ICM Indonesian Journal of Computing and Modeling

e-ISSN : 2598-9421

Model Keamanan pada *Virtual Local Area Network* (VLAN) untuk Mengatasi DHCP *Rogue*

Teguh Indra Bayu [1], Nurhanif[2]

[1,2] Fakultas Teknologi Informasi, Program Studi Teknik Informatika Universitas Kristen Satya Wacana Salatiga

Keamanan jaringan di era ini sangat dibutuhkan, dibalik kemudahan dalam mengakses informasi terdapat pula banyak ancaman. Dengan aplikasi GNS3 pengguna dapat membuat simulasi jaringan dengan perangkat yang dibutuhkan seperti aslinya serta dalam perangkat dapat dikonfigurasi langsung. Pada simulasi ini membuat Perancangan Keamanan pada Virtual Local Area Network (VLAN) untuk Mengatasi DHCP Rogue dengan penggunaan ACL solution serta trusted-servers yang menjadi salah satu cara agar menjadikan jaringan tersebut tetap aman dan stabil. Dari hasil penelitian yang dilakukan GNS3 mampu Merancangan Keamanan Virtual Local Area Network (VLAN) untuk Mengatasi DHCP Rogue dengan memasukkan ACL solution serta fitur trusted-servers ke dalam switch ExtremeXOS.

Keywords : GNS3, VLAN, ACL solution, trusted-servers, switch ExtremeXOS.

I. PENDAHULUAN

Peran DHCP pada sebuah jaringan sangatlah penting sekarang ini karena permintaan *client* yang banyak penggunaan DHCP sangat membantu untuk memberikan alamat IP (*internet protocol*) secara otomatis kepada *client*, ketika memanfaatkan DHCP berarti IP *Address* secara lengkap akan diberikan kepada *client* secara otomatis, pemberian IP secara otomatis ini sering juga disebut dengan IP *Dinamic*. Jadi dengan DHCP IP yang diberikan merupakan IP *Dinamic*, sedangkan apabila IP diberikan secara manual disebut IP *Statis.*

Pada saat DHCP *client* dihidupkan, komputer *client* tersebut melakukan *request* ke DHCP *Server* untuk mendapatkan IP *address*. DHCP menjawab dengan memberikan nomor IP yang ada di *database* DHCP *Server*. DHCP *Server* setelah memberikan nomor IP, *server* meminjamkan (*lease*) nomor IP yang ada ke DHCP *Client* dan mencoret nomor IP tersebut dari daftar *pool*. Nomor IP diberikan bersama dengan *subnet mask* dan *default gateway*. Jika tidak ada lagi nomor IP yang dapat diberikan, maka *client* tidak dapat menginisialisasi TCP/IP, dengan sendirinya tidak dapat tersambung pada jaringan tersebut.

ExtremeXOS merupakan sebuah perangkat lunak atau sistem operasi jaringan yang digunakan dalam *switch extreme* yang dimana *switch* tersebut mampu menerima informasi dari berbagai sumber yang tersambung dengannya, kemudian menyalurkan informasi tersebut kepada pihak yang membutuhkannya saja. Tetapi selain itu *switch* juga memiliki fungsi lainnya yang berkaitan dengan area komunikasinya di layer kedua. ExtremeXOS adalah perangkat lunak atau sistem operasi jaringan yang digunakan dalam *switch* jaringan *Extreme Networks* yang lebih baru. Ini adalah sistem operasi generasi kedua *Extreme Networks* setelah sistem operasi *ExtremeWare* berbasis *VxWorks*[1].

Virtual Local Area Network (VLAN) adalah suatu model jaringan yang tidak terbatas pada lokasi fisik seperti *Local Area Network* (LAN). Hal ini mengakibatkan suatu jaringan dapat dikonfigurasi secara virtual tanpa harus mengikuti lokasi fisik peralatan. Dengan adanya VLAN dalam suatu jaringan, dapat membantu memudahkan pengaturan jaringan dan membuat jaringan lebih fleksibel karena konfigurasi jaringan dapat diubah tanpa memindahkan lokasi fisik *workstations*. VLAN diciptakan untuk menyediakan layanan *segmentasi* secara tradisional disediakan oleh *router* di konfigurasi LAN. VLAN menangani masalah-masalah seperti skalabilitas, keamanan, dan manajemen jaringan[2]. Penggunaan VLAN mampu membagi sebuah *broadcast* domain yang besar menjadi beberapa *broadcast* domain yang lebih kecil bekerja dengan cara melakukan pembagian jaringan secara logika ke dalam beberapa *subnet*.

