

**ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ
ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ**

**Μάθημα: Ασφάλεια Πληροφοριακών και Επικοινωνιακών
Συστημάτων**

Εργαστηριακός Διδάσκων: Αναστασία Δούμα

ΑΣΚΗΣΗ 3:

**ΜΗΧΑΝΙΣΜΟΙ ΕΛΕΓΧΟΥ ΠΡΟΣΒΑΣΗΣ ΣΤΑ ΛΕΙΤΟΥΡΓΙΚΑ
ΣΥΣΤΗΜΑΤΑ WINDOWS ΚΑΙ UNIX**

Μέλοι ομάδας εργασίας:

Μαρία Θεοδωράκη Α.Μ.:321/2008041

Βερροιοπούλου Αθηνά Α.Μ.:321/2008011



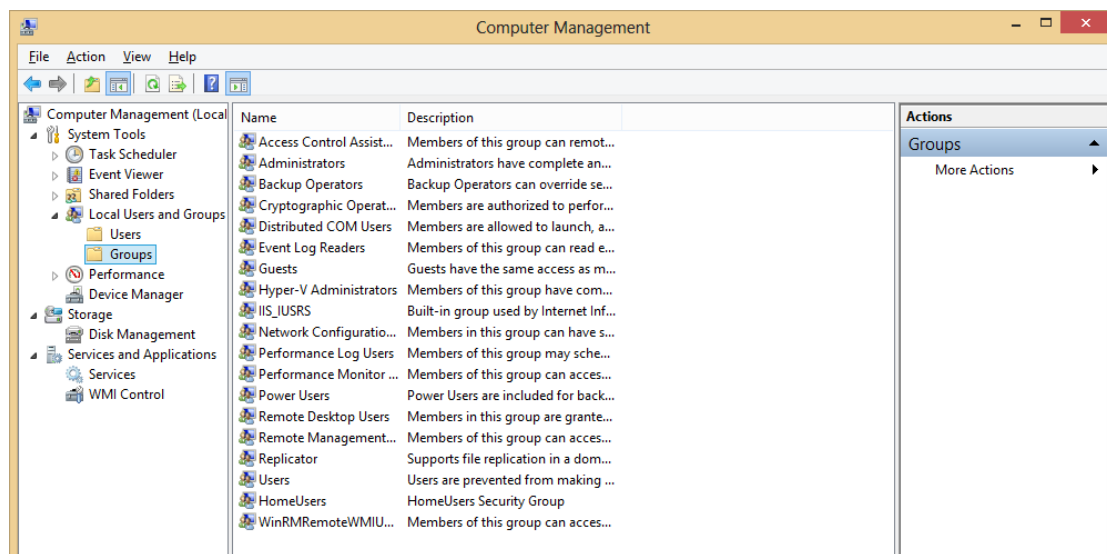
Ημερομηνία Παράδοσης: 21/04/2013

Στην πρώτη φάση της εργασίας θα πρέπει να εργαστείτε σε έναν υπολογιστή με Windows λειτουργικό σύστημα και κατά προτίμηση με Windows 7, στο οποίο θα έχετε δικαιώματα διαχειριστή.

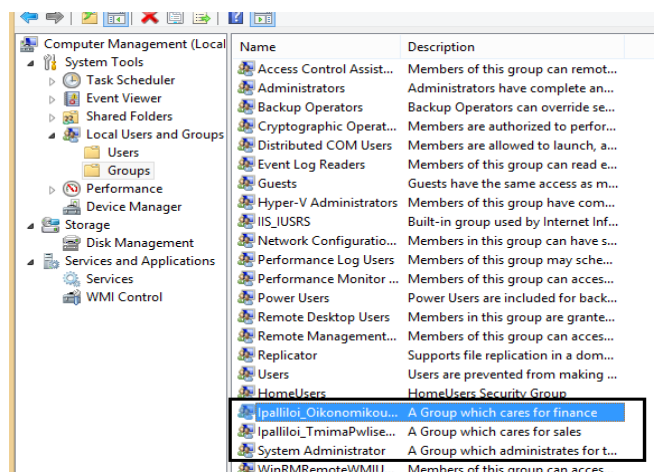
Εμείς κάναμε χρήση του Windows 7 Professional

Πριν διαμορφώσετε το σύστημα διαχείρισης αρχείων θα πρέπει να δημιουργήσετε 3 ομάδες χρηστών (μία για κάθε τμήμα της επιχείρησης)

Βλέπω τα Group στον υπολογιστή μου και επιλέγω στο Local Users and Groups to Groups

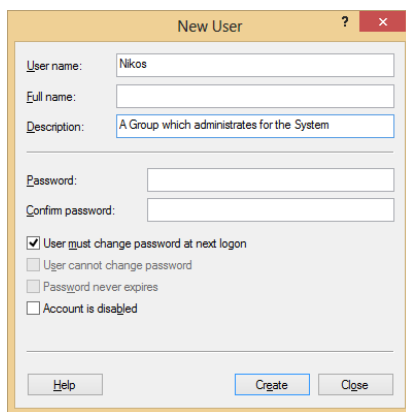
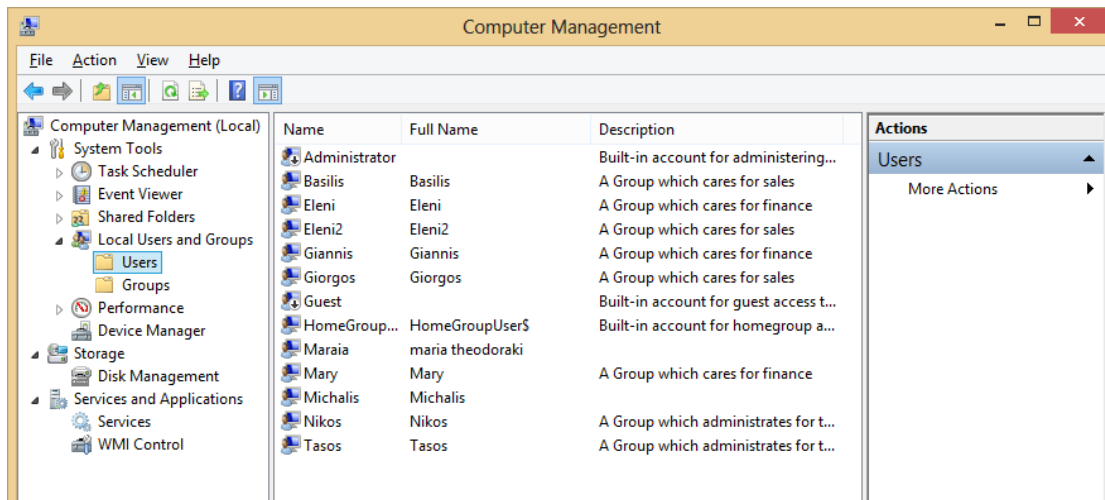


Φτιάχνω τις ομάδες : ipallilwnTmima pwlisewn, Ipalliloi oikonomikou tmimatos, Diaxeiristes sustimatos

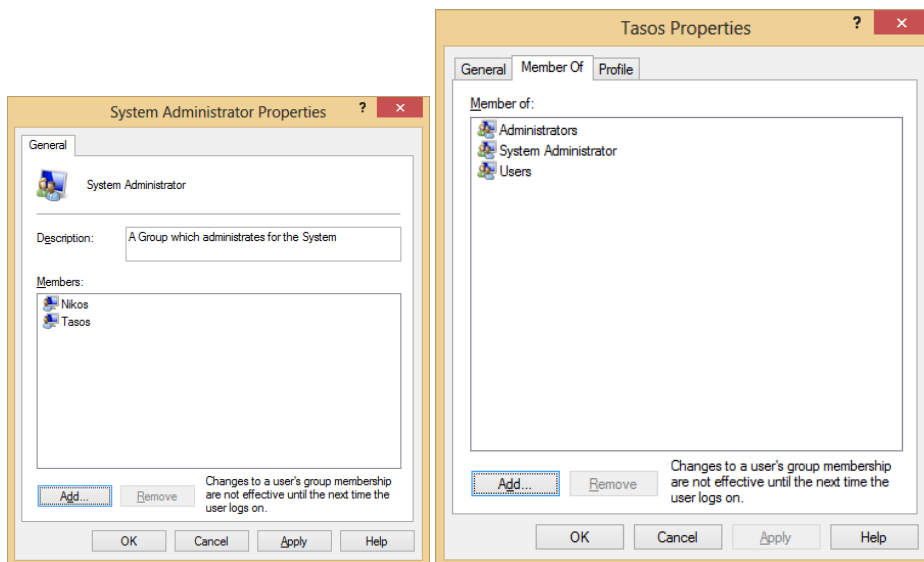


λογαριασμούς χρηστών για κάθε έναν από τους υπαλλήλους της εταιρείας.

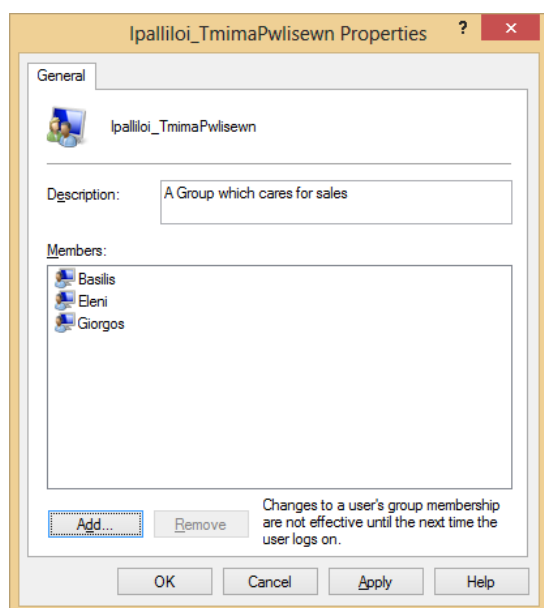
Η εταιρεία έχει 7 υπαλλήλους και τους δημιουργώ όπως φαίνετε παρακάτω:



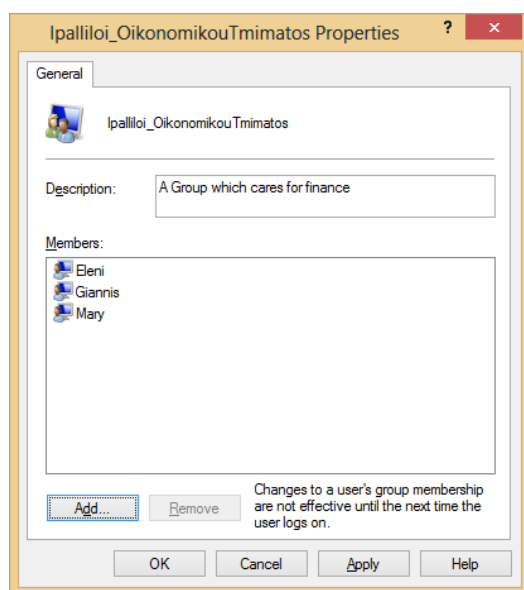
Tasos-Nikos διαχειριστές:



Τμήμα πωλήσεων Vasilis-Giorgos-Eleni



Οικονομικό τμήμα Giannis-Mary-Eleni



Επίσης κάθε χρήστης πρέπει να έχει την προσωπική του περιοχή αποθήκευσης αρχείων στην οποία θα έχει πλήρη δικαιώματα πρόσβασης μόνο ο ίδιος. Υλοποιήστε όλη την υποδομή που απαιτείται (οργάνωση φακέλων και καθορισμός δικαιωμάτων πρόσβασης) η οποία όμως να ικανοποιεί πλήρως τις απαιτήσεις ασφάλειας που περιγράφηκαν προηγουμένως. Χρησιμοποιήστε την εντολή icacls για να δημιουργήσετε αρχεία κειμένου με τις λίστες ελέγχου πρόσβασης που ορίσατε (ACLs).

Φτιάχνω τους φακέλους για κάθε περιοχή public,privet,perioxi και perioxi_xristi και παρακάτω πατάω dir για να δω την υπαρχή τους στο σύστημα.

```
Command Prompt

C:\Users\Maraia>dir
Volume in drive C has no label.
Volume Serial Number is 605A-5BD4

Directory of C:\Users\Maraia

18-Apr-13 07:41 PM <DIR>      .
18-Apr-13 07:41 PM <DIR>      ..
19-Feb-13 03:11 PM <DIR>      .m2
18-Feb-13 11:56 PM <DIR>      .nbi
23-Mar-13 06:49 PM <DIR>      .RapidMiner5
18-Apr-13 12:40 AM <DIR>      VirtualBox
14-Apr-13 04:20 AM <DIR>      Contacts
18-Apr-13 07:06 PM <DIR>      Desktop
16-Apr-13 02:17 AM <DIR>      Documents
17-Apr-13 05:40 PM <DIR>      Downloads
22-Feb-13 12:46 PM <DIR>      Dropbox
14-Apr-13 04:20 AM <DIR>      Favorites
14-Apr-13 04:21 AM <DIR>      Links
14-Apr-13 04:20 AM <DIR>      Music
18-Apr-13 07:39 PM <DIR>      Perioxi_Basilis
18-Apr-13 07:37 PM <DIR>      Perioxi_Diaxeiristes
18-Apr-13 07:38 PM <DIR>      Perioxi_Eleni
18-Apr-13 07:39 PM <DIR>      Perioxi_Giannis
18-Apr-13 07:40 PM <DIR>      Perioxi_Giorgos
18-Apr-13 07:40 PM <DIR>      Perioxi_Mary
18-Apr-13 07:40 PM <DIR>      Perioxi_Nikos
18-Apr-13 07:37 PM <DIR>      Perioxi_OikonomikoTmima
18-Apr-13 07:36 PM <DIR>      Perioxi_Pwliseis
18-Apr-13 07:40 PM <DIR>      Perioxi_Iasos
14-Apr-13 04:20 AM <DIR>      Pictures
18-Apr-13 07:27 PM <DIR>      Private_Diaxeiristes
18-Apr-13 07:26 PM <DIR>      Private_OikonomikoTmima
18-Apr-13 07:26 PM <DIR>      Private_Pwliseis
18-Apr-13 07:20 PM <DIR>      Public_Pwliseis
18-Apr-13 07:21 PM <DIR>      Public_Diaxeiristes
18-Apr-13 07:21 PM <DIR>      Public_OikonomikoTmima
14-Apr-13 04:21 AM <DIR>      Saved Games
14-Apr-13 04:21 AM <DIR>      Searches
14-Apr-13 04:20 AM <DIR>      Videos
28-Mar-13 04:41 PM <DIR>      VirtualBox VMs
               0 File(s)              0 bytes
```

Τώρα πρέπει να βάλω δικαιώματα στους φακέλους που δημιουργήσαμε σε αντιστοιχία με το κάθε τμήμα. Αυτό γίνεται με την εντολή icacls <path> /grant <tmima>:F

Για τα public του κάθε τμήματος κάνω τα παρακάτω:

```
Command Prompt

C:\Users\Maraia>clear
'clear' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Maraia>icacls C:\Users\Maraia\Public_Pwliseis /grant Ipalliloi_TmimaPwliseis:F
processed file: C:\Users\Maraia\Public_Pwliseis
Successfully processed 1 files; Failed processing 0 files

C:\Users\Maraia>icacls C:\Users\Maraia\Public_Pwliseis /grant Ipalliloi_OikonomikouTmimatos:F
processed file: C:\Users\Maraia\Public_Pwliseis
Successfully processed 1 files; Failed processing 0 files

C:\Users\Maraia>icacls C:\Users\Maraia\Public_Pwliseis /grant System_Administrator:F
processed file: C:\Users\Maraia\Public_Pwliseis
Successfully processed 1 files; Failed processing 0 files

C:\Users\Maraia>
```

```
Command Prompt

C:\Users\Maraia>icacls C:\Users\Maraia\Public_Pwliseis /grant System_Administrator:F
processed file: C:\Users\Maraia\Public_Pwliseis
Successfully processed 1 files; Failed processing 0 files

C:\Users\Maraia>icacls C:\Users\Maraia\Public_OikonomikoTmima /grant Ipalliloi_TmimaPwliseis:F
processed file: C:\Users\Maraia\Public_OikonomikoTmima
Successfully processed 1 files; Failed processing 0 files

C:\Users\Maraia>icacls C:\Users\Maraia\Public_OikonomikoTmima /grant Ipalliloi_OikonomikouTmimatos:F
processed file: C:\Users\Maraia\Public_OikonomikoTmima
Successfully processed 1 files; Failed processing 0 files

C:\Users\Maraia>icacls C:\Users\Maraia\Public_OikonomikoTmima /grant System_Administrator:F
processed file: C:\Users\Maraia\Public_OikonomikoTmima
Successfully processed 1 files; Failed processing 0 files

C:\Users\Maraia>
```

```
Command Prompt
Successfully processed 1 files; Failed processing 0 files
C:\Users\Maraia>icacls C:\Users\Maraia\Public_Diaxeiristes /grant System_Administrator:F
processed file: C:\Users\Maraia\Public_Diaxeiristes
Successfully processed 1 files; Failed processing 0 files
C:\Users\Maraia>icacls C:\Users\Maraia\Public_Diaxeiristes /grant Ipalliloi_OikonomikouTmimatos:F
processed file: C:\Users\Maraia\Public_Diaxeiristes
Successfully processed 1 files; Failed processing 0 files
C:\Users\Maraia>icacls C:\Users\Maraia\Public_Diaxeiristes /grant Ipalliloi_TmimaPwlisewn:F
processed file: C:\Users\Maraia\Public_Diaxeiristes
Successfully processed 1 files; Failed processing 0 files
C:\Users\Maraia>
```

Για τα private του κάθε τμήματος κάνω τα παρακάτω:

```
Command Prompt
C:\Users\Maraia>icacls C:\Users\Maraia\Private_Pwliseis /grant Ipalliloi_TmimaPwlisewn:F
processed file: C:\Users\Maraia\Private_Pwliseis
Successfully processed 1 files; Failed processing 0 files
C:\Users\Maraia>icacls C:\Users\Maraia\Private_Pwliseis /deny Ipalliloi_OikonomikouTmimatos:F
processed file: C:\Users\Maraia\Private_Pwliseis
Successfully processed 1 files; Failed processing 0 files
C:\Users\Maraia>icacls C:\Users\Maraia\Private_Pwliseis /deny System_Administrator:F
processed file: C:\Users\Maraia\Private_Pwliseis
Successfully processed 1 files; Failed processing 0 files
C:\Users\Maraia>
```

```
Command Prompt
Successfully processed 1 files; Failed processing 0 files
C:\Users\Maraia>icacls C:\Users\Maraia\Private_OikonomikoTmima /deny System_Administrator:F
processed file: C:\Users\Maraia\Private_OikonomikoTmima
Successfully processed 1 files; Failed processing 0 files
C:\Users\Maraia>icacls C:\Users\Maraia\Private_OikonomikoTmima /deny Ipalliloi_TmimaPwlisewn:F
processed file: C:\Users\Maraia\Private_OikonomikoTmima
Successfully processed 1 files; Failed processing 0 files
C:\Users\Maraia>icacls C:\Users\Maraia\Private_OikonomikoTmima /grant Ipalliloi_OikonomikouTmimatos:F
processed file: C:\Users\Maraia\Private_OikonomikoTmima
Successfully processed 1 files; Failed processing 0 files
C:\Users\Maraia>
```

```
Command Prompt
Successfully processed 1 files; Failed processing 0 files
C:\Users\Maraia>icacls C:\Users\Maraia\Private_Diaxeiristes /grant System_Administrator:F
processed file: C:\Users\Maraia\Private_Diaxeiristes
Successfully processed 1 files; Failed processing 0 files
C:\Users\Maraia>icacls C:\Users\Maraia\Private_Diaxeiristes /deny Ipalliloi_TmimaPwlisewn:F
processed file: C:\Users\Maraia\Private_Diaxeiristes
Successfully processed 1 files; Failed processing 0 files
C:\Users\Maraia>icacls C:\Users\Maraia\Private_Diaxeiristes /deny Ipalliloi_OikonomikouTmimatos:F
processed file: C:\Users\Maraia\Private_Diaxeiristes
Successfully processed 1 files; Failed processing 0 files
C:\Users\Maraia>
```

Κάθε μία από τις ομάδες υπαλλήλων θα πρέπει να έχει πλήρη πρόσβαση σε μία συγκεκριμένη περιοχή του συστήματος αρχείων και οι υπάλληλοι των υπολοίπων ομάδων να έχουν πρόσβαση μόνο για την ανάγνωση των αρχείων που εμπεριέχονται σε αυτή.

