



**SIMULASI KEAMANAN JARINGAN DENGAN METODE NETWORK
DEVELOPMENT LIFE CYCLE MENGGUNAKAN SWITCH PORT
SECURITY PADA PT PINUS MERAH ABADI**

SKRIPSI

**Karya tulis sebagai salah satu syarat
untuk memperoleh gelar Sarjana dari
Universitas Indo Global Mandiri**

Oleh

RA MARTASYA PUTRI

NPM: 2019310071

(Program Studi Sarjana Sistem Komputer)

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS INDO GLOBAL MANDIRI
AGUSTUS 2023**

**SIMULASI KEAMANAN JARINGAN DENGAN METODE NETWORK
DEVELOPMENT LIFE CYCLE MENGGUNAKAN SWITCH PORT
SECURITY PADA PT PINUS MERAH ABADI**

SKRIPSI



Oleh:

NPM	: 2019310071
NAMA	: RA MARTASYA P
JENJANG STUDI	: STRATA SATU (S1)
PROGRAM STUDI	: SISTEM KOMPUTER

**PROGRAM STUDI SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS INDO GLOBAL MANDIRI
AGUSTUS 2023**

LEMBAR PENGESAHAN

LEMBAR PERSETUJUAN DEWAN PENGUJI

Pada hari ini Jumat Tanggal 25 Agustus 2023 telah dilaksanakan Ujian Skripsi oleh Program Studi Sistem Komputer Fakultas Ilmu Komputer Universitas Indo Global Mandiri Palembang.

Menyetujui
Tim Penguji

Palembang 25 Agustus 2023

Ketua Penguji



Ir Zulkifli, M.Sc
NIK.2011.01.01.11

Penguji 1



Tasmi, S. Si., M.Kom
NIK. 2017.01.02.30

Penguji 2



Ir. Hasta Sunardi, MT
NIK.2003.01.0072

Mengetahui
Ketua Program Studi Sistem Komputer



Tasmi, S. Si., M.Kom
NIK. 2017.01.02.30

LEMBAR PERSETUJUAN DEWAN PENGUJI

Pada hari ini Jumat Tanggal 25 Agustus 2023 telah dilaksanakan Ujian Skripsi oleh Program Studi Sistem Komputer Fakultas Ilmu Komputer Universitas Indo Global Mandiri Palembang.

Menyetujui
Tim Penguji

Palembang 25 Agustus 2023

Ketua Penguji



Ir Zulkifli, M.Sc
NIK.2011.01.01.11

Penguji 1



Tasmi, S. Si., M.Kom
NIK. 2017.01.02.30

Penguji 2



Ir. Hasta Sunardi, MT
NIK.2003.01.0072

Mengetahui
Ketua Program Studi Sistem Komputer



Tasmi, S. Si., M.Kom
NIK. 2017.01.02.30

SURAT KETERANGAN REVISI SKRIPSI

Kami yang bertanda tangan dibawah ini, menerangkan bahwa:

Nama : Ra Martasya Putri
NPM : 2019310071
Judul Skripsi : Simulasi Keamanan Jaringan Dengan Metode *Network Development Life Cycle* Menggunakan *Switch Port Security* Pada PT Pinus Merah Abadi

Mahasiswa yang namanya tercantum diatas, telah selesai merevisi penulisan skripsi.

Menyetujui
Tim Penguji

Tanggal 25 Agustus 2023

Ketua Penguji



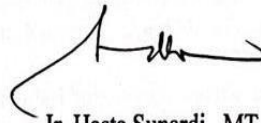
Ir Zulkifli, M.Sc
NIK.2011.01.01.11

Penguji 1



Tasmi, S. Si., M.Kom
NIK. 2017.01.02.30

Penguji 2



Ir. Hasta Sunardi, MT
NIK.2003.01.0072

Mengetahui
Ketua Program Studi Sistem Komputer



Tasmi, S. Si., M.Kom
NIK. 2017.01.02.30

ABSTRAK

SIMULASI KEAMANAN JARINGAN DENGAN METODE NETWORK DEVELOPMENT LIFE CYCLE MENGGUNAKAN SWITCH PORT SECURITY PADA PT PINUS MERAH ABADI

Perkembangan teknologi dalam jaringan komputer lambat laun semakin pesat seiring dengan meningkatnya kebutuhan akan akses jaringan yang efisien, stabil dan cepat serta keamanan yang handal. Salah satu faktor yang mempengaruhi kualitas dalam jaringan adalah network security atau keamanan jaringan, banyak teknik yang dapat dilakukan dalam meningkatkan keamanan jaringan, baik dengan membangun sistem firewall atau port security. Port security memanfaatkan port-port yang ada untuk mengizinkan akses ke jaringan. Pada PT Pinus Merah Abadi bekerja dengan menggunakan aplikasi berbasis jaringan komputer dimana dalam penggunaannya selama ini sering terjadi permasalahan koneksi yang lambat karena banyak trafik data berlebihan pada jaringan dan keamanan jaringannya juga masih lemah. Supaya jaringan komputer di PT Pinus Merah Abadi lebih aman maka Penulis akan melakukan simulasi dengan keamanan port-security pada setiap switch yang ada di PT Pinus Merah Abadi.

Kata kunci: Keamanan Jaringan, Port Security, VLAN

ABSTRACT

NETWORK SECURITY SIMULATION USING THE NETWORK DEVELOPMENT LIFE CYCLE METHOD USING THE SWITCH PORT SECURITY IN PT PINUS MERAH ABADI

Technological developments in computer networks are gradually increasing rapidly in line with the increasing need for efficient, stable and fast network access as well as reliable security. One of the factors that affect network quality is network security or network security, many techniques can be done to improve network security, either by building a firewall system or Port security utilizes existing ports to allow access to the network. PT Pinus Merah Abadi works by using a computer network- based application where in its use so far slow connection problems often occur because there is a lot of excessive data traffic on the network and network security is also still weak. In order for the computer network at PT Pinus Merah Abadi to be more secure, the author will implement port-security security on every switch at PT Pinus Merah Abadi.

Keywords: Network Security, Port Security, VLAN

KATA PENGANTAR

Puji dan syukur Saya ucapkan atas kehadiran Allah Subhanahu Wata'ala berkat Rahmat dan Hidayahnyalah akhirnya penulis dapat menyelesaikan penelitian ini dengan baik tepat pada waktunya, tidak lupa shalawat serta salam selalu dilimpahkan kepada junjungan kita Nabi Muhammad Shallallahu'alaihi Wassallam beserta keluarga sahabat para pengikut dan insyaallah kita semua hingga akhir zaman.

Proposal Skripsi yang penulis buat dengan judul "SIMULASI KEAMANAN JARINGAN DENGAN METODE NDLC MENGGUNAKAN SWITCH PORT SECURITY PADA PT PINUS MERAH ABADI" disusun guna memenuhi syarat kelulusan dalam memperoleh gelar Sarjana (S1) pada Program Studi Sistem Komputer, Fakultas Ilmu Komputer, Universitas Indo Global Mandiri (UIGM) Palembang.

Tidak lupa penulis mengucapkan terimakasih atas bantuan yang diberikan selama penyusunan skripsi ini kepada:

1. Dr. Marzuki Alie, SE.,MM, selaku Rektor Universitas Indo Global Mandiri Palembang.
2. Rudi Heriansyah, ST., M.Eng. Ph.D selaku Dekan Fakultas Ilmu Komputer Universitas Indo Global Mandiri.
3. Tasmi, S.Si., M.Kom, sebagai Ketua Program Studi Teknik Informatika Universitas Indo Global Mandiri.
4. Ir. Zulkifli, M.Sc, sebagai Dosen Pembimbing I.
5. Ricky Maulana Fajri, S.Kom., M.Sc, sebagai Dosen Pembimbing II.
6. Rachmansyah, S.Kom sebagai Dosen Pembimbing Akademik.
7. Bapak/Ibu Dosen Fakultas Ilmu Komputer dan Karyawan/Karyawati Universitas Indo Global Mandiri.
8. Kedua Orang Tua saya Kakak saya serta adik-adik saya terimakasih selalu disamping saya, memberi semangat dalam keadaan apapun.
9. Prada Arief Mulya yang menjadi suport disetiap perjuangan saya
10. Semua teman-teman seperjuangan Sistem Komputer Angkatan 2019.

Dengan segala kerendahan hati penulis menyadari bahwa tugas akhir ini masih jauh dari kata sempurna, oleh karena itu dibutuhkan kritik dan saran untuk

perbaikan dan pengembangan tugas akhir ini sangat diharapkan. Akhir kata, semoga tugas akhir ini bermanfaat bagi semua pihak, terima kasih.

Palembang, 25 Aug 2023

Penulis

RA Martasya Putri

2019.31.0071

DAFTAR ISI

HALAMAN JUDUL LUAR.....
HALAMAN JUDUL DALAM.....
LEMBAR PENGESAHAN	i
LEMBAR PERSETUJUAN DEWAN PENGUJI	ii
SURAT KETERANGAN REVISI SKRIPSI.....	iii
ABSTRAK	iv
ABSTRACT	v
KATA PENGANTAR.....	vi
DAFTAR ISI.....	viii
DAFTAR GAMBAR DAN ILUSTRASI.....	x
DAFTAR TABEL.....	xi
DAFTAR LAMPIRAN	xii
BAB I PENDAHULUAN.....	1
I.1 Latar Belakang	1
I.2 Masalah Penelitian	2
I.3 Batasan Masalah.....	2
I.4 Tujuan Penelitian	3
I.5 Manfaat Penelitian	3
I.6 Sistematika Penulisan.....	3
BAB II TINJAUAN PUSTAKA.....	5
II.1 Jaringan Komputer	5
II.1.1 Jenis Jaringan Komputer	6
II.2 Virtual Local Area Network (VLAN).....	7
II.3 Komponen Jaringan Komputer	8
II.3.1 Network Interface Card (NIC)	8
II.3.2 Router	8
II.3.3 Switch.....	9
II.4 Keamanan Jaringan	9
II.5 Switch Port Security.....	11
II.6 Serangan Keamanan Jaringan	11
II.7 Penelitian Terdahulu	14

BAB III METODE PENELITIAN	19
III.1 Gambaran Umum Objek Penelitian	19
III.2 Metode Pengumpulan Data	19
III.2.1 Data Primer	20
III.2.2 Data Sekunder	20
III.3 Metode Network Development Life Cycle (NDLC)	21
III.4 Alat Pnelitan	22
III.4.1 Perangkat Keras (<i>Hardware</i>).....	22
III.4.2 Perangkat Lunak (<i>Software</i>).....	23
III.5 Skema Penelitian.....	23
III.5.1 Analisis Jaringan	23
III.5.3 Penetration Testing.....	27
III.5.2 Pencegahan Serangan.....	33
III.6 Tahapan Penelitian	35
BAB IV HASIL DAN PEMBAHASAN.....	38
IV.1 Analisis Jaringan Berjalan.....	38
IV.2 Pembuatan Skenario.....	39
IV.2.1 Skenario Komputer	39
IV.2.2 Skenario Penyerang.....	40
IV.3 Simulasi Serangan Dos	41
IV.4 Rancangan Jaringan Usulan	45
IV.5 Simulasi Keamanan Jaringan (<i>Switch Port Security</i>).....	45
IV.5.1 Desain Simulasi.....	47
IV.5.2 Pelaksanaan Simulasi	48
IV.5.3 Hasil Simulasi.....	50
BAB V KESIMPULAN DAN SARAN	55
V.1 Kesimpulan	55
V.2 Saran.....	55
DAFTAR PUSTAKA	57

DAFTAR GAMBAR DAN ILUSTRASI

Gambar II. 1 Jaringan Local Area Network (LAN)	6
Gambar II. 2 Jaringan Wide Area Network (WAN)	7
Gambar III. 1 Network Development Life Cycle (NDLC)	20
Gambar III. 2 Flowchart Alur Pengujian Penelitian Penetration Testing	25
Gambar III. 3 Topologi Jaringan PT Pinus Merah Abadi (Sekarang).....	27
Gambar III. 4 Attacing/Strassing dengan DoS	30
Gambar III. 5 Topologi Jaringan PT Pinus Merah Abadi (Usulan)	32
Gambar III. 6 Tahapan Penelitian	33
Gambar III. 7 Flowchart Bangun Jaringan.....	35
Gambar IV. 1 Topologi Berjalan PT Pinus Merah Abadi.....	38
Gambar IV. 2 Screenshoot Aplikasi Distribusi PMA	41
Gambar IV. 3 Screenshot kinerja Windows Tanpa Serangan.....	42
Gambar IV. 4 Screenshot LOIC protokol TCP target	42
Gambar IV. 5 Screenshot kinerja Windows Komputer saat DoS melalui TCP ...	43
Gambar IV. 6 Screenshot LOIC protokol UDP target	43
Gambar IV. 7 Screenshot kinerja Windows Komputer saat DoS melalui UDP ...	44
Gambar IV. 8 Topologi Jaringan Usulan	45
Gambar IV. 9 Topologi Simulasi	47
Gambar IV. 10 Status Switch Port Fa0/2	59
Gambar IV. 11 Ping dari PC12	59
Gambar IV. 12 Koneksi tidak terputus walaupun pada PC12.....	60
Gambar IV. 13 Status Switch Port Fa0/3	60
Gambar IV. 14 Memindahkan koneksi pada PC11	61
Gambar IV. 15 Ping dari PC11	61
Gambar IV. 16 Status Akhir Switch Port Fa0/3 MAC Address berbeda	62
Gambar IV. 17 Status Switch Port Fa0/4	62
Gambar IV. 18 Ping dari PC10	63
Gambar IV. 19 Setelah melakukan ping pada PC10.....	63
Gambar IV. 20 Status port fa0/4 setelah dilakukan ping MAC Address berbeda	63

DAFTAR TABEL

Table II.1 Penelitian Terdahulu	14
Tabel IV.1 Tabel Addressing	47

DAFTAR LAMPIRAN

lampiran 1 Daftar Riwayat Hidup.	59
lampiran 2 Kartu Bimbingan.....	60
lampiran 3 Surat pernyataan bebas plagiat.....	61
lampiran 4 surat persetujuan ujian skripsi.....	62
lampiran 5 surat keterangan revisi skripsi.....	63

BAB I PENDAHULUAN

I.1 Latar Belakang

Perkembangan teknologi informasi sangat dibutuhkan oleh semua orang untuk mempermudah pekerjaan manusia. Hal ini terlihat dari banyaknya penggunaan teknologi informasi dalam berbagai aspek perusahaan. Contoh penggunaan teknologi informasi adalah jaringan komputer. Jaringan komputer adalah kumpulan dari beberapa komputer yang saling terhubung satu sama lain, sehingga memungkinkan pengguna dapat saling bertukar informasi berupa suara, video dan data pada jaringan yang sama [1].

Kebutuhan jaringan komputer semakin bertambah penting seiring kemajuan teknologi dan tuntutan dalam kehidupan dalam banyak bidang termasuk bidang pekerjaan, salah satu yang paling penting dalam mengelola jaringan adalah masalah keamanan. Banyak sekali tindak kejahatan di dalam jaringan contohnya seperti penyebaran virus, pencurian data dan lain sebagainya. Salah satu cara untuk mempersempit peluang dalam melakukan kejahatan di dalam jaringan adalah membuat sebuah keamanan di perangkat switch. Disinilah nanti akan dibatasi siapa saja dan perangkat apa saja yang bisa mengakses atau bisa masuk dalam sebuah jaringan [1].

