Universitas Bina Darma

# SURAT TUGAS

Nomor : 0758 /ST/Univ-BD/VII/2018

Dekan Fakultas Ilmu Komputer Universitas Bina Darma menugaskan kepada Saudara:

| No. | Nama | Keterangan |
|---|---|---|
| 1. | Dr. Widya Cholil, S.Kom., M.I.T. | Dosen Fakultas Ilmu Komputer Universitas Bina Darma |
| 2. | Febriyanti Panjaitan, M.Kom. | Dosen Fakultas Ilmu Komputer Universitas Bina Darma |
| 3. | Ilman Zuhri Yadi, M.M., M.Kom. | Dosen Fakultas Ilmu Komputer Universitas Bina Darma |
| 4. | Yesi Novaria Kunang, S.T., M.Kom. | Dosen Fakultas Ilmu Komputer Universitas Bina Darma |
| 5. | Suzi Oktavia Kunang, S.T., M.Kom. | Dosen Fakultas Ilmu Komputer Universitas Bina Darma |
| 6. | Alex Wijaya, S.Kom., M.I.T. | Dosen Fakultas Ilmu Komputer Universitas Bina Darma |
| 7. | Rahayu Amalia, M.Kom. | Dosen Fakultas Ilmu Komputer Universitas Bina Darma |
| 8. | Nyimas Sopiah, M.M., M.Kom. | Dosen Fakultas Ilmu Komputer Universitas Bina Darma |
| 9. | Eka Puji Agustina, MM., M.Kom. | Dosen Fakultas Ilmu Komputer Universitas Bina Darma |
| 10. | Aan Restu Mukti, M.Kom. | Dosen Fakultas Ilmu Komputer Universitas Bina Darma |
| 11. | Chairul Mukmin, M.Kom. | Dosen Fakultas Ilmu Komputer Universitas Bina Darma |
| 12. | Hutrianto, M.M., M.Kom. | Dosen Fakultas Ilmu Komputer Universitas Bina Darma |

sebagai Tim Penulis dalam Jurnal Ilmiah MATRIK Fakultas Ilmu Komputer Universitas Bina Darma Volume 20 No. 2 bulan Agustus 2018 ISSN: 1411-1624.

Demikianlah surat tugas ini dibuat agar dapat dilaksanakan dengan penuh rasa tanggung jawab.

Dikeluarkan di : Palembang
Pada tanggal : 2 Juli 2018

Dekan,

Universitas Bina Darma

M. Izman Herdiansyah, S.T., M.M., Ph.D.

Tembusan disampaikan kepada yth:
1. Rektor Universitas Bina Darma (sebagai laporan);
2. Kepala Biro Administrasi Universitas Bina Darma;
3. Koordinator Jurnal Ilmiah Terpadu (JIT) Universitas Bina Darma;
4. Yang bersangkutan untuk dilaksanakan;
5. Arsip.

Universitas Bina Darma
Lembaga Penelitian dan Pengabdian kepada Masyarakat

# SURAT KETERANGAN

Nomor: 002/SK/LPPM-UBD/IX/2018

Lembaga Penelitian dan Pengabdian kepada Masyarakat ( LPPM ) Universitas Bina Darma menerangkan bahwa :

| No | Nama | Jabatan |
|---|---|---|
| 1 | Ilman Zuhri Yadi, M.M., M.Kom. | Dosen Program Studi Sistem Informasi |
| 2 | Suzi Oktavia Kunang, S.T., M.Kom. | Dosen Program Studi Sistem Informasi |

Adalah benar telah mempublikasikan artikel yang berjudul **" Celah Ipv6 Router Advertisement Pada Sistem Operasi Windows ".** Jurnal Nasional **MATRIK ,** yang **Belum Terakreditasi**, Volume **20**, No.**2** , Halaman **85-94** Tahun **2018**, p-ISSN **1411-1624.**

Palembang, 5 September 2018
Direktur ,

Dr. Hardiyansyah, M.Si.
NIP. 196610181992031008

Jl.Jend.A.Yani No. 3 Palembang 30264 Indonesia Telp.(+62 711) 515679, 515581,515582
Fax.(+62 711) 515581, 515582 Web site:www.binadarma.ac.id e-mail:universitas@mail.binadarma.ac.id

Vol. 20 No.2, Agustus 2018 ISSN : 1411-1624

JURNAL ILMIAH

# MATRIK

(Ilmu Komputer)



Diterbitkan Oleh:
Fakultas Ilmu Komputer
Universitas Bina Darma, Palembang

Jurnal Ilmiah MATRIK
Jl. A. Yani no. 3 Plaju Palembang SumSel, Indonesia



# MATRIK Vol.20 No.2 Agustus 2018

TABLE OF CONTENTS

Vol. 20 No.2, Agustus 2018 ISSN :

JURNAL ILMIAH

# MATRIK

(Ilmu Komputer)



Diterbitkan Oleh:
Fakultas Ilmu Komputer
Universitas Bina Darma, Palembang

| MATRIK | Vol.20 | No.2 | Hal. 85-178 | Agustus 2018 |
|---|---|---|---|---|

Jurnal Ilmiah MATRIK
Jl. A. Yani no. 3 Plaju Palembang SumSel, Indonesia



# MATRIK Vol.20 No.2 Agustus 2018

## Table of Contents

### Articles



**Indexed in: >>**

# CELAH IPV6 *ROUTER ADVERTISEMENT* PADA SISTEM OPERASI *WINDOWS*

**Ilman Zuhri Yadi[1], Suzi Oktavia Kunang[2]**
**Universitas Bina Darma**
**Jalan Jenderal Ahmad Yani No.3 Palembang**
**Sur-el: ilmanzuhriyadi@binadarma.ac.id[1], suzi_oktavia@binadarma.ac.id[2]**

