

PROSIDING

SEMINAR NASIONAL ILMU KOMPUTER

**CYBER WAR AND
DATA SECURITY**

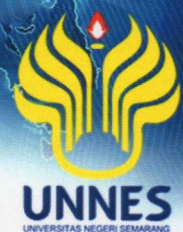
VOLUME 1

10 OKTOBER 2017

Penyelenggara:

Jurusan Ilmu Komputer
Fakultas Matematika dan
Ilmu Pengetahuan Alam

Universitas Negeri Semarang
Semarang - Indonesia



<https://conf.unnes.ac.id/index.php/snik/>

PROSIDING SEMINAR NASIONAL ILMU KOMPUTER 2017

"Cyber War and Data Security"

Editor:

Much Aziz Muslim, S.Kom., M.Kom.

Aji Purwinarko, S.Si., M.Cs.

Budi Prasetyo S.Si., M.Kom.

Anggyi Trisnawan Putra, S.Si., M.Si.

Maulana Nur Ardian

Nova Cahyani

Anita Ayu Septiantina

Fadli Dony Pradana



FMIPA

Universitas Negeri Semarang

PROSIDING

SEMINAR NASIONAL ILMU KOMPUTER 2017

"Cyber War and Data Security"

ISSN: 2614-1205

Susunan Editorial

Penanggung jawab

Prof. Dr. Zaenuri, S.E., M.Si., Akt.

Tim Review

Dr. Dwijanto, M.S. (Matematika Unnes)

Dewi Handayani Untariningsih, S.Kom., M.Kom. (Unisbank)

Endang Sugiharti, S.Kom., M.Kom. (Ilkom UNNES)

Alamsyah, S.Si., M.Kom. (Ilkom UNNES)

Riza Arifudin, S.Pd., M.Cs. (Ilkom UNNES)

Zaenal Abidin, S.Si., M.Cs. (Ilkom UNNES)

Much Aziz Muslim, S.Kom., M.Kom. (Ilkom UNNES)

Ketua

Anggyi Trisnawan Putra, S.Si., M.Si.

Tim Editor

Much Aziz Muslim, S.Kom., M.Kom.

Aji Purwinarko, S.Si., M.Cs.

Budi Prasetyo S.Si., M.Kom.

Maulana Nur Ardian

Nova Cahyani

Anita Ayu Septiantina

Fadli Dony Pradana

Cover Layout

Adinda Audia Caessarani Adrian

Distribusi

Florentina Yuni Arini, S.Kom., M.Cs.

Penerbit:



SUSUNAN PANITIA

Pengarah

Endang Sugiharti, S.Si., M.Kom.

Ketua

Anggyi Trisnawan Putra, S.Si., M.Si.

Koordinator Mahasiswa

Maulana Nur Ardian

Sekretaris

Aji Purwinarko, S.Si., M.Cs

Nova Cahyani

Bendahara & Konsumsi

Florentina Yuni Arini, S.Kom., M.Cs.

Anita Ayu Septiantina

Sie. Acara

Much Aziz Muslim, S.Kom., M.Kom.

Anita Ayu Septiantina

Sie. Multimedia & Publikasi

Budi Prasetyo, S.Si., M.Kom.

Adinda Audia Caessarani Adrian

Nurinda Delviana

Sie. Pendaftaran & Prosiding

Riza Arifudin, S.Pd., M.Cs.

Maulana Nur Ardian

Nova Cahyani

Fadli Dony Pradana

Sie. Perlengkapan

Alamsyah, S.Si., M.Kom.

Subhan, S.Pd., M.Pd., M.Kom.

Moh Minhajul Mubarak

Adisakti Almajid

DAFTAR ISI

PROSIDING SEMINAR NASIONAL ILMU KOMPUTER 2017 "Cyber War and Data Security"

Kode	Penulis	Judul	Halaman
Bidang Kajian: Bioinformatika			
884	Sri Karnila, Rio Kurniawan, Sri Lestari, Suhendro Y. Irianto	Aplikasi Pengenalan Wajah Menggunakan Teknik CBIR untuk Objek Tampak Depan	1-5
885	Dona Yuliawati, Wasilah, Suhendro Irianto	<i>Search Engine-Like</i> Berbasis Citra untuk Fauna Indonesia	6-13
891	Jani Kusanti, Yusuf Zain Santosa	Optimum Parameter Citra Sel Kanker Payudara Dalam Mengidentifikasi Sel Kanker Payudara	14-22
Bidang Kajian: Data Warehouse and Data Mining			
966	Dian Adi Nugroho, Ristu Saptono, Denis Eka Cahyani	Rekomendasi Lokasi Cabang Baru Menggunakan Metode <i>Single Pass Clustering</i> (Studi Kasus: Waralaba Susu dan Perlengkapan Bayi Murah di Karanganyar)	23-30
Bidang Kajian: Keamanan Data dan Jaringan (KJ)			
908	Ilman Zuhri Yadi, Yesi Novaria Kunang, Suzi Oktavia Kunang	Analisis Celah Keamanan Serangan <i>Router</i> <i>Advertisement IPv6 Flood</i> di Jaringan	31-39
913	Rubiyanto, Selo, Widyawan	Konseptual Model Keamanan Sistem Pemanfaatan Data Kependudukan di Tingkat Kabupaten	40-48
10001	Budi Handoko, Aisyatul Karima, Ari Saputro	Efektifitas Algoritma ElGamal untuk Perlindungan Dokumen PDF	49-57
Bidang Kajian: Komputasi Terdistribusi			
963	Rosalinan Br Ginting, Maryanto, Ika Menarianti	Desain Media Pembelajaran Mata Kuliah Kebijakan Publik Berbasis <i>Interactive Whiteboard</i>	58-64
Bidang Kajian: Machine Learning			
879	Sukmawati Nur Endah, Retno Kusumaningrum, Helmie Arif Wibawa	Ruang Warna untuk Deteksi Citra Kulit: Kinerja dan Implikasinya	65-70
888	Adriana Fanggidae, Meito Boru	Analisis Algoritma DE, ABC, PSO dalam Penentuan Parameter Karakteristik <i>Input-Output</i> Pembangkit Termal	71-78
Bidang Kajian: Sistem Informasi dan Aplikasinya			
863	Irma Salamah, RD Kusumanto	Analisis Faktor- Faktor yang Mempengaruhi Minat Perilaku Pengguna Layanan 3G di Politeknik Negeri Sriwijaya	79-85

