View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by UMS Digital Library - Selamat datang di UMS Digital Library

ANALISIS PENGGUNAAN PORTSENTRY SEBAGAI TOOLS INTRUSION DETECTION SYSTEM PADA JARINGAN KOMPUTER

MAKALAH

Diajukan oleh :

Nama : **Misbahul Munir**

Pembimbing Utama : **Endah Sudarmilah,S.T.,M.Eng.**

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS KOMUNIKASI DAN INFORMATIKA

UNIVERSITAS MUHAMMADIYAH SURAKARTA

2015

HALAMAN PENGESAHAN

Publikasi ilmiah dengan judul :

ANALISIS PENGGUNAAN PORTSENTRY SEBAGAI TOOLS INTRUSION DETECTION SYSTEM PADA JARINGAN KOMPUTER

dipersiapkan dan disusun oleh

Misbahul Munir

NIM : L 200 080 175

ini telah disetujui pada :

Hari : Sabtu

Tanggal : 28 Maret 2015

Pembimbing Utama

Endah Sudarmilah, S.T.,M.Eng.
NIP/NIK: 969

Publikasi ilimiah ini telah diterima sebagai salah satu persyaratan

Untuk memperoleh gelar sarjana

Tanggal 4-04-2015

Mengetahui,

Ketua Program Studi
Teknik Informatika

Dr. Heru Supriyono,M.Sc.
NIK : 970

UNIVERSITAS MUHAMMADIYAH SURAKARTA
FAKULTAS KOMUNIKASI DAN INFORMATIKA
PROGRAM STUDI INFORMATIKA
Jl. A Yani Tromol Pos 1 Pabelan Kartasura Telp. (0271)717417, 719483 Fax (0271) 714448
Surakarta 57102 Indonesia. Web: http://informatika.ums.ac.id. Email: informatika@fki.ums.ac.id

SURAT KETERANGAN LULUS PLAGIASI

/A.3-II.3/INF-FKI/IV/2015

Assalamu'alaikum Wr. Wb

Biro Skripsi Program Studi Informatika menerangkan bahwa :

Nama	:	MISBAHUL MUNIR
NIM	:	L200080175
Judul	:	ANALISIS PENGGUNAAN PORTSENTRY SEBAGAI TOOLS INTRUSION DETECTION SYSTEM PADA JARINGAN KOMPUTER
Program Studi	:	Informatika
Status	:	**Lulus**

Adalah benar-benar sudah lulus pengecekan plagiasi dari Naskah Publikasi Skripsi, dengan menggunakan aplikasi Turnitin.

Demikian surat keterangan ini dibuat agar dipergunakan sebagaimana mestinya.

Wassalamu'alaikum Wr. Wb

Surakarta, 1 April 2015

Biro Skripsi
Informatika

Adjie Sapoetra, S.Kom

ANALISIS PENGGUNAAN PORTSENTRY SEBAGAI TOOLS INTRUSION DETECTION SYSTEM PADA JARINGAN KOMPUTER by Misbahul Munir

From publikasi (publikasi)

Processed on 01-Apr-2015 10:05 WIB
ID: 523294871
Word Count: 1840

Similarity Index	Similarity by Source	
23%	Internet Sources:	15%
	Publications:	0%
	Student Papers:	14%

sources:

1 4% match (Internet from 09-Mar-2015)
http://kualiskmpsinformatika.blogspot.com/2013_08_01_archive.html

2 3% match (Internet from 18-Apr-2014)
http://goeheadit.blogspot.com/

3 3% match (student papers from 19-Jul-2013)
Submitted to Universitas Muhammadiyah Surakarta on 2013-07-19

4 2% match (student papers from 12-Jun-2014)
Class: publikasi maret 2014
Assignment:
Paper ID: 434376622

5 1% match (student papers from 07-Jul-2014)
Class: publikasi maret 2014
Assignment:
Paper ID: 438186043

6 1% match (Internet from 19-Nov-2013)
http://ilmuti.org/2012/12/pengamanan-jaringan-komputer/

7 1% match (student papers from 18-Jul-2013)
Submitted to Universitas Muhammadiyah Surakarta on 2013-07-18

8 1% match (student papers from 02-Aug-2012)
Submitted to Universitas Muhammadiyah Surakarta on 2012-08-02

9 1% match (Internet from 03-Nov-2014)
http://ferrysudirafei.blogspot.com/

10 1% match (Internet from 18-Mar-2010)
http://digilib.sunan-ampel.ac.id/gdl.php?

