



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ  
Τμήμα Πληροφορικής



Εργασία Μαθήματος **Ασφάλεια Πληροφοριακών Συστημάτων**

Άσκηση <<αριθμός άσκησης>>	<b>6η Άσκηση - Πολιτικές Ασφάλειας Λειτουργικών Συστημάτων</b>
Όνομα φοιτητή – Αρ. Μητρώου (όλων σε περίπτωση ομαδικής εργασίας)	Κουσουνής Κωνσταντίνος ρ14086
Ημερομηνία παράδοσης	8-1-2019

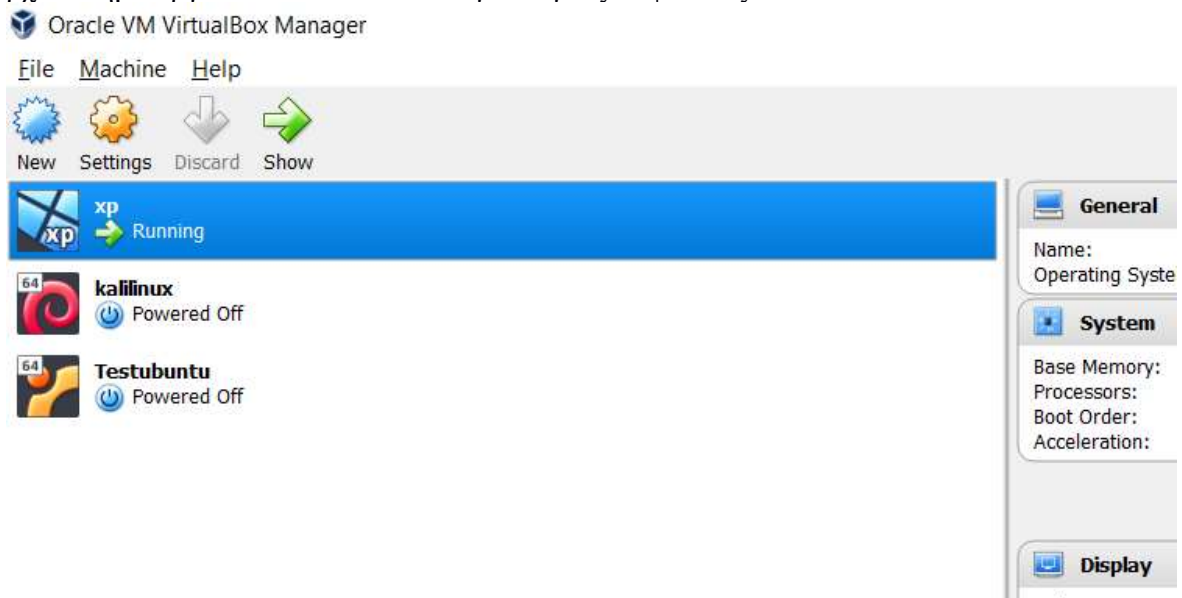


## Α) ΠΟΛΙΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ ΣΕ ΠΕΡΙΒΑΛΛΟΝ WINDOWS

Να εγκατασταθεί σε μια εικονική μηχανή μία έκδοση των windows. Να δημιουργηθούν στο λειτουργικό σύστημα τρεις λογαριασμοί χρηστών: admin, user και guest. Να ρυθμιστούν κατάλληλα οι πολιτικές ασφάλειας ώστε:

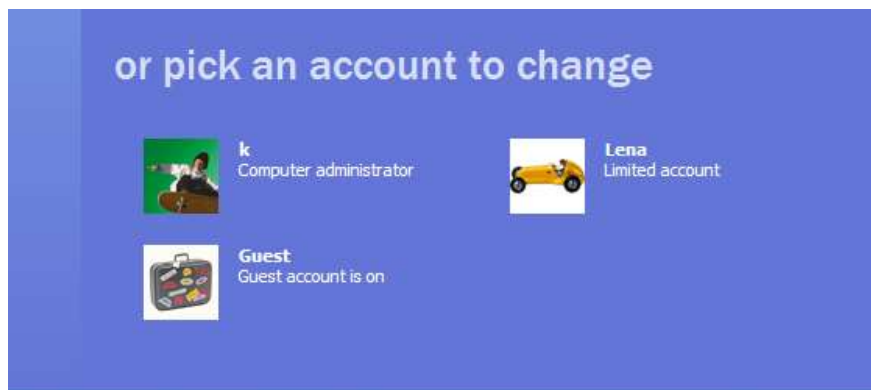
- 1) Όλοι οι κωδικοί πρόσβασης να είναι υποχρεωτικά τουλάχιστον 8 χαρακτήρες.
- 2) Για όλους τους χρήστες: Μετά από τρεις αποτυχημένες προσπάθειες εισόδου ο λογαριασμός να κλειδώνει για 10'.
- 3) Ο χρήστης user να μην έχει πρόσβαση στον πίνακα ελέγχου και στο command line
- 4) Ο χρήστης guest να έχει πρόσβαση μόνο στο διαδίκτυο (browser) και σε καμία άλλη εφαρμογή.

