PERANCANGAN SISTEM DETEKSI DAN MITIGASI ICMP FLOOD BERBASIS SOFTWARE DEFINED NETWORK DAN SFLOW-RT DI STMIK AMIKOM YOGYAKARTA

SKRIPSI

disusun oleh

Rangga Warsito

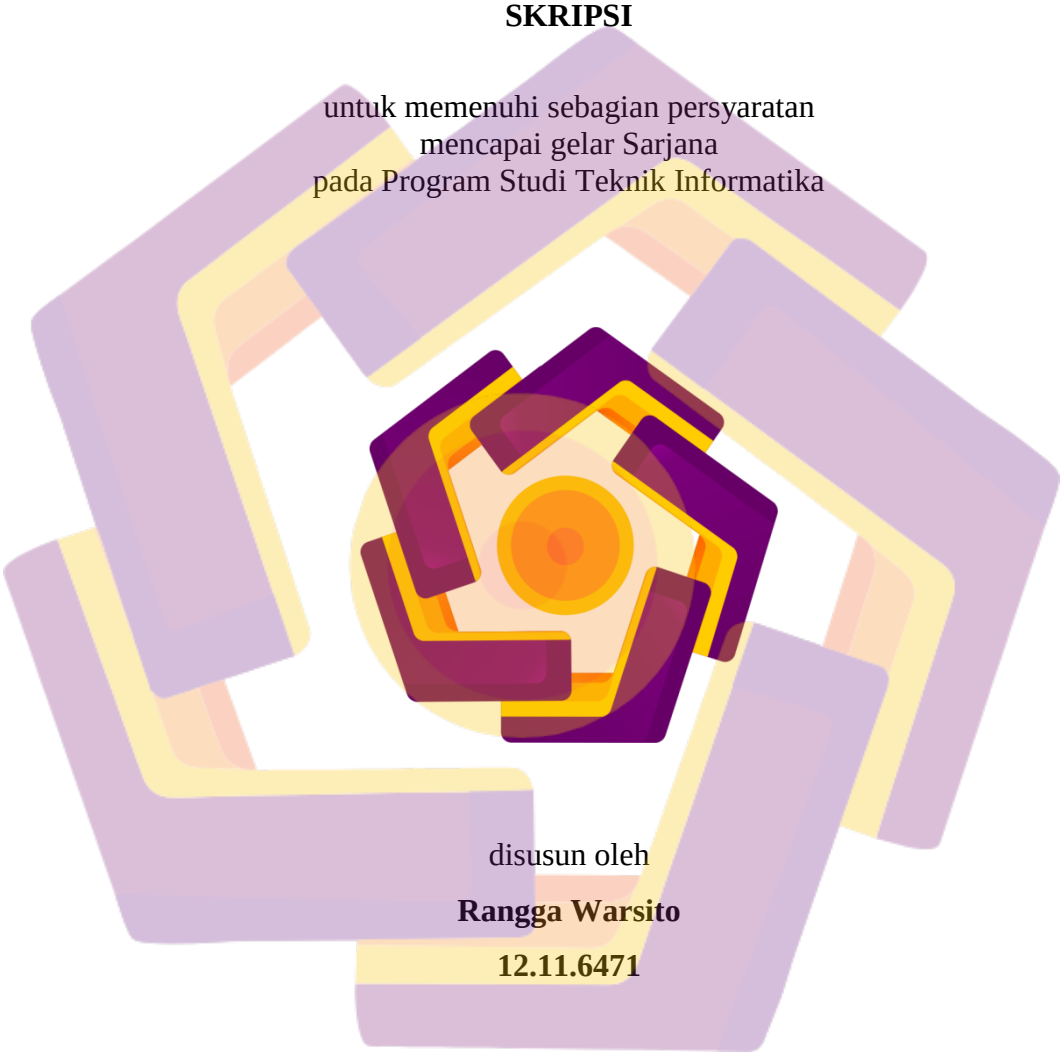
12.11.6471

PROGRAM SARJANA
PROGRAM STUDI TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2016

PERANCANGAN SISTEM DETEKSI DAN MITIGASI ICMP FLOOD BERBASIS SOFTWARE DEFINED NETWORK DAN SFLOW-RT DI STMIK AMIKOM YOGYAKARTA

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Teknik Informatika



disusun oleh

Rangga Warsito

12.11.6471

PROGRAM SARJANA
PROGRAM STUDI TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2016

