BAB I

PENDAHULUAN

1.1. Latar Belakang

Perkembangan dan kemajuan teknologi *internet* meningkat pesat dari tahun ke tahun, begitu juga dengan pengguna layanan jaringan *internet*. Tanpa disadari bahwa dalam perkembangan teknologi jaringan *internet* yang memudahkan kehidupan kita ternyata juga memiliki kerentanan atau resiko serius dalam hal privasi dan keamanan data pengguna. Dalam sebuah jaringan tentunya diperlukan adanya keamanan jaringan namun keamanan jaringan juga perlu didukung oleh faktor-faktor pendukungnya sebagai lapisan keamanan jaringan tersebut. Pengimplementasikan *Honeypot Dionaea* pada keamanan jaringan akan menjadi salah satu kunci terjaminnya keamanan *port* dan jaringan.

Sistem komputer menjadi bagian yang sangat penting dan tidak dapat dipisahkan dari bidang pekerjaan manapun. *Internet* merupakan jaringan komputer yang bersifat publik. *Malware* (*Malicious Software*) merupakan sebuah perangkat lunak yang dirancang dengan tujuan untuk masuk dan menyusupi sebuah sistem komputer, kemudian akan merusak sistem komputer tersebut. *Malware* dapat menyusup ke banyak komputer melalui jaringan *internet* seperti *e-mail*, *download file* dari *internet*, atau melalui program yang terinfeksi **(**Tedyyana & Supria, 2018**).** *Malware* yang dimaksut bisa dalam bentuk *virus*, *worm* dan *trojan* merupakan ancaman utama bagi keamanan sistem jaringan komputer. *Honeypot Dionaea* akan berpura-pura menjadi sumber daya yang memikat perhatian penyerang dalam suatu jaringan yang sama.

Teknik pengamanan jaringan biasanya dengan memblokade serangan dengan *firewall* atau mendeteksi serangan yang ada dengan *IDS* (*Intrusion Detection System*) yang bertugas untuk menjaga dari

serangan-serangan yang ada. Menurut (Sutarti et al., 2018) *Intrusion Detection System* (*IDS*) adalah sebuah sistem yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. Namun *IDS* sendiri tidak serta merta dapat menahan serangan para penyerang. Selain menggunakan cara konvensional tersebut pengamanan sistem jaringan dapat menggunakan *Honeypot*. Implementasi *Honeypot low interaction* memanfaatkan dua aplikasi yang berbeda, yaitu *Dionaea* dan *Honeyd* berhasil membuat layanan palsu sebagai target serangan dan mencatat aktivitas yang dianggap dapat membahayakan sistem dan jaringan, namun tidak adanya interaksi lebih lanjut ketika penyerang berhasil mengeksploitasi dan masuk dalam *Honeypot* (Arkaan & Sakti, 2019).

Dionaea adalah jenis *Honeypot* yang bersifat *Low Interaction Honeypot,* yang diciptakan sebagai pengganti *Nepenthes*. *Dionaea* termasuk kategori dari *low-interaction Honeypot* terbaru yang merupakan suksesor dari *Nephentes*. *Honeypot Dionaea* dengan lisensi *open source* merupakan salah satu varian dari beberapa *low-interactioan Honeypot* seperti *Nephentes*, *HoneyD*, dll. yang termasuk kedalam kategori *Honeypot low-interaction*. Karena *Dionaea* dapat menentukan *host* yang terinfeksi *malware* lebih awal, maka host dapat memberhentikan penyebaran *malware* tersebut ke *host* lain dalam jaringan secara cepat. Dari masalah dan kerentanan yang timbul pada lingkup keamanan jaringan maka akan diimplementasikan *low-interaction Honeypot Dionaea* secara *virtual*.

Dengan diterapkannya *Honeypot Dionaea* kedalam suatu jaringan komputer *server* lokal, maka akan meningkatkan pengamanan port secara berlapis, dengan mengandalkan kamuflase port maka pelaku (penyerangan jaringan) yang mencoba untuk mencari celah atau mencoba mencuri data rahasia *server* dan *client* pada komputer *server* tidak akan bisa menembus port yang dilakukan serangan, dengan begitu akses komputer *server* tidak akan diambil alih dengan mudah oleh para peretas (pelaku penyerangan jaringan).

Tidak berhenti sampai disitu, meskipun serangan yang dilancarkan oleh penyerang tidak dapat menembus *port* asli dari komputer *server* tersebut, namun *Honeypot Dionaea* akan tetap menyimpan informasi komputer peretas. Jenis-jenis serangan yang dilancarkan oleh penyerang juga akan dapat dengan mudah diketahui oleh *Administrator* jaringan. *Honeypot Dionaea* akan sangat membantu pekerjaan seorang *Administrator* jaringan secara langsung maupun tidak langsung dengan mengandalkan indikator berbasis *CLI* dan *GUI* pada *web server Honeypot Dionaea Catches Bug*, dengan begitu seorang *Administrator* jaringan akan dengan mudah menentukan penyerang komputer server tersebut dan melakukan tindak hukuman yang sesuai dengan sebagaimana mestinya atau setara dengan peraturan perundang-undangan teknologi dan informasi yang berlaku di Indonesia apabila telah membuat kerugian secara serius baik dalam skala individu maupun skala besar (Instansi, Perusahaan, Universitas, dll).

