Сигурност в UNIX операционни системи

1. UNIX Oses

- Кратка история, основни идеи
  - Много малки програми, small is beautiful
  - multitasking (многозадачна)
  - multiuser (многопотребителска)
  - portable (преносима)

- Архитектура
  - Kernel
    - Управление на hardware
    - Управление на паметта
    - Управление на процесите
    - kernel modules

- User space
  - Unix Shell
  - Daemons
  - Безброй малки програмки

2. Преглед на механизмите за сигурност в Unix Oses

- Потребители
  - UID, GID, Additional groups
  - Special users / root (UID == 0)

- Процеси
  - Обяснение какво е process
    - Идеи за thread и daemon

    RUID, RGID - реални UID и GID на потребителя, който е стартирал процеса

    EUID, EGID - ефективни UID и GID използвани от процеса (освен за достъпа до файловата ситема) (!!???!!)

    SUID, SGID - запазени UID и GID; използват се за “включване и изключване” на привилегии. Не се поддържат от всички UNIX-и.

    supplemental groups (допълнителни групи) – списък с групи, в които участва процеса (добавено като възможност в BSD).

    umask – Определя правата на създаваните от процеса файлове, обяснява се по-подробно в частта за файловата система.

    scheduling parameters – Параметри за scheduling на процеса
    - Идеята за scheduler
    - Приоритет (nice) и scheduling policy

    limits – Лимити на ресурсите, използвани от процеса
    - Hard и Soft лимити
    - Примерни лимити – брой процеси, заемана памет, използвано време на процесора

    filesystem root – Къде за почва файловата система за процеса, chroot(2)

- Други атрибути

  FSUID, FSGID - UID и GID използвани за достъп до файловата система, по принцип същите като EUID и EGID. Специфично при Linux.

  capabilities - POSIX capability information – ограничения на правата на UID0 за различни процеси

3. Файлова система

- Обекти
  - файлове
  - директории
  - символни връзки (symbolic links)
  - FIFOs (named pipes)
  - sockets
  - devices

- Атрибути
  - UID и GID на притежателя (само root потребителя може ги промени)

  - permission bits (read, write, execute) за всеки един от (owner, group, other)
    - кратко обяснение за осмична бройна система, кой bit как се смята
    - rwxr-xr-x == 755

      При директориите правата за четене са нужни, за да се види списък на елементите в директорията, докато правата за изпълнение дават право за “търсене” и са нужни за влизане в директорията. Правата за писане ни позволяват да трием, местим и създаваме файлове в нея.

  - sticky bit (+t)
    - Когато е зададен за директория, изтриванията и преименуванията в директория са позволени само за притежателя на файла, притежателя на директорията, или root. Използва се за tmp.

  - setuid, setgid (u+s, g+s)

  - timestamps (access time, modify time, creation time)

- Специфични атрибути

  - Immutable bit
  - Append only bit

  - ACLs

- Quota

4. IPC

- POSIX & SYSV IPC
  - PIPOs и FIFOs
  - File locking
    - Advisory
    - Mandatory

  - Semaphores
  - Shared memory
  - Message queues

- Signals
  - Права за изпращане на сигнали
  - Специфични сигнали
    - SIGTERM, SIGINT
    - SIGKILL
    - SIGSTOP, SIGCONT
    - SIGURG

5. Authentication

- Потребители и пароли
  - /etc/passwd
  - /etc/shadow

- BSD вариации по темата

- PAM

6. Auditing
    - syslogd
    - wtmp, utmp, lastlog
7. Security Extensions
    - Jail (Linux vservers, *BSD)
    - Usermode linux
8. Generic атаки
    - /tmp race conditions (symlink attacks)
    - атаки върху SUID файлове
    - разбиване на hash-ове на пароли