Pada PT Pinus Merah Abadi memiliki banyak bagian yang menggunakan komputer yang terintegrasi dengan jaringan komputer dalam lingkup jaringan LAN (Local Area Network). Dengan adanya jaringan komputer yang saling terhubung, para karyawan dari berbagai divisi yang ada dapat memanfaatkan jaringan komputer sebagai sarana untuk melakukan kegiatan yang dapat menunjang kegiatan pekerjaan agar dapat bekerja dengan baik, jaringan tersebut harus dikelola dengan benar, baik dari segi performa maupun keamanannya. Untuk memudahkan

administrator jaringan dalam meningkatkan keamanan pada perangkat yang ada dalam jaringan, maka perlu pengamanan jaringan lokal yaitu salah satunya dengan menerapkan sistem keamanan security port pada switch.

Menerapkan sistem keamanan security port ini dapat berguna untuk membatasi hak akses komputer yang tidak terdaftar dalam port switch tersebut dan dapat mencegah terjadinya penyalahgunaan hak akses oleh orang asing atau admin yang keliru pada saat melakukan perpindahan sehingga security port ini merupakan teknik yang mengizinkan siapa saja yang berhak menggunakan akses jaringan melalui port yang tersedia di switch berdasarkan latar belakang diatas, maka penelitian ini penulis mengambil judul “Simulasi Keamanan Jaringan Dengan Metode NDLC Menggunakan Switch Port Security Pada PT Pinus Merah Abadi”.

I.2 Masalah Penelitian

Berdasarkan latar belakang yang telah diuraikan, maka masalah yang akan dibahas dalam penelitian ini adalah bagaimana bentuk keamanan jaringan dengan switch port security pada PT Pinus Merah Abadi agar setiap pengguna dalam jaringan bisa bekerja sesuai hak aksesnya masing-masing?

I.3 Batasan Masalah

Batasan masalah dibuat agar penelitian ini berfokus pada topik yang akan dibahas. Adapun batasan masalah dari topik ini diantaranya sebagai berikut:

1. Menganalisis keamanan jaringan pada PT Pinus Merah Abadi.
2. Simulasi keamanan port pada Jaringan komputer dengan Metode NDLC menggunakan Switch Port Security.
3. Menggunakan Cisco Packet Tracer sebagai alat simulasi keamanan jaringan.

I.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk mengetahui fungsi dan cara kerja port pada switch dengan menerapkan sistem keamanan port security serta mengkonfigurasi dan merancang port security pada Jaringan Komputer yang ada pada PT Pinus Merah Abadi.

I.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah:

1. Mengetahui fungsi dan cara kerja port pada switch dengan menerapkan sistem keamanan port security.
2. Mewujudkan keamanan port pada switch dengan metode keamanan yang dapat melindungi, membatasi, atau bahkan menolak hak akses dari perangkat yang tidak dikenal.

I.6 Sistematika Penulisan

Sistematika penulisan penelitian ini disusun untuk memberikan penjelasan umum tentang penelitian yang dilakukan. Sistematika penulisan penelitian ini adalah sebagai berikut:

BAB 1 PENDAHULUAN

Bab ini akan membahas mengenai:

1. Latar Belakang
2. Perumusan Masalah
3. Batasan Masalah
4. Tujuan Penelitian
5. Manfaat Penelitian

6. Sistematika penelitian

BAB 2 LANDASAN TEORI

Pada bab landasan teori ini akan menjelaskan tentang beberapa teori untuk dipergunakan pada penelitian kali ini, diantaranya sebagai berikut:

1. Jaringan Komputer
2. VLAN (Virtual Local Area Network)
3. Komponen Jaringan Komputer
 - a. Network Interface Card (NIC)
 - b. Router
 - c. Switch
4. Keamanan Jaringan
5. Penelitian Terdahulu

BAB 3 METODOLOGI PENELITIAN

Pada bab ini mengenai metodologi penelitian yang berisi:

1. Metode Pengumpulan Data
2. Metode Network Development Life Cycle (NDLC)
3. Tahapan Penelitian

BAB 4 HASIL DAN IMPLENTASI

Bab ini menjelaskan tentang hasil dan pembahasan simulasi dari Perancangan Jaringan Simulasi Packet Tracer dan Konfigurasi Simulasi Cisco Packet Tracer.

BAB 5 KESIMPULAN DAN SARAN

Bab ini menjelaskan kesimpulan dari penelitian ini berdasarkan hasil yang telah diperoleh, kemudian memberi saran untuk perancangan monitoring atau maintenance sistem secara berlaka.

BAB II TINJAUAN PUSTAKA

II.1 Jaringan Komputer

Jaringan komputer merupakan sebuah sistem yang terdiri dari sekelompok komputer yang saling terkoneksi satu dengan yang lainnya menggunakan protokol komunikasi melalui media komunikasi untuk dapat saling berbagi informasi, program atau pun penggunaan perangkat. Jaringan komputer terdiri dari komputer, software dan perangkat jaringan yang bekerja sama dalam suatu ruang lingkup untuk mencapai suatu tujuan. Untuk mencapai tujuan tersebut, setiap bagian dari jaringan komputer meminta dan memberikan layanan [1].

Jaringan Komputer berkembang dengan sangat pesat, akses terhadap internet sangat dibutuhkan oleh semua kalangan sekarang ini. Interent tidak hanya di akses untuk mencari informasi bagi orang-orang yang membutuhkannya, tetapi juga di akses oleh hacker atau cracker. Dengan alasan tertentu mereka melakukan penyusupan yang dapat merugikan para pemilik server dan jaringan komputer. Mereka menggunakan berbagai macam serangan jaringan komputer dengan tools yang dibuat secara mandiri ataupun yang telah ada. Kecanggihan serangan dan tools pada jaringan komputer berbanding terbalik dengan pengetahuan tentang penyusupan pada jaringan computer [2].

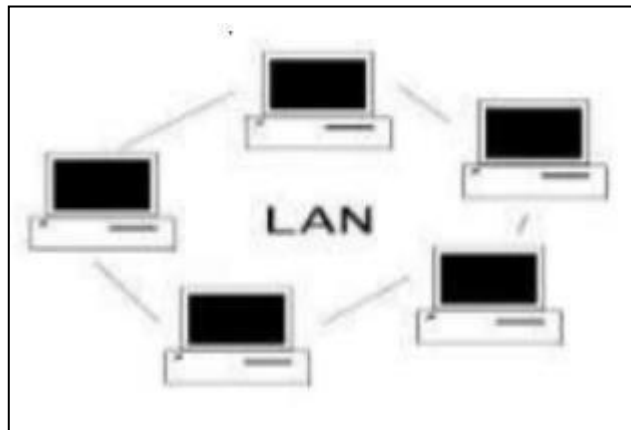
Berdasarkan berbagai pengertian jaringan komputer diatas, maka dapat disimpulkan bahwa Jaringan komputer adalah jaringan telekomunikasi yang memungkinkan antar komputer untuk saling berkomunikasi dengan bertukar data.

Tujuan dari jaringan komputer adalah agar dapat mencapai tujuannya, setiap bagian dari jaringan komputer dapat meminta dan memberikan layanan (service) dan untuk menghindari adanya serangan atau pencurian data pada jaringan komputer,

diperlukan tools atau alat yang bisa menghindari penyusupan atau pencurian data dalam suatu jaringan komputer yang ada di perusahaan.

II.1.1 Jenis Jaringan Komputer

1. Local Area Network (LAN)



Gambar II.1 Jaringan Local Area Network (LAN)

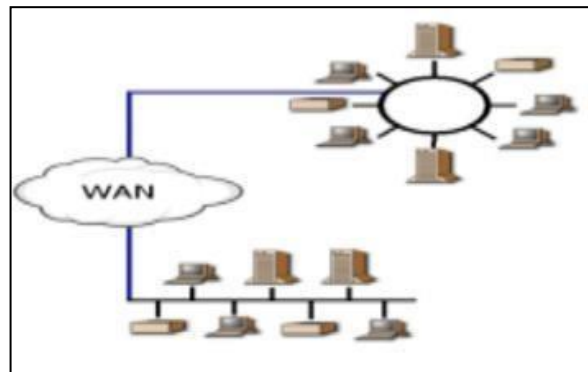
Sebuah LAN adalah jaringan yang dibatasi oleh area yang relatif kecil, umumnya dibatasi oleh area lingkungan, seperti sebuah kantor pada sebuah gedung, atau tiap-tiap ruangan pada sebuah sekolah. Biasanya jarak antar node tidak lebih jauh dari sekitar 200 m [1].

2. Metropolitan Area Network (MAN)

Sebuah MAN biasanya meliputi area yang lebih besar dari LAN, misalnya antar gedung dalam suatu daerah (wilayah seperti provinsi atau negara bagian). Dalam hal ini jaringan menghubungkan beberapa buah jaringan kecil ke dalam lingkungan area yang lebih besar. Sebagai contoh, jaringan beberapa kantor cabang sebuah bank di dalam sebuah kota besar yang dihubungkan antara satu dengan lainnya [1].

3. Wide Area Network (WAN)

Wide Area Network (WAN) adalah jaringan yang biasanya sudah menggunakan media wireless, sarana satelit, ataupun kabel serat optic, karena jangkauannya yang lebih luas, bukan hanya meliputi satu kota atau antar kota dalam suatu wilayah, tetapi mulai menjangkau area/wilayah otoritas negara lain [1].



Gambar II.2 Jaringan Wide Area Network (WAN)

II.2 Vitual Local Area Network (VLAN)

VLAN (Virtual LAN) adalah suatu model jaringan yang membagi jaringan secara logikal ke dalam beberapa VLAN yang berbeda. VLAN tidak terbatas pada kondisi fisik jaringan seperti pada LAN, VLAN dapat di konfigurasi secara virtual tanpa harus melihat kondisi peralatan, sehingga VLAN memiliki fleksibilitas di dalam pengaturan jaringan dan memudahkan administrator jaringan dalam membagi jaringannya sesuai dengan fungsi dan kebutuhan keamanan jaringan tersebut [3].

Dalam bidang lain internet dipakai sebagai penunjang yang sangat penting misalkan perusahaan atau ruangan dengan kantor yang terpisah-pisah maka bisa dibuat akses komunikasi dengan menggunakan jaringan LAN atau VLAN sehinga komunikasi bisa dilakukan dengan cepat. Penambahan teknologi virtual local area network (VLAN) memungkinkan pembuatan jaringan lebih aman dan lebih menghemat device karena jaringan yang berbeda-beda bisa dibuat dalam satu network [3].

Dari berbagai definisi mengenai VLAN diatas, maka bisa disimpulkan bahwa VLAN adalah VLAN merupakan suatu model jaringan yang tidak terbatas pada lokasi fisik seperti LAN, hal ini mengakibatkan suatu network dapat dikonfigurasi secara virtual tanpa harus menuruti lokasi fisik peralatan. Penggunaan VLAN akan membuat pengaturan jaringan menjadi sangat fleksibel serta dapat dibuat segmen yang bergantung pada organisasi atau departemen, tanpa bergantung pada lokasi workstation, VLAN juga akan membuat penggunaan kabel semakin sedikit.

II.3 Komponen Jaringan Komputer

II.3.1 Network Interface Card (NIC)

NIC adalah perangkat keras utama yang harus ada di setiap komputer. NIC bertugas melakukan menyesuaikan tegangan dan arus listrik yang keluar/masuk komputer. Informasi yang melalui media penghantar dapat dikirim/diterima oleh komputer berkat keberadaan NIC. NIC juga mengontrol dataflow antara sistem komputer dengan sistem kabel yang terpasang dan menerima data yang dikirim dari komputer lain lewat media kabel dan menterjemahkannya ke dalam BIT yang dimengerti oleh komputer [4].

II.3.2 Router

Router merupakan perangkat yang dikhususkan untuk menangani koneksi antara dua atau lebih jaringan yang terhubung melalui paket switching. Router bekerja dengan melihat alamat asal dan alamat tujuan dari paket yang melewatinya dan memutuskan rute yang akan dilewati paket tersebut untuk sampai ke tujuan. Router mengetahui alamat masing-masing komputer di lingkungan jaringan lokalnya, mengetahui alamat bridge, dan router lainnya [4].

II.3.3 Switch

Switch pada dasarnya mempunyai fungsi seperti Hub yaitu sebagai pembagi sinyal dan penguat sinyal pada jaringan komputer akan tetapi switch lebih cerdas dari pada Hub karena Switch dapat mengenali alamat data yang harus ditransmisikan dan mampu mengatur lalu lintas data dalam jaringan secara lebih baik dibandingkan dengan Hub. Switch merupakan titik percabangan dari proses transfer data sehingga jika switch mengalami masalah maka seluruh koneksi jaringan dan proses transfer data akan terganggu. Switch biasanya memiliki banyak port yang akan menghubungkan ke jaringan komputer dan port-port tersebut akan berhubungan dengan konektor RJ 45 [4].

II.4 Keamanan Jaringan

Keamanan jaringan atau network security adalah sebuah sistem yang bertugas untuk mengidentifikasi dan mencegah akses tidak sah pada suatu jaringan. Upaya ini bertujuan agar akses penyusup pada sistem jaringan tersebut dapat segera dihentikan. Dengan kata lain, network security mengantisipasi ancaman serangan yang berpotensi merusak sistem keamanan jaringan, baik logic maupun fisik.

Network security sendiri mencakup berbagai jaringan perangkat, baik pribadi maupun jaringan yang bersifat publik. Keamanan jaringan melibatkan access authorization ke data yang ada di dalam suatu jaringan. Sebagai proteksi sumber daya atau network resource, cara paling umum yang biasanya digunakan adalah penggunaan username dan password [5].

Prinsip keamanan jaringan dapat dibedakan menjadi lima, yaitu [5]:

1. Kerahasiaan (secrecy)

Secrecy berhubungan dengan hak akses buat membaca informasi, data serta sesuatu sistem komputer. Dalam perihal ini sesuatu sistem komputer bisa dikatakan nyaman bila sesuatu informasi maupun data cuma bisa dibaca oleh pihak yang sudah diberi wewenang secara legal.

2. Integritas (integrity)

Integrity berhubungan dengan hak akses buat mengganti informasi ataupun data dari sesuatu sistem pc. Dalam perihal ini sesuatu sistem pc bisa dikatakan nyaman bila sesuatu informasi ataupun data cuma bisa diganti oleh pihak yang sudah diberi perihal.

3. Ketersediaan (availability)

Availability berhubungan dengan ketersediaan informasi ataupun data pada dikala yang diperlukan. Dalam perihal ini sesuatu sistem pc bisa dikatakan nyaman bila sesuatu informasi ataupun data yang ada pada sistem pc bisa diakses serta dimanfaatkan oleh pihak yang berhak.

4. Authentication

Aspek ini berhubungan dengan metoda buat melaporkan kalau data betulbetul asli, orang yang mengakses serta membagikan data merupakan benar orang yang diartikan, ataupun server yang kita mendatangi merupakan server yang asli.

5. Akses Kontrol (Access Control)

Aspek kontrol ialah fitur- fitur keamanan yang mengendalikan dimana user berbicara dengan sistem. Akses kontrol melindungi sistem dari akses yang tidak berhak serta biasanya memastikan tingkatan otorisasi sehabis prosedur autentikasi sukses dilengkapi.

II.5 Switch Port Security

Switch port security adalah sebuah trafik control yang bekerja di layer 2 data link, yang berfungsi untuk mendaftarkan dan membatasi perangkat end device mana saja yang dapat terkoneksi pada suatu port di switch tersebut. Suatu keahlian switch manageable dalam meningkatkan keamanan jaringan dengan menggunakan port- port yang terdapat pada switch tersebut. Switch port security dipecah jadi 3 jenis yakni [6]:

1. Default/static port security

Ketika port security ini di fungsikan sampai Macc Address port security hendak diaktifkan pada port switch, sehingga port tidak hendak mem- forward packets apabila source address bukanlah address yang telah kita defenisikan/tentukan sebelumnya. membenarkan alamat mac tertentu yang di perbolehkan buat terhubung ke port tersebut secara manual.

