PEMBANGUNAN SISTEM MONITORING *NETWORK SECURITY* MENGGUNAKAN *INTRUSION DETECTION SYSTEM* SNORT DENGAN LOG ANALISIS SPLUNK

(Studi Kasus : PT. H-One Kogi Prima Auto Technologies Indonesia)

TUGAS AKHIR

Disusun sebagai salah satu syarat untuk kelulusan Program Strata I.
Program Studi Teknik Informatika Universitas Pasundan Bandung

Disusun oleh :

Herdy Imam Febrianto
Nrp. 18.304.0108

POGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS PASUNDAN

BANDUNG

AGUSTUS 2022

LEMBAR PENGESAHAN

LAPORAN TUGAS AKHIR

Telah ditunjukan dan dipertahankan dalam Seminar Kualifikasi Penelitian Sarjana Program Studi Teknik Informatika Universitas Pasundan Bandung, pada hari dan tanggal seminar sesuai berita acara Seminar Kualifikasi Penelitian tugas akhir dari :

Nama : Herdy Imam Febrianto

NRP : 18.304.0108

Dengan Judul :

"Pembangunan Sistem Monitoring *Network Security* Menggunakan *Intrusion Detection System* Snort Dengan Log Analisis Splunk (Studi Kasus : PT. H-One Kogi Prima Auto Technologies Indonesia)"

Bandung, 31 Agustus 2022

Menyetujui,

Pembimbing Utama	Pembimbing Pendamping
(**Doddy Ferdiansyah, S.T., M.T**)	(**Miftahul Fadli Muttaqin, S.T., M.T**)

ABSTRAK

Kejahatan dunia siber di internet yang cepat meluas dikalangan saat ini dapat memasuki sebuah jaringan hingga merusak dan meretas sebuah sistem, menjadi permasalahan pada perusahaan maupun institusi dalam aspek keamanan informasi. Seringkali jaringan tersebut mengalami *down* pada pelayanan, dan pencurian informasi yang terjadi antara jaringan yang di susupi oleh peretas dengan metode pengujian yang beragam dilakukan oleh penyusup dan memungkinkan adanya penyusup yang mengakses informasi penting dalam perusahaan maupun institusi tersebut. Walau belum bisa dipastikan jaringan bermasalah dikarenakan kesalahan teknis.

Untuk itu pada penelitian ini penulis menawarkan sistem monitoring dalam pengamanan insiden jaringan menggunakan *Intrusion Detection System* (IDS) yang di integrasikan dengan manajemen log SIEM yang dilakukan pada mesin virtual di lingkungan jaringan internal server PT. H-One Kogi Prima Auto Technologies Indonesia, untuk dipasangkan di jaringan yang diperlukan dalam proses monitoring. IDS sendiri bertugas sebagai pengawas sistem yang akan melakukan identifikasi akses oleh siapa saja yang menggunakan sistem. Hal ini dapat membantu admin dalam mengamankan sebuah sistem dengan *rules* yang dapat di kostumasi serta konfigurasi sesuai kebutuhan proses monitoring dan direkam secara *real-time*

Kata kunci : IDS, Snort 3, SIEM, keamanan jaringan, *Splunk*

ABSTRACT

Cyber crimes on the internet that are rapidly expanding among today can enter a network to damage and hack a system, becoming a problem for companies and institutions in the aspect of information security. Often the network is down in service, and the theft of information that occurs between networks infiltrated by hackers with various testing methods is carried out by intruders and allows intruders to access important information within the company or institution. Although it is not certain that the network has problems due to technical errors.

For this reason, in this study the author offers a monitoring system in securing network incidents using an Intrusion Detection System (IDS) which is integrated with SIEM log management carried out on virtual machines in the PT. H-One Kogi Prima Auto Technologies Indonesia, to be installed in the network needed in the monitoring process. The IDS itself serves as a system supervisor who will identify access by anyone who uses the system. This can help admins in securing a system with rules that can be customized and configured according to the needs of the monitoring process and recorded in real-time.

Keywords: IDS, Snort 3, SIEM, network security, Splunk.

DAFTAR ISI

BAB I

PENDAHULUAN

Bab ini berisi penjelasan umum mengenai usulan yang dilakukan dalam pengerjaan tugas akhir. Didalam nya berisi latar belakang penelitian, identifikasi masalah, metodologi yang digunakan, lingkup, batasan, tujuan penelitian dan sistematika penulisan tugas akhir.

