Available *online* at : http://bit.ly/InfoTekJar

InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan

ISSN (Print) 2540-7597 | ISSN (Online) 2540-7600

Keamanan Jaringan Menggunakan *Switch Port Security*

Khashaaisha Al Fikri, Djuniadi

Universitas Negeri Semarang, Gunung Pati, Kota Semarang 50229, Indonesia

KEYWORDS

Keamanan jaringan, *Switch*, *Port security*

CORRESPONDENCE

Phone: -

E-mail: khaalfikri@students.unnes.ac.id

A B S T R A C T

Currently, the network is one of the most influential elements in human life. Almost everyone who has an electronic device must be connected to the internet network, whether connected by cable or wireless. In connection with the human need for the network, network security was created to protect the data contained in the network from access by irresponsible parties. one of the network security methods, namely port security which is carried out on a network device port named Switch. Switch functions to connect several computers which allow distribution of data between komputers. By using switch port security will prevent access from unknown devices from irresponsible parties. With this simulation the reader can easily select the type of port security system that is best for him. Sticky port security model is effective for registering multiple MAC addresses automatically. Then violation mode which is best used is shutdown mode.

ABSTRAK

Saat ini jaringan merupakan salah satu elemen yang berpengaruh besar dalam kehidupan umat manusia. Hampir setiap orang yang memiliki perangkat elektronik pasti terhubung oleh jaringan internet, baik yang terhubung dengan kabel maupun nirkabel. Sehubungan dengan kebutuhan manusia terhadap jaringan itulah akhirnya diciptakan keamanan jaringan untuk menjaga data yang terdapat dalam jaringan tersebut dari akses pihak tidak bertanggung jawab. Salah satu metode keamanan jaringan yaitu port security yang dilakukan pada port perangkat jaringan bernama Switch. Switch berfungsi untk menghubungkan beberapa komputer yang memungkinkan distribusi data antar komputer. Dengan menggunakan switch port security akan mencegah akses dari perangkat tak dikenal dari pihak tak bertanggung jawab. Dengan simulasi ini pembaca dapat dengan mudah memilih jenis sistem keamanan port yang terbaik baginya. Model sticky port security efektif untuk mendaftarkan banyak MAC address secara otomatis. Kemudian violation mode yang paling baik digunakan adalah *shutdown mode*.

INTRODUCTION

Perkembangan teknologi komunikasi dan informasi yang semakin canggih tidak lepas dari peran jaringan yang berperan untuk menghubungkan perangkat yang dimiliki manusia sehingga dapat bertukar data/informasi dalam hitungan sepersekian detik. Jaringan ini digunakan diberbagai perangkat, salah satunya adalah komputer, jaringan pada komputer merupakan himpunan interkoneksi antara dua komputer atau lebih yang terhubung dengan media kabel atau tanpa kabel (*wireless*). Jaringan ini memungkinkan setiap *device* yang terhubung dapat mengirim dan menerima atau bertukar data yang terdapat dalam masing-masing *device.*

Dewasa ini, kebutuhan manusia terhadap jaringan komputer semakin bertambah banyak dan penting dalam berbagai bidang. Misalnya dalam bidang pendidikan, jaringan komputer digunakan untuk siswa memperoleh pelajaran. Dalam bidang pekerjaan, jaringan komputer digunakan untuk mengirim dan menerima data/dokumen penting. Bahkan dalam sebuah permainan, jaringan digunakan untuk bertemu teman dan bermain secara *online*. Penggunaan jaringan komputer ini sudah dilakukan sejak tahun 1988 untuk membantu menyelesaikan pekerjaan di universitas-universitas dan perusahaan-perusahaan [1]. Karena jaringan ini telah menjadi bagian dari setiap kegiatan manusia tentu dalam pengelolaannya tidak boleh luput dalam segi keamanan. Kemanan jaringan digunakan untuk mencegah tindakan kejahatan yang mungkin dilakukan oleh orang yang tidak bertanggung jawab seperti tindakan penipuan, *cracking*, dsb.

