BAB III

KEGIATAN SELAMA KERJA PRAKTEK

3.1 Jadwal Kerja Pratek

Kerja praktek di laksanakan dari tanggal 1 september sampai dengan 30 September 2004. Untuk mengetahui jadwal kerja praktek yang lebih terperinci dapat dilihat pada Lampiran.

3.2 Cara/Teknik Kerja Praktek

Proses pengumpulan data yang penyusun lakukan adalah sebagai berikut:

1. penelitian lapangan, kegiatan ini dilakukan dengan mengumpulkan data dengan cara membuat aplikasi tutorial, ini di lakukan selama melakukan kerja praktek.
2. Penelitian kepustakaan, kegiatan ini diakukan dengan membaca buku-buku yang ada hubungannya dengan masalah yang diteliti.
3. Wawancara, kegiatan ini dilakukan dengan cara diskusi dan wawancara orang yang dapat memberikan sumbangan pengetahuan terhadap penyusunan laporan kerja praktek ini.

3.3 Data Kerja Praktek

3.3.1 Definisi Jaringan

Jaringan komputer adalah sebuah kumpulan komputer, printer dan peralatan lainnya yang terhubung jadi satu kesatuan, sehingga

memungkinkan pengguna jaringan komputer dapat saling bertukar informasi dan data, dan bersama-sama menggunakan hardware/software yang terhubung dengan jaringan.

Komputer-komputer yang terhubung dalam suatu jaringan dapat berkomunikasi satu sama lain menggunakan sejumlah prosedur aturan yang disebut dengan protokol. Protokol tersebut mendefinisikan sintak (susunan, format, pola bit dan bytes) dan semantik (pengendalian sistem dan konteks informasi atau pengertian dari pola deretan bit dan byte) dari pertukaran data serta sejumlah karakteristik lain seperti laju data dan pewaktuan (timing).

3.3.2 Jenis Jaringan

Secara umum jaringan komputer dibagi atas lima jenis,yaitu:

1. Local Area Network (LAN)
2. Metropolitan Area Network (MAN)
3. Wide Area Network (WAN)
4. Internet
5. jaringan tanpa kabel

Jaringan yang dipakai diperusahaan tempat saya kerja praktek adalah Jaringan Local Area Network (LAN).

3.3.3 Mengenal Virus Komputer

3.3.3.1 Asal Muasal Virus

1949, John von Neumann, menggungkapkan " teori self altering automata " yang merupakan hasil riset dari para ahli matematika.1960, Lab BELL

(AT&T), para ahli di lab BELL (AT&T) mencoba-coba teori yang diungkapkan oleh John von Neumann, dengan membuat suatu jenis permainan/game. Mereka membuat program yang dapat memperbanyak dirinya dan dapat menghancurkan program buatan lawan. Program yang mampu bertahan dan menghancurkansemua program lain, akan dianggap sebagai pemenangnya. Permainan ini akhirnya menjadi permainan favorit di tiap-tiap lab komputer. Tetapi, semakin lama program yang diciptakan makin berbahaya, sehingga mereka melakukan pengawasan dan pengamanan yang ketat terhadap permainan ini. 1980, Program-Program tersebut yang akhirnya dikenal dengan sebutan "virus" ini berhasil menyebar keluar lingkungan laboratorium, dan mulai beredar di masyarakat umum.

3.3.3.2 Pengertian Virus

Virus komputer bisa diartikan sebagai suatu program komputer biasa. Tetapi memiliki perbedaan yang mendasar dengan program-program lainnya,yaitu virus dibuat untuk menulari program-program lainnya, mengubah, memanipulasinya bahkan sampai merusaknya. Ada yang perlu dicatat disini, virus hanya akan menulari apabila program pemicu atau program yang telah terinfeksi tadi dieksekusi, disinilah perbedaannya dengan "worm".

3.3.3.3 Kriteria Virus

Suatu program dapat disebut sebagai suatu virus apabila memenuhi minimal 5 kriteria berikut :

1. Kemampuan untuk mendapatkan informasi

2. Kemampuan untuk memeriksa suatu file
3. Kemampuan untuk menggandakan diri dan menularkan diri
4. Kemampuan melakukan manipulasi
5. Kemampuan untuk menyembunyikan diri.

Sekarang akan coba dijelaskan dengan singkat apa yang dimaksud dari tiap-tiap kemampuan itu dan mengapa ini sangat diperlukan.

