

...

MCSE

.

:____

•

...

administrator

.guest

users

•

.

server operator

п

:task manager "

Options View Shu	t Down Help			
pplications Processes	Performance Netw	orking	Users	
Image Name	User Name	CPU	Mem Usage	
taskmgr.exe	Dr.Bill Gates	00	5,300 K	
NeroStartSmart.exe	Administrator	00	1,112 K	
cmd.exe	Administrator	00	88 K	
svchost.exe	SYSTEM	00	4,016 K	
Photoshop.exe	Dr.Bill Gates	00	7,048 K	
WINWORD.EXE	Dr.Bill Gates	00	2,420 K	
HDDlifePro.exe	Dr.Bill Gates	00	7,180 K	
ONENOTEM.EXE	Dr.Bill Gates	00	356 K	
spoolsv.exe	SYSTEM	00	4,708 K	
svchost.exe	LOCAL SERVICE	00	4,244 K	
acrotray.exe	Dr.Bill Gates	00	1,992 K	
point32.exe	Dr.Bill Gates	00	4,688 K	
svchost.exe	NETWORK SERVICE	00	2,716 K	
realsched.exe	Dr.Bill Gates	00	176 K	
InCDsrv.exe	SYSTEM	00	4,052 K	
svchost.exe	SYSTEM	00	19,728 K	
alg.exe	LOCAL SERVICE	00	3,300 K	
InCD.exe	Dr.Bill Gates	00	8,744 K	
explorer.exe	Dr.Bill Gates	00	16,508 K	-
Show processes fro	om all users	는 문	End Proces	55

process

Security context

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

.

Domain

system

•

" SVCHOST "

process

•

:

: tasklist

🕶 Dr.Bill Gates		<u>× 0 -</u>	۲
C:\>tasklist ∕svc		A	-
Image Name	PID	Services	
System Idle Process System	9 4	=====================================	
smss.exe csrss.exe	504 560	N/A N/A	
winlogon.exe	584	N/A	
Services.exe	628	Eventlog, PlugPlay PolicuAgent ProtectedStorage SamSs	
svchost.exe	788	DcomLaunch, TermService	
svchost.exe	852	RpcSs	
suchost.exe	888	AudioSrv, CryptSvc, Dhcp, dmserver, ERSvc, EventSystem, helpsvc, lanmanserver, lanmanworkstation, Netman, Nla, RasMan, Schedule, seclogon, SENS, SharedAccess, ShellHWDetection, srservice, TapiSrv, Themes, TrkWks, W32Time, winmgmt, wscsvc, wuauserv, WZCSUC	
svchost.exe	944	Dnscache	
svchost.exe	1020	LmHosts, RemoteRegistry, SSDPSRV, WebClient	
SDOOISV.exe MDM_FXF	1256	Spooler MDM	
nvsvc32.exe	1280	NUSuc	
snmp.exe	1316	SNMP	
wdfmgr.exe	1344	UMWdf	
alg.exe	1030	HLG NZO	
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	
DICLE.exe	388	N/H	
HDDlife eve	1092	N/A	
WINWORD, EXE	536	N/A	
cmd.exe	400	N/A	
tasklist.exe	1892	N/A	
wmiprvse.exe	172	N/A	
C:\>_			-

svchost Taskill Tasklist Task Manger

rpcSc

•

)

.

.Nla,rasman,W32Time

5



: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		
	Dr.Bill Gates	

:

C:∖>net user Kill-Israel 159357 ⁄add The command completed successfully.

:()

C:\>_

User name: Kill-Israel Password: 159357

Windows XP

.

:

: Dos

Professional

•

:

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

.logoff

.

