BAB III

TINJAUAN PUSTAKA

3.1 Landasan Teori

3.1.1 Sistem

Menurut Nurlalela (2013), Pengertian sistem informasi adalah sistem yang menyediakan informasi dengan cara sedemikian rupa sehingga bermanfaat bagi penerima. Secara lebih detil, sistem informasi dapat didefinisikan sebagai seperangkat entitas yang terdiri dari *hardaware*, *software* dan *brainware* yang saling bekerjasama untuk menyediakan data yang diolah sehingga berguna dan bermanfaat bagi penerima data tersebut.

3.1.2 Kemanan

Dalam Kamus Bahasa Indonesia keamanan didefinisikan sebagai keadaan aman dan ketentraman, atau jika mengambil pengertian dari kata dasarnya yakni aman dapat didefinisikan sebagai bebas dari bahaya.

3.1.3 Jaringan Komputer

Menurut Sofana (2013 : 3), jaringan komputer adalah suatu himpunan yang terkoneksi sejumlah komputer *autonomous.* Dalam bahasa yang popoler dapat dijelaskan bahwa jaringan komputer adalah kumpulan beberapa komputer yang saling terhubung satu sama lain melalui media perantara. Media perantara ini bisa berupa media kabel

ataupun media tanpa kabel (*nirkabel*). Informasi berupa data akan mengalir dari satu komputer ke perangkat yang lain, sehingga masing-masing komputer yang terhubung tersebut bisa saling bertukar data atau berbagi perangkat keras.

3.1.4 *Honeypot*

Menurut Laksana, (2017:1816), *Honeypot* adalah suatu cara untuk menjebak atau menangkal usaha – usaha penggunaan tak terotorisasi dalam sebuah *system* informasi. *Honeypot* merupakan pengalih perhatian hacker, agar seolah-olah berhasil menjebol dan mengambil data dari sebuah jaringan, padahal sesungguhnya data tersebut tidak penting dan lokasi tersebut sudah terisolir.

3.1.5 *Intrusion Prevention System*

Menurut Monoarfa, M.N.H, dkk (2016:36), *Intrusion Prevention System* adalah sebuah aplikasi yang bekerja untuk mendeteksi aktivitas mencurigakan, dan melakukan pencegahan terhadap intrusi atau kejadian yang dapat membuat jaringan menjadi berjalan tidak seperti bagaimana mestinnya. Produk IPS sendiri dapat berupa perangkat keras (*Hardware*) atau perangkat lunak (*Software*). Secara umum, ada dua jenis IPS, yaitu :

3.1.5.1 *Host Based* IPS (HIPS)

Host Based IPS (HIPS) bekerja dengan memaksa sekelompok perangkat lunak fundamental untuk berkovensi

secara konstan. Hal ini disebut dengan *Application Binary Interface* (ABI).

3.1.5.2 *Network Based IPS* (NIPS)

Network Based IPS (NIPS) melakukan pantauan dan proteksi dalam satu jaringan secara *global*. NIPS menggabungkan fitur IPS dengan *firewall*. NIPS biasanya dibangun dengan tujuan tertentu, sama halnya dengan *switch* dan *router*. Beberapa teknologi sudah diterapkan pada NIPS, seperti *signature matching*, analisa *protocol* dan kelainan pada *protocol*, identifikasi dari pola trafik, dan sebagainya. NIPS dibuat untuk menganalisa, mendeteksi, dan melaporkan seluruh arus data dan disetting dengan konfigurasi kebijakan keamanan NIPS, sehingga segala serangan yang datang dapat langsung terdeteksi dan langsung di blokir.

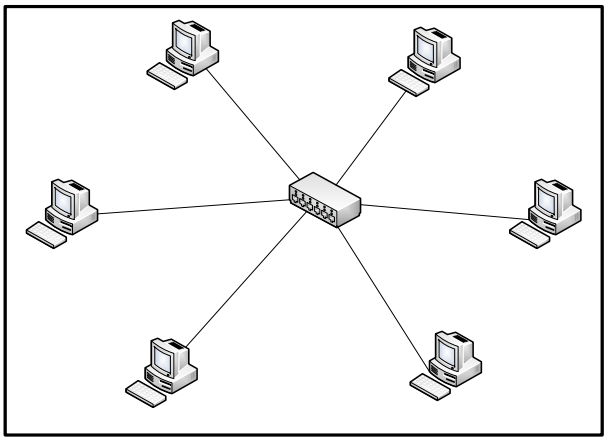
3.1.6 Terminologi Jaringan Komputer

Berdasarkan luas areanya maka jaringan komputer di bagi menjadi 4 yaitu :

