MODUL PEMBELAJARAN
ADMINISTRASI SERVER DAN KEAMANAN JARINGAN
Tingkat XII TKJ
T.P. 2018/2019

A. Control Panel Hosting

Kontrol panel hosting menyediakan solusi elegan sebagai host dari beberapa situs website yang berjalan pada Share hosting, VPS (Virtual Private Server) dan Dedicated Server. Kontrol panel hosting semacam ini menawarkan kemudahan untuk mengelola perangkat lunak berbasis web untuk menyederhanakan proses penanganan server, tanpa perlu memiliki pengetahuan akan server administration.

Kontrol panel yang paling populer saat ini dan kuat brandingnya adalah cPanel dan Plesk. Kedua kontrol panel ini merupakan aplikasi berbayar yang dibayar setiap bulan bagi sebuah provider hosting untuk di install dalam servernya. Namun untungnya, ada beberapa kontrol panel alternatif yang bersifat open source yang tersedia untuk di download secara gratis dengan fitur hampir sama dengan yang berbayar, yaitu sebagai berikut:

1. Cpanel

Cpanel Adalah kontrol panel hosting yang berbasis Unix/Linux. Antarmuka grafisnya membantu Anda untuk mengelola website beserta account hosting Anda dengan sangat mudah dan cepat. Cpanel memberi Anda akses penuh atas berbagai elemen pengaturan dari situs web dan administrasi hostingnya melalui web browser misalnya seperti Membuat database, membuat account email, auto responder, dan mengelola file website.

2. Plesk

Plesk adalah control panel hosting yang mirip dengan cPanel. Plesk memungkinkan Anda untuk mengelola account hosting Anda melalui antarmuka berbasis web. Anda dapat menginstall kontrol panel ini didalam VPS atau dedicated server. Plesk juga memungkinkan Anda untuk mengontrol ribuan virtual host dalam satu mesin. Kontrol panel memungkinkan Anda untuk mengotomatisasi banyak tugas yang pada gilirannya mengurangi biaya dan sumber daya. Hal ini juga meningkatkan profitabilitas, efisiensi dan kepuasan pelanggan.

Fitur yang ditawarkan oleh Plesk, yaitu seperti berikut ini:

a) Membuat akun FTP.
b) Mengelola dan membuat akun email dan database seperti MySQL dan PsotgreSQL.
c) Menambahkan domain dan subdomain.
d) Restore dan Backup data.
e) Mengelola DNS dan sumber daya lainnya.

3. ISPConfig

ISPConfig adalah kontrol panel open source multi bahasa yang memungkinkan Anda untuk mengelola beberapa server di bawah satu control panel. ISPConfig berlisensi di bawah lisensi BSD. Kontrol panel open source ini juga mampu mengelola FTP, SQL, BIND DNS, database dan virtual server.

Fitur yang disediakan oleh ISPConfig adalah seperti berikut ini:

a) Dapat memanage lebih dari satu server dari satu panel kontrol.
b) Antarmuka web yang memudahkan untuk administrator, reseller dan klien login.
c) Mendukung webserver seperti Apache dan Nginx.
d) Konfigurasi mirroring dan cluster.
e) Mengelola akun email dan FTP.
f) Dan masih banyak lagi

4. Kloxo

Kloxo adalah salah satu kontrol panel website yang terbilang canggih dan disediakan secara gratis untuk distro Redhat dan CentOS. Memiliki fitur seperti FTP, spam filter, PHP, Perl, CGI, dan banyak lagi. Fitur seperti Messaging, Backup restore dan modul Ticketing juga tersedia

dalam kontrol panel tersebut. Ini membantu user untuk mengelola/menjalankan kombinasi Apache dengan BIND, dan beralih antarmuka antara program ini tanpa kehilangan data Anda.

5. Zpanel

Zpanel adalah kontrol panel hosting yang disediakan secara gratis dan sangat mudah digunakan pada kontrol panel webhosting kelas enterprise seperti Linux, UNIX, MacOS, dan Microsoft Windows. Zpanel ditulis dalam bahasa PHP murni dan berjalan dengan baik pada Apache, PHP dan MySQL. Muncul dengan serangkaian fitur inti penting untuk menjalankan layanan hosting web Anda. Fitur inti tersebut meliputi Apache Web Server, hMailServer, FileZilla Server, MySQL, PHP, Webalizer, RoundCube, phpMyAdmin, phpSysInfo, FTP Jailing dan masih banyak lagi.

6. Webmin

Webmin merupakan kontrol panel webhosting yang powerfull dan sangat fungsional. Software yang dirancang untuk platform Unix dan Linux dengan cara yang sederhana. Webmin cukup mampu untuk mengelola berbagai komponen lingkungan berbasis web dari pengaturan webserver untuk maintaining FTP dan Email Server.

Fitur yang disediakan pada Webmin, adalah sebagai berikut:

a) Mengkonfigurasi dan membuat server virtual pada Apache.
b) Mengelola, menginstal atau menghapus paket perangkat lunak (RPM format).
c) Untuk keamanan, Anda dapat menyetting fitur firewall.
d) Mengubah pengaturan DNS, alamat IP, konfigurasi routing.
e) Mengelola database, tabel dan field MySQL.

7. EHCP

EHCP (*Easy Hosting Control Panel*) adalah software kontrol panel gratis untuk menjaga server hosting berbasis web. Dengan penggunaan EHCP Anda dapat mengelola database MySQL, account email, account domain, account FTP dan banyak lagi. Ini adalah satu-satunya control panel yang telah built-in support untuk Nginx dan PHP-FPM yang tidak menggunakan Apache dan memberikan kinerja yang baik untuk server low end.

8. DTC

Domain Technologie Control (DTC) adalah control panel hosting terutama untuk admin dan akuntansi layanan hosting GPL. Dengan bantuan interface web berbasis GUI, DTC dapat mendelegasikan tugas seperti membuat email, account FTP, subdomain, database dan banyak lagi. Ia mengatur database MySQL yang berisi semua informasi hosting.

9. Interworx

Interworx adalah sistem manajemen server Linux dan kontrol panel webhosting. Interworx memiliki seperangkat tool yang memberikan kewenangan administrator untuk memerintah servernya sendiri dan end user dapat melihat atau meninjau hasil pengelolaan website mereka. Kontrol panel ini pada dasarnya dibagi menjadi dua mode operasi, yaitu:

a) **Nodeworx**, yaitu modus administrator yang membantu mengelolaan server.
b) **SiteWorx**, yaitu website owner view yang membantu end users untuk mengelola account mereka hosting dan fitur-fitur didalamnya.

10. Ajenti

Ajenti merupakan satu-satunya kontrol panel berbasis open source yang kaya fitur, kuat dan ringan. Kontrol panel yang menyediakan antarmuka web responsif untuk mengelola server kecil set-up dan juga paling cocok untuk Dedicated dan VPS hosting. Muncul dengan banyak built-in plugin untuk mengkonfigurasi dan mengelola perangkat lunak server dan layanan seperti Apache, Nginx, MySQL, FTP, Firewall, File System, Cron, Munin, Samba, Squid dan banyak program lainnya seperti File Manager, Kode Editor untuk developer serta akses Terminal.

B. Share Hosting Server

Hosting adalah tempat atau jasa internet untuk membuat halaman website yang telah anda buat menjadi online dan bisa diakses oleh orang lain. Sedangkan Hosting Itu sendiri adalah

jasa layanan internet yang menyediakan sumber daya server-server untuk disewakan sehingga memungkinkan organisasi atau individu menempatkan informasi di internet berupa HTTP, FTP, EMAIL atau DNS.

Server hosting terdiri dari gabungan server-server atau sebuah server yang terhubung dengan jaringan internet berkecepatan tinggi. Ada beberapa jenis layanan hosting yaitu shared hosting, VPS atau Virtual Dedicated Server, dedicated server, colocation server.

a) Shared Hosting adalah menggunakan server hosting bersama sama dengan pengguna lain satu server dipergunakan oleh lebih dari satu nama domain. Artinya dalam satu server tersebut terdapat beberapa account yang dibedakan antara account satu dan lainnya dengan username dan password.
b) VPS, Virtual Private Server, atau juga dikenal sebagai Virtual Dedicated Server merupakan proses virtualisasi dari lingkungan software sistem operasi yang dipergunakan oleh server. Karena lingkungan ini merupakan lingkungan virtual, hal tersebut memungkinkan untuk menginstall sistem operasi yang dapat berjalan diatas sistem operasi lain.
c) Dedicated Server adalah penggunaan server yang dikhususkan untuk aplikasi yang lebih besar dan tidak bisa dioperasikan dalam shared hosting atau virtual dedicated server. Dalam hal ini, penyediaan server ditanggung oleh perusahaan hosting yang biasanya bekerja sama dengan vendor.
d) Colocation Server adalah layanan penyewaan tempat untuk meletakkan server yang dipergunakan untuk hosting. Server disediakan oleh pelanggan yang biasanya bekerja sama dengan vendor.

Ketika anda memutuskan untuk memiliki blog atau website yang hosting sendiri, maka anda harus bisa memilih-milih jasa web hosting yang baik. Yang harus anda perhatikan ketika memilih hosting untuk blog atau website anda adalah:

a) Kebutuhan anda terhadap space dan bandwidth. Semakin banyak tulisan anda, maka semakin besar space yang akan dibutuhkan. Semakin banyak pengunjung blog anda maka semakin besar bandwidth yang dibutuhkan agar tidak terjadi server full load.
b) Perhatikan layanan dan fitur dari tempat anda akan menghostingkan blog atau website anda. Bisa mencakup software apa saja yang ada di hostingnya serta support dari jasa hostingnya.
c) Target pembaca. Jika anda memilih target pembaca dari dalam negeri ada baiknya menggunakan server lokal saja agar lebih menghemat bandwidth. Tetapi jika anda memilih target yang global, maka tak ada salahnya anda memilih server luar negeri seperti di Amerika. Tapi keadaan ini tidaklah mutlak.
d) Harga yang pas. Konsultasikan kepada mereka yang lebih paham tentang kebutuhan hosting anda agar jasa yang anda sewa sesuai dengan uang yang akan anda keluarkan.

C. Vitual Private Server

VPS (*Virtual Private Server*) secara sederhana dapat diartikan computer server yang berada di dunia maya. Artinya tidak nyata (*virtual*) namun kita dapat memiliki dengan cara menyewa. Hampir sama dengan komputer di dunia nyata,

VPS memiliki harddisk, memory, prosesor sampai dengan operasi sistem (OS). Yang paling menyolok dari Pengertian VPS adalah beroperasi selama 24 jam tanpa henti dan terhubung dengan jaringan internet. Dengan demikian data serta aplikasi yang ada di VPS dapat diakses atau dijalankan terus menerus selama 24 jam lewat jaringan internet kapan dan dimana saja.

VPS dapat dibagi menjadi beberapa VM (*Virtual Machines*), dimana di setiap VM adalah berupa "*Virtual server*" yang dapat di install system operasi tersendiri. VPS terasa seperti sebuah Dedicated Server. Dibanding dengan shared hosting, menyewa VPS akan mendapatkan resource yang lebih baik sehingga tidak terganggu jika ada problem pada website yang dikelola. Selain itu VPS mendapatkan root akses sehingga lebih leluasa dalam mengkustomasi server sesuai kebutuhan anda.

Kelebihan VPS dibanding Dedicated Server antara lain VPS lebih Fleksibel. Anda hanya perlu membayar resource yang anda butuhkan, nanti jika kebutuhan meningkat, bisa di upgrade tahap demi tahap. Namun, anda dituntut belajar VPS mengingat pengopersiannya sedikit rimit dari pada shared hosting yang bisanya tinggal pakai saja.

Fungsi VPS (*Virtual Private Server*)

a) SSH Tunneling. Berfungsi hampir sama dengan VPN yaitu mengubah IP menjadi IP VPS tersebut. (Konten – VPS – ISP – Komputer anda)
b) VPN atau Virtual Private Network berfungsi mirip seperti SSH Tunneling, yaitu mengubah IP karena Konten akan melewati VPS Terlebih dahulu sebelum mengirim ke ISP anda, lalu ke Komputer anda.
c) Proxy berfungsi mirip seperti VPN, tetapi tidak seleluasa VPN dalam penggunaanya.
d) VPS dapat difungsikan menjadi tempat menyimpan Web anda (Web Hosting). Anda dapat dengan leluasa menggunakan resource VPS anda untuk Web Pribadi anda juga.
e) VPS juga dapat digunakan untuk menyimpan File-file yang ingin anda bagikan secara online dengan orang-orang disekitar anda atau dengan publik.
f) VPS juga dapat dipergunakan untuk Game Private Server seperti Ragnarok, RF Online, Minecraft, dan lain-lainnya.
g) Shoutcast Hosting untuk membuat Radio Online sendiri menggunakan VPS.

