Jurnal Teknik Informatika (JUTIF)
Vol. 4, No. 1, Februari 2023, hlm. 39-48

DOI: https://doi.org/10.20884/1.jutif.2023.4.1.644
p-ISSN: 2723-3863
e-ISSN: 2723-3871

ANALYSIS OF BRUTE FORCE ATTACK LOGS TOWARD NGINX WEB SERVER ON DASHBOARD IMPROVED LOG LOGGING SYSTEM USING FORENSIC INVESTIGATION METHOD

Rio Pradana Aji[*1], Yudi Prayudi[2], Ahmad Luthfi[*3]

[1,2,3]Program Studi Informatika Program Magister Fakultas Teknologi Industri, Universitas Islam Indonesia
Email: [1]20917052@students.uii.ac.id, [2]prayudi@uii.ac.id, [3]ahmad.luthfi@uii.ac.id

(Naskah masuk: 17 Oktober 2022, Revisi : 04 November 2022, diterbitkan: 10 Februari 2023)

Abstract

Since it was first launched in 1990, the Web Server is still in use today. No exception, almost all companies entering industry 4.0 use Web Servers to show the existence of the company's website and its products. Starting from the websites provided for free by WordPress and Blogspot to independent websites created by their respective companies. The web server itself is available in several types, ranging from apache, nginx, litespeed, etc. Of course, the use of a Web Server for websites cannot be separated from internet crimes or cyber crimes. One of the crimes committed is the hacker's attempt to login to the website Administrator page. The loophole used by hackers is brute force or forced entry by trying every combination of existing Administrator User and Password. This research focuses on building and updating a website monitoring dashboard system with Wazuh technology. The method used in this study is the Quantitative Forensic Investigation Method by examining the logs generated by the System Dashboard using Digital Forensic procedures. This monitoring process aims to detect brute force threats on managed websites by showing the website Administrator login activity log. The results of the metadata log shown by the optimized dashboard show the number of brute force attacks on managed websites. The number of attacks recorded was 259646 attacks on the first cluster and 288676 attacks on the second cluster. In addition, the results of the metadata log can be investigated further to find the location of the Hacker. The location of the hackers found was only limited to the VPN (Virtual Private Network) server used. One of the VPN servers used in this case is Amazon Data Center.

Keywords: *Bruteforce, Digital Forensics, Monitoring, Wazuh, Website.*

ANALISIS LOG SERANGAN BRUTEFORCE TERHADAP WEB SERVER NGINX PADA DASHBOR SISTEM PENCATATAN LOG TERIMPROVISASI MENGGUNAKAN METODE INVESTIGASI FORENSIK

Abstrak

Sejak pertama kali diluncurkan pada tahun 1990 *Web Server* hingga saat ini masih digunakan. Tidak terkecuali hampir semua perusahaan yang memasuki industri 4.0 menggunakan *Web Server* untuk menunjukkan eksistensi *website* perusahaan dan produk yang dimiliki. Mulai dari *Website* yang disediakan gratis oleh Wordpress maupun Blogspot hingga *website* mandiri yang dibuat oleh perusahaan masing-masing. *Web server* sendiri tersedia dalam beberapa macam, mulai dari *apache, nginx, litespeed*, dll. Tentu saja penggunaan *Web Server* untuk *website* tidak lepas dari tindak kejahatan internet atau *cyber crime*. Salah satu tindak kejahatan yang dilakukan adalah usaha *hacker* untuk *login* ke halaman Administrator *website*. Celah yang digunakan oleh *hacker* adalah tindakan *brute force* atau pemaksaan masuk dengan mencoba setiap kombinasi *User* dan *Password* Administrator yang ada. Pada penelitian ini berfokus untuk membangun dan memperbarui sistem dasbor *monitoring website* dengan teknologi Wazuh. Metode yang digunakan dalam penelitian ini adalah Metode Investigasi Forensik Kuantitatif dengan meneliti *log* yang dihasilkan oleh Dasbor Sistem menggunakan prosedur Forensika Digital. Proses *monitoring* ini bertujuan untuk mendeteksi ancaman *brute force* pada *website* yang dikelola dengan menunjukkan *log* aktivitas *login* Administrator *website*. Hasil metadata *log* yang ditunjukan oleh dasbor teroptimasi menunjukkan jumlah serangan *brute force* pada website yang dikelola. Jumlah serangan yang tercatat ialah 259646 serangan pada klaster pertama dan 288676 serangan pada klister kedua. Selain itu hasil metadata *log* dapat diteliti lebih lanjut untuk menemukan lokasi *Hacker*. Adapun lokasi *hacker* yang ditemukan hanya terbatas hingga *server VPN (Virtual Private Network)* yang digunakan. Salah satu *server VPN* yang dalam kasus ini digunakan ialah *Amazon Data Center*.

Kata kunci: *Bruteforce, Forensik Digital, Monitoring, Wazuh, Website.*

1. PENDAHULUAN

Salah satu teknologi internet yang hingga saat ini masih terus digunakan adalah *web server*. *Web Server* merupakan sebuah *engine* yang digunakan untuk menjalankan world wide web(www) dengan menggunakan menerima layanan HTTP atau HTTPS[1]. Teknologi yang diluncurkan pada tahun 1990 telah sangat membantu umat manusia dalam berbagai aspek kehidupan. Mulai dari mudahnya mengakses informasi terbaru, kebutuhan primer dan sekunder manusia, tempat hiburan, tempat bekerja, dan berbagai hal lainnya. Mulanya hanya berbentuk website yang menampilkan tulisan saja namun lambat laun *web server* yang sudah berbentuk website tersebut mulai mengalami berbagai macam perubahan. Web server bekerja dengan menerima *request* dari user ketika user menginputkan data atau melakukan pencarian pada browser yang kemudian browser memproses *request* dengan menghasilkan tampilan website[2]. Website saat ini tidak hanya berisi tulisan saja, mulai dari gambar, video, *game*, hingga konsol interaktif telah tersedia pada website. *Web Server* yang tersedia saat ini ada berbagai macam namanya, yaitu *apache, nginx, lighspeed, microsoft iis, lighttpd,* dan lain sebagainya. Hingga saat ini *web server* yang paling banyak digunakan adalah *apache* dan *nginx*[3].

Perkembangan teknologi *web server* yang menjadi website ini selain dibarengi dengan nilai positif terdapat pula hal negatif. Salah satu tindakan negatif adalah upaya pembobolan website, yaitu usaha untuk masuk ke server tempat *web server* berada (*hosting*) yang sulit teridentifikasi[4]. Permasalahan ini timbul ketika *traffic/*kunjungan ke website yang dikelola meningkat pesat dan mengundang banyak individu yang tidak bertanggung jawab untuk melakukan tindak kejahatan. *Hacker* merupakan sebutan individu/kelompok yang memiliki kemampuan membuat dan membaca program serta mengamati celah keamanan program tersebut[5]. Salah satu tindak kejahatan tersebut ialah usaha untuk mendapatkan akses Administrator ke website yang ditargetkan. Motif yang dilakukan *Hacker* tersebut bermacam-macam, ada yang tidak suka, ada yang berniat mencuri data atau hanya sekedar bermain-main saja. Sebagai Administrator pengelola website hal tersebut merupakan hal berbahaya dan merugikan. Tindakan preventif harus dilakukan agar website yang dikelola tidak jatuh ke tangan yang tidak bertanggung jawab.

