BAB II
KAJIAN PUSTAKA

2.1 Teori Dasar

Teori dasar menjelaskan definisi dan hal mendasar mengenai jaringan. Secara umum, teori adalah suatu penalaran yang merupakan gabungan dari definisi dan konsep yang disusun secara sistematis (Sudaryono, 2015). Berikut adalah penjelasannya tentang jaringan komputer, standar dan jenis jaringan komputer, model lapisan OSI (*Open System Interconnection*), *Honeypot*, dan *Raspberry Pi*.

2.1.1 Jaringan Komputer

Jaringan komputer adalah sekumpulan komputer yang saling terkoneksi dengan tujuan pembagian data dan sumber daya jaringan. Dengan adanya pengembangan internet, teknologi jaringan pun dapat digunakan secara *mobile*. Pengembangan yang cepat ini menyebabkan transisi dari transmisi data dengan kabel berubah menjadi nirkabel yang sifatnya lebih fleksibel dan cocok untuk penggunaan *mobile* (Malhotra, Gupta, & K Bansal, 2011).

2.1.2 Standar Jaringan Komputer

Standarisasi jaringan komputer diselenggarakan oleh ISO (*International Organization for Standardization*), ANSI (*American National Standard Institute*),

ITU (*International Telecommunication Union*), NCITS (*National Committee for Information Technology Standardization*), dan lembaga IEEE (*Institute of Electrical and Electronics Engineers*). Berikut adalah standar jaringan telekomunikasi yang dibuat oleh IEEE (Maslan & Wangdra, 2012):

1. IEEE802.1 merupakan standarisasi *interface* lapisan atas HILI dan *Data Link* (*Medium Access Control* dan *Logical Link Control*).
2. IEEE802.2 merupakan standarisasi lapisan LLC/*Logical Link Control*.
3. IEEE802.3 merupakan standarisasi lapisan MAC/*Medium Access Control* untuk CSMA/CD. Standar ini merupakan generasi pertama dari Ethernet dengan kecepatan 10Mbps (Malhotra et al., 2011).
4. IEEE802.4 merupakan standarisasi lapisan MAC untuk *Token Bus.*
5. IEEE802.5 merupakan standarisasi lapisan MAC untuk *Token Ring*.
6. IEEE802.6 merupakan standarisasi lapisan MAC untuk MAN-DQDB/*Metropolitan Area Network-Distributed Queue Dual Bus*.
7. IEEE802.7 merupakan kelompok pendukung *Broadband Technical Advisory Group* pada jaringan LAN.
8. IEEE802.8 merupakan kelompok pendukung *Fiber Optic Technical Advisory Group*.
9. IEEE802.9 merupakan standarisasi ISDN (*Intergrated Services Digital Network* dan IS (*Integrated Services*) pada jaringan LAN.
10. IEEE802.10 merupakan standarisasi dari masalah pengamanan jaringan LAN.

11. IEEE802.11 merupakan standarisasi dari masalah WLAN (*Wireless* LAN) dan CSMA/CD.
12. IEEE802.12 merupakan standarisasi dari masalah 100VG-AnyLAN.
13. IEEE802.14 merupakan standarisasi dari masalah *protocol* CATV.
14. IEEE802.15.2-2003 merupakan standar yang menggabungkan IEEE802.15 (WPAN) dengan perangkat nirkabel lain yang beroperasi di frekuensi tanpa lisensi.
15. IEEE802.15.4-2003 merupakan standar yang mendefinisikan protokol dan hubungan beberapa perangkat menggunakan komunikasi radio pada PAN (*Personal Area Network*) (Sherman, Mody, Martinez, Rodriguez, & Reddy, 2008).

2.1.3 Jenis Jaringan Komputer

Dalam jaringan komputer, ada beberapa jenis jaringan komputer, yaitu:

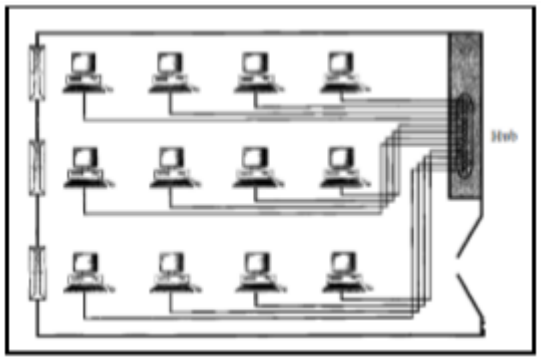
1. Berdasarkan jangkauan (Wongkar, Sinsuw, & Xaverius, 2015)
   a. PAN (*Personal Area Network*)

      Jaringan PAN adalah jaringan yang berhubungan antara dua atau lebih komputer dengan jarak yang dekat, yaitu sampai 6 meter.