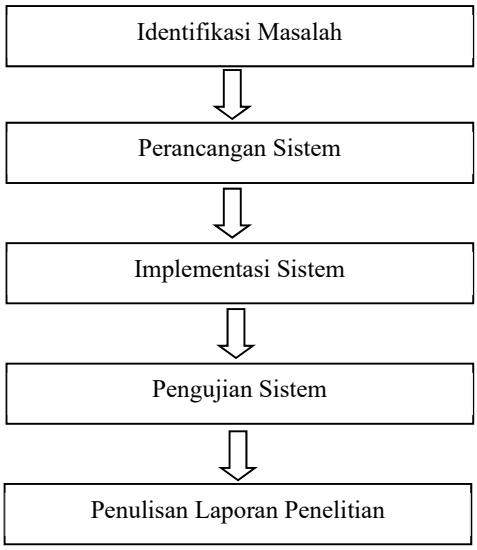
GNS3 (Graphical Network Simulator). GNS3 mampu mensimulasikan desain mekanisme keamanan VLAN yang memiliki kelebihan dapat disimulasikan beberapa perangkat jaringan yang saling terkoneksi. Desain mekanisme keamanan VLAN merupakan bagian dari sistem jaringan luas yang dalam mempelajarinya membutuhkan beberapa perangkat. Dengan adanya GNS3, maka kebutuhan untuk edukasi dibidang desain keamanan jaringan yang membutuhkan banyak pengeluaran sudah teratasi. Kedepannya diharapkan GNS3 merupakan satu-satunya kebutuhan sarana edukasi untuk kegiatan belajar mengajar dibidang jaringan karena untuk saat ini hanya GNS3 yang mampu mensimulasikan beberapa sistem operasi perangkat jaringan[3].

Penelitian ini dilakukan untuk mengetahui bagaimana proses pertukaran paket DHCP beserta parameter yang terkandung di dalamnya, sebelum adanya DHCP *Rogue*, setelah adanya DHCP *Rogue*, dan setelah adanya pencegahan terhadap DHCP *Rogue* di dalam sebuah jaringan.

Perancangan model keamanan dibuat dengan DHCP *server* utama dibangun dalam mikrotik dengan penggunaan VLAN, penggunaan ExtremeXOS untuk pencegahan DHCP *Rogue*, *Access Point* (AP) *router* yang difungsikan sebagai DHCP *Rogue*, dan sebuah *client* yang digunakan sebagai percobaan nantinya. Perancangan ini difokuskan pada pengamatan paket DHCP beserta parameter yang ada di dalamnya menggunakan *wireshark network protocol analyzer* yang bertujuan untuk menciptakan sistem kemanan jaringan berupa monitoring dan pencegahan terhadap DHCP *Rogue* dimana untuk menanggulangi ancaman tersebut salah satu caranya dengan membatasinya pada model OSI *layer* 2 yang ada di ExtremeXOS, dan diperlukan konfigurasi VLAN serta *access control list* (ACL), yang diharapkan dapat menjadi solusi agar jaringan stabil.

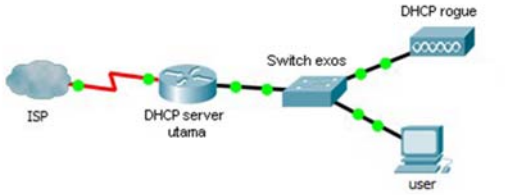
II. METODE PENELITIAN

Tahapan penelitian yang digunakan dalam membuat Perancangan Keamanan pada *Virtual Local Area Network* (VLAN) untuk Mengatasi DHCP *Rogue*, dapat dilihat pada Gambar 1.



Gambar 1 Tahapan Penelitian

Tahap-tahap dalam tahapan penelitian yang ada pada Gambar 1, dijelaskan sebagai berikut: Pada tahap Identifikasi Masalah: Syarat keamanan jaringan yaitu yang pertama sistem keamanan jaringan harus mampu melindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak. Kedua sistem pendeteksi penyusup harus mampu mendeteksi berbagai macam serangan dan harus mampu mengambil tindakan pada saat serangan itu terjadi. Ketiga sistem harus memiliki interaktivitas dengan administrator pada saat administrator tidak sedang mengadministrasi sistemnya. Permasalahan jaringan yang dijumpai yaitu ketika sudah terdapat DHCP dari *server* namun terdapat lagi DHCP *Rogue* yang berasal dari perangkat lain kemudian jika ada *client* yang terhubung dengan jaringan tersebut dimungkinkan terjadinya penyadapan, karena DHCP *Rogue* akan bisa melakukan setting terhadap IP *Default Gateway* sehingga akan dimungkinkan komunikasi disadap dari komputer *Default Gateway*. Perancangan sistem: Pada tahap ini akan dilakukan analisis permasalahan dan kebutuhan dalam perancangan yang berkaitan dengan keefektifan suatu keamanan yang nantinya akan diterapkan. Perancangan ini dimulai dari bagaimana skema topologi jaringan yang akan diterapkan dalam perancangan keamanan pada *Virtual Local Area Network* (VLAN) untuk mengatasi DHCP *Rogue*.