3.1.6.1 *Local Area Network* (LAN)

Menurut Madcoms (2013 : 5), *Local Area Network* adalah jaringan yang dibatasi oleh area yang *relative* kecil. Jaringan jenis ini biasanya menghubungkan antar komputer satu dengan lainya atau juga *node* satu dengan *node* yang lainya. Daerah jangkauan LAN tidak terlalu jauh, dalam satu ruangan

atau satu area dengan radius antar 100 m sampai 2 km, tergantung dari jenis kabel yang digunakan, penempatan jaringan LAN biasanya dibangun untuk perkantoan, laboratorium, kelas *warnet* atau Usaha Kecil Menengah (UKM) yang skalanya kecil, jika diterapkan pada perusahaan besar maka penggunaanya hanya dalam ruang lingkup kecil. Kecepatan pada jaringan LAN *relative* tinggi yaitu mulai dari 1, 10, 100, sampai 1000 Mbps. Jaringan LAN dapat dilihat pada gambar 3.1.



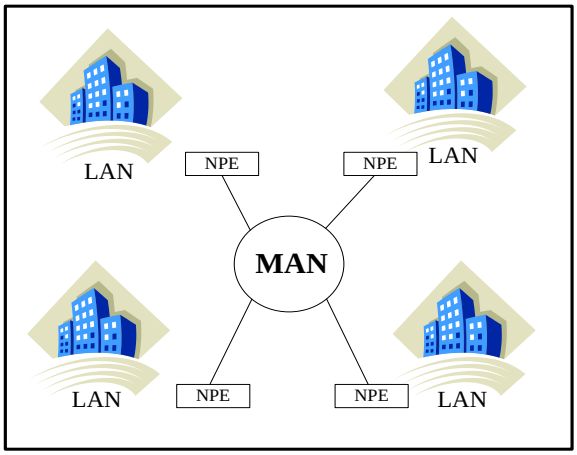
Sumber : Diolah Sendiri

Gambar 3.1 Ilustrasi Jaringan LAN

3.1.6.2 *Metropolitan Area Network* (MAN)

Menurut Madcoms (2013 : 6), *Metropolitan Area Network* adalah jaringan komputer yang memiliki area yang lebih besar dari LAN, biasanya antar wilayah dalam satu provinsi. Jangkauan MAN menghubungkan beberapa buah jaringan kecil dalam lingkungan area yang lebih besar.

Contohnya jika suatu instansi atau perusahaan memiliki cabang dalam kota atau provinsi dengan jarak antara 10-100 km, dan setiap cabang saling terhubung untuk bertukar data dan informasi. Jaringan MAN dapat dilihat pada gambar 3.2.

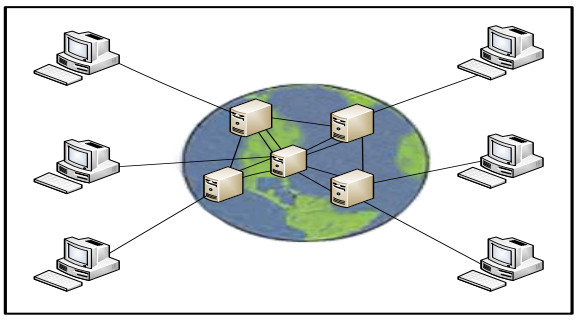


Sumber : Diolah Sendiri

Gambar 3.2 Ilustrasi Jaringan MAN

3.1.6.3 *Wide Area Network* (WAN)

Menurut Winarno (2013:64) *Wide Area Network* merupakan jaringan komputer yang lebih besar dari LAN. Jangkauannya bisa antar gedung. Jika jangkauanya satu kota, bisa juga disebut MAN.



Sumber : Diolah Sendiri

Gambar 3.3 Ilustrasi Jaringan WAN

3.1.6.4 Internet

Menurut Yatiningsi (2013 : 55), Internet merupakan jaringan komputer yang dibentuk oleh Departemen Pertahanan Amerika Serikat di tahun 1969, melalui proyek ARPANET yang disebut *Advanced Research Project Agency Network*. Mereka mendemonstrasikan bagaimana *hardware* dan *software* komputer dapat berkomunikasi dalam jarak yang tidak terhingga melalui saluran telepon. Tujuan awal dibangunya projek ini adalah untuk keperluan militer.

