Perancangan dan Implementasi Sistem Keamanan Jaringan dengan Port Security Menggunakan Switch CISCO di PT. Citra Solusi Pratama

Laily Azharuddin, Jenih, Tony Sugiarso, Tiwi Nurhastuti
Program Studi Ilmu Komputer
Fakultas Teknologi Informasi, Universitas Respati Indonesia
Email : Laily.azhar7@gmail.com, jenih@fti.urindo.ac.id,
tony.sugiarso@urindo.ac.id, tiwi@urindo.ac.id

ABSTRAK

Port Security merupakan mekanisme keamanan yang digunakan pada switch Cisco. Dengan port security, kita bisa membatasi jumlah host yang dapat terkoneksi pada sebuah port yang ada di switch serta menentukan host mana saja yang bisa terkoneksi ke switch. *Port Security* dapat menjadi salah satu alternatif untuk mengamankan data pada jaringan lan (*local area netwok*), dari pencurian data oleh pihak yang tidak di inginkan. terdapat beberapa metode dalam pembuatan *Port Security* , salah satunya sticky port security di mana kemampuan switch dalam mengenal *Mac address* tiap tiap perangkat yang terhubung dan akan memblok setiap *Mac* yang melebihi dari *Mac* yang telah terdaftar. dengan menggunakan *Security Port*, maka system keamanan jaringan yang diterapkan lebih aman untuk menghidari koneksi jaringan dari akses yang tidak berkepentingan.

Kata kunci : *port, security, switch*

ABSTRACT

Port Security is a security mechanism used on Cisco switches. With port security, we can limit the number of hosts that can connect to a port on the switch and determine which hosts can connect to the switch. Port Security can be an alternative to securing data on a LAN (local area network) network, from data theft by unwanted parties. There are several methods in creating Port Security, one of which is sticky port security where the switch's ability to recognize the Mac address of each connected device and will block any Mac that exceeds the registered Mac. By using Port Security, the network security system implemented is safer to avoid network connections from unauthorized access.

Keywords: port, security, switch

PENDAHULUAN

Kebutuhan akan jaringan komputer semakin bertambah penting, baik dalam pendidikan, pekerjaan maupun dalam sebuah permainan. Salah satu hal penting dalam mengelola jaringan komputer yaitu kemanan dari jaringan itu sendiri, dengan banyaknya akses ke jaringan tersebut maka akan banyak pula peluang kejahatan yang terjadi didalam jaringan tersebut, misalkan adanya pencurian data yang terjadi dijaringan tersebut ataupun adanya peretas yang mematikan sumber daya jaringan tersebut.

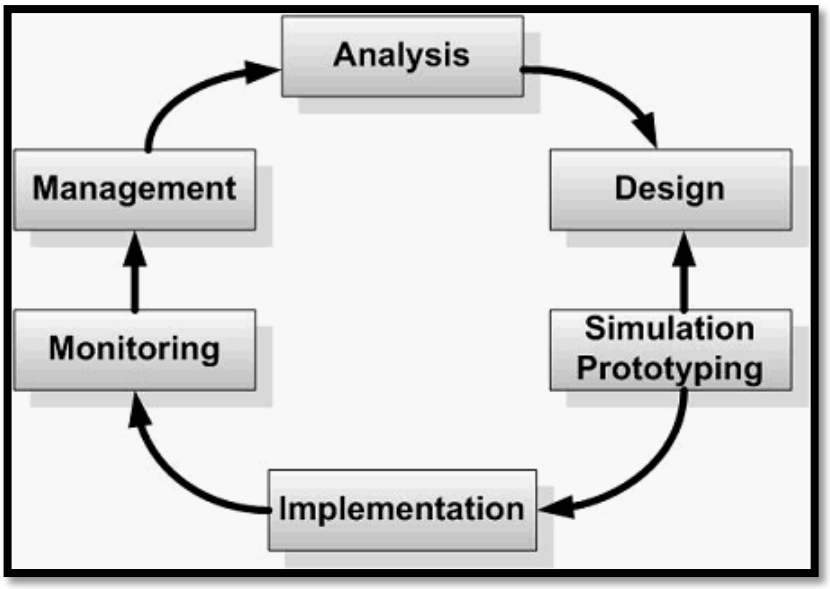
Banyak teknik yang dapat diupayakan dalam memperkecil tingkat kejahatan dalam jaringan ini, salah satu teknik yang banyak digunakan untuk pengamanan jaringan lokal adalah dengan menggunakan switch port security, switch port security merupakan teknik yang akan mengizinkan siapa saja yang berhak menggunakan akses jaringan melalui port yang tersedia di switch, dalam hal ini sangat perlu diterapkan karena setiap perangkat user akan menginformasikan mac address-nya dan terdeksripsi dalam port yang digunakan.

