Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id

E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 5 No. 3 (2024) | September
OPEN ACCESS

https://doi.org/10.35870/jimik.v5i3.975

Analisis Efektivitas Keamanan Jaringan *Layer 2*: *Port Security*, *VLAN Hopping*, *DHCP Snooping*

Muhammad Dzaky Nurfaishal [1*], Yuma Akbar [2]

[1*,2] Program Studi Teknik Informatika, Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika, Kota Jakarta Timur, Daerah Khusus Ibukota Jakarta, Indonesia.

Email: dzaky5201@gmail.com [1*], yuma.pjj@gmail.com [2]

Histori Artikel:
Dikirim 21 Juli 2024; *Diterima dalam bentuk revisi* 13 Agustus 2024; *Diterima* 30 Agustus 2024; *Diterbitkan* 30 September 2024.

Abstrak

Dalam era industri 4.0 yang ditandai oleh kemajuan jaringan komputer dan internet yang pesat, keamanan jaringan pada Layer 2, yang merupakan bagian dari Data Link Layer dalam model OSI, sangat penting mengingat meningkatnya ancaman siber. Penelitian ini bertujuan untuk membandingkan efektivitas berbagai algoritma keamanan yang diterapkan pada Layer 2 switch, yaitu MAC Address Filter, Port Security, VLAN Hopping Mitigation, dan DHCP Snooping. Beberapa metode tersebut memiliki fungsi atau tujuan seperti MAC address filtering, limitasi port, penjagaan VLAN, ARP, dan lain-lain. Perangkat yang digunakan dalam penelitian ini adalah Cisco Switch. Penelitian ini menggunakan pendekatan eksperimental dengan mengimplementasikan setiap metode pada skenario jaringan yang berbeda, serta membandingkan dengan data eksternal. Pengukuran efektivitas dilakukan berdasarkan deteksi dan pencegahan serangan, serta dampaknya terhadap kinerja jaringan, yang kemudian menggabungkan beberapa metode tersebut ke dalam satu kesatuan. Hasil menunjukkan bahwa setiap metode memiliki kelebihan dan kekurangan masing-masing, yang berfungsi untuk memblokir berbagai macam serangan seperti flooding, snooping, dan DHCP Rogue. Sangat disarankan untuk menyatukan semua metode pengamanan menjadi satu sistem terpadu.

Kata Kunci: Layer 2; Port Security; DHCP Snooping; Network Security.

Abstract

In the industrial era 4.0, which is marked by the rapid progress of computer networks and the internet, network security at Layer 2 is part of the Data Link Layer in the OSI model, which is very important considering the increasing number of cyber threats. This research aims to compare the effectiveness of various security algorithms applied to Layer 2 switches, namely MAC Address Filtering with Port Security, VLAN Hopping Mitigation, and DHCP Snooping. Some of these methods have the function or purpose of creating MAC address filtering, port limitations, VLAN protection, ARP, etc. The device used to conduct this research is a Cisco Switch. This research uses an experimental approach by implementing each method in different network scenarios and comparing it with external data, measuring effectiveness based on attack detection and prevention, as well as its impact on network performance, then combining several of these methods into one scope. The results show that each method has its own advantages and disadvantages, which function to block various types of attacks such as Flooding, Snooping, and Rogue DHCP. It is highly recommended to combine all security methods into one integrated system.

Keyword: Layer 2; Port Security; DHCP Snooping; Network Security.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 5 No. 3 (2024) | September
OPEN ACCESS
https://doi.org/10.35870/jimik.v5i3.975

1. Pendahuluan

Keamanan jaringan merupakan salah satu aspek yang sangat krusial dalam pengelolaan infrastruktur teknologi informasi. Dalam era digital yang semakin maju, ancaman siber berkembang dengan cepat dan menjadi semakin kompleks. Jaringan komputer, terutama pada *Layer 2* yang beroperasi di *Data Link Layer* dalam model OSI, sering kali menjadi target serangan yang dapat mengakibatkan kerugian besar bagi organisasi. *Layer 2 switch*, yang mengatur lalu lintas data antar perangkat dalam jaringan lokal, menjadi titik kritis dalam menjaga keamanan dan integritas data.

Port Security berfungsi untuk membatasi akses berdasarkan alamat *MAC* tertentu, *VLAN Hopping Mitigation* mencegah akses tidak sah antar *VLAN*, sementara *DHCP Snooping* memastikan tidak munculnya *DHCP server* palsu yang dapat mengganggu konektivitas pengguna dan mencegah serangan *phishing* atau pencurian data. Di samping itu, *Dynamic ARP Inspection* memverifikasi keabsahan pesan *ARP*. Namun, efektivitas dari setiap metode ini dapat bervariasi tergantung pada situasi dan konfigurasi jaringan yang digunakan.