1. Kemampuan untuk mendapatkan informasi

   Pada umumnya suatu virus memerlukan daftar nama-nama file yang ada dalam suatu directory. Untuk apa? Agar dia dapat memperoleh daftar file yang bisa dia tulari. Misalnya, virus makro yang akan menginfeksi semua file data MS Word, akan mencari daftar file berekstensi *.doc. Disinilah kemampuan mengumpulkan informasi itu diperlukan agar virus dapat membuat daftar/data semua file, lalu memilahnya dengan mencari file-file yang bisa ditulari. Biasanya data ini tercipta saat file yang tertular/terinfeksi virus atau file program virus itu sendiri dibuka oleh user. Sang virus akan segera melakukan pengumpulan data dan menaruhnya (biasanya) di RAM, sehingga

   apabila komputer dimatikan semua data hilang. Tetapi data-data ini akan tercipta kembali setiap kali virus itu diaktifkan. Biasanya data-data ini disimpan juga sebagai hidden file oleh virus tersebut.

2. Kemampuan memeriksa suatu program

Suatu virus juga harus bisa memeriksa suatu file yang akan ditulari, misalnya dia bertugas menulari program berekstensi *.doc, maka dia harus memeriksa apakah file dokumen tersebut telah terinfeksi ataupun belum, karena jika sudah, akan percuma menularinya lagi. Ini sangat berguna untuk meningkatkan kemampuan suatu virus dalam hal kecepatan menginfeksi suatu file/program. Yang umum dilakukan oleh virus adalah memiliki/memberi tanda pada file/program yang telah terinfeksi sehingga mudah untuk dikenali oleh virus tersebut. Contoh penandaan adalah misalnya memberikan suatu byte yang unik di setiap file yang telah terinfeksi.

3. Kemampuan untuk menggandakan diri

Inti dari virus adalah kemampuan menggandakan diri dengan cara menulari file lainnya. Suatu virus apabila telah menemukan calon korbannya maka ia akan mengenalinya dengan memeriksanya. Jika belum terinfeksi maka sang virus akan memulai aksinya, penularan dengan cara menuliskan byte pengenal pada file tersebut dan seterusnya mengcopikan/menulis kode objek virus diatas file sasaran. Beberapa cara umum yang dilakukan oleh virus untuk menulari/menggandakan dirinya adalah :

a. File yang akan ditulari dihapus atau diubah namanya. Kemudian diciptakan suatu file berisi program virus itu sendiri menggunakan nama file yang asli.

b. Program virus yang sudah dieksekusi/load ke memori akan langsung menulari file-file lain dengan cara menumpangi seluruh file yang ada.

4. Kemampuan mengadakan manipulasi

Rutin (routine) yang dimiliki suatu virus akan dijalankan setelah virus menulari suatu file. Isi dari suatu rutin ini dapat beragam mulai dari yang tidak berbahaya sampai yang melakukan perusakan. Rutin ini umumnya digunakan untuk memanipulasi file atau pun mempopulerkan pembuatnya ! Rutin ini memanfaatkan kemampuan dari suatu sistem operasi (Operating System), sehingga memiliki kemampuan yang sama dengan yang dimiliki sistem operasi. Misal :

a. Membuat gambar atau pesan pada monitor
b. Mengganti/mengubah-ubah label dari tiap file, direktori, atau label dari drive di PC
c. Memanipulasi file yang ditulari
d. Merusak file
e. Mengacaukan kerja printer, dan sebagainya.

5. Kemampuan Menyembunyikan diri

Kemampuan menyembunyikan diri ini harus dimiliki oleh suatu virus agar semua pekerjaan baik dari awalsampai berhasilnya penularan dapat terlaksana.

Langkah langkah yang biasa dilakukan adalah:



- Program virus disimpan dalam bentuk kode mesin dan digabung dengan program lain yang dianggap berguna oleh pemakai
- Program virus diletakkan pada Boot Record atau track pada disk yang jarang diperhatikan oleh komputer itu sendiri
- Program virus dibuat sependek mungkin, dan hasil file yang diinfeksi tidak terlalu berubah ukurannya
- Virus tidak mengubah keterangan/informasi waktu suatu file
- dll

3.3.4 Manajemen Antivirus dalam Jaringan

Banyak para pengguna komputer yang tidak mengetahui apa perbedaan mendasar antara antivirus untuk komputer satuan (standalone) dengan antivirus untuk jaringan dan menganggap bahwa penanganan antivirus dalam jaringan sama dengan antivirus untuk komputer standalone. Hal ini sama saja dengan membandingkan antara mini compo dengan tape mobil. Jika kita diberi hadiah mini compo, pada umumnya kita akan dengan mudah dapat mengoperasikan mini compo tersebut karena tinggal colok dan semua sistem sudah terpasang. Tetapi lain halnya jika kita diberi satu set tape mobil, dimana seluruh sistem belum terpasang dan harus dipasang oleh instalatir yang berpengalaman. Kalau dicoba-coba untuk memasang sendiri, tanpa pengalaman yang cukup kemungkinan besar tape mobil tidak akan terpasang dengan baik. Kecuali kita memaksa menggunakan mini compo di mobil, yang pada akhirnya malah menimbulkan masalah

baru karena mini compo memang tidak dirancang untuk digunakan sebagai tape mobil.