1.1. Latar Belakang

Sebuah jaringan komputer yang saling terhubung satu dengan perangkat lainnya dalam jaringan lokal, terdapat beberapa aktivitas yang tidak dapat diketahui oleh orang yang tidak memperhatikan hal tersebut, hal itu dapat dibocorkan oleh oknum *cyber crime* yang berhasil mengakses sumber yang tidak sah, melakukan kerusakan dijaringan dan mengambil data sensitif mengenai informasi penting, aset maupun layanan sebuah jaringan. Sistem keamanan yang menerapkan *firewall* tidaklah cukup untuk meminimalisir adanya sebuah serangan di jaringan yang dapat memantau adanya *traffic* anomali dari paket yang melintas di jaringan *internal* atau lokal disebuah perusahaan. Perlu adanya sebuah keamanan yang dapat mengeksekusi dan mengidentifikasi setiap bit didalam paket, analisa aktivitas mencurigakan dan memonitoring secara *real-time*. Maka perlu memerlukan sistem yang mendukung dalam keamanan sebuah jaringan dan dapat membantu pekerjaan administratif jaringan dalam melakukan kegiatan monitoring terhadap terjadinya insiden pada jaringan yaitu dengan sistem *Intrusion Detection System (IDS).*

Intrusion Detection System merupakan sistem keamanan jaringan yang dapat mendeteksi aktivitas mencurigakan pada sebuah paket dalam *traffic* di jaringan. secara umum IDS dibagi menjadi dua lingkup yakni sebagai *NIDS (Network Intrusion Detection System)* yaitu memonitoring dan mengidentifikasi paket yang mengalir di jaringan secara *Real-time* dan HIDS (*Host Intrusion Detection System*) yaitu memonitoring pada area *host* tertentu dan digunakan untuk memantau, mendeteksi, dan menganalisis peristiwa yang terjadi pada *host* tersebut. IDS menganalisa paket berdasarkan aturan atau *rules* yang ada untuk mengenali adanya *threat* dijaringan. Banyaknya pengujian dini yang mencoba masuk kedalam sistem tanpa sepengetahuan ataupun hak yang tidak memiliki izin untuk mengakses sumber daya, dengan solusi keamanan IDS yang terintegrasikan SIEM (*Security Information and Event Management*) akan membantu pencatatan *Anomaly Detection* secara terpusat dan proses dalam memberikan notifikasi dari insiden yang terjadi.

Pada penelitian penulis kali ini, akan membangun sistem yang di terapkan pada jaringan internal server PT. H-One Kogi Prima Auto Technologies Indonesia, hal ini belum ada penerapan keamanan pendeteksi sistem intrusi khusus seperti IDS pada jaringan kritikal server untuk mengidentifikasi beberapa aktivitas ancaman dini yang mencurigakan di tingkat jaringan internal dan tidak bisa di deteksi oleh sistem firewall atau memberikan alarm false negative pada *behavior* internal. kesalahan tersebut bisa berupa aturan yang belum *up-to-date* pada *vendor* firewall atau kurang nya pembuatan aturan yang spesifik di firewall. Oleh karena itu, pembangunan sistem ini dilakukan dapat mengetahui, menganalisa

dan mendeteksi *traffic* anomali ancaman dalam, melakukan penulisan aturan yang spesifik dan integrasi sistem IDS ke SIEM untuk memantau log IDS di jaringan internal PT. H-One Kogi Prima Auto Technologies Indonesia.

1.2. Identifikasi Masalah

Dari latar belakang diatas dapat diperoleh beberapa rumusan masalah dimana sebagai identifikasi penelitian ini diantaranya :

1. Bagaimana menerapkan Mekanisme monitoring insiden ancaman dengan IDS di jaringan internal PT. H-One Kogi Prima Auto Technologies Indonesia?
2. Bagaimana integrasi sistem dalam memusatkan dan analisis log dari IDS ke SIEM di jaringan internal PT. H-One Kogi Prima Auto Technologies Indonesia?

1.3. Lingkup Penelitian

Dari sekian permasalahan yang telah dirumuskan, maka penelitian ini dapat memfokuskan dalam membatasi permasalahan yang akan dibahas.