Terdapat beberapa penelitian terdahulu yang relevan dengan topik keamanan jaringan *Layer 2 switch* menggunakan berbagai metode. Andi Purnomo (2024) telah menerapkan *DHCP Snooping* dengan tujuan meningkatkan standar keamanan. Brian Rinanto Saputra dan Dian Widiyanto Chandra (2022) melakukan konfigurasi *DHCP Snooping* yang terintegrasi dengan *VLAN*. Sebagai perbandingan, Dio Aditya Pradana dan Ade Surya Budiman (2020) menganalisis dan mengonfigurasi *DHCP Snooping* bersama dengan metode peringatan (*alert*). Penelitian yang dilakukan oleh Hannah A. S. Adjei *et al.* (2022) mengimplementasikan *DHCP Snooping* dengan teknik *SSL Stripping* untuk inspeksi *ARP* dan *DHCP*. Andy Satria dan Fanny Ramadhani (2023) mengonfigurasi *Port Security* untuk pengamanan jaringan pada *Cisco Packet Tracer*. Firmansyah *et al.* (2022) menggabungkan dua metode, yaitu *dynamic sticky* dan *static MAC address* dalam implementasi *Port Security*.

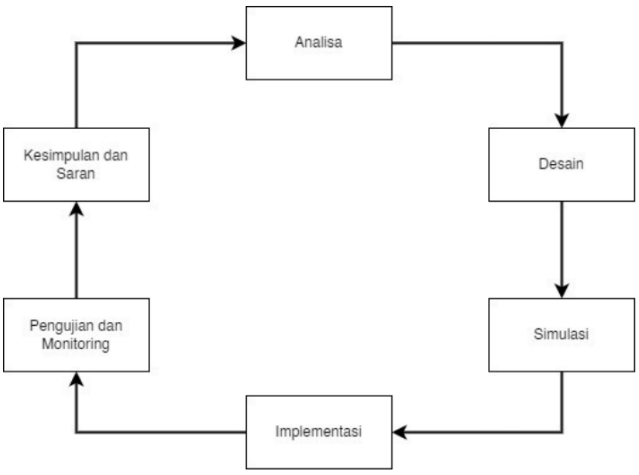
Selain penelitian yang secara langsung membahas metode keamanan, beberapa penelitian lain juga relevan. Hiba Imad Nasser dan Mohammed Abdulridha Hussain (2022) menyoroti ancaman yang berasal dari serangan *man in the middle* (MITM). Wahyu Saputra (2017) membahas implementasi mitigasi *VLAN Hopping* dan pengujian protokol *Spanning Tree*. Penelitian yang dilakukan oleh Yoga Bayu Setiawan *et al.* (2022) mengeksplorasi integrasi *Port Security* dengan protokol *OSPF*.

Penelitian sebelumnya mengenai penerapan metode keamanan pada *Layer 2 switch* dan kinerja jaringan memberikan landasan yang kuat untuk mengeksplorasi efektivitas berbagai metode. Sejumlah penelitian telah menguji berbagai konfigurasi dan integrasi metode yang berbeda, yang menjadi referensi penting dalam upaya meningkatkan keamanan jaringan *Layer 2* dalam model OSI. Dengan menggabungkan temuan dari penelitian-penelitian tersebut, penelitian ini dapat mengidentifikasi strategi yang tepat dan langkah-langkah konkret untuk melakukan analisis yang lebih rinci terkait setiap metode, baik dari aspek positif maupun negatif. Selain itu, penelitian ini bertujuan untuk meningkatkan keamanan jaringan dengan menerapkan metode yang sesuai dengan kebutuhan dan kondisi jaringan, serta mengoptimalkan aspek keamanan. Hal ini akan membantu organisasi atau individu mencapai jaringan *LAN* yang lebih aman, efisien, dan andal.

2. Metode Penelitian

Penelitian ini menggunakan metode NDLC (*Network Development Life Cycle*). Metode NDLC mencakup beberapa aspek yang meliputi perancangan, penerapan, dan pengelolaan jaringan komputer. Berikut ini adalah penjelasan dari masing-masing tahapannya.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 5 No. 3 (2024) | September
OPEN ACCESS
https://doi.org/10.35870/jimik.v5i3.975