Gambar 2. Topologi Jaringan

Dapat dilihat pada gambar 2 sumber internet yang terhubung ke *router* DHCP *server* utama, dalam *router server* utama tersebut akan dikonfigurasi vlan yang nantinya akan terhubung ke *switch exos*. Pada *switch exos* akan di konfigurasi vlan yang sudah tertera dalam *router* DHCP *server* utama yang kemudian akan memasukkan *script* ACL s*olution* untuk keamanan VLAN serta mencegah agar tidak meracuni jaringan yang lainnya, serta akan dilakukan perintah *trusted server* agar dia hanya bis meminta DHCP ke DHCP *server*. *Port* untuk DHCP *rogue* dibuat *mode acccess* karena dipakai untuk ke arah *end-device.* Lalu *port* yang lainnya menggunakan *port mode trunk* yang nantinya akan bisa menghubungkan antara beberapa VLAN antar *switch*, *switch* dengan *router* maupun untuk mengangkut VLAN antar *switch* atau *router*. Lalu DHCP *rogue* dari perangkat *access point* TP-link yang disetting akan memberikan IP *address* dalam satu jaringan, namun alamat IP tersebut harus dibedakan dengan pemberian alamat IP dari vlan *router* agar nantinya dapat dilihat dari user yang terkoneksi ke dalam *switch exos* tersebut mendapatkan *dynamic* IP dari vlan *router* atau *access point.* Terakhir yaitu *user* yang akan mencoba terkoneksi dengan *switch* ketika *access point* juga terhubung didalamnya. Apakah *user* masih mendapat IP dari vlan *router* atau bahkan sebaliknya mendapat IP dari *access point*. Pada tahap ini juga akan dilakukan monitoring menggunakan *Wireshark Network Protocol Analyzer* untuk mengetahui sumber alamat IP yang didapatkan. Implementasi sistem: Pada tahap ini menggunakan simulasi GNS3 dengan cara mulai mencari *image router*, *switch exsos*, serta *access point* yang akan diinstall pada GNS3. Dalam konfigurasi *router* di buat daftar vlan seperti Tabel 1.

Tabel 1. Konfigurasi router

Name	Type	VLAN ID	Interface
ether4-vlan100	VLAN	100	*ether4*
ether4-vlan200	VLAN	200	*ether4*
ether4-vlan300	VLAN	300	*ether4*
ether4-vlan400	VLAN	400	*ether4*
ether4-vlan500	VLAN	500	*ether4*

```
1.  exos X440x. 1# create vlan vlan100
```

```
2. exos X440x. 2# configure vlan “vlan100” tag
   100
3. exos X440x. 3# configure vlan “vlan100”
   ipaddress10.10.10.0/24
```

Kode Program 1 Konfigurasi vlan

Dalam kode program 1. Dijelaskan pembuatan nama vlan, ID, serta konfigurasi IP *address* yang nantinya akan dibagi ke dalam 5 vlan. Pemberian IP *address* ke suatu port harus dibuat terlebih dahulu vlan untuk port tersebut, lalu konfigurasi IP address-nya baru kemudian port tersebut di add ke vlan entah sebagai *tagged* atau *untagged*. Pembuatan vlan mulai dari vlan100, vlan200, vlan300, vlan400, dan vlan 500. Nama dari vlan tersebut disamakan dengan konfigurasi *router* agar dapat terhubung, konfigurasi ini akan sukses ketika selesai penulisan kode program di enter akan muncul tulisan IP interface for VLAN data *has been created*.

Setelah konfigurasi pembuatan vlan maka selanjutnya akan dibuat untuk pengaturan *tagged* yang digunakan hanya untuk *port* yang diset melewatkan lebih dari satu VLAN. Lalu ketika *port* tersebut hanya masuk ke dalam satu VLAN maka set *untagged* pada *port* VLAN tersebut. Disini port 1 switch diset *tagged* untuk menghubungkan router dengan switch lalu yang lainnya akan di buat *untagged.* Lalu untuk mengetahui vlan tersebut telah dibuat dapat ditampilkan dengan penggunaan perintah pada kode program 2.

```
1. exos X440x. 16# show vlan
```

