L1 SOC ANALYST

Modul Praktikum 4

Menganalisis Log pada Security Operations Center (SOC)

J.62SOC00.011.1

MODUL PRAKTIKUM L1 SOC ANALYST

Unit Kompetensi

Menganalisis Log pada *Security Operations Center* (SOC)

Tujuan Praktikum

1. Mengakses Lokasi Penyimpanan Log
2. Menganalisis Apache Log Access
3. Mengoperasikan Wazuh

Mengakses dan Menganalisis Log Apache (P.11.1.A, P.11.1.B)

Skenario Praktikum

Anda adalah seorang *L1 SOC Analyst* yang bekerja di Pemerintah Daerah Kabupaten Lengkeng. Anda memiliki tugas untuk mengawasi dan memantau seluruh aktivitas jaringan ke dalam infrastruktur TI Pemkab Lengkeng dengan bantuan SIEM. Meskipun anda dapat menggunakan SIEM dalam menganalisis log, sebagai seorang L1 SOC Analyst anda tetap harus mampu menganalisis log tanpa bantuan SIEM agar familiar dengan berbagai jenis log.

Tujuan Praktikum

Praktikum ini bertujuan untuk membantu perserta didik dalam mengakses dan menganalisis log pada Ubuntu Server

Enviroment Laboratorium Virtual

Praktikum ini membutuhkan:

- VM Kali Linux
- VM Target Web 1.

Durasi Praktikum

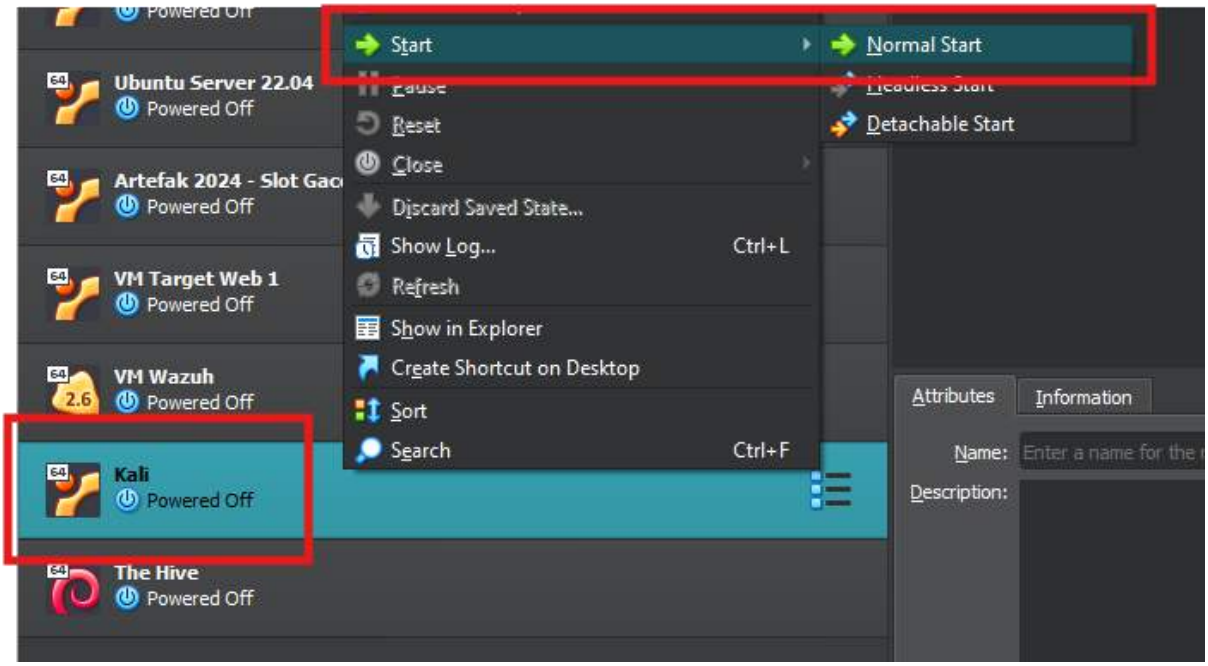
10 Menit

Catatan Khusus

- Siapkan *enviroment* laboratorium virtual sesuai panduan installasi laboratorium virtual
- Dokumentasikan setiap langkah praktikum karena dapat membantu menjawab pertanyaan pada soal yang diberikan

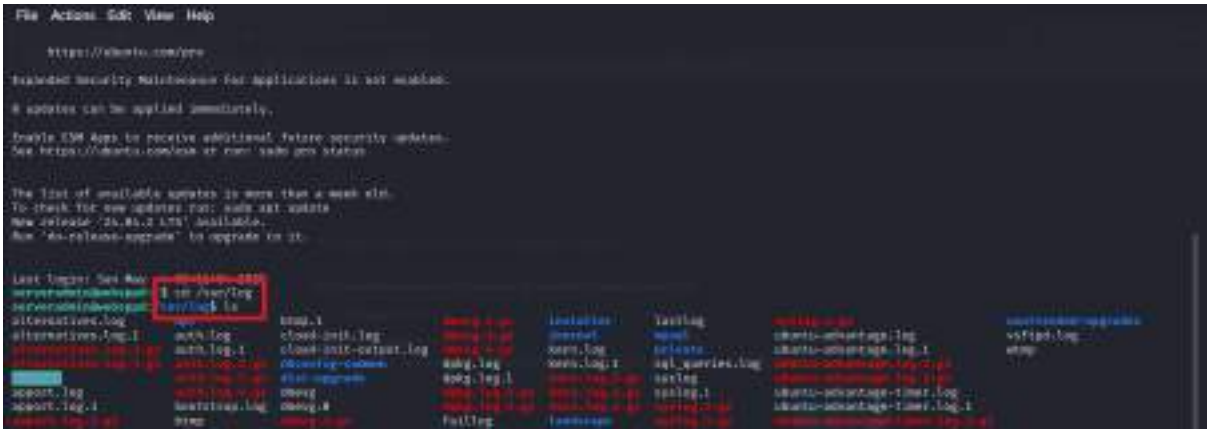
Langkah-Langkah

1. Siapkan Virtualbox, nyalakan VM Web Target 1 dan VM Desktop yang dapat mengakses *browser*, pada contoh kali ini menggunakan dekstop Kali Linux

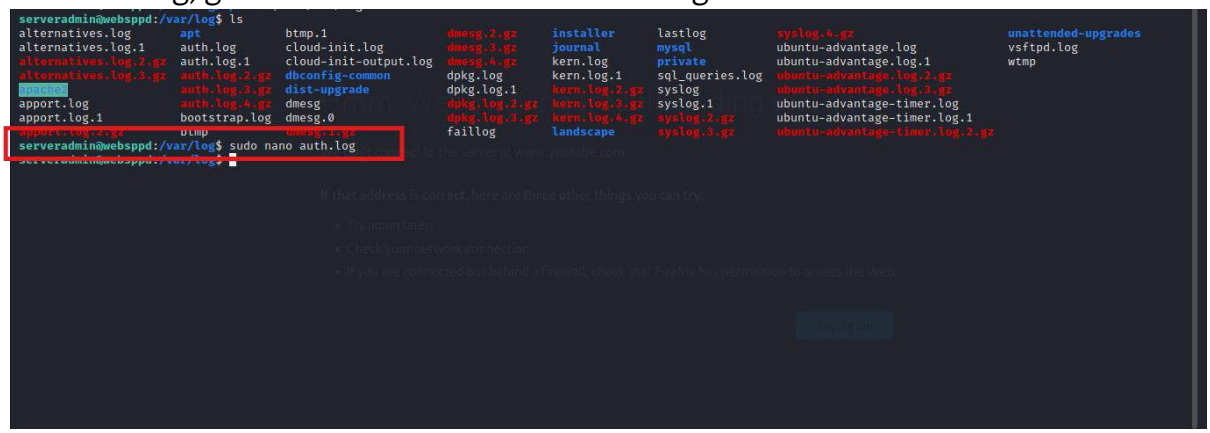


2. Lakukan hal yang sama pada VM Target Web 1
3. Lakukan SSH pada VM Target Web 1 melalui kali dengan memasukan perintah `ssh serveradmin@10.0.11`

