TESIS

Analisis *Log* Serangan *BruteForce* Terhadap *Web Server Nginx* Pada Dasbor Sistem Pencatatan Log Teroptimasi Menggunakan Metode Investigasi Forensik

Rio Pradana Aji

20917052

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer

Konsentrasi Forensika Digital

Program Studi Informatika Program Magister

Fakultas Teknologi Industri

Universitas Islam Indonesia

2022

Halaman Pengesahan Dosen Pembimbing

Analisis *Log* Serangan *Bruteforce* Terhadap *Web Server Nginx* Pada Dasbor Sistem Pencatatan Log Teroptimasi Menggunakan Metode Investigasi Forensik

Rio Pradana Aji
20917052

Yogyakarta, Desember 2022

Pembimbing	Pembimbing
Dr. Yudi Prayudi S.SI., M.Kom.	Dr. Ahmad Luthfi, S.Kom., M.Kom.

Lembar Pengesahan Penguji

Analisis *Log* Serangan *Bruteforce* Terhadap *Web Server Nginx* Pada Dasbor Sistem Pencatatan Log Teroptimasi Menggunakan Metode Investigasi Forensik

Rio Pradana Aji

20917052

Yogyakarta, 24 Desember 2022

Tim Penguji,

Dr. Yudi Prayudi, S.Si., M.Kom.
Ketua

Dr. Ahmad Luthfi, S.Kom., M.Kom.
Anggota I

Dr. Imam Riadi, M.Kom.
Anggota II

Mengetahui,

Ketua Program Studi Informatika Program Magister

Universitas Islam Indonesia

Irving Vitra Paputungan, S.T., M.Sc., Ph.D.

Abstrak

Analisis Log Serangan BruteForce Terhadap Web Server Nginx Pada Dasbor Sistem Pencatatan Log Teroptimasi Menggunakan Metode Investigasi Forensik

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 Investigasi Forensik Kuantitatif yang memiliki 5 tahapan yaitu *Identification, Problem Scope, Collection Examination, Analysis, and Presentation* digunakan dalam penelitian ini untuk menganalisis *log* yang dihasilkan Dasbor Sistem. Adapun *log* yang diteliti berdasarkan *rule id* bawaan wazuh (*rule id* 5710 dan 31509) dan Rule id hasil optimasi (*rule id* 5712 dan 31510) dan *tweak* yang dilakukan selama proses penelitian berlangsung. 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

website, bruteforce, monitoring, wazuh, forensik digital.

Abstract

Analysis Of BruteForce Attack Logs Toward Nginx Web Server On Dashboard Optimized Log Logging System Using Forensic Investigation Method

Since it was first launched in 1990 the Web Server is still in use today. It is no exception that almost all companies entering industry 4.0 use Web Servers to show the existence of company websites and products they have. Starting from websites that are provided free of charge by Wordpress and Blogspot to independent websites created by their respective companies. The web server itself is available in several types, starting from Apache, Nginx, Litespeed, etc. Of course the use of Web Servers for websites cannot be separated from internet crimes or cyber crimes. One of the crimes committed is the hacker's attempt to log into the website Administrator page. The loophole used by hackers is brute force or forced entry by trying every existing combination of User and Administrator Password. This research focuses on building and updating a website monitoring dashboard system with Wazuh technology. The Quantitative Forensic Investigation Method which has 5 stages, namely Identification, Problem Scope, Collection Examination, Analysis, and Presentation is used in this study to analyze the logs generated by the System Dashboard. The logs studied were based on the default wazuh rule id (rule id 5710 and 31509) and the optimized rule id (rule id 5712 and 31510) and tweaks made during the research process. This monitoring process aims to detect brute force threats on websites that are managed by showing the activity log of the website Administrator login. The results of the metadata log shown by the optimized dashboard show the number of brute force attacks on the website being managed. The number of attacks recorded was 259646 attacks in the first cluster and 288676 attacks in the second cluster. In addition, the results of the metadata log can be further investigated to find the location of the hacker. The location of the hackers found was limited to the VPN (Virtual Private Network) server used. One of the VPN servers used in this case is the Amazon Data Center.

Kata kunci

website, bruteforce, monitoring, wazuh, digital forensics.

Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, Desember 2022

Rio Pradana Aji, S.Kom

Daftar Publikasi

Publikasi yang menjadi bagian dari tesis

R. P. Aji, S.Kom, D. Y. Prayudi, S.SI., M.Kom., and D. A. L. S.Kom., M.Kom., "ANALISIS LOG SERANGAN BRUTEFORCE TERHADAP WEB SERVER NGINX PADA DASHBOR SISTEM PENCATATAN LOG TERIMPROVISASI MENGGUNAKAN METODE INVESTIGASI FORENSIK," *Jurnal Teknik Informatika (JUTIF) UNIVERSITAS JENDERAL SOEDIRMAN (UNSOED)*, vol. 4, no. 1, Feb. 2023.

Kontributor	Jenis Kontribusi
Rio Pradana Aji, S.Kom	Studi Literatur (100%) Mendesain eksperimen (90%) Merumuskan *Framework* (80%) Menulis *paper* (90%)
Dr. Yudi Prayudi, S.Si., M.Kom.	Mengevaluasi *paper* (20%)
Dr. Ahmad Luthfi, S.Kom., M.Kom.	Mendesain eksperimen (10%) Merumuskan *Framework* (20%) Mengevaluasi *paper* (100%)

Halaman Kontribusi

Kontribusi dari beberapa pihak terkait dalam penyelesaian penelitian tesis ini, diantaranya:

1. Bapak Dr. Yudi Prayudi, S.Si., M.Kom. selaku Dosen Pembimbing I (Dosen Payung) yang telah memberikan bimbingan dan dukungan untuk menyelesaikan penelitian tesis mulai dari proses proposal, progress, hingga sidang pendadaran tesis.
2. Bapak Dr. Ahmad Luthfi, S.Kom., M.Kom. selaku Dosen Pembimbing II yang telah banyak memberikan bimbingan, arahan, motivasi, ilmu, dukungan, serta waktu dan tenaga dalam menuntun saya menyelesaikan penelitian mulai dari proses pencarian judul/tema, proses proposal, progress, hingga sidang pendadaran tesis.
3. Dinharjaya dan Erna Listiyani selaku Ayah dan Ibu yang telah membiayai seluruh biaya perkuliahan serta memberikan dukungan moral dalam tahap penyelesaian tesis ini.
4. Indah Ridhawati selaku istri tercinta selalu memberikan semangat dan dukungan dari mulai awal perkuliahan hingga sidang pendadaran tesis
5. Seluruh teman-teman Angkatan FD-23 dan teman-teman di Magister Informatika UII lainnya yang telah meluangkan waktu untuk berbagi terkait tahapan penyelesaian tesis.

Kata Pengantar

Assalamu'alaikum Warahmatullahi Wabarakatuh

Alhamdulillah saya haturkan kepada Allah *Subhanahu wa ta'ala*, yang telah melimpahkan rahmat dan taufiq serta hidayat-Nya, sehingga Tesis yang berjudul "**Analisis *Log* Serangan *BruteForce* Terhadap *Web Server Nginx* Pada Dasbor Sistem Pencatatan Log Teroptimasi Menggunakan Metode Investigasi Forensik**" ini dapat terselesaikan. Shalawat serta salam tak lupa penulis haturkan kepada junjungan kita Nabi Muhammad *shalallahu 'alaihi wa salam.*

Penulisan Tesis ini bertujuan untuk memenuhi persyaratan mendapatkan gelar Master di Program Studi Magister Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia.

Selama penulisan Tesis ini, penulis banyak menerima dukungan dan masukan sehingga dapat menyelesaikan laporan ini, oleh karena itu, penulis mengucapkan terima kasih setulusnya kepada :

1. Allah *Subhanahu wa ta'ala* karena tanpa izin-Nya penulis tidak akan mampu menyelesaikan laporan ini.
2. Bapak Dinharjaya dan Ibu Erna Listiyani selaku kedua orang tua, Adik saya Dyah Ayu Pramesti Regita Putri, serta Istri saya Indah Ridhawati yang selama ini selalu mendoakan dan memberi dukungan moral dan materi.
3. Bapak Ahmad Luthfi, S.Kom., M.Kom., Ph.D. selaku dosen pembimbing kedua yang banyak membantu dan meluangkan waktu untuk membimbing, memeriksa, dan memberikan saran dalam penyusunan laporan ini.
4. Bapak Dr. Yudi Prayudi S.SI., M.Kom. selaku dosen pembimbing pertama yang banyak membantu dan meluangkan waktu untuk membimbing, memeriksa, dan memberikan saran dalam penyusunan laporan ini.

Akhir kata penulis menyadari bahwa laporan ini masih jauh dari kata sempurna oleh karena itu kritik dan saran yang bersifat membangun akan penulis terima dengan senang hati dan semoga laporan ini bermanfaat bagi semua pihak yang memerlukan.

Wassalamualaikum Warahmatullahi Wabarakatuh

Yogyakarta, 10 Desember 2022

Rio Pradana Aji

Glosarium

Dasbor	Alat yang digunakan dalam manajemen informasi atau kumpulan informasi.
Log	file yang berisikan sejarah/*history* penggunaan suatu aplikasi, *tools,* maupun perangkat keras.
CLM	CLM atau *Centralized Log Management* merupakan suatu *tools* yang digunakan untuk memonitor *log* secara terpusat.
Klaster	Pengelompokan atau bisa disebut dengan suatu kelompok.
Hacker	Suatu individu atau kelompok yang bertujuan menginfiltrasi sistem aplikasi/server.
BruteForce	Usaha paksa yang dilakukan hacker untuk masuk ke dalam sistem.
Rule Id	Standarisasi Wazuh dalam menentukan informasi *log* yang diberikan.

Daftar Isi

Halaman Pengesahan Dosen Pembimbing i

Lembar Pengesahan Penguji ii

Abstrak iii

Abstract iv

Pernyataan Keaslian Tulisan v

Daftar Publikasi vi

Halaman Kontribusi vii

Kata Pengantar viii

Glosarium ix

Daftar Isi x

Daftar Gambar xii

Daftar Tabel xiv

BAB 1 1

1.1. Latar Belakang 1

1.2. Rumusan Masalah 5

1.3. Batasan Masalah 5

1.4. Tujuan Penelitian 6

1.5. Manfaat Penelitian 6

BAB 2 7

2.1. Optimasi Dasbor 7

2.2. Literatur Review 10

2.3. Kajian Log Web Server 13

2.3.1. Elasticstack 13

2.3.2. Elasticsearch 14

2.3.3. Filebeat 14

2.3.4. Logstash 15
2.3.5. Kibana 15
2.3.6. Wazuh 16
2.3.7. Log 17
BAB 3 18
3.1. Langkah Penelitian 18
3.2. Optimasi Dasbor 21
3.3. Analisis Log 22
3.4. Metode Investigasi Forensik 23
BAB 4 HASIL DAN PEMBAHASAN 34
4.1. Hasil Implementasi Sistem Dasbor Teroptimasi 34
4.2. Pembahasan Proses Investigasi Forensik 36
4.2.1 Pengumpulan Data Klaster Pertama 36
4.2.2 Hasil Analisis Klaster Pertama 44
4.2.3 Laporan Hasil Analisis Klaster Pertama 52
4.2.4 Pengumpulan Data klaster Kedua 53
4.2.5 Hasil Analisis Klaster Kedua 63
4.2.6 Laporan Hasil Analisis Klaster Kedua 72
4.3. Perbedaan Hasil Analisis Klaster Pertama dan Klaster Kedua 74
4.4. Hasil Analisis Penelitian Terbaru dengan Penelitian Sebelumnya 75
BAB 5 KESIMPULAN DAN SARAN 77
5.1. Kesimpulan 77
5.2. Saran 77
Daftar Pustaka 78

Daftar Gambar

Gambar 2.1 Komponen dari Elasticstack 13
Gambar 2.2 Logo Wazuh..... 16
Gambar 2.3 Contoh Log Pada OS Linux..... 17
Gambar 3.1 Alur Metode Penelitian..... 18
Gambar 3. 2 Alur Proses Investigasi 19
Gambar 3.3 Skenario Penelitian 20
Gambar 3.4 Optimasi Dasbor 22
Gambar 3.5 *Log* SSH..... 25
Gambar 3.6 *Log* Nginx 25
Gambar 3.7 *Log* Auditd..... 25
Gambar 3.8 Tutorial Wazuh 26
Gambar 3.9 Letak ossec.conf 26
Gambar 3.10 Path pengambilan Log SSH..... 27
Gambar 3.11 Path pengambilan Log SSH..... 27
Gambar 3.12 Path pengambilan Log Auditd..... 27
Gambar 3.13 Rules baru pada local_rules..... 28
Gambar 3.14 Hasil *Log* yang di-*generate* Wazuh..... 29
Gambar 3.15 *Log brute force* yang di-*generate* Wazuh..... 29
Gambar 3.16 Isi dari keterangan *log brute force*..... 30
Gambar 3.17 Menunjukkan Serangan *brute force ke Website* 30
Gambar 3.18 Isi dari keterangan *brute force* website..... 31
Gambar 3.19 *Log* Auditd tidak ter-*compromise*..... 32
Gambar 3.20 *Log* Auditd dalam keadaan Normal..... 32
Gambar 4. 1 Rule id 5710 klaster pertama 37
Gambar 4.2 Rule id 5712 klaster pertama 37
Gambar 4.3 Rule id 31509 klaster pertama 38
Gambar 4.4 Rule id 31510 klaster pertama 38
Gambar 4.5 Hasil Rule id 31509 ke website canyoubruteforceme.my.id 39
Gambar 4. 6 Hasil Rule id 31510 ke website canyoubruteforceme.my.id 39
Gambar 4.7 Hasil Rule id 31509 ke website datapenelitiantesis.my.id..... 40
Gambar 4.8 Hasil Rule id 31510 ke website datapenelitiantesis.my.id..... 40

Gambar 4.9 Hasil Rule id 31509 ke website websitepenelitiantesis.my.id 41
Gambar 4.10 Hasil Rule id 31509 ke website websitepenelitiantesis.my.id 42
Gambar 4.11 Hasil Rule id 31509 ke website bruteforcethiswebsite.my.id 42
Gambar 4.12 Hasil Rule id 31510 ke website bruteforcethiswebsite.my.id 43
Gambar 4.13 Hasil Rule id 31509 ke website penelitiantesis.my.id 44
Gambar 4.14 Hasil Rule id 31510 ke website penelitiantesis.my.id 44
Gambar 4.15 Metadata Log SSH Rule id 5710 46
Gambar 4.16 Metadata Log SSH rule id 5712 48
Gambar 4.17 Tempat *Hacker* melancarkan serangan 52
Gambar 4.18 Indikasi *brute force* dilakukan oleh orang yang sama 53
Gambar 4.19 Contoh Metadata Log serangan yang intens 53
Gambar 4.20 Rule id 5710 klaster kedua 54
Gambar 4.21 Rule id 5712 klaster kedua 54
Gambar 4.22 Rule id 31509 klaster kedua 55
Gambar 4.23 Rule id 31509 klaster kedua 55
Gambar 4.24 Hasil Rule id 31509 ke website law.uii.ac.id 56
Gambar 4.25 Hasil Rule id 31510 ke website law.uii.ac.id 56
Gambar 4.26 Hasil Rule id 31509 ke website fis.uii.ac.id 57
Gambar 4.27 Hasil Rule id 31510 ke website fis.uii.ac.id 58
Gambar 4.28 Hasil Rule id 31509 ke website ee.uii.ac.id 59
Gambar 4.29 Hasil Rule id 31510 ke website ee.uii.ac.id 59
Gambar 4.30 Hasil Rule id 31509 ke website fit.uii.ac.id 60
Gambar 4. 31 Hasil Rule id 31510 ke website fit.uii.ac.id 61
Gambar 4.32 Hasil Rule id 31509 ke website conference.communication.uii.ac.id 62
Gambar 4.33 Hasil Rule id 31510 ke website conference.communication.uii.ac.id 62
Gambar 4.34 Metadata Log Nginx Rule id 31510 65
Gambar 4. 35 Lokasi *Hacker* melancarkan serangan 73
Gambar 4.36 Perubahan Dasbor Yang Dilakukan 76

Daftar Tabel

Tabel 2. 1 Literatur Review 10
Tabel 3.1 Rancangan Tabel Perbandingan Hasil Analisis 20
Tabel 3.2 Tahapan Investigasi Forensik 24
Tabel 4.1 5 Negara terbesar penyerang website canyoubruteforceme.my.id 39
Tabel 4.2 5 Negara terbesar penyerang website datapenelitiantesis.my.id 40
Tabel 4.3 5 Negara terbesar penyerang website websitepenelitiantesis.my.id 42
Tabel 4.4 5 Negara terbesar penyerang website bruteforcethiswebsite.my.id 43
Tabel 4.5 5 Negara terbesar penyerang website penelitiantesis.my.id 44
Tabel 4.6 Penjelasan Metadata Log Rule id 5712 48
Tabel 4.7 5 Negara terbesar penyerang website law.uii.ac.id 57
Tabel 4.8 Negara terbesar penyerang website fis.uii.ac.id 58
Tabel 4.9 5 Negara terbesar penyerang website ee.uii.ac.id 59
Tabel 4.10 5 Negara terbesar penyerang website fit.uii.ac.id 61
Tabel 4.11 5 Negara terbesar penyerang website conference.communication.uii.ac.id 62
Tabel 4.12 Penjelasan Metadata Log Rule id 31510 66
Tabel 4.13 Perbedaan Hasil Analisis Kedua Klaster 75

BAB 1
PENDAHULUAN

1.1. Latar Belakang

Salah satu teknologi internet yang hingga saat ini masih terus digunakan adalah *web server*. 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. 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, lightspeed, microsoft iis, lighttpd,* dan lain sebagainya. Hingga saat ini *web server* yang paling banyak digunakan adalah *apache* dan *nginx.*

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 atau usaha untuk masuk ke server tempat *web server* berada (*hosting*). 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 menjalankan tindakan kejahatan ini. 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,* yaitu mencoba setiap kombinasi User dan Password Administrator yang ada pada halaman login website. User dan Password Administrator yang lemah biasanya akan dengan mudah didapatkan. Kejahatan dunia maya *brute force* ini pada dasarnya telah sedari dulu pertama kali form login diciptakan. Pada dasarnya tindak kejahatan ini bertujuan untuk memperoleh hak tertinggi pada suatu sistem atau organisasi. Organisasi maupun perusahaan yang

menggunakan website sebagai *backbone* dalam menjalankan aktivitasnya merupakan sasaran empuk bagi Hacker, terlebih jika website yang dikelola ramai dikunjungi. Tindak kejahatan ini tidak dapat terdeteksi, tiba-tiba saja data hilang hingga website yang dikelola hilang atau rusak karena tanpa sadar *Hacker* sudah masuk ke dalam website tersebut. Tindakan pencegahan paling awal adalah membuat kombinasi User dan Password sebaik mungkin dengan menggunakan kombinasi huruf kecil dan besar, angka, dan simbol.

Selain tindakan pencegahan dengan membuat kombinasi User dan Password yang unik terdapat cara lainnya. Monitoring merupakan salah satu cara lain dalam tindakan pencegahan tersebut. Hal yang dilakukan adalah melihat/memonitor server terkait siapa saja yang berusaha masuk ke dalam website yang dikelola dengan menggunakan akun Administrator. Proses monitoring 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. Hal ini sering terjadi kepada Administrator pengelola website yang menyepelekan jumlah website yang harus dipantau/dikelola. Solusi dari permasalahan tersebut dapat dicapai dengan mengembangkan *Centralized Log Management* server. Diharapkan dengan dikembangkanya CLM dapat mempersingkat waktu dalam menemukan *issue* serta perbaikan dapat dilakukan dengan segera.

Pada pengembangan CLM tersebut dapat dibantu dengan berbagai macam sarana aplikas/*tools* yang disesuaikan 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.

Adapun penelitian yang dilakukan oleh (Danur, 2020) menggunakan EFK stack untuk membuat *Log Monitoring System* dengan server-server yang berada di AWS (Amazon Web Service) dan kemudian diintegrasikan ke Slack untuk notifikasi alert yang terjadi di server AWS tersebut. Penelitian yang dilakukan oleh (Yhoga, 2019) menggunakan ELK stack untuk Memonitor *web server* dan radius server yang ada di Badan Sistem Informasi

(BSI) Universitas Islam Indonesia (UII) terkait keamanan website dan server yang terdapat di BSI UII. Terakhir penelitian yang dilakukan oleh (Walidatush, 2020) menggunakan ELK stack untuk membuat *Log Event Management Server* yang memonitor berhasil dan gagalnya akses ssh ke sebuah server.

Pada penelitian sebelumnya, peneliti telah melakukan pengembangan dasbor sistem pencatatan *log* server dengan permasalahan belum terdapat dasbor sistem pencatatan *log* pada perusahaan tempat peneliti bekerja. Sebelum dibuatnya dasbor sistem pencatatan *log* ini para SysAdmin melakukan pengecekan *log* pada server secara manual dengan masuk ke server secara satu persatu. Tujuan dikembangkannya dasbor sistem pencatatan *log* adalah untuk mempermudah SysAdmin dalam memonitoring log yang ada pada server sehingga SysAdmin tidak perlu mengecek *log* secara satu persatu pada server. Hasilnya adalah dasbor sistem pencatatan *log* tersebut memberikan informasi terkait error *log* pada server yang kemudian diinvestigasi/dimonitor oleh SysAdmin. Namun, hasil visualisasi masih sangat sederhana dan dibuatnya visualisasi masih berdasarkan rumusan sederhana dasbor.

Berangkat dari pengalaman inilah dilakukannya proses optimasi dasbor sistem pencatatan log server. Optimasi dilakukan berkaitan dengan hasil dasbor sistem pencatatan log yang dikembangkan sebelumnya belum memberikan informasi yang informatif bagi para SysAdmin. Padahal informasi yang informatif yang dihasilkan oleh dasbor merupakan sarana SysAdmin dalam memahami permasalahan dan keadaan website dan server yang dikelola. Tanpa adanya informasi yang informatif ini CLM yang telah dikembangkan menjadi sia-sia dan SysAdmin perlu mengerahkan waktu lagi dalam memahami permasalahan/*issue* yang terjadi pada website dan server yang dikelola. Maka dari itu setelah optimasi selesai dilakukan, diharapkan dasbor sistem pencatatan log dapat memberikan informasi yang informatif bagi SysAdmin sehingga proses penemuan dan penyelesaian masalah dapat dilakukan dengan cepat dan tepat.

Proses optimasi dasbor sistem pencatatan log ini dapat dicapai dengan beberapa metode. Tepatnya ada 3 metode atau opsi yang dapat dilakukan dalam proses optimasi dasbor sistem pencatatan log server. Pertama proses optimasi dilakukan dengan meneruskan dasbor sistem yang lama dengan membuat visualisasi yang lebih kompleks dan informatif, namun hal ini tidak dilakukan dengan alasan akan memakan waktu lama untuk mencoba membuat *log* informatif tersebut (riset, *trial and error*). Kedua proses optimasi dilakukan dengan menggunakan *tools* kompleks semacam Security Onion (SO) dalam membangun dasbor sistem, meskipun Security Onion sangat mumpuni hal ini tidak dipilih karena kompleksitas penggunaan, fokus utama SO pada *network sniffing*, alokasi waktu untuk

belajar menggunakan SO karena kompleksitasnya. Ketiga proses optimasi dilakukan dengan menggunakan *tools* Wazuh yang merupakan *add-ons* pada Kibana. Opsi ketiga Wazuh inilah yang dipilih dalam mengoptimasi CLM atau dasbor sistem pencatatan log server. Dipilihnya Wazuh sebagai optimasi dasbor sistem pencatatan log karena pada Wazuh telah terdapat *built-in* log, *open source,* penggunaan yang mudah, dan komunitas yang solid sebagai wadah untuk bertanya perihal pengaplikasian Wazuh.

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. 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.

Solusi dari penelitian sebelumnya yaitu dasbor sistem pencatatan log belum memberikan informasi yang informatif dapat dicapai dengan mengoptimasi dasbor sistem menggunakan Wazuh klaster. Diharapkan pula solusi ini dapat membantu SysAdmin dalam memonitor server dan website yang dikelola dengan mudah.

Tujuan dari penelitian tesis ini adalah untuk mengoptimasi Dasbor Sistem Pencatatan Log Server dengan fokus pada Web Server Nginx dan Server tempat website di-*hosting*. Selain itu tujuan lainnya adalah memberikan analisis 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.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang sudah dipaparkan di atas, penelitian ini memiliki rumusan masalah yaitu :

a. Apakah hasil analisis pada dasbor sistem pencatatan log teroptimasi sudah memberikan informasi mengenai serangan *brute force* secara informatif untuk Administrator atau SysAdmin ?.
b. Apakah informasi *log* yang diberikan dasbor teroptimasi lebih informatif dibandingkan dasbor sistem pencatatan *log* sebelumnya pada saat server atau website terkena serangan *brute force* ?.
c. Apakah Wazuh mampu menjadi *tools* yang berguna dalam membangun CLM untuk memonitor server dan website yang dikelola oleh Administrator atau SysAdmin ?.

1.3. Batasan Masalah

Berdasarkan pemaparan latar belakang di atas, batasan masalah penelitian ini akan dipaparkan juga untuk membatasi ruang lingkup penelitian sehingga tidak keluar dari masalah yang diteliti. Adapun berikut adalah batasan masalah yang ada :

a. Analisis penelitian berfokus pada log serangan *brute force* pada Web Server Nginx. Adapun penjelasannya *log* nginx untuk mengetahui *brute force* dari sisi website.
b. Log lainnya untuk mendukung analisis adalah log ssh dan auditd. Adapun penjelasannya log ssh untuk mengetahui *brute force* pada sisi server website yang di *hosting.* Sedangkan log auditd untuk mengetahui *malicious command* yang dilakukan user pada server bila terdapat indikasi *hacker* sudah masuk ke dalam serverwebsite.
c. Penelitian ini dilakukan dengan metode Investigasi Forensik dengan fokus log yang akan dianalisis adalah 3 log yang sudah dijabarkan pada poin a dan b diatas.

d. Optimasi dasbor sistem pencatatan log server menggunakan *tools* Wazuh.