***Abstract:*** *With the decrease in the number of IPv4 available it is necessary to consider IPv6 usage. However, IPv6 itself still has security holes such as security flood hole Router Advertisement false. Router Advertisement flood itself is an IPv6 DoS attack on the local network. This attack floods the local network segment with malicious Router Advertisement to replace the legitimate routing entry on the host interface. The purpose of this research is to study the response of Operating System with Windows platform against IPv6 Router Advertisement attack on the network, and to recommend solution to close the security hole. Attack testing is done with two stages of RA flood packet delivery with single prefix and multi prefix.*

***Keywords:*** *Router Advertisement, IPv6, Sistem Operasi*

***Abstrak:*** *Dengan makin berkurangnya jumlah IPv4 yang tersedia maka perlu dipertimbangkan penggunaan IPv6. Akan tetapi IPv6 sendiri masih memiliki celah keamanan antara lain celah keamanan serangan flooding Router Advertisement palsu. Router Advertisement flood sendiri adalah merupakan serangan IPv6 DoS di jaringan lokal. Serangan ini membanjiri segmen jaringan lokal dengan malicious Router Advertisement untuk menggantikan entri routing yang sah pada antarmuka suatu host. Tujuan dari penelitian ini adalah mempelajari respon Sistem Operasi dengan platform Windows terhadap serangan IPv6 Router Advertisement di jaringan, serta memberikan rekomendasi solusi untuk menutup celah keamanan tersebut. Pengujian serangan dilakukan dengan dua tahapan yaitu pengiriman paket flood RA dengan single prefix dan multi prefix.*

***Kata Kunci****: Router Advertisement, IPv6, Sistem Operasi*

## 1. PENDAHULUAN

Berdasarkan RFC 791, "protokol internet didesain penggunaannya untuk menginterkoneksikan sistem *host* jaringan komunikasi komputer. Internet Protokol digunakan untuk mentransmisikan blok data yang disebut datagram dari sumber ke tujuan, di mana sumber dan tujuan berupa *host* yang diidentifikasikan menggunakan panjang alamat tetap "(*University of Southern California*, 1981). Ada dua *Protokol Internet* yang digunakan secara umum, yaitu Internet Protokol versi 4 (*IPv4*) dan *Internet Protokol* versi 6 (*IPv6*).

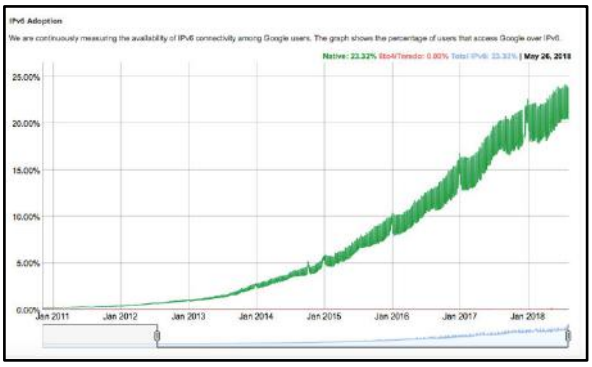
Standar *Protokol Internet IPv4* sudah digunakan sejak tahun 1970-an. Beberapa keterbatasan dari protokol IPv4 antara lain keterbatasan jumlah alamat IP karena hanya menggunakan alamat IP 32 bit. Dengan jumlah bit yang terbatas tersebut maka jumlah maksimal IPv4 yang dapat ditampung hanya 4.294 juta alamat *host* untuk seluruh dunia. Dengan makin berkembangnya penggunaan jaringan internet di seluruh dunia maka IPv4 yang tersedia cepat habis.

Di Indonesia sendiri *Internet Protokol* versi 4 (*IPv4*) sampai saat ini masih banyak digunakan sebagai *Protokol Internet* utama. Berdasarkan *Report Geoff Houston IPv4 Adrress Report, IPv4* mulai mengalami fase jenuh pada

awal tahun 2011 (Houston, 2018). Pada 3 Februari 2011 *Internet Assigned Numbers Authority (IANA)* kehabisan alamat *IPv4* yang belum dialokasikan mereka. Dalam beberapa tahun, setiap *Regional Internet Registry (RIR)* akan kehabisan *IPv4* yang belum dialokasikan. Kejenuhan yang terjadi ini karena pesatnya perkembangan pengguna Internet. Dampaknya, dalam beberapa tahun ke depan pengguna internet baru tidak akan bisa mendapatkan alamat *IPv4*, yang berarti mereka akan sulit terkoneksi ke Internet.

