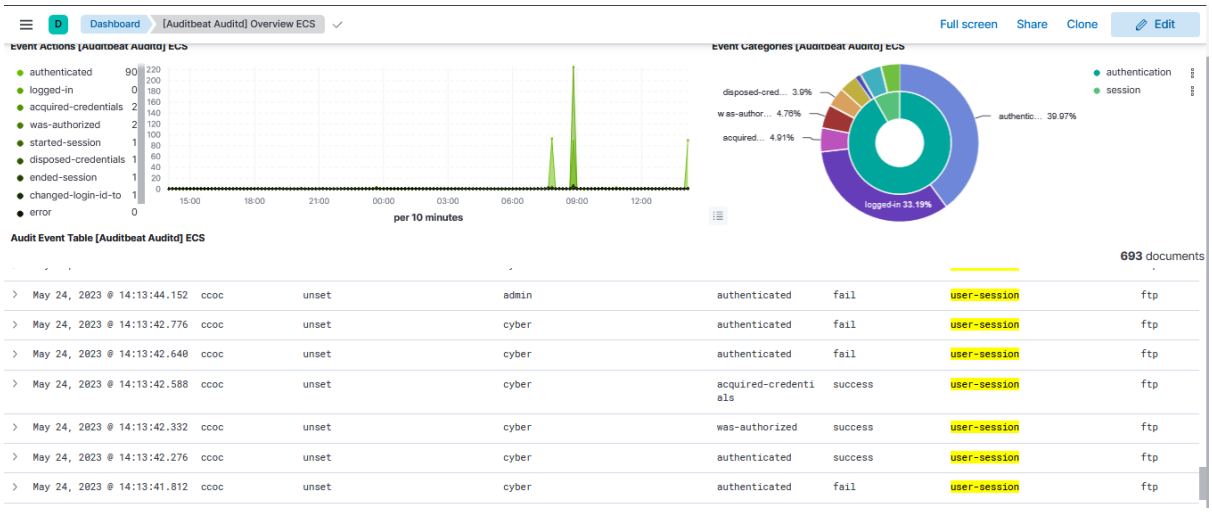
3.2 Hasil Simulasi Serangan

Pada proses pengujian sistem dengan metode serangan *Brute Force* pada service SSH dan FTP terdapat situasi *false-negative* yaitu pada proses pengujian dengan menggunakan metode yang memanfaatkan kredensial "*anonymous*" pada service FTP tidak mendeteksi adanya serangan. SIEM tidak melakukan visualisasi untuk serangan tersebut dengan baik, namun pada log file yang terdapat pada */var/log/vsftpd.log* mencatat bahwa ada aktivitas yang masuk ke dalam sistem dengan menggunakan kredensial "*anonymous*" seperti pada Gambar 5. Untuk proses pengujian lain seperti *Brute Force*, SIEM atau sistem monitoring dapat melakukan visualisasi dengan baik seperti memberikan informasi untuk serangan tersebut berhasil atau tidak, informasi mengenai actor (username), ataupun timestamp. Berikut hasil visualisasi setelah proses pengujian sistem pada service FTP dan SSH:

3.2.1 FTP

Hasil serangan yang telah dilakukan pada service FTP dengan metode *Brute Force* dan *wordlist "cyber, admin, superadmin, toor, root, cangehgar, Cangehgar2122, TNIJuara, Arhanud12345"* mendapatkan hasil yang kurang baik karena adanya kecacatan berupa *false-negative* yang merupakan kegagalan sistem dalam mendeteksi adanya serangan. Serangan tersebut merupakan serangan yang memanfaatkan kredensial "*anonymous*". Kecacatan tersebut terjadi karena sistem monitoring tidak memvisualisasikan data yang terdapat pada log file *"/var/log/vsftpd.log"* yang telah mencatat serangan kredensial "*anonymous*" namun dapat memvisualisasikan aktivitas dengan kredensial lainnya selain menggunakan "*anonymous*". Dalam melakukan remediasi untuk menanggulangi kecacatan tersebut dapat dilakukan dengan mengubah "anonymous_enable=YES" menjadi "NO" pada file "/etc/vsftpd.conf". Serangan yang dilakukan dengan menggunakan metode *Brute Force* dapat tervisualisasikan dengan data yang telah diparsing oleh Logstash dan *indexing* oleh Elasticsearch melalui Kibana. Data tersebut meliputi timestamp, actor, action, type, dan result. Hal tersebut memudahkan

administrator dalam menganalisa suatu insiden ataupun peristiwa yang masuk ke dalam sistem yang telah mencatat seluruhnya ke dalam log file.

