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

**RA Martasya Putri[1)], Ir. Zulkifli, M.T.[2)], Ricky Maulana Fajri, S.Kom., M.Sc.[3)]**

*Program Studi Sistem Komputer UNIVERSITAS INDO GLOBAL MANDIRI*
*JL. Jend Sudirman No. 629, Palembang 30129, Sumatera Selatan*
*Email: 2019310071@students.uigm.ac.id[1)], zulkifli@uigm.ac.id [2)], rickymaulanafajri@uigm.ac.id[3)]*

## ABSTRAK

Perkembangan teknologi di dunia jaringan komputer semakin cepat seiring dengan meningkatnya tuntutan akan koneksi yang efisien, stabil, dan aman. Salah satu faktor penting dalam meningkatkan kualitas jaringan adalah keamanan jaringan atau network security. Terdapat berbagai teknik yang dapat digunakan untuk meningkatkan tingkat keamanan, seperti membangun sistem firewall atau mengimplementasikan port security. Port security melibatkan penggunaan port-port yang ada untuk mengatur akses ke jaringan. Dalam lingkungan kerja PT Pinus Merah Abadi, seringkali terjadi masalah seperti koneksi yang lambat dan kelemahan dalam aspek keamanan jaringan. Untuk mengatasi ini, penulis akan melakukan simulasi penggunaan port-security pada setiap switch di PT Pinus Merah Abadi agar jaringan komputer menjadi lebih aman dan terhindar dari masalah-masalah tersebut.

**Kata Kunci :** Keamanan Jaringan, *Port Security*, VLAN

## *ABSTRACT*

*Technological developments in the world of computer networks are increasingly rapid along with increasing demands for efficient, stable and secure connections. One important factor in improving network quality is network security. There are various techniques that can be used to increase the level of security, such as building a firewall system or implementing port security. Port security involves using existing ports to regulate access to the network. In the PT Pinus Merah Abadi work environment, problems often occur such as slow connections and weaknesses in network security aspects. To overcome this, the author will simulate the use of port-security on each switch at PT Pinus Merah Abadi so that the computer network becomes safer and avoids these problems.*

***Keywords :*** *Network Security, Port Security, VLAN.*

## 1. PENDAHULUAN

### 1.1 Latar Belakang

Perkembangan teknologi informasi memiliki peranan penting dalam memfasilitasi aktivitas manusia. Fenomena ini dapat diilustrasikan dengan maraknya penerapan teknologi informasi dalam berbagai sektor bisnis. Salah satu contoh implementasi teknologi informasi yang signifikan adalah penggunaan jaringan komputer. Jaringan komputer merupakan suatu konsep di mana beberapa perangkat komputer terkoneksi satu sama lain, memungkinkan pengguna untuk berbagi informasi berupa suara, video, dan data dalam satu infrastruktur jaringan yang sama.

Ketika teknologi terus berkembang dan kebutuhan dalam berbagai aspek, termasuk dunia pekerjaan, semakin meningkat, jaringan komputer menjadi semakin esensial. Dalam manajemen jaringan, isu keamanan memiliki peran yang sangat krusial. Terdapat berbagai bentuk tindak kejahatan dalam jaringan, seperti penyebaran virus dan pencurian data, yang menunjukkan urgensi untuk menjaga keamanan jaringan.

Salah satu pendekatan untuk mengurangi risiko tindak kejahatan dalam jaringan adalah melalui penerapan langkah-langkah keamanan pada perangkat *switch*. Hal ini memungkinkan pengaturan yang lebih ketat terkait dengan akses dan keterbatasan perangkat dan individu yang diizinkan untuk bergabung atau mengakses jaringan tersebut. [1]

PT Pinus Merah Abadi melibatkan berbagai bagian yang menggunakan komputer yang terhubung dalam jaringan LAN (*Local Area Network*). Dengan jaringan ini yang terhubung secara sinergis, karyawan dari berbagai divisi dapat menggabungkan potensi jaringan komputer untuk mendukung pekerjaan mereka secara optimal. Untuk menjaga kinerja dan keamanan jaringan tetap prima, perlu dilakukan manajemen yang cermat.

Sebagai langkah untuk membantu administrator jaringan meningkatkan keamanan perangkat dalam jaringan, salah satu tindakan yang

dapat diambil adalah menerapkan sistem keamanan port pada *switch*. [2]

Menerapkan sistem keamanan port ini bermanfaat untuk mengontrol akses komputer yang tidak terdaftar di port *switch*, yang dapat mencegah penyalahgunaan akses oleh individu yang tidak berwenang atau kesalahan administratif saat berpindah. Oleh karena itu, metode keamanan port ini adalah teknik yang memungkinkan penggunaan akses jaringan melalui port yang tersedia di *switch* sesuai dengan konteks yang telah dijelaskan di atas. Oleh karena itu, penelitian ini berjudul "Simulasi Keamanan Jaringan dengan Pendekatan NDLC Menggunakan Keamanan *Port Switch* di PT Pinus Merah Abadi."

### 1.2 Perumusan Masalah

Berdasarkan latar belakang diatas, maka rumusan masalah dalam penulisan ini adalah sebagai berikut:

1. Bagaimana tampilan keamanan jaringan yang diterapkan melalui fitur switch port security di PT Pinus Merah Abadi, sehingga setiap pengguna dalam jaringan dapat beroperasi sesuai dengan izin akses yang mereka miliki?

