

**IMPLEMENTASI PENGAMANAN OWNCLOUD
PADA PT. KEBAB KINGS INDONESIA MENGGUNAKAN
SNORT TERHADAP SERANGAN SYN FLOOD**

SKRIPSI



Oleh:

RIZKY INDRASUKMA RAMADHAN

1234010153

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN"
JAWA TIMUR**

2019

HALAMAN PENGESAHAN

Judul : Implementasi Pengamanan Owncloud Pada PT. Kebab Kings Indonesia Menggunakan Snort Terhadap Serangan SYN Flood
Oleh : Rizky Indrasukma Ramadhan
NPM : 1234010153


Telah Diseminarkan Dalam Ujian Skripsi Pada :
Hari Jum'at Tanggal 17 Mei 2019

Menyetujui

Dosen Pembimbing 1

Dosen Penguji 1

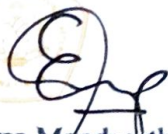

Fawwaz Ali Akbar, S.Kom., M.Kom.
NIP. 19920317201 8031002


Mohammad Idhom, SP., S.Kom., MT
NPT. 3 8303 10 0285 1

Dosen Pembimbing 2

Dosen Penguji 2


Eka Prakarsa Mandyartha, S.T., M.Kom.
NIP. 19880525201 8031001


Eka Prakarsa Mandyartha, S.T., M.Kom.
NIP. 19880525201 8031001


Dosen Penguji 3

Mengetahui

Koordinator Program Studi
Teknik Informatika

Dekan
Fakultas Ilmu Komputer


Dr. Ir. Ni Ketut Sari, MT.
NIP. 19650731 199203 2 001


Budi Nugroho, S.Kom., M.Kom.
NPT. 3 8009 05 0205 1

SURAT PERNYATAAN ANTI PLAGIAT

Saya, mahasiswa Teknik Informatika UPN “Veteran” Jawa Timur, yang bertandatangan di bawah ini.

Nama : RIZKY INDRASUKMA RAMADHAN

NPM : 1234010153

Menyatakan bahwa Judul Skripsi/ Tugas Akhir yang Saya ajukan dan akan dikerjakan, yang berjudul:

IMPLEMENTASI PENGAMANAN OWNCLOUD PADA PT. KEBAB KINGS INDONESIA
MENGUNAKAN SNORT TERHADAP SERANGAN SYN FLOOD

Bukan merupakan plagiat dari Skripsi/ Tugas Akhir/ Penelitian orang lain dan juga bukan merupakan produk dan atau *software* yang saya beli dari pihak lain. Saya juga menyatakan bahwa Skripsi/ Tugas Akhir ini adalah pekerjaan Saya sendiri, kecuali yang dinyatakan dalam Daftar Pustaka dan tidak pernah diajukan untuk syarat memperoleh gelar di UPN “Veteran” Jawa Timur maupun di institusi pendidikan lain.

Jika ternyata di kemudian hari pernyataan ini terbukti tidak benar, maka Saya siap menerima segala konsekuensinya.

Surabaya, 27 Mei 2019

Hormat Saya,



RIZKY INDRASUKMA RAMADHAN

NPM. 1234010153

IMPLEMENTASI PENGAMANAN OWNCLOUD PADA PT. KEBAB KINGS INDONESIA MENGGUNAKAN SNORT TERHADAP SERANGAN SYN FLOOD

DOSEN PEMBIMBING 1 : FAWWAZ ALI AKBAR, S.KOM, M.KOM

DOSEN PEMBIMBING 2 : EKA PRAKARSA MANDYARTHA, S.T., M.KOM

PENYUSUN : RIZKY INDRASUKMA RAMADHAN

ABSTRAK

Penelitian ini adalah sebuah penelitian studi kasus yang dilakukan disebuah perusahaan bernama PT. Kebab Kings Indonesia yang bergerak di bidang kuliner dan penyedia bahan baku kebab yang berlokasi di Surabaya. Tujuan dari penelitian ini adalah membuat server *cloud computing* yang bersifat *hybrid cloud* dan dipadukan dengan *tools Intrusion Detection System* untuk mendeteksi serangan terhadap server.