2. Port security dynamic learning

Macc Address di pelajari secara dinamis pada dikala fitur terhubung ke switch, Macc Address tersebut di simpan di Macc Address table.

3. Sticky port security

Suatu keahlian switch dalam memahami Macc Address masing- masing fitur yang tersambung serta hendak memblok tiap Macc Address yang melebihi dari Macc Address yang sudah terdaftar.

II.6 Serangan Keamanan Jaringan

Serangan jaringan (*network attack*) dapat didefinisikan sebagai tindakan tidak sah pada aset digital dalam jaringan komputer sebuah organisasi atau perusahaan. Pihak penyerang biasanya melakukan serangan jaringan untuk mengubah, menghancurkan, atau mencuri data pribadi ataupun data perusahaan. Pelaku dalam serangan jaringan cenderung menargetkan batas jaringan untuk mendapatkan akses ke sistem internal [7].

Bahaya yang mengancam keamanan jaringan umumnya hadir dalam bentuk upaya sabotase atau pencurian data terhadap jaringan komputer. Penyebar ancaman ini adalah pelaku kejahatan siber yang memiliki motif tertentu. Mereka berusaha menyusup ke dalam jaringan dan berusaha menyabotase jaringan komputer sehingga tidak bisa diakses.

Ada pun bentuk ancaman keamanan jaringannya bermacam-macam dan tidak terbatas pada malicious code seperti virus atau trojan horse. Ancaman tersebut bisa juga menimpa fisik atau hardware komputer. Berikut beberapa jenis ancaman dalam sebuah jaringan computer [7].

1. Ancaman Fisik

Jenis ancaman ini masih banyak disepelekan oleh pengguna lantaran mereka berpikir bahwa serangan hanya terjadi pada software. Padahal, ancaman terhadap keamanan jaringan juga muncul pada hardware atau perangkat fisik. Contoh ancaman fisik adalah kerusakan pada software berupa data, file, aplikasi akibat ulah pihak tidak bertanggung jawab. Kerusakan tersebut ternyata mengancam keselamatan hardware kita sehingga tidak bisa berfungsi seperti biasa. Kerugian pada hardware biasanya berupa harddisk rusak, korsleting listrik, gangguan koneksi, dan sebagainya.

2. Virus

Virus adalah program yang dirancang untuk menduplikasi dirinya agar bisa menyusup ke program komputer lain. Virus bisa berasal dari website atau spam e-mail. Virus bekerja untuk merusak data dalam komputer sehingga tidak bisa diakses oleh pengguna.

3. Worm

Sama seperti virus, worm juga bisa berduplikasi sehingga bisa menyebar ke seluruh jaringan internet. Aktivitas duplikasi worm bersifat otomatis dan tidak melibatkan penggunanya. Perbedaannya dengan virus adalah worm tidak menyerang aplikasi lain di komputer.

4. Trojan Horse

Trojan horse merupakan malware atau program berbahaya yang mampu berkamuflase sehingga terlihat normal dan bekerja sesuai keinginan kita. Sumber trojan biasanya berasal dari software yang di-install dalam perangkat. Itulah alasan pentingnya meninjau aplikasi yang ada dalam computer.

5. Eavesdropping

Pada dasarnya, komunikasi antar jaringan memang tidak aman dan rawan dari penyadapan (eavesdropping). Ancaman ini dilakukan oleh pelaku penipuan agar mereka bisa memata-matai alur komunikasi atau transmisi data pada jaringan komputer. Contoh eavesdropping adalah penanaman penyadap suara pada jaringan komputer.

6. Logic Bomb

Ancaman ini muncul dalam bentuk potongan kode yang disusupkan ke dalam software secara sengaja. Logic bomb dirancang atau ditulis oleh orang dalam yang sudah mengetahui seluk-beluk jaringan komputer perusahaan. Karena isinya familier, logic bomb bekerja secara normal padahal mengandung fungsi yang mencurigakan.

7. Spoofing

Teknik ancaman ini dikerjakan oleh pelaku dengan cara memalsukan pengguna agar bisa dipercepat oleh sebuah jaringan. Spoofing dilakukan berkat bantuan beberapa tools, di antaranya URL spoofing yang bekerja dengan cara menampilkan URL palsu dan menyalahgunakan DNS Cache.

8. Sniffing

Sniffing biasanya digunakan oleh hacker untuk mengintip informasi penting seperti username dan password yang dikirim melalui jaringan. Data yang bisa di-sniffing biasanya berupa data yang dikirim melalui jaringan komputer, seperti email, file, dan chat. Sniffing juga bisa digunakan untuk mengintip traffic jaringan, sehingga hacker bisa mengetahui apa saja yang sedang terjadi di jaringan tersebut. Namun, sniffing hanya bisa dilakukan jika hacker bisa mengakses jaringan tersebut. Namun, teknik ini juga bisa digunakan oleh administrator jaringan untuk mencari tahu adanya kegiatan yang tidak diinginkan di jaringan.

9. Denial-of-Service

Ancaman ini menargetkan server website sehingga situs web tidak bisa diakses untuk sementara waktu. Pelaku Denial-of-Service melumpuhkan sistem server dengan cara mengirim traffic sebanyak-banyaknya sampai server tidak mampu menampung request lagi. Ketika server-nya tumbang, pelaku langsung melancarkan aksi pembobolan dan mencuri data di dalamnya.

10. Phishing

Metode ini dilancarkan dengan cara memancing korban agar memberikan informasi atau data pribadinya. Pelaku menyaru sebagai pihak tepercaya agar bisa mencuri akun pengguna dan menyalahgunakannya

11. Man-in-The-Middle

Terakhir, man-in-the-middle melibatkan seorang penyerang yang bekerja menghalangi komunikasi antara pengirim dan penerima pesan. Istilah lainnya, pembicaraan antara kedua belah pihak tersebut harus melalui penyerang tersebut. Kesempatan tersebut menjadi celah bagi penyerang untuk menyadap dan memalsukan komunikasi yang sedang berlangsung.

II.7 Penelitian Terdahulu

Adapun beberapa penelitian sebelumnya yang menjadi referensi bagi penulis untuk melakukan penelitian ini, untuk lebih jelas dapat dilihat pada tabel Penelitian Terdahulu.

Table II.1 Penelitian Terdahulu

No.	Tahun	Penulis	Judul	Hasil Bahasan
1	2018	Oris Krianto Sulaiman	Analisis sistem keamanan jaringan dengan menggunakan switch port security	Berdasarkan uji coba implementasi secara simulasi dengan menggunakan cisco packet tracer 6.2 maka dapat hasil dari penelitian ini: 1. Default/static port security digunakan untuk satu port yang

				<p>akan diblok, pada kemampuan pengamanan ini terbilangsangat minim dikarenakan kemampuan static port security hanya mampu mendaftarkan satu mac-address.</p> <p>2. Port security dynamic learning kemampuan port security dynamic learning mampu mempelajari mac-address hingga 132 mac address namun memiliki kelemahan disisi admin jaringan yang kesulitan untuk mendaftarkan mac address yang akan diizinkan menggunakan jaringan tersebut.</p> <p>3. Sticky port security sangat efisien digunakan karena kemampuannya yang dapat mempelajari secara dynamic mac-address yang akan didaftarkan.</p>
2	2019	Ridatu Ocanita, Muhamad Ryansyah	Implementasi Sistem Keamanan Jaringan Menggunakan Firewall Security Port pada Vitaa MultiOxygen	<p>Jaringan komputer yang berada di gedung Vitta Multi Jakarta adalah sebagai berikut:</p> <ol style="list-style-type: none"> 1. Penerapan sistem keamanan yang digunakan dengan dhcp

				<p>pada ip client sangat mudah merespon koneksi jaringan dan dapat memudahkan user bekerja diseluruh port tempat kerja yang ada.</p> <p>2. Dengan menggunakan Security port, maka system keamanan jaringan diterapkan lebih aman untuk menghindari koneksi jaringan dari akses yang tidak berkepentingan, serta menjaga data tersebut karena dapat dicuri oleh pihak yang tidak bertanggung jawab.</p>
3	2021	Khashaaisha Al Fikri, Djuniadi	Keamanan Jaringan Menggunakan Switch Port Security	<p>Berdasarkan hasil simulasi diperoleh bahwakonfigurasi switch port security menggunakan sticky port security paling efektif dan efisien dilakukan karena dapat mendaftarkan MAC address yang sangat banyak dengan otomatis.</p> <p>Penggunaan violation mode yang paling aman adalah mode shutdown karena koneksi dari perangkat yang tidak dikenal akan langsung</p>

				<p>terputus otomatis. Ini tentu akan meningkatkan keamanan data pada perangkatperangkat yang lain. Walaupun begitu port security merupakan teknik keamanan jaringan paling dasar sehingga perlu dilakukan teknik lanjutan untuk menjaga data yang lebih besar seperti IP source guard, DHCP snooping, dynamic ARP, dll.</p>
4	2022	Sartomo, Wiwin Sulistyo	Model Keamanan Jaringan Menggunakan Firewall Port Blocking	<p>Hasil dari penelitian ini dapat disimpulkan bahwa bahwa keamanan jaringan sangat mudah merespon koneksi jaringan yang digunakan dengan DHCP pada IP client sehingga mempermudah user bekerja di seluruh port-port yang ada. Penerapan keamanan menggunakan firewall port blocking lebih aman digunakan untuk mencegah segala bentuk koneksi jaringan yang dapat diakses, hal tersebut untuk menjaga keamanan data yang menjadi hal utama untuk mencegah terjadinya pencurian.</p> <p>Penerapan firewall security port dapat melakukan aksi block pada koneksi jaringan tersebut ketika terjadi perpindahan hak akses.</p>
5	2023	Nursalima Ishak, Sahriar Hamza,	Analisis Keamanan Jaringan Menggunakan	<p>Hasil dari penelitian yang di lakukan penulis pada warnet gramit adalah bahwa dengan melakukan pengujian port</p>

		Mustamin Hamid	Switch Port Security Pada warnet Gramit Kelurahan Sasa Ternate Selatan	terhadap PC server, client dan CCTV terkoneksi dan terhubung dengan baik setelah pengujian ping dilakukan, hal ini di perkuat dengan keterangan bahwa status ping berhasil dengan paket loss 0%.
--	--	-------------------	--	--

Berdasarkan rujukan dari penelitian-penelitian yang dilakukan sebelumnya, penelitian yang dilakukan oleh peneliti tidak jauh berbeda dengan penelitian sebelumnya yaitu mengimplementasikan sistem keamanan jaringan dengan Metode NDLC menggunakan port switch security di PT Pinus Merah Abadi dengan menggunakan metode static port security. Untuk memudahkan administrator jaringan dalam meningkatkan keamanan pada perangkat yang ada di laboratorium jaringan, maka perlu melakukan pengamanan jaringan lokal yaitu salah satunya dengan menerapkan sistem keamanan security port pada Cisco switch dan perbedaannya akan dilakukan simulasi keamanan jaringannya menggunakan aplikasi Cisco Packet Tracer.

BAB III METODE PENELITIAN

III.1 Gambaran Umum Objek Penelitian

Berdasarkan pendahuluan dan tinjauan Pustaka pada bab sebelumnya, penelitian yang akan dilakukan adalah simulasi *switch port security* sebagai keamanan jaringan di PT Pinus Merah Abadi yang sebelumnya hanya berupa *firewall*.

Masalah jaringan yang sering dialami PT Pinus Merah berdasarkan wawancara dan pengamatan atau observasi penulis adalah seringnya terjadi kesalahan data yang tidak sesuai dengan tugas masing-masing divisi yang ada di perusahaan.

III.2 Metode Pengumpulan Data

Pada penelitian ini akan menggunakan metode pengumpulan data berupa wawancara, observasi, studi pustaka dan dokumentasi.

Wawancara adalah metode dalam pengumpulan data yang dilakukan dengan cara melakukan percakapan antar dua orang atau lebih dan berlangsung antara narasumber dan pewawancara. Tujuannya adalah mendapatkan informasi secara langsung dengan memberikan sebuah pertanyaan yang sudah dipersiapkan sebelumnya dengan menemukan permasalahan yang terjadi.

Observasi ialah sebuah metode yang dilakukan dengan mengamati sebuah proses permasalahan yang terjadi dengan peneliti mencatat semua informasi yang didapat secara langsung dari pengamatan tersebut. Oleh karena itu penulis akan melakukan wawancara dan observasi di PT Pinus Merah Abadi.

Studi Pustaka merupakan cara pengumpulan data yang dilakukan dengan cara membaca dan mempelajari buku-buku, makalah ataupun referensi lain yang berhubungan dengan masalah yang dibahas.

III.2.1 Data Primer

1. Data Simulasi

Penulis mengumpulka data-data simulasi dengan melakukan serangan jaringan menggunakan simulator *Cisco Packet Tracer ver 8.2*. Simulasi sistem jaringan yang digunakan merupakan hasil dari studi literatur sejenis. Data hasil simulasi ini kemudian dianalisis untuk menguraikan kebutuhan keamanan system jaringan dalam memenuhi kriteria keamanan jaringan yang dibutuhkan. Hasil anlisis ini akan dijadikan penulis sebagai hasil penelitian.

III.2.2 Data Sekunder

1. Data Wawancara

Penulis mengumpulkan data wawancara dengan beberapa karyawan PT Pinus Merah Abadi terkait kebutuhan keamanan jaringan, permasalahan yang terjadi. Kemudian data wawancara tersebut digunakan menjadi landasan penulis melakuka penelitian.

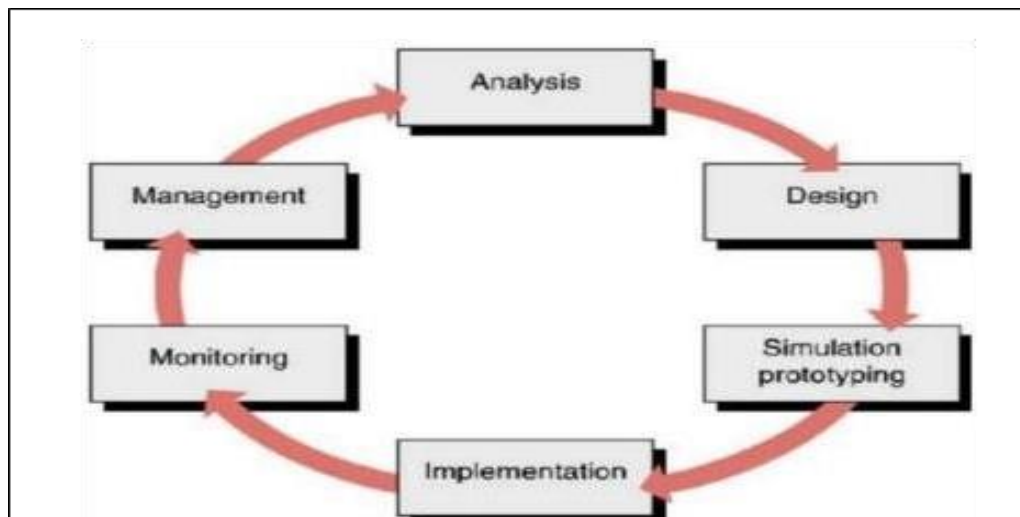
2. Studi Pustaka

Penulis melakukan pengumpulan data dengan cara studi Pustaka yang mana referensi-refeensi tersebut diambil dari jurnal, thesis, *e-book*, maupun secara online lainnya. Hasil referensi tersebut dapat digunakan dalam Menyusun landasa teori, metodologi penelitian, menentukan simulasi jaringan dan aplikasi yang digunakan serta cara melakukan simulasi. Salah satu pengumpulan data yang dilakukan penulis dengan studi Pustaka, yakni studi literatur dimana bisa dilihat pada Table II.1 Penelitian Terdahulu pada Bab II.