### 1.3 Tujuan dan Manfaat Penelitian

A. Adapun tujuan penelitian dari peneliti yaitu:

1. Penelitian ini bertujuan untuk memahami operasi dan mekanisme port pada *switch*, dengan fokus pada implementasi fitur keamanan *port security* dan konfigurasi serta perancangan port security dalam lingkungan Jaringan Komputer di PT Pinus Merah Abadi.

B. Adapun manfaat penelitian dari peneliti yaitu:

1. Memahami operasi dan prinsip kerja *port* pada *switch* melalui penerapan sistem keamanan *port security*.
2. Menciptakan tingkat keamanan yang lebih tinggi pada *port switch* dengan metode keamanan yang memiliki kemampuan untuk melindungi, membatasi, atau bahkan menolak hak akses dari perangkat yang tidak diidentifikasi.

## 2. PEMBAHASAN

### 2.1 Jaringan Komputer

Jaringan komputer merupakan suatu sistem yang terdiri dari sekelompok komputer yang saling terhubung melalui media komunikasi dan menggunakan protokol komunikasi. Tujuannya adalah untuk memungkinkan pertukaran informasi, program, dan penggunaan perangkat antara komputer-komputer tersebut. Jaringan komputer melibatkan perangkat keras, perangkat lunak, dan perangkat jaringan yang beroperasi secara bersinergi dalam konteks tertentu untuk mencapai suatu sasaran. Untuk mencapai tujuan ini, setiap komponen dalam jaringan komputer berpartisipasi dengan cara meminta dan memberikan layanan. Dari berbagai definisi tentang jaringan komputer di atas, dapat disimpulkan bahwa jaringan komputer adalah suatu infrastruktur telekomunikasi yang memungkinkan komunikasi antara komputer-komputer dengan pertukaran data sebagai tujuannya. Tujuan utama jaringan komputer adalah untuk memfasilitasi pertukaran layanan antar komponen jaringan, sementara juga menghadapi risiko serangan atau pencurian data dalam konteks jaringan perusahaan. Oleh karena itu, diperlukan alat atau perangkat yang dapat mencegah penyusupan atau pencurian data dalam jaringan komputer perusahaan tersebut [3]

### 2.2 *Local Area Network* (LAN)

Sebuah *Local Area Network* (LAN) adalah jenis jaringan yang memiliki cakupan terbatas pada area yang relatif kecil, seringkali dibatasi oleh lingkungan tertentu, seperti kantor di dalam suatu gedung atau berbagai ruangan di dalam sebuah sekolah. Biasanya, jarak antara setiap titik (node) dalam jaringan ini tidak melebihi sekitar 200 meter [4]

### 2.3 *Metropolitan Area Network* (MAN)

Sebuah *Metropolitan Area Network* (MAN) umumnya mencakup wilayah yang lebih luas daripada LAN, seperti menghubungkan berbagai gedung dalam suatu area geografis yang lebih besar, seperti provinsi atau negara bagian. Dalam konteks ini, MAN menggabungkan beberapa jaringan lokal ke dalam lingkungan yang lebih besar. Sebagai ilustrasi, MAN dapat digunakan untuk menghubungkan beberapa cabang bank di dalam kota besar, mengintegrasikan mereka ke dalam satu jaringan yang saling terhubung [5]

### 2.4 *Wide Area Network* (WAN)

*Wide Area Network* (WAN) adalah jenis jaringan yang seringkali mengandalkan media nirkabel, koneksi melalui satelit, atau kabel serat optik, karena cakupannya yang luas, tidak hanya terbatas pada satu kota atau hubungan antara kota dalam satu wilayah, tetapi dapat merentang ke wilayah yang berada di yurisdiksi negara lain [6]

### 2.5 *Virtual Local Area Network* (VLAN)

VLAN (Virtual LAN) adalah sebuah konsep jaringan yang membagi jaringan secara logis menjadi beberapa VLAN yang berbeda. Keistimewaan VLAN adalah tidak terikat pada aspek fisik jaringan seperti yang berlaku pada LAN, sehingga memungkinkan konfigurasi virtual tanpa perlu memperhatikan peralatan fisik. Dengan demikian, VLAN menawarkan fleksibilitas dalam manajemen jaringan, memudahkan administrator jaringan dalam mempartisi jaringan sesuai dengan fungsi dan kebutuhan keamanan. Dari berbagai definisi mengenai VLAN, dapat disimpulkan bahwa

VLAN merupakan sebuah model jaringan yang tidak bergantung pada lokasi fisik seperti LAN, sehingga memungkinkan konfigurasi virtual tanpa mempertimbangkan posisi fisik peralatan. Penggunaan VLAN mempermudah pengaturan jaringan, memungkinkan pembagian segmen yang berdasarkan organisasi atau departemen tanpa memperhatikan lokasi perangkat kerja, dan juga mengurangi kebutuhan akan kabel fisik [7]

