BAB II

DASAR TEORI

Pada bab ini akan dibahas mengenai teori dan komponen penunjang yang akan digunakan dalam implementasi IDS menggunakan teknik HIDS. Pembahasan berisi tentang dasar dari jaringan serta klasifikasinya, sistem operasi yang akan digunakan, teknik HIDS, dan program yang digunakan.

2.1 Jaringan Komputer

Jaringan komputer adalah sistem yang terdiri dari komputer-komputer, serta piranti-piranti yang saling terhubung sabagai satu kesatuan. Dengan dihubungkanya piranti-piranti tersebut, komputer akan dapat saling berbagi sumber daya antara satu piranti dengan piranti lainya[8].

Jaringan komputer dapat diklasifikasikan menurut beberapa kategori, diantaranya:

1. Berdasarkan area cakupan
2. Berdasarkan media transmisi
3. Berdasarkan fungsi

2.1.2 Berdasarkan Area Cakupan

Jaringan komputer dapat dibedakan berdasarkan cakupan geografisnya. Ada tiga kategori utama jaringan komputer menurut cakupannya[7], yaitu:

1. LAN (*Local Area Network*)

   LAN merupakan jaringan kecil yang terdiri dari dua atau lebih komputer dan satu atau lebih server yang terhubung dalam suatu area. Area yang dimaksud adalah dalam satu gedung atau lingkungan.

2. MAN (*Metropolitan Area Network*)

   MAN pada dasarnya adalah LAN yang berukuran lebih besar. Jangkauan geografis MAN dapat mencakup beberapa gedung, kantor-kantor yang letaknya terpisah satu sama lain ataupun mencakup sebuah kota.

3. WAN (*Wide Area network*)

   WAN merupakan jaringan yang jangkauan geografisnya sangatlah luas, seringkali mencakup sebuah negara bahkan benua. WAN dirancang untuk menghubungkan komputer yang jaraknya sangat jauh, sehingga dibutuhkan media transmisi khusus seperti *fiber optic* ataupun satelit.

2.1.3 Berdasarkan Media Transmisi

Berdasarkan media transmisinya, jaringan komputer dapat dibagi menjadi dua jenis[7], yaitu:

1. *Wire Network (Guided Media)*

   Wire Network adalah jaringan komputer yang menggunakan kabel sebagai media transmisinya. Kabel yang digunakan pun ada beberapa macam, antara lain:

   - Kabel Coaxial
   - Kabel *Twisted Pair*
   - *Fiber Optic*

2. *Wireless Network (Unguided Media)*

   Wireless Network adalah jaringan komputer yang menggunakan gelobang radio, *microwave*, ataupun *infrared* sebagai media transmisinya. Spektrum yang digunakan pada *wireless network* antara 3 kHz hingga 900 THz.

2.1.4 Berdasarkan Fungsi

Berdasarkan fungsinya, jaringan komputer dapat dibagi menjadi dua jenis[7], yaitu:

1. *Client Server*

   Client server adalah jaringan komputer dimana salah satu komputer pada jaringan tersebut dijadikan sebuah *server* yang melayani komputer lain yang disebut *client*. Layanan yang diberikan bisanya berupa akses halaman *web, e-mail, file sharing* atau layanan lainya yang bisanya tersedia di dalam jaringan.

2. *Peer to Peer*

   Peer to Peer adalah jaringan komputer dimana setiap komputer dalam satu jaringan dapat bertindak sebagai server dan client secara bersamaan. Setiap komputer akan menerima atau memberikan akses dari atau ke komputer lain.

2.2 Topologi Jaringan Komputer

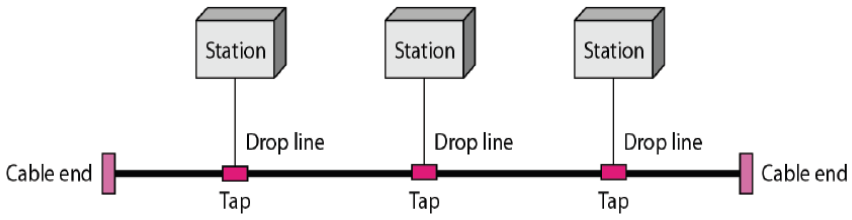
Topologi adalah pola aturan untuk menghungkan komputer dan komponen jaringan satu sama lain secara fisik dan pola hubungan antar komponen yang berkomunikasi di dalam jaringan[7].

2.2.1 Topologi Fisik

Berikut ini adalah jenis-jenis topologi fisik yang digunakan pada sebuah jaringan[4], yaitu:

1. Topologi *Bus*

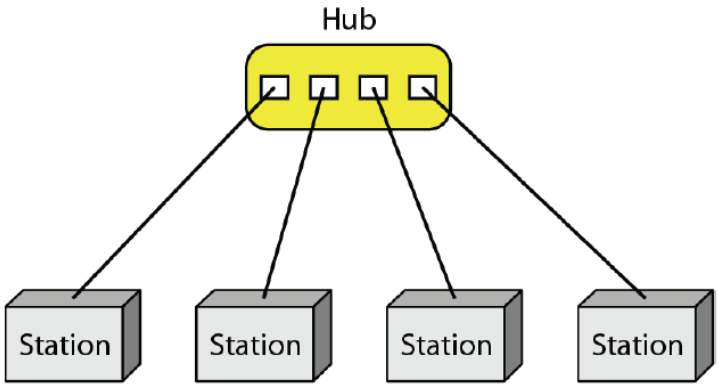
   Topologi *Bus* terdiri dari satu jalur kabel utama dimana pada setiap ujungnya dipasang sebuah terminator. Semua *node* pada jaringan terkoneksi ke kabel utama (*Backbone*) tersebut seperti yang terlihat pada Gambar II.1.