Teknik keamanan jaringan yang dapat dilakukan untuk mencegah tindakan kejahatan dalam jaringan ini banyak sekali. Contohnya adalah *firewall*, metode ini digunakan pada software maupun hardware untuk melindungi, menyaring bahkan menolak kegiatan pada jaringan yang berpotensi untuk merusak atau mendapatkan informasi pribadi melalui software/hardware tersebut. Cara kerja *firewall* ini cukup sederhana, bila ada *traffic* data masuk ke suatu jaringan *firewall* memeriksa *traffic* tersebut kemudian meneruskannya ke tujuan [2]. Kemudian terdapat teknik

https://doi.org/10.30743/infotekjar.v5i2.3501

pengamanan sederhana dalam lingkup lokal dengan menggunakan *port security*. Teknik *port security* merupakan teknik yang membatasi penggunaaan akses jaringan melalui *port* pada *switch* oleh perangkat yang MAC address-nya sudah terdaftar. Perangkat computer MAC address-nya belum terdaftar tidak memiliki hak untuk mengakses *port* tersebut. *Port* sendiri merupakan bagian yang dapat dikatakan sebagai pintu keluar-masuknya data pada komputer [3].

LANDASAN TEORI

A. Jaringan Komputer

Seperti yang sudah disinggung di atas, jaringan komputer adalah interkoneksi antar banyak komputer autonomous yang terhubung baik menggunakan media kabel maupun nirkabel yang tersambung bersama-sama. Autonomous sendiri diartikan jika sebuah komputer tidak dapat mengatur komputer lain secara penuh melalui koneksi hingga komputer lain dapat mati, menghidupkan ulang, hingga mengakses file dan merusak sistem. Jadi dalam sebuah jaringan tersebut setiap komputer berlaku independen terhadap memanajemen filenya sendiri, contohnya adalah internet. Internet memungkinkan suatu komputer mengirim/menerima data, tetapi tidak dapat mengontrol komputer lain secara penuh [4].

Pada jaringan komputer terdapat istilah *client*-server, yaitu merupakan desain jaringan yang digunakan pada hampir semua pengaplikasian jaringan komputer di dunia. *Client* adalah pihak yang meminta atau menerima *service*, sedangkan yang memberikan atau mengirim *service* disebut *server* [5].

B. Internet

Internet merupakan akronim dari interconnection network yang berarti berbagai komputer yang terhubung dengan bermacam-macam tipe jaringan dengan cakupan ruang seluruh dunia. Dengan internet semua orang di seluruh penjuru dunia bisa mendapatkan informasi yang sama dalam waktu yang bersamaan pula. Namun terkadang banyak orang menjadikan kesempatan untuk menyebar informasi yang salah (*hoax*) yang bisa berdampak buruk pada suatu individu maupun organisasi.

Dalam pengaturan integrasi serta komunikasi antar jaringan komputer dibutuhkan protokol. Protokol ini biasanya disebut *TCP/IP*. Untuk memastikan semua koneksi jaringan bekerja dengan benar digunakanlah *TCP* (*Transmission Control Protocol*), sedangkan *IP* (*Internet Protocol*) berfungsi untuk mentransmisikan data antar komputer. Keduanya secara umum bekerja dengan cara memilih rute terbaik dalam pengiriman data dan memilih rute alternatif bila rute yang sebelumnya tidak dapat melakukan pengiriman data [6].

C. Switch

Dalam implementasi jaringan komputer, terdapat perangkat keras khusus yang berfungsi untuk menghubungkan sumber jaringan ke beberapa komputer sekaligus, alat itu adalah *switch*. Terdapat dua jenis *switch*, yaitu:

1. Switch Unmanageable: Switch ini berfungsi untuk mendistrubusikan paket data antar komputer yang tersambung pada satu jaringan yang sama, *switch* ini juga mampu mengenali topologi jaringan pada banyak layer yang membuat data lebih cepat terdistribusi dan langsung tiba ke tujuan. *Switch* jenis ini bekerja secara plug and play, artinya switch otomatis bekerja ketika tersambung dengan sumber daya dan perangkat jaringan lainnya. *Switch* jenis ini tidak dapat melakukan pengaturan konfigurasi, artinya hanya dapat bekerja dengan menggunakan setelan pabrik. Contoh *switch unmanageable* dapat dilihat pada Gambar 1. [7]

