khazanah informatika

Jurnal Ilmu Komputer dan Informatika

Implementasi *VLAN* dan *Spanning Tree Protocol* Menggunakan *GNS 3* dan Pengujian Sistem Keamanannya

Wahyu Saputra[1*], Fajar Suryawan[2]
[1]Program Studi Informatika
Universitas Muhammadiyah Surakarta
[2] Program Studi Teknik Elektro
Universitas Muhammadiyah Surakarta
*wahyusaputra12@outlook.com

Absstrak-Pada saat ini setiap perusahaan atau organisasi menggunakan jaringan komputer. Oleh karena itu maka perlu dibuat sebuah jaringan komputer dengan memiliki kinerja yang lebih baik. Dari hasil analisis, *Virtual Local Area Network (VLAN)* merupakan sebuah konsep jaringan yang mampu memberikan hasil maksimal baik dari segi efisiensi perangkat, konfigurasi, dan keamanan jaringan yang digunakan. Selain itu, banyak perusahaan atau organisasi juga menerapkan konsep *Spanning Tree Protocol*. Penggunaan *Spanning Tree Protocol* adalah untuk mencegah terjadinya *broadcast storm* apabila sebuah perusahaan atau organisasi menerapkan sistem *redundant* pada perangkat jaringan digunakan. Meskipun telah memiliki tingkat keamanan yang baik namun masih perlu diuji dengan beberapa serangan dari pihak luar. Beberapa serangan yang mampu mengganggu jaringan *VLAN* dan *Spanning Tree Protocol* adalah *VLAN Hopping* dan *Spanning Tree Protocol Attack*. Dalam penelitian ini dilakukan implementasi jaringan *VLAN* dan *Spanning Tree Protocol* menggunakan aplikasi *GNS 3* serta pengujian sistem keamanan pada jaringan *VLAN* dan *Spanning Tree Protocol* dari *VLAN Hopping* dan *Spanning Tree Protocol Attack*.

Kata Kunci: *Spanning Tree Protocol, Spanning Tree Protocol Attack, VLAN, VLAN Hopping.*

1. Pendahuluan

Perkembangan teknologi jaringan komputer pada saat ini telah tumbuh dengan pesat. Banyak perusahaan maupun organisasi yang memanfaatkan jaringan komputer untuk kegiatan operasional sehari-hari. Jaringan *local area network* (*LAN*) merupakan salah satu konsep yang banyak diterapkan berbagai perusahaan maupun organisasi. Pada dasarnya, jaringan *LAN* sudah cukup membantu bagi perusahaan atau organisasi dalam membantu kegiatan operasional sehari-hari. Namun seiring dengan berkembangnya kebutuhan jaringan komputer, maka ditemukan beberapa kelemahan dari jaringan *LAN*. Untuk mengatasi kelemahan tersebut, maka dilakukan pengembangan dari jaringan *LAN* menjadi konsep jaringan *virtual local area network* (*VLAN*). Tambe (2015) mendefinisikan *VLAN* sebagai kumpulan beberapa *workstation* dalam *LAN* yang mampu berkomunikasi satu sama lain pada *LAN* yang sama dan saling terisolasi. Tulloh (2015) mendefinisikan VLAN (Virtual LAN) adalah sebuah teknologi yang dapat mengkonfigurasi jaringan logis independen dari struktur jaringan fisik. Selain definisi tersebut, Ali (2015) mendefinisikan bahwa *VLAN* merupakan sebuah *LAN* yang terkonfigurasi secara *software* bukan menggunakan kabel fisik. Prasetyo (2014) mengatakan bahwa *VLAN* dapat membagi jaringan berdasarkan *subnet*, hak akses, serta aplikasi yang digunakan oleh beberapa *host* di dalam satu perangkat *switch* yang sama. Lewis (2008) dalam bukunya yang berjudul *LAN Switching and Wireless: CCNA Exploration Companion Guide* mengatakan bahwa sebuah *VLAN* memungkinkan seorang *administrator* untuk menciptakan sekelompok peralatan yang secara *logic* dihubungkan satu sama lain. Dari beberapa pernyataan tersebut, penerapan konsep *VLAN* membuat jaringan *switch* dapat dibagi secara *logic* berdasarkan fungsi, departemen atau *project* sebuah tim. *VLAN* mampu mengurangi trafik jaringan dengan membentuk beberapa domain *broadcast* untuk memecah jaringan yang besar menjadi segmen-segmen independen yang lebih kecil sehingga pengiriman *broadcast* ke setiap perangkat jaringan secara keseluruhan menjadi lebih sedikit. Selain itu, konsep *VLAN* yang diterapkan memungkinkan sebuah jaringan menjadi lebih fleksibel sehingga tujuan bisnis yang diinginkan oleh perusahaan maupun organisasi dapat tercapai.

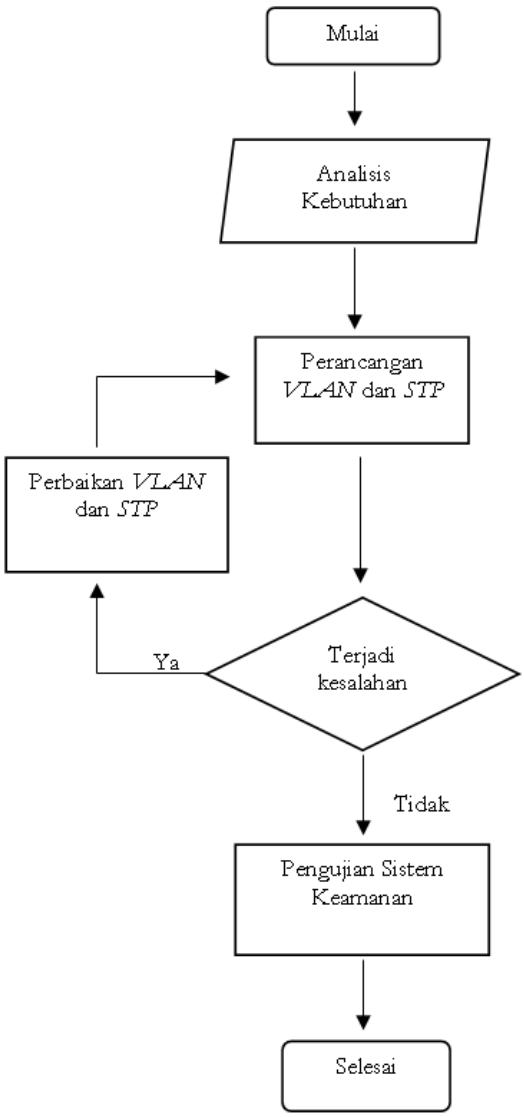
Implementasi konsep jaringan *VLAN* banyak menawarkan kelebihan bagi perusahaan maupun organisasi. Lewis (2008) menyebutkan bahwa jaringan *VLAN* memiliki beberapa kelebihan yaitu dari aspek keamanan, jaringan *VLAN* dapat memberikan keuntungan apabila sebuah departemen yang memiliki data sensitif terpisah dari jaringan yang ada, maka akan mengurangi peluang pelanggaran akses ke informasi rahasia dan penting. Dari sisi penghematan biaya, jaringan *VLAN* membuat biaya menjadi lebih hemat karena tidak diperlukannya biaya yang mahal untuk *upgrade* jaringan dan efisiensi penggunaan *bandwidth* dan *uplink* yang tersedia. Dari sisi performa, jaringan *VLAN* memberikan

