DETEKSI DAN PENCEGAHAN SERANGAN REMOTE CODE EXECUTION TERHADAP WING FTP WEB SERVER MENGGUNAKAN SNORT

Makalah

Program Studi Informatika

Fakultas Komunikasi dan Informatika

Diajukan Oleh :

Muhammad Triwibowo

Helman Muhammad, S.T,M.T.

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS KOMUNIKASI DAN INFORMATIKA

UNIVERSITAS MUHAMMADIYAH SURAKARTA

JULI 2015

HALAMAN PENGESAHAN

Publikasi ilmiah dengan judul :

DETEKSI DAN PENCEGAHAN SERANGAN REMOTE CODE EXECUTION TERHADAP WING FTP WEB SERVER MENGGUNAKAN SNORT

Yang dipersiapkan dan disusun oleh :

Muhammad Triwibowo

L200110114

Telah disetujui pada :

Hari : Rabu

Tanggal : 1 Juli 2015

Pembimbing

Helman Muhammad, S.T,M.T.

NIK : DTT 1397

Publikasi ilmiah ini telah diterima sebagai salah satu persyaratan

Untuk memperoleh gelar sarjana

Tanggal :

Mengetahui,

Ketua Program Studi

Informatika

Dr. Heru Supriyono, M.sc

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	:	MUHAMMAD TRIWIBOWO
NIM	:	L200110114
Judul	:	DETEKSI DAN PENCEGAHAN SERANGAN REMOTE CODE EXECUTION TERHADAP WING FTP WEB SERVER MENGGUNAKAN SNORT
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, 7 Juli 2015

Biro Skripsi
Informatika

Adjie Sapoetra, S.Kom

Turnitin Originality Report

ETEKSI DAN PENCEGAHAN
ERANGAN REMOTE CODE EXECUTION
ERHADAP WING FTP WEB SERVER
ENGGUNAKAN SNORT by Muhammad
Triwibowo

From publikasi september 2015 (publikasi)

Processed on 07-Jul-2015 13:41 WIB
ID: 554455752
Word Count: 2973

Similarity Index	Similarity by Source	
25%	Internet Sources:	15%
	Publications:	1%
	Student Papers:	16%

sources:

1 12% match (student papers from 02-Dec-2014)
Class: publikasi
Assignment:
Paper ID: 484675899

2 2% match (Internet from 14-Jan-2013)
http://blog.binadarma.ac.id/akbar/wp-content/uploads/2010/09/fulltext2.pdf

3 1% match (Internet from 03-Jul-2014)
http://jakinformatika.blogspot.com/2012/07/deteksi-dan-pencegahan-flooding-data.html

4 1% match (Internet from 08-May-2013)
http://www.as-shiddiq.com/laporan-praktikum-snorttools-host-basedh.xhtml

5 1% match (Internet from 18-Feb-2014)
http://www.jaringankomputer.org/firewall-pengertian-fungsi-manfaat-dan-cara-kerja-firewall/

6 1% match (Internet from 07-Sep-2013)
http://jurnalonline.itenas.ac.id/index.php/rekaelkomika/article/view/119

7 1% match (Internet from 05-Jul-2015)
http://jaringankomputer.org/firewall-pengertian-fungsi-manfaat-dan-cara-kerja-firewall/

8 1% match (Internet from 11-Jun-2015)
http://repository.amikom.ac.id/index.php/type/6/Undergraduate%20Thesis

9 1% match (Internet from 11-Jun-2015)
http://eprints.ums.ac.id/view/type/s1/2014.html

10 1% match (Internet from 15-Jun-2014)
http://ilmukomputer.org/wp-content/uploads/2013/02/keamanan-jaringan-komputer.pdf

DETEKSI DAN PENCEGAHAN SERANGAN REMOTE CODE EXECUTION TERHADAP WING FTP WEB SERVER MENGGUNAKAN SNORT

Muhammad Triwibowo, Helman Muhammad

Informatika, Fakultas Komunikasi dan Informatika

Universitas Muhammadiyah Surakarta

E-mail : bowobw02@gmail.com

ABSTRAKSI

Banyak masalah keamanan yang terjadi pada sebuah jaringan yang rentan oleh serangan. Berbagai macam alasan yang terjadi diantaranya dengan merusak, balas dendam, cuman iseng-iseng sebagai unjuk kemampuan. Di internet banyak informasi yang disediakan akan tetapi dibalik kemudahan dalam pengaksesan banyak juga masalah-masalah kejahatan yang mengintai yang ingin berusaha masuk untuk mengambil celah kerentanan dari sistem keamanan jaringan komputer yang digunakan. Akibat dari serangan-serangan yang dilakukan akan terjadi kerusakan pada sistem komputer jaringan tersebut.

