DESAIN KEAMANAN DHCP *SNOOPING* UNTUK MENGURANGI SERANGAN *LOCAL AREA NETWORK*(LAN)

Tamsir Ariyadi[1]
[1]Program Studi Teknik Komputer Fakultas Vokasi Universitas Bina Darma
Jl. A. Yani No. 3 Plaju Kode Pos 30264 Palembang Sumatera Selatan

e-mail: tamsirariyadi@binadarma.ac.id

Abstrak

Keamanan jaringan telah menjadi perhatian lebih karena pesatnya pertumbuhan dan perluasan Internet. Sementara ada beberapa cara untuk memberikan keamanan pada layer application, transport, atau network layers, *data link layer* (Layer 2) keamanan belum bisa diterapkan secara maksimal. protokol data *link layer* yang digunakan dalam *Local Area Network* (LAN) tidak dirancang dengan keamanan yang secara signature. *Dynamic Host Control Protocol (DHCP)* adalah salah satu jaringan yang paling banyak digunakan untuk konfigurasi host yang bekerja dalam data menghubungkan lapisan. DHCP rentan terhadap sejumlah serangan, seperti serangan DHCP *rogue* Server, serangan DHCP *Starvation*, dan serangan DHCP *Snooping*. Penelitian ini memperkenalkan skema baru yang disebut Desain Keamanan DHCP Snooping Untuk Mengurangi Serangan *Local Area Network*(LAN).

Kata kunci: Desain; DHCP Snooping; Keamanan Jaringan

Abstract

Network security has become a greater concern due to the rapid growth and expansion the Internet. While there are several ways to provide security at the application layer, transport, or network layers, the data link layer (Layer 2) of the security has not been implemented to its full potential. data link layer protocol used in Local Area Network (LAN) was not designed with security that is signature. Dynamic Host Control Protocol (DHCP) is one of the most widely used network for host configuration that works in data linking layers. DHCP is susceptible to a number of attacks, such as DHCP rogue Server attack, DHCP Starvation attack, and DHCP Snooping attacks. This study introduces a new scheme called Security Design DHCP Starvation attack is to reduce the Local Area Network (LAN).

Keywords*—Design, DHCP Snooping, Network Security*

I. PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi sangat dibutuhkan oleh semua orang untuk melakukan suatu pekerjaan ataupun pembelajaran agar pekerjaan dan pembelajaran tersebut menjadi lebih mudah apalagi teknologi informasi ini sangat sangat penting dalam segala aspek yang terhubung dengan teknologi informasi dan komunikasi. Dengan berkembangnya teknologi secara global seperti jaringan komputer, jaringan komputer adalah kumpulan dari beberapa komputer yang saling terhubung satu sama lain, sehingga memungkinkan penggunaan dapat saling bertukar informasi berupa suara, video, dan data pada jaringan yang sama. Jaringan komputer memerlukan keamanan jaringan komputer agar terhindar dari kejahatan *cyber* yang dilakukan orang yang tidak bertanggung jawab yang mengakibatkan kehilangan data.

Beberapa instansi menggunakan jaringan komputer untuk mendukung proses

pekerjaan, sehingga secara tidak langsung jaringan komputer sangat penting bagi pengguna internet. Dengan adanya jaringan komputer sebagai proses belajar mengajar ataupun untuk membantu pekerjaan, jaringan komputer memerlukan keamanan jaringan internet agar terhindar dari kejahataan *cyber* yang dilakukan oleh orang yang tidak bertanggung jawab.

Sehingga jaringan komputer sangat membutuhkan untuk saling berkomunikasi dan mengirim data. Jaringan komputer masih memiliki kekurangan karena keamanan yang belum baik maka sering terjadi kejahatan *cyber* dilakukan oleh orang yang tidak bertanggung jawab. Dengan keadaan tersebut makan jaringan komputer perlu meningkatkan keamanan jaringannya dengan menggunakan DHCP *snooping.* Dengan menggunakan DHCP snooping diharapkan dapat membantu keamanan jaringan internet dimana DHCP *snooping* hanya memberikan akses terhadap IP *address* atau MAC *address* yang telah terdaftar pada *router* tidak dapat mengakses ataupun masuk ke dalam jaringan tersebut.

