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

Отслеживание событий и управление информационными ресурсами операционной системы с помощью инструментария управления Windows

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 631 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Маркина Дениса Игоревича

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

В настоящее время проблема отслеживания событий и управления ресурсами в современных операционных системах набирает все большую и большую актуальность, так как на решении данных проблем основывается контроль над удаленными компьютерами локальных сетей, системное администрирование и обеспечение безопасности информационных систем.

В системах семейства Unix для решения проблемы отслеживания событий существуют специальные утилиты, такие как syslog, которая при вызове собирает всю возможную информацию о системе и записывает ее в определяемые пользователем журналы, но в основном сбор информации, отслеживание событий и управление ресурсами реализуется за счет комплексного использования тех или иных утилит при написании скриптов под конкретную задачу.

Сбор информации и отслеживание событий в операционных системах Microsoft Windows в основном производится стандартными утилитами, поставляемыми в комплекте с ОС. Примерами таких утилит могут послужить стандартные журналы Windows или множество оснасток консоли управления Microsoft (MMC). Сбор данных обычно происходит либо напрямую через графический интерфейс подобных утилит, либо с помощью сторонних продуктов, взаимодействующих с данными утилитами через интерфейс Windows API.

Большинство современных решений, осуществляющих взаимодействие с ресурсами системы, весьма требовательны к системе и зачастую не позволяют удаленно управлять ресурсами без клиентской части-агента, устанавливаемой непосредственно в целевой компьютер.

Целью данной дипломной работы было изучение инструментария управления Windows, анализ его возможностей и особенностей (в том числе и удаленного использования инструментария) и создание на основе полученных данных программного продукта для безопасного сбора информации о ресурсах

конкретного устройства под управлением ОС Windows, отслеживания значимых событий, происходящих в операционной среде устройства и управления базовыми функциями устройства.

Программный продукт, разработанный в рамках данной дипломной работы, осуществляет как локальное, так и удаленное взаимодействие с системой с помощью WMI и не требует дополнительной установки клиентской части. Подобным функционалом обладает комплекс средств серверных операционных систем, но разработанное решение позволяет удаленно взаимодействовать с разрозненным набором целей, не связанных в один домен.

Дипломная работа состоит из введения, 4 разделов, заключения, списка использованных источников и одного приложения, включающего в себя 8 фрагментов исходного кода программы, разработанной в рамках дипломной работы. Общий объем работы – 74 страницы, из них 43 страницы – основное содержание, включая 19 рисунков и список использованных источников из 20 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

Первый раздел дипломной работы носит название «WMI. Описание, принципы работы и возможности» и разделяется на четыре подраздела. Первый подраздел описывает технологию веб-ориентированного управления предприятием (WBEM) и общей информационной модели (CIM), на которых строится логика работы WMI. За счет данных технологий возможно унифицированное управление различными ресурсами системы, причем как программными, так и аппаратными. Данные технологии поддерживаются большинством производителей аппаратных элементов технических средств под управлением ОС семейства Windows.

Во втором подразделе приводится результат анализа структуры инструментария управления Windows, особенностей физического хранения данных. В данном подразделе описаны основные пространства имен, в которых хранятся классы и объекты построенного по объектно-ориентированному принципу WMI. Также в подразделе приводится типизация классов, составляющих основу инструментария и описание механизм взаимодействия с его объектами.

В третьем подразделе описан результат анализа механизмов обработки системных событий WMI. В инструментарии реализовано два основных метода отслеживания событий: временная и постоянная подписка. Временная подписка представляет собой вызов предварительно сконфигурированной функции, которая выполняется при наступлении заданного события. Постоянная подписка основывается на создании фильтров и так называемых «потребителей». Первые фиксируют системные события как изменение состояния объектов WMI, вторые описывают необходимую реакцию на событие, такую как запись определенных данных в журнал или текстовый файл.

Четвертый подраздел представляет собой описание процесса работы WMI с классами и объектами, а также основных директорий файловой системы и веток реестра, содержащих конфигурацию и классы WMI.

Второй раздел полностью описывает меры защиты, используемые как при локальном, так и удаленном взаимодействии с WMI. В ходе анализа механизмов защиты было выделено два основных механизма: контроль доступа к репозиториям на основе списков доступа (ACL) самой ОС и настройки распределенной общей модели компонентов (DCOM). Реализация модели DCOM используется при удаленном управлении WMI, взаимодействие происходит за счет передачи DCERPC пакетов, а механизмы олицетворения и аутентификации обеспечивают конфиденциальность, целостность и доступность передаваемой информации. Также в данном разделе приведен результат моделирования перехвата передаваемых WMI пакетов с их последующим анализом, наглядно показавший эффективность изученных мер защиты.

