Звіт

Безпека ОС

Завдання:

-написати відповіді на питання

ПІБ Гапей Максим Юрійович група № ПД-31

|  |  |
| --- | --- |
| Етапи побудови засобу захисту | 1.Формування вимог  Розроблення політики безпеки, моделі  безпеки  Розроблення ТЗ  Проектування  Реалізація  Тестування (сертифікація)  Впровадження  8. Супроводження |
| 2. Модель загроз для операційної системи | -Сканування файлової системи  Викрадення ключової інформації  Підбирання паролів  Збирання сміття  Перевищення повноважень  Програмні закладки  - Жадібні програми |
| 3. Описати загрозу сканування файлової системи | Ця загроза полягає в тому, що порушник переглядає (сканує) всю  файлову систему, і намагається прочитати усі файли поспіль   Замість зчитування порушник може намагатись скопіювати або  видалити файли   Якщо він не може отримати доступ до деякого об’єкта файлової  системи (окремого файлу або каталогу), то він пропускає захищений  об’єкт і продовжує сканування   Порушник може здійснювати цю атаку, використовуючи спеціальне  програмне забезпечення |
| 4. Описати зміст загрозі викрадення ключової інформації |  На рівні ОС використовується різна інформація, яку можна віднести до ключової.  Найпоширеніший вид такої інформації – паролі доступу до системи   Типові способи викрадення паролів:   викрадення пароля, що записаний на папері   підглядання пароля в момент, коли користувач його набирає   достатньо всього кілька тижнів тренувань для того, щоби фіксувати пароль за рухами рук  користувача по клавіатурі   підглядання пароля на екрані   усі сучасні ОС приховують і не демонструють пароль, що вводиться   пароль на екрані видно, якщо його помилково вводять у інше поле введення   пароль видно, коли його вводять як аргумент в командному рядку   зчитування пароля у командних файлах (сценаріях)   користувачі можуть створювати командні файли для автоматизації входу на віддалені мережні  ресурси   отримання паролів, що ненадійно зберігаються   іноді паролі ховаються у деякому файлі у відкритому вигляді   часто паролі ненадійно кодують (наприклад, за допомогою операції XOR   якщо використовуються зовнішні носії ключової інформації (дискети, пристрої флеш-  пам’яті, токени), то ці носії можуть бути просто викрадені. |
| 5. Описати зміст загрозі підбір паролів | Підбирання паролів передбачає використання засобів автентифікації  для знаходження того пароля, який буде прийнятий як правильний   Порушник отримує несанкціонований доступ до певного ресурсу, якщо  пароль використовується для обмеження доступу до ресурсу   або можливість працювати в системі від імені іншого користувача, якщо  пароль використовується для автентифікації |
| 6. Описати зміст загрозі збір сміття | Збирання сміття – це отримання даних, які залишаються у  об’єктах, що звільняються ОС після їх використання   Найтиповішими з таких об’єктів є файли на дисках і ділянки  оперативної пам’яті   У більшості файлових систем файли після їх видалення не  знищуються фізично, а лише помічаються як знищені |
| Описати зміст загрозі перевищення повноважень | Ця загроза полягає у тому, що порушник якимось  чином отримує повноваження, що перевищують ті, які  йому надані згідно політики безпеки   Перевищення повноважень можливе або через помилки в  розробці й реалізації політики безпеки (наприклад, невірні  настроювання системи розмежування доступу)   або шляхом використання наявних вразливостей в  програмному забезпеченні, яке входить до складу ОС |
| Описати зміст загрозі програмні закладки | До програмних закладок відносять програми або окремі модулі програм, які  протягом тривалого часу функціонують в комп’ютерній системі, здійснюючи  заходи щодо приховування свого існування від користувача   Програмні закладки можуть впроваджуватись вірусом, “троянським конем”,  мережним хробаком або безпосередньо користувачем-зловмисником   Функції програмних закладок:   перехоплення і передавання інформації:   крадіжка паролів;   шпигунські програми (Spyware);   порушення функціонування систем (“логічні бомби”):   знищення інформації;   зловмисна модифікація інформації;   блокування системи;   модифікація програмного забезпечення:   утиліти віддаленого адміністрування (люки);   Інтернет-клікери;   проксі-сервера;   дзвінки на платні ресурси;   організація DoS і DdoS атак;   психологічний тиск на користувача:   реклама (Adware);   злі жарти і містифікації. |
| Описати зміст загрозі жадібні програми |  Жадібні програми – це шкідливі програми, які  захоплюють значну частину ресурсів комп’ютера,  внаслідок чого робота інших користувачів та/або  процесів помітно утруднюється або взагалі стає  неможливою. Часто жадібні програми можуть  призводити до краху ОС   Здебільшого, жадібні програми належать до класу  “троянських коней”   Жадібні програми можуть бути Web-застосунками, які  запускаються при заході браузером на певні Web-  сторінки |