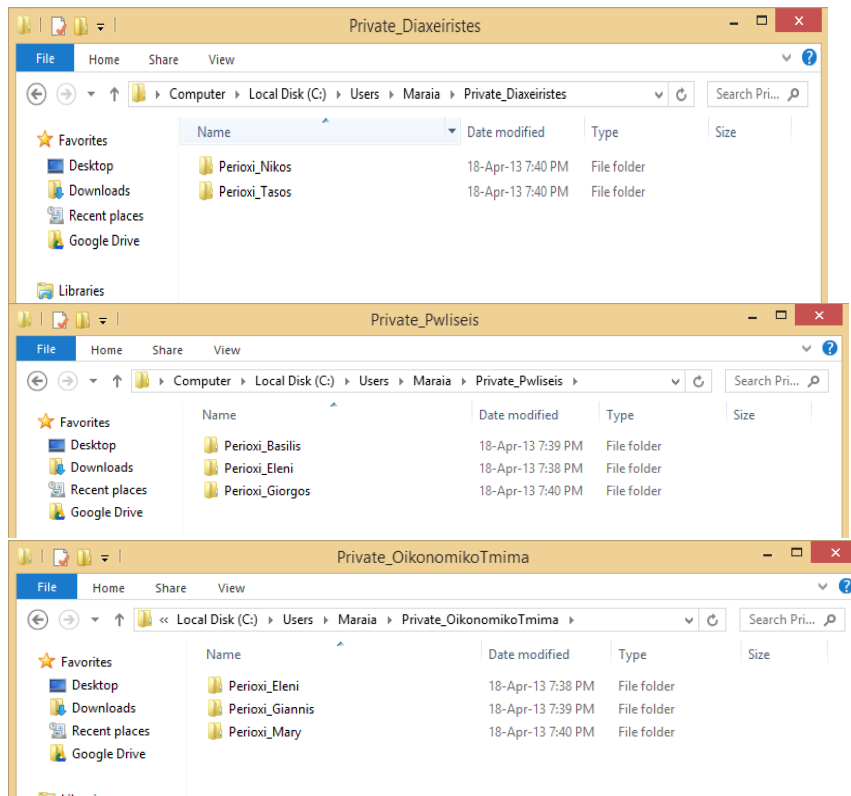
Για τις περιοχές του κάθε τμήματος κάνω τα παρακάτω:

```
Command Prompt
Successfully processed 1 files; Failed processing 0 files
C:\Users\Maraia>icacls C:\Users\Maraia\Perioxi_Pwliseis /grant Ipalliloi_TmimaPwlisewn:F
processed file: C:\Users\Maraia\Perioxi_Pwliseis
Successfully processed 1 files; Failed processing 0 files
C:\Users\Maraia>icacls C:\Users\Maraia\Perioxi_Pwliseis /grant Ipalliloi_OikonomikouTmimatos:R
processed file: C:\Users\Maraia\Perioxi_Pwliseis
Successfully processed 1 files; Failed processing 0 files
C:\Users\Maraia>icacls C:\Users\Maraia\Perioxi_Pwliseis /grant System_Administrator:R
processed file: C:\Users\Maraia\Perioxi_Pwliseis
Successfully processed 1 files; Failed processing 0 files
C:\Users\Maraia>
```

```
Command Prompt
Successfully processed 1 files; Failed processing 0 files
C:\Users\Maraia>icacls C:\Users\Maraia\Perioxi_OikonomikoTmima /grant Ipalliloi_OikonomikouTmimatos:F
processed file: C:\Users\Maraia\Perioxi_OikonomikoTmima
Successfully processed 1 files; Failed processing 0 files
C:\Users\Maraia>icacls C:\Users\Maraia\Perioxi_OikonomikoTmima /grant Ipalliloi_TmimaPwlisewn:R
processed file: C:\Users\Maraia\Perioxi_OikonomikoTmima
Successfully processed 1 files; Failed processing 0 files
C:\Users\Maraia>icacls C:\Users\Maraia\Perioxi_OikonomikoTmima /grant System_Administrator:R
processed file: C:\Users\Maraia\Perioxi_OikonomikoTmima
Successfully processed 1 files; Failed processing 0 files
C:\Users\Maraia>
```

```
Command Prompt
Successfully processed 1 files; Failed processing 0 files
C:\Users\Maraia>icacls C:\Users\Maraia\Perioxi_Diaxeiristes /grant System_Administrator:F
processed file: C:\Users\Maraia\Perioxi_Diaxeiristes
Successfully processed 1 files; Failed processing 0 files
C:\Users\Maraia>icacls C:\Users\Maraia\Perioxi_Diaxeiristes /grant Ipalliloi_TmimaPwlisewn:R
processed file: C:\Users\Maraia\Perioxi_Diaxeiristes
Successfully processed 1 files; Failed processing 0 files
C:\Users\Maraia>icacls C:\Users\Maraia\Perioxi_Diaxeiristes /grant Ipalliloi_OikonomikouTmimatos:R
processed file: C:\Users\Maraia\Perioxi_Diaxeiristes
Successfully processed 1 files; Failed processing 0 files
C:\Users\Maraia>
```

Επίσης κάθε χρήστης πρέπει να έχει την προσωπική του περιοχή αποθήκευσης αρχείων στην οποία θα έχει πλήρη δικαιώματα πρόσβασης μόνο ο ίδιος.



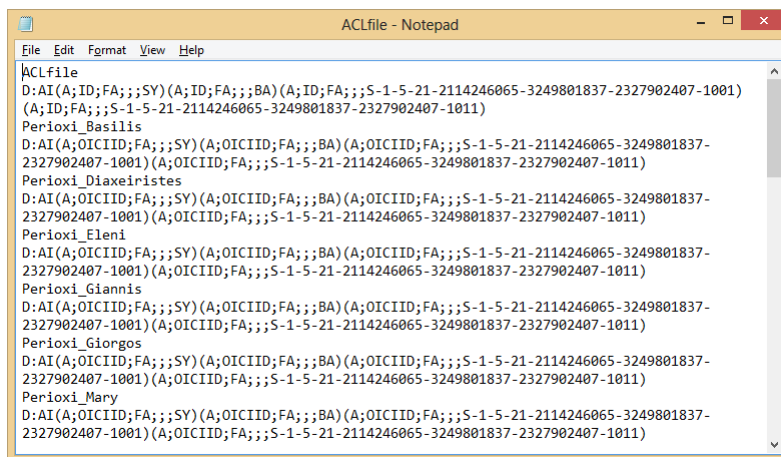
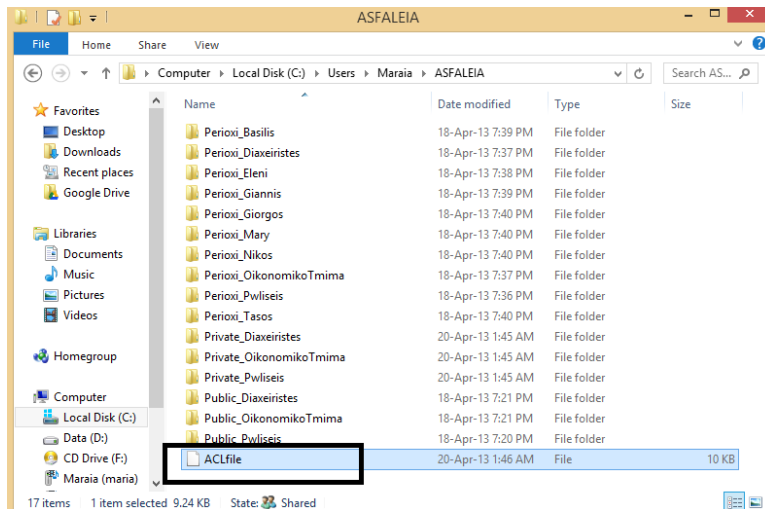
Δημιουργώ αρχεία κειμένου με τις λίστες ελέγχου πρόσβασης που όρισα (ACLs) με την εντολή `icacls * /save ACLfile /T`

```

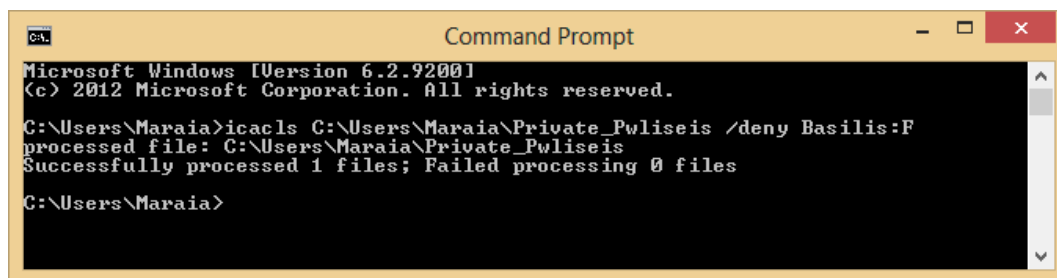
C:\Users\Maraia>cd C:\Users\Maraia\ASFALEIA
C:\Users\Maraia\ASFALEIA>icacls * /save ACLfile /T
processed file: ACLfile
processed file: Perioxi_Basilis
processed file: Perioxi_Diaxeiristes
processed file: Perioxi_Eleni
processed file: Perioxi_Giannis
processed file: Perioxi_Giorgos
processed file: Perioxi_Mary
processed file: Perioxi_Nikos
processed file: Perioxi_OikonomikoTmima
processed file: Perioxi_Pwliseis
processed file: Perioxi_Tasos
processed file: Private_Diaxeiristes
processed file: Private_OikonomikoTmima
processed file: Private_Pwliseis
processed file: Public_Diaxeiristes
processed file: Public_OikonomikoTmima
processed file: Private_Diaxeiristes\Perioxi_Nikos
processed file: Private_Diaxeiristes\Perioxi_Tasos
processed file: Private_OikonomikoTmima\Perioxi_Eleni
processed file: Private_OikonomikoTmima\Perioxi_Giannis
processed file: Private_OikonomikoTmima\Perioxi_Mary
processed file: Private_Pwliseis\Perioxi_Basilis
processed file: Private_Pwliseis\Perioxi_Eleni
processed file: Private_Pwliseis\Perioxi_Giorgos
Successfully processed 25 files; Failed processing 0 files
C:\Users\Maraia\ASFALEIA>

```

Και βλέπω το αρχείο **ACLs**



Τι θα αλλάζατε στα δικαιώματα πρόσβασης αν για κάποιο λόγο ο Βασίλης θα έπρεπε να αποκλειστεί εντελώς από την πρόσβαση στην αυστηρά ελεγχόμενη περιοχή εργασίας της ομάδας του;

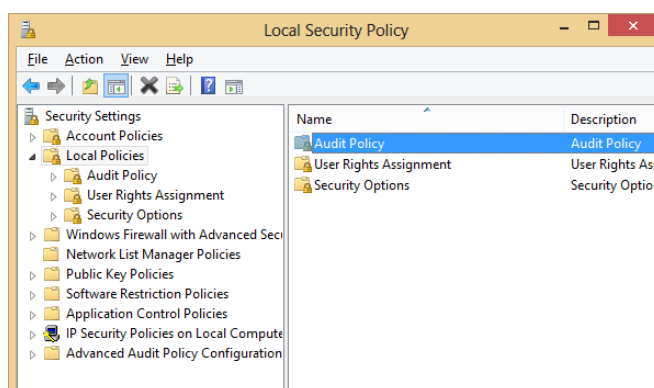
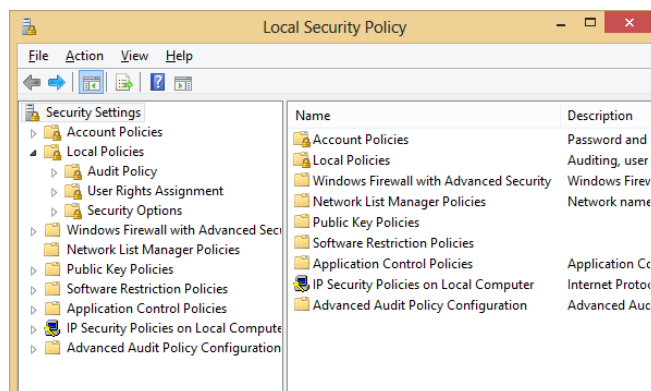


Ρυθμίστε κατάλληλα τον εξυπηρετητή που εργάζεστε έτσι ώστε να παράγονται συμβάντα (logs) κάθε φορά που ένας χρήστης προσπαθεί να αποκτήσει πρόσβαση σε περιοχή που δεν έχει τα απαραίτητα δικαιώματα. Εκτελέστε κάποια σενάρια έτσι ώστε να προκαλείται η δημιουργία αυτών των συμβάντων.

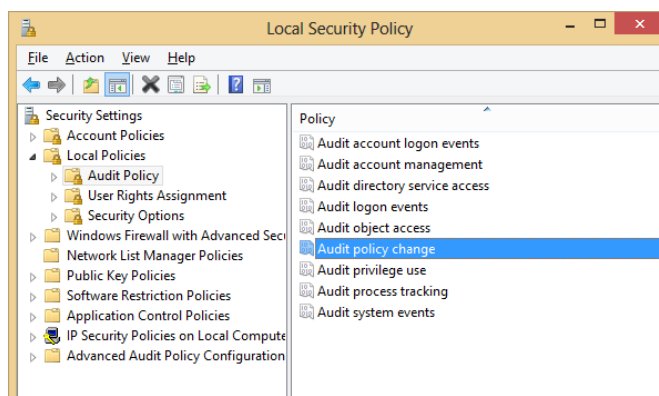
Το αρχείο καταγραφής ασφαλείας καταγράφει συμβάντα, όπως έγκυρες και μη έγκυρες προσπάθειες σύνδεσης, καθώς και συμβάντα που σχετίζονται με τη χρήση

πόρων, όπως η δημιουργία, το άνοιγμα ή η διαγραφή αρχείων. Για παράδειγμα, όταν είναι ενεργοποιημένος ο έλεγχος σύνδεσης, καταγράφεται ένα συμβάν στο αρχείο καταγραφής συμβάντων, κάθε φορά που ο χρήστης προσπαθεί να συνδεθεί στον υπολογιστή. Για να ενεργοποιήσετε, να χρησιμοποιήσετε και να καθορίσετε τα συμβάντα που καταγράφονται στο αρχείο καταγραφής ασφαλείας, πρέπει να έχετε συνδεθεί ως διαχειριστής ή ως μέλος της ομάδας Administrators.

