PERANCANGAN IDS DENGAN TEKNIK HIDS (*HOST BASED INTRUSION DETECTION SYSTEM*) MENGGUNAKAN SOFTWARE OSSEC

Aulia Arip Rakhman[1], Susmini Indriani Lestariningati[2]
[1,2] Jurusan Sistem Komputer Universitas Komputer Indonesia, Bandung
[1] auliaarip@gmail.com, [2] lestariningati@gmail.com

ABSTRAK

IDS (Intrusion Detection System). IDS adalah sebuah sistem yang dapat secara otomatis memonitor kejadian pada jaringan komputer dan dapat menganalisa masalah keamanan jaringan. IDS mampu mendeteksi penyusup dan memberikan respon secara real time. Terdapat dua teknik yang digunakan dalam IDS yaitu, NIDS (Network Based Intrusion Detection System) dan HIDS (Host Based Intrusion Detection System). HIDS memiliki beberapa kelebihan dibandingkan dengan NIDS, sehingga yang akan diimplementasikan kali ini adalah IDS dengan teknik HIDS dengan menggunakan perangkat lunak bernama OSSEC (Open Source Security). Pada percobaan ini PC Server menggunakan sistem operasi Linux Ubuntu 13.10. Pengujian dilakukan pada Local Area Network dengan topologi Star. Hasil dari pengujian ini didapat 128.576 peringatan yang terdiri 23.650 peringatan level 0, 62 peringatan level 1, 103.821 peringatan level 2, 286 peringatan level 3, 6 peringatan level 4, 691 peringatan level 5, 8 peringatan level 7, 1 peringatan level 8 dan 51 peringatan level 10.

Kata kunci: Keamanan Jaringan, IDS, NIDS, HIDS, OSSEC

1. PENDAHULUAN

Keamanan pada sebuah jaringan Internet merupakan hal yang sangat penting untuk menjaga jaringan tersebut dari aktifitas yang bertujuan untuk menyerang dan menyusup ke dalam jaringan tersebut. Serangan yang masuk pada sebuah jaringan bisa menyebabkan jaringan tersebut lumpuh, atau menurunnya performa jaringan tersebut jika tidak ditangani dengan cepat dan tepat.

Salah satu solusi yang dapat digunakan adalah IDS (*Intrusion Detection System*). IDS adalah sebuah sistem yang dapat secara otomatis memonitor kejadian pada jaringan komputer dan dapat menganalisa masalah keamanan jaringan. Ada dua teknik yang dipakai untuk implementasi IDS yaitu NIDS (*Network Based Intrusion Detection System*) dan HIDS (*Host Based Intrusion Detection System*). Perangkat lunak yang dipakai bernama OSSEC yang menggunakan teknik HIDS.

Dengan adanya IDS dalam sebuah jaringan, maka kemungkinan adanya serangan atau penyusup kedalam sebuah jaringan akan semakin kecil karena akan terdeteksi oleh IDS dan juga IDS akan memberi peringatan kepada administrator bila terjadi gangguan ataupun penyusup pada jaringan.

2. DASAR TEORI

2.1 Jaringan Komputer

Jaringan komputer adalah sistem yang terdiri dari komputer-komputer, serta piranti-piranti yang saling terhubung sabagai satu kesatuan. Dengan dihubungkanya piranti-piranti tersebut, komputer akan dapat saling berbagi sumber daya antara satu piranti dengan piranti lainya.

Jaringan komputer dapat diklasifikasikan menurut beberapa kategori, diantaranya:

1. Berdasarkan area cakupan
2. Berdasarkan media transmisi
3. Berdasarkan fungsi

2.2 Topologi Jaringan Komputer

Topologi adalah pola aturan untuk menghungkan komputer dan komponen jaringan satu sama lain secara fisik dan pola hubungan antar komponen yang

berkomunikasi di dalam jaringan. Ada dua jenis topologi yaitu topologi fisik dan topologi logika.