IETF RFC 791, 1981 sudah membahas keterbatasan infrastruktur Internet yang didasarkan pada Internet Protokol 4 (IPv4). *Network Working Group* dari *Internet Engineering Task Force* (*IETF*) mengusulkan sebuah Paket protokol baru disebut *Internet Protocol versi 6* (IPv6). Sebagai hasilnya, IETF telah mengatur spesifikasi IPv6, bersama dengan sejumlah kinerja, kemudahan konfigurasi, dan masalah manajemen jaringan. Spesifikasi IPv6 telah diaturdalam berbagai *Request for Comments (RFC)* seperti RFC 2460 (tentang *IPv6 Protocol*), RFC4861 (mengenai *IPv6 Neighbor Discovery*), RFC 4862 (mengatur *IPv6 Stateless Address Auto-Configuration*), RFC 4443 (mengenai *Internet Control Message Protocol* untuk *IPv6*ICMPv6), RFC 4291 (mengatur *IPv6Addressing Architecture*), dan RFC 4301 (tentang *Security Architecture for IP or IPsec*). (Durdagi, 2010)

Dalam dokumen RFC Internet Protokol versi 6 (*IPv6*) adalah versi terbaru dari Internet Protokol, yang dirancang sebagai pengganti *Internet Protokol* versi 4 (*Network Working Group*, 1998). *IPv6* dirancang untuk memenuhi pertumbuhan pengguna internet yang makin pesat. *IPv6* memiliki panjang alamat 128-bit, sehingga dapat mendukung $2^{128}$ alamat atau sekitar $3.4x10^{38}$ alamat. Selain jumlah alamat yang lebih banyak *IPv6* juga memiliki beberapa perubahan lain.




(Sumber: https://www.google.com/intl/en/ipv6/statistics.html)

**Gambar 1. Penggunaan IPv6 berdasarkan Google Statistik**

Dalam penggunaan IPv6 ada beberapa masalah yang ditemui terkait dengan keamanannya. Misalnya untuk dukungan penggunaan Ipv6 yang belum didukung oleh beberapa perangkat pengamanan di jaringan. Sedangkan pada beberapa perangkat pengamanan yang mendukung IPv6 masalah konfigurasi yang tidak dikonfigurasi secara benar mengakibatkan celah keamanan. Contohnya pada beberapa *firewall*, dan IDS yang bisa mendeteksi serangan berbahayapada trafik data protokol *IPv4*, pada saat penyerang mengirimkan trafik data berbahaya pada protocol IPv6 mekanisme kontrol dan deteksi perangkat bisa dilewati. Masalah lain pada kelemahan IPv6 bisa dimanfaatkan penyerang untuk melakukan serangan jaringan ke *IPv6*. Beberapa penelitian yang membahas pengujian keamananan jaringan, antara lain dilakukan oleh A. Pilihanto dalam SANS Institute yang membahas mengenai

serangan ke *IPv6* dan mekanisme pertahanannya (Pilihanto, 2011). Penelitian lain yang membahas berbagai serangan pada IPv6 dilakukan oleh (Vikram, 2014).

Salah satu celah keamanan IPv6 adalah celah *Router Advertisment* (RA) *flood attack.* Celah ini dikarenakan adanya *Router Discovery* (RD) dan *Stateless Address Autoconfiguration* (SLAAC) pada protokol *Neighbor Discovery Protocol* (NDP) IPv6. RD memungkinkan *host* menemukan router terdekat di jaringan dan SLAAC memungkinkan *host* meng-*generate* alamat IPv6. Dengan kedua fungsi tersebut, paket *Router Advertisement broadcast* tidak memerlukan konfirmasi dari *host* penerima. Sehingga dengan membanjiri jaringan dengan *broadcast* paket *Router Advertisement (RA)* mengakibatkan serangan *DoS* pada seluruh *host* di jaringan lokal.

Hampir seluruh platform Sistem Operasi modern mendukung penggunaan IPv6, khususnya system operasi *Windows.* Sistem Operasi *Windows* sendiri merupakan yang merupakan Sistem Operasi yang paling banyak penggunanya, dan semenjak penggunaan *Windows 7* secara default sudah mendukung implementasi (penggunaan) IPv6. Untuk itu pada penelitian ini berfokus pada analisis celah keamanan IPv6 terhadap serangan *Router Advertisement flooding*khususnya di jaringan yang clientnya menggunakan platform Sistem Operasi *Windows* mulai dari *Windows XP, Windows 7, Windows 8, Windows 10, Windows Server 2008, Windows Server 2012* dan *Windows Server 2016.*

## 2. METODOLOGI PENELITIAN

Berdasarkan jenis penelitian, maka penelitian yang dilakukan merupakan penelitian eksperimen. Langkah-langkah dalam penelitian eksperimen pada dasarnya hampir sama dengan penelitian lainnya. Berdasarkan Marguerite (2010) maka 10 tahapan dalam penelitian eksperimen ini yaitu: (1) Penentuan topik yang tentang serangan IPv6 *Router Advertisement* pada platform Sistem Operasi *Windows*; (2) meninjau referensi yang relevan terkait dengan IPv6 dan serangan *Router Advertisement*; (3) menyusun hipotesis, yaitu: "tidak semua dari platform Sistem Operasi *Windows* siap dengan implementasi IPv6 khususnya dampak dari serangan IPv6 *RA flood*.; (4) memilih platform Sistem operasi yang akan diuji yaitu *Windows XP, Windows 7, Windows 8, Windows 10, Windows Server 2008, Windows Server 2012* dan *Windows Server* 2016; (5) menentukan instrumen pengukuran, instrumen yang diukur antara lain beban kerja processor dan *memory* dari berbagai platform tersebut; (6) menentukan kelompok variabel eksperimen dan kontrol, yang menjadi variabel ekperimen disini adalah paket data *RA flood* yang dikirim, sedangkan variabel kontrol berupa pemakaian *processor* dan *memory*; (7) menyusun *treatment*/tindakan, berdasarkan fase *metodology testing*; (8) mengumpulkan dan menganalisa data; (9) membuat keputusan tentanghipotesis (sesuai atau tidak sesuai); (10) menyusun simpulan.

