Jurnal Sains, Teknologi dan Industri, Vol. 11, No. 2, Juni 2014, pp. 314 - 320
ISSN 1693-2390 print/ISSN 2407-0939 online

QUICK REPORT FOR HOST BASED INTRUSION DETECTION SYSTEM (HIDS)

Rahmad Abdillah
Teknik Informatika
Fakultas Sains dan Teknologi
Universitas Islam Negeri Sultan Syarif Kasim Riau
rahmad.abdillah@uin-suska.ac.id

ABSTRAK

Saat ini, Notifikasi penyusup pada *Intrusion detection system* masih menggunakan teknologi pager. Penelitian ini mengusulkan *quick report* pada sistem pendeteksian penyusupan berbasis *hosts* (HIDS) sebagai alternatif notifikasi instrusi kepada administrator ketika terdeteksi oleh IDS. *Quick report* ini dibangun menggunakan konsep SMS Gateway. HIDS dihubungkan dengan teknologi SMS gateway sebagai media penyampaian notifikasi intrusi, sehingga administrator lebih cepat mendapatkan informasi penyusup di dalam server.

Kata Kunci: (*Host Based* , Sistem Pendeteksi Penyusup, *Quick Report*)

ABSTRACT

Today, Notifications intruder in Intrusion detection systems are still using pager technology. This study proposes a "quick report" on an intrusion detection system based hosts (HIDS) as an alternative intrusion notification to the administrator when it is detected by the IDS. "Quick report" is built using the concept of SMS Gateway. HIDS is associated with the SMS gateway technology as a medium to deliver intrusion notification, so that administrators to more quickly get information intruder inside the server.

***Key Words**: (Host Based, Based Intrusion Detection System, Quick Report)*

PENDAHULUAN

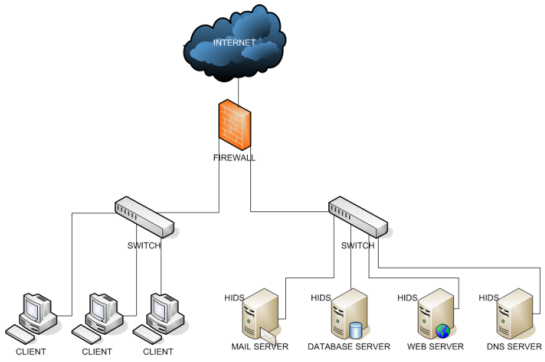
Intrusion Detection System (IDS) memantau penggunaan sistem informasi ataupun jaringan komputer untuk mendeteksi suau keadaan yang tidak aman (Jalali & Baraani, 2012). Keaadan yang tidak aman maksudnya adalah suatu tindakan penyalahgunaan terhadap hak akses ataupun melakukan ekploitasi terhadap kerentanan keamanan. Ada dua jenis IDS menurut Jalali dan Baraani (2012) yaitu Network-based Intrusion Detection System (NIDS) dan Host-based Intrusion Detection System (HIDS). Terdapat berbagai macam produk yang berkonsentrasi pada IDS, salah satunya Snort. Snort juga memberikan dukungan terhadap pengiriman notifikasi secara *realtime* (saat terjadi peristiwa tersebut) (Baker & Esler, 2007). Notifikasi tersebut hanya dapat digunakan jika menggunakan aplikasi tambahan (third party) seperti QuickPage (Babbin et al., 2005). QuickPage sebuah perangkat lunak yang bersifat gratis, dengan memiliki dukungan client server terhadap sistem operasi Unix/Linux untuk melakukan pengiriman pesan ke perangkat komunikasi pager. (http://www.qpage.org/). Komunikasi pager ini tergolong teknologi yang tidak aman dan sudah ketinggalan jaman (http://id.wikipedia.org/wiki/Radio_panggil). Percakapan pada pager ini dapat ditangkap asal menggunakan frekuensi yang telah ditetapkan atau bersifat nasional.

Penelitian ini, mengusulkan *quick repor*t pada sistem pendeteksian penyusupan berbasis host (HIDS) sebagai alternatif notifikasi kepada administrator untuk segera menindak lanjuti intrusi yang ada. Semakin cepat administrator mendapatkan notifikasi intrusi maka semakin cepat pula untuk mengambil tindakan. Notifikasi intrusi quick report ini akan dibangun menggunakan konsep SMS Gateway.