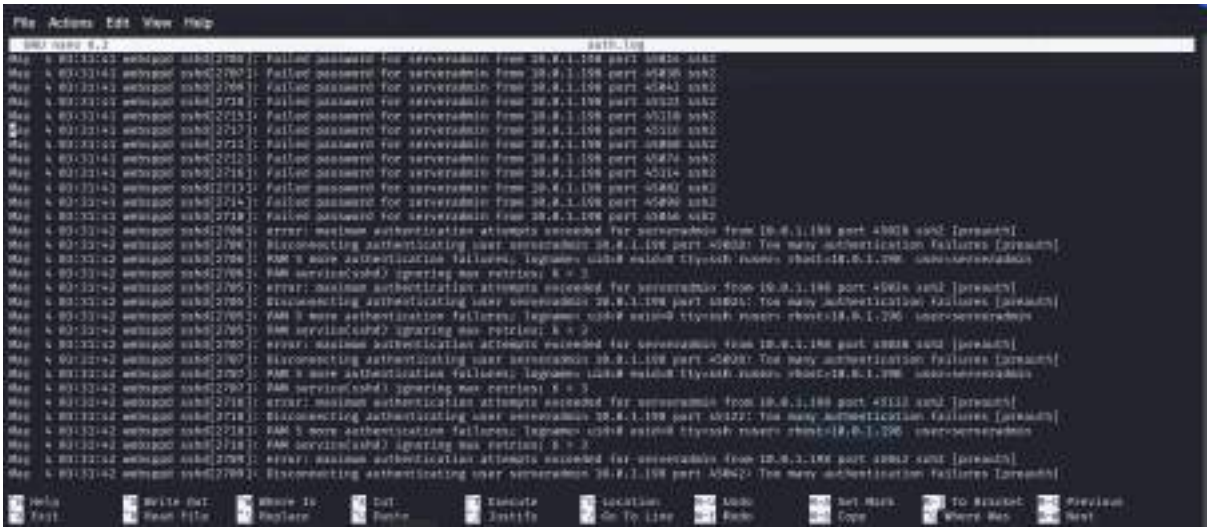
4. Log pada ubuntu server secara default akan disimpan pada /var/log, pindah direktori tersebut dan cek apa saja yang terdapat didalamnya dengan perintah `cd /var/log` dan `ls`.



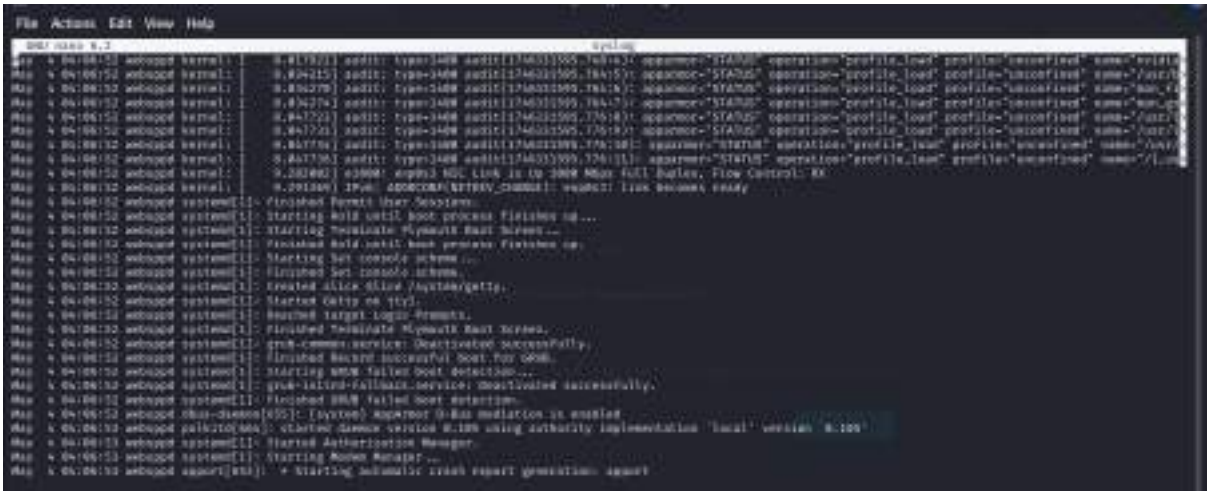
5. Akan terdapat banyak log, seperti auth.log berisi yang berisi log autentikasi, apache yang didalamnya banyak log dari layanan apache, dpkg.log berisi manajer paket debian, sql_queris.log berisi log query sql.
6. Terdapat log yang berekstensi .log dan .gz. Log yang berkestensi .gz merupakan file log lama yang sudah dikompres, bagian dari mekanisme log rotation di Linux.
7. Buka auth.log, gunakan berintah sudo nano auth.log



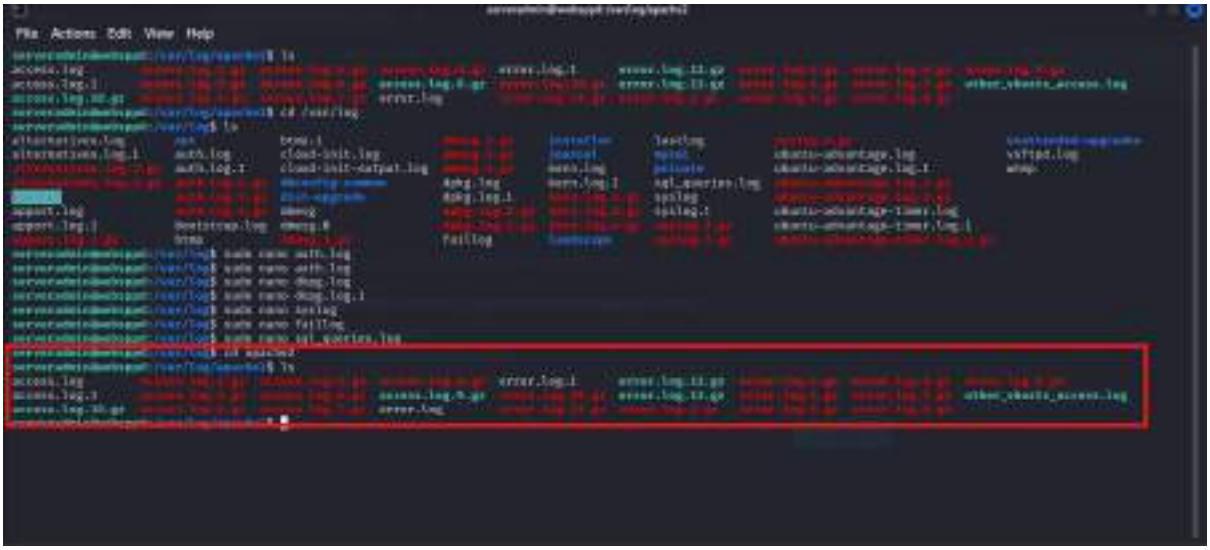
8. Pada auth.log dapat dilihat hari dan tanggal terjadinya autentikasi, hostname (websppd), aktivitas autentikasi (failed password for serveradmin from 10.0.1.198) yang berarti bahwa gagalnya upaya login menggunakan username serveradmin dari 10.0.1.198, layanan yang berusaha dimasuki merupakan ssh2.



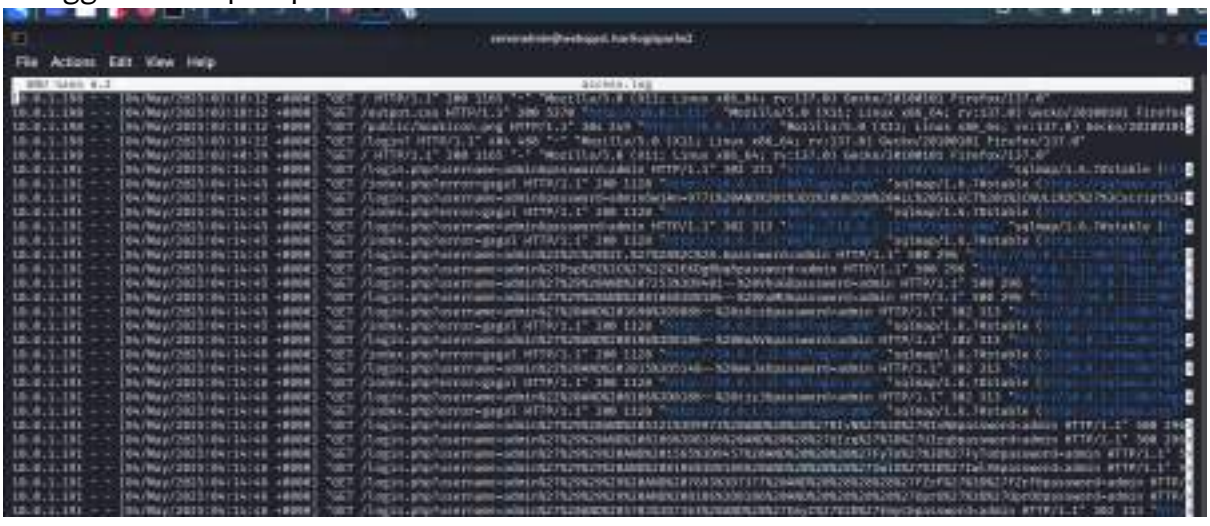
9. Buka syslog, log ini merupakan log utama di sistem Linux yang mencatat berbagai macam pesan sistem umum. Disini juga dapat dilihat dari mana log berasal seperti log yang berasal dari kernel yang mengatur hardware dan inti OS serta systemd yang mengatur service dan user.



