ANALISA SERANGAN *REMOTE EXPLOIT* MELALUI *JAVA APPLET ATTACK METHOD* TERHADAP SISTEM OPERASI *WINDOWS* 8

Makalah

Program Studi Informatika
Fakultas Komunikasi dan Informatika

Diajukan oleh :
Bryan Pingkan Ramadhan
Gunawan Ariyanto, Ph.D.

PROGRAM STUDI INFORMATIKA
FAKULTAS KOMUNIKASI DAN INFORMATIKA
UNIBERSITAS MUHAMMADIYAH SURAKARTA
JULI 2015

HALAMAN PENGESAHAN

Publikasi ilmiah dengan judul :

ANALISA SERANGAN *REMOTE EXPLOIT* MELALUI *JAVA APPLET ATTACK METHOD* TERHADAP SISTEM OPERASI *WINDOWS* 8

Dipersiapkan dan disusun oleh :

BRYAN PINGKAN RAMADHAN

NIM : L200110143

Telah disetujui pada :

Hari : Sabtu 9 Juli 2015

Tanggal :

Pembimbing I

Gunawan Ariyanto, Ph.D.

NIK : 968

Publikasi ini telah diterima sebagai salah satu persyaratan

untuk memperoleh gelar sarjana

Tanggal 11 Juli 2015

Mengetahui,

Ketua Program Studi Informatika

Dr. Heru Supriyono, M.Eng.

NIK : 970

UNIVERSITAS MUHAMMADIYAH SURAKARTA
FAKULTAS KOMUNIKASI DAN INFORMATIKA
PROGRAM STUDI INFORMATIKA
Jl. A Yani Tromol Pos 1 Pabelan Kartasura Telp. (0271)717417, 719483 Fax (0271) 714448
Surakarta 57102 Indonesia. Web: http://informatika.ums.ac.id. Email: informatika@fki.ums.ac.id

SURAT KETERANGAN LULUS PLAGIASI

/A.3-II.3/INF-FKI/VII/2015

Assalamu'alaikum Wr. Wb

Biro Skripsi Program Studi Informatika menerangkan bahwa :

Nama	:	BRYAN PINGKAN RAMADHAN
NIM	:	L200110143
Judul	:	ANALISA SERANGAN REMOTE EXPLOIT MELALUI JAVA APPLET ATTACK METHOD TERHADAP SISTEM OPERASI WINDOWS 8
Program Studi	:	Informatika
Status	:	**Lulus**

Adalah benar-benar sudah lulus pengecekan plagiasi dari Naskah Publikasi Skripsi, dengan menggunakan aplikasi Turnitin.

Demikian surat keterangan ini dibuat agar dipergunakan sebagaimana mestinya.

Wassalamu'alaikum Wr. Wb

Surakarta, 10 Juli 2015

Biro Skripsi
Informatika

Adjie Sapoetra, S.Kom

Turnitin Originality Report

ANALISA SERANGAN REMOTE EXPLOIT MELALUI JAVA APPLET ATTACK METHOD TERHADAP SISTEM OPERASI WINDOWS 8 by Bryan Pingkan Ramadhan

From publikasi september 2015 (publikasi)

Processed on 09-Jul-2015 16:48 WIB
ID: 554819035
Word Count: 1985

Similarity Index	Similarity by Source	
19%	Internet Sources:	8%
	Publications:	2%
	Student Papers:	18%

sources:

1 4% match (student papers from 07-Jul-2015)
Class: publikasi
Assignment:
Paper ID: 554455546

2 2% match (student papers from 07-Jul-2015)
Class: publikasi
Assignment:
Paper ID: 554421047

3 2% match (student papers from 16-Mar-2015)
Class: publikasi
Assignment:
Paper ID: 516773507

4 2% match (student papers from 06-Jul-2015)
Class: publikasi
Assignment:
Paper ID: 554231941