### 2.6 *Network Interface Card* (NIC)

NIC (*Network Interface Card*) adalah komponen hardware esensial yang wajib ada pada setiap komputer. Tugas utama NIC adalah mengatur aliran tegangan dan arus listrik yang masuk dan keluar dari komputer. Kemampuan NIC memungkinkan komputer untuk mengirim dan menerima informasi melalui media penghantar. Selain itu, NIC juga mengendalikan aliran data antara sistem komputer dan kabel yang terhubung, serta menerima data yang dikirimkan oleh komputer lain melalui media kabel, dan menerjemahkannya ke dalam format bit yang dapat dipahami oleh komputer [8]

### 2.7 Router

Router adalah perangkat yang dirancang khusus untuk mengatur hubungan antara dua atau lebih jaringan yang terkoneksi melalui teknik paket switching. Cara kerja router melibatkan pengamatan alamat pengirim dan alamat penerima dalam setiap paket data yang melewatinya, dan kemudian menentukan jalur atau rute yang paling sesuai bagi paket tersebut agar sampai ke tujuan yang dituju. Router memiliki pengetahuan tentang alamat individu untuk setiap komputer dalam jaringan lokalnya, alamat bridge, serta router lainnya [9]

### 2.8 *Switch*

*Switch* pada dasarnya memiliki peran serupa dengan Hub, yaitu berfungsi sebagai perangkat yang membagi sinyal dan memperkuat sinyal dalam jaringan komputer. Namun, keunggulan Switch terletak pada kemampuannya yang lebih cerdas dibandingkan Hub, karena Switch mampu mengenali alamat data yang harus dikirimkan dan memiliki kemampuan mengelola lalu lintas data dalam jaringan secara lebih efisien jika dibandingkan dengan Hub. *Switch* berperan sebagai titik sentral dalam proses transfer data dalam jaringan, sehingga apabila terjadi masalah pada Switch, dapat berdampak pada seluruh koneksi jaringan dan proses transfer data. *Switch* biasanya memiliki sejumlah port yang digunakan untuk menghubungkan ke perangkat-perangkat dalam jaringan komputer, dan port-port ini umumnya terhubung melalui konektor RJ-45. [10]

### 2.9 *Keamanan Jaringan*

Keamanan jaringan, yang juga dikenal sebagai *network security*, adalah suatu sistem yang berperan dalam mengenali serta mencegah upaya akses yang tidak sah ke dalam sebuah jaringan. Tujuannya adalah untuk dengan cepat menghentikan akses oleh pihak yang tidak berwenang ke dalam sistem jaringan. Dengan kata lain, *network security* berfokus pada deteksi dan pencegahan potensi ancaman yang dapat merusak integritas sistem jaringan, baik dari segi logika maupun fisiknya. Konsep keamanan jaringan mencakup berbagai jenis perangkat jaringan, baik yang digunakan dalam lingkup pribadi maupun jaringan yang bersifat publik. Salah satu aspek penting dari keamanan jaringan adalah otorisasi akses ke data yang ada dalam jaringan tersebut. Untuk melindungi sumber daya jaringan atau *network resource*, metode yang umum digunakan adalah penggunaan kombinasi *username dan password*.

### 2.10 *Switch Port Security*

*Port security* pada *switch* adalah sebuah mekanisme pengendalian lalu lintas yang beroperasi pada lapisan data link (layer 2). Fungsinya adalah untuk mencatat dan membatasi perangkat end yang diizinkan untuk terhubung ke suatu port pada switch tersebut. Kemampuan manajemen switch yang dapat dikonfigurasi pada tingkat ini dapat meningkatkan tingkat keamanan jaringan dengan memanfaatkan port-port yang tersedia pada *switch*.

### 2.11 Virus

Virus adalah sebuah perangkat lunak yang diciptakan dengan tujuan untuk menggandakan dirinya sendiri, dengan maksud agar dapat menyebar ke dalam program-program komputer lainnya. Sumber penyebaran virus bisa berasal dari situs web atau email spam. Fungsi utama dari virus adalah merusak data dalam komputer sehingga pengguna tidak dapat mengaksesnya.

### 2.12 Worm

Sama seperti virus, worm juga memiliki kemampuan untuk menggandakan dirinya sendiri sehingga dapat menyebar ke seluruh jaringan internet. Proses duplikasi yang dilakukan oleh worm adalah otomatis dan tidak memerlukan intervensi dari pengguna. Salah satu perbedaannya dengan virus adalah bahwa worm tidak menginfeksi atau merusak aplikasi lain di dalam komputer.

### 2.13 *Trojan Horse*

*Trojan horse* adalah jenis malware atau perangkat berbahaya yang memiliki kemampuan untuk menyamar sehingga terlihat seolah-olah berfungsi normal dan dapat digunakan sesuai dengan keinginan pengguna. Biasanya, sumber trojan berasal dari perangkat lunak yang diinstal di dalam perangkat. Oleh karena itu, penting untuk

melakukan tinjauan terhadap aplikasi yang terdapat dalam komputer.

### 2.14 *Denial Of Service*

Ancaman ini fokus pada server situs web dengan tujuan untuk membuat situs web tidak dapat diakses sementara waktu. Pelaku Denial-of-Service mengganggu operasi server dengan cara mengirim sejumlah besar lalu lintas data sehingga server tidak lagi dapat menangani permintaan yang datang. Setelah server mengalami kegagalan, pelaku seringkali mencoba melakukan pembobolan dan mengakses data yang ada di dalamnya.

