Analisis Paket DHCP Rogue Pada Jaringan *Local Area Network* (LAN) Menggunakan *Wireshark*

Tamsir Ariyadi[1], Ali Kasim[2]
1Teknik Komputer, 2Teknik Elektro Universitas Bina Darma Palembang
Jalan Jendral Ahmad Yani No. 3, Palembang 30264
tamsirariyadi@gmail.com, ali.kasim@binadarma.ac.id

***Abstrak— Rogue DHCP server* adalah salah satu pemenfaatan keamanan pada mekanisme konfigurasi alamat jaringan menggunakan *DHCP*. *Rogue DHCP server* memberikan konfigurasi alamat jaringan yang salah kepada client yang bergabung didalam jaringan dengan tujuan menciptakan serangan berupa *man-in-the-middle*, sehingga dapat menimbulkan ancaman terhadap privasi *client* yang bergabung didalam jaringan.Penelitian difokuskan pada analisis *DHCP packets* seperti *DHCPDISCOVER, DHCPREQUES, DHCPOFFER, DHCPACK* yang melewati sebuah *Bridge* Mikrotik menggunakan aplikasi *Wireshark* sebelum adanya dan setelah adanya *Rogue DHCP server* didalam jaringan DHCP, sehingga dapat diamati bagaimana *DHCP server* asli dan *Rogue* DHCP *server* saling bertukar pada *packets* DHCP dengan *DHCP client* yang selanjutnya dilakukan analisis terhadap *Rogue DHCP packets.* Dari hasil analisis didapatkan informasi parameter-parameter yang terkandung di dalam Rogue DHCP *Packets* yang difungsikan untuk membangun sistem keamanan jaringan DHCP berupa monitoring dan pencegahan terhadap Rogue DHCP Server menggunakan DHCP Alert yang dikombinasikan dengan *Firewall Filter Rule* pada sebuah Bridge Mikrotik, dengan diperoleh hasil bahwa sistem dapat mendeteksi dan mencegah adanya Rogue DHCP Server di dalam jaringan DHCP berbasis IPv4.**

Kata kunci— DHCP; packets rogue DHCP, server rogue DHCP, wireshark, mikrotik

I. LATAR BELAKANG

Seiring dengan semakin berkembangnya teknologi internet, kejahatan yang memanfaatkan teknologi ini juga semakin meningkat. Hal ini ditambah lagi dengan semakin banyaknya peredaran aplikasi gratis yang dapat digunakan untuk melancarkan usaha pembobolan suatu sistem berbasis teknologi jaringan *internet.* bertambahnya kebutuhan atas jaringan *internet* untuk melakukan transaksi, kegiatan-kegiatan yang bertujuan jahat seperti *deface* atau pencurian data yang dilakukan oleh orang yang tidak bertanggung jawab juga meningkat.

Dynamic Host Configuration Protocol (DHCP)protokol yang paling banyak digunakan di dunia, baik digunakan dalam jaringan kabel maupun nirkabel seperti pengelolaan jaringan warung intiernet, jaringan perkantoran, jaringan lab kampus, hostpot pada *cafe* atau secara umumnya, jaringan antar ISP dan *tethering* atau *portable hostpot* pada *smatrphone*.. Penggunaan DHCP diperlukan sebuah server untuk bertanggung jawab atas pemberian alamat IP kepada *clinet*, Jika DHCP server mati maka seluruh *client*/host dalam jaringan tersebut tidak terhubung satu sama lain karena DHCP dibangun dengan sistem terpusat.Kelemahan lain dari protokol ini adalah adanya celah keamanan jaringan komputer yang dapat digunakan oleh *network attcker* untuk melakukan jenis serangan *man-in-the-middle* menggunakan *Rogue* DHCP *server*. *Rogue* DHCP *server* adalah DHCP *server* pada sebuah jaringan komputer yang tidak memiliki wewenang adminitratif atau bisa disebut server palsu yang digunakan untuk melakukan serangan jaringan dengan menggunakan tools atau aplikasi didalamnya terhadap server maupun *client*, sehingga DHCP *server* asli tidak dapat berfungsi secara optimal dalam memberikan layanan terhadap client. *Rogue* DHCP server didalam sebuah jaringan akan merusak sistem keamanan dan menimbulkan masalah privasi bagi *client* yang dapat menciptakan serangan jahat. Mengintersepsi lalu lintas jaringan dari perangkat apapun yang tergabung dalam jaringan DHCP sehingga penyerang menjadi *man-in-the-middle* yang dapat melihat dan memodifikasi isi asli dari komunikasi. Permasalah tersebut dapat diselesaikan dengan adanya analisis pengamatan paket DHCP beserta parameter yang ada didalamnya menggunakan *wireshark* yang bertujuan untuk menciptakan sistem keamanan jaringan berupa monitoring dan pencegahan terhadap *Rogue* DHCP *server*.

