

PEMBUATAN WEB INTERFACE SNORT

UNTUK MANAJEMEN FIREWALL

Tugas Akhir

Disusun untuk memenuhi salah satu syarat dalam memperoleh gelar

Ahli Madya pada Program Studi Diploma III Teknik Informatika

Universitas Sebelas Maret



Disusun Oleh :

MUHAMAD AGUNG SABEKTI

M3115087

PROGRAM DIPLOMA III TEKNIK INFORMATIKA

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS SEBELAS MARET SURAKARTA

2018

HALAMAN PERSETUJUAN

**PEMBUATAN WEB INTERFACE SNORT
UNTUK MANAJEMEN FIREWALL**

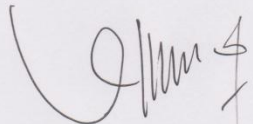
Disusun Oleh :

Muhamad Agung Sabekti

M3115087

Tugas Akhir ini telah disetujui untuk diujikan
di hadapan dewan penguji pada tanggal
.....20 Januari 2019.....

Pembimbing Utama

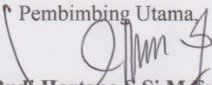


Rudi Hartono, S.Si, M.Eng

NIK. 1984122620160601

HALAMAN PENGESAHAN
PEMBUATAN WEB INTERFACE SNORT
UNTUK MANAJEMEN FIREWALL

Disusun Oleh :
Muhamad Agung Sabekti
M3115087

Pembimbing Utama

Rudi Hartono, S.Si, M.Eng
NIK. 1984122620160601


Tugas akhir ini telah diterima dan disahkan oleh dewan penguji tugas akhir
Program Diploma III Teknik Informatika
Pada hari *Senin* tanggal *28 Januari 2019*

Dewan Penguji :

1. Penguji 1 **RUDI HARTONO, SS.i, M.Eng.**
NIK. 1984122620160601
2. Penguji 2 **OVIDE DECROLY WISNU A.S.T., M.Eng.**
NIK. 1986050320130201
3. Penguji 3 **AGUS PURNOMO, S.SI, M.Eng.**
NIK. 1985030720160601



Disahkan Oleh,
Ketua Program Studi
D3 Teknik Informatika UNS


Abdul Aziz, S.Kom., M.Cs.
NIK. 198104132005011001



HALAMAN PERNYATAN

Dengan ini saya menyatakan bahwa dalam Laporan Tugas Akhir ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu 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.



INTISARI

MUHAMAD AGUNG SABEKTI. M3115087. PEMBUATAN WEB INTERFACE SNORT UNTUK MANAJEMEN FIREWALL. Diploma III Teknik Informatika dan Ilmu Pengetahuan Alam Universitas Sebelas Maret Surakarta, September 2018.

Secara umum snort merupakan salah satu aplikasi firewall yang dikonfigurasi dalam terminal linux, meliputi konfigurasi snort, input rule snort, dan hasil alert snort pada terminal linux. Untuk mempermudah monitoring alert di terminal linux, maka alert diimplementasikan pada email dan telegram, serta guna mempermudah dalam aktifitas input rule snort maka dibuatlah web interface snort.

Snort berjalan pada mode inline dengan menggunakan modul `daq_afpacket` dalam snort itu sendiri, dan untuk melakukan blok ketika terjadi serangan snort menggunakan firewall iptables. Alert diimplementasikan pada email menggunakan protokol smtp dan pada telegram menggunakan id dan api telegram.

Pembuatan web interface diharapkan dapat dengan mudah mengelola rule dan alert snort, serta dapat diaplikasikan dalam serangan yang diujikan.

Kata kunci: aplikasi firewall, alert, snort, web interface, rule snort, serangan, dan notifikasi.

ABSTRACT

MUHAMAD AGUNG SABEKTI. M3115087. WEB INTERFACE SNORT MAKING FOR FIREWALL MANAGEMENT. Diploma III Informatics Engineering and Natural Sciences Sebelas Maret University Surakarta, September 2018.

In general, snort is a firewall application that is configured in Linux terminals, including the implementation of snort, input snort rules, and snort warning results on Linux terminals. To monitor the linux warning alarm, the alerts are implemented on e-mail and telegram, as well as for input information in snort mode and then create a snort web interface.

Snort runs in inline mode using the daq_afpacket module in the snort itself, and to block makes snorting attacks using the iptables firewall. Warnings are implemented on e-mail using the smtp and telegram protocols using ID and telegram API.

It is hoped that the creation of a web interface can easily manage the rules and snort alerts, and can be applied in the appropriate attacks that have been tested.

Keywords: firewall application, alert, snort, web interface, snort rule, attack, and notification..



MOTTO

1. Bacalah dengan nama Tuhanmu yang menciptakan (QS. Al – Alaq ayat 1)
2. Menuntut ilmu adalah kewajiban bagi setiap Muslim. (HR. Ibnu Majah)
3. Sesungguhnya jika kamu bersyukur, pasti Kami akan menambah (nikmat) kepadamu. (QS. Ibrahim ayat 7)
4. Janganlah kamu bersikap lemah (QS. Ali Imran ayat 139)
5. Allah ta'ala tidak membebani seseorang itu melainkan sesuai dengan kesanggupannya. (QS. Al - Baqarah ayat 286)
6. Sesungguhnya sesudah kesulitan itu ada kemudahan (QS. Al-Insyirah ayat 6)
7. Sesungguhnya kami adalah kepunyaan Allah dan kepada Allah jugalah kami kembali (QS. Al-Baqarah ayat 156)
8. Kesederhanaan yang paling bernilai adalah kebaikan.

HALAMAN PERSEMBAHAN

Tugas Akhir ini penulis persembahkan kepada :

1. Allah Subhanahu Wa Ta'ala yang telah memudahkan penulis dalam memahami setiap ilmu baik ilmu perkuliahan ataupun di luar perkuliahan yang disampaikan oleh bapak/ibu dosen dan pemateri yang lain.
2. Bapak Widodo (alm) dan Ibu Sarmiatun sebagai orang tua penulis yang telah mengizinkan penulis untuk kuliah di Universitas Sebelas Maret dan selalu mendoakan yang terbaik bagi penulis.
3. Sulaiman Dwi Nugroho, Anisa Nur Afifah beserta anggota keluarga penulis yang telah mendukung penulis dalam melaksanakan perkuliahan.
4. Teman-teman penulis di kampus terutama SKI FMIPA UNS, Relawan Lazis UNS, Muhammad Faisal dan teman-teman TI 2015 yang telah memberikan ilmu dan pengalaman yang sangat banyak yang tidak akan penulis lupakan.
5. Rekan Kerja Solonet & Sambeng Crew yang juga kebersamai dan mendukung penyusunan laporan penulis.

KATA PENGANTAR

Puji syukur Alhamdulillah kepada Allah Subhanahu Wa Ta'ala yang telah melimpahkan nikmat dan rahmat yang tak terhitung banyaknya sehingga penulis dapat menyelesaikan Tugas Akhir dengan judul “Pembuatan Web Interfaces Snort untuk Manajemen Firewall”. Laporan Tugas Akhir ini disusun untuk memenuhi salah satu syarat untuk memperoleh gelar Ahli Madya (A.Md) pada Program Studi Diploma III Teknik Informatika Universitas Negeri Sebelas Maret Surakarta.

Dalam melakukan penelitian, pengerjaan, dan penyusunan laporan Tugas Akhir ini penulis telah mendapatkan banyak dukungan dan bantuan dari berbagai pihak. Penulis mengucapkan terima kasih kepada :

1. Abdul Aziz, S.Kom, M.Cs. selaku Ketua Program Studi Diploma III Teknik Informatika UNS.
2. Rudi Hartono, S.Si, M.Eng. selaku dosen pembimbing yang telah memberikan saran dan masukan, serta membimbing penulis dalam pengerjaan tugas akhir.
4. Keluarga dan teman-teman yang penulis sayangi

Penulis meyakini bahwa masih banyak kekurangan dalam penyusunan laporan ini. Maka dari itu, penulis mohon kritik dan saran yang membangun untuk memperbaiki laporan yang penulis susun ini.

Semoga laporan Tugas Akhir ini dapat bermanfaat bagi semua pihak, terutama bagi mahasiswa DIII Teknik Informatika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Sebelas Maret.

Surakarta, Desember 2018

Muhamad Agung Sabekti

DAFTAR ISI

HALAMAN PERSETUJUAN.....	Error! Bookmark not defined.
HALAMAN PENGESAHAN.....	Error! Bookmark not defined.
HALAMAN PERNYATAN	iv
INTISARI.....	v
ABSTRACT.....	vi
MOTTO	vii
HALAMAN PERSEMBAHAN	viii
KATA PENGANTAR	ix
DAFTAR ISI.....	1
DAFTAR TABEL.....	4
DAFTAR GAMBAR	5
BAB I PENDAHULUAN.....	6
1.1. Latar Belakang	6
1.2. Rumusan Masalah	6
1.3. Tujuan Penelitian.....	7
1.4. Manfaat Penelitian.....	7
1.5. Batasan Masalah.....	7
1.6. Metodologi Penelitian	7
1.7. Sistematika Penulisan.....	9
BAB II TINJAUAN PUSTAKA DAN LANDASAN TEORI	11
2.1. Tinjauan Pustaka	11
2.2. Landasan Teori	12
2.2.1 Snort	12
2.2.2 Mode Snort.....	13
2.2.3 Perintah Snort.....	14
2.2.4 Rule Snort	18
2.2.5 Protokol.....	19

2.2.6	Protokol SMTP	22
2.2.7	Keamanan Jaringan	22
2.2.9	Prinsip Keamanan Jaringan.....	23
2.2.10	Jenis-Jenis Serangan Terhadap Keamanan Jaringan.....	23
2.2.11	Firewall	27
2.2.15	MySQL database.....	29
2.2.16	PHP File System	30
2.2.17	<i>Upstart</i>	33
2.2.18	Log Notifikasi Email dan Telegram.....	33
BAB III ANALISIS DAN RANCANGAN SISTEM.....		34
3.1.	Deskripsi Data	34
3.2.	Deskripsi Umum Sistem.....	34
3.3.	Diagram Alur Snort	36
3.4.	Alur Notifikasi Email	37
3.5.	Alur Notifikasi Telegram	38
3.6.	Alat dan Bahan	41
3.6.1.	Perangkat Keras	41
3.6.2.	Perangkat Lunak.....	42
3.7.	Perancangan Sistem.....	43
3.7.1.	Desain Interface Halaman Web Login	43
3.7.2.	Desain Interface Dashboard Admin Web	44
3.7.3.	Desain Interface Tambah Rule Web	45
3.7.4.	Desain Interface Edit Rule Di Web.....	46
3.7.5.	Desain Interface di Email.....	47
3.7.6.	Desain Interface di Telegram	48
3.8.	Skenario Pengujian.....	49
BAB IV IMPLEMENTASI DAN PENGUJIAN.....		50
4.1.	Implementasi Sistem	50

4.1.1.	Konfigurasi IP Address PC Router	50
4.1.2.	Konfigurasi IP Address PC Tester	50
4.1.3.	Konfigurasi IP Address Server.....	51
4.1.4.	Konfigurasi Snort IPS	51
4.1.5.	Hasil dan Laporan Web Snort.....	53
4.2.	Pengujian Sistem	60
4.2.1.	Skenario Port Scanning	60
4.2.2.	Skenario FTP Brute Force.....	61
4.2.3.	Skenario SSH Brute Force	62
4.2.4.	Skenario Ddos Attack.	62
4.2.5.	Pengujian Notifikasi.....	64
4.2.6.	Analisa Hasil Pengujian	65
4.2.7.	Kesimpulan Pengujian	65
BAB V KESIMPULAN DAN SARAN.....		66
5.1.	Kesimpulan.....	66
5.2.	Saran	66
DAFTAR PUSTAKA		67

DAFTAR TABEL

Tabel 2.3. Membaca File.....	31
Tabel 2.4. Menulis kedalam File.....	31
Tabel 2.5. Menambahkan File.....	32
Tabel 2.6. Membuat File Baru	33
Tabel 4.1. Konfigurasi IP Address PC Router	50
Tabel 4.2. Konfigurasi IP Address PC Tester	50
Tabel 4.3. Konfigurasi IP Address PC Server.....	51
Tabel 4.4. Data Log serangan Ddos	63
Tabel 4.6. Hasil Pengujian.	65



DAFTAR GAMBAR

Gambar 2.1. Bagian Rule Snort	18
Gambar 3.1. Gambaran Umum Sistem.	35
Gambar 3.2. Topologi Jaringan.....	35
Gambar 3.3. Diagram Alur Snort.....	36
Gambar 3.4. Alur Notifikasi Email	38
Gambar 3.5. Alur Noifikasi Telegram.	39
Gambar 3.6. Desain Interface Halaman Web Login.....	44
Gambar 3.7. Interface Dashboard Admin Web.....	45
Gambar 3.8. Interface Tambah Rule Web.....	46
Gambar 3.9. Interface Edit Rule.....	47
Gambar 3.10. Desain Interface di Email.....	48
Gambar 3.11. Desain Interface di Telegram.....	49
Gambar 4.1. Implementasi Halaman Login.....	54
Gambar 4.2. Implementasi Halaman Dashboard.....	54
Gambar 4.3. Implementasi Halaman Daftar Rule.....	55
Gambar 4.4. Implementasi Halaman Tambah Rule.....	56
Gambar 4.5. Implementasi Halaman Edit Rule.....	56
Gambar 4.6. Respon <i>BotFather</i>	57
Gambar 4.7. API Telegram.....	57
Gambar 4.8. Scanning Port sebelum rule aktif.....	60
Gambar 4.9. Scanning Port setelah rule aktif.....	61
Gambar 4.10. Pengujian Ftp attack.....	61
Gambar 4.11. Pengujian SSH Brute Force.....	62
Gambar 4.12. <i>Ddos Syn Attack</i>	62
Gambar 4.13. Indikasi ketika serangan <i>Ddos</i> berjalan.....	63
Gambar 4.14. Notifikasi Email.....	64
Gambar 4.15. Notifikasi Telegram.....	64