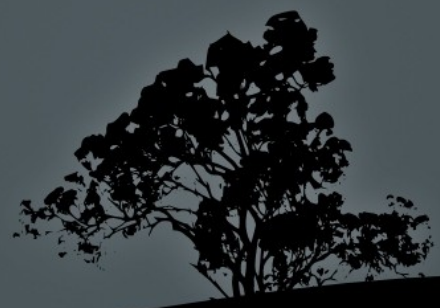
Εξέταση 102 – Μάθημα 7

107.1 Ρύθμιση λογαριασμών χρηστών και ομάδων και σχετικών αρχείων συστήματος



Διαχείριση χρηστών

- Ένα από τα πλέον σημαντικά καθήκοντα ενός διαχειριστή συστημάτων είναι η διαχείριση χρηστών (users)
- Δικαίωμα στην διαχείριση χρηστών έχει ο χρήστης root με ταυτότητα χρήστη (UID) ίσον με 0.
- Κάθε χρήστης έχει ένα όνομα και μια ταυτότητα με την οποία αναγνωρίζεται στο σύστημα
- Οι χρήστες ανήκουν σε μια ή περισσότερες ομάδες (groups) οι οποίες έχουν την δική του ξεχωριστή ταυτότητα ομάδας (GID)

Κατηγορίες χρηστών

- **Υπερχρήστες**: είναι βασικά ο χρήστης **root** με καθολικά δικαιώματα διαχείρισης του συστήματος και UID ίσον με 0
- **Χρήστες διαχείρισης συστήματος**: είναι λογαριασμοί που χρησιμοποιούνται από δαίμονες και υπηρεσίες του συστήματος. Η UID τους κυμαίνεται από 1 μέχρι 500
- **Κανονικοί χρήστες**: είναι λογαριασμοί που δημιουργούνται με σκοπό την χρήση από φυσικά πρόσωπα. Στις πλείστες διανομές ξεκινούν από UID ίσον με 500 αλλά σε κάποιες διανομές μπορεί να ξεκινούν ακόμη και από 1000

Το αρχείο */etc/passwd*

- Οι χρήστες (users) του συστήματος δηλώνονται στο αρχείο **/etc/passwd** το οποίο έχει την πιο κάτω δομή:

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
...
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
sshd:x:113:65534::/var/run/sshd:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
gdm:x:106:114:Gnome Display Manager:/var/lib/gdm:/bin/false
user:x:500:500:User Userides,23,99773377,Boss:/home/user:/bin/bash
george:x:501:501:George Papas,,,:/home/george:/bin/csh

Τα πεδία του αρχείου /etc/passwd

root:x:0:0:root:/root:/bin/bash # λογαριασμός χρήστη root
sshd:x:113:65534::/var/run/sshd:/usr/sbin/nologin # λογαριασμός διαχείρισης συστήματος
user:x:500:500:User Userides,,,:/home/user:/bin/bash # λογαριασμός κανονικού χρήστη

- **Όνομα χρήστη (username)**: ένα μοναδικό όνομα μέχρι 32 χαρακτήρες. Έχει σημασία αν είναι πεζά ή κεφαλαία αλλά γενικά συστήνονται τα πεζά γράμματα του λατινικού αλφάβητου. Επιτρέπονται οι παύλες (-), οι υπογραμμίσεις (_) και οι αριθμοί αλλά το όνομα θα πρέπει να ξεκινά με γράμμα

- **Κωδικός (password)**: εδώ αποθηκεύεται ο κωδικός σε μη αναστρέψιμη κρυπτογραφημένη μορφή (hashed). Στα σύγχρονα συστήματα το πεδίο αυτό έχει αντικατασταθεί με το αρχείο **/etc/shadow** και απλά μπαίνει ένα **x**

