BAB 3
METODE PENELITIAN

3.1 BAHAN PENELITIAN

Bahan yang digunakan dalam penelitian yaitu data akses pada *domain* situs *web* yang disisipkan iklan daring mengganggu (*malvertising*) maupun tidak. Pada penelitian ini mengambil 22 objek untuk dilakukan analisis perbandingan. Objeknya adalah situs *web* yang diakses pada perangkat PC (*Personal Computer*) sebanyak 10 situs *web*. 12 objek lainnya berasal dari perangkat *smartphone*, diantaranya aplikasi yang berjalan pada *smartphone* dan situs *web*.

Pada penelitian ini mengimplementasikan sistem pertahanan jaringan dari serangan *malvertising* menggunakan Pi-Hole yang diinstal pada perangkat Raspberry Pi 3 model B+. Sistem tersebut dipasangkan pada jaringan *internet* FTTI Universitas Jenderal Achmad Yani Yogyakarta. Pengambilan data dilakukan pada tanggal 26 Juli sampai dengan 8 Agustus 2022. Maka dari itu, data akses yang dimaksud yaitu data *log query* yang ditangkap oleh Pi-Hole.

3.2 ALAT PENELITIAN

Penelitian dilakukan berdasarkan pada berbagai literatur terkait teori dasar keamanan jaringan. Pada penelitian ini, alat yang digunakan dalam penelitian dapat dispesifikasikan sebagai berikut.

3.2.1 Raspberry Pi

Raspberry Pi adalah salah satu jenis SBC *(Single Board Computer)* yang memiliki ukuran sebesar kartu kredit. Raspberry Pi pertama kali dikembangkan oleh Raspberry Pi Foundation di Inggris pada tahun 2011(Prabowo, 2015). Pada tahun 2012, Raspberry Pi Foundation meluncurkan SBC pertamanya yaitu Raspberry Pi 1. Diikuti oleh Raspberry Pi 2 dan Raspberry Pi Zero yang diluncurkan pada tahun 2015. Lalu Raspberry pi 3 yang diluncurkan pada tahun 2016. Sampailah pada seri terbarunya yaitu Raspberry 4 yang diluncurkan pada tahun 2020 silam. Di dalam setiap seri Raspberry Pi memiliki empat model, antara

lain model A, model A+, model B, dan model B+. Masing-masing model memiliki fitur yang sedikit berbeda, dan ukuran dimana model A memiliki ukuran yang lebih kecil dibandingkan dengan model B(*Tutorialspoint Simply Easily Learning*, 2021). Raspberry Pi memiliki fungsi yang sama layaknya sebuah komputer dan memiliki kemampuan untuk menjalankan sistem operasi berbasis Linux dan berbagai jenis aplikasi yang ada di dalamnya, seperti *multimedia*, *programming*, bahkan untuk melakukan pemrosesan data seperti tulisan, gambar, *audio*, dan *video*(Wijaya, 2017).