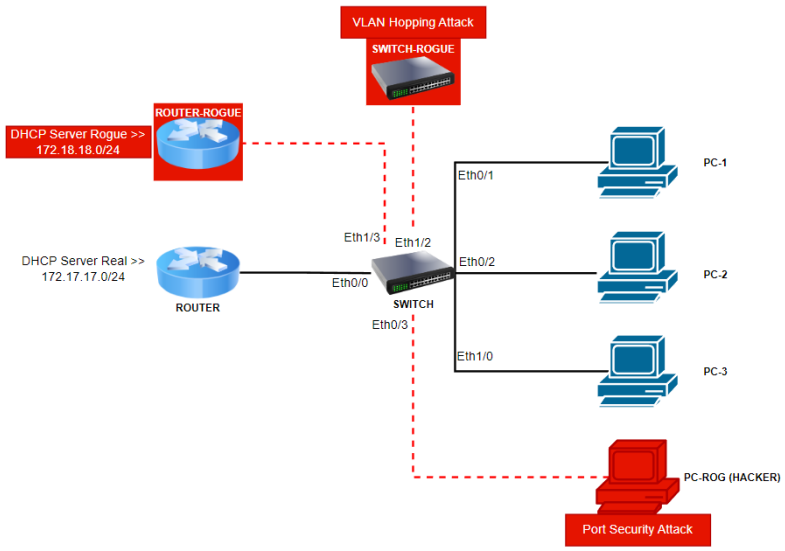
Gambar 1. Model Proses Penelitian

1) Analisa
Tahap ini dimulai dengan melakukan analisa permasalahan yang muncul yaitu bagaimana cara mengetahui efektivitas dari setiap metode yang akan digunakan pada penelitian kali yang bertujuan untuk melakukan pengamanan jaringan Layer 2 Switch.
2) Desain
Pada tahap ini, peneliti akan merancang topologi jaringan berdasarkan data yang telah dikumpulkan sebelumnya. Desain ini akan memberikan gambaran lengkap tentang kebutuhan jaringan.
3) Simulasi
Pada tahap simulasi, peneliti menggunakan EVE-NG untuk meniru kondisi operasional sebenarnya dari jaringan yang dirancang. Simulasi ini bertujuan untuk memeriksa kinerja, mengidentifikasi potensi masalah, dan melakukan penyesuaian jika diperlukan sebelum implementasi nyata, guna mengurangi risiko kegagalan dan memastikan desain jaringan memenuhi kebutuhan dan spesifikasi yang ditetapkan.
4) Implementasi
Pada tahap ini, peneliti melaksanakan implementasi sesuai dengan analisis kebutuhan dan perancangan yang telah dibuat, serta melakukan pengujian unit sistem untuk membandingkan efektivitas berbagai metode pengamanan jaringan Layer 2.
5) Pengujian dan Monitoring
Setelah implementasi selesai, peneliti melakukan pengujian untuk membuktikan hasil dari implementasi yang telah dibangun. Monitoring dilakukan untuk memastikan kinerja jaringan tetap optimal dan mengidentifikasi serta mengatasi masalah yang mungkin terjadi.
6) Kesimpulan dan saran
Pada tahap terakhir, peneliti mengevaluasi hasil yang didapatkan dari tahap sebelumnya dan membandingkan hasil tersebut dengan dataset publik. Kesimpulan akan berisi temuan penelitian, dan saran-saran diberikan berdasarkan temuan tersebut.

2.1 Topologi Jaringan

Topologi yang akan dibangun menggunakan lingkungan *virtual* EVE-NG, terdiri dari beberapa perangkat jaringan, di mana setiap perangkat memiliki peranannya masing – masing, ada fungsi router yang digunakan sebagai gateway dhcp server, fungsi switch sebagai perangkat yang akan digunakan lebih banyak dalam penelitian ini, dan *Personal Computer (*PC) sebagai alat untuk melakukan pengetesan dari setiap mekanisme percobaan.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 5 No. 3 (2024) | September
OPEN ACCESS
https://doi.org/10.35870/jimik.v5i3.975



Gambar 2. Topologi Testing

2.2 Parameter Pengujian

Pada penelitian ini, parameter uji difokuskan pada tiga aspek, diantaranya:

1) Memastikan bahwa konfigurasi setiap metode pengamanan jaringan Layer 2 switch pada setiap perangkat jaringan telah dilakukan dengan benar dan melakukan testing sebelum dilakukan konfigurasi pengamanan Layer 2 switch.
2) Pengujian dengan menggunakan masing – masing metode yang memiliki tujuan sama dan melihat seberapa efektif setiap metodenya berjalan sesuai dengan cara kerjanya serta melakukan perbandingan baik dengan data *private* dan eksternal.
3) Pengujian dengan cara melakukan *mixing* metode pengamanan Layer 2 Switch yang bertujuan untuk mengetahui efektivitas perbandingannya dengan yang dilakukan pada skema 2 dan mengetahui seberapa fleksibel setiap metode tersebut agar jaringan yang berjalan saat ini tidak mengalami penurunan kinerja jaringan.

2.3 Alat Penelitian

Alat-alat yang akan digunakan untuk mendukung penelitian ini meliputi hardware berupa laptop atau komputer dan juga aplikasi pendukung seperti EVE-NG yang sudah terinstal didalamnya. Berikut merupakan detail alat yang akan digunakan dalam penelitian ini.

Tabel 1. Spesifikasi Hardware

No	Jenis Hardware	Spesifikasi
1	Personal Computer	PC Pribadi
2	CPU	Intel(R) Core(TM) i5-10400 CPU @ 2.90GHz(12 CPUs) 2.9 GHz
3	RAM	16GB
4	HDD	1000Gb

Tabel 2. Spesifikasi Software

No	Jenis Software	Spesifikasi
1	Windows 10 Enterprise	PC Pribadi
2	EVE-NG	Memory 8GB, vProcessor 4GB, vNetwork Adapter 2
3	VM	vRam 8GB
4	HDD	40Gb

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 5 No. 3 (2024) | September
OPEN ACCESS
https://doi.org/10.35870/jimik.v5i3.975

3. Hasil dan Pembahasan

3.1 Hasil

Setelah menyelesaikan tahap implementasi, langkah berikutnya adalah pengujian. Berikut ini adalah pengujian yang akan dilakukan dalam penelitian ini.

