WINDOWS KURULUMUNDA GÜVENLİK AYARLARI

BİLGİ İŞLEM DAİRE BAŞKANLIĞI

Hazırlayanlar:

Ahmet YURDAKUL

Ulaş CANATALI

WINDOWS KURULURKEN

KURULUMA BAŞLAMADAN ÖNCE AĞ KABLOSUNUN TAKILI OLMAMASI GEREKİR

WINDOWS KURULURKEN DOSYA SİSTEMİ NTFS SEÇİLMELİ

- Güvenliği büyük ölçüde artıran dosya şifrelemesi.
- Yalnızca klasörlere değil, tekil dosyalara da uygulanabilen izinler.
- Sistem sorunları yaşanması durumunda NTFS'nin bilgileri hızla geri yüklemesine yardımcı olan, disk etkinlikleri kurtarma günlüğü.
- Bireysel kullanıcıların kullandığı disk alanı miktarını izleyip sınırlama koymanıza olanak veren disk kotaları.

GÜVENLİ ŞİFRELER OLUŞTURULMALI

- Sekiz karakterden uzun olmalıdır.
- Harfler, sayılar ve simgelerden oluşmalıdır.
- Ardışık veya yinelenen birleşimler olmamalı ("12345678," "222222," "abcdefg" gibi).
- Oturum açma adınız, eşinizin adı veya doğum gününüz gibi şeyler olmamalıdır.
- Herhangi bir dil için sözlükte bulunan sözcükler olmamalıdır.

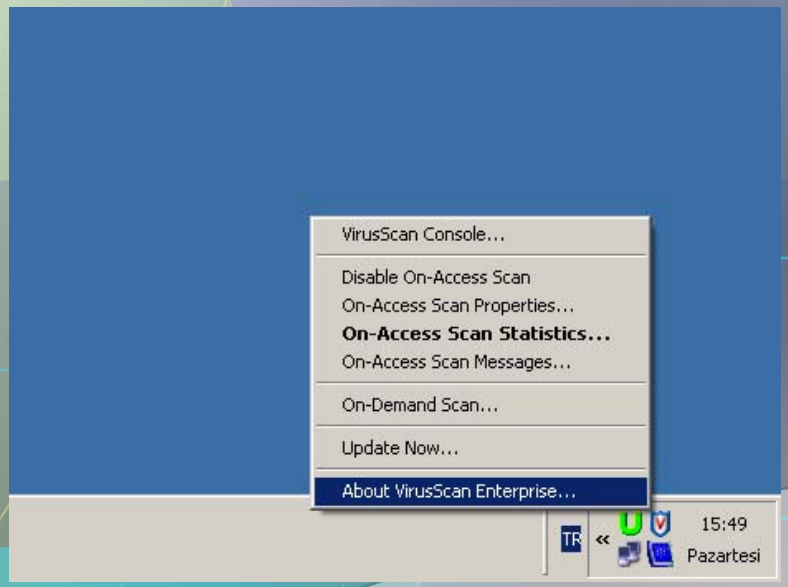
WINDOWS KURULDUKTAN SONRA

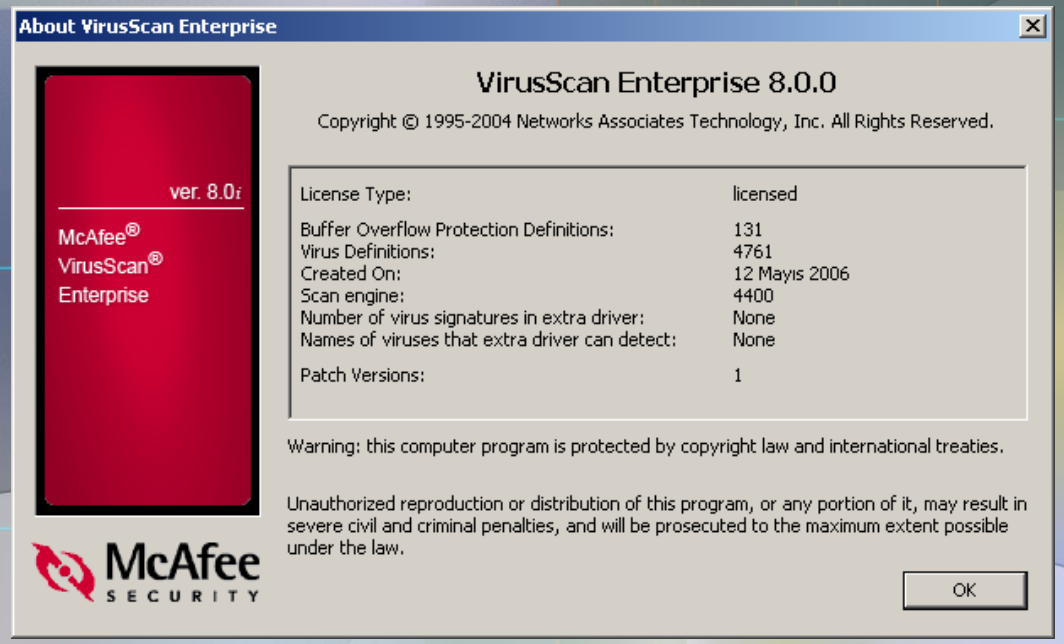
WINDOWS GÜNCELLEMELERİNİ INTERNET'e BAĞLANMADAN BIDB'den TEMİN EDİLEBİLEN GÜVENLİK CD'den YAPMAK MÜMKÜN

