

# **DETEKSI DAN PENCEGAHAN BUFFER OVERFLOW TERHADAP EFM WEB SERVER MENGGUNAKAN SNORT**



## **SKRIPSI**

Disusun sebagai salah satu syarat menyelesaikan Program Studi Strata I  
pada Program Studi Teknik Informatika Fakultas Komunikasi dan Informatika  
Universitas Muhammadiyah Surakarta

**Oleh:**

*Jarwanto*  
**NIM : L200110151**

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS KOMUNIKASI DAN INFORMATIKA  
UNIVERSITAS MUHAMMADIYAH SURAKARTA**

**2014**

**HALAMAN PERSETUJUAN**

Skripsi dengan judul

**“DETEKSI DAN PENCEGAHAN BUFFER OVERFLOW TERHADAP  
EFM WEB SERVER MENGGUNAKAN SNORT”**

ini telah diperiksa dan disetujui pada :

Hari : Rabu

Tanggal : 26 November 2014

Pembimbing



**Helman Muhammad, S.T., M.T.**  
**NIK. 1564**

**HALAMAN PENGESAHAN**

**DETEKSI DAN PENCEGAHAN BUFFER OVERFLOW TERHADAP EFM  
WEB SERVER MENGGUNAKAN SNORT**

dipersiapkan dan disusun oleh

**Jarwanto**

NIM :L200110151

telah dipertahankan di depan Dewan Penguji

pada tanggal 29 November 2014

**Susunan Dewan Penguji**

Pembimbing



**Helman Muhammad, S.T., M.T.**

NIK: 1564

Dewan Penguji I



**Hernawan Sulistyanto, S.T., M.T.**

NIK: 882

Dewan Penguji II



**Muhammad Kusban, S.T., M.T.**

NIK: 663

Skripsi ini telah diterima sebagai salah satu persyaratan

untuk memperoleh gelar sarjana

Tanggal *19 Desember 2014*.

Dekan  
Fakultas Komunikasi dan Informatika

  
**Husni Thamrin, S.T., MT., Ph.D.**  
NIK :706

Ketua Program Studi  
Teknik Informatika

  
**Dr. Heru Supriyono, M.Sc.**  
NIK : 970

## DAFTAR KONTRIBUSI

Dengan ini saya menyatakan bahwa skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Berikut saya sampaikan daftar kontribusi dalam penyusunan skripsi:

1. Penulis merancang sistem keamanan jaringan komputer ini dengan beberapa referensi baik dari buku, skripsi, jurnal, maupun internet.
2. Tahap installasi beberapa software baik pada komputer client maupun komputer server, konfigurasi snort dan *firewall*, dilakukan sendiri oleh penulis dengan mengikuti panduan referensi yang disebutkan dalam daftar pustaka laporan skripsi ini.
3. Persiapan peralatan penelitian, tahap deteksi serangan, tahap pencegahan serangan, dan langkah pengujian snort dilakukan penulis dengan dibantu oleh Bryan Pingkan Ramadhan
4. Penulisan laporan skripsi ini murni dilakukan oleh penulis sendiri.

Demikian pernyataan dan daftar kontribusi ini saya buat dengan sejujurnya. Saya bertanggungjawab atas isi dan kebenaran daftar di atas.

Surakarta, 5 November 2014



Jarwanto

Mengetahui:  
Pembimbing



**Helman Muhammad, S.T., M.T.**

NIK : 1564

## MOTTO DAN PERSEMBAHAN

### MOTTO

*Dan hendaklah ada di antara kamu segolongan umat yang menyeru kepada kebajikan,  
menyuruh kepada yang ma'ruf dan mencegah dari yang munkar, merekalah orang-  
orang yang beruntung*

*(Q.S Ali Imran :104)*

*“Usaha tanpa do'a sombong, do'a tanpa usaha omong kosong,  
Do'a dan ikhtiar 2 hal yang utama maka selalu berdo'a dan berusaha tanpa asa,  
taati orang tua dan Allah ta'ala  
jangan menjadikan kesulitan sebagai penghalang untuk meraih cita - cita,  
karena sukses atau tidak tergantung kamu sendiri,  
tidak ada orang yang mampu mengubah nasibmu kecuali dirimu sendiri  
dan harus sukses atau melihat orang sukses “*