Penelitian ini dapat mengidentifikasi cara bagaimana suatu serangan *Remote Code Execution* dapat bekerja terhadap *Wing File Transfer Protokol* (*Wing* FTP *Web Server*), dan kemudian melakukan pendeteksian terhadap serangan menggunakan snort. Deteksi dan pencegahan dapat dilakukan dengan membuat *firewall* aktif untuk mengidentifikasi setiap data yang masuk kedalam *server*, bagaimana data tersebut merupakan serangan *Remote Code Execution* atau bukan.

Hasil dari penelitian ini adalah bagaimana suatu sistem keamanan jaringan yang mampu mendeteksi dan mencegah terjadinya serangan Remote Code Execution terhadap Wing FTP Web Server. Sistem yang dihasilkan dalam penelitian ini melakukan pengujian terhadap sistem dan melihat. Selanjutnya melakukan 2 tahap yaitu dengan melakukan pendeteksian serangan dan melakukan pencegahan serangan.

Kata Kunci : Keamanan Jaringan Komputer, *Remote Code Execution*, *Wing* FTP *Web Server*, *Firewall*, *Snort*

PENDAHULUAN

Berbagai macam serangan dinternet terdapat bahaya besar yang mengintai untuk mencari celah dari sistem keamanan jaringan komputer yang digunakan. Serangan tersebut dapat mengakibatkan kerusakan data dan bahkan kerusakan hardware. Di Indonesia contohnya, untuk setiap harinya terjadi ratusan ribu serangan terhadap keamanan internet, dengan melakukan tindakan yang meretas atau melakukan kejahatan dunia maya, *transmisi* dari satu pihak dengan pihak lainnya. Tindakan tersebut dapat menagkibatkan terjadinya kerusakan komunikasi dengan dua pihak yang berkomunikasi.

Salah bentuk jenis serangan yang banyak terjadi adalah yang dapat dikenal sebagai serangan *Remote Code Execution* (eksekusi perintah dari jauh). *Remote Code Execution* dapat terjadi apabila terdapat suatu celah yang dapat memungkinkan pihak dari luar (penyerang) dapat mengakses suatu *server* melalui perintah yang dikirim dari s*erver* lain. Sangat besar kerugian yang terjadi akibat serangan oleh terjadinya *Remote Code Execution* kemudian itu dibutuhkan ilmu yang berhubungan dengan jaringan komputer untuk dapat bisa melakukan keamanan jaringan dengan baik. Cara dalam melakukan peningkatan keamanan jaringan komputer dengan cara membuat atau merancang keamanan dengan *firewall.*

Penelitian ini bertujuan untuk mewujudkan suatu cara untuk mendeteksi dan mencegah serangan *Remote Code Execution,* yang didasarkan oleh pemanfaatan *software* IDS ialah Snort. Snort adalah *software* yang tergolong mudah digunakan, *user friendly*, serta dapat di-*download* dengan gratis di *web* resminya. Target serangan dipilih Wing FTP *Web Server* karenan masih memiliki celah untuk diserang dengan serangan *Remote Code Execution*, sehingga sangat cocok digunakan dalam penelitian ini.

TINJAUAN PUSTAKA

Riyantika & Lidyawati (2013) dalam tugas akhirnya yang berjudul " Analisis Kinerja Sistem Pengamanan Jaringan dengan Menggunakan Snort IDS dan IP-Tables di Area Laboratorium RDNMP.T."X" dalam penelitian ini dibangun suatu sistem keamanan jaringan dengan menggunakan snort dan *iptables*. Dalam penelitian ini snort digunakan untuk mendeteksi serangan, sedangkan untuk mencegah serangan digunakan iptables.

Jarwanto (2014) dalam tugas akhirnya yang berjudul " Deteksi dan Pencegahan *Buffer Overflow* Terhadap EFM *Web Server* Menggunakan Snort" dalam penelitian ini dibangun suatu sistem pendeteksian dan pencegahan untuk mengamati serangan *buffer overflow* terhadap *efm web server* dan melakukan pencegahan dengan *firewall.*

Lidia Putri (2011) dalam tugas akhirnya yang berjudul "Implementasi *Intrusion Detection System* Menggunakan Snort Jaringan *Wireless* Studi Kasus: SMK Triguna Ciputat" dalam penelitian ini dibangun sistem IDS untuk melakukan pendeteksian pada jaringan *wireless* di SMK Triguna Ciputat dan melakukan pencegahan serangan dengan *iptables*.