Celah yang digunakan oleh *Hacker* tersebut adalah teknik *brute force.* Teknik ini digunakan oleh penyerang/*Hacker* untuk masuk ke dalam server dan dengan leluasa mengakses informasi yang ada di dalam server[6]. User dan Password Administrator yang pendek dan lemah biasanya akan dengan mudah didapatkan. Tindakan pencegahan paling awal adalah membuat kombinasi User dan Password sebaik mungkin dengan menggunakan kombinasi huruf kecil dan besar, angka, dan simbol[7].

Selain tindakan pencegahan dengan membuat kombinasi User dan Password yang unik terdapat cara lainnya. Monitoring *log* merupakan metode yang dilakukan administrator dalam memantau kondisi sebuah sistem melalui catatan aktivitas *user* yang tersimpan pada *log* server[8]. Proses monitoring *log* yang dilakukan dengan cara melihat *log web server* maupun *log* server lainnya yang ada di server website berada (*hosting*) kemudian dilakukan analisis. Namun permasalahan baru muncul ketika proses monitoring dilakukan secara manual karena harus masuk ke server website yang dikelola kemudian mengecek *log* tersebut satu persatu. Hal ini tentunya memakan banyak waktu dalam mencari *issue* pada website yang dikelola. Munculnya permasalahan ini dikarenakan tidak adanya *Centralized Log Management* (CLM) server atau server yang digunakan untuk memantau/memonitor keadaan server maupun website yang dimiliki. Solusi dari permasalahan tersebut dapat dicapai dengan mengembangkan *Centralized Log Management* server. Karena manajemen *log* yang efektif, penting untuk menunjang keamanan server yang dimiliki[9]. Karena sejatinya pembuatan *log* terpusat juga merupakan hal sangat penting bagi strategi pengamanan yang kuat untuk dimiliki[10].

Pada pengembangan CLM tersebut dapat dibantu dengan berbagai macam sarana aplikas/*tools* yang diesuaikan kebutuhan (berbayar maupun *open source*). Aplikasi paling populer yang digunakan dalam proses membangun CLM atau monitoring *log* adalah ELK (Elasticsearch, Logstash, Kibana) atau EFK(Elasticsearch, Fluentd, Kibana) stack. Stack tersebut bersifat *open source* dan banyak digunakan sebagai aplikasi untuk memonitor *log*. Sayangnya pada stack tersebut pembuatan visualisasi masih dilakukan secara manual. Serta hasil *log* yang dihasilkan masih *raw* dan perlu dilakukan *filter* secara manual. Hal ini merujuk pada penelitian penulis sebelumnya[11].

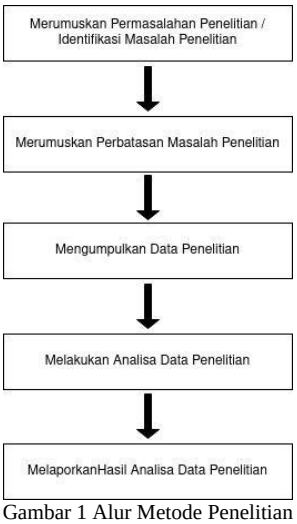
Wazuh merupakan aplikasi yang digunakan sebagai *log grabber*, kemudian *log* tersebut diolah untuk menyajikan *log* yang mulanya tidak beraturan menjadi informasi yang informatif dan dapat dipahami oleh manusia. *Log* aktivitas yang dapat diambil oleh Wazuh tidak hanya *web server* saja, *log* aktivitas login ssh dan rdp, *log* aktivitas user di dalam server melakukan *command* apa saja, *log* saat nama direktori berubah, serta dapat mendeteksi proses mencurigakan yang berjalan di *background* sistem. Secara singkat wazuh dapat dikatakan sebagai perangkat yang menyediakan visibilitas keamanan pada suatu infrastruktur sistem operasi[12]. Karena

modelnya sebagai *add-ons* maka Wazuh tidak bisa dilepaskan dari Elasticsearch dan Kibana. Sedangkan pada teknologi lainnya seperti Logstash, Filebeat, Fluentd, dan Fluentbit yang mengirimkan data log yang *raw* pada Wazuh sudah terdapat *build-in parse* sehingga *log* yang didapat langsung diubah oleh Wazuh agar mudah terbaca oleh manusia. Hal ini menyingkat waktu seorang Administrator atau Investigator untuk tidak membaca *raw log* tersebut satu per satu atau harus mengubah *raw log* tersebut ke bahasa yang lebih manusiawi.

Tujuan dari penelitian ini adalah untuk membangun/memperbarui Dasbor Sistem Pencatatan Log Server dengan fokus pada Web Server Nginx dan Server tempat website di-*hosting*. Selain itu tujuan lainnya adalah memberikan analisisa yang berkontribusi pada tahapan investigasi forensik pada sisi *web server* karena pada penelitian sebelumnya hanya berfokus pada monitoring file log saja. Hal ini bertujuan untuk mengerucutkan dan menjadikan penelitian lebih berfokus pada bagian *web server* sebuah website. Fokus ini berdasarkan dasbor sistem pencatatan *log* sebelumnya yang banyak mencatat serangan *brute force* menuju website dan server tempat website di *hosting*. Selain itu menguji apakah optimasi yang Wazuh berikan dapat memberi informasi yang informatif dalam kondisi server terkena serangan *brute force*. Skenario *brute force* pada penelitian adalah ketika memiliki sebuah website kemudian *hacker* melakukan usaha *brute force* ke website maupun server website tersebut di *hosting* lalu Wazuh secara otomatis mencatat hal ini. Setelah itu dalam proses investigasi dapat mengecek panel website apakah terdapat anomali ataupun melihat Wazuh untuk mengecek indikasi *malicious command* pada server. Investigasi *malicious command* tersebut dilakukan untuk mengetahui *hacker* telah masuk ke dalam server atau tidak. Hal ini merupakan kelebihan Wazuh yaitu menawarkan berbagai macam *log* untuk dianalisis/diinvestigasi. Sehingga dapat membantu Administrator/SysAdmin dalam mengawasi website yang dikelolanya. Diharapkan juga aplikasi Wazuh ini dapat menjadi kontributor baru dalam dunia forensika digital dan mampu membantu investigator dalam menangani kasus *cyber crime* yang ada.

