SISTEM PENGUMPULAN PERISIAN HASAD SECARA AUTOMATIK MENGGUNAKAN HONEYPOT BERASASKAN AWAN (PPH)

YOHANANTHNI A/P RAVICHANDRAN
WAN FARIZA BINTI FAUZI

Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Perisian hasad merupakan ancaman yang semakin meningkat yang membawa banyak kesan negatif terutama dari segi kewangan kepada individu, perniagaan, dan organisasi. Perisian hasad ialah pisau tentera swiss bagi penjenayah siber dan mana-mana musuh lain kepada syarikat atau organisasi. Pada zaman yang semakin berkembang ini, mengesan dan mengalih keluar artifak perisian hasad tidak mencukupi tetapi amat penting untuk memahami cara ia beroperasi untuk memahami konteks, motivasi dan matlamat pelanggaran. Tenaga kerja keselamatan siber dengan kemahiran analisis perisian hasad diperlukan. Penting untuk mendalami tentang perisian hasad dalam persekitaran yang selamat. Perisian hasad adalah berbahaya sehingga tidak boleh hanya menganalisisnya tanpa mempunyai alat yang betul. Terdapat pelbagai alat/sistem untuk analisa perisian hasad yang terdiri daripada sistem komersial Intezer Analyze yang berkos tinggi dan sumber terbuka seperti Cuckoo Sandbox yang percuma. Cuckoo sandbox, yang merupakan sistem analisis perisian hasad automatik sumber terbuka terkemuka, menyediakan persekitaran selamat untuk mengendalikan analisis perisian hasad dalam projek ini. Kebanyakan pengguna mengguna persekitaran Cuckoo secara terpencil. Kos yang tinggi diperlukan untuk menggunakan sistem komersial dan mengambil masa yang lama untuk mengumpulkan perisian hasad secara manual. Untuk menyelesaikan masalah akses terhad, kos tinggi dan pengumpulan data secara manual, projek ini telah menambahbaik sistem analisis perisian hasad sumber terbuka Cuckoo dengan membangun dan mengintegrasi modul pengumpulan perisian hasad secara automatik dari Honeypot yang berasaskan awan. Oleh itu, Honeypot berasaskan awan dibangunkan di AWS untuk mengumpul binari perisian hasad. Satu laman web perisian hasad dibangunkan untuk memudahkan pengguna memuat turun binari perisian hasad tersebut. Binari perisian hasad yang dimuat turun akan disalur ke Cuckoo sandbox untuk dianalisa. Sistem ini akan memberi latihan padanya untuk kakitangan dan pelajar menganalisis dan memahami perisian hasad dengan lebih baik.

1 PENGENALAN

Tenaga kerja keselamatan siber pada masa kini kurang mempunyai kemahiran, latihan dan kelayakan. Laporan State of Cybersecurity 2021 mendapati bahawa 61 peratus pasukan keselamatan siber kekurangan kakitangan (Security, 2021). Rajah 1.1 di bawah menujukkan peratusan jurang kemahiran dan cara organisasi menanganinya. "Ia telah menjadi lebih jelas pada tahun lalu betapa pentingnya keselamatan siber untuk memastikan kesinambungan perniagaan, namun perjuangan selama bertahun-tahun untuk kakitangan pasukan ini berterusan," kata Jonathan Brandt, peneraju amalan profesional keselamatan maklumat ISACA. “Sebagai komuniti keselamatan siber global, adalah mustahak untuk kita semua berkumpul untuk menentukur semula cara kita mengupah, melatih dan mengekalkan pemimpin siber masa depan kita untuk memastikan kita mempunyai tenaga kerja yang kukuh untuk memenuhi keperluan keselamatan siber yang sedang berkembang ini (Security, 2021).

Rangkaian siber *(cyber range)* ialah platform yang membolehkan pasukan profesional melaksanakan keselamatan siber *(cyber security).* Rangkaian siber menawarkan tempat yang selamat dan sah untuk latihan, amalan dan peperangan keselamatan siber.

Pengaturan berasaskan awan *(cloud-based arrangements)* telah bertukar menjadi cara yang mudah semasa situasi pandemik Covid-19 ini untuk organisasi. Syarikat semakin beralih kepada penyelesaian berasaskan awan untuk menyediakan kakitangan mereka dengan alat latihan keselamatan siber yang selamat, terjamin dan terkini. Perisian hasad adalah singkatan untuk 'perisian berniat jahat', iaitu sebarang program yang melakukan aktiviti berniat jahat. Perisian hasad datang dengan pelbagai jenis bentuk dan dengan klasifikasi berbeza yang sewajarnya. Sebagai contohnya, virus, *trojan*, *worm*, perisian pengintip, botnet, perisian tebusan dan lain-lain. Terdapat beberapa sebab mengapa penyerang ingin melakukan serangan mereka melalui perisian hasad. Penyerang boleh menggunakan perisian hasad untuk menipu mangsa supaya memberikan data peribadi untuk kecurian identiti. Selain itu, mereka juga menggunakan perisian hasad untuk mencuri data kad kredit pengguna atau data kewangan lain. Perisian hasad ialah ancaman luar yang paling biasa kepada kebanyakan hos, menyebabkan kerosakan dan gangguan yang meluas dan memerlukan usaha pemulihan yang meluas dalam kebanyakan organisasi. Oleh itu, tenaga kerja keselamatan siber perlu mempunyai kemahiran tentang analisis perisian hasad.

2 PENYATAAN MASALAH

Rangkaian siber boleh terdiri daripada perkakasan dan perisian sebenar atau gabungan komponen sebenar dan maya. Rangkaian siber ini boleh berada di premis *(on-premises)* atau dalam awan *(cloud),* dan ia mungkin memerlukan pemasangan perisian pihak pelanggan atau tidak.

Kebanyakkan organisasi masih tergantung kepada platform rangkaian siber menggunakan pendekatan tradisional *(traditional on-premises approach).* Dengan pandemik Covid-19, platform sebegini menjadi sukar untuk diakses. Antara kelemahan rangkaian siber sepenuhnya berasaskan perkakasan, dengan infrastruktur sebenar terkandung dalam rak rangkaian adalah ia sukar untuk skala, mempunyai akses terhad dan memerlukan kos yang tinggi. Kos yang tinggi diperlukan untuk menggunakan sistem komersial. Oleh itu, projek ini telah dibangunkan ini adalah berasaskan awan mengguna infrastruktur maya.

