Implementasi Network Intrusion Detection System pada Sistem Smart Identification

Sofyan Hadi
D3 Teknik Komputer Fakultas Ilmu Terapan
Universitas Telkom
Bandung, Indonesia
sofyanhadi.mr@gmail.com

Periyadi, S.T., M.T.
D3 Teknik Komputer Fakultas Ilmu Terapan
Universitas Telkom
Bandung, Indonesia
periyadi2k9@gmail.com

Anang Sularsa, S.T., M.T.
D3 Teknik Komputer Fakultas Ilmu Terapan
Universitas Telkom
Bandung, Indonesia
ananks@gmail.com

Abstrak—Smart Identification merupakan system yang mengintegrasikan *server* dengan perangkat *mobile* yang digunakan mahasiswa dengan memanfaatkan teknologi wireless untuk melakukan absensi. Smart identification akan mengidentifikasi *Mac address* yang terdapat pada perangkat *mobile* yang digunakan mahasiswa untuk pencatatan absensi, maka akan lebih efisien jika melakukan absensi hanya dengan menghubungkan smartphone pada *access point*. Terhubungnya perangkat pada suatu jaringan pasti akan ada masalah yang terjadi. Masalah yang sering terjadi adalah *Port-Scanning, Exploit* dan *Denial of Services*. Untuk mengatasi masalah keamanan jaringan perlu adanya pengawasan dalam jaringan. *Network Intrusion Detection System* merupakan perangkat lunak yang bekerja secara otomatis untuk memonitor suatu kejadian serta paket data yang masuk pada jaringan. NIDS dapat mendeteksi adanya serangan yang terjadi dan mengirimkan notifikasi berupa sms atau melalui *web interface*. Dalam penelitian ini Aplikasi NIDS yang digunakan adalah suricata, untuk mengirimkan sms melalui aplikasi gammu dan web interface menggunakan snorby.

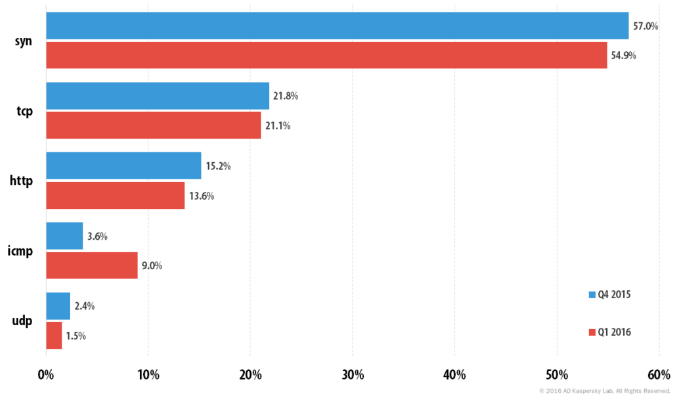
Kata Kunci—*Smart Identification; Mac address; Keamanan Jaringan; Network Intrusion Detection System*

Abstract— Smart identification is a system that integrates server with mobile devices that are used by students using wireless technology to mark the attendance. Smart identification will identify the student's mobile device's MAC address, so it'll be more efficient for the attendace system 'cause it'll only require students to connect to access points. Connection of devices on a network would have a problem occurs. Port scanning, Exploit and Denial of Services is some of the problems that often occur in network security. To solve those network serity problems, a network monitoring system is needed. NIDS is a software that automatically works to monitor an event and data packets that comes through the network. With NIDS server in the smart identification system, it can detect any attacks and sending notifications like sms or web interface. In this research, suricata is the NIDS aplication used, to send sms via gammu and web interface using snorby.

Keywords—Smart Identification; Mac address; Network Security; Network Intrusion Detection System

I. PENDAHULUAN

Smart Identification merupakan sistem yang mengintegrasikan *access point* dengan perangkat *mobile* untuk melakukan absensi secara otomatisasi. Server akan mendapatkan data dari perangkat *mobile* yang terhubung dengan Access point. Data yang didapat berupa *Mac address* dari setiap perangkat *mobile* yang terhubung. Setiap perangkat yang terhubung pada jaringan komputer pasti akan mengalami masalah pada sisi keamanan jaringan. Banyak masalah yang sering terjadi pada keamanan jaringan dikarenakan sering terjadi *Port-Scanning*, *Malware* dan *Denial of Services* (DoS/DDoS). Berikut data hasil dari perbandingan tipe serangan DdoS attack yang terjadi pada kuartal keempat 2015 dan kuartal pertama 2016.



