RANCANG BANGUN ANOMALY DETECTION SYSTEM BERBASIS NAÏVE BAYES PADA JARINGAN OPENFLOW

SKRIPSI

Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana Teknik

Nehemia Edbertus

14110210009

PROGRAM STUDI TEKNIK KOMPUTER

FAKULTAS TEKNIK DAN INFORMATIKA

UNIVERSITAS MULTIMEDIA NUSANTARA

TANGERANG

2018

HALAMAN PENGESAHAN SKRIPSI

RANCANG BANGUN ANOMALY DETECTION SYSTEM BERBASIS NAÏVE BAYES PADA JARINGAN OPENFLOW

Oleh

Nama	: Nehemia Edbertus
NIM	: 14110210009
Fakultas	: Teknik dan Informatika
Program Studi	: Teknik Komputer

Telah diujikan pada hari Selasa, 7 Agustus 2018 dan dinyatakan lulus dengan susunan Tim Penguji sebagai berikut,

Ketua Sidang

Dareen K. Halim, S.Kom., M.Eng.Sc.

Dosen Penguji

Dr. Hugeng, S.T., M.T.

Dosen Pembimbing I,

Samuel Hutagalung, M.T.I.

Dosen Pembimbing II,

Hargyo Tri Nugroho, S.Kom., M.Sc.

Disahkan oleh,

Ketua Program Studi Teknik Komputer,

Hargyo Tri Nugroho, S.Kom., M.Sc.

PERNYATAAN TIDAK MELAKUKAN PLAGIAT

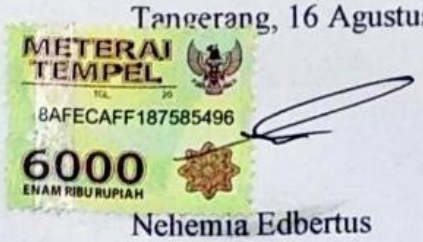
Dengan ini saya,

Nama	: Nehemia Edbertus
NIM	: 14110210009
Fakultas	: Teknik dan Informatika
Program Studi	: Teknik Komputer

Menyatakan bahwa skripsi yang berjudul "RANCANG BANGUN ANOMALY DETECTION SYSTEM BERBASIS NAÏVE BAYES PADA JARINGAN OPENFLOW" ini adalah karya ilmiah saya sendiri, bukan plagiat dari karya ilmiah yang ditulis oleh orang lain atau lembaga lain, dan semua karya ilmiah orang lain atau lembaga lain yang dirujuk dalam skripsi ini telah disebutkan sumber kutipannya serta dicantumkan di Daftar Pustaka.

Jika di kemudian hari terbukti ditemukan kecurangan / penyimpangan, baik dalam pelaksanaan skripsi maupun dalam penulisan laporan skripsi, saya bersedia menerima konsekuensi dinyatakan TIDAK LULUS untuk mata kuliah Skripsi yang telah saya tempuh.

Tangerang, 16 Agustus 2018



Nehemia Edbertus

KATA PENGANTAR

Puji syukur kepada Tuhan Yang Maha Esa yang selalu menyertai selama masa pengerjaan skripsi dan laporan skripsi berjudul "RANCANG BANGUN ANOMALY DETECTION SYSTEM BERBASIS NAÏVE BAYES PADA JARINGAN OPENFLOW" sehingga dapat diselesaikan dengan baik dan benar. Skripsi ini diajukan kepada Program Studi Teknik Komputer, Fakultas Teknik dan Informatika, Universitas Multimedia Nusantara.