Selain itu, pengumpulan data secara manual perlu dikumpul dengan kerap kerana perisian hasad baharu setiap hari muncul. Ia juga merupakan salah satu kelemahannya. Perisian hasad ialah ancaman yang semakin serius yang akan membawa banyak kesan negatif kepada individu, perniagaan dan organisasi, terutamanya dari segi kewangan. Memandangkan pertahanan antivirus berasaskan tandatangan standard tidak berkesan terhadap ancaman malware atau serangan APT yang baru ditemui, kakitangan keselamatan siber yang mempunyai kemahiran analisis perisian hasad diperlukan. Kebanyakkan platform rangkaian siber menggunkan analisis statik ialah pendekatan popular untuk pengesanan perisian hasad. Analisis statik menyediakan analisis menyeluruh kod sumber fail boleh laku mudah alih (PE) tanpa melaksanakannya, membenarkan pengesanan peringkat awal program berniat jahat. Ia juga mengambil masa yang banyak untuk melaksanakannya.

3 OBJEKTIF KAJIAN

Objektif umum pelaksanaan projek ini adalah membangunkan sistem pengumpulan perisian hasad secara automatik menggunakan honeypot berasaskan awan. Ini bagi memastikkan latihan keselamatan siber dapat dilaksanakan dalam tempat yang selamat dan pengguna system lebih memahami perisian hasad. Untuk mencapai objektif ini, kajian akan dipandu oleh objektif khusus berikut:

a. Untuk mengkaji pengumpulan perisian hasad secara automatik berasaskan awan.
b. Untuk membangunkan pengumpulan perisian hasad secara automatik menggunakan honeypot berasaskan awan bagi memudahkan proses pengumpulan data tentang perisian hasad.
c. Untuk menguji sistem pengumpulan perisian hasad secara automatik menggunakan honeypot berasaskan awan yang dibangunkan.

4 METOD KAJIAN

Projek ini dibangunkan menggunakan methodologi Agile. Metodologi Agile ialah koleksi prinsip yang menghargai kebolehsuaian dan fleksibiliti. Agile bertujuan untuk memberikan responsif yang lebih baik kepada perubahan keperluan. Kitaran hayat dalam pembangunan

sistem Agile adalah hampir sama dengan metodologi Waterfall kecuali bentuk konsep yang berlainan, iaitu berbentuk lelaran. Dalam projek ini, menggunakan semua fasa yang ada dalam methodologi Agile supaya dapat membangunkan sistem pengumpulan dan analisis perisian hasad yang lengkap dengan tepat pada masa yang diberikan.

4.1 Fasa Perancangan

Fasa perancangan merupakan fasa pertama dan penting dalam pembangunan sistem. Fasa ini mengandungi dua proses iaitu mengenal pasti masalah yang perlu diselesaikan dan cadangan objektif untuk masalah tersebut.

Kajian perpustakaan atau sorotan susastera merupakan fasa yang seterusnya yang dilalukan dalam fasa perancangan. Pelaksanaan sorotan susastera ini adalah bagi mengenalpasti teknologi semasa berkaitan dengan platform rangkaian siber yang terdapat di pasaran. Kajian ini juga adalah untuk mencari masalah yang wujud dengan teknik sedia ada dan cara penyelesaian yang boleh diaplikasikan supaya sistem yang dibangunkan dapat digunakan di persekitaran yang telah dicadangkan.

Berdasarkan kajian perpustakaan, terdapat dua pendekatan untuk analisis perisian hasad iaitu statik dan dinamik. Analisis statik melibatkan pemeriksaan kod (sumber, perantaraan atau binari) untuk menilai tingkah laku sesuatu program tanpa benar-benar melaksanakannya. Pelbagai teknik analisis perisian hasad termasuk dalam kategori analisis statik. Analisis dinamik memantau tingkah laku pelaksanaan perisian hasad untuk mengenal pasti tingkah laku berniat jahat. Selain itu, didapati juga tiga sistem sedia ada yang boleh dijadikan rujukan dan perbandingan dalam proses pembangunan sistem PPH iaitu Cyberbit, KYPO, CYBER RANGES dan Cloud Range. Walaupun terdapat pelbagai platform rangkaian siber sedia ada di pasaran yang diperkenalkan oleh pelbagai syarikat, masih terdapat penembahbaikan yang boleh dilaksanakan bagi memenuhi keperluan sesebuah organisasi.

4.2 Fasa Analisis

Fasa analisis akan menerangkan mengenai spesifikasi pembangunan sistem pengumpulan perisian hasad secara automatik menggunakan honeypot berasaskan awan yang akan dibangunkan dan boleh diguna pakai di mana-mana agensi kerajaan, swasta ataupun individu. Spesifikasi keperluan pembangunan sistem yang terdiri daripada keperluan perkakasan,

perisian, keperluan fungsian, keperluan bukan fungsian dan juga seni bina sistem akan dibincangkan di dalam bab ini secara terperinci. Perkakasan yang digunakan adalah komputer riba dan perisian yang terlibat adalah Windows, Ubuntu, Debian dan Python.

Menentukan keperluan fungsian sistem yang dibangunkan dipanggil keperluan fungsian. Keperluan ini menerangkan interaksi antara sistem dan persekitarannya. Keperluan fungsian perlu dititikberatkan. Hal ini demikian kerana untuk memastikan sistem yang dibangunkan dapat beroperasi secara normal dan memaparkan hasil yang diinginkan. Keperluan fungsi yang menentukan kejayaan sesuatu pembangunan sistem mempunyai dua faktor. Faktor pertama ialah keperluan pengguna. Faktor kedua ialah keperluan sistem itu sendiri. Keperluan pengguna menerangkan kehendak pengguna terhadap sistem yang dibangunkan. Keperluan sistem pula berkaitan dengan fungsi terperinci sistem yang dibangunkan.

Pengguna utama bagi sistem ini terdiri daripada pengguna yang ingin meningkatkan kemahiran mengenai keselamatan siber. Pengguna kedua sistem ini ialah pentadbir sistem. Pengguna biasa mempunyai tiga fungsi iaitu Fungsi Akses Laman Web Perisian Hasad, Fungsi Pilih Modul dan Binari Perisian Hasad dan Fungsi Analisis Perisian Hasad. Manakala pentadbir mempunyai dua fungsi iaitu Fungsi Pengumpulan Perisian Hasad dan Fungsi Kemaskini Laman Web Perisian Hasad. Jadual 1 menerangakan keperluan fungsian. Keperluan bukan fungsian sangat penting untuk memastikan kebolehgunaan dan keberkesanan keseluruhan sistem. Kegagalan untuk memenuhi keperluan bukan fungsian boleh mengakibatkan sistem gagal memenuhi keperluan pengguna dan tidak boleh menggunakan sistem tersebut. Keperluan bukan fungsian merangkumi faktor kebolehgunaan, keselamatan, kecekapan, kebolehpercayaan dan ketersediaan.