PT. Vaksincom menyadari benar akan hal ini dan tulisan ini memberikan gambaran yang cukup lengkap mengenai penanganan virus di dalam jaringan komputer menggunakan Norman Virus Control. Seluruh pelanggan PT. Vaksincom selain mendapatkan program antivirus yang sesuai dengan kebutuhannya, juga mendapatkan :

1. Instalasi antivirus dalam jaringan dimana seluruh komputer akan melakukan update definisi antivirus secara otomatis tanpa memerlukan keterlibatan user. Jadi user tinggal menyalakan komputer saja dan bekerja, sedangkan Norman Virus Control akan secara otomatis mengupdate dirinya setiap hari ke server lokal.
2. Pembersihan Virus, setiap komputer yang di instal antivirus akan dikunjungi secara langsung oleh teknisi PT. Vaksincom sehingga menjamin jalannya program antivirus di jaringan dan pembasmian virus yang ada di setiap komputer dalam jaringan.
3. Support FULL dari teknisi PT. Vaksincom tanpa ada biaya tambahan per kunjungan. Dengan adanya dukungan dari teknisi PT. Vaksincom bagian IT / EDP dapat mengkonsentrasikan dirinya pada tugasnya dan menyerahkan semua penanganan virus pada pihak yang berkompeten. Perusahaan anda seperti mendapatkan tambahan IT baru yang ahli dalam masalah virus tanpa mengeluarkan biaya tambahan.
4. Update Patch Gratis dilakukan oleh teknisi PT. Vaksincom. Setiap

pelanggan PT. Vaksincom mendapatkan fasilitas update patch dan service pack gratis. Hal ini sangat membantu karena terbukti bahwa > 80 % virus yang mengganas sekarang memanfaatkan celah keamanan dan memerlukan satu usaha khusus dan konsisten agar jaringan komputer perusahaan dapat terupdate pada waktu yang tepat sebelum mengalami serangan virus.

Sulitnya menginstall sebuah antivirus di dalam perusahaan dalam jumlah yang cukup besar,merupakan suatu masalah yang harus di hadapi pada saat ini. Dan bagaimana kita dapat mengawasi para pengguna komputer, apakah mereka telah mengupdate database virus mereka, apakah mereka terkena virus. Kalau kita mengandalkan diri kita sendiri tentunya akan membuang-buang waktu, hanya untuk mengawasi para client dalam menjaga komputernya dari serangan virus. Kita harus mengunjungi dan melihat satu persatu komputer client, yang sebenarnya ada cara yang lebih mudah dalam mengatasi hal ini.

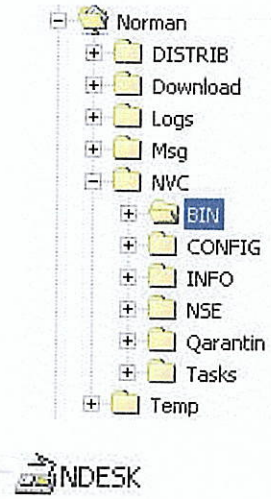
Kalau dengan cara menginstall program antivirus mungkin tidak semua fasilitas yang diharapkan dapat terpenuhi. Kita harus mengisi ulang semua konfigurasi yang dibutuhkan oleh client. Yang parahnya, setelah meninggalkan komputer tersebut, client dapat merubah konfigurasi antivirus tersebut, dan yang pasti tidak menyadari kalau hal tersebut telah terjadi.

Jadi harus ada sebuah solusi yang praktis, murah dan tidak perlu

membuang-buang waktu dalam menghadapi hal-hal demikian.

Norman Virus Control telah memberikan kemudahan-kemudahan yang cukup berarti dalam penginstallan antivirus di dalam sebuah jaringan komputer yang besar. Kita hanya menginstall **Norman Virus Control** di dalam sebuah komputer yang akan menjadi sebuah server antivirus. Kita hanya melakukan beberapa konfigurasi untuk digunakan di komputer client yang ada di perusahaan. Dan setelah itu, dari komputer client kita cukup menekan 2 buah file saja yang ada di komputer server antivirus. Kemudian kita dapat meninggalkan komputer client kita tersebut, dan install ditempat yang lain. Seluruh konfigurasi yang telah dibuat di server antivirus, akan sama di semua komputer client. Ini akan cukup berarti bagi para administrator komputer, karena mereka tidak hanya mengurusi virus komputer saja, tetapi masih banyak lagi pekerjaan-pekerjaan lainnya yang telah menanti.

