Filter Paket Berdasarkan *Differentiated Services Code Point* untuk Pencegahan Serangan DHCP *Starvation*

Packet Filtering Based on Differentiated Services Code Point for DHCP Starvation Attacks Prevention

Sarip[1)], Arief Setyanto[2)]

[1,2]Departemen Computer Engineering Universitas AMIKOM Yogyakarta
Jl. Ring Road Utara, Ngringin, Condongcatur, Sleman, Daerah Istimewa Yogyakarta 55281, Telp. (0274) 884201

syerif.solver@gmail.com[1)], arief_s@amikom.ac.id[2)]

Diterima: 11 Juni 2019 || Revisi: 5 Agustus 2019 || Disetujui: 17 September 2019

Abstrak – Pemanfaatan internet saat ini telah menjadi kebutuhan. Media yang paling umum digunakan untuk terkoneksi ke internet adalah jaringan Wireless LAN. Untuk kemudahan akses ke jaringan, layanan DHCP menjadi fitur standar yang harus ada karena pengguna awam tidak perlu lagi memikirkan tentang tata cara konfigurasi alamat IP. Semua telah dilakukan secara otomatis oleh layanan DHCP. Ternyata terdapat ancaman keamanan terhadap layanan DHCP, yaitu serangan DHCP *Starvation* yang dapat menghabiskan ketersediaan alamat IP pada layanan DHCP, sehingga pengguna tidak dapat lagi melakukan konfigurasi alamat IP secara otomatis. Peneliti melakukan pencegahan terhadap serangan DHCP *Starvation* melalui beragam metode. Seperti otentikasi, kriptografi, dan *machine learning*, namun isu efektivitas dan efisiensi masih membuka peluang penelitian lebih lanjut. Dalam penelitian ini, metode filter paket berdasarkan kode DSCP yang diterapkan pada sistem *Netfilter* yang digunakan untuk melakukan pencegahan serangan DHCP *Starvation*. Metode ini terbukti sangat efektif dalam melakukan pencegahan dan lebih efisien ketika diterapkan pada jaringan *wireless* skala kecil di sebuah kantor atau kafe yang menyediakan koneksi internet.

Kata Kunci: DHCP, DHCP *Starvation*, DSCP, *Netfilter*, *Wireless* LAN

Abstract *– The use of the internet today has become a necessity, the most commonly used media to connect to the internet is a Wireless LAN network. For easy access to the network, DHCP service become a standard feature that must exist, because ordinary users no longer need to think about procedures for configuring IP addresses, all of which have been done automatically by the DHCP service. But it turns out that there is a security threat to DHCP service, namely DHCP Starvation attacks that can be exhausting the availability of IP addresses in DHCP service so that the configuration of IP address automatically can no longer be done on the client. Various methods such as authentication, cryptography, and machine learning are used by researchers in preventing DHCP Starvation attacks, but the issue of effectiveness and efficiency still opens up further research opportunities. In this research, packet filtering methods based on DSCP code applied to the Netfilter system are used to do prevention of DHCP Starvation attacks, this method has proven to be very effective in making prevention and more efficient when applied on small scale wireless networks such as at office networks and internet cafe.*

Keywords: *DHCP, DHCP Starvation, DSCP, Netfilter, Wireless LAN*

PENDAHULUAN

Layanan *Dynamic Host Configuration Protocol* (*DHCP*) memberikan kemudahan bagi pengguna awam yang akan terkoneksi baik ke jaringan lokal maupun ke jaringan internet. Hal ini dimungkinkan karena layanan *DHCP* akan melakukan konfigurasi alamat *Internet Protocol* (*IP*) yang dibutuhkan oleh setiap *client* secara otomatis (Droms & Lemon, 2003).

Pada awal implementasi protokol *DHCP*, interaksi antara *DHCP client* dan *DHCP server* mulai dari pengiriman paket *DHCP Discover*, *Offer*, *Request* dan *ACK* atau yang umum disingkat dengan istilah "*DORA*" (Duangphasuk dkk., 2011) nampak tidak ada masalah. Akan tetapi, dalam penelitian yang dilakukan oleh Mukhtar dkk. (2012) mengungkapkan bahwa ketersediaan layanan *DHCP* dapat terganggu dengan adanya serangan *DHCP Starvation* yang merupakan salah satu jenis teknik dalam *Denial of Service* (DoS). Serangan *DHCP Starvation* dilakukan dengan mengirimkan paket *DHCP DISCOVER* sebanyak mungkin, sehingga *DHCP server* akan kehabisan persediaan alamat *IP* dan mengakibatkan *client* yang sah tidak akan dapat melakukan konfigurasi alamat *IP* secara otomatis (Umasuthan, 2016; Naaz & Badroo, 2016). Menurut Stewart dkk. (2005), salah satu ancaman dalam keamanan komunikasi dan informasi

secara umum adalah masalah ketersediaan (*availability*) layanan. Zhang & Chen (2016) menjelaskan bahwa awal protokol dibuat, belum mempertimbangkan masalah keamanan, karena fokus utama baru sebatas pada fungsi dari protokol tersebut.

Berkembangnya penggunaan jaringan *Wireless LAN* (*WLAN*) terutama jaringan *wireless* skala kecil seperti yang diimplementasikan di sebuah kantor atau kafe internet yang terdiri atas 20 sampai 30 komputer (Shuai dkk., 2016), menyebabkan fokus penelitian terkait serangan terhadap layanan *DHCP* cenderung mengarah pada pencarian solusi efektif dan efisien dalam pencegahan serangan *DHCP Starvation* di lingkungan jaringan *WLAN* (Hubballi & Tripathi, 2017). Penyebab lain adalah penelitian di lingkungan jaringan *Local Area Connection* (*LAN*) terkait masalah pencegahan serangan terhadap layanan *DHCP* telah cukup komprehensif dilakukan oleh banyak peneliti, salah satunya adalah Bhaiji (2007) yang menggunakan fitur *Port Security* pada perangkat *cisco* untuk membatasi jumlah *frame* berdasarkan alamat *Media Access Control* (*MAC)* pada setiap *port switch* untuk mencegah serangan *DHCP Starvation* di jaringan *LAN*. Berbeda halnya dengan jaringan *WLAN* yang tidak memiliki *port* fisik seperti pada *switch* atau *bridge*, sehingga perlakuan pencegahannya akan berbeda.