3.1.1 Pengujian konfigurasi semua perangkat telah sesuai

Pengujian ini bertujuan untuk memastikan seluruh konfigurasi terkait sudah sesuai dengan peruntukannya, serta menunjukan kondisi apabila konfigurasi Keamanan Layer 2 switch belum dilakukan.

```
PC-3> show ip

NAME          : PC-3[1]
IP/MASK       : 172.17.17.4/24
GATEWAY       : 172.17.17.254
DNS           : 8.8.8.8
DHCP SERVER   : 172.17.17.254
DHCP LEASE    : 86391, 86400/43200/75600
MAC           : 00:50:79:66:68:05
LPORT         : 20000
RHOST:PORT    : 127.0.0.1:30000
MTU           : 1500

PC-3>
```

```
PC-ROG> show ip

NAME          : PC-ROG[1]
IP/MASK       : 172.17.17.1/24
GATEWAY       : 172.17.17.254
DNS           : 8.8.8.8
DHCP SERVER   : 172.17.17.254
DHCP LEASE    : 86398, 86400/43200/75600
MAC           : 00:50:79:66:68:06
LPORT         : 20000
RHOST:PORT    : 127.0.0.1:30000
MTU           : 1500

PC-ROG>
```

Gambar 3. Kondisi PC Sebelum dilakukan konfigurasi *Port Security*

```
PC-1> show ip

NAME          : PC-1[1]
IP/MASK       : 172.17.17.1/24
GATEWAY       : 172.17.17.254
DNS           : 8.8.8.8
DHCP SERVER   : 172.17.17.254
```

```
PC-2> show ip

NAME          : PC-2[1]
IP/MASK       : 172.18.18.2/24
GATEWAY       : 172.18.18.254
DNS           : 1.1.1.1
DHCP SERVER   : 172.18.18.254
```

Gambar 4. Kondisi PC sebelum dilakukan konfigurasi DHCP *Snooping*

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

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0050.7966.6803    DYNAMIC     Et0/1
   1    0050.7966.6804    DYNAMIC     Et0/2
   1    0050.7966.6805    DYNAMIC     Et1/0
   1    5000.0001.0000    DYNAMIC     Et0/0
   1    5000.0008.0000    DYNAMIC     Et1/3
   1    aabb.cc80.7000    DYNAMIC     Et1/2
Total Mac Addresses for this criterion: 6
Switch#
```

```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/0, Et0/1, Et0/2, Et0/3
                                                Et1/0, Et1/1, Et1/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------

Switch#
```

Gambar 5. Kondisi *Mac address* dan *default* vlan yang terbaca sebelum dilakukan konfigurasi VLAN *Hopping Mitigation*

```
Switch#sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
none
DHCP snooping is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: aabb.cc00.2000 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                  Trusted    Allow option    Rate limit (pps)
-------------------------  -------    ------------    ----------------
Ethernet0/0                yes        yes             unlimited
  Custom circuit-ids:
Ethernet1/3                no         no              100
  Custom circuit-ids:
Switch#
```

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 5 No. 3 (2024) | September
OPEN ACCESS
https://doi.org/10.35870/jimik.v5i3.975

```
Switch#show inter trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       desirable        n-802.1q       trunking      1
Et1/2       desirable        n-isl          trunking      1

Port        Vlans allowed on trunk
Et0/0       1-4094
Et1/2       1-4094

Port        Vlans allowed and active in management domain
Et0/0       1
Et1/2       1

Port        Vlans in spanning tree forwarding state and not pruned
Et0/0       1
Et1/2       1
Switch#
```

Gambar 6. Kondisi pada Switch sebelum dilakukan konfigurasi Keamanan Layer 2 Switch

Dari hasil pengujian diatas dapat peneliti simpulkan apabila menggunakan konfigurasi default atau bawaan sangat tidak direkomendasikan karena akan menimbulkan celah penyerangan siber yang cukup besar dan akan menimbulkan efek buruk pada sebuah jaringan LAN, sebagai contoh di Gambar 3 memperlihatkan bahwa semua PC dapat terkoneksi secara langsung dengan switch apabila tidak dilakukan limitasi *port security*, Gambar 4 memperlihatkan Gambaran PC yang mengalami perbedaan DHCP *Lease* dimana biasanya dilakukan oleh orang yang tidak bertanggung jawab dengan tujuan meretas sebuah jaringan, Gambar 5 semua perangkat yang terkoneksi ke switch bisa terbaca dimana bisa menimbulkan celah yang sangat besar untuk hacker bisa melakukan akses ke jaringan internal.

3.1.2 Pengujian masing – masing metode

Pada pengujian kali ini, memiliki tujuan untuk memastikan setiap metode berjalan sesuai dengan peruntukan beserta dengan pengetesan setiap metode.

