SANDBOX DAN PENJANA INDIKATOR KOMPROMI

ADAILTON ANAK JOSEPH
KHAIRUL AKRAM BIN ZAINOL ARIFFIN

Fakulti Teknologi dan Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Perisian hasad merupakan salah satu serangan yang sering berlaku dalam sesebuah sistem komputer dan rangkaian. Indikator kompromi (IOC) merujuk kepada ciri-ciri forensik yang digunakan sebagai petunjuk seperti URL, proses, atau tingkah laku yang tidak normal dikesan pada sesebuah sistem yang telah dikomplomi. Objektif projek ini adalah membangunkan sebuah sistem berdasarkan platform berteraskan simulasi pengasingan dan sandbox. Sistem ini akan berkemampuan untuk menganalisis dan menjana IOC secara automatik untuk membuktikan kebarangkalian sesuatu sampel fail dianggap sebagai sebuah perisian hasad atau sebaliknya. Dalam sistem ini, beberapa teknik pengesanan seperti rujukan padanan tandatangan perisian hasad akan diintegrasi bersama dengan sistem projek. Projek ini akan memanfaatkan penggunaan perisian sandbox sumber terbuka iaitu Cuckoo Sandbox bersama sistem operasi perumah Ubuntu 18.04 dengan integrasi bersama perisian mesin maya VirtualBox dalam membina sebuah persekitaran terasing dengan Microsoft, Windows 7 sebagai sistem operasi tetamu. Beberapa mekasnisme keselamatan dan pengerasan sistem juga diterapkan seperti penetapan tembok api, jadual penghalaan rangkaian dan penyulitan rangkaian menggunakan VPN. Hasil dari projek akan berupaya untuk menjana IOC bagi sesuatu sampel fail atau perisian hasad yang diharapkan dapat menyumbang kepada penghasilan set data IOC.

1 PENGENALAN

Keselamatan rangkaian merupakan salah satu cabang dalam bidang sains komputer yang menekankan kepada melindungi data dan sumber komputer dalam sesebuah rangkaian. Perisian hasad merujuk kepada perisian yang direka khas dengan fungsi tidak baik seperti memintas atau merosakkan sistem komputer tanpa kebenaran (Daniel Schatz, 2017). Sebagai langkah untuk mencegah serangan perisian hasad, analisis perisian hasad akan dilakukan dan akan melibatkan proses seperti mengenal pasti fungsi, asal dan kesan yang dapat dilakukan oleh sesebuah sampel perisian hasad. Hasil laporan dari analisis pula dapat digunakan untuk

membantu dalam mengesan dan mencegah serangan di masa depan. Hasil laporan yang dimaksud adalah penunjuk kompromi (Lord, 2018). Projek ini akan memberi tumpuan kepada kaedah analisis perisian hasad dan penjanaan penunjuk kompromi secara automatik. Cadangan untuk projek ini adalah untuk menghasilkan sebuah system analisis dan penjana penunjuk kompromi automatik berdasarkan teknik analisis. Pembangunan sistem akan menerapkan mekanisme sandbox dalam memastikan proses analisis dijalankan dengan selamat dan terasing. Hasil daripada analisis akan dijadikan set data yang mengandungi pelbagai maklumat varian dan evolusi perisian hasad yang telah dikenal pasti. Projek ini juga bertujuan untuk mengkaji tingkah laku dan hasil analisis perisian hasad dalam persekitaran mesin yang sebenar dan mesin maya.

2 PENYATAAN MASALAH

Berdasarkan penyata masalah yang telah dikenal pasti, projek ini akan dijalankan untuk memenuhi dua objektif berikut:

1. Membina sebuah sistem berasaskan platform yang mampu menganalisis perisian hasad dalam persekitaran terasing, menjana penunjuk kompromi secara automatik serta mampu menyimpan set data penunjuk kompromi untuk sesebuah perisian hasad.

2. Mengkaji keberhasilan mekanisme dan teknik pengerasan keselamatan sistem analisis dalam menjalankan dan menjana hasil analisis yang tepat.

3 OBJEKTIF KAJIAN

Berdasarkan penyata masalah yang telah dikenal pasti, projek ini akan dijalankan untuk memenuhi dua objektif. Pertama, untuk membina sebuah sistem berasaskan platform yang mampu menganalisis perisian hasad dalam persekitaran terasing, menjana penunjuk kompromi secara automatik serta mampu menyimpan set data penunjuk kompromi untuk sesebuah perisian hasad. Kedua, untuk mengkaji keberhasilan mekanisme dan teknik pengerasan keselamatan sistem analisis dalam menjalankan dan menjana hasil analisis yang tepat.

4 METOD KAJIAN

Metod tangkas ataupun agile bakal digunakan dalam pembangunan projek ini. Metod agile dipilih kerana konsepnya yang berdasarkan pendekatan berulang dan kenaikan sistematik untuk menguruskan aktiviti projek dengan lebih baik dalam usaha untuk terus meningkatkan pengembangan produk atau perkhidmatan. Pendekatan ini amat diperlukan dalam perlaksanaan projek ini kerana ianya membolehkan pasukan atau perlaksana projek menerapkan pendekatan berdasarkan perlaksanaan yang lebih pantas, fleksibel, dan kolaboratif ketika bekerja. Metod agile mempunyai empat fasa iaitu keperluan (Requirement), reka bentuk (Design), perlaksanaan (Development), pengujian (Testing), dan perlancaran (Deployment).

