

Analisis Rogue DHCP Packets Menggunakan Wireshark Network Protocol Analyzer

Muamar Kadafi*¹, Khusnawi²

^{1,2}Teknik Informatika STMIK AMIKOM Yogyakarta

E-mail: *¹muamar.k@students.amikom.ac.id, ²khusnawi@amikom.ac.id

Abstrak

Rogue DHCP server adalah salah satu pemanfaatan celah keamanan pada mekanisme konfigurasi alamat jaringan menggunakan DHCP. Rogue DHCP server memberikan konfigurasi alamat jaringan yang salah kepada client yang tergabung di dalam jaringan dengan tujuan menciptakan serangan jaringan berupa man in the middle, sehingga dapat menimbulkan ancaman terhadap privasi client yang tergabung di dalam jaringan.

Penelitian difokuskan pada analisis DHCP packets seperti DHCPDISCOVER, DHCPREQUEST, DHCPOFFER, DHCPACK yang melewati sebuah Bridge Mikrotik menggunakan aplikasi Wireshark Network Protocol Analyzer sebelum dan setelah adanya Rogue DHCP server di dalam jaringan DHCP, sehingga dapat diamati bagaimana DHCP server asli dan Rogue DHCP server saling bertukar paket 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, Paket Rogue DHCP, Server Rogue DHCP, Wireshark, Mikrotik

Abstract

Rogue DHCP server is one of exploiting security holes in the mechanism of configuration the network address using DHCP. Rogue DHCP server provides incorrect configuration network address to a client who joined in the network with the aim of creating a network attacks such as "man in the middle", so it can pose a threat to client privacy who joined in the network.

The research focused on the analysis of DHCP packets such as DHCPDISCOVER, DHCPREQUEST, DHCPOFFER, DHCPACK which passes through a Bridge Mikrotik using Wireshark Network Protocol Analyzer application before and after the Rogue DHCP server in the DHCP network, so it can be observed how the original DHCP server and Rogue DHCP Server exchanging packets with a DHCP Client and then make an analysis of the Rogue DHCP packets.

The result of analysis obtained information of parameters that contained in the Rogue DHCP Packets that enabled to build a DHCP network security system in the form of monitoring and prevention of Rogue DHCP server using DHCP Alert combined with Firewall Filter Rule on a Bridge Mikrotik, with result that the system can detect and prevent existence of Rogue DHCP Server in the DHCP based IPv4 network.

Keywords — DHCP, Rogue DHCP Packets, Rogue DHCP Server, Wireshark, Mikrotik

1. PENDAHULUAN

DHCP adalah protokol yang paling banyak digunakan di dunia, baik digunakan dalam jaringan kabel maupun nirkabel seperti pengelolaan jaringan warung internet, jaringan perkantoran, jaringan lab kampus, hotspot pada cafe atau sarana umum, jaringan antar ISP dan tethering atau portable hotspot pada smartphone.

Di antara banyak keunggulan serta keuntungan yang ada, DHCP juga mempunyai beberapa kelemahan. Penggunaan DHCP diperlukan sebuah server untuk bertanggung jawab atas pemberian alamat IP kepada client, 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 yang dapat digunakan oleh network attacker 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 administratif atau bisa disebut server palsu yang digunakan untuk melakukan serangan jaringan dengan menggunakan beberapa 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 di dalam 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. Hal ini dapat digunakan oleh para penyerang untuk mengarahkan dan 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 [1].

Penelitian dilakukan untuk mengetahui bagaimana proses pertukaran paket DHCP beserta parameter yang terkandung di dalamnya, sebelum adanya Rogue DHCP server, setelah adanya Rogue DHCP server, dan setelah adanya pencegahan terhadap Rogue DHCP server di dalam jaringan DHCP berbasis IPv4.

Skenario penelitian dibuat dengan DHCP server asli dibangun di dalam intermediate device berupa bridge mikrotik, 2 buah client menggunakan Windows XP, dan 1 client menggunakan linux backtrack yang difungsikan sebagai Rogue DHCP server menggunakan mesin virtual VMware workstation. Analisis difokuskan pada pengamatan paket DHCP beserta parameter yang ada di dalamnya menggunakan Wireshark network protocol analyzer yang bertujuan untuk menciptakan sistem keamanan jaringan berupa monitoring dan pencegahan terhadap Rogue DHCP server dengan menggunakan fitur yang ada pada mikrotik yaitu DHCP alert yang dikombinasikan dengan Firewall filter.

Tujuan dari penelitian ini dimaksudkan untuk menganalisis Rogue DHCP packets yang disebarkan oleh Rogue DHCP server di dalam jaringan DHCP, serta memberikan solusi pencegahan dan monitoring pada intermediate device yang menghubungkan antara DHCP server dengan DHCP client terhadap Rogue DHCP server di dalam jaringan DHCP, dengan hasil akhir penelitian dapat digunakan sebagai acuan dalam penerapan sistem keamanan jaringan DHCP terhadap Rogue DHCP server serta dapat sebagai referensi untuk pengembangan fitur pada perangkat jaringan intermediate device berupa switch atau bridge dalam pencegahan Rogue DHCP server.

1.1. Tinjauan Pustaka

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[2].

Razaque dan Elleithy meneliti tentang adanya ancaman Rogue DHCP server pada jaringan perangkat mobile. Jika Rogue DHCP server lebih cepat dibanding DHCP server asli ketika pemberian alamat IP kepada client, maka pengguna perangkat mobile yang masuk kedalam jaringan dipastikan mendapat alamat IP yang salah. Selanjutnya, penyerang dapat mengarahkan lalu lintas jaringan dan memodifikasi isi asli dari komunikasi yang ada sehingga ancaman tersebut menimbulkan masalah yang signifikan bagi para pengguna[1].

Dari tinjauan diatas, penelitian difokuskan terhadap analisis DHCP packets dalam struktur jaringan client-server menggunakan Wireshark Network Protocol Analyzer antara DHCP server dengan DHCP client yang dikembangkan dengan adanya Rogue DHCP server di dalam jaringan DHCP pada jaringan IPv4, serta dikembangkan pula pemecahan masalah atas hasil analisis yang dilakukan, dengan pengimplementasian sistem keamanan jaringan yang layak untuk digunakan terhadap ancaman yang diteliti.

1.2. DHCP

Dynamic Host Configuration Protocol (DHCP) digunakan sebagai protokol untuk mengatur pemberian alamat IP secara otomatis pada sebuah jaringan[3].

1.3. DHCP Packets

Percakapan antara DHCP *client* dengan DHCP *server* untuk mendapatkan konfigurasi alamat IP secara otomatis akan berhasil setelah melakukan pertukaran empat paket yaitu DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, dan DHCPACK[2].

1.4. Rogue DHCP Packets

Rogue DHCP server adalah DHCP server pada sebuah jaringan komputer yang tidak memiliki wewenang administratif atau bisa disebut server palsu dengan memberikan alamat IP yang salah kepada DHCP client yang digunakan untuk melakukan serangan jaringan dengan menggunakan beberapa 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 di dalam 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[1].