III.3 Metode Network Development Life Cycle (NDLC)

Network Development Life Cycle (NDLC) merupakan sebuah metode yang bergantung pada proses pembangunan sebelumnya seperti perencanaan strategi bisnis, daur hidup pengembangan aplikasi, dan analisis pendistribusian data [8].

Metode tersebut terdiri dari analysis, design, simulation prototype, implementation, dan monitoring. Berikut merupakan tahapan dari metode NDLC sebagai berikut [8]:



Gambar II.1 Network Development Life Cycle (NDLC)

Adapun penjelasan dari tahapan diatas yaitu sebagai berikut:

1. Tahap Analysis, Tahapan awal yang dilakukan dalam menganalisis adalah analisa kebutuhan, analisa permasalahan yang ada, analisa keinginan user, dan analisa topologi jaringan yang sudah ada, bisa dibidang tahapan ini adalah tahapan pengumpulan data yang dibutuhkan untuk perumusan masalah dalam menyelesaikan kendala yang ada. Dengan mengidentifikasi sistem jaringan yang sedang berjalan lalu mencoba untuk menganalisa suatu pengembangan sistem seperti apa yang akan diterapkan pada sistem tersebut.

2. Tahap Design, Tahap ini dari data-data yang didapatkan sebelumnya, tahapan desain ini penulis akan membuat desain gambar topologi jaringan yang akan dibangun, desain akses data dan sebagainya
3. Tahap Simulation Prototype, Tahap ini melakukan pengembangan jaringan yang akan membuat dalam bentuk simulasi dengan bantuan tools Cisco Packet Tracer. Hal ini dimaksudkan untuk melihat kinerja dari network yang akan dibangun dan menjadi bahan presentasi dan sharing dengan pengembangan system jaringan
4. Tahap Implementation, Tahap ini akan sedikit memakan waktu lama. dalam melakukan implementasi, penulis telah menerapkan semua yang direncanakan dan dirancang sebelumnya. Pada tahapan ini akan terlihat bagaimana pengembangan yang akan dibangun akan memberikan pengaruh terhadap system yang ada.
5. Tahap Monitoring, Tahap ini Setelah diimplementasi, tahapan monitoring merupakan tahapan penting agar jaringan dan komunikasi dapat berjalan sesuai dengan keinginan dan tujuan penulis pada tahap awal analisis. Penulis akan menggunakan tools yang berfungsi untuk memonitor lalu lintas jaringan
6. Tahap Management, Tahap ini salah satu yang menjadi perhatian khusus adalah masalah kebijakan, yaitu dalam dalam hal aktivitas, pemeliharaan dan pengelolaan dikategorikan pada tahap ini. Kebijakan perlu dibuat untuk membuat dan mengatur agar sistem yang telah dibangun dan berjalan dengan baik dapat berlangsung lama dan unsur reliability terjaga.

III.4 Alat Pnenelitan

Adapun alat atau perangkat yang diperlukan dalam penelitian ini adalah:

III.4.1 Perangkat Keras (*Hardware*)

Alat dari perangkat keras atau *Hardware* yang akan digunakan pada penelitian ini adalah:

1. Laptop Core II3 (RAM 4GB DDR3, HDD 1TB)

2. Modem
3. PC / Laptop Client (Processor Dual Core, RAM 2GB, HDD 500GB)

III.4.2 Perangkat Lunak (*Software*)

Alat dari perangkat lunak atau *Software* yang akan digunakan pada penelitian ini adalah:

1. Cisco Packet Tracer 8.2

III.5 Skema Penelitian

Sesuai dengan penjelasan keamanan jaringan pada Bab II, Keamanan jaringan merupakan sistem yang bekerja untuk pencegahan aktifitas yang tidak diinginkan dengan melakukan identifikasi pengguna yang tidak memiliki hak akses dalam suatu jaringan. Menghubungkan komputer dengan komputer lain baik menggunakan jaringan kabel atau nirkabel memungkinkan orang lain untuk mengakses data, mengubah isi, sampai menghapus data dalam jaringan tersebut.

Pengontrolan keamanan jaringan dapat dilakukan dengan menyesuaikan *network sharing properties* pada komputer, hal ini membatasi folder dan file yang hanya dapat dilihat oleh pengguna tertentu. Hal ini mengakibatkan pengguna yang tidak terdaftar tidak dapat melihat folder/file tersebut [6].

Adapun skema penelitian yang akan dilakukan pada penelitian ini adalah sebagai berikut:

III.5.1 Analisis Jaringan

Analisis keamanan jaringan perlu dilakukan supaya bisa mengetahui tingkat atau status keamanannya. Ada empat tahap awal dalam melakukan analisis tersebut, yaitu [7]:

1. Vulnerability

Aktivitas ini mencakup analisa jaringan komputer yang sedang berjalan bertujuan untuk mendeteksi bagian dari sistem yang rawan terhadap serangan.

Berdasarkan data observasi penulis, PT Pinus Merah abadi memiliki 3 divisi pembagian hak akses jaringan, yaitu divisi Administrasi, Divisi Keuangan, dan Manager. Dimana PT Pinus Merah Abadi ini memiliki 1 buah ISP untuk memberikan layanan internet kepada pengguna. Terdapat 1 buah router, 2 buah switch, 1 access point di gedung A dan 1 access point di gedung B. Jenis keamanan yang sudah berlaku di PT Pinus Merah Abadi adalah dengan mengandalkan *firewall*. Serangan yang datang hanya bisa dideteksi dan memunculkan peringatan tanpa adanya identifikasi pelaku serangan dan juga pengamanan dengan aplikasi deepfreeze pada PC yang bisa digunakan oleh pengguna. Padahal serangan yang masuk dapat membahayakan data-data di dalam *database* perusahaan maupun sistem yang berlaku disana.

2. Threat

Threat merupakan aktivitas yang bertujuan untuk mempelajari ancaman atau serangan dari luar atau dalam jaringan komputer.

Pada jaringan komputer PT Pinus Merah Abadi, metode penyerangan yang terjadi adalah *Sniffing* dan *DoS (Denial of Service)*. Sniffing adalah bentuk cybercrime dimana pelaku mencuri username dan password orang lain secara sengaja maupun tidak sengaja. Pelaku kemudian dapat memakai akun korban untuk melakukan penipuan atas nama korban atau meusak/menghapus data milik korban. Sering kali dilakukan dengan program sniffer yang berfungsi sebagai penganalisis jaringan dan berkerja untuk memonitor jaringan computer. Program tersebut mengatur kartu jaringan (LAN Card) untuk memonitor menangkal semua lalu lintas

paket data yang melalui jaringan, tanpa mepedulikan kepada siapa paket data yang melalui jaringan, dan tanpa kepada siapa paket data tersebut di kirimkan.

Kemudian DoS adalah serangan dimana pihak penyerang mengirimkan request berkali-kali untuk menyibukkan server hingga rusak atau hang. Setelah itu penyerang akan dengan mudah mengambil atau merusak data dari jaringan tersebut.

DoS merupakan serangan yang terbilang cukup kuat untuk melukai sebuah infrastruktur dari suatu organisasi. Serangan ini bertujuan untuk mencegah pengguna menikmati layanan yang diberikan suatu server. Ciri-ciri jaringan yang terkena Serangan DoS adalah sebagai berikut [9]:

- a. Merusak layanan yang disediakan, sehingga layanan menjadi tidak tersedia.
- b. Pihak yang tidak berwenang berusaha memperoleh akses sistem, tujuan seperti ini adalah gambaran klasik dari seorang hacker. Mereka biasanya berusaha mencapai tujuannya keluar dari sistem dengan melakukan beberapa pengrusakan pada sistem, kemudian melaporkan ke administrator bahwa ada “bug” ditemukan dalam sistem.
- c. Berusaha mengakses informasi yang dibatasi pengaksesannya (restricted), informasi yang sensitif.
- d. Adanya penggunaan bandwidth yang mencurigakan
- e. Kecepatan respon website. Seperti tiba-tiba sulit diakses atau menjadi tidak responsive.
- f. Load CPU meningkat drastis tanpa ada eksekusi request apapun

3. Impact

Tindakan ini memeriksa pengaruh (*impact*) dari serangan atau ancaman yang terjadi dalam sebuah jaringan.

Serangan *Sniffing* dan *DoS (Denial of Service)* pada jaringan komputer PT Pinus Merah Abadi melemahkan atau membuat kurang optimal jaringan komputer ketika di serang oleh penyusup atau hacker dan cracker untuk kepentingan atau keuntungan pihak lain. Penyusup baik berupa hacker dan cracker selalu mencoba untuk mendapatkan akses dari sebuah sistem keamanan. Intrusi merupakan aktifitas ketika orang yang tidak berhak mencoba untuk mendapatkan akses atau mengganggu operasi normal.

Setelah melakukan observasi terhadap kegiatan jaringan yang ada di perusahaan, gejala jaringan komputer pada PT Pinus Merah Abadi yang terkena serangan adalah:

- a. Kecepatan akses jaringan lemot, sulit membuka aplikasi transaksi di perusahaan dan menjadi tidak responsive.
- b. Akun pada beberapa pengguna aplikasi perusahaan tidak bisa dibuka karena informasi akun pengguna berubah.
- c. Hak akses pada masing-masing pengguna bisa dibuka oleh pengguna lain yang tidak sesuai wewenang atau hak aksesnya.

4. Frequency

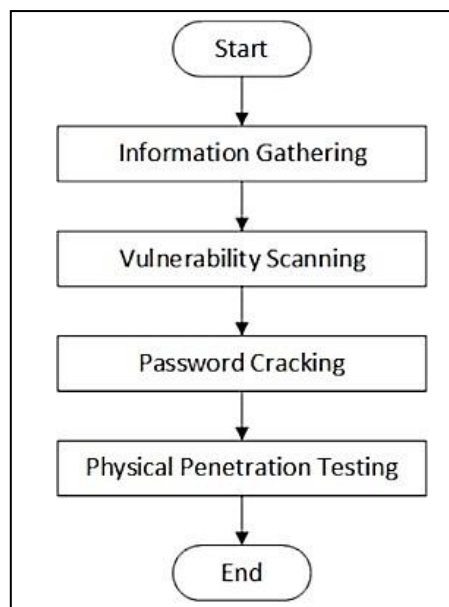
Langkah analisis ini mencatat frekuensi atau seberapa sering suatu serangan muncul dalam jangka waktu tertentu. Tahapan ini akan dibahas lebih jelas pada Bab IV.

5. Recommended Countermeasures

Langkah ini merupakan tahap terakhir setelah melakukan keempat analisis di atas. Dalam tahap ini, harus menyusun langkah pencegahan terhadap serangan tersebut sehingga berguna sebagai pedoman untuk meningkatkan keamanan jaringan.

III.5.3 Penetration Testing

Penetration Testing pada gambar di bawah Teknik yang digunakan dalam demo simulasi serangan dapat dikatakan merupakan salah satu komponen penting dari Security Audit. Langkah-langkah dalam Penetration Testing [10].

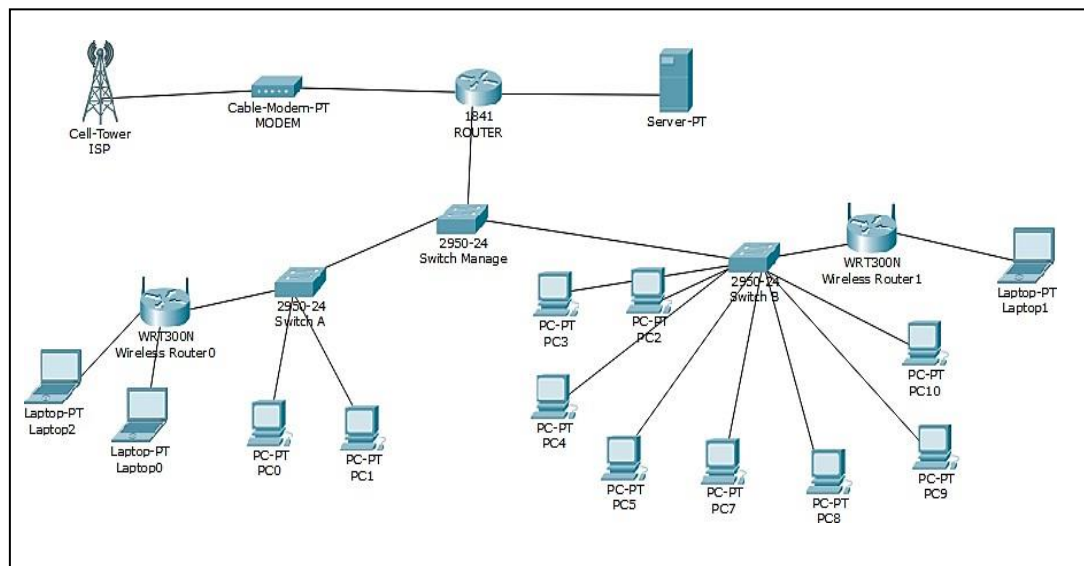


Gambar III. 2 Flowchart Alur Pengujian Penelitian Penetration Testing

- a. Langkah pertama yang dilakukan pada Pentest adalah perencanaan. Pada tahapan ini harus dibicarakan ruang lingkup pentest, range waktu, dokumen legal (kontrak), jumlah tim yang dibutuhkan serta apakah staff dan karyawan diberitahukan terlebih dahulu atau tidak tentang adanya pentest.
- b. Langkah berikutnya adalah information gathering dan analysis. Pada tahapan ini dikumpulkan semua informasi tentang sistem target. Ada banyak alat bantu

yang bisa digunakan, diantaranya adalah www.netcraft.com. Kemudian dilakukan network survey untuk mengumpulkan informasi domain, server, layanan yang ada, ip adress, host, adanya firewall, dll. Tools yang dapat digunakan misalnya Nmap.

- c. Langkah selanjutnya adalah vulnerability detection (pencarian celah keamanan). Setelah mengetahui informasi tentang sistem, pencarian celah keamanan bisa dilakukan manual atau secara otomatis misalnya dengan Nessus.
- d. Setelah menemukan celah keamanan, maka langkah berikutnya adalah percobaan penyerangan (penetration attempt). Pada proses ini dilakukan penentuan target, pemilihan tools dan exploit yang tepat. Umumnya diperlukan juga kemampuan password cracking. Cara lain yang dapat dilakukan adalah dengan melakukan social engineering dan pengujian physical security dari sistem.
- e. Tahap berikutnya adalah analisis dan pembuatan laporan. Disini biasanya dilaporkan tentang langkah kerja yang dilakukan, celah keamanan yang ditemukan serta usulan perbaikan. Tahapan selanjutnya biasanya tindak lanjut, yang biasanya harus dilakukan bersama-sama dengan admin untuk memperbaiki sistem.



Gambar III. 3 Topologi Jaringan PT Pinus Merah Abadi (Sekarang)

Setelah penulis melakukan penelitian di PT Pinus Merah Abadi penulis dapat menggambarkan rangkaian dari jaringan komputer local area network yang terdapat dilokasi tersebut, sesuai dengan kebutuhan jaringan komputer-komputer Client atau yang dinamakan dengan Workstation, alur dari jaringan yang di terapkan pada perusahaan meliputi workstation dari tiap-tiap divisi yang ada di PT Pinus Merah Abadi.