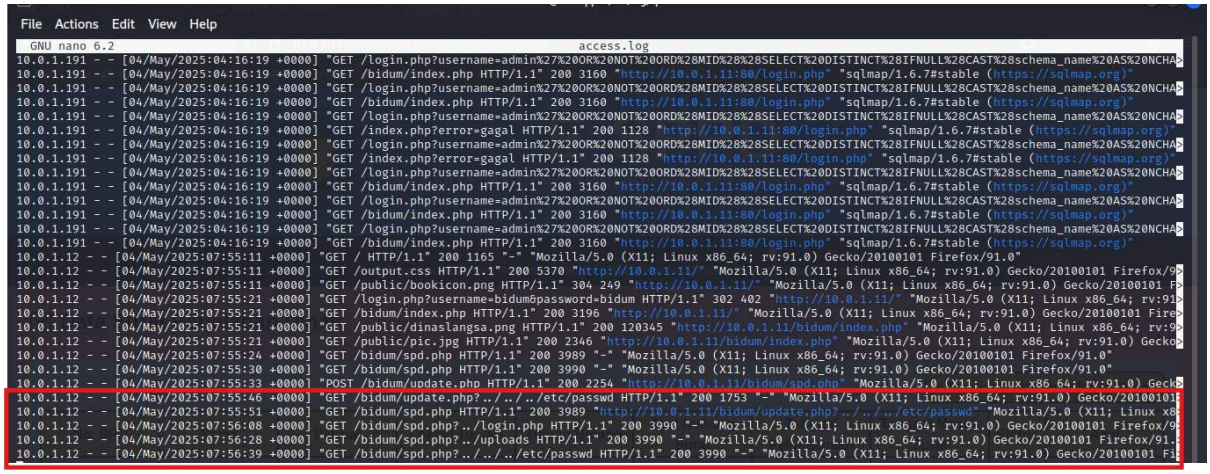
10. Masuk ke direktori lebih dalam yaitu apache2 dengan perintah `cd apache2`



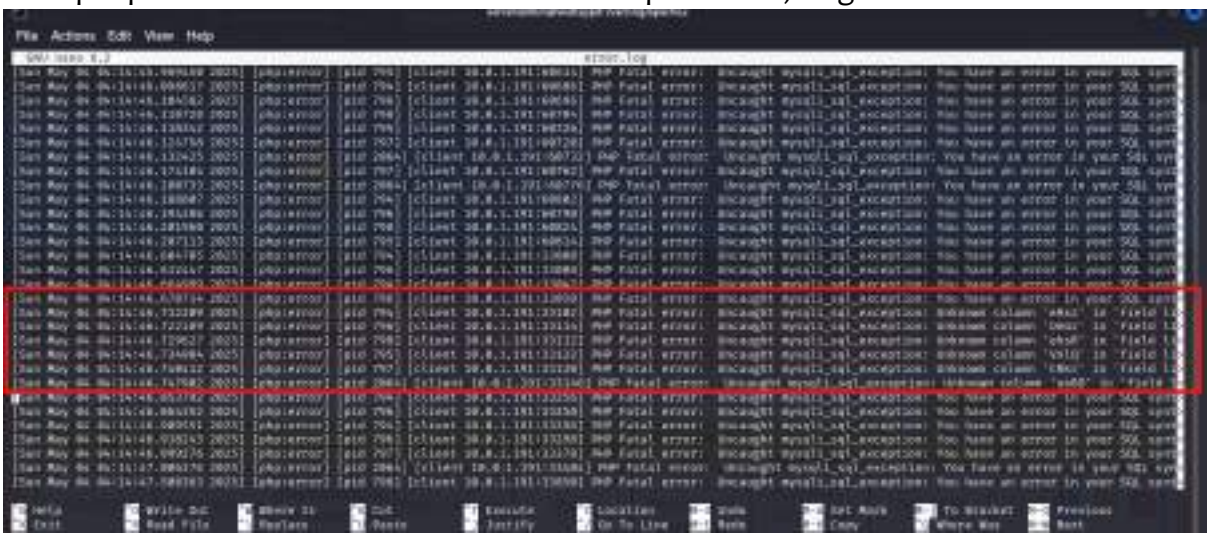
11. Buka access.log, log akan berisi permintaan akses pada web. Pada gambar dibawah ini dapat diketahui kandungan dari access.log diantaranya IP client, waktu permintaan akses, method yang digunakan, serta tautan serta response yang diberikan. Dibawah ini merupakan contoh log jika terjadi serangan sql injection menggunakan sql map.



12. Didalam access log anda juga dapat melihat adanya ujicoba path transversal



13. Anda juga harus mengecek error.log. File log ini akan mencatat terjadinya error pada web. Anda harus mengecek error.log dikarenakan biasanya penyerang tidak langsung berhasil dalam melakukan serangan dan terkadang terjadi error. Pada gambar dibawah ini contoh error yang disebabkan sql injection dikarenakan terdapat percobaan memasukan kolom aneh seperti eHxz, Oegr.



Mengoperasikan Wazuh (P.11.1.C)

Skenario Praktikum

Anda adalah seorang *L1 SOC Analyst* yang bekerja di Pemerintah Daerah Kabupaten Lengkeng. Anda memiliki tugas untuk mengawasi dan memantau seluruh aktivitas jaringan ke dalam infrastruktur TI Pemkab Lengkeng dengan bantuan SIEM. Instansi tempat anda bekerja menggunakan Wazuh sebagai SIEM. Dikarenakan operasional yang masif, jumlah *alert* yang dikelola oleh wazuh juga menjadi besar, oleh karena itu anda sebagai seorang *L1 SOC Analyst* harus terampil dalam mengoperasikan Wazuh dan mengetahui filter yang dapat digunakan dalam mempermudah tugas anda.

Tujuan Praktikum

Praktikum ini bertujuan untuk membantu perserta didik dalam mengoperasikan Wazuh

Enviroment Laboratorium Virtual

Praktikum ini membutuhkan:

