BAB 1 PENDAHULUAN

1.1 Latar Belakang

Cloud Computing atau komputasi awan ialah teknologi yang memanfaatkan layanan internet untuk mengakses pusat *server* yang bersifat virtual dengan tujuan pemeliharaan data dan aplikasi. *Cloud computing* membantu perusahaan menjadi lebih lincah dan responsif, dapat mengurangi biaya dan kompleksitas teknologi informasi secara signifikan melalui optimalisasi beban kerja. Pada *cloud computing*, sumber daya yang dibutuhkan pengguna seperti *prosesor/computing power*, *storage, network, software* diberikan melalui jaringan internet (Maarif, 2017).

Pemanfaatan *cloud computing* di bidang *e-health* (penggunaan teknologi informasi dan komunikasi pada bidang kesehatan) bertujuan untuk memperbaiki layanan kesehatan dan membantu penelitian di bidang kesehatan, namun di sisi lain juga harus menanggung risiko sehubungan dengan aspek keamanan dan privasi yang perlu ditangani secara hati-hati. Contoh implementasi dari *e-health cloud* saat ini adalah *telemedicine* yakni teknologi informasi dan komunikasi yang digabungkan dengan kepakaran medis untuk memberikan layanan kesehatan (Iryani, 2015).

Keamanan menjadi suatu komponen yang sangat penting dan krusial untuk diperhatikan dalam penerapan *e-health cloud*. Isu keamanan terkait pemanfaatan *cloud* diantaranya, UDP *flood,* ICMP *flood,* spoofing, SQL *injection, packet sniffing, port scanning,, ransomware,* dan *distributed denial of service* (DDoS).

Serangan yang paling sering terjadi adalah *port scanning* dan DDoS. *Port scanning* adalah serangan yang bekerja untuk mencari *port* yang terbuka pada suatu jaringan komputer. Hasil *port scanning* adalah ditemukannya kelemahan suatu sistem jaringan komputer. *Distributed denial of service* (DDoS) adalah serangan yang bekerja dengan cara mengirim *request* ke *server* secara terus menerus dan bertujuan untuk membuat *server* menjadi sibuk menanggapi *request* tersebut lalu *server* akan mengalami kerusakan atau tidak dapat diakses (Laksono, 2017).

Intrusion detection system (IDS*)* adalah sistem untuk mendeteksi adanya penyusup yang dilakukan oleh *intruder* (penyusup) dalam sistem jaringan. Pada awal serangan, penyusup biasanya hanya mengeksploitasi data. Namun pada tingkat lebih lanjut penyusup dapat berusaha untuk mendapatkan akses ke *server* seperti membaca data

rahasia, memodifikasi tanpa izin dan mengurangi hak akses ke sistem sampai menghentikan sistem (*server down*) (Putra, 2014).

Salah satu optimalisasi sumber daya dan pencegahan dini terhadap serangan DDoS yaitu dengan menggunakan Honeypot. Honeypot adalah sumber daya sistem informasi yang meniru *service* yang ada pada *server* atau *workstation* dan digunakan dalam lingkungan produksi dengan tujuan untuk dieksploitasi oleh penyerang (Kurniawan, 2015). Penerapan Honeypot bertujuan untuk mendapatkan data-data dari para penyerang diantaranya cara mereka masuk ke dalam sistem. Honeypot merupakan *server* palsu yang menyerupai sistem aslinya, sehingga serangan yang ditunjukan untuk *server* tersebut tidak akan mengganggu data yang sebenarnya dan data terlindungi dari serangan. Dengan menggunakan *software* Honeyd-viz melalui *web interface*, admin jaringan dapat melihat dan menganalisa serangan dari penyerang terhadap sistem tersebut (Putra, 2014).

Impementasi kombinasi NIDS dan Honeypot adalah salah satu cara untuk melindungi *server* dan menjaga suatu informasi dari ancaman yang merugikan. Melindungi suatu informasi sama dengan menjaga harta benda yang dimiliki. Menurut pandangan agama Islam melindungi harta benda merupakan sesuatu yang dianjurkan (Iswandi, 2015). Sebagaimana firman Allah SWT:

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 atas harta memberi hartanya kepada yang tidak mempunyai kapabilitas dalam mengelolanya. Dari penjelasan tersebut agama Islam menganjurkan bahwa melindungi harta benda merupakan sesuatu yang baik.

Pada skripsi ini diimplementasikan kombinasi NIDS dan Honeypot sebagai pertahanan jaringan dari serangan yang sering terjadi pada jaringan komputer yang berada

di dalam *router virtual* sehingga dapat membantu mengatasi trafik yang mencurigakan pada model *e-health cloud.* Selain itu, juga akan dikaji penggunaan IDS dan Honeypot untuk keamanan model *e-health cloud* menurut pandangan Islam.

1.2 Perumusan Masalah

Berdasarkan latar belakang di atas, maka perumusan masalah dalam skripsi ini adalah sebagai berikut:

a. Bagaimana mengimplementasikan IDS dan Honeypot untuk keamanan pada model *e-health Cloud* Indonesia?
b. Apakah IDS dan Honeypot dapat digunakan sebagai proteksi yang dapat mendeteksi dan menahan serangan?
c. Bagaimana mengarahkan serangan yang sudah diblok oleh IDS ke dalam *server* Honeypot?
d. Bagaimana penggunaan mekanisme IDS dan Honeypot untuk keamanan model *e-health cloud* Indonesia menurut pandangan Islam?

1.3 Tujuan Penelitian

Tujuan yang ingin dicapai dari penelitian ini adalah sebagai berikut:

1. Memperkuat sistem keamanan model *e-health cloud* Indonesia dengan mengimplementasikan kombinasi IDS dan Honeypot.
2. Menguji kinerja IDS dan Honeypot terhadap serangan Slowloris, SYN *flooding attack*, dan *port scanning*.
3. Menguji penggunaan mekanisme IDS dalam meneruskan serangan ke Honeypot.
4. Mengkaji mekanisme IDS dan Honeypot untuk keamanan model *e-health cloud* Indonesia menurut pandangan Islam.

1.4 Manfaat Penelitian

Manfaat yang dapat diambil dari penelitian ini adalah sebagai berikut:

1. Membantu administrator *e-health cloud* Indonesia dalam mengantisipasi serangan ke *server*.
2. Membantu administrator untuk melihat dan menganalisis serangan terhadap sistem dengan menggunakan *software* Honeyd-viz yang diterapkan pada Honeypot.
3. Mengetahui kinerja dari sistem IDS dan Honeypot yang diserang dari berbagai macam serangan DDoS.
4. Memberikan rekomendasi metode untuk pencegahan dini terhadap serangan DDoS.

1.5 Batasan Masalah

Batasan masalah pada skripsi ini adalah sebagai berikut:

1. Implementasi *e-health cloud* Indonesia menggunakan VMware Workstation sebagai media untuk simulasi.
2. *Virtual router* dan *server* dibangun menggunakan Proxmox VE.
3. Metode penyerangan DDoS menggunakan *script* Slowloris yang mengirimkan paket dalam jumlah banyak secara terus menerus dan *script* SYN *flooding attack* pada Kali Linux serta dengan penyerangan *port scanning.*
4. Serangan SYN *flooding attack* menggunakan *command hping3*.
5. Serangan dianalisis dengan menggunakan Honeyd-viz.
6. Pengujian dilakukan berdasarkan skenario yang telah dibuat.