1.4. Tujuan Penelitian

Tujuan dari dilakukannya penelitian ini adalah :

a. Menganalisis log server yang menunjukkan indikasi *brute force* pada website dan server website dengan menggunakan metode Investigasi Forensik dan kaidah Forensika Digital. Sehingga nantinya penelitian ini terdapat irisan antara analisis log dan forensika digital. Hasil dari dasbor teroptimasi diharapkan memberikan informasi mengenai serangan *bruteforce* secara informatif,
b. Analisis yang dilakukan diharapkan memberikan informasi apakah dasbor sistem pencatatan log teroptimasi menghasilkan informasi yang informatif dan dapat menggantikan dasbor pada penelitian sebelumnya yang masih minim informasi.
c. Penelitian ini memanfaatkan *tool* Wazuh untuk memberikan informasi mengenai serangan *brute force* yang ada pada server dan website. Hasil akhirnya adalah analisis terhadap metadata yang dihasilkan oleh Wazuh untuk kemudian dilakukan penjabaran serta membuktikan kegunaan Wazuh sebagai opsi *Centralized Log Management*.

1.5. Manfaat Penelitian

Manfaat yang dihasilkan oleh penelitian ini ada berbagai macam, yaitu :

a. Membantu *owner* website atau SysAdmin dalam memantau website yang dikelola dalam sisi keamanan.
b. Mengetahui indikasi *brute force* yang terjadi pada website maupun server website agar dapat dilakukan pencegahan dan penanganan dini.
c. Mengoptimasi Dasbor Sistem Pencatatan Log Server pada penelitian sebelumnya.
d. Menghasilkan *knowledge* baru bagi dunia forensika digital berdasarkan analisis yang dilakukan oleh Wazuh.

BAB 2
LANDASAN TEORI

2.1. Optimasi Dasbor

Proses optimasi dasbor sistem pencatatan *log* ini merupakan optimasi dari dasbor sistem pencatatan *log* yang telah dibuat sebelumnya. Pada penelitian sebelumnya dasbor sistem pencatatan *log* yang dibuat masih kurang informatif lantaran hanya dibuat ala kadar saja pada visualisasinya. Sedangkan dasbor sistem pencatatan *log* yang akan dioptimasi pada penelitian ini sudah memakai bantuan teknologi Wazuh yang dalam menampilkan *log* sangat informatif. Adapun dasbor sistem pencatatan *log* yang dioptimasi akan berfokus pada *log* terkait *web server nginx* dan server website yang dikelola oleh Administrator website meskipun tidak dapat dipungkiri Wazuh menawarkan berbagai macam log lainnya. Namun untuk fokus penelitian maka log yang akan menjadi objek penelitian adalah *log brute force* pada *web server nginx* dan server website. Hasil *log* yang di-*generate* oleh Wazuh diharapkan dapat membantu memberikan *knowledge base* baru pada bidang Forensika Digital bagi Investigator. Sehingga dalam menyelesaikan kasus yang ada dapat dilakukan secara cepat dan akurat.

Adapun hal yang dilakukan dalam penelitian ini yaitu dengan menganalisis *log* kedua klaster server yang berbeda. Kedua Klaster yang berbeda ini memiliki sifat yang berbeda satu dengan yang lainnya. Pada klaster pertama merupakan sebuah klaster baru dengan isi website yang baru dibuat pula sedangkan pada klaster kedua merupakan klaster lama dengan isi website yang sudah lama *exist*. Hal ini dilakukan untuk melihat *behavior* yang terjadi ketika *brute force* sedang terjadi. Hasil dari kedua klaster tersebut yang berupa metadata log *brute force* dapat ditampilkan menggunakan visualisasi Dasbor Sistem Pencatatan Log Teroptimasi yang Wazuh berikan secara informatif dibandingkan Dasbor Sistem Pencatatan Log sebelumnya. Sehingga para Administrator dan Investigator dapat mendapatkan data *log* secara cepat tanpa harus melakukan pencarian/penelitian *log* manual dengan masuk ke server klaster.

Langkah yang dilakukan oleh (Ega Pratama, 2019) dalam mengoptimasi Radius Server yaitu dengan mengintegrasikan Radius server dengan Mikrotik Router OS. Integrasi tersebut dilakukan untuk memberikan batas waktu penggunaan dan batas waktu *download* bagi pengguna yang menggunakan *wifi hotspot*. Hal ini dapat dicapai lantaran optimasi dari Radius Server yang semula hanya memberikan akses internet saja tanpa batas *bandwidth*

kemudian diintegrasikan dengan Mikrotik Router OS untuk memberikan batas-batas bandwidth yang sudah dikonfigurasi.

Penelitian yang dilakukan oleh (Fahmi Kurniawan, 2020) dalam optimasi *live streaming* pada website dengan menggunakan teknologi *microservices* docker dan *load balancer* pada nginx alih-alih menggunakan teknologi *monolith*. Optimasi yang dilakukan adalah dengan mengganti teknologi monolith yang bertopang pada 1 VPS (Virtual Private Server) untuk menampung semua *services* dengan teknologi *microservices*. Teknologi ini menggantikan VPS tersebut dengan *container* agar *services* website *streaming* ketika *down* dapat kembali *up* dengan cepat karena *services* satu dengan yang lainnya terisolasi. *Load balancer* juga berfungsi ketika permintaan akses server *overload* maka akan segera disortir berdasarkan server yang tersedia.

Optimasi pada server yang dilakukan oleh (Wahyu Hidayat, 2018) menggunakan Mirror Server dan Men-*cached* untuk meningkatkan server *response time*. Respon server ini berpengaruh terkait jumlah mahasiswa yang meningkat dan mengakses sistem akademik kampus. Tanpa digunakannya kedua teknologi ini maka respon server akan sangat lambat bahkan bisa terjadi *system down*. Dalam menangani hal tersebut optimasi server dilakukan dengan menambahkan *Mirror Server* untuk bertindak sebagai server yang sama persis dengan server utama. Sedangkan fungsi Mem-*cached* adalah *script* yang diletakkan pada server dan berfungsi ketika ada *request* akan menyeleksi apakah data tersebut ada di *Mirror Server* atau server utama. Proses seleksi inilah yang meningkatkan respon server karena *request* tadi tidak perlu sampai di server utama jika data ada di *Mirror Server*.

Proses optimasi pada dasbor sistem pencatatan data yang dilakukan oleh (Sumiari, 2019) menggunakan algoritma Levenshtein Distance untuk mengatasi kesalahan input data oleh Administrator. Dasbor sistem pencatatan data yang dimiliki oleh STMIK STIKOM Bali merupakan aplikasi yang mereka miliki untuk mengumpulkan semua data aplikasi lainnya yang telah terintegrasi. Aplikasi yang berbasis website ini dibangun menggunakan bahasa pemrograman PHP dan framework bootstrap. Hal yang dioptimasi dalam aplikasi Dasbor Sistem Pencatatan Data ini adalah proses dalam pencarian data yang diimplementasikan algoritma Levenshtein Distance sehingga ketika Administrator atau User yang menggunakan Dasbor ini mencari kata yang salah atau tidak ada maka terdapat kata rekomendasi serupa dari kata yang diinputkan oleh Administrator ataupun User.

Hal yang dilakukan oleh (Jefi dkk 2020) yaitu mengoptimasi data gaji karyawan Perusahaan Outsourcing yang semula hanya di Ms. Excel menjadi aplikasi yang menggunakan bahasa pemrograman PHP dan CSS berbasis Website. Pengoptimasian yang

dilakukan pada Perusahaan Outsourcing ini merupakan usaha mempermudah dalam mengelola data karyawan yang dimiliki. File yang memuat data krusial perusahaan tersebut yang berpotensi hilang, tercuri, dan dimanipulasi telah menjadi sebuah dasbor sistem pencatatan data. Pemilik tidak lagi takut kehilangan data hingga dapat melakukan proses pengawasan sederhana dimana user dan password untuk masuk ke dalam aplikasi diberikan kepada beberapa orang saja. Sehingga jika terdapat kesalahan input atau indikasi kecurangan dapat diketahui siapa yang dapat mengakses website aplikasi tersebut.

Usaha yang dilakukan oleh (Ardian Prima dkk, 2019) mengoptimasi Sistem Informasi Manajemen dan Akuntansi Barang Milik Negara (SIMAK BMN). Keterbatasan penggunaan SIMAK BMN merupakan hal yang mendasari dilakukannya proses optimasi.Proses optimasi yang dilakukan ialah menjadikan sistem tersebut dapat diakses melalui internet serta membuat aplikasi *mobile* berbasis android SIMAK BMN. Hal ini nantinya akan mempermudah pegawai dalam melakukan proses monitoring barang tersebut. Terutama kemudahan dalam men-*scan* barang menggunakan QR Code yang ada di *Smartphone* sehingga barang dapat tercatat saat itu juga tanpa proses yang bertele-tele seperti mencatat di kertas kemudian baru di-*input* pada komputer.

Tindakan yang dilakukan oleh (Mahardika dkk, 2018) yaitu mengoptimasi metode K-Nearest Neighbour (KNN) menggunakan Particle Swarm Optimization (PSO) pada sistem pakar yang digunakan untuk memonitor pengendalian hama pada tanaman jeruk. Proses optimasi yang dilakukan ini berbeda dengan yang lainnya karena hal yang dioptimasi adalah rumus/metode yang digunakan pada sistem pakar monitoring. Hasil yang didapat menunjukkan terdapat sebuah peningkatan akurasi pada sebelum dan sesudah dilakukannya optimasi sebanyak 90% pada KNN tertinggi dan 96,25% pada PSO-KNN tertinggi. Adanya peningkatan akurasi menunjukkan bahwa metode PSO mampu memperbaiki kekurangan yang ada pada metode KNN.

Pengoptimasian yang dilakukan oleh (Setiawan dkk. 2022) yaitu melakukan pembaruan dari proses pencatatan produk gula yang sudah selesai di *packing* masih menggunakan tenaga manusia diubah menggunakan sistem aplikasi. Aplikasi SCADA yang digunakan berbasis *Distributed Control System* (DCS) diharapkan dapat membantu proses monitoring serta meningkatkan proses pencatatan dan pendataan produk yang sudah di produksi. Hasil yang didapatkan melalui simulasi penelitian menunjukkan bahwa waktu produksi gula tertinggi dan terendah dapat diketahui dengan jelas. Hal ini dapat digunakan oleh operator untuk meningkatkan efisiensi dan produktifitas dalam melakukan pencatatan dan pendataan produksi gula.

Berdasarkan pemaparan penelitian sebelumnya sebagai fondasi *Knowledge Base* didapatkan informasi bahwa proses optimasi dapat dilakukan dengan mengenalkan hal baru kepada objek penelitian baik itu metode, fungsi, fitur, dan cara kerja. Pada penelitian ini dilakukan proses optimasi terhadap objek penelitian yaitu dasbor sistem pencatatan *log* yang semula hanya menggunakan komponen Elasticsearch, Fluentd, dan Kibana (EFK) stack ditambahkan *add-ons* Wazuh. Selain itu terdapat peningkatan metode dimana dasbor lama yang berfokus hanya pada monitoring server sekarang diteliti pula *log* tersebut dapat muncul dengan metode Investigasi Forensik. Fungsi yang Wazuh berikan juga sangat berguna dalam menampilkan monitoring *log* server secara *realtime* dan kaya akan informasi. Pada sisi fitur dapat dilakukan *tweak* atau konfigurasi rule id sehingga Wazuh dapat men-*generate* log sesuai dengan kriteria yang sudah di set. Cara kerja yang dilakukan juga sudah berbeda dibandingkan pada dasbor sebelumnya, Administrator hanya perlu melakukan penginstalan Wazuh Client pada server tempat proses monitoring dilakukan. Sehingga output yang diharapkan dari penelitian ini yaitu keilmuan baru dari sisi Forensika Digital bagi investigator forensik serta Optimasi dasbor sistem pencatatan *log* berhasil memberikan informasi yang informatif bagi Administrator website.

2.2. Literatur Review

Pada **Tabel 2.1** merupakan penelitian terdahulu terkait pengoptimalan pada server :

Tabel 2. 1 Literatur Review

No	Peneliti	Bagian Pengembangan Penelitian	Metode Penelitian	Area Kontribusi Penelitian	Hasil Penelitian yang Dikembangkan
1	Lintang (2020)	Mengembangkan sebuah *File Integrity Monitoring* menggunakan EFK Stack untuk memonitor aktivitas yang dilakukan oleh server dan user di dalam server tersebut	Perancangan dan pengembangan Aplikasi berdasarkan hasil riset yang dilakukan serta wawancara terhadap *engineer* maupun *sysadmin* yang berkecimpung pada pekerjaan monitoring *system*	*Log Management* pada server	Terbukti EFK stack dapat memonitor user yang mencoba masuk ke dalam sistem serta dapat memonitor aktivitas user di dalam server. Hal ini berdasarkan *alert* yang aplikasi Slack kirim ke *channel* yang dimiliki Administrator. *File Integrity*

Tabel 2. 1 Literatur Review (Lanjutan)

No	Peneliti	Bagian Pengembangan Penelitian	Metode Penelitian	Area Kontribusi Penelitian	Hasil Penelitian yang Dikembangkan
					Monitoring juga berhasil dilakukan menggunakan *tools* auditd
2	Erwinsyah (2019)	Membuat sebuah *Log Management System* dengan menggunakan ELK Stack untuk memonitor server-server yang ada pada suatu Badan Sistem Informasi yang menangani layanan Internet pada suatu kampus Universitas Islam Indonesia	Perancangan dan pengembangan Aplikasi berdasarkan kebutuhan yang ada pada Badan Sistem Informasi di Kampus UII	*Log Management* pada server	Terbukti *Log Management System* yang dibuat dengan menggunakan ELK stack tersebut dapat memberikan informasi yang berguna bagi Administrator di Badan Sistem Informasi UII
3	Walidatush Sholihah, dkk (2020)	Mengembangkan sebuah *Log Event Management* menggunakan ELK Stack untuk memonitor *service* ssh pada server sehingga dapat diketahui berapa persentase keberhasilan dan kegagalan user ketika mencoba	Metode yang digunakan dalam penelitian ini mencakup 5 tahapan yaitu : Analisis, Desain Topologi, Konfigurasi Server, Konfigurasi Klien, dan Pengujian	*Log Management* pada server	Hasil yang didapat menyatakan bahwa semua *log* service ssh pada *client* dapat dikirimkan ke server utama sekalipun *log* pada server tersebut sudah terhapus. Selain mengirimkan *log* pada penelitian ini dibuat juga persentase atas keberhasilan serta kegagalan yang dialami ketika mencoba masuk ke server atau sistem.

Tabel 2. 1 Literatur Review (Lanjutan)

No	Peneliti	Bagian Pengembangan Penelitian	Metode Penelitian	*Area Kontribusi Penelitian*	Hasil Penelitian yang Dikembangkan
		Masuk ke dalam server			Pengujian serangan *brute force* pada
4	Muhammad Nur Arifin, dkk (2018)	Merancang dan Membangun *Event Log Management Server* Menggunakan ELK Stack untuk memonitor *log* ssh pada client server	Metode yang dikembangkan dalam penelitian ini adalah metode pengujian *tools* ELK dengan 3 buah client server serta 1 server sebagai ELK server	*Event Log Management* Pada Server	Hasil yang didapatkan menunjukkan bahwa *log* service SSH yang berada di client dapat 100% dikirimkan secara *real-time* sekalipun file *log* yang ada di server telah terhapus.
5	Chen-Kun Tsung, dkk (2020)	Memvisualisasikan keadaan lalu lintas jalan tol dari ETC (*Electronic Toll Collection*) menggunakan ELK Stack	Metode yang dikembangkan dalam penelitian ini adalah menganalisa jumlah kendaraan yang masuk di dalam tol dengan *tools* ETC untuk kemudian dibuat analisa menggunakan ELK stack.	*Visualization using Log Management* pada server	Hasil menunjukkan bahwa visualisasi yang dibuat berhasil memberikan gambaran bagaimana arus lalu lintas pada jalan tol serta kecepatan pengendara. Hasil lain menunjukkan persentase seberapa ramai jalan tol bagi pengguna kendaraan yang akan masuk lewat tol.
6	Ibrahim Yahya Mohammed Al-Mahbashi, dkk (2017)	Merancang dan membangun *Log Management Server* Menggunakan ELK Stack untuk memonitor aktivitas internal jaringan yang menggunakan *tools safeguard*	Metode yang dikembangkan dalam penelitian ini adalah menganalisis *internal network* dari hasil *log* yang diberikan *safeguard* ke ELK stack server yang sudah dibuat	*Network Security using Log Management* pada server	Hasil menunjukkan bahwa *log* yang diterima ELK dari *safeguard* mengindikasikan sebuah *vulnerability* yang tidak dapat dideteksi oleh *safeguard*, namun dapat terdeteksi oleh ELK stack melalui analisis yang dilakukan.

Berdasarkan literatur review yang telah dibahas pada **Tabel 2.1** menunjukkan penelitian yang dilakukan kebanyakan menggunakan ELK stack, masih menggunakan format *log/*rule default dari ELK stack, serta *log* yang berfokus pada sisi server saja. Adapun penelitian yang dilakukan akan berbeda dengan literatur review yang telah dijabarkan. Perbedaan yang ada ialah penggunaan Elasticsearch dan Kibana saja dalam ELK stack yang ada. Logstash tidak digunakan melainkan digantikan oleh *tools* Wazuh. Rule yang ditampilkan berdasarkan Rule id yang dimiliki Wazuh serta beberapa modifikasi Rule id untuk menampilkan informasi yang lebih akurat. Fokus *log* pada penelitian ini akan lebih ditekankan pada *log web server nginx* untuk menunjukkan indikasi *brute force* pada website yang dikelola oleh Administrator.

2.3. Kajian Log Web Server

2.3.1. Elasticstack

Elasticstack merupakan kumpulan *tools open source* yang didistribusikan oleh perusahaan Elastic. Stack/kumpulan *tools* ini didesain untuk membantu user dalam mendapatkan data *log*, menganalisis data *log*, serta membuat visualisasi terhadap data *log* (TechTarget, 2016). *Tools* tersebut terdiri dari Elasticsearch yaitu mesin pencari*/query* untuk mencari teks data pada *log* yang sudah diambil, Logstash merupakan sebuah *pipeline* untuk mengumpulkan setiap data log yang masuk kemudian disimpan di Elasticsearch. Kibana adalah visualisasi dari data *log* yang telah diambil. Sedangkan Filebeat merupakan *data shipper* yang berada pada setiap *agent* server untuk mengirimkan data *log* ke Logstash. Elasticstack biasanya digunakan untuk membangun Centralized Log Management (CLM) server untuk memonitor server yang dimiliki.

Gambar 2.1 Komponen dari Elasticstack

Namun pada penelitian kali ini *tools* dari Elasticsearch tidak akan digunakan semuanya. *Tools* yang akan difokuskan hanya Elasticsearch, Kibana dan Filebeat. Kenapa demikian ?

Karena sejak Elasticsearch 7.x Filebeat dapat mengirimkan data *log* langsung menuju Elasticsearch tanpa harus melewati Logstash terlebih dahulu. Tidak digunakannya Logstash juga menghemat *resource* pada server dan menjadikan Elasticstack semakin ringan digunakan. Kebutuhan pada Wazuh juga menyatakan tidak perlu digunakannya Logstash, Filebeat sudah cukup membantu pada stack tersebut untuk menjalankan Wazuh *klaster*.

2.3.2. Elasticsearch

Elasticsearch merupakan mesin analitik dan pencarian terdistribusi yang sifatnya gratis dan terbuka untuk semua jenis data, termasuk data tekstual, numerik, geospasial, terstruktur dan tidak terstruktur. Diluncurkan pada tahun 2010 oleh perusahaan Elasticsearch N.V dan sekarang lebih dikenal dengan nama Elastic (What is Elastic, 2022). Pada Elasticstack, Elasticsearch berperan sangat krusial karena merupakan komponen utama dalam stack ini. Hal ini disebabkan Elasticsearch merupakan tempat data *log* disimpan dalam bentuk *instance.* Bentuk *instance* tersebut dapat dikatakan juga sebagai *database*. Sehingga peran Elasticsearch selain sebagai mesin *query* juga sebagai *database* untuk menyimpan data *log* yang dikirimkan oleh Logstash maupun Beats/Filebeat.

Penelitian kali ini akan memfokuskan Elasticsearch sebagai *database* dan *log query*. Dalam Wazuh *klaster* fungsi Elasticsearch adalah sebagai *log storage/database log* berdasarkan *log* yang dikirimkan oleh Filebeat dari Wazuh Master. Bentuk data *log* yang dikirimkan oleh Wazuh Master adalah *raw log* dan *alert log* yang merupakan hasil analisis Wazuh Master. Data *log* yang disimpan oleh Elasticsearch ini berbentuk *instance* dan ketika menggunakan Kibana data *log* tersebut akan di *query*/diambil dan ditampilkan oleh visualisasi Kibana.

2.3.3. Filebeat

Filebeat adalah *tools* yang digunakan untuk mengirim *log* data ke Elasticsearch. Data yang dikirimkan baik dari *security device, cloud, container,* maupun *host server*, Filebeat membantu user dalam memudahkan segala proses karena sifat *log shipper* nya ringan pada server (What is Filebeat, 2022). Pada server biasanya Filebeat diinstall untuk memonitor dan mengecek *log* apa saja yang perlu dikirimkan ke tujuan. Elasticsearch dan Logstash digunakan sebagai tujuan dari *log* yang dikirimkan oleh Filebeat.

Penelitian ini berfokus pada Filebeat sebagai jembatan antara Elasticsearch dan Wazuh Master. Sehingga Filebeat tidak digunakan dan diinstall pada tiap agent server yang ingin di monitor melainkan hanya sebagai jembatan atau *log shipper* antara data *log* yang

sudah dianalisis dan diubah oleh Wazuh Master ke Elasticsearch sebagai tempat penyimpanan data *log* tersebut.

2.3.4. Logstash

Logstash merupakan sebuah *tools* data *pipeline* yang berfungsi sebagai penerima data *log* dari berbagai tujuan/data *source* yang kemudian data tersebut diubah dan dikirimkan ke '*stash*' yang dimiliki (What is Logstash, 2022). Tujuan akhir dari Logstash biasanya adalah Elasticsearch sebagai *database* data terhadap *log* yang telah diubah oleh Logstash. Selain Elasticsearch terdapat tujuan lain sebagai *endpoint* yang dapat dituju oleh Logstash, misalnya adalah aplikasi Slack dan masih banyak aplikasi lainnya yang dapat menjadi tujuan akhir dari Logstash.

Pada penelitian ini Logstash tidak akan digunakan. Fungsi Logstash sudah tergantikan oleh Wazuh Agent dan Wazuh Master sebagai *log collector* dan penerima data *log* pada Wazuh klaster. Filebeat juga berperan sebagai pengganti Logstash dalam hal meneruskan data *log* yang sudah diubah Wazuh Master ke Elasticsearch.

2.3.5. Kibana

Kibana merupakan aplikasi yang berada pada lapisan paling atas di Elasticstack yang berguna untuk visualisasi dari data *log* yang disimpan/di indeks pada Elasticsearch. Sifatnya sama seperti Elasticstack lainnya yaitu *open source* dan Kibana baru muncul pada tahun 2013, tepatnya setelah 3 tahun Elasticsearch dirilis (What is Kibana, 2022). Data yang ditampilkan dari Kibana adalah *raw log* dari Elasticsearch *instance* ataupun data yang sudah dimodifikasi yang ditaruh di *instance* tersebut. Tampilan yang ditawarkan Kibana tidak hanya berupa teks tertulis berdasarkan *log* saja, namun data *log* tersebut dapat disajikan sebagai grafik yang informatif. Grafik tersebut dapat dibuat sesuai dengan keperluan atau bila tidak sempat untuk membuat grafik tersebut terdapat Wazuh sebagai *add-ons* di Kibana untuk mengubah data *log* yang semula tidak beraturan menjadi informasi yang informatif, baik berupa teks maupun grafik.

Pada penelitian ini Kibana akan digunakan sebagai Visualisasi terhadap *log* yang sudah diubah oleh Wazuh Master. Informasi dan Grafik yang dihasilkan murni dibuat oleh Wazuh dan bukan oleh Kibana. Namun user dapat juga menambah beberapa *rule* baru dan juga membuat grafik baru bila dirasa perlu atau ingin mengubah grafik *default* yang dihasilkan oleh Wazuh. Tentunya ketika mengubah grafik *default* disinilah peran Kibana

digunakan. Selain daripada itu peran Kibana hanyalah murni sebagai visualisasi *log* yang telah didapatkan.

2.3.6. Wazuh

Wazuh merupakan sebuah *tools open source* dan dapat digunakan oleh semua orang yang berfungsi sebagai sistem deteksi intrusi yang basisnya adalah server (*endpoint*) (What is Wazuh, 2022). Lebih detailnya lagi Wazuh merupakan sebuah aplikasi monitoring untuk mendeteksi ancaman pada server, memonitor integritas server, hingga melaporkan insiden yang ada pada server. *klaster* Wazuh sendiri tidak dapat berdiri sendiri melainkan harus dibangun di atas Elasticstack karena sifatnya yang merupakan *add ons* dari Kibana. Meskipun memerlukan Elasticstack untuk dapat digunakan fitur yang dimiliki Wazuh tidak kalah oleh Elasticstack. Data yang dihasilkan lebih informatif karena sudah memiliki *built-in* visualisasi *log* sendiri dan user tidak perlu repot-repot membuat visualisasi dari nol. Sifatnya yang *open source* juga menambah nilai tersendiri karena dapat digunakan pada skala perusahaan kecil, menengah hingga besar. Komunitas pada *platform* aplikasi Slack yang dibentuk pun sudah solid dan dapat menanyakan berbagai macam pertanyaan terkait Wazuh didalamnya. Kemudahan penggunaan dibandingkan Elasticstack inilah yang mendorong Wazuh maju dengan sangat pesat.