Landasan teori yang digunakan dalam tugas akhir ini adalah:

1. Keamanan Jaringan Komputer

   Keamanan jaringan komputer adalah suatu bentuk penanggulangan serangan yang dilakukan oleh attacker untuk masuk kedalam suatu jaringan

komputer melalui lalu lintas jaringan yang tidak sah dari jaringan komputer luar. (Unswagati, 2010)

2. Intruction Detection System (IDS)

   Instruction Detection System (IDS) adalah suatu bentuk sistem yang dapat melakukan pengawasan terhadap kegiatan-kegiatan yang illegal yang terhubung dengan lalu lintas jaringan, maka IDS akan memberi tindakan peringatan kepada administrator jatringan apabila akan terjadi serangan (Shafitri, 2012)

3. Intruction Prevention System

   Instruction Prevention System (IPS) adalah suatu bentuk metode untuk keamanan jaringan yang sangat baik. IPS dapat melakukan pendeteksian sekaligus dapat melakukan pencegahan ketika terjadi serangan. (Jarwanto, 2015)

4. Snort

   Snort adalah sebuah software yang berfungsi untuk mengawasi aktivitas dalam suatu jaringan komputer. Snort menggunakan sistem aturan (*rules system*) untuk melakukan deteksi dan pencatatan (*logging*) terhadap berbagai macam serangan yang terdapat pada jaringan komputer. Dengan membuat berbagai *rule* untuk mendeteksi ciri-ciri khas signature dari berbagai macam serangan, maka snort dapat mendeteksi serangan-serangan tersebut. (Shafitri, 2012)

5. Metasploit framework

   Metasploit framework adalah sebuah *platform* pengembangan untuk membuat *tools* keamanan dan *exploit*. *Metasploit framework* terdiri atas *tools, libraries, modules* dan *user interface*. Fungsi dasar dari *metasploit framework* adalah memunculkan modul yang membiarkan penggunanya mengkonfigurasi modul *exploit* dan mencobanya pada target yang dituju. Apabila *exploit* berhasil, *payload* akan tereksekusi pada sistem target dan bagi pengguna akan disediakan sebuah *sell* untuk berinteraksi dengan *payload*. (Rochim, 2010)

6. Wing FTP Web Server

   Wing FTP *Web Server* adalah aplikasi *server transfer protocol* yang mudah digunakan dan dapat dijalankan pada *windows, linux, Mac OSX* dan solaris. *Wing* FTP *Web Server* memberikan kemudahan kepada *user* dalam cara mereka terhubung ke *server* dan menyediakan antarmuka berbasis *web* untuk mengelola *server* dari mana saja. *User* juga dapat memonitor kinerja server dan sesi *online* pemberitahuan tentang berbagai peristiwa yang terjadi di *server* (Sera, 2015)

7. Remote Code Execution

   Remote Code Execution adalah sebuah celah yang membuat kita terhubung pada sebuah *command* atau terminal sistem operasi. Dengan celah ini kita dapat menggunakan perintah-perintah yang ada pada sistem operasi *server* tersebut. *Remote Code Execution* dapat terjadi karena kesalahan dalam sebuah kode dan tidak adanya *filter* terhadap kode *injeksi* yang berbahaya seperti *wget, curl, cat,* dan lain-lain. (Yantu, 2014)

8. Firewall

   Firewall adalah sebuah sistem atau perangkat yang memberikan otoritas pada sebuah lalu lintas jaringan komputer yang dianggapnya aman untuk melaluinya dan melakukan pencegahan terhadap jaringan yang dianggap tidak aman. Perlindungan *firewall* mutlak diperlukan komputasi perangkat seperti komputer yang

diaktifkan dengan koneksi internet maupun tidak. Meningkatkan keamanan jaringan komputer dengan memberikan informasi rinci tentang pola-pola lalu lintas jaringan. (http://jaringankomputer.org: 2011)

METODE PENELITIAN

Tugas akhir dengan judul "Deteksi Dan Pencegahan Serangan *Remote Code Execution* Terhadap *Wing* FTP *Web Server* Menggunakan Snort" mengamati bagaimana suatu serangan *Remote Code Execution* bekerja terhadap *Wing* FTP *Web Server*, dan kemudian melakukan pendeteksian serangan menggunakan snort. Deteksi dan pencegahan dilakukan dengan membuat *firewall* aktif untuk mengamati lalu lintas jaringan yang masuk kedalam *server*, apakah lalu lintas jaringan tersebut merupakan serangan *Remote Code Execution* atau bukan.

