PLATFORM PENGESANAN PERISIAN HASAD UNTUK SISTEM OPERASI WINDOWS BERDASARKAN KOTAK PASIR, ANALISIS MEMORI DAN FUZZY HASHING

THIVYA POOVANANDRAN
KHAIRUL AKRAM BIN ZAINOL ARIFFIN

Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Perisian berbahaya telah wujud sejak awal komputer, tetapi kecanggihan dan penemuan perisian hasad telah berkembang dari masa ke masa. Gelombang ransomware baru-baru ini telah mencetuskan perhatian kearah perisian berbahaya, yang mungkin mempengaruhi individu, perniagaan, perkhidmatan awam, dan agensi keselamatan. Perisian hasad ditakrifkan sebagai perisian yang menjalankan tujuan jahat penyerang. Analisis perisian hasad pula adalah proses menentukan tingkah laku dan niat sampel perisian hasad. Untuk mengembangkan teknik pengesanan dan penyingkiran yang berkesan, prosedur ini diperlukan. Namun begitu, didapati bahawa beberapa tindakan berbahaya hanya diaktifkan dalam situasi yang ditentukan (mis., pada hari tertentu, ketika fail tertentu ada, atau ketika perintah tertentu diterima). Sebilangan besar antivirus standard tidak berkesan dalam mengesan perisian hasad yang tidak diketahui, mengakibatkan perisian hasad tersebut tetap aktif dan tidak ditemui. Tambahan pula, analisis tingkah laku memerlukan masa yang lama dan mempunyai kadar penggera palsu yang tinggi. Untuk mengatasi masalah ini, teknologi pengesanan malware berdasarkan fuzzy hashing telah diusulkan. Algoritma SSDEEP digunakan untuk menerapkan konsep fuzzy hashing. SSDEEP membolehkan pengguna mengenal pasti fail yang merupakan pendua fail lain. Ini akan digunakan untuk membandingkan hasil carian untuk kesamaan kandungan dengan pangkalan data perisian hasad yang terkenal. Ini membolehkan pengguna memperoleh gambaran yang lebih komprehensif mengenai aplikasi yang sedang disiasat dan menentukan tempoh masa tindakan mencurigakan tersebut berlaku. Tujuan penyelidikan ini adalah untuk menawarkan teknik analisis hibrid yang lebih baik untuk data perisian hasad dengan menggabungkan analisis tingkah laku dan memori untuk mengekstrak ciri yang lebih berguna. Untuk melindungi institusi ini dan orang awam daripada serangan perisian hasad, isu ini mesti diakui secepat mungkin, sebaiknya sebelum melakukan tindakan berbahaya.

1 PENGENALAN

Perisian hasad ialah satu set arahan atau atur cara yang dilaksanakan pada sistem komputer dan menyebabkan mesin melaksanakan perkara yang diingini oleh penyerang (Ed Skoudis dan Lenny Zeltser,2004. Serangan jenis ‘targeted attack’ adalah serangan yang disasarkan khas kepada individu, kumpulan, laman web atau perkhidmatan tertentu (Search Security,2020). Serangan jenis ini selalunya menggunakan kaedah serupa yang terdapat dalam ancaman dalam talian tradisional seperti e-mel atau jaringan halaman web yang mengadungi perisian hasad. Motif utama serangan terhadap organisasi tersebut adalah untuk memperoleh data data peribadi dan untuk mencuri harta intelek (Security Magazine, 2021). Antara contoh perisian hasad adalah virus komputer, cecacing, dan kuda trojan. Pengendalian sebilangan besar fail perisian hasad secara manual adalah mustahil. Akibatnya, pendekatan

berasaskan tandatangan digunakan terutamanya oleh sistem pengesanan anti-virus dan sistem pencerobohan perisian hasad (IDS). Turutan bait yang unik diperoleh daripada perisian hasad yang direkodkan dan digunakan untuk mengesan fail berbahaya yang serupa dalam rekod perisian hasad berasaskan tandatangan. Namu begitu, pengodam siber boleh menukar tandatangan perisian hasad dengan kaedah kekeliruan seperti pengubahsuaian kod, penggantian arahan, penugasan semula daftar dan pemasukan kod mati untuk menghalang pengesanan oleh perisian anti-virus. Akibatnya, kaedah pengenalan perisian hasad berdasarkan tandatangan ini tidak dapat mengenal pasti perisian hasad yang baru, dan ia mudah tertipu oleh perisian hasad yang menggunakan teknik pengeliruan, atau penyulitan (Ye, Y, Li, T, Adjeroh dan D.Iyengar, S.S,2017). Dalam kertas penyelidikan ini, platform untuk mengesan perisian hasad berdasarkan kotak pasir (Cuckoo), analisis memori dan 'fuzzy hash' (SSDEEP) dicadangkan. Teknik analisis memori dipilih untuk mengatasi had analisis statik dan dinamik. Ini kerana analisis memori ialah cara terbaik untuk menemui aktiviti berniat jahat dalam sistem kerana 'volatile memory' mengekalkan kandungannya selagi belum 'power off''. Algoritma 'fuzzy hash' dan analisis dalam bentuk alat sumber terbuka yang dipanggil ssdeep akan diimplementasikan untuk mengenal pasti dua fail yang mungkin hampir salinan antara satu sama lain yang mungkin tidak dilakukan oleh kaedah 'traditional hash'.

2 PENYATAAN MASALAH

Terdapat kekangan yang dihadapi dalam pelaksanaan projek ini iaitu kurang pengetahuan pengaturcaraan dalam 'pyhton'. Oleh itu, pembelajaran kendiri untuk bahasa pengaturcaraan tersebut harus dilaksanakan dengan masa yang ditetapkan.Selain itu, kurang pengetahuan untuk mengatasi ralat pemasangan kotak pasir Cuckoo. Ini telah menyebabkan kelemahan besar untuk melengkapkan keseluruhan platform pengesanan perisian hasad. Oleh itu, pengguna tidak mendapat pengalaman menggunakan platform yang dicadangkan pada fasa perancangan.

3 OBJEKTIF KAJIAN

Plaform pengesanan perisian hasad berdasarkan kotak pasir, analisis memori dan fuzzy hashing telah diusul untuk mencapai beberapa objektif seperti berikut:

1. Mengekstrak ciri berasaskan memori yang boleh menyatakan aktiviti dan ciri perisian hasad dalam sistem.
2. Mewujudkan platform pengesanan perisian hasad yang mampu mengesan perisian hasad yang diubah suai tandatangannya dalam sistem.