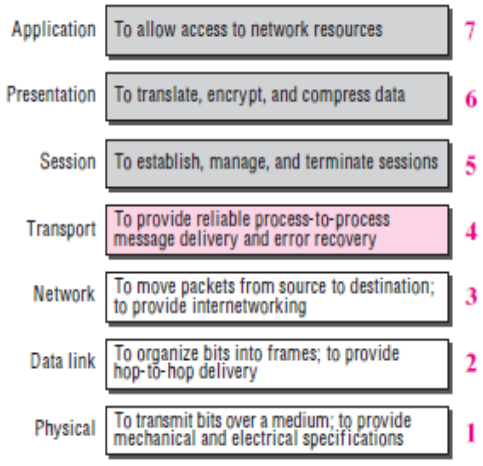
Topologi fisik terdiri dari topologi *Bus*, *Star, Ring* dan *Mesh*. Sedangkan topologi logika terdiri dari *Shared Media* dan *Token Based*.

2.3 Protokol Jaringan Komputer

Protokol adalah seperangkat aturan yang megatur komunikasi data. Protokol mendefinisikan apa itu komunikasi, bagaimana cara berkomunikasi dan apa yang terjadi ketika berkomunikasi.

2.3.1 Model OSI

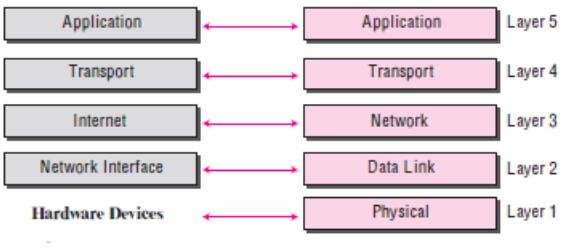
Model OSI ini diperkenalkan pada akhir 1970an. Model OSI memungkinkan dua sistem yang berbeda untuk berkomunikasi terlepas dari arsitektur yang mendasari mereka. Tujuan dari model OSI adalah untuk menunjukkan bagaimana untuk memfasilitasi komunikasi antara sistem yang berbeda tanpa memerlukan perubahan logika dari *hardware* dan *software*.



Gambar 1. Layer pada Model OSI

2.3.2 TCP/IP Protocol Suite

Protokol TCP/IP yang original didefinisikan sebagai empat lapisan perangkat lunak yang dibangun diatas perangkat keras. Tapi saat ini TCP/IP dianggap sebagai model dengan lima layer dengan lapisan yang bernama sama dengan yang ada di model OSI.



Gambar 2. Protokol TCP/IP Original dan Saat ini

Berikut ini adalah lapisan-lapisan dari protokol TCP/IP yang digunakan sebagai standar saat ini: *Physical Layer, Data Link Layer, Network Layer, Transport Layer* dan *Application layer*.

2.4 IDS

Pengertian dari IDS berdasarkan NIST adalah perangkat lunak atau perangkat keras yang mengautomatisasi proses pemantauan kejadian yang terjadi pada sebuah sistem komputer atau jaringan, menganalisa kejadian tersebut untuk menentukan tanda-tanda masalah keamanan.

IDS berfungsi untuk membantu sistem informasi untuk bersiap dan menangani sebuah serangan yang datang pada jaringan. Itu dilakukan dengan cara mengumpulkan informasi dari berbagai sistem dan jaringan sumber lalu menganalisis informasi tersebut bila ada kemungkinan masalah keamanan.

Ada dua teknik IDS yaitu *Network based* IDS (NIDS) dan *Host based* IDS (HIDS).

2.4.1 NIDS

NIDS telah menjadi banyak digunakan selama beberapa dekade terakhir karena kemampuan mengesankan untuk memberikan pandangan granular dari apa yang terjadi pada jaringan. NIDS memonitor lalu lintas jaringan menggunakan *Network Interface Card* (NIC) yang terhubung langsung ke jaringan Anda.

2.4.2 HIDS

Jenis IDS yang melibatkan perangkat lunak atau komponen agen yang dijalankan pada server, router, switch atau alat

jaringan. Namun, versi agen harus melaporkan ke konsol atau dapat dijalankan bersama-sama pada host yang sama. Pada dasarnya, HIDS jauh lebih baik dalam mendeteksi dan merespon serangan jangka panjang seperti pencurian data.

