www.uom.gr
ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΟΙΚΟΝΟΜΙΚΩΝ ΚΑΙ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
τμήμα Εφαρμοσμένης Πληροφορικής

Προγραμματισμός Διαχείρισης Συστημάτων ΙΙ

Μάθημα 3ο

Λογαριασμοί χρηστών

Μιχαηλίδης Παναγιώτης

Περιεχόμενα

- Λογαριασμοί χρηστών
  - Το αρχείο /etc/passwd
  - Το αρχείο /etc/shadow
  - Το αρχείο /etc/group
  - Προσθήκη χρηστών
  - Διαγραφή χρηστών
  - Απενεργοποίηση σύνδεσης
  - Εργαλεία διαχείρισης λογαριασμών

Το αρχείο /etc/passwd

- /etc/passwd αναφέρει όλους τους αναγνωρισμένους χρήστες και περιέχει:
  - Όνομα χρήστη (login name)
  - Κρυπτογραφημένος κωδικός πρόσβασης (εκτός αν χρησιμοποιείται /etc/shadow)
  - Αριθμός UID
  - Εξ ορισμού αριθμός GID
  - Πλήρες όνομα, γραφείο, τηλέφωνο οικίας (προαιρετικό)
  - Προσωπικός κατάλογος
  - Φλοιός σύνδεσης
- Παραδείγματα
  - root:lga4FjuGpZ2so:0:0:The System,,x6096,:/:/bin/csh
  - jl:x:100:0:Jim Lane,ECT83,,:/staff/fl:/bin/sh

Όνομα σύνδεσης

- Σύνταξη
  - Τα ονόματα χρηστών πρέπει να είναι μοναδικά
  - <= 32 χαρ. (παλιότερα συστήματα περιοριζόνταν σε 8 χαρ.)
  - Οτιδήποτε χαρακτήρες εκτός της νέας γραμμής και διαχωριστικά
- Συστάσεις
  - Να χρησιμοποιούμε μικρά γράμματα
  - Να επιλέγουμε εύκολο όνομα για να θυμόμαστε
  - Να απογεύγουμε συντομογραφικά ονόματα

Κρυπτογραφημένους κωδικούς

- Οι περισσότεροι κωδικοί είναι στο /etc/shadow και όχι στο /etc/passwd
- Οι κωδικοί πρόσβασης αποθηκεύονται κρυπτογραφημένοι
  - Δεν μπορούμε να αλλάξουμε χειροκίνητα
  - Μπορούν να αντιγραφούν από άλλο λογαριασμό
  - Βάζουμε κωδικό χρησιμοποιώντας την passwd (ή yppasswd για NIS)

Κρυπτογραφημένους κωδικούς

- Δεν πρέπει ποτέ να αφήνουμε κενό στους κωδικούς
  - Στην θέση του βάζουμε ένα αστερίσκο (*) (x για χρήση shadow)
  - Διαφορετικά δεν χρειάζεται κωδικό
- Κωδικοί MD5 (πρότυπο στο RH) μπορεί έχουν οτιδήποτε μήκος
  - Άλλα συστήματα χρησιμοποιούν μόνο τους 8 πρώτους χαρακτήρες

Αριθμός UID

- Στο Linux, οι αριθμοί UID είναι 32-bits μη προσημασμένοι ακέραιοι (4B!)
  - Παλιότερα συστήματα επιτρεπόνταν μόνο μέχρι 32,767
- Ο root έχει UID 0
- Οι συνδέσεις συστημάτων τυπικά έχουν χαμηλά UIDs
  - Τοποθετούμε πραγματικούς χρήστες >= 100
- Αποφεύγουμε την ανακύκλωση των UIDs
  - Παλιά αρχεία, εφεδρικά αντίγραφα αναγνωρίζονται από UID
- Διατηρούμε τους αριθμούς UID μοναδικά μέσω οργανισμού
  - Χρήσιμο για NFS

Υπόλοιπα πεδία

- Εξ ορισμού αριθμός GID
  - Όπως στους UIDs, είναι 32 bits μη προσημασμένοι ακέραιοι
  - GID – είναι για την ομάδα "root"
- Πεδία GECOS (προαιρετικά) [**chfn**]
  - General Electric Comprehensive OS
  - Πλήρες όνομα, γραφείο, τηλέφωνο οικίας
- Προσωπικός κατάλογος
  - Είναι ο κατάλογος που ξεκινάει όταν ο χρήστης συνδέεται
- Φλοιός σύνδεσης [**chsh**]
  - Όπως **sh/bash, csh/tcsh, ksh**, κλπ

Το αρχείο /etc/shadow

- Διαβάζεται μόνο από τον υπερχρήστη
- Εμπλουτισμένες πληροφορίες λογαριασμών
- Συστήνεται να χρησιμοποιείται
- Για να τροποποιήσουμε τα περιεχόμενα χρησιμοποιούμε την **`usermod`**

- Περιέχει:
  - Όνομα σύνδεσης
  - Κρυπτογραφημένος κωδικός
  - Ημερομηνία αλλαγής κωδικού
  - Ελάχιστος αριθμός ημερών ανάμεσα στις αλλαγές κωδικού
  - Μέγιστος αριθμός ημερών ανάμεσα στις αλλαγές κωδικού
  - Αριθμός ημερών για προειδοποίηση
  - Αριθμός ημερών μετά την λήξη για απενεργοποίηση λογαριασμού
  - Ημερομηνίας λήξης λογ/σμού