- **Ταυτότητα χρήστη (UID)**: είναι μια αριθμητική τιμή που καθορίζει την ταυτότητα του χρήστη. Η τιμή αυτή αποθηκεύεται στα inodes για να καθορίζει τον ιδιοκτήτη του αρχείου

- **Ταυτότητα ομάδας (GID)**: είναι μια αριθμητική τιμή που καθορίζει την ταυτότητα της κύριας ομάδας του χρήστη. Η τιμή αυτή αποθηκεύεται στα inodes για να καθορίζει την ιδιοκτήτρια ομάδα του αρχείου

Τα πεδία του αρχείου /etc/passwd

- **Ονοματεπώνυμο ή Σχόλια (Full name or comments)**: εδώ μπαίνουν κάποια σχόλια για το σκοπό χρήσης του συγκεκριμένου λογαριασμού. Στην περίπτωση κανονικών χρηστών περιέχει το ονοματεπώνυμο και ίσως επιπρόσθετες πληροφορίες όπως αριθμός δωματίου, τηλέφωνο κάποια σχόλια όλα διαχωρισμένα με κόμμα “,”. Μπορεί και να παραληφθεί εντελώς
- **Προσωπικός κατάλογος (Home Directory)**: δηλώνει τον προσωπικό κατάλογο σε κανονικούς χρήστες και τον κατάλογο λειτουργίας σε λογαριασμούς διαχείρισης συστήματος. Στους κανονικούς χρήστες παίρνει την μορφή και ιδιότητες του **/etc/skel** κατά την δημιουργία του
- **Κέλυφος (Shell)**: καθορίζει το αρχικό κέλυφος ενός χρήστη το οποίο ξεκινά με την σύνδεση (login) του χρήστη στο σύστημα. Σε πολλές περιπτώσεις λογαριασμών διαχείρισης παραπέμπει στις εφαρμογές **false** ή **nologin** για να εμποδίζει την λειτουργία κελύφους σε αυτούς. Αυτό γίνεται για λόγους ασφαλείας. Το ίδιο μπορεί να γίνει αν θέλουμε να απενεργοποιήσουμε κάποιο χρήστη

Το αρχείο */etc/shadow*

- Το αρχείο **/etc/passwd** έχει καθολική άδεια ανάγνωσης (644) επειδή χρειάζεται να είναι προσβάσιμο από όλους τους χρήστες. Αυτό όμως έδινε σε κάποιο κακόβουλο χρήστη το κρυπτογραφημένο (hashed) κωδικό που μπορούσε να τον χρησιμοποιήσει με κάποιο πρόγραμμα «σπασίματος» κωδικών για να τον εκμαιεύσει.
- Για να λυθεί αυτό το πρόβλημα δημιουργήθηκε το υποσύστημα Shadow Password για να κρατούνται οι κρυπτογραφημένοι κωδικοί μαζί με άλλες πληροφορίες κάτω από το αρχείο **/etc/shadow** το οποίο δεν είναι καθολικά αναγνώσιμο. Οι άδειες πρόσβασης του είναι 400 σε RedHat και 640 σε Debian

Τα πεδία του αρχείου /etc/shadow

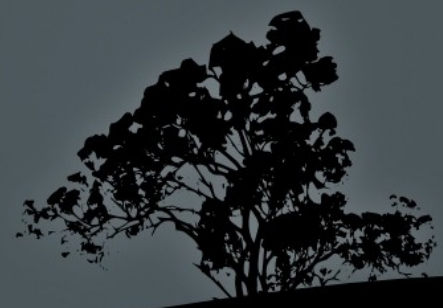
root:6CGpBa7JP$ROaMeOyDIQSKNNrZUFnjhAXgfYwpMqJf7G/tt/:15316:0:99999:7:::
sshd:*:15214:0:99999:7:::
user:$6$04ZF/yDL$Yc2crio0H.A.KlkvhmfnUF/eB0ibQac5mjkXjrjO5/k/:15221:0:99999:7:::

