ANALISA PENDETEKSIAN DAN PENCEGAHAN SERANGAN BUFFER OVERFLOW TERHADAP ACHAT

Makalah

Program Studi Informatika

Fakultas Komunikasi dan Informatika

Diajukan oleh :

Theoremanto Aji Wibisono

Fatah Yasin Al-Irsyadi, S.T.,M.T

PROGRAM STUDI INFORMATIKA

FAKULTAS KOMUNIKASI DAN INFORMATIKA

UNIVERSITAS MUHAMMADIYAH SURAKARTA

JULI 2015

HALAMAN PENGESAHAN

Publikasi ilmiah dengan judul :

ANALISA PENDETEKSIAN DAN PENCEGAHAN SERANGAN BUFFER OVERFLOW TERHADAP ACHAT

Yang dipersiapkan dan disusun oleh :

Theoremanto Aji Wibisono

L200110039

Telah disetujui pada :

Hari : Sabtu

Tanggal : 10 Juli 2015

Pembimbing

Fatah Yasin Al-Irsyadi, S.T,M.T.

NIK : 738

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	:	THEOREMANTO AJI WIBISONO
NIM	:	L200110039
Judul	:	ANALISA PENDETEKSIAN DAN PENCEGAHAN SERANGAN BUFFER OVERFLOW TERHADAP ACHAT
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, 13 Juli 2015

Biro Skripsi
Informatika

Adjie Sapoetra, S.Kom

Turnitin Originality Report

ANALISA PENDETEKSIAN DAN PENCEGAHAN SERANGAN BUFFER OVERFLOW TERHADAP ACHAT by Theoremanto Aji Wibisono

From publikasi september 2015 (publikasi)

Processed on 09-Jul-2015 17:15 WIB
ID: 554820042
Word Count: 2589

Similarity Index	Similarity by Source	
27%	Internet Sources:	7%
	Publications:	0%
	Student Papers:	24%

sources:

1 10% match (student papers from 06-Jul-2015)
Class: publikasi
Assignment:
Paper ID: 554234951

2 5% match (student papers from 07-Jul-2015)
Class: publikasi
Assignment:
Paper ID: 554420538

3 3% match (student papers from 02-Dec-2014)
Class: publikasi
Assignment:
Paper ID: 484675899

4 2% match (student papers from 24-Nov-2014)
Class: publikasi
Assignment:
Paper ID: 481855234

5 2% match (student papers from 07-Jul-2015)
Class: publikasi
Assignment:
Paper ID: 554455752

6 1% match (student papers from 09-Jul-2015)
Class: publikasi
Assignment:
Paper ID: 554819906

7 1% match (Internet from 03-Jun-2014)
http://smancaontheair.blogspot.com/

8 1% match (student papers from 25-Jun-2013)
Submitted to American Public University System on 2013-06-25

ANALISA PENDETEKSIAN DAN PENCEGAHAN SERANGAN BUFFER OVERFLOW TERHADAP ACHAT

Theoremanto Aji Wibisono, Fatah Yasin Al-Irsyadi

Informatika, Fakultas Komunikasi dan Informatika

Universitas Muhammadiyah Surakarta

E-Mail : theorem.d19@gmail.com

ABSTRAKSI

Masalah keamanan sebuah jaringan komputer sangat rentan terhadap serangan dari berbagai kalangan. Ada berbagai alasan atau motif dari serangan-serangan tersebut. Adapun macam alasannya yaitu untuk, balas dendam, politik, atau cuma untuk unjuk kemampuan. Di balik mudahnya akses informasi-informasi yang ada di internet ada pula bahaya besar yang sewaktu-waktu dapat mengintai, yaitu dengan berbagai macam serangan untuk berusaha mencari kelemahan dari sistem keamanan jaringan komputer yang digunakan. Serangan tersebut dapat mengakibatkan kerusakan data, kehilangan data atau bahkan kerusakan pada *hardware* komputer.

Penelitian ini akan menganalisis bagaimana suatu *serangan Buffer Overflow* bekerja pada software *AChat* Protokol, dan kemudian melakukan deteksi serangan menggunakan snort IDS. Pendeteksian dan pencegahan dilakukan dengan membuat rancangan *firewall* aktif untuk memonitor setiap data yang masuk kedalam *server*, apakah data tersebut merupakan serangan *Buffer Overflow* atau bukan.