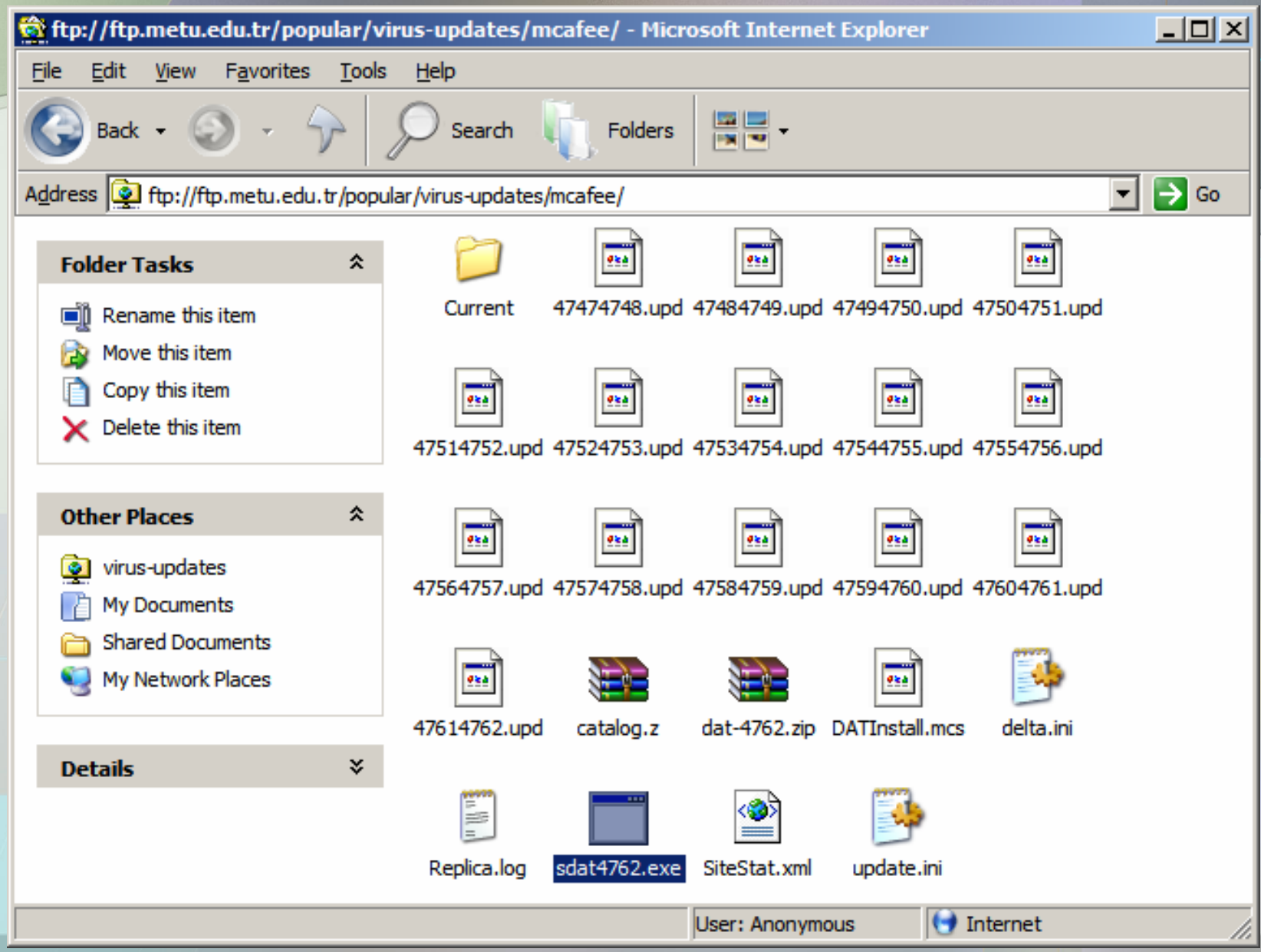
ANTİVİRÜS YAZILIMI KURULUR, AYARLARI VE GÜNCELLEMELERİ YAPILIR

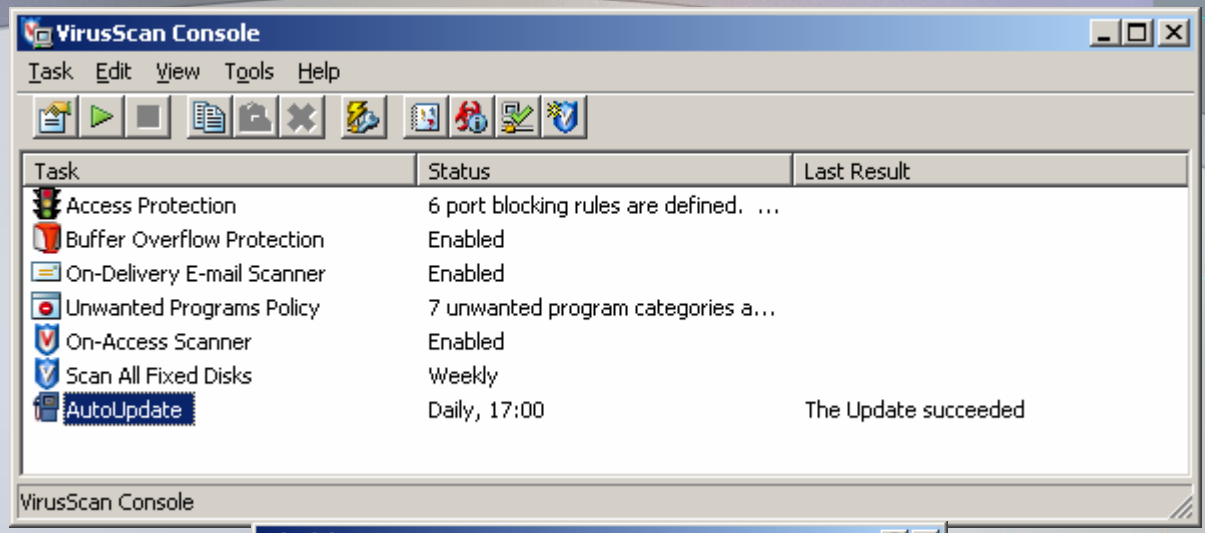
-McAfee-

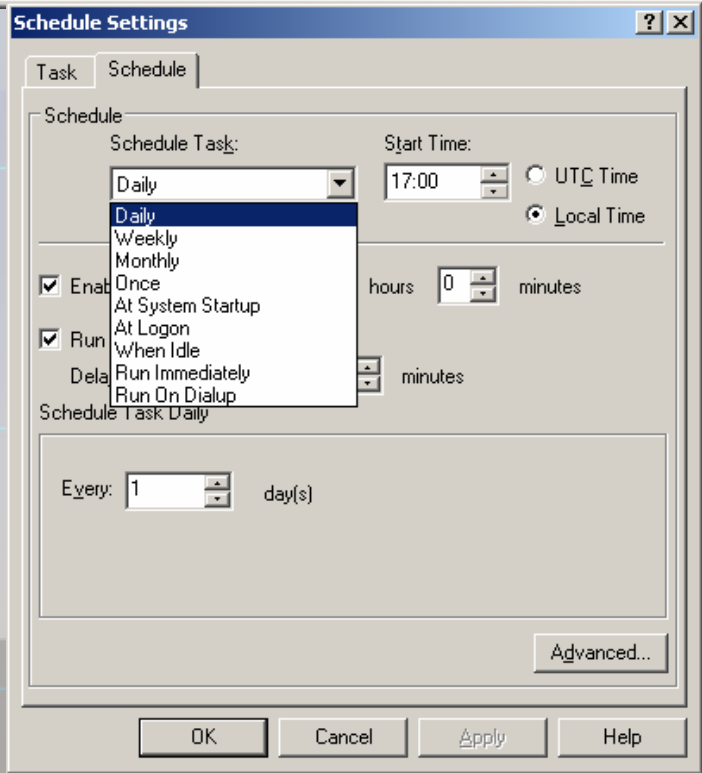
ftp://ftp.metu.edu.tr/popular/virus-updates/mcafee/

