

**ANALISIS SIMULASI KEAMANAN DENGAN METODE DHCP SNOOPING
DAN EXTENDED ACCESS LIST**

SKRIPSI



disusun oleh

Karlos Anton Mansumber

17.11.1062

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2021

**ANALISIS SIMULASI KEAMANAN DENGAN METODE DHCP SNOOPING
DAN EXTENDED ACCESS LIST**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika



disusun oleh

Karlos Anton Mansumber

17.11.1062

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2021

PERSETUJUAN

SKRIPSI

**PERBANDINGAN SIMULASI KEAMANAN DENGAN METODE DHCP
SNOOPING DAN EXTENDED ACCESS LIST**

Yang Dipersiapkan Dan Disusun Oleh

Karlos Anton Mansumber

17.11.1062

Telah Disetujui Oleh Dosen Pembimbing Skripsi

Pada Tanggal 10 Agustus 2021

Dosen Pembimbing,

Andika Agus Slameto, M.Kom

Nik. 190302109

PENGESAHAN

SKRIPSI

**PERBANDINGAN SIMULASI KEAMANAN DENGAN METODE DHCP
SNOOPING DAN EXTENDED ACCESS LIST**

yang dipersiapkan dan disusun oleh

Karlos Anton Mansumber

17.11.1062

telah dipertahankan di depan Dewan Penguji

pada tanggal 16 September 2021

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Eli Pujastuti, M.Kom

NIK. 190302227

Joko Dwi Santoso, M.Kom

NIK. 190302181

Andika Agus Slameto, M.Kom

NIK. 190302109

Skripsi ini telah diterima sebagai salah satu persyaratan

untuk memperoleh gelar Sarjana Komputer

Tanggal 16 September 2021

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, M.Kom

NIK. 190302096

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 3 November 2021



Karlos Anton Mansumber

NIM. 17.11.1062

MOTTO

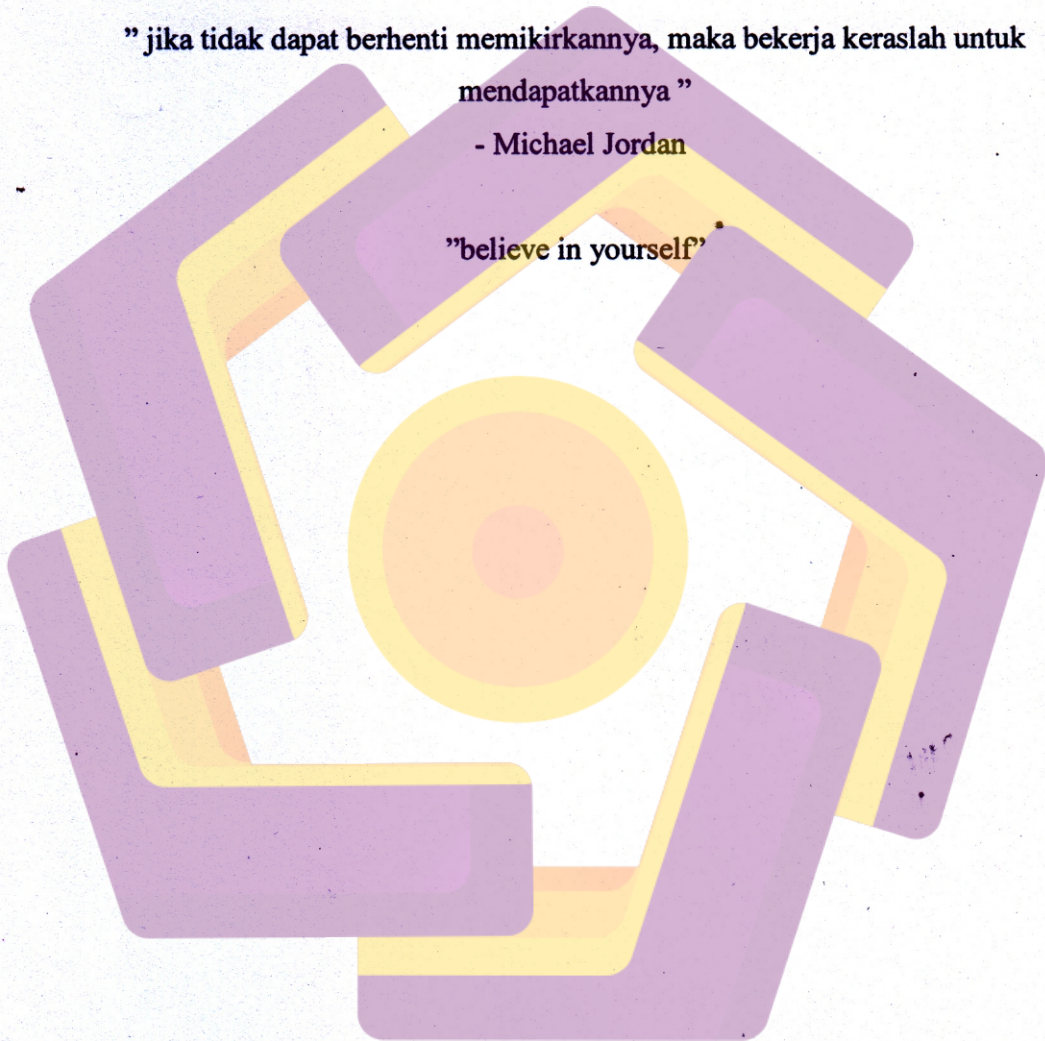
” orang yang ingin bergembira harus menyukai kelelahan akibat bekerja”

