

## KEAMANAN JARINGAN KOMPUTER

Dalam bab ini Anda akan belajar :

1. Klasifikasi Keamanan Jaringan Komputer
2. Macam-Macam Serangan Jaringan Komputer
3. Membangun Sistem Keamanan Jaringan Komputer Yang Kuat

Dengan selesainya kita membangun jaringan komputer, suatu komputer akan lebih mudah dan lebih sering diakses oleh orang lain. Dengan makin banyaknya akses, otomatis keamanan komputer tersebut makin rentan, apalagi jika ada yang pemakai yang mempunyai niat buruk. Ini bukan pekerjaan mudah sebab jika tidak dijaga komputer kita dalam jaringan bisa diakses tanpa isi bahkan pengambilan data dan informasi secara ilegal.

### 1. Klasifikasi Keamanan Jaringan Komputer

Jika diamati mengenai keamanan maka keamanan jaringan komputer dapat ditinjau dari segi bentuknya yaitu seperti berikut:

#### 1) Keamanan hardware

Keamanan hardware berkaitan dengan perangkat keras yang digunakan dalam jaringan komputer. Keamanan hardware sering dilupakan padahal merupakan hal utama untuk menjaga jaringan dari agar tetap stabil. Dalam keamanan hardware, server dan tempat penyimpanan data harus menjadi perhatian utama. Akses secara fisik terhadap server dan data-data penting harus dibatasi semaksimal mungkin.

Akan lebih mudah bagi pencuri data untuk mengambil harddisk atau tape backup dari server dan tempat penyimpanannya daripada harus menyadap data secara software dari jaringan. Sampah juga harus diperhatikan karena banyak sekali hacker yang mendatangi tempat sampah perusahaan untuk mencari informasi mengenai jaringan komputernya. Salah satu cara mengamankan hardware adalah menempatkan di ruangan yang memiliki keamanan yang baik.

Lubang saluran udara perlu diberi perhatian karena dapat saja orang masuk ke ruangan server melalui saluran tersebut. Kabel-kabel jaringan harus dilindungi agar tidak mudah bagi hacker memotong kabel lalu menyambungkan ke komputernya.

Akses terhadap komputer juga dapat dibatasi dengan mengeset keamanan di level BIOS yang dapat mencegah akses terhadap komputer, memformat harddisk, dan mengubah isi Main Boot Record (tempat informasi partisi) harddisk. Penggunaan hardware autentifikasiseperti smart card dan finger print detector juga layak dipertimbangkan untuk meningkatkan keamanan.

## 2) Keamanan software.

Sesuai dengan namanya, maka yang harus diamankan adalah perangkat lunak. Perangkat lunak yang kita maksud disini bisa berupa sistem operasi, sistem aplikasi, data dan informasi yang tersimpan dalam komputer jaringan terutama pada server. Contohnya, jika server hanya bertugas menjadi router, tidak perlu software web server dan FTP server diinstal. Membatasi software yang dipasang akan mengurangi konflik antar software dan membatasi akses, contohnya jika router dipasang juga dengan FTP server, maka orang dari luar dengan login anonymous mungkin akan dapat mengakses router tersebut.

Software yang akan diinstal sebaiknya juga memiliki pengaturan keamanan yang baik. Kemampuan enkripsi (mengacak data) adalah spesifikasi yang harus dimiliki oleh software yang akan digunakan, khususnya enkripsi 128 bit karena enkripsi dengan sistem 56 bit sudah dapat dipecahkan dengan mudah saat ini. Beberapa software yang memiliki lubang keamanan adalah mail server sendmail dan aplikasi telnet. Sendmail memiliki kekurangan yaitu dapat ditelnet tanpa login di port (25) dan pengakses dapat membuat email dengan alamat palsu. Aplikasi telnet memiliki kekurangan mengirimkan data tanpa mengenkripsinya (mengacak data) sehingga bila dapat disadap akan sangat mudah untuk mendapatkan data.

Hal kedua yang perlu diperhatikan adalah password. Sebaiknya diset panjang password minimum untuk mempersulit hacker memecahkan password. Password juga akan semakin baik jika tidak terdiri huruf atau angka saja, huruf kecil atau kapital semua, namun sebaiknya dikombinasi. Enkripsi dapat menambah keamanan jaringan dengan cara mengacak password dan username, baik dalam record di host maupun pada saat password dan username itu dilewatkan jaringan saat melakukan login ke komputer lain.

Untuk user yang tidak perlu mengakses server secara fisik, juga perlu diset agar user tersebut hanya bisa mengakses dari komputer klien. Dalam Windows NT, istilahnya adalah logon locally. User juga perlu dibatasi agar tidak bisa mematikan atau mereboot komputer. Pada sistem UNIX secara default, menekan control-Alt-Delete akan menyebabkan sistem mereboot.

Membatasi lalu-lintas TCP/IP merupakan cara yang paling banyak dipakai. Membatasi lalu-lintas disini, misalnya tidak mengijinkan suatu host atau jaringan melewati paket melalui router apalagi jika telah mengetahui host tersebut adalah milik hacker. Yang paling banyak dilakukan adalah menutup port tertentu yang tidak dibutuhkan, misalnya port telnet (23) dan port FTP (21).

Routing tidak terlepas pula dari gangguan keamanan. Gangguan yang sering muncul adalah pemberian informasi palsu mengenai jalur routing (source routing pada header IP). Pemberian informasi palsu ini biasanya dimaksudkan agar datagram-datagram dapat disadap. Untuk mencegah hal seperti itu, router harus diset agar tidak mengijinkan source routing dan dalam protokol routing diseertakan autentifikasi atau semacam password agar informasi routing hanya didapat dari router yang terpercaya. Autentifikasi ini terdapat pada RIP versi 2 dan OSPF versi 2.

## 2. Macam-Macam Serangan Jaringan Komputer

Pertanyaannya sekarang adalah siapa yang harus diwaspadai dalam keamanan jaringan komputer? Jawabannya hanya satu, MANUSIA. Serangan manusia ini bisa berupa fisik misalnya pencurian perangkat komputer dan bisa berupa non-fisik yaitu serangan dengan menggunakan software. Berikut ini saya akan berikan uraian singkat mengenai bentuk serangan terhadap jaringan komputer;

### 2.1. HACKING

Hacking adalah setiap usaha atau kegiatan di luar izin atau sepengetahuan pemilik jaringan untuk memasuki sebuah jaringan serta mencoba mencuri file password dan sebagainya. Menurut R. Kresno Aji, hacking adalah suatu seni dalam memahami sistem operasi dan sekaligus salah satu cara dalam mendalami sistem keamanan jaringan, sehingga kita bisa menemukan cara yang lebih baik dalam mengamankan sistem dan jaringan.

Pelakunya disebut hacker. Hacker adalah sebutan untuk mereka yang memberikan sumbangan yang bermanfaat kepada jaringan komputer, membuat program kecil dan membagikannya dengan orang-orang di internet. Hacker muncul pada awal tahun 1960-an diantara para anggota

organisasi mahasiswa Tech Model Railroad Club di Laboratorium Kecerdasan Artifisial Massachusetts Institute of Technology (MIT).

Kata hacker pertama kali muncul dengan arti positif untuk menyebut seorang anggota yang memiliki keahlian dalam bidang komputer dan mampu membuat program komputer yang lebih baik dari yang telah dirancang bersama. Kemudian pada tahun 1983, analogi hacker semakin berkembang untuk menyebut seseorang yang memiliki obsesi untuk memahami dan menguasai sistem komputer.

## 2.2. VULNERABILITY

Sering kali kita menemukan kerawanan (vulnerability) ataupun missconfiguration pada sistem sendiri, kita akan menganggap hal itu adalah hal yang kecil karena menganggapnya bukan sebagai lubang keamanan.

## 2.3. TROJAN-VIRUS

Trojan Horse atau lebih dikenal dengan Trojan dalam sistem komputer adalah bagian dari infeksi digital yang kehadirannya tidak diharapkan oleh pemilik komputer. Trojan terdiri dari fungsi – fungsi yang tidak diketahui tujuannya, tetapi secara garis besar mempunyai sifat merusak. Trojan masuk ke suatu komputer melalui jaringan dengan cara disisipkan pada saat berinternet dengan media fisik.

Trojan tidak berpengaruh secara langsung seperti halnya virus komputer, tetapi potensi bahayanya dapat jauh lebih besar dari virus komputer. Trojan dapat diaktifkan dan dikendalikan secara jarak jauh atau menggunakan timer. Pengendalian jarak jauh seperti halnya Remote Administration Tools, yaitu versi server akan dikendalikan oleh penyerang lewat versi client-nya. Banyak hal yang dapat dilakukan oleh penyerang jika komputer korban telah dikendalikan. Port tertentu yang tidak lazim terbuka mengindikasikan adanya kegiatan aktif Trojan.

Penanganan Trojan dapat dilakukan dengan dua cara, yaitu pencegahan (preventif) atau pengobatan (recovery). Usaha pencegahan dilakukan sebelum terjadinya infeksi, yaitu usaha agar sistem tidak mempunyai lubang keamanan. Usaha pengobatan dilakukan setelah sistem terinfeksi, yaitu usaha untuk menutup lubang keamanan yang telah dieksploitasi dan menghilangkan penyebab infeksi.

#### 2.4. THREAT

Threat merupakan salah satu dari tiga komponen yang memberikan kontribusi kepada Risk Management Model, yang digunakan untuk menghadapi ancaman (managing threats).

#### 2.5. ATTACK

Denial of Service adalah aktifitas menghambat kerja sebuah layanan (servis) atau mematikan-nya, sehingga user yang berhak / berkepentingan tidak dapat menggunakan layanan tersebut. Serangan Denial of Service (DOS) ini terjadi apabila penyerang atau yang sering terdengar dengan istilah hacker ini merusak host atau sevice yang ada sehingga host atau service itu tidak dapat lagi berkomunikasi secara lancar di dalam network neighborhood-nya. Perkembangan dari serangan DOS adalah DDOS. Serangan DDoS adalah jenis serangan dengan cara memenuhi trafik server situs tersebut hingga situs menjadi lambat dan susah diakses. Pengertian lain tentang DDOS adalah mengirimkan data secara terus menerus dengan menggunakan satu komputer tidak begitu efektif karena biasanya sumber daya server yang diserang lebih besar dari komputer penyerang.

