ANALISIS SEGMENTASI VLAN TERHADAP KEAMANAN JARINGAN MENGGUNAKAN METODE CIA TRIAD



SKRIPSI

Untuk Memenuhi Persyaratan Mencapai Gelar Sarjana Komputer (S.Kom)
Pada Program Studi Teknologi Informasi Fakultas Teknik
Universitas Muhammadiyah Palembang

Oleh:

M.Hajaji Alfarizi

162022075

PROGRAM STUDI TEKNOLOGI INFORMASI
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH PALEMBANG
2026

HALAMAN PENGESAHAN

ANALISIS SEGMENTASI VLAN TERHADAP KEAMANAN JARINGAN MENGGUNAKAN METODE CIA TRIAD

Oleh

M.Hajaji Alfarizi

162022075

Menyetujui,

Pembimbing Utama	Pembimbing Pendamping
Assoc. Prof. Dr.Ir. Zulhipni Reno S E, S.T., M.Kom	**Muhammad Ihsan, S. T., M. Kom**
NBM/NIDN: 1338529/0205118002	**NBM/NIDN: 1399825/0207129001**

~~Disetujui.~~
Dekan Fakultas Teknik

Ir. A. Junaidi, M.T
NBM/NIDN: 763050/0202026502

Program Studi Teknologi Informasi
Ketua Program Studi

Dr. Kamadi, S.Kom., M.Kom
NBM/NIDN: 1088893/0212059002

HALAMAN PERSETUJUAN

Judul Skripsi : Analisis Segmentasi Vlan Terhadap Keamanan Jaringan Menggunakan Metode Cia Triad

Oleh **M. Hajaji Alfarizi** NIM **162022075** Skripsi ini telah disetujui dan disahkan oleh Tim Penguji Program Studi Teknologi Informasi Konsentrasi Manajemen Tata Kelola Program Strata 1 Universitas Muhammadiyah Palembang pada 22 Agustus 2026 dan telah Dinyatakan Lulus

Palembang, 22 Agustus 2026

Mengetahui,

Ketua Program Studi Teknologi Informasi
Universitas Muhammadiyah Palembang

Dr. Karnadi, S. Kom., M. Kom
NBM/NIDN: 1088893/0210038202

Tim Penguji

Ketua Penguji

Assoc. Prof. Dr.Ir. Zulhipni Reno S E, S.T., M.Kom
NBM/NIDN: 1338529/0205118002

Penguji 1,

Apriansyah, S.Kom., M.Kom
NBM/NIDN: 1339399/0204049001

Penguji 2,

Dr. Karnadi, S. Kom., M. Kom
NBM/NIDN: 1088893/0210038202

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : M. Hajaji Alfarizi

NIM : 162022075

Fakultas/Prodi : Teknik / Teknologi Informasi

Judul Skripsi : Analisis Segmentasi VLAN Terhadap Keamanan Jaringan Menggunakan Metode CIA Triad

Menyatakan dengan sebenar-benarnya bahwa skripsi ini adalah benar-benar hasil karya asli saya sendiri dan bukan merupakan plagiarisme, pencurian hasil karya milik orang lain, hasil kerja orang lain untuk kepentingan saya karena hubungan material maupun non-material, ataupun segala kemungkinan lain yang pada hakekatnya bukan merupakan karya tulis skripsi saya secara orisinil dan otentik.

Bila dikemudian hari diduga kuat ada ketidaksesuaian antara fakta dengan kenyataan ini, saya bersedia diproses oleh tim Fakultas yang dibentuk untuk melakukan verifikasi, dengan sanksi terberat berupa pembatalan kelulusan/kesarjanaan.

Demikian surat pernyataan ini saya buat dengan kesadaran sendiri dan tidak atas tekanan ataupun paksaan dari pihak manapun demi menegakan integritas akademik di institusi ini.

Hormat Saya,



M. Hajaji Alfarizi

162022075

MOTTO DAN PERSEMBAHAN

MOTTO

*"*Ibu mempertaruhkan hidupnya agar aku bisa melihat dunia, ayah mengorbankan tenaganya agar aku bisa menggapai mimpi. Tugasku adalah memastikan tidak ada satu pun pengorbanan mereka yang sia-sia*"*

PERSEMBAHAN

Dengan penuh rasa syukur atas segala nikmat dan kekuatan yang diberikan serta dengan segala kerendahan hati, izinkan penulis untuk mempersembahkan skripsi ini kepada:

1. Kedua orang tua tercinta, Bapak Samsul, S.Pd. dan Ibu Holilah, S.Pd. Terima kasih atas kasih sayang yang tidak pernah berkurang, doa yang selalu mengiringi setiap langkah, serta segala pengorbanan yang diberikan tanpa mengenal lelah. Setiap tetes keringat, setiap usaha, dan setiap doa yang dipanjatkan menjadi alasan terbesar bagi penulis untuk terus bangkit dan menyelesaikan perjalanan ini. Penulis menyadari bahwa tidak ada pencapaian yang mampu membalas seluruh cinta dan pengorbanan Ayah dan Ibu. Semoga skripsi ini menjadi salah satu wujud rasa syukur dan bakti yang dapat menghadirkan kebahagiaan serta kebanggaan bagi Ayah dan Ibu. Semoga Allah SWT senantiasa melimpahkan kesehatan, umur yang penuh berkah, serta kebahagiaan di setiap langkah kehidupan.
2. Kakak tercinta, Monalisa, Am.Keb. Terima kasih atas setiap perhatian, doa, motivasi, dan dukungan yang selalu diberikan. Terima kasih telah menjadi tempat berbagi cerita, memberikan semangat di saat penulis merasa lelah, dan selalu percaya bahwa setiap kesulitan akan berakhir dengan hasil yang baik. Semoga segala kebaikan yang telah diberikan

menjadi amal yang bernilai di sisi Allah SWT dan dibalas dengan keberkahan serta kesuksesan.

