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

Προγραμματισμός Διαχείρισης Συστημάτων ΙΙ

Μάθημα 2ο

Δυνάμεις Υπερχρήστη

Μιχαηλίδης Παναγιώτης

Περιεχόμενα

- Δυνάμεις υπερχρήστη
  - Ιδιοκτησία αρχείων και διεργασιών
  - Υπερχρήστης
  - Επιλογή κωδικού πρόσβασης υπερχρήστη
  - Αλλαγή σε υπερχρήστη
  - Ψευδοχρήστες

Ιδιοκτησία αρχείων και διεργασιών

- Κάθε αρχείο έχει έναν ιδιοκτήτη και έναν "ιδιοκτήτη ομάδας"
- Ο ιδιοκτήτης μπορεί να τροποποιήσει τις άδειες του αρχείου
  - Μπορεί να κάνει αλλαγή στο αρχείο ώστε κανένας άλλος να μην έχει πρόσβαση στο αρχείο
- Η ιδιοκτησία ομάδας μοιράζεται μεταξύ των μελών της ομάδας.
  - Οι ομάδες ορίζονται στο /etc/group

```
$ ls -l /home/panosm/bio.txt
-rw-r----- 1 panosm gstudent 1560 Oct 7 15:15
  /home/brian/bio.txt
```

- Ο ιδιοκτήτης του αρχείου είναι ο χρήστης panosm και η ομάδα gstudent.

Ιδιοκτήτες αρχείου χρήστη και ομάδας

- Το Linux κρατάει την ιδιοκτησία χρήστη και ομάδας με αριθμούς ταυτότητας (UID, GID)
  - Χρησιμοποιεί τα /etc/group και /etc/passwd για να πάρει τα ονόματα κειμένου που απεικονίζουν στους αριθμούς ταυτότητας (ids)
- Τα εκτελέσιμα setuid ή setgid μπορούν να αλλάξουν τους αριθμούς ταυτότητας χρήστη ή ομάδας για την διεργασία που δημιουργήθηκε από το εκτελέσιμο
- Χρησιμοποιούμε την chmod για να αλλάξουμε τις άδειες

Υπερχρήστης

- Ο λογαριασμός root έχει UID 0
  - Μπορούμε να αλλάξουμε το όνομα και να δημιουργήσουμε άλλους χρήστες με το ίδιο UID αλλά δεν προτείνονται
- Επιτρέπεται στον υπερχρήστη (οποιαδήποτε διεργασία με UID να είναι 0) να εκτελεί οποιαδήποτε λειτουργία σε οποιοδήποτε αρχείο ή διεργασία
- Οι υπόλοιποι χρήστες είναι κανονικοί

Περιορισμένες λειτουργίες

- Τα δικαιώματα του υπερχρήστη απαιτούνται για:
  - Για αλλαγή του καταλόγου root μιας διεργασίας με την `chroot`
  - Για δημιουργία αρχείων συσκευών
  - Για ρύθμιση της ώρας συστήματος
  - Για προτεραιότητες διεργασιών
  - Για ρύθμιση του ονόματος υπολογιστή του συστήματος
  - Για παραμετροποίηση των διεπαφών δικτύου
  - Για άνοιγμα θυρών δικτύου ή υπηρεσιών (<=1024)
  - Για τερματισμός συστήματος
  - Για αλλαγή UID και GID της διεργασίας

Επιλογή κωδικού πρόσβασης root

- Οποιοδήποτε κωδικός πρόσβασης? Όχι αν θέλουμε να είναι δύσκολος για να υποκλαπεί
- Πρέπει να
  - Είναι τουλάχιστον 8 χαρακτήρες
  - Μην μαντεύεται εύκολα ή να εντοπίζεται κατά λάθος ή με δοκιμή
  - Το θυμόμαστε (ώστε να μην χρειάζεται να το σημειώσουμε στο χαρτί)
  - Είναι συνδυασμός τυχαίων γραμμάτων, αριθμών και σημείων στίξης

Αλλαγή κωδικού πρόσβασης root

- Πρέπει να εκτελείται
  - Τουλάχιστον κάθε τρεις μήνες
  - Κάθε φορά που κάποιος γνωρίζει τον κωδικό πρόσβασης και αποχωρεί από την δουλειά

Αλλαγή σε υπερχρήστη

- Μπορούμε να συνδεθούμε σαν λογαριασμό root
  - Καμία καταγραφή για τις λειτουργίες που εκτελέστηκαν
    - Συχνά χρειαζόμαστε μια καταγραφή!
      - Όταν ο υπερχρήστης ήταν ένας συνάδελφος που δεν είναι παρών
      - Όταν δεν θυμόμαστε τι ακριβώς κάναμε
      - Όταν η πρόσβαση ήταν μη πιστοποιημένη και θέλουμε να γνωρίζουμε τι έκανε
  - Καμιά καταγραφή για το ποιος ήταν υπερχρήστης
- Τυπικά απενεργοποιούμε τα logins του root εκτός στην κονσόλα