VPS (*Virtual Privat Server*) adalah teknologi server side tentang system operasi dan perangkat lunak yang memungkinkan sebuah mesin dengan kapasitas besar dibagi ke beberapa virtual mesin. Tiap virtual mesin ini melayani sistem operasi dan perangkat lunak secara mandiri dan dengan konfigurasi yang cepat. Secara global VPS sering digunakan untuk Cloud Computing, Software Bot, Menjalankan Software robot forex (untuk trading), dsb.

VPS juga dapat di artikan sebagai sebuah metode untik mempartisi atau membagi sumber daya atau resource sebuah server menjadi beberapa server virtual. Server virtual tersebut memiliki kemampuan menjalankan operating system sendiri seperti layaknya sebuah server. Bahkan Anda dapat me-reboot sebuah server virtual secara terpisah (tidak harus mem-reboot server utama).

Kita dapat mengendalikan VPS dengan Remote Access Dekstrop atau biasa di sebut pengendali jarak jauh, dengan menggunakan aplikasi seperti Putty untuk yang menggunakan OS windows dan Terminal untuk Linux.

Dasar-Dasar VPS

VPS bekerja seperti sebuah server yang terpisah. VPS memiliki processes, users, files dan menyediakan full root access. Setiap VPS mempunyai IP address, port number, tables, filtering dan routing rules sendiri. VPS dapat melakukan configurasi file untuk sistem dan aplikasi software.

Setiap VPS dapat memiliki system libraries atau mengubah menjadi salah satu system libraries yang lain. Setiap VPS dapat delete, add, modify file apa saja, termasuk file yang ada di dalam root, dan menginstall software aplikasi sendiri atau menkonfigurasi root application software.

Dalam sebuah VPS, resource server yang alokasikan adalah meliputi CPU Core, CPU Usage, RAM, dan Storage atau ruang penyimpananan. Spesifikasi sebuah VPS itu sendiri berbagai macam, baik dari segi Hard disk, memorynya, jenis prosesornya, pilihan operasi sistemnya (Windows/Linux/ dan sebagainya).

VPS sudah terhubung dengan internet selama 24 jam dengan kecepatan tinggi agar setiap user bisa dengan mudah mengaksesnya. VPS biasanya diakses melalui komputer pribadai menggunakan software Remote Desktop Connection (RDC) yang biasanya sudah tersedia di operasi sistem WINDOWS.

VPS dilengkapi dengan pengaturan sendiri untuk init script, users, pemrosesan, filesystem dan sebagainya. VPS bekerja seperti sebuah server yang terpisah memiliki processes, users, files dan menyediakan full root access. Setiap VPS mempunyai ip address, port number, tables, filtering dan routing rules sendiri. VPS juga dapat melakukan configurasi file untuk sistem dan aplikasi software.

Dengan VPS Anda sebagai pengguna tidak perlu lagi merawat Server Virtual ini, karena perusahaan penyedia VPS akan merawat secara berkala serta mengupgrade OS, RAM, dsb.

Penyewaan VPS terdiri dari 2 Macam:

a) VPS Managed : Server kosong /hanya diberi IP, root dan password.
b) VPS Unmanaged : Suda terinstal OS Linux atau Windows atau yg lainnya, sesuai dengan hosting.

Fungsi VPS

VPS memiliki banyak sekali fungsi dan kegunaan, diataranya adalah:

a) **Web Hosting** Salah satu penggunaan yang populer adalah untuk menyediakan web hosting. Virtual Private Server sangat tepat untuk level menengah dan situs web perusahaan, dimana aplikasi membutuhkan konfigurasi yang spesifik dan hanya bisa dilakukan oleh Superuser. Penggunaan ini juga cocok untuk memulai bisnis web hosting dengan anggaran yang terbatas namun layanan dengan yang berkualitas.
b) **Backup Server** Kebutuhan backup server untuk menjamin layanan selalu berjalan normal adalah sangat penting. Backup server ini bisa meliputi situs web, surel, berkas, dan basis data. Semua layanan ini berada dalam kondisi fisik dan logical yang terpisah sehingga meminimalisasi kerusakaan atau kehilangan data.
c) **Sebagai file server** atau storage server dimana kita bisa menyimpan file dan data baik melalui ftp, maupun http.
d) **Sebagai server remote desktop**, dimana kita bisa mendownload dan mengupload file secara remote, menjalankan aplikasi forex, bot/ robot & automation, spinner.
e) **Sebagai host server** untuk VPN dan Tunneling.
f) **Application Hosting** Dengan Virtual Private Server, memungkinkan untuk membangun custom mission critical software tanpa harus mengeluarkan biaya yang terlalu mahal. Melakukan outsource development aplikasi juga sudah menjadi trend untuk menghemat biaya sehingga investasi jauh lebih efisien.
g) **Development/Test Environments** Virtual Private Server juga membantu untuk melakukan serangkaian development testing secara efisien, beberapa sistem operasi dan alamat IP publik dengan mudah bisa dilakukan, koneksi secara remote untuk reboot dan penggantian interface cukup dilakukan dengan cepat, sama seperti halnya mempunyai 1 rak yang penuh dengan server testing.
h) **Educational Outpost** Virtual Private Server menjadikan ajang untuk bereksperimen UNIX Operating System dengan berbagai macam distribusi sekaligus. Membuat proses ekperimen lebih beragam dan lebih mudah membandingkannya.

Jadi, ketika Anda memutuskan untuk membangun sebuah website atau blog untuk kepentingan komersial, sangat disarankan untuk menyewa VPS. Karena VPS sangat membantu kinerja Anda dalam mengelola website yang Anda miliki, bahkan lebih dari satu website. Khusunya bagi para web developer yang memiliki domain dalam jumlah banyak tentu Anda akan sangat membutuhkan kustomisasi untuk berbagai macam aplikasi yang Anda gunakan.

Pengertian Virtual Private Server (VPS) inilah bisa menjadi referensi bagi Anda yang hendak membangun domain-domain tersebut. VPS juga sangat cocok bagi Anda yang mengutamakan privasi dalam mengelola sebuah website. Selain itu dari Pengertian *Virtual Private Server* (VPS) diatas Anda dapat menarik kesimpulan bahwa server ini memberikan fasilitas yang mungkin tidak terdapat pada paket *shared hosting*. Masih banyak fungsi lainnya yang dapat diterapkan di VPS misalnya Rapidleech, Torrentleech, DNS Name Server, Proxy Server, dan lain-lain.

Kelemahan dari VPS itu sendiri yaitu agak lambat proses menjalankannya di PC/laptop. Ini biasanya dikarenakan oleh kecepatan internet pengguna dalam mengakses VPS itu sendiri, sedangkan VPS itu sendiri sudah bekerja dengan baik dan dengan kecepatan yang tinggi dalam melakukan proses ke internet.

D. Dedicated Hosting Server

Selain *Pengertian Dedicated Server*, pertanyaan lainnya adalah tentang Apa itu Virtual Server? *Dedicated server adalah* penyewaan satu server secara utuh tanpa dibagi dengan user yang lain, sehingga hanya Anda sendiri yang menempati dan menggunakan dedicated server tersebut. Anda berkuasa penuh atas pengelolaan dedicated server tersebut termasuk pemilihan sistem operasi, hardware, dan sebagainya. Namun anda tidak perlu repot untuk

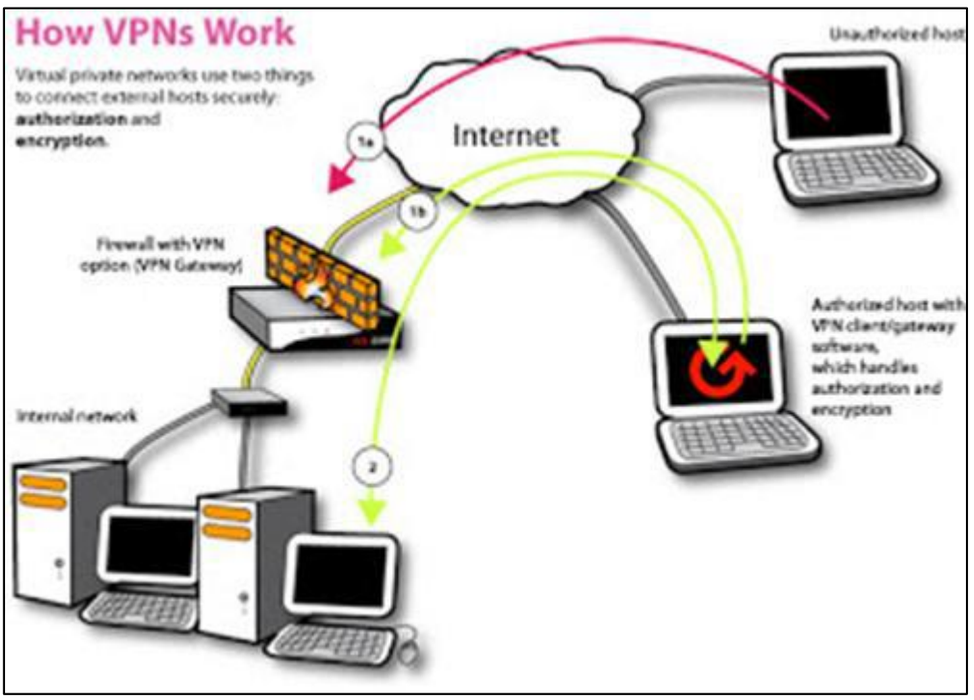
melakukan instalasi dan penyediaan hardware lainnya, karena kami menyediakan support untuk instalasi software tersebut sehingga siap di gunakan. Sementara Virtual Server Adalah layanan yang mirip dengan Dedicated Server, Namun tidak memiliki fisik server, karena dibangun menggunakan teknologi virtual dari dedicated server.

Dedicated Server akan menjadi satu-satunya pilihan ketika bisnis / usaha atau situs anda berkembang dengan baik. Traffic pengunjung yang semakin bertambah akan menuntut power lebih dari server yang melayaninya. Provider biasanya menawarkan layanan ini dengan pilihan spesifikasi dan harga bertingkat sesuai dengan budget dan kebutuhan Anda, sehingga Anda tetap bisa menggunakan layanan secara optimal.

Jenis Layanan Dedicated Server

Layanan ini bersifat unmanaged, dukungan teknis diberikan sampai pada tatanan jaringan dan hardware, kami hanya melakukan instalasi dan konfigurasi awal sesuai dengan permintaan anda. Untuk Dedicated Server indonesia, Server akan diletakkan di Data Center Indonesia yang terkoneksi dengan Jaringan 1 GBps Shared IIX / Open IXP Connection Unmetered, serta link internasional melalui Nusanet Internet Service Provider sebesar 5 Mbps Shared International Connection. Pilihan untuk bandwidth dedicated juga dapat anda miliki apabila anda membutuhkannya.

E. VPN Server



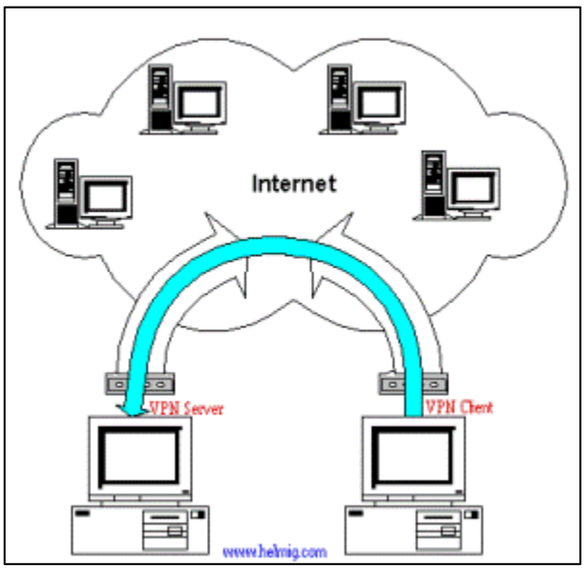
VPN merupakan singkatan dari *Virtual Private Network*, yaitu sebuah koneksi private melalui jaringan publik (dalam hal ini internet). Disini ada 2 kata yang dapat kita garis bawahi yaitu:

a) **virtual network**, yang berarti jaringan yang terjadi hanya bersifat virtual. Tidak ada koneksi jaringan secara riil antara 2 titik yang akan berhubungan.
b) **private**, jaringan yang terbentuk bersifat private dimana tidak semua orang bisa mengaksesnya. Data yang dikirimkan terenkripsi sehingga tetap rahasia meskipun melalui jaringan publik.

