**Практичне завдання №2 “Механізми захисту ОС Windows”.**

**Хід роботи:**

1. Запустіть Windows 7 або Windows 2008. Увійдіть в систему під обліковим записом адміністратора.

2. Вивчіть налаштування політики облікових записів і паролів (Control Panel -> Administrative Tools -> Local Security Policy -> Account Policies).

3. Запустіть Process Explorer і знайдіть параметри маркера доступу поточного користувача (SID, Group, Privilege). Покажіть, які SID має даний користувач. Яку інформацію містить структура SID. Які SID існують в системі.

4. Створіть папку і файл в ній і перегляньте (вкладка Security → Advanced) список контролю доступу на дані обе'кти. Яким типам суб'єктів доступу можуть призначатися дозволи.

5. Вивчіть і випишіть набір стандартних (Full Control, Modify, Read & execute, List folder contents, Read, Write) і спеціальних дозволів на каталоги і файли. Подумайте, які можливості дає кожний дозвіл окремо і якому набору спеціальних дозволів відповідає кожний зі стандартних дозволів.

6. Створіть три облікові записи користувачів і одну адміністратора (Control Panel -> Administrative Tools -> Computer Management -> Local Users and Groups). Задайте паролі.

Для одного з користувачів встановіть квоту дискового простору в 50 MB (вкладка Quota у властивостях логічного диска).

7. Створіть три групи користувачів і введіть раніше створених користувачів в ці групи (по одному користувачеві в групі).

8. *Сформулюйте і запишіть політку контролю доступу робочої станції,* яка регламентувала б вимоги управління обліковими записами і паролями, контролю доступу та реєстрації. Оформіть у вигляді таблиці правила розмежування доступу, де користувачі кожної групи мали б **різні** права доступу до файлів інших груп.

* При реалізації політики контролю доступу повинні використовуватися не тільки явні дозволи, але і дозволи, одержувані через групи, і дозволи, успадковані від каталогів, а також явні заборони для користувачів і груп.

9. Для кожного створеного раніше користувача створіть папку (яка містить вкладену папку і кілька документів) і назначте користувача її власником. Встановіть дозволи на папки користувачів відповідно до політики контролю доступу в п.8.

10. Перевірте діючі (вкладка Security → Advanced → Effective Permissions) дозволи і переконайтеся в дотриманні вимог політики контролю доступу.

11. Увійдіть в систему під обліковим записом непривілейованого користувача і перегляньте парметри його маркера доступу.

12. Від імені поточного користувача явно забороніть іншому користувачеві доступ до вкладеної папки і деякого документу (за умови, що раніше доступ був дозволений).

13. Надайте деякому користувачеві можливість стати власником каталогу поточного користувача. Увійдіть під цим користувачем і перевірте дану можливість. Як тепер змінилися дозволи на дану папку.

14. Змініть обліковий запис на новоствореного привілейованого користувача. Перегляньте загальні налаштування прав (Rights) в системі (Control Panel -> Administrative Tools -> Local Security Policy -> Local Policies → User Rights Assignment).

15. Вивчіть налаштування аудиту системи (Control Panel -> Administrative Tools -> Local Security Policy -> Local Policies -> Audit Policy і Advanced Audit Policy Configuration).

16. Налаштуйте і перевірте роботу аудиту подій доступу до файлової системи (створення файлів). Налаштування аудиту полягає у включенні аудиту необхідної події (Control Panel -> Administrative Tools -> Local Security Policy -> Local Policies -> Audit Policy) в системі і безпосередньо налаштуванні аудиту у властивостях папки (вкладка Security -> Advanced -> Auditing). Відтворіть необхідні події та перевірте записи в журналах реєстрації (Control Panel -> Administrative Tools -> Event Viewer).

17. Вивчіть загальні налаштування системи захисту (Control Panel -> Administrative Tools -> Local Security Policy -> Local Policies → Security Options).

18. Створіть і налаштуйте деяку папку диска C як зашифровану (Advanced attributes у властивостях папки) і забезпечте можливість її використання одним із створених в п.6 користувачів. Перевірте, чи зможе цей користувач отримати доступ до файлів з зашифрованої папки. Надайте ще одному користувачеві можливість доступу до зашифрованих файлів. Перевірте цю можливість.

19. Запишіть встановлені вами права доступу, а також ефективні права доступу у вигляді таблиці. Проаналізуйте виконання заданої в п.8 політики безпеки.

**Контрольні питання:**

- Що включає в себе політика безпеки операційної системи.
- Які підсистеми захисту повинні бути в операційній системі. У чому полягає їх робота. У чому полягає їх налаштування в ОС Windows.
- Типові властивості політик облікових записів і паролів.
- Яку інформацію містить обліковий запис користувача.
- Які налаштування облікового запису дозволяють керувати обліковими записами інших користувачів.
- Які користувачі і групи користувачів є у вашій системі та які SID вони мають.
- Які спеціальні SID вам відомі. Навіщо потрібен LOGON SID.
- Чим в ОС Windows права (привілеї) відрізняються від дозволів. Чи можуть суперечити права і привілеї.
- Які права (привілеї) користувача ви знаєте.
- Збережіть (перепишіть :) налаштування прав доступу в тій системі, де ви виконували дану роботу.
- Дозволи NTFS для файлів і папок. Стандартні дозволи.
- Як називається структура даних, в якій зберігаються дозволу для файлів і папок.
- Для яких ще об'єктів ОС, окрім файлів і папок, можуть бути встановлені дозволи.
- Що розуміється під ефективними (дійсними) дозволами. Як вони визначаються.
- Що впливає на ефективні дозволи користувача на папку / файл. Як обчислюються ефективні дозволи (Алгоритм визначення дійсних дозволів).
- Які дії над об'єктом дозволяють виконувати «права власника».
- Які дозволи доступу на каталог впливають на вкладені файли і каталоги.
- Коли дозволи доступу на каталоги поширюються на вкладені каталоги і файли і як обмежити спадкування дозволів.
- Які суб'єкти мають дозволи доступу на файлову систему (розділ жорсткого диска) в цілому.
- Як здійснюється передача дозволів між суб'єктами (користувачами);
- Які дозволи мають пріоритет (явні або успадковані; «персональні» або групові).
- Як налаштовуються квоти на файлову систему.
- Що в ОС Windows називається маркером доступу і дескриптором захисту. Яку інформацію вони містять.
- В чому полягає процедура налаштування аудиту.
- Які повідомлення можуть реєструватися підсистемою аудиту. Основні події аудиту. Події файлової системи.

- Як ви думаєте, яким алгоритмом шифрування і в якому режимі шифруються файли в EFS.
- Порівняйте (знайдіть подібності та відмінності) механізми захисту Unix і Windows.

**Перевірте практично (чи можете ви перевірити і як?):**

- Як успадковуються привілеї, призначені деякому користувачеві на каталог, на вкладені каталоги і файли. Чи може бути обмежене спадкування.
- Чи буде явна заборона мати пріоритет над явними дозволами.
- Чи буде при спадкуванні явна заборона мати пріоритет над явними дозволами.
- Чи може бути дозволено «виконання» файлу без його «читання».
- Які дії над об'єктом дозволяють виконувати права власника.
- Які можливості в даній системі є у користувача (групи) Guest.
- * Які дії потенційно можуть бути заборонені користувачеві з правами адміністратора.