Механизми за сигурност в UNIX OSes

Представена от Георги Чорбаджийски
http://georgi.unixsol.org/
georgi@unixsol.org

и Васил Колев
http://vasil.ludost.net/
vasil@ludost.net

базирана на лекция водена в курса по
Мрежова сигурност във ФМИ
http://nedyalkov.com/security/

Механизми за сигурност в UNIX OSes

- UNIX Oses
  - многозадачна, многопотребителска, преносимост
- Архитектура
  - kernel space, user space
- Механизми за сигурност
  - Потребители
  - Процеси
  - Файлова система
  - Сигнали
  - Authentication
  - Auditing
  - Limits
  - Security extensions

Механизми за сигурност в UNIX OSes

- Потребители
  - User identifiers (UID)
  - Group identifiers (GID)
  - Допълнителни групи (additional groups)
  - Специални потребители
    - root
    - UID == 0

Механизми за сигурност в UNIX OSes

- Процеси
  - Идентификатори
    - RUID/RGID
    - EUID/EGID
    - SUID/SGID
  - Supplemental groups
  - umask
  - resource limits
  - scheduling parameters
  - fs root

Механизми за сигурност в UNIX OSes

- Обекти във файловата система
  - директории
  - файлове
  - символни връзки (symbolic links)
  - устройства
  - FIFOs (named pipes)
  - sockets

Механизми за сигурност в UNIX OSes

- Атрибути на обектите във файловата система
  - собственик (UID, GID)
  - Права за достъп
    - четене, писане, изпълнение (rwx)
    - собственик, група, други
  - Специални атрибути
    - SetUID (u+s), SetGID (g+s)
    - Sticky bit (+t)
    - timestamps (access time, modify time, creation time)
  - Специфични за Линукс
    - Immutable, appned only, ACLs

Механизми за сигурност в UNIX OSes

- Сигнали
  - Кой може да ги праща?
  - SIGURG
  - SIGTERM
  - SIGKILL
  - SIGSTOP, SIGCONT

Механизми за сигурност в UNIX OSes

- Authentication
  - Потребители и пароли
    - /etc/passwd
    - /etc/shadow
    - BSD вариации по темата
  - PAM
  - NIS, NIS+

Механизми за сигурност в UNIX OSes

- Auditing
  - syslogd
  - wtmp
  - utmp
  - lastlog

Механизми за сигурност в UNIX OSes

- Security extensions
  - Jail
  - Usermode Linux
  - SELinux / LSM

Механизми за сигурност в UNIX OSes

Въпроси?

Механизми за сигурност в UNIX OSes

Благодаря за вниманието!