Mitigasi Keamanan *Dynamic Host Control Protocl* (DHCP) Untuk Mengurangi Serangan Pada *Local Area Network* (LAN)

Tamsir Ariyadi[1]
Program Studi Teknik Komputer, Universitas Bina Darma
Universitas Bina Darma, Jl. Jendral A. Yani No.03 Plaju Palembang
email: tamsirariyadi@binadarma.ac.id[1]

Abstrack - 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 discusses a prototype of network security called Dynamic Host Control Protocol (DHCP) Security Mitigation to Reduce Local Area Network (LAN) Attacks.

Keywords*: Mitigation, DHCP, Network Security*

Intisari - 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. Pembahasan prototype terhadap keamanan jaringan yang disebut Mitigasi Keamanan Dynamic Host Control Protocol (DHCP) Untuk Mengurangi Serangan pada Local Area Network (LAN).

Kata Kunci : *Mittigation, DHCP, Network Security*

I. PENDAHULUAN

Pengaruh 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. [1]

Berbagai tempat 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. [2]

Sehingga jaringan komputer sangat dibutuhkan untuk saling berkomunikasi dan mengirim data. Jaringan komputer masih memiliki kelemahan karena keamanan yang belum maksimal maka sering terjadi kejahatan cyber yang dilakukan oleh orang yang tidak bertanggung jawab. Dengan keadaan tersebut maka jaringan komputer perlu meningkatkan keamanan jaringannya yang salah satunya 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 dan penyerang tidak dapat mengakses ataupun masuk ke dalam jaringan tersebut.

II. SIGNIFIKASI STUDI

A. Studi Literatur

1. 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:

a. Toplogi Bus atau *Linier*
   Toplogi Bus atau *Linier* merupakan topologi yang banyak dipergunakan pada masa penggunaan kabel *coaxial* menjamur.
b. Topologi *Ring*
   Topologi *Ring* ini memanfaatkan kurva tertutup, artinya informasi dan data serta *trafic* disalurkan sedemikian rupa sehingga masing-masing *node*.
c. 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.
d. 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. Keamanan Jaringan Komputer

Keamanan jaringan komputer meliputi empat aspek [3], antara lain:

a. *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.
b. *Integrity*, keaslian pesan yang dikirim melalui jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi orang yang tidak berhak.
c. *Confidentiality*, merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Kerahasiaan ini biasanya berhubungan dengan informasi yang diberikan ke pihak lain.
d. *Privacy*, lebih ke arah data-data yang bersifat pribadi.
e. *Availability* aspek availabilitas berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan akses ke informasi.

3. Aspek-Aspek Ancaman Keamanan

Aspek ancaman keamanan yang terjadi terhadap informasi [4] adalah:

a. *Interruption*
   Merupakan ancaman terhadap *availability* informasi, data yang ada dalam sistem komputer dirusak atau dihapus sehingga jika data atau informasi tersebut dibutuhkan maka pemiliknya akan mengalami kesulitan untuk mengaksesnya, bahkan mungkin informasi itu hilang. Contohnya adalah

perusakan/modifikasi terhadap piranti keras atau saluran jaringan.

b. *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.

c. *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.

d. *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.

4. Jenis-Jenis Serangan Jaringan Komputer

Jenis-jenis serangan jaringan komputer yang terjadi terhadap informasi [5] antara lain:

a. *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 protokol sehingga data biner acak dapat dipecahkan. Fungsi *sniffer* bagi pengelola bisa untuk pemeliharaan jaringan, bagi orang luar bisa untuk masuk ke dalam sistem.

b. *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.

5. 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. [6]. Jenis-Jenis Jaringan terdiri dari:

a. *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.

b. *Metropolitan Area Network* (MAN)
Metropolitan Area Network (MAN)
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.

c. *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.

6. 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*). [7]

a. Physical Layer
Physical layer merupakan layer pertama atau yang terendah dari model OSI. Layer ini bertanggung jawab untuk mentransmisikan bit data digital dari physical layer perangkat pengirim (sumber) menuju ke physical layer perangkat penerima (tujuan) melalui media komunikasi jaringan. Pada physical layer data ditransmisikan menggunakan jenis sinyal yang didukung oleh media fisik, seperti tegangan listrik, kabel, frekuensi radio atau infrared maupun cahaya biasa.

