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

Laily Azharuddin, Tiwi Nurhastuti
Program Studi Ilmu Komputer
Fakultas Teknologi Informasi, Universitas Respati Indonesia
Email : Laily.azhar7@gmail.com, 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 diamana 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, firewall, knocking*

ABSTRACT

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

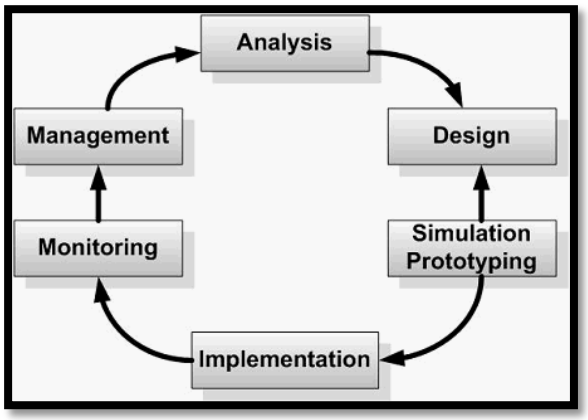
PENDAHULUAN

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. 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. Tujuan penelitian ini adalah untuk meningkatkan Sistem Keamanan Jaringan dengan Menggunakan Switch *Port Security* PT. Citra Solusi Pratama, sehingga dapat diketahui tingkat keamanan jaringan yang ada dan dibuatkan usulan sistem keamanan jaringan yang lebih aman.

METODE PENELITIAN

A. Pendekatan 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

1. Konfigurasi dan analisis yang meliputi proses instalasi dan konfigurasi terhadap rancangan topologi jaringan dan komponen jaringan yang perlu dilakukan konfigurasi yaitu:
   a. Switch
   b. Pc / Laptop
2. 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

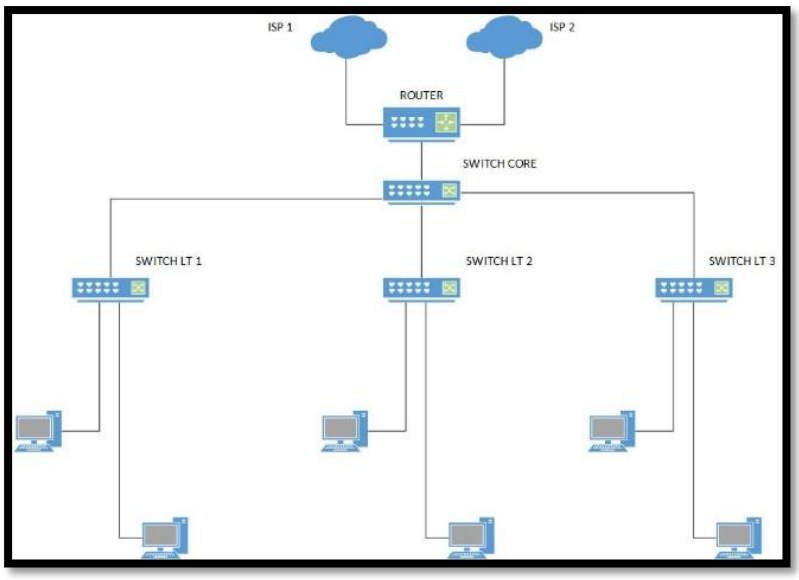
Pada tahap ini pentingnya monitoring untuk memantau secara rutin perangkat yang bermasalahah dan berpotensi mengganggu jaringan internet atau jaringan internal dalam kantor.

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*

B. Topologi jaringan

Topologi yang sedang berjalan di PT.Citra Solusi Pratama menggunakan topologi *tree*. Topologi jaringan disini hanya mencakup satu area kantor dan belum mencakup ke kantor cabang. Berikut topologi jaringan dari PT.Citra Solusi Pratama:



Gambar 2. Topologi Jaringan kantor 80

C. Rancangan sistem jaringan

Dalam menetapkan keamanan jaringan yang akan diusulkan, akan dilakukan dalam sebuah simulasi. Dimana akan diberikan 3 jenis konfigurasi switch *security Port* yaitu, *Default /Static Port Security, Port Security Dynamic learning, Sticky Port Security*. Ketiga jenis konfigurasi ini yang akan diberikan pada setiap *Port* yang ada diswitch. Dengan PC yang sudah mendaftarkan *Mac address* akan terkoneksi pada jaringan, namun pada perangkat laptop tidak mendaftarkan *Mac address* ,jika mengubungkan koneksi jaringan yang di pc maka akan otamatis jaringan akan di *shutdown* atau ter-*protect* (*Port* akan tetap menyala tetapi tidak bisa digunakan). Simulasi keamanan jaringan komputer *Port Security* menggunakan software simulator *Cisco Packet Tracer.*

1. **Konfigurasi switch cisco *Static Port Security***

Ketika *Mac address Port Security* diaktifkan pada *Port* switch, maka *Port* tidak akan mem-forward packets jika source *address* bukanlah *address* yang telah kita defenisikan/tentukan sebelumnya. *Static* dimaksud disini adalah menentukan alamat *Mac* tertentu yang di perbolehkan untuk terhubung ke *Port* tersebut secara manual.

Berikut adalah langkah-langkah konfigurasi *Static Port Security* :

a) langkah Pertama, masuk ke dalam menu konfigurasi switch

```
LANTAI1$show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0090.2be1.1eb7    DYNAMIC     Fa0/24
  10    0002.4aae.696d    DYNAMIC     Fa0/2
  10    0090.0cdd.d701    DYNAMIC     Fa0/24
  10    0090.2be1.1eb7    DYNAMIC     Fa0/24
  20    0090.2be1.1eb7    DYNAMIC     Fa0/24
  30    0090.2be1.1eb7    DYNAMIC     Fa0/24
LANTAI1#
```

Gambar 3. Gambar Tabel Mac Address

b). Langkah kedua, masuk ke dalam menu konfigurasi switch lalu ketikan " configure Terminal " kemudian Ketikan LANTAI1(config)#interface fastEthernet 0/2
LANTAI1(config-if)#switch*Port*
Port-security
lalu ketikan " enable " kemudian ketik show *Macaddress*-tabel lalu akan muncul seperti pada gambar di bawah ini.

LANTAI1(config-if)#switch*Port*
Port-security *Mac-address* 0002.4aae.696d
Ini artinya *Mac address* 0002.4aae.696d yang dimiliki oleh PC1 yang hanya diizinkan oleh switch di interface fastehternet 0/2.

```
LANTAI1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
LANTAI1(config)#interface fastethernet 0/2
LANTAI1(config-if)#switchport port-security
LANTAI1(config-if)#switchport port-security mac-address 0002.4aae.696d
LANTAI1(config-if)#exit
LANTAI1(config)#
```

Gambar 4. Gambar konfigurasi Static Port Security

2. Port Security Dynamic learning

MAC address di pelajari secara dinamis ketika perangkat terhubung ke switch, *Mac address* tersebut di simpan di *Mac address* table.

Berikut adalah langkah-langkah konfigurasi *Dynamic Port* security :

1) langkah Pertama, masuk ke dalam menu konfigurasi switch lalu ketikan " enable " kemudian ketik show *Macaddress*-tabel lalu akan muncul seperti pada gambar di bawah ini.

```
LANTAI2#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0060.3eab.7d6e    DYNAMIC     Fa0/23
  20    0005.5eac.7954    DYNAMIC     Fa0/7
  20    0009.7c15.6e17    DYNAMIC     Fa0/6
  20    0090.0cdd.d701    DYNAMIC     Fa0/23
LANTAI2#
```

Gambar 5. Gambar Tabel Mac Address

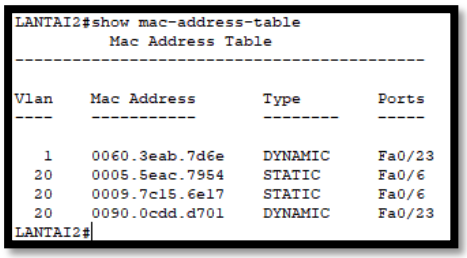
2) Langkah kedua, masuk ke dalam menu konfigurasi switch lalu ketikan " configure Terminal " kemudian Ketikan

