Лабораторна робота №1. Частина 1.

Механізми захисту операційної системи Windows NT/2000/XP

Мета роботи

ознайомити студентів з підсистемою захисту ОС Windows NT/2000/XP.

Теоретичні відомості

Windows NT — це єдине сімейство операційних систем Microsoft, при розробці якого з самого початку було поставлено завдання створити операційну систему, що відповідає вимогам рівня захищеності С2 за «Критеріями оцінювання захищених комп'ютерних систем» (TCSEC) Міністерства оборони США, що відомі як «Оранжева книга».

Захищеність операційної системи по класу С2 вимагає відповідність наступним вимогам:

1. Обов'язкова ідентифікація й автентифікація всіх користувачів операційної системи.
2. Розмежувальний контроль доступу — надання користувачам можливості захисту даних, що їм належать.
3. Системний аудит — здатність системи вести докладний аудит усіх дій, що виконують користувачі й сама операційна система.
4. Захист об'єктів від повторного використання — здатність системи запобігти доступу користувача до ресурсів, з якими до цього працював інший користувач (наприклад, забезпечення неможливості повторного використання звільненої пам'яті або читання інформації з файлів, що були вилучені).

2 грудня 1999 року уряд США оголосив, що операційні системи Windows NT 4.0 Workstation і Windows NT 4.0 Server успішно пройшли сертифікацію по класу С2. Для Windows 2000 подібна процедура сертифікації відбулась в 2002 році, але вже не за «Критеріями оцінювання захищених комп'ютерних систем» (TCSEC) Міністерства оборони США, а за міжнародним стандартом ISO 15408, що введено в дію з 1999 року.

Розглянемо детальніше можливості засобів захисту операційної системи Windows NT. Система підтримує 4 типи суб'єктів та 13 типів об'єктів доступу.

Аутентифікація та ідентифікація відбуваються за допомогою процесу WinLogon, що перевіряє істинність користувача за допомогою інших модулів підсистеми авторизації (LSA, MSV) та запускає в разі успіху процес UserInit.exe. Останній виконується з повноваженнями даного користувача і створює для останнього робоче середовище – підключає відповідний користувачеві ключ реєстру, настройки з user profile, та запускає програмну

оболонку (explorer.exe). Архітектура підсистеми авторизації досить гнучка і дозволяє використовувати будь-які способи перевірки істинності. Проте в стандартній конфігурації використовується лише проста парольна автентифікація. Образи паролів зберігаються в спеціальному розділі реєстру, при цьому використовуються два типи хеш-функцій: за алгоритмом MD4 (NT-hash) та менш стійка з використанням DES (LM-hash), остання для сумісності з клієнтами попередньої серверної ОС Microsoft — Lan Manager. Важливою особливістю є те, що авторизація користувача може відбуватися як локально, так і делегуватися контролерові домену NT.

За допомогою утіліти User Manager Windows NT забезпечує широкі можливості по керуванню обліковими записами користувачів. Так, для кожного користувача може бути задано ряд атрибутів, таких як належність до груп, місцезнаходження user profile, робочі години, повноваження на доступ по комутованих лініях і т.д. Крім того, може бути задана політика керування обліковими записами, що регламентує:

1) мінімальний та максимальний терміни життя паролю;
2) мінімальну довжину паролю;
3) унікальність паролю як вимога не належати до заданої кількості востаннє використаних;
4) кількість невдалих спроб автентифікації, після яких обліковий запис блокується, та відрізок часу, протягом якого вони мають відбутися;
5) тривалість блокування облікового запису.

Також ця утіліта дозволяє призначати користувачам привілеї (права на всю систему, а не на конкретний об’єкт, наприклад входити в систему локально або змінювати системний час) та задавати політику аудиту.

Windows NT реалізує дискреційну модель розмежування доступу. Керування доступом здійснюється в Windows NT за допомогою спеціального модулю, що носить назву reference monitor та реалізується викликом функції SeAccessCheck ядра ОС при будь-якій спробі суб’єкта отримати доступ. При цьому використовуються дві структури даних – **маркер доступу суб’єкта**, що є носієм його повноважень, **та дескриптор захисту об’єкта**, що містить ідентифікатори власника об’єкта та його первинної групи, список контролю доступу (ACL) та список аудиту (SACL). Матриця доступу в даній ОС, таким чином, зберігається у вигляді множини списків контролю доступу об’єктів. Останні, на відміну від ОС Unix, мають нефіксовану довжину і можуть містити довільну кількість елементів контролю доступу (Access Control Entry, ACE). Кожен з ACE містить ідентифікатор суб’єкта та список методів (прав), за якими йому дозволено або заборонено доступ до даного об’єкта. ACE, що забороняють доступ, мають більший пріоритет. У випадку відсутності ACE, що визначає потрібні права, у доступі буде відмовлено. Основними правами є R-читання, W-запис, X-виконання, D-видалення, P-зміна прав доступу до даного об’єкта, O-право стати власником об’єкту.

