Linux Permissions & PAM

ΚΟΤΖΑΝΙΚΟΛΑΟΥ ΠΑΝΑΓΙΩΤΗΣ

ΧΑΤΖΗΣΩΦΡΟΝΙΟΥ ΓΙΩΡΓΟΣ

ΚΟΡΕΑΣ ΠΛΑΤΩΝ

Χρήστες (Unix Accounts)

- ✓Όνομα χρήστη (Username)
- ✓Κωδικός (Password)
- ✓/home
- ✓uid (user id)
- ✓shell

Ομάδες (Unix Groups)

✓Ένα σύνολο από χρήστες

✓Μας επιτρέπει να ορίσουμε συγκεκριμένα δικαιώματα πάνω σε μια ομάδα χρηστών

Ο ειδικός λογαριασμός root

- ✓Έχει πρόσβαση σε όλες τις εντολές και στα αρχεία
- ✓/root
- ✓uid=0

Εντολές διαχείρισης χρηστών

- ✓useradd
- ✓deluser
- ✓usermod
- ✓passwd

Εντολές διαχείρισης ομάδων

- ✓groupadd
- ✓groupdel
- ✓groupmod

/etc/passwd

- ✓Περιέχει εγγραφές με όλους τους χρήστες του συστήματος
- ✓Μορφή εγγραφής: username:x:uid:gid:username:home:shell

/etc/passwd

✓Εργαλεία και προγράμματα χρησιμοποιούν λογαριασμούς για λόγους ασφάλειας

- έχουν uid < 1000
- /bin/false για shell

/etc/shadow

- ✓Περιέχει τα **hashes των κωδικών των χρηστών**
- ✓Μπορεί να διαβαστεί μόνο από τον root
- ✓Κάθε εγγραφή περιέχει κι άλλες πληροφορίες
  - τις μέρες πριν το σύστημα αναγκάσει το χρήστη να αλλάξει κωδικό
  - τις μέρες πριν το σύστημα απενεργοποιήσει το λογαριασμό

/etc/group

- ✓Αντίστοιχο του /etc/passwd για ομάδες
- ✓Εγγραφές όλων των group με τα μέλη τους

Μοντέλο δικαιωμάτων

- ✓Κάθε αρχείο ανήκει σε ένα χρήστη (owner) και μία ομάδα
- ✓Αλλάζω την ιδιοκτησία με chown και chgrp

Μοντέλο δικαιωμάτων

✓Wildcards στο ls -l

- w - write
- r - read
- e - execute

✓Απεικόνιση δικαιωμάτων με χαρακτήρες

- 3 τριάδες χαρακτήρων για owner, group, others
- για παράδειγμα, r-xrwxrwx

Μοντέλο δικαιωμάτων

- ✓Απεικόνιση χαρακτήρων με αθροίσματα αριθμών
  - x = 1
  - w = 2
  - r = 4
- ✓chmod

suid & sgid

✓Όταν εκτελείται ένα πρόγραμμα, τρέχει με τα δικαιώματα του χρήστη που κάνει την εκτέλεση

✓Με τα ειδικά bits suid και sgid **το πρόγραμμα εκτελείται με τα δικαιώματα του ιδιοκτήτη του**

Φτιάχνοντας χρήστη “με το χέρι”

Τί θα πρέπει να κάνουμε για να φτιάξουμε ένα χρήστη με το group του χωρίς την εντολή useradd;

Φτιάχνοντας χρήστη “με το χέρι”

1. Προσθήκη εγγραφής στο /etc/passwd
2. Προσθήκη εγγραφής στο /etc/shadow
3. Προσθήκη εγγραφής στο /etc/group
4. Δημιουργία home directory με τα κατάλληλα δικαιώματα

Ανέλιξη Δικαιωμάτων (Privilege Escalation)

✓Εκμετάλλευση τεχνικού σφάλματος (bug) ή σχεδιαστικού λάθος (design flaw) ή λάθους παραμετροποίησης (misconfiguration) σε ένα λογισμικό ή λειτουργικό σύστημα με στόχο την πρόσβαση σε πόρους που είναι κανονικά προστατευμένα από έναν χρήστη ή ένα πρόγραμμα