| Описати зміст захищеної ОС | Можна вважати захищеною таку ОС, яка  передбачає захист від основних загроз:   Сканування файлової системи   Викрадення ключової інформації   Підбирання паролів   Збирання сміття   Перевищення повноважень   Програмних закладок   Жадібних програм |
| Описати принципи створення захищених ОС | Принцип інтегрованості   Засоби захисту повинні бути вбудовані  в систему таким чином, щоби усі без  виключення механізми взаємодії  знаходились під їх контролем  Найпростішим методом, що реалізує цей  принцип при створенні ОС, є максимальне  обмеження числа механізмів взаємодії та  інтеграція засобів захисту безпосередньо в  ці механізми  Принцип інваріантності   Засоби захисту не повинні залежати від  особливостей реалізації утиліт і прикладних  програм, і не повинні враховувати логіку їх  функціонування   Засоби захисту повинні бути універсальними  для усіх типів взаємодій   Для ОС інваріантність засобів захисту може бути  досягнута шляхом застосування строго  регламентованої парадигми функціонування  програм, що обмежує способи взаємодій  Принцип уніфікації   Засоби захисту мають бути універсальними, що  дозволяє використовувати їх без змін як для  реалізації різних моделей безпеки, так і для  керування доступом до об’єктів різної природи   Повинна існувати однозначна відповідність між взаємодіями  суб’єктів і об’єктів, що контролюються, та операціями  доступу, керування якими описується моделями безпеки   При розробленні ОС слідування цьому принципу приводить  до необхідності створення універсального інтерфейсу  доступу, що об’єднує всі способи взаємодій між суб’єктами й  об’єктами, всі функції якого однозначним чином  відображаються на множину операцій, що описуються  моделлю безпеки  Принцип адекватності   Для забезпечення реальної здатності протидіяти атакам  необхідно виключити усі чинники, які спричиняють виникнення  вразливостей   Усі механізми реалізації атак базуються на використанні наявних  вразливостей   Головною причиною появи вразливостей є непослідовність в  реалізації контролю доступу   Існуючі системи містять привілейовані засоби та служби, які передають  користувачам частину своїх повноважень, минаючи засоби контролю   Типовий приклад – механізм SUID/SGID в системі UNIX   Переважну більшість причин появи вразливостей можна усунути,  реалізувавши в системі керування доступом на основі  універсального інтерфейсу та єдиного механізму взаємодії без  будь-яких виключень   Також необхідною є мінімізація обсягу довіреного коду самих  засобів захисту з метою зменшення ймовірності появи в них  помилок.  Принцип коректності   Засоби захисту повинні реалізовувати  керування доступом відповідно до  формальних моделей  Наявність несуперечливої моделі безпеки:   дозволяє формально обґрунтувати безпеку  системи,   надає об’єктивний критерій коректності її  роботи,   може бути основою для побудови вичерпних  тестів, що перевіряють правильність роботи  засобів захисту в усіх режимах і обставинах. |
| Перелік основних підсистем КЗЗ ОС (комплексного захисту засобів операційних систем) | Розмежування доступу   Кожному користувачеві надається доступ лише до тих захищених  об’єктів, доступ до яких дозволений йому політикою безпеки   Ця підсистема безпосередньо реалізовує політику безпеки  Ідентифікація й автентифікація   Жодний користувач не може розпочати роботу в середовищі  захищеної ОС, не надавши системі свого ідентифікатора і не  підтвердивши справжність наданого ідентифікатора за допомогою  додаткової інформації, що автентифікує цього користувача  Аудит   В захищеній ОС здійснюється реєстрація всіх подій, що є  потенційно небезпечними   Підсистема аудиту здійснює захист журналів, в яких відбувається  реєстрація, від НСД   Також ця підсистема може надавати засоби для аналізу журналів і  відстеження джерел тих чи інших подій  Керування політикою безпеки   Захищена ОС повинна надавати інтерфейси, які дозволяють  адміністраторам ефективно вирішувати завдання з підтримання адекватної  політики безпеки   Обов’язково надаються інтерфейси для настроювання підсистем  розмежування доступу, ідентифікації й автентифікації, аудиту  Криптографічні функції   Криптографічні функції застосовуються для захисту конфіденційності і  цілісності інформації, для автентифікації і забезпечення неможливості  відмовлення від авторства   Криптографічні функції можуть використовуватись в якості самостійних  засобів захисту, або в якості допоміжних механізмів в інших засобах  Забезпечення цілісності   Будь-яка сучасна ОС надає додаткові засоби для захисту цілісності даних не  лише від НСД, але й від випадкових помилок, а також від аварій і збоїв  системи   В першу чергу це стосується даних у файлових системах   Такі засоби реалізують можливості відкату, а також автоматизацію процесу  створення резервних копій і відновлення з них  Антивірусний захист   Як правило, під підсистемою антивірусного захисту розуміють  сукупність програм, які надають можливість виявляти і  знешкоджувати відомі шкідливі програми, які відносяться як до  вірусів (у широкому розумінні – включаючи троянських коней,  мережевих хробаків, шпигунські програми), так і до засобів  здійснення атак   Без антивірусного захисту в наш час неможливо підтримувати ОС у  безпечному стані, особливо якщо вона встановлена на комп’ютері,  що підключений до мережі   Як правило, антивірусні засоби не входять до складу ОС, а  постачаються окремо  Апаратні засоби   КЗЗ ОС спирається на функції захисту, реалізовані в апаратних  засобах – процесорі і системній платі |