4.1 FASA KEPERLUAN

Pada bahagian ini, akan diterangkan berkenaan spesifikasi keperluan yang dicadangkan sesuai dengan objektif projek. Spesifikasi yang akan diterangkan adalah definisi keperluan pengguna, spesifikasi keperluan sistem dan model sistem. Definisi keperluan pengguna akan menghuraikan perkhidmatan yang disediakan untuk pengguna manakala spesifikasi keperluan sistem pula mennyatakan keperluan sistem untuk setiap keperluan pengguna berfungsi, menyatakan kualiti dan keperluan domain yang tidak berfungsi, dan menentukan keperluan perkakasan dan perisian semasa pembangunan serta penggunaan keperluan tersebut.

Skop kegunaan sistem ini adalah berkhususkan kepada keselamatan dan analisis perisian hasad. Ianya hanya ditujukan untuk kegunaan penganalisis perisian hasad yang akan menjadi kedua-dua pengguna dan pentadbir sistem. Sistem sandbox dan penjana indikator kompromi automatik akan digunakan oleh dua kumpulan pengguna iaitu pentadbir dan pengguna biasa yang terdiri daripada penganalisis perisian hasad. Senarai berikut menerangkan kempulan pengguna tersebut.

Pentadbir

Pentadbir ini merujuk kepada individu yang akan mengurus dan mentadbir segala tetapan kepada sistem analisis perisian hasad dan akses kepada pangkalan data analisis dan IOC. Berikut adalah senarai tugas kepada pentadbir.

1. Menyediakan persekitaran analisis perisian hasad yang terasing dan bersih.
2. Menyediakan alatan yang diperlukan untuk menjalankan analisis perisian hasad.

3. Menyediakan mekanisme *pengerasan* kepada sistem hos dan sistem maya untuk tujuan keselamatan
4. Menyediakan mekanisme penyelenggaraan dan pemulihan sistem
5. Membangunkan pangkalan data untuk menyimpan data laporan analisis dan IOC.
6. Menyediakan platform yang membolehkan pengguna untuk melihat hasil laporan analisis.

Pengguna

Pengguna ini merujuk kepada individu yang akan menggunakan sistem penjana penunjuk kompromi. Berikut adalah senarai tugas kepada pengguna.

1. Menjalankan analisis kepada sampel perisian hasad menggunakan sistem analisis
2. Menetapkan peraturan tambahan kepada proses penapisan IOC
3. Menjalankan pencarian dan penjaan IOC berdasarkan hasil dapatan sistem analisis
4. Dapat memuat naik hasil analisis dan IOC ke dalam pengkalan data

Berdasarkan spesifikasi keperluan pengguna yang telah dikenal pasti, spesifikasi keperluan sistem akan dikenal pasti dan akan selaras dengan keperluan pengguna. Keperluan tersebut termasuklah keperluan fungsian pengguna, keperluan fungsian sistem, keperluan bukan berfungsi, keperluan perkakasan dan perisian

4.2 FASA REKA BENTUK

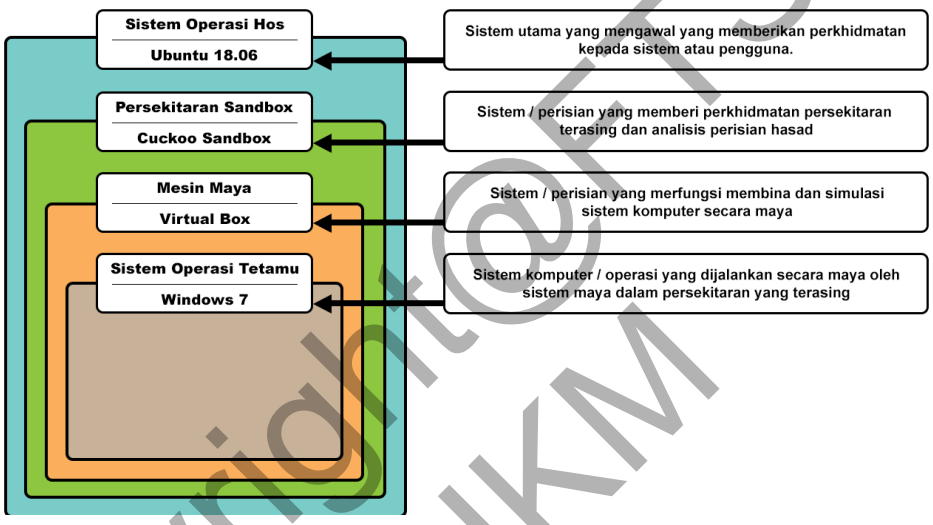
Pada bahagian ini, akan diterangkan berkenaan reka bentuk dan pelan keseluruhan dalam pembangunan sistem dalam memenuhi objektif, perancangan dan keperluan sistem yang telah didokumentasikan. reka bentuk sistem merujuk kepada sebuah dokumentasi yang terperinci kepada reka bentuk seni bina, pangkalan data, algoritma dan integrasi sistem untuk sesebuah sistem atau aplikasi yang bakal dibangunkan (MAHMUD, 2015). Dalam fasa ini, terdapat empat reka bentuk yang dibincangkan iaitu reka bentuk seni bina, reka bentuk pangkalan data, reka bentuk algoritma dan reka bentuk antara muka.