Gambar 2.1 Jaringan PAN (*Personal Area Network*)

b. LAN (*Local Area Network*)

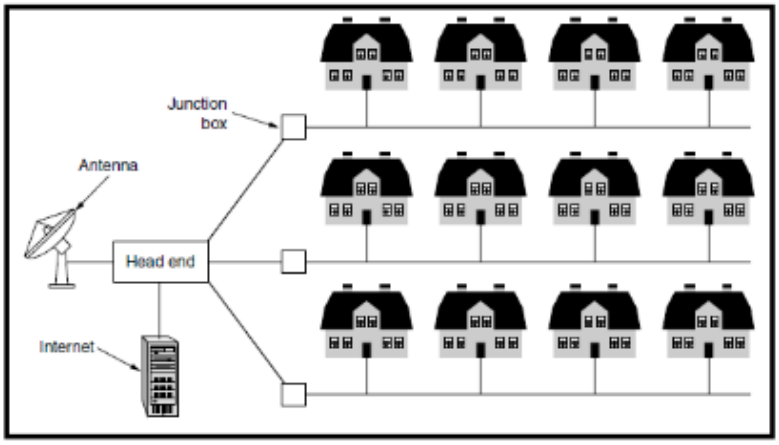
Jaringan LAN adalah jaringan dimana sejumlah komputer dihubungkan satu sama lain dalam satu area tertentu sebesar satu gedung.



Gambar 2.2 Jaringan LAN (*Local Area Network*) (Masero, Triyono, & Andayati, 2013)

c. MAN (*Metropolitan Area Network*)

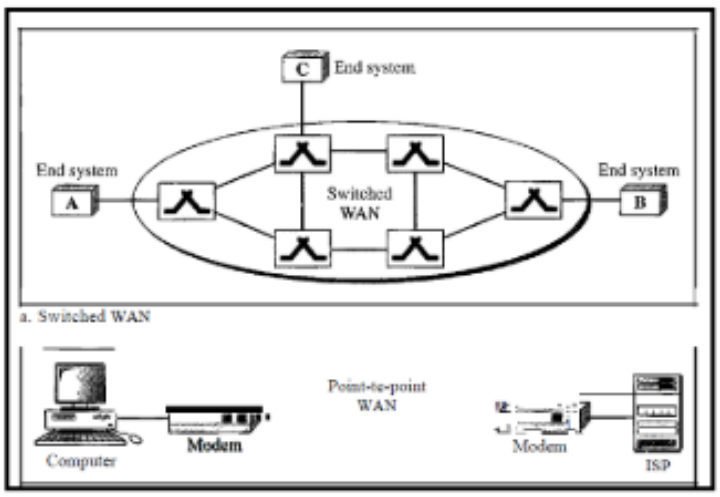
Jaringan PAN merupakan jaringan LAN yang digabungkan satu sama lain, dimana jaringan ini mencakup beberapa kantor berdekatan atau sebuah area kota, dan memiliki kecepatan transfer yang lebih tinggi. Jangkuan jaringan MAN bisa mencapai 50 kilometer.



Gambar 2.3 Jaringan MAN (*Metropolitan Area Network*) (Masero et al., 2013)

d. WAN (*Wide Area Network*)

Jaringan WAN merupakan jaringan yang mencakup area yang sangat luas, dan biasanya menghubungkan beberapa komputer dengan kabel *fiber optic* atau satelit. Jangkauan jaringan ini bisa mencapai ke beberapa provinsi atau bahkan negara.



Gambar 2.4 Jaringan WAN (*Wide Area Network*) (Masero et al., 2013)

e. *WLAN* (*Wireless LAN*)

Jaringan *wireless LAN* merupakan alternatif dari jaringan kabel LAN dengan menggunakan teknologi frekuensi radio. Teknologi ini bisa mengirim dan menerima data melalui media udara, sehingga jaringan ini bisa menggabungkan konektivitas data dan mobilitas pengguna.

2. Berdasarkan fungsi (Varianto & Mohammad badrul, 2015)

a. *Client Server*

Dalam jaringan *Client Server*, beberapa komputer dapat berperan sebagai *server* untuk membagi data dan *resources* pada komputer *client*. Komputer *Server* mempunyai kemampuan untuk mengatur akses data atau *resource* mana saja yang boleh digunakan. Peran komputer sebagai *client* adalah mengakses data dari komputer *server*, sedangkan peran komputer sebagai *server* adalah menyediakan data untuk komputer *client*.

b. *Peer to Peer*

Dalam jaringan *peer to peer*, semua komputer dalam jaringan tersebut bisa berperan sebagai komputer *client*, maupun komputer *server*. Komputer bisa melakukan komunikasi dengan SSID (*Service Set Identifier*) yang merupakan nama identitas komputer. Jaringan ini biasanya juga disebut sebagai *Ad Hoc Wireless LAN*.