Gambar 3.1 Raspberry Pi 3 Model B+

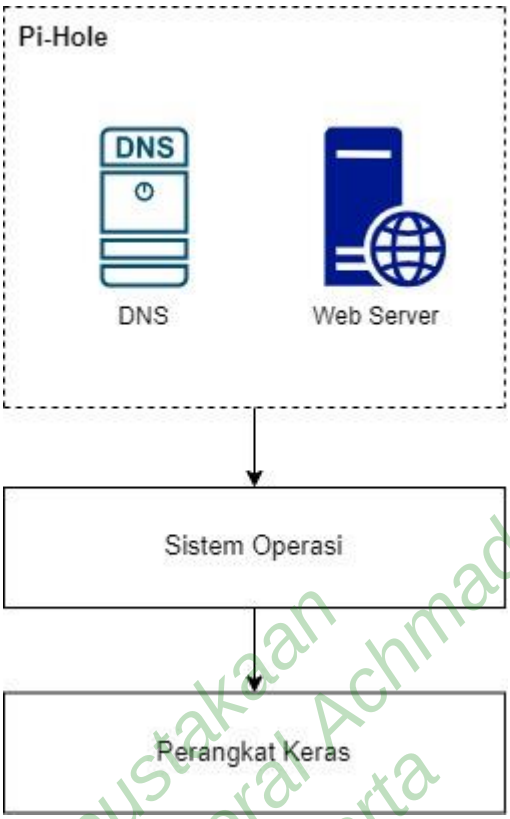
Seri yang digunakan pada penelitian ini adalah Raspberry Pi 3 model B+ seperti yang ditunjukkan pada Gambar 3.1. Seri tersebut memiliki mikroprosesor berupa SoC *(System-on-a-Chip)* jenis Broadcom BCM2837B0, CPU Cortex-A53 64-bit, dan kecepatan prosesor sebesar 1.4 GHz. Perangkat tersebut memiliki RAM sebesar 1GB dan mendukung penyimpanan eksternal berupa MicroSD. Pada penelitian ini menggunakan MicroSD SanDisk berukuran 16GB. Sementara itu, Raspberry Pi 3 model B+ juga memiliki beberapa *port* tambahan, seperti konektor HDMI untuk menghubungkan antara perangkat dengan *monitor*. Selain itu, memiliki *port* USB tipe 2.0 GHz sebanyak empat buah, beserta satu buah MicroUSB untuk pengisian daya pada perangkat. Raspberry Pi 3 model B+ memiliki *port Ethernet* untuk menghubungkan perangkat ke jaringan *internet* berupa LAN dengan menggunakan kabel sebesar 10/100 Mbit/s. Namun, perangkat Raspberry Pi tidak memiliki sistem operasi bawaan sehingga setiap penggunanya

harus melakukan instalasi sistem operasi yang dilakukan *burn* dalam MicroSD, Pada penelitian ini menggunakan sistem operasi Raspberry Pi OS Lite yang merupakan CLI *(Command Line Interface)* atau disebut juga sebagai *headless interface*.

3.2.2 Pi-Hole

Pi-Hole adalah program yang berfungsi sebagai DNS *sinkhole* untuk melindungi perangkat pada jaringan dari konten yang tidak diinginkan, misalnya iklan daring mengganggu atau *malvertising*. Berbeda dengan *ad-blocker* yang hanya akan bekerja ketika perangkat menginstal *plugin* tersebut, Pi-Hole menghalau iklan daring dengan melakukan penyaringan seluruh trafik *internet* ke semua perangkat yang menggunakan DNS *server* Pi-Hole. Hal ini terjadi karena pada awalnya *client* mendapatkan IP, *gateway*, dan DNS dari *router*, tetapi hanya DNS saja yang diubah menjadi DNS yang diberikan oleh Pi-Hole karena Pi-Hole pada dasarnya dapat membuat server DNS-nya sendiri(Wahyudi, Diansyah and Handoko, 2020).