- Plato

” jika tidak dapat berhenti memikirkannya, maka bekerja keraslah untuk mendapatkannya ”

- Michael Jordan

”believe in yourself”



PERSEMBAHAN

Puji syukur kepada Tuhan yang Maha Esa, karena berkat rahmat dan ridho-Nya, penulis diberi ilmu, kemudahan, ketabahan, dan kekuatan sehingga dapat mengerjakan serta menyelesaikan skripsi ini sebagai salah satu syarat untuk lulus dan meraih gelar sarjana. Skripsi ini penulis persembahkan kepada :

1. Kepada kedua orang tua penulis yang selalu mendoakan penulis dari jauh dan selalu bekerja keras untuk memenuhi kebutuhan penulis selama ini.
2. Kakak-kakak penulis Kores, Aidil, Alan, Erzenna yang selalu memberi semangat.
3. Kepada Ibu kos dan Bapak kos yang telah memberi tempat tinggal selama penulis merantau di Yogyakarta.
4. Kepada seluruh keluarga, teman, dan siapapun yang telah mendukung penulis selama ini.
5. Kepada Nathaline Thania Raunsai yang telah membantu, mendampingi, dan menyemangati penulis selama ini
6. Kepada rekan-rekan penulis, Harun, Deden, Adnan, Yoga, Khusnanto, Rizal, Feri, Alawi, dan Agung yang telah menghabiskan masa kuliah Bersama.
7. Kepada teman-teman kelas 17 S1-IF-3.

KATA PENGANTAR

Puji Syukur kehadiran Tuhan yang Maha Esa, Tuhan semesta alam yang senantiasa memberikan Rahmat dan Karunia-Nya, sehingga penulis dapat menyelesaikan skripsi yang berjudul “Perbandingan Simulasi Keamanan Dengan Metode DHCP Snooping Dan Extended Access List”.

Penulisan skripsi ini merupakan salah satu syarat dalam rangka mendapatkan gelar sarjana khususnya untuk Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta. Penulis menyadari bahwa dalam menyelesaikan penelitian skripsi ini tak lepas dari bantuan berbagai pihak, maka penulis berterima kasih kepada :

1. Bapak Andika Agus Slameto selaku Dosen Pembimbing.
2. Keluarga Besar, Ayah dan Ibu serta Kakak-kakak.
3. Rekan-rekan seperjuangan.
4. Temanku Dimas yang telah membantu proses penelitian ini.

