Λειτουργικά Συστήματα Ι

Ασκήσεις Πράξης

Τμήμα Μηχανικών Πληροφορικής & Υπολογιστών

Σχολή Μηχανικών

© Δ. Καρολίδης - Π. Πρεντάκης

Διαχείριση Χρηστών

Λογαριασμός Χρήστη

- Κατά τη δημιουργία ενός νέου χρήστη, το όνομα του χρήστη σχετίζεται με έναν μοναδικό θετικό αριθμό, ο οποίος αναφέρεται ως αριθμός ταυτότητας χρήστη (user identifier - UID).
- Το UID με τιμή **0** (μηδέν) ανατίθεται πάντα στον χρήστη **root**. Τα UID από **1** έως και **99** ανατίθενται κατά σύμβαση στους χρήστες συστήματος (π.χ. 1 για daemon, 8 για mail). Οι αριθμοί από **100** και πάνω αποτελούν συνήθως τους αριθμούς ταυτότητας των απλών χρηστών.

Λογαριασμός Χρήστη

Τα αναγνωριστικά όλων των χρηστών του συστήματος μαζί με τις σχετικές πληροφορίες είναι αποθηκευμένα στο αρχείο κειμένου **/etc/passwd**, το οποίο είναι αναγνώσιμο από όλους και έχει την παρακάτω μορφή:

$ **cat /etc/passwd**

root:x:0:0:root:/root:/bin/bash

daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

bin:x:2:2:bin:/bin:/usr/sbin/nologin

…

nemo:x:1000:100:Nemo, EDUTel, 5397,:/home/nemo:/bin/bash

alice:x:1001:500:Alice:/home/alice:/bin/bash

bob:x:1002:500:Bob:/home/bob:/bin/bash

/etc/shadow

Το αρχείο /etc/shadow περιέχει τον κρυπτογραφημένο κωδικό πρόσβασης του χρήστη και είναι προσπελάσιμο μόνο από τον υπερχρήστη. Κάθε γραμμή αντιστοιχεί σε έναν χρήστη και έχει την εξής μορφή:

 # cat /etc/shadow | grep bob # execute as root

bob: 6$$c0lFWOQo$HEpc.QbRimDdOU1oiUcel78V1IDIoUE kzSAjflcEknsqui8Ftu8cPFtu8cPLUK8NR0:17608:0:99999:7:::

Το πρώτο πεδίο αποτελείται από το όνομα χρήστη και ακολουθεί ο κρυπτογραφημένος κωδικός πρόσβασης. Οι τρεις πρώτοι χαρακτήρες προσδιορίζουν τον αλγόριθμο κρυπτογράφησης που χρησιμοποιείται. Η τιμή **6** αντιστοιχεί σε κρυπτογράφηση με **SHA 512**.

Δημιουργία νέου χρήστη

Η δημιουργία νέων χρηστών γίνεται από τον υπερχρήστη με την εντολή **useradd**. Η σύνταξη της εντολής έχει ως εξής:

useradd [options] LOGIN

όπου LOGIN είναι το όνομα λογαριασμού του νέου χρήστη.

Οι σημαντικότερες επιλογές της εντολής είναι:

-c, **--comment** COMMENT προσθέτει προσωπικές πληροφορίες για τον χρήστη

-d, **--home-dir** HOME_DIR καθορίζει τον προσωπικό κατάλογο του χρήστη, αντί του προκαθορισμένου

-e, **--expiredate** EXPIRE-DATE ημερομηνία απενεργοποίησης του λογαριασμού σε μορφή YYYY-MM-DD

Δημιουργία νέου χρήστη

-g, **--gid** GROUP η αρχική ομάδα ένταξης του χρήστη

-G, **--groups** GROUP1[,…] λίστα με τις δευτερεύουσες ομάδες στις οποίες θα ενταχθεί ο χρήστης