Dengan VPN ini kita seolah-olah membuat jaringan didalam jaringan atau biasa disebut tunnel (terowongan). **Tunneling** adalah suatu cara membuat jalur privat dengan menggunakan infrastruktur pihak ketiga. VPN menggunakan salah satu dari tiga teknologi tunneling yang ada yaitu: PPTP, L2TP dan standar terbaru, Internet Protocol Security (biasa disingkat menjadi IPSec). VPN merupakan perpaduan antara teknologi tunneling dan enkripsi.

Dibawah ini adalah gambaran tentang koneksi VPN yang menggunakan protokol PPTP. PPTP (Pont to Point Tunneling Protocol) adalah sebuah protocol yang mengizinkan hubungan

Point-to Point Protocol (PPP) melewati jaringan IP, dengan membuat Virtual Private Network (VPN).



Cara Kerja VPN

Dari gambar diatas secara sederhana cara kerja VPN (dengan protocol PPTP) adalah sebagai berikut:

a) VPN membutuhkan sebuah server yang berfungsi sebagai penghubung antar PC, **Server VPN** ini bisa berupa komputer dengan aplikasi VPN Server atau sebuah Router, misalnya MikroTik RB 750.
b) Untuk memulai sebuah koneksi, komputer dengan aplikasi VPN Client mengontak Server VPN, VPN Server kemudian memverifikasi username dan password dan apabila berhasil maka VPN Server memberikan IP Address baru pada komputer client dan selanjutnya sebuah koneksi / tunnel akan terbentuk.
c) Untuk selanjutnya komputer client bisa digunakan untuk mengakses berbagai resource (komputer atu LAN) yang berada dibelakang VPN Server misalnya melakukan transfer data, ngeprint dokument, browsing dengan gateway yang diberikan dari VPN Server, melakukan remote desktop dan lain sebagainya.

Keuntungan VPN

Beberapa keuntungan dari teknologi VPN diantaranya adalah:

a) Remote Access, dengan VPN kita dapat mengakses komputer atau jaringan kantor, dari mana saja selama terhubung ke internet
b) Keamanan, dengan koneksi VPN kita bisa berselancar dengan aman ketika menggunakan akses internet publik seperti hotspot atau internet cafe.
c) Menghemat biaya setup jaringan, VPN dapat digunakan sebagai teknologi alternatif untuk menghubungkan jaringan lokal yang luas dengan biaya yang relatif kecil, karena transmisi data teknologi VPN menggunakan media jaringan public yang sudah ada tanpa perlu membangun jaringan pribadi.

Kekurangan atau Kelemahan VPN

Beberapa kekurangan dari VPN diantaranya adalah:

a) Koneksi internet (jaringan publik) yang tidak bisa kita prediksi. Hal ini dapat kita maklumi karena pada dasarnya kita hanya "nebeng" koneksi pada jaringan pihak lain sehingga otomatis kita tidak mempunyai kontrol terhadap jaringan tersebut.
b) Perhatian lebih terhadap keamanan. Lagi-lagi karena faktor penggunaan jaringan publik, maka kita perlu memberikan perhatian yang lebih untuk mencegah terjadinya hal-hal yang tidak diinginkan seperti penyadapan, hacking dan tindakan cyber crime pada jaringan VPN.

Manfaat & Kegunaan VPN

VPN merupakan paket solusi komunikasi data (baik berupa data suara, video, atau file digital lainnya) yang memberikan layanan berbasis IP ke end user. Layanan VPN dapat mengirimkan data antar-dua komputer yang melewati jaringan publik, misal nya Internet, sehingga seolah-olah terhubung secara point to point.

Beberapa manfaat dan kegunaan VPN yaitu:

a) Kemampuan membentuk jaringan LAN yang tidak di batasi tempat dan waktu, karena koneksitasnya dilakukan via internet. Koneksi internet apapun dapat digunakan seperti Dial-Up, ADSL, Cable Modem, WIFI, 3G, CDMA Net, GPRS, dan sistem PVN ini paling tepat digunakan untuk penggunaan suatu database terpusat untuk mengkomunikasikan antara server dan client via internet seperti Aplikasi Perdagangan, Purchase, P.O.S, Accounting, Cashir, Billing system, General Ledger, dll.
b) Tidak ada ketergantungan terhadap keharusan memiliki IP Publik yang berharga mahal. Cukup menggunakan IP dynamic saja dengan kata lain asal PC anda bisa berinternet.
c) Mampu mencetak dokumen dari rumah kekantor via internet.
d) Mampu melakukan transfer data atau remote view untuk mengendalikan komputer di rumah/kantor anda dimana saja
e) Tidak membutuhkan Peralatan/hardware tambahan yang berfungsi sebagai IP forwarder/Port Forwader yang menambah investasi anda.
f) Dapat melakukan koneksitas dengan PC dikantor anda misalnya dengan memanfaatkan software yang bekerja dijaringan LAN seperti Citrix, Windows Terminal Server 2003, VNC, Radmin, VOIP, dll
g) Dengan menggunakan software yang bekerja dijaringan LAN anda dapat melakukan pertukaran data secara langsung, Printing , Remote View, mengatur administrasi PC anda, yang kesemua itu dapat dilakukan dimanapun anda berada selama anda bisa terhubung ke internet
h) Dapat mengakses akses yang diblok.
i) Berselancar dengan aman ketika di akses internet publik / hotspot.
j) Jika perusahaan ingin mengoptimalkan biaya untuk membangun jaringan mereka yang luas. Oleh karena itu VPN dapat digunakan sebagai teknologi alternatif untuk menghubungkan jaringan lokal yang luas dengan biaya yang relatif kecil, karena transmisi data teknologi VPN menggunakan media jaringan public yang sudah ada.
k) Jangkauan jaringan lokal yang dimiliki suatu perusahaan akan menjadi luas, sehingga perusahaan dapat mengembangkan bisnisnya di daerah lain. Waktu yang dibutuhkan untuk menghubungkan jaringan lokal ke tempat lain juga semakin cepat, karena proses instalasi infrastruktur jaringan dilakukan dari perusahaan/kantor cabang yang baru dengan ISP terdekat di daerahnya. Penggunaan VPN secara tidak langsung akan meningkatkan efektivitas dan efisiensi kerja.
l) Penggunaaan VPN dapat mengurangi biaya operasional bila dibandingkan dengan penggunaan leased line sebagai cara tradisional untuk mengimplementasikan WAN.
m) VPN dapat mengurangi biaya pembuatan jaringan karena tidak membutuhkan kabel (leased line) yang panjang. Penggunaan kabel yang panjang akan membutuhkan biaya produksi yang sangat besar. Semakin jauh jarak yang diinginkan, semakin meningkat pula biaya produksinya.
n) VPN menggunakan internet sebagai media komunikasinya. Perusahaan hanya membutuhkan biaya dalam jumlah yang relatif kecil untuk menghubungkan perusahaan tersebut dengan pihak ISP (internet service provider) terdekat.
o) Penggunaan VPN akan meningkatkan skalabilitas.
p) VPN memberi kemudahan untuk diakses dari mana saja, karena VPN terhubung ke internet. Sehingga pegawai yang mobile dapat mengakses jaringan khusus perusahaan di manapun dia berada. Selama dia bias mendapatkan akses ke internet ke ISP terdekat, pegawai tersebut tetap dapat melakukan koneksi dengan jaringan khusus perusahaan.

F. Sistem Kontrol dan Monitoring

Monitoring Jaringan Komputer

Monitoring jaringan adalah proses pengumpulan dan melakukan analisis terhadap data-data pada lalu lintas jaringan dengan tujuan memaksimalkan seluruh sumber daya yang dimiliki Jaringan Komputer dimana salah satu fungsi dari management yang berguna untuk

menganalisa apakah jaringan masih cukup layak untuk digunakan atau perlu tambahan kapasitas. Hasil monitoring juga dapat membantu jika admin ingin mendesain ulang jaringan yang telah ada.

Banyak hal dalam jaringan yang bisa dimonitoring, salah satu diantaranya load traffic jaringan yang lewat pada sebuah router atau interface komputer. Monitoring dapat dilakukan dengan str SNMP, selain load traffic jaringan, kondisi jaringan pun harus dimonitoring, misalnya status up atau down dari sebuah peralatan jaringan. Monitoring Jaringan Komputer dapat dibagi menjadi 2 bagian yaitu:

a) Connection Monitoring, Connection monitoring adalah teknik monitoring jaringan yang dapat dilakukan dengan melakukan tes ping antara monitoring station dan device target, sehingga dapatdiketahui bila koneksi terputus.
b) Traffic Monitoring, Traffic monitoring adalah teknik monitoring jaringan dengan melihat paket aktual dari traffic pada jaringan dan menghasilkan laporan berdasarkan traffic jaringan.

Tujuan Monitoring Jaringan Komputer adalah untuk mengumpulkan informasi yang berguna dari berbagai bagian jaringan sehingga jaringan dapat diatur dan dikontrol dengan menggunakan informasi yang telah terkumpul. Dengan begitu diharapkan jika terjadi touble atau permasalahan dalam jaringan akan cepat diketahui dan diperbaiki sehingga stabilitas jaringan lebih terjamin.

Berikut ini beberapa alasan utama dilakukan monitoring jaringan:

a) Untuk menjaga stabilitas jaringan.
b) Sulit untuk mengawasi apa yang sedang terjadi di dalam jaringan yang memiliki sejumlah besar mesin (host) tanpa alat pengawas yang baik.
c) Untuk mendeteksi kesalahan pada jaringan, gateway, server, maupun user.
d) Untuk memberitahu trouble kepada administrator jaringan secepatnya.
e) Mempermudah analisis troubleshooting pada jaringan.
f) Mendokumentasikan jaringan.

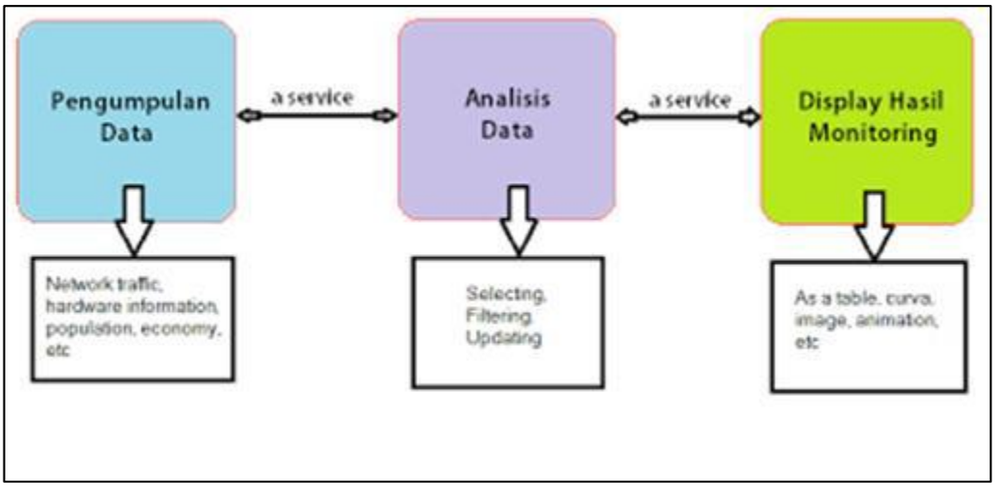
Sebuah sistem monitoring melakukan proses pengumpulan data mengenai dirinya sendiri dan melakukan analisis terhadap data-data tersebut dengan tujuan untuk memaksimalkan seluruh sumber daya yang dimiliki. Data yang dikumpulkan pada umumnya merupakan data yang real-time, baik data yang diperoleh dari sistem yang hard real-time maupun sistem yang soft real-time.

Sistem yang real-time merupakan sebuah sistem dimana waktu yang diperlukan oleh sebuah komputer didalam memberikan stimulus ke lingkungan eksternal adalah suatu hal yang vital. Waktu didalam pengertian tersebut berarti bahwa sistem yang real-time menjalankan suatu pekerjaan yang memiliki batas waktu (deadline). Di dalam batas waktu tersebut suatu pekerjaan mungkin dapat terselesaikan dengan benar atau dapat juga belum terselesaikan.