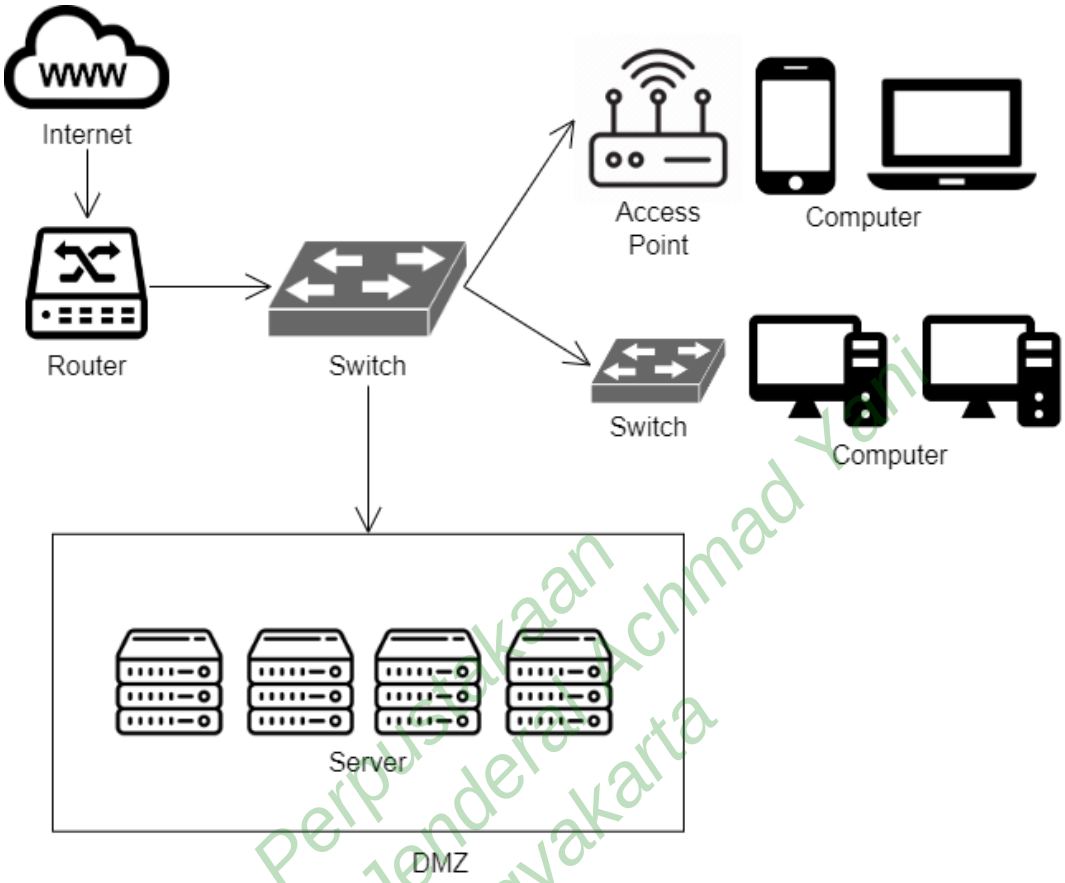
Pi-Hole bekerja sebagai *blackhole* atau lubang hitam bagi *malvertising* yang ada di situs *web* dan aplikasi *mobile*. Secara teknis, Pi-Hole menerima DNS *request* dari *client* yang menggunakan jaringan tersebut. Kemudian Pi-Hole akan membentuk daftar kosong untuk kategori *blacklist* pada *domain* yang diakses oleh *client*. *Blacklist* berfungsi untuk mengumpulkan data *query* yang terblokir oleh Pi-Hole, dalam hal ini adalah *malvertising*. Pi-Hole menangkap seluruh *query* yang masuk, dan secara otomatis memasukkan *domain* yang dicurigai sebagai *malvertising* masuk ke dalam daftar *blacklist*. Seluruh *malvertising* yang masuk ke dalam *blacklist* tidak akan dilepaskan ke perangkat *client* yang mengakses situs menggunakan *router* yang telah dikonfigurasikan dengan Pi-Hole. Di samping itu, Pi-Hole akan melepaskan *query* yang tidak termasuk pada daftar dan *client* dapat mengakses *domain* tanpa terganggu dengan adanya serangan *malvertising*(Habibi, 2022).