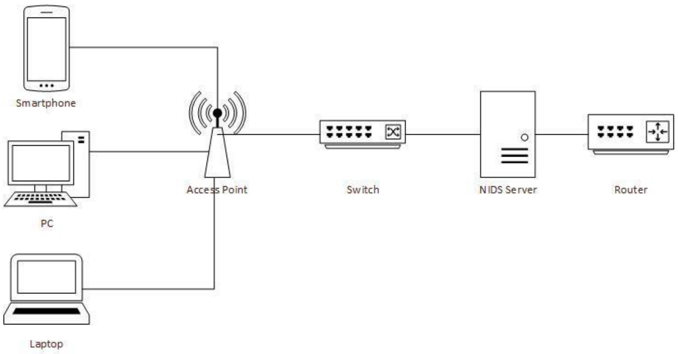
Gambar I-1 Perbandingan tipe Serangan DDoS

Masalah tersebut terjadi akibat dari kelemahan sistem keamanan jaringan. Untuk mengatasi masalah keamanan jaringan dan sistem pada jaringan perlu adanya pengawasan dalam suatu jaringan, *Network Intrusion Detection System* (NIDS) adalah perangkat lunak (*software*) yang bekerja secara otomatis untuk memonitor suatu *event*/kejadian serta paket data yang masuk pada jaringan. Dalam penelitian ini aplikasi Intrusion Detection System yang digunakan adalah suricata. Untuk mengirimkan notifikasi serangan yang terjadi suricata membutuhkan beberapa aplikasi tambahan seperti : barnyard2, snorby, gammu, MySQL dan PHP.

Penelitian ini dilakukan untuk memudahkan pemberitahuan notifikasi serangan kepada administrator agar administrator dapat langsung melakukan tindakan jika terjadi masalah pada server Smart Identification.

II. TINJAUAN PUSTAKA

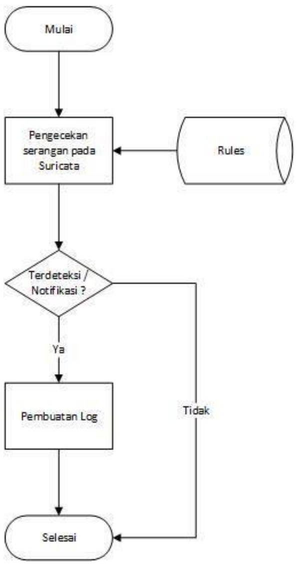
A. Intrusion Detection System (IDS)



Gambar II-1 Ilustrasi Skema NIDS

IDS merupakan perangkat keras atau lunak yang digunakan untuk memonitoring aktifitas jaringan yang dapat merusak atau melanggar aturan dan melaporkan nya. IDS hanya berfokus untuk mengidentifikasi serangan yang terjadi dan ketika serangan itu terjadi IDS akan membuat sebuah *report/*laporan. [1]

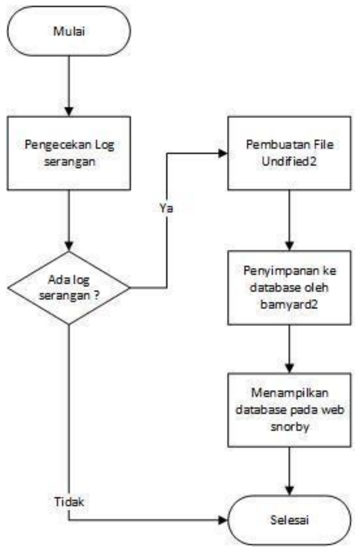
B. Suricata



Gambar II-2 Cara kerja suricata

Suricata merupakan IDS yang dapat mendeteksi aktifitas ancaman serangan pada jaringan yang dibantu dengan rules yang telah ada. [2] Cara kerja dari suricata adalah ketika adanya penyerangan suricata akan melakukan pengecekan paket/serangan yang ada melalui rules yang dibuat. Ketika serangan terdeteksi maka suricata akan membuat log serangan yang dilakukan.