-k, **--skel** SKEL_DIR τα περιεχόμενα του καταλόγου skeleton (/etc/skel) αντιγράφονται στον προσωπικό κατάλογο του χρήστη

-m, **--create-home** δημιουργία προσωπικού καταλόγου χρήστη, αν δεν υπάρχει

-r, **--system** δημιουργία χρήστη συστήματος

-s, **--shell** SHELL καθορίζει τον φλοιό που θα χρησιμοποιήσει ο χρήστης κατά την είσοδό του στο

Δημιουργία νέου χρήστη

Η εντολή που ακολουθεί θα δημιουργήσει έναν νέο λογαριασμό χρήστη:

 # useradd -m -g 500 -s /bin/bash carol # create new user

 # passwd carol # set password for user carol

Enter new UNIX password:

Retype new UNIX password:

passwd: password updated successfully

Η εντολή useradd αν και δημιούργησε τον νέο λογαριασμό, τον κρατάει κλειδωμένο μέχρι να ορίσουμε έναν κωδικό πρόσβασης με την εντολή **passwd** που ακολουθεί.

Δημιουργία νέου χρήστη

Η επόμενη εντολή δημιουργεί έναν νέο χρήστη του οποίου ο λογαριασμός λήγει στις 31/12/2020 και προσθέτει επίσης προσωπικές πληροφορίες:

 # useradd -e 2020-31-12 -c "Dave Kovic,B54" dave

Η τελευταία γραμμή του αρχείου /etc/passwd έχει τώρα ως εξής:

$ **tail -1 /etc/passwd**

dave:1004:500:Dave Kovic,B54:/home/dave:/bin/bash

Δημιουργία νέου χρήστη

 # adduser --shell /bin/bash --gid 500 eve
Adding user `eve' ...
Adding new user `eve' (500) with group `students' ...
Creating home directory `/home/eve' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for eve
Enter the new value, or press ENTER for the default
Full Name []: Eve Mentes
…
Is the information correct? [Y/n] Y

Διαγραφή χρήστη

Η διαγραφή ενός χρήστη από το σύστημα γίνεται με την εντολή **userdel**, που έχει την παρακάτω σύνταξη:

userdel [options] LOGIN

όπου LOGIN είναι το όνομα του χρήστη που θέλουμε να διαγράψουμε. Εναλλακτικά μπορούμε να χρησιμοποιήσουμε την εντολή **deluser** που είναι πιο φιλική στον χρήστη.

Η σημαντικότερη επιλογή της εντολής userdel είναι:
-r, **--remove** διαγράφει επιπρόσθετα τον προσωπικό κατάλογο του χρήστη καθώς και τα μηνύματα του ηλεκτρονικού ταχυδρομείου. Αρχεία σε άλλα συστήματα αρχείων πρέπει να διαγραφούν χειρωνακτικά.

Διαγραφή χρήστη

Η εντολή που ακολουθεί διαγράφει τον χρήστη *oscar* μαζί με τον προσωπικό του κατάλογο:

 # userdel -r oscar # delete account of user oscar

userdel: oscar mail spool (/var/mail/oscar) not found

Στη συγκεκριμένη περίπτωση η userdel μας ενημερώνει πως δε μπόρεσε να διαγράψει τα ηλεκτρονικά μηνύματα του χρήστη καθώς δε βρέθηκε ο αντίστοιχος κατάλογος.

Στην περίπτωση που ο χρήστης που θέλουμε να διαγράψουμε είναι συνδεδεμένος θα εμφανιστεί το μήνυμα:

 # userdel alice

userdel: user alice is currently used by process 1995

Διαγραφή χρήστη

Η εντολή **deluser** είναι πιο φιλική προς τον χρήστη και παρέχει επιπλέον δυνατότητες. Η κλήση της χωρίς κάποια επιλογή διαγράφει τον χρήστη χωρίς όμως να διαγράψει τον προσωπικό του κατάλογο. Η επιλογή **--remove-home** διαγράφει τον προσωπικό κατάλογο του χρήστη, ενώ η **--remove-all-file** διαγράφει όλα τα αρχεία τα οποία είναι ιδιοκτησίας του.

deluser --remove-all-files juri # delete juri and all files
Looking for files to backup/remove ...
Removing user `juri` ...
Done.