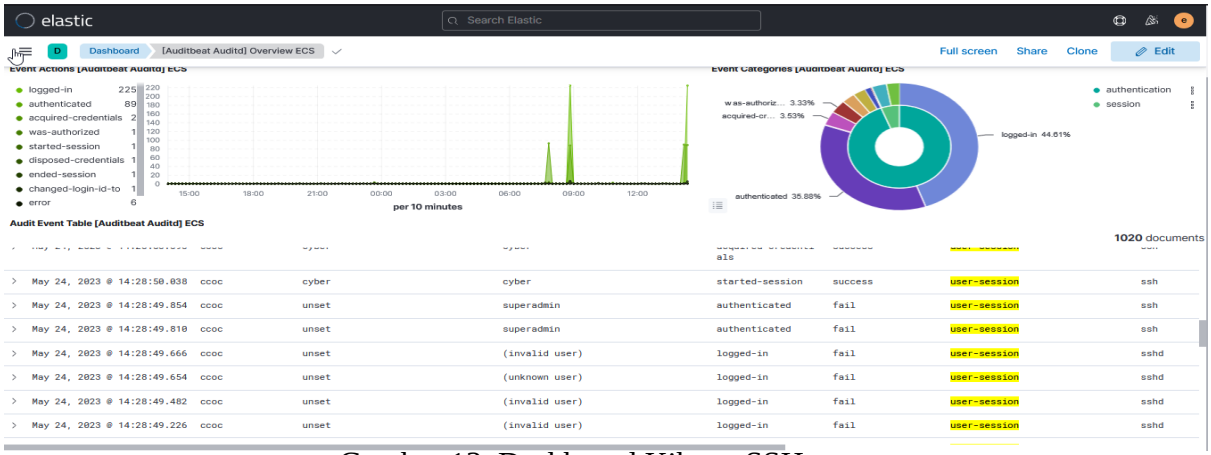


Gambar 12. Dashboard Kibana FTP

Pada Gambar 11. data yang terdapat pada log file "/var/log/vsftpd.log" telah tervisualisasikan di Kibana dengan memberikan informasi berupa timestamp, agent name (nama server), actor, type dan result. Hasil dari pengujian sistem dengan menggunakan metode *Brute Force* juga tercatat dan tervisualisasikan baik *fail* ataupun *success*.

3.2.2 SSH

Berbeda dengan hasil proses pengujian pada service FTP sebelumnya, SSH memiliki hasil deteksi yang tanpa adanya kecacatan seperti *false-positive* ataupun *false-negative*. Hasil tersebut sesuai dengan catatan pada log file dan tevisualisasikan oleh Kibana.



Gambar 13. Dashboard Kibana SSH

Berbeda dengan FTP yang terdapat pada Gambar 11. SSH memiliki perbedaan dalam hal penamaan service seperti pada Gambar 12. yaitu SSH dan SSHd. Hal tersebut berbeda karena SSH merupakan sebuah protokol, dan SSHd adalah sebuah program server yang menjalankan protokol SSH dan menerima koneksi dari klien.

Informasi mengenai tabel-tabel yang terdapat pada Dashboard Kibana akan dijelaskan pada Tabel 3.

Tabel 3. Dashboard Kibana

No	Nama	Deskripsi
1	Time	Waktu pada saat terdeteksi
2	auditd.summary.actor.primary	Nama akun yang digunakan untuk percobaan penyerangan
3	auditd.summary.actor.secondary	Nama akun yang digunakan untuk percobaan penyerangan
4	event.action	Aksi pada proses penyerangan
5	auditd.summary.object.type	Tipe object dalam proses penyerangan
6	auditd.summary.object.primary	Nama service yang dituju
7	auditd.result	Hasil pada proses penyerangan (fail dan success)

Tabel 3. Menjelaskan mengenai isi tabel yang terdapat pada Dashboard Kibana dengan index pattern Auditbeat. Penjelasan tersebut dapat memudahkan Administrator dalam melakukan analisa terhadap sistem yang sedang di monitoring.

Hasil dari kedua pengujian tersebut akan dilihat pada Tabel 4.

Tabel 4. Hasil Deteksi

No	Metode Serangan	Waktu Serangan	Waktu Tercatat	Waktu Deteksi SIEM	Keterangan
1	FTP Attack (Anonymous)	10:51:09	10:51:09	-	Tidak terdeteksi
2	FTP Attack (Brute Force)	14:13:17	14:13:17	14:13:17	Berhasil Terdeteksi
3	SSH Attack (Brute Force)	14:28:41	14:28:41	14:28:41	Berhasil Terdeteksi

Hasil tersebut sesuai dengan proses pengujian sistem dengan metode *Brute Force* dan *Anonymous* untuk FTP, dan waktu yang ada pada Tabel 4 merupakan hasil yang ditunjukkan oleh log file dan SIEM.