Sistem yang real-time mengharuskan bahwa suatu pekerjaan harus terselesaikan dengan benar. Sesuatu yang buruk akan terjadi apabila computer tidak mampu menghasilkan output tepat waktu. Hal ini seperti yang terjadi pada embedded system untuk kontrol suatu benda, seperti pesawat terbang, dan lain-lain. Sistem yang soft real-time tidak mengharuskan bahwa suatu pekerjaan harus terselesaikan dengan benar.

Secara garis besar tahapan dalam sebuah sistem monitoring terbagi ke dalam tiga proses besar, yaitu:

a) Proses di dalam pengumpulan data monitoring.
b) Proses di dalam analisis data monitoring.
c) Proses di dalam menampilkan data hasil monitoring.



Analogi proses dapat dilihat pada gambar diatas dimanasumber data dapat berupa network traffic, informasi mengenai hardware, atau sumber-sumber lain yang ingin diperoleh informasi mengenai dirinya. Proses dalam analisis data dapat berupa pemilihan data dari sejumlah data telah telah terkumpul atau bias juga berupa manipulasi data sehingga diperoleh informasi yang diharapkan. Sedangkan tahap menampilkan data hasil monitoring menjadi informasi yang berguna di dalam pengambilankeputusan atau kebijakan terhadap sistem yang sedang berjalan dapat berupa sebuah tabel, gambar, gambar kurva, atau dapat juga berupa gambar animasi.

Aplikasi Monitoring Server

a) IPTABLES
IPTABLES adalah suatu tools yang berfungsi sebagai alat untuk melakukan filter (penyaringan) terhadap (trafic) lalulintas data dan salah satu firewall popular dan powerfull dalam sistem operasi linux. Secara sederhana digambarkan sebagai pengatur lalulintas data.

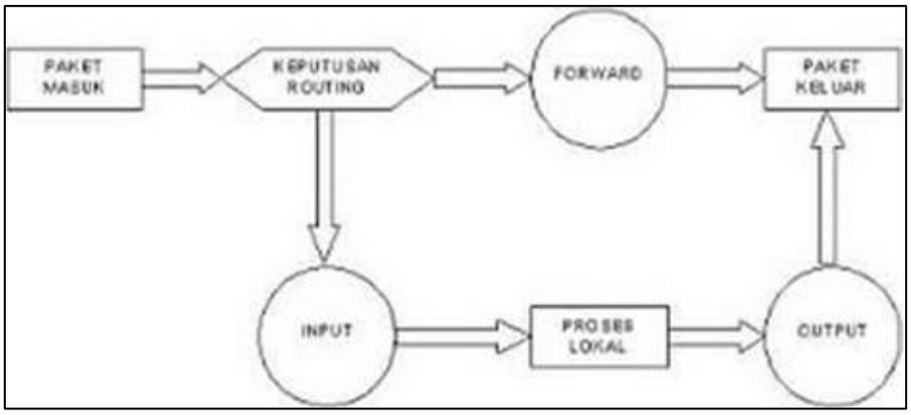
Fungsi IPTABLES adalah untuk konfigurasi, merawat dan memeriksa rules tables (tabel aturan) tentang filter paket IP yang terdapat di kernel linux dan kita dapat mengatur semua lalulintas dalam komputer kita, baik yang masuk ke komputer, keluar dari komputer, ataupun traffic yang sekedar melewati komputer kita.

IPTABLES memiliki 4 tabel aturan yaitu :

- Filter, untuk melakukan pemfiteran/penyaringan paket data apakah paket tersebut akan di DROP, LOG, ACCEPT atau REJECT.
- NAT, melakukan Network Address Translation yang merupakan pegganti alamat asal atau tujuan dari paket data.
- Mangle, untuk melakukan penghalusan (mangle) paket data seperti TTL, TOS dan MARK.
- Raw, untuk mengkonfigurasi pengecualian dari connection tracking bersama-sama NOTRACK.

Pada table terdapat chains (rantai) yang berisi rules/aturan yang berbeda-beda. Chains pada table filter yaitu:

- INPUT, Untuk paket yang disiapkan untuk soket lokal atau komputer kita sendiri atau untuk mengatasi paket data yang masuk.
- FORWARD, Untuk paket yang diarahkan/routing ke box atau untuk mengalihkan paket yang datang.
- OUTPUT, Untuk paket yang generate/dibuat sendiri atau untuk menghasilkan paket data yang akan diteruskan.



Istilah-istilah tersebut misalnya, memberitahu apa yang harus dilakukan terhadap lanjutan sintaks perintah, dan dilakukan untuk penambahan atau penghapusan sesuatu dari tabel atau yang lain, seperti dibawah ini :

sintaks IPTABLES

#IPTABLES [-t table] command [match] [target/jump]

Paket-paket yang masuk akan diperiksa, apakah rusak, salah infornasi atau tidak, kemudian diberikan ke chain INPUT, keputusan yang diambil untuk suatu paket dapat berupa:

- ACCEPT, Menerima paket dan diproses lebih lanjut oleh kernel.
- DROP, Menolak paket tanpa pemberitahuan terlebih dahulu.
- REJECT, Mengembalikan paket je asalnya dengan pesan kesalahan ICMP.
- LOG, Melakukan log (pencatatan) terhadap paket yang bersesuaian.
- RETURN, Untuk chain user-defined akan dikebalikan ke chain yang memanggil, sedangkan untuk chain INPUT, OUTPUT dan FORWARD akan dijalankan kebijakan default.
- Mengirim ke chain user-defined.

Sedangkan yang dimaksud dengan Chain/rantai digambarkan sebagai jalur aliran data. Chains yang diperlukan untuk IPTABLES ini antara lain:

- FORWARD Route packet akan di FORWARD tanpa di proses lanjut di local.
- INPUT Route packet masuk ke dalam proses lokal sistem.
- OUTPUT Route packet keluar dari local sistem.
- PREROUTING Chain yang digunakan untuk keperluan perlakuan sebelum packet masuk route. Biasanya dipakai untuk proses NAT.
- POSTROUTING Chain yang digunakan untuk keperluan perlakuan sesudah packet masuk route. Biasanya dipakai untuk proses NAT.

Chain PREROUTING dan POSTROUTING dimaksudkan sebagai jalur data sebelum dan sesudah data tersebut masuk ke dalam route. Beberapa target yang lain biasanya memerlukan parameter tambahan:

- LOG Target, tingkatan log yang bisa digunakan dalam option pertama adalah debug, info, notice, warning, err, crit, alert dan emerg. Option kedua adalah -j LOG –log-prefix untuk memberikan string yang tertulis pada awal log, sehingga memudahkan pembacaan log. Sintaksnya adalah:
  IPTABLES –A FORWARD –p tcp –j LOG –log-level debug
  IPTABLES –A INPUT –p tcp –j LOG –log-prefix “INPUT Packets”
- REJECT Target, memblok paket dan menolak untuk memproses lebih lanjut paket tersebut. REJECT akan mengirimkan pesan error ke pengirim paket, tidak seperti DROP. REJECT bekerja pada chain INPUT, OUTPUT dan FORWARD atau pada chain tambahan dari chain tersebut.
  IPTABLES –A FORWARD –p tcp –dport 80 –j REJECT –reject-with icmp-host-unreachable
  Tipe pesan yang bisa dikirimkan yaitu icmp-net-unreachable, icmp-host-unreachable, icmp-port-unreachable, icmp-proto-unrachable, icmp-netprohibited dan icmp-host-prohibited.

- SNAT Target, berguna untuk melakukan perubahan alamat asal paket (Source Network Address Translation). Target ini hanya berlaku untuk tabel nat pada chain POSTROUTING. Jika paket pertama dari satu koneksi mengalami SNAT, paket-paket berikutnya dalam koneksi juga akan mengalaminya. Sintaksnya adalah :
  IPTABLES –t nat –A POSTROUTING –o eth0 –j SNAT –to-source *192.168.0.1-192.168.0.254*:*1024-32000*
- DNAT Target, Digunakan untuk melakukan translasi alamat tujuan (Destination Network Address Translation) pada header dari paket yang memenuhi aturan match. DNAT hanya bekerja untuk tabel nat pada chain PREROUTING dan OUTPUT atau chain buatan yang dipanggil oleh chain tersebut. Sintaksnya adalah
  IPTABLES –t nat –A PREROUTING –p tcp –d *10.10.10.10* –dport 80 –j DNAT –to-destination *192.168.0.1*
- MASQUERADE Target, Hampir sama dengan SNAT, tetapi tidak perlu option –to-source. Target ini hanya bekerja untuk tabel nat pada chain POSTROUTING. Sintaksnya adalah :
  IPTABLES –t nat –A POSTROUTING –o ppp0 –j MASQUERADE
- REDIRECT Target, Mengalihkan paket ke komputer itu sendiri. Mengarahkan paket yang menuju suatu port tertentu untuk memasuki proxy, berguna untuk membangun transparent proxy. Misal untuk mengalihkan semua koneksi yang menuju port http untuk memasuki aplikasi http proxy seperti squid. Hanya bekerja untuk tabel nat pada chain PREROUTING dan OUTPUT atau pada chain buatan dari chain tersebut. Sintaksnya adalah :
  IPTABLES –t nat –A PREROUTING –i eth1 –p tcp –dport 80 –j REDIRECT –to-port 8080

b) Multi Router Traffic Grapher (MRTG)

Multi Router Traffic Grapher atau yang disingkat MRTG adalah free software yang digunakan untuk memonitoring traffik load pada link jaringan. Dimana pengguna dapat melihat laporan dalam bentuk grafik. MRTG ditulis dalam bentuk bahasa perl dan C dan berjalan di UNIX/Linux dan juga pada sistem operasi Windows dan juga pada Netware. MRTG menggunakan lisensi GNU GPL.

Cara Kerja MRTG

Data hasil logging olah MRTG disimpan dalam file ASCII, file ini akan ditulis ulang setiap lima menit sekali sesuai dengan update yang dilakukan oleh MRTG dan secara instant digabungkan dan dianalisis sehingga file logging tersebut membesarnya terkendali. File logging tersebut hanya digunakan untuk menyimpan data yang dibutuhkan untuk menggambar pada halaman web. Grafik ini dikonversi ke format GIF dari format PNM menggunakan tool pnmtogif.

Konfigurasi ini yang mengakibatkan MRTG terbatas untuk memonitor sekitar dua puluh router dari workstation.Kendala lain yang sangat potensial bagi user adalahtool smnpget dari package CMU SNMP yang diperlukan oleh MRTG untuk mengumpulkan data. Paket CMU SNMP ini sangat sulit untuk dikompilasi pada berbagai macam platform waktu itu.Karena keterbatasan-keterbatasan diatas maka penemu dan rekannya melakukan perombakan pada MRTG versi pertama, mereka membuat sebuah program rateup yang memecah MRTG dalam masalah kinerja dengan mengimplementasikan dua hal subprogram dalam MRTG yang menghabiskan CPU paling banyak dalam bahasa C dan menghilangkan subprogram tersebut ke dalam skrip perl MRTG.

Rateup ini melakukan penulisan ke file log dan menggambar grafik. Masalah portabilitas SNMP diselesaikan dengan mengganti snmpget dari CMU SNMO ke modul SNMP perl yang ditulis dalam bahasa perl secara murni, dengan begitu masalah platform dapat teratasi. Asumsi dasar untuk mendesain file log MRTG versi baru adalah ketertarikan pada informasi secara detail tentang load jaringan dikurangi secara proporsional dalam satuan waktu untuk memungkinkan antara koleksi data dan analisisnya, konfigurasi ini memungkinkan implementasi dari file log yang menyimpan data trafik dengan mengurangi resolusi ke dalam masa lalu.

Install MRTG

Untuk menginstall MRTG membutuhkan beberapa paket yaitu net-snmp, net-snmp-utils, dan mrtg.

- SNMP, *Simple Network Management Protocol* adalah suatu program untuk mempermudah dalam memonitor dan mengatur perangkat-perangkat jaringan, seperti router, switch, server, printer dan lain-lain. Informasi yang dapat di monitor pun bermacam-macam dari hal-hal biasa seperti memonitor traffic di suatu perangkat sampai yang tidak biasa seperti temperatur udara di dalam router.