Terdapat beberapa metode yang umum diusulkan oleh para peneliti, baik dalam rangka melakukan deteksi maupun pencegahan terhadap serangan *DHCP Starvation*. Hal-hal yang akan menjadi fokus peninjauan (*review*) dari metode-metode yang diusulkan tersebut adalah masalah efektivitas pencegahan dan masalah efisiensi ketika diterapkan pada jaringan *wireless* skala kecil.

Metode keamanan komunikasi *DHCP* menggunakan teknik kriptografi (Younes, 2017) dan otentikasi berbasis *One Time Password* (*OTP*) (Shete dkk., 2018) merupakan sebagian dari solusi yang diusulkan, metode tersebut efektif digunakan dalam proses pencegahan serangan *DHCP Starvation*, namun kurang efisien ketika diterapkan, karena mengharuskan adanya penambahan aplikasi baik di sisi *server* maupun di sisi *client*. Hal lain yang juga menjadi perhatian adalah masalah spesifikasi perangkat *server* yang cukup tinggi, sehingga kurang efisien jika diterapkan pada jaringan *wireless* skala kecil.

Metode lain yang diusulkan oleh peneliti adalah deteksi anomali pada layanan *DHCP* dengan metode *Machine Learning* (Tripathi & Hubballi, 2018). Metode yang digunakan cukup efektif dalam mendeteksi jenis serangan terhadap layanan *DHCP*. Salah satunya adalah serangan *DHCP Starvation*, namun dalam penelitian yang dilakukan baru sebatas melakukan deteksi dan belum sampai pada tahap pencegahan. Proses deteksi serangan membutuhkan spesifikasi perangkat yang cukup tinggi karena harus mengolah *dataset* yang dihasilkan dari komunikasi *DHCP* yang sangat banyak, sehingga kurang efisien ketika diimplementasikan pada jaringan *wireless* kecil.

Deteksi *malicious client* dilakukan dengan memanfaatkan protokol *Internet Control Message Protocol* (*ICMP*) untuk kebutuhan deteksi *client* yang melakukan penyerangan terhadap layanan *DHCP*, merupakan metode yang diusulkan oleh Yaibuates & Chaisricharoen (2017) yang kemudian dilanjutkan lagi pada tahun berikutnya oleh Yaibuates dkk. (2018) dengan menambahkan fitur pemulihan kembali alamat *IP* (*IP Address Recovery*) pada layanan *DHCP*, namun tetap dengan konsep pendeteksian yang sama seperti sebelumnya. Metode ini memiliki celah dalam masalah efektivitas deteksi yang memungkinkan terjadinya kesalahan deteksi karena umumnya *client* menerapkan *firewall* untuk keamanan, termasuk di dalamnya aturan blokir terhadap protokol *ICMP*, sehingga *client* yang sah tidak akan memberikan balasan saat dikirimkan paket *ICMP* dan *client* tersebut akan dideteksi sebagai penyerang.

Kelemahan-kelemahan metode sebelumnya dapat diperbaiki dengan menerapkan filter paket berdasarkan *Differentiated Services Code Point* (*DSCP*). Kode DSCP yang melekat pada sebuah paket dapat dimanfaatkan untuk melakukan klasifikasi dan pembatasan trafik (Breabăn dkk., 2017). Pada penelitian ini *DSCP* digunakan untuk melakukan filter paket *DHCP* dengan tujuan mencegah serangan *DHCP Starvation*.

Penerapan filter paket *DHCP* memanfaatkan *DSCP* diharapkan dapat mencegah dampak yang ditimbulkan oleh serangan *DHCP Starvation* secara efektif. Metode ini juga diharapkan lebih efisien sehingga dapat diimplementasikan pada jaringan *wireless* skala kecil yang saat ini banyak digunakan di tengah-tengah masyarakat, seperti pada institusi area perkantoran dan kafe *internet*.

METODOLOGI PENELITIAN

Masalah penelitian yang diteliti telah jelas, yakni dampak yang ditimbulkan oleh serangan *DHCP Starvation* terhadap layanan *DHCP*, sehingga fokus dalam penelitian ini adalah penemuan solusi terhadap

gangguan dari serangan *DHCP Starvation* pada layanan *DHCP* di jaringan *WLAN*. Oleh karena itu, pendekatan penelitian yang digunakan adalah penelitian kuantitatif. Jenis atau desain penelitian yang tepat digunakan adalah penelitian eksperimen, sedangkan lokasi penelitian eksperimen dilakukan pada lab. jaringan SMK Negeri 1 Palopo dalam rentang waktu bulan April hingga bulan Mei 2019. Keterbatasan perangkat pendukung penelitian berakibat pada kesulitan membentuk kelompok kontrol dan kelompok eksperimen secara terpisah, sehingga jenis penelitian eksperimen yang digunakan adalah *Quasi-Experimental* dengan model desain *Time-Series* (Marczyk dkk., 2005).

Alur penelitian yang digunakan pada penelitian ini mengikuti alur penelitian kuantitatif pada umumnya, yaitu:

1. Studi Pustaka

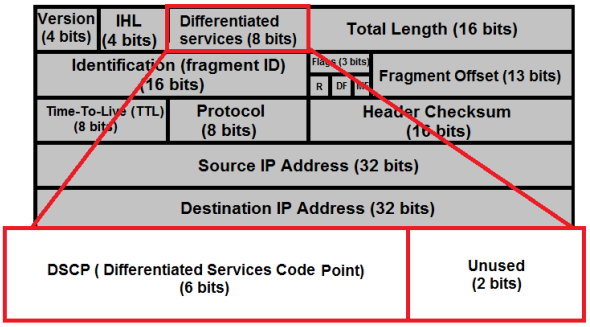
Studi pustaka (*literature review*) dilakukan untuk menemukan celah penelitian (*research gap*), sehingga penelitian yang dilakukan mengandung nilai orisinalitas yang membedakan dari penelitian sebelumnya. Ada dua hal yang dilakukan pada tahap ini.

(a) Identifikasi Masalah

Seperti yang telah dijelaskan pada bagian pendahuluan, masalah efektivitas dan efisiensi pencegahan serangan *DHCP Starvation* menjadi pembeda dari penelitian sebelumnya dan sekaligus menjadi rumusan masalah yang akan dijawab dalam penelitian ini. Definisi efektivitas yang dimaksud dalam penelitian ini adalah apakah metode yang digunakan terbukti efektif dalam melakukan pencegahan terhadap serangan *DHCP Starvation*, tanpa kendala yang dapat memengaruhi efektivitasnya, seperti adanya *firewall* di sisi *client*. ementara definisi efisiensi yang dimaksud adalah apakah dibutuhkan tambahan aplikasi baik di sisi *server* atau di sisi *client* sehingga dalam beberapa kondisi hal itu justru menjadi sulit untuk diimplementasikan dalam kondisi nyata.

