Вопросы к экзамену по курсу Безопасность Операционных Систем
январь 2026

Физическая безопасность сервера на базе ОС Linux

1. Сброс пароля пользователя ОС Linux: Single User Mode и внедрение в ход загрузки ОС. Оболочки `/sbin/sushell` и `/sbin/sulogin`.
2. Способы защиты от сброса пароля пользователя ОС Linux.
3. Прозрачное шифрование дисков и файловых контейнеров. Служба `dm-crypt` и подсистема LUKS.

Управление и безопасность УЗ пользователя в ОС Linux

4. Пользователи в ОС Linux. Файл паролей `/etc/passwd` и теневой файл паролей `/etc/shadow`, их структура и назначение.
5. Группы пользователей в ОС Linux. Назначение групп пользователей, файл `/etc/group`.
6. Хранение паролей в ОС Linux. Структура записи хэша пароля. Виды алгоритмов хэширования паролей.
7. Система подключаемых модулей аутентификации (Pluggable Authentication Module, PAM). Основные компоненты архитектуры PAM и их назначение. Типичное расположение модулей и конфигурационных файлов в ОС Linux.
8. Конфигурация системы PAM для конкретного сервиса. Формат конфигурационного файла PAM, группы управления и контрольные флаги (сокращённая и подробная форма).
9. Исполнение сценария PAM: порядок запуска модулей, обработка результатов исполнения модулей. Понятие стека модулей.
10. Типичная конфигурация подсистемы аутентификации и авторизации ОС Linux на примере ОС Ubuntu 24.04.
11. Реализация классической модели парольной аутентификации Unix (с помощью файлов `/etc/passwd` и `/etc/shadow`) в ОС Linux средствами системы PAM.
12. Способы блокировки пользователей средствами системы PAM.
13. Конфигурация парольной политики средствами системы PAM.
14. Поддержка аутентификации и авторизации в собственных приложениях средствами системы PAM: программный интерфейс и конфигурация сценария.

Механизмы разграничения доступа ОС Linux

15. Классическая модель разграничения доступа Unix. Триплеты прав, расширенные права доступа (`sticky bit`, `SUID`, `SGID`).
16. Файловые списки управления доступом (Access Control List, ACL, `facl`). Назначение, типы списков, примеры использования.
17. Атрибуты файла (file attributes). Назначение, основные типы атрибутов. Примеры использования атрибутов `append only`, `immutable` и `secure deletion`.
18. Идентификаторы пользователя и группы запущенного процесса (`real`, `effective`, `saved IDs`). Алгоритм определения права доступа к объекту ОС Linux.

19. Эффект битов SUID и SGID исполняемого файла на значения идентификаторов процесса. Назначение setuid-root программ. Написание защищённых привилегированных приложений: концепция защищённого программирования, secure programming.
20. Linux Capabilities. Назначение, типы разрешений. Механизмы работы с привилегиями.

Разграничение ресурсов и изоляция процессов ОС Linux

21. Контроль выделенных пользователю ресурсов средствами системы ulimit. Основные типы ресурсов, hard и soft лимиты. Управление лимитами ресурсов с помощью команды ulimit.
22. Управление лимитами ресурсов средствами системы PAM.
23. Механизм chroot: назначение, принцип работы, примеры использования.
24. Механизм seccomp: назначение, принцип работы, примеры использования.
25. Механизм пространств имён namespaces. Назначение, типы пространств имён, способы создания. Примеры использования пространств имён.
26. PID namespace: назначение, принцип работы, способы создания и примеры использования.
27. NET namespace: назначение, принцип работы, способы создания и примеры использования.
28. MOUNT namespace: назначение, принцип работы, способы создания и примеры использования.
29. Механизм cgroup v2, его назначение. Основные компоненты архитектуры системы: понятие контрольной группы и контроллера, интерфейс системы cgroup. Принцип единой иерархии контрольных групп.
30. Создание новой контрольной группы. Файлы cgroup.controllers и cgroup.subtree_control, их назначение. Добавление процессов в контрольную группу, файл cgroup.procs.
31. Настройка лимитов потребления CPU и привязка к подмножеству ядер (например, NUMA-узлу) группы процессов средствами системы cgroup.
32. Настройка лимитов потребления RAM и операций ввода-вывода (I/O) группы процессов средствами системы cgroup.

Безопасность процессов ОС Linux

33. Переполнение на стеке: источники уязвимости, типичные способы эксплуатации. Понятие шелл-код, его назначение.
34. Return oriented programming. Назначение техники эксплуатации, понятие гаджета и ROP-цепочки.
35. Уязвимость форматной строки: источники уязвимости, типичные способы эксплуатации.
36. Предотвращение исполнения данных (Data Execution Prevention, DEP). Назначение механизма защиты, способы реализации (аппаратные и программные).
37. Рандомизация адресного пространства (Address Space Layout Randomization, ASLR). Назначение механизма защиты, способы реализации.
38. Позиционно-независимый код/исполняемый файл (Position-Independent Code, PIC, также Position-Independent Executables, PIE), его назначение.

39. Защита от переполнения на стеке (Stack Smashing Protector, SSP). Назначение механизма защиты, способы реализации.
40. Понятие безопасного стека, принцип разделения стека. Механизм LLVM/Clang Safe Stack.
41. Контроль целостности потока исполнения (Control-Flow Integrity, CFI). Реализация CFI в LLVM/Clang.
42. Контроль целостности потока исполнения (Control-Flow Integrity, CFI). Механизм Intel Control-flow Enforcement Technology (CET).