Akhir kata, penulis mengucapkan terima kasih dan semoga Tuhan membalas segala kebaikan semua pihak yang telah terlibat dan membantu proses penelitian ini. Semoga penelitian skripsi yang telah penulis lakukan dapat bermanfaat bagi pengembangan ilmu pengetahuan di masa yang akan datang.

Yogyakarta, 3 November 2021



Penulis

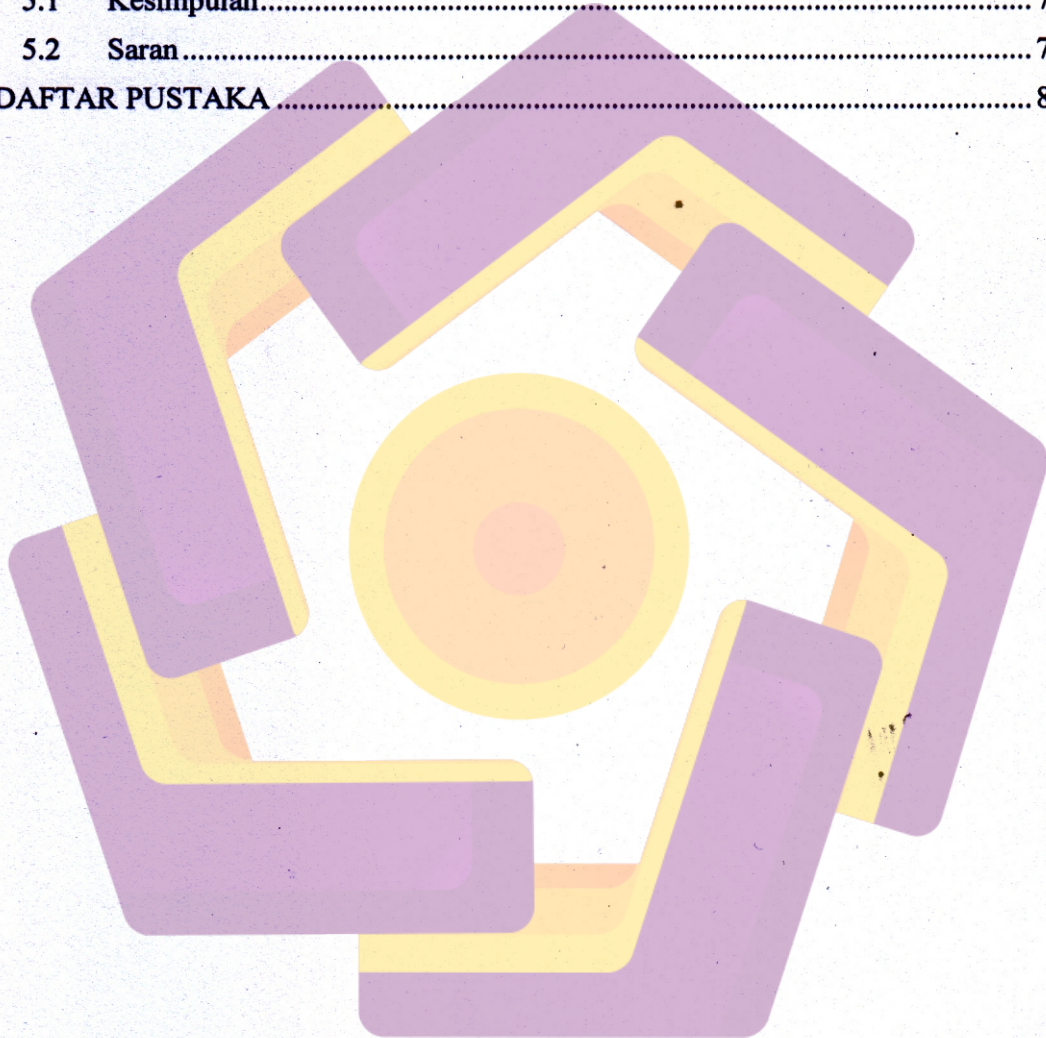
DAFTAR ISI

HALAMAN JUDUL	ii
PERSETUJUAN	iii
PENGESAHAN	iv
SKRIPSI.....	iv
PENGESAHAN	iv
SKRIPSI.....	iv
PENGESAHAN	iv
SKRIPSI.....	iv
PENGESAHAN	iv
SKRIPSI.....	iv
PERNYATAAN.....	v
MOTTO	vi
PERSEMBAHAN	vii
KATA PENGANTAR	viii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	Error! Bookmark not defined.
DAFTAR GAMBAR	Error! Bookmark not defined.
INTISARI.....	xvii
ABSTRACT.....	xviii
BAB I.....	1
PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah.....	4
1.4 Maksud Dan Tujuan Penelitian	4
