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

Съдържание

- Какво е UNIX?
  - История
  - Функционалност
  - Архитектура
- Механизми за сигурност
  - Потребители
  - Процеси
  - Файлова система
  - IPC
  - Сигнали
  - Authentication
  - Auditing
  - Limits
  - Security extensions
- Стандартни атаки

UNIX

- Кратка история
- Основни функционалности
  - Многозадачна
    - Preemtive vs. Cooperative multitasking
  - Многопотебителска
  - Преносима (portable)
- Архитектура
  - Kernel space
  - User space

Потребители

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

Процеси

- Идентификатори
  - RUID/RGID
  - EUID/EGID
  - SUID/SGID
- Supplemental groups
- umask
- Resource limits
- Scheduling parameters
- fs root – See chroot(2)
- Специфични
  - capabilities

Обекти във файловата система

- Директории
- Файлове
- Символни връзки (symbolic links)
- Твърди връзки (hard links)
- Устройства
- FIFOs (named pipes)
- Sockets

Атрибути на обектите

- 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
  - Immutable
  - Append only
  - ACLs

IPC

- Заключване на файлове
  - Advisory
  - Mandatory
- Semaphores
- Shared memory
- Message queues

Сигнали

- Какво са сигналите?
- Кой може да ги праща?
- Специфични сигнали
  - SIGTERM
  - SIGKILL
  - SIGSTOP, SIGCONT
  - SIGURG

Authentication

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

Ограничения

- Квоти
  - Групи
  - Потребители
- Лимити

Auditing

- syslogd
- wtmp
- utmp
- lastlog

Security extensions

- Linux
  - Capabilities
  - Linux Security Modules (LSM)
    - SELinux
    - BSDJail
  - Linux-VServer
  - GRSec
- BSD
  - Jail

Стандартни атаки

- /tmp race conditions (symlink attacks)
- Атаки върху SUID файлове
- Атаки върху /etc/passwd

Въпроси?

Сега е момента да питате...

Това е краят

Благодаря за вниманието!