(b) Merumuskan Metode

Mungkin belum terpikirkan sebelumnya bahwa komponen *Differentiated Services Code Point* (*DSCP*) yang umumnya baru sebatas digunakan untuk keperluan manajemen prioritas paket (Custura dkk., 2018), sebenarnya dapat pula digunakan untuk klasifikasi paket dengan tujuan yang lain, misalnya untuk filter paket *DHCP*. Tampak pada Gambar 1 bahwa *DSCP* terletak pada *Header IP* yang juga akan dijumpai pada setiap paket *DHCP* yang dikirimkan saat komunikasi protokol *DHCP* terjadi. Kode *DSCP* terdiri dari 6 bit, sehingga kode yang dapat digunakan bernilai dari angka 0 hingga 63 (Barik dkk., 2018).



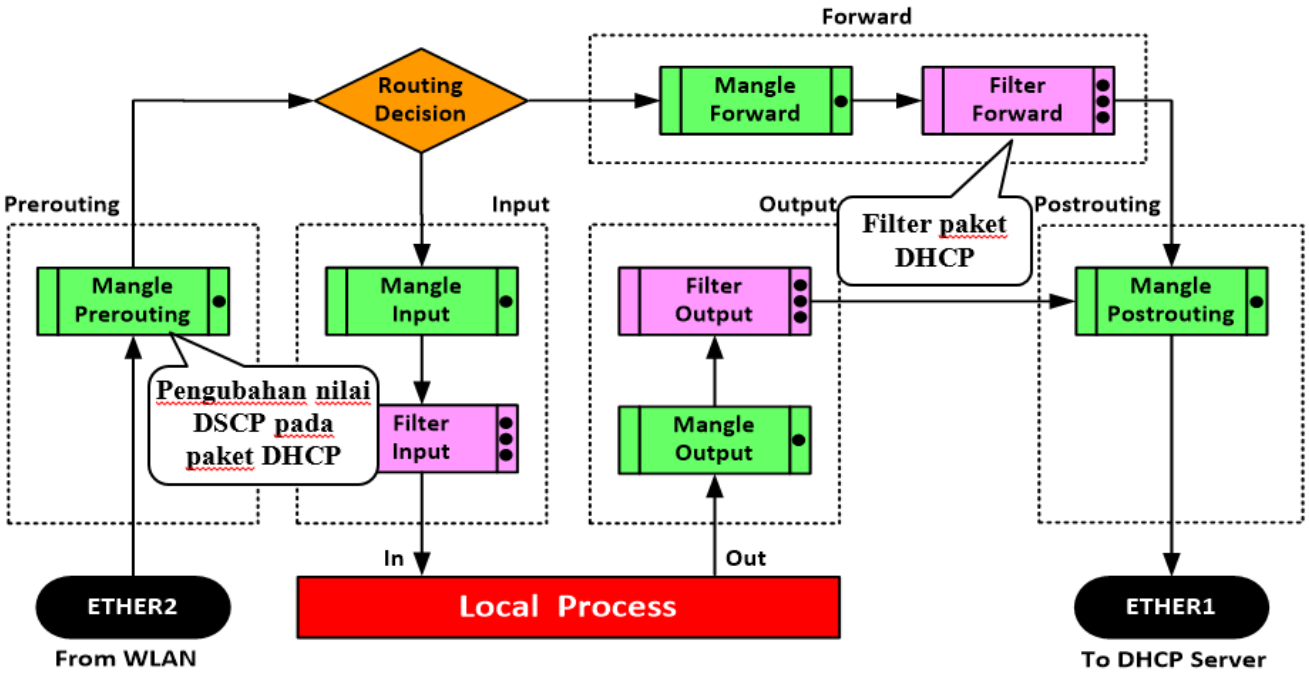
Gambar 1 Posisi DSCP pada Header IP

Telah dibuat standardisasi klasifikasi paket berdasarkan kode *DSCP*, seperti tampak pada Tabel 1 (Sudarsono dkk., 2015). Pada penelitian ini, kode *DSCP* yang masuk kategori dicadangkan, akan digunakan dalam proses klasifikasi paket *DHCP* untuk tujuan pencegahan serangan *DHCP Starvation*. Hal ini untuk menghindari kesalahan klasifikasi saat metode digunakan pada kondisi nyata di lapangan.

Tabel 1 Kode klasifikasi paket berdasarkan DSCP

Tipe Paket	Kode DSCP	Keterangan
Reserved	***56***	***Dicadangkan***
Reserved	***48***	***Dicadangkan***
Voice	46	EF: Cocok untuk *Voice VoIP (RTP)* *Expedited Forwarding (EF)*
Video Conference	34	AF41: Cocok untuk *video conference*
Call Control	26	AF31: *Voice Signalling (SCCP)*
High Priority Data	18	AF21: Prioritas tinggi
Medium Priority Data	10	AF11: Prioritas menengah *Assured Forwarding (AF)*
Best Effort Data	0	BE: Prioritas paling rendah

