МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САМАРСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА С.П. КОРОЛЕВА»
(САМАРСКИЙ УНИВЕРСИТЕТ)

М.Е. БУРЛАКОВ, М.Н. ОСИПОВ

КОНТРОЛЬ ЗАЩИЩЕННОСТИ ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА. ЛАБОРАТОРНЫЙ ПРАКТИКУМ

Рекомендовано редакционно-издательским советом федерального государственного автономного образовательного учреждения высшего образования «Самарский национальный исследовательский университет имени академика С.П. Королева» в качестве практикума для обучающихся по основным образовательным программам высшего образования по направлению подготовки 10.03.01 Информационная безопасность и специальностям 10.05.01 Компьютерная безопасность, 10.05.03 Информационная безопасность автоматизированных систем

САМАРА
Издательство Самарского университета
2022

УДК 004.9(075)
ББК 32.973я7
Б915

Рецензенты: канд. физ-мат. наук, доц. А.С. Луканов
канд. техн. наук, зав. лаб. Г.В. Богомолов

Бурлаков, Михаил Евгеньевич

Б915 Контроль защищенности локальных вычислительных сетей от несанкционированного доступа. Лабораторный практикум : практикум / *М.Е. Бурлаков. М.Н. Осипов*. – Самара : Издательство Самарского университета, 2022. – 116 с. : с ил.

ISBN 978-5-7883-1749-6

Данный практикум позволяет расширить практические навыки обучающихся в области защиты информации от несанкционированного доступа в компьютерных системах и сетях. Представлены лабораторные работы по контролю защищенности локальных вычислительных сетей от несанкционированного доступа.

Представленный в практикуме материал соответствует требованиям ФГОС ВО по направлениям подготовки 10.03.01 Информационная безопасность и специальностям 10.05.01 Компьютерная безопасность, 10.05.03 Информационная безопасность автоматизированных систем.

Подготовлено на кафедре безопасности информационных систем.

УДК 004.9(075)
ББК 32.973я7

ISBN 978-5-7883-1749-6

СОДЕРЖАНИЕ

Основные термины и определения 4
Введение 9
Лабораторная работа № 1 14
Лабораторная работа № 2 59
Лабораторная работа № 3 62
Лабораторная работа № 4 72
Лабораторная работа № 5 75
Список использованных источников 113

ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Основные термины и определения даны на основании утверждённых нормативных документов организаций ответственных за их разработку и контроль [1-9].

Информация, Information – сведения (сообщения, данные) независимо от формы их представления.

Конфиденциальность (информации [ресурсов автоматизированной информационной системы]), Confidentiality – состояние информации [ресурсов автоматизированной информационной системы], при котором доступ к ней [к ним] осуществляют только субъекты, имеющие на него право.

Целостность (информации [ресурсов автоматизированной информационной системы]), Integrity – состояние информации [ресурсов автоматизированной информационной системы], при котором ее [их] изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Доступность (информации [ресурсов автоматизированной информационной системы]), Availability – состояние информации [ресурсов автоматизированной информационной системы], при котором субъекты, имеющие право доступа, могут реализовать их беспрепятственно.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

Информационная безопасность объекта информатизации – состояние защищенности объекта информатизации, при котором обеспечивается безопасность информации и автоматизированных средств ее обработки.

Защита информации (ЗИ), Protection of information – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Система защиты информации (СЗИ), System of protection of information – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.

Правовая защита информации – защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

Техническая защита информации (ТЗИ) – защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

Криптографическая защита информации – защита информации с помощью ее криптографического преобразования.

Физическая защита информации – защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

Средство вычислительной техники (СВТ), Computer – совокупность технических устройств и программ, обеспечивающих их функционирование, способных функционировать самостоятельно или в составе других систем.

Автоматизированная система (АС) – система, состоящая из комплекса средств автоматизации, реализующего информационную технологию выполнения установленных функций, и персонала, обеспечивающего его функционирование.

Автоматизированное рабочее место (АРМ) – программно-технический комплекс АС, предназначенный для автоматизации деятельности определенной категории пользователей или определенного вида деятельности.

Вычислительная сеть (ВС), Computer network – совокупность средств вычислительной техники. соединенных между собой, обеспечивающих передачу данных посредством телекоммуникационной связи.

Угроза (безопасности информации), Threat – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения конфиденциальности, доступности и (или) целостности информации.

Источник угрозы безопасности информации – субъект, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Уязвимость (автоматизированной информационной системы), Vulnerability – недостаток или слабое место в автоматизи-

рованной информационной системе, которые могут быть условием реализации угрозы безопасности обрабатываемой в ней информации.

Компьютерная атака – целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств.

Доступ к информации (Доступ), Access to information – ознакомление с информацией, ее обработка, в частности, копирование модификация или уничтожение информации.

Субъект доступа (Субъект), Access subject – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Объект доступа (Объект), Access object – единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа

Правила разграничения доступа (ПРД), Security policy – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа

Санкционированный доступ к информации, Authorized access to information – доступ к информации, не нарушающий правила разграничения доступа

Несанкционированный доступ к информации (НСД), Unauthorized access to information – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Защита информации от несанкционированного доступа (ЗИ от НСД), Protection of information from unauthorized access – предотвращение получения защищаемой информации заинтересо-

ванными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

Система защиты информации от несанкционированного доступа (СЗИ НСД), System of protection from unauthorized access to information – комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации в автоматизированных системах

Средство защиты от несанкционированного доступа (Средство защиты от НСД), Protection facility – программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа.

Мониторинг безопасности информации – постоянное наблюдение за процессом обеспечения безопасности информации в информационной системе с целью установить его соответствие требованиям безопасности информации.

ВВЕДЕНИЕ

В настоящий момент, для обнаружения потенциальных информационных угроз и элементов несанкционированного доступа в вычислительных сетях существует широкий перечень мер и методов, как организационно-правового, так и технического характеров. Среди технических существуют четко определенные классы и системы, такие как: комплексные системы управления безопасностью, пассивные и активные средства мониторинга доступности сетевых ресурсов, системы обнаружения и предотвращения вторжений и т.д.

Ко всем информационным ресурсам, с которыми работает информационная вычислительная система, в обязательном порядке предъявляется требование конфиденциальности, целостности и доступности. Обеспечение этих требований является первостепенным в задачах обеспечения информационной безопасности. Несанкционированный доступ к информационным ресурсам, располагающимся в вычислительных системах и на сетевых ресурсах, как правило имеет целью нарушение этих требований. Следовательно, несанкционированный доступ может нанести существенный ущерб объекту информатизации. В связи с этим одной из важнейших задач обеспечения информационной безопасности является задача максимально возможного снижения угрозы несанкционированного доступа.

Информационные угрозы в вычислительных системах можно классифицировать следующим образом:

- перехват и подмена трафика;
- несанкционированный доступ к информационным ресурсам;
- подбор пароля;
- взлом систем защиты и администрирования.

- отказ в обслуживании (DoS);
- IP-спуфинг;
- атака на уровне приложений;
- сканирование сетей или сетевая разведка;
- использование отношений доверия в сети;

Обеспечение квалифицированной защиты информации в локальных вычислительных сетях (ЛВС) предполагает:

- обеспечение безопасности информации в ЛВС – это процесс:
  - непрерывный, заключающийся в систематическом контроле защищённости, выявлении узких и слабых мест в системе защиты;
  - комплексный, предполагающий использование всего арсенала имеющихся средств зашиты, как организационно-правовых, так и технических средств;
  - плановый, предполагающий постоянное совершенствование и развитие системы защиты;
- надлежащую профессиональную подготовку пользователей;
- соблюдение сотрудниками правил пользования информацией ограниченного пользования;
- учитывать, что ни одна система защиты информации не считается абсолютно защищённой.