Jadual 1 : Keperluan Fungsian

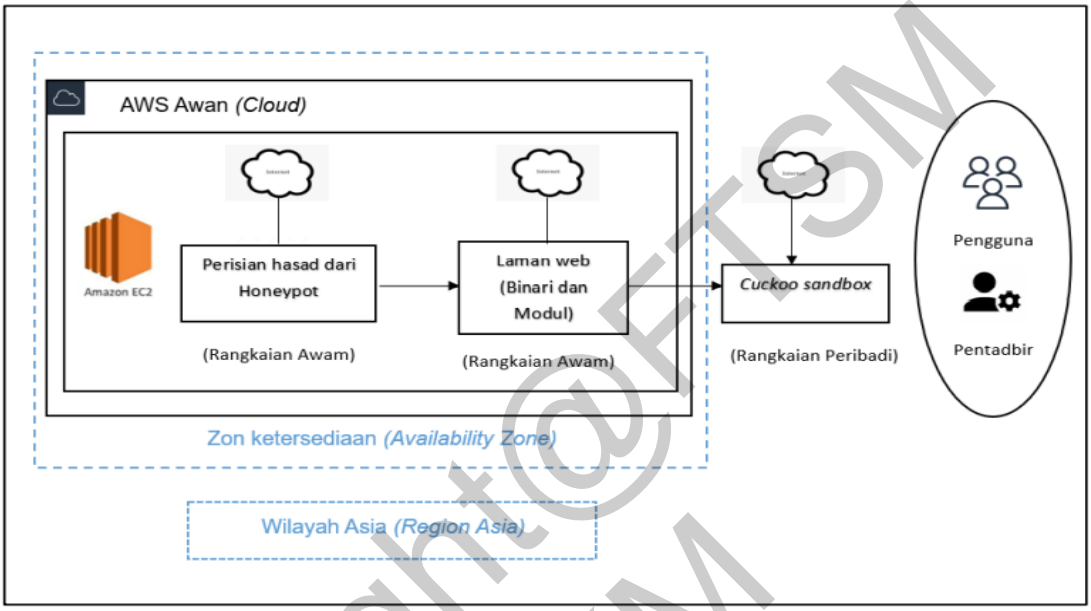
FUNGSI	PENERANGAN
PENGGUNA	
Fungsi Akses Laman Web Perisian Hasad	Pengguna akses laman web perisian hasad untuk muat turun binari dan modul
Fungsi Pilih Modul dan Binari Perisian Hasad	Fungsi ini membolehkan pengguna untuk melihat perisian hasad yang dikumpulkan secara automatik dan memilih salah satu binari perisian hasad untuk muat turun dari laman web perisian hasad.

	Fungsi ini juga menyediakan modul dalam jenis file pdf. Modul ini adalah panduan pengguna tentang perisian hasad. Pengguna dapat mengetahui tentang perisian hasad dengan lebih lanjut melalui fungsi ini. Pengguna boleh muat turun modul.
Fungsi Analisis Perisian Hasad	Setelah memilih dan muat turun binari perisian hasad, pengguna boleh membuat analisis tentang binari perisian hasad yang dipilih. Pengguna perlu muat naik binari perisian hasad dalam Cuckoo Sandbox untuk membuat analisis.
PENTADBIR	
Fungsi Pengumpulan Perisian Hasad	Fungsi ini membolehkan Honeypot untuk mengumpul binari perisian hasad.
Fungsi Kemaskini Laman Web Perisian Hasad	Fungsi ini membolehkan pentadbir untuk kemaskini maklumat yang sedia ada dalam laman web perisian hasad.
SISTEM ATAU PLATFORM	
Fungsi Koleksi Perisian Hasad	Fungi ini akan mengumpul dan menyimpan perisian hasad daripada Honeypot secara automatik.
Fungsi Alat Analisis Perisian Hasad	Fungsi ini akan menggunakan perisisan hasad yang dikumpulkan untuk mengalisis perisisan hasad tersebut secara dinamik. Fungsi ini akan menggunakan alat Cuckoo Sandbox untuk melaksanakan proses analisis perisian hasad. Cuckoo Sandbox akan ditetapkan dalam awan.
Fungsi Bahan latihan (Modul)	Fungsi ini membuat simpanan bahan latihan iaitu modul yang akan digunakan oleh pengguna.

4.3 Fasa Reka Bentuk

Reka bentuk seni bina adalah penyusuran dan pengaturan struktur-struktur bagi sesuatu sistem yang ingin dibangunkan. Reka bentuk seni bina juga merupakan satu gambaran awal keseluruhan sistem. Ia merupakan representasi konseptual bagi komponen dan subkomponen yang mencerminkan tingkah laku sistem yang akan dibangunkan. Reka bentuk senibina merupakan hubungan yang kritikal di antara reka bentuk dan kejuteraan keperluan. Matlamatnya adalah untuk mengenal pasti komponen-komponen berstruktur yang utama di dalam sistem serta hubungan-hubungan di antara setiap komponen tersebut. Reka bentuk seni

bina adalah penting untuk memenuhi keperluan fungsian dan juga bukan fungsian. Hal ini demikian kerana impaknya kepada prestasi sistem yang akan dibangunkan. Reka bentuk seni bina, reka bentuk pangkalan data, reka bentuk antara muka dan reka bentuk algorithma bagi sistem PPH diterangkan dalam fasa ini. Fasa ini juga diterangkan dengan lebih lanjut dengan menggunkan raja kes guna, raja interaksi, raja aktiviti dan reka bentuk seni bina. Reka bentuk seni bina rangkaian bagi sistem ini ditunjukkan dalam Rajah 1.



Rajah 1 : Rekabentuk Senibina Rangkaian PPH

Seterusnya, penyediaan reka bentuk antara muka adalah proses untuk menentukan kaedah interaksi di antara pengguna dengan sistem yang akan dibangunkan. Kita perlu memberi keutamaan kepada reka bentuk antara muka supaya dapat menjadikan sesuatu aplikasi atau sistem mudah untuk dilayari, fleksibel dan selesa untuk digunakan. Antara muka mestilah direka dengan ciri-ciri yang mudah difahami dan mesra pengguna. Selanjutnya, antara muka pengguna yang dibangunkan perlu dipadankan dengan medan-medan data di dalam jadual pangkalan data. Pemetaan data ini bermatlamat untuk memudahkan pembangun sistem mengetahui senarai medan data yang diperlukan bagi satu-satu antara muka pengguna yang akan dibangunkan. Contoh reka bentuk antara muka ditunjukkan dalam Rajah 2.