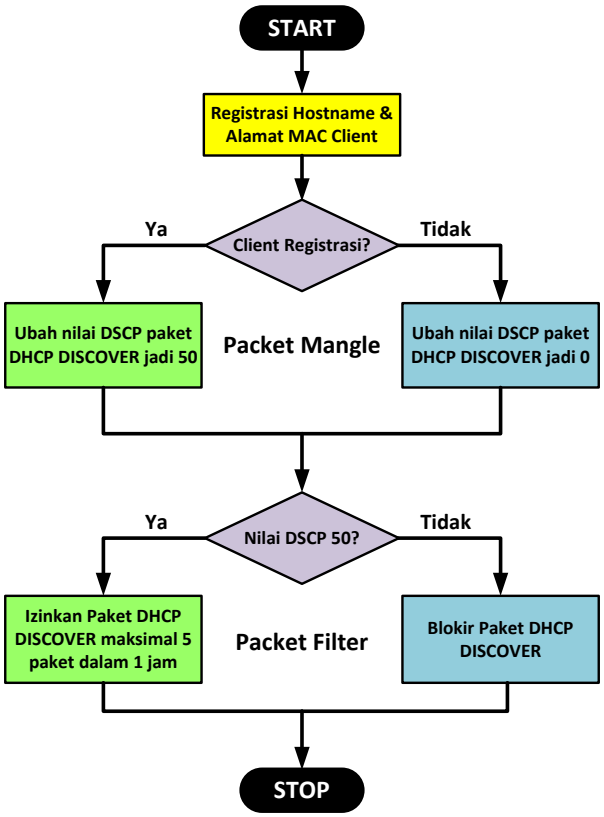
Dalam proses penerapan filter paket berdasarkan *DSCP*, nantinya akan menggunakan *netfilter* yang bekerja lebih cepat dibanding aplikasi filter paket yang lainnya (Sharma, 2018). Tiga fungsi utama *netfiter*, yaitu: 1. Fungsi filter paket (*packet filter*) yang akan menyaring paket yang diizinkan atau tidak diizinkan melewati perangkat filter, 2. Fungsi translasi alamat IP atau umum dikenal dengan *NAT* (*Network Address Translation*), dan 3. Fungsi modifikasi *header* paket (*packet mangle*) yang akan mengubah variabel tertentu pada *header* paket (Wang dkk., 2016).



Gambar 2 Diagram alir paket pada netfilter

Gambar 2 menunjukkan diagram alir paket (*packet flow diagram*) dari *netfilter* pada sistem operasi RouterOS MikroTik yang digunakan pada penelitian ini (MikroTik, 2019). Sebagai pemandu saat implementasi dan pengujian, dibuatlah bagan alir yang menunjukkan algoritma kerja sistem pencegahan *DHCP Starvation*, seperti tampak pada Gambar 3.

Gambar 3 menunjukkan alur kerja sistem pencegahan *DHCP Starvation*, diawali dengan proses registrasi yang harus dilakukan oleh setiap *client WLAN* yang akan terhubung ke jaringan. Data yang dimasukkan dalam proses registrasi adalah nama mesin (*hostname*) dan alamat *MAC*. Paket *DHCP* yang berasal dari *client* terdaftar akan diubah nilai *default DSCP* yang awalnya 0 menjadi 50, proses pengubahan ini dilakukan pada fungsi *mangle prerouting* di *netfilter* (Wang dkk., 2016). Selain dari *client* terdaftar, nilai *DSCP* dari paket *DHCP* yang dikirimkan akan diubah menjadi 0. Pada tahap selanjutnya pada fungsi *filter forward* akan disaring dari setiap paket DHCP yang melaluinya, jika paket *DHCP* mengandung nilai *DSCP* 50 maka akan diizinkan lewat. Namun jika tidak, paket *DHCP* akan dibuang. Untuk antisipasi terhadap usaha penyerang melakukan manipulasi sehingga tetap bisa melancarkan serangan *DHCP Starvation* menggunakan identitas *client* terdaftar. Pada *filter forward* ditetapkan pula aturan pembatasan maksimal jumlah paket *DHCP* yang bisa dilewatkan dalam rentang waktu tertentu.



Gambar 3 Alur kerja sistem pencegahan DHCP *Starvation*

Berikut adalah format konfigurasi pada *netfilter* untuk pencegahan serangan *DHCP Starvation*. Konfigurasi ini diterapkan pada perangkat *Bridge Filter* MikroTik Router OS setelah mengaktifkan fitur "*IP Firewall*", sehingga fungsi filter pada *Bridge* dapat terhubung ke *netfilter*.

Baris konfigurasi berikut untuk mengubah nilai *DSCP* menjadi 50 pada setiap paket *DHCP DISCOVER* yang mengandung *hostname* dan alamat *MAC* yang terdaftar.

/ip firewall mangle add chain=prerouting protocol=udp src-port=68 dst-port=67 content="Hostname" src-mac-address="Mac-Address" action=change-dscp new-dscp=50

Baris konfigurasi berikut untuk memastikan bahwa hanya paket *DHCP DISCOVER* yang mengandung *hostname* dan kode *DSCP* 50 saja yang akan diteruskan ke *DHCP server*. Untuk antisipasi penyalahgunaan oleh *client* terdaftar, jumlah paket *DHCP DISCOVER* yang diizinkan untuk diteruskan maksimal sebanyak 5 paket dalam waktu 1 jam.

/ip firewall filter add chain=forward protocol=udp src-port=68 dst-port=67 content="Hostname" dscp=50 action=accept limit=5/1h,5:packet

Jika *hostname* tertentu digunakan untuk mengirimkan serangan *DHCP Starvation*, maka pesan akan dikirimkan lewat log sistem.

/ip firewall filter add chain=forward protocol=udp src-port=68 dst-port=67 content="Hostname" dscp=50 action=drop log=yes log-prefix="DHCP Starvation dari Hostname"

Paket *DHCP DISCOVER* yang berasal dari *client* yang tidak terdaftar akan diblokir.

/ip firewall filter add chain=forward protocol=udp src-port=68 dst-port=67 action=drop