4 METOD KAJIAN

Model SDLC digunakan dalam pembangunan projek ini ialah Model Air Terjun.Model ini adalah relevan kepada projek ini kerana tidak akan ada pertindihan antara peringkat kerana fasa. Semua fasa adalah 7 berturutan dimana output fasa pertama mengalir ke fasa kedua dan seterusnya linear. Ia memerlukan setiap langkah diselesaikan sebelum beralih ke langkah seterusnya. Metodologi ini terdiri daripada 5 fasa iaitu fasa perancangan, fasa analisis, fasa reka bentuk, fasa implementasi dan fasa pengujian..

4.1 Fasa Perancangan

Fasa perancangan merupakan fasa penting dalam pembangunan platform pengenalan perisian hasad ini, dimana perancangan dalam membangunkan platform tersebut adalah jelas dan kajian awal terhadap sistem ditelitikan. Isu permasalahan yang terlibat dengan projek yang akan dibangunkan akan dikenalpasti pada tempoh ini. Dalam fasa ini juga, saya akan mengenalpasti tujuan dan langkah untuk membina sistem ini. Selain itu, skop dan objektif projek juga dibincangkan dalam fasa ini.

4.2 Fasa Analisis

Fasa analisis adalah sangat penting bagi mengenal pasti kelemahan yang dihadapi oleh platform semasa. ‘Host Based Intrusion Detection System (HIDS)’ sedia ada yang telah dikaji akan dijadikan sebagai rujukan bagi memudahkan maklumat yang dikumpul dianalisis. Tujuan mengkaji sistem ini adalah untuk membanggunkan sebuah sistem yang dapat memenuhi keperluan dan kehendak semasa pengguna. Selain itu, pengumpulan informasi tentang memori analisis dan kotak pasir juga dilakukan dalam fasa ini. Isi kandungan projek juga dikenalpastikan dalam fasa ini.

4.3 Fasa Reka Bentuk

Spesifikasi keperluan yang dikumpul pada fasa satu dikaji dan digunakan dalam reka bentuk sistem. Alat yang digunakan untuk projek yang diusul akan dimuktamadkan. Bagi kotak pasir, kotak pasir Cuckoo akan digunakan. Seterusnya,Votaliti akan digunakan sebagai tool analisis memori dan algoritma ‘fuzzy hash’ Sseep akan dilaksanakan pada platform yang dicadangkan.

4.4 Fasa Implementasi

Dengan adanya input darireka bentuk sistem, platformpengenalan malware dibangunkan secara berperingkat. Platform tersebut dibangunkan dengan phyton dan Ssdeep. Pembangunan platform akan mula dengan menguji the sampel fail perisian hasad dalam kotak pasir. Analisis memori akan menjalankan forensik memori untuk menyiasat dan mengenal pasti serangan atau tingkah laku berniat jahat. Berdasarkan pengekstrakan analisis, ‘fuzzy hash’ akan dilakukan untuk membandingkan persamaan tandatangan perisian hasad.Kesemua kaedah seterusnya digabung dan dijadikan satu platform yang lengkap untuk mengesan perisian hasad dalam Sistem Pengendalian Windows.

4.5 Fasa Pengujian

Semua unit yang dibangunkan akan disatukan ke dalam sistem selepas menguji setiap unit. Integrasi keseluruhan sistem akan diuji untuk memastikan tiada sebarang kesalahan atau kegagalan. Sistem ini akan diuji sama ada dapat mencapai objektif atau tidak.

5 HASIL KAJIAN

Bahagian ini akan membincangkan hasil yang didapati daripada pembangunan platform pengesanan perisian hasad berdasarkan kotak pasir Cuckoo, memori analisis dan fuzzy hashing. Oleh itu, penerangan secara mendalam tentang reka bentuk,implementasi dan pengujian platform akan diperihalkan dalam bahagian ini.

5.1 REKA BENTUK DAN SENI BENI

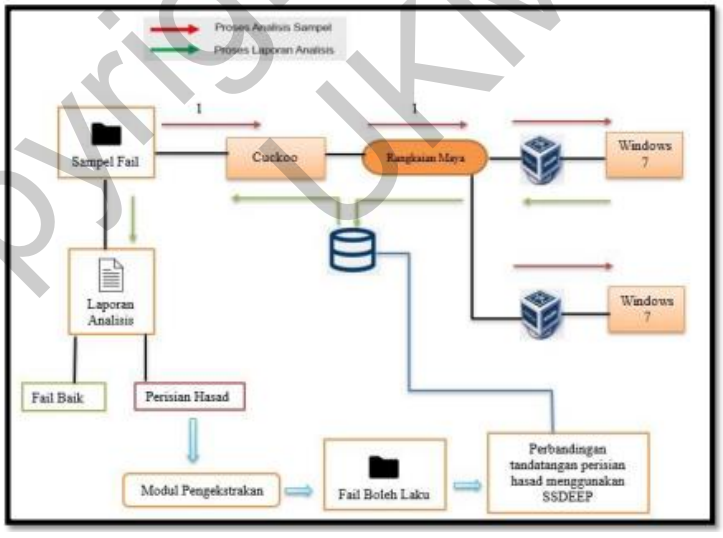
Fungsi utama bab spesifikasi reka bentuk ini adalah untuk menghasilkan garis panduan dan mencipta penerangan yang jelas tentang keseluruhan pembangunan sistem untuk memenuhi objektif dan keperluan sistem yang telah didokumentasikan.Spesifikasi reka bentuk akan

dilakukan untuk mengimbangi keperluan dan keupayaan yang boleh dicapai. Ini akan membantu untuk menghasilkan pembangunan dan rancangan ujian (OfniSystems.com, 2020). Skop reka bentuk sistem ini akan fokus kepada aspek berikut.

1. Reka bentuk seni bina
2. Antara muka sistem dan pangkalan data
3. Algoritma yang digunakan untuk menyediakan fungsi sistem

a) Seni Bina Pelayan

Berdasarkan rajah 1.1, penggunaan dan perlaksanaan modul analisis akan bermula setelah penyerahan fail diserahkan ke dalam platform pengesanan perisian hasad. Seterusnya, sampel fail tersebut akan dianalisis dalam kotak pasir Cuckoo. Cuckoo terdiri daripada perisian pengurusan pusat, yang mengendalikan pelaksanaan dan analisis sampel perisian hasad. Kotak pasir Cuckoo terdiri daripada 2 peranti. Ia terutamanya hos Linux Ubuntu yang kemudiannya mengandungi mesin Windows 7 bersarang. Hos Ubuntu mempunyai pakej Cuckoo utama yang dipasang padanya yang berasaskan python, bersama-sama dengan beberapa kebergantungan yang dikonfigurasikan untuk menggunakan ciri modular Cuckoo.