Третий раздел дипломной работы полностью посвящен прикладному использованию WMI и особенностей реализации программного продукта в рамках дипломной работы. В частности, описываются основные классы пространства имен, обеспечивающего взаимодействие с WMI на уровне разработки программных продуктов на языке C#. Также в данном разделе приводится полный список исследованных ресурсов ОС, взаимодействие с которыми было реализовано в рамках данной дипломной работы. В отдельный подраздел выделены особенности реализации множественного удаленного подключения и взаимодействия с WMI.

Полный обзор разработанного программного продукта под названием «WMIWatcher» приведен в четвертом разделе дипломной работы. В рамках данного раздела приводится поэтапное и тщательное описание работы с графическим интерфейсом программного продукта, снабженное большим количеством иллюстраций.

ЗАКЛЮЧЕНИЕ

Результатом исследования механизмов WMI и классов, содержащихся в пространствах имен WMI, проведенного в рамках дипломной работы, стал программный продукт «WMIWatcher», который позволяет осуществлять сбор информации о наиболее актуальных ресурсах нескольких компьютеров локальной сети под управлением ОС Windows, вести как централизованное, так и распределенное журналирование и сбор подробных сведений о тех или иных компонентах системы. Также «WMIWatcher» предоставляет возможность управлять функционированием целевых компьютеров и изменять конфигурации наиболее значимых аспектов системы. Но одной из важнейших особенностей разработанного продукта является реализация распределенного запуска скриптов. Данный спектр возможностей может быть полезен как для системного администратора, следящего за компонентами сети и осуществляющего распределенное управление ресурсами, так и для экспертов, за счет набора криминалистически важной информации. Также данный программный продукт может быть полезен при расследовании тех или иных инцидентов, произошедших в локальной сети, так как с помощью данных, фиксируемых «WMIWatcher» возможно выявить сведения, прямо или косвенно касающиеся расследуемого инцидента.

Так как технология WMI несправедливо считается устаревающей, основные продукты, использующие инструментарий, это скрипты (зачастую написанные на Visual Basic), требующие определенного навыка системного программирования и знания структуры и принципов работы WMI.

Одним из немногих решений, использующих инструментарий, является средство управления ИТ-активами «iTMan», разработанное одноименной российской компанией. Но основной задачей, выполняемой данным программных продуктом, является сбор сведений о системе для инвентаризации и учета активов, а WMI является одной из нескольких используемых технологий. Задачей же, обозначенной в рамках дипломной

работы, является реализация не только сбора информации, но и отслеживания событий и управления ресурсами ОС, то есть программный продукт «WMIWatcher» акцентирует внимание только на WMI и позволяет шире использовать его возможности.

Разработанное решение позволяет абстрагироваться от работы непосредственно с компонентами WMI и эффективно использовать имеющийся функционал. Наиболее эффективно программный продукт может быть использован при администрировании локальных сетей под управлением ОС семейства Windows с предварительно настроенными правами доступа к WMI, корректной конфигурацией межсетевых экранов, не допускающих блокирование пакетов WMI. Правильная настройка параметров безопасности «WMIWatcher» в зависимости от защищенности сети в свою очередь является залогом защищенного и эффективного использования механизмов WMI.

Поставленные задачи в дипломной работе были решены в полной мере, инструментарий управления Windows был исследован, программный продукт, взаимодействующий с WMI и выполняющий определенные действия разработан. Дополнительно было проведено тестирование защищенности разработанного продукта и системы защиты WMI в целом. Результаты тестирования отражены в дипломной работе.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Руссинович, М. Внутри Windows Management Interface / М. Руссинович // Windows 2000 Magazine. 2000. № 3. С. 37-45.

2 Спецификация WBEM [Электронный ресурс] // Компьютерный информационный портал [Электронный ресурс]. URL: http://www.oszone.net/672/ (дата обращения: 15.04.2015). Загл. с экрана. Яз. рус.

3 Людоговский, А. Введение в WMI [Электронный ресурс] / А. Людоговский // Разработка скриптов [Электронный ресурс]. URL: http://www.script-coding.com/WMI.html (дата обращения: 25.06.2015). Загл. с экрана. Яз. рус.