1.5 Manfaat Penelitian.....	5
1.6 Metode Penelitian.....	5
1.6.1 Metode Pengumpulan Data.....	5

1.6.2 Analysis	6
1.6.3 Design	6
1.6.4 Simulation Prototyping	6
1.6.5 Implementation	6
1.6.6 Monitoring	7
1.6.7 Result	7
1.7 Sistematika	7
BAB II.....	9
LANDASAN TEORI.....	9
2.1 Kajian Pustaka.....	9
2.1.1 Tinjauan Pustaka	13
2.2 Dasar Teori.....	16
2.3 Keamanan Jaringan Komputer	16
2.3.1 Pengertian Aspek-Aspek Pada Keamanan Jaringan	16
2.3.2 Virtual Local Area Network (Vlan)	17
2.4 DHCP	20
2.4.1 DHCP Server.....	20
2.4.2 DHCP Rouge.....	21
2.5 Access Control List (ACL).....	22
2.5.1 Access Control List Standar (ACL)	22
2.5.2 Access Control List Extended (ACL)	22
2.7 Protokol Jaringan.....	23
2.7.1 TCP	23
2.8 IP Address	24
2.9 Gateway.....	24
2.10 Subnetting.....	25
2.11 Osi Layer	25
2.11.1 Data Link Layer	26
2.12 Metode Penelitian.....	26
2.13 Software Cisco Packet Tracer	27