Dari beberapa pengertian di atas dapat disimpulkan bahwa serangan DDOS (Denial Distribute Of Service) sangat merugikan bagi yang diserang, karena serangan ini dapat menghambat kerja pengguna dari komputer korban. Dimana komputer korban menjadi lambat dan sulit untuk diakses akibat dari penuhnya trafik dalam komputer tersebut.

#### 2.6. EXPLOIT

Exploit adalah sebuah perangkat lunak (software) yang menyerang kerapuhan keamanan (security vulnerability) yang spesifik namun tidak selalu bertujuan untuk melancarkan aksi yang tidak diinginkan. Banyak peneliti keamanan komputer menggunakan exploit untuk mendemonstrasikan bahwa suatu sistem memiliki kerapuhan. Ada badan peneliti yang bekerja sama dengan produsen perangkat lunak. Peneliti itu bertugas mencari kerapuhan dari sebuah perangkat lunak dan kalau mereka menemukannya, mereka melaporkan hasil temuan ke produsen agar produsen dapat mengambil tindakan. Meskipun demikian, exploit kadang menjadi bagian dari suatu malware yang bertugas menyerang kerapuhan keamanan.

#### 2.7. CRACKERS

Cracker adalah sebutan untuk mereka yang masuk ke sistem orang lain dan cracker lebih bersifat destruktif, biasanya di jaringan komputer, mem-bypass password atau lisensi program komputer, secara sengaja melawan keamanan komputer, men-defaced (merusak halaman muka

web) milik orang lain, bahkan hingga men-delete data orang lain, mencuri data dan umumnya melakukan cracking untuk keuntungan sendiri.

Cracker tidak mempunyai kode etik ataupun aturan main, karena cracker sifatnya merusak. Cracker mempunyai situs ataupun cenel dalam IRC yang tersembunyi, yang hanya orang – orang tertentu yang bisa mengaksesnya. Cracker juga mempunyai IP yang tidak bisa dilacak. Kasus yang paling sering dilakukan oleh cracker ialah Carding yaitu Pencurian Kartu Kredit, kemudian pembobolan situs dan mengubah segala isinya menjadi berantakan.

### 3. Membangun Sistem Keamanan Jaringan Komputer Yang Kuat

Agar memudahkan pemahaman kita maka sistem pertahanan di sini saya bagi 2 yaitu sistem pertahanan jaringan Wired (misalnya pada jaringan lab komputer sekolah) dan sistem pertahanan jaringan Wireless untuk koneksi internet.

#### 3.1. Sistem Pertahanan Pada Jaringan Wired Komputer

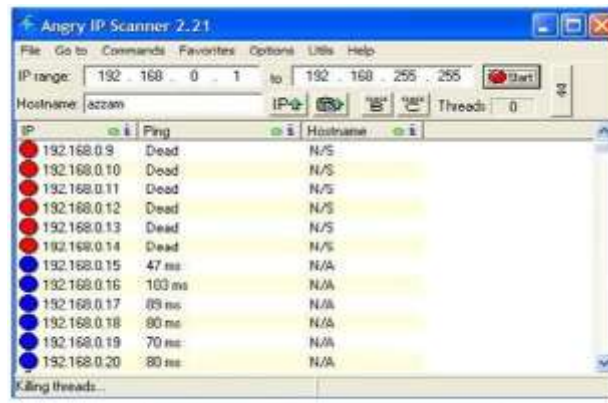
Pertahanan jaringan kabel biasanya pada komputer kantor atau sekolah. Ini berkaitan dengan kewanatan data server yang bisa diserang oleh komputer klien. Pada dasarnya untuk membuat suatu sistem jaringan yang aman tidak lepas dari bagaimana mengelola suatu sistem dengan baik. Persyaratan standar *good practice* seperti *Standard Operating Procedure (SOP)* dan *security policy* haruslah diterapkan di samping memikirkan teknologinya. *Network security* tidak akan efektif kecuali *user* yang menggunakan jaringan mengetahui tanggung jawab masing-masing. Dalam hal menentukan *security policy*, kebijakan harus mencakup :

- 1) Tanggung jawab *user* pada keamanan jaringan, yang meliputi keharusan *user* untuk mengganti *password* dalam periode tertentu, aturan tertentu, atau memeriksa kemungkinan terjadinya pengaksesan oleh orang lain.
- 2) Tanggung jawab *administrator* pada keamanan sistem, misalnya memantau prosedur-prosedur yang digunakan pada *host*.
- 3) Penggunaan yang benar atas *resource network*, dengan menentukan siapa yang dapat menggunakan *resource* tersebut, apa yang dapat dan tidak boleh dilakukan.

Berikut ini beberapa *interface* aplikasi *software* yang digunakan dalam pengelolaan laboratorium komputer di sekolah:

### 1) IPScan

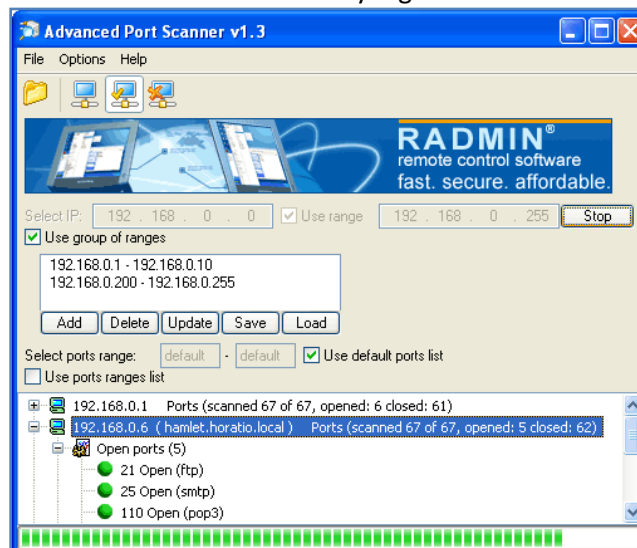
IPscan dimanfaatkan sebagai *tool* ringan dan termasuk *software* yang bebas didownload (*freeware*) untuk mengetahui *Internet Protocol* dari masing-masing *host* (komputer *client* untuk siswa). Seorang administrator dapat pula menggunakan perintah *ping* dengan *command* dari *run*, misal **ping 192.168.0.9** untuk mengetahui status *client* tersebut (ternyata *off*).



Gambar 5.1: Jendela Utama IP scanner

### 2) Portscan

Portscan dimanfaatkan sebagai *tool* ringan dan termasuk *software* yang bebas didownload (*freeware*) untuk mengetahui *port* yang terbuka maupun tertutup di dalam *remote access* dari *host-host* yang ada.



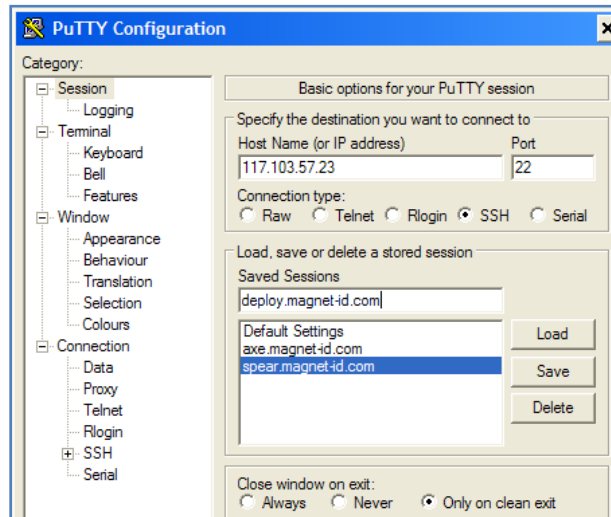
Gambar 5.2: Jendela Utama Port scanner

### 3) Putty, VNC, WinSCP

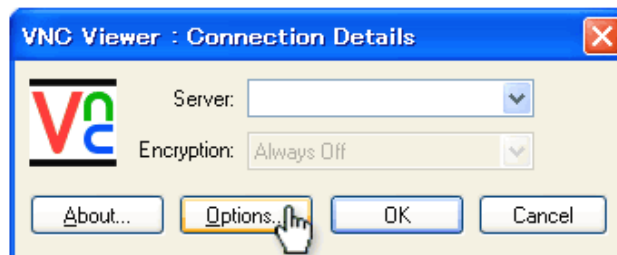
Putty, VNC, WinSCP, SSH, OpenSSH dan yang lain meskipun secara *interface* mempunyai perbedaan-perbedaan namun pemanfaatannya seringkali untuk kepentingan *remote*

*access* antar komputer baik yang berbasis Windows maupun Linux. Dengan *remote access* ini kita dapat masuk ke dalam komputer lain dan memerintahkannya untuk bekerja meskipun secara fisik kita berada di komputer yang berbeda.

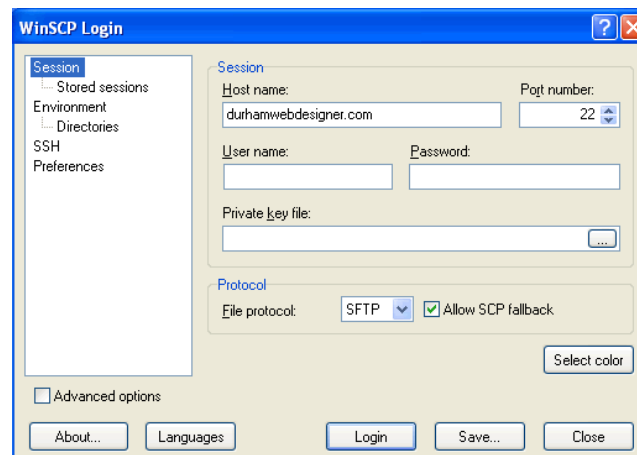
Jika beberapa tahun yang lalu orang mengenal telnet untuk aktivitas *remote access*, saat ini banyak pengguna yang beralih ke aplikasi yang lain.