- VM Kali Linux
- VM Wazuh

Durasi Praktikum

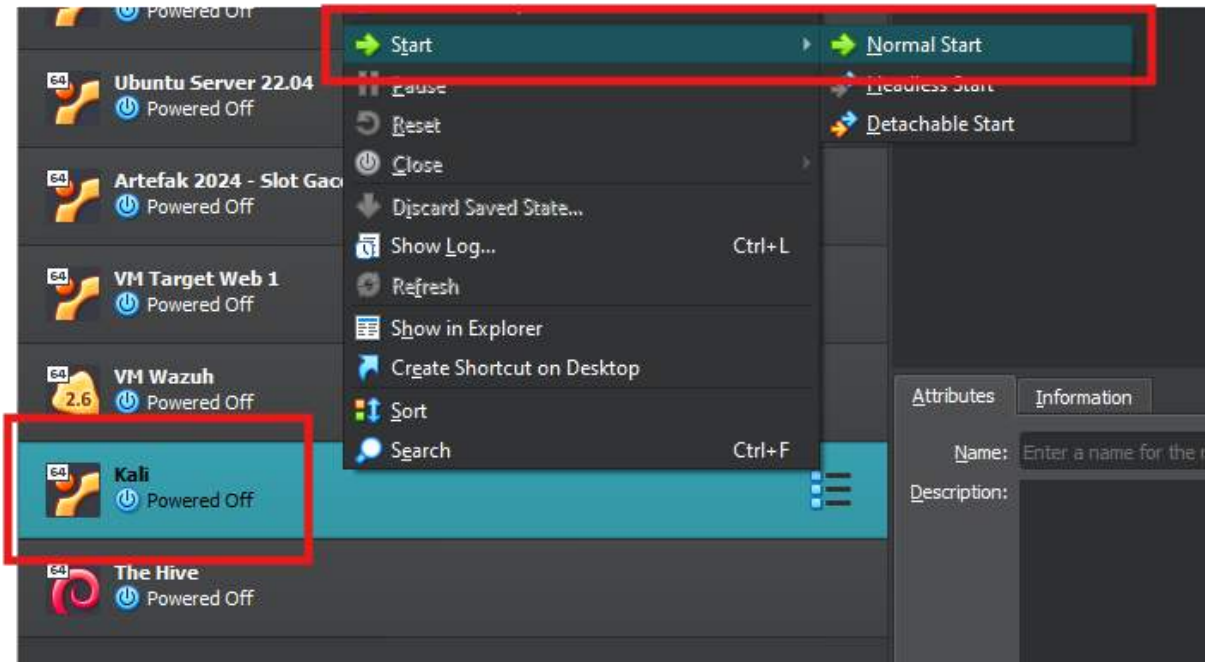
15 Menit

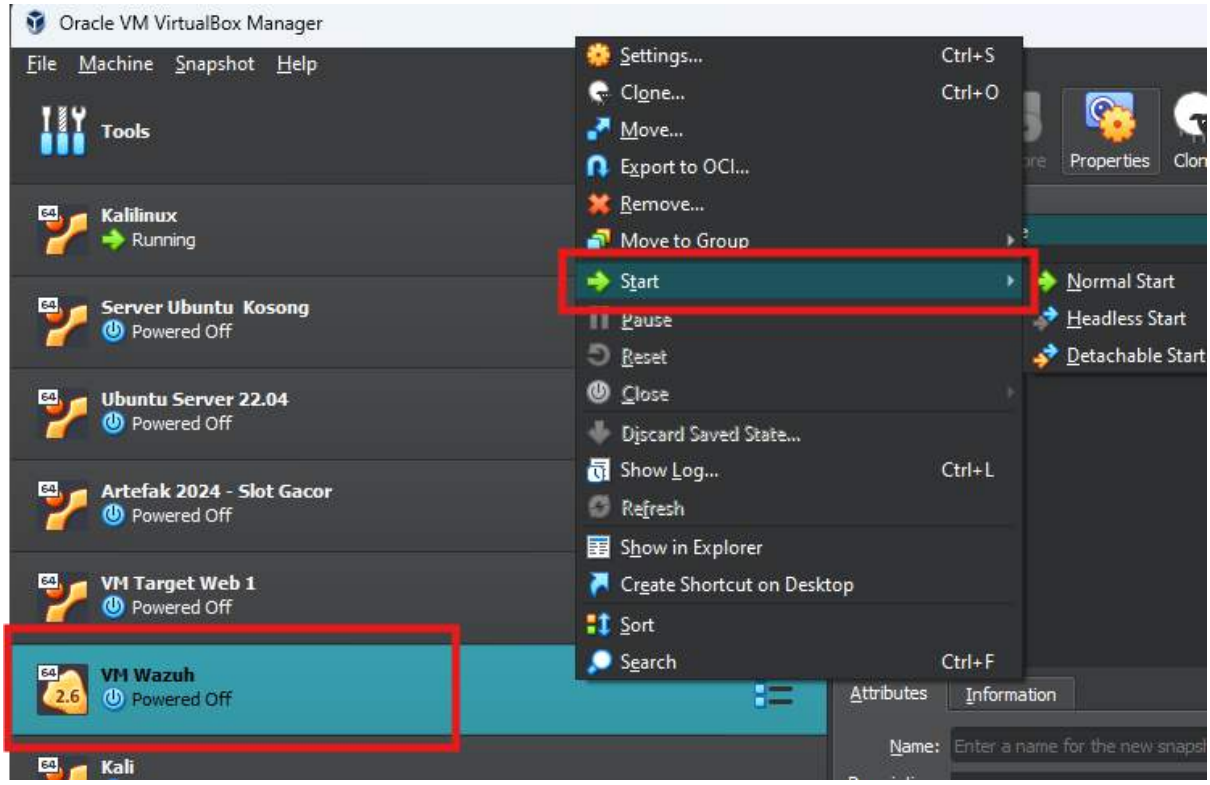
Catatan Khusus

- Siapkan *enviroment* laboratorium virtual sesuai panduan installasi laboratorium virtual
- Dokumentasikan setiap langkah praktikum karena dapat membantu menjawab pertanyaan pada soal yang diberikan