Namun jika pemberian alamat IP dilakukan secara statik akan membuat hasil yang negatif terhadap admin jaringan, sebab menghasilkan waktu yang lama untuk pemberian alamat IP. Tetapi masalah ini dapat di tangani dengan memilih pemberian alamat IP menggunakan DHCP. *Dynamic Host Configuration Protocol* (DHCP) adalah salah satu metode pemberian alamat IP otomatis, PC akan meminta IP yang benar dari router. Setting DHCP dapat dilakukan pada router dengan menggunakan CLI (Command Line Interface). Dengan DHCP administrator jaringan tidak memerlukan waktu untuk memikirkan host IP yang akan digunakan karena sudah disediakan router secara otomatis. Admin jaringan hanya memilih DHCP atau obtain IP Address Automatically pada pemberian alamat IP.

Langkah Awal Skenario Pengujian

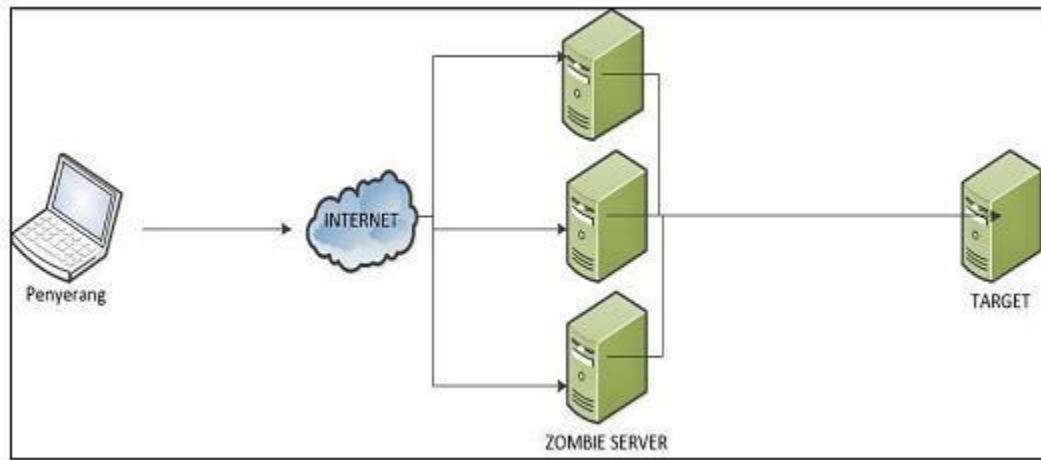
- a. Dilakukan Penetration testing dengan menggunakan Ping untuk mencari IP domain dengan menggunakan command prompt (CMD) yang akan di jadikan target dengan tujuan untuk mendapatkan IP address yang terdeteksi. Setelah itu pihak penyerang sebagai Attacker mengecek Port terbuka dengan menggunakan tools Drakfantasy sebagai Open Sources, dengan dasar agar mendapatkan target yang akan di serang/Attacing, penyerang untuk mengetahui agar port-port mana saja terbuka pada jaringan dengan menggunakan NAMP.
- b. Lakukan Analisa Penetration testing kedua untuk scanning port dengan Hack Tool dengan menggunakan Drakfantasy untuk Scanning port Enter Host Site or movie name domain untuk mengetahui port-port mana saja yang terbuka, apabila tersecanning pada hack tool teridentifikasi sehingga pihak hacker akan memasukkan IP domain dengan DoS sebagai Strassing Attacker berupa paket flooding yang akan terkirim attacker (penyerang).
- c. Loic sebagai penyerangan dari metode TCP target port-port yang sudah terbuka untuk di serang.
- d. Melakukan pengujian dan pengecekan pada lalu lintas log IP DNS yang telah diuji diawal dengan menyerang ip target dan secanning dengan membuka testing Wireshark sebagai Captrure log yang masuk pada beberapa tool Drakfantasy, loic IP DNS yang berjalan.
- e. Komputer pengguna dihubungkan model bintang (star) dengan switch kemudian berturut-turut dihubungkan dengan router kemudian dibuat firewall sebagai sistem pengaman dan yang terakhir dihubungkan dengan internet. Jaringan tersebut dapat diakses baik dari dalam maupun dari luar jaringan komputer PT Pinus Merah Abadi.
- f. Untuk simulasi serangan jaringan computer diserang menggunakan serangan DoS dengan software LOIC. Serangan dilakukan dengan memasukan IP Address target pada baris "IP" dan menekan tombol "Lock

on”, kemudian memilih menu “methode” ada 3 pilihan yaitu “TCP”, “UDP”, dan “HTTP”. LOIC siap untuk melakukan serangan menuju target yaitu layanan jaringan PT Pinus Merah Abadi.

Jaringan komputer objek tidak aman karena masih bisa terserang dengan serangan DoS. Pencegahan dari serangan DoS menggunakan Snort. Snort merupakan tool atau aplikasi open source dari Intrusion Detection System (IDS). Snort dirancang untuk beroperasi pada command line dan telah diintegrasikan ke beberapa aplikasi pihak ketiga serta mendukung cross platform. Snort menganalisis semua lalu lintas jaringan untuk melakukan sniffing dan mencari beberapa jenis penyusupan maupun serangan dalam sebuah jaringan.

- a. Sniffer mode: untuk melihat paket yang lewat di jaringan.
- b. Packet logger mode: untuk mencatat semua paket yang lewat di jaringan untuk di analisa di kemudian hari.
- c. Intrusion Detection mode: pada mode ini snort akan berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan komputer.

Bentuk penyerangan tujuan dimana Loic dan drakfantasy sebagai tools Strassing/Attacing adalah sebelum penyerangan model sistem penyerangan yang bersifat system *Opensource* yang dijalankan dengan menggunakan tools Drakfantasy dengan membuka domain IP yang dituju sehingga keluarlah port-port yang terbuka yang akan diserang dengan menggunakan DoS pada tools sebagai strassing/Attacing untuk meflooding dengan jumlah paket yang akan diserang. Dalam sistem menganalisis dari penelitian penyerangan diharapkan sistem bekerja dengan baik pada suatu jaringan yang ditunjukkan pada Gambar dibawah ini.



Gambar III. 4 Attacing/Strassing dengan DoS

Pada Gambar III.4 Attacing/Strassing dengan DoS di ilustrasikan bahwa, DDOS sendiri merupakan jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (*resource*) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut. Gambar diatas memperlihatkan serangan DoS dimana penyerang menggunakan komputer zombie untuk menyerang.

Dalam sebuah serangan DoS penyerang atau hacker akan mencoba untuk mencegah akses seorang pengguna terhadap sistem atau jaringan, Membanjiri lalu lintas jaringan dengan mengirim banyak data sehingga membuat lalu lintas jaringan yang datang dari pengguna menjadi tidak dapat masuk ke dalam sistem jaringan dan akan mengganggu komunikasi antara sebuah host dan kliennya yang terdaftar dengan menggunakan banyak cara, termasuk dengan mengubah informasi konfigurasi sistem atau bahkan merusakkan fisik terhadap komponen dan server pada target yang akan di tuju.

III.5.2 Pencegahan Serangan

Solusi dari permasalahan keamanan jaringan ini adalah dengan *switch port security* yaitu dengan membatasi jumlah perangkat yang tersambung dengan port pada sebuah switch dan menentukan perangkat mana saja yang dapat tersambung pada port tersebut. *Switch port security* sendiri bekerja dengan mendaftarkan MAC address dari perangkat yang dapat tersambung dengan jaringan tersebut. Terdapat tiga jenis switch port security, yaitu [6]:

- Default/static port security
- Dynamic Port security
- Sticky port security

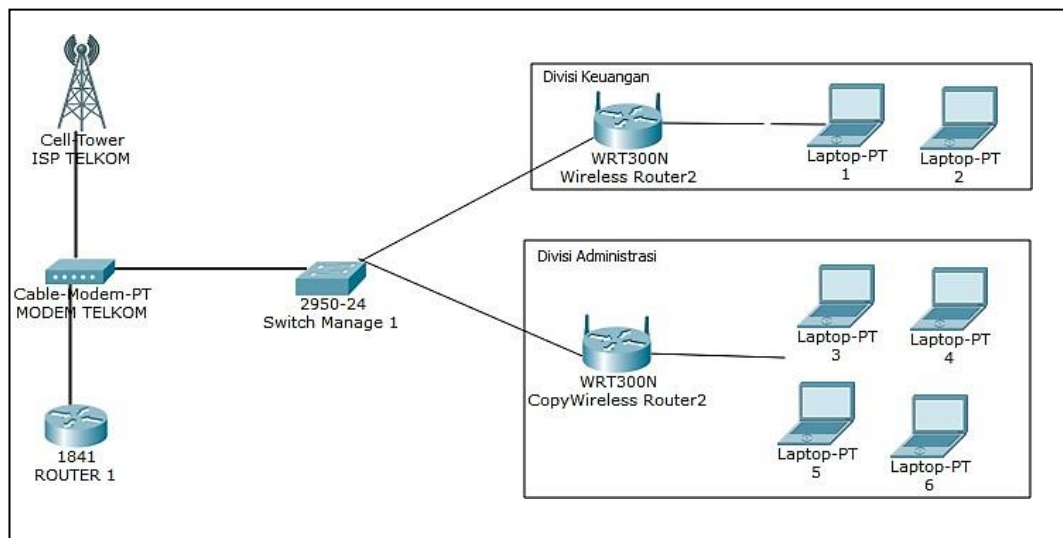
Pada interface port sendiri dapat diberlakukan sistem keamanan yang disebut *violation mode* yaitu tindakan yang akan dilakukan port ketika terdeteksi akses dari perangkat yang tidak terdaftar MAC addressnya. *Violation mode* sendiri ada tiga, yaitu:

1. Protect: Pada mode protect, interface akan membuang (*drop*) paket data yang dikirim oleh perangkat yang tidak terdaftar tersebut. Outputnya akan menghasilkan request timed out saat dilakukan ping. Jadi data yang dikirimkan akan terhenti saat itu juga.
2. Restrict: Interface yang menggunakan violation ini akan membuang (*drop*) paket data seperti pada mode protect. Bedanya interface akan menghitung berapa jumlah violation yang terjadi. Jumlah ini berfungsi sebagai penanda berapa kali terjadi serangan dari pihak yang tidak terdaftar.
3. Shutdown: Interface yang menggunakan mode ini akan seketika menonaktifkan port yang digunakan perangkat yang tidak memiliki hak akses. Ketika host mengirim paket data otomatis port akan melakukan shutdown/mati.

Dengan menggunakan port security, keamanan jaringan bisa lebih ditingkatkan dan ancaman dari host yang tidak dikenal dapat diminimalisir. Untuk selanjutnya akan saya bahas mengenai konfigurasi port security menggunakan cisco packet tracer.

Usulan Topologi Jaringan

Pada penelitian ini penulis mencoba untuk menggambarkan dalam bentuk simulasi jaringan usulan tersebut menggunakan software simulator. Software yang penulis gunakan adalah Cisco Packet Tracer.



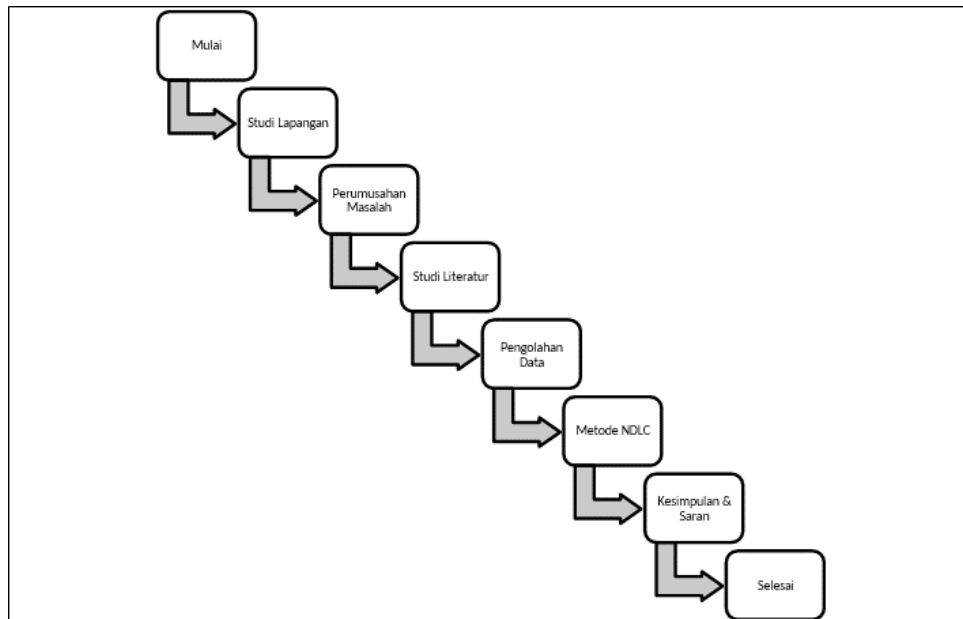
Gambar III. 5 Topologi Jaringan PT Pinus Merah Abadi (Usulan)

Topologi yang akan di gunakan dalam bentuk Gambar dan simulasi adalah topologi star. Hasil dari perancangan jaringan komputer dapat dilihat pada Gambar, dimana Switch akan dikonfigurasi tanpa menggunakan DHCP. Penelitian ini dimulai dengan observasi dan pemilihan tools yangsesuai dengan sistem, tools yang digunakan adalah Drakfantasy, Loic, dan Snort. Selanjutnya dilanjutkan dengan dimulainya stress testing dilanjutkan dengan analisa hasil pengujian untuk diterapka

dalam solusi switch port. Setelah keaman jaringan menggunakan switch port berhasil, maka akan dilakukan implementasi ke jaringan di PT Pinus Merah Abadi.

III.6 Tahapan Penelitian

Tahapan penelitian merupakan suatu bentuk tahapan berpikir yang dapat digunakan sebagai pendekatan dalam pemecahan masalah. Metode penelitian yang digunakan yaitu metode eksperimen dimana dilakukan percobaan atau simulasi menggunakan aplikasi Cisco Packet Tracer. Adapun tahapan penelitian yang digunakan dalam penelitian ini adalah sebagai berikut:



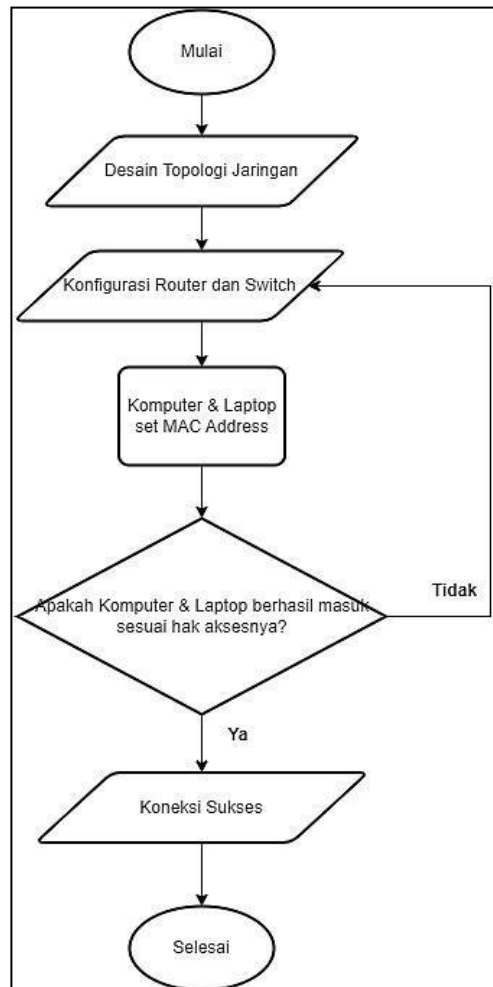
Gambar III. 6 Tahapan Penelitian

Tahapan penelitian yang ada pada Gambar III.6 akan dijelaskan dalam uraian berikut:

- a. Persiapan awal penelitian, tahap ini merupakan tahap studi lapangan melihat secara langsung bentuk jaringan komputer yang ada di PT Pinus Merah Abadi, kemudian menyusun rumusan masalah yang ditemukan di lapangan

dan dilanjutkan dengan studi literatur yang berkaitan dengan topik dalam penelitian.