Sehingga notifikasi intrusi lebih cepat sampai kepada administrator.

BAHAN DAN METODE

Host-Based Intrusion Detection System (HIDS) memiliki konsep yakni memonitoring segala bentuk karakteristik dan event yang terjadi suatu host yang berkaitan dengan kegiatan yang dianggap mencurigakan (Scarfone & Mell, 2007). HIDS memonitoring perubahan konfigurasi *network traffic* (hanya pada host), log pada sistem, proses yang sedang berjalan, aktivitas pada aplikasi, akses dan modifikasi terhadap file serta sistem dan aplikasi (Abdillah, 2012).



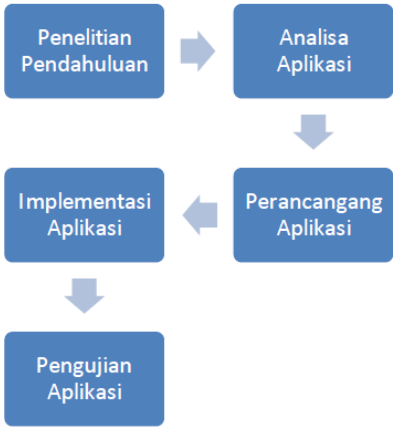
Gambar 1. Implementasi HIDS

Short Messages Service (SMS) sangat tergantung dari jumlah data yang disimpan. Oleh sebab itu, 1 karakter sms berisikan 160 karakter atau 1120 bites (Ridwan, 2010).

Secara garis besar, mekanisme kerja pengiriman SMS dapat dibagi menjadi tiga macam, yaitu:

A. Pengiriman SMS dalam satu operator atau sering disebut dengan intra-operator. SMS yang dikirimkan dari nomor pengirim akan diterima oleh SMS Center. kemudian SMS Center meneruskan SMS tersebut kenomor tujuan secara langsung.
B. Pengiriman SMS antar operator atau lebih dikenal dengan inter-operator
   Selain masuk ke SMS Center operator sang pengirim, SMS dikirim diteruskan ke SMS Center operator penerima, kemudian baru diteruskan ke nomor tujuan.
C. Pengiriman SMS dari operator suatu Negara kenegara lain atau lebih dikenal SMS internasional.
   Cara kerja hampir sama dengan pengiriman SMS inter-operator. Hanya pada SMS Center pengirim berada pada negara berbeda dengan SMS Center penerima serta penambahan kode Negara nomor tujuan.

Metode penelitian digunakan agar penelitian yang akan dikerjakan lebih terarah, berikut metode peneltian yang digunakan.



Gambar 2. Metode Penelitian

Berdasarkan Gambar 2, terdapat beberapa tahapan yaitu penelitian pendahuluan, analisa aplikasi, implemtasi aplikasi, perancangan aplikasi dan pengujian aplikasi. Berikut penjelasan masing-masing tahapan:

1. Penelitian pendahuluan

Tahapan ini berisikan tentang bagaimana ide penelitian ini muncul, mulai dari melakukan tanya jawab dengan para narasumber, buku, jurnal dan media informasi lainnya yang sejenis.

2. Analisa aplikasi

Aplikasi ini harus terintegrasi dengan server yang telah memiliki HIDS, misalkan untuk mencegah serangan *bruteforce authentication* pada protokol *login Secure Shell* (SSH). Jika HIDS dari server tersebut mendeteksi serangan *bruteforce authentication* maka secara otomatis aplikasi akan memberikan notifikasi kepada *administrator* bahwa ada

hacker yang mencoba masuk ke dalam *server* menggunakan konsep SMS *Gateway*.

3. Perancangan aplikasi

Tahapan ini berisikan tentang bagaimana merancang aplikasi hasil analisa, seperti perancangan kebutuhan data.

