

**ANALISIS PENGGUNAAN PORTSENTRY SEBAGAI
TOOLS INTRUSION DETECTION SYSTEM
PADA JARINGAN KOMPUTER**



SKRIPSI

Disusun sebagai salah satu syarat menyelesaikan Program Studi
Strata I pada Jurusan Teknik Informatika Fakultas Komunikasi dan Informatika
Universitas Muhammadiyah Surakarta

Oleh:

Misbahul Munir
NIM : L200080175

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS KOMUNIKASI DAN INFORMATIKA
UNIVERSITAS MUHAMMADIYAH SURAKARTA**

2015

HALAMAN PERSETUJUAN

Skripsi dengan judul
**ANALISIS PENGGUNAAN PORTSENTRY SEBAGAI
TOOLS INTRUSION DETECTION SYSTEM
PADA JARINGAN KOMPUTER**

ini telah diperiksa dan disetujui untuk diajukan dalam sidang pendadaran :

Hari : Sabtu.....

Tanggal : 28 Maret 2015.....

Pembimbing



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

HALAMAN PENGESAHAN

**ANALISIS PENGGUNAAN PORTSENTRY SEBAGAI
TOOLS INTRUSION DETECTION SYSTEM
PADA JARINGAN KOMPUTER**

dipersiapkan dan disusun oleh

Misbahul Munir

NIM : L200080175

telah dipertahankan di depan Dewan Penguji

pada tanggal 28-03-2015

Susunan Dewan Penguji

Pembimbing



Endah Sudarmilah, S.T.,M.Eng.

NIP/NIK: 969

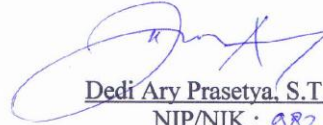
Dewan Penguji 1

Dewan Penguji 2



Muhammad Kusban, S.T, M.T.

NIP/NIK : 663



Dedi Ary Prasetya, S.T.

NIP/NIK : 982

Skripsi ini telah diterima sebagai salah satu persyaratan

untuk memperoleh gelar sarjana

Tanggal 4-04-2015



Dekan
Fakultas Komunikasi dan Informatika

Husni Thamrin, S.T, MT., Ph.D.

NIK : 706



Ketua Program Studi
Teknik Informatika

Dr. Heru Supriyono, M.Sc.

NIK : 970

DAFTAR KONTRIBUSI

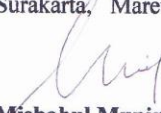
Dengan ini saya menyatakan bahwa skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Berikut saya sampaikan daftar kontribusi dalam penyusunan skripsi:

1. Saya merancang dan menganalisis sistem jaringan ini dengan bantuan internet dan buku yang dilampirkan dalam daftar pustaka.
2. Perancangan jaringan virtual menggunakan *virtualbox*.
3. Program aplikasi yang digunakan untuk menguji adalah *angry IP scanner*, *superscan 4*, *NMap*, dan *wireshark*.
4. Sistem operasi yang digunakan untuk *server* adalah *ubuntu 14.04* dan sistem operasi yang digunakan untuk *client* adalah *ubuntu 14.04* dan *windows 8*.
5. Saya menggunakan komputer dengan spesifikasi *processor* AMD Phenom x4 955, 3.2 GHz, RAM 6GB, HDD 500GB, vga Radeon HD 5850 sebagai *server* dan laptop dengan spesifikasi *processor* Intel Celeron 1007U 1.50 GHz, RAM 2GB, HDD 500GB, vga Intel HD sebagai *client*.

Demikian pernyataan dan daftar kontribusi ini saya buat dengan sejujurnya. Saya bertanggungjawab atas isi dan kebenaran daftar di atas.

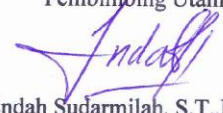
Surakarta, Maret 2015



Misbahul Munir

Mengetahui:

Pembimbing Utama



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

MOTTO DAN PERSEMBAHAN

MOTTO:

Allah akan meninggikan orang-orang yang berilmu di antaramu dan orang-orang yang diberi ilmu pengetahuan beberapa derajat. Dan Allah Maha Mengetahui apa yang kamu kerjakan.