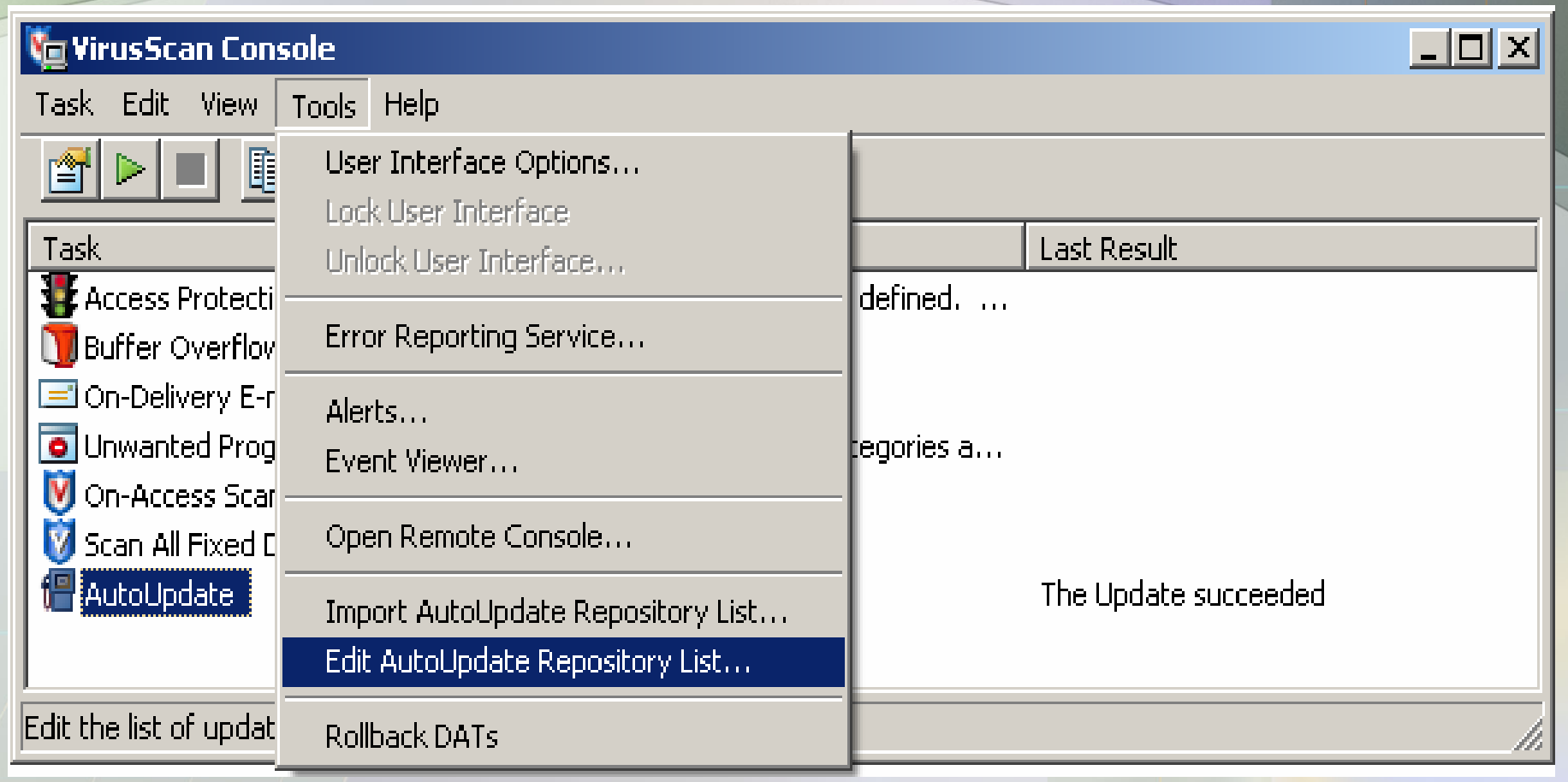


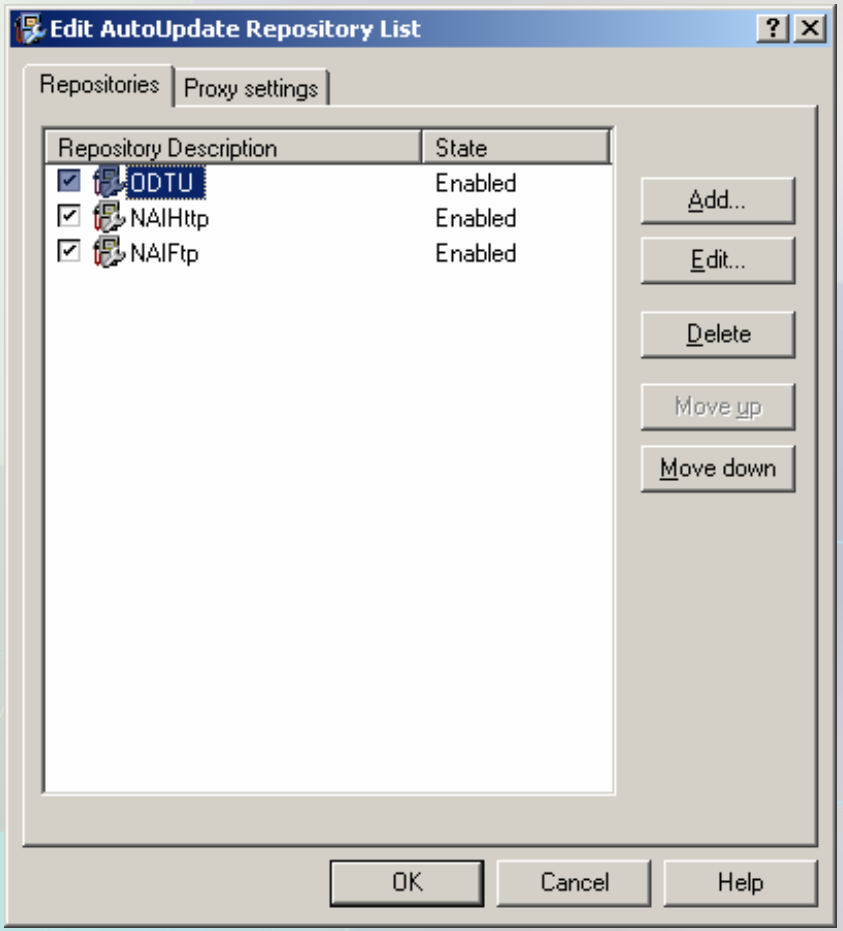


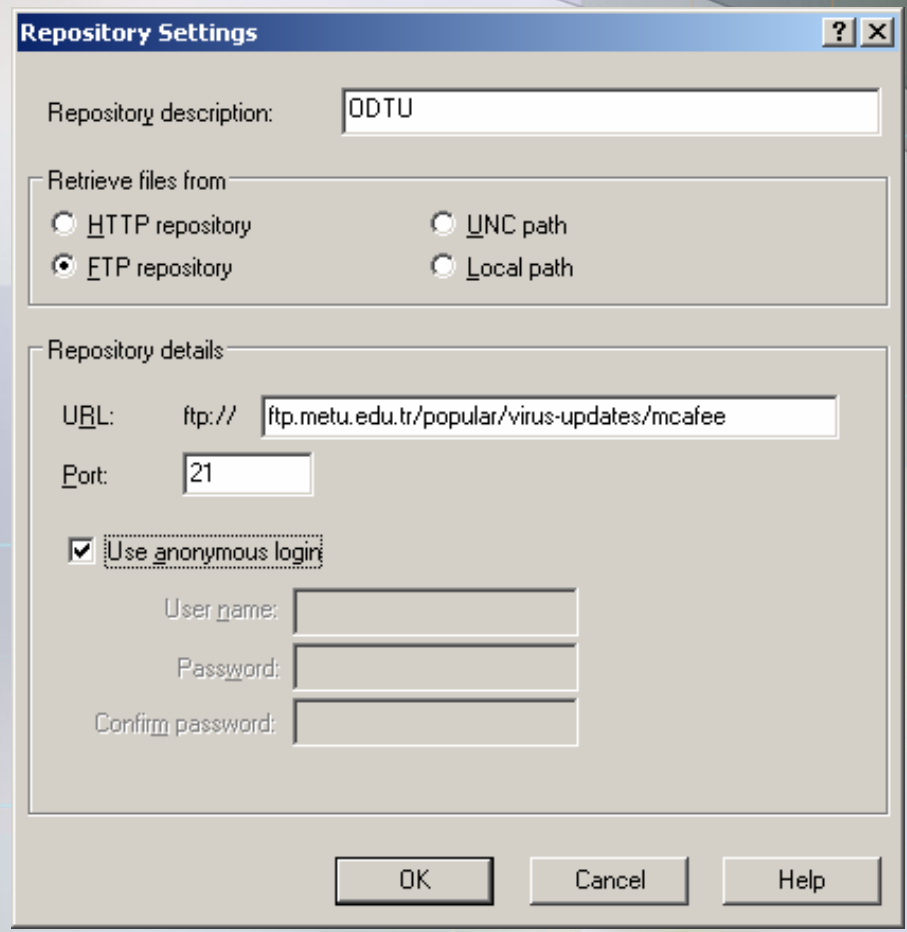

ftp://ftp.metu.edu.tr/popular/virus-updates/mcafee/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Folders
Address
ftp://ftp.metu.edu.tr/popular/virus-updates/mcafee/
Go
Folder Tasks
Rename this item
Move this item
Copy this item
Delete this item
Other Places
virus-updates
My Documents
Shared Documents
My Network Places
Details
Current
47474748.upd
47484749.upd
47494750.upd
47504751.upd
47514752.upd
47524753.upd
47534754.upd
47544755.upd
47554756.upd
47564757.upd
47574758.upd
47584759.upd
47594760.upd
47604761.upd
47614762.upd
catalog.z
dat-4762.zip
DATInstall.mcs
delta.ini
Replica.log
sdat4762.exe
SiteStat.xml
update.ini
User: Anonymous
Internet


VirusScan Console
Task Edit View Tools Help
Task
Status
Last Result
Access Protection
6 port blocking rules are defined. ...
Buffer Overflow Protection
Enabled
On-Delivery E-mail Scanner
Enabled
Unwanted Programs Policy
7 unwanted program categories a...
On-Access Scanner
Enabled
Scan All Fixed Disks
Weekly
AutoUpdate
Daily, 17:00
The Update succeeded
VirusScan Console


Schedule Settings
Task
Schedule
Schedule
Schedule Task:
Start Time:
Daily
17:00
UTC Time
Local Time
Daily
Weekly
Monthly
Once
At System Startup
At Logon
When Idle
Run Immediately
Run On Dialup
hours
0
minutes
minutes
Schedule Task Daily
Every:
1
day(s)
Advanced...
OK
Cancel
Apply
Help

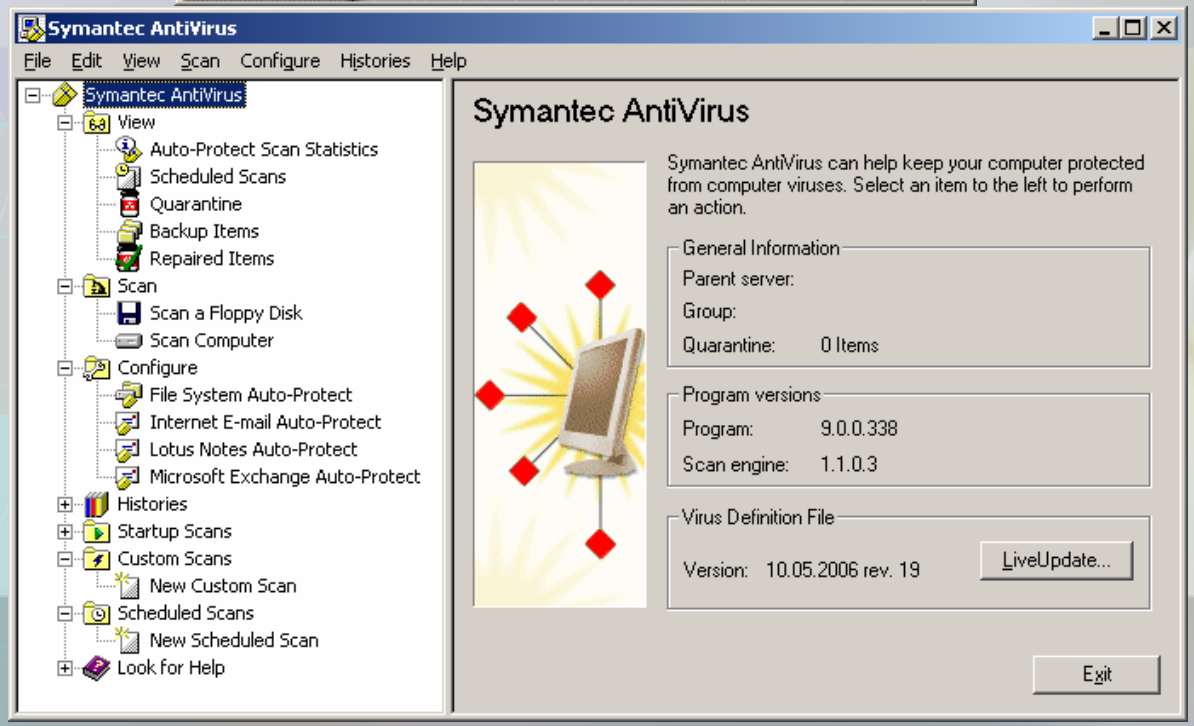

VirusScan Console
Task
Edit
View
Tools
Help
User Interface Options...
Lock User Interface
Unlock User Interface...
Error Reporting Service...
Alerts...
Event Viewer...
Open Remote Console...
Import AutoUpdate Repository List...
Edit AutoUpdate Repository List...
Rollback DATs
Task
Last Result
Access Protecti
Buffer Overflov
On-Delivery E-r
Unwanted Prog
On-Access Scar
Scan All Fixed D
AutoUpdate
defined. ...
egories a...
The Update succeeded
Edit the list of updat

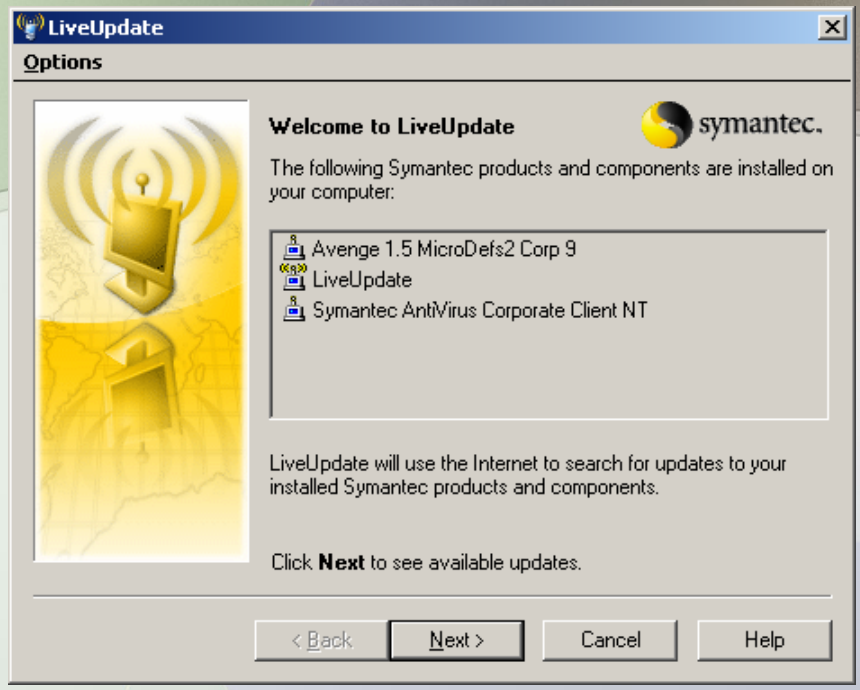

Edit AutoUpdate Repository List
Repositories
Proxy settings
Repository Description
State
ODTU
Enabled
NAIHttp
Enabled
NAIFtp
Enabled
Add...
Edit...
Delete
Move up
Move down
OK
Cancel
Help