HIDS juga mampu melakukan pemeriksaan sistem tambahan yang hanya bisa dilakukan bila aplikasi IDS dipasang pada *host*, seperti *file integrity checking, registry monitoring, log analysis, rootkit detection* dan *active response*.

2.5 OSSEC

OSSEC adalah *open source* HIDS. Perangkat lunak ini melakukan *log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting* dan *active response.*

OSSEC memberikan fungsi yang sama seperti SIEM (*Security Information and Event Management*) dan STRM (*Security Threat Response Management*).

Aplikasi ini menggunakan arsitektur *client-server*. Komunikasi antara keduanya menggunakan protokol UDP dengan port 1514 dan dienkripsi menggunakan algoritma symmetric key Blowfish.

Agent yang dimonitor dapat berjalan pada bermacam-macam sistem operasi, tetapi server haruslah dipasang pada sistem operasi BSD/Linux/Unix.

2.6 Web Server Apache

Apache adalah *Web Server* yang dapat dijalankan pada banyak sistem operasi (Unix, BSD, Linux, dan Microsoft Windows) yang berguna untuk melayani dan memfungsikan situs web. Protokol yang digunakan untuk melayani fasilitas ini adalah HTTP.

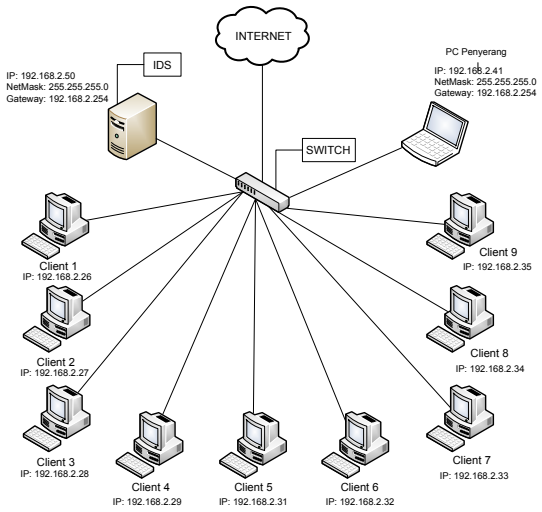
Apache memiliki fitur-fitur canggih seperti pesan kesalahan yang dapat dikonfigurasi, autentikasi berbasis basis data dan lain-lain. Apache juga didukung oleh sejumlah antarmuka pengguna berbasis grafik (GUI) yang memungkinkan penanganan *server* menjadi mudah. Apache merupakan perangkat lunak sumber terbuka dikembangkan oleh komunitas terbuka yang terdiri dari pengembang-pengembang dibawah naungan *Apache Software Foundation*.

2.7 Sistem Operasi Ubuntu

Salah satu komponen utama dalam jaringan adalah sistem operasi komputer. Sistem operasi ini berfungsi untuk mengatur komunikasi jaringan berupa dokumen, printer, scanner dan perangkat-perangkat lainnya. Sistem operasi dapat membedakan arsitektur dalam pemanfaatan fasilitas-fasilitas yang ada di jaringan.

Ubuntu berasal dari bahasa Afrika yakni "Humanity to Others" yang berarti "Kemanusiaan Untuk Sesama". Atas dasar itulah diluncurkannya Linux Ubuntu yang dirilis pada tahun 2004. Sistem operasi ini adalah merupakan turunan dari sistem operasi linux yang lain, yakni Debian. Ubuntu didukung oleh perusahaan bernama Canonical, Ltd. Perusahaan ini bermarkas di Eropa dan dipimpin oleh seseorang bernama Mark Shuttleworth.