kinerja yang lebih tinggi, yaitu dengan membagi jaringan *layer 2* menjadi beberapa *workgroup* secara *logic* (*broadcast domain*) serta mengurangi trafik yang tidak diperlukan pada jaringan sehingga dapat meningkatkan performa. Dari segi efisiensi dan 3 kemudahan, dengan menerapkan konsep jaringan *VLAN* maka pengelolaan jaringan lebih mudah, karena *user-user* dengan kebutuhan jaringan yang sama berbagi *VLAN* yang sama.

Banyak perusahaan atau organisasi memiliki jaringan yang cukup kompleks, selain memiliki jaringan *VLAN* yang sangat besar. Hal tersebut membuat perangkat jaringan terutama *switch* dapat digunakan semaksimal mungkin. Sistem *redundant switch* merupakan salah satu konsep yang dapat digunakan untuk mencegah terjadinya gangguan kegiatan operasional sebuah perusahaan atau organisasi apabila perangkat *switch* mengalami kerusakan. Efendi (2013) mengatakan bahwa *redundancy* merupakan langkah antisipasi terhadap suatu kegagalan dalam suatu proses aktivitas pengiriman data. Apabila sistem *redundant* diterapkan maka terjadinya *loop* dan *broadcast storm* data akan semakin besar. Oleh karena itu diperlukan *Spanning Tree Protocol* pada sebuah jaringan *VLAN*. Wiguna *et al.* (2013) mendefinisikan bahwa *spanning tree protocol* merupakan *link* manajemen protokol pada *layer 2* yang menyediakan sistem jalur *backup* dan juga mencegah terjadinya *loop* dan *broadcast storm* yang tidak diinginkan pada jaringan yang memiliki beberapa jalur menuju ke satu tujuan dari suatu *host*.

Dari aspek keamanan, meskipun jaringan *VLAN* telah memiliki tingkat keamanan yang cukup baik namun masih perlu diuji dengan beberapa serangan dari pihak luar. Beberapa serangan yang mampu mengganggu adalah *VLAN hopping* dan *spanning tree protocol attack*. Bajpai *et al.* (2016) mengatakan bahwa *VLAN hopping* bertujuan untuk membuat penyerang mendapatkan akses dari satu *VLAN* ke *VLAN* yang lainnya, sedangkan *spanning tree protocol attack* melibatkan seorang penyerang yang akan mengambil alih hak akses *root bridge* pada sebuah topologi. Vyncke *et al.* (2008) dalam bukunya yang berjudul *LAN Switch Security: What Hackers Know about Your Switches* mengatakan bahwa *spanning tree protocol attack* memiliki beberapa skenario serangan yaitu mengambil alih hak akses *root bridge* dan menimbulkan *denial of service* menggunakan pengiriman konfigurasi *bridge protocol data unit* (*BPDU*). Bajpai *et al.* (2016) mengatakan bahwa *VLAN hopping* memiliki beberapa skenario serangan yaitu *double tagging attack*. Serangan *VLAN hopping* dan *spanning tree protocol attack* dapat mengancam kerahasiaan data penting yang dimiliki oleh perusahaan. Supriyono *et al.* (2013) mengatakan bahwa data-data perusahaan adalah termasuk informasi rahasia yang harus dijaga.

Dalam penelitian ini dilakukan implementasi jaringan *VLAN* dan *spanning tree protocol* menggunakan aplikasi *GNS 3* serta menguji jaringan *VLAN* dan *spanning tree protocol* dari aspek sistem keamanannya. Tujuan utama dari penelitian ini adalah bagaimana perancangan jaringan *VLAN* dan *spanning tree protocol* yang diimplementasikan menggunakan simulator jaringan *GNS 3* serta bagaimana meningkatkan sistem keamanan dari jaringan *VLAN* dan *spanning tree protocol* yaitu dengan cara mengambil tindakan mitigasi yang tepat dari jaringan *VLAN* dan *spanning tree protocol* apabila terjadi serangan *VLAN hopping* maupun *spanning tree protocol attack*.



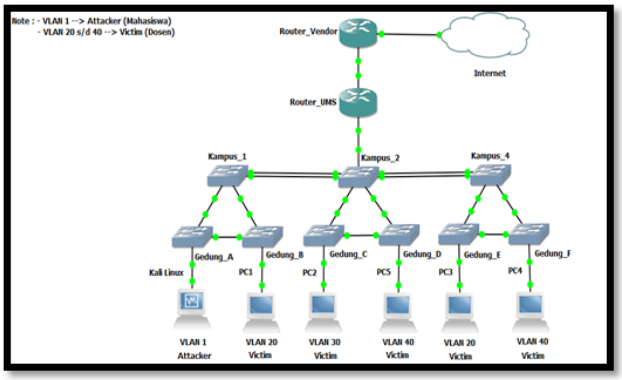
Gambar 1. Diagram alir penelitian.

2. Metode

Pada penelitian ini, untuk mengimplementasikan *VLAN* dan *spanning tree protocol* menggunakan aplikasi *GNS 3* dan sebuah *tool* yaitu *yersinia* sebagai pengujian dari sistem keamanannya. Rancangan jaringan *VLAN* dan *spanning tree protocol* menggunakan contoh topologi dari sebagian gedung di Universitas Muhammadiyah Surakarta. Topologi jaringan *VLAN* dan *spanning tree protocol* yang dirancang akan dilakukan pengujian terhadap sistem keamanannya dengan beberapa serangan yaitu *VLAN hopping* dan *spanning tree protocol attack*. Gambaran umum penelitian yang akan dilakukan dapat dilihat pada Gambar 1.