Hasil dari percobaan ini adalah suatu system yang sudah dibangun dapat bekerja pada keamanan jaringan yang dapat mendeteksi dan mencegah terjadinya serangan *Buffer Overflow* terhadap *Software AChat*. Sistem yang sudah di bangun tersebut sudah berhasil dengan cara dilakukan suatu simulasi atau pengujian sistem, yaitu snort IDS sudah berhasil untuk mendeteksi serangan dan konfigurasi firewall sudah dapat mencegah serangan yang masuk ke sistem.

Kata kunci : Keamanan Jaringan Komputer, *Buffer Oveflow*, IDS *Snort, AChat*, Metasploit *Faramework, Firewall*

PENDAHULUAN

Diskusi tentang masalah keamanan sebuah jaringan komputer, sudah pasti sangat rawan terhadap serangan dari luar. Banyak sebab yang digunakan untuk melakukan kegiatan penyerangan pada suatu jaringan komputer. Istilah *hacker* pada umum nya adalah seseorang yang memiliki keinginan dalam mengetahui secara mendalam mengenai kerja *system* dan jaringan computer, sehingga menjadi orang yang ahli dalam bidang penguasaan *system* dan jaringan computer. Tetapi dengan kemudahan dalam pengaksesan internet ada pula ancaman besar yang mengintai, yaitu beberapa macam serangan yang bertujuan untuk mencari kerentanan dari sebuah system keamanan jaringan computer.

Buffer Overflow adalah salah satu dari banyak nya serangan yang dapat mengintai dengan menyerang software dalam memanfaattkan kelemahan memory. Buffer Oveflow sering terjadi dalam software yang memakai bahasa pemrograman yang rendah seperti C. Pada bahasa pemrograman itu, beberapa fungsi standar yang digunakan tidak melakukan pengecekan memori untuk variable data. Secara keseluruhan system kerja buffer overflow yaitu dengan memberikan input an ke dalam suatu program yang melebihi jumlah atau ukuran file yang seharusnya.

Di karenakan suatu serangan dapat dating kapan saja, dibutuhkan suatu system keamanan yang dapat memonitor suatu paket data yang masuk, apakah itu termasuk serangan atau bukan. Salah satu upaya pencegahan dan meningkatkan keamanan komputer yaitu dengan menggunkan *tools* dari windows sendiri firewall. Berdasarkan beberapa pertimbangan dengan bahanya serangan terhadap jaringan computer, maka penelitian ini akan membahas pendeteksian dan pencegahan *Buffer Overflow* terhadap *software Achat*. Adapun system pendeteksian yang digunakan dalam penelitian ini adalah *IDS snort*, *snort* adalah salah satu *IDS* yang tergolong mudah, pembuatan rule-rule nya pun juga mudah. Serta dapat di *download free* di situs resminya.

TINJAUAN PUSTAKA

Khairul Anam (2011) dalam tugas akhirnya yang berjudul "Sistem Pendeteksi Serangan pada Jaringan Komputer Menggunakan *Snort* Berbasis *SMS Gateway*" dalam penelitian ini dibangun suatu sistem pendeteksian serangan menggunakan *snort* sebagai *IDS* nya dan pemberitahuan atau alertnya berbasis *SMS Gateway*

Petrani Restanti L (2014) dalam tugas akhirnya yang berjudul "Implementasi Analisis Kolaborasi *IDS Snort* dan *Honeypot*" dalam penelitian ini dibangun dua buah system *IDS* yaitu *Snort* dan *Honeypot*, kedua system *IDS* tersebut kemudian di kolaborasikan untuk menganalisis sebuah serangan. Dan hasilnya *Snort* dan *Honeypot* dapat meningkatkan keamanan computer.

Nur Muhammad (2011) dalam tugas akhirnya yang berjudul "*Snort Intrusion Detection System (IDS)* Untuk Keamanan Jaringan" dalam penelitian ini dibangun sistem *IDS snort* mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan.