Gambar 3.2 Arsitektur Pi-Hole

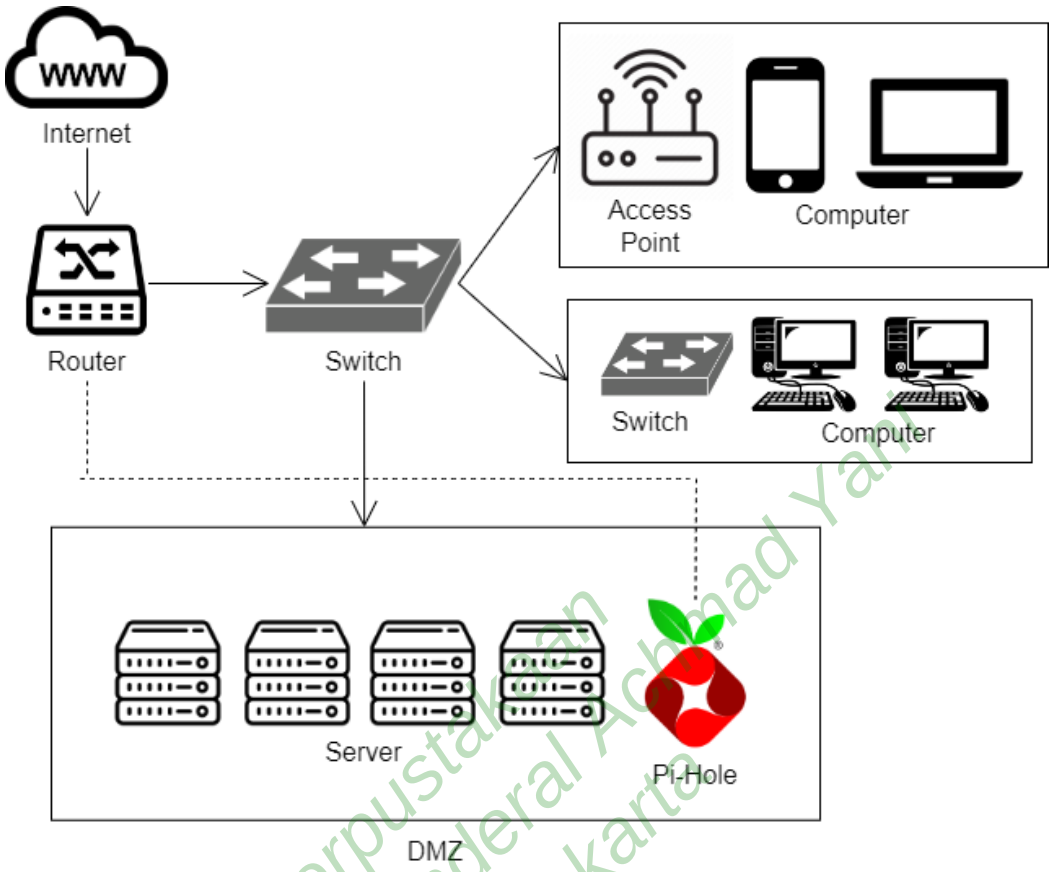
Arsitektur pada Pi-Hole ditunjukkan dalam Gambar 3.2. Pada penelitian ini, Pi-Hole berjalan dalam sistem operasi Raspberry Pi OS atau Pi OS. Kemudian layanan yang berjalan pada Pi-Hole yaitu *web server* dan DNS. *Web server* adalah perangkat lunak yang berjalan di sisi *server* dan bertanggung jawab menerima permintaan dari *web browser*, mengelola permintaan tersebut, kemudian dikirimkan kembali hasil permintaan tersebut ke *web browser*. Pada penelitian ini menggunakan *web server* berupa Lighttpd(Dawood, Qiana and Muchallil, 2014). Sementara itu, Pi-Hole menggunakan dnsmasq. Dnsmasq merupakan perangkat lunak yang menyediakan layanan DNS *caching*, dengan kata lain menyimpan alamat IP dari seluruh situs yang diakses *client*(Valkeinen, 2018).

3.3 JALAN PENELITIAN



Gambar 3.3 Topologi Jaringan Sebelum Implementasi Sistem Pertahanan Menggunakan Pi-Hole

Berdasarkan Gambar 3.3, *router* menangkap semua informasi dan data secara langsung dari *internet*, kemudian disalurkan ke perangkat lainnya yang terhubung, seperti *switch*, dan perangkat lainnya. Sementara itu, informasi yang ditangkap oleh *router* tidak melalui proses penyaringan konten iklan daring yang mengganggu atau *malvertising*. Ketika *client* mengakses *internet* melalui *router* tersebut, semua iklan daring tetap bermunculan. Pada kemungkinan terburuknya, iklan daring dapat disisipi *malware* sebagai media untuk menyerang para korbannya. Bahkan, *router* membiarkan situs dengan konten negatif dapat diakses oleh *client*(Rolon, Hinds and Doswell, 2019).