Kode	Penulis	Judul	Halaman
869	Munengsih Sari Bunga, Ahmad Lubis Ghozali, Willy Permana Putra	Analisis dan Perancangan Sistem Informasi Realisasi Pendapatan dan Belanja Berbasis Web di Dinas Pendidikan Indramayu	86-93
875	Yoga Pratama, Rudy Hartanto, Sri Suning Kusumawardani	Pengembangan Awal Model Evaluasi Dukungan YouTube terhadap <i>Learning Performance</i>	94-99
886	Erzan Miftah Faridi, Sukmawati Nur Endah	Penerapan <i>Vector Space Model</i> dalam Pencarian Dokumen Jurnal Berbahasa Indonesia Dengan Query Berupa Ucapan	100-108
889	Bayu Mukti, Bambang Soedijono W.A., Hanif Al Fatta	Pengaruh <i>User Interface</i> Aplikasi <i>Mobile</i> Terhadap <i>Learnability</i> dan <i>Efficiency</i> Pengguna	109-117
893	Robet Habibi	Arsitektur Aplikasi untuk <i>Smart Campus</i> dengan Teknologi <i>Internet of Things</i> Berdasarkan Perencanaan Strategis Sistem Informasi STMIK Bina Patria	118-125
894	Wahyu Priyoatmoko, Robet Habibi	Analisis Arsitektur Jaringan untuk <i>Smart Campus</i> di STMIK Bina Patria	126-131
897	Dinar Budi Saputro, Ristu Saptano, Winarno	Lapak Sragen: Pengembangan <i>Close Registration</i> <i>E-Commerce</i> Produk Lokal dengan Metode Prototyping	132-140
898	Erika Devi Udayanti, Fajar Agung Nugroho, Indah Hapsari Putri	TB <i>eScoring</i> Berbasis Android sebagai Alat Bantu Penegakan Diagnosis Tuberkulosis Anak	141-148
903	Deny Martha, Marsani Asfi, Abdul Fatoni	Aplikasi Perhitungan Pembagian Harta Waris Berdasarkan Islamologi Berbasis <i>Mobile</i>	149-157
905	Lena Magdalena, Resti Puji Astuti, Imas Mufti, Deny Martha	Pengembangan Sistem Informasi Akuntansi Penerimaan Kas dan Pengeluaran Kas di Eka Jaya Berrindo Cirebon	158-166
906	Bimo Hario Andityo, Sasongko Pramono Hadi, Lukito Edi Nugroho	Perancangan Standar Operasional Prosedur (SOP) Manajemen Proyek Teknologi Informasi pada Tahap Pengadaan di Biro TI BPK RI	167-174
911	Ida Sekarsari, Eko Nugroho, Ridi Ferdiana	Model <i>Hot-Fit</i> Modifikasi untuk Mengukur Kesuksesan dan Penerimaan Sistem Informasi dan Manajemen Objek Pajak (SISMIOP)	175-181
912	Titik Purwantiningsih, Eko Nugroho, Ridi Ferdiana	Evaluasi Kualitas Website BPS Provinsi Jawa Tengah Menurut Persepsi Pengguna	182-188
914	Titik Purwantiningsih, Eko Nugroho, Ridi Ferdiana	Model Konseptual: Pengaruh Kualitas Website terhadap Loyalitas	189-196
915	Paras Trapsiladi, Lukito Edi Nugroho, Sri Suning Kusumawardani	Urgensi Identifikasi Kepemilikan Data dan <i>Service</i> pada Sistem Berbasis SOA Pemerintahan (Studi Kasus GSB Kementerian Kominfo RI)	197-204
916	Aris Irwanto, Lukito Edi Nugroho, Eko Nugroho	Pengendalian Internal Teknologi Informasi Sistem Informasi Pengelolaan Keuangan Negara	205-210
917	Ida Sekarsari, Eko Nugroho, Ridi Ferdiana	Evaluasi Faktor-Faktor Keberhasilan Implementasi Sistem Informasi dan Manajemen Objek Pajak	211-216

Kode	Penulis	Judul	Halaman
		(SISMIOP) pada Badan Keuangan dan Aset daerah Kabupaten Bantul dengan Metode <i>Hot-Fit</i> Modifikasi	
925	Dita Amalia, Rudy Hartanto, Ridi Ferdiana	<i>Scenario Development method: Literature Review</i>	217-224
964	Perry Sunandar, Sasongko Pramono Hadi, Wing Wahyu Winarko	Perancangan Aplikasi Dukcapil Berbasis Android pada Pelayanan Kependudukan dan Catatan Sipil	225-230
984	Anggyi Trisnawan Putra, Alamsyah	Perancangan Struktur Basis Data Aplikasi Asesmen Online (e-ujian)	231-237
1004	Anggyi Trisnawan Putra, Mona Subagja	Perancangan Struktur Basis Data Tunggal di Universitas Negeri Semarang	238-241
Bidang Kajian: Sistem Pendukung Keputusan			
880	Mazaya Galva Santoso, Retno Kusumaningrum	Sistem Pendukung Keputusan Penentuan Pemenang Pengadaan Mobil Dinas Menggunakan Metode <i>Promethee</i> (Studi Kasus: PT PLN (Persero) Pusat Sertifikasi)	242-248
890	Ramadhian Agus Triono, Noor Abdul Haris	Persepsi Risiko Film <i>Battle of Surabaya</i> pada Karakteristik <i>Leader/Follower</i> yang Mempengaruhi Perilaku Terhadap Risiko	249-255
918	Juliana, Jasmir, Pareza Alam Jusia	Sistem Pendukung Keputusan untuk Pemilihan Supplier menggunakan Metode <i>Analytical Aierarchy Process</i> (AHP) (Studi Kasus: Toko Harapan Baru)	256-264
922	Anita Ayu Septiantina, Irahayu Sukmadewanti, Feroza Rosalina Devi	Penentuan Mahasiswa Berprestasi Berbasis Sistem Pendukung Keputusan Menggunakan Metode <i>Simple Additive Weighting</i> (SAW)	265-270
923	Nova Cahyani, Shinta Hardiyanti, Aldi Nurzahputra	Penerapan Metode <i>Net Present Value</i> (NPV) pada <i>Decision Support System</i> Analisis Kelayakan Usaha Mikro Kecil dan Menengah	271-279
967	Mirra Prasasti, Ristu Saptono, Winarno	Sistem Rekomendasi Peminjaman Buku di UPT Perpustakaan UNS dengan Metode <i>Item-based Collaborative Filtering</i> dan <i>Rating</i> Implisit	280-287