(Q.S. Al Mujadilah : 11)

PERSEMBAHAN :

1. Ibu dan Bapak saya yang selalu memberikan doa dan restu hingga saya senantiasa diberikan jalan dan kemudahan dalam menghadapi segala hal, semoga Allah SWT selalu melindungi mereka berdua, amin.
2. Dosen Pembimbing saya Ibu Endah Sudarmilah, S.T.,M.Eng. yang telah bersedia meluangkan waktunya untuk membimbing, mengarahkan, dan memberi saya masukan dalam pengerjaan skripsi.
3. Adik saya Nisa dan seluruh keluarga saya yang telah mendukung dan memberi saya motivasi.
4. Sahabat saya Aan Zaini, Asrul Sani, Dwi Marjoko, Adit dan teman-teman satu angkatan saya Teknik Informatika 08' UMS yang selalu memberi motivasi dan masukan.
5. Sahabat akrab saya Aan Kunaifi, Fandi, Wahab, Soni, Hasan dan teman-teman kos California yang lain, yang selalu mendukung dan memberikan motivasi.

KATA PENGANTAR

Dengan mengucapkan syukur Alhamdulillah hanya kepada Allah Subhanahu Wata'ala yang telah memberikan rahmat, hidayah serta nikmat yang tiada terkira kepada hamba-Nya, sehingga penyusun dapat menyelesaikan skripsi ini dengan judul “Analisis Penggunaan Portsentry Sebagai Tools Intrusion Detection System pada Jaringan Komputer”.

Skripsi ini disusun untuk memenuhi kurikulum pada Program Studi Teknik Informatika Universitas Muhammadiyah Surakarta, sebagai kewajiban mahasiswa dalam rangka menyelesaikan program sarjana.

Dengan segala kemampuan yang maksimal, penyusun telah berusaha untuk menyelesaikan laporan skripsi ini, namun demikian penyusun menyadari bahwa laporan ini tentunya masih jauh dari kesempurnaan. Oleh karena itu penyusun mengharapkan dengan sangat saran serta kritik yang bersifat membangun demi perbaikan. Di sisi lain, skripsi ini juga merupakan hasil karya dan kerjasama dari banyak pihak, walaupun yang terlihat dimuka mungkin hanyalah sebuah nama. Sehingga dalam kesempatan ini penyusun mempersembahkan ucapan terima kasih dan penghargaan setinggi-tingginya dengan segala kerendahan hati, kepada:

1. Allah SWT dengan sebaik-baik pujian, puji yang tidak bisa diungkapkan dengan kata. Bagi-Mu puji atas iman dan islam yang Engkau anugrahkan. Maha mulia Engkau, Maha Suci nama-nama-Mu.

2. Shalawat dan salam semoga tetap dilimpahkan kepada Rasul Muhammad SAW dan keluarganya, dan para sahabatnya.
3. Bapak Dr. Heru Supriyono, S.T., M.Eng.Sc. selaku Ketua Jurusan Teknik Informatika Fakultas Komunikasi dan Informatika Universitas Muhammadiyah Surakarta.
4. Ibu Endah Sudarmilah, S.T., M.Eng. selaku Pembimbing Utama yang telah memberikan nasehat, bimbingan, dorongan, dan pengarahan kepada penulis sehingga dapat menyelesaikan skripsi ini.
5. Bapak dan Ibu dosen yang telah membimbing dan membagi ilmunya selama masa perkuliahan.
6. Ibu dan Adik yang telah memberikan dukungan dan doa.

Akhirnya penyusun berharap semoga skripsi ini berguna bagi semua pihak dan bermanfaat bagi penyusun khususnya dan pembaca pada umumnya dalam menambah pengetahuan dan wawasan ilmu. Amiin.

Surakarta, Maret 2015

Penulis

Misbahul Munir

DAFTAR ISI

Halaman Judul	i
Halaman Persetujuan	ii
Halaman Pengesahan	iii
Daftar Kontribusi	iv
Motto dan Persembahan	vi
Kata Pengantar	vii
Daftar Isi	ix
Daftar Tabel	xii
Daftar Gambar.....	xiii
Abstraksi	xvi
BAB I PENDAHULUAN	1
A. Latar Belakang Masalah	1
B. Rumusan Masalah	2
C. Tujuan Penelitian	3
D. Batasa Masalah.....	3
E. Manfaat Penelitian	4
F. Sistematika Penulisan	4
BAB II TINJAUAN PUSTAKA	6
A. Telaah Penelitian	6
B. Landasan Teori	9
1. Jaringan Komputer	9