3.1.7 Jenis *Malware*

3.1.7.1 Virus

Menurut Septiani, (2016), Virus merupakan program komputer yang bersifat mengganggu dan merugikan pengguna komputer. Virus adalah *Malware* pertama yang dikenalkan sebagai program yang memiliki kemampuan untuk mengganggu kinerja sistem komputer. Hingga saat ini biasanya masyarakat lebih populer dengan kata virus komputer dibandingkan dengan istilah *Malware* sendiri. Biasanya virus berbentuk *file* eksekusi exe (*executable*) yang baru akan beraktivitas bila *user* mengaktifkannya. Setelah diaktifkan virus akan menyerang *file* yang juga bertipe *executable* (*.exe*) atau juga tipe *file* lainnya sesuai dengan perintah yang dituliskan pembuatnya.

3.1.7.2 *Worm*

Menurut Septiani, (2016), *Worm* yang berarti cacing merupakan *Malware* yang cukup berbahaya. *Worm* mampu untuk menyebar melalui jaringan komputer tanpa harus tereksekusi sebelumnya. Setelah masuk ke dalam sistem komputer, *Worm* memiliki kemampuan untuk mereplikasi diri sehingga mampu memperbanyak jumlahnya di dalam sistem komputer. Hal yang diakibatkan dari aktivitas *Worm* adalah merusak data dan memenuhi *memory* dengan *Worm* lainnya hasil dari penggandaan diri yang dilakukannya. Replikasi ini membuat memory akan menjadi penuh dan dapat menngakibatkan aktivitas komputer menjadi macet (hang). Kebiasaan komputer menjadi hang dapat menjadi gejala awal terdapatnya *Worm* pada komputer tersebut. Contoh *Worm* yang populer akhir-akhir ini adalah *Conficker*.

3.1.7.3 *Trojan Horse*

Menurut Septiani, (2016), Teknik *Malware* ini terinspirasi dari kisah peperangan kerajaan Yunani kuno yang juga diangkat ke *Hollywood* dalam *film* berjudul '*Troy*'. Modus dari *Trojan Horse* ini adalah menumpangi *file* biasa yang bila sudah dieksekusi akan menjalankan aktivitas lain yang merugikan sekalipun tidak menghilangkan fungsi utama *file* yang ditumpanginya. *Trojan Horse* merupakan *Malware*

berbahaya, lebih dari sekedar keberadaannya tidak diketahui oleh pengguna komputer. *Trojan* dapat melakukan aktivitas tak terbatas bila sudah masuk ke dalam sistem komputer. Kegiatan yang biasa dilakukan adalah merusak sistem dan *file*, mencuri data, melihat aktivitas *user (spyware*), mengetahui apa saja yang diketikkan oleh *user* termasuk *password* (*keylogger*) bahkan menguasai sepenuhnya komputer yang telah terinfeksi *Trojan Horse*.