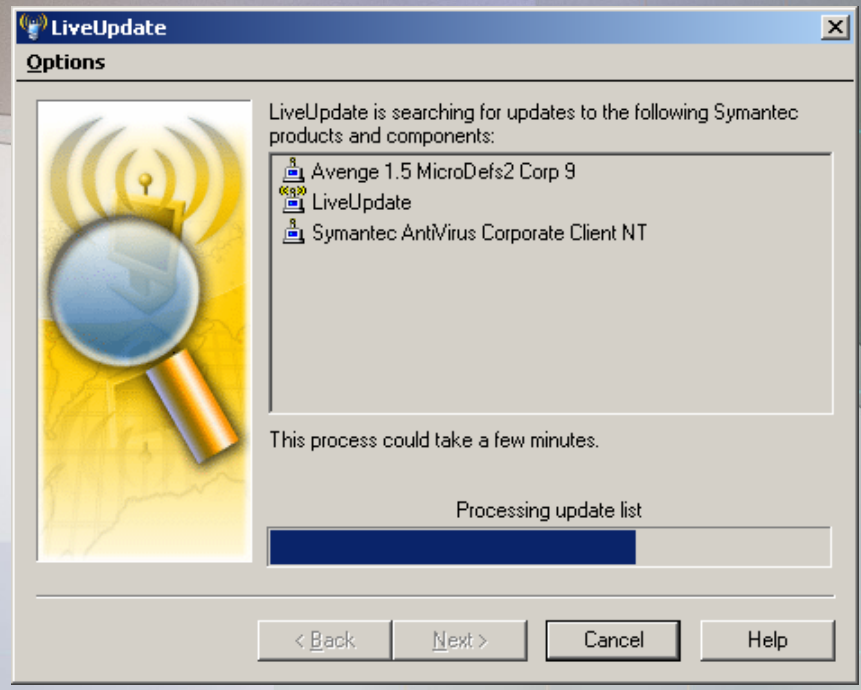

Repository Settings
Repository description:
ODTU
Retrieve files from
HTTP repository
UNC path
FTP repository
Local path
Repository details
URL:
ftp://
ftp.metu.edu.tr/popular/virus-updates/mcafee
Port:
21
Use anonymous login
User name:
Password:
Confirm password:
OK
Cancel
Help

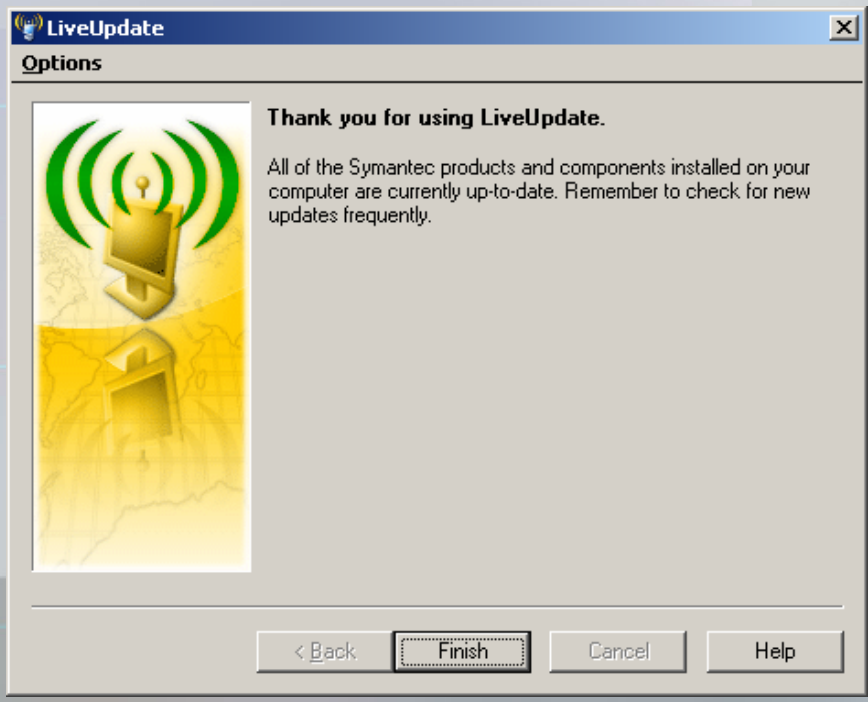
-Symantec AntiVirus-

http://securityresponse.symantec.com/avcenter/download.html



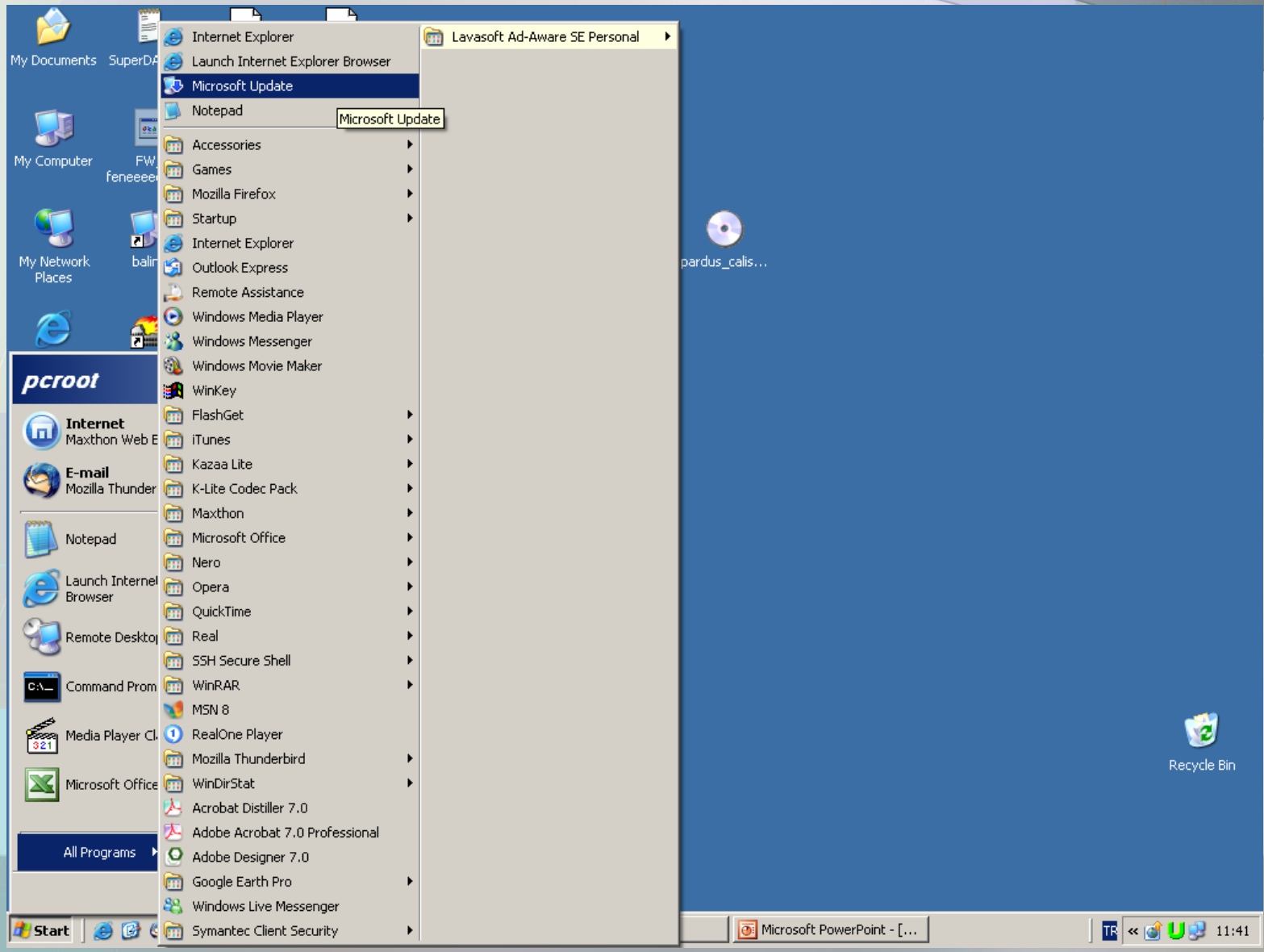

LiveUpdate
Options
Welcome to LiveUpdate
symantec.
The following Symantec products and components are installed on your computer:
Avenge 1.5 MicroDefs2 Corp 9
LiveUpdate
Symantec AntiVirus Corporate Client NT
LiveUpdate will use the Internet to search for updates to your installed Symantec products and components.
Click Next to see available updates.
< Back
Next >
Cancel
Help

