Министерство образования и науки Российской Федерации

Санкт-Петербургский Политехнический Университет Петра Великого

—

Институт прикладной математики и механики

Кафедра «Информационная безопасность компьютерных систем»

**ЛАБОРАТОРНАЯ РАБОТА № 4**

**«ИССЛЕДОВАНИЕ ТЕХНОЛОГИИ WINDOWS MANAGEMENT**

**INSTRUMENTATION»**

по дисциплине «Безопасность современных информационных технологий»

Выполнил

студент гр. 33636/1 Валиева К.М.

<подпись>

Преподаватель Иванов Д.В.

<подпись>

Санкт-Петербург

2018

**1. Цель работы**

Получить навыки работы с инструментарием управления Windows.

**2. Задача**

Написать клиент-серверное приложение под ОС Windows 7-10. Программа-клиент должна запрашивать по интерфейсу WMI информацию об удаленной системе, на которой работает программа-сервер. Возможна архитектура приложения, где роль сервера играет

WMI API.

**3. Ход работы**

В ходе работы было реализовано приложение, в котором в качестве сервера выступает WMI API. Клиент может получать такую информацию об удаленной системе, как имя операционной системы, установленные приложения, название антивируса, информацию о загрузочном устройстве, антишпионском ПО, производитель материнской платы, название BIOS.

В данном приложении уровень олицетворения принимает значение «имперсонация», то есть WMI-объект имеет такие же права, какие имеет пользователь.

Кроме того, производится проверка подлинности и целостности всех пакетов к компьютеру-цели команды, заголовки и содержимое пакетов подписываются и шифруются.

