TUGAS UAS

KEAMANAN INFORMASI

Riza Anis Istifadah

1310651103

D

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH JEMBER

2014/2015

TUGAS 1

Keamanan Operasi berkaitan dengan ancaman terhadap lingkungan operasi produksi. Agen ancaman bisa menjadi aktor internal atau eksternal, dan keamanan operasi harus memperhitungkan untuk kedua sumber ancaman tersebut agar efektif. Operasi keamanan adalah tentang orang, data, media, perangkat keras, dan ancaman yang terkait dengan masing-masing di produksi lingkungan Hidup.

Pengamanan perangkat lunak cenderung memfokuskan pada pengamanan system operasi, karena perangkat lunak aplikasi juga memberi resiko keamanan.Keamanan sistem operasi merupakan bagian masalah keamanan sistem komputer secara total. Pengamanan sistem operasi berarti kecil jika setiap orang dapat melenggang di ruang sistem komputer. Pengamanan secara fisik dengan membatasi pengaksesan fisik secara langsung dengan fasilitas sistem computer harus dilakukan juga. Keamanan sistem komputer adalah untuk menjamin sumber daya tidak digunakan atau dimodifikasi orang tak terotorisasi. Pengamanan termasuk masalah teknis, manajerial, legalitas dan politis.

Keamanan sistem terbagi menjadi tiga, yaitu :

1. Keamanan eksternal (external security).
   Berkaitan dengan pengamanan fasilitas komputer dari penyusup (hacker) dan bencana seperti kebakaran dan kebanjiran.
2. Keamanan interface pemakai (user interface security).
   Berkaitan dengan identifikasi pemakai sebelum pemakai diijinkan mengakses program dan data yang disimpan.
3. Keamanan internal (internal security).
   Berkaitan dengan pengamanan beragam kendali yang dibangun pada perangkat keras dan sistem operasi yang menjamin operasi yang handal dan tak terkorupsi untuk menjaga integritas program dan data.

Istilah keamanan (security) dan proteksi (protection) sering digunakan secara bergantian. Untuk menghindari kesalahpahaman, istilah keamanan mengacu ke seluruh masalah keamanan dan istilah mekanisme proteksi mengacu ke mekanisme sistem yang digunakan untuk memproteksi/melindungi informasi pada sistem komputer.

Ancaman-ancaman keamanan

Sasaran pengamanan adalah menghindari, mencegah dan mengatasi ancaman terhadap sistem. Kebutuhan keamanan sistem komputer dikategorikan tiga aspek, yaitu :

1. Kerahasiaan (secrecy) adalah keterjaminan bahwa informasi disistem komputer hanya dapat diakses oleh pihak-pihak yang diotorisasi dan modifikasi tetap menjaga konsistensi dan keutuhan data di sistem.
2. Integritas (integrity) adalah keterjaminan bahwa sumber daya sistem komputer hanya dapat dimodifikasi oleh pihak-pihak yang diotorisasi.
3. Ketersediaan (availability) adalah keterjaminan bahwa susmber daya sistem komputer tersedia bagi pihak-pihak yang diotorisasi saat diperlukan.

Petunjuk Pengamanan Sistem

Terdapat beberapa prinsip pengamanan sistem komputer, yaitu :