Rajah 2 : Antara Muka Laman Web Perisian Hasad

4.4 Fasa Implementasi

Fasa implementasi ialah fasa di mana sistem yang dirancang pada fasa sebelumnya dibangunkan menjadi sistem sebenar. Laporan ini menerangkan tentang persediaan perkakasan dan perisian bagi persekitaran pembangunan, pembangunan reka bentuk antara muka, pangkalan data dan pengaturcaraan program, yang melibatkan kod-kod kritikal bagi sistem pengumpulan perisian hasad secara automatik untuk latihan di platform rangkaian siber berasaskan awan. Fasa pembangunan ini dijalankan mengikut perancangan dan keperluan sistem yang dibentangkan dalam metodologi penyelidikan. Semua proses pembangunan pada peringkat ini dilaksanakan dalam persekitaran awan *(AWS Cloud)*. Rangka kerja bagi pembangunan sistem ini ialah *AWS Well-Architected Framework*. Sistem ini telah dibangunkan dengan menggunakan Perkhidmatan *Web amazon EC2 (Amazon Web Services EC2).* Jenis instance yang digunakan untuk Honeypot ialah t2.xlarge. Python merupakan bahasa pengaturcaraan yang digunakan. Honeypot telah dipasangkan dalam perisian pengendalian Debian 11 manakala Cuckoo Sandbox dipasangkan dalam perisian pengendalian Ubuntu 18.04. Sistem ini terdiri daripada tiga bahagian iaitu mengumpul perisian hasad, analisis dan modul. Sistem ini dibangunkan secara berperingkat. Peringkat 1 adalah Pemasangan Perisian Honeypot untuk pengumpulan perisian hasad. Peringkat 2 adalah Pemasangan Cuckoo Sandbox untuk analisis perisian hasad. Peringkat 3 adalah Laman web perisian hasad.

4.5 Fasa Pengujian

Fasa pengujian ialah fasa yang menerangkan pengujian yang dilakukan pada sistem PPH. Fasa pengujian ini bertujuan untuk menguji tahap kebolehgunaan sistem tersebut. Semasa fasa pengujian, pembangun mengetahui sama ada kod dan pengaturcaraan berfungsi mengikut keperluan pelanggan. Walaupun tidak mungkin untuk menyelesaikan semua kegagalan yang temui semasa fasa ujian, tetapi mungkin untuk menggunakan keputusan daripada fasa ini untuk mengurangkan bilangan ralat dalam program perisian. Pengujian sistem ini sangat penting untuk memastikan semua objektif dan matlamat pembangunan sistem telah dicapai.

Sebelum ujian dimulakan, perlu membangunkan rancangan pengujian. Pelan ujian termasuk jenis ujian yang akan digunakan, sumber untuk ujian, cara perisian akan diuji, siapa yang sepatutnya menjadi penguji semasa setiap fasa dan skrip ujian, yang merupakan arahan yang digunakan oleh setiap penguji untuk menguji perisian. Pengujian sistem ditamatkan berasakan perbandingan hasil yang dijankakan dan hasil sebenar setiap ujian mengikut prosedur pengujian Kes Guna. Terdapat beberapa kriteria yang mesti dipenuhi untu k menentukan sesuatu proses pengujian ditamatkan. Antaranya ialah mematuhi setiap prosedur yang telah ditetapkan bagi setiap ujian Kes Guna. Selain itu, status pengujian bagi setiap ujian Kes Guna adalah ‘Berjaya’. Fasa pengujian sistem ini melibatkan pengujian secara persekitaran dalaman *(Local Area Network - LAN)* tanpa wayar *(wireless)*. Pengujian berfungsi dan pengujian tidak berfunsi dijalankan. Pengujian berfungsi yang dijalankan ialah Pengujian Kotak Hitam *(Black Box Testing)*. Pengujian tidak berfungsi yang dijalankan ialah Pengujian Keselamatan *(Security Testing)*. Jadual 2 dan Jadual 3 menunjukkan senarai kes guna (UC-1 hingga UC-5) dan perincian berkaitan pengujian yang akan dilaksanakan.

Jadual 2 : Pengujian Berfungsi

PENGUJIAN BERFUNGSI			
KES GUNA	**KEPERLUAN FUNGSI**	**PERINCIAN PENGUJIAN**	**HASIL PENGUJIAN**
UC-1	Akses Laman Web Perisian Hasad	Menguji pengguna boleh akses laman web.	Senario 1: Sistem akan memaparkan laman web perisian hasad.

			Senario 2: Sistem akan memparkan ralat.
UC-2	Pilih Modul dan Binari Perisian Hasad	Menguji fungsi pilih modul dan binari perisian hasad**.** Menguji pengguna boleh muat turun modul dan binari perisian hasad.	Binari dan modul akan ada dalam *Downloads folder local device* pengguna.
UC-3	Analisis Perisian Hasad	Menguji perisian hasad yang dimuat turun adalah binari perisian hasad ataupun tidak menggunakan Cuckoo Sandbox**.** Menguji fungsi analisis perisian hasad.	Senario 1: Sistem akan memaparkan laman web Cuckoo Sandbox dan pengguna membuat analisis perisian hasad. Senario 2: Cuckoo rooter akan memparkan ralat dan tidak boleh akses Cuckoo Sandbox.
UC-4	Pengumpulan perisian hasad	Menguji Honeypot mengumpul perisian hasad.	Senario 1: Sistem akan memaparkan laman web Honeypot. Honeypot mengumpul dan memaparkan perisian hasad. Senario 2: Laman web Honeypot dan *Command Prompt*

			akan memparkan ralat.
UC-5	Kemaskini Laman Web Perisian Hasad	Menguji fungsi pengemaskinian maklumat laman web dan modul.	.Laman web memaparkan maklumat yang dikemaskini.

Jadual 3 : Pengujian Tidak Berfungsi

PENGUJIAN TIDAK BERFUNGSI			
KES GUNA	**KEPERLUAN FUNGSI**	**PERINCIAN PENGUJIAN**	**HASIL PENGUJIAN**
UC-3	Analisis Perisian Hasad	Pengguna berjaya akses Cuckoo Rooter untuk membuat analisis perisian hasad	Senario 1: Sistem akan memaparkan laman Web Cuckoo Sandbox dan pengguna membuat analisis perisian hasad. Senario 2: Cuckoo rooter akan memparkan ralat dan tidak boleh akses Cuckoo Sandbox.
UC-4	Pengumpulan perisian hasad	Pentabdir berjaya log masuk Honeypot.	Senario 1: Sistem akan memaparkan laman Web Honeypot. Senario 2: Laman web Honeypot dan Command

			Prompt akan memparkan ralat.