```
PC-3> show ip

NAME        : PC-3[1]
IP/MASK     : 172.17.17.4/24
GATEWAY     : 172.17.17.254
DNS         : 8.8.8.8
DHCP SERVER : 172.17.17.254
DHCP LEASE  : 86391, 86400/43200/75600
MAC         : 00:50:79:66:68:05
LPORT       : 20000
RHOST:PORT  : 127.0.0.1:30000
MTU         : 1500

PC-3>
```

```
Switch#show port-security interface ethernet 0/3
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   : 0050.7966.6805:1
Security Violation Count   : 0

Switch#
```

Gambar 7. Kondisi setelah dikonfigurasi port security pada port 0/3

```
Switch#
*Jul 14 08:31:39.826: %PM-4-ERR_DISABLE: psecure-violation error detected on Et0/3,
 putting Et0/3 in err-disable state
Switch#
*Jul 14 08:31:39.826: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurr
ed, caused by MAC address 0050.7966.6806 on port Ethernet0/3.
*Jul 14 08:31:40.826: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3,
changed state to down
Switch#
*Jul 14 08:31:41.827: %LINK-3-UPDOWN: Interface Ethernet0/3, changed state to down
Switch#
```

```
Switch#show port-security interface ethernet 0/3
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   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0050.7966.6806:1
Security Violation Count   : 1

Switch#
```

Gambar 8. Pengujian ganti kabel fisik ke PC *Rogue* untuk pengetesan *Port security*

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 5 No. 3 (2024) | September
OPEN ACCESS
https://doi.org/10.35870/jimik.v5i3.975

```
Switch#sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
none
DHCP snooping is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: aabb.cc00.2000 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                Trusted    Allow option    Rate limit (pps)
-----------------------  -------    ------------    ----------------
Ethernet0/0              yes        yes             unlimited
  Custom circuit-ids:
Ethernet1/3              no         no              100
  Custom circuit-ids:
Switch#
```

```
PC-1> show ip

NAME        : PC-1[1]
IP/MASK     : 172.17.17.1/24
GATEWAY     : 172.17.17.254
DNS         : 8.8.8.8
DHCP SERVER : 172.17.17.254
```

```
PC-2> show ip

NAME        : PC-2[1]
IP/MASK     : 172.17.17.5/24
GATEWAY     : 172.17.17.254
DNS         : 8.8.8.8
DHCP SERVER : 172.17.17.254
```

Gambar 9. Pengujian DHCP Snooping dari sisi switch dan PC

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

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    5000.0008.0000    DYNAMIC     Et1/3
 100    0050.7966.6803    DYNAMIC     Et0/1
 100    0050.7966.6804    DYNAMIC     Et0/2
 100    0050.7966.6805    DYNAMIC     Et1/0
 100    5000.0001.0000    DYNAMIC     Et0/0
Total Mac Addresses for this criterion: 5
Switch#
Switch#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Et0/0       100

Port        Vlans allowed and active in management domain
Et0/0       100

Port        Vlans in spanning tree forwarding state and not pruned
Et0/0       100
Switch#
```

Gambar 10. Pengujian Konfigurasi VLAN *Hopping Mitigation*

Dari hasil pengujian diatas dapat disimpulkan secara keseluruhan, pengujian implementasi VLAN, DHCP *Snooping*, dan segmentasi jaringan menunjukkan bahwa metode ini efektif untuk mengamankan jaringan. Setelah perpindahan port, DHCP *Snooping* berhasil mencegah perangkat yang tidak sah memperoleh IP, sementara VLAN memastikan lalu lintas data hanya melewati jalur yang telah ditentukan. Konfigurasi VLAN menunjukkan bahwa alamat MAC terbaca sesuai dengan segmentasi yang telah dibuat. Ini tidak hanya meningkatkan keamanan tetapi juga efisiensi dan stabilitas jaringan. Penggunaan DHCP *Snooping* pada interface yang tepat memastikan setiap PC mendapatkan alamat IP yang benar, menambah lapisan keamanan penting dalam manajemen jaringan.

3.1.3 Pengujian akhir semua metode menjadi satu

Pada pengujian kali ini, memiliki tujuan untuk memastikan setiap metode berjalan sesuai dengan peruntukan beserta dengan pengetesan setiap metode.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id

E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 5 No. 3 (2024) | September
OPEN ACCESS

https://doi.org/10.35870/jimik.v5i3.975

```
Switch#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)         (Count)
---------------------------------------------------------------------------
      Et0/1             1            1                  0         Shutdown
      Et0/2             1            1                  0         Shutdown
      Et1/0             1            1                  0         Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
Switch#
```

Gambar 11. Konfigurasi *Port Security*

```
Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
none
DHCP snooping is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: aabb.cc00.2000 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
Ethernet0/0                yes        yes             unlimited
  Custom circuit-ids:
Ethernet1/3                no         no              100
  Custom circuit-ids:
Switch#
```

Gambar 12. Konfigurasi DHCP *Snooping*

```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/3, Et1/1, Et1/2, Et1/3
100  TEST                             active    Et0/1, Et0/2, Et1/0
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
100  enet  100100     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------

Switch#
Switch#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Et0/0       100

Port        Vlans allowed and active in management domain
Et0/0       100

Port        Vlans in spanning tree forwarding state and not pruned
Et0/0       100
Switch#
```