Analisis Celah Keamanan Serangan *Router Advertisement IPv6 Flood* di Jaringan

Ilman Zuhri Yadi¹, Yesi Novaria Kunang², Suzi Oktavia Kunang³

^{1,2,3}Program Studi Sistem Informasi, Fak. Ilmu Komputer, Universitas Bina Darma
Email: ¹ilmanzuhriyadi@binadarma.ac.id, ²yesinovariakunang@binadarma.ac.id,
³suzi_oktavia@binadarma.ac.id

Abstrak

Protokol IPv6 dikembangkan untuk menggantikan IPv4. Akan tetapi beberapa fitur yang ada di IPv6 bisa dimanfaatkan sebagai serangan *Denial of Service* (DOS). Salah satunya adalah *Neighbour Discovery Protocol* (NDP) yang dikembangkan di *protocol* IPv6. Proses NDP menggunakan *Internet Control Message Protocol IPv6* (ICMPv6). Sebagai contoh, proses NDP *Stateless Address Autoconfiguration* menggunakan ICMPv6 *Router Advertisement messages* (*Router Advertisement*). *Router Advertisement* memungkinkan komputer di jaringan IPv6 untuk menghasilkan sendiri alamat IPv6. *Router Advertisement* bisa digunakan untuk melakukan serangan DoS di jaringan IPv6 DoS yang disebut serangan *Router Advertisement Flood*. Penelitian ini merupakan penelitian eksperimen yang akan adalah menganalisis sejauh mana perangkat komputer dan *smartphone* dengan berbagai *platform OS* yang terkoneksi di jaringan IPv6 bereaksi terhadap serangan RA IPv6 flooding. Hasil penelitian memperlihatkan *platform MacOS* tidak terpengaruh dengan serangan flooding IPv6 RA, sedangkan *platform Windows, Linux* dan *Android* cukup terpengaruh dengan banjir paket di jaringan. Hasil penelitian juga memberikan rekomendasi untuk menutupi kelemahan di masing-masing *platform* (*Windows, Linux, Mac* dan *Android*) tersebut.

Kata Kunci: DOS, IPv6, Router Advertisement

Abstract

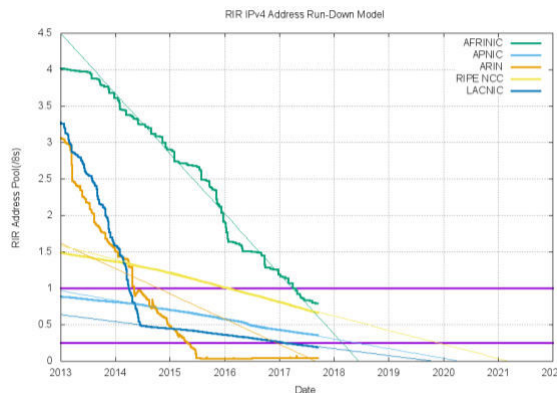
The IPv6 protocol was developed to replace IPv4. However, some features in IPv6 can be used as Denial of Service (DoS) attacks. One is the Neighbor Discovery Protocol (NDP) developed in the IPv6 protocol. The NDP process uses Internet Control Message Protocol IPv6 (ICMPv6). For example, the NDP Stateless Address Autoconfiguration process uses ICMPv6 Router Advertisement messages (Router Advertisement). Router Advertisement allows computers on IPv6 networks to generate their own IPv6 addresses. Router Advertisement can be used to perform DoS attacks on IPv6 network DoS called Router Advertisement Flood attacks. This study is an experimental research that will be analyzing the extent to which computer devices and smartphones with various OS platforms connected to the IPv6 network react to RA IPv6 flooding attacks. The results show the MacOS platform is not affected by IPv6 RA flooding attacks, while the Windows, Linux and Android platforms are quite affected by packet flooding on the network. The results also provide recommendations to cover the weaknesses in their respective platforms (Windows, Linux, Mac and Android).

Keyword: DOS, IPv6, Router Advertisement

1. PENDAHULUAN

Internet Protocol versi 4 (IPv4) khususnya di Indonesia sampai saat ini masih banyak digunakan sebagai Protokol Internet utama. IPv4 memiliki panjang alamat 32-bit yang mendukung 2^{32} alamat atau sekitar 4,294 juta alamat. Berdasarkan Report Geoff

Houston *IPv4 Address Report*, *IPv4* mulai mengalami fase jenuh pada awal tahun 2011 [1]. Pada 3 Februari 2011 *Internet Assigned Numbers Authority (IANA)* kehabisan alamat *IPv4* yang belum dialokasikan mereka pada 3 Februari 2011. Dalam beberapa tahun, setiap *Regional Internet Registry (RIR)* akan kehabisan *IPv4* yang belum dialokasikan; kecuali *Asia Pacific Network Information Centre (APNIC)* yang sudah kehabisan alamat yang bisa dialokasikan pada 19 April 2011. 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*. Gambaran penggunaan *RIR address pools* yang tersisa dapat dilihat pada Gambar 1 dibawah ini.



Gambar 1. Gambaran penggunaan *RIR address pools* yang tersisa [1]

Internet Protokol versi 6 (*IPv6*) adalah versi terbaru dari *Internet Protocol*, dirancang sebagai pengganti *Internet Protocol* versi 4 [2]. *IPv6* dirancang untuk memenuhi pertumbuhan pengguna *internet* yang makin pesat. *IPv6* memiliki panjang alamat 128-bit, sehingga dapat mendukung 2^{128} alamat atau sekitar 3.4×10^{38} alamat. Selain jumlah alamat yang lebih banyak *IPv6* juga memiliki beberapa perubahan lain.