PERSETUJUAN

SKRIPSI

PERANCANGAN SISTEM DETEKSI DAN MITIGASI ICMP FLOOD BERBASIS SOFTWARE DEFINED NETWORK DAN SFLOW-RT DI STMIK AMIKOM YOGYAKARTA

yang dipersiapkan dan disusun oleh

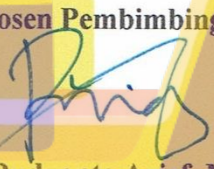
Rangga Warsito

12.11.6471

telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal 23 Juni 2016

Dosen Pembimbing,



M. Rudyanto Arief, M.T

NIK. 190302098

PENGESAHAN

SKRIPSI

PERANCANGAN SISTEM DETEKSI DAN MITIGASI ICMP FLOOD BERBASIS SOFTWARE DEFINED NETWORK DAN SFLOW-RT DI STMIK AMIKOM YOGYAKARTA

yang dipersiapkan dan disusun oleh

Rangga Warsito

12.11.6471

telah dipertahankan di depan Dewan Penguji
pada tanggal 23 Agustus 2016

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Hartatik, S.T., M.Cs **NIK. 190302232**	
Windha Mega Pradnya D, M.Kom **NIK. 190302185**	
M. Rudyanto Arief, M.T **NIK. 190302098**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 7 September 2016

KETUA STMIK AMIKOM YOGYAKARTA

Prof. Dr. M. Suyanto, M.M.
NIK. 190302001

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggung jawab saya pribadi.

Yogyakarta, 7 September 2016

Rangga Warsito

NIM. 12.11.6471

MOTTO

- Karena Sesungguhnya beserta kesulitan itu ada kemudahan **(Q.S Asy-Syarh, 94:5-6)**
- Gantungkan cita-cita mu setinggi langit! Bermimpilah setinggi langit. Jika engkau jatuh, engkau akan jatuh di antara bintang-bintang. **(Soekarno)**

PERSEMBAHAN

Puji dan syukur saya panjatkan kepada Allah SWT, karena atas limpahan rahmat dan karunia-Nya, saya dapat menyelesaikan skripsi ini sesuai dengan waktu yang saya harapkan. Skripsi ini saya persembahkan untuk:

1. Kedua orang tua tercinta, Ayah Wiji S. dan Ibu Hj. Rosmini untuk seluruh dukungan, kasih sayang, pengorbanan baik waktu, biaya dan tenaga, beserta semua hal yang sudah diberikan untuk saya, yang tidak dapat terhitung lagi jumlahnya. Semoga ini dapat menjadi langkah awal bagi saya untuk membuat Ayah dan Ibu bangga dan bahagia.
2. Kakanda Wiwin Yuniarti Ningrum yang selalu memberikan dukungan baik secara moril maupun materiil sampai saat ini.
3. Bapak dosen pembimbing, Bapak M. Rudyanto Arief, M.T, yang tidak lelah memberikan bimbingan, masukan, serta revisi demi kemajuan skripsi ini. Terima kasih sebanyak-banyaknya untuk Bapak.
4. Bapak Rikie Kartadie, S.T., M.Kom yang telah memberikan waktu dan tenaganya untuk membantu dalam menyelesaikan skripsi ini.
5. Tante, paman, sepupu, dan keponakan, keluarga besar di kabupaten Soppeng dan kota Makassar, yang selalu memberikan nasihat juga dukungannya, terima kasih banyak saya ucapkan untuk semuanya.
6. Sahabat dan keluarga Gorongan, Ikhwanur W, Bony Fasius G, Abdul Kholid, Yusuf Fikri R, Fathana Erlangga dan Fahmi Sahru Ramadhan yang selalu menghibur disaat-saat suntuk mengerjakan skripsi, terima kasih untuk kalian.

7. Terima kasih kepada Nurfani Abdillah yang sudah banyak memberikan bantuan dan motivasi dalam menyusun skripsi ini hingga selesai dengan lancar.
8. Keluarga besar Asrama Mahasiswa Sulawesi Selatan Wisma Sawerigading Yogyakarta yang telah menghiasi keseharian penulis selama tinggal di Yogyakarta.
9. Teman-teman S1-TI-11 yang sudah memberikan banyak kenangan dan pengalaman selama menjalani pendidikan. Terima kasih untuk kebersamaan kita selama ini, sukses untuk kita semua, aamiin.
10. Semua pihak yang sudah sangat membantu tersusunnya skripsi ini.

KATA PENGANTAR

Puji syukur Allah S.W.T atas segala karunia, rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan laporan skripsi dengan judul ***"Perancangan Sistem Deteksi Dan Mitigasi ICMP Flood berbasis Software Defined Network Dan sFlow-RT Di STMIK Amikom Yogyakarta".*** Laporan skripsi ini disusun sebagai syarat kelulusan program studi Strata-1 di Sekolah Tinggi Informatika dan Komputer "Amikom Yogyakarta" Jurusan Teknik Informatika.