5 1% match (student papers from 01-Dec-2014)
Class: publikasi
Assignment:
Paper ID: 484107756

6 1% match (student papers from 09-Dec-2014)
Submitted to Strayer University on 2014-12-09

7 1% match (Internet from 30-Apr-2014)
http://journeyintoir.blogspot.co.uk/

1% match (student papers from 21-Feb-2015)

ANALISA SERANGAN *REMOTE EXPLOIT* MELALUI *JAVA APPLET ATTACK METHOD* TERHADAP SISTEM OPERASI *WINDOWS* 8

Bryan Pingkan Ramadhan, Gunawan Ariyanto
Program Studi Informatika, Fakultas Komunikasi dan Informatika
Universitas Muhammadiyah Surakarta
Email : ray0yan@gmail.com

ABSTRAKSI

Dalam 5 tahun terakhir jenis serangan *client-side attacks* jumlahnya meningkat secara dramatis. Penyerang mengalihkan fokus mereka ke sisi klien yang memiliki celah lebih besar karena klien mempunyai perlindungan terhadap sistem yang lebih sederhana daripada *server*. Eksploitasi dengan menggunakan *malicous Java* yang memanfaatkan kerentanan pada *Java* adalah yang paling sering terdeteksi oleh *Trustwave Secure Web Gateway anti-malware technology* dengan persentase sebesar 78% dan sebagian besar penjahat *cyber* mengandalkan *Java applet* sebagai metode untuk mengirimkan *malware* maupun *payload*. *Java applet attack method* adalah salah satu teknik serangan yang memanfaatkan kerentananan pada *Java* untuk mengeksploitasi sistem *user* menggunakan *Java applet* dan dapat menyerang ke berbagai sistem operasi termasuk *Windows* 8 yang merupakan sistem operasi keluaran terbaru dari *Microsoft*. Skripsi ini bertujuan untuk menganalisa serangan *remote exploit* melalui *Java applet attack method* terhadap sistem operasi *Windows* 8 yang terproteksi *firewall*. Penelitian yang dilakukan menggunakan metode studi pustaka dan melakukan eksperimen yang melalui beberapa tahapan diantaranya studi kepustakaan, pengolahan data, pengujian serangan, analisa serangan, optimalisasi *firewall*, pengujian *firewall* dan penulisan laporan. Dengan menganalisa serangan tersebut akan diketahui perilaku dan karakterisiknya yaitu pada Java exploit dan Java payload yang ada didalam *Java applet*. *Java exploit* berfungsi untuk melewati *Java Virtual Machine* (JVM) *sandbox* dan menonaktifkan *SecurityManager* dan *payload Java meterpreter* berfungsi untuk mengelabuhi *firewall* dan sebagai media interaksi antara penyerang dengan sistem klien. Kemudian dibuat *rule firewall* pada *Comodo Firewall* yang mampu mencegah *payload* untuk melakukan *reverse connection* dan mencegah *payload* melakukan *staging*.

Kata Kunci : *Remote exploit, Java applet attack method, Windows 8, firewall*

PENDAHULUAN

System Administration Networking Security (SANS) *Institute* menyatakan bahwa dalam 5 tahun terakhir jenis serangan *client-side attacks* jumlahnya meningkat secara dramatis. Peningkatan serangan terhadap klien terjadi karena saat ini serangan terhadap *server* semakin sulit dilakukan sehingga penyerang mengalihkan fokus mereka ke sisi klien yang memiliki celah lebih besar karena klien mempunyai perlindungan terhadap sistem yang lebih sederhana daripada *server*. Menurut *Global Security Report* yang dirilis oleh perusahaan riset keamanan *Trustwave* pada tahun 2014, eksploitasi dengan menggunakan *malicous Java* yang memanfaatkan kerentanan pada *Java* adalah yang paling sering terdeteksi oleh *Trustwave Secure Web Gateway anti-malware technology dengan persentase* sebesar 78% dan sebagian besar penjahat *cyber* mengandalkan *Java applet* sebagai metode untuk mengirimkan *malware* maupun *payload*.