Penyelesaian skripsi ini juga dibantu dan didukung oleh berbagai pihak, seperti teman-teman, dosen-dosen pembimbing, dan keluarga. Oleh karena itu, ucapan terima kasih yang sebesar-besarnya diucapkan kepada:

1. Dr. Ninok Leksono, selaku Rektor Universitas Multimedia Nusantara;
2. Hira Meidia, Ph. D., selaku Wakil Rektor Bidang Akademik serta sebagai Dekan Fakultas Teknik dan Informatika;
3. Ir. Andrey Andoko, M.Sc., selaku Wakil Rektor Bidang Administrasi Umum dan Keuangan;
4. Ika Yanuarti, S.E., MSF., selaku Wakil Rektor Bidang Kemahasiswaan;
5. Prof. Dr. Muliawati G. Siswanto, M.Eng.Sc., selaku Wakil Rektor Bidang Hubungan dan Kerjasama;
6. Hargyo Tri Nugroho, S.Kom., M.Sc., selaku dosen pembimbing dan Ketua Program Studi Teknik Komputer yang selalu mau membimbing, mendukung, serta memberikan solusi menghadapi

berbagai persoalan yang penulis temui selama proses penyelesaian skripsi;

7. Samuel Hutagalung, M.T.I., selaku dosen yang selalu memberikan dorongan, mendukung dan masukan yang sangat membantu dalam proses pengerjaan dan penulisan skripsi;
8. Kedua orang tua dan kakak yang selalu mendukung serta mendoakan selama proses pengerjaan skripsi;
9. Richard Alvianto sebagai teman seperjalanan menuju kampus yang rela mengantar pergi dan pulang selama penulis berkuliah;
10. Wira, Andrew, dan Nathan selaku kolega yang saling mengingatkan untuk mengerjakan skripsi selama semester 7 dan 8;
11. Michael, Aida, Bisma, Fanno dan Eriksen selaku rekan seperjuangan dalam menyelesaikan laporan skripsi di lab 508;
12. Farell yang telah menjadi motivasi saya untuk segera bertoga;
13. Seluruh rekan mahasiswa program studi Teknik Komputer, khususnya angkatan 2014 yang telah menyemangati penulis untuk menyelesaikan skripsi;
14. Boby dan Monica teman SMA yang menjadi teman curhat penulis meskipun terpaut jarak yang jauh;
15. Semua pihak yang tidak dapat disebutkan satu persatu, terima kasih atas segalanya.

Semoga skripsi ini dapat bermanfaat bagi pembaca, baik sebagai informasi maupun sumber inspirasi, terutama untuk mahasiswa Universitas Multimedia Nusantara dalam mengembangkan teknologi informasi dan komunikasi.

Tangerang, 16 Agustus 2018

Nehemia Edbertus

RANCANG BANGUN ANOMALY DETECTION SYSTEM BERBASIS NAÏVE BAYES PADA JARINGAN OPENFLOW

ABSTRAK

Anomaly Detection System adalah sebuah sistem untuk mendeteksi adanya serangan pada jaringan atau tidak. Salah satu jenis serangan jaringan yang masih umum dilancarkan adalah *Distributed Denial of Service* yang menyebabkan target tidak dapat menyediakan layanannya. Salah satu teknik mendeteksi serangan tersebut adalah dengan menggunakan *Gaussian Naïve Bayes Classifier* yang dapat mengklasifikasikan *traffic* jaringan dalam suatu *window* merupakan serangan atau *traffic* normal menggunakan acuan dari distribusi normal yang didapat dari hasil *training* menggunakan *dataset traffic* normal dan serangan. Penelitian ini merancang *Anomaly Detection System* berbasis *Naïve Bayes* untuk mendeteksi serangan *DDoS* berjenis *SYN Flood* pada jaringan OpenFlow menggunakan *switch Zodiac FX*. Sistem yang dikembangkan memanfaatkan protokol OpenFlow untuk membuat *flow rule* pada *flow table switch* mendeteksi dan memitigasi serangan *SYN Flood* secara *real-time*. Langkah mitigasi yang diterapkan oleh sistem adalah mengalihkan semua paket masuk ke *SYN Proxy* sehingga hanya *legitimate TCP packet* yang dapat mencapai server. Hasil pengujian menunjukkan sistem memiliki *bandwidth* sebesar 60Mbps saat dalam keadaan normal dan 5,03Mbps saat dalam serangan. Jumlah paket serangan terbanyak yang dapat mencapai *server* sebelum dialihkan menuju *SYN Proxy* diestimasi sebanyak 400 paket tanpa melihat jumlah paket serangan yang dikirim dan dengan asumsi *flow rule* dari *controller* langsung diterapkan.