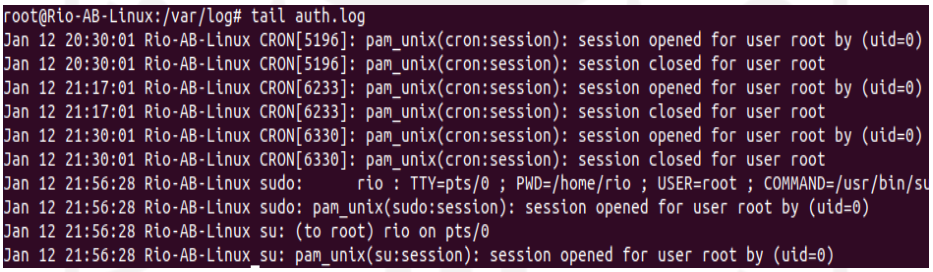
Gambar 2.2 Logo Wazuh

Pada penelitian ini Wazuh merupakan peran paling krusial dari penelitian. Karena tanpa Wazuh maka penelitian ini hanya akan sama dengan penelitian sebelumnya. Fungsi dari Wazuh dalam penelitian ini adalah visualisasi monitor *web server* nginx beserta server website tempat website diletakkan. Adapun hal yang dimonitor adalah usaha *brute force* yang dilakukan oleh *hacker* untuk mendapatkan akses masuk ke website maupun server website. Proses dari monitoring tersebut adalah dengan memantau *log* nginx serta *log* ssh pada server tempat website di *hosting* dengan menggunakan Wazuh agent yang ada di server tersebut. *Log* tersebut kemudian dikirimkan ke Wazuh Master untuk dianalisa apakah termasuk sumber ancaman atau *error* biasa. Kemudian hasil analisis tersebut akan disimpan pada Elasticsearch dan nantinya Administrator akan mengecek hasil visualisasi tersebut dengan bantuan Kibana. Dengan digunakannya Wazuh diharapkan usaha *brute force*

tersebut dapat dideteksi secara dini dan dapat diambil langkah untuk meminimalisir kejadian yang tidak diinginkan. Terakhir diharapkan juga Wazuh dapat membantu seorang investigator dalam menemukan *knowledge* baru sehingga bukti kejahatan pada server dengan lebih cepat karena tidak perlu menganalisis *raw log* secara satu persatu karena *raw log* sudah di-*parse* oleh Wazuh.

2.3.7. Log

Log merupakan sebuah catatan yang dihasilkan pada *event* di *operating system*, aplikasi, maupun pesan yang dihasilkan oleh dua *users* yang berbeda pada aplikasi komunikasi (What is Log, 2022). Sifat *log* sendiri akan dihasilkan atau di-*generate* ketika pada aplikasi maupun sistem operasi melakukan suatu *event* pekerjaan. Misalnya ketika terdapat *error* padawebsite makan otomatis *log* yang menunjukkan *error* akan ter-*record* pada error.log yang dimiliki oleh Nginx. Tentunya *log* tersebut formatnya berbeda beda pada tiap aplikasi maupun sistem informasi.



Gambar 2.3 Contoh Log Pada OS Linux

Pada penelitian kali ini *log* yang akan digunakan adalah error.log dan access.log milik Nginx serta auth.log milik SSH pada server website di-*hosting*. *Log* ini berperan krusial juga karena pada *log* tersebut memberitahukan apa yang terjadi pada website dan server website. Meskipun *log* dapat dibaca tanpa menggunakan Wazuh, namun hal tersebut akan memakan banyak waktu karena harus mengakses server untuk tiap kali ingin mengecek *log* tersebut. Belum lagi banyak *log* yang sifatnya tidak beraturan dan perlu di cermati dengan teliti agar mengetahui makna dari *log* tersebut. Maka dari itu Wazuh sangat membantu dalam menerjemahkan *raw log* menjadi *log* yang dapat mudah dibaca bahkan oleh orang awam sekalipun.

BAB 3
METODOLOGI PENELITIAN

3.1. Langkah Penelitian

Sebelum memulai penelitian terdapat langkah-langkah yang digunakan sebagai acuan dalam menyelesaikan kasus yang diteliti. Adapun penelitian ini terdiri atas beberapa langkah, yaitu:

1. Merumuskan Permasalahan Penelitian/Identifikasi Masalah Penelitian
2. Merumuskan Perbatasan Masalah Penelitian
3. Mengumpulkan Data Penelitian
4. Melakukan Analisa Data Penelitian
5. Melaporkan Hasil Analisa Data Penelitian

Metodologi penelitian yang digunakan adalah Metode Investigasi Forensik. 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 yangme-*hosting* website dengan melihat metadata *log* informasi yang dihasilkan oleh Wazuh. Data *log* tersebut didapatkan melalui server website pada Perguruan Tinggi Universitas Islam Indonesia yaitu Badan Sistem Informasi. 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 3.1 Alur Metode Penelitian

Pada **Gambar 3.1** 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. 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. Adapun proses investigasi forensik mengambil 3 langkah terakhir yaitu langkah 3-5 dari metode penelitian pada **Gambar 3.1** yang menjadi **Gambar 3.2** untuk keperluan proses investigasi forensik.

.

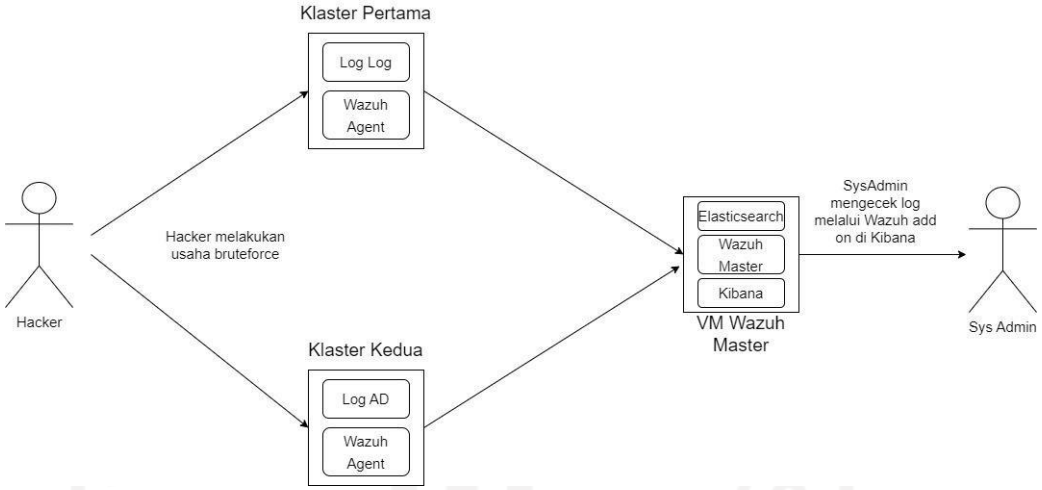
Gambar 3. 2 Alur Proses Investigasi

Pada **Gambar 3.2** 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.

Penelitian ini dilakukan pada kedua klaster yang berbeda. Klaster pertama merupakan klaster baru dan memiliki 5 website baru pula. Klaster kedua merupakan klaster lama yang dimiliki oleh Badan Sistem Informasi Universitas Islam Indonesia yang memiliki puluhan website di dalamnya. Alasan kenapa dipilihnya 2 klaster ini dikarenakan usia kedua klaster tersebut berbeda dan bagaimana *behavior* yang ada ketika terjadi serangan *bruteforce* sehingga didapatkan pengetahuan baru dari kedua klaster tersebut. Adapun website yang digunakan pada klaster pertama merupakan 5 website baru yang dibuat sedangkan klaster kedua merupakan 5 website teratas yang mengalami serangan *bruteforce*. Hal ini dikarenakan klaster pertama baru berjalan terhitung dari akhir bulan Maret 2022. Dalam proses pengambilan *log* dibutuhkan 1 bulan sehingga 5 website baru tersebut didiamkan hingga akhir April 2022 untuk kemudian *log* yang didapatkan dapat diteliti. Pada klaster kedua *log* diambil pada bulan Januari 2022.

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.



Gambar 3.3 Skenario Penelitian

Terakhir yaitu rancangan tabel perbandingan hasil analisis yang dilakukan pada kedua klaster. Tabel perbandingan ini dibuat berdasarkan informasi yang didapatkan melalui *literatur review* / *knowledge base* yang dijelaskan pada sub bab 2.2 diatas. Berdasarkan penjelasan itulah didapatkan rancangan tabel sebagai berikut :

Tabel 3.1 Rancangan Tabel Perbandingan Hasil Analisis

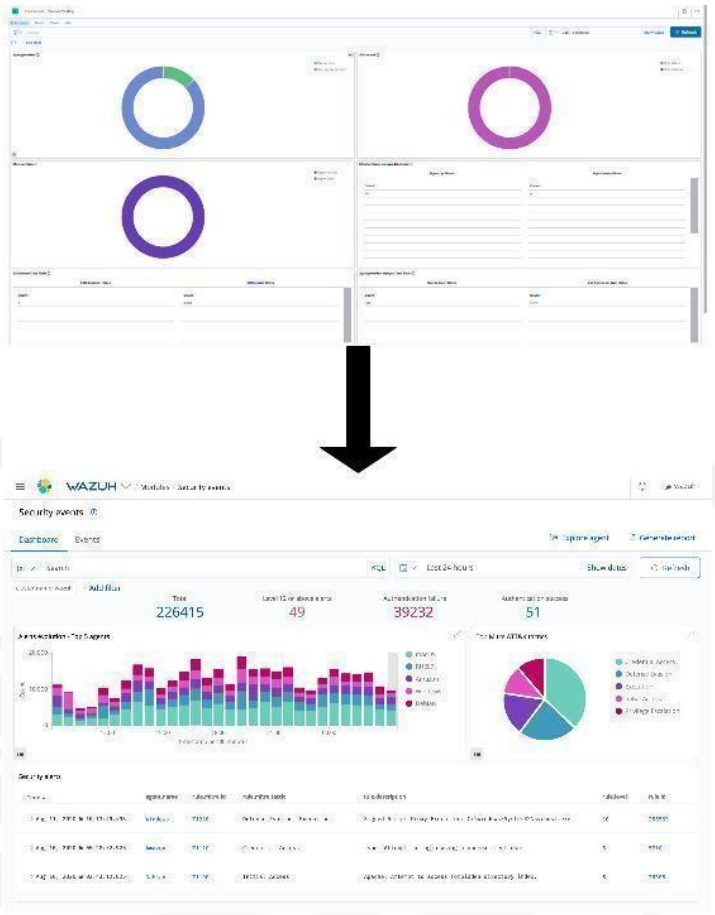
Parameter Perbandingan	Klaster Pertama	Klaster Kedua
Informasi Serangan *Bruteforce*		
Tujuan Serangan *Bruteforce*		
Intensitas Serangan		
Analisis Metadata *Log*		
Rule Id		
Anomali Serangan		
Usia Website		

3.2. Optimasi Dasbor

Langkah-langkah dalam mengoptimasi dasbor sistem pencatatan *log* terbaru tidak akan ditampilkan pada penelitian kali ini. Adapun hal yang akan disampaikan merupakan penjelasan tentang perubahan yang terjadi pada dasbor sistem pencatatan log baru. Dasbor sistem pencatatan *log* pada penelitian sebelumnya murni hanya menggunakan EFK Stack tanpa tambahan *add ons* Wazuh. Sehingga mulai dari proses pengambilan *log* hingga *log* ditampilkan semuanya dikerjakan secara manual. Proses yang paling sulit dalam penelitian sebelumnya adalah membuat visualisasi berdasarkan *log* yang diambil. Cara pembuatan visualisasi tersebut masih murni dengan melakukan *filter* kata yang terdapat pada *log* kemudian dijadikan visualisasi berdasarkan hasil *filter* tersebut.

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* yang terdapat pada Kibana tersebut. 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.

Adapun rincian dari proses optimasi dasbor sistem pencatatan log tersebut adalah sebagai berikut. Pertama 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). Kedua Wazuh-Agent mengirimkan *log* yang sesuai pada file konfigurasi ke Wazuh Master. KetigaWazuh master menerima *raw log* kemudian mengubah *raw log* tersebut berdasarkan *built- in* rule yang dimiliki dan menghasilkan metadata *log* untuk ditampilkan. Terakhir diharapkanhasil dasbor baru dapat menampilkan informasi yang informatif dan memberikan *knowledge* mengenai keadaan server berdasarkan metadata *log* yang dihasilkan Wazuh.



Gambar 3.4 Optimasi Dasbor

Pada **Gambar 3.4** diatas menunjukkan perubahan signifikan terhadap dasbor sistem pencatatan *log* yang telah dikembangkan dan yang akan dilakukan penelitian selanjutnya. Perubahan signifikan tersebut tidak dapat dilakukan tanpa bantuan Wazuh yang sudah memiliki *built-in* Visualisasi dasbor sistem pencatatan *log* dan keterangan *log.* Informasi yang diberikan baik visual maupun tulisan tersebut sangat informatif daripada informasi pada dasbor sistem pencatatan *log* penelitian sebelumnya dan tidak hanya asal dibuat saja.

3.3. Analisis Log

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 *brute force* 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**.

Berdasarkan pemaparan *log* mana saja yang akan diteliti pada penjelasan di atas maka *log* selain fokus di atas dapat diabaikan saja.

3.4. Metode Investigasi Forensik

Pada bagian ini selain dijelaskan bagaimana proses penelitian yang dilakukan berdasarkan Metode Investigasi Forensik serta cara kerja Wazuh akan dijelaskan pula. Acuan penjelasan dan metode agar lebih mudah dipahami dan tidak terpecah pecah maka dibagi menjadi 5 bagian penjelasan seperti **Tabel 3.1** dibawah.

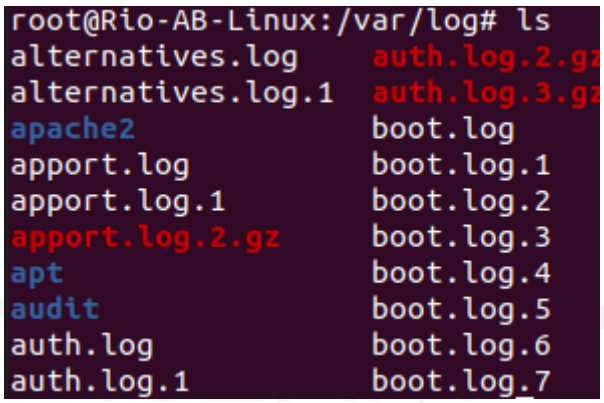
Tabel 3.2 Tahapan Investigasi Forensik

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

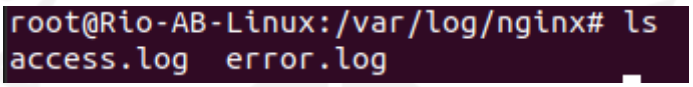
Berdasarkan **Tabel 3.2** diatas metode investigasi forensik akan ditekankan dan berfokus pada investigasi metadata *log* yang dihasilkan oleh Wazuh. Selain itu juga akan dilakukan rekonstruksi metadata *log* untuk memberikan informasi mengenai karakteristik serangan yang dilakukan oleh Hacker. Penjabaran 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* error 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

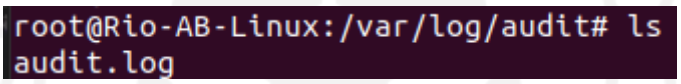
ke arah Wazuh Master/Wazuh klaster. Sebagai gambaran, pada server letak dari ke 3 *log* ssh, nginx dan auditd ada pada **Gambar 3.5** , **Gambar 3.6** , **Gambar 3.7**.



Gambar 3.5 *Log* SSH

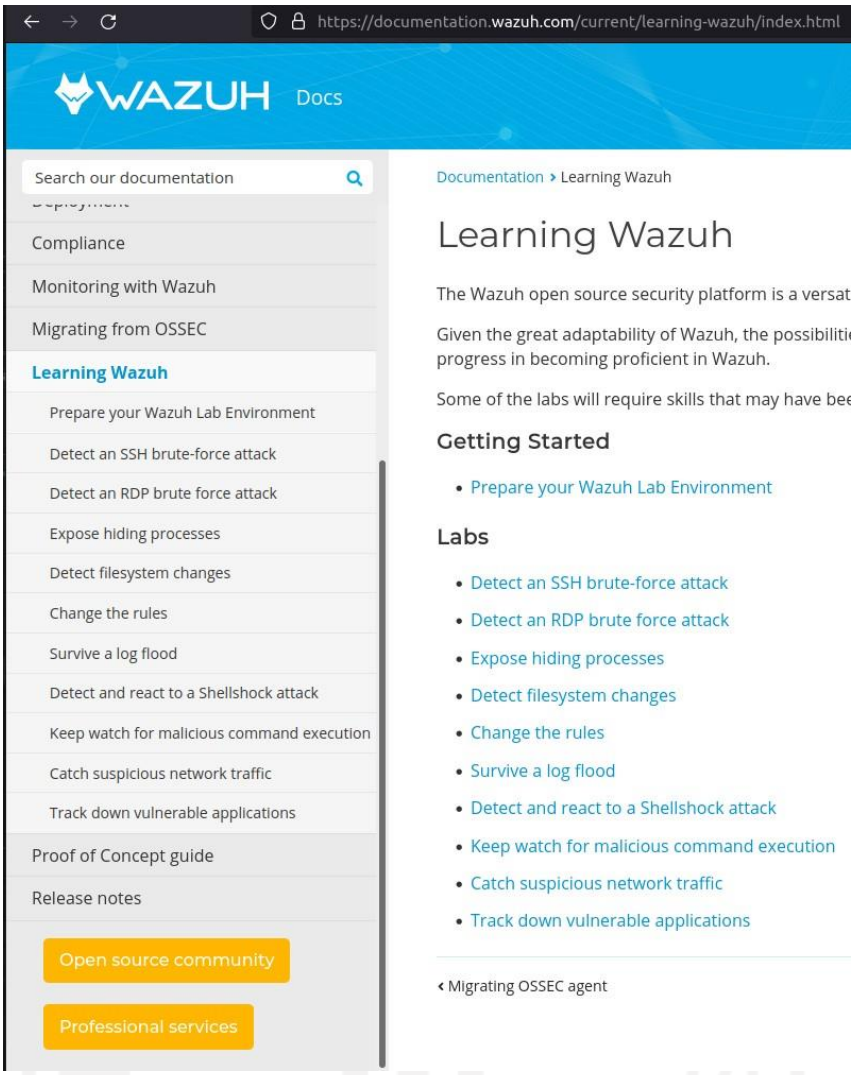


Gambar 3.6 *Log* Nginx



Gambar 3.7 *Log* Auditd

Informasi selanjutnya yaitu Pengumpulan *log* adalah hal yang akan dilakukan oleh Wazuh Agent dan Wazuh klaster. Setelah *log* diidentifikasi dan sudah jelas *log* mana saja yang perlu diambil maka langkah selanjutnya adalah mengumpulkan *log*. Proses pengumpulan *log* ini tidak lepas dari peran Wazuh dalam membantu user untuk menggunakan Wazuh. Langkah-langkah dalam mengambil *log* serta caranya terdapat pada website resmi Wazuh dan pilih ke tab Learning Wazuh yang ada dibagian sebelah kiri Website seperti pada **Gambar 3.8.**



Gambar 3.8 Tutorial Wazuh

Karena sudah menentukan *log* mana saja yang perlu diambil maka dari tutorial tersebut yang perlu diambil hanya "**Detect an SSH brute force attack**" untuk *log* ssh, "**Detect and react to a Shellshock attack**" untuk *log* nginx, dan terakhir "**Keep watch for malicious command execution**" untuk *log* auditd.

Pada Wazuh Agent sendiri letak dari 3 konfigurasi diatas terdapat pada file yang bernama **ossec.conf**. Letak dari **ossec.conf** ini akan muncul setelah menginstall Wazuh Agent pada direktori **/var/ossec/etc/** seperti **Gambar 3.9.**

```
root@Rio-AB-Linux:/var/ossec/etc# ls
client.keys  internal_options.conf  local_internal_options.conf  localtime  ossec.conf
root@Rio-AB-Linux:/var/ossec/etc#
```

Gambar 3.9 Letak ossec.conf

Adapun isi dari **ossec.conf** yang mewakili 3 konfigurasi dari *log* tersebut merujuk pada **Gambar 3.10, Gambar 3.11, dan Gambar 3.12** berikut.

```
<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/auth.log</location>
</localfile>
```

Gambar 3.10 Path pengambilan Log SSH

```
<ossec_config>
  <localfile>
    <log_format>apache</log_format>
    <location>/var/log/nginx/access.log</location>
  </localfile>

  <localfile>
    <log_format>apache</log_format>
    <location>/var/log/nginx/error.log</location>
  </localfile>
```

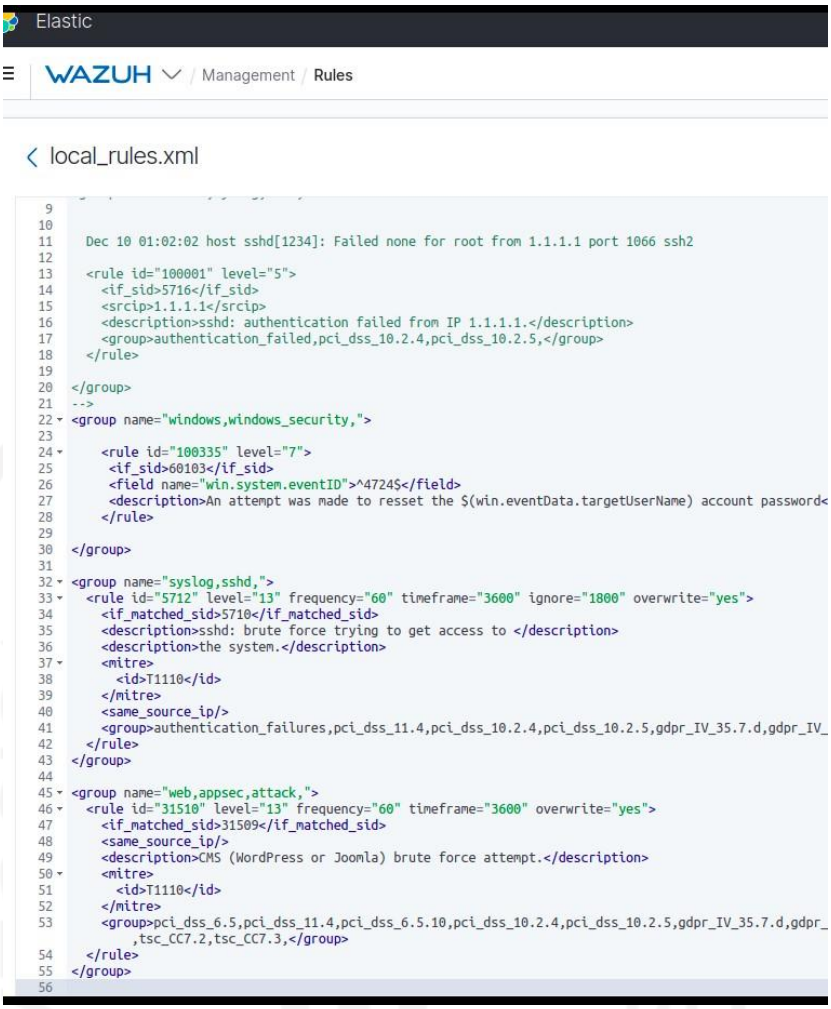
Gambar 3.11 Path pengambilan Log SSH

```
<localfile>
  <location>/var/log/audit/audit.log</location>
  <log_format>audit</log_format>
</localfile>
```

Gambar 3.12 Path pengambilan Log Auditd

Namun dalam *log* Auditd dalam menentukan *suspicious command* hanya dapat dikonfigurasi di Wazuh Master saja. Pada Wazuh Agent hanya meregistrasi user apa saja yang masuk dalam pengawasan.

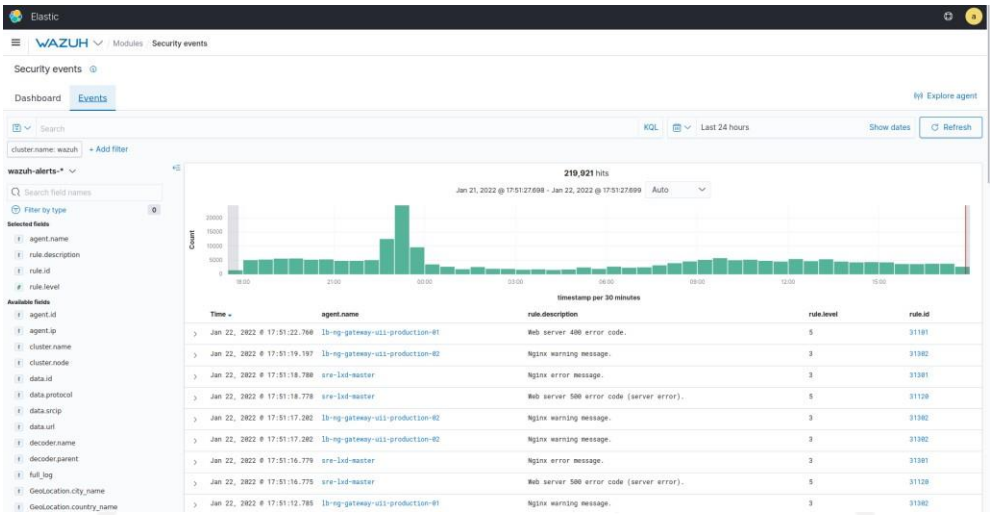
Pada Wazuh Master yang ada di Kibana dilakukan konfigurasi tambahan yaitu menambahkan *rules* baru. Tujuan dari ditambahnya *rules* baru ini untuk memantau tingkat *brute force* yang tinggi sehingga tidak terjadi *flooding log* pada Kibana. Karena pada dasarnya Wazuh sudah memiliki *rules* untuk memberitahukan *brute force* namun frekuensinya yang kecil membuat terjadinya *log flooding* pada Kibana. Maka dari itu dibuatnya *rules* baru ini untuk mencegah terjadinya hal tersebut dengan menimpa *rules* lama tersebut dan membuatnya menjadi *rules* baru yang frekuensinya cukup tinggi sehingga tidak menimbulkan *log flooding* pada Kibana.



Gambar 3.13 Rules baru pada local_rules

Rules baru tersebut dapat dilihat pada **Gambar 3.13** diatas. Selanjutnya tinggal menunggu hasil *log* yang akan dikumpulkan dan di-*generate* oleh Wazuh berdasarkan tindakan *brute force* yang dilakukan oleh Hacker.