Penulis melakukan pembuatan server *cloud computing* berbasis *platform* dengan menggunakan perangkat lunak *Owncloud* dan melakukan pengamanan terhadap server *cloud computing* tersebut dengan menggunakan *Snort* sebagai *tools intrusion detection system* berbasis *network* untuk mendeteksi adanya intrusi pada jaringan server.

Penulis melakukan instalasi *Owncloud* dan mengkonfigurasi fitur *VPN* melalui *Ngrok* untuk membuat server *Owncloud* dapat diakses melalui internet tanpa menggunakan *ip public*. Memberikan keamanan terhadap server *Owncloud* dengan menginstalasi *Snort* serta mengkonfigurasi *Snort* untuk mendeteksi serangan *SYN Flood*. Percobaan intrusi dilakukan dengan cara melakukan percobaan serangan *SYN Flood* kedalam server.

Hasil dari penelitian ini menyatakan bahwa *Snort* sebagai *Network Intrusion Detection System* mampu mendeteksi serangan yang bersifat *network* seperti serangan *SYN Flood*, *Ping of Death*, *DDoS* dan lain-lain serangan bersifat *network*. Namun, *Snort* juga memiliki kekurangan karena tidak mampu mencegah adanya serangan yang terjadi pada jaringan sehingga membutuhkan modul tambahan untuk pencegahan serangan terhadap jaringan pada server.

Kata kunci : *Cloud Computing, Intrusion Detection System, Owncloud, Snort, VPN, Ngrok.*

KATA PENGANTAR

Syukur Alhamdulillah penulis panjatkan kehadirat Allah SWT yang telah memberikan rahmat serta hidayah-Nya sehingga penyusunan Laporan Skripsi ini dapat diselesaikan.

Laporan Skripsi ini disusun untuk memenuhi syarat dalam memperoleh gelar sarjana komputer, program studi Teknik Informatika. Judul yang diambil dalam penulisan Skripsi ini adalah :

**“IMPLEMENTASI PENGAMANAN OWNCLOUD PADA PT. KEBAB
KINGS INDONESIA MENGGUNAKAN SNORT TERHADAP
SERANGAN SYN FLOOD”**

Penulis menyadari bahwa penulisan Laporan Skripsi ini masih belum sempurna. Oleh karena itu, saran dan kritik yang membangun akan penulis terima dengan senang hati.

Akhir kata semoga Laporan Skripsi ini dapat memberikan manfaat bagi para mahasiswa khususnya dan pengetahuan pada umumnya.

Surabaya, 14 Mei 2019

Penulis

UCAPAN TERIMA KASIH

Selama melaksanakan pengerjaan tugas akhir dan dalam menyelesaikan laporan skripsi ini, penulis telah banyak menerima bimbingan, pengarahan, petunjuk dan saran, serta fasilitas yang membantu hingga akhir dari penulisan laporan ini. Untuk itu penulis menyampaikan ucapan terimakasih yang sebesar - besarnya kepada :

1. Rasa syukur dan terimakasih kepada Allah SWT atas segala berkah, rahmat dan hidayah yang diberikan kepada penulis sehingga penulis dapat menyelesaikan penulisan skripsi ini.
2. Kedua orang tua dan kakak saya yang telah memberikan doa, kasih sayang, serta semangat.
3. Ibu Dr. Ir. Ni Ketut Sari, MT selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jawa Timur.
4. Bapak Budi Nugroho, S.Kom, M.Kom selaku Ketua Jurusan Teknik Informatika Universitas Pembangunan Nasional “Veteran” Jawa Timur.
5. Bapak Fawwaz Ali Akbar, S.Kom, M.Kom, selaku Dosen Pembimbing pertama skripsi yang telah membimbing penulis selama pelaksanaan dan penyusunan laporan skripsi.