2. METODE PENELITIAN

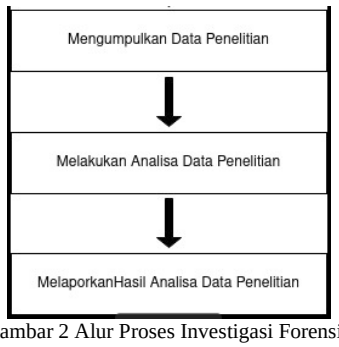
Metodologi penelitian yang digunakan adalah Metode Investigasi Forensik[13]. Dipilihnya metode ini dikarenakan meneliti/menganalisis data *log* Server pada Website yang memakai *web server* nginx dan *operating system* Ubuntu 18. Hal yang diteliti pada studi kasus adalah metadata *log* serangan *brute force* pada *web server nginx* dan server yang me-*hosting* website dengan melihat metadata *log* informasi yang dihasilkan oleh Wazuh. Data *log* tersebut didapatkan melalui server website pada perusahaan tempat penulis pernah bekerja. Selanjutnya melalui dasbor sistem pencatatan *log* yang sudah teroptimasi analisis dapat dilakukan berdasarkan metadata *log* yang diberikan oleh dasbor sistem pencatatan *log* tersebut. Hasil analisis diharapkan informatif dengan memberikan *log* informasi mengenai siapa, kapan, dimana, bagaimana serangan *brute force* dilakukan dan menunjukkan karakteristik pada tiap serangan yang dilakukan oleh Hacker. Serta dapat membantu investigator dalam menemukan bukti telah terjadi serangan *brute force* berbentuk *log* informasi yang dihasilkan Wazuh.



Gambar 1 Alur Metode Penelitian

Pada Gambar 1 merupakan alur penelitian yang akan dilakukan. Dimulai dari bagaimana skenario *brute force* dilakukan hingga informasi tentang *brute force* di-*generate* oleh Wazuh pada Dasbor Sistem Pencatatan *Log* yang sudah teroptimasi.

Alur yang digunakan dalam proses investigasi forensik dalam penelitian ini merujuk pada Model Proses Umum untuk Insiden dan Forensik Komputer karya Felix C Freiling dan Bastian Schwittay[14]. Sebelum memulai proses investigasi, terlebih dahulu dilakukan optimasi dasbor pencatatan *log*. Hal ini bertujuan untuk menyiapkan lingkup kerja analisis terlebih dahulu sebelum dapat dilakukannya proses analisis pada log *web server* dan server website.



Gambar 2 Alur Proses Investigasi Forensik

Pada Gambar 2 menunjukkan alur skema bagaimana *log* akan diteliti. Alur yang diambil mengambil poin 3 hingga 5 pada metode penelitian. Data penelitian yang diambil adalah metadata *log* yang dihasilkan oleh Wazuh. Sementara analisis

dilakukan pada *log* metadata tersebut dengan kaidah forensika digital. Terakhir laporan hasil penelitian akan dibuat berdasarkan hasil analisis metadata *log* dan karakteristik tiap serangan yang dilancarkan oleh Hacker.

Adapun skenario serangan yang akan dilakukan adalah sebagai berikut. Serangan yang terjadi adalah Hacker melakukan usaha *brute force* pada sisi server (ssh) dan halaman login administrator website (nginx). Selain Hacker proses atau inisiasi serangan dapat dilakukan oleh peneliti sendiri atau Administrator website. Proses serangan ini akan tercatat pada *log* ssh dan *log* nginx pada server tempat website di-*hosting*. Setelah itu proses akuisisi *log* ssh dan nginx tersebut dilakukan oleh Wazuh. Wazuh agent yang berada pada server *hosting* tersebut mengirim *log* ssh dan nginx ke Wazuh master untuk dilakukan parse *log* yang semula *raw log* menjadi *log* yang informatif atau dalam kata lain menjelaskan bahwa telah terjadi serangan *brute force* pada server. *Log* yang informatif tersebut memiliki susunan metadata atau bisa disebut metadata *log*. Langkah selanjutnya merupakan analisis yang dapat dilakukan dengan menggunakan metode investigasi forensik untuk menganalisis metadata *log* maupun karakteristik serangan yang dilancarkan oleh Hacker tersebut. Terakhir adalah pelaporan hasil analisis yang telah dilakukan.

Pada penelitian ini dari ELK stack hanya memanfaatkan 2 *tools* dari stack tersebut, yaitu Elasticsearch dan Kibana. Peran Wazuh pada penelitian ini masuk di Kibana karena pada dasarnya Wazuh adalah *add ons/plugins* yang terdapat pada Kibana[15]. Dalam komunikasi antara Elasticsearch, Kibana, dan Wazuh yang berada di dalam server dilakukan oleh Filebeat/Beats. Dari keempat *tools* tersebut menciptakan *Centralized Log Management* atau Dasbor Sistem Pencatatan *Log* untuk memonitor *log* pada server.

Proses pengembangan/optimasi yang dilakukan adalah dengan menggunakan Wazuh sehingga tidak perlu membuat *rule* set baru dalam mem-*parse raw* log yang dimiliki oleh server. Ditanamkannya Wazuh-Agent pada tiap server merupakan satu cara yang lebih baik dibandingkan menginstall dan membuat *rule* pada fluentbit (penelitian lama). Wazuh-Agent mengirimkan *log* yang sesuai pada file konfigurasi ke Wazuh Master. Wazuh master menerima *raw log* kemudian mengubah *raw log* tersebut berdasarkan *built-in* rule yang dimiliki dan menghasilkan metadata *log* untuk ditampilkan. Hasil dasbor baru dapat menampilkan informasi yang informatif dan memberikan *knowledge* mengenai keadaan server berdasarkan metadata *log* yang dihasilkan Wazuh.

Penelitian ini akan berfokus pada 3 *log*, 2 *log* pertama yaitu nginx dan ssh merupakan fokus utama, sedangkan 1 *log* terakhir yaitu auditd untuk membantu proses investigasi jika diperlukan. Adapun penjelasan dari ke 3 *log* tersebut adalah sebagai berikut :

a) *Log* nginx akan berfokus pada bagaimana keadaan ketika *web server* menerima request pada website, namun karena penelitian ini akan berfokus pada *brute force* maka selain memonitor keadaan *web server*, indikasi *brute force* juga akan terekam. Pada penelitian ini digunakan contoh website yang menggunakan Wordpress. Pada server tempat nginx berada Wazuh akan memonitor *log* pada 2 buah *log* yaitu **access.log** dan **error.log** yang berada pada direktori ***/var/log/nginx*** pada server tempat website tersebut di *hosting.*
b) *Log* ssh akan berfokus pada bagaimana keadaan server selama menjadi tempat *hosting* website tersebut, namun karena penelitian ini akan berfokus pada *brute force* maka selain memonitor keadaan server, indikasi terjadinya *bruteforce* yang berusaha masuk ke server akan terekam. Pada penelitian ini digunakan contoh server yang memakai Linux Ubuntu 18.04. Pada server tempat website di *hosting* tersebut diperlukan Wazuh-Agent yang digunakan untuk mengirimkan *log* ssh untuk dilakukan monitoring pada siapa saja yang mencoba untuk mengakses/masuk ke dalam server. Lokasi *log* ssh tersebut pada server ada pada file yang bernama **auth.log** yang ada pada direktori ***/var/log/auth.log***.
c) *Log* auditd akan berfokus pada bagaimana keadaan server yang telah terindikasi disusupi oleh *hacker*. Karena fungsi dari auditd adalah memonitor *command* berbahaya yang sudah tersimpan pada *rules* dan jika dilanggar(*command* tersebut dijalankan oleh user tanpa ada notifikasi kepada SysAdmin) maka server tersebut terindikasi sudah dimasuki oleh *hacker*. Auditd merupakan *tools* keamanan yang ada pada Linux Server dan sifatnya bukan bawaan melainkan dari pihak ketiga. Pada Wazuh *tools* ini dimanfaatkan untuk mendeteksi *command* berbahaya yang dijalankan oleh user pada suatu server. Pendeteksian *command* tersebut menggunakan *rules* yang bebas ditentukan oleh pengguna server atau SysAdmin terkait *command* apa saja yang tidak boleh/berbahaya ketika dijalankan pada server. Lokasi *log* Auditd yang akan dimonitor oleh Wazuh ada pada ***/var/log/audit/*** dan nama file pada direktori tersebut adalah **audit.log**.