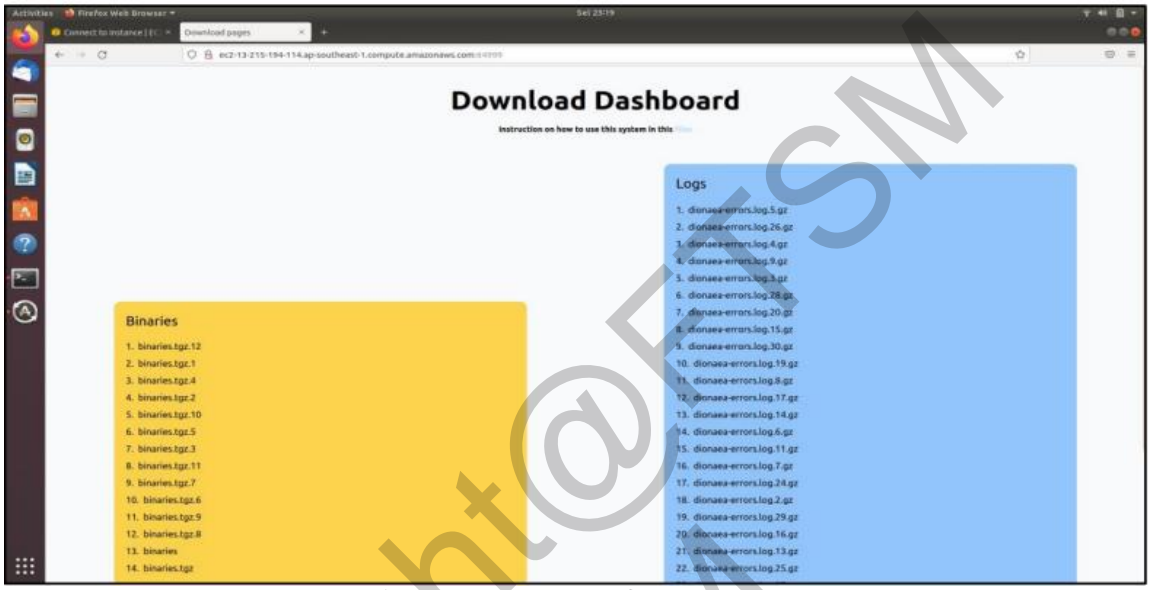
5 HASIL KAJIAN

Kelebihan sistem ini adalah sistem ini dibangunkan beradasarkan awan dan segala proses penyelenggaraan tidak melibatkan kos yang tinggi. Selain itu, Honeypot dan Cuckoo Sandbox adalah sumber terbuka yang boleh dipasangkan secara percuma. Penambahbaikan sistem hanya melibatkan faktor masa dan kepakaran individu dalam bidang pengaturcaraan, AWS Cloud dan rangkaian. Selanjutnya, sistem ini berjaya mencapai objektifnya iaitu mengumpulkan perisian hasad dan membuat analisis. Objektif ini berjaya dicapai dan dibuktikan melalui keputusan hasil pengujian yang telah dilaksanakan. Seterusnya, binari perisian hasad yang dimuat turun dari laman web juga tidak memberi kesan kepada peranti kita. Akhirnya, dari segi integriti sistem di peringkat pengguna adalah terjamin. Sistem ini dibangunkan dengan menggunakan bahasa pengaturcaraan Python dan Framework Django. Perisian yang digunakan ialah Visual Studio Code (VSCode).

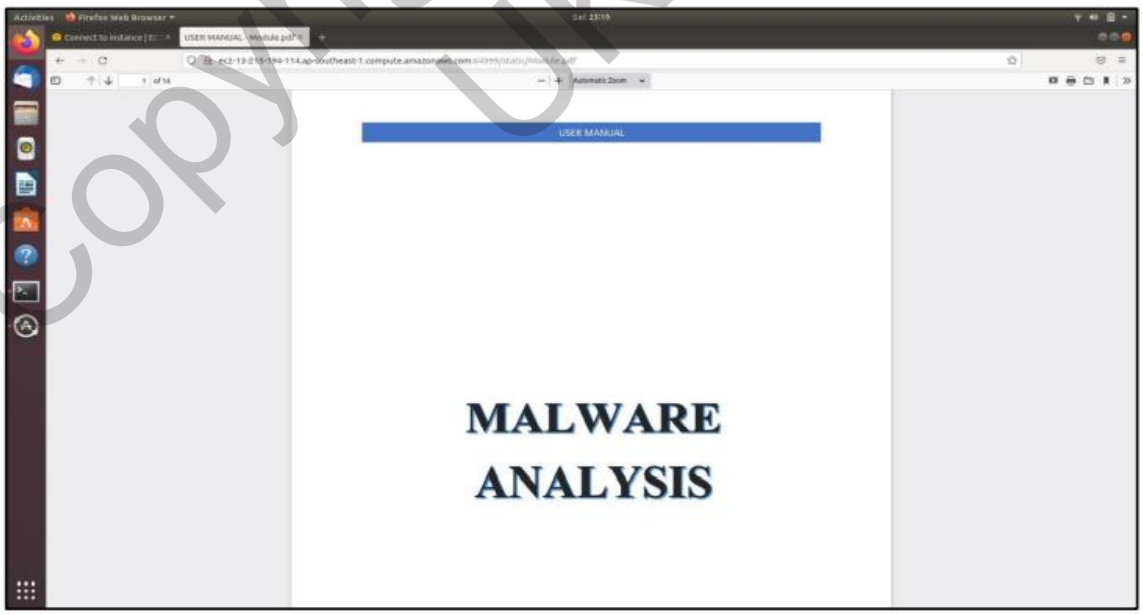
Pada mulanya, pentadbir akan log masuk akaun AWS Cloud dan mulakan *instance Honeypot Server*. Selepas itu, pentadbir akan akses Laman Web Tpot dengan menggunkan *ip instance* dan *port number*. Pentadbir akan masukkan *username* dan kata laluan untuk akses tpot. Pentadbir akan pilih kibana dan tpot. Pentadbir perlu biarkan tpot untuk berjalan selama beberapa jam untuk mendapatkan binari perisian hasad. Kemudian pentadbir akan semak binari perisian hasad wujud ataupun tidak dengan menggunakan beberapa *commands*. Seterusnya, pentadbir juga boleh kemaskini kod laman web perisian hasad dan muat naik modul yang dikemaskini. Proses ini ditunjukkan seperti Rajah 3.

Rajah 3 : Proses Fungsi Pentadbir

Manakala pengguna akan akses laman web perisian hasad dan muat turun modul dan binari perisian hasad. Modul mengandungi cara untuk menggunkan sistem dan maklumat tentang perisian hasad. Pengguna boleh pilih salah satu binari untuk muat turun. Pengguna juga boleh melihat *log* perisian hasad dengan muat turun fail l*ogs*. Antara muka laman web perisian dan modul ditunjukkan dalam Rajah 4 dan Rajah 5.

