BAB 1. PENDAHULUAN

1.1. Latar Belakang

Penetrasi pengguna internet Indonesia berdasarkan pada hasil survey dari APJII (Asosiasi Penyelenggara Jasa Internet Indonesia) pada tahun 2018, sebanyak 171.17 juta jiwa atau 64.8% dari total populasi penduduk Indonesia(APJII, 2019). Kementerian Komunikasi dan Informatika juga menyebutkan pengguna internet di Indonesia mencapai lebih dari 50% total populasi penduduk Indonesia. Hal tersebut semakin menunjukkan betapa banyaknya pengguna internet di Indonesia.

Dengan perkembangan pengguna internet di Indonesia maka intensitas kemunculan berbagai jasa berbasis daring atau *online* juga semakin meningkat seperti transportasi *online,* pembelajaran daring, dan *e-commerce*. Salah satu contoh tahun 2019, Indonesia juga merupakan negara 10 terbesar pertumbuhan *e-commerce* dengan pertumbuhan 78% dan berada di peringkat ke-1. Sementara Meksiko berada di peringkat kedua, dengan nilai pertumbuhan 59% menurut data dari Kementerian Komunikasi dan Informatika.

Disamping itu, Kementerian Komunikasi dan Informatika juga menunjukkan betapa masih banyak penyalahgunaan fungsi dari internet oleh para pengguna, mulai dari penyebaran berita bohong, video porno, peretasan sebuah situs, dan pencurian data pribadi seseorang. Dimana pada tahun 2012 saja, sudah dapat dibuktikan dengan adanya sebanyak 50% website pemerintah yang diretas menggunakan domain go.id atau yang selama ini digunakan oleh pemerintah maupun domain lain seperti .com, .net, .org . Pada tahun 2018, sistem dari Kementerian Komunikasi dan Informatika juga mendeteksi setidaknya ada 1.225 miliar serangan siber setiap harinya, dimana *malware* terutama *ransomware* menjadi serangan paling banyak terjadi. Data tersebut juga diperkuat oleh pernyataan Badan Siber dan Sandi Negara dan Kementerian Koordinator Bidang Politik, Hukum, dan Keamanan, dimana serangan – serangan tersebut diperjelas oleh adanya sensor dari Badan Siber dan Sandi Negara melalui

laporan tahunan *Honeynet Project* tahun tersebut, dengan rincian jumlah total serangan siber di Indonesia pada 21 sensor yang telah terpasang yaitu sebanyak 12.895.554 serangan, dengan jumlah serangan *malware* sebanyak 513.863 serangan. Terdapat tiga sumber serangan tertinggi berasal dari Rusia dengan 2.597.256 serangan, China dengan 1.871.363 serangan, dan Amerika Serikat dengan 1.428.440 serangan.

Penyerangan biasanya dilakukan untuk mengambil data privasi yang ada dalam sebuah *database*, merusak tampilan sebuah sistem informasi, merubah hingga merusak integritas data yang ada didalamnya untuk kepentingan tertentu. Serangan tersebut bisa berupa *SQLinejction*, *DDoS*, *Phishing*, *Web Flooding* melewati *front-end* maupun langsung ke *back-end* dari sebuah sistem tergantung dari mana celah yang paling rentan untuk di retas. Tentu ini sangat merugikan pengguna jasa sistem informasi dan juga penyedia layanan tersebut karena integritas dari penyedia layanan akan buruk di pandangan penggunanya.

Oleh karena itu, diperlukan sinergi yang baik antara pemerintah dan praktisi atau tenaga bidang teknologi informasi. Dari sisi pemerintah perlu adanya sebuah regulasi dan penanganan yang serius dari berbagai pihak, baik pemerintah yang harus segera menerbitkan undang-undang tentang keamanan siber, privasi data pribadi seseorang yang lebih jelas dan akurat. Dari Kita, sebagai praktisi atau tenaga bidang teknologi informasi harus selalu melakukan pengembangan cara pengamanan dalam sebuah sistem informasi yang dikembangakan untuk meminimalisir sebuah peretasan.