Berdasarkan uraian permasalahan diatas tersebut, maka penulis tertarik untuk mengambil tema dengan judul penelitian "Analisis Paket DHCP *Rogue* Pada Jaringan *Local Area Netwrork* (LAN) Menggunakan *Wireshark"*

II. LANDASAN TEORI

A. Analisis

Analisis adalah sebuah teknik pemecahan masalah yang menguraikan sebuah sistem menjadi bagian-bagian komponen dengan tujuan mempelajari seberapa bagus bagian-bagian komponen tersebut bekerja dan berinteraksi untuk meraih tujuan mereka [1].

Analisis merupakan penguraian dari suatu sistem informasi yang utuh ke dalam bagian-bagian komponennya dengan

maksud untuk mengidentifikasi dan mengevaluasi permasalahan-permasalahan, kesempatan-kesempatan, hambatan-hambatan yang terjadi dan kebutuhan-kebutuhan yang diharapkan sehingga dapat diusulkan perbaikan-perbaikannya.[2].

B. Pengertian DHCP

Menurut Zulhijah [3] *Dynamic host configuration pratocol*(DHCP) merupakan sebuah protokol yang menggunakan arsitektur *client/server* yang dipakai untuk mempermudah pengalokasian alamat IP dalam suatu jaringan. Sebuah jaringan lokal yang tidak menggunakan DHCP harus memberikan alamat IP kepada semua komputer secara menual. Maka dalam DHCP terdapat dua pihak yang terlibat, yakni DHCP *Server* dan DHCP *Client.*

1) DHCP *Server* merupakan sebuah mesin yang menjalankan layanan yang dapat menyewahkan alamat IP dan informasi TCP/IP lainnya kepada semua klien yang memintanya. Beberapa sistem operasi jaringan seperti *Windows NT server*, *Windows* 2000 *server*, atau linux memiliki layanan seperti ini.

2) DHCP Client merupakan mesin klien yang menjalankan perangkat lunak klien DHCP yang memungkinkan mereka untuk dapat berkomunikasi dengan DHCP Server. Sebagian besar sistem operasi klien jaringan (*windows NT Workstation, Windows 2000 Professional, Windows XP, Windows Vista* atau *Linux* memeliki perangkat seperti ini.

C. Pengertian DHCP Rogue

Menurut Kadafi [4] *Rogue* DHCP *server* adalah DHCP *server* pada sebuah jaringan komputer yang tidak memiliki wewenang adminitratif atau bisa disebut *server* palsu yang digunakan untuk melakukan serangan jaringan dengan menggunakan *tools* atau aplikasi didalamnya terhadap server maupun *client*, sehingga DHCP *server* asli tidak dapat berfungsi secara optimal dalam memberikan layanan terhadap client. *Rogue* DHCP *server* didalam sebuah jaringan akan merusak sistem keamanan dan menimbulkan masalah privasi bagi *client* yang dapat menciptakan serangan jahat seperti *sniffing* lalu-lintas jaringan, serangan *masquerading*, dan serangan DOS.

III. ANALISIS DAN PERANCANGAN

Metode yang digunakan dalam penelitian ini menggunakan metode penelitian tindakan atau *action research*. Menurut Guritno, Sudaryono [5] *Action Research* merupakan bentuk penelitian tahapan (*applied research*) yang bertujuan mencari cara efektif yang menghasilkan perubahan disengaja dalam suatu lingkungan yang sebagian dikendalikan (dikontrol).