Akan tetapi dalam implementasinya ada beberapa masalah yang ditemui pada penggunaan *IPv6* dan keamanannya. Beberapa perangkat pengamanan masih belum mendukung *IPv6* sementara pada beberapa perangkat yang mendukung *IPv6* tidak dikonfigurasi dengan benar oleh administrator. Oleh karenanya, beberapa *firewall*, dan *IDS* dapat mendeteksi serangan lalu lintas data (*traffic data*) berbahaya pada protokol *IPv4*, akan tetapi penyerang masih bisa melewati mekanisme kontrol dan deteksi dengan mengirimkan lalu lintas data *IPv6* berbahaya. Kekhawatiran lainnya adalah kelemahan pada *IPv6* yang dapat digunakan oleh penyerang untuk melakukan serangan jaringan ke *IPv6*. Penelitian untuk pengujian keamanan jaringan *IPv6* telah dilakukan. Misalnya, A Pilihanto menerbitkan makalahnya tentang serangan ke *IPv6* dan mekanisme pertahanannya dalam *SANS Institute* [3], sementara Vicram 2014 melakukan penelitian berbagai serangan pada *IPv6* [4].

Neighbor Discovery Protocol (NDP) merupakan salah satu protokol utama yang digunakan pada *IPv6*. Proses *NDP* termasuk di dalamnya *Router Discovery (RD)* dan *Stateless Address Autoconfiguration (SLAAC)*. *RD* memungkinkan *node* untuk menemukan router terdekat di jaringan dan *SLAAC* memberikan parameter jaringan

untuk memungkinkan *host* menghasilkan alamat *IPv6* untuk diri mereka sendiri. RD dan *SLAAC* dibutuhkan Internet Protocol versi 6 (*ICMPv6*) *RA messages* (*Router Advertisement*).

Router Advertisement (*RA*) pada saat *broadcast* ke jaringan tidak perlu dikonfirmasi oleh *host* yang menerima paket tersebut, sehingga paket *RA* bisa digunakan untuk melakukan serangan *link-local DoS* dengan cara membanjiri jaringan dengan paket *RA*. Serangan *RA Flood* ditemukan pada tahun 2011 [5]. Alangar & Swaminathan (2013) menyebutkan meskipun serangan *RA Flood* sudah ditemukan beberapa waktu lalu, sampai saat ini masih bisa dieksploitasi [6].

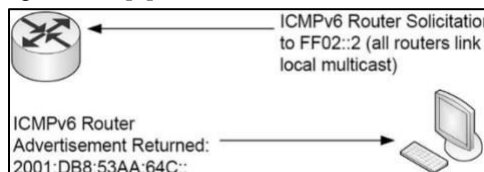
Beberapa penelitian telah membahas mekanisme pertahanan yang bisa digunakan untuk menghadapi berbagai *link-local* serangan *IPv6 DoS* termasuk *RA flood*. Penelitian lain juga telah mengembangkan dan menguji sejumlah mekanisme pertahanan terhadap serangan tersebut. Namun penelitian tersebut belum ada yang melakukan percobaan untuk membandingkan efisiensi pertahanan terhadap serangan *RA Flood* terhadap beberapa sistem operasi (SO) dan perangkat yang terkoneksi ke jaringan terutama untuk SO dan perangkat terbaru. Untuk itu pada penelitian ini bertujuan menganalisis sejauh mana perangkat komputer dan *smartphone* dengan berbagai *platform OS* yang terkoneksi di jaringan *IPv6* bereaksi terhadap serangan *RA IPv6 flooding*. Serta mencari solusi terbaik untuk menutupi kelemahan di masing-masing *platform* (*Windows, Linux, Mac* dan *Android*) tersebut.

2. METODE

2.1. Router Advertisement Flood Attack

NDP Stateless Address merupakan proses konfigurasi otomatis yang menggunakan pesan *ICMPv6* tertentu untuk menghasilkan alamat *IPv6* pada segmen jaringan lokal. Pesan *ICMPv6* yang digunakan oleh proses *SLAAC* adalah *Router Solicitations* (*RS*) dan *Router Advertisement* (*RA*). *Host* dari jaringan *IPv6* dapat secara otomatis menghasilkan alamat *IPv6* untuk dirinya sendiri.

Untuk komunikasi antara LAN, *node* memerlukan alamat *IPv6* global [7]. Untuk menghasilkan alamat *IPv6* global, *host* memerlukan informasi dari *router* menengah. Dengan demikian, administrator jaringan perlu mengatur atau menyusun *router* untuk mengaktifkan *host* untuk menghasilkan alamat *IPv6* global untuk diri mereka sendiri. Gambar 2. Menunjukkan contoh bagaimana cara *RS* dan *RA* dipertukarkan selama proses *SLAAC*. Untuk menghasilkan alamat *IPv6* global, *router* dan *host* menggunakan pesan *ICMPv6* dan *multicasting*. Setelah *router* dikonfigurasi, *router* bergabung dengan *multicast group ff02::2* [8].



Gambar 2. Pertukaran pesan selama *SLAAC* process [9]

Kemudian, jika sebuah *host* mengirimkan *Router Solicitation* ke semua-router *multicast address* ff02::2. Router langsung bereaksi dengan mengirimkan *Router Advertisement* ke alamat *multicast*, ff02::1. *Router Advertisement* dikirim ke semua *link-local* alamat *IPv6* yang aktif [3]. *Router Advertisement* berisi informasi tentang *router default* dan informasi yang diperlukan oleh *host* untuk menghasilkan alamat *IPv6* [8].

Tidak ada mekanisme pembuktian (*authentication*) untuk *Router Discovery* dan proses *SLAAC* [10]. Setiap *node* dalam jaringan dapat mengklaim sebagai *router default* [7]. Dengan demikian, penyerang bisa mengaktifkan klien untuk menggunakan alamat *IPv6 link-local* *host* penyerang sebagai alamat dari *router default* [8].

Seorang penyerang bisa menjalankan serangan *DoS* dikenal sebagai serangan *Router Advertisement (RA) flood* dengan mengirimkan serangan banyak paket *Router Advertisement* ke segmen jaringan lokal untuk menimpa *entry routing* yang sah pada antarmuka suatu *host* [10].

