Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Установление некоторых обстоятельств воздействия пользователя ОС Windows на файловую систему NTFS

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 631 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Гаврилова Алексея Леонидовича

Научный руководитель

доцент, к.ю.н. _____ А.В. Гортинский

31.12.2016 г.

Заведующий кафедрой

профессор, к.ф.-м.н. _____ В.Н. Салий

31.12.2016 г.

Саратов 2017

ВВЕДЕНИЕ

Для успешного расследования преступлений в сфере информационных технологий нередко приходится проводить компьютерно-технические экспертизы. Они дают возможность определить, по каким назначениям применялась обследуемая техника, а также первоначальное состояние информации на носителях данных и характер воздействий на исследуемую информацию.

Специалисты этой области для работы используют внушительный объем инструментов и собственный опыт, чтобы выполнить поставленную перед ними задачу в полном объеме. Экспертиза компьютеров, аппаратно-технических средств, ПО, баз данных вследствие постоянного совершенствования компьютерной техники и программного обеспечения являются одним из самых сложных видов исследований.

Задача выявления владельца отдельного файла ОС семейства Windows или их набора является довольно обыденной для компьютерной экспертизы, не выделяется среди прочих подобных задач. Узнав, кто владеет указанным файлом, для установления обстоятельств воздействия этого пользователя на систему, можно провести дальнейшее исследование, пытаясь найти остальные его файлы.

Простой перебор файлов с использованием программ, позволяющих получить доступ к их свойствам, не выглядит эффективным. Менее тривиальный способ основан на использовании уникальных идентификаторов безопасности, или SID, которые есть у каждого пользователя в системе. С их помощью поставленная задача может быть выполнена довольно быстро. Но перед этим необходимо разобраться в структуре SID, а также какую информацию о владельце можно из него получить.

Также в рамках экспертизы зачастую требуется получить подробные личные данные определенного пользователя, например, его реальное имя,

фамилию и прочее, используя лишь его идентификатор безопасности. Поиск этих сведений на локальной машине зачастую неэффективен хотя бы потому, что имеющийся идентификатор владельца может быть неизвестен данной системе. В этом случае можно обратиться к локальному контроллеру домена с целью получения нужной информации.

Целью работы является автоматизация процесса получения сведений об актуальных владельцах файлов в файловой системе NTFS операционной системы семейства Windows на локальном компьютере и в домене, а также определение набора файлов для каждого такого владельца.

Ее актуальность в том, что результаты, полученные в ходе практики, позволяют несколько упростить и сделать более эффективным процесс компьютерных экспертиз, благодаря тому, что дают возможность оперативно находить подробную информацию о владельце файла, а также получать полный и интерактивный список файлов этого пользователя, используя его SID в качестве поискового информации.

Дипломная работа состоит из введения, четырех разделов, заключения, списка использованных источников и одного приложения. Общий объем работы – 73 страницы, из них 36 страниц – основное содержание, включая 21 рисунок и три таблицы, список использованных источников из 16 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

1 Использование SID системой безопасности Windows

SID – Security Identifier, используется в NT/2000 в качестве уникального идентификатора объекта, такого как пользователь или группа. Является уникальным в пределах домена или локально и никогда не используется повторно.

SID-ы от удаленных учетных записей также не используются. Даже если создать новый аккаунт с абсолютно теми же данными (ФИО и т.д.), что и у удаленного, ОС сгенерирует для него новый SID. Этот SID не совпадает со старым, никакие из разрешений старого аккаунта не переместятся в новый.

1.1 Структура SID

SID – это структура данных в двоичном формате, который содержит изменяющееся количество величин. В первых величинах содержится информация о самой структуре SID (рисунок 1), а оставшиеся величины расположены иерархически, наподобие телефонного номера. Они определяют орган, который выдал SID (например, операционная система), домен выдачи SID, а также определенное лицо или группу пользователей, отвечающих за безопасность.

Компоненты SID легче воспринимать в виде строки, которая получается из двоичной интерпретации, используя стандартный способ:

$$S-R-X-Y_1-Y_2-\ldots-Y_n,$$

где S – указатель того, что данная строка это SID;

R – версия SID;

X – класс учетной записи / значение SID Authority;

Y_i – подклассовые величины, где n – количество классов.

После первого захода в систему с использованием доменной учетной записи, некоторая информация о пользователе (например, его логин), ассоциированная с SID пользователя, остается на данном компьютере, что

позволяет ограниченно идентифицировать пользователя по его идентификатору безопасности и без участия контроллера домена.

2 Консолидированная безопасность в NTFS

NTFS всегда располагала функциями безопасности, позволяющими администратору указать пользователей, которым разрешен или запрещен доступ к тем или иным файлам и каталогам. В версиях NTFS, предшествовавших Windows 2000 (т.е. старше NTFS 3.0), дескриптор безопасности каждого файла и каталога хранился в его собственном атрибуте безопасности. Дескриптор безопасности – это специальная структура, которая хранит информацию о безопасности объекта.