1.5. Wireshark Network Protocol Analyzer

Wireshark Network Protocol Analyzer adalah tool yang ditujukan untuk penganalisisan paket data jaringan. Wireshark melakukan pengawasan paket secara waktu nyata (real time) dan kemudian menangkap data dan menampilkannya selangkap mungkin. Wireshark bisa digunakan secara gratis karena aplikasi ini berbasis sumber terbuka. Aplikasi wireshark dapat berjalan di banyak platform, seperti linux, windows, dan mac[3].

1.6. Mikrotik

Mikrotik adalah sebuah merek dari sebuah perangkat jaringan, pada awalnya Mikrotik hanyalah sebuah perangkat lunak atau software yang dipasang dalam komputer yang digunakan untuk mengontrol jaringan, tetapi dalam perkembangannya saat ini menjadi sebuah device atau perangkat jaringan dengan harga terjangkau, serta banyak digunakan pada level perusahaan jasa internet[4].

1.7. Firewall Filter

Firewall *filter* berfungsi meningkatkan keamanan jaringan dengan cara menentukan paket data apa saja yang bisa masuk maupun keluar dari jaringan tersebut untuk menentukan paket mana yang akan diterima (*accept*) atau dibuang (*drop*), firewall akan memeriksa *header* dari sebuah IP paket[5].

1.8. DHCP Alert

Router mikrotik memiliki fasilitas DHCP server yang dilengkapi dengan DHCP Alert. Jika terdapat DHCP server yang tidak dikenali dalam jaringan maka DHCP Alert akan mengirimkan pesan ke sistem log dari router[5].

1.9. VMware

VMware adalah suatu perangkat lunak yang dapat menciptakan atau menyimulasikan PC baru, yang disebut mesin virtual. Perangkat keras yang terdapat di dalam mesin virtual sama seperti perangkat yang dipakai PC, dengan kata lain, ada PC di dalam PC[6].

2. METODE PENELITIAN

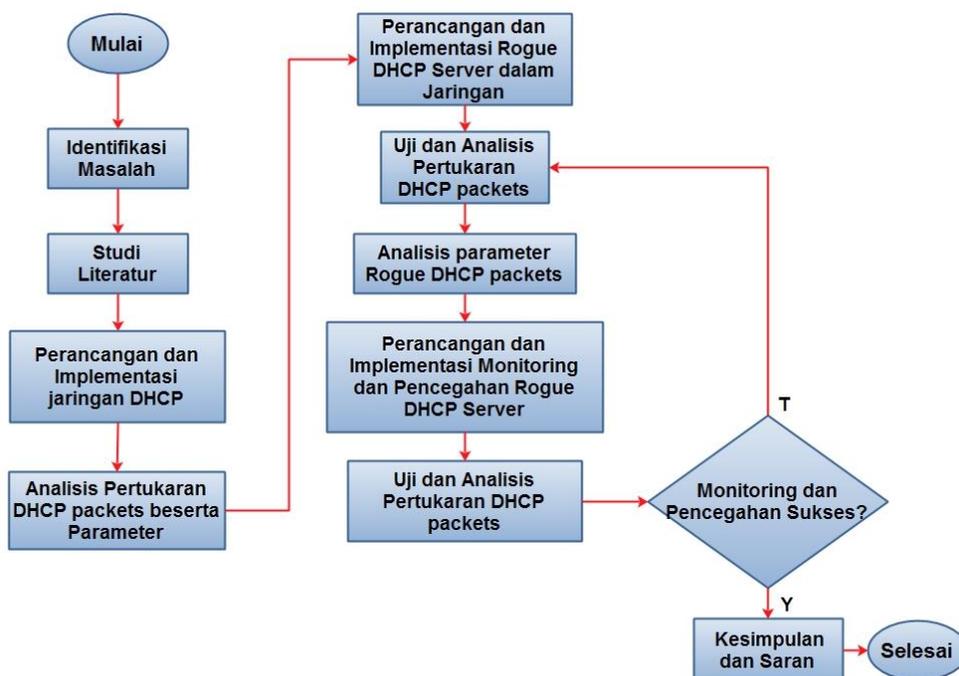
2.1. Analisis Masalah

Terdapat celah keamanan yang ditemukan pada mekanisme pengalamatan IP dengan menggunakan DHCP sehingga dimanfaatkan oleh pihak yang dalam artian “Tidak bertanggungjawab” untuk menciptakan tindakan yang sekiranya merugikan client lain dalam satu jaringan. Salah satu pemanfaatan celah keamanan tersebut adalah dengan membangun DHCP server palsu atau sering disebut Rogue DHCP server yang dalam penelitian ini akan dibangun pada salah satu komputer client yang sebenarnya bertindak hanya sebagai DHCP client dalam jaringan. Akibatnya adalah terdapat dua DHCP server yaitu DHCP server asli dan Rogue DHCP server, yang saling berebut memberikan pelayanan DHCP terhadap client yang tergabung dalam satu jaringan, sehingga apabila client tersebut menerima alamat IP dari Rogue DHCP server, maka akan diberikan alamat yang salah yang dibuat untuk menjadikan aliran data yang diproses oleh client menuju server asli dilewatkan terlebih dahulu ke dalam komputer client yang bertindak sebagai Rogue DHCP server sehingga dapat menimbulkan masalah seperti sniffing lalu-lintas jaringan, serangan masquerading, dan serangan DOS[1] atau dengan kata lain sebuah client yang bertindak sebagai Rogue DHCP server dapat melakukan jenis serangan man-in-the-middle.

Dari hasil analisis masalah yang sudah dipaparkan, penelitian dilakukan untuk menganalisis mekanisme DHCP apabila terdapat Rogue DHCP di dalam sebuah jaringan, dengan lebih fokus terhadap analisis proses pertukaran paket DHCP beserta parameter yang ada di dalamnya. Analisis dilakukan dengan menggunakan skenario jaringan yang telah dibuat.