Run



:





. access is denied





setup

•



:

windows installer

:

Start > Run > eventvwr

⇔ → 🗈 🖪 🚰 🗟	8						
Event Viewer (Local)	Application 221	Application 221 event(s)					
Application	Туре	Date	Time	Source	Cal 🔺		
-B Security	Information	01/09/2005	ص 03:29:52	MsiInstaller	Nor		
System	Warning	01/09/2005	ص 03:29:09	WinMgmt	Nor		
	A Warning	01/09/2005	ص 03:29:09	WinMgmt	Nor		
	Information	01/09/2005	ص 03:26:40	MsiInstaller	Noi		
	Error	01/09/2005	ص 03:26:08	MsiInstaller	Nor		
	Information	01/09/2005	ص 03:26:07	MsiInstaller	Nor		
	A Warning	01/09/2005	ص 03:23:56	WinMgmt	Nor		
	A Warning	01/09/2005	ص 03:23:56	WinMgmt	Nor		
	S Error	01/09/2005	ص 03:22:34	MsiInstaller	Nor		
	Information	01/09/2005	ص 03:17:38	EvntAgnt	Nor		
	A Warning	01/09/2005	ص 03:16:09	EvntAgnt	Nor		
	A Warning	01/09/2005	ص 03:16:09	EvntAgnt	Nor		
	Information	01/09/2005	ص 03:16:03	LoadPerf	Nor		
	Information	01/09/2005	ص 03:16:03	LoadPerf	Nor		
	Information	01/09/2005	ص 03:16:03	LoadPerf	Nor		
	Information	01/09/2005	ص 03:16:03	LoadPerf	Nor		
	Information	01/09/2005	ص 03:16:03	LoadPerf	No		
	(1) Information	01/00/2005	03-16-03	InadDarf	Alog		

ent Prop	erties			?
Event				
D <u>a</u> te:	01/09/2005	Source:	Msilnstaller	+
Time:	ص 03:26:08	Category:	None	
Typ <u>e</u> :	Error	Event ID:	11500	+
<u>U</u> ser:	SOUL-ALNE	T\Dr.Bill Ga	ates	
Compute	er: SOUL-ALNE	T		
Descript	ion:			
Product complet	: HDDlife Error e that installatior	1500. And before co	ther installation is in p ntinuing this one.	progress. You must
For more	e information, se o.microsoft.com	e Help and /fwlink/eve	Support Center at nts.asp.]	





registry



security

system restore

.

:

:

н

•

.

п

•

•

malfunction

•



secondary logon

:

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

🍇 Services (Local)			
Secondary Logon	Name A	Description	Status
	QoS RSVP	Provides n	
Pause the service	Remote Access Auto Connection Manager	Creates a	
	Remote Access Connection Manager	Creates a	Started
Description:	Remote Desktop Help Session Manager	Manages a	
Enables starting processes under	Remote Procedure Call (RPC)	Provides th	Started
alternate credentials. If this service is stopped, this type of logon access will be	Remote Procedure Call (RPC) Locator	Manages t	
unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.	Remote Registry	Enables re	
	Removable Storage		
	Routing and Remote Access	Offers rout	18
	Secondary Logon	Enables st	Started

.local system

runas

:

runas



cpl msc exe

runas



:

runas

•

secondary logon

.

: **Dos** /

🗪 Dr.Bill_Gaties		×
C:\>runas /? RUNAS USAGE:		_
RUNAS [[/noprof /user: <u< td=""><td>ile ¦ /profile] [/env] [/netonly]] serName> program</td><td></td></u<>	ile ¦ /profile] [/env] [/netonly]] serName> program	
RUNAS [[/noprof /smartca	ile ¦ /profile] [/env] [/netonly]] rd [/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.	
/prof 11e	This is the default.	
∕env ∕netonly	to use current environment instead of user's. 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	
∕user program	<pre></pre> <username> should be in form USER@DOMAIN or DOMAIN\USER command line for EXE. See below for examples</username>	
Examples:		
> runas /noprofi > runas /profile > runas /env /use	le /user:mymachine\administrator cmd /env /user:mydomain\admin "mmc zwindirz\system32\dsa.msc" er:user@domain.microsoft.com "notepad \"my file.txt\""	
NOTE: Enter use: NOTE: USER@DOMA NOTE: /profile	r's password only when prompted. IN is not compatible with /netonly. is not compatible with /netonly.	
c:\>		

•

: .