3.1.7.4 *Spyware*

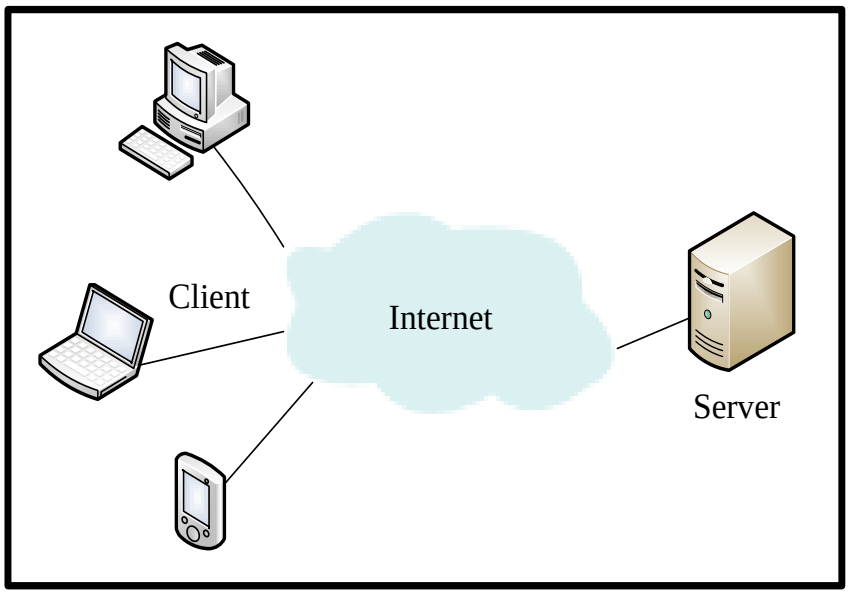
Menurut Septiani, (2016), *Spyware* merupakan *Malware* yang dirancang khusus untuk mengumpulkan segala informasi dari komputer yang telah dijangkitinya. Kegiatan *Spyware* jelas sangat merugikan *user* karena segala aktivitasnya yang mungkin menyangkut privasi telah diketahui oleh orang lain tanpa mendapat izin sebelumnya. Aktivitas *Spyware* terasa sangat berbahaya karena rentan terhadap pencurian *password*. Dari kegiatan ini juga akhirnya lahir istilah *Adware* yang merupakan iklan yang mampu muncul secara tiba-tiba di komputer korban hasil dari mempelajari aktivitas korban dalam kegiatan berkomputer. Spam yang muncul secara tak terduga di komputer juga merupakan salah satu dampak aktivitas *Spyware* yang dirasa sangat menjengkelkan.

3.1.7.5 *Backdoor*

Menurut Septiani, (2016), Kerja dari *Backdoor* sangat berkaitan dengan aktivitas *hacking*. *Backdoor* merupakan metode yang digunakan untuk melewati *autentifikasi* normal (*login*) dan berusaha tidak terdeteksi. *Backdoor* sendiri sering kali disusupkan bersama dengan *Trojan* dan *Worm*. Dapat diartikan secara singkat *Backdoor* berarti masuk ke sistem komputer melalui jalur pintu belakang secara tidak sah. Dengan metode *Backdoor* maka akan sangat mudah untuk mengambil alih kendali dari komputer yang telah berhasil disusupi. Setelah berhasil masuk maka aktivitas yang dilakukan oleh *Backdoor* antara lain adalah mengacaukan lalu lintas jaringan, melakukan *brute force attack* untuk mengcrack *password* dan enkripsi dan mendistribusikan serangan *Distributed Denial of Service* (DDoS).

3.1.8 Jaringan *Client* Server

Menurut Sofana (2013 : 7), *Client* server adalah jaringan komputer yang mengharuskan salah-satu atau lebih komputer difungsingkan sebagai server atau *central.* Server melayani komputer yang disebut *client,* layanan yang diberikan oleh server bisa berupa akses *web, email, file,* gambar atau yang lain. Jaringan *client* dapat dilihat pada gambar 3.4.



Sumber : Diolah Sendiri

Gambar 3.4 *Client* Server

3.1.9 IP *Address*

Menurut Winarno (2013 : 65), IP *Address* adalah singkatan dari *Internet Protocol Address. Internet Protocol* (IP) *address* adalah identitas numerik yang diberikan kepada suatu alat seperti komputer, *router* atau *printer* yang terdapat dalam suatu jaringan komputer yang menggunakan *internet protocol* (IP) *Address* sebagai sarana komunikasi.

IP *Address* sendiri memakai sistem bilangan 32 bit. Sistem ini dikenal dengan nama *Internet Protocol version* 4 atau IPv4. IP versi 4 umumnya diekspresikan dalam notasi *decimal* bertitik, yang dibagi dalam 4 buah oktat berukuran 8 bit maka nilainya berkisar antara 0 sampai 255. Saat ini IPv4 masih digunakan. Walaupun IPv6 juga sudah

keluar, dan sudah diperkenalkan sejak tahun 1995. Tabel Kelas IP *Address* dapat dilihat pada tabel 3.1.