Το αρχείο /etc/group

- Περιέχει ονόματα ομάδων και αναφέρει κάθε μέλος
- Παράδειγμα
  - wheel:*:10:root,evi,garth,trent,brian
  - Όνομα ομάδας:κρυπτογρ. κωδικός:GID:Λίστα μελών, που διαχωρίζονται με κόμμα (όχι κενά)
- Συστήνεται να θέτουμε στις ομάδες ανά χρήστη
  - Καλύτερη εξ ορισμού ασφάλεια

Προσθήκη χρηστών

- Για μικρές εγκαταστάσεις, η προσθήκη χρηστών είναι απλή
  - Έχει υπογράψει ο χρήστης και αποδέχεται την συμφωνία
  - Δημιουργούμε λογαριασμό χρήστη με **useradd**
  - Θέτουμε κωδικό πρόσβασης με **passwd**
  - Αλλάζουμε τις εξ΄ορισμού ρυθμίσεις με **usermod**

Βήματα για την προσθήκη χρήστη (1)

- Επεξεργαζόμαστε τα αρχεία /etc/passwd και /etc/shadow για να ορίζουμε λογαριασμό
  - Χρησιμοποιούμε την **vipw** για να κλειδώσουμε και να επεξεργαστούμε με την EDITOR
- Θέτουμε ένα αρχικό κωδικό πρόσβασης
  - passwd user
- Δημιουργούμε, **chown** και **chmod** το προσωπικό κατάλογο του χρήστη
  - **mkdir /home/staff/tyler**
  - **chown tyler.staff /home/staff/tyler**
  - **chmod 700 /home/staff/tyler**

Βήματα για την προσθήκη χρήστη (2)

- Αντιγράφουμε τα εξ ορισμού αρχεία εκκίνησης στο προσωπικό κατάλογο του χρήστη
  - bash
    - .bashrc, .bash_profile
  - csh/tcsh
    - .login, .cshrc, .logout
  - X-Windows
    - .Xdefaults, .Xclients, .xsession
- Χρειάζεται να δημιουργήσουμε και να αποθηκεύσουμε τα εξ ορισμού αρχεία.

Βήματα για την προσθήκη χρήστη (3)

- Αντιγράφουμε αρχεία στο καινούργιο κατάλογο
  - `cp /etc/skel/.[a-zA-Z]* ~tyler`
  - `chmod 644 ~tyler/.[a-zA-Z]*`
  - `chown tyler ~tyler/.[a-zA-Z]*`
  - `chgrp staff ~tyler/.[a-zA-Z]*`
- Δεν μπορούμε να χρησιμοποιήσουμε την `chown tyler ~tyler/.*`
- Θέτουμε το αρχικό mail
  - Ίσως επεξεργαστούμε το `/etc/mail/aliases`

Βήματα για την προσθήκη χρήστη (4)

- Επεξεργαζόμαστε το αρχείο **/etc/group**
  - Προσθέτουμε τις σχετικές ομάδες
- Θέτουμε χώρο δίσκου με **edquota**
- Επιβεβαιώνουμε το καινούργιο login
  - Συνδεόμαστε σαν καινούργιος χρήστης
  - Εκτελούμε τις εντολές **pwd** και **ls -al**
- Δίνουμε στον καινούργιο χρήστη το όνομα λογαριασμού και το αρχικό κωδικό πρόσβασης
- Καταγράφουμε την κατάσταση του χρήστη και πληροφορίες επαφής

Διαγραφή χρηστών

- Γενικά χρησιμοποιούμε την **`userdel`**
  - Θέτουμε το χώρο δίσκου σε μηδέν
  - Διαγράφουμε το χρήστη από τις τοπικές βάσεις δεδομένων ή τηλεφωνικές λίστες
  - Διαγράφουμε το χρήστη από το αρχείο aliases
  - Διαγράφουμε το crontab και οτιδήποτε εκρεμμότητες
  - Τερματίζουμε οτιδήποτε εκτελέσιμες διεργασίες
  - Διαγράφουμε προσωρινά αρχεία από /var/tmp ή /tmp
  - Διαγράφουμε από τα αρχεία passwd, shadow και group
  - Διαγράφουμε το προσωπικό κατάλογο (πρώτα εφεδρικά αντίγραφα) και mail spool

Απενεργοποίηση σύνδεσης

- Μερικές φορές χρειαζόμαστε να απενεργοποιήσουμε προσωρινά την σύνδεση
- Δεν μπορούμε να βάλουμε ένα αστερίσκο μπροστά στο κρυπτογραφημένο κωδικό πρόσβασης
  - Ίσως ακόμη είναι ικανό να συνδεθεί μέσω δικτύου χωρίς κωδικό
- Τρέχουσα πρακτική
  - Αντικαθιστούμε το φλοιό με ένα πρόγραμμα που εμφανίζει ένα μήνυμα εξηγώντας την κατάσταση

Εργαλεία διαχείρισης λογαριασμών

- Βασικά εργαλεία
  - **useradd** - προσθέτει στα αρχεία passwd και shadow
  - **usermod** - αλλάζει το υπάρχων κωδικό πρόσβασης
  - **userdel** - διαγράφει χρήστη και προσωπικό κατάλογο
  - **groupadd, groupmod, groupdel** λειτουργούν πάνω στο /etc/group
- Συνήθως γράφουμε προσαρμομένα σενάρια adduser και rmuser