IMPLEMENTASI *PORT SECURITY* UNTUK MEMBATASI AKSES *PORT* PADA *SWITCH* CISCO

PROJEK

Oleh

MUHAMMAD FIERO PANGESTU PRATAMA
NIM 09040581822029

PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
AGUSTUS 2021

IMPLEMENTASI *PORT SECURITY* UNTUK MEMBATASI AKSES *PORT* PADA *SWITCH* CISCO

PROJEK

Sebagai salah satu syarat untuk menyelesaikan studi di
Program Studi Teknik Komputer DIII

Oleh

MUHAMMAD FIERO PANGESTU PRATAMA
NIM 09040581822029

PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
AGUSTUS 2021

HALAMAN PENGESAHAN

IMPLEMENTASI *PORT SECURITY* UNTUK MEMBATASI AKSES *PORT* PADA *SWITCH* CISCO

PROJEK

Sebagai salah satu syarat untuk menyelesaikan studi di
Program Studi Teknik Komputer DIII

Oleh

MUHAMMAD FIERO PANGESTU PRATAMA
NIM 09040581822029

Palembang, Agustus 2021

Pembimbing I,	Pembimbing II,
Ahmad Heryanto, M.T.	**Tri Wanda Septian, M.Sc.**
NIP 198701222015041002	**NIK 1901062809890001**

Mengetahui

Koordinator Program Studi Teknik Komputer,

Huda Ubaya, M.T.
NIP 198106162012121003

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : **Senin**

Tanggal : **19 Juli 2021**

Tim Penguji :

1. Ketua : Sarmayanta Sembiring, M.T.
2. Pembimbing I : Ahmad Heryanto, M.T.
3. Pembimbing II : Tri Wanda Septian, M.Sc.
4. Penguji : Adi Hermansyah, M.T.

Mengetahui

Koordinator Program Studi Teknik Komputer,

Huda Ubaya, M.T.
NIP 198106162012121003

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama	:	Muhammad Fiero Pangestu
NIM	:	09040581822029
Program Studi	:	Teknik Komputer
Jenjang	:	DIII
Judul Projek	:	Impelementasi *Port Security* Untuk Membatasi Akses *Port* Pada *Switch* Cisco
Hasil Pengecekan Software *iThenticate/Turnitin*	:	19 %

Menyatakan bahwa Laporan Projek saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan projek ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian, pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.

Palembang, Agustus 2021

Muhammad Fiero Pangestu
NIM 09040581822029

HALAMAN PERSEMBAHAN

"Siapa pun yang bersungguh-sungguh, dia pasti berhasil."

"Whoever meant it, he'd make it."

"Bersungguh-sungguhlah pada perkara-perkara yang bermanfaat bagimu dan mintalah pertolongan kepada Allah."
(HR. Imam Muslim)

Alhamdulillah, bersyukur kepada Allah SWT atas segala rahmat serta nikmat islam yang telah di anugerahkan oleh Allah Subhanahu wa Ta'ala, sehingga atas berkat itu semua dapat terselesaikan karya kecil ini yang akan kupersembahkan untuk. . .

Kedua orang tuaku yang tercinta
(Bapak Ayatullah dan Ibu Emi Ruspianti)
Teman-teman seperjuangan prodi,
(Teknik Komputer Jaringan 2018)
Teman-teman organisasi,
(BEM KM Fasilkom Unsri)
Almamater perjuangan
(Universitas Sriwijaya)

Agustus 2021

KATA PENGANTAR

Bersyukur kepada Allah SWT yang telah memberikan rahmat dan nikmat islam serta kasih perlindungan-Nya sehingga penulis dapat menyelesaikan penulisan projek akhir ini dengan baik yang berjudul "**Implementasi *Port Security* Untuk Membatasi Akses *Port* Pada *Switch* Cisco**". Penulisan projek akhir ini dibuat dalam rangka memenuhi persyaratan untuk menyelesaikan pendidikan Diploma III Jurusan Sistem Komputer Program Studi Teknik Komputer Fakultas Ilmu Komputer Universitas Sriwijaya untuk memperoleh gelar Ahli Madya Komputer.