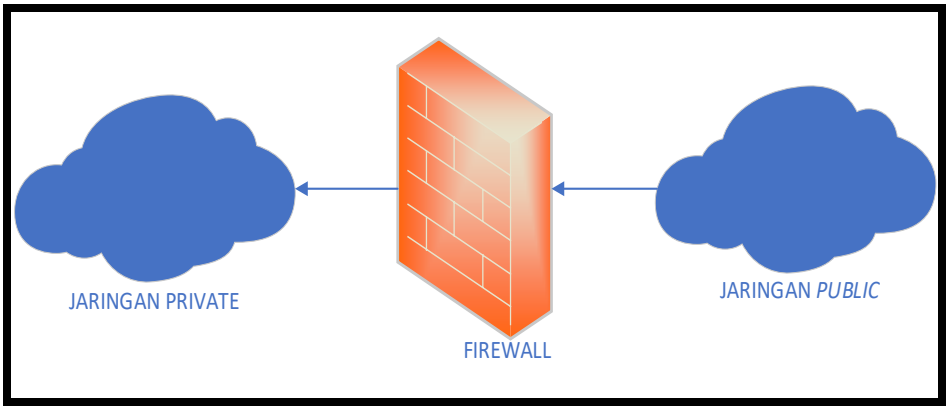
Tabel 3.1 Kelas IP *Address*

Kelas	**Oktat Pertama *Decimal***	**Jumlah *Network* ID**	**Jumlah Maks *Host/Network***	***Default Subnet Mask***
A	1 – 126	172	16777214	255.0.0.0
B	128 – 191	16384	155534	255.255.0.0
C	192 – 223	2097152	254	255.255.255.0
D	224 – 239	-	-	-
E	240 – 255	-	-	-

Sumber : Diolah Sendiri

3.1.10 *Firewall*

Menurut Pernama, (2016), *Firewall* merupakan sebuah mekanisme pengemenan yang dilakukan dengan kegiatan penyaringan paket data yang masuk dan keluar jaringan paket data yang masuk dan keluar jaringan. Sehinggan untuk dapat mengelolah keamanan informasi yang baik, dibutuhkan suatu tata kelola IT.



Sumber : Diolah Sendiri

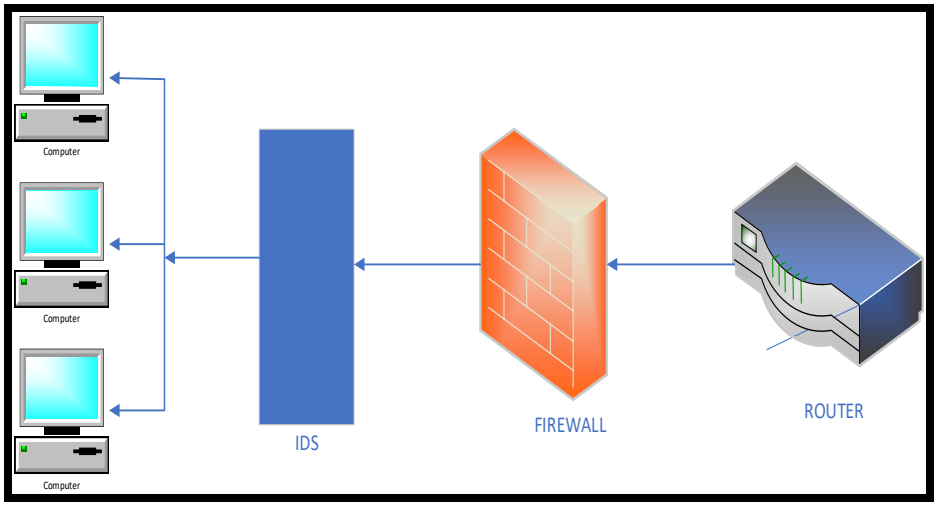
Gambar 3.5 Ilustrasi *Firewall*

3.1.11 *Iptables*

Menurut Yani (2005 : 69), *Iptables* adalah parameter yang digunakan untuk membuat aturan lebih spesifik (biasa digunakan pada penambahan, penghapusan, penyisipan atau operasi penggantian)

3.1.12 *Intrusion Detection System* (IDS)

Menurut Kusnadi (2018 : 2), IDS adalah seperangkat teknik atau metode yang digunakan untuk mendeteksi aktivitas mencurigakan baik di jaringan dan host, terdapat dua kategori dasar yaitu deteksi intrusi berbasis *signiture* dan anomali.