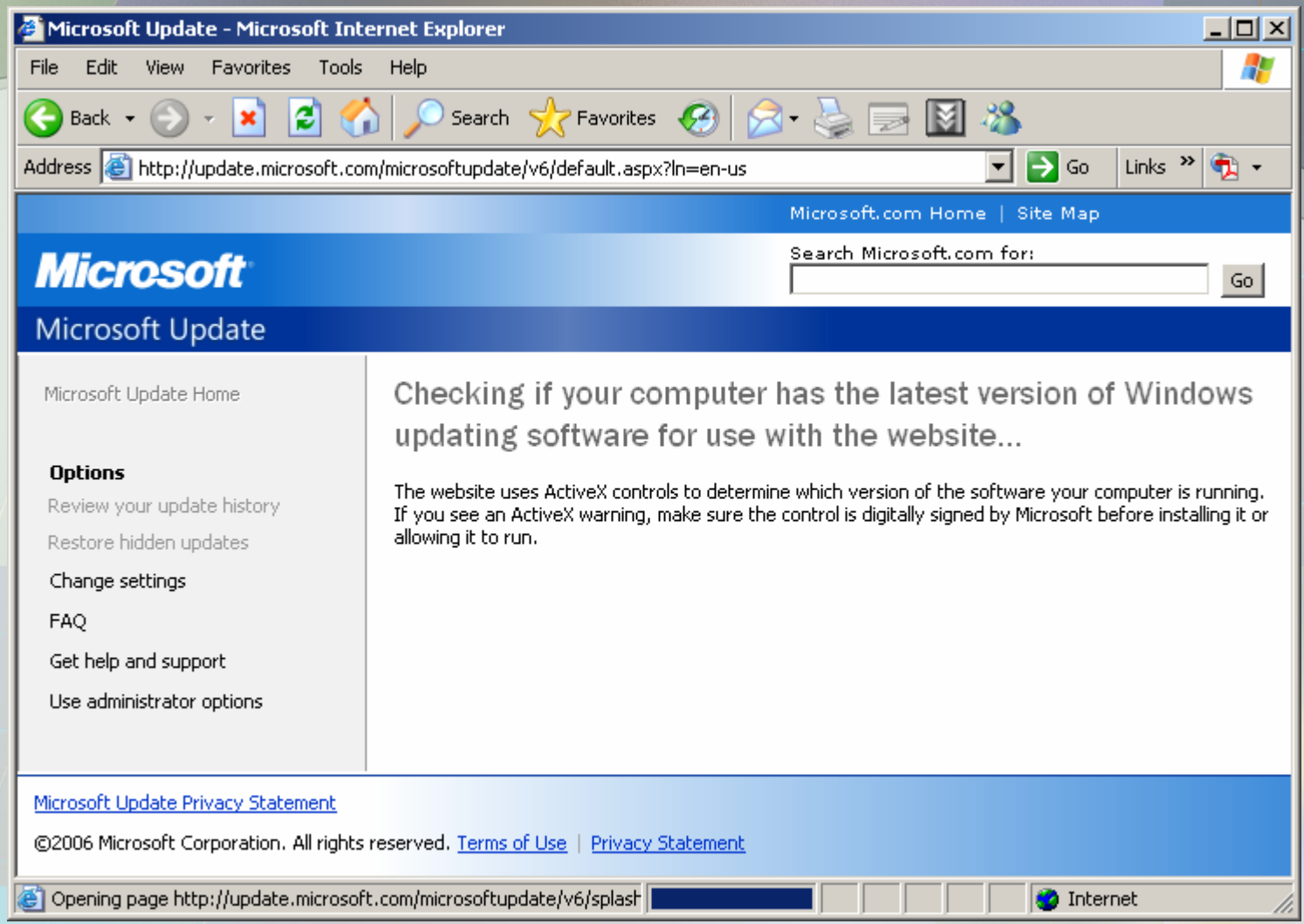

LiveUpdate
Options
LiveUpdate is searching for updates to the following Symantec products and components:
Avenge 1.5 MicroDefs2 Corp 9
LiveUpdate
Symantec AntiVirus Corporate Client NT
This process could take a few minutes.
Processing update list
< Back
Next >
Cancel
Help

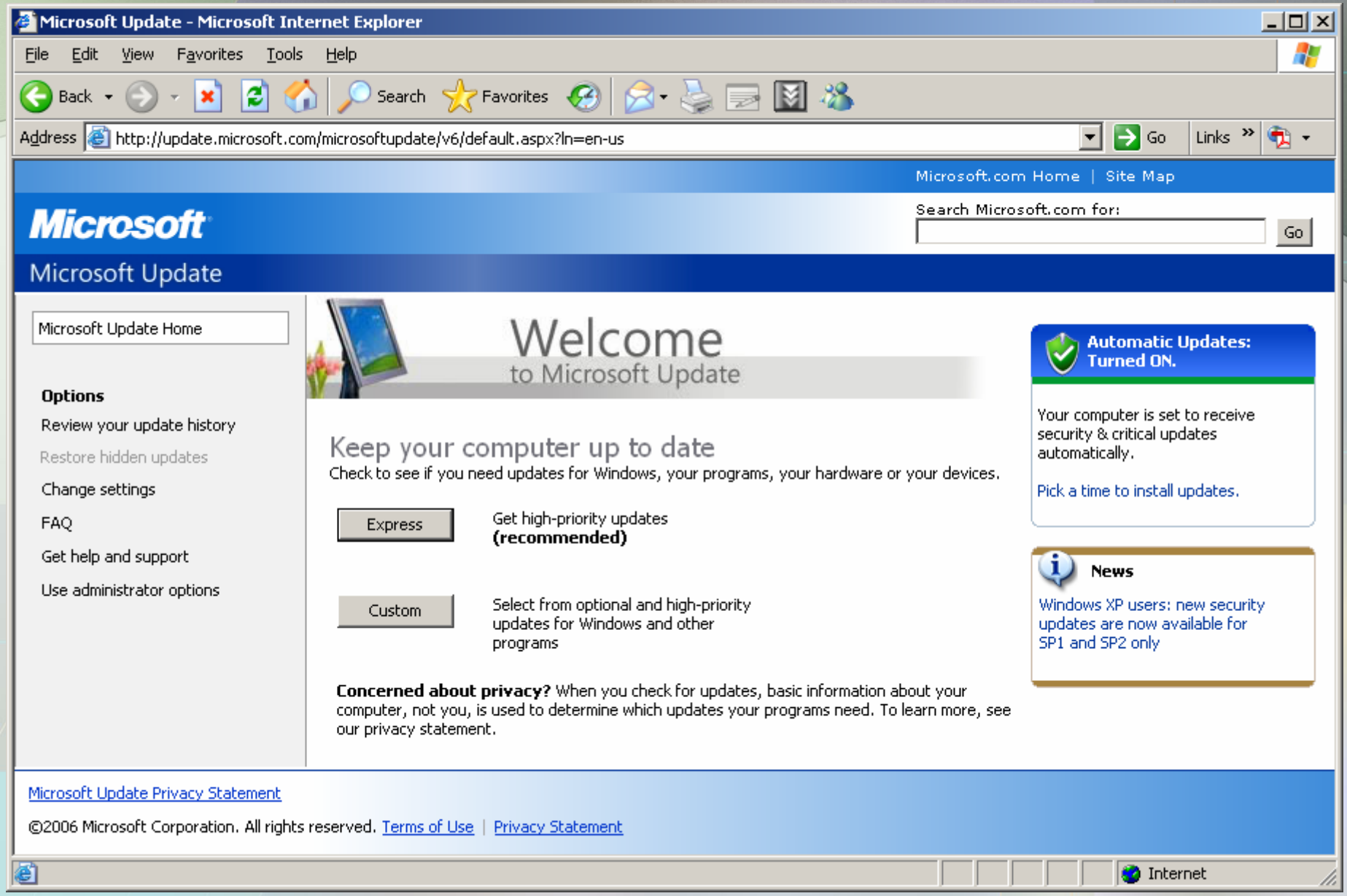

LiveUpdate
Options
Thank you for using LiveUpdate.
All of the Symantec products and components installed on your computer are currently up-to-date. Remember to check for new updates frequently.
< Back
Finish
Cancel
Help