ANALISIS PENGGUNAAN PORTSENTRY SEBAGAI TOOLS INTRUSION DETECTION SYSTEM PADA JARINGAN KOMPUTER

Teknik Informatika, Fakultas Komunikasi dan Informatika

Universitas Muhammadiyah Surakarta

E-Mail : sinyo3207@gmail.com

ABSTRAK

Intrusion Detection Sistem (IDS) adalah sebuah perangkat lunak atau perangkat keras yang digunakan untuk mendeteksi akses tidak sah dari sistem komputer atau jaringan. Sebuah IDS melakukan tugas ini secara eksklusif untuk jaringan. Sistem ini memonitor lalu lintas dan mencari ancaman dalam jaringan. Portsentry merupakan salah satu perangkat lunak *open source* berbasis *Intrusion Detection Sistem (IDS).* Tujuan dari penelitian ini adalah menguji kehandalan *portsentry* sebagai *tools* IDS dan menguji seberapa besar pengaruh penggunaan *portsentry* terhadap kecepatan *transfer data rate* dalam jaringan komputer.

Penelitian ini menggunakan metode eksperimen dengan membangun sebuah sistem jaringan komputer kemudian mengujinya. Pengujian dilakukan dalam dua tipe jaringan, yaitu jaringan virtual untuk menguji kehandalan *portsentry* terhadap aktifitas *scanning* dan *sniffing,* dan jaringan fisik untuk menguji kecepatan *transfer data rate* pada jaringan komputer.

Portsentry dapat mendeteksi adanya proses *scanning* yang dilakukan oleh aplikasi *angry IP scanner*, *superscan 4*, dan *NMap* terhadap *server* yang dilindunginya. Akan tetapi *portsentry* tidak dapat mendeteksi adanya proses *sniffing* yang dilakukan oleh aplikasi *wireshark* terhadap jaringan. Penggunaan *portsentry* pada *server* juga berpengaruh terhadap kecepatan *transfer data rate* pada jaringan komputer. Setiap mode pada *portsentry* menunjukkan tingkatan proses *scanning port* oleh *portsentry* dalam menjaga keamanan *server*. Hal tersebut ditunjukkan dengan perbedaan kecepatan *transfer data rate* pada setiap mode *portsentry*.

Kata Kunci *: Portsentry, scanning, sniffing, transfer data rate.*

PENDAHULUAN

Jaringan komputer saat ini mengalami perkembangan yang sangat pesat, kemajuan teknik jaringan komputer juga tidak hanya membawa dampak positif saja, melaikan juga dampak negatif. Kejahatan-kejahatan baru kian muncul, yang tadinya menggunakan teknik yang biasa, sekarang menggunakan teknik yang lebih modern.

Tidak hanya teknik penyerangan terhadap jaringan komputer yang berkembang, sistem keamanan komputer juga mengalami perkembangan yang pesat seiring dengan kebutuhan sistem keamanan yang kuat untuk menjamin sumber daya sistem tidak digunakan/dimodifikasi, diinterupsi dan diganggu oleh orang yang tidak diotorisasi.

Intrusion Detection Sistem (IDS) adalah sebuah perangkat lunak atau perangkat keras yang digunakan untuk mendeteksi akses tidak sah dari sistem komputer atau jaringan. Sebuah IDS melakukan tugas ini secara eksklusif untuk jaringan. Sistem ini memonitor lalu lintas dan mencari ancaman dalam jaringan. *Portsentry* merupakan salah satu perangkat lunak *open source* berbasis *Intrusion Detection Sistem (IDS).*

Seperti juga ada begitu banyak cara untuk melakukan deteksi intrusi maka dapat ditemukan juga berbagai macam produk IDS yang ditawarkan oleh vendor yang berbeda-beda. Suatu sistem keamanan jaringan baik perangkat keras maupun lunak akan berpengaruh terhadap kecepatan transfer data dalam suatu jaringan. Setiap produk IDS memiliki keunggulan dan kelemahan masing-masing. Oleh karena itu akan sangat menguntungkan bila dapat mengetahui kemampuan dan kelemahan dari suatu IDS.