Dalam Kasus PT. citra solusi pratama adalah seringnya terjadi pencurian data disaat karyawan tersebut pindah ruangan atau keluar dari perusahaan sehingga membutuhkan pengamanan data menggunakan perangkat yang bisa mengontrol hak akses jaringan, sehingga perusahaan ini sangat membutuhkan adanya pengamanan jaringan pada setiap *Port* LAN (*Local Area Network*) yaitu dengan menggunakan metode *Port security* pada *Port* yang berada diruang kerja tersebut. Fungsi dari port security adalah membatasi dan mendaftarkan perangkat end device mana saja yang dibolehkan di pasang di switch. Jadi switch tersebut akan menghafal atau menyimpan mac address dari host yang terhubung, sehingga yang dapat mengakses hanya host si pemilik dari mac address tersebut. Sehingga data yang kita miliki akan aman dari orang-orang yang ingin

mengambilnya, hal ini bertujuan untuk membatasi akses jaringan sehingga mencegah terjadinya pencurian data oleh orang asing maupun karyawan perusahaan.

METODE PENELITIAN

NDLC (*Network Developmen Life Cycle*) yaitu metode yang digunakan untuk mengembangkan atau merancang suatu jaringan infrastruktur yang memungkinkan terjadinya pemantauan jaringan untuk mengetahui statistik kinerja jaringan. Metode ini terdiri dari *analysis, design, simulation prototype,* implementasi, dan juga monitoring.



Gambar 1 Metode NDLC

1. Analisis

Tahap awal ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul di PT. Citra Solusi Pratama, analisa keinginan pengguna, dan analisa topologi jaringan yang sudah ada. Metode yang biasa digunakan pada tahap ini diantaranya:

a. Wawancara, dilakukan dengan pihak terkait melibatkan dari struktur manajemen atas sampai ke level bawah agar mendapatkan data yang konkrit dan lengkap dari Karyawan PT. Citra Solusi Pratama.
b. Survei langsung kelapangan, pada tahap analisis juga dilakukan survei langsung ke lapangan untuk mendapatkan kondisi sesungguhnya dan gambaran seutuhnya sebelum masuk ke tahap desain.
c. Membaca manual atau *blueprint* dokumentasi, pada analisis awal ini juga dilakukan dengan mencari informasi dari manual-manual atau *blueprint* dokumentasi yang mungkin pernah dibuat sebelumnya.

2. Desain

Maksud dari tahap perancangan (*design*) adalah membuat spesifikasi kebutuhan sistem dari hasil analisis sebagai masukan dan spesifikasi rancangan atau desain sebagai solusi dari permasalahan. Spesifikasi desain sistem yang akan dibuat, dibentuk dengan merancang topologi sistem jaringan.

3. Simulasi Prototipe

Pada tahap ini penulis akan menganalisa dengan cara membuat dalam bentuk simulasi dengan bantuan *tools* khusus dibidang jaringannya, yaitu C*isco Packet Tracer*.

4. Implementasi

a. Konfigurasi dan analisis yang meliputi proses instalasi dan konfigurasi terhadap rancangan topologi jaringan dan komponen jaringan yang perlu dilakukan konfigurasi yaitu:

1) Switch
2) Pc / Laptop

b. Proses instalasi dan konfigurasi

Proses instalasi dan konfigurasi dilakukan untuk menjamin

interkonektifitas keseluruhan komponen jaringan agar dapat bekerja secara efektif, baik pada topologi jaringan maupun pada komponen jaringan yang akan dibangun.

5. Monitoring

Pada tahap ini pentingnya monitoring untuk memantau secara rutin perangkat yang bermasalahah dan berpotensi mengganggu jaringan internet atau jaringan internal dalam kantor.