Jika perusahaan tidak menggunakan *IPv6*, maka asumsinya, jaringan tersebut aman dari serangan *IPv6*; Namun *IPv6* diaktifkan secara *default* pada banyak sistem operasi. Oleh karena itu, *host* yang menggunakan *IPv4* dapat membentuk alamat *IPv6* dari serangan *malicious Router Advertisement*. Kemudian penyerang dapat memulai serangan *IPv6* pada jaringan.

Semua *node link-lokal IPv6* akan mengganti *prefix* yang ada dengan *prefix* baru yang *router* sebarikan. *Node* tidak memiliki kemampuan untuk membedakan antara *Router Advertisement* yang sah dan yang berbahaya. Dengan alasan ini, jika *node* penyerang mengirimkan *prefix* invalid yang ada *Router Advertisement*, maka *host* akan mengubah *prefix* mereka yang sah dengan *prefix* yang dikirim. Dengan demikian, berarti komputer yang bisa mengkonfigurasi alamat *IPv6* menggunakan proses *SLAAC* rentan terhadap *spoofing* dan serangan *DoS* [11].

Router Advertisement flood adalah merupakan serangan *IPv6 DoS* di jaringan lokal. Serangan ini membanjiri segmen jaringan lokal dengan *malicious Router Advertisement* untuk menggantikan *entry routing* yang sah pada antarmuka suatu *host* [10].

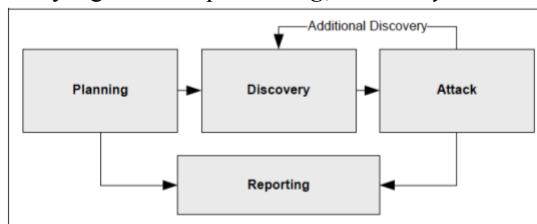
2.2. Metode Penelitian

Penelitian ini merupakan penelitian eksperimen Kuantitatif, karena penelitian ini akan menghasilkan data numerik yang diperoleh dengan berbagai simulasi yang dicoba pada berbagai *platform*. Data yang dihasilkan antara lain *CPU utilisasi*, *memori utilisasi* dan *TCP throughput*. Hasil yang diperoleh akan dievaluasi.

Untuk pengujian celah keamanan paket *RA flooding* ini menerapkan *White Box Testing* yang memperhitungkan mekanisme internal dari sebuah sistem atau komponen. *Penetration testing* yang dilakukan terhadap sistem atau jaringan dengan tipe *white box* ini, biasanya informasi-informasi mengenai sistem atau jaringan sudah diketahui. Tetapi hal tersebut tidak serta-merta memberikan kemudahan dalam melakukan

penetrasi, hal tersebut tergantung dari tester yang melakukan pengujian menilai sejauh mana kelemahan-kelemahan yang terdapat di dalam sistem atau jaringan [12].

Selain menggunakan metode penelitian pengujian *White Box*, penelitian ini juga mengacu pada dokumen *Guideline* untuk Pengujian *Information Security* yang dikeluarkan *United States National Institute of Standards and Technology (NIST)* [13]. Gambar 3. Memperlihatkan rujukan tersebut untuk melakukan fase *Penetration Testing* terdiri dari empat fase yang mencakup *Planning*, *Discovery*, *Attack* dan *Reporting*.

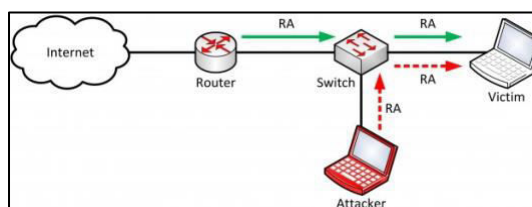


Gambar 3. Fase *methodology penetration testing* [13]

3. HASIL DAN PEMBAHASAN

3.1. Tahapan *Planning*

Pada tahapan *Planning* ini desain simulasi pengujian bisa dilihat seperti pada gambar 4. Untuk *Attacker* menggunakan *host Kali Linux Rolling (kernel Linux kali 4.3.0-kali1-686-pae)*. Sistem operasi (SO) Kali Linux ini dipasang pada Komputer *VirtualBox*. Sebagai *host* korban dilakukan pada 16 Platform Sistem Operasi (SO) sebagai berikut: (1) SO Windows XP; (2) SO Windows 7; (3) SO Windows 8.1; (4) SO Windows 10; (5) SO Windows Server 2008; (6) SO Windows Server 2012; (7) SO Windows Server 2016; (8) SO Linux Ubuntu 14.10; (9) SO Linux Ubuntu 16.04; (10) SO Linux Ubuntu 17.04; (11) SO MacOS El Capitan; (12) SO MacOS Sierra; (13) SO Android versi 4; (14) SO Android versi 5; (15) SO Android versi 6; dan (16) SO Android versi 7.



Gambar 4. Desain simulasi pengujian

Pemilihan *platform* Sistem Operasi Target berdasarkan *platform* terbaru dan yang banyak digunakan. Untuk Target pada penelitian ini digunakan komputer virtual yang di *install* Sistem Operasi yang akan diuji (jika memungkinkan) dengan alasan kemudahan pengujian dan keterbatasan *resource* yang dimiliki saat pengujian. Sedangkan untuk beberapa Sistem Operasi yang membutuhkan *resource* besar maka dilakukan pengujian pada komputer yang di *install* OS target yang terhubung ke komputer penyerang baik dengan koneksi *wireless* ataupun kabel yang terhubung dengan *switch* / *wireless router*.

3.2. Tahapan *Discovery* dan *Penyerangan*

Pada komputer penyerang dibuat *script* sederhana menggunakan *Python* yang dibuat untuk meng-*generate* paket *Router Advertisement* palsu dengan perintah terminal sederhana seperti pada Gambar 5 dan 6.