4. PENUTUP

4.1 Kesimpulan

Selama proses penelitian ini telah dilakukan beberapa proses seperti membuat arsitektur, installasi, konfigurasi, serta pengujian terdapat hasil yang tidak diperhitungkan yaitu adanya kecacatan *false-negative* untuk pengujian dengan menggunakan metode kredensial "*anonymous*" pada service FTP karena SIEM tidak mendeteksi adanya serangan yang masuk. Kecacatan tersebut karena tidak adanya suatu alert atau event yang tervisualisasi dari log file "/var/log/vsftpd.log" ke dashboard Kibana. Kecacatan tersebut dapat dicegah dengan mengubah "anonymous_enable=YES" menjadi "anonymous_enable=NO" pada file "/etc/vsftpd.conf". Berbeda apabila dalam proses pengujian dengan menggunakan metode *Brute Force* yang terdapat kredensial yang digunakan untuk *service SSH* ataupun *FTP* maka akan menemukan semua file ataupun folder yang terdapat pada sistem. Namun pada dasarnya apabila memaksa masuk ke dalam sistem dengan menggunakan metode *Brute Force* harus dilakukan pencegahan dengan membatasi jumlah percobaan masuk.

4.2 Saran

Diharapkan untuk penelitian kedepannya dapat dikembangkan kembali dengan mengedepankan pembenahan kecacatan pada rule yang digunakan dalam SIEM ini agar tidak ada event yang terlewat untuk dianalisa oleh administrator, serta diharapkan dapat melakukan integrasi dengan aplikasi lain agar dapat mempermudah administrator.

DAFTAR PUSTAKA

Agrawal, V., Kotia, D., Moshirian, K., & Kim, M. (2018). Log-based cloud monitoring system for OpenStack. *Proceedings - IEEE 4th International Conference on Big Data Computing Service and Applications, BigDataService 2018*, 276–281. https://doi.org/10.1109/BIGDATASERVICE.2018.00049

Alamsyah, H., -, R., & Al Akbar, A. (2020). Analisa Keamanan Jaringan Menggunakan Network Intrusion Detection and Prevention System. *JOINTECS (Journal of*

Information Technology and Computer Science), *5*(1), 17. https://doi.org/10.31328/jointecs.v5i1.1240

ARFANUDIN, C., Sugiantoro, B., & Prayudi, Y. (2019). ANALYSIS OF ROUTER ATTACK WITH SECURITY INFORMATION AND EVENT MANAGEMENT AND IMPLICATIONS IN INFORMATION SECURITY INDEX. *Cyber Security Dan Forensik Digital*, *2*(1), 1–7. https://doi.org/10.14421/CSECURITY.2019.2.1.1388

Ari Setiawan, C., & Tria Putra Abza, A. (2020). Keamanan Jaringan Menggunakan Teknik Network Intrusion Detection System (NIDS) Di Kantor Setwan Kepulauan Meranti. In *Jurnal Intra Tech* (Vol. 4, Issue 2).

Irma Anggraeni, F. N. F. (2022). *DESAIN PLATFORM MONITORING DAN OBSERVABILITY UNTUK MICROSERVICE BERBASIS ELASTIC STACK | anggraeni | Jurnal Aplikasi Bisnis dan Komputer*. https://journal.unpak.ac.id/index.php/jubikom/article/view/4831

Jokić, A., Baraković, S., Husić, J. B., & Pleho, J. (2021). Partial rule security information and event management concept in detecting cyber incidents. *International Journal of Security and Networks*, *16*(2), 117–128. https://doi.org/10.1504/IJSN.2021.116777

Komang, I., Marta1, K. A., Nyoman, I., Hartawan2, B., Kadek, I., & Satwika3, S. (2020). Analisis Sistem Monitoring Keamanan Server dengan SMS Alert Berbasis Snort. *INSERT : Information System and Emerging Technology Journal*, *1*(1), 25–40. https://doi.org/10.23887/INSERT.V1I1.25874

Park, J., Kim, J., Gupta, B. B., & Park, N. (n.d.). *Network Log-Based SSH Brute-Force Attack Detection Model*. https://doi.org/10.32604/cmc.2021.015172

Putra, A. D., & Alghozy, M. T. R. B. (2022). Analisis dan Implementasi Keamanan Jaringan File Transfer Protocol (FTP) Menggunakan Intrusion Prevention System (IPS) pada Mikrotik. *Smart Comp :Jurnalnya Orang Pintar Komputer*, *11*(4), 762–775. https://doi.org/10.30591/SMARTCOMP.V11I4.4263

ROMADHON, WAHYU DWI and , Devi Afriyantari Puspa Putri, S.Kom., M. S. (2021). *Implementasi Suricata Idps Untuk Monitoring Jaringan Dengan Visualisasi Elk (Elasticsearch, Logtash, Kibana) Dan Notifikasi Melalui Bot Telegram*. http://eprints.ums.ac.id/78171/

Sholihah, W., Pripambudi, S., & Mardiyono, A. (2020). Log Event Management Server Menggunakan Elastic Search Logstash Kibana (ELK Stack). *JTIM : Jurnal Teknologi Informasi Dan Multimedia*, *2*(1), 12–20. https://doi.org/10.35746/JTIM.V2I1.79