

**ANALISA KEAMANAN JARINGAN PADA VLAN
MENGUNAKAN DHCP SNOOPING**

SKRIPSI



disusun oleh

Setiawan Eko Nugroho

17.11.1555

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2022**

**ANALISA KEAMANAN JARINGAN PADA VLAN
MENGUNAKAN DHCP SNOOPING**

SKRIPSI

untuk memenuhi sebagian persyaratan mencapai gelar Sarjana
pada jenjang Program Sarjana – Program Studi Informatika



disusun oleh

Setiawan Eko Nugroho

17.11.1555

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2022**

PERSETUJUAN

SKRIPSI

ANALISA KEAMANAN JARINGAN PADA VLAN MENGUNAKAN METODE DHCP SNOOPING

yang dipersiapkan dan disusun oleh

Setiawan Eko Nugroho

17.11.1555

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 21 Februari 2022

Dosen Pembimbing

Andika Agus Slameto, M.Kom.

NIK. 190302109

PENGESAHAN

SKRIPSI

ANALISA KEAMANAN JARINGAN PADA VLAN MENGUNAKAN METODE DHCP SNOOPING

yang dipersiapkan dan disusun oleh

Setiawan Eko Nugroho 17.11.1555

telah dipertahankan di depan Dewan Penguji

pada tanggal 21 Februari 2022

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Andika Agus Slameto, M.Kom

NIK. 190302109

Yudi Sutanto, M.Kom

NIK. 19030203

Melwin Syafrizal, S.Kom., M.Eng

NIK. 190302057

Skripsi ini telah diterima sebagai salah satu persyaratan

untuk memperoleh gelar Sarjana Komputer

Tanggal 21 Februari 2022

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fattah, S.Kom., M.Kom.

NIK. 190302096

PERNYATAAN

PERNYATAAN

Saya yang bertanda tangan di bawah ini menyatakan, skripsi ini merupakan karya saya sendiri (ASLI) dan isi didalam skripsi tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu Instansi Pendidikan dan sepanjang pengetahuan saya tidak terdapat karya atau pendapat yang pernah ditulis / 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 tanggung jawab saya pribadi.