Ανέλιξη Δικαιωμάτων (Privilege Escalation)

✓Έστω ο ακόλουθος C κώδικας:

```
setuid(0);
system(argv[1]);
```

✓Έστω ότι τα δικαιώματα του αντίστοιχου εκτελέσιμου είναι:

-rwsrwxr-x 1 root root 8792 Dec 13 22:22 run_command

Πού είναι η ευπάθεια;

Ανέλιξη Δικαιωμάτων (Privilege Escalation)

test@cs-unipi-sec:~$ ./run_command whoami
The argument supplied is whoami
root

test@cs-unipi-sec:~$ ./run_command /bin/bash

The argument supplied is /bin/bash

root@cs-unipi-sec:~# cat /etc/shadow

[...]

SSH

✓Κρυπτογραφικό πρωτόκολλο επικοινωνίας δύο απομακρυσμένων κόμβων (Server - Client)

✓Εγκαθίσταται ένα ασφαλές κανάλι επικοινωνίας σε ένα μη ασφαλές δίκτυο

✓Ασύμμετρη κρυπτογραφία για αυθεντικοποίηση :)

✓Υλοποίηση OpenSSH σε συστήματα τύπου Unix

✓Standard TCP πόρτα 22

Επιθέσεις ωμής βίας / λεξικού στο SSH

✓Οριζόντιο brute-forcing σε δημοφιλή usernames

- Δεδομένα από honeypots:

```
#attempts #username
      9012  root (58%)
      179  test (1%)
      116  oracle (< 1%)
      87  admin
      82  info
      70  user
      69  postgres
      68  mysql
```

✓Χρήση λεξικών

- Συλλογές από βάσεις δεδομένων που έχουν διαρρεύσει ή παραβιαστεί

Αντίμετρα σε επιθέσεις ωμής βίας

✓Πώς μπορούμε να αμυνθούμε από επιθέσεις ωμής βίας;

Αντίμετρα σε επιθέσεις ωμής βίας

✓Ας εισάγουμε μία πολιτική ασφάλειας

- Μόνο δυνατοί κωδικοί!
- Το σύστημα θα επιβάλει την αλλαγή κωδικών των χρηστών σε τακτά χρονικά διαστήματα

Linux PAM

- ✓Pluggable Authentication Method
- ✓Μηχανισμός του Linux για αυθεντικοποίηση υπηρεσιών και εφαρμογών
  - Παρέχει API υπηρεσιών αυθεντικοποίησης
- ✓Μας επιτρέπει να ορίσουμε τη δική μας πολιτική ασφάλειας

Η λειτουργία του PAM

- ✓Ο έλεγχος πρόσβασης πραγματοποιείται εκτός του περιβάλλοντος Kernel σε αντίθεση με την κλασσική αυθεντικοποίηση των Linux
- ✓Το PAM υποστηρίζει κοινόχρηστες βιβλιοθήκες για την κατασκευή μηχανισμών ελέγχου ταυτότητας οι οποίες βρίσκονται υπό του φακέλου (/lib/security)
- ✓Οι εφαρμογές χρησιμοποιούν το module pam_authenticate για την αυθεντικοποίηση και το αρχείο /etc/pam.conf ή /etc/pam.d/ για την παραμετροποίηση
- ✓Υπάρχουν πάνω από 70 μονάδες/modules PAM, η καθεμία με τις δικές της επιλογές και ανταποκρίσεις ως προς το σύστημα.
- ✓Όλες οι μονάδες βρίσκονται μέσα στον φάκελο /lib/security

Πλεονεκτήματα του PAM

Ο διαχειριστής του συστήματος μπορεί να επιλέξει:

- ✓ τον προεπιλεγμένο μηχανισμό ελέγχου αυθεντικοποίησης για το σύστημα του.
- ✓ μέσα από μια μεγάλη γκάμα από μηχανισμούς αυθεντικοποίησης, από την χρήση ενός απλού κωδικού πρόσβασης μέχρι ένα σύστημα αναγνώρισης προσώπων
- ✓ να διαμορφώσει τον μηχανισμό ελέγχου ταυτότητας του χρήστη βάσει της εφαρμογής που επιθυμεί.
- ✓ πολλαπλούς κωδικούς πρόσβασης εάν κρίνεται απαραίτητο, για την επίτευξη υψηλότερης ασφάλειας
- ✓ την χρήση ενός module PAM χωρίς να αλλάξει τον βασικό μηχανισμό αυθεντικοποίησης του συστήματος