*(Penulis)*

*“Milikilah hari ini dengan bersyukur,  
kenanglah hari kemarin sebagai pelajaran,  
dan menangkanlah hari esok dengan kesiapsiagaan”*

*(Anisya Puji Lestari)*

## **PERSEMBAHAN**

Sebagai rasa syukur penulis persembahkan karya ini kepada :

- 1) Allah SWT yang selalu melimpahkan rahmat dan hidayah bagi hambaNya serta yang selalu menunjuki ke jalan yang lurus.
- 2) Kedua orang tuaku tercinta, Bapak Atmo Wiyono dan Ibu Sami untuk kasih sayang selama ini yang tak terbatas, untuk setiap nasihat, setiap doa yang dipanjatkan untuk kesuksesan penulis, serta dukungan moril dan materiilnya.
- 3) Bapak dan Ibu Asuh, Bapak Agus Sumadi S.Ag., M.Pd dan Ibu Siti Aminah yang telah membimbing penulis serta motivasi dan do'a yang luar biasa sehingga penulis mampu study lanjut sampai sekarang.
- 4) Dek Anisya Puji Lestari atas do'a dan motivasinya
- 5) Adik-adik Panti 'Aisyiyah yang selalu memberi motivasi
- 6) Almamater

## KATA PENGANTAR



Syukur Alhamdulillah hanya pantas kita haturkan kehadiran Allah Rabb semesta alam yang telah memberikan rahmat, hidayah serta nikmat yang tak terhingga kepada hamba-Nya, sehingga penulis dapat menyelesaikan skripsi ini dengan judul “Deteksi dan Pencegahan Buffer Overflow terhadap EFM Web Server Menggunakan Snort”.

Skripsi ini disusun untuk memenuhi kurikulum pada Program Studi Teknik Informatika Universitas Muhammadiyah Surakarta, sebagai kewajiban mahasiswa dalam rangka menyelesaikan program sarjana.

Dengan segala kemampuan fikiran yang maksimal, penulis telah berusaha untuk menyelesaikan laporan skripsi ini, namun demikian penulis menyadari bahwa laporan ini tentunya masih jauh dari kesempurnaan dan masih banyak kekurangan. Oleh karena itu penulis mengharapkan saran serta kritik yang bersifat membangun demi perbaikan. Di sisi lain, skripsi ini juga merupakan hasil karya dan kerjasama dari banyak pihak, walaupun yang terlihat dimuka mungkin hanyalah satu nama. Sehingga dalam kesempatan ini penulis mempersembahkan ucapan terima kasih dan penghargaan setinggi-tingginya dengan segala kerendahan hati, kepada:

1. Allah Subhanahu Wata’ala yang maha segalanya.
2. Shalawat dan salam kepada Rasul Muhammad SAW, keluarganya, dan para sahabatnya, la nabiya wala rasula ba’da, tiada nabi dan Rasul Setelah beliau, suri tauladan yang utama bagi kita semua umatnya.

3. Bapak Husni Thamrin, S.T., M.T., Ph.D. selaku Dekan Fakultas Komunikasi dan Informatika Universitas Muhammadiyah Surakarta yang memberikan izin penelitian.
4. Bapak Dr. Heru Supriyono, S.T., M.Sc selaku Ketua Jurusan Teknik Informatika Universitas Muhammadiyah Surakarta.
5. Bapak Helman Muhammad, S.T., M.T. selaku Pembimbing yang telah berkenan untuk meluangkan waktu dan membimbing serta mengarahkan penulis sehingga terselesaikannya penyusunan skripsi ini.
6. Bapak Hernawan Sulistyanto, S.T., M.T. selaku Dewan Penguji I atas masukan dan saran yang sangat membangun.
7. Bapak Muhammad Kusban, S.T., M.T. selaku Dewan Penguji II atas masukan dan saran yang sangat berarti dalam penelitian ini.
8. Ibu Endah Sudarmilah, S.T, M.Eng selaku Pembimbing Akademik yang telah memberikan banyak arahan dalam proses akademik sejak dari awal hingga akhir studi penulis meraih gelar sarjana.
9. Para Dosen dan Staff pengajar Fakultas Komunikasi dan Informatika Universitas Muhammadiyah Surakarta, yang telah membekali dengan berbagai ilmu pengetahuan yang banyak bermanfaat.
10. Kedua orang tuaku tercinta, Bapak Atmo Wiyono dan Ibu Sami untuk kasih sayang selama ini yang tak terbatas, untuk setiap nasihat, serta dukungan moril dan materiilnya.