  Konfigurasi SNPM:

  Install SNMP dan SNMPD dengan menjalankan perintah:

```
# apt-get install snmp snmpd
```

  Kemudian nyalakan service dari snmpd, caranya :

```
# /etc/init.d/snmpd restart
# chkconfig snmpd on
```

  Kemudian test menggunakan program snmpwalk, caranya:

```
# snmpwalk -v 2c -c public localhost system
```

  Kemudian untuk mempermudah ganti saja file konfigurasi-nya dengan yang baru.

```
# cd /etc/snmp
# mv snmpd.conf snmpd.conf-old
# chmod 0600 snmpd.conf
# nano /etc/snmp/snmpd.conf
```

  Tambahkan sintaks berikut ini

```
##/etc/snmp/snmpd.conf
##      sec.name        source                  community
##      =======         ======                  =========
com2sec local           localhost               123456
com2sec lan             192.168.1.0/24          123456
#
##      group.name              sec.model               sec.name
##      =========               =========               ========
group           ROGroup_1       v1                      local
group           ROGroup_1       v1                      lan
group           ROGroup_1       v2c                     local
group           ROGroup_1       v2c                     lan
#
##MIB.view.name      incl/excl       MIB.subtree     mask
##============      =========       =========       ====
view all-mibs           included        1               80
#
## MIB
## group.name context sec.model sec.level prefix read write notif
## ========== ====== ======== ======= ===== === ==== =====
access ROGroup_1""v1noauth exact all-mibs none none
access ROGroup_1""v2c noauth exact all-mibs none none
```

  Kemudian cek kembali apakah sudah berubah konfigurasi snmp-nya dengan merestart service snmp dan lakukan percobaan akses snmp.

```
# /etc/init.d/snmpd restart
# snmpwalk -v 2c -c 123456 localhost system
```

- Konfigurasi Strd MRTG
  Install MRTG dengan melakukan perintah dibawah ini:
  #apt-get install mrtg

Secara default file mrtg akan diletakkan pada posisi /var/www/mrtg Pertama kali harus membuat file kofigurasi dari MRTG, dimana akan dibuat supaya MRTG memonitor semua perangkat jaringan di komputer. Caranya adalah :

```
# cfgmaker --output=/etc/mrtg/mrtg.cfg --global "workdir:
/var/www/html/bandwidth" \ -ifref=ip --global 'options[_]:
growright,bits' 123456@localhost
```

Keterangan:

- --output=/etc/mrtg/mrtg.cfg ==> adalah file konfigurasi yang akan dibuat.
- --global: /var/www/html/bandwidth ==> adalah lokasi direktori tempat grafik dari mrtg akan disajikan.
- -ifref=ip ==> MRTG akan mengecek traffic berdasarkan IP address dari setiap device.
- --global 'options[_]: growright,bits' ==> berarti grafik ditampilkan dari sebelah kanan dan traffic akan diukur berdasarkan bit.
- 123456@localhost ==> adalah community string atau "password" dari snmp server dan lokasi snmp server.

Kemudian jalankan mrtg secara manual, untuk memulai membentuk grafiknya.

```
# mrtg /etc/mrtg/mrtg.cfg
```

Tetapi apabila cara tersebut gagal yang disebabkan variabel LANG dalam format UTF-8 tidak disupport MRTG, maka untuk merubahnya gunakan :

```
# env LANG=C /usr/bin/mrtg /etc/mrtg.cfg
```

Setelah itu bentuk file index supaya halaman web dapat diakses.

```
# mkdir /var/www/html/bandwidth

# chmod 755 /var/www/html/bandwidth

# indexmaker –

output=/var/www/html/bandwidth/index.html/etc/mrtg/mrtg.cfg
```

Pembuatan grafik traffic jaringan dilakukan secara periodik, untuk itu diperlukan penjadwalan agar grafik akan selalu terbentuk dalam jangka waktu tertentu. unutk mengcek penjadwalan yang telah ada dengan cara:

```
# cat /etc/cron.d/mrtg
```

Apabila file konfigurasi tidak ada bisa buat penjadwalan sendiri

```
# crontab –e
```

Diisi dengan :

```
*/5 * * * * env LANG=C /usr/bin/mrtg /etc/mrtg/mrtg.cfg
```

Sekarang MRTG sudah berjalan bisa dilihat pada browser pada alamat : *"http:///(ip address)/bandiwidth"...*

- NagiOS
  Nagios merupakan aplikasi monitoring yang dapat memonitor system komputer, monitoring jaringan dan monitoring infrastruktur suatu aplikasi berbasis open source. Nagios menawarkan layanan monitoring dan peringatan untuk server, switch, aplikasi dan layanan yang lainnya. User akan diberi pesan peringatan ketika suatu masalah terjadi pada server, switch aplikasi dan layanan yang di monitoring lainnya.

  Mengingat kayanya fitur yang ditawarkan oleh Nagios maka kita akan mencoba untuk menginstall dan mengkonfigurasi aplikasi monitoring tersebut pada suatu sistem yang dikelola.

- Cacti

Cacti adalah salah satu aplikasi open source yang merupakan solusi pembuatan grafik network yang lengkap yang di design untuk memanfaatkan kemampuan fungsi RRDTool sebagai penyimpanan data dan pembuatan grafik. Cacti menyediakan pengumpulan data yang cepat, pola grafik advanced, metoda yang mudah digunakan mudah dipahami untuk local area network sehingga network yang kompleks dengan ratusan device. Dengan menggunakan cacti kita dapat memonitor trafik yang mengalir pada sebuah server dan cacti juga merupakan fronted dari RDDTool yang menyimpan informasi ke dalam database MySQL dan membuat graph dari informasi tersebut.

Konfigurasi Cacti :

Instalasi paket-paket software yang di butuhkan cacti

```
# apt-get install apache2 apache2-common apache2-mpm-prefork apache2-utils libapache2-mod-php5 php5-cli php5-common php5-cgi
```

```
# apt-get install mysql-server mysql-client libmysqlclient16-dev php5-mysql make gcc g++ cgilib libfreetype6 libttf-dev libttf2 libpngwriter0-dev libpng3-dev libfreetype6-dev libart-2.0-dev snmp
```

Install RRDTool

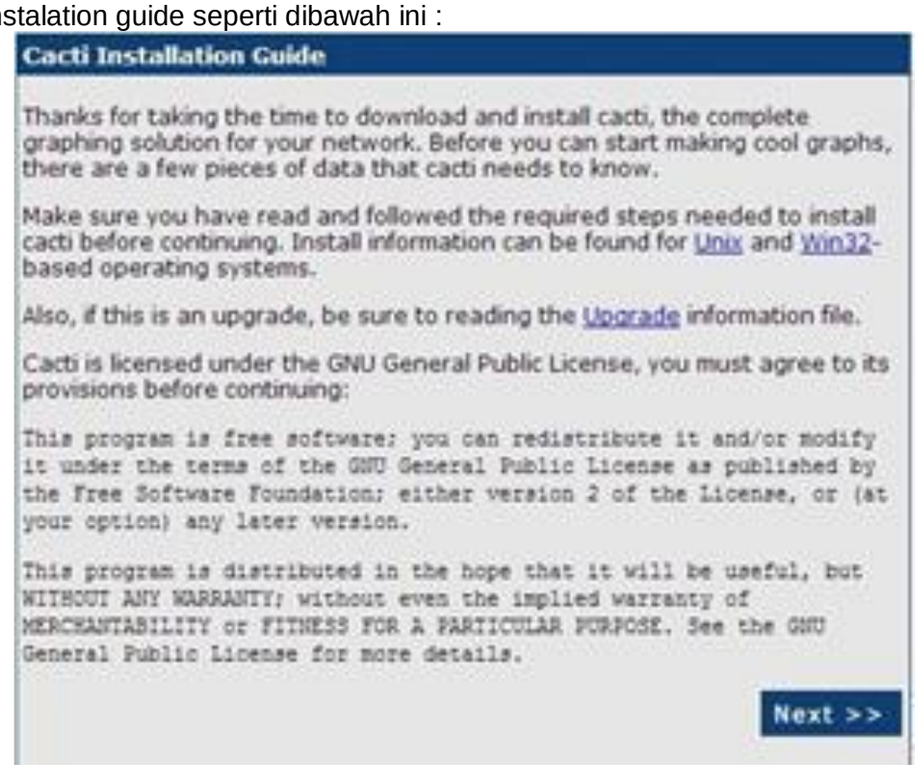
```
# apt-get install rrdtool
```

Install Cacti dengan

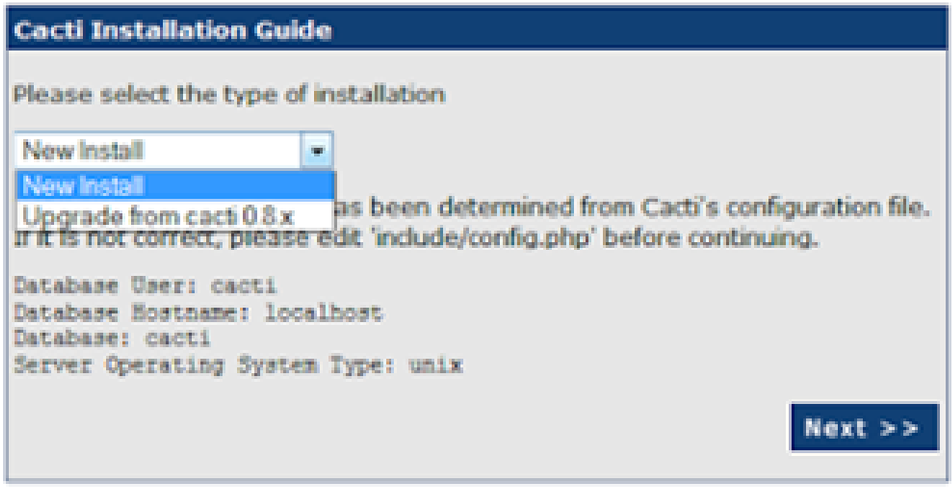
```
apt-get install cacti
```

Pada saat proses instalasi mysql akan ada form untuk pengisian password “root” mysql nya, isi saja sesuai dengan keinginan dan databasenya akan otomatis ter-*create* ketika proses instalasi Cactinya. Pastikan semua paket yang diinstall itu tidak mengalami error dan failed.

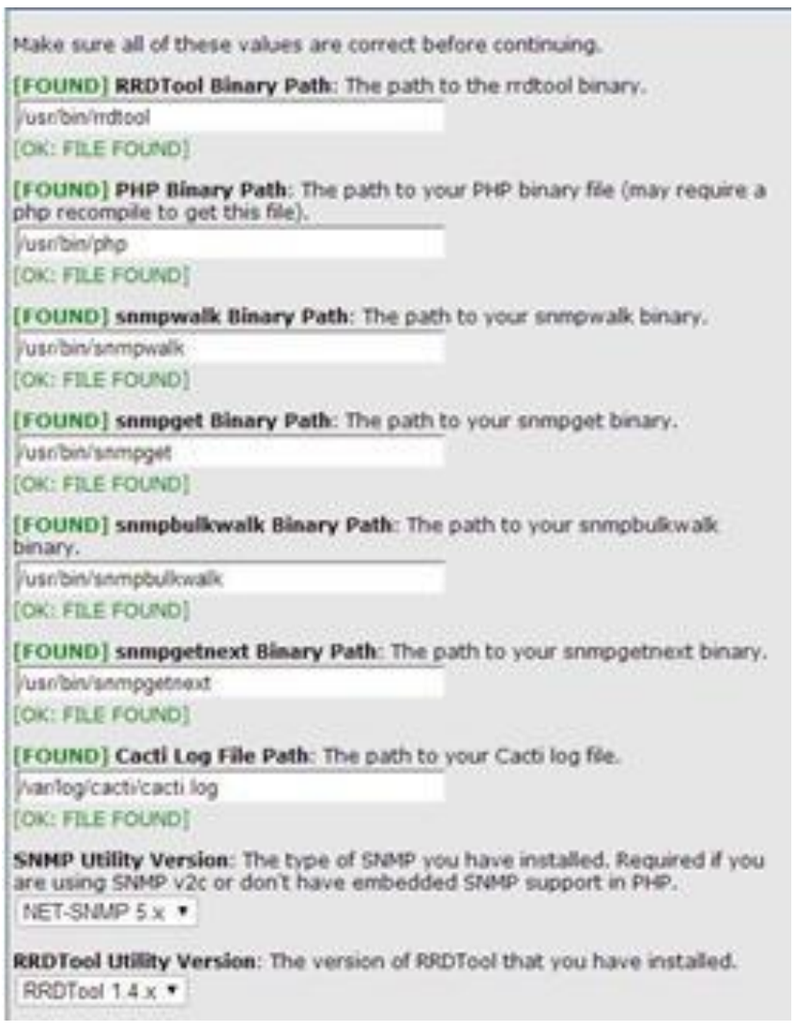
Setelah itu maka langkah berikutnya adalah mengkonfigurasi cactinya, dengan cara diakses via browser dengan alamat http://*ip-server*/cacti/ atau kalau dari localhost gunakan url : http://*localhost*/cacti/ maka akan keluar tampilan instalation guide seperti dibawah ini :