Java applet attack method adalah salah satu teknik serangan yang memanfaatkan kerentananan pada *Java* untuk mengeksplotasi sistem *user* dan dapat menyerang ke berbagai sistem operasi termasuk *Windows* 8 yang merupakan sistem operasi keluaran terbaru dari *Microsoft*. Teknik ini menggunakan *malicious Java applet* yang diinjeksikan kedalam *website*. Saat user mengakses *website* tersebut dan menjalankan *Java applet* maka tanpa disadari oleh *user* penyerang telah mendapatkan akses ke sistem user secara *remote*. Menyikapi permasalahan tersebut, peneliti mencoba untuk menganalisa serangan tersebut dan sehingga akan diketahui perilaku dan karakterisiknya yang dapat digunakan untuk melakukan antisipasi sehingga sistem dapat bertahan dari serangan tersebut.

TINJAUAN PUSTAKA

Pangaria, Shrivastava dan Soni (2012) dalam penelitiannya melakukan *penetration testing* terhadap sistem operasi *Windows* 8 menggunakan *Metasploit* dan *PEScambler*. Hasil dari penelitian tersebut adalah berhasil mengeksploitasi sistem operasi *Windows* 8 dengan menggunakan *expolit ms08_067_netapi* dan *Meterpreter payload*, serta menggunakan *PEScambler* agar *payload* tidak terdeteksi oleh *anti virus* atau *anti malware*.

Agarwal dan vishnoi (2013) dalam penelitianya menyatakan bahwa *Windows* 8 lebih aman dari versi sebelumnya. Didalamnya dibangun sistem perlindungan *anti malware* sehingga tidak perlu khawatir jika anti *virus* tidak diinstal. Tujuan utama penelitian tersebut adalah melakukan penetrasi terhadap sistem operasi *Windows* 8 menggunakan *exploit* dan *payload* pada *Metasploit Framework* yang memberikan

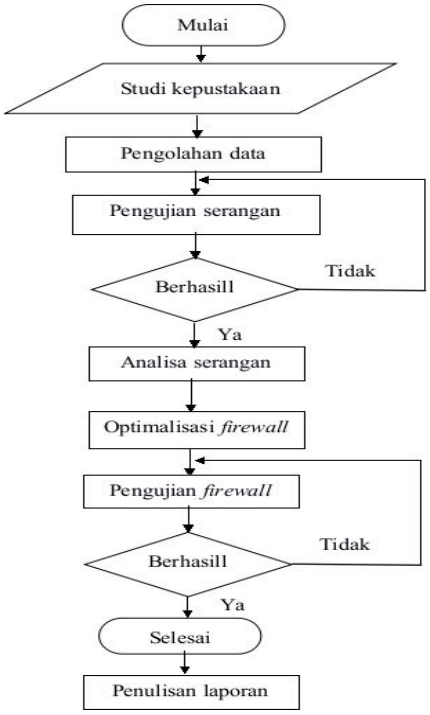
reverse connection ke sistem target. Untuk mengeksekusi *Metasploit payload* agar tidak terdeteksi oleh anti *virus* digunakan *tool* yaitu *Sryinge*.

Byalla, Reddy dan Sudeep (2014), dalam penelitianya membahas tentang keamanan pada *Java applet*. *Untrusted applet* akan dijalankan pada lingkungan yang aman atau disebut *sandbox* yang akan membatasi akses *applet* terhadap komputer *user* namun baru-baru ini terdapat lubang keamanan yang memungkinkan *applet* untuk melakukan *bypass* pada *Java security sandbox*, memberikan ijin pada *applet* untuk mengeksekusi *arbitrary code.*

Špiláková, Jašek dan Schauer (2014), menyatakan bahwa *Java applet* memiliki masalah keamanan pada *Java security* model yang dapat disalahgunakan oleh *hacker*, oleh karena itu dilakukan penelitian dengan membandingkan beberapa bahasa pemrograman seperti *JavaScript, ActiveX* dan *Dart*, perbandingan tersebut bertujuan untuk memilih alternatif terbaik sebagai pengganti dari *Java applet* dalam pengembangan ISES (*Internet School Experimental system*).