Διαγραφή χρήστη

Επιπρόσθετα οι επιλογές **--backup** και **--backup-to** μας επιτρέπουν να δημιουργήσουμε ένα αντίγραφο ασφαλείας του προσωπικού καταλόγου του χρήστη πριν τον διαγράψουμε. Η εντολή που ακολουθεί δημιουργεί ένα αντίγραφο ασφαλείας των αρχείων του χρήστη στον κατάλογο /root/backup, διαγράφει τον προσωπικό του κατάλογο, και τέλος, διαγράφει και τον χρήστη:

deluser --backup-to /root/backup --remove-home petra
Backing up files to be removed to /root/backup ...
backup_name = /root/backup/petra.tar
Removing user `petra` ...
Done.

Αλλαγή ρυθμίσεων λογαριασμού

Η εντολή usermod επιτρέπει την αλλαγή των ρυθμίσεων ενός λογαριασμού χρήστη. Η σύνταξή της έχει τη μορφή:

usermod [options] LOGIN

όπου LOGIN είναι το όνομα λογαριασμού χρήστη.

Οι σημαντικότερες επιλογές της εντολής είναι:

-a, **--append** προσθέτει τον χρήστη σε επιπλέον ομάδες (χρήση σε συνδυασμό με την επιλογή -G).

-c, **--comment** COMMENT αλλάζει τις προσωπικές πληροφορίες του χρήστη.

Αλλαγή ρυθμίσεων λογαριασμού

-d, **--home** HOME_DIR αλλάζει τον προσωπικό κατάλογο του χρήστη. Με την επιλογή -m τα αρχεία του αρχικού προσωπικού καταλόγου μεταφέρονται στον καινούργιο κατάλογο.

-g, **--gid** GROUP αλλάζει την πρωτεύουσα ομάδα του χρήστη.

-G, **--groups** GROUPS προσθέτει τον χρήστη σε δευτερεύουσες ομάδες. Αν ο χρήστης είναι μέλος κάποιας ομάδας που δεν αναφέρεται στη λίστα, διαγράφεται απ' αυτή εκτός αν συνδυαστεί με την επιλογή -a.

-m, **--move-home** μεταφέρει τον προσωπικό κατάλογο του χρήστη στη νέα θέση (έγκυρη μόνο με την επιλογή -d).

Αλλαγή ρυθμίσεων λογαριασμού

Η εντολή που ακολουθεί προσθέτει τον χρήστη alice στην ομάδα staff:

 # usermod -a -G staff alice # add alice to group staff

 # groups alice

alice: students staff

Η επόμενη εντολή αλλάζει τις πληροφορίες GECKO

 # usermod -c "Alice Cooper,D1948" alice # GECOS

 # cat /etc/passwd | grep alice

alice:x:1001:500:Alice Cooper,D1948:/home/alice:/bin/bash

Διαχείριση ομάδων

Οι ομάδες παίζουν έναν πολύ σημαντικό ρόλο στη διαχείριση χρηστών στα συστήματα UNIX/Linux καθώς εκφράζουν μία λογική οργάνωση των χρηστών. Για παράδειγμα, οι χρήστες που εργάζονται στο ίδιο έργο μπορεί να ενταχθούν σε μια ομάδα, ώστε να έχουν πρόσβαση στα κοινά αρχεία αλλά και σε συγκεκριμένες συσκευές (π.χ. cdrom, scanner).

Οι χρήστες εντάσσονται σε μία πρωτεύουσα ομάδα, την οποία καθορίζει ο διαχειριστής κατά τη δημιουργία του λογαριασμού. Στην πορεία μπορούν να ενταχθούν και σε άλλες ομάδες εφόσον κρίνει ο διαχειριστής πως η ένταξή τους διευκολύνει το έργο της διαχείρισης του συστήματος.