Gambar 2.5 Desain jaringan *Peer to Peer* (Maslan & Wangdra, 2012)

3. Berdasarkan media transmisi (Sitohang & Setiawan, 2018)

   a. Jaringan Nirkabel

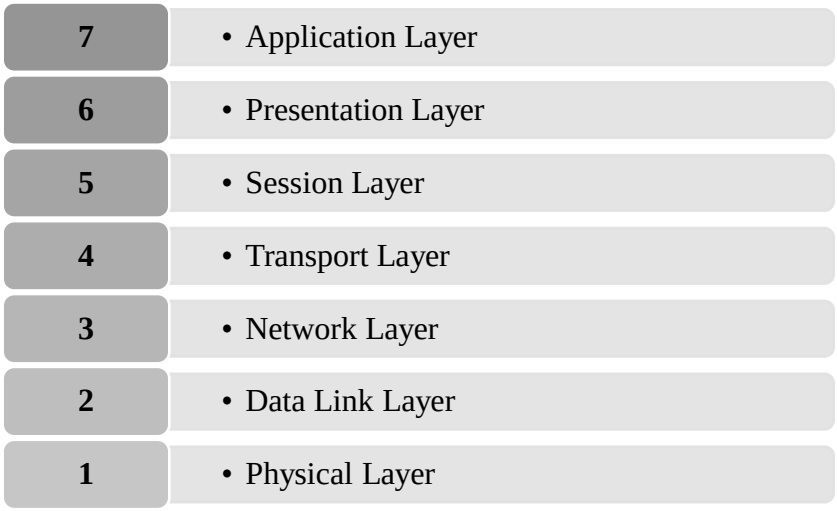
      Jaringan nirkabel merupakan suatu jenis jaringan dimana media transmisinya bersifat *wireless* atau tanpa kabel menggunakan gelombang/frekuensi radio. Pada jaringan ini, sinyal menyebar ke semua client dari hasil broadcast link *access point*. Kegunaan jaringan nirkabel dapat membantu dalam penghematan biaya pada bidang *enterprise* karena tidak memerlukan kabel dan menghilangkan kompleksitivitas koneksi dari alat-alat yang berbeda.

   b. Jaringan Kabel

      Jaringan kabel merupakan suatu bentuk jaringan yang terdiri dari beberapa komputer yang saling tersambung melalui saluran fisik (kabel).

2.1.4 Model OSI Layer

Arsitektur OSI (*Open System Interconnection*) merupakan panduan interkoneksi yang awalnya dibuat sebagai standar untuk membangun jaringan komputer, yang model referensi nya dirancang oleh organisasi ISO (*The International Organization for Standardization*). Saat ini, model OSI digunakan sebagai bahan/materi pembelajaran yang menjelaskan bagaimana cara kerja interkoneksi jaringan yang benar. Cara kerja ini dibagi menjadi 7 lapisan, dimana masing-masing lapisan mempunyai fungsi yang berbeda. Penggambaran OSI dibuat oleh kontribusi beberapa orang di *Honeywell Information Systems*. Berikut adalah gambar lapisan OSI (Mehta et al., 2016):



Gambar 2.6 Model Lapisan OSI

Berikut adalah penjelasan dari masing-masing lapisan OSI:

1. *Physical Layer*

Lapisan ini meliputi kabel secara fisik, *optic*, *switch*, dan semua alat fisik yang dibutuhkan untuk membangun sebuah jaringan. Lapisan *Physical*

mempunyai peran untuk mengubah data digital menjadi *pulse* yang dikirim melalui kabel untuk mentransfer data. Selain itu, lapisan ini juga bertanggung jawab dalam pemilihan dan generasi frekuensi, mendeteksi signal, enkripsi, dan modulasi. (Mary & Kannammal, 2017)

2. *Data Link Layer*

Pada lapisan ini, data *pulse* dari lapisan *Physical* ini akan diubah menjadi *frame* yang bisa ditransfer ke lapisan diatasnya (*Network Layer*). Tujuan dari lapisan ini adalah membangun, mempertahankan, dan mengeluarkan hubungan data ke dalam jaringan. Selain itu, *data link layer* mempunyai peran untuk menangkap dan memperbaiki *frame* yang rusak pada lapisan tersebut, yang bisa diandalkan untuk komunikasi *point-to-point* dan *point-to-multipoint* (Mehta et al., 2016).

3. *Network Layer*

Lapisan ini merupakan tempat dimana perangkat yang disebut *router* berperan untuk menentukan jalur pengiriman paling cepat dan menentukan prosedur pengiriman data sekuensial dari sumber ke tujuan. Selain itu, lapisan ini juga mengendalikan masalah yang berhubungan dengan *buffer memory* dan *congestion*, yang mengakibatkan kemacetan pada saat pengiriman data. Protokol yang digunakan pada lapisan ini adalah IP (*Internet Protocol*) (Mehta et al., 2016).

4. *Transport Layer*

Transport layer bertanggung jawab dalam pengiriman data melalui suatu jaringan. Lapisan ini mempunyai fungsi *reliability* dan penghindaran

congestion, dimana protokol DTLS (*Datagram Transport Layer Security*) untuk menyediakan fungsi tersebut dirancang pada komunikasi *upstream*, maupun *downstream*. Selain itu, protokol tersebut juga memperhatikan transfer paket dan meminta *host* untuk melakukan transmisi ulang jika ada kesalahan/error (Mehta et al., 2016).

