BAB III

TINJAUAN PUSTAKA

3.1. Landasan Teori

3.1.1 Analisis

Menurut Fatta (2007 : 27) Analisis adalah tahapan dimana sistem yang sedang berjalan dipelajari dan sistem penganti diusulkan. Dalam tahapan ini di deskripsikan sistem yang sedang berjalan, masalah dan kesempatan di definisikan, dan rekomendasi umum untuk bagaimana memperbaiki, meningkatkan atau mengganti sistem yang sedang berjalan.

3.1.2 *Open Source Security Information Management* (OSSIM)

Menurut Rihal (2010 : 14) OSSIM atau *Open Source Security Information Management* adalah sebuah *Platform Security Information Management* yang berbasiskan *open source* dan merupakan kumpulan lebih dari 15 *open source security* program yang semuanya terkandung didalam teknologi atau sistem ini untuk menghasilkan kontrol manajemen keamanan pada sebuah jaringan .Pada dasarnya OSSIM ini berupaya mengintegrasikan beberapa perangkat lunak dan *existing tools* lainnya untuk bekerjasama melakukan suatu penyimpanan, melakukan korelasi dan manajemen perangkat. Sehingga dapat menghasilkan kumpulan *event, log* dan informasi kondisi keamanan jaringan dari sebuah *single console*. Dengan adanya kerjasama beberapa aplikasi dan

perangkat keamanan jaringan, memungkinkan untuk dapat mengontrol jaringan dengan mengurangi waktu yang diperlukan dan mengelola informasi secara terpusat pada sebuah jaringan suatu perusahaan yang besar.

OSSIM terdiri dari kumpulan beberapa *tools* atau program-program *security* menjadi sebuah *server single console* untuk menghasilkan informasi keamanan pada sebuah jaringan. Tools tersebut diantaranya adalah:

1. *Snort* sebagai *Ids*
2. *Nessus* sebagai *Vulnerability Scanner*
3. *Ntop* adalah *tools* untuk monitor jaringan
4. *Nagios* digunakan untuk *availability monitor*
5. *Osiris* dan *snare* sebagai *host IDS*
6. *Arpwatch* dan *Pads* sebagai *anomaly detector*
7. *Pof* dan *Fprobe* sebagai *detektor pasif*
8. *Nmap* sebagai *network scanner*
9. *Acid/Base* sebagai *forensinc analyzer*
10. *Oinkmaster, PHPAcl, fw1logcheck, scanMap3D*
11. *OSVDB* sebagai *vulnerability* database

A. Arsitektur OSSIM

OSSIM terdiri dari 4 elemen bagian yaitu :

1. *Sensors*

2. Manajemen Server

3. Database

4. Frontend

B. *Sensors*

Sensor dipakai atau disebarkan pada sebuah jaringan untuk memantau aktivitas-aktivitas suatu sistem jaringan. Segala peristiwa-peristiwa atau kejadian pada suatu jaringan dapat diterima oleh *server* OSSIM ini melalui sensor, dalam hal ini sensor dapat disebut sebagai pendetektor. Suatu hal yang sangat penting bahwa OSSIM juga dapat menerima pada jaringan dari peralatan-peralatan komersial atau suatu aplikasi yang di kostumisasi sebagai sensor yang ditanam, sehingga dapat berkolaborasi dengan OSSIM. Sensor-sensor tersebut pada umumnya sebagai suatu *host* dan mempunyai tingkatan konfigurasi yang berbeda.

1. Untuk level konfigurasi tingkat paling bawah, sensor atau detektor OSSIM ini bersifat pasif monitor hanya menerima atau mengkoleksi data dari suatu jaringan.
2. Sensor pada OSSIM dapat pula dikonfigurasi sebagai suatu host *scanners* yang mana bersifat aktif sensor dimana sensor ini dapat melakukan *scanning* pada jaringan untuk melihat dan mengetahui celah pada suatu jaringan.
3. Untuk level yang paling atas dalam melakukan konfigurasi sensor OSSIM, dapat menambahkan OSSIM *Agent* sebagai detektor

sehingga dapat menerima data dari *host* yang ditunjuk sebagai *agent* OSSIM tersebut untuk melakukan pendeteksian pada jaringan sepeti *router* atau *firewall*, *detector* tersebut dapat berkomunkasi untuk mengirimkan data mereka kepada manajemen *server* OSSIM.