b. Data Link Layer
Data link layer bertanggung jawab untuk memeriksa kesalahan yang mungkin terjadi pada saat proses transmisi data dan juga membungkus bit kedalam bentuk data frame. Data link layer juga mengelola skema pengalamatan fisik seperti alamat MAC pada suatu jaringan. Data link layer merupakan salah satu layer OSI yang cukup kompleks, oleh karena itu layer ini kemudian dibagi lagi menjadi dua sublayer, yaitu layer Media Access Control (MAC) dan Layer Logical Link Control (LLC). Layer Media Access Control (MAC) bertanggung jawab untuk mengendalikan bagaimana sebuah perangkat pada suatu jaringan memperoleh akses ke medium dan izin untuk melakukan transmisi data. Layer Logical Link Control (LLC) bertanggung jawab untuk mengidentifikasi dan membungkus protokol network layer dan mengontrol pemeriksaan kesalahan dan juga melakukan sinkronisasi pada frame.

c. Network Layer
Network layer bertanggung jawab untuk menetapkan jalur yang akan digunakan untuk melakukan transfer data antar perangkat di dalam suatu jaringan. Router jaringan beroperasi pada layer ini, yang mana juga menjadi fungsi utama pada layer network dalam hal melakukan routing. Routing memungkinkan paket dipindahkan antar komputer yang terhubung satu sama lain. Untuk mendukung proses routing ini, network layer menyimpan alamat logis seperti alamat IP untuk setiap perangkat pada jaringan. Layer Network juga mengelola pemetaan antara alamat logikal dan alamat fisik. Dalam jaringan IP, pemetaan ini dilakukan melalui Address Resolution Protocol (ARP).

d. Transport Layer
Transport layer bertanggung jawab untuk mengirimkan pesan antara dua atau lebih host didalam jaringan. Transport layer juga menangani pemecahan dan penggabungan pesan dan juga mengontrol kehandalan jalur koneksi yang diberikan. Protokol TCP merupakan contoh yang paling sering digunakan pada transport layer.

e. Session Layer
Session layer bertanggung jawab untuk mengendalikan sesi koneksi dialog seperti menetapkan, mengelola dan memutuskan koneksi antar komputer. Untuk dapat membentuk sebuah sesi komunikasi, session layer menggunakan sirkuit virtual yang dibuat oleh transport layer.

f. Presentation Layer
Presentation layer bertanggung jawab untuk mendefinisikan sintaks yang

digunakan host jaringan untuk berkomunikasi. Presentation layer juga melakukan proses enkripsi/ dekripsi informasi atau data sehingga mampu digunakan pada lapisan aplikasi.

g. Application Layer
Application layer merupakan lapisan paling atas dari model OSI dan bertanggung jawab untuk menyediakan sebuah interface antara protokol jaringan dengan aplikasi yang ada pada komputer. Application layer menyediakan layanan yang dibutuhkan oleh aplikasi, seperti menyediakan sebuah interface untuk Simple Mail Transfer Protocol (SMTP), telnet dan File Transfer Protocol (FTP). Pada bagian sinilah dimana aplikasi saling terkait dengan jaringan.

B. Pemodelan

1. Peralatan

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:

a. Perangkat Keras berupa Router mikrotik, HAPlite, Komputer *server* PC dan Laptop sebagai *client Switch Hub* Kabel UTP Modem DSL (*Speedy)*

b. Perangkat Lunak berupa *Sistem Operasi, Windows 10* Winbox, Putty

2. Media Transmisi

Media 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.*

3. Simulasi DHCP

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 dijalankan, 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, dan berjalan dalam mesin virtual, dan komputer induk terlihat sebagai mesin virtual dapat bekerja sama secara optimal. Dalam implementasi *mittigation* DHCP yang penulis deskripsikan mempunyai konsep LAN yang nantinya bisa di aplikasikan pada lingkup sebenarnya.

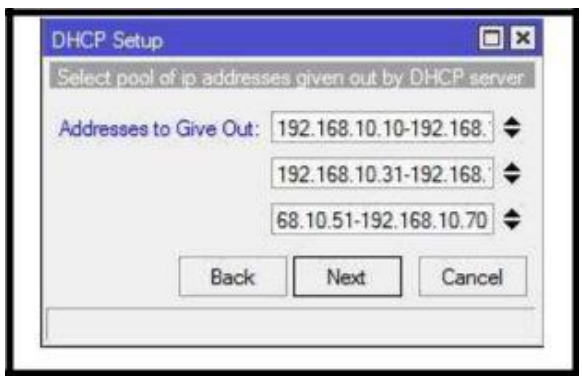
4. Desain

Menginterpretasikan *mittigation* DHCP 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 yaitu *server* dan *client* yang dapat di gambarkan sebagai bentuk perancangan topologi dan perancangan Mittigation Attack.