6. Bapak Eka Prakarsa Mandyartha, S.T., M.Kom, selaku Dosen Pembimbing kedua skripsi yang telah membimbing penulis selama pelaksanaan dan penyusunan laporan skripsi.
7. Bapak Hendra Maulana, S.Kom, M.Kom selaku Koordinator Tugas Akhir / PIA Universitas Pembangunan Nasional “Veteran” Jawa Timur.
8. Aya Sophia Wigneswara, terima kasih tak terhingga telah menemani penulis waktu suka dan duka, menemani penulis dari awal sebelum seminar hingga penulisan skripsi ini selesai. Terima kasih untuk segala bantuan, arahan dan motivasinya agar penulis menjadi dewasa.
9. An Say Aryanto, Mochammad Reza Fadillah, Andika Permana, Adi Hassby, Arief Rialdy, dan Fajar Sudiono atas semua support yang diberikan kepada penulis. Terima kasih sudah membuat penulis mendapat keluarga baru diluar sana. Maafkan jika penulis selalu merepotkan dan terima kasih atas semua motivasi yang diberi.
10. Muchammad Aziz Al Kautsar dan Wahyu Tanoto, terima kasih telah menjadi teman bermain selama ini dan juga telah mensupport penulis agar cepat selesai dalam pengerjaan skripsi.
11. Teman - teman Teknik Informatika UPN “Veteran” Jawa Timur tidak bisa penulis sebutkan satu persatu.

DAFTAR ISI

ABSTRAK	i
KATA PENGANTAR.....	ii
UCAPAN TERIMA KASIH.....	ii
DAFTAR ISI.....	v
DAFTAR GAMBAR.....	ix
DAFTAR TABEL.....	xii
DAFTAR LAMPIRAN	xiii
BAB I PENDAHULUAN	1
1.1. Latar Belakang.....	1
1.2. Rumusan Masalah	2
1.3. Batasan Masalah.....	3
1.4. Tujuan.....	3
1.5. Manfaat.....	4
1.6. Sistematika Penulisan.....	5
BAB II TINJAUAN PUSTAKA.....	7
2.1. Penelitian Terdahulu.....	7
2.2. Dasar Teori.....	8

2.2.1. Cloud Computing.....	8
2.2.2. Ubuntu.....	10
2.2.3. Owncloud	15
2.2.4. MySQL.....	16
2.2.5. VPN (<i>Virtual Private Network</i>)	17
2.2.6. Ngrok.....	19
2.2.7. Snort	20
BAB III METODOLOGI PENELITIAN	21
3.1. Alur Penelitian.....	21
3.1.1. Studi Pustaka.....	22
3.1.2. Perancangan Sistem	22
3.1.3. Pengujian Sistem.....	22
3.1.4. Analisa Sistem.....	22
3.1.5. Kesimpulan	23
3.2. Rancangan Penelitian	23
3.2.1. Definisi Kebutuhan Sistem	23
3.2.2. Kebutuhan Sistem Perusahaan	24
3.2.3. Rancangan Jaringan	27
3.2.4. Rancangan Sistem	28

3.3.	Pengujian Sistem	32
3.3.1.	Skenario Percobaan Login	32
3.3.2.	Skenario Percobaan Serangan	33
3.4.	Analisa Sistem	33
BAB IV HASIL DAN PEMBAHASAN.....		35
4.1.	Instalasi Sistem.....	35
4.1.1.	Instalasi Owncloud.....	35
4.1.2.	Konfigurasi Ngrok	39
4.1.3.	Instalasi Sistem Snort.....	41
4.2.	Konfigurasi Sistem	46
4.2.1.	Konfigurasi Owncloud	47
4.2.2.	Konfigurasi Snort.....	49
4.3.	Implementasi Sistem Cloud.....	54
4.3.1.	Percobaan Login Owncloud.....	55
4.3.2.	Percobaan Serangan Syn Flood.....	57
4.3.3.	Pendeteksian Syn Flood	62
BAB V KESIMPULAN DAN SARAN		65
5.1.	Kesimpulan.....	65
5.2.	Saran.....	66

