PLATFORM PENGESANAN PERISIAN HASAD UNTUK SISTEM OPERASI WINDOW BERDASARKAN ANALISIS MEMORI SANDBOX DAN PERATURAN YARA

NATRAH BINTI ABDUL HALIM

KHAIRUL AKRAM BIN ZANOL ARIFFIN

Fakulti Teknologi Dan Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Menurut Cisco perisian hasad adalah perisian mengganggu yang direka oleh penjenayah siber untuk mencuri data, memusnahkan komputer dan merosakkan komputer dengan menggunakan perisian hasad seperti virus, Virus Trojan, ransomware, perisian hasad tanpa fail, ancaman mudah berubah dan banyak lagi. Analisis perisian hasad adalah proses pemahaman tingkah laku dan tujuan fail atau url yang mencurigakan yang membantu dalam pengesanan dan pengurangan kemungkinan ancaman. Perisian hasad tanpa fail adalah jenis perisian berbahaya yang menggunakan program yang sah untuk menjangkiti komputer dan perisian hasad dan tidak dapat dikesan oleh antivirus dan tidak akan meninggalkan jejak kaki serta juga akan beroperasi dalam memori. Terdapat beberapa serangan tanpa nama seperti Operation Cobalt Kitty yang menggunakan PowerShell untuk menyasarkan syarikat Asia selama hampir 6 bulan. Malware ini merupakan ancaman terbesar bagi syarikat pada masa ini. Oleh itu projek ini adalah platform pengenalan perisian hasad untuk sistem operasi Window berdasarkan analisis memori sandbox dan peraturan Yara di mana analisis data malware dari memori sandbox akan digunakan untuk menetapkan peraturan Yara baru dan peraturan tersebut akan dilaksanakan dalam memori Cuckoo Sandbox. Objektifnya adalah mengenal pasti perisian hasad seperti perisian hasad tanpa file dan serangan tidak stabil serta yang tidak dapat dikesan akan dikenal pasti data-datanya.Objektif seterusnya adalah meningkatkan memori Cuckoo Sandbox dengan menggunakan peraturan Yara baru. Kaedah ini akan dimulakan dengan Cuckoo sandbox dan analisis perisian hasad automatik akan dipasang di window 7. Sampel akan dimasukkan ke dalam sandbox dan dalam beberapa minit laporan terperinci yang menunjukkan tingkah laku fail. Selanjutnya data dari memori analisis sandbox akan digunakan untuk membuat peraturan Yara baru. Semasa menganalisis corak dan rentetan unik dalam perisian hasad itu, sampel dapat dikenal pasti dari kumpulan ancaman dan keluarga perisian hasad mana yang dijadikan serta peraturan Yara baru mungkin dibuat untuk sampel baru dan ia akan mengenal pasti dan

mengklasifikasikan perisian hasad jika sampel dari keluarga perisian hasad yang sama. Seterusnya, peraturan tersebut akan dilaksanakan di Cuckoo Sandbox yang akan menjalankan proses pengimbasan fail. Ciri memori di Cuckoo Sandbox akan diimprovisasi dengan peraturan YARA baru sehingga ia dapat mengesan perisian hasad baru dan mencegahnya daripada merosakkan komputer atau mencuri data di dalam kompuuter. Projek ini menggunakan perisian sandbox iaitu sumber terbuka Cuckoo Sandbox dengan sistem operasi host Ubuntu 18.04 dan window 7 sebagai sistem operasi tetamu.

1 PENGENALAN

Keselamatan siber menjadi penting dalam dunia teknologi maklumat. Dalam dunia hari ini, salah satu isu yang paling rumit ialah keselamatan maklumat. Walaupun, pelbagai taktik untuk memerangi jenayah sibertelah dilaksanakan namun setiap individu atau organisasi tetap menjadi mangasa jenayah siber. Perisian hasad, merujuk kepada program jangkitan komputer yang direka untuk menjejaskan, merosakkan atau menyusup ke komputer, menggunakan rangkaian tanpa pengetahuan atau persetujuan pengguna dengan tujuan untuk keuntungan(Daniel G Arce, 2018).

Pencegahan serta langkah untuk mengelakkan pengguna menjadi mangsa jenayah siber adalah dengan memastikkan setiap fail mahupun URL yang ingin di akses wajarlah dipastikan bahawa tiada perisian hasad yang tersembunyi di dalamnya. Hal ini dapat dilaksanakan dengan memerhati, mengkaji serta merekod tingkahlaku dan ciri-cirinya berdasarkan laporan yang dihasilkan melalui proses analisis. Oleh hal yang demikian, perlindungan data dan komputer dapat dijamin dengan melaksanakan analisis perisian hasad iaitu melalui analisis perisian hasad statik dan dinamik. Cadangan projek ini adalah untuk mendapatkan data yang disediakan oleh analisis memori VirusTotal bagi mencipta peraturan Yara baru yang dapat diaplikasikan pada memori Cuckoo Sandbox. Cuckoo Sandbox merupakan sumber terbuka dimana pengguna boleh menggunakannya untuk menganalisis sesuatu sampel fail mahupun URL. Namun, tidak semua perisian hasad dapat dikesan olehnya. Maka, dengan penulisan peraturan Yara baharu, pengguna dapat menggunakan setiap bahan dengan selamat. Mlaah, projek ini turut membantu mengkaji ciri-ciri serta tingkah laku perisian hasad mahupun yang sama tetapi dengan penambahan ciri-ciri baru atau perisian hasad baharu melalui analisis di VirusTotal kemudian melalui analisis dariCuckoo Sandbox.

2 PENYATAAN MASALAH

Antara masalah yang dikenalpasti dalam projek ini bagimencapai objektif projek adalah seperti berikut :

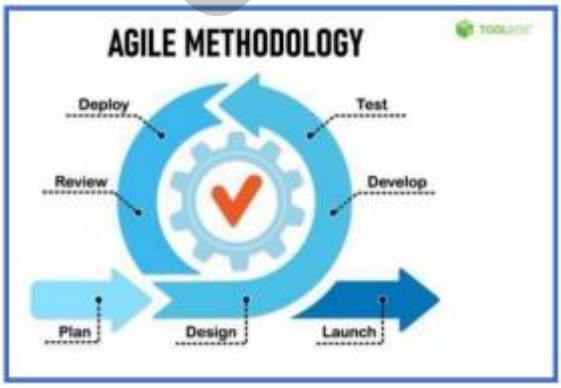
- Teknik dan pengesanan perisian hasad yang terkini tidak dapat emnghentikan atau menghalang penggodam daripada menghasilakn alat automatik bagi mengaktifkan perisian hasad.
- Struktur serta fungsi perisian hasad telah berubah malah menjadi lebih canggih sehingga kodnya tidak dapat dikesan.
- Platform untuk mengesan serta untuk meningkatkan peraturan tersedia ada dan peraturan baharu bagi perisian hasad perlu dibina.