Gambar 5.3: Jendela Utama Putty



Gambar 5.4: Jendela Utama VNC



Gambar 5.5: Jendela Utama WinSCP



#### 4) Dfd NetOp, Radmin dan Netsupport

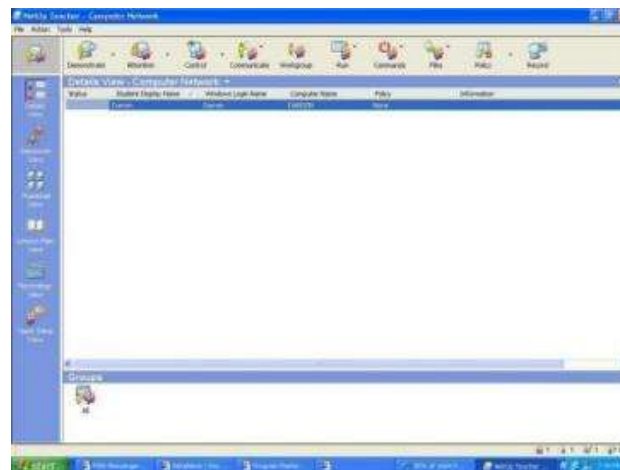
NetOp, Radmin dan Netsupport adalah *tool* aplikasi yang seringkali dimanfaatkan di dalam pengelolaan sebuah laboratorium komputer untuk melakukan *monitoring* terhadap aktifitas para klien dalam memanfaatkan komputer.

Dengan *tool* aplikasi tersebut, seorang administrator atau guru dapat melakukan aktifitas *monitoring* terhadap semua komputer, aktifitas apapun yang dilakukan termasuk memberikan *message* baik berupa *voice* maupun *text* sebagai bentuk *reward* maupun *peringatan*.

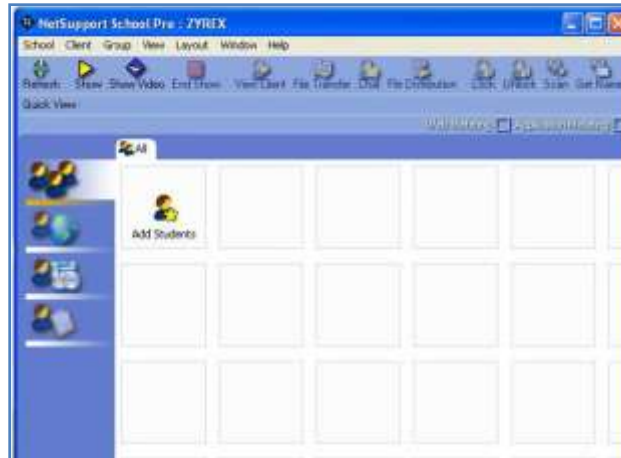
Dengan *tool* di atas administrator dapat pula melakukan *lock* (penguncian) pada sebuah atau beberapa komputer *client* bila user melakukan aktifitas yang melanggar norma. Bahkan administrator dapat melakukan perintah *shutdown* pada komputer-komputer *client* sebagai alternatif terakhir.



Gambar 5.6: Jendela Utama Radmin



Gambar 5.7: Jendela Utama DFD Netop



Gambar 5.8: Jendela Utama Net Support

#### 5) Aplikasi Netsupport Untuk Aktifitas Client Server

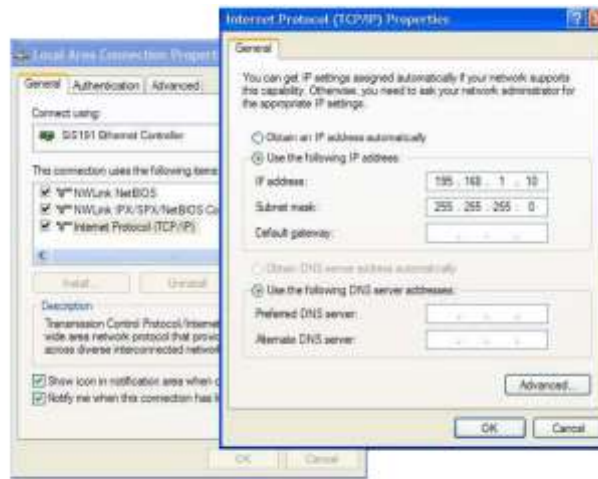
Sebelum melakukan aktifitas dengan aplikasi NetSupport atau yang lain maka diperlukan konfigurasi jaringan terlebih dahulu, *workgroup*, *TCP/IP* maupun menggunakan sarana yang lain. Pengaturan jaringan komputer pada Windows XP tidak jauh berbeda dengan Windows 9x/Me. Pengaturan ini dilakukan agar komputer-komputer dapat saling berkomunikasi di dalam jaringan tersebut. Untuk itu diperlukan pengaturan *IP (Internet Protocol)* yang sekilas terhadap komputer-komputer yang ada. Berikut langkah konfigurasinya, klik kanan **My Network Places**, pada *Desktop* maupun *Control Panel* untuk memunculkan menu *pop-up*.

Setelah itu akan muncul jendela baru yang menampilkan *setting* koneksi jaringan yang dimiliki (yang aktif) oleh sebuah komputer, baik *dial up*, *local area network*, *wireless*.



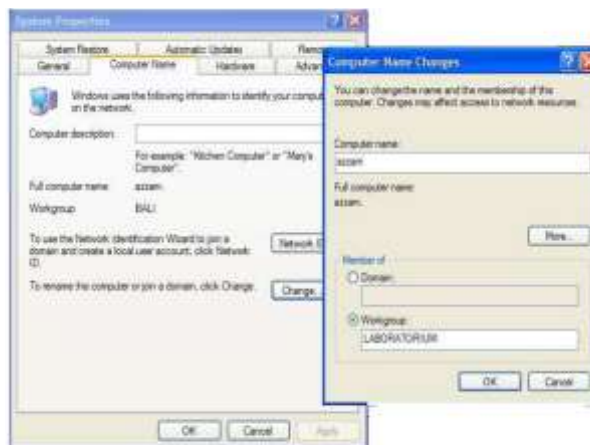
Gambar 5.9: Jendela Utama Network Connection

Klik kanan *mouse* pada *local area connection*, pilih *properties* yang berisi komponen-komponen jaringan komputer yang digunakan oleh Windows XP. Pilih *Internet protocol (TCP/IP)* untuk melakukan pengaturan *NetId*, *HostId* dan *Maskingnya*.



Gambar 5.10: Pengisian IP

Untuk memudahkan pengaturan beberapa jaringan, lebih baik dilakukan pengaturan *workgroup* untuk tiap-tiap jaringan yang berbeda. Misalnya sebuah *workgroup* dengan nama laboratorium (atau bisa apa saja untuk sebuah nama) untuk menandakan sebuah jaringan di laboratorium komputer, *workgroup* TU untuk mengatur jaringan di TU dan sebagainya. Klik kanan pada **My Computer** pilih **Properties**, pada **System Properties** pilih tab **Computer Name** dan klik **change** untuk melakukan perubahan pada nama komputer (tuliskan nama komputer di *Computer Name* misalnya azzam dan lakukan perubahan *workgroup* misalnya laboratorium. Setelah selesai klik OK, bila komputer menghendaki *restart* ikuti untuk melakukan konfigurasi.



Gambar 5.11: Pengisian Computer name dan Workgroup

Bila pengaturan (*hardware* dan *software*) telah dilakukan maka selanjutnya adalah :

- a. Menyiapkan *software* NetSupport School Pro;
- b. Melakukan instalasi *software*, pilih **teacher** untuk komputer *server* dan pilih **student** untuk komputer *client*;
- c. Melakukan konfigurasi dan deteksi seluruh komputer *client*. Bila semua komputer *client* telah terdeteksi dengan baik lakukan pengaturan grup pada *server*. Misalnya komputer 1, komputer 2, komputer 3, komputer 4, komputer 5 dijadikan satu grup menjadi grup barat. Komputer 6, komputer 7, komputer 8, komputer 9 dan komputer 10 untuk grup utara dan sebagainya.



Gambar 5.12: Jendela utama Netsupport

- d. Fasilitas-fasilitas yang dimiliki oleh NetSupport antara lain sebagai berikut:
  - a. **Chat**, baik dengan *text* maupun *voice*;
  - b. **Show**, kepada seluruh atau sebagian komputer *client*;
  - c. **View** (melihat *desktop*), seluruh atau sebagian komputer *client*.
  - d. **File Transfer Protocol**, untuk aktifitas transfer data/file; Penguncian pada sebagian fungsi atau seluruh fungsi komputer *client*; *Remote* jarak jauh. *Reboot* atau mematikan komputer *client*.
- e. Melakukan aktifitas 5. *monitoring*, melihat jalur koneksi dan *peripheral* yang dipakai oleh *client*.

### 3.2. Sistem Pertahanan Jaringan Pada Koneksi Internet

Selain keamanan jaringan kabel yang sudah kita bahas di atas, yang tidak kalah penting adalah keamanan jaringan wireless terutama dalam komunikasi internet anda. Pada bagian ini secara khusus kita akan bahas mengenai jaringan wireless dan pengaturan keamanan yang harus kita lakukan.

Seperti yang Anda ketahui, membuka komputer internet Anda untuk koneksi internet dapat menyebabkan infeksi program jahat seperti virus dan spyware atau juga hacker. Selain virus, Anda perlu khawatir tentang ancaman online lainnya, seperti spam dan phishing e-mail. Bagaimana melindunginya? Anda dapat melindungi diri sendiri, tetapi pertama Anda perlu tahu bagaimana. Bab ini menunjukkan Anda bagaimana caranya.

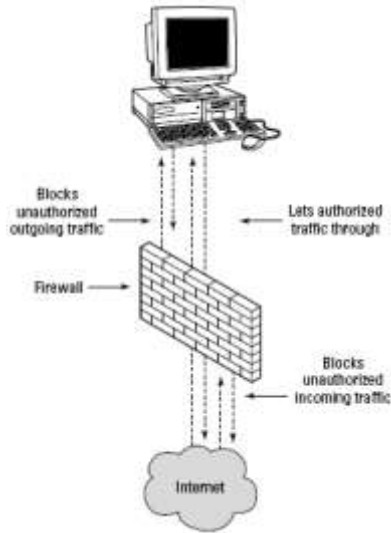
#### 3.2.1. Blokir Hacker internet Menggunakan Firewall

Internet ini adalah jaringan besar, mirip dengan jaringan rumah Anda, tetapi dengan miliaran komputer yang saling berhubungan dari seluruh dunia. Beberapa orang di belakang komputer ini dapat dipercaya, tetapi yang lain jahat. Menghubungkan komputer Anda ke Internet tanpa perlindungan yang tepat memberikan hacker kesempatan untuk terhubung ke komputer Anda untuk melakukan hal-hal jahat seperti

- 1) Mendapatkan file Anda dan informasi sensitif
- 2) Pemantauan lalu lintas Internet Anda
- 3) Mengambil alih komputer Anda untuk mengubah pengaturan dan menyebabkan kekacauan komputer anda, gunakan firewall untuk melindungi diri dari hacker ini.

