BAB I
PENDAHULUAN

1.1 Latar Belakang

Teknologi merupakan elemen yang penting untuk kehidupan saat ini. Pesatnya perkembangan teknologi memungkinkan banyaknya pengguna komputer yang terkoneksi dengan internet. Adanya internet dapat membantu banyak orang untuk mendapatkan informasi dari semua topik yang dicarinya, mulai dari jurnal riset, berita, forum perbincangan, hingga akses pada media hiburan. Hal ini didukung dengan adanya perangkat yang dapat terhubung melalui jaringan internet dengan biaya yang lebih murah dan akses yang lebih mudah, sehingga, penggunaan internet semakin lama semakin banyak.

Dalam sisi lain, banyaknya pengguna internet memungkinkan mendapatkan serangan yang cukup berbahaya. Beberapa situs web yang diakses pengguna berupa sosial media, *internet banking*, dan *e-commerce* juga berarti semakin banyak informasi yang dikeluarkan oleh pengguna itu sendiri ke internet. Hal ini menyebabkan situs-situs tersebut menjadi bahan serangan *hacker* untuk mencuri informasi data dan mengincar keuntungan besar. Salah satu cara serangan yang dilakukan adalah *malware*, dimana *malware* merupakan kode yang berbahaya dan dapat menyebar ke seluruh jaringan, termasuk internet (Rizwan, Hazarika, & Chetia, 2011).

Adanya penggunaan internet yang besar juga berarti penyebaran *malware* dapat dilakukan dengan hanya mengunjungi suatu situs web saja. Ini tentu sangat berbahaya, terutama untuk pengguna yang belum mengerti bahayanya situs web yang sudah terinfeksi dengan *malware*. Keamanan jaringan pun sering kali dianggap tidak penting oleh pengguna, dan kurangnya pemantauan jaringan juga meningkatkan resiko serangan. Jaringan nirkabel sering menjadi bahan serangan dikarenakan jaringan tersebut bersifat terbuka dan sistem keamanan yang bersifat terbatas. *Malware* bisa mencapai ke sistem komputer melalui banyak cara. Salah satunya yang paling umum adalah melalui unduh dari internet. Biasanya, *malware* hanya memperlambat performa komputer yang sudah terinfeksi. Namun, ada beberapa *malware* yang bersifat *spyware* dimana *malware* akan tersembunyi dalam sistem komputer yang sudah terserang dan akan mengirimkan informasi komputer terinfeksi ke sumber pembuat *malware* tersebut.

Salah satu solusi untuk menghindari serangan *malware* adalah membuat suatu *honeypot*. Secara singkat, *honeypot* bekerja sebagai *host* yang berjalan seakan-akan seperti komputer pengguna awam yang biasa. *Honeypot* dirancang untuk rentan terhadap serangan, sehingga penyerang bisa masuk ke sistem *honeypot.* Ini menyebabkan serangan dilakukan pada *honeypot* itu sendiri dan bukan ke komputer atau perangkat pribadi pengguna. *Honeypot* kemudian akan berinteraksi dengan penyerang, merekam semua aktifitas, dan menyimpan *malware* yang terlibat sebagai *log* (Charles Lim, Mario Marcello, Andrew Japar, Joshua Tommy, & I Eng Kho, 2014).

Honeypot *Dionaea* tidak membutuhkan spesifikasi *hardware* yang besar. Sehingga, instalasi *honeypot* tersebut akan dilakukan pada *Raspberry Pi 3 B+*. *Raspberry Pi* adalah sebuah komputer kecil yang ukurannya sebesar suatu kartu kredit. Selain harganya yang murah, *Raspberry Pi* juga tidak membutuhkan daya yang besar, sehingga penggunaan *Raspberry Pi* yang terus menerus bersifat efisien. Berdasarkan uraian diatas, maka penulis akan melakukan penelitian dengan judul **"Implementasi *Honeypot Dionaea* untuk Mendeteksi *Malware* Menggunakan Raspberry Pi"**.

1.2 Identifikasi Masalah

Dari latar belakang yang sudah di uraikan sebelumnya, maka dapat diidentifikasikan masalah sebagai berikut:

1. Belum adanya proteksi serangan *malware* di jaringan.
2. Kurangnya pemantauan keamanan jaringan terhadap serangan.
3. Keamanan jaringan sering dianggap tidak penting oleh pengguna komputer.

1.3 Batasan Masalah

Dengan adanya keterbatasan baik dari segi waktu, pemikiran, maupun biaya, maka penelitian ini dibatasi pada hal-hal tersebut:

1. Keterbatasan waktu dan biaya membuat penelitian ini akan dilakukan dirumah.

2. Implementasi *honeypot* yang digunakan adalah *honeypot Dionaea.*
3. Penelitian dilakukan pada *Raspberry Pi 3 Model B+* dengan sistem operasi *Raspbian*.

1.4 Rumusan Masalah

Perumusan permasalahan dalam penulisan skripsi ini adalah:

1. Bagaimana cara mengimplementasikan *honeypot* tanpa mengurangi keamanan jaringan secara nirkabel?
2. Bagaimana cara mengimplementasikan *honeypot* dengan menggunakan *Raspberry Pi*?
3. Bagaimana cara untuk melakukan simulasi hasil penangkapan serangan *malware*?

1.5 Tujuan Penelitian

Tujuan penelitian ini adalah:

1. Melakukan implementasi *honeypot Dionaea* tanpa mengurangi keamanan jaringan secara nirkabel.
2. Melakukan implementasi *honeypot Dionaea* ke *Raspberry Pi.*
3. Melakukan simulasi penangkapan *malware* yang bisa diakses melalui komputer pengguna.

1.6 Manfaat

Adapun manfaat penelitian ini adalah:

1.6.1 Manfaat Teoritis

Adapun manfaat penelitian ini secara teoritis adalah:

1. Hasil penelitian dapat memberikan kontribusi dalam ilmu pengetahuan, pendidikan, dan teknologi.
2. Hasil penelitian bisa menjadi bahan acuan dan pertimbangan untuk penelitian selanjutnya.

1.6.2 Manfaat Praktis

Manfaat penelitian secara praktis adalah:

1. Meningkatkan keamanan jaringan untuk menghindari serangan *malware* ke komputer pengguna.
2. Meningkatkan keamanan jaringan dengan biaya lebih kecil.
3. Melakukan analisa pada *malware* yang sudah tertangkap oleh *honeypot*.
4. Munculnya kesadaran akan pentingnya keamanan jaringan, sekecil apapun sistem jaringan yang digunakan.