1. Seni Bina

Dalam projek sandbox dan penjana indikator kompromi, terdapat dua seni bina yang terlibat iaitu seni bina berlapis dan seni bina pelayan-pelanggan. Seni bina berlapis adalah khusus untuk reka bentuk pembinaan sistem sandbox dan mesin maya secara bersih dan terasing. Ini ada termasuk

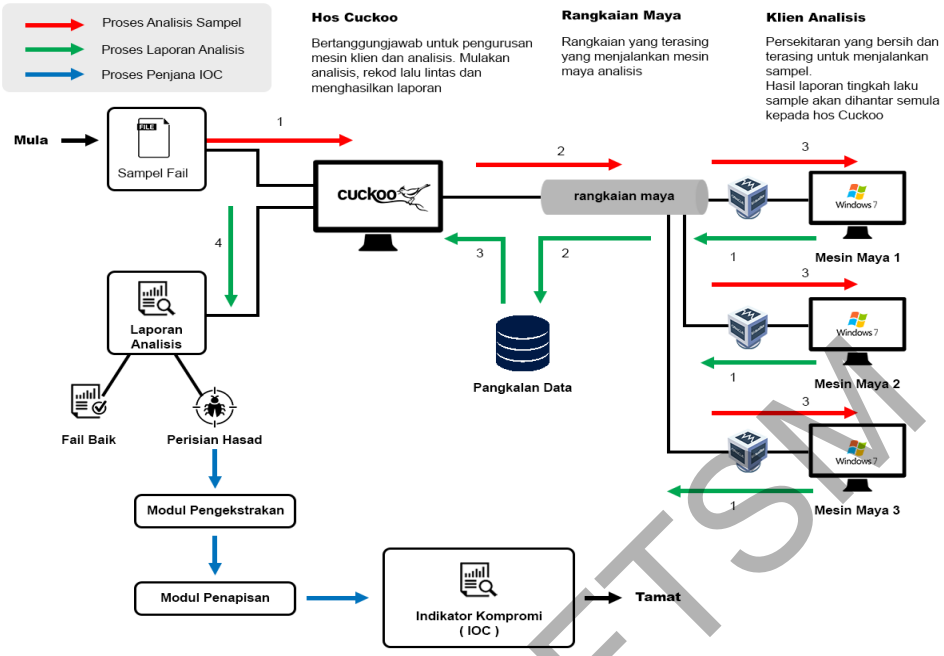
dalam keperluan sistem iaitu pengerasan sistem. Kedua, seni bina pelayan-pelanggan adalah khusus untuk pembinaan modul analisis, laporan dan penjanaan indikator kompromi.

Rajah 1.0 menunjukkan gambaran seni bina berlapis yang diterapkan dalam pembinaan sistem dan mekanisme persekitaran terasing. Pembinaan dimulakan dengan pemilihan sistem operasi hos atau tuan rumah yang akan menempatkan dan mengendalikan sistem sandbox dan analisis yang sebenar. Setelah sistem sandbox dan perisian mesin maya berjaya dipasang, maka sistem operasi tetamu akan dipilih untuk digunakan sebagai sistem pengoperasian kepada proses analisis dan sistem operasi tetamu akan dipilih untuk digunakan sebagai sistem pengoperasian kepada proses analisis.



Rajah 1.0 Ilustrasi Bagi Seni Bina Berlapis Sistem Projek

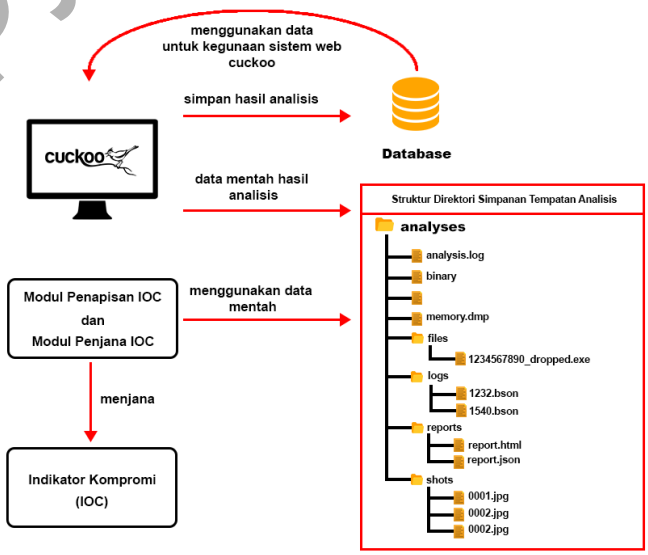
Rajah 2.0 menunjukkan ilustrasi bagi seni bina sistem projek. Penggunaan dan perlaksanaan modul analisis akan bermula setelah penyerahan fail atau URL diserahkan kepada Cuckoo Sandbox. Entri baru akan direkod dalam pangkalan data Cuckoo. Entri ini merujuk kepada maklumat pendaftaran permulaan kepada satu-satu proses analisis yang bakal dilakukan. Sebelum memulakan mesin maya, modul tambahan modul penjadual tugas, pengurus analisis dan pengurus tetamu akan dimulakan. Setelah dimulakan, konfigurasi dan sampel fail akan dimuat naik ke dalam mesin maya oleh pengurus tetamu. Pengurus tetamu bertanggungjawab dalam komunikasi di antara sistem pelayan Cuckoo dan mesin maya.



Rajah 2.0 Ilustrasi Bagi Seni Bina Pelayan-Pelanggan Sistem Projek

Pangkalan Data

Untuk menjalankan analisis dan menyimpan laporan hasil analisis, sistem Cuckoo Sandbox memerlukan struktur data yang flexible dan mudah difahami. Dengan itu, menggunakan dua jenis reka bentuk pangkalan data iaitu penggunaan struktur skema NoSQL (MongoDB) dan JavaScript Object Notation (JSON). Rajah 3.0 menunjukkan aliran yang penyinpanan, struktur dan penggunaan data hasil analisis daripada Cuckoo.