5. *Session Layer*

Lapisan ini mengizinkan pengguna dalam menggunakan perangkat yang berbeda dan memiliki fungsi mengendalikan dialog, pengelolaan token, dan sinkronisasi. Lapisan ini bertanggung jawab untuk mencegah dua pihak untuk melakukan operasi secara bersamaan, dan memberikan tanda bagian data yang tidak terkirim agar pengiriman bisa dilanjutkan dengan benar (Maslan & Wangdra, 2012).

6. *Presentation Layer*

Lapisan presentasi merupakan lapisan dimana data yang telah dikumpulan dari lapisan sebelumnya diubah, atau disebut sebagai *translation*. Hasil pengubahan data ini dapat dikenali oleh *software* yang memiliki antarmuka interaktif (*Graphical User Interface*). Lapisan ini juga bertanggung jawab dalam manipulasi data, seperti kompresi dan enkripsi. (Mehta et al., 2016)

7. *Application Layer*

Lapisan ini mendukung akses jaringan pada *software* yang bisa digunakan oleh pengguna. Protokol dari lapisan ini akan mengendalikan

permintaan dari layanan yang diminta, sehingga standar atau protokol yang diberikan bisa digunakan sesuai fungsi *software*-nya (Mehta et al., 2016).

2.2 Teori Khusus

Teori khusus memberikan penjelasan mengenai variabel-variabel khusus yang diteliti. Secara teoritis, variabel dapat didefinisikan sebagai objek yang mempunyai variasi antara satu dengan lainnya. Berikut adalah variabel-variabel yang digunakan dalam penelitian ini:

2.2.1 *Raspberry Pi*

Raspberry Pi adalah sebuah komputer kecil dengan ukuran sebesar kartu kredit yang bisa dihubungkan pada monitor komputer ataupun TV. Alat ini sering disebut sebagai komputer kecil karena dapat melakukan aktifitas seperti komputer biasa pada umumnya. Karena ukurannya yang sangat kecil, *Raspberry Pi* dapat dibawa kemana saja. Alat ini sering digunakan oleh anak-anak sebagai alat untuk mempelajari pemrograman dan komputer, dan sering digunakan oleh orang awam untuk melakukan otomasi pada rumah. *Raspberry Pi* merupakan hasil pengembangan negara *United Kingdom* dari organisasi *Raspberry Pi Foundation* (Ms. Sejal V. Gawande, 2015).

Saat ini, ada 6 macam *Raspberry Pi* yang sudah dikembangkan, dimulai dari *Raspberry Pi* Model A+, *Raspberry Pi* 2 Model B, hingga *Raspberry Pi Zero* W. Pada generasi pertama *Raspberry Pi*, varian Model A+ adalah varian dengan harga

yang lebih murah dibandingkan dengan Model B+, dimana varian Model B merupakan revisi akhir dari *Raspberry Pi* pertama. Kemudian, *Raspberry Pi* 2 Model B diumumkan sebagai generasi kedua dari *Raspberry Pi*. Komputer kecil generasi kedua ini mempunyai peningkatan spesifikasi, seperti kapasitas RAM yang lebih besar dan kecepatan frekuensi yang lebih tinggi. *Raspberry Pi* generasi ketiga Model B diluncurkan pada awal 2016 dan kemudian *Raspberry Pi Zero* dan *Zero* W diumumkan sebagai varian yang memiliki ukuran lebih kecil dari *Raspberry Pi* generasi pertama. Berikut adalah spesifikasi perbandingan dari *Raspberry Pi* generasi pertama hingga *Raspberry Pi* terbarunya (Dinata, 2017):

1. *Raspberry Pi* Model A+ mempunyai prosessor BCM2835 (700MHz single-core ARM11), 512MB RAM, 1 port USB tanpa *Ethernet*, *Bluetooth* dan Wi-Fi.
2. *Raspberry Pi* Model B+ mempunyai prosesor BCM2835, 512MB RAM, 4 port USB, dan 1 port *Ethernet*. Wi-Fi dan *Bluetooth* tidak tersedia.
3. *Raspberry Pi* 2 Model B mempunyai prosesor BCM2836 (900MHz Quad-core Cortex A7), 1GB RAM, 4 port USB, dan 1 port *Ethernet*. Wi-Fi dan *Bluetooth* tidak tersedia. Revisi versi 1.2 dari *Raspberry Pi* 2 Model B tersedia dengan peningkatan pada prosesor (BCM2837 900MHz Quad-core Cortex A53).
4. *Raspberry Pi* 3 Model B mempunyai prosesor BCM2837 (1200MHz Quad-core Cortex A53), 1GB RAM, GPIO (General Purpose Input Output) 40-pin, 4 port USB 2.0, 1 port HDMI, 1 port CSI *camera*, 1

port DSI *display*, 3.5mm *stereo output*, 1 port MicroSD untuk store data dan sistem operasi, 1 port Micro USB dengan input 2.5A, 1 port *Ethernet*, Wi-Fi, dan *Bluetooth*.

5. *Raspberry Pi Zero* mempunyai spesifikasi yang sama seperti *Raspberry Pi* generasi pertama, dengan pengecualian pada ukuran fisik dan frekuensi prosesor menjadi 1000MHz.
6. *Raspberry Pi Zero* W bersifat hampir sama persis dengan *Raspberry Pi Zero*, dengan pengecualian tersedianya Wi-Fi dan *Bluetooth*.