Honeypot Dionaea dapat disimulasikan juga melalui *VM (Virtual Machine)* yang dimana akan lebih mempermudah penerapannya sebelum pada akhirnya diterapkan pada sebuah jaringan komputer yang nyata, baik skala jaringan kecil maupun besar. Dengan menggunakan *VM* seorang *Administrator* jaringan hanya mempersiapkan 1 buah komputer yang digunakan sebagai *Host*, sistem operasi *Honeydrive 3* sebagai layanan *Honeypot* dan *Kali linux* sebagai *penetration testing*. Dengan spesifikasi kebutuhan yang terbatas akan lebih mempermudah dalam simulasi proses penyerangan dan pertahanan secara nyata, serta seorang *Administrator* jaringan dapat mempelajari lebih dalam terkait *trial and error* sebelum *Honeypot Dionaea* diimplementasikan secara nyata.

Dengan seiring berkembangnya kemajuan teknologi membuat *Honeypot Dionaea* menjadi salah satu metode layanan yang dapat mengikuti perkembangan jenis-jenis metode serangan eksploitasi dan

penetrasi, sehingga tentunya *Honeypot Dionaea* menjadi sistem kemanan jaringan yang dapat diandalkan untuk saat ini.

Dari celah-celah keamanan yang muncul terutama melalui *port* jaringan, maka penulis menggunakan *Honeypot Dionaea* sebagai salah satu terobosan besar dalam menampik kerentanan-kerentanan *port* jaringan khususnya *port SMB* yang akan dibahas pada penelitian skripsi ini dan juga lebih meningkatkan keamanan pada komputer, terutama komputer *server*.

1.2. Rumusan Masalah

Rumusan masalah yang ditimbulkan berdasarkan situasi dan kondisi nyata serangan pada sebuah keamanan *port* komputer *server* adalah:

a. Apa saja bentuk serangan terhadap *port* komputer *server* sehingga dapat mengambil alih akses secara sebagaian maupun keseluruhan?
b. Mengapa komputer *server* menjadi sasaran penyerangan peretas?
c. Bagaimana cara meningkatkan keamanan *port* komputer *server* menggunakan *Honeypot Dionaea*?

1.3. Tujuan

Tujuan yang ingin dicapai dalam penulisan proposal skripsi ini adalah meningkatkan sistem keamanan jaringan terbaru dengan mengimplementasikan *Honeypot Dionaea* pada komputer *server*. Menguji kinerja dan keefektifan *Honeypot Dionaea* dengan melakukan simulasi serangan dan memonitoring dan mencatat aktivitas serangan yang masuk ke jaringan komputer menggunakan *localhost web Honeypot DionaeaFR.*

Dengan diimplementasikan sistem *Honeypot* tersebut, sebuah *port* manipulasi dapat melayani serangan yang dilakukan oleh peretas dalam melakukan penetrasi terhadap komputer yang diduga sebagai server tersebut. Sehingga komputer *server* akan lebih terjaga keamanannya dari segala celah-celah yang ada khususnya celah kerentanan dari sebuah *port.*

Dengan diimplementasikan *Honeypot Dionaea* dapat memberikan manfaat secara langsung dan tidak langsung. Salah satu manfaat secara langsung yakni membuat jaringan dan *port* pada komputer menjadi lebih aman dan terpantau, sedangkan manfaat secara tidak langsung dari pengimplementasian *Honeypot Dionaea* yakni keamanan data pada *storage server* akan menjadi lebih terjaga dari pihak yang berusaha melakukan peretasan. Dengan simulasi yang dilakukan secara *virtual*, maka spesifikasi perangkat keras yang dibutuhkan juga terbatas.

1.4. Manfaat Penelitian

Adapun manfaat yang diharapkan dari hasil penelitian proposal skripsi ini untuk penulis dan pembaca adalah sebagai berikut:

a. Bagi Penulis:

Meningkatkan sistem keamanan jaringan terbaru pada komputer *server* baik pada lingkup jaringan skala kecil maupun besar dengan mengimplementasikan *Honeypot Dionaea* secara *virtual* maupun nyata.

b. Bagi Pembaca:

Penelitian proposal skripsi ini dapat menjadi referensi bagi pembaca (masyarakat umum) yang berprofesi sebagai *administrator* jaringan atau sekedar memiliki bidang minat pada keamanan jaringan komputer baik secara skala kecil maupun besar guna menambah ruang lingkup pengetahuan dalam hal melindungi dan mengamankan jaringan komputer khususnya perangkat *server*.

1.5. Batasan Penelitian

Batasan penelitian pada Implementasi *Dionaea* pada *Low Interaction Honeypot* Sebagai Penunjang Keamanan Jaringan adalah sebagai berikut:

a. Serangan hanya akan dilakukan pada komputer yang berada pada jaringan skala kecil, yakni tersusun dari 1 komputer dengan menggunakan 2 buah sistem operasi *virtual* (*Honeydrive 3* dan *Kali linux*) serta 1 buah *router* yang digunakan sebagai penghubung jaringannya. Pengimplementasian *Honeypot Dionaea* dilakukan secara *virtual*isasi dengan menggunakan *VirtualBox.*

b. Simulasi penyerangan dengan menggunakan *Honeypot Dionaea* diawali dengan *scanning port TCP* dengan menggunakan *tools NMAP* lalu melakukan eksploitasi terhadap *port* 445 *SMB* dan *port* 135 *RPC* dengan metode eksploitasi *Metasploit* sebagai berikut: *MS06_040_Netapi, MS04_011_LSASS, MS03_026_DCOM*

c. Menggunakan sumber daya sistem operasi *Kali linux* sebagai penyerang dan sistem operasi *Honedrive 3* dengan *Dionaea* yang bertindak sebagai sasaran serangan.