Dalam menyusun tugas akhir ini diperlukan beberapa tahapan agar pembuatan sistem tercapai dengan tujuan yang diinginkan diperlukan beberapa tahapan untuk membuat sistem tersebut. Memulai dengan membuat tugas akhir dengan judul "Deteksi Dan Pencegahan Serangan *Remote Code Execution* Terhadap *Wing* FTP *Web Server* Menggunakan Snort" dengan tujuan mengamati bagaimana suatu serangan *Remote Code Execution* bekerja terhadap *Wing* FTP *Web Server* dan kemudian melakukan deteksi serangan dengan snort dan melakukan pencegahan dengan *firewall*.

1. Pengumpulan data yaitu mengumpulkan data-data yang diperlukan untuk merancang dan membangun sistem dengan menggunakan teknik pengumpulan data yang telah dijelaskan pada sebelumnya dengan mencari dan menggabungkan dari beberapa sumber diantaranya dari buku dan internet.
2. Pengolahan dan analisis data yang dilakukan dengan menggunakan data-data yang diperoleh dari proses pengumpulan data.
3. Perancangan sistem ini merupakan proses yang lebih kompleks adapun langkah-langkah yang dimaksud akan dijelaskan pada subbab berikutnya.
4. Implementasi sistem yaitu melakukan installasi *software* yang dibutuhkan sebelumnya dalam peranacngan sistem.
5. Pengujian sistem dilakukan dengan melakukan serangan *Remote Code Execution* dengan aplikasi *metasploit framework* dan melakukan pendeteksian menggunakan aplikasi *snort*.
6. Pada tahap ini dapat dilihat apakah sistem yang dibuat sudah berjalan dengan baik dan benar, apabila belum berjalan dengan baik lakukan perbaikan sistem kemudian lakukan pengujian kembali.
7. analisi sistem setelah dilakukan pengujian terhadap sistem yang dirancang sebelumnya.
8. Tahapan penyusunan tugas akhir.

PERANCANGAN

Perancangan sistem ini melakukan beberapa proses tahapan-tahapa yaitu:

1. Installasi *Metasploit* pada *client* komputer penyerang.
2. Installasi Wing FTP Web Server pada komputer server.
3. Installasi snort dan melakukan konfigurasi snort untuk menjalankan snort sebagai *Intruction Detection System* (IDS) pada komputer *server*.

4. Installasi *kiwi log viewer* pada komputer server.
5. Pengoperasian *kiwi log viewer* pada komputer server.
6. Konfigurasi *firewall* pada komputer server.
7. Konfigurasi *rule snort* pada komputer server.
8. Pengujian sistem

Setelah melakukan installasi *snort* maka langkah selanjutnya untuk menjalankan *snort* kita terlebih dahulu harus mengkonfigurasi *snort*. Ada bebrapa pengeditan yang kita lakukan sebelum menjalankan snort sebagai *Intruction Detection System* (IDS).

Berikut langkah-langkah pensettingan snort:

a. Menjalankan snort dengan perintah c:\snort\bin\snort –iX –s –l c:\snort\log\ -c c:\snort\etc\snort.conf –v (gantilah X dengan device interface number). Sebelum menjalankan snort tersebut, dibutuhkan bebrapa langkah untuk mengkonfigurasi file snort.conf agar aplikasi snort dapat berjalan dengan baik
b. Agar mudah dalam pengeditan snort.conf maka digunakan notepad++ Berikut ini yang harus dilakukan pengeditan pada file snort.conf yaitu :

Dari :

```
var RULE_PATH ../rules
var SO_RULE_PATH ../so_rules
var PREPROC_RULE_PATH ../preproc_rules
```

Gambar 1. Edit rules 1

Menajdi :

```
var RULE_PATH C:\Snort\rules
var SO_RULE_PATH C:\Snort\so_rules
var PREPROC_RULE_PATH C:\Snort\preproc_rules
```

Gambar 2. Edit rules 2

Dari :

```
dynamicpreprocessor directory /usr/local/lib/snort_dynamicpreprocessor/
```

Gambar 3. Edit rules 3

Menjadi :

```
dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor
```

Gambar 4. Edit rule 4

Dari :

```
dynamicengine /usr/local/lib/snort_dynamicengine/libsf_engine.so
```

Gambar 5. Edit rules 5

Menjadi :

```
dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll
```

Gambar 6. Edit rules 6

Dari :

```
dynamicdetection directory /usr/local/lib/snort_dynamicrules
```

Gambar 7. Edit rules 7

Menjadi

```
# dynamicdetection directory /usr/local/lib/snort_dynamicrules
```

Gambar 8. Edit rules 8

Dari :

```
# output alert_syslog: LOG_AUTH LOG_ALERT
```

Gambar 9. Edit rules 9

Menjadi :

```
output alert_syslog: host=127.0.0.1:514, LOG_AUTH LOG_ALERT
```

Gambar 10. Edit rules 10

c. Setelah selesai melakukan pengeditan, agar mengetahui apakah snort dapat

berjalan dengan baik diperlukan untuk memvertifikasi snort dengan perintah yaitu c:\snort\bin\snort – W.

d. Setelah selesai melakukan vertifikasi snort, langkah selanjutnya menjalankan kembali *command prompt* lalu mengetik perintah:c:\snort\bin\snort –i3 –s –l c:\snort\log\-c c:\snort\etc\snort.conf –v.