2.2.2 *Honeypot*

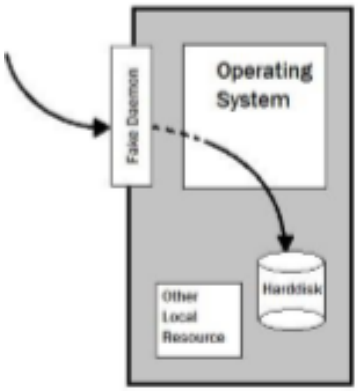
Honeypot merupakan teknologi baru dalam bidang keamanan jaringan komputer, dimana bentuknya berupa sistem atau komputer yang dirancang untuk menyerupai komputer asli. Teknologi keamanan jaringan baru ini melengkapi teknologi lama seperti *firewall* dan IDS (*Intrusion Detection System*). Namun, tidak seperti *firewall* atau IDS, *honeypot* bukan digunakan untuk menyelesaikan suatu masalah, melainkan memberikan kontribusi untuk menjaga keamanan jaringan secara menyeluruh.

Honeypot dirancang sebagai korban sasaran penyerang yang sengaja dibuat rentan terhadap serangan (*vulnerable*) pada jaringan internet. Karena *honeypot* bukan merupakan sistem yang asli, perancangan ini menyebabkan *honeypot* tidak memerlukan banyak trafik jaringan. Ini berarti jika trafik pada *honeypot* muncul, maka trafik tersebut harus dicurigai sebagai aktifitas yang berbahaya atau tidak sah, karena memang seharusnya tidak ada pengguna yang melakukan interaksi dengan

honeypot. *Honeypot* mempunyai kemampuan untuk mendeteksi dan mencatat serangan yang dilakukan pada *honeypot* itu sendiri. Hasil deteksi dan catatan tersebut akan ditaruh sebagai file *log* yang bisa dianalisis dan digunakan sebagai penelitian lanjut. (Khairunnisa & Sutarti, 2017).

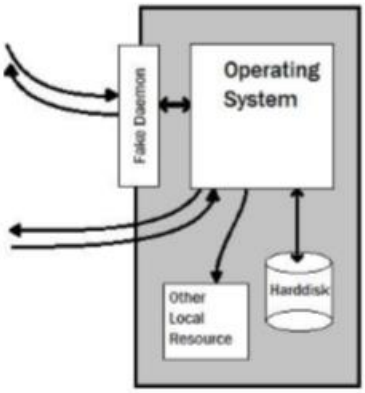
Ada beberapa jenis *honeypot* yang bisa digunakan. Perbedaan *honeypot* ini terletak pada tingkat keterlibatan dengan interaksi penyerang. Jenis-jenis *honeypot* berdasarkan tingkat keterlibatan adalah sebagai berikut (Aidin, Nasution, & Azmi, 2015):

1. *Low interaction honeypot* adalah *honeypot* yang hanya meniru layanan tertentu saja, yang berarti tidak ada sistem operasi nyata pada sistem *honeypot*.



Gambar 2.7 Diagram *Low interaction honeypot*

2. *Medium interaction honeypot* adalah jenis *honeypot* yang menyerupai sistem operasi asli dan dapat berkomunikasi langsung dengan penyerang.
3. *High interaction honeypot* adalah jenis *honeypot* yang memberikan sistem operasi penuh untuk diinteraksi dengan penyerang. Ini berarti penyerang mendapatkan kendali penuh pada sistem *honeypot*.



Gambar 2.8 Diagram *high interaction honeypot*

2.2.2.1 *Honeypot Dionaea*

Honeypot Dionaea adalah sistem *low interaction honeypot* yang dapat mendeteksi serangan *malware* dengan *port-port* palsu. Sistem *honeypot* ini dapat meniru layanan yang dapat diserang, yaitu, HTTP, FTP, MySQL, SMB, dan VOIP. Untuk mendapatkan catatan *log* serangan dari *Dionaea*, sistem *honeypot* ini harus dikonfigurasi untuk digunakan dan diakses terus menerus dari jaringan internet. Spesifikasi sistem paling rendah yang bisa digunakan sebagai *honeypot Dionaea* adalah prosesor *Pentium* dan tidak memerlukan konsumsi daya yang besar, sehingga *honeypot* ini bisa dijalankan pada kebanyakan komputer. Sering kali, *honeypot* ini dijalankan pada laptop lama yang tidak digunakan lagi, seperti *Raspberry Pi, Cubieboard, Beagle Board*, dll (Charles Lim et al., 2014).

2.3 Tools

Dalam penelitian in, beberapa perangkat akan digunakan untuk membangun jaringan dan *honeypot* yang terhubung pada jaringan tersebut. Berikut adalah alat-alat yang digunakan:

2.3.1 ISP (Internet Service Provider)

Internet Service Provider merupakan perusahaan telekomunikasi yang melayani komunikasi data melalui jaringan seluler atau jaringan nirkabel. Salah satu layanan yang diberikan ISP adalah akses internet dengan kecepatan tinggi (Budiman, 2016).

