BAB 1
PENDAHULUAN

1.1 Latar Belakang

Perkembangan industri teknologi modern telah mencapai versi 4.0. Hal ini tentu lebih sulit dan karena itulah teknologi tidak dapat dipisahkan dari kehidupan manusia dalam segala aspek. Kehidupan sosial, termasuk teknologi melalui penciptaan media sosial, misalnya.

Namun yang jadi masalah adalah *malware* atau virus yang menyebar di *internet* (Dirja Nur Ilham, 2018). *Malware* adalah sebuah perangkat lunak yang dibuat dan dikembangkan untuk menyusup dan merusak pada sistem komputer, *server*, atau jaringan komputer.

Saat ini, keamanan jaringan memainkan peran kunci dalam mengurangi kerentanan terhadap serangan siber dan kejahatan yang ditimbulkannya. Keamanan adalah salah satu komponen utama yang perlu dipertimbangkan saat menghubungkan sistem ke jaringan komputer. Firewall digunakan untuk mencegah hal ini, tetapi jika penyerang sangat berbahaya di jaringan lokal, mereka dapat dengan mudah melewati Firewall dan sulit untuk dideteksi.

Pada tahun 2013, Akamai menemukan bahwa Indonesia menjadi nomor satu sebagai sumber serangan siber (*malicous traffic). Traffic* serangan dari IP Indonesia berkisar 35% dari seluruh serangan di internet dibandingkan *traffic* dari sekitar 175 negara yang disurvei.

Banyak alat dapat diidentifikasi untuk mendeteksi serangan pada jaringan, termasuk penggunaan sistem dan aplikasi Honeypot. Honeypot adalah sistem informasi yang terhubung ke jaringan komputer yang digunakan sebagai umpan untuk menarik atau menjebak peretas. Dengan Honeypot, peretas jatuh ke dalam jebakan. Sistem di dalamnya sama persis dengan sistem yang sebenarnya. Oleh karena itu, peretas mengira mereka telah membobol jaringan sebaliknya.

Secara umum, serangan yang paling umum terhadap *server* adalah serangan penolakan layanan *DoS* (*denial of service*). Serangan ini dapat menghabiskan sumber daya seperti *bandwidth* jaringan, pemrosesan CPU, dan memori. Serangan *DoS* yang dimulai pada lapisan aplikasi mengurangi *bandwidth* yang diperlukan untuk mencegah penjelajahan ke *server web* dan memalsukan lalu lintas sebenarnya (Molavi Arman N. R., 2020).

Brute force adalah tindakan peretas yang mencoba menebak nama pengguna dan kata sandi untuk memaksa akses ke sistem atau jaringan. Saat melancarkan serangan, pelaku selalu berusaha menghindari proses otentikasi dengan kombinasi kata sandi, tetapi serangan Brute force ini adalah metode serangan lama dan sederhana.

Di sisi lain, penelitian terkait keamanan *server web* menunjukkan bahwa fail2ban dapat mencegah serangan Brute force pada *server* dengan melakukan konfigurasi aturan pada fail2ban untuk membaca serangan pada port *HTTP / HTTPS* (Mohammad Idhom, Network Security System on Multiple Servers Against Brute Force Attacks, 2020)

Menerapkan kombinasi Firewall dan Honeypot adalah salah satu cara untuk melindungi *server* dari informasi dan ancaman berbahaya. Melindungi informasi sama dengan melindungi properti. Menurut pandangan agama Islam melindungi properti dianjurkan. Sebagaimana firman Allah SWT:

اِنَّ الْاَرْضَ لِلّٰهِ ۗيُوْرِثُهَا مَنْ يَّشَاۤءُ مِنْ عِبَادِهٖ ۗوَالْعَاقِبَةُ لِلْمُتَّقِيْنَ

Yang artinya :

" *Sesungguhnya bumi* (*ini*) *milik Allah. Dia akan mewariskannya kepada siapa saja yang dia hendaki di antara hamba-hamba-Nya. Kesudahan* (*yang baik*) *adalah bagi orang-orang yang bertaqwa."* (Q.S. al-A'raf(7): 128).

Tujuan Penelitian ini adalah untuk mengimplementasikan honeypot terhadap serangan Brute force dan *DoS* pada keamanan *web server*. Honeypot dalam penelitian ini digunakan untuk memantau dan mendeteksi aktivitas penyerang, dan juga sebagai *server* tiruan untuk meniru *server* nyata.

1.2 Perumusan Masalah

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

a. Bagaimana menerapkan Firewall dan Honeypot untuk keamanan pada *web server*?
b. Bisakah Firewall dan Honeypot digunakan sebagai perlindungan untuk mendeteksi dan memblokir serangan?
c. Bagaimana cara mengalihkan serangan yang diblokir oleh Firewall ke *server* Honeypot?
d. Bagaimana mendeteksi serangan dari sudut pandang islam menggunakan Firewall keamanan Raspberry Pi dan mekanisme Honeypot??

1.3 Tujuan Penelitian

Tujuan yang ingin dicapai dari penelitian ini adalah sebagai berikut:

1. Menerapkan kombinasi Firewall dan Honeypot meningkatkan sistem keamanan Raspberry Pi saat mendeteksi serangan.
2. Menguji kinerja Firewall dan Honeypot terhadap serangan Slowloris, Brute force, dan *port scan.*
3. Menguji penggunaan mekanisme Firewall terhadap serangan yang sedang berlangsung pada Honeypot.
4. Evaluasi mekanisme Firewall dan Honeypot untuk keamanan Raspberry Pi dalam mendeteksi serangan dari sudut pandangan Islam.

1.4 Manfaat Penelitian

Manfaat yang dapat diambil dari penelitian ini adalah sebagai berikut:

1. Memungkinkan administrator untuk memprediksi serangan pada *server*.
2. Memungkinkan administrator untuk melihat dan menganalisis serangan pada sistem.
3. Mengetahui tentang kinerja dari Firewall dan Honeypot yang diserang dari berbagai jenis serangan.

1.5 Batasan Masalah

Batasan masalah pada skripsi ini adalah sebagai berikut:

1. Implementasi menggunakan Virtualbox dan simulator jaringan GNS3 sebagai media simulasi.
2. Metode penyerangan *DDoS* menggunakan *script* Slowloris yang mengirimkan paket dalam jumlah banyak secara terus menerus dan Brute force *attack*, pada kali linux yang sudah dibuat serta dengan penyerangan *port scanning.*
3. Serangan dapat dianalisis dengan menggunakan aplikasi Atop.
4. Pengujian dilakukan berdasarkan skenario yang telah dibuat.