TINJAUAN PUSTAKA

Penelitian dikembangkan dari beberapa referensi yang telah didapat yang berhubungan dengan objek permasalahan. Telaah penelitian tersebut diantaranya :

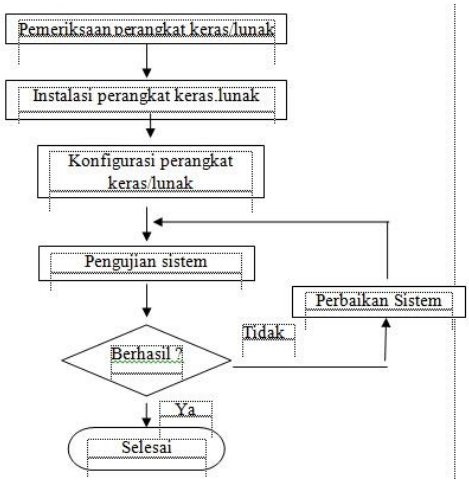
Menurut Firdaus, Atiq Zahrial (2012). Dalam penelitiannya yang berjudul Implementasi Snort Sebagai *Tool Intrusion Detection System* pada *Server* FreeBSD di PT. Power Telecom. Sistem keamanan jaringan pada perusahaan *Internet Service Provider* (ISP) merupakan faktor penting untuk menjamin stabilitas, integritas dan validitas data. Implementasi *Intrusion Detection System* berbasis *Snort* dapat menghemat biaya pengadaan *software* karena bersifat gratis dan cukup handal dalam mendeteksi serangan keamanan. Sistem IDS berbasis Snort dapat di-implementasikan pada sistem operasi FreeBSD yang banyak dipakai sebagai sistem operasi server di PT. Power Telecom cabang Solo.

Menurut Hamdan, Avicenna (2008) dalam penelitiannya yang berjudul *Self Defending Linux Network.* Dengan metode Intrusion Detection, kita dapat mengumpulkan dan menggunakan informasi dari tipe penyerangan yang telah diketahui dan menemukan jika sseseorang mencoba menyerang jaringan atau host tertentu. *Software Intrusion Detection* yang digunakan adalah menggunakan *Snort*. *Snort* adalah *Network Intrusion Detection System* (NIDS) open source yang gratis. Snort akan diintregasikan dengan dengan beberapa software dan bahasa pemrograman. Bahasa pemrograman yang digunakan adalah bahasa PHP dan database MySql. *Software* lain yang digunakan adalah *Apache Web Server* dan BASE.

Menurut Setyaningtyas, Meidhita (2013) dalam penelitiannya yang berjudul Implementasi *Portsentry* Sebagai Keamanan *Server Ubuntu* Dari Aktifitas Serangan Di Smk Negeri 2 Pekalongan. *Portsentry* dapat diimplementasikan kedalam sistem operasi Ubuntu yang saat ini sudah banyak digunakan terutama di SMK Negeri 2 Pekalongan. Sebuah scanning port dapat terdeteksi dan dilihat jejaknya pada *Syslog*. Berdasarkan hasil pengujian sistem *Portsentry* dapat memberikan peringatan adanya serangan keamanan terhadap sistem melalui paket-paket yang melewati jaringan.

METODE PENELITIAN

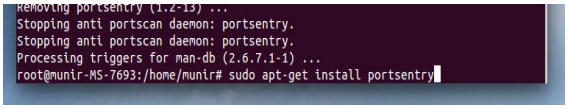
Penelitian ini menggunakan metode eksperimen. Pada metode ini penulis melakukan beberapa tahap yaitu observasi, desain dan perancangan sistem pada jaringan komputer, implementasi pada sistem yang dibuat serta melakukan pengujian terhadap sistem yang telah terpasang.