ФСТЭК России принял к руководству документ устанавливающий классификацию средств вычислительной техники (СВТ) по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

Согласно документу [10] устанавливается семь классов защищенности СВТ от НСД к информации. Самый низкий класс – седьмой, самый высокий – первый.

Классы подразделяются на четыре группы, отличающиеся качественным уровнем защиты:

– первая группа содержит только один седьмой класс;
– вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;
– третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;
– четвертая группа характеризуется верифицированной защитой и содержит только первый класс.

Выбор класса защищенности СВТ, создаваемых на базе защищенных СВТ, зависит от грифа секретности обрабатываемой информации ограниченного доступа, условий эксплуатации и расположения объектов вычислительной системы.

Кроме того, ФСТЭК России принял к руководству документ деления автоматизированных систем (АС) на соответствующие классы по условиям их функционирования с точки зрения защиты информации. Дифференциация подхода к выбору методов и средств защиты определяется важностью обрабатываемой информации, различием АС по своему составу, структуре, способам обработки информации, количественному и качественному составу пользователей и обслуживающего персонала. Выбор класса АС производится заказчиком и разработчиком с привлечением специалистов по защите информации. Устанавливается девять классов защищенности АС от НСД к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности информации.

Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса – 3Б и 3А. Вторая группа включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях

различного уровня конфиденциальности. Группа содержит два класса – 2Б и 2А. Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов – 1Д, 1Г, 1В, 1Б и 1А [11]. Самый низкий класс – девятый, самый высокий – первый.

Защита информации от НСД является составной частью общей проблемы обеспечения безопасности информации. Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприятиями по специальной защите основных и вспомогательных средств вычислительной техники, средств и систем связи от технических средств разведки и промышленного шпионажа [12].

Вопросы в области защиты ЛВС программными средства от угроз лежат в плоскости разработки и внедрения средств проактивной защиты и активного аудита. Программные средства позволяют решить несколько из обозначенных выше проблем путем использования технологий интеллектуального анализа данных, модульности, масштабируемости и многоагентности подхода.

Программные средства защиты информации включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др. Преимущества программных средств − универсальность, гибкость, надежность, простота установки, способность к модификации и развитию. Недостатки − ограниченная функциональность сети, использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств) [13].

Представленное учебное пособие, направлено на выработку практических навыков по контролю защищенности локальных вы-

числительных сетей от несанкционированного доступа применением программных средств.

При выполнении практических заданий первой части предполагается рассмотрение следующих вопросов. Изучение средств инвентаризация актуального состава технических и программных средств объекта информатизации с использованием штатных средств операционной системы и программного обеспечения, позволяющее актуализировать состав защищаемых объектов (лабораторная работа № 1). Выработка навыков сравнительного анализа при поиске отличий реально полученной информации по результатам инвентаризации от информации, заявленной в исходных данных на объекте информатизации (лабораторная работа № 2). Изучение вопросов, связанных с контролем уязвимости на уровне сети (лабораторная работа № 3). Ознакомление с принципами контроля уязвимостей на уровне операционных систем и прикладного ПО (лабораторная работа № 4), а также контроля уязвимостей на уровне системы управления базами данных (лабораторная работа № 5).

ЛАБОРАТОРНАЯ РАБОТА № 1

Инвентаризация актуального состава технических и программных средств объекта информатизации с использованием штатных средств операционной системы и программного обеспечения

Цель: Проведение работ по инвентаризации актуального состава технических и программных средств объекта информатизации с использованием штатных средств операционной системы и программного обеспечения. Выработка навыков по работе с автоматизированными средствами инвентаризации.

Описание программного обеспечения

Назначение программы «Агент инвентаризации»

«Агент инвентаризации» предназначен для автоматизированного сбора информации об аппаратном и программном обеспечении АРМ. При этом выполняются следующие функции:

– сбор информации об аппаратных и программных средствах в составе АРМ;

– сохранение полученной информации и возможность просмотра ее в будущем;

– генерация отчетов на основе полученной информации;

– взаимодействие с другими программами (за счет открытого и документированного формата входных и выходных данных).

Условия применения:

Требования к техническим средствам:

Рекомендуемая конфигурация ПЭВМ:

– процессор – Intel Pentium и выше;

– ОЗУ – 256 МБ;

– на ЖМД не менее 100 Мбайт дискового пространства.

При улучшении конфигурации «Агент инвентаризации» выполняется быстрее.

Требования к программному обеспечению:

«Агент инвентаризации» работает под управлением ОС Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016. Дополнительных требований к программному обеспечению не предъявляется. При выполнении программы необходимо находиться в системе с правами администратора.

Входные и выходные данные.

Входными данными «Агента инвентаризации» являются:

– указываемый пользователем требуемый состав получаемой информации;

– указываемые пользователем параметры выполнения программы.

– Выходными данными «Агента инвентаризации» являются:

– информация об аппаратном и программном обеспечении, полученная в ходе работы программы и сохраненная в файле;

– отчеты на основе информации, полученной в ходе работы программы (в формате HTML).

Состав и функции программы.

Программа состоит из нескольких модулей, каждый из которых реализован в виде отдельного файла (табл. 1.1).

Таблица 1.1. **Описание модулей**

Имя файла	Описание
Agent.exe	Модуль графического интерфейса для работы с программой.
sysinfo.exe	Основной исполняемый модуль
sysinfo.dll	Библиотека функций по сбору информации о системе
sysinfo9x.dll	Библиотека функций по сбору информации о системе
SysInfo.sys	Драйвер, используемый для непосредственного доступа к оборудованию
sysinfo1.dat sysinfo2.dat	Файлы данных, содержащие информацию, используемую при декодировании идентификаторов PCI устройств

Сбор системной информации выполняется основным исполняемым модулем. Модуль графического интерфейса используется для управления запуском основного исполняемого модуля, отображения результатов работы программы в удобной для пользователя форме и генерации отчетов.

Выполняемые функции:

Сбор информации о программном и аппаратном обеспечении. Во время работы «Агент инвентаризации» получает информацию о программном и аппаратном обеспечении в составе АРМ, а также информацию о настройках аппаратного и программного обеспечения. Полученная информация сохраняется в файле для дальнейшего использования.

Генерация отчетов. На основе полученной информации может быть создан отчет в формате HTML. Состав отчета определяется пользователем. Генерация отчетов выполняется с помощью модуля графического интерфейса.

Взаимодействие с другими программами. Работа основного исполняемого модуля управляется с помощью параметров командной строки, что позволяет другим программам автоматически запускать его, используя заранее сформированную строку параметров. Формат выходных результатов оптимизирован для загрузки в базу данных.

Выполнение программы.

Для установки «Агента инвентаризации» нужно скопировать файлы программы в любой каталог на жестком диске. Никаких дополнительных действий по установке не требуется.

Порядок выполнения зависит от поставленной задачи. Для запуска программы из командной строки нужно выполнить файл sysinfo.exe с указанием требуемых параметров работы. Для запуска программы с использованием графического интерфейса используется файл Agent.exe

Выполнение с использованием графического интерфейса.

Модуль графического интерфейса предназначен для упрощения взаимодействия между пользователем и основным исполняемым модулем. Основными функциями модуля графического интерфейса являются: запуск основного исполняемого модуля для сбора информации, просмотр результатов работы и генерация отчетов. Также он может быть использован для формирования командной строки запуска основного исполняемого модуля, если «Агент инвентаризации» применяется как часть программного комплекса.