- **Όνομα χρήστη (username)**: το όνομα που υπάρχει σε αυτό το πεδίο πρέπει να ταυτίζεται με το αντίστοιχο όνομα χρήστη στο αρχείο **/etc/passwd**
- **Κωδικός (password)**: εδώ αποθηκεύεται ο κωδικός σε μη αναστρέψιμη κρυπτογραφημένη μορφή (hashed). Η κρυπτογράφηση που γινόταν παλιά ήταν με βάση το **crypt** (**des**) αλλά στα σύγχρονα συστήματα χρησιμοποιείται **md5** ή **sha**. Το πεδίο αυτό μπορεί να έχει την τιμή "*" όταν δεν υπάρχει κωδικός. Σε αυτή την περίπτωση ο χρήστης δεν μπορεί να κάνει login. Μπορεί όμως να χρησιμοποιηθεί σαν χρήστης κάποιας διεργασίας και αυτό συμβαίνει στην περίπτωση υπηρεσιών του συστημάτων (δαιμόνων)
- **Άλλα πεδία**: χρησιμοποιούνται από τις εντολές **passwd**, **usermod** και **chage** για να καθορίζουν παραμέτρους όπως την τελευταία αλλαγή του κωδικού, μέρες πριν από τις οποίες επιτρέπεται η αλλαγή του κωδικού, ημερομηνία λήξης κτλ

Το αρχείο */etc/group*

- Οι ομάδες του συστήματος δηλώνονται στο αρχείο **/etc/group**. Ένας χρήστης μπορεί να ανήκει σε περισσότερες ομάδες αλλά έχει μια κύρια ομάδα που δηλώνεται στο **/etc/passwd**. Παράδειγμα:

root:x:0:
daemon:x:1:
bin:x:2:
adm:x:4:theodotos.andreou,yioryos
tty:x:5:
admin:x:121:theodotos.andreou
theodotos.andreou:x:1000:
sambashare:x:122:theodotos.andreou
winbindd_priv:x:123:
mysql:x:124:
yioryos:x:1001:



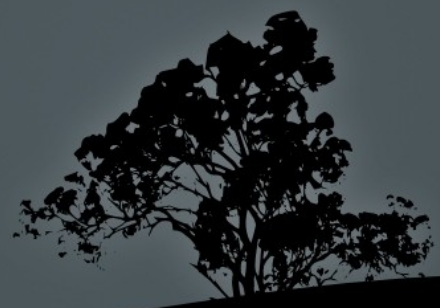
Τα πεδία του αρχείου /etc/group

root:x:0: # ομάδα χρήστη root
nogroup:x:65534: # ομάδα διαχείρισης συστήματος
plugdev:x:46:user,george # ομάδα διαχείρισης συστήματος
user:x:500:: # προσωπική ομάδα κανονικού χρήστη

- **Όνομα ομάδας (group name)**: ένα μοναδικό όνομα ομάδας. Οι ομάδες καθορίζουν την πρόσβαση σε διάφορες υπηρεσίες και πόρους του συστήματος. Υπάρχουν και προσωπικές ομάδες που δημιουργούνται με την δημιουργία κάποιου χρήστη.
- **Κωδικός (password)**: εδώ αποθηκεύεται ο κωδικός της ομάδας σε μη αναστρέψιμη κρυπτογραφημένη μορφή (hashed). Ο κωδικός των ομάδων μπορεί να χρησιμοποιηθεί για να δώσει πρόσβαση σε κάποιο μη μέλος της ομάδας ή από συγκεκριμένες εφαρμογές. Στα σύγχρονα συστήματα το πεδίο αυτό έχει αντικατασταθεί με το αρχείο **/etc/gshadow** και απλά μπαίνει ένα **x**
- **Ταυτότητα ομάδας (GID)**: είναι μια αριθμητική τιμή που καθορίζει την ταυτότητα της κύριας ομάδας του χρήστη. Η τιμή αυτή αποθηκεύεται στα inodes για να καθορίζει την ιδιοκτήτρια ομάδα του αρχείου
- **Μέλη ομάδας (group members)**: είναι μια λίστα διαχωρισμένη με κόμματα που δηλώνει τους χρήστες που είναι μέλη σε αυτή την ομάδα