3. Dosen pembimbing skripsi, Bapak Assoc. Prof. Dr.Ir. Zulhipni Reno S E, S.T., M.Kom. selaku Dosen Pembimbing Utama dan Bapak Muhammad Ihsan, S. T., M. Kom. selaku Dosen Pembimbing Pendamping. Dengan penuh rasa hormat dan ketulusan, penulis mengucapkan terima kasih atas segala bimbingan, ilmu, arahan, kritik, saran, serta kesabaran yang telah diberikan selama proses penyusunan skripsi ini. Setiap masukan yang diberikan menjadi bekal berharga bagi penulis, tidak hanya dalam menyelesaikan penelitian ini, tetapi juga sebagai pelajaran dalam menjalani kehidupan akademik dan profesional. Semoga Allah SWT membalas setiap kebaikan dan dedikasi Bapak/Ibu dengan pahala yang berlimpah.
4. Sahabat dan teman-teman seperjuangan, M Aidil Hutamam Aji, Agestya Prabu Marsyadi, Ronaldo Julian PK, Syahrul Arya Ramadhan. Terima kasih telah menjadi bagian dari perjalanan yang penuh cerita, memberikan dukungan, semangat, bantuan, dan kebersamaan yang begitu berarti. Terima kasih atas setiap tawa, diskusi, kerja sama, dan kenangan yang akan selalu menjadi bagian indah dalam perjalanan hidup penulis. Semoga persahabatan ini tetap terjaga dan semoga kita semua dipertemukan kembali dalam keadaan terbaik dengan kesuksesan yang telah diraih masing-masing.
5. Seluruh keluarga besar, terima kasih atas doa, perhatian, kasih sayang, serta dukungan yang tidak pernah putus. Kehangatan keluarga menjadi sumber kekuatan bagi penulis untuk terus melangkah dan menyelesaikan setiap proses yang dihadapi. Semoga Allah SWT senantiasa memberikan rahmat, kesehatan, dan keberkahan kepada seluruh keluarga.
6. Seluruh teman-teman Angkatan 2022 Program Studi Teknologi Informasi. Terima kasih atas kebersamaan, kerja sama, pengalaman, dan kenangan yang telah kita lalui bersama sejak awal perkuliahan hingga akhirnya dapat menyelesaikan perjalanan akademik ini. Semoga setiap

langkah yang kita tempuh setelah ini dipenuhi keberhasilan, kebahagiaan, dan keberkahan

7. Almamater tercinta, Terima kasih telah menjadi tempat penulis belajar, bertumbuh, dan mengembangkan ilmu pengetahuan serta karakter. Semoga almamater senantiasa menjadi institusi yang melahirkan generasi-generasi unggul yang mampu memberikan manfaat bagi masyarakat, bangsa, dan negara.
8. Terakhir, kepada diri sendiri, Muhammad Hajaji Alfarizi. Terima kasih karena telah memilih untuk tetap bertahan, terus berjuang, dan tidak menyerah meskipun perjalanan ini dipenuhi berbagai tantangan, kegagalan, dan rasa lelah. Terima kasih telah percaya bahwa setiap usaha yang dilakukan dengan doa, kesabaran, dan kerja keras akan menemukan hasil terbaik pada waktunya. Skripsi ini bukanlah akhir dari perjalanan, melainkan awal dari langkah baru untuk terus belajar, berkembang, dan memberikan manfaat bagi banyak orang. Semoga setiap mimpi yang telah diperjuangkan dapat diwujudkan dengan penuh keberkahan dan menjadi jalan untuk membanggakan keluarga serta memberikan manfaat bagi sesama.

ABSTRAK

Keamanan jaringan merupakan aspek penting dalam pengelolaan infrastruktur teknologi informasi, khususnya pada lingkungan kampus yang memiliki banyak pengguna dan perangkat yang saling terhubung. Jaringan yang tidak tersegmentasi dapat menempatkan perangkat dalam satu *broadcast domain* sehingga lalu lintas jaringan lebih mudah diamati oleh pihak yang tidak berwenang. Penelitian ini bertujuan menganalisis pengaruh segmentasi *Virtual Local Area Network* (VLAN) terhadap keamanan jaringan berdasarkan aspek *Confidentiality, Integrity,* dan *Availability* (CIA Triad), serta efektivitasnya dalam membatasi lalu lintas dan meningkatkan isolasi komunikasi antar host. Penelitian menggunakan metode kuantitatif dengan pendekatan eksperimen melalui simulasi jaringan menggunakan GNS3. Pengujian dilakukan dengan membandingkan kondisi sebelum dan sesudah segmentasi VLAN melalui pengujian konektivitas dan analisis *packet capture* menggunakan Wireshark. Hasil penelitian menunjukkan bahwa sebelum segmentasi, host attacker berada pada subnet dan *broadcast domain* yang sama sehingga dapat mengamati lalu lintas jaringan. Setelah segmentasi, host attacker dipindahkan ke subnet berbeda sehingga akses terhadap lalu lintas pada segmen utama menjadi lebih terbatas dan isolasi komunikasi meningkat. Berdasarkan analisis CIA Triad, segmentasi VLAN memberikan pengaruh positif terhadap *Confidentiality*, mendukung *Integrity* melalui isolasi komunikasi antarsegmen, serta mempertahankan *Availability*. Faktor teknis yang berkontribusi meliputi pemisahan subnet, *broadcast domain*, dan penempatan host attacker pada segmen berbeda.