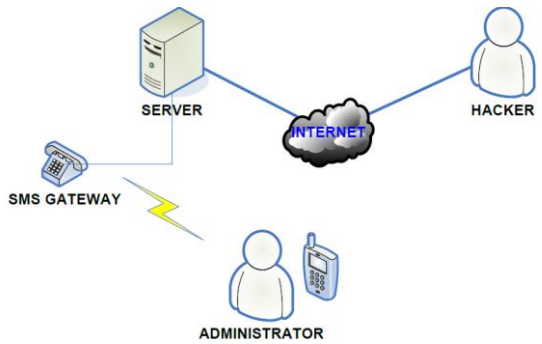
4. Implementasi Aplikasi

Implementasi aplikasi menggunakan sebuah komputer yang memberikan layanan server tertentu dengan dilengkapi konsep SMS Gateway dengan spesifikasi sebagai berikut.

a. Operating system : Linux Ubuntu
b. Memory : 1 GB
c. HDD : 120 GB
d. Bahasa Pemograman : Gambas
e. Editor : vi

5. Pengujian aplikasi

Berdasarkan Gambar 3, ketika hacker akan melakukan suatu tindakan penyerangan, misalkan tindakan bruteforce authentication terhadap protokol *Secure Shell* (SSH) kepada server maka secara otomatis server merekam tindakannya. Seketika itu juga server yang telah memiliki HIDS khusus mendeteksi tindakan tersebut, maka HIDS akan langsung memberikan notifikasi bahwa hacker telah mencoba masuk kedalam sistem kepada administrator menggunakan konsep *SMS Gateway*.

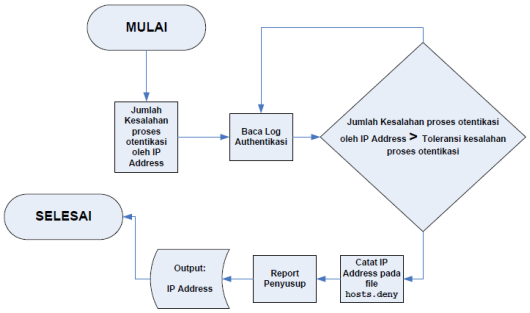


Gambar 3. Implementasi HIDS

HASIL DAN PEMBAHASAN

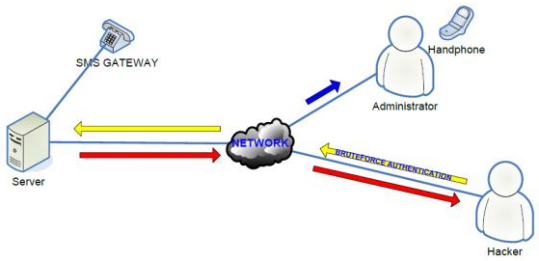
Alur kerja aplikasi dapat digambarkan pada Gambar 4, berikut penjelasan dari flowchart sistem:

Admin akan menentukan parameter penyusup pada aplikasi, seperti jumlah kesalahan yang dapat ditolerir dan protokol yang akan digunakan. Aplikasi ini membutuhkan dukungan terhadap proses penjadwalan eksekusi. Aplikasi pendukung tersebut adalah Crontab. Aplikasi ini memastikan setiap aplikasi yang telah dijadwalkan akan berjalan sebagaimana mestinya. Misalkan aplikasi pendeteksian penyusup ini berjalan pada x waktu, maka setiap x waktu akan terjadi pengecekkan log otentikasi pada server. Jika ditemukan pada log otentikasi jumlah IP address yang melakukan proses otentikasi pada protokol SSH lebih dari jumlah kesalahan yang dapat ditolerir maka IP address akan dicatat pada file hosts.deny dan memberikan informasi kepada admin melalui teknologi sms gateway.



Gambar 4. Flowchart Sistem

Hasil dari penelitian ini dapat dilihat pada gambar 5.



Gambar 5 . Pengujian Penyusupan Server

Rincian penjelasan Gambar 5, dapat dilihat pada uraian dibawah ini, sebagai berikut :

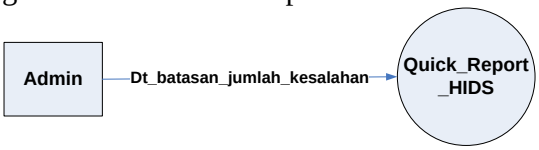
1. Hacker mencoba melakukan penyerangan brute force authentication pada server yang berada di lingkup network
2. Quick Report HIDS merupakan aplikasi utama yang memegang kendali terhadap keamanan login pada server. Quick Report HIDS memiliki beberapa tugas, yaitu:

a. Menganalisa log authentikasi pada server secara berkala.