1. Membangun sistem keamanan jaringan IDS menggunakan Snort versi 3 dan membuat rules sederhana dalam mendeteksi *Network level attack.*
2. Memusatkan dan analisis log dari IDS Snort ke SIEM menggunakan Splunk.
3. Mengimplementasikan sistem di lingkungan *virtual machine* jaringan internal.
4. Mengidentifikasi jaringan server internal PT. H-One Kogi Prima Auto Technologies Indonesia sebagai penerapan sistem IDS Snort dan SIEM Splunk.
5. Melakukan pengujian fungsional dari IDS Snort beserta SIEM Splunk, *Alerting System* IDS Snort dan SIEM Splunk) dan pengujian serangan berbasis jaringan.

1.4. Tujuan Tugas Akhir

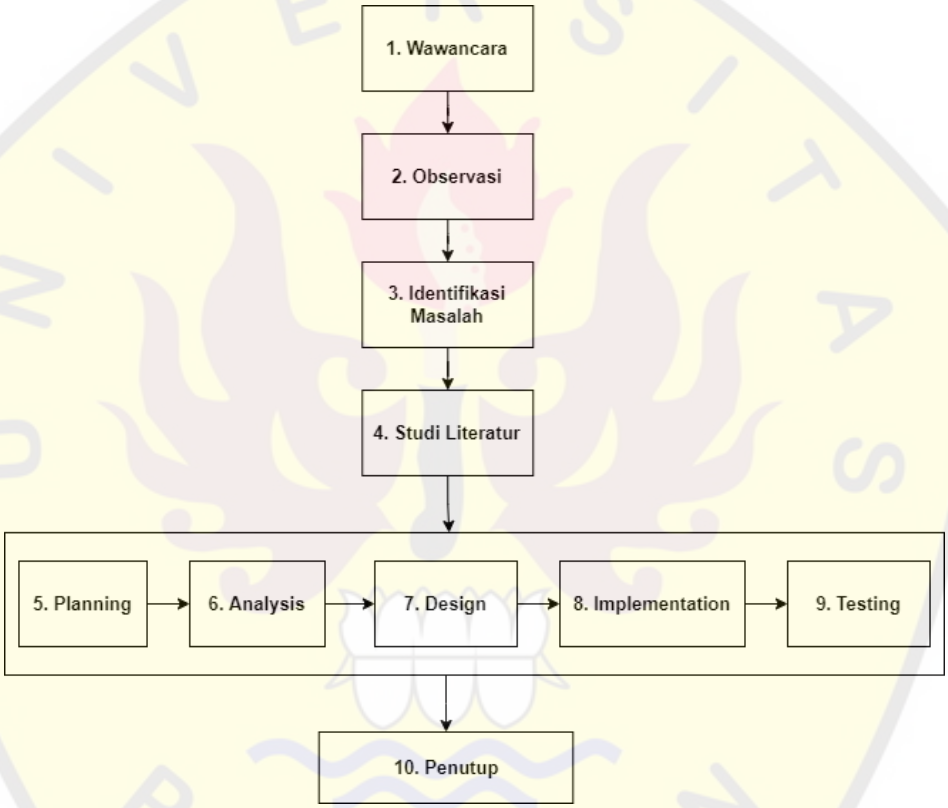
Penelitian tugas akhir ini bertujuan untuk membangun sistem keamanan jaringan dengan pengoperasian monitoring aktivitas mencurigakan menggunakan *Intrusion Detection System* (IDS) dan juga memodifikasi aturan-aturan atau *rules* sederhana didalam sistem IDS yang dapat disesuaikan dengan kebutuhan layanan yang berjalan. Sistem IDS kali ini penulis melakukan analisa *traffic* jaringan, modifikasi *rules* sederhana sesuai *traffic* yang dihasilkan dan melakukan sentralisasi log yang dapat menganalisa *log file* mentahan IDS menjadi log bervariabel yang mudah dibaca dan tervisualisasi. Berikut beberapa tujuan tugas akhir yang penulis buat diantaranya :

1. Dapat mengetahui cara kerja IDS, mengenali pola dari aktivitas insiden jaringan, dan pembuatan *rules* sederhana untuk mendeteksi insiden keamanan jaringan internal PT. H-One Kogi Prima Auto Technologies Indonesia.