Διαχείριση ομάδων

Η βασική ρύθμιση των ομάδων γίνεται στο αρχείο **/etc/group** που έχει την παρακάτω μορφή:

$ **cat /etc/group**

root:x:0

daemon:x:1

bin:x:2

sys:x:3

...

users:x:100:nemo

students:x:500:alice,bob,carol,dave,eve

Διαχείριση ομάδων

Η εντολή **groups** εμφανίζει τις ομάδες στις οποίες είναι μέλος ένας χρήστης:

$ **groups** # groups where i am member

students

$ **groups nemo** # groups where user nemo is member

users cdrom floppy audio video plugdev netdev lpadmin scanner

Διαχείριση ομάδων

Το δε αρχείο **/etc/gshadow** έχει τη μορφή:

 # cat /etc/gshadow

root:*::

daemon:*::

bin:*::

sys:*::

...

staff:6RJXd4/9pI2$2k/mPKLHgzrW1CxzCbc1gN0b1dAs2z
YvHOe4de.dlpeYRiNNSBEn/Cx4SfMOb39WmyWtF2F5s9jYL8
zSsLmyv1:helga:

students:!::

Διαχείριση ομάδων

Το πρώτο πεδίο αποτελείται από το όνομα της ομάδας και το δεύτερο από τον κωδικό πρόσβασης. Αν ο κωδικός πρόσβασης δεν αποτελείται από ένα κρυπτογραφημένο αλφαριθμητικό αλλά από έναν χαρακτήρα όπως είναι ο αστερίσκος "*****" ή το θαυμαστικό "**!**", τότε οι χρήστες που δεν είναι μέλη της ομάδας δεν μπορούν να γίνουν προσωρινά μέλη της ομάδας. Το τρίτο πεδίο περιέχει τους διαχειριστές της ομάδας, οι οποίοι έχουν το δικαίωμα να αλλάζουν τον κωδικό πρόσβασης και τα μέλη της ομάδας. Τέλος, το τέταρτο πεδίο περιέχει τα μέλη της ομάδας. Αν υπάρχει λίστα μελών, τότε αυτή υπερισχύει της αντίστοιχης εγγραφής του αρχείου /etc/group.

Διαχείριση ομάδων

Για να γίνει ένας χρήστης προσωρινά μέλος μιας ομάδας μπορεί να χρησιμοποιήσει την εντολή **newgrp** και τον αντίστοιχο κωδικό πρόσβασης. Η εντολή newgrp εκτελείται από έναν νέο φλοιό, που δεν κληρονομεί εξ ορισμού το περιβάλλον του αρχικού φλοιού.

```
$ groups                    # show groups where i am member
students
$ newgrp staff              # log in to group staff
Password:
$ groups
students staff
$ exit
```

Διαχείριση ομάδων

Ο κωδικός πρόσβασης μιας ομάδας ορίζεται με την εντολή **gpasswd**. Η εντολή αυτή διαθέτει διάφορες επιλογές, οι σημαντικότερες εκ των οποίων είναι η **-R** με την οποία περιορίζουμε την πρόσβαση μη μελών (θέτει στο πεδίο του κωδικού πρόσβασης τον χαρακτήρα θαυμαστικό) και η **-A user** με την οποία προσθέτουμε έναν χρήστη ως διαχειριστή ομάδας.

Γενικά, η χρήση κωδικού πρόσβασης για ομάδες δε συνιστάται καθώς ο κωδικός κινδυνεύει να γίνει γνωστός. Είναι ασφαλέστερο να προστεθεί ένας χρήστης ως μέλος μιας ομάδας και να διαγραφεί από μέλος όταν δεν είναι άλλο απαραίτητο.

