(Borang JKPTA FTSM UKM 3)

UNIVERSITI KEBANGSAAN MALAYSIA
National University of Malaysia

FAKULTI TEKNOLOGI DAN SAINS MAKLUMAT

BORANG PENYERAHAN LAPORAN ILMIAH

SEM 2 **SESI** 2021 / 2022

Bahagian A: Maklumat Diri Pelajar
Part A: Student's Details

No. Matrik *(Matric Number)*	A182518
Nama *(Name)*	NURUL AINI ZAFIRAH BINTI NORAZAM
Program pengajian (*Programme*)	TEKNOLOGI MAKLUMAT
No. Telefon (*Telephone Number*)	011-16951979
Emel (*Email*)	a182518@siswa.ukm.edu.my

Tajuk Projek (*Project Title*):

Reka Bentuk Pembangunan Sistem Pengesan Pencerobohan Berasaskan Hos Menggunakan Agen Wazuh

Tandatangan (*Signature*): _____ Tarikh (*Date*) : 22 Julai 2022

Bahagian B: Perakuan Penyelia
Part B: Supervisor's Approval

Saya peraku laporan ini telah disemak dan dibaiki, dan **menyokong / ~~tidak menyokong~~*** penyerahan laporan ilmiah ini.
*I certify that this report has been reviewed and amended, and **approved / rejected*** the report submission.*

Tandatangan (*Signature*): _____ Tarikh (*Date*) : 22 Julai 2022

Cap Rasmi :
(Official Stamp)

Ts. Noor Faridatul Ainun Zainal
GURU BAHASA
Fakulti Teknologi dan Sains Maklumat
Universiti Kebangsaan Malaysia
43600 Bangi, Selangor
03-89216756
019-2755388
faridatul@ukm.edu.my

REKA BENTUK PEMBANGUNAN SISTEM PENGESAN PENCEROBOHAN BERASAKAN HOS MENGGUNAKAN AGEN WAZUH

Nurul Aini Zafirah Binti Norazam

Noor Faridatul Ainun Binti Zainal

Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Alat pemantauan direka untuk mengesan status aplikasi IT, rangkaian, infrastruktur, laman sesawang dan banyak lagi yang kritikal dan bermasalah. Pada masa kini, organisasi telah menggunakan kemudahan teknologi. Oleh itu, fungsi ekuiti, rangkaian dan sistem yang baik akan menjadi kunci untuk perniagaan sesebuah organisasi itu terus beroperasi dan berkembang atau dalam erti lain, pelanggan akan ditawarkan secara langsung melalui perkhidmatan teknologi. Walaupun teknologi merupakan sesuatu yang penting, ia tidak bermakna sempurna. Kesalahan yang berlaku secara tiba-tiba akan menimbulkan situasi yang kritikal. Penyelesaian untuk masalah tersebut adalah membangunkan Sistem Pengesan Pencerobohan (IDS). IDS memainkan peranan yang penting dalam menangani serangan dari pengguna hasad. Sistem ini merupakan alat teknologi yang digunakan untuk mengesan pelbagai bentuk pencerobohan. Berbanding dengan kaedah keselamatan tradisional yang biasa dipasang iaitu tembok api, IDS berasaskan pengesan anomali berkebolehan untuk mengesan serangan baru dengan membuat perbandingan kelakuan antara normal dan anomali. Kaedah kualitatif dengan penyediaan *Google forms* secara dalam talian yang telah diisi oleh beberapa responden dalam kajian awal telah membantu dalam membangunkan IDS ini. Perisian yang telah digunakan dalam membangunkan sistem ini adalah Digital Ocean, Elastic Search, Kibana dan juga Wazuh. Pangkalan Data bagi sistem ini adalah menggunakan servis perisian Digital Ocean. Akhir sekali, alat pemantau ini dapat membantu pengguna dalam mengeluarkan laporan untuk 24 jam aktiviti yang berlaku di dalam hos di mana IDS ini telah dipasang. Tujuan laporan tersebut dikeluarkan adalah untuk mengesan jika terdapat aktiviti yang asing seperti akses yang tidak dibenarkan atau terdapat pengubahan fail. Selain itu, sistem ini juga dapat memvisualisasikan data secara langsung di Kibana. Jadi, pengguna mampu untuk mengambil tindakan awal dalam menghalang sebarang aktiviti jahat seperti menyekat alamat IP.

1 PENGENALAN

Internet kian berkembang ke serata dunia dan telah diguna pakai secara meluas sehingga dunia dikenali sebagai dunia tanpa sempadan. Perkembangan teknologi yang pesat dengan munculnya rangkaian komputer tanpa wayar atau lebih mudah dikenali sebagai ‘Wi-Fi’ menjadikan pengguna terdedah kepada pelbagai serangan dan ancaman terhadap sistem komputer mereka. Beberapa tahun kebelakangan ini, semakin meningkat bilangan penggunaan Sistem Pengesan Pencerobohan (IDS) di dalam organisasi.

Bidang penyelidikan dalam keselamatan sistem pengkomputeran berkaitan dengan pengesanan pencerobohan telah dijalankan semenjak tahun l980an. Telah banyak IDS dibangunkan bagi mengesan penceroboh yang cuba menceroboh sistem. Namun begitu

penyelidikan ke atas data laporan yang telah dihasilkan oleh sesuatu IDS masih lagi kekurangan. Atur cara ini telah dibangunkan berasaskan konsep model umum metodologi penggodam dan juga kaedah Pemadanan Log. Seterusnya, penyelidik telah menggunakan kaedah Pemadanan Log ke atas hasil huraian data imbasan dan juga log amaran serangan bagi menjana laporan alamat IP Penceroboh yang sebenar dengan lebih tepat.

Laporan yang dikeluarkan oleh MyCert (2016), IDS disenaraikan sebagai salah satu daripada teknologi untuk menghalang serangan terhadap rangkaian selain daripada dinding api (firewall). IDS boleh ditakrifkan sebagai sistem yang mencuba untuk mengidentifikasikan penggunaan yang tidak dibenarkan, keganjilan dan penyalahgunaan sistem komputer (Puketza et al. 1996, Ferguson & Senie 1998).