Adapun pada kesempatan yang baik ini, penulis ingin menyampaikan ucapan terima kasih kepada semua pihak yang telah membantu dan membimbing penulis sehingga dapat terselesaikannya projek akhir ini dengan baik. Ucapan terima kasih penulis ucapkan kepada:

1. Allah SWT, atas rahmat dan nikmat islam serta perlindungan yang telah diberikan kepada penulis sehingga dapat menyelesaikan laporan projek akhir ini dengan baik.
2. Yang saya cintai Ayah, Ibu, Kakak dan adik, serta sepupu yang selalu ada menemani dalam kondisi apapun dan terus memberikan dukungan moril maupun materil kepada penulis sehingga berjalan dengan lancar saat proses penulisan projek akhir ini.
3. Bapak Ahmad Heryanto, S.Kom., M.T. dan Bapak Tri Wanda Septian, S.Kom., M.Sc selaku sebagai Dosen Pembimbing projek akhir, yang telah memberikan bimbingan dan semangat terus-menerus kepada

penulis dalam menyelesaikan projek akhir ini.

4. Bapak Adi Hermansyah, M.T. selaku sebagai Dosen penguji sidang projek akhir yang telah memberikan kritik dan saran serta ilmu yang sangat bermanfaat sehingga tulisan ini menjadi lebih baik.
5. Bapak Muhammad Ali Buchari, M.T. selaku sebagai Pembimbing Akademik penulis, yang telah membimbing penulis dari semester awal sampai proses terselesainnya projek ahir ini dengan baik.
6. Bapak Huda Ubaya, S.T., M.T. selaku sebagai Koordinator Program Studi Teknik Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
7. Serta seluruh Dosen Program Studi Teknik Komputer, Fakultas Ilmu Komputer,Univeristas Sriwijaya.
8. Mbak Faula selaku sebagai Staff administrasi di Program Studi Teknik Komputer, yang sudah membantu dalam penyelesaian proses administrasi.
9. Seluruh Staff di Fakultas Ilmu Komputer,Universitas Sriwijaya bagian akademik, kemahasiswaan, tata usaha, perlengkapan, dan keuangan, dan seluruhnya yang telah membantu dalam penyelesaian proses administrasi.
10. Seluruh petinggi dan pimpinan pada lingkungan Fakultas Ilmu Komputer, Universitas Sriwijaya, yang telah membantu dalam penyelesaian proses administrasi.
11. Seluruh Teman-teman Laboratorium Jaringan komputer yang telah membantu dalam proses terselesainya projek akhir ini.
12. Seluruh Teman-teman satu angkatan, Teknik Komputer dan Jaringan

2018, Muhammad Fahrie Fatihah, Alfina, Dwi, Dippo, dan Muhammad Agung, Ahmad Arbain, Dirga, Faris, Fikri. Angga dan semuanya. Semoga sukses dimasa yang akan datang untuk kita semua.

13. Serta Organisasi di Fakultas Ilmu Komputer Universitas Sriwijaya, BEM KM (Badan Eksekutif Mahasiswa). Terima kasih atas kesempatannya telah diterima menjadi keluarga besar, serta ilmu yang bermanfaat.
14. Terakhir penulis mengucapkan terima kasih kepada semua pihak yang telah membantu penulis dalam proses terselesainya projek akhir ini. Jazakumullah Khairan.

Semoga dengan terselesaikan projek akhir ini akan bermanfaat untuk menambah ilmu pengetahuan serta wawasan untuk kita semua dalam mempelajari Implementasi *Port Security* Untuk Membatasi Akses *Port* Pada *Switch* Cisco.

Palembang, Agustus 2021

Penulis

IMPLEMENTASI *PORT SECURITY* UNTUK MEMBATASI AKSES *PORT* PADA *SWITCH* CISCO

Oleh

MUHAMMAD FIERO PANGESTU PRATAMA
NIM 09040581822029

Abstrak

Fokus penelitian ini adalah melindungi jaringan komputer dengan implementasi *port security* untuk membatasi akses *port* pada *switch* guna untuk meningkatkan performa pada *switch* dan mencegah dari akses koneksi jaringan yang tidak berkepentingan serta mengurangi tindakan pencurian data pada jaringan komputer. Pada penelitian ini dilakukan tiga skenario pengujian : (i) *port security violation protect* paket data dari perangkat atau perangkat akan dibuang (dihentikan) dan oleh karena itu tidak dapat dihubungkan, (ii) *port security violation restrict* paket data perangkat tidak akan dibuang (dihentikan), tetapi hanya akan direkam, dan kemudian tidak diizinkan untuk memasuki jaringan, dan (iii) *port security violation shutdown port* akan segera dimatikan, dan perangkat akan tidak dapat terhubung secara otomatis. Hasil setelah dilakukan pengujian yaitu berhasil membatasi akses *port* pada *switch* cisco.