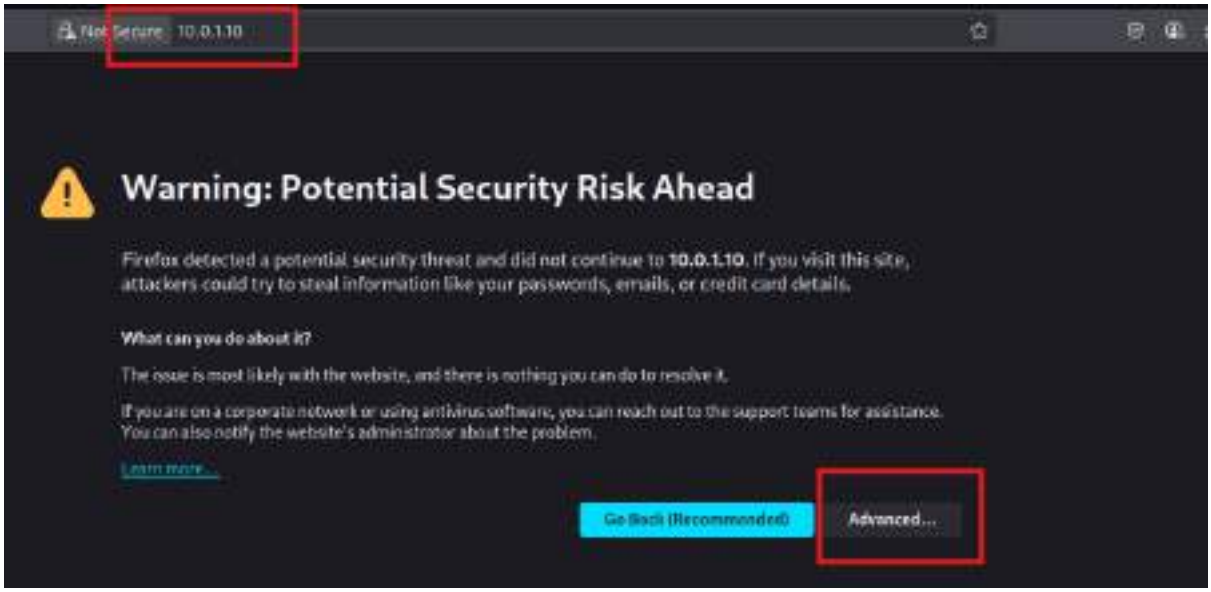
Langkah-Langkah

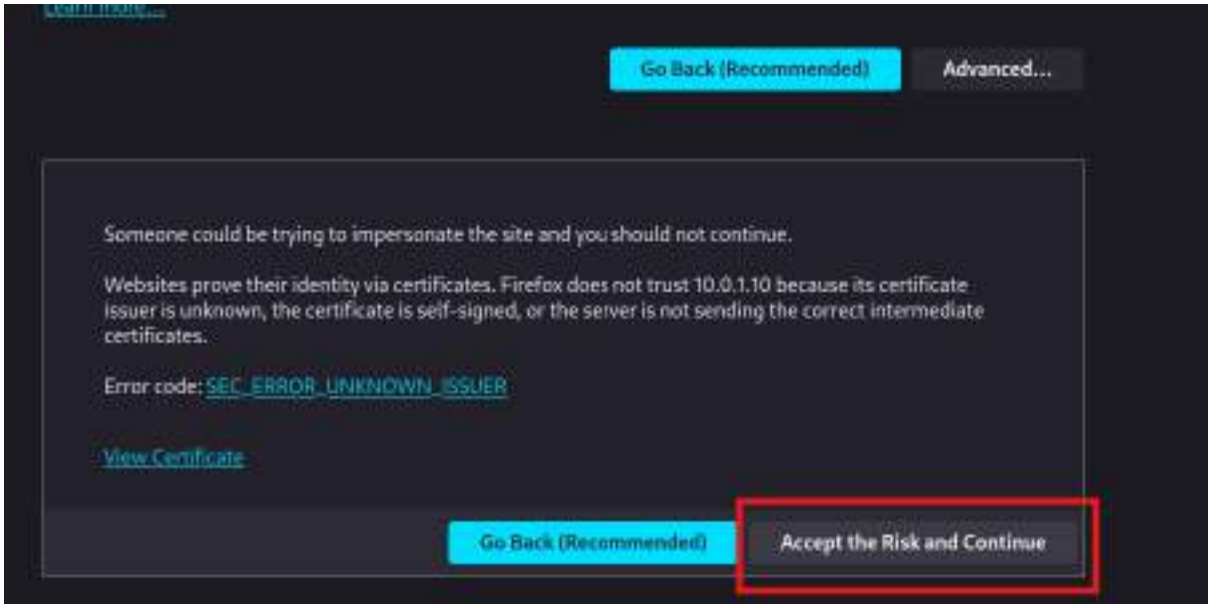
1. Siapkan Virtualbox, nyalakan VM Wazuh dan VM Desktop yang dapat mengakses *browser*, pada contoh kali ini menggunakan dekstop Kali Linux





2. Buka *browser* pada VM Dekstop, masukan IP VM Wazuh

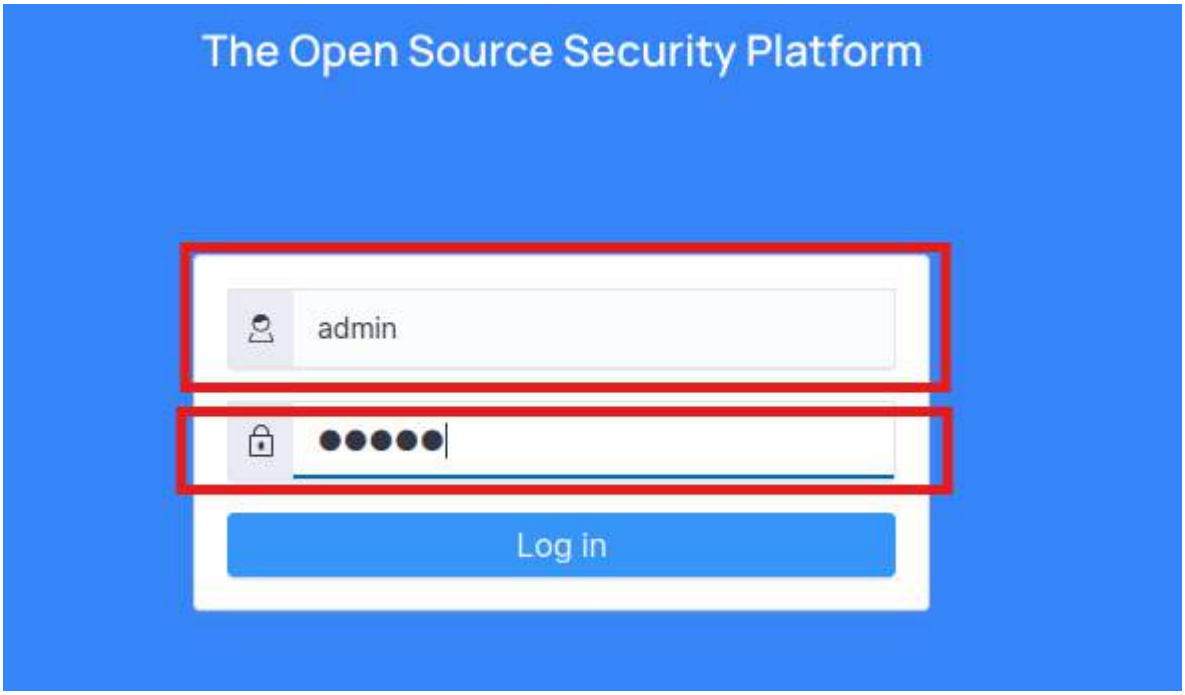




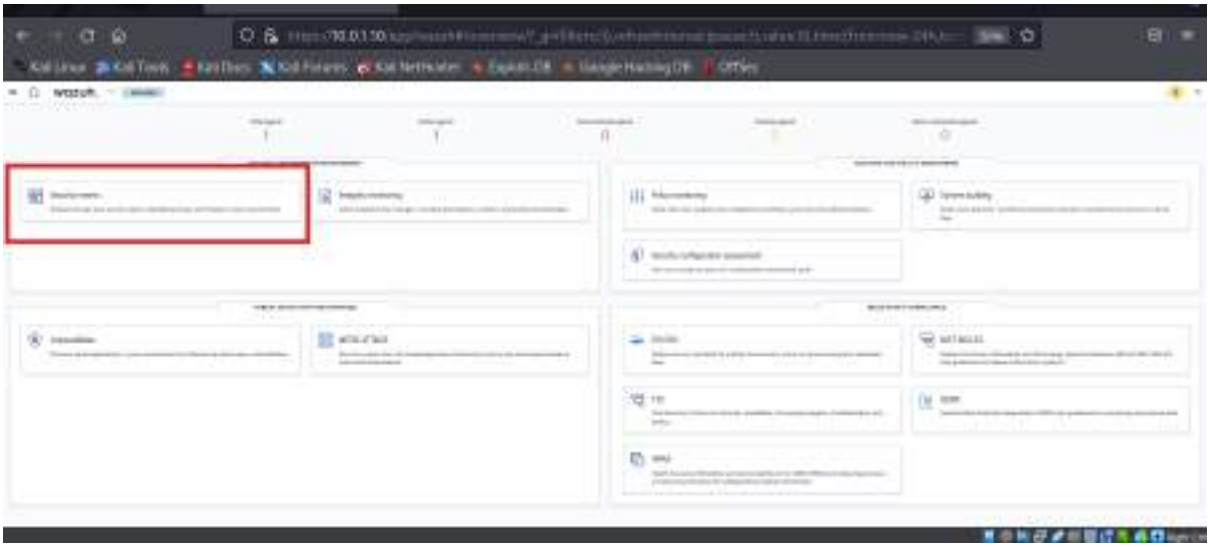
3. Jika tidak mengetahui IP VM Wazuh, dapat dilakukan dengan *login* ke VM Wazuh dengan kredensial *username* `wazuh-user` dan *password* `wazuh`. Cek ip VM dengan `IP A` atau `ifconfig`. Pastikan VM Dekstop yang anda gunakan dapat terkoneksi dengan IP VM Wazuh.

```
[wazuh-user@wazuh-server ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP gr
oup default qlen 1000
    link/ether 08:00:27:fa:c1:2b brd ff:ff:ff:ff:ff:ff
    inet 10.0.1.10/24 brd 10.0.1.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fefa:c12b/64 scope link
       valid_lft forever preferred_lft forever
[wazuh-user@wazuh-server ~]$
```

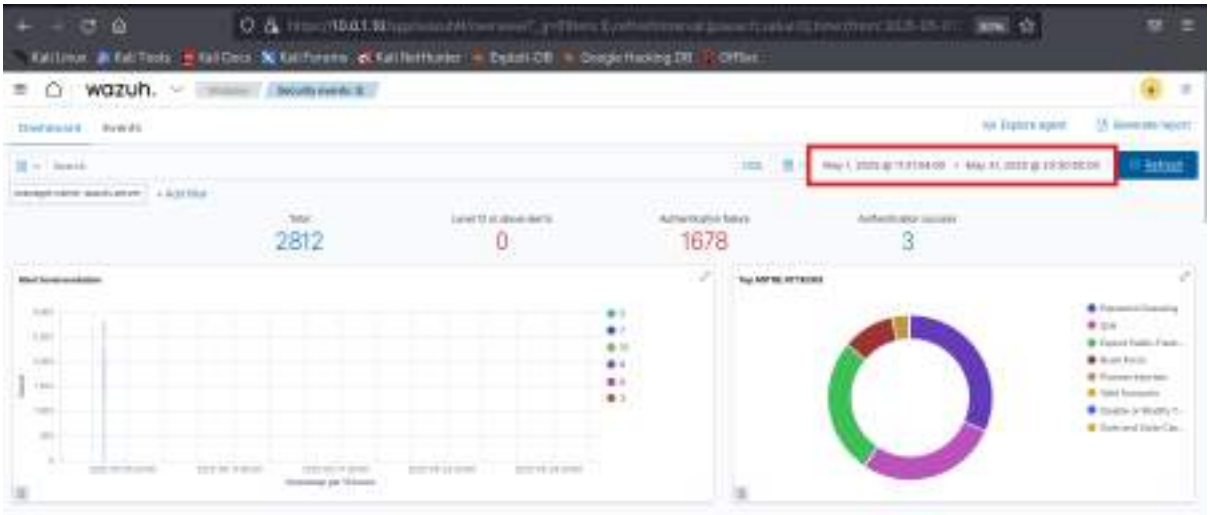
4. *Login* Wazuh Dashboard dengan kredensial *username* `admin` dan *password* `admin`



5. Tampilan Wazuh Dashboard akan seperti gambar dibawah, untuk melakukan pemantaun terhadap aset yang anda miliki, tekan Security Event. Modul Security Event akan menampilkan aktivitas yang berhubungan dengan keamanan pada aset yang anda awasi.

