

بِسْمِ اللّٰهِ الرَّحْمٰنِ الرَّحِیْمِ

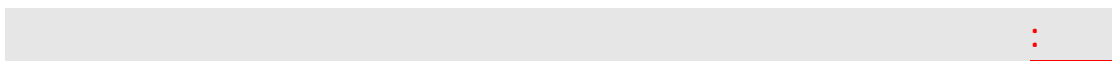


Written by: Salah Ahssen

[www.Server4Arb.com](http://www.Server4Arb.com)

...

.



**MCSE**

.

...

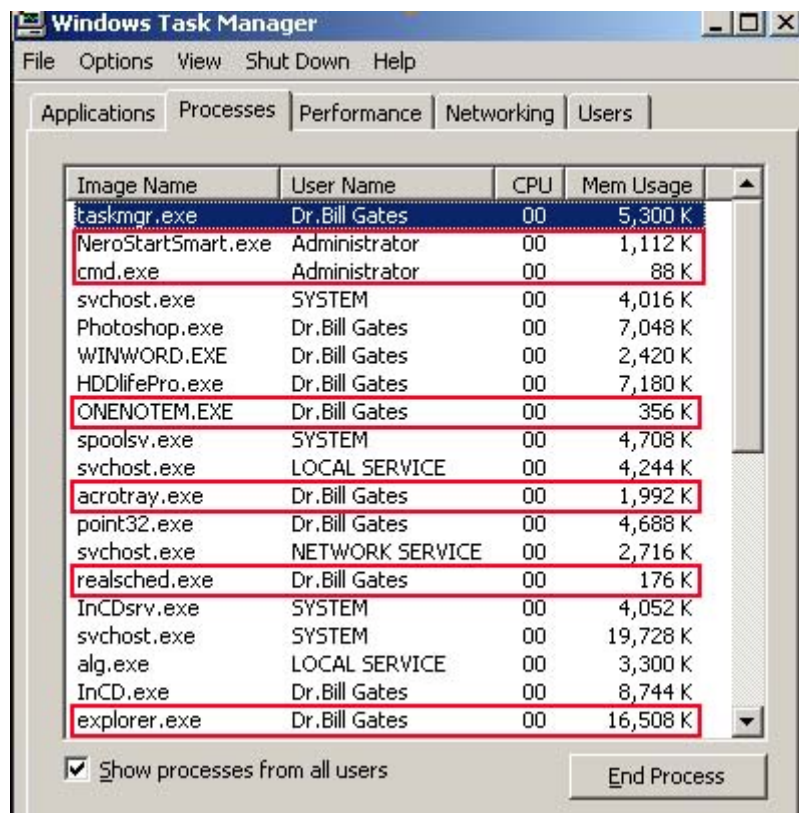
**administrator**

**.guest**

**users**

**server operator**

**:task manager " "**



**process**

**Security context**

- 1- local service
- 2- network service
- 3- system

Domain

system

" SVCHOST "

process

: tasklist

```
Dr. Bill Gates
C:\>tasklist /svc
Image Name          PID  Services
-----
System Idle Process 0     N/A
System              4     N/A
smss.exe            504   N/A
csrss.exe           560   N/A
winlogon.exe        584   N/A
services.exe        628   Eventlog, PlugPlay
lsass.exe            640   PolicyAgent, ProtectedStorage, SamSs
svchost.exe          788   DcomLaunch, TermService
svchost.exe          852   RpcSs
svchost.exe          888   AudioSrv, CryptSvc, Dhcp, dmserver, ERSvc,
EventSystem, helpsvc, lanmanserver,
lanmanworkstation, Netman, Nla, RasMan,
Schedule, seclogon, SENS, SharedAccess,
ShellHWDetection, srsservice, TapiSrv,
Themes, TrkWks, W32Time, winmgmt, wscsvc,
wuauclt, WZCSC
svchost.exe          944   Dnscache
svchost.exe          1020  LmHosts, RemoteRegistry, SSDPSRV, WebClient
spoolsv.exe          1140  Spooler
MDM.EXE              1256  MDM
nsvsvc32.exe         1280  NUSvc
snmp.exe             1316  SNMP
wdfmgr.exe           1344  UMWdf
alg.exe              1636  ALG
explorer.exe         1992  N/A
realsched.exe        240   N/A
SOUNDMAN.EXE         252   N/A
rundll32.exe         280   N/A
ctfmon.exe           304   N/A
lockpc.exe           328   N/A
DnclE.exe            388   N/A
acrotroy.exe         456   N/A
HDDlife.exe          1092  N/A
WINWORD.EXE          536   N/A
cmd.exe              400   N/A
tasklist.exe         1892  N/A
wmiprouse.exe        172   N/A
C:\>
```

svchost

Taskill Tasklist

5

Task Manger

rpcSc

.Nla,rasman,W32Time














( )

2003

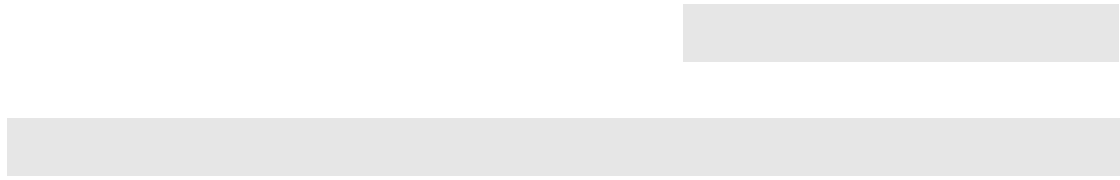
:2003



### . Domain controller

Name	Description
 Administrators	Administrators have complete and unrestricted access to the computer/domain
 Backup Operators	Backup Operators can override security restrictions for the sole purpose of backing up or restoring files
 Guests	Guests have the same access as members of the Users group by default, except for the Guest account which is...
 Network Configuration Operators	Members in this group can have some administrative privileges to manage configuration of networking features
 Performance Log Users	Members of this group have remote access to schedule logging of performance counters on this computer
 Performance Monitor Users	Members of this group have remote access to monitor this computer
 Power Users	Power Users possess most administrative powers with some restrictions. Thus, Power Users can run legacy ap...
 Print Operators	Members can administer domain printers
 Remote Desktop Users	Members in this group are granted the right to logon remotely
 Replicator	Supports file replication in a domain
 Users	Users are prevented from making accidental or intentional system-wide changes. Thus, Users can run certified ...
 HelpServicesGroup	Group for the Help and Support Center
 TelnetClients	Members of this group have access to Telnet Server on this system.

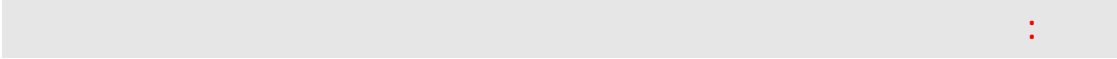
**administrators**  
**backup Operators**  
**print Operators**



**.Performance Monitor Users**

:

.1  
.2  
.3



Users

XP

.Windows Server 2003

XP

administrator

users

Dos

:

A screenshot of a Windows command prompt window. The title bar reads "c:\ Dr.Bill Gates". The command prompt shows the command "C:\>net user Kill-Israel 159357 /add" and the output "The command completed successfully." followed by a new prompt "C:\>\_".

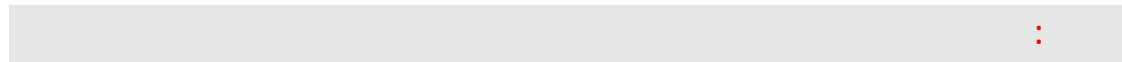
```
c:\ Dr.Bill Gates
C:\>net user Kill-Israel 159357 /add
The command completed successfully.
C:\>_
```

:( )

**User name: Kill-Israel**

**Password: 159357**

[www.Server4Arb.com](http://www.Server4Arb.com)



**Windows XP**

**: Dos**

**Professional**

**C:\shutdown -r -m -f \\nameOF Computer**

**.logoff**

**Run**





[www.Server4Arb.com](http://www.Server4Arb.com)

:

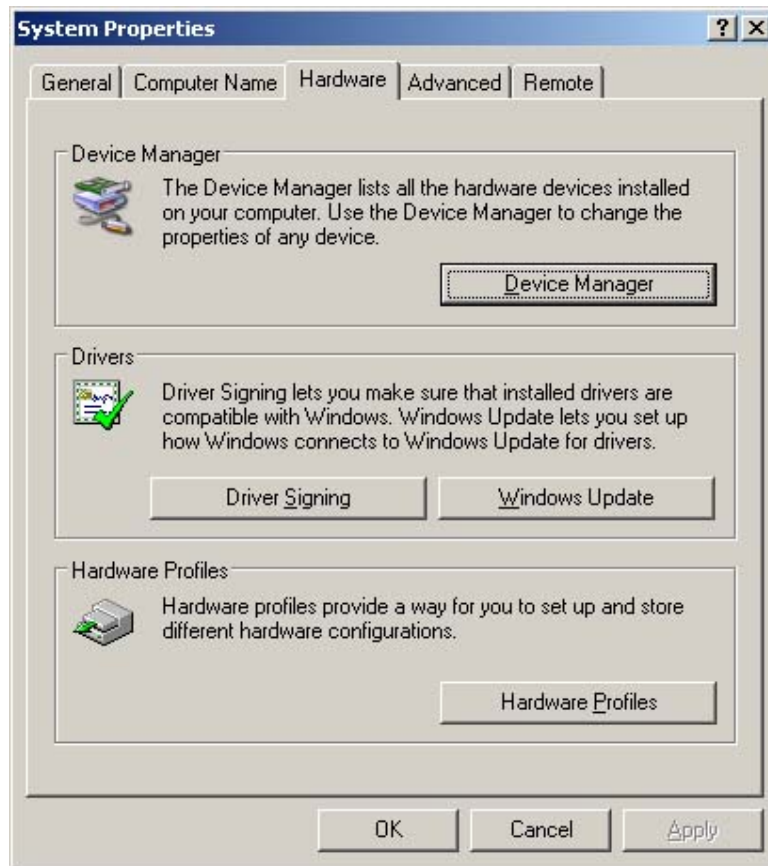


:



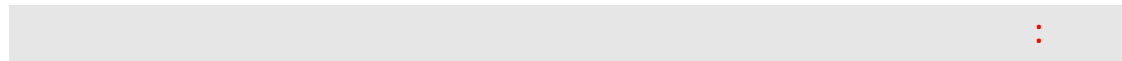
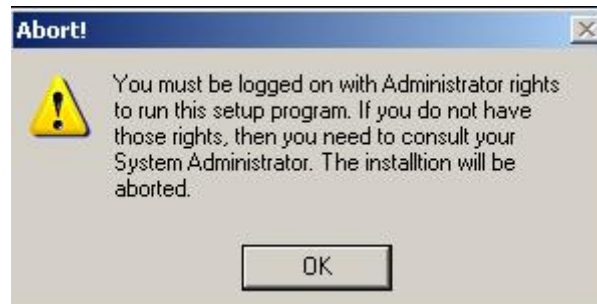
. access is denied

:



[www.Server4Arb.com](http://www.Server4Arb.com)

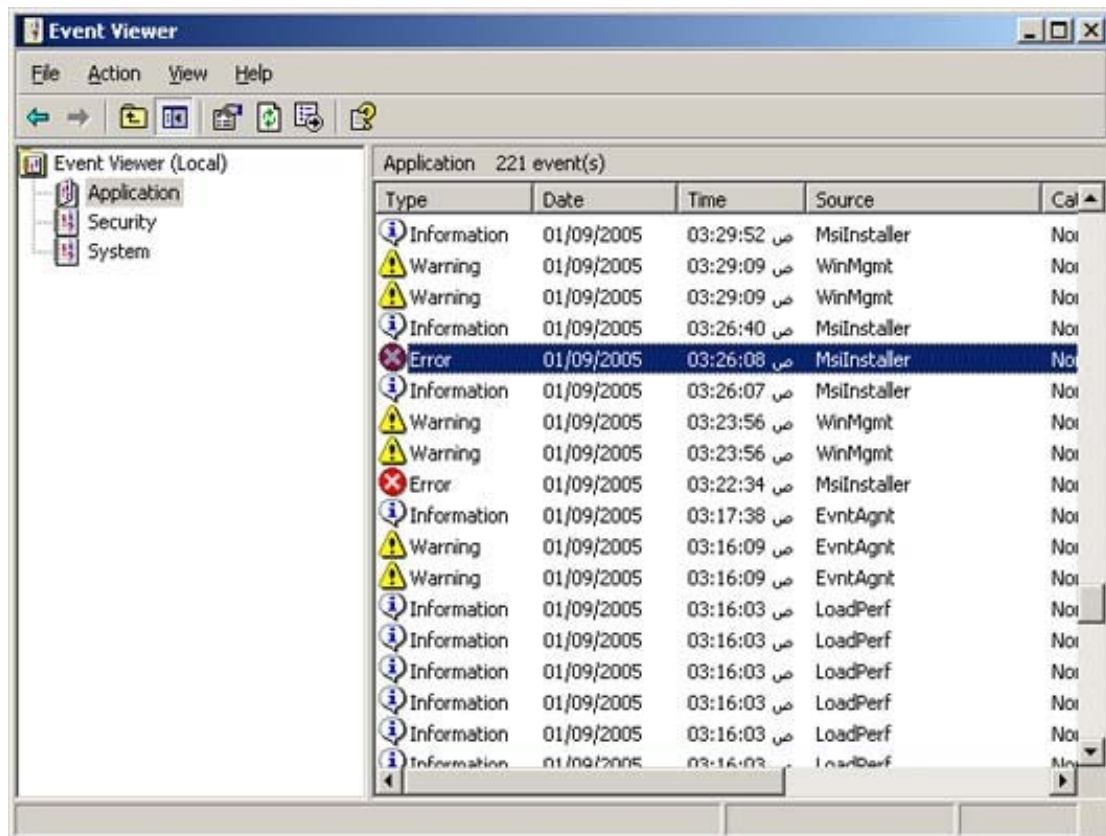
**setup**



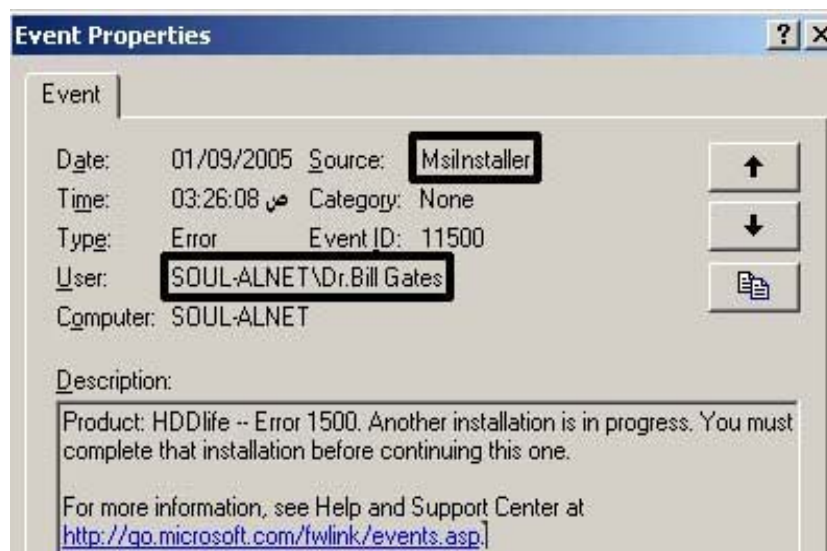
**windows installer**

:  
:

**Start > Run > eventvwr**

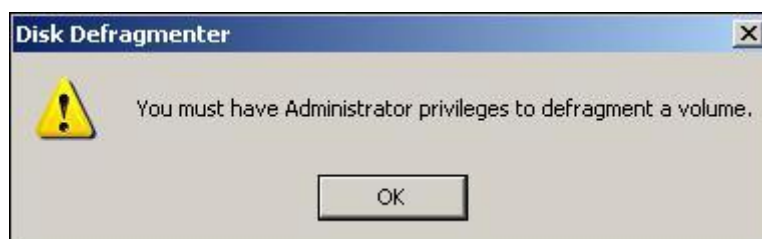


:



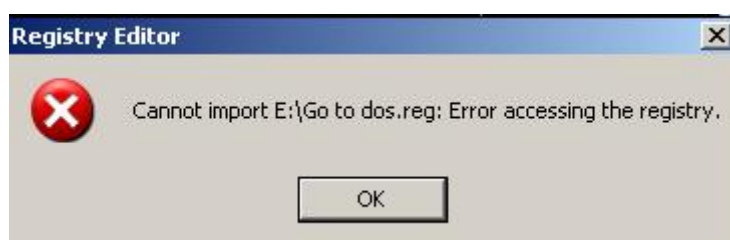
.

:



### registry

:

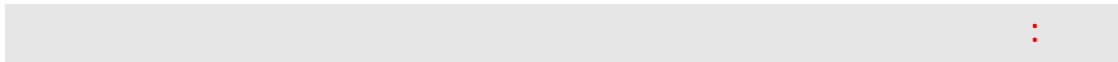


security

system restore

.

[www.Server4Arb.com](http://www.Server4Arb.com)



" "

**malfunction**

limited

administrator

Me

.

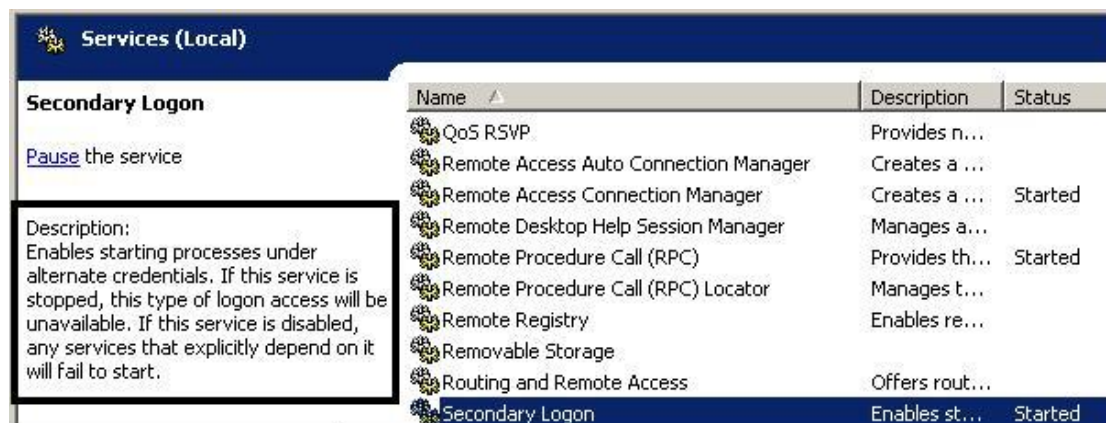


:

secondary logon

:

Start>>Run>> %SystemRoot%\system32\services.msc /s



**.local system**

**runas**

**runas**

:





cpl msc exe

:

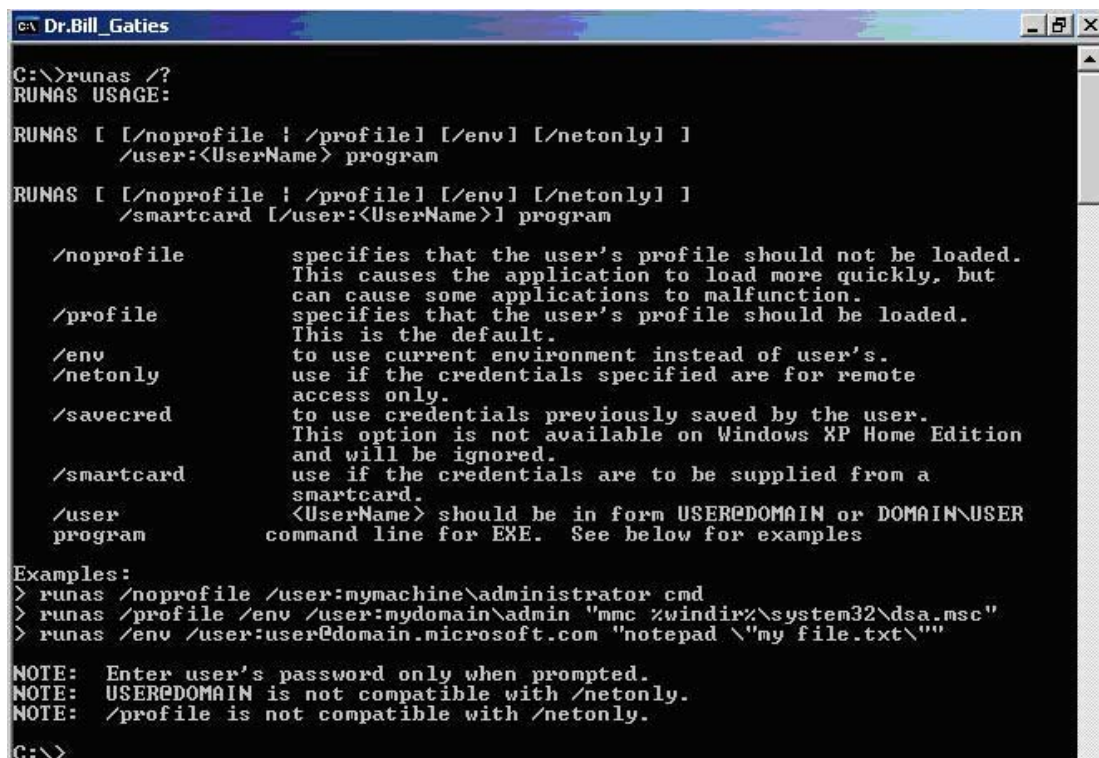
runas



runas

secondary logon

: Dos /



```
Dr.Bill_Gaties
C:\>runas /?
RUNAS USAGE:

RUNAS [ [/noprofile | /profile] [/env] [/netonly] ]
      /user:<UserName> program

RUNAS [ [/noprofile | /profile] [/env] [/netonly] ]
      /smartcard [/user:<UserName>] program

      /noprofile      specifies that the user's profile should not be loaded.
                     This causes the application to load more quickly, but
                     can cause some applications to malfunction.
      /profile        specifies that the user's profile should be loaded.
                     This is the default.
      /env            to use current environment instead of user's.
      /netonly       use if the credentials specified are for remote
                     access only.
      /savecred      to use credentials previously saved by the user.
                     This option is not available on Windows XP Home Edition
                     and will be ignored.
      /smartcard     use if the credentials are to be supplied from a
                     smartcard.
      /user          <UserName> should be in form USER@DOMAIN or DOMAIN\USER
      program       command line for EXE. See below for examples

Examples:
> runas /noprofile /user:mymachine\administrator cmd
> runas /profile /env /user:mydomain\admin "mmc %windir%\system32\dsa.msc"
> runas /env /user:user@domain.microsoft.com "notepad \"my file.txt\"

NOTE: Enter user's password only when prompted.
NOTE: USER@DOMAIN is not compatible with /netonly.
NOTE: /profile is not compatible with /netonly.

C:\>
```

Start > Run > cmd

[www.Server4Arb.com](http://www.Server4Arb.com)

:

:

**administrator**



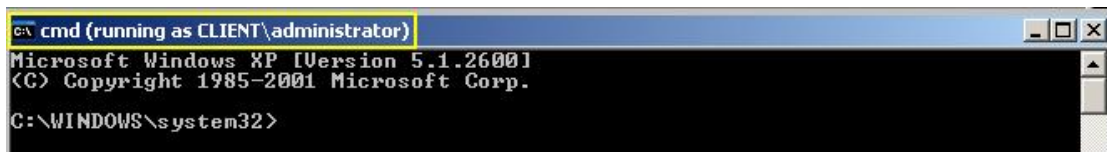
```
Dr.Bill Gates
C:\Documents and Settings\Dr.Bill Gates>runas /user:administrator cmd
```

:



```
Muslim_Haqer - runas /user:administrator cmd
C:\Documents and Settings\Dr.Bill Gates>runas /user:administrator cmd
Enter the password for administrator:
```

:



```
cmd (running as CLIENT\administrator)
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\WINDOWS\system32>
```

:

**Timedate.cpl, devmgmt.msc, defrag c: chkdsk, etc.....**

## MSC

```
C:\WINDOWS\system32\cmd.exe - runas /user:administrator "mmc C:\WINDOWS\system32\diskmgmt.msc"
C:\>runas /user:administrator "mmc %windir%\system32\diskmgmt.msc"
Enter the password for administrator:
```

```
Muslim_Haqer
C:\>runas /user:administrator cmd
Enter the password for administrator:
Attempting to start cmd as user "CLIENT\administrator" ...
RUNAS ERROR: Unable to run - cmd
1326: Logon failure: unknown user name or bad password.
C:\>
```

## disabled

```
Dr.Bill Gates
C:\>runas /user:administrator cmd
Enter the password for administrator:
Attempting to start cmd as user "CLIENT\administrator" ...
RUNAS ERROR: Unable to run - cmd
1327: Logon failure: user account restriction. Possible reasons are blank passwords not allowed, logon hour restrictions, or a policy restriction has been enforced.
C:\>
```

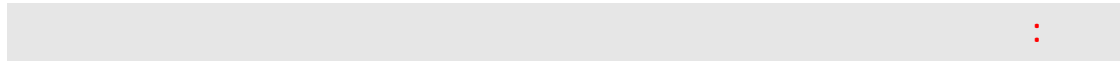
[www.Server4Arb.com](http://www.Server4Arb.com)

.( )

guest

Server operator

.



secondary

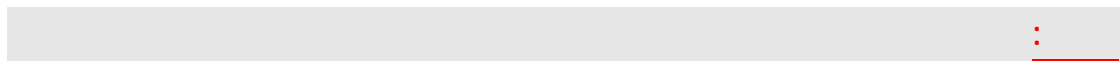
logon

runas

users rights

.(XP

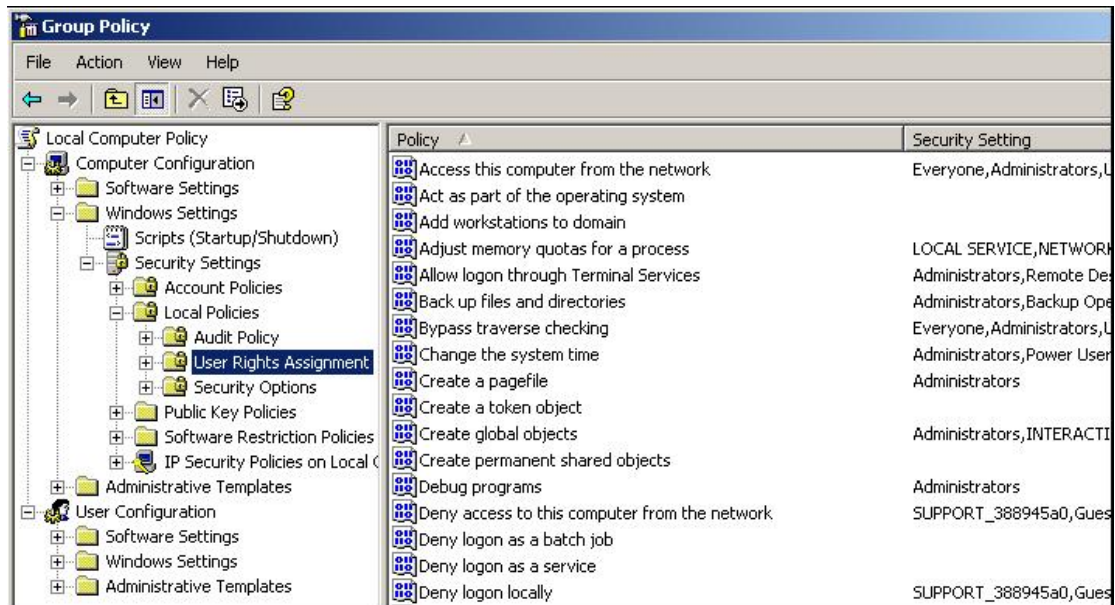
) group policy



group policy

Start > Run > gpedit.msc

:



users

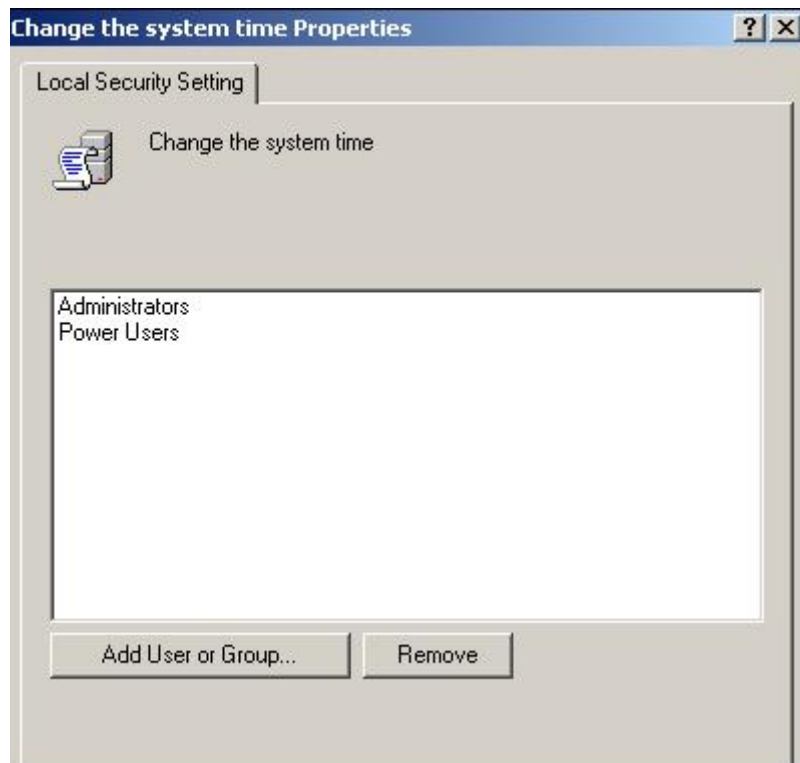
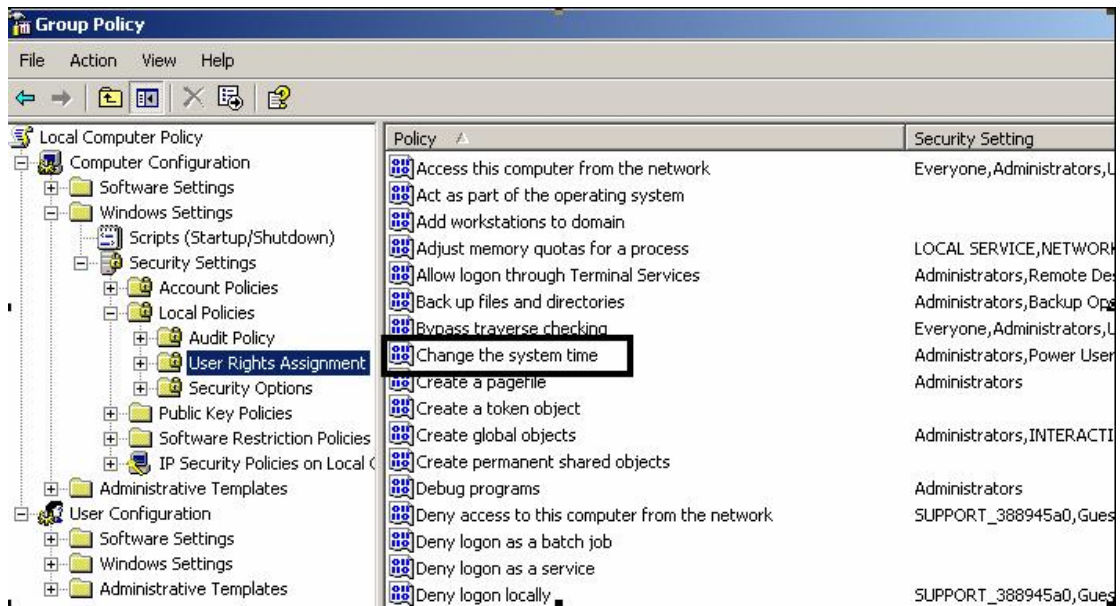
users

:

group policy

Start > Run > gpedit.msc

## Change the system time





**Power Users**      **administrator**

.



**Power users**

.

**add User or**

"

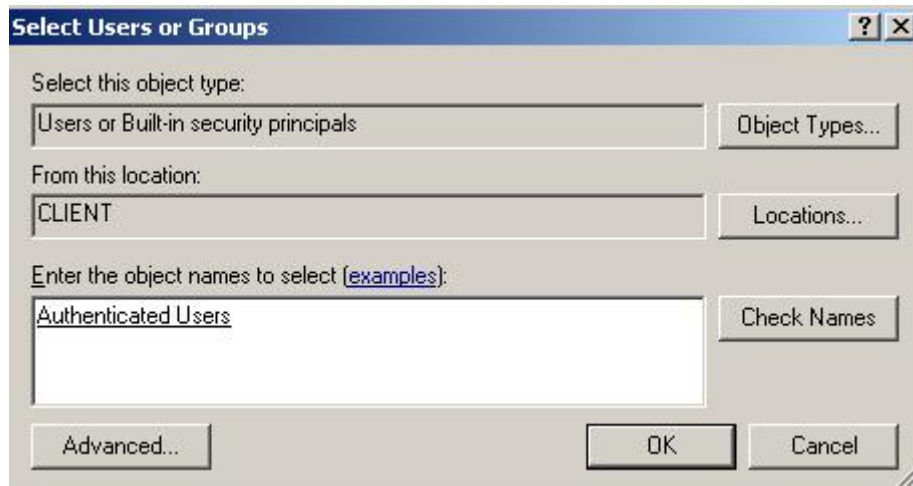
"

:

**Group**



:



**check names**

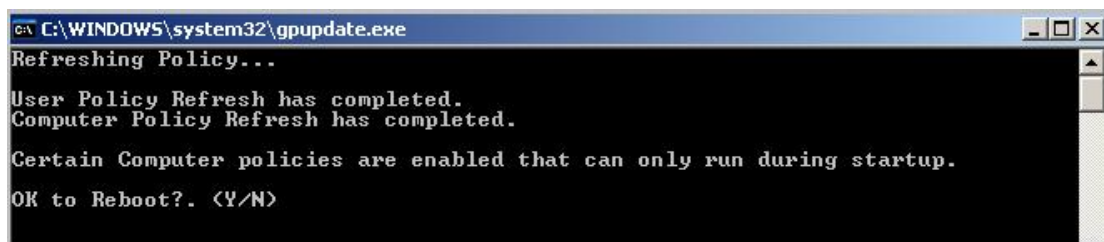
**Users**

**.group policy**

:

**Start < Run < gpupdate /force**

:



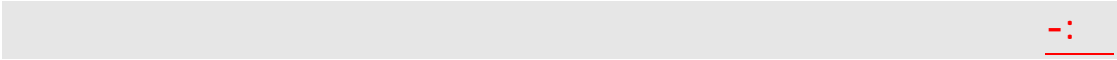
[www.Server4Arb.com](http://www.Server4Arb.com)