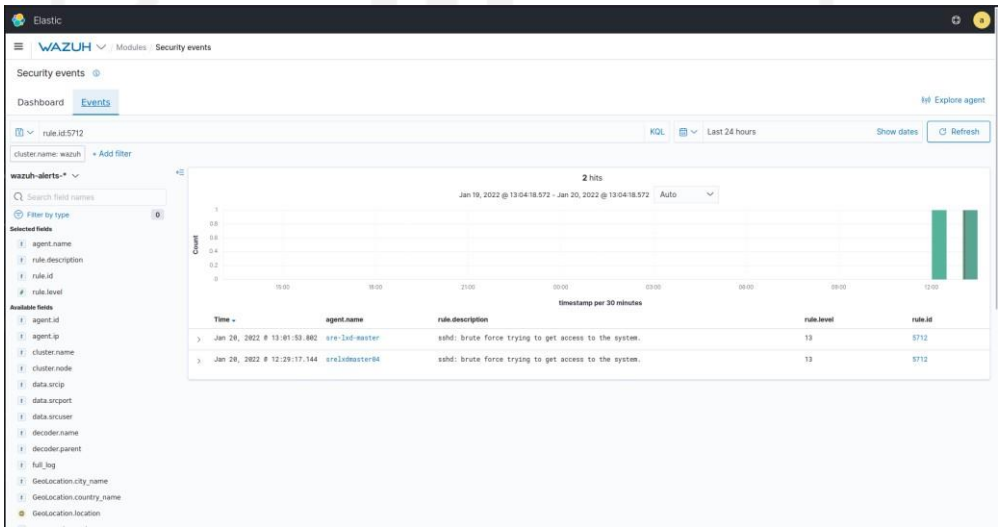
Eksaminasi *Log* adalah menganalisa metadata *log* yang dihasilkan oleh Wazuh. Pada bagian ini akan dilakukan analisa berdasarkan *log* yang berhasil di *generate* oleh Wazuh. Karena pada dasarnya *rules* pada Wazuh ada banyak sekali dan terkadang terdapat *log* yang tidak relevan dengan tujuan awal identifikasi maka bagian ini akan langsung membahas *log* yang relevan. Pada **Gambar 3.14** dibawah merupakan hasil *log* yang di *generate* oleh Wazuh bagian Security Event dan *log* yang berbentuk kalimat.



Gambar 3.14 Hasil *Log* yang di-*generate* Wazuh

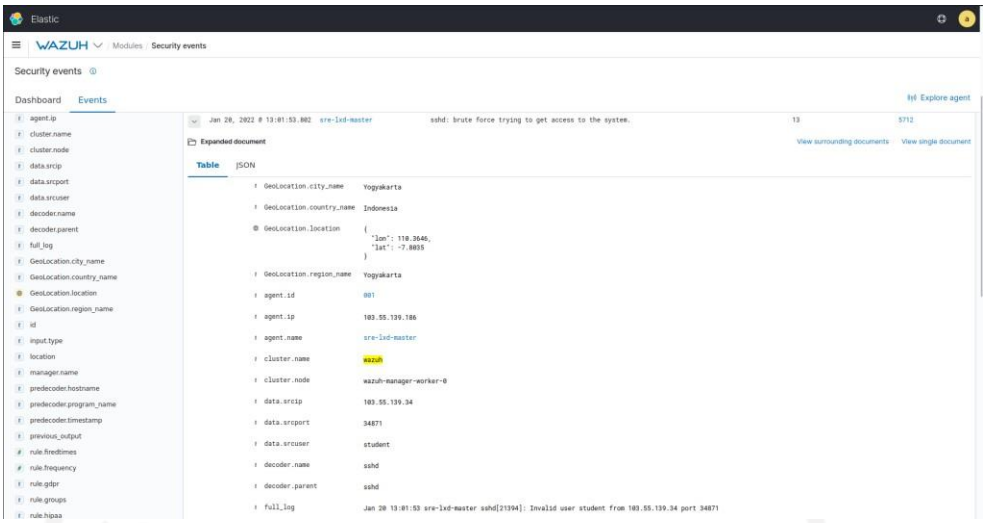
Penelitian ini akan berfokus pada bagan Security Event yang ada pada Wazuh. Selain Security Event terdapat bagan lain yang ada pada Wazuh, namun karena kebanyakan hal keamanan (Security) terdapat pada bagan tersebut maka bagan tersebutlah yang menjadi fokus. Adapun untuk memudahkan tindak analisa maka *log* yang akan dianalisa adalah *log* yang berbentuk kalimat seperti pada **Gambar 3.14.**

Hal yang pertama akan dianalisa adalah bagian *log* ssh. Pada **Gambar 3.15** menunjukkan hasil *brute force* yang dilakukan oleh hacker dalam menyerang server tempat website di-*hosting.*



Gambar 3.15 *Log brute force* yang di-*generate* Wazuh

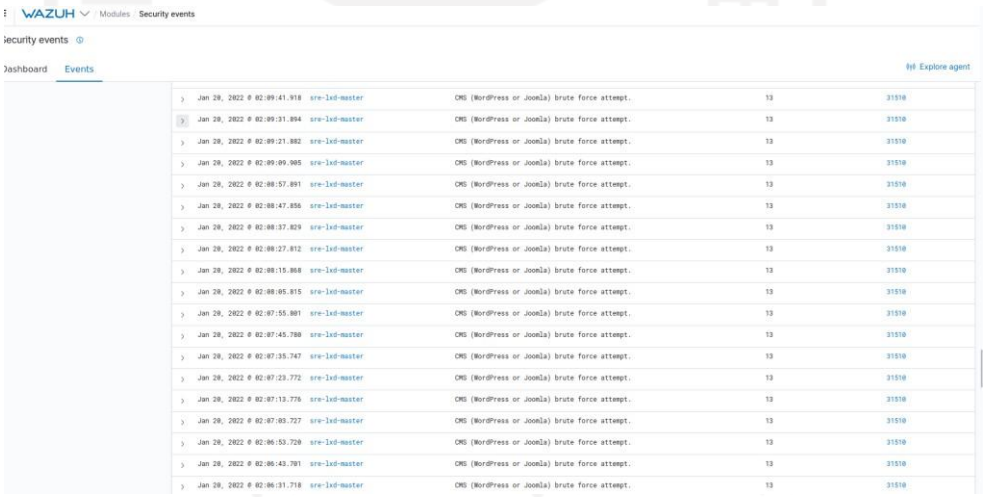
Serangan yang dilakukan oleh *hacker* tersebut pada *log* yang diberikan oleh Wazuh dapat diteliti lebih lanjut dengan memperhatikan **Gambar 3.16** berikut.



Gambar 3.16 Isi dari keterangan *log brute force*

Keterangan mengenai dimana lokasi *hacker* melakukan, ip yang digunakan oleh hacker, user dan port yang digunakan oleh hacker dalam melakukan *brute force* akan tampak terlihat pada bagian ini.

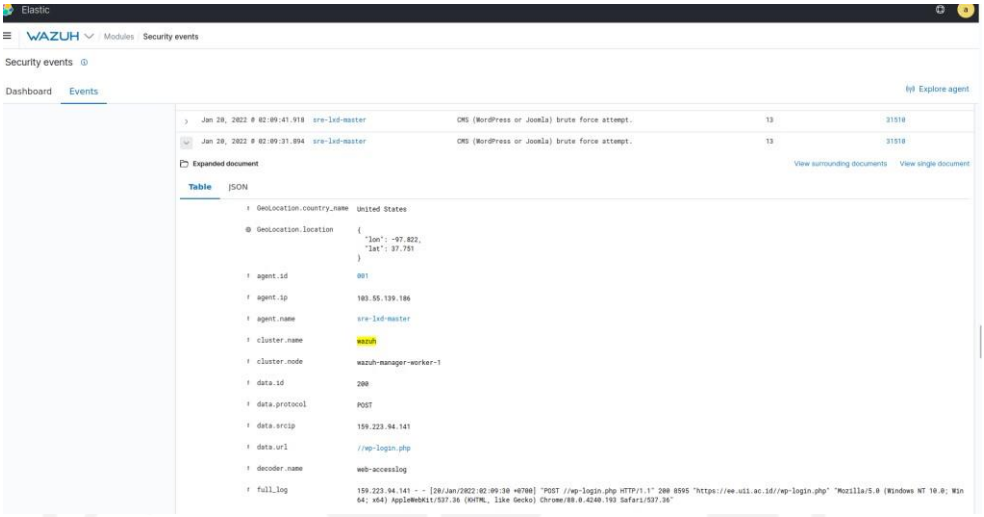
Analisa selanjutnya merujuk pada serangan *brute force* yang ditujukan pada website yang dimiliki. Pada **Gambar 3.17** menunjukkan banyaknya serangan *brute force* yang dilakukan oleh *hacker* meskipun *rules* baru sudah diterapkan.



Gambar 3.17 Menunjukkan Serangan *brute force ke Website*

Walaupun keterangan pada **Gambar 3.17** menunjukkan nama server (hal tersebut merujuk pada nama Agen yang diinstal Wazuh Agent)Ini menunjukkan banyaknya serangan yang ditujukan pada Website. Keterangan tersebut menunjukkan serangan ditujukan pada Wordpress dan bukan ke Server tempat Website di *hosting.* Serangan tersebut merujuk pada dilakukannya *brute force* pada halaman login Admin Website pada https://namawebsite.namadomain/wp-login. Website yang memiliki reputasi

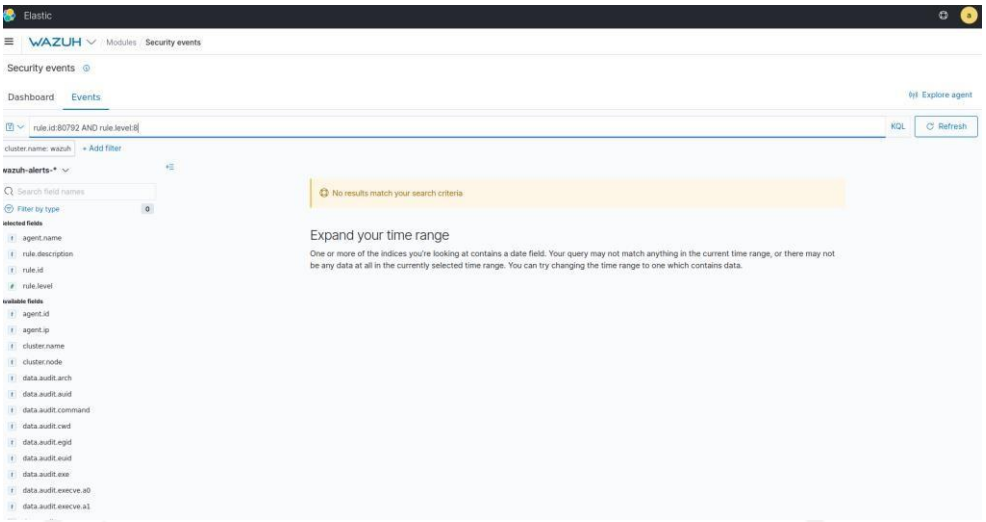
akan mendapatkan serangan yang banyak, contoh pada penelitian ini adalah Website salah satu kampus besar yang ada di Jogja yaitu Universitas Islam Indonesia pada Badan Sistem Informasi.



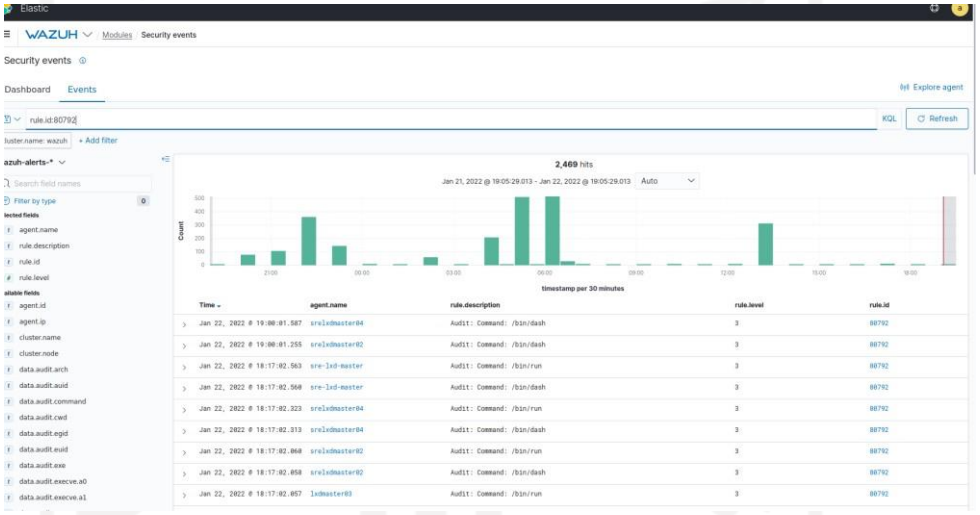
Gambar 3.18 Isi dari keterangan *brute force* website

Pada **Gambar 3.18** diatas merupakan hasil dari keterangan lanjutan terhadap *log* pada **Gambar 3.17**. Disini dapat dilakukan analisis dengan merujuk pada lokasi website apa yang diserang (kondisi bila server hosting memiliki banyak website yang di hosting) *hacker*, ip address yang digunakan *hacker*, serta link tujuan *hacker* melakukan *brute force.*

Analisa terakhir pada tahap ini adalah analisis yang dilakukan ketika keadaan website diragukan/*compromise* dikarenakan terdapat perubahan di dalam server tanpa diketahui. Hal ini dikarenakan bahwa terdapat indikasi bahwa *hacker* telah berhasil masuk ke dalam server dan melakukan perubahan pada server. Maka dari itu *log* auditd sangat berguna karena merekam *command* apa saja yang telah dijalankan oleh user di dalam server. Sehingga ketika pada Wazuh dilihat ada *log* dengan level diatas 8 dan merasa tidak menjalankan perintah tersebut maka dapat dipastikan itu olah *hacker*, namun bisa jadi dilakukan oleh sistem sendiri. Perlu dilakukan investigasi lebih lanjut pada bagian pada *log* tersebut.



Gambar 3.19 *Log* Auditd tidak ter-*compromise*



Gambar 3.20 *Log* Auditd dalam keadaan Normal

Gambar 3.19 Menunjukkan bahwa saat ini Website masih aman dan tidak ada indikasi ter-*compromise* oleh *hacker*. Sedangkan pada **Gambar 3.20** merupakan *log* level 3 merupakan perintah yang dijalankan oleh sistem itu sendiri sehingga hanya merupakan informasi saja bagi SysAdmin.

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 maupun organisasi yang diikuti.

BAB 4
HASIL DAN PEMBAHASAN

4.1. Hasil Implementasi Sistem Dasbor Teroptimasi

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

List Website yang akan dilakukan penelitian :

a. Klaster Pertama
   - canyoubruteforceme.my.id
   - datapenelitiantesis.my.id
   - websitepenelitiantesis.my.id
   - bruteforcethiswebsite.my.id
   - penelitiantesis.my.id

b. Klaster Kedua

   Pada klaster 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 klaster pertama.

Latar belakang mengapa klaster Pertama dan klaster Kedua berbeda adalah: klaster Pertama telah ditentukan nama websitenya sedangkan pada klaster Kedua mengambil secara acak. Hal ini dikarenakan pada klaster Pertama diuji seberapa banyak terkena serangan *brute force* pada website yang tidak/belum terkenal. Sedangkan pada klaster Kedua menguji seberapa banyak terkena serangan *brute force* pada website yang sudah lama/terkenal. Diharapkan dari dua klaster yang berbeda ini menghasilkan pengetahuan baru yang dapat dijadikan preferensi dalam mengembangkan website di masa depan. Penelitian ini berusaha dilakukan agar sejalan dengan penelitian sebelumnya dengan cara dilakukannya optimasi dasbor sistem pencatatan log.

Hasil dari implementasi diharapkan dapat memberikan pengetahuan baru mengenai *brute force* yang dilakukan oleh *Hacker.* Adapun *log brute force* 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.

Alasan dipilihnya 4 **rule id** ialah karena **rule id** tersebut berhubungan dengan *bruteforce* pada sisi server (ssh) dan website (web server) sesuai dengan standarisasi *log bruteforce* dari *tools* Wazuh (Castro, 2020). **Rule id 5710** dan **rule id 5712** mewakili/menghasilkan *log* serangan *bruteforce* pada server tempat website di-*hosting*. Sedangkan kenapa **rule id 5710** melompat ke **5712** dan tidak menggunakan **rule id 5711** ialah karena **rule id 5711** sudah dipakai untuk keterangan *log* salah memasukkan username di server dengan kondisi password sudah benar. Kemudian **rule id 31509** dan **rule id 31510** menghasilkan/mewakili *log* serangan *bruteforce* pada website(web server) yang dikelola dan masuk dalam monitoring Wazuh.

Perincian dari keempat *log* tersebut adalah sebagai berikut :

- **rule id 5710** merupakan identifikasi bahwa telah terjadi usaha untuk login ke dalam server hosting sebanyak 1 kali.
- **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**.
- **rule id 31509** merupakan identifikasi bahwa telah terjadi usaha untuk login ke dalam website sebanyak 1 kali.
- **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 *brute force.*

4.2. Pembahasan Proses Investigasi Forensik

Adapun pembahasan yang dilakukan ialah menginvestigasi/meneliti struktur metadata *log* yang dihasilkan oleh Wazuh pada Dasbor Sistem Pencatatan Log Teroptimasi. Hal ini berdasarkan minimnya pengetahuan terkait proses investigasi forensik pada halaman website yang terkena serangan *brute force*. Penelitian ini juga nantinya diharapkan akan memberikan informasi kepada para pengelola website/Administrator mengenai *behavior* serangan *brute force.* Hal yang akan diteliti merupakan *log* serangan *brute force* yang di-*generate* oleh Wazuh tersebut. Adapun *log* tersebut merupakan *log* ssh dan *log* nginx. Selain itu karakteristik dari masing-masing *log* tersebut juga akan diteliti guna mendapatkanpola serangan yang dilakukan oleh *Hacker* sehingga dapat dilakukan pelacakan kembali sumber serangan *brute force.* Proses Investigasi ini dilakukan melalui 3 tahap, sama seperti**Tabel 3.1**.

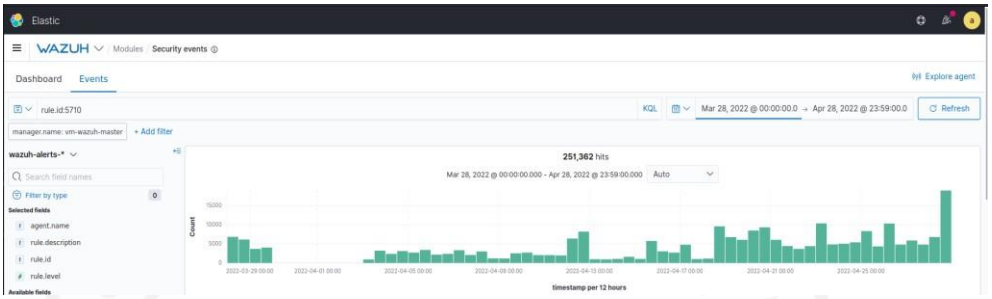
Tahapan dalam proses investigasi ini mengambil ilmu disiplin / framework dari keilmuan investigasi forensik yang meliputi : *Identification, Preservation, Collection, Examination, Analysis, and Presentation*. Proses investigasi forensik yang dilakukan diharapkan nantinya dapat menghasilkan pengetahuan/keilmuan baru bagi Investigator Forensik. Adapun keilmuan baru yang diharapkan diperoleh yaitu kemudahan dalam menganalisis kasus yang melibatkan pembobolan web. Mulai dari identifikasi penyerang/*hacker*, frekuensi serangan yang dilakukan oleh *hacker*, lokasi penyerang/*hacker*, hingga proses mitigasi yang seharusnya dilakukan oleh Administrator/pengelola website untuk mengamankan website mereka dari potensi serangan *brute force* yang dilancarkan oleh *hacker*.

4.2.1 Pengumpulan Data Klaster Pertama

Pada hasil analisis yang dilakukan di klaster kedua selama 1 Bulan (terhitung dari tanggal 28 Maret 2022 hingga 28 April 2022) menunjukkan hasil *brute force* yang dilakukan oleh hacker berjumlah :

a. **Rule id 5710** mendapatkan serangan sebanyak **251362 hits** seperti pada **Gambar 4.1.** Hasil serangan ini ditujukan pada server tempat website di-hosting oleh

Administrator. Sesuai dengan **rule id** yang diberikan bahwa serangan ini menyerang dengan teknik *brute force* lewat jalur login ssh kredensial. Pada **Gambar 4.1** 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.



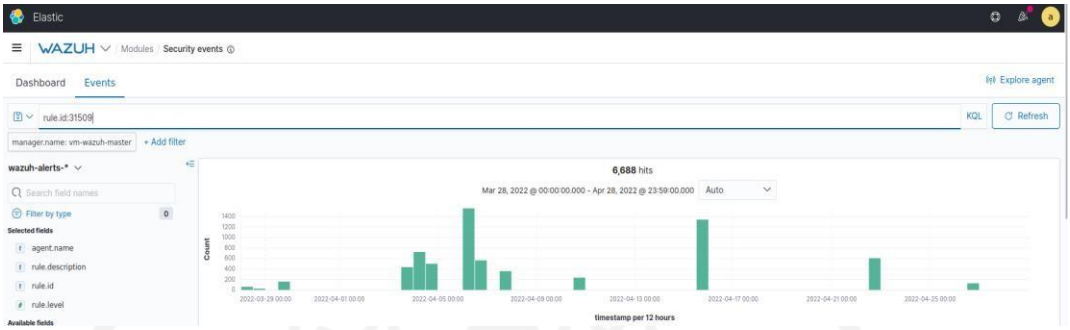
Gambar 4. 1 Rule id 5710 klaster pertama

b. **Rule id 5712** mendapatkan serangan sebanyak **1245 hits** seperti pada **Gambar 4.2.** Hasil serangan ini ditujukan pada server tempat website di-hosting oleh Administrator 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 4.1** dan **Gambar 4.2** 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 4.2 Rule id 5712 klaster pertama

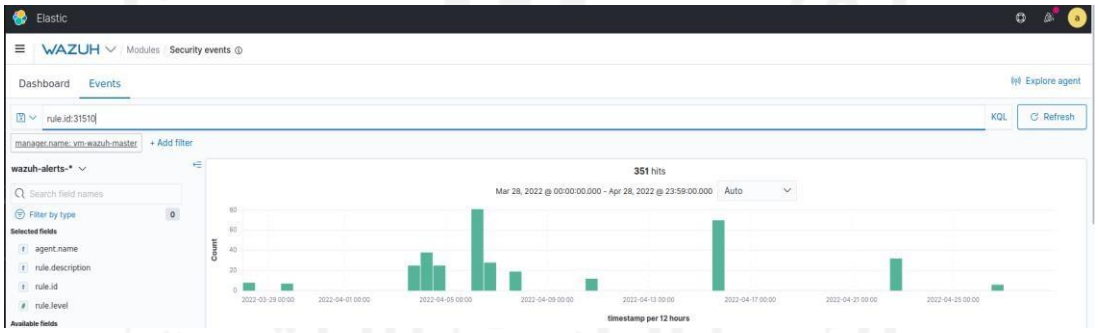
c. **Rule id 31509** mendapatkan serangan sebanyak **6688 hits** seperti pada **Gambar 4.3.** Hasil serangan ini ditujukan pada halaman administrator website yang dikelola oleh Administrator website. Sesuai dengan rule id yang diberikan bahwa serangan ini menyerang dengan teknik *brute force* lewat jalur login admin di halaman Administrator website. Pada **Gambar 4.3** 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 4.3 Rule id 31509 klaster pertama

d. **Rule id 31510** mendapatkan serangan sebanyak **351 hits** seperti pada **Gambar 4.4.** 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 4.3** dan **Gambar 4.4** menunjukkan aktivitas yang dilakukan oleh *Hacker* konsisten dalam usahanya 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.



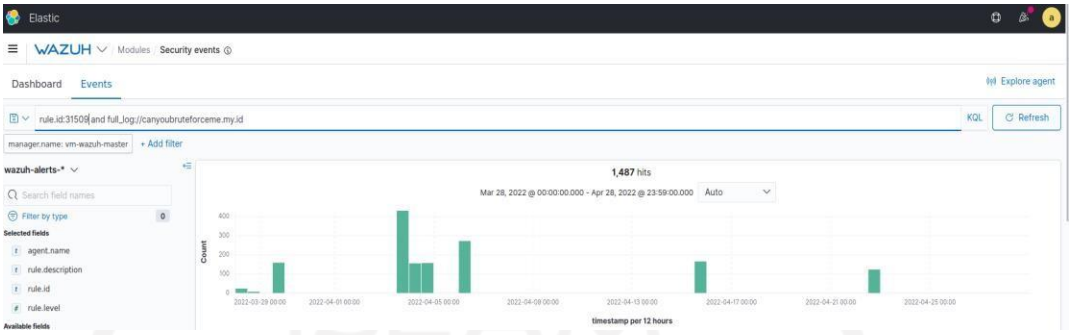
Gambar 4.4 Rule id 31510 klaster pertama

Perincian terhadap serangan yang mengarah pada 5 website teratas tersebut adalah sebagai berikut :

a. Perincian terhadap serangan ke website **canyoubruteforceme.my.id** berdasarkan rule id *brute force web server* adalah sebagai berikut :

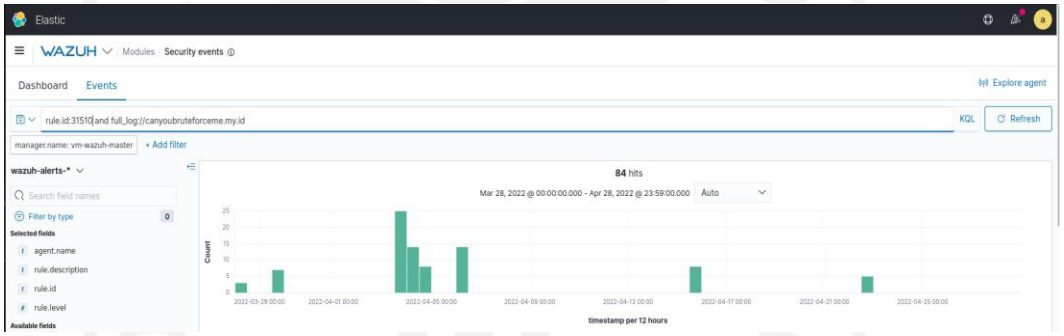
   Hasil data yang didapatkan berdasarkan filtering **rule id 31509** dan nama website menunjukkan bahwa website **canyoubruteforceme.my.id** mendapatkan **1487** serangan sesuai **Gambar 4.5.** Serangan yang dilakukan terlihat tidak setiap hari

dilakukan, dan hanya terlihat dilakukan beberapa kali saja dalam kurun waktu 1 bulan. Namun tingkat intensitas serangan yang dilakukan paling tinggi dibanding 4 website lainnya.