Главное окно программы имеет следующие элементы (рис. 1.1):

- Строка меню
- Панель инструментов
- Дерево объектов
- Список свойств текущего объекта
- Строка состояния

Меню дублирует все функции, доступные с панели инструментов. На панели инструментов расположены следующие кнопки (табл. 1.2):

Таблица 1.2. **Кнопки панели инструментов**

	Загрузка и просмотр результатов, полученных при предыдущих запусках программы
	Сбор системной информации
	Создание отчета

Кнопки панели инструментов имеют всплывающие подсказки, появляющиеся при задержке курсора мыши над ними. Если команда, соответствующая кнопке, недоступна, кнопка также недоступна и отображается в сером цвете.

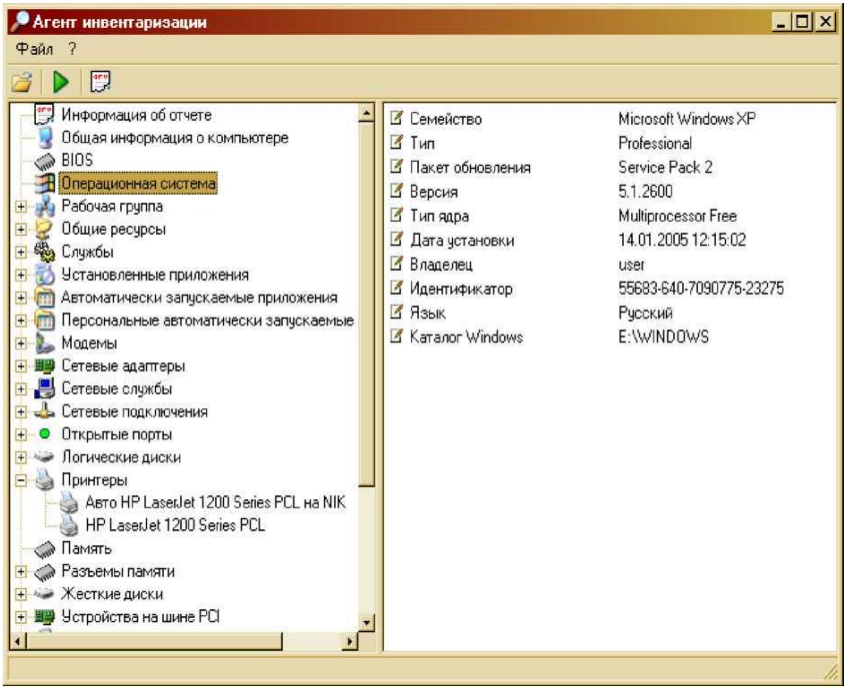


Рис. 1.1. Главное окно программы

Вся полученная информация отображается в виде набора объектов, каждый из которых имеет собственный набор свойств. Перечень объектов отображается в дереве объектов (с разбиением по классам). Справа, в списке свойств, отображаются свойства текущего (выделенного в дереве) объекта.

Строка состояния отображает информацию о текущей выполняемой операции.

Сбор информации.

Для сбора информации о системе используется кнопка панели инструментов. После ее нажатия на экране появляется диалоговое окно, в котором можно за несколько шагов настроить параметры сбора информации.

Шаг 1. Настройка параметров работы программы (рис. 1.2).

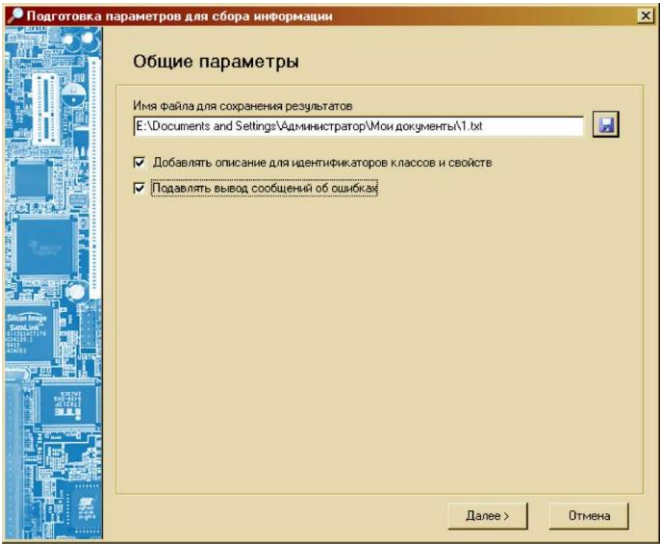


Рис. 1.2. Настройка параметров работы программы

На этом шаге устанавливаются основные параметры, определяющие работу программы. Прежде всего, это имя файла для сохранения результатов (указывается с помощью кнопки). Также можно включить режимы «Добавлять описание для идентификаторов классов и свойств» (добавляет параметр /descr к строке запуска основного исполняемого модуля) и «Подавлять вывод сообщений об ошибках» (параметр /silent).

Шаг 2. Определение состава получаемой информации (рис. 1.3).

На этом шаге определяется, какая информация должна быть получена в ходе работы программы. При этом используются групповые параметры. Если требуется детально определить состав получаемой информации, то нужно выделить вариант «Выбрать вручную».

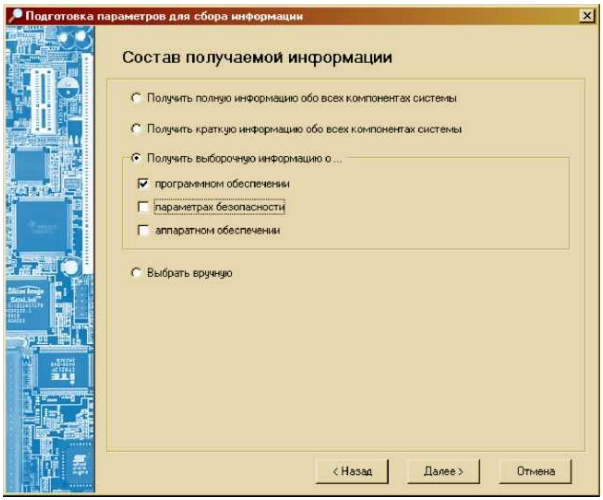


Рис. 1.3. Определение состава получаемой информации

Шаг 3. Определение состава получаемой информации (дополнительно) **(рис. 1.4).**

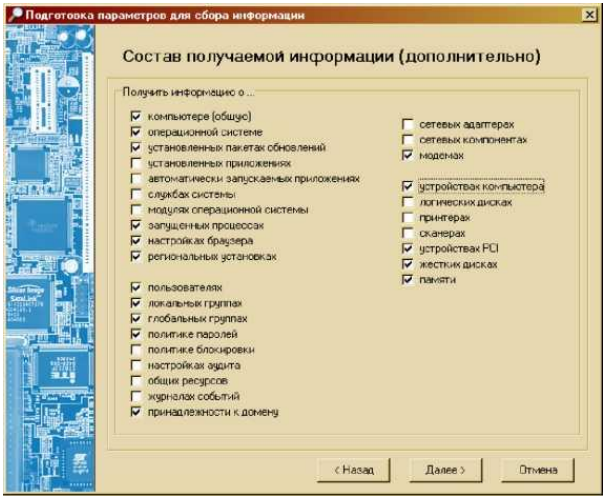


Рис. 1.4. Определение состава получаемой информации (дополнительно)

Этот шаг выполняется, только если был выбран вариант «Выбрать вручную» на предыдущем шаге. Пользователю предоставляется возможность более точно определить состав получаемой информации. Для удобства можно использовать функции «Выделить все» и «Снять все отметки», доступные через контекстное меню.