Terdapat dua contoh IDS iaitu Sistem Pengesan Pencerobohan berasaskan Hos (HIDS) dan Sistem Pengesan Pencerobohan berasaskan Rangkaian (NIDS). NIDS 2 bergantung pada paket data yang bergerak di rangkaian untuk memastikan semuanya baik-baik saja. Ia berfungsi dengan membandingkan paket data dengan jenis serangan yang diketahui dan dengan mengetahui penyelewengan dalam paket data yang bergerak di rangkaian. Contoh-contoh anomali boleh hilang tandatangan, jenis data yang tidak wajar dan sebagainya. HIDS ini lebih bergantung kepada tetapan sistem untuk melihat sama ada terdapat sebarang kompromi atau jika ada perisian cuba memaksa perubahan pada komputer atau rangkaian komputer anda. Pendek kata, IDS memerhatikan paket data yang bergerak melalui rangkaian dan memberi isyarat apabila sebarang serangan disyaki atau apabila pelanggaran dasar berlaku. Ia juga akan memberitahu apabila seseorang sedang cuba masuk ke dalam komputer dan menerangkan apa yang berlaku semasa serangan siber. Kedua-dua ini mempunyai kelebihan dan kekurangan masing-masing.

Projek ini akan menumpukan pada HIDS yang merujuk kepada pencerobohan yang berlaku pada sistem hos. Kebiasaannya HIDS ini dipasang pada pelayan dan akan lebih tertumpu kepada menganalisis sistem pengendalian dan aplikasi, penggunaan sumber dan aktiviti sistem lain yang menetap di hos

2 PENYATAAN MASALAH

Dalam tempoh lima tahun kebelakangan ini, organisasi telah menggabungkan teknologi maklumat ke dalam operasi dalaman dan penyelesaian perniagaan mereka pada skala yang besar. Fenomena ini telah mendapat pujian atas peningkatan keperluan untuk mengakses sumber sistem dari jarak jauh dan disebabkan oleh trend yang semakin meningkat ke arah

telekomunikasi, penggunaan video dan persidangan suara. Walau bagaimanapun, ini juga menyebabkan perniagaan dan organisasi berada dalam kedudukan yang berbahaya. Memandangkan organisasi-organisasi ini sangat bergantung pada operasi rangkaian dan kebanyakannya membiarkan sistem terdedah kepada aktiviti yang berniat jahat.

Pada masa kini kesedaran tentang langkah menjaga keselamatan untuk sistem telah meningkat dengan pesat. Organisasi mula melaksanakan tembok api atau dasar keselamatan, akan tetapi pengalaman telah menunjukkan bahawa langkah dan kesedaran itu sahaja tidak mencukupi. Organisasi perlu bergantung pada langkah keselamatan yang lebih maju dan bersepadu untuk melindungi sistem mereka daripada sebarang 3 serangan. Walaupun beberapa kaedah wujud untuk menyediakan keselamatan rangkaian, boleh dikatakan salah satu alat terbaik yang dapat dipraktikkan adalah penggunaan IDS. Sistem ini adalah pelengkap tembok api rangkaian dan menguruskan keselamatan dengan baik.

3 OBJEKTIF KAJIAN

1. Mengenal pasti sumber di sebalik setiap serangan dengan menganalisis log daripada pelbagai ejen dan sistem operasi untuk memberi amaran jika terdapat sebarang aktiviti yang berniat jahat merubah integriti dan pengauditan data dokumen-dokumen sulit.
2. Mereka bentuk pembangunan HIDS yang diberi nama PingPong.

4 METOD KAJIAN

Dalam pembangunan PingPong ini, model proses yang digunakan ialah kaedah Tangkas (Agile). Metodologi Tangkas ini dicipta oleh AgileAlliance, sekumpulan profesional perisian (Paulk 2012). Matlamat utama konsep membangunkan perisian Tangkas ini adalah untuk memuaskan pengguna atau pelanggan melalui penghantaran awal projek, iaitu awal daripada tempoh yang telah ditetapkan dan pengguna atau pelanggan boleh mengubah permintaan mereka bila-bila walaupun perisian sudah berada dalam fasa yang akhir (Paulk 2012). Selain itu, pengguna atau pelanggan dan pembangun haruslah bekerjasama sepanjang projek dijalankan untuk memastikan benda yang di bangun menepati permintaan pengguna atau pelanggan. Proses Tangkas juga menggalakkan pembangunan yang mengekalkan prestasi yang baik. Rajah 4.1 menunjukkan 5 fasa yang terdapat dalam model Tangkas iaitu fasa perancangan, fasa reka bentuk, fasa pembangunan, fasa pengujian dan juga fasa maklum balas.

Rajah 4.1 Model Tangkas

4.1 Fasa Perancangan

Fasa ini bertujuan untuk merancang projek yang akan dibangunkan. Apabila perancangan projek telah dilaksanakan kajian kesusasteraan akan dijalankan untuk mengenal pasti masalah serta mengaji latar belakang masalah. Selain itu, dalam fasa ini juga perbandingan aplikasi atau sistem yang sedia ada juga akan di senaraikan dan dikaji satu per satu. Segala keperluan projek ini dari segi pengguna, sistem, perisian dan perkakasan akan disenaraikan dalam fasa ini untuk kelancaran dan meminimumkan ralat yang akan berlaku dalam fasa pembangunan.

4.2 Fasa Reka Bentuk

Dalam fasa ini, antara muka akan di reka bagi setiap fungsi yang diperlukan oleh sistem ini. Kajian yang dilakukan semasa fasa ini berjalan termasuk pembangunan pangkalan data dan algoritma dan bagaimana sistem ini berinteraksi dengan pengguna. Melalui pendekatan soal selidik yang dijalankan dengan menggunakan *Google Form* dalam mengumpul maklum balas oleh responden akan memastikan reka bentuk yang direka mudah difahami dan mesra pengguna.