Pemaparan *log* mana saja yang akan diteliti pada penjelasan di atas maka *log* selainnya dapat diabaikan saja.

Proses penelitian yang dilakukan berdasarkan Metode Investigasi Forensik serta cara kerja Wazuh akan dijelaskan. Acuan penjelasan dan metode agar lebih mudah dipahami dan tidak terpecah pecah maka dibagi menjadi 5 bagian penjelasan seperti **Tabel 1** dibawah.

Tabel 1 Tahapan Investigasi Forensik

Langkah	Penjelasan
Identification	Identifikasi kejahatan serangan *brute force* yang dilakukan oleh Hacker.
Problem Scope	Perbatasan masalah yang dibuat terhadap masalah/kejadian yang berlangsung.
Collection Examination	Mengamankan/mengambil barang bukti berdasarkan *log* yang ada pada server. Melakukan pelacakan pelaku berdasarkan metadata *log* yang dihasilkan oleh Wazuh.
Analysis	Menganalisis karakteristik serangan yang dilancarkan oleh Hacker.
Presentation	Penyampaian laporan hasil analisis / dokumentasi kegiatan analisis.

Berdasarkan Tabel 1 diatas merupakan metode investigasi forensik akan ditekankan dan berfokus pada investigasi metadata *log* yang dihasilkan oleh Wazuh. Selain itu juga akan dilakukan rekontruksi metadata *log* untuk memberikan informasi mengenai karakteristik serangan yang dilakukan oleh Hacker. Penjabaran 5 proses tersebut adalah sebagai berikut :

a) Tahap identifikasi adalah mengidentifikasi serangan *brute force* yang biasanya dilakukan oleh *hacker*. Pada penelitian ini identifikasi dapat dilakukan dengan cara melihat *log* ssh dan nginx apakah terdapat *log flooding* yang mengindikasikan adanya usaha untuk masuk berkali kali dengan tempo singkat dan kebanyakan adalah *log* eror karena username, password atau keduanya salah. Dari situ dapat ditarik kesimpulan bahwa telah terjadi serangan *brute force* pada website dan server yang dikelola.

b) Tahap batasan masalah adalah tahap menguraikan batasan terhadap kasus kejahatan dunia maya/*cyber crime* yang sedang diteliti. Pengolahan pada penelitian ini memanfaatkan teknologi *Centralized Log Management* (CLM) server atau Dasbor Pencatatan Log Server. Teknologi yang digunakan untuk mengembangkan CLM tersebut adalah Elasticstack dan Wazuh. Log yang diteliti ada 3 jenis *log*, yang mana *log web server* akan lebih banyak dibahas/diteliti.

c) Tahap pengumpulan dan eksaminasi *log* yaitu seperti sudah dijelaskan pada poin sebelumnya menyatakan bahwa ada 3 *log* yang akan diambil dan di analisa. Sifat dari *log* tersebut berada pada server tempat website di *hosting.* Sehingga di server tersebut perlu di-*Install* Wazuh Agent sebagai agent yang akan mengirimkan 3 *log* tersebut ke arah Wazuh Master/Wazuh Cluster.

d) Pada tahap analisis ini adalah dengan menganalisis bagaimana *behavior* atau karakteristik penyerang (Hacker) dalam melancarkan aksinya. Pada tahapan ini perlu dilakukan analisis mendalam mengenai jumlah *log* yang dihasilkan oleh Wazuh berkaitan dengan IP Address Hacker yang sama dalam beberapa waktu menyerang website maupun server yang dikelola. Nama objek serangan website ataupun server perlu dicatat juga jumlahnya sehingga dapat disimpulkan bagaimana pola serangan yang dilancarkan Hacker tersebut.

e) Tahap presentasi adalah tahap dalam menyampaikan laporan mengenai hasil analisis yang dilakukan pada penelitian berkaitan dengan serangan yang dilakukan Hacker. Hal ini merupakan langkah akhir dalam metode untuk menginvestigasi permasalahan yang dihadapi oleh baik SysAdmin maupun investigator. Pada tahapan ini SysAdmin dapat membuat laporan tentang website apa saja yang sering diserang, lokasi mana saja yang biasa menyerang, serta IP address mana saja yang sering melakukan serangan. Hal ini untuk dilaporkan kepada atasan dan dapat dilakukan tindakan selanjutnya yaitu pencegahan *brute force* misalnya berupa memblokir IP addres yang melakukan serangan tersebut selama beberapa hari. Pada sisi Investigator hal ini dapat dijadikan *knowledge* baru untuk dilakukan analisis tambahan atau dapat langsung dilaporkan bila sedang menghadapi kasus yang melibatkan pembobolan website. Terkait informasi pelaku yang tidak terlalu lengkap dapat ditelusuri lebih lanjut berdasarkan informasi yang didapatkan, misalnya menelusuri dari lokasi *hacker* dan IP address yang dipakai oleh *Hacker*. Pembuatan laporan ini berbeda tergantung oleh SysAdmin pada perusahaan satu dengan lainnya. Begitu juga terhadap seorang Investigator bentuk laporannya berbeda-beda tiap instansi maupu organisasi yang diikuti.

3. HASIL DAN PEMBAHASAN

Pada tahapan ini dijabarkan hasil implementasi Dasbor Sistem Pencatatan Log Web Server Nginx yang telah di improvisasi pada **2 cluster**. Cluster pertama adalah cluster milik penulis dengan kondisi memiliki 5 website yang di-*monitoring*. Adapun website yang di-*monitoring* pada cluster pertama merupakan website yang baru dibuat dan belum terkenal seperti website pada cluster kedua. Cluster kedua adalah cluster milik Badan Sistem Informasi (BSI) yang merupakan penyedia layanan internet pada Kampus Universitas Islam Indonesia. Website yang di-*monitoring* pada cluster kedua merupakan website fakultas dan prodi Kampus UII yang sudah ada sejak lama.