Hasil *file-file* ekstraksi dari *rule* Snort yang telah diedit sebelumnya kemudian dapat dipasang dengan cara dipindahkan ke *server* pada direktori c:\snort\rules\local. *Rule* ini dibuat khusus untuk pengujian sistem yang ditambahkan pada *local.rules*. *Rule* yang dibuat untuk pengujian yang direncanakan tersebut adalah sebagai berikut : *alert tcp any any -> any any (msg:"serangan Remote Code Execution";content:"os.execute"; dsize:>1022; classtype: attempted-admin; sid:1;)*

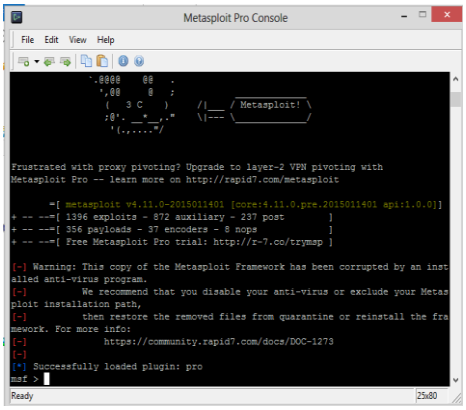
HASIL

Hasil dari penelitian ini adalah sebuah sistem keamanan yang bisa melakukan pendeteksian dan pencegahan apabila terjadi serangan *Remote Code Execution* terhadap Wing FTP Server. Sistem dapat dihasilkan dengan melakukan pengujian dengan sistem yang dibuat yaitu dengan pendeteksian serangan dan pencegahan serangan. Proses pengujian sistem akan dibuat dengan membuat *client* dan *server* sebagai alat percobaan penelitian yang dilakukan dari *client* terhadap *server* sehingga pengamatan trafik data hanya dilakukan pada perangkat jaringan yang dimana aplikasi snort ditempatkan.

Secara teknis, komputer server akan menjalankan aplikasi snort serta layanan yang ada pada snort yaitu *http server* dan *database server*. Komputer *server* dan komputer *client* terhubung dalam satu jaringan dengan memnggunakan *LAN UTP RJ 45*. Selanjutnya melakukan pengujian setelah selesai mengumpulkan data yang digunakan untuk sebagai analisa dalam pengambilan kesimpulan. Pengujian sistem akan dilakukan dengan cara simulasi serangan *Remote Code Execution* terhadap *Wing* FTP *Web Server*. Selanjutnya pengujian ini aplikasi snort akan mendeteksi adanya sebuah serangan yang terjadi pada *server*, sehingga snort akan menampilkan *alert* pada *user*.

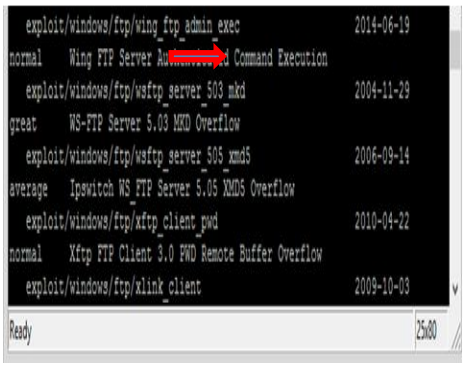
Kemudian *user* akan melakukan pencegahan terhadap serangan tersebut dengan menggunakan *firewall* yang telah di konfigurasi sebelumnya.

1. Pengujian Sistem Tahap Deteksi Serangan
   a. Di komputer target aktifkan terlebih dahulu aplikasi snort dan kiwi log viewer untuk melakukan pendeteksian serangan terhadap komputer *attacker* (penyerang), selanjutnya *alert* dapat diketahui dengan *log snort* maupun *Kiwi Log Viewer* apabila terjadi serangan kepada komputer target.
   b. Proses ini komputer penyerang menggunakan aplikasi *metasploit framework* untuk melakukan simulasi serangan *Remote Code Execution* terhadap *Wing FTP Web Server*, dengan langkah sebagai berikut. Buka aplikasi *metasploit framework*, yang sudah diinstal pada komputer *client*.
   c. Tampilan *metasploit console* siap digunakan