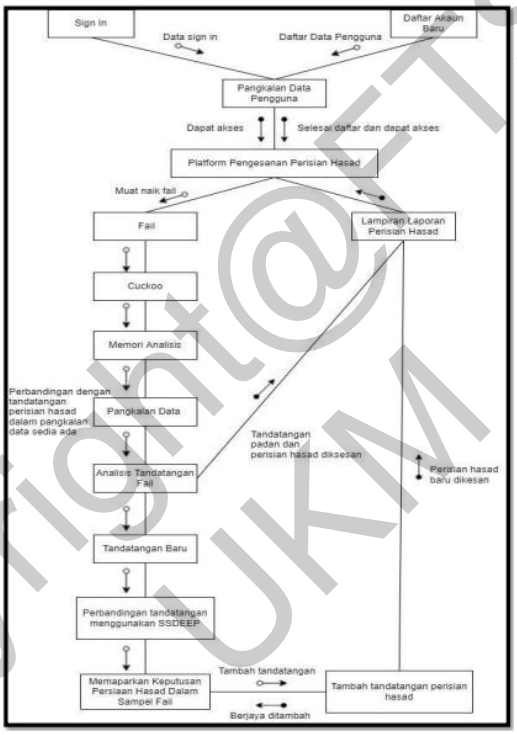


Rajah 1.1 Seni Bina Modul Analisis, Mesin Maya dan Fuzzy Hashing Bahagian Pelayan

Pada hos Ubuntu, VirtualBox dipasang dan tetamu Windows 7 dibina. Mesin Windows 7 mempunyai ejen Cuckoo yang dipasang padanya yang membolehkan kedua-dua mesin berinteraksi antara satu sama lain.Pada mesin hos, sampel fail boleh dimuat naik kepada mesin tetamu menggunakan platform yang dibina uang akan menjalani analisis dalam

Cuckoo. Langkah seterusnya ialah menganalisis longgokan memori dengan mengunakan alat Volatility dan modul pengekstrakan dilakukan dan fail boleh laku tersebut akan melalui proses perbandingan tandatangan perisian hasad menggunakan SSDEEP. Ini ialah alat untuk pengkomputeran rekursif dan padanan Context Triggered Piecewise Hashing.Proses ini akan membandingkan fail dan mengira skor padanan antara dua tandatangan 'hashes'. Hasil output tersebut dapat mengenal pasti fail perisian hasad yang diubah suai.Kemudian tandatangan perisian baru ini akan dikemas kini dalam pangkalan data sistem.

b) Carta Struktur

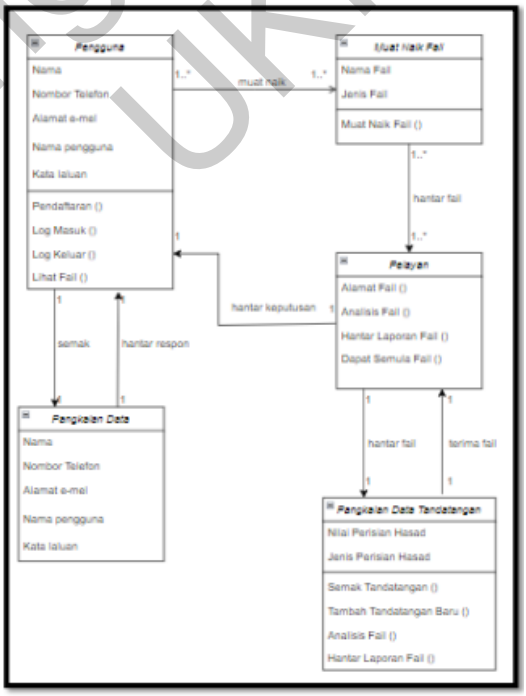


Rajah 1.2 Carta Struktur Platform Pengesanan Perisian Hasad

Rajah 1.2 menerangkan keseluruhan proses dari titik permulaan platform hingga akhir proses. Untuk menggunakan platform pengesan perisian hasad, pengguna dikehendaki sama ada memasukkan maklumat mereka atau membuat akaun baharu untuk log masuk. Kemudian, maklumat tersebut akan disemak oleh pangkalan data pengguna dan akses akan diberikan kepada pengguna untuk menggunakan sistem. Setelah pengguna memuat naik fail sampel untuk dianalisis, fail tersebut akan diarahkan ke Kotak Pasir Cuckoo. Seperti yang dinyatakan sebelum ini dalam bab sebelumnya, Kotak Pasir Cuckoo ialah alat yang digunakan untuk melancarkan perisian hasad dalam persekitaran yang selamat dan terpencil.Kotak pasir kemudiannya akan merekodkan aktiviti fail sampel dan kemudian memerhatikan aktiviti yang

cuba dilakukan oleh perisian hasad semasa berada dalam persekitaran selamat ini. Proses analisis seterusnya ialah analisis memori, di mana proses ini menangkap '*running memory'* peranti dan kemudian menganalisis output yang ditangkap untuk bukti perisian berniat jahat dalam fail sampel. Dalam pembangunan projek ini, Volatiliti digunakan sebagai alat pilihan untuk analisis memori. 'Proses seterusnya ialah platform akan menyemak tandatangan fail sampel dengan pangkalan data tandatangan perisian hasad sedia ada untuk melihat sama ada terdapat padanan tandatangan. Jika ya, platform akan terus menjana laporan kepada pengguna yang mengatakan fail sampel itu berniat jahat. Jika tiada padanan dan fail sampel dianggap sebagai fail tandatangan baharu, platform akan menganalisis sampel fail menggunakan SSDEEP. Ini dilakukan untuk mengesan perisian hasad dengan menyiasat integriti dan persamaan fail sampel. Kaedah ini membahagikan sampel fail kepada bilangan blok berdasarkan kandungan fail tersebut dan persamaan antara dua fail (fail sampel semasa dan fail perisian hasad sebelumnya) dikira. Oleh itu, jika persamaan dikesan, sistem akan membuat kesimpulan bahawa sampel fail adalah berniat jahat. Kemudian, tandatangan perisian hasad baru akan ditambahkan pada pangkalan data tandatangan perisian hasad dan laporan analisis akan dihantar kepada pengguna.

