Практическая работа №15

*Выполнил Шардт М.А.*

1. Задание 1
   1. Что такое SAS и для чего она используется?
   2. Какая программа управляет процедурой аутентификации пользователя?
   3. Что такое GINA и как она взаимодействует с процессом WinLogon?
   4. Какая системная функция используется для аутентификации пользователя?
   5. Что такое аудит и для чего он используется в системах защиты?
   6. Что такое SACL и как он используется для регистрации событий в журнале аудита?
   7. Что такое повторное использование объектов и для чего нужна их очистка перед выделением новому пользователю?
   8. Что такое PFN и как он используется для обеспечения безопасности повторного использования областей физической памяти?
   9. Что такое Windows File Protection и как она защищает системные файлы от изменений со стороны пользователя с административными правами?
   10. Что такое Sfc.exe и SigVerif.exe и для чего они?
2. Задание 2
   1. SAS (Secure Attention Sequence) - комбинация клавиш "ctrl+alt+del", используемая для инициации процедуры аутентификации пользователя в Windows.
   2. GINA (Graphic Identification aNd Authentication) - графическая библиотека идентификации и аутентификации, которая взаимодействует с процессом WinLogon для аутентификации пользователя.
   3. LogonUser - системная функция, используемая для аутентификации пользователя в Windows и возвращающая указатель на маркер доступа пользователя.
   4. Аудит - регистрация специальных данных о различных событиях, происходящих в системе и влияющих на состояние безопасности компьютерной системы.
   5. SACL (System Access Control List) - список, содержащий информацию о пользователях, чьи попытки доступа к объекту должны быть зафиксированы в журнале аудита.
   6. Повторное использование объектов - процесс, когда объект, ранее использованный одним пользователем, может быть использован другим пользователем без предварительной инициализации и очистки.
   7. PFN (Page Frame Number) - база данных, хранящая информацию о страницах физической памяти в ОС Windows.
   8. Windows File Protection (WFP) - средства защиты файлов в ОС Windows, которые защищают системные файлы от изменений со стороны пользователя с административными правами.
   9. Sfc.exe (system file checker) - утилита в ОС Windows, которая позволяет проверить корректность версии всех системных файлов.
   10. SigVerif.exe - утилита в ОС Windows, которая позволяет проверить подпись системных файлов и выявить неподписанные файлы.
   11. Маркер доступа - объект, создаваемый при интерактивном входе пользователя в систему, который хранит сведения о контексте пользователя и используется для контроля доступа к ресурсам.
   12. LSA - процесс в операционной системе Windows, ответственный за аутентификацию пользователей и создание маркеров доступа.
   13. AdjustTokenPrivileges - функция API в операционной системе Windows, используемая для включения и отключения определенных привилегий в маркере доступа.
   14. CreateProcessAsUser - функция API в операционной системе Windows, используемая для запуска нового процесса с указанным маркером доступа.
   15. Impersonation - процесс выполнения кода с маркером доступа, отличным от маркера данного процесса.
   16. Протокол – набор соглашений, заключенных между пользователями компьютерных сетей, в которых оговариваются технические параметры устройств и программные средства для организации приёма и передачи информации в этих сетях
   17. Сервер – это программное или аппаратное устройство, которое принимает и отвечает на запросы, сделанные по компьютерной сети
   18. Пароль – условное слово или произвольный набор знаков, состоящий из букв, цифр и других символов, и предназначенный для подтверждения личности или полномочий
   19. Аудит информационной безопасности – системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности автоматизированной системы в соответствии с определенными критериями и показателями безопасности
   20. Субъекты безопасности – любая сущность, которую может проверить операционная система, например учетную запись пользователя, учетную запись компьютера, поток или процесс, выполняемый в контексте безопасности учетной записи пользователя или компьютера