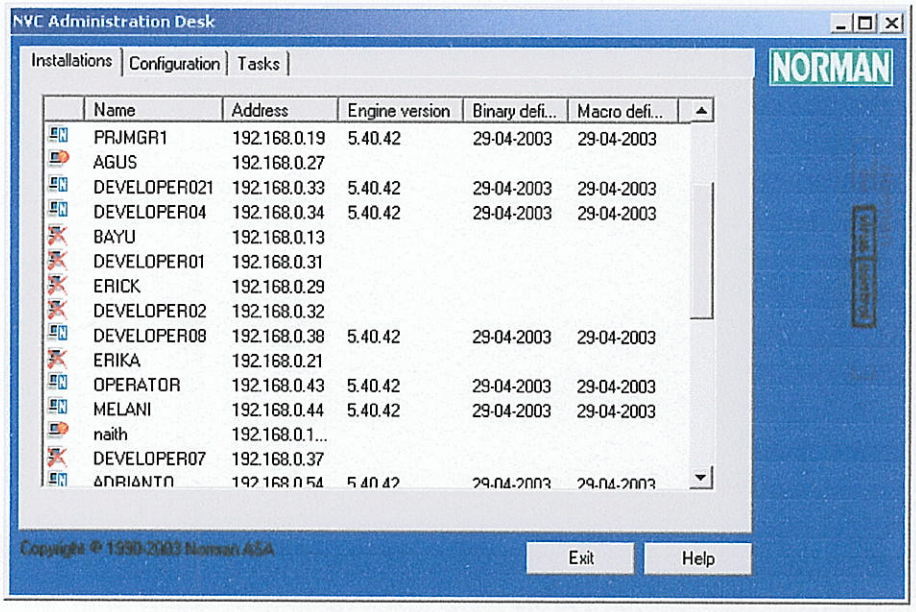
Dengan beberapa kemudahan itu, waktu yang dibutuhkan hanya sedikit. Dan **Norman Virus Control** akan membuat kita menjadi seorang administrator yang handal, sebab dengan hanya menjalankan sebuah program yang bernama NDESK(terdapat di ...\\Norman\NVC\BIN\NDESK.EXE), kita sudah dapat memantau seluruh aktifitas client di perusahaan.



Gambar III.1 Program NDESK

Ada beberapa kelebihan dari tools NDESK ini yaitu :

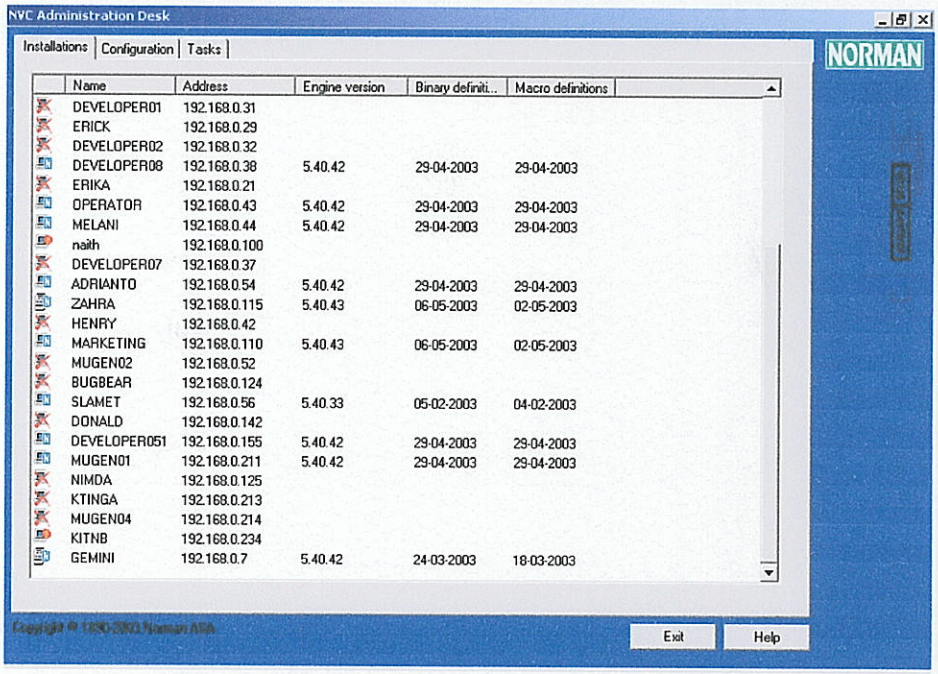
1. Mengetahui komputer mana yang sudah terinstall antivirus **Norman Virus Control** dan yang belum. Pada gambar di bawah ini, bisa melihat ada beberapa komputer yang belum dan yang sudah terinstall antivirus **Norman Virus Control**.