Gambar 13. Konfigurasi VLAN *Hopping Mitigation*

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 5 No. 3 (2024) | September
OPEN ACCESS
https://doi.org/10.35870/jimik.v5i3.975


```
Switch(config)#ip dhcp snooping
Switch(config)#vlan 100
Switch(config-vlan)#name TEST
=======Konfigurasi kearah interface Router========
Switch(config)#interface Ethernet0/0
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 100
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#exit
=======Konfigurasi kearah interface PC-1========
Switch(config)#interface Ethernet0/1
Switch(config-if)#switchport access vlan 100
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#exit
Switch(config)#
=======Konfigurasi kearah interface PC-2========
Switch(config)#interface Ethernet0/2
Switch(config-if)#switchport access vlan 100
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#exit
Switch(config)#
=======Konfigurasi kearah interface PC-3========
Switch(config)#interface Ethernet1/0
Switch(config-if)#switchport access vlan 100
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#exit
Switch(config)#
```

Gambar 14. Rekap Konfigurasi semua metode

Dari gambar diatas dapat diambil Kesimpulan bahwa semua metode dapat dilakukan konfigurasi secara bersamaan dalam satu waktu yang sama dengan memiliki tujuannya masing – masing, beserta rangkuman dari konfigurasi yang telah dilakukan ada di gambar 14 dengan ditandai list berwarna. Dari hasil pengujian yang telah dilakukan, dapat disimpulkan bahwa semua metode keamanan, yakni *Port Security*, *DHCP Snooping*, dan *VLAN Hopping Mitigation*, dapat diterapkan secara bersamaan tanpa menyebabkan konflik atau gangguan pada kinerja jaringan. Masing-masing metode berfungsi sesuai dengan peranannya dalam menjaga keamanan jaringan, dan implementasi terpadu ini menunjukkan bahwa metode-metode tersebut dapat bekerja dengan sinergis untuk memberikan perlindungan menyeluruh pada jaringan *Layer 2*.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 5 No. 3 (2024) | September
OPEN ACCESS
https://doi.org/10.35870/jimik.v5i3.975

3.2 Pembahasan

Hasil penelitian ini menunjukkan bahwa penggabungan metode keamanan *Layer 2* pada jaringan, seperti *Port Security*, *DHCP Snooping*, dan *VLAN Hopping Mitigation*, mampu memberikan perlindungan yang lebih efektif terhadap serangan siber yang sering terjadi pada jaringan lokal. Hal ini sejalan dengan penelitian sebelumnya yang juga mengevaluasi efektivitas metode ini, namun dengan fokus yang berbeda. Andi Purnomo (2024) dan Brian Rinanto Saputra serta Dian Widiyanto Chandra (2022) menyoroti efektivitas *DHCP Snooping* dalam mencegah distribusi alamat IP yang tidak sah dan melindungi jaringan dari serangan *rogue DHCP*. Penelitian ini memperluas penerapan *DHCP Snooping* dengan mengintegrasikannya bersama *Port Security* dan *VLAN Hopping Mitigation* untuk memberikan perlindungan yang lebih solid terhadap serangan yang berupaya memanipulasi distribusi alamat IP dan mengakses segmen VLAN tanpa izin.

Selain itu, penelitian oleh Dio Aditya Pradana dan Ade Surya Budiman (2020) mengenai *DHCP Snooping* dan peringatan (*alert*) serta Firmansyah *et al.* (2022) terkait *Port Security* pada *Layer 2* menunjukkan bahwa metode ini sangat efektif dalam mencegah akses perangkat yang tidak sah ke jaringan. Studi-studi tersebut mengindikasikan pentingnya implementasi kontrol akses perangkat untuk menjaga stabilitas dan keamanan jaringan. Hasil penelitian ini menunjukkan bahwa kombinasi kedua metode tersebut tidak hanya mampu mencegah perangkat tidak sah, tetapi juga memberikan lapisan keamanan tambahan ketika diterapkan bersama segmentasi jaringan melalui *VLAN Hopping Mitigation*, sebagaimana yang disarankan oleh Wahyu Saputra (2017).

Lebih lanjut, penelitian yang dilakukan oleh Hannah A. S. Adjei *et al.* (2022) dan Hiba Imad Nasser serta Mohammed Abdulridha Hussain (2022) terkait inspeksi *DHCP* dan *ARP* dalam menghadapi serangan *man-in-the-middle* dan *ARP spoofing* memperkuat gagasan bahwa penggabungan beberapa metode keamanan dalam jaringan *Layer 2* memberikan perlindungan yang lebih kuat terhadap serangan siber. Penelitian kami mendukung temuan ini dengan menunjukkan bahwa ketika *DHCP Snooping* dipadukan dengan *Port Security* dan mitigasi *VLAN Hopping*, perlindungan terhadap serangan yang mengeksploitasi kelemahan dalam distribusi IP dan segmentasi jaringan menjadi lebih efektif.

Studi lain seperti yang dilakukan oleh Andy Satria dan Fanny Ramadhani (2023) dan Ni Komang Ayu Sri Anggreni serta Lie Jasa (2022) terkait *Port Security* dan protokol keamanan lainnya juga menunjukkan bahwa kontrol akses perangkat memainkan peran penting dalam mencegah penyusupan. Namun, penelitian kami menemukan bahwa ketika metode ini diterapkan secara bersamaan dengan metode lain seperti *DHCP Snooping*, perlindungan terhadap jaringan tidak hanya terbatas pada kontrol fisik akses perangkat, tetapi juga meliputi pencegahan manipulasi alokasi IP dan isolasi segmen VLAN yang lebih baik. Dengan demikian, penelitian ini menegaskan pentingnya penggunaan beberapa metode keamanan secara terpadu, sebagaimana juga ditunjukkan oleh penelitian dari Shahid Mahmood *et al.* (2020) yang menyebutkan bahwa *Layer 2* sering kali menjadi target serangan karena kelemahan dalam kontrol keamanannya.