3 OBJEKTIF KAJIAN

Berdasarkan masalah yang dikenalpasti. Projek ini dijalankan untuk memenuhi tiga objektifiaitu:

- Membangunkan analsiis perisian hasad yang mampu mengesan perisian hasad tersedia ada mahupun perisian hasad baharu yang menggunakan ciri-ciri berlainan walaupun daripada keluarga perisian hasad yang sama.
- Menilai kebolehan teknik tersedia ada untuk mengesan perisian hasad serta menulis peraturan baharu menggunakan peraturan Yara di dalam memori analisis sandbox hasad.
- Mengkaji tingkah laku perisian hasad berdasarkan laporan analisis sandbox untuk mengemaskini datanya di pangkalan data anti-perisian hasad.

4 METOD KAJIAN



Rajah 1 Gambaran Metadologi Agile

Metodologi adalah cara menguruskan perkembangan perisian (David Young, 2013). Untuk projek ini Agile ataupun ketangkasan metodologi akan digunakan kerana ia adalah model yang dapat menyesuaikan dengan persekitaran yang berubah-ubah, meminimumkan kos pembangunan dan memberikanperisian yang lebih efektif. Di samping itu, agile mungkin tidak

dapat mengenal pasti penyelesaian di awal peringkat tetapi akan mencapai objektif sebelum peringkat akhir serta sepanjang pembangunan projek. Ia juga melibatkan pelbagai ujian supaya dapat mencapai kemahuan pengguna dan perubahanpembangunan di dalam perisian mengikut maklumbalas pelanggan dan keperluan projek.

4.1 SPESIFIKASI KEPERLUAN

i. Spesifikasi Keperluan Pengguna

Keperluan pengguna merupakan perkhidmatan yang diperlukan oleh pengguna akhir melalui perisian yang dibangunkan. Keperluan ini menyatakan bagaimana kemudahan dan peralatan harus berfungsi. Keperluan pengguna menyediakan maklumat yang berfungsi sebagai asas untuk spesifikasi lanjut, reka bentuk dan pengesahan sistem pembuatan (iaitu, penyelesaian reka bentuk daripada vendor untuk memenuhi keperluan pengguna yang dinilai semasa proses semakan/kelayakan reka bentuk).

- Pengguna & Pentadbir

Spesifikasi keperluan pengguna	
Pengguna	**Pentadbir**
Berikut merupakan tugasan yang perlu dilakukan oleh seorang pengguna ketika menggunakan VirusTotal ini dan sandbox: - Melaksanakan analisis kepada sesuatu sample fail - Mendapatkan hasil laporan analisis - Memohon pengesanan perisian hasad - Mendapatkan laporan terbaru bagi perisian hasad	Terdapat beberapa tugas yang perlu dilaksanakan oleh seorang pentadbir: -Menyediakan persekitaran analisis perisian hasad yang terasing dan bersih. -Menyediakan alatan yang diperlukan untuk menjalankan analisis perisianhasad (komputer riba, sandbox, Ubuntu, sebagainya). -Menyediakan mekanisme penyelenggaraan dan pemulihan sistem -Menyediakan peraturan baharu iaitu Peraturan Yara -Membangunkan pangkalan data untuk menyimpan data laporan analisis -Platform ini membolehkan pengguna untuk melihat hasil laporan analisis

Jadual 1 Spesifikasi Keprluan Pengguna Dn Pentadbir

ii. Spesifikasi Keperluan Fungsian Sistem(Pentadbir dan Pengguna)

Spesifikasi keperluan sistem pula menyatakan keperluan sistem untuk setiap keperluan pengguna berfungsi dan keperluan pengguna tidak berfungsi, menyatakan kualiti dan keperluan domain yang tidak berfungsi, menentukan keperluan perkakasan dan perisian semasa pembangunan serta penggunaan keperluan tersebut.

Spesifikasi Keperluan Sistem		
	Keperluan fungsian pengguna	**Keperluan fungsian sistem**
Pengguna	Memuat naik sampel fail dengan menggunakan sistem analisis iaitu sandbox	**W**ajarlah berkemampuan untukmemilih dan memuat naik sampel perisian hasad untuk tujuan analisis serta perlu mendapatkan hasil analisis
	Menjalankan perisian hasad serta pencarian data	Mampu mengenalpasti perisian hasad
	Mendapatkan analisis laporan data	Mendapatkan hasil analisis Menganalisis perisian hasad jika tidak dijumpai penulisan peraturan secara manual dilaksanakan Penyimpanan data di pangkalan data Mampu menghasilkan laporan analisis perisian hasad
Pentadbir	Penyediaan persekitaran isolasi serta selamat untuk menjalankan analisis perisian hasad	Pemasangan sumber terbuka sandbox akan membantu menjalankan analisis stati
	Penyediaan alatan bagi melaksanakan analisis perisian hasad	Pemasangan sumber terbuka sandbox akan membantu menjalankan analisis stati
	Pemasangan anti-perisian hasad untuk menjalankan analisis perisian hasad dan menulis peraturan Yara	Pemasangan Cuckoo sandbox hasad untuk menjalankan analisis perisian hasad dan menulis peraturan Yara

Jadual 2 Spesifikasi Keperluan Fungsian Sistem(Pengguna Dan Pentadbir)

Spesifikasi Keperluan Bukan Fungsian Pengguna

Keperluan Bukan Fungsian	Penjelasan
Mudah alih	Merupakan bagaimana sesuatu sistem dapat dipasang pada peranti tertentu. Cuckoo sandbox, VirusTotal dan Ubuntu merupakan sumber terbuka yang dapat dipasang pada pelbagai operasi sistem misalnya Window 7, mesin maya dan sebaginya untuk menjalankan analisis perisian hasad dengan selamat
Kselamatan	**S**istem haruslah berupaya untuk menghadapi sebarang ancaman apabila analisis dijalankan . Oleh itu mesin maya digunakan bagi mengelakkan sebarang isu berlaku.
Kebolehgunaan	Rangka kerja volatil akan digunakan memandangkan ia merupakan sumber terbuka malah dapat mengesan perisian hasad dengan lebih terperinci. Malah antara muka Cuckoo Sandbox adalah lebih mesra pengguna serta mudah difahami.
Kebolehlanjutan	Ia merupakan kebolehan sistem untuk diubah serta disusun oleh pentadbir mahupun pengguna dari masa ke masa dengan menggunakan peraturan tertentu
Integriti data	Data hasil daripada laporan analisis wajarlah tepat supaya penulisan peraturan dapat dihasilkan bagi mengesan perisian hasad baharu