Pilih type Installasi, Pilih new install – Next



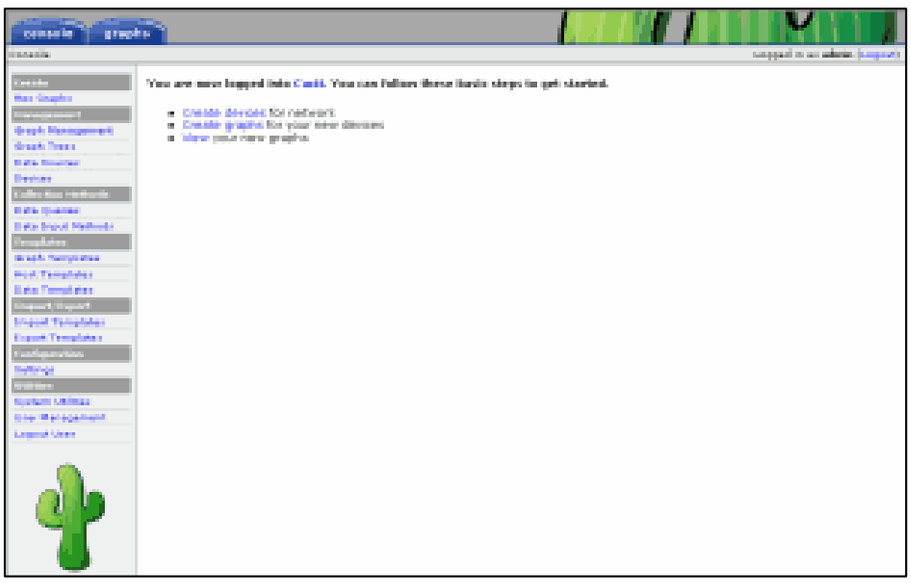
Pada tahap selanjutnya seperti gambar dibawah ini, langsung klik Finish kita tidak perlu mengubah-ubahnya.



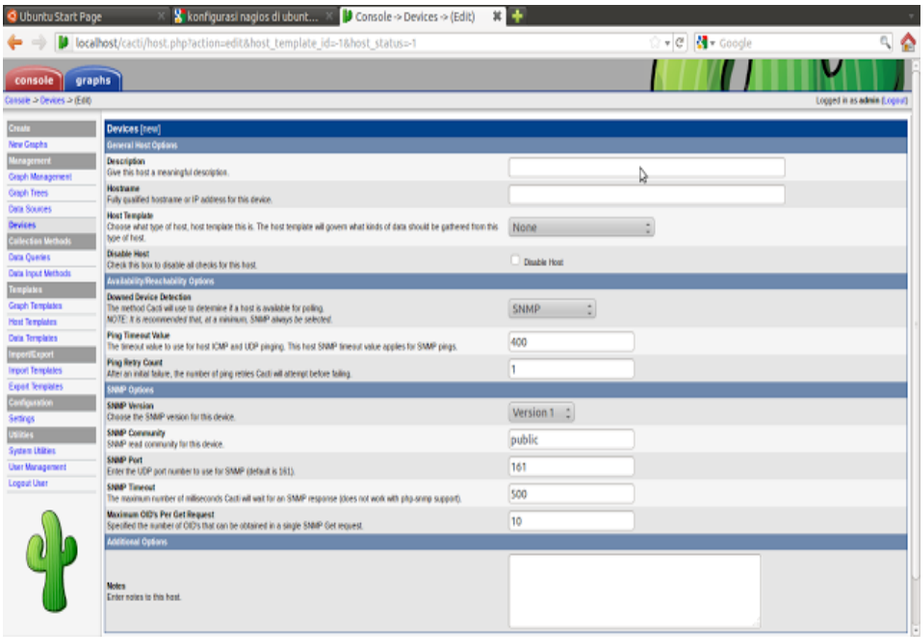
Jika instalasi berjalan lancar tanpa adanya erorr maka langkah selanjutnya klik finish. Kemudian akan muncul user login seperti dibawah ini :

Untuk login defaultnya adalah username: admin, passwordnya: admin

Kemudian setelah login akan muncul tampilan seperti berikut ini yang merupakan halaman depan dari cacti.



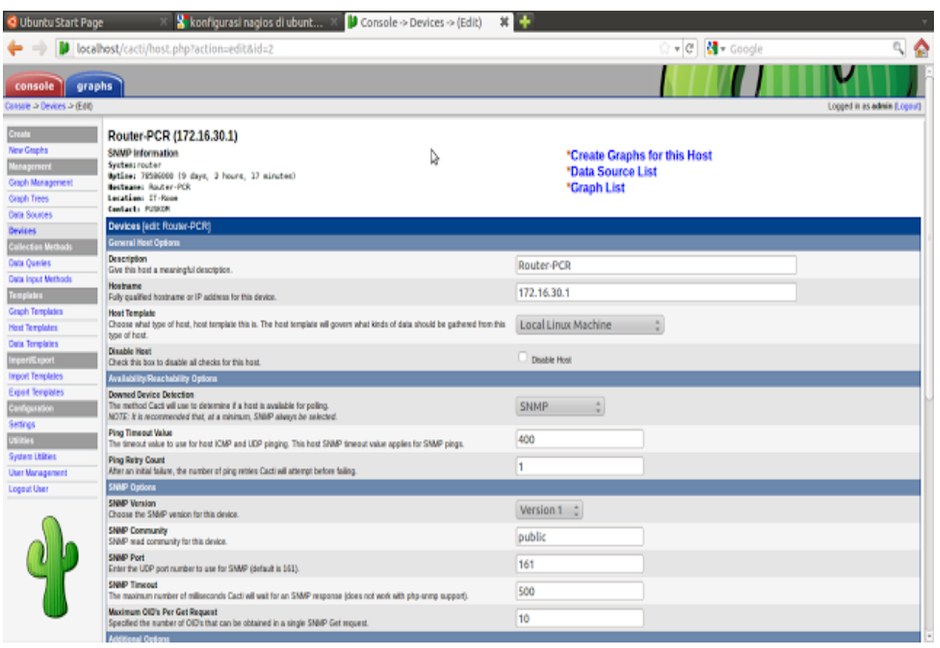
Setelah muncul gambar diatas, Klik menu device dan kemudian klik add (sebelah kiri atas), Kemudian akan muncul gambar seperti dibawah ini setelah itu silakan isi :



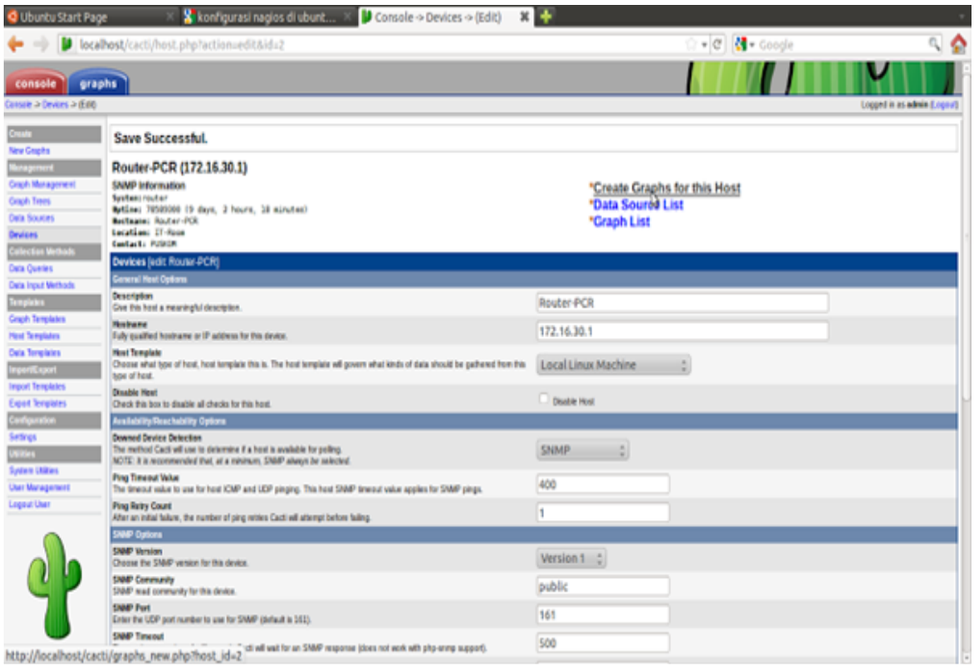
- Description : Isikan nama device yang akan dimonitoring (Gateway).
- Hostname : Isikan IP Address dari device yang akan dimonitoring (Gateway)
- Host Template : Pilih “Local Linux Machine” atau ucd/net SNMP Host jika device yang akan dimonitoring PC biasa seperti windows client
- SNMP Version : Pilih sesuai versi SNMP yang di setup di device Gateway, dalam hal ini version
- SNMP Communitiy : umumnya pakai “public” tapi jika memang di set lain, tinggal menyesuaikan.

Pada bagian “associated data query” pilih “**add data query=SNMPInterface Statistic**” dengan “**index method=Uptime Goes Backward**” lalu klik add.

Kemudian untuk memastikan SNMP nya jalan di device tersebut, klik “**verbose query**” pada bagian “**associated data query**” di SNMPInterface Statistic. Jika tidak ada *error* di SNMP (lihat bagian paling bawah kanan) klik save.



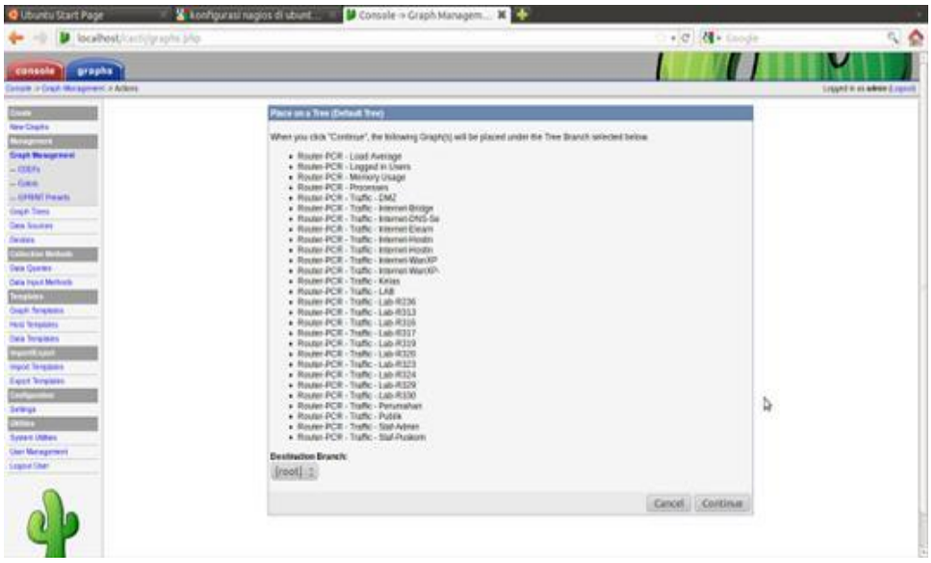
Kemudian pada menu device klik device yang sudah kita buat yaitu gateway, selanjutnya klik “**create graphs for this host**”. Seperti tampilan dibawah ini :



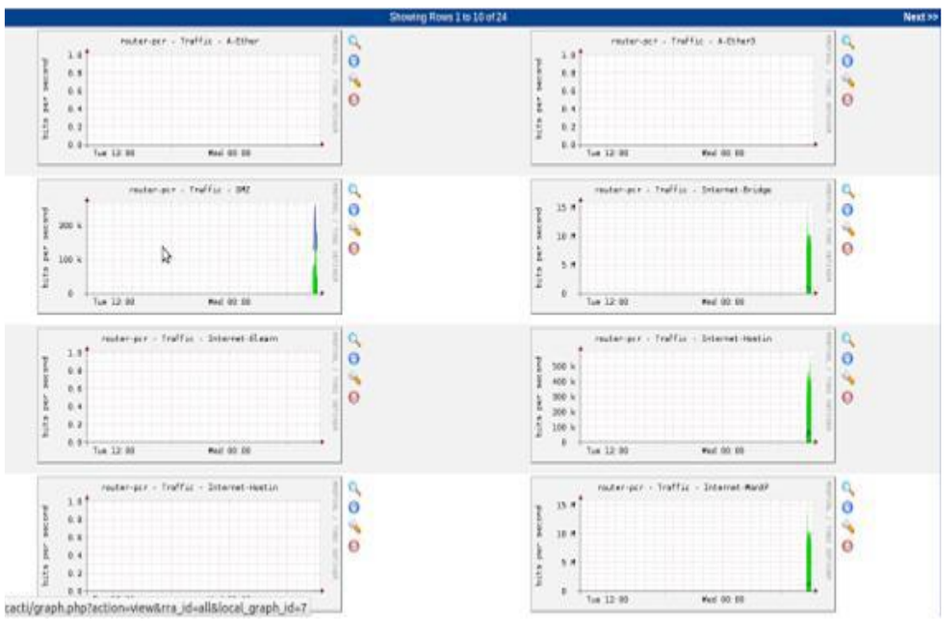
Pada bagian data query [SNMP-Interface statistic] centang bagian interface dari device gateway yang akan ditampilkan grafik trafiknya. Pada bagian select graph type, pilih "**In/Out Bits with total bandwidth**" atau pilih sesuai selera. Dan klik create.