- b. Pengumpulan Data. Pengumpulan data dilakukan dengan cara observasi yaitu dengan mengamati secara langsung jaringan komputer serta topologi jaringan yang sedang berjalan. Selain itu, ada tahap pengumpulan data dengan cara wawancara secara langsung dengan para pihak terkait guna memberikan informasi terkait permasalahan yang dihadapi perusahaan dan kebutuhan jaringan komputer yang diinginkan.
- c. Metode NDLC. Network Development Life Cycle (NDLC) merupakan suatu metode yang digunakan dalam mengembangkan atau merancang jaringan untuk mengetahui kinerja jaringan. Metode ini bersifat *continuous improvement* dimana hasil dari analisa ini akan terus dijadikan bahan pertimbangan untuk melakukan perbaikan terus menerus. Langkah- langkah dari NDLC sudah dijelaskan pada subbab sebelumnya.
- d. Setelah selesai tahapan NDLC dilakukan, maka bisa ditarik kesimpulan dari implementasi keamana jaringan dan saran sebagai pengembangan keamanan jaringan di kemudian hari.



Gambar III. 7 Flowchart Bangun Jaringan

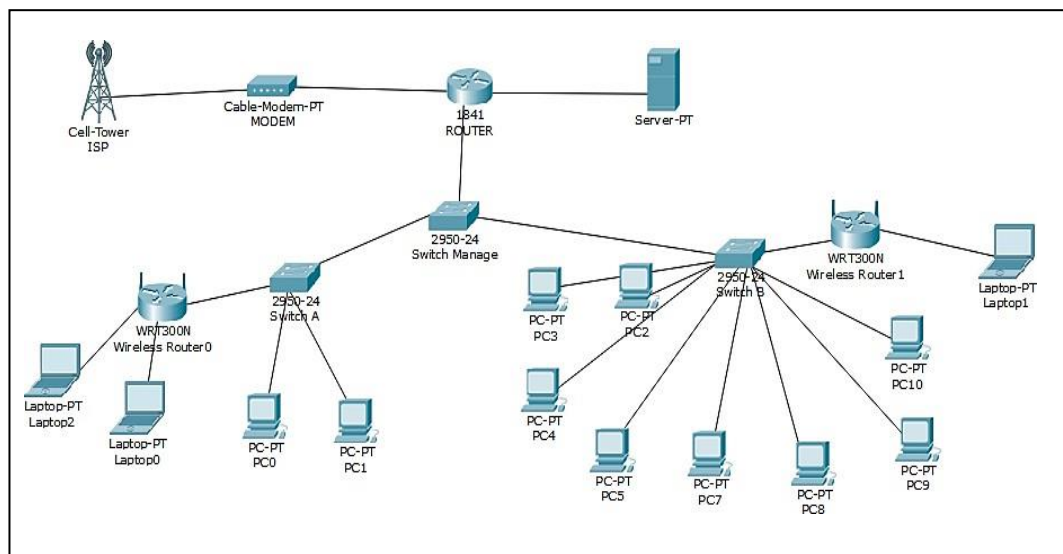
Pada flowchart penelitian, akan dilakukan desain topologi jaringan terlebih dahulu, dan kemudian dilanjutkan dengan proses mengkonfigurasi router dan switch, kemudian memasukkan data MAC Address dari masing-masing perangkat yang ada di ruangan yaitu komputer dan laptop ke dalam konfigurasi jaringan, kemudian melakukan validasi apakah MAC address yang telah didaftarkan ke dalam konfigurasi jaringan berhasil masuk atau tidak. Apabila berhasil masuk, maka koneksi dinyatakan berhasil dan keamanan jaringannya berhasil di konfigurasi. Namun, apabila MAC address perangkat yang telah didaftarkan gagal masuk, maka dilakukan pengecekan ulang atau mengkonfigurasi kembali router dan switchnya.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menjelaskan tahapan dari metode NDLC yang juga akan ada pembahasan mulai dari skenario penyerangan jaringan, simulasi pengamanan jaringan dan pengajuan penyesuaian ulang jaringan sesuai dengan solusi keamanan jaringan yang telah dilakukan.

IV.1 Analisis Jaringan Berjalan

Analisis jaringan berjalan berisi topologi jaringan yang merupakan tahapan dari metode NDLC. Topologi jaringan pada PT PMA sudah mempunyai topologi jaringan berjalan. Topologi Jaringan yang digunakan oleh PT PMA adalah Topologi Star. Berikut ini topologi yang ada pada PT PMA.



Gamba IV. 1 Topologi Berjalan PT Pinus Merah Abadi

Berdasarkan konsep gambar diatas, PT PMA menggunakan router sebagai router utamanya lalu switch unmanageable lah yang membagikan akses internet kepada client dengan settingan DHCP sehingga setiap client mendapatkan IP secara otomatis.

PT Pinus Merah Abadi sekarang ini sedang menggunakan dua jenis aplikasi untuk kegiatan perusahaan yang hanya bisa dibuka dalam lingkungan jaringan PMA saja. Aplikasi yang digunakan yaitu aplikasi distribusi untuk pengelolaan stok barang dan juga aplikasi keuangan.

IV.2 Pembuatan Skenario

Sebagai penunjang pada penelitian yang dilakukan, maka diperlukan suatu skenario dalam melakukan eksperimen sampai pengambilan data. Skenario ini disesuaikan dengan kondisi lingkungan yang diinginkan. Secara umum, antinya skenario akan dilihat pada kondisi tanpa serangan, ngadat dan down. Skenario dibagi menjadi dua yaitu scenario untuk komputer dan penyerang.

IV.2.1 Skenario Komputer

Skenario untuk komputer yang diserang diperlukan karena hasil dari sebelum dan sesudah diserang. Hal yang perlu di lakukan pada komputer terserang adalah menangkap data pada traffic jaringan. Skenario untuk kompuer yang akan dibuat adalh dengan memperhatikan factor:

- Waktu

Skenario perlu dibuat menyesuaikan waktu antara pelaku dan penulis. Waktu yang cocok untuk melakukan dalam mendefinisikan kondisi tanpa serangan adalah pada saat jam kerja. Jam kerja yang dimaksud adalah pukul 08.00 – 16.00. karena pada saat itu para karyawan menggunakan jaringan untuk melakukan kegiatan.

- Perlakuan pada komputer

Perlakuan pada komputer bertujuan untuk mengetahui kinerja yang bisa dilakukan. Perlakuan yang dilakukan komputer tidak di install firewall, diinstal firewall, dan di konfigurasi.

- Lingkungan

Komputer diletakkan pada ruang kerja PT Pinus Merah Abadi lantai 1 Divisi keuangan yang tersambung dengan jaringan.

- IP Address

IP Address pada server dibuat static agar dapat dimasukkan ke dalam jaringan Telkom. IP Address dari komputer adalah 10.126.10.70.

IV.2.2 Skenario Penyerang

Penyerang juga perlu diperhatikan beberapa faktor untuk kelengkapan penelitian. Pada penyerang ada beberapa faktor yaitu:

- Waktu

Maksud dari waktu untuk scenario penyerang adalah waktu yang cocok untuk melakukan simulasi penyerangan ke komputer. Dikarenakan penggunaan jaringan PT Pinus Merah Abadi pada jam kerja terlalu padat, maka penyerangan dilakukan setelah jam kerja atau sekitar jam 5 sore sampai jam 6 pagi.

- Jumlah Threads

Jumlah Threads bertujuan untuk membatasi serangan DoS yang diberikan kepada komputer. Jumlah Threads ini dibuat tetap yaitu 10 Threads.

- Tipe Serangan

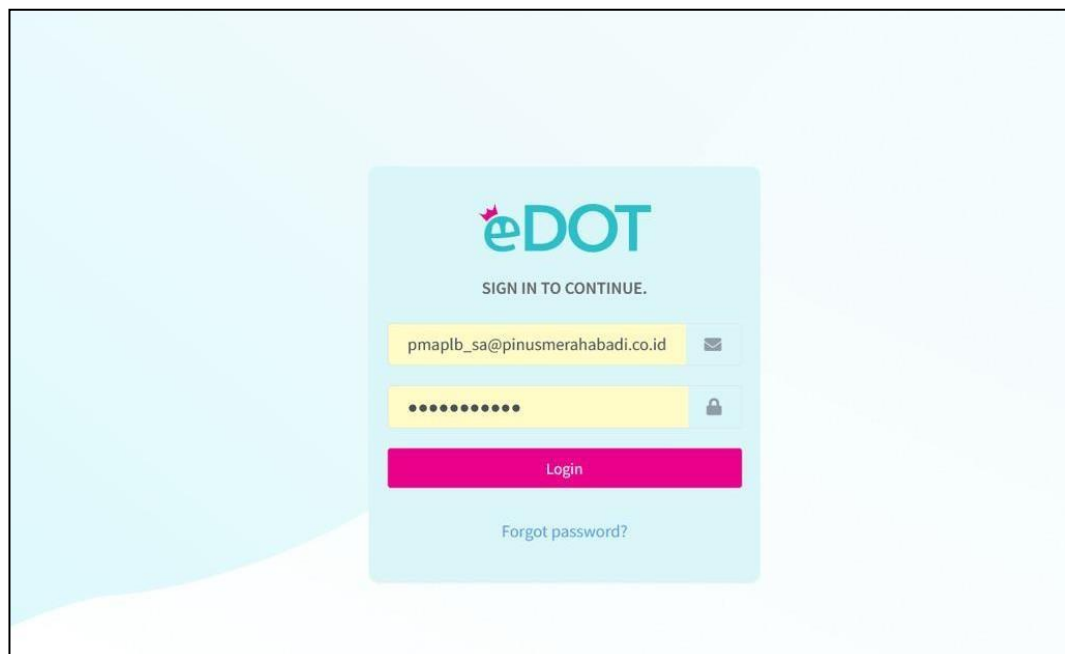
Tipe serangan bertujuan untuk membedakan jenis serangan yang akan diberikan pada komputer. Tipe serangan nantinya ada 2 yaitu melalui TCP dan UDP

- Lingkungan

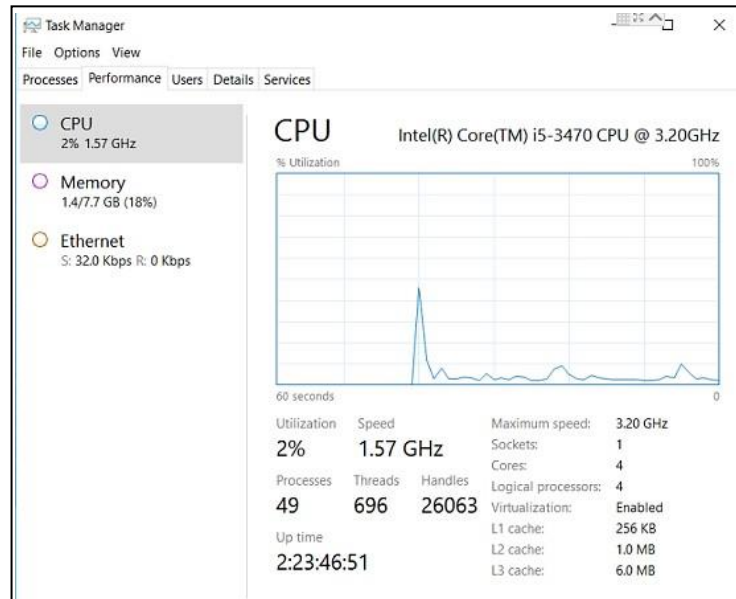
Penyerang melakukan serangan DoS akan di simulasikan pada jaringan PT Pinus Merah Abadi lantai 1 Divisi keuangan yang tersambung dengan jaringan.

IV.3 Simulasi Serangan Dos

Sebelum memulai simulasi serangan DoS, performa dari komputer yang sedang membuka aplikasi distribusi yang belum terkena serangan bisa dilihat pada gambar dibawah ini. Pada kondisi tanpa serangan, performa komputer Ketika membuka aplikasi tidak terlalu memakan resource yang ada. Gambar diatas diambil dari Task Manager pada feature Windows. Resource ini adalah CPU, memory, dan aktifitas jaringan. Pada kondisi ini, CPU hanya memakan 2% (1.5ghz), memory 18% (1,4gb) dan aktifitas jaringan hanya 32kbps.

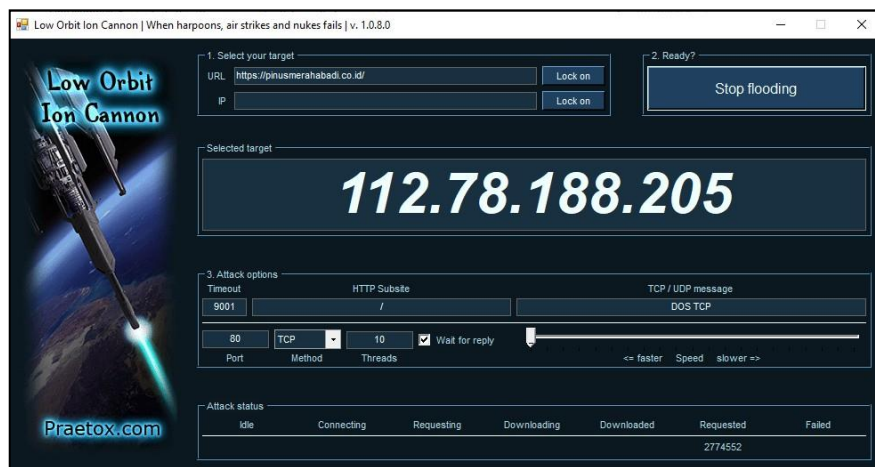


Gambar IV. 2 Screenshoot Aplikasi Distribusi PMA



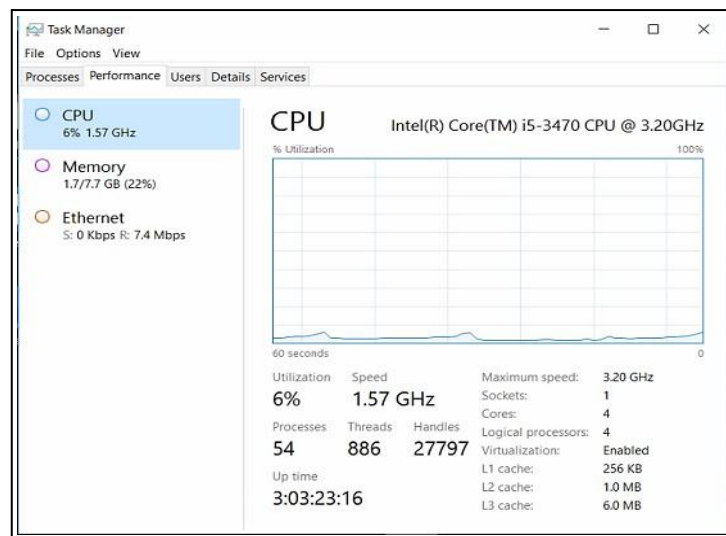
Gambar IV. 3 Screenshot kinerja Windows Tanpa Serangan

Simulasi serangan dos dimulai dengan menggunakan aplikasi bernama Low Orbit Ion Cannon (LOIC). Berikut merupakan eksperimen dos ke komputer melalui TCP. Masukkan URL <https://pinusmerahabadi.co.id/> sebagai tujuan lalu Lock, selanjutnya masukan threads sejumlah 10 dan pilih TCP sebagai method. Masukkan message “Dos TCP”.