Gambar 4.5 Hasil Rule id 31509 ke website canyoubruteforceme.my.id

Sedangkan hasil data yang didapatkan berdasarkan filtering **rule id 31510** pada **Gambar 4.6** menunjukkan bahwa website **canyoubruteforceme.my.id** mendapatkan serangan beruntun/konsisten sebanyak **84** pada beberapa IP Address tertentu. Jumlah penyerang konsisten tersebut diklasifikasikan berdasarkan Negara penyerang sesuai dengan **Tabel 4.1** dibawah.



Gambar 4. 6 Hasil Rule id 31510 ke website canyoubruteforceme.my.id

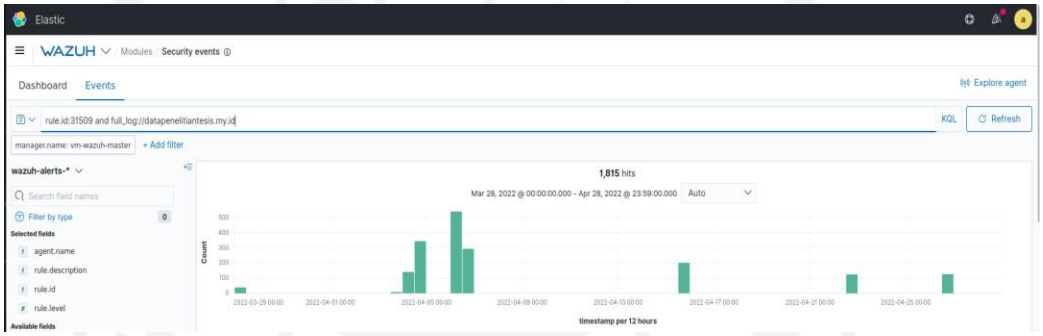
Adapun negara penyerang menurut jumlah serangan pada **rule id 31510** adalah sebagai berikut :

Tabel 4.1 5 Negara terbesar penyerang website canyoubruteforceme.my.id

No	Negara	Jumlah Serangan
1	Indonesia	42
2	Singapore	14
3	Turkey	13
4	Romania	8
5	United States	7

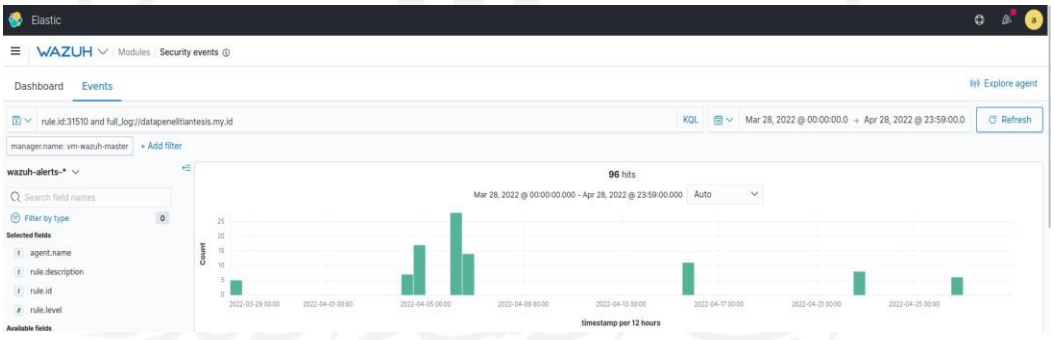
Perincian terhadap serangan ke website **datapenelitiantesis.my.id** berdasarkan rule id *brute force web server* adalah sebagai berikut :

Hasil data yang didapatkan berdasarkan filtering **rule id 31509** dan nama website menunjukkan bahwa website **datapenelitiantesis.my.id** mendapatkan **1815** serangan sesuai **Gambar 4.7.** Serangan yang dilakukan terlihat tidak setiap hari dilakukan, dan hanya terlihat dilakukan beberapa kali saja dalam kurun waktu 1 bulan yaitu pada sepertiga bulan awal dan menjelang akhir bulan.



Gambar 4.7 Hasil Rule id 31509 ke website datapenelitiantesis.my.id

Sedangkan hasil data yang didapatkan berdasarkan filtering **rule id 31510** pada **Gambar 4.8** menunjukkan bahwa website **datapenelitiantesis.my.id** mendapatkan serangan beruntun/konsisten sebanyak **96** pada beberapa IP Address tertentu. Jumlah penyerang konsisten tersebut diklasifikasikan berdasarkan Negara penyerang sesuai dengan **Tabel 4.2** dibawah.



Gambar 4.8 Hasil Rule id 31510 ke website datapenelitiantesis.my.id

Adapun negara penyerang menurut jumlah serangan pada rule id **31510** adalah sebagai berikut :

Tabel 4.2 5 Negara terbesar penyerang website datapenelitiantesis.my.id

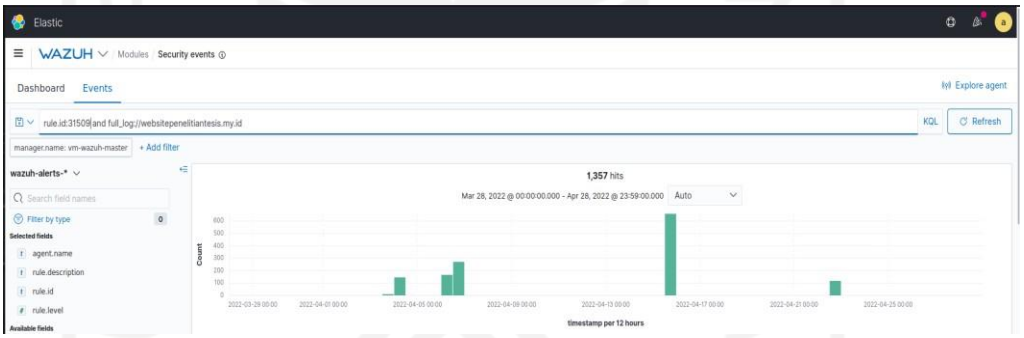
No	Negara	Jumlah Serangan
1	Singapore	28

Tabel 4.3 5 Negara terbesar penyerang website datapenelitiantesis.my.id (Lanjutan)

No	Negara	Jumlah Serangan
2	United Kingdom	23
3	United States	22
4	Indonesia	16
5	Turkey	7

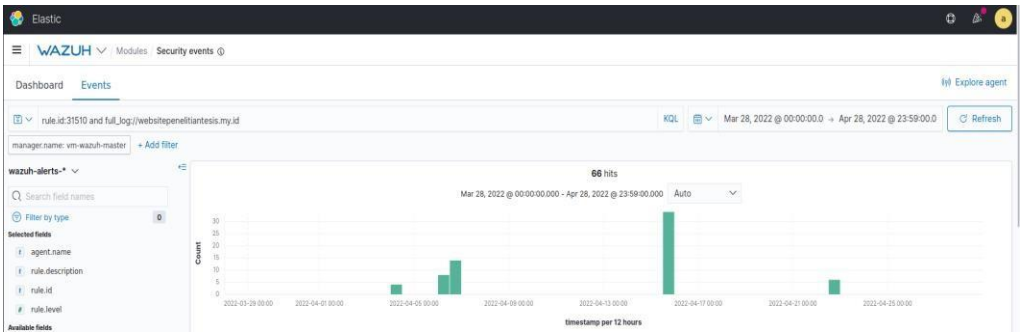
b. Perincian terhadap serangan ke website **websitepenelitiantesis.my.id** berdasarkan rule id *brute force web server* adalah sebagai berikut :

Hasil data yang didapatkan berdasarkan filtering **rule id 31509** dan nama website menunjukkan bahwa website **websitepenelitiantesis.my.id** mendapatkan **1357** serangan sesuai **Gambar 4.9.** Serangan yang dilakukan terlihat tidak setiap hari dilakukan, dan hanya terlihat dilakukan beberapa kali saja dalam kurun waktu 1 bulan yaitu pada sepertiga bulan awal dan sepertiga akhir bulan.



Gambar 4.9 Hasil Rule id 31509 ke website websitepenelitiantesis.my.id

Sedangkan hasil data yang didapatkan berdasarkan filtering **rule id 31510** pada **Gambar 4.10** menunjukkan bahwa website **websitepenelitiantesis.my.id** mendapatkan serangan beruntun/konsisten sebanyak **66** pada beberapa IP Address tertentu. Jumlah penyerang konsisten tersebut diklasifikasikan berdasarkan Negara penyerang sesuai dengan **Tabel 4.3** dibawah.



Gambar 4.10 Hasil Rule id 31509 ke website websitepenelitiantesis.my.id

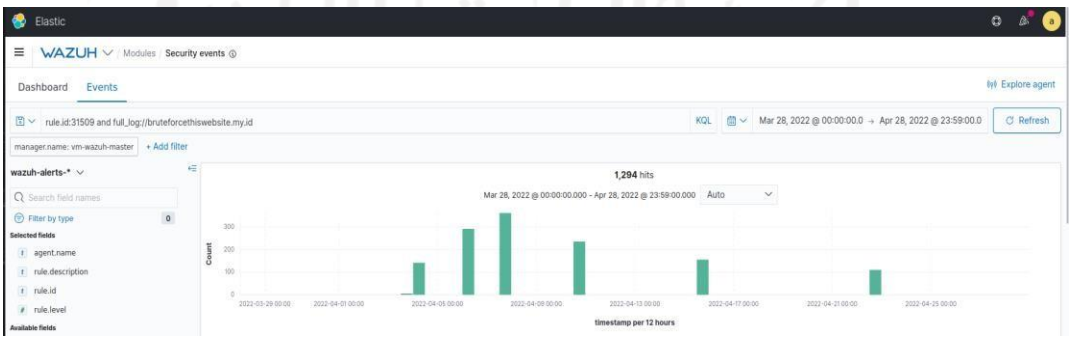
Adapun negara penyerang menurut jumlah serangan pada rule id **31510** adalah sebagai berikut :

Tabel 4.4 5 Negara terbesar penyerang website websitepenelitiantesis.my.id

No	Negara	Jumlah Serangan
1	United States	32
2	Indonesia	16
3	Turkey	10
4	Singapore	8
5	-	-

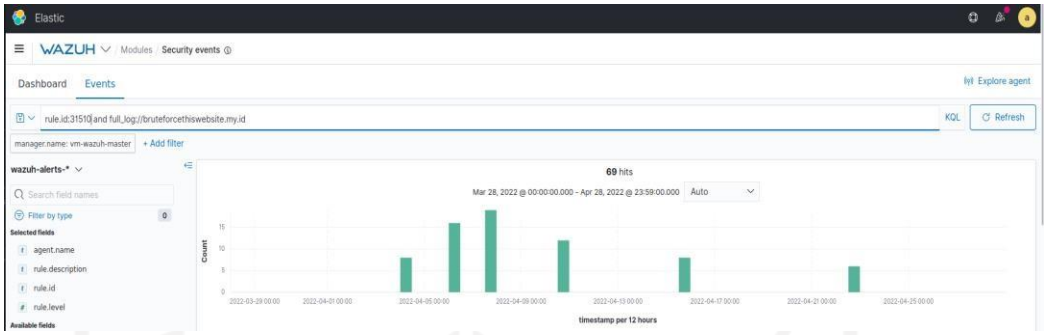
c. Perincian terhadap serangan ke website **bruteforcethiswebsite.my.id** berdasarkan rule id *brute force web server* adalah sebagai berikut :

Hasil data yang didapatkan berdasarkan filtering **rule id 31509** dan nama website menunjukkan bahwa website **websitepenelitiantesis.my.id** mendapatkan **1294** serangan sesuai **Gambar 4.11.** Serangan yang dilakukan terlihat tidak setiap hari dilakukan, dan hanya terlihat dilakukan beberapa kali saja dalam kurun waktu 1 bulan yaitu pada pertengahan bulan saja.



Gambar 4.11 Hasil Rule id 31509 ke website bruteforcethiswebsite.my.id

Sedangkan hasil data yang didapatkan berdasarkan filtering **rule id 31510** pada **Gambar 4.12** menunjukkan bahwa website **bruteforcethiswebsite.my.id** mendapatkan serangan beruntun/konsisten sebanyak **69** pada beberapa IP Address tertentu. Jumlah penyerang konsisten tersebut diklasifikasikan berdasarkan Negara penyerang sesuai dengan **Tabel 4.4** dibawah.



Gambar 4.12 Hasil Rule id 31510 ke website bruteforcethiswebsite.my.id

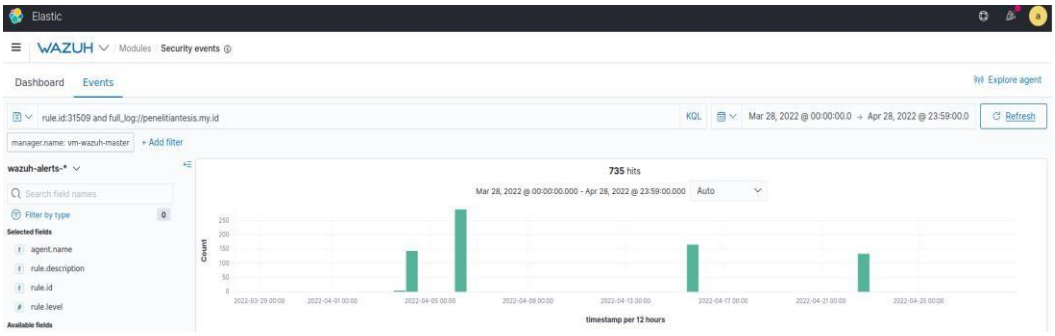
Adapun negara penyerang menurut jumlah serangan pada rule id **31510** adalah sebagai berikut :

Tabel 4.5 5 Negara terbesar penyerang website bruteforcethiswebsite.my.id

No	Negara	Jumlah Serangan
1	United States	20
2	Romania	19
3	Singapore	16
4	Turkey	14
5	-	-

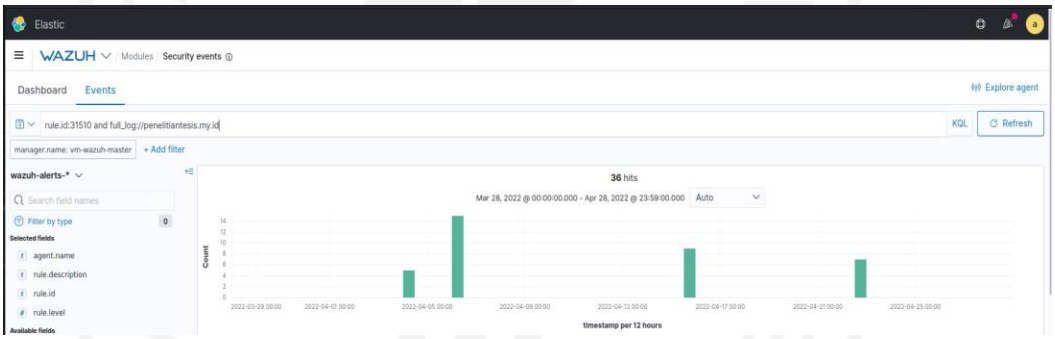
d. Perincian terhadap serangan ke website **penelitiantesis.my.id** berdasarkan rule id *brute force web server* adalah sebagai berikut :

Hasil data yang didapatkan berdasarkan filtering **rule id 31509** dan nama website menunjukkan bahwa website **penelitiantesis.my.id** mendapatkan **735** serangan sesuai **Gambar 4.13.** Serangan yang dilakukan terlihat tidak setiap hari dilakukan, dan hanya terlihat dilakukan beberapa kali saja dalam kurun waktu 1 bulan yaitu pada sepertiga awal dan akhir bulan saja. Merupakan website dengan tingkat intensitas paling rendah dibandingkan 4 website lainnya.



Gambar 4.13 Hasil Rule id 31509 ke website penelitiantesis.my.id

Sedangkan hasil data yang didapatkan berdasarkan filtering **rule id 31510** pada **Gambar 4.14** menunjukkan bahwa website **penelitiantesis.my.id** mendapatkan serangan beruntun/konsisten sebanyak 3**6** pada beberapa IP Address tertentu. Jumlah penyerang konsisten tersebut diklasifikasikan berdasarkan Negara penyerang sesuai dengan **Tabel 4.5** dibawah.



Gambar 4.14 Hasil Rule id 31510 ke website penelitiantesis.my.id

Adapun negara penyerang menurut jumlah serangan pada rule id **31510** adalah sebagai berikut :

Tabel 4.6 5 Negara terbesar penyerang website penelitiantesis.my.id

No	Negara	Jumlah Serangan
1	Singapore	15
2	United States	9
3	Romania	7
4	Turkey	5
5	-	-

4.2.2 Hasil Analisis Klaster Pertama

Berdasarkan analisis serangan yang dilakukan oleh *Hacker* pada klaster 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 baru dibuat dan dikelola mendapatkan serangan *brute force* yang sedikit. Berbeda dengan server tempat me-*hosting* websitetersebut 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 *brute force* menuju keserver tempat website di-*hosting* (**rule id 5710 & 5712**) menunjukkan angka serangan yangtinggi.

Metadata log yang diterima pada klaster pertama bagian **rule id 5710** menghasilkan **251362 hits** dan **rule id 5712** yang menghasilkan **1245 hits.** Sedangkan pada klaster kedua **rule id 5710** menghasilkan **465 hits** dan **rule id 5712** menghasilkan **4 hits**. Hasil ini menunjukkan bahwa serangan dari *Hacker* yang ada di seluruh 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 yang dilakukan oleh user maupun *Hacker*, seperti **Gambar 4.15** Metadata Log SSH pada klaster Pertama *:*

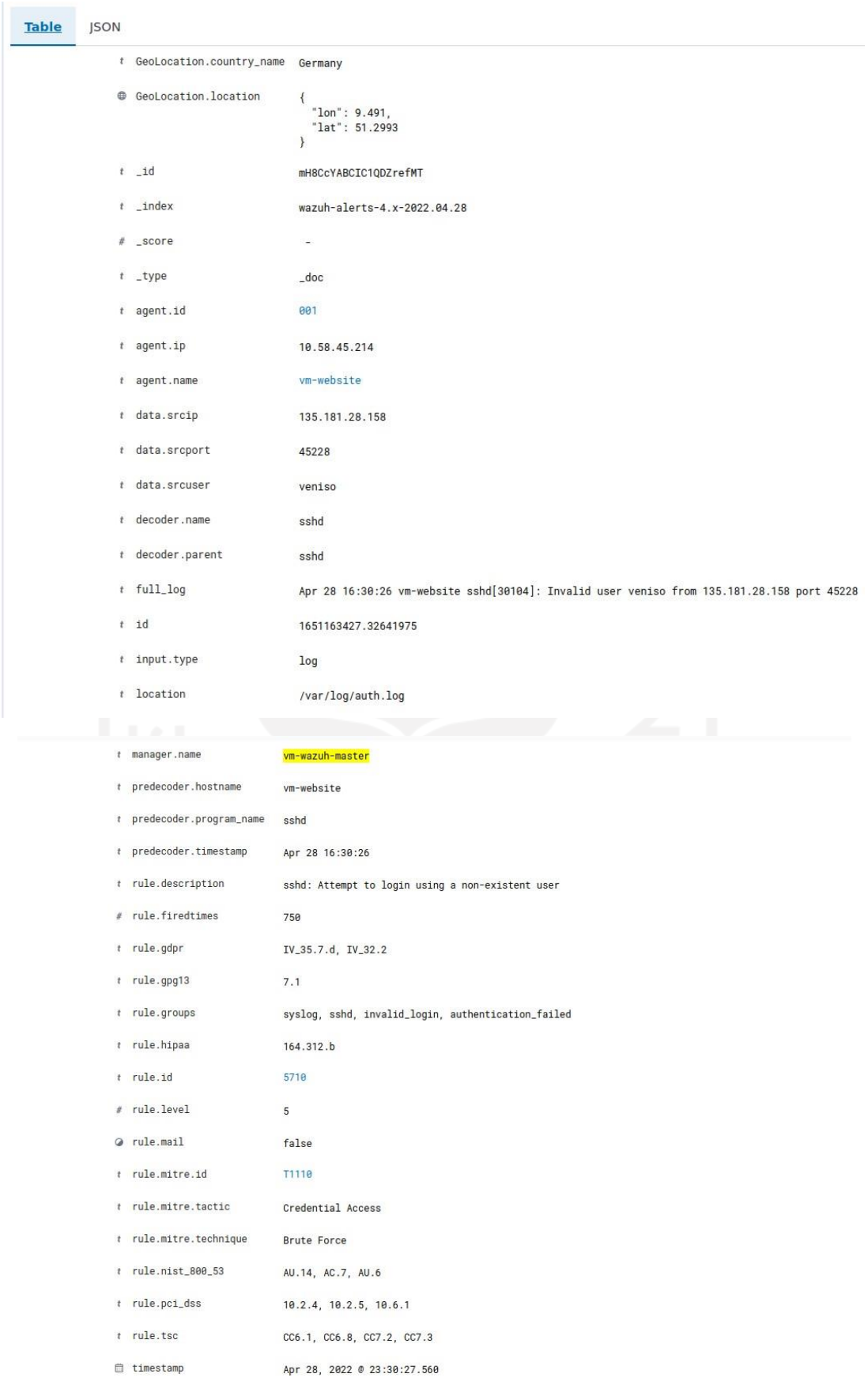


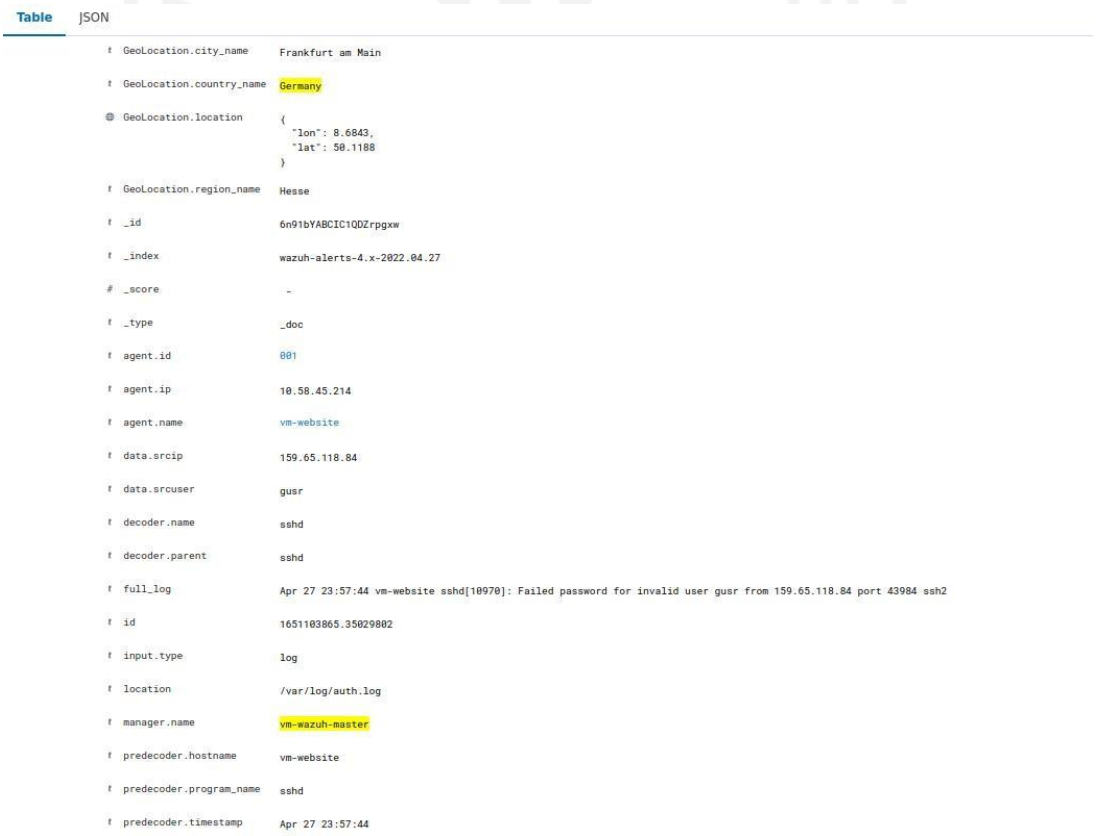
Table | JSON

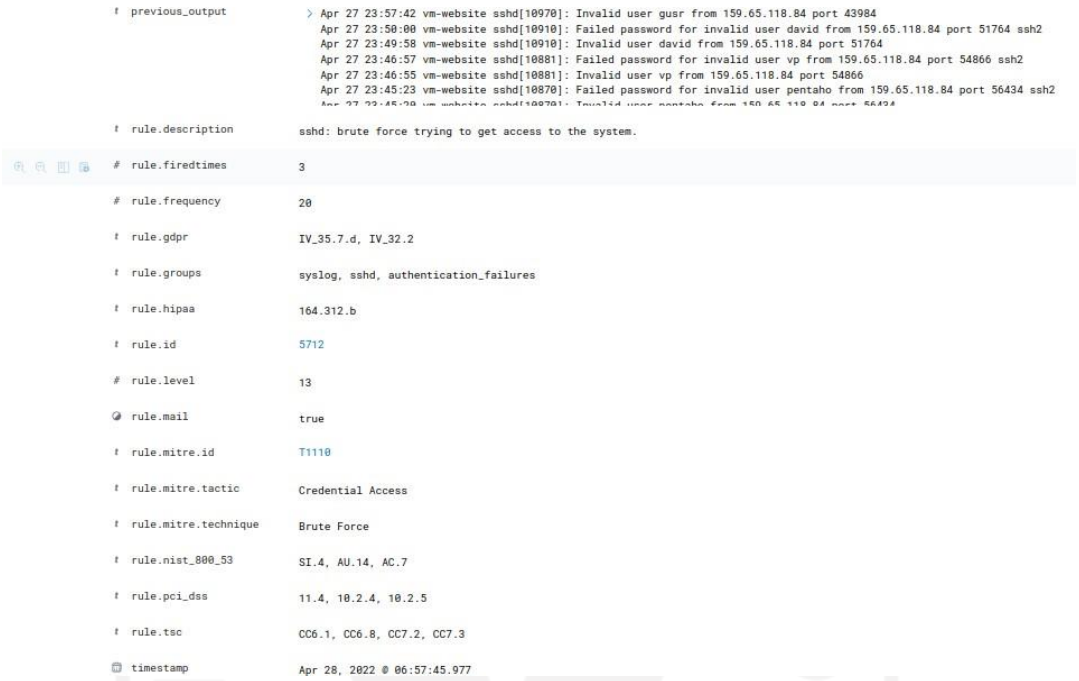
t GeoLocation.country_name	Germany
GeoLocation.location	{ "lon": 9.491, "lat": 51.2993 }
t _id	mH8CcYABCIC1QDZrefMT
t _index	wazuh-alerts-4.x-2022.04.28
# _score	-
t _type	_doc
t agent.id	001
t agent.ip	10.58.45.214
t agent.name	vm-website
t data.srcip	135.181.28.158
t data.srcport	45228
t data.srcuser	veniso
t decoder.name	sshd
t decoder.parent	sshd
t full_log	Apr 28 16:30:26 vm-website sshd[30104]: Invalid user veniso from 135.181.28.158 port 45228
t id	1651163427.32641975
t input.type	log
t location	/var/log/auth.log
t manager.name	vm-wazuh-master
t predecoder.hostname	vm-website
t predecoder.program_name	sshd
t predecoder.timestamp	Apr 28 16:30:26
t rule.description	sshd: Attempt to login using a non-existent user
# rule.firedtimes	750
t rule.gdpr	IV_35.7.d, IV_32.2
t rule.gpg13	7.1
t rule.groups	syslog, sshd, invalid_login, authentication_failed
t rule.hipaa	164.312.b
t rule.id	5710
# rule.level	5
rule.mail	false
t rule.mitre.id	T1110
t rule.mitre.tactic	Credential Access
t rule.mitre.technique	Brute Force
t rule.nist_800_53	AU.14, AC.7, AU.6
t rule.pci_dss	10.2.4, 10.2.5, 10.6.1
t rule.tsc	CC6.1, CC6.8, CC7.2, CC7.3
timestamp	Apr 28, 2022 @ 23:30:27.560

Gambar 4.15 Metadata Log SSH Rule id 5710

Pada **Gambar 4.15** diatas menunjukkan salah satu serangan yang tidak terorganisir atau serangan coba coba yang dilakukan oleh *Hacker*. Maksud dari serangan tidak terorganisir merupakan serangan sekali atau dua kali saja tanpa ada tujuan untuk membobol atau mencari kredensial yang dimiliki oleh user yang diserang. Adapun untuk cara membaca Metadata log akan disampaikan pada penjelasan Metadata log **rule id 5712** dibawah. Selain serangan dari serangan yang dilakukan oleh *Hacker* ini terdapat pula hal lain yang dapat men-*trigger* **rule id 5710** ini, yaitu kesalahan saat menginputkan kredensial ketika login ke server/ssh ke server. Maka dari itu jumlah dari serangan ini sangat banyak sekali dibandingkan rule id turunannya. Sehingga meskipun **rule id 5710** menghasilkan banyak hits/serangan dapat diabaikan.