WINDOWS GÜNCELLEMELERİNİN ELLE YAPILMASI -1

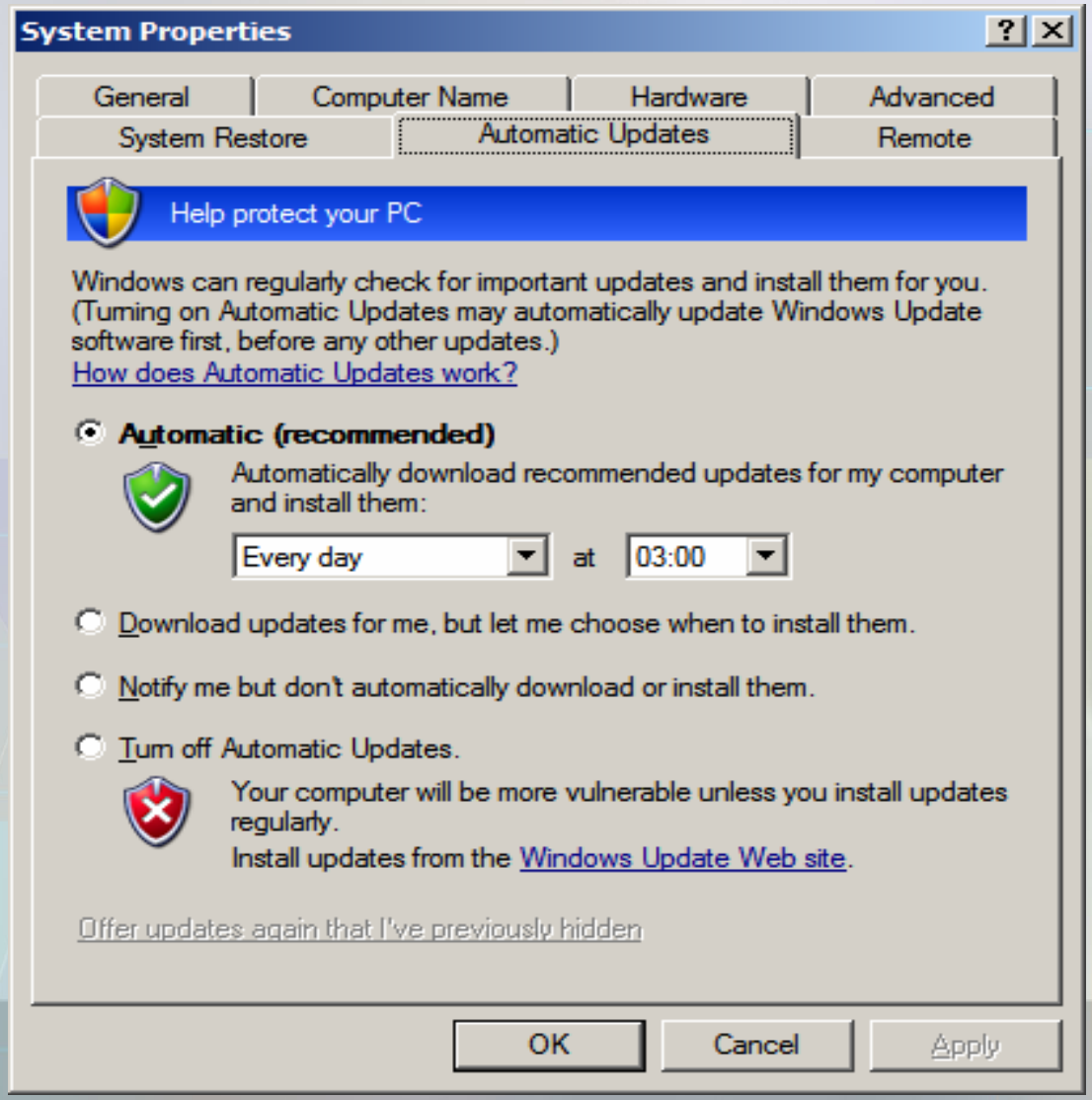
WINDOWS GÜNCELLEMELERİNİN ELLE YAPILMASI -2




Microsoft Update - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://update.microsoft.com/microsoftupdate/v6/default.aspx?ln=en-us
Go Links
Microsoft.com Home | Site Map
Microsoft
Search Microsoft.com for:
Go
Microsoft Update
Microsoft Update Home
Options
Review your update history
Restore hidden updates
Change settings
FAQ
Get help and support
Use administrator options
Checking if your computer has the latest version of Windows updating software for use with the website...
The website uses ActiveX controls to determine which version of the software your computer is running. If you see an ActiveX warning, make sure the control is digitally signed by Microsoft before installing it or allowing it to run.
Microsoft Update Privacy Statement
©2006 Microsoft Corporation. All rights reserved. Terms of Use | Privacy Statement
Opening page http://update.microsoft.com/microsoftupdate/v6/splash
Internet

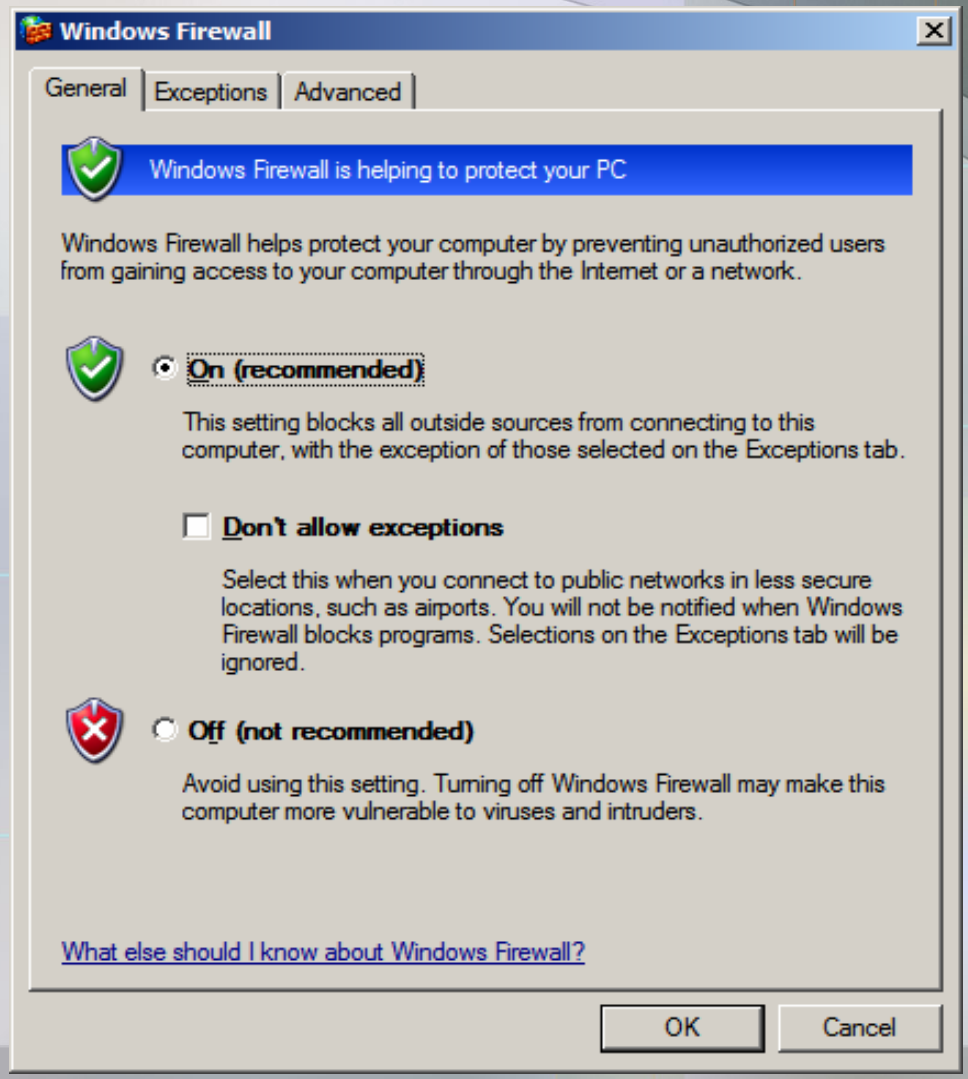

Microsoft Update - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://update.microsoft.com/microsoftupdate/v6/default.aspx?ln=en-us
Go Links
Microsoft.com Home | Site Map
Search Microsoft.com for:
Go
Microsoft
Microsoft Update
Microsoft Update Home
Options
Review your update history
Restore hidden updates
Change settings
FAQ
Get help and support
Use administrator options
Welcome
to Microsoft Update
Keep your computer up to date
Check to see if you need updates for Windows, your programs, your hardware or your devices.
Express
Get high-priority updates
(recommended)
Custom
Select from optional and high-priority updates for Windows and other programs
Concerned about privacy? When you check for updates, basic information about your computer, not you, is used to determine which updates your programs need. To learn more, see our privacy statement.
Automatic Updates: Turned ON.
Your computer is set to receive security & critical updates automatically.
Pick a time to install updates.
News
Windows XP users: new security updates are now available for SP1 and SP2 only
Microsoft Update Privacy Statement
©2006 Microsoft Corporation. All rights reserved. Terms of Use | Privacy Statement
Internet

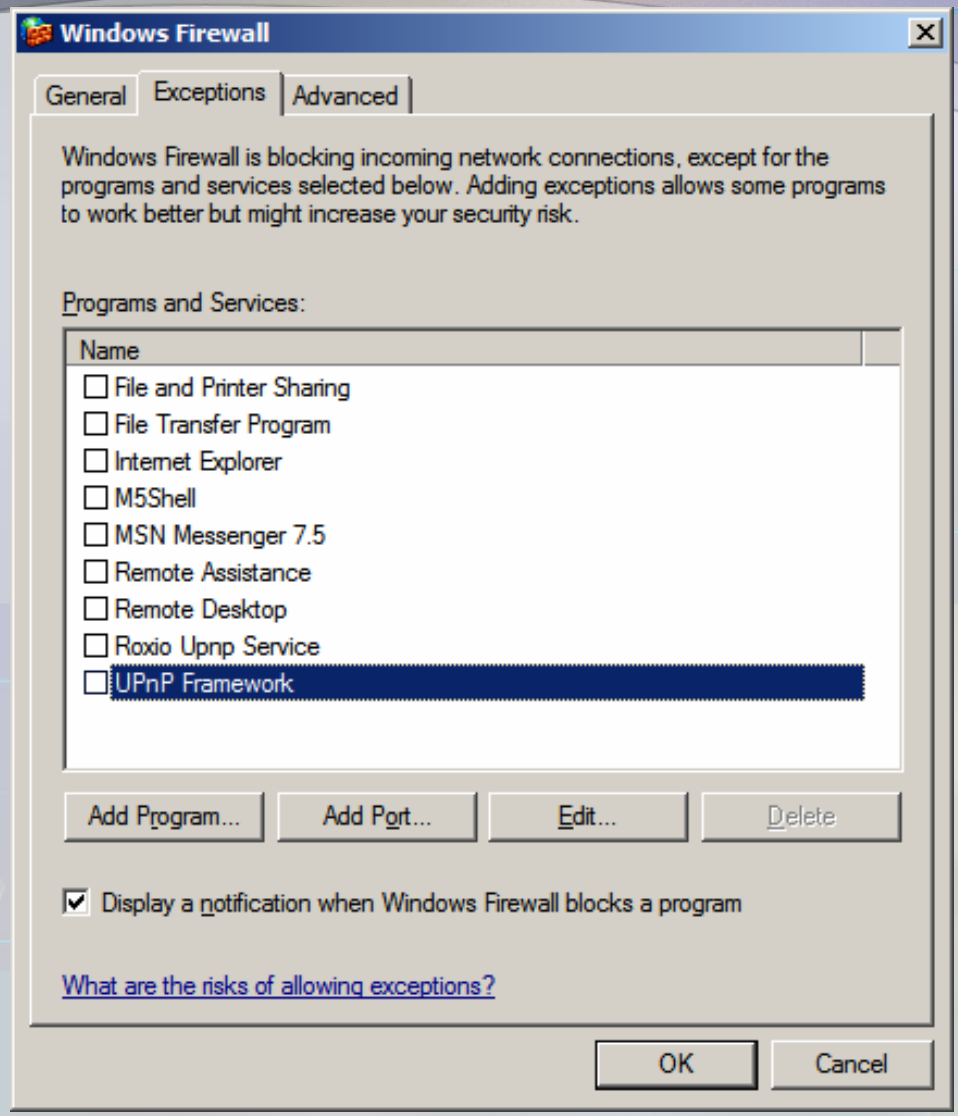
WINDOWS GÜNCELLEMELERİNİN OTOMATİK YAPILMASI