Gambar II.1 Topologi Bus

2. Topologi *Star*

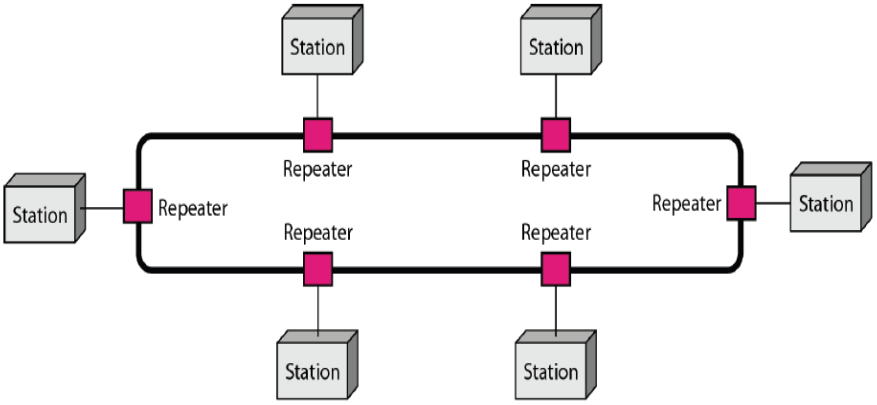
   Topologi ini dirancang agar setiap *node* yang terhubung dalam sebuah jaringan terkoneksi melalui sebuah konsentrator seperti yang terlihat pada Gambar II.2. Bisanya konsentrator ini menggunakan switch atau hub. Semua data yang akan dikirim akan melewati konsentrator terlebih dahulu sebelum dikirim ke tempat tujuan. Atas dasar ini pula konsentrator ini berfungsi untuk mengendalikan jaringan itu dan juga bertindak sebagai *repeater*.



Gambar II.2 Topologi Star

3. Topologi *Ring*

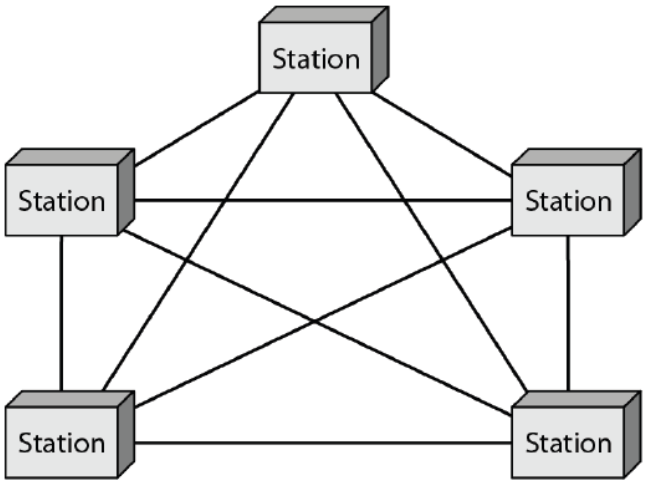
   Topologi Ring mempunyai konfigurasi yang mirip dengan topologi star, tetapi tanpa ada konsentrator, sehingga media transmisi akan menyerupai sebuah cincin tertutup seperti yang terlihat pada Gambar II.3 berikut ini.



Gambar II.3 Topologi Ring

4. Topologi *Mesh*

   Pada topologi *mesh* ini, setiap perangkat yang ada akan mempunyai koneksi khusus point-to-point terhadap semua perangkat lain yang ada dalam satu jaringan. Maksud dari koneksi khusus ini adalah bahwa satu koneksi ini hanya membawa paket antara dua perangkat yang saling terkoneksi seperti yang terlihat pada di Gambar II.4 bawah ini.



Gambar II.4 Topologi Mesh

2.2.2 Topologi Logikal

Topologi logikal mempunyai hubungan dengan bagaimana data ditransmisikan pada sebuah jaringan. Berikut ini adalah topologi logikal berdasarkan metode aksesnya[7].

1. *Shared Media Topology*

   Pada topologi ini setiap *node* atau *device* yang terhubung dalam jaringan dapat mengakses media jaringan kapan saja ketika media itu diperlukan. Akses bisa dilakukan kapan saja dan tidak ada pembatasan.

2. *Token Based Topology*

   Topologi ini menggunakan sebuah *frame* data bernama *token* yang ditransmisikan mengelilingi jaringan. Data yang ditransmisikan akan

melewati setiap *device* dengan satu arah. Akses setiap *device* akan diatur oleh *token* sehingga pengiriman data dilakukan secara bergantian.

2.3 Protokol Jaringan Komputer

Protokol adalah seperangkat aturan yang megatur komunikasi data. Protokol mendefinisikan apa itu komunikasi, bagaimana cara berkomunikasi dan apa yang terjadi ketika berkomunikasi[5].