Kode Program 2 menampilkan konfigurasi vlan

Tabel 2. Konfigurasi *switch* ExtremeXOS

Name	VID	Protocol Addr	Ports Active/Total	Virtual rouuter
Mgmt	4095	192.168.0.1/24	0 /1	VR-Mgmt
vlan100	100	10.10.10.0/24	0 /5	VR-Default
vlan200	200	10.10.20.0/24	0 /5	VR-Default
vlan300	300	10.10.30.0/24	0 /5	VR-Default
vlan400	400	10.10.40.0/24	0 /5	VR-Default
vlan500	500	10.10.50.0/24	0 /4	VR-Default

Dalam tabel 2 terlihat bahwa vlan 100 diatur dengan alamat IP yaitu 10.10.10.0/24 serta dalam *router* utama vlan tersebut juga sudah dibuat pengaturan *range* IP sehingga ketika *user* mendapat alamat IP yang benar dari *router* utama maka akan didapatkan alamat DHCP *server* antara IP 10.10.10.2 sampai 10.10.10.254. Kemudian lanjut konfigurasi untuk *access point* TP-link sebagai DHCP *Rogue* yaitu dengan masuk pengaturan DHCP *server* yang kemudian diberi alamat IP 192.168.0.1/24 yang nantinya *user* akan mendapat *dynamic* IP mulai dari 192.168.0.2 sampai 192.168.0.254.

Pengujian sistem: Tahap pengujian sistem dilakukan percobaan melalui simulasi menggunakan GNS3 yang sudah dikonfigurasi sehingga akan diketahui apakah *client* nantinya akan mendapat IP dari *router* (DHCP *server* utama) atau mendapatkan IP dari *Access Point* (DHCP *Rogue*) tersebut. Penulisan Laporan Penelitian: Tahap akhir dari penelitian ini yaitu menulis laporan mulai dari tahap awal sampai tahap terakhir perancangan keamanan pada *Virtual Local Area Network* (VLAN) untuk Mengatasi DHCP *Rogue*.

III. HASIL DAN PEMBAHASAN

Penelitian yang berjudul Rancangan Bangunan VLAN untuk Segmentasi Jaringan pada *Cyber Campus Laboratorium* Universitas Stikubank. Membahas mengenai penelitian VLAN pada jaringan *cyber campus laboratory* agar peralatan yang ada dapat dioptimasi untuk memberikan manajemen jaringan dengan mudah serta penggunakan untuk segmentasi jaringan dalam peralatan *switch* yang dapat menghubungkan semua VLAN[4].

Pada penelitian yang berjudul Analisis dan Implementasi *Virtual Local Area Network* (VLAN) untuk Optimalisasi Keamanan Jaringan *Local Area Network*. Berhasil membuat perancangan VLAN yang dapat dikelompokkan berdasarkan fungsi dan kebutuhannya, serta hasil rancangan VLAN yang dibuat dapat meningkatkan *response time* dengan aplikasi *net tool*. Dan untuk meningkatkan keamanan jaringan lokal menggunakan penerapan VLAN dengan metode *access list* [5].

Khan, Alshomrani, dan Qamar melakukan penelitian pada jaringan *client-server* dengan menggunakan *Wireshark Network Protocol Analyzer* tentang proses pertukaran paket DHCP yang terjadi pada DHCP *server* dengan DHCP *client*. Penelitian menyimpulkan bahwa proses pembentukan komunikasi antara DHCP *server* dengan DHCP *client* menggunakan empat paket DHCP yaitu DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, dan DHCPACK. Penelitian ini juga menambahkan penjelasan tentang adanya celah keamanan pada konsep DHCP yang menimbulkan ancaman serius terhadap jaringan dalam bentuk DHCP *spoofing* yaitu penyerang yang dengan maksud jahat datang di tengah-tengah komunikasi antara dua sistem, dimana penyerang dapat mendengar maupun berpartisipasi aktif di dalamnya[6].

Acuan penelitian yang terakhir adalah penelitian yang dilakukan oleh Prismana putra., (2015) berjudul Simulasi Jaringan Komputer *Multi Device* Menggunakan GNS3 menjelaskan bahwa mahalnya biaya untuk sebuah perangkat jaringan seperti *router* dan *switch* dapat dilakukan alternatif untuk mempelajari perangkat tersebut dengan memanfaatkan aplikasi simulasi jaringan yang bernama Cisco Packet Treacer. Karena keterbatasan penggunaan Cisco Packet Tracer itulah hadir sebuah komunitas berusaha mengembangkan aplikasi *open source* untuk simulasi jaringan, lahirlah GNS3 (Graphical Network Simulator 3). Dengan aplikasi GNS3 pengguna dapat membuat topologi jaringan seperti topologi *mesh* juga dapat dikonfigurasi menggunakan *routing* OSPF sebagai media pembelajaran dalam bidang jaringan komputer. Hasil penelitian yang dilakukan GNS3 mampu mensimulasikan jaringan *multi device* dengan baik dapat melakukan hubungan antara GNS3 pada dua komputer berbeda dan juga dapat dikonfigurasi untuk tersambung di jaringan internet[3].