Rajah 3.0 Aliran Yang Penyinpanan, Struktur Dan Penggunaan Data Hasil Analisis Daripada Cuckoo

2. Algoritma

Untuk projek ini, dua algoritma akan digunakan dalam mencapai objektif projek iaitu algoritma analisis dan algoritma penapisan dan penjana IOC. Berikut merupakan penerangan kepada kedua-dua algoritma tersebut.

a. Algotitma Analisis

Algoritma yang diperlukan dalam modul analisis dan pemantauan untuk melaksanakan proses analisis dan pemantauan tingkah laku sampel fail.

b. Algoritma Penapisan Dan Penjana IOC

Algoritma yang berfungsi untuk melakukan penapisan dan pemilihan hasil dapatan analisis untuk dijadikan IOC yang tepat.

3. Antara Muka

Untuk projek ini, tiada reka bentuk antara muka akan dibuat kerana projek ini akan menggunakan reka bentuk antara muka yang disediakan oleh Cuckoo Sandbox. Oleh kerana seni bina antara muka Cuckoo telah memenuhi sepenuhnya keperluan kepada penggunaan sistem ini. Cuckoo menggunakan platform web untuk mengendalikan sistem secara grafik menggunakan sistem Django.

4.3 FASA PERLAKSANAAN

Pada bahagian ini, akan diterangkan langkah-langkah serta dokumentasi kepada fasa pembangunan projek. Fasa ini akan menukar prototaip reka bentuk sistem dalam fasa reka bentuk menjadi sistem maklumat berfungsi yang memenuhi semua keperluan sistem yang didokumentasikan. Dalam fasa perlaksaan dan pembangunan projekini, terdapat beberapa proses yang akan dijalankan. Proses-proses tersebut termasuklah penyediaan keperluan sistem, pemasangan sistem perumah, pemasangan sistem sandbox dan mesin maya, dan pengubahsuaian konfigurasi sistem Cuckoo Sandbox dan mesin maya.

Sebelum proses pemasangan dan pembangunan sistem bagi projek bermula, penyediaan keperluan sistem merupakan proses yang paling asas dan terawal dijalankan. Berikut merupakan perincian keperluan sistem yang perlu dipenuhi.

Jadual 1.0 Senarai Perisian Dan Sistem Yang Diperlukan Untuk Permulaan Projek

Perisian/Sistem		
Nama	Versi	Pautan Sumber Dapatan
Ubuntu OS	18.04.5 (LTS)	https://rufus.ie/en_US/
Rufus	3.13	https://releases.ubuntu.com/18.04/

Jadual 2.0 Senarai Peranti Yang Diperlukan Untuk Permulaan Projek

	Peranti
Nama	Spesifikasi
Alat Simpanan Komputer	Kapasiti minimum 480GB Jenis SSD (cadangan) atau HDD
Memori Capaian Rawak (RAM)	Kapasiti minimum 8GB
Pemacu Kilat Jenis USB	Kapasiti minimum 8GB

Item dalam senarai jadual 1 merupakan keperluan perisian dan sistem yang diperlukan untuk memasang sistem perumah bagi projek ini iaitu Ubuntu 18.04. Manakala, item dalam senarai jadual 2 merupakan peranti-peranti bagi keperluan projek. Seterusnya, berikut merupakan proses pambangunan sistem sandbox dan penjana indikator kompromi yang terdiri daripada proses pembuatan media pemasangan sistem operasi perumah, pemasangan sistem sandbox & mesin maya, ubah suai konfigurasi cuckoo sandbox, tetapan mekanisme pengerasan sistem perumah dan cuckoo, dan tetapan mekanisme pengerasan sistem.

1. Pembuatan Media Pemasangan Sistem Operasi Perumah

a. Ubah Suai Tetapan Sistem BIOS
   i. Nyahaktif Tetapan Secure Boot
   ii. Tukar sususan media boot keutamaan sistem kepada peranti media pemasangan sistem operasi perumah

b. Pemasangan Sistem Operasi Perumah

2. Pemasangan Sistem Sandbox & Mesin Maya

Berikut merupakan arahan system terminal Ubuntu yang diperlukan untuk pemasangan pakej cuckoo sandbox dalam projek ini.

a. Pasang Perisan Pemulihan Sistem Pada Ubuntu 18.04
b. Kemas Kini Sistem Ubuntu 18.04
c. Membuat Pengguna Baru Dengan Tahap Akses Sistem Bawahan
d. Pemasangan Pakej Kebergantungan Sistem Sandbox & Mesin Maya
    i. Cara Pemasangan Pakej Secara Manual
    ii. Cara Pemasangan Pakej Secara Automatik

```
$ sudo apt update
$ sudo apt install python python-pip python-dev libffi-dev libssl-dev
$ sudo apt install python-virtualenv python-setuptools
$ sudo apt install libjpeg-dev zlib1g-dev swig
$ sudo apt install mongodb
$ sudo apt install postgresql libpq-dev
$ 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 apt install volatility
$ sudo pip install m2crypto
$ wget https://cuckoo.sh/win7ultimate.iso
$ sudo mkdir /mnt/win7
$ sudo mount -o ro,loop win7ultimate.iso /mnt/win7
$ sudo apt update && sudo apt -y install virtualenv
$ sudo apt -y install virtualenvwrapper
$ echo "source /usr/share/virtualenvwrapper/virtualenvwrapper.sh" >> ~/.bashrc
# Pasang pip untuk python3
$ sudo apt-get -y install python3-pip
# Aktifkan bash untuk pip
$ pip3 completion --bash >> ~/.bashrc
# Menghalang permasangan sekali dengan root
$ pip3 install --user virtualenvwrapper
```