KATA KUNCI: *VLAN*, Keamanan Jaringan, CIA Triad, Segmentasi Jaringan*, Wireshark.*

ABSTRACT

Network security is an important aspect of information technology infrastructure management, particularly in campus environments with many interconnected users and devices. An unsegmented network may place devices within the same broadcast domain, making network traffic more accessible to unauthorized parties. This study aims to analyze the effect of Virtual Local Area Network (VLAN) segmentation on network security based on Confidentiality, Integrity, and Availability (CIA Triad), as well as its effectiveness in limiting network traffic and improving communication isolation between hosts. The study employed a quantitative experimental approach using network simulation in GNS3. Testing was conducted by comparing network conditions before and after VLAN segmentation through connectivity testing and packet capture analysis using Wireshark. The results showed that before segmentation, the attacker host was in the same subnet and broadcast domain and could observe network traffic. After segmentation, the attacker host was placed in a different subnet, limiting access to traffic on the main segment and improving communication isolation. Based on the CIA Triad analysis, VLAN segmentation positively affected Confidentiality by limiting traffic access, supported Integrity through improved communication isolation between segments, and maintained Availability because communication within each segment continued to operate properly. The contributing technical factors included subnet separation, broadcast domain separation, and placement of the attacker host in a different network segment.

Keywords: *VLAN, Network Security, CIA Triad, Network Segmentation, Wireshark.*

KATA PENGANTAR

Alhamdulillahirabbil'alamin, puji syukur penulis panjatkan ke hadirat Allah SWT yang telah memberikan rahmat, hidayah, dan karunia-Nya, sehingga penyusunan skripsi ini dapat diselesaikan dengan baik dan tepat pada waktu yang telah ditentukan. Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer (S.Kom.) pada Program Studi Teknologi Informasi Fakultas Teknik Universitas Muhammadiyah Palembang.

Pada kesempatan ini penulis mengucapkan terima kasih kepada pihak-pihak yang telah membantu dalam pelaksanaan dan penyusunan skripsi diantaranya:

1. Bapak Prof. Dr. Abid Djazuli, S.E., M.M. selaku Rektor Universitas Muhammadiyah Palembang.
2. Bapak Ir. A. Junaidi, M.T. selaku Dekan Fakultas Teknik Universitas Muhammadiyah Palembang.
3. Bapak Dr. Karnadi, S.Kom., M.Kom. selaku Ketua Program Studi Teknologi Informasi.
4. Bapak Assoc. Prof. Dr.Ir. Zulhipni Reno S E, S.T., M.Kom selaku Dosen Pembimbing Utama.
5. Bapak Muhammad Ihsan, S. T.,M. Kom. selaku Dosen Pembimbing Pendamping.
6. Bapak / Ibu Dosen dan Staff Program Studi Teknologi Informasi.

Penulis menyadari keterbatasan kemampuan yang dimiliki, karena itu kritik dan saran yang membangun dari berbagai pihak sangat dibutuhkan untuk perbaikan dan kesempurnaan skripsi ini.

Palembang, 12 Agustus 2026

M. Hajaji Alfarizi
162022075

DAFTAR ISI

HALAMAN JUDUL ..... **i**
HALAMAN PENGESAHAN ..... **ii**
HALAMAN PERSETUJUAN ..... **iii**
HALAMAN PERNYATAAN ..... **iv**
MOTTO DAN PERSEMBAHAN ..... **v**
ABSTRAK ..... **viii**
ABSTRACT ..... **ix**
KATA PENGANTAR ..... **x**
DAFTAR ISI ..... **xi**
DAFTAR GAMBAR ..... **xiv**
DAFTAR TABEL ..... **xv**
BAB I PENDAHULUAN **1**
1.1 Latar Belakang 1
1.2 Identifikasi Masalah 6
1.3 Rumusan Masalah 7
1.4 Batasan Penelitian 7
1.5 Tujuan Penelitian 8
1.6 Manfaat Penelitian 9
1.7 Sistematika Penulisan 9
BAB II TINJAUAN PUSTAKA **11**
2.1 Jaringan Komputer 11
2.2 Local Area Network (LAN) 12
2.3 Virtual Local Area Network (VLAN) 12
2.4 Segmentasi Jaringan 13
2.5 Keamanan Jaringan 14
2.6 *CIA Triad* 15
2.6.1 *Confidentiality* 17
2.6.2 *Integrity* 17
2.6.3 *Availability* 18
2.7 Parameter CIA Triad dalam Analisis Keamanan Jaringan 19

2.7.1 Parameter *Confidentiality*.....20
2.7.2 Parameter *Integrity*.....20
2.7.3 Parameter *Availability*.....21
2.8 Hubungan Segmentasi VLAN terhadap CIA Triad 22
2.9 *State Of The Art* dan Keterbaruan.....24
BAB III METODOLOGI PENELITIAN 31
3.1 Jenis Penelitian.....31
3.2 Waktu dan Tempat Penelitian.....31
3.2.1 Tempat Penelitian.....31
3.2.2 Jadwal Penelitian.....32
3.3 Kerangka Penelitian 34
3.4 Metode Pengumpulan Data 37
3.4.1 Studi Dokumentasi dan Literatur 38
3.4.2 Eksperimen Jaringan Menggunakan Simulasi 38
3.4.3 Pengambilan Data Lalu Lintas Jaringan.....39
3.4.4 Pengumpulan Data Performa Jaringan.....39
3.5 Metode Penelitian.....39
3.6 Metode Analisis Data.....45
3.6.1 Analisis *Confidentiality*.....45
3.6.2 Analisis *Integrity*.....46
3.6.3 Analisis *Availability*.....47
3.7 Tahapan Penelitian.....48
3.7.1 Identifikasi Masalah.....49
3.7.2 Studi Literatur 50
3.7.3 Perancangan Topologi Jaringan 51
3.7.4 Implementasi Segmentasi VLAN.....51
3.7.5 Pengujian Keamanan Jaringan 52
3.7.6 Analisis Data Berdasarkan CIA Triad.....53
3.7.7 Penarikan Kesimpulan dan Penyusunan Laporan.....54
BAB IV HASIL DAN PEMBAHASAN.....55
4.1 Gambaran Umum Jaringan Kampus 55
4.2 Topologi Simulasi Penelitian 57