3. PERANCANGAN SISTEM



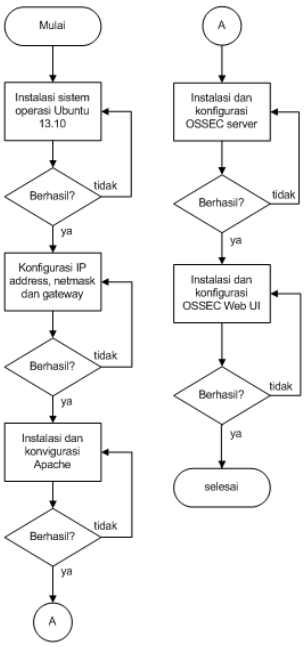
Gambar 3. Topologi Sistem Secara Umum

Dari gambar 3 di atas, dapat dijelaskan bagaimana topologi perancangan IDS:

1. Pada PC *Server* IDS dipasang satu *ethernet card* dengan alamat IP 192.168.2.50 dengan *subnet mask* 255.255.255.0.

2. PC IDS dan semua perangkat jaringan lokal (LAN) dihubungkan oleh sebuah *switch*.
3. PC penyerang terdapat pada satu jaringan dengan alamat IP 192.168.2.41 dan *subnet mask* 255.255.255.0.

Berikut ini diagram alir perancangan sistem.



Gambar 4. Diagram Alir Perancangan Sistem

Pada diagram alir diatas dijelaskan bahwa proses awal untuk merancang sistem ini diawali dengan instalasi sistem operasi, konfigurasi PC *server* dan *client*, instalasi Apache, instalasi dan konfigurasi OSSEC *Server* serta instalasi dan konfigurasi OSSEC Web UI.

3.1 Instalasi Apache

Setelah tahap instalasi sistem operasi dan konfigurasi PC *server* dan *client*, selanjutnya adalah tahap instalasi *web server* Apache.

```
#apt-get install apache2 libapache2-
mod-php5
```

3.2 Instalasi dan konfigurasi OSSEC *Server*

Tahap senjutnya adalah instalasi dan konfigurasi OSSEC *server*.

```
#apt-get install build-essential
```

mengunduh file source OSSEC dengan menggunakan perintah `wget`:

```
#wget http://www.ossec.net/files/ossec-
hids-2.7.1.tar.gz
```

Ekstraksi dan instalasi dengan perintah berikut ini.

```
#tar -xzvf ossec-hids-2.7.1.tar.gz
#cd ossec-hids-2.7.1/
#sudo ./install.sh
```

3.3 Instalasi dan konfigurasi OSSEC Web UI

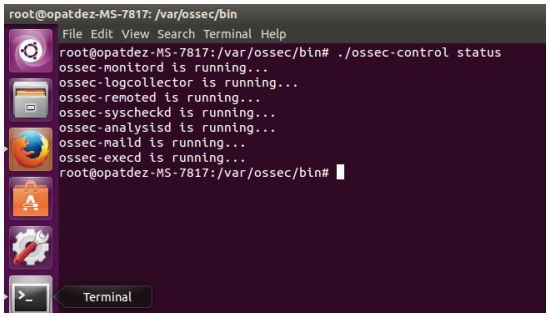
Selanjutnya dilakukan tahap instalasi OSSEC Web UI dengan mengikuti perintah-perintah berikut ini.

```
{download Web UI}
#wget http://www.ossec.net/files/ossec-
wui-0.8.tar.gz
{extract}
#tar -zxvf ossec-wui-0.8.tar.gz
{make directory and move extraction
files}
#mkdir /var/www/ossec/
#mv ossec-wui-0.8 /var/www/ossec/
{move to /var/www/ossec/ and install
Web UI}
#cd /var/www/ossec/
#./setup.sh
{add www-data to ossec group}
#usermod -a -G ossec www-data
{fix /tmp permissions}
#chmod 770 tmp/
#chgrp www-data tmp/
#apache2ctl restart
```

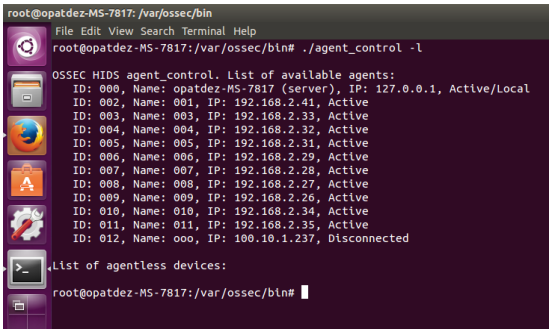
4. PENGUJIAN DAN ANALISA

4.1 Pengujian Fungsonalitas OSSEC *Server*

Pengujian ini dilakukan dengan cara mengecek fungsi-fungsi pada OSSEC server dan memeriksa koneksi antara server dengan agent.