Шаг 4. Настройка параметров фильтрации журналов аудита (рис. 1.5 и рис. 1.6).

Этот шаг выполняется только в том случае, если в ходе работы программы должна быть получена информация из журналов аудита.

С целью сокращения объема выходных данных, в «Агенте инвентаризации» предусмотрена возможность фильтрации записей системных журналов событий.

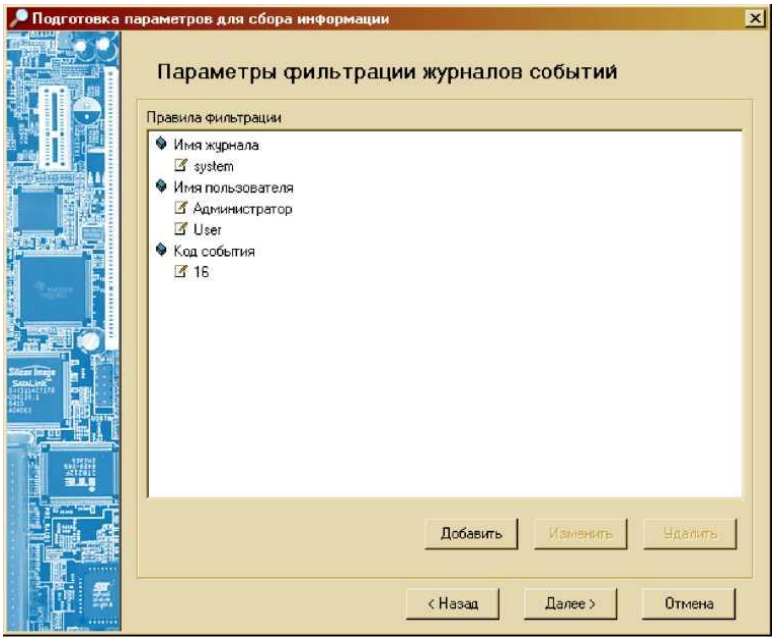


Рис. 1.5. Параметры фильтрации журналов событий

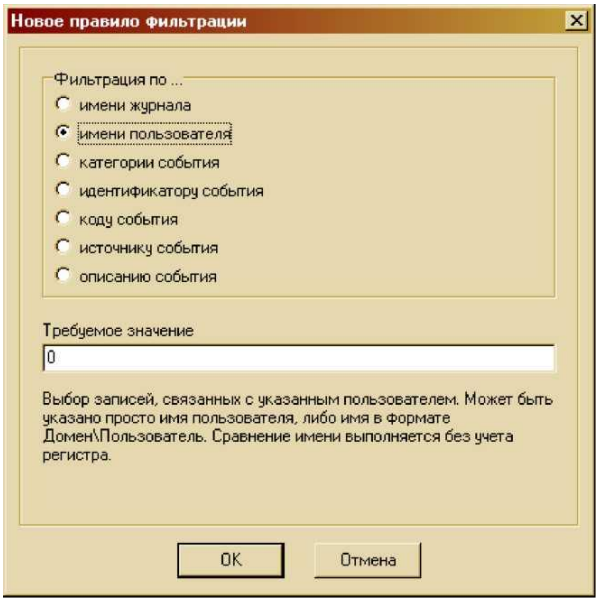


Рис. 1.6. Создание правила фильтрации журнала событий

Для добавления правила фильтрации нужно нажать кнопку «Добавить», после чего на экране появится окно настройки параметров создаваемого правила. В нем указывается, к какому из полей записи в журнале событий применяется правило, и требуемое значение поля. В дальнейшем правила фильтрации можно будет удалять и редактировать.

Анализ полей «Категория», «Источник» и «Описание» проводится с помощью регулярных выражений. Это дает возможность гибко описывать требования к значению полей. В простейшем случае, если не используются управляющие символы, удовлетворяющими требованию считаются все строки, содержащие заданную подстроку. Более подробную информацию можно найти в документации по регулярным выражениям.

Если используются несколько условий, то они объединяются следующим образом: однотипные условия объединяются с помо-

щью логического оператора ИЛИ, затем результаты объединения однотипных условий объединяются с помощью логического оператора И. Запись признается соответствующей требованиям, если она удовлетворяет хотя бы одному условию каждого типа.

Шаг 5. Завершение формирования параметров (рис. 1.7).

На этом этапе формирование параметров уже завершено, и на экран выводится командная строка, которая будет использована при запуске основного исполняемого модуля. Эта строка может быть скопирована и использована в дальнейшем для запуска основного исполняемого модуля без использования графического интерфейса. По нажатию кнопки «Готово» выполняется запуск основного исполняемого модуля и ожидание завершения его работы. Все результаты сохраняются в файл, указанный в шаге № 1. После завершения результаты работы отображаются в главном окне программы.

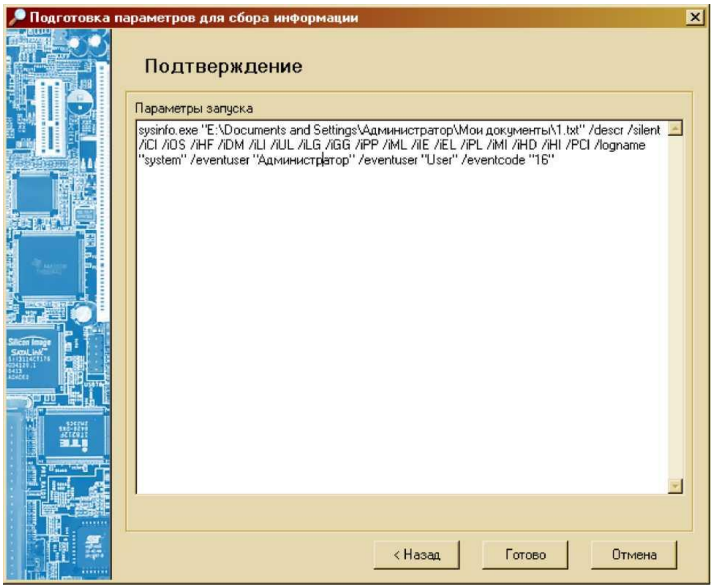


Рис. 1.7. Завершение подготовки параметров

Результаты сохраняются в файл, указанный в шаге № 1. После завершения результаты работы отображаются в главном окне программы.

Формирование отчетов (рис. 1.8).

Создание отчета осуществляется с помощью кнопки . После нажатия этой кнопки, на экране появляется окно настройки состава формируемого отчета. Для удобства можно использовать функции «Выделить все» и «Снять все отметки», доступные через контекстное меню.

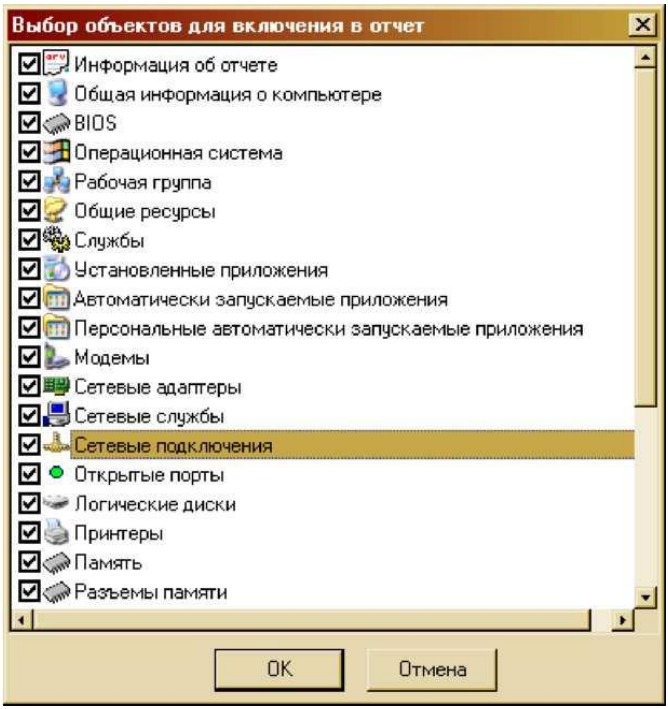


Рис. 1.8. Формирование отчета

После завершения выбора и нажатия кнопки «ОК» будет запрошено имя файла для сохранения отчета, и, затем, создан отчет.