2.2. Alur Penelitian

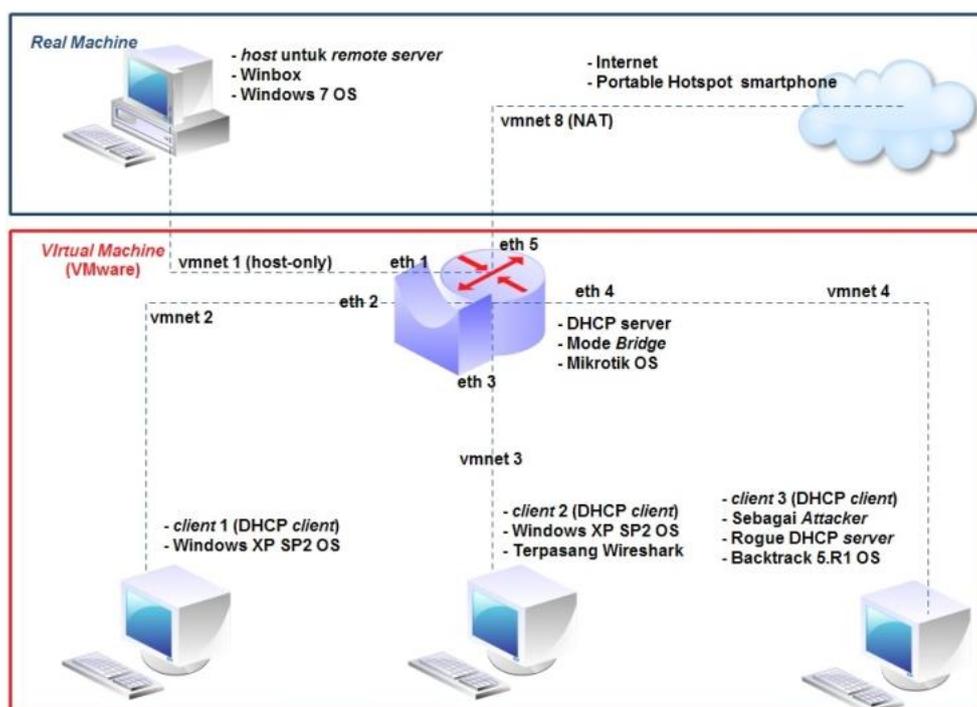
Ada beberapa proses yang harus dilakukan di dalam penelitian ini untuk memperoleh hasil yang diharapkan, dari identifikasi masalah sampai dengan solusi pencegahan serta pemberian kesimpulan dan saran untuk penelitian lebih lanjut. Adapun proses tertuang dalam diagram alur pada gambar dibawah ini:



Gambar 1. Diagram Alur Penelitian

2.3. Topologi Jaringan Penelitian

Adapun topologi jaringan yang akan digunakan di dalam penelitian ini adalah topologi Star, dibangun pada Real Machine yang dikombinasikan dengan Virtual Machine. Jalur komunikasi data antar host di dalam topologi dilewatkan melalui vmnet.



Gambar 2. Rancangan Topologi Jaringan

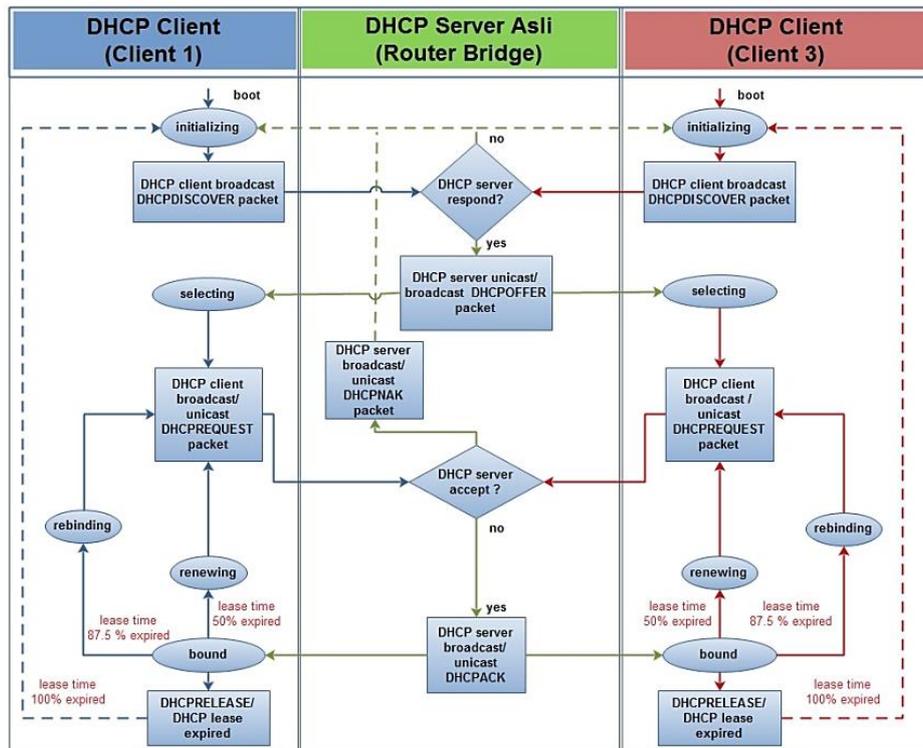
Dari rancangan topologi jaringan yang sudah dibuat, agar topologi berjalan semestinya perlu ditambahkan alamat IP pada setiap host di dalam jaringan tersebut sehingga perlu dibuat tabel rancangan pengalamatan IP agar penelitian lebih mudah untuk dilakukan, serta lebih mudah dalam troubleshooting jaringan. Adapun tabel rancangan pengalamatan IP pada penelitian ditujukan pada table 1.

Tabel 1. Rancangan Alamat IP pada Penelitian

No	Device	Interface	Mac Address	IP Address	Subnet Mask	Gate-way
1	Real PC vmnet 1	NIC	00:50:56:C0:00:01	10.10.10.2	255.255.255.252	-
2	Router Bridge	Eth1	00:0C:29:FB:5B:C3	10.10.10.1	255.255.255.252	-
		Eth2, Eth3, Eth4 (Bridge1)	00:0C:29:FB:5B:E1	192.168.1.1	255.255.255.0	-
		Eth5	00:0C:29:FB:5B:EB	Assingned by DHCP		
3	Client 1	NIC	00:0C:29:48:C5:17	Assingned by DHCP		
4	Client 2	NIC	00:0C:29:FC:DF:58	Assingned by DHCP		
5	Client 3	NIC	00:0C:29:EF:14:B6	Assingned by DHCP		

2.4. Analisis DHCP Packets sebelum Adanya Rogue DHCP Server

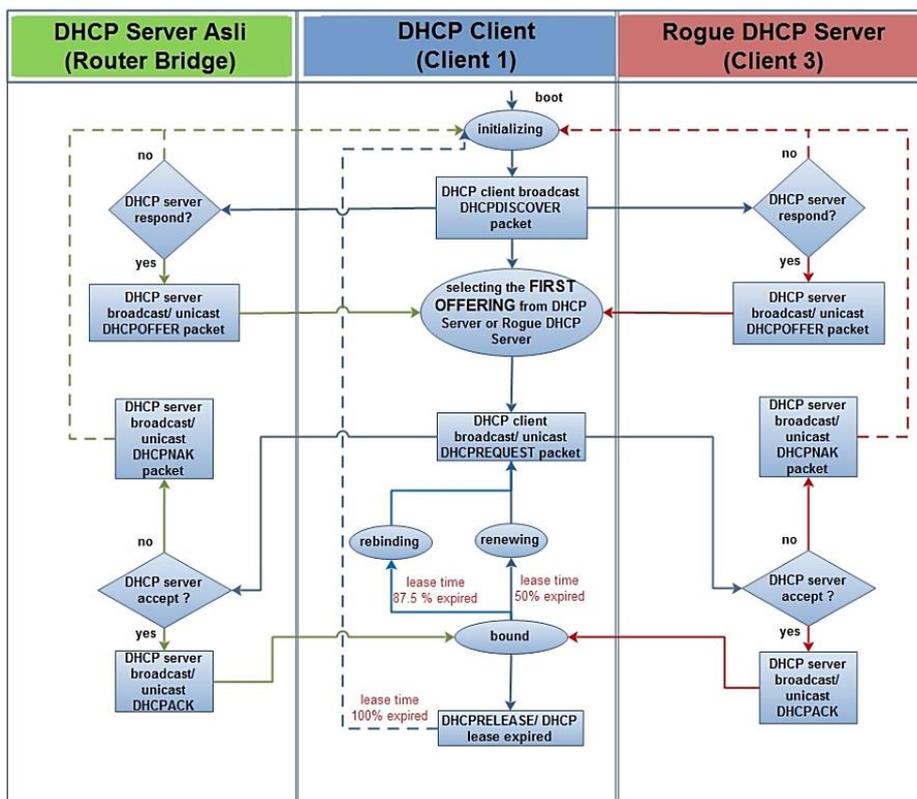
Pada kondisi ini DHCP server memberikan alamat IP kepada 2 (dua) DHCP client yang berada dalam satu jaringan, yang nantinya salah satu dari DHCP client bertindak sebagai Rogue DHCP server. Pada kondisi ini mekanisme pertukaran paket DHCP masih standar/normal, dimana hanya ada 1 (satu) server DHCP di dalam jaringan dengan proses pertukaran paket DHCPDISCOVER, DHCPPOFFER, DHCPREQUEST, dan DHCPACK. Adapun alur paket DHCP yang terjadi dalam kondisi ini ditunjukkan pada Gambar 3.