Adapun pembahasan yang dilakukan ialah menginvestigasi/meneliti struktur metadata log yang dihasilkan oleh Wazuh pada Dasbor Sistem Pencatatan Log. Hal yang diteliti merupakan log serangan brute force yang di-generate oleh Wazuh tersebut. Selain itu karakteristik dari masing-masing serangan tersebut juga akan diteliti guna

mendapatkan pola serangan yang dilakukan oleh Hacker sehingga dapat dilakukan pelacakan kembali sumber serangan brute force

List Website yang akan dilakukan penelitian :

a) Cluster Pertama
- canyoubruteforceme.my.id
- datapenelitiantesis.my.id
- websitepenelitiantesis.my.id
- bruteforcethiswebsite.my.id
- penelitiantesis.my.id

b) Cluster Kedua

Pada cluster kedua akan diambil 5 website yang paling banyak mendapatkan serangan pada bulan Januari 2022. Website tersebut akan dipilih secara random pada bulan Januari dikarenakan sifatnya berbeda dengan cluster pertama.

Adapun *log bruteforce* yang diteliti mengacu pada 2 *log* yaitu *log nginx* serta *log* ssh pada server tempat website di-*hosting*. Informasi yang didapatkan dari kedua *log* ini berguna untuk mengidentifikasi serangan yang dilakukan oleh *Hacker* serta lokasi serangan yang dilakukan oleh *Hacker*. Sehingga dari kedua *log* informasi tersebut dapat ditemukan metode baru dalam investigasi forensik untuk menemukan sumber kejahatan yang dilakukan.

Perincian dari kedua *log* tersebut adalah sebagai berikut:

a) **rule id 5710** merupakan identifikasi bahwa telah terjadi usaha untuk login ke dalam server hosting sebanyak 1 kali.
b) **rule id 5712** merupakan identifikasi bahwa telah terjadi usaha untuk login ke dalam server hosting sebanyak 8 kali. Hal ini menyatakan bahwa setiap 8 kali **rule id 5710** ter-"trigger" maka menghasilkan 1 kali **rule id 5712**.
c) **rule id 31509** merupakan identifikasi bahwa telah terjadi usaha untuk login ke dalam website sebanyak 1 kali.
d) **rule id 31510** merupakan identifikasi bahwa telah terjadi usaha untuk login ke dalam website sebanyak 8 kali. Hal ini menyatakan bahwa setiap 8 kali **rule id 31509** ter-"trigger" maka menghasilkan 1 kali **rule id 31510**.

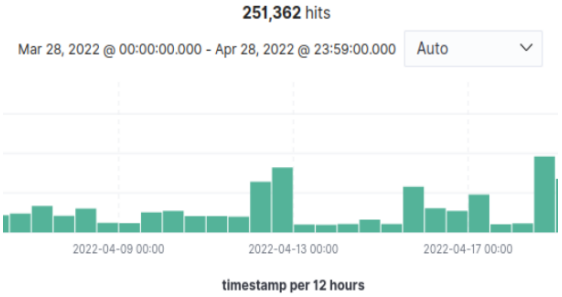
Asal negara penyerang website akan diambil berdasarkan **rule id 31510** karena rule id tersebut dihitung berdasarkan jumlah intensitas serangan yang dilakukan oleh Hacker. Meskipun secara gamblang jumlah serangan menuju website terlihat lebih banyak pada **rule id 31509** namun karena intensitas **rule id 31509** sangat kecil maka fokus pembahasan akan ditujukan kepada **rule id 31510**. Sama halnya dengan **rule id 5712, rule id** ini memiliki jumlah intensitas serangan menuju server yang di-*hosting* sangat tinggi dibandingkan dengan **rule id 5710**. Maka fokus pada pembahasan mengenai serangan yang ditujukan pada server tempat website di-*hosting* adalah **rule id 5712** alih alih **rule id 5710**. Jenis intensitas serangan yang dibahas atau dimiliki pada kedua **rule id** tersebut tidak lain dan tidak bukan merupakan *bruteforce.*

Berikut penjabaran penlitian dari kedua kluster:

A. Kluster Pertama

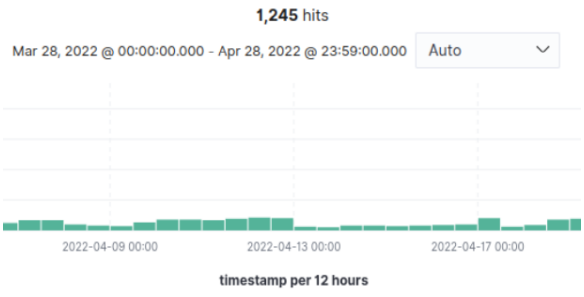
Pada hasil analisis yang dilakukan di cluster kedua selama 1 Bulan (terhitung dari tanggal 28 Maret 2022 hingga 28 April 2022) menunjukkan hasil *bruteforce* yang dilakukan oleh hacker berjumlah 259646 serangan. Adapun penjabaran serangan berdasarkan rule id ialah :

a) **Rule id 5710** mendapatkan serangan sebanyak **251362 hits** seperti pada Gambar 3. Hasil serangan ini ditujukan pada server tempat website di-hosting oleh Adminisrator. Sesuai dengan **rule id** yang diberikan bahwa serangan ini menyerang dengan teknik *brute force* lewat jalur login ssh kredensial. Pada Gambar 3 menunjukkan bahwa serangan yang hacker lakukan hampir tiap hari dilakukan. Selain serangan yang dilancarkan oleh *Hacker* bisa juga *log* yang di-*generate* ini merupakan kesalahan input ketika memasukan kredensial.



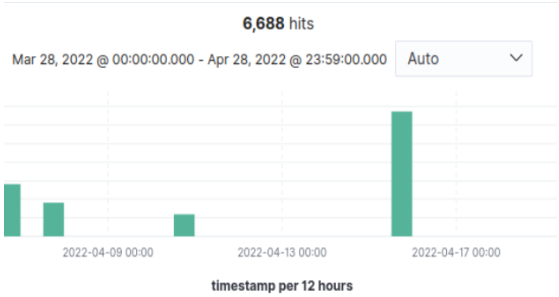
Gambar 3 Rule id 5710 cluster pertama

b) **Rule id 5712** mendapatkan serangan sebanyak **1245 hits** seperti pada Gambar 4. Hasil serangan ini ditujukan pada server tempat website di-hosting oleh Adminisrator juga. Sesuai dengan **rule id** yang diberikan bahwa serangan ini menyerang dengan teknik *brute force* lewat jalur login ssh kredensial juga. Perbedaan yang dimiliki oleh Gambar 3 dan Gambar 4 ialah terlihat konsistensi serangan yang dilancarkan oleh *Hacker* bisa terlihat. Hal ini terlihat dengan karakteristik **Rule id 5712** mencatat/menghasilkan 1 *log* **Rule id 5712** setelah **Rule id 5710** ter-*trigger* oleh sumber IP Addres yang sama sebanyak 8 kali. Ini menunjukkan bahwa usaha *brute force* memang gigih dilakukan oleh *Hacker* dan bukan merupakan kesalahan input yang dilakukan oleh Administrator.