2.1 Analisis Kebutuhan

Pada tahapan ini dilakukan analisis terhadap alat maupun bahan yang dibutuhkan seperti spesifikasi *hardware* maupun *software* untuk mendukung penelitian. Spesifikasi *hardware* komputer yang dibutuhkan untuk mendukung penelitian ini yaitu: *Processor Intel Core i3-2348M 2.30 GHz, RAM 4 GB DDR3*, *Harddisk 500 GB HDD* dengan sistem



Gambar 2. Topologi *virtual local area network* (*VLAN*) dan *spanning tree protocol*

```
Gedung_B#vlan database
Gedung_B(vlan)#vlan 20
VLAN 20 added:
    Name: VLAN0020
```

```
Gedung_B(config)#int fa2/2
Gedung_B(config-if)#switchport mode access
Gedung_B(config-if)#switchport access vlan 20
```

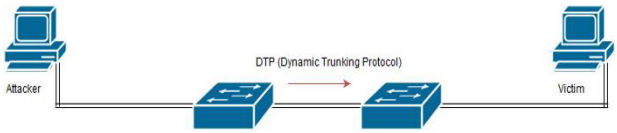
```
Gedung_B(config)#int fa2/1
Gedung_B(config-if)#switchport mode trunk
```

```
Gedung_B#sh vlan-switch

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa2/3, Fa2/4, Fa2/5, Fa2/6
                                                Fa2/7, Fa2/8, Fa2/9, Fa2/10
                                                Fa2/11, Fa2/12, Fa2/13, Fa2/14
                                                Fa2/15, Fa3/0, Fa3/1, Fa3/2
                                                Fa3/3, Fa3/4, Fa3/5, Fa3/6
                                                Fa3/7, Fa3/8, Fa3/9, Fa3/10
                                                Fa3/11, Fa3/12, Fa3/13, Fa3/14
                                                Fa3/15
20   VLAN0020                         active    Fa2/2
30   VLAN0030                         active
40   VLAN0040                         active
```

Gambar 3. Konfigurasi *virtual local area network* (*VLAN*)

```
Gedung_B#sh spanning-tree vlan 1 brief

VLAN1
  Spanning tree enabled protocol ieee
  Root ID    Priority    8192
             Address     cc03.0df8.0000
             Cost        19
             Port        81 (FastEthernet2/0)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768
             Address     cc05.0b38.0000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface                                  Designated
Name               Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
------------------ ------- ---- ----- --- ----- -------------------- -------
FastEthernet2/0    128.81   128    19 FWD     0  8192 cc03.0df8.0000 128.84
FastEthernet2/1    128.82   128    19 BLK    19 32768 cc04.1d78.0000 128.82
```

Gambar 4. Konfigurasi *spanning tree protocol*



Gambar 5. *VLAN hopping*

operasi yaitu *Windows 10* (32 bit) pada *hostcomputer* dan *kali linux* (32 bit) pada *guest virtual machine*. Spesifikasi *software* yang digunakan untuk mendukung penelitian ini yaitu: *Graphic Network Simulator* (*GNS*) *3*, *Virtual box*, *Yersinia, Wireshark*.

2.2 Perancangan *Virtual Local Area Network (VLAN)* dan *Spanning Tree Protocol*

Pada tahapan ini, dilakukan perancangan topologi untuk jaringan *VLAN* dan *spanning tree protocol* serta konfigurasinya di masing-masing perangkat. Topologi jaringan *VLAN* dan *spanning tree protocol* yang dirancang menggunakan contoh topologi sebagian gedung kampus di Universitas Muhammadiyah Surakarta. Gambaran topologi yang dirancang menggunakan *GNS 3* dapat dilihat pada Gambar 2.

Dari Gambar 2 dapat dilihat bahwa ada 3 kampus di Universitas Muhammadiyah Surakarta yang digunakan sebagai topologi jaringan *VLAN* dan *spanning tree protocol*. Setiap kampus masing-masing memiliki beberapa *switch* yang digunakan untuk mendistribusikan jaringan ke *client* dan terdapat *backbone switch* yang digunakan untuk menghubungkan jaringan antar kampus. *Backbone switch* yang terdapat di salah satu kampus juga digunakan untuk menghubungkan jaringan ke perangkat *router* utama di Universitas Muhammadiyah Surakarta yang nantinya akan terhubung ke jaringan internet. Konfigurasi *VLAN* dan *spanning tree protocol* dari topologi jaringan yang dirancang menggunakan *GNS 3* adalah sebagai berikut :