Keyword : *Anomaly Detection System*, *Naïve Bayes*, Protokol OpenFlow, Zodiac FX, *SYN Proxy*

NAÏVE BAYES ANOMALY DETECTION SYSTEM DESIGN ON OPENFLOW NETWORK

ABSTRACT

Anomaly Detection System is used to detect attacks in the network. One of the generally launched attacks is Distributed Denial of Service that renders its target unable to provide its service. Gaussian Naïve Bayes Classifier is one out of several techniques used in detecting those attacks by classifying network traffic in a window as an attack or a normal traffic based on normal distribution previously calculated from normal and attack traffic datasets. This research designs a Naïve Bayes Anomaly Detection System focusing on SYN Flood Type DDoS attacks on OpenFlow Network using Zodiac FX as a switch. The developed system utilizes OpenFlow Protocol to apply flow rule in switch's flow table in order to detect and mitigate SYN Flood attacks in real-time. Applied mitigation procedure is to divert incoming packets into SYN Proxy so that only legitimate TCP packets are able to reach the server. The results show that the system has a bandwidth of up to 60Mbps under normal condition and 5,03Mbps under attack. Maximum malicious packets that could reach server before it is diverted to SYN Proxy is estimated to be 400 packets and not affected by the number of attacks, assuming that the flow rule sent by the controller are enacted immediately.

Keyword : Anomaly Detection System, Naïve Bayes, OpenFlow Protocol, Zodiac FX, SYN Proxy

DAFTAR ISI

HALAMAN PENGESAHAN SKRIPSI.....**Error! Bookmark not defined.**

PERNYATAAN TIDAK MELAKUKAN PLAGIAT ..... **Error! Bookmark not defined.**

KATA PENGANTAR iv

ABSTRAK vii

ABSTRACT viii

DAFTAR ISI ix

DAFTAR GAMBAR xi

DAFTAR TABEL xiii

BAB I PENDAHULUAN 1

1.1. Latar Belakang 1

1.2. Rumusan Masalah 3

1.3. Batasan Penelitian 3

1.4. Tujuan Penelitian 3

1.5. Manfaat Penelitian 4

BAB II TINJAUAN PUSTAKA 5

2.1. Denial of Service (DoS) 5

2.1.1. SYN Flood 8

2.2. OpenFlow Protocol 9

2.2.1. RYU Controller 10

2.3. Moving Average 10

2.3.1. Exponential Moving Average 10

2.4. Naïve Bayes Classifier 11

2.4.1. Gaussian Naïve Bayes 12

2.5. SYN Proxy 14

2.6. Penelitian Terdahulu 15

2.6.1. Implementasi Count-Min Sketch pada Anomaly Detection System Berbasis Naïve Bayes 16

2.6.2. Detection of DoS/DDoS attack against HTTP Servers using Naïve Bayesian 16

2.6.3. An Efficient DDoS Detection with Bloom Filter in SDN 17

2.6.4. Real-time detection of changes in network with OpenFlow based on NetFPGA implementation 17

BAB III METODE PENELITIAN.....19
3.1. Diagram Blok Arsitektur Sistem 19
3.1.1. Diagram Alur Paket Masuk.....21
3.1.2. Diagram Alur Buffer Fitur Paket 23
3.1.3. Diagram Alur Naïve Bayes Classifier.....25
3.1.4. Diagram Alur Exponential Moving Average 26
3.2. Instrumen Penelitian.....27
BAB IV IMPLEMENTASI DAN PENGUJIAN 28
4.1. Topologi Jaringan.....28
4.2. SYN Proxy.....29
4.3. Pengalihan Paket dengan OpenFlow 33
4.4. Hasil Mitigasi Anomaly Detection System 35
4.5. Pengujian Throughput Sistem 38
BAB V SIMPULAN DAN SARAN 41
5.1. Simpulan.....41
5.2. Saran 41
DAFTAR PUSTAKA 43
LAMPIRAN I FORMULIR BIMBINGAN SKRIPSI..... **Error! Bookmark not defined.**