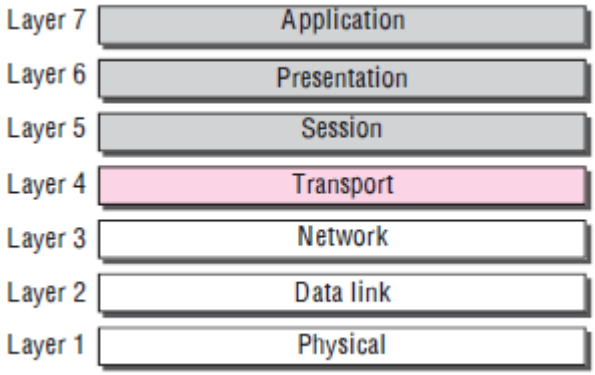
2.3.1 Model OSI (Open System Interconnection)

Didirikan pada tahun 1947, *International Standards Organizations* (ISO) adalah organisasi multinasional yang didedikasikan untuk menentukan standar-standar internasional untuk setiap aspek. Hampir tiga per empat negara di dunia bergabung dalam organisasi ini. Standar ISO yang menangani semua aspek dari komunikasi jaringan adalah *Open System Interconnection (OSI)* model[4]. OSI model ini diperkenalkan pada akhir 1970an.

Model OSI memungkinkan dua sistem yang berbeda untuk berkomunikasi terlepas dari arsitektur yang mendasari mereka. Tujuan dari model OSI adalah untuk menunjukkan bagaimana untuk memfasilitasi komunikasi antara sistem yang berbeda tanpa memerlukan perubahan logika dari *hardware* dan *software*. Model OSI bukanlah sebuah protokol, ini adalah model untuk memahami dan merancang arsitektur jaringan yang fleksibel, kuat, dan *interoperable*.

OSI adalah suatu standar komunikasi antar entitas yang terdiriatas 7 lapisan. Ketujuh lapisan tersebut mempunyai peran dan fungsi yang berbeda antara satu terhadap yang lainnya. Setiap layer bertanggung jawab secara khusus pada proses komunikasi data. Tujuan utama penggunaan model OSI adalah untuk membantu desainer jaringan memahami fungsi dari tiap-tiap layer yang berhubungan dengan aliran komunikasi data, termasuk jenis-jenis protokol jaringan dan metode transmisi. Model OSI dibagi menjadi 7 layer seperti yang ditunjukan oleh Gambar II.5, dengan karakteristik dan fungsinya masing-masing. Tiap layer harus dapat

berkomunikasi dengan layer di atasnya maupun di bawahnya secara langsung melalai beberapa protokol dan standard.



Gambar II.5 Layer pada Model OSI

Berikut ini adalah penjelasan untuk tiap-tiap lapisan dari Gambar II.5:

1. *Physical Layer (Layer 1)*

   Layer ini berfungsi untuk mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan (seperti halnya *Ethernet* atau *Token Ring*), dan pengabelan. Selain itu, *layer* ini juga mendefinisikan bagaimana *Network Interface Card* (NIC) dapat berinteraksi dengan media kabel atau radio**.**

2. *Data Link Layer (Layer 2)*

   Layer ini mendefinisikan bagaimana cara mengirimkan data melalui suatu media, baik media kabel maupun nirkabel dengan *physical addressing.* Tugas utama dari *layer* ini adalah *error checking, flow control* dan *Media Acces Control* untuk mengatur paket yang akan dikirim.

3. *Network Layer (Layer 3)*

   Layer ini berfungsi untuk mendefinisikan alamat-alamat IP, membuat *header* untuk paket-paket dan mencari jalur terbaik lalu kemudian melakukan *routing* melalui *internetworking* dengan menggunakan *router* dan *switch* agar data sampai ditujuan dengan benar.

4. *Transport Layer (Layer 4)*

   Lapisan ini mengatur keutuhan data, menerima data dari lapisan *session* dan meneruskannya ke lapisan *network* juga sebaliknya.

Lapisan ini berfungsi untuk memecah data ke dalam paket-paket data serta memberikan nomor urut ke paket-paket tersebut sehingga dapat disusun kembali pada sisi tujuan setelah diterima.

5. *Session Layer (Layer 5)*

   Lapisan ini menyiapkan saluran komunikasi dan terminal dalam hubungan antar terminal, mengoordinasikan proses pengiriman dan penerimaan serta mengatur pertukaran data. Lapisan ini membangun, mempertahankan dan menyelaraskan interaksi antara sistem komunikasi.

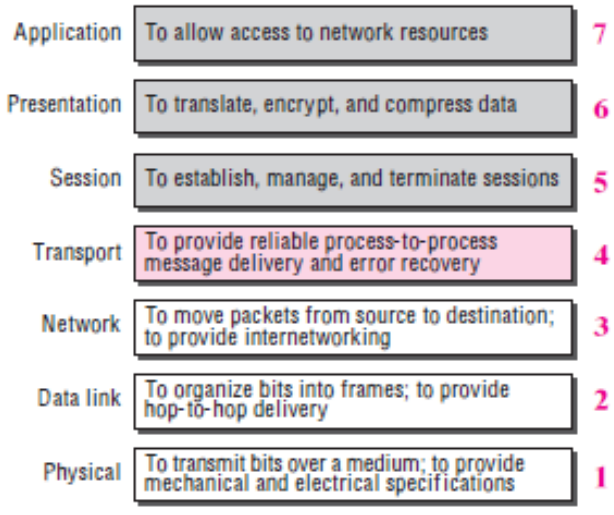
6. *Presentation Layer (Layer 6)*

   Layer ini bertugas untuk mendefinisikan format data, menampilkan data dan menangani kompresi dan enkripsi data.