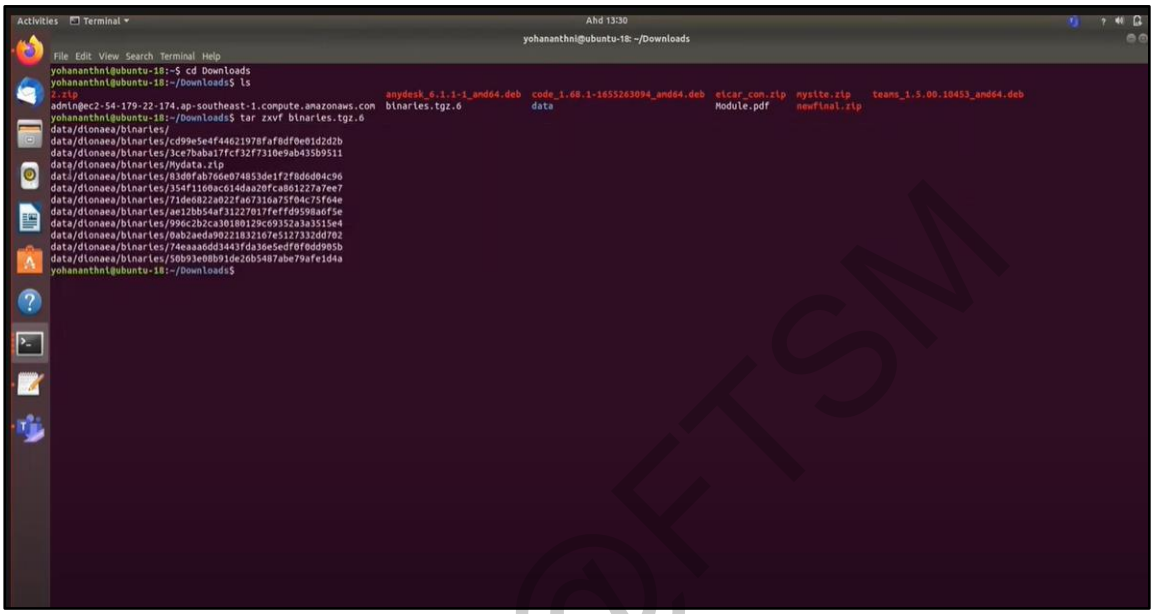


Rajah 4 : Antara Muka Laman Web Perisian Hasad



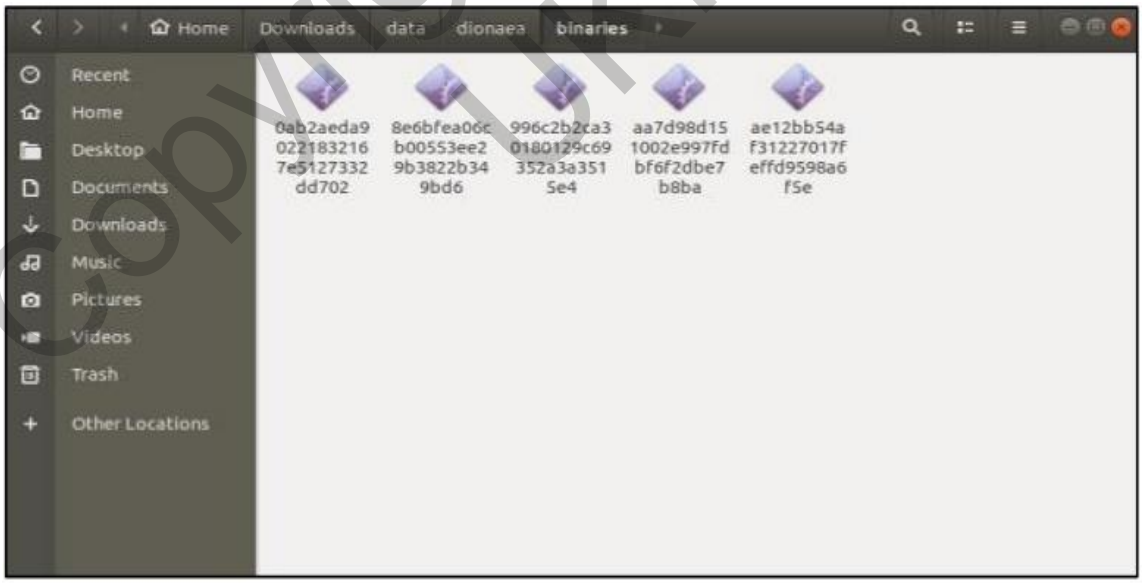
Rajah 5 : Antara Muka Modul

Seterusnya, pengguna perlu ekstrak binari yang dimuat turun dengan menggunkan beberapa *commands* untuk membuat analisis seperti Rajah 6.



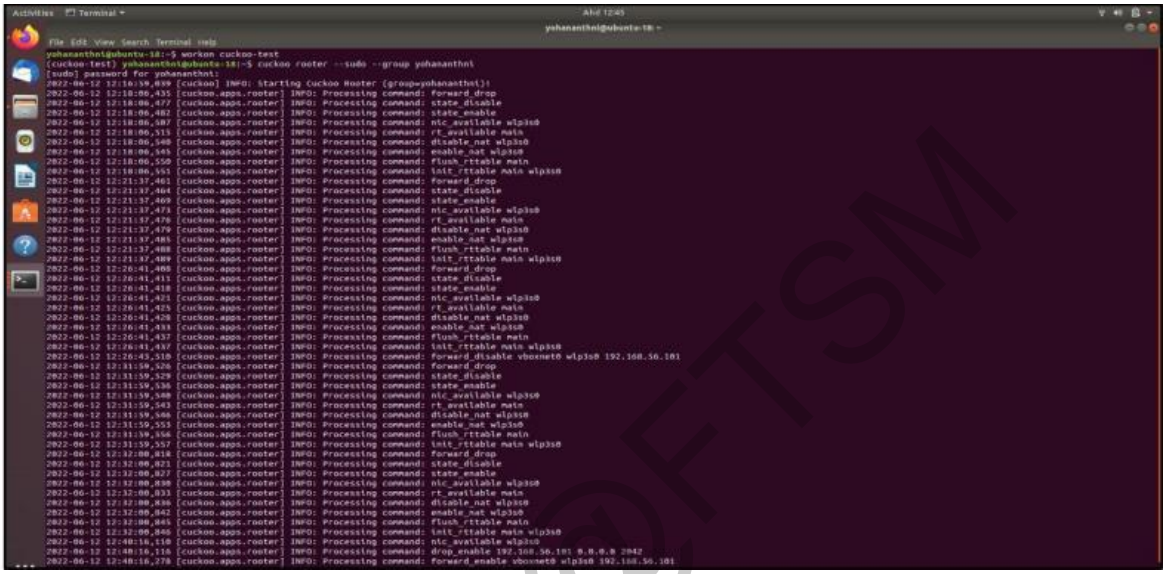
Rajah 6 : Binari Diekstrak

Binari perisian hasad yang diekstrak akan ada dalam Folder Downloads/data/dionaea/binaries seperti Rajah 7.