C. Manajemen *Server*

Suatu manajemen *server* atau *server* pada umumnya terdiri dari beberapa komponen bagian yaitu:

1. *Frameworked* adalah suatu kontrol *daemon* atau proses yang berjalan di belakang, yang mengikat bagian-bagian untuk bekerjasama.
2. OSSIM *server* adalah pusat dari segala informasi yang diterima dari sensor-sensor OSSIM. Adapun fungsi dari Manajemen *Server* ini adalah:

1. *Server* utama yang mempunyai tugas untuk menormalisasi, memberikan prioritas, mengkoleksi, melakukan *risk assessment* dan mengkorelasi perangkat-perangkat lainnya.
2. Melakukan perawatan dan tugas-tugas eksternal seperti *back up* data, *back up scheduled, inventory* secara *online,* dan melakukan atau mengajukan penscanan.

D. *Database*

Database pada OSSIM berfungsi untuk melakukan penyimpanan data dari semua kejadian pada suatu jaringan yang

berguna sebagai informasi untuk manajemen sistem. *Database* pada OSSIM adalah *SQL database.*

E. *Frontend*

Frontend adalah suatu *console* yang memberikan visualisasi informasi secara *web base system* pada layar komputer. Adapun Interaksi komponen pada OSSIM adalah sebagai berikut:

1. Agent atau sebuah sensor OSSIM mengirimkan data ke *database* OSSIM,dan juga melakukan kontrol atau komunikasi data tersebut dengan *server* untuk dilakukan prioritas dan korelasi
2. Server bertugas menerima data dan melakukan prioritas, korelasi dan *risk assesment* dan mengirimkan hasil data tersebut ke *database* OSSIM.
3. *User* atau admin melakukan pengecekan, konfigurasi terhadap *server* melalui *Frameworkd.*
4. OSSIM *framework* adalah sebuah panel yang memberikan informasi pada admin. Semua komponen yang ada pada OSSIM berdiri sendiri dan dapat di konfigurasi sesuai kebutuhan admin jaringan. Semua komponennya dapat terpisah atau dapat pula di integrasikan dalam satu mesin.

3.1.3 *Intrusion Prevention System*

Menurut Nurul (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 *Host-based Intrusion Prevention System (HIPS)* dan *Network Intrusion Prevention System (NIPS).*

1. *Host Based IPS (HIPS)* bekerja dengan memaksa sekelompok perangkat lunak fundamental untuk berkovensi secara konstan. Hal ini disebut dengan *Application Binary Interface (ABI).*
2. *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.

3.1.4 Linux

Menurut Sofana (2010:3) *Linux* adalah sistem turunan *UNIX* yang sangat lengkap, bisa dipergunakan untuk jaringan, pengembangan *software* dan bahkan untuk pekerjaan sehari-hari.

3.1.5 *Open Source*

Menurut Halim (2010:81) *Open source* adalah kode pemrograman pada *linux operation system* dapat dilihat oleh *public* dan menjadi proyek *public* sehingga kualitas *system* operasinya dapat ditingkatkan oleh para penggemar *linux.*

3.1.6 Jaringan komputer

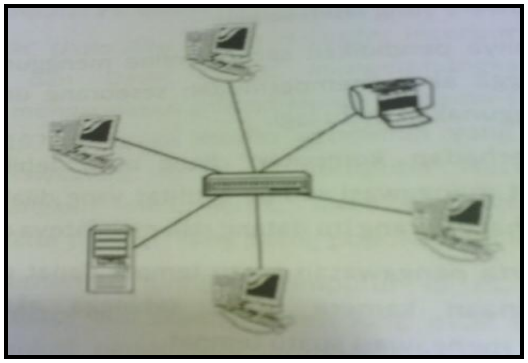
Menurut Sofana (2013:3) jaringan komputer adalah suatu himpunan interkoneksi komputer *autonomous.* Dalam bahasa yang popular dapat di jelaskan bahwa jaringan komputer adalah kumpulan beberapa komputer (dan perangkat lain seperti *router, switch,* dan sebagainya) yang saling terhubung satu sama lain melalui media perantara.