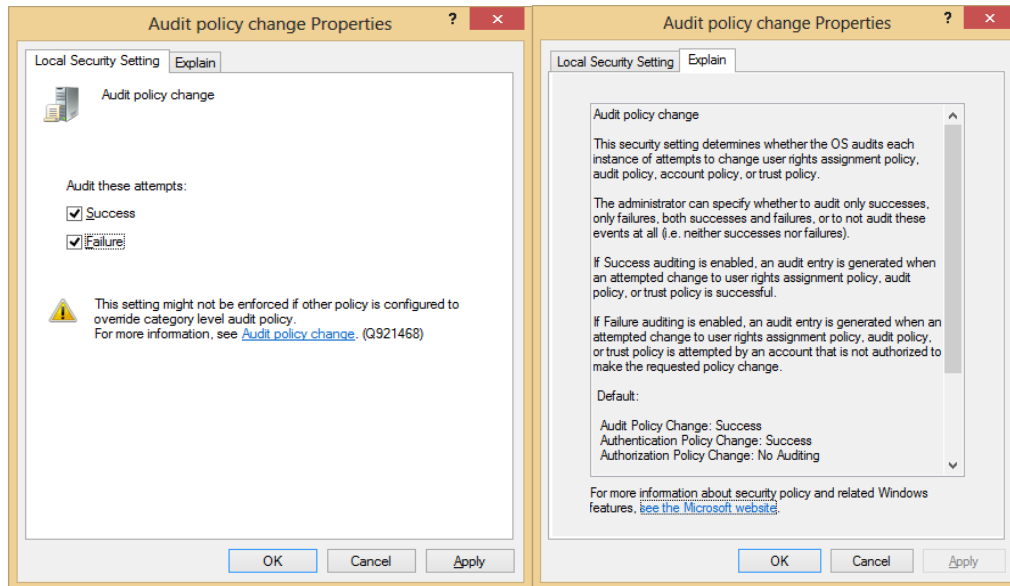
Αρχικά πηγαίνω στο Control Panel και επιλέγω το Administrative tools, στην συνέχεια κάνω διπλό κλικ στο στοιχείο **Τοπική πολιτική ασφαλείας (Local Security Policy)**, για να ξεκινήσει το συμπληρωματικό πρόγραμμα "Τοπικές ρυθμίσεις ασφαλείας" (Local Security Settings) της κονσόλας MMC. Κάνω διπλό κλικ στον κλάδο **Τοπικές πολιτικές (Local Policies)** για να τον αναπτύξω και στη συνέχεια κάνω διπλό κλικ στο στοιχείο **Πολιτική ελέγχου (Audit Policy)**.



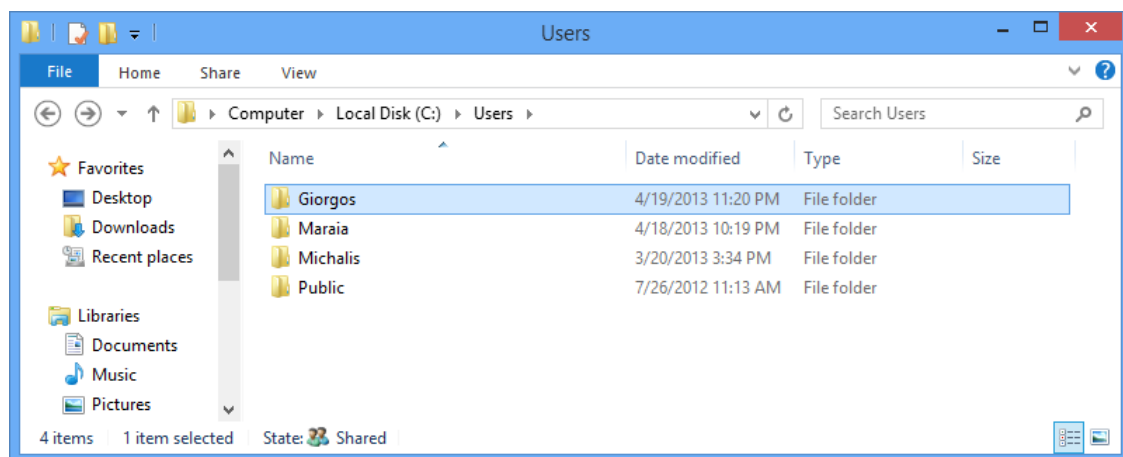
Στο δεξιό τμήμα του παραθύρου, κάνω διπλό κλικ στην πολιτική που θέλω να ενεργοποιήσω ή να απενεργοποιήσω.

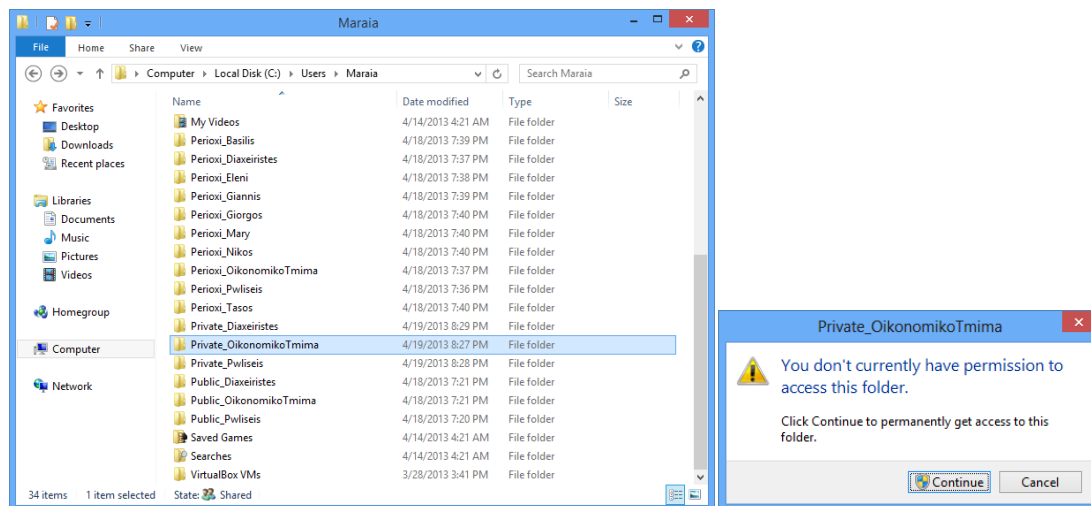


Κάνω κλικ στα πλαίσια ελέγχου **Επιτυχία (Success)** (**προσπάθεια πρόσβασης με έλεγχο ασφαλείας η οποία επιτυγχάνει**) και **Αποτυχία (Fail)** (**προσπάθεια πρόσβασης με έλεγχο ασφαλείας η οποία αποτυγχάνει**) για να ενεργοποιήσω και να απενεργοποιήσω την καταγραφή των αντίστοιχων ελέγχων. Για παράδειγμα, με τη ρύθμιση αυτή, η επιτυχημένη προσπάθεια πρόσβασης ενός χρήστη στο σύστημα καταγράφεται ως συμβάν τύπου "Επιτυχημένος έλεγχος" (Success Audit). Αν ένας χρήστης προσπαθήσει να αποκτήσει πρόσβαση σε μια μονάδα δίσκου δικτύου και αποτύχει, η προσπάθεια καταγράφεται ως συμβάν τύπου "Αποτυχημένος έλεγχος" (Failure Audit), και στην συνέχεια επιλέγω OK.

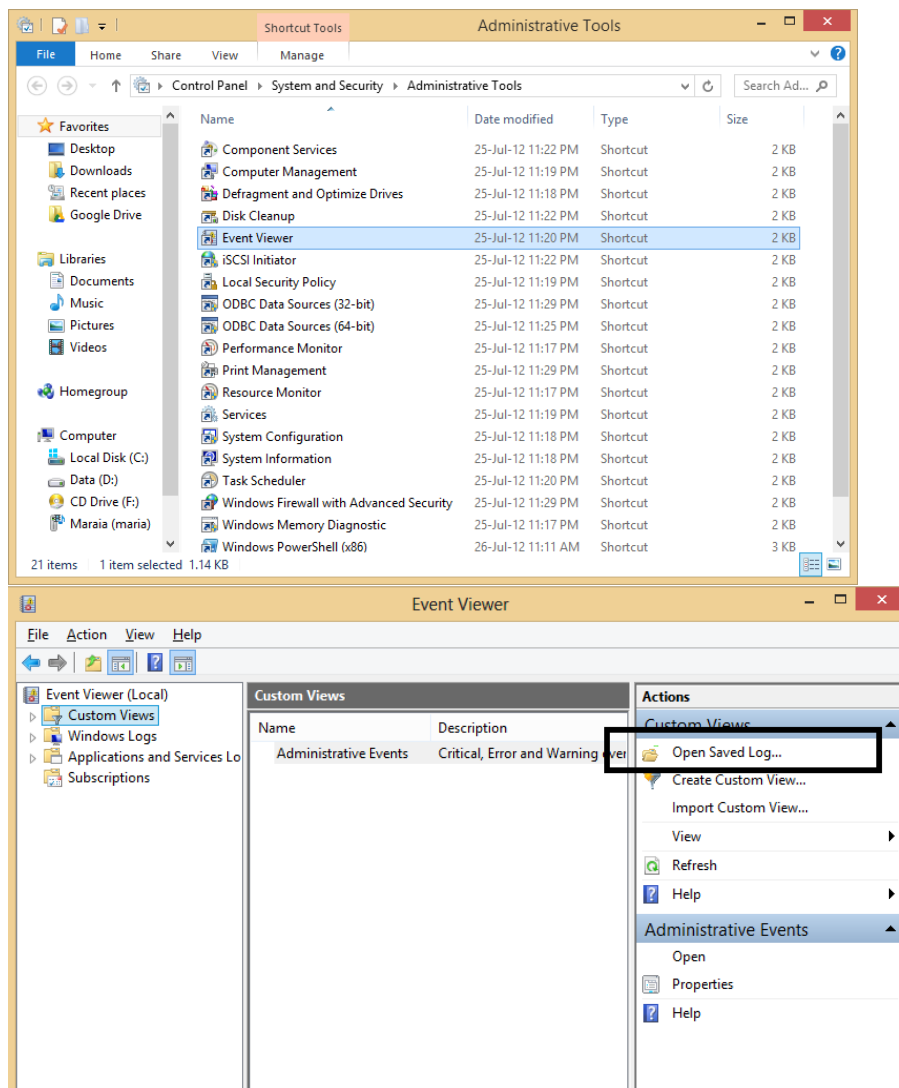


Ο Χρήστης **Γιώργος (Giorgos)** δεν μπορεί να έχει πρόσβαση στην περιοχή **Private_OikonomikoTomea**

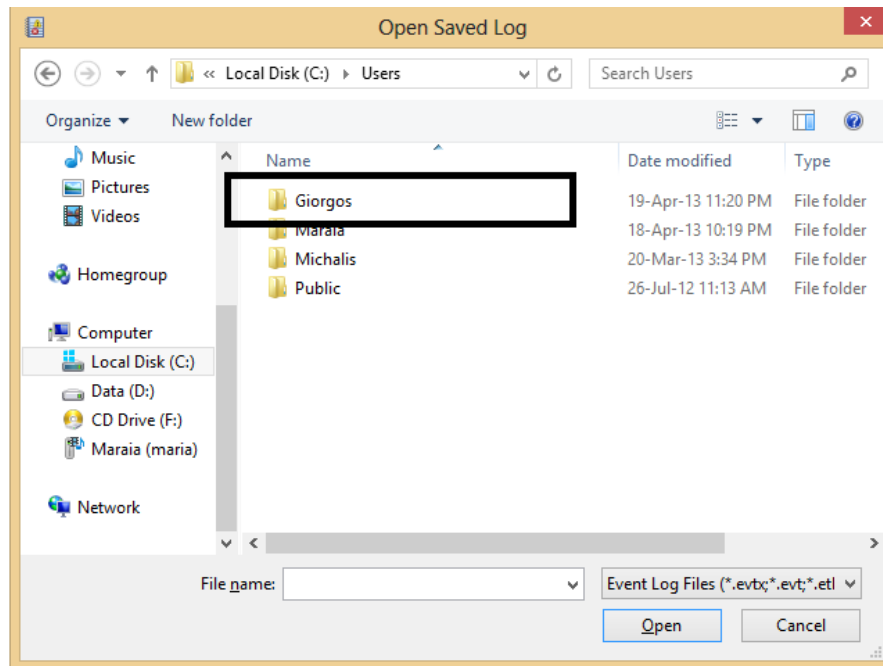




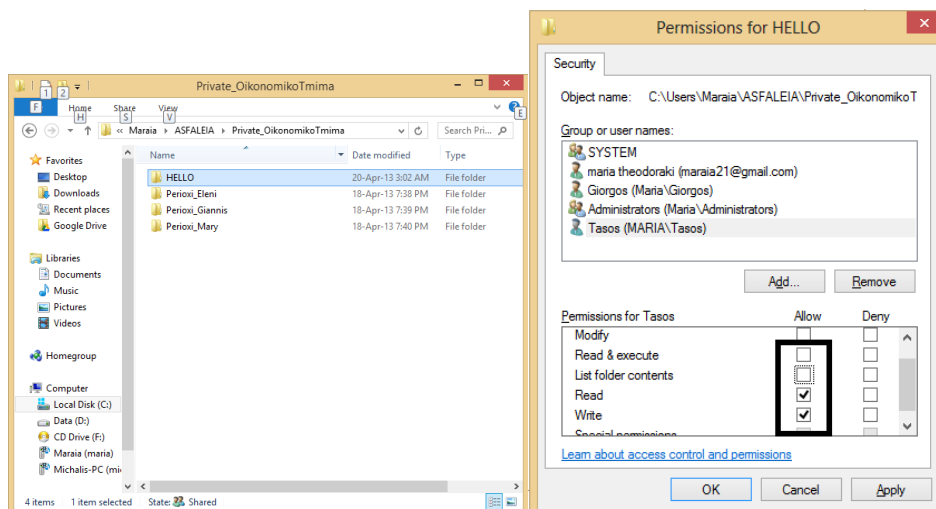
Και για να ελέγξω την προσπάθεια πρόσβασης του Γιώργου κάνω:

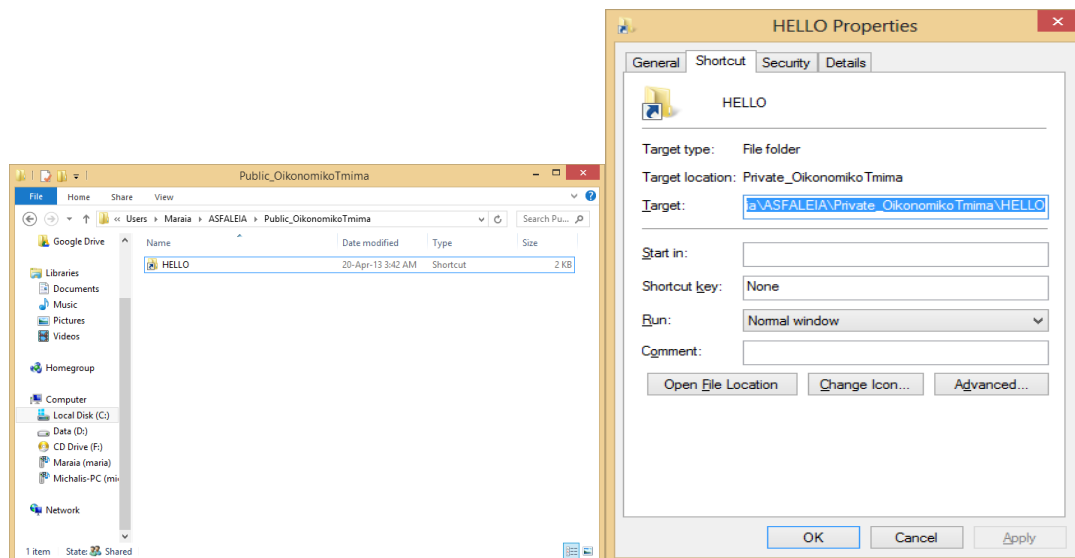


Και στην συνέχεια με την επιλογή **Open Saved Log** ελέγχο την είσοδο του Γιώργου στο σύστημα.



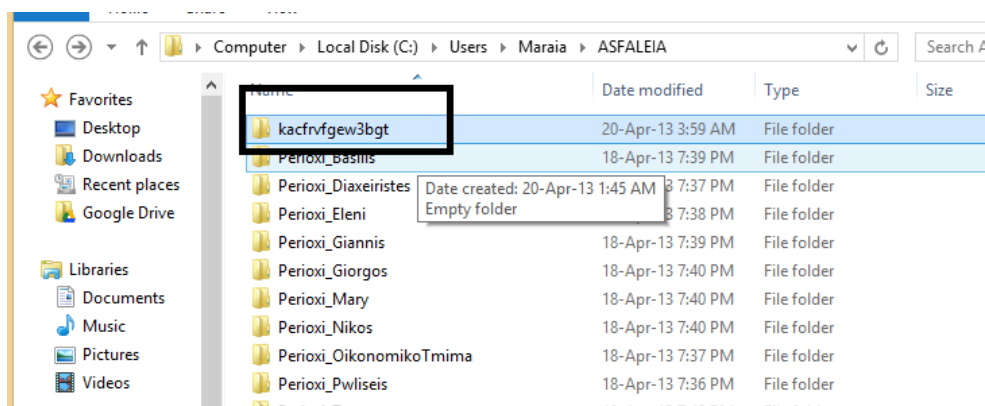
Στους φακέλους που έχουν πρόσβαση αποκλειστικά μόνο τα μέλη της κάθε ομάδας μπορούμε να δημιουργήσουμε μεμονωμένους υποφακέλους ή αρχεία στα οποία να επιτρέψουμε την πρόσβαση (ανάγνωση/εγγραφή) σε χρήστες που δεν είναι μέλη της ομάδας; Περιγράψτε τη διαδικασία

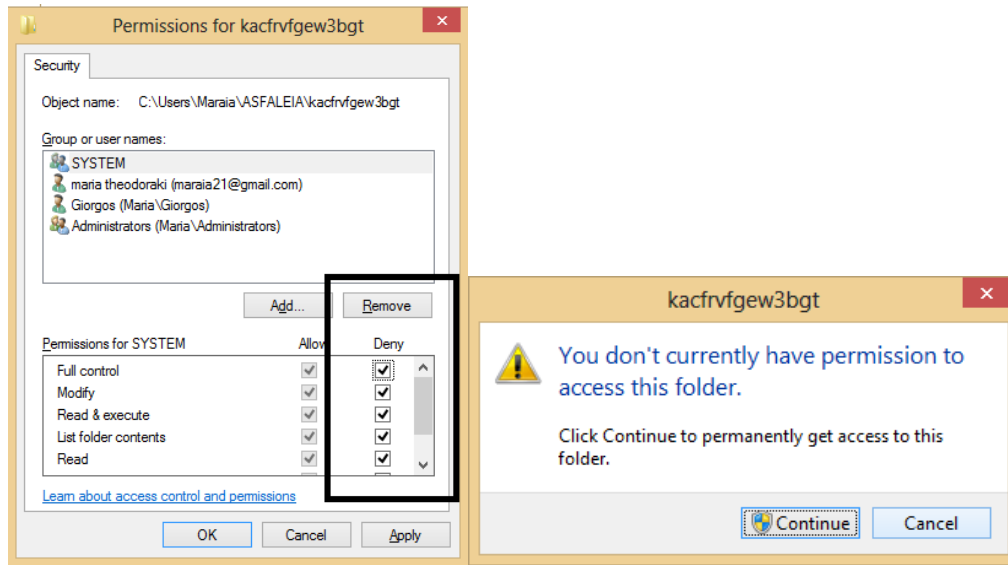




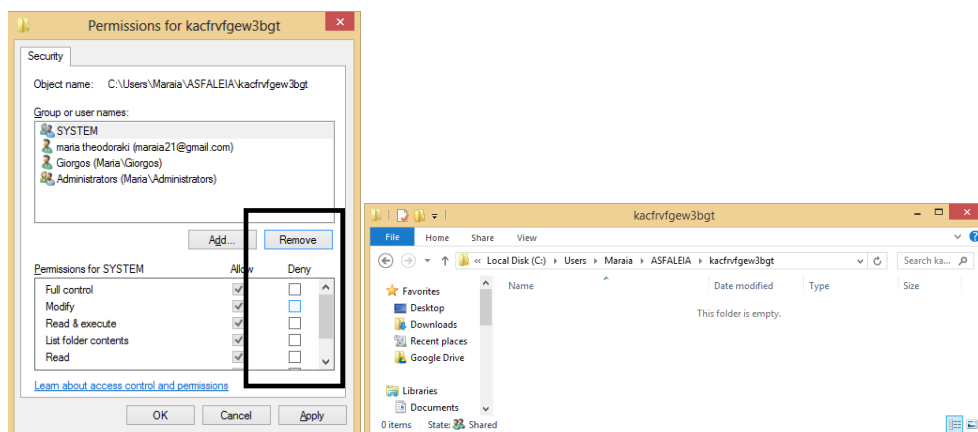
Υπάρχει τρόπος να αποτρέψουμε την πρόσβαση σε μια συγκεκριμένη περιοχή από τους διαχειριστές του συστήματος (System Administrators). Υπάρχει η δυνατότητα ο διαχειριστής να παρακάμψει τα δικαιώματα πρόσβασης που έχουμε ορίσει; Περιγράψτε αντίστοιχο σενάριο.