Gambar 5. Status OSSEC *Server*



Gambar 6. Status *Agent*

Dari dua gambar diatas diketahui semua fungsi dari OSSEC *Server* berjalan dan juga ada 10 buah *agent* yang terkoneksi pada jaringan dengan status *active*.

4.1.1 Pengujian OSSEC *Server* Terhadap Serangan

Pada pengujian ini dilakukan dengan cara menyerang web server dengan beberapa teknik serangan yang bisa dilakukan para *hacker* terhadap sebuah jaringan yaitu DoS (Denial of Services) dan *SQL Injection*. server HIDS diaktifkan selama 5-6 jam per hari selama 6 hari dan penyerangan dilakukan secara acak setiap harinya.

Dari pengujian tersebut diketahui jumlah *alert* selama 6 hari dari hasil penyerangan yang dilakukan sebanyak 128.476. Hasil dari pengujian tersebut terlihat pada tabel dibawah ini.

Tabel 1. Jumlah *alert* berdasarkan level

Level Alert	Jumlah Alert
Level 0	23.650
Level 1	62
Level 2	103.821
Level 3	286
Level 4	6
Level 5	691
Level 7	8
Level 8	1
Level 10	51
TOTAL	128.576

Dari Tabel 1 diatas terlihat bahwa *alert* yang terjadi selama 6 hari uji coba sebanyak 128.576 kali dan alert paling banyak adalah *alert level 2*. Selain dikategorikan berdasarkan level, tabel berikut ini mengkategorikan jumlah alert per hari nya yang ditangkap oleh HIDS

Tabel 2. Jumlah *alert* per hari

Hari	Jumlah Alert	Presentase
Hari ke-1	40.631	31,6%
Hari ke-2	72	0,1%
Hari ke-3	51.626	40,2%
Hari ke-4	26.779	20,8%
Hari ke-5	4.559	3,5%
Hari ke-6	4.909	3,8%

Dari Tabel 2 diatas terlihat bahwa pada hari ke-3 merupakan jumlah *alert* terbanyak selama 6 hari percobaan. tabel selanjutnya adalah *alert* yang dikategorikan berdasarkan *rule* diurutkan berdasarkan jumlah alert paling sedikit hingga paling banyak.

Tabel 3. *Alert* berdasarkan *rule*

Rule ID	Jumlah Alert
551, 2501, 18111, 504	1
18145	2
5503, 550	3
552	4
18105	6
514, 5303, 591, 31102	7
512	8
502, 5502, 18103, 5402	9
18149	10
501, 18119	11
503	13
18102	17
18107	21
5501	24
18104	34
7320	35
5521, 5522	39
18100	40
515	40
31151	51
535	62
31100	69
7301	82
31530	109
509	135
18101	329
31101	678
530	862
3320	2679
31108	19278
1002	103814

Lalu berikut ini adalah hasil *alert log* pada server OSSEC setelah terjadi serangan DoS pada HIDS.

```
** Alert 1421376785.7780: mail  -
web,accesslog,web_scan,recon,
2015 Jan 16 09:53:05 opatdez-MS-7817-
>/var/log/apache2/access.log
```

```
Rule: 31151 (level 10) -> 'Multiple web
server 400 error codes from same source
ip.'
Src IP: 192.168.2.41
192.168.2.41 - - [16/Jan/2015:09:53:03
+0700] "GET /index.php HTTP/1.0" 404
460 "-" "-"
192.168.2.41 - - [16/Jan/2015:09:53:03
+0700] "GET /index.php HTTP/1.0" 404
460 "-" "-"
192.168.2.41 - - [16/Jan/2015:09:53:03
+0700] "GET /index.php HTTP/1.0" 404
460 "-" "-"
192.168.2.41 - - [16/Jan/2015:09:53:03
+0700] "GET /index.php HTTP/1.0" 404
460 "-" "-"
```

Berdasarkan pada pengujian yang dilakukan, terlihar seperti log di atas bahwa serangan tersebut terdeteksi dan muncul pada daftar peringatan dengan level peringatan level 10 dengan ruleID 31151.