Задати права доступу до файлових та принтерних об’єктів можна за допомогою Windows NT Explorer. Для цього необхідно виділити об’єкт, за допомогою правої кнопки миші викликати меню, в якому вибрати пункт

“Properties” (в російській локалізації “Свойства”), далі у діалоговому вікні вибрати вкладку “Security” (“Безопасность”). У вікні, що відкривається, для кожного суб’єкта доступу (користувача, псевдокористувача або групи) можна вибрати так звані “відображувані” права. Відображувані права фактично є попередньо сформованими наборами елементарних прав. Якщо є необхідність, можна керувати безпосередньо елементарними правами доступу, яких для певних видів об’єктів є більше 20. Для цього слід натиснути кнопку “Advanced...” (“Дополнительно...”). У вікні, що відкривається, можна переглядати і змінювати власника об’єкта, керувати наслідуванням прав доступу до підкаталогів і файлів, викликати додаткове вікно для перегляду і заміни всіх прав доступу для кожного суб’єкта, а також задавати параметри аудита цього об’єкта (див. далі).

Реєстрація подій у Windows NT здійснюється шляхом виклику спеціальних функцій ядра ОС, що додають записи у файли *.evt директорії \winnt\system32\config. Усього є три журнали – системний, прикладного ПО та безпеки. Реєстрацію подій, таким чином, може здійснювати будь-який компонент робочого середовища, проте сама ОС забезпечує її шляхом виклику цих функцій з модулю reference monitor. Для цього використовується список аудиту, що носить дещо неправильну назву “системний список контролю доступу” (SACL) та визначає для кожного об’єкту, що саме буде реєструватися при спробах отримати доступ тим чи іншим суб’єктом. На додаток до цього, можна фільтрувати записи реєстрації шляхом визначення так званої “політики аудиту”.

Перегляд журналів реєстрації за звичай здійснюється утилітою Event Viewer, що надає досить широкі можливості завдання фільтрів відображення записів, зокрема за часом реєстрації, типом, категорією та джерелом події. У Windows 2000 адміністратори мають доступ до перегляду журналів реєстрації через Control Panel (в російській локалізації “Панель управления”), що доступна через стартове меню, а також через пункт меню “Administrative tasks” (в російській локалізації “Администрирование”). Списки аудиту об’єктів можна задати за допомогою Windows NT Explorer: “Properties” → “Security” → “Advanced…” → “Auditing” (в російській локалізації “Свойства” → “Безопасность” → “Дополнительно...” → “Параметры аудита”). Політику аудиту задають окремо – за допомогою User Manager в Windows NT 4.0 або “Administrative tasks” → “Local security policy” (“Администрирование” → “Локальная политика безопасности”) в Windows 2000/XP.

Хід роботи

1. Створіть політику безпеки КС, що регламентувала б вимоги до керування паролями, контролю доступу та реєстрації.
2. Здійсніть вхід у систему як адміністратор. Очистіть журнали реєстрації.
3. Ознайомтеся з можливостями User Manager, створивши декілька користувачів та груп і призначивши їм відповідні політиці атрибути. Реалізуйте вимоги політики безпеки у відповідних меню.

4. Ознайомтеся з можливостями Windows NT Explorer по керуванню доступом та реєстрацією, створивши декілька файлових об'єктів та відредагувавши їх ACL і SACL.
5. Послідовно здійснюючи вхід в систему в якості створених користувачів і намагаючись отримати доступ до створених об'єктів, переконайтеся у дотриманні вимог політики безпеки стосовно керування паролями та контролю доступу.
6. Ознайомтеся з можливостями Event Viewer, здійснивши перегляд зареєстрованих подій.
7. Оформіть звіт.

Звіт повинен містити:

1) неформально задану політику безпеки для не менш ніж 3 користувачів і 2 груп та не менш ніж 6 файлових об'єктів;
2) протокол спроб отримати доступ з п.5 ходу роботи;
3) роздруківку фрагментів журналу реєстрації.

Контрольні запитання

1) Які особливості має архітектура ОС Windows NT/2000/XP? Яке значення це має для властивостей системи?
2) Які суб'єкти доступу існують в Windows NT/2000/XP?
3) Яка архітектура системи ідентифікації і аутентифікації Windows NT/2000/XP? В чому переваги такої архітектури?
4) Де і в якому вигляді зберігаються образи паролів? Які вразливості обраної системи?
5) Назвіть деякі типові об'єкти доступу Windows NT/2000/XP. Доступ до яких об'єктів контролює система розмежування доступу?
6) Які існують методи доступу, що їх розрізняє система розмежування доступу Windows NT/2000/XP? Які з них спільні для всіх видів об'єктів?
7) Які стандартні групи користувачів існують в Windows NT/2000/XP? Які їхні повноваження?
8) Яким чином Windows NT/2000/XP перевіряє можливість доступу?
9) В чому різниця в інтерпретації прав доступу для файлу і каталогу?
10) Як відбувається в Windows NT/2000/XP тимчасове підвищення повноважень?
11) Де зберігає система журнал реєстрації? Які можливості і недоліки системи захисту журналу реєстрації від НСД?