Εργασία 2 Γεώργιος Μιχούλης dai16067

ISS: ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ

Θέμα 1. Γενικά στο αρχείο /etc/passwd αποθηκεύονται σημαντικές πληροφορίες που χρειάζονται στο login ,δηλαδή οι πληροφορίες του λογαριασμού του. Το αρχείο αυτό είναι τύπου κειμένου-txt στο οποίο περιλαμβάνονται στοιχεία για τους λογαριασμούς του συστήματος και για κάθε λογαριασμό κρατάει το groupID to userID, shell κ.α. Έχει ένα read permission και πολλές λειτουργίες και μεταβάλλετε μόνο οι superuser/root λογαριασμοί. Οι κρυπτογραφημένοι κωδικοί βρίσκονται στο /shadow αρχείο και όχι στο /passwd. Ο μηχανισμός που χρησιμοποιείται για να προστατευτούν οι κωδικοί πρόσβασης είναι το πακέτο shadow-utils, το οποίo μεταφέρει τους κωδικούς από το /etc/passwd στο /etc/shadow. Βασικά παράγει μια μέθοδο τύπου hashing το οποίο φτιάχνει ένα τυχαίο string με βάση ένα άλλο string ( πχ κωδικός χρήστη) το οποίο δεν προδίδει το δεύτερο σε καμία περίπτωση.

Θέμα 2ο. α. 0666 -rw-rw-rw- β.0777 -rwxrwxrwx γ.0000 ---------- δ. 0555 dr-xr-x---

Θέμα 3ο. α. Από την στιγμή που το group έχει δικαιώματα ανάγνωσης και εγγραφής τότε αυτά κληρονομούνται και στον χρήστη του που αυτός θα μπορούσε να έχει εξαρχής μόνο ανάγνωσης δικαίωμα οπότε ο χρήστης θα έχει και το δικαίωμα ανάγνωσης (read) αλλά και εγγραφής (write).

β. Στην περίπτωση που αφαιρείται ένα δικαίωμα από έναν χρήστη συγκεκριμένα δεν μπορεί να το κληρονομήσει από το group οπότε ο χρήστης θα έχει μόνο το δικαίωμα της ανάγνωσης (read).

Θέμα 6ο. a) $ sudo groupadd guest b) $ sudo useradd -G guest student110

c) $ sudo useradd -G guest student011 d) $ sudo chgrp guest traff1c.out

Θέμα 4ο. Δεν επιτρέπετε η μεταφορά δικαιωμάτων σε έναν απλό χρήστη καθώς αυτός με την σειρά του θα μπορούσε να αποκλείσει τον λογαριασμό του από το να έχει πρόσβαση σε κάποιο αρχείο που ο ίδιος έχει κατασκευάσει πχ εντολή chown otheruser ownfile. Τέλος κάποιος τρίτος θα μπορούσε να αποκτήσει πρόσβαση στον λογαριασμό και τον φάκελο του χρήστη , τροποποιώντας έτσι τα δεδομένα του ή ακόμα και θα μπορούσε να τα κλέψει ή να τα διαγράψει εντελώς ή ακόμα και να τα κλειδώσει ζητώντας του λύτρα για την ανάκτηση τους.

Θέμα 5ο. ls –l umount

-rwsr-xr-x. 1 root root 53472 Oct 21 2011 /bin/umount

ls –l uname

-rwxr-xr-x. 1 root root 24232 Oct 21 2011 /bin/uname

H διαφορά βρίσκεται στο -rw**s**r-xr-x, το οποίο ουσιαστικά είναι το setuid bit. Το unmount εκτελείται με root από όλους του χρήστες. Ο ιδιοκτήτης του προγράμματος είναι ο root.

Θέμα 9ο. $sudo setfacl -m u:alice:r rules.pdf $sudo setfacl –m g:guests:rx file2.obt

$sudo setfacl -m u:alice:--- readme.txt

Θέμα 7ο. Το ΡΑΜ έχει αρκετά πλεονεκτήματα μερικά από αυτά είναι: 1) ότι έχει ένα μοναδικό κοινό σύστημα ταυτοποίησης και ελέγχου που μπορεί να χρησιμοποιηθεί από πολλές εφαρμογές, 2) επιτρέπει στους προγραμματιστές να αναπτύξουν τις εφαρμογές τους χωρίς να χεριάζετε να δημιουργήσουν ένα δικό τους σύστημα ταυτοποίησης και ελέγχου, 3) έχει ευελιξία όσον αφορά την ταυτοποίηση τόσο για τους διαχειριστές όσο και για τους προγραμματιστές των προγραμμάτων.

Θέμα 8ο. Το Discretionary Access control είναι ένα μέσο για τον περιορισμό της πρόσβασης σε αντικείμενα με βάση την ταυτότητα των ατόμων που προσπαθούν να τα λειτουργήσουν ή να έχουν πρόσβαση σε αυτά για παράδειγμα ο μηχανισμός των δικαιωμάτων δημιουργείται από τον ιδιοκτήτη του υποκείμενου , οπότε και είναι ο ιδιοκτήτης του αντικειμένου και ορίζει ποιοι χρήστες και τι προνομία πρόσβασης θα έχουν στα αντικείμενα του. Αυτό το είδος της πρόσβασης ελέγχει την ικανότητα του να χρησιμοποιεί χαρακτηριστικά όπως είναι η ανάγνωση, γραφή, εκτέλεση κ.α. , για να ορισει τα δικαιώματα που εφαρμόζεται στο αντικείμενο. Τέλος υπάρχει και ο ιδιοκτήτης και ο χρήστης και πολλές επιλογές που μπορούν να μοιραστούν όπως είναι οι ομάδες.