a. Konfigurasi *IP address*
   Proses awal dimulai dengan melakukan konfigurasi *IP address* di setiap perangkat jaringan. Jaringan yang menghubungkan antara *router vendor* dengan internet menggunakan *network IP* 192.168.100.0/24 dengan *IP address* 192.168.100.20/24 untuk *router vendor*. Koneksi antara *router vendor* dengan *router* UMS menggunakan *network IP* 192.168.1.0/24 dengan *IP address* 192.168.1.1/24 untuk *router vendor* dan *IP address* 192.168.1.2/24 untuk *router* UMS. Jaringan yang menghubungkan antara *router* UMS dengan *client* yang ada di setiap gedung kampus menggunakan *network IP* 192.168.10.0/24 dengan *IP address* 192.168.10.1/24 untuk *router* UMS dan *IP address* 192.168.10.2/24-192.168.10.7/24 untuk setiap *client* di kampus yang berbeda. *IP address* 192.168.10.1/24 digunakan sebagai *gateway* oleh *client* yang ada di setiap gedung kampus.
b. Konfigurasi *Virtual Local Area Network* (*VLAN*)
   Dalam topologi jaringan pada Gambar 2 terdapat perbedaan *VLAN ID* di setiap *client* yang bertujuan untuk mengisolasi jaringan di setiap unit kerja yang berbeda. *VLAN ID* yang digunakan dalam topologi jaringan pada Gambar 2 yaitu *VLAN 1*, *VLAN 20*, *VLAN 30*, *VLAN 40*. *VLAN ID* yang digunakan oleh mahasiswa berada di *VLAN 1* sedangkan *VLAN 20* sampai dengan *VLAN 40* digunakan oleh para dosen. Untuk dapat saling bertukar informasi antar *VLAN*, setiap *client* menggunakan *port* yang terhubung ke *switch*. Setiap *client* hanya dapat mentransmisikan *frame* atau paket dalam 1 *VLAN ID* saja. *Port* yang menghubungkan antara *client* dengan *switch* menggunakan konfigurasi *mode access*. Setiap *switch* akan menerima *frame* atau paket *VLAN ID* dari *port client* kemudian akan mentransmisikan *frame* atau paket kembali ke *VLAN ID* yang menjadi tujuan menggunakan *port* yang menghubungkan antar *switch*. Setiap *switch* dapat mentransmisikan *frame* atau paket dengan lebih dari 1 *VLAN ID* yang berbeda. *Port* yang menghubungkan antar *switch* menggunakan konfigurasi *mode trunk*. Konfigurasi *virtual local area network* (*VLAN*) dapat dilihat pada Gambar 3.
c. Konfigurasi *Spanning Tree Protocol*
   Dari Gambar 2 dapat dilihat bahwa setiap *switch* memiliki beberapa jalur *backup* yang digunakan apabila salah satu koneksi jaringan terjadi kerusakan dapat menggunakan jalur koneksi yang lain agar jaringan masih dapat berjalan dengan normal. Penggunaan jalur yang digunakan sebagai *backup* dapat memperlambat kinerja sebuah jaringan dan akan mengakibatkan terjadinya *loop* dan *broadcast storm*, maka setiap *switch* menggunakan konsep *spanning tree protocol* untuk meminimalisir kerugian penggunaan jalur *backup*. Konsep *spanning tree protocol* akan mencegah terjadinya *redundant link* pada jaringan dengan menerapkan beberapa proses algoritma yaitu menentukan nilai *bridge ID* paling rendah, menentukan *root path cost* paling rendah, menentukan *sender bridge ID* paling rendah, dan menentukan *port ID* paling rendah. Dari penggunaan algoritma *spanning tree protocol* dapat menentukan pemilihan *root bridge*, *root port* untuk setiap *non-root bridge*, dan *designated port* dan *non-designated port* untuk setiap segmen *network* agar terjadi konvergensi. Dalam penelitian ini digunakan *spanning tree protocol* jenis *per VLAN spanning tree protocol* (*PVST*). Penggunaan *PVST* membuat *spanning tree protocol* dapat dikonfigurasi secara terpisah dan mengakibatkan perbedaan konfigurasi di masing-masing *VLAN* sehingga proses menuju konvergensi menjadi lebih cepat. Konfigurasi *spanning tree protocol* dapat dilihat pada Gambar 4.

2.3 Pengujian Sistem Keamanan

Pada tahapan ini, dilakukan pengujian sistem keamanan dari rancangan jaringan *VLAN* dan *spanning tree protocol* dengan menggunakan *tool* yaitu *yersinia*. Pada Gambar 2 dapat dilihat bahwa *host* dengan *VLAN ID 1* akan menjadi *attacker* untuk melakukan serangan terhadap *host* dengan *VLAN ID 20* sampai dengan *VLAN ID 40* yang akan menjadi target serangan atau *victim* dengan asumsi bahwa *attacker* mempunyai hak akses untuk bergabung dalam jaringan *VLAN* dan *spanning tree protocol* yang telah dirancang. Skenario serangan yang digunakan untuk menguji sistem keamanan dari jaringan *VLAN* dan *spanning tree protocol* yaitu:

a. *VLAN hopping*
b. *Spanning tree protocol attack*.

Skenario serangan pertama yang digunakan oleh *VLAN ID 1* adalah *VLAN hopping*. Skenario *VLAN hopping* merupakan jenis serangan yang dilakukan dengan cara mengambil hak akses dari satu *VLAN* ke *VLAN* lainnya. Metode yang dapat digunakan dalam skenario

VLAN hopping yaitu *double tagging attack*. Metode *double tagging attack* merupakan metode serangan dalam *VLAN hopping* yang dilakukan dengan cara menanamkan tag *802.1Q encapsulation* tambahan di dalam *frame* agar *attacker* dapat berkomunikasi dengan *host* yang menjadi target serangan. Skenario serangan *VLAN hopping* dapat dilihat pada Gambar 5.

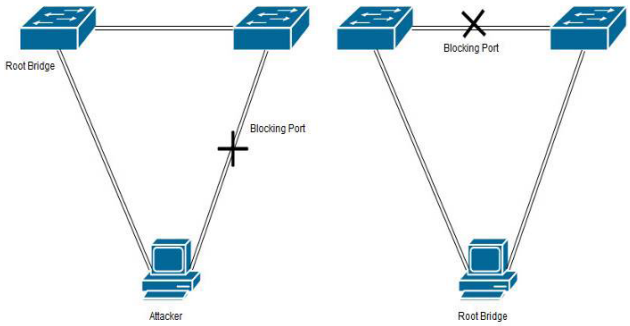
Skenario serangan kedua yang digunakan oleh *VLAN ID 1* adalah *spanning tree protocol attack*. Skenario *spanning tree protocol attack* merupakan jenis serangan yang dilakukan dengan cara mengubah nilai *bridge ID* terendah pada sebuah *switch* agar *attacker* dapat mengambil hak akses menjadi *root bridge*. Metode yang digunakan dalam skenario *spanning tree protocol attack* ada 2 jenis yaitu *taking over root bridge* dan *DoS using flood of config BPDU*. Metode *taking over root bridge* merupakan sebuah metode serangan dalam *spanning tree protocol attack* yang dilakukan dengan cara mengambil hak akses *root bridge* dari *switch* yang memiliki nilai *bridge ID* terendah. Apabila serangan *taking over root bridge* berhasil dilakukan, maka seorang *attacker* akan menjadi *root bridge* dan dapat melihat beberapa variasi *frame*. Metode *DoS using flood of config BPDU* merupakan metode serangan *spanning tree protocol attack* selanjutnya yang dilakukan dengan cara mengirimkan konfigurasi *BPDU* per detik dengan jumlah yang besar sehingga penggunaan *resource CPU* pada switch akan menjadi lebih tinggi dan membuat sistem jaringan menjadi *down*. Skenario serangan *spanning tree protocol attack* dapat dilihat pada Gambar 6.

c. Pengujian Sistem Keamanan *Virtual Local Area Network* (*VLAN*)

Pada tahap ini dilakukan pengujian sistem keamanan *VLAN* menggunakan metode serangan *VLAN hopping* yaitu *double tagging attack*. Dari Gambar 2 dapat dilihat bahwa *host* dengan *VLAN ID 1* akan menjadi *attacker* untuk melakukan *double tagging attack*. Sebelum melakukan serangan *double tagging*, *port attacker* yang terhubung ke *switch* gedung A diasumsikan telah bergabung dalam jaringan *VLAN* dan *spanning tree protocol* dan memiliki hak akses untuk menjadi *trunk port*. Konfigurasi *port attacker* yang terhubung ke *switch* gedung A dapat dilihat pada Gambar 7.