2.3.2 Laptop

Laptop merupakan komputer yang dirancang untuk mobilitas pengguna dan mempunyai sifat *portable* dengan desain bentuk seperti kerang (*Clamshell*). Ukuran komponen laptop biasanya lebih kecil daripada komputer secara umum. Laptop yang digunakan pada penelitian ini adalah Lenovo G40-45 (dengan sistem operasi Ubuntu 18.04).

2.3.3 Router

Router adalah perangkat jaringan yang mempunyai peran untuk menentukan jalur pengiriman dan prosedur pengiriman data sekuensial paling cepat dari sumber

ke tujuan. Jalur pengiriman ini bisa dilakukan secara statis (untuk jaringan yang jarang berubah) dan dinamis (Maslan & Wangdra, 2012). Aksi *routing* pada router digunakan oleh perangkat elektronik agar dapat berkomunikasi dan saling berbagi informasi (Hakim, 2017). Router yang digunakan pada penelitian ini adalah router TP-Link TL-MR6400 dengan slot kartu SIM (*Subscriber Identity Module*) yang dihubungkan langsung ke layanan ISP.

2.3.4 Raspberry Pi 3 Model B+

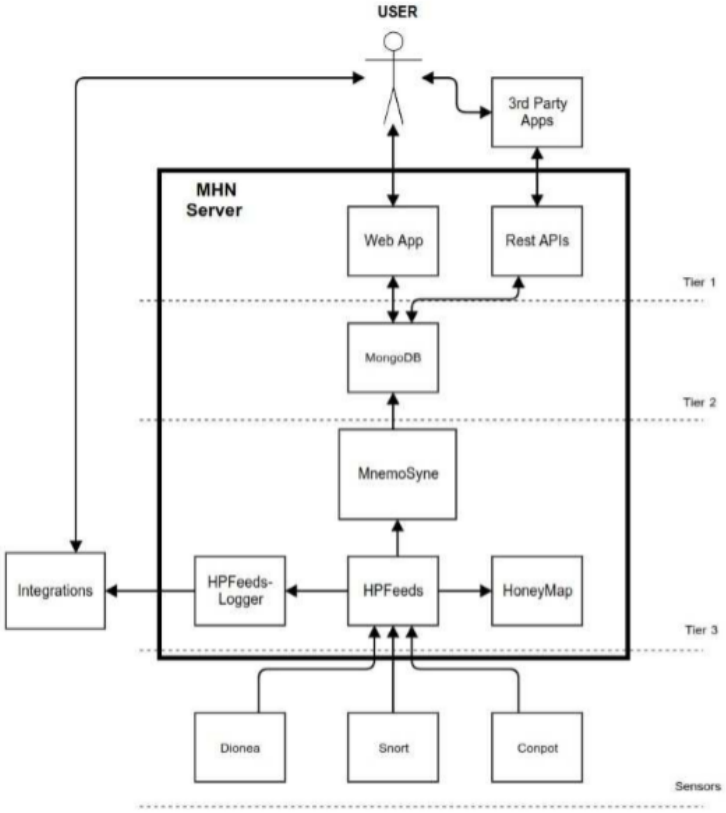
Raspberry Pi 3 Model B+ merupakan model paling awal dari Raspberry Pi generasi ketiga yang menggantikan *Raspberry Pi* 2 Model B. *Raspberry Pi* 3 Model B menggunakan prosesor Broadcom BCM2837B0 yang mempunyai 4 inti core dengan kecepatan frekuensi 1.4GHz. Prosesor ini menggunakan arsitektur CPU 64-bit dengan tipe ARM Cortex A53. Selain itu, Raspberry Pi 3 Model B+ juga mempunyai wireless LAN dengan dukungan *dual-band* 2.4GHz dan 5GHz.

Menurut website RaspberryPi (https://www.raspberrypi.org), spesifikasi *Raspberry Pi* 3 Model B+ lainnya adalah RAM 1GB, GPIO (*General Purpose Input Output*) 40-pin, 4 port USB 2.0, *Bluetooth* 4.2 (*Bluetooth Low Energy*), 1 port HDMI, 1 port CSI (*Camera Serial Interface*) *camera*, 1 port DSI (*Display Serial Interface*) display, 3.5mm *stereo output*, 1 port MicroSD untuk *store* data dan sistem operasi, dan 1 port Micro USB dengan input 2.5A.

Gambar 2.9 *Raspberry Pi 3* Model B+

2.3.5 *Modern Honeypot Network*

Modern Honeypot Network merupakan suatu proyek yang dibuat oleh perusahaan *security* bernama *Threatstream*. MHN dirancang sebagai alternatif gratis dan bersifat *open source* dari produk/solusi yang serupa. Tujuan proyek ini adalah memberikan solusi keamanan jaringan dengan *honeypot software* yang mudah diimplementasikan pada suatu perangkat. Proyek ini juga menggabungkan beberapa alat *open souce* lainnya seperti *HPFeeds* untuk mengumpulkan data sensor, *Mnemosyne* untuk mengindeks data ke *database* MongoDB, dan *HoneyMap* untuk visualisasi informasi secara *real-time* (Jigneshkumar, 2016).