Jadual 3 Spesifikasi Keperluan Bukan Fungsian

Spesifikasi Keperluan Perkakasan Dan Perisian

Projek ini melibatkan penggunaan beberapa perkakasan yang khas serta akan digunakan pada fasa kedua iaitu fasa pembangunaa, percubaan dan perlaksanaan

Spesifikasi Keperluan Perkakasan Dan Perisian	
Perkakasan	-Dua komputer riba iaitu Laptop hp 8GB RAM, processor Ryzen 3 dan Acer Aspire 3 8GB RAM, processor intel i5 - USB 8Gb peranti untuk proses format

Perisian	-Sistem VirusTotal(Sumber terbuka) -Perisian maya(Virtual Box) -Microsoft Window versi 7 6.1.7601(Softonic.2019) -Ubuntu 18.04 -Rufus Versi 3.13 -Volatiliti -MongoDB

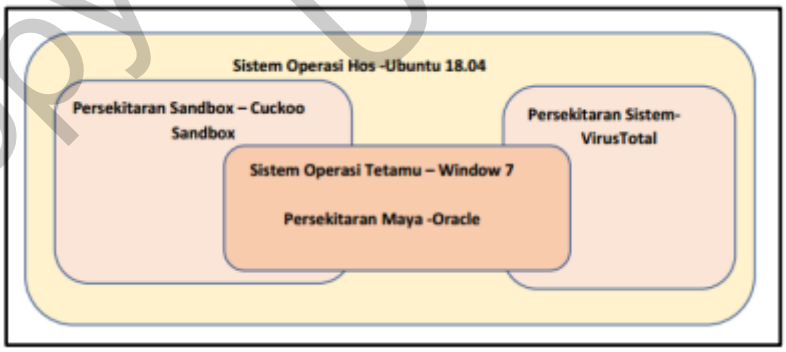
Jadual 4 Spesifikasi Keperluan Perkasasan Dan Perisian

4.2 FASA REKA BENTUK

Reka bentuk seni bina merupakan proses pengenalpastian sub-sistem yang membentuk serta menjadi kerangka untuk komunikasi sub-sistem.Dalam projek ini, terdapat beberapa seni bina yang terlibat iaitu seni bina berlapis dan seni bina pelayan-pelanggan bagi sandbox. Seni bina berlapis adalah penting ketika mereka bentuk pembinaan sistem sandbox dan mesin maya secara terasing supaya keselamatan peranti sentiasa terjamin. Seterusnya, seni bina pelayan-pelanggan adalah penting untuk pembinaan modul analisis, laporan dan penulisan peraturan Yara.

A. Seni Bina

i. Seni Bina Berlapis

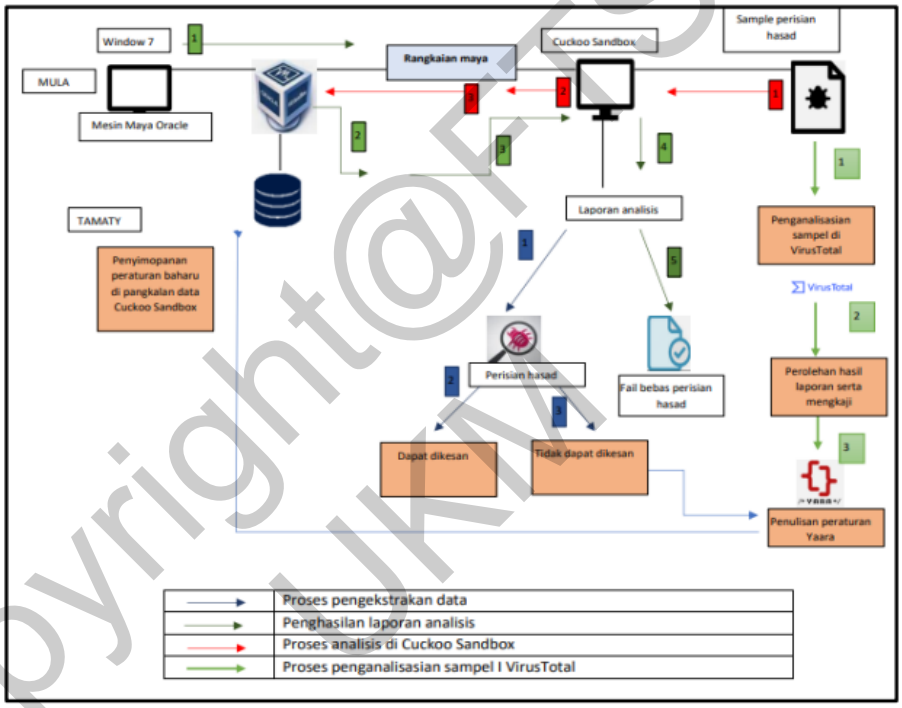


Rajah 2 Seni Bina Berlapis

Berdasarkan rajah 2 di atas, mesin maya akan dipasang di dalam Window 7 supaya analisis perisian hasad dijalankan dalam keadaan isolasi serta operasi utama tidak akan terganggu ketika analisis. Sistem operasi tetamu akan dipilih sebagai sistem pengoperasian unutk proses analisis ini serta pengguna bebas untuk memilih sistem operasi untuk menganalisis sesuatu sampel. Bagi projek ini, sistem operasi secara maya akan digunakan. Disamping itu, bebrapa

keprluan sebelum analisis dimulakan akan disediakan terlebih dahulu misalanya sistem bahasa pengaturcaraan Python versi 7.2, perisian analisis Volatil "Volatility",mesin maya "virtual box", anti-perisian hasad dan Cuckoo sandbox. Seterusnya, pembinaan sistem sandbox yang terasing dan selamat ini di laksanakan dengan pemilihan sistem operasi hos atau tuan rumah. Tuan rumah mahupun hos ini akan menempatkan, mengendalikan sistem sandbox dan analisis bagi perisian hasad. Oleh itu, Ubuntu 18.04 akan dijadikan hos bagi mengendalikan sistem analisis, sandbox dan mesin maya memandangkan ia merupakan sumber terbuka serta selamat untuk menjalankan analisis perisian hasad.