Gambar 3. Diagram Alur DHCP Packets antara DHCP Server Asli, DHCP Client 1, dan DHCP Client 3

2.5. Analisis DHCP Packets setelah Adanya Rogue DHCP Server

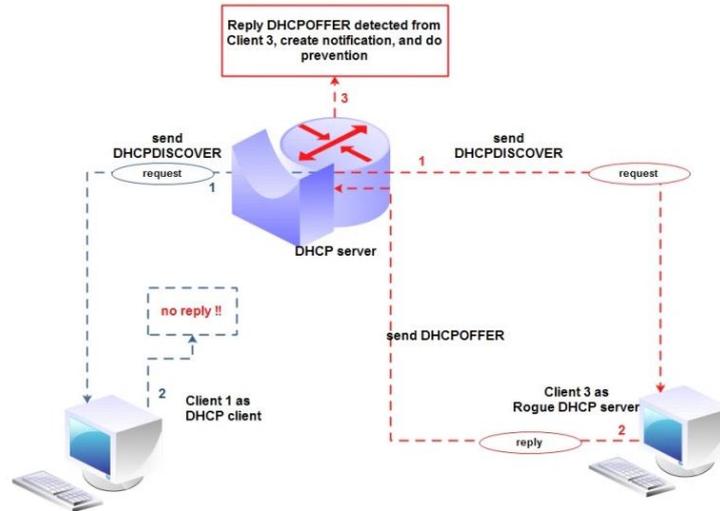
Pada kondisi ini client 3 sudah menjadi Rogue DHCP server yang bertindak sebagai DHCP server palsu, sehingga terdapat 2 (dua) DHCP server dan 1 (satu) DHCP client di dalam jaringan. Kondisi ini mengakibatkan 2 (dua) DHCP server saling berebut memberikan pelayanan terhadap DHCP client, dimana pelayanan tercepat akan dipilih oleh DHCP client. Dalam hal ini, parameter pelayanan tercepat ditujukan pada proses pemberian paket DHCP OFFER oleh DHCP server ketika sebuah client request alamat IP kepada DHCP server dengan mengirimkan paket DHCPDISCOVER secara broadcast. Adapun alur DHCP packets yang terjadi dalam kondisi ini dapat diamati pada Gambar 4.



Gambar 4. Diagram Alur DHCP Packets antara DHCP Server Asli, Client 1, dan Client 3 sebagai Rogue DHCP Server

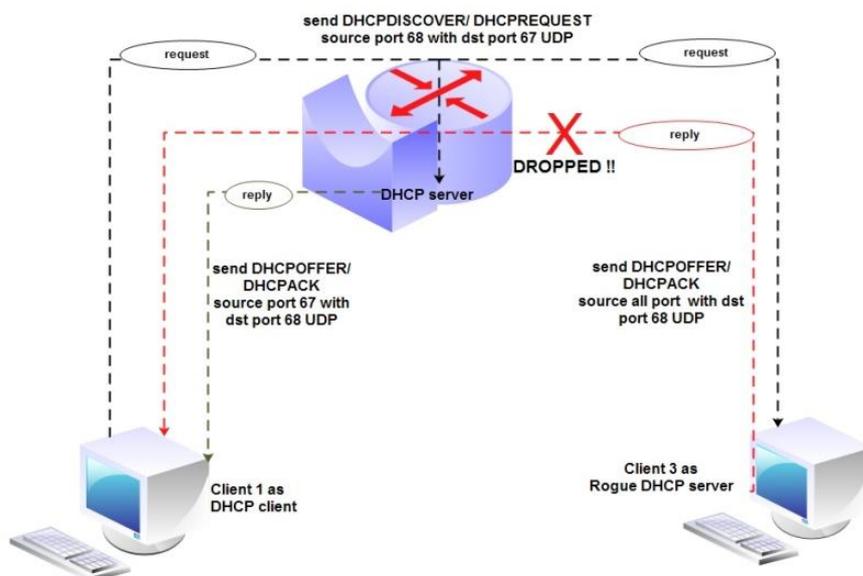
2.6. Analisis Monitoring dan Pencegahan Rogue DHCP Server

Sistem monitoring ini sudah terdapat dalam fitur alert dalam konfigurasi DHCP server pada mikrotik, dimana sebuah DHCP server melakukan request alamat IP kepada seluruh host yang ada di dalam jaringan dengan cara mem-broadcast paket DHCPDISCOVER (dengan asumsi DHCP server menjadi DHCP client). Ketika terdapat host di dalam jaringan yang membalas dengan paket DHCP OFFER, lalu server mencatat informasi sumber alamat mac, alamat IP, dan interface yang digunakan untuk melakukan pesan reply berupa DHCP OFFER tersebut dan memberikan notifikasi ke dalam log server yang dapat juga dikirim ke e-mail administrator jaringan bahwa di dalam jaringan terdapat Rogue DHCP server serta dapat dilakukan tindakan berupa pencegahan sesuai kebijakan yang ditentukan menggunakan sebuah script. Setelah itu, DHCP server asli tidak membalas dengan paket DHCPREQUEST melainkan hanya menerima DHCP OFFER yang diberikan oleh Rogue DHCP server.