METODE

Metode penelitian dapat dilihat pada *flowchart* Gambar 1.



Gambar 1. *Flowchart* penelitian

1. **Studi Kepustakaan**

   Pada tahap ini peneliti mengumpulkan data-data yang diperlukan untuk melakukan penelitian dengan mempelajari literatur, artikel, buku, journal, karya ilmiah, ataupun kepustakaan lainnya serta mengutip pendapat-pendapat para ahli dari buku-buku bacaan yang ada kaitannya dengan materi pembahasan penelitian ini.

2. **Pengolahan Data**

   Pada tahap ini peneliti mengolah data yang sudah didapatkan dari proses pengumpulan data.

3. **Pengujian Serangan**

   Pada tahap ini penulis melakukan ujicoba serangan *remote exploit* melalui *Java applet attack method*

terhadap sistem operasi *Windows* 8. Pengujian serangan dilakukan menggunakan aplikasi *Metasploit Framework* dengan melalui 4 proses yaitu, fase persiapan, fase eksploitasi, fase *gaining access* dan fase *maintaining access*.

4. **Analisa Serangan**

   Pada tahap ini dilakukan analisa terhadap serangan tersebut dengan menggunakan teknik analisa *runtime* yaitu mencoba untuk menemukan proses-proses yang terjadi pada sistem klien saat serangan dilakukan terhadap sistem klien. Dengan memperhatikan proses-proses yang terjadi pada sistem yang mendapat serangan akan diketahui perilaku dari serangan tersebut. Untuk dapat melihat proses tersebut dibutuhkan beberapa aplikasi bantuan karena kebanyakan proses sistem berjalan secara *background* dan tidak kasat mata. Oleh karena itu diperlukan aplikasi bantuan yaitu *Volatility, CaptureBat* dan *Wireshark* serta dilakukan *decompiling* pada *malicious Java applet* tersebut.

5. **Optimalisasi *Firewall***

   Pada tahap ini dilakukan optimalisasi pada *firewall* dengan membuat rule firewall yang dapat mengantisipasi serangan tersebut.

6. **Pengujian *Firewall***

   Setelah dilakukan optimalisasi terhadap *firewall* pada sistem klien , perlu dilakukan pengujian untuk mengetahui apakah optimalisasi terhadap *firewall* sudah berhasil atau belum. Langkah pengujian dilakukan dengan melakukan serangan kembali pada sistem klien yang setelah dilakukan optimalisasi pada *firewall*.

7. **Penulisan Laporan**

   Pada tahap terakhir ini, peneliti menyusun laporan dari hasi penelitian dengan data-data yang sudah dilakukan dengan menarik sebuah kesimpulan dari semua kegiatan penelitian.

HASIL DAN PEMBAHASAN

Hasil dari penelitian ini adalah diketahuinya perilaku dan karakteristik dari serangan *remote exploit* melalui *Java applet attack method* terhadap *Windows* 8 yang terproteksi *firewall*. Karakteristik dari serangan tersebut terletak pada *Java exploit* dan *Java payload* yang ada didalam *Java applet. Java exploit* berfungsi untuk melewati *Java Virtual Machine* (JVM) *sandbox* dan menonaktifkan *SecurityManager* dan *payload Java meterpreter* berfungsi untuk mengelabuhi *firewall* dan sebagai media interaksi antara penyerang dengan sistem klien. Setelah mengetahui perilaku dari serangan tersebut kemudian dilakukan optimalisasi pada

firewall klien sehingga dapat mencegah serangan tersebut.