## 2.1 Prosedur Penelitian

Untuk tahapan tindakan pada prosedur eksperimen ini mengacu pada dokumen *United States National Institute of Standards and Technology (NIST)* mengenai pengujian *Information Security* (K. Scarfone, dkk., 2008). Fase *Penetrasi Testing* pada dokumen NIST terdiri dari empat fase yang mencakup *Planning, Discovery, Attack dan Reporting*.

## 2.2 Serangan *Denial of Services*

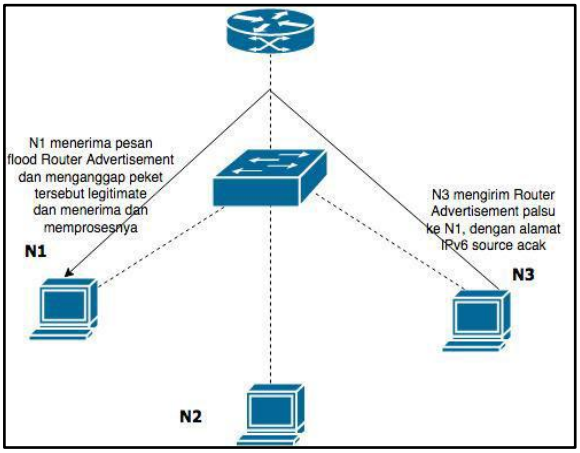
*Internet Engineering Task Force* (IETF) mengembangkan *IPv6* untuk mengatasi keterbatasan *IPv4* (Kaur & Sharma, 2014). Namun, beberapa kerentanan keamanan *IPv4* masih ada di *IPv6*. Sebagai contoh, Kedua jaringan *IPv4* dan *IPv6* rentan terhadap serangan *Denial of Service* (DoS).

Serangan DoS merupakan upaya menghentikan *node* yang sah untuk mendapatkan akses ke sumber daya jaringan. Selama serangan DoS berlangsung, *node* penyerang menyebabkan *node* korban berhenti berkomunikasi dengan semua *node* atau *node* tertentu pada di jaringan (Beck *dkk*., 2007). Meskipun serangan DoS mengganggu keamanan jaringan, serangan tersebut tidak melakukan pencurian informasi. Melainkan, serangan DOS mencoba untuk memutuskan koneksi jaringan (Shrivastava, Sharma, & Rai, 2010).

Setiap sistem operasi dapat menjadi target serangan DoS karena serangan tersebut ditujukan pada *Internet Protocol* (IP). Dengan demikian, setiap sistem operasi yang menggunakan *IPv4* atau *IPv6* bisa diserang (Bosworth dkk., 2012). Meskipun serangan DoS sering hanya mempengaruhi layanan jaringan IP, mereka juga dapat mempengaruhi *VoIP* dan layanan *real-time* lainnya (Brashars, 2007). Penyerang sering menggunakan *spoofing* untuk menyembunyikan sumber serangan DoS. Misalnya, IP *address spoofing* atau MAC *address spoofing* (Tripathi & Mehtre, 2013).

## *2.3* Serangan *Router Advertisement Flood*

Serangan *Router Advertisement flood*di jaringan merupakan serangan Dos pada IPv6. Serangan ini bekerja dengan membanjiri jaringan lokal dengan malicious *Router Advertisement. Router advertisement* ini pada *host* yang menerima pesan akan menggantikan entri routing yang sah pada antarmuka jaringan (Shrivastava, Sharma, & Rai, 2010).




**Gambar 2. Proses Serangan Router Advertisement**

Pada gambar 2 R1 tidak harus mendukung IPv6, karena messages akan dikirim langsung melalui LAN. Sebagai dampaknya N3 akan mengirim *source address random* dari RA *packets sent* ke N1, N1. *Host* yang

menerimaakan memproses setiap single paket yang di *broadcast*. Sebagai dampaknya setiap proses akan direspon. Hal ini berarti setiap *Router Advertisement* yang diterima, N1 akan meng-*assign* dirinya sendiri baik untuk alamat *temporary* dan *public link local address*.

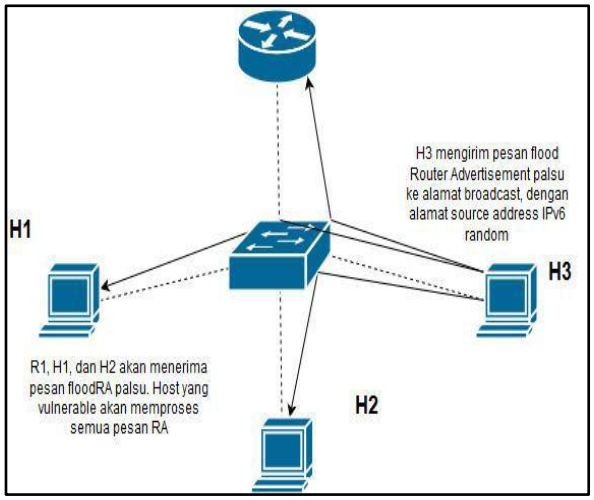
Selama banjir paket RA ke *host* IPv6 yang rawan, maka pemakaian CPU akan meningkat hingga 90 – 100%, dan sistem operasi di dalam *host* menjadi tidak bisa digunakan, menjadi sangat lambat untuk memproses semua trafik yang dikirim.