Landasan teori yang digunakan dalam tugas akhir ini adalah :

1. Keamanan Jaringan Komputer

Keamanan komputer adalah sebuah teknologi yang biasa disebut keamanan informasi yang terapkan dalam komputer. Sistem keamanan computer merupakan salah satu usaha dalam meningkatkan dan mengamankan kinerja computer.

2. Intruction Detection System (IDS)

   IDS merupakan salah satu pendeteksian yang bekerja dengan cara mendeteksi berdasarkan lalu lintas data yang kemudian mencari keanehan dari lalu lintas data tersebut. IDS juga berguna sebagai pemonitor dan memberi alert atau pemberitahuan ketika terjadi serangan.

3. *Intrusion Prevention System* (IPS)

   IPS adalah suatu system yang digunakan untuk pencegahan serangan, yaitu dengan menyatukan system firewall dan IDS. IPS menggukan signature dari data yang memonitor aktivitas traffic di jaringan, jadi ketika data yang masuk dan keluar sebelum merusak system dilakukan pencegegahan terlebih dahulu

4. Snort

   Snort adalah sebuah aplikasi yang bertujuan untuk mengawasi sebuah lalulintas data di suatu jaringan computer. Aplikasi ini bersifat opensource sehingga dapat digunakan secara free atau gratis. Snort sendiri tergolong mudah digunakan dan dalam pembuatan rule-rule nya mudah di konfigurasi. Tetapi snort sendiri termasuk aplikasi yang command-line, sehingga menggunakan nya sedikit menyulitkan bagi yang belum terbiasa menggunakan command-line. Snort sendiri hanya dapat mendeteksi serangan aja, belum bias untuk melakukan pencegahan serangan sekaligus.

5. Metasploit

   Metasploit ini merupakan aplikasi keamanan yang sering sekali digunakan dalam melakukan simulasi ketahanan suatu system. Sistem kerja metasploit ini sendiri yaitu menyerang application layer yang merupakan metode penyerangan pada aplikasi yang belum di encode. Metasploit bias disebut juga sebagai *remote exploitation*, artinya penyerang dapat mengendalikan server dari jarak jauh.

6. Achat

   Achat adalah sebuah aplikasi yang dapat berhubungan atau chatting dengan teman dan kolega yang sangat mudah dilakukan, terutama jika mereka berada di *LAN* yang sama (*Local Area Network*). *Achat* dapat memulai percakapan dalam waktu singkat dan *Achat* adalah sebuah aplikasi utilitas yang diciptakan tepat untuk tujuan ini.

7. Buffer Overflow

   Buffer Overflow adalah salah satu serangan yang dapat menyebabkan banyak masalah dalam suatu system komputer. Jadi system kerja *Buffer Overflow* sendiri yaitu dengan memberikan input an ke dalam suatu program yang melebihi jumlah atau ukuran file yang seharusnya.

8. Firewall

   Firewall adalah sebuah system yang memperbolehkan traffic jaringan yang dianggap aman untuk melewatinya dan mencegah yang dianggap tidak aman untuk system. Firewall pada

umumnya digunakan untuk mengendalikan akses terhadap siapa-siapa saja yang dapat mengakses jaringan.

METODE PENELITIAN

Metode penelitian ini dilakukan dengan cara pustaka yaitu cara mengumpulkan data dengan cara mempelajari literatur, artikel, buku, karya ilmiah, atau pustaka yang lainnya serta mengutip pendapat-pendapat para ahli dari buku-buku bacaan yang ada kaitannya dengan materi pembahasan penelitian ini.

ALUR PENELITIAN

Tahapan-tahapan yang dilakukan dalam kegiatan penelitian dituliskan sebagai berikut:

1. Memulai Pengumpulan Data yaitu mengumpulkan data-data yang diperlukan untuk merancang dan membangun system meliputi pencarian software Achat sebagai objek penelitian, kemudian pencarian tipe serangan yang dapat menyerang software Achat yaitu dengan tipe serangan Buffer Overflow.
2. Tahap ini pengolahan dan analisis yang dilakukan dengan menggunakan data-data yang diperoleh dari proses pengumpulan data.Pengolahan dan analisis data yang dilakukan dengan menggunakan data-data yang diperoleh dari proses pengumpulan data.
3. Perancangan sistem langkah ini merupakan langkah persiapan sebelum melanjutkan ke langkah berikutnya, dengan mempersiapkan beberapa software yang sudah di ada pada tahap pengumpulan data
4. Implementasi yaitu melakukan installasi software yang dibutuhkan sebelumnya dalam perancangan system, yaitu :
   a. Installasi Metasploit di client
   b. Konfigurasi Software Achat
   c. Installasi dan Konfigurasi IDS Software
   d. Me-edit snort, Berikut ini adalah beberapa yang harus dilakukan konfigurasi sekaligus penambahan pada snort.conf yaitu :
   C:/Snort/etc/snort.conf
   Dari:

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

Gambar 1 Konfigurasi 1

Menjadi:

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

Gambar 2 Konfigurasi 2

Dari :

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

Gambar 3 Konfigurasi 3

Menjadi :

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

Gambar 4 Konfigurasi 4

Dari :

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

Gambar 5 Konfigurasi 5

Menjadi :

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

Gambar 6 Konfigurasi 6

Dari :

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

Gambar 7 Konfigurasi 7

Menjadi :

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

Gambar 8 Konfigurasi 8

Dari :

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

Gambar 9 Konfigurasi 9

Menjadi :

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

Gambar 10 Konfigurasi 10

e. Installasi Kiwi Log Viewer

f. Konfigurasi Rule Snort

alert udp any any -> any 9256 (msg:"Achat buffer overflow"; content:"55 2a 55 6e 58 6e 05 14"; content:"43 55 6e 58 6e 2a 2a 05"; sid:1000006; rev:1;)

Pada rule yang sudah dibuat di sini menggunakan UDP, karena protocol yang digunakan dalam aplikasi yang berhubungan dengan chat menggunakan protocol UDP. UDP sendiri adalah sebuah protocol yang dimana ketika ada pesan dari server ke client maka UDP itu hanya memastikan pesan itu sampai tujuan, tetapi UDP ini tidak tahu apakah pesan itu masih lengkap atau tidak.

g. Konfigurasi Firewall

5. Pengujian Sistem
6. Pengujian sistem dilakukan dengan melakukan serangan *Buffer Overflow* menggunakan aplikasi *metasploit* dan melakukan deteksi dengan aplikasi *snort* IDS.

HASIL PENELITIAN

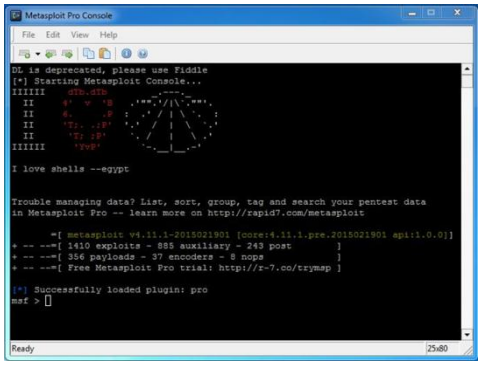
Hasil dari penelitian ini adalah suatu sistem keamanan jaringan yang mampu mendeteksi dan mencegah terjadinya serangan *Buffer Overflow* pada aplikasi Achat. Sistem yang dikeluarkan dalam penelitian ini bisa mencakup 2 tahap yaitu tahap deteksi serangan dan tahap pencegahan serangan.

1. Pengujian Sistem Tahap Peneteksian Serangan

a. Di komputer server diaktifkan dulu Snort untuk melakukan deteksi serangan dari komputer client, jadi peringatan serangan dapat dilihat melalui *log* Snort ketika ada serangan masuk ke komputer server.