Gambar III.2 installasi Norman Virus Control

2. Mengetahui komputer mana yang sudah terupdate dan yang belum.

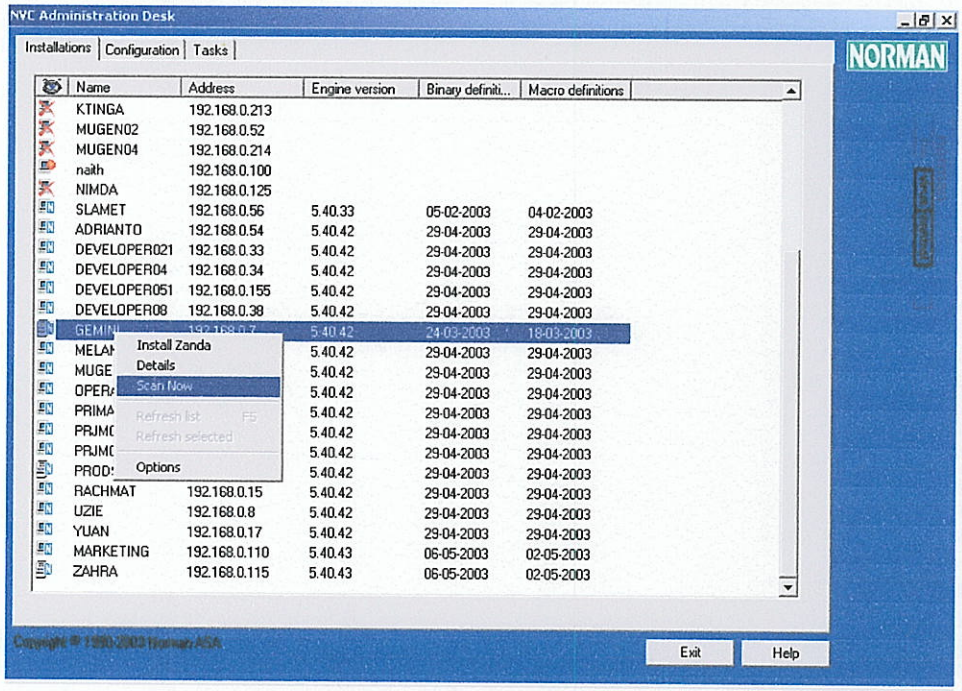
   Pada gambar di bawah ini



Gambar III.3 Update virus definition file

Keterangan :

Ternyata ada beberapa komputer yang belum terupdate *virus definition file*-nya. Kejadian ini mungkin dapat disebabkan, hubungan antara server dan client terganggu. Kalau client anda menggunakan Windows 9x/ME hal ini dapat diatasi dengan cara :