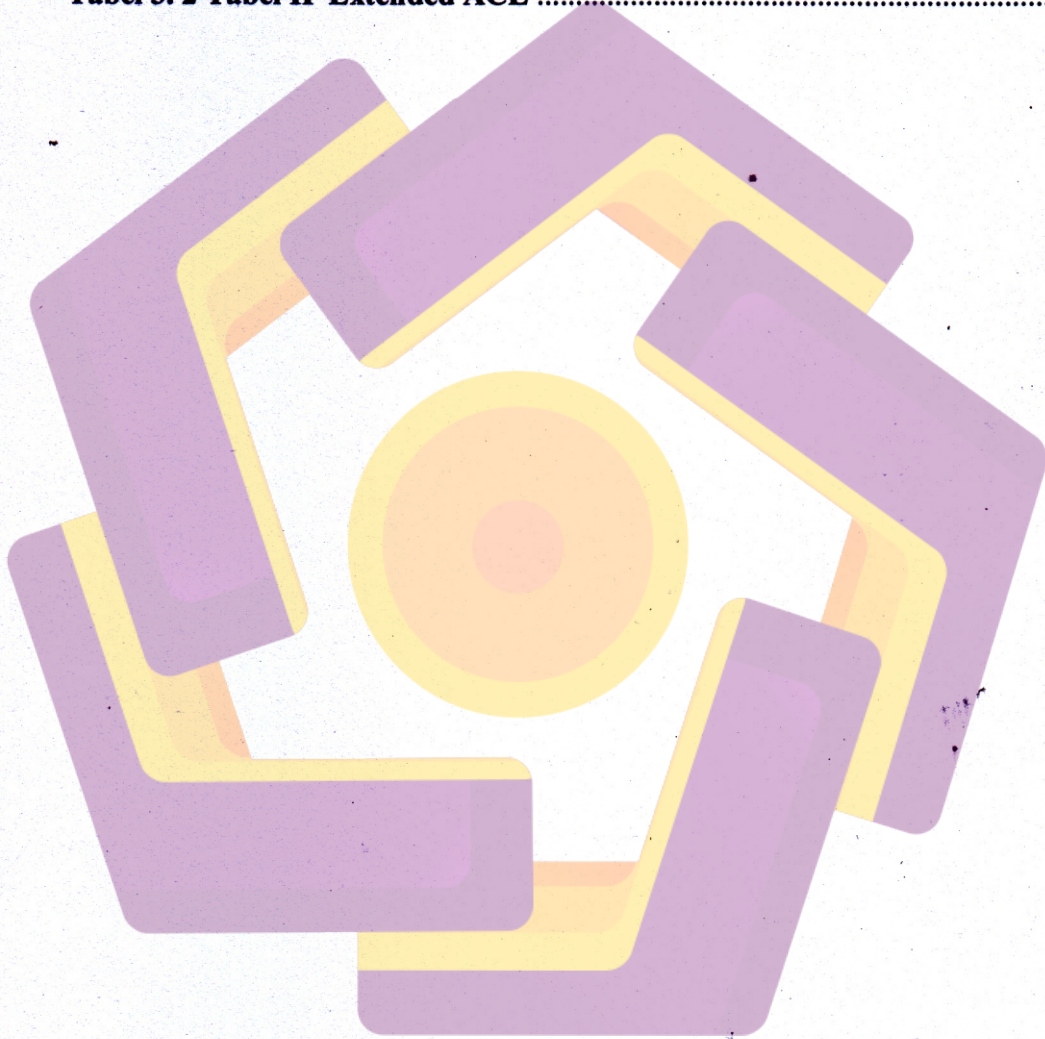
2.14	Perangkat Jaringan	27
2.14.1	Router	28
2.14.2	Switch.....	28
2.14.3	Server	28
2.14.4	Personal Computer (<i>PC</i>)	29
2.14.5	Kabel jaringan	29
BAB III		31
METODE PENELITIAN.....		31
3.1	Gambaran Umum	31
3.2	Alat dan Bahan Penelitian	32
3.2.1	Perangkat Keras (<i>Hardware</i>)	32
3.2.2	Perangkat Lunak (<i>Software</i>).....	33
3.3	Rancangan Tabel IP Address	33
3.3.1	Table IP DHCP Snooping	33
3.3.2	Rancangan Tabel IP Extended ACL	34
3.4	Rancangan Topologi Jaringan	34
3.4.1	Rancangan Topologi Metode DHCP Snooping	35
3.4.2	Rancangan Topologi Metode Extended (ACL)	36
3.5	Rancangan Pengujian	36
3.5.1	Diagram Pengujian.....	38
BAB IV		40
IMPLEMENTASI DAN PEMBAHASAN.....		40
4.1	Implementasi	40
4.2	Implementasi DHCP Snooping	40
4.3	Konfigurasi DHCP Server.....	40
4.4	Konfigurasi DHCP Rouge.....	47
4.5	Konfigurasi Snooping.....	51
4.6	Pengujian DHCP Rouge.....	54
4.7	Pengujian DHCP Snooping	56
4.8	Implementasi Extended Access-List	61

4.8.1	konfigurasi Extended Access-List.....	61
4.8.2	Pengujian Standard Access-List Dan Extended Access-List.....	68
BAB V.....		78
PENUTUP.....		78
5.1	Kesimpulan.....	78
5.2	Saran.....	79
DAFTAR PUSTAKA.....		80



DAFTAR TABEL

Tabel 2. 1 Tabel Perbandingan Pengujian.....	13
Tabel 3. 1 Tabel IP DHCP Snooping.....	33
Tabel 3. 2 Tabel IP Extended ACL	34