4.3 Fasa Pembangunan

Setelah melengkapi fasa perancangan dan reka bentuk, fasa pembangunan akan dilaksanakan berpandukan kajian dan dokumen yang telah dikaji di fasa sebelumnya. Fasa pembangunan ini akan mengambil masa yang lebih lama berbanding fasa yang lain. Dalam fasa ini, pembangunan dijalankan mestilah bersesuaian dengan fungsi-fungsi yang telah dinyatakan dan objektif kajian dapat dicapai dengan jaya.

4.4 Fasa Pengujian

Fasa pengujian yang akan dilakukan adalah bertujuan untuk memastikan pembangunan sistem ini berjaya tanpa ralat yang banyak dan segala fungsi dapat bekerja dengan baiknya.

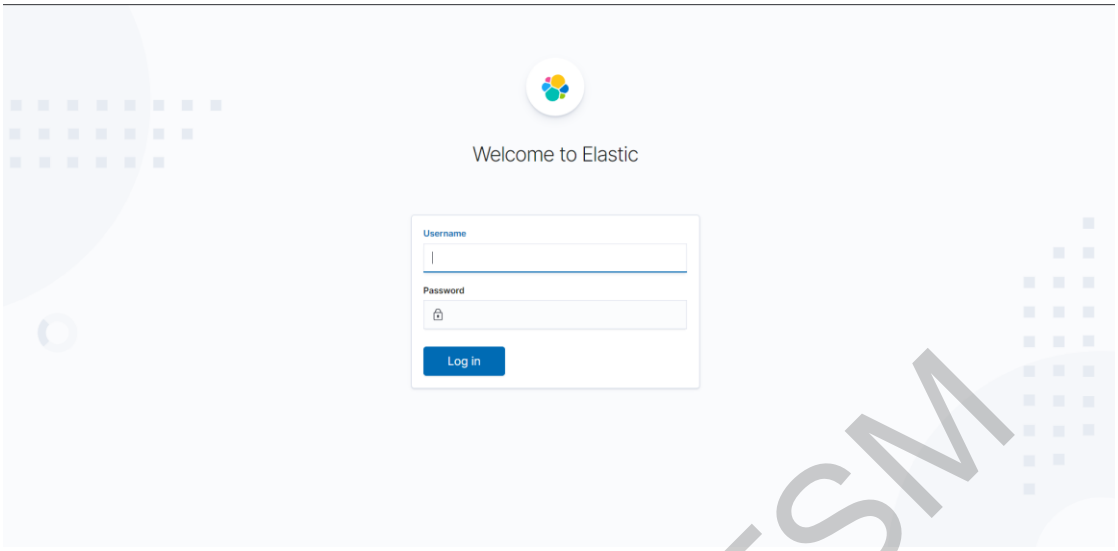
4.5 Fasa Maklum Balas

Maklum balas adalah fasa yang akan dijalankan apabila fasa yang lain telah berjaya disempurnakan. Bagi mengambil maklum balas dari penguji sistem, pendekatan melalui soal selidik di *Google Form* telah dilaksanakan. Penguji akan memberi respons terhadap keberkesanan sistem ini bekerja. Hasil dari maklum balas ini penambahbaikan boleh dilakukan.

5 HASIL KAJIAN

5.1 Log Masuk ke dalam sistem PingPong

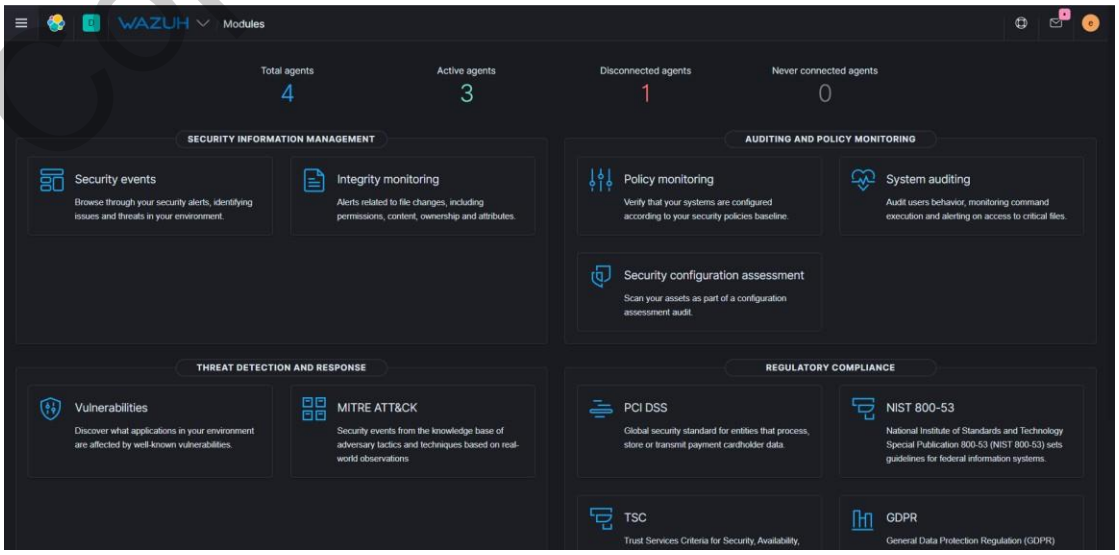
Rajah 5.1 menunjukkan antara muka yang mana nama pengguna dan kata laluan akan diberikan kepada agen yang telah didaftarkan.