Berbeda dengan **rule id 5712** yang merupakan turunan atau versi rule yang lebih unggul dari **rule id 5710**. **Rule id 5712** mencatat kesalahan atau serangan yang dilakukan oleh *Hacker* yang mencoba usaha *brute force* berdasarkan IP Address yang dimiliki oleh penyerang. Hal ini membuktikan bahwa serangan *brute force* pada **rule id 5712** terlihat lebih baik dibandingkan **rule id 5710**. Karena dengan ini bisa diketahui siapa yang memang sengaja melakukan usaha *brute force* untuk mendapatkan kredensial server dan bukan merupakan kesalahan input username dan password saja. Pada **rule id 5712** bisa dilihat bukti yang diambil berdasarkan metadata log pada **Gambar 4.16** :





Gambar 4.16 Metadata Log SSH rule id 5712

Adapun penjabaran lebih lanjut dari analisis kedua metadata tersebut adalah sebagai berikut :

Tabel 4.7 Penjelasan Metadata Log Rule id 5712

Nama Metadata	Isi Metadata	Arti
GeoLocation.city_name	Frankfurt am Main	Kota tempat *Hacker* menyerang
GeoLocation.country_name	Germany	Negara tempat *Hacker* menyerang
GeoLocation.location	{ "lon": 8.6843, "lat": 50.1188 }	Garis Lintang dan Bujur tempat *Hacker* menyerang, biasanya disamakan dengan kota maupun negara.
GeoLocation.region_name	Hesse	Daerah tempat *Hacker* menyerang, biasanya lokasi server atau bila beruntung tempat isp yang digunakan oleh *Hacker*
_index	wazuh-alerts-4.x-2022.04.27	Indeks tempat menyimpan *log* yang ada di wazuh

Tabel 4.6 Penjelasan Metadata Log Rule id 5712 (Lanjutan)

Nama Metadata	Isi Metadata	Arti
_type	_doc	Tipe *log* yang dihasilkan oleh wazuh
agent.id	001	Nomor agen yang menjadi tempat serangan diterima
agent.ip	10.58.45.214	IP Address agen yang diserang oleh *Hacker*
agent.name	vm-website	Nama agen yang diserang oleh *Hacker*
data.srcip	159.65.118.84	IP Address penyerang / *Hacker*
data.srcuser	gusr	Nama yang digunakan untuk login pada server
decoder.parent	Sshd Apr 27 23:57:44 vm-website sshd[10970]: Failed password for invalid user gusr from 159.65.118.84 port 43984 ssh2	Rule parent yang digunakan oleh Wazuh Full log pada server yang diserang oleh *Hacker* kemudian di parse berbentuk kalimat oleh Wazuh
manager.name	vm-wazuh-master	Wazuh manager yang digunakan untuk mengelola agen yang diregister
predecoder.timestamp	Apr 27 23:57:44	Waktu kejadiannya log pertama.
previous_output	Apr 27 23:57:42 vm-website sshd[10970]: Invalid user gusr from 159.65.118.84 port 43984 Apr 27 23:50:00 vm-website sshd[10910]: Failed password for invalid user david from 159.65.118.84 port 51764 ssh2 Apr 27 23:49:58 vm-website sshd[10910]: Invalid user david from 159.65.118.84 port 51764 Apr 27 23:46:57 vm-	Log log yang mengindikasikan serangan *brute force.* Pada *log* ini dicatat bahwa sumber IP Address yang disebutkan diatas telah berusaha melakukan usaha untuk masuk ke server tempat website di-*hosting* dengan mencoba berbagai username (Seperti terlihat pada log, *Hacker* mencoba beberapa username sebagai berikut : david, vp,

Tabel 4.6 Penjelasan Metadata Log Rule id 5712 (Lanjutan)

Nama Metadata	Isi Metadata	Arti
	website sshd[10881]: Failed password for invalid user vp from 159.65.118.84 port 54866 ssh2 Apr 27 23:46:55 vm-website sshd[10881]: Invalid user vp from 159.65.118.84 port 54866 Apr 27 23:45:23 vm-website sshd[10870]: Failed password for invalid user pentaho from 159.65.118.84 port 56434 ssh2 Apr 27 23:45:20 vm-website sshd[10870]: Invalid user pentaho from 159.65.118.84 port 56434 Apr 27 23:43:48 vm-w Failed password for invalid user kawaguchi from 159.65.118.84 port 57990 ssh2 Apr 27 23:43:46 vm-website sshd[10853]: Invalid user kawaguchi from 159.65.118.84 port 57990 Apr 27 23:34:27 vm-website sshd[10351]: Failed password for invalid user svnuser from 159.65.118.84 port 39090 ssh2 Apr 27 23:34:25 vm-website sshd[10351]: Invalid user svnuser from 159.65.118.84 port 39090	pentaho, kawaguchi, svnuser).
rule.description	sshd: brute force trying to get access to the system.	Deskripsi rule yang digunakan oleh Wazuh
rule.firedtimes	3	Jumlah rule id 5712 yang telah dihasilkan oleh Wazuh sesuai dengan serangan Hacker yang memiliki IP Address diatas

Tabel 4.6 Penjelasan Metadata Log Rule id 5712 (Lanjutan)

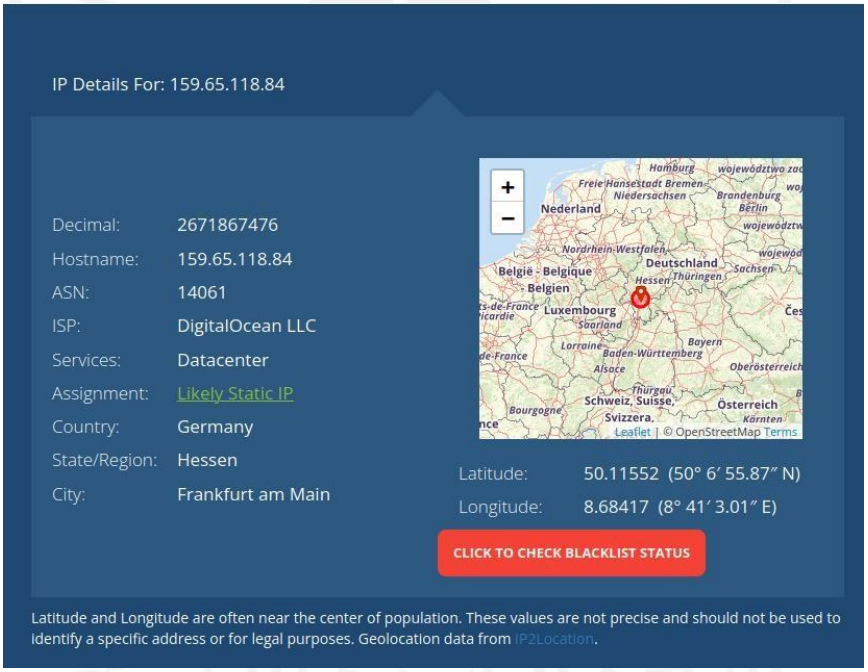
Nama Metadata	Isi Metadata	Arti
rule.frequency	20	Jumlah rule id 5710 yang dihasilkan oleh Wazuh sesuai dengan serangan Hacker yang memiliki IP Address diatas
rule.groups	syslog, sshd, authentication_failures	Rule grup yang dimiliki oleh Wazuh dan log ini masuk pada rule group sesuai value isi metadata log
rule.id	5712	Rule id yang dimiliki oleh Wazuh dalam mengidentifikasi serangan brute force pada server
rule.level	13	Rule level yang dimiliki oleh Wazuh dalam mengidentifikasi level
rule.mail	true	Jika di set true maka akan mengirimkan alert atau notifikasi kepada email yang sudah di konfigurasi oleh Administrator kritis pada log yang dihasilkan Wazuh
rule.mitre.technique	Brute Force	Nama rule mitre yang dimiliki oleh Wazuh
timestamp	Apr 28, 2022 @ 06:57:45.977	Waktu berakhirnya log / rule id yang dihasilkan oleh Wazuh .

Metadata *log* yang dihasilkan diatas tidak semuanya dicatat berdasarkan **Gambar 4.16** Wazuh hasilkan. Hal yang dicatat dan dijelaskan merupakan metadata yang berguna dalam proses analisis penelitian. Adapun hal yang ditampilkan pada **Tabel 4.6** merupakan informasi metadata *log* yang berguna dalam proses analisis penelitian.

4.2.3 Laporan Hasil Analisis Klaster Pertama

Laporan pembahasan dari analisis pada klaster pertama menunjukkan bahwa tingkat serangan *brute force* 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. Tidak terlihat indikasi bahwa *hacker* telah masuk ke dalam server. Maka dari itu proses analisis terhadap log *auditd* tidak dilakukan/dilewati.

Berdasarkan hasil sub-bab analisis yang didapatkan pada **Tabel 4.6** menunjukkan bahwa lokasi tempat *Hacker* menyerang dapat didapatkan hingga lokasi daerah tempat *Hacker* berada. Hal tersebut diasumsikan bahwa *Hacker* tidak menggunakan VPN atau *tools* lainnya untuk menyamarkan keberadaannya, Namun setelah ditilik menggunakan website https://whatismyipaddress.com pada **Gambar 4.17** dibawah *Hacker* menggunakan ISP DigitalOcean LLC yang berada di kota Frankfurt, Hesse negara bagian dari Jerman.

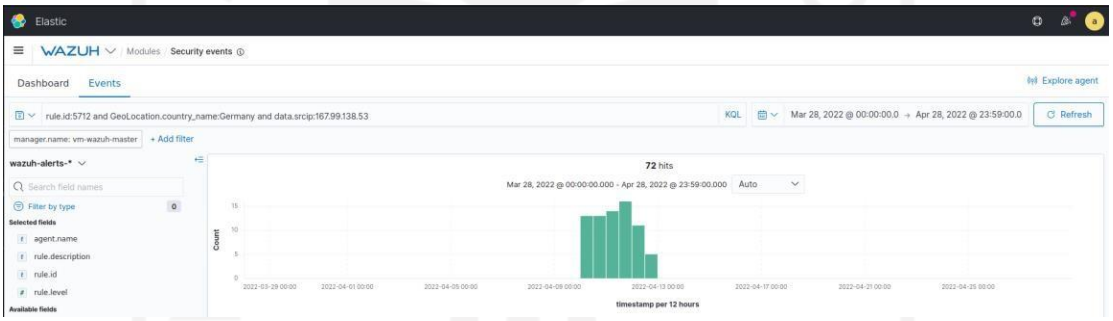


Gambar 4.17 Tempat *Hacker* melancarkan serangan

Tentunya hal ini mempersulit dalam pengungkapan lokasi sebenarnya dari *Hacker*, namun setidaknya telah didapatkan informasi bahwa penyerang menggunakan VPN atau benar berasal dari negara sesuai informasi yang diberikan oleh website https://whatismyipaddress.com. Langkah selanjutnya dalam mengecilkan dugaan bahwa *Hacker* ini berasal dari negara tersebut atau memakai VPN adalah dengan melihat *log brute force* pada hari itu dan jam yang berdekatan dengan *log* yang dihasilkan Wazuh ini. Pada **Gambar 4.18** menunjukkan bahwa pada Tanggal 28 April 2022 dengan selisih waktu kurang dari 1 jam terdapat indikasi *brute force* pada server Wazuh master berada.

Gambar 4.18 Indikasi *brute force* dilakukan oleh orang yang sama

Hasil yang diberikan metadata *log* pada *log* baru yang terpaut tidak kurang dari 1 jam dengan *log* yang dijelaskan ini mengindikasikan bahwa sebenarnya serangan dilakukan oleh orang yang sama. Namun dalam waktu satu hari serangan yang dilakukan berhenti pada 2 serangan saja dan tidak dilanjutkan kembali oleh *Hacker* tersebut. Tentunya hal ini mengacu pada contoh metadata log pada **Gambar 4.18** di atas. Bila digunakan contoh metadata log lainnya seperti pada **Gambar 4.19** yang mengacu pada IP Address 67.99.138.53 menunjukkan serangan yang dilakukan selama 3 hari berturut turut dimulai dari 10 April dan berhenti pada 12 April 2022.



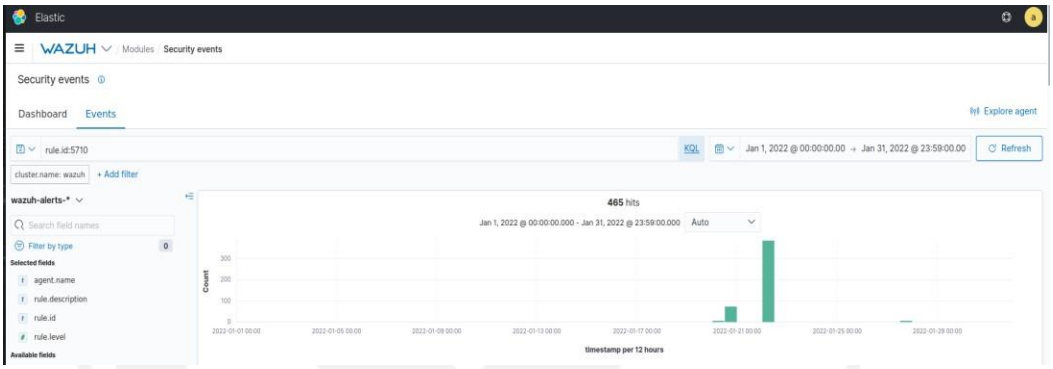
Gambar 4.19 Contoh Metadata Log serangan yang intens

Bila dilihat berdasarkan contoh metadata *log* lainnya yang merujuk pada IP Address 67.99.138.53 serangan dilakukan secara intens hingga men-*trigger* **rule id 5712** sebanyak 72 kali. Dengan kondisi IP sumber serangan tersebut berasal dari Hesse, Frankfurt Jerman juga. Bahkan ketika dilihat dari https://whatismyipaddress.com menunjukkan bahwa serangan berasal dari Data Center DigitalOcean LLC juga. Ini mengindikasikan bahwa serangan bisa jadi berasal dari orang yang sama diturut berdasarkan tempat/lokasi di lacaknya IP Address penyerang atau *Hacker*.

4.2.4 Pengumpulan Data klaster Kedua

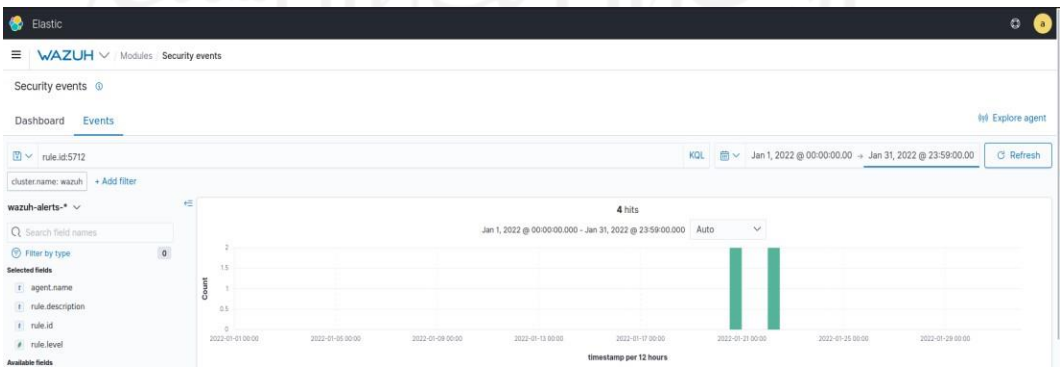
Pada hasil analisis yang dilakukan di klaster kedua selama 1 Bulan (terhitung dari tanggal 1 Januari 2022 hingga 31 Januari 2022) menunjukkan hasil *brute force* yang dilakukan oleh hacker berjumlah :

a. **Rule id 5710** mendapatkan serangan sebanyak **465 hits** seperti pada **Gambar 4.20.** Hasil serangan ini ditujukan pada server tempat website di-hosting oleh Administrator. Sesuai dengan **rule id** yang diberikan bahwa serangan ini menyerang dengan teknik *brute force* lewat jalur login ssh kredensial. Pada **Gambar 4.20** 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.



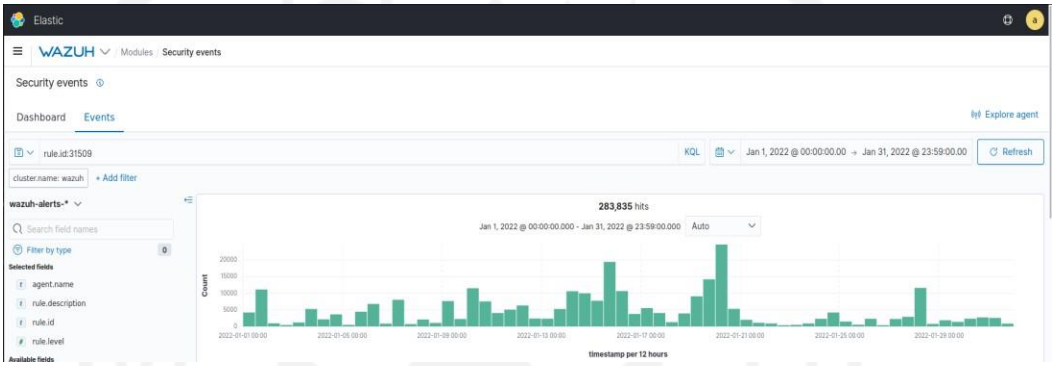
Gambar 4.20 Rule id 5710 klaster kedua

b. **Rule id 5712** mendapatkan serangan sebanyak **4 hits** seperti pada **Gambar 4.21.** Hasil serangan ini ditujukan pada server tempat website di-hosting oleh Administrator 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 4.20** dan **Gambar 4.21** 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.



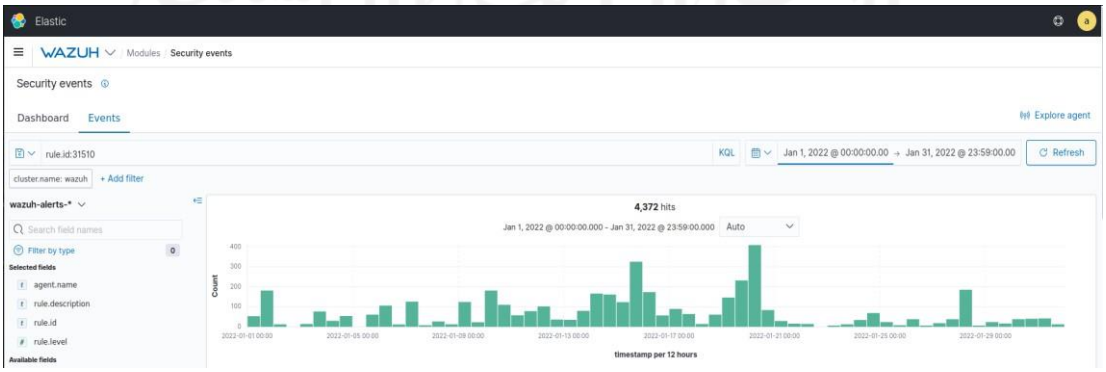
Gambar 4.21 Rule id 5712 klaster kedua

c. **Rule id 31509** mendapatkan serangan sebanyak **283835 hits** seperti pada **Gambar 4.22.** 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 4.22** 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 4.22 Rule id 31509 klaster kedua

d. **Rule id 31510** mendapatkan serangan sebanyak **4372 hits** seperti pada **Gambar 4.23.** 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 4.22** dan **Gambar 4.23** menunjukkan aktivitas yang dilakukan oleh *Hacker* konsisten dalam usahanya 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.

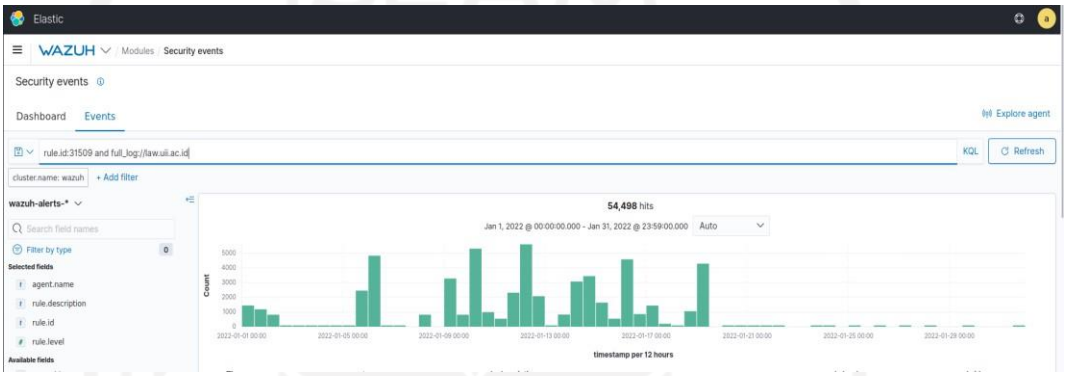


Gambar 4.23 Rule id 31509 klaster kedua

Perincian terhadap serangan yang mengarah pada 5 website teratas tersebut adalah sebagai berikut :

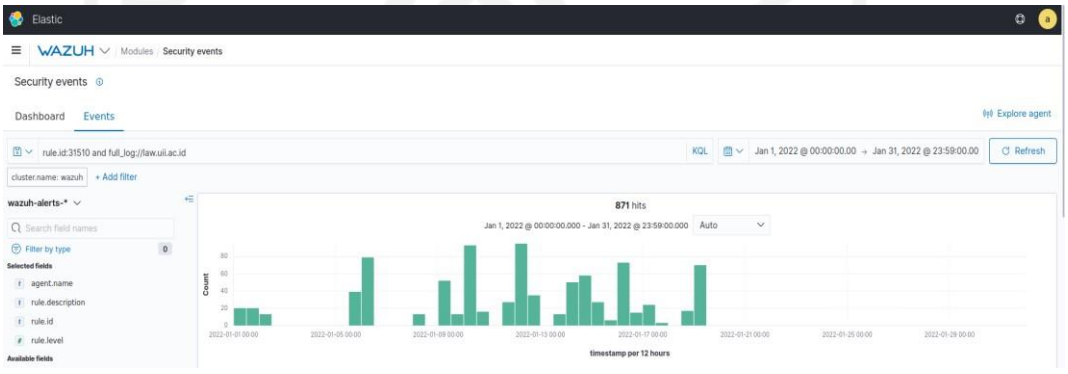
a. Perincian terhadap serangan ke website **law.uii.ac.id** berdasarkan rule id *brute force web server* adalah sebagai berikut :

   Hasil data yang didapatkan berdasarkan filtering **rule id 31509** dan nama website menunjukkan bahwa website **law.uii.ac.id** mendapatkan **54498** serangan sesuai **Gambar 4.24.** Serangan yang dilakukan terlihat hampir setiap hari dilakukan, hanya terlihat mengalami penurunan serangan pada akhir bulan. Namun tingkat intensitas serangan yang dilakukan paling tinggi dibanding 4 website lainnya.



Gambar 4.24 Hasil Rule id 31509 ke website law.uii.ac.id

Sedangkan hasil data yang didapatkan berdasarkan filtering **rule id 31510** pada **Gambar 4.25** menunjukkan bahwa website **law.uii.ac.id** mendapatkan serangan beruntun/konsisten sebanyak **871** pada beberapa IP Address tertentu. Jumlah penyerang konsisten tersebut diklasifikasikan berdasarkan Negara penyerang sesuai dengan **Tabel 4.7** dibawah.