Gambar 1 *Flowchart* Alur Perancangan Sistem yang Akan Diteliti

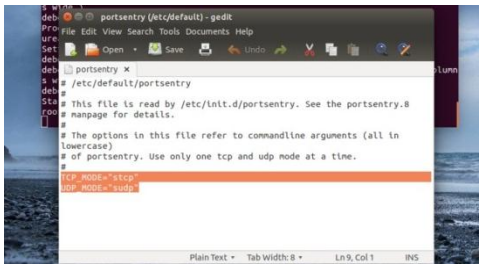
Pemasangan dan Konfigurasi *Portsentry* pada Komputer *Server.*

Pemasangan *portsentry* dapat dilakukan dengan mengetikkan perintah sudo apt-get install portsentry



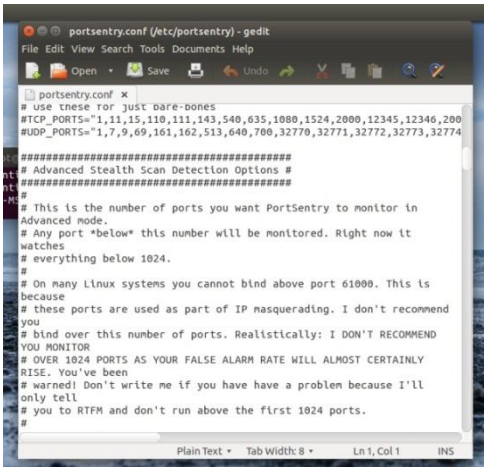
Gambar 2 Instalasi *Portsentry*

Konfigurasi *portsentry* untuk *setting default* pada *portsentry* dapat mengetikkan perintah gedit /etc/default/portsentry. cara mengganti konfigurasi *default* adalah dengan mengganti tulisan pada baris terakhir file konfigurasi.



Gambar 3 Konfigurasi *Default Portsentry*

Konfigurasi untuk sistem *portsentry* serta penerapan aturan-aturan tambahan pada portsentry dapat dilakukan dengan mengedit file konfiguras pada direktori /etc/portsentry/portsentry.conf .



Gambar 4 *File* Konfigurasi *Portsentry*

Alat dan perangkat lunak yang mendukung penelitian ini adalah sebagai berikut : komputer sebagai sever, laptop sebagai client, OS ubuntu dan windows 8, *software virtual box, angry IP scanner, superscan 4 NMap* dan *wireshark*.

Dalam penelitian ini, penulis akan membangun 2 jenis sistem jaringan yaitu jaringan *virtual* dan jaringan fisik. Jaringan *virtual* digunakan untuk menganalisa kemampuan *portsentry* dalam mendeteksi serangan *scanner* dan *sniffer*. Jaringan fisik digunakan untuk menganalisa pengaruh penggunaan *portsentry* terhadap *transfer data rate* pada jaringan komputer.

HASIL PENELITIAN

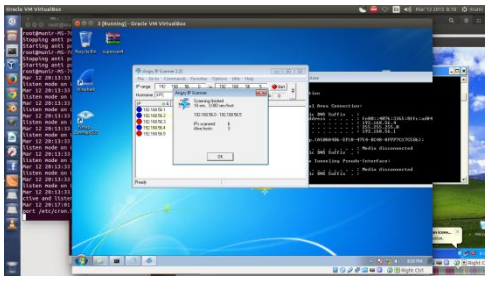
Penelitian ini termasuk dalam penelitian eksperimen yang dilakukan untuk menguji kehandalan *portsentry* sebagai *tools Intrusion Detection System* pada jaringan komputer. Serta mempelajari pengaruh *portsentry* terhadap kecepatan *transfer data rate* pada jaringan.