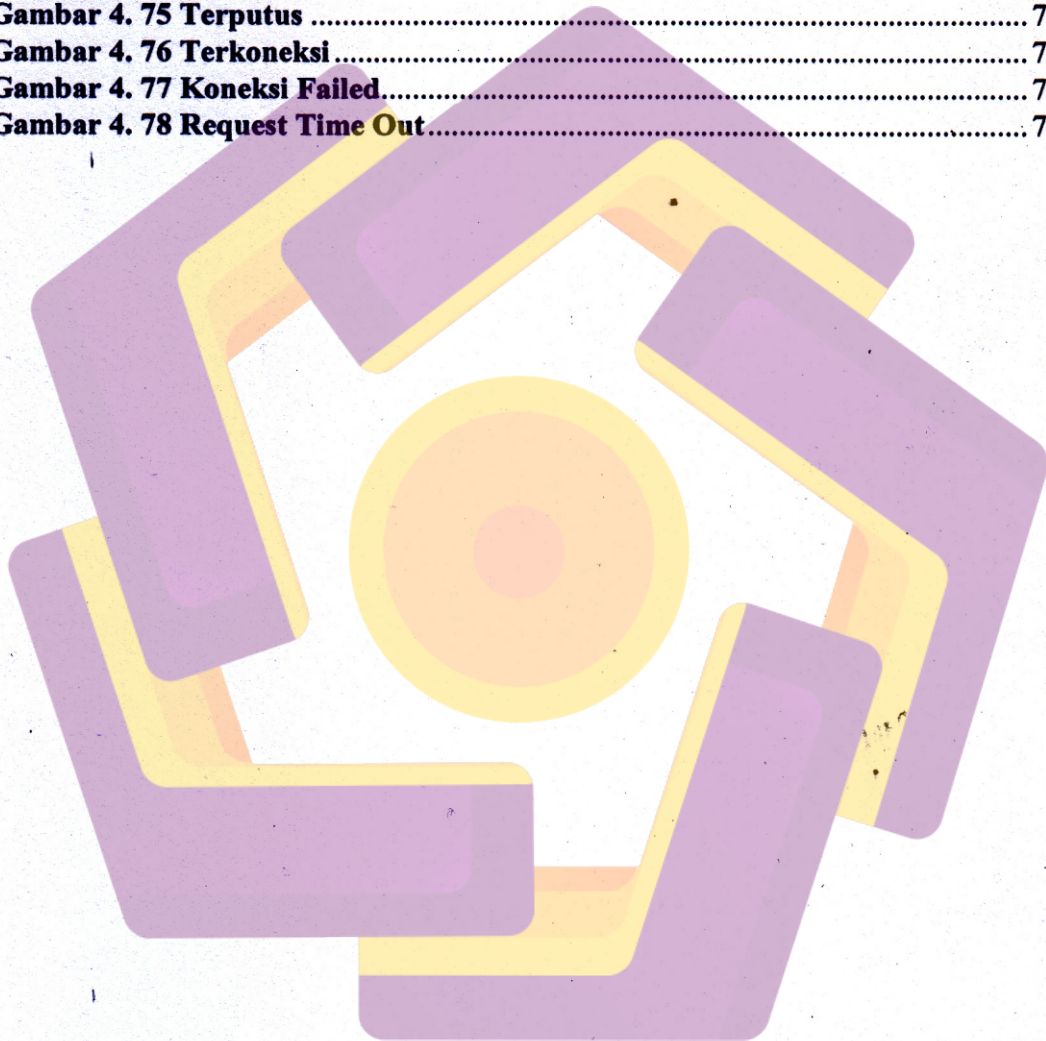


DAFTAR GAMBAR

Gambar 2. 1 Jaringan Vlan.....	18
Gambar 2. 2 Jaringan Komputer Dengan Vlan.....	18
Gambar 2. 3 Port Based Vlan	19
Gambar 2. 4 Mac Based Vlan	20
Gambar 2. 5 Kabel Straight Throught.....	30
Gambar 2. 6 Kabel Cross Over.....	30
Gambar 3. 1 Snooping Topologi	35
Gambar 3. 2 Topologi Extended ACL	36
Gambar 3. 3 Diagram Pengujian.....	38
Gambar 4. 1 Konfigurasi IP Address.....	41
Gambar 4. 2 Konfigurasi DHCP Pool Asli	41
Gambar 4. 3 Konfigurasi IP Network.....	41
Gambar 4. 4 Konfigurasi Default-Router.....	42
Gambar 4. 5 PC0.....	43
Gambar 4. 6 PC1.....	43
Gambar 4. 7 PC2.....	44
Gambar 4. 8 PC3.....	44
Gambar 4. 9 Laptop0.....	45
Gambar 4. 10 Laptop1.....	45
Gambar 4. 11 Laptop2.....	46
Gambar 4. 12 Server.....	46
Gambar 4. 13 Konfigurasi Server	47
Gambar 4. 14 Setting Ip DHCP Rouge	48
Gambar 4. 15 Seting DHCP Pool Rouge.....	48
Gambar 4. 16 Seting Ip Network.....	48
Gambar 4. 17 Seting Default-Router.....	49
Gambar 4. 18 PC0.....	49
Gambar 4. 19 Laptop0.....	50
Gambar 4. 20 PC1.....	51
Gambar 4. 21 Seting Ip DHCP Snooping	51
Gambar 4. 22 Seting DHCP Snooping Vlan 1	52
Gambar 4. 23 Seting No Ip DHCP Snooping Information Option.....	52
Gambar 4. 24 Seting Interface Router Utama.....	52
Gambar 4. 25 Seting Legit Dhcp.....	52
Gambar 4. 26 Seting Ip DHCP Sooping Trust	53
Gambar 4. 27 Exit.....	53
Gambar 4. 28Seting Int Fa0/7.....	53