Attacker akan melakukan *double tagging attack* dengan cara mengubah menanamkan tag *802.1Q encapsulation* tambahan di dalam *frame* untuk diteruskan ke *host* yang akan menjadi target serangan menggunakan *tool* yaitu *yersinia*. Metode serangan yang digunakan *attacker* pada *tool yersinia* adalah *sending 802.1Q double encapsulation packet*. Proses serangan *double tagging* dengan *tool yersinia* dapat dilihat pada Gambar 8.

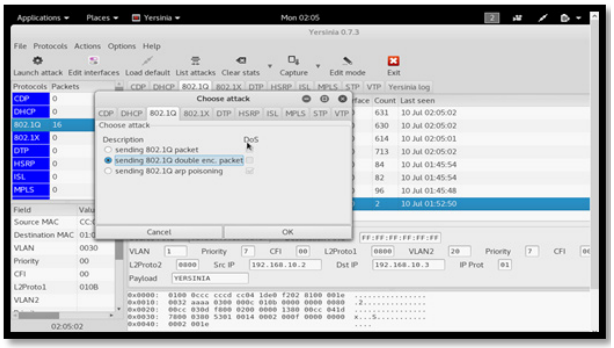
Metode serangan *sending 802.1Q double encapsulation packet* dari *tool yersinia* berhasil menanamkan tag *802.1Q encapsulation* tambahan di dalam *frame* yang dikirimkan menuju *host* target serangan sehingga *attacker* dapat berkomunikasi dengan *host* yang menjadi target serangan. Proses komunikasi yang berhasil dilakukan *attacker* dengan *host* yang memiliki *VLAN ID* yang berbeda dapat dilihat pada Gambar 9.



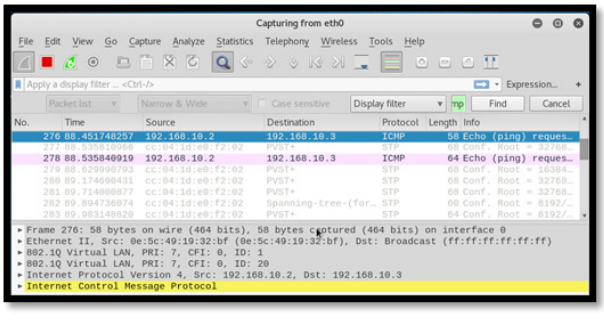
Gambar 6. *Spanning tree protocol attack*

```
Gedung_A#sh int fa2/2 switchport
Name: Fa2/2
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Disabled
Access Mode VLAN: 0 ((Inactive))
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Trunking VLANs Active: 1,20,30,40
Priority for untagged frames: 0
Override vlan tag priority: FALSE
Voice VLAN: none
Appliance trust: none
```

Gambar 7. Konfigurasi *port attacker* yang terhubung ke *switch* gedung A



Gambar 8. Proses *double tagging attack*



Gambar 9. Hasil *capture double tagging attack* di *Wireshark*

d. Pengujian Sistem Keamanan *Spanning Tree Protocol*

Tahap pertama untuk menguji sistem keamanan dari *spanning tree protocol* digunakan metode serangan *spanning tree protocol attack* yaitu *taking over root bridge*. Dari Gambar 2 dapat dilihat bahwa *host* dengan *VLAN ID 1* akan menjadi *attacker* untuk melakukan *taking over root bridge* dengan asumsi bahwa *attacker* mempunyai hak akses untuk bergabung dalam jaringan *VLAN* dan *spanning tree*

protocol. Sebelum *attacker* melakukan *taking over root bridge, backbone switch* di kampus 1 UMS bertugas menjadi *root bridge*. Konfigurasi *spanning tree protocol* pada *backbone switch* di kampus 1 UMS dapat dilihat pada Gambar 10.

Pada saat *backbone switch* kampus 1 UMS menjadi *root bridge*, status salah satu *port switch* antara gedung A dan gedung B yang terhubung ke kampus 1 adalah *blocking*. Konfigurasi *spanning tree protocol* pada *switch* gedung A yang menghubungkan *port attacker* dapat dilihat pada Gambar 11.

Attacker akan melakukan *taking over root bridge* dari *backbone switch* kampus 1 UMS dengan menggunakan *tool* yaitu *yersinia*. Metode serangan yang digunakan *attacker* pada *tool yersinia* adalah *claiming root role*. Proses serangan *taking over root bridge* dengan *tool yersinia* dapat dilihat pada Gambar 12.

Metode serangan *claiming root role* dari *tool yersinia* berhasil mengambil hak akses *root bridge* dari *backbone switch* kampus 1 UMS dengan cara memperkecil nilai *MAC address* sehingga terjadi konvergensi dan mengubah status *attacker* menjadi *root bridge*. Konfigurasi *spanning tree protocol* pada *attacker* setelah terjadi *taking over root bridge* dapat dilihat pada Gambar 13.

Pada tahap yang kedua dalam menguji sistem keamanan *spanning tree protocol* digunakan metode serangan *spanning tree protocol attack* yang lainnya yaitu *DoS using flood config BPDU* dengan asumsi bahwa *attacker* mempunyai hak akses untuk bergabung dalam jaringan *VLAN* dan *spanning tree protocol*. Sebelum *attacker* melakukan serangan *DoS using flood config BPDU*, tingkat penggunaan *resource CPU* pada *switch* dan trafik penerimaan konfigurasi *BPDU* pada *switch* gedung A masih terlihat normal. Tingkat penggunaan *resource CPU* pada *switch* dan trafik penerimaan konfigurasi *BPDU* pada *switch* gedung A dapat dilihat pada Gambar 14.

Attacker akan melakukan serangan menggunakan metode yang tersedia pada *tool yersinia* yaitu *sending conf BPDUs* dengan tujuan meningkatkan penggunaan *resource CPU* dan trafik penerimaan konfigurasi *BPDU* pada *switch* gedung A. Proses serangan *DoS using flood config BPDU* dengan *tool yersinia* dapat dilihat pada Gambar 15.