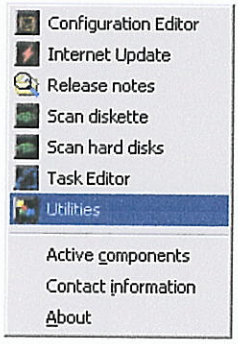
Gambar III.4 Scan Virus

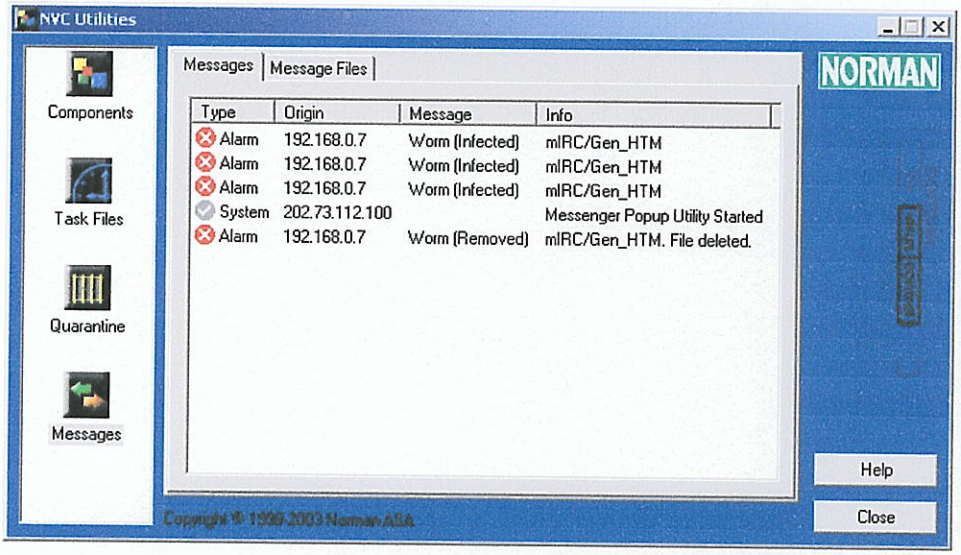
Anda klik kanan pada nama client yang bermasalah, pada menu propertis anda klik 'Scan Now'. Opsi ini sebenarnya akan melakukan pemeriksaan di komputer client tersebut melalui server antivirus. Tetapi oleh **Norman Virus Control** telah disempurnakan, sehingga bukan hanya memeriksa apakah pada komputer tersebut ada virusnya atau tidak, tetapi ia memeriksa juga *virus definition file, engine* dari program antivirus yang

ada di client. Kalau ternyata ada perbedaan dengan yang di server antivirus, maka langsung akan diperbaharui.

3. Melakukan pemeriksaan komputer client dari komputer server antivirus.

Kita bisa melalukannya seperti petunjuk di atas, komputer server dapat melakukan pemeriksaan virus dan hasilnya dapat lihat di NVC Utilities.





Gambar III.5 NVC Utilities

Keterangan :

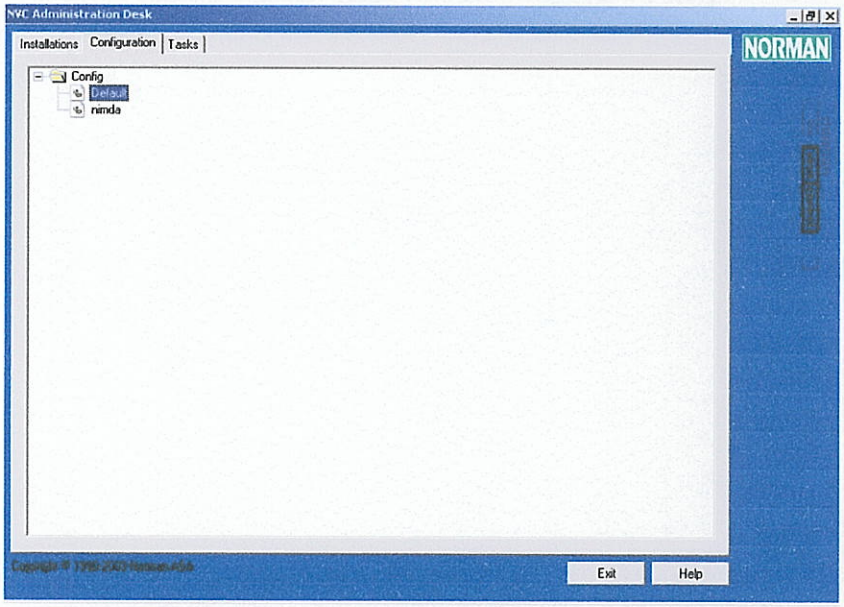
Kita dapat melakukan dengan cara, mengklik icon **Norman Virus**

Control yang terletak pada taskbar sebelah kanan bawah 

. Dengan cara seperti ini para administrator dapat mengetahui bahwa pada komputer dengan IP address sekian ternyata ada virus. Pembersihan dilakukan di komputer yang bersangkutan, dan setelah bersih dari virus akan diberikan lagi pemberitahuan bahwa IP address tersebut telah clean.

4. Membuat Konfigurasi untuk Client.

   Norman Virus Control melalui NDESK, dapat melakukan konfigurasi dari server antivirus yang baru. Dengan cara ini setiap opsi-opsi atau konfigurasi yang anda perbaharui dapat langsung mengganti konfigurasi yang lama pada komputer client.