Kata Kunci : Keamanan Jaringan, *Port Security*, *Port Switch* Cisco

Palembang, Agustus 2021

Pembimbing I,	**Pembimbing II,**
Ahmad Heryanto, M.T.	**Tri Wanda Septian, M.Sc.**
NIP 198701222015041002	**NIK 1901062809890001**

Mengetahui

Koordinator Program Studi Teknik Komputer,

Huda Ubaya, M.T.
NIP 198106162012121003

IMPLEMENTASI *PORT SECURITY* UNTUK MEMBATASI AKSES *PORT* PADA *SWITCH* CISCO

Oleh

MUHAMMAD FIERO PANGESTU PRATAMA
NIM 09040581822029

Abstrak

Fokus penelitian ini adalah melindungi jaringan komputer dengan implementasi *port security* untuk membatasi akses *port* pada *switch* guna untuk meningkatkan performa pada *switch* dan mencegah dari akses koneksi jaringan yang tidak berkepentingan serta mengurangi tindakan pencurian data pada jaringan komputer. Pada penelitian ini dilakukan tiga skenario pengujian : (i) *port security violation protect* paket data dari perangkat atau perangkat akan dibuang (dihentikan) dan oleh karena itu tidak dapat dihubungkan, (ii) *port security violation restrict* paket data perangkat tidak akan dibuang (dihentikan), tetapi hanya akan direkam, dan kemudian tidak diizinkan untuk memasuki jaringan, dan (iii) *port security violation shutdown port* akan segera dimatikan, dan perangkat akan tidak dapat terhubung secara otomatis. Hasil setelah dilakukan pengujian yaitu berhasil membatasi akses *port* pada *switch* cisco.

Kata Kunci : Keamanan Jaringan, *Port Security*, *Port Switch* Cisco

Palembang, Agustus 2021

Pembimbing I,

Ahmad Heryanto, M.T.
NIP 198701222015041002

Pembimbing II,

Tri Wanda Septian, M.Sc.
NIK 1901062809890001

Mengetahui

Koordinator Program Studi Teknik Komputer,

Huda Ubaya, M.T.
NIP 198106162012121003

DAFTAR ISI

Halaman

DAFTAR NOMENKLATUR

Port	=	Pelabuhan
VLAN	=	*Virtual Local Area Network*
Encapsulasi	=	*Proses pemaketa / Penyatu data*
LAN	=	*Local Area Network*
TCP	=	*Transmission Control Protocol*
IP Address	=	*Internet Protocol Address*
Layer	=	*Lapisan-lapisan pada model jaringan*
OSI	=	*Open System Interconnection*
VLAN ID	=	*Virtual Local Area Network Identifier*
MAC Address	=	*Media Access Control Address*
Client	=	Komputer yang menerima layanan
ID	=	Pengenal
Broadcast	=	Pengiriman data ke banyak penerima
Violation	=	Pelanggaran
CLI	=	*Command Line Interface*
Scanning	=	Pemindaian
Enabled	=	Memungkinkan
SSH	=	*Secure Shell*
Disable	=	Dengan disabilitas
Security	=	Keamanan
Remote Login	=	Pengoperasian jarak jauh
Shutdown	=	Mematikan
Flowchart	=	Urutan suatu proses
Interface	=	Sebuah titik penghubung antar benda
UTP	=	*Unshielded twisted pair*
Protect	=	Melindungi
Restrict	=	Membatasi

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR LAMPIRAN

Halaman

BAB I. PENDAHULUAN

1.1 Latar Belakang

Kebutuhan akan jaringan komputer semakin bertambah penting, salah satu hal penting dalam mengelola sebuah jaringan komputer adalah keamanan dari jaringan itu sendiri. Dengan begitu banyak akses ke jaringan, ada banyak peluang kejahatan terjadi di dalam jaringan. Salah satu teknologi yang digunakan untuk mengamankan jaringan adalah dengan menggunakan keamanan *port*.