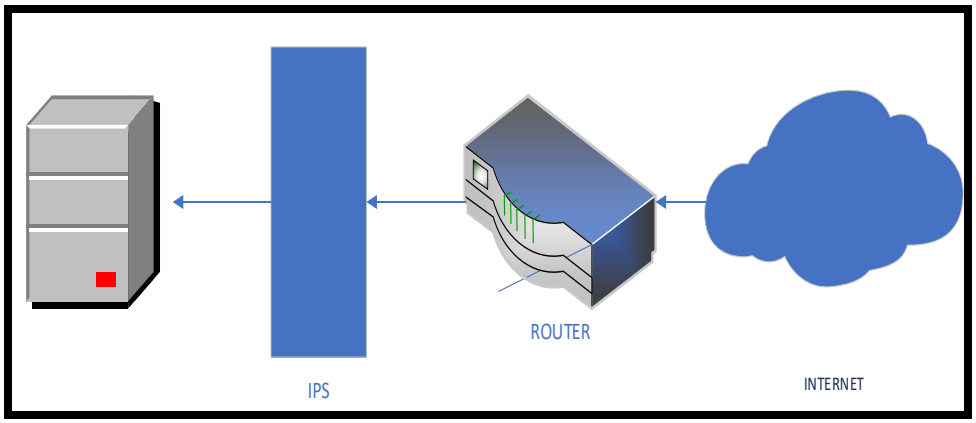


Sumber : Diolah Sendiri

Gambar 3.6 Ilustrasi IDS

3.1.13 IPS (*Intrusion Prevention System*)

Menurut Kusnadi (2018 : 2), IPS adalah perangkat yang digunakan untuk mendeteksi tanda-tanda gangguan dalam jaringan dan mengambil tindakan tindakan yang terdiri dari menghasilkan alarm dan secara aktif akan memblokir gangguan.



Sumber : Diolah Sendiri

Gambar 3.7 Ilustrasi IPS

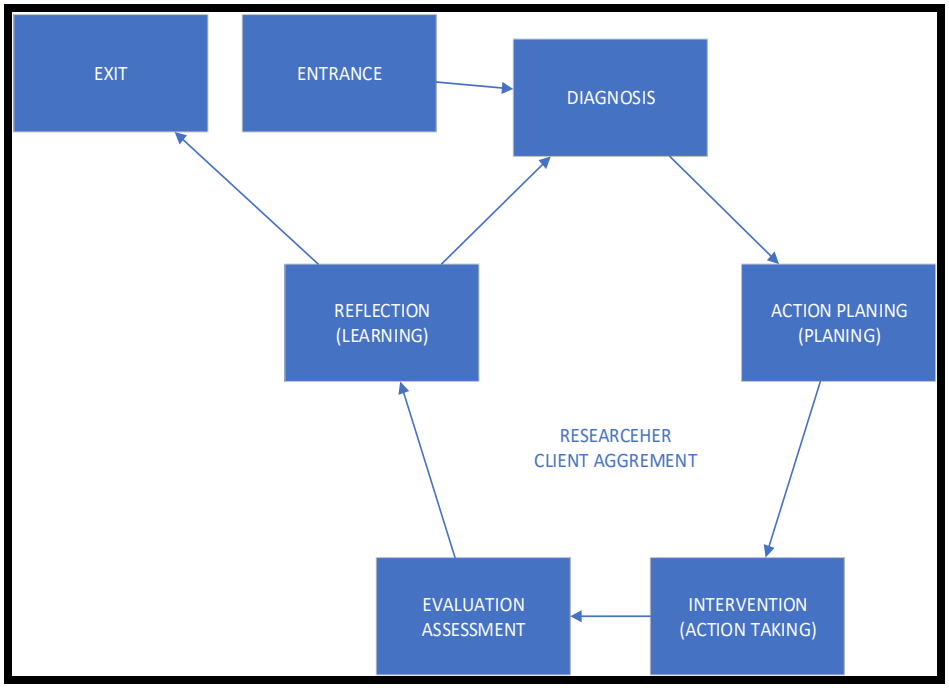
3.1.14 *Snort*

Menurut Rafiudin (2010 : 1), *Snort* tidak lain sebuah aplikasi atau *tool* sekuriti yang berfungsi untuk mendeteksi intrusi-intrusi jaringan (penyusup, penyerangan, pemindaian dan beragam bentuk ancaman lainnya), sekaligus juga melakukan pencegahan. Istilah populernya, *Sort* merupakan salah satu *tool Network Intrusion Prevention System* (NIPS) dan *Network Intrusion Detection System* (NIDS).