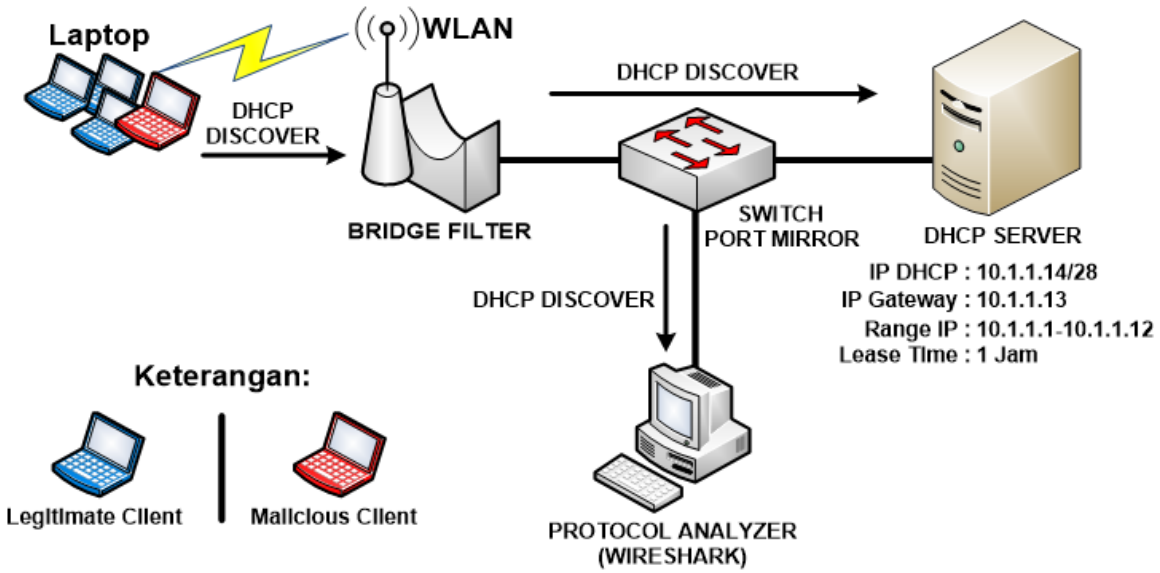
2. Pengujian Metode

Untuk mewakili kelompok kontrol dilakukan uji awal (*pre-test*) dengan mengirimkan serangan *DHCP Starvation* sebanyak empat kali sebelum perlakuan atau solusi pencegahan diterapkan, untuk mengetahui bahwa serangan memang berdampak pada ketersediaan layanan *DHCP.*, Selanjutnya untuk mewakili kelompok eksperimen dilakukan uji akhir (*post-test*) dengan mengirimkan serangan *DHCP Starvation* yang sama sebanyak empat kali untuk mengetahui apakah setelah perlakukan atau solusi diterapkan terdapat perubahan kondisi terhadap ketersediaan layanan *DHCP*.

Gambar 4 menunjukkan topologi jaringan yang akan digunakan dalam proses eksperimen, sedang pada Tabel 2 berikut ini dilampirkan rincian spesifikasi perangkat keras yang digunakan dalam eksperimen.

Tabel 2 Spesifikasi perangkat eksperimen

Jenis	Spesifikasi	Jumlah
Laptop Client	Core i3 2GHz, RAM 2GB	11 Unit
Laptop Analisa paket DHCP	Core i3 2GHz, RAM 2GB	1 Unit
DHCP *Server*	MikroTik RB750	1 Unit
WLAN Bridge Filter	MikroTik RB951Ui-2nD	1 Unit
Switch Port Mirror	MikroTik RB250GS	1 Unit



Gambar 4 Topologi jaringan eksperimen pencegahan serangan DHCP *Starvation*

Laptop client yang berjumlah 11 unit dibagi menjadi tiga bagian dengan tugas yang berbeda, lima unit menggunakan sistem operasi *Microsoft Windows 7*, 5 unit berikutnya menggunakan sistem *operasi Linux*

Ubuntu 16.04, 1 unit lagi digunakan untuk melancarkan serangan *DHCP Starvation* yang menggunakan sistem operasi *Microsoft Windows 7* dan *Linux Backtrack 5*. Untuk kebutuhan melancarkan serangan *DHCP Starvation*, sebenarnya ada beberapa jenis aplikasi yang bisa digunakan, beberapa berjalan di atas sistem operasi *Linux* seperti *Yersinia* (Salsabil dkk., 2014; Zhang dkk., 2017) dan *DHCPig* (Tripathi & Hubballi, 2016), ada pula yang berjalan di atas sistem operasi *Microsoft Windows* seperti *Hyenae* (Amaral dkk., 2017) dan *Colasoft Packet Builder* (Murti dkk., 2016). Pada penelitian ini, aplikasi yang akan digunakan dalam melancarkan serangan *DHCP Starvation* adalah *Colasoft Packet Builder*. Hal ini karena aplikasi tersebut lebih fleksibel dalam memodifikasi paket *DHCP* yang akan dikirimkan sebagai serangan *DHCP Starvation*.

Sebuah laptop khusus digunakan untuk kebutuhan analisa paket *DHCP* yang akan menjalankan aplikasi khusus yang bernama *network analyzer wireshark* (Radha dkk., 2016). Aplikasi *wireshark* akan digunakan untuk menangkap semua paket *DHCP* yang keluar dari *Bridge Filter*, baik saat sebelum dan setelah diterapkannya pencegahan serangan *DHCP Starvation*.

Mesin yang digunakan untuk keperluan membuat *DHCP Server*, *Bridge Filter* dan *Switch Port Mirror* semuanya menggunakan perangkat MiroTik RouterBoard (MikroTik RB). MikroTik adalah salah satu vendor bidang jaringan yang berpusat di Latvia (Eropa), selain memproduksi perangkat keras jaringan, juga membuat sistem operasinya yang bernama RouterOS dan SwOS yang berbasis Linux (Jílek & Žalud, 2012). Dengan sistem operasi RouterOS dan SwOS, RouterBoard kemudian tidak hanya dapat difungsikan sebagai *router* saja, namun juga sebagai *bridge*, *firewall,* dan beberapa layanan *server* seperti *DHCP Server* serta difungsikan sebagai *Switch Manageable* (Cheng & Wu, 2010). MikroTik RB951Ui-2nD difungsikan sebagai *Bridge Filter* yang akan melakukan dua hal, yaitu melakukan modifikasi nilai *DSCP* berdasarkan *hostname* dan alamat *MAC* yang terlampir pada paket *DHCP DISCOVER* yang diterimanya, dan juga melakukan filter untuk menentukan apakah paket *DHCP DISCOVER* yang diterimanya diizinkan untuk diteruskan atau diblokir. Kelebihan dari *Bridge Filter MikroTik* adalah fungsi filternya dapat dihubungkan ke fungsi *netfilter* sehingga dalam melakukan filter tidak hanya terbatas pada filter terhadap *frame*, namun juga dapat melakukan filter terhadap *packet* (Abdulatteef, 2012).

3. Pengumpulan Data

Setelah melakukan pengujian metode di tahap sebelumnya, selanjutnya paket *DHCP DISCOVER* akan dikumpulkan menggunakan aplikasi *protocol analyzer wireshark*. Paket *DHCP DISCOVER* yang dikumpulkan dibagi dalam dua sesi, yaitu pengumpulan data paket *DHCP DISCOVER* sebelum metode pencegahan diterapkan dan setelah metode pencegahan diterapkan. Pengumpulan paket *DHCP DISCOVER* akan digunakan untuk mengetahui tingkat efektivitas metode pencegahan serangan *DHCP Starvation*, selain itu juga akan dikumpulkan data penggunaan sumber daya *CPU* saat sebelum dan setelah metode pencegahan diterapkan.