Sebelum melakukan penelitian, peneliti harus merancang sistem jaringan terlebih dahulu kemudian memasang dan mengkonfigurasi *portsentry* agar berjalan dengan baik. Perancangan sistem yang pertama adalah perancangan sistem jaringan dengan sistem keamanan *portsentry* pada komputer *server* yang dibuat dengan tujuan agar bisa diuji dengan aplikasi *scanner* dan *sniffer*. Perancangan jaringan dibuat menggunakan sistem *virtual machine* dan dikonfigurasi agar serupa dengan jaringan LAN (*Local Area Network*).

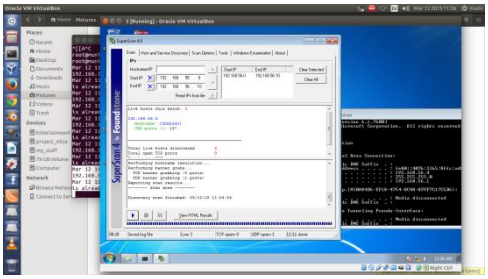
Gambar 5 Tampilan 3 Komputer Virtual yang Sedang Berjalan

1. Pengujian *Portsentry* Terhadap Aktifitas *Scanning* dan *Sniffing*

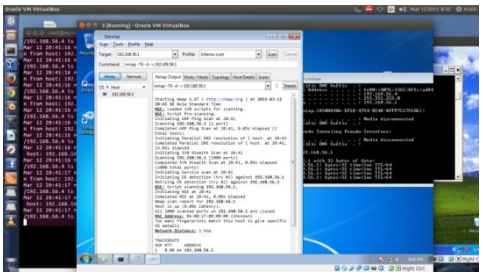
Pengujian dilakukan dengan menggunakan 3 *software scanning* yang berbeda yaitu *angry IP scanner*, *superscan 4*, *NMap*, dan sebuah software *sniffing wireshark* terhadap komputer *server* dengan konfigurasi *portsentry* yang berbeda yaitu tcp/udp, atcp/audp, dan stcp/sudp.



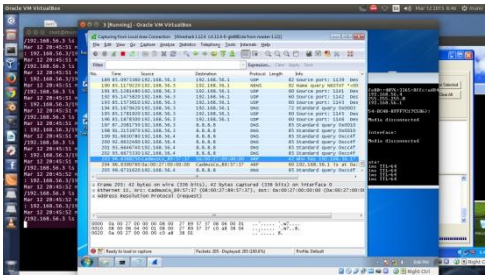
Gambar 6 Proses *Scanning* Menggunakan angry *IP scanner*



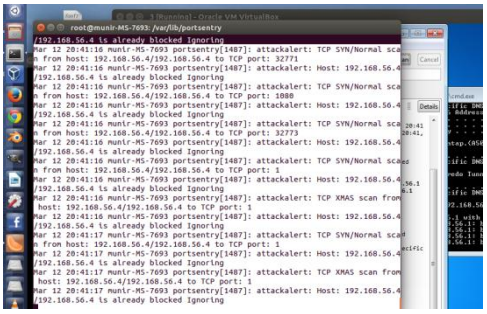
Gambar 7 Proses *Scanning* Menggunakan *superscan* 4



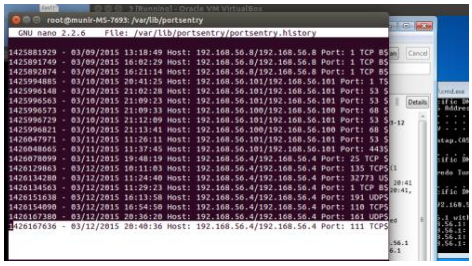
Gambar 8 Proses *Scanning* Menggunakan *NMap*



Gambar 9 Proses *sniffing* Menggunakan *Wireshark*



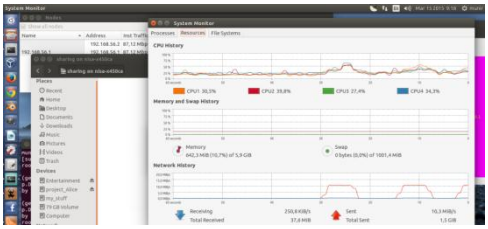
Gambar 10 Pendeteksian *Portsentry* Melalui *Syslog*



