Лекция 15
Особенности реализации системы безопасности в ОС Windows

Практическое задание по лекции

Используя учебный материал лекции, составьте терминологический словарь, состоящий по объему из 20 терминов и определений.

1. Аутентификация пользователя: Процесс проверки подлинности и идентификации пользователя для предоставления доступа к системе или ресурсу.
2. Системный аудит: Процесс мониторинга и регистрации действий и событий в компьютерной системе или сети.
3. Защита от повторного использования объектов: Мера безопасности, направленная на предотвращение несанкционированного использования или доступа к объектам после их первичного использования.
4. Внешнее навязывание: Техника злоумышленников, при которой они заставляют пользователя выполнить нежелательные действия или раскрыть конфиденциальную информацию.
5. Контекст пользователя: Совокупность параметров и настроек, определяющих условия и ограничения, в которых пользователь взаимодействует с компьютерной системой.
6. Выявление вторжений: Процесс обнаружения и регистрации попыток несанкционированного доступа или аномального поведения в компьютерной системе с целью защиты от взлома и нарушений безопасности.
7. Аудит: Систематическая регистрация и анализ событий, происходящих в компьютерной системе, включая входы и выходы из системы, операции с файлами, обращения к удаленным системам и изменения привилегий или атрибутов безопасности.
8. Дескриптор безопасности: Структура данных, содержащая информацию о безопасности объекта в операционной системе, включая права доступа, привилегии и список аудита (SACL).
9. Security Access Control List: Список контроля доступа, содержащий перечень пользователей, чьи попытки доступа к объекту подлежат аудиту.

10. Журнал событий безопасности: Хранилище системных записей, содержащих информацию о событиях безопасности, произошедших в компьютерной системе, включая информацию об аудите доступа к файлам и другим действиям пользователей.
11. Повторное использование объектов: Процесс использования ранее освобожденных объектов системы, таких как память и файлы.
12. Безопасность повторного использования: Гарантированная системой мера для предотвращения несанкционированного доступа к ранее использованным объектам путем проинициализации и очистки этих объектов перед выделением их новому пользователю.
13. Windows File Protection: Механизм защиты файлов в операционной системе Windows, который предотвращает изменения системных файлов
14. Sfc.exe (System File Checker): Утилита в операционной системе Windows, позволяющая проверить корректность версии всех системных файлов и обнаружить неподписанные файлы.
15. Principle of Least Privilege - принцип безопасности, рекомендующий выполнение операций с минимальным набором привилегий, необходимым для достижения требуемого результата.
16. AdjustTokenPrivileges - функция в ОС Windows, которая позволяет включать и отключать определенные привилегии в маркере доступа.
17. Impersonation - процесс, при котором один поток процесса функционирует с маркером доступа, отличным от маркера текущего процесса.
18. DuplicateTokenEx - функция в ОС Windows, которая позволяет создать дубликат существующего маркера доступа с заданными правами доступа и уровнем перевоплощения.
19. Impersonation Level: Параметр маркера доступа, определяющий уровень доверия и возможности имперсонации потока процесса.
20. Restricted Token: Маркер доступа, созданный с помощью функции CreateRestrictedToken, в котором можно внести изменения, такие как удаление привилегий, отключение SID-идентификаторов и добавление "ограниченных" SID'ов учетных записей.