4.2.1 Perangkat yang Digunakan.....59
4.2.2 Konfigurasi Alamat IP 60
4.2.3 Pengujian Konektivitas Jaringan.....60
4.3 Pengujian Jaringan Sebelum Segmentasi.....61
4.3.1 Konfigurasi Jaringan Sebelum Segmentasi.....62
4.3.2 Pengujian Konektivitas Jaringan.....62
4.3.3 Pengujian *Packet Sniffing* Menggunakan Wireshark.....63
4.3.4 Analisis Hasil Pengujian Sebelum Segmentasi.....64
4.4 Pengujian Jaringan Setelah Segmentasi.....65
4.4.1 Konfigurasi Segmentasi Jaringan.....66
4.4.2 Pengujian Packet *Capture* Setelah Segmentasi.....69
4.4.3 Analisis Hasil Pengujian Setelah Segmentasi.....71
4.5 Analisis Keamanan berdasarkan CIA Triad.....72
4.5.1 Analisis *Confidentiality*.....72
4.5.2 Analisis *Integrity*.....75
4.5.3 Analisis *Availability*.....77
4.5.4 Perbandingan Hasil Pengujian 79
4.5.5 Analisis Perbandingan Hasil Pengujian 81
BAB V KESIMPULAN DAN SARAN 84
5.1 Kesimpulan 84
5.2 Saran.....85
DAFTAR PUSTAKA
LAMPIRAN

DAFTAR GAMBAR

Gambar 2. 1 CIA Kerangka Evaluasi Keamanan.....16
Gambar 3. 1 Lokasi Penelitian.....32
Gambar 3. 2 Kerangka Penelitian.....35
Gambar 4. 1 Topologi Jaringan Universitas Muhammadiyah Palembang.....57
Gambar 4. 2 Topologi Simulasi Penelitian.....59
Gambar 4. 3 IP Mahasiswa dan *Attacker*.....62
Gambar 4. 4 Hasil Pengujian Ping Sebelum Segmentasi.....63
Gambar 4. 5 Hasil Capture Wireshark Sebelum Segmentasi.....64
Gambar 4. 6 Konfigurasi Segmentasi Jaringan.....67
Gambar 4. 7 Konfigurasi Alamat IP Host Attacker Setelah Segmentasi.....68
Gambar 4. 8 Hasil *Capture* Wireshark Setelah Segmentasi.....70

DAFTAR TABEL

Tabel 2. 1 State Of The Art 24
Tabel 3. 1 Jadwal Penelitian.....33
Tabel 3. 2 Metode Penelitian.....43
Tabel 4. 1 Perangkat yang digunakan.....60
Tabel 4. 2 Konfigurasi IP 60
Tabel 4. 3 Jaringan Sebelum Segmentasi 62
Tabel 4. 4 Jaringan Setelah Segmentasi 68
Tabel 4. 5 Hasil Pengujian Confidentiality 74
Tabel 4. 6 Hasil Pengujian Integrity.....77
Tabel 4. 7 Hasil Pengujian Availability 79
Tabel 4. 8 Perbandingan Pengujian.....81
Tabel 4. 9 Analisis Perbandingan Hasil Uji 82

BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan jaringan menjadi salah satu aspek paling krusial dalam pengelolaan infrastruktur teknologi informasi pada organisasi, institusi pendidikan, dan perusahaan. Dalam sistem informasi modern, jaringan komputer berperan sebagai tulang punggung utama dalam pertukaran data, komunikasi internal, serta penyediaan layanan berbasis digital. Ketergantungan yang tinggi terhadap jaringan komputer menyebabkan kebutuhan akan keamanan jaringan menjadi semakin mendesak. Lingkungan jaringan lokal (Local Area Network/LAN) sering menjadi target serangan karena sifatnya yang saling terhubung dan sering kali tidak dilengkapi mekanisme segmentasi yang memadai. Ketika seluruh perangkat berada dalam domain broadcast yang sama, setiap paket data yang dikirimkan berpotensi dapat diamati oleh pihak yang tidak berwenang melalui aktivitas *Packet Sniffing* dan pemantauan lalu lintas jaringan [1].

Ketika jaringan tidak tersegmentasi, lalu lintas data berjalan melalui jalur yang sama sehingga data sensitif seperti kredensial login, data sistem, hingga informasi pribadi pengguna dapat terekspos. Kondisi ini tidak hanya menurunkan tingkat keamanan, tetapi juga mengurangi kualitas layanan jaringan. Serangan terhadap domain broadcast tunggal dapat menyebabkan penurunan performa, meningkatnya risiko manipulasi data, hingga pencurian informasi dalam jumlah besar. Pada beberapa kasus, satu perangkat yang terinfeksi malware dapat menyebarkan serangan ke seluruh jaringan tanpa hambatan karena tidak adanya pemisahan logis

antarbagian jaringan [2] Oleh karena itu, metode segmentasi menjadi kebutuhan mendasar dalam arsitektur jaringan modern.