Selain itu, *NDP RFC*ini memungkinkan pengiriman *RA messages*ke alamat *broadcast address*, yang berarti satu *host* yang mengirim pesan RA palsu bisa melumpuhkan semua perangkat di dalam jaringan sekaligus.

## 3. HASIL DAN PEMBAHASAN

### 3.1 *Planning*

Pada tahapan *Planning* ini desain simulasi pengujian bisa dilihat seperti pada gambar 3.




**Gambar 3. Desain Simulasi Pengujian**

Untuk *Attacker* (H3) menggunakan *host* Kali Linux Rolling (kernel Linux kali 4.3.0-kali1-686-pae) seperti pada gambar yang akan mengirim paket broadcast RA ke H1 dan H2. Sistem operasi Kali Linux ini diinstal pada Komputer *Virtual Box*. Sedangkan yang menjadi target serangan adalah Sistem Operasi *Windows XP, 7, 8.1, 10, Windows Server 2008, Windows Server 2012* dan *Windows Server 2016.*

### 3.2 Proses *Discovery* dan Penyerangan

Pada tahapan *discovery* dan penyerangan dilakukan dengan dua skenario. Skenario pertama dilakukan serangan dengan *Single Router Advertisement Attack*, skenario kedua melakukan serangan dengan *Multi Router Advertisement Attack*.

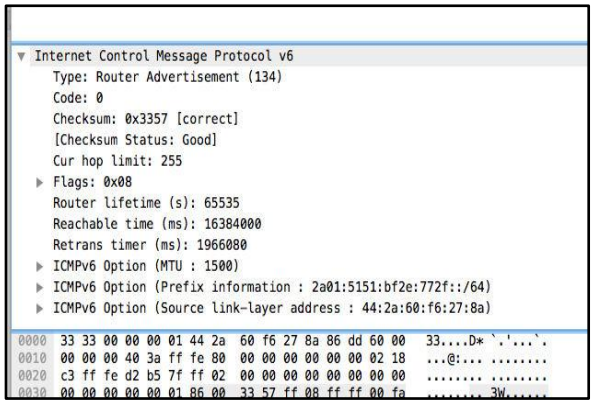
#### 3.2.1 *Single Prefix Router Advertisement Attack*

Pada komputer penyerang dibuat *script* sederhana menggunakan perintah *atk-fake_router26* yang dibuat untuk meng-*generate* paket *Router Advertisment* palsu dengan *script* pada gambar 4.

```
#!/bin/bash
for i in {1..1000}
do
atk6-fake_router26 -A 1:$i::/64 -n 1 eth0
done
```

**Gambar 4. Contoh *Script* untuk *Router Advertisement* Palsu**

Paket *Router advertisement* yang dikirim ke *host* di jaringan yang hanya terdiri dari satu *prefix* dan satu *Source link layer address*. *Script* ini dites dengan mengirim 1000 dan 10.000 paket ke jaringan untuk melihat pengaruh paket *Router Advertisement Broadcast* ke *host* target.

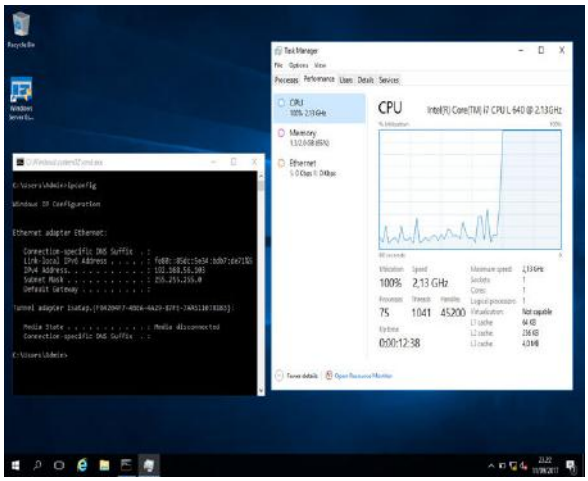



**Gambar 5. Paket *Single Prefix Router Advertisement* Palsu**

Pengujian serangan dilakukan pada seluruh Platform sistema operasi *Windows* yang diuji dengan pengujian 1000 paket flood dan 10.000 paket *flood.* Kemudian diamati Utilisasi CPU dan Penggunaan Memori pada masing-masing *platform Windows.*

Pada pengujian serangan dengan single prefix (satu *host* yang mem-*broadcast RA flood*), sbagian besar platform yang diuji mengalami *crash* (tidak meresepon). Hasil lebih detail bisa dilihat di tabel 1. Pada saat dilakukan serangan, hampir seluruh platform Sistem Operasi *Windows* terganggu terlihat dari Utilisasi CPU mencapai 100% termasuk pada Platform sistem Operasi *Windows Server* 2016 (pada gambar 6).

Kecuali pada sistema dengan platform Sistem Operasi *Windows* 10 dan *Windows Server* 2012.