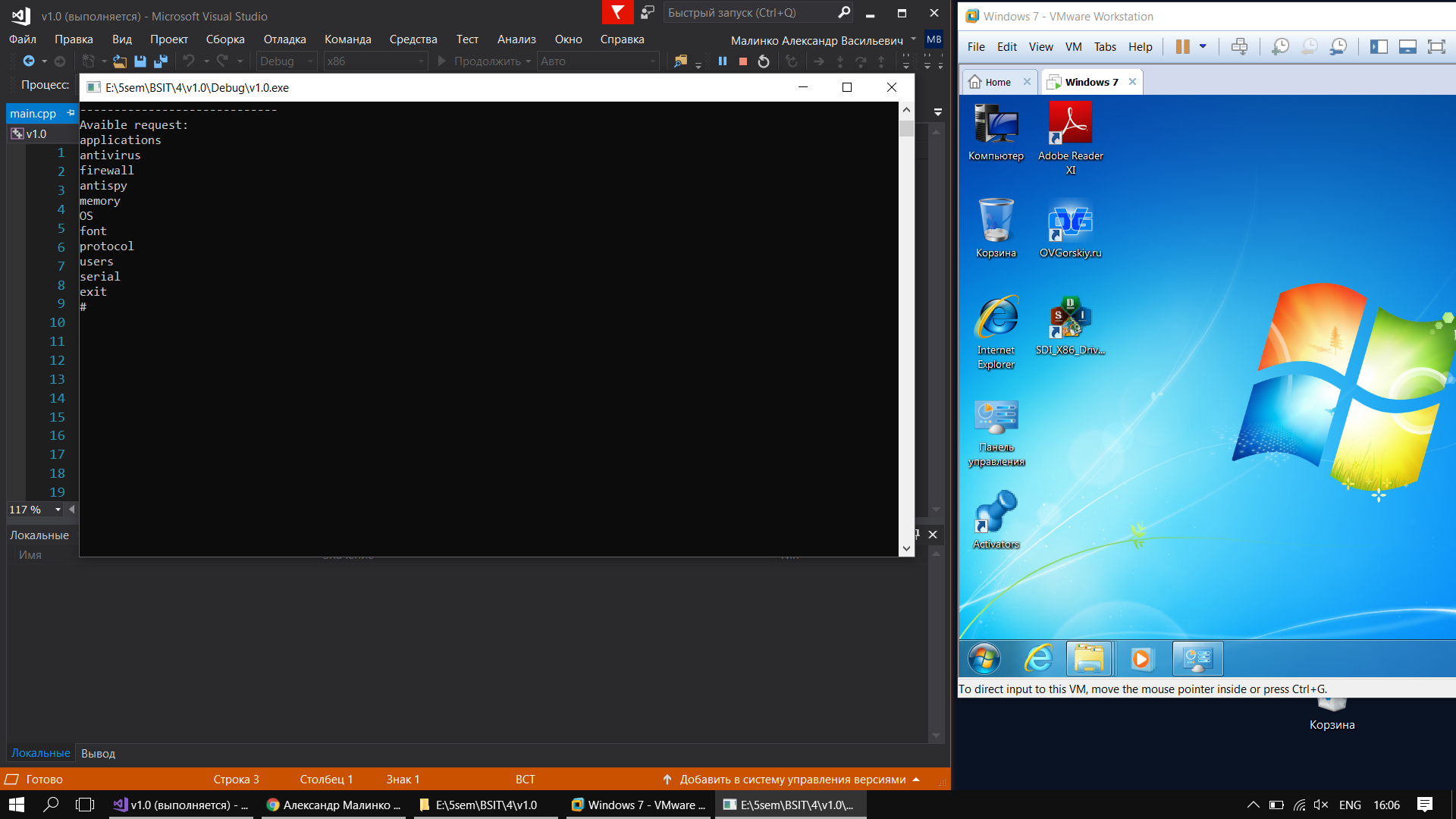


Рисунок 1. Интерфейс приложения.

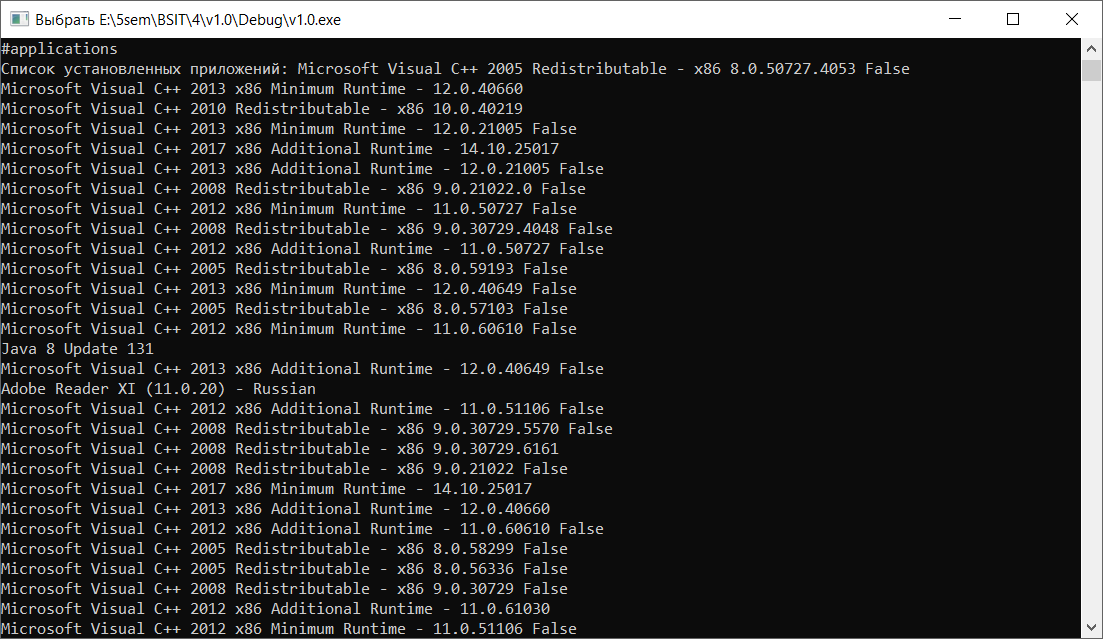


Рисунок 2. Запрос списка установленных приложений.