Ναι γίνεται να αποτρέψουμε την πρόσβαση σε μια συγκεκριμένη περιοχή από τους διαχειριστές του συστήματος.





Ναι γίνεται υπάρχει η δυνατότητα ο διαχειριστής να παρακάμψει τα δικαιώματα πρόσβασης που έχουμε ορίσει.



Ποιες οι διαφορές όσον αφορά τις ρυθμίσεις δικαιωμάτων μεταξύ Write και Modify;

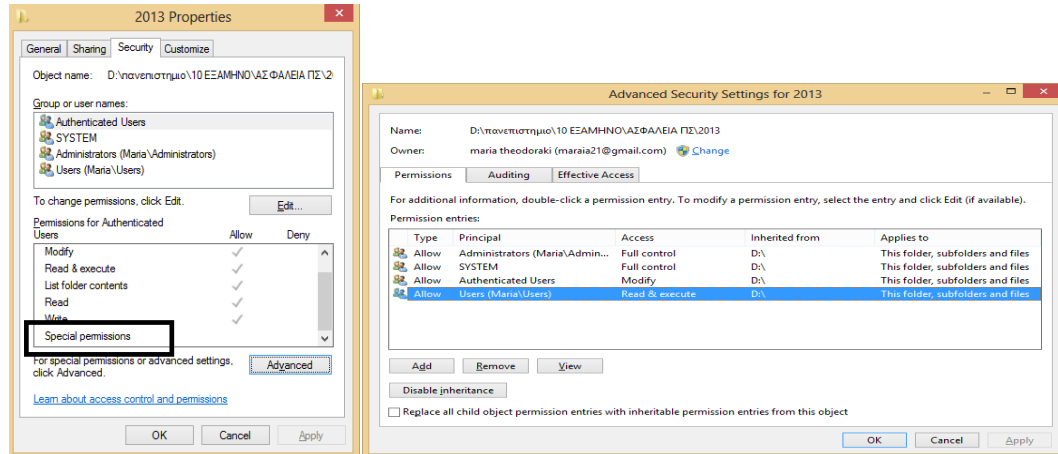
Όσον αφορά τις ρυθμίσεις δικαιωμάτων **write** για έναν φάκελο επιτρέπεται η πρόσθεση φακέλων και υποφακέλων και για ένα αρχείο επιτρέπεται να γράφεις μέσα σε αυτό. Ενώ με τις ρυθμίσεις **modify** η σημασία για τους φακέλους είναι ότι επιτρέπεται να διαβάσεις και να γράφεις σε φακέλους και υποφακέλους καθώς επίσης και να διαγράψεις έναν φάκελο. Όσον αφορά τα αρχεία με το **modify** επιτρέπεται να διαβάσεις και να γράφεις σε ένα αρχείο καθώς επίσης και να διαγράψεις ένα αρχείο.

Τι δικαιώματα απαιτείται να δώσετε σε ένα φάκελο έτσι ώστε:

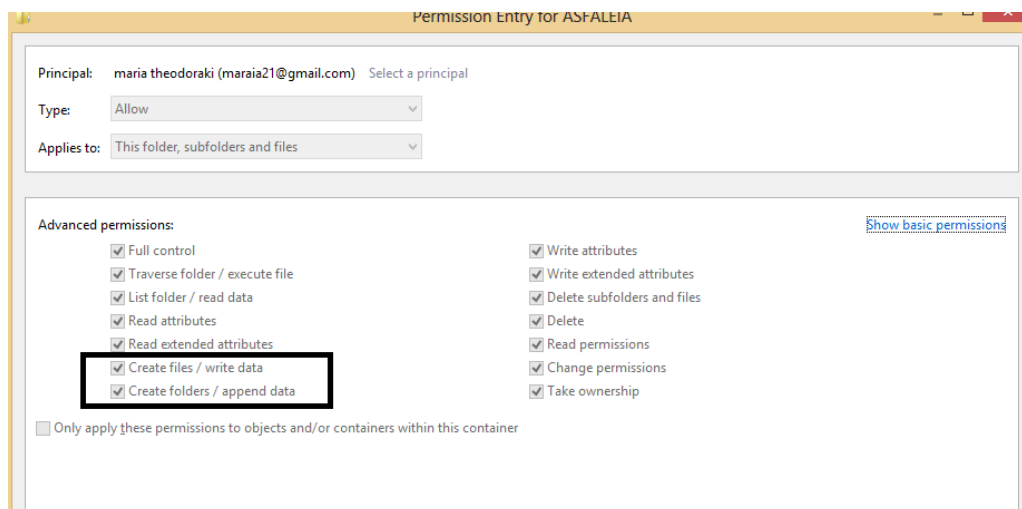
α) να μην μπορεί κάποιος να δημιουργήσει νέους υποφακέλους αλλά μόνο αρχεία

β) να μην μπορεί κάποιος να σβήσει αρχεία (ή υποφακέλους), αλλά μόνο να προσθέσει (ή να δημιουργήσει) νέα αρχεία και νέους υποφακέλους;

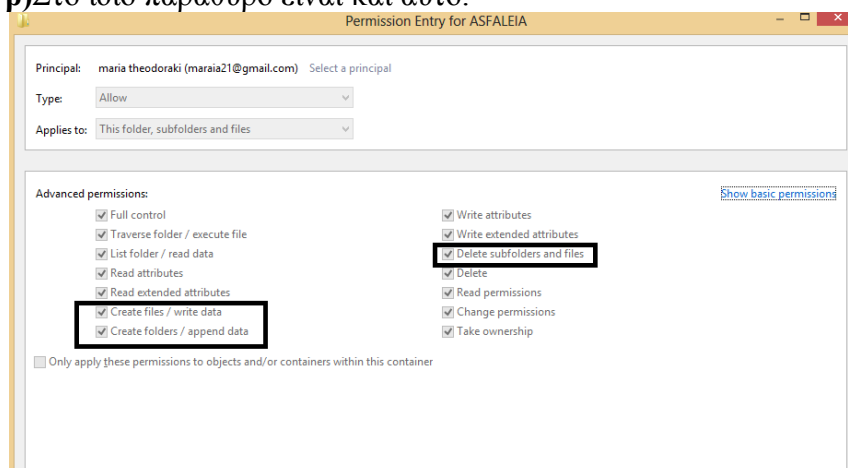
α) Σε έναν φάκελο π.χ τον φάκελο ASFALEIA αν πατήσω δεξί κλικ->properties και μετά επιλέξω security αν παρατηρήσω δεν υπάρχουν special permissions γι' αυτό. Μετά αν επιλέξω Advanced και πατήσω διπλό κλικ στο Users(Maraia\Users) θα πατήσω Show advanced options.



Εκεί αν ξετικάρω τα δύο που φαίνονται τότε επιτυγχάνω να μην μπορεί κάποιος να δημιουργήσει νέους υποφακέλους, αλλά μόνο αρχεία.

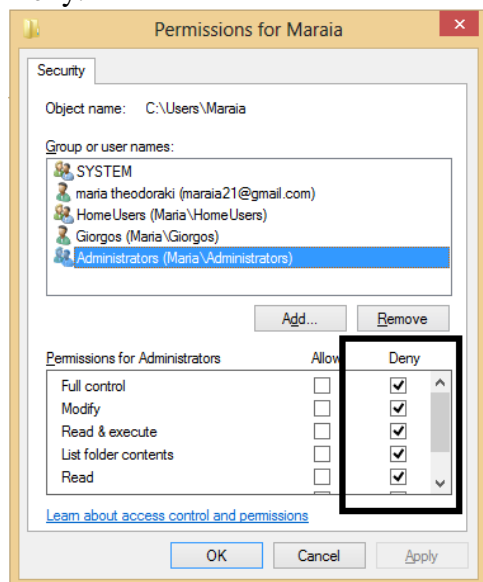


β) Στο ίδιο παράθυρο είναι και αυτό.

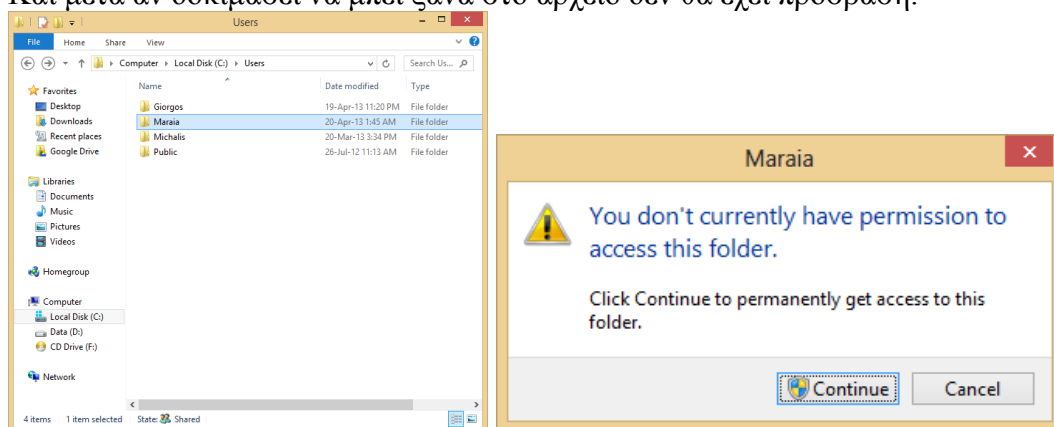


Υπάρχει τρόπος ο διαχειριστής να παρακολουθήσει την πρόσβαση σε κάποιο κρίσιμο αρχείο (π.χ. ένα αρχείο με passwords) :

Ναι υπάρχει αρκεί ο Administrator να ρυθμίσει τα permissions δηλαδή να τα κάνει Deny.



Και μετά αν δοκιμάσει να μπει ξανά στο αρχείο δεν θα έχει πρόσβαση.



Σε νεότερες εκδόσεις των Windows (Windows Vista, Windows 7) έχει προστεθεί ένας νέος μηχανισμός προστασίας γνωστός ως WIC (Windows Mandatory Integrity Control Mechanism). Σχετικά με αυτό το νέο χαρακτηριστικό:

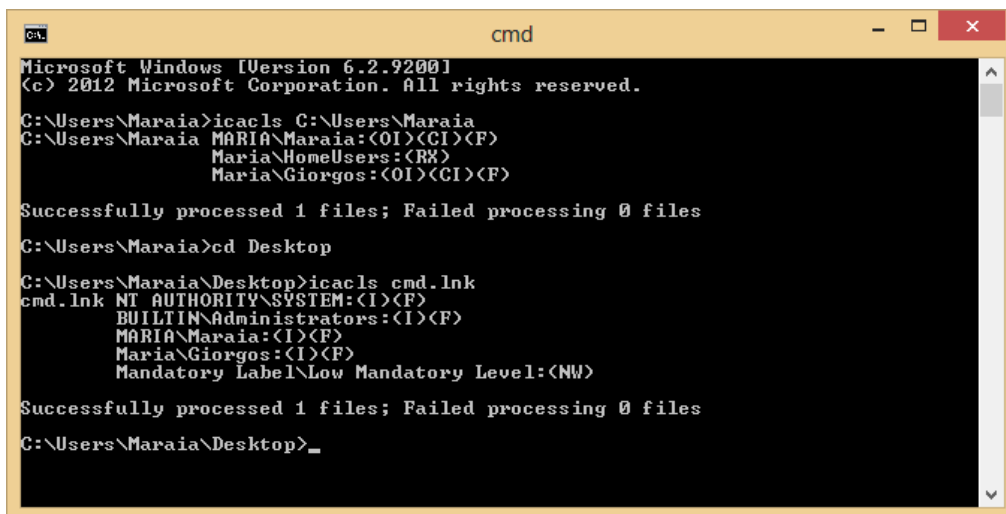
- Μελετήστε τι παραπάνω επίπεδο ασφάλειας μας παρέχει αυτός ο μηχανισμός και πώς αλληλεπιδρά με τα δικαιώματα πρόσβασης που ορίζονται σε ένα NTFS σύστημα αρχείων.

Ο WIC (Windows Mandatory Integrity Control Mechanism) παρέχει έναν μηχανισμό για τον έλεγχο της πρόσβασης σε ασφαλιζόμενα αντικείμενα. Ο μηχανισμός αυτός αξιολογείται και είναι επιπρόσθετος στην διακριτική ευχαίρεια ελέγχου πρόσβασης και αξιολογεί την πρόσβαση πριν την διεξαγωγή ελέγχου

πρόσβασης ενάντια σε μία λιστα διακριτικού ελέγχου πρόσβασης. Χρησιμοποιεί επίπεδα ακεραιότητας και υποχρεωτική πολιτική για να αξιολογήσει την πρόσβαση. Οι αρχές ασφαλείας και τα ασφαλιζόμενα αντικείμενα έχουν αναθέσει επίπεδα ακεραιότητας που καθορίζουν τα επίπεδα προστασίας τους ή την πρόσβαση. Για παράδειγμα μία αρχή με χαμηλό επίπεδο ακεραιότητας δεν μπορεί να γράψει σε ένα αντικείμενο με μεσαίο επίπεδο ακεραιότητας ακόμα και αν το αντικείμενο του DACL επιτρέπει πρόσβαση εγγραφής στον φάκελο.

Τα επίπεδα ακεραιότητας της Microsoft έχουν ενσωματωθεί στα Windows για να περιορίσουν τα δικαιώματα πρόσβασης των εφαρμογών που τρέχουν κάτω από τον ίδιο λογαριασμό χρήστη. Αυτοί οι υποχρεωτικοί έλεγχοι πρόσβασης εκχωρούν ετικέτες εμπιστοσύνης όπως Low, Medium και High, ώστε να λειτουργούν τα αντικείμενα του συστήματος όπως τα αρχεία και οι διεργασίες. Τα επίπεδα ακεραιότητας υπερσχύουν έναντι στους παραδοσιακούς διακριτικούς ελέγχους, που εξακολουθούν να υπάρχουν στην θέση Windows σε NTFS και επίπεδα registry. Ακόμα και όταν οι χρήστες είναι συνδεδεμένοι στα Windows με τα διοικητικά προνόμια, οι διεργασίες που έχουν ανατεθεί θα ξεκινήσουν από προεπιλογή, στο μέσο επίπεδο ακεραιότητας.

- Πως μπορούμε να δούμε τα επίπεδα αξιοπιστίας των διεργασιών και των αρχείων;



```
cmd
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Maraia>icacls C:\Users\Maraia
C:\Users\Maraia MARIÁ\Maraia:(OI)(CI)(F)
                Maria\HomeUsers:(RX)
                Maria\Giorgos:(OI)(CI)(F)

Successfully processed 1 files; Failed processing 0 files

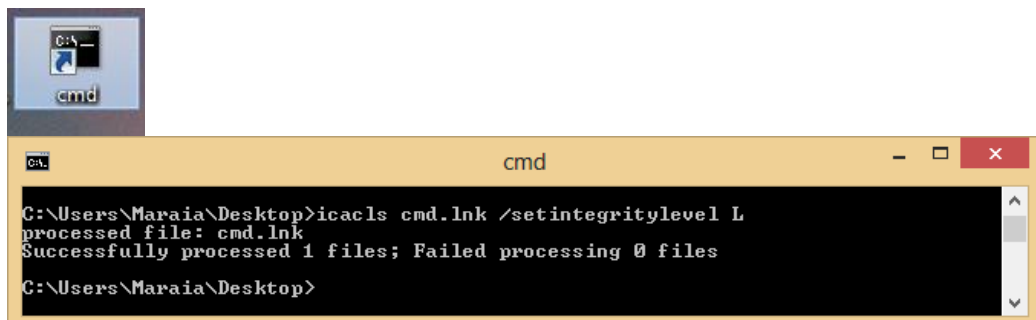
C:\Users\Maraia>cd Desktop

C:\Users\Maraia\Desktop>icacls cmd.lnk
cmd.lnk NT AUTHORITY\SYSTEM:(I)(F)
        BUILTIN\Administrators:(I)(F)
        MARIÁ\Maraia:(I)(F)
        Maria\Giorgos:(I)(F)
        Mandatory Label\Low Mandatory Level:(NW)

Successfully processed 1 files; Failed processing 0 files

C:\Users\Maraia\Desktop>_
```

- Δημιουργήστε ένα αντίγραφο του προγράμματος cmd.exe και προσπαθήστε να αλλάξετε το επίπεδο αξιοπιστίας σε low.



```
cmd

C:\Users\Maraia\Desktop>icacls cmd.lnk /setintegritylevel L
processed file: cmd.lnk
Successfully processed 1 files; Failed processing 0 files

C:\Users\Maraia\Desktop>
```

- Δώστε ένα παράδειγμα για το πώς μπορώ να καθορίσω την πολιτική ασφαλείας «no read up».