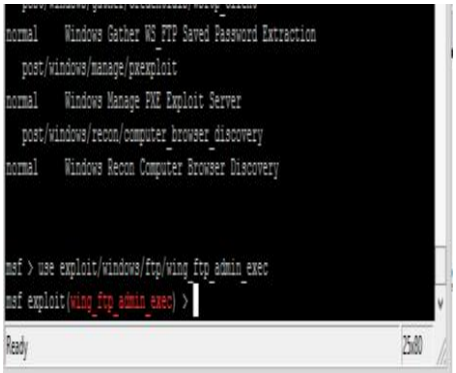
Gambar 11. Tampilan metasploit

d. Kemudian mulai seranga dengan mencari terlebih dahulu serangan *exploit Wing FTP Web Server*, dengan perintah : "*search Wing Ftp Server*"



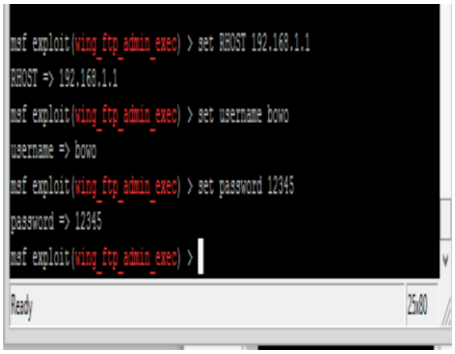
Gambar 12. Tampilan metasploit

e. Selanjutnya melakukan serangan dengan perintah "*use exploit/windows/ftp/wing_ftp_admin_exec*" seperti tampilan gambar dibawah ini:



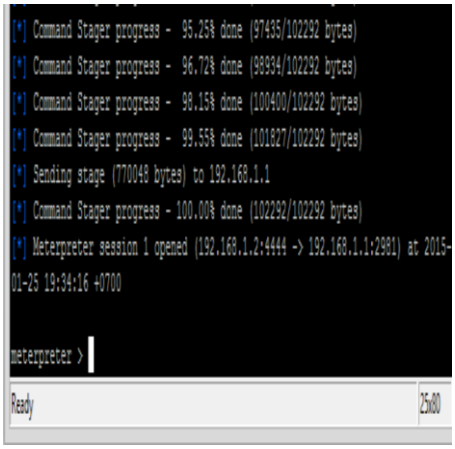
Gambar 13. Tampilan perintah serangan

f. Menentukan *host*, *username*, dan *password* target yang di *exploit*, seperti pada tampilan dibawah ini:



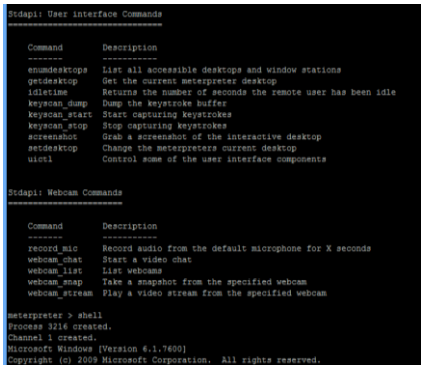
Gambar 14. Tampilan menentukan *host,username,* dan *password*

g. Kemudian menjalankan eksploitasi pada target dengan perintah *exploit*. Seperti pada tampilan dibawah ini:



Gambar 15. Tampilan proses *exsploit*

h. Tampilan bahwa penyerang telah masuk ke target serangan

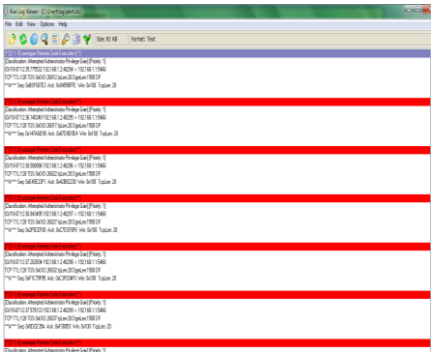


Gambar 16. Tampilan penyerang telah masuk ke sistem target.

i. Komputer target, snort dapat mendeteksi sebuah serangan, selanjutnya akan merespon *alert* bentuk serangan tersebut dan aplikasi kiwi log viewer akan

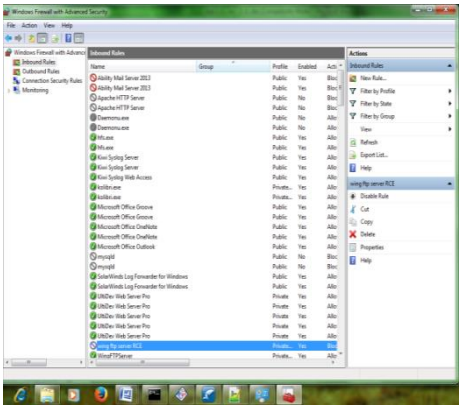
menampilkan serangan tersebut. Namun dari pengujian dengan *snort* dapat menangkap serangan *Remote Code Execution* yang dilakukan oleh *attacker.*