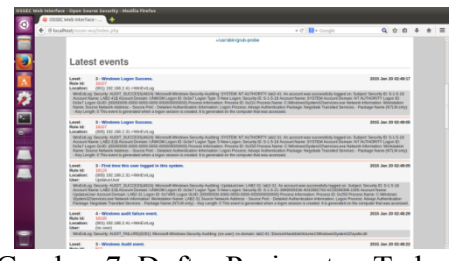
Selain menggunakan teknik DoS, dilakukan juga penyerangan menggunakan teknik *SQL Injection*. Berikut ini adalah hasil *alert log* setelah terjadi serangan *SQL Injection* pada HIDS.

```
    ** Alert 1421474225.2726: -
web,accesslog,
    2015 Jan 17 12:57:05 opatdez-MS-
7817->/var/log/apache2/access.log
    Rule: 31101 (level 5) -> 'Web
server 400 error code.'
    Src IP: 192.168.2.41
    192.168.2.41 - -
[17/Jan/2015:12:57:04 +0700] "HEAD
/login.php HTTP/1.1" 404 195 "-"
"Java/1.7.0_02"
```

Berdasarkan pada pengujian yang dilakukan terlihar seperti log diatas bahwa serangan tersebut terdeteksi dan muncul pada daftar peringatan dengan level peringatan level 5 dengan ruleID 31101.

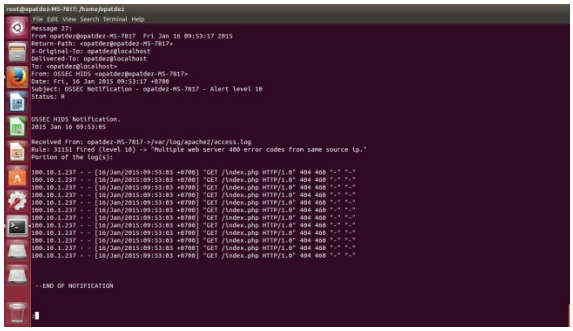
4.1.2 Pengujian Fungsi Notifikasi

Pengujian ini dilakukan dengan cara mengecek daftar peringatan pada OSSEC Web UI dan email yang dikirim oleh OSSEC Server.



Gambar 7. Daftar Peringatan Terbaru

Selain dengan melihat daftar peringatan pada OSSEC Web UI, sebuah email pun akan dikirim bila level peringatan level 6 ke atas. Berikut ini adalah email yang dikirim pada administrator.

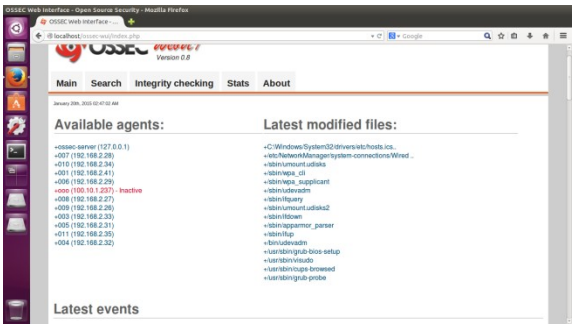


Gambar 8. Notifikasi Email

Pada email tersebut diperlihatkan bahwa level peringatan adalah level 10 dan isinya adalah adanya banyak permintaan index.php dari alamat yang sama yang melanggar aturan 31151.

4.2 Pengujian fungsionalisat OSSEC Web UI

Pada pengujian ini, diuji halaman-halaman yang ada pada OSSEC Web UI seperti pada gambar berikut ini adalah tampilan OSSEC Web UI yang telah terkonfigurasi dengan baik.



Gambar 9. Halaman utama OSSEC web UI

Terlihat dari gambar tersebut bahwa terdapat tampilan banyaknya *Agent* yang terdeteksi oleh *Server* dengan statusnya masing-masing juga terdapat kolom file terakhir yang dimodifikasi oleh user dan peringatan terbaru pada jaringan.