Gambar 5. Monitoring Rogue DHCP Server

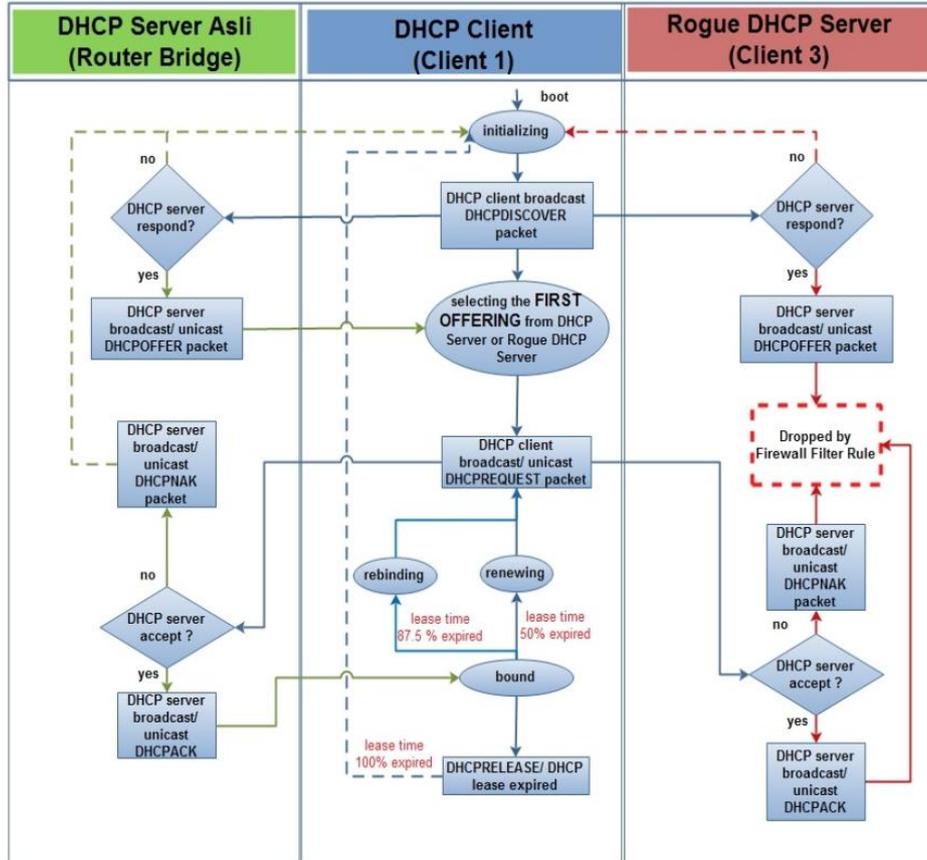
Untuk memaksimalkan sistem monitoring yang ada, perlu adanya pencegahan yang dilakukan terhadap munculnya Rogue DHCP server sebelum berkembang untuk melakukan serangan yang dapat membahayakan jaringan, dengan ditindaklanjuti sesuai kebijakan yang ada. Pencegahan dijalankan ketika sistem monitoring mendapatkan informasi adanya Rogue DHCP server di dalam jaringan. Pencegahan dilakukan berdasarkan hasil analisis terhadap Rogue DHCP packets dengan parameter-parameter yang terkandung di dalamnya. Dari alur Rogue DHCP packets yang telah dianalisis, ancaman terjadi ketika sebuah DHCP client di dalam sebuah jaringan DHCP melakukan broadcast paket DHCPDISCOVER, DHCP server asli dan Rogue DHCP server menerima broadcast dan membalas dengan paket DHCPOFFER terhadap client tersebut. paket DHCPOFFER yang pertama diterima client itu yang akan diproses selanjutnya. Selain pada paket DHCPOFFER ancaman juga dapat terjadi ketika sebuah DHCP client mengirimkan paket DHCPREQUEST pada saat renewing maupun rebinding konfigurasi alamat IP sedangkan dari sisi DHCP server setelah itu membalas dengan mengirimkan paket DHCPACK untuk memberikan konfigurasi alamat IP yang baru kepada DHCP client. Dengan demikian pencegahan dapat dilakukan dengan menutup aktifitas paket DHCP yang berasal dari DHCP Rogue server menggunakan parameter yang diamati sebelumnya. DHCPOFFER dan DHCPACK merupakan paket dengan tipe pesan reply yang berjalan dari DHCP server melalui protokol UDP port 67 menuju port 68 pada DHCP client, dengan demikian solusi yang dapat diberikan adalah menutup lalu-lintas paket yang bersumber dari seluruh port logic Rogue DHCP server yang menuju port 68 pada protokol UDP. Penutupan dilakukan pada seluruh port logic yang berasal dari sumber, dikarenakan jika terdapat manipulasi terhadap port logic dari Rogue DHCP server masih dapat diantisipasi.



Gambar 6. Pencegahan Rogue DHCP Server

2.7. Analisis DHCP Packets setelah Adanya Pencegahan Terhadap Rogue DHCP Server

Pada kondisi ini client 3 masih menjadi Rogue DHCP server yang bertindak sebagai DHCP server palsu, sehingga terdapat 2 (dua) DHCP server dan 1 (satu) DHCP client di dalam jaringan. Kondisi ini mengakibatkan 2 (dua) DHCP server saling berebut memberikan pelayanan terhadap DHCP client, dimana pelayanan tercepat akan dipilih oleh DHCP client. Akan tetapi dalam hal ini Rogue DHCP server tidak dapat mengirimkan paket DHCPOFFER sampai kepada DHCP client, setelah DHCP client mengirimkan permintaan dengan paket DHCPDISCOVER secara broadcast di dalam jaringan, dikarenakan router bridge yang berfungsi sebagai penghubung (intermediate device) antara Rogue DHCP server dengan DHCP client menolak aliran Rogue DHCP packet berupa paket DHCPOFFER yang di-forward-kan melalui router bridge, dan pada kondisi lain Rogue DHCP packet berupa paket DHCPACK juga akan ditolak oleh router bridge, karena parameter untuk pencegahan terhadap Rogue DHCP packet berupa paket DHCPOFFER dan paket DHCPACK adalah sama. Adapun alur DHCP packets yang terjadi dalam kondisi ini dapat diamati pada gambar 7.

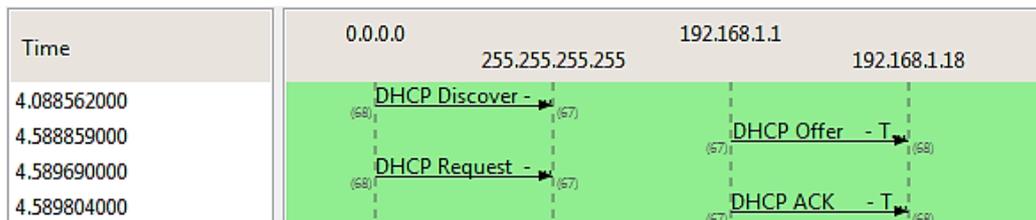


Gambar 7. Diagram Alur DHCP Packets setelah adanya pencegahan terhadap Rogue DHCP Server

3. HASIL DAN PEMBAHASAN

3.1. Pengujian DHCP Packets Sebelum Adanya Rouge DHCP Sever

Pertukaran DHCP packets yang terjadi antara DHCP server asli dengan client 1 pada kondisi sebelum adanya Rogue DHCP server dapat dilihat dalam bentuk grafik yang dibuat menggunakan flow graph pada wireshark, dengan memfilter DHCP packets yang berasal dari streaming ether2 pada router bridge. Adapun grafik dapat dilihat pada gambar 8.