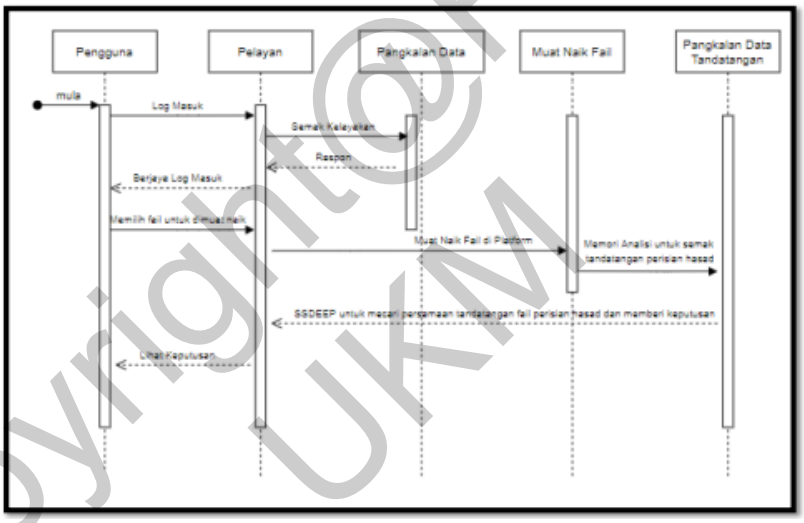
c) Rajah Kelas



Rajah 1.3 Rajah Kelas Platform Pengesanan Perisian Hasad

Rajah 1.3 merujuk kapada rajah kelas pangkalan data platform pengesanan perisian hasad yang igin dibangunkan. Melalui rajah tersebut, dapat ditunjukkan hubungan set entiti (yang disimpan dalam pangkalan data. Berdasarkan pengkhususan proses yang diterangkan dalam seni bina, proses yang paling utama sebelum analisis dijalankan adalah mendaftar akaun dalam sistem dan muat naik sampel fail. Tandatangan fail tersebut adalah unik yang membezakan atau rujukan kepada satu-satu proses. 51 Fail ini seterusnya akan diturunkepada entiti Pelayan dan akan dikaitkan entiti Pangkalan Data Tandatangan untuk proses penambahan tandatangan perisian hasad baru ke dalam pangkalan data. Jadual 4.1 akan menunjukkan fungsi dan hubungan di antara jadual dan entiti yang terdapat dalam pangkalan data Cuckoo

d) Rajah Urutan



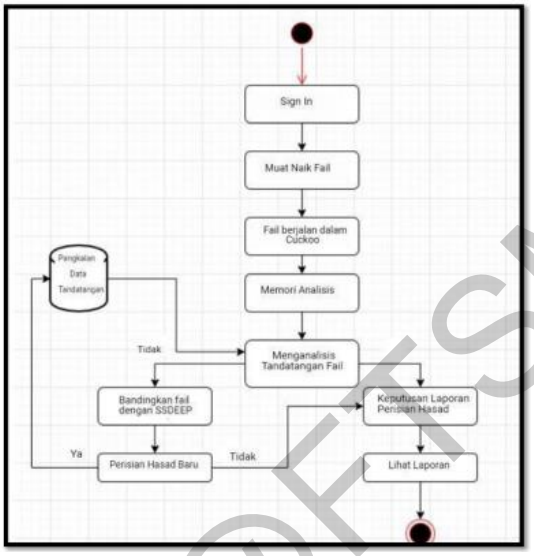
Rajah 1.4 Rajah Urutan Platform Pengesanan Perisian Hasad

Berdasarkan rajah di atas, dapat dilihat scenario pertama adalah di mana pengguna perlu log masuk ke dalam sistem menggunakan informasi yang ditetapkan.Pelayan akan menyemak kelayakan pengguna tersebut dalam pangkalan data kemudian mengantar respon kepada pengguna.Seterusnya, pengguna boleh muat naik sampel fail dalam sistem untuk dianalisis dan proses analasis perisian hasad akan dilakukan.SSDEEP akan digunakan untuk mencari persamaan tandatangan fail dan memberi keputusan laporan analisis.Laporan tersebut akan dipaparkan dalam sistem kepada pengguna.

e) Rajah Mesin Keadaan

Reka bentuk algoritma adalah satu kaedah atau proses yang diperlukan untuk penyelesaian sesuatu masalah. Untuk projek ini, algoritma akan digunakan dalam mencapai objektif projek

iaitu algoritma rajah mesin keadaan (State Machine Diagram). Rajah mesin keadaan digunakan untuk menerangkan tingkah laku sistem, subsistem, komponen dan kelas platform perisian hasad yang hendak dibina



Rajah 1.5 Rajah Mesin Keadaan Platform Pengesanan Perisian Hasad

Berdasarkan Rajah 1.5, algoritma analisis ini adalah ringaksan dari Rajah 3.5. Proses ini dimulakan dengan pengguna memasukkan maklumat mereka atau membuat akaun baharu untuk log masuk. Seterusnya, setelah pengguna memuat naik fail sampel untuk dianalisis, fail tersebut akan diarahkan ke Kotak Pasir Cuckoo dan kemudiannya akan merekodkan aktiviti fail sampel dan menganalisis aktiviti yang dilakukan oleh fail tersebut sekiranya fail itu mengadungi perisian hasad. Proses analisis seterusnya ialah analisis memori menggunakan alat Volatiliti. Proses seterusnya ialah platform akan menyemak tandatangan fail sampel dengan pangkalan data tandatangan perisian hasad sedia ada untuk melihat sama ada terdapat padanan tandatangan. Jika ya, platform akan terus menjana laporan kepada pengguna yang mengatakan fail sampel itu berniat jahat. Jika tiada padanan dan fail sampel dianggap sebagai fail tandatangan baharu, platform akan menganalisis sampel fail menggunakan SSDEEP. Jika persamaan dikesan, sistemakan membuat kesimpulan bahawa sampel fail adalah berniat jahat. Kemudian, tandatangan perisian hasad baru akan ditambahkan pada pangkalan data tandatangan perisian hasad dan analisis algoritma ini tamat apabila laporan analisis dihantar kepada pengguna.

f) Antara Muka Platform

Reka bentuk antara muka berfungsi sebagai medium interaksi antara sistem dan pengguna. Berikut adalah rajah antara muka yang dibangunkan berdasarkan keperluan platform dan bersifat mesra pengguna.