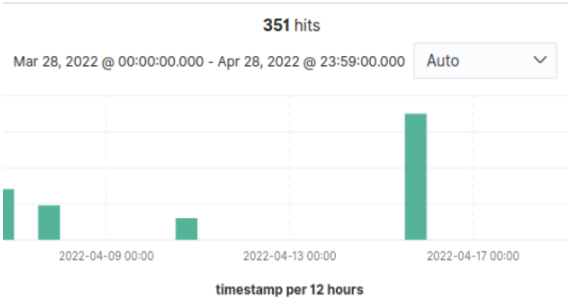
Gambar 4 Rule id 5712 cluster pertama

c) **Rule id 31509** mendapatkan serangan sebanyak **6688 hits** seperti pada Gambar 5. Hasil serangan ini ditujukan pada halaman administrator website yang dikelola oleh Administrator website. Sesuai dengan rule id yang diberikan bahwa serangan ini menyerang dengan teknik *brute force* lewat jalur login admin di halaman Administrator website. Pada Gambar 5 menunjukkan aktivitas kesalahan login yang tinggi dalam kurun waktu 1 bulan di 5 website yang baru selesai dibuat. Selain aktivitas serangan *Hacker* bisa juga *log* yang dihasilkan merupakan kesalahan Administrator ketika memasukan kredensial.



Gambar 5 Rule id 31509 cluster pertama

d) **Rule id 31510** mendapatkan serangan sebanyak **351 hits** seperti pada Gambar 6. Hasil serangan ini ditujukan pada halaman administrator website yang dikelola oleh Administrator website juga. Sesuai dengan rule id yang diberikan bahwa serangan ini menyerang dengan teknik *brute force* lewat jalur login admin di halaman Administrator website juga. Perbedaan yang dimiliki oleh Gambar 5 dan Gambar 6 menunjukkan aktivitas yang dilakukan oleh *Hacker* konsisten dalam usahnya untuk masuk ke salah 1 dari 5 website yang dikelola. Sesuai dengan **Rule id 31510** hal yang dilakukan *Hacker* berdasarkan IP Addressnya memang sengaja dan bukan kesalahan input yang dilakukan oleh Administrator.



Gambar 6 Rule id 31510 cluster pertama

Berdasarkan analisis serangan yang dilakukan oleh *Hacker* pada Cluster Pertama menunjukkan bahwa serangan yang dituju oleh *Hacker* kebanyakan semua mengarah pada server tempat hosting website (**rule id 5710 & 5712**) yang dikelola oleh peneliti. Sedangkan Serangan yang ditujukan kepada website yang baru dibuat juga (**rule id 31509 & 31510**) menunjukkan hasil yang minim. Pada 5 website yang dibuat baru dan dikelola oleh penulis mendapatkan serangan *bruteforce* yang sedikit. Berbeda dengan server tempat me-*hosting* website tersebut memiliki riwayat serangan yang cukup tinggi selama 1 bulan. Berdasarkan data yang diambil selama 1 bulan hanya 6688 serangan (**rule id 31509**) yang ditujukan pada website dalam kurun waktu 1 bulan. Sedangkan jika **rule id 31509** tersebut diperkuat lagi dengan **rule id 31510** maka hanya menghasilkan 351 serangan saja dalam 1 bulan yang mengarah pada website baru tersebut. Berbeda dengan data serangan *bruteforce* menuju ke server tempat website di-*hosting* (**rule id 5710 & 5712**) menunjukkan angka serangan yang tinggi.

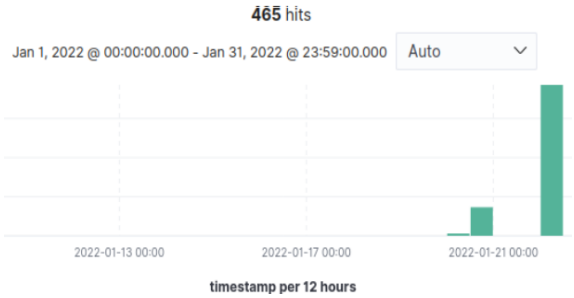
Metadata log yang diterima pada cluster pertama bagian **rule id 5710** menghasilkan **251362 hits** dan **rule id 5712** yang menghasilkan **1245 hits.** Sedangkan pada cluster kedua **rule id 5710** menghasilkan **465 hits** dan **rule id 5712** menghasilkan **4 hits**. Hasil ini menunjukkan bahwa serangan dari *Hacker* yang ada diseluruh dunia sebenarnya banyak bila diturut atau dilihat berdasarkan **rule id 5710**, namun serangan yang dilancarkan hanya sebatas serangan sekali saja atau serangan yang tidak terorganisir. Kenapa demikian ? Karena jumlah serangan pada **rule id 5710** ini hanya me-*record* serangan atau kesalahan saat login ke server tempat website di-*hosting* yang dilakukan oleh user maupun *Hacker*.

Laporan pembahasan dari analisis pada cluster pertama menunjukkan bahwa tingkat serangan *bruteforce* pada website yang baru dibuat dan belum lama ada, dilancarkan oleh hacker dengan sasaran server tempat website di-*hosting* alih-alih website yang baru diluncurkan tersebut.

B. Kluster Kedua

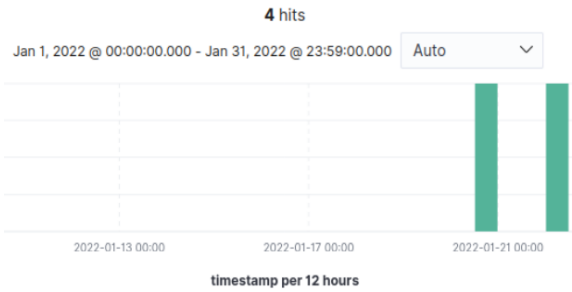
Pada hasil analisis yang dilakukan di cluster kedua selama 1 Bulan (terhitung dari tanggal 1 Januari 2022 hingga 31 Januari 2022) menunjukkan hasil *bruteforce* yang dilakukan oleh hacker berjumlah 288676 serangan. Adapun penjabaran serangan berdasarkan rule id ialah :

a) **Rule id 5710** mendapatkan serangan sebanyak **465 hits** seperti pada Gambar 7. Hasil serangan ini ditujukan pada server tempat website di-hosting oleh Adminisrator. Sesuai dengan **rule id** yang diberikan bahwa serangan ini menyerang dengan teknik *brute force* lewat jalur login ssh kredensial. Pada Gambar 7 menunjukkan bahwa serangan yang hacker lakukan berada di penghujung bulan saja. Hal ini bisa terjadi dengan banyak kemungkinan, salah satunya server dalam keadaan mati saat awal bulan atau memang tidak ada serangan di awal bulan.