Программа формирует отчет в формате HTML. Файлы в этом формате могут быть открыты любым Web браузером (например, Google Chrome), либо импортированы в офисные приложения, такие как Microsoft Word.

Выполнение с использованием командной строки.

Для запуска «Агента инвентаризации» из командной строки используется файл sysinfo.exe. В общем виде команда запуска имеет следующий вид:

sysinfo.exe имя файла [список параметров]

имя файла – обязательный параметр, в этот файл будут сохранены результаты работы программы.

список параметров – определяет состав получаемой информации и параметры работы программы. Если никаких параметров не указано, то программа работает в стандартном режиме и собирает всю доступную информацию за исключением информации о системных журналах событий.

В списке параметров могут быть использованы значения, перечисленные ниже.

Параметры, определяющие режим работы программы:

/silent – необязательный параметр, использование его запрещает вывод сообщений об ошибках, возникающих в ходе работы программы (например, сообщение о невозможности записи в выходной файл);

/descr – необязательный параметр, включает режим добавления текстовых описаний для кодов классов и свойств.

Параметры, определяющие состав получаемой информации:

/iCI – получить общую информацию о компьютере;

/iOS – получить информацию об операционной системе;

/iHF – получить информацию об установленных пакетах обновлений;

/iDM – получить информацию о принадлежности к домену;

/iLI – получить информацию о региональных установках;

/iOM – получить информацию о модулях операционной системы;

/iUL – получить информацию о пользователях;

/iLG – получить информацию о локальных группах;

/iGG – получить информацию о глобальных группах;

/iLP – получить информацию о политике блокировки;

/iPP – получить информацию о политике паролей;

/iAS – получить информацию о настройках аудита;

/iSL – получить список служб системы;

/iAL – получить список установленных приложений;

/iSA – получить список автоматически запускаемых приложений;

/iML – получить список модемов;

/iNL – получить список сетевых адаптеров;

/iNC – получить список сетевых компонентов (протоколов, служб, клиентов);

/iLD – получить информацию о логических дисках;

/iIE – получить настройки браузера;

/iEL – получить содержимое журналов событий;

/iPL – получить информацию о запущенных процессах;

/iPR – получить информацию о принтерах;

/iSH – получить список общих ресурсов;

/iMI – получить информацию о памяти

/iHD – получить информацию о жестких дисках;

/iHI – получить информацию об устройствах компьютера;

/iSI – получить информацию о сканерах;

/PCI – получить информацию об устройствах на шине PCI.

Групповые параметры получения информации:

/All – получить всю информацию;

/Software – получить всю информацию о программном обеспечении;

/Hardware – получить всю информацию об аппаратном обеспечении;

/Security – получить всю информацию о настройках безопасности;

/Summary – формирование краткого свободного отчета по конфигурации системы. Этот параметр отменяет действие всех прочих параметров.

Параметры фильтрации содержимого системных журналов событий:

/logname имя_журнала – выбор записей только из указанного журнала. В качестве имени журнала может быть указано как отображаемое имя (Приложение, Система, Безопасность, ...), так и системное имя журнала (application, system, security, ...)

Данный параметр может быть использован несколько раз. Например, запуск программы следующим образом:

sysinfo info.txt /iel /logname system /logname Безопасность

добавит в отчет содержимое журналов «Система» и «Безопасность».

/eventuser имя_полъзователя – выбор записей из журналов событий, относящихся только к указанному пользователю.

Имя пользователя может быть указано как непосредственно (например, «Администратор»), так и с указанием домена («DOMAIN\Администратор»).

Данный параметр может использоваться несколько раз для выбора записей, относящихся к нескольким различным пользователям.

/catname имя_категории – выбор записей из журнала, поле «Категория» которых удовлетворяет условию.

/eventid идентификатор_события – выбор из журнала записей с заданным значением поля «Идентификатор». Значение должно быть числовым.

/eventcode код_события – выбор из журнала записей с заданным значением поля «Код (ID)». Значение должно быть числовым. Значения кодов событий являются стандартными. Доступны следующие коды событий (табл. 1.3):

Таблица 1.3. **Значения кодов событий**

Значение	Описание
0	Успех
1	Ошибка
2	Предупреждение
4	Уведомление
8	Аудит успехов
16	Аудит отказов

/eventsource имя_источника – выбор записей из журнала, поле «Источник» которых удовлетворяет условию

/eventdetails дополнительная_информация – выбор записей из журнала, поле «Описание» которых удовлетворяет условию

Эти параметры имеют силу только если в отчет добавляются журналы событий (использован ключ /iEL, /Security или /All)

Примеры применения фильтрации.

sysinfo info.txt /iel /logname Безопасность

Вывод в отчет содержимого журнала «Безопасность»

sysinfo info.txt /iel /catname «Изменение политики»/eventuser Администратор

Вывод информации обо всех случаях изменения политики безопасности пользователем «Администратор». Следует обратить внимание, что строковые значения, содержащие пробелы, должны быть заключены в кавычки.

sysinfo info.txt /iel /eventcode 1 /eventcode 16 /eventuser Администратор

Вывод информации о событиях типа «Ошибка (код 1) или «Аудит отказов» (код 16), связанных с пользователем Администратор.

sysinfo info.txt /iel /eventdetails ошибка /eventdetails отказ

Вывод информации о событиях, содержащих слова «ошибка» или «отказ» в поле «Описание».

Назначение программы «Ревизор сети 2.0».

Сетевой сканер «Ревизор Сети» предназначен для использования администраторами и службами информационной безопасности вычислительных сетей, а также органами по аттестации объектов информатизации в целях обнаружения уязвимостей установленного сетевого программного и аппаратного обеспечения, использующего протоколы стека TCP/IP.

Объектами исследования сетевого сканера являются ПЭВМ, сервера, коммутационное оборудование, межсетевые экраны и другие узлы сети, имеющие IP адреса.

«Ревизор Сети» позиционируется в качестве одного из элементов создаваемой Центром безопасности информации линейки интегрированных между собой программных продуктов, обеспечивающих комплексное тестирование, анализ и контроль защищенности вычислительных сетей различного уровня и назначения в условиях гетерогенной программной среды.

Условия применения

Программа «Ревизор Сети» может быть установлена только на компьютеры, оснащенные процессорами семейства INTEL X86 или совместимыми с ними. Требования к конфигурации компьютеров содержатся в табл. 1.4.

Таблица 1.4. **Требования к конфигурации компьютера**

Элемент	**Минимально**	**Рекомендуется**
Процессор	Pentium Ш – 500 МГ ц	Pentium IV – 1.6 ГГц
Оперативная память	128 Мб	512 Мб
Жесткий диск (свободное пространство)	500 Мб	1 Гб
Монитор	15” (800x600 – 256 цветов)	17” (1024x768 – 256 цветов)

Тип операционной системы на ПЭВМ.