Yogyakarta, 20 Juni 2022

Hormat saya,

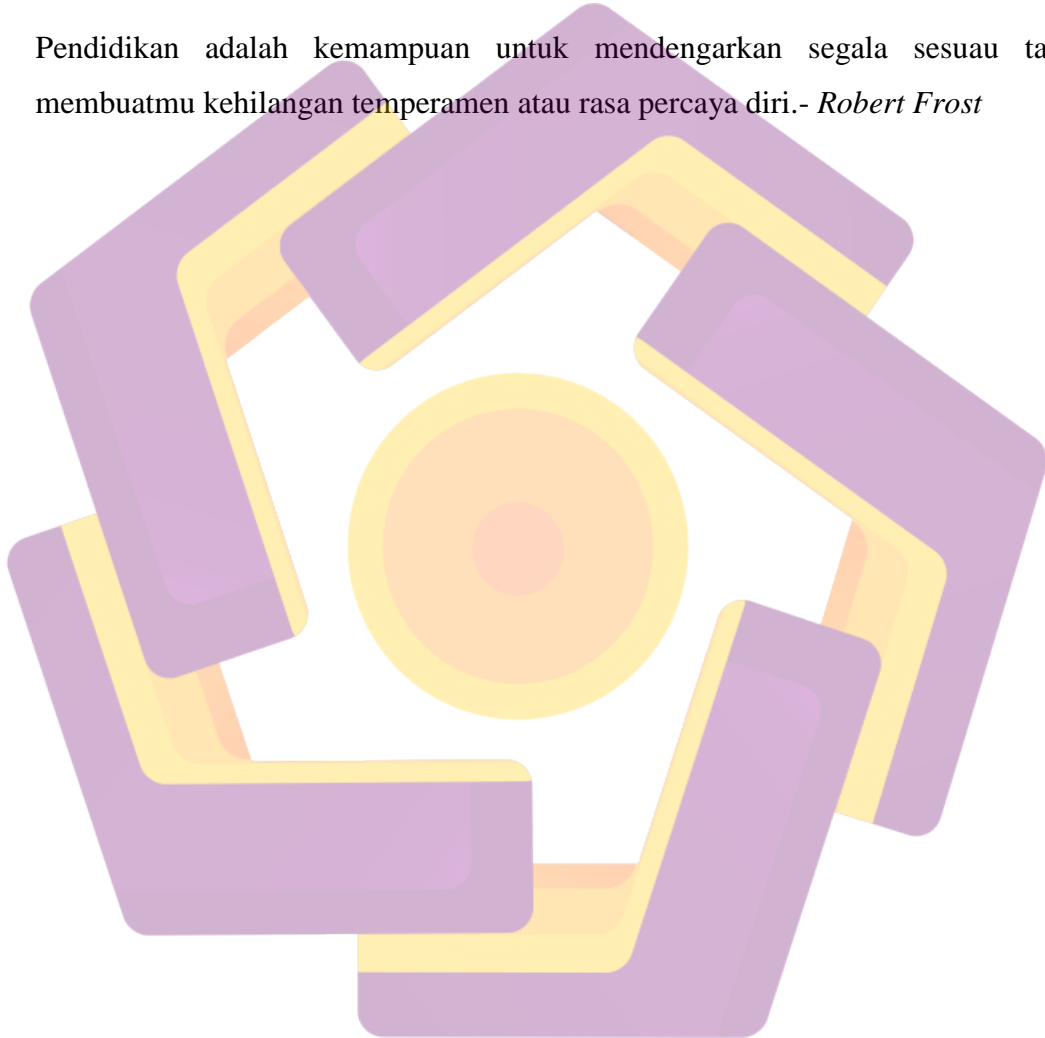


Setiawan Eko Nugroho
NIM. 17.11.1555

MOTTO

Jangan pergi mengikuti kemana jalan akan berujung. Buat jalanmu sendiri dan tinggalkanlah jejak.- *Ralph Waldo Emerson*

Pendidikan adalah kemampuan untuk mendengarkan segala sesuau tanpa membuatmu kehilangan temperamen atau rasa percaya diri.- *Robert Frost*



HALAMAN PERSEMBAHAN

Puji syukur saya haturkan kepada Allah SWT dengan rahmat serta hidayahnya telah memberikan kenikmatan, kesehatan, serta rasa syukur ini sehingga saya dapat menyelesaikan Tugas akhir skripsi ini dengan baik. Sholawat serta salam senantiasa saya tujukan kepada nabi agung Muhammad SAW yang kita nantikan syafa'at nya besok di hari akhir.

Pada kesempatan ini saya mengucapkan terimakasih kepada semua pihak yang telah membantu dalam semua proses pembuata skripsi ini, maka dari itu saya persembahkan skripsi ini untuk :

1. Kedua orang tua serta keluarga besar saya yang selalu mendukung serta memberikan do'a yang terbaik pada pendidikan saya.
2. Bapak Andika Agus Slameto, M.Kom selaku dosen pembimbing saya yang tidak henti – hentinya membimbing saya sehingga pengerjaan skripsi ini dapat diselesaikan.
3. Sahabat saya, teman kontrakan, teman kelas yang selalu mensupport dan membantu memberikan masukan kepada saya.
4. Semua pihak yang mendukung saya secara langsung dan tidak langsung yang tidak bisa saya sebutkan semua.

KATA PENGANTAR

Puji dan syukur senantiasa saya panjatkan kepada ALLAH SWT, karena berkat pertolongan-Nya Alhamdulillah penelitian ini dapat diselesaikan dengan baik. Laporan skripsi yang dibuat untuk memenuhi syarat memperoleh gelar kesarjanaan Strata-1 (S1) jurusan Informatika Universitas AMIKOM Yogyakarta diharapkan bisa menjadi salah satu referensi pembuatan skripsi di Universitas AMIKOM Yogyakarta serta dapat memberikan penambahan ide yang dapat dikembangkan dimasa depan.