##### 3.2.1.1. Gambaran besar di balik apa yang dilakukan firewall

Firewall adalah filter yang memonitor lalu lintas data bisa mengisinkan dan bisa mem-blok jika diperlukan, tergantung pada pengaturan yang Anda buat ketika Anda mengatur firewall Anda. Perhatikan ilustrasi di bawah ini;



Gambar 5.13: Ilustrasi firewall

#### 3.2.1.2. Dimana mendapatkan firewall

Sebuah firewall dapat menjadi program perangkat lunak diinstall dalam komputer Anda atau bagian dari hardware yang duduk antara koneksi Internet dan komputer Anda (atau router). Sistem operasi baru seperti berikut ini built-in dengan perangkat lunak firewall:

- Windows 7
- Windows XP

Anda juga dapat menemukan perangkat lunak firewall yang tersedia sebagai produk mandiri atau sebagai bagian dari suite keamanan seluruh Internet, untuk pembelian (atau gratis) dari perusahaan seperti:

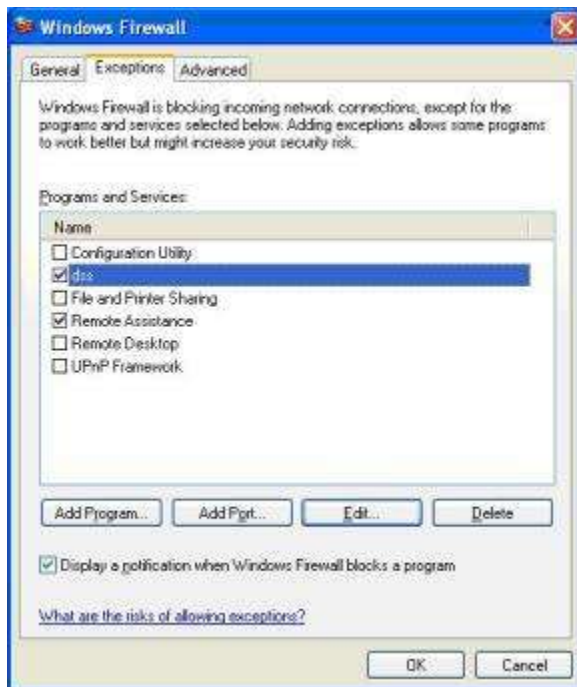
- 1) **McAfee:** [www.mcafee.com](http://www.mcafee.com)
- 2) **CA (Computer Associates):** [shop.ca.com](http://shop.ca.com)
- 3) **Norton (Symantec):** [www.symantec.com/norton](http://www.symantec.com/norton)
- 4) **ZoneAlarm (basic firewall software is free):** [www.zonealarm.com](http://www.zonealarm.com)
- 5) **Comodo Firewall Pro (free):** [www.personalfirewall.comodo.com](http://www.personalfirewall.comodo.com)

#### 3.2.1.3. Konfigurasi Firewall Windows XP

- 1) Klik [Start]->[Control Panel]->[Network and Internet Connections]->[Windows Firewall].
- 2) Klik tab [Exceptions] untuk melihat semua program/port yang diizinkan oleh firewall. Lihat gambar;



Gambar 5.14: Jendela utama firewall

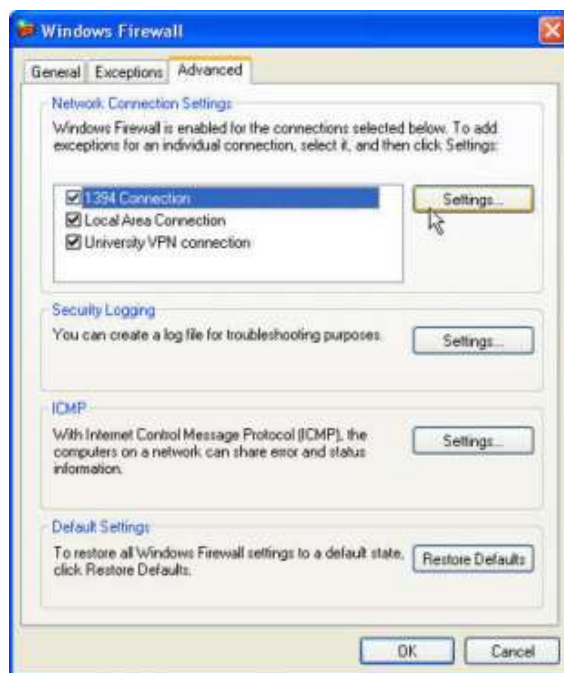


Gambar 5.15: Jendela dan tab Exception firewall

- 3) Klik the [Advanced] untuk melihat lebih banyak:
  - a. Mengaktifkan/menonaktifkan proteksi firewall untuk adapter jaringan tertentu



- b. Mengkonfigurasi pengaturan logging Windows Firewall
- c. Mengkonfigurasi Internet Control Message Protocol (ICMP)
- d. Mengembalikan Windows Firewall ke default, yang berguna jika Anda berpikir firewall telah menyebabkan masalah dengan mengubah pengaturannya



Gambar 5.16: Jendela dan tab Advanced firewall

### 3.2.2. Blocking Viruses, Spyware, dan Adware dengan Software

Meskipun sistem operasi yang lebih Windows XP lebih tahan dari versi sebelumnya, Anda perlu melindungi komputer Anda dari infeksi virus dan spyware. Anda dapat menggunakan program perangkat lunak dimuat pada semua komputer Anda, atau menginstal hardware antara koneksi Internet Anda dan komputer Anda (atau router). Ini solusi anti-infeksi biasanya yang bekerja dengan;

- 1) Terus-menerus melakukan scan daerah yang sering terinfeksi sehingga serangan dapat ditemukan dengan cepat dan kerusakan yang mereka lakukan adalah minimal, jika ada.
- 2) Melakukan secara rutin scan penuh semua sistem file dari infeksi untuk memastikan komputer Anda benar-benar bebas dari infeksi.
- 3) Memperingatkan Anda untuk setiap infeksi yang ditemukan dan secara otomatis memperbaiki mereka atau meminta Anda apa yang harus dilakukan. Anda dapat menemukan antivirus, antispyware, dan software AntiAdware sebagai produk mandiri atau sebagai bagian dari suite keamanan seluruh Internet untuk membeli dari perusahaan seperti;



- a. **McAfee:** [www.mcafee.com](http://www.mcafee.com)
- b. **CA (Computer Associates):** [shop.ca.com](http://shop.ca.com)
- c. **Norton (Symantec):** [www.symantec.com/norton](http://www.symantec.com/norton)

Untuk yang versi free ada bisa menggunakan yang ini;

- 1) **AVG Anti-Virus Free Edition:** [free.grisoft.com](http://free.grisoft.com)
- 2) **avast! 4 Home Edition:** [www.avast.com](http://www.avast.com)
- 3) **PC Tools AntiVirus:** [www.pctools.com/free-antivirus](http://www.pctools.com/free-antivirus)
- 4) **AVG Anti-Spyware Free Edition:** [www.grisoft.com](http://www.grisoft.com)
- 5) **Ad-Aware:** [www.lavasoftusa.com](http://www.lavasoftusa.com)
- 6) **Avira AntiVir:** [www.free-av.com](http://www.free-av.com)

### 3.2.3. Proteksi Diri Dari Phishing Scams

Phishing adalah upaya kriminal dan curang yang mengekstrak informasi sensitif dari Anda. Orang-orang di balik upaya ini menggunakan hal-hal sebagai umpan mereka, dan Anda adalah ikan yang mereka berharap dapat ditangkap. Mereka akan meminta anda menyerahkan informasi sensitif seperti;

- 1) Info Rekening: username dan password e-mail account, situs jejaring sosial, situs lelang online, atau, yang lebih penting, situs Web keuangan anda.
- 2) Info Kartu Kredit: kartu kredit Anda, nomor verifikasi, dan alamat penagihan
- 3) Identitas Anda: rincian lengkap pribadi Anda, seperti nama lengkap Anda, alamat, dan nomor HP dll, beberapa phisher atau scammer bahkan mungkin meminta Anda mengeluarkan uang tunai. Sebagai contoh, Anda mungkin menerima e-mail yang mengatakan bahwa Anda telah memenangkan hadiah atau telah mewarisi uang tetapi bahwa Anda harus mengirimkan sejumlah biaya sebelum uang Anda diserahkan kepada Anda.

Selain mengawasi tanda-tanda penipuan phishing, Anda dapat menggunakan detektor phishing. Alat-alat ini memelihara daftar situs phishing yang sudah dikenal dan mengingatkan Anda jika Anda mengunjungi sebuah situs pada daftar. Berikut adalah beberapa tempat Anda mungkin dapat menemukan fitur ini:

- 1) Built-in dalam Web browser: Sebagian besar versi terbaru dari Web browser populer (misalnya, Microsoft Internet Explorer dan Mozilla Firefox) sudah terpasang fitur anti-phishing.

- 2) perangkat lunak keamanan Internet: suite Banyak anti-phishing keamanan Internet dijual dipasaran.

Jika anda menggunakan Firefox sebagai default webbrowser, berikut ini cara setting anti phisingnya;

- 1) buka Firefox.
- 2) Pilih [Tools]->[Options]->[Security].
- 3) Pilih pilihan [Tell Me If the Site I'm Visiting Is a Suspected Forgery].
- 4) Pilih dan cek [Using a Downloaded List of Suspected Sites for basic protection] atau [Check By Asking (Google or Another Service) About Each Site I Visit].

Daftar-download dari situs yang dicurigai secara otomatis diperbarui secara teratur. Memeriksa situs di Google atau mesin pencari lain, akan memberikan perlindungan terbesar karena setiap situs yang Anda kunjungi akan diperiksa secara real time dari daftar yang diperbarui sepanjang waktu.

- 5) Klik [OK] dan tutup jendela Options.

#### 3.2.4. Menggunakan Internet Security Hardware Solutions untuk Jaringan Komputer

Sebuah metode baru untuk melindungi komputer Anda dari semua infeksi dan ancaman adalah dengan menggunakan solusi hardware. Anda dapat melihat produk ini bernama Adapter Internet Security, dijual sekitar \$ 100 dan menawarkan dukungan untuk beberapa komputer.