Υποθετικό παράδειγμα

1. Το πρόγραμμα X

2. χρησιμοποιεί ένα PAM module /lib/security/foo

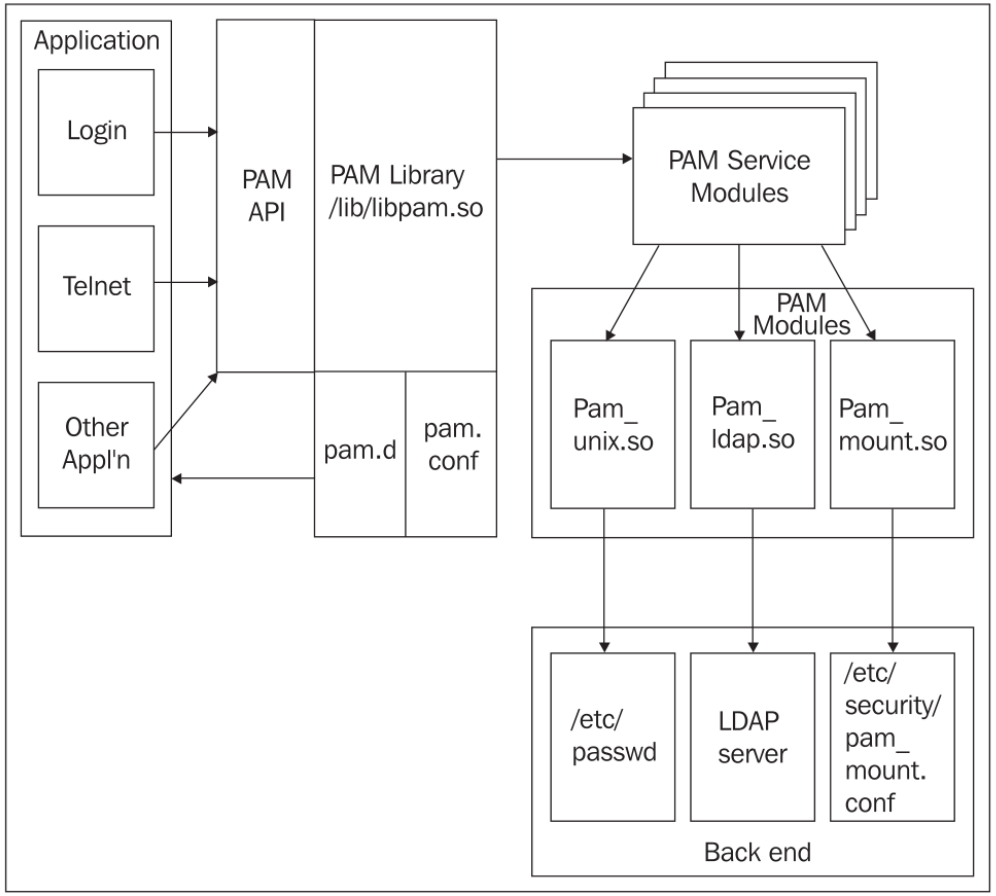
3. Παραμετροποιείται από το αρχείο ρυθμίσεων του /etc/pam.d/foo