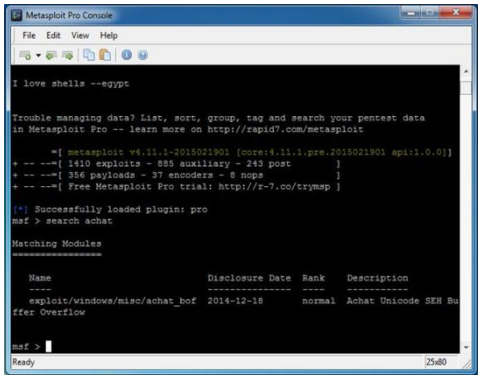
b. Pada tahap ini komputer client dengan aplikasi *metasploit* melakukan simulasi serangan *Buffer Overflow* pada aplikasi *Achat*, dengan langkah sebagai berikut.

c. Tampilan *metasploit*



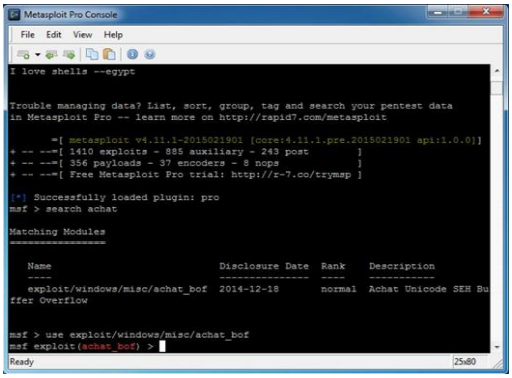
Gambar 1. Tampilan metasploit

d. Kemudian mencari dahulu serangan *exploit Achat*, dengan perintah : "*search Achat*"



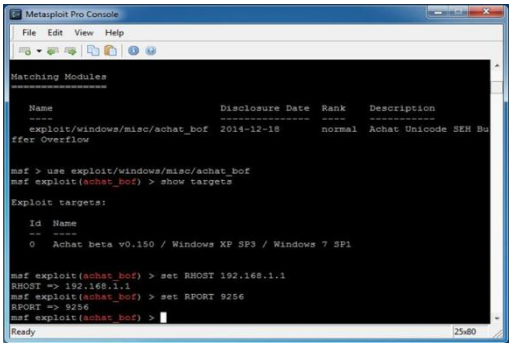
Gambar 2. Tampilan metasploit

e. Selanjutnya melakukan simulasi serangan dengan perintah *"use exploit/windows/misc/achat_bof"* seperti tampilan gambar dibawah ini:



Gambar 3. Tampilan perintah serangan

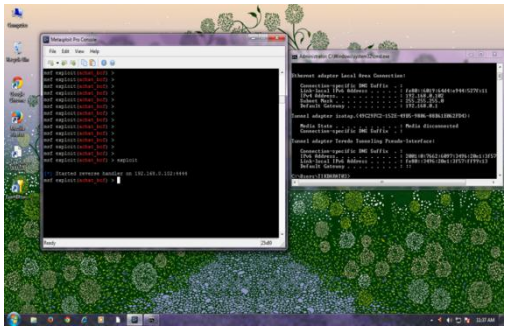
f. Menentukan host dan port target yang di exploit, seperti pada tampilan dibawah ini:



Gambar 4. Tampilan menentukan *host* dan *port*

g. Kemudian menjalankan eksploitasi pada target dengan perintah *exploit* pada :

1) Client 1 dengan IP 192.168.0.102. Seperti pada tampilan dibawah ini :

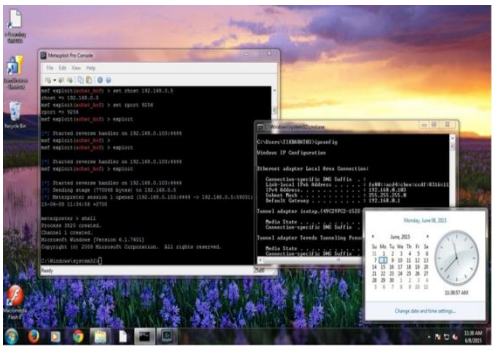


Gambar 5 Tampilan client 1 menjalankan exploit pada target

2) Client 2 dengan IP 192.168.0.165. Seperti pada tampilan dibawah ini :

Gambar 6. Tampilan client 2 menjalankan exploit pada target

3) Client 3 dengan IP 192.168.0.103. Seperti pada tampilan dibawah ini :