Από προεπιλογή ένα αρχείο που έχει ήδη δημιουργηθεί από τον χρήστη των Windows ακόμα και αν το άτομο έχει συνδεθεί με δικαιώματα διαχειριστή αποδίδεται το Μεσαίο επίπεδο ακεραιότητας. Οι πολιτικές ακεραιότητας δείχνουν ότι ένα αντικείμενο με χαμηλότερο επίπεδο ακεραιότητας θα είναι σε θέση να διαβάσει και να εκτελέσει το αρχείο. Αυτό συμβαίνει γιατί η “no read up” πολιτική έχει απενεργοποιηθεί από προεπιλογή. Ωστόσο το αντικείμενο θα μπορεί να γράψει στο αρχείο επειδή η “no write up” πολιτική είναι ενεργοποιημένη. Για να είναι πιο δύσκολο για το κακόβουλο λογισμικό να διαβάσει τον ευαίσθητο φάκελο ο χρήστης μπορεί να ρυθμίσει το επίπεδο της ακεραιότητας του αρχείου σε υψηλό και επίσης την δυνατότητα να ενεργοποιήσει την “no read up” πολιτική.

Σε δεύτερη φάση το ίδιο σενάριο που περιγράφηκε παραπάνω θα πρέπει να το εφαρμόσετε ως διαχειριστής σε ένα λειτουργικό σύστημα Linux.

Εμείς κάναμε χρήση του ubuntu server στο virtual box

Δημιουργήστε 3 ομάδες χρηστών (μία για κάθε τμήμα της επιχείρησης) καθώς και λογαριασμούς χρηστών για κάθε έναν από τους υπαλλήλους της εταιρείας.

Με την εντολή `sudo apt-get install gnome-system-tools` εγκαθιστώ μια λειτουργία για να φτιάξω χρήστες και ομάδες.

```

Terminal: File Edit View Search Terminal Help
anjelina@anjli: ~
anjelina@anjli:~$ sudo apt-get install gnome-system-tools
[sudo] password for anjelina:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libencode-locale-perl libfile-listing-perl libfont-afm-perl
  libhtml-form-perl libhtml-format-perl libhtml-parser-perl
  libhtml-tagset-perl libhtml-tree-perl libhttp-cookies-perl
  libhttp-daemon-perl libhttp-date-perl libhttp-message-perl
  libhttp-negotiate-perl libio-socket-ssl-perl liblwp-mediatypes-perl
  liblwp-protocol-https-perl libnet-dbus-perl libnet-http-perl
  libnet-ssleay-perl liboobs-1-5 libtie-ixhash-perl libwww-perl
  libwww-robotrules-perl libxml-parser-perl libxml-twig-perl libxml-xpath-perl
  system-tools-backends
Suggested packages:
  ntp libdata-dump-perl libcrypt-ssleay-perl libauthen-ntlm-perl
  libunicode-map8-perl libunicode-string-perl xml-twig-tools
The following NEW packages will be installed:
  gnome-system-tools libencode-locale-perl libfile-listing-perl
  libfont-afm-perl libhtml-form-perl libhtml-format-perl libhtml-parser-perl
  libhtml-tagset-perl libhtml-tree-perl libhttp-cookies-perl
  libhttp-daemon-perl libhttp-date-perl libhttp-message-perl
  libhttp-negotiate-perl libio-socket-ssl-perl liblwp-mediatypes-perl

```

Με την εντολή `sudo groupadd tmima pwlisewn` , `sudo groupadd oikonomiko tmima`, `sudo groupadd tmima diaxeiristwn` προστέτω τις 3 ομάδες χρηστών για κάθε τμήμα της επιχείρησης.

```
Terminal
anjelina@anji: ~
anjelina@anji:~$ sudo apt-get install acl
Reading package lists... Done
Building dependency tree
Reading state information... Done
acl is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
anjelina@anji:~$ sudo groupadd tmima pwlisewn
Usage: groupadd [options] GROUP

Options:
  -f, --force                exit successfully if the group already exists,
                             and cancel -g if the GID is already used
  -g, --gid GID              use GID for the new group
  -h, --help                 display this help message and exit
  -K, --key KEY=VALUE        override /etc/login.defs defaults
  -o, --non-unique            allow to create groups with duplicate
                             (non-unique) GID
  -p, --password PASSWORD    use this encrypted password for the new group
  -r, --system               create a system account

anjelina@anji:~$ sudo groupadd tmima_pwlisewn
anjelina@anji:~$ sudo groupadd oikonomiko_tmima
anjelina@anji:~$ sudo groupadd tmima_diaxeiristwn
anjelina@anji:~$
```

Μετά βλέπω παρακάτω την ύπαρξή τους με την εντολή cat/etc/groups

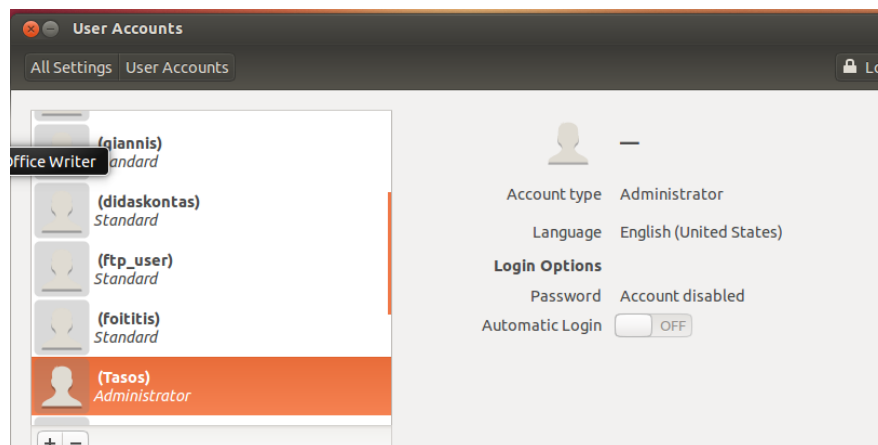
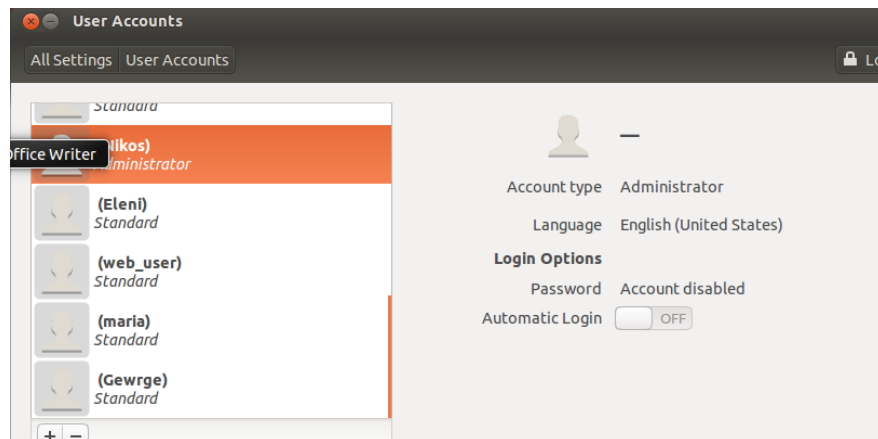
```
Terminal
anjelina@anji: ~
sambashare:x:113:anjelina
ftp:x:114:
ssl_cert:x:115:
Home Folder :x:1001:
ftp_user:x:1002:
web_user:x:1003:
didaskontas:x:1004:
foititis:x:1005:
avahi-autoipd:x:116:
bluetooth:x:117:
scanner:x:118:
colord:x:119:
lightdm:x:120:
nopasswdlogin:x:121:
avahi:x:122:
utempter:x:123:
rtkit:x:124:
saned:x:125:
pulse:x:126:
pulse-access:x:127:
tmima_pwlisewn:x:1006:
oikonomiko_tmima:x:1007:
tmima_diaxeiristwn:x:1008:
anjelina@anji:~$
```

Για να φτιάξω τους χρήστες που ανήκουν στο κάθε τμήμα κάνω τις παρακάτω εντολές:

sudo useradd -G tmima_pwlisewn,oikonomiko_tmima Eleni
sudo useradd -G tmima_pwlisewn Vasilis
sudo useradd -G tmima_pwlisewn Gewrge
sudo useradd -G oikonomiko_tmima giannis
sudo useradd -G oikonomiko_tmima maria
sudo useradd -G tmima_diaxeiristwn Tasos
sudo useradd -G tmima_diaxeiristwn Nikos

```
anjelina@anji:~$ sudo useradd -G tmima_pwlisewn,oikonomiko_tmima Eleni
anjelina@anji:~$ sudo useradd -G tmima_pwlisewn Vasilis
anjelina@anji:~$ sudo useradd -G tmima_pwlisewn Gewrge
anjelina@anji:~$ sudo useradd -G oikonomiko_tmima giannis
anjelina@anji:~$ sudo useradd -G oikonomiko_tmima maria
anjelina@anji:~$ sudo useradd -G tmima_diaxeiristwn Tasos
anjelina@anji:~$ sudo useradd -G tmima_diaxeiristwn Nikos
anjelina@anji:~$
```

Μετά πάω στις ρυθμίσεις και πάω στους λογαριασμούς χρηστών για να κάνω τον Τάσο και τον Νίκο administrators.



Επίσης κάθε χρήστης πρέπει να έχει την προσωπική του περιοχή αποθήκευσης αρχείων στην οποία θα έχει πλήρη δικαιώματα πρόσβασης μόνο ο ίδιος. Υλοποιήστε όλη την υποδομή που απαιτείται (οργάνωση φακέλων και καθορισμός δικαιωμάτων πρόσβασης) η οποία όμως να ικανοποιεί πλήρως τις απαιτήσεις ασφάλειας που περιγράφηκαν προηγουμένως. Χρησιμοποιήστε την εντολή icacls για να δημιουργήσετε αρχεία κειμένου με τις λίστες ελέγχου πρόσβασης που ορίσατε (ACLs).

Δημιουργούμε φακέλους για κάθε ομάδα (δύο περιοχές με διαφορετικά επίπεδα πρόσβασης και περιοχές) με την εντολή mkdir όνομα φακέλου.

Μία κοινόχρηστη περιοχή εργασίας (public area) όπου όλοι οι υπάλληλοι της εταιρείας μπορούν να έχουν τη δυνατότητα να διαβάσουν και να προσθέσουν αρχεία που αφορούν τη συγκεκριμένη ομάδα.

Μια αυστηρά ελεγχόμενη περιοχή εργασίας (private area) όπου μόνο οι υπάλληλοι του ίδιου τμήματος έχουν πλήρη δικαιώματα πρόσβασης σε αυτή.

```

anjelina@anji:~$ mkdir public_tmima_Pwliisewn
anjelina@anji:~$ mkdir public_Oikonomiko_tmima
anjelina@anji:~$ mkdir public_tmima_diaxeiristwn
anjelina@anji:~$ mkdir private_tmima_Pwliisewn
anjelina@anji:~$ mkdir private_Oikonomiko_tmima
anjelina@anji:~$ mkdir private_tmima_diaxeiristwn
anjelina@anji:~$

```

Και μια περιοχή που η κάθε ομάδα έχει πλήρη πρόσβαση αλλά οι υπόλοιποι υπάλληλοι των άλλων ομάδων έχουν μόνο δικαιώματα ανάγνωσης των αρχείων που εμπεριέχονται σε αυτή. Τα ονόματα που ακολουθούν αυτές τις περιοχές περιοχές αποτελούν το προσωπικό χώρο του κάθε χρήστη.

```

anjelina@anji:~$ mkdir private_tmima_diaxeiristwn
anjelina@anji:~$ mkdir perioxi_tmima_Pwliisewn
anjelina@anji:~$ mkdir perioxi_Oikonomiko_tmima
anjelina@anji:~$ mkdir perioxi_tmima_diaxeiristwn
anjelina@anji:~$ mkdir perioxi_Eleni
anjelina@anji:~$ mkdir perioxi_Vasilis
anjelina@anji:~$ mkdir perioxi_Giorgos
anjelina@anji:~$ mkdir perioxi_Giannis
anjelina@anji:~$ mkdir perioxi_Maria
anjelina@anji:~$ mkdir perioxi_Tasos
anjelina@anji:~$ mkdir perioxi_Nikos
anjelina@anji:~$

```

Βλέπω ότι φτιάχτηκαν στο σύστημα με την εντολή ls-l

```

anjelina@anji:~$ ls -l
LibreOffice Calc
drwxr-xr-x 2 anjelina anjelina 4096 Apr 1 22:43 Desktop
drwxr-xr-x 2 anjelina anjelina 4096 Apr 1 22:43 Documents
drwxr-xr-x 2 anjelina anjelina 4096 Apr 1 22:43 Downloads
drwxr-xr-x 2 anjelina anjelina 4096 Apr 1 22:43 Music
drwxrwxr-x 2 anjelina anjelina 4096 Apr 18 19:38 perioxi_Eleni
drwxrwxr-x 2 anjelina anjelina 4096 Apr 18 19:39 perioxi_Giannis
drwxrwxr-x 2 anjelina anjelina 4096 Apr 18 19:39 perioxi_Giorgos
drwxrwxr-x 2 anjelina anjelina 4096 Apr 18 19:39 perioxi_Maria
drwxrwxr-x 2 anjelina anjelina 4096 Apr 18 19:39 perioxi_Nikos
drwxrwxr-x 2 anjelina anjelina 4096 Apr 18 19:37 perioxi_Oikonomiko_tmima
drwxrwxr-x 2 anjelina anjelina 4096 Apr 18 19:39 perioxi_Tasos
drwxrwxr-x 2 anjelina anjelina 4096 Apr 18 19:38 perioxi_tmima_diaxeiristwn
drwxrwxr-x 2 anjelina anjelina 4096 Apr 18 19:37 perioxi_tmima_Pwliisewn
drwxrwxr-x 2 anjelina anjelina 4096 Apr 18 19:39 perioxi_Vasilis
drwxr-xr-x 2 anjelina anjelina 4096 Apr 1 22:43 Pictures
drwxrwxr-x 2 anjelina anjelina 4096 Apr 18 19:33 private_Oikonomiko_tmima
drwxrwxr-x 2 anjelina anjelina 4096 Apr 18 19:33 private_tmima_diaxeiristwn
drwxrwxr-x 2 anjelina anjelina 4096 Apr 18 19:33 private_tmima_Pwliisewn
drwxr-xr-x 2 anjelina anjelina 4096 Apr 1 22:43 Public
drwxrwxr-x 2 anjelina anjelina 4096 Apr 18 19:33 public_Oikonomiko_tmima
drwxrwxr-x 2 anjelina anjelina 4096 Apr 18 19:33 public_tmima_diaxeiristwn
drwxrwxr-x 2 anjelina anjelina 4096 Apr 18 19:32 public_tmima_Pwliisewn
drwxr-xr-x 2 anjelina anjelina 4096 Apr 1 22:43 Templates
drwxr-xr-x 2 anjelina anjelina 4096 Apr 1 22:43 Videos
anjelina@anji:~$

```

Τώρα πρέπει να αλλάξω τα δικαιώματα. Όλες οι κατηγορίες users, έχουν δικαιώματα πρόσβασης στο αρχείο, τα οποία μπορούν είτε να παραχωρηθούν είτε να αρθούν. Τα δικαιώματα πρόσβασης της κάθε κατηγορίας είναι τρία:

Ανάγνωση (r), η οποία δηλώνει τη δυνατότητα προβολής (ή αντιγραφής) του περιεχομένου του αρχείου.

Εγγραφή (w), η οποία δηλώνει τη δυνατότητα τροποποίησης (ή διαγραφής) του περιεχομένου του αρχείου.

Εκτέλεση (x). η οποία χρησιμοποιείται αν το αρχείο είναι το εκτελέσιμο κάποιας εφαρμογής.

Τα δικαιώματα πρόσβασης που έχει κάθε κατηγορία δίνονται σε τριάδες της μορφής rwx. Η σειρά των γραμμάτων παίζει σημασία και έτσι, το πρώτο αφορά την δυνατότητα ανάγνωσης, το δεύτερο τη δυνατότητα εγγραφής και το τρίτο τη δυνατότητα εκτέλεσης του αρχείου. Αν ο χρήστης δεν έχει κάποιο από τα δικαιώματα, τότε το αντίστοιχο γράμμα αντικαθίσταται από μία παύλα. Πχ η τριάδα rw- δηλώνει ότι ο χρήστης έχει δικαίωμα μόνο ανάγνωσης και εγγραφής ενώ η τριάδα r-x δηλώνει ότι έχει δικαίωμα μόνο ανάγνωσης και εκτέλεσης. Η τριάδα --- δηλώνει ότι ο χρήστης δεν έχει τη δυνατότητα ούτε να διαβάσει, ούτε να εγγράψει αλλά ούτε και να εκτελέσει το αρχείο. Τα δικαιώματα πρόσβασης των αρχείων δίνονται μέσω μία αλληλουχίας 10 χαρακτήρων της μορφής -rw-rw-r--, της οποίας ο πρώτος χαρακτήρας δηλώνει το είδος του αρχείου ενώ οι 9 χαρακτήρες που ακολουθούν είναι οι τριάδες που αντιστοιχούν στην κάθε κατηγορία δικαιωμάτων. Ο πρώτος χαρακτήρας παίρνει την τιμή (**d**) αν το αρχείο είναι κατάλογος, την τιμή (**-**) αν είναι απλό αρχείο, ενώ αν είναι συντόμευση παίρνει την τιμή (**l**).