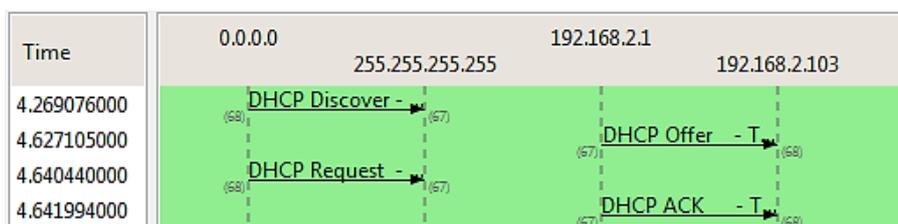
Gambar 8. Flow Graph DHCP Packets pada Client 1 sebelum Adanya Rouge DHCP Server

Pertukaran DHCP packets yang terjadi masih berjalan normal, dengan indikasi client 1 mendapatkan paket DHCPACK yang sekaligus mendapatkan konfigurasi alamat IP yang berasal dari DHCP server asli yaitu berasal dari alamat IP 192.168.1.1.

3.2. Pengujian DHCP Packets Setelah Adanya Rogue DHCP Server

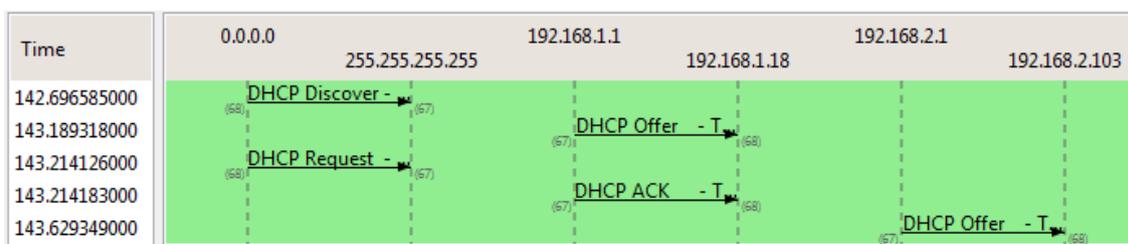
Pengujian dilakukan dengan me-release IP DHCP yang sudah diterima *client 1* sebelumnya dengan sintak ipconfig /release yang dijalankan pada command prompt, lalu merestart PC client 1 berulang sampai 40 kali, untuk mendapatkan hasil data yang lebih valid. Diambil 2 sampel dari 40 pengujian dimana paket DHCPACK didapatkan berdasarkan paket DHCPOFFER pertama yang berasal dari Rogue DHCP server (pada pengujian ke-1) dan paket DHCPACK didapatkan berdasarkan paket DHCPOFFER pertama yang berasal dari DHCP server asli (pada pengujian ke-3) dan untuk diamati proses pertukaran dan parameter paketnya.

Pada pengujian ke-1 pertukaran DHCP packets hanya terjadi antara Rogue DHCP server dengan client 1 yang dapat dilihat dalam bentuk grafik, dibuat menggunakan flow graph pada wireshark, dengan memfilter DHCP packets pada pengujian ke-1 yang berasal dari streaming ether2 router bridge . Adapun grafik dapat dilihat pada gambar 9.



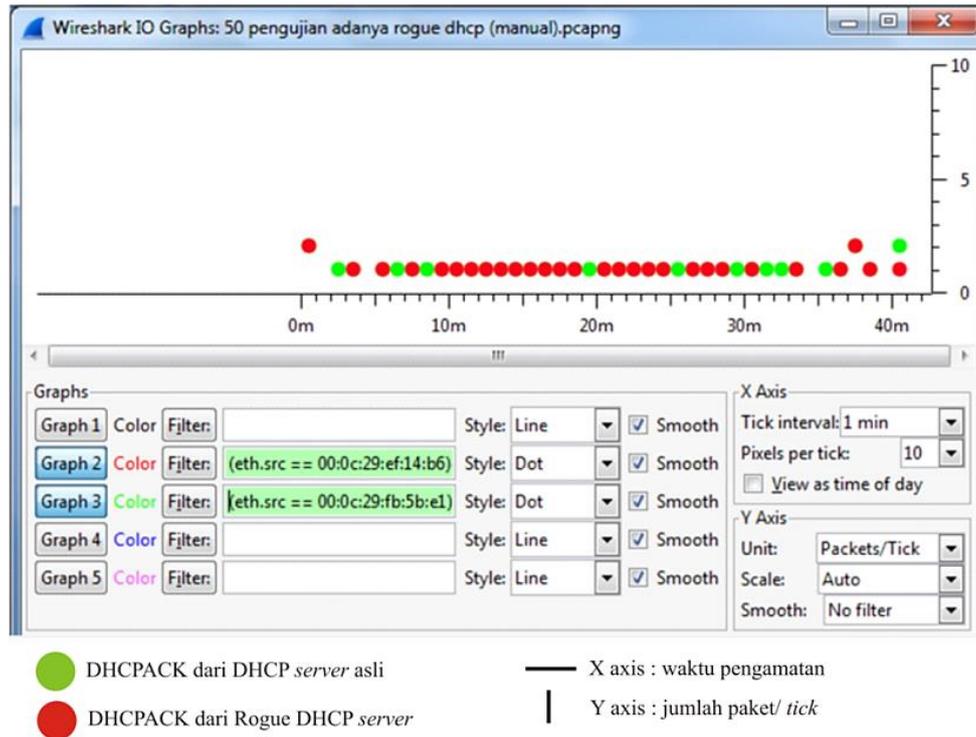
Gambar 9. Flow Graph DHCP Packets pada Pengujian ke-1 setelah Adanya Rogue DHCP Server

Pada pengujian ke-3 Ketika DHCPDISCOVER di-broadcast oleh client 1, terdapat 2 balasan paket DHCPOFFER yang diberikan oleh DHCP server asli dan Rogue DHCP server, akan tetapi balasan paket DHCPOFFER yang pertama berasal dari DHCP server asli dengan sumber alamat IP 192.168.1.1, sedangkan paket DHCPOFFER dari Rogue DHCP server dengan sumber alamat IP 192.168.2.1 berada pada posisi kedua, sehingga client 1 memproses lebih lanjut paket DHCPOFFER yang pertama diterima sampai memperoleh paket DHCPACK yang berisi konfigurasi alamat IP DHCP dari DHCP server asli, sedangkan DHCPOFFER dari Rogue DHCP server diabaikan. Adapun grafik dapat dilihat pada gambar 10.



Gambar 10. Flow Graph DHCP Packets pada Pengujian ke-3 setelah Adanya Rogue DHCP Server

Untuk mendapatkan hasil berupa perbandingan banyaknya perolehan konfigurasi alamat IP berdasarkan DHCPACK yang diperoleh client 1 dari DHCP server asli maupun Rogue DHCP server, maka dari sejumlah pengujian, dilakukan analisis menggunakan wireshark terhadap paket DHCPACK serta diolah untuk menghasilkan informasi berupa grafik menggunakan IO Graph pada menu statistics.