Y

" NTFS  
Format

.NTFS file system

fat,fat32  
fat,fat32 partition



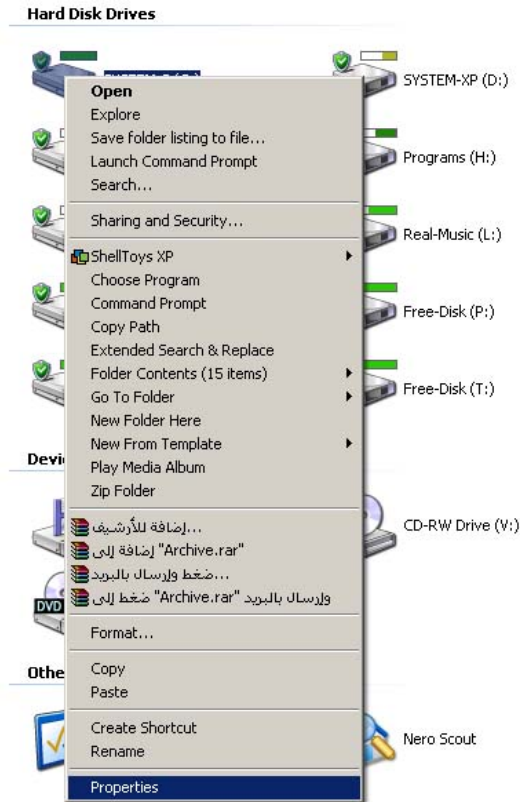
ntfs , C + D

partition 2

C

properties

## :XP

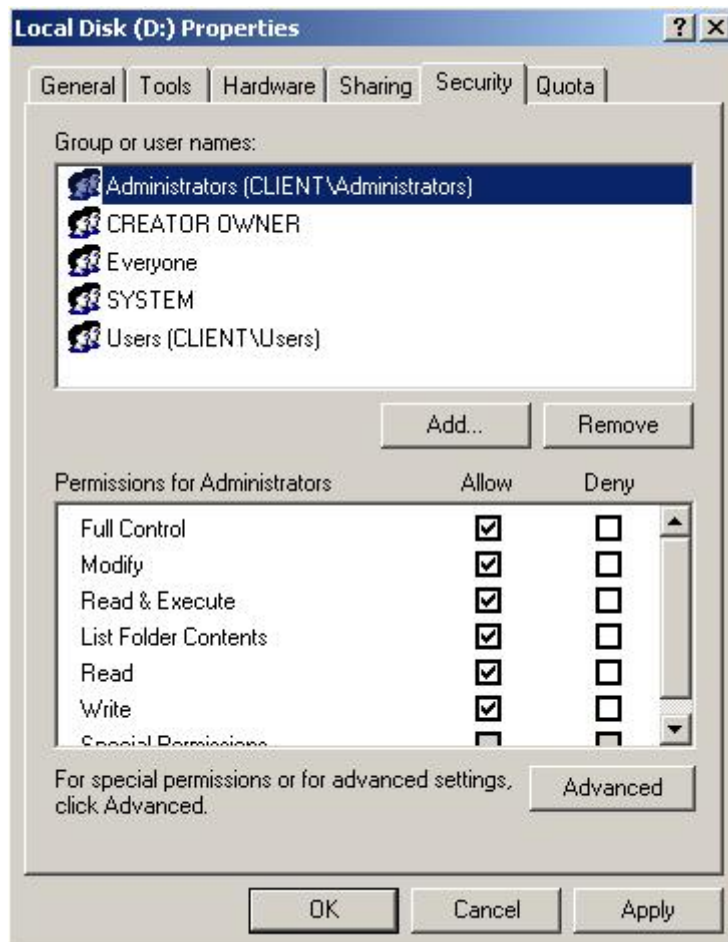


## D



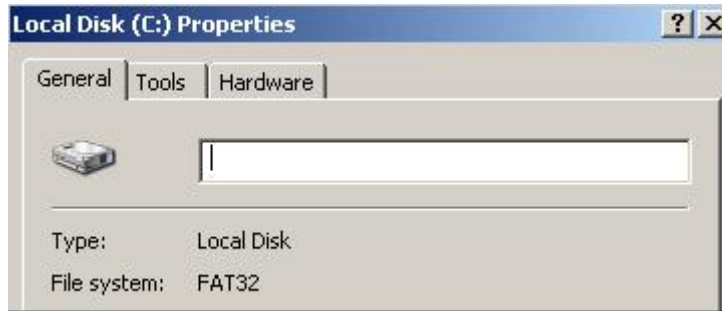
:

### security



⋮

: security



FAT32

.

: NTFS FAT32

**CONVERT c: /FS:NTFS**

**.NTFS FAT32 :C**

**. NTFS security**

**XP**

**Security**

**Simple File Sharing user**

**"**

**."**

**security**

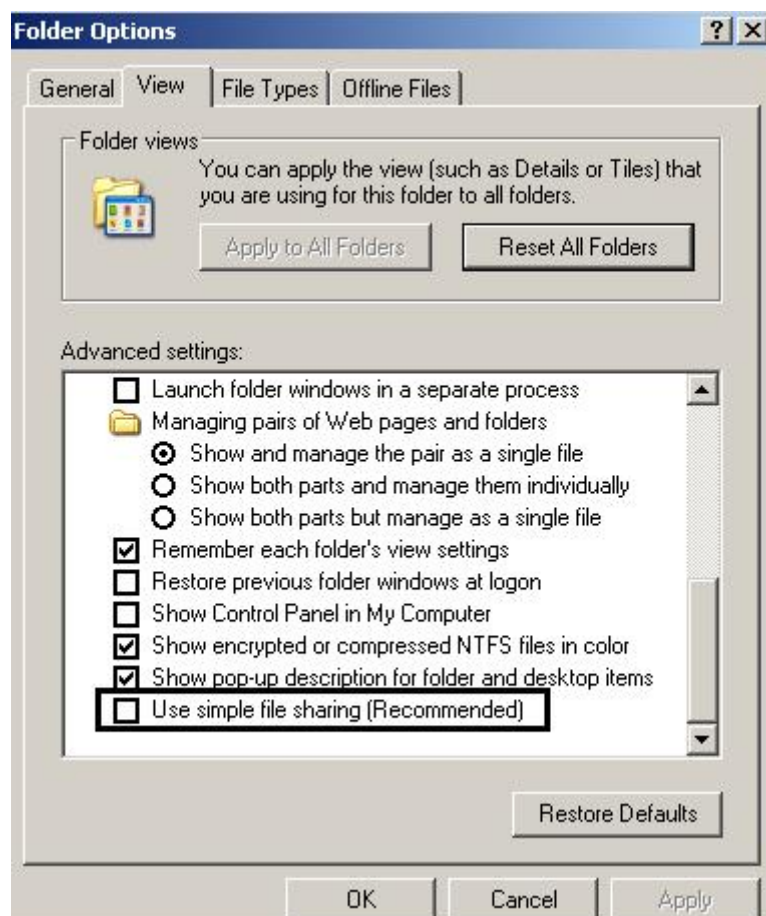
**interface**

:

Start > Run > control

. folder options

:



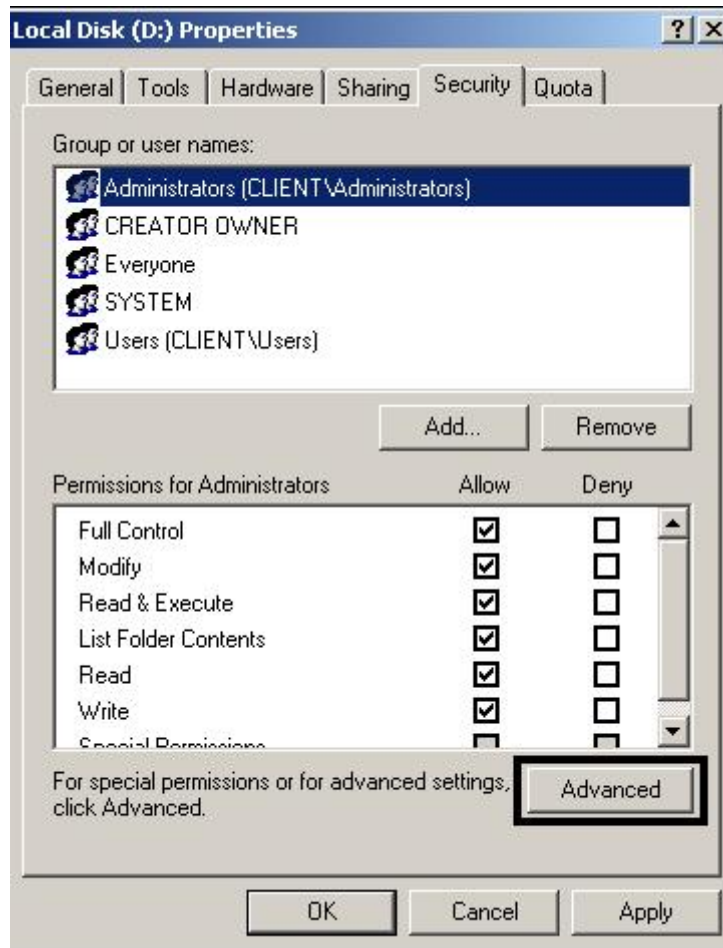
view  
.security

security



## ACL / Access Control List

entries



.( ) deny allow

2003

:

**1. Full control :**

**system administrator**

**2. Modify :**

" "

:

**Read & Execute, List folder Contents, read, write**

**3. Read & execute:**

**4. List folder Contents:**

**5. Read:**

**6. Write:**

## 7. Special Permissions

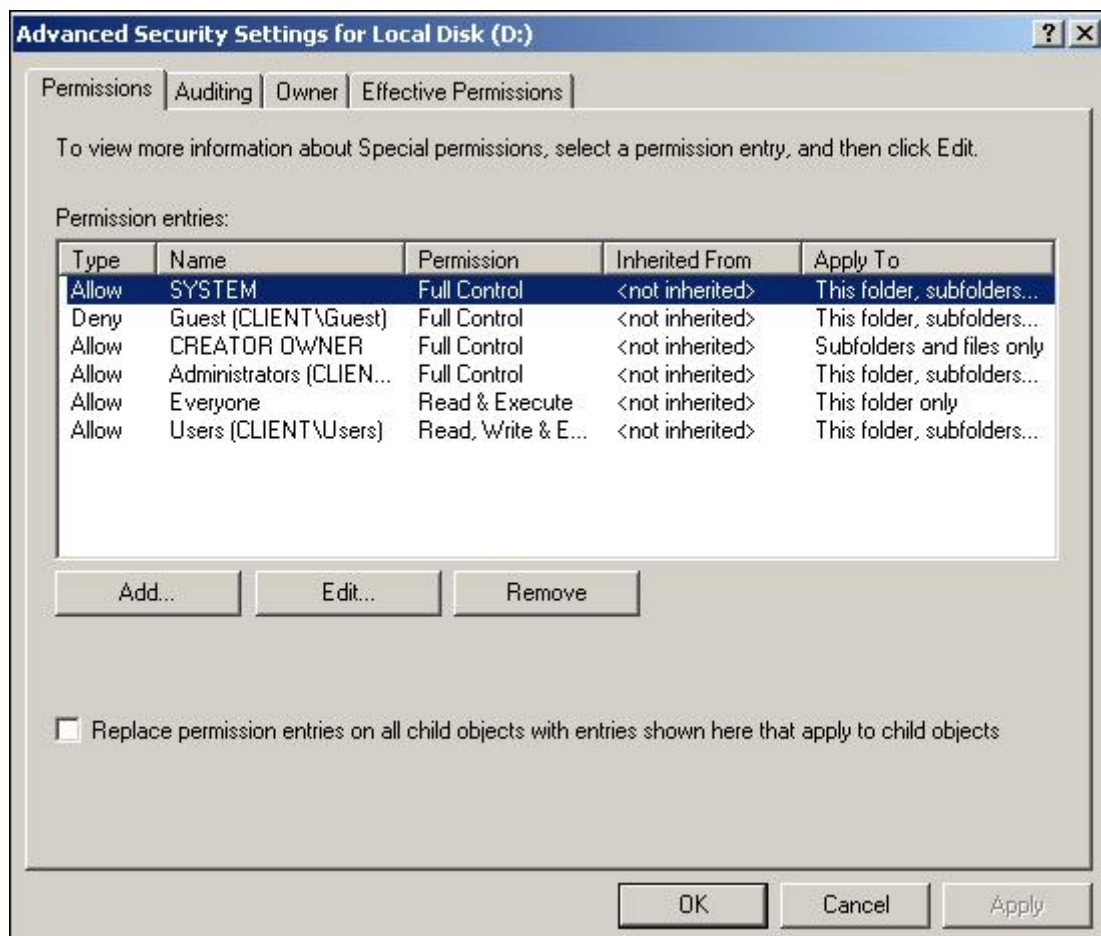
Change permissions

Take Ownership

( )