## 3. METODOLOGI PENELITIAN

### 3.1 Gambaran Umum Objek Penelitan

Berdasarkan latar belakang dan ulasan literatur yang telah dijelaskan dalam bab sebelumnya, penelitian yang akan dilakukan bertujuan untuk mensimulasikan implementasi keamanan jaringan melalui fitur switch port security di PT Pinus Merah Abadi, yang sebelumnya hanya mengandalkan firewall sebagai metode keamanan. Masalah yang sering dihadapi oleh PT Pinus Merah Abadi dalam hal jaringan, sebagaimana yang diidentifikasi melalui wawancara dan pengamatan oleh penulis, adalah terjadinya kesalahan data yang tidak sesuai dengan tugas masing-masing divisi di dalam perusahaan tersebut.

### 3.2 Metode Pengumpulan Data

Dalam penelitian ini, berbagai metode pengumpulan data akan digunakan, termasuk wawancara, observasi, studi pustaka, dan dokumentasi. Wawancara adalah suatu metode pengumpulan data yang dilakukan melalui interaksi langsung antara peneliti dan narasumber, di mana pertanyaan-pertanyaan yang telah dipersiapkan sebelumnya diajukan untuk mendapatkan informasi yang relevan terkait permasalahan yang tengah diteliti. Observasi adalah metode yang melibatkan pengamatan langsung terhadap suatu proses atau situasi tertentu, dan peneliti akan mencatat semua informasi yang diperoleh dari pengamatan tersebut. Oleh karena itu, penulis akan melakukan wawancara dan observasi di PT Pinus Merah Abadi untuk mendapatkan pemahaman yang lebih baik tentang masalah yang sedang diinvestigasi. Studi Pustaka merupakan metode pengumpulan data yang dilakukan dengan membaca dan mempelajari literatur yang relevan, seperti buku, makalah, atau referensi lainnya yang berkaitan dengan masalah yang sedang dibahas. Penulis mengumpulkan data simulasi dengan melakukan serangan jaringan menggunakan simulator Cisco Packet Tracer versi 8.2. Sistem jaringan yang disimulasikan telah didasarkan pada temuan dari studi literatur sejenis. Data hasil simulasi ini kemudian dianalisis untuk mengidentifikasi kebutuhan keamanan sistem jaringan yang dapat memenuhi kriteria keamanan jaringan yang dibutuhkan. Hasil dari analisis ini akan menjadi kontribusi penulis dalam penelitian ini.

### 3.3 Metode *Network Development Life Cycle* (NDLC)

Siklus Pengembangan Jaringan (*Network Development Life Cycle* - NDLC) adalah sebuah pendekatan yang bergantung pada tahap-tahap pembangunan yang telah ada, termasuk perencanaan strategi bisnis, tahap siklus hidup pengembangan aplikasi, dan analisis distribusi data. Pendekatan ini terdiri dari langkah-langkah seperti analisis, desain, prototipe simulasi, implementasi, dan pemantauan.

### 3.4 Skema Penelitian

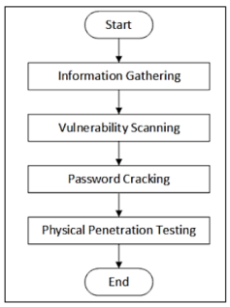
Sesuai dengan penjelasan tentang keamanan jaringan pada Bab II, keamanan jaringan adalah suatu sistem yang berfungsi untuk menghindari aktivitas yang tidak diinginkan dengan cara mengidentifikasi pengguna yang tidak memiliki hak akses di dalam suatu jaringan. Saat menghubungkan komputer dengan komputer lain, baik melalui jaringan kabel atau nirkabel, dapat membuka kemungkinan bagi pihak lain untuk mengakses data, mengubah konten, bahkan menghapus data yang ada dalam jaringan tersebut. Pengendalian keamanan jaringan dapat dilakukan dengan menyesuaikan pengaturan berbagi jaringan pada komputer, yang bertujuan untuk membatasi folder dan file yang hanya bisa diakses oleh pengguna tertentu. Hasilnya, pengguna yang tidak memiliki izin tidak dapat melihat folder atau file tersebut.

### 3.5 Analisis Jaringan

Dalam jaringan komputer PT Pinus Merah Abadi, terdapat dua metode serangan yang umum terjadi, yaitu *Sniffing* dan DoS (*Denial of Service*). *Sniffing* adalah suatu tindakan *cybercrime* di mana pelaku dengan sengaja atau tanpa sengaja mencuri *username dan password* orang lain. Pelaku kemudian dapat menggunakan akun korban untuk melakukan penipuan atas nama korban atau merusak dan menghapus data milik korban. Serangan ini seringkali dilakukan dengan menggunakan program sniffer yang berfungsi sebagai alat untuk menganalisis jaringan dan memantau lalu lintas data dalam jaringan komputer. Program tersebut mengkonfigurasi kartu jaringan (LAN Card) untuk memantau semua paket data yang melewati jaringan, tanpa memedulikan siapa pengirim atau penerima paket data tersebut.