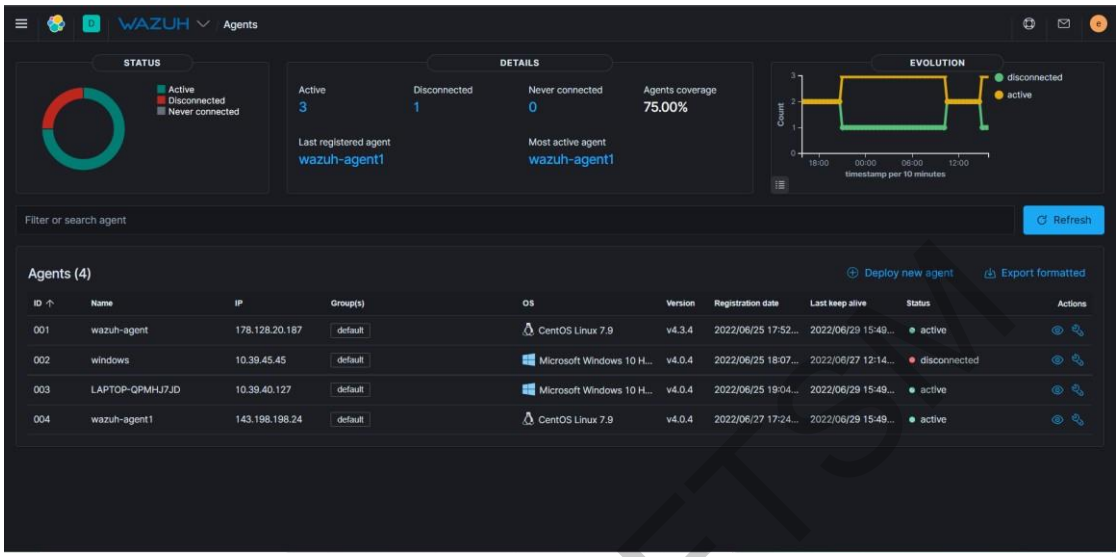
Rajah 5.1 Antara Muka Log Masuk PingPong

5.2 Paparan graf untuk agen yang telah berjaya didaftarkan.

Rajah 5.2 dan Rajah 5.3 menunjukkan antara muka untuk paparan agen yang telah berjaya didaftarkan ke dalam sistem PingPong ini. Seperti yang dapat dilihat di dalam rajah 5.2, terdapat empat agen yang didaftarkan dan tiga daripadanya aktif manakala satu agen tidak aktif. Di dalam rajah 5.3, kesemua agen di paparkan sistem operasi yang digunakan, Nombor ID, nama agen, tarikh agen didaftarkan, status agen dan juga alamat IP untuk pengguna yang memasang agen di dalam hos pelayan.



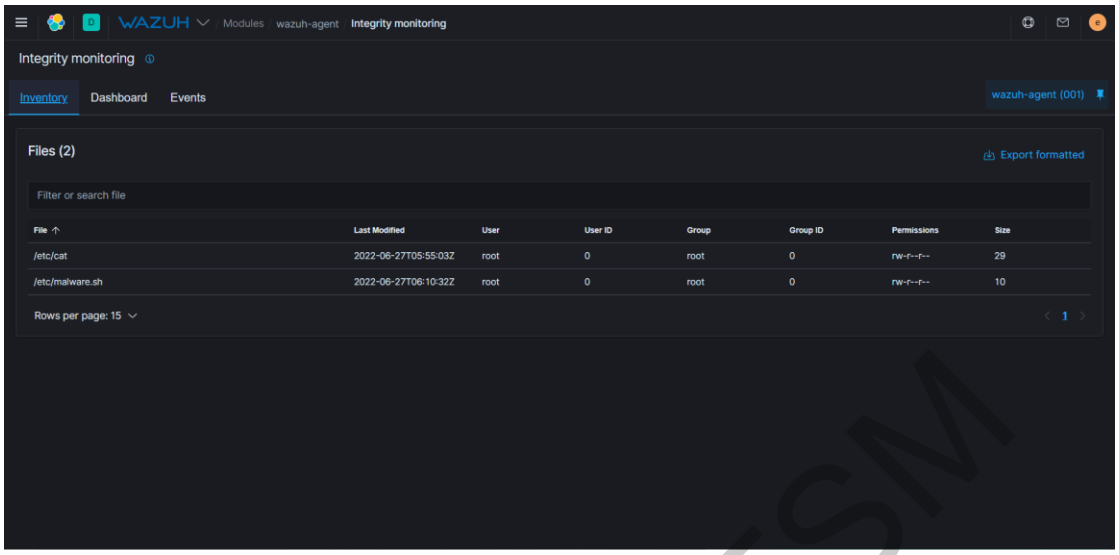
Rajah 5.2 Antara Muka Graf Agen yang Telah Didaftarkan



