Analisis Performansi IDS Snort dan IDS Suricata dengan *Many-Core Processor* pada *Virtual Machine* Terhadap Serangan *Dos / DDoS*

TESIS

Oleh

Dede Fadhilah

55418110007

PROGRAM MAGISTER TEKNIK ELEKTRO

PROGRAM PASCASARJANA

UNIVERSITAS MERCU BUANA

2020

Analisis Performansi IDS Snort dan IDS Suricata dengan *Many-Core Processor* pada *Virtual Machine* Terhadap Serangan *DoS / DDoS*

TESIS

Diajukan sebagai Salah Satu Syarat untuk Menyelesaikan Program Pascasarjana Program Magister Teknik Elektro

Oleh

Dede Fadhilah

55418110007

PROGRAM MAGISTER TEKNIK ELEKTRO

PROGRAM PASCASARJANA

UNIVERSITAS MERCU BUANA

ABSTRAK

Pesatnya perkembangan teknologi memungkinkan sebuah *physical machine* dapat diubah menjadi sebuah *virtual machine*, yang dapat mengoperasikan beberapa sistem operasi dan dijalankan secara bersamaan serta dapat terhubung ke internet**.** Serangan DoS/DDoS merupakan serangan *cyber* yang dapat mengancam sektor telekomunikasi karena serangan ini menyebabkan layanan menjadi terganggu dan sulit diakses. Terdapat beberapa aplikasi untuk melakukan monitoring dari aktivitas abnormal pada jaringan, diantaranya IDS Snort dan IDS Suricata. Dari penelitian sebelumnya, IDS Suricata lebih unggul daripada IDS Snort versi 2 dikarenakan IDS Suricata sudah mendukung *multi-threading*, sedangkan IDS Snort versi 2 hanya mendukung *single threading*.

Tesis ini bertujuan untuk menguji IDS Snort versi 3.0 yang sudah mendukung *multi-threading* dengan IDS Suricata. Penelitian ini dijalankan pada mesin *virtual* dengan pengaturan 1 *core*, 2 *core*, dan 4 *core processor* terhadap penggunaan CPU, *memory*, dan *capture* paket serangan pada IDS Snort dan IDS Suricata. Skenario serangan dibagi dalam 2 bagian yaitu skenario serangan DoS menggunakan 1 *physical* komputer dan skenario serangan DDoS menggunakan 5 *physical* komputer.

Berdasarkan pengujian keseluruhan, hasil umumnya IDS Snort lebih baik daripada IDS Suricata. Dengan hasil ketika penggunaan maksimum 4 *core processor*, penggunaan CPU stabil pada 55% - 58%, dan *memory* maksimum 3.000 MB serta dapat mendeteksi serangan DoS dengan jumlah 27.034.751 paket, dan serangan DDoS dengan jumlah 36.919.395 paket. Berbeda hasil yang diperoleh oleh IDS Suricata, dimana penggunaan CPU lebih baik dengan penggunaan hanya 10% - 40%, dan *memory* maksimum 1.800 MB, namun hasil pendeteksian serangan DoS lebih kecil dengan jumlah 3.671.305 paket, dan serangan DDoS dengan jumlah 7.619.317 paket pada uji coba serangan *TCP Flood.*

Kata Kunci: IDS, Intrusion Detection System, Snort, Suricata, DoS, DDoS

ABSTRACT

The rapid development of technology makes it possible for a physical machine to be converted into a virtual machine, which can operate multiple operating systems that is running simultaneously and can be connected to the internet. DoS/DDoS attacks are cyber attacks that can threaten the telecommunications sector because these attacks cause services to be disrupted and be difficult to access. There are several software tools for monitoring abnormal activities on the network, such as IDS Snort and IDS Suricata. From previous studies, IDS Suricata is superior to IDS Snort version 2 because IDS Suricata already supports multi-threading, while IDS Snort version 2 still only supports single-threading.