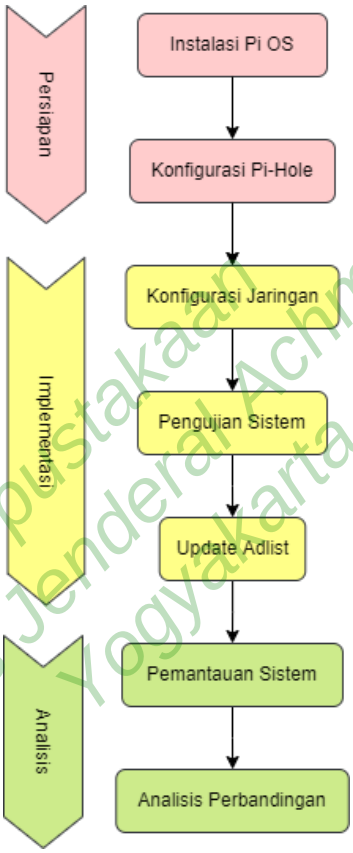


Gambar 3.4 Topologi Jaringan dengan Implementasi Sistem Menggunakan Pi-Hole

Berdasarkan Gambar 3.4 menunjukkan bahwa Pi-Hole yang telah diinstal ke perangkat Raspberry Pi 3 model B+, kemudian dikonfigurasikan dengan IP *router*. Hal ini dikarenakan *router* lah yang menjadi penghubung utama antara *internet* dan perangkat komputer. *Router* memiliki beberapa fitur, diantaranya DHCP (*Dynamic Host Configuration Tool*) dan NAT (*Network Address Translator*). DHCP merupakan layanan yang bertugas mendistribusikan alamat IP kepada perangkat komputer. Sementara itu, NAT memungkinkan suatu alamat IP yang diakses dapat dibagikan ke perangkat komputer lain. Dalam hal ini, alamat IP yang diperoleh dapat menjadi penghubung antara suatu perangkat ke perangkat lainnya(Ardianto, 2020).

Sistem yang dibangun menggunakan Pi-Hole ini bekerja dengan cara *filtering* seluruh trafik akses *internet* yang dilakukan oleh *client*. Pi-Hole yang dikonfigurasikan ke *router* menyebabkan semua perangkat yang terhubung ke

router akan mendapatkan alamat IP dan *gateway* dari *router*. Namun tidak dengan DNS, melainkan DNS akan diberikan dari Pi-Hole. Dengan demikian, semua informasi data situs yang ditangkap *router* dikirimkan ke Pi-Hole dan proses *filtering* dapat berjalan. Maka dari itu, berdasarkan tujuan penelitian ini, pengembangan sistem pertahanan untuk memerangi serangan *malvertising* dilakukan dengan alur penelitian seperti pada Gambar 3.5.



Gambar 3.5 Alur Penelitian

Penelitian dilakukan dengan menjalankan tiga tahapan utama, yaitu tahapan persiapan, tahapan implementasi, dan tahapan analisis. Tahapan persiapan pada penelitian ini antara lain melakukan instalasi sistem operasi untuk perangkat Raspberry Pi 3 model B+ dan melakukan konfigurasi Pi-Hole. Sistem operasi yang digunakan untuk diinstalasi pada perangkat tersebut yaitu Raspberry Pi OS Lite. Sistem operasi di-*burn* pada MicroSD SanDisk yang berukuran 16GB. Penelitian menggunakan versi Lite karena tidak memerlukan sistem operasi dengan tampilan GUI (*Graphical User Interface*), melainkan menggunakan CLI (*Command Line*

Interface) atau disebut juga dengan *headless interface*. Selain itu, mempersiapkan *terminal emulator* guna mempermudah penelitian dalam melakukan konfigurasi lanjutan yang akan dijalankan secara *remote* menggunakan perangkat komputer lainnya. Pada penelitian ini menggunakan perangkat lunak PuTTY. Di samping itu, PuTTY juga mempermudah penelitian dalam mengimplementasikan Pi-Hole ke dalam perangkat Raspberry Pi 3 model B+. Proses konfigurasi Pi-Hole dijalankan dengan menjalankan beberapa *command line*.

Tahapan kedua yaitu tahapan implementasi. Tahapan yang dilakukan pertama kali yaitu melakukan konfigurasi jaringan pada Raspberry Pi 3 model B+. Pada penelitian melakukan proses pengaturan DHCP (*Dynamic Host Configuration Protocol*) *server*, guna mempermudah mendistribusikan alamat IP dari *client* secara otomatis selama berada pada satu jaringan *internet* yang sama. Selain itu, melakukan konfigurasi SSH pada Raspberry Pi 3 model B+ dan pengubahan DNS Raspberry Pi menjadi DNS Pi-Hole, sehingga *client* akan mendapatkan DNS milik Pi-Hole. Hal ini dilakukan agar seluruh akses pada *port* 53 dialihkan menuju Pi-Hole, dan Pi-Hole dapat merekam seluruh trafik dan masuk ke dalam data *query* yang dicatat dalam sistem.