Αλλάζω τα δικαιώματα με την εντολή chmod [options] [MODE] FileName όπου ακολουθώ τον παρακάτω πίνακα για να βάλω τον αριθμό για τα δικαιώματα.

File Permission

#	File Permission
0	none
1	execute only
2	write only
3	write and execute
4	read only
5	read and execute
6	read and write
7	set all permissions

```
anjelina@anji:~$ chmod 777 public_tmima_Pwlisewn
anjelina@anji:~$ chmod 777 public_Oikonomiko_tmima
anjelina@anji:~$ chmod 777 public_tmima_diaxeiristwn
anjelina@anji:~$ chmod 770 private_tmima_Pwlisewn
anjelina@anji:~$ chmod 770 private_Oikonomiko_tmima
anjelina@anji:~$ chmod 770 private_tmima_diaxeiristwn
```

Και για τις περιοχές του κάθε τμήματος:

```
anjelina@anji:~$ chmod 774 periox_i_tmima_Pwlisewn
anjelina@anji:~$ chmod 774 periox_i_Oikonomiko_tmima
anjelina@anji:~$ chmod 774 periox_i_tmima_diaxeiristwn
anjelina@anji:~$
```

Τώρα στο κάθε τμήμα βάζω τα ανάλογα στοιχεία-φακέλους με την εντολή

```
sudo chgrp tmima_pwlisewn public_tmima_Pwlisewn
sudo chgrp tmima_pwlisewn private_tmima_Pwlisewn
sudo chgrp tmima_pwlisewn periox_i_tmima_Pwlisewn
```

```
sudo chgrp tmima_pwlisewn perioxi_Vasilis
sudo chgrp tmima_pwlisewn perioxi_Giurgos
```

```
anjelina@anji:~$ sudo chgrp tmima_pwlisewn public_tmima_Pwlisewn
anjelina@anji:~$ sudo chgrp tmima_pwlisewn private_tmima_Pwlisewn
anjelina@anji:~$ sudo chgrp tmima_pwlisewn perioxi_tmima_Pwlisewn
[sudo] password for anjelina:
anjelina@anji:~$ sudo chgrp tmima_pwlisewn perioxi_Vasilis
anjelina@anji:~$ sudo chgrp tmima_pwlisewn perioxi_Giurgos
anjelina@anji:~$
```

```
sudo chgrp oikonomiko_tmima public_Oikonomiko_tmima
sudo chgrp oikonomiko_tmima private_Oikonomiko_tmima
sudo chgrp oikonomiko_tmima perioxi_Oikonomiko_tmima
sudo chgrp oikonomiko_tmima perioxi_Giannis
sudo chgrp oikonomiko_tmima perioxi_Maria
sudo chgrp oikonomiko_tmima perioxi_Eleni
sudo chgrp tmima_pwlisewn perioxi_Eleni
```

```
anjelina@anji:~$ sudo chgrp tmima_pwlisewn public_tmima_Pwlisewn
anjelina@anji:~$ sudo chgrp tmima_pwlisewn private_tmima_Pwlisewn
anjelina@anji:~$ sudo chgrp tmima_pwlisewn perioxi_tmima_Pwlisewn
[sudo] password for anjelina:
anjelina@anji:~$ sudo chgrp tmima_pwlisewn perioxi_Vasilis
anjelina@anji:~$ sudo chgrp tmima_pwlisewn perioxi_Giurgos
anjelina@anji:~$ sudo chgrp oikonomiko_tmima public_oikonomiko_tmima
chgrp: cannot access `public_oikonomiko_tmima': No such file or directory
anjelina@anji:~$ sudo chgrp oikonomiko_tmima public_Oikonomiko_tmima
anjelina@anji:~$ sudo chgrp oikonomiko_tmima private_Oikonomiko_tmima
anjelina@anji:~$ sudo chgrp oikonomiko_tmima perioxi_Oikonomiko_tmima
anjelina@anji:~$ sudo chgrp oikonomiko_tmima perioxi_Giannis
anjelina@anji:~$ sudo chgrp oikonomiko_tmima perioxi_Maria
anjelina@anji:~$ sudo chgrp oikonomiko_tmima perioxi_Eleni
anjelina@anji:~$ sudo chgrp tmima_pwlisewn perioxi_Eleni
anjelina@anji:~$
```

```
sudo chgrp tmima_diaxeiristwn public_tmima_diaxeiristwn
sudo chgrp tmima_diaxeiristwn private_tmima_diaxeiristwn
sudo chgrp tmima_diaxeiristwn perioxi_tmima_diaxeiristwn
sudo chgrp tmima_diaxeiristwn perioxi_Nikos
sudo chgrp tmima_diaxeiristwn perioxi_Tasos
```

```
anjelina@anji:~$ sudo chgrp tmima_diaxeiristwn public_tmima_diaxeiristwn
[sudo] password for anjelina:
anjelina@anji:~$ sudo chgrp tmima_diaxeiristwn private_tmima_diaxeiristwn
anjelina@anji:~$ sudo chgrp tmima_diaxeiristwn perioxi_tmima_diaxeiristwn
anjelina@anji:~$ sudo chgrp tmima_diaxeiristwn perioxi_Nikos
anjelina@anji:~$ sudo chgrp tmima_diaxeiristwn perioxi_Tasos
anjelina@anji:~$
```

Βλέπω με την εντολή `ls-l` τις αλλαγές στα δικαιώματα που έκανα:


```
Desktop
anjelina@anjli: ~
anjelina@anjli:~$ ls -l
total 96
drwxr-xr-x 2 anjelina anjelina      4096 Apr  1 22:43 Desktop
drwxr-xr-x 2 anjelina anjelina      4096 Apr  1 22:43 Documents
drwxr-xr-x 2 anjelina anjelina      4096 Apr  1 22:43 Downloads
drwxr-xr-x 2 anjelina anjelina      4096 Apr  1 22:43 Music
drwxrwxr-x 2 anjelina tmima_pwlisewn 4096 Apr 18 19:38 perioxi_Eleni
drwxrwxr-x 2 anjelina oikonomiko_tmima 4096 Apr 18 19:39 perioxi_Gianni
s
drwxrwxr-x 2 anjelina tmima_pwlisewn 4096 Apr 18 19:39 perioxi_Glwrgo
s
drwxrwxr-x 2 anjelina oikonomiko_tmima 4096 Apr 18 19:39 perioxi_Maria
drwxrwxr-x 2 anjelina tmima_diaxeiristwn 4096 Apr 18 19:39 perioxi_Nikos
drwxrwxr-- 2 anjelina oikonomiko_tmima 4096 Apr 18 19:37 perioxi_Oikono
miko_tmima
drwxrwxr-x 2 anjelina tmima_diaxeiristwn 4096 Apr 18 19:39 perioxi_Tasos
drwxrwxr-- 2 anjelina tmima_diaxeiristwn 4096 Apr 18 19:38 perioxi_tmima_
diaxeiristwn
drwxrwxr-- 2 anjelina tmima_pwlisewn 4096 Apr 18 19:37 perioxi_tmima_
Pwlisewn
drwxrwxr-x 2 anjelina tmima_pwlisewn 4096 Apr 18 19:39 perioxi_Vasilli
s
drwxr-xr-x 2 anjelina anjelina      4096 Apr  1 22:43 Pictures
drwxrwx-- 2 anjelina oikonomiko_tmima 4096 Apr 18 19:33 private_Oikono
miko_tmima
drwxrwxr-x 2 anjelina tmima_diaxeiristwn 4096 Apr 18 19:33 private_tmima_
diaxeiristwn
drwxrwx-- 2 anjelina tmima_pwlisewn 4096 Apr 18 19:33 private_tmima_
Pwlisewn
drwxr-xr-x 2 anjelina anjelina      4096 Apr  1 22:43 Public
drwxrwxrwx 2 anjelina oikonomiko_tmima 4096 Apr 18 19:33 public_oikonom
iko_tmima
drwxrwxrwx 2 anjelina tmima_diaxeiristwn 4096 Apr 18 19:33 public_tmima_d
iaxeiristwn
drwxrwxrwx 2 anjelina tmima_pwlisewn 4096 Apr 18 19:32 public_tmima_P
wlisewn
drwxr-xr-x 2 anjelina anjelina      4096 Apr  1 22:43 Templates
drwxr-xr-x 2 anjelina anjelina      4096 Apr  1 22:43 Videos
anjelina@anjli:~$
```

Μετά μετακινώ τις προσωπικές περιοχές του κάθε χρήστη στην ιδιωτική περιοχή της ομάδας του με την εντολή mv private_tmima perioxi_onomaXristi

```
Termina File Edit View Search Terminal Help
anjelina@anjli: ~
anjelina@anjli:~$ mv perioxi_Vasilis private_tmima_Pwlisewn
anjelina@anjli:~$ mv perioxi_Glwrgos private_tmima_Pwlisewn
anjelina@anjli:~$ mv perioxi_Eleni private_tmima_Pwlisewn
anjelina@anjli:~$ mv perioxi_Eleni private_Oikonomiko_tmima
anjelina@anjli:~$ mv perioxi_Maria private_Oikonomiko_tmima
anjelina@anjli:~$ mv perioxi_Giannis private_Oikonomiko_tmima
anjelina@anjli:~$ mv perioxi_Nikos private_tmima_diaxeiristwn
anjelina@anjli:~$ mv perioxi_Tasos private_tmima_diaxeiristwn
anjelina@anjli:~$
```

Και μετά επιβεβαιώνω την μετακίνηση

```
anjelina@anjli:~$ ls -l
total 68
drwxr-xr-x 2 anjelina anjelina      4096 Apr  1 22:43 Desktop
drwxr-xr-x 2 anjelina anjelina      4096 Apr  1 22:43 Documents
drwxr-xr-x 2 anjelina anjelina      4096 Apr  1 22:43 Downloads
drwxr-xr-x 2 anjelina anjelina      4096 Apr  1 22:43 Music
drwxrwxr-- 2 anjelina oikonomiko_tmima 4096 Apr 18 19:37 perioxi_Oikonomiko_tm
ima
drwxrwxr-- 2 anjelina tmima_diaxeiristwn 4096 Apr 18 19:38 perioxi_tmima_diaxeir
istwn
drwxrwxr-- 2 anjelina tmima_pwlisewn 4096 Apr 18 19:37 perioxi_tmima_Pwlisew
n
drwxr-xr-x 2 anjelina anjelina      4096 Apr  1 22:43 Pictures
drwxrwx-- 4 anjelina oikonomiko_tmima 4096 Apr 19 20:54 private_Oikonomiko_tm
ima
drwxrwxr-x 4 anjelina tmima_diaxeiristwn 4096 Apr 19 20:55 private_tmima_diaxeir
istwn
drwxrwx-- 5 anjelina tmima_pwlisewn 4096 Apr 19 20:51 private_tmima_Pwlisew
n
drwxr-xr-x 2 anjelina anjelina      4096 Apr  1 22:43 Public
drwxrwxrwx 2 anjelina oikonomiko_tmima 4096 Apr 18 19:33 public_Oikonomiko_tm
ima
drwxrwxrwx 2 anjelina tmima_diaxeiristwn 4096 Apr 18 19:33 public_tmima_diaxeir
istwn
drwxrwxrwx 2 anjelina tmima_pwlisewn 4096 Apr 18 19:32 public_tmima_Pwlisew
n
drwxr-xr-x 2 anjelina anjelina      4096 Apr  1 22:43 Templates
drwxr-xr-x 2 anjelina anjelina      4096 Apr  1 22:43 Videos
anjelina@anjli:~$
```

Μετά πρέπει να αλλάξουμε και του ιδιοκτήτες των αρχείων με την εντολή chown για να μην βγάξει το anjelina αλλά τα ονόματα των χρηστών.

```
anjelina@anji:~$ cd private_tmima_Pwliisewn
anjelina@anji:~/private_tmima_Pwliisewn$ ls -l
total 12
drwxrwxr-x 2 anjelina tmima_Pwliisewn 4096 Apr 18 19:38 perioxi_Eleni
drwxrwxr-x 2 anjelina tmima_Pwliisewn 4096 Apr 18 19:39 perioxi_Giurgos
drwxrwxr-x 2 anjelina tmima_Pwliisewn 4096 Apr 18 19:39 perioxi_Vasilis
anjelina@anji:~/private_tmima_Pwliisewn$ cd..
cd..: command not found
anjelina@anji:~/private_tmima_Pwliisewn$ cd ..
anjelina@anji:~$ sudo chown Vasilis private_tmima_Pwliisewn/perioxi_Vasilis
[sudo] password for anjelina:
anjelina@anji:~$ sudo chown Eleni private_tmima_Pwliisewn/perioxi_Eleni
anjelina@anji:~$ sudo chown Giurgos private_tmima_Pwliisewn/perioxi_Giurgos
chown: invalid user: 'Giurgos'
anjelina@anji:~$ sudo chown Gewrge private_tmima_Pwliisewn/perioxi_Giurgos
anjelina@anji:~$
```

```
anjelina@anji:~$ sudo chown Maria private_Oikonomiko_tmima/perioxi_Maria
chown: invalid user: 'Maria'
anjelina@anji:~$ sudo chown maria private_Oikonomiko_tmima/perioxi_Maria
anjelina@anji:~$ sudo chown giannis private_Oikonomiko_tmima/perioxi_Giannis
anjelina@anji:~$ sudo chown Nikos private_Oikonomiko_tmima/perioxi_Nikos
chown: cannot access 'private_Oikonomiko_tmima/perioxi_Nikos': No such file or directory
anjelina@anji:~$ sudo chown Nikos private_tmima_diaxeiristwn/perioxi_Nikos
anjelina@anji:~$ sudo chown Tasos private_tmima_diaxeiristwn/perioxi_Tasos
anjelina@anji:~$
```

Πρέπει μόνο οι χρήστες αυτοί να έχουν πρόσβαση σε αυτούς τους φακέλους και όχι άλλοι (groups - others) οπότε αλλάζω και άλλα δικαιώματα. Πάω στο φάκελο του κάθε τμήματος και πατάω τα παρακάτω:

```
sudo chmod 700 perioxi_Eleni
sudo chmod 700 perioxi_Vasilis
sudo chmod 700 perioxi_Giurgos
```

```
@anji: ~/private_tmima_diaxeiristwn
anjelina@anji:~/private_tmima_Pwliisewn$ sudo chmod 700 perioxi_Eleni
anjelina@anji:~/private_tmima_Pwliisewn$ sudo chmod 700 perioxi_Giurgos
anjelina@anji:~/private_tmima_Pwliisewn$ sudo chmod 700 perioxi_Vasilis
anjelina@anji:~/private_tmima_Pwliisewn$ cd ..
anjelina@anji:~$ cd private_Oikonomiko_tmima
anjelina@anji:~/private_Oikonomiko_tmima$ sudo chmod 700 perioxi_Maria
anjelina@anji:~/private_Oikonomiko_tmima$ sudo chmod 700 perioxi_Giannis
anjelina@anji:~/private_Oikonomiko_tmima$ cd ..
Firefox Web Browser private_tmima_diaxeiristwn
anjelina@anji:~/private_tmima_diaxeiristwn$ sudo chmod 700 perioxi_Tasos
anjelina@anji:~/private_tmima_diaxeiristwn$ sudo chmod 700 perioxi_Nikos
anjelina@anji:~/private_tmima_diaxeiristwn$
```

Οπότε τώρα βλέπω τις περιοχές του κάθε χρήστη και τα δικαιώματα:

```
LibreOffice Writer private_tmima_diaxeiristwn$ ls -l
total 8
drwx----- 2 Nikos tmima_diaxeiristwn 4096 Apr 18 19:39 perioxi_Nikos
drwx----- 2 Tasos tmima_diaxeiristwn 4096 Apr 18 19:39 perioxi_Tasos
anjelina@anji:~/private_tmima_diaxeiristwn$ cd ..
anjelina@anji:~$ cd private_Oikonomiko_tmima
anjelina@anji:~/private_Oikonomiko_tmima$ ls -l
total 8
drwx----- 2 giannis oikonomiko_tmima 4096 Apr 18 19:39 perioxi_Giannis
drwx----- 2 maria oikonomiko_tmima 4096 Apr 18 19:39 perioxi_Maria
anjelina@anji:~/private_Oikonomiko_tmima$ cd ..
anjelina@anji:~$ cd private_tmima_Pwlisewn
anjelina@anji:~/private_tmima_Pwlisewn$ ls -l
total 12
drwx----- 2 Eleni tmima_pwlisewn 4096 Apr 18 19:38 perioxi_Eleni
drwx----- 2 Gewrge tmima_pwlisewn 4096 Apr 18 19:39 perioxi_Giwrghos
drwx----- 2 Vasilis tmima_pwlisewn 4096 Apr 18 19:39 perioxi_Vasilis
anjelina@anji:~/private_tmima_Pwlisewn$
```

Τι θα αλλάζατε στα δικαιώματα πρόσβασης αν για κάποιο λόγο ο Βασίλης θα έπρεπε να αποκλειστεί εντελώς από την πρόσβαση στην αυστηρά ελεγχόμενη περιοχή εργασίας της ομάδας του;

Αφού θα αποκλειστεί θα τον διέγραφα για να μην έχει κανένα δικαίωμα με την εντολή:

```
userdel Vasilis private_tmima_Pwlisewn
```

Ρυθμίστε κατάλληλα τον εξυπηρετητή που εργάζεστε έτσι ώστε να παράγονται συμβάντα (logs) κάθε φορά που ένας χρήστης προσπαθεί να αποκτήσει πρόσβαση σε περιοχή που δεν έχει τα απαραίτητα δικαιώματα. Εκτελέστε κάποια σενάρια έτσι ώστε να προκαλείται η δημιουργία αυτών των συμβάντων.