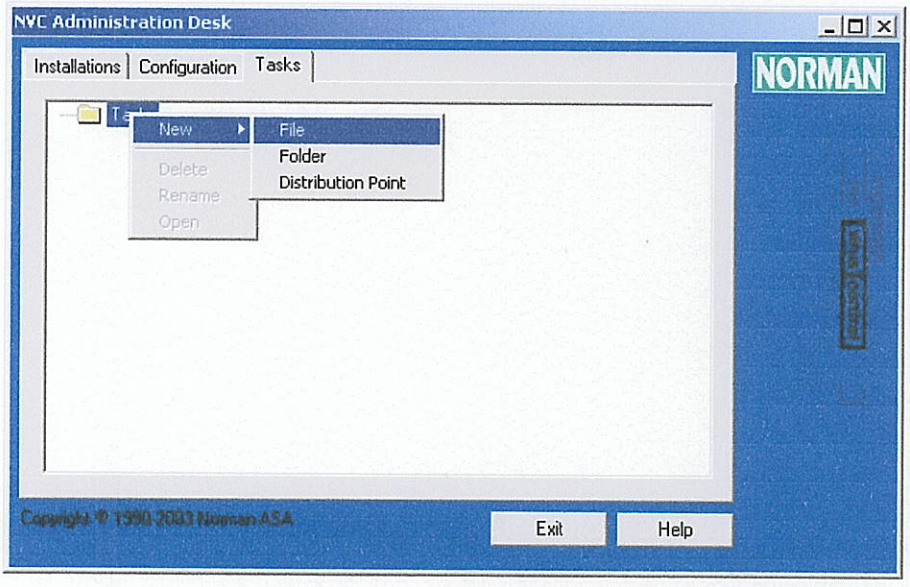
Gambar III.6 Konfigurasi Client

Setelah masuk ke dalam konfigurasi ini, lalu klik kata "default" kemudian akan tampil menu-menu konfigurasi. Kita dapat menambahkan atau mengurangi opsi-opsi yang akan atau telah di pilih.

Setelah selesai melakukan perubahan, simpan terlebih dahulu kemudian tutup. Kemudian untuk setiap komputer client akan segera merubah konfigurasinya sesuai dengan komputer antivirus server.

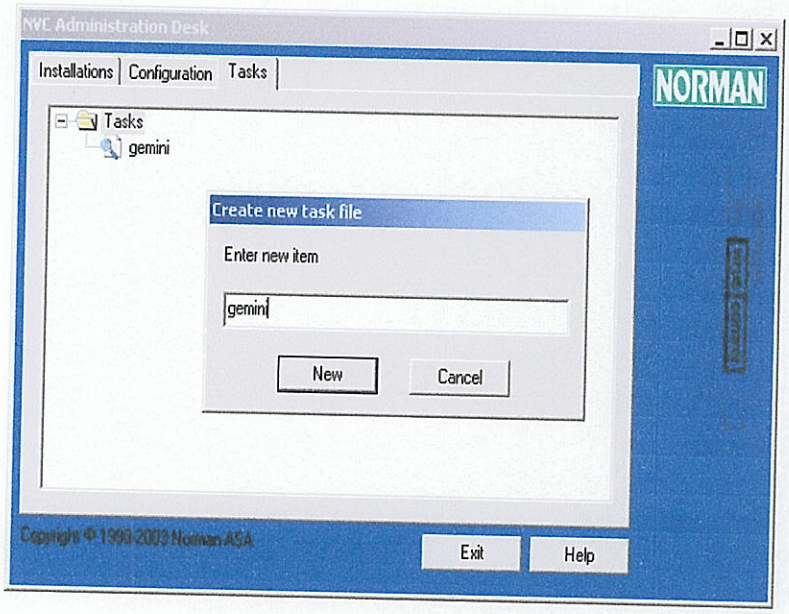
5. Membuat Schedule Task

Dengan cara membuat Schedule Task, kita dapat memerintahkan komputer client untuk memeriksa target pemeriksaan (Harddisk, floppy disk, memori, boot sector, file-file terkompresi, subfolder), dan jadwal pemeriksaan. Opsi ini dapat di lakukan melalui NDESK, klik tab TASK, kemudian klik kanan pada kata TASK, akan muncul pilihan dan klik New, lalu File.