6. Management

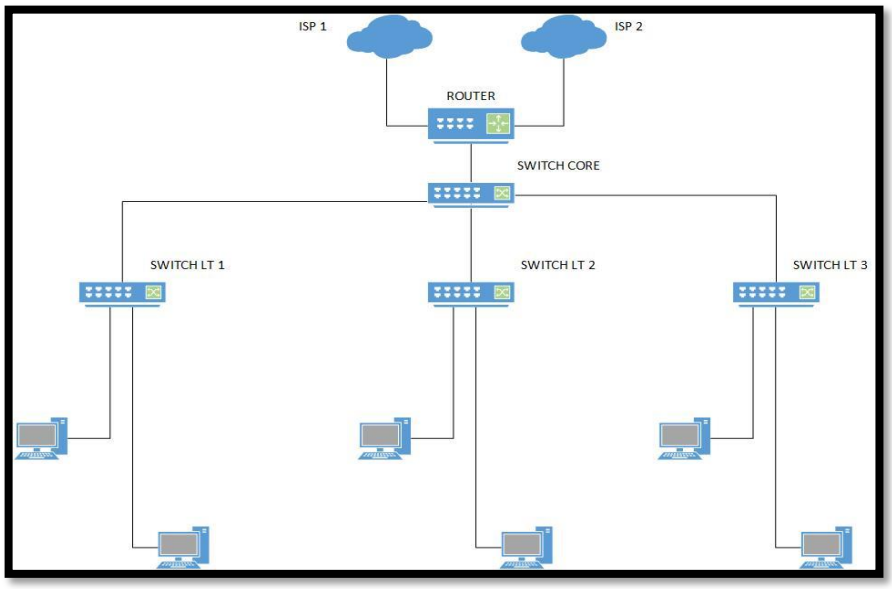
Tahapan metode pengembangan NDLC adalah manajemen. Manajemen dibuat untuk untuk mengatur dan membuat sistem yang telah di buat dapat terjaga dengan baik sehingga diperlukan *backup* konfigurasi dan *log monitoring*

PEMBAHASAN DAN HASIL

1. Konfigurasi Sistem Jaringan

Konfigurasi sistem jaringan disini menjelaskan alur dari topologi jaringan, Spesifikasi teknik hardwaret dan Spesifikasi teknik software apa saja yang digunakan.

a. Topologi Jaringan



Gambar 2. Topologi jaringan

b. **Spesifikasi Teknis *hardware***

Dalam penelitian ini terdapat beberapa hardware sebagai perangkat yang sudah berjalan. Adapun perangkat dan spesifikasinya adalah sebagai berikut:

1) Switch Cisco Catalys 2960

Switch untuk memfasilitasi berbagi sumber daya dengan menghubungkan semua perangkat, termasuk komputer, printer, dan *server*, dalam jaringan bisnis kecil

2) Kabel UTP Cat6

Kabel UTP *(Unshielded Twisted Pair)* yang digunakan untuk melakukan instalasi ataupun konfigurasi jaringan pada PT. Citra Solusi Pratama

3) Konektor RJ45

Konektor yang dipasang pada ujung kabel UTP pada PT. Citra Solusi Pratama menggunakan konektor RJ45.

c. Spesifikasi Teknis Software

Dalam pengujian, penulis menggunakan *software* sebagai media implementasi rancangan jaringan baru. Untuk *software* yang digunakan yaitu:

***Cisco* Packet Tracert**

Packet Tracer adalah simulasi jaringan yang telah di kembangkan oleh *cisco*, dan dapat digunakan dalam pelatihan untuk ujian sertifikasi CCNA dan CCNP dengan memungkinkan membuat jaringan dengan jumlah perangkat yang hampir tidak terbatas dan mengalami pemecahan masalah tanpa harus membeli *router* atau *switch cisco* yang sebenarnya.

2. Pengecekan Prioritas Switch *Port Security*

Sebelum melakukan pengujian, diperlukan pengecekan prioritas yang sudah dikonfigurasi. Bertujuan untuk memastikan konfigurasi yang dimasukkan sudah berhasil tersimpan didalam *switch*. Berikut ini adalah tampilan status *Port Security* di setiap *switch*.