Salah satu metode segmentasi yang paling luas digunakan adalah *Virtual Local Area Network* (VLAN). Pada penerapannya, *Virtual Local Area Network* (VLAN) memungkinkan perangkat dikelompokkan secara logis ke dalam jaringan yang berbeda meskipun menggunakan infrastruktur fisik yang sama. Setiap VLAN memiliki domain broadcast tersendiri sehingga lalu lintas broadcast dari suatu segmen tidak secara langsung tersebar ke segmen lainnya. Kondisi tersebut dapat meningkatkan isolasi komunikasi antar host dan membatasi visibilitas lalu lintas jaringan, sehingga segmentasi VLAN dapat menjadi salah satu mekanisme pendukung dalam meningkatkan keamanan jaringan. VLAN memungkinkan pemisahan jaringan berdasarkan kebutuhan organisasi tanpa harus memisahkan perangkat secara fisik. Melalui VLAN, lalu lintas jaringan dapat diisolasi sehingga setiap segmen bekerja secara terpisah. Segmentasi ini mampu mengurangi domain broadcast dan mencegah perangkat dari segmen lain untuk mengakses trafik yang tidak relevan. Penerapan VLAN memberikan beberapa manfaat seperti peningkatan efisiensi jaringan, kemudahan manajemen, serta peningkatan keamanan melalui isolasi trafik [3]. Hasil penelitian sebelumnya menunjukkan bahwa VLAN dapat membatasi penyebaran broadcast, mengurangi konsumsi bandwidth, serta mengurangi risiko penyadapan trafik dalam jaringan [4].

Pada sejumlah kasus implementasi, VLAN juga terbukti meningkatkan stabilitas dan kinerja layanan jaringan di lingkungan pendidikan dan pemerintahan. Misalnya, segmentasi VLAN pada jaringan sistem informasi pendidikan terbukti

mampu menurunkan risiko kebocoran data dan menstabilkan konektivitas aplikasi yang membutuhkan komunikasi aman antarserver dan klien [5]. Hal ini menunjukkan bahwa segmentasi VLAN bukan sekadar metode pengelolaan jaringan, tetapi juga solusi keamanan yang dapat memberikan dampak signifikan terhadap kualitas layanan.

Meskipun demikian, efektivitas VLAN dalam meningkatkan keamanan jaringan tidak terlepas dari konfigurasi yang diterapkan. Banyak serangan yang ternyata masih mampu menembus segmentasi VLAN apabila konfigurasi switch tidak dilakukan dengan benar. Kerentanan seperti VLAN hopping, double tagging, dan serangan berbasis trunk port dapat terjadi ketika pengaturan native VLAN dibiarkan default atau ketika trunking tidak dibatasi dengan ketat [6]. Selain itu, VLAN yang tidak dilengkapi dengan kebijakan keamanan tambahan seperti Access Control List (ACL), DHCP filtering, atau port security masih rentan terhadap berbagai bentuk akses tidak sah dan penyalahgunaan lalu lintas jaringan [7]. Artinya, segmentasi VLAN hanya akan efektif apabila dikombinasikan dengan kebijakan keamanan yang tepat dan diuji menggunakan analisis yang mendalam.

Untuk dapat menilai tingkat keamanan jaringan secara menyeluruh setelah implementasi VLAN, dibutuhkan sebuah model evaluasi yang mampu mengukur aspek penting dalam keamanan jaringan. CIA Triad, yang terdiri dari *Confidentiality, Integrity*, dan *Availability*, adalah model yang paling banyak digunakan dalam analisis keamanan sistem informasi. CIA Triad merupakan kerangka dasar keamanan informasi yang mencakup tiga aspek utama, yaitu *Confidentiality* yang berkaitan dengan perlindungan informasi dari akses yang tidak

berwenang, *Integrity* yang berkaitan dengan menjaga informasi agar tetap akurat dan tidak mengalami perubahan yang tidak sah, serta *Availability* yang berkaitan dengan memastikan informasi dan layanan tetap tersedia ketika dibutuhkan CIA Triad memberikan gambaran mengenai bagaimana jaringan mempertahankan kerahasiaan data dari penyadapan, menjaga integritas data dari upaya manipulasi, serta memastikan ketersediaan layanan ketika terjadi beban tinggi atau gangguan teknis [23]. Model ini sangat relevan diterapkan dalam penelitian keamanan jaringan karena dapat memberikan pengukuran terstandarisasi berdasarkan Indikator yang terukur. Namun, sebagian besar penelitian yang telah dilakukan terkait VLAN tidak secara khusus menggunakan kerangka CIA Triad dalam mengukur keamanan jaringan. Penelitian sebelumnya banyak berfokus pada peningkatan performa jaringan, manajemen trafik, dan efisiensi penggunaan perangkat, tetapi belum melakukan evaluasi keamanan yang komprehensif dengan pendekatan terukur. Studi yang membahas aspek keamanan umumnya bersifat konseptual atau terbatas pada simulasi konfigurasi tanpa melakukan analisis lalu lintas jaringan secara mendalam menggunakan pendekatan keamanan yang terukur [9]. Ini menunjukkan adanya celah penelitian (research gap) yang penting untuk diisi.