2. Intrusion Detection System	9
3. Portsentry	11
4. Port Scanning	13
5. Sniffing.....	18
6. Sistem Operasi Komputer	19
a. Ubuntu.....	19
b. Windows 8.....	19
7. Virtual Machine	20
BAB III METODE PENELITIAN	21
A. Waktu dan Tempat	21
B. Alur Penelitian	21
C. Langkah Penelitian.....	23
1. Analisa Kebutuhan	23
2. Perancangan Sistem	25
3. Pengujian Sistem	34
BAB IV HASIL DAN PEMBAHASAN	37
A. Hasil Penelitian	37
B. Analisa dan Pembahasan	39
1. Pengujian Portsentry Terhadap Aktifitas Scanning dan Sniffing	39
a. Portsentry dengan konfigurasi default mode tcp/udp.....	39
b. Portsentry dengan konfigurasi default mode atcp/audp	45
c. Portsentry dengan konfigurasi default mode stcp/sudp.....	53

2. Pengujian pengaruh portsentry terhadap kecepatan transfer data rate dalam jaringan.....	60
a. Kecepatan transfer data rate pada server ke client dengan sistem operasi ubuntu	60
b. Kecepatan transfer data rate pada server ke client dengan sistem operasi windows 8.....	63
3. Analisa Hasil.....	65
BAB V PENUTUP	69
A. Kesimpulan	69
B. Saran	70
DAFTAR PUSTAKA	71

DAFTAR TABEL

Tabel 2.1 Software scanning dan tipe scanning yang digunakan untuk pengujian	18
Tabel 4.1 Hasil Pengujian Transfer Data Rate Dengan Client Ubuntu dan server Portsentry Off	61
Tabel 4.2 Hasil Pengujian Transfer Data Rate Dengan Client Ubuntu dan server Portsentry Mode Tcp/Udp	62
Tabel 4.3 Hasil Pengujian Transfer Data Rate Dengan Client Ubuntu dan server Portsentry Mode atcp/audp.....	63
Tabel 4.4 Hasil Pengujian Transfer Data Rate Dengan Client Ubuntu dan server Portsentry Mode stcp/sudp	63
Tabel 4.5 Hasil Pengujian Transfer Data Rate Dengan Client Windows 8 dan server Portsentry off	64
Tabel 4.6 Hasil Pengujian Transfer Data Rate Dengan Client Windows 8 dan server Portsentry Mode tcp/udp.....	64
Tabel 4.7 Hasil Pengujian Transfer Data Rate Dengan Client Windows 8 dan server Portsentry Mode atcp/audp	65
Tabel 4.8 Hasil Pengujian Transfer Data Rate Dengan Client Windows 8 dan server Portsentry Mode stcp/sudp	65
Tabel 4.9 Hasil Pengujian Keandalan Portsentry terhadap Aplikasi Scanner dan Sniffer	66
Tabel 4.10 Hasil Pengujian Pengaruh Penggunaan Portsentry terhadap Transfer Data Rate pada Jaringan Komputer	67

DAFTAR GAMBAR

Gambar 3.1 Flowchart alur penelitian.....	22
Gambar 3.2 Flowchart alur perancangan	25
Gambar 3.3 Instalasi Portsentry	26
Gambar 3.4 Konfigurasi default portsentry	26
Gambar 3.5 Konfigurasi rules portsentry.....	27
Gambar 3.6 Tampilan virtualbox	27
Gambar 3.7 Pengaturan pada <i>Virtual Machine</i>	28
Gambar 3.8 Tampilan 3 Virtual Machine yang Sedang Berjalan	28
Gambar 3.9 Pengaturan IP untuk Komputer Fisik pada Virtualbox	28
Gambar 3.10 Pengaturan Kartu Jaringan untuk Virtual Machine.....	29
Gambar 3.11 Pengaturan IP pada Virtual Machine 1	29
Gambar 3.12 Pengaturan IP pada Virtual Machine 2	30
Gambar 3.13 Pengaturan IP pada Virtual Machine 3	30
Gambar 3.14 Virtual Machine 3 Dengan Aplikasi Scanner dan Sniffer yang Telah Terpasang.....	31
Gambar 3.15 Pengaturan IP pada Server	32
Gambar 3.16 Pengaturan IP pada Client Ubuntu	32
Gambar 3.17 Pengaturan IP pada Client Windows 8.....	32
Gambar 3.18 Pengaturan Folder Sharing pada Client Ubuntu.....	33
Gambar 3.19 Pengaturan Folder Sharing pada Client Windows 8	33
Gambar 3.20 Aliran Data Pengujian 1	34
Gambar 3.21 Aliran Data Pengujian 2	35
Gambar 4.1 Konfigurasi Default Portsentry Mode tcp/udp	39
Gambar 4.2 Proses Scanning Menggunakan Angry IP Scanner	39
Gambar 4.3 Tampilan Syslog pada Proses Scanning Angry IP Scanner	40
Gambar 4.4 Tampilan History Portsentry	40
Gambar 4.5 Proses Scanning Menggunakan Superscan 4	41
Gambar 4.6 Tampilan Syslog pada Proses Scanning Superscan 4	41