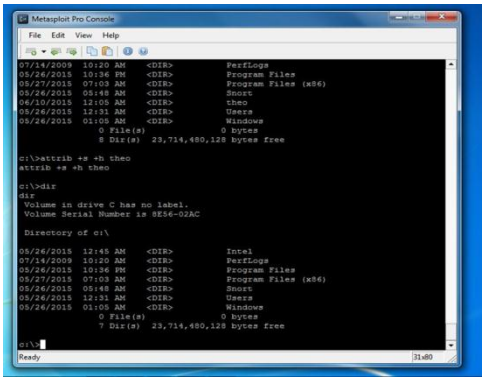
Gambar 7. Tampilan client 3 menjalankan exploit pada target

Setelah melakukan uji coba atau simulasi serangan Buffer Overflow terhadap software Achat dengan 1 server dan 3 client dapat disimpulkan, bahwa jika ketiga client tersebut menyerang server dengan bersamaan maka hanya 1 client yang berhasil menyerang atau masuk ke system server. Client yang berhasil menyerang server itu adalah client yang terlebih dahulu menyerang, alasannya karena jika server sudah terserang aplikasi Achat di server akan eror. Jadi client berikutnya sudah tidak dapat menyerang ke server lagi

h. Setelah masuk kedalam sistem target penyerang dapat mengakses sistem yang ada di komputer target. Disini kita mencoba menyerang PC

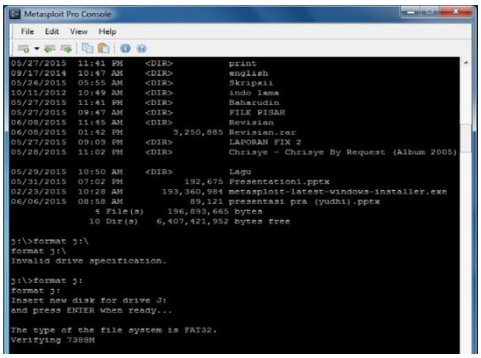
server dengan 5 krakteristik penyerangan yang berbeda.