Gambar 11 Tampilan *History Portsentry*

2. Pengujian Pengaruh Portsentry Terhadap Kecepatan *Transfer Data Rate* Dalam Jaringan

Perancangan sistem yang kedua adalah perancangan sistem jaringan dengan sistem keamanan *portsentry* pada komputer *server* agar bisa diteliti pengaruhnya terhadap kecepatan *transfer data rate*. Perancangan jaringan dibuat dengan menggunakan 2 buah komputer yang saling terhubung menggunakan kabel *cross-over*. Pengujian dilakukan dengan mengirim paket data berupa file video dengan format .flv berukuran 60211 Kb dari komputer *server* ke komputer *client*. Kemudian mengamati aktifitas jaringan menggunakan *software Etherape* dan mencatat kecepatan transfer data menggunakan *software System Monitor* di komputer *server*. Komputer *server* yang telah terpasang *portsentry* menggunakan sistem operasi *Ubuntu* sedangkan komputer client menggunakan 2 sistem operasi yang bisa dipilih yaitu *Ubuntu* dan *Windows 8*. Secara singkat pengujian dilakukan pada komputer *server Ubuntu* ke *client Ubuntu* dan komputer *server Ubuntu* ke *client Windows 8*. Pengujian dilakukan sebanyak 5 kali dengan konfigurasi mode *default portsentry* yang berbeda yaitu *portsentry* tidak aktif, mode tcp/udp, atcp/audp, dan stcp/sudp agar mendapatkan nilai rata-rata dari data yang telah tercatat.



Gambar 12 Aktifitas Lalu Lintas Data pada Jaringan Komputer Yang Sedang Dalam Proses Pengiriman Data

Dari pengujian diatas dapat diketahui kemampuan portsentry terhadap aplikasi *scanner* dan *sniffer*. *Portsentry* dapat mendeteksi adanya proses *scanning* terhadap *server* yang dilindunginya. Akan tetapi *portsentry* tidak dapat mendeteksi adanya proses *sniffing* yang

dilakukan oleh aplikasi *wireshark* terhadap jaringan.

Tabel 1 Hasil Pengujian Kehandalan *Portsentry* terhadap Aplikasi *Scanner* dan *Sniffer*

No	Scanner dan Sniffer	Mode pada Portsentry		
		tcp/udp	atcp/audp	stcp/sudp
1	Angry IP scanner	tidak bisa	bisa*	bisa*
2	Superscan 4	bisa	bisa	bisa
3	NMap	bisa	bisa	bisa
4	Wireshark	tidak bisa	tidak bisa	tidak bisa

* *syslog* bisa mendeteksi adanya kejanggalan dalam jaringan akan tetapi *portsentry* tidak mampu mendeteksi dan merekem ip penyerang

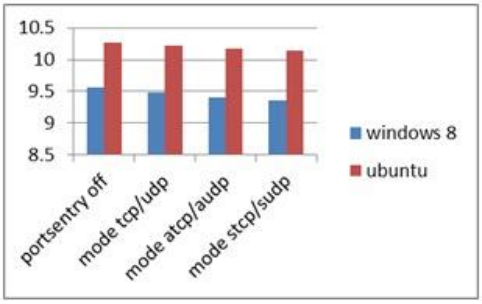
Penggunaan *portsentry* pada *server* juga berpengaruh terhadap kecepatan *transfer data rate* pada jaringan komputer. Setiap mode pada *portsentry* menunjukkan tingkatan proses *scanning port* oleh *portsentry* dalam menjaga keamanan *server*. Hal tersebut ditunjukkan dengan perbedaan kecepatan *transfer data rate* pada setiap mode *portsentry*.