Gambar 4.7 Tampilan History Portsentry	42
Gambar 4.8 Proses Scanning Menggunakan NMap	42
Gambar 4.9 Tampilan Syslog pada Proses Scanning NMap	43
Gambar 4.10 Tampilan History Portsentry	43
Gambar 4.11 Proses Sniffing Menggunakan Wireshark	44
Gambar 4.12 Proses Ping pada Virtual Machine 1	44
Gambar 4.13 Tampilan Syslog pada Proses Sniffing Wireshark	45
Gambar 4.14 Tampilan History Portsentry	45
Gambar 4.15 Konfigurasi Default Portsentry Mode atcp/audp	46
Gambar 4.16 Proses Scanning Menggunakan Angry IP Scanner	46
Gambar 4.17 Tampilan Syslog pada Proses Scanning Angry IP Scanner	47
Gambar 4.18 Tampilan History Portsentry	47
Gambar 4.19 Proses Scanning Menggunakan Superscan 4	48
Gambar 4.20 Tampilan Syslog pada Proses Scanning Superscan 4	48
Gambar 4.21 Tampilan History Portsentry	49
Gambar 4.22 Proses Scanning Menggunakan NMap	49
Gambar 4.23 Tampilan Syslog pada Proses Scanning NMap	50
Gambar 4.24 Tampilan History Portsentry	50
Gambar 4.25 Proses Sniffing Menggunakan Wireshark.....	51
Gambar 4.26 Proses Ping pada Virtual Machine 2 dan 1	51
Gambar 4.27 Tampilan syslog pada proses sniffing Wireshark	52
Gambar 4.28 Tampilan History Portsentry	52
Gambar 4.29 Konfigurasi Default Portsentry Mode stcp/sudp.....	53
Gambar 4.30 Proses Scanning Menggunakan Angry IP Scanner	53
Gambar 4.31 Tampilan Syslog pada Proses Scanning Angry IP Scanner	54
Gambar 4.32 Tampilan History Portsentry	54
Gambar 4.33 Proses Scanning Menggunakan Superscan 4	55
Gambar 4.34 Tampilan Syslog pada Proses Scanning Superscan 4	55
Gambar 4.35 Tampilan History Portsentry	56
Gambar 4.36 Proses Scanning Menggunakan Nmap.....	56
Gambar 4.37 Tampilan Syslog pada Proses Scanning Nmap.....	57

Gambar 4.38 Tampilan History Portsentry	57
Gambar 4.39 Proses Sniffing Menggunakan Wireshark.....	58
Gambar 4.40 Proses Ping pada Virtual Machine 1	58
Gambar 4.41 Tampilan Syslog pada Proses Sniffing Wireshark.....	59
Gambar 4.42 Tampilan History Portsentry	59
Gambar 4.43 Portsentry Tidak Aktif.....	60
Gambar 4.44 Aktifitas Lalu Lintas Data pada Jaringan Komputer.....	60
Gambar 4.45 Portsentry Setelah Dikonfigurasi dan Di-restart	62
Gambar 4.46 Grafik Perbandingan Transfer Data Rate pada Client Windows 8 dan Ubuntu Dengan Mode Portsentry yang Berbeda	67

ABSTRAKSI

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 aplikasi *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*.