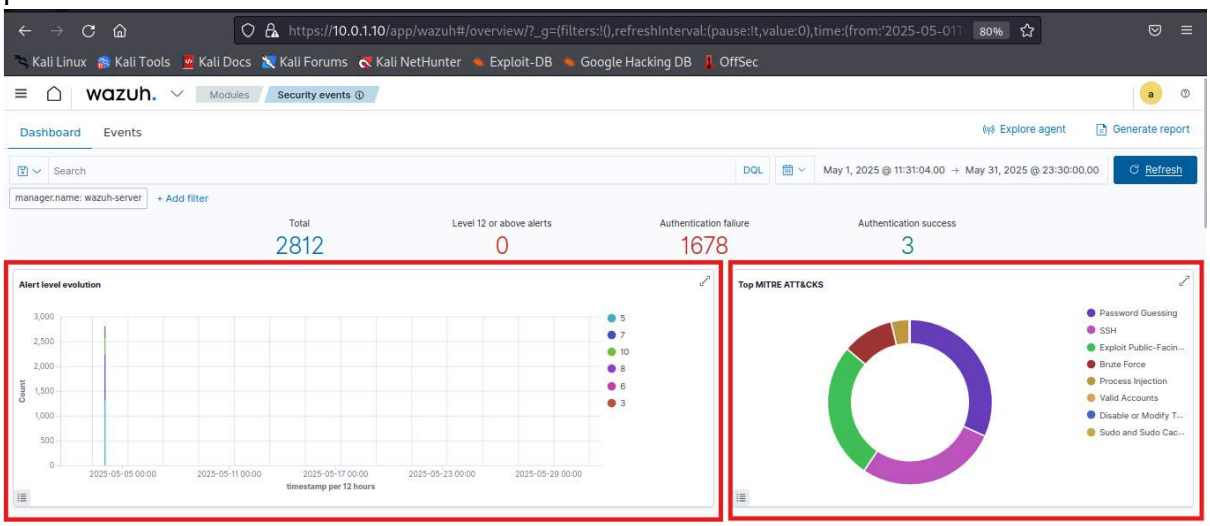


6. Pastikan alert yang ditampilkan sesuai dengan waktu yang dituliskan dalam skenario



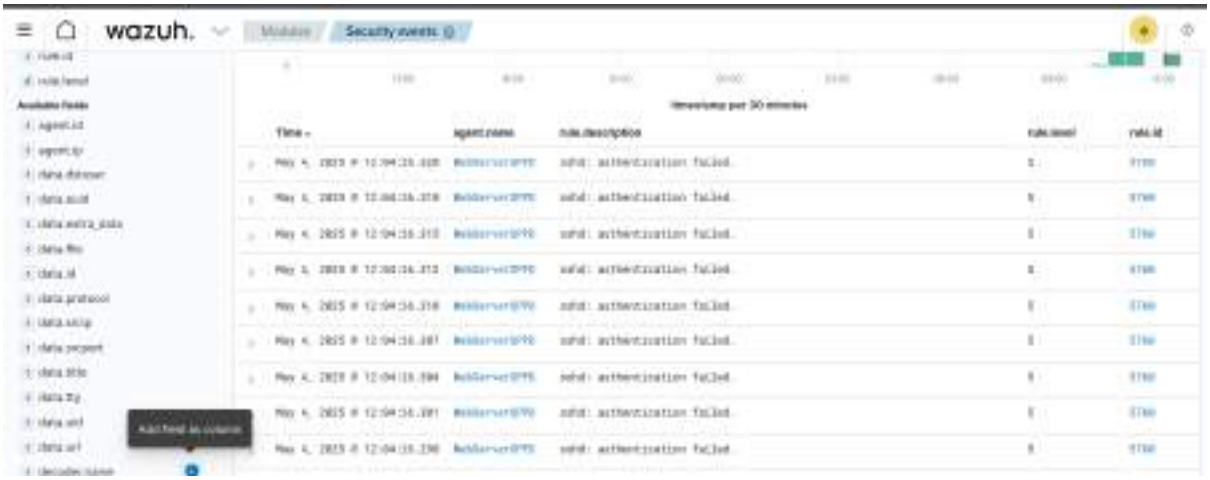
7. Grafik pada dashboard dapat memberikan gambaran umum mengenai aktivitas apa saya yang terjadi pada kurun waktu tertentu. Total merupakan jumlah alert yang ada, pada kasus ini terdapat 2812 alert, Level 12 or above alerts merupakan jumlah alert yang memiliki level diatas 12. Authentication failure menunjukan jumlah autentikasi yang gagal pada aset yang anda miliki, pada kasus ini memiliki jumlah yang besar menunjukan adanya indikasi brute force attacks. Authentication succes menunjukan jumlah autentikasi yang berhasil

8. Alert level evolution menunjukan grafik jumlah alert dan waktu terjadinya alert. Top Mitre ATTACK menunjukan jumlah taktik dan teknik yang paling sering dijumpai pada alert.