**Gambar 6. Dampak Serangan pada *Windows Server* 2016 dengan 1000 Paket *Flood***

### 3.2.2 *Multi Prefix Router Advertisement Attack*

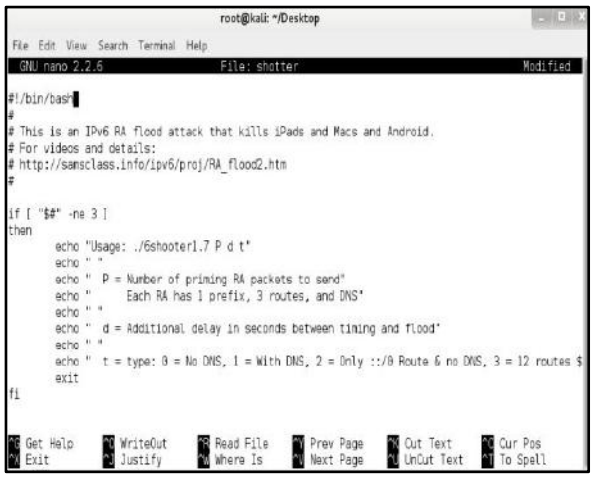
Pada pengujian selanjutnya dilakukan dengan penambahan *multi prefix Router Advertisement* yang menyerang yang melakukan *RA flood*. Untuk melakukan serangan dengan *multi route* ini digunakan *tools thc-ipv6-3.2.* Setelah diinstal pada komputer maka dibuat *script* yang dikembangkan oleh (Bowne, 2012) untuk menjalankan *fake router*secara simultan. Untuk *script* yang dibuat bisa dilihat pada gambar 7.

**Tabel 1. Hasil Pengujian Serangan Paket *RA Flood Single Prefix***

| Platform OS Target | 1000 paket *flood* | | 10.000 paket *flood* | | Keterangan |
|---|---|---|---|---|---|
| | *% memori* | *% CPU* | %memori | %CPU | |
| *Windows* XP Service Pack 1 | 30% | Menyentuh 90% tapi langsung turun | 30% | hingga 100% stagnan | Terganggu dengan serangan *RA flood* |
| *Windows* 7 | 22% | hingga 100% stagnan | 33% | hingga 100% stagnan | Terganggu dengan serangan *RA flood* |
| *Windows* 8.1 | 45% | Menyentuh 97% kemudian menurun | 50% | Stagnan di 100% | Terganggu dengan serangan *RA flood* |
| *Windows* 10 Pro | 50% | Normal | 50% | Normal | Tidak terganggu dengan serangan *RA flood* |
| *Windows Server* 2008 | 20% | Stagnan 100% | 37% | Stagnan 100% | Sistem *Crash* dengan serangan *RA flood* |
| *Windows Server* 2012 | 20% | Normal | 20% | Normal | Tidak terganggu dengan serangan *RA flood* |
| *Windows Server* 2016 | 60% | stagnan hingga 100% | 60% | stagnan hingga100% | Terganggu dengan serangan *RA flood* |

### 3.2.3 *Multi Prefix Router Advertisement Attack*

Pada pengujian selanjutnya dilakukan dengan penambahan *multi prefix Router Advertisement* yang menyerang yang melakukan *RA flood*. Untuk melakukan serangan dengan *multi route* ini digunakan *tools thc-ipv6-3.2.* Setelah diinstal pada komputer maka dibuat *script* yang dikembangkan oleh (Bowne, 2012) untuk menjalankan *fake router*secara simultan.Untuk *script* yang dibuat bisa dilihat pada gambar 7.

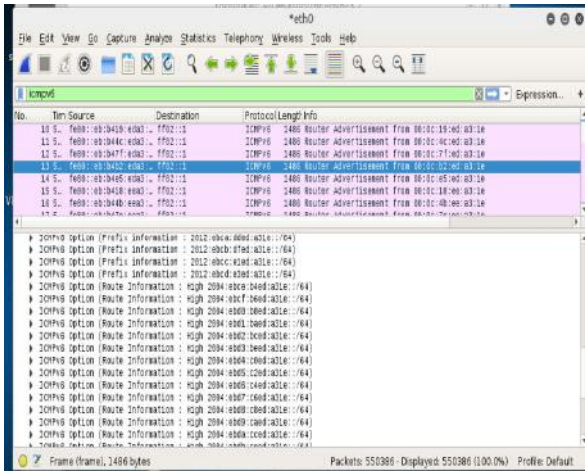



**Gambar 7. *Script* Serangan dengan *Multi Prefix Router Advertisement***

Setelah *script* dibuat kemudian dijalankan seperti pada gambar 8.


**Gambar 8. Proses Pengiriman Paket Serangan dengan *Multi Prefix Router Advertisement***

Pada gambar 8 *script* router dijalankan dengan diikuti dengan angka 3 5 3. Angka 3 yang pertama berarti dikirim 3 paket RA (masing-masing terdiri dari 1 prefix, 3 route dan DNS). Angka 5 menunjukkkan delay paket RA dalam detik antar *flood.* Opsi 3 menunjukkan jenis serangan untuk route dan DNS. Dan dampak dari proses serangan bisa dilihat detail paket yang dikirim dengan menggunakan *tools wireshark* seperti pada gambar 9.




**Gambar 9. Paket serangan *Multi Prefix***

Dari gambar 9 bisa dilihat normal paket RA yang dikirim yang terdiri dari 17 *Route information Section*, 18 *Prefix Information Section* dan 1 *source link layer address*. Sehingga lebih banyak paket yang membanjiri jaringan. Dampaknya sangat berdampak besar pada jaringan yang dibanjiri terutama pada *host-host* yang terhubung ke jaringan.