Чаще всего всему дереву каталогов администраторами назначаются единые параметры безопасности, из-за чего дублируются дескрипторы безопасности тех объектов этого дерева. В NTFS 5 все дескрипторы безопасности хранятся в единственном экземпляре в файле метаданных $Secure. Идентификатор назначенного дескриптора хранится в атрибуте $STANDARD_INFORMATION файла или каталога.

2.1 Роль Access Control List (ACL) в обеспечении контроля доступа

Access Control List, или ACL – список контроля доступа, который определяет, кто или что может получать доступ к конкретному объекту и какие именно операции разрешено или запрещено этому субъекту проводить над объектом.

Дескриптор безопасности для объекта может содержать два ACL:

1) DACL (Discretionary ACL – список разграничительного контроля доступа), который определяет пользователей и группы, которым разрешен или запрещен доступ;
2) SACL (System ACL – системный список контроля доступа), который контролирует наблюдение за доступом к объекту – кто и когда получал к нему доступ.

В системе с моделью безопасности, основанной на ACL, когда субъект запрашивает выполнение операции над объектом, система сначала проверяет список разрешённых для этого субъекта операций и только после этого даёт (или не даёт) доступ к запрошенному действию.

2.1.1 Структура ACL

Размер ACL меняется в зависимости от количества и размера ACE в его составе. Максимальный размер ACL – 64 Кб, что приблизительно равно 1820 ACE, в зависимости от их размера.

Все ACE хранятся в упорядоченном виде, во время проверки возможности доступа они проверяются в порядке следования. Поскольку проверка ACE прекращается, как только находится соответствие SID пользователя, для которого проверяется доступ, порядок следования DACL очень важен.

Все явные правила доступа имеют преимущество над наследованными, а правила запрета имеют больший приоритет, нежели правила разрешения.

2.1.2 Структура ACE

Каждая запись содержит SID того пользователя или группы, правило доступа для которого она определяет, маску доступа, которая и определяет описываемое правило доступа. Также она содержит набор флагов, которые определяют, могут или нет дочерние объекты наследовать эту запись ACE.

Каждый бит маски доступа может быть активен и неактивен, но его смысл будет зависеть от типа ACE. Например, если активен бит, отвечающий за правило чтения и записи, а тип рассматриваемой ACE – «запретить», то эта ACE будет давать запрет на чтение и запись. Если же тип этой ACE – «разрешить», эта запись контроля доступа уже разрешит доступ к файлу.

3 Протокол LDAP

LDAP – это протокол, определяющий методы, посредством которых осуществляется доступ к данным каталога. Он также определяет и описывает,

как данные представлены в службе каталогов. LDAP не определяет, как происходит хранение и манипулирование данными.

От данных, обычно хранящихся в каталоге LDAP, не ожидается, чтобы они менялись при каждом доступе. Отличный пример LDAP-приложения – адресная книга, где данные меняются довольно редко.

3.1 Информационная модель LDAP

Каталоги LDAP используют модель данных, которая представляет данные как иерархию объектов.

Краткое описание модели данных LDAP таково:

1) каждая запись состоит из одного или нескольких объектных классов;
2) у каждого объектного класса есть имя;
3) у каждого атрибута есть имя, он является членом объектного класса и обычно содержит данные.

3.2 LDAP и служба каталогов Active Directory

Для управления, в частности, учетными записями пользователей и группами в ОС семейства Windows Server используется оснастка «Active Directory – пользователи и компьютеры» (рус. – Активный каталог), которая является LDAP-совместимой реализацией службы каталогов корпорации Microsoft. Этот инструмент позволяет создавать объекты, настраивать их атрибуты и выполнять с ними ряд других операций. Все настройки хранятся в централизованной базе данных.

Active Directory имеет иерархическую структуру, состоящую из объектов. Объекты разделяются на три основные категории: ресурсы (например, принтеры), службы (например, электронная почта) и учётные записи пользователей и компьютеров. В рамках данной работы рассмотрены объекты последней категории – учетные записи пользователей. Их также называют субъектами безопасности. Субъекты безопасности — это объекты службы

каталогов, которым автоматически назначаются идентификаторы безопасности (SID), их можно использовать для доступа к доменным ресурсам.

3.2.1 Именование объектов

Одним из условий успешного манипулирования объектами каталога является однозначная идентификация каждого объекта. Для именования и идентификации объектов в каталоге протокол LDAP использует механизм отличительных имен (Distinguished Name, DN), которые однозначно определяет положение объекта в информационном дереве каталога.

Для формирования отличительного имени используются спецификаторы, определяющие тип объекта:

- DC (Domain Component) – спецификатор «составная часть доменного имени»;
- OU (Organizational Unit) – спецификатор «организационная единица»;
- CN (Common Name) – спецификатор «общее имя».