Gambar 4.25 Hasil Rule id 31510 ke website law.uii.ac.id

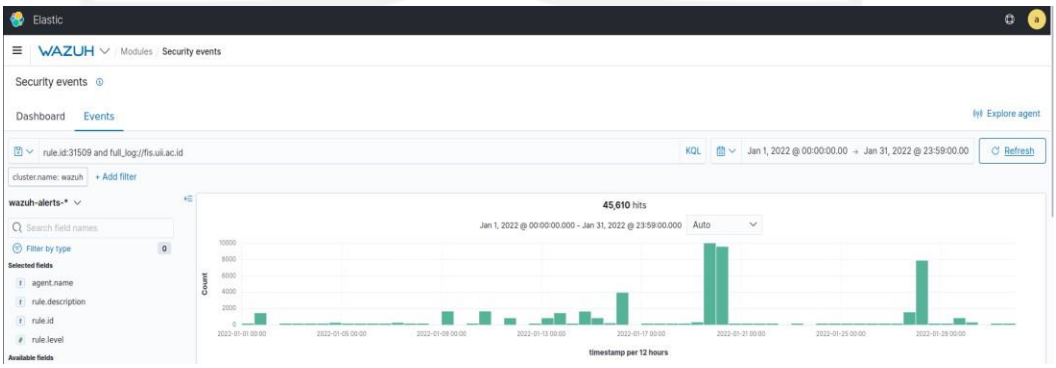
Adapun negara penyerang menurut jumlah serangan pada rule id **31510** adalah sebagai berikut :

Tabel 4.8 5 Negara terbesar penyerang website law.uii.ac.id

No	Negara	Jumlah Serangan
1	United States	272
2	Singapore	214
3	United Kingdom	141
4	Turkey	110
5	France	69
6	South Africa	36
7	Netherlands	13
8	Canada	11
9	Italy	5

b. Perincian terhadap serangan ke website **fis.uii.ac.id** berdasarkan rule id *brute force web server* adalah sebagai berikut :

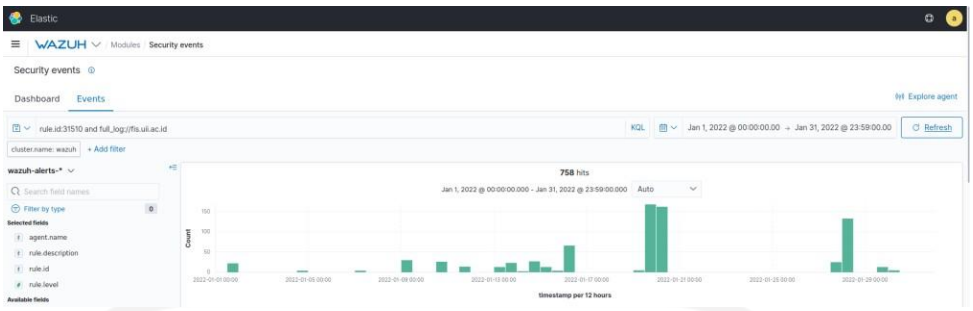
Hasil data yang didapatkan berdasarkan filtering **rule id 31509** dan nama website menunjukkan bahwa website **fis.uii.ac.id** mendapatkan **45610** serangan sesuai **Gambar 4.26.** Serangan yang dilakukan terlihat hampir setiap hari namun dengan intensitas yang minim. Serangan terlihat memuncak pada akhir bulan.



Gambar 4.26 Hasil Rule id 31509 ke website fis.uii.ac.id

Sedangkan hasil data yang didapatkan berdasarkan filtering **rule id 31510** pada **Gambar 4.27** menunjukkan bahwa website **fis.uii.ac.id** mendapatkan serangan beruntun/konsisten sebanyak **758** pada beberapa IP Address tertentu. Jumlah

penyerang konsisten tersebut diklasifikasikan berdasarkan Negara penyerang sesuai dengan **Tabel 4.8** dibawah.



Gambar 4.27 Hasil Rule id 31510 ke website fis.uii.ac.id

Adapun negara penyerang menurut jumlah serangan pada rule id **31510** adalah sebagai berikut :

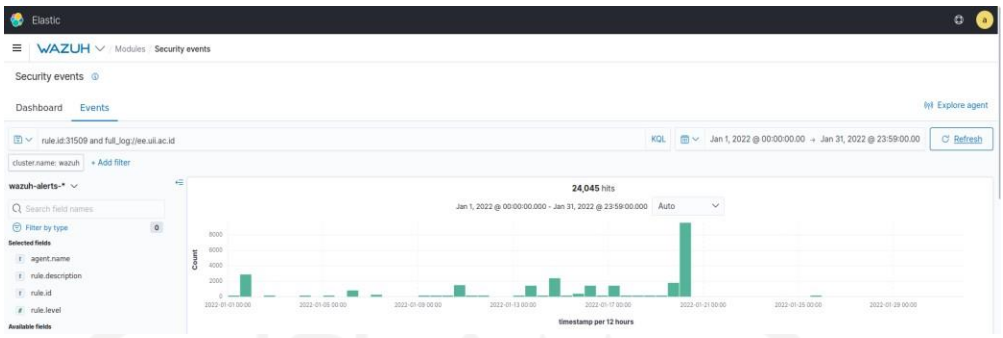
Tabel 4.9 Negara terbesar penyerang website fis.uii.ac.id

No	Negara	Jumlah Serangan
1	United States	237
2	United Kingdom	209
3	Netherlands	156
4	Turkey	62
5	Singapore	48
6	France	26
7	Canada	10
8	South Africa	5
9	Italy	5

c. Perincian terhadap serangan ke website **ee.uii.ac.id** berdasarkan rule id *brute force web server* adalah sebagai berikut :

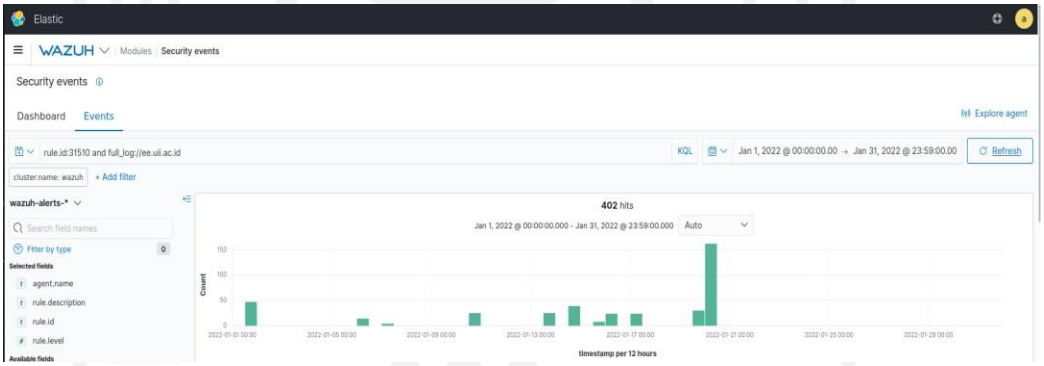
Hasil data yang didapatkan berdasarkan filtering **rule id 31509** dan nama website menunjukkan bahwa website **ee.uii.ac.id** mendapatkan **24045** serangan sesuai **Gambar 4.28.** Serangan yang dilakukan terlihat hampir setiap hari namun dengan intensitas yang minim. Serangan terlihat konsisten pada dua pertiga awal bulan saja

dan memuncak pada akhir dua pertiga bulan tersebut kemudian diikuti dengan selesainya serangan yang dilakukan oleh *Hacker*.



Gambar 4.28 Hasil Rule id 31509 ke website ee.uii.ac.id

Sedangkan hasil data yang didapatkan berdasarkan filtering **rule id 31510** pada **Gambar 4.29** menunjukkan bahwa website **ee.uii.ac.id** mendapatkan serangan beruntun/konsisten sebanyak **402** pada beberapa IP Address tertentu. Jumlah penyerang konsisten tersebut diklasifikasikan berdasarkan Negara penyerang sesuai dengan **Tabel 4.9** dibawah.



Gambar 4.29 Hasil Rule id 31510 ke website ee.uii.ac.id

Adapun negara penyerang menurut jumlah serangan pada rule id **31510** adalah sebagai berikut :

Tabel 4.10 5 Negara terbesar penyerang website ee.uii.ac.id

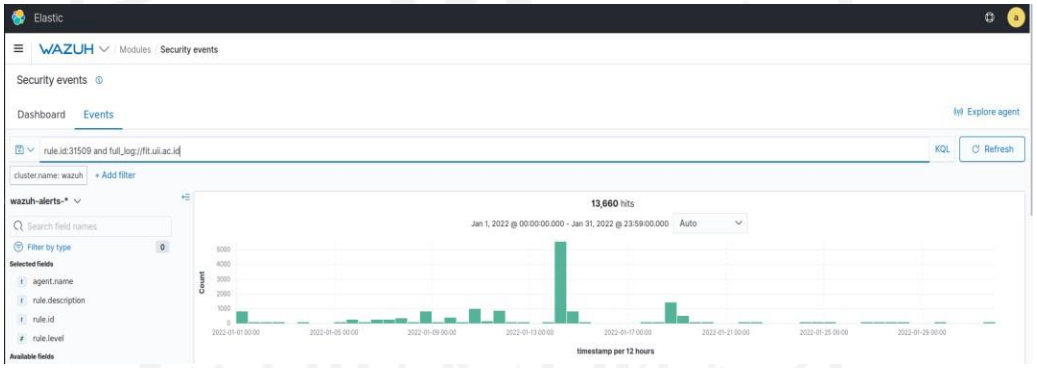
No	Negara	Jumlah Serangan
1	United States	301
2	Italy	22
3	United Kingdom	16
4	Netherlands	14
5	France	14

Tabel 4.9 5 Negara terbesar penyerang website ee.uii.ac.id (Lanjutan)

No	Negara	Jumlah Serangan
6	Singapore	14
7	Turkey	12
8	South Africa	8
9	Canada	1

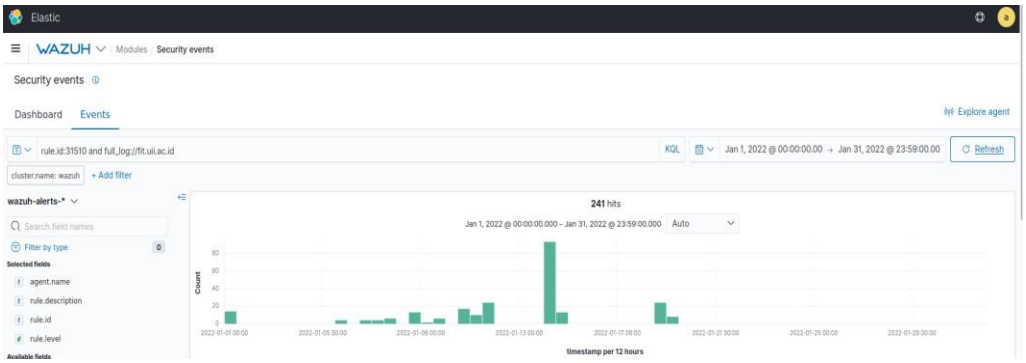
d. Perincian terhadap serangan ke website **fit.uii.ac.id** berdasarkan rule id *brute force web server* adalah sebagai berikut :

Hasil data yang didapatkan berdasarkan filtering **rule id 31509** dan nama website menunjukkan bahwa website **fit.uii.ac.id** mendapatkan **13660** serangan sesuai **Gambar 4.30.** Serangan yang dilakukan terlihat hampir setiap hari namun dengan intensitas yang minim. Serangan terlihat konsisten pada dua pertiga awal bulan saja dan memuncak pada pertengahan bulan tersebut kemudian diikuti dengan serangan berintensitas kecil yang dilakukan oleh *Hacker*.



Gambar 4.30 Hasil Rule id 31509 ke website fit.uii.ac.id

Sedangkan hasil data yang didapatkan berdasarkan filtering **rule id 31510** pada **Gambar 4.31** menunjukkan bahwa website **fit.uii.ac.id** mendapatkan serangan beruntun/konsisten sebanyak **241** pada beberapa IP Address tertentu. Jumlah penyerang konsisten tersebut diklasifikasikan berdasarkan Negara penyerang sesuai dengan **Tabel 4.10** dibawah.



Gambar 4. 31 Hasil Rule id 31510 ke website fit.uii.ac.id

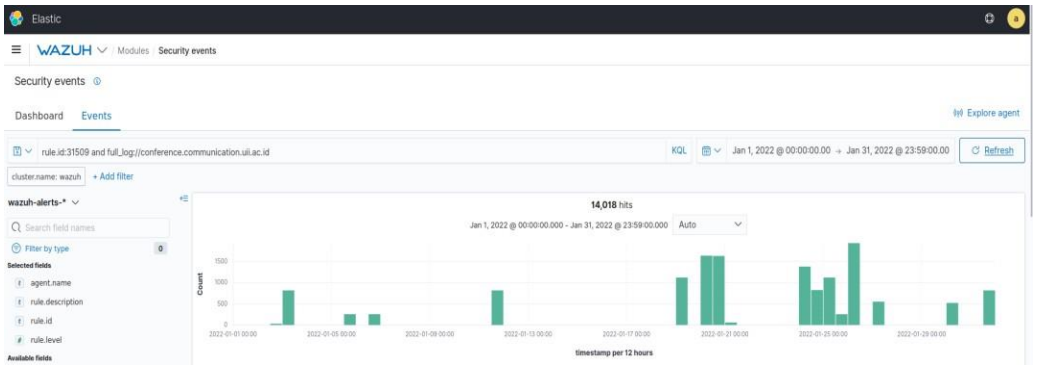
Adapun negara penyerang menurut jumlah serangan pada rule id **31510** adalah sebagai berikut :

Tabel 4.11 5 Negara terbesar penyerang website fit.uii.ac.id

No	Negara	Jumlah Serangan
1	United Kingdom	120
2	United States	115
3	Japan	4
4	Russia	2
5	-	-

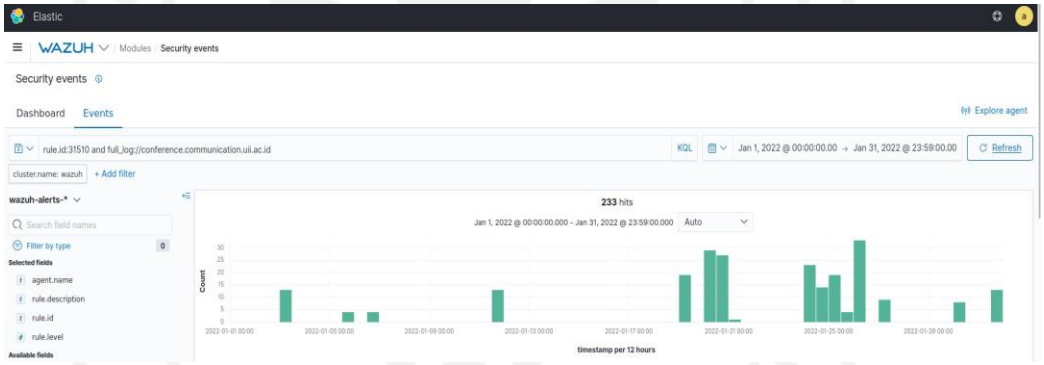
e. Perincian terhadap serangan ke website **conference.communication.uii.ac.id** berdasarkan rule id *brute force web server* adalah sebagai berikut :

Hasil data yang didapatkan berdasarkan filtering **rule id 31509** dan nama website menunjukkan bahwa website **conference.communication.uii.ac.id** mendapatkan **14018** serangan sesuai **Gambar 4.32.** Serangan yang dilakukan terlihat tidak setiap hari. Namun serangan terlihat konsisten pada akhir bulan dengan intensitas tertinggi dilakukan pada sepertiga akhir bulan tersebut.



Gambar 4.32 Hasil Rule id 31509 ke website conference.communication.uii.ac.id

Sedangkan hasil data yang didapatkan berdasarkan filtering **rule id 31510** pada **Gambar 4.33** menunjukkan bahwa website **conference.communication.uii.ac.id.uii.ac.id** mendapatkan serangan beruntun/konsisten sebanyak **233** pada beberapa IP Address tertentu. Jumlah penyerang konsisten tersebut diklasifikasikan berdasarkan Negara penyerang sesuai dengan **Tabel 4.11** dibawah.



Gambar 4.33 Hasil Rule id 31510 ke website conference.communication.uii.ac.id

Adapun negara penyerang menurut jumlah serangan pada rule id **31510** adalah sebagai berikut :

Tabel 4.12 5 Negara terbesar penyerang website conference.communication.uii.ac.id

No	Negara	Jumlah Serangan
1	Turkey	148
2	United States	30
3	Russia	23
4	Singapore	14

Tabel 4.11 5 Negara terbesar penyerang website conference.communication.uii.ac.id (Lanjutan)

No	Negara	Jumlah Serangan
5	Indonesia	13
6	Japan	4
7	Australia	1

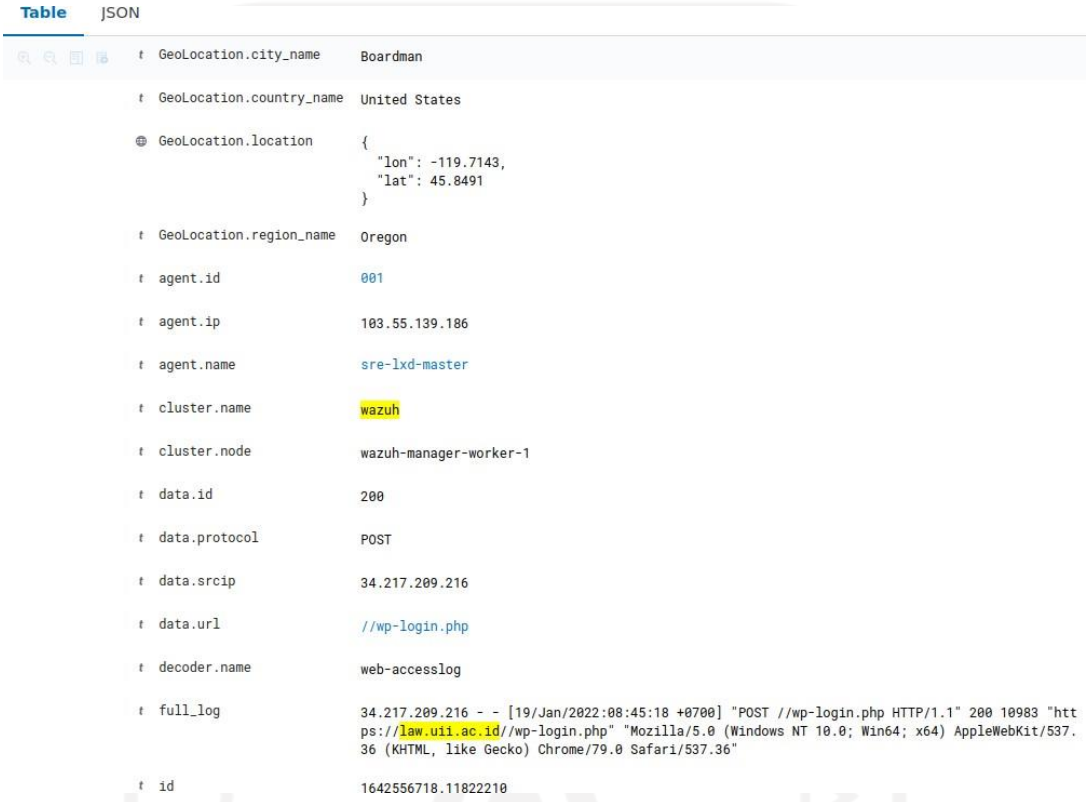
4.2.5 Hasil Analisis Klaster Kedua

Berdasarkan analisis serangan yang dilakukan oleh *Hacker* pada klaster 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 *brute force*, 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 diperkuat 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 *brute force* menuju ke website (**rule id 31509 & 31510**) menunjukkan angka serangan yang tinggi.

Pada sub-bab sebelumnya telah dibahas mengenai hasil analisis Metadata *Log* SSH. Selanjutnya pada sub-bab ini akan dibahas mengenai hasil analisis Metadata *Log* Nginx pada kedua klaster yang telah dilakukan penelitian. Berdasarkan penelitian yang dilakukan didapatkan hasil sebagai berikut. Metadata *Log* yang diterima pada klaster pertama bagian **rule id 31509** menghasilkan **6688 hits** dan **rule id 31510** menghasilkan **351 hits**. Sedangkan pada klaster 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.** Hal ini didasari bahwa pada klaster kedua merupakan klaster yang memuat website lama dari Universitas Islam Indonesia yang sudah lama ada/*exist.* Berbeda dengan website yang ada pada klaster

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. **Rule id 31509** tidak akan dibahas karena penjelasannya hampir sama dengan penjelasan **rule id 5710**. Penjelasan akan ditekankan dan difokuskan pada **rule id 31510**.

Adapun pada **Gambar 4.34** merupakan Metadata *Log* Nginx yang akan dianalisis pada klaster kedua :



t input.type	log
t location	/var/log/nginx/access.log
t manager.name	wazuh-manager-worker-1
t previous_output	34.217.209.216 - - [19/Jan/2022:08:45:16 +0700] "POST //wp-login.php HTTP/1.1" 200 10983 "https://law.uii.ac.id//wp-login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0 Safari/537.36" 34.217.209.216 - - [19/Jan/2022:08:45:15 +0700] "POST //wp-login.php HTTP/1.1" 200 10983 "https://law.uii.ac.id//wp-login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0 Safari/537.36" 34.217.209.216 - - [19/Jan/2022:08:45:14 +0700] "POST //wp-login.php HTTP/1.1" 200 10983 "https://law.uii.ac.id//wp-login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0 Safari/537.36" 34.217.209.216 - - [19/Jan/2022:08:45:13 +0700] "POST //wp-login.php HTTP/1.1" 200 10983 "https://law.uii.ac.id//wp-login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0 Safari/537.36" 34.217.209.216 - - [19/Jan/2022:08:45:12 +0700] "POST //wp-login.php HTTP/1.1" 200 10983 "https://law.uii.ac.id//wp-login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0 Safari/537.36" 34.217.209.216 - - [19/Jan/2022:08:45:11 +0700] "POST //wp-login.php HTTP/1.1" 200 10983 "https://law.uii.ac.id//wp-login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0 Safari/537.36" 34.217.209.216 - - [19/Jan/2022:08:45:09 +0700] "POST //wp-login.php HTTP/1.1" 200 10983 "https://law.uii.ac.id//wp-login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0 Safari/537.36" 34.217.209.216 - - [19/Jan/2022:08:45:08 +0700] "POST //wp-login.php HTTP/1.1" 200 10983 "https://law.uii.ac.id//wp-login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0 Safari/537.36" 34.217.209.216 - - [19/Jan/2022:08:45:07 +0700] "POST //wp-login.php HTTP/1.1" 200 10983 "https://law.uii.ac.id//wp-login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0 Safari/537.36" 34.217.209.216 - - [19/Jan/2022:08:45:06 +0700] "POST //wp-login.php HTTP/1.1" 200 10983 "https://law.uii.ac.id//wp-login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0 Safari/537.36" 34.217.209.216 - - [19/Jan/2022:08:45:06 +0700] "POST //wp-login.php HTTP/1.1" 200 10983 "https://law.uii.ac.id//wp-login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0 Safari/537.36"
t rule.description	CMS (WordPress or Joomla) brute force attempt.
# rule.firedtimes	16
# rule.frequency	60
t rule.gdpr	IV_35.7.d, IV_32.2
t rule.groups	web, appsec, attack
t rule.hipaa	164.312.b
t rule.id	31510
# rule.level	13
rule.mail	true
t rule.mitre.id	T1110
t rule.mitre.tactic	Credential Access
t rule.mitre.technique	Brute Force
t rule.nist_800_53	SA.11, SI.4, AU.14, AC.7
t rule.pci_dss	6.5, 11.4, 6.5.10, 10.2.4, 10.2.5
t rule.tsc	CC6.6, CC7.1, CC8.1, CC6.1, CC6.8, CC7.2, CC7.3
timestamp	Jan 19, 2022 @ 08:45:18.156

Gambar 4.34 Metadata Log Nginx Rule id 31510

Pada **Gambar 4.34** diatas merupakan salah satu contoh log yang dihasilkan wazuh berdasarkan **rule id 31510**. Keunggulan dari **rule id 31510** dibandingkan **rule id 31509** adalah **rule id 31510** mencatat kesalahan atau serangan yang dilakukan oleh *Hacker* berdasarkan IP Address yang dimiliki oleh *Hacker* tersebut.