Gambar 11. Grafik Perolehan DHCPACK pada Client 1

Dari 40 pengujian yang sudah dilakukan, hasil yang diperoleh dengan melihat parameter pada y axis dan x axis dapat diamati pada tabel 2.

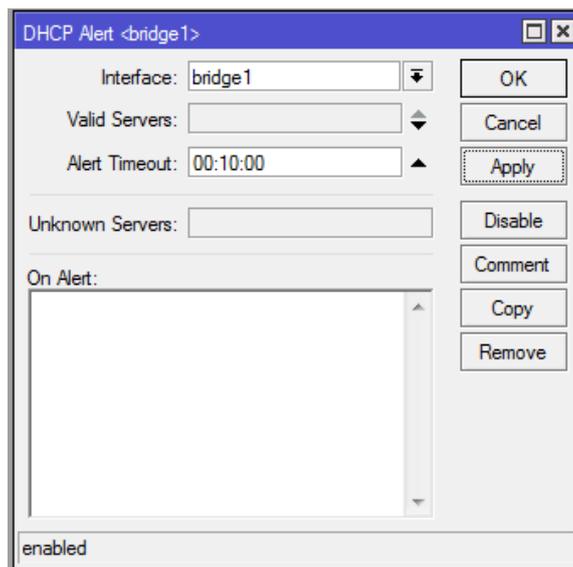
Tabel 2. Perolehan Konfigurasi Alamat IP pada Client 1

Simbol	Uraian	Jumlah
●	DHCP <i>client (client 1)</i> mendapatkan DHCPACK sekaligus mendapatkan konfigurasi alamat IP dari DHCP <i>server</i> asli	10 kali
●	DHCP <i>client (client 1)</i> mendapatkan DHCPACK sekaligus mendapatkan konfigurasi alamat IP dari Rogue DHCP <i>server</i>	30 kali

Dari tabel perolehan konfigurasi alamat IP, dapat dilihat bahwa 30 dari 40 pengujian yang dilakukan, client 1 mendapatkan paket DHCPACK dari Rogue DHCP server, sehingga diindikasikan bahwa ketika client 1 melakukan release IP dan merestart sistem operasi, presentase kemungkinan mendapatkan alamat IP dari Rogue DHCP server lebih banyak dibandingkan mendapatkan alamat IP dari DHCP server asli. Dengan demikian Rogue DHCP server sangat kuat dalam menginterupsi pertukaran paket DHCP sehingga sangat membahayakan bagi jaringan DHCP terutama bagi client yang tergabung di dalam jaringan. Selanjutnya akan dianalisis lebih lanjut parameter-parameter penting yang terkandung di dalam Rogue DHCP packets yang sudah tertangkap sebagai acuan dalam pembuatan solusi keamanan jaringan berupa monitoring dan pencegahan.

3.3. Konfigurasi dan Hasil Monitoring dengan Fitur DHCP Alert

Dari hasil analisis parameter dan analisis pertukaran Rogue DHCP *packet* yang dilakukan, pembuatan sistem monitoring dapat menggunakan Fitur DHCP alert yang terdapat pada konfigurasi DHCP server pada menu /IP DHCP server di dalam mikrotik. Adapun konfigurasi yang dilakukan pada fitur alert dapat dilihat pada gambar 12.



Gambar 12. Konfigurasi Fitur DHCP Alert pada DHCP Server Asli di Mikrotik

Adapun hasil dari monitoring menggunakan Fitur DHCP alert adalah memberitahukan pada sistem log bahwa terdapat Rogue DHCP server di dalam jaringan dengan alamat mac 00:0C:29:EF:14:B6 dan alamat IP 192.168.2.1 dimana alamat tersebut adalah alamat mac dan IP dari client 3 yang dapat dilihat pada gambar 13.

Dec/20/2014 10:49:38	system info	DHCP alert changed by admin
Dec/20/2014 11:11:20	dhcp critical error	dhcp alert on bridge 1: discovered unknown dhcp server, mac 00:0C:29:EF:14:B6, ip 192.168.2.1

Gambar 13. Notifikasi pada Log Hasil Monitoring

3.4. Konfigurasi Pencegahan Menggunakan Firewall Filter

Dari hasil analisis parameter dan analisis pertukaran Rogue DHCP *packet* yang dilakukan, pembuatan sistem pencegahan menggunakan firewall filter dapat dijalankan dalam bridge dengan mengaktifkan filtering paket yang diarahkan pada fungsi /IP Firewall Filter di dalam mikrotik, sehingga filtering pada router bridge dapat dikonfigurasi pada firewall filter. Konfigurasi firewall filter dengan memberikan nilai pada field chain adalah forward, field source port adalah kosong, field destination port adalah 68 dengan field protocol adalah UDP, sedangkan action yang dilakukan adalah drop, dimaksudkan bahwa semua paket yang melewati (forward) router bridge menuju port 68 pada protokol UDP (port DHCP client yang melakukan request) akan di-drop atau dengan kata lain tidak akan diteruskan melewati router bridge, yang berarti Rogue DHCP packets berupa paket DHCP OFFER dan paket DHCP ACK yang dikirim kepada DHCP client akan ditolak oleh router bridge. Konfigurasi dapat dilihat pada gambar 14.

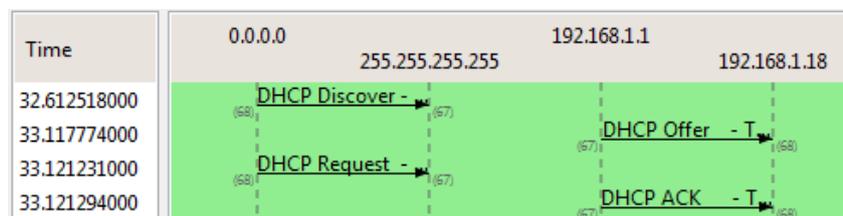
#	Action	Chain	Protocol	Bytes	Packets
0	drop	forward	17 (udp)	984 B	3