Το αρχείο */etc/gshadow*

- Το αρχείο **/etc/group** έχει καθολική άδεια ανάγνωσης (644) επειδή χρειάζεται να είναι προσβάσιμο από όλους τους χρήστες. Αυτό δεν είναι επιθυμητό για τους ίδιους λόγους με το **/etc/passwd**
- Για να λυθεί αυτό το πρόβλημα δημιουργήθηκε το υποσύστημα Shadow Group για να κρατούνται οι κρυπτογραφημένοι κωδικοί μαζί με άλλες πληροφορίες κάτω από το αρχείο **/etc/gshadow** το οποίο δεν είναι καθολικά αναγνώσιμο. Οι άδειες πρόσβασης του είναι 400 σε RedHat και 640 σε Debian



Τα πεδία του αρχείου /etc/gshadow

root:*::
sshd:!::
sales:$6$04ZF/yDL$Yc2crio0H.A.KlkvhmfnUF/eB0ibQac5mjkXjrjO5/k/::

- **Όνομα ομάδας (group name)**: το όνομα που υπάρχει σε αυτό το πεδίο πρέπει να ταυτίζεται με το αντίστοιχο όνομα ομάδας στο αρχείο **/etc/group**
- **Κωδικός (password)**: εδώ αποθηκεύεται ο κωδικός σε μη αναστρέψιμη κρυπτογραφημένη μορφή (hashed). Η κρυπτογράφηση που γινόταν παλιά ήταν με βαση το **crypt** (**des**) αλλά στα σύγχρονα συστήματα χρησιμοποιείται **md5** ή **sha**. Το πεδίο αυτό μπορεί να έχει την τιμή "*****" ή "**!**" όταν δεν υπάρχει κωδικός. Οι κωδικοί στις ομάδες σπάνια χρησιμοποιούνται και έχουν διαφορετική χρήση από τους κωδικούς των χρηστών
- **Άλλα πεδία**: χρησιμοποιούνται για να δηλώνουν τους διαχειριστές και τα μέλη της ομάδας

Προσθήκη χρηστών με *useradd*

- Η εντολή **useradd** είναι η βασική εντολή σε γραμμή εντολών για προσθήκη χρηστών
- **# useradd user** # προσθήκη χρήστη **user** στο σύστημα. Θα πρέπει να χρησιμοποιήσουμε την εντολή **passwd** για καθορισμό του κωδικού προσβασης
- **# useradd -m user** # προσθήκη χρήστη **user** στο σύστημα με ταυτόχρονη δημιουργία προσωπικού καταλόγου χρησιμοποιώντας σαν βάση τον κατάλογο **/etc/skel**
- **# useradd -m -c "User Userides" -s /bin/bash user** # προσθήκη χρήστη **user** στο σύστημα με ταυτόχρονη δημιουργία προσωπικού καταλόγου, καθορισμού του πεδίου σχολίων και καθορισμό του προκαθορισμένου κελύφους του χρήστη
- **# useradd -D** # προβολή προκαθορισμένων ρυθμίσεων. Αυτές καθορίζονται στο αρχείο ρυθμίσεων **/etc/login.defs**

Προσθήκη χρηστών με *useradd*

Επιλογές:

- **-m** # δημιουργία προσωπικού καταλόγου κάτω από **/home** με το ίδιο όνομα όπως και ο χρήστης
- **-d** # καθορισμός ονόματος προσωπικού καταλόγου διαφορετικού από το όνομα χρήστη. Δεν προϋποθέτει και ταυτόχρονη δημιουργία του καταλόγου εκτός και αν συνδυαστεί με το **-m**
- **-c** # προσθήκη σχολίων. Στη περίπτωση ενός συνηθισμένου χρήστη μπορεί να είναι το ονοματεπώνυμο του
- **-e** # ημερομηνία λήξης του λογαριασμού στη μορφή YYYY-MM-DD
- **-f** # αριθμός ημερών μέχρι την πλήρη απενεργοποίηση του λογαριασμού μετά την ημερομηνία λήξης
- **-r** # δημιουργία χρήστη συστήματος με UID μικρότερο από 500
- **-D** # προβολή προκαθορισμένων ρυθμίσεων από **/etc/login/defs**

Καθορισμός κωδικού πρόσβασης με *passwd*

- Η εντολή **passwd** καθορίζει τον κωδικό πρόσβασης του χρήστη. Αν μετά την δημιουργία του λογαριασμού χρήστη δεν καθοριστεί κωδικός ο λογαριασμός μένει ανενεργός.
- Συστήνεται να χρησιμοποιούνται πολύπλοκοι κωδικοί με 8 ή περισσότερους χαρακτήρες, κεφαλαία και πεζά, αριθμούς και σημεία στίξης
- **# passwd user** # αλλαγή ή προσθήκη κωδικού για χρήστη **user** από χρήστη **root**
- **$ passwd** # αλλαγή κωδικού του τρέχοντος χρήστη (όπως καθορίζεται από **$USER**). Οι απλοί χρήστες μπορούν να αλλάξουν μόνο τον δικό τους κωδικό

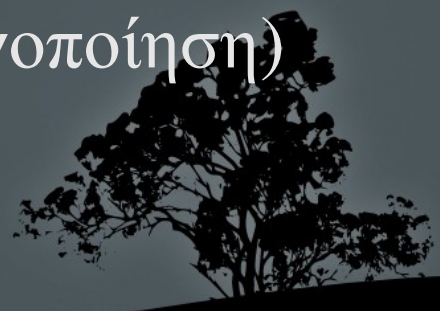
Καθορισμός κωδικού πρόσβασης με *passwd*

Επιλογές:

- **-d** # διαγραφή κωδικού χρήστη (απενεργοποίηση λογαριασμού)
- **-e** # υποχρεωτική λήξη του λογαριασμού και προτροπή του χρήστη για αλλαγή κωδικού στην επόμενη σύνδεση
- **-i DAYS** # απενεργοποίηση λογαριασμού μετά την λήξη, αφού περάσουν οι μέρες που καθορίζονται στο DAYS χωρίς αλλαγή κωδικού
- **-n DAYS** # ελάχιστος αριθμός ημερών όπου απαγορεύεται η αλλαγή κωδικού
- **-m DAYS** # **μέγιστος** αριθμός ημερών όπου είναι υποχρεωτική η αλλαγή κωδικού
- **-l** # κλείδωμα λογαριασμού με την προσθήκη ! Μπροστά από το κρυπτογραφημένο κωδικό
- **-u** # ξεκλείδωμα λογαριασμού
- **-w DAYS** # καθορισμός προειδοποίησης λήξης κωδικού κάποιες μέρες πριν από την λήξη
- **-x DAYS** # καθορισμός μέγιστου αριθμού ημερών όπου ένας κωδικός πρέπει να λήξει

Τροποποίηση χρηστών με *usermod*

- Η εντολή **usermod** χρησιμοποιείται για την αλλαγή υφιστάμενων χρηστών
- **# usermod -g users user** # αλλαγή κύριας ομάδας του χρήστη **user** σε **users**
- **# usermod -a -G admin user** # προσθήκη του χρήστη **user** στην συμπληρωματική ομάδα **admin**
- **# usermod -L user** # κλείδωμα (απενεργοποίηση) λογαριασμού
- **# usermod -U user** # ξεκλείδωμα (ενεργοποίηση) λογαριασμού