Switch lantai 1 (*Static Port Security*)

Tampilan status *Static Port Security* pada *Port* 02 switch

```
LANTAI1#sh port-security interface fa0/2
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   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0002.4AAE.696D:10
Security Violation Count   : 0
```

Gambar 3 Static Port switch lantai 1

3. Pengujian Jaringan

Test ping dapi laptop 1 ke *Port* interface fa02 di switch (*Static Port Security*)

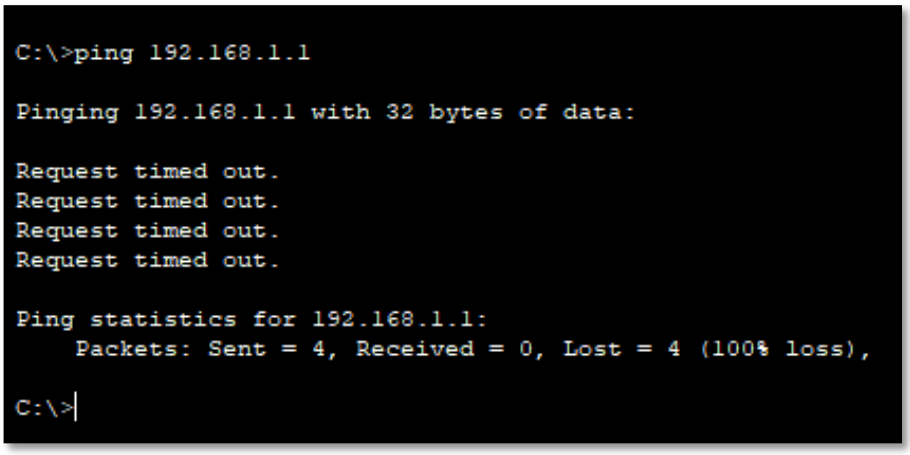
```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Gambar 4 Test ping Static Port 2

Hasil dari gambar di atas menunjukkan bahwa *test ping* dari komputer ke *switch Port 2* sudah berhasil dilakukan, dimana uji koneksi menunjukkan hasil "Reply from 192.168.1.1: bytes=32 time=1ms TTL=255" yang artinya sudah berhasil, pengujian menggunakan laptop

yang sudah di daftarkan *Mac* addresnya.

Selanjutnya akan dilakukan pengujian dengan menghubungkan laptop client dengan memindah koneksi pada Lapto1 ke laptop 2 yang belum di daftarkan *Mac* addresnya di *Port* 2



Gambar 1 Hasil test ping dari Laptop 2

Hasil dari gambar di atas menunjukkan bahwa *test ping* dari komputer ke *switch Port 2* sudah berhasil dilakukan, dimana uji koneksi menunjukkan hasil Request time out yang artinya sudah berhasil, pengujian menggunakan Laptop yang belum di daftarkan *Mac* addresnya, maka hasilnya tidak bisa terhubung ke jaringan dan *Port* otomatis langsung dinonaktifkan.

SIMPULAN

Berdasarkan hasil dari implementasi dan pengujian, maka dapat diambil kesimpulan yaitu Default / *Static Port Security* digunakan untuk satu *Port* yang akan diblok, pada kemampuan pengamanan ini cocok di gunakan untuk kepala devisi dikarenakan kemampuan *Static Port Security* hanya mampu mendaftarkan satu *Mac-address*. Dengan menggunakan Security *Port*, maka system keamanan jaringan diterapkan lebih aman untuk menghidari koneksi jaringan dari akses yang tidak berkepentingan, serta menjaga data tersebut karena dapat dicuri oleh pihak yang tidak bertanggung jawab.

DAFTAR PUSTAKA

Ilahi, Ilham. 2020. *Administrasi Infrastruktur Jaringan*. Surabaya: CV.Xp Solution.

Suprapto, Untung. 2018. *Komputer dan Jaringan Dasar*. Jakarta: PT.Gramedia Widiasarana Indonesia.

Tri Rachmadi, S.Kom. 2020. *Jaringan Komputer*. Tiga Ebook, Jakarta.

Abdul Karim, Andi Achmadi. 2018. Analisis Kinerja Koneksi Jaringan Switch Ethernet pada Local Area Network (LAN). p-ISSN : 2657 – 0653 di akses pada 22 juni 2022 https://journal.unismuh.ac.id/index.php/ainet/article/view/2283/1797

A. Haryadi, H. Priyanto, H. Anra. 2017.RANCANG BANGUN APLIKASI PENYISIPAN BERITA DENGAN INTERNET CONTENT ADAPTATION PROTOCOL, Jurnal Sistem dan Teknologi Informasi (JUSTIN) Vol. 5, No. 3.di akses dari https://jurnal.untan.ac.id/index.php/justin/article/view/20575/16829

Aji, S., Fadlil, A., & Riadi, I. (2018). Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan. Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika, 3 No. 1. Diakses pada 24 juni 2022 https://doi.org/10.26555/jiteki.v3i1.5665