Karena itu DHCP *snooping* merupakan solusi yang tepat untuk mengatasi masalah keamanan jaringan yang lebih baik. Dengan latar belakang tersebut, maka menarik untuk menguraikan dan membahas mengenai perancangan keamanan DHCP *snooping* pada jaringan komputer sebagai salah satu solusi untuk menangani masalah keamanan yang ada.

1.2 Perumusan Masalah

Sesuai dengan latar belakang yang telah dijelaskan di atas, maka perumusan masalah yang akan dikaji di dalam penelitian ini "Bagaimana mendesain Desain Keamanan DHCP Snooping Untuk Mengurangi Serangan Local Area Network (LAN)?".

1.3 Batasan Masalah

Agar permasalahan lebih terarah dan tidak menyimpang dari permasalahan yang diteliti, maka ditentukanlah batasan masalah sebagai berikut :

1. Desain keamanan jaringan dilakukan dengan simulasi jaringan komputer.
2. Desain keamanan di fokuskan pada keamanan *layer* 2 pada jaringan komputer.

1.4 Tujuan

Berdasarkan rumusan masalah yang penulis kaji maka penelitian ini bertujuan untuk mendesain keamanan jaringan pada *layer* 2 dengan menggunakan DHCP *snooping* agar jaringan komputer terhindar dari ancaman kejahatan *cyber*.

1.5 Manfaat

Adapun manfaat dari penelitian ini adalah sebagai berikut :

1. Manfaatnya agar terhindar dari pihak yang tidak bertanggung jawab, pencurian data baik itu pencurian *password* maupun pembajakan email dan lain-lain.
2. Manfaat bagi penulis yaitu dari penelitian ini diharapkan penyusun dapat lebih memahami dan menguasai serta dapat menerapkan pada dunia kerja yang sebenarnya. Sehingga dapat menambah ilmu pengetahuan dan wawasan berfikir, serta dapat mengembangkan ilmu pengetahuan.

II. METODE PENELITIAN

2.1 Topologi Jaringan LAN

Topologi yang digunakan dalam penelitian adalah topologi *star* dengan teknik pengkabelan *straight trough* dan konfigurasi IP secara static, serta penamaan komputer yang terkoordinir dengan baik, sehingga memudahkan admin atau petugas jaringan dalam me-monitor dan me-maintenance jaringan setiap kali terdapat kerusakan pada koneksi jaringan di komputer user.

Media transmisi yang digunakan dalam pada jaringan ini terdapat tiga media transmisi yaitu kabel *fiber* optik yang digunakan untuk menghubungkan ke *Internet service provider* (ISP) dan untuk menghubungkan *router mikrotik* ke *switch* ke setiap hub. Kemudian media transmisi kabel *unshielded twisted pair* (UTP) digunakan sebagai media transmisi hub ke

setiap komputer klien, yang ketiga yaitu media *transmisi wireless* digunakan untuk user yang menggunakan laptop atau perangkat yang mendukung wi-fi atau *hotspot*.

2.2 Simulasi DHCP *Server* dan DHCP *Snooping*

Tahapan selanjutnya adalah pembuatan prototipe sistem yang akan dibangun, sebagai simulasi dari implementasi, penulis membangun prototipe sistem ini pada lingkungan virtual, dengan menggunakan mesin virtual, sebagai replikasi dari sistem yang akan djalankan, karena mesin virtual memngkinkan suatu program yang sudah terdidikasi pada suatu sistem, dapat berjalan pada lingkup mesin virtual tersebut.

Software mesin virtual yang digunakan adalah Winbox yang support dengan beberapa platform Operating system (OS) yang digunakan dalam penelitian ini, dan berjalan dalam mesin virtual, dan komputer induk terlihat sebagai mesin virtual dapat bekerja sama secara optimal. Dalam implementasi DHCP *snooping* yang penulis deskripsikan mempunyai konsep LAN yang nantinya bisa di aplikasikan pada lingkup sebenarnya.