Pada kesempatan ini penulis menyampaikan rasa hormat dan terima kasih kepada :

1. Bapak Prof. Dr. M. Suyanto, M.M selaku ketua STMIK AMIKOM Yogyakarta.
2. Bapak Sudarmawan, M.T selaku ketua Jurusan Teknik Informatika.
3. Bapak M. Rudyanto Arief, M.T selaku dosen pembimbing yang telah memberikan arahan, bimbingan, motivasi, waktu serta masukan yang sangat bermanfaat dalam penyusunan skripsi ini.
4. Bapak/Ibu dosen, staff serta karyawan STMIK Amikom Yogyakarta yang telah memberikan ilmu dan bantuan yang bermanfaat bagi penulis.
5. Bapak Drs. Asro Nasiri, M.Kom selaku Direktur dan Bapak Rahmat Agung S., A.Md selaku Manajer Infrastruktur Innovation Centre STMIK AMIKOM Yogyakarta yang telah memberikan kesempatan untuk penulis melakukan penelitian.

Penulis menyadari bahwa dalam penyusunan skripsi ini masih jauh dari sempurna karena keterbatasan juga minimnya pengalaman penulis. Walau demikian, penulis berharap laporan skripsi ini bermanfaat bagi pembacanya. Penulis dengan senang hati menerima kritik dan saran yang bersifat konstruktif dari para pembaca sekalian.

Akhir kata, semoga laporan skripsi ini dapat bermanfaat bagi penulis danpara pembaca.

Yogyakarta, 7 September 2016

Rangga Warsito

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

STMIK Amikom Yogyakarta merupakan institusi perguruan tinggi dibidang teknologi informasi yang mengimplementasikan beberapa *server* yang digunakan untuk melayani berbagai aktivitas akademik. Tidak adanya pembatasan dan terbukanya protokol ICMP (*Internet Control Message Protocol*) tentunya dapat dimanfaatkan untuk melakukan serangan ke *server* dengan teknik *ICMP flood* yang mengirimkan sejumlah paket ICMP dalam jumlah yang cukup besar ke komputer target.

Untuk dapat meningkatkan kinerja dalam memproteksi sebuah sistem terutama untuk memitigasi serangan *ICMP flood*, maka dapat digunakan teknologi *software defined network* dengan membangun suatu mekanisme mitigasi yang memanfaatkan *OpenFlow* dan *sFlow*.

Dengan pemanfaatan teknologi ini, serangan *ICMP flood* dapat dideteksi dan dimitigasi. Hal tersebut terbukti dari jumlah paket ICMP yang masuk ke *server* dapat berkurang secara signifikan yaitu menjadi 99 paket dibandingkan saat terjadi pengiriman *ICMP flood* yaitu 311.130,2 paket. Berdasarkan performa jaringan dalam hal ini *latency*, sistem keamanan yang digunakan juga dapat mengurangi nilai *latency* pada saat terjadi serangan dari 42,822 *ms* menjadi 8.807 *ms* untuk kondisi 30 *user*. Hal tersebut menunjukkan bahwa kondisi jaringan atau trafik yang terjadi saat serangan berhasil di blok oleh sistem yang telah dibuat.

Kata Kunci : *ICMP flood, software defined network, OpenFlow, sFlow*

ABSTRACT

STMIK Amikom Yogyakarta is a higher education institution in the field of information technology that implements some of the servers used to serve a variety of academic activities. The absence of restrictions and the opening of protocol ICMP (Internet Control Message Protocol) must be utilized to carry out the attack to the server with ICMP flood technique that sends a series of ICMP packets in large enough quantities to the target computer.

In order to improve performance in protecting a system mainly to mitigate the ICMP flood attacks, it can use a software defined network technology to build a mitigation mechanism that utilizes OpenFlow and sFlow.

With the use of this technology, ICMP flood attacks can be detected and mitigated. This is evident from the number of incoming ICMP packets to the server can be significantly reduced that to 99 packet than when delivery occurs ICMP flood is 311.130,2 packet. Based on the performance of network latency in this case, a security system that is used can also reduce the value of latency in the event of an attack from 42,822 ms becomes 8,807 ms to 30 user conditions. It shows that the network conditions or traffic that occurs when a successful attack on the block by a system that has been created.

Keywords: *ICMP flood, software defined network, OpenFlow, sFlow*