1) Penyerang sudah dapat menyembunyikan file atau folder dari computer server

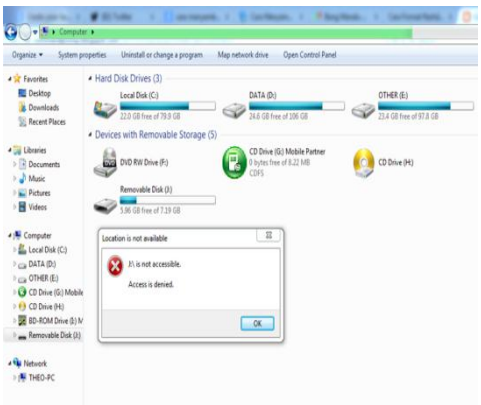


Gambar 8. Tampilan file theo telah disembunyikan

2) Penyerang dapat mem-format salah satu drive dari computer server

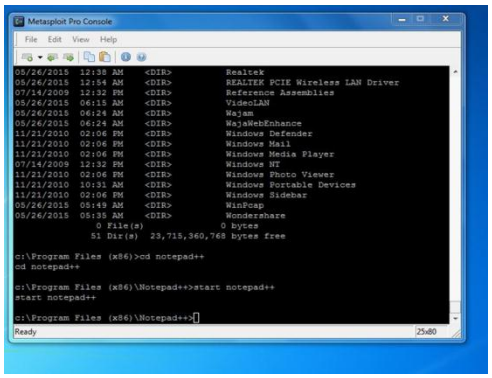


Gambar 9. Tampilan drive J telah di format

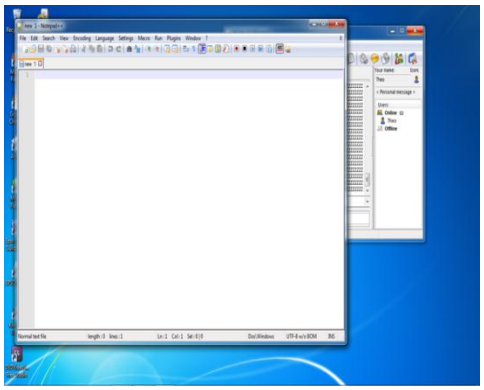


Gambar 10. Tampilan di server saat sedang di format

3) Penyerang dapat menjalankan program di computer server

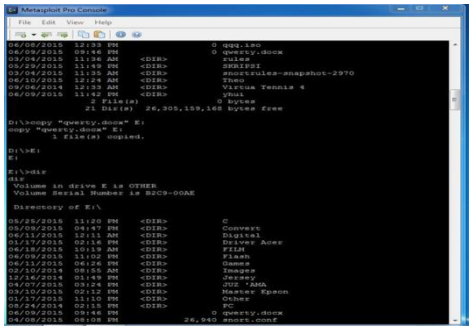


Gambar 11. Tampilan saat program berhasil dijalankan



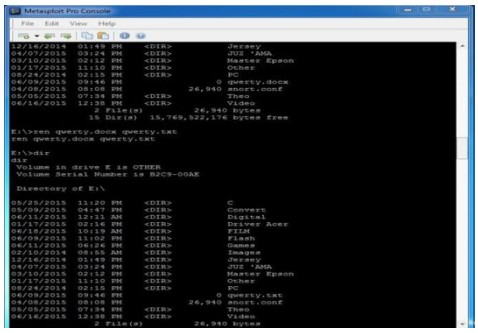
Gambar 12. Tampilan di server saat notepad berhasil dijalankan

4) Penyerang dapat meng-copy file atau folder di computer server, meng-copy file qwerty.docx ke drive E



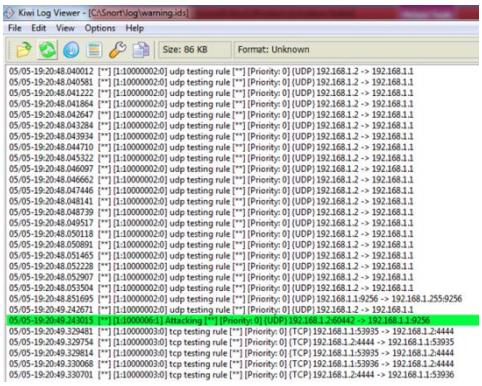
Gambar 13. Tampilan setelah file berhasil di copy

5) Penyerang dapat me rename file atau folder di computer server, me rename file qwerty.docx menjadi qwerty.txt



Gambar 14. Tampilan setelah file berhasil di rename

i. Di komputer target, snort mendeteksi adanya serangan, dan kemudian memunculkan *alert* atau peringatan tentang serangan yang ditampilkan oleh *kiwi log viewer*. Dalam pengujian ini *snort* menangkap serangan *Buffer Overflow* yang dilakukan oleh komputer client.



Gambar 15. Tampilan peringatan ada serangan Buffer Overflow terhadap target.

2. Pengujian Sistem Pencegahan Serangan

Pada tahap ini adalah proses melakukan pencegahan terhadap serangan Buffer Overflow pada aplikasi Achat.

Berikut ini tahapan dalam melakukan pencegahan terhadap serangan Buffer Overflow sebagai berikut:

a. Tahap I. Mulai melakukan pencegahan serangan.
b. Tahap II. Tahap ini request serangan datang.
c. Tahap III. Tahap ini snort mendeteksi paket yang datang dan menyamakan paket dengan rule pada snort.
d. Tahap IV. Tahap ini dapat dilihat apakah snort dapat menangkap request yang masuk dengan baik dan tepat, apabila belum berjalan dengan baik maka snort akan menghentikan proses dan lanjut ke alamat berikutnya.
e. Tahap V. Tahap ini apabila snort telah menangkap request dengan benar, maka snort akan menyimpan log serangan tersebut di snort.conf.
f. Tahap VI. Tahap ini kiwi log viewer membaca log serangan tersebut.
g. Tahap VII. Tahap ini firewall memblok alamat IP client yang melakukan serangan tersebut.