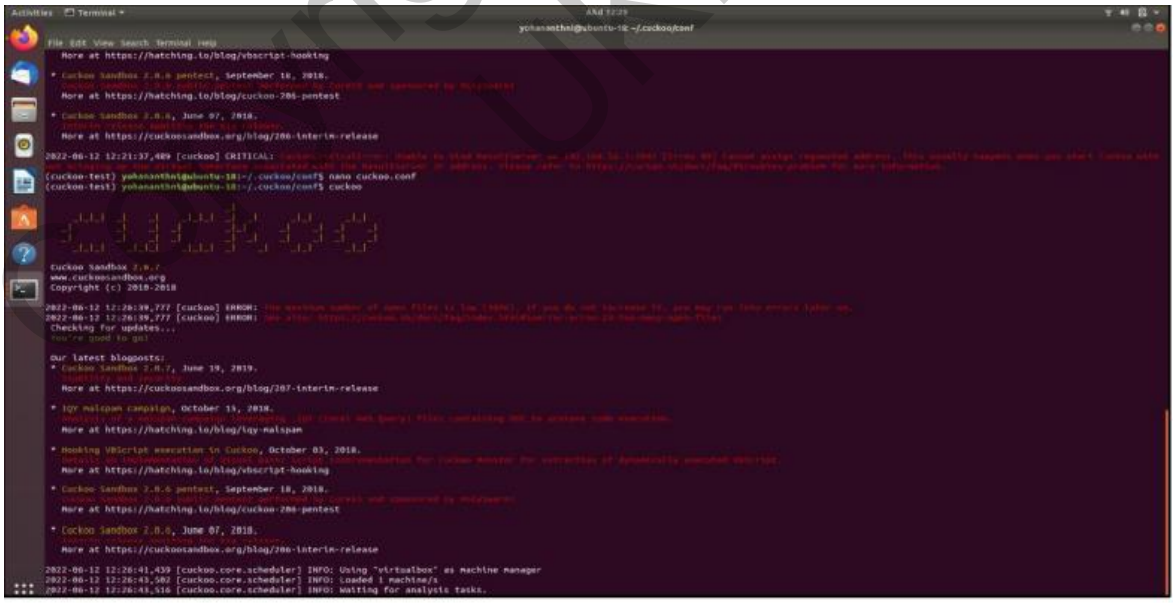
Rajah 7 : Folder Downloads

Pengguna akan menggunakan Cuckoo Snadbox untuk membuat analisis. Pengguna perlu mulakan tiga terminal. Terminal pertama untuk mulakan cuckoo rooter seperti Rajah 8.



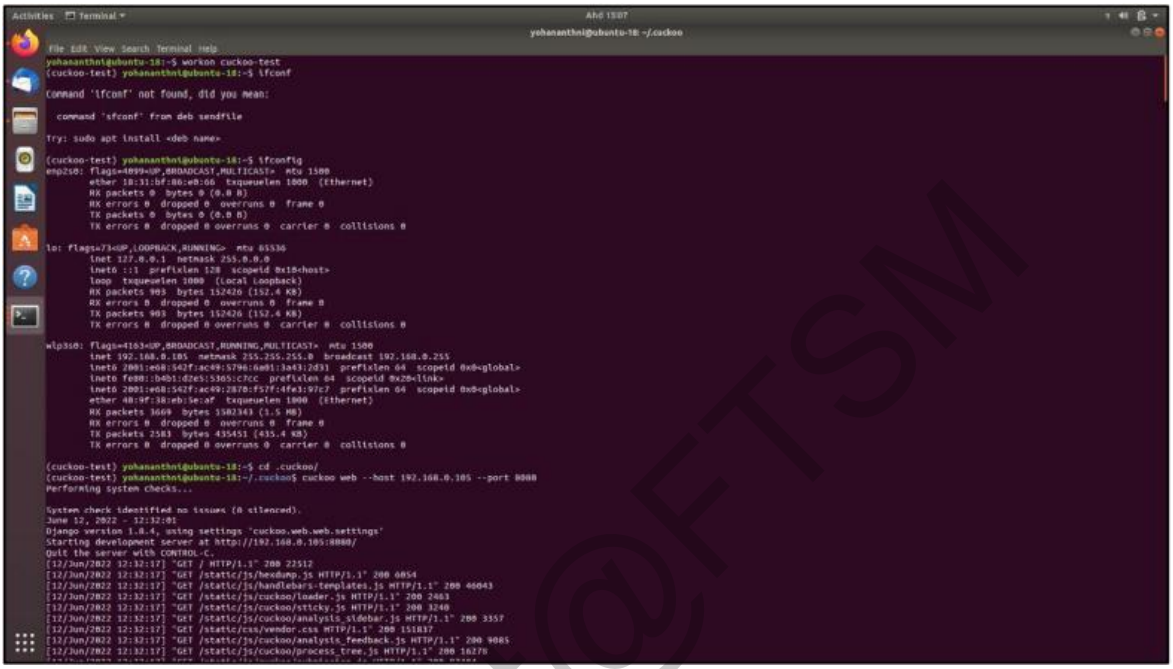
Rajah 8 : Cuckoo Rooter

Terminal kedua untuk mulakan Cuckoo seperti Rajah 9.



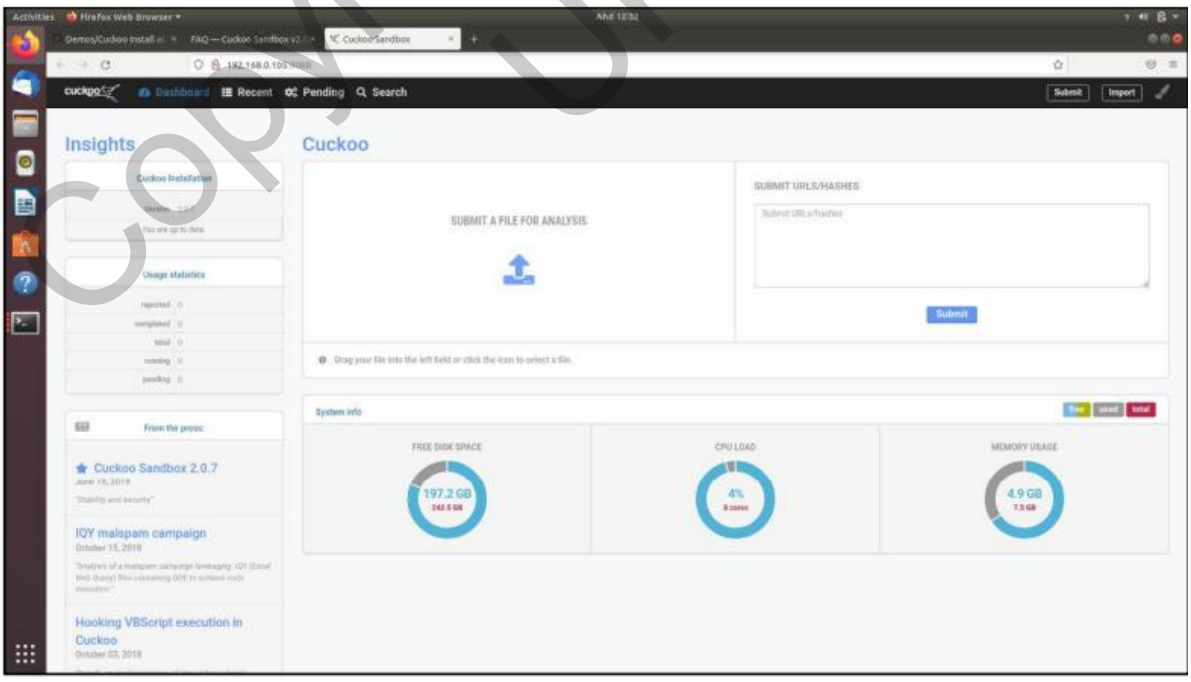
Rajah 9 : Cuckoo

Terminal ketiga untuk mulakan Cuckoo Web seperti Rajah 10.