Gambar 1. *Switch unmanageable*

2. *Switch manageable: switch* jenis ini kurang lebih memiliki fungsi yang sama dengan *switch unmanageable* namun memiliki fitur tambahan dan sudah dapat dilakukan pengaturan konfigurasi pada pemakaiannya. Contoh fitur yang terdapat pada *switch* ini diantaranya *Quality of Service*, yaitu pengaturan bandwidth untuk memprioritaskan data yang dikirim lebih dulu. Kemudian terdapat fitur monitoring kinerja jaringan bernama *Simple Network Management Protocol* (SNMP). Ada pula fitur yang paling banyak digunakan yaitu *Virtual Local Access Network* (VLAN). Kemudian *switch* jenis inilah yang dapat menambah tingkat keamanan dengan melakukan konfigurasi keamanan jaringan *port security*, dengan memeriksa hak akses setiap perangkat jaringan yang tersambung. Contoh *switch manageable* dapat dilihat pada Gambar 2.[8]

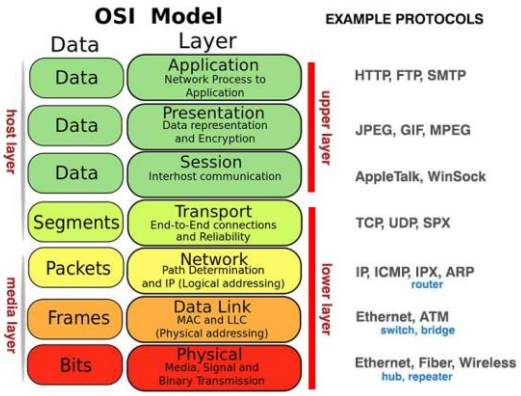
Gambar 2. *Switch manageable*

D. OSI Layer

Open System Interconnection (OSI) merupakan standard yang ditetapkan menjadi model komunikasi pada jaringan komputer. Model komunikasi ini dipakai oleh perangkat komunikasi di seluruh dunia, hal tersebut menyebabkan semua perangkat dari berbagai macam system operasi dan pabrikan dapat berkomunikasi melalui jaringan. OSI *layer* dibagi menjadi tujuh lapisan dan dikelompokkan menjadi dua grup, yaitu *upper* dan *lower layer* [9]. Ketujuh *layer* dalam model komunikasi OSI layer, yaitu:

- *Physical layer*
- *Data-link layer*
- *Network layer*
- *Transport layer*
- *Session layer*
- *Presentation layer*
- *Application layer*

Untuk memperjelas tentang model OSI layer ini dapat dilihat pada Gambar 3.



Gambar 3. *Model OSI layer*

E. Keamanan Jaringan

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.

Keamanan jaringan melindungi dari tepi jaringan dan juga dalam jaringan, dengan pendekatan berlapis. Kerentanan ada di mana-mana, dari perangkat dan jalur data hingga aplikasi dan pengguna. Setiap organisasi, bisnis kecil hingga perusahaan dan penyedia layanan terbesar, memerlukan keamanan jaringan untuk melindungi aset dan infrastruktur penting dari serangan yang berkembang pesat.

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. [10]

Pada jaringan komputer, metode penyerangan yang paling banyak dipakai adalah *Port Scanning* dan DoS (Denial of Service). Bila menggunakan *port scanning*, pihak penyerang mencari 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. [11].

F. Solusi Keamanan

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 perangkay yang dapat tersambung dengan jaringan terebut. Terdapat tiga jenis *switch port security*, yaitu:

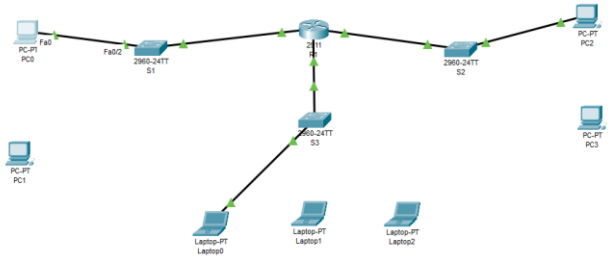
- *Default/static port security*
- *Dynamic Port security*
- *Sticky port security*

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.

HASIL DAN PEMBAHASAN

A. Desain Simulasi



Gambar 4. *Topologi yang digunakan*

TABEL I ADDRESSING

Device	Interface	IP address	Subnet mask	Default gateway
R1	gigabitEthernet 0/0	192.168.1.1	255.255.255.0	N/A
	gigabitEthernet 0/1	192.168.2.1	255.255.255.0	N/A
	gigabitEthernet 0/3	192.168.3.1	255.255.255.0	N/A
PC0	FastEthernet 0/0	192.168.1.10	255.255.255.0	192.168.1.1
PC1	FastEthernet 0/0	192.168.1.11	255.255.255.0	192.168.1.1
PC2	FastEthernet 0/0	192.168.2.10	255.255.255.0	192.168.2.1
PC3	FastEthernet 0/0	192.168.2.11	255.255.255.0	192.168.2.1
Laptop0	FastEthernet 0/0	192.168.3.10	255.255.255.0	192.168.3.1
Laptop1	FastEthernet 0/0	192.168.3.11	255.255.255.0	192.168.3.1