2. Dapat memahami integrasi log IDS ke *log collector* menggunakan SIEM, melakukan analisa insiden dari *log data* yang sudah terstruktur dan melakukan visualisasi laporan dari aktivitas insiden pada jaringan yang dihasilkan.
3. Dapat memahami persoalan penerapan sistem keamanan di jaringan internal saat ini dan memberikan rekomendasi sistem keamanan internal jaringan server di PT. H-One Kogi Prima Auto Technologies Indonesia.

1.5. Metodologi Tugas Akhir

Sebagai penunjang dalam menyusun tugas akhir ini, ada beberapa langkah-langkah yang akan di lakukan, yaitu :



Gambar 1.5 1Metodologi Tugas Akhir

1. Wawancara

   Tahap awal tanya dan jawab kepada narasumber di PT. H-One Kogi Prima Auto Technologies Indonesia untuk mengetahui informasi mengenai sistem jaringan pada perusahaan dan menentukan lingkup penelitian.
2. Observasi

   Pada tahap ini mengamati informasi yang sudah didapatkan di lingkungan jaringan PT. H-One Kogi Prima Auto Technologies Indonesia dan menyesuaikan lingkup jaringan sebagai obyek penelitian yang akan diangkat sesuai kebutuhan.

3. Identifikasi Masalah

   Tahap ini merupakan proses mengidentifikasi dan analisa persoalan mengenai obyek penelitian dengan permasalahan yang ada, sehingga dengan menemukan permasalahan yang terjadi di lapangan akan menjadi topik untuk pengumpulan fakta dan sistem yang dibangun.

4. Studi Literatur

   Tahap ini penulis melakukan pengumpulan fakta-fakta, informasi, dan referensi pengembangan terkait objek penelitian yang akan dikerjakan.

5. *Planning*, merupakan tahap awal konsep perencanaan sebelum merancang sebuah sistem.
6. *Analysis*, menjelaskan proses analisa informasi, komponen maupun kebutuhan didalam sistem untuk mencapai tujuan fungsional.
7. *Design*, menjelaskan bagaimana proses merancang sistem seperti topologi yang digunakan dan spesifikasi yang akan digunakan pada sistem.
8. *Implementation*, menjelaskan proses pembangunan sebuah sistem dari rancangan yang dibuat, baik secara fungsional sistem, *rules* yang akan digunakan, dan konfigurasi *trigger alert* dari aktivitas mencurigakan.
9. *Testing*, menjelaskan proses pengujian dari sistem yang dibangun, melakukan penilaian pemindaian dan performa dari sistem.
10. Kesimpulan dan Saran, tahap akhir untuk menyimpulkan dan memberikan saran pada lingkup perusahaan dari objek penelitian yang sudah dibangun.

1.6. Sistematika Penulisan Tugas Akhir

Adapaun penulisan Tugas Akhir ditulis dengan mengikuti sistematika sebagai berikut :

a. BAB I : Pendahuluan

Dalam bab ini menjelaskan tentang latar belakang masalah, identifikasi masalah, batasan masalah dan tujuan akhir penelitian.

b. BAB II : Landasan Teori

Dalam bab ini menjelaskan pembahasan tentang teori – teori dan konsep praktik yang berhubungan dengan penelitian yang dilakukan dan mendukung pemecahan masalah yang dibahas, selain itu bab ini memuat teori – teori pelaksanaan pengumpulan dan pengolahan data serta penganalisaan penelitian. Dalam bab ini juga menjelaskan kajian ilmu penelitian, teori penelitian dan mepaparkan penelitian – penelitian terdahulu yang berhubungan dengan permasalahan topik tugas akhir.

c. BAB III : Skema Penelitian

Dalam bab ini menjelaskan bagaimana alur penyelesaian tugas akhir, lingkup penelitian, kerangka berpikir teoritis dan topologi jaringan yang digunakan pada obyek penelitian.

d. BAB IV : Analisis dan Perancangan Sistem

Dalam bab ini menjelaskan analisa kebutuhan sistem yang dibangun sesuai dengan identifikasi masalah yang diangkat, dan merancang sistem dari hasil analisis sebagai acuan untuk gambaran dalam mengimplementasikan sistem ke lingkup penelitian.

e. BAB V: Pembangunan Sistem

Dalam bab ini menjelaskan bagaiamana alur penmbangunan solusi sistem keamanan jaringan, membangun sistematis serta fungsi mengenai sistem yang diteliti dan integrasi dengan keamanan sistem pengelolaan data secara terpusat.