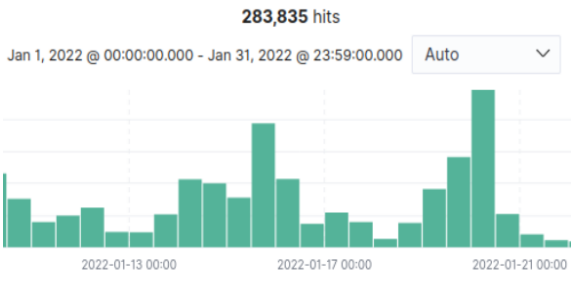
Gambar 7 Rule id 5710 cluster kedua

b) **Rule id 5712** mendapatkan serangan sebanyak **4 hits** seperti pada Gambar 8. Hasil serangan ini ditujukan pada server tempat website di-hosting oleh Adminisrator juga. Sesuai dengan **rule id** yang diberikan bahwa serangan ini menyerang dengan teknik *brute force* lewat jalur login ssh kredensial juga. Perbedaan yang dimiliki oleh Gambar 7 dan Gambar 8 ialah terlihat konsistensi serangan yang dilancarkan oleh *Hacker* bisa terlihat. Hal ini terlihat dengan karakteristik **Rule id 5712** mencatat/menghasilkan 1 *log* **Rule id 5712** setelah **Rule id 5710** ter-*trigger* oleh sumber IP Addres yang sama sebanyak 8 kali. Ini menunjukkan bahwa usaha *brute force* memang gigih dilakukan oleh *Hacker* dan bukan merupakan kesalahan input yang dilakukan oleh Administrator.



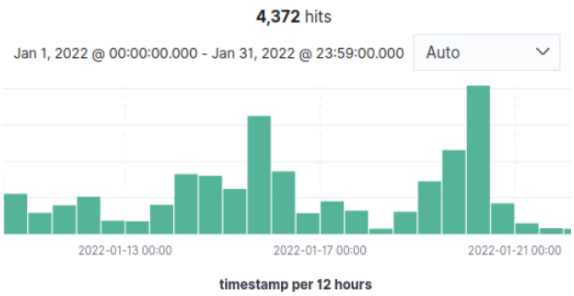
Gambar 8 Rule id 5712 cluster kedua

c) **Rule id 31509** mendapatkan serangan sebanyak **283835 hits** seperti pada Gambar 9. Hasil serangan ini ditujukan pada halaman administrator website yang dikelola oleh Administrator website. Sesuai dengan rule id yang diberikan bahwa serangan ini menyerang dengan teknik *brute force* lewat jalur login admin di halaman Administrator website. Pada Gambar 9 menunjukkan aktivitas kesalahan login yang tinggi dalam kurun waktu 1 bulan di 5 website yang dikelola oleh BSI UII. Selain aktivitas serangan *Hacker* bisa juga *log* yang dihasilkan merupakan kesalahan Administrator ketika memasukan kredensial.



Gambar 9 Rule id 31509 cluster kedua

d) **Rule id 31510** mendapatkan serangan sebanyak **4372 hits** seperti pada Gambar 10. Hasil serangan ini ditujukan pada halaman administrator website yang dikelola oleh Administrator website juga. Sesuai dengan rule id yang diberikan bahwa serangan ini menyerang dengan teknik *brute force* lewat jalur login admin di halaman Administrator website juga. Perbedaan yang dimiliki oleh Gambar 9 dan Gambar 10 menunjukkan aktivitas yang dilakukan oleh *Hacker* konsisten dalam usahnya untuk masuk ke salah 1 dari 5 website yang dikelola. Sesuai dengan **Rule id 31510** hal yang dilakukan *Hacker* berdasarkan IP Addressnya memang sengaja dan bukan kesalahan input yang dilakukan oleh Administrator.



Gambar 10 Rule id 31510 cluster kedua

Berdasarkan analisis serangan yang dilakukan oleh *Hacker* pada Cluster Kedua menunjukkan bahwa serangan yang dituju oleh *Hacker* kebanyakan semua mengarah pada website (**rule id 31509 & 31510**) yang dikelola oleh kampus UII (BSI). Sedangkan Serangan yang ditujukan kepada server tempat website di-*hosting* (**rule id 5710 & 5712**) minim sekali. Pada 5 website terbanyak yang mendapatkan serangan *bruteforce*, server tempat me-*hosting* website tersebut memiliki riwayat serangan yang cukup rendah selama 1 bulan. Berdasarkan data yang diambil selama 1 bulan hanya 465 serangan (**rule id 5710**) yang ditujukan pada server tempat hosting website dalam kurun waktu 1 bulan. Sedangkan jika rule id 5710 tersebut di perkuat lagi dengan rule id 5712 maka hanya menghasilkan 4 serangan saja dalam 1 bulan yang mengarah pada server tempat website di-*hosting*. Dapat dilihat bahwa serangan ini tidak dilakukan secara intens(**Rule id 5712**). Berbeda dengan data serangan *bruteforce* menuju ke website

(**rule id 31509 & 31510**) menunjukkan angka serangan yang tinggi.

Metadata *Log* yang diterima pada cluster pertama bagian **rule id 31509** menghasilkan **6688 hits** dan **rule id 31510** menghasilkan **351 hits**. Sedangkan pada cluster kedua **rule id 31509** menghasilkan **283835 hits** dan **rule id 31510** menghasilkan **4372 hits**. Hasil ini menunjukkan bahwa serangan *Hacker* dari seluruh dunia sangat banyak bila disangkut pautkan dengan serangan menuju *website*. Serangan yang dilakukan oleh *Hacker* ini bisa dibilang telah terorganisir bila dilitik melalui **rule id 31510.** Karena rule id tersebut menyatakan target serangan hacker ialah website. Hal ini didasari bahwa pada klaster kedua merupakan klaster yang memuat website lama dari Universitas Islam Indonesia sudah lama ada/*exist.* Berbeda dengan website yang ada pada kluster pertama yang berisikan website baru dan belum memiliki konten sebanyak website website yang telah dikelola Universitas Islam Indonesia. Hingga dapat diketahui tujuan *Hacker* adalah untuk menguasai website ternama tersebut.

Laporan dari hasil analisis pada cluster kedua menunjukkan bahwa tingkat serangan bruteforce pada website yang sudah lama ada dan dikenal dilancarkan oleh hacker dengan sasaran website tersebut alih-alih server tempat website tersebut di-hosting.