b. Melakukan penulisan IP Address dan protokol SSH pada file konfigurasi sistem /etc/hosts.deny.
c. Mengirimkan IP Address penyusup kepada admin.
3.Runtutan peristiwa pengujian penyerangan, sebagai berikut :
a. Hacker melakukan penyerangan terhadap server pada network sebanyak x kali dengan metode brute force authentication
b. Aplikasi melakukan pengecekan terhadap file log authntication secara berkala dan melakukan analisa bila terdapat error login sebanyak x kali yang dilakukan oleh sebuah IP address, serta akan melakukan penulisan IP Address dan protokol SSH pada file konfigurasi pada server, /etc/hosts.deny. kemudian aplikasi akan mengirimkan informasi IP Address penyusup kepada admin menggunakan teknologi SMS Gateway.
c. TCPD akan melakukan pengecekkan terhadap file /etc/hosts.allow dan /etc/hots.deny, jika ditemukan pada salah satu file maka akan dilakukan access control dalam peristiwa diatas maka yang access control yang dilakukan adalah blocking access.

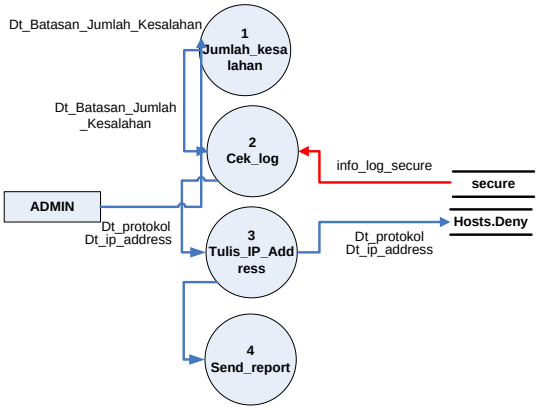
Analisa Fungsional

Analisa fungsional meliputi pembahasan kepada *Data Flow Diagram* (DFD) dan *Context Diagram*. Gambar 1 menjelaskan tentang bagaimana *context diagram* berjalan di aplikasi.. *context diagram* merupakan gambaran umum dari aplikasi.



Gambar 1. Context Diagram

Sedangkan pada Gambar 2 menjelaskan tentang DFD pada aplikasi yang akan dibangun. DFD ini merupakan penjelasan secara detil dari context diagram.



Gambar 2. Data Flow Diagram

Tabel 1 merupakan penjelasan mengenai aliran data yang akan digunakan oleh aplikasi.

Tabel 1. keterangan proses pada DFD level 1

No	Nama proses	Masukan	Keluaran	Deskripsi
1	Jumlah_kesalahan	Dt_batasan_jumlah_kesalahan	-	Proses untuk mendefinisikan jumlah kesalahan yang diizinkan
2	Cek_log	info_log_secure	-	Proses untuk membaca Log Authentikasi
3	Tulis_IP_Address	-	Dt_ip_address	Proses untuk penulisan pada file hosts.deny
4	Send_Report	-	Dt_ip_address	Proses untuk pengiriman laporan kepada admin menggunakan teknologi SMS Gateway

Tabel Tabel 2 merupakan penjelasan mengenai aliran data yang akan digunakan oleh aplikasi.

Jurnal Sains, Teknologi dan Industri, Vol. 11, No. 2, Juni 2014, pp. 314 - 320
ISSN 1693-2390 print/ISSN 2407-0939 online

Tabel 2. keterangan aliran data pada DFD level 1

No	Nama	Deskripsi
1	Dt_batasan_jumlah_kesalahan	Data yang digunakan untuk mendefinisikan jumlah kesalahan *login* yang diizinkan
2	info_log_secure	informasi yang digunakan untuk menganalisa status authentikasi
3	Dt_ip_address	Data berupa IP Address yang telah ditetapkan oleh aplikasi sebagai tindakan penyerangan
4	Dt_protokol	Data berupa protokol SSH

Perancangan Aplikasi

Perancangan aplikasi ini menggunakan konsep perancangan procedural, yaitu perancangan algoritma *pseudo code* untuk masing masing proses dalam aplikasi. Berikut perancangan aplikasi ini secara procedural.