2.3 Desain

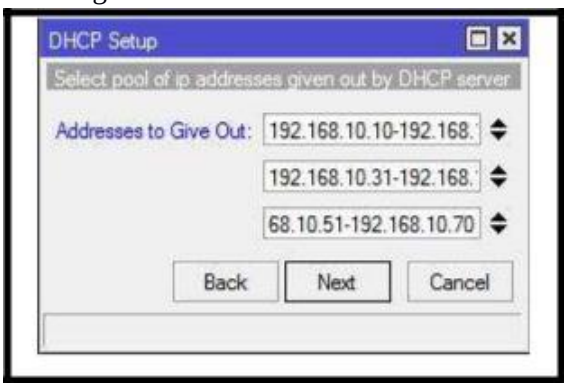
Penulis menginterprestasikan DHCP *snooping* dengan menggunakan perangkat yang sebenarnya seperti jaringan *local area networking* serta alat-alat pendukung seperti *switch*, PC *local area network* dan *router mikrotik* dalam perancangan DHCP *snooping* yaitu *server* dan *client* yang dapat di gambarkan sebagai bentuk perancangan topologi dan perancangan DHCP *snooping*.

2.4 Implementasi

Pada tahap implementasi adalah mengimplementasikan DHCP *server* pada router mikrotik dan mengimplementasikan DHCP *snooping* pada switch pada jaringan komputer.

Langkah-langkah yang dibutuhkan dalam konfigurasi DHCP *server d*an DHCP *snooping* untuk dapat berjalan, sebagai berikut :

1. Konfigurasi DHCP



Gambar 1 Konfigurasi DHCP Pada Winbox

2. Konfigurasi DHCP Snooping

Setelah pembuatan IP DHCP *server* telah selesai, peneliti melakukan konfigurasi DHCP *snooping* pada *switch*. Dengan menggunakan VLAN 1, dimana terdapat beberapa port yang digunakan dalam konfigurasi.

1. Konfigurasi IP *snooping trust*, dimana trust berfungsi mengamankan IP *address* agar terhindar dari IP *fake* atau *attacker*.

Gambar 2 Konfigurasi DHCP *Snooping Trust*

2. Konfigurasi ip snooping limit rate, dimana limit rate berfungsi menentukan beberapa user yang boleh masuk ke dalam jaringan.

Gambar 3 Konfigurasi DHCP *Snooping Limit Rate*

II. METODE PENELITIAN

2.1 Kajian Pustaka

2.1.1 Desain

Desain adalah kegiatan kreatif yang membawa pembaruan (Reswick,1965). Desain juga dapat merupakan pemecahan masalah dengan suatu target yang jelas (Archer, 1965).

2.1.2 Keamanan jaringan komputer

Keamanan Jaringan Komputer merupakan segala sesuatu yang berkaitan dengan perlindungan data dan pembatasan akses ke data tersebut. Tujuan utama dari keamanan jaringan adalah mengamankan aset-aset yang dianggap vital bagi kelangsungan hidup sebuah organisasi atau perusahaan. Aspek keamanan data dan jaringan melibatkan perencanaan untuk mengantisipasi masalah kegagalan daya listrik maupun hilangnya fasilitas-fasilitas fisik tertentu, karena sebab-sebab semisal terjadi kebakaran (Tittel, 2004:218).

2.1.3 Jaringan Komputer

Jaringan Komputer adalah sekelompok otonom yang saling berhubungan antara satu dengan yang lainnya menggunakan protokol komunikasi melalui meda komunikasi sehingga dapat saling berbagi informasi, program-program, penggunaan bersama perangkat keras seperti printer, *hardisk*, dan sebagainya. Selain itu jaringan komputer bisa diartikan sebagai kumpulan sejumlah terminal komunikasi yang berada di berbagai lokasi yang terdiri dari lebih satu komputer yang seling berhubungan (Wahana Komputer,2003:2).

2.1.4 Tujuan Jaringan Komputer

Tujuan dibangunnya suatu jaringan komputer adalah membawa informasi secara tepat dan tanpa adanya kesalahan dari sisi pengirim (*transmitter*), menuju ke sisi penerima (*receiver*) melalui media komunikasi (Wahana Komputer, 2003:2).

2.1.5 Manfaat Jaringan Komputer

Secara umum, jaringan komputer mempunyai beberapa manfaat yang lebih dibandingkan dengan komputer yang berdiri sendiri dan dunia usaha telah mengakui bahwa akses ke teknologi modern selalu memiliki keunggulan kompetitif dibandingkan pesaing yang terbatas dalam bidang teknologi.

2.1.6 Jenis-Jenis Jaringan Komputer

Jenis-jenis jaringan komputer terdiri dari :

2.1.6.1 Local Area Network (LAN)

Local Area Network (LAN), merupakan jaringan milik pribadi di dalam sebuah gedung atau kampus yang berukuran sampai beberapa kilometer. LAN seringkali digunakan untuk menghubungkan komputer-komputer pribadi dan *workstation* dalam kantor suatu perusahaan atau pabrik-pabrik untuk memakai bersama sumber daya (*resources*, misalnya printer) dan saling bertukar informasi.