7. *Application Layer (Layer 7)*

   Layer paling atas ini mengatur interaksi pengguna komputer dengan program aplikasi yang dipakai (*user interface*). Lapisan ini juga mengatur bagaimana aplikasi dapat mengakses jaringan.

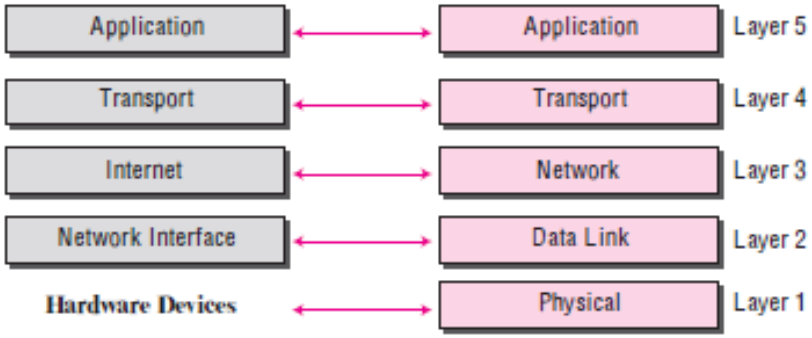
Secara garis besar, fungsi dari ketujuh *layer* tersebut bisa dilihat di Gambar II.6 berikut ini.



Gambar II.6 Fungsi OSI Layer

2.3.2 TCP/IP Protocol Suite

TCP/IP protocol suite dikembangkan sebelum model OSI. Oleh karena itu, lapisan di *TCP/IP protocol suite* tidak sama persis dalam model OSI. Protokol TCP/IP yang original didefinisikan sebagai empat lapisan perangkat lunak yang dibangun diatas perangkat keras. Tapi saat ini TCP/IP dianggap sebagai model dengan lima layer dengan lapisan yang bernama sama dengan yang ada di model OSI[4]. Gambar II.7 menunjukan kedua konfigurasi.



Gambar II.7 TCP/IP Original dan TCP/IP Saat Ini

Berikut ini penjelasan tiap lapisan dari Gambar II.7:

1. *Physical Layer*

   Pada lapisan *physical*, TCP/IP tidak mendefinisikan protokol yang spesifik. Mendukung semua protokol standar dan proprietary. Pada lapisan ini, komunikasi terjadi antara dua *hop* atau *node* baik itu komputer ataupun router.

2. *Data Link Layer*

   Layer ini berfungsi untuk menyimpan frame-frame data yang akan dikirim ke media jaringan. Layer ini bertugas mengatur semua hal yang diperlukan sebuah paket IP.

3. *Network Layer atau Internet Layer*

   Pada lapisan *network* (atau lebih akuratnya lapisan *internetwork*), TCP/IP mendukung Internet Protokol (IP). pada gilirannya, menggunakan empat protokol pendukung: ARP, RARP, ICMP, dan IGMP.

Layer ini berfungsi untuk melakukan routing dan pembuatan paket IP menggunakan teknik *encapsulation* (*header* dan *data*). Network/Internet layer memiliki tugas utama untuk memilih rute dalam sebuah jaringan. Selain itu, layer ini juga bertugas untuk melakukan *packet swictching* untuk mendukung tugas utama tersebut.

4. *Transport Layer*

   UDP dan TCP adalah protokol tingkat *transport* yang bertanggung jawab untuk pengiriman pesan dari suatu proses untuk proses lain. Sebuah protokol transportasi baru pada lapisan *transport* adalah SCTP yang dirancang untuk memenuhi standar kebutuhan beberapa aplikasi baru.

   Layer ini berfungsi membuat komunikasi antar dua host. *Layer Transport* menyediakan layanan pengiriman dari sumber data menuju ke tujuan data dengan cara membuat *logical connection* di antara keduanya.

5. *Application layer*

   Layer ini setara dengan gabungan atara *session, presentation* dan *application layer* pada layer OSI. Layer ini berfungsi menyediakan akses aplikasi terhadap jaringan TCP/IP. Layer ini menangani *high-level protocol,* masalah representasi data, proses *encoding* dan *dialog control* yang memungkinkan terjadinya komunikasi antar aplikasi jaringan.

2.4 IP Address

Internet terdiri dari jutaan *host* dan dimana masing–masing diidentifikasi secara unik oleh pengalamatan pada layer *Network.* Untuk berharap setiap *host* dapat mengetahui alamat dari *host* yang lain di dalam jaringan yang sangat besar, terutama di internet akan menguras banyak sumber daya[1]. Salah satu solusinya adalah membagi jaringan besar menjadi kumpulan grup yang lebih kecil sehingga dapat mengurangi *overhead* yang tidak perlu.