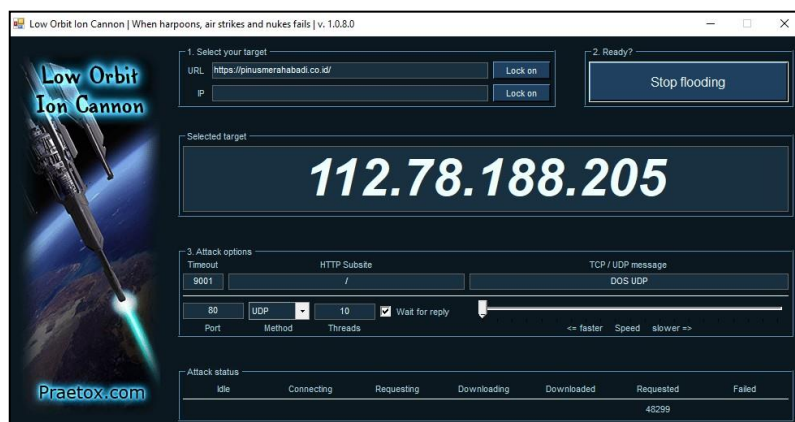
Gambar IV. 4 Screenshot LOIC protokol TCP target

Setelah dilakukannya eksperimen serangan dos ke komputer melalui protokol tcp. Pada eksperimen ini, CPU naik (4%), memory naik (6%) dan akitifitas jaringan naik pesat dimana yang sebelumnya maksimal 320kbps sekarang menjadi 7,4mbps. Ini menandakan bahwa dos melalui TCP cukup berpengaruh pada kinerja komputer. Selain itu, Windows pada komputer cukup handal dalam menangani dos ini karena CPU dan memory tidak sampai 70%.



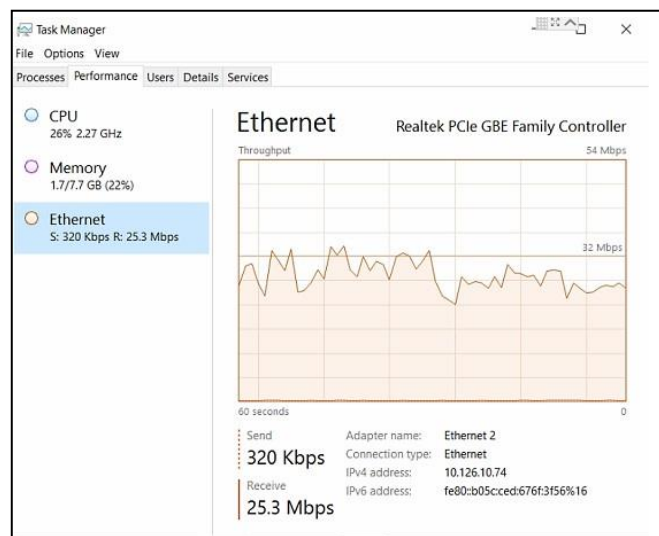
Gambar IV. 5 Screenshot kinerja Windows Komputer saat DoS melalui TCP

Berikut merupakan eksperimen dos ke komputer melalui TCP. Masukkan URL <https://pinusmerahabadi.co.id/> sebagai tujuan lalu Lock, selanjutnya masukan threads sejumlah 10 dan pilih UDP sebagai method. Masukkan message “Dos UDP”.



Gambar IV. 6 Screenshot LOIC protokol UDP target

Setelah dilakukannya eksperimen serangan dos ke komputer melalui protokol udp. Pada eksperimen ini, CPU naik drastis (dari 2% menuju 26%), memory sama seperti dos melalui tcp (18% menjadi 22%), Ethernet sedikit dibawah dos melalui tcp (320Kbps menjadi 25.3mbps). Hal ini menandakan bahwa DOS melalui UDP lebih berpengaruh daripada DOS melalui TCP pada Windows Komputer.



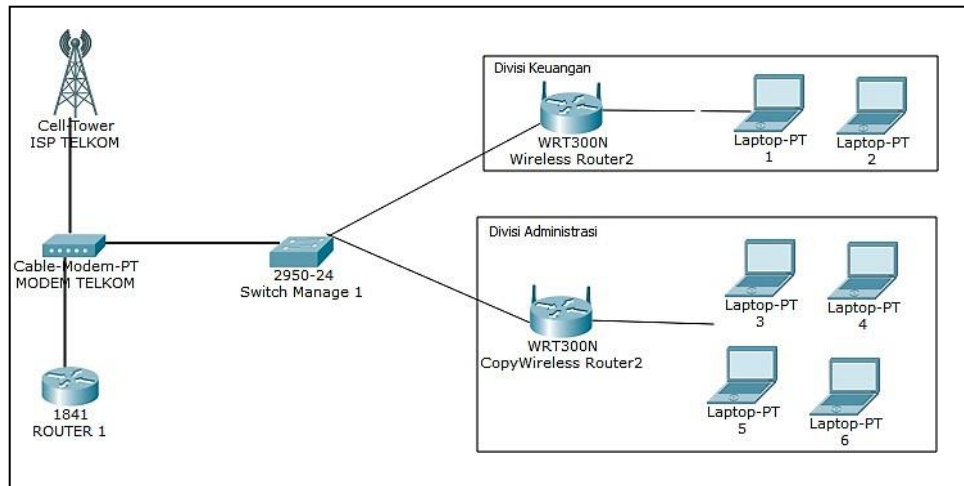
Gambar IV. 7 Screenshot kinerja Windows Komputer saat DoS melalui UDP

Bisa di lihat dari penjelasan diatas, pada jaringan PT Pinus Merah Abadi yang terhubung melalui jaringan LAN apabila terserang jaringan Dos dapat melemahkan peforma dari komputer yang digunakan untuk melakukan kegiatan perusahaan. Komputer perusahaan sering nge-*bug* dan juga website perusahaan menjadi tidak bisa di akses.

Setelah mendapatkan port yang terbuka pada jaringan, kemudian akan didapat titik lemah dari sistem jaringan tersebut. Kemudian DoS adalah metode serangan dimana pihak penyerang mengirimkan request berkali-kali untuk menyibukkan server hingga rusak atau hang. Setelah itu penyerang akan dengan mudah mengambil atau merusak data dari jaringan tersebut.

IV.4 Rancangan Jaringan Usulan

Rancangan jaringan usulan berisi topologi jaringan yang merupakan tahap design dari metode Network Development Life Cycle.



Gamba IV. 8 Topologi Jaringan Usulan

Setelah melakukan analisa pada jaringan PT Pinus Merah Abadi, maka dapat disimpulkan bahwa topologi yang diusulkan ini hanya perlu mengganti switch unmanageable dengan switch manageable agar sesuai dengan konsep jaringan yang telah dirancang. Usulan tambahan adalah adanya penggunaan vlan yang membuat pengaturan jaringan lebih flexible dan mudah dan dengan adanya vlan pengguna dapat menghemat perangkat yang akan digunakan. Keamanan data lebih terjamin karena dapat dipisah dan dibuat tersendiri. Performa yang lebih baik dikarenakan broadcast terbagi menjadi lebih kecil.

IV.5 Simulasi Keamanan Jaringan (*Switch Port Security*)

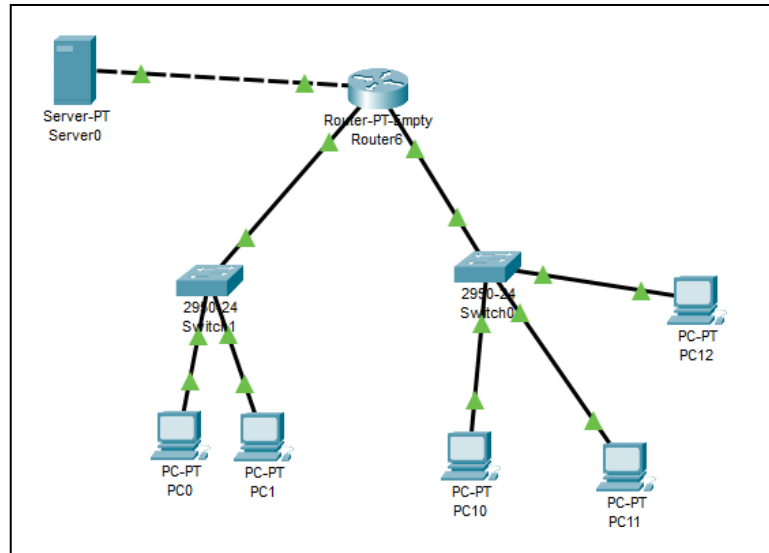
Solusi yang bisa diajukan atas permasalahan jaringan diatas adalah dengan memberikan kewanaman *switch port security*. Cara kerja port security yaitu dengan membatasi jumlah perangkat yang tersambung dengan port pada sebuah switch dan menentukan perangkat mana saja yang dapat tersambung pada port tersebut. *Switch*

port security sendiri bekerja dengan mendaftarkan MAC address dari perangkat yang dapat tersambung dengan jaringan tersebut.

Pada interface port sendiri dapat diberlakukan sistem keamanan yang disebut violation mode. Yaitu tindakan yang akan dilakukan port ketika terdeteksi akses dari perangkat yang tidak terdaftar MAC addressnya. Violation mode sendiri ada tiga, yaitu:

1. Protect: Pada mode protect, interface akan membuang (drop) paket data yang dikirim oleh perangkat yang tidak terdaftar tersebut. Outputnya akan menghasilkan request timed out saat dilakukan ping. Jadi data yang dikirimkan akan terhenti saat itu juga.
2. Restrict: Interface yang menggunakan violation ini akan membuang (drop) paket data seperti pada mode protect. Bedanya interface akan menghitung berapa jumlah violation yang terjadi. Jumlah ini berfungsi sebagai penanda berapa kali terjadi serangan dari pihak yang tidak terdaftar.
3. Shutdown: Interface yang menggunakan mode ini akan seketika menonaktifkan port yang digunakan perangkat yang tidak memiliki hak akses. Ketika host mengirim paket data otomatis port akan melakukan shutdown/mati.

IV.5.1 Desain Simulasi



Gambar IV. 9 Topologi Simulasi

Pada simulasi switch port security, penulis menggunakan topologi star dimana sesuai dengan device yang ada yaitu satu router, dua switch dan pada simulasi ini di uji coba dengan lima client. Berikut Tabel Addressing.

Tabel IV. 1 Tabel Addressing

Device	Interface	IP Address	Subnetmask	Default gateway
Server0	FastEthernet0	192.168.1.2	255.255.255.0	192.168.1.1
R1	FastEthernet0/0	192.168.1.1	255.255.255.0	N/A
	FastEthernet1/0	192.168.2.1	255.255.255.0	N/A
	FastEthernet2/0	192.168.3.1	255.255.255.0	N/A
PC0	FastEthernet0	192.168.2.2	255.255.255.0	192.168.1.1

PC1	FastEthernet0	192.168.2.3	255.255.255.0	192.168.1.1
PC10	FastEthernet0	192.168.3.2	255.255.255.0	192.168.1.1
PC11	FastEthernet0	192.168.3.3	255.255.255.0	192.168.1.1
PC12	FastEthernet0	192.168.3.4	255.255.255.0	192.168.1.1

IV.5.2 Pelaksanaan Simulasi

Simulasi keamanan jaringan dengan switch port dimulai dengan Konfigurasi switch port Fa0/2 untuk dijadikan sticky port security dimana switch mengambil MAC address pada PC10 secara otomatis. Kemudian karena defaultnya port security pada switch belum aktif kita perlu mengaktifkannya dengan perintah:

```
switch(config)#int fa0/2
switch(config-if)#sw mode-access
switch(config-if)#sw port-security
```

Setelah itu daftarkan 1 MAC address, port security pada switch akan aktif tapi masih static. Untuk membuatnya menjadi sticky port security perlu ditambahkan perintah berikut

```
switch(config)#int fa0/2
switch(config-if)#sw port-security max 1
switch(config-if)#sw port-security mac-address
sticky
```

Untuk memastikan apakah sudah aktif lakukan ping dari PC10 ke alamat IP host lain. Port Fa0/2 sudah mengaktifkan port-security dengan MAC address dari PC10 sehingga tidak bisa dipakai oleh host lain. Sebagai pembeda berikan violation mode yang berbeda pada switch dengan perintah sebagai berikut

```
switch(config)#int fa0/2
```

```
switch(config-if)#sw port-security violation
protect
```

Konfigurasi pada switch kali ini dibedakan dengan MAC address yang didaftarkan pada port Fa0/3. Pertama aktifkan port security pada port Fa0/3 menjadi stickyport security.

```
switch(config)#int fa0/3

switch(config-if)#sw mode-access

switch(config-if)#sw port-security

switch(config-if)#sw port-security max 1

switch(config-if)#sw port-security mac-address
sticky
```

Selanjutnya ubah mode violationnya menjadi *restrict* dengan perintah berikut

```
switch(config)#int fa0/3

switch(config-if)#sw port-security violation
restrict
```

Konfigurasi pada switch kali ini dibedakan dengan MAC address yang didaftarkan pada port Fa0/4. Seperti konfigurasi switch port Fa0/2, pertama aktifkan port security pada port Fa0/4 menjadi stickyport security.

```
switch(config)#int fa0/4

switch(config-if)#sw mode-access

switch(config-if)#sw port-security

switch(config-if)#sw port-security max 1

switch(config-if)#sw port-security mac-address
sticky
```

Selanjutnya ubah mode violationnya menjadi *shutdown*, kemudian simpan konfigurasi dengan perintah berikut

```
switch(config)#int fa0/4

switch(config-if)#sw port-security violation
shutdown

switch(config-if)#exit

switch#do wr
```

IV.5.3 Hasil Simulasi

Hasil simulasi jaringan dengan switch port dimulai dari port Fa0/2, dapat di lihat status switch port Fa0/2 pada gambar berikut.

```
Switch#sh port-security int fa0/2
Port Security          : Enabled
Port Status           : Secure-up
Violation Mode        : Protect
Aging Time            : 0 mins
Aging Type            : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses  : 1
Configured MAC Addresses : 0
Sticky MAC Addresses  : 1
Last Source Address:Vlan : 000B.BE26.6500:1
Security Violation Count : 0
```

Gambar III. 10 Status Switch Port Fa0/2

Pada Gambar IV. 10 Status port security switch port Fa0/2 aktif dengan jenis sticky port security dan violation modenya *protection*. . Mode ini akan membuang data yang dikirimkan dari host yang tidak terdaftar. Contoh jika switch port Fa0/2 dihubungkan dengan PC12 dan melakukan ping maka outputnya adalah request timed out tapi koneksi tidak terputus dapat dilihat pada Gambar IV. 11 dan IV. 12.

