BAB 1
PENDAHULUAN

1.1 LATAR BELAKANG

Pada era digital, *internet* menjadi salah satu teknologi yang paling dibutuhkan hampir di seluruh dunia, termasuk Indonesia. Segala informasi dapat dikirim dan diterima ke seluruh penjuru dunia hanya dengan menggunakan jaringan *internet*. Dalam hal ini, *internet* memiliki peran yang sangat penting dalam membantu aktivitas dan proses bisnis manusia. Selaras dengan Laporan Survei Asosiasi Penyelenggara Jasa *Internet* Indonesia (APJII), pengguna *internet* di Indonesia pada tahun 2019 - 2020 Kuartal II mencapai 73,7% atau 196,71 juta penduduk Indonesia (Asosiasi Penyelenggara Jasa Internet Indonesia, 2020). Kemajuan *internet* juga menumbuhkan inovasi bagi perusahaan untuk mulai menyiarkan iklan daring produk melalui *internet*. Iklan daring yang disebarluaskan melalui *internet*, yang biasa disebut iklan daring, merupakan salah satu cara paling efektif bagi pengiklan daring menjangkau berbagai jenis audien dan tidak terhalang oleh jarak, serta biaya yang dikeluarkan jauh lebih terjangkau dibandingkan dengan metode pengiklan yang dilakukan dengan media tradisional (Bermudez-Villalva, Musolesi and Stringhini, 2020).

Namun, kejahatan siber pada era digital bisa terjadi dimana saja, termasuk kejahatan yang memanfaatkan iklan daring pada situs *web* sebagai umpan untuk menarik audiens. Iklan daring menjadi target untuk dieksploitasi, membuat iklan daring yang dibuat secara berlebihan sehingga mengganggu kenyamanan pengguna atau *client*. Bahkan iklan daring dapat dieksploitasi para kriminal siber dengan menyisipkan *malware* pada iklan daring untuk menyerang perangkat korbannya (Rolon, Hinds and Doswell, 2019) (Hopkins and Dehghantanha, 2016). Kejahatan yang memanfaatkan iklan daring disebut juga dengan *malicious advertising* atau *malvertising*. *Malvertising* memiliki mekanisme yang lebih kuat dibandingkan dengan metode penyebaran lainnya, karena iklan daring memiliki kepercayaan tersirat antara pihak yang terlibat dalam penayangan iklan daring tersebut (Kumar,

Rautaray and Pandey, 2018) Selain itu, *malvertising* juga memungkinkan penyebaran *malware* atau serangan lainnya, dengan interaksi dari pengguna maupun tanpa interaksi dari pengguna ((Huang et al., 2017. Salah satu upaya yang pernah digunakan untuk menangani *malvertising* adalah perangkat lunak *ad-blocker*. Menurut survei yang dilakukan oleh PageFair, lebih dari 600 juta perangkat menjalankan perangkat lunak pemblokiran iklan daring secara global pada tahun 2016. Meskipun upaya pemblokiran dapat mengurangi beberapa masalah yang ditimbulkan oleh *malvertising*, tetapi jika dilakukan dalam jangka panjang akan menghancurkan struktur yang mendasari iklan daring itu sendiri, yaitu memutus pendapatan pengiklan daring yang dihasilkan dari iklan daring (Wang *et al.*, 2017).

Menurut penjelasan di atas, dapat dikatakan bahwa serangan *malvertising* dapat terjadi di situs *web* besar sekalipun. Maka dari itu, *malvertising* perlu ditangani dengan menerapkan teknik inspeksi pada iklan daring yang dikirimkan, termasuk melakukan pemantauan secara langsung atau analisis kode didalamnya. Hal ini dibuktikan dalam penelitian mengenai *malvertising* yang dilakukan oleh Chin-Tser Huang, bertujuan untuk merumuskan masalah dalam menginspeksi *malvertising*. Penelitian dilakukan dengan menerapkan model teori *game* Bayesian dan menyajikan dua *game* Bayesian antara *malvertiser* dan jaringan iklan daring berbasis web (Huang *et al.*, 2018). Penelitian lainnya dilakukan oleh Muhammad N. Sakib, dimana peneliti membuat sistem otomatisasi yang meniru aktivitas penelusuran berisiko tinggi seperti mengklik iklan daring mencurigakan sehingga dapat dianalisis dan diagnosis lebih lanjut. Sistem tersebut menangkap *source code* HTML, JavaScript, dan Action Script dari iklan daring mencurigakan sehingga dapat dianalisis mengenai pola *malvertising* sebelum akhirnya dieksekusi (Sakib and Huang, 2015). Penelitian tentang *malvertising* juga dilakukan oleh Joshua Rolon, yang bertujuan membuat sistem lapisan pertahanan terhadap *malvertising* menggunakan SpartanShield, yaitu konfigurasi penjelajahan *web* dari ekstensi Browser Brave *ad-blocker*, uBlock Origin *ad-blocker*, dan *sinkhole* DNS Pi-Hole (Rolon, Hinds and Doswell, 2019).