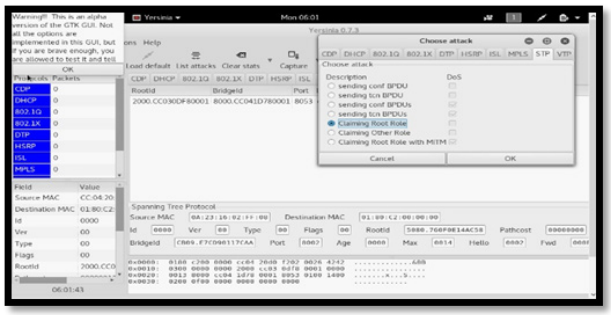
Metode serangan *sending conf BPDUs* dari *tool yersinia* berhasil meningkatkan penggunaan *resource CPU* dan trafik penerimaan konfigurasi *BPDU*. Tingkat penggunaan *resource CPU* pada *switch* dan trafik penerimaan konfigurasi *BPDU* pada *switch* gedung A setelah terjadi *DoS using flood config BPDU* dapat dilihat pada Gambar 16.

```
Kampus_1#sh spanning-tree vlan 1 brief

VLAN1
  Spanning tree enabled protocol ieee
  Root ID     Priority    8192
              Address     cc03.0df8.0000
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    8192
              Address     cc03.0df8.0000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface                                    Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet2/0      128.81   128    19 FWD     0  8192 cc03.0df8.0000 128.81
FastEthernet2/1      128.82   128    19 FWD     0  8192 cc03.0df8.0000 128.82
FastEthernet2/2      128.83   128    19 FWD     0  8192 cc03.0df8.0000 128.83
FastEthernet2/3      128.84   128    19 FWD     0  8192 cc03.0df8.0000 128.84
```

Gambar 10. Konfigurasi *spanning tree protocol* pada *switch* kampus 1 UMS

```
Gedung_A#sh spanning-tree vlan 1 brief

VLAN1
  Spanning tree enabled protocol ieee
  Root ID     Priority    8192
              Address     cc03.0df8.0000
              Cost        19
              Port        81 (FastEthernet2/0)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32768
              Address     cc04.1d78.0000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface                                    Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet2/0      128.81   128    19 FWD     0  8192 cc03.0df8.0000 128.83
FastEthernet2/1      128.82   128    19 FWD    19 32768 cc04.1d78.0000 128.82
FastEthernet2/2      128.83   128    19 FWD    19 32768 cc04.1d78.0000 128.83
```

Gambar 11. Konfigurasi *Spanning Tree Protocol* pada *switch* gedung A



Gambar 12. Proses *taking over root bridge*

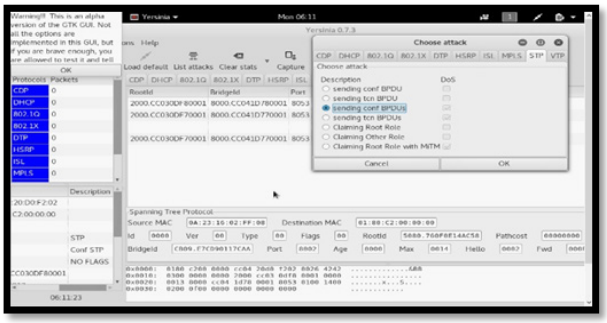
```
Gedung_A#sh spanning-tree vlan 1 brief

VLAN1
  Spanning tree enabled protocol ieee
  Root ID     Priority    8192
              Address     cc03.0df7.0000
              Cost        38
              Port        83 (FastEthernet2/2)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32768
              Address     cc04.1d78.0000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface                                    Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet2/0      128.81   128    19 FWD    38 32768 cc04.1d78.0000 128.81
FastEthernet2/1      128.82   128    19 FWD    38 32768 cc04.1d78.0000 128.82
FastEthernet2/2      128.83   128    19 FWD    19 32768 cc04.1d77.0000 128.83
```

Gambar 13. Konfigurasi *spanning tree protocol* pada *switch* gedung A

```
Gedung_A#sh proc cpu | incl sec
CPU utilization for five seconds: 1%/0%; one minute: 1%; five minutes: 1%
```

```
Gedung_A#sh spanning-tree vlan 1 int fa2/2
 Port 83 (FastEthernet2/2) of VLAN1 is forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.83.
   Designated root has priority 8192, address cc03.0df7.0000
   Designated bridge has priority 32768, address cc04.1d77.0000
   Designated port id is 128.83, designated path cost 19
   Timers: message age 3, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   BPDU: sent 7893, received 179
```

Gambar 14. Tingkat penggunaan *resource CPU* dan trafik penerimaan konfigurasi *BPDU*



Gambar 15. Proses *DoS using flood config BPDU*

```
Gedung_A#sh proc cpu | incl second
CPU utilization for five seconds: 20%/100%; one minute: 10%; five minutes: 4%
```

```
Gedung_A#sh spanning-tree vlan 1 int fa2/2
 Port 83 (FastEthernet2/2) of VLAN1 is forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.83.
   Designated root has priority 1, address 8cda.5c71.1ccd
   Designated bridge has priority 32768, address cc04.1d78.0000
   Designated port id is 128.83, designated path cost 133   Hello is pending
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   BPDU: sent 8079, received 21231
```

Gambar 16. Tingkat penggunaan *resource CPU* dan trafik penerimaan konfigurasi *BPDU*

```
Gedung_A(config)#int e0/1
Gedung_A(config-if)#switchport trunk native vlan 99
Gedung_A(config-if)#end
Gedung_A#sh int e1/0 switchport
*Nov 20 13:03:36.563: %SYS-5-CONFIG_I: Configured from console by console
Gedung_A#sh int e0/1 switchport
Name: Et0/1
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: trunk
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: isl
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (VLAN0099)
Administrative Native VLAN tagging: enabled
```

Gambar 17. Teknik mitigasi dengan tidak menggunakan *native VLAN 1*

```
Gedung_A(config)#int e0/2
Gedung_A(config-if)#switchport mode ?
  access        Set trunking mode to ACCESS unconditionally
  dot1q-tunnel  set trunking mode to TUNNEL unconditionally
  private-vlan  Set private-vlan mode
  trunk         Set trunking mode to TRUNK unconditionally

Gedung_A(config-if)#switchport mode dot1q-tunnel
Gedung_A(config-if)#end
Gedung_A#
*Nov 20 13:05:31.902: %SYS-5-CONFIG_I: Configured from console by console
Gedung_A#sh int e0/2 switchport
Name: Et0/2
Switchport: Enabled
Administrative Mode: tunnel
Operational Mode: tunnel
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
```