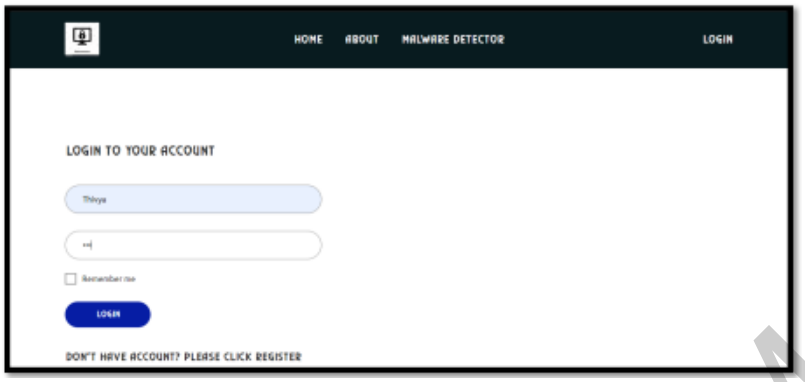
1. **Pendaftaran Akaun Baru (*Create Account*)**

Pengguna perlu daftar akaun baru dengan mengisi butiran nama, e-mel, kata laluan yang dingini. Hal ini kerana, ciri muat naik fail dan menerima keputusan pengesanan hanya boleh dilakukan oleh pengguna yang mempunyai akuan berdaftar untuk platform tersebut.

Rajah 1.6 Antara Muka Pendaftaran Akaun Baru

2. **Log Masuk dan Log Keluar (*Log in and Log Out*)**

Pengguna boleh log masuk menggunakan nama pengguna dan kata laluan yang mereka telah didaftar. Platform ini akan membenarkan pengguna log masuk ke dalam sistem jika nama pengguna dan kata laluanya adalah betul manakal jika sistem mengesan kata laluan pengguna adalah salah maka sistem aplikasi akan mengeluarkan mesej “wrong name/password combination”.



Rajah 1.7 Antara Muka Log Masuk dan Log Keluar

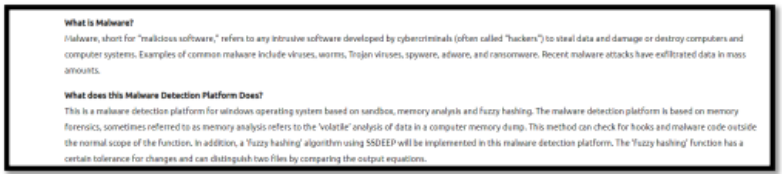
3. Halaman Utama Platform (*Home*)

Apabila pengguna log masuk ataupun layari laman web platform ini, mereka akan dibawa ke halaman utama platform iaitu Home. Di sini, pengguna akan melihat pilihan butang lain di bahagian atas seperti Home, About, Malware Detector dan Log In. Maklumat tentang definisi keselamatan siber dalam sektor teknologi maklumat juga dipaparkan di bahagian halaman utama ini.

Rajah 1.8 Antara Muka Halaman Utama

4. Informasi Platform Pengesanan Perisian Hasad (*About*)

Pengguna boleh meneroka bahagian ini untuk membaca dan mendapatkan maklumat tentang tujuan platform pengesanan persisan hasad ini dibangunkan.



Rajah 1.9 Antara Muka Informasi Platform Pengesanan Perisian Hasad

5. Muat Naik Fail dan Menerima Keputusan Pengesanan (*Malware Detector*)

Pengguna boleh muat naik fail di bahagian ini dan mendapatkan keputusan pengesanan perisian hasad untuk fail tersebut.

Rajah 1.10 Antara Muka Muat Naik Fail dan Menerima Keputusan Pengesanan

5.2 PROSES PEMBANGUNAN (*back-end)*

Dalam fasa pembangunan ‘back-end’, terdapat beberapa proses yang akan dijalankan. Proses tersebut termasuklah proses pemasangan mesin maya Oracle VM VirtualBox, pemasangan sistem Ubuntu,dan pengubahsuaian konfigurasi sistem Cuckoo Sandbox.

a) Oracle VM VirtualBox dan Sistem Operasi Ubuntu

Dalam projek ini, mesin maya dipasang untuk menggunakan sistem pengendalian Ubuntu dalam komputer peribadi yang sama. Untuk memasang VirtualBox pada Windows 10, ia boleh dimuat turun terus dari halaman web Oracle. Di bawah bahagian "VirtualBox binari", pautan hos Windows harus dipilih dan klik pada fail VirtualBox-Win.exe untuk melancarkan pemasang.Seterusnya. kosongkan pilihan yang tidak mahu gunakan dan klik butang ‘Next’ untuk meneruskan pemasangan VirtualBox pada Windows 10. Setelah a melengkapkan langkah, perisian akan menyelesaikan pemasangan dan akan dilancarkan secara automatik. Seterusnya, penyediaan keperluan sistem operasi Ubuntu dikonfigurasikan. Fail sistem operasi perumah yang dalam bentuk salinan cakera padat atau dalam bahasa Inggeris, optical disc image (ISO) perlulah dimuat naik. Dalam projek ini, sistem operasi Ubuntu versi 18.04.6 LTS telah dipilih. Buat masa ini, Ubuntu 18.04 merupakan versi paling stabil bagi penggunaan sistem sandbox pilihan projek ini iaitu Cuckoo Sandbox 64 versi 2.0.7. Adalah tidak digalakkan untuk menggunakan Ubuntu dengan versi yang lebih tinggi daripada 18.04 kerana Cuckoo Sandbox buat masa kini hanya mempunyai integrasi penuh kepada Ubuntu 18.04.

Antara langkah yang dilakukan dalam proses konfigurasi Ubuntu 18.04.6 dalam mesin maya :

a) Memberi Ubuntu 18.04.6 sebagai nama sistem operasi maya dan versi Ubuntu 64-bit dipilih.

b) Bawah kategori Settings > General> Advanced > Shared Clipboard, ciri 'Bidirectional' dipilih.

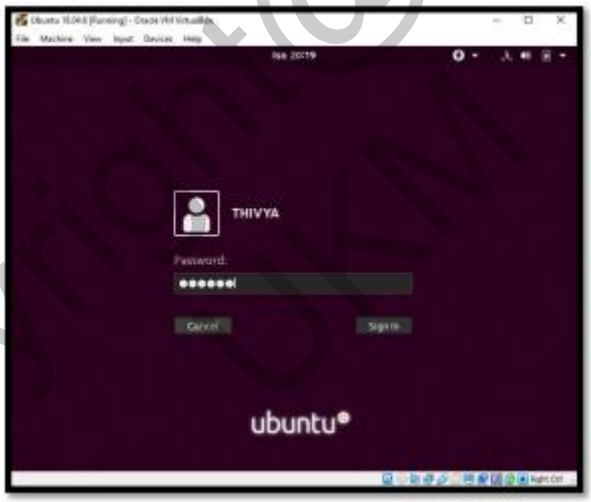
c) Memperuntukkan 2GB RAM kepada sistem operasi maya.