Αρχικά δημιουργώ ένα Virtual machine για λόγους ασφαλείας.

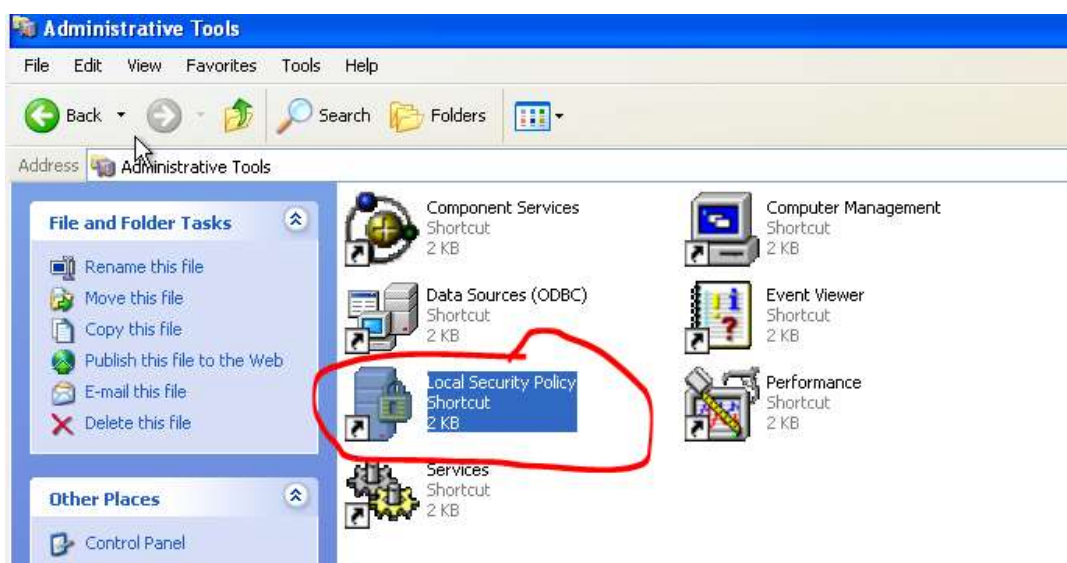
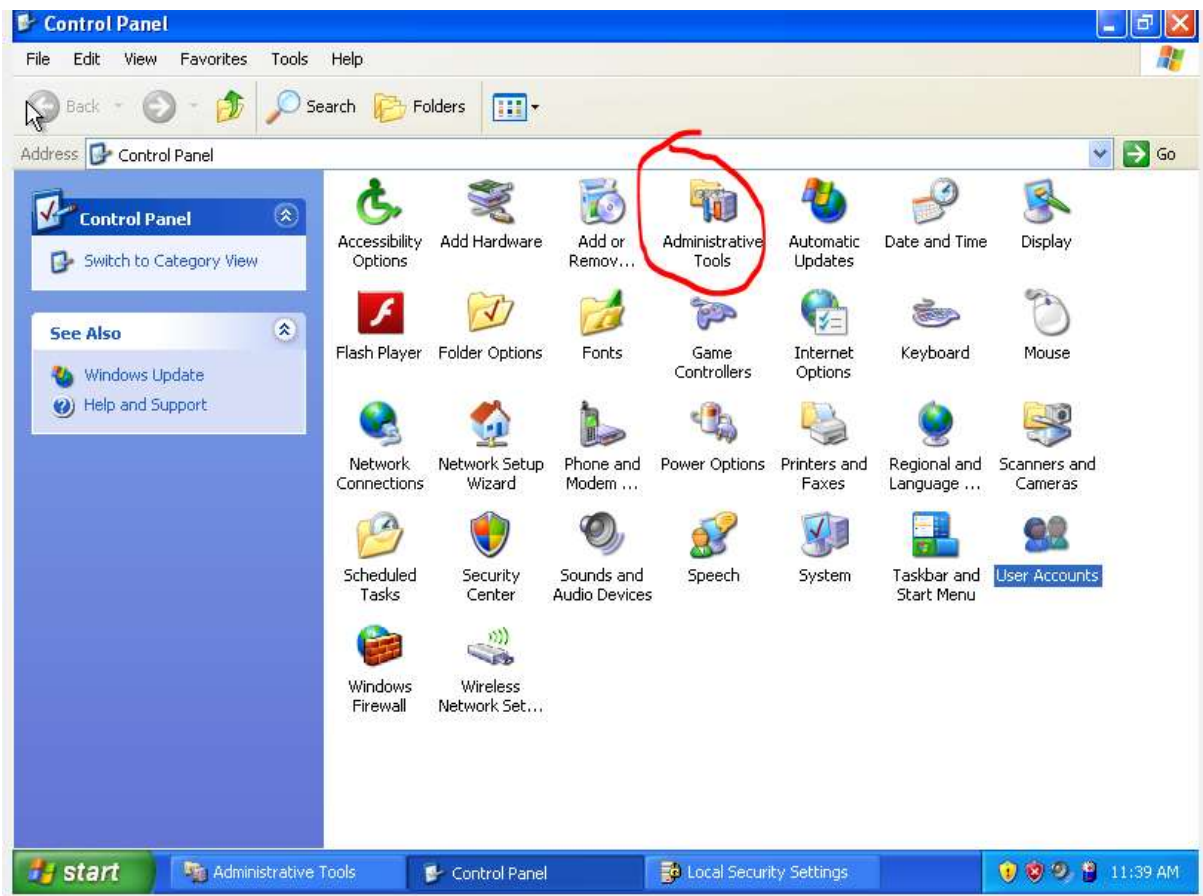