Dalam penelitian ini peneliti mengucapkan terimakasih yang sebesar – besarnya kepada semua pihak yang telah terlibat dalam penyusunan skripsi ini dari awal sampai akhir , oleh sebab itu disini penulis menyampaikan apresiasi kepada :

1. Bapak Andika Agus Slameto, M.Kom selaku dosen pembimbing.
2. Kedua orang tua saya dan keluarga saya.
3. Sahabat – sahabat saya yang membantu dalam proses berjalannya penelitian ini

Terakhir semoga segala bantuan yang telah diberikan, sebagai amal soleh senantiasa mendapat Ridho Allah SWT. Sehingga pada akhirnya skripsi ini dapat bermanfaat

Yogyakarta 20 Juni 2022

DAFTAR ISI

PERNYATAAN.....	v
MOTTO	vi
HALAMAN PERSEMBAHAN	vii
KATA PENGANTAR	viii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xi
DAFTAR GAMBAR	xi
INTISARI.....	xiv
<i>ABSTRACT</i>	xv
BAB I.....	1
PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah.....	2
1.4 Maksud dan Tujuan Penelitian.....	3
1.5 Manfaat Penelitian	3
1.6 Analisis dan Perancangan	4
1.6.1 Study Pustaka	4
1.6.2 Perancangan Sistem.....	4
1.6.3 Perancangan Pengujian.....	4
1.7 Sistematika Penulisan	5
BAB II.....	6
LANDASAN TEORI.....	6
2.1 Sistematika Penulisan	6
2.1.2 Literature Review	8
2.2 Dasar Teori.....	11
2.2.1 Pengertian VLAN.....	11
2.2.2 OSI Layer	13

2.2.3 Classless IP	15
2.2.4 Cisco Packet Tracer	16
2.2.6 Sistem Keamanan Jaringan	20
2.2.7 DHCP Snooping	21
BAB III	25
ANALISIS DAN PERANCANGAN.....	25
3.1 Analisa Masalah	25
3.2 Solusi Permasalahan.....	26
3.2 Analisa Kebutuhan	26
3.2.1 Perangkat Keras (Hardware)	26
3.2.3 Perangkat Lunak (Software).....	27
3.4 Perancangan Sistem	30
3.4.1 Perancangan Alur Proses.....	31
3.4.2 Perancangan Topologi	32
3.4.3 Perancangan Konfigurasi Sistem.....	33
3.5 Perancangan Pengujian	35
BAB IV	36
HASIL DAN PEMBAHASAN.....	36
4.1 Tahap Implementasi	36
4.1.1 Tahap Konfigurasi Simulasi.....	36
4.1.2 Tahap konfigurasi IP DHCP Trusted dan Untrusted.....	37
4.1.3 Tahap Konfigurasi Switch dan Router dengan DHCP Snooping.....	44
4.2 Tahap Pengujian.....	51
4.2.1 Tahap Pengujian IP DHCP (Tanpa DHCP Snooping)	51
4.2.2 Tahap Pengujian ulang IP DHCP (dengan DHCP Snooping).....	53
4.2.3 Perbandingan IP DHCP Sebelum dan Sesudah di DHCP Snooping.....	54
BAB V.....	59
PENUTUP.....	59
5.1 Kesimpulan	59
5.2 Saran.....	60
DAFTAR PUSTAKA	61