Με την παρακάτω εντολή φαίνονται τα log που υπάρχουν

```
anjelina@anji:~$ ls -l /var/log
total 4208
-rw-r--r-- 1 root root 34179 Apr 1 21:34 alternatives.log
drwxr-x--- 2 root adm 4096 Apr 19 22:54 apache2
drwxr-xr-x 2 root root 4096 Mar 29 17:13 apt
-rw-r----- 1 syslog adm 3969 Apr 20 00:17 auth.log
-rw-r----- 1 syslog adm 113788 Apr 19 22:49 auth.log-20130419
-rw-r----- 1 root adm 31 Oct 17 2012 boot
-rw-r--r-- 1 root root 2495 Apr 19 20:46 boot.log
-rw-r--r-- 1 root root 49450 Oct 17 2012 bootstrap.log
-rw-rw---- 1 root utmp 1152 Mar 31 17:17 btmp
```

Εμάς μας ενδιαφέρει το faillog στο οποίο καταγράφονται οι αποτυχημένες προσπάθειες σύνδεσης από ένα χρήστη σε περιοχές χωρίς δικαιώματα. Με την εντολή faillog -u root βλέπω τα υπάρχον συμβάντα για συγκεκριμένο χρήστη.

```
anjelina@anji: ~
anjelina@anji:~$ faillog -u root
Login      Failures Maximum Latest      On
root       0          0      01/01/70 02:00:00 +0200
anjelina@anji:~$
```

Και παρακάτω όλα τα συμβάντα:

```
anjelina@anji: ~
anjelina@anji:~$ faillog -r anjelina
faillog: Cannot open /var/log/faillog: Permission denied
anjelina@anji:~$ faillog -t anjelina
faillog: invalid numeric argument 'anjelina'
anjelina@anji:~$ faillog -a
Login      Failures Maximum Latest      On
root       0          0      01/01/70 02:00:00 +0200
breOffice Impress 0          0      01/01/70 02:00:00 +0200
ben        0          0      01/01/70 02:00:00 +0200
sys        0          0      01/01/70 02:00:00 +0200
sync       0          0      01/01/70 02:00:00 +0200
games      0          0      01/01/70 02:00:00 +0200
man        0          0      01/01/70 02:00:00 +0200
lp         0          0      01/01/70 02:00:00 +0200
mail       0          0      01/01/70 02:00:00 +0200
news       0          0      01/01/70 02:00:00 +0200
uucp       0          0      01/01/70 02:00:00 +0200
proxy      0          0      01/01/70 02:00:00 +0200
www-data   0          0      01/01/70 02:00:00 +0200
backup     0          0      01/01/70 02:00:00 +0200
list       0          0      01/01/70 02:00:00 +0200
irc        0          0      01/01/70 02:00:00 +0200
gnats      0          0      01/01/70 02:00:00 +0200
```

Στους φακέλους που έχουν πρόσβαση αποκλειστικά μόνο τα μέλη της κάθε ομάδας μπορούμε να δημιουργήσουμε μεμονωμένους υποφακέλους ή αρχεία στα οποία να επιτρέψουμε την πρόσβαση (ανάγνωση/εγγραφή) σε χρήστες που δεν είναι μέλη της ομάδας; Περιγράψτε τη διαδικασία.

Μπορούμε να δημιουργήσουμε αρκεί να μπούμε στον private χώρο κάθε τμήματος και να φτιάξουμε φακέλους και αρχεία με δικαιώματα 774 για ανάγνωση μόνο από άλλους χρήστες ή 776 και για ανάγνωση και εγγραφή.

Παρακάτω κάνω ένα παράδειγμα με φάκελο :

```
anjelina@anji: ~/private_tmima_Pwllisewn
anjelina@anji:~$ cd private_tmima_Pwllisewn
anjelina@anji:~/private_tmima_Pwllisewn$ mkdir arxeio_anagnwsis
anjelina@anji:~/private_tmima_Pwllisewn$ ls -l
total 16
drwxrwxr-x 2 anjelina anjelina 4096 Apr 20 20:24 arxeio_anagnwsis
drwx----- 2 Eleni tmima_pwllisewn 4096 Apr 18 19:38 perioxi_Eleni
drwx----- 2 Gewrge tmima_pwllisewn 4096 Apr 18 19:39 perioxi_Giwrkos
drwx----- 2 Vasilis tmima_pwllisewn 4096 Apr 18 19:39 perioxi_Vasilis
anjelina@anji:~/private_tmima_Pwllisewn$ chmod 774 arxeio_anagnwsis
anjelina@anji:~/private_tmima_Pwllisewn$ ls -l
total 16
drwxrwxr-- 2 anjelina anjelina 4096 Apr 20 20:24 arxeio_anagnwsis
drwx----- 2 Eleni tmima_pwllisewn 4096 Apr 18 19:38 perioxi_Eleni
drwx----- 2 Gewrge tmima_pwllisewn 4096 Apr 18 19:39 perioxi_Giwrkos
drwx----- 2 Vasilis tmima_pwllisewn 4096 Apr 18 19:39 perioxi_Vasilis
anjelina@anji:~/private_tmima_Pwllisewn$ chmod 776 arxeio_anagnwsis
anjelina@anji:~/private_tmima_Pwllisewn$ ls -l
total 16
drwxrwxrw- 2 anjelina anjelina 4096 Apr 20 20:24 arxeio_anagnwsis
drwx----- 2 Eleni tmima_pwllisewn 4096 Apr 18 19:38 perioxi_Eleni
drwx----- 2 Gewrge tmima_pwllisewn 4096 Apr 18 19:39 perioxi_Giwrkos
drwx----- 2 Vasilis tmima_pwllisewn 4096 Apr 18 19:39 perioxi_Vasilis
anjelina@anji:~/private_tmima_Pwllisewn$
```

Παρακάτω κάνω ένα παράδειγμα με αρχείο :

```
anjelina@anji: ~/private_tmima_Pwllisewn
drwx----- 2 Vasilis tmima_pwllisewn 4096 Apr 18 19:39 perioxi_Vasilis
anjelina@anji:~/private_tmima_Pwllisewn$ nano _arxeio
anjelina@anji:~/private_tmima_Pwllisewn$ ls -l
total 28
-rw-rw-r-- 1 anjelina anjelina 13 Apr 20 20:37 arxeio
drwxrwxrw- 2 anjelina anjelina 4096 Apr 20 20:24 arxeio_anagnwsis
drwx----- 2 Eleni tmima_pwllisewn 4096 Apr 18 19:38 perioxi_Eleni
drwx----- 2 Gewrge tmima_pwllisewn 4096 Apr 18 19:39 perioxi_Giwrkos
drwx----- 2 Vasilis tmima_pwllisewn 4096 Apr 18 19:39 perioxi_Vasilis
anjelina@anji:~/private_tmima_Pwllisewn$ chmod 774 arxeio
anjelina@anji:~/private_tmima_Pwllisewn$ ls -l
total 28
-rwxrwxr-- 1 anjelina anjelina 13 Apr 20 20:37 arxeio
drwxrwxrw- 2 anjelina anjelina 4096 Apr 20 20:24 arxeio_anagnwsis
drwx----- 2 Eleni tmima_pwllisewn 4096 Apr 18 19:38 perioxi_Eleni
drwx----- 2 Gewrge tmima_pwllisewn 4096 Apr 18 19:39 perioxi_Giwrkos
drwx----- 2 Vasilis tmima_pwllisewn 4096 Apr 18 19:39 perioxi_Vasilis
anjelina@anji:~/private_tmima_Pwllisewn$ chmod 776 arxeio
anjelina@anji:~/private_tmima_Pwllisewn$ ls -l
total 28
-rwxrwxrw- 1 anjelina anjelina 13 Apr 20 20:37 arxeio
drwxrwxrw- 2 anjelina anjelina 4096 Apr 20 20:24 arxeio_anagnwsis
drwx----- 2 Eleni tmima_pwllisewn 4096 Apr 18 19:38 perioxi_Eleni
drwx----- 2 Gewrge tmima_pwllisewn 4096 Apr 18 19:39 perioxi_Giwrkos
drwx----- 2 Vasilis tmima_pwllisewn 4096 Apr 18 19:39 perioxi_Vasilis
anjelina@anji:~/private_tmima_Pwllisewn$
```

Υπάρχει τρόπος να αποτρέψουμε την πρόσβαση σε μια συγκεκριμένη περιοχή από τους διαχειριστές του συστήματος (System Administrators). Υπάρχει η δυνατότητα ο διαχειριστής να παρακάμψει τα δικαιώματα πρόσβασης που έχουμε ορίσει; Περιγράψτε αντίστοιχο σενάριο.

Αν βάλω στους users δικαιώματα 0 τότε δέν μπορούν να μπουν σε μια περιοχή. Δίνω ένα παράδειγμα με την δημιουργία φακέλου στην περιοχή των διαχειριστών.


```

anjelina@anji:~$ cd private_tmima_diaxeiristwn
anjelina@anji:~/private_tmima_diaxeiristwn$ mkdir test1
anjelina@anji:~/private_tmima_diaxeiristwn$ ls -l
total 12
drwx----- 2 Nikos      tmima_diaxeiristwn 4096 Apr 18 19:39 perioxi_Nikos
drwx----- 2 Tasos      tmima_diaxeiristwn 4096 Apr 18 19:39 perioxi_Tasos
drwxrwxr-x 2 anjelina  anjelina          4096 Apr 20 19:46 test1
anjelina@anji:~/private_tmima_diaxeiristwn$ chmod 072 test1
anjelina@anji:~/private_tmima_diaxeiristwn$ ls -l
total 12
drwx----- 2 Nikos      tmima_diaxeiristwn 4096 Apr 18 19:39 perioxi_Nikos
drwx----- 2 Tasos      tmima_diaxeiristwn 4096 Apr 18 19:39 perioxi_Tasos
d---rwx-w- 2 anjelina  anjelina          4096 Apr 20 19:46 test1
anjelina@anji:~/private_tmima_diaxeiristwn$ cd test1
bash: cd: test1: Permission denied
anjelina@anji:~/private_tmima_diaxeiristwn$

```

Παρακάτω φτιάχνω αρχείο

```

anjelina@anji: ~
private_tmima_diaxeiristwn
private_tmima_Pwlisewn
Public
public_Oikonomiko_tmima
public_tmima_diaxeiristwn
public_tmima_Pwlisewn
Templates
Videos
anjelina@anji:~$ mkdir oxiprosvasi
anjelina@anji:~$ ls -l
total 72
drwxr-xr-x 2 anjelina anjelina          4096 Apr  1 22:43 Desktop
drwxr-xr-x 2 anjelina anjelina          4096 Apr  1 22:43 Documents
drwxr-xr-x 2 anjelina anjelina          4096 Apr  1 22:43 Downloads
drwxr-xr-x 2 anjelina anjelina          4096 Apr  1 22:43 Music
drwxrwxr-x 2 anjelina anjelina          4096 Apr 20 20:59 oxiprosvasi
drwxrwxr-- 2 anjelina oikonomiko_tmima  4096 Apr 18 19:37 perioxi_Oikonomiko_tmima
drwxrwxr-- 2 anjelina tmima_diaxeiristwn 4096 Apr 18 19:38 perioxi_tmima_diaxeiristwn

```

Αλλάζω δικαιώματα και βλέπω ότι δεν έχω δικαίωμα να δω τον φάκελο

```

anjelina@anji:~$ ls -l
total 72
drwxrwxrwx 2 anjelina tmima_pwlisewn    4096 Apr 18 19:32 public_tmima_Pwlisewn
drwxr-xr-x 2 anjelina anjelina          4096 Apr  1 22:43 Templates
drwxr-xr-x 2 anjelina anjelina          4096 Apr  1 22:43 Videos
anjelina@anji:~$ chmod 077 oxiprosvasi
anjelina@anji:~$ cd oxiprosvasi
bash: cd: oxiprosvasi: Permission denied
anjelina@anji:~$ ls oxiprosvasi
ls: cannot open directory oxiprosvasi: Permission denied

```

Υπάρχει όμως η δυνατότητα ο διαχειριστής να παρακάμψει τα δικαιώματα πρόσβασης που έχουμε ορίσει με την εντολή sudo όπως φαίνετε παρακάτω:

```

Videos
anjelina@anji:~$ cd | sudo tee /root/oxiprosvasi
anjelina@anji:~$ ls | sudo tee /root/oxiprosvasi
Desktop
Documents
Downloads
Music
oxiprosvasi
perioxi_Oikonomiko_tmima
perioxi_tmima_diaxeiristwn
perioxi_tmima_Pwlisewn
Pictures
private_Oikonomiko_tmima
private_tmima_diaxeiristwn
private_tmima_Pwlisewn
Public
public_Oikonomiko_tmima
public_tmima_diaxeiristwn
public_tmima_Pwlisewn
Templates
Videos
anjelina@anji:~$

```

Θα μπορούσαμε να περάσουμε το σύνολο εντολών σε μια διαδικασία κέλυφος που λειτουργεί υπό sudo για να έχουμε στο αρχείο δικαίωμα για γράψιμο με δικαιώματα root.

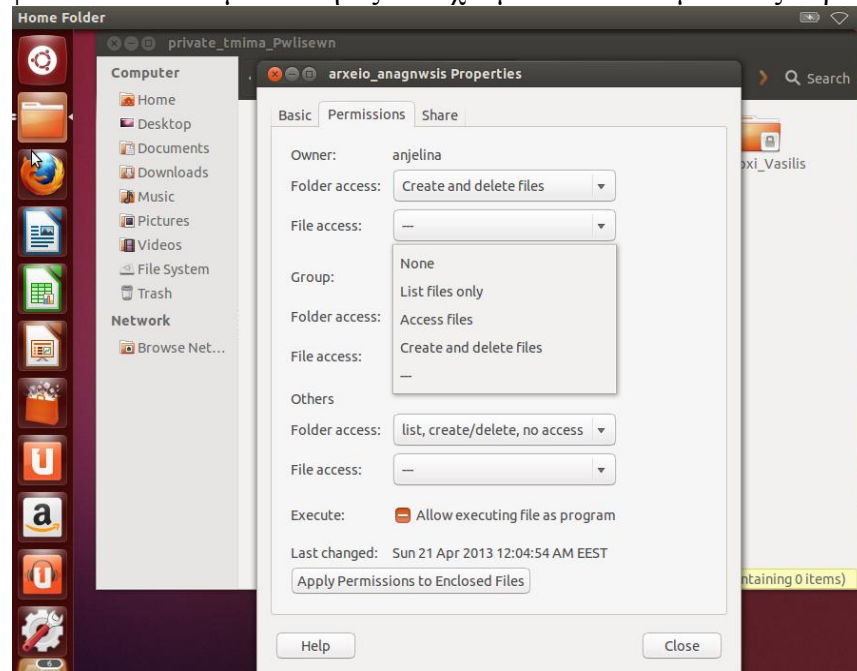
```

anjelina@anji:~$ sh -c "ls > /root/oxiprosvasi"
sh: 1: cannot create /root/oxiprosvasi: Permission denied
anjelina@anji:~$ sudo sh -c "ls > /root/oxiprosvasi"
anjelina@anji:~$

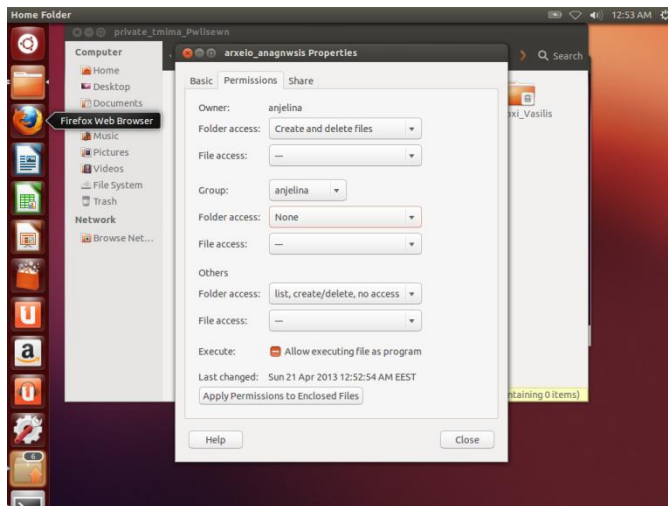
```

Τι δικαιώματα απαιτείται να δώσετε σε ένα φάκελο έτσι ώστε:
α) να μην μπορεί κάποιος να δημιουργήσει νέους υποφακέλους αλλά μόνο αρχεία

Μπορούμε να το κάνουμε γραφικά πηγαίνοντας στις ρυθμίσεις, πάμε πάνω στον φάκελο και πατάμε ιδιότητες και έχουμε στα δικαιώματα τις παρακάτω επιλογές:



Αν θέλουμε για παράδειγμα το group να μην μπορεί να κάνει υποφακέλους τότε πάμε στην κατηγορία του group και επιλέγω οτιδήποτε άλλο εκτός από το create and delete files όπως φαίνετε παρακάτω:



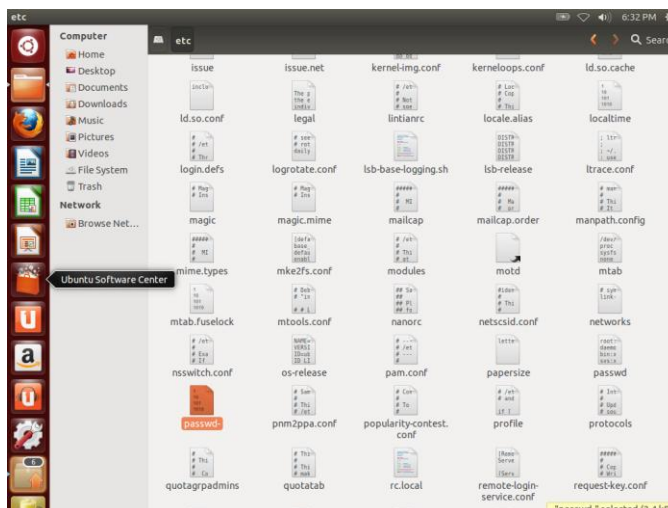
β) να μην μπορεί κάποιος να σβήσει αρχεία (ή υποφακέλους), αλλά μόνο να προσθέσει (ή να δημιουργήσει) νέα αρχεία και νέους υποφακέλους;

Με την εντολή `chmod 0+t private_tmima_pwlisewn` θέτω σε κατάσταση Sticky bit τον κατάλογο και δεν μπορεί κάποιος να τον σβήσει. Με τις παρακάτω εντολές δεν επιτρέπω την διαγραφή υποφακέλων.

```
setfacl --set u::rwx,g::rwx /controlled
setfacl -d --set u::r-x,g::r-x,o::- /controlled
```

Υπάρχει τρόπος ο διαχειριστής να παρακολουθήσει την πρόσβαση σε κάποιο κρίσιμο αρχείο (π.χ. ένα αρχείο με passwords) ;

Το αρχείο passwords στα linux είναι το `passwd` που βρίσκετε μέσα στον `/etc`

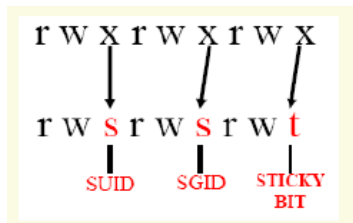


Όπου μπορούμε να δούμε τι περιέχει ως διαχειριστής.

