Лекція 6. Системні журнали. Перегляд подій системного журналу

Журнал подій (Event Log) — в Microsoft Windows стандартний спосіб для додатків і операційної системи запису і централізованого зберігання інформації про важливі програмні і апаратні події. Служба журналів подій зберігає події від різних джерел в єдиному журналі подій, програма перегляду подій дозволяє користувачеві спостерігати за журналом подій, програмний інтерфейс (API) дозволяє додаткам записувати в журнал інформацію і переглядати існуючі записи.

Записи журналу подій зберігаються в ключі реєстру

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog

Даний ключ містить підключі, звані файлами журналу. За замовчуванням присутні:

- файл журналу додатків — для застосунків і служб;
- файл журналу безпеки — для подій системи аудиту;
- файл системного журналу — для подій драйверів пристроїв.

Є можливість створювати додаткові журнали. Для кожного джерела подій в журналі створюється окремий підключ. Події від кожного джерела можуть включатися в окрему для кожного джерела категорію. Події повинні належати до одного з п'яти визначених типів.

Тип	Опис
Інформація	Події вказують на рідкісні і важливі успішні операції.
Попередження	Події вказують на проблеми, які не вимагають негайного втручання, але можуть призвести до помилок у майбутньому. Прикладом такого роду подій може служити вичерпання ресурсів.
Помилка	Події вказують на істотні проблеми, які зазвичай призводять до втрати функціональності або даних. Прикладом може служити неможливість запуску служби при завантаженні.

Успішний аудит	Події безпеки, які відбуваються при успішному зверненні до ресурсів, які проходять аудит. Прикладом може служити успішний вхід в систему.
Не успішний аудит	Події безпеки, які відбуваються при неуспішному зверненні до ресурсів, які проходять аудит. Прикладом може служити спроба відкрити файл, не маючи відповідних прав доступу.

Запис про подію включає в себе: ідентифікатор події, тип події, категорію події, масив рядків і додаткові, специфічні для події, двійкові дані. Кожне джерело подій повинне зареєструвати свій файл-повідомлення, в якому зберігаються рядок опису ідентифікаторів повідомлень, категорій і параметрів. Рядок опису може містити місце для вставки рядків з масиву, зазначеного при запису події, наприклад:

Неможливо відкрити %1, помилка %2

Додаткові дані ніяк не інтерпретуються програмою перегляду подій і відображаються в шістнадцятковому і текстовому форматі.

Основні функції роботи з подіями:

- OpenEventLog — відкриття журналу на певному комп'ютері для адміністративних операцій;
- ReadEventLog — зчитування частини журналу в буфер;
- GetOldestEventLogRecord — отримати номер найстарішого запису;
- GetNumberOfEventLogRecords — отримати кількість записів в зазначеному журналі;
- NotifyChangeEventLog — отримувати повідомлення при записі в зазначений журнал;
- BackupEventLog — запис журналу в архів;
- ClearEventLog — очищення журналу з можливістю запису в архів;
- OpenBackupEventLog — відкриття архівної копії журналу;
- CloseEventLog — закриття журналу;

- RegisterEventSource — відкриття журналу для запису подій від вказаного джерела;
- ReportEvent — запис події в журнал;
- DeregisterEventSource — закриття журналу, відкритого для запису.

Адміністратори можуть оглянути і очистити журнал, розділити права на читання і очищення неможливо. Крім того, адміністратор може використовувати спеціальну утиліту Winzapper для видалення записів про конкретні події з журналу. З цієї причини, у разі якщо обліковий запис адміністратора був зламаний, історія подій, що містяться в журналі подій, стає недостовірною. Протистояти цьому можна шляхом створення віддаленого сервера журналу, доступ до якого буде здійснюватися лише за допомогою консолі.

Як тільки журнал досягає максимально допустимого розміру, він може або заміняти старі події, або зупинити запис. Це робить його сприйнятливим до атак, в яких порушник намагається заповнити журнал шляхом створення великої кількості нових подій. Частково проти цього може допомогти збільшення максимального розміру журналу. Таким чином, для переповнення журналу потрібно ініціювати більшу кількість подій. Можна дати команду журналу не заміняти старі події, але це може стати причиною збою.

Ще один спосіб атакувати журнал подій - зареєструватися під обліковим записом адміністратора і змінити політику аудиту, а саме - зупинити запис у журнал несанкціонованої активності. В залежності від налаштувань політики аудиту, її зміна може бути записано в журналі. Запис про цю подію можна очистити за допомогою Winzapper. З цього моменту активність не буде фіксуватися в журналі подій.

Звичайно, доступ до журналу потрібен не для всіх атак. Але знаючи про те, яким чином працює журнал подій, можна вжити заходів обережності, щоб уникнути виявлення. Наприклад, користувач, що бажає увійти в систему під обліковим записом товариша по службі по корпоративній мережі, може чекати до тих пір, поки не зможе непомітно скористатися комп'ютером. Далі він використовує апаратні засоби для підбору пароля і реєструється в системі. Потім

ім'я облікового запису користувача передається в службу терміналів з Wi-Fi Hotspot, IP-адресу якої буде неможливо відстежити і вийти через нього на зломщика.

Після того як журнал очищається через вікно перегляду подій, одразу створюється один запис в свіжому журналі, зазначаючи час очищення та адміністратора-виконавця. Ця інформація може стати відправною точкою в розслідуванні підозрілих дій.

Крім журналу подій Windows, адміністратори також можуть перевірити журнал безпеки Брандмауера Windows.