Gambar 5.17: **Internet Security Hardware**

Produk ini menawarkan fitur dan komponen sebagai suite perangkat lunak, dan memiliki beberapa manfaat tambahan, seperti:

- 1) Melindungi seluruh jaringan Anda: Alih-alih melindungi satu komputer saja, seperti dengan perangkat lunak, solusi perangkat keras dapat memberikan perlindungan untuk seluruh jaringan Anda.
- 2) Lebih mudah pengaturan pada PC Anda: Karena perlindungan berbasis hardware, tidak akan pengaturan dalam sistem operasi komputer Anda. Terus-menerus menjalankan perangkat lunak membuat komputasi anda jauh lebih aman.

### 3.2.5. Upgrading Sistem Operasi Anda

Jika Anda menggunakan versi kuno dari suatu sistem operasi (seperti 98, atau ME untuk Windows), Anda harus berpikir tentang upgrade ke versi yang lebih baik (seperti Windows 7 atau Windows XP). Usahakan sistem operasi anda selalu diupdate sesuai perkembangan sistem operasi bersangkutan. Cara ini bisa manual dan bisa secara otomatis anda atur pada komputer.

### 3.2.6. Memblock Iklan Pop-Ups

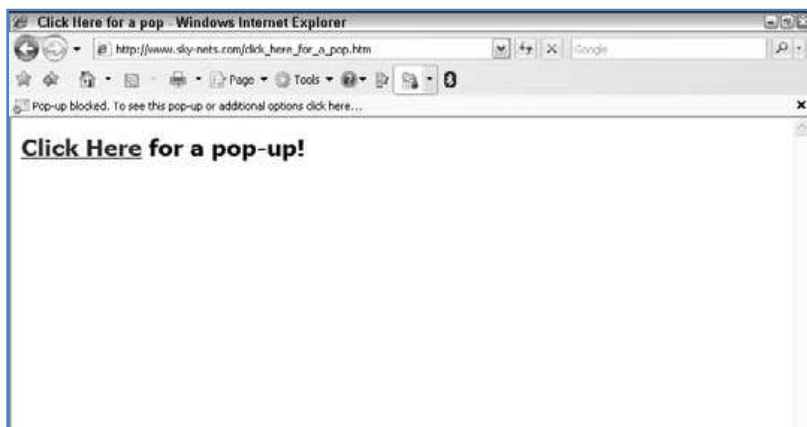
Pop-up adalah iklan yang biasanya berupa jendela kecil yang muncul pada layar komputer Anda. Sebagian pop-up menampilkan halaman web atau gambar dari Internet, namun mereka dapat muncul di berbagai tempat dan di berbagai waktu:

- 1) Ketika Anda memasuki atau meninggalkan suatu situs Web atau halaman Web.
- 2) Ketika Anda membuka atau menutup browser Web Anda.
- 3) Kapan pun Anda terhubung ke Internet, jika komputer Anda terinfeksi dengan adware atau spyware.

Hentikan bahaya itu dengan pop-up blockers. Untuk menghentikan pop-ups ini, anda dapat menggunakan pop-up blocker berupa;

- 1) **Built-in pada Web browsers:** Microsoft's Internet Explorer, Mozilla Firefox, dan Opera sudah include dengan pop-up blocker feature.
- 2) **Web browser toolbars:** Yahoo! or Google
- 3) **Internet security software:** Some Internet security suites include a popup blocker. When you're running pop-up blockers, any pop-up windows that try to open are blocked. You are usually notified when this happens. Figure 1-9 shows an example of Internet Explorer's pop-up blocker alert. Beberapa keamanan Internet termasuk popup blocker. Ketika Anda menjalankan pop-up blocker, beberapa jendela pop-up yang coba-coba untuk membuka menjadi diblokir. Anda

biasanya diberitahu ketika hal ini terjadi. Gambar dibawah menunjukkan contoh dari pop-up blocker peringatan Internet Explorer



Gambar 5.18: **PopUp**

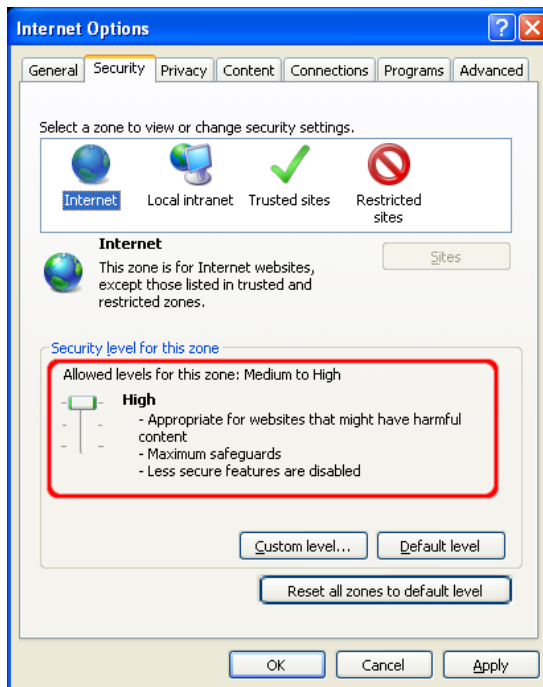
Sebagai contoh dibawah ini diberikan contoh cara menggunakan pop-up blocker pada Firefox;

- 1) Buka Firefox.
- 2) Pilih [Tools]->[Options]->[Content].
- 3) Buat seleksi pada pilihan [Block Pop-Up Windows].
- 4) Ketika pilihan [Block Pop-Up Windows] diaktifkan, anda bisa mengklik tombol [Exceptions] untuk menambah alamat Web sites yang ingin anda blokir.

### 3.2.7. Pencegahan Bahaya ketika Browsing

Pengaturan browser Web Anda dan situs yang Anda kunjungi memainkan peran utama dalam apakah komputer Anda aman atau mendapat infeksi. Jika keamanan Anda atau pengaturan privasi diset ke posisi rendah, komputer Anda jauh lebih rentan mendapatkan virus, spyware, dan adware. Anda harus melakukan pengaturan keamanan browser Web Anda untuk memastikan telah diatur ke tingkat yang wajar. Anda biasanya dapat mengakses preferensi browser atau opsi dari File, Edit, atau menu Tools pada toolbar. Metodologi balik pengaturan keamanan dan privasi browser adalah hampir sama pada setiap webbrowser. Contoh pada Internet Explorer:

- 1) Buka Internet Explorer.
- 2) Klik [Tools] pada menu bar.
- 3) Klik [Internet Options].
- 4) Klik [Security] tab.



Gambar 5.19: Internet Explorer's security settings.

Dari gambar diatas, silahkan lakukan pengaturan keamanan sesuai kebutuhan anda dengan menggeser slider ke atas atau ke bawah. Setelah itu periksa privacy settings seperti berikut ini;



Gambar 5.20: Internet Explorer's privacy settings.

Dari gambar diatas silahkan anda atur level Privacy anda dengan menggeser slider.

### 3.3. Keamanan Jaringan Wi-Fi

Jika jaringan nirkabel tidak aman (tanpa enkripsi), Anda memiliki dua masalah utama untuk:

- 1) Real-time traffic Anda tidak aman.
  - a. Orang-orang dapat melihat apa situs Web yang Anda kunjungi.
  - b. Informasi login Anda dan isi dari situs Web yang Anda kunjungi tidak aman.
  - c. Login informasi dan konten dari layanan seperti e-mail POP3 account dan File Transfer Protocol (FTP) aka terganggu.
- 2) Jaringan nirkabel Anda terbuka bagi orang lain untuk tersambung.
  - a. Koneksi Internet Anda dapat digunakan untuk mengirim atau menerima informasi ilegal, seperti perangkat lunak spam e-mail dan pembajakan.
  - b. Orang lain dapat mengakses file bersama pada PC atau server yang terhubung ke jaringan.

#### 3.3.1. Mengamankan Wireless Network

Untuk memastikan bahwa Anda tidak jadi korban pengintai Wi-Fi atau hacker, pastikan bahwa Anda melakukan hal ini:

- 1) Mengamankan lalu lintas jaringan wireless secara real-time dan mencegah koneksi dari orang lain yang tidak sah.
- 2) Gunakan enkripsi, seperti WPA (Wi-Fi Protected Access) atau WPA2.
- 3) Lakukan perubahan awal yang diperlukan:
  - a. Ubah password router anda.
  - b. Mengubah nama jaringan default dari router anda.
- 4) Menerapkan perlindungan lainnya (opsional) untuk menyediakan pencegahan lebih lanjut terhadap koneksi penyusup:
  - a. Nonaktifkan nama jaringan (SSID) broadcasting.
  - b. Gunakan alamat MAC filtering. Menggunakan enkripsi terbaru (WPA atau WP2) saja biasanya memberikan perlindungan yang memadai terhadap Wi-Fi penyadap dan hacker. Di sisi lain, idealnya Anda harus membahas keamanan jaringan lebih mendalam yang berarti bahwa Anda harus menggunakan metode lain selain enkripsi. Tapi untuk jangka panjang, itu semua terserah Anda.

### 3.3.2. Enkripsi Wi-Fi Anda

Kebanyakan wireless router meminta Anda untuk mengkonfigurasi pengaturan keamanan dan enkripsi saat pemasangan awal, apakah itu melalui program perangkat lunak dari CD atau di Web berbasis konfigurasi utilitas router. Jika Anda belum melakukan penyiapan awal router, Anda dapat memilih untuk menggunakan rekomendasi dan terminologi yang diberikan untuk membantu Anda mengatur enkripsi selama pengaturan awal, atau Anda hanya dapat melewati pengaturan tersebut (tidak mengaktifkan enkripsi apapun) dan menggunakan petunjuk berikut untuk mengaktifkan enkripsi setelah Anda memiliki router dan jaringan. Anda memiliki dua langkah dasar untuk mengatur enkripsi:

- 1) Mengkonfigurasi pengaturan enkripsi dan tombol pada router nirkabel Anda. Untuk membuat keamanan Wi-Fi lebih mudah (dan mungkin lebih menarik) bagi konsumen seperti Anda, beberapa produsen telah mengembangkan jaringan enkripsi-memungkinkan mereka sendiri metode menggunakan tombol-tombol. Tombol pada perangkat keras itu sendiri atau pada aplikasi perangkat lunak memungkinkan Anda untuk mengatur enkripsi hanya dengan menekan beberapa atau klik. Untuk mengetahui apakah peralatan Anda memiliki kemampuan ini, lihat di router Wi-Fi Anda dan utilitas adaptor nirkabel untuk melihat apakah ada tombol berlabel dengan istilah-istilah seperti Keamanan, Enkripsi, atau Secure.
- 2) Konfigurasi atau masukkan kunci enkripsi pada komputer Anda.