11. Bapak dan Ibu Asuh, Bapak Agus Sumadi, S.Ag., M.Pd. dan Ibu Siti Aminah yang telah membimbing penulis serta motivasi dan do'a yang luar biasa sehingga penulis mampu study lanjut sampai sekarang.
12. Bryan Pingkan Ramadhan, yang telah banyak memberikan bantuan dan masukan untuk hasil penulisan skripsi ini.
13. Dek Anisya Puji Lestari, terima kasih atas doa, motivasi semangat yang diberikan pada penulis selama ini.
14. Teman – teman anggota IDM (Ikatan Downloader Muhammadiyah) 2011 atas berbagai ilmu dan canda tawa yang selalu memberikan keceriaan, serta inspirasi kepada penulis.
15. Seluruh teman-teman angkatan 2011 khususnya kelas D berikut teman – teman konsentrasi Jarkom, terimakasih untuk kegembiraan dan kebersamaan yang telah tercipta selama ini.
16. Semua pihak yang telah membantu dalam menyelesaikan skripsi ini yang tentunya tidak dapat penulis sebut satu persatu.

Akhirnya penulis hanya dapat membalas dengan do'a semoga Allah SWT membalas semua budi baik Bapak, Ibu, Saudara dan Sahabat semua. Penulis berharap semoga skripsi ini berguna bagi semua pihak dan bermanfaat bagi penyusun khususnya dan pembaca pada umumnya dalam menambah pengetahuan dan wawasan ilmu. Amin

Surakarta, November 2014

Penulis

## DAFTAR ISI

Halaman Judul.....	i
Halaman Persetujuan.....	ii
Halaman Pengesahan .....	iii
Daftar Kontribusi .....	iv
Motto.....	v
Persembahan .....	vi
Kata pengantar .....	vii
Daftar isi.....	x
Daftar Table .....	xiii
Daftar Gambar.....	xiv
Daftar Bagan .....	xviii
Abstraksi .....	xix
<b>BAB I PENDAHULUAN.....</b>	<b>1</b>
A. Latar Belakang.....	1
B. Rumusan Masalah.....	5
C. Batasan Masalah .....	5
D. Tujuan Penelitian .....	5
E. Manfaat Penelitian.....	6
F. Sistematika Laporan Penelitian .....	6
<b>BAB II TINJAUAN PUSTAKA.....</b>	<b>8</b>
A. Telaah Penelitian Terdahulu .....	8
B. Landasan Teori.....	13
1. Keamanan Jaringan Komputer.....	13

2. Intrusion Detection System.....	14
3. Intrusion Prevention System .....	17
4. Snort.....	19
5. Metasploit framework.....	27
6. Easy File Managemen web Server.....	27
7. Buffer overflow.....	28
<b>BAB III METODOLOGI.....</b>	<b>30</b>
A. Gambaran Umum Penelitian.....	30
B. Alokasi Waktu.....	30
C. Perangkat yang Dibutuhkan .....	31
F. Tahapan Penelitian .....	31
1. Instalasi Metasploit di Client .....	36
2. Instalasi EFM Web Server .....	40
3. Instalasi dan Konfigurasi IDS Software .....	46
4. Installasi Kiwi Log Viewer.....	54
5. Konfigurasi Rule Snort .....	56
6. Konfigurasi Firewall .....	57
7. Pengujian Sistem.....	63
<b>BAB IV HASIL DAN PEMBAHASAN .....</b>	<b>65</b>
A. Hasil Penulisan .....	65
1. Pengujian Sistem Tahap Deteksi Serangan.....	65
2. Pengujian Sistem Tahap Pencegahan Serangan.....	75
B. Pembahasan.....	77

BAB V PENUTUP.....	80
A. Kesimpulan.....	80
B. Saran.....	81
DAFTAR PUSTAKA .....	82

## DAFTAR TABEL

Tabel 1.1 Jumlah serangan terhadap jaringan komputer di Indonesia, dalam jutaan .....	3
Tabel 3.1 Alokasi waktu pelaksanaan penelitian.....	31
Tabel 3.2 Spesifikasi perangkat yang digunakan dalam penelitian .....	32