Το λειτουργικό σύστημα που έχω φτιάξει είναι Windows xp.  
Τρέχω το λειτουργικό μου και δημιουργώ δύο νέους χρήστες με διαφορετικά δικαιώματα  
Έναν **User** και ένα **Guest**.

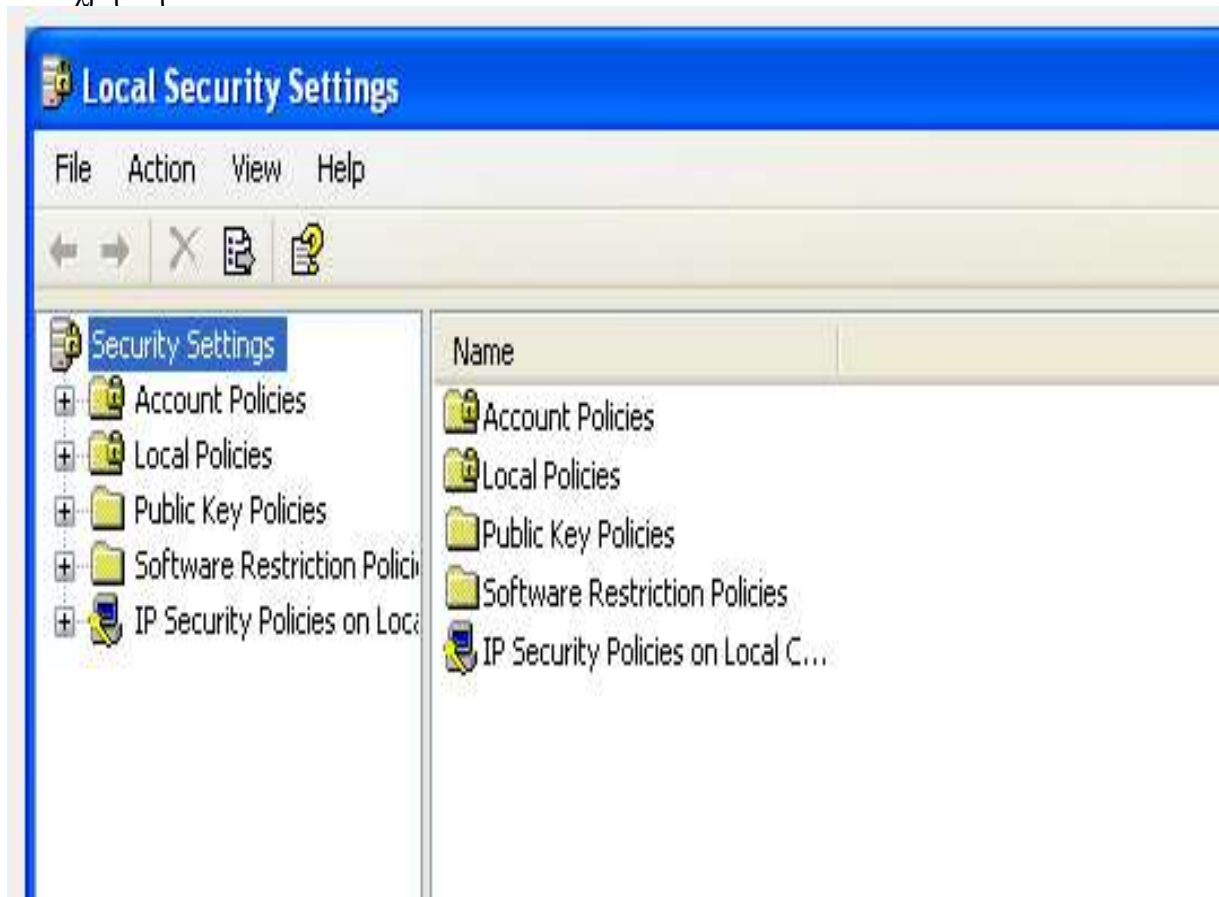


Ο guest είναι η Lena και έχω και έναν guest account στον οποίο μπαίνει ο οποιοδήποτε.  
Στην συνέχεια ανοίγω τον Πίνακα ελέγχου και ανοίγω το Εργαλεία διαχειριστή (Administrative Tools)

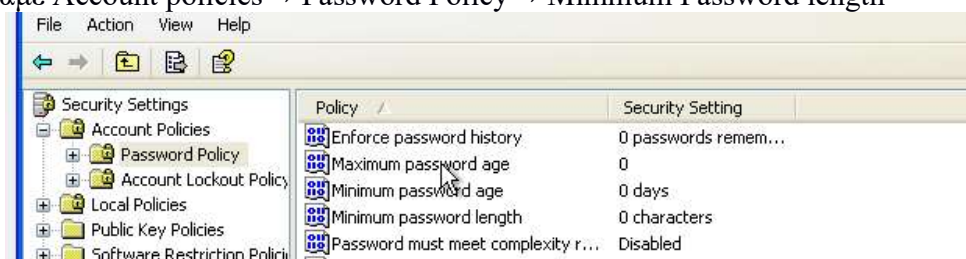




Εδώ ανοίγουμε το Local Security Policy για να ξεκινήσουμε να μοιράζουμε τα δικαιώματα σε κάθε χρήστη.