Gambar 5.21: Contoh wireless router dengan tombol security.

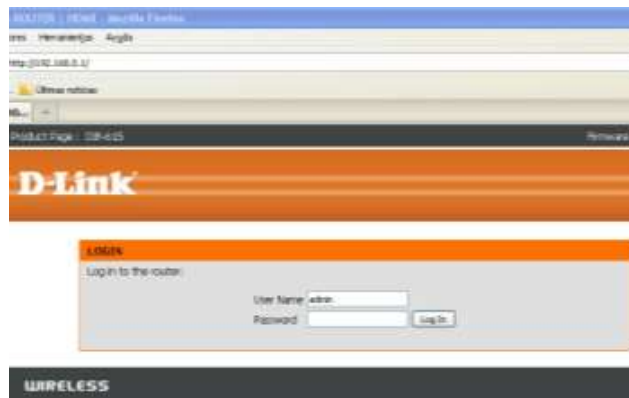
Perlu diingat bahwa produsen biasanya menjual produk sesuai dengan nama merek dagang mereka sendiri pernyediaan jenis fitur. Jika Anda melihat bahwa router Anda

memiliki beberapa fitur, Anda harus lihat dokumentasi produk Anda untuk informasi tentang bagaimana menggunakannya. Namun, biasanya Anda menekan tombol pada router Wi-Fi dan, dalam jumlah waktu tertentu dan tekan tombol adaptor pada semua utilitas nirkabel Anda.

### 3.3.3. Enkripsi Manual Wireless Router

Untuk mengenkripsi jaringan nirkabel Anda, pertama Anda harus memilih pengaturan tombol di atasnya. Berikut caranya:

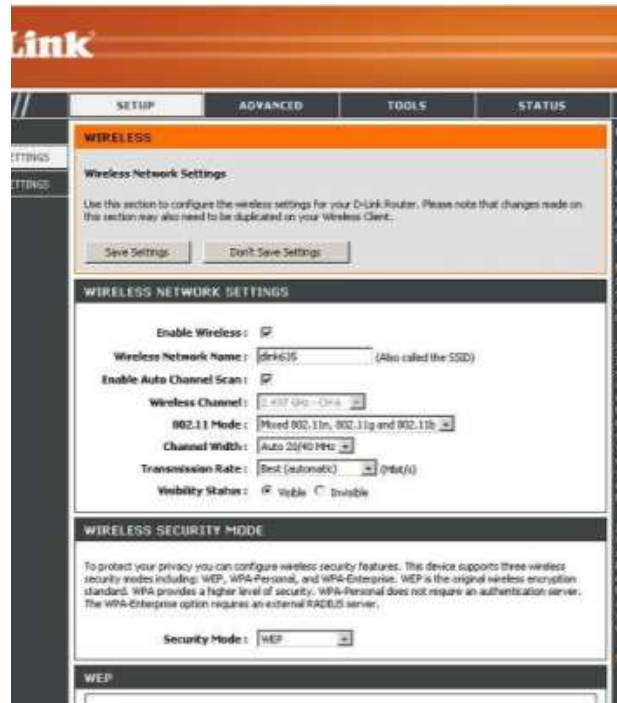
- 1) Buka Web browser Anda (Internet Explorer, Netscape, Firefox, atau lainnya), ketik alamat IP router anda, dan tekan Enter. Perlu diingat bahwa beberapa produsen dapat menggunakan nama domain, yang terlihat seperti alamat situs Web, bukan alamat IP. Dibawah ini saya berikan cara enkripsi router dari merek D-LINK.
- 2) Bila diminta, masukkan login Anda, seperti yang ditunjukkan pada Gambar di bawah.



Gambar 5.22: Login ke router dengan IP address.

- 3) Cari pengaturan enkripsi, biasanya pada tab [Security] berlabel [Wireless Security], dalam bagian [Wireless].





Gambar 5.23: setting encrypsi pada wireless router.

Beberapa router nirkabel baru mungkin menawarkan wizards untuk membantu dalam konfigurasi keamanan, namun Anda masih dapat secara manual mengkonfigurasi pengaturan keamanan nirkabel, yang lebih disukai.

- 4) Tentukan apa metode enkripsi yang didukung oleh router Anda, seperti dengan mengklik daftar menu drop-down.
- 5) Pilih metode enkripsi terbaik yang didukung oleh semua komputer Anda (atau adapter nirkabel). Dalam urutan berikut, diurutkan dari terbaik sampai terburuk, pilih salah satu dari metode berikut:
  - i. WPA2-PSK (Pribadi)
  - ii. WPA-PSK (Pribadi)
  - iii. WEP

Penjelasan lengkap mengenai ini include dengan Merk Router yang anda gunakan.

## MELAKUKAN KONEKSI PADA JARINGAN

Dalam bab ini Anda akan belajar :

1. Melakukan Koneksi Jaringan Kabel.
2. Melakukan Koneksi Jaringan Wireless.
3. Memeriksa Status Koneksi Jaringan
4. Set Up dan Tes Remote Desktop Pada Windows
5. Set Up dan Tes Remote Desktop Web Connection

Setelah Anda menyiapkan jaringan computer dan sudah dipastikan semua baik, sekarang waktunya Anda menghubungkan jaringan. Koneksi kabel membutuhkan hanya menghubungkan kabel, namun jaringan nirkabel memerlukan beberapa klik mouse. Juga, kedua jenis koneksi memiliki berbagai tugas yang mungkin Anda perlu tahu bagaimana melakukannya, seperti memeriksa apakah Anda sudah terhubung, mengubah pengaturan jaringan, dan preferensi.

Dalam bab ini, Anda akan melihat mengenai cara melakukan koneksi jaringan dan cara melakukan sharing dalam jaringan computer lokal

### 1. Melakukan Koneksi Jaringan Kabel.

Sebelum melakukan koneksi dalam jaringan kabel, pastikan bahwa computer server dan klien telah siap, termasuk pemasangan kabel dan Hub/Switch secara benar. Setelah selesai silahkan hidupkan semua computer dalam jaringan. Setelah semua computer dihidupkan, silakan kunjungi setiap computer dalam jaringan dan lakukan hal berikut;

- 1) Amati status koneksi local area pada system tray setiap komputer baik server maupun Klien.

Lihat gambar di bawah ini;



Gambar 6.1: Ikon network pada system tray

- 2) Dobel klik ikon diatas untuk melihat propertinya.



Gambar 6.2: Local area networks connection status

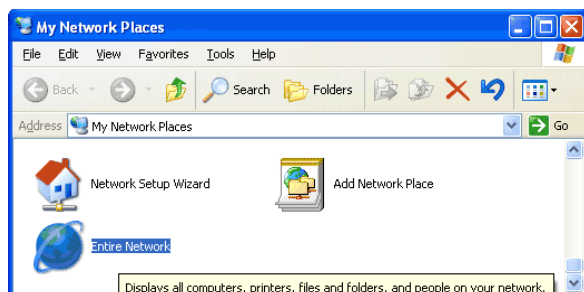
- 3) Gambar diatas menunjukkan komputer bersangkutan terkoneksi ke jaringan dengan baik. Lakukan hal yang sama untuk komputer yang lain untuk memastikan koneksi jaringan anda.

Jika Anda tidak menemukan ikon Quick access network pada System Tray, mungkin tidak diatur sebelumnya untuk muncul atau mungkin dinonaktifkan. Berikut adalah bagaimana Anda dapat mengaktifkan atau menonaktifkan ikon tersebut:

- 1) Pilih [Start]->[Connect To]->[Show All Connections]. Jika menggunakan Desktop setelah menu Classic Start, Klik [Start] lalu klik [Settings], Klik kanan [Network Connections] dan klik [Open] dan kemudian lanjut ke Langkah 2 dibawah.
- 2) Pada jendela [Network Connections] yang terbuka, klik kanan ikon jaringan yang dikehendaki dan pilih Properties.
- 3) Pada jendela [Network Connection Properties], pilih atau hapus **[Show Icon in Notification Area When Connected]** yang dekat bagian bawah jendela.
- 4) Itu saja dan tutup jendela yang terbuka.

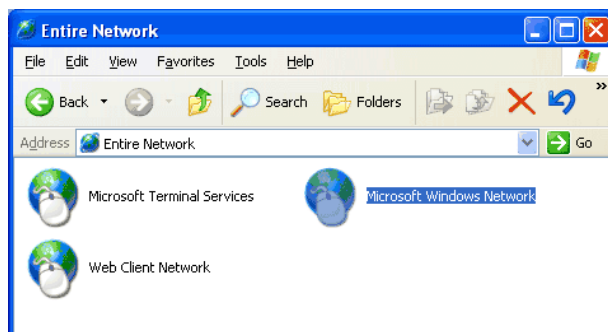
Cara lain untuk melihat status koneksi jaringan adalah melalui fasilitas My Network places pada komputer. Lakukan langkah-langkah berikut;

- 1) Klik tombol [Start] lalu pilih [My Network Places]. Jika tidak ada silahkan klik [Control Panel] dan klik dua kali [Network Connection] sehingga di kolom sebelah kiri layar akan muncul My Network Places
- 2) Klik dua kali [My Network Places]
- 3) Dari jendela [My Network Places] klik dua kali [Entire Network]



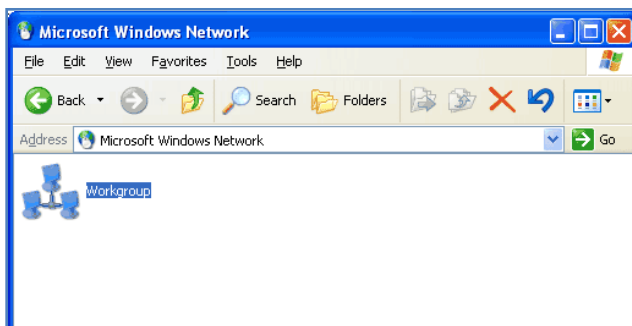
Gambar 6.3: Jendela my Network Places

- 4) Selanjutnya klik double klik pada [Microsoft Windows Network], lihat gambar di bawah;