f. BAB VI : Pengujian Sistem

Dalam bab ini menjelaskan bagaimana pengujian sistem di gunakan, dengan metode-metode serangan ke sistem target yang sudah ditentukan sesuai dengan fungsional sistem keamanan yang di rancang, pengujian ini meliputi cara proses peringatan dari aturan, klasifikasi dan kecepatan data yang diperoleh.

g. BAB VII : Penutup

Bab ini membahas mengenai kesimpulan dari kesuluruhan tugas akhir dalam bentuk paragraf, saran yang dapat menjadi acuan dalam penelitian atau pengembangan selanjutnya dan juga rekomendasi sebagai usulan solusi kedepannya pada penelitian yang diajukan.

DAFTAR PUSTAKA

[ABI21] Abidian, Wahluf. “Implementasi Splunk Dalam Membangun Security Information And Event Managament Berdasarkan Log Firewall Traffic Type (Studi Kasus: Jaringan UII).” Universitas Islam Indonesia. Yogyakarta, 2021.

[ABI16] Abidin, Nanan. “Optimalisasi Firewall Pada Jaringan Komputer Berskala Besar.” Universitas Suryadarma, Jakarta, 2016.

[AFF13] Affandi, M., Setyowibowo, S., “Implementasi Snort Sebagai Alat Pendeteksi Intrusi Menggunakan Linux.” STMIK PPKIA Pradnya Paramita. Malang.

[AJI21] Aji, Ilyas Bayu. “Analisis Penerimaan Sinyal Sqf (Signal Quality Factor) Access Vsat Di Atm Bjb Rumah Sakit Umum Kasih Bunda Cimahi.” Universitas Pasundan, Bandung, 2021.

[AKB21] Akbi, Denar Regata. "Analisis Address Resolution Protocol Poisoning Attack Pada Router Wlan Menggunakan Metode Live Forensics." *Jurnal Komputer Terapan* 7.1 (2021): 62-73.

[ALF22] Alfandi, Muhammad. “Analisa Security Information And Event Management (SIEM) Menggunakan Elastic Stack SIEM Dan Splunk.” Unversitas Islam Riau, 2022.

[ANG13] Anggraeni, Rinda Tri Yuniar. “Analisis Perbandingan Untuk Kerja Protokol TCP,UDP Dan SCTP Menggunakan Simulasi Lalu Lintas Data Multimedia.” Sekola Tinggi Manajemen Informatika & Teknik Komputer, 2013

[CHA12] Chappell, Laura. Wireshark Network Analysis. The Official Wireshark Certified Network Analyst™ Study Guide 2nd Edition (Version 2.1b). Laura Chappell University, 2012.

[ECC19A] EC-Council. Certified SOC Analyst (CSA) eBook w/ iLabs. EC-Council Academia, 2019. VitalBook file.

[ECC19B] EC-Council. EC-Council Certified Incident Handler (ECIH) Version 2 eBook w/ iLabs, 2nd Edition. EC-Council Academia, 2019. VitalBook file.

[ECC20] EC-Council. Certified Network Defender (CND) Version 2 eBook w/ iLabs (Volumes 1 through 4), 2nd Edition. EC-Council Academia, 2020. VitalBook file.

[ECC21] EC-Council. Ethical Hacking Essentials eBook. EC-Council Academia, 2021. VitalBook file.

[EFE19] Efendi N.P., Kusuma J.F., “Sistem Keamanan Jaringan Menggunakan Snort.” Universitas Lancang Kuning, Riau, 2019.

[FAR19] Farhan, Ali. “Implementasi Intrusion Detection System (Ids) Menggunakan Snort Untuk Mendeteksi Serangan Pada Server.” Diss. Universitas Mataram, 2019.

[FEB11] Febrero, Borja Merino. Traffic Analysis With Wireshark. The National Communications Technology Institute, Uruguay, 2021.

[FYO08] Fyodor, L.G., “Nmap Network Scanning.” United States, no. Insecure.Com LLC, 2008.

[GUN18] Gunawan, Garrey Baldo, Parman Sukarno, and Aji Gautama Putrada. "Pendeteksian Serangan Denial of Service (DoS) pada Perangkat Smartlock Berbasis Wifi Menggunakan SNORT IDS." *eProceedings of Engineering* 5.3 (2018): 7875-7884.