A. Algoritma *pseudo code* proses batasan jumlah kesalahan

```
Jumlah_kesalahan()
{
Jumlah_kesalahan=”3”
}
```

B. Algoritma *pseudo code* proses cek log authentikasi

```
Cek_log()
{
jumlah_kesalahan
find "Invalid user"
while
read i
do
tulis_ip_address
done
```

C. Algoritma *pseudo code* proses tulis IP address

```
tulis_ip_address()
{
count= "Invalid
user"
ip=ip
already=false
if already = false
then
if count >
jumlah_kesalahan
then
write ip
send ip
endif
endif
}
```

Implementasi Aplikasi

Pada proses implementasi terdapat dua bagian utama dalam pengembangan aplikasi ini. Berikut deskripsi implementasi aplikasi yang telah dilaksanakan, yaitu:

a. Implementasi *Engine*, adalah inti dari tahapan pengembangan aplikasi. pada tahap ini terdapat beberapa sub bagian, sebagai berikut:
   - Cek_Log adalah implementasi pengecekan error login pada log authentikasi.
   - Tulis_IP_Address adalah implementasi data yang dihasilkan ketika proses pengecekan log authentikasi terdapat error login.

b. Implementasi *Support Application*
   - *Crontab* adalah aplikasi management waktu ekeskusi dari sebuah aplikasi. *crontab* berjalan disisi *server.*
   - *TCPD* adalah aplikasi *management access control internet service* pada komputer
   - SMS Gateway adalah aplikasi untuk melakukan *broadcast* SMS.

Pengujian Aplikasi

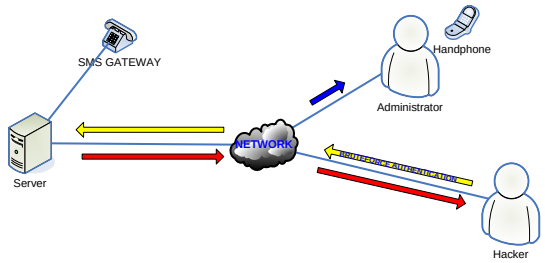
Pengujian aplikasi meliputi bagaimana aplikasi diuji seperti menentukan jenis kelas uji, kemudian tingkat pengujian, jenis pengujian dan jadwal pengujian. Identifikasi pengujian aplikasi dapat dilihat pada tabel 3.

Tabel 3 Identifikasi dan rencana pengujian aplikasi

Kelas Uji	Butir Uji	Tingkat Pengujian	Jenis Pengujian	Jadwal
Percobaan penyusupan kedalam *server*	Normal	Pengujian tindakan serangan *Brute Force Prevention*	*Black box*	31Agustus 2014

Analisa Hasil Pengujian

Berikut penggambaran pengujian penyusupan *server* yang akan dilaksanakan, pada Gambar 3

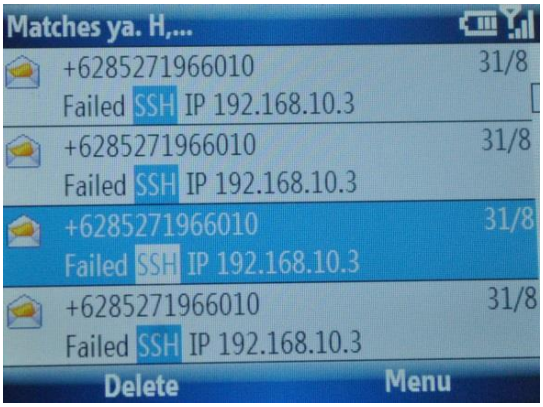


Gambar 3. Pengujian Penyusupan Server

Rincian penjelasan Gambar 3, dapat dilihat pada uraian dibawah ini, sebagai berikut :

1. *Hacker* mencoba melakukan penyerangan *brute force authentication* pada *server* yang berada di lingkup *network*
2. *Quick Report HIDS* merupakan aplikasi utama yang memegang kendali terhadap keamanan *login* pada *server*. *Quick Report HIDS* memiliki beberapa tugas, yaitu:
   a. Menganalisa log authentikasi pada *server* secara berkala.
   b. Melakukan penulisan *IP Address* dan protokol SSH pada file konfigurasi sistem /etc/hosts.deny.
   c. Mengirimkan *IP Address* penyusup kepada admin.
3. Runtutan peristiwa pengujian penyerangan, sebagai berikut :
   a. *Hacker* melakukan penyerangan terhadap *server* pada *network* sebanyak x kali dengan metode *brute force authentication*
   b. Aplikasi melakukan pengecekan terhadap *file log authntication* secara berkala dan melakukan analisa bila terdapat *error login* sebanyak x kali yang dilakukan oleh sebuah *IP address*, serta akan melakukan penulisan *IP Address* dan protokol SSH pada file konfigurasi pada *server*, /etc/hosts.deny. kemudian aplikasi akan mengirimkan informasi IP Address penyusup kepada admin menggunakan teknologi SMS Gateway.
   c. TCPD akan melakukan pengecekkan terhadap file /etc/hosts.allow dan /etc/hots.deny, jika ditemukan pada salah satu file maka akan dilakukan *access control* dalam peristiwa diatas maka yang *access control* yang dilakukan adalah *blocking access*.