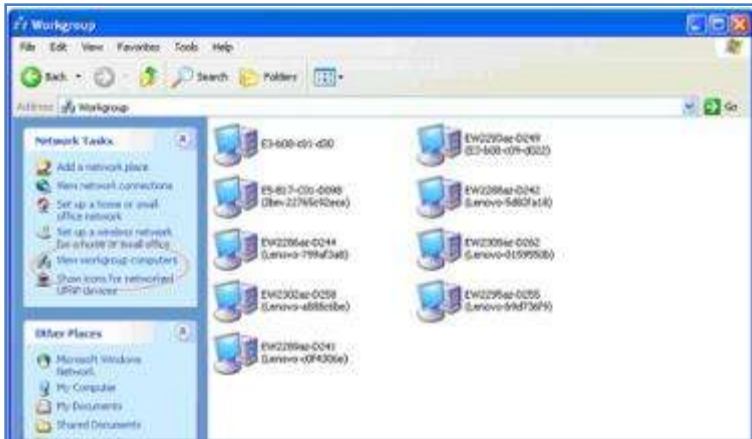
Gambar 6.4: Jendela Entire Network

- 5) Setelah jendela [Microsoft Windows Network] terbuka, silahkan klik dua kali [Workgroup]



Gambar 6.5: Jendela Microsoft Windows Network

- 6) Setelah langkah diatas, akan muncul jendela Workgroup seperti dibawah ini;



*Gambar 6.5: Komputer yang aktif dalam Workgroup*

Dari jendela di atas, pastikan jumlah computer yang muncul adalah sejumlah computer klien dalam jaringan yang anda bangun. Jika tidak ada yang hilang, bias dipastikan ada sambungan kabel yang tidak baik waktu pemasangan.

**Catatan:** Jika ada komputer yang tidak terkoneksi dalam tes di atas, akan dibahas pada Network Troubleshooting.

## 2. Melakukan Koneksi Jaringan Wireless.

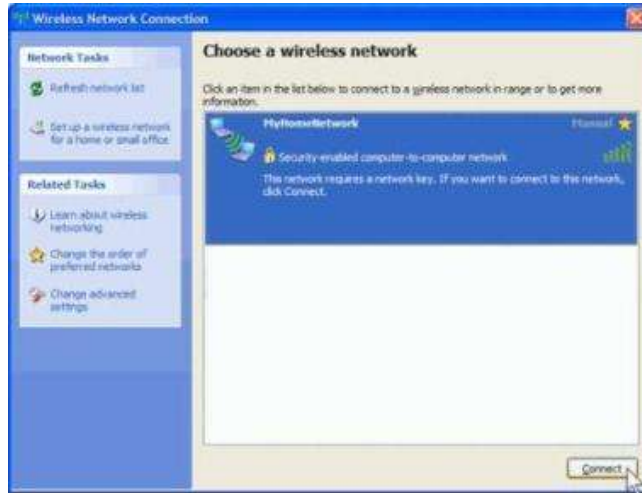
Untuk memastikan bahwa wireless router yang berfungsi sebagai access point yang kita bangun, kita akan tes dengan mencoba melakukan koneksi.

2.1. Menggunakan Ikon Network Quick Access untuk Pilihan Pengaturan Jaringan. Windows XP mempunyai ikon-ikon dan fitur network adapter pada system tray (area pemberitahuan), yang di sudut kanan bawah Windows. Windows XP memiliki ikon untuk setiap adapter jaringan yang aktif. Ikon ini memungkinkan Anda mengakses utilitas jaringan. Lihat gambar di bawah ini;



*Gambar 6.6: Melihat jaringan wireless yang sedang aktif*

- 2) Muncul jendela [Wireless Network Connection] dan menampilkan jaringan nirkabel anda. Klik jaringan wireless anda, lalu klik [Connect] disudut kanan bawah. Lihat gambar dibawah ini;



Gambar 6.7: Memilih jaringan wireless yang sedang aktif

- 3) Jika jendela [Wireless Network Connection] di atas ternyata kosong atau tidak ada wireless yang terdeteksi berarti Router Access Point anda masih ada masalah. Jika wireless network terdeteksi, lanjutkan dengan langkah dibawah ini.
- 4) Windows XP akan meminta anda memasukkan kata kunci, masukkan kata kunci ke kotak [Network key] dan [Confirm network key], lalu klik [Connect].



Gambar 6.8: Autentikasi dalam koneksi

- 5) Sekarang Windows xp akan melakukan koneksi ke Router anda.

### 3. Memeriksa Status Koneksi Jaringan

Kadang-kadang Anda mungkin ingin memeriksa status koneksi jaringan, anda dapat dengan mudah memeriksa status jaringan komputer ini dan mendapatkan gambaran singkat tentang status jaringan Anda. Ikon jaringan pada system tray memiliki X merah apabila Anda tidak terhubung, baik pada jaringan kabel (Ethernet) atau nirkabel.

Jika Anda tersambung dan ada aktivitas dari komputer dalam jaringan, akan kelihatan beberapa jenis animasi, misalnya, ikon nirkabel, ikon gelombang radio kecil menyala dalam warna hijau sekali-sekali. Anda juga dapat melayangkan kursor mouse di atas ikon untuk mendapatkan gambaran singkat tentang status. Jika Anda ingin informasi lebih lanjut tentang status, klik dua kali ikon jaringan dan jendela [Network Connection Status] akan muncul jika Anda sedang terhubung ke jaringan.

Pada jendela [Network Connection Status], baik untuk koneksi kabel atau nirkabel, Anda akan melihat status (jika terhubung atau tidak), durasi koneksi Anda ke jaringan, kecepatan data rate dari koneksi Anda, dan bagian kegiatan yang menunjukkan jumlah paket data yang telah dikirim dan diterima komputer Anda. Pada jendela [Network Connection Status], untuk koneksi nirkabel, Anda juga melihat nama jaringan (SSID) dan kekuatan sinyal koneksi Anda.

Pada jendela [Network Connection Status], baik untuk koneksi kabel atau nirkabel, Anda dapat klik tab [Support] untuk melihat informasi alamat IP. Ini adalah tempat umum untuk dikunjungi ketika troubleshooting masalah jaringan. Daftar berikut menjelaskan item pada tab [Support]:

- 1) **Address Type:** Menentukan bagaimana alamat IP Anda muncul, yang dapat mencakup sebagai berikut:
  - a. **Assigned by DHCP:** Alamat diberikan ke komputer Anda dari jaringan (router).
  - b. **Manually Configured:** Ini berarti bahwa Anda yang memberi alamat IP tertentu ke komputer Anda, yang biasanya tidak diperlukan kecuali Anda menonaktifkan DHCP server di router Anda karena beberapa alasan keamanan.
  - c. **Automatic Private Address:** Ini menunjukkan bahwa Anda tidak diberikan alamat secara manual dan komputer Anda tidak bisa mendapatkan salah satu dari jaringan. Hal ini biasa terjadi saat menghubungkan jaringan computer to komputer (jaringan ad hoc), namun jika Anda menghubungkan ke jaringan nirkabel biasa, pemunculan hal ini dalam Address Type menandakan jaringan Anda memiliki masalah.



- 2) IP Address: Ini adalah alamat unik IP komputer Anda di jaringan, yang dapat digambarkan sebagai "nomor ID" Anda untuk mengirim dan menerima lalu lintas internet dan jaringan.
- 3) Subnet Mask: Ini adalah nomor yang mengidentifikasi subnet jaringan. Anda tidak perlu khawatir apa-apa dengan nomor ini. (Ini mungkin harus 255.255.255.0.)
- 4) Default Gateway: IP address dari router atau komputer anda yang terhubung ke internet.
- 5) **Details:** klik tombol ini untuk menampilkan jendela kecil dengan beberapa informasi singkat, termasuk Alamat Fisik adaptor jaringan Anda (MAC), yang dapat berguna jika Anda mengatur filtering alamat MAC pada router untuk tujuan keamanan.
- 6) **Repair:** Jika Anda mengalami masalah dengan koneksi jaringan Anda (mendapatkan **Automatic Private Address**), Anda dapat mengklik tombol ini untuk mencoba memperbaikinya. Windows akan mencoba beberapa hal, termasuk menonaktifkan dan reenabling adaptor jaringan dan meminta alamat IP untuk komputer Anda.

**Catatan :** Disini hanya tes koneksi saja, semua permasalahan yang muncul akan dibahas pada bab Troubleshooting.

#### 4. Set Up dan Tes Remote Desktop Pada Windows

Mungkin anda bertanya, mengapa kita melakukan koneksi remote ke desktop pada jaringan? Katakanlah Anda di rumah dengan nyaman bekerja di tempat tidur dan laptop Anda tidak memiliki aplikasi pengolah kata yang Anda butuhkan, tapi komputer di ruang tamu memilikinya. Jika jaringan nirkabel atau kabel menghubungkan komputer, Anda dapat mengakses aplikasi yang Anda butuhkan dari komputer di ruang tamu tanpa meninggalkan kamar tidur Anda. Hal yang sama berlaku untuk kantor.

Ada beberapa aplikasi lainnya selain Windows XP Remote Desktop yang akan memungkinkan Anda untuk koneksi secara remote ke komputer lain di jaringan lokal atau melalui Internet. Namun, hal terbaik tentang Windows XP Remote Desktop adalah bahwa fasilitas itu disertakan dengan paket Sistem Operasi Windows XP, dan mungkin sudah diinstal di komputer Anda. Aplikasi lain biasanya harus dibeli dan men-download perangkat lunak, kemudian mengkonfigurasi built-in Windows Firewall.

Anda juga dapat mencetak dokumen Anda menggunakan printer komputer remote, dan mengambil audio dari komputer remote ke speaker Anda sendiri. Selain itu, Anda akan selalu



menggunakan aplikasi tertentu setiap kali Anda menghubungkan jarak jauh. Anda dapat mengatur Remote Desktop untuk meluncurkan aplikasi yang Anda butuhkan secara otomatis setiap kali Anda terhubung, menghemat waktu Anda yang berharga.

Untuk pengguna dengan beberapa komputer pada jaringan di rumah atau kantor yang membutuhkan program-program dan aplikasi yang akan dibagi antara komputer, Remote Desktop akan melakukan trik. Remote Desktop sudah dibangun ke dalam sistem operasi Windows XP dan mudah diatur. Langkah-langkah di bawah ini akan memandu Anda melalui proses pengaturan Remote Desktop pada komputer Anda.