This thesis aims to conduct tests on IDS Snort version 3.0 which already supports multi-threading and IDS Suricata. This research was carried out on a virtual machine with 1 core, 2 core, and 4 core processor settings for CPU, memory, and capture packet attacks on IDS Snort and IDS Suricata. The attack scenario is divided into 2 parts, the DoS attack scenario using 1 physical computer and the DDoS attack scenario using 5 physical computers.

Based on overall testing, the results are generally IDS Snort better than IDS Suricata. With the results when using a maximum of 4 core processor, CPU usage is stable at 55% - 58%, and a maximum memory of 3,000 MB and can detect DoS attacks with 27,034,751 packets, and DDoS attacks with 36,919,395 packets. Different results obtained by IDS Suricata, where CPU usage is better with only 10% - 40% usage, and a maximum memory of 1,800 MB, but the results of detecting DoS attacks are smaller with 3,671,305 packets, and DDoS attacks with a total of 7,619,317 packet on a TCP Flood attack test.

Keywords: IDS, Intrusion Detection System, Snort, Suricata, DoS, DDoS

PENGESAHAN TESIS

Judul	:	Analisis Performansi IDS Snort dan IDS Suricata dengan *Many-Core Processor* pada *Virtual Machine* terhadap Serangan DoS / DDoS
Nama	:	Dede Fadhilah
NIM	:	55418110007
Program Studi	:	Pascasarjana Program Magister Teknik Elektro
Konsentrasi	:	Manajemen Telekomunikasi
Tanggal	:	04 Agustus 2020

Pembimbing :

Dr. Marza Ihsan Marzuki, MT

Mengesahkan :

Direktur Pascasarjana	Ketua Program Studi
Prof. Dr. -Ing. Mudrik Alaydrus	Prof. Dr. Andi Adriansyah, M.Eng

PERNYATAAN *SIMILARITY CHECK*

Saya yang bertanda tangan di bawah ini menyatakan, bahwa karya ilmiah yang ditulis oleh:

Nama	: Dede Fadhilah
NIM	: 55418110007
Program Studi	: Magister Teknik Elektro

dengan judul *"Performance Analysis of IDS Snort and IDS Suricata with Many-Core Processor in Virtual Machines Against DoS/DDoS Attacks"*, telah dilakukan pengecekan *similarity* dengan sistem Turnitin pada tanggal 10 Agustus 2020, didapatkan nilai persentase sebesar 18%.

Jakarta, 10 Agustus 2020
Administrator Turnitin

Arie Pangudi, A.Md

PERNYATAAN

Saya yang bertandatangan di bawah ini menyatakan yang sebenar-benarnya bahwa seluruh tulisan dan pernyataan dalam Tesis ini :

Judul	: Analisis Performansi IDS Snort dan IDS Suricata dengan *Many-Core Processor* pada *Virtual Machine* Terhadap Serangan Dos / DDoS
Nama	: Dede Fadhilah
Nim	: 55418110007
Program	: Magister Teknik Elektro
Konsentrasi	: Manajemen Telekomunikasi

Merupakan hasil studi pustaka, penelitian lapangan, dan karya saya sendiri dengan bimbingan Pembimbing dengan surat Keputusan Ketua Program Studi Magister Teknik Elektro Universitas Mercu Buana tertanggal 20 Agustus 2019 dengan Nomor: 09-4/630/F-STT/VIII/2019/.

Tesis ini belum pernah diajukan untuk memperoleh gelar Magister pada program sejenis di perguruan tinggi lain. Semua informasi, data, dan hasil pengolahan yang digunakan, telah dinyatakan secara jelas sumbernya dan dapat diperiksa kebenarannya.

Jakarta, 06 Juli 2020

Dede Fadhilah

KATA PENGANTAR

Dengan nama Allah yang Maha Pengasih lagi Maha Penyayang. Alhamdulillah, Puji syukur atas segala Rahmat dan Karunia-Nya, disertai do'a restu keluarga, akhirnya dapat menyelesaikan tesis ini.