### 3.6 *Penetration Testing*

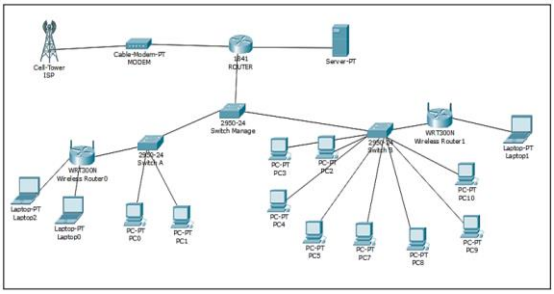
Pada ilustrasi di bawah ini, teknik yang diterapkan dalam simulasi serangan adalah salah satu elemen krusial dalam audit keamanan. Proses-langkah dalam melakukan *Penetration Testing*.




**Gambar 1** Flowchart Pengujian Penelitian Penetration Testing

### 3.7 Topologi Jaringan PT Pinus Merah Abadi

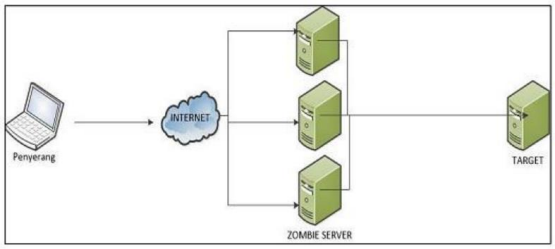
Setelah melakukan penelitian di PT Pinus Merah Abadi, penulis dapat menggambarkan susunan jaringan *local area network* (LAN) yang ada di lokasi tersebut, sesuai dengan kebutuhan komputer-komputer klien atau yang disebut juga sebagai *Workstation*. Struktur jaringan ini mencakup workstations dari setiap divisi yang beroperasi di PT Pinus Merah Abadi. Namun, jika alamat IP diberikan secara statis, ini dapat menimbulkan masalah bagi administrator jaringan karena memerlukan waktu yang cukup lama untuk memberikan alamat IP kepada setiap perangkat. Namun, masalah ini dapat diatasi dengan menggunakan DHCP (*Dynamic Host Configuration Protocol*). DHCP adalah salah satu metode otomatisasi pemberian alamat IP, di mana komputer akan meminta alamat IP yang benar dari router. Pengaturan DHCP dapat dilakukan pada router melalui antarmuka baris perintah (CLI - *Command Line Interface*). Dengan penggunaan DHCP, administrator jaringan tidak perlu lagi menghabiskan waktu untuk memikirkan alamat IP host yang akan digunakan, karena router akan secara otomatis memberikan alamat IP kepada perangkat tersebut. Administrator jaringan hanya perlu memilih opsi DHCP atau "Dapatkan Alamat IP Secara Otomatis" dalam pengaturan alamat IP.



**Gambar 2** Topologi Jaringan di PT Pinus Merah Abadi

### 3.8 Skenario Pengujian

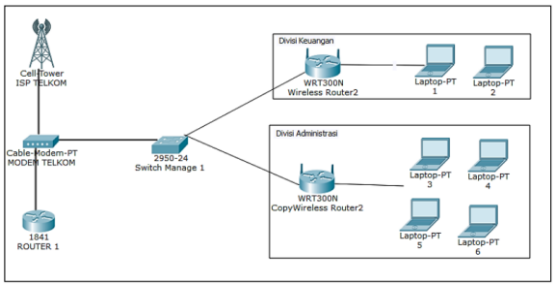
DDoS (*Distributed Denial of Service*) adalah bentuk serangan terhadap komputer atau server dalam jaringan internet dengan tujuan menggunakan sumber daya yang dimiliki oleh komputer tersebut hingga komputer tersebut tidak dapat menjalankan fungsinya dengan baik. Ini mengakibatkan secara tidak langsung mencegah pengguna lain untuk mengakses layanan dari komputer yang diserang. Ilustrasi di atas menggambarkan serangan DoS di mana penyerang menggunakan komputer zombie untuk melancarkan serangan. Dalam serangan DoS, penyerang atau hacker berusaha menghalangi akses seorang pengguna terhadap sistem atau jaringan dengan cara membanjiri lalu lintas jaringan dengan mengirimkan sejumlah besar data. Hal ini membuat lalu lintas jaringan dari pengguna lain menjadi terhambat untuk masuk ke dalam sistem jaringan, dan dengan berbagai cara, termasuk mengubah konfigurasi sistem atau bahkan merusak fisik komponen dan server target yang dituju.




**Gambar 3** Attacking/Strassing dengan DDoS

### 3.9 Usulan Topologi Jaringan

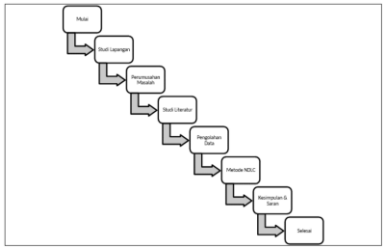
Pada penelitian ini penulis mencoba untuk menggambarkan dalam bentuk simulasi jaringan usulan tersebut menggunakan software simulator. Software yang penulis gunakan adalah Cisco Packet Tracer.




