МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ "ЛЬВІВСЬКА ПОЛІТЕХНІКА"

КАФЕДРА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ



*Звіт*

до лабораторної роботи № 4 на тему:

"**АУДИТ І НАЛАШТУВАННЯ БЕЗПЕКИ У WINDOWS XP** "

з дисципліни:*"Основи системного адміністрування"*

**ВИКОНАВ:**

Середа І.С.

ПЗС 11

**ПЕРЕВІРИВ:**

доц. Яковина В.С.

Львів – 2014

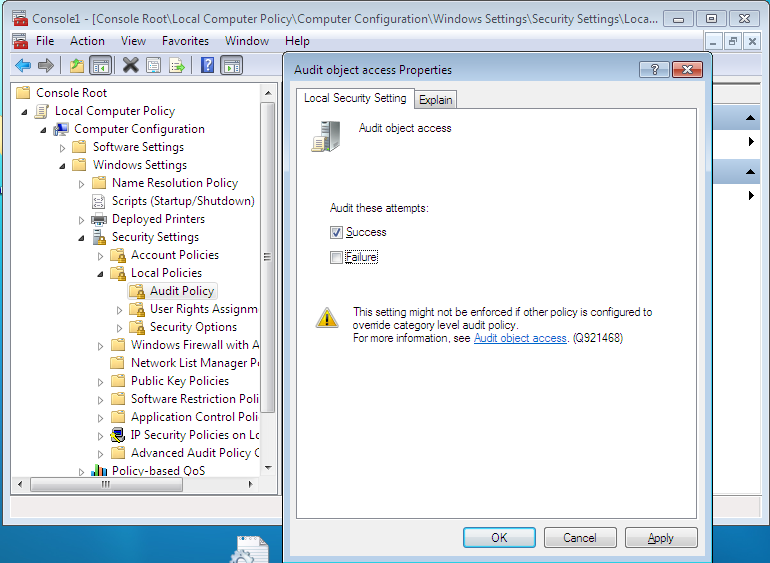
**Мета роботи:** Ознайомлення зі структурою, принципом роботи та налаштуванням об’єкта групової політики на локальному комп’ютері під управлінням ОС Windows XP. Навчитись використовувати та створювати шаблони безпеки для ефективного налаштування та аналізу типових параметрів безпеки.

**Завдання до виконання роботи**

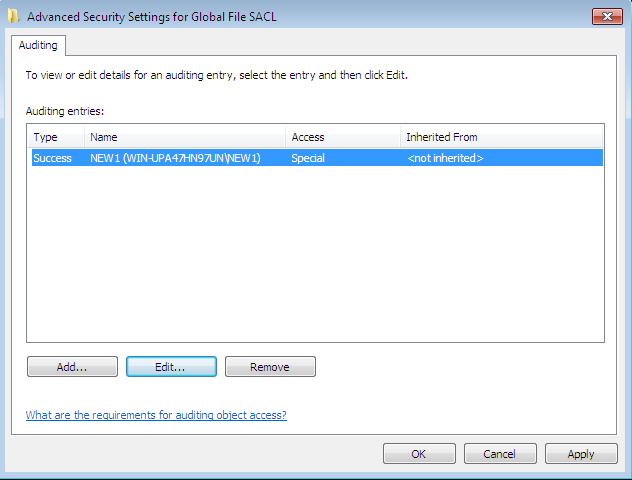
1. Відкрити оснастку mmc "Групповая политика". Перейти в гілку "Политика аудита", включити аудит доступу до об’єктів. Після цього у властивостях безпеки об’єкту, за яким повинно проводитись спостереження (папки чи файлу), перейти у вкладку "Аудит" та увімкнути аудит для визначених суб’єктів безпеки та їх активності (наприклад видалення). (Переконатись, що без налаштування аудиту на об’єкті файлової системи записів в журнал не відбувається – п. 2.) Виконати умови аудиту (тобто дії над цим об’єктом та тим користувачем для яких налаштовано аудит).
2. Відкрити оснастку mmc "Просмотр событий" та журнал "Безопасность" в ній. Знайти в журналі записи категорії "Доступ к объектам" та записи про дію, яку контролювалося. (Додаткові відомості про подію за номером її коду (ID) можна знайти на сайті Microsoft або в Resource Kit).
3. В політиках аудиту увімкнути аудит зміни політики та системних подій. Виконати умови аудиту (наприклад змінити системний час). В журналі безпеки відстежити записи про ці події. Увімкнути аудит управління обліковими записами користувачів; відключити обліковий запис існуючого користувача, створити нового користувача, задати пароль користувачу. В журналі безпеки відстежити записи про ці події. Увімкнути аудит входу в систему; вийти зі системи та зайти під іншим користувачем. В журналі безпеки знайти записи категорії "Вход/Выход" та відстежити записи про ці події.
4. В контекстному меню журналу безпеки вибрати пункт "Свойства". Задати якнайменший розмір журналу та політику "Не затирать события". Після цього в редакторі об’єкту групової політики (гілка "Параметры безопасности") включити параметр політики "Аудит: немедленное отключение системы, если невозможно внести в журнал записи об аудите безопасности". Заповнити журнал аудиту увімкнувши політики та виконавши достатню кількість дій, що підлягають аудиту. Якщо це виконувалось користувачем з адміністративними повноваженнями, спробувати увійти в систему як звичайний користувач. Переконатись у неможливості входу в систему через переповненість журналу аудиту. Увійти як адміністратор; вимкнути увесь аудит. В контекстному меню журналу безпеки вибрати пункт "Стереть все события" для очищення журналу. Чи усі події вдалося видалити? Чи з’явились нові записи?