Διαχείριση ομάδων

Η εντολή **groupadd** δημιουργεί μία νέα ομάδα χρηστών στο σύστημα. Η σύνταξή της έχει τη μορφή:

groupradd [options] group

και η σημαντικότερή επιλογή της **-g** GID επιτρέπει τον ορισμό της τιμής του αριθμού ομάδας (Group ID).

 # groupadd testgroup # create new group
testgroup
 # tail -1 /etc/group
testgroup:x:1000:
 # groupadd -g 502 teachers # new group teachers
 # tail -1 /etc/group
testgroup:x:502:

Διαχείριση ομάδων

Η εντολή **groupdel** διαγράφει μια ομάδα χρηστών του συστήματος. Η εντολή έχει σύνταξη:

groupdel [options] group

Η groupdel δε μπορεί να διαγράψει την πρωτεύουσα ομάδα ενός υπάρχοντος χρήστη. Πρέπει πρώτα να αλλάξει η πρωτεύουσα ομάδα του χρήστη ή να διαγραφεί ο χρήστης και μετά να διαγραφεί η ομάδα. Η εντολή αφήνει όμως ανέπαφα τα δικαιώματα πρόσβασης στα αρχεία της ομάδας. Οι πληροφορίες αυτές πρέπει να αλλάξουν χειροκίνητα καθώς τα αρχεία θα ανήκουν σε μία ανύπαρκτη ομάδα (εντολές chown, chgrp).

Διαχείριση ομάδων

Οι επόμενες δύο εντολές διαγράφουν την ομάδα *testgroup* που δημιουργήσαμε προηγουμένως και εμφανίζουν την τιμή εξόδου της τελευταίας εντολής που εκτελέσθηκε στο προσκήνιο:

```
# groupdel testgroup                    # delete group testgroup
# echo $?                               # check return code
0                                       # success
```

Η επόμενη εντολή προσπαθεί να διαγράψει την πρωτεύουσα ομάδα ενός χρήστη:

```
# groupdel students     # try to remove alices primary group
groupdel: cannot remove the primary group of user 'alice'
```

Διαχείριση ομάδων

Η εντολή **groupmod** τροποποιεί τις ιδιότητες μιας ομάδας και έχει την ακόλουθη σύνταξη:

groupmod [options] group

Οι πιο σημαντικές επιλογές της είναι:

-g, **--gid** GID αλλαγή του αριθμού ομάδας σε GID.

Η ενημέρωση των χρηστών που χρησιμοποιούν τη συγκεκριμένη ομάδα ως πρωτεύουσα ομάδα γίνεται αυτόματα, σε αντίθεση με τα αρχεία που πρέπει να ενημερωθούν χειροκίνητα.

-n, **--new-name** NEW_GROUP αλλαγή του ονόματος ομάδας σε NEW_GROUP.

Διαχείριση ομάδων

Η εντολή που ακολουθεί αλλάζει τον αριθμό της ομάδας teachers σε 666 :

 # groupmod -g 666 teachers # change gid of group teachers

 # grep teachers /etc/group

teachers:x:666:

Η επόμενη εντολή αλλάζει το όνομα της ομάδας teachers σε lecturers:

 # groupmod -n lecturers teachers # rename group teachers

Δικαιώματα Διαχειριστή σε Χρήστες

Η δημιουργία ενός χρήστη με δικαιώματα υπερχρήστη είναι μια επικίνδυνη ενέργεια που πρέπει γενικά να αποφεύγεται. Γίνεται εύκολα με την εντολή *useradd* ορίζοντας τον ίδιο αριθμό χρήστη και αριθμό ομάδας με τον χρήστη root, δηλαδή την τιμή μηδέν.

 # useradd -ou 0 -g 0 root2 # grant root privileges to new user

 # passwd root2 # set his password immediately

Η επιλογή **-o** ή **--non-unique** επιτρέπει τη δημιουργία νέου χρήστη με διπλό uid και είναι έγκυρη μόνο σε συνδυασμό με την επιλογή **-u**.