4. για να εκτελεστούν ενέργειες αυθεντικοποίησης Y

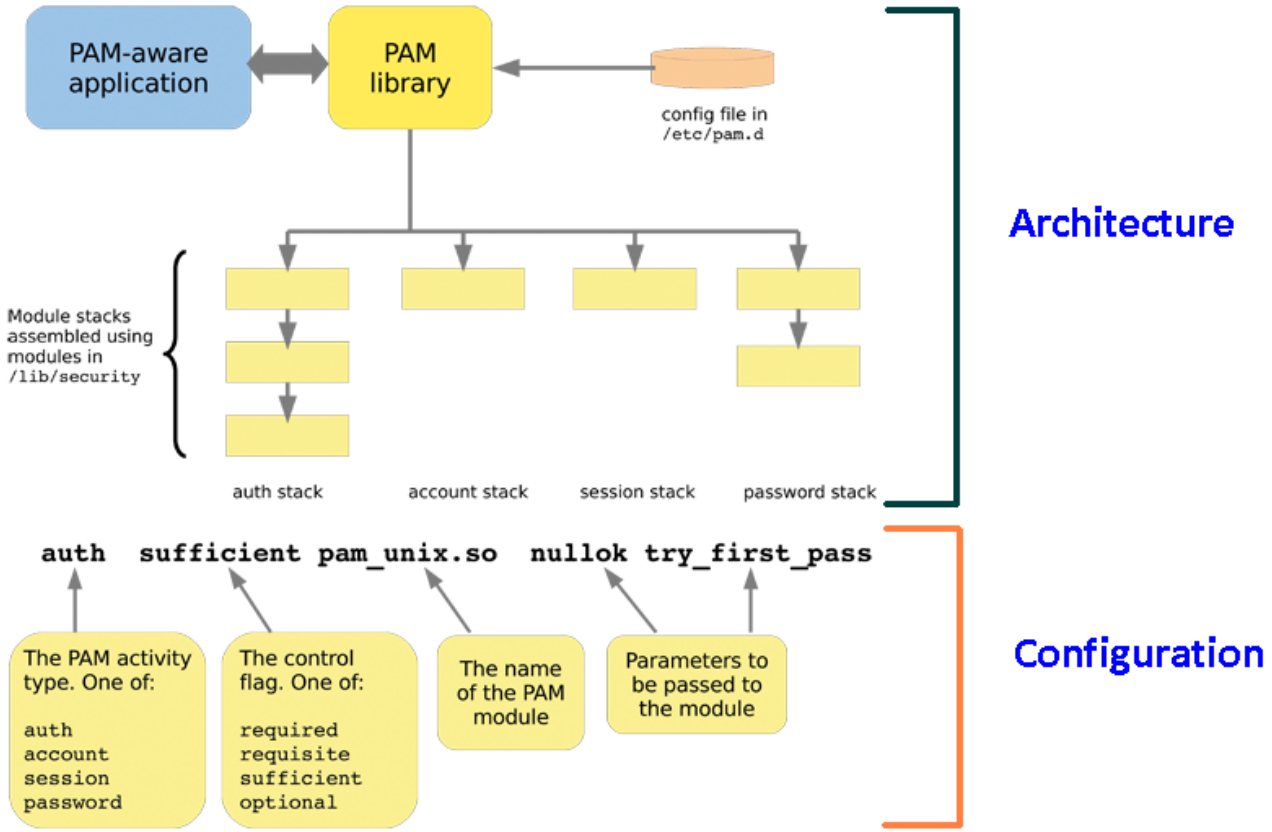
Κοινές μονάδες PAM

- ✓pam_cracklib - αξιολογεί την ισχύ του συνθηματικού πρόσβασης
- ✓pam_issue – προσθέτει προκαθορισμένο κείμενο κατά την σύνδεση του χρήστη
- ✓pam_nologin – ελέγχει εάν υπάρχει /etc/nologin
- ✓pam_rootok – ελέγχει εάν ο χρήστης είναι root
- ✓pam_securetty - ελέγχει εάν η τρέχουσα tty είναι κατοχυρωμένη στο /etc/securetty
- ✓pam_time - ελέγχει τον επιτρεπόμενο χρόνο μεταξύ των διαδοχικών συνδέσεων /etc/security/time.conf