Berdasarkan perilaku dan karakteristik dari serangan tersebut kemudian dibuat *rule firewall* yang mampu mendeteksi dan mencegah serangan tersebut untuk mengoptimalkan *firewall* pada sistem klien yang sebelumnya tidak dapat mendeteksi maupun mengantisipasi serangan tersebut. Dari perilaku serangan tersebut telah diketahui bahwa untuk mendapatkan akses ke sistem klien, penyerang menggunakan *payload* yang melakukan *reverse connection* ke *listener* penyerang pada *port* 4444 dan kemudian menjalankan *Java meterpreter* yang juga menggunakan *port* 4444 untuk terhubung dengan *Metasploit framework* milik penyerang. *Payload* tersebut di *handle* oleh proses Java.exe, oleh karena itu perlu dibuat *rule firewall* yang mampu mencegah Java.exe untuk melakukan *reverse connection* ke *listerner* penyerang pada *port* 4444 sehingga saat Java.exe mengeksekusi *payload*, *payload* tersebut gagal melakukan *staging* sehingga komponen-komponen dari *Java meterpreter* tidak dapat terkirim ke sistem klien dan *meterpreter session* milik penyerang tidak dapat terbuka. Hal tersebut dapat di implementasikan dengan membuat *rule fiewall* pada *Comodo Firewall*. Dengan *rule firewall* tersebut *Comodo Firewall* akan memblokir *reverse connection* yang dilakukan oleh *payload* tersebut.

KESIMPULAN

Setelah melakukan serangkaian penelitian, kesimpulan yang dapat diambil berdasarkan hasil penelitian ini adalah sebagai berikut :

1. Setelah dilakukan ujicoba dan analisa pada serangan tersebut, diketahui *Java applet* dapat disalahgunakan untuk melakukan eksploitasi secara *remote* terhadap sistem klien yang menggunakan sistem operasi *Windows* 8, dengan memanfaatkan celah keamanan pada *Java sandbox* sebuah *applet* dapat berjalan diluar lingkungan *sandbox* sehingga *applet* dapat melakukan operasi-operasi berbahaya yang dimanfaatkan penyerang untuk mengusai sistem klien.
2. *Reverse TCP connection* dapat melewati (*bypass*) *firewall* yang memfilter dan memblokir semua koneksi yang masuk pada komputer klien, karena dalam *reverse connection* klien yang akan menghubungi atau melakukan koneksi ke penyerang bukan penyerang yang menerobos masuk ke sistem klien.
3. *Metasploit framework* menyediakan berbagai macam *module exploit* yang dapat digunakan untuk mengekspoitasi celah keamanan pada sistem komputer

salah satunya adalah *module exploit* java_jre17_provider_skeleton, dengan *module exploit* tersebut dapat dibuat *malicious Java applet* secara otomatis, yang didalamnya terdapat *java exploit* dan *payload*.

4. Melakukan analisa *runtime* terhadap sistem yang telah mendapat serangan dapat digunakan sebagai metode untuk mempelajari perilaku dan karakteristik dari sebuah serangan yang dilakukan oleh penyerang.
5. *Comodo Firewall* memiliki beberapa fitur yang tidak dimiliki *Windows firewall* yaitu dapat memantau atau *monitoring* terhadap koneksi yang masuk maupun keluar, dapat memunculkan peringatan saat terjadi intrusi dan dapat menyimpan *log* maupun menampilkanya, dengan fitur tersebut dapat menutupi keterbatasan dari *Windows firewall. Rule firewall* yang dibuat berdasarkan perilaku dan karakteristik serangan tersebut mampu mencegah *payload* untuk melakukan *reverse connection* dan mencegah *payload* melakukan *staging.*