Δικαιώματα Διαχειριστή σε Χρήστες

- Η εντολή *usermod* με τις παραπάνω επιλογές επιτρέπει τη μεταβίβαση των προνομίων του υπερχρήστη σε υπάρχοντες χρήστες.
- Εναλλακτικά μπορούμε να επεξεργαστούμε το αρχείο /etc/passwd και να αλλάξουμε χειρωνακτικά τον αριθμό ταυτότητας χρήστη και την πρωτεύουσα ομάδα του σε μηδέν.

Δικαιώματα Διαχειριστή σε Χρήστες

Η εντολή **su** (substitute user) επιτρέπει την προσωρινή μας είσοδο στο σύστημα με το λογαριασμό κάποιου άλλου χρήστη χωρίς να είναι απαραίτητο να αποσυνδεθεί πρώτα ο χρήστης από το λογαριασμό του. Προφανώς για να συνδεθούμε ως άλλος χρήστης θα πρέπει να γνωρίζουμε τον κωδικό του πρόσβασης, κάτι που δεν ισχύει για τον υπερχρήστη. Η σύνταξη της εντολής έχει ως εξής:

su [options] [username]

Αν την καλέσουμε χωρίς να προσδιορίσουμε το όνομα χρήστη, χρησιμοποιεί ως προκαθορισμένο όνομα το root. Αυτή άλλωστε είναι η συνήθης χρήση της εντολής.

Δικαιώματα Διαχειριστή σε Χρήστες

Η πιο σημαντική επιλογή της εντολής είναι η παύλα “**–**”, η χρήση της οποίας παρέχει ένα περιβάλλον παρόμοιο με αυτό που αναμένει ο χρήστης αν έκανε απ’ ευθείας σύνδεση.

Η επόμενη εντολή συνδέει τον χρήστη alice ως χρήστη bob:

```
alice@debian:~$ su bob                  # login as user bob
Password:                               # enter bob's password
bob@debian:/home/alice$                 # directory not changed
```

Δικαιώματα Διαχειριστή σε Χρήστες

Η συμπεριφορά του φλοιού καθορίζεται από αρχεία ρυθμίσεων, τα οποία ο φλοιός διαβάζει κατά την εκκίνησή του και ενημερώνει διάφορες μεταβλητές οι οποίες αποτελούν το λεγόμενο περιβάλλον του φλοιού (shell environment). Πληροφορίες για το τρέχον περιβάλλον μπορούμε να πάρουμε με τις εντολές **env** ή **printenv**:

```
$ env                                    # print environment
USER=bob
PWD=/home/alice
HOME=/home/bob
...
PATH=/usr/local/bin:/usr/bin:/bin:/usr/local/games
```

Δικαιώματα Διαχειριστή σε Χρήστες

Η σύνδεση με τον λογαριασμό root γίνεται με την εντολή:

```
$ su -                          # su – root, login as root
Password:                       # enter root's password
# whoami; pwd                   # print working directory
root
/root
```

Η επιλογή "**–**" έχει ως αποτέλεσμα να αλλάξει ο κατάλογος εργασίας και το περιβάλλον του φλοιού, τα οποία προσαρμόζονται σύμφωνα με τον λογαριασμό εισόδου. Η αποσύνδεση και επιστροφή στον αρχικό λογαριασμό γίνεται με την εντολή **exit.**

Δικαιώματα Διαχειριστή σε Χρήστες

- Η εντολή **sudo** (superuser do - substitute user do) παρέχει έναν εναλλακτικό τρόπο διαχείρισης του συστήματος. Πιο συγκεκριμένα, η εντολή επιτρέπει την εκτέλεση εντολών ή προγραμμάτων με τα δικαιώματα κάποιου άλλου χρήστη (συνήθως του υπερχρήστη).
- Σε αντίθεση με την εντολή su, οι χρήστες χρησιμοποιούν τον δικό τους κωδικό πρόσβασης αντί για τον κωδικό του root. Μετά την ταυτοποίηση του χρήστη και τον έλεγχο του αρχείου ρυθμίσεων **/etc/sudoers**, ο φλοιός θα εκτελέσει το πρόγραμμα που ζήτησε ο χρήστης.