Inilah langkah-langkahnya;

- 1) Klik kanan pada [My Computer] dari desktop, lalu klik [Properties] lalu akan muncul jendela berikut;



Gambar 6.9: Jendela System Properties

- 2) Klik tab [Remote].



Gambar 6.10: Jendela System Properties pada tab Remote

- 3) Dari jendela [Remote] cari dan beri tanda centang pada [Allow users to connect remotely to this computer]. Anda mungkin tidak ingin memilih pilihan ini pada saat ini. Anda hanya perlu mengklik [Select remote user...] di sini jika Anda akan tersambung ke komputer ini dengan account selain account default untuk sistem lokal. Setelah Anda selesai, klik [Apply] dan kemudian klik [OK] untuk menutup jendela.
- 4) Langkah selanjutnya adalah klik tombol [Start] dan masuk ke [All Programs] -> [Accessories] -> [Communications] lalu klik [Remote Desktop Connection]
- 5) Dari langkah diatas, akan muncul jendela berikut;



Gambar 6.11: Permintaan nama komputer pada remote connection

- 6) Dari jendela [Remote Desktop Connection], klik tombol [Options>>] dan akan muncul pilihan untuk membuka [Remote Desktop Connection] anda. Ini juga merupakan daerah di mana Anda

memasukkan nama komputer pada jaringan Anda yang ingin Anda akses dari jarak jauh, atau menelusuri komputer yang terhubung ke jaringan komputer Anda. Anda juga dapat memasukkan nama pengguna dan password jika Anda ingin untuk otentikasi pada komputer lokal yang Anda hubungkan dari jarak jauh. Setelah Anda mengatur opsi yang Anda inginkan, klik tombol [Connect].



Gambar 6.12: Jendela remote desktop connection

- 7) Setelah mengklik tombol [Connect], anda akan melihat desktop dengan remote computer. Setelah itu silahkan Anda mengakses komputer remote, dan klik "X" pada tab berwarna krem di bagian atas layar untuk full screen remote desktop session atau "X" merah untuk windowed remote desktop session.



Gambar 6.13: Jendela komputer lain dalam jendela komputer remote

- 8) Bagian terakhir adalah tampilan jendela komputer lain (yang anda akses) dari komputer anda. Anda bisa menggunakan layar penuh dan layar tidak penuh.

Menyiapkan Remote Desktop di Windows XP dapat dikerjakan bahkan oleh pengguna komputer yang belum berpengalaman. Di rumah dan kantor akses ke komputer lain jadi dan peralatan peripheral meningkatkan fleksibilitas, memaksimalkan produktivitas, dan menghemat waktu, uang, dan energi. memanfaatkan keuntungan dari fitur Windows ini akan membantu Anda mencapai tujuan jaringan komputer Anda.

##### 5. Set Up dan Tes Remote Desktop Web Connection

Remote Desktop Web Connection adalah klien Remote Desktop yang dikemas sebagai kontrol ActiveX yang dapat tertanam di halaman Web untuk menyediakan akses ke Server Terminal atau komputer yang menjalankan Windows XP Professional atau Windows Server 2003 dengan Remote Desktop yang diaktifkan. Remoter Desktop Web Connection menyediakan sebagian besar fungsi yang sama sebagai perangkat lunak Remote Desktop Connection, tetapi tidak memerlukan sebuah jaringan kabel, atau koneksi jaringan virtual pribadi.

Kebutuhan untuk fasilitas ini;

- Di sisi komputer server, Anda membutuhkan Internet Information Server 4.0 atau yang lebih tinggi. Windows XP dan Windows Server 2003 telah memiliki komponen ini tapi pertama-tama harus diinstal dari Add / Remove Programs
- Di sisi komputer client, dapat dijalankan pada platform Windows dengan Internet Explorer 4 atau yang lebih baru dengan mengaktifkan ActiveX.

Langkah-langkah instalasi;

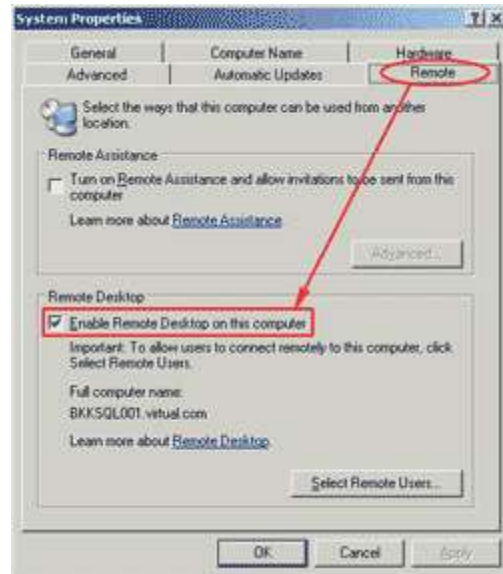
- 1) Aktifkan Remote Desktop Connection pada komputer server.
- 2) Masuk ke [Control Panel] dan pilih [System]



Gambar 6.14: Jendela Control Panel

- 3) Pada jendela [System Properties], klik pada tab [Remote]. Pastikan bahwa [Enable Remote Desktop] di komputer ini dicentang. Hal ini akan memungkinkan koneksi remote desktop dari komputer remote ke komputer ini.

**Catatan:** Anda dapat mengizinkan pengguna tertentu untuk terhubung ke server ini secara remote dengan mengklik pada **[Select Remote Users]**. Secara default, Administrator telah memiliki akses. Silahkan klik [OK] pada gambar di bawah ini



Gambar 6.15: Jendela System Properties pada tab Remote

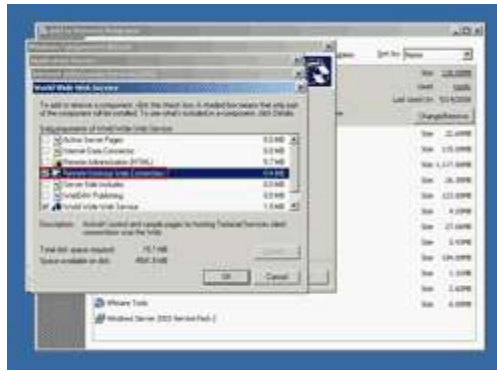
- 4) Selanjutnya kita akan menginstall Remote Desktop Web Connection. Bagian ini memerlukan CD Installer Windows XP yang anda gunakan pada komputer server (bukan versi windows yang lain).
- 5) Buka [Control Panel] dan pilih [Add or Remove Programs].
- 6) Klik pada [Add/Remove Windows Components] di kolom kiri jendela.



Gambar 6.16: Jendela Add or Remove Programs

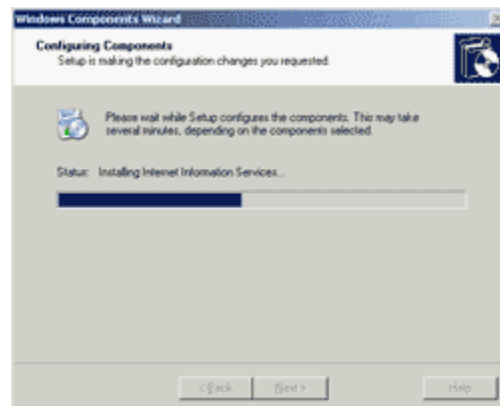
- 7) Pada Windows Components Wizard, klik-ganda pada Internet Information Services (IIS) > World Wide Web Service. Kemudian, beri centang [Remote Desktop Web Connection].  
**Catatan:** Anda akan melihat bahwa komponen lain yang dibutuhkan oleh alat ini diperiksa secara otomatis.





Gambar 6.17: Jendela Remote Desktop Web Connection

- 8) klik [OK] sampai anda kembali ke halaman pertama Windows Components Wizard, klik [Next] untuk menginstall komponen.

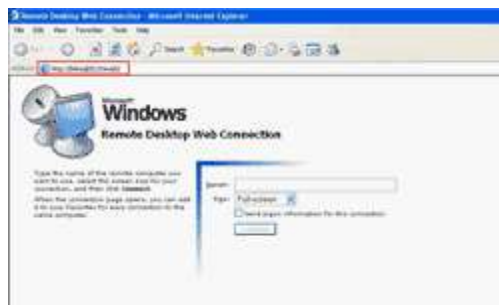


Gambar 6.18: Proses instalasi

- 9) Setelah proses diatas selesa, maka instalasi Remote Desktop Web Connection selesai

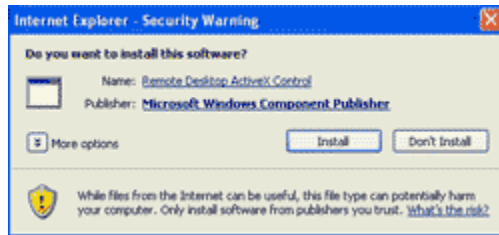
Tes Koneksi:

- 1) Masuk ke komputer klien, buka Internet Explorer dan tulis **"http://computername/tsweb"** dimana terdapat terminal [computername] dari nama komputer server



Gambar 6.19: Jendela remote desktop pada web browser

- 2) Proses ini mengharuskan Anda untuk menginstal Control Remote Desktop ActiveX. Klik [Install].



Gambar 6.20: konfirmasi instalasi

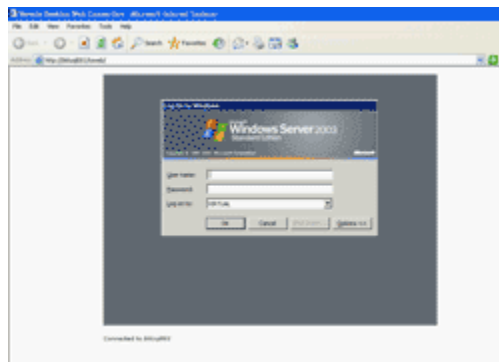
- 3) Sekarang coba koneksi ke komputer server, ubah resolusi sesuai kemauan anda dan klik [Connect].

**Note:** Anda tidak perlu menentukan nama server karena Anda baru saja terhubung ke komputer server (dalam URL).



Gambar 6.21: Tes koneksi melalui web browser

- 4) Anda akan melihat desktop komputer server dari jendela Internet Explorer.



Gambar 6.22: Pengisian data untuk koneksi



- 5) Anda dapat melakukan perintah apa saja sebagai Remote Desktop Connection.

127



Gambar 6.23: Hasil pada internet explorer

- 6) Proses tes selesai. Semoga berhasil.