Berikut adalah tabel perbedaan yang ditemukan saat proses analisis pada klaster pertama dan klaster kedua:

Tabel 2 Perbedaan Hasil Analisis Kedua Klaster

Klaster Pertama	Klaster Kedua
Website yang ada berusia kurang dari 1 tahun sehingga dapat dikatakan sebagai 'website baru'	Website yang ada berusia lebih dari 1 tahun sehingga dapat dikatakan sebagai 'website lama'
Serangan yang ditujukan kepada server tempat website di-hosting jauh lebih banyak dibandingkan website yang ada	Serangan yang ditujukan kepada website yang ada jauh lebih banyak dibandingkan server tempat website di-*hosting*
Rule id 5712 lebih akurat dalam memberikan informasi serangan yang diterima dibandingkan rule id 5710	Rule id 31510 lebih akurat dalam memberikan informasi serangan yang diterima dibandingkan rule id 31509
Menganalisis rule id 5712 yang berfokus pada metadata serangan log yang ditujukan pada ssh server	Menganalisis rule id 31510 yang berfokus pada metadata serangan log yang ditujukan pada web-server nginx
Nama user yang digunakan untuk *brute force* pada rule id 5710 terlihat pada metadata log	Nama user yang digunakan untuk brute force pada rule id 31510 tidak terlihat pada metadata log

4. KESIMPULAN

Hasil analisis forensik menunjukkan pengetahuan baru bahwa serangan yang dilakukan oleh Hacker tidak selamanya dilakukan secara berkelanjutan. Terdapat keadaan dimana Hacker berhenti menyerang dan tidak melanjutkan serangan bruteforce. Kemudian diteliti lebih lanjut dengan memperhatikan IP Address yang sama menunjukkan bahwa Hacker telah berhenti menyerang dan tidak lagi ditujukan ke website manapun. Jumlah serangan yang ditujukan pada klaster pertama sebanyak 259646 serangan menunjukkan serangan kepada Server tempat website di-*hosting* sedangkan pada klaster kedua sebanyak 288676 serangan menunjukkan serangan langsung ditujukan di halaman login Administrator website. Lokasi yang didapatkan pun beragam. Mulai dari ISP yang digunakan oleh hacker hingga server tempat hacker menggunakan VPN untuk menyamarkan lokasi aslinya. Sejauh ini didapatkan informasi bahwa kebanyakan serangan dilancarkan melalui server VPN tersebut. Untuk dapat melacak lokasi hacker dengan lebih akurat dibutuhkan penelitian lebih lanjut, metode baru, serta aplikasi/software pembatu lainnya pula dalam melakukan pelacakan lokasi.

Penelitian ini memberikan kontribusi pada investigasi forensik bagian web server. Hal teknis yang dilakukan adalah membandingkan tingkat serangan yang diterima oleh website baru dan lama menunjukkan perbedaan sisi serangan yang dilancarkan oleh Hacker. Pengetahuan baru dalam penelitian ini menunjukkan bahwa website yang sudah lama ada cenderung diserang bagian login menuju administartor website(log web server), sedangkan pada website baru yang exist belum lama cenderung diserang bagian login server tempat website tersebut di hosting(log ssh).

Selain hal diatas kesimpulan yang dapat diambil yaitu Dasbor Sistem Pencatatan Log Teroptimasi dapat memberikan informasi yang informatif kepada Administrator, SysAdmin maupun User yang menggunakan Dasbor Sistem ini. Hal ini terbukti dengan informasi yang diberikan pada Rule id 5710, 5712, 31509, dan 31510. Dasbor Sistem Pencatatan Log Teroptimasi juga memberikan informasi yang informatif. Hal tersebut berkat bantuan add-ons Wazuh yang dapat memberikan visualisasi yang informatif. Wazuh juga berkontribusi dalam pengembangan Dasbor Sistem Pencatatan Log Teroptimasi dan terbukti layak dan berguna dalam pengembangan CLM (*Centralized Log Management*).

DAFTAR PUSTAKA

[1] I. Arnomo, "Simulasi Pengamanan Database Web Server Repository Institusi Melalui Jaringan Lan Menggunakan Remote Access," *Jurnal Sistem Informasi, Teknologi Informasi dan Komputer*, vol. 9, no. 1, pp. 65–65, Sep. 2018.

[2] C. W. Hukama, B. D. Yuwono, and A. L. Nugraha, "Pembuatan Sistem Informasi Gnss Cors Undip Berbasis Web," *Jurnal Geodesi UNDIP*, vol. 7, no. 1, pp. 90-99, Jan. 2018.

[3] I. K. Satwika and K. N. Semadi, "Perbandingan performansi web server

Apache dan Nginx Dengan menggunakan ipv6," *SCAN - Jurnal Teknologi Informasi dan Komunikasi*, vol. 15, no. 1, 2020.

[4] T. Butar, "Pertanggungjawaban Pidana Pelaku Yang Melakukan Pembobolan Website Pengadilan Negeri Yang Mengakibatkan Sistem Elektronik Tidak Bekerja (Studi Putusan No.25/Pid.Sus/2019/PN Unh).," *Repository Universitas HKBP Nommensen*, pp. 1–52, Feb. 2022.

[5] A. Antoni, "Kejahatan Dunia Maya (cyber crime) Dalam Simak online," Nurani: Jurnal Kajian Syari'ah dan Masyarakat, vol. 17, no. 2, pp. 261–274, Feb. 2018.

[6] Kris Andre Prasetyo, Mohammad Idhom, and Henni Endah Wahanani, "Sistem Pencegahan Serangan Bruteforce Pada Multiple Server Dengan Menggunakan Fail2ban", JIFoSI, vol. 1, no. 3, pp. 789-796, Nov. 2020.

[7] N. K. Ulya, L. E. Nugroho, and D. Adhipta, "Evaluasi Sistem Otentikasi Graphical Password Menggunakan Random Color Berbasis Web," *Repository Universitas Gadjah Mada*, pp. 1–86, 2017.

[8] A. D. Septian, "Monitoring 3 Log Web Server Menggunakan Splunk," *Repository Universitas Muhammadiyah Malang*, pp. 1–38, Dec. 2021.

[9] W. Sholihah, S. Pripambudi, and A. Mardiyono, "Log event management server menggunakan elastic search Logstash Kibana (elk stack)," JTIM : Jurnal Teknologi Informasi dan Multimedia, vol. 2, no. 1, pp. 12–20, May 2020.

[10] D. Lintang, "Monitoring Aktivitas User pada System dengan Menggunakan EFK (Elasticsearch, Fluentd, Kibana) Stack," *Repository Universitas Islam Indonesia (dspace)*, pp. 1–62, Nov. 2019.

[11] R. P. Aji, "'Pengembangan Dasbor Sistem Pencatatan Log Server Menggunakan Elasticsearch-Fluentd- Kibana (Efk) Stack," *Automata*, vol. 1, no. 2, Jun. 2020.

[12] F. Nova, M. D. Pratama, and D. Prayama, "Wazuh Sebagai log event management Dan Deteksi Celah Keamanan Pada server dari serangan dos," JITSI : Jurnal Ilmiah Teknologi Sistem Informasi, vol. 3, no. 1, pp. 1–7, Mar. 2022.

[13] R. Watrianthos, A. Iskandar, A. F. Pakpahan, E. B. Wagiu, J. Simarmata, O. K. Sulaiman, and Jamaludin, "Prinsip dan Metodologi Forensika Digital," in Forensika Digital, A. Rikki, Ed. Medan, Sumatra Barat: Yayasan Kita Menulis, 2021, pp. 5–5.

[14] F. C. Freiling and B. Schwittay, "A Common Process Model for Incident Response and Computer Forensics (2007)," Proceedings of Conference on IT Incident Management and IT Forensics, 2007.

[15] F. Mulyadi, L. A. Annam, R. Promya, and C. Charnsripinyo, "Implementing dockerized elastic stack for security information and event management," 2020 - 5th International Conference on Information Technology (InCIT), Oct. 2020..