Kemudian untuk menampilkan di graph tree, pada bagian graph management pilih host:gateway yaitu device yang sudah dibuat sebelumnya. Centang semua graph yang muncul dan di bagian action pilih "**Place on a Tree**" klik go. Seperti gambar dibawah ini :

Selanjutnya akan timbul tampilan Place on a Tree (Default Tree).

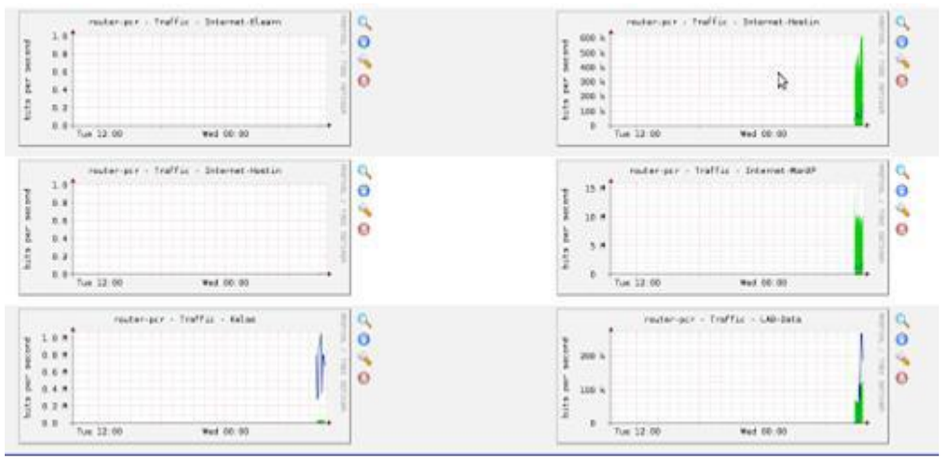


Kemudian tampilan di graph akan muncul device gateway, pada waktu awalnya memang grafiknya tidak muncul langsung karena perlu waktu untuk query data ke device gateway. Setelah beberapa menit akan muncul trafik data untuk tiap interface yang sudah kita centang sebelumya.

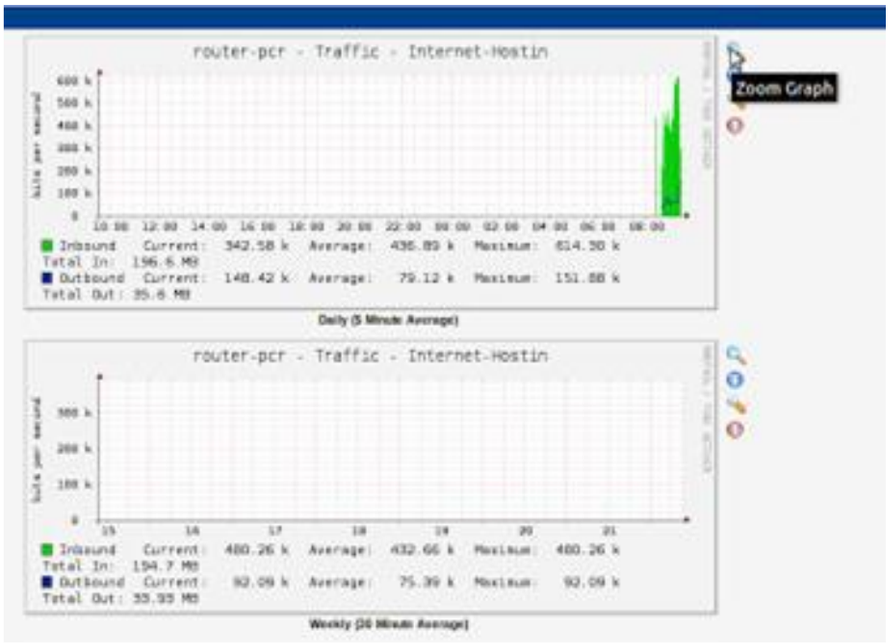


Jika ingin memperkecil skala waktunya bisa dengan cara berikut ini :

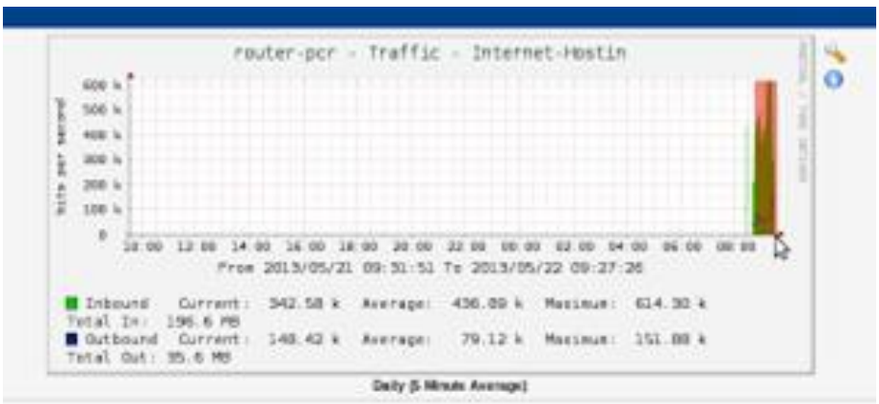
a) Klik salah satu yang ingin diperbesar, misalnya seperti yang ditunjuk kursor berikut :



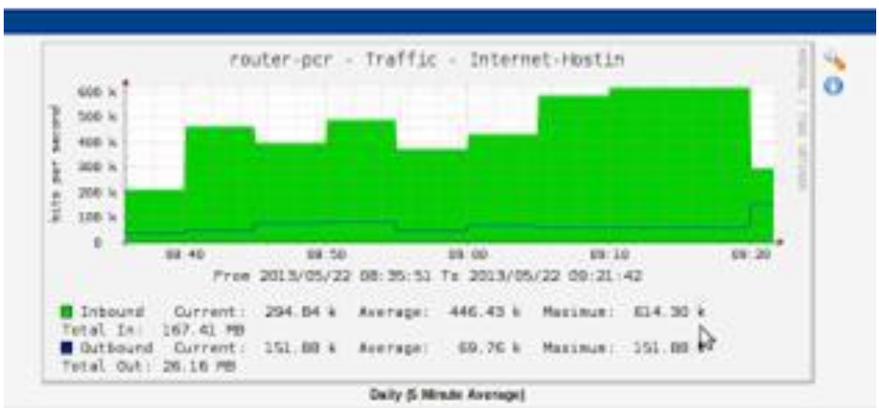
b) Kemudian akan ditampilkan seperti gambar berikut, pilih zoom graph :



c) Setelah di zoom, blok grafik yang ingin di zoom :



d) Kemudian akan muncul grafik yang telah di zoom sebagai berikut :



Monitoring dan Sistem Kontrol Jarak Jauh

Telemetri atau komunikasi data tanpa kabel (*wireless*) merupakan cara yang efektif untuk komunikasi jarak jauh tanpa harus terganggu dengan jalur kabel yang panjang. Modul telemetri pun beragam, ada yang menggunakan komunikasi serial, ethernet atau firewall (jaringan internet). Sebagai contoh data yang dikirimkan oleh sensor temperatur dari jarak ratusan kilometer dapat dikirimkan ke lokasi lain (unit pengolah data central) dengan menggunakan media komunikasi tadi. Aktifitas dan kendali pompa air ataupun disel ataupun genset seringkali menggunakan sistem telemetry. Terbukti beberapa produk menambahkan sistem software dan hardware guna aktifitas kendali dan monitoring jarak jauh.

Untuk membuat sistem wireless tersebut tentu memerlukan beberapa unit bagian yang masing2 bisa dibahas berikut :

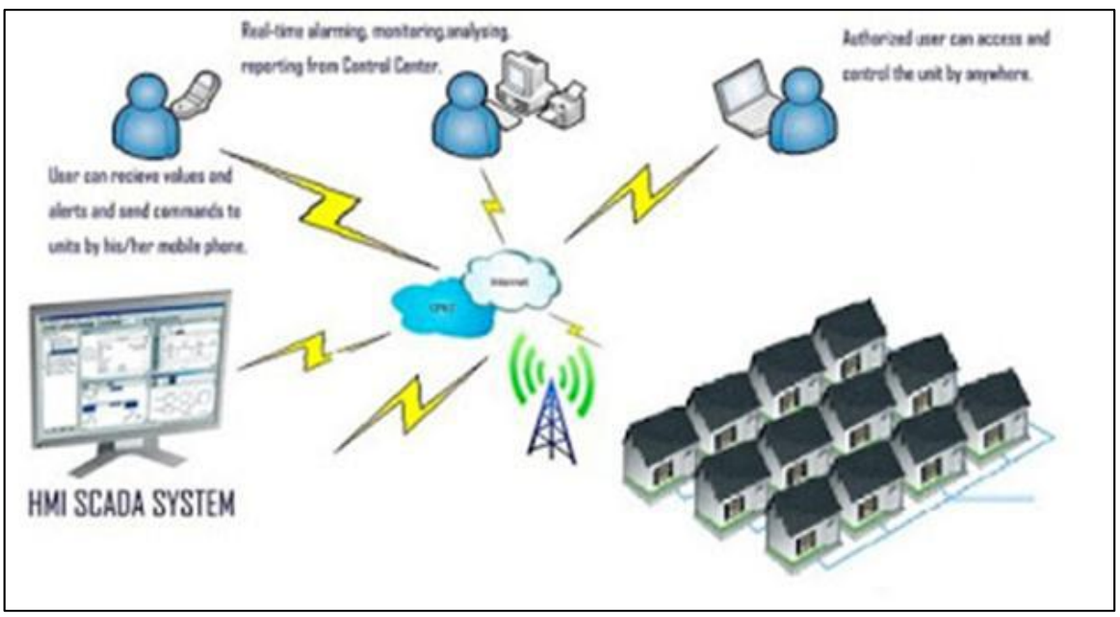
- Sumber dan Pengiriman data (*Transmitter*)
- Saluran Transmisi
- Penerima Data (*Receiver*)

Transmitter merupakan salah satu komponen utama yang menjadi pesawat yang digunakan untuk menyiarkan atau memancarkan data informasi untuk keperluan tertentu. Saluran transmisi merupakan saluran yang dipergunakan untuk menyalurkan informasi yang telah dipancarkan oleh transmitter. Pada sistem telemetri biasanya menggunakan sistem wireless atau wireline, namun pada akhirnya sekarang banyak menggunakan wireless sebagai media komunikasi. Receiver adalah pesawat penerima yang dipergunakan untuk menerima data informasi yang telah dipancarkan oleh transmitter yang kemudian diolah sehingga didapatkan data hasil yang diperlukan. Ketiga komponen ini dan bagaimana teknik pengiriman sampai penerimaan data akan menentukan kualitas sistem yang akan dibangun.

Metoda sistem tramsimi data dari *tranceiver* ke *receiver* bisa melalui 3 metoda berikut yaitu :

- Transfer data dengan satelit
- Transfer data dengan GSM / GPRS
- Transfer data dengan Radio Frekuensi (RF)

Beberapa aplikasi sistem telemetri banyak diterapkan dalam beberapa bidang seperti property emergency warning, building automation, energy, otomatisasi pompa PDAM jarak jauh, ruang kendali pasien rumah sakit, flow switch hydrant system, kontrol monitoring batery jarak jauh , dan masih banyak lagi.