3.1.15 *Action Research*

Menurut Yaumi (2014), *Action Research* merupakan metode penelitian yang menekankan pada praktik soal, bertujuan ke arah peningkatan, suatu proses siklus, diikuti oleh penemuan yang sistematis, proses reflektif, bersifat partisipatif, dan ditentukan oleh pelaksana.

Penelitian ini bersifat partisipatif dan kolaboratif. Disebut partisipatif karena melibatkan peneliti, guru, pemerintahan, pendamping program dan *stakeholder*.



Sumber : Diolah Sendiri

Gambar 3.8 Metode Penelitian *Action Research*

1. ***Diagnosis***

   Melakukan identifikasi masalah pokok yang ada guna menjadi dasar kelompok atau organisasi sehingga terjadi perubahan, untuk pengembangan pada tahap ini melakukan indentifikasi dengan wawancara kepada stakeholder yag terkait langsung maupun yang tidak langsung.

2. ***Action Planning***

   Peneliti dan partisipan bersama-sama memahami pokok masalah yang ada kemudian melanjutkan dengan rencana tindakan yang tepat untuk menyelesaikan masalah yang ada. Pada tahap ini memasuki tahap desain, dengan memperhatikan kebutuhan *stakeholder* dan mulai menentukan isi tampilan nantinya.

3. *Intervention*

Selanjutnya setelah model dibuat berdasarkan sketsa dan menyesuaikan isi tampilan berdasarkan kebutuhan *stakeholder* dilanjutkan dengan megadakan uji coba.

4. *Evaluation*

Setelah *Intervention* kemudian melakukan evaluasi dari hasil, dalam tahap ini dilihat penerimaan pengguna ditandai dengan berbagai aktivitas-aktivitas.

5. Reflection

Ini merupakan tahap terakhir dengan melakukan review tahap-pertahap yang telah berakhir. Seluruh kriteria dalam prinsip pembelajaran harus dipelajari, perubahan dalam situasi organisasi dievaluasi oleh peneliti dan dikomunikasikan dengan klien.