## 3.3 Hasil Pengujian

Dari hasil pengujian pengiriman paket RA flood yang dilakukan bisa dilihat pada tabel 1. Dari tujuh platform Sistem Operasi *Windows*

yang diuji hampir semua platform secara default meng-*enable IPv6*. Kecuali untuk Sistem Operasi *Windows* XP IPv6 harus diinstal. Sehingga hampir semua platform yang mengaktifkan IPv6 akan meresponse pada saat dikirimi paket *RA flood*. Dari seluruh platform Sistem Operasi *Windows* yang diuji hampir seluruh platform terganggu dengan pengiriman *Single Prefix router Advertisement* secara terus menerus kecuali pada Sistem operasi *Windows* 10 dan *Windows Server* 2012.

Dampak dari serangan *RA flood IPv6* sangat berpengaruh pada penggunaan prosesor pada *host* yang menerima paket. Untuk penggunaan *memory* tidak terlihat peningkatan penggunaan *memory* secara signifikan. Dengan meningkatnya penggunaan CPU yang mencapai 100% berdampak pada komputer menjadi *crash* dan hampir tidak bisa menjalankan aplikasi atau perintah lainnya.

Untuk pengujian dengan menggunakan *thc-ipv6* yang bisa menambah jumlah *route* penyerang yang mengirim paket *flood* yang lebih banyak secara serentak memperlihatkan utilisasi *CPU* yang cukup berat termasuk pada Sistem Operasi *Windows* 10 yang terkoneksi di jaringan. Jika dilakukan pada jaringan system virtual yang memiliki resource yang terbatas, maka OS yang menerima paket dalam waktu hitungan menit langsung *crash* tidak bisa merespon untuk semua Platform. Sedangkan pada Sistem Operasi *Windows* 10 dan *Windows Server* 2012 diuji pada sistemyang tidak virtual, serangan tersebut mengakibatkan kenaikan utilisasi CPU secara signifikan meskipun dan respon dari system menjadi melambat. Respon dari sistem bisa dilihat pada tabel 2.

**Tabel 2. Hasil Pengujian Serangan *RA Floodmulti Prefix***

| OS Target | Respon |
|---|---|
| *Windows* XP | Sistem crash tidak merespon |
| *Windows* 7 | Sistem crash tidak merespon |
| ***Windows* 8.1** | Sistem crash tidak merespon |
| ***Windows* 10 Pro** | Utilisasi CPU meningkat, tapi tidak crash |
| ***Windows Server* 2008** | Sistem crash tidak merespon |
| ***Windows Server* 2012** | Utilisasi CPU meningkat , tapi tidak crash |
| ***Windows Server* 2016** | Respon sistem menjadi lambat |

## 3.4 Penanganan Serangan *IPv6 RA flood*

Untuk menangani serangan *IPv6 Router Advertisement,* ada beberapa mekanisme yang bisa dilakukan, yaitu antara lain:

1) IPv6 sebaiknya di-*disable* jika memang tidak diperlukan. Kecuali jika kita harus terkoneksi pada jaringan IPv6 maka perlu kita aktifkan.
2) Melakukan konfigurasi manual untuk *Router Discovery* dan firewall.
   a. Menurut Bowne & Prince, 2013 proses menonaktifkan *Router Discovery*bisa mencegah *Router Advertisement* meng-generate IPv6 untuk diri mereka sendiri. Cara ini bisa mencegah sistem menggunakan *Stateless Auto Configuration* (konfigurasi alamat IPv6 secara otomatis). Sebaiknya sistem diseting menggunakan IPv6 statis. Akan tetapi cara ini tidak memungkinkan digunakan pada client, untuk mengkonfigurasi sendiri alamat IPv6 secara statis. Pilihan ini bisa kita lakukan pada sistema yang terbatas, misalnya *Server*.

b. Alternatif kedua melakukan konfigurasi *firewall* di masing-masing perangkat untuk memblokir paket *Router Advertisement* palsu. Di *firewall* dibuat *Accsess Control List*yang akan mengizinkan Router Advertisement dari gateway yang sebenarnya. Meskipun dalam prakteknya IP *Gateway* bisa di-*defeated*. Kendala lain proses konfigurasi firewall.
c. Alternatif lain untuk mengatasi *Router Advertisement Flood* ini dengan menggunakan *Smart Switch* yang memiliki fitur *RA Guard*, seperti dijelaskan oleh (Chown, T., & Venaas, S. 2011).

Untuk pengujian dilakukan konfigurasi pada setiap platform untuk menonakatifkan *Router Discovery.* Kemudian setelah menonaktifkan *Router Discovery* maka dilakukan pengujian dengan membanjiri paket*Router Advertisement.* Terlihat hasil dari masing-masing platform yang dicoba proses utilisasi CPU berjalan normal, tidak terganggu dengan paket *flooding Router Advertisement* yang dikirim.

Konfigurasi paket *Router Advertisement* dan *firewall* pada client bisa mengatasi paket *flooding Router Advertisement.* Akan tetapi bagi pengguna awam tentu saja solusi ini sangat menyulitkan. Sehingga solusi terbaik adalah sangat diperlukannya *update patching* dari pengembang Sistem Operasi khususnya Microsoft *Windows* untuk masing-masing platform. Solusi lain yang terbaik OS sehingga tidak menyulitkan penggunanya. Dan untuk perusahaan yang sudah siap menggunakan IPv6 sebaiknya menggunakan *smart switch* untuk mengatasi serangan *IPv6 Router Advertisement flood* di jaringan.