2.1.6.2 *Metropolitan Area Network* (MAN)

Metropolitan Area Network (MAN), pada dasarnya MAN merupakan versi LAN yang berukuran lebih besar dan biasanya menggunakan teknologi yang sama dengan LAN. MAN dapat mencangkup kantor-kantor perusahaan yang letaknya berdekatan atau juga sebuah kota, dan dapat dimanfaatkan untuk keperluan pribadi (swasta) atau umum. MAN mampu menunjang data dan suara, bahkan dapat berhubungan dengan jaringan televisi kabel.

2.1.6.3 *Wide Area Network* (WAN)

Wide Area Network (WAN), jangkauannya mencangkup daerah geografis yang luas, seringkali mencangkup sebuah Negara, bahkan benua. WAN terdiri dari kumpulan mesin-mesin yang bertujuan untuk menjalankan program-program (aplikasi) pemakai.

2.1.6.4 internet

Merupakan suatu jaringan komputer yang global, jaringan-jaringan komputer yang terhubung secara mendunia sehingga komunikasi dan transfer data atau file menjadi lebih mudah. Internet merupakan perpaduan antara berbagai jenis jaringan komputer beserta topologi dan tipe jaringan yang berhubungan satu dengan lain.

2.1.6.5 Wireless

Merupakan jaringan tanpa kabel merupakan jenis jaringan yang menggunakan media transmisi data tanpa menggunakan kabel. Digunakan media seperti gelombang radio, inframerah, bluetooth, dan microwave. Wireless bisa digunakan kedalam jaringan LAN, MAN, juga WAN. Wireless ditujukan untuk kebutuhan mobilitas tinggi. Keuntungan jenis jaringan Wireless adalah kenyamanan untuk terhubung ke jaringan tanpa dibatasi kabel, lebih ke arah pengguna yang memerlukan mobilitas yang tinggi.

Kerugian jenis jaringan Wireless adalah transmisi data kepada para pengguna yang lambat dari penggunaan jaringan dengan kabel, memerlukan keamanan yang ketat karena orang yang berada di luar jaringan bisa menerobos masuk ke dalam jaringan Wireless.

2.1.7 Topologi Jaringan

Topologi jaringan adalah struktur jaringan untuk mengidentifikasi cara bagaimana simpul atau pusat di dalam jaringan saling berhubungan. Hubungan dalam jaringan sangat bergantung jenis aplikasi yang digunakan. Setiap topologi jaringan mempunyai kelebihan dan kekurangan masing-masing. Adapun topologi jaringan yang ada, yaitu :

2.1.7.1 Toplogi Bus atau *Linier*

Toplogi Bus atau *Linier* merupakan topologi yang banyak dipergunakan pada masa penggunaan kabel *coaxial* menjamur.

2.1.7.2 Topologi *Ring*

Topologi *Ring* ini memanfaatkan kurva tertutup, artinya informasi dan data serta *trafic* disalurkan sedemikian rupa sehingga masing-masing *node*.

2.1.7.3 Topologi *Star*

Topologi jaringan *star* ini banyak digunakan diberbagai tempat, karena kemudahan untuk menambah atau mengurangi serta mudah untuk mendeteksi kerusakan pada *system* jaringan yang ada.

2.1.7.4 *Mesh*

Mesh adalah topologi ini setiap komputer akan terhubung dengan komputer lain dalam jaringannya menggunakan kabel tunggal, jadi proses pengiriman data akan langsung mencapai komputer tujuan tanpa melalui komputer lain ataupun switch atau hub.

2.1.7.5 Topologi Tree

Topologi Jaringan Tree merupakan gabungan dari beberapa topologi star yang dihubungan dengan topologi bus, jadi setiap topologi star akan terhubung ke topologi star lainnya menggunakan topologi bus, biasanya dalam topologi ini terdapat beberapa tingkatan jaringan, dan jaringan yang berada pada tingkat yang lebih tinggi dapat mengontrol jaringan yang berada pada tingkat yang lebih rendah.