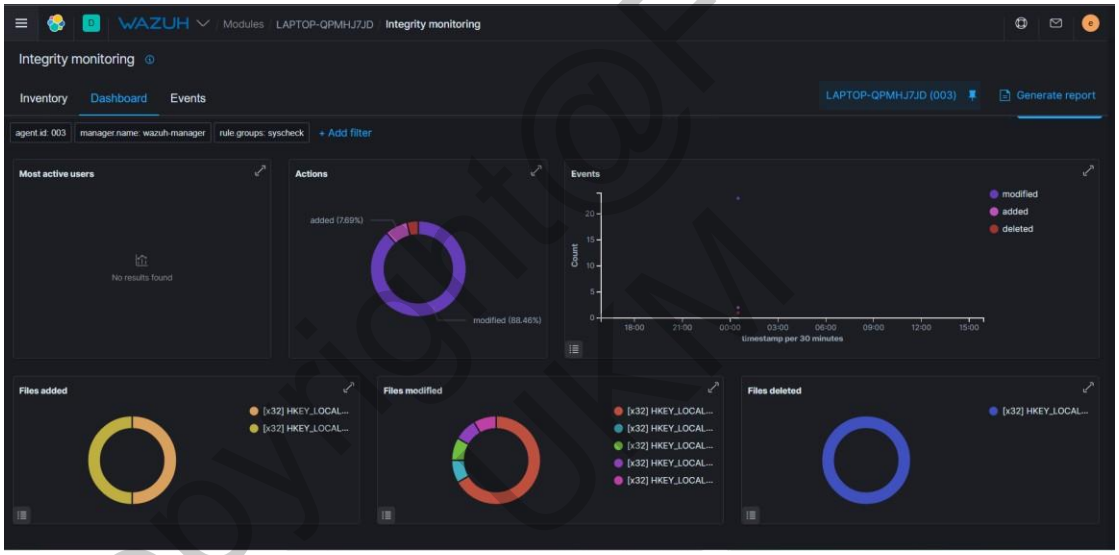
Rajah 5.3 Senarai Agen Yang Didaftarkan

5.3 Paparan senarai amaran yang dikeluarkan

Rajah 5.4 dan rajah 5.5 menunjukkan senarai amaran yang dikeluarkan oleh PingPong jika ada sebarang pengubahan fail. Pengguna dapat memantau integriti fail penting yang mereka simpan di dalam hos kerana sistem ini dapat memberi amaran seperti tarikh fail itu ditambah, dihapus atau diubahsuai. Pengguna juga dapat mengesan individu yang melaku sesuatu ke atas fail penting mereka dengan menekan pilihan kebenaran *(permissions).* Di dalam rajah 5.5 fail yang telah diubahsuai akan dipaparkan dalam bentuk graf yang memudahkan pengguna untuk menganalisis segala aktiviti yang dilakukan ke atas fail-fail tersebut.



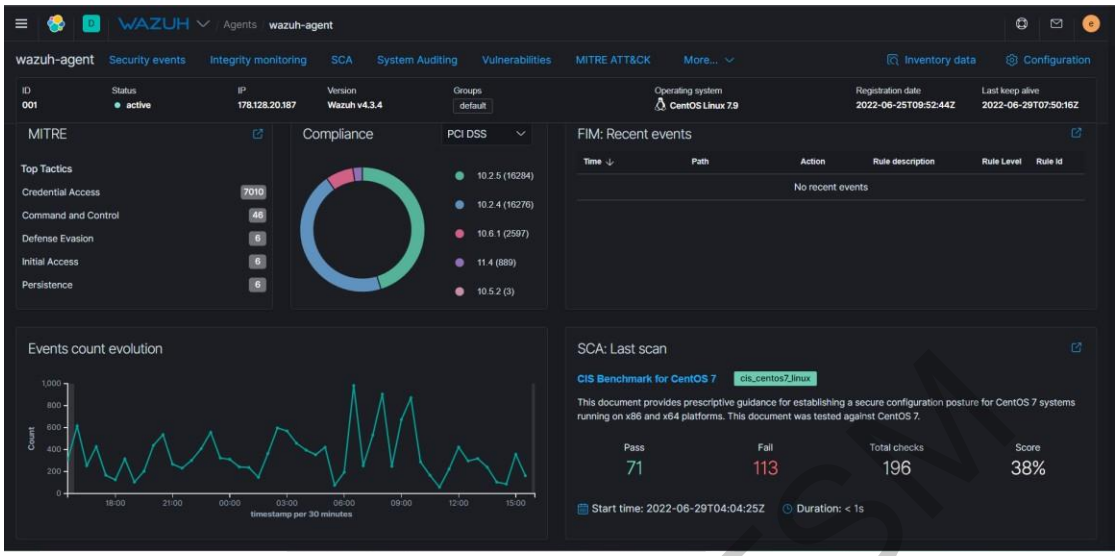
Rajah 5.4 Antara Muka Amaran yang Dikeluarkan Apabila ada Fail Ditambah atau Diubah



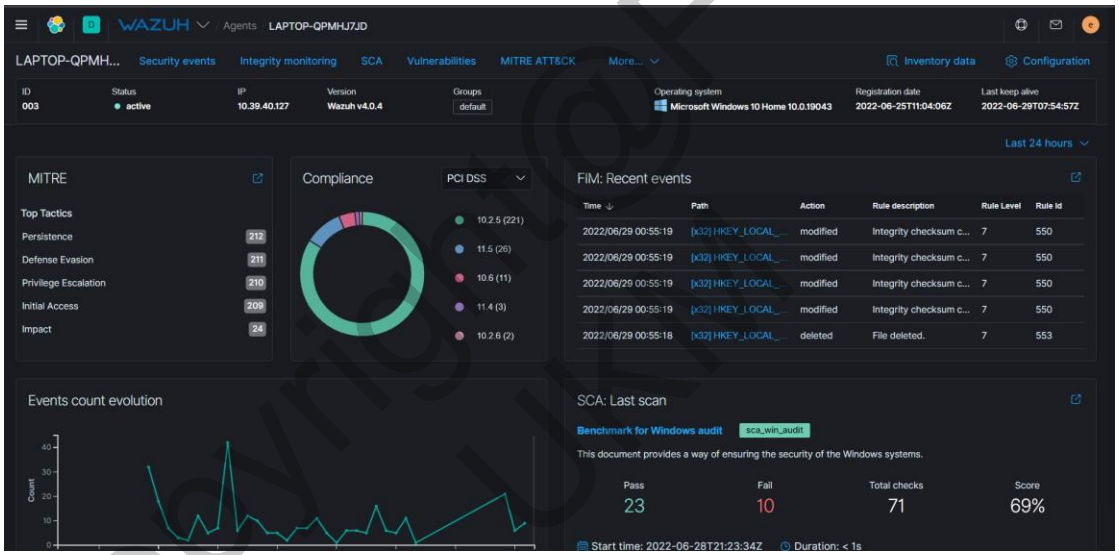
Rajah 5.5 Antara Muka Graf Fail Ditambah, Diubah dan Dipadam oleh Agen Windows

5.4 Paparan dalam bentuk graf setiap aktiviti yang dilakukan oleh agen

Rajah 5.6 dan rajah 5.7 menunjukkan antara muka paparan aktiviti agen yang dikeluarkan dalam bentuk graf. Di dalam paparan ini, pengguna dapat melihat jumlah keseluruhan fail yang telah disemak. Seperti yang dapat dilihat di dalam rajah 5.6 ini adalah aktiviti untuk agen yang di pasang di dalam hos pelayan yang mengguna kan sistem operasi *Centos 7 Linux.* Manakala rajah 5.7 menunjukkan aktiviti yang dilakukan oleh agen yang dipasang di *Windows.*