DAFTAR GAMBAR

Gambar 1.1 Distribusi Serangan *DDoS* Berdasarkan Tipe Pada Q4 2017 [3].....2
Gambar 2.1 Skema *Volume-based DDoS attacks* dengan *botnet* [8].....6
Gambar 2.2 Skema *Volume-based DDoS attacks* dengan *cloud server* yang diretas [8].....7
Gambar 2.3 Skema TCP *Three-way Handshake* [8].....8
Gambar 2.4 Skema Serangan *SYN Flood* [8].....9
Gambar 2.5 Visualisasi *Exponential Moving Average* [12].....11
Gambar 2.6 Alur Komunikasi *SYN Proxy* Dalam Kondisi Normal.....14
Gambar 2.7 Alur Komunikasi *SYN Proxy* Dalam Kondisi Diserang.....15
Gambar 3.1 Diagram Blok *Anomaly Detection System*.....19
Gambar 3.2 Alur Paket Masuk pada *Traffic* Jaringan Normal.....19
Gambar 3.3 Alur Paket Masuk pada *Traffic* Jaringan Anomali.....20
Gambar 3.4 Flowchart Paket Masuk.....21
Gambar 3.5 Flowchart *Buffer* Fitur Paket.....23
Gambar 3.6 Diagram Alur *Naïve Bayes Classifier*.....25
Gambar 3.7 Diagram Alur *Exponential Moving Average*.....26
Gambar 4.1 Topologi Jaringan saat Pengujian.....28
Gambar 4.2 Konfigurasi *SYN Proxy* dengan firehol.....29
Gambar 4.3 Capture Wireshark pada *SYN Proxy* saat *SYN Flood* menggunakan random source ip.....29
Gambar 4.4 Capture Wireshark pada *client* saat *SYN Flood* menggunakan random source ip.....30
Gambar 4.5 Capture Wireshark pada *SYN Proxy* saat *SYN Flood* menggunakan random source ip.....30
Gambar 4.6 Capture Wireshark pada *client*2 saat *SYN Flood* menggunakan spoofed source ip.....30
Gambar 4.7 Capture Wireshark pada *client*1 saat *SYN Flood* menggunakan spoofed source ip.....31
Gambar 4.8 Capture Wireshark pada *SYN Proxy* saat *SYN Flood* menggunakan spoofed source ip.....31
Gambar 4.9 Capture Wireshark pada *client* saat *legitimate connection*.....31
Gambar 4.10 Capture Wireshark pada *interface* ens33 *SYN Proxy* saat menerima *legitimate connection*.....32
Gambar 4.11 Capture Wireshark pada *interface* ens38 *SYN Proxy* saat menerima *legitimate connection*.....32
Gambar 4.12 *Flow Table* switch dalam keadaan normal.....33
Gambar 4.13 Capture Wireshark pada *client* dalam keadaan normal.....33
Gambar 4.14 Capture Wireshark pada interface eth0 *server* dalam keadaan normal.....34
Gambar 4.15 *Flow Table* switch dalam kedaan *under attack*.....34
Gambar 4.16 Capture Wireshark pada *client* saat serangan.....35
Gambar 4.17 Capture Wireshark pada interface eth0 *server* saat serangan.....35
Gambar 4.18 Capture Wireshark pada interface ens33 *SYN Proxy* saat serangan.35

Gambar 4.19 Capture *SYN Flood* yang diterima *server*.....36
Gambar 4.20 Capture *SYN Flood* yang dialihkan ke *SYN Proxy*.....36
Gambar 4.21 Hasil iperf *client* dalam keadaan normal.....38
Gambar 4 22 Hasil iperf *server* dalam keadaan normal.....38
Gambar 4.23 Hasil iperf *client* saat dalam keadaan *under attack*.....39
Gambar 4.24 Hasil iperf *server* saat dalam keadaan *under attack*.....39

DAFTAR TABEL

Tabel 4.1 Tabel Kalkulasi *Exponential Moving Average* 37