DAFTAR TABEL

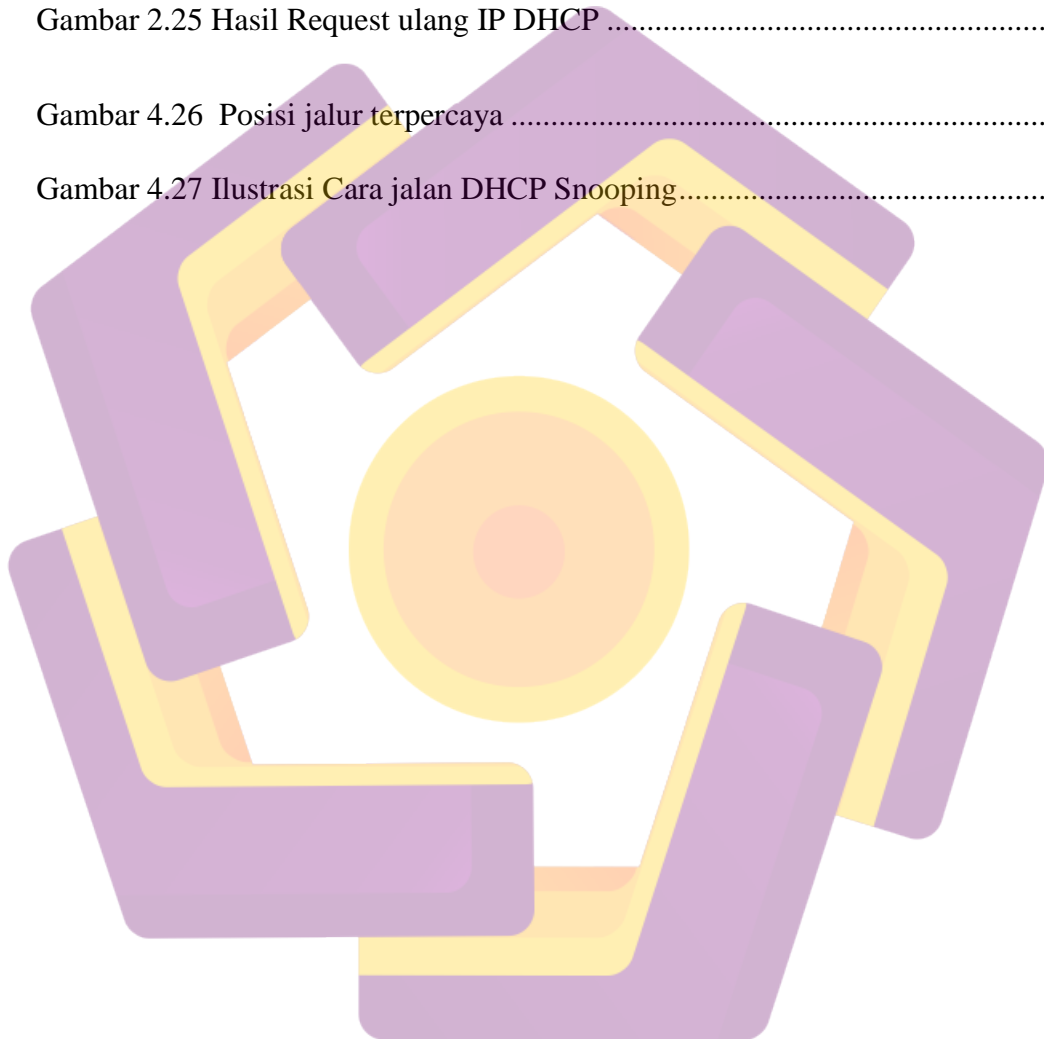
Tabel 2.1 Literatur Review	8
Tabel 3.1 Spesifikasi Laptop.....	27
Table 3.2 Spesifikasi Cisco Packet Tracer.....	27
Tabel 3.3 Perangkat Cisco.....	27
Tabel 3.4 Addressing	34
Tabel 3.5 Hasil Akhir Pencatatan Request IP DHCP	35
Table 4.1 Hasil Request IP DHCP server dari PC	52
Tabel 4.2 Hasil Request IP DHCP server dari PC	54
Tabel 4.3 Perbandingan IP Client sebelum dan sesudah di terapkan DHCP Snooping.	55

DAFTAR GAMBAR

Gambar 2.1 Tampilan Launcher Aplikasi Cisco Packet Tracer.....	17
Gambar 2.2 Tampilan Main Toolbar	17
Gambar 2.3 Tab menu Network Device	18
Gambar 2.4 Tab menu End device	18
Gambar 2.5 Tab menu connection	18
Gambar 2.6 Tampilan kerangka Kerja	19
Gambar 3.1 Alur Rancangan Sistem.....	30
Gambar 3.2 Diagram Alur Penelitian.....	31

