BAB 1
PENDAHULUAN

1.1 Latar Belakang

Cloud computing merupakan penggambaran dari jaringan internet yang diabstraksi dari infrastruktur yang kompleks. Sumber daya seperti *processor/computing power, storage, network, software* pada suatu *cloud computing* menjadi abstrak (*virtual*) dan diberikan sebagai layanan di jaringan internet saat ini (Maarif 2017). Dengan adanya *cloud computing* menimbulkan perubahan dalam kinerja suatu sistem informasi teknologi baik dalam organisasi ataupun perusahaan. *Cloud computing* menyediakan infrastruktur yang fleksibel dan efisien sehingga *cloud computing* banyak digunakan dalam banyak hal. Hal ini karena *cloud computing* mempunyai konsep virtualisasi, standarisasi yang dapat mengurangi biaya teknologi informasi, memudahkan pengelolaan layanan dalam informasi teknologi dan dapat mempercepat suatu layanan teknologi informasi (Aryani and Ningrum, Ira Tyas 2011).

Salah satu bidang yang penggunaan *cloud computing* makin meningkat adalah *e-health* (penggunaan teknologi informasi dan komunikasi pada bidang kesehatan). Negara di Asia Timur yang sudah menerapkan sistem informasi kesehatan yang terintegrasi dengan *cloud computing* misalnya Taiwan menggunakan sistem media elektronik *Medical Record Template* (TMT) yang merupakan kartu elektronik untuk kesehatan (Lu, Ranjan, and Strazdins 2015).

E-health merupakan jenis layanan kesehatan yang pertukaran informasi nya sangat kompleks. Sehingga *e-health* diintegrasikan dengan *cloud computing* untuk menghemat sumber daya dan memudahkan dalam pertukaran informasinya (Ramadhani 2015). Kompleksitas alur pertukaran informasi data pada *e-health cloud*, menyebabkan *e-ehealth cloud* rentan terhadap beberapa ancaman-ancaman keamanan sistem e-*health*. Isu keamanan yang perlu diperhatikan pada sistem *e-health cloud* adalah kerahasiaan data pasien atau proteksi data, dan pelayanan *outsource* (Ramadhani 2015)

Isu keamanan terkait *e-health cloud* terhadap ancaman salah satunya, *request synchronize* (SYN) *flooding attack*, yang merupakan ancaman yangm sering terjadi, SYN *flooding attack* merupakan salah satu serangan yang mengeksploitasi kelemahan yang terdapat di dalam protokol *Transmission Control Protocol* (TCP). Serangan ini akan membanjiri lalu lintas jaringan dengan banyak data sehingga lalu lintas jaringan yang datang dari pengguna yang terdaftar menjadi tidak dapat masuk ke dalam sistem jaringan.

Sysmantec yang merupakan perusahaan asal Amerika yang memproduksi *software* pengamanan data. Perusahaan ini bermarkas di Mountain View Californ melaporkan pada tahun 2011, Symantec telah memblokir total lebih dari 5,5 miliar serangan *malware*, meningkat 81% dari tahun 2010, dan serangan berbasis Web meningkat 36% dengan lebih dari 4.500 serangan baru setiap hari (Umar, Li, and Ahmad 2014).

Network intrusion detection system (NIDS) adalah sebuah sistem yang berupa perangkat keras maupun perangkat lunak yang mampu melakukan pengawasan terhadap trafik jaringan dan pengawasan terhadap kegiatan-kegiatan yang mencurigakan di dalam sebuah sistem jaringan *internet* yang diletakkan pada pintu masuk lalu lintas jaringan terdapat pada *switch, router, firewall*. *Network Intrusion detection system signature-based* merupakan mekanisme pencegahan yang paling cocok untuk ancaman serperti SYN *flooding attack* (Patil et al. 2018). NIDS ini akan melakukan pengawasan terhadap paket-paket yang masuk ke dalam jaringan dan melakukan pembandingan terhadap *rules* yang dimiliki oleh sistem. Namun NIDS *signature-based* akan terjadi keterlambatan saat melakukan pembandingan paket terhadap *rules* yang dimiliki oleh sistem. Dengan teknik *multithread* pada NIDS *signature-based* ini dapat memungkinkan proses lebih cepat mendeteksi suatu ancaman, karena proses pembandingan terhadap paket-paket yang diterima akan diproses secara bersamaan sehingga dapat memiliki keakuratan yang tinggi (Patil et al. 2018).

