Κεφάλαιο 6:SELinux – RH134 Συμπληρωματικές σημειώσεις

Γεώργιος Μαγκλάρας PhD
Associate Instructor
RedHat Academy
Πανεπιστήμιο Δυτικής Αττικής

Η ασφάλεια πληροφοριακών συστημάτων

- Ευρεία έννοια, πολυπαραγοντική
- Ένα σύστημα είναι ασφαλές όταν η συμπεριφορά του κάτω απο ένα εύρος λειτουργικών συνθηκών είναι προβλέψιμη και τεκμηριωμένη.
- Μέρος της διαδικασίας θωράκισης ενός συστήματος έχει να κάνει με τον έλεγχο πρόσβασης. Αυτό είναι και το αντικείμενο του κεφαλαίου 6 του 134.
  - Ποιός έχει πρόσβαση στο σύστημα;
  - Τι είναι προσβάσιμο στο σύστημα και απο κάποιον/κάποιους;
  - Τι σημαίνει πρόσβαση;
    - Απο ποιόν;
    - Σε τι βάθος γίνεται η πρόσβαση;
    - Απο τι;

Οι δύο τρόποι ελέγχου πρόσβασης

Σε ένα λειτουργικό σύστημα (διανομή) Linux υπάρχουν δύο μηχανισμοί ελέγχου πρόσβασης, **χωρίς να αποκλείει ο ένας τον άλλον**:

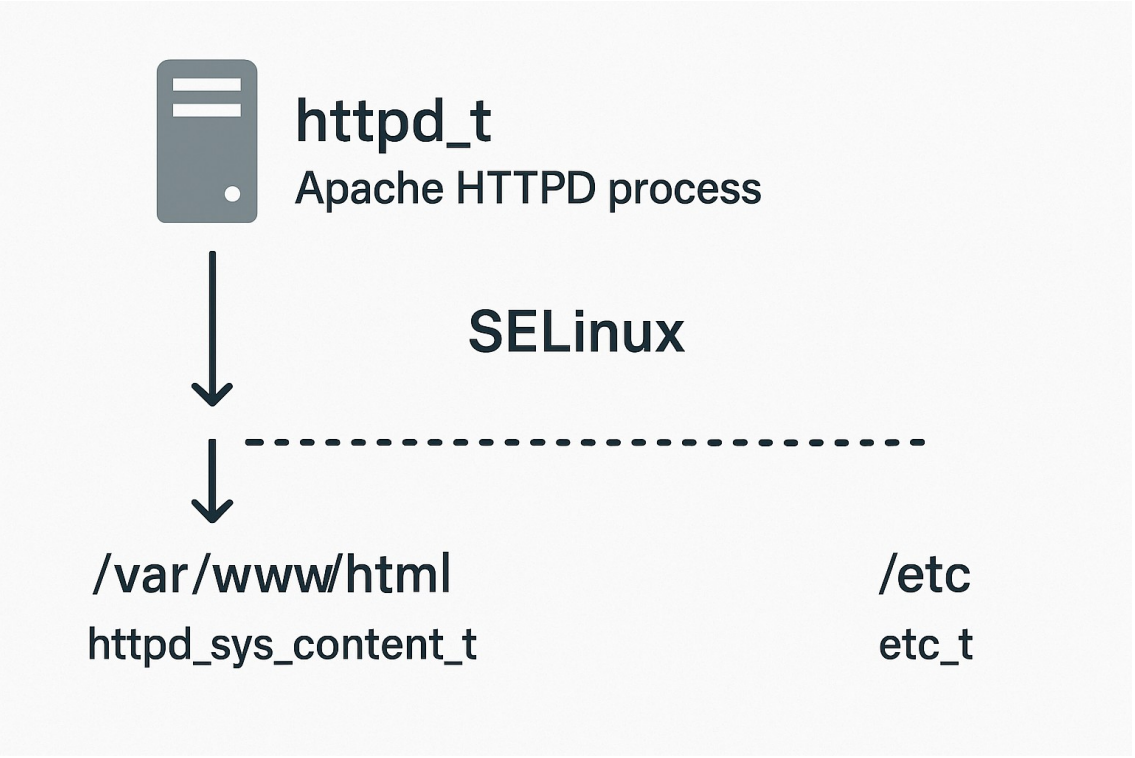
- Mandatory Access Control (Υποχρεωτικός Έλεγχος Πρόσβασης)
  - Οι κανόνες/μηχανισμοί του ιεραρχούνται πιο πάνω απο κανόνες που προέρχονται απο τη θέληση/κρίση των χρηστών του συστήματος
  - Πιο ισχυρότερος και κεντρικότερος μηχανισμός πρόσβασης ελέγχου σε σχέση με το Διακριτικό Έλεγχο Πρόσβασης
  - Συναντάται συνήθως σε συστήματα στρατιωτικών/τραπεζικών ή υποδομών που πρέπει να διατηρούν λειτουργική αξιοπιστία
- Discretionary Access Control (Διακριτικός Έλεγχος Πρόσβασης)
  - Ο χρήστης μπορεί να καθορίζει το επίπεδο πρόσβασης σε σημεία του συστήματος.
  - Λιγότερο ισχυροί και πιο αποκεντρωμένοι κανόες, ο κάθε χρήστης για παράδειγμα μπορεί να καθορίζει ποιος θα έχει πρόσβαση στα δικά του αρχεία.
  - Συναντάται σε συστήματα που δεν έχουν υψηλές ανάγκες ασφάλειας και αξιοπιστίας.