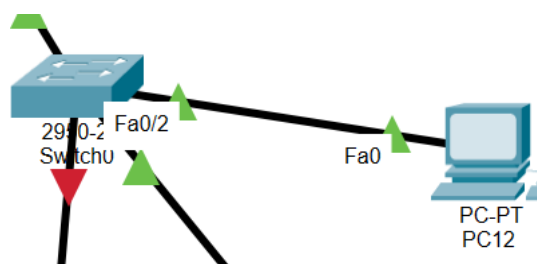

```
C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Gambar IV. 11 Ping dari PC12



Gambar IV. 12 Koneksi tidak terputus walaupun pada PC12

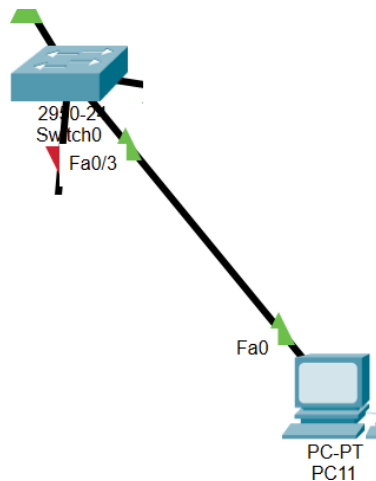
Hasil simulasi jaringan dengan switch port Fa0/3, dapat di lihat status switch port Fa0/3 pada gambar berikut.

```
Switch#sh port-security int fa0/3
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Restrict
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 0
Sticky MAC Addresses    : 1
Last Source Address:Vlan : 0007.EC47.ED66:1
Security Violation Count : 0
```

Gambar IV. 13 Status Switch Port Fa0/3

Terlihat pada Gambar IV. 13, port security pada port Fa0/3 aktif dengan maksimum MAC address yang sudah terpenuhi dan violation modenya adalah restrict. Mode ini berbeda dengan mode protection karena pada saat port Fa0/3 digunakan oleh

host dengan MAC address berbeda tidak akan terputus sambungannya namun data tetap didrop dan dilakukan penghitungan violation count yang terjadi.



Gambar IV. 14 Memindahkan koneksi pada PC11

Contoh pada Gambar IV. 14, jika PC11 melakukan ping maka akan terjadi request timed out dan violation countnya bertambah seperti terlihat pada Gambar IV. 15 dan 16.

```
C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Gambar IV. 15 Ping dari PC11

```

Switch#show port-security int fa0/3
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Restrict
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 0
Sticky MAC Addresses    : 1
Last Source Address:Vlan : 00D0.BCD0.B0DA:1
Security Violation Count : 4

```

Gambar IV. 16 Status Akhir Switch Port Fa0/3 dengan MAC Address berbeda

Hasil simulasi jaringan dengan switch port Fa0/4, dapat di lihat status switch port Fa0/4 pada gambar berikut.

```

Switch#show port-security int fa0/4
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 0
Sticky MAC Addresses    : 1
Last Source Address:Vlan : 00D0.BCD0.B0DA:1
Security Violation Count : 0

```

Gambar IV. 17 Status Switch Port Fa0/4

Pada Gambar IV. 17, port security pada switch port Fa0/4 aktif dengan jenis sticky port security dan violation modenya *shutdown*. Mode *shutdown* membuat koneksi otomatis terputus pada saat disambungkan ke host dengan MAC address yang berbeda. Contoh port fa0/4 dihubungkan pada PC10 kemudian dilakukan ping, secara otomatis koneksi akan terputus, dapat dilihat pada Gambar IV. 19.

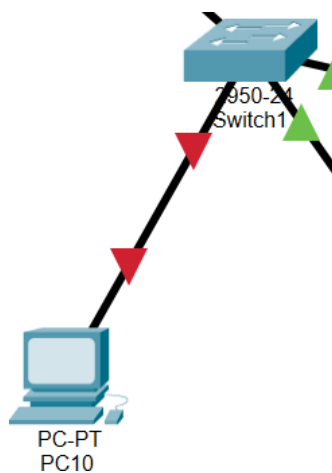
```
C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Gambar IV. 18 Ping dari PC10



Gambar IV. 19 Setelah melakukan ping pada PC10

```
Switch#show port-security int fa0/4
Port Security           : Enabled
Port Status             : Secure-shutdown
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 0
Sticky MAC Addresses    : 1
Last Source Address:Vlan : 000B.BE26.6500:1
Security Violation Count : 1
```

Gambar IV. 20 Status port fa0/4 setelah dilakukan ping dengan MAC Address berbeda

Dapat dilihat pada Gambar IV. 20, status dari portnya secure shutdown yang berarti sudah tidak aktif secara otomatis dan violation countnya bertambah.

BAB V KESIMPULAN DAN SARAN

V.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan pada sistem keamanan jaringan pada PT Pinus Merah Abadi, didapatkan beberapa kesimpulan diantaranya:

1. Pada eksperimen pengujian serangan DoS dengan tools LOIC pada komputer client yang terhubung pada jaringan di PT Pinus Merah Abadi, terlihat menurunkan kinerja CPU sebanyak 16% melalui UDP dan menaikkan memori sebanyak 10%. Hal ini membuat kinerja komputer PMA tidak berkerja secara maksimal. Ketika mencoba akses login aplikasi, juga tak jarang komputer langsung hang atau bug yang mengakibatkan kegiatan perusahaan terganggu.
2. Hasil simulasi keamanan jaringan dengan tools Cisco Packet Tracer, diperoleh bahwa konfigurasi switch port security menggunakan sticky port security paling efektif dan efisien dilakukan karena dapat mendaftarkan MAC address yang sangat banyak dengan otomatis. Penggunaan violation mode yang paling aman adalah mode shutdown karena koneksi dari perangkat yang tidak dikenal akan langsung terputus otomatis. Ini tentu akan meningkatkan keamanan data pada perangkat-perangkat yang lain.
3. Switch port security melindungi jaringan dari serangan luar yang *device*-nya tidak terdaftar pada konfigurasi switch. Seperti serangan DoS yang ingin mengakses perangkat yang digunakan pengguna melalui IP, atau username password yang digunakan pada komputer.

V.2 Saran

Berdasarkan hasil penelitian pada keamanan jaringan PT Pinus Merah Abadi, dibutuhkan penyempurnaan lebih lanjut agar didapatkan hasil yang maksimal.

Berikut saran yang dapat disampaikan penulis untuk penelitian selanjutnya adalah sebagai berikut:

1. Pengujian serangan disarankan menggunakan tools lain seperti Hoic atau Tor Hammer untuk dijadikan perbandingan dalam penelitian.
2. *Port security* merupakan teknik keamanan jaringan paling dasar sehingga perlu dilakukan teknik lanjutan untuk menjaga data yang lebih besar seperti IP source guard, DHCP snooping, dynamic ARP, dll.

DAFTAR PUSTAKA

- [1] M. Syafrizal, Pengantar Jaringan Komputer, Yogyakarta: Andi, 2018.
- [2] R. Permana, D. Ramadhani and I. Lestari, "Proteksi Keamanan Jaringan Komputer di Sekolah Menengah Kejuruan Al-Madani Pontianak," *International Journal of Natural Science and Engineering*, vol. 3, pp. 37-43, 2019.
- [3] A. P. Wahyu, "Optimasi Jaringan Local Area Network Menggunakan VLAN dan VOIP," *Jurnal Informatika: Jurnal Pengembangan IT*, vol. 2, pp. 54-57, 2018.
- [4] I. Sofana, Membangun Jaringan Komputer : Mudah membuat Jaringan Komputer (Wire & Wireless) untuk pengguna Windows dan Linux, Bandung: Informatika, 2018.
- [5] S. Rushadi, "Konsep Keamanan Jaringan Komputer dengan Infrastruktur Demilitarized Zone," October 2018. [Online]. Available: <https://www.researchgate.net/publication/328130248>. [Accessed 26 June 2023].
- [6] O. K. Sulaiman, "ANALISIS SISTEM KEAMANAN JARINGAN DENGAN MENGGUNAKAN SWITCH PORT SECURITY," *CESS (Journal Of Computer Engineering, System And Science)*, pp. 9-14, 2016.
- [7] Cloudmatika, "Cloudmatika," 6 October 2022. [Online]. Available: <https://cloudmatika.co.id/blog-detail/ancaman-keamanan-jaringan>. [Accessed 26 June 2023].
- [8] Zsa-Zsa, Amelia and T. Dali, "REDESIGN INFRASTRUKTUR DAN MANAJEMEN JARINGAN DENGAN METODE NETWORK DEVELOPMENT LIFE CYCLE (NDLC) DI KANTOR POS REGIONAL III PALEMBANG," *Repository Universitas Bina Darma*, 2019.
- [9] R. Hermawan, "ANALISIS KONSEP DAN CARA KERJA SERANGAN KOMPUTER DISTRIBUTED DENIAL OF SERVICE (DDOS)," *E-Journal Universitas Indrapastra PGRI*, vol. 5, pp. 1-4.
- [10] F. Fachri, A. Fadlil and I. Riadi, "Analisis Keamanan Webserver Menggunakan Penetration Test," *JURNAL INFORMATIKA*, vol. 8, pp. 183-190, 2021.

LAMPIRAN

Lampiran 1 Daftar Riwayat Hidup

Bahwa saya bertanda tangan dibawah ini:

Nama : Ra Martasya Putri
Tempat, Tanggal Lahir : Palembang, 06 Maret 2000
Jenis Kelamin : Perempuan
Pekerjaan : Mahasiswa
Alamat : jalan soekarno hatta lr musi raya rt 50 rw 1 no 2500
Status : Lajang / Belum Menikah
Kewarganegaraan : Indonesia
Agama : Islam
No. HP : 0895-3270-88734
Email : 2019310071@students.uigm.ac.id

RIWAYAT PENDIDIKAN

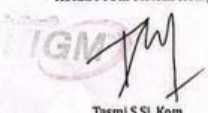
1. SD Negeri 94 Palembang (2006 – 2012)
2. SMP Negeri 35 Palembang (2012 – 2015)
3. SMA Negeri 5 Palembang (2015 – 2018)

Demikian daftar Riwayat hidup saya buat dengan sebenarnya.

Peraturan Bimbingan Skripsi

1. Kartu Bimbingan harus diisi identitas mahasiswa bimbingan Skripsi dengan jelas dan benar;
2. ~~Kartu~~ Bimbingan harus disertai foto terbaru mahasiswa bimbingan Skripsi;
3. Kartu Bimbingan harus diberi tanda tangan Ketua Prodi dan cap Fasilkom UIGM sebagai tanda Sah;
4. Kartu Bimbingan ini harus diparaf Pembimbing Skripsi setiap kali melaksanakan bimbingan, minimal 6x pada Proposal Skripsi dan 12x untuk masing-masing dosen;
5. Kartu Bimbingan ini tidak boleh rusak atau hilang;
6. Jika Kartu Bimbingan hilang, mahasiswa bimbingan Skripsi akan dikenai biaya penggantian Kartu Bimbingan baru sebesar Rp 50.000,00.

Palembang, 12 Juni 2023
Ketua Prodi Sistem Komputer




Tasmi.S.Si, Kom

UIGM UNIVERSITAS INDO GLOBAL MANDIRI
Fakultas Ilmu Komputer

KARTU BIMBINGAN SKRIPSI

Judul Skripsi : Simulasi Keamanan Jaringan Dengan Metode *Network Development Life Cycle* Menggunakan *Switch Port Security* Pada PT Pinus Merah Abadi

Nama	: RA Martasya Putri
NPM	: 2019310071
Program Studi	: Sistem Komputer
Alamat	: Jalan Soekarno Hatta Lr Musi Raya Rt 50 Rw 11 No 2500 Palembang
Telp / HP	: 0895-3270-88734



Pembimbing Skripsi

1. Ir. Zulkifli, M.Sc
2. Ricky Maulana Fajri, S.KOM, M.Sc

Pembimbing 1 : Ir. Zulkifli, M.Sc

No	Tanggal Bimbingan	Permasalahan	Paraf
1	29/3/23	Bab I Revisi bab II	
2	6/4/23	Bab I Revisi bab II	
3	12/04/23	Praktik Reri	
4	05/05/23	Parab bab II tera	
5	10/05/23	Revisi III, judul, Metode	
6	17/05/23	Bab III ok	
7	17/05/23	Siak Simpro	
8	03/08/23	Bab IV Revisi	
9	03/08/23	Bab IV OK layout	
10	08/08/23	Ujian Kompro	

Pembimbing 2 : Ricky Maulana Fajri, S.Kom., M.Sc

No	Tanggal Bimbingan	Permasalahan	Paraf
1	29/3/23	BAB I Revisi	
2	6/4/23	BAB II Revisi	
3	12/4/23	BAB I Revisi	
4	03/5/23	BAB II ACC	
5	10/05/23	Revisi BAB III	
6	17/05/23	ACC BAB III	
7	18/05/23	ACC Simpro	
8	01/08/23	Revisi BAB IV	
9	03/08/23	ACC BAB IV	
10	08/08/23	ACC Sidang	

SURAT PERNYATAAN BEBAS PLAGIAT

Saya yang bertandatangan di bawah ini.

Nama : Ra Martasya Putri

Tempat/Tanggal Lahir: Palembang . 06 Maret 2000

Program Studi : Sistem Komputer

Tahun Akademik : 2022/2023

Menyatakan bahwa saya tidak melakukan kegiatan plagiat dalam penulisan skripsi saya yang berjudul:

Simulasi Keamanan Jaringan Dengan Metode *Network Development Life Cycle* Menggunakan *Switch Port Security* Pada PT Pinus Merah Abadi

Apabila suatu saat nanti terbukti saya melakukan plagiat maka saya akan menerima sanksi yang telah ditetapkan.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya.

Palembang, 21 Agustus 2023

Yang Membuat Pernyataan



Ra Martasya Putri
NIM. 2019310071



**PERSETUJUAN SIDANG SKRIPSI
FAKULTAS ILMU KOMPUTER
PROGRAM STUDI SISTEM KOMPUTER
FM-PM-10.3/12-02/R0**

Program Studi : Sistem Komputer
Bidang Kajian : Jaringan
Nama : Ra Martasya Putri
NPM : 2019310071
Judul : Implementasi Keamanan Jaringan Dengan Metode
Network Development Life Cycle Menggunakan *Switch Port Security* Pada PT Pinus Merah Abadi

Pembimbing : 1. Ir.Zulkifli, M.Sc
2. Ricky Maulana Fajri, M.Sc

Skripsi telah disetujui untuk dipertahankan di hadapan Tim Penguji Skripsi
Persetujuan.

No.	Nama	Tanggal Persetujuann	Tanda Tangan
1.	Pembimbing I Ir.Zulkifli, M.Sc	21/8 - 2023	
2.	Pembimbing II Ricky Maulana Fajri, M.Sc	21/8/2023	

SURAT KETERANGAN REVISI SKRIPSI

Kami yang bertanda tangan dibawah ini, menerangkan bahwa:

Nama : Ra Martasya Putri
NPM : 2019310071
Judul Skripsi : Simulasi Keamanan Jaringan Dengan Metode *Network Development Life Cycle* Menggunakan *Switch Port Security* Pada PT Pinus Merah Abadi

Mahasiswa yang namanya tercantum diatas, telah selesai merevisi penulisan skripsi.

Menyetujui
Tim Penguji

Tanggal 25 Agustus 2023

Ketua Penguji



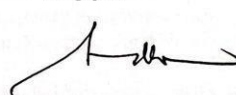
Ir Zulkifli, M.Sc
NIK.2011.01.01.11

Penguji 1



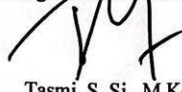
Tasmi, S. Si., M.Kom
NIK. 2017.01.02.30

Penguji 2



Ir. Hasta Sunardi, MT
NIK.2003.01.0072

Mengetahui
Ketua Program Studi Sistem Komputer



Tasmi, S. Si., M.Kom
NIK. 2017.01.02.30