| Перелік основних компонент КЗЗ Windows |  Монітор безпеки   Підсистема локальної автентифікації   База даних політики Lsass   Диспетчер облікових записів безпеки (   База даних SAM   Active Directory   Пакети автентифікації   Інтерактивний диспетчер входу в систему (Winlogon)   Користувацький інтерфейс входу в систему — Logon user  interface (LogonUI)   Постачальники облікових даних — Credential providers (CP)   COM-об’єкти, що використовують для одержання імені користувача  і пароля, PIN-кода смарт-карти або біометричних даних (наприклад,  відбитка пальця)   Стандартними CP є бібліотеки %SystemRoot%\System32\authui.dll и  %SystemRoot%\System32\SmartcardCredentialProvider.dll.  Компоненти КЗЗ Windows (6/7)   Служба мережного входу до системи (Net Logon, Netlogon)   Win32сервіс (%SystemRoot%\System32\Netlogon.dll), виконується в  Lsass і реагує на запити мережного входу від Microsoft LAN Manager  2 під керуванням Windows NT (будь-яких версій до Windows 2000).  В цьому випадку автентифікація відпрацьовується як при локальній  реєстрації – дані передаються Lsass для перевірки. У Netlogon  також вбудовано службу локатора, що потрібна для пошуку  контролерів домену.   Kernel Security Device Driver (KSecDD)   Бібліотека функцій режиму ядра, що реалізує інтерфейси  локального виклику процедур (англ. – local procedure call, LPC), які  використовуються іншими компонентами захисту режиму ядра – у  тому числі файловою системою, що шифрує (англ. – Encrypting File  System, EFS) – для взаємодії з Lsass у режимі користувача   KSecDD знаходиться у %SystemRoot%\System32\Drivers\Ksecdd.sys  Компоненти КЗЗ Windows (7/7)   AppLocker   Механізм, що дозволяє адміністраторам визначати, які виконувані  файли, DLL-бібліотеки і сценарії можуть використовуватись  конкретними користувачами і групами.   AppLocker складається з драйвера  (%SystemRoot%\System32\Drivers\AppId.sys) і служби  (%SystemRoot%\System32\AppIdSvc.dll), |
| Суб‘єкти доступу Windows | Користувачі   звичайні користувачі   псевдокористувачі:   SYSTEM – ОС локального комп’ютера   <ім’я\_комп’ютера>$, де ім’я\_комп’ютера – мережеве ім’я комп’ютера;  представляють ОС інших комп’ютерів в мережі і використовуються під час  автентифікації робочої станції на контролері домену  Групи користувачів  Спеціальні (тимчасові) групи   Належність користувача до спеціальних груп визначається ОС в  залежності від його дій:   INTERACTIVE   NETWORK   DIAL\_UP   Спеціальна група не може бути первинною групою користувача  Відносні суб’єкти   мають сенс лише стосовно об’єкта, для якого визначаються права доступу   CREATOR\_OWNER – власник об’єкта   CREATOR\_GROUP – первинна група власника об’єкта |
| Методи доступу Windows |  Загалом ОС Windows підтримує 22 методи доступу  суб’єктів до об’єктів   6 з них підтримуються для об’єктів усіх типів, а саме:   видалення об’єкта,   отримання атрибутів захисту об’єкта,   зміна атрибутів захисту об’єкта,   зміна власника об’єкта,   отримання та зміна параметрів аудиту по відношенню до  об’єкта (ACCESS\_SYSTEM\_SECURITY),   синхронізація (SYNCHRONIZE).   Названі методи є стандартними методами доступу   Для кожного типу об’єктів також підтримуються до 16  типів специфічних методів доступу |
| Права доступу |  Специфічні   Кожному специфічному методу доступу, що підтримується для  певного типу об’єктів, відповідає право на його здійснення   Стандартні   Кожному стандартному методу доступу, за виключенням  ACCESS\_SYSTEM\_SECURITY, також відповідає право доступу   Загальні (generic) або відображувані (mapped)   Відображувані права доступу введені, головним чином, для  сумісності з програмним інтерфейсом POSIX, який підтримує лише  три права доступу, що визначені для усіх типів об’єктів, –  зчитування, записування і виконання.   Віртуальні   Віртуальні права доступу можуть бути запитані суб’єктом, але не  можуть бути йому наданими |
| Привілеї доступу |  Частина методів доступу вимагають від суб’єкта  доступу спеціальних привілеїв. До таких методів  належать:   створення нового сервісу;   блокування списку сервісів;   запуск сервісу;   зупинка сервісу;   призупинення / поновлення сервісу;   призначення процесу маркера доступу;   отримання або зміна параметрів аудиту по відношенню до  об’єкта. |

Відправити на [kyi12kyi12@gmail.com](mailto:kyi12kyi12@gmail.com)