- 1) Όλοι οι κωδικοί πρόσβασης να είναι υποχρεωτικά τουλάχιστον 8 χαρακτήρες.  
Πάμε Account policies→ Password Policy→ Minimum Password length





Το ορίζουμε στους 8 χαρακτήρες και πατάμε apply.



olicy	Maximum password age	0 days
olicy	Minimum password age	0 days
olicy	Minimum password length	8 characters
olicy	Password must meet complexity requirements	Disabled
Local	Store password using reversible encryption	Disabled

Οπως βλέπουμε έχει ρυθμιστεί στους 8 χαρακτήρες.

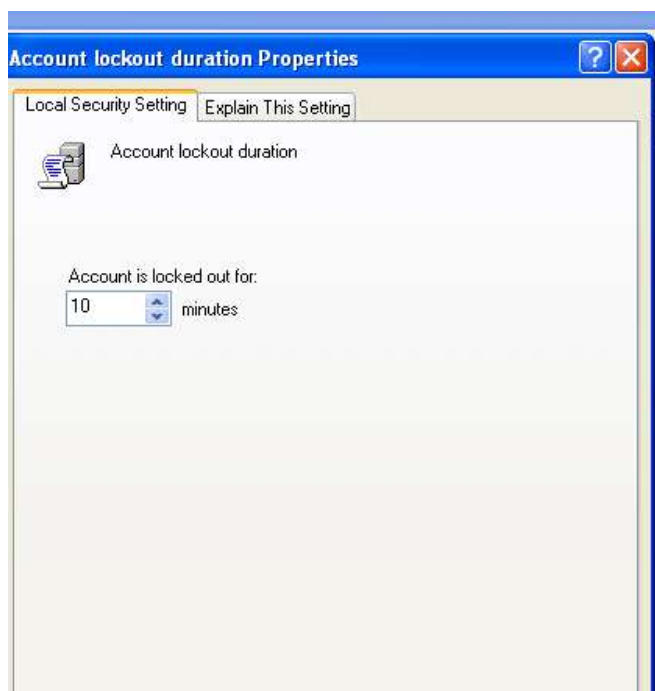
**2)Για όλους τους χρήστες: Μετά απο τρείς αποτυχημένες προσπάθειες εισόδου ο λογαριασμός να κλειδώνει για 10'.**