4 Леонтьев, К. Вы все еще не используете WMI? Часть I / К. Леонтьев // Системный администратор. 2006. № 1(38). С. 4-11.

5 Бочкарев, В. System Engineering - Администрирование с помощью WMI [Электронный ресурс] / В. Бочкарев // System Engineering [Электронный ресурс]. URL: http://www.sysengineering.ru/Administration/AdministrationUsingWMI.aspx (дата обращения: 19.09.2015). Загл. с экрана. Яз. рус.

6 Леонтьев, К. Узнай секреты WMI: события и провайдеры / К. Леонтьев // Системный администратор. 2006. № 3(40). С. 15-35.

7 Попов, А. Администрирование Windows с помощью WMI и WMIC / А. Попов. СПб. : БХВ-Петербург, 2004. 752 с.

8 Соломон, М. Д. Внутреннее устройство Microsoft Windows: Windows Server 2003, Windows XP и Windows 2000. Мастер-класс / М. Д. Соломон. М. : Русская Редакция, 2005. 856 с.

9 Модель COM/DCOM [Электронный ресурс] // Интерфейс Ltd. [Электронный ресурс]. URL: http://www.interface.ru/home.asp?artId=4219 (дата обращения: 12.03.2016). Загл. с экрана. Яз. рус.

10 [MS-DCOM]: Distributed Component Object Model (DCOM) Remote Protocol Specification [Электронный ресурс] // MSDN – сеть разработчиков Майкрософт [Электронный ресурс]. URL: https://msdn.microsoft.com/library/cc201989.aspx (дата обращения: 04.05.2016). Загл. с экрана. Яз. англ.

11 Securing a Remote WMI Connection [Электронный ресурс] // MSDN – сеть разработчиков Майкрософт [Электронный ресурс]. URL: https://msdn.microsoft.com/ru-ru/library/aa393266(v=vs.85).aspx (дата обращения: 01.07.2016). Загл. с экрана. Яз. англ.

12 Secure Password Strings in Java and C# [Электронный ресурс] // nVisium: Your partner in building secure applications [Электронный ресурс]. URL: https://nvisium.com/blog/2016/03/31/secure-password-strings/ (дата обращения: 01.09.2016). Загл. с экрана. Яз. англ.

13 Gittler, F. The DCE Security Service / F. Gittler, A. C. Hopkins // Hewlett-Packard Journal. 1995. Vol. 46, № 6. P. 41-48.

14 Wireshark User's Guide [Электронный ресурс] // Wireshark. Go Deep. [Электронный ресурс]. URL: https://www.wireshark.org/docs/wsug_html_chunked/ (дата обращения: 22.09.2016). Загл. с экрана. Яз. англ.

15 Kong, M. M. DCE: An Environment for Secure Client/Server Computing / M. M. Kong // Hewlett-Packard Journal. 1995. Vol. 46, № 6. P. 41-48.

16 Timkov, A. M. How to Avoid Information Disclosure when Managing Windows with WMI / A. M. Timkov // GSEC Gold Certification. 2007. 85 p.

17 Класс ConnectionOptions Connection [Электронный ресурс] // MSDN – сеть разработчиков Майкрософт [Электронный ресурс]. URL: https://msdn.microsoft.com/ru-ru/library/ system.management.connectionoptions(v=vs.110).aspx (дата обращения: 23.11.2016). Загл. с экрана. Яз. рус.

18 Людоговский, А. WMI: управление процессами [Электронный ресурс] / А. Людоговский // Разработка скриптов [Электронный ресурс]. URL: http://www.script-coding.com/WMI_Processes.html (дата обращения: 23.11.2016). Загл. с экрана. Яз. рус.

19 System.Management – пространство имен [Электронный ресурс] // MSDN – сеть разработчиков Майкрософт [Электронный ресурс]. URL: https://msdn.microsoft.com/ru-ru/library/system.management(v=vs.110).aspx (дата обращения: 27.11.2016). Загл. с экрана. Яз. рус.

20 WMI Classes (Windows) [Электронный ресурс] // MSDN – сеть разработчиков Майкрософт [Электронный ресурс]. URL: http://msdn.microsoft.com/ru-ru/windows/desktop/aa394554(v=vs.85) (дата обращения: 01.12.2016). Загл. с экрана. Яз. рус.