Gambar 3.3 Skema Topologi	32
Gambar 3.4 Topologi VLAN	32
Gambar 3.5 Alur Koneksi Proses Keamanan.....	33
Gambar 4.1 Susunan Jaringan VLAN	36
Gambar 4.2 Posisi Router Trusted VLAN	38
Gambar 4.3 Jendela Konfigurasi Router Trusted.....	38
Gambar 4.4 Konfigurasi Port Router Trusted.....	39
Gambar 4.5 Konfigurasi Port Router Trusted.....	40
Gambar 4.6 Langkah Konfigurasi DHCP Server.....	41
Gambar 4.7 Langkah Konfigurasi ISP Server pada Router	41
Gambar 4.8 Posisi Router Untrusted.....	42
Gambar 4.9 Tampilan Konfigurasi Port Router Untrusted	42
Gambar 4.10 Hasil Akhir Router Untrusted	43
Gambar 4.11 Langkah Konfigurasi Router Untrusted	43
Gambar 4.12 Posisi Core Switch & router Trusted.....	44
Gambar 4.13 Posisi trusted port yang akan dikonfigurasi	45
Gambar 4.14 Jendela CLI Trusted Router	46
Gambar 4.15 Perintah DHCP Snooping Router.....	46
Gambar 4.16 Jendela CLI Core Switch	47
Gambar 4.17 Konfigurasi DHCP Snooping pada Core Switch	48
Gambar 4.18 Jendela CLI Switch 1	49
Gambar 4.19 Konfigurasi Switch 1.....	49
Gambar 4.20 Jendela CLI Switch 2	50

Gambar 4.21 Konfigurasi Switch 2.....	50
Gambar 4.22 Tampilan Jendela Baru IP Configuration.....	51
Gambar 2.23 Hasil Request IP DHCP Server	52
Gambar 4.24 Jendela konfigurasi IP Client	53
Gambar 2.25 Hasil Request ulang IP DHCP	53
Gambar 4.26 Posisi jalur terpercaya	57
Gambar 4.27 Ilustrasi Cara jalan DHCP Snooping.....	58



INTISARI

Kurangnya kesadaran masyarakat akan pentingnya keamanan jaringan menyebabkan jaringan internet sangat bermasalah. Pengguna melakukan untuk memberikan pelayanan jaringan komputer dan internet seperti manajemen bandwidth, memberikan keamanan pada jaringan seperti menggunakan IDS, IPS, ACL, Switchport Security, Sticky Port Security, DHCP Spoofing dan DHCP Snooping. Metode penelitian yang digunakan penulis dengan melakukan penelitian Analisa jaringan pada VLAN adalah menggunakan Metode DHCP Snooping.

Penulis bertujuan untuk menyelesaikan masalah metode serangan jaringan DHCP Rogue dengan menggunakan DHCP Snooping yang merupakan fitur keamanan jaringan yang jarang digunakan orang. DHCP Snooping merupakan keamanan pada jaringan komputer dan internet yang digunakan untuk mencegah atau memfilter adanya server lain yang tidak dipercaya dalam memberikan akses jaringan kepada pengguna atau komputer client.

Peneliti akan melakukan analisa perbandingan jaringan pada VLAN dan membuktikan bahwa pengaruh DHCP Snooping mampu membendung server DHCP lain yang memiliki IP Address yang berbeda. Dengan metode DHCP Snooping dan tanpa DHCP Snooping menggunakan software simulasi Cisco Packet Tracer.

Kata Kunci : VLAN, DHCP Snooping, Network Security, DHCP Rouge, Cisco Packet Tracer

ABSTRACT

Lack of public awareness of the importance of network security causes the internet network to be very problematic. Users perform to provide computer and internet network services such as bandwidth management, providing security on the network such as using IDS, IPS, ACL, Switchport Security, Sticky Port Security, DHCP Spoofing and DHCP Snooping. The research method used by the author by conducting research on network analysis on VLANs is using the DHCP Snooping method.

The author aims to solve the problem of the DHCP Rogue network attack method by using DHCP Snooping which is a network security feature that people rarely use. DHCP Snooping is security on computer networks and the internet that is used to prevent or filter other servers that are not trusted in providing network access to users or client computers.

Researchers will conduct a network comparison analysis on VLANs and prove that the effect of DHCP Snooping is able to stem other DHCP servers that have different IP addresses. With DHCP Snooping method and without DHCP Snooping using Cisco Packet Tracer simulation software.

Keywords : VLAN, DHCP Snooping, Network Security, DHCP Rouge, Cisco Packet Tracer