3.2 Penelitian Terdahulu

Tabel 3.2 Penelitian Terdahulu

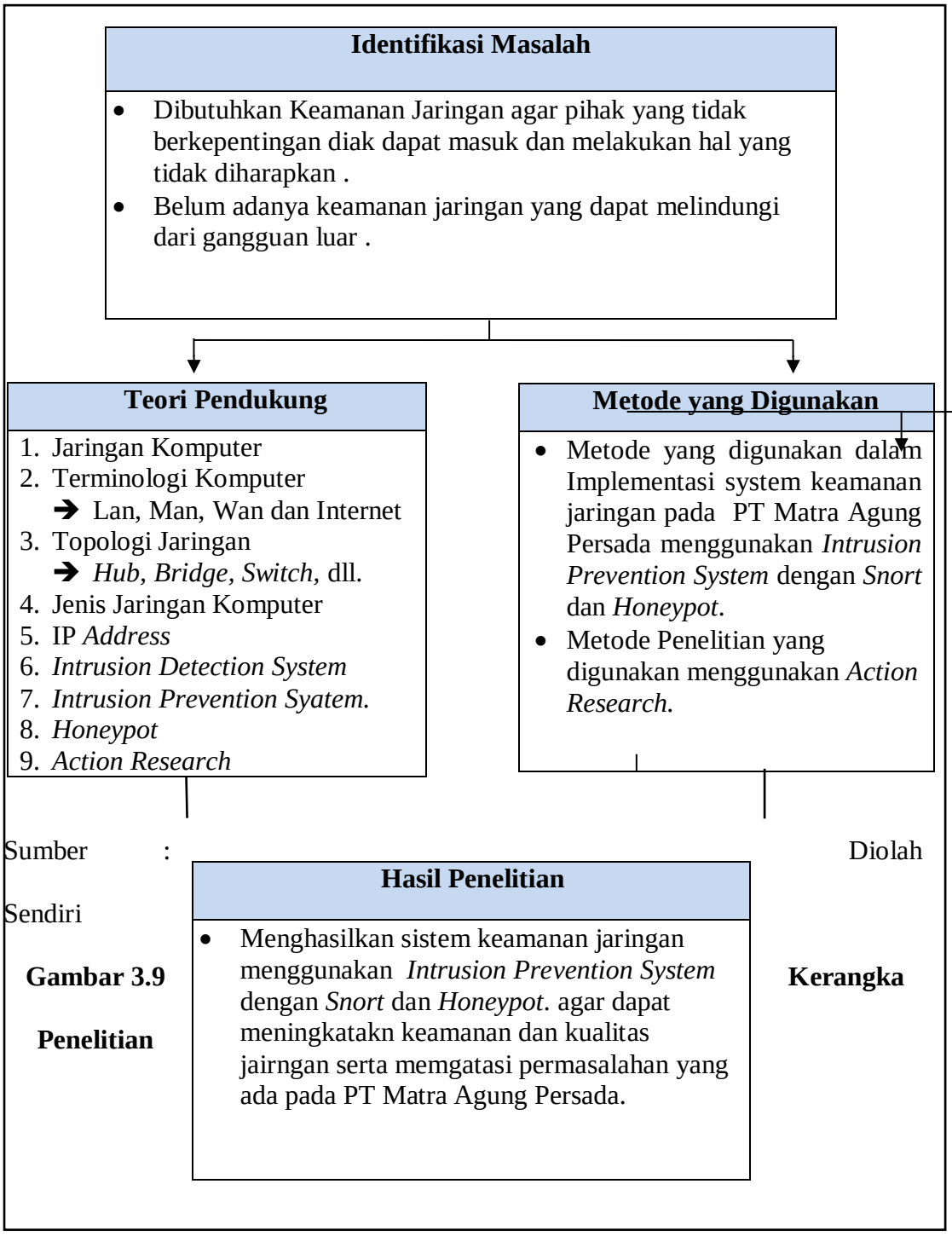
Judul	Nama	Hasil Penelitian
AnaIisa Dan Implementasi *Network Intrusion Prevention System* Di Jaringan Universitas Sam Ratunglangi	Mohamad Nurul Huda Monoarfa, Najoan, Alicia A.E Sinsuw	Hasil dari Penelitan yang berjudul AnaIisa Dan Implementasi *Network Intrusion Prevention System* Di Jaringan Universitas Sam Ratunglangi perlu disimpulkan : 1. Sistem NIPS dalam mencegah serangan yang terjadi adalah dengan melakukan scanning terhadap sejumlah packet dan Traffic yang melewati sensor dalam jaringan. 2. *Mekanisme sistem kerja snort yang telah berhasil di implementasikan dengan baik. Dalam pengujian sistem snort*

Judul	**Nama**	**Hasil Penelitian**
		dilakukan dengan Brute Force Attack. 3. *Pencegahan yang dapat dilakukan terhadap penyerangan adalah dengan menggunakan snort inline dipadukan dengan Iptables.*
Implementasi *Honeypot* Dengan *Modern Honey Network*	Dimans Danang Laksana, Setia Juli Irzal Ismail, Nina Hendrarini	Berdasarkan hasil penelitian ini adalah sebagai berikut : 1. Berdasarkan Sistem Modern Honey Network bertujuan untuk mengumpulkan log dari sensor kippo seperti negara, IP, waktu, port dan honeypot. 2. Honeypot kippo hanya dapat mendeteksi IP dari serangan.

Judul	**Nama**	**Hasil Penelitian**
Perancangan *Intrusion Prevention System* Pada Jaringan *Software Defined Networks*	Muhammad Arief Nugroho, Novian Anggis Suwastika	Berdasarkan hasil dan penelitian yang telah dilakukan, diperoleh simpulan sebagai berikut: 1. IPS di dalam jaringan SDN dapat meningkatkan tingkat keamanan di dalam jaringan. Hal ini dibuktikan dengan pengujian serangan dari layer network, transport, dan application mampu di deteksi dan diblok oleh IPS. Integrasi IPS dalam jaringan SDN memberikan pengaruh terhadap throughput, delay dan jitter. Kinerja ketiga parameter tersebut menurun setelah integrasi IPS ke jaringan SDN.

		Untuk setiap kenaikan 50 rule dalam IPS, nilai throughput berkurang rata rata 100 kbs, delay naik rata rata 0.1 ms, dan jitter naik rata rata 0.02 msuser.

3.3 Kerangka Pemikiran



Sumber : Diolah Sendiri

Gambar 3.9 Kerangka Penelitian