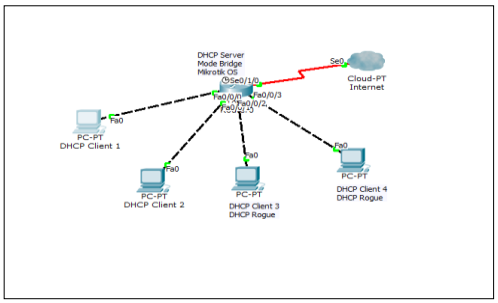
A. Melakukan Diagnosa

Peneliti melakukan pengumpulkan data jaringan maupun infrastruktur yang digunakan untuk mengumpulkan data pada Laboratorium Cisco Kampus C Universitas Bina Darma Palembang ,alat dan bahan yaitu Perangkat Keras (*Hardware*) seperti Laptop/Pc, Printer, dan Perangkat Lunak (*Software*) seperti Sistem Operasi Windows 7 ultimate, Firefox Mozilla, *Software*, Hub/Switch, *Wireshark*, Winbox dan Mikrotik.

Serangan Rogue DHCP yang terjadi pada suatu jaringan akan mengakibatkan pertukaran data yang terjadi pada jaringan tersebut akan melambat atau bahkan akan merusak suatu sistem jaringan. Insiden keamanan jaringan adalah suatu aktivitas terhadap keamanan sistem yang secara langsung atau tidak bertentangan dengan *security policy* sistem tersebut. *Rogue* DHCP server didalam sebuah jaringan akan merusak sistem keamanan dan menimbulkan masalah privasi bagi *client* yang dapat menciptakan serangan jahat. Mengintersepsi lalu lintas jaringan dari perangkat apapun yang tergabung dalam jaringan DHCP sehingga penyerang menjadi *man-in-the-middle* yang dapat melihat dan memodifikasi isi asli dari komunikasi. Permasalah tersebut dapat diselesaikan dengan adanya analisis pengamatan paket DHCP beserta parameter yang ada didalamnya menggunakan *wiresharky*ang bertujuan untuk menciptakan sistem keamanan jaringan berupa monitoring dan pencegahan terhadap *Rogue* DHCP *server*.

B. Perancangan Topologi Jaringan

Topologi jaringan adalah hal yang menjelaskan hubungan geometris antara unsur-unsur dasar penyusun jaringan. Perancangan topologi jaringan menggunakan *pakcet tracer* dengan sistem operasi *windows 10*. Untuk lebih jelasnya topologi jaringan yang diterapkan dapat dilihat pada Gbr. 1. berikut :



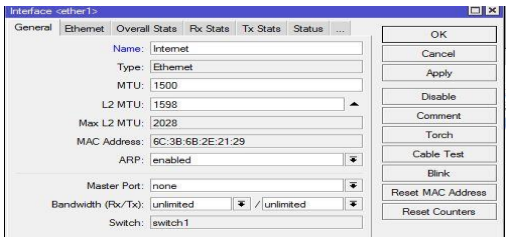
Gbr. 1. Topologi jaringan

C. Melakukan Tindakan

KonfigurasiDHCP PadaWinbox

Langkah-langkah konfigurasi DHCP Internet pada mikrotik, sebagai berikut :

Pada Winbox pilih menu *Interfaces* kemudian masukkan name Internet



Gbr. 2. Membuat *interfaces* internet

IV. HASIL DAN PEMBAHASAN

A. *Hasil Penelitian*

1) PerancanganTopologi Jaringan

Topologi jaringan adalah hal yang menjelaskan hubungan *geometris* antara unsur-unsur dasar penyusun jaringan. Perancangan topologi jaringan menggunakan sistem operasi *windows 10* . dan kali linux.

2) Pengujian Koneksi

Pada bagian ini penulis akan menjelaskan uji koneksi antar client ke *server* dan *server* ke *client*. *Server* melakukan pengujian dengan ip *client* 1 192.168.100.1 , *client* 2 dengan ip dan ip 192.168.20.1.

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::291b:2dd9:6ea2:e8c%5
   IPv4 Address. . . . . . . . . . . : 192.168.100.254
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.100.1
```

Gbr. 3. IP DHCP *server* Client-1

Pada gambar diatas adalah *IP DHCP server client* 1 yang mendapatkan *IP* 192.168.100.254 dengan *subnet mask* 255.255.255.0 dan *gateway* 192.168.100.1

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::291b:2dd9:6ea2:e8c%14
   IPv4 Address. . . . . . . . . . . : 192.168.20.253
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.20.1
```

Gbr. 4. IP DHCP *server* Client-2

Hasil dari Gbr. 3. dan Gbr. 4. menunjukan bahwa *IP DHCPserver* telah berhasil dan dapat dihubungkan *router* kemudian ke *client* agar *client* mendapatkan *IP DHCP*.