2.1.8 OSI Layer

OSI *Layer* merupakan model referensi yang digunakan untuk memahami jaringan komputer secara umum. Secara *de facto*, OSI *layer* telah dijadikan sebagai acuan saat mempelajari *network* yang dibangun menggunakan perangkat Cisco. OSI *Reference Model* atau model referensi OSI terdiri atas lapisan berjumlah 7 buah (*layer*) (Sofana, 2012:18).

2.1.9 Data *Link Layer*

Data *Link Layer* merupakan lapisan kedua dari standard OSI. Tugas utama *data link layer* adalah sebagai fasilitas transmisi *raw* data dan mentransformasi data tersebut ke saluran yang bebas dari kesalahan transmisi. Sebelum ditersan ke *network layer*, *data link layer* melaksanakan tugas ini dengan memungkinkan pengirim memecah-mecah data input menjadi sejumlah data frame (biasanya berjumlah ratusan atau ribuan *byte*). Kemudian *data link layer* mentransmisikan frame tersebut secara berurutan dan memproses *acknowledgement frame* yang dikim kembali oleh penerima. Karena *physical layer* menerima dan mengirim aliran bit tanpa mengindahkan arti atau *arsitektur frame*, maka tergantung pada *data link layer*-lah untuk membuat dan mengenali batas-batas *frame* itu. Hal ini bisa dilakukan dengan cara membubuhkan bit khusus ke

awal dan akhir *frame* (Wahana Komputer, 2003:80). Contoh *protokol data link layer* : 802.3 (*Ethernet*), 802.11 a/b/g/n MAC/Llc, 802.1Q (VLAN), ATM, CDP, HDP, FDDI, *Fibre Channel*, *Frame Relay*, SDLC, HDLC, ISL, PPP, Q.921, *Token Ring*.

2.2 Perangkat

Adapun peralatan atau perangkat yang digunakan dalam penelitian dapat digolongkan menjadi dua jenis, yaitu sebagai berikut :
perangkat keras dan perangkat lunak antara lain sebagai berikut :

1. Perangkat Keras
   a. Router mikrotik, HAPlite
   b. Komputer *server*
   c. PC atau Laptop sebagai *client*
   d. Switch
   e. Hub
   f. Kabel UTP
   g. Modem DSL (*Speedy)*
2. Perangkat Lunak
   a. Sistem Operasi Windows 7
   b. Winbox
   c. Putty

2.3 Aspek-aspek Keamanan Jaringan

Keamanan komputer meliputi empat aspek, antara lain:

2.3.1 *Authentication*, penerima informasi dapat memastikan keaslian pesan, bahwa pesan itu datang dari orang yang dimintai informasi. Dengan kata lain, informasi itu benar- benar datang dari orang yang dikehendaki.

2.3.2 *Integrity*, keaslian pesan yang dikirim melalui jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi orang yang tidak berhak.

2.3.3 *Confidentiality*, merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Kerahasiaan ini biasanya berhubungan dengan informasi yang diberikan ke pihak lain.

2.3.4 *Privacy*, lebih ke arah data-data yang bersifat pribadi.

2.3.5 *Availability*, aspekavailabilitas yang berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan akses ke informasi.

2.4 Ancaman Keamanan Jaringan

Aspek ancaman keamanan yang terjadi terhadap informasi adalah:

2.4.1 *Interruption*

Merupakan ancaman terhadap *availability* informasi, data yang ada dalam sistem komputer dirusak atau dihapus sehingga jika data atau informasi tersebutdibutuhkan maka pemiliknya akan mengalami kesulitan untuk mengaksesnya, bahkan mungkin informasi itu hilang. Contohnya adalah perusakan/modifikasi terhadap piranti keras atau saluran jaringan.

TABLE I.

2.4.2 *Interception*

Merupakan ancaman terhadap kerahasiaan *(secrery*). Informasi disadap sehingga orang yang tidak berhak dapat mengakses komputer dimana informasi tersebut disimpan. Contohnya adalah penyadapan terhadap data dalam suatu jaringan.

2.4.3 *Modification*

Merupakan ancaman terhadap integritas. Orang yang tidak berhasil menyadap lau lintas informasi yang sedang dikirim dan kemudian mengubahnya sesuai keinginan orang tersebut. Contohnya adalah perubahan nilai pada file data, modifikasi program sehingga berjalan dengan tidak semestinya, dan modifikasi pesan yang sedang ditransmisikan dalam jaringan.