Untuk dapat membagi suatu jaringan, kita memerlukan pengalamatan yang terstruktur, yang juga akan digunakan untuk komunikasi data antar jaringan melalui internetwork.

Pengalamatan IP versi 4 memiliki pengalamatan terstruktur, terdiri dari 32 bit yang dibagi dalam 4 segmen. Tiap segmen terdiri atas 8 bit yang berarti memiliki nilai decimal dari 0 sampai 255. Jadi jaringan TCP/IP dengan alamat 32 bit ini mampu membuat sebanyak 2^{32} atau lebih dari 4 milyar *host*.

IP versi 4 didefinisikan pada RFC 791, dimana dijelaskan juga pembagian kedalam kelas–kelas. Alamat IP terdiri dari dua bagian yaitu *network* ID dan *host* ID. Dimana *network* ID menentukan alamat jaringan dan *host* ID menentukan alamat *host* atau komputer. Untuk menentukan alamat kelas IP, dilakukan dengan memeriksa 4 bit pertama (bit yang paling kiri) dari alamat IP.

Ada 5 kelas IP Address namun ada 3 kelas yang utama dalam TCP /IP, yakni Kelas A, Kelas B dan Kelas C sedangkan kelas D digunakan sebagai *multicast* dan kelas E sebagai *research* serta tidak digunakan untuk umum. Berikut ini adalah kelas-kelas pada IP Address versi 4.

1. IP Address kelas A

   Jika bit pertama dari IP Address adalah 0, maka network merupakan kelas A. bit awal dan 7 bit berikutnya (8 bit pertama) merupakan bit network sedangkan 24 bit terakhir merupakan bit host. Dengan demikian hanya ada 128 *network* di kelas A, yakni nomor 0.xxx.xxx.xxx sampai 127.xxx.xxx.xxx, tetapi setiap network dapat mendukung lebih dari 16 juta host.

Tabel II.1 Struktur IP Address Kelas A

0-127	0-225	0-225	0-225
0nnnnnnn	hhhhhhhh	hhhhhhhh	hhhhhhh
Bit-bit network ⟷	Bit-bit host ⟷		

2. IP Address kelas B

   Jika 2 bit pertama dari IP Address adalah 10, maka network merupakan kelas B. dua bitawal dan 14 bit berikutnya (16 bit

pertama) merupakan bit *network* sedangkan 16 bit terakhir merupakan bit host. Dengan demikian terdapat lebih dari 16 ribu *network* kelas B (64 x 256), yakni dari *network* 128.0.xxx.xxx sampai 192.255.xxx.xxx. tiap jaringan dapat menampung sekitar 65 ribu *host.*

Tabel II.2 Struktur IP Address Kelas B

128-191	0-225	0-225	0-225
10nnnnnn	nnnnnnnn	hhhhhhhh	hhhhhhh
Bit-bit network		Bit-bit host	

3. IP Address kelas C

   Jika bit pertama dari IP Address adalah 110,maka network merupakan kelas C. Tiga bit awal dan 21 bit berikutnya (24 bit pertama) merupakan bit network sedangkan 8 bit terakhir merupakan bit host. Dengan demikian terdapat lebih dari 2 juta network kelas C (32 x 256 x 256), yakni dari nomor 192.0.0.xxx sampai 223.255.255.xxx. Setiap network kelas C hanya mampu mendukung sekitar 256 host.

Tabel II.3 Struktur IP Address Kelas C

192-223	0-225	0-225	0-225
110nhhhh	hhhhhhhh	hhhhhhhh	hhhhhhh
Bit-bit network			Bit-bit host

4. IP Address kelas D

   Empat bit awal dari kelas D selalu diset 1110, sehingga *byte* pertama kelas D bernilai antara 224 - 239. Kelas D digunakan untuk keperluan multicast, yaitu suatu metode pengiriman yang digunakan bila suatu *host* ingin berkomunikasi dengan beberapa *host* sekaligus, dengan hanya mengirim satu datagram saja. Alamat dari kelas D adalah 224.0.0.0 sampai dengan 239.255.255.255. Alokasi

alamat tersebut ditujukan untuk keperluan sebuah grup, bukan untuk *host* seperti pada kelas A, B dan C.

Tabel II.4 Struktur IP Address Kelas D

224-239	0-225	0-225	0-225
1110hhhh	hhhhhhhh	hhhhhhhh	hhhhhhh
Multicast Address			

5. IP Address kelas E

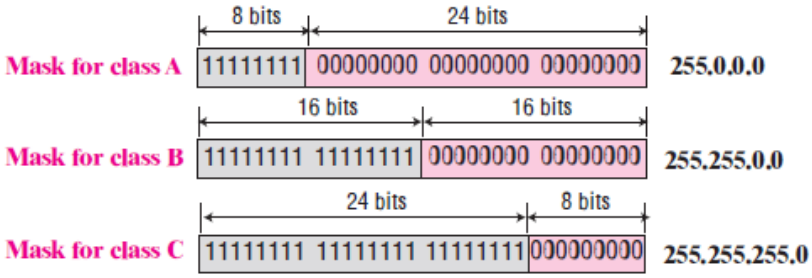
   Empat bit awal dari kelas E selalu diset 1111, sehingga *byte* pertama kelas E bernilai antara 240 – 254. Kelas E digunakan sebagai kelas eksperimental yang disiapkan untuk keperluan di masa mendatang.