**Gambar 4** Topologi Jaringan PT Pinus Merah Abadi (Usulan)

### 3.10 Tahapan Penelitian

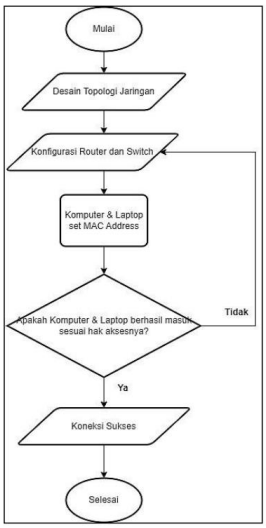
Tahapan penelitian merupakan suatu langkah berpikir yang dapat digunakan sebagai pendekatan untuk mengatasi masalah. Dalam penelitian ini, metode yang digunakan adalah metode eksperimen, di mana eksperimen atau simulasi dilakukan menggunakan aplikasi Cisco Packet Tracer. Berikut adalah langkah-langkah penelitian yang diterapkan dalam penelitian ini.



**Gambar 5** Tahapan Penelitian

### 3.11 Rancang Bangun Jaringan

Dalam alur diagram penelitian, langkah pertama adalah merancang topologi jaringan, diikuti oleh proses konfigurasi router dan switch. Selanjutnya, data MAC Address dari setiap perangkat dalam ruangan, seperti komputer dan laptop, dimasukkan ke dalam pengaturan jaringan. Kemudian, dilakukan validasi untuk memeriksa apakah MAC Address yang telah terdaftar berhasil masuk ke dalam konfigurasi jaringan atau tidak. Jika berhasil, koneksi dianggap berhasil dan keamanan jaringan telah berhasil dikonfigurasi. Namun, jika MAC Address perangkat yang telah terdaftar tidak berhasil masuk, maka akan dilakukan pengecekan ulang atau rekonfigurasi router dan switch.

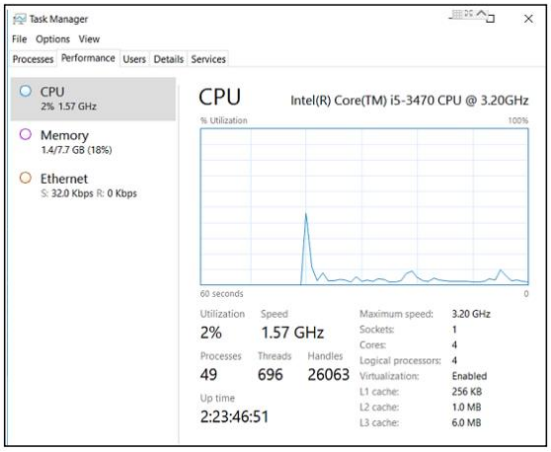



**Gambar 7** *Flowchart* Rancang Bangun Jaringan

## 4. HASIL DAN PEMBAHASAN

### 4.1 Simulasi Serangan DoS

Sebelum memulai simulasi serangan DoS, kita dapat mengamati performa komputer yang sedang menjalankan aplikasi distribusi yang belum terkena serangan, seperti yang terlihat pada ilustrasi di bawah ini. Pada situasi normal tanpa adanya serangan, penggunaan sumber daya komputer saat membuka aplikasi tidak terlalu signifikan. Ilustrasi ini diambil dari Task Manager dalam sistem operasi Windows, dan sumber daya yang diamati mencakup CPU, memori, serta aktivitas jaringan. Dalam keadaan ini, penggunaan CPU hanya sekitar 2% dengan frekuensi 1.5 GHz, penggunaan memori sekitar 18% dengan kapasitas 1.4 GB, dan aktivitas jaringan hanya sekitar 32 kbps.



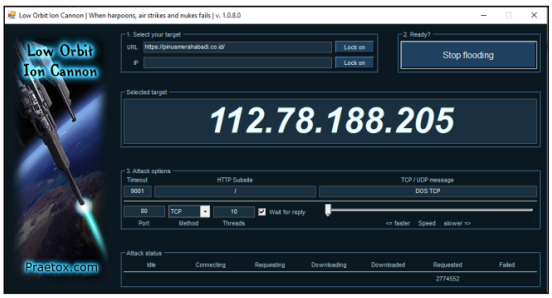

**Gambar 8** Kinerja windows tanpa serangan

### 4.2 Proses Kinerja Komputer Saat DoS Menyerang

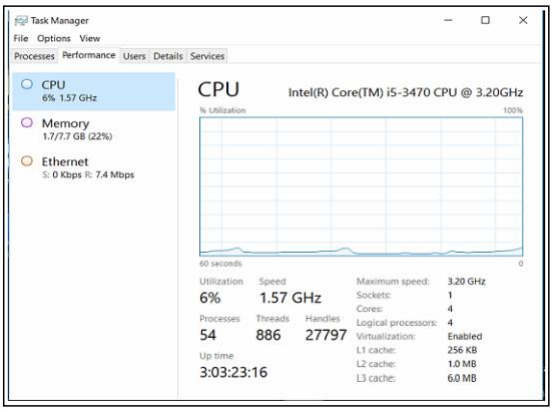
Simulasi serangan DoS dimulai dengan menggunakan aplikasi yang disebut *Low Orbit Ion Cannon* (LOIC). Berikut adalah percobaan DoS pada komputer melalui protokol TCP. Mulailah dengan memasukkan URL https://pinusmerahabadi.co.id/ sebagai target, kemudian aktivasi. Selanjutnya, masukkan 10 thread dan pilih metode TCP. Tambahkan pesan "Serangan TCP" sebagai payload. Setelah percobaan serangan DoS dilakukan pada komputer melalui protokol TCP, terlihat peningkatan penggunaan sumber daya komputer. Pada percobaan ini, penggunaan CPU meningkat sebesar 4%, penggunaan memori juga mengalami peningkatan sebesar 6%, dan aktivitas jaringan meningkat secara signifikan dari sebelumnya, yang awalnya maksimal 320 kbps menjadi 7,4 Mbps. Hal ini menunjukkan bahwa serangan DoS melalui protokol TCP memiliki dampak yang cukup besar terhadap kinerja komputer. Meskipun demikian, sistem Windows pada komputer tetap mampu menangani serangan DoS ini dengan baik karena penggunaan CPU dan memori tidak melebihi 70%.