[HAN11] Hanggara, Patricius Danang Karismayuri. "Simulasi Jaringan Menggunakan Network Simulator 2", Universitas Sanata Dharma, Yogyakarta, 2011.

[HUM17] Humairah, Nabilah. "Penjelasan Tentang Layanan Pada Protokol TCP Dan UDP." Universitas Sriwijaya, Palembang, 2017.

[KHA17] Khadafi, Shah., Meilani, Budanis Dwi., Arifin, Samsul., "Sistem Keamanan Open Cloud Computing Menggunakan Ids (Intrusion Detection System) Dan Ips(Intrusion Prevention System)", Institut Teknologi Adhi Tama, 2017

[MOH17] Mohammed, Mustapha A., Degadzor, Ashigbi F., Effrim Botchey Francis, Appiah Kwame Anim. "Brute Force Attack Detection And Prevention On A Network Using Wireshark Analysis." Koforidua Technical University, Ghana, 2017

[PRA14] Prabowo, Tony. "Penerapan Intrusion Detection System Pada Web Server Menggunakan Metode Signature Based." Universitas Komputer Indonesia. Bandung, 2014.

[PRA18] Pratama, I Putu A.E., Handayani, Ni Kade Mega. "Implementasi IDS Menggunakan Snort Pada Ubuntu." Universitas Udayana. Denpasar. Bali, 2018.

[PRI18] Primartha, Rifkie. "Network Security Dan Cyber Security." Informatika Bandung, 2018

[PUT18] Putrada, Garrey Baldo Gunawan; Parman Sukarno; Aji Gautama. "Pendeteksian Serangan Denial of Service (DoS) Pada Perangkat Smartlock Berbasis Wifi Menggunakan SNORT IDS", Universitas Telkom, Bandung, 2018.

[REH03] Rehman, Rafeeq Ur. "Intrusion Detection Systems with Snort: Advanced IDS Techniques with Snort, Apache, MySQL, PHP, and ACID." United States of America, 2003

[SEP21] Septian, Aldy Dwi. "Monitoring 3 Log Web Server Menggunakan Splunk", Universitas Muhammadiyah Malang, Malang 2021.

[SNO21A] Snort, "Snort 3 Upgrade Manual" tersedia: Juni 2022, https://github.com/snort3/snort3/releases/download/3.1.36.0/snort_upgrade.pdf, Januari 2021.

[SNO21B] Snort, "Snort 3 Reference Manual", tersedia Juni 2022, https://github.com/snort3/snort3/releases/download/3.1.36.0/snort_reference.pdf , Januari 2021.

[SNO21C] Snort, "Snort 3.1.18.0 on Ubuntu 18 & 20", tersedia Juni 2022, https://snort-org-site3.s3.amazonaws.com/production/document_files/000/011/074/original/Snort_3_on_Ubuntu_18_and_20.pdf, Desember 2021.

[SNO22] Snort, "Snort 3 User Manual", tersedia Juni 2022, https://github.com/snort3/snort3/releases/download/3.1.38.0/snort_user.pdf, Mei 2022.

[SPL22A] Splunk, “Splunk Enterpise 8.2.6 Documentation”, tersedia juni 2022, https://docs.splunk.com/Documentation/Splunk/8.2.6, Mei 2022

[SPL22B] Splunkbase, “Snort Alert for Splunk”, tersedia Juli 2022, https://splunkbase.splunk.com/app/5488/#/details, Juli 2022

[SPL22C] Splunk, “Splunk Universal Forwarder”. Tersedia juni 2022, https://docs.splunk.com/Documentation /Forwarder/8.2.6/Forwarder/Abouttheuniversalforwarder.

[TRI16] Triandini, Rizki. “Implementasi Intrusion Detection System Menggunakan Snort, Barnyard2 Dan Base Pada Sistem Operasi Linux”, Universitas Komputer Indonesia, Bandung, 2016

[WAH17] Wahyudi, Johan. “Threat Packet Analysis Using Snort.” Universitas Sriwijaya. Palembang, 2017.

[WIJ12] Wijaya, Chandra, S.T, M.T. “VLAN sebagai solusi infrastruktur jaringan yang lebih efisien”. Universitas Katolik Parahyangan, 2012