Start > Run > cmd

•

administrator

:

:

.

ex Dr.Bill Gates	
C:\Documents and Settings\Dr.Bill Gate <u>s</u> }runas /user:administrator cmd	
:	
🔤 Muslim_Hager - runas /user:administrator cmd	
<u>C:\Documents and Settings\Dr.Bill Gate</u> s>runas /user:administrator cmd Enter the password for administrator:	
:	
📾 cmd (running as CLIENT\administrator)	_ 🗆 ×

C:\WINDOWS\system32>

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

MSC

.

:

:

🔤 C:\WINDOWS\system32\cmd.exe - runas /user:administrator "mmc C:\WINDOWS\system32\diskmg	_ 🗆 ×
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 "CLIENI\administrator" RUNAS ERROR: Unable to run - cmd 1326: Logon failure: unknown user name or had password.	
C: \>	

disabled



.()

•

guest

Server operator

secondary

logon

•

:

runas

•

users rights

•

.(XP

•

) group policy

:

group policy

Start > Run > gpedit.msc

•

:

🚡 Group Policy		
File Action View Help		
🗊 Local Computer Policy	Policy A	Security Setting
Computer Configuration General Software Settings General Windows Settings	Computer from the network Computer from the network Computer from the network Computer from the operating system Computer from the operating system Computer from the operating system	Everyone,Administrators,L
Scripts (Startup/Shutdown)	Adjust memory quotas for a process	LOCAL SERVICE, NETWOR
	Back up files and directories	Administrators, Backup Ope
⊕	Change the system time	Administrators,Power User
E 🔁 Security Options	腾이Create a pagefile 양이Create a token object	Administrators
Gold Key Folicies Software Restriction Policies The Security Policies on Local (Create global objects	Administrators, INTERACTI
🗉 🧰 Administrative Templates	B Debug programs	Administrators
User Configuration Image Software Settings	Deny access to this computer from the network Deny logon as a batch job	SUPPORT_388945a0,Gues
🕀 🧰 Windows Settings	BDeny logon as a service	
Administrative Templates	B Deny logon locally	SUPPORT_388945a0,Gues



.

group policy

Start > Run > gpedit.msc

:

.

.

Change the system time



:

hange the system time Properties	<u>?</u> ×
Local Security Setting	
Change the system time	
Administrators Power Users	
Add User or Group Remove	

Power Users administrator



Power users

•

ш

.

add User or

	:	Gre
erties	<u>? ×</u>	
ne		
	ne	ne

"

Select Users or Groups	<u>? ×</u>
Select this object type:	
Users or Built-in security principals	Object Types
From this location:	
CLIENT	Locations
Enter the object names to select (<u>examples</u>): Authenticated Users	Check Names
Advanced	OK Cancel

:

check names

•

Users

.group policy

:

:

Start < Run < gpupdate /force

🔤 C:\WINDOW5\system32\gpupdate.exe	
Refreshing Policy	
User Policy Refresh has completed. Computer Policy Refresh has completed.	
Certain Computer policies are enabled that can only run during startup.	
OK to Reboot?. (Y/N)	

•

.

.

•

" NTFS Format

•

.NTFS file system

fat,fat32

fat,fat32 partition

.

п

п

п

ntfs, C + D

partition 2

.

С

•

-:-

properties

:XP

D

















:

security

a.

	inistratorsj	
	Add	Remove
Permissions for Administrators	Allow	Deny
Full Control		
Modify		
Read & Execute		
List Folder Contents		
Read		
Write		
Coopiel Permissions		

:

security

Local Disk (C:)	Properties	? ×
General Tools	s Hardware	1
9	<u> </u>	
Туре:	Local Disk	
File system:	FAT32	



: NTFS FAT32

II

CONVERT c: /FS:NTFS

.