Tabel II.5 Struktur IP Address Kelas E

240-255	0-225	0-225	0-225
1111hhhh	hhhhhhhh	hhhhhhhh	hhhhhhh
Eksperimental Address			

2.5 Network mask dan Subnet Mask

Secara standar, alamat IP didesain dengan dua level alamat yaitu bit *network* dan bit *host*. Untuk mencapai *host* dalam Internet, pertama-tama kita harus mencapai *network* nya lalu *host*. Untuk mencapai network kita harus mencari alamat network. Router akan menggunakan algoritma untuk mengekstraksi alamat *network* dari paket yang dikirim[4]. Untuk melakukan ini diperlukan sebuah netmask. Netmask atau *network* mask adalah 32 bit angka dengan *n* bit terkiri diset 1 dan 32-*n* paling kanan diset 0. Pada Gambar II.8 berikut ini dapat dilihat netmask pada tiap kelas IP.



Gambar II.8 Network Mask untuk tiap kelas IP

Untuk melihat alamat *network*, router menggunakan operator logika AND pada alamat IP tujuan dengan netmask tujuan.

Tetapi dengan pengalamatan dua level tersebut, jumlah *host* yang ada dalam satu *network* terbatas. Sehingga subnet atau subnetwork harus dibentuk didalam suatu *network*. Setiap subnet akan memiliki alamat masing-masing dalam *network*.

Karena *network* sudah terbagi menjadi beberapa subnetwork, maka diperlukan subnet mask untuk setiap subnetwork. Fungsi subnet mask ini sama seperti fungsi netmask. Dengan adanya subnet ini, maka akan membuat bit *network* ID menjadi lebih panjang dan bit *host* ID menjadi lebih pendek.

2.6 Switch

Switch adalah alat penghubung jaringan dengan *forwarding* berdasarkan alamat MAC. *Switch* membagi *collision domain* tetapi tidak membagi *broadcast domain*. *Switch* bekerja pada *layer 2* pada model OSI *(Data link Layer)* dan ada juga yang bekerja pada *layer* 3 (*Network layer*) pada model OSI. Perbedaan yang mendasar antara *switch layer* 2 dan *switch layer* 3 adalah kemampuan switch layer 3 dapat melakukan proses *routing*.

2.7 IDS (Intrusion Detection System)

Pengertian dari IDS berdasarkan NIST adalah perangkat lunak atau perangkat keras yang mengautomatisasi proses pemantauan kejadian yang terjadi pada sebuah sistem komputer atau jaringan, menganalisa kejadian tersebut untuk menentukan tanda-tanda masalah keamanan[3].

IDS berfungsi untuk membantu sistem informasi untuk bersiap dan menangani sebuah serangan yang datang pada jaringan. Itu dilakukan dengan cara mengumpulkan informasi dari berbagai sistem dan jaringan sumber lalu menganalisis informasi tersebut bila ada kemungkinan masalah keamanan.

IDS menyediakan layanan dasar yaitu:

1. Memonitoring dan menganalisis aktifitas dari user dan sistem.
2. Mengaudit konfigurasi dan kerentanan sistem.
3. Menilai integritas dari sistem penting dan data file.
4. Analisis statisktik dari pola aktifitas berdasarkan pencocokan terhadap serangan yang sudah dikenali.
5. Analisis aktifitas yang tidak wajar.
6. Mengaudit sistem operasi.

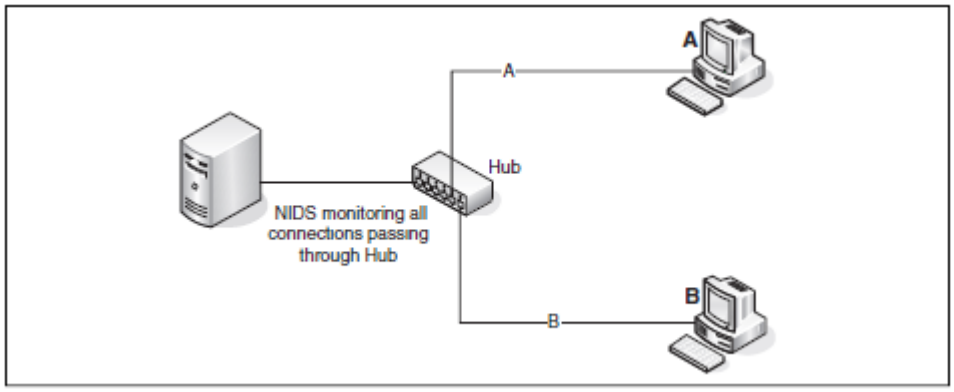
Yang bisa dilakukan oleh sebuah IDS menurut Danny Rozenblum adalah:

1. Bisa meningkatkan intergritas dari sebuah infrastruktur jaringan.
2. Bisa melacak aktifitas pengguna dari mulai masuk hingga selesai.
3. Bisa mengetahui dan melaporkan aktifitas perubahan data.
4. Bisa mengautomatisasi pekerjaan untuk memantau pencarian internet guna mengetahui penyerangan terbaru.
5. Bisa mengetahui jika sistem anda sedang diserang.
6. Bisa mengetahui kesalahan pada konfigurasi sistem anda.
7. Bisa membimbing administrator untuk membuat sebuah aturan penting untuk komputer atau jaringan.
8. Bisa membuat pengaturan keamanan untuk sistem oleh seorang yang bukan ahlinya.