Τροποποίηση χρηστών με *usermod*

Επιλογές:

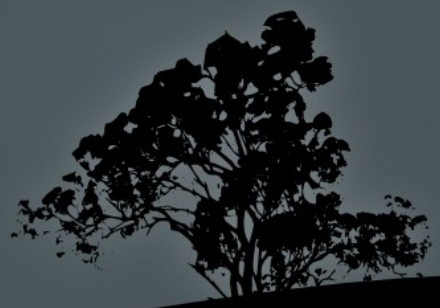
- **-a** # προσθήκη χρήστη σε συμπληρωματικές ομάδες. Συνδυάζεται πάντα με το **-G**.
- **-d** # αλλαγή ονόματος προσωπικού καταλόγου. Συνδυάζεται με **-m** για την μετακίνηση του υφιστάμενου προσωπικού καταλόγου
- **-c** # Αλλαγή σχολίων.
- **-e** # ημερομηνία λήξης του λογαριασμού στη μορφή YYYY-MM-DD
- **-f** # αριθμός ημερών μέχρι την πλήρη απενεργοποίηση του λογαριασμού μετά την ημερομηνία λήξης
- **-g** # αλλαγή κύριας ομάδας χρήστη
- **-G group1,gpoup2,group3** # επιλογή συμπληρωματικών ομάδων. Συνδυάζεται με **-a** αν δεν θέλουμε να διαγραφούν οι άλλες ομάδες
- **-l** # αλλαγή ονόματος χρήστη (username)
- **-L, -U** # κλείδωμα, ξεκλείδωμα λογαριασμού
- **-s** # αλλαγή κελύφους

Διαγραφή χρηστών με *userdel*

- Η εντολή **userdel** χρησιμοποιείται για την διαγραφή χρηστών από το σύστημα
- **# userdel user** # διαγραφή χρήστη από το σύστημα αλλά διατήρηση του προσωπικού του καταλόγου
- **# userdel -r user** # διαγραφή χρήστη από το σύστημα και διαγραφή του προσωπικού του καταλόγου
- **# userdel -f user** # διαγραφή χρήστη από το σύστημα ακόμη και αν είναι ήδη συνδεδεμένος!

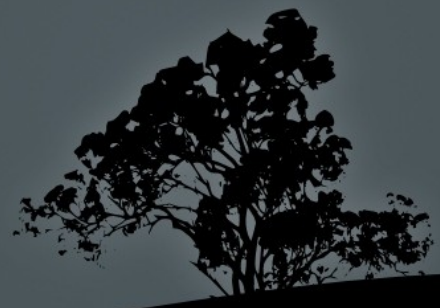
Δημιουργία ομάδων με *groupadd*

- Η εντολή **groupadd** χρησιμοποιείται για την δημιουργία ομάδων στο σύστημα
- **# groupadd sales** # δημιουργία ομάδας για χρήστες
- **# groupadd -r httpd** # δημιουργία ομάδας συστήματος με GID μικρότερο από 500
- **# groupadd -g 45 httpd** # δημιουργία ομάδας συστήματος με GID ίσον με 45



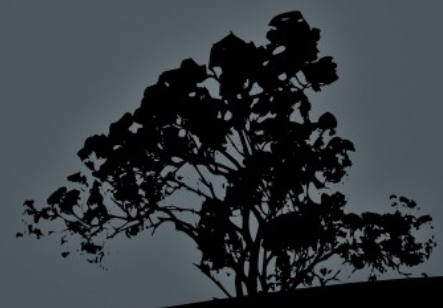
Καθορισμός κωδικού πρόσβασης ομάδας με *gpasswd*