3.1.7 Jenis-Jenis Jaringan Komputer

1. *Local Area Network* (LAN)

Menurut Madcoms (2013:5) LAN adalah jaringan yang dibatasi oleh area yang relatif kecil. Jenis jaringan ini biasanya menghubungkan antar-komputer satu dengan lainnya atau bisa juga node satu dengan node lainnya. Daerah jangkauan LAN tidaklah terlalu jauh, missal dalam suatu ruangan atau suatu area dengan radius antara 100 meter

sampai 2.000 meter, tergantung dari jenis kabel yang di gunakan. seperti yang terlihat pada gambar 3.1

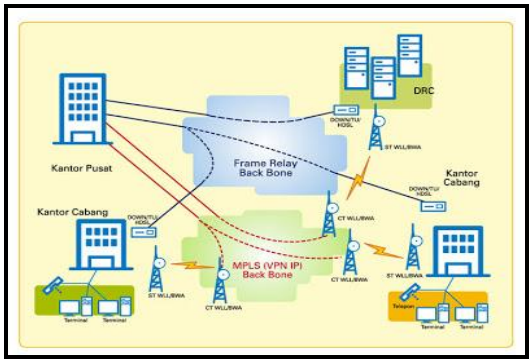


Sumber : Madcom (2013:6

Gambar 3.1 *Local Area Network*

2. *Metropolitan Area Network* (MAN)

Menurut Waloeya (2012:6) *Metropolitan Area Network* (MAN) merupakan jaringan yang mencakup satu kota besar, beserta daerah setempat, missal jaringan telepon lokal, sistem telepon seluler, serta jaringan *relay* beberapa ISP *internet.* seperti yang terlihat pada gambar 3.2

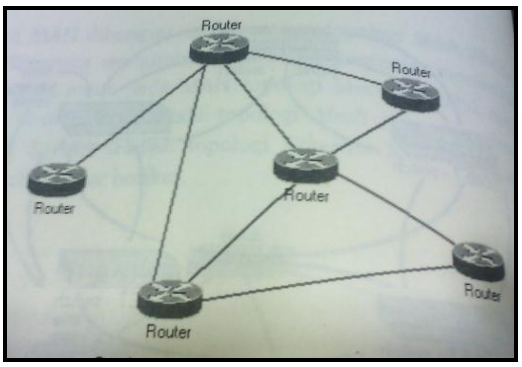


Sumber : Waloeya (2012:6)

Gambar 3.2 *Metropolitan Area Network*

3. *Wide Area Network* (WAN)

Menurut Sofana (2011:29) *Wide Area Network* (WAN) merupakan jaringan komputer yang meliputi area geografis sangat besar, seperti antarkota, antar-negara, antar-benua (mugkin saja antarplanet). seperti yang terlihat pada gambar 3.3



Sumber : Sofana (2011:29)

Gambar 3.3 *Wide Area Network*

3.1.8 Jenis-Jenis Topologi Jaringan Komputer

Topologi jaringan komputer adalah suatu cara atau konsep untuk menghubungkan beberapa atau banyak komputer sekaligus menjadi suatu jaringan yang saling terkoneksi, topologi jaringan komputer adalah sebagai berikut:

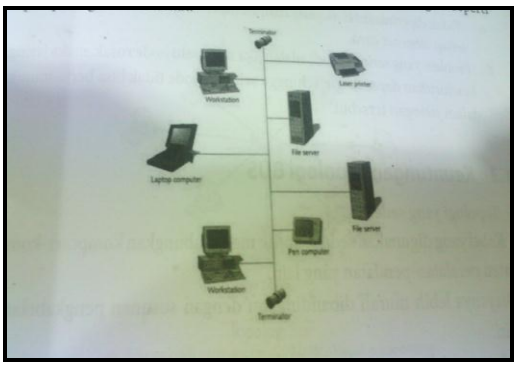
1. *Point to point* (PTP)

Menurut sofana (2013:9), Salah satu komputer/perangkat yang disambungkan ke satu perangkat/komputer saja baik menggunakan perangkat *wireless* maupun menggunakan kabel LAN saja. Jaringan ini .hanya melibatkan dua komputer saja. Misalnya dua buah komputer yang berkomunikasi via modem. Komunikasi dua buah komputer via kabel *null* modem atau *laplink* atau LASER,

merupakan contoh lain implementasi topologi ini. Karena media transmisi data hanya digunakan oleh dua buah komputer maka metode akses dan protokol yang digunakan umumnya relatif sederhana.