ii. Seni Bina Pelanggan-Pelayan

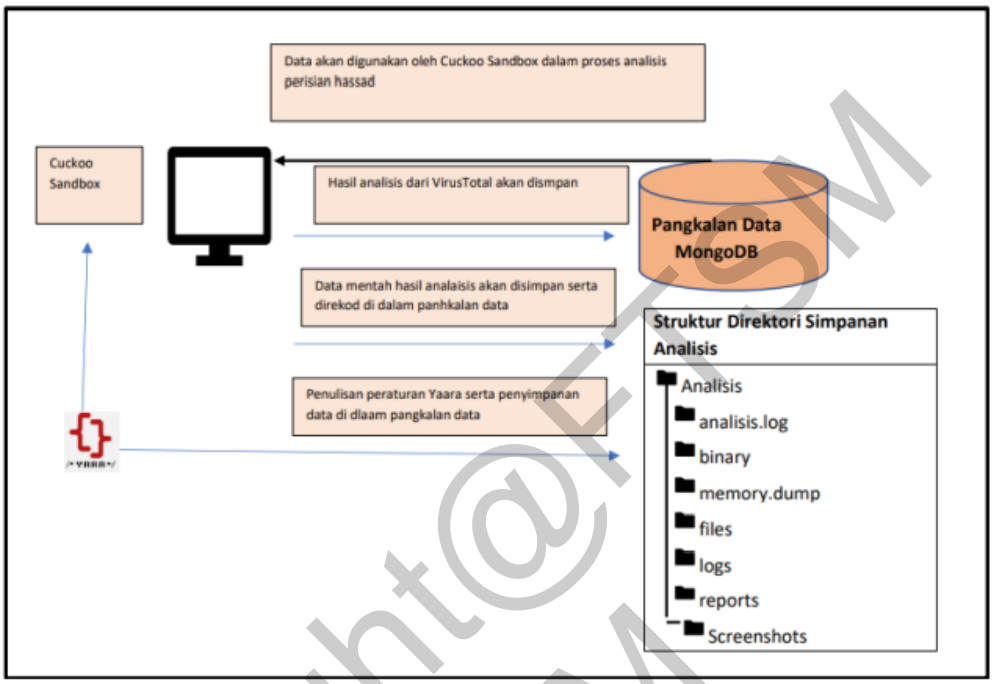


Rajah 3 Seni Bina Pelanggan-Pelayan

Berdasarkan rajah 3 di atas, persekitaran yang terasing akandisediakan dahulu iaitu pemasangan mesin maya Oracle. Kemudian, pemasangan Ubuntu 18.04, pemasangan Cuckoo sandbox akan dilakukan. Rangkaian maya merupakan rangkaian terasing yang memberi laluan untuk melakukan analisis dalam mesin maya. Cukcoo sandbox pula akan menjadi mesin hos yang menguruskan perisian manakala mesin maya akan menjadi mesin tetamu/pelanggan. Hos akan menjalankan komponen teras sandbox yang menguruskan keseluruhan proses analisis, membuang trafik “traffic dump” dan menjana laporan, manakala pelanggan iaitu mesin maya(virtual amchine) merupakan persekitaran yang terpencil dan bersih akan menjadi tempat untuk sampel perisian hasad dilaksanakan dan dianalisis dengan selamat. Tingkahlaku sampel

yang diperolehi melalui hasil laporan analisis oleh VirusTotal tersebut akan direkodkan oleh penganalisis untuk penulisan peraturan Yara sekirannya perisian hasad yang dikaji tidak boleh dikesan oleh Cuckoo Sandbox

B. Pangkalan Data



Rajah 4 Aliran Penyimpanan, Struktur Dan Penggunaan Data

Sistem Cuckoo Sandbox menggunakan NoSQL (MongoDB) untuk menjalankan analisis serta untuk penyimpanan hasil laporan analisis. MongoDB merupakan pangkalan data NoSQL berorientasikan dokumen yang digunakan untuk penyimpanan data. Daripada menggunakan jadual dan baris seperti dalam pangkalan data hubungan tradisional, MongoDBmenggunakan koleksi dan dokumen. Dokumen terdiri daripada pasangan nilai kunci (“primarykey”) yang merupakan unit asas data dalam MongoDB. Terdapat beberapa ciri bagi MongoDb ini, antaranya model data yang tersedia dalam MongoDB bantu membina perhubungan hierarki, menyimpan tatasusunan dan struktur lain yang lebih kompleks dengan lebih mudah. Seterusnya, kebolehskalaan MongoDB dimana persekitaran MongoDB sangat berskala. Berdasarkan rajah 4 diatas menunjukkan aliran penyimpanan, struktur dan penggunaan data oleh Cuckoo sandbox(Cuckoo Sandbox, 2020). Sistem Cuckoo Sandbox menggunakan NoSQL (MongoDB) untuk menjalankan analisis serta untuk penyimpanan hasil laporan analisis. MongoDB merupakan pangkalan data NoSQL berorientasikan dokumen yang digunakan untuk penyimpanan data. Daripada menggunakan jadual dan baris seperti dalam pangkalan data hubungan tradisional, MongoDBmenggunakan koleksi dan dokumen.

Dokumen terdiri daripada pasangan nilai kunci (“primarykey”) yang merupakan unit asas data dalam MongoDB. Terdapat beberapa ciri bagi MongoDb ini, antaranya model data yang tersedia dalam MongoDB bantu membina perhubungan hierarki, menyimpan tatasusunan dan struktur lain yang lebih kompleks dengan lebih mudah. Seterusnya, kebolehskalaan MongoDB dimana persekitaran MongoDB sangat berskala. Berdasarkan rajah 4 diatas menunjukkan aliran penyimpanan, struktur dan penggunaan data oleh Cuckoo sandbox(Cuckoo Sandbox, 2020).

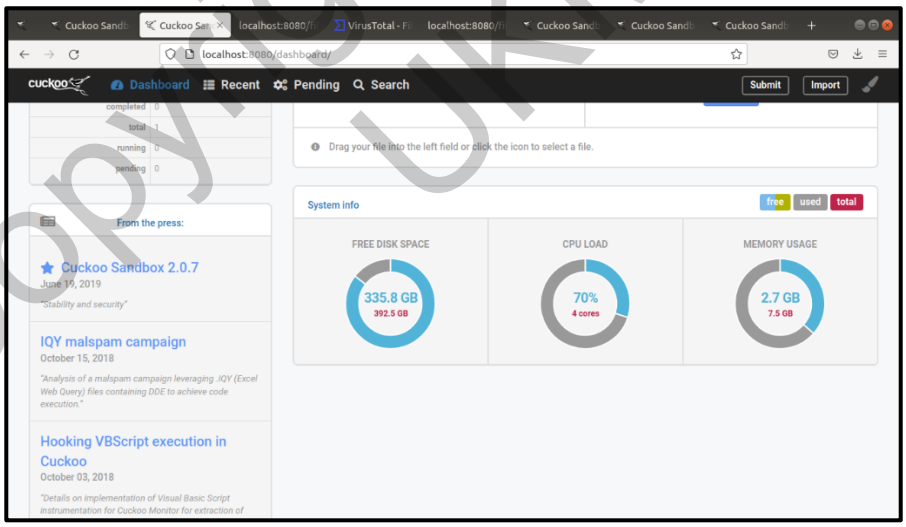
C. Algoritma

Reka bentuk algoritma merupakan satu set langkah yang digunakan untuk menyelesaikan tugas tertentu serta proses untuk menyelesaika sesuatu masalah. Algoritma ini terdiri daripada kod yang memberitahu tugas apa yang perludilakukan Bagi projek ini, terdapat algoritma analisis dari Cuckoo Sandbox.