Penelitian sebelumnya dari Firmansyah *et al.* (2022) dan Oris Krianto Sulaiman (2016) juga menunjukkan bahwa *Port Security* dapat membatasi akses perangkat yang tidak diizinkan melalui *MAC address*, namun penelitian kami memperlihatkan bahwa ketika metode ini dipadukan dengan *DHCP Snooping* dan *VLAN Hopping Mitigation*, efektivitas dalam mencegah serangan berbasis perangkat dan manipulasi jaringan meningkat. Integrasi metode tersebut menciptakan lingkungan jaringan yang lebih terlindungi dari berbagai jenis ancaman siber, termasuk serangan *VLAN hopping* dan *MAC spoofing*, yang sering kali menjadi kelemahan pada jaringan *Layer 2*.

Penelitian ini memperkuat pentingnya integrasi berbagai metode keamanan pada jaringan *Layer 2*, sebagaimana ditegaskan oleh Wahyu Saputra (2017) dan Travis Quitiquit serta Vijay Bhuse (2022), yang menyoroti perlunya segmentasi VLAN yang baik untuk menghindari serangan lateral dalam jaringan. Implementasi terintegrasi dari *Port Security*, *DHCP Snooping*, dan *VLAN Hopping Mitigation* terbukti mampu memberikan perlindungan yang lebih menyeluruh dan efisien dalam menjaga

E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 5 No. 3 (2024) | September
OPEN ACCESS
https://doi.org/10.35870/jimik.v5i3.975

stabilitas dan keamanan jaringan dari berbagai jenis serangan siber, sesuai dengan tantangan yang dijelaskan oleh Arif Ali Mughal (2020) dalam studi terkait serangan pada lapisan OSI.

4. Kesimpulan

Berdasarkan hasil pengujian dan perbandingan berbagai metode pengamanan, ditemukan bahwa setiap metode memiliki algoritma dan tujuan yang berbeda secara signifikan. Misalnya, *Port Security* berfungsi untuk memblokir *mac-address* dari perangkat yang tidak diizinkan dalam jaringan LAN, sementara DHCP *Snooping* bertujuan untuk membatasi server DHCP sehingga hanya server yang terpercaya yang dapat memberikan alamat IP, serta memblokir server DHCP yang tidak dikenal atau disebut sebagai untrusted server. Selain itu, Vlan *Hopping Mitigation* digunakan untuk melakukan segmentasi jaringan agar lebih terstruktur dan membatasi perangkat luar yang tiba-tiba terhubung ke switch. Dari penelitian dan perbandingan ini, disimpulkan bahwa setiap metode sangat efektif dalam menghadapi serangan *spoofing*, *man-in-the-middle* (MITM), dan *flooding*, khususnya pada Layer 2 OSI. *Port Security* mencegah *MITM* dan *spoofing*, sedangkan Vlan *Hopping Mitigation* dan DHCP *Snooping* efektif mencegah *flooding*. *Network engineer* memiliki fleksibilitas dalam memilih metode yang sesuai dengan kebutuhan jaringan LAN yang dimiliki.

5. Daftar Pustaka

Adjei, H. A., Shunhua, M. T., Agordzo, G. K., Li, Y., Peprah, G., & Gyarteng, E. S. (2021, February). SSL stripping technique (DHCP snooping and ARP spoofing inspection). In *2021 23rd International Conference on Advanced Communication Technology (ICACT)* (pp. 187-193). IEEE. https://doi.org/10.23919/ICACT51234.2021.9370460.

Akashi, S., & Tong, Y. (2019). Classification of DHCP spoofing and effectiveness of DHCP snooping. In *Proceedings on 2018 International Conference on Advances in Computer Technology, Information Science and Communication, edited by Wen-Bing Horng and Yong Yue* (pp. 233-238).

Al Fikri, K., & Djuniadi, D. (2021). Keamanan Jaringan Menggunakan Switch Port Security. *InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan*, *5*(2), 302-307. https://doi.org/10.30743/infotekjar.v5i2.3501

Alsaadi, R. R., & Abdul-Zahra, D. S. Security DHCP Server on Lan Network. *Turkish Journal of Physiotherapy and Rehabilitation*, *32*(3). 5121–5132.

Anggreni, N. K. A. S., & Jasa, L. (2022). Literatur Review Analisis metode De-Militarized Zone (DMZ) dan Switch Port Security Sebagai Metode Keamanan Jaringan. Majalah Ilmiah Teknologi Elektro, 21(2), 195.

Hayaty, N. (2020). Buku Ajar: Sistem Keamanan. *Jakarta: Universitas Maritim*.

Iskandar, D., Farisyihab, J. R., Bahari, M. H. T., Nurfaishal, M. D., & Khairullah, M. D. (2024). Application of The SD-WAN Load Balancing Method in Managing Internet Bandwidth at IDN Bogor Vocational School. *International Journal Software Engineering and Computer Science (IJSECS)*, *4*(1), 24-39. https://doi.org/10.35870/ijsecs.v4i1.2100.