Kesimpulan dari pengujian yang telah dilakukan pada penelitian ini adalah Penyusupan pada *server* ketika menggunakan *login* protokol SSH dapat dideteksi, dianalisa dan melakukan penulisan IP address pada file konfigurasi *server* yaitu `/etc/hosts.deny` dan melakukan laporan penyusup kepada admin seperti pada Gambar 6. Kemudian akan dilakukan *access control* oleh TCPD berupa *blocking access.*



Gambar 6 . Report HIDS

KESIMPULAN

Kesimpulan yang didapat pada pengembangan aplikasi yang telah dilaksanakan, yaitu Quick Report HIDS berhasil memberikan notifikasi intrusi melalui penggunaan teknologi SMS gateway.

Kombinasi HIDS dan tekologi SMS Gateway memberikan solusi terhadap notifikasi intrusi yang terbaik. Ketika terjadi penyusupan di dalam server maka seketika itu pula notifikasi intrusi dikirim ke administrator.

Berdasarkan kesimpulan yang telah dijelaskan sebelumnya, sebaiknya dapat dimplementasikan menggunakan protokol komunikasi yang berbeda misalkan FTP, EMAIL dan lain sebagainya.

DAFTAR PUSTAKA

Abdillah, R., 2012. Pencegahan Brute Force Authentication Via Protokol Ssh (Secure Shell) Menggunakan Metode Host Based Intrusion Detection System (HIDS). In Konferensi Nasional Sistem Informasi (KNSI). Bali, 2012.

Al-Saedi, K. et al., 2013. RESEARCH PROPOSAL: AN INTRUSION DETECTION SYSTEM ALERT REDUCTION AND ASSESSMENT FRAMEWORK BASED ON DATA MINING. Journal of Computer Science, 9(4), pp.421-26.

Anon., 2012. Internet World Stats - Usage and Population Statistic. [Online] Available at: HYPERLINK "http://www.internetworldstats.com/top20.htm" http://www.internetworldstats.com/top20.htm [Accessed 1 May 2014].

Anon., 2013. BBC - Homepage. [Online] Available at: HYPERLINK "http://www.bbc.co.uk/news/technology-25547738" http://www.bbc.co.uk/news/technology-25547738 .

Anon., 2014. BBC - Homepage. [Online] Available at: HYPERLINK "http://www.bbc.com/news/technology-13846031" http://www.bbc.com/news/technology-13846031 .

Babbin, J., Biles, S. & Orebaugh, A.D., 2005. Snort Cookbook. O'Reilly.

Baker, A.R. & Esler, J., 2007. Snort® IDS and IPS Toolkit. Burlington: Syngress.

Beale, J., Baker, A.R. & Caswell, B.P.M., 2004. Snort 2.1 Intrusion Detection. 2nd ed. Rockland, United States of America: Syngress Publishing.

ID-SIRTII/CC, 2014. ID-SIRTII/CC. [Online] Available at: HYPERLINK "http://idsirtii.or.id/berita/baca/41/setahun-40-juta-konsumen-jadi-korban-hacking-.html" http://idsirtii.or.id/berita/baca/41/setahun-40-juta-konsumen-jadi-korban-hacking-.html [Accessed 1 May 2014].

Jalali, H. & Baraani, A., 2012. Process Aware Host-based Intrusion Detection Model. International Journal of Communication Networks and Information Security (IJCNIS), 4(2), pp.117-24.

Ridwan, T., 2010. APLIKASI REMOTE ACCESS CONSOLE LINUX BERBASIS SMS GATEWAY MENGGUNAKAN GAMMU DAN GAMBAS (STUDY KASUS PROXY SERVER GLOBAL DEVELOPMENT LEARNING NETWORK UNIVERSITY OF RIAU). Tugas Akhir. Pekanbaru: Universitas Islam Negeri Sultan Syarif Kasim Riau.

Scarfone, K. & Mell, P., 2007. 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS). Special Publication. Gaithersburg: National Institute of Standards and Technology (NIST).