- Windows 7;
- Windows 8;
- Windows 10.

Привилегии пользователя программы.

При установке и эксплуатации ПО «Ревизор Сети» необходимы привилегии локального администратора компьютера или администратора домена сети.

Требования к сетевому ПО.

«Ревизор Сети» версии 2.0 предназначен для использования в сетях Ethernet, функционирующих на основе протокола TCP/IP. На компьютере должны быть установлены компоненты операционной системы, обеспечивающие работу с сетевым протоколом TCP/IP.

Дополнительное программное обеспечение.

Для обеспечения работы ПО «Ревизор Сети» необходимо, чтобы на компьютере было установлено следующее дополнительное программное обеспечение:

- Internet Explorer версии 5.0 или выше;
- ПО сервера баз данных Firebird версии 2.0.;
- сетевой драйвер WinPcap версии 3.1;
- драйвер для электронного ключа Guardant.

Все вышеуказанное ПО входит в дистрибутивный комплект поставки сетевого сканера.

В ПО «Ревизор Сети» предусмотрена возможность интеграции с сетевым сканером Nmap, так же имеющемся на дистрибутивном диске и необходимом для проведения некоторых проверок.

Состав «Ревизора Сети» версии 2.0

«Ревизор Сети» версии 2.0 включает в свой состав:

- основной исполняемый модуль – Scaner3.exe;
- модуль сканирующего ядра – Scaner3Dispatcher.exe;
- модуль визуализации сетевого трафика – MapInfo3.exe;

– модули библиотек с тестирующими проверками;
– модули вспомогательных библиотек;
– ключ авторизации на основе электронного ключа Guardant для USB портов.

Основные характеристики.

Функциональные возможности.

«Ревизор Сети» позволяет проводить тестирование (выполнение заданных наборов проверок) сетевых устройств (узлов) и операционных систем, поддерживающих стек протоколов TCP/IP, функционирующих в составе вычислительных сетей и систем, использующих технологии Ethernet и Fast Ethernet, и однозначно идентифицирующийся собственным IP-адресом.

Функции, выполняемые «Ревизором Сети»:

– «Ревизор Сети» содержит базу данных по доступным проверкам. Регистрация наборов проверок в базе данных «Ревизора Сети» осуществляется вручную при первом запуске программы в соответствии с библиотеками проверок, поставляемыми в составе «Ревизора Сети». Просмотр зарегистрированных проверок осуществляется в интерфейсной части «Ревизора Сети» в виде раскрывающегося графического «дерева» проверок.

– «Ревизор Сети» позволяет осуществлять одновременное параллельное многопоточное тестирование узлов сети.

– «Ревизор Сети» позволяет осуществлять параллельное выполнение взаимно независимых проверок.

– Запуск «Ревизора Сети» и выполнение проверок возможны только при наличии установленного на компьютере электронного ключа авторизации. При отсутствии электронного ключа выполнение программы прекращается.

– Тестирование осуществляется путем проведения сеанса работы в рамках вновь создаваемой или созданной ранее сессии. «Ревизор Сети» позволяет сохранить настройки последнего сеанса,

проведенного с сессией, для их использования при следующем сеансе.

– Тестирование осуществляется в рамках диапазона IP-адресов, заданных при создании новой сессии. Количество тестируемых IP адресов не превышает количество, указанное в лицензии при поставке программного продукта, и задается в поставляемом вместе с программным обеспечением электронном ключе авторизации.

– Тестирование осуществляется только для узлов сети, доступных в момент проведения сеанса работы с сессией. Доступность узлов сети определятся путем запуска любой из поставляемых проверок для определения доступности или их любой совокупности. Проверки, связанные с определением доступности автоматически выделяются в отдельную группу.

– Тестирование осуществляется путем создания плана проверок на основе доступных наборов проверок различных категорий, зарегистрированных в базе данных «Ревизора Сети».

– Проверки, результаты которых необходимы для работы какой-либо из выбираемых (отмечаемых при построении плана) проверок, включаются в план автоматически.

– Последовательность выполнения проверок для сформированного плана определяется.

– «Ревизор Сети» позволяет в динамике отображать процесс выполнения плана проверок в части выполняющихся и закончивших выполнение проверок.

– В ходе сеанса работы с сессией «Ревизор Сети» позволяет в любой момент времени в графическом виде визуализировать процессы обмена информацией между отдельными узлами сети.

– «Ревизор Сети» позволяет в любой момент времени прервать выполнение плана проверок.

– Все результаты выполненных проверок для каждого из сеансов работы могут быть сохранены в базе данных «Ревизора Се-

ти» и в дальнейшем просмотрены в интерфейсной части сетевого сканера в виде соответствующего дерева результатов.

– «Ревизор Сети» позволяет осуществлять объединение узлов сети в группы по IP-адресам. Каждый из узлов сети может входить в любое количество созданных групп.

– «Ревизор Сети» позволяет осуществить просмотр отдельных обобщенных результатов работы для всей совокупности узлов сети, по группам и по отдельному IP-адресу за любой из проведенных сеансов работы и за всю сессию.

– «Ревизор Сети» позволяет осуществить формирование отчетов по результатам работы сетевого сканера. Отчеты формируются для любой совокупности IP-адресов.

– По каждому из выполненных планов работы «Ревизор Сети» позволяет осуществить формирование отчетов различной степени детализации, а также в обобщенном виде в части обнаруженных уязвимостей.

– «Ревизор Сети» формирует отчеты в формате HTML и виде документов Microsoft Word.

– «Ревизор Сети» позволяет проводить обновление базы выполняемых проверок путем регистрации новых библиотек проверок, поставляемых разработчиками программного продукта.

– «Ревизор Сети» имеет полностью русскоязычный интерфейс.

– В процессе работы «Ревизор Сети» позволяет осуществлять взаимодействие с сетевым сканером Nmap в части идентификации сервисов, сетевых устройств и типов операционных систем.

– «Ревизор Сети» включает наборы проверок по следующим категориям:

1) определение доступности узлов проверяемой сети не менее чем тремя различными методами;

2) определение открытых TCP и UDP портов на узлах проверяемой сети;

3) верификация типа операционной системы, установленной на проверяемом узле сети,

4) верификация сетевых сервисов;

5) определение NetBios-имени проверяемого узла сети;

6) определение DNS-имени проверяемого узла сети;

7) проверка учетных записей для узлов сети, функционирующих под управлением операционных систем семейства Windows;

8) определение наличия и доступности общих сетевых ресурсов на проверяемых узлах сети;

9) сопоставление служб и сервисов, запущенных на узлах сети портов, назначенных и контролируемых организацией IANA;

10) проверка известных уязвимостей операционных систем семейства Windows;

11) проверка установленных обновлений программного обеспечения операционных систем семейства UNIX;

12) проверка известных уязвимостей сервиса FTP;

13) проверка известных уязвимостей сервиса RPC;

14) проверка известных уязвимостей электронной почты;

15) детальный анализ структуры и контента WEB-сайта;

16) проверка узлов сети на наличие DOS-уязвимости (отказ в обслуживании);

17) проверка наличия удаленного доступа к приложениям;

18) проверка возможности получения прав удаленного администратора;

19) проверка наличия паролей по умолчанию;

20) подбор паролей через SMB.

Установка ПО «Ревизор Сети».

Дистрибутив «Ревизора Сети» поставляется на диске или посредством сетевой инфраструктуры университета. После активации установщика на экране появится окно интерфейса программы установщика (при установленном режиме AutoRun).