Gambar 4. 29 Deskripsikan Rouge.....	53
Gambar 4. 30 Pc0 To Server Terputus	54
Gambar 4. 31 Pc1 To Server Terputus	55
Gambar 4. 32 Laptop0 To Server Terputus	55
Gambar 4. 33 Rouge Icmp Client To Server Failed	56
Gambar 4. 34 Pc0 To Server	56
Gambar 4. 35 Pc1 To Server	57
Gambar 4. 36 Laptop0 To Server	57
Gambar 4. 37 Icmp Client To Server Successful	58
Gambar 4. 38 Pc2 To Server	58
Gambar 4. 39 Pc3 To Server	59
Gambar 4. 40 Laptop1 To Server	59
Gambar 4. 41 Laptop2 To Server	60
Gambar 4. 42 koneksi successful	60
Gambar 4. 43 koneksi successful	60
Gambar 4. 44 Pc0 Ip Teracak Gambar 4. 45 Pc1 Ip Teracak.....	61
Gambar 4. 46 Laptop0 Ip Teracak.....	61
Gambar 4. 47 Seting Ip Address Kearah Client.....	62
Gambar 4. 48 Konfigurasi Server.....	63
Gambar 4. 49 pc0	63
Gambar 4. 50 PC1	64
Gambar 4. 51 PC2.....	64
Gambar 4. 52 PC3.....	65
Gambar 4. 53 Laptop0.....	65
Gambar 4. 54 Laptop1	66
Gambar 4. 55 Laptop2.....	66
Gambar 4. 56 Proses Memblok ip Layanan Pc0	67
Gambar 4. 57 Proses Mengijinkan Host Lain lewat.....	67
Gambar 4. 58 Out/Keluar.....	67
Gambar 4. 59 Exit	67
Gambar 4. 60 Proses Blok Layanan Laptop1 Ke Server	68
Gambar 4. 61 Seting Izinkan Akses Host Lain Lewat.....	68
Gambar 4. 62 In/Masuk.....	68
Gambar 4. 63 Ping Pc1 To Server	69
Gambar 4. 64 Ping Pc2 To Server	70
Gambar 4. 65 Pc3 To Server	70
Gambar 4. 66 Ping Laptop0 To Server	71
Gambar 4. 67 Laptop2 To Server.....	71
Gambar 4. 68 Icmp Dari Pc1 Sampai Laptop2	72