Gambar 14. Konfigurasi Firewall Filter Rule

3.5. Pengujian DHCP Packets setelah Adanya Pencegahan terhadap Rogue DHCP Server

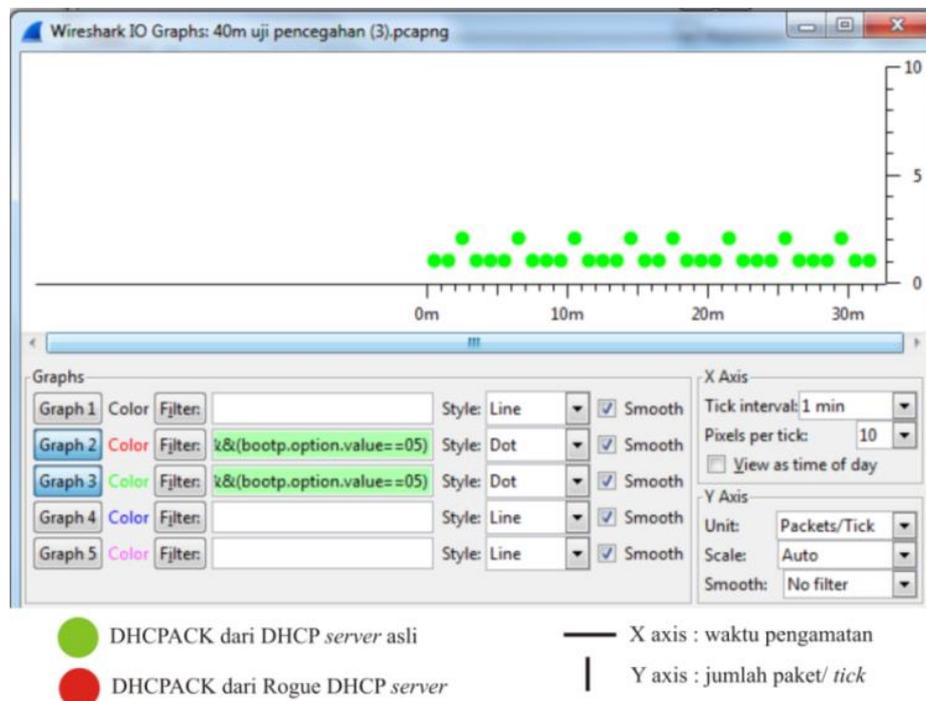
Pengujian dilakukan dengan me-release IP DHCP yang sudah diterima *client 1* sebelumnya dengan sintak `ipconfig /release` yang dijalankan pada command prompt, lalu merestart PC client 1 berulang sampai 40 kali, untuk mendapatkan hasil data yang lebih valid. Diambil 1 sampel dari 40 pengujian untuk diamati proses pertukaran dan parameter pakatnya, dimana paket DHCPACK didapatkan berdasarkan paket DHCPOFFER pertama. Dari 40 pengujian yang dilakukan, hanya ada satu paket DHCPOFFER tiap pengujian yang diterima oleh client 1 yaitu paket yang berasal dari DHCP server asli, sedangkan paket DHCPOFFER yang berasal dari Rogue DHCP server di-drop oleh firewall filter pada ether4 router bridge sehingga tidak tertangkap oleh wireshark pada pengamatan ini.

Pertukaran DHCP packets dapat dilihat dalam bentuk grafik, dibuat menggunakan flow graph pada wireshark, dengan memfilter DHCP packets dari 1 sampel pengujian yaitu pada pengujian ke-1 yang berasal dari streaming ether2 router bridge. Adapun grafik dapat dilihat pada gambar 15.



Gambar 15. Flow Graph DHCP Packets pada Pengujian ke-1 setelah Pencegahan

Hasil akhir pengujian yang didapat berupa perbandingan banyaknya perolehan konfigurasi alamat IP berdasarkan DHCPACK yang diperoleh client 1 dari DHCP server asli dengan Rogue DHCP server. Dari sejumlah pengujian, dilakukan analisis menggunakan wireshark terhadap paket DHCPACK serta diolah untuk menghasilkan informasi berupa grafik menggunakan IO Graph pada menu statistics.



Gambar 16. Grafik Perolehan DHCPACK pada Client 1 Setelah Pencegahan

Dari 40 pengujian yang sudah dilakukan, hasil yang diperoleh dengan melihat parameter pada y axis dan x axis dapat diamati pada tabel 3.

Tabel 3. Perolehan Konfigurasi Alamat IP pada Client 1 Setelah Pencegahan

Simbol	Uraian	Jumlah
	DHCP <i>client</i> (<i>client 1</i>) mendapatkan DHCPACK sekaligus mendapatkan konfigurasi alamat IP dari DHCP <i>server</i> asli	40 kali
	DHCP <i>client</i> (<i>client 1</i>) mendapatkan DHCPACK sekaligus mendapatkan konfigurasi alamat IP dari Rogue DHCP <i>server</i>	0 kali

Dari tabel perolehan konfigurasi alamat IP pada client 1 dapat dilihat bahwa 40 dari 40 pengujian yang dilakukan, client 1 mendapatkan paket DHCPACK dari DHCP server asli, sedangkan paket DHCPACK dari Rogue DHCP server tidak ada satu pun yang diterima oleh client 1, sehingga diindikasikan bahwa pencegahan terhadap Rogue DHCP server menggunakan firewall filter berjalan dengan baik.

4. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan dapat diambil kesimpulan sebagai berikut:

1. Pertukaran Rogue DHCP *packets* menggunakan komunikasi paket-paket DHCP pada umumnya yaitu menggunakan paket DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, dan DHCPACK.
2. Rogue DHCP server menginterupsi pertukaran paket DHCP menggunakan Rogue DHCP *packets* berupa paket DHCPOFFER dan paket DHCPACK.
3. Ketika DHCP *client* melakukan booting di dalam jaringan DHCP yang terdapat Rogue DHCP *server* aktif, maka akan terjadi 2 kemungkinan yaitu mendapatkan konfigurasi alamat IP yang benar dari DHCP *server* asli atau bisa jadi mendapatkan konfigurasi alamat IP yang salah dari Rogue DHCP *server*.
4. Ketika DHCP *client* mendapatkan alamat IP yang salah dari Rogue DHCP *server* dengan alamat IP *gateway* ditujukan pada Rogue DHCP *server*, maka akan menimbulkan serangan jaringan *man-in-the-middle*.
5. Solusi keamanan jaringan berupa monitoring dan pencegahan terhadap Rogue DHCP server dapat dilakukan menggunakan fitur yang ada pada mikrotik yaitu DHCP Alert dan Firewall Filter Rule, yang diaktifkan pada intermediate device.
6. Hasil yang diperoleh bahwa sistem keamanan jaringan yang dibangun dapat mendeteksi dan mencegah adanya Rogue DHCP Server di dalam jaringan DHCP berbasis IPv4.

5. SARAN

Penelitian dapat dikembangkan dengan melakukan implementasi skenario pada real machine (mesin nyata), dan dapat dikembangkan dengan melakukan implementasi pada topologi secara umum, seperti menggantikan bridge dengan sebuah switch yang secara umum lebih banyak digunakan pada infrastruktur jaringan lokal, serta membangun DHCP server di luar intermediate device tersebut.

DAFTAR PUSTAKA

- [1] Razaque, A., Elleithy, K., 2012, Discovery of Malicious Attacks to Improve Mobile Collaborative Learning (MCL). *International Journal of Computer Networks & Communications (IJCNC)*, Vol 4, No 4, Hal 21-40.
 - [2] 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.
 - [3] Kurniawan, A., 2012, *Network Forensics: Panduan Analisis & Investigasi Paket Data Jaringan Menggunakan Wireshark*, Andi, Yogyakarta.
 - [4] Athailah, 2013, *Mikrotik untuk Pemula*, Mediakita, Jakarta.
 - [5] Towidjojo, R., 2013, *Mikrotik Kungfu Kitab 2*, Jasakom.
 - [6] Sugiri, Saputro, H., 2006, *VMware Solusi Menjalankan Beberapa Sistem Operasi*. Andi, Yogyakarta.
-