Melihat berbagai fenomena dan temuan tersebut, penelitian ini menjadi semakin relevan karena menggabungkan implementasi segmentasi VLAN dengan evaluasi keamanan jaringan menggunakan metode CIA Triad. Penelitian ini tidak hanya menerapkan VLAN dalam jaringan lokal, tetapi juga melakukan analisis lalu lintas jaringan menggunakan Wireshark melalui proses *packet capture* sebelum dan

sesudah segmentasi jaringan diterapkan. Dengan demikian, penelitian ini memberikan kontribusi dalam bentuk analisis kuantitatif yang mengukur pengaruh segmentasi VLAN terhadap aspek *Confidentiality*, *Integrity*, dan *Availability* secara menyeluruh. Dengan demikian, penelitian ini memberikan kontribusi baru dalam bentuk analisis kuantitatif yang mengukur dampak segmentasi VLAN terhadap aspek *Confidentiality*, *Integrity*, dan *Availability* secara menyeluruh. Hasil dari penelitian ini diharapkan memberikan pemahaman lebih mendalam mengenai sejauh mana segmentasi VLAN dapat meningkatkan keamanan jaringan, faktor-faktor konfigurasi apa saja yang memengaruhinya, serta bagaimana organisasi dapat menerapkan segmentasi yang lebih efektif untuk melindungi layanan jaringan mereka. Selain itu, penelitian ini juga dapat menjadi referensi bagi institusi pendidikan maupun organisasi yang ingin mengembangkan kebijakan keamanan jaringan berbasis segmentasi.

Berdasarkan uraian permasalahan, penelitian terdahulu, dan celah penelitian yang telah diidentifikasi, diperlukan penelitian yang secara khusus menganalisis pengaruh segmentasi *Virtual Local Area Network (VLAN)* terhadap keamanan jaringan pada lingkungan Universitas Muhammadiyah Palembang. Penelitian ini dilakukan dengan membandingkan kondisi jaringan sebelum dan sesudah penerapan segmentasi VLAN melalui analisis packet *capture* menggunakan Wireshark, kemudian mengevaluasi perubahan keamanan jaringan berdasarkan aspek *Confidentiality*, *Integrity*, dan *Availability* (CIA Triad). Pemilihan pendekatan tersebut diharapkan dapat memberikan gambaran yang terukur mengenai pengaruh segmentasi VLAN terhadap keamanan jaringan dan

efektivitasnya dalam meningkatkan isolasi komunikasi antar host. Berdasarkan permasalahan dan pendekatan yang digunakan tersebut, penelitian ini diangkat dengan judul "Analisis Segmentasi VLAN terhadap Keamanan Jaringan Menggunakan Metode CIA Triad"

1.2 Identifikasi Masalah

Berdasarkan latar belakang di atas, dapat diidentifikasi beberapa permasalahan yang masih dihadapi, antara lain:

1. Belum diketahui secara terukur pengaruh penerapan segmentasi VLAN terhadap tingkat keamanan jaringan berdasarkan aspek *Confidentiality, Integrity, dan Availability* (CIA Triad).
2. Belum diketahui secara jelas sejauh mana penerapan segmentasi VLAN mampu membatasi lalu lintas jaringan dan meningkatkan isolasi komunikasi antar host berdasarkan hasil analisis *packet capture* menggunakan Wireshark.
3. Belum teridentifikasi secara menyeluruh faktor-faktor yang memengaruhi peningkatan keamanan jaringan setelah penerapan segmentasi VLAN serta bagaimana hasil evaluasi tersebut dapat digunakan sebagai dasar dalam penyusunan model evaluasi keamanan jaringan.

Berdasarkan uraian tersebut, dapat disimpulkan bahwa permasalahan utama dalam penelitian ini terletak pada belum optimalnya pemanfaatan segmentasi VLAN dalam meningkatkan keamanan jaringan pada Universitas Muhammadiyah Palembang. Selain itu, belum adanya pengukuran keamanan jaringan menggunakan

pendekatan CIA Triad menyebabkan tingkat keamanan jaringan belum dapat dievaluasi secara terukur. Di sisi lain, masih belum diketahui secara jelas sejauh mana segmentasi VLAN mampu membatasi lalu lintas jaringan, mengurangi penyebaran broadcast, serta meningkatkan isolasi komunikasi antar perangkat sehingga diperlukan penelitian yang mampu menganalisis dan mengevaluasi keamanan jaringan berbasis VLAN secara kuantitatif dan sistematis.

1.3 Rumusan Masalah

1. Bagaimana pengaruh penerapan segmentasi Virtual Local Area Network (VLAN) terhadap tingkat keamanan jaringan berdasarkan aspek *Confidentiality, Integrity,* dan *Availability* (CIA Triad)?
2. Sejauh mana penerapan segmentasi VLAN mampu membatasi lalu lintas jaringan dan meningkatkan isolasi komunikasi antar *host* berdasarkan hasil analisis *packet capture* menggunakan Wireshark?
3. Faktor-faktor apa saja yang memengaruhi peningkatan keamanan jaringan setelah penerapan segmentasi VLAN serta bagaimana hasil evaluasi tersebut dapat digunakan sebagai dasar dalam penyusunan model evaluasi keamanan jaringan?

1.4 Batasan Penelitian

Agar penelitian lebih terarah dan tidak menyimpang dari tujuan yang telah ditentukan, maka penelitian ini memiliki beberapa batasan sebagai berikut:

1. Penelitian difokuskan pada analisis pengaruh segmentasi *Virtual Local Area Network* (VLAN) terhadap keamanan jaringan.