4.3 Analisa

Dari hasil pengujian fungsionalitas *server* HIDS yang telah dilakukan, *server* tersebut telah bekerja optimal sesuai dengan rancangan. Hal ini dibuktikan dengan

berjalannya semua fungsi pada OSSEC baik *server* ataupun *agent* serta adanya laporan dan peringatan yang dikirimkan oleh *server* ke administrator jaringan.

Pada pengujian *server* HIDS terhadap serangan DoS dan *SQL Injection*, server OSSEC juga bekerja dengan baik. Dari pengujian ini didapat 128.576 peringatan yang terdiri 23.650 peringatan level 0, 62 peringatan level 1, 103.821 peringatan level 2, 286 peringatan level 3, 6 peringatan level 4, 691 peringatan level 5, 8 peringatan level 7, 1 peringatan level 8 dan 51 peringatan level 10.

Diketahui pula bahwa DoS termasuk serangan level 10, rule ID 31151 dengan 51 kali peringatan serta *SQL Injection* termasuk serangan level 5, rule ID 31101 dengan 678 kali peringatan.

Pada pengujian lainya yaitu pengujian fungsionalitas OSSEC Web UI, Web yang ditampilkan pun berjalan secara semestinya dan semua halaman yang ada didalamnya berjalan secara baik dan benar.

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan uraian dan pembahasan juga pengujian yang telah dilakukan maka dapat diambil kesimpulan terhadap perancangan IDS dengan teknik HIDS (Host-based Intrusion Detection System) menggunakan software OSSEC adalah sebagai berikut:

1 Pada pengujian fungsionalitas *server* HIDS, fungsi-fungsi yang ada berjalan sesuai dengan rancagan yang telah dibangun.
2 Pada pengujian *server* HIDS terhadap serangan, *server* mampu mendeteksi serangan yang muncul dan menampilkan peringatan pada administrator.
3 Berdasarkan percobaan yang telah dilakukan, terdapat total 128.576 peringatan yang 51 diantaranya adalah peringatan tentang serangan DoS dan 678 diantaranya adalah peringatan serangan *SQL Injection*.
4 IDS dengan teknik HIDS yang diimplementasikan pada Linux Ubuntu dapat memantau kejadian pada jaringan dan OSSEC Web UI yang digunakan sangat membantu proses pemantauan jaringan dikarenakan berbasis GUI.

5.2 Saran

Saran-saran yang diajukan agar menjadi masukan untuk pengembangan berikutnya adalah sebagai berikut:

1. Untuk mempermudah pemasangan dan pengaturan IDS ini, diharapkan sistem yang sudah dikonfigurasi dapat dibuat dalam sebuah *LiveCD*.
2. Untuk perkembangan selanjutnya perlu dicoba juga untuk menggabungkan kedua teknik IDS yaitu NIDS dan HIDS dalam sebuah sistem sehingga menutupi kekurangan dari masing-masing teknik.

DAFTAR PUSTAKA

[1.] **Forouzan, Behrouz A.** *TCP/IP Protocol Suite Fourth Edition.* New York : McGraw-Hill, 2010.

[2.] **Andi.** *Panduan Lengkap Pengembangan Jaringan Linux*. Semarang : Wahana Komputer, 2008.

[3.] **Sofana, I.** *Membangun Jaringan Komputer.* Bandung : Informatika, 2008.

[4.] **Sopandi, D.** *Instalasi Dan Konfigurasi Jaringan Komputer.* Bandung : Informatika, 2008.

[5.] **Ariyus, D.** *Intrusion Detection System*. Yogyakarta : Andi Yogyakarta, 2007.

[6.] **Forouzan, Behrouz A and Chung Fegan, Sophia.** *Data Comunication and Networking.* 4th. New York : McGraw-Hill, 2007.

[7.] **Hay, Andrew, Cid, Daniel and Bray, Rory.** *OSSEC HIDS Host-Based Intrusion Detection Guide.* Burlington : Syngress Publishing, Inc., 2008.