**Результат виконання завдань:**

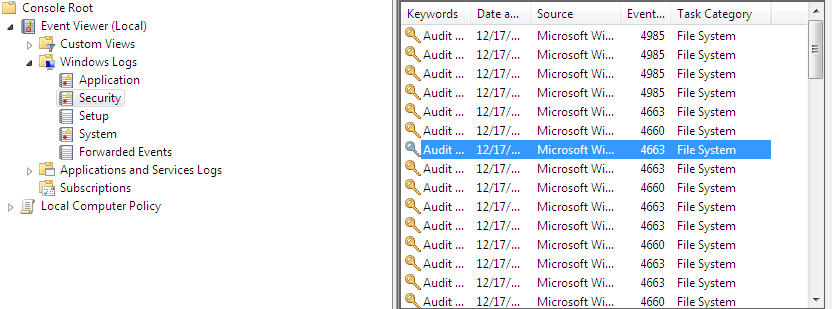
**1.** Відкриваємо оснастку mmc "Групповая политика". Переходимо в гілку "Политика аудита" , включаємо аудит доступу до об’єктів

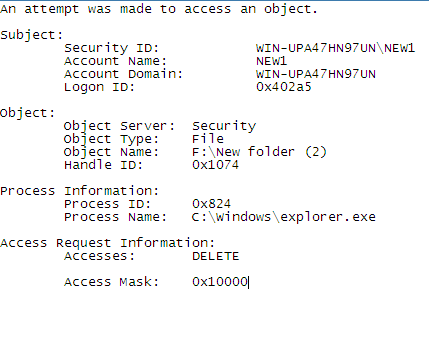


Після цього у властивостях безпеки об’єкту, за яким повинно проводитись спостереження (папки чи файлу), переходимо у вкладку "Аудит" та вмикаємо аудит для користувача new1 виконання та видалення файлів.

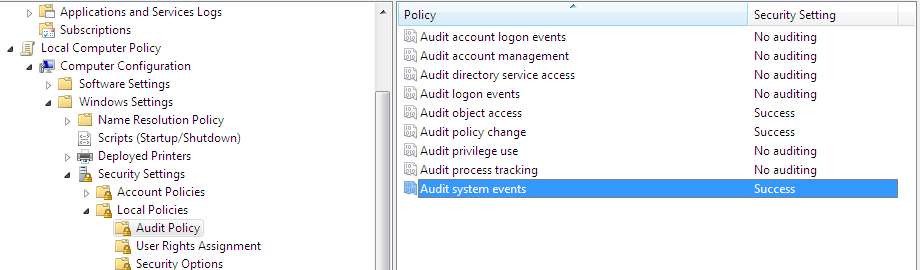


2.Відкриваємо оснастку mmc "Просмотр событий" та журнал "Безопасность" в ній. Знаходимо в журналі записи категорії "Доступ к объектам" та записи про дію, яку контролювалося.