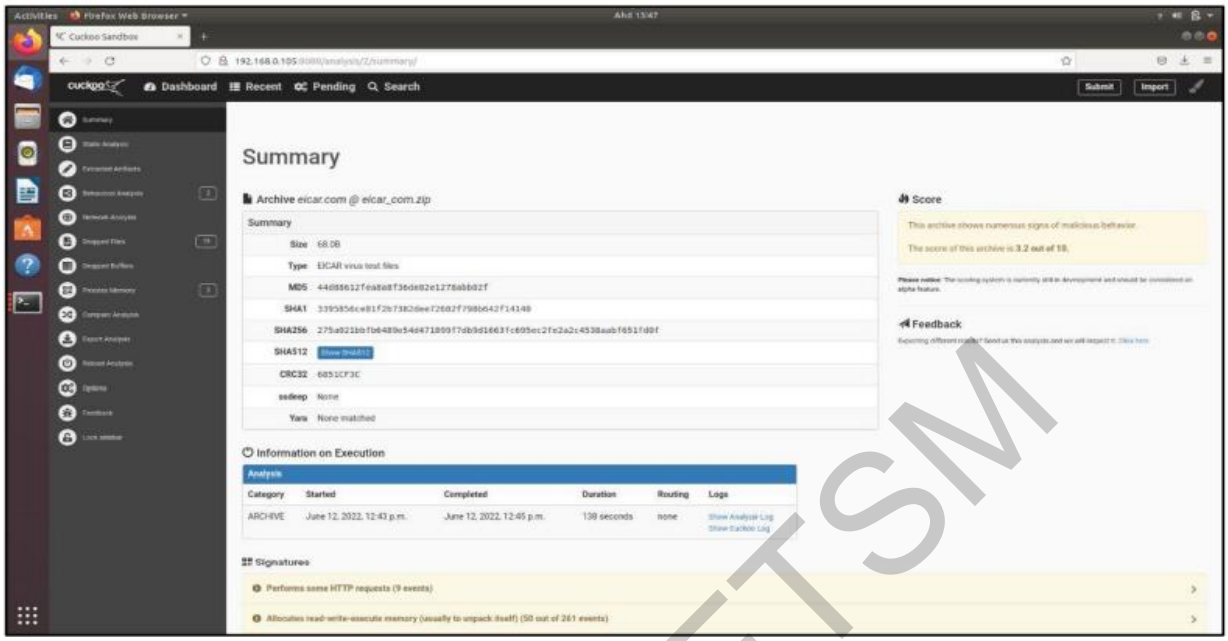


Rajah 10 : Cuckoo Web

Kemudian pengguna boleh akses Cuckoo Website dan mengendalikan analisis seperti Rajah 11 dan Rajah 12.



Rajah 11 : Dashboard Cuckoo Web



Rajah 12 : Analisis Perisian Hasad

6 KESIMPULAN

Secara keseluruhannya, projek ini mencadangkan sistem pengumpulan perisian hasad secara automatik menggunakan honeypot berasaskan awan yang boleh diguna pakai oleh organisasi atau individu. Laporan ini juga memperincikan fasa perancangan dan reka bentuk pembangunan sistem ini. Selanjutnya menjelaskan tentang fasa pembangunan sistem. Akhirnya, fasa pengujian juga dijalankan untuk memastikan sistem yang dibangunkan memenuhi keperluan.

Berdasarkan kekangan yang dikenal pasti, kelemahan dalam pembangunan sistem ini boleh diperbaiki dan ditambah baik pada masa hadapan. Cuckoo sandbox boleh dipasangkan dalam awan dan mengintegrasikannya dengan Honeypot. Sistem ini juga boleh ditambah baik dari segi keselamatan dan rangkaian. Selanjutnya, bahasa yang digunakan dalam sistem ini boleh ditambah dan diperluaskan lagi kerana sistem ini hanya menggunkanan satu bahasa iaitu Bahasa Inggeris. Secara keseluruhannya, sistem ini boleh ditambahbaik pada masa akan datang bagi memaksimumkan fungsinya dalam persekitaran awan.

Projek sistem pengumpulan perisian hasad secara automatik menggunakan honeypot berasaskan awan ini dibangunkan supaya dapat menyelesaikan masalah kos tinggi dalam

masa yang sama menghasilkan tenaga kerja yang mempunyai kemahiran dalam analisis perisian hasad. Akhir sekali, diharap sistem ini dapat diguna pakai oleh organisasi dan individu.

7 RUJUKAN

Kmety, M. (2020, July 2). Deploying T-pot — The all in one honeypot platform on AWS EC2.Medium. https://medium.com/@mkmety/deploying-t-pot-the-all-in-one-honeypot-platform-on-aws-ec2-33f019c645fb . [10 April 2022].

Linuxize. (2020). How to Upgrade Debian 10 Buster to Debian *11* Bullseye. https://linuxize.com/post/how-to-upgrade-debian-10-to-debian-11/ . [10 April 2022].

Lou Bichard. (2021, June 28). Which AWS region is cheapest? A costing report. Open Up The Cloud. https://openupthecloud.com/which-aws-region-cheapest/ . [8 Disember 2021].

Telekom-security/tpotce. (2022). GitHub. https://github.com/telekom-security/tpotce . [10 April 2022].

Von Andreas. (2020). Setting up T-pot in AWS cloud (2020). Andreas Wienes. https://www.andreaswienes.de/cybersecurity/setting-up-t-pot-in-aws-cloud-2020/ . [10 April 2022].

Von Andreas. (2020). Analyzing honeypot data after 2 weeks. Andreas Wienes. https://www.andreaswienes.de/cybersecurity/analyzing-honeypot-data-after-2-weeks/ . [22 April 2022]

Zach Martin. (2018, August 29). A honeypot guide: Why researchers use honeypots for malware analysis. The Mac Security Blog. https://www.intego.com/mac-security-blog/a-honeypot-guide-why-researchers-use-honeypots-for-malware-analysis/ . [11 November 2021].

Yohananthni A/P Ravichandran (A173453)
Wan Fariza Binti Fauzi
Fakulti Teknologi & Sains Maklumat,
Universiti Kebangsaan Malaysia