e. Pemasangan Sistem Sandbox Cuckoo dan Mesin Maya VirtualBox

Berikut merupakan arahan dan tetapan yang diperlukan untuk memasang sistem sandbox Cuckoo dan mesin maya VirtualBox dalam persekitaran yang terasing.

```
$ sudo su cuckoo
$ virtualenv ~/cuckoo
$ . ~/cuckoo/bin/activate
$ workon cuckoo-test
(cuckoo) $ pip install -U pip setuptools
(cuckoo) $ pip install -U cuckoo
(cuckoo) $ pip install -U vmcloak
(cuckoo) $ vmcloak-vboxnet0
(cuckoo) $ vmcloak init --verbose --win7x64 win7x64base --cpus 2 --ramsize 2048
(cuckoo) $ vmcloak clone win7x64base win7x64cuckoo
(cuckoo) $ vmcloak install win7x64cuckoo adobe9.version=11.0.19 adobepdf.version=11.0.19
pillow java java.version=8u151 java.version=jdk8u121 firefox_41 chrome.version=latest flash
vcredist vcredist.version=2015u3 winrar wallpaper
(cuckoo-test) $ vmcloak snapshot --count 3 win7x64cuckoo 192.168.56.101
$ workon cuckoo-test
(cuckoo) $ cuckoo init
(cuckoo) $ cd ~/.cuckoo/conf
(cuckoo) $  cuckoo community –force
(cuckoo) $ while read -r vm ip; do cuckoo machine --add $vm $ip; done < <(vmcloak list vms)
```

Maka dengan ini, selesailah proses pemasangan sistem sandbox dan mesin maya projek ini iaitu Cuckoo Sandbox dan VirtualBox. Pada peringkat ini, Cuckoo telah berjaya dipasang tetapi masih belum boleh digunakan.

3. Ubah Suai Konfigurasi Cuckoo Sandbox

a. Meningkatkan Had Fail

Buka fail ***limits.conf*** pada lokasi ***/etc/security/*** sebagai root atau pentadbir.

```
$sudo nano /etc/security/limits.conf
```

Masukkan baris berikut pada pengakhiran fail ***limit.conf***

```
*       hard    nofile  500000
*       soft    nofile  500000
Root    hard    nofile  500000
```

```
Root    soft    nofile  500000
```

b. Postgres Sebagai Sistem Pengurusan Pangkalan Data

Berdasarkan dokumentasi sistem Cuckoo Sandbox (Sandbox, Cuckoo Sandbox Book, 2020), pengguna di syorkan untuk beralih ke pangkalan data MySQL atau PostgreSQL kerana SQLite boleh memyebabkan masalah seperti had menjalankan analisis mesin maya berganda. Berikut merupakan arahan yg diperlukan untuk tetapan tersebut.

```
$ sudo apt-get postgresql postgresql-contrib
$sudo -u postgres psql
```

Arahan konfigurasi Postgres:

```
CREATE DATABASE cuckoo;
CREATE USER cuckoo WITH ENCRYPTED PASSWORD 'password';
GRANT ALL PRIVILEGES ON DATABASE cuckoo TO cuckoo;
\q
```

```
$ workon cuckoo-test
(cuckoo-test) $ pip install psycopg2
(cuckoo-test) $ cd ~/.cuckoo/conf
(cuckoo-test) $ nano ~/.cuckoo/conf/cuckoo.conf
```

Tetapkan konfigurasi Cuckoo untuk menggunakan Postgres dan bukannya SQLite seperti berikut:

```
connection = postgresql://cuckoo:password@localhost/cuckoo
```

Tetapan Mekanisme Pengerasan Sistem Perumah dan Cuckoo

1. Peraturan Pemajuan Global Internet

```
$sudo sysctl -w net.ipv4.conf.vboxnet0.forwarding=1
$sudo sysctl -w net.ipv4.conf.wlp2s0.forwarding=1

$sudo iptables -t nat -A POSTROUTING -o eth0 -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
```

Tetapkan kebenaran penghalaan permintaan keluar-masuk dalam rangkaian kepada antara muka vboxnet0 dan antara muka keluar sistem perumah, ***wlp2s0.*** Alamat IP 192.168.56.0/24 pada arahan diatas merujuk kepada alamat IP mesin-mesin maya yang didaftarkan pada Cuckoo

2. Penghalaan Rangkaian Melalui VPN

Untuk projek ini, sistem VPN TunnelBear akan digunakan sebagai sistem pelayan VPN utama sistem perumah dan Cuckoo Sandbox dalam melayari Internet. Berikut merupakan langkah yang dilaksanakan untuk mendaftar dan membenarkan VPN pada sistem perumah Ubuntu dan juga pada mekamisme penghalaan sistem Cuckoo.

```
https://www.tunnelbear.com/account/login
https://tunnelbear.s3.amazonaws.com/support/linux/openvpn.zip
```

```
sudo apt install network-manager-openvpn-gnome -y
```