Berdasarkan penelitian yang pernah ada terkait dengan mekanisme keamanan *Virtual Local Area Network* (VLAN) untuk mengatasi DHCP Rogue, serta penggunaan simulasi jaringan komputer menggunakan GNS3 (Graphical Network Simulator 3) maka akan dilakukan penelitian yang membahas mengenai perancangan keamanan pada *Virtual Local Area Network* (VLAN) untuk mengatasi DHCP *Rogue*. Penelitian difokuskan terhadap perancangan keamanan VLAN serta dikembangkan pemecahan masalah DHCP *Rogue* menggunakan ACL *solution*.

Virtual Local Area Network (VLAN) merupakan suatu kumpulan perangkat dalam *Local Area Network* (LAN) yang dikonfigurasi sehingga dapat berkomunikasi seolah-olah dihubungkan dengan kabel padahal berada pada segment yang berbeda dalam LAN. Sebuah jaringan LAN dapat dikatakan sebagai sebuah *broadcast* domain dan VLAN berfungsi untuk membagi *broadcast* domain yang semula lebih besar menjadi dua atau lebih *broadcast* domain yang lebih kecil. VLAN dapat dibuat berdasarkan departemen, fungsi pekerjaan, dan lain-lain tanpa terpengaruh oleh lokasi fisik *host*. VLAN dapat meningkatkan kinerja jaringan secara keseluruhan[7].

Keuntungan *Virtual Local Area Network* (VLAN) Menurut Hucaby (2010), beberapa tujuan utama dari implementasi VLAN pada jaringan antara lain[8] :

a. *Security*
Implementasi VLAN dalam suatu perusahaan memungkinkan terkontrolnya keamanan data dalam tiap-tiap departemen karena berada dalam satu *broadcast* domain yang sama.

b. *Cost Reduction*
Mengurangi biaya yang akan dikeluarkan apabila terdapat penambahan jaringan dan lebih efisien dalam pemakaian *bandwidth* dan *uplinks*.

c. *Higher Performance*
Memisahkan jaringan *layer* 2 ke dalam berbagai *logical workgroup* (*broadcast* domain) yang dapat mengurangi *traffic* data yang tidak diperlukan dan meningkatkan *performance* jaringan.

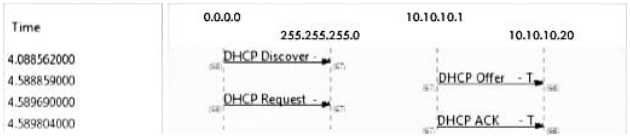
d. *Broadcast Storm Mitigation*
Penerapan VLAN dapat mengurangi jumlah *device* yang turut serta dalam sebuah *broadcast storm*.

e. *Improved IT Staff Efficiency*
Penerapan VLAN memudahkan pengaturan jaringan dan konfigurasi VLAN dapat langsung tersebar apabila ada sebuah *switch* baru yang terhubung ke dalam jaringan tersebut.

Extreme Networks telah menciptakan ExtremeXOS modular *Operating System* (OS) untuk jaringan dengan kinerja tinggi dan *extensible* tinggi. Arsitektur ketersediaan tinggi ExtremeXOS dengan protokol EAPS membantu mengurangi *downtime* jaringan untuk kelangsungan bisnis dan akses ke aplikasi *mission-critical* seperti CRM, gudang data dan VoIP untuk jaringan operator dan suara tingkat. Kemampuan keamanan terpasang menyediakan kontrol akses jaringan yang terintegrasi dengan pemeriksaan integritas titik akhir, manajemen identitas, dan perlindungan untuk kontrol jaringan dan bidang manajemen.