4. Analisis Data

Pada tahap ini data paket *DHCP DISCOVER* dan penggunaan sumber daya *CPU* akan dikelompokkan menjadi dua jenis, yaitu: (a) Data paket *DHCP DISCOVER* dan penggunaan sumber daya *CPU* yang terkumpul sebelum pencegahan *DHCP Starvation* dilakukan dan (b) Data paket *DHCP DISCOVER* dan penggunaan sumber daya *CPU* yang terkumpul setelah pencegahan *DHCP Starvation* diterapkan. Setelah dilakukan pengelompokan, selanjutnya data disajikan dalam bentuk tabel dan grafik agar lebih mudah dibaca.

5. Kesimpulan

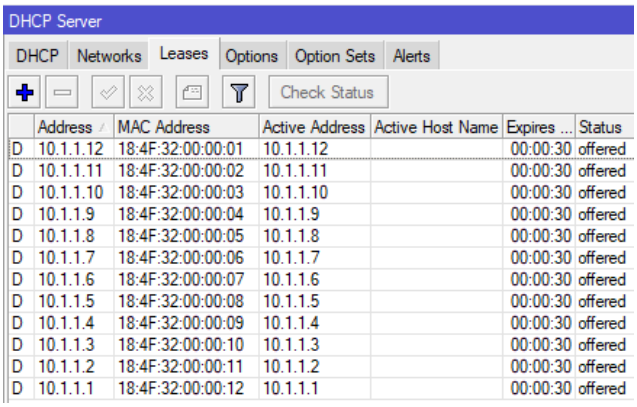
Berdasarkan analisis data, selanjutnya akan disimpulkan apakah metode pencegahan yang diusulkan dapat melakukan pencegahan serangan *DHCP Starvation* secara efektif, agar semakin spesifik maka ditentukan pula seberapa tinggi tingkat efektivitas pencegahan yang dilakukan. Hal lain yang juga akan dilampirkan adalah perbandingan metode yang digunakan pada penelitian ini dengan metode yang digunakan pada penelitian sebelumnya terkait pencegahan serangan *DHCP Starvation*, hal yang dibandingkan adalah masalah efektivitas dan efisiensi.

HASIL DAN PEMBAHASAN

Gambar 5 menunjukkan dampak yang terjadi saat serangan *DHCP Starvation* dilakukan oleh *client* penyerang (*malicious client*) terhadap layanan *DHCP server*, dan semua persediaan alamat *IP* pada *DHCP server* akan ditawarkan (*offered*). Hal ini akan mengakibatkan *client* yang sah (*legitimate client*) tidak akan mendapatkan tawaran alamat *IP* lagi.

Pada tahap pengujian, aplikasi Colasoft Packet Builder mengirimkan paket *DHCP DISCOVER* dengan jumlah bertahap, dimulai dari 20 paket/detik hingga

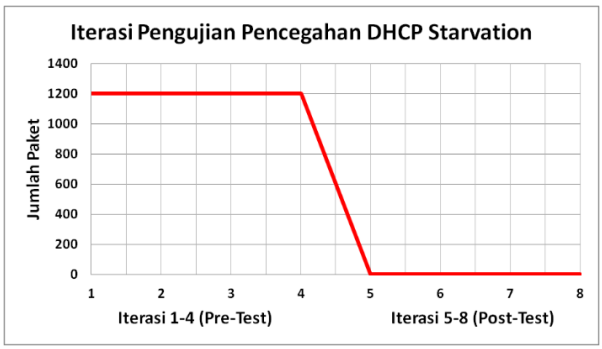
180 paket/detik. Hal ini dilakukan selain untuk menghabiskan persediaan alamat *IP* pada *DHCP server*, juga untuk mengukur pengaruh jumlah paket yang dikirim dengan penggunaan sumber daya *CPU* baik pada *DHCP server* maupun pada *Bridge Filter* saat sebelum dan setelah metode pencegahan serangan *DHCP Starvation* diterapkan.



	Address	MAC Address	Active Address	Active Host Name	Expires ...	Status
D	10.1.1.12	18:4F:32:00:00:01	10.1.1.12		00:00:30	offered
D	10.1.1.11	18:4F:32:00:00:02	10.1.1.11		00:00:30	offered
D	10.1.1.10	18:4F:32:00:00:03	10.1.1.10		00:00:30	offered
D	10.1.1.9	18:4F:32:00:00:04	10.1.1.9		00:00:30	offered
D	10.1.1.8	18:4F:32:00:00:05	10.1.1.8		00:00:30	offered
D	10.1.1.7	18:4F:32:00:00:06	10.1.1.7		00:00:30	offered
D	10.1.1.6	18:4F:32:00:00:07	10.1.1.6		00:00:30	offered
D	10.1.1.5	18:4F:32:00:00:08	10.1.1.5		00:00:30	offered
D	10.1.1.4	18:4F:32:00:00:09	10.1.1.4		00:00:30	offered
D	10.1.1.3	18:4F:32:00:00:10	10.1.1.3		00:00:30	offered
D	10.1.1.2	18:4F:32:00:00:11	10.1.1.2		00:00:30	offered
D	10.1.1.1	18:4F:32:00:00:12	10.1.1.1		00:00:30	offered

Gambar 5 Dampak serangan DHCP *Starvation*

Pengujian efektivitas metode pencegahan serangan *DHCP Starvation* dilakukan dengan mengirimkan paket *DHCP DISCOVER* sebanyak 20 paket/detik selama 60 detik, sehingga total paket yang terkirim sebanyak 1200 paket. Pengujian dilakukan sebanyak empat kali, baik sebelum dan setelah metode pencegahan serangan *DHCP Starvation* diterapkan.