Selanjutnya, berikut adalah percobaan serangan DoS ke komputer melalui protokol UDP. Masukkan URL https://pinusmerahabadi.co.id/ sebagai target, kemudian aktifkan. Selanjutnya, tambahkan 10 thread dan pilih metode UDP. Masukkan pesan "Serangan UDP" sebagai payload. Setelah percobaan serangan DoS dilakukan pada komputer melalui protokol UDP, terlihat peningkatan yang lebih drastis dalam penggunaan sumber daya komputer. Pada percobaan ini, penggunaan CPU meningkat secara signifikan dari 2% menjadi 26%, penggunaan memori tetap sekitar 18% seperti pada serangan DoS melalui TCP, dan aktivitas jaringan juga mengalami peningkatan, meskipun sedikit lebih rendah daripada serangan DoS melalui TCP, yaitu dari 320 kbps menjadi 25,3 Mbps. Hal ini menunjukkan bahwa serangan DoS melalui protokol UDP memiliki dampak yang lebih

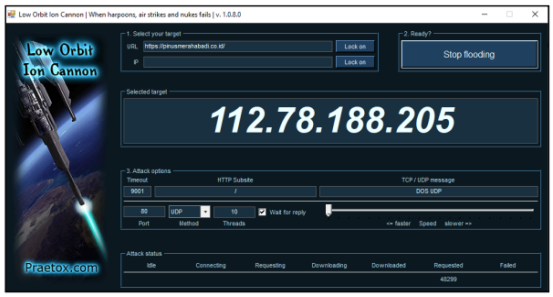
besar daripada serangan DoS melalui protokol TCP pada komputer berbasis Windows.



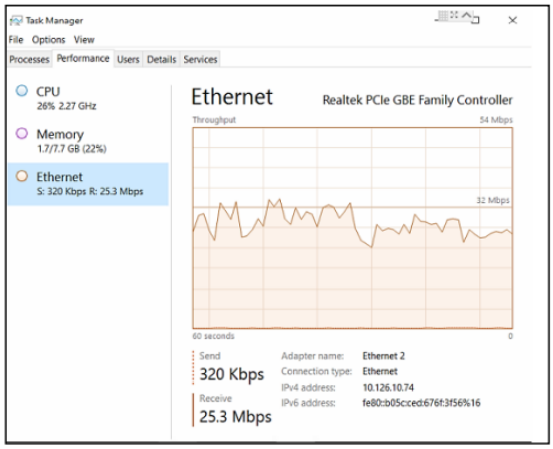

**Gambar 9** LOIC protokol TCP target




**Gambar 10** Kinerja Windows Komputer saat DoS melalui TCP




**Gambar 11** LOIC protokol UDP target




**Gambar 12** Kinerja Windows Komputer saat DoS melalui UDP

### 4.3 Desain Simulasi

Dalam simulasi mengenai keamanan port switch, penulis memanfaatkan konfigurasi topologi bintang, yang sesuai dengan perangkat yang tersedia, yaitu satu router dan dua switch. Dalam percobaan simulasi ini, penulis melakukan pengujian dengan melibatkan lima klien. Berikut ini adalah tabel alamat yang digunakan.

**Tabel 1** 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 |

### 4.4 Hasil Simulasi

Dalam hasil simulasi jaringan dengan switch port, kita memulai dari port Fa0/2. Status switch port Fa0/2 dapat ditemukan dalam ilustrasi berikut ini.

```
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 13** Status Switch Port Fa0/2

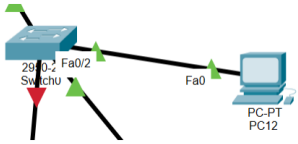
```
C:\>ping 192.168.3.3

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 14** Ping dari PC 12



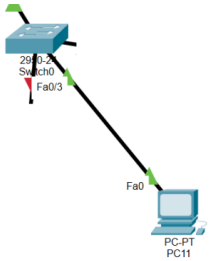

**Gambar 15** Koneksi tidak terputus walaupun pada PC12

Gambar 13 menampilkan bahwa switch port Fa0/2 memiliki status aktif dengan pengaturan keamanan port jenis "sticky port security" dan mode pelanggarannya diatur ke "protection". Mode ini berfungsi untuk menghapus data yang berasal dari host yang tidak terdaftar dalam daftar keamanan. Sebagai contoh, jika switch port Fa0/2 terhubung dengan PC12 dan PC tersebut melakukan ping, hasilnya akan menunjukkan "request timed out," namun koneksi tetap aktif, seperti yang terlihat pada Gambar 14 dan 15.