Algoritma Analisis bagi Cuckoo Sandbox

Algoritma analisis adalah proses menganalisis tingkah laku sampel fail (perisian hasad) malah algoritma memberi gambaran keseluruhan proses dalam projek ini.

D. Antara Muka



Rajah 5 Halaman Hadapan Cuckoo Sndbox

Projek ini akan menggunakan reka bentuk antara muka yang sedia ada iaitu telah disediakan oleh Cuckoo Sandbox. Rajah 3.13 menunjukkan laman utama web Cuckoo. Berdasarkan rajah dibawah, didapati bahawa beberpa maklumat dipaparkan seperti memori, versi perisian Cuckoo, info sistem dan sebagainya bagi Cuckoo Sandbox. Bagi laman web Cuckoo, laman utamanya terdapat beberapa perincian maklumat memori, simpanan, versi perisian Cuckoo,

statistik penggunaan sistem Cuckoo, paparan muat naik sampel fail, pautan URL dan hash ke sistem pelayan Cuckoo, maklumat sistem dan maklumat “Central Processing Unit”(CPU).

4.3 FASA PELAKSANAAN

Fasa ini akan menerangkan fasa pembangunan yang dilaksanakan selepas fasa reka bentuk selesai diselesai. Bab ini akan menjurus kepada langkah-langkah serta dokumentasi kepada fasa pembangunan projek ini. Di dalam fasa ini prototaip reka bentuk akan ditukarkan menjadi sistem makluamt yang lengkap malah memenuhi keprluan sistem dan pengguna seperti yang telah didokumentasikan. Terdapat beberapa proses bagi membangunkan projek ini iaitu menyediakan keperluan sistem, memformat peranti, mengubah suai tetapan sistem BIOS, pemasangan sistemperumah(Ubuntu), pemasangan sistem Cuckoo Sandbox, pemasangan mesin maya(Virtual Machine) dan mengubah suai konfigurasi sistem Cuckoo.

Penyediaan Perisian, Sistem Dan Peranti

Perisian/sistem	Rufus versi 3.17 **(**https://rufus.ie/en/**)**
	Ubuntu 18.04 (https://releases.ubuntu.com/18.04/)
Peranti	Memori Capaian Rawak RAM (berkapasiti 8 GB)
	Pemacu Kilat (USB) (berkapasiti GB)
	Peranti Komputer (berkapasiti 480 GB)

Jadual 5 Perisian, Sistem Dan Peranti Yang Perlu Disediakan

Pembuatan Media Pemasangan Sistem Operasi Perumah

Langkah	**Penjelasan**
Tetapan sistem BIOS perlu diubah suai	- Secure Boot dinyahaktifkan - Susnan media boot diubah suai mengikut keutamaan sistem kepada peranti media
Memasang sistem operasi perumah	- Ubuntu 18.04 dipasang pada peranti menggunakan USB

Jadual 6 Pembuatan Media Pemasangan Sistem Operasi Perumah

Pengemaskinian Sistem Ubuntu 18.04

Membuka terminal Ubuntu unutk mengemaskini data di dalamnya dengan menggunakan arahan dibawah :

Arahan

- sudo apt update
- apt list --upgradable
- sudo apt upgrade

Pemasangan Sistem Sandbox Dan Mesin Maya

<table>
<tr><td>1# Python
$ sudo apt-get install python python-pip python-dev libffi-dev libssl-dev -y
$ sudo apt-get install python-virtualenv python-setuptools -y
$ sudo apt-get install libjpeg-dev zlib1g-dev swig -y
$ sudo apt-get install mongodb -y
$ sudo apt-get install postgresql libpq-dev -y</td><td>2# Virtualization SW
$ sudo add-apt-repository multiverse -y
$ sudo apt-get update -y
$ sudo apt install virtualbox -y

3#Muat turun iso window 7
$ wget https://cuckoo.sh/win7ultimate.iso</td></tr>
<tr><td>4#Simpan dalam folder Download
# TCPDUMP
$ sudo apt-get install tcpdump apparmor-utils -y
$ sudo aa-disable /usr/sbin/tcpdump
# Python Tambahan
$ sudo apt-get -y install python virtualenv python-pip python-dev build-essential -y
$ 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
$ sudo pip install m2crypto
$ sudo usermod -a -G vboxusers cuckoo</td><td>5#Muat turun file secara mentah dan simpan seperti nama asalny di laman tersbut
https://gist.github.com/jstroch/de20131dda2aac5cd1116dd44b8f2474

$ chmod +x ./cuckoo-setup-virtualenv.sh
$ sudo -u cuckoo ./cuckoo-setup-virtualenv.sh

$ source ~/.bashrc

$ mkvirtualenv -p python2.7 cuckoo-ukm</td></tr>
</table>

Jadual 7 Pemasangan Sistem Sandbox Dan Mesin Maya

Pemasangan Cuckoo Sandbox Dan Mesin Maya Virtualbox

<table>
<tr><td>1#Berada dalam keadaan isolasi
$ workon cuckoo-ukm</td><td>2#Memasang keperluan untuk memasang Cuckoo Sandbox
(cuckoo-ukm) $ pip install -U pip setuptools</td></tr>
</table>

	(cuckoo-ukm) $ pip install -U cuckoo (cuckoo-ukm) $ pip install -U vmcloak (cuckoo-ukm) $ vmcloak-vboxnet0 (cuckoo-ukm) $ vmcloak init --verbose --win7x64 win7x64base --cpus 2 --ramsize 2048 (cuckoo-ukm) $ vmcloak clone win7x64base win7x64cuckoo-ukm
2#Smbung memasng keperluan lain (cuckoo-ukm) $ vmcloak install win7x64cuckoo-ukm adobe9.version=11.0.19 pillow java java.version=8u151 java.version=jdk8u121 firefox_41 flash winrar (cuckoo-ukm) $ vmcloak snapshot --count 2 win7x64cuckoo-ukm 192.168.5.101 (cuckoo-ukm) $ cuckoo init (cuckoo-ukm) $ cd ~/.cuckoo/conf (cuckoo-ukm) $ cuckoo community (cuckoo-ukm) $ while read -r vm ip; do cuckoo machine --add $vm $ip; done < <(vmcloak list vms) (cuckoo-ukm) $ nano ~/.cuckoo/conf/virtualbox.conf	