Gambar 2.10 Arsitektur dari server *Modern Honeypot Network*

2.4 Penelitian Terdahulu

Penelitian terdahulu diperlukan sebagai referensi maupun materi dasar yang dilanjutkan untuk penelitian selanjutnya. Berikut adalah penelitian terdahulu untuk penelitian ini.

Penelitian terdahulu pertama adalah penelitian berjudul "*Honeypots Deployment for the Analysis and Visualization of Malware Activity and Malicious Connections*" pada tahun 2014 (ISBN 978-1-4799-2003-7). Penelitian ini ditulis oleh Ioannis Koniaris, Georgios Papadimirtiou, Pertros Nicopolitidis, dan Mohammad Obaidat di Universitas Thessaloniki, Yunani. Dari hasil penelitian

tersebut, penulis-penulis tersebut menjelaskan bahwa *honeypot* merupakan konsep keamanan jaringan yang cukup unik. *Honeypot* bisa membantu dalam penangkapan dan analisis proses *malware*, sehingga dapat memberikan pemberitahuan serangan lebih awal dan mampu menangkap eksploitasi yang belum diketahui. Serangan yang dilakukan bersifat acak, yang seakan-akan berarti tidak ada alamat IP yang aman. Penggunaan *honeypot Dionaea, HoneyD, Firewall,* dan *Intrusion Detection Sistem* merupakan tahap awal yang bagus dalam menjaga resiko serangan dan memberikan *warning* yang lebih awal (Koniaris, Papadimitriou, Nicopolitidis, & Obaidat, 2014).

Penelitian terdahulu kedua adalah penelitian yang berjudul "*HoneyPot systems in practice*" pada tahun 2015 (ISSN 0033-2097, DOI 10.15199/48.2015.02.16). Penelitian ini ditulis oleh Krzysztof Cabaj dan Piotr Gawkowski di Universitas *Warsaw*, Polandia. Berdasarkan dari hasil penelitian ini, dapat disimpulkan bahwa sistem *honeypot Dionaea* dapat mengidentifikasi beberapa serangan baru. Sistem *honeypot* yang dicoba oleh Kryzysztof Cabaj dan Piotr Gawkowski membantu menmberitahu serangan melalui koneksi yang berhubungan dengan *bug* dari implementasi *Supermicro IPMI* yang paling baru. Serangan yang diketahui oleh peneliti-peneliti tersebut dilakukan pada port 49152 pada tanggal 29 April 2014, sedangkan *bug* tersebut diumumkan secara resmi pada tanggal 19 Juni 2014. Peneliti tersebut menyimpulkan bahwa sistem *honeypot* yang disebarkan di Institut *Computer Science* bersifat cocok dan praktis dalam meningkatkan keamanan jaringan karena penggunaan *honeypot* mampu mengenali

aktivitas serangan *Zero-time exploit* tanpa harus mengakses *software* yang tidak aman (Cabaj & Gawkowski, 2015).

Penelitian ketiga adalah penelitian dengan judul "*Honeypot System for Local Network Attacks*" pada tahun 2016 (ISSN 2249-9555), yang ditulis oleh M. Solomon Zemene dan P.S. Avadhani di India. Penelitian ini dilakukan dengan menyebarkan sistem *honeypot* untuk mengumpulkan *malware* dan *log* berisi koneksi-koneksi dalam jaringan lokal. Implementasi *honeypot* dilakukan melalui VMware pada perangkat komputer dengan sistem operasi *Ubuntu* 12.04. *Honeypot* yang digunakan adalah *honeypot dionaea* dan sistem tersebut dijalankan selama 47 hari. Hasil penangkapan dan pengumpulan *log* menunjukan adanya *request* koneksi dengan sistem *honeypot* sebanyak 6997 *requests*. Penulis menyimpulkan bahwa sebagian besar serangan menggunakan kerentanan/*vulnerabilities* pada layanan SMB (*Server Message Block*), dan mempunyai potensi penyebaran *malware* ke seluruh jaringan dengan perangkat yang menggunakan layanan tersebut. Selain penangkapan *malware*, sistem *honeypot* tersebut juga bantu menghindari *malware* dari menyerang ke *host* dalam jaringan (Zemene, 2016).

Penelitian keempat adalah penelitian berjudul "Perancangan dan Analisis Keamanan Jaringan Nirkabel dari Serangan DDOS berbasis *Honeypot*" pada tahun 2017 (ISSN 2406-7733). Penelitian ini ditulis oleh Sutarti dan Khairunnisa di Universitas Serang Raya. Masalah yang dirujuk dari penelitian ini adalah seringnya masalah dan gangguan pada jaringan *server* yang disebabkan oleh serangan DDoS/*Distributed Denial of Service* di ruang *server* PDAM Tirta Al Bantani. Solusi yang ditawarkan adalah sistem *honeypot* yang berperan sebagai *server*

dengan sistem operasi yang bisa diserang dengan mudah. *Honeypot* yang digunakan dari penelitian tersebut adalah *honeypot Dionaea*. Berdasarkan hasil penelitian yang didapatkan, sistem *honeypot* tersebut tidak hanya mampu menghentikan serangan DDoS, tetapi juga serangan berupa *spam*, *malware*, *scanner*, dan *virus*. Saran yang dianjurkan dari penelitian ini adalah pelapisan sistem keamanan jaringan nirkabel/*wireless* dengan sistem *honeypot* yang bisa mendeteksi serangan dini dan pengecekan jaringan secara bekala untuk penghindaran *error* jaringan (Khairunnisa & Sutarti, 2017).