SARAN

Salah satu yang menjadi kendala dalam jaringan komputer adalah dalam bidang keamanannya. Sesempurna apapun sistem keamanan yang dibangun oleh *user* tentunya masih memiliki celah untuk diserang. Oleh karena itu, *user* yang dalam jaringan komputer berposisi sebagai klien harus terus meningkatkan sistem keamananya mengingat saat ini jenis serangan yang menjadikan klien target (*client-side attacks*) sedang menjadi trend. Dalam keamanan komputer *user* perlu memahami dan mengetahui bagaimana penyerang melakukan serangan terhadap target, dengan melakukan analisa terhadap serangan yang dilakukan oleh penyerang akan diketahui perilaku dan karakteristiknya sehingga *user* bisa menyiapkan lebih awal sebuah sistem keamanan yang dapat menangkal serangan tersebut. Konfigurasi *firewall* dapat dilakukan sebagai upaya pencegahan terhadap suatu serangan. Semakin ketat kebijakan atau *rule* yang dibuat dan diterapkan maka akan semakin sulit bagi penyerang untuk mengusai sistem *user*.

DAFTAR PUSTAKA

IBISA 2011, Keamanan sistem informasi, Penerbitt ANDI, Yogyakarta.

Perdhana, R Mada 2011, Harmless hacking malware analysis dan vulnerability development, Graha Ilmu, Yogyakarta.

Patel, Rahul Singh 2013, Kali linux social engineering, Packt Publishing, Birmingham.

Schildt, Herbert 2012, Java a beginner's guide, 5th Edn, McGraw-Hill, New York.

Weidman, Georgia 2014, Penetration testing a hands-on introduction to hacking, No Starch Press, San Francisco.

Argawal, M & Singh, A 2013, Metasploit penetration testing cookbook, 2nd Edn, Packt Publishing, Birmingham.

Kennedy, D, O'Gorman, J, Kearns, D, Aharoni, M 2011, Metasploit the penetration tester's guide, No Starch Press, San Francisco.

Shimonski, R & Oriyano, SP 2012, Client-side attacks and defense, Syngress, United State of America.

Tanenbaum, A & Wetherall, D 1994, Computer networks, 5th Edn, Pearson Education, United State of America.

Ligh, M, Case, A, Levy, J & Walters AA 2014, The art of memory forensics : detecting malware and threats in windows, linux, and mac memory, John Wiley & Sons Inc, Indianapolis.

Sikorski, M & Honig, A 2012, Practical malware analysis, No Starch Press, San Francisco.

Ligh, M, Adair, S, Hartstein, B & Richard, M 2011, Malware analyst's cookbook and dvd: tools and techniques for fighting malicious code, Wiley Publishing Inc, Indianapolis

Pangaria, M, Shrivastava, V & Soni, P 2012, 'Compromising windows 8 with metasploit's exploit', IOSR Journal of Computer Engineering, vol. 5, no.6, hh. 1-4.

Agarwal, M & vishnoi, L 2013, 'Penetrating Windows 8 with syringe utility', IOSR Journal of Computer Engineering, vol. 13, no. 4, hh. 39-43.

Špiláková, P, Jašek, R & Schauer, F 2014, ' Security risks of java applets in remote experimentation and available alternatives ' , paper presented to the international conference on applied mathematics computational science & engineering, Varna, Bulgaria, 13-15 September.

BIODATA PENULIS

Nama	: Bryan Pingkan Ramadhan
NIM	: L200110143
Tempat lahir	: Kab. Boyolali
Tanggal Lahir	: 25 Pebruari 1993
Jenis Kelamin	: Laki-laki
Agama	: Islam
Pendidikan	: S1
Jurusan/Fakultas	: Informatika / Komunikasi dan Infromatika
Perguruan Tinggi	: Universitas Muhammadiyah Surakarta
Alamat	: Bangunharjo Rt. 5/III, Pulisen, Boyoali 57316
No. Hp	: 0888291415
Email	: ray0yan@gmail.com