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

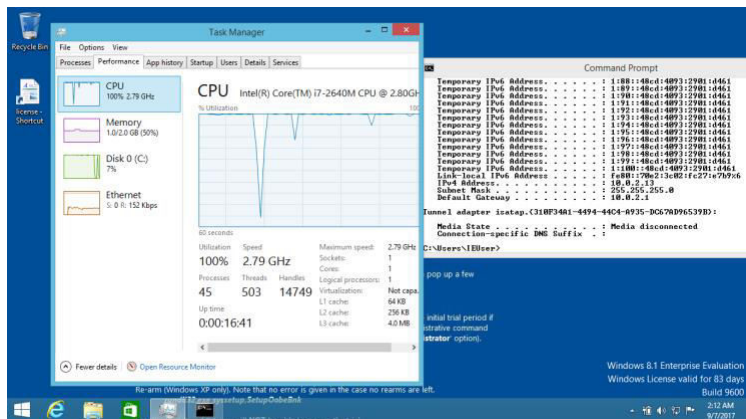
Gambar 5. *Script* untuk meng-*generate* 1.000 paket *router advertisement* palsu.

```
#!/bin/bash
for i in {1..10000}
do
atk6-fake_router26 -A 1:$i::/64 -n 1 eth0
done
```

Gambar 6. *Script* untuk meng-*generate* 10.000 paket *router advertisement* palsu.

Script tersebut dijalankan pada komputer penyerang dengan dua kondisi: (1) Penyerang mengirim 1.000 paket.; (2) Penyerang mengirim 10.000 paket secara simultan. Tujuan dari pengiriman paket tersebut untuk melihat reaksi dari Sistem Operasi target dengan melihat performa *Resource* khususnya pemakaian *Utilisasi CPU* dan juga pemakaian *memory*.

Pada Gambar 7 bisa dilihat salah satu contoh dampak serangan paket *RA flood* di *Windows 8.1* yang memperlihatkan lonjakan *Utilities CPU* yang hampir stagnan menyentuh 100%. Serangan ini jika dibiarkan terus menerus dapat menyebabkan beberapa sistem menjadi *crash* tidak ada reaksi(contoh *Windows Server 2008*).



Gambar 7. Contoh dampak serangan pada *Windows 8.1* dengan 10000 paket *RA*

3.3. Tahapan *Reporting*

Dari hasil pengujian pengiriman paket *RA flood* yang dilakukan bisa dilihat pada tabel 1. Dari empat *platform* yang diuji (*Windows*, *Linux Ubuntu*, *MacOS* dan *Android*)

hampir semua platform secara *default* meng-*enable* IPv6 kecuali *android* versi 4 dan 5 dan *Windows XP*. Sehingga hampir semua *platform* yang mengaktifkan IPv6 akan me-*response* pada saat dikirim paket *RA flood*. Dari keempat platform yang sudah mengantisipasi serangan paket *RA flood* adalah *MacOS* terlihat dari *response utilisasi CPU* yang tidak terganggu dengan adanya paket *RA flood*. Sedangkan *platform* yang paling terganggu dengan adanya serangan IPv6 paket *RA flood* adalah Sistem Operasi *Windows* yang sepertinya *bug*-nya sudah diselesaikan pada *Windows 10*.

Untuk serangan IPv6 paket *RA flood* jika dilihat dari hasil hanya mengganggu *Utilisasi CPU* sedangkan untuk penggunaan *memory* tidak mengalami peningkatan. Akan tetapi jika dibiarkan dampak serangan tersebut dapat mengakibatkan komputer menjadi *crash* tidak me-*response* seperti yang terlihat pada Tabel 1.

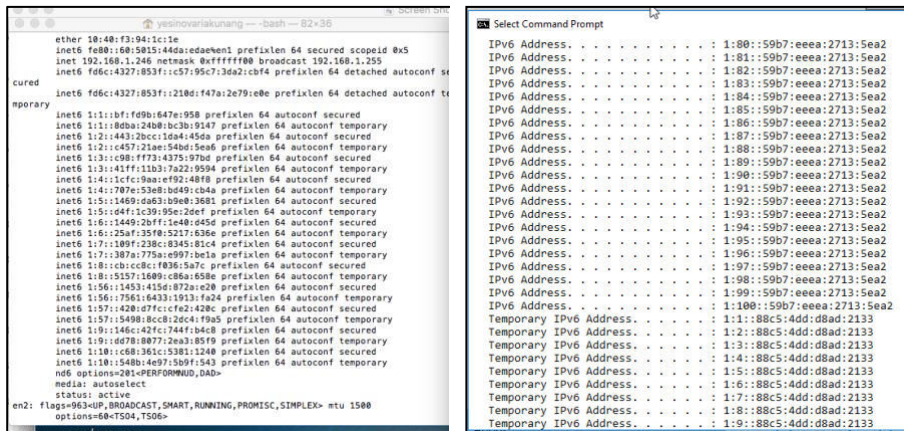
Tabel 1. Hasil Pengujian serangan paket *RA flood*

Platform OS Target	1000 paket		10000 paket		Keterangan
	Utilisasi CPU	Utilisasi memori	Utilisasi CPU	Utilisasi memori	
Windows XP Service Pack 1	Menyentuh 90% tapi langsung turun	30%	Menyentuh 100% stagnan	30%	Terganggu dengan serangan <i>RA flood</i>
Windows 7	Menyentuh 100% stagnan	22%	Menyentuh 100% stagnan	33%	Terganggu dengan serangan <i>RA flood</i>
Windows 8.1	Menyentuh 97% kemudian menurun	45%	Cenderung Stagnan di 100%	50%	Terganggu dengan serangan <i>RA flood</i>
Windows 10 Pro	Normal	50%	Normal	50%	Tidak terganggu dengan serangan <i>RA flood</i>
Windows Server 2008	Stagnan di 100%	20%	Stagnan di 100%	37%	Sistem <i>Crash</i> dengan serangan <i>RA flood</i>
Windows Server 2012	Normal	20%	Normal	20%	Tidak terganggu dengan serangan <i>RA flood</i>
Windows Server 2016	Cukup stagnan Menyentuh 100%	60%	Cukup stagnan Menyentuh 100%	60%	Terganggu dengan serangan <i>RA flood</i>
Ubuntu 14.10	Menyentuh 50% cenderung normal	28.9%	Fluktuatif Antara 70%-90%	29.2%	Cukup mengganggu utilisasi CPU
Ubuntu 16.04	Menyentuh 97% hampir stagnan	37.2%	Hampir 100% dan hampir stagnan	40%	Terganggu dengan serangan <i>RA flood</i>
Ubuntu 17.04	Fluktuatif cenderung normal	50%	100% dan hampir stagnan	51%	Terganggu dengan serangan <i>RA flood</i>
MacOS El Capitan	Normal berkisar 20-25%	60%	Normal berkisar 20-20%	60%	Tidak terganggu dengan serangan <i>RA flood</i>
MacOS Sierra	Normal <20%	30%	Normal <20%	30%	Tidak terganggu dengan serangan <i>RA flood</i>
Android versi 4	-	-	-	-	Secara <i>default</i> tidak men- <i>disable</i> IPv6
Android versi 5	-	-	-	-	Secara <i>default</i> tidak men- <i>disable</i> IPv6
Android versi 6	Normal	60%	Normal	60%	Tidak terganggu dengan serangan <i>RA flood</i>
Android versi 7	Utilisasi CPU berkisar antara 70%-80%	60%	Cukup stagnan >80% sempat menyentuh 98%	60%	Terganggu dengan serangan <i>RA flood</i>