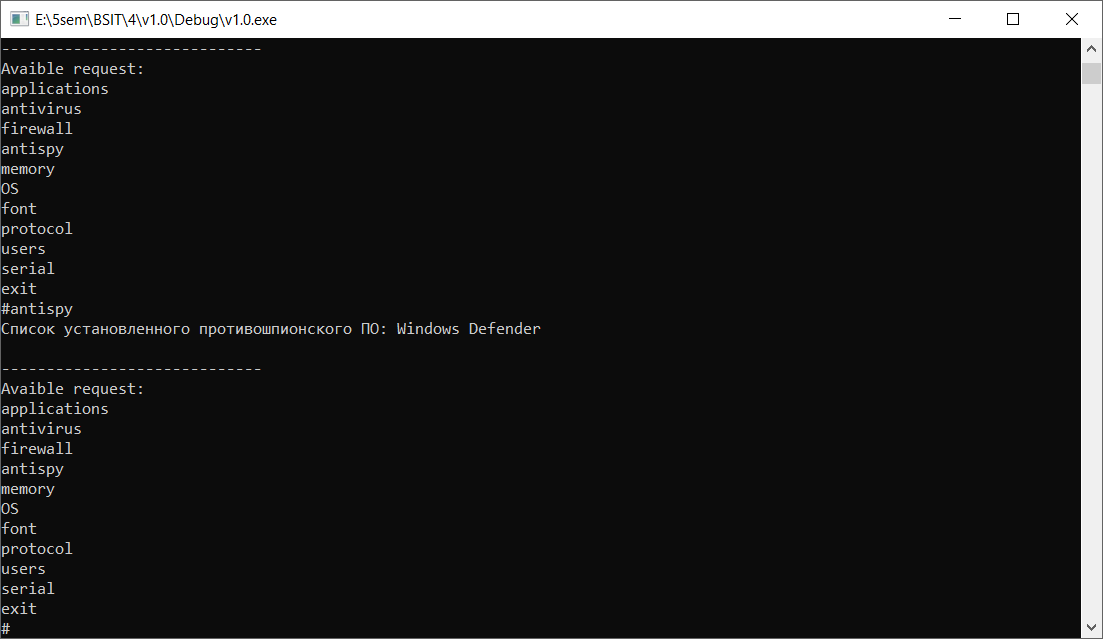


Рисунок 3. Запрос списка установленного противошпионского ПО

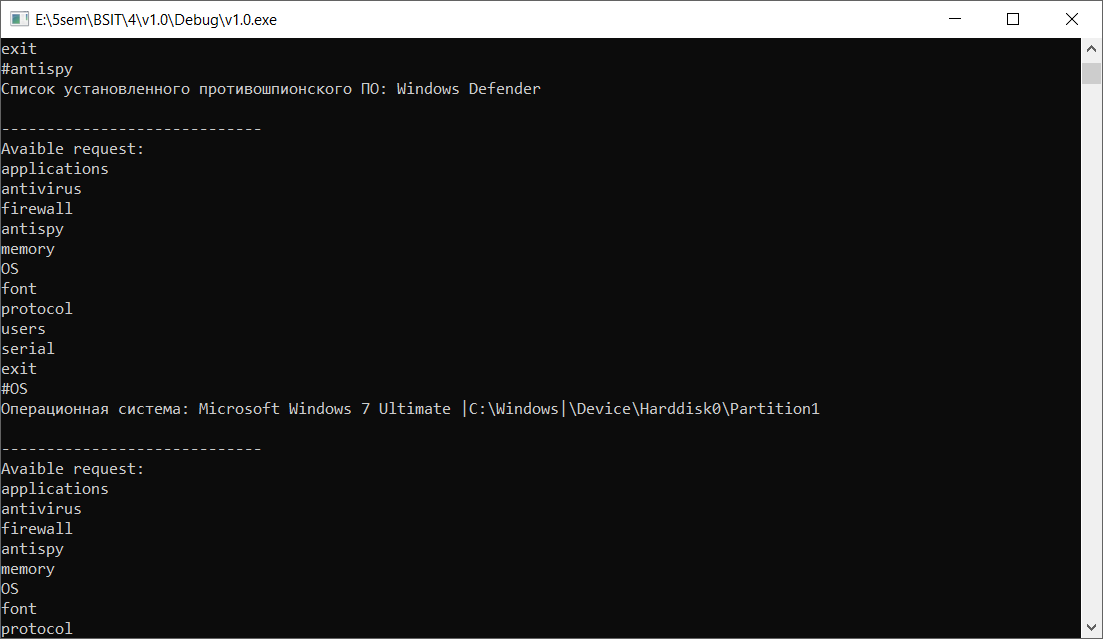


Рисунок 4. Запрос имени операционной системы.