1. Rancangan sistem seharusnya publik.
   Keamanan sistem seharusnya tidak bergantung pada kerahasiaan rancangan mekanisme pengamanan. Mengasumsikan penyusup tidak akan mengetahui cara kerja sistem pengamanan hanya menipu/memperdaya perancang sehingga tidak membuat mekanisme proteksi yang bagus.
2. Dapat diterima.
   Skema yang dipilih harus dapat diterima secara psikologis. Mekanisme proteksi seharusnya tidak menganggu kerja pemakai dan memenuhi kebutuhan otorisasi pengaksesan. Jika mekanisme tidak mudah digunakan maka tidak akan digunakan atau digunakan secara tak benar.
3. Pemeriksaan otoritas saat itu.
   Sistem tidak seharusnya memeriksa ijin dan menyatakan pengaksesan diijinkan, serta kemudian menetapkan terus informasi ini untuk penggunaan selanjutnya. Banyak sistem memeriksa ijin ketika file dibuka dan setelah itu (operasi-operasi lain) tidak diperiksa. Pemakai yang membuka file dan lupa menutup file akan terus dapat walaupun pemilik file telah mengubah atribut proteksi file.
4. Kewenangan serendah mungkin.
   Program atau pemakai sistem seharusnya beroperasi dengan kumpulan wewenang serendah mungkin yang diperlukan untuk menyelesaikantugasnya. Default sistem yang digunakan harus tak ada akses sama sekali.
5. Mekanisme yang ekonomis.
   Mekanisme proteksi seharusnya sekecil, sesederhana mungkin dan seragam sehingga memudahkan verifikasi. Proteksi seharusnya dibangun dilapisan terbawah. Proteksi merupakan bagian integral rancangan sistem, bukan mekanisme yang ditambahkan pada rancangan yang telah ada.