Salah satu cara meminimalisir hal tersebut adalah dengan menerapkan sebuah akses khusus terhadap sebuah server yang dibuat, memberi batasan akses pada pengguna. Namun sisi kenyaman dalam menggunakan sistem informasi yang dikembangkan juga harus diperhatikan maka perlu juga manajemen alokasi *cache* dalam sistem.

Implementasi *proxy* dengan menggunakan *nginx* sebagai sebuah *reverse proxy.*

untuk menjadi pengubung antara *back-end* dan *front-end.* Reverse proxy sebagai salah

satu cara untuk mengurangi penggunaan *ip public* yang saat ini slot untuk *IPv4* sudah semakin menipis(Suprayogi & Pungkasanti, 2017). Manajemen *cache* adalah menyimpan konten dari akses informasi dan meneruskannya kembali ke pengguna(Dwijaya, 2018). *Load balancing* diperlukan untuk efisiensi ,yaitu merelokasi beban sehingga nanti titik penerima beban jumlahnya akan sama(Rahmad Dani, 2017). Penelitian tersebut juga mengutip penelitian lain yang mengatakan bahwa teknik *load balance* bekerja dengan cara membagi beban yang diterima oleh server dan ketika salah satu mati, maka server lain akan melayani permintaan dari pengguna(Handoko Yoga Hartomo, Ir. Bana Handaga, M.T., 2015). Penelitiannya juga turut membuktikan hasil penggunaan dua software *load balancing* pound dan haproxy di mana keduanya sama-sama mampu meningkatkan kemampuan server namun terbukti haproxy sedikit lebih unggul. Hal tersebut dilakukan untuk meningkatkan kualitas koneksi dari sebuah *server* terhadap penggunanya, sehingga masalah seperti *server down* dapat diatasi karena dengan mekanisme tersebut server bekerja dengan lebih efisien. Selain itu juga untuk mengatasi dan meminimalisir serangan – serangan seperti di atas sekaligus memperbaiki kualitas sistem yang diharapkan dengan usaha pengamanan tersebut, integritas data dalam sebuah sistem informasi dapat terjaga sehingga rasa nyaman dalam menggunakan sistem tersebut dapat meningkat dan rasa resah maupun risau tentang keamanan data privasi pengguna dapat berkurang.

Setelah implementasi tadi dilakukan maka pengujian untuk mengukur keandalan, efektivitas dan efisiensi dari hal tersebut mulai dari penggunaan JMeter untuk mengukur performa dari server, kemudian melakukan serangan atau penetrasi langsung pada server seperti DDoS, dan lain lain.

1.2.Rumusan Masalah

Berdasarkan latar belakang diatas, maka rumusan masalah dalam penelitian ini adalah

1. Bagaimana *nginx* yang sejatinya lebih dikenal sebagai sebuah web server akan menjalankan tugas lain, yaitu sebagai *reverse proxy* yaitu menjadi penghubung antara *back-end* dan *front-end.*
2. Bagaimana *nginx* melakukan mekanisme *Load balancing* untuk efisiensi penggunaan sumber daya dalam sistem paralel dan terdistribusi.

1.3. Tujuan

Tujuan dari penelitian ini adalah untuk menguji seberapa efektif dari pemilihan *nginx* untuk menjalankan fungsi tersebut dan memenuhi harapan tentang keandalan, keefektifan, dan keamanan dari sebuah sistem yang berjalan dan kenyamanan dalam penggunaan sistem nantinya.

1.4. Manfaat

Manfaat dari penelitian ini adalah menjadi salah satu referensi dalam pengembangan sebuah sistem informasi dimana keaman dan kenyaman pengguna dapat terjaga. Selain itu, paradigma tentang *nginx* yang pada umumnya dikenal sebagai *web server* dapat perlahan berkembang bahwa *nginx* juga bisa sebagai reverse proxy dan load balancing.