C. Snorby



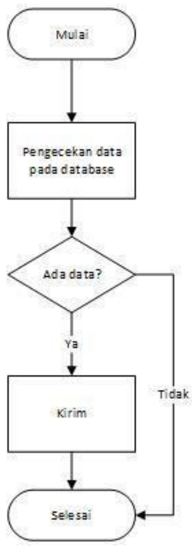
Gambar II-3 Cara kerja snorby

Snorby merupakan web interface yang digunakan untuk memonitoring suatu keamanan jaringan komputer dengan tampilan berbasis GUI (Graphical User Interface) yang terintegrasi dengan suricata. Fitur dari snorby adalah dapat menampilkan data kejadian/event serangan dari suricata dalam tampilan grafis. [3] Cara kerja snorby adalah ketika adanya serangan suricata akan membuat file berupa log penyerangan yang terhubung dengan barnyard2. File tersebut adalah file undified2 adalah file notifikasi yang dibuat oleh barnyard2. Setelah log terbuat barnyard2 akan memasukan log tersebut ke dalam database, lalu snorby akan menampilkan log penyerangan pada web interface snorby.

D. Barnyard2

Barnyard2 adalah aplikasi yang melakukan perekaman data hasil dari serangan pada suricata dan menyimpannya dalam bentuk database yang ditentukan dengan format tersendiri. [4]

E. Gammu



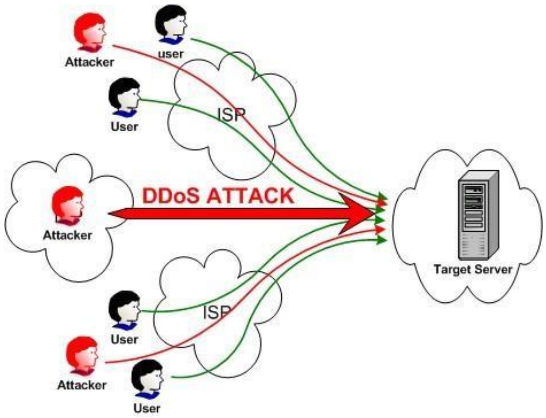
Gambar II-4 Cara kerja gammu

Gammu merupakan aplikasi yang digunakan untuk membuat SMS gateway [5]. Cara kerja gammu adalah database akan di tampilkan ke web interface mengenai pesan masuk ataupun keluar dan ketika menjalankan gammu smsd maka setiap data inputan ke dalam tabel outbox maka pesan akan di kirim ke nomortujuan melalui modem.

F. Port Scanning

Port Scanning merupakan metode mendeteksi port pada suatu target untuk melihat port apa saja yang aktif. Port scanning biasanya digunakan untuk memulai suatu serangan pada target yang akan diserang. [6]

G. Denial of Service (DoS)



Gambar II-5 Ilustrasi penyerangan dos attack [7]

DoS attack merupakan salah satu serangan yang sering digunakan. Serangan yang dilakukan adalah menggunakan banyak komputer untuk menyerang satu target, penyerangan dilakukan secara bersamaan tanpa melihat jarak dan waktu. [8]

H. Exploit

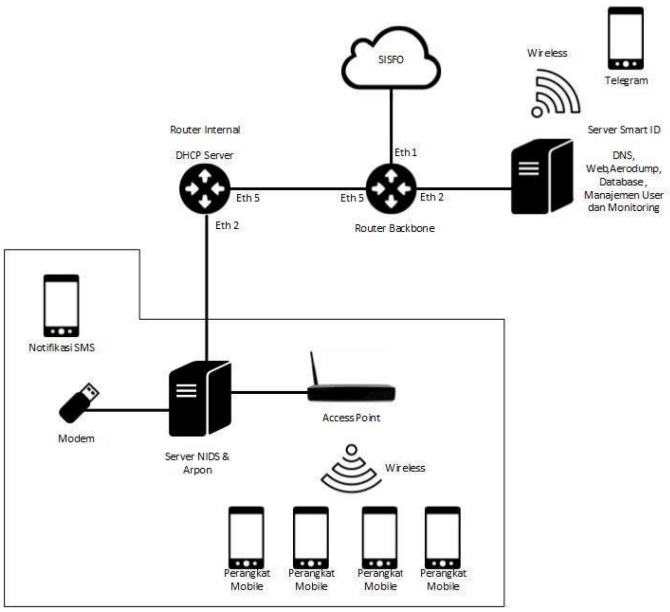
Gambar II-6 Metasplot, Salah satu tools exploit [9]

Exploit adlaah suatu pernagkat lunak yang digunakan untuk menyerang kelemahan dalam suatu sistem secara spesifik untuk mendapatkan hak akses atau melakukan infeksi terhadap target yang diserang. [10]

III. ANALISIS DAN PERANCANGAN

Jaringan sistem *smart identification* menggunakan beberapa perangkat seperti server, router dan akses point. Pada bagian ini akan dijelaskan mengenai gambaran sistem, analisis kebutuhan sistem dan kebutuhan perangkat.