## DAFTAR GAMBAR

Gambar 1.1 Sebaran bidang pemanfaatan internet di Indonesia.....	1
Gambar 1.2 Jumlah Pengguna Internet di Indonesia .....	2
Gambar 2.1 Skema jaringan <i>Snort</i> NIDS.....	21
Gambar 2.2 Skema jaringan <i>snort</i> HIDS .....	23
Gambar 2.3 Skema jaringan <i>snort</i> DIDS .....	24
Gambar 2.4 Komponen IDS <i>snort</i> .....	25
Gambar 2.5 Contoh penulisan rule <i>snort</i> .....	26
Gambar 3.1 Instalasi metasploit tahap 1 .....	36
Gambar 3.2 Instalasi metasploit tahap 2 .....	36
Gambar 3.3 Instalasi metasploit tahap 3 .....	37
Gambar 3.4 Instalasi metasploit tahap 4 .....	37
Gambar 3.5 Instalasi metasploit tahap 5 .....	38
Gambar 3.6 Instalasi metasploit tahap 6.....	38
Gambar 3.7 Instalasi metasploit tahap 7 .....	39
Gambar 3.8 Instalasi metasploit tahap 8 .....	39
Gambar 3.9 Instalasi metasploit tahap 9 .....	40
Gambar 3.10 Instalasi efm tahap 1 .....	40
Gambar 3.11 Instalasi efm tahap 2 .....	41
Gambar 3.12 Instalasi efm tahap 3 .....	41
Gambar 3.13 Instalasi efm tahap 4.....	42

Gambar 3.14 Installasi efm tahap 5.....	42
Gambar 3.15 Installasi efm tahap 6.....	43
Gambar 3.16 Installasi efm tahap 7.....	43
Gambar 3.17 Tampilan Interface .....	44
Gambar 3.18 Seting akses user .....	44
Gambar 3.19 Login Admin .....	45
Gambar 3.20 Tampilan interface setelah login .....	45
Gambar 3.21 Tampilan installasi snort tahap 1.....	47
Gambar 3.22 Tampilan installasi snort tahap 2.....	48
Gambar 3.23 Tampilan installasi snort tahap 3.....	48
Gambar 3.24 Tampilan installasi snort tahap 4.....	49
Gambar 3.25 Tampilan installasi snort tahap 5.....	49
Gambar 3.26 Tampilan edit rule snort 1 .....	50
Gambar 3.27 Tampilan edit rule snort 2 .....	50
Gambar 3.28 Tampilan edit rule snort 3 .....	51
Gambar 3.29 Tampilan edit rule snort 4 .....	51
Gambar 3.30 Tampilan edit rule snort 5 .....	51
Gambar 3.31 Tampilan edit rule snort 6 .....	51
Gambar 3.32 Tampilan edit rule snort 7 .....	51
Gambar 3.33 Tampilan edit rule snort 8 .....	52
Gambar 3.34 Tampilan verifikasi operasi snort.....	52
Gambar 3.35 Proses inisialisasi snort telah berjalan dengan baik .....	53
Gambar 3.36 Tampilan installasi kiwi log viewer tahap 1.....	54

Gambar 3.37 Tampilan installasi kiwi log viewer tahap 2.....	54
Gambar 3.38 Tampilan installasi kiwi log viewer tahap 3.....	55
Gambar 3.39 Tampilan installasi kiwi log viewer tahap 4.....	55
Gambar 3.40 Tampilan installasi kiwi log viewer tahap 5.....	55
Gambar 3.41 Tampilan interface kiwi log viewer .....	56
Gambar 3.42 Tampilan konfigurasi firewall 1 .....	57
Gambar 3.43 Tampilan profil firewall .....	58
Gambar 3.44 Tampilan Aturan Inbound atau Outbound .....	59
Gambar 3.45 Jenis pilihan aturan.....	59
Gambar 3.46 Panel program .....	60
Gambar 3.47 Panel Protokol dan Port .....	60
Gambar 3.48 Panel Scope .....	61
Gambar 3.49 Panel Action .....	61
Gambar 3.50 Panel Profile .....	62
Gambar 3.51 Panel Name .....	62
Gambar 3.52 Tampilan konfigurasi firewall yang siap digunakan .....	63
Gambar 4.1 Mekanisme simulasi penyerangan .....	65
Gambar 4.2 Alamat IP komputer target (korban) .....	67
Gambar 4.3 Alamat IP komputer penyerang (attacker) .....	67
Gambar 4.4 Tampilan start services pada metasploit.....	68
Gambar 4.5 Tampilan metasploit yang siap untuk digunakan.....	68
Gambar 4.6 Tampilan Mencari exploit buffer overflow .....	69
Gambar 4.7 Tampilan menggunakan exploit buffer overflow.....	69