ALFRIDA MAKKALO 2020 ANALISIS SISTEM KEAMANAN JARINGAN DENGAN MENGGUNAKAN SWITCH PORT SECURITY PADA SEKOLAH MENENGAH PERTAMA NEGERI 7 PALOPO. http://repository.uncp.ac.id/406/1/Alfrida%20Makkalo-1604411449.pdf

D. Alfurqon. 2018. Analisis Dan Perancangan Jaringan Local Area Network Pada Laboratorium Smk Negeri 1 Kota Jambi. J. Manaj. Sist. Inf., vol. 3, no. 3, pp. 1149–1163. Diakses pada tanggal 23 juni 2022 https://docplayer.info/storage/89/99070693/99070693.pdf.

Irwansyah. 2021. PEMANFATAAN METODE *PORT* KNOCKING DAN BLOCKING UNTUK KEAMANAN JARINGAN BPKAD PROVINSI SUMSEL. Vol 3 No2. ISSN: 2654-5438 di akses pada 29 juni 2022 https://conference.binadarma.ac.id/index.php/semhavok/article/view/2456/995

Khashaaisha Al Fikri, Djuniadi. 2021. Keamanan Jaringan Menggunakan Switch *Port Security*. Jurnal Nasional Informatika dan Teknologi Jaringan ISSN 2540-7597 | ISSN 2540-7600. Vol 5, No 2 di akses pada 23 juni 2022 https://jurnal.uisu.ac.id/index.php/infotekjar/article/view/3501/pdf

Oris Krianto Sulaiman. 2016. ANALISIS SISTEM KEAMANAN JARINGAN DENGAN MENGGUNAKAN SWITCH *PORT SECURITY*, CESS (Journal Of Computer Engineering, System And Science) p-ISSN :2502-7131 Vol 1, No 1 di akses pada 20 juni 2022 https://core.ac.uk/download/pdf/144780313.pdf

Robby Rizky. 2019. Sistem Pakar Diagnosis Kerusakan Jaringan Local Area Network (LAN) Menggunakan Metode Forward Chaining, p-ISSN: 2252-5351 e-ISSN: 2656-0860. Vol 7 No 2. Jutis (Jurnal Teknik Informatika) diakses pada 27 juni 2022 http://ejournal.unis.ac.id/index.php/jutis/article/view/396/287

Randi Rizal. 2020. Implementasi Keamanan Jaringan Menggunakan Metode *Port* Blocking dan *Port* Knocking Pada Mikrotik RB-94. p-ISSN: 2302-0261, e-ISSN: 2303-3363 https://ejournal.ikmi.ac.id/index.php/jict-ikmi/article/view/119/134

Sendy Dwi Putra. 2021. PENGEMBANGAN KEAMANAN JARINGAN LAN DAN MANANJEMEN VLAN DI PT. PDAM TIRTA BETUAH DENGAN MENGGUNAKAN SIMULASI PACKET TRACER. Vol 3 No 1. ISSN: 2654-5438 https://conference.binadarma.ac.id/index.php/semhavok/article/view/1928/653

Sutiman. A.Gunawan. FIREWALL *PORT SECURITY* SWITCH UNTUK KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN CISCO ROUTER 1600S PADA PT. TIRTA KENCANA TATA WARNA SUKABUMI. Vol. 1, No. 1 ISSN: 2797-5274 di akses pada 30 juni 2022 http://jurnal.bsi.ac.id/index.php/conten/article/view/402/225

Syaiful Jamal. 2018 (12140391), Analisa Keamanan Jaringan dengan Menggunakan Switch Port Security Pada Suku Dinas Komunikasi dan Informatika Jakarta Barat. https://repository.nusamandiri.ac.id/index.php/unduh/item/230489/12140391_12_8A_05_56575.pdf

Sudaryanto. 2018. IMPLEMENTATION *PORT SECURITY* FOR SECURITY SYSTEMS NETWORK AT THE COMPUTING LABORATORY OF ADISUTJIPTO TECHNOLOGY COLLEGE. ISBN 978-602-52742-0-6. Vol. IV di akses pda 25 juni 2022 https://senatik.itda.ac.id/index.php/senatik/article/view/239/pdf

Tony Sanjaya. Didik Setiyadi. 2019. Network Development Life Cycle (Ndlc) Dalam Perancangan Jaringan Komputer Pada Rumah Shalom Mahanaim. Jurnal Mahasiswa Bina Insani, Vol. 4, No. 1, Agustus 2019