PEMBAHASAN

Penelitian ini bias berhasil karena dilengkapi dengan ada beberapa tahap installasi software-sofware yang open source atau gratis. Banyak tutorial installasi software yang sudah disediakan di *web-web* resmi, *youtube*, dan lain-lain yang di dapat secara mudah, dengan demikian bisa memberikan kemudahan dalam proses installasi aplikasi yang dibutuhkan dalam karya ini. Namun dalam proses installasi masih banyak kendala-kendala yang ditemui dalam karya ini

Pada deteksi serangan *Buffer Overflow rule* yang digunakan sebagai

berikut *alert udp any any -> any 9256 (msg:"Achat buffer overflow"; content:"55 2a 55 6e 58 6e 05 14"; content:"43 55 6e 58 6e 2a 2a 05"; sid:1000006; rev:1;)* Maksud dari rule tersebut merupakan rule yang dibuat untuk alert atau pemberitahuan serangan *Buffer Overflow*. Dimana ketika ada pesan atau inputan yang berlebihan pada program yang dijalankan maka akan ada peringatan oleh snort. Isi dari peringatan tersebut adalah pesan "Attacking" yang berarti computer server telah diserang.

Sistem pencegahan dalam penelitian ini adalah menggunakan firewall, yaitu dengan mengconfigurasi firewall dengan mem-blok IP client atau penyerang

KESIMPULAN

Setelah melakukan simulasi penelitian dari tahap awal sampai akhir, penelitian ini menghasilkan beberapa kesimpulan, diantaranya adalah sebagai berikut:

1. Penelitian ini sudah berhasil membangun suatu *sistem* IDS yang sudah dibuat untuk mendeteksi serangan *Buffer Overflow* pada aplikas*i Achat*.
2. *Snort IDS* berhasil memberikan pemberitahuan adanya sebuah serangan ke computer server, sehingga dapat meningkatkan keamanan komputer. Berhasil atau tidaknya sebuah serangan dapat di deteksi oleh *Snort* IDS tergantung rule yang sudah dibuat
3. *Firewall* sudah berhasil melakukan pencegahan serangan *Buffer Overflow* terhadap *Software Achat*, dengan cara melakukan blok IP pada penyerang.

DAFTAR PUSTAKA

Arief, Muhammad Rudyanto. (2013). Penggunaan Sistem IDS (Intrution detection System) untuk Pengamanan Jaringan dan Komputer, Skripsi, AMIKOM Yogyakarta.

Arora, Himanshu. (2013). Buffer Overflow Attack Explained with a C Program Example, http://www.thegeekstuff.com/2013/06/buffer-overflow/ diakses pada tanggal 18 Mei 2015.

Gondohanindijo, Jutono. (2012). Sistem Untuk Mendeteksi Adanya Penyusup (IDS : Intrusion Detection System), Fakultas Ilmu Komputer Universitas AKI.

Iswahyudi, Catur dkk. (2014). Implementasi IDS Menggunakan Jejaring Sosial sebagai Media Notifikasi, Makalah, Jurusan Teknik Informatika, FTI, IST AKPRIND.

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

Nur, Muhammad. (2011). Snort Intrusion Detection System (IDS) Untuk Keamanan Jaringan, Skripsi, Fakultas Pendidikan dan Ilmu Pengetahuan Alam (FPMIPA) Universitas Pendidikan Indonesia.

Pentrani, Restanti L (2014). Analisis Kolaborasi IDS Snort dan Honeypot. Skripsi, Fakultas Ilmu Komputer Universitas Dian Nuswantoro.

Ritonga, Yesarela. (2014). Buffer overflow (keamanan komputer), http://prediss.com/blog/it-tutorial/buffer-overflow-keamanan-komputer
diakses pada tanggal 18 Mei 2015.

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

Suwandono, Wisnu Hadi. (2013). Analisa Generalisasi Rules menggunakan Snort IDS, Skripsi, Universitas Pembangunan Nasional “Veteran”.

Syujak, Ahmad Rois. (2012). Deteksi Dan Pencegahan Flooding Data Pada Jaringan Komputer, Skripsi, Universitas muhammadiyah Surakarta.

Windowsecurity. (2015). Analysis of Buffer Overflow Attacks, http://www.windowsecurity.com/articlestutorials/windows_os_security/Analysis_of_Buffer_Overflow_Attacks.html diakses pada tanggal 16 April 2015.

Wulan Nuryanti. (2014). Pengaruh Pengembangan Karier Terhadap Kinerja Karyawan Pada PT. IDS MEDICAL SYSTEM INDONESIA. Skripsi. Universitas pamulang.