Tahapan implementasi dilanjutkan dengan melakukan pengujian sistem yang sudah dikembangkan sebelumnya. Raspberry Pi 3 model B+ yang sudah terpasang Pi-Hole ditanamkan pada DMZ (*demilitarized zone*), yaitu sebuah wilayah pada jaringan yang berfungsi melindungi sistem dari serangan peretas yang mencoba masuk ke dalamnya tanpa memiliki hak akses (Webb, 2015). Pada penelitian ini, sistem disematkan dalam jaringan *internet* FTTI Universitas Jenderal Achmad Yani Yogyakarta. Proses pengujian sistem juga dilakukan dengan memastikan apakah sistem berjalan sesuai dengan rencana, sehingga proses pengambilan data dapat dilakukan.

Pada tahapan ini, perlu melakukan *update* secara berkala *adlist*. *Adlist* merupakan daftar *domain* yang terkait dengan layanan iklan daring yang dapat disisipkan pada situs *web* atau aplikasi yang berbasis *web*. Pada dasarnya, iklan daring yang muncul dalam situs *web* tidak serta merta berupa iklan yang muncul pada halaman tersebut, tetapi juga pada saat *client* klik sebuah *link*, justru *web* tidak

membuka alamat yang dituju, melainkan dialihkan atau *redirect* ke halaman *web* lainnya yang merupakan *domain* terkait layanan iklan daring. Prinsip dasar inilah yang mendasari pentingnya melakukan penambahan *adlist*.

Penambahan *adlist* dapat diatur oleh pengelola jaringan. Implementasi *adlist* sendiri dilakukan dengan cara memasukkan *domain* yang dapat dimodifikasi oleh *admin* dalam perizinan akses oleh *client* saat menggunakan jaringan *internet* tersebut. Selain memblokir *malvertising*, Pi-Hole juga memiliki fitur *blacklist* yang berfungsi untuk mempermudah *admin* memblokir situs pornografi, situs judi *online*, dan sebagainya. Namun demikian *update* pada *adlist* dan *blacklist* harus dilakukan secara *manual* oleh *admin*, dan pelaksanaan *update* harus dilakukan secara berkala. Pada penelitian ini, proses *update adlist* berjalan setiap satu minggu sekali. Dalam pencarian situs yang ingin diblokir melalui *adlist* juga mudah ditemukan situs berbasis komunitas yang mengumpulkan situs-situs yang harus dimasukkan ke dalam *adlist* untuk dilakukan pemblokiran.

Tahapan terakhir yaitu melakukan analisis dari DNS *query* pada rentang waktu 26 Juli sampai dengan 5 Agustus 2022. Pertama-tama, tahapan analisis dimulai dengan pemantauan sistem terhadap setiap data yang ditangkap oleh Pi-Hole. Dalam hal ini, data yang ditangkap merupakan data pengaksesan yang dilakukan *client* selama menggunakan jaringan *internet* FTTI Universitas Jenderal Achmad Yani Yogyakarta. Pemantauan ini dijalankan bersamaan dengan pengumpulan data akses *internet client* yang dicatat oleh Pi-Hole dan ditampilkan melalui *dashboard* Pi-Hole. Di dalam *dashboard*, pengelola jaringan dapat memantau trafik akses *internet* yang ditangkap Pi-Hole. Hal ini meliputi seluruh situs yang diakses, berapa perangkat yang mengakses, berapa *domain* yang diakses, dan seluruh *malvertising* yang berhasil diblokir dan dimasukkan ke dalam *blacklist*. Pengelola jaringan juga dapat melihat daftar URL yang sudah ditambahkan ke dalam *adlist* dan melakukan modifikasi terhadap daftar-daftar tersebut.

Pada tahapan analisis juga melakukan klasifikasi akses dari *client* yang diantaranya, penghalauan *malvertising*, penghalauan konten ilegal, dan konten yang diperbolehkan atau dinyatakan telah bersih dari *malvertising*. Penelitian mengambil 20 situs *web* dan 2 aplikasi *mobile*. Hal ini bertujuan sebagai analisis perbandingan

terkait 22 objek yang dibuka sebelumnya terkena serangan *malvertising*, kemudian situs-situs tersebut diakses kembali setelah sistem pertahanan dengan Pi-Hole ini diimplementasikan pada jaringan FTTI Universitas Jenderal Achmad Yani Yogyakarta. Maka dari itu, dapat dinyatakan bahwa sistem pertahanan yang dikembangkan berhasil mengurangi potensi serangan *malvertising*.