d) Memilih ciri diperuntukkan secara dinamik untuk mencipta cakera keras maya. Saiz yang dipilih ialah 10 GB.

e) Bawah kategori Settings > General> Storage > Controller IDE, pilih ikon cakera padat dan memberikan laluan arah ISO fail yang dimuat turun.

f) Klik sistem operasi maya Ubuntu 18.04.6 dan pilih bahasa Inggeris dan klik butang 'Install Ubuntu'

g) Tetapkan nama pengguna, nama komputer dan kata laluan h) Klik 'Restart Now' untuk mulakan semula komputer

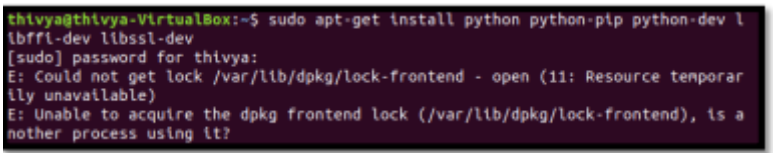


Rajah 1.11 Halaman Ubuntu 18.04.6

b) Kotak Pasir Cuckoo

Setelah proses penyediaan dan pemasangan pakej kebergantungan Cuckoo telah selesai, maka proses pemasangan Cuckoo akan dimulakan. Langkah pertama memerlukan beberapa pakej perisian dan perpustakaan. Komponen hos Cuckoo ditulis sepenuhnya dalam Python. Oleh itu, ia dikehendaki memasang versi Python yang sesuai iaitu Python 2.7.

Ralat dihadapi:



Rajah 1.12 Ralat Pemasangan Repositori Apt

Rajah 1.12 Ralat Pemasangan Repositori Apt Ralat ini berlaku kerana beberapa program lain cuba mengemas kini Ubuntu. Apabila arahan atau aplikasi sedang mengemas kini sistem atau memasang perisian baharu, ia mengunci fail dpkg (pengurus pakej Debian). Penguncian ini dilakukan supaya dua proses tidak mengubah kandungan pada masa yang sama kerana boleh menjadikan sistem rosak.

Kaedah penyelesaian:

Semak sama ada beberapa program lain sedang menjalankan kemas kini sistem atau memasang program. Memandangkan baris arahan digunakan, perlu juga semak sama ada aplikasi seperti Pusat Perisian dan Pengemas Kini Perisian sedang menjalankan sebarang kemas kini/pemasangan. Dalam proses pemasangan yang telah dijalankan, didapati tiada aplikasi seperti itu berjalan. Oleh itu, langkah seterusnya iaitu semak semua tetingkap terminal terbuka dan lihat jika terdapat sebarang kemas kini yang sedang berjalan telah dilakukan. Dalam kes ini, terdapat situasi seperti itu berlaku. Justeru, untuk pengesahan, 70 arahan apt telah digunakan (pengurus pakej untuk mengendalikan perisian) untuk menyemak proses lain yang sedang berjalan. Baris arahan ini digunakan:

Rajah 1.13 Baris Arahan Apt

Didapati bahawa apt.systemd.daily menggunakan proses apt dan memerlukan beberapa minit masa untuk menyelesaikan proses kemas kini automatik. Dalam proses ini, ciri pemasangan automatik kemas kini juga telah ditutup.Langkah seterusnya diimplementasikan untuk menggunakan Antara Muka Web berasaskan Django dan untuk menggunakan PostgreSQL sebagai pangkalan data: **$ sudo apt-get install mongodb. $ sudo apt-get install postgresql libpq-dev**.Cuckoo menyokong kebanyakan penyelesaian Perisian Virtualisasi. Cuckoo telah disediakan untuk kekal sebagai modular yang mungkin dan sekiranya integrasi dengan

sekeping perisian hilang, ini boleh ditambah dengan mudah. Memandangkan VirtualBox telah pun dikonfigurasikan, arahan untuk memasang versi terkini VirtualBox pada mesin Ubuntu LTS adalah: **$ sudo apt-get** install virtualbox.Untuk membuang aktiviti rangkaian yang dilakukan oleh perisian hasad semasa pelaksanaan, diperlukan '*network sniffer'* yang dikonfigurasikan dengan betul untuk menangkap trafik dan membuangnya ke fail. Secara lalai Cuckoo menggunakan tcpdump iaitu penyelesaian sumber terbuka: **$ sudo apt-get install tcpdump apparmor-utils $ sudo aa-disable /usr/sbin/tcpdump**.Tcpdump memerlukan keistimewaan root tetapi dalam kajian ini, Cuckoo tidak perlu dijalankan sebagai root. Oleh itu, perlulah untuk menetapkan keupayaan Linux tertentu kepada binari: **$ sudo groupadd pcap $ sudo usermod -a -G pcap cuckoo $ sudo chgrp pcap /usr/sbin/tcpdump $ sudo setcap cap_net_raw,cap_net_admin=eip /usr/sbin/tcpdump**

Ralat dihadapi:

```
thivya@thivya-VirtualBox:~$ sudo groupadd pcap
thivya@thivya-VirtualBox:~$ sudo usermod -a -G pcap cuckoo
usermod: user 'cuckoo' does not exist
```

Rajah 1.14 Ralat Penetapan Keupayaan Linux

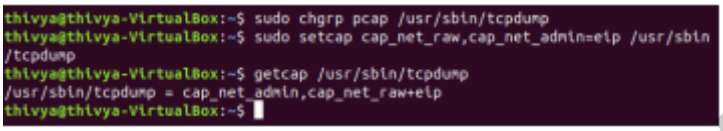
Kaedah penyelesaian:

```
thivya@thivya-VirtualBox:~$ sudo adduser cuckoo
[sudo] password for thivya:
Sorry, try again.
[sudo] password for thivya:
Adding user `cuckoo' ...
Adding new group `cuckoo' (1002) ...
Adding new user `cuckoo' (1001) with group `cuckoo' ...
Creating home directory `/home/cuckoo' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for cuckoo
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n]
thivya@thivya-VirtualBox:~$ sudo usermod -a -G cuckoo cuckoo
thivya@thivya-VirtualBox:~$
```

Rajah 1.15 Barisan Arahan 'adduser'

Barsian arahan usermod menambahkan pengguna ke kumpulan Linux. Bendera -a -G harus digunakan untuk menambah akaun pengguna sedia ada pada kumpulan. Sintaks untuk arahan usermod ialah: usermod -a -G nama pengguna nama kumpulan. Bendera -a memberitahu usermod untuk menambah pengguna pada kumpulan. Bendera -G menentukan nama kumpulan kedua yang anda ingin tambahkan pengguna. Untuk ralat ini, ia adalah kes yang memerlukan untuk mencipta pengguna baharu dan serta-merta menambah mereka pada