Root

- Υπευθυνότητες!
  - Δεν δίνουμε το κωδικό πρόσβασης του root
  - Δεν δημιουργούμε καινούργιους λογαριασμούς με UID 0
  - Χρησιμοποιούμε το λογαριασμό root μόνο για εργασίες διαχείρισης
  - Αλλάζουμε συχνά το κωδικό πρόσβασης root
  - Δεν αφήνουμε το φλοιό root ανοιχτό
  - Να είμαστε πολύ προσεκτικοί!

su

- su: αντικαθιστά την ταυτότητα χρήστη (εναλλαγή χρηστών)
  - Χωρίς ορίσματα, η su ζητάει το κωδικό πρόσβασης root και έπειτα ξεκινά ο φλοιός root
  - Καταγραφή ποιος χρησιμοποίησε το root και πότε
  - Μπορεί επίσης su username
    - Αν γνωρίζουμε το κωδικό του username ή αν είμαστε ήδη root
  - Χρησιμοποιούμε "su -" για να εκτελέσουμε το φλοιό του νέου χρήστη
    - Διαφορετικά δεν θα εγκατασταθεί το καινούργιο PATH
  - Καλή ιδέα να χρησιμοποιούμε το απόλυτο μονοπάτι για την su (Γιατί;)
    - Linux: /bin/su

sudo

- su: περιορισμένη su
  - Όταν θέλουμε να δώσουμε περιορισμένα δικαιώματα root
  - sudo <πρόγραμμα που θα εκτελεστεί>
    - Ελέγχει το /etc/sudoers για πιστοποίηση
    - Ζητάει το κωδικό πρόσβασης του χρήστη
    - Καταγράφει την εντολή που εκτελείται, το άτομο, το χρόνο και το κατάλογο
    - Εκτελεί την εντολή
    - Μπορούν να εκτελεστούν επιπλέον εντολές sudo χωρίς κωδικό για άλλα πέντε λεπτά
    - Παράδειγμα:
      - sudo /bin/cat /etc/sudoers

Παράδειγμα αρχείου sudoers

```
# Define aliases for machines in CS & Physics departments
Host_Alias CS = tigger, anchor, piper, moet, sigi
Host_Alias PHYSICS = eprince, pprince, icarus

# Define collections of commands
Cmnd_Alias DUMP = /sbin/dump, /sbin/restore
Cmnd_Alias PRINTING = /usr/sbin/lpc, /usr/bin/lprm
Cmnd_Alias SHELLS = /bin/sh, /bin/csh/, /bin/bash, /bin/ash

#Permissions
mark, ed PHYSICS = ALL
herb CS = /usr/local/bin/tcpdump: PHYSICS = (operator) DUMP
lynda ALL = (ALL) ALL, !SHELLS
%wheel ALL, !Physics = NOPASSWD: PRINTING
```

Συζήτηση sudoers

- Κάθε γραμμή αδειών περιλαμβάνει:
  - Χρήστες στους οποίους αναφέρεται η γραμμή
  - Υπολογιστές στους οποίους αναφέρεται η γραμμή
  - Εντολές που οι χρήστες μπορούν να εκτελέσουν
  - Χρήστες οι οποίοι μπορούν να εκτελέσουν εντολές
- Για να επεξεργαστούμε, χρησιμοποιούμε την visudo
  - Αν είναι σωστά ρυθμισμένη η μεταβλητή περιβάλλοντος EDITOR
  - Κλειδώνει αρχείο
  - Ελέγχει τις αλλαγές που πραγματοποιήσαμε
- Παράδειγμα
  - `$ sudo -u operator /sbin/dump 0u /dev/hda2`

Πλεονεκτήματα sudo

- Λογιστικότητα – εντολές καταγράφονται
- Οι χειριστές μπορούν να κάνουν μικρές εργασίες χωρίς τα δικαιώματα root
- Το πραγματικό κωδικό πρόσβασης root μπορεί να είναι γνωστό σε ένα ή δύο άτομα
- Η sudo είναι ταχύτερη στην χρήση από την su ή απευθείας σύνδεση σαν root
- Διατηρείται μια πλήρη λίστα χρηστών με root
- Δεν υπάρχει ευκαιρία ο φλοιός του root να είναι ανοικτός
- Ένα αρχείο μπορεί να ελέγχει την πρόσβαση για ένα ολόκληρο δίκτυο

Μειονεκτήματα sudo

- Το αρχείο /etc/sudoers είναι παντού!
- Χρήστες με δικαιώματα sudo πρέπει να προστατεύψουν τους λογαριασμούς τους αν ήταν root!
- Η καταγραφή εντολών μπορεί να αποφεύγεται με την εκτέλεση ενός φλοιού ή την εκτέλεση κάποιου προγράμματος που επιτρέπει το τερματισμό του φλοιού

Άλλοι ψευδοχρήστες

- bin
  - Νόμιμος ιδιοκτήτης εντολών συστήματος
- daemon
  - Ιδιοκτήτης μη προνομιούχων αρχείων και διεργασιών
- nobody
  - Λογαριασμός για απομακρυσμένους roots των συστημάτων NFS
    - Οι roots δεν μπορούν να έχουν UID 0!
    - Οι roots χρειάζονται να απεικονιστούν σε κάτι