Dalam hasil simulasi jaringan dengan switch port Fa0/3, kita dapat melihat status dari switch port Fa0/3 dalam ilustrasi berikut ini.

```
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 16** Status Switch Port Fa0/3




**Gambar 17** Memindahkan koneksi pada PC11

```
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 18** 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 19** Status akhir Switch Port Fa0/3 dengan MAC Address berbeda

Seperti yang tergambar dalam Gambar 16, dapat diamati bahwa port security pada port Fa0/3 beroperasi dalam kondisi aktif dengan jumlah maksimal alamat MAC yang sudah tercapai dan pengaturan mode pelanggaran (violation mode) yang diatur sebagai "restrict". Berbeda dengan mode "protection", dalam mode ini ketika port Fa0/3 digunakan oleh host dengan alamat MAC yang berbeda, sambungan tidak akan terputus, namun data akan dihapus, dan penghitungan pelanggaran (violation count) akan tercatat. Sebagai contoh, pada Gambar 17, ketika PC11 melakukan ping, akan terjadi "request timed out," dan pada saat yang bersamaan, jumlah pelanggaran (violation count) akan bertambah, seperti yang diperlihatkan pada Gambar 18 dan 19.

Dalam hasil simulasi jaringan dengan switch port Fa0/4, kita bisa melihat status dari switch port Fa0/4 pada ilustrasi berikut ini.

```
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 20** Status Switch Port Fa0/4

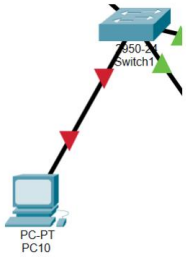
```
C:\>ping 192.168.3.3

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 21** Ping dari PC10




**Gambar 22** 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 23** Status port fa0/4 setelah dilakukan ping dengan MAC Address berbeda

Dalam Gambar 20, terlihat bahwa port security pada switch port Fa0/4 berada dalam keadaan aktif dengan pengaturan jenis "sticky port security" dan mode pelanggarannya diatur sebagai "shutdown". Mode "shutdown" akan mengakibatkan pemutusan koneksi otomatis ketika port Fa0/4 dihubungkan dengan host yang memiliki alamat MAC yang berbeda. Sebagai contoh, ketika port Fa0/4 terhubung dengan PC10 dan kemudian dilakukan ping, koneksi akan secara otomatis terputus, seperti yang terlihat dalam Gambar 22. Selanjutnya, dalam Gambar 23, status portnya menunjukkan "secure shutdown," yang berarti sudah tidak aktif secara otomatis, dan jumlah pelanggaran (violation count) akan terus bertambah.

## 5 KESIMPULAN DAN SARAN

### 5.1 Kesimpulan

Berdasarkan penelitian dan pengujian pada Simulasi Keamanan Jaringan Dengan Metode Network Development Life Cycle Menggunakan Switch Port Security Pada PT Pinus Merah Abadi

yang telah dilakukan oleh penulis pada penelitian ini dapat disimpulkan sebagai berikut:

1. Dalam percobaan untuk menguji kerentanan serangan DoS dengan alat LOIC pada komputer klien yang terhubung ke jaringan di perusahaan PT Pinus Merah Abadi, terdeteksi penurunan kinerja CPU sebesar 16% melalui protokol UDP, sementara penggunaan memori meningkat sebesar 10%. Dampaknya adalah bahwa komputer di PT Pinus Merah Abadi mengalami kendala dalam menjalankan tugasnya secara efisien. Saat mencoba mengakses aplikasi login, seringkali komputer mengalami kegagalan atau bug yang mengganggu operasional perusahaan.
2. Hasil simulasi keamanan jaringan menggunakan perangkat Cisco Packet Tracer menunjukkan bahwa penggunaan konfigurasi switch port security dengan pengaturan sticky port security adalah pilihan yang paling efektif dan efisien. Pendekatan ini memungkinkan pendaftaran otomatis dari sejumlah besar alamat MAC yang digunakan, sambil mengimplementasikan mode pelanggaran "shutdown" yang aman. Dengan cara ini, koneksi perangkat yang tidak dikenal secara otomatis terputus, yang pada gilirannya meningkatkan tingkat keamanan data pada perangkat lain dalam jaringan.
3. Port security pada switch bertindak sebagai perlindungan terhadap serangan luar yang dilakukan oleh perangkat yang tidak terdaftar dalam konfigurasi switch. Ini mencakup serangan DoS yang berupaya mengakses perangkat pengguna melalui IP atau mencoba menggunakan username dan password pada komputer.

### 5.2 Saran

Berdasarkan temuan dari studi tentang keamanan jaringan di PT Pinus Merah Abadi, terdapat kebutuhan akan peningkatan yang lebih lanjut guna mencapai hasil yang optimal. Penulis ingin mengusulkan beberapa rekomendasi untuk studi lanjutan sebagai berikut:

1. Dalam rangka pengujian serangan, disarankan untuk mempertimbangkan penggunaan alat-alat lain, seperti Hoic atau Tor Hammer, sebagai perbandingan yang relevan dalam kerangka penelitian ini.
2. Port security adalah salah satu aspek dasar dalam strategi keamanan jaringan, oleh karena itu, diperlukan penerapan teknik-teknik lanjutan seperti IP source guard, DHCP snooping, dynamic ARP, dan sebagainya, untuk menjaga keamanan data dalam skala yang lebih besar.

## 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 Kejuran 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.