LANTAI2(config)#interface fastEthernet 0/6
LANTAI2(config-if)#switch*Port Port*-security
LANTAI2(config-if)#switch*Port Port*-security max 2
LANTAI2(config-if)#switch*Port Port*-security *Mac-address* 0009.7c15.6e17

```
Enter configuration commands, one per line.  End with CNTL/Z.
LANTAI2(config)#int fastethernet0/6
LANTAI2(config-if)#switchport port-security
LANTAI2(config-if)#switchport port-security max 2
LANTAI2(config-if)#switchport port-security mac-address 0009.7c15.6e17
LANTAI2(config-if)#
```

Gambar 6 Gambar konfigurasi Dynamic Port Security

3) Untuk mendaftarkan *Mac* addres yang ke dua di *Port* tinggal hubungka saja pc yang di inginkan ke *Port* fa0/6 maka *Mac* addres akan otomatis terdaftar di tabel *Port Security*

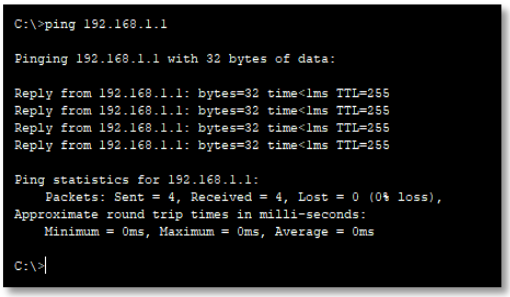


Gambar 7 Gambar Tabel Mac Address

HASIL DAN PEMBAHASAN

A. Pengujian Jaringan

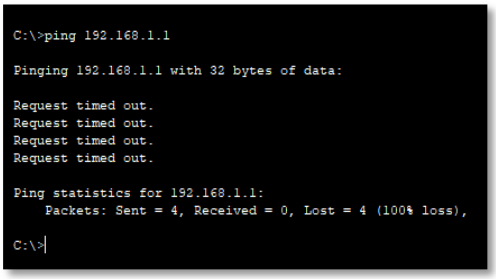
a. Test ping dapi laptop 1 ke *Port* interface fa02 di switch (*Static Port Security*)



Gambar 8 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.

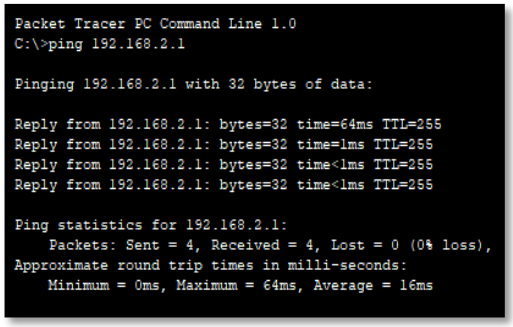
Selanjutnya akan dilakukan pengujian dengan menghubungkan laptop client dengan memindah koneksi pada Lapto1 ke laptop 2 yang belum di daftarkan *Mac* addresnya di *Port* 2



Gambar 9 Hasil test ping dari Laptop 2

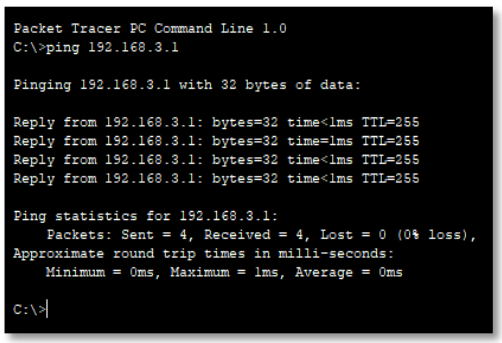
Hasil dari gambar di atas menunjukkan bahwa *test ping* dari komputer ke *switch Port 2* sudah berhasil dilakukan, dimana uji koneksi menunjukkan hasil Request time out yang artinya sudah berhasil, pengujian menggunakan Laptop yang belum di daftarkan *Mac* addresnya, maka hasilnya tidak bisa terhubung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

b. Test ping dapi laptop 2 ke *Port* interface fa06 di switch (*Dynamic Port Security*)