Gambar 6 Iterasi pengujian pencegahan DHCP *Starvation*

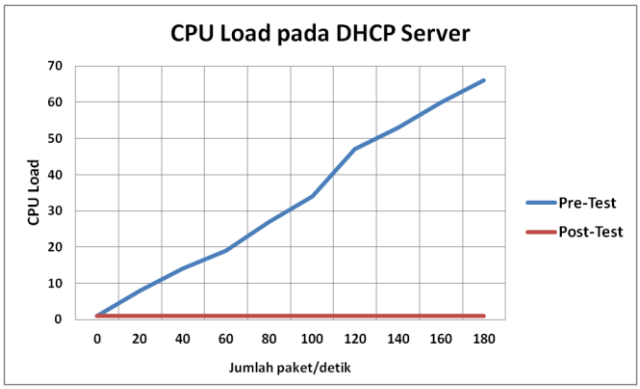
Gambar 6 menunjukkan bahwa sebelum metode pencegahan diterapkan, 1200 paket tersebut diteruskan ke *DHCP server* tanpa ada proses filter, namun setelah metode pencegahan diterapkan, *Bridge Filter* memblokir semua paket sehingga tidak ada satu paket pun yang diteruskan ke *DHCP server*.

Berikut adalah penghitungan tingkat efektivitas metode pencegahan *DHCP Starvation*:

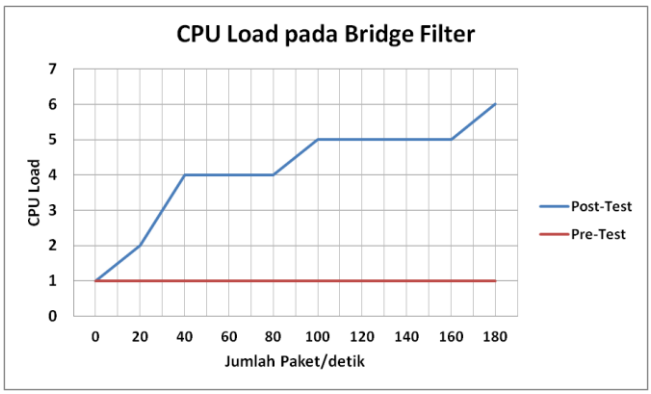
$$Efektivitas = \frac{\sum DHCP\ DISCOVER\ Cegah}{\sum DHCP\ DISCOVER\ Kirim} x\ 100\%$$

$$Efektivitas = \frac{1200}{1200} x\ 100\% = 100\%$$

Saat terjadi serangan *DHCP Starvation* dengan jumlah paket *DHCP DISCOVER* yang sangat banyak, dapat mempengaruhi penggunaan sumber daya *CPU* pada *DHCP server*. Terlihat pada Gambar 7, *CPU Load* akan terus meningkat seiring jumlah paket yang dikirimkan setiap detiknya sebelum pencegahan dilakukan (*pre-test*), namun setelah pencegahan dilakukan (*post-test*) *CPU Load* akan menurun karena *Bridge Filter* telah berhasil memblokir paket serangan *DHCP Starvation* sehingga tidak akan diteruskan ke *DHCP server*.



Gambar 7 CPU Load pada DHCP *Server*



Gambar 8 CPU Load pada Bridge Filter

Gambar 8 adalah grafik penggunaan *CPU* di *Bridge Filter*, nampak bahwa peningkatan *CPU Load* tidak terlalu siginifikan saat penanganan pencegahan serangan *DHCP Starvation* dilakukan oleh *Bridge Filter*, sehingga masih sangat memungkinkan client yang sah masih dapat berkomunikasi dengan *DHCP server* untuk meminta layanan konfigurasi alamat *IP* secara otomatis.

Dari penyajian data sebelumnya diketahui bahwa metode pencegahan serangan *DHCP Starvation* berbasis filter paket berdasarkan nilai *DSCP* terbukti sangat efektif dalam melakukan pencegahan terhadap serangan *DHCP Starvation*. Untuk merangkum perbedaan mendasar dari metode yang digunakan

dalam penelitian ini dengan penelitian sebelumnya, berikut disajikan dalam Tabel 3. Kriteria dianggap lebih efektif jika metode yang digunakan mampu melakukan pencegahan terhadap serangan *DHCP Starvation* dan tidak bermasalah dengan adanya *firewall* di sisi *client*. Sementara kriteria dianggap lebih efisien jika dalam penerapan metode tidak membutuhkan tambahan aplikasi baik di sisi *client* maupun di sisi *server*.

Tabel 3 Perbandingan metode pencegahan DHCP *Starvation* dengan penelitian sebelumnya

Metode	Efektivitas	Efisiensi
Yaibuates (2014)	Mencegah: Tidak Masalah Firewall: Ya	App. Client: Tidak App. *Server*: Ya
Younes (2017)	Mencegah: Tidak Masalah Firewall: Tidak	App. Client: Ya App. *Server*: Ya
Tripathi (2017)	Mencegah: Tidak Masalah Firewall: Tidak	App. Client: Tidak App *Server*: Ya
Shete (2018)	Mencegah: Ya Masalah Firewall: Tidak	App. Client: Ya App. *Server*: Ya
Yaibuates (2018)	Mencegah: Ya Masalah Firewall: Ya	App. Client:Tidak App. *Server*: Ya
Sarip (2019)	***Mencegah: Ya*** ***Masalah Firewall: Tidak***	***App. Client: Tidak*** ***App. Server: Tidak***

KESIMPULAN

Dari hasil penelitian yang telah dilakukan dapat disimpulkan bahwa serangan *DHCP Starvation* dapat dicegah secara efektif melalui metode pencegahan dengan filter paket berdasarkan *Differentiated Services Code Point* (DSCP) yang diterapkan pada perangkat *Bridge* RouterBoard dengan sistem operasi RouterOS. Metode yang digunakan cukup efisien diterapkan pada jaringan *wireless* skala kecil dalam ruang lingkup jaringan *wireless* atau *hotspot*. Hal ini dapat dilihat dari spesifikasi perangkat yang dibutuhkan untuk proses deteksi dan pencegahan serta tanpa perlu dilakukan penambahan apapun baik di sisi *server* maupun di sisi *client*.

Penelitian lebih lanjut perlu dilakukan penyederhanaan dalam proses registrasi, sehingga pengguna tidak perlu bertatap muka dengan *admin* jaringan, terutama di area akses publik.

UCAPAN TERIMA KASIH

Terima kasih banyak kami ucapkan kepada seluruh pihak yang telah membantu dalam proses penelitian ini.

DAFTAR PUSTAKA

Abdulatteef, S. W. (2012). An Implementation Of Firewall System Using MikroTik Router OS. *Journal of University of Anbar for Pure Science*, vol.6 (2), pp.65-69.

Amaral, A. A., Mendes, L. de S., Zarpelão, B. B., & Junior, M. L. P. (2017). Deep IP Flow Inspection to Detect Beyond Network Anomalies. *Computer Communications*, vol.98, pp.80–96.