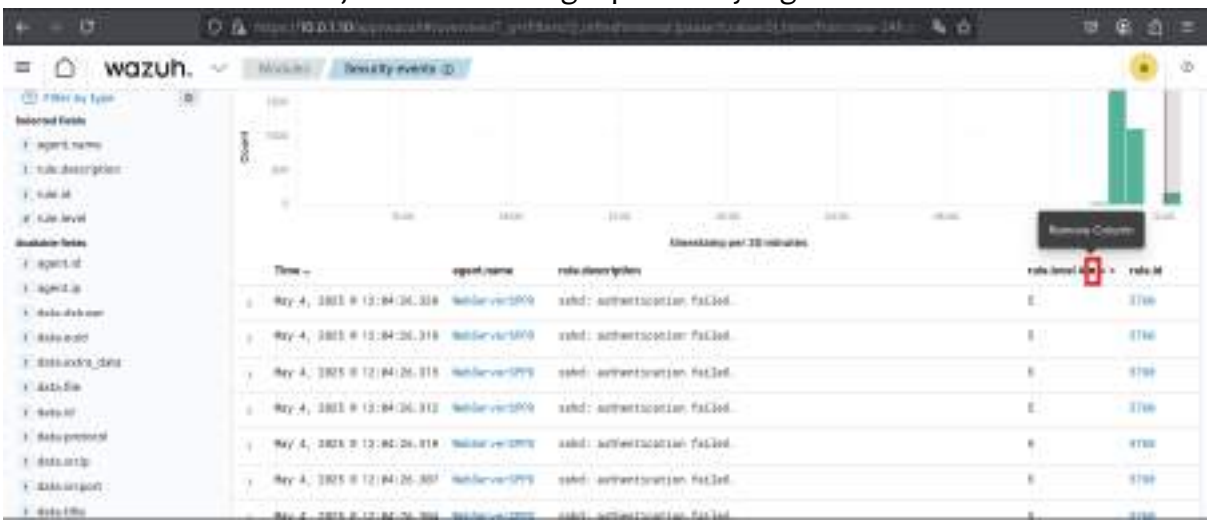


9. Untuk melihat lebih detail mengenai setiap aktivitas yang terjadi, pindah dari tab dashboard menuju tab event.

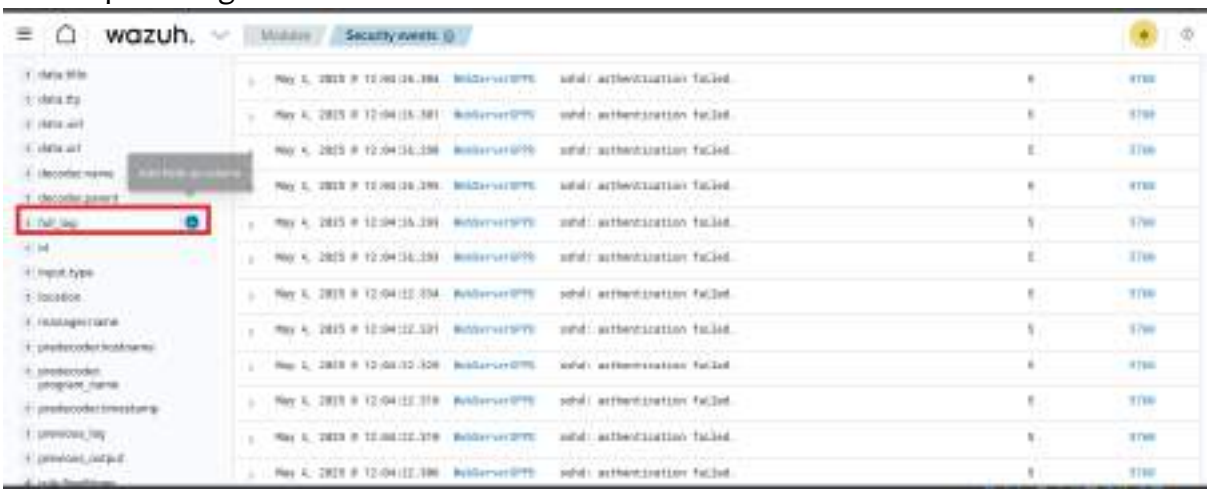
10. Tampilan default field yang ada pada tab event seperti gambar dibawah ini

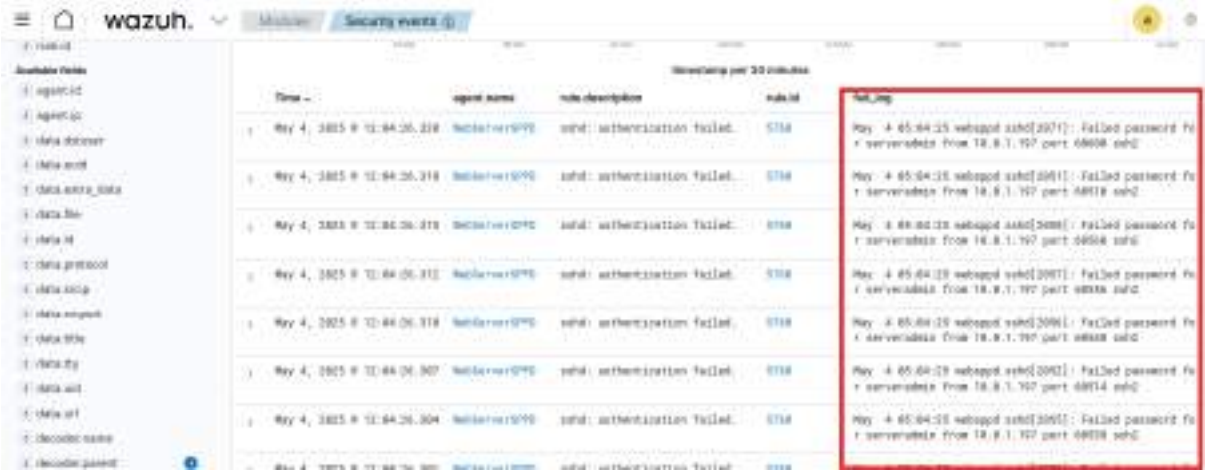


11. Lakukan remove coloum jika hendak menghapus field yang tidak anda butuhkan

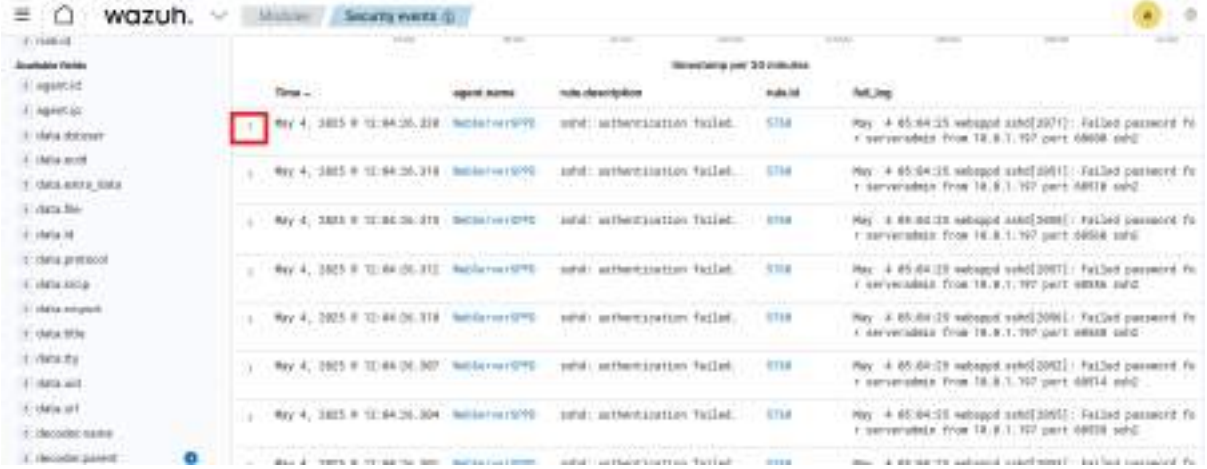


12. Jika anda membutuhkan field baru, anda dapat menambahkam field baru pada sebelah kiri layar, sebagai contoh saya akan menambahkan field full.log untuk menampilkan log secara keseluruhan.



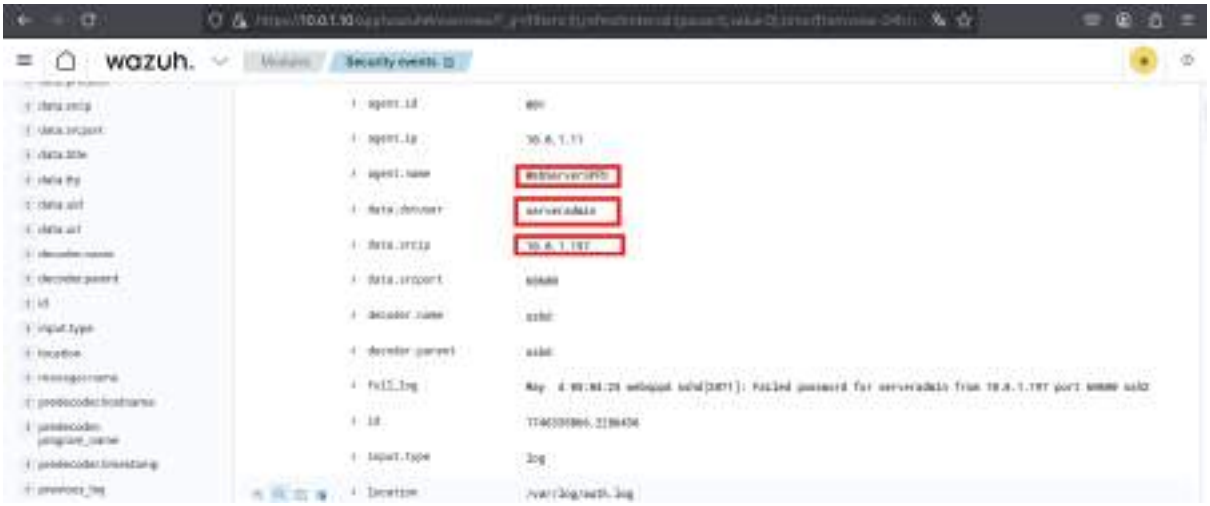


13. Untuk melibat lebih dalam terhadap alert, tekan simbol expand.



14. Dengan melakukan expand anda dapat melihat semua field pada alert

15. Pada gambar dibawah ini anda dapat mengambil informasi bahwa terjadi percobaan masuk pada WebServerSPPD oleh IP 10.0.1.97 menargetkan user serveradmin