В части отдельных результатов «Ревизор Сети» интегрирован со сканером Nmap. Данное ПО свободно распространяется в рамках лицензии производителя (Free Software Foundation, Inc. 59

Temple Place – Suite 330, Boston, MA 02111-1307, USA, http://insecure.org/).

Рис. 1.9. Установка ПО «Ревизор сети»

Установку программного обеспечения рекомендовано выполнять в следующей последовательности:

- установить сканер Nmap;
- установить сервер баз данных Firebird версии 2.0.
- установить ПО «Ревизор Сети»;
- установить и провести конфигурацию драйвера электронного ключа защиты Guardant.

В процессе установки сканера Nmap рекомендуется выбирать параметры установки по умолчанию.

При установке ПО сервера баз данных Firebird версии 2.0 и ПО «Ревизор Сети» пользователю выдаются стандартные диалоги по принятию лицензионного соглашения и выбору каталогов для установки ПО. В выдаваемых диалогах установщика необходимо выбирать значения параметров, принятые по умолчанию.

В процессе установки драйвера для электронного ключа защиты Guardant, сам ключ не должен быть установлен в USB порт ПЭВМ. После установки драйвера на экране появится следующее окно (рис. 1.10).

Рис. 1.10. Установка драйвера

Выбрав пункт «Конфигурировать драйвер» можно просмотреть и изменить настройки драйвера Guardant (рис. 1.11):

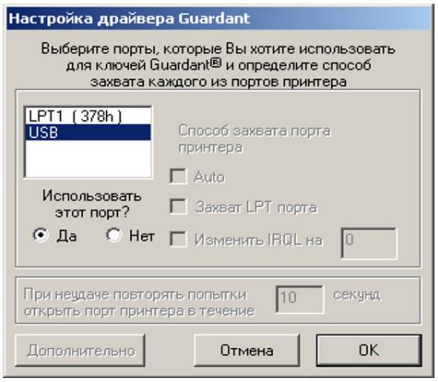


Рис. 1.11. Установка драйвера

ПО Guardant автоматически определяет тип ключа, установленного в текущий момент времени на компьютере. При возникновении каких-либо проблем, связанных с определением ключа защиты, рекомендуется вручную проставить отметку для использования порта USB в данном окне настройки драйвера. При запуске «Ревизора Сети» возможно появление следующего сообщения (рис. 1.12):

Рис. 1.12. Ошибка

Данное сообщение связано с логикой работы сервера баз данных Firebird версии 2.0 и не свидетельствует о некорректной работе «Ревизора Сети». При появлении такого сообщения необходимо выполнить следующую последовательность операций:

1. Завершить выполнение «Ревизора сети».
2. Через панель управления запустить менеджер Firebird сервера.
3. В открывшемся окне менеджера сервера (рис. 1.13) нажать кнопку «Stop», затем появившуюся кнопку «Start» (перезапустить сервер).

Рис. 1.13. Окно менеджера

4. Повторно запустить ПО «Ревизор Сети».

После выполнения указанной последовательности действий «Ревизор Сети» должен успешно стартовать.

При первом запуске карты активности «Ревизора Сети», (кнопка «Карта») возможно появление сообщений «Системе не удается найти указанный путь» или «Класс не зарегистрирован» (рис. 1.14):

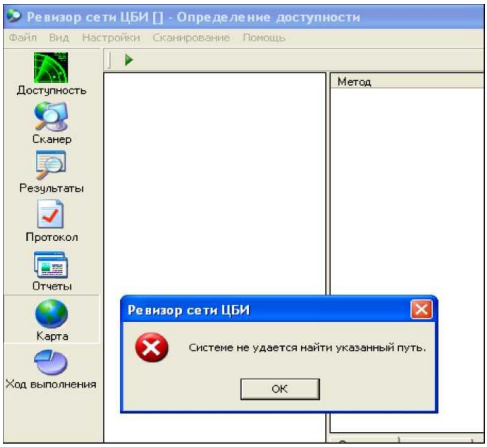


Рис. 1.14. Ошибка невозможности нахождения пути

В случае появления такого сообщения необходимо выполнить следующие действия:

1. Завершить «Ревизор Сети».
2. Запустить выполняемый файл карты активности («MapInfo3.exe») используя средства Windows.
3. Завершить выполнение файла MapInfo3.exe.
4. Файл MapInfo3.exe находится в каталоге с установленным ПО «Ревизора Сети» в подкаталоге «bin»).

После выполнения указанной последовательности действий ПО карты активности, запускаемое в «Ревизоре Сети» должно стартовать корректно.

Запуск программы возможен только при подключенном к USB или LPT порту электронном ключе защиты из комплекта поставки ПО!

Применение Ревизора Сети.

Запуск программы.

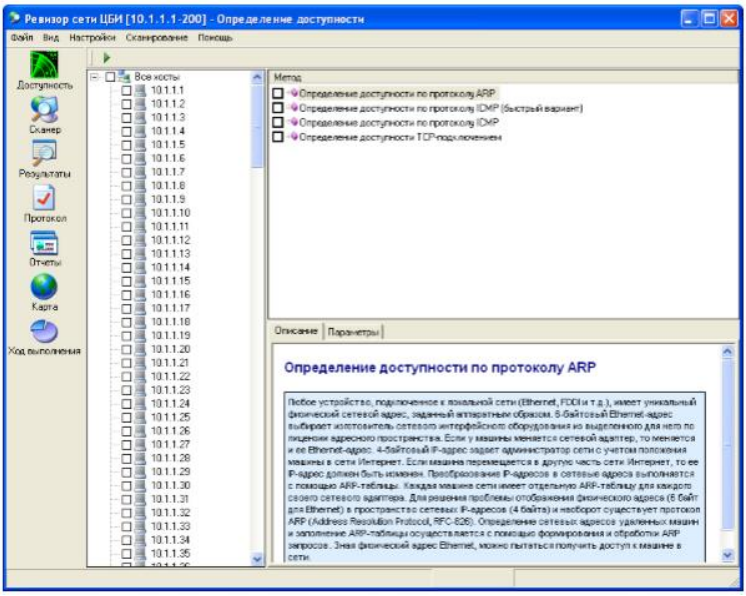
Программа «Ревизор Сети» запускается посредством меню Пуск / Программы рабочего стола Windows или путем клика левой кнопкой мыши на ярлыке «Ревизор Сети», размещенном на рабочем столе после инсталляции ПО.

После запуска программы на экране монитора появляется заставка (рис. 1.15).

Рис. 1.15. Запуск программы

При первом запуске программы необходимо зарегистрировать библиотеки, входящие в состав дистрибутива. Для этого в меню Файл / Регистрация библиотек выбираются библиотеки с модулями проверок для дальнейшего использования. Рекомендуется выбрать все библиотеки.

Далее открывается главное окно программы (рис. 1.16).



1.16. Главное окно программы

Начало работы с программой

Работа с Ревизором Сети осуществляется в рамках сессии. Под сессией подразумевается совокупность устанавливаемых пользователем параметров проверок, атрибутов работы программы и результатов проверок.

Пользователю предоставлена возможность экспорта сессии в файл и импорта сессии из файла. В базе данных может храниться только текущая сессия, для работы с несколькими сессиями нужно пользоваться операциями экспорта и импорта.

Установка параметров сессии

Основным параметром сессии является рабочий диапазона IP-адресов тестируемой сети. Его необходимо указать при первом запуске «Ревизора Сети», либо при изменении состава тестируемой сети.

Создание новой сессии осуществляется путем выбора пункта меню Настройки / Параметры сессии. При этом появится окно создания новой сессии.