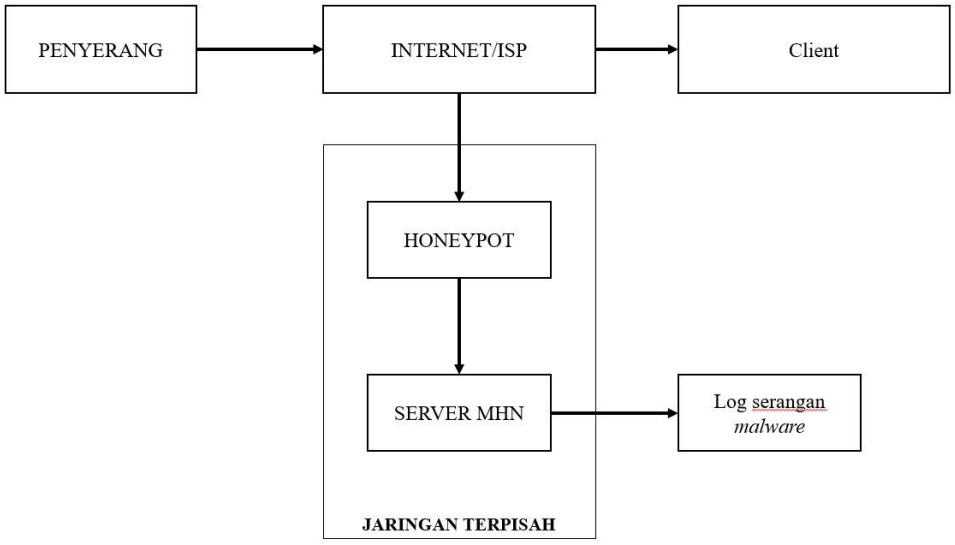
Penelitian kelima adalah penelitian berjudul "Implementasi *Honeypot* dengan *Modern Honey Network*" pada tahun 2017 (ISSN 2442-5826). Penelitian ini ditulis oleh Dimas Danang Laksana, Setia Juli Irzal Ismail, dan Nina Hendrarini di Universitas Telkom. Permasalahan yang diangkat dari penelitian tersebut adalah besarnya peningkatan kasus *cybercrime* di Indonesia, dimana mengakibatkan perlunya suatu sistem keamanan. *Honeypot* diangkat sebagai solusi dalam penelitian ini. Secara rinci, *honeypot* yang digunakan adalah *honeypot Kippo* yang bisa mengamankan akses SSH. Pengumpulan data serangan yang cukup rumit membuat penulis menggunakan layanan MHN (*Modern Honeypot Network*), dimana layanan tersebut mampu mengatur dan mengelola *honeypot*. Selain itu, MHN juga dapat dengan mudah diimplementasikan karena sistemnya bersifat *open source*. Pengujian yang dilakukan dalam penelitian ini adalah pengujian serangan *dictionary attack*, *DoS attack*, dan *Metasploit*. Hasil penelitian menunjukan *honeypot kippo* hanya mampu mendeteksi alamat IP serangan, tetapi sistem MHN

bisa mengumpulkan kumpulan *log* dari *honeypot Kippo* dengan data IP serangan, negara, waktu, *port*, dan *honeypot* (Laksana, Ismail, & Hendrarini, 2017).

2.5 Kerangka Pemikiran

Kerangka pemikiran merupakan penjelasan sementara pada gejala-gejala yang menjadi objek permasalahan, dimana modelnya menjelaskan bagaimana teori dapat berhubungan dengan berbagai faktor. Kerangka berpikir yang disarankan adalah kerangka yang dinyatakan dalam bentuk diagram agar pembaca bisa memahami kerangka berpikir yang dikemukakan dalam penelitian (Sudaryono, 2015).

Berdasarkan teori yang dibahas sebelumnya, maka kerangka berpikir yang dibuat dalam penelitian ini adalah sebagai berikut:



Gambar 2.11 Kerangka Pemikiran

Pada kerangka pemikiran yang sudah diatas, sistem *honeypot* akan dihubungkan ke *router* agar dapat mengakses ke jaringan internet. Untuk menjaga keamanan jaringan secara keseluruhan, maka jaringan untuk *honeypot* dan perangkat lain harus dipisah. Komputer yang berperan sebagai *server* dan *database* akan dihubungkan dengan *honeypot* melalui layanan MHN (*Modern Honeypot Network*). Komputer tersebut dapat diakses untuk melihat serangan *log* dari *malware* yang menyerang ke *honeypot*.