E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 5 No. 3 (2024) | September
OPEN ACCESS
https://doi.org/10.35870/jimik.v5i3.975

Mahmood, S., Mohsin, S. M., & Akber, S. M. A. (2020, January). Network security issues of data link layer: An overview. In *2020 3rd international conference on computing, mathematics and engineering technologies (iCoMET)* (pp. 1-6). IEEE. https://doi.org/10.1109/iCoMET48670.2020.9073825

Medianto, M. (2020). Analisis Keamanan Jaringan Local Area Network yang Menggunakan DHCP Server Berbasis Cisco dengan metode Penetration Testing. *Journal of Information System and Technology (JOINT)*, *1*(1), 100-124. https://doi.org/10.37253/joint.v1i1.1386.

Mughal, A. A. (2020). Cyber Attacks on OSI Layers: Understanding the Threat Landscape. *Journal of Humanities and Applied Science Research*, *3*(1), 1-18. https://orcid.org/0009-0006-8460-8006.

Nasser, H. I., & Hussain, M. A. (2022). Provably curb man-in-the-middle attack-based ARP spoofing in a local network. *Bulletin of Electrical Engineering and Informatics*, *11*(4), 2280-2291. https://doi.org/10.11591/eei.v11i4.3810.

Pradana, D. A., & Budiman, A. S. (2021). The dhcp snooping and dhcp alert method in securing dhcp server from dhcp rogue attack. *IJID (International Journal on Informatics for Development)*, *10*(1), 38-46. https://doi.org/10.14421/ijid.2021.2287

Purnomo, A. (2024). Implementation of DHCP Snooping Method to Improve Security on Computer Networks. *bit-Tech*, *6*(3). https://doi.org/10.32877/bt.v6i3.1174

Quitiqut, T., & Bhuse, V. (2022, March). Utilizing Switch Port Link State to Detect Rogue Switches. In *International Conference on Cyber Warfare and Security* (Vol. 17, No. 1, pp. 272-278).

Sandi, T. A. A., Firmansyah, F., Dewi, S., Pratama, E. K., & Astuti, R. D. (2022). Comparison of Port Security Switch Layer 2 MAC Address Dynamic With MAC Address Static Sticky. *Inspiration: Jurnal Teknologi Informasi dan Komunikasi*, *12*(2), 65-75. https://doi.org/10.35585/inspir.v12i2.8.

Saputra, B. R. (2022). Simulasi Keamanan Jaringan Dengan Metode DHCP Snooping Dan VLAN Mengggunakan CISCO. *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, *9*(4), 3481-3488. https://doi.org/10.35957/jatisi.v9i4.2730.

Saputra, W., & Fajar Suryawan, S. T. (2017). *Implementasi VLAN dan Spanning Tree Protocol Menggunakan GNS 3 dan Pengujian Sistem Keamanannya* (Doctoral dissertation, Universitas Muhammadiyah Surakarta). https://eprints.ums.ac.id/id/eprint/56316.

Satria, A., & Ramadhani, F. (2023). Analisis Keamanan Jaringan Komputer dengan Menggunakan Switch Port Security di Cisco Packet Tracer. *sudo Jurnal Teknik Informatika*, *2*(2), 52-60.

Setiawan, Y. B., Nawawi, I., & Pravitasari, D. (2022). Desain Infrastruktrur Jaringan Inter-Vlan dengan Keamanan Port Security dan Secure Shell Berbasis Protocol Open Short Path First. *ULIL ALBAB: Jurnal Ilmiah Multidisiplin*, *2*(1), 250-258.

Sukaridhoto, S., & ST Ph, D. (2014). Buku Jaringan Komputer I. *Surabaya: Politeknik Elektronika Negeri Surabaya*.

Sulaiman, O. K. (2016). Analisis Sistem Keamanan Jaringan Dengan Menggunakan Switch Port Security. *CESS (Journal Of Computer Engineering, System And Science)*, *1*(1), 9-14.

E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 5 No. 3 (2024) | September
OPEN ACCESS
https://doi.org/10.35870/jimik.v5i3.975

Sutiman, S., & Gunawan, A. (2021). Firewall port security switch untuk keamanan jaringan komputer menggunakan cisco router 1600s pada pt. tirta kencana tata warna sukabumi. *CONTEN: Computer and Network Technology*, *1*(1), 13-22. https://doi.org/10.31294/conten.v1i1.402

Tripathi, N., & Hubballi, N. (2018). Detecting stealth DHCP starvation attack using machine learning approach. *Journal of Computer Virology and Hacking Techniques*, *14*, 233-244. https://doi.org/10.1007/s11416-017-0310-x.

Wibowo, A. (2022). *Sistem jaringan komputer*. Yayasan Prima Agus Teknik.

Zara, S. S., Elhanafi, A. M., & Handoko, D. (2020). Pemodelan jaringan WAN dengan teknologi frame relay dengan memanfaatkan switch port security sebagai sistem keamanan jaringan. *SNASTIKOM*, 1(2).