Buka pelayar web dan masuk kepada laman sesawang daftar akaun TunnelBear dan muat turun turun fail konfigurasi TunnelBear OpenVPN. Seterusnya, daftarkan perkhidmatan VPN pada sistem Ubuntu.Akhir sekali, tetapkan konfigurasi berikut kepada cuckoo dan daftarkan perkhidmatan VPN pada senarai jadual penghalaan rangkaian Ubuntu.

```
[vpn]
enabled = yes
vpns = vpn0

[vpn0]
name = vpn0
description = Spain, Europe
interface = vpn0
rt_table = vpn0
```

```
# reserved values
255     local
254     main
253     default
0       unspec
# local
300     wlp2s0
400     tun0
```

4.4 FASA PENGUJIAN

Pada bahagian ini, akan diterangkan berkenaan penghasilan pelan pengujian, reka bentuk kes pegujian, pengujian dan penghasilan keputusan pengujian sebelum sistem dilancarkan. Sebelum proses pengujian dijalankan, pelan pengujian hendaklah dirancang bagi membolehkan kelancaran dan tiada kekurangan dari segi keperluan projek. Perancangan akan dibahagikan kepada dua iaitu pengujian fungsional yang menguji apa dilakukan oleh sesebuah sistem dan pengujian bukan fungsional yang menguji cara sesebuah sistem beroperasi, dan bukannya tingkah laku khusus sistem tersebut. Berikut merupakan senarai pengujian fungsional dan pengujian bukan fungsional projek.

Jadual 3.0 Seenarai Pengujian Fungsional Dan Pengujian Bukan Fungsional Projek

Pengujian	**Butiran Fungsi**
Fungsional	1. Muat Naik Sampel Fail atau Pautan URL 2. Memilih Tetapan Analisis Dengan Sambungan Rangkaian (Internet, VPN, None) 3. Memilih tetapan masa perlaksanaan analisis 4. Pemilihan mesin maya proses analisis 5. Menjalankan analisis perisian hasad 6. Melihat dan muat turun laporan analisis
Bukan Fungsional	1. Mekanisme penyulitan dan terowong VPN 2. Akses kepada rangkaian utama daripada sistem tetamu

1. Reka Bentuk Pengujian Kes

Jenis pengujian yang bakal digunakan adalah kaedah pengujian kotak hitam dan kotak putih. Bagi kaedah ujian kotak hitam, ianya akan dijalankan untuk pengujian berfungsi projek. Pengujian kotak hitam merupakan teknik pengujian yang menguji fungsi sesebuah sistem tanpa mengetahui struktur dalaman atau cara kerja sistem tersebut. Untuk pengujian bukan fungsional projek akan dilaksanakan mengguna kaedah pengujian kotak putih. Ujian ini akan dijalankan dengan memantau dan analisa sambungan rangkaian daripada sistem perumah, Ubuntu dan sistem tetamu, mesin maya. Segala perancangan pengujian akan dilaksanakan dan hasilnya akan direkod. Perlaksanaan ini akan fokus kepada pengujian kotak hitam dan kotak putih.

2. Ujian Penerimaan Pengguna

Untuk mendapatkan maklum balas dan hasil ujian yang lebih baik, ujian penerimaan pengguna akan dilaksanakan. Ujian ini akan dilakukan oleh pengguna sebenarnya bagi menguji sistem untuk melihat sama ada ianya dapat melaksanakan tugas yang sepatutnya berdasarkan perancangan projek. Pengguna ini akan diarahkan untuk menggunakan sistem yang telah dibangunkan untuk menganalisis sample fail. Sepanjang menggunakan sistem tersebut, segala komen dan cara penggunaan mereka akan direkod. Pada akhir proses ini, maka sebuah laporan akan dibuat untuk melaporkan secara bertulis tentang hasil pengujian yang dijalankan. Berikut merupakan soalan maklum balas pengguna untuk projek ini.

Borang Maklum Balas Pengujian Sistem

BORANG MAKLUM BALAS PENGUJIAN SISTEM ANALISIS PERISIAN HASAD MENGGUNAKAN CUCKOO SANDBOX

Arahan: Tandakan [✓] pada pilihan jawapan yang paling sesuai berdasarkan panduan yang diberikan. Pilih satu jawapan sahaja dan diharapkan maklum balas yang diberikan adalah jujur berdasarkan pengalaman menggunakan sistem yang diuji.

BAHAGIAN A:

Kepakaran Dalam Bidang IT:

Pengaturcaraan	**[ ]**	Teknologi Rangkaian	**[ ]**

Sains Data	**[ ]**	Keselamatan Siber	**[ ]**
Kecerdasan Buatan	**[ ]**	Multimedia	**[ ]**

Jantina:

Lelaki	[ ]	Perempuan	**[ ]**

Soalan ini berkaitan dengan penerimaan dan maklum balas terhadap penggunaan sistem yang diuji untuk menjalankan analisis dan menjana penunjuk kompromi perisian hasad.