ExtremeXOS dirancang dari bawah ke atas untuk memenuhi kebutuhan *cloud* besar dan pusat data pribadi, penyedia layanan, jaringan perusahaan cerdas, terkonvergensi, dan segala sesuatu di antaranya. Ini menyediakan kinerja tinggi dan fitur kaya yang dibutuhkan oleh lingkungan yang beragam ini. Berdasarkan arsitektur dan protokol yang tangguh, ExtremeXOS mendukung virtualisasi jaringan dan kemampuan SDN berbasis standar seperti *gateway* VXLAN, *OpenFlow*, dan *OpenStack Cloud Orchestration.* ExtremeXOS mendukung kebijakan berbasis peran yang komprehensif. Fitur ini menetapkan kerangka aman di mana setiap pengguna menerima seperangkat aturan yang telah ditentukan untuk mengakses jaringan berdasarkan peran mereka dalam organisasi. Kebijakan ditentukan dan dikelola secara terpusat oleh pusat kontrol, sistem manajemen *pane-of-glass* tunggal yang secara otomatis mendorong kebijakan ke titik akses dan *switch extreme networks*. Ini secara signifikan menyederhanakan tugas IT untuk mengelola jaringan yang aman dan meningkatkan efisiensi operasional. Diatas segalanya, ia menyediakan seperangkat fitur keamanan komprehensif yang melindungi aplikasi, lalu lintas, dan infrastruktur anda secara proaktif[9].

Pertukaran DHCP *packets* yang terjadi antara DHCP *server* utama dengan *user* pada kondisi sebelum adanya DHCP *Rogue* dapat dilihat dalam bentuk grafik yang dibuat menggunakan flow graph pada *wireshark*. Adapun grafik dapat dilihat pada gambar 3.



Gambar 3. Flow Graph DHCP Packets pada user sebelum adanya DHCP *Rogue*

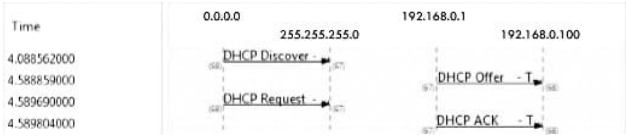
Pertukaran DHCP packets yang terjadi masih berjalan normal, dengan indikasi *user* mendapatkan paket DHCPACK yang sekaligus mendapatkan konfigurasi alamat IP yang berasal dari DHCP *server* utama yaitu berasal dari alamat IP 10.10.10.1. Pada percobaan awal mendapatkan hasil bahwa *user* mendapatkan IP 10.10.10.20 yang merupakan *dynamic* yang diberikan dari vlan100 hal ini dibuktikan pada gambar 4.

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a178:5ff5:9504:afce%13
   IPv4 Address. . . . . . . . . . . : 10.10.10.20
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.1
```

Gambar 4. *Dynamic* IP dari vlan Server DHCP utama

User mendapat *dynamic* IP dari vlan server DHCP utama yang telah dibuat sebelumnya yang berarti pembuatan vlan sebelumnya berhasil di konfigurasikan dengan *router* atau DHCP *server* utama. Lanjut percobaan kedua ketika *access point* yang sudah di konfigurasi DHCP server tadi dihubungkan dengan *switch* melalui *port* vlan, Pada percobaan kedua pertukaran DHCP *packets* terjadi antara DHCP *Rogue* dengan *user* yang dapat dilihat dalam bentuk grafik, dibuat menggunakan flow graph pada *wireshark.* Adapun grafik dapat dilihat pada gambar 5.



Gambar 5. Flow Graph DHCP Packets pada user setelah adanya DHCP *Rogue*

Pertukaran DHCP *packets* yang terjadi yaitu *user* mendapatkan paket DHCPACK yang sekaligus mendapatkan konfigurasi alamat IP yang berasal dari DHCP *Rogue* yaitu berasal dari alamat IP 192.168.0.1. Pada percobaan kedua mendapatkan hasil bahwa *user* mendapatkan IP 192.168.0.100 yang merupakan *dynamic* yang diberikan dari DHCP *Rogue* hal ini dibuktikan pada gambar 6.

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a178:5ff5:9504:afce%13
   IPv4 Address. . . . . . . . . . . : 192.168.0.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
```

Gambar 6. Dynamic IP dari access point

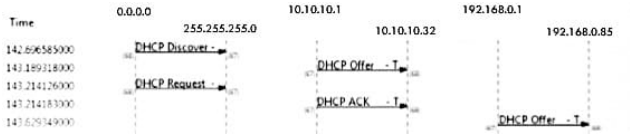
User mendapat *dynamic* IP dari DHCP *Rogue* yang sudah di konfigurasi dapat memberikan DHCP tadi, disini terbukti bahwa ketika terdapat perangkat tambahan yang terhubung dengan *switch* ExtremeXOS maka jaringan di dalamnya akan mengalami gangguan atau bahkan meracuni jaringan yang lainnya. Disini dapat dimungkinkan akan terjadinya penyadapan, karena DHCP *Rogue* akan bisa melakukan setting terhadap IP Default Gateway sehingga akan dimungkinkan komunikasi disadap dari komputer Default Gateway. Langkah selanjutnya yaitu mencoba mengaktifkan ACL *solution* yang sudah dibuat pada *switch* ExtremeXOS tadi sehingga bisa mencegah terjadinya pergantian *dynamic* IP walaupun ada perangkat TP-link atau DHCP *Rogue* yang terhubung ke *switch* ExtremeXOS tersebut.

```
1.  entry dhcp_whitelist {
2.  if {destination-address 10.10.10.0/24;
3.  protocol udp;
4.  source-port 68-69;
5.  } then {
6.  permit;}}
7.  entry dhcp_rogue {
8.  if {destination-address 192.168.0.1/24;
9.  protocol udp;
10. source-port 68-69;
11. } then {
12. deny;}}
```