Gambar 4.8 Tampilan menampilkan target exploit.....	70
Gambar 4.9 Tampilan menentukan target exploit.....	70
Gambar 4.10 Tampilan menggunakan payload meterpreter .....	71
Gambar 4.11 Tampilan setting IP & port target.....	71
Gambar 4.12 Tampilan opsi – opsi yang dibutuhkan .....	71
Gambar 4.13 Tampilan menjalankan eksploitasi.....	72
Gambar 4.14 Tampilan bahwa penyerang telah masuk ke sistem target .....	72
Gambar 4.15 Tampilan sebelum file dihapus oleh penyerang.....	73
Gambar 4.16 Tampilan setelah file dihapus oleh penyerang .....	73
Gambar 4.17 Tampilan log snort mendeteksi serangan buffer overflow.....	74
Gambar 4.18 Tampilan Kiwi Log Viewer yang mendeteksi serangan .....	74
Gambar 4.19 Tampilan firewall yang telah dikonfigurasi mencegah buffer overflow.....	76
Gambar 4.20 Tampilan serangan metasploit yang gagal menyerang target ....	76

## DAFTAR BAGAN

Bagan 3.1. Diagram alir tahapan penelitian .....	33
Bagan 3.2. Diagram alir perancangan dan pengujian system .....	35
Bagan 4.1. Diagram alir Proses pencegahan serangan.....	62

# DETEKSI DAN PENCEGAHAN BUFFER OVERFLOW TERHADAP EFM WEB SERVER MENGGUNAKAN SNORT

**Jarwanto**

Teknik Informatika, Fakultas Komunikasi dan Informatika

Universitas Muhammadiyah Surakarta

Email : djar1too@gmail.com

## **Abstrak**

Teknologi informasi telah berkembang dengan pesat seiring berkembangnya teknologi lain, terutama dengan adanya jaringan komputer baik yang bersifat lokal maupun jaringan internet yang dapat memudahkan untuk melakukan komunikasi dengan pihak lain. Keamanan jaringan komputer sebagai bagian dari sebuah sistem menjadi sangat penting untuk menjaga validitas data. *Buffer overflow* merupakan salah satu serangan yang sangat bahaya ke dalam server jaringan komputer dan dapat terjadi kapan saja. Baik pada saat administrator yang sedang bekerja ataupun tidak. Dengan demikian diperlukan sistem keamanan di dalam server itu sendiri yang mampu mendeteksi langsung apakah setiap paket yang masuk tersebut adalah paket data yang sebenarnya atau tidak. Sehingga keamanan jaringan komputer terjamin dan tidak ada serangan yang dapat menguasainya.

Sistem keamanan ini menggunakan *Operating System Windows 8* dan *EFM Web Server* sebagai target yang merupakan salah satu *web server* untuk sharing file/folder. Sistem ini dibagi menjadi beberapa modul diantaranya IDS software yaitu *snort*, *report viewer* software yaitu *Kiwi Log Viewer*, dan juga *penetration testing* software yaitu *metasploit framework*.

Deteksi dan pencegahan dilakukan dengan sistem yang didesain dengan jalan membuat *firewall* aktif dan *snort* bisa mendefinisikan setiap data yang masuk kedalam server, apakah data yang datang itu merupakan sebuah serangan *buffer overflow* ataukah bukan. Jika yang datang merupakan serangan *buffer overflow* maka *firewall* akan memblokir alamat IP pengirim yang sudah disetting sebelumnya berdasarkan *alert* yang ditampilkan melalui *Kiwi Log Viewer*.

**Kata kunci :** Keamanan Jaringan Komputer, *Buffer Overflow*, *EFM Web Server*, *IDS*, *Snort*, *Kiwi Log Viewer*, *Metasploit Framework*, *Firewall*.