Jadual 8 Pemasangan Cuckoo Sandbox Serta Virtualbox

Pengubahsuaian Konfigurasi Cuckoo Sandbox

Terdapat beberapa situasi di mana akan jatuhnya kebanyakkan fail daripada sistem tetamu semasa proses analisis sampel fail dijalankan, oleh itu tidak akan dapat mempruntukkan simpanan fail baharu yang berkuantiti berlebihan. Hal ini demikian kerana Ubuntu peruntukkan 10GB had saiz simpanan minimum. Oleh itu, berikut adalah langkah untuk meningkatkan had fail bagi pengguna cuckoo (sistem ubuntu). Manakala berdasarkan Cuckoo Sandbox, 2020 konfigurasi menukar sistem pengurusan pangkalan data SQLite kepada PostgresSQL ataupun MYSQL perlu dilakukan supaya Cuckoo Sandbox boleh menggunakan lebih daripada satu mesin maya analisis sampel malah mengurangkan kemungkinan berlaku masalah(“Error”). Setereusnya, peraturan penghalaan global dieprlukan untuk diaktifkan supaya mesin maya mengarahkan permintaan keluar masuk kepada Internet mahupun pelayanarahan dana kawalan (C&C) perisian hasad. Peraturan ini juga untuk semua mesin maya yang telah disambung ke antara vboxnet0 yang perlu diaktifkan. Berikut meruopkan arahan untuk konfigurasi Cuckoo Sandbox:

Peningkatan Had Fail	Membuka fail limits.conf lokais /etc/security/ (sebagai root)
	$sudo nano /etc/security/limits.conf
	Memasukkan baris dibawah di akhir fail limits.conf * hard nofile 500000 * soft nofile 500000 root hard nofile 500000 root soft nofile 500000
Pemasangan Postgres	$sudo apt-get postgresql postgresql-contrib
	$sudo -u postgres psql
	CREATE DATABASE cuckoo; CREATE USER cuckoo WITH ENCRYPTED PASSWORD 'password'; GRANT ALL PRIVILEGES ON DATABASE cuckoo TO cuckoo; \q
	#Memasang Postgres pada Cuckoo dengan memasuki persekitaran terasing virtualenv dengan menggunakna arahan dibawah: $ workon cuckoo-test (cuckoo-test) $ pip install psycopg2 **Kemudian, buka fail cuckoo.conf. dengan memasuki fail konfigurasi Cuckoo dengan menggunakan arahan dibawah ini:** (cuckoo-test) $ cd ~/.cuckoo/conf (cuckoo-test) $ nano ~/.cuckoo/conf/cuckoo.conf **Seterusnya, menukar bahagian yang berlabel connection= yang terdapat pada bahagian [database] kepada yang bawah.** **Peringatan : nama dan kata laluan perlu diingati.** connection = postgresql://cuckoo:password@localhost/cuckoo
Peraturan Pemajuan Global Internet	**#Memasuki akaun hak root** $sudo ip address
	$sudo sysctl -w net.ipv4.conf.vboxnet0.forwarding=1 $sudo sysctl -w net.ipv4.conf.enp3s0f1.forwarding=1
	#Mengaktifkan penghalaan global untuk kesemua mesin mayaVM

	yang telah disambungkan kepada antara muka vboxnet0 pada tetapan sistem tembok api dengan menggunakan arahan berikut iaitu : $sudo iptables -t nat -A POSTROUTING -o enp3s0f1 -s 192.168.56.0/24 -j MASQUERADE $sudo iptables -P FORWARD DROP $sudo iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT $ sudo iptables -A FORWARD -s 192.168.56.0/24 -j ACCEPT

Jadual 9 Pengubahsuaian Konfiguras Cuckoo Sandbox

4.4 FASA PENGUJIAN

Fasa ini merupakan proses penghasilan perancangan proses pengujian, reka bentuk kes pengujian, pengujian serta penghasilan keputusan pengujian. Disamping itu, pengujian ini lebih menjurus kepada pengujian fungsi serta keselamatan sistem. Malah, fasa ini juga penting untuk menguji keberkesanan peraturan Yara yang telah ditulis pada memori Cuckoo Sandbox bagi beberapa perisian hasad yang terpilih. Peraturan ini juga dihasilkan untuk perisian hasad yang boleh dikesan oleh Cuckoo Sandbox namun peraturan ini ditulis berdasarkan ciri-ciri daripada VirusTotal.Ciri-ciri tersebut tidak sesekali sama dengan peraturan sedia ada di dalam Cuckoo Sandbox. Pengujian ini juga untuk menguji keberkesanan peraturan Yara yang baharu bagi beberapa perisian hasad yang tidak dapat dikenal pasti oleh Cuckoo juga.

Jenis Pengujian

Jenis Pengujian	Penjelasan
Pengujian Berfungsi	Memuat naik sampel (Fail/URL) memilih mesin maya untuk proses analisis, perlaksanaan analsisi perisian hasad
	Memilih tetapan analisis dengan sambungan rnagkaian (Internet, VPN, Tiada)
	emilihan tetapan masa perlaksanaan analisis
	Memilih mesin maya untuk proses analisis
	Perlaksanaan analsisi perisian hasad

	Mengkajiserta memuat turun hasil laporan analisis
Pengujian Bukan Fungsian	Pengaksesan kepada rangkaian utama daripada sistem tetamu

Jadual 10 Pengujian Berfungsi Serta Bukan Berfungsi

Reka Bentuk Pengujian Kes

- **Kaedah Pengujian**

Rekabentuk pengujian kes ini akan dilaksanakan dengan menggunakan dua kaedah iaitu kaedah pengujian kotak hitam dan kotak putih. Kaedah **pengujian kotak hitam** ini merupakan kaedah ujian perisian yang digunakan untuk menguji perisian tanpa mengetahui struktur dalaman kod atau program malah akan dijalankan oleh penguji mahupun penganalisis. Penguji atau penaganalisis tidak memerlukan pengetahuan pengaturcaraan untuk menjalankan ujian kotak hitam ini. Ujian ini turut boleh digunakan pada tahap ujian yang lebih tinggi seperti Ujian Sistem dan ujian Penerimaan. Selain itu, ujian kotak hitam bermaksud ujian berfungsi atau ujian luaran yang bermatlamat untuk menyemak kefungsian yang dilakukan oleh sistem yang sedang diuji. Manakala, kaedah **pengujian kotak putih** merupakan kaedah ujian perisian di mana struktur dalaman diketahui oleh penguji ketika menguji perisian tersebut. Pengujian ini akan dijalankan oleh pembangun perisian yang mengetahui pengaturcaraan. Ujian ini boleh digunakan pada tahap ujian yang lebih rendah seperti Ujian Unit dan ujian Integrasi. Ujian kotak putih ini turut bermaksud ujian struktur atau ujian dalaman.