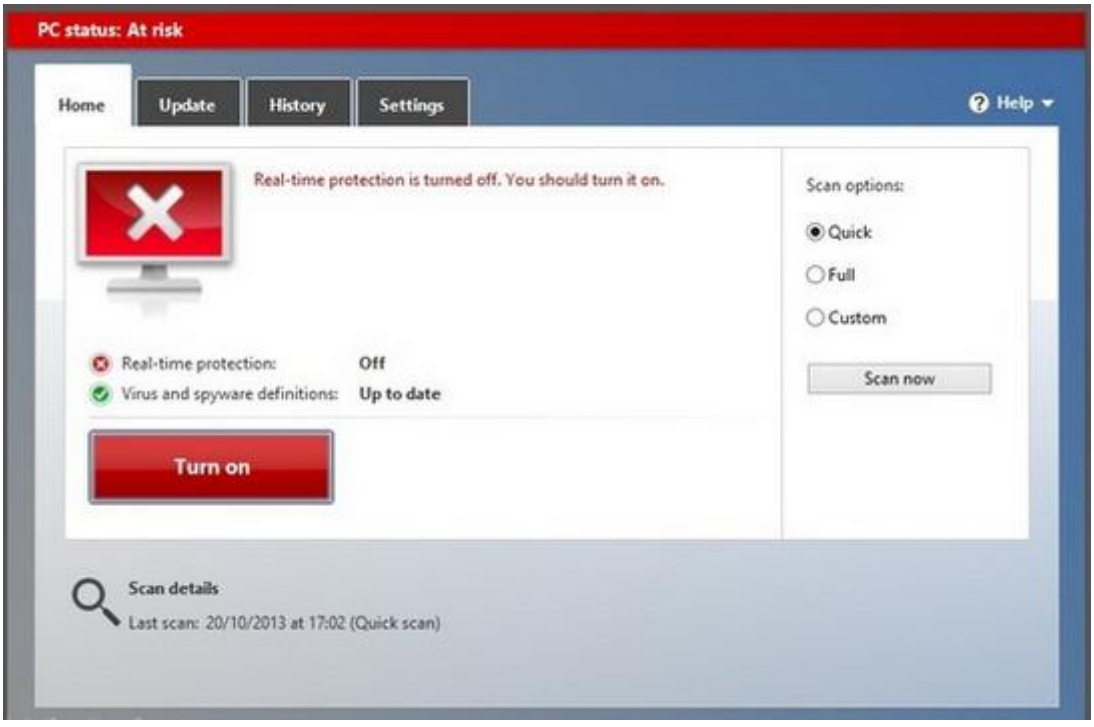
TUGAS 2

Cara Mengaktifkan Windows Defender di Windows 8

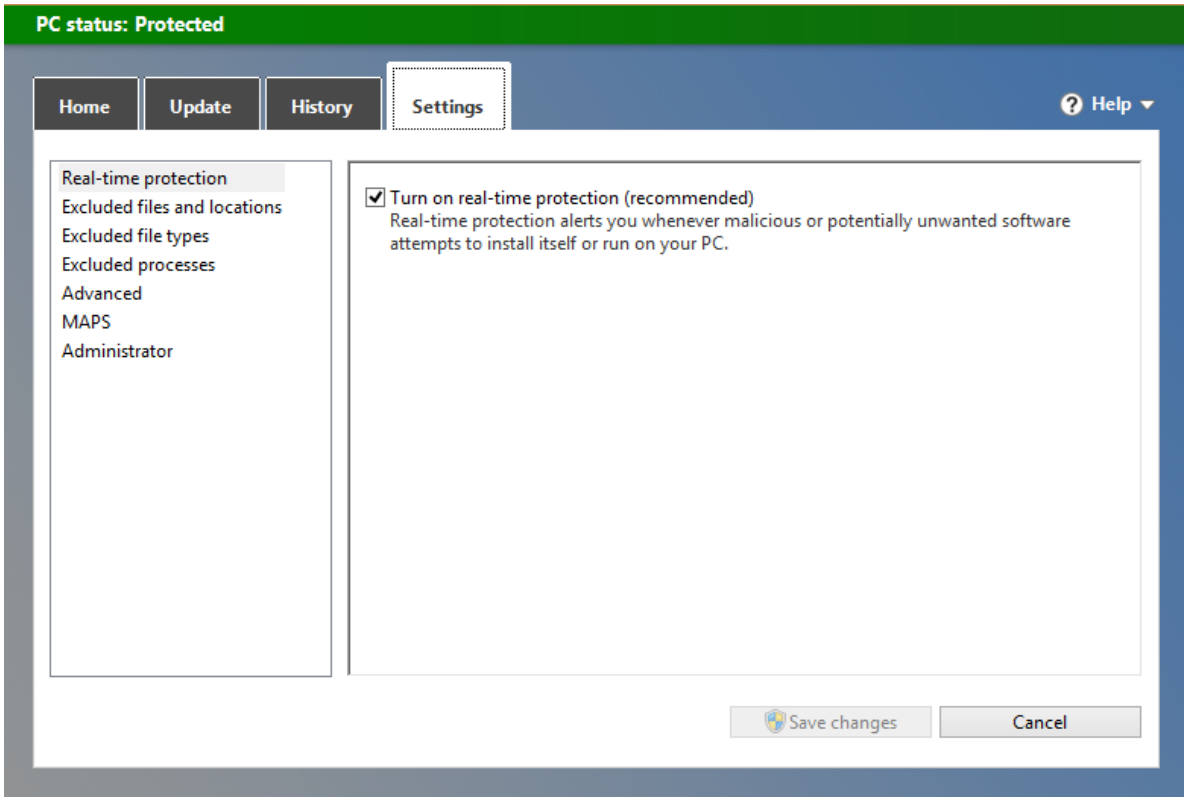
Widows Defender adalah perangkat lunak dari Microsoft untuk melindungi sistem operasi Microsoft Windows dari perangkat pengintai (*spyware*). Windows Defender memiliki fitur dengan kemampuan perangkat anti-pengintaian (*antispyware*). Windows Defender meliputi sejumlah real-time security agents yang mengawasi beberapa area umum pada Windows yang mengalami perubahan-perubahan yang mungkin disebabkan oleh *spyware*. Perangkat ini juga menyertakan kemampuan untuk menghapus secara mudah perangkat ActiveX yang terpasang. Windows Defender juga terintegrasi dengan Microsoft SpyNet, sehingga para pengguna dapat melaporkan kepada Microsoft mengenai kemungkinan-kemungkinan *spyware*, serta aplikasi dan pemacu peranti (*device drivers*) yang dimungkinkan untuk dipasang pada sistem mereka.