GÜVENLİK DUVARI KURULUR

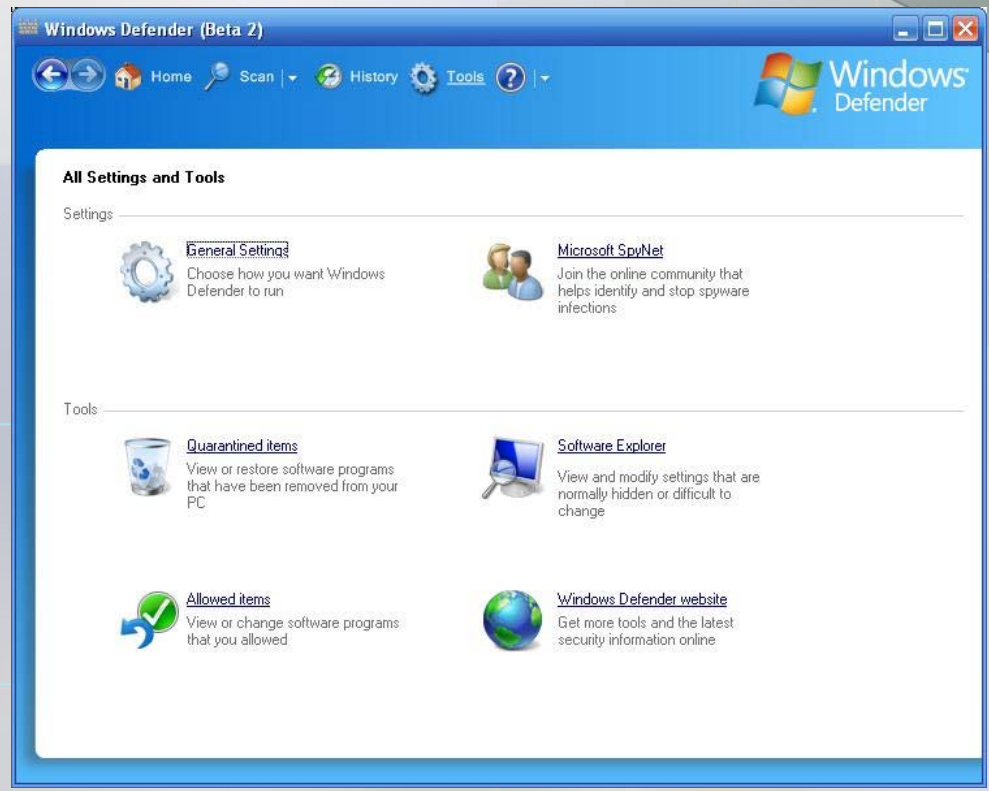
- Windows Firewall
- Symantec Firewall
- Mcafee Firewall




Windows Firewall
General
Exceptions
Advanced
Windows Firewall is blocking incoming network connections, except for the programs and services selected below. Adding exceptions allows some programs to work better but might increase your security risk.
Programs and Services:
Name
File and Printer Sharing
File Transfer Program
Internet Explorer
M5Shell
MSN Messenger 7.5
Remote Assistance
Remote Desktop
Roxio Upnp Service
UPnP Framework
Add Program...
Add Port...
Edit...
Delete
Display a notification when Windows Firewall blocks a program
What are the risks of allowing exceptions?
OK
Cancel