Ujian Keberkesanan Fungsian Oleh Pengguna

Setelah ujian dijalankan oleh pengguna berlatar Pendidikan Teknologi Maklumat yang berbeza, maklumbalas daripada pengguna dicatat melalui beberapa soalan yang diberikan melalui pautan URL. Maklumbalas ini adalah untuk memastikan bahawa pengguna berasa puas dengan pengujian yang telah dilasksanakan, untuk memastikan keperluan dan kehendak pengguna yang telah disenaraikan pada bab-bab sebelum ini tercapai dan untuk mengetahui keselamatan ketika pengujian dijalankan oleh pengguna. Terdapat tiga pengguna berlatarbelakang pendidikan berbeza telah menjalankan ujian ini serta telah menjawab soalan-soalan seperti Rajah 6 di bawah senarai soalan berkenaan keberkesanan pengujian dan rumusan maklumbalas pengguna yang telah menjalankan pengujian. Segala komen, hasil ujian dan keberkesanan setiap fungsian akan diperhatikan, direkod dan dianalisis bagi penghasilan laporan di akhir projek serta untuk penambah baikan pada masa yang akan datang

No.Soalan	Soalan Ujian	Maklumbalas Pengguna				
		SS	S	AS	KS	TM
1	Sample fail dan URL perisian hasad dapat dipilih dan dimuat naik	3				
2	Setiap tetapan analisis perisian hasad telah berfungsi dengan baik	3				
3	Mesin maya telah berjalan malah berfungsi baik seperti yang dijangkakan bagi setiap kali proses analisis dimulakan	3				
4	Fungsi penghalaan rangkaian melalui Internet telah berjalan dengan baik	3				
5	Fungsi penghalaan rangkaian Internet melalui VPN telah berjalan seperti yang dijangkakan malah dapat dijalankan dengan amat baik				3	
6	Sistem memberikan laporan yang lengkap untuk setiap analisis.	3				
7	Hasil laporan yang diperolehi dapat dilihat semula dan proses memuat naik semula turut berfungsi dengan baik	3				
8	Saya rasa sistem yang disediakan ini selamat untuk digunakan bagi menganalisis perisian hasad	1	2			
9	Sistem ini memiliki fungsi yang lengkap bagi menganalisis perisian hasad	3				
10	Sistem ini membolehkan saya unutk mudah difahami serta mudah untuk digunakan malah rasa lebih terjamin apabila ingin menggunakan sesuatu fail atau URL dengan adanya sistem ini	3				

Penunjuk :

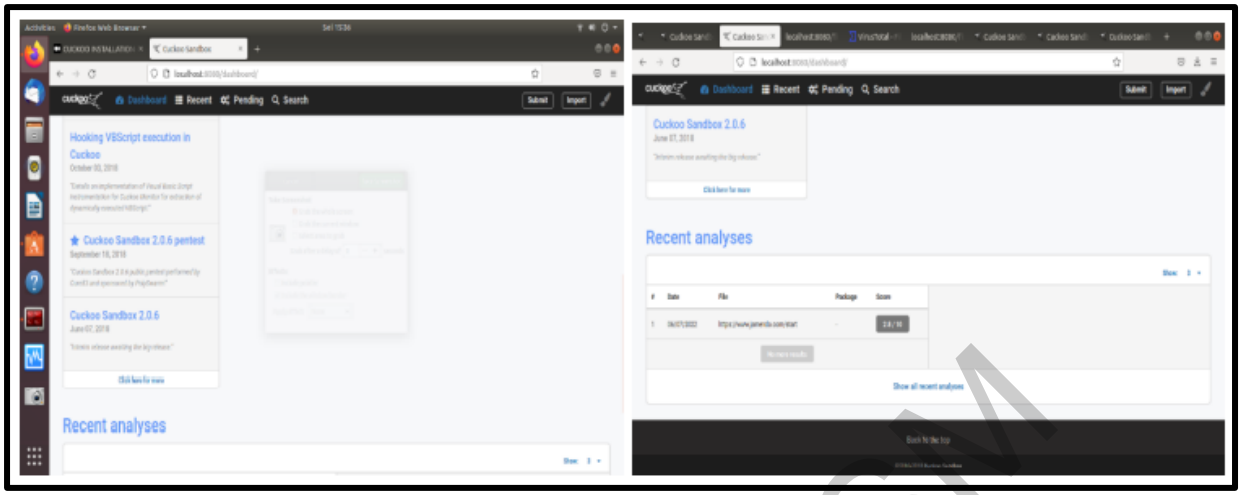
Simbol	Penerangan
SS	Sangat Setuju
S	Setuju
AS	Agak Setuju
KS	Kurang Setuju
TM	Tidak Memuaskan

Rajah 6 Ujian Keberkesanan Fungsian Oleh Pengguna (Borang Maklum Balas)

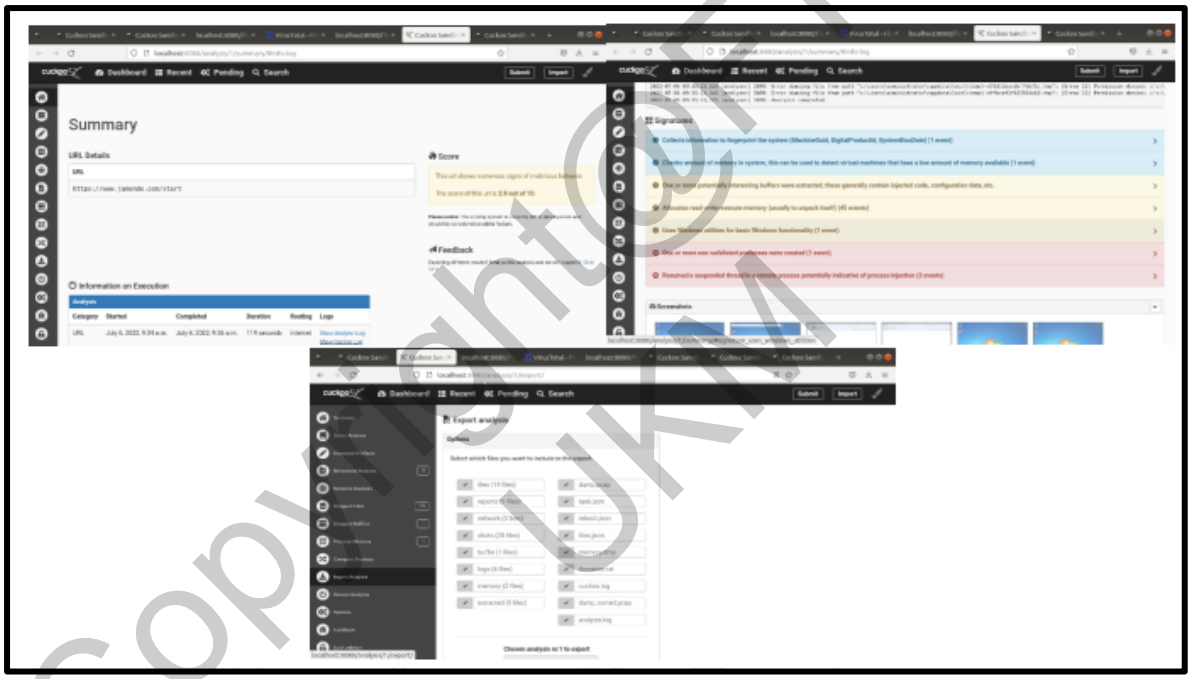
4.5 HASIL KAJIAN DAN PENGUJIAN

Fasa ini akan menerangkan hasil kajian ini dijalnakna serta maklumbalas yang telah diperolehi melalui pengujian fungsian yang telah dilakukan oleh pengguna. Berikut merupakan antara muka Cuckoo Sandbox dan peraturan Yara yang dihasilkan bagi perisian hasad jenis tebusan beradasarkan ciri-ciri yang diperolehi melalui VirusTotal