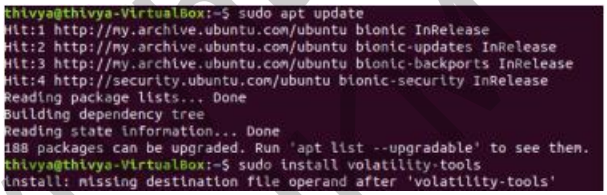
kumpulan. Di situlah arahan useradd masuk. Perintah useradd membenarkan untuk mencipta pengguna baharu dan dengan juga menggunakan pilihan -g, tambah pengguna ke kumpulan. Keputusan arahan terakhir boleh disahkan dengan barisan arahan :



Rajah 1.16 Keputusan Arahan Terakhir Keupayaan Linux Binari

Untuk projek ini, Volatility adalah alat yang mesti dilakukan untuk melakukan analisis pada pembuangan memori. Dalam kombinasi dengan Cuckoo, secara automatik boleh memberikan keterlihatan tambahan kepada pengubahsuaian mendalam dalam sistem pengendalian serta mengesan kehadiran teknologi rootkit yang terlepas daripada domain pemantauan Penganalisis Cuckoo.

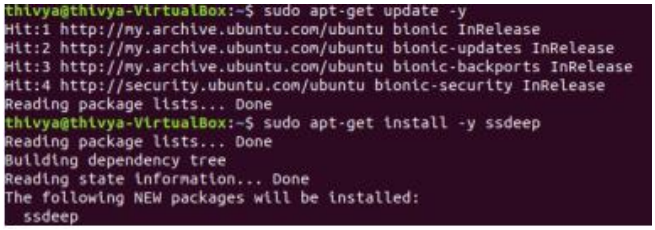
Ralat dihadapi:



Rajah 1.17 Ralat Pemasangan Volatility

Kaedah penyelesaian:

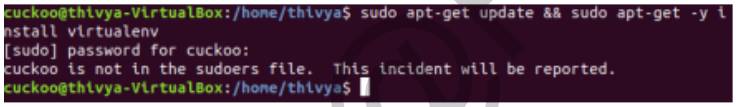
Barisan arahan pertama , **$ sudo apt-get** digunakan untuk memuat turun maklumat pakej daripada semua sumber yang dikonfigurasikan sebelum ini.Sumber sering ditakrifkan dalam fail /etc/apt/sources.list dan fail lain yang terdapat dalam direktori/etc/apt/sources.list.d.Jadi apabila menjalankan perintah kemas kini, ini berguna untuk mendapatkan maklumat tentang versi pakej yang dikemas kini atau kebergantungannya.Kedua, barisan arahan apt-get ‘Advanced Packaging Tool’ membenarkan pengguna memasang, mengalih keluar dan mengemas kini pakej pada sistem. Seterusnya perlu memasang pydeep untuk cincangan ssdeep fuzzy sampel:



Rajah 1.18 Rajah Pemasangan Pakej SSDEEP

PIP ialah pengurus pakej untuk python dalam mengendalikan pakej perisian yang dibangunkan menggunakan python.Berikut adalah barisan arahan untuk pemasangan PIP dan juga persekitaran maya: **$ sudo pip install -U pip setuptools $ sudo pip install -U cuckoo $ virtualenv venv $. venv/bin/activate (venv)$ pip install -U pip setuptools (venv)$ pip install -U cuckoo.**

Ralat dihadapi:



Rajah 1.19 Ralat Pemasangan Barsian Arahan Persekitaran Maya

Apabila cuba melaksanakan barisan arahan dengan keistimewaan root menggunakan sudo, ia menunjukkan mesej ralat kerana pengguna semasa tiada dalam fail ‘sudoers’.Ini ialah ciri keselamatan pada sistem Linux untuk menghalang pengguna biasa daripada meningkatkan perintah mereka kepada keistimewaan pentadbir. Kaedah penyelesaian untuk ralat ini ialah menambah pengguna kepada kumpulan sudo pada sistem berasaskan DEB (format pakej untuk pengedaran Ubuntu). Langkah pertama yang dinasihatkan untuk membuka terminal baris arahan dan log masuk ke akaun pengguna root dan taip : $ su -i. Kemudian, tambahkan pengguna ke kumpulan sudo. Dalam kes ini ia akan menambah pengguna cuckoo kepada kumpulan : # usermod -aG sudo cuckoo. Untuk membuat perubahan berkuat kuasa, perlu log keluar sepenuhnya dan log masuk semula. Walau bagaimanapun, walaupun selepas mencuba langkah ini, ralat masih muncul dan kebenaran telah ditolak.

5.3 PERLAKSANAAN PENGUJIAN

Jadual 1.1 Senarai Soalan Responden Pengujian Penggunaan Sistem

ID Ujian	Soalan
Soalan 1	Berjaya mencipta akaun baru untuk platform pengesanan perisian hasad
Soalan 2	Dapat melihat halaman sistem web yang mengadungi informasi tentang platform pengesanan perisisan
Soalan 3	Sampel fail perisian hasad dapat dipilih dan dimuat naik untuk tujuan analisis
Soalan 4	Mesin maya dapat berjalan dan berfungsi dengan baik setiap kali proses analisis dimulakan
Soalan 5	Sistem memberikan laporan yang lengkap dan consisten untuk setiap analisis.
Soalan 6	Antara muka sistem web mudah difahami.

Ujian penerimaan pengguna dilaksanakan bagi menguji sistem untuk melihat sama ada ianya dapat melaksanakan tugas yang sepatutnya berdasarkan perancangan projek. Ianya juga bertujuan untuk menguji kepatuhan terhadap kehendak pelanggan dan untuk mengesahkan sebarang perubahan yang telah dibuat terhadap keperluan yang asal. Seperti yang dilaporkan, seorang sahaja dipanggil untuk melakukan ujian. Pengguna ini diarahkan untuk menggunakan sistem yang mampu dibangunkan untuk menganalisis sampel fail. Pada akhir proses ini, sebuah rumusan maklum balas responden dilampirkan untuk melaporkan secara bertulis tentang hasil pengujian yang dijalankan.