**4. Контрольные вопросы**

*1) Что такое WMI и зачем данный инструмент нужен?*

Windows Management Instrumentation (WMI) — это одна из базовых технологий для

централизованного управления и слежения за работой различных частей компьютерной

инфраструктуры под управлением платформы Windows.

Технология WMI — это расширенная и адаптированная под Windows реализация

стандарта WBEM, в основе которого лежит идея создания универсального интерфейса

мониторинга и управления различными системами и компонентами распределенной

информационной среды предприятия с использованием объектно-ориентированных

идеологий и протоколов HTML и XML.

*2) Какие основные возможности у WMI?*

А) Экземпляры классов могут генерировать события, к которым можно подписываться.

При наступлении события WMI автоматически создает экземпляр того класса, которому

соответствует это событие. Такой механизм удобно использовать для выполнения

определенной команды при наступлении определенного события, то есть следить за

состоянием объектов операционной системы.

Б) Общая безопасность в WMI реализуется на уровне операционной системы, а

дополнительная политика безопасности основана на уровнях пространств имен и протокола DCOM.

В) При помощи WMI можно управлять запущенными процессами и сервисами, изменять настройки реестра и т.д.

*3) Опишите архитектуру и принципы работы WMI.*

WMI состоит из следующих частей:

\* Менеджер объектов CIM (Common Information Model Object Manager, CIMOM), который обеспечивает обработку всех запросов конечных приложений к WMI и доставку информации от WMI к конечным приложениям. Все провайдеры WMI (см. ниже) должны быть зарегистрированы с помощью CIMOM для правильного перенаправления полученных от конечного приложения запросов к нужному

провайдеру. Функциональность CIMOM обеспечивает файл winmgmt.exe, который находится в каталоге %SystemRoot%\System32\Wbem\. Этот файл запускается как сервис.

\* Репозиторий (хранилище классов) CIM. Объекты-экземпляры таких классов создаются провайдером WMI (см. ниже) по запросу потребителя. В Windows Server 2003 и Windows XP репозиторий физически располагается в каталоге %SystemRoot%\System32\Wbem\Repositiry\FS\ в файлах objects.data (репозиторий), index.btr (индексный файл), index.map и object.map (файлы контроля над транзакциями). В более ранних версиях Windows репозиторий располагается в файле cim.rep.

\* Провайдеры WMI, которые скрывают детали внутренней реализации управляемых объектов, позволяя CIMOM обращаться к этим объектам единообразно, используя WMI API. Фактически провайдеры являются COM-серверами, которые представлены dll-библиотеками в каталоге %SystemRoot%\System32\Wbem\. WMI включает множество встроенных провайдеров, которые предназначены для получения данных из различных источников, например, журналов событий, системного реестра и т.д.

\* Библиотека поддержки сценариев (WMI scripting library), которая располагается в файле wbemdisp.dll в каталоге %SystemRoot%\System32\Wbem\.

В этой технологии все данные ОС представлены как объекты и их свойства и методы. Все классы группируются в пространства имен, которые иерархически упорядочены

и логически связаны друг с другом по определенной технологии или области управления.

В WMI имеется одно корневое пространство имен Root, которое в свою очередь имеет 4

подпространства: CIMv2, Default, Security и WMI.

Классы имеют свойства и методы и находятся в иерархической зависимости друг от

друга, то есть классы-потомки могут наследовать или переопределять свойства классов родителей,

а также добавлять свои свойства.

Свойства классов используются для однозначной идентификации экземпляра класса

и для описания состояния используемого ресурса. Обычно все свойства классов доступны

только для чтения, хотя некоторые из них можно модифицировать определенным методом.

Методы классов позволяют выполнить действия над управляемым ресурсом.

**5. Выводы**

В ходе выполнения данной лабораторной работы были получены навыки работы с технологией WMI

**6. Листинг.**