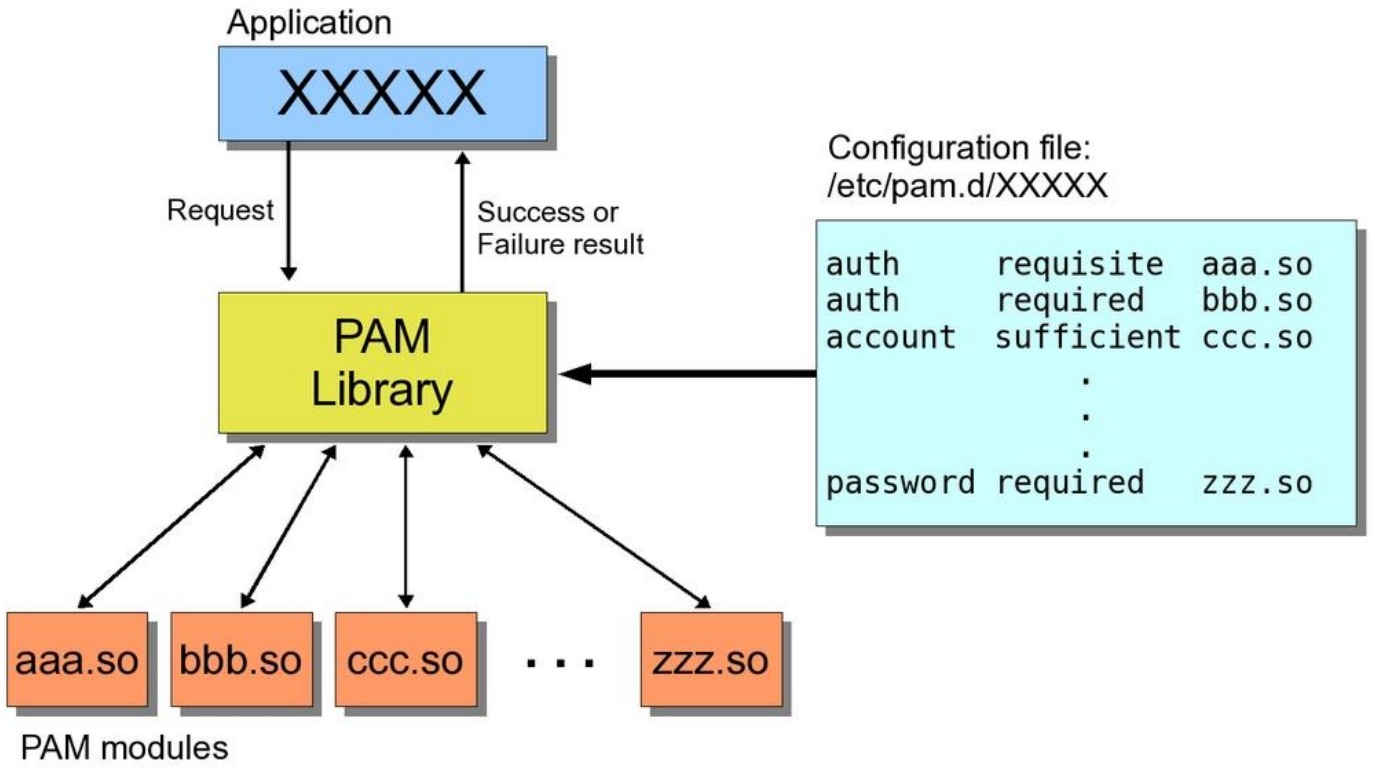
Αρχιτεκτονική PAM



Αρχιτεκτονική PAM



Αρχιτεκτονική PAM



Τύποι Διεπαφών των PAM

✓**Auth** : ελέγχει ποιος είναι ο χρήστης

(Λειτουργεί τόσο για τον έλεγχο του χρήστη μέσω του κωδικού του πρόσβασης όσο και για να παρέχει προνόμια στα μέλη μιας ομάδας/group.)

✓**Account** : ελέγχει εάν επιτρέπεται η πρόσβαση στον λογαριασμό

(Εκτελείται ξεχωριστά από το σύστημα διαχείρισης χρηστών και συνήθως χρησιμοποιείται για το περιορισμό ή τη πρόσβαση σε μια υπηρεσία ανάλογα με την χρονική περίοδο μέσα σε μια ημέρα)

Τύποι Διεπαφών των PAM

✓**Password** : ελέγχει εάν έχει αλλαχθεί ο κωδικός και τον ενημερώνει για τον κάθε χρήστη

✓**Session** : ελέγχει & διαχειρίζεται την συνεδρία σύνδεσης

(Λειτουργεί για να το υπάρχει έλεγχος σε υπηρεσίες κατά την συνεδρία του χρήστη όπως έλεγχος αρχείων καταγραφής)