B. Pelaksanaan Simulasi

1. Sticky port security: Konfigurasi switch port S1 untuk dijadikan sticky port security dimana switch mengambil MAC address pada PC0 secara otomatis. Sebelumnya matikan dulu port-port fastEthernet dan gigabitEthernet yang tidak dipakai pada switch S1 dengan perintah:

```
S1(config)#int range f 0/3-24, g0/1-2
S1(config-if-range)#shutdown
```


https://doi.org/10.30743/infotekjar.v5i2.3501

Hasilnya *port* Fa0/3-24 dan g0/1-2 berstatus down atau nonaktif. Kemudian karena defaultnya *port security* pada *switch* belum aktif kita perlu mengaktifkannya dengan perintah:

```
S1(config)#int f 0/2
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
```

Setelah itu *port security* pada *switch* akan aktif tapi masih static. Untuk membuatnya menjadi *sticky port security* perlu ditambahkan perintah berikut

```
S1(config)#int f 0/2
S1(config-if)#switchport port-security
mac-address sticky
```

Untuk *setting* MAC address dari PC0 secara otomatis lakukan ping menggunakan PC0 ke IP address PC2 atau R1, nantinya MAC address akan terdaftar secara otomatis.

2. *Static Port Security:* Konfigurasi pada *switch* S2 untuk dijadikan static *port security*. Pertama nonaktifkan dulu *port* interface yang tidak terpakai seperti pada *switch* S1. Kemudian aktifkan *port security* seperti pada S1

```
S2(config)#int f 0/2
S2(config-if)#switchport mode access
S2(config-if)#switchport port-security
```

Setelah itu lakukan pendaftaran MAC address secara manual, sebelumnya cek MAC address pada PC2 menggunakan perintah ipconfig /all pada command prompt PC2, copy kemudian paste-kan pada konfigurasi *switch* S2 seperti berikut

```
S2(config)#int f 0/2
S2(config-if)#switchport port-security
mac-address (MAC address)
```

Untuk memastikan apakah sudah aktif lakukan ping dari PC2 ke alamat IP host lain. *Port* Fa0/2 sudah mengaktifkan *port-security* dengan MAC address dari PC2 sehingga tidak bisa dipakai oleh host lain. Sebagai pembeda berikan violation mode yang berbeda pada *switch* S2 dengan perintah sebagai berikut

```
S2(config)#int f 0/2
S2(config-if)#switchport port-security
violation restrict
```

Hal ini akan memberikan perbedaan karena default dari *port security* adalah shutdown mode

3. *Dynamic Port:* Konfigurasi pada *switch* S3 kali ini dibedakan dengan maksimum jumlah MAC address yang didaftarkan pada *port* dan. Pertama lakukan shutdown untuk *port-port* yang tidak diperlukan sama seperti *switch* S1 dan S2. Setelah itu aktifkan *port security* pada *port* Fa0/2 dan set menjadi *sticky port security*.

```
S3(config)#int f 0/2
S3(config-if)#switchport mode access
S3(config-if)#switchport port-security
S3(config-if)#switchport port-security
mac-address sticky
```

Kemudian ubah maksimum MAC address agar *port* bisa digunakan lebih dari satu host. Selanjutnya ubah *mode violation*nya menjadi *protection* dengan perintah berikut

```
S3(config)#int f 0/2
S3(config-if)#switchport port-security
maximum 2
S3(config-if)#switchport port-security
violation protection
```

Untuk mendaftarkan MAC address lakukan ping menggunakan Laptop0 dan Laptop1. Hasilnya MAC address dari masing-masing laptop akan terdaftar secara otomatis.

