UNIVERSITAS
MERCU BUANA

PENERAPAN IDS DAN ANALISIS KEAMANAN PADA JARINGAN PUBLIC CLOUD MENGGUNAKAN ROUTEROS DAN ALERT NOTIFICATION DENGAN INSTANT MESSAGING

TESIS

Oleh

Ekky Rega Prabowo

55417110017

PROGRAM STUDI MAGISTER TEKNIK ELEKTRO
FAKULTAS TEKNIK
UNIVERSITAS MERCUBUANA JAKARTA
2020

ABSTRAK

Serangan Siber merupakan ancaman yang serius bagi kemanan jaringan, terutama pada jaringan public cloud karena bisa diakses oleh siapapun dari seluruh dunia. Akibat dari serangan siber berdampak besar jika attacker berhasil mengganggu suatu kinerja jaringan bahkan hingga bisa menguasainya, terutama pada jaringan yang menyediakan layanan bagi public. Seorang sysadmins jaringan harus siap tanggap dalam menangani setiap serangan pada server yang dikelolanya. Tahap pertama dalam mencegah serangan yang mengancam suatu jaringan public cloud yaitu dengan merancang sistem untuk mendeteksi dan memberikan peringatan dini akan suatu serangan yang dinamakan Intruision Detection System (IDS). Aplikasi yang digunakan sebagai IDS yaitu RouterOS yang berfungsi untuk mendeteksi serangan berdasarkan rules yang dicocokan dengan signature dari serangan tersebut, kemudian akan disimpan ke database untuk diteruskan kepada sysadmins. Hasil dari penggunaan IDS dengan notifikasi melalui instant messaging menggunakan system API mampu mendeteksi serangan ICMP Flooding, Port Scanning, dan HttpFlooding berdasar rules yang telah dikonfigurasi pada RouterOS. Berdasarkan hasil analisis respon waktu pengiriman notifikasi yang dilakukan dalam 10x percobaan dari setiap serangan didapatkan hasil rata-rata sebagai berikut ICMP Flooding 21.5 detik, Port Scanning 26 detik, dan HTTP Flooding 29.8 detik, respone ini sesuai dengan standard ISO 27001:2013-point A.13.1.1 NetworkControls, dimana IDS dan alert notification mendeteksi serta memberikan peringatan valid dan realtime. Hal ini diharapkan dapat

membantu sysadmin untuk melakukan next action penanganan terhadap ancaman pada jaringan di public cloud..

Kata Kunci : Keamanan, Intrusion detection sistem, RouterOS, Public Cloud, Instant Messaging

ABSTRACT

Cyber attacks are a serious threat to network security, especially on public cloud that can be accessed by anyone from all over the world. As a result of cyber attack is very big impact if it successfully disrupt a network performance even to take over the server, especially on networks that provide public service. A sysadmins must be responsive in handling any attacks on the server they manage. The first step in preventing attacks that can threaten a network public cloud is by designing a system to detect and provide early warning of an attack called Intruision Detection System (IDS). The application used as IDS is RouterOS that serves to detect attacks based on rules that will be matched with the signature of the attack, and will be saved to the database to be forwarded to the sysadmins via instant messaging. The results of using IDS with notifications via instant messaging bot using system API, capable of detecting ICMP Flooding, Port Scanning, and HttpFlooding based on rules configured on RouterOS. Based on the results of the analysis of the response time for send notifications carried out in 10 attempts from each attack, the following average results are ICMP Flooding 21.5 seconds, Port Scanning 26 seconds, and HTTP Flooding 29.8 seconds, this response following ISO standard 27001:2013-point A.13.1.1 NetworkControls, where IDS and alert notification detect and provide valid and realtime warnings. This is expected to help sysadmin perform the next action handling against threats on the public cloud network.