Αρχείο ρύθμισης του PAM

Βρίσκεται το αρχείο ρύθμισης του PAM στο /etc/pam.d ή το/etc/pam.conf

service-name module-type control-flag module-path module-options

service-name: το όνομα της υπηρεσίας, μπορεί να είναι για παράδειγμα su, ftp, login ή passwd κτλ.

module-type: auth, account, session ,password

control-flag: η παράμετρος αυτή ελέγχει την συμπεριφορά του PAM module σε περίπτωση που θα επιτύχει ή αποτύχει η διαδικασία ελέγχου ταυτότητας. Τα control flags που χρησιμοποιούνται είναι τα binding, include, optional, required, requisite και sufficient

Αρχείο ρύθμισης του PAM

service-name module-type control-flag module-path module-options

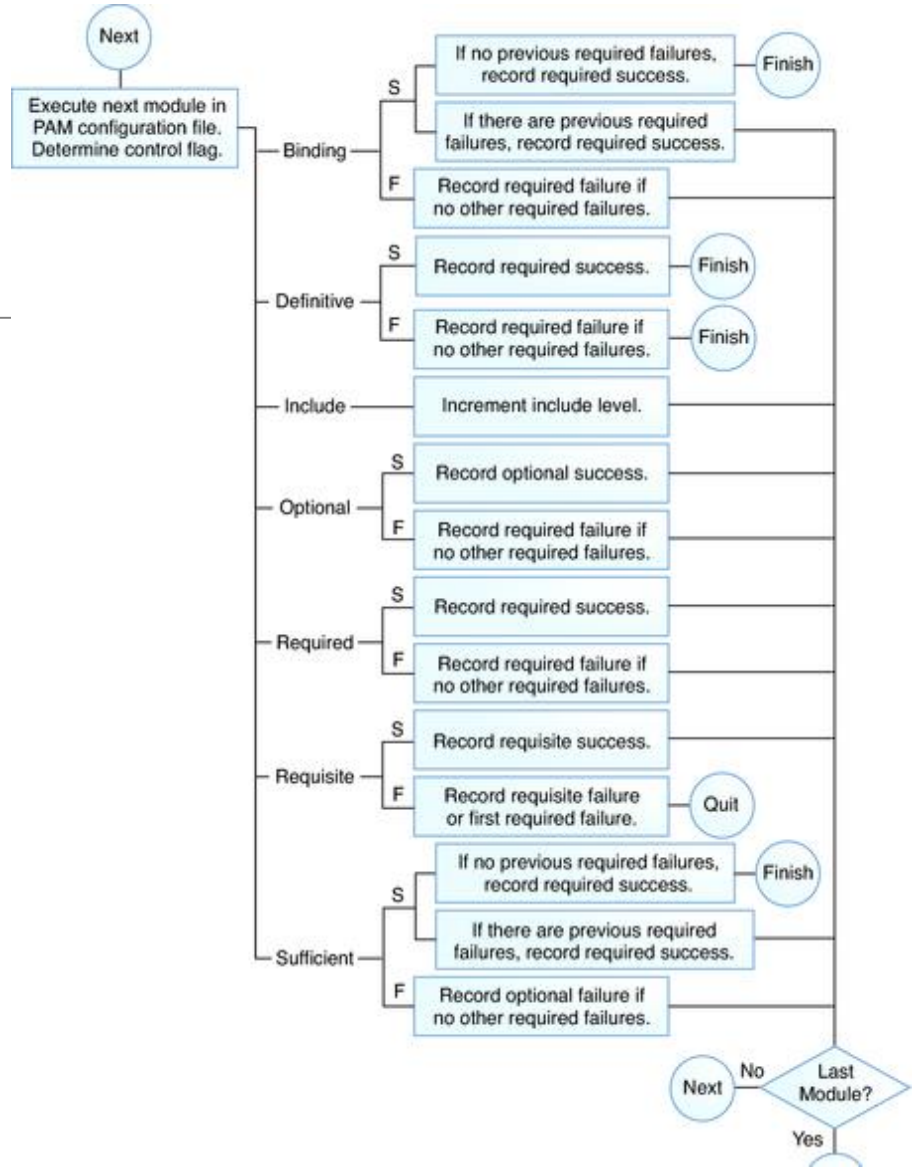
module-path: η παράμετρος αυτή οδηγεί στην διαδρομή προς το αντικείμενο της βιβλιοθήκης που υλοποιεί την υπηρεσία. Εάν η διαδρομή δεν είναι απόλυτη τότε θεωρείται ότι είναι σχετική με το με το /usr /lib /security

module-options : η παράμετρος αυτή μας δίνει την δυνατότητα να προσθέσουμε επιπρόσθετες επιλογές του module με βάση τον τρόπο κατασκευή του καθενός. Συνήθως περιλαμβάνουν την nowarn και την debug επιλογή.