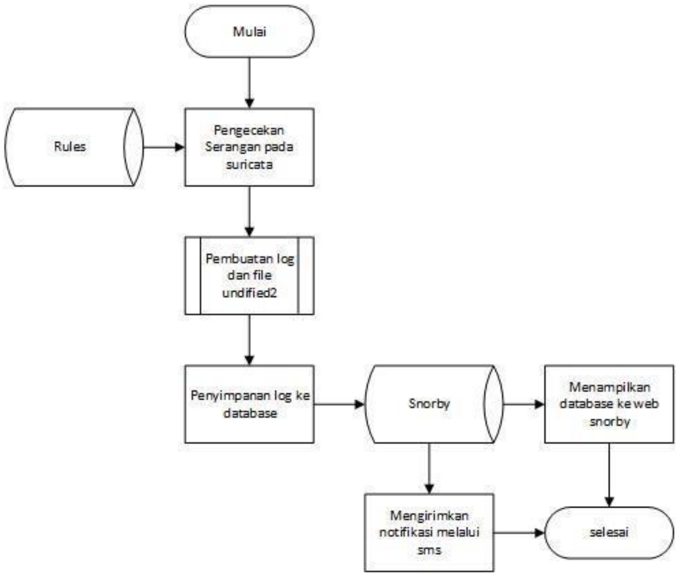
A. Gambaran Sistem



Gambar III-1 Struktur sistem

IDS Suricata akan diimplementasikan pada OS Linux yang dipasangi juga DNS dan Web Server sebagai layanan yang diberikan. Suricata dan layanan dipasang pada OS Ubuntu Server 14.04. OS tersebut dipasang pada server. Web server dibangun untuk membuat Gammu web interface. Modem digunakan untuk melakukan pengiriman sms gateway. Sedangkan DNS Server untuk memudahkan pengaksesan terhadap nama domain. Pada proyek akhir ini sistem yang dikerjakan diberi tanda dengan kotak garis hitam

B. Analisis Kebutuhan Sistem



Gambar III-2 Alur Sistem

Network Intrusion Detection System (NIDS) server membutuhkan beberapa aplikasi dan program yang digunakan. Suricata digunakan untuk mendeteksi adanya serangan yang terjadi dan hasil notifikasi tersebut tersimpan dalam bentuk log. Untuk menyimpan log tersebut menjadi database dibutuhkannya barnyard2 dan snorby untuk menyimpan data notifikasi tersebut ke dalam database. Data tersebut akan diintegrasikan dengan snorby melalui barnyard2 dengan membuat sensor. Sensor tersebut yang akan mengambil data dari barnyard untuk ditampilkan pada web interface snorby. Kemudian database yang berisikan event/notifikasi serangan yang terdapat pada snorby diambil untuk dikirimkan melalui sms dengan menggunakan gammu. Sedangkan Linux Dash dan Sar digunakan untuk menampilkan informasi mengenai penggunaan pemakaian Disk, CPU, RAM, Users, dan Network.

C. Kebutuhan Perangakat.

1) Kebutuhan perangkat keras

Tabel III-1 Kebutuhan perangkat keras

No.	Nama	Spesifikasi	Deskripsi
1.	Server IDS	Intel (R) Xeon 4GHz 4 GB DDR3 300 GB *Harddisk*	Perangkat yang digunakan sebagai server NIDS
2.	Modem	Huawei Mobile Broadband E1553	Perangkat yang digunakan untuk mengirimkan notifikasi melalui sms
3.	Switch	Switch Allied Talesyn 8 Port Switch 8 port	Perangkat penghubung antara server dengan access point
4.	Access Point	Cisco Cataliyst e 800	Perangkat penghubung dengan server
5.	Laptop Penyerang	Intel (R) Core i3(R) CPU 2.40GHz 4 GB DDR3 320 GB *Harddisk*	Perangkat yang digunakan untuk melakukan penyerangan