- **Η εντολή gpasswd** χρησιμοποιείται για το καθορισμό κωδικού για την ομάδα αλλά και για άλλες αλλαγές στην ομάδα (man gpasswd)
- Ο κωδικός αυτός χρησιμοποιείται από τους χρήστες που δεν ανήκουν στην ομάδα για πρόσβαση σε αρχεία ή εντολές της ομάδας
- **# gpasswd httpd** # καθορισμός κωδικού για ομάδα



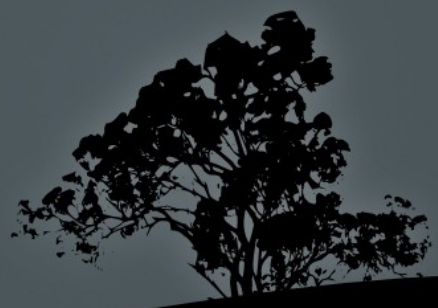
Τροποποίηση ομάδας με *groupmod*

- Η εντολή **groupmod** χρησιμοποιείται για την τροποποίηση ομάδων στο σύστημα.
- **# groupmod -g 50 httpd** # αλλαγή GID σε 50
- **# groupmod -n apache httpd** # αλλαγή ονόματος ομάδας από **httpd** σε **apache**



Διαγραφή ομάδας με groupdel

- Η εντολή **groupmod** χρησιμοποιείται για την τροποποίηση μιας ομάδας από το σύστημα.
- **# groupdel httpd** # διαγραφή ομάδας **httpd**



Εργαστήριο 7

Ξεκινήστε και τις δύο εικονικές μηχανές και συνδεθείτε σαν ”root”

- **# vi /etc/passwd**
- **# ls -la /etc/passwd**
- **# vi /etc/shadow**
- **# ls -la /etc/shadow**
- **# ps aux | less**
- **# ls -la /home**
- **# vi /etc/group**
- **# ls /etc/group**
- **# vi /etc/gshadow**
- **# ls /etc/gshadow**
- **# useradd -c "Test User" -m -s \ /bin/bash tuser** # σε Debian
- **# useradd -c "Test User" -s /bin/bash \ tuser** # σε RedHat
- **# grep tuser /etc/passwd \ /etc/shadow /etc/group**
- **# ls -la /home**
- Ανοίξτε άλλο τερματικό και δοκιμάστε να συνδεθείτε σαν tuser
- **# passwd tuser** # χρησιμοποιείστε την λέξη **secret**
- **# grep tuser /etc/shadow**

Εργαστήριο 7

- Ανοίξτε άλλο τερματικό και δοκιμάστε να συνδεθείτε σαν tuser
- **# usermod -a -G adm,lp,games tuser**
- **# grep tuser /etc/group**
- **# usermod -L tuser**
- **# grep tuser /etc/shadow**
- **# usermod -L tuser**
- **# grep tuser /etc/shadow**
- **# usermod -s /bin/sh tuser**
- **# grep tuser /etc/passwd**
- **# userdel user**
- **# grep tuser /etc/passwd \ /etc/shadow /etc/group**
- **# ls -la /home**
- **# useradd -c "Test User" -m -s \ /bin/bash tuser** # σε Debian
- **# useradd -c "Test User" -s /bin/bash \ tuser** # σε RedHat
- **# groupadd sales**
- **# grep sales /etc/group**
- **# usermod -a -G sales tuser**
- **# grep sales /etc/group**
- **# groupadd -r httpd**
- **# grep httpd /etc/group**
- **# gpasswd httpd** # βάλτε τον κωδικό "fred"

Εργαστήριο 7

- **# mkdir /var/lib/httpd**
- **# echo "Some info" > /var/lib/httpd/index**
- **# chgrp -R httpd /var/lib/httpd**
- **# chmod -R o-rx /var/lib/httpd**
- **# ls -ld /var/lib/httpd**
- **# ls -l /var/lib/httpd**
- **# id tuser**
- **# su – tuser**
- **$ cat /var/lib/httpd/index**
- **$ sg httpd -c "cat /var/lib/httpd/index"**