2.4.4 Fabrication Merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil meniru atau memalsukan informasi sehingga orang yang menerima informasi tersebut menyangka bahwa informasi tersebut berasal dari orang yang dikehendaki oleh si penerima informasi. Contohnya adalah pengiriman pesan palsu kepada orang lain.

2.5 Jenis Serangan

2.5.1 *Sniffer*

Sniffer adalah sebuah *device* penyadapan komunikasi jaringan komputer

dengan memanfaatkan mode *premicious* pada ethernet. Karena jaringan komunikasi terdiri dari biner acak maka *sniffer* ini biasanya memiliki penganalisis protokl sehingga data biner acak dapat dipecahkan. Fungsi sniffer bagi pengelola bisa untuk pemeliharaan jaringan, bagi orang luar bisa untuk masuk ke dalam sistem.

2.5.1 Spoofing

Spoofing (penyamaran) biasanya dilakukan oleh pihak yang tidak bertanggung jawab untuk menggunakan fasilitas dan resource sistem. Spoofing adalah teknik melakukan penyamaran sehingga terdeteksi sebagai identitas yang bukan sebenarnya.

2.6 DHCP

DHCP (*Dynamic Host Configuration Protocol*) merupakan salah satu protokol standar pada jaringan komputer yang berfungsi untuk membantu pengguna jaringan komputer memperoleh alamat (IP *address*) secara cepat dan otomatis. Dengan pengalamatan yang otomatis ini, maka pengguna jaringan komputer yang tidak memiliki seluk beluk pemahaman tentang pengalamatan jaringan (IP *address*, *subnetting*, blok alamat IP, kelas IP *address*) akan terbantu (Pratama, 2014:154).

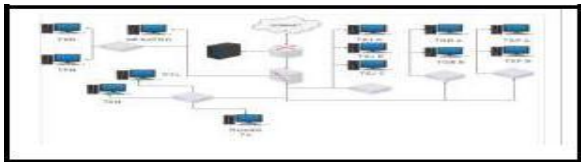
2.7 DHCP Snooping

Dalam jaringan komputer, DHCP *snooping* adalah serangkaian teknik yang diterapkan untuk meningkatkan keamanan jaringan DHCP. Ketika server DHCP mengalokasikan alamat IP untuk klien di LAN, DHCP *snooping* dapat dikonfigurasi pada switch LAN untuk mengizinkan hanya klien dengan IP tertentu dan alamat MAC untuk memiliki akses ke jaringan. DHCP *snooping* dapat memastikan integritas IP pada *Layer* 2 *switched domain*. Dengan DHCP *snooping* , informasi tentang alamat IP dan sesuai alamat MAC disimpan dalam database pada switch. DHCP *snooping* dapat digunakan untuk fitur keamanan lain seperti penjaga sumber IP dan ARP *dinamis*, yang membuatnya menjadi komponen utama dari keamanan akses LAN. DHCP *snooping* juga dapat mencegah penyerang menambahkan server DHCP ke jaringan, menyebabkan kerusakan jaringan dan menambahkan komponen tidak sah.

III. HASIL DAN PEMBAHASAN

3.1 Topologi Jaringan

Perancangan topologi jaringan komputer yang disimulasikan dalam penerapan keamanan jaringan.



Gambar 4 Simulasi Topologi Jaringan

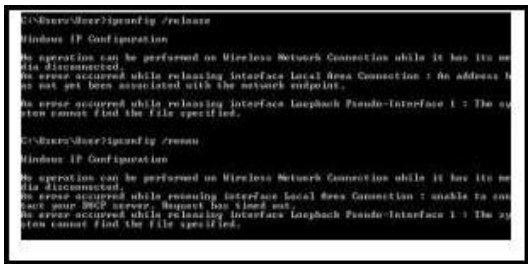
3.2 DHCP *Snooping Trust*

Dari analisis keamanan jaringan komputer, maka dirancang keamanan jaringan *layer* 2 menggunakan DHCP *snooping trust* dengan tujuan agar terhindar dari *attacker* atau pihak yang tidak bertanggung jawab dalam pengambilan data pada jaringan. Rancangan keamanan *layer* 2 dibuat pada *router mikrotik* dan *switch*.

Gambar 5 Hasil DHCP *Snooping Trust*

3.3 Pembatasan User

Dari analisis keamanan jaringan komputer, maka dirancang keamanan jaringan menggunakan DHCP *snooping limit rate* dimana *limit rate* berfungsi untuk pembatasan user atau pemakai dengan tujuan agar keamanan jaringan terhindar dari para *attacker* yang tidak bertanggung jawab.