BAHAGIAN B: **Panduan:**

1 Sangat Setuju (SS)
2 Setuju (S)
3 Agak Setuju (AS)
4 **Kurang Setuju (KS)**

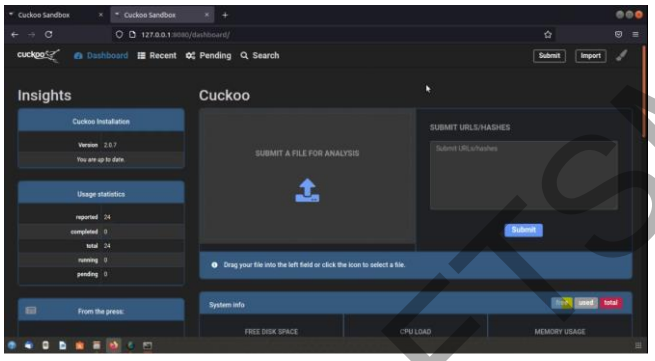
BIL	ITEM	1 (SS)	2 (S)	3 (AS)	4 (KS)
1	Sample fail dan URL perisian hasad dapat dipilih dan dimuat naik untuk tujuan analisis.				
2	Semua tetapan analisis perisian hasad yang disediakan berfungsi dengan baik.				
3	Mesin maya dapat berjalan dan berfungsi dengan baik setiap kali proses analisis dimulakan.				
4	Fungsi penghalaan rangkaian melalui Internet secara terus berjalan dengan baik				
5	Fungsi penghalaan rangkaian Internet melalui VPN berjalan dengan baik.				
6	Sistem memberikan laporan yang lengkap dan consisten untuk setiap analisis.				
7	Hasil laporan semasa dan terdahulu dapat dilihat berulang kali dan dimuat naik dengan sempurna.				
8	Saya berasa selamat dan yakin dengan keselamatan semasa menjalankan analisis perisian hasad menggunakan sistem yang disediakan.				
9	Sistem menyediakan fungsi lengkap untuk menganalisis perisian hasad.				
10	Saya mudah faham dan mampu menggunakan sistem ini dengan baik setelah satu hingga dua kali pencubaan.				

Komen tambahan:

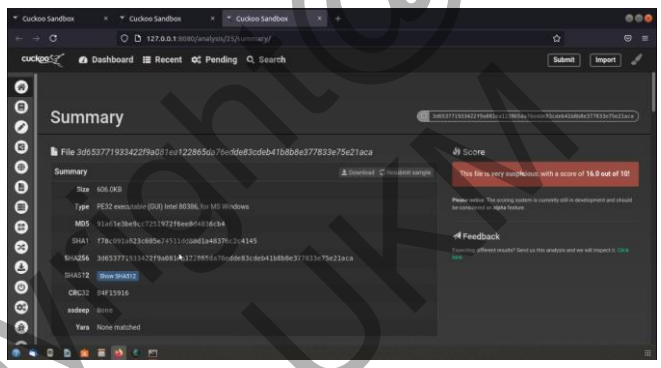
SEKIAN TERIMA KASIH
TAMAT

5 HASIL KAJIAN

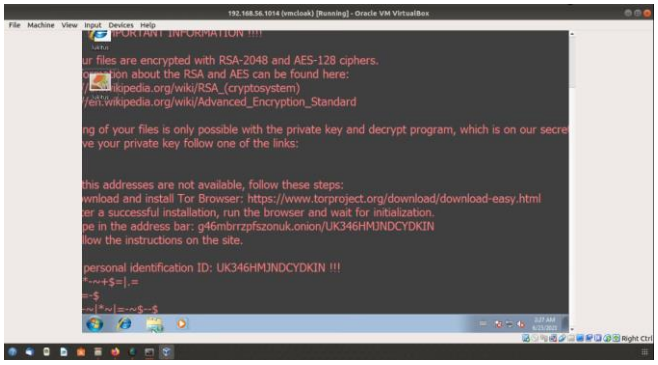
Bahagian ini menerangkan hasil daripada fasa pembangunan dan perlaksanaan projek sandbox dan penjana indikator kompromi automatik. Selain itu, ianya juga akan menerangkan hasil daripada fasa pengujian sistem projek. Berikut merupakan hasil daripada pembangunan projek sandbox dan penjana indikator kompromi automatik.



Rajah 4.0 Antara Muka Utama Web Cuckoo Sandbox



Rajah 5.0 Contoh Laporan Analisis Perisian Hasad Perisian Tebusan



Rajah 6.0 Contoh Analisis Perisian Hasad Jenis Perisian Tebusan

Setelah borang maklum balas diberikan kepada pengguna selesai sahaja menggunakan sistem dan berhasil menjalankan analisis perisian hasad. Rumusan daripada pengujian akan dikumpul dan telah berjaya dirumuskan seperti yang ditunjukkan pada jadual 3.0.

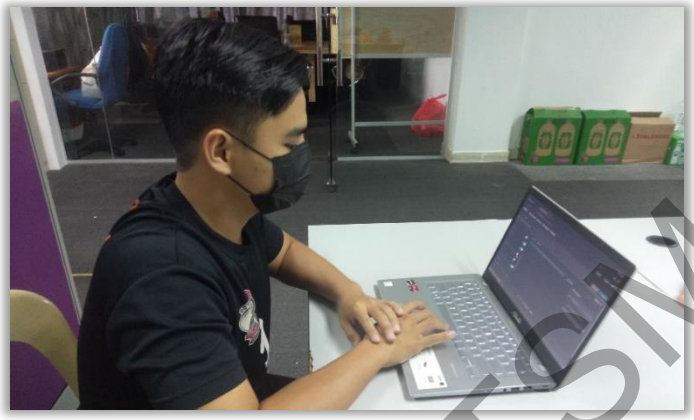
Jadual 3.0 Rumusan Maklum Balas Responden Pengujian Sistem

ID Ujian	Sangat Setuju	Setuju	Agak Setuju	Kurang Setuju
Soalan 1	5	-	-	-
Soalan 2	1	-	3	1
Soalan 3	5	-	-	-
Soalan 4	5	-	-	-
Soalan 5	1	-	-	4
Soalan 6	1	4	-	-
Soalan 7	5	-	-	-
Soalan 8	1	3	1	-
Soalan 9	4	-	1	-
Soalan 10	2	2	1	-

Berdasarkan rumusan tersebut, hampir kesemua pengguna berpuas hati dengan kebolehan analisis, dan penghasilan laporan analisis daripada sistem yang diperkenalkan. Namun begitu, terdapat beberapa perkara yang boleh diperlihatkan semula seperti kebolehgunaan fungsi dan tetapan yang disediakan. Berdasarkan soalan 3, dapat dilihat bahawa 80% responden memberikan maklum balas yang kurang baik di mana terdapat beberapa fungsi tidak dapat dijalankan dengan baik seperti fungsi sambungan rangakaian Internet melalui VPN yang tidak berfungsi semasa pengujian dilaksanankan. 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.