2. Penelitian dilakukan menggunakan simulasi jaringan berbasis GNS3 dan tidak diterapkan secara langsung pada jaringan produksi di lingkungan Universitas Muhammadiyah Palembang.
3. Pengujian keamanan jaringan dilakukan melalui analisis lalu lintas jaringan *(packet capture)* menggunakan Wireshark untuk membandingkan kondisi jaringan sebelum dan sesudah penerapan segmentasi VLAN.
4. Analisis keamanan jaringan dilakukan menggunakan pendekatan CIA Triad yang meliputi aspek *Confidentiality, Integrity,* dan *Availability.*
5. Perangkat jaringan yang digunakan dalam simulasi terdiri dari Open vSwitch, beberapa host pengguna yang mewakili server, staf, dan mahasiswa, serta satu host *attacker.*
6. Penelitian tidak membahas mekanisme keamanan jaringan lainnya seperti *Intrusion Detection System* (IDS), *Virtual Private Network* (VPN), *firewall* tingkat lanjut, maupun teknik enkripsi data.

1.5 Tujuan Penelitian

1. Menganalisis pengaruh penerapan segmentasi Virtual Local Area Network (VLAN) terhadap tingkat keamanan jaringan berdasarkan aspek *Confidentiality, Integrity,* dan *Availability* (CIA Triad).
2. Menganalisis efektivitas penerapan segmentasi VLAN dalam membatasi lalu lintas jaringan dan meningkatkan isolasi komunikasi antar *host* berdasarkan hasil analisis *packet capture* menggunakan Wireshark.
3. Mengidentifikasi faktor-faktor yang memengaruhi peningkatan keamanan jaringan setelah penerapan segmentasi VLAN serta menyusun model

evaluasi keamanan jaringan berdasarkan hasil penelitian.

1.6 Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini adalah sebagai berikut:

1. Memberikan pemahaman mengenai pengaruh penerapan segmentasi Virtual Local Area Network (VLAN) terhadap tingkat keamanan jaringan berdasarkan aspek *Confidentiality, Integrity,* dan *Availability* (CIA Triad) pada lingkungan kampus.
2. Memberikan gambaran mengenai efektivitas segmentasi VLAN dalam membatasi lalu lintas jaringan dan meningkatkan isolasi komunikasi antar host berdasarkan hasil analisis packet capture menggunakan Wireshark.
3. Memberikan informasi mengenai faktor-faktor yang memengaruhi peningkatan keamanan jaringan setelah penerapan segmentasi VLAN serta menyediakan model evaluasi keamanan jaringan yang dapat menjadi bahan pertimbangan dalam pengembangan dan pengelolaan keamanan jaringan.
4. Menjadi referensi bagi institusi pendidikan maupun peneliti selanjutnya dalam pengembangan dan pengelolaan keamanan jaringan berbasis segmentasi VLAN

1.7 Sistematika Penulisan

penulisan dalam penelitian ini disusun untuk mempermudah pembahasan serta memberikan gambaran umum mengenai isi penelitian. Adapun sistematika penulisan penelitian ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi latar belakang, identifikasi masalah, rumusan masalah, batasan penelitian, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini membahas landasan teori yang berkaitan dengan jaringan komputer, VLAN, keamanan jaringan, CIA Triad, penelitian terdahulu (*State Of The Art*), novelty penelitian, serta kerangka penelitian.

BAB III METODE PENELITIAN

Bab ini berisi metode penelitian, metode pengumpulan data, perancangan topologi jaringan, tahapan implementasi VLAN, serta metode pengujian keamanan jaringan.

BAB IV HASIL DAN PEMBAHASAN

Bab ini membahas hasil implementasi jaringan, hasil pengujian sebelum dan sesudah penerapan VLAN, analisis keamanan jaringan berdasarkan CIA Triad, serta pembahasan hasil penelitian.

BAB V PENUTUP

Bab ini berisi kesimpulan dari hasil penelitian yang telah dilakukan serta saran untuk pengembangan penelitian selanjutnya.

DAFTAR PUSTAKA

[1] K. Y. J. Ndun, "Penerapan VLAN untuk Meningkatkan Keamanan dan Efisiensi Jaringan Aplikasi Dapodik di SDN Oesusu," *Jurnal Teknik Unila*, 2025. https://journal.eng.unila.ac.id/index.php/jitet/article/view/6851

[2] Fatkhurrahman dan Witanti, "Optimasi Segmentasi Jaringan melalui Implementasi VLAN Dinamis dengan MikroTik," *Jurnal JEKIN*, 2024. https://rumahjurnal.or.id/index.php/JEKIN/article/view/904

[3] Fuji dan Jarti, "Pengaruh Penggunaan VLAN terhadap Efisiensi dan Keamanan Jaringan Lokal (LAN)," *Jurnal Tambora*, 2024. https://jurnal.uts.ac.id/index.php/Tambora/article/view/6845

[4] Agustio dan Nainggolan, "Penerapan VLAN pada Jaringan MAN dengan ACL Filtering," *Jurnal Keamanan Aplikasi*, 2023. https://ejournal.mediaantartika.id/index.php/jka/article/view/5

[5] Ramadhan dan Junaidi, "Perancangan Jaringan VLAN SMA Fatahillah," *Jurnal BSI*, 2023. https://jurnal.bsi.ac.id/index.php/conten/article/view/4909

[6] Marsehan et al., "Perancangan Jaringan VLAN di SMK Pertanian Negeri 2 Tugumulyo," *Digitech Journal*, 2025. https://jurnal.itscience.org/index.php/digitech/article/view/5891

[7] Djumhadi et al., "VLAN sebagai Media Keamanan Isolasi Jaringan di SMKN 6 Balikpapan," *Jurnal SINERGI*, 2024. https://manggalajournal.org/index.php/SINERGI/article/view/39

[8] Rahman, "Implementasi VLAN dan Firewall pada MikroTik dan Switch," *JITK*, 2023. https://ejournal.nusamandiri.ac.id/index.php/jitk/article/view/315