Kode Program 3 *Sricpt* ACL

Dalam kode program 3 terdapat *script* ACL yang dikonfigurasikan pada *switch* ExtremeXOS ketika terdapat *user* yang terkoneksi ke dalam *switch* ExtremeXOS dan masuk ke dalam *port* vlan maka *user* akan mendapat alamat IP DHCP dari vlan tersebut,namun ketika terdapat DHCP lagi dari sumber *acces point* TP-link yang nantinya menjadi DHCP *Rogue* maka *switch* ExtremeXOS akan menyangkal. Dimungkinkan terjadinya penyadapan, karena DHCP Rogue akan bisa melakukan setting terhadap IP Default Gateway sehingga akan dimungkinkan komunikasi disadap dari komputer Default Gateway.

Setelah script ACL tersebut dijalankan, melakukan percobaan kembali dengan langkah seperti yang digunakan sebelumnya yaitu menghubungkan *access point* dengan *switch* ExtremeXOS yang sudah di konfigurasi kembali. Apakah masih mendapat *dynamic* IP dari *access point* atau sudah terganti degan *dynamic* IP dari vlan yang dibuat. Pertukaran DHCP packet dapat dilihat dalam bentuk grafik menggukan flow graph pada gambar 7.



Gambar 7. Flow Graph DHCP Packets pada user setelah script ACL dijalankan.

Pada pengujian ini ketika DHCPDISCOVER dibroadcast oleh *user*, terdapat 2 balasan paket DHCPOFFER yang diberikan oleh DHCP *server* utama dan DHCP *Rogue*, akan tetapi balasan paket DHCPOFFER yang pertama berasal dari DHCP *server* utama dengan sumber alamat IP 10.10.10.1, sedangkan paket DHCPOFFER dari DHCP *Rogue* dengan sumber alamat IP 192.168.0.1 berada pada posisi kedua, sehingga *user* memproses lebih lanjut paket DHCPOFFER yang pertama diterima sampai memperoleh paket DHCPACK yang berisi konfigurasi alamat IP DHCP dari DHCP *server* utama, sedangkan DHCPOFFER dari DHCP *Rogue* diabaikan.

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a178:5ff5:9504:afce%13
   IPv4 Address. . . . . . . . . . . : 10.10.10.32
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.1
```

Gambar 8. *Dynamic* IP setelah *script* ACL dijalankan

Terbukti pada gambar 8 setelah *script* ACL di konfigurasi pada s*witch* ExtremeXOS, ketika *user* terhubung dengan *switch* maka akan meminta *dynamic* IP kepada *switch* yang telah membaca *script* perintah ketika *request* ke alamat yang aktif yaitu 10.10.10.0/24 maka akan disetujui dan mendapat IP antara 10.10.10.2 sampai 10.10.10.254 namun akan menyangkal *dynamic* IP dari 192.168.0.1 yang berasal dari DHCP *Rougue* tersebut dan tetap mendapatkan *dynamic* IP dari DHCP *server* utama yang telah dibuat. Langkah terakhir dari pengujian ini dengan memanfaatkan fitur trusted-servers dengan melakukan perintah kode program 4.