.NTFS FAT32 :C

NTFS

."

security

XP

Simple File Sharing user

Security

security interface

Start > Run > control

. folder options



view

:

:

.security

security

ACL / Access Control List

•

entries

merai 100is Haroware Shar	ing second [1	anora I
aroup or user names:	nistrators)	
CREATOR OWNER	1/1	
1 Everyone		
SYSTEM		
🕵 Users (CLIENT\Users)		
	A-1-1	Permette
	Auu	nemove
^D ermissions for Administrators	Allow	Deny
Full Control		
Modify		
Read & Execute		
List Folder Contents		
Read		
Write		
Coopiel Pormissions	F	
oi special permissions of for advar click Advanced.	iced settings,	Advanced

.() deny allow

2003

и и

•

•

•

•

:

:

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

)

(

уре	Name	Permission	Inherited From	Apply To
Jeny Allow Allow Allow	Guest (LLIENT Guest) CREATOR OWNER Administrators (CLIEN Everyone Users (CLIENT \Users)	Full Control Full Control Full Control Read & Execute Read, Write & E	<not inherited=""> <not inherited=""> <not inherited=""> <not inherited=""> <not inherited=""></not></not></not></not></not>	This folder, subfolders Subfolders and files only This folder, subfolders This folder only This folder, subfolders
Now	Users (CLIENT\Users)	Read, Write & E	<not inherited=""></not>	This folder, subfolders
6.4	a E40	Pamaua	1	
Au				

auditing

administrator

и и

•

1. Type : allow

•

2. Name : administrator

3. Permission : Full control

.

4. Inherited from : < not inherited <

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

.

()

•

•

•

п

permissions

•

inheriting

:

п

.parent directory "

🕶 Dr.Bill Gates	
H:\>tree Folder PATH listing for Volume serial number is H:. MCSE2003 QUESTIONS TRAINING KITS	volume New Volume 0000672F E424:74FD
H:\>	

:

MCSE2003

.parent Directory

ш

•

•

п

Type Name Allow Users	(CLIENT\Users)	Permission Full Control	Inherited From	Apply To
Allow Users	(UEIEN I \Users)	Full Control	EXMCSE2003	
			H.MMCJE2003V	I his folder, subfolders

MCSE2003

•

.Effective permissions "

.

... .

allow

.

.

deny

.

:

:

Effective Permissions tab

vanced Security Settings for Local Disk (D:)	?
Permissions Owner Effective Permissions	
The following list displays the permissions that would be granted to the sele relevant permissions.	ected group or user, based on all
Group or user name:	
	Select
Effective permissions:	
Full Control	
Traverse Folder / Execute File	
List Folder / Read Data	
Read Attributes	
Read Extended Attributes	
🗖 Create Files / Write Data	
Create Folders / Append Data	
Write Attributes	
Write Extended Attributes	
Delete Subfolders and Files	
Delete	
Read Permissions	
Change Permissions	
Taka Dumanshia	

select

Select this object type:	
User, Group, or Built-in security principal	Object Types
From this location:	
CLIENT	Locations
Enter the object name to select (<u>examples</u>):	
SOUL-ALNET\Dr.Bill Gates	Check Names
SOUL-ALNET\Dr.Bill Gates	Check Names
SOUL-ALNET\Dr.Bill Gates	Check Names

vanced Security Settings for Local Disk (D:)	?
ermissions Owner Effective Permissions	
The following list displays the permissions that would be granted to the selected relevant permissions.	group or user, based on all
Group or user name:	
Dr.Bill Gates	Select
, Effective permissions:	
Full Control	
I Traverse Folder / Execute File	
🗹 List Folder / Read Data	
Read Attributes	
Read Extended Attributes	
🗹 Create Files / Write Data	
Create Folders / Append Data	
☑ Write Attributes	
Write Extended Attributes	
Delete Subfolders and Files	
Delete	
Read Permissions	
Change Permissions	
Take Ownership	
ок (Cancel Apply

:

Auditing

•

:

cacls

•

.