Jadual 1.2 Rumusan Maklum Balas Responden Pengujian Penggunaan Sistem

ID Ujian	Sangat Setuju	Setuju	Agak Setuju	Kurang Setuju
Soalan 1	✓	-	-	-
Soalan 2	✓	-	-	-
Soalan 3	-	-	-	✓
Soalan 4	-	-	-	✓
Soalan 5	-	-	-	✓
Soalan 6	-	✓	-	-

Berdasarkan rumusan tersebut, pengguna kurang berpuas hati dengan kebolehan platform pengesanan perisian hasad ini. Dapat dilihat bahawa punca utama fungsi platform tersebut tidak dapat digunakan dengan sempurna adalah kerana '*back-end'* platform tidak berfungsi. Perkara ini telah memberikan pengalaman pengguna berkurang kerana tidak semua fungsi yang dijanjikan dapat digunakan. Dengan ini, masalah tersebut telah dikenal pasti dan

diajukan untuk tindakan penyelesaian dan secara rumusnya projek ini tidak menepati kriteria pengguna.

6 KESIMPULAN

Secara keseluruhannya, projek platform pengesanan perisian hasad berdasarkan kotak pasir, memori analisis dan ‘fuzzy hashing’ tidak dapat melengkapkan keperluan dalam proses usulan dan perancangan projek. Proses yang telah dijalankan termasuklah penghasilan projek, sorotan sastera berkaitan projek, mengenal pasti keperluan pengguna dan reka bentuk sistem. Hasil daripada ke semua proses tersebut telah didokumentasikan dalam laporan ini. Projek ini diusul untuk menangani masalah dalam keselamatan sistem komputer dan rangkaian yang berkaitan dengan menangani serangan daripada perisian hasad. Pembangunan projek ini adalah yang berasaskan platfom yang bermakna ianya integrasi beberapa sistem sumber terbuka dalam membangunkan sebuah sistem yang baru. Sistem utama yang digunakan dalam projek ini ada sistem Cuckoo Sandbox iaitu sebuah sistem pengujian yang dipakai untuk tujuan menganalisis perisian hasad secara terasing daripada sistem pengguna yang sebenar. Dengan proses analisis tersebut, pemantauan tingkah laku perisian hasad boleh dikenal pasti dan dapat melaporkan hasil analisis dengan selamat. Untuk projek ini, terdapat dua kumpulan pengguna yang telah dikenal pasti daripada kajian keperluan pengguna iaitu admin dan pengguna biasa. Admin merujuk kepada pengguna yang akan mengurus tetapan sistem, mempunyai kawalan penuh dan pengurus kepada perkara berkaitan dengan kepenggunaan dan keselamatan sistem analisis. Pengguna biasa pula merujuk kepada pengguna seperti pegawai keselamatan yang akan menggunakan sistem dalam menjalankan analisis sampel fail.

Dalam perlaksanaan dan pembangunan projek ini, dapat dirumuskan dua kekangan perlu dipertimbangkan, yang pertama kurang pengetahuan untuk mengatasi ralat pemasangan kotak pasir Cuckoo. Ini telah menyebabkan kelemahan besar untuk melengkapkan keseluruhan platform pengesanan perisian hasad. Oleh itu, pengguna tidak mendapat pengalaman menggunakan platform yang dicadangkan pada fasa perancangan. Kedua adalah keselamatan penuh sistem analisis dan fungsi pengesanan perjalanan mesin maya atau kotak pasir dalam perisian hasad. Walaupun sistem menjalankan sampel perisian hasad dalam persekitaran yang terasing, namun ianya masih tidak dapat menjamin sepenuhnya keselamatan terhadap perisian hasad tersebut. Sekiranya platform pengesanan perisian hasad ini telah dibangunkan

dengan berjaya, peluang untuk berlakunya pintasan terhadap sistem analisis kepada sistem hos adalah tinggi sekiranya tetapan keselamatan tidak di reka dengan baik. Oleh itu, pengetahuan yang tinggi dalam keselamatan sistem komputer dan rangkaian adalah diperlukan untuk melaksanakan pengerasan dalam sistem.

Bagi rancangan peningkatan masa hadapan, bahagian ‘back-end’ platform ini akan dikonfigurasikan semula dari awal. Memandangkan Cuckoo sukar untuk dikonfigurasikan kerana terdapat banyak ralat yang dihadapi sepanjang proses, alternatif lain untuknya seperti Avira Cloud Sandbox dan Cisco Secure Malware Analytics akan cuba digunakan. Seperti Cuckoo, Cisco Secure Malware Analytics dan Avira Cloud Sandbox menggabungkan kotak pasir lanjutan dengan perisikan ancaman menjadi satu penyelesaian bersatu untuk melindungi organisasi daripada perisian hasad. Hanya satu perbezaan yang ditemui apabila dibanding dengan Cuckoo iaitu kedua-dua kotak pasir alternatif ini tidak berjalan pada platform Linux. Namun begitu. dalam skop projek ini, iaitu platform pengesanan perisian hasad untuk sistem Windows, alternatif kotak pasir ini masih boleh digunakan.Seterusnya,diharapkan projek ini dapat digunakan oleh skop pengguna yang lebih besar. Ini dapat dicapai apabila wujudnya pembangunan aplikasi telefon pintar untuk platform pengesanan perisian hasad yang menggunakan sistem operasi Android dan iOS. Pengguna juga tidak perlu menggunakan komputer ribaatau komputer meja untuk mengesan perisian hasad dalam sesebuah fail malah boleh berbuat demikian di mana-mana tempat dengan syarat ada akses ke internet.

7 RUJUKAN

Ed Skoudis dan Lenny Zeltser, Malware: Fighting Malicious Code, New Jersey: PrenticeHall, 2004.

Cyberattacks increased 17% in Q1 of 2020, with 77% being targeted attacks. (2021, July16). Security Magazine | The business magazine for security executives.

Targeted attacks. (n.d.). Trend Micro | Enterprise Cybersecurity Solutions. What is malware and how does it work? (2020, November 3). SearchSecurity.

What is a malware file signature (And how does it work)? (2021, October 6). SentinelOne.

Shiel, Ian & O'Shaughnessy, Stephen. (2019). Improving file-level fuzzy hashes for malware variant classification. Digital Investigation. 28. S88-S94. 10.1016/j.diin.2019.01.018.

Ye, Y.; Li, T.; Adjeroh, D.; Iyengar, S.S. A Survey on Malware Detection Using Data Mining Techniques. ACM Comput. Surv. 2017, 50, 41

Damodaran, A.; di Troia, F.; Visaggio, C.A.; Austin, T.H.; Stamp, M. A comparison of static, dynamic, and hybrid analysis for malware detection. J. Comput. Virol. Hacking Tech. 2017, 13, 1–12

Sihwail, R.; Omar, K.; Ariffin, K.A.Z. A Survey on Malware Analysis Techniques: Static. Dyn. Hybrid Mem. Anal. 2018, 8, 1662–167