УДК 004.07

ПРОБЛЕМЫ КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ В ACTIVE DIRECTORY

Чиж В.А.
ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича»
Научный руководитель - преподаватель Кривоносова Н.В.
ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича»

Проблема защиты ИТ-инфраструктуры предприятия актуальна не первый год. Но сегодня крайне важным вопросом в организации защиты является правильный выбор программного и аппаратного обеспечения, а так же настройка программного обеспечения. В этой работе представлено решение штатными средствами уязвимости в ПО Active Directory, позволяющей любому пользователю системы при помощи утилиты для PowerShell - PowerTool просмотреть информацию, содержащуюся в учетной записи каждого пользователя системы.

Несмотря на значительное расширение рынка сбыта серверного оборудования, работающего на основе *nix систем, более 70% поставляемых серверов предназначены для работы с операционными системами класса Windows Server. Несмотря на значительный спад продаж серверов на Windows в 2010 и 2011 годах в последнее время, благодаря выходу на рынок новых версий ПО, Windows Server смогла утвердить свои позиции на рынке и показать значительный рост в последние два года.

В связи с этим, каждому сетевому администратору необходимо уметь работать с ПО Windows Server, в том числе и с Active Directory – одним из основных инструментов системного администратора по управлению группами пользователей.

Active Directory - система служб каталогов, предназначенная для операционных систем класса MS Windows Server. Главная предоставляемая системой возможность - использование групповых политик для обеспечения единообразия настройки пользовательских рабочих станций, развертки программного обеспечения на множестве этих рабочих узлов, а также организованной удаленной установке на них обновлений операционной системы, используя службу обновлений Windows.

Проблема безопасности при использовании Active Directory стоит достаточно остро, так как в системе находится множество личных данных пользователей. Информация про каждого пользователя AD включает в себя: ФИО пользователя, его контактный номер, адрес электронной почты, домашний адрес, занимаемую должность, личную веб-страницу и т.д.

Очевидно, что представленная в службе каталогов Active Directory информация не должна быть доступна всем без исключения сотрудникам компании. Просмотр данных учетных записей пользователей AD возможен при использовании набора инструментов для средства автоматизации PowerShell – PowerTool.

Данный набор инструментов представляет собой командный интерфейс, предназначенный для работы с теми функциями Win32, которые обращаются к Active Directory. В системе AD присутствуют функции, позволяющие задать разрешения для разных групп доступа, очень похожие по функциям и строению на ACL-списки. Администраторы системы имеют право редактировать такие листы. Для редактирования необходимо в подменю AD Users And Computers зайти в расширенные настройки, а затем выбрать вкладку “Безопасность”. В этом меню возможно разрешить или запретить определенным группам права на чтение других учетных записей.

В данной статье рассмотрен способ сокрытия конфиденциальной информации, содержащейся в учетных записях пользователей различных групп Active Directory от других клиентов системы, не входящих в группу «Администраторы».

Представленное решение гарантирует администратору системы то, что данные пользователей, содержащиеся в их учетных записях, такие как: личные телефонные номера, адреса электронной почты, домашние адреса и т.д. не будут получены несанкционированными пользователями.

Стоит отметить, что несмотря на популярность ПО Windows Server и служб Active Directory в этих программных продуктах содержится множество уязвимостей, в том числе и те, которые невозможно закрыть стандартными средствами. Некоторые из таких уязвимостей будут рассмотрены в следующих статьях.