1. Topologi Bus

Menurut Badrul (2012:38) Topologi bus merupakan topologi yang banyak digunakan pada masa penggunaan kabel sepaksi menjamur. Dengan mengunakan T-*Connector* (dengan terminator 50 ohm pada ujung *network*), maka komputer atau perangkat jaringan lainnya bias dengan mudah di hubungkan satu sama lain. seperti yang terlihat pada gambar 3.4

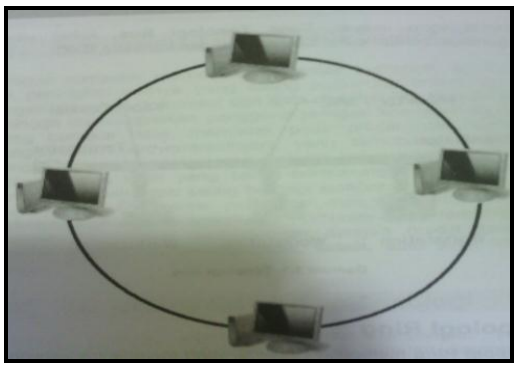


Sumber :Badrul (2012:38)
Gambar 3.4 Topologi Bus

2. Topologi *Ring*

Menurut Budi (2011:3) Topologi *ring* merupakan topologi yang membentuk sebuah lingkaran (cincin/ring). Pada topologi *ring*, sinyal data akan bergerak searah dari satu perangkat ke perangkat lainnya

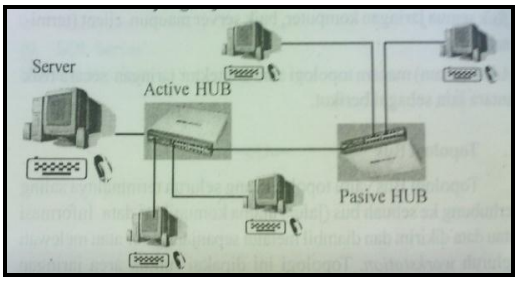
hingga berhenti pada perangkat tujuan. seperti yang terlihat pada gambar 3.5



Sumber : Budi (2011:3)
Gambar 3.5 Topologi *Ring*

3. Topologi *Star*

Menurut Suarna (2007:32) topologi *star* yaitu topologi yang masing-masing terminal dalam jaringan dihubungkan ke titik pusat (*server*) mengunkan jalur dan semua sambungan antarterminal harus diteruskan melalui *server*. *Server* bertindak sebagai pengatur dan pengendali seluruh komunikasi data yang terjadi. seperti yang terlihat pada gambar 3.6

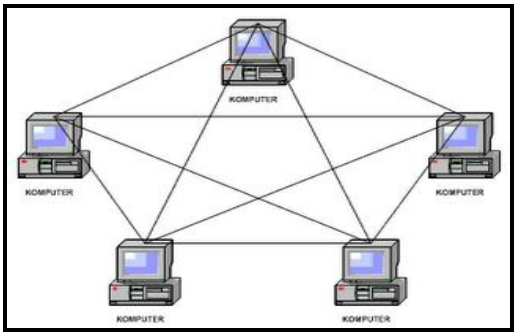


Sumber : Suarna (2007:32)
Gambar 3.6 Topologi *Star*

4. Topologi MESH

Menurut Badrul (2012:43) Topologi mesh adalah suatu bentuk hubungan antar perangkat dimana setiap perangkat terhubung secara

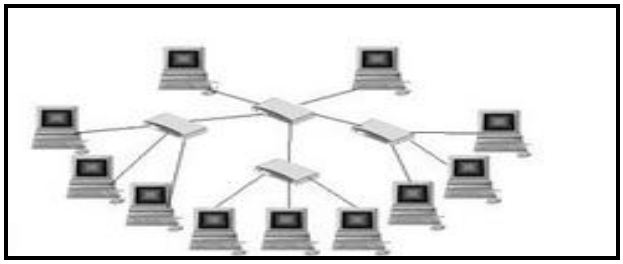
langsung ke perangkat lainnya yang ada dalam jaringan. seperti yang terlihat pada gambar 3.7



Sumber : Badrul (2012:43)
Gambar 3.7 Topologi Mesh

5. Topologi *Tree*

Menurut Badrul (2012:45) Topologi *Tree* adalah kombinasi karakteristik antara topologi bintang dan topologi bus. Topologi ini terdiri atas kumpulan topologi bintang yang di hubungkan dalam satu topologi bus sebagai jalur tulang punggung atau *backbone.* seperti yang terlihat pada gambar 3.8



Sumber : Badrul (2012:45)
Gambar 3.8 Topologi *Tree*

3.1.9 Teknologi Jaringan

Perkembangan jaringan komputer tidak terlepas dari berkembangnya teknologi yang mendukung, pertama kali jaringan komputer diperkenalkan menggunakan teknologi yang masih sangat terbatas dan mahal harganya. Namun untuk saat ini teknologi untuk *networking* sudah sedemikian

canggih, sehingga semakin mudah digunakan dan semakin murah harganya.