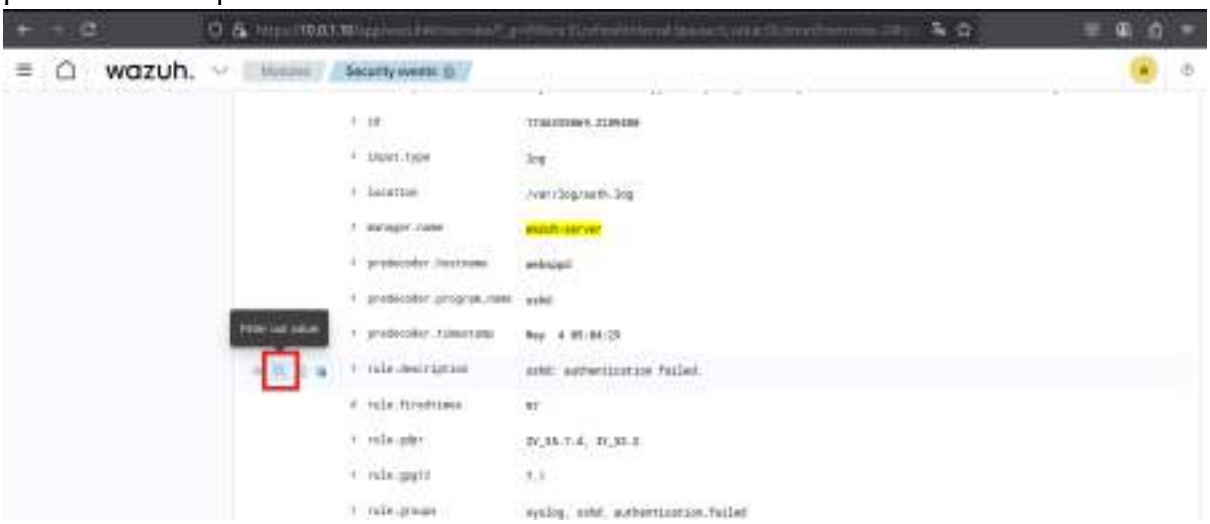


16. Berbekal mengetahui IP Penyerang anda menelusuri IP tersebut dengan menjadikannya filter.

17. Dengan ini Wazuh hanya akan menampilkan aktivitas yang bersumber dari IP 10.0.1.97.

18. Untuk membantu anda dalam mencari aktivitas lain yang dilakukan IP 10.0.1.97, anda mengkerucutkan pencarian dengan melakukan filtering agar tidak menampilkan aktivitas yang berhubungan dengan kegagalan autentikasi dikarenakan anda sudah mendapatkan cukup informasi mengenai serangan brute

force. Expand pada alert yang berhubungan dengan autentikasi kemudian filter out pada rule description



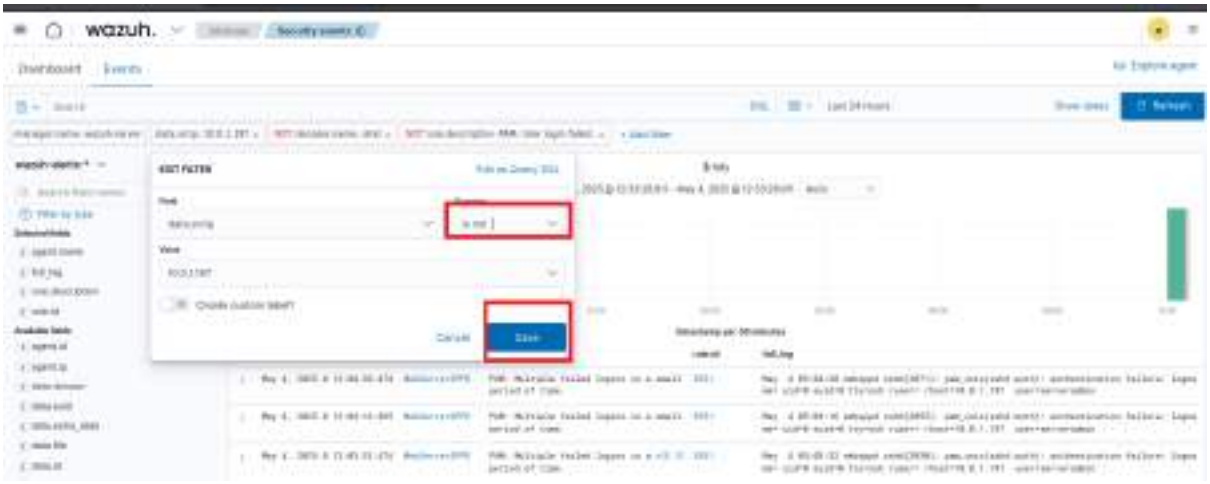
19. Anda dapat melakukan filter yang bertumpuk untuk hasil yang lebih maksimal, pada gambar dibawah ini menunjukan filter menggunakan rule.description yang memiliki hubungan dengan bruteforce attack

20. Anda juga dapat melakukan filtering berdasarkan teknik tertentu seperti brute force

21. Dikarenakan bruteforce menggunakan SSH, anda juga dapat menggunakan decoder.name sshd untuk melakukan filtering, hasil ini lebih cepat karena semua aktivitas yang berhubungand dengan ssh akan ditampilkan

22. Hasil penelusuran menunjukan bahwa tidak ada aktivitas mencurigakan lain yang dilakukan oleh IP 10.0.1.97

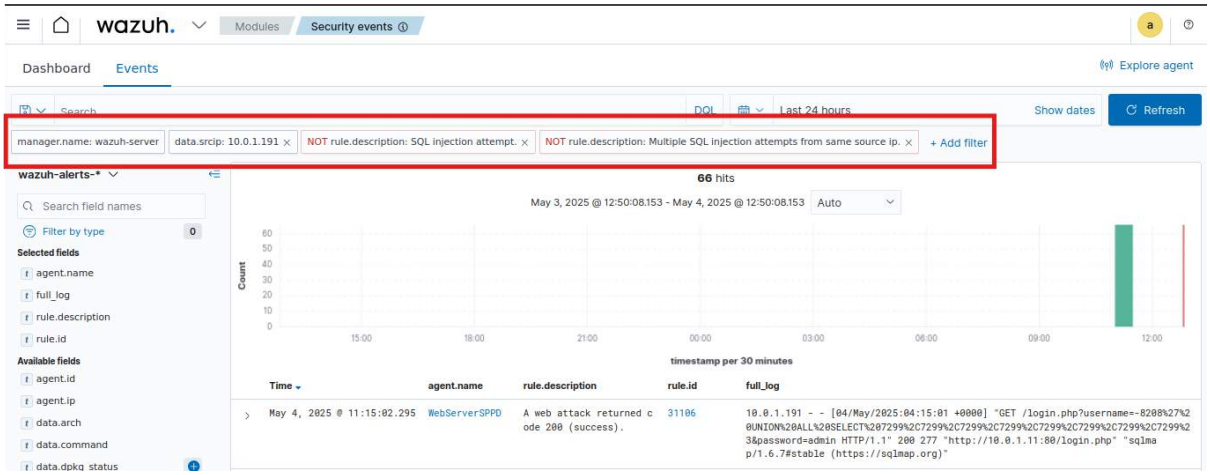
23. Untuk melakukan penelusuran lebih lanjut, ubah filter dengan cara menekan filter yang anda ingin ubah, pada kasus ini anda harus mengubah filter yang seharusnya hanya menampilkan alert aktivitas dari IP 10.0.1.97 menjadi hanya akan menampilkan IP yang tidak berasal dari IP 10.0.1.97.



24. Setelah melakukan perubahan filter tersebut anda akan langsung menemukan bahwa terjadi serangan SQL Injection pada WebServerSPPD. Selisih waktu antar setiap alert cukup kecil (kurang dari satu detik) mengindikasikan serangan menggunakan tools otomatis seperti SQL Map.

25. Lakukan expand pada salah satu alert dapat diketahui bahwa IP penyerang merupakan 10.0.1.191, payload dapat dilihat pada gambar dan menggunakan sqlmap.

26. Lakukan filtering untuk mencari aktivitas lain yang dilakukan IP 10.0.1.191. Hasil filtering tidak menunjukan aktivitas lain selain SQL Injection.



27. Lakukan Eksplorasi secara mandiri mengenai pemanfaatan filter dan field pada wazuh.