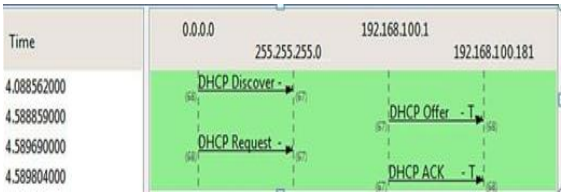
B. *Pembahasan*

Pada pembahasan ini penulis akan menjelaskan cara menganalisis paket DHCP sebelum dan sesudah adanya *Rogue* DHCP server pada client dengan menggunaka *wireshark*.

1) Melakukan Evaluasi

a) Analisis paket DHCP sebelum adanya Rogue DHCP Server

Pada analisis *DHCP Rogue Server* akan dilakukan pengujian dalam satu jaringan, yang mana *DHCP Server* memberikan *IP* ke *Client-Client* berdasarkan topologi. Pada kondisi ini mekanisme pertukaran paket *DHCP* masih standar atau normal, dimana masih ada satu *Server DHCP* didalam jaringan dengan pertukaran paket seperti, *DHCPDISCOVER, DHCPOFFER, DHCPREQUEST,* dan *DHCPACK.*



Gbr. 5. *Flow graph* DHCP *packets* pada *client* sebelum adanya Rogue DHCP server

Pertukaran *DHCP* paket yang terjadi masih berjalan normal, dengan indikasi client mendapatkan paket *DHCPACK* yang sekaligus mendapatkan konfigurasi *IP DHCP Server* asli yaitu yang berasal dari alamat *gateway* 192.168.100.1.

b) Konfigurasi DHCP Rogue Server

Pembahasan ini penulis akan menggunakan metode serangan yang lain. Serangan ini akan sepenuhnya memanfaatkan proses alokasi *IP DHCP*.Pertama, penyerang mengirimkan paket penemuan *DHCP* ke *server DHCP* seperti biasa *Server DHCP* juga merespons penyerang dengan Penawaran *DHCP* Penyerang terus mengirim paket Permintaan *DHCP* untuk menerima *IP* yang diberikan *DHCP Rogue* pada *DHCP server*.

```
root@kali:~# ifconfig eth0 192.168.10.10 netmask 255.255.255.0
root@kali:~# ifconfig eth0 192.168.10.10 netmask 255.255.255.255
root@kali:~# ifconfig eth0:1
eth0:1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 08:00:27:85:a6:f8  txqueuelen 1000  (Ethernet)
```

Gbr. 6. Konfigurasi *ifconfig* pada *kali linux*

c) Pengujian DHCP Packets setelah adanya Rogue DHCP Server

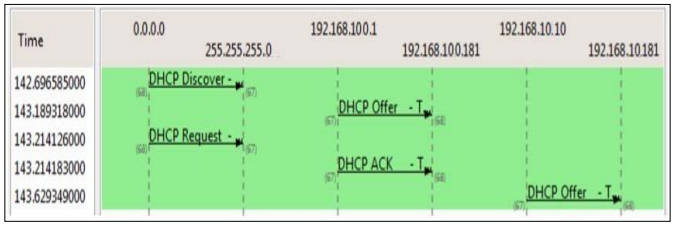
Pada pengujian setelah adanya *DHCP Rogue Server* yang menggunakan *IP Client* , diambil 2 pengujian dimana packets *DHCPACK* didapatkan berdasarkan *packets DHCPOFFER* pertama yang berhasil dari *Rogue DHCP* Server pengujian ke-1 dan *packets DHCPACK* didapatkan berdasarkan *DHCPOFFER* pertama yang berasal dari *DHCP Server* asli pengujian ke-2 dan untuk diamati proses pertukaran serta para meter *packetsnya*. Pengujian ke-1 pertukaran *DHCP packets* hanya terjadi antara *Rogue DHCP Server* dengan

Client yang dapat dilihat dalam bentuk grafik, dibuat menggunakan *flow graph* pada *wireshark* dengan memfilter *DHCP packets* yang berasal dari router *bridge*

Gbr. 7. *Flow Graph* DHCP *Packets* pada Pengujian setelah adanya Rogue DHCP *Server*