C. *Hasil*

1. *Switch S1*

```
S1#show port int f 0/2
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   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 00E0.A3D1.1222:1
Security Violation Count   : 0
```

Gambar 5. *Status switch S1*

Pada Gambar 5, *port security* pada *switch* S1 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 S1 dihubungkan pada PC1 kemudian dilakukan ping, secara otomatis koneksi akan terputus, dapat dilihat pada Gambar 6.

```
C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

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

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Gambar 6. *Ping S1 dengan PC1*

```
S1#show port int f 0/2
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.BE64.AD05:1
Security Violation Count   : 1
```

Gambar 7. *Status S1 setelah dilakukan ping dengan MAC berbeda*

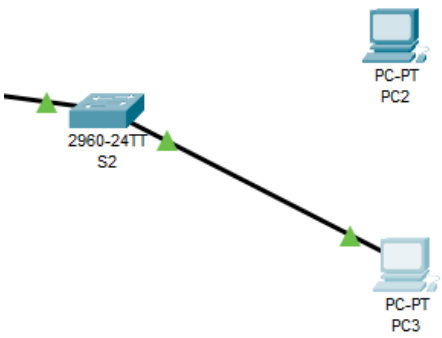
Dapat dilihat pada Gambar 7, status dari *port*nya *secure shutdown* yang berarti sudah tidak aktif secara otomatis dan *violation count*nya bertambah.

2. Switch S2

```
S2#show port int f 0/2
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   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 00D0.BA79.BBB8:1
Security Violation Count   : 0
```

Gambar 8. *Status S2*

Terlihat pada Gambar 8, *port security* pada *port* Fa0/2 di *switch* S2 aktif dengan maksimum MAC address yang sudah terpenuhi dan *violation mode*nya adalah *restrict*. Mode ini berbeda dengan *mode shutdown* karena pada saat *port* Fa0/2 digunakan oleh *host* dengan MAC address berbeda tidak akan terputus sambungannya namun data tetap didrop dan dilakukan penghitungan *violation count* yang terjadi.



Gambar 9. *Memindahkan koneksi switch S2*

Contoh pada Gambar 9, jika PC3 melakukan ping maka akan terjadi *request timed out* dan *violation count*nya bertambah seperti terlihat pada Gambar 10 dan 11.

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

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

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Gambar 10. *ping dari PC3*

```
S2#show port int f 0/2
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   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0001.63E6.EA72:1
Security Violation Count   : 4
```

Gambar 11. *status akhir switch S2*

1) Switch S3

```
S3#show port int f 0/2
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Protect
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 2
Last Source Address:Vlan   : 00D0.BAAA.5EC1:1
Security Violation Count   : 0
```

Gambar 12. *status switch S3*

Pada Gambar 12 dapat dilihat *switch* S3 mempunyai dua MAC address yang sudah terdaftar dengan metode sticky dan juga *violation mode protect* yang telah aktif. Mode ini akan membuang data yang dikirimkan dari host yang tidak terdaftar. Contoh jika *switch* S3 dihubungkan dengan Laptop2 dan melakukan ping maka outputnya adalah *request timed out* tapi koneksi tidak terputus dapat dilihat pada Gambar 13 dan 14.

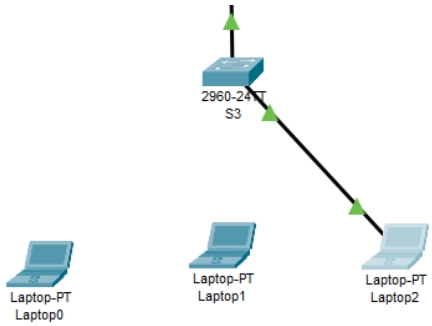
```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

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

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Gambar 13. *ping dari Laptop2*



Gambar 14. *koneksi yang tidak terputus walaupun pada Laptop2*

Pada mode *protect* tidak terjadi penambahan *violation count* walaupun dilakukan *ping* dari MAC address yang tidak terdaftar, lebih lengkapnya dapat dilihat pada Gambar 15.

```
S3#show port int f 0/2
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Protect
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 2
Last Source Address:Vlan   : 0060.3E7A.B5A2:1
Security Violation Count   : 0
```

Gambar 15. *status akhir switch S2*

https://doi.org/10.30743/infotekjar.v5i2.3501

D. Pembahasan

Pada *switch* S1 dilakukan konfigurasi *sticky port security* sehingga MAC address akan terdaftar secara otomatis setelah dilakukan *ping*, pada kasus ini menggunakan address PC0. Pada *switch* ini menggunakan *violation mode shutdown* sehingga jika ada MAC address yang tidak dikenal mengirimkan data outputnya akan *request timed out* dan otomatis koneksi antara *switch* dan host akan terputus dan jika ingin menyambungkan kembali dengan PC0 *port* harus direstart dengan cara manual (*shutdown-no shutdown* pada konfigurasi *switch*).