Οι δύο τρόποι ελέγχου πρόσβασης (Παραδείγματα)

- **Παράδειγμα 1**: Ο χρήστης georgios ορίζει οτι ο home φακελός του θα είναι απολύτως προσβάσιμος απο τον ίδιο, μόνο αναγνώσιμος απο το group ‘engineers’ και για όλους τους άλλους δεν πρέπει να είναι προσβάσιμος. (chown georgios:georgios /home/georgios; chmod 750 /home/georgios) → Discretionary Access Control

- **Παράδειγμα 2**: Οτιδήποτε βρίσκεται εκτός του φακέλου ‘/var/www’ ΔΕΝ πρέπει να είναι προσβάσιμο απο το Apache Web Server process, ακόμα και αν ο χρήστης κάτω απο τον οποίο τρέχει ο Apache Web server έχει πρόσβαση σε αυτό με βάση τα permissions του συστήματος αρχειοθέτησης. → Mandatory Access Control

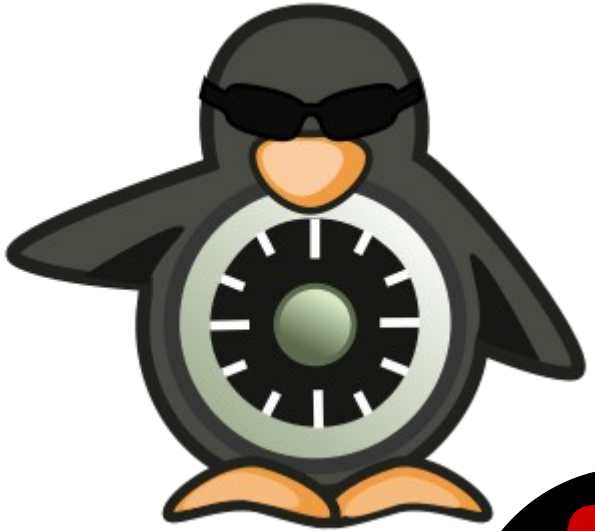
Mandatory Access Control



- **<u>Συζήτηση:</u>** Θα ήταν φρόνιμο ο Apache να μπορεί να γράψει και να διαβάσει κάτω απο το /etc?

- Χρησιμοποιεί κανόνες (policies) για να περιγράψουν
  - Την επιτρεπόμενη πρόσβαση σε ένα resource (αρχείο, socket, κτλ)
  - Βάζει ετικέτες labels στα resources για να τα διαχωρίζει
  - Δεν αναφέρεται στο ποιος αλλά κυρίως στο ποιό πρόγραμμα τρέχει
- Στόχος είναι να περιορίσουμε ΠΡΟΛΗΠΤΙΚΑ αλλά αποτελεσματικά την πρόσβαση
- Παίρνεις πρόσβαση σε αυτό που χρειάζεται. Τίποτα περισσότερο και τίποτα λιγότερο.

SELinux



- Δωράκι του NSA των ΗΠΑ στην κοινότητα του ανοιχτού λογισμικού με ύστερη συμμετοχή και εταιριών όπως η Redhat και άλλες.
- Όχι δε σας κατασκοπεύει, ο πηγαίος του κώδικας είναι πλέον μέρος του πυρήνα Linux απο το 2003 και είναι ορατός σε όλους.
- Επιβάλλει μηχανισμούς ελέγχου προσβασιμότητας, κυρίως μέσω Mandatory Access Control αλλά όχι μόνο.
- Έμφαση στο διαχωρισμό μεταξύ της περιγραφής των κανόνων (security policies) και του τρόπου επιβολής.
- Τα προνόμια πρόσβασης αποδίδονται εκεί που χρειάζονται με στόχο να εξαλείψουμε προβλήματα που έχουν να κάνουν με τους περιορισμούς των DAC, setuid/setgid, buffer overflows και άλλων προβλημάτων ασφαλείας.

Ερωτήσεις