- **Antara muka hadapan :**



Rajah 7 Laman Hadapan Cuckoo



Rajah 8 Laman Hasil Laporan

- **Rumusan Hasil Pengujian Oleh Pengguna**

Berdasarkan hasil maklumbals dari Rajah 6 diatas, pengguna yang menjalankan pengujian ini merupakan berlatar belakng teknologi maklumat. Selain itu, berdasarkan 10 soalan yang telah diajukkan, didapati bahawa ketiga-tiga pengguna sangat setuju dengan bagi No.Soalan 1 hingga 4, 6 hingga 7 dan 9 hingga 10. Manakala, bagi No.Soalan 5 pulan ketiga-tiga pengguna kurang setuju dan bagi No.Soalan 9 pula 1 pengguna sangat setuju serta 2 orang pengguna setuju sahaja Pengguna kurang setuju bagi No.Soalan 5 memandangkan penghalaan VPN tidak ada ketika pemilihan tetapan analisis dilakukan . Insiden ini telah menyebabkan pengguna

berasa kurang memuaskan dengan sistem yang telah dihasilkan serta kurang berasa selamat untuk menggunakanya ketika analisis perisian hasad. Kesimpulannya, didapati keseluruhan projek ini berfungsi dengan baik serta masalah yang didapati boleh diselesaikan pada masa akan datang malah lebihan peraturan Yara juga dapat dihasilkan sera konfigurasi yang lebih mendalam juga dapat dilaksanakan supaya peisian hasad yang canggih dapat dikesan malah lebih selamat bagi pengguna sebelum menggunakan sebarang sampel fail mahupun URL. Berikut merupakan gambar rajah 9 pengguna yang menguji projek yang telah dihasilkan.

Rajah 9 Pengguna Mneguji Fungsian Bagi Cuckoo Sandbox

5 KESIMPULAN

Dengan ini, dapat disimpulkan bahawa fasa pengujian ini membantu untuk menguji projek yang telah dihasilkan bagi melihat keberkesanan setiap kefungsian seperti yang telaah disenaraikan dalam bab-bab sebelum ini malah reka bentuk dan seni bina yang telah dirancang pada bab-bab sebelum ini juga dapat dicapai. Maka, dengan pengujian yang telah dijalankan, dapat disimpulkan bahawa projek ini selamat dan berfungsi dengan baik apabila digunakan oleh pengguna. Seterusnya, sistem Cuckoo sandbox telah dinaik tarafkan memori analisisnya dengan penulisan peraturan Yara yang baharu . Penulisan peraturan ini telah dilaksanakan bagi perisian hasad tebusan sahaja dan peraturan tersebut juga berjaya mengesan perisian hasad berjenis tebusan. Hal ini, menunjukkan memori analisis Cuckoo Sandbox perlu di kemaskini dengan peraturan aara yang baharu spenganalisis sistem keselamatan dapat mencegahnya

Terdapat beberapa kekeangan ketika menjalankan projek ini, iaitu peranti yang digunakan unutk menbangunkan projek ini haruslah tidak mempunyai sebarang an masalah hardware kerana ia boleh menyebabkan penyediaan semula dan format sistem yang telah dihasilkan. Selain itu, perisian hasad terkini turut memiliki pelbagai ciri-ciri serta tingkah laku yang berbez

sehingga ia tidak mudah dikesan oleh penganalisis. Maka segala tetapan pada Cuckoo Sandbox dan Terminal Ubuntu 18.04, wajarla ditetapkan dengan berhati-hati serta perlu menggunakan arahan-arahan yang berpatutan bagi memastikkan sesuatu tetapan itu dapat berfungsi dalam mengesan perisian hasad.

Penambahbaikkan yang perlu dilaksanakakn pada masa hadapan adalah mempelbagaikan pilihan tetapan konfigurasi iaitu network sebelum analisis perisian hasad dijalankan di Cuckoo Sandbox. Seterusnya, penulisan peraturan Yara bagi perisian hasad yang sama mahupun baharu dengan menguji lebih banyak sampel perisian hasad supaya peraturan tersebut dapat mengesan perisian hasad tersebut. Yang terakhir, memastikan penggunaan segala peranti, hardware mahupun software adalah memenuhi keperluan projek serta memastikan ia tidak menimbulkan sebarang isu ketika projke dijalankan

6 RUJUKAN

Hatching.io. 2022. Hatching - Automated malware analysis solutions. Available at: https://hatching.io/blog/cuckoo-sandbox-setup/ . Accessed 3 June 2022]

Aviani, G. (2019, July 30). Virtualenv with Virtualenvwrapper on Ubuntu 18.04. Medium. https://itnext.io/virtualenv-with-virtualenvwrapper-on-ubuntu-18-04-goranaviani-d7b712d906d

Configuration—Cuckoosandboxv2.0.7book.(n.d.).Cuckoo. https://cuckoo.sh/docs/installation/host/configu ration.htm

freeCodeCamp.org. 2022. How to Set Up Virtualenv with Virtualenvwrapper on Ubuntu 18.04. Available at: https://www.freecodecamp.org/news/virtualenv-withvirtualenvwrapper-on-ubuntu-18-04/ . Accessed 3 June 2022

Virtualenvwrapper.readthedocs.io. 2022. virtualenvwrapper 5.0.1.dev2 — virtualenvwrapper 5.0.1.dev2 documentation. [online] Available at: https://virtualenvwrapper.readthedocs.io/en/latest/ . Accessed 3 June 2022

Amarasinghe, H. (2022, March 27). CUCKOO INSTALLATION (work in progress) #malwareanalysis. Medium.https://hasanka-amarasinghe.medium.com/cuckooinstallation-work-in-progress-malwareanalysis-7c0f95ebb740

Available at: https://virtualenvwrapper.readthedocs.io/en/latest/(virtualwrapper). Accessed 3 June 2022 Setting up Cuckoo Sandbox For Dummies (Malware Analysis).