Tabel 2 Hasil Pengujian Pengaruh Penggunaan *Portsentry* terhadap *Transfer Data Rate* pada Jaringan Komputer

No	Mode pada Portsentry	*Transfer Data Rate* (Mb/s) Dengan *File* Sebesar 60Mb**	
		Windows 8	Ubuntu
1	portsentry off	9.56	10.26
2	tcp/udp	9.48	10.22
3	atcp/audp	9.4	10.18
4	stcp/supd	9.36	10.14

** Merupakan file video dengan ekstensi .flv dengan ukuran 60.211Kb dengan koneksi *peer-to-peer* antara *server* dan *client*

Dari hasil penelitan dapat disimpulkan bahwa penggunaan *portsentry* sebagai *tools* IDS pada *server* akan lebih baik apabila menggunakan sistem operasi *Ubuntu* sebagai *client*.



Gambar 10 Grafik Perbandingan *Transfer Data Rate* pada *Client Windows 8* Dan *Ubuntu* Dengan Mode *Portsentry* yang Berbeda

Prosentase selisih kecepatan *transfer data rate* antara *client ubuntu* dengan *client Windwos 8* dengan koneksi *peer-to-peer* antara *server* dan client adalah sebagai berikut :

a. *Server portsentry* tidak aktif : $\frac{(10.26-9.56)}{9.56}\ 100 = 7.5\%$ lebih cepat *Ubuntu*
b. *Server portsentry* mode tcp/udp $\frac{(10.22-9.48)}{9.48}\ 100 = 7.8\%$ lebih cepat *Ubuntu*
c. *Server portsentry* mode atcp/audp

$\frac{(10.18-9.4)}{9.4}$ 100 = 8.3% lebih cepat *Ubuntu*

d. *Server portsentry* mode stcp/sudp
$\frac{(10.14-9.36)}{9.36}$ 100 = 8.3% lebih cepat *Ubuntu*

KESIMPULAN

1. *Portsentry* dapat mendeteksi aktifitas dari *scanner super scan 4* dan *NMap* pada jaringan komputer pada semua mode *portsentry* dengan sebagaimana mestinya.
2. *Syslog* dapat mendeteksi aktifitas dari *scanner angry IP scanner* hanya pada mode atcp/audp dan stcp/sudp dengan pendeteksian yang terbatas. *Portsentry* hanya dapat menunjukkan kejanggalan pada sistem komputer melalui *syslog* akan tetapi tidak dapat mengenali dan mengidentifikasi aktifitas *scanner*.
3. *Portsentry* tidak dapat mendeteksi aktifitas dari *sniffer wireshark* pada jaringan komputer.
4. Penggunaan *portsentry* berpengaruh terhadap *kecepatan transfer data rate* pada jaringan.
5. Prosentase selisih kecepatan *transfer data rate* antara *client ubuntu* dengan *client Windwos 8* dengan koneksi *peer-to-peer* antara *server* dan *client* adalah sebagai berikut: pada *server portsentry* tidak aktif 7.5%, pada *server portsentry* mode tcp/udp 7.8%, pada *server portsentry* mode atcp/audp 8.3%, dan pada *server portsentry* mode stcp/sudp 8.3% lebih cepat *Ubuntu*.

DAFTAR PUSTAKA

Tasmil. (2012). *"Kajian Wireless Intrusion Detection System (WIDS) Terhadap Keamanan Jaringan Nirkabel IEEE 802.11".* Jurnal Ilmiah Balai Besar Pengkajian dan Pengembangan Komunikasi dan Informatika Makassar, Makassar.

Anasanti, Mila Desi. (2007). "*Kajian Integrasi Host Based Dan Network Based Intrusion Detection System Menggunakan Web Based Entrprise Management*". Naskah Publikasi Laporan Tugas Akhir Program Studi Teknik Informatika Institut Teknologi Bandung, Bandung.

Prabowo, Yunan Arie. (2014). "*Penggunaan NMAP Dan HPING 3 Dalam Menganalisa Keamanan Jaringan Pada B2P2TO2T (Karanganyar, Tawangmangu)".* Skrikpsi Program Studi Teknik Informatika Universitas Muhammadiyah Surakarta, surakarta.

Handaya, Wilfridus B.T., B.R. Sutaja, dan A.Ashari. (2010)."*Linux System Administrator".* Bandung : penerbit Informatika.