Keterangan:

- 1) *Utilisasi* normal berarti *utilisasi* fluktuatif naik turun tapi cenderung sama dengan pemakaian normal sebelum dibanjiri paket
- 2) *Utilisasi* CPU terganggu berarti *utilisasi* CPU stagnan >70.

Secara keseluruhan dua Platform Sistem Operasi yang diuji yang sudah menutup *bug* ini adalah *Windows 10* dan *MacOS Sierra*. Terlihat pada Gambar 8.a SO *MacOS Sierra* sudah menggunakan mekanisme *autoconf secured*, untuk membatasi jumlah *IPv6* yang di-generate dari hasil *flood*. Sedangkan pada SO *Windows 10* mekanisme pengamanannya dengan membatasi jumlah *IPv6* yang di-generate (maksimal 100), selebihnya berupa *Temporary IPv6 Address* seperti yang terlihat pada Gambar 8.b.



Gambar 8. *IPv6 Address* yang di-generate karena adanya paket *IPv6 RA flood*, (a). Pada Sistem Operasi *MacOS Sierra*; (b) Pada Sistem Operasi *Windows 10*.

Pada *Windows Server 2012* serangan *IPv6 RA flood* tidak terlalu mengganggu *Utilisasi CPU* tapi pada SO *Windows Server 2016* *Utilisasi CPU* sangat terpengaruh dengan serangan *RA flood*. Demikian juga pada platform SO *Android*, *Android* versi 6 *response* lebih baik serangan *IPv6 RA flood* dibandingkan *Android* versi 7.

3.4. Mekanisme Mengatasi Serangan *IPv6 RA flood*

Berdasarkan *literature* yang ada beberapa mekanisme yang bisa digunakan untuk mengatasi serangan *IPv6 Router Advertisement*, yaitu antara lain:

1. Lakukan *disable IPv6* jika memang tidak diperlukan, akan tetapi jika di jaringan yang menggunakan *IPv6* maka tentu saja pilihan ini tidak bisa kita lakukan.
2. Dengan konfigurasi manual pada masing-masing platform perangkat.
 - a) Metode menonaktifkan *Router Discovery* dapat digunakan untuk mencegah *host* dari *RA* untuk meng-generate *IPv6* untuk diri mereka sendiri [5]. Dengan cara ini mencegah sistem menggunakan *Stateless Autoconfiguration* (yang secara otomatis mengatur alamat *IPv6*). Jadi sistem menggunakan *IPv6* statis. Cara ini sesuai untuk *server* tapi tidak memungkinkan untuk *client* jika harus mengatur sendiri alamat *IPv6*.
 - b) Menggunakan *firewall* di masing-masing perangkat untuk memblokir *RA* palsu, akan tetapi tetap mengizinkan *RA* dari *gateway* yang sebenarnya (*Access Control List*). Akan tetapi tetap saja ada resiko di-defeated penyerang berpura-pura sebagai *Gateway*.

3. Menggunakan *Smart Switch* yang memiliki fitur *RA Guard* [14].

Dalam penelitian ini dicoba dengan melakukan pilihan ke 2 dengan konfigurasi pada masing-masing *platform*. Pada contoh yang diuji dengan cara menonaktifkan *Router Discovery* pada Windows 7 dengan menjalankan *command* berikut di terminal:

```
netsh interface ipv6 set interface "Local Area Connection"  
routerdiscovery=disabled
```

Kemudian setelah diuji dengan *flooding RA*, *utilisasi CPU* nya berjalan normal pada saat dibanjiri paket 10.000 *RA IPv6*.

Demikian juga pada Sistem Operasi Ubuntu 14.10 untuk men-*disable Router Discovery* dengan perintah berikut:

```
net.ipv6.conf.all.accept_ra = 1 → dirubah jadi 0 (disable)
```

Pada saat dilakukan pengiriman paket *flooding*, *Utilisasi CPU* tetap berjalan normal. Akan tetapi solusi ini sangat menyulitkan bagi pengguna awam, terutama untuk meng-*konfigurasi firewall* di setiap *client* dengan platform yang berbeda-beda. Perintah *firewall* nya di *platform* dengan versi berbeda sangat beragam. Contoh pada SO Ubuntu 14.10, 16.04 dan 17.04 perintahnya tidak sama. *Firewall* yang diuji pada SO Ubuntu 14.10 pada saat diuji pada versi 16.04 dan 17.04 tidak berjalan sesuai yang diharapkan. Untuk SO Android tentu saja untuk melakukan konfigurasi *firewall* pada sistem yang belum di *rooting* tidak bisa dilakukan, sehingga untuk men-*disable* paket *Router Discovery* dan *Router Advertisement* hanya bisa dilakukan oleh pengguna mahir dengan segala resikonya. Sehingga sangat diperlukan *update patching* dari masing-masing platform OS sehingga tidak menyulitkan penggunanya.