Gambar 18. Teknik mitigasi dengan tidak menggunakan *switchport dynamic auto*

3. Hasil dan Pembahasan

Dari hasil penelitian terdapat 2 topik utama yang dapat didiskusikan yaitu:

a. Hasil Implementasi VLAN dan Spanning Tree Protocol Menggunakan GNS 3

Berdasarkan hasil implementasi *VLAN* dan *spanning tree protocol* menggunakan *GNS 3* dapat dilihat bahwa konsep *VLAN* sangat efektif dalam mengisolasi jaringan sehingga mempermudah bagi *administrator* untuk melakukan pengelolaan jaringan yang bersifat kompleks. Dengan menggunakan konsep *VLAN* dapat mengurangi beban trafik jaringan sehingga performa jaringan menjadi semakin meningkat. Dari hasil implementasi juga menunjukkan bahwa konsep *spanning tree protocol* menyediakan jalur backup pada topologi yang berpotensi memiliki jalur *redundant*. Dengan menerapkan jalur *backup*, maka *spanning tree protocol* dapat mencegah terjadinya *loop* dan *broadcast storm* yang berakibat performa jaringan menjadi menurun.

b. Teknik Mitigasi Serangan *VLAN Hopping* dan *Spanning Tree Protocol Attack*

Berdasarkan hasil penelitian dapat diketahui bahwa konsep *VLAN* dan *spanning tree protocol* masih memiliki beberapa kelemahan dari aspek sistem keamanan. Namun, serangan *VLAN hopping* dan *spanning tree protocol attack* dapat diatasi dengan menggunakan beberapa teknik mitigasi.

c. Teknik mitigasi serangan *VLAN hopping* yaitu:

a) Tidak menggunakan *native vlan 1*.

Attacker dapat melakukan serangan *VLAN hopping* yaitu dengan memanfaatkan konfigurasi *native VLAN* dengan *default* nilai 1 pada *port* yang menghubungkan antar *switch*. Namun serangan *VLAN hopping* dapat diatasi dengan melakukan perubahan konfigurasi pada nilai *native VLAN*. Teknik mitigasi dengan tidak menggunakan *native VLAN 1* dapat dilihat pada Gambar 17.

b) Tidak menggunakan mode *switchport dynamic auto*.

Attacker dapat melakukan serangan *VLAN hopping* yaitu dengan memanfaatkan konfigurasi *switch* yang menggunakan mode *switchport dynamic auto*. Namun serangan *VLAN hopping* dapat diatasi dengan tidak menggunakan mode *switchport dynamic auto* dan melakukan perubahan konfigurasi mode *switchport* dari *dynamic auto* menjadi *dot1q-tunnel*. Teknik mitigasi dengan tidak menggunakan *switchport dynamic auto* dapat dilihat pada Gambar 18.

c) Menggunakan mode *switchport access* dan *switchport nonegotiate*.

Attacker tidak dapat melakukan serangan *VLAN hopping* apabila konfigurasi mode *switchport* pada *switch* menggunakan mode *switchport access* dan *switchport nonegotiate*. Teknik mitigasi dengan menggunakan mode *switchport access* dan *switchport nonegotiate* dapat dilihat pada Gambar 19.

```
Gedung_A(config)#int e0/2
Gedung_A(config-if)#switchport mode access
Gedung_A(config-if)#end
Gedung_A#sh int e0/1 switchport
*Nov 20 13:09:02.453: %SYS-5-CONFIG_I: Configured from console by console
Gedung_A#sh int e0/2 switchport
Name: Et0/2
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
```

Gambar 19. Teknik mitigasi dengan menggunakan mode *switchport access* dan *switchport nonegotiate*

```
Gedung_A#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Gedung_A(config)#int e0/2
Gedung_A(config-if)#spanning-tree guard root
Gedung_A(config-if)#
*Nov 21 02:29:00.406: %SPANTREE-2-ROOTGUARD_CONFIG_CHANGE: Root guard enabled on port Ethernet0/2.
Gedung_A(config-if)#end
Gedung_A#
*Nov 21 02:29:16.160: %SYS-5-CONFIG_I: Configured from console by console
Gedung_A#
*Nov 21 02:29:40.047: %SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port Ethernet0/2 on VLAN0001.
```

Gambar 20. Teknik mitigasi dengan menggunakan *root guard*

```
edung_A#conf t
nter configuration commands, one per line.  End with CNTL/Z.
edung_A(config)#int e0/2
edung_A(config-if)#spanning-tree bpduguard enable
edung_A(config-if)#ex
edung_A(config)#errdisable recovery cause bpduguard
edung_A(config)#errdisable recovery interval 30
edung_A(config)#
Nov 21 02:50:47.600: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port Et0/2 with BPDU Guard enabled. Disab
ng port.
edung_A(config)#
Nov 21 02:50:47.600: %PM-4-ERR_DISABLE: bpduguard error detected on Et0/2, putting Et0/2 in err-disable stat
Nov 21 02:50:48.603: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2, changed state to down
edung_A(config)#
Nov 21 02:50:49.605: %LINK-3-UPDOWN: Interface Ethernet0/2, changed state to down
edung_A(config)#
Nov 21 02:51:17.594: %PM-4-ERR_RECOVER: Attempting to recover from bpduguard err-disable state on Et0/2
Nov 21 02:51:17.685: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port Et0/2 with BPDU Guard enabled. Disab
ng port.
```

Gambar 21. Teknik mitigasi dengan menggunakan *BPDU guard*.

```
Gedung_A#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Gedung_A(config)#int e0/2
Gedung_A(config-if)#spanning-tree bpdufilter enable
Gedung_A(config-if)#end
Gedung_A#s
*Nov 21 02:56:41.752: %SYS-5-CONFIG_I: Configured from console by console
Gedung_A#sh spanning-tree vlan 1 int e0/2 detail | include filter
   Bpdu filter is enabled
Gedung_A#sh spanning-tree vlan 1 int e0/2 detail
 Port 3 (Ethernet0/2) of VLAN0001 is designated forwarding
   Port path cost 100, Port priority 128, Port Identifier 128.3.
   Designated root has priority 32769, address aabb.cc00.0500
   Designated bridge has priority 32769, address aabb.cc00.0500
   Designated port id is 128.3, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is shared by default
   Bpdu filter is enabled
   BPDU: sent 24, received 0
```