Secara rumus, 70% hingga 80% daripada responden berpendapat projek ini berjalan dengan baik walaupun terdapat sedikit masalah berkaitan fungsi yang tidak berfungsi dengan baik. Selain itu, responden juga memberikan maklum balas positif terhadap keselamatan

semasa menjalankan analisis walaupun mereka sedia maklum bahawa analisis yang dijalankan adalah melibatkan perisian hasad yang aktif dan berbahaya.



Rajah 7.0 Contoh Pengguna dan Responden Pengujian Sistem

6 KESIMPULAN

Secara keseluruhannya, projek sandbox dan penjana indikator kompromi automatik telah berjaya melengkapkan segala keperluan dalam proses usulan dan perancangan projek. Proses yang telah dijalankan termasuklah penghasilan projek, kajian sastera berkaitan projek, mengenal pasti keperluan pengguna dan reka bentuk sistem. Hasil daripada ke semua proses tersebut telah didokumentasikan dalam kertas laporan ataupun tesis ini. Projek ini dibangunkan untuk menangasi masalah dalam keselamatan sistem komputer dan rangkaian yang berkaitan dengan menangani serangan daripada perisian hasad. Objektif projek adalah untuk menjana indikator kompromi iaitu sesuatu petunjuk atau tandatangan sesuatu perisian hasad yang boleh digunakan oleh sistem keselamatan dalam mengenal pasti kehadiran perisian hasad.

Dalam perlaksanaan dan pembangunan projek ini, dapat dirumuskan beberapa kekangan dan batasan yang dihadapi adalah keselamatan penuh sistem analisis dan fungsi pengesanan perjalanan mesin maya atau sandbox dalam perisian hasad. Untuk kekangan keselamatan penuh sistem analisis, walaupun sistem menjalankan sampel perisian hasad dalam persekitaran yang terasing daripada sistem pengguna yang sebenar, namun ianya masih tidak dapat menjamin sepenuhnya keselamatan terhadap perisian hasad tersebut kerana peluang untuk berlakunya pintasan terhadap sistem analisis kepada sistem hos adalah tinggi sekiranya tetapan keselamatan tidak di reka dengan baik. Seterusnya, sesetengah perisian hasad mempunyai fungsi atau variasi yang membolehkan ianya untuk mengesan persekitaran di mana

dijalankan. Oleh itu, apabila ianya dijalankan dalam persekitaran mesin maya atau sandbox, kebarangkalian untuk perisian hasad tersebut untuk akan tidak berjalan sepenuhnya atau menunjukkan tingkah lakunya yang sebenar adalah tinggi.

Untuk rancangan peningkatan masa hadapan, diharapkan projek ini dapat ditambahkan fungsi analisis secara dalam talian yang bermaksud pengguna dapat memuat naik sampel fail melalui akses jauh atau dalam talian. Juga diharapkan supaya penerapan kaedah pengerasan keselamatan boleh ditambah dengan lebih banyak seperti pembolehan akses internet dalam sistem analisis tanpa membolehkan akses daripada perisian hasad untuk melepasi sistem utama atau hos.

Secara keseluruhan, bahagian ini telah merumuskan kajian dan dapatan daripada permulaan proses dokumentasi bermula daripada tujuan dan proses pembangunan projek, kekangan dan penambahbaikan masa hadapan projek. Daripada kekangan yang dikenal pasti, diharapkan penambahbaikan masa hadapan yang dirancang dapat mengatasi kenangan tersebut sekaligus mampu menambahkan nilai komersial dan kebolehgunaan projek untuk tujuan analisis perisian hasad dan penghasilan indikator kompromi

7 RUJUKAN

Assor, Y. (2016, August 5). *Anti-VM and Anti-Sandbox Explained*. Didapatkan 11 5, 2020, daripada CYBERBIT: https://www.cyberbit.com/blog/endpoint-security/anti-vm-and-anti-sandbox-explained/

Daniel Schatz, R. B. (2017). *Towards a More Representative Definition of Cyber Security.* Asociation of Digital Forensics, Security and Law (ADFSL. Didapatkan March 20, 2021, daripada https://commons.erau.edu/jdfsl/vol12/iss2/8/

Liza Hazevytch . (2020, February 26). *Agile Advantages for Software Development and Your Business.* Didapatkan dari DevCom: https://devcom.com/tech-blog/agile-advantages-for-business/

Lord, N. (2018). *What are Indicators of Compromise?* (N. Lord, Editor) Didapatkan 2020, daripada Data Insider: https://digitalguardian.com/blog/what-are-indicators-compromise

McAfee. (2019). *McAfee Labs Threats Report.* Statistics. Didapatkan November 2020, daripada https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf

Rigby, D. K., Sutherland, J., & Takeuchi, H. (2016). *Embracing Agile*. Didapatkan dari Harvard Business Review: https://hbr.org/2016/05/embracing-agile