Τιμές ελέγχου PAM

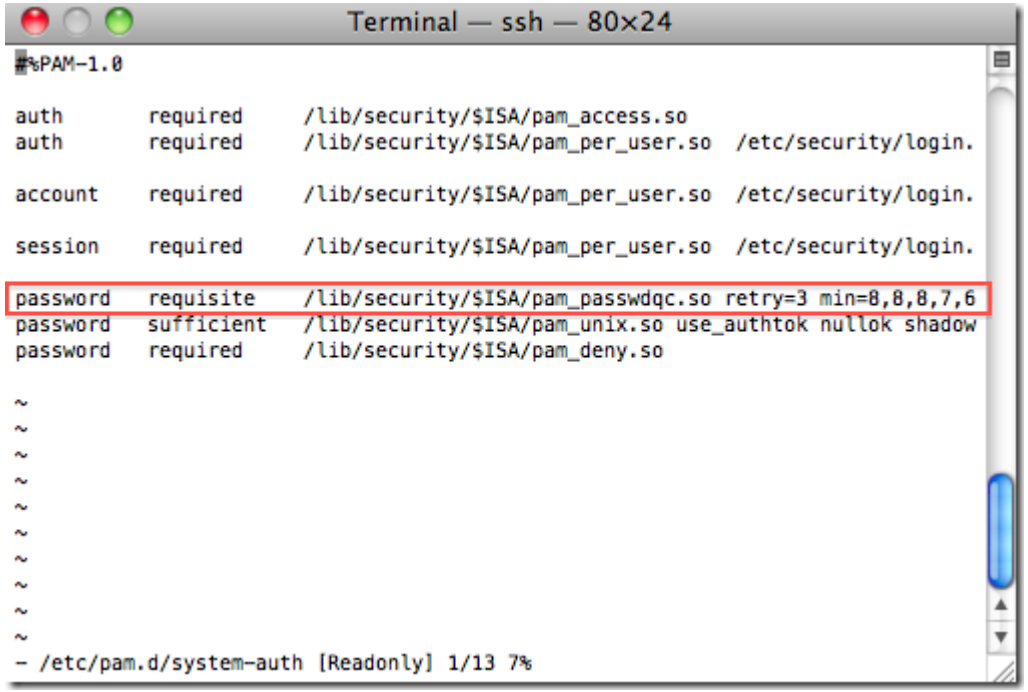
Τιμή	Επιτυχία εκτέλεση	Αποτυχία εκτέλεσης
requisite	Συνεχεία της εκτέλεσης	Διακοπή της εκτέλεσης
required	Συνεχεία της εκτέλεσης	Μήνυμα σφάλματος εφόσον όμως εκτελεστούν όλα τα υπόλοιπα modules
Sufficient	Σταματά η εκτέλεση εφόσον υπάρχει προηγούμενο module required με σφάλμα	Συνεχεία της εκτέλεσης
optional	Συνεχεία της εκτέλεσης	Συνεχεία της εκτέλεσης εφόσον όμως δεν υπάρχουν άλλα σφάλματα από τα υπόλοιπα modules