advanced

advanced



[www.Server4Arb.com](http://www.Server4Arb.com)

**auditing**

" "

**:administrator**

**1. Type : allow**

**2. Name : administrator**

**3. Permission : Full control**

**4. Inherited from : < not inherited <**

**5. Apply to : This folder , subfolders , and files**

( )

[www.Server4Arb.com](http://www.Server4Arb.com)

permissions

"

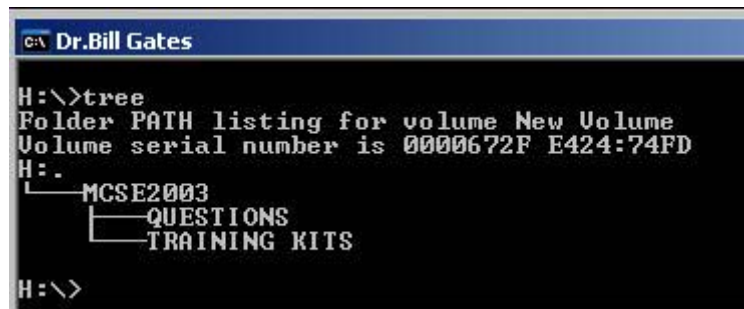
"

inheriting

.parent directory "

"

:

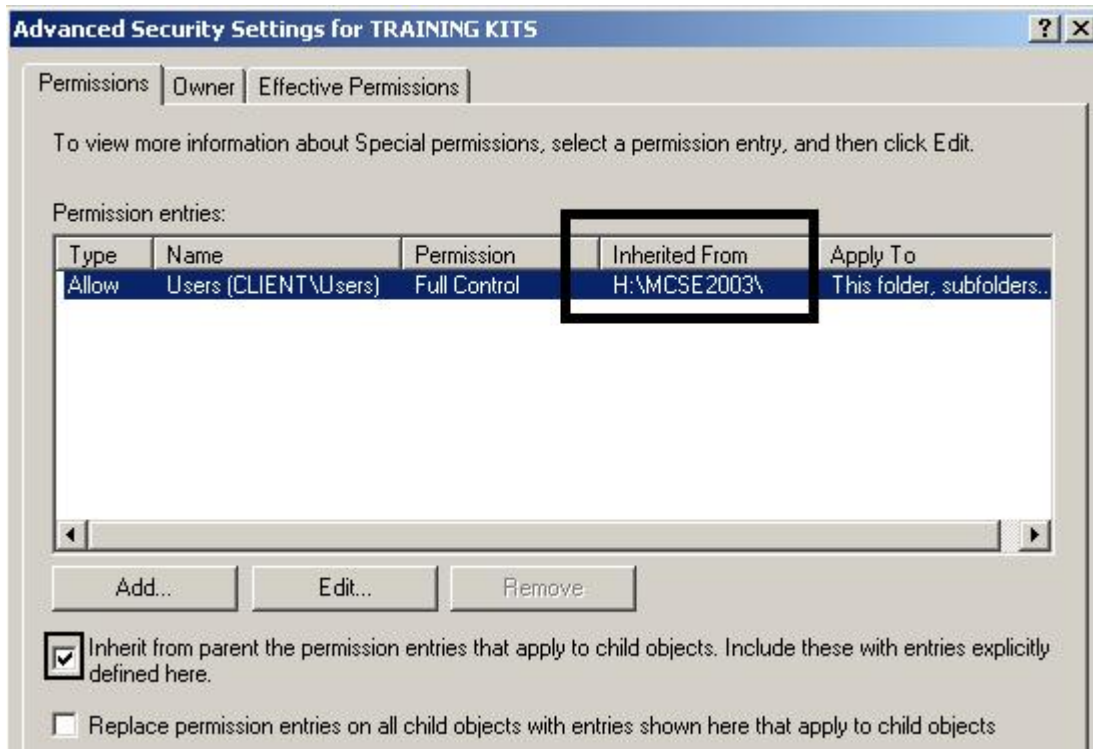


```
C:\> tree
Folder PATH listing for volume New Volume
Volume serial number is 0000672F E424:74FD
H:
├── MCSE2003
│   ├── QUESTIONS
│   └── TRAINING KITS
H:\>
```

MCSE2003

.parent Directory

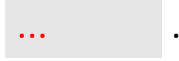
:



**MCSE2003**

**.Effective permissions "**

[www.Server4Arb.com](http://www.Server4Arb.com)



**allow**

**deny**

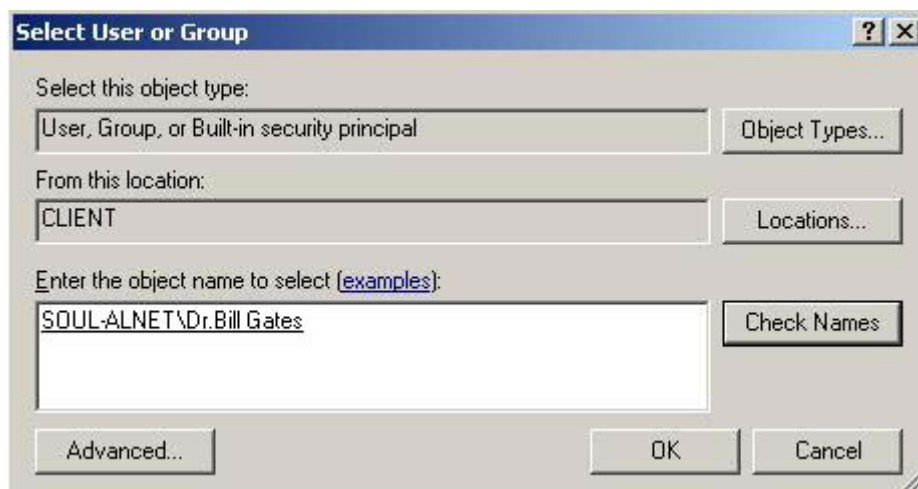
:

## Effective Permissions tab



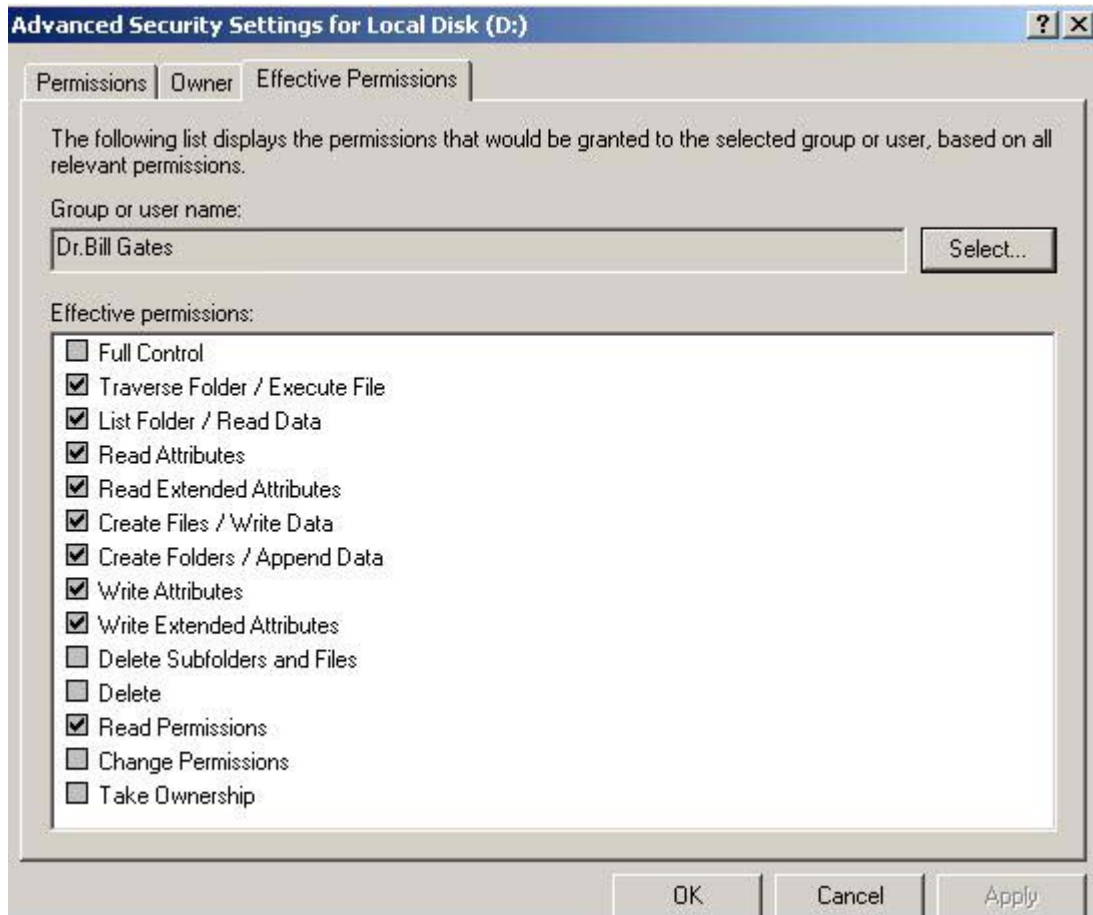
:

## select





:



:

## Auditing

**cacsl**

**runas**

```
C:\WINDOWS\system32>cacls /?
Displays or modifies access control lists (ACLs) of files

CACLS filename [/I] [/E] [/C] [/G user:perm] [/R user [...]]
[P user:perm [...]] [/D user [...]]
filename      Displays ACLs.
/I            Changes ACLs of specified files in
             the current directory and all subdirectories.
/E           Edit ACL instead of replacing it.
/C           Continue on access denied errors.
/G user:perm  Grant specified user access rights.
             Perm can be: R Read
                   W Write
                   C Change (write)
                   F Full control
/R user       Revoke specified user's access rights (only valid with /E).
/P user:perm  Replace specified user's access rights.
             Perm can be: N None
                   R Read
                   W Write
                   C Change (write)
                   F Full control
/D user       Deny specified user access.

Wildcards can be used to specify more than one file in a command.
You can specify more than one user in a command.

Abbreviations:
CI - Container Inherit.
    The ACE will be inherited by directories.
OI - Object Inherit.
    The ACE will be inherited by files.
IO - Inherit Only.
    The ACE does not apply to the current file/directory.

C:\WINDOWS\system32>
```

:



```
cmd (running as CLIENT\administrator)
D:\>cacls winnt.txt
D:\winnt.txt BUILTIN\Administrators:F
              <Account Domain not found>R
              NT AUTHORITY\SYSTEM:F
              BUILTIN\Users:(special access:)
                READ_CONTROL
                SYNCHRONIZE
                FILE_GENERIC_READ
                FILE_GENERIC_WRITE
                FILE_GENERIC_EXECUTE
                FILE_READ_DATA
                FILE_WRITE_DATA
                FILE_APPEND_DATA
                FILE_READ_EA
                FILE_WRITE_EA
                FILE_EXECUTE
                FILE_READ_ATTRIBUTES
                FILE_WRITE_ATTRIBUTES
D:\>
```

. F , R

:

Value	Description
n	None
r	Read
w	Write
c	Change (Write)
f	Full Control

**F**

**system**

:

```
c:\ cmd (running as CLIENT\administrator)
D:\>caccls winnt.txt /G Users:F
Are you sure (Y/N)?y
processed file: D:\winnt.txt
D:\>
```

:

```
c:\ cmd (running as CLIENT\administrator)
D:\>caccls winnt.txt /D Dr.Bill Gates
Are you sure (Y/N)?y
processed file: D:\winnt.txt
D:\>
```

**Dr.Bill Gates**  
**.access is denied**

:

```
c:\ cmd (running as CLIENT\administrator)
D:\>caccls winnt.txt /D Dr.Bill Gates administrator
Are you sure (Y/N)?y
processed file: D:\winnt.txt
D:\>
```

**Dr.Bill Gates, administrator**

:

```
cmd (running as CLIENT\administrator)
D:\>cacls *.* /G Users:F
Are you sure (Y/N)?y
processed dir: D:\03-08-2004
processed file: D:\0349.exe
processed dir: D:\15-09-2004
processed dir: D:\22-10-2004
processed file: D:\5.htm
processed dir: D:\Adobe acrobat 6.0 PRO
processed dir: D:\after backup
processed dir: D:\arabsecure
processed dir: D:\C code
processed dir: D:\dm
processed dir: D:\DOCS
processed file: D:\efinfo.exe
processed dir: D:\I386
processed file: D:\IIS.exe
processed dir: D:\ISA
processed dir: D:\isa1
processed dir: D:\john
processed file: D:\livekd.exe
processed dir: D:\Magic_folder
processed file: D:\mawsoal.pdf
processed file: D:\mawsu3a.pdf
processed dir: D:\MCSE2003
processed file: D:\My startup Template.inf
processed file: D:\nc.exe
processed file: D:\netdom.exe
processed dir: D:\NTFSDOS
processed dir: D:\RECYCLER
processed file: D:\redhat.pdf
```

" "

Txt.\*

.D

.txt

:

```
Dr.Bill Gates
H:\>cacls h:\MCSE2003\*.* /g users:F /t
Are you sure (Y/N)?y
processed dir: h:\MCSE2003\QUESTIONS
processed dir: h:\MCSE2003\TRAINING KITS
H:\>
```

. NTFS permissions

**auditing**

. ( )  
)

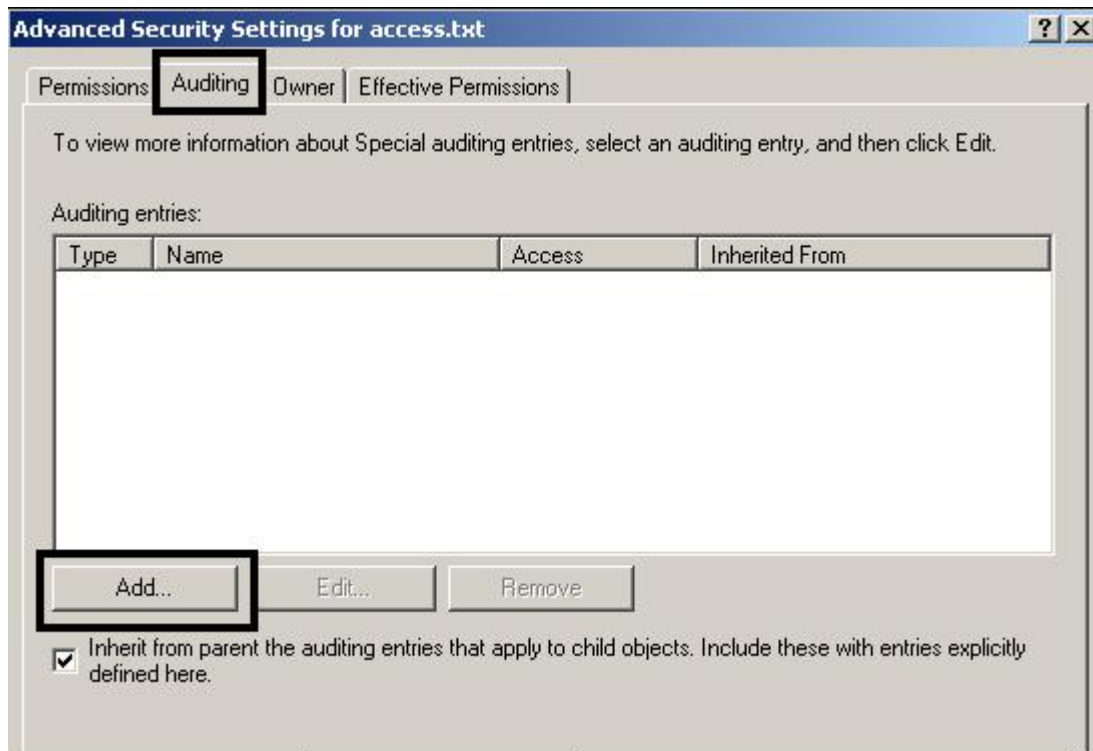
(

**NTFS partition**

.( access.txt )  
.properties

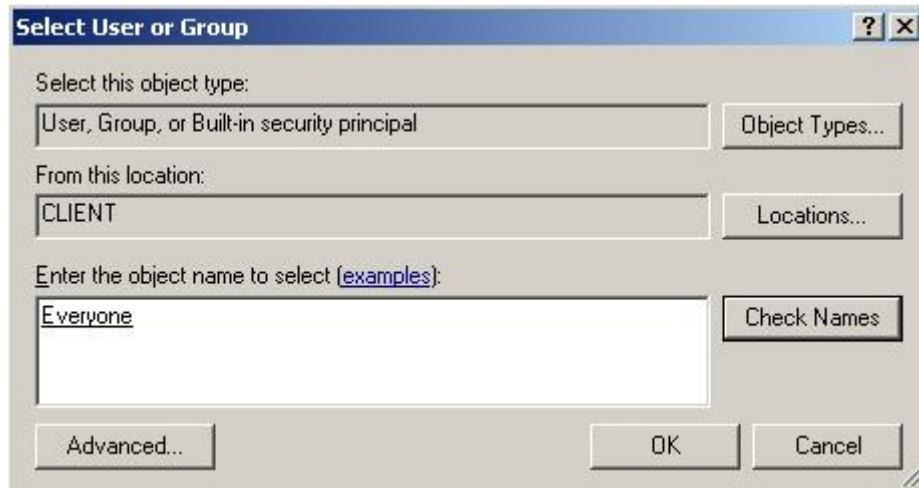
:

**advanced**



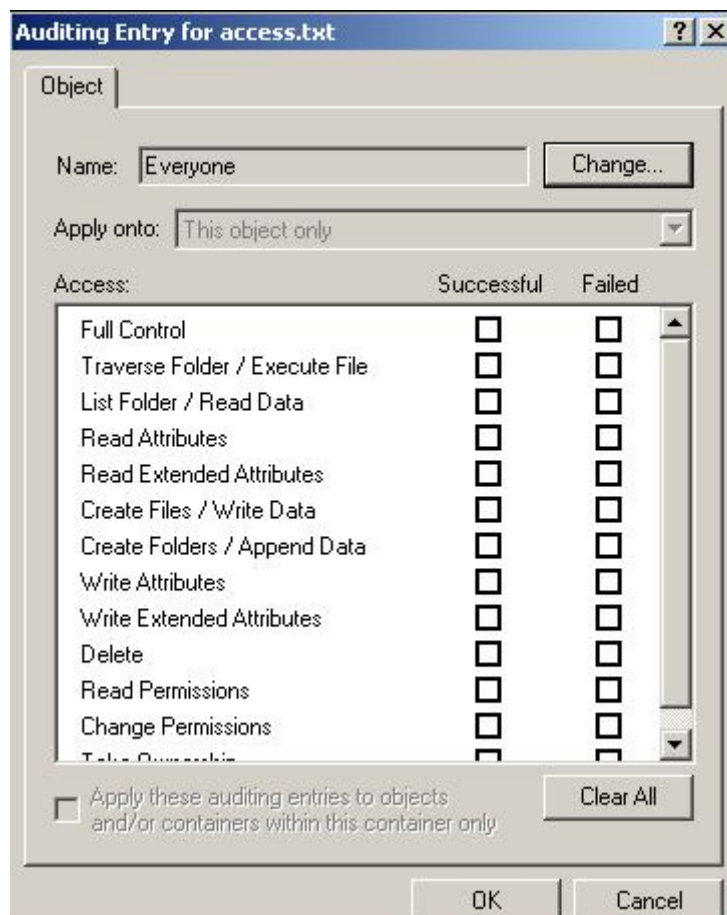
## add auditing

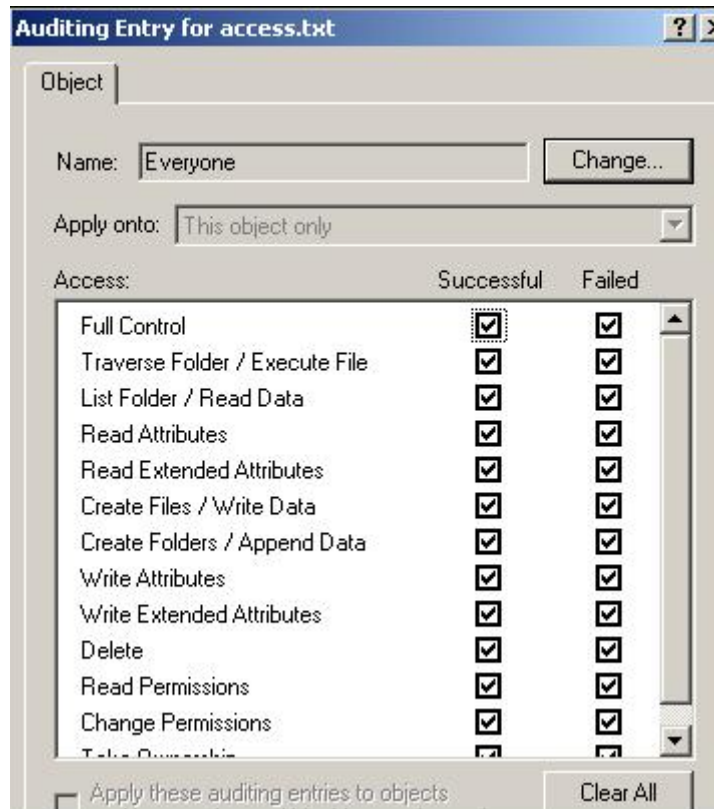
:



## everyone

:







:



**.local policy editor**

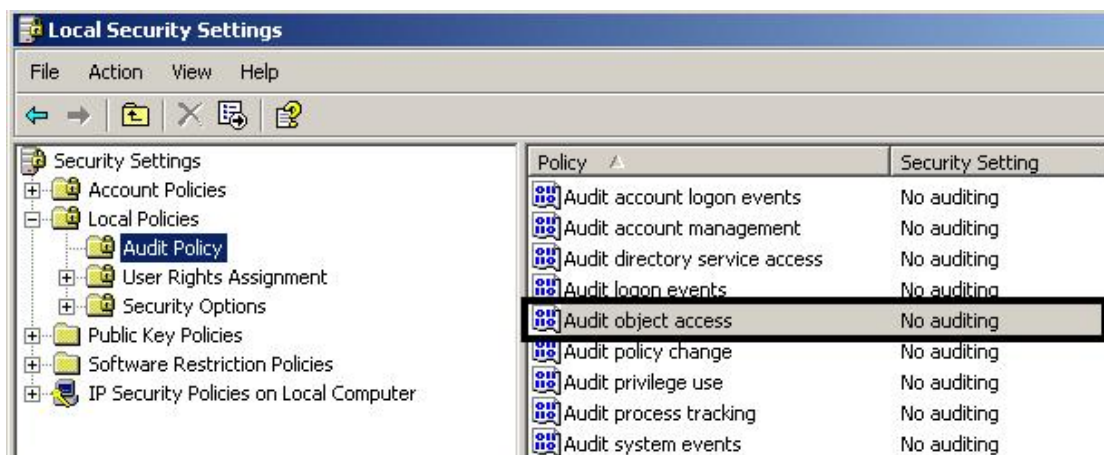
**domain group policy**

**group policy**

:

**Start << Run << secpol.msc**

:



[www.Server4Arb.com](http://www.Server4Arb.com)

**audit object access**

**audit policy**

:



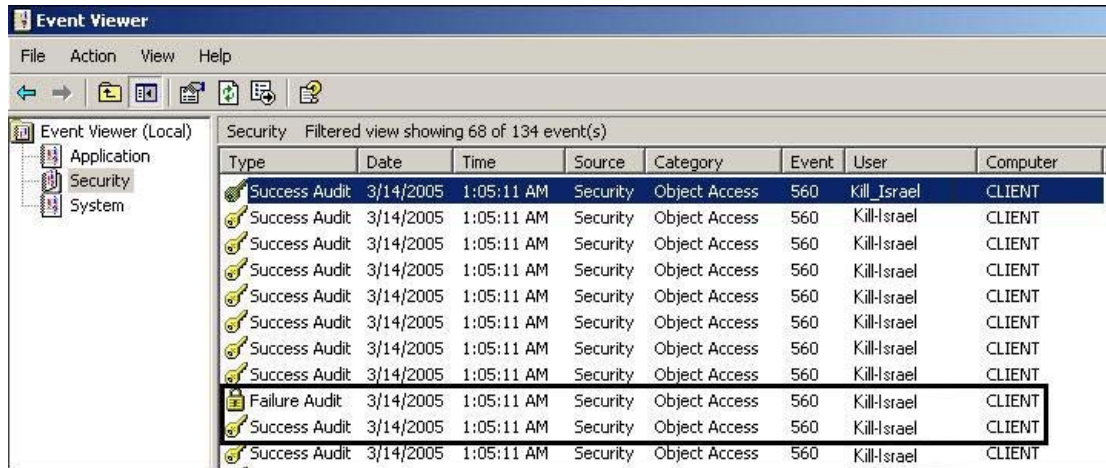
**event viewer**

**security**

:

Start < Run < eventvwr

: 560 security



Type	Date	Time	Source	Category	Event	User	Computer
Success Audit	3/14/2005	1:05:11 AM	Security	Object Access	560	Kill_Israel	CLIENT
Success Audit	3/14/2005	1:05:11 AM	Security	Object Access	560	Kill-Israel	CLIENT
Success Audit	3/14/2005	1:05:11 AM	Security	Object Access	560	Kill-Israel	CLIENT
Success Audit	3/14/2005	1:05:11 AM	Security	Object Access	560	Kill-Israel	CLIENT
Success Audit	3/14/2005	1:05:11 AM	Security	Object Access	560	Kill-Israel	CLIENT
Success Audit	3/14/2005	1:05:11 AM	Security	Object Access	560	Kill-Israel	CLIENT
Success Audit	3/14/2005	1:05:11 AM	Security	Object Access	560	Kill-Israel	CLIENT
Failure Audit	3/14/2005	1:05:11 AM	Security	Object Access	560	Kill-Israel	CLIENT
Success Audit	3/14/2005	1:05:11 AM	Security	Object Access	560	Kill-Israel	CLIENT
Success Audit	3/14/2005	1:05:11 AM	Security	Object Access	560	Kill-Israel	CLIENT



)

.(...

**access.txt**

**Kill-Israel**

.( )

Hack\_1Killer/

[Bill\\_Gaties@hotmail.com](mailto:Bill_Gaties@hotmail.com)

[Bill\\_Gates@maktoob.com](mailto:Bill_Gates@maktoob.com)

All rights reserved 2005

**Microsoft**  
**CERTIFIED**  
Systems Administrator

OR

**Microsoft**  
**CERTIFIED**  
Systems Engineer