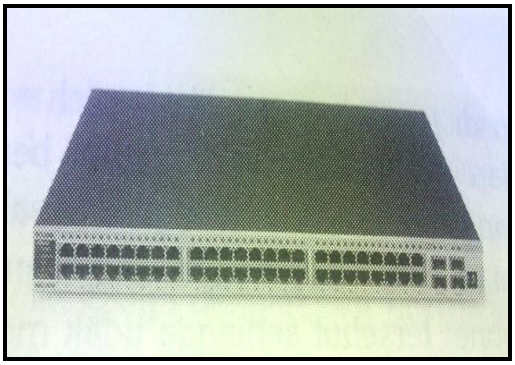
1. *Router*

Menurut Winarno (2011:25) *router* merupakan peranti jaringan yang lebih canggih dibandingkan dengan *bridge* dan *switch*. Sebuah *router* terdiri atas *hardware* dan *software* (memiliki sistem operasi sendiri) untuk mengatur rute data dari asal sumber ke tujuan. seperti yang terlihat pada gambar 3.9

Sumber : Winarno (2011:25)
Gambar : 3.9 *router*

2. *Switch*

Menurut Winarno (2011:24) *Switch* adalah peranti jaringan yang digunakan untuk mengatur *bandwidth* di jaringan berukuran besar. Walaupun demikian, harganya yang makin murah, *switch* juga mulai digunakan di jaringan rumahan ukuran kecil. seperti yang terlihat pada gambar 3.11



Sumber : Winarno (2011:24)
Gambar : 3.11 *switch*

3.2 Penelitian terdahulu

Beberapa contoh penelitian terdahulu dengan pembahasan yang hampir sama, seperti yang akan penulis lakukan terlihat pada tabel 3.1

3.1 Tabel Penelitian Terdahulu

no	Judul	Penulis /Tahun	Hasil
1	Analisa dan Implementasi *Network Intrusion Prevention System* Di Jaringan Universitas Sam Ratulangi ISSN: 2406-7768	Nurul, Najoan, Alicia, Sinsuw, /2016	Metode NIPS (Network Intrusion Prevention System) mampu mendeteksi serangan dan melakukan Drop pada serangan. Melakukan penerapan pada sistem operasi Linux menggunakan Snort, Konfigurasi sistem dibangun dalam jaringan local Universitas Sam Ratulangi yang dirancang untuk merepresentasikan pengujian. Hasil analisis dari setiap pengujian yang dilakukan menyimpulkan bahwa setiap tindakan yang dilakukan oleh penyerang terhadap jaringan dapat diketahui dan dicegah, sehingga dapat dilakukan penanganan sebelum terjadi kerusakan lebih luas.

	Analisis dan Implementasi Sistem Monitoring Koneksi Internet Menggunakan The Dude Di STIKOM Al Khairiyah ISSN : 2301-8402	Sutarti, Alif /2017	Monitoring jaringan yang dilakukan menggunakan software the Dude dengan sistem operasi Mikrotik, Sistem monitoring ini dipergunakan untuk mempermudah teknisi dalam melakukan pemantauan secara rutin kondisi jaringan di server. Selain untuk pemantauan koneksi internet bisa juga untuk memantau bandwidth user yang sedang dipakai, Hasil yang diperoleh setelah diimplementasikan adalah staf lebih cepat dalam mendeteksi trouble pada jaringan dan mempermudah dalam penanganannya.

Persamaan penelitian kami dengan jurnal satu dan dua sama-sama melakukan analisis dan implementasi pada jaringan komputer pada sebuah objek dalam hal ini perusahaan dan instansi pendidikan, persamaan selanjutnya pada jurnal satu terletak pada penggunaan aplikasi snort dan dilakukan pengujian pada jaringan yang tidak dilakukan pada jurnal dua. Untuk perbedaan jurnal satu dan dua terletak pada tempat penelitian yang menggunakan topologi, konfigurasi dan masalah jaringan yang berbeda-beda. Perbedaan selanjutnya pada jurnal satu menggunakan Ubuntu, jurnal dua menggunakan mikrotik, dan paenelitian kami menggunakan Alienvault.