Λογικό διάγραμμα με την χρήση των τιμών ελέγχου PAM



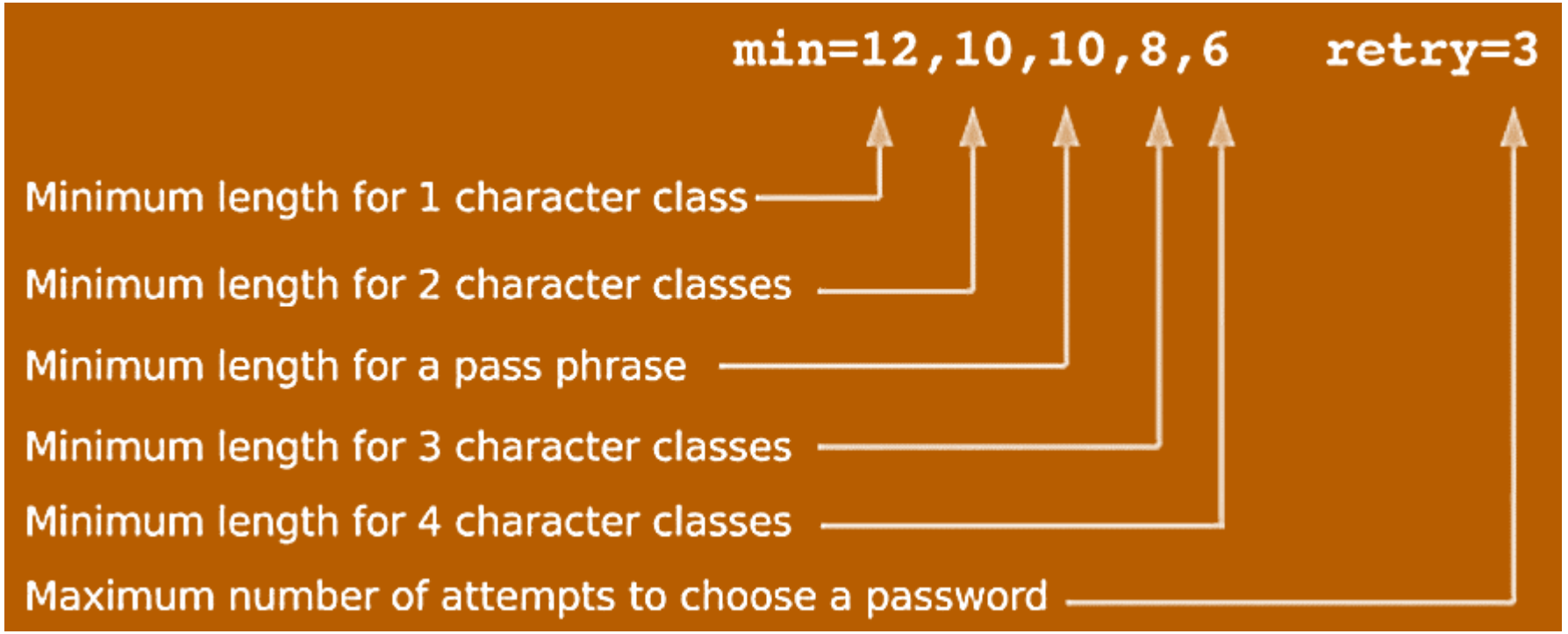
Παράδειγμα για έλεγχο ισχυρών κωδικών πρόσβασης

```
~ # cat /etc/pam.d/system-auth
#%PAM-1.0

auth        required      /lib/security/$ISA/pam_access.so
auth        required      /lib/security/$ISA/pam_per_user.so  /etc/security/login.map

account     required      /lib/security/$ISA/pam_per_user.so  /etc/security/login.map

session     required      /lib/security/$ISA/pam_per_user.so  /etc/security/login.map

password    requisite     /lib/security/$ISA/pam_passwdqc.so retry=3 min=8,8,8,7,6
password    sufficient    /lib/security/$ISA/pam_unix.so use_authtok nullok shadow
password    required      /lib/security/$ISA/pam_deny.so
```



Παράδειγμα για έλεγχο ισχυρών κωδικών πρόσβασης

password requisite pam_passwdqc.so min=12,10,10,8,6 retry=3



Βιβλιογραφία

Έντυπη

✓Pluggable Authentication Modules, Packt Publishing

Ηλεκτρονική

https://docs.oracle.com/cd/E26502_01/html/E29015/pam-32.html

http://www.linux-pam.org/Linux-PAM-html

https://en.opensuse.org/openSUSE:Pam-face-authentication_project

https://linux.die.net/man/8/pam_passwdqc

https://www.techrepublic.com/article/enforce-strong-passwords-with-pam-passwdqc/