Gambar 4. 69 Icmp Dari Pc1 Sampai Laptop2	72
Gambar 4. 70 Pc1 Terkoneksi.....	72
Gambar 4. 71 Terkoneksi	73
Gambar 4. 72 Terkoneksi	73
Gambar 4. 73laptop0 Terkoneksi	74
Gambar 4. 74 Terkoneksi	74
Gambar 4. 75 Terputus	75
Gambar 4. 76 Terkoneksi	75
Gambar 4. 77 Koneksi Failed.....	76
Gambar 4. 78 Request Time Out.....	76



INTISARI

Jaringan komputer berkembang dengan sangat pesat, baik di instansi-instansi komersil, dunia akademik, bahkan rumah-rumah penduduk yang membutuhkan akses internet. Internet merupakan sebuah singkatan dari Interconnection Networking, atau yang berarti jaringan yang terhubung secara luas. Internet merupakan keterkaitan jaringan komputer melalui standard yang disebut global *Transmission Control Protocol* atau *Internet Protocol* (TCP/IP) yang terdapat sistem pertukaran paket komunikasi yang berasal melalui data.

Penelitian ini dilakukan analisis perbandingan dari kinerja teknologi keamanan jaringan pada (*Virtual Lan*) VLAN, dimana metode-metode keamanan jaringan yang akan diterapkan pada keamanan jaringan ini adalah DHCP SNOOPING dan EXTENDED ACCESS LIST yang akan di terapkan Vlan untuk melakukan simulasi perbandingan keamanan jaringan metode-metode tersebut.

Setelah dilakukan pengujian perbandingan hasil menunjukkan kinerja dari DHCP Snooping dan Extended Access List pada jaringan Lan berbasis Vlan maka dapat disimpulkan bahwa DHCP SNOOPING dapat memfilter dan memvalidasi terhadap port yang terpercaya dan tidak terpercaya. Dengan menggunakan DHCP Snooping jaringan komputer akan lebih aman tidak terganggu dengan adanya server DHCP yang lain atau palsu. Extended Access List dapat melakukan pengendalian trafik jaringan dengan menyaring paket data yang melewati router. Router akan melakukan pengecekan access list pada saat setiap paket data akan masuk pada port yang di router tersebut. Extended access list melakukan pengecekan terhadap beberapa atribut, yaitu alamat sumber, alamat tujuan, protokol, dan nama port.

Kata kunci : *DHCP Snooping, Extended Accesslist, Vlan, Security Network.*

ABSTRACT

Computer networks are growing very rapidly, both in commercial institutions, the academic world, and even people's homes that need internet access. Internet is an abbreviation of Interconnection Networking, or which means a widely connected network. The Internet is a computer network linkage through a standard called the Global Transmission Control Protocol or Internet Protocol TCP / IP which is a system for exchanging communication packets originating through data.

This study conducted a comparative analysis of the performance of network security technology on (Virtual Lan) VLANs, where the network security methods that will be applied to this network security are DHCP SNOOPING and EXTENDED ACCESS LIST which will be applied to VLANs to perform a comparison simulation of network security methods. the method.

After a comparison test of the results shows the performance of DHCP Snooping and Extended Access List on a VLAN-based Lan network, it can be concluded that DHCP snooping can filter and validate trusted and untrusted ports. By using DHCP Snooping, your computer network will be safer not to be disturbed by other or fake DHCP servers. The Extended Access List can control network traffic by filtering data packets that pass through the router. The router will check the access list when each data packet will enter the port on the router. The extended access list checks several attributes, namely source address, destination address, protocol, and port name.

Keyword: DHCP Snooping, Extended Accesslist, Vlan, Security Network.