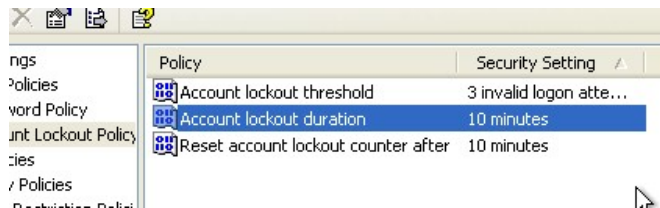
**Account Lockout Policy→ Account Lockout Threshold**



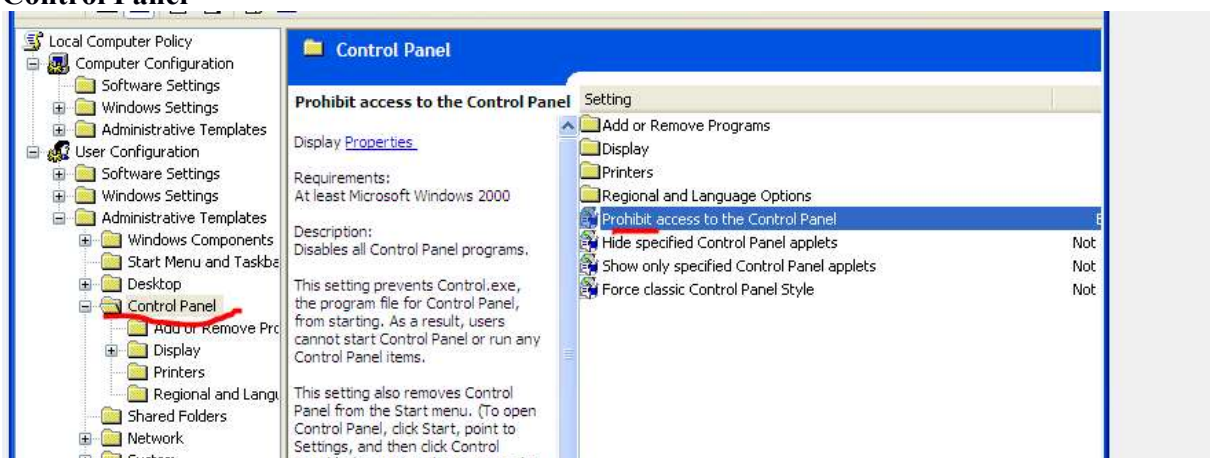
Το ορίζουμε για τρεις αποτυχημένες προσπάθειες και στην συνέχεια όριζομαι να παραμένει κλειδωμένος για 10 λεπτά.

Account lockout duration

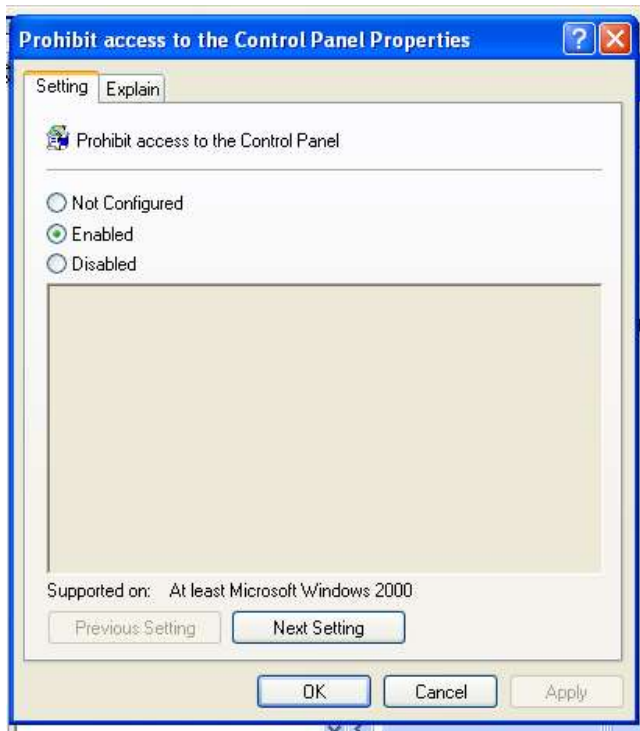




**3)Ο χρήστης user να μην έχει πρόσβαση στον πίνακα ελέγχου και στο command line.  
Αρχικά πάμε στο Group Policy→ User Configuration→ Administrative templates → Control Panel**







Πατάμε **Enabled** για να απαγορεύσουμε την πρόσβαση στους χρήστες.