III. HASIL DAN PEMBAHASAN

Pada tahap implementasi adalah mengimplementasikan DHCP *server* pada *router* mikrotik dan mengimplementasikan DHCP pada switch pada jaringan komputer. Langkah-langkah yang dibutuhkan dalam konfigurasi DHCP *server:*

1. Konfigurasi DHCP



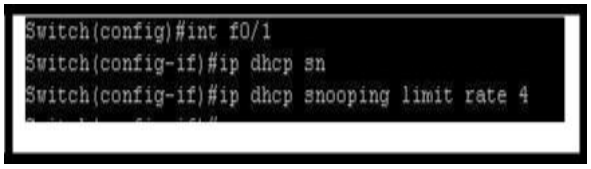
Gambar 1. Konfigurasi DHCP Pada *Winbox*

2. Konfigurasi DHCP Snooping
   Setelah pembuatan IP DHCP s*erver* telah selesai, konfigurasi DHCP *snooping* pada *switch*. Dengan menggunakan VLAN 1, dimana terdapat beberapa port yang digunakan dalam konfigurasi.

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

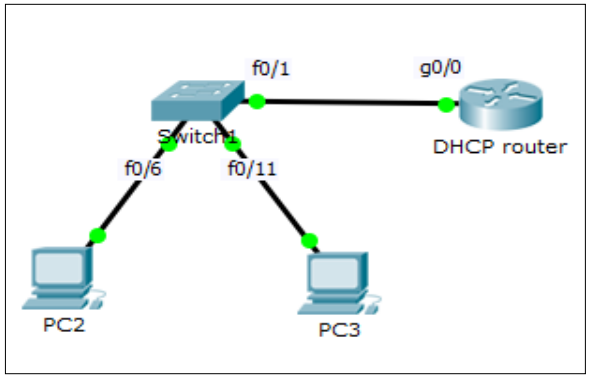
Gambar 2. IP *snooping trust*

4. 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*

A. Rancangan Topologi

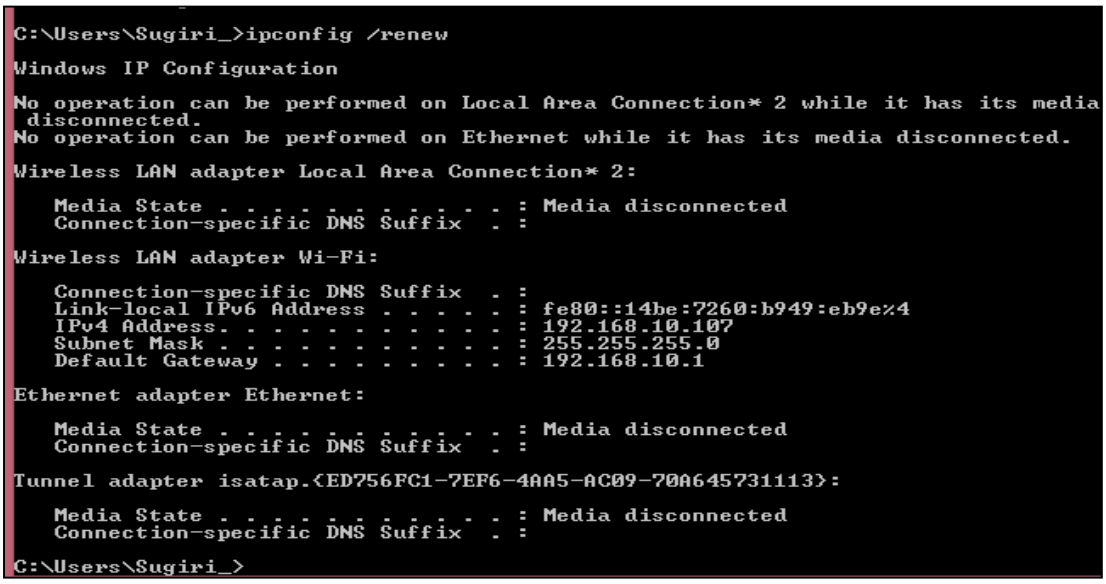


Gambar 4. Topologi DHCP DHCP

Snooping adalah suatu teknologi untuk mengamankan paket DHCP, maksud mengamankan disini adalah DHCP klien mendapatkan IP dari DHCP Server yang terpercaya.