runas

:

```
C:\WINDOWS\system32>cacls /?

Displays or modifies access control lists (ACLs) of files

CACLS filename [/T] [/E] [/C] [/C user:perm] [/R user [...]]

filename Displays ACLs.

/T 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

/P user Deny specified user access.

Wildcards can be used to specify more that one file in a command.

Mou can specify more that one file in a command.

Abbreviations:

C1 - Container Inherit.

The ACE will be inherited by directories.

01 - Object Inherit.

The ACE will be inherited by files.

10 - 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:\>cacls winnt.txt B:\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_GENERIC_EXECUTE FILE_READ_DATA FILE_APPEND_DATA FILE_WRITE_BA FILE_WRITE_BA 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

•

:

ex cmd (running as CLIENT\administrator)

D:\>cacls winnt.txt /G Users:F Are you sure (Y/N)?y processed file: D:\winnt.txt

:

D:/>

:

.



Dr.Bill Gates

.access is denied

```
cmd (running as CLIENT\administrator)
D:\>cacls 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)	_ 8 ×
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:\efsinfo.exe	
processed dir: D:\1386	
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:\mawsoa1.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	



н

п

.**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 KIT;	**			
H:\>				

. NTFS permissions



NTFS partition

:



•

advanced

	nore information about S	pecial auditing entries, select	an auditing entry, and then click Ec	dit.
diting	entries:			
уре	Name	Access	Inherited From	
Ac	ld	Remove		

add auditing

.

:

elect User or Group	<u>? ×</u>
Select this object type:	
User, Group, or Built-in security princi	pal Object Types
From this location:	
CLIENT	Locations
Enter the object name to select (<u>exam</u> Everyone	iples): Check Names
Advanced	OK Cancel

everyone

Name: Everyone Apply onto: This object only		Change
Apply onto: This object only		
		<u></u>
Access:	Successful	Failed
Full Control Traverse Folder / Execute File List Folder / Read Data Read Attributes Read Extended Attributes Create Files / Write Data Create Folders / Append Data Write Attributes Write Extended Attributes Delete Read Permissions Change Permissions		

)bject			
Name: Everyone		Change.	
Apply onto: This object only			-
Access:	Successful	Failed	
Full Control Traverse Folder / Execute File List Folder / Read Data Read Attributes Read Extended Attributes Create Files / Write Data Create Folders / Append Data Write Attributes Write Extended Attributes Delete Read Permissions Change Permissions			

.

•



:

local policy editor

domain group policy

.

:

:

group policy

Start << Run << secpol.msc

•

File Action View Help		
⇔ → € X 등 ĝ		
Security Settings	Policy A	Security Setting
Account Policies	Image: Audit account logon events Image: Audit account management Image: Audit directory service access Image: Audit logon events	No auditing No auditing No auditing No auditing
	👸 Audit object access	No auditing
Software Restriction Policies	Audit policy change Audit privilege use Audit privilege use Audit process tracking Audit system events	No auditing No auditing No auditing No auditing

audit object access audit policy

event viewer

security

Start < Run < eventvwr

: 560 security

•

🖥 Event Viewer								
File Action View H	Help							
(→) 🖻 🖬 😭	1 🗟 🛃							
Event Viewer (Local)	Security Filtered	l view showir	ng 68 of 134 ev	ent(s)				
Application	Туре	Date	Time	Source	Category	Event	User	Computer
Security	Success Audit	3/14/2005	1:05:11 AM	Security	Object Access	560	Kill_Israel	CLIENT
System	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

ine intopi	erties		?
vent			
Date:	3/14/2005 Sour	ce: Security	+
Time:	1:05:11 AM Cate	gory: Object Access	
Туре:	Success AL Even	nt ID: 560	+
User:	CLIENT\Kill-Israel		82
Descriptio	on:		

:

.(...

.

•

access.txt

.

•

Kill-Israel

•

)

)

:

Hack_1Killer/

Bill_Gaties@hotmail.com Bill_Gates@maktoob.com

•





.(



OR