Αντιστοίχα κανουμε την ίδια διαδικασία για το command prompt

**Αρχικά πάμε στο Group Policy → User Configuration → Administrative templates → System → Prevent Access to the Command prompt.**



The screenshot shows the Windows Group Policy console. The left pane displays the 'Local Computer Policy' tree, with 'System' selected under 'Administrative Templates'. The right pane shows the 'Prevent access to the command prompt' policy, which is currently disabled. The policy description states: 'Prevents users from running the interactive command prompt, Cmd.exe. This setting also determines whether batch files (.cmd and .bat) can run on the computer.' The requirements are 'At least Microsoft Windows 2000'. A note at the bottom states: 'Note: Do not prevent the computer from running batch files if the computer uses logon, logoff, startup, or shutdown batch file scripts, or for users that use Terminal Services.' The right pane also lists other system settings, such as 'User Profiles', 'Scripts', 'Ctrl+Alt+Del Options', 'Logon', 'Group Policy', 'Power Management', 'Internet Communication Management', 'Don't display the Getting Started welcome screen at logon', 'Century interpretation for Year 2000', 'Configure driver search locations', 'Code signing for device drivers', 'Custom user interface', 'Prevent access to the command prompt', 'Prevent access to registry editing tools', 'Run only allowed Windows applications', 'Don't run specified Windows applications', 'Turn off Autoplay', 'Restrict these programs from being launched from Help', 'Download missing COM components', 'Windows Automatic Updates', and 'Turn off Windows Update device driver search prompt'. The bottom status bar shows the 'start' button, the 'Group Policy' title, and the time '12:33 PM'.

**Group Policy**

File Action View Help

Local Computer Policy

- Computer Configuration
  - Software Settings
  - Windows Settings
  - Administrative Templates
- User Configuration
  - Software Settings
  - Windows Settings
  - Administrative Templates
    - Windows Components
    - Start Menu and Taskbar
    - Desktop
    - Control Panel
    - Shared Folders
    - Network
    - System
      - User Profiles
      - Scripts
      - Ctrl+Alt+Del Options
      - Logon
      - Group Policy
      - Power Management
      - Internet Communication Management

**System**

**Prevent access to the command prompt**

Display [Properties](#)

Requirements:  
At least Microsoft Windows 2000

Description:  
Prevents users from running the interactive command prompt, Cmd.exe. This setting also determines whether batch files (.cmd and .bat) can run on the computer.

If you enable this setting and the user tries to open a command window, the system displays a message explaining that a setting prevents the action.

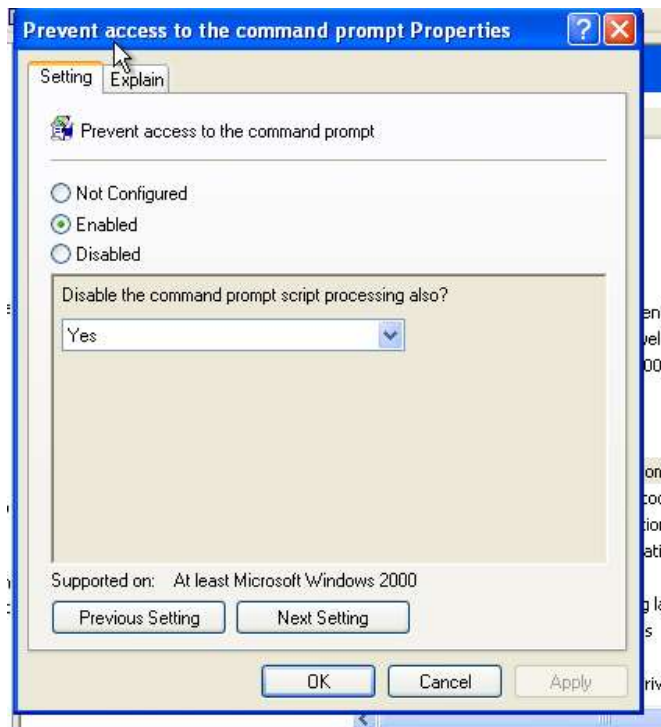
Note: Do not prevent the computer from running batch files if the computer uses logon, logoff, startup, or shutdown batch file scripts, or for users that use Terminal Services.