Tampilan gambar dibawah ini:



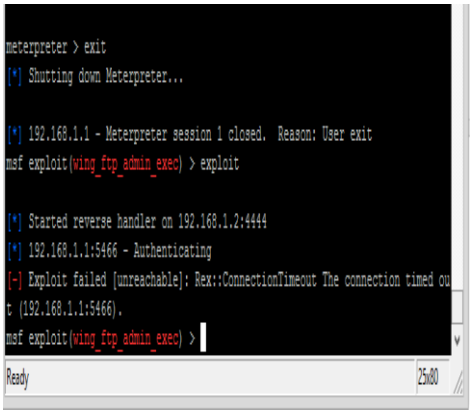
Gambar 17. Tampilan kiwi log viewer peringatan serangan *Remote Code Execution*

2. Pengujian Sistem Pencegahan Serangan
   a. Pengujian pencegahan serangan tersebut dilakuakn dengan cara menggunakan snort dan juga mengoperasikan *kiwi log viewer*, sehingga saat serangan masuk maka akan diketahui bentuk serangan yang masuk ke *server* dan dilakukan pencegahan langsung dengan menggunakan *firewall.*



Gambar 18. Pencegahan *Remote Code Execution* menggunakan *firewall*

   b. Setelah melakukan pencegahan maka penyerang tidak bisa lagi menyerang ke dalam sistem target.



Gambar 19. Gagal menyerang target

PEMBAHASAN

Penelitian ini hanya dilakukan dengan bebrapa tahapan intallasi aplikasi yang bisa didapatkan secara gratis pada web resminya. Sehingga dalam penelitian ini tidak banyak mengeluarkan biaya. Banyak cara atau tutorial installasi yang telah disediakan. Namun dalam prosesnya banyak sekali masalah-masalah yang ditemui dalam penelitian ini, khususnya pada saat menyesuaikan *software* yang satu dengan *software* yang lain, yang seharusnya dapat berjalan secara bersama.

Pendeteksian serangan *Remote Code Execution* memnggunakan *rule* yang telah dibuat khusus untuk mendeteksi serangan RCE yaitu

alert tcp any any -> any any (msg:"serangan Remote Code Execution";content:"os.execute"; dsize:>1022; classtype: attempted-admin; sid:1;).

Maksud dari rule tersebut merupakan rule yang dibuat untuk alert serangan *Remote Code Execution*. Dimana ketika ada perintah *os.execute* yang masuk dengan ukuran data masuk yang melebihi 1 MB maka akan ada peringatan oleh *snort*.

Sistem keamanan pada penelitian ini menggunakan *Firewall* bawaan pada windows 7. *Firewall* digunakan untuk melakukan pencegahan serangan *Remote Code Execution* terhadap *Wing FTP web Server*. Hanya saja kita masih perlu untuk melakukan pengeditan agar serangan *Remote Code Execution* tidak dapat masuk ke server kembali.

Penelitian ini menggunakan bebrapa aplikasi yang sangat penting yaitu dengan IDS *software snort, kiwi log viewer,* dan *firewall*. Pada *software* tersebut digunakan untuk menghasilkan sebuah sistem yang baik dalam melakukan pencegahan dan pendetreksian serangan *Remote Code Execution* terhadap *Wing* FTP *Web Server* yang sangat berbahaya. Terbukti dari pengujian sebelumnya dan dilakukan simulasi maka masih ada kerentanan pada target dari penelitian yang saya lakukan ini semoga penelitian ini bisa bermanfaat.

KESIMPULAN

Setelah melakukan penelitian dari tahap awal dan sampai akhir, maka penelitian ini mendapatkan hasil kesimpulan, diantaranya yaitu sebagai berikut:

1. Penelitian ini telah berhasil membangun *sistem Intrusion Detection System* (IDS) pada sistem operasi windows 7 yang telah dibuat sebelumnya untuk mendeteksi serangan *Remote Code Execution* terhadap *Wing FTP Web Server*.
2. *Snort* dapat melakukan bentuk peringatan jika terjadi serangan keamanan pada jaringan komputer, maka snort dapat meningkatkan keamanan dalam suatu jaringan komputer. Bagaimana snort dapat melakukan pendeteksian tergantung dari rancangan rule yang dibuat sesuai dengan pola serangan tersebut.
3. Masih ada kerentana sistem pada *Wing FTP Server*, terbukti dalam penelitian ini *wing ftp server* masih bisa ditembus dengan aplikasi *metasploit farmework*.
4. *Firewall* telah berhasil melakukan pencegahan serangan *Remote Code Execution* terhadap *Wing FTP Server*, dengan cara melakukan blok IP pada penyerang.
5. *Firewall* dapat digunakan untuk bagaimana melakukan pencegahan apabila ada suatu serangan. Semakin baik keamanan jaringan yang dibuat, maka semakin lengkap layanan firewall yang dikonfigurasi dan semakin kurang baik keamanan yang di terapkan, maka akan mudah serangan akan masuk.

DAFTAR PUSTAKA

Diyah, Handry Fratama. (2010). *Pengenalan IDS (Intrusion Detection System) dan IPS (Instrusion Prevention System) sebagai Manajemen Keamanan Informasi dan Pengamanan Jaringan.* Skripsi Dipublikasikan. Universitas Sriwijaya Palembang.

Riyantika & Lidyawati. (2013). *Analisis Kinerja Sistem Pengamanan Snort IDS dan IP-Tables di Area Laboratorium RDNM PT. "X"*. Diksi: *Jurnal Ilmiah: Reka Elkomika*, 1 (3) 186 – 197.

Jarwanto. (2014). *Deteksi dan Pencegahan Buffer Overflow Terhadap EFM Web Server Menggunakan Snort*. Skripsi Dipublikasikan. FKI Universitas Muhammadiyah Surakarta.

Kusumawati, Monika. (2010). *Implementasi IDS (Intrusion Detection System) serta Monitoring Jaringan dengan Interface Web Berbasis BASE pada Keamanan Jaringan*. Skripsi Dipublikasikan. Universitas Indonesia.

Putri, Lidia. (2011). *Implementasi Intrusion Detection System (IDS) Menggunakan Snort Pada Jaringan Wireless Studi Kasus: SMK TRIGUNA CIPUTA*. Skripsi Dipublikasikan. Universitas Islam Negeri Syarif Hidayatullah Jakarta.

Pratomo, Baskoro Adi. (2011). *ITS-Undergraduate-14614-5106100068-Chapter1.pdf*. Institut Teknologi Surabaya: Master's Thesis.

Rochim , Asadu Rahmatika.(2010). *Eksploitasi Keamanan Sistem Operasi Windows XP Pada Jaringan LAN*. Skripsi Dipublikasikan. Sekolah Tinggi Manajemen Informatika Dan Komputer AMIKOM Yogyakarta.

Serea, Razvan. (2015). *Wing FTP Server*. Diakses dari http://www.neowin.net/news/wing-ftp-server-443/ (diakses pada tanggal 13 Februari 2015).

Suherman. (2011). *Secure Programming Untuk Mencegah Buffer overflow*. Skripsi Dipublikasiakan. Universitas Islam Negeri (UIN) Alauddin Makassar.

Sukirmanto. 2013. *Rancang Bangun dan Implementasi Keamanan Jaringan Komputer Menggunakan Metode Intrusion Detection System (IDS) pada SMP Islam Terpadu PAPB.* Jurnal. Universitas Semarang.

Shafitri, Ira Vaoliya. (2012). *Analisi dan Implementasi Intrusion Detection System (IDS) Untuk Pemberitahuan Serangan Pada Keamanan Sistem Jaringan Komputer Melalui Email*. Skripsi Dipublikasikan. Institut Teknologi Telkom Bandung.

Unswagati, (2010). *Keamanan Jaringan Komputer*. Diakses dari http://unswagati-crb.ac.id/component/option,com_phocadownload/Itemid,73/download,55/id,11/view,category/ (diakses pada tanggal 13 Februari 2015).

Wibowo, Rian Adi. (2014). Analisi dan Implementasi IDS Menggunakan Snort Pada Cloud Server Di Jogja Digital Vallley. Skripsi Dipublikasikan. Stimik Amikom Yogyakarta.

Yantu, Ramdan. (2014). *Tutorial Celah Keamanan Pada PHP Scripts*.Diakses dari https://dl.packetstormsecurity.net/papers/general/phpbugs-tutorial.pdf dl.packetstormsecurity.net/papers/general/phpbugs-tutorial.pdf/ (diakses pada tanggal 13 Februari 2015).

Zulhikam, Ahmad. 2011. Firewall. Diakses dari http://jaringankomputer.org/firewall-pengertian-fungsi-manfaat-dan-cara-kerja-firewall/ (diakses pada tanggal 6 Juni 2015).