4. SIMPULAN

Dari pengujian yang dilakukan maka dapat ditarik beberapa bahwa platform Sistem Operasi *MacOS* lebih siap untuk penggunaan *IPv6* terbukti dari hasil pengujian yang dilakukan Sistem tidak terganggu dengan serangan paket *Routing Advertisement IPv6 flood*. Sedangkan 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*. Untuk Platform Linux Ubuntu, hanya Platform Linux 14.10 yang tidak terlalu terpengaruh dengan serangan paket *IPv6 flood*. Khusus untuk platform Android secara umum tidak terlampau siap migrasi ke *IPv6* dilihat dari dukungan *IPv6* secara *default*, kecuali untuk versi 6 dan 7. Bahkan pada versi 7 yang terbaru bisa dilihat cukup terganggu dengan serangan *IPv6 RA flood* meskipun tidak membuat sistem menjadi *crash*.

Untuk mengatasi serangan *IPv6 RA flood* sebaiknya di masing-masing *platform IPv6* di-*disable* di jaringan *IPv4* (jika tidak dibutuhkan). Akan tetapi jika dibutuhkan sebaiknya untuk menonaktifkan fitur *Router Advertisery/Advertisement* atau membatasinya dengan *Acces Control List* di *firewall*. Sedangkan untuk penggunaan *IPv6* di instansi harus menggunakan *smart switch* yang mendukung fitur *RA Guard* untuk melindungi pengguna jaringan di instansi tersebut.

5. REFERENSI

- [1] Huston, G. 2017. *IPv4 Address Report*. <https://ipv4.potaroo.net/>, diakses 13 September 2017.
- [2] Deering & Hinden, Network Working Group. 1998. *RFC 2460 Internet Protocol Version 6 (IPv6) Specification*. <https://www.ietf.org/rfc/rfc2460.txt>, diakses 20 Mei 2017.
- [3] Pilihanto, A., Wanner, R. 2012. *A Complete Guide on IPv6 Attack and Defense*. SANS Institute InfoSec Reading Room.
- [4] Vikram, P. S., Mitesh, T. 2014. A Comprehensive Study on Various Security Attacks against IPv6. *International Journal Of Engineering Development and Research* – IJEDR Vol 1(3): 198-201.
- [5] Bowne, S., Prince, M. 2013. *Evil DoS Attacks and Strong Defenses*. <https://www.defcon.org/images/defcon-21/dc-21-presentations/Bowne-Prince/DEFCON-21-Bowne-Prince-Evil-DoS-Attacks-and-Strong-Defenses.pdf>, diakses 23 Mei 2017.
- [6] Alangar, V., Swaminathan, A. 2013. IPv6 Security: Issue of Anonymity. *International Journal of Engineering and Computer Science*. Vol 2(8): 2486-2493.
- [7] Liu, W., Duan, H. X., Lin, T., Li, X., & Wu, J. P. 2009. H6Proxy: ICMPv6 Weakness Analysis and Implementation of IPv6 Attacking Test Proxy. Proceedings of a meeting *Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing*. Brisbane, Australia, July 7-9 2009.
- [8] Barker, K. 2013. The Security Implications of IPv6. *Journal Network Security*, Vol 2013 (6): 5-9.
- [9] Frankel, S., Graveman, R., Pearce, J., & Rooks, M. 2010. *Guidelines for the Secure Deployment of IPv6: Special Publication 800-119*. National Institute of Standards and Technology. Gaithersburg, MD 20899-89330.
- [10] Kaur, R., & Sharma, S. 2014. The Security Issues of IPv6 Routing Protocol - A Study. *International Journal of Computer Applications & Information Technology*. Vol 5(2):53-60.
- [11] Grob, M., & Hoffmann, E. 2012, May. *What is wrong with the IPv6 RA protocol? Some analysis and proposed solutions*. IPv6-Kongress, Frankfurt, German. <http://www.fehcom.de/ipnet/ipv6/ipv6-ra.pdf>, diakses 13 September 2017
- [12] Shakeel, A., & Heriyanto, T. 2011. *BackTrack 4: Assuring Security by Penetration Testing*. Packt Publishing Ltd, Birmingham, B27 6PA, UK.
- [13] 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. Gaithersburg, MD.
- [14] Chown, T., & Venaas, S. 2011. *Rogue IPv6 Router Advertisement Problem Statement*. RFC 6104, February 2011. <https://tools.ietf.org/html/rfc6104>, diakses 12 September 2017.



Sertifikat

No. 9658/UN37.1.4/SR/2017

Diberikan kepada

YESI NOVARIA KUNANG

Atas Partisipasinya sebagai

Pemakalah

pada Seminar Nasional Ilmu Komputer (SNIK) 2017 dengan tema
"Cyber War and Data Security"

yang diselenggarakan oleh Jurusan Ilmu Komputer FMIPA
Universitas Negeri Semarang pada tanggal 10 Oktober 2017 di Hotel Grasia Semarang

Semarang, 10 Oktober 2017

Dekan FMIPA UNNES



Prof. Dr. Zaenuri, S.E., M.Si., Akt
NIP 196412231988031001

Ketua SNIK 2017



Anggyi Trisnawan Putra, S.Si., M.Si
NIP 198707062014041003

SURAT TUGAS

Nomor : 0616 /ST/Univ-BD/X/2017

Rektor Universitas Bina Darma menugaskan kepada Saudara:

No.	Nama	Jabatan	Materi
1.	Ilman Zuhri Yadi, M.M., M.Kom., Yesi Novaria Kunang, S.T., M.Kom., dan Suzi Oktavia Kunang, S.T., M.Kom.	Dosen Fakultas Ilmu Komputer Universitas Bina Darma	Analisis Celah Keamanan Serangan <i>Router Advertisement Ipv6 Flood</i> di Jaringan

sebagai Peserta dan Pemakalah dalam Seminar Nasional Ilmu Komputer (SNIK) 2017, yang dilaksanakan di Universitas Negeri Semarang pada tanggal 9 sampai dengan tanggal 11 Oktober 2017.

Setelah acara, yang bersangkutan wajib memberikan presentasi (laporan) hasil acara tersebut.

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

Dikeluarkan di : Palembang
Pada tanggal : 7 Oktober 2017

Kepala Biro Administrasi,


Universitas Bina Darma

Muhammad Nasir, M.M., M.Kom.

Tembusan disampaikan kepada yth:

1. Rektor Universitas Bina Darma (sebagai laporoan);
2. Yang bersangkutan untuk dilaksanakan;
3. Arsip.