Adapun penjabaran lebih lanjut dari analisis metadata log **rule id 31510** tersebut adalah sebagai berikut :

Tabel 4.13 Penjelasan Metadata Log Rule id 31510

Nama Metadata	Isi Metadata	Arti
GeoLocation.city_name	Boardman	Kota tempat *Hacker* menyerang
GeoLocation.country_name	United States	Negara tempat *Hacker* menyerang
GeoLocation.location	{ "lon": -119.7143, "lat": 45.8491 }	Garis Lintang dan Bujur tempat *Hacker* menyerang, biasanya disamakan dengan kota maupun negara.
GeoLocation.region_name	Oregon	Daerah tempat *Hacker* menyerang, biasanya lokasi server atau bila beruntung tempat isp yang digunakan oleh *Hacker*
Nama Metadata	Isi Metadata	Arti
agent.id	001	Nomor agen yang menjadi tempat serangan diterima
agent.ip	103.55.139.186	IP Address agen yang diserang oleh *Hacker*
agent.name	sre-lxd-master	Nama agen yang diserang oleh *Hacker*
klaster.name	wazuh	Nama klaster Wazuh
klaster.node	wazuh-manager-worker-1	Nama node tempat Wazuh klaster
data.id	200	Respon OK dari HTTP
data.protocol	POST	Protocol yang digunakan *Hacker* dalam menginput username dan password
data.srcip	34.217.209.216	IP Address penyerang / *Hacker*
data.url	//wp-login.php	Halaman yang digunakan untuk login pada website

Tabel 4.12 Penjelasan Metadata Log Rule id 31510 (Lanjutan)

Nama Metadata	Isi Metadata	Arti
decoder.name	web-accesslog	Decoder log untuk menerjemahkan log
full_log	34.217.209.216 - - [19/Jan/2022:08:45:18 +0700] "POST //wp-login.php HTTP/1.1" 200 10983 "https://law.uii.ac.id//wp-login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0 Safari/537.36"	Full log pada website yang diserang oleh *Hacker* kemudian di parse berbentuk kalimat oleh Wazuh
id	1642556718.11822210	Id logstash tempat log disimpan
input.type	log	Format yang diambil wazuh
decoder.name	web-accesslog	Decoder log untuk menerjemahkan log
location	/var/log/nginx/access.log	Lokasi tempat log diambil, yaitu pada server tempat website di-*hosting*
manager.name	wazuh-manager-worker-1	Wazuh manager yang digunakan untuk mengelola agen yang diregister
previous_output	34.217.209.216 - - [19/Jan/2022:08:45:16 +0700] "POST //wp-login.php HTTP/1.1" 200 10983 "https://law.uii.ac.id//wp-login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0	Log log yang mengindikasikan serangan *brute force.* Pada *log* ini dicatat bahwa sumber IP Address yang disebutkan diatas telah berusaha melakukan usaha untuk masuk ke Website dengan mencoba berbagai username dan password yang dimiliki. Dalam log yang dihasilkan oleh web

Tabel 4.12 Penjelasan Metadata Log Rule id 31510 (Lanjutan)

Nama Metadata	Isi Metadata	Arti
	Safari/537.36" 34.217.209.216 - - [19/Jan/2022:08:45:15 +0700] "POST //wp-login.php HTTP/1.1" 200 10983 "https://law.uii.ac.id//wp-login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0 Safari/537.36" 34.217.209.216 - - [19/Jan/2022:08:45:14 +0700] "POST //wp-login.php HTTP/1.1" 200 10983 "https://law.uii.ac.id//wp-login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0 Safari/537.36" 34.217.209.216 - - [19/Jan/2022:08:45:13 +0700] "POST //wp-login.php HTTP/1.1" 200 10983 "https://law.uii.ac.id//wp-login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0 Safari/537.36" 34.217.209.216 - - [19/Jan/2022:08:45:12 +0700] "POST //wp-login.php HTTP/1.1" 200 10983	Decoder log untuk menerjem server *nginx* tidak diperlihatkan username yang di *input*-kan oleh *Hacker*. Hal yang diperlihatkan adalah metode POST yang dilakukan oleh *Hacker* ketika meng-*input*-kan username dan password pada Website yang diserang.ahkan log

Tabel 4.12 Penjelasan Metadata Log Rule id 31510 (Lanjutan)

Nama Metadata	Isi Metadata	Arti
	"https://law.uii.ac.id//wp-login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0 Safari/537.36" 34.217.209.216 - - [19/Jan/2022:08:45:11 +0700] "POST //wp-login.php HTTP/1.1" 200 10983 "https://law.uii.ac.id//wp-login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0 Safari/537.36" 34.217.209.216 - - [19/Jan/2022:08:45:09 +0700] "POST //wp-login.php HTTP/1.1" 200 10983 Safari/537.36" 34.217.209.216 - - [19/Jan/2022:08:45:06 +0700] "POST //wp-login.php HTTP/1.1" 200 10983 "https://law.uii.ac.id//wp-login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0 Safari/537.36"	
rule.description	CMS (WordPress or Joomla) brute force attempt.	Deskripsi rule yang digunakan oleh Wazuh

Tabel 4.12 Penjelasan Metadata Log Rule id 31510 (Lanjutan)

Nama Metadata	Isi Metadata	Arti
rule.firedtimes	16	Jumlah rule id 31510 yang telah dihasilkan oleh Wazuh sesuai dengan serangan *Hacker* yang memiliki IP Address diatas
rule.frequency	60	Jumlah rule id 31509 yang dihasilkan oleh Wazuh sesuai dengan serangan *Hacker* yang memiliki IP Address diatas
rule.gdpr	IV_35.7.d, IV_32.2	Kode rule GDPR
rule.groups	web, appsec, attack	Rule grup yang dimiliki oleh Wazuh dan log ini masuk pada rule group sesuai value isi metadata log
rule.hippa	164.312.b	Kode rule Hippa
rule.id	31510	Rule id yang dimiliki oleh Wazuh dalam mengidentifikasi serangan *brute force* pada server. Rule id ini merupakan kelanjutan atau versi lebih tinggi dari Rule id 31509
rule.level	13	Rule level yang dimiliki oleh Wazuh dalam mengidentifikasi level kritis pada *log* yang dihasilkan Wazuh
rule.mail	true	Jika di set true maka akan mengirimkan alert atau notifikasi kepada email yang sudah di konfigurasi oleh Administrator
rule.mitre.id	T1110	Rule mitre id
rule.mitre.tactic	Credential Access	Rule mitre tactic
rule.mitre.technique	Brute Force	Nama rule mitre yang dimiliki oleh Wazuh

Tabel 4.12 Penjelasan Metadata Log Rule id 31510 (Lanjutan)

Nama Metadata	Isi Metadata	Arti
rule.nist_800_53	SA.11, SI.4, AU.14, AC.7	Rule Nist
rule.pci_dss	6.5, 11.4, 6.5.10, 10.2.4, 10.2.5	Rule Pci
rule.tsc	CC6.6, CC7.1, CC8.1, CC6.1, CC6.8, CC7.2, CC7.3	Rule Tsc
timestamp	Jan 19, 2022 @ 08:45:18.156	Waktu berakhirnya log / rule id yang dihasilkan oleh Wazuh .

Metadata log yang dihasilkan diatas dicatat semuanya berdasarkan **Gambar 4.35** yang Wazuh hasilkan. Meskipun ada beberapa metadata log yang tidak dapat membantu banyak dalam proses analisis penelitian. Adapun hal yang ditampilkan pada **Tabel 4.12** merupakan informasi metadata log yang akan menjadi fokus dalam proses analisis penelitian dikarenakan menyangkut dengan tema penelitian yaitu analisis web-server.

Dalam rangka mendapatkan pengetahuan dan informasi baru berdasarkan Metadata log pada **Tabel 4.12** dilakukan penyusutan analisis metadata. Adapun metadata yang sangat membantu dalam proses analisis adalah metadata berikut :

A. GeoLocation.city_name
B. GeoLocation.country_name
C. GeoLocation.location
D. GeoLocation.region_name
E. data.srcip
F. full_log
G. previous_output
H. rule.firedtimes
I. rule.frequency
J. timestamp

Penjelasan mengenai 10 metadata tersebut dalam membantu penelitian adalah sebagai berikut :

A. Pada poin A hingga D menyatakan *GeoLocation* yang mengartikan sebuah lokasi geologi atau dapat dikatakan sebagai lokasi dimana penyerang/*Hacker* melakukan aksinya.
B. Poin E yang menyatakan *data.srcip* merupakan *data.sourceip* yang berarti IP

milik *Hacker* ketika melakukan tindakan serangan *brute force.*

C. Pada poin F yang menyatakan *full_log* merupakan hasil *log* yang di-*generate* oleh **Rule id 31510**, meskipun demikian *log* ini tidak berbeda dan memiliki struktur yang sama dengan log **Rule id 31509**.
D. Kemudian pada poin G yang menyatakan *previous_output* merupakan kumpulan *log* **Rule id 31509** yang berjumlah lebih dari 1 (sesuai frekuensi yang ditentukan pada local_rules.xml) untuk menyatakan bahwa dari sekian *log* **Rule id 31509** itu telah men-*trigger log* **Rule id 31510**.
E. Selanjutnya poin H yang menyatakan *rule.firedtimes* merupakan jumlah *log* **Rule id 31510** yang di-*generate* oleh wazuh ada sekian jumlah, contoh *log* pada **Gambar 4.x** merupakan salah satu dari *log* tersebut.
F. Sedangkan pada poin I yang menyatakan *rule.frequency* merupakan jumlah *log* **Rule id 31509** yang telah di-*generate* oleh Wazuh sebelum kemudian men-*trigger log* **Rule id 31510**.
G. Poin terakhir yaitu J yang menyatakan *timestamp* merupakan waktu berakhirnya log serangan ini sesuai dengan **Gambar 4.35**.

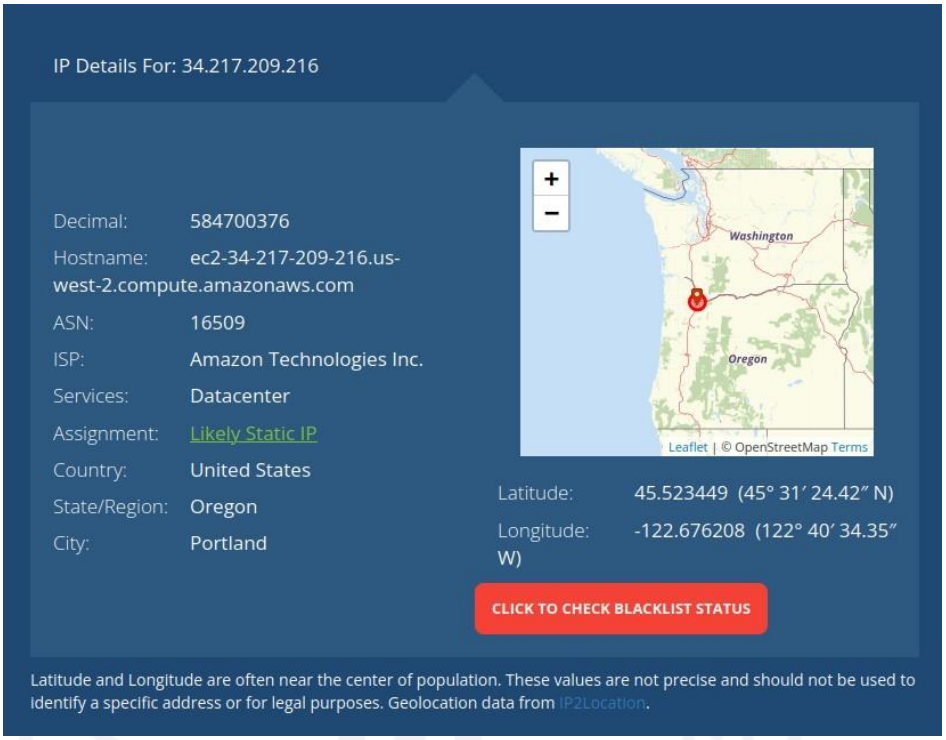
4.2.6 Laporan Hasil Analisis Klaster Kedua

Laporan dari hasil analisis pada klaster kedua menunjukkan bahwa tingkat serangan *brute force* pada website yang sudah lama ada dan dikenal dilancarkan oleh hacker dengan sasaran website tersebut alih-alih server tempat website tersebut di-*hosting*. Tidak terlihat indikasi bahwa *hacker* telah masuk ke dalam server. Maka dari itu proses analisis terhadap log *auditd* tidak dilakukan/dilewati

Berdasarkan hasil sub-bab analisis diatas maka proses analisis **Tabel 4.12** dapat dilakukan. Adapun hasil analisis yang telah dilakukan adalah sebagai berikut :

A. Isi dari metadata GeoLocation menyatakan bahwa serangan yang dilakukan oleh *Hacker* berasal dari kota Boardman, Negara bagian Oregon, Negara Amerika Serikat. Hal ini dapat dibuktikan dengan menggunakan penelusuran IP Address penyerang yang akan dijelaskan pada poin selanjutnya. Meskipun Wazuh telah mengkonfirmasi hingga lokasi Kota namun hanya sejauh ini saja kemampuan Wazuh dalam mendeteksi lokasi penyerang/*Hacker*, sisanya harus ditelusuri sendiri menggunakan aplikasi maupun alat lainnya. Hal ini akan dibahas pada poin selanjutnya yaitu poin B.
B. Metadata selanjutnya adalah *data.srcip* menyatakan bahwa sumber IP Address

dari *Hacker* adalah 34.217.209.216. Informasi ini sangat berguna untuk melakukan pelacakan sumber dari mana IP Address tersebut berasal, apakah valid dengan metadata GeoLocation berikan. Dalam membantu pelacakan ip ini digunakan website https://whatismyipaddress.com. Pada **Gambar 4.35** merupakan hasil pencarian IP Address menggunakan website tersebut :



Gambar 4. 35 Lokasi *Hacker* melancarkan serangan

Terlihat bahwa IP Address yang menunjukkan lokasi yang sesuai dengan metadata GeoLocation. Namun informasi ini hanya terbatas hingga sampai disini saja, untuk titik lokasi pasti *Hacker* belum dapat dilacak hingga presisi pasti. Hal lain yang ditemukan ialah kebanyakan penyerang biasanya menggunakan server VPN untuk lebih menyamarkan diri lagi. Selain hal tersebut informasi data source IP Address yang diberikan Wazuh juga ditemukan ada yang berbeda dengan GeoLocation yang diberikan.

C. Metadata selanjutnya adalah *full_log* menyatakan bahwa IP Address yang sama dengan metadata *data.srcip* menyerang website law.uii.ac.id menggunakan metode POST pada halaman /wp-login.php. Informasi yang didapat kali ini merupakan metode *brute force* yang digunakan oleh *Hacker* untuk memasuki website. Adapun hal yang dilakukan oleh *Hacker* adalah mencoba setiap kombinasi yang ada baik itu username dan password pada halaman https://law.uii.ac.id/wp-login.php yang mana halaman tersebut merupakan

halaman default untuk masuk ke bagian Administrator pada website yang berbasis wordpress. Tidak ditemukan kredensial yang digunakan *Hacker* untuk masuk ke website baik itu username maupun password. Pada *full_log* metadata log nginx berbeda dengan metadata log ssh yang menunjukkan kredensial username yang digunakan untuk masuk ke server.

D. Metadata selanjutnya adalah *previous_log* merupakan kumpulan *log* yang isinya sama dengan metadata *full_log*, namun berjumlah banyak serta dalam kurun waktu singkat antara satu log dengan log lainnya. Sehingga dari kumpulan log yang banyak serta memiliki tempo waktu yang singkat itulah kemudian me-*trigger* **Rule id 31510**. Meskipun isinya sama namun hal yang membedakan adalah Rule id yang me-*trigger* Wazuh. Pada metadata *previous_log* juga tidak ditemukan kredensial yang digunakan penyerang untuk melakukan usaha login ke website.
E. Metadata berikutnya adalah *rule.firedtimes* merupakan indikasi mengenai log pada **Rule id 31510** ini telah ter-generate berapa kali berdasarkan metadata *frequency*. Biasanya pada bagian atas dan bawah *log* ini merupakan isi *log* yang sama. Hal yang membedakan ialah pada metadata *timestamp* yang berjarak beberapa detik. Jumlah log yang ter-*generate* ada 13 *log*.
F. Metadata selanjutnya ialah *rule.frequency* merupakan jumlah *log* pada **Rule id 31509** ini harus ter-*generate* berapa kali hingga dapat men-*trigger* **Rule id 31510**. Pada contoh analisis yang diberikan menunjukkan bahwa **Rule id 31509** haruslah berjumlah 60 sebelum akhirnya meng-*trigger* **Rule id 31510** sebanyak 1 kali.
G. Metadata terakhir merupakan *timestamp* ialah metadata yang menunjukkan berakhirnya suatu log setelah ter-*trigger* atau ter-*generate.* Pada penelitian ini waktu selesainya log adalah pada tanggal 19 Januari tahun 2022 pukul 8 menit ke 45 dan detik ke 18.

4.3. Perbedaan Hasil Analisis Klaster Pertama dan Klaster Kedua

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

Tabel 4.14 Perbedaan Hasil Analisis Kedua Klaster

Parameter Perbandingan	Klaster Pertama	Klaster Kedua
Informasi Serangan *Bruteforce*	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*
Tujuan Serangan *Bruteforce*	5 website yang baru dibuat pada akhir Maret 2022	5 website yang dikelola BSI UII
Intensitas Serangan	Serangan yang dilakukan beberapa hari sekali	Serangan dilakukan setiap hari
Analisis Metadata *Log*	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
Rule Id	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
Anomali *Log*	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
Usia Website	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’

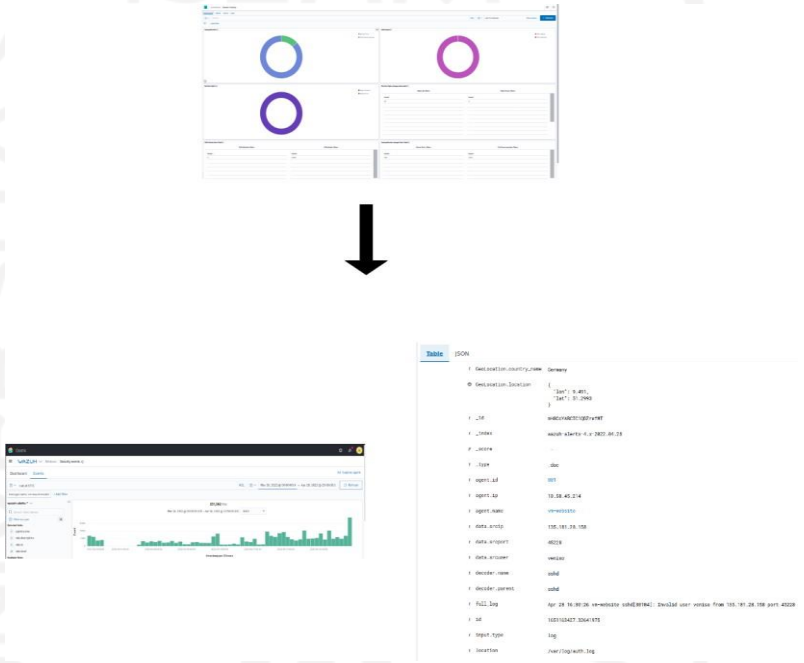
4.4. Hasil Analisis Penelitian Terbaru dengan Penelitian Sebelumnya

Hasil analisis kedua penelitian yang ada pada sub bab 1 Rumusan Masalah diuraikan sebagai berikut :

a. Penelitian terbaru yang dilakukan terbukti memberikan hasil analisis serangan *bruteforce* yang lebih informatif dibandingkan pada penelitian sebelumnya. Hal ini berdasarkan penjelasan pada uraian sub **bab 4.2** dan **sub bab 4.3** Wazuh memberikan penjelasan *log* yang lebih detail dibandingkan dasbor sebelumnya. Sehingga hasil

analisis pada dasbor sistem pencatatan log teroptimasi telah memberikan informasi yang informatif kepada Administrator/SysAdmin.

b. Informasi log yang diberikan ini juga di dukung pada pada uraian **sub bab 4.2** serta **Gambar 4.36** dibawah. Gambar tersebut menunjukkan informasi log yang dihasilkan dasbor penelitian baru lebih kaya dan informatif dibandingkan dengan dasbor penelitian lama sedangkan uraian pada **sub bab 4.2** membantu penjelasan informasi mengenai *log* yang dihasilkan dasbor teroptimasi. Sehingga dapat diambil kesimpulan bahwa dasbor penelitian baru memberikan informasi yang informatif pada Administrator/SysAdmin dibandingkan dengan dasbor penelitian sebelumnya.



Gambar 4.36 Perubahan Dasbor Yang Dilakukan

c. Wazuh dapat menjadi opsi yang digunakan dalam membangun Centralized Log Management. Hal ini didasari dengan kemampuan Wazuh dalam mengolah log yang tadinya tidak beraturan dan sulit dibaca menjadi sebuah informasi yang mudah dibaca dan dipahami oleh Administrator/. Tujuan untuk mengoptimasi dasbor juga telah tercapai dengan menggunakan *tools* Wazuh. Hasil yang didapatkan ditujukan pada uraian yang telah dijelaskan pada **bab 4** dengan menganalisis 2 klaster yang berbeda menunjukkan peningkatan informasi yang diberikan Wazuh jauh lebih informatif dibandingkan dasbor penelitian sebelumnya yang hanya menggunakan EFK Stack. Sehingga dapat dikatakan bahwa proses penelitian yang telah dilakukan sejalan dengan penelitian sebelumnya dengan proses optimasi yang dilakukan memperoleh hasil yang lebih baik.

BAB 5
KESIMPULAN DAN SARAN

5.1. Kesimpulan

Kesimpulan yang dapat diambil berdasarkan hasil analisis yang telah dilakukan yaitu :

a. Dasbor Sistem Pencatatan Log Teroptimasi dapat memberikan informasi yang informatif mengenai serangan *bruteforce* kepada Administrator, SysAdmin maupun User yang menggunakan Dasbor Sistem ini. Hal ini terbukti dengan informasi yang diberikan *log* Wazuh berdasarkan **Rule id 5710, 5712, 31509**, dan **31510** serta penjelasan yang sudah dipaparkan pada **bab 4**.
b. Dasbor Sistem Pencatatan Log Teroptimasi juga memberikan informasi yang lebih informatif dibandingkan dengan Dasbor Sistem penelitian sebelumnya. Hal tersebut berkat bantuan add-ons Wazuh yang dapat memberikan visualisasi yang informatif.
c. Wazuh juga berkontribusi dalam pengembangan Dasbor Sistem Pencatatan Log Teroptimasi dan terbukti layak dan berguna dalam pengembangan CLM (*Centralized Log Management*) dilihat dari hasil informasi *log* yang ter-*generate* memberikan informasi tulisan yang mudah dipahami.

Analisis forensik didapatkan pengetahuan baru bahwa serangan yang dilakukan oleh *Hacker* tidak selamanya dilakukan secara berkelanjutan. Terdapat keadaan dimana *Hacker* berhenti menyerang dan tidak melanjutkan serangan *brute force.* Kemudian ketika diteliti lebih lanjut dengan memperhatikan IP Address yang sama menunjukkan bahwa *Hacker* telah berhenti menyerang dan tidak lagi ditujukan ke website manapun. Namun tidak semua IP Address yang di-*generate* Wazuh menunjukkan hasil yang akurat, beberapa menunjukkan hasil lokasi yang berbeda. Seperti hasil *log* menunjukkan lokasi Negara Amerika Serikat, namun setelah ditelusuri ternyata lokasi server terdapat di Negara India.

5.2. Saran

Terdapat beberapa saran yang dapat dilakukan pada penelitian selanjutnya, yaitu :

1. Mengusulkan metode baru dengan irisan keilmuan mengenai investigasi forensik dan *cyber security* atau metode investigasi forensic yang berbeda.
2. Membandingkan *tools* wazuh dengan *tools security* lainnya, seperti Datadog, Ossec, Graylog, Splunk, Security Onion, dan lain lain.
3. Menambahkan *tools* untuk melacak IP Address yang diberikan Wazuh sehingga lokasi dari penyerang dapat dilacak seakurat mungkin.

Daftar Pustaka

A. P. Atmaja and F. Susanto, "Optimasi aplikasi Simak-BMN untuk Inventarisasi Barang milik Negara Berbasis aplikasi mobile android," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 6, no. 2, p. 201, 2019.

Castro, s. P. (2020, Mei 19). *wazuh-ruleset*. Diambil kembali dari github.com: https://github.com/wazuh/wazuh-ruleset/blob/master/rules/0095-sshd_rules.xml ; https://github.com/wazuh/wazuh-ruleset/blob/master/rules/0270-web_appsec_rules.xml

Contributor, T. (2016, September). *Definition Elastic Stack*. Diambil kembali dari TechTarget Search ITOperations: https://searchitoperations.techtarget.com/definition/Elastic-Stack

C.-K. Tsung, C.-T. Yang, and S.-W. Yang, "Visualizing Potential Transportation Demand from ETC log analysis using Elk Stack," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6623–6633, 2020.

Eka Wahyu Hidayat, A. R. (2015). Optimasi Server SIMAK Menggunakan Memcached dan Mirror Server Untuk Meningkatkan Kecepatan Akses Layanan Akademik Universitas Siliwangi. *Jurnal Ilmu Komputer dan Ilmu Sains Terapan*, 63-135.

Elastic. (2022, January 27). *Filebeat*. Diambil kembali dari Elastic.co: https://www.elastic.co/beats/filebeat

Elastic. (2022, January 27). *Logstash*. Diambil kembali dari Elastic.co: https://www.elastic.co/logstash/

Elastic. (2022, Januari 27). *What is Elasticsearch?* Diambil kembali dari Elastic.co: elastic.co/what-is/elasticsearch

Elastic. (2022, January 27). *What is Kibana*. Diambil kembali dari Elastic.co: https://www.elastic.co/what-is/kibana

Erwinsyah, Y. B. (2019). *KONSOLIDASI DAN VISUALISASI LOG SERVER BSI UII MENGGUNAKAN ELK STACK*. Yogyakarta: dspace.uii.ac.id.

I Putu Agus Eka Pratama, I. G. (2019). OPTIMASI RADIUS SERVER UNTUK PENGATURAN ALOKASI BANDWIDTH PADA JARINGAN HOTSPOT. *Jurnal Sains dan Sistem Informasi*, 18-24.

I. Y. Al-Mahbashi, M. B. Potdar, and P. Chauhan, "Network security enhancement through effective log analysis using Elk," *2017 International Conference on Computing Methodologies and Communication (ICCMC)*, 2017.

J.- Jefi, A. M. Joddy, and K. Solecha, "OPTIMASI Sistem Informasi Penggajian Karyawan Berbasis website," *Jurnal Infortech*, vol. 2, no. 2, pp. 184–189, 2020.

K. W. Mahardika, "Optimasi K-Nearest Neighbour Menggunakan Particle Swarm Optimization Pada Sistem Pakar Untuk Monitoring Pengendalian Hama Pada Tanaman Jeruk," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 02, no. 09, pp. 3333–3344, Feb. 2018.

Kurniawan, M. F. (2020). *Optimasi Server Live Streaming Menggunakan Microservices dan Load Balancer*. Malang: Universitas Islam Negeri Maulana Malik Ibrahim Malang.

Lintang, D. (2020). *Monitoring Aktivitas User pada System dengan Menggunakan EFK (Elasticsearch, Fluentd, Kibana) Stack.* Yogyakarta: dspace.uii.ac.id.

M. N. Arifin, Sugiartowo, and Emisusilowati, "DESAIN DAN IMPLEMENTASI LOG EVENT MANAGEMENT SERVER MENGGUNAKAN ELASTICSEARCH LOGSTASH KIBANA (ELK STACK)," *Prosiding SEMNASTEK Fakultas Teknik Universitas Muhammadiyah Jakarta*, pp. 1–7, Oct. 2018.

M. Setiawan, E. Endryansyah, S. Haryudo, and A. Agung, "Optimasi Sistem Monitoring Penghitung Produk Gula dengan Menggunakan SCADA Berbasis Distributed Control System (DCS)", *JTE*, vol. 11, no. 3, pp. 463-470, Sep. 2022.

N. K. Sumiari and N. K. Ari Jayanti, "Optimasi Dashboard Information system Stikom Bali dengan algoritma levenshtein distance," *Creative Information Technology Journal*, vol. 6, no. 1, p. 12, 2020.

Walidatush Sholihah, S. A. (2020). Log Event Management Server Menggunakan Elastic Search Logstash Kibana(ELK Stack). *Jurnal Teknologi Informasi dan Multimedia*, 12-20.

Wazuh. (2022, January 27). *The Open Source Security Platform*. Diambil kembali dari wazuh.com: https://wazuh.com/

Wikipedia. (2022, January 27). *Logging (software)*. Diambil kembali dari wikipedia.org: https://en.wikipedia.org/wiki/Logging_(software)