```
1.  exos X440x. 16# configure trusted-servers
    vlan100 add server 10.10.10.0 trust-for
    dhcp-server
```

Kode Program 4 perintah tusted-servers

Dengan perintah ini maka DHCP *rogue* tidak bisa membalas pesan permintaan DHCP karena *client* hanya bisa meminta DHCP ke DHCP *server*. Perintah ini dibuat ketika DHCP *rogue* berada pada range alamat 10.10.10.0/24 maka penggunaan ACL s*olution* akan tidak efektif. Setelah melakukan beberapa kali percobaan menggunakan konfigurasi ExtremeXOS maka dibuatkah tabel simulasi dan hasil pengujian akhir pada tabel 3.

Tabel 3. Simulasi dan Pengujian

Network/IP DHCP *rogue*	ExtremeXOS config	Hasil
192.168.0.0/24	ACL *solution*	DHCP *rogue* berhasil ditangani
192.168.0.0/24	Trusted-servers	DHCP *rogue* berhasil ditangani
10.10.10.0/24	ACL *solution*	*Service* DHCP menjadi tidak berfungsi
10.10.10.0/24	Trusted-servers	DHCP *rogue* berhasil ditangani

Dalam tabel simulasi dan hasil pengujian dapat ditarik kesimpulan ketika penggunaan DHCP *Rogue* menggunakaan ACL *solution* serta penggunaan trusted-servers keduanya dapat berhasil menangani DHCP *rogue* namun *service* DHCP menjadi tidak berfungsi ketika DHCP *Rogue* tersebut berada pada alamat IP yang sama dengan *server* utama yaitu range alamat 10.10.10.0/24 sebab penggunaan ACL *solution* yang dibuat hanya akan menyangkal IP dari range alamat 192.168.0.1/24 namun ketika menggunakan fitur atau perintah trustes-servers maka DHCP *rogue* tidak bisa membalas permintaan DHCP dan hanya bisa meminta DHCP ke DHCP *server.*

IV. SIMPULAN

Berdasarkan penelitian yang berjudul Perancangan Keamanan pada *Virtual Local Area Network* (VLAN) untuk mengatasi DHCP *Rogue* serta dari hasil dan pembahasan dapat ditarik kesimpulan bahwa Ketika DHCP *user* melakukan *booting* didalam jaringan DHCP yang terdapat DHCP *Rogue* aktif, maka akan terjadi 2 kemungkinan yaitu mendapatkan konfigurasi alamat IP yang benar dari DHCP *server* utama atau bisa jadi mendapatkan konfigurasi alamat IP yang salah dari DHCP *Rogue*. Lalu Ketika DHCP *user* mendapatkan alamat IP yang salah dari DHCP *Rogue* dengan alamat IP *gateway* ditujukan pada DHCP *Rogue* maka dimungkinkan terjadinya penyadapan, karena DHCP *Rogue* akan bisa melakukan setting terhadap IP Default Gateway sehingga akan dimungkinkan komunikasi disadap dari komputer Default Gateway. Dan yang terakhir yaitu penggunaan keamanan pada VLAN dengan ACL *solution* dan pemanfaatan petintah trusted-servers yang disimulasikan pada GNS3 dapat bekerja dengan semestinnya. Pada pengujian ACL *solution* ketika *switch* terdapat *acces point* TP-link yang juga dapat memberi IP DHCP maka *user* sudah tidak mendapat IP dari *acces point* melainkan dapat dari VLAN seperti yang di harapkan serta ketika terdapat DHCP *Rogue* dengan range sama seperti alamat server maka dapat diatasinya menggunakan perintah trusted-servers. Pada penelitian ini tidak terlepas dari kekurangan yang kemungkinan dapat di sempurnakan pada penelitian lain, ada beberapa saran yang bisa dijadikan sebagai tambahan seperti dalam melakukan pengujian langsung pada perangkat *switch* ExtremeXos, menambahkan *device* atau menggunakan *acces point* selain TP-link.

DAFTAR PUSTAKA

[1] Sistem Operasi Jaringan ExtremeXOS, Extreme Networks (13 November 2001). "Laporan kuartalan" . Formulir 10Q . US Securities and Exchange Commission

[2] Sofana Iwan. 2012. CISCO CCNA & JARINGAN KOMPUTER (Edisi Revisis). Bandung : Informatika. ISBN : 9786028758772.

[3] Prismana putra., 2015. Simulasi Jaringan Komputer Multi Device Dengan Menggunakan GNS3.

[4] Sutanto, Yulianton, Razaq., 2011. Rancangan Bangunan VLAN untuk Segmentasi Jaringan pada *Cyber Campus Laboratorium* Universitas Stikubank.

[5] Fuadi, K., 2016. Analisis dan Implementasi *Virtual Local Area Network* (VLAN) untuk Optimalisasi Keamanan Jaringan *Local Area Network.*

[6] Khan, M., Alshomrani, S., and Qamar, S., 2013, Investigation of DHCP Packets using Wireshark, International Journal of Computer Applications, Vol 63, No 4, 1-9.

[7] Odom,W., 2013. *Ccent/CCNA Icnd1 100-101 Official Cert Guide.* Indianapolis: Pearson Education.

[8] Hucaby, D. (2010). *CCNP SWITCH 642-813 Official Certification Guide*. Indianapolis: Cisco Press.

[9] ExtremeXOS. 2018. https://www.extremenetworks.com/resources/extremexos-operating-system/, Diakses pada 18 April 2018)