2) Kebutuhan perangkat lunak

Tabel III-2Kebutuhan perangkat lunak

No.	Nama	Versi	Deskripsi
1.	Ubuntu Server	14.04	Sistem Operasi yang digunakan untuk Server IDS.
2.	Suricata	3.0.1	Perangkat lunak yang digunakan untuk mendeteksi serangan.
3.	Kali Linux	2	Sistem Operasi yang digunakan untuk sebagai penyerang.
4.	Snorby	2	Perangkat lunak yang digunakan untuk menampilkan notifikasi melalui *web interface*
5.	Barnyard2	2.1.14	Perangkat lunak yang digunakan untuk membuat alert menjadi database dan dimasukan kedalam *database* Snorby
6.	Gammu	1.33.0	Perangkat lunak yang digunakan untuk mengirimkan notifikasi melalui *sms gateway*
7.	Linux Dash	-	Perangkat lunak yang digunakan untuk melihat performansi dan perbandingan performansi server
8.	Bind9, Virtual host	9.10	Perangkat lunak yang digunakan untuk membuat DNS dari alamat IP dan menampilkan *web interface.*
9.	Nmap	6.49BETA 4	Perangkat lunak yang digunakan untuk melakukan *port scanning* pada server target.
10.	Hping	3.0.0-alpha-2	Perangkat lunak yang digunakan untuk melakukan serangan sistem.
11.	Metasploit	4.11.4-2015071403	Perangkat lunak yang digunakan untuk melakukan eksploitasi pada server target.

IV. IMPLEMENTASI DAN PENGUJIAN

setelah melakukan analisis dan perancangan mengenai sistem yang dibuat. Pada bagian ini akan di lakukan implementasi dan pengujian.

A. Implementasi

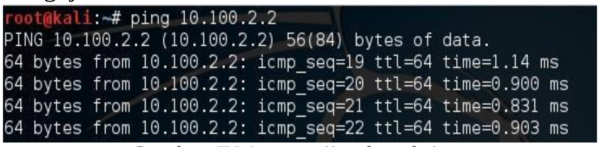
Implementasi yang akan dilakukan pada penilitian ini adalah sebagai berikut :

Gambar IV-1 Alur implementasi sistem

B. Pengujian

Pengujian yang dilakukan pada penilitian ini adalah sebagai berikut :

1) Pengujian Koneksi



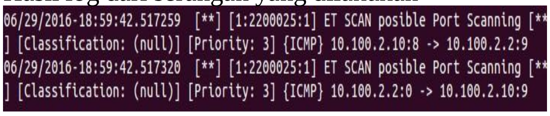
Gambar IV-2 pengujian koneksi

2) Pengujian *Port Scanning*

a. Perintah yang dilakukan untuk *Port Scanning*

```
# nmap -sV 10.100.2.2
```

b. Hasil log dari serangan yang dilakukan



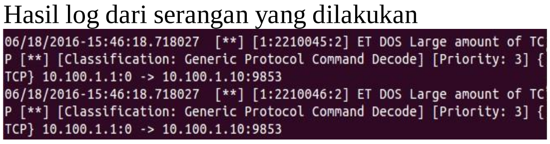
Gambar IV-3 log serangan Port Scanning

3) Pengujian *Dos Attack*

a. Perintah yang dilakukan untuk *Dos Attack*

```
# hping3 -c 10000 -d 120 -S -w
64 -p 21 --flood 10.100.2.2
```

b. Hasil log dari serangan yang dilakukan



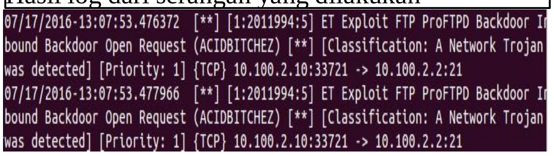
Gambar IV-4 log serangan Dos Attack

4) Pengujian *Exploit*

a. Perintah yang dilakukan untuk *Exploit*

```
# msfconsole msf > use
exploit/unix/ftp/proftpd_133c_b
ackdoor
msf > set target 0
msf > set RHOST 10.100.2.2
msf > exploit
```