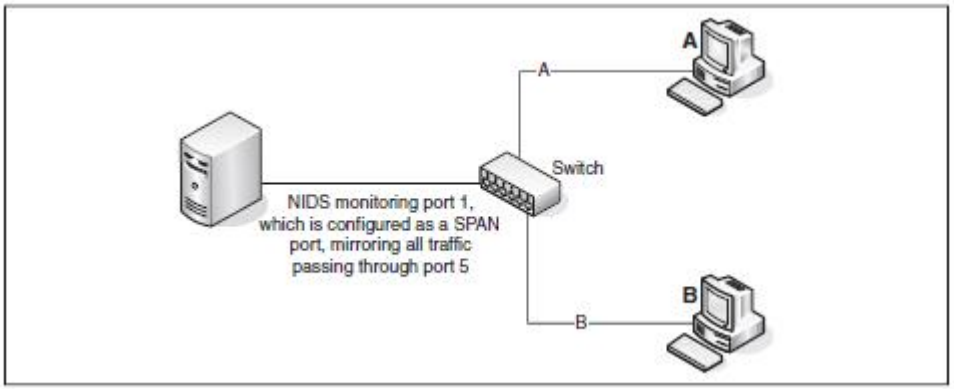
IDS pada umumnya terbagi menjadi dua jenis yaitu *rule based system* yang mendeteksi serangan berdasarkan aturan yang telah didefinisikan sebelumnya dan *adaptive system* yang mampu mengenali jenis serangan baru. Sedangkan terdapat dua teknik dalam IDS yaitu *Network based* IDS (NIDS) dan *Host based* IDS (HIDS).

2.7.1 NIDS (Network Based Intrusion Detection System)

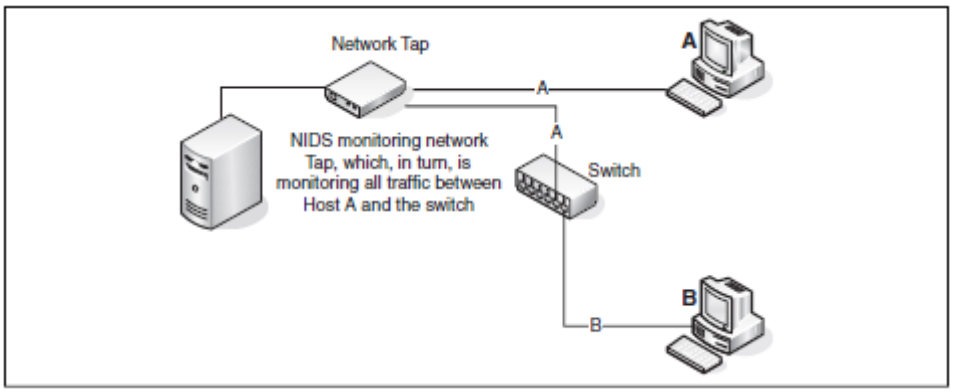
NIDS telah menjadi banyak digunakan selama beberapa dekade terakhir karena kemampuan mengesankan untuk memberikan pandangan granular dari apa yang terjadi pada jaringan. NIDS memonitor lalu lintas jaringan menggunakan *Network Interface Card* (NIC) yang terhubung langsung ke jaringan[6]. Pemantauan dapat diimplementasikan dengan menghubungkan NIC Anda ke HUB (Gambar II.9), sambungkan ke port SPAN pada switch (Gambar II.10), atau menghubungkan ke *network tap* (Gambar II.11), yang merupakan perangkat *inline* yang berada di antara dua antarmuka dan cermin lalu lintas yang lewat di antara perangkat.



Gambar II.9 NIDS Monitoring Menggunakan Hub



Gambar II.10 NIDS Monitoring Menggunakan SPAN Port Pada Switch



Gambar II.11 NIDS Monitoring Menggunakan Network Tap

2.7.2 HIDS (Host Based Intrusion Detection System)

Jenis IDS melibatkan perangkat lunak atau komponen agen yang dijalankan pada server, router, switch atau alat jaringan. Namun, versi agen harus melaporkan ke konsol atau dapat dijalankan bersama-sama pada host yang sama. Pada dasarnya, HIDS jauh lebih baik dalam mendeteksi dan merespon serangan jangka panjang seperti pencurian data[6].

Sebuah HIDS mendeteksi peristiwa pada server atau workstation dan dapat menghasilkan peringatan mirip dengan NIDS. Sebuah HIDS, mampu memeriksa semua aliran komunikasi. Teknik penghindaran NIDS, seperti serangan fragmentasi atau *session splicing* tidak berlaku karena HIDS mampu memeriksa *session* sepenuhnya seperti ketika *session* tersebut diberikan ke sistem operasi. Komunikasi terenkripsi dapat dipantau karena pemeriksaan HIDS akan dapat melihat lalu lintas sebelum dienkripsi. Ini berarti bahwa HIDS *signatures* masih dapat melawan serangan umum dan HIDS tidak dipengaruhi oleh enkripsi.