Gambar 22. Teknik mitigasi dengan menggunakan *BPDU Filtering*.

```
Gedung_A#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Gedung_A(config)#mls rate-limit layer2 pdu 200 20
```

Gambar 23. Teknik mitigasi dengan menggunakan *layer 2 PDU rate limiter*.

d. Teknik mitigasi serangan *spanning tree protocol attack* yaitu:
   a) *Root Guard*
      Root guard berfungsi untuk memproteksi *switch* lainnya yang ingin menjadi *root* yang baru dengan cara tidak mengaktifkan *interface* pada *switch* lainnya. Teknik mitigasi serangan *spanning tree protocol attack* menggunakan *root guard* dapat dilihat pada Gambar 20.
   b) *BPDU Guard*
      BPDU Guard berfungsi untuk memproteksi port yang telah aktif agar tidak terjadi pengiriman konfigurasi *bpdu* yang baru. Teknik mitigasi serangan *spanning tree protocol attack* menggunakan *bpdu guard* dapat dilihat pada Gambar 21.
   d) *BPDU Filtering*
      BPDU filtering berfungsi untuk memproteksi *port* yang telah aktif agar tidak terjadi pengiriman maupun penerimaan konfigurasi *bpdu* yang baru. Teknik mitigasi serangan *spanning tree protocol attack* menggunakan *bpdu filtering* dapat dilihat pada Gambar 22.
   e) *Layer 2 PDU Rate Limiter*
      Layer 2 PDU rate limiter berfungsi untuk membatasi jumlah paket pada *layer 2 pdu* protokol termasuk (*BPDUs*, *DTP*, *Port Aggregation Protocol [PagP]*, *CDP*, *STP*, dan *VTP* paket) yang ditujukan untuk *supervisor engine's processor* pada *CPU*. Namun teknik mitigasi *layer 2 pdu rate limiter* hanya dapat digunakan untuk jenis *switch catalyst 6500*. Teknik mitigasi serangan *spanning tree protocol attack* menggunakan *layer 2 pdu rate limiter* dapat dilihat pada Gambar 23.

Untuk mengatasi serangan *spanning tree protocol attack* dengan metode *taking over root bridge* menggunakan teknik mitigasi *root guard* dan *BPDU guard* sedangkan metode serangan *DoS using flood config BPDU* dapat diatasi menggunakan teknik *BPDU guard*, *BPDU filtering*, dan *layer 2 PDU rate limiter*.

5. Penutup

Berdasarkan hasil penelitian yang dilakukan, menghasilkan beberapa kesimpulan yaitu implementasi *VLAN* dan *spanning tree protocol* yang dilakukan menggunakan *GNS 3* menunjukkan bahwa konsep *VLAN* dan *spanning tree protocol* sangat efektif digunakan apabila sebuah organisasi atau perusahaan memiliki topologi jaringan yang bersifat kompleks dan berpotensi mengalami *redundant link*.

Jaringan *VLAN* dan *spanning tree protocol* masih memiliki kelemahan dari segi aspek kemananan. Serangan yang dapat mengancam jaringan *VLAN* dan *spanning tree protocol* yaitu *VLAN hopping* dan *spanning tree protocol attack*. Namun serangan *VLAN hopping* dan *spanning tree protocol attack* mampu diatasi dengan menerapkan beberapa teknik mitigasi pada jaringan *VLAN* dan *spanning tree protocol*.

Setelah melakukan implementasi *VLAN* dan *spanning tree protocol* serta pengujian sistem keamanannya menggunakan aplikasi *GNS 3* dan *yersinia* dapat diketahui bahwa penggunaan aplikasi *GNS 3* dapat mempermudah untuk membuat desain perancangan jaringan dan lebih menggambarkan kondisi secara *real* dalam melakukan konfigurasi perangkat jaringan sedangkan aplikasi *yersinia* dapat digunakan untuk melakukan simulasi dan analisis serangan pada beberapa jenis protokol jaringan *layer 2*.

6. Daftar Pustaka

[1] Ali, S.Y. (2015). Implementation of Virtual Local Area Network using Network Simulator, *International Journal of Scientific Research Engineering & Technology*, 4(10), 1060-1065.

[2] Bajpai, A. & Singh, I. (2016). Implementing Secured LAN Environment: Case Study, *International Journal*

of Computer Science and Technology, 7(2), 41-51.

[3] Efendi, R. (2013). Percepatan Konvergensi dan Pencegahan Frame Loop Pada Virtual Local Area Network Dengan Memanfaatkan Rapid Spanning Tree Protocol, *Jurnal Teknologi Informasi dan Komunikasi*, 4(1), 45-51.

[4] Lewis, W. (2008). *LAN Switching Wireless: CCNA Exploration Companion Guide*, Cisco Press, Indianapolis.

[5] Prasetyo, E. (2014). Perancangan VLAN (Virtual Local Area Network) untuk Manajemen IP Address pada Politeknik Sekayu, *Jurnal Teknik Informatika Politeknik Sekayu*. 1(1), 10-23.

[6] Supriyono, H., Widjaya, J.A. & Supardi, A. (2013). Penerapan Jaringan Virtual Private Network Untuk Keamanan Komunikasi Data Bagi PT. Mega Tirta Alami, *Jurnal WARTA*, 16(2), 88-101.

[7] Tambe, S.S. (2015). Understanding Virtual Local Area Networks, *International Journal of Engineering Trends and Technology*, 25(4), 174-176.

[8] Tulloh, R., Negara, R.M. & Hidayat, A.N. (2015). Simulasi Virtual Local Area Network (VLAN) Berbasis Software Defined Network (SDN) Menggunakan POX Controller, *Jurnal Infotel*, 7(2), 130-136.

[9] Vyncke, E. & Paggen, C. (2007). *LAN Switch Security: What Hackers Know About Your Switches*, Cisco Press, Indianapolis.

[10] Wiguna, A.W., Herlawati & Santoso, B. (2013). Penerapan Spanning Tree Protocol Terhadap Wide Area Network (WAN) Pada PT. Duta Lestari Sentratama Jakarta, *Jurnal Techno Nusa Mandiri*, 9(1),