Barik, R., Welzl, M., Elmokashfi, A. M., Dreibholz, T., & Gjessing, S. (2018). Can WebRTC QoS Work? A DSCP Measurement Study. *In 2018 30th International Teletraffic Congress (ITC 30)*, vol.1, pp.167-175.

Bhaiji, Y. (2007). *Understanding, preventing, and defending against layer 2 attacks*. Diakses dari http://www.nanog. org/meetings/nanog42/presentations/Bhaiji_Layer_2 _Attacks.pdf tanggal 12 April 2019.

Breabăn, M. C., Graur, A., Potorac, A. D., & Bălan, D. G. (2017). New Approach of Traffic Limitation Management on Local Networks. In *2017 International Conference on Optimization of Electrical and Electronic Equipment (OPTIM) & 2017 Intl Aegean Conference on Electrical Machines and Power Electronics (ACEMP)* (pp. 941-946).

Cheng, J., & Wu, H. (2010). The Application of the PPPoE for Network Security Management Using RouterOS. *In 2010 International Conference on Computer Design and Applications*, vol.5, pp.5-569.

Custura, A., Secchi, R., & Fairhurst, G. (2018). Exploring DSCP Modificatio Pathologies in the Internet. *Computer Communications*, vol.127, pp.86–94.

Droms, R. & Lemon, T. (2003). *The DHCP Handbook*. 2nd edition, SAMS Publishing.

Duangphasuk, S., Kungpisdan, S., & Hankla, S. (2011). Design and Implementation of Improved Security Protocols for DHCP Using Digital Certificates. *17th IEEE International Conference on Networks*.

Hubballi, N., Tripathi, N. (2017). A Closer Look into DHCP *Starvation* Attack in Wireless Networks. *Computers & Security*, vol.65, pp.387-404.

Jílek, T., & Žalud, L. (2012). Security of Remote Management of Embedded Systems Running MikroTik RouterOS Operating System Using Proprietary Protocols. *IFAC Proceedings Volumes*, vol.45(7), pp.169-173.

Marczyk, G., DeMatteo, D., & Festinger, D. (2005). *Essentials of Research Design and Methodology*. John Wiley & Sons Inc.

MikroTik. (2019). *MikroTik: Packet Flow Diagram*. Diakses dari https://wiki.mikrotik.com/wiki/Manual:Packet_Flow tanggal 12 April 2019.

Mukhtar, H., Salah, K. & Iraqi, Y. (2012). Mitigation of DHCP *Starvation* Attack. *Computers and Electrical Engineering 38*, p.1115–1128.

Murti, M. A., Tjokronegoro, H. A., Leksono, E., & Agung, W. (2016). Performance Analysis of HSPA Technology for Networked Control System Application. *International Journal of Computer and Communication Engineering*, 5(3), pp.165.

Naaz, S. & Badroo, F.A. (2016). Investigating DHCP and DNS Protocols Using Wireshark. *IOSR Journal of Computer Engineering*, vol.18 (3), p.1-8.

Salsabil, U., Ali, M. T., & Islam, M. M. (2014). A Practical Approach to Asses Fatal Attacks in Enterprise Network to Identify Effective Mitigation Techniques, International *Journal of Computer Networks and Communications Security*, 2(9), 298-307

Sharma, G. (2018). *Evaluating the Performance of Netfilter Architecture in Private Realm Gateway*. Communications Engineering, Alto University.

Shete, A., Lahade, A., Patil, T. & Pawar R. (2018). DHCP Protocol Using OTP Based Two-Factor Authentication. *Proceedings of the 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*.

Shuai, Y., Qianli, Z., & Xing, L. (2016). A Tunnel Broker Based IPv6 Access System for aA Small Scale Network with IPv4 upstream. *2016 IEEE Information Technology, Networking, Electronic and Automation Control Conference*.

Stewart, J.M., Tittel, E. & Chapple, M. (2005). *Certified Information Systems Security Professional Study Guide*. 3rd edition, SYBEX Inc.

Sudarsono, A., Siswanto, A., Iswanto, H., & Setiawan, Q. (2016). Traffic Analysis of Quality of Service (QoS) for Video Conferencing between Main Campus and Sub Campus in Laboratory Scale. *EMITTER International Journal of Engineering Technology*, vol.3 (2), pp.1-17.

Tripathi, N., & Hubballi, N. (2015). Exploiting DHCP *Server*-Side IP Address Conflict Detection: A DHCP *Starvation* Attack. *In 2015 IEEE International Conference on Advanced Networks and Telecommuncations Systems (ANTS)*, pp.1-3.

Tripathi, N., & Hubballi, N. (2016). A Probabilistic Anomaly Detection Scheme to Detect DHCP *Starvation* Attacks. *In 2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pp.1-6.

Tripathi, N., & Hubballi, N. (2018). Detecting Stealth DHCP *Starvation* Attack Using Machine Learning Approach. *Journal of Computer Virology and Hacking Techniques*, vol.14(3), pp.233-244.

Umasuthan, V. (2016). Protecting the Communications Network at Layer 2. *In 2016 IEEE/PES Transmission and Distribution Conference and Exposition*.

Wang, B., Lu, K., & Chang, P. (2016). Design and Implementation of Linux Firewall Based on the Frame of Netfilter/Iptables. *In 2016 11th International Conference on Computer Science & Education (ICCSE)*, pp. 949-953.

Yaibuates, M. & Chaisricharoen, R. (2014). ICMP Based Malicious Attack Identification Method for DHCP. *Joint International Conference on Information and Communication Technology, Electronic and Electrical Engineering*.

Yaibuates, M., Chaisricharoen, R. & Rai, C. (2018). Implementing of IP address Recovery for DHCP Service. *International Journal of Applied Engineering Research*.

Younes, O. S. (2017). Securing ARP and DHCP for Mitigating Link Layer Attacks. *Sādhanā Journal*.

Zhang, F., & Chen, L. (2016). OTP_SAM: DHCP Security Authentication Model Based on OTP. *IEEE 20th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*.

Zhang, L., Wang, Y., Jin, R., & Gao, K. (2017). Approaches for a Stand-alone Network Attack and Defense Platform Using Yersinia Toolkits. *International Journal of All Research Education and Scientific Methods (IJARESM)*, Vol.5, Issue 3, pp.2455-6211.

Halaman ini sengaja dikosongkan