HIDS juga mampu melakukan pemeriksaan sistem tambahan yang hanya bisa dilakukan bila aplikasi IDS dipasang pada *host*, seperti *file integrity checking, registry monitoring, log analysis, rootkit detection* dan *active response*.

2.8 OSSEC

OSSEC adalah *open source Host-based Intrusion Detection Sistem* dengan jenis *rule based system*. Aplikasi ini melakukan beberapa pekerjaan seperti

analisis log, *file integrity checking, policy monitoring, rootkit detection, real-time alerting* dan *active response.* Selain dapat digunakan sebagai HIDS, OSSEC juga bisa digunakan sebagai alat log analisis, monitoring dan analisis *firewall,* juga log autentikasi *user*[6].

OSSEC memberikan fungsi yang sama seperti SIEM (*Security Information and Event Management*) dan STRM (*Security Threat Response Management*) dengan biaya lebih murah. Juga bila pada jaringan sudah terdapat SIEM / STRM, OSSEC dapat diintegrasikan didalamnya guna mendapatkan keuntungan tambahan.

Aplikasi ini menggunakan arsitektur *client-server*. *Agent* yang dimonitor dapat berjalan pada bermacam-macam sistem operasi, tetapi *server* haruslah dipasang pada sistem operasi BSD/Linux/Unix. Komunikasi antara keduanya menggunakan protokol UDP dengan port 1514 dan dienkripsi menggunakan algoritma symmetric key Blowfish.

2.9 Web Server Apache

Web Server adalah software *server* yang menjadi inti dari *World Wide Web* (WWW). *Web server* menunggu permintaan dari *client* yang menggunakan *browser* seperti Netscape Navigator, Internet Explorer, Mozilla, dan program *browser* lainnya. Jika ada permintaan dari *browser*, maka *web server* akan memproses permintaan itu dan kemudian memberikan hasil prosesnya berupa data yang diinginkan kembali ke *browser*. Data ini mempunyai format yang standar disebut dengan format SGML (*Standard General Markup Language*). Data yang berupa format ini kemudian akan ditampilkan oleh *browser* sesuai dengan kemampuan *browser* itu.

Apache adalah *Web Server* yang dapat dijalankan pada banyak sistem operasi (Unix, BSD, Linux, dan Microsoft Windows) yang berguna untuk melayani dan memfungsikan situs web. Protokol yang digunakan untuk melayani fasilitas ini adalah HTTP.

Apache memiliki fitur-fitur canggih seperti pesan kesalahan yang dapat dikonfigurasi, autentikasi berbasis basis data dan lain-lain. Apache juga didukung oleh sejumlah antarmuka pengguna berbasis grafik (GUI) yang memungkinkan

penanganan *server* menjadi mudah. Apache merupakan perangkat lunak sumber terbuka dikembangkan oleh komunitas terbuka yang terdiri dari pengembang-pengembang dibawah naungan *Apache Software Foundation*.

2.10 Sistem Operasi Ubuntu

Salah satu komponen utama dalam jaringan adalah sistem operasi komputer. Sistem operasi ini berfungsi untuk mengatur komunikasi jaringan berupa dokumen, printer, scanner dan perangkat-perangkat lainnya. Sistem operasi dapat membedakan arsitektur dalam pemanfaatan fasilitas-fasilitas yang ada di jaringan. Misalkan membedakan perangat jaringan seperti *Ethernet* dan *Token Ring* atau arsitektur lainnya.

Banyak sekali sistem operasi yang ada pada saat ini. Salah satunya adalah Linux dengan berbagai distro atau distribusinya, seperti RedHat, Mandrake, Debian, SuSe, Slakware, CentOS, Ubuntu dan lain sebagainya. Masing-masing distro Linux mempunyai keuntungan tersendiri, tergantung digunakan untuk apa.

Ubuntu berasal dari bahasa Afrika yakni "Humanity to Others" yang berarti "Kemanusiaan Untuk Sesama". Atas dasar itulah diluncurkannya Linux Ubuntu yang dirilis pada tahun 2004. Sistem operasi ini adalah merupakan turunan dari sistem operasi linux yang lain, yakni Debian.

Ubuntu itu sendiri dibuat dengan tujuan selalu gratis tanpa adanya biaya lisensi, bersifat *open source*, dan siap untuk dipergunakan dalam kondisi yang stabil. Ubuntu didukung oleh perusahaan bernama Canonical, Ltd yang memiliki tujuan untuk membantu perkembangan, distribusi, dan promosi dari produk-produk yang bersifat *open source*. Perusahaan ini bermarkas di Eropa dan dipimpin oleh seseorang bernama Mark Shuttleworth. Sejak pertama kali diluncurkan, Ubuntu mendapat perhatian yang sangat besar dari pengguna Linux yang lain. Hal ini disebabkan karena kestabilan yang dimiliki oleh Ubuntu itu sendiri. Selain itu kenyamanan dan kemudahan yang dimiliki Ubuntu menjadi daya tarik yang besar bagi pengguna Linux di seluruh belahan dunia.