Dalam studi sebelumnya yang telah menjelaskan implementasi jaringan area lokal virtual dan daftar akses. *Study* kedua menggunakan daftar kontrol akses sebagai *filter* lalu lintas jaringan untuk melakukan konfigurasi jaringan. Studi ketiga menganalisis penggunaan daftar kontrol akses dalam jaringan komputer. Dari beberapa penelitian terdahulu tersebut, kami dapat menjelaskan beberapa perbedaan dalam penelitian ini, user lebih mudah digunakan karena penulis menggunakan antarmuka pengguna grafis, fungsionalitas lebih lengkap, dan lebih aman karena menggunakan *firewall router* dan lebih efisien karena satu kebijakan dapat memuat banyak aturan serta dapat menjalankan *filter* jaringan berdasarkan aplikasi *DNS*, *https*, dan lainnya. Manfaat menggunakan *VLAN* diantaranya :

1. Bertambah dan tertingkatnya kualitas kinerja jaringan dengan cara dibagi domain siaran menjadi beberapa bagian.
2. Tingkatkan fleksibilitas keamanan jaringan, atur apakah paket siaran yang dikirim dari satu unit kerja tidak diterima oleh komputer di unit kerja yang berbeda, dan izinkan jaringan untuk mengizinkan komputer terhubung ke *server* atau komputer lain di *subnet* lain, kelebihan dari *VLAN* :

1. Kombinasi administrator jaringan statis mengkonfigurasi port switching pada *VLAN* tertentu *port* dinamis secara langsung ditetapkan ke *VLAN* tertentu melalui server kebijakan *VLAN*.
2. *Trunk* dan *Switch* menggunakan port trunk untuk menyeret *frame* dari semua *VLAN* ke *switch* lain. Port trunk digunakan untuk koneksi antar *switch*. Beri label setiap *frame* dengan nomor *VLAN* [1].

Namun dari beberapa Penelitian diatas yang telah dilakukan oleh beberapa penulis sebelumnya tadi masih terdapat kelemahan terhadap keamanan jaringannya dan masih besar kemungkinan terkena serangan-serangan jaringan seperti *port scanning* dan *ip spoofing*. Oleh karena itu Implementasi *port security* perlu diterapkan, yaitu guna meningkatkan keamanan *port default / statis, port learning dinamis, sticky port* untuk menentukan keandalan, ketersediaan dan penggunaan di lapangan, dan guna untuk mengetahui keamanan *port* yang harus digunakan saat menganalisis, berbeda dengan keamanan tersebut dengan cara menyadap *port* menggunakan *iptables* sebagai *firewall*, coba diimplementasikan penggunaan keamanan *port* pada jaringan cisco *switch* pada penelitian ini.

Berdasarkan penjelasan latar belakang tersebut, maka penulis melakukan penelitian lebih lanjut dengan memindahkan kasus di atas ke sebuah projek bernama **"Implementasi *Port Security* Untuk Membatasi Akses *Port* Pada *Switch Cisco*".**

1.2 Tujuan

Adapun tujuan dari penelitian ini adalah :

1. Menerapkan konsep teknologi keamanan *port* jaringan.
2. Tingkatkan kinerja dan keamanan jaringan.

3. Pahami konfigurasi *switch* cisco.

1.3 Manfaat

Manfaat yang diharapkan adalah :

1. Menentukan sekelompok *end devices* yang di izinkan mengakses *port*.
2. Hanya mengizinkan *mac-address* tertentu yang dapat mengakses *port*.
3. Menentukan tindakan yang akan dilakukan apabila terdeteksi *mac-address* yang di izinkan.

1.4 Rumusan Masalah

Rumusan masalah dalam penelitian ini sebagai berikut :

1. Menerapkan *port security* menggunakan cisco *switch*.
2. Melakukan konfigurasi *port security* pada cisco *switch*

1.5 Batasan Masalah

Keterbatasan masalah dalam penelitian ini sebagai berikut :

1. Terterap *port security* di *switch* cisco.
2. Konfigurasikan keamanan *port* dengan apllikasi paket Cisco dan PuTTY sesuai dengan protokol untuk manajemen keamanan jaringan yang mudah.