[9] Fitriansyah et al., "Penerapan Static VLAN dan Access List untuk Meningkatkan Keamanan Jaringan," *JTIK*, 2024. https://journal.thamrin.ac.id/index.php/jtik/article/view/176

[10] Syarif et al., "Analisis dan Implementasi VLAN pada Laboratorium Teknik Informatika," *INOVA-TIF*, 2020.

https://ejournal.uikabogor.ac.id/index.php/INOVATIF/article/view/4065

[11] Yudanto et al., "Evaluasi Segmentasi VLAN dalam Optimalisasi Kinerja dan Keamanan LAN," *J-ILKOMINFO*, 2025. https://www.jilkominfo.org/index.php/ejournalaikom/article/download/313/97

[12] V. Zaizafun dan M. Syahroni, "Perancangan dan Implementasi *Virtual Local Area Network* (VLAN) Berbasis Switch Cisco 2960," *Jurnal LITEK*, 2024. https://ejournal.pnl.ac.id/index.php/litek/article/download/3/28/146

[13] R. Oktiana dan L. Widyawati, "Desain dan Implementasi VLAN untuk Manajemen Akses User pada Access Point Multi SSID," *Jurnal Teknologi, Kesehatan, dan Sosial*, 2025. https://journal.universitasbumigora.ac.id/juteks/article/view/5192

[14] A. D. Nugraha et al., "Analisis Keamanan Data terhadap Sniffing Menggunakan Serangan Man-in-the-Middle," *Jurnal Teknologi Rekayasa Informasi dan Komputer*, 2023. https://e-jurnal.pnl.ac.id/TRIK/article/view/4757

[15] F. W. Christanto et al., "Implementasi Keamanan Jaringan LAN Berbasis ACL dan VLAN," *Jurnal SISFOKOM*, 2022. https://jurnal.atmaluhur.ac.id/index.php/sisfokom/article/view/20

[16] Herman et al., "Analisis Keamanan Jaringan LAN terhadap Ancaman DDoS," *Jurnal Riset Komputer (JURIKOM)*, 2023. https://ejurnal.stmikbudidarma.ac.id/index.php/jurikom/article/view/583

[17] S. Sitohang dan H. Pangaribuan, "Analisis keamanan dan kinerja jaringan pada implementasi VLAN," *Jurnal Sains Informatika Terapan*, vol. 4, no. 2, 2025. https://doi.org/10.62357/jsit.v4i2.673

[18] M. A. Noval Bijaksa et al., "Analisis dan pengujian keamanan jaringan VLAN berbasis firewall security port," *RABIT: Jurnal Teknologi dan Sistem Informasi Univrab*, vol. 10, no. 2, 2025. https://jurnal.univrab.ac.id/index.php/rabit/article/view/6333

[19] H. Fuji dan A. Fuji, “Pengaruh penggunaan VLAN terhadap efisiensi dan keamanan jaringan lokal (LAN),” *Jurnal Tambora*, vol. 9, no. 3, 2025. https://jurnal.uts.ac.id/index.php/Tambora/article/view/6845

[20] M. Rahman dan M. Dasuki, “Implementasi Access Control List (ACL) sebagai metode proteksi dan traffic control pada infrastruktur jaringan LAN,” *Jurnal CoSciTech*, vol. 6, no. 1, 2025.

[21] S. Sayfudin, "Monitoring Jaringan Internet Kantor Pusat Administrasi Universitas Muhammadiyah Palembang," OKTAL: Jurnal Ilmu Komputer dan Science, vol. 2, no. 10, pp. 2593–2599, 2023. https://journal.mediapublikasi.id/index.php/oktal/article/view/3644

[22] M. A. Darmawan, "Analisis Keamanan Jaringan Terhadap Sniffing Menggunakan Wireshark dan Ettercap," JUST IT, 2024.

[23] J. Cawthra, M. Ekstrom, L. Lusty, J. Sexton, J. Sweetnam, and A. Townsend, “Data *Integrity*: Detecting and Responding to Ransomware and Other Destructive Events,” NIST Special Publication 1800-26A, National Institute of Standards and Technology, Gaithersburg, MD, USA, Dec. 2020, doi: 10.6028/NIST.SP.1800-26.

[24] A. S. Tanenbaum, N. Feamster, and D. J. Wetherall, *Computer Networks*, 6th ed. Pearson, 2021.

[25] H. Herdiansyah, T. U. Kalsum, and Rizka, “An Analysis and Implementation of Local Area Network (LAN) As Data Communication Media In Computer-Based Test at SMPN 19 of Central Bengkulu,” *Jurnal Komputer, Informasi dan Teknologi*, vol. 1, no. 2, pp. 180–186, 2021, doi: 10.53697/jkomitek.v1i2.221.

[26] IEEE, *IEEE Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks*, IEEE Std 802.1Q-2022, 2022.

[27] N. Mhaskar, M. Alabbad, and R. Khedri, “A Formal Approach to Network Segmentation,” *Computers & Security*, vol. 103, Art. no. 102162, 2021, doi: 10.1016/j.cose.2020.102162.

[28] D. Herrmann and H. Pridöhl, “Basic Concepts and Models of Cybersecurity,” in *The Ethics of Cybersecurity*. Cham, Switzerland: Springer, 2020, pp. 11–44, doi: 10.1007/978-3-030-29053-5_2.

[29] A. Anggraeni, J. G. A. Ginting, and S. Ikhwan, “Implementation of intrusion prevention system (IPS) to analysis triad CIA on network security attacks on web server,” *Jurnal Infotel*, vol. 14, no. 4, pp. 277–286, 2022, doi: 10.20895/infotel.v14i4.813.