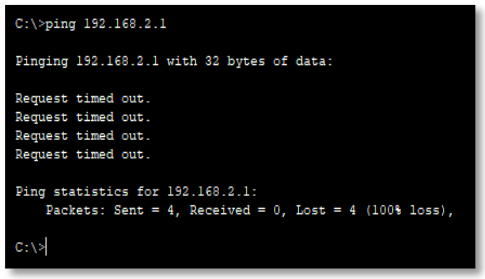
Gambar 10 Test ping Dynamic Port 6

Hasil dari gambar di atas menunjukkan bahwa *test ping* dari komputer ke *switch Port 6* sudah berhasil dilakukan, dimana uji koneksi menunjukkan hasil "Reply from 192.168.2.1: bytes=32 time=1ms TTL=255" yang artinya sudah berhasil, pengujian menggunakan laptop yang sudah di daftarkan *Mac* addresnya. Selanjutnuya akan dilakukan pengecekan dengan laptop baru yang akan di daftarkan menggunakan *Dynamic* di mana hanya perlu terhubung ke *Port* 6 karena batas maximal *Mac-address*nya ada 2



Gambar 11 Hasil test ping dari Laptop 2

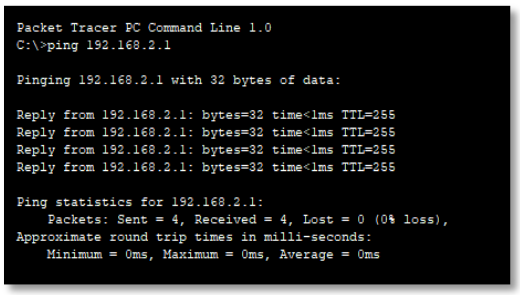
Hasil dari gambar di atas menunjukkan bahwa *test ping* dari laptop 2 ke *switch Port 6* sudah berhasil dilakukan, dimana uji koneksi menunjukkan hasil "Reply from 192.168.2.1: bytes=32 time=1ms TTL=255" yang artinya sudah berhasil, Selanjutnya akan di lakuakan pengujian test ping di *Port* 06 menggunakan Laptop3 di mana konfigurasi maxsimal *Mac*c addres sudah digunakan *Port* laptop 2



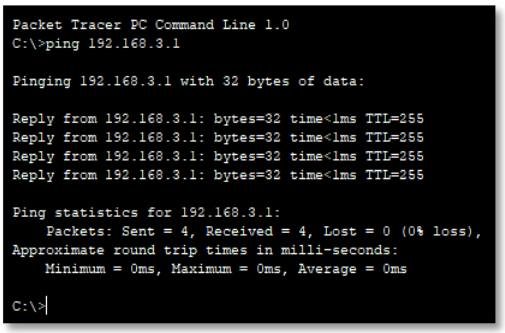
Gambar 12 hasil test ping laptop 3

Hasil dari gambar di atas menunjukkan bahwa *test ping* dari komputer ke *switch Port 6* sudah berhasil dilakukan, dimana uji koneksi menunjukkan hasil Request time out yang artinya sudah berhasil.

c. Test ping dapi laptop 1 ke *Port* interface fa11 di switch

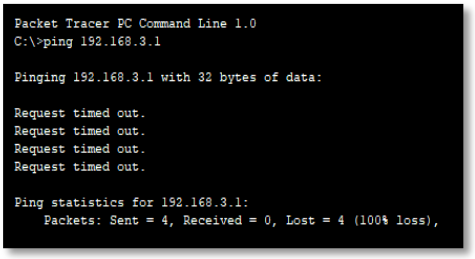


Gambar 13 Test ping Sticky Port 11



Gambar 14 hasil test ping laptop 2

Hasil dari gambar di atas menunjukkan bahwa *test ping* dari laptop 1 dan 2 ke *switch Port 1* sudah berhasil dilakukan, dimana uji koneksi menunjukkan hasil “Reply from 192.168.2.1: bytes=32 time=1ms TTL=255” yang artinya sudah berhasil, pengujian menggunakan laptop yang pertama dan kedua terhubung ke *Port*11 switch.



Gambar 15 pengecekan dari laptop 3

Pengecekan dilakukan dari laptop 3 ke *Port* 11 switch diamana hasilnya Request time out ,hasil sesuai dengan yang di inginkan penuli dan sudah berhasil karena tabel *Mac* addres hanya dapat menyimpan 2 *Mac address*.

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*. *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.

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.