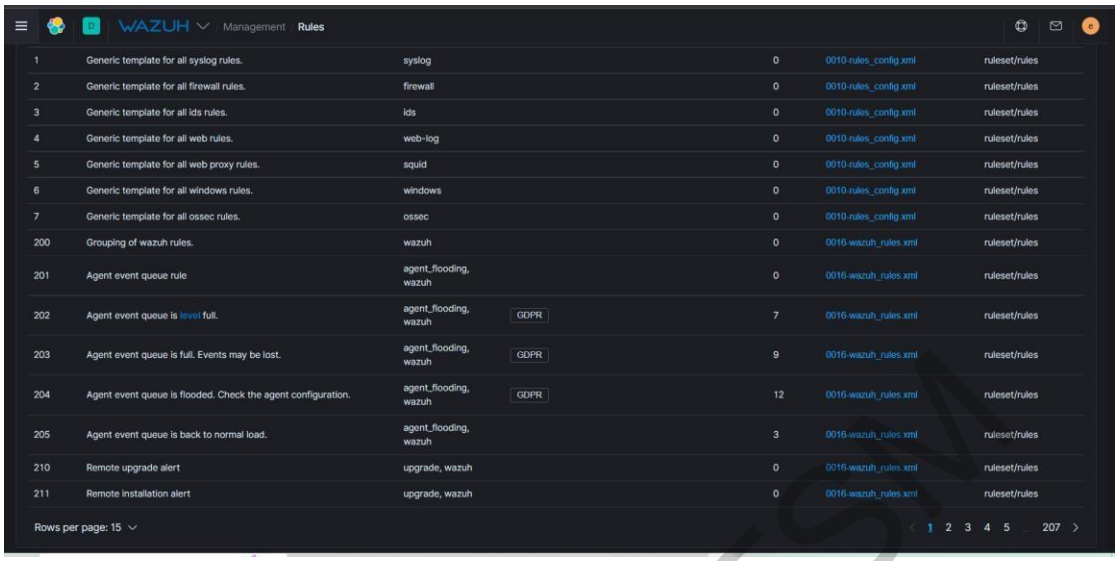
Rajah 5.6 Antara Muka dalam Bentuk Graf Keseluruhan Aktiviti yang Dilakukan oleh Agen Linux



Rajah 5.7 Antara Muka dalam Bentuk Graf Keseluruhan Aktiviti yang Dilakukan oleh Agen Windows

5.5 Paparan senarai peraturan amaran yang telah disetkan di dalam Pengurus Wazuh

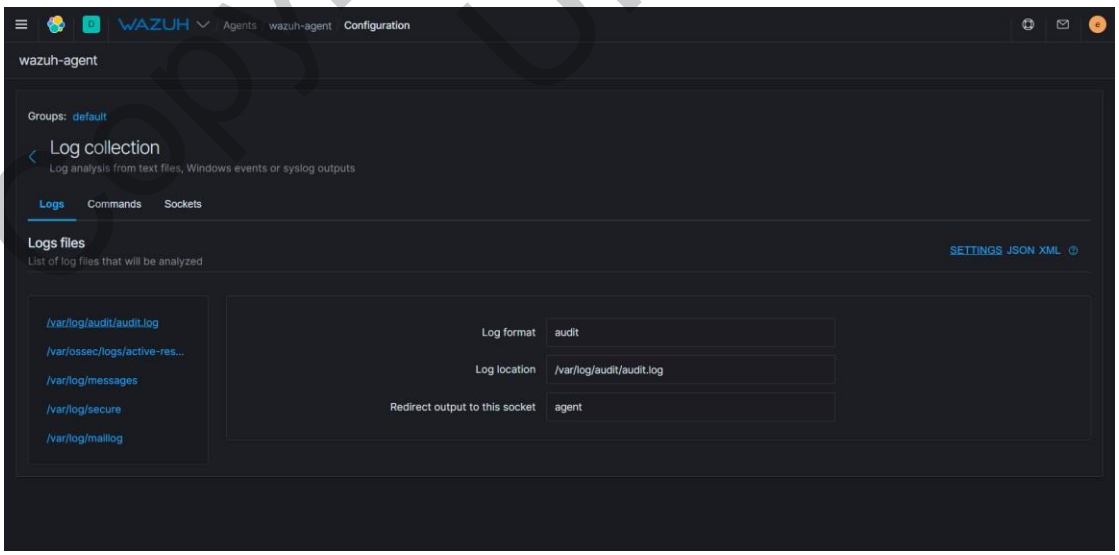
Rajah 5.8 menunjukkan antara muka paparan senarai peraturan yang telah disetkan oleh pengurus Wazuh. Pengguna yang kurang faham peraturan yang dikeluarkan oleh PingPong ini boleh merujuk paparan ini untuk lebih teliti.



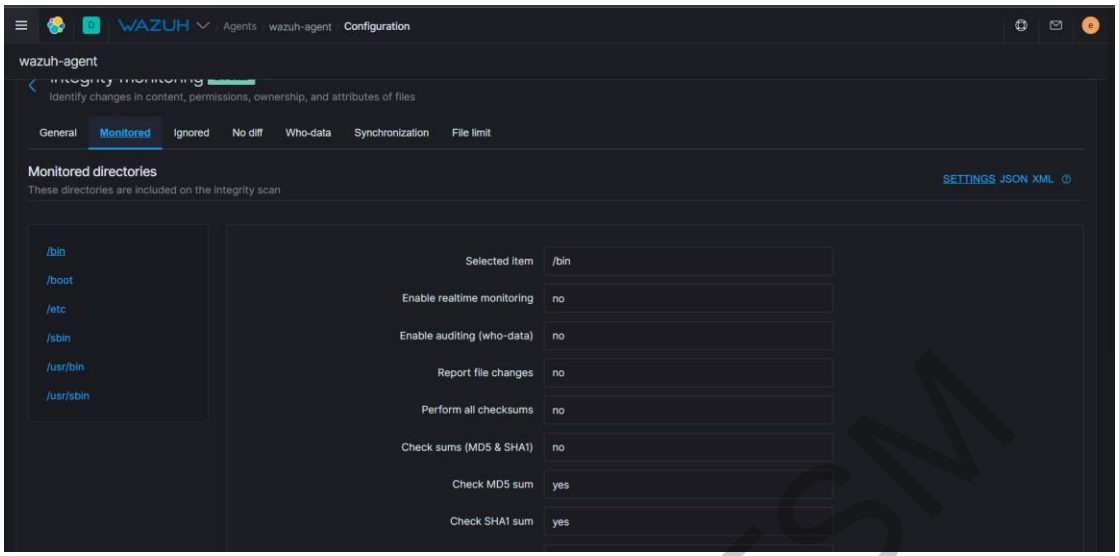
Rajah 5.8 Antara Muka Senarai Peraturan yang Telah Disetkan Oleh Pengurus Wazuh