B. DHCP Snooping Trust

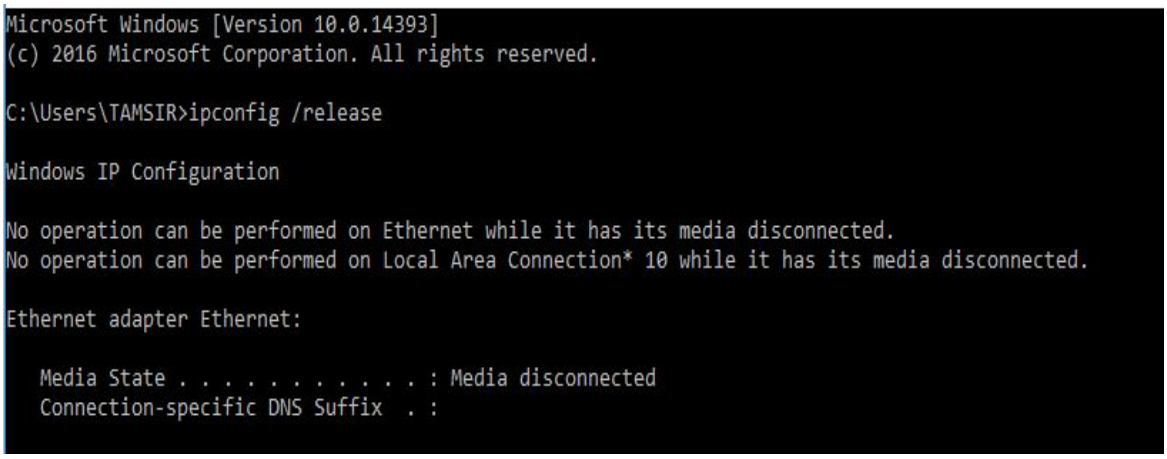
Dari analisis keamanan jaringan komputer, maka dirancang keamanan jaringan *layer* 2 menggunakan DHCP *snooping trust* dengan tujuan agar terhindar dari *attacker* atau pihak yang tidak bertanggung jawab dalam pengambilan data pada jaringan. Rancangan keamanan *layer* 2 dibuat pada *router mikrotik*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



Gambar 5. Hasil DHCP *Snooping Trust*

C. 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. Setelah dikonfigurasi bisa dilihat dengan ipconfig /release, kemudian akan menampilkan window no IP configuration.



Gambar 5 Hasil DHCP Snooping Limit Rate

IV. KESIMPULAN

Adapun kesimpulan yang diperoleh mitigasi DHCP untuk mengurangi serangan 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.

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

Berdasarkan kesimpulan yang telah disajikan, maka hal yang perlu dilakukan yaitu perancangan keamanan jaringan dengan menggunakan DHCP *snooping* dapat dikembangkan sesuai dengan kebutuhan keamanan pada *layer* 2, seperti 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) Mitigasi keamanan Dynamic Host Control Protocol (DHCP) untuk mengurangi serangan pada *Local Area Network* (LAN) dapat dikembangkan sesuai dengan kebutuhan keamanan jaringan dengan mendesain pada *layer* 2, seperti penambahan DHCP *starvation* dan DHCP *roque* agar lebih meningkatkan keamanan jaringan yang berada pada lapisar kedua atau *layer 2*. (2) Mitigasi keamanan dynamic host control protocol (DHCP) untuk mengurangi Serangan keamanan jaringan dengan menggunakan DHCP *snooping* dapat dikembangkan sesuai dengan kebutuhan keamanan pada *layer* 2, seperti penambahan DHCP *starvation* agar lebih memperkuat keamanan jaringan *layer* 2.

REFERENSI

[1] www.cisco.com
[2] www.netacad.com
[3] Sofana, Iwan. 2012. *CISCO CCNP dan Jaringan Komputer (Materi, Route,*

Switch, & Troubleshooting), Informatika, Bandung.

[4] Sofana, Iwan. 2010. *Cisco CCNA & Jaringan Komputer*. Informatika, Bandung.

[5] Sukmaaji, Anjik dan Rianto. 2008. *Jaringan Komputer*, Penerbit Andi, Yogyakarta.

[6] Komputer, Wahana. 2003. *Konsep Jaringan Komputer dan Pengembangannya*, Penerbit Salemba Infotek, Jakarta.

[7] Andi. 2005. *Menjadi Administrator Jaringan Komputer,* Andi, Yogyakarta.