Наблюдение за параметрами безопасности системы

Архитектура и безопасность Windows сетей

Севрюков С.Ю.

Уровень рабочей станции

Наблюдение за системой

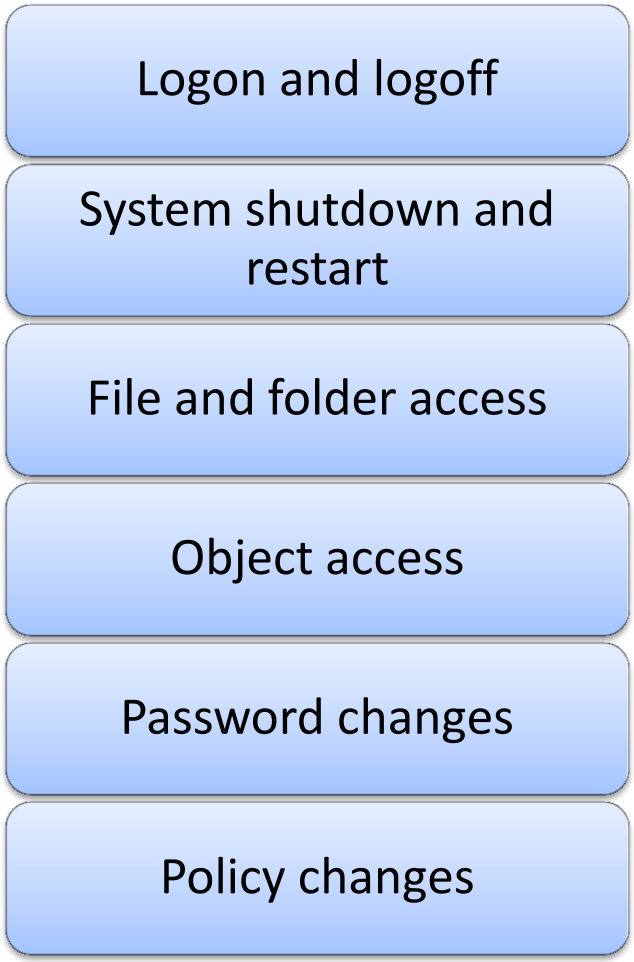
- Системный монитор
- Системный аудит
- Сетевые подключения к общим ресурсам

Уровень домена

Мониторинг сети и ресурсов

- Сбор логов
- Анализ логов
- Оповещения

Основные события аудита



Порядок действий

- Включить аудит
- Настроить аудит
- Сопровождать систему аудита
- Настраивать оповещения
- Разработать регламенты реагирования
- Реагировать на события

Средства

- Журналы событий и Event Viewer
- Log parser
- Анализаторы

Журналы событий

Интенсивность заполнения журнала

- **Генерация уведомления администратору при заполнении журнала**
- HKLM\SYSTEM\CurrentControlSet\Services\Alerter\Parameters
- Параметр AlertNames указывает имя получателя сообщения

График просмотра журнала

График архивация журнала для отслеживания тенденций

Разрешение на файл журнала

Политика безопасности для аудита

*Set Maximum * Log Size*

- По умолчанию 512 Kb, максимальный размер 4 Gb (4,194,240 Kb)

*Restrict Guest Access to the * Log*

- Запрещает анонимный доступ к журналу

*Retain * Log*

- Определяет срок жизни события в журнале

*Retention Method for * Log*

- Механизм перезаписи журнала

Shutdown the computer when the security audit log is full

- Остановка системы при заполнении журнала безопасности

Системный аудит - DEMO

- Настройка аудита
  - Состав политики
    - Конфигурация аудита
    - Административные шаблоны
  - Работа с журналами
    - Оснастка Event Viewer
    - Журналы Windows
    - Фильтрация и представления
    - Примеры событий и их анализ
- Log Parser
  - Установка Log parser и Log parser Lizard
  - Запуск программ
  - Log parser
  - Log parser Lizard
  - Дополнительные возможности Log parser Lizard (графики, управление скриптами)

Управление общим доступом

- Инструменты
  - Оснастка Общие папки
  - Windows Explorer
  - Утилиты командной строки
    - NET SHARE
    - NET SESSION
    - NET FILE

Рекомендуемые ресурсы

- Аудит
  - Advanced Security Audit Policy Settings
  - Active Directory: изменения в системе аудита
- Инструменты анализа
  - Log parser
    - Анализ журналов с помощью LogParser
  - Log parser Lizard
  - Log Parser Studio
- Мониторинг
  - Более 60 инструментов для мониторинга Windows
  - Более чем 80 средств мониторинга системы Linux
- Управление общими папками
  - Управление общими папками
  - Общие папки - раздел документации

Задайте свой вопрос

http://bit.ly/ask4me