ЗАКЛЮЧЕНИЕ

В рамках этой работы были рассмотрены уникальные идентификаторы SID и их участие в безопасности системы и разграничении доступа, протокол LDAP и его использование при отправке запросов на контроллер домена под управлением ОС Windows Server. Зачастую, в домены входит большое количество как компьютеров, так и пользователей, поэтому поиск информации о владельце того или иного файла не на конкретном компьютере, а в централизованной базе, существенно повышает шансы получить искомый результат.

В результате исследований было написано приложение на языке Java, позволяющее узнать владельца указанного файла или владельцев всех файлов в папке и затем использовать их уникальные идентификаторы безопасности для поиска всех их файлов, а также для получения расширенной информации о них от локального контроллера домена.

Полученное приложение может использоваться специалистами в процессе проведения компьютерно-технических экспертиз.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Независимая компьютерная экспертиза [Электронный ресурс] // ООО «Центр оценки и экспертизы» [Электронный ресурс]. URL: http://www.ekspertizaspb.ru/nezavisimaya-ekspertiza/kompyuterno-tehnicheskaya-ekspertiza/#nezav (дата обращения: 10.12.2016). Загл. с экрана. Яз. рус.

2 Компьютерная экспертиза [Электронный ресурс] // Центр независимой экспертизы «Аспект» [Электронный ресурс]. URL: http://a-aspect.ru/komp_exp/ (дата обращения: 10.12.2016). Загл. с экрана. Яз. рус.

3 Savill, J. What is a Security ID? [Электронный ресурс] / J. Savill // Windows IT Pro [Электронный ресурс]. URL: http://windowsitpro.com/windows/what-sid-security-id (дата обращения: 23.10.16). Загл. с экрана. Яз. англ.

4 Руссинович, М. Миф о дублировании SID компьютера / М. Руссинович // журн. Хакер. 2009. №12 (132).

5 Microsoft TechNet. How security identifiers work [Электронный ресурс] // Microsoft TechNet [Электронный ресурс]. URL: http://technet.microsoft.com/ en-us/library/cc778824%28WS.10%29.aspx (дата обращения: 23.10.2016). Загл. с экрана. Яз. англ.

6 Osterman, L. Larry Osterman's WebLog [Электронный ресурс] / L. Osterman // URL: http://blogs.msdn.com/b/larryosterman/archive/2004/09/01/224051.aspx (дата обращения: 5.11.2016). Загл. с экрана. Яз. англ.

7 Руссинович, М. NTFS позволяют оптимизировать использование диска и расширить функциональность программ [Электронный ресурс] / М. Руссинович // URL: http://www.windxp.com.ru/ntfs.htm (дата обращения: 13.11.2016). Загл. с экрана. Яз. рус.

8 Security Principals Technical Overview [Электронный ресурс] // Microsoft MSDN [Электронный ресурс]. URL: https://msdn.microsoft.com/

ru-ru/library/dn486814(v=ws.11).aspx. (дата обращения: 23.10.2016). Загл. с экрана. Яз. англ.

9 How the System Uses ACLs [Электронный ресурс] // NTFS.com. [Электронный ресурс]. URL: http://www.ntfs.com/ntfs-permissions-acl-use.htm (дата обращения: 20.11.2016). Загл. с экрана. Яз. англ.

10 Russon, R., Fledel, Y. NTFS Documentation [Электронный ресурс] / R. Russuon, Y. Fledel // URL: http://ftp.kolibrios.org/users/Asper/docs/NTFS/ntfsdoc.html (дата обращения: 20.11.2016). Загл. с экрана. Яз. англ.

11 LDAP Concepts & Overview [Электронный ресурс] // zytrax.com [Электронный ресурс]. URL: http://www.zytrax.com/books/ldap/ch2/ (дата обращения: 15.09.2016). Загл. с экрана. Яз. англ.

12 Понятия и обзор LDAP [Электронный ресурс] // pro-ldap.ru [Электронный ресурс]. URL: http://pro-ldap.ru/tr/zytrax/ch2 (дата обращения 20.09.2016). Загл. с экрана. Яз. рус.

13 Оснастка Active Directory - пользователи и компьютеры (Active Directory Users and Computers) [Электронный ресурс] // OSZone.net [Электронный ресурс]. URL: http://www.oszone.net/1137 (дата обращения: 20.09.2016). Загл. с экрана. Яз. рус.

14 Правила именования объектов в LDAP [Электронный ресурс] // vrnka.ru [Электронный ресурс]. URL: http://vrnka.ru/active/direct7.html (дата обращения 21.09.2016). Загл. с экрана. Яз. рус.

15 Klein, H. Tools for IT Pros [Электронный ресурс] / H. Klein // URL: https://helgeklein.com/setacl/ (дата обращения: 18.11.2016). Загл. с экрана. Яз. англ.

16 Kouti, S. User Attributes – Inside Active Director [Электронный ресурс] / Kouti S. // URL: http://www.kouti.com/tables/userattributes.htm (дата обращения: 01.12.2016). Загл. с экрана. Яз. англ.