Setting

- User Profiles
- Scripts
- Ctrl+Alt+Del Options
- Logon
- Group Policy
- Power Management
- Internet Communication Management
- Don't display the Getting Started welcome screen at logon
- Century interpretation for Year 2000
- Configure driver search locations
- Code signing for device drivers
- Custom user interface
- Prevent access to the command prompt
- Prevent access to registry editing tools
- Run only allowed Windows applications
- Don't run specified Windows applications
- Turn off Autoplay
- Restrict these programs from being launched from Help
- Download missing COM components
- Windows Automatic Updates
- Turn off Windows Update device driver search prompt

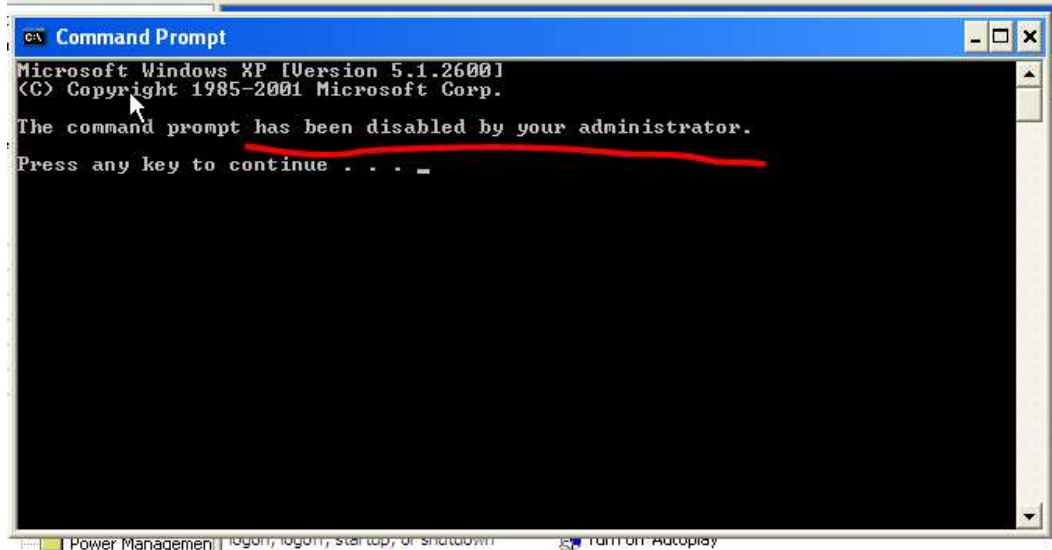
Extended Standard

start Group Policy 12:33 PM



Το κάνουμε enabled.

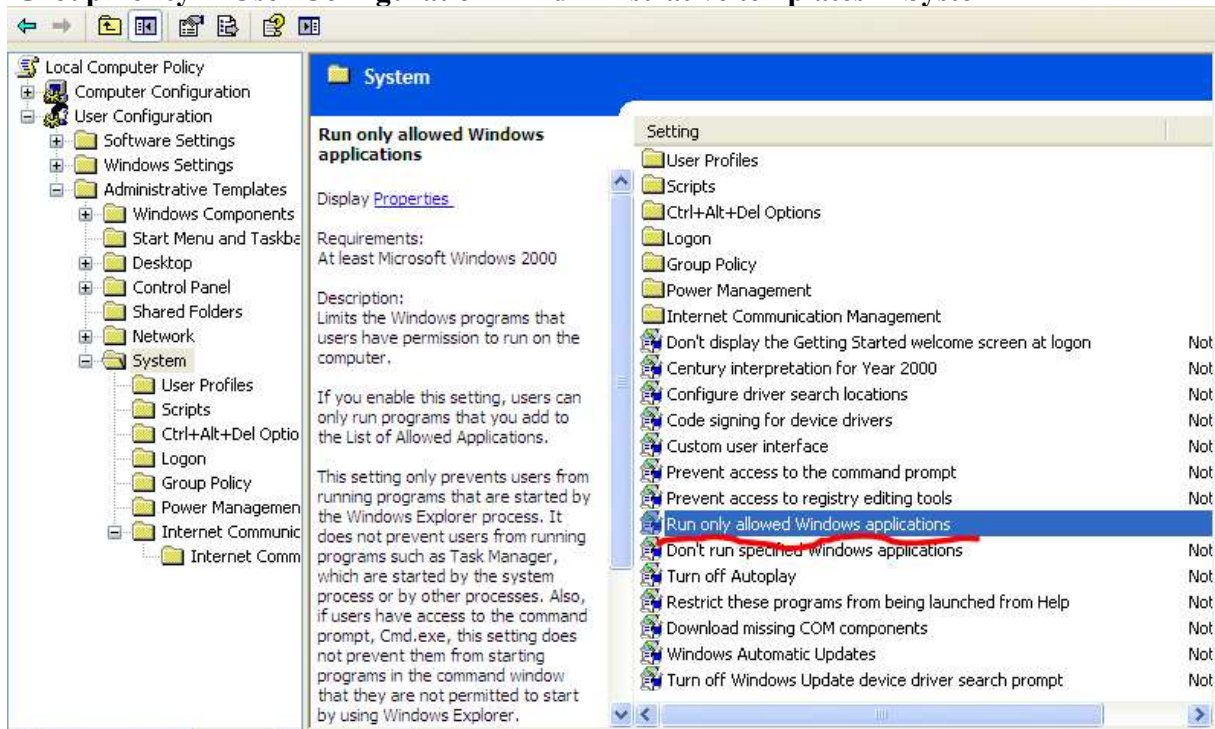
Όταν συνδεθούμε σαν χρήστης βλέπουμε οτι δεν μπορούμε να συνδεθούμε σαν χρήστης.