При задании адресов можно через запятую (без пробела) указывать диапазоны нескольких сетей класса С или отдельные IP-адреса, например: 192.168.20.1-254, 192.168.21.5-70, 10.1.1.5, 10.1.1.36 (рис. 1.17).

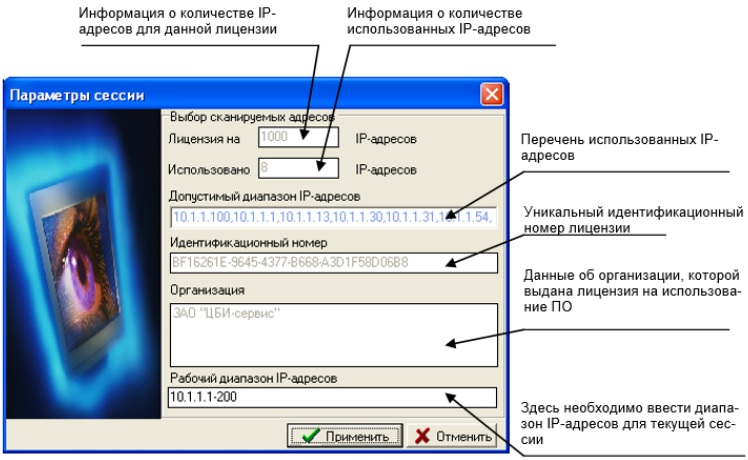


Рис. 1.17. Установка параметров сессии

При желании можно сохранить указанный в сессии диапазон адресов в текстовом файле или загрузить из текстового файла при создании новой сессии.

Необходимо помнить, что использование программного продукта осуществляется в рамках лицензии на определенное количество IP-адресов.

Если проводилось сканирование каких-либо узлов сети, то при создании новой сессии можно видеть информацию о количестве использованных/неиспользованных IP-адресов, а также перечень использованных IP-адресов.

При этом в поле «Рабочий диапазон IP-адресов» автоматически выводится ранее заданное значение диапазона.

При изменении параметров сессии, предыдущая сессия удаляется и создается новая с указанными параметрами. Если предыдущая сессия содержит какую-либо важную информацию, ее можно сохранить в файл.

Сохранение сессии в файл

Сохранение новой сессии осуществляется путем выбора пункта меню Файл/Сохранить сессию. После выбора файла все данные сессии будут сохранены в указанный файл в XML-формате.

Загрузка сессии из файла

Загрузка новой сессии осуществляется путем выбора пункта меню Файл/Загрузить сессию. После выбора файла сессия будет загружена из указанного файла. Текущая сессия при этом будет удалена.

Описание режимов работы

Во время сеанса работы пользователь может находиться в одном из следующих основных режимов работы:

- формирование плана проверки доступности узлов проверяемой сети;
- проверка доступности узлов сети;
- формирования плана проверок для проведения сканирования сети;
- выполнение сформированных планов проверок;
- просмотр результатов;
- формирование отчетов.

Каждому из режимов работы соответствует одно или несколько экранных «окон» в графическом интерфейсе сетевого сканера:

- окно формирования плана проверки доступности узлов сети;
- окно формирования плана проверок для проведения сканирования сети;
- окно отображения динамики выполняемых проверок;

– окно протокола работы и просмотра «дерева» результатов;
– окно просмотра обобщенных результатов работы;
– окно формирования отчетов (рис. 1.18).

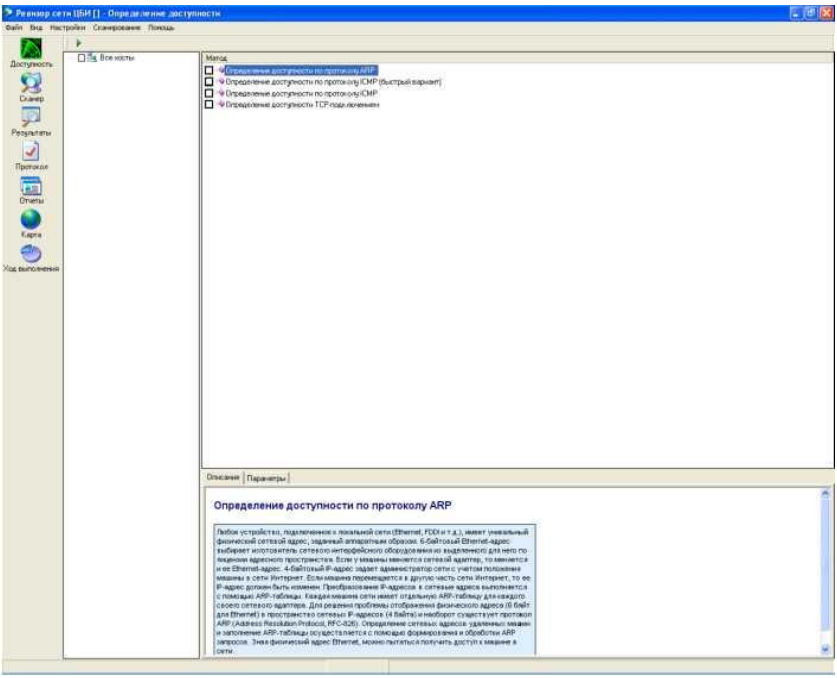


Рис. 1.18. Определение доступности

Переход в то или иное окно осуществляется через соответствующие кнопки панели инструментов в левой части экрана или посредством выбора требуемого пункта меню. Наименование текущего окна отображается в строке статуса в нижней части экрана.

Формирование плана проверки доступности узлов сети

Логика работы «Ревизора Сети» построена таким образом, что пользователю предоставлена возможность выполнения проверок только для доступных в настоящий момент узлов сети.

Таким образом, выполнению проверок предшествует определение доступных для сканирования узлов сети (IP-адресов). После начала работы с «Ревизором Сети» пользователь автоматически попадает в окно формирования плана проверок для определения доступности узлов сети. В этом окне пользователь должен определить, доступность каких узлов нужно определить, а также какие методы должны при этом использоваться.

Предоставляемые пользователю методы определения доступности узлов сети являются единственными проверками, которые можно выполнять для любого узла в рамках заданного диапазона IP-адресов без учета ограничений приобретенной лицензии на ПО. Все другие проверки выполняются только для определенной совокупности доступных узлов.

Проверки определения доступности узлов не зависят от количества IP-адресов, на которое выдана лицензия и могут всегда выполняться для любых узлов проверяемой сети.

Формирование плана сканирования сети

Основной задачей сетевого сканера является выявление потенциальных уязвимых мест в настройках программного обеспечения узлов проверяемой сети, отвечающего за обеспечение сетевого взаимодействия. Для решения данной задачи в «Ревизоре Сети» предусмотрены проверки по различным категориям.

План выполнения проверок формируется в соответствующем окне формирования плана проверок для сканирования сети. Пользователь отмечает узлы, на которые хочет пустить проверки, выбирает требуемые проверки и формирует план проверок.

Необходимо помнить, что IP-адреса узлов, попавших однажды в план проверок после нажатия кнопки «Сформировать план проверок», сразу автоматически фиксируются как IP-адреса диапазона лицензии, выданной на программный продукт.

Формирование плана проверок в «Ревизоре Сети» осуществляется путем проставления отметки против соответствующей про-

верки, коррекции (при необходимости) отдельных входных параметров проверок и нажатия кнопки «Добавить проверки в план».

Для удобства формирования плана проверок предусмотрен режим автоматического выделения зависимых проверок. Если это режим включен, то при выделении проверки автоматически выделяются все другие проверки, результаты которых необходимы для ее выполнения. Режим автоматического выделения зависимых проверок можно включать и выключать