Δικαιώματα Διαχειριστή σε Χρήστες

Σε κάποια συστήματα, όπως για παράδειγμα στο Ubuntu, ο λογαριασμός root είναι απενεργοποιημένος και η διαχείριση του συστήματος γίνεται αποκλειστικά με τη χρήση της εντολής sudo. Αν δεν είναι εγκατεστημένη στο σύστημά μας μπορούμε να την εγκαταστήσουμε με την εντολή:

 # apt-get install sudo # install sudo in Debian

Η σύνταξη της εντολής έχει τη μορφή:

sudo [options] [user] command

και στην περίπτωση που δεν δοθεί όνομα χρήστη χρησιμοποιείται ως προκαθορισμένο όνομα ο λογαριασμός του χρήστη root.

Δικαιώματα Διαχειριστή σε Χρήστες

Ο πιο απλός τρόπος για να ορίσουμε τους χρήστες που θα έχουν τη δυνατότητα να εκτελούν εντολές ως υπερχρήστης είναι να τους προσθέσουμε στην ομάδα sudo:

 # usermod -a -G sudo helga # add helga to group sudo

 # grep sudo /etc/group

sudo:x:27:helga

Όταν στη συνέχεια ο χρήστης helga θέλει να εκτελέσει μια εντολή που απαιτεί δικαιώματα διαχειριστή θα πρέπει να πληκτρολογήσει και τον κωδικό πρόσβασης:

$ **sudo apt-get update** # apt-get needs root permission

[sudo] password for helga: # enter helga's password

Δικαιώματα Διαχειριστή σε Χρήστες

Το αρχείο /etc/sudoers πρέπει να τροποποιείται πάντα με τη χρήση της εντολής **visudo**, καθώς η απευθείας επεξεργασία του μπορεί να δημιουργήσει λάθη ρυθμίσεων με αποτέλεσμα να μη μπορεί να εκτελεστεί η εντολή sudo.

Η κλήση της εντολής visudo

 # visudo

εμφανίζει το αρχείο /etc/sudoers στον προκαθορισμένο κειμενογράφο:

```
# This file MUST be edited with the 'visudo' command as root.
# Please consider adding local content in /etc/sudoers.d/
# instead of directly modifying this file.
```

Δικαιώματα Διαχειριστή σε Χρήστες

```
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/sbin:/bin"

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:
#includedir /etc/sudoers.d
```

Δικαιώματα Διαχειριστή σε Χρήστες

- Η γραμμή **Defaults env_reset** έχει ως αποτέλεσμα να αφαιρούνται από το περιβάλλον του τερματικού μεταβλητές που ορίστηκαν από τον χρήστη για λόγους α-σφαλείας.
- Η επόμενη γραμμή **Defaults mail_badpass** ενεργοποιεί την ενημέρωση του χρήστη root με ηλεκτρονικό ταχυδρομείο για ανεπιτυχείς προσπάθειες εισόδου με λανθασμένο κωδικό πρόσβασης.
- Τέλος, η τρίτη γραμμή που αρχίζει με **Defaults secure_path=** καθορίζει τα μονοπάτια, τους καταλόγους δηλαδή του συστήματος, στα οποία η εντολή sudo επιτρέπεται να αναζητήσει εφαρμογές προς εκτέλεση.

Δικαιώματα Διαχειριστή σε Χρήστες

Η γραμμή

root ALL=(ALL:ALL) ALL

καθορίζει πως ο χρήστης root μπορεί σε οποιοδήποτε υπολογιστή, λειτουργώντας ως οποιοσδήποτε χρήσης ή μέλος ομάδας, να εκτελέσει οποιαδήποτε εντολή.