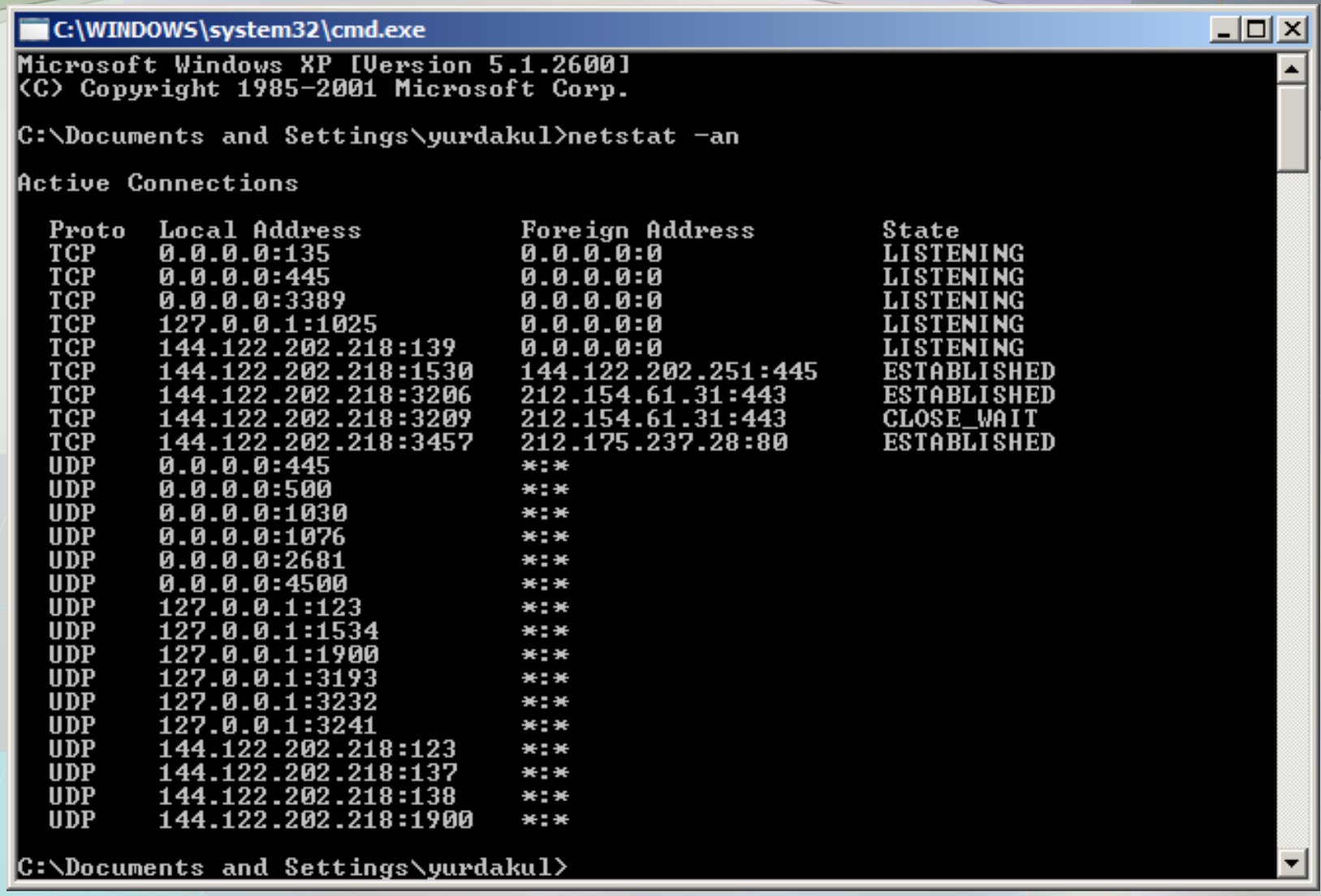
ANTİSPYWARE YAZILIMI KURULUR, AYARLARI VE GÜNCELLEMELERİ YAPILIR

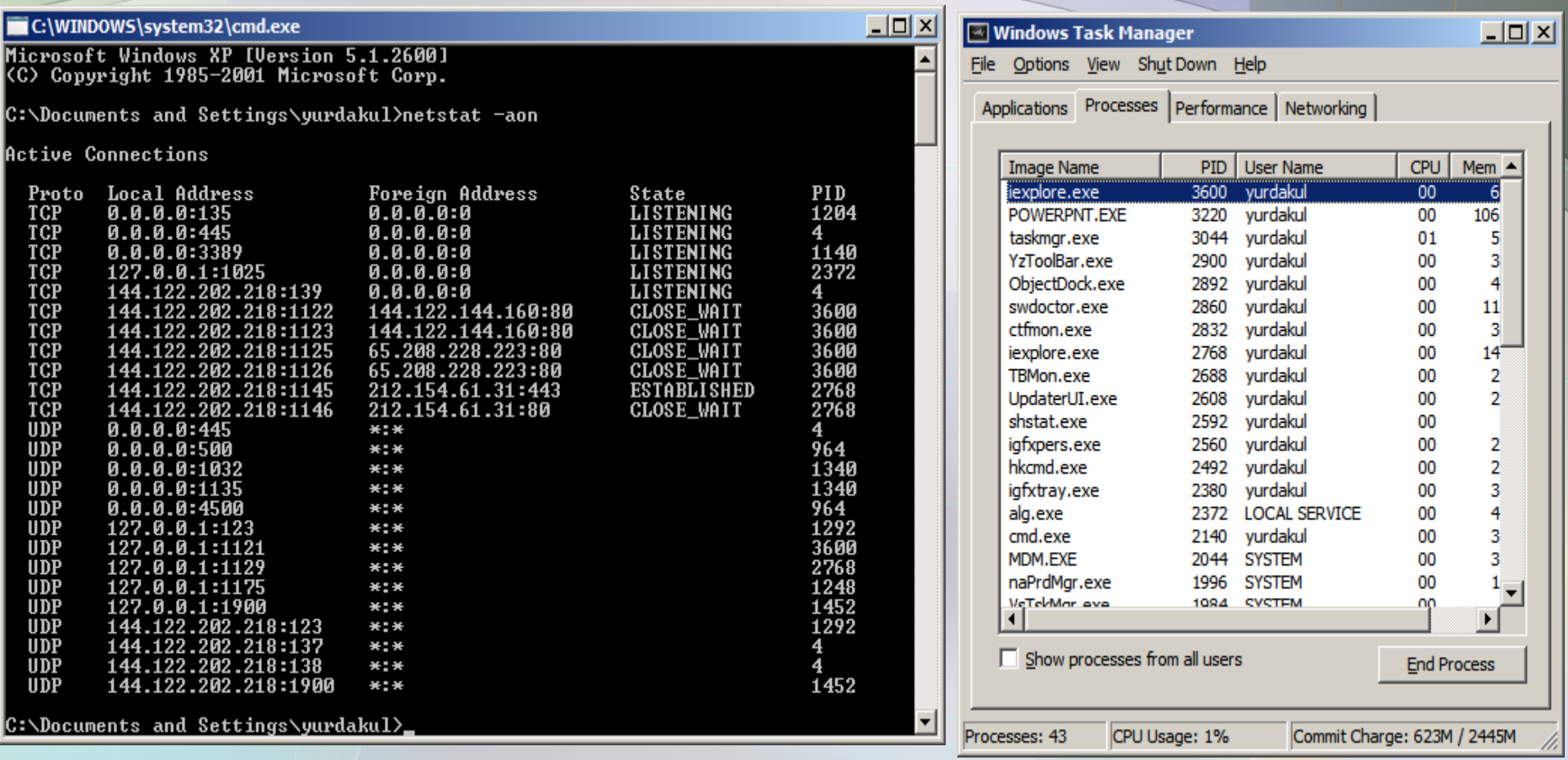

Windows Defender
Windows Defender
Copyright © 2004-2005, Microsoft Corporation. All rights reserved.
Windows Defender system information:
Windows Defender Version: 1.1.963.0
Engine Version: 1.1.963.0
Spyware Signatures Version: 1.11.963.0
Support
For more information on the Windows Defender (Beta) product, visit the Microsoft Spyware page at http://go.microsoft.com/fwlink/?LinkId=55273.
Assisted support for this beta product is not available. Once the final release of Windows Defender has been made publicly available, customers will be able to contact Product Support Services for help. In the meantime, we have provided online support resources to help you try
View Windows Defender information on the web
Warning: This software program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it may result in severe civil or criminal penalties, and will be prosecuted to the fullest extent of the law.
OK
Check for Updates


Windows Defender (Beta 2)
Home
Scan
History
Tools
Windows Defender
All Settings and Tools
Settings
General Settings
Choose how you want Windows Defender to run
Microsoft SpyNet
Join the online community that helps identify and stop spyware infections
Tools
Quarantined items
View or restore software programs that have been removed from your PC
Software Explorer
View and modify settings that are normally hidden or difficult to change
Allowed items
View or change software programs that you allowed
Windows Defender website
Get more tools and the latest security information online


Spyware Doctor
Spyware Doctor
Smart Update
Help
Status
Start Scan
OnGuard
Tools
Settings
Register
Select an Action
Scan Computer Now
Click here to scan your computer for infections now!
Immunize Computer
Click to immunize computer against all known threats
OnGuard Protection is OFF
Click to turn OnGuard real-time protection ON or OFF
System Status: Attention Required
Version is Current
Last Scan 3 days ago
Last Update 14 days ago
Trial Subscription
Product Version: 3.8.0.1557
Database Version: 3.04580
Intelli-Signatures: 59837
Last Scan: (found 43 infection(s))
PC Tools Software
Essential tools for your PC

Netstat


C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\yurdakul>netstat -an
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING
TCP 127.0.0.1:1025 0.0.0.0:0 LISTENING
TCP 144.122.202.218:139 0.0.0.0:0 LISTENING
TCP 144.122.202.218:1530 144.122.202.251:445 ESTABLISHED
TCP 144.122.202.218:3206 212.154.61.31:443 ESTABLISHED
TCP 144.122.202.218:3209 212.154.61.31:443 CLOSE_WAIT
TCP 144.122.202.218:3457 212.175.237.28:80 ESTABLISHED
UDP 0.0.0.0:445 *:*
UDP 0.0.0.0:500 *:*
UDP 0.0.0.0:1030 *:*
UDP 0.0.0.0:1076 *:*
UDP 0.0.0.0:2681 *:*
UDP 0.0.0.0:4500 *:*
UDP 127.0.0.1:123 *:*
UDP 127.0.0.1:1534 *:*
UDP 127.0.0.1:1900 *:*
UDP 127.0.0.1:3193 *:*
UDP 127.0.0.1:3232 *:*
UDP 127.0.0.1:3241 *:*
UDP 144.122.202.218:123 *:*
UDP 144.122.202.218:137 *:*
UDP 144.122.202.218:138 *:*
UDP 144.122.202.218:1900 *:*
C:\Documents and Settings\yurdakul>


C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\yurdakul>netstat -aon
Active Connections
Proto Local Address Foreign Address State PID
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 1204
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING 1140
TCP 127.0.0.1:1025 0.0.0.0:0 LISTENING 2372
TCP 144.122.202.218:139 0.0.0.0:0 LISTENING 4
TCP 144.122.202.218:1122 144.122.144.160:80 CLOSE_WAIT 3600
TCP 144.122.202.218:1123 144.122.144.160:80 CLOSE_WAIT 3600
TCP 144.122.202.218:1125 65.208.228.223:80 CLOSE_WAIT 3600
TCP 144.122.202.218:1126 65.208.228.223:80 CLOSE_WAIT 3600
TCP 144.122.202.218:1145 212.154.61.31:443 ESTABLISHED 2768
TCP 144.122.202.218:1146 212.154.61.31:80 CLOSE_WAIT 2768
UDP 0.0.0.0:445 *:* 4
UDP 0.0.0.0:500 *:* 964
UDP 0.0.0.0:1032 *:* 1340
UDP 0.0.0.0:1135 *:* 1340
UDP 0.0.0.0:4500 *:* 964
UDP 127.0.0.1:123 *:* 1292
UDP 127.0.0.1:1121 *:* 3600
UDP 127.0.0.1:1129 *:* 2768
UDP 127.0.0.1:1175 *:* 1248
UDP 127.0.0.1:1900 *:* 1452
UDP 144.122.202.218:123 *:* 1292
UDP 144.122.202.218:137 *:* 4
UDP 144.122.202.218:138 *:* 4
UDP 144.122.202.218:1900 *:* 1452
C:\Documents and Settings\yurdakul>
Windows Task Manager
File Options View Shut Down Help
Applications Processes Performance Networking
Image Name PID User Name CPU Mem
iexplore.exe 3600 yurdakul 00 6
POWERPNT.EXE 3220 yurdakul 00 106
taskmgr.exe 3044 yurdakul 01 5
YzToolBar.exe 2900 yurdakul 00 3
ObjectDock.exe 2892 yurdakul 00 4
swdoctor.exe 2860 yurdakul 00 11
ctfmon.exe 2832 yurdakul 00 3
iexplore.exe 2768 yurdakul 00 14
TBMon.exe 2688 yurdakul 00 2
UpdaterUI.exe 2608 yurdakul 00 2
shstat.exe 2592 yurdakul 00
igfxpers.exe 2560 yurdakul 00 2
hkcmd.exe 2492 yurdakul 00 2
igfxtray.exe 2380 yurdakul 00 3
alg.exe 2372 LOCAL SERVICE 00 4
cmd.exe 2140 yurdakul 00 3
MDM.EXE 2044 SYSTEM 00 3
naPrdMgr.exe 1996 SYSTEM 00 1
Show processes from all users
End Process
Processes: 43
CPU Usage: 1%
Commit Charge: 623M / 2445M

AĞ GÜVENLİĞİNDE KULLANILABİLECEK ARAÇLAR

- WinDump
- Ethereal
- Nesus
- NMap

PC SALONLARI İÇİN GÜVENLİK

- Kullanıcı haklarının sınırlandırılması (mmc ayarları, sistem dizinine erişim kontrolü).
- Günlük tutulması(Event Log).
- Kullanıcı profillerinin silinmesi.
- Kimlik kontrolü yapılması.
- Merkezi yönetimden güncellemelerin yapılması.
- Belirli aralıklarla sistemlerin güvenlik taramalarının yapılması.

TEŞEKKÜR EDERİZ