Keywords: Security, Intrusion detection system, RouterOS, Public Cloud, Instant Messaging

PENGESAHAN TESIS

Judul	: Penerapan IDS dan Analisis Keamanan pada Jaringan Public Cloud menggunakan RouterOS dan Alert Notification dengan Instant Messaging
Nama	: Ekky Rega Prabowo
NIM	: 55417110017
Program	: Pascasarjana Program Magister Teknik Elektro
Konsentrasi	: Security ICT
Tanggal	: 7 Januari 2021

Mengesahkan

Pembimbing

Dr. Marza Ihsan Marzuki, MT.

Direktur Pascasarjana	Ketua Program Studi
(Prof. Dr. -Ing. Mudrik Alaydrus)	**(Dr. Andi Andriansyah, M. Eng)**

PERNYATAAN SIMILARITY CHECK

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

Nama : Ekky Rega Prabowo

NIM : 55417110017

Program Studi : Magister Teknik Elektro

Dengan judul "**Penerapan IDS dan Analisis Keamanan pada Jaringan Public Cloud menggunakan RouterOS dan Alert Notification dengan Instant Messaging**" telah dilakukan pengecekan *similarity* dengan *sistem* Turnitin pada tanggal 6 Januari 2021 didapatkan nilai persentase sebesar 6 %.

Jakarta, 7 Januari 2021

Adminitrator Turnitin

Arie Pangudi, A.Md

PERNYATAAN KEASLIAN

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

Judul	: **Penerapan IDS dan Analisis Keamanan pada Jaringan Public Cloud menggunakan RouterOS dan Alert Notification dengan Instant Messaging**
Nama	: Ekky Rega Prabowo
NIM	: 55417110017
Program	: Pascasarjana Program Magister Teknik Elektro
Konsentrasi	: Security ICT
Tanggal	: 7 Januari 2021

Merupakan hasil studi pustaka, penelitan lapangan, dan karya saya sendiri dengan bimbingan pembimbing yang ditetapkan dengan Surat Keputusan Ketua Program Studi Magister Teknik Elektro Universitas Mercu Buana.

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

Jakarta, 7 Januari 2021

Ekky Rega Prabowo

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.

Tesis ini berjudul "**Penerapan IDS dan Analisis Keamanan pada Jaringan Public Cloud menggunakan RouterOS dan Alert Notification dengan Instant Messaging".** Penyusunan tesis ini bukanlah hal yang mudah bagi penulis, ada beragam kendala yang dihadapi, hanya dengan izin Allah SWT sajalah kemudahan itu datang.

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 Prof. Dr. -Ing. Mudrik Alaydrus sebagai Direktur Pasca Sarjana.
2. Bapak Dr. Andi Adriansyah, M. Eng sebagai Ketua Program Studi Magister Teknik Elektro, yang memotivasi diselesaikannya penulisan tesis ini.
3. Bapak Dr. Marza Ihsan Marzuki, MT sebagai Dosen Pembimbing dengan kesabaran dan motivasinya membuat penyusunan tesis ini menjadi lebih memiliki warna diakhir studi penulis.
4. Seluruh Dosen Program Pascasarjana Program Magister Teknik Elektro UMB yang telah memberikan arahan dan bimbingannya.

5. Seluruh Tata Usaha Program Pascasarjana UMB khususnya buat Mas Miyono atas bantuannya di bidang administrasi dalam menyelesaikan studi ini.
6. Orang tua dan keluarga tercinta (istriku dan anakku), doa'mu memberi kekuatan menyelesaikan ini semua. Terima kasih sudah mempercayai saya menyelesaikan ini.
7. Rekan-rekan mahasiswa MTEL angkatan 21 Mas Singgih, Mba Novi, Mba Roza Pak Sigit dan semua yang tidak bisa disebutkan satu persatu dan Rekan perjuangan Tesis dari Binus Bimandika Hasanah.
8. 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.

Jakarta, 7 Januari 2021

Ekky Rega Prabowo

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR SINGKATAN

IDS = Intrusion Detection Sistem

IaaS = Infrastructure as a Service

PaaS = Platform as a Service

SaaS = Software as a Service

VM = Virtual Machine

OS = Operating System

ICMP = Internet Control Message Protocol

HTTP = Hypertext Transfer Protocol