a. Hasil log dari serangan yang dilakukan



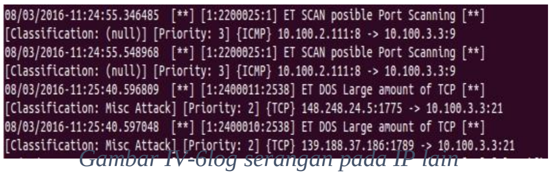
Gambar IV-5log serangan Exploit

5) Pengujian Serangan ke IP Lain

c. Perintah yang dilakukan untuk *Port Scanning dan Dos Attack* pada IP lain

```
# nmap -sV 10.100.3.3
# hping3 -c 10000 -d 120 -S -w
64 -p 21 --flood 10.100.2.2
```

a. Hasil log dari serangan yang dilakukan



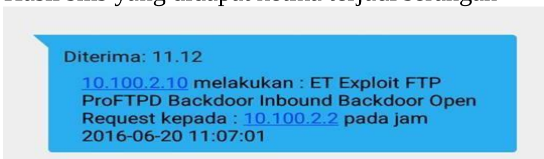
Gambar IV-6log serangan pada IP lain

6) Pengujian Sms gatewat

a. Log serangan pada web interface gammu.

Gambar IV-7 web interface gammu

b. Hasil sms yang didapat ketika terjadi serangan



Gambar IV-8 hasil sms

7) Analisis Hasil Pengujian

Berikut adalah analisis hasil pengujian :

Tabel IV-1 Analisis hasil pengujian

No	Jenis Pengujian	Tools	Hasil Pengujian
1	Koneksi	Terminal	*Attacker* dapat terhubung ke target
2	*Port Scanning*	Nmap	Suricata mengenali serangan dan mengeluarkan *alert.*
3	*Dos Attack*	Hping3	Suricata mengenali serangan dan mengeluarkan *alert.*
4	*Exploit*	Metasploit	Suricata mengenali serangan dan mengeluarkan *alert.*
5	Serangan ketarget lain	Nmap dan Hping3	Suricata mengenali serangan dan mengeluarkan *alert.*
6	Gammu	Gammu	Notifikasi dapat dikirim melalui sms

V. KESIMPULAN

Dengan adanya suricata sebagai IDS yang digunakan, setiap serangan yang ditujukan ke dalam jaringan akan dideteksi oleh suricata dengan pengecekan terhadap rules yang digunakan. Setiap serangan yang sudah masuk ke dalam database akan ditampilkan melalui web interface snorby dan di kirimkan melalui sms menggunakan gammu. Sehingga memudahkan administartor jaringan untuk melakukan pengecekan atau pengawasan terhadap jaringan.

DAFTAR PUSTAKA

[1] I. N. Rosyidin, "Jakethitam.com," [Online]. Available: http://www.jakethitam.com/2012/12/sekilas-tentang-ids-intrusion-detection.html. [Accessed 28 Januari 2016].

[2] M. K. S. M. Alim Nuryanto, "ANALISIS DAN IMPLEMENTASI SURICATA, SNORBY, DAN BARNYARD2," 2015.

[3] R. A. Wibowo, "Analisis DAN IMPLEMENTASI IDS MENGGUNAKAN SNORT," p. 8, 2014.

[4] S. A. Marogi, "Pencegahan Serangan Ddos Menggunakan Suricata Dan Snorby Sebagai Web Interface," P. 8, 2014.

[5] T. Prasetio, "Perancangan Sistem Sms Gateway Sebagai Media," P. 6, 2013.

[6] I. Mahardika, "Secure Remote Login Pada Sistem Operasi Slackware Linux," 2003.

[7] "faculty-web.msoe.edu," [Online]. Available: http://www.tothenew.com/blog/wp-content/uploads/2015/03/ddos.jpg. [Accessed 2016].

[8] B. Saputra, "Perancangan Dan Implementasi Nids (Network Intrusion Detection System) Menggunakan Snort Dan Base Pada Freebsd 10," p. 14, 2015.

[9] "wonderhowto," [Online]. Available: http://img.wonderhowto.com/img/58/65/63545252017877/0/hack-like-pro-metasploit-for-aspiring-hacker-part-3-payloads.300x140.jpg. [Accessed 2016].

[10] Reynaldo, "hong.web.id," [Online]. Available: http://www.hong.web.id/news/apa-saja-istilah-seputar-keamanan-komputer. [Accessed 18 Juni 2016].