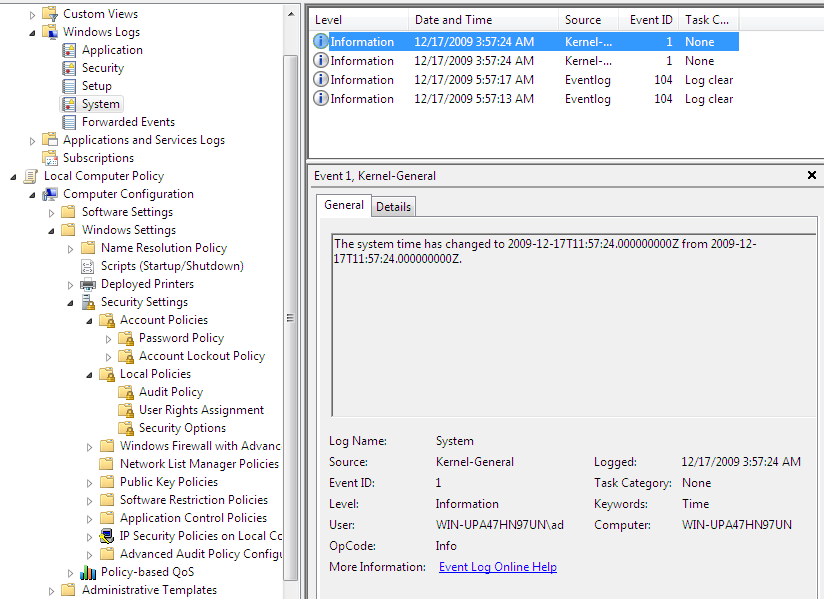




3. В політиках аудиту вмикаємо аудит зміни політики та системних подій.

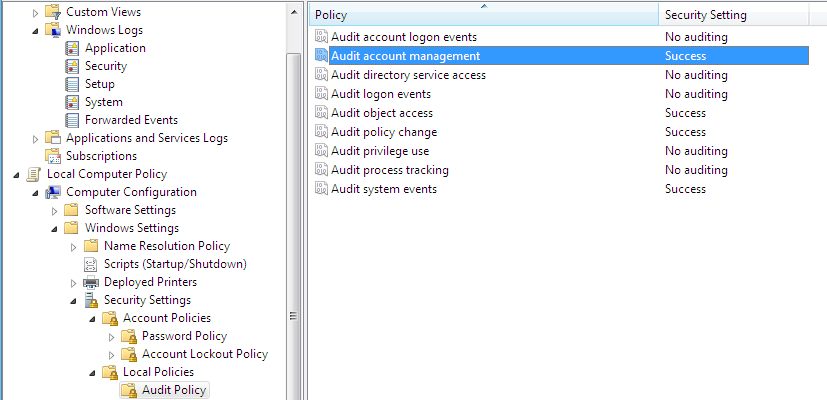


Змінив системний час. В журналі безпеки відстежуємо записи про ці події.

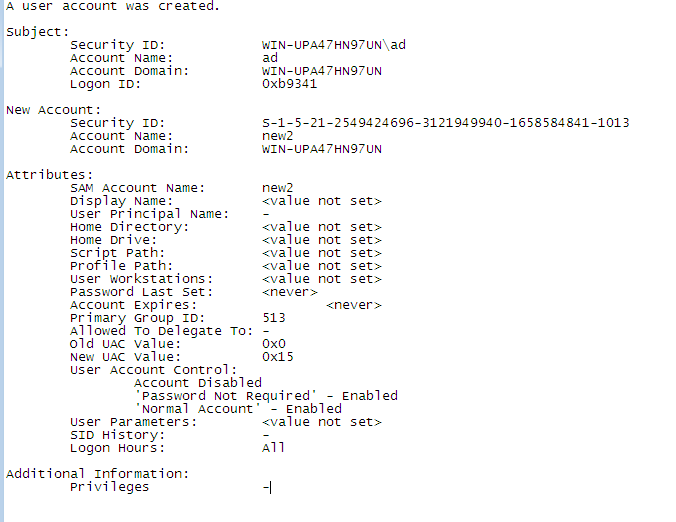


Вмикаємо аудит управління обліковими записами користувачів. відключаємо обліковий

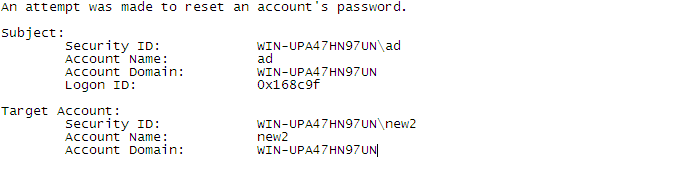
запис існуючого користувача.