5.6 Paparan *path* bagi fail yang dipantau dan dianalisis oleh agen yang dipasang.

Rajah 5.9 dan rajah 5.10 menunjukkan antara muka untuk laluan *(path)* untuk pengguna memantau laluan yang tepat untuk sistem PingPong ini mengesan sebarang aktiviti yang asing dan mencurigakan. Seperti contoh di rajah 5.9, sistem ini akan memantau laluan */var/log/secure* untuk mengesan jika ada akses dari individu yang tidak dibenarkan.



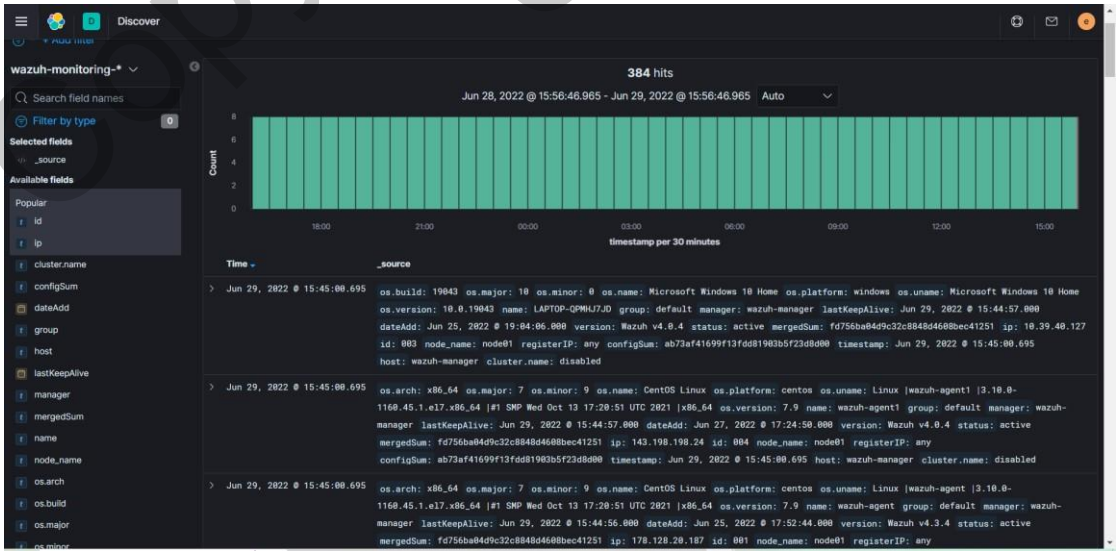
Rajah 5.9 Antara Muka Path Log Collection



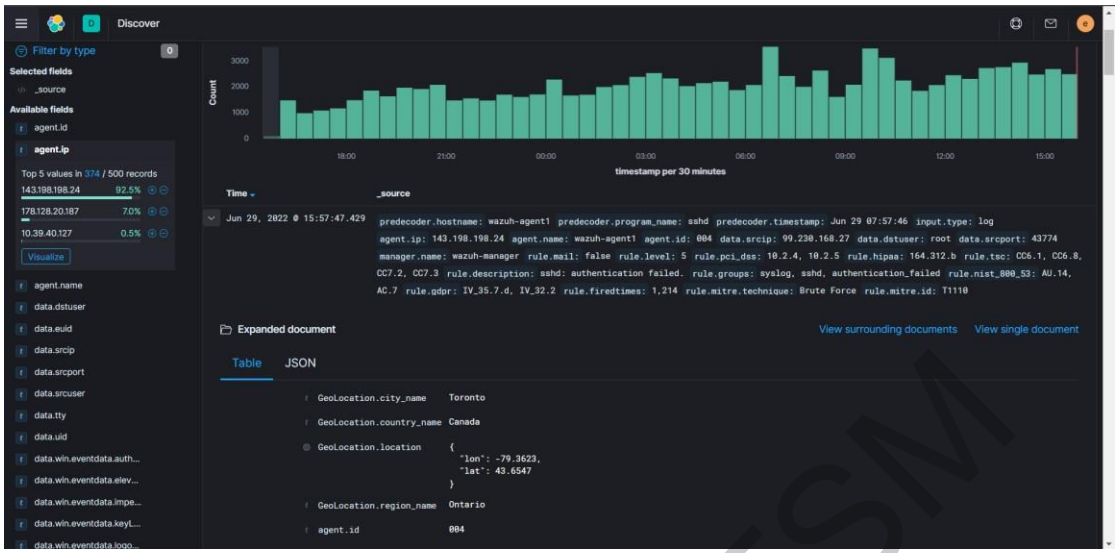
Rajah 5.10 Antara Muka Path Fail yang Dipantau

5.7 Data dipamerkan secara langsung

Rajah 5.11 dan rajah 5.12 menunjukkan data yang di pamerkan secara keseluruhan dan langsung di papan muka. Pengguna boleh menyaksikan secara langsung segala akses ke dalam hos di mana agen yang berdaftar telah dipasangkan dan jika ada pengubahan integriti fail. Di rajah 5.12 terdapat paparan pangkalan data untuk setiap amaran yang dikeluarkan. Pangkalan data yang dikeluarkan mempunyai alamat IP, nama agen dan lain-lain juga.