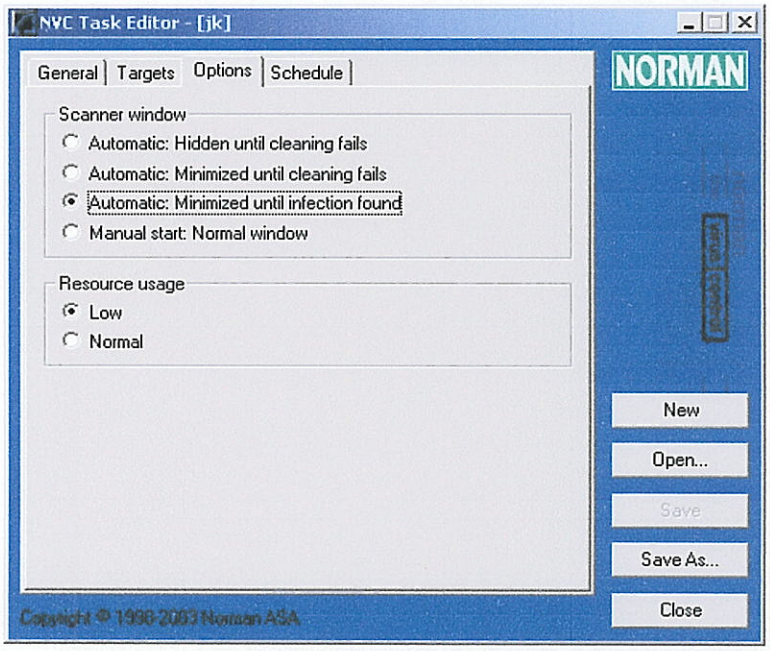
Gambar III.7 Schedule Task

Masukan sembarang nama untuk file task yang baru. Kemudian klik tombol yang bertuliskan kata NEW.

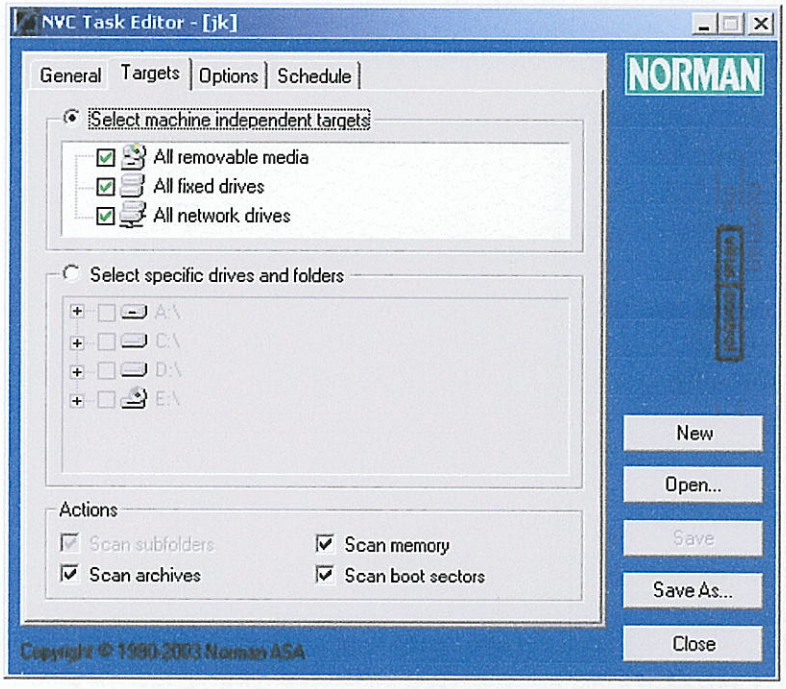


Gambar III.8 Mengganti File Task

Setelah itu akan diberikan pilihan-pilihan untuk target dan waktu pemeriksaan komputer anda secara automatis.



Gambar III.9 Options Task Editor



Gambar III.10 Target Task Editor

6. Mengetahui Status Komputer Client.

Dengan menggunakan NDESK, kita bisa melihat status dari komputer client kita. Jika kita melihat pada gambar-gambar yang terdahulu, ada berbagai macam icon-icon yang tampak. Icon-icon tersebut mewakili status dari client-client anda.

Tabel 1. Icon-icon

Gambar Icon	Keterangan
	Komputer tersebut telah diistall NVC dan dapat di ketahui up-date terakhir, versi berapa, binari dan macro virus yang ada di komputer tersebut (komputer server)
	Komputer tersebut telah diistall NVC dan dapat di ketahui up-date terakhir, versi berapa, binari dan macro virus yang ada di komputer tersebut (Komputer Workstation/Client)
	Komputer Workstation telah terinstall NVC , tapi dilaporkan ada satu atau beberapa kompunen yang mengalami masalah.
	Komputer server telah terinstall NVC, tapi dilaporkan ada satu atau beberapa kompunen yang mengalami masalah
	Komputer Workstation telah terupdate tapi masih menunggu proses restart
	Komputer Server telah terupdate tapi masih menunggu proses restart

Dengan adanya kemudahan-kemudahan ini, para administrator akan berkurang kegiatannya dalam masalah penanggulangan virus, semua telah diambil alih oleh server antivirus sendiri.


UNIVERSITAS KOMPUTER INDONESIA
UNIKOM