-Анализ Linux утилит ( функционирование утилиты, пример её использование, применение, форматы, профилирование, исходный код утилиты – из исходного кода ОС выделить (ОС с исходным кодом, провести декомпозицию кода, предоставить структуру кода декомпозита), состав и порядок системных вызовов strace ptrace. Отладочные дириктивы вставить в код. Восстановить алгоритм функционирования, трассировка, снабдить код собственными комментариями, берем исходный код, делаем копию и нумеруем все строки, чтобы они были привязаны к инструкциям, при декомпозиции поверх кода, содержащего оригинал. Обращается ли утилита к ядру при своей работе, с какими структурами данных она работает, либо берет информацию из файлов, псевдофайловая система prog – соответсивие pid процессам, к которым обращается. Модификация кода утилиты, выборка тогоЮ что получилось в результате анализа. Либо методом исключения. Утилита df – презентация об утилите, функционирование на уровне пользователя, трассировку сделать, какие вызовы используются и показать исходный код. А потом начать заниматься декомпозицией. Находим исхоный код, скачиваем файл,

Мониторинг обращения к заданному файлу

Мониторинг деятельности пользования

Журналирование запуска файлов

Утилита аналтза типов файлов

Реестр

Организация обращения к файлам по паролю

Отладчик на api

Ограничение доступа пользования к порту и переферийным устройствам

Утилита сбора

Блокировка запуска приложений

++++++++++++++Анализ аппаратного состава компьютера c драйверами и тд

Аналог утилиты nm