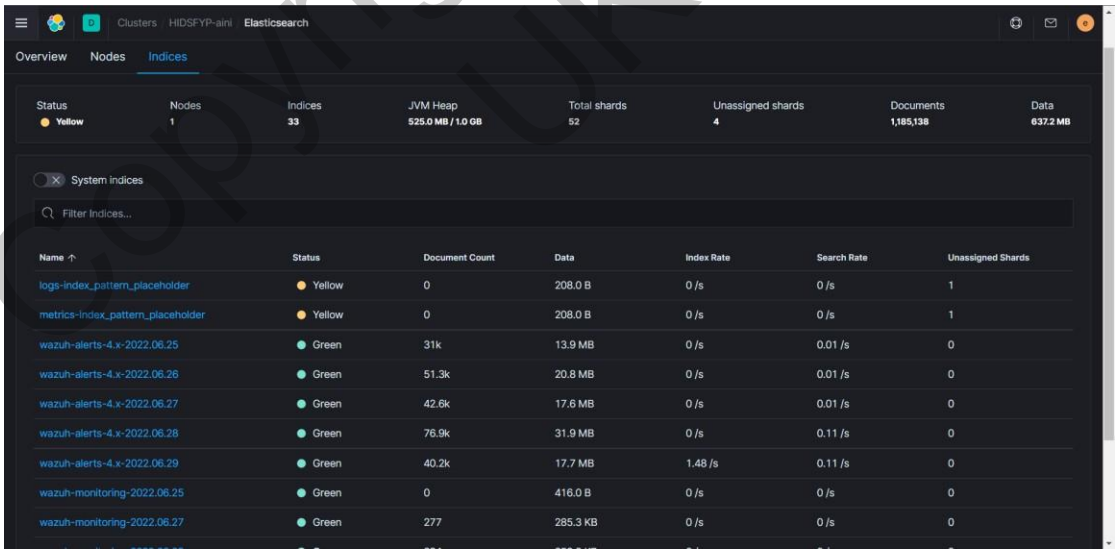
Rajah 5.11 Antara Muka Amaran yang Dikeluarkan



Rajah 5.12 Antara Muka Pangkalan Data Amaran yang Dikeluarkan

5.8 Laporan aktiviti untuk sepanjang 24 jam yang dikeluarkan dan statistik data

Rajah 5.13 dan ra 5.14 menunjukkan laporan aktiviti yang dikeluarkan sistem PingPong ini untuk sepanjang 24 jam dan statistik data yang dipantau. Pengguna boleh rujuk laporan yang mengeluarkan amaran untuk aktiviti yang berlaku di dalam hos di mana agen telah dipasang.



Rajah 5.13 Antara Muka Laporan yang Dikeluarkan Untuk 24 Jam

Rajah 5.14 Antara Muka Statistik Data Yang Di Pantau

6 KESIMPULAN

Sistem PingPong yang dibangunkan ini mempunyai kelebihan dan kekurangannya yang tersendiri. Kelebihan sistem ini ia dapat membantu pengguna menganalisis data di dalam hos sistem ini dipasangkan. Pengguna dapat mengambil langkah awal dalam menangani sebarang serangan berniat jahat. Manakala kekurangannya, sistem ini akan tidak dapat berfungsi jika sistem operasi rosak dan tidak dapat menghalang serangan Dos. Bagi kelebihan diharapkan dapat memberi manfaat kepada para pengguna yang akan menggunakannya pada masa akan datang. Bagi kekurangan pula seharusnya diambil perhatian dan akan ditambah penambahbaikan supaya kekurangan tersebut dapat ditangani dengan baik dan sempurna. Secara keseluruhannya, sistem ini berjaya di bangunkan dan mencapai semua objektif yang diingini. Namun jika terdapat penambah fungsian, ia perlu dikaji terlebih dahulu agar fungsi tersebut dapat memberikan serta dapat di implementasikan kepada pengguna.

6.1 Objektif 1

Objektif kajian pertama ialah mengenal pasti sumber di sebalik setiap serangan dengan menganalisis log daripada pelbagai ejen dan sistem operasi untuk memberi amaran jika terdapat sebarang aktiviti yang berniat jahat merubah integriti dan pengauditan data dokumen-dokumen sulit. Objektif ini dicapai dengan menetapkan peraturan-peraturan untuk setiap ancaman yang telah disetkan oleh di dalam pelayan pengurus *Wazuh.*

6.2 Objektif II

Objektif kedua ialah mereka bentuk pembangunan HIDS yang diberi nama PingPong. Objektif ini dicapai dengan mereka bentuk pembangunan HIDS dengan menggunakan agen *Wazuh* dan juga perisian yang lain seperti *Kibana, Elastic Search,* dan juga Pengurus *Wazuh.*

7 RUJUKAN

Anon. 2019. 8 Best HIDS Tools—Host-Based Intrusion Detection Systems.

dynatrace. n.d. Intelligent Log Analytics. https://www.dynatrace.com/monitoring/platform/log-analytics/?utm_source=google&utm_medium=cpc&utm_term=log%20analyser%20tool&utm_campaign=my-infrastructure-monitoring&utm_content=none&gclid=EAIaIQobChMIr_XF6Jy39QIVrZNmAh1sogrfEAAYASAAEgLhh_D_BwE&gclsrc=aw.

Girardin, L & Brodbeck, D. 1998. A Visual Approach or Monitoring Logs . *In Proceedings of the 12th System Administration Conferences (LISA '98), Boston, MA, December, pp, 299-308*.

Lippmann, R. P. & Cunningham, R. K. 2000. Improving intrusion detection performance using keyword selection and neural networks. Computer Networks, Vol. 34(4), pp. 597-603.

MyCert. 2016. Reported Incidents based on General Incident Classsification Statistic 2016, 5802.

Ferguson, P. & Senie, D. 1998. Network Ingress Filtering: Defeating Denial of Service Attack which employ IP Source Address Spoofing. *Internet Engineering Task Force, RFC 2267*.

Paulk, M. C. 2012. Agile Methodologies and Process Discipline," Crosstalk.

Puketza, N. J., Zhang, K., Chung, M., Mukherjee B. & Olsson, R. A. 1996. A methodology for testing intrusion detection systems. IEEE Transactions on Software Engineering, Vol. 22(10), pp. 719-729.