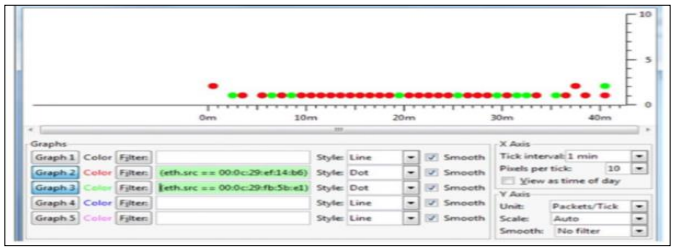
Pada pengujian ini ketika *DHCPDISCOVER* di-*broadcash* oleh *client*, terdapat 2 balasan paket *DHCPOFFER* yang diberikan oleh *DHCP Server* asli dan *Rogue DHCP Server*, terdapat balasan paket *DHCPOFFER* yang pertama berasal dari *DHCP Server* asli dengan sumber *IP* 192.168.100.1, sedangkan paket *DHCPOFFER* dari *Rogue DHCP Server* dengan sumber 192.168.10.10 berada pada posisi ke-2 sehinggga *client* memperoses lebih lanjut konfigurasi alamat

DHCP server asli, sedangkan *DHCPOFFER* dari *Rogue DHCP Server* diabaikan. Kita bisa melihat grafik dari proses pengujian ke-2.



Gbr. 8. *Flow Graph DHCP Packets* pada Gbr. 7. Pengujian ke-2 setelah Adanya *Rogue DHCP Server*

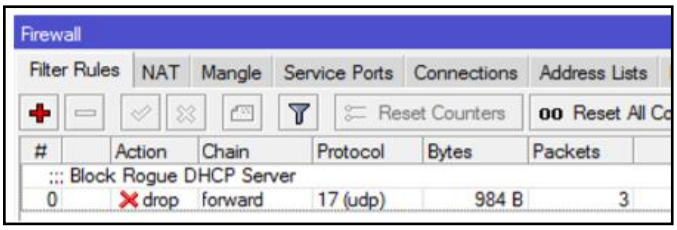
Dari *flow graph DHCP packets* pada pengujian ke-2 setelah adanya *Rogue DHCP Server*, untuk mendapatkan hasilnya yang berupa perbandingan banyaknya konfigurasi berdasarkan *DHCPACK* yang diperoleh *client* dari *DHCP Server* asli maupun *Rogue DHCPACK* dan menghasilkan berupa informasi yang ada dalam bentuk IO Graph yang bisa dilihat pada wireshark yaitu pada menu *statistics*.



Gbr. 9. Grafik perolehan *DHCPACK* pada *client*

d) Konfigurasi pencegahan pada firewall filter

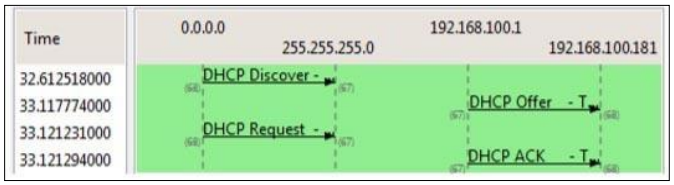
Hasil analisis yang berupa parameter dan pertukaran Rogue DHCP *packets* yang dilakukan, dibuatlah sistem pencegahan menggunakan *firewall filter* yang dapat dijalankan pada brige 1 atau *client* 1 dengan mengaktifkan *filtering packets* yang diarahkan pada fungsi /IP *firewall filter* mikrotik, sehinggah *filtering* pada *router brigde* atu *client* 1 dikonfigurasi pada *firewall filter*. Caranya dengan melakukan konfigurasi firewall filter pada field chain sebagai *forward*, *field source port* adalah kosong, *field destination port* adalah 68 dengan *field protocol* adalah UDP, sedangkan *action* dilakukan adalah *drop*, dimana dengan cara dimasukan smua packet yang melewati (*forward*) pada *router brigde* atau *client* 1 nenuju *protocol* UDP (*Port* DHCP *client* yang melakukan *request*) akan di-*drop* atau dengan kata lain yang berarti Rogue DHCP *packtes* berupa paket DHCPOFFER dan paket DHCPACK yang dikirim kepada DHCP *client* akan ditolak oleh *router brigde*. Ada beberapa langkah yang harus dikonfigurasi.