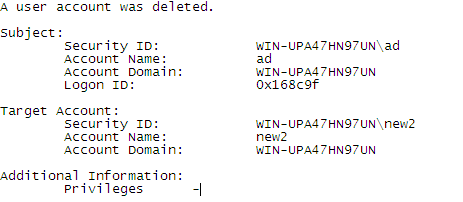
Після створення нового користувача в журналі буде запис:



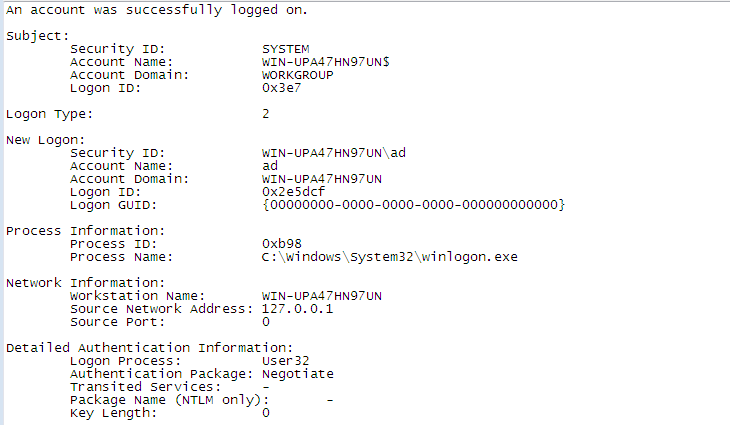
Після зміни паролю обліковому запису new2 в журналі отримуємо такий запис:



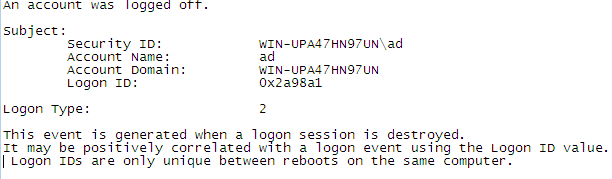
Видаливши обліковий запис отримаємо наступний запис:



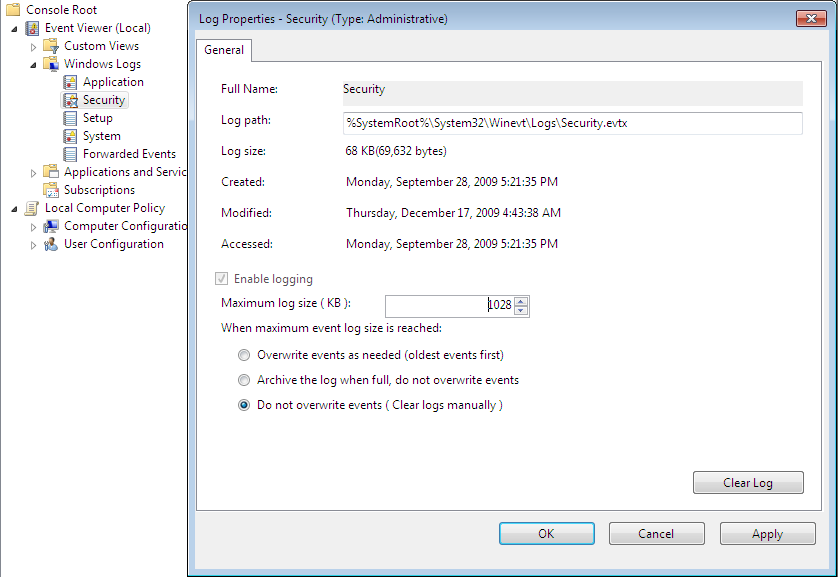
При вході користувача в систему робиться такий запис:



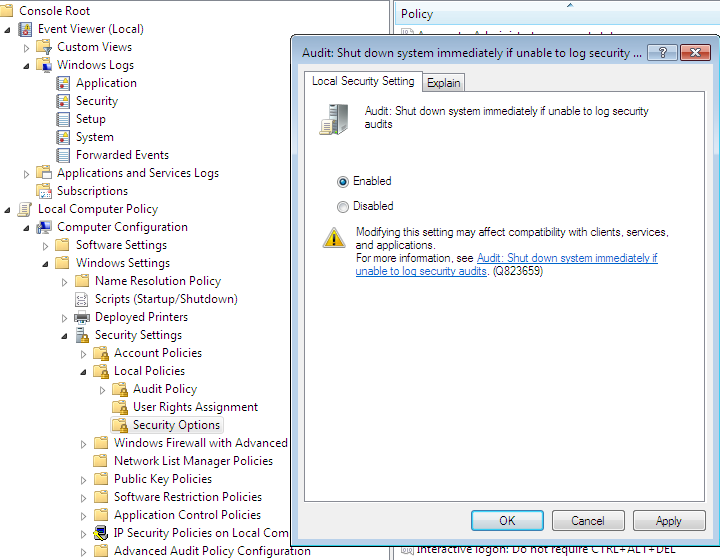
При виході користувача з системи робиться такий запис:



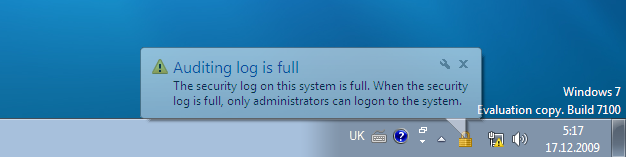
4. В контекстному меню журналу безпеки вибираю пункт "Свойства" . Задаю як найменший розмір журналу та політику "Не затирать события".



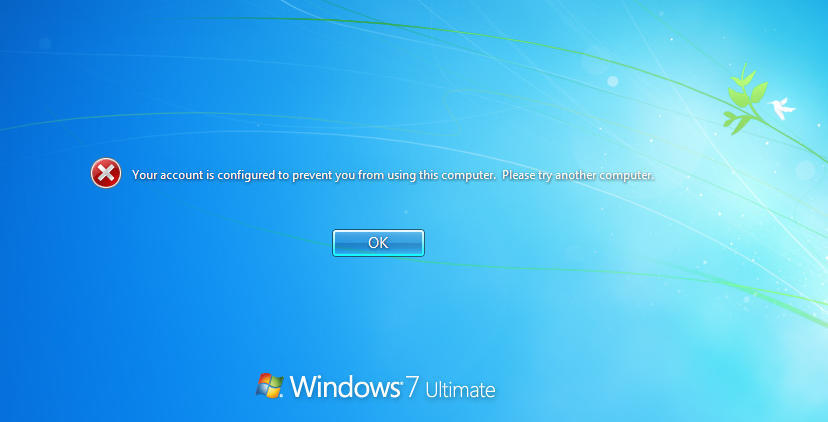
Після цього в редакторі об’єкту групової політики (гілка "Параметры безопасности") включаю параметр політики "Аудит: немедленное отключение системы, если невозможно внести в журнал записи об аудите безопасности"



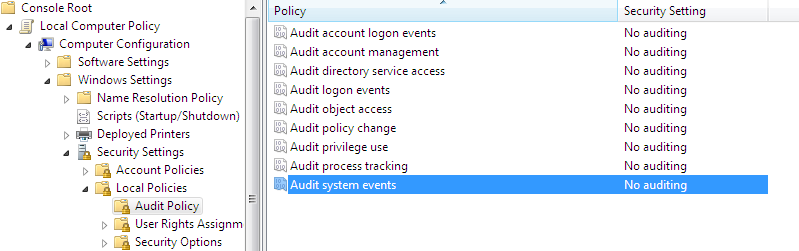
Після заповнення журналу отримаємо повідомлення:



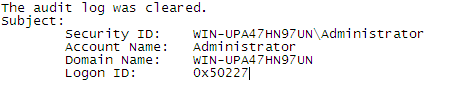
Після переповнення журналу спробував ввійти в систему з правами користувача:



Заходимо в систему з правами адміністратора і вимикаємо в весь аудит



Коли ми очистили журнал безпеки в ньому стерлися не всі записи, залишився один з інформацією про те що журнал було очищено і хто його очистив:



**Висновки:** Виконавши дану роботу я ознайомився зі структурою, принципом роботи та налаштуванням об’єкта групової політики на локальному комп’ютері та навчився використовувати та створювати шаблони безпеки для ефективного налаштування та аналізу типових параметрів безпеки.