1.6 Metode Penelitian

Berikut metode pada penelitian ini sebagai berikut :

1. Metode Literatur

   Mengumpulkan informasi dari buku, majalah, dan Internet terkait pembuatan projek “Implementasi *Port Security* Untuk Membatasi Akses *Port* Pada *Switch* Cisco”.

2. Metode Observasi

   Diakukan penerapan secara langsung ke tempat penelitian.

3. Metode Konsultasi

   Metode konsultasi, mengajukan pertanyaan dan menjawabnya dengan atasan sebagai pelengkap laporan saat membuat dan mendesain.

4. Metode Implementasi dan Pengujian

   Gunakan konfigurasi yang sesuai untuk menjadi sistem jaringan nyata. Tidak hanya untuk pengujian hasil konfigurasi. Tes ini untuk membantu memverifikasi bahwa sistem jaringan berfungsi dengan baik dengan Keamanan *Port*.

1.7 Sistematika Penelitian

Untuk memudahkan proses penyusunan Tugas Akhir dan memperjelas isi setiap bab, maka secara sistematis ditulis sebagai berikut:

BAB I PENDAHULUAN

Bab ini menerangkan topik penelitian dasar, termasuk latar belakang, tujuan, manfaat, rumusan masalah, batasan masalah, metodologi penelitian, dan deskripsi sistematis.

BAB II TINJAUAN PUSTAKA

Bab ini berisi penjelasan tentang bagaimana teori pemecahan masalah yang akan digunakan penelitian ini, berdasarkan sumber dari penelitian sebelumnya.

BAB III METODOLOGI PENELITIAN

Bab ini memberikan gambaran sistematis tentang proses penelitian. Penjelasan pada bab ini meliputi tahapan perancangan sistem dan penggunaan metode penelitian.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menyajikan hasil pengujian yang dilakukan dan membahas informasi yang diperoleh dari hasil pengujian. Pembahasan data akan didasarkan pada kriteria yang telah ditentukan.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi ringkasan hasil percobaan didasarkan pada yang dibahas dalam Bab I, dan memberikan informasi tambahan untuk penelitian lebih lanj

DAFTAR PUSTAKA

[1] A. M. Lukman and Y. Bachtia, "Analisis sistem keamanan jaringan dengan," *Comput. Eng. Syst. Sci.*, vol. 1, no. 1, pp. 9–14, 2016.

[2] R. K. Sianipar, "Implementasi Sistem Keamanan Koneksi Wireless Distribution Sisytem (Wds)," vol. 14, no. 2, pp. 33–38, 2017.

[3] L. Belakang, "Bab I ْ ب ا ُ ض ح ي ِ خ ,," no. 2504, pp. 1–9, 2015.

[4] P. S. Informatika, S. Tinggi, T. Adisutjipto, and L. A. Yogyakarta, "IMPLEMENTATION PORT SECURITY FOR SECURITY SYSTEMS NETWORK AT THE COMPUTING LABORATORY OF ADISUTJIPTO," vol. IV, 2018.

[5] I. Card, "Data Link Layer," *SpringerReference*, 2011, doi: 10.1007/springerreference_11718.

[6] Sudana, Haryanto (2015) *MERANCANG APLIKASI SWITCH REMOTE DETECTOR DENGAN MENGGUNAKAN METODE DETEKSI TEPI Studi Kasus : Switch Sentral Gedung Fakultas Teknik Universitas Darma Persada.* Universitas Darma Persada.

[7] U. T. Pair *et al.*, "JARINGAN KOMPUTER – KABEL UTP a. Pengertian kabel UTP."

[8] S. Sukaridhoto ST. Ph.D, "Buku Jaringan Komputer," p. 129, 2016.

[9] E. K. O. YANDRI, "Analisis Perancangan Dan Implementasi Koneksi Jaringan Vlan (Virtual Local Area Network) Dengan Menggunakan Vtp (Vlan Trunking Protocol) Pruning Di Gedung Dewi Sartika Universitas Negeri Jakarta," 2015