Sistem yang dilakukan oleh Joshua Rolon mengenai sistem pertahanan *malvertising* menggunakan SpartanShield, menunjukkan bahwa sistem tersebut bukan merupakan langkah efektif dalam mengurangi risiko serangan *malvertising*. Hal ini karena SpartanShield belum cukup mendukung tiga *platform desktop* utama, yaitu Windows, Linux, dan MacOS, sehingga *platform* yang SpartanShield pilih untuk dapat digunakan hanya pada penyedia virtualisasi, seperti VirtualBox dan Vagrant (Rolon, Hinds and Doswell, 2019). Maka dari itu, untuk mengurangi tingkat risiko pengguna dari serangan *malvertising*, penulis bermaksud untuk mengembangkan sistem pertahanan jaringan dari serangan *malvertising* berbasis *web* menggunakan Pi-Hole. Implementasi sistem tersebut diterapkan secara *wide system*, dalam artian tidak bergantung pada perangkat *client* atau sistem operasi tertentu, melainkan terhadap infrastruktur utama pada jaringan. Implementasi sistem digunakan untuk menghalau iklan daring yang disebarkan melalui situs *web*, sehingga diharapkan sistem tersebut dapat menurunkan potensi serangan *malvertising* yang terjadi pada situs *web*.

1.2 PERUMUSAN MASALAH

Berlandaskan latar belakang di atas, dapat dirumuskan sebuah permasalahan penelitian, yaitu tersebarluasnya serangan siber yang memanfaatkan jaringan iklan daring, atau disebut juga dengan *malvertising*. Serangan *malvertising* berisiko terjadi serangan siber lainnya, seperti penyebaran *malware*, dan menurunkan tingkat efektivitas pada situs *web* dan aplikasi *mobile* itu sendiri karena pengguna merasa iklan daring tersebut mengganggu aktivitas *browsing*. Walaupun telah dilakukan upaya mengurangi risiko malvertising dengan perangkat lunak *ad-blocker*, justru jika dilakukan dalam jangka panjang akan menghancurkan struktur dasar dari iklan daring, yaitu berhentinya pendapatan yang dihasilkan dari iklan daring.

1.3 PERTANYAAN PENELITIAN

Berdasarkan rumusan masalah, maka dapat dijabarkan menjadi beberapa pertanyaan penelitian, antara lain:

1. Bagaimana mengimplementasikan Pi-Hole dalam membangun sistem pertahanan untuk memerangi *malvertising*?
2. Bagaimana sistem pertahanan menggunakan Pi-Hole dapat mengurangi risiko serangan *malvertising* pada situs *web*?
3. Bagaimana mengetahui tingkat efektivitas pada sistem pertahanan menggunakan Pi-Hole dalam memerangi serangan *malvertising*?

1.4 TUJUAN PENELITIAN

Adapun tujuan dari penelitian ini yaitu membangun sistem pertahanan jaringan dari serangan *malvertising* dengan mengimplementasikan Pi-Hole ke dalam infrastruktur utama jaringan. Pengembangan sistem ini dilakukan karena belum ada penelitian yang membuat sistem pertahanan yang menggunakan Pi-Hole. Sistem ini diujikan pada situs *web* dan aplikasi *mobile* yang pada umumnya terdapat banyak iklan daring yang mengganggu.

1.5 MANFAAT HASIL PENELITIAN

Manfaat yang diperoleh berdasarkan penelitian yang dilakukan, yaitu mengurangi tingkat risiko serangan *malvertising* pada saat mengakses situs *web* dan aplikasi *mobile*. Sistem penghalauan pada penelitian ini dapat diterapkan pada berbagai sektor diantaranya, perkantoran, rumah, pendidikan, dan tempat usaha lainnya. Dengan terhubungnya sistem ini, pengguna diharapkan dapat merasa lebih nyaman melakukan akses *internet* tanpa adanya iklan daring yang mengganggu.