## 4. SIMPULAN

Dari hasil penelitian dapat disimpulkan antara lain: (1) Untuk Platform Sistem Operasi *Windows* hanya Sistem Operasi *Windows 10* dan *Windows Server 2012 R2* yang tidak terganggu dengan pengujian serangan paket *RA Ipv6 flood,* tetapi pada saat diuji dengan serangan multi *prefix Router Advertisement* utilisasi *CPU* cukup berat meskipun tidak mengakibatkan sistem menjadi crash.; (2) Pada jaringan IPv4 untuk mengatasi serangan *IPv6 RA flood* sebaiknya di masing-masing platform IPv6 di non aktifkan. Khusus untuk platform jaringan IPv6 sebaiknya Router *Advertisary* dinonaktifkan, kecuali jika *host* berfungsi sebagai *router*.; (3) instansi/kantor yang sudah menggunakan IPv6 sebaiknya menggunakan *smart switch* yang mendukung fitur *RA Guard* untuk melindungi *host client* dari serangan *Router Advertisement flood*.; (4) Untuk pengujian *RA flood Advertisemen*t perlu juga diuji pada *Router Managable* untuk melihat dampak dari serangan tersebut.

## DAFTAR RUJUKAN

Atik Pilihanto, Rick Wanner. 2012. *A Complete Guide on IPv6 Attack and Defense*, SANS Institute InfoSec Reading Room.

Beck, F., Cholez, T., Festor, O., & Chrisment, I. 2007. *Monitoring the Neighbor Discovery Protocol.* International Multi-Conference on Computing in the Global Information Technology, Guadeloupe City, France.

Bosworth, S., Kabay, M. E., & Whyne, E. (Eds.). 2012. *Computer Security Handbook, Set* (5th ed.). John Wiley & Sons, Inc. Hoboken, NJ.

Bowne, S., & Prince, M. 2013. *Evil DoS Attacks and Strong Defenses.* PowerPoint slides. [Online]. (Diakses https://www.defcon.org/images/defcon-21/dc-21- presentations/Bowne-Prince/DEFCON-21-Bowne-Prince-Evil-DoS-Attacks-and- Strong-Defenses.pdf, tanggal 23 Mei 2017).

Bowne, S. 2012.*New RA Flood Attack.* [Online]. (Diakses https://www.researchgate.net/ publication/266022049_ICMPv6_Router_ Advertisement_Flooding, tanggal 7 Juli 2018).

Brashars, J. 2007. *Asterisk Hacking.* Syngress Publishing, Inc. Burlington, MA.

Chown, T., & Venaas, S. 2011. *Rogue IPv6Router Advertisement Problem Statement*. RFC 6104, February 2011.

Durdagi, E. dan Buldu, A. 2010. *Ipv4/Ipv6 Security And Threat Comparisons*. Procedia-Social and Behavioral Sciences, 2(2), pp.5285-5291.

Google. 2018. [Online]. (Diakses https://www.google.com/intl/en/ipv6/ statistics.html, tanggal 6 Agustus 2018).

Houston, Geof. 2016. *IPv4 Address Report.* [Online]. (Diakses http://www.potaroo.net/tools/*IPv4*/index.html., tanggal 18 Mei 2018).

Kaur, R., & Sharma, S. 2014. *The Security Issues of IPv6 Routing Protocol - A Study.* International Journal of Computer Applications & Information Technology, *5*(2), 53-60. [Online]. (Diakses http://www.ijcait.com/IJCAIT/52/ 523.pdf, tanggal 18 Mei 2018).

K. Scarfone, M. Souppaya, A. Cody, A.ngela Orebaugh. 2008. *Technical Guide to Information Security Testing and Assesment.* Recomendations of the National Standard and Technology. NIST Special Publicaton 800-115.

Marguerite G. Lodico, Dean T. Spaulding, Katherine H. Voegtle. 2010. *Methods In Educational Research: From Theory To Practice, 2nd Edition* (United States of Jossey-Bass A Wiley imprint, h. 230. America.

Network Working Group. 1998. *RFC 2460 Internet Protocol Version 6 (IPv6) Specification.* [Online]. (Diakses https://www.ietf.org/rfc/rfc2460.txt., tanggal 20 Mei 2018).

Shrivastava, G., Sharma, K., & Rai, S. 2010. *The Detection & Defence of DoS & DDoS Attack: A Technical Overview*. International Conference on Computer Engineering and Technology, New Delhi, [Online]. (Diakses http://jietjodhpur.com., tanggal 10 Mei 2018).

Tripathi, N., & Mehtre, B. M. 2013. *DoS and DDoS Attacks: Impact, Analysis and Countermeasures*. National Conference on Advances in Computing, Networking and Security, Nanded, India.

University of Southern California. 1981. *RFC 791 Internet Protocol*. [Online]. (Diakses https://www.ietf.org/rfc/rfc791.txt., tanggal 20 Mei 2017]

Vikram P. Solanki, Prof. Mitesh Thakkar. 2014. *A Comprehensive Study on Various Security Attacks against IPv6.* International Journal Of Engineering Development And Research - IJEDR Volume 1, Issue 3 Dec 2014, hal. 198-201.