Switch S2 konfigurasi MAC addressnya secara manual dan menggunakan violation mode restrict. Pada *switch* ini MAC address dari PC2 langsung terdaftar tapi tidak dihitung sebagai sticky MAC address. Kemudian violation mode restrict mengakibatkan violation count bertambah sejumlah dengan pengiriman data yang dilakukan, dalam hal ini PC3 melakukan ping satu kali menghasilkan 4 kali *request timed out* sehingga violation count yang terhitung sebanyak 4 kali, namun pada mode ini tidak terjadi pemutusan koneksi secara otomatis.

Selanjutnya *switch* S3 melakukan konfigurasi *sticky port security* juga dengan jumlah maksimum MAC address sebanyak dua alamat dan violation mode protect. Seperti pada *switch* S1, MAC address akan terdaftar secara otomatis setelah dilakukan ping, dalam kasus ini adalah Laptop0 dan Laptop1. Pada saat *switch* dihubungkan dengan Laptop2 dan melakukan ping outputnya adalah *request timed out*, tetapi karena menggunakan mode protection violation countnya tidak dihitung sehingga tetap nol tapi tetap tidak bisa mengakses atau mengirim paket data.

PENUTUP

Berdasarkan hasil simulasi 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. 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.

REFERENCES

[1] D. Alfurqon, "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, 2018, [Online]. Available: www.ucokhamongan.com.

[2] S. A. Pamuji, C. Iswahyudi, and T. Informatika, "Jurnal JARKOM Vol . 5 No . 1 Desember 2017 ISSN : 2338-6304 Jurnal JARKOM Vol . 5 No . 1 Desember 2017 ISSN : 2338-6304," vol. 5, no. 1, pp. 65–75, 2017.

[3] R. O. Nitra and M. Ryansyah, "Implementasi Sistem Keamanan Jaringan Menggunakan Firewall Security Port pada Vitaa Multi Oxygen," *J. Sist. dan Teknol. Inf.*, vol. 7, no. 1, p. 52, 2019, doi: 10.26418/justin.v7i1.29979.

[4] D. Irawan, "Keamanan jaringan komputer dengan metode blocking port pada laboratorium komputer program diploma-iii sistem informasi universitas muhammadiyah metro," *Manaj. Inform. Progr. Diploma III UM Metro*, vol. 02, no. 05, pp. 1–9, 2015.

[5] M. J. N. Yudianto, "Jaringan Komputer dan Pengertiannya," *Ilmukomputer.Com*, vol. Vol.1, pp. 1–10, 2014.

[6] Ertie Nur Hartiwati, "Keamanan Jaringan Dan Keamanan Sistem Komputer Yang Mempengaruhi Kualitas Pelayanan Warnet," *J. Ilm. Inform. Komput. Univ. Gunadarma*, pp. 27–33, 2014.

[7] O. K. Sulaiman, "Analisis Sistem Keamanan Jaringan dengan Menggunakan Switch Port Security," *CESS (Journal Comput. Eng. Syst. Sci.*, vol. 1, no. 1, pp. 9–14, 2016, [Online]. Available: http://jurnal.unimed.ac.id/2012/index.php/cess/article/view/4036/3590.

[8] S. Sudaryanto, "Implementation Port Security for Security Systems Network at the Computing Laboratory of Adisutjipto College of Technology," *Conf. Senat. STT Adisutjipto Yogyakarta*, vol. 4, 2018, doi: 10.28989/senatik.v4i0.239.

[9] Hardiana, "Jurnal Ilmiah d ' ComPutarE Volume 5 Edisi Juni Fakultas Teknik Komputer Universitas Cokroaminoto Palopo | 18 Jurnal Ilmiah d ' ComPutarE Volume 5 Edisi Juni Fakultas Teknik Komputer Universitas Cokroaminoto Palopo | 19," vol. 5, pp. 18–24, 2015.

[10] Sugiyono, "Sistem keamanan jaringan komputer menggunakan metode watchguard firebox pada pt guna karya indonesia," *J. CKI*, vol. 9, no. 1, pp. 1–8, 2016.

[11] I. Anugrah and R. H. Rahmanto, "Sistem Keamanan Jaringan Local Area Network Menggunakan Teknik De-Militarized Zone," *PIKSEL Penelit. Ilmu Komput. Sist. Embed. Log.*, vol. 5, no. 2, pp. 91–106, 2018, doi: 10.33558/piksel.v5i2.271.