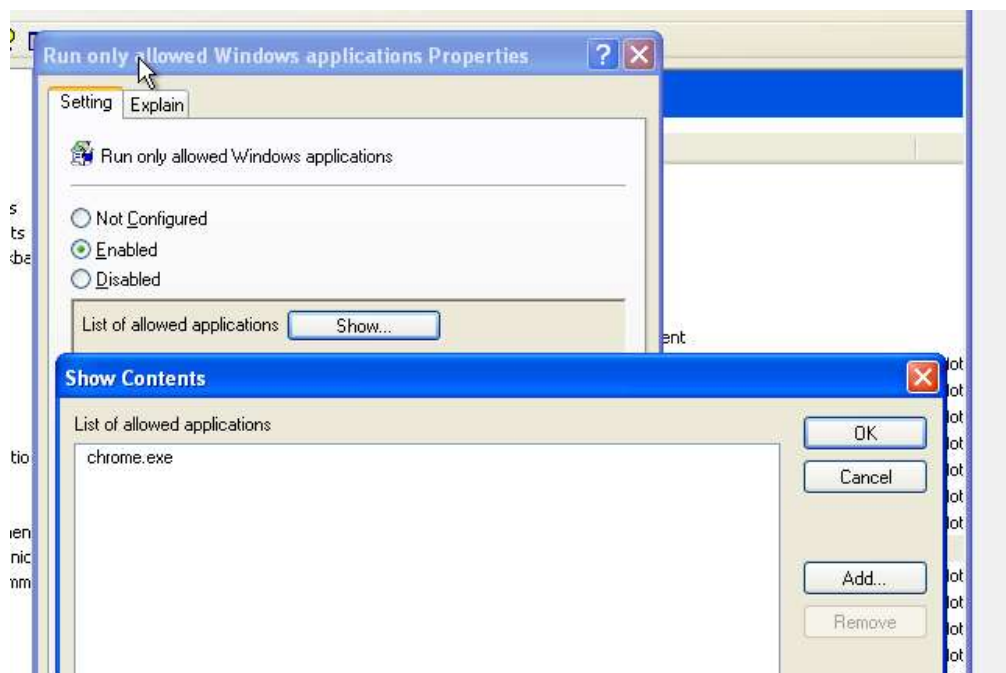


4)Ο χρήστης guest να έχει πρόσβαση μόνο στο διαδίκτυο (browser) και σε καμία άλλη εφαρμογή.

**Group Policy→ User Configuration→ Administrative templates →System**



**Run only allowed Windows applications**



Και πληκτολογούμε μόνο το αρχείο chrome.exe και είναι η μόνη εφαρμογή που μπορεί να τρέξει ο χρήστης.



Συνδέομαι σαν guest όπως βλέπουμε μας λέει οτι αυτη η λειτουργια δεν μπορεί να πραγματοποιηθεί και το μόνο που μπορούμε να κάνουμε είναι να μπούμε στο chrome και μονο στο internet.