Η επόμενη γραμμή αρχίζει με τον χαρακτήρα **%**, η οποία υποδηλώνει πως η οδηγία αναφέρεται σε ομάδα, αφορά δηλαδή όλα τα μέλη της συγκεκριμένης ομάδας:

%sudo ALL=(ALL:ALL) ALL

Σύμφωνα με αυτήν, τα μέλη της ομάδας sudo έχουν παρόμοια προνόμια με αυτά του χρήστη root.

Δικαιώματα Διαχειριστή σε Χρήστες

Αν θέλουμε να επιτρέψουμε στον χρήστη nemo να εκτελεί την εντολή useradd χωρίς να χρειάζεται να πληκτρολογεί συνθηματικό, μπορούμε να προσθέσουμε την επόμενη γραμμή στο αρχείο:

nemo ALL=NOPASSWD: /usr/sbin/useradd

Δικαιώματα Διαχειριστή σε Χρήστες

Για την καλύτερη οργάνωση του αρχείου ρυθμίσεων μας δίνεται η δυνατότητα να ορίσουμε ομάδες χρηστών, υπολογιστών και εντολών:

User_Alias OPERATORS = alice, nemo

Host_Alias SRV = *.teiath.gr

Cmnd_Alias POWER = /sbin/shutdown, /sbin/reboot

Στη συνέχεια μπορούμε να προσθέσουμε οδηγίες στο αρχείο ρυθμίσεων, αναφερόμενοι στις ομάδες αυτές ως εξής:

OPERATORS SRV = POWER

Οι χρήστες alice και nemo, που είναι μέλη της ομάδας OPERATORS έχουν δικαίωμα να εκτελούν με sudo τις εντολές shutdown και reboot στους υπολογιστές του domain teiath.gr

Δικαιώματα Διαχειριστή σε Χρήστες

Κατά την αποθήκευση του αρχείου αν τυχόν έχουμε κάνει κάποιο συντακτικό λάθος θα εμφανιστεί ένα μήνυμα της μορφής:

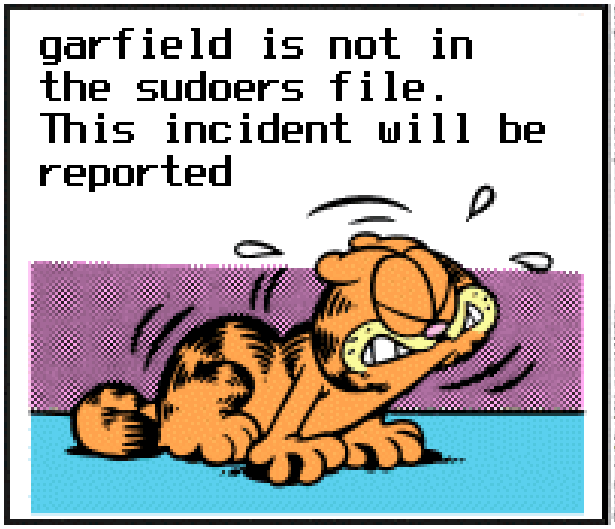
>>> /etc/sudoers: syntax error near line 30 <<<

What now?

Εδώ έχουμε τη δυνατότητα να επιλέξουμε μεταξύ των επιλογών (**e**)dit για επεξεργασία, e(x)it για έξοδο χωρίς αποθήκευση και (**Q**)uit για έξοδο με αποθήκευση, το οποίο προφανώς δε συνιστάται.

Από προεπιλογή, η εντολή sudo αποθηκεύει τα στοιχεία ελέγχου ταυτότητας ενός χρήστη για ένα συγκεκριμένο χρονικό διάστημα (συνήθως 15 min).

Ερωτήσεις


garfield is not in
the sudoers file.
This incident will be
reported


HEY- WHO DOES SUDO REPORT THESE TO?
I'VE NEVER CHECKED


HE TRIED TO USE THE SUDO COM-MAND AGAIN, SIR
MAN, THAT CAT CAN'T HACK