Impementasi NIDS-*signature-based* dengan teknik *multithread* adalah salah satu cara untuk melindungi *server* dan perangkat lainnya dari ancaman yang merugikan dan menjaga suatu informasi seseorang. Melindungi suatu informasi sama juga menjaga harta benda milik sendiri, menurut pandangan agama Islam melindungi harta benda merupakan sesuatu yang dianjurkan (Iswandi 2015). Sebagaimana firman Allah SWT:

وَلَا تُؤْتُوا۟ ٱلسُّفَهَآءَ أَمْوَٰلَكُمُ ٱلَّتِى جَعَلَ ٱللَّهُ لَكُمْ قِيَٰمًا وَٱرْزُقُوهُمْ فِيهَا
وَٱكْسُوهُمْ وَقُولُوا۟ لَهُمْ قَوْلًا مَّعْرُوفًا ٥

Artinya:

"*Dan janganlah kamu serahkan kepada orang yang belum sempurna akalnya, harta (mereka yang ada dalam kekuasaan) kamu yang dijadikan Allah sebagai pokok kehidupan. Berilah mereka belanja dan pakaian (dari hasil harta itu) dan ucapkanlah kepada mereka perkataaan yang baik*" (Q.S. An-Nisa [4]:5)

Dalam tafsir Syaikh Dr. Muhammad Sulaiman Al Asyqar, Ayat ini merupakan perintah untuk menjaga harta agar tidak diserahkan dan diatur oleh seorang yang belum sempurna akalnya, dan melarang orang yang berhak untuk mendapatkan harta dengan memberi harta kepada yang tidak mempunyai kapabilitas dalam mengelolanya. Dari penjelasan tersebut agama Islam menganjurkan bahwa melindungi harta benda merupakan sesuatu yang baik.

Pada skripsi ini akan mengimplementasikan *NIDS signature-based* dengan teknik *multithread* pada *e-health cloud* sebagai pencegah dari ancaman SYN *flood attack. NIDS signature-based* dengan teknik *multithread* yang berada di dalam *router* virtual dapat membantu mengatasi trafik mencurigakan di *e-health cloud*. Selain itu, akan dikaji penggunaan *network intrusion detection system signature-based* dengan teknik *multithread* untuk model *e-health cloud* Indonesia menurut pandangan Islam.

1.2 Perumusan Masalah

Berdasarkan latar belakang di atas, maka dapat disimpulkan perumusan masalah adalah sebagai berikut :

1. Apakah *NIDS signature-based* dengan teknik *multithread* dapat digunakan sebagai proteksi yang dapat medeteksi dan menahan serangan *SYN flooding attack*?
2. Bagaimana mengimplementasikan *NIDS signature-based* dengan teknik *multithread* untuk model *e-health cloud* Indonesia?
3. Bagaimana merumuskan aturan yang digunakan *NIDS signature-based* terhadap model *e-health cloud* Indonesia*?*
4. Bagaimana pandangan Islam terhadap *NIDS signature-based* dengan teknik *multithreading* yang menjaga informasi.

1.3. Tujuan Penelitian

Tujuan yang ingin dicapai dari penelitian ini adalah sebagai berikut:

1. Merumuskan aturan dan mengimplementasi *NIDS signature-based* menggunakan teknik *multithread* sebagai panahan serangan SYN *flooding attack* bagi *e-health cloud* Indonesia.
2. Menguji *e-health cloud* Indonesia yang menggunakan *NIDS signature-based* dengan teknik *multithread* terhadap serangan *SYN flooding attack*.

3. Mengkaji penggunaan *NIDS* model *e-health cloud* Indonesia menurut pandangan Islam.

1.4. Manfaat Penelitian

Manfaat yang dapat diambil dari penelitian ini sebagai berikut:

1. Melindungi model *e-health cloud* Indonesia dari serangan *SYN flooding attack.*
2. Meningkatkan keamanan untuk model *e-health cloud* Indonesia.
3. Mengetahui pandangan Islam terhadap pengunaan mekanisme *NIDS.*

1.5. Batasan Masalah

Dengan rumusan masalah tersebut, maka diperlukan batasan masalah sehingga pembahasan dapat terarah sesuai dengan tujuan penelitian. Adapun batasan masalah tersebut adalah sebagai berikut :

1. Implementasi ini dirancang dengan menggunakan *vmware workstation* sebagai media untuk simulasi
2. Metode serangan menggunakan *SYN flooding attack*.
3. Serangan SYN *flooding attack* menggunakan *command* hping3 kali linux.
4. Topologi yang digunakan mengacu model penyebaran *deployment* model *e-health could* Indonesia.
5. Mekanisme penahan dari serangan *SYN flooding attack* menggunakan *NIDS signature-based* dengan teknik *multithread*
6. *Router* virtual dan *server* virtual dibangun menggunakan virtualisasi pada *node Proxmox VE*.
7. Pengujian ketahanan serangan terhadap SYN *flooding attack* dilakukan berdasarkan skenario yang telah dibuat.