Gbr. 10. Konfigurasi *firewall filter*

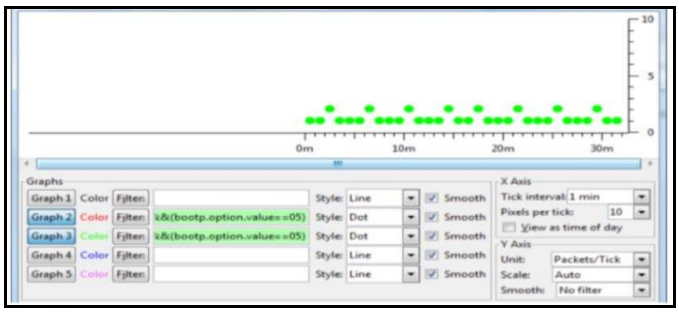
2) Pengujian DHCP Packets setelah adanya pencegahan Rogue DHCP Server

Pengamatan dilalukan dengan IP DHCP yang sudah di terima oleh client sebelumnya dengan perintah IP config yang dijalankan pada *command promt*, kemudian dilakukan dengan cara restart client untuk mendapatkan hasil yang lebih akurat. Pengujian yang dilakukan untuk mengamati proses pertukaran dan parameter dari paket-paket DHCPACK yang didapatkan berdasarkan dari paket DHCPOFFER. Paket DHCPOFFER yang diterima oleh *client* adalah bersumber dari DHCP server asli sedangkan paket DHCPOFFER yang berasal dari Rogue DHCP server di*drop* oleh *firewall filter* pada ether2 *router brigde* yang tak tertangkap oleh wireshark oleh pengamatan. Pertukaran DHCP bisa dilihat dalam bentuk grafik, kita bisa menggunakan *flow grahp* pada *wireshark* yang dapat dilhat pada Gbr. 11.



Gbr. 11. Flow grahp dhcp paket pada pengujian

Hasil akhir pengujian yang dapat berupa perbandingan banyaknya konfigurasi alamat IP Address berdasarkan DHCPACK yang diproleh *client* 1 dari DHCP Server asli dengan Rogue DHCP *Server* setelah adanya pengamatan dan analisis menggunakan *wireshark*. Sehingga kita bisa melihatnya dalam bentuk informasi berupah grafik IO Grahp pada menu statistik pada Gbr. 12.



Gbr. 12. Grafik perolehan DHCP ACK pada client.

Dari tabel konfigurasi alamat IP pada *client* dapat dilihat pada gambar diatas, bahwa pengujian yang dilakukan pada

client mendapatkan DHCPACK dari DHCP *server* asli, sedangkan DHCPACK dari Rogue tidak ada satu pun yang diterima oleh *client.*

V. KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkna hasil pembahasan dan analisis yang telah diuraikan pada bab sebelumnya, dalam penelitian yang berjudul Analisis Paket DHCP Rogue pada Jaringan Komputer Menggunakan *Wireshark* maka dapat disimpulkan sebagai berikut.

1. pada saat DHCP *client* mendapatkan alamat IP yang salah dari Rogue DHCP *server* dengan alamat IP *gateway* ditujuhkan pada Rogue DHCP *server* bisa mengakibatkan menimbulkan celah keamanan jaringan yang disebut dengan *man-in-the-middle attack.*
2. Sistem keamanan jaringan akan menghasilkan pencegahan terhadap adanya Rogue DHCP *Server* yang sebelumnya didekteksi oleh *wireshark* pada jaringan IPV4.
3. Sistem monitoring dan pencegahan terdahap Rogue DHCP *server* dapat menggunakan DHCP *alert* dan *firewall filter* pada mirotik.

B. Saran

1. Implementasi keamanan DHCP Rogue *server* pada jaringan komputer yang memiliki aktifitas atau *traffic* yang tinggi.
2. Dapat dikembangkan dengan menggunakan peralatan atau perangkat jaringan seperti Cisco dan Huawei karena didalam penelitian menggunakan mikrotik.

REFERENSI

[1] Whitten, Jeffrey, L, etc, 2004, System Analysis and Design Methods, The McGraw- Hill Companies, Inc..

[2] Kurniawan, Agus.2012. ***Network Forensics.*** Panduan analisis & investigasi paket data jaringan menggunakan wireshark. Yogyakarta:Andi.

[3] Zulhijah, Siti. Pengertian DHCP. https://izulmen.wordpress.com/dhcp-dynamic-host- configuration-protocol/

[4] Kadafi, februari 2015. DHCP, Paket Rogue DHCP, Server Rogue DHCP. Vol. 2, No. 2.

[5] Guritno, S, Sudaryono, dan Raharja, U. 2011. Theory and Application of IT Research. Yogyakarta : Andi.