Penulis bersyukur, bahwa setelah berupaya keras, berdo'a dan bertawakal kepada Allah SWT serta atas bantuan dan dukungan dari semua pihak, akhirnya dapat menyelesaikan pembuatan dan penulisan tesis ini dengan baik dan sesuai dengan waktu yang telah ditentukan. Pada kesempatan ini, penulis ingin mengucapkan terima kasih kepada:

1. Bapak Dr. Marza Ihsan Marzuki, MT, selaku Dosen Pembimbing yang telah banyak memberikan masukan dan dorongan dalam pembuatan dan penulisan tesis ini.
2. Bapak Dr. Setiyo Budiyanto, ST, MT, selaku Dosen Penguji yang telah banyak memberikan review dan saran yang membangun untuk membuat penelitian ini menjadi lebih baik.
3. Bapak Prof. Dr. Andi Adriansyah, M.Eng, sebagai Ketua Jurusan Program Magister Teknik Elektro UMB.
4. Bapak Prof. Dr. -Ing. Mudrik Alaydrus, Selaku Direktur Program Pascasarjana UMB
5. Seluruh Dosen Program Pascasarjana Program Magister Teknik Elektro UMB yang telah memberikan arahan dan bimbingannya.
6. Orang Tua tercinta, Ibu Tati Sumiati, dan Bapak Tohari, serta kakak – kakak Ristuna Mangun Kesuma, Indri Suci Mulyati, dan Nur Adhi Pranata.
7. Istri tercinta Siti Mujanah yang telah setia mendampingi dan membantu dalam segala proses pembuatan tesis ini
8. Ananda Muhammad Tsabit Khanz Fadhilah yang selalu ceria dalam menungu Ayah dalam menyelesaikan tesis ini, dan ananda Ahnaf Khalif Fadhilah yang selalu menghibur Ayah dan membangkitkan semangat Ayah untuk menyelesaikan tesis ini.

9. Mas Krisnawanto selaku teman baik yang selalu memberikan masukan dalam proses hal teknis pada tesis ini
10. Mas Rahmatsyah selaku teman baik yang bersedia meminjamkan laptopnya untuk pengujian tesis dan membantu dalam memberikan ide penulisan yang baik
11. Mas Arif Romansyah selaku teman baik yang memberikan satu referensi paper penting yang sangat membantu penulisan tesis ini.
12. Semua Pihak yang telah membantu menyelesaikan pembuatan dan penulisan tesis ini.

Saya menyadari bahwa dalam penulisan tesis ini masih banyak terdapat kekurangan. Oleh karena itu saran dan kritik yang membangun akan penulis terima dengan senang hati. Akhir kata penulis berharap agar tesis ini bermanfaat khususnya bagi penulis maupun pihak-pihak yang berkepentingan.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR SINGKATAN

CAIDA	: Center for Applied Internet Data Analysis
CPU	: Central Processing Unit
DoS	: Denial-of-Service
DDoS	: Distributed Denial-of-Service
DNS	: Domain Name Server
GB	: Giga Byte
HIDS	: Host Intrusion Detection System
IP	: Internet Protocol
ICMP	: Internet Control Message Protocol
IDS	: Intrusion Detection System
IPS	: Intrusion Prevention System
IETF	: Internet Engineering Task Force
LOIC	: Low Orbit Ion Cannon
MB	: Mega Byte
NIDS	: Network Intrusion Detection System
NTP	: Network Time Protocol
OISF	: Open Information Security Foundation
PCA	: Principal Component Analysis
PPS	: Packet Per Second
QoS	: Quality of Service
RAM	: Random Access Memory
RFC	: Request For Comments
SNMP	: Simple Network Management Protocol
TCP	: Transmission Control Protocol
UDP	: User Datagram Protocol
VM	: Virtual Machine