Ποια είναι η χρησιμότητα των πρόσθετων ειδικών δικαιωμάτων που παρέχονται σε ένα Unix λειτουργικό σύστημα δηλαδή των δικαιωμάτων Set User ID (SUID), Set Group ID (SGID) και Sticky bit (STB); Περιγράψτε και εφαρμόστε χαρακτηριστικά σενάρια που να είναι απαραίτητη η χρήση των συγκεκριμένων δικαιωμάτων πρόσβασης.

Ειδικά Δικαιώματα (Special Permissions)

Η κατάσταση των δικαιωμάτων πρόσβασης που εμφανίζεται με την εντολή «*ls -l*» δεν έχει ξεχωριστό τμήμα για τα ειδικά δικαιώματα. – Επειδή τα ειδικά δικαιώματα απαιτούν «*execute*», καλύπτουν/αντικαθιστούν το δικαίωμα *execute* με την εντολή «*ls -l*».



Εάν τα ειδικά δικαιώματα ρυθμίζονται σε αρχεία ή καταλόγους που δεν έχουν *execute* δικαίωμα, τότε τα ειδικά δικαιώματα εμφανίζονται με κεφαλαία γράμματα.

Ρύθμιση Ειδικών Δικαιωμάτων π.χ. *chmod 7777 filename* με

suid	sgid	stb
4	2	1
7		
Special		

Set User ID (SUID) σε εκτελέσιμο αρχείο

Το *SUID* επιτρέπει στους χρήστες να εκτελέσουν ένα αρχείο και να γίνουν οι ιδιοκτήτες του αρχείου κατά τη διάρκεια της εκτέλεσης. Η εντολή θα εκτελεστεί με τα δικαιώματα του ιδιοκτήτη του αρχείου και όχι με τα δικαιώματα του χρήστη που εκτελεί την εντολή.

Παράδειγμα:

Η εντολή *passwd* με ιδιοκτήτη τον *root* έχει τις ακόλουθες ειδικές ρυθμίσεις:

ls -l /usr/bin/passwd

-rwsr-xr-x 1 root root 25064 2007-04-05 /usr/bin/passwd

Όταν ένας χρήστης εκτελεί την εντολή *passwd*, ο χρήστης γίνεται προσωρινά ο «*root*» χρήστης για όσο τρέχει η εντολή (συνεπώς μπορεί να γράψει στο */etc/shadow*).

Παράδειγμα:

Η παρακάτω εντολή: **chmod u+s /bin/file1** Θέτει ένα δυαδικό αρχείο σε κατάσταση SUID, δηλαδή ο χρήστης ο οποίος εκτελεί αυτό αρχείο έχει σχεδόν τα ίδια προνόμια με τον ιδιοκτήτη του αρχείου

Παράδειγμα:

Αν a1 είναι ο ιδιοκτήτης του σεναρίου και b2 προσπαθεί να τρέξει το ίδιο σενάριο, το σενάριο τρέχει με την ιδιοκτησία της A1.

Εάν ο χρήστης root επιθυμεί να δώσει άδειες για ορισμένα σενάρια για να τρέξει από διαφορετικούς χρήστες, μπορεί να θέσει τον SUID bit για το συγκεκριμένο σενάριο. Έτσι, αν κάποιος χρήστης στο σύστημα ξεκινά αυτό το σενάριο, θα λειτουργεί υπό την ιδιοκτησία root.

Set Group ID (SGID) σε εκτελέσιμο αρχείο ή Set Group ID (SGID) σε κατάλογο

Όπως η *SUID*, η *SGID* επιτρέπει στους χρήστες να εκτελέσουν ένα αρχείο και να γίνουν μέλος της ομάδας που ανήκει το αρχείο κατά τη διάρκεια της εκτέλεσης.

Το *SGID* για ένα κατάλογο, σημαίνει ότι τα αρχεία που δημιουργούνται μέσα σε αυτόν τον κατάλογο, θα συσχετίζονται με την ομάδα με την οποία είναι συσχετισμένος ο κατάλογος και όχι με την ομάδα του χρήστη.

Sticky bit (STB) σε κατάλογο

Το *Sticky Bit* εκτελεί μια χρήσιμη λειτουργία στους καταλόγους

Να θυμηθούμε ότι το *write* δικαίωμα σε κατάλογο επιτρέπει να προσθέτουμε και να διαγράφουμε αρχεία στον κατάλογο.

Εάν εφαρμοστεί το *Sticky Bit* τότε ορίζεται ότι τα αρχεία που περιέχονται σε ένα κατάλογο, μπορούν να σβηστούν μόνο από τον ιδιοκτήτη τους ή τον χρήστη root, ανεξάρτητα από τα δικαιώματα εγγραφής που έχουν ορισθεί σε κάθε ένα από αυτά.

Παράδειγμα:

sticky bit σε έναν κατάλογο με όνομα mydir ο οποίος βρίσκεται στον προσωπικό μας χώρο.

cd

chmod 1777 mydir

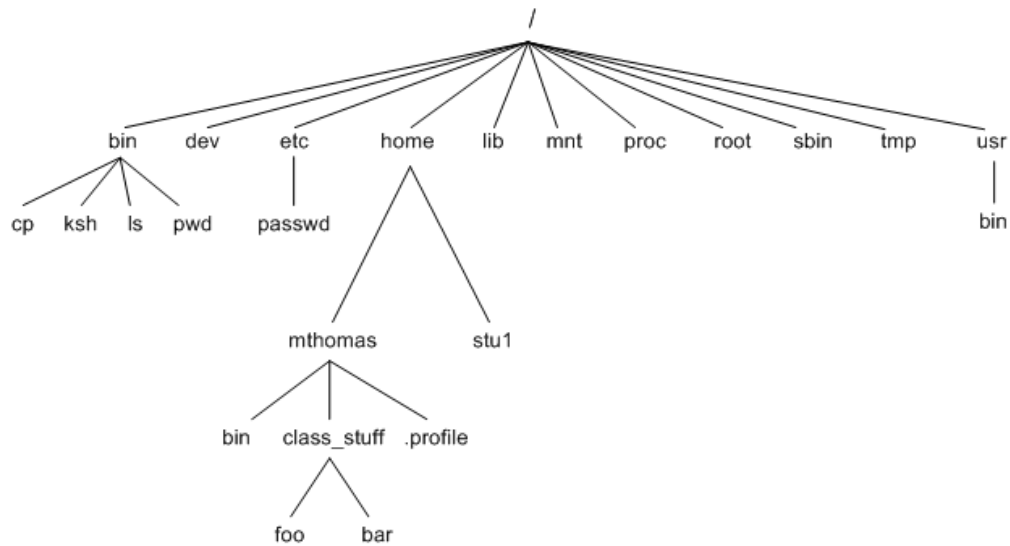
Πόσο διαφορετική είναι η αρχιτεκτονική ελέγχου πρόσβασης σε ένα Unix σύστημα σε σχέση με ένα λειτουργικό σύστημα Windows.

Γενικές διαφορές στις αρχιτεκτονικές των δύο λειτουργικών:

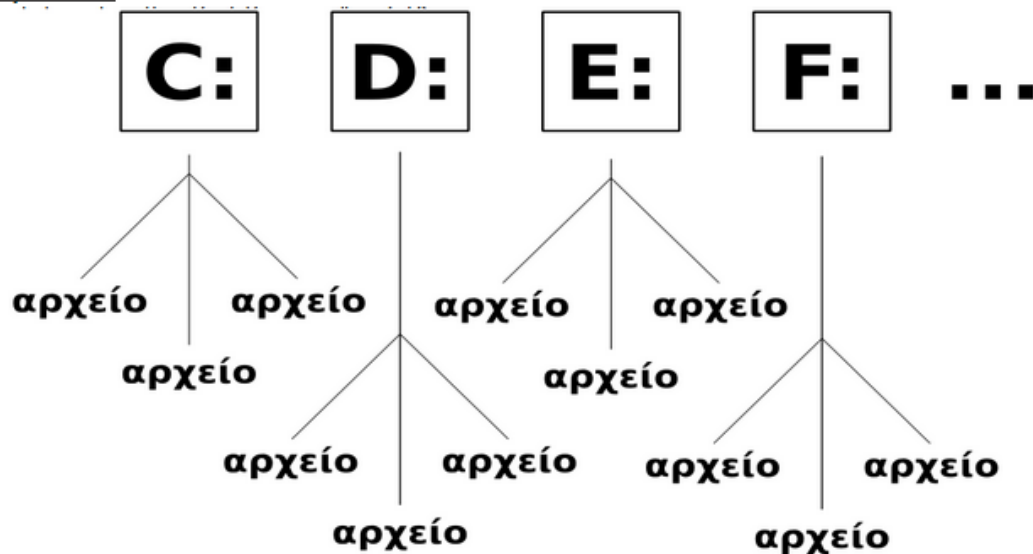
Η δομή των 2 λειτουργικών είναι εντελώς διαφορετική. Στα linux τα πάντα βρίσκονται κάτω από το root directory. Για αυτό και όταν δίνουμε ολόκληρη την διαδρομή ενός αρχείου ξεκινάμε με `' / '`. Είναι παρόμοιο με το C: των windows αν και το Linux δεν έχει γράμματα. Εδώ είναι και μια βασική διαφορά τους, η δομή των αρχείων είναι τέτοια ώστε να θυμίζει δέντρο με κορυφή το `' / '` και μετά

διακλαδώνεται, ενώ στα windows έχουμε δάση από δέντρα καθώς δεν έχουν κοινή αρχή τα partitions, είναι διαφορετικά και έχουν διαφορετικές διακλαδώσεις.

Δέντρο Linux



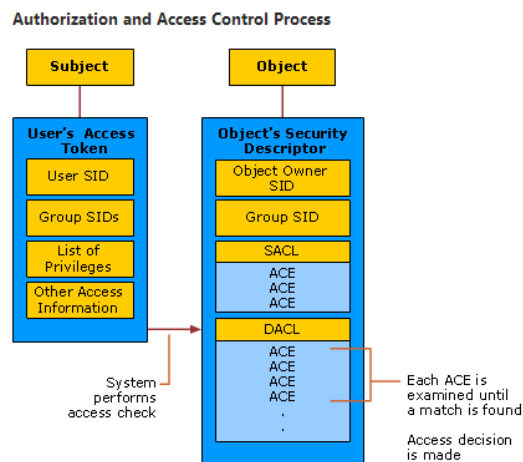
Δάσος Windows



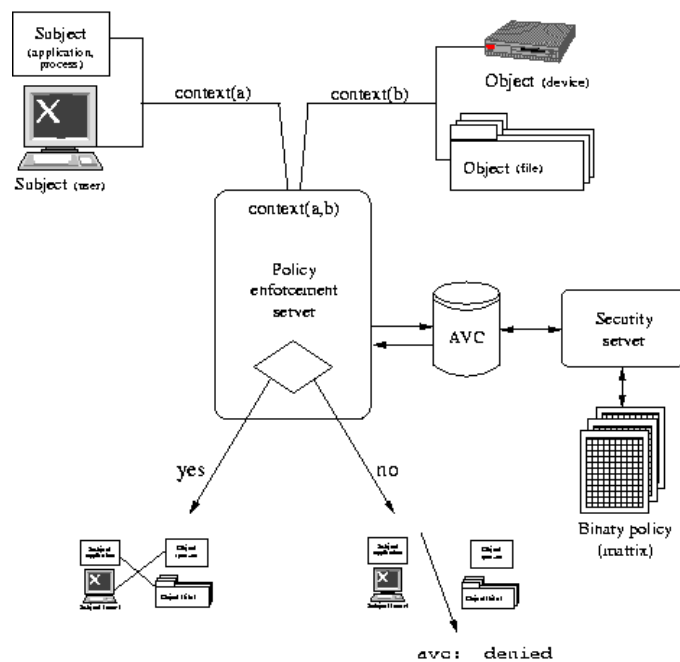
Ο έλεγχος πρόσβασης είναι ένας εσωτερικός (σε ένα λειτουργικό σύστημα) μηχανισμός προστασίας. Μια μορφή ελέγχου πρόσβασης παρατηρείται στις οδηγίες CPU που μπορεί να εκτελεστεί μόνο στη λειτουργία εποπτείας, η οποία συνήθως ανέρχεται μέσα στον πυρήνα. Η διαίρεση της εικονικής μνήμης στον πυρήνα και των χρηστών μέρη είναι επίσης μια μορφή ελέγχου πρόσβασης.

Η έγκριση και η πρόσβαση στο μοντέλο ελέγχου που χρησιμοποιείται στα Windows βασίζεται στις ακόλουθες αρχές:

Χρήστη με βάση την άδεια, διακριτική πρόσβαση σε ασφαλιζόμενα αντικείμενα, μεταβίβαση των δικαιωμάτων, διοικητικά προνόμια και έλεγχος των συμβάντων του συστήματος. Παρακάτω φαίνεται η αρχιτεκτονική



Η έγκριση και η πρόσβαση στο μοντέλο ελέγχου που χρησιμοποιείται στα linux βασίζεται στις ακόλουθες αρχές:



Πόσο διαφορετική είναι η διαχείριση του ελέγχου πρόσβασης στα Windows, σε σύγκριση με τη διαχείριση σε UNIX σύστημα; Ποιο σύστημα διαχείρισης θα λέγατε ότι είναι πιο εύκολο για έναν διαχειριστή; Ποιο θεωρείται ότι είναι πιο αποτελεσματικό;

Σε ένα κουτί των Windows, μπορούμε να ρυθμίσουμε την πρόσβαση μηχανισμών ελέγχου χωρίς λογισμικό add-on. Όπως και στα **Windows** οι σύγχρονες διανομές **Linux** υποστηρίζουν λίστες ελέγχου **Access Control Lists (ACLs)** που βασίζονται στην ασφάλεια για τα αρχεία και

τους καταλόγους.Ωστόσο εκτός από τις ρυθμίσεις των επιχειρήσεων ή όταν χρησιμοποιείται από administrators του συστήματος Linux, οι ACLs δεν είναι πλέον σε χρήση, εκτός αν οι διαχειριστές του συστήματος συνεχίσουν να χρησιμοποιούν το λιγότερο ισχυρό μοντέλο **UNIX** ιδιοκτήτη-ομάδας-κόσμου. Τα Windows User Access Control (UAC),σχεδιάστηκαν ειδικά για να αντιμετωπίσουν το πρόβλημα των χρηστών των Windows και των εφαρμογών για τα οποία δίνεται πολύ μεγάλη δύναμη out-of-the-box.Σε τεχνολογικό επίπεδο συγκρίνω το **UAC** με το **sudo**.Για μένα η πραγματική διαφορά ελέγχου πρόσβασης μεταξύ των Windows και των Linux είναι περισσότερο στην νοοτροπία των χρηστών παρά στην τεχνολογία.Οι χρήστες των Windows χρησιμοποιούν το αρχείο σε επίπεδο ACLs από συνήθεια ,που είναι κάτι καλό,ενώ οι χρήστες των Linux θα συνεχίσουν να χρησιμοποιούν μια παρωχημένη ιδιοκτήτη-ομάδα-μοντέλο άδεια που είναι ξεπερασμένη ακόμα και όταν οι ACLs υποστηρίζουν το ίδιο το σύστημα Linux.

Επομένως μετά την χρήση και των δύο λειτουργικών διαπιστώσαμε ότι τα **Windows** σε επίπεδο ελέγχου πρόσβασης είναι πιο αποτελεσματικά και πιο εύχρηστα στην διαχείριση επειδή διαθέτουν πιο φιλικό γραφικό περιβάλλον ως προς τον χρήστη.Επιπρόσθετα τα Windows έχουν περισσότερες επιλογές διαχείρισης από ότι τα **Linux**.

Βιβλιογραφία:

[http://technet.microsoft.com/en-us/library/cc782880\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc782880(v=ws.10).aspx)

<http://www.networkworld.com/community/blog/comparing-access-control-windows-and-linux>

http://www.linuxguide.it/command_line/linux_commands_gr.html

<http://osarena.net/tutorials/domit-tou-file-system-tou-linux.html>

<http://www.dartmouth.edu/~rc/help/faq/permissions.html>

<http://www.bashguru.com/2010/03/unixlinux-advanced-file-permissions.htm>

<http://www.sevenforums.com/tutorials/7539-local-users-groups-manager-open.html>

<http://support.microsoft.com/kb/300549/el>

<http://www.edugeek.net/forums/windows-7/59575-icacls-windows-7-modify-permissions-everyone-user-file-folder.html>