Sistem transmisi data dengan GSM/GPRS mempunyai beberapa keunggulan dalam hal :

- Infrastrukturnya murah karena tidak memerlukan pembangunan infrastruktur yang baru, hanya memanfaatkan infrastruktur yang sudah ada. Namun bukan berarti tidak ada masalah, karena sistem ini tergantung juga keandalan provider / penyedia jasa telekomunikasi yang kita sewa / bayar.
- Cakupannya lebih luas dibandingkan dengan sisten RF (Radio Frequensi)
- Format data digital yang ditransmisikan lebih akurat
- Frekwensi yang digunakan sangat tinggi, hampir sama dengan frekwensi satelit yaitu sebesar 850 MHz sampai dengan 2100 Mhz.

Namun beberapa kelemahan pada sistem transmisi GSM/GPRS adalah :

- Cakupan areanya terbatas pada sistem yang memiliki BTS (*Base Tranceiver Station*).
- Kekuatan sinyal terbatas dan sangat dipengaruhi oleh kondisi geografis.
- Kapasitas transfer data terbatas, karena karakter yang ditransmisikan juga terbatas.

Beberapa produk dengan sistem transmisi data GSM/GPRS:

- Sistem Kontrol AMF Generator
  Spesifikasi :
  a) Automatic SMS saat kejadian alarm pada saat overload genset, dan kejadian overtemperatur bisa dikirimkan lewat SMS.
  b) Sistem monitoring dan kontrol online melalui halaman website (*embedded we server*).
  c) Pemilihan penggunaan modem/wireless GSM/GPRS internet menggunakan teknologi GPRS.

- Sistem Data Logger
  GSM GPRS Data Logger , RTU telemetry Data Logger dengan harga yang sangat murah. Dapat dipergunakan untuk mengetahui data kejadian motor pompa trip, **genset temperatur over limit**, storage tank overflow, dan dapat juga melakukan operasi Start dan Stop mesin secara jarak jauh. Dengan beberapa modul lain seperti PLC, peralatan ukur teganhan, temperatur, flowmeter dapat dikomunikasikan dengan media telephone atau website secara serempak dalam ruang kontrol atau ruang monitoring.

Aplikasi sistem komunikasi data dengan GPRS memungkinkan pengiriman dan penerimaan data lebih cepat jika dibandingkan dengan penggunaan teknologi circuit switch data / CSD. Sistem GPRS mampu menjangkau kecepatan 56 Kbps sampai 115 Kbps sehingga memungkinkan akses internet. Sistem GPRS bekerja dengan prinsip tunelling, yaitu membungkus paket data agar bisa dilewatkan lewat gelombang radio.

Beberapa aplikasi dengan penggunaan sistem GPRS ini telah diterapkan di beberapa instansi pemerintah atau swasta yaitu PT. Telkom Ventus dan PT Indosat. Sistem GPRS ini memperbaharui sistem layanan lama soal surat meyurat elektronis dari semula hanya ke PC ke media handphone.

G. Sistem Keamanan Jaringan

Keamanan jaringan adalah suatu cara atau suatu system yang digunakan untuk memberikan proteksi atau perlindungan pada suatu jaringan agar terhindar dari berbagai ancaman luar yang mampu merusak jaringan.

1. Elemen pembentukan keamanan jaringan
Ada dua elemen utama pembentuk keamanan jaringan :
a) Tembok pengamanan (baik secara fisik maupun maya), yaitu suatu cara untuk memberikan proteksi atau perlindugan pada jarigan, baik secara fisik (kenyataan) maupun maya (menggunakan software).
b) Rencana pengamanan, yaitu suatu rancangan yang nantinya akan diimplementasikan uantuk melindungi jaringan agar terhindar dari berbagai ancaman dalam jaringan.

2. Alasan keamanan jaringan sangat penting
Alasan keaman jaringan sangat penting karena :
a) Privacy/Confidentiality
Defenisi : menjaga informasi dari orang yang tidak berhak mengakses.
Privacy : lebih kearah data-data yang sifatnya privat , Contoh : e-mail seorang pemakai (*user*) tidak boleh dibaca oleh administrator.
Confidentiality : berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu tersebut. Contoh: data-data yang sifatnya pribadi (seperti nama, tempat tanggal lahir, social security number, agama, status perkawinan, penyakit yang pernah diderita, nomor kartu kredit, dan sebagainya) harus dapat diproteksi dalam penggunaan dan penyebarannya. Bentuk Serangan : usaha penyadapan (dengan program sniffer). Usaha-usaha yang dapat dilakukan untuk meningkatkan privacy dan confidentiality adalah dengan menggunakan teknologi kriptografi.

b) Integrity

Defenisi : informasi tidak boleh diubah tanpa seijin pemilik informasi. Contoh : e-mail di intercept di tengah jalan, diubah isinya, kemudian diteruskan ke alamat yang dituju.
Bentuk serangan : Adanya virus, trojan horse, atau pemakai lain yang mengubah informasi tanpa ijin, “man in the middle attack” dimana seseorang menempatkan diri di tengah pembicaraan dan menyamar sebagai orang lain.

c) Authentication
Defenisi : metoda untuk menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud.
Dukungan :
- Adanya Tools membuktikan keaslian dokumen, dapat dilakukan dengan teknologi watermarking (untuk menjaga “intellectual property”, yaitu dengan menandai dokumen atau hasil karya dengan “tanda tangan” pembuat) dan digital signature.
- Access control, yaitu berkaitan dengan pembatasan orang yang dapat mengakses informasi. User harus menggunakan password, biometric (ciri-ciri khas orang), dan sejenisnya.

d) Availability
Defenisi : berhubungan dengan ketersediaan informasi ketika dibutuhkan. Contoh hambatan :
- “Denial of Service Attack” (DoS Attack), dimana server dikirimi permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai down, hang, crash.
- Mailbomb, dimana seorang pemakai dikirimi e-mail bertubi-tubi (katakanlah ribuan e-mail) dengan ukuran yang besar sehingga sang pemakai tidak dapat membuka e-mailnya atau kesulitan mengakses e-mailnya.

e) Access Control
Defenisi : cara pengaturan akses kepada informasi. berhubungan dengan masalah authentication dan juga privacy Metode: menggunakan kombinasi *user id/password* atau dengan menggunakan mekanisme lain.

f) Non-repudiation
Defenisi : Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Dukungan bagi electronic commerce.

3. Dasar-dasar keamanan jaringan

a) *Availability*/ketersedian, hanya user tertentu saja yang mempunyai hak akses atau authorized diberi akses tepat waktu dan tidak terkendala apapun.
b) *Reliability*/Kehandalan, object tetap orisinil atau tidak diragukan keasliannya dan tidak dimodifikasi dalam perjalanannya dari sumber menuju penerimanya.
c) *Confidentiality*/Kerahasiaan, object tidak diumbar/dibocorkan kepada subject yang tidak seharusnya berhak terhadap object tersebut, lazim disebut tidak *authorize*.

4. Syarat keamanan jaringan

a) Prevention (pencegahan)
Kebanyakan dari ancaman akan dapat ditepis dengan mudah, walaupun keadaan yang benarbenar 100% aman belum tentu dapat dicapai. Akses yang tidak diinginkan kedalam jaringan komputer dapat dicegah dengan memilih dan melakukan konfigurasi layanan (services) yang berjalan dengan hati-hati.

b) Observation (observasi)

Ketika sebuah jaringan komputer sedang berjalan, dan sebuah akses yang tidak diinginkandicegah, maka proses perawatan dilakukan. Perawatan jaringan komputer harus termasuk melihat isi log yang tidak normal yang dapat merujuk ke masalah keamanan yang tidak terpantau. System IDS dapat digunakan sebagai bagian dari proses observasi tetapi menggunakan IDS seharusnya tidak merujuk kepada ketidak-pedulian pada informasi log yang disediakan.

c) Response (respon).
Bila sesuatu yang tidak diinginkan terjadi dan keamanan suatu system telah berhasil disusupi,maka personil perawatan harus segera mengambil tindakan. Tergantung pada proses produktifitas dan masalah yang menyangkut dengan keamanan maka tindakan yang tepat harus segera dilaksanakan. Bila sebuah proses sangat vital pengaruhnya kepada fungsi system dan apabila di-shutdown akan menyebabkan lebih banyak kerugian daripada membiarkan system yang telah berhasil disusupi tetap dibiarkan berjalan, maka harus dipertimbangkan untuk direncakan perawatan pada saat yang tepat. Ini merupakan masalah yang sulit dikarenakan tidak seorangpun akan segera tahu apa yang menjadi celah begitu system telah berhasil disusupi dari luar.

5. Katagori keamanan jaringan

- *Interruption*
  Suatu aset dari suatu sistem diserang sehingga menjadi tidak tersedia atau tidak dapat dipakai oleh yang berwenang. Contohnya adalah perusakan/modifikasi terhadap piranti keras atau saluran jaringan.

- *Interception*
  Suatu pihak yang tidak berwenang mendapatkan akses pada suatu aset. Pihak yang dimaksud bisa berupa orang, program, atau sistem yang lain. Contohnya adalah penyadapan terhadap data dalam suatu jaringan.

- *Modification*
  Suatu pihak yang tidak berwenang dapat melakukan perubahan terhadap suatu aset. Contohnya adalah perubahan nilai pada file data, modifikasi program sehingga berjalan dengan tidak semestinya, dan modifikasi pesan yang sedang ditransmisikan dalam jaringan.

- *Fabrication*
  Suatu pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contohnya adalah pengiriman pesan palsu kepada orang lain.

6. Jenis-jenis serangan atau gangguan dalam jaringan

- **DOS / DDOS,** Denial of Services dan Distributed Denial of Services adalah sebuah metode serangan yangbertujuan untuk menghabiskan sumber daya sebuah peralatan jaringan komputer sehingga layanan jaringan computer menjadi terganggu.
- **Paket Sniffing,** sebuah metode serangan dengan cara mendengarkan seluruh paket yang lewat pada sebuah media komunikasi, baik itu media kabel maupun radio. Setelah paket-paket yang lewat itu didapatkan, paket-paket tersebut kemudian disusun ulang sehingga data yang dikirimkan oleh sebuah pihak dapat dicuri oleh pihak yang tidak berwenang.
- **IP Spoofing,** sebuah model serangan yang bertujuan untuk menipu seseorang. Serangan ini dilakukan dengan cara mengubah alamat asal sebuah paket, sehingga dapat melewati perlindungan firewall dan menipu host penerima data.
- **DNS Forgery,** Salah satu cara yang dapat dilakukan oleh seseorang untuk mencuri data-data penting orang lain adalah dengan cara melakukan penipuan. Salah satu bentuk penipuan yang bisa dilakukan adalah penipuan data-data DNS.
- **Trojan Horse,** program yang disisipkn tanpa pengetahuan si pemilik komputer, dapat dikendalikan dari jarak jauh & memakai timer.
- **Probe :** Usaha yang tak lazim untuk memperoleh akses ke dalam suatu sistem/ untuk menemukan informasi tentang sistem tersebut. Dapat dianalogikan sebagai usaha

untuk memasuki sebuah ruangan dengan mencoba-coba apakah pintunya terkunci atau tidak.

- **Scan :** kegiatan probe dalam jumlah besar dengan menggunakan tool secara otomatis. Tool tersebut secara otomatis dapat mengetahui port-port yang terbuka pada host lokal/host remote, IP address yang aktif bahkan bisa untuk mengetahui sistem operasi yang digunakan pada host yang dituju.
- **Account Compromise :** penggunaan account sebuah komputer secara illegal oleh seseorang yang bukan pemilik account tersebut. Account Compromise dapat mengakibatkan korban mengalami kehilangan atau kerusakan data.
- **Root Compromise :** mirip dengan account compromise, dengan perbedaan account yang digunakan secara ilegal adalah account yang mempunyai priviliege sebagai administrator sistem. Akibat yang ditimbulkan bias mengubah kinerja sistem, menjalankan program yang tidak sah.

Tugas

Buatlah ringkasan dan laporan praktikum mengenai:

a) DHCP Server
b) FTP Server
c) Remove Server
d) File Server
e) Web Server
f) DNS Server
g) Database Server
h) Mail Server
i) Control Panel Hosting
j) Share Hosting Server
k) Vitual Private Server
l) Dedicated Hosting Server
m) VPN Server