Pertama-tama buka Start Screen dan ketikkan Windows Defender.

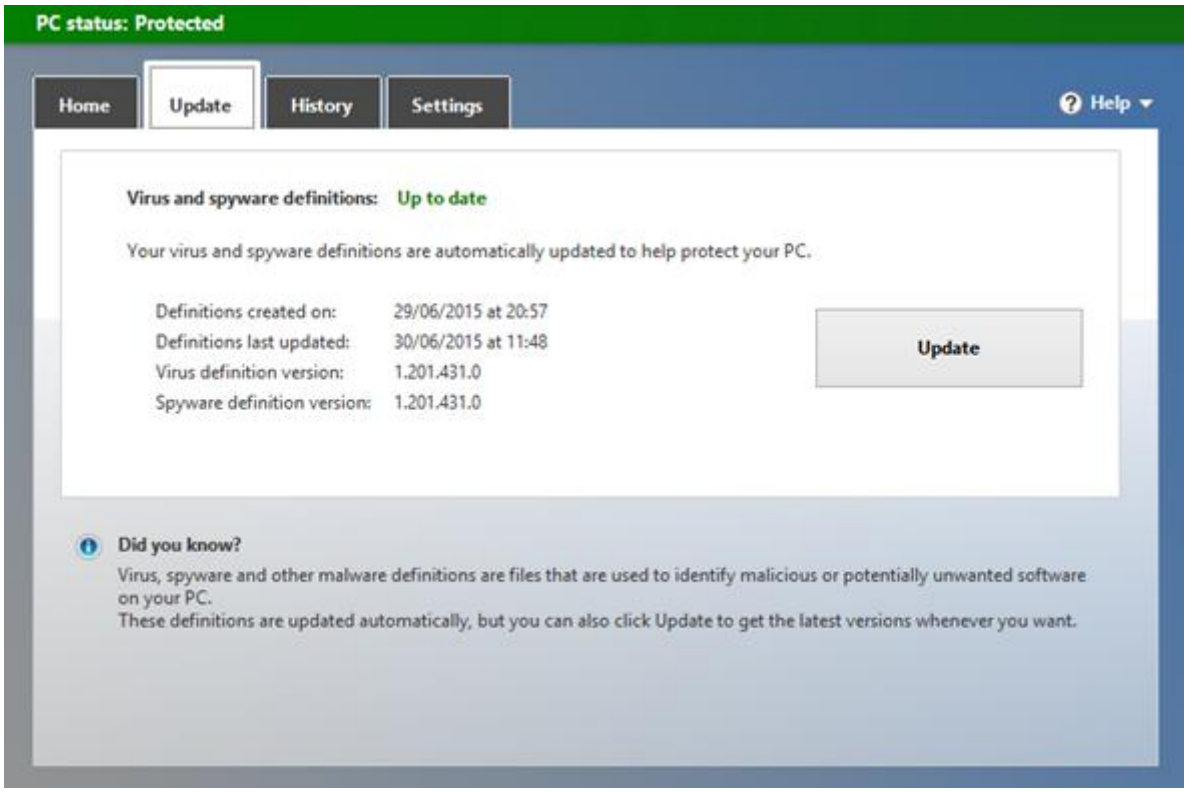
Setelah itu buka aplikasi Windows Defender, ketika window Windows Defender terbuka dan Real-time protection Off maka Windows Defender mati.



Untuk mengaktifkan klik tab Settings dan centang menu Real time protection dan klik Save Changes. Setelah Windows Defender aktif akan berubah menjadi warna hijau.



Lalu lakukan update Windows Defender untuk memperkuat keamanan dari virus dan spyware, caranya klik tab Update dan klik tombol Update.



Terakhir agar Windows 8 aman dari virus lakukan scan, caranya klik tab Home dan pilih Full pada scan options. Terakhir klik Scan now untuk memulai scan virus dan spyware di komputer .