Gambar 6 Hasil DHCP Snooping Limit Rate

IV. KESIMPULAN

Adapun kesimpulan yang diperoleh dalam penelitian ini adalah DHCP *Snooping* adalah sebuah teknik keamanan yang menentukan port mana saja yang mendapatkan IP DHCP dan membatasi lalu lintas DHCP dari sumber terpercaya dan tidak terpercaya. Jika perangkat penipu atau *fake* mencoba untuk mengirim paket DHCP *offer* ke dalam jaringan maka port akan mati secara otomatis.

V. SARAN

Perancangan keamanan jaringan dengan menggunakan DHCP *snooping* dapat dikembangkan sesuai dengan kebutuhan keamanan pada *layer* 2, sepert penambahan DHCP *starvation* agar lebih memperkuat keamanan jaringan *layer* 2.

Berdasarkan kesimpulan yang telah disajikan, maka ada beberapa saran yang penulis ingin sampaikan antara lain :

1. Perancangan keamanan jaringan dengan menggunakan DHCP *snooping* dapat dikembangkan sesuai dengan kebutuhan keamanan pada *layer* 2, sepert penambahan DHCP *starvation* agar lebih memperkuat keamanan jaringan *layer* 2.
2. Penulis mengharapkan perancangan ini dapat di *maintenace* atau diupdate secara rutin dan dapat juga sebagai referensi bagi peneliti lainnya.

VI. UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Universitas Bina Darma dan cisco networking academy UBD yang telah memberi dukungannya terhadap penelitian ini. Penelitian ini sangat dibutuhkan penulis untuk membantu meningkatkan kualitas penelitian dan semoga bisa bermanfaat bagi yang membutuhkan sebagai referensi. Penulis juga mengucapkan terima kasih kepada pengelola Jurnal STMIK MURA yang telah *accepted* jurnal saya karena saya sangat membutuhkan jurnal ini untuk menunjang kepengurusan jenjang akademik.

VII. DAFTAR PUSTAKA

Andi. 2005. *Menjadi Administrator Jaringan Komputer.* Yogyakarta : Andi.

Komputer, Wahana. 2003. "Konsep Jaringan Komputer dan Pengembangannya", Penerbit Salemba Infotek, Jakarta.

Perti. 2004. "Schaum's Outlines Of Computer Networking Ed Title". Penerbit Erlangga.

Sofana, Iwan. 2012. "CISCO CCNP dan Jaringan Komputer(Materi, Route, Switch,&Troubleshooting)", Penerbit Informatika, Bandung.

Sofana, Iwan. 2010. *CISCO CCNA & JARINGAN KOMPUTER.* Bandung: Informatika.

Sukmaaji, Anjik & Rianto. 2008."Jaringan Komputer", Penerbit ANDI : Yogyakarta.

Harliana. Putri, Perdana Adidtya, Khalil M.Raden Prasetyo." Sniffing dan Spoofing Pada Aspek Keamanan Komputer".http://www.academia.edu/5088063/Jurnal-Keamanann Komputer. Diakses *pada tanggal 25 Januari 2017.*

Muhajirin."Desain Produk, Pengertian dan Ruang lingkupnya".*https://www.google.com/url sa=t&rct=j&q=&esrc=s&source=web &cd=&cad=rja&uact=8&ved=0ahUK Ewim6tGod7RahWKnpQKHWemBtoQF ggbMAA&url=http%3A%2 %2Feprints.uny.ac.id%2F 4131%2F1%2FHandout_Desain_Produ k_Kerajinan.doc&usg=AFQjCNEbb2F mEhOI1LToawi2UTv4Akk8nw Diakses pada tanggal 25 Januari 2017.*

Gunawan, Albert."Evaluasi *Security Protection Wireless* LAN Berbasisradius"http://digilib.binadarma.ac.id/download.php?id=1195. *Diakses pada tanggal 25 Januari 2017*.

Guritno, S, Sudaryono, and Raharja, u. 2011. Theory and Application of IT Research. Yogyakarta: Andi.

Davison, R. M., Martinsons, M. G., Kock N., (2004), *Journal:* Information Systems *Journal : Principles of Canonical Action Research* 14, 65–86

www.cisco.com

www.netacad.com