DAFTAR PUSTAKA..... 67

LAMPIRAN..... 69

DAFTAR GAMBAR

Gambar 2.1 <i>Tunneling</i> VPN di interkoneksi jaringan.....	18
Gambar 3.1 Alur Rancangan Penelitian.....	21
Gambar 3.2 Skema Database Lokal Perusahaan.....	25
Gambar 3.3 Skema Fungsi Cloud Pada Perusahaan	26
Gambar 3.4 Topologi Jaringan.....	27
Gambar 3.5 Alur Instalasi Owncloud.....	28
Gambar 3.6 Alur Instalasi Ngrok.....	29
Gambar 3.7 Alur Instalasi Snort.....	30
Gambar 3.8 Alur Sistem Secara Keseluruhan.....	31
Gambar 3.9 Skenario Percobaan Login	32
Gambar 3.10 Skenario Percobaan Serangan	33
Gambar 4.1 Instalasi Paket Apache2.	35
Gambar 4.2 Instalasi Paket MariaDB.....	36
Gambar 4.3 Proses <i>Download</i> Paket PHP.....	36
Gambar 4.4 Membuat database Owncloud.	37
Gambar 4.5 Proses Download Owncloud.....	37
Gambar 4.6 Proses pemindahan dan instalasi owncloud.	38

Gambar 4.7 Instalasi Owncloud Melalui Website	39
Gambar 4.8 Proses Download Ngrok.....	40
Gambar 4.9 Konfigurasi <i>Ngrok</i>	40
Gambar 4.10 Proses <i>Ngrok</i> berjalan.....	41
Gambar 4.11 Proses Instalasi Paket Tambahan Snort.....	42
Gambar 4.12 Proses Download dan Ekstrasi DAQ library Snort	42
Gambar 4.13 Proses Instalasi DAQ snort	43
Gambar 4.14 Proses Download Snort.	43
Gambar 4.15 Proses Instalasi Snort.	44
Gambar 4.16 Proses Konfigurasi Library Snort.....	44
Gambar 4.17 Membuat folder keperluan Snort.....	45
Gambar 4.18 Membuat file untuk mencatat rules.....	45
Gambar 4.19 Mengatur hak akses pada folder snort.....	45
Gambar 4.20 Proses memindahkan <i>file config</i> ke dalam snort	46
Gambar 4.21 Konfigurasi Owncloud	47
Gambar 4.22 Konfigurasi <i>Rules Apache2</i>	48
Gambar 4.23 Perintah untuk mematikan semua rule pada snort.....	49
Gambar 4.24 Konfigurasi IP server	49
Gambar 4.25 Konfigurasi Folder rules snort.....	50

Gambar 4.26 Perintah Mengaktifkan <i>local.rules</i>	51
Gambar 4.27 Validasi <i>Snort.conf</i>	51
Gambar 4.28 Validasi sukses	52
Gambar 4.29 Konfigurasi Rule deteksi Syn Flood	53
Gambar 4.30 Konfigurasi Snort Service	53
Gambar 4.31 Proses Menjalankan Snort Service.....	54
Gambar 4.32 Halaman Utama Owncloud.....	55
Gambar 4.33 Proses mengunggah file pada owncloud	55
Gambar 4.34 Proses mengunggah sukses	56
Gambar 4.35 Proses mengunggah sukses	56
Gambar 4.36 Percobaan serangan Syn Flood	57
Gambar 4.37 Grafik Efek Serangan Pada CPU dan RAM.....	58
Gambar 4.38 Grafik Efek Serangan pada Response Reply Server	60
Gambar 4.39 Rule untuk mendeteksi Syn Flood	63
Gambar 4.40 Proses Serangan Syn Flood.....	63
Gambar 4.41 Tampilan Alert pada snort.....	64

DAFTAR TABEL

Tabel 2.1 Penelitian Terdahulu	7
Tabel 4.1 Tabel Efek Serangan pada CPU dan RAM.....	58
Tabel 4.2 Tabel Efek Serangan pada Response Reply Server	60

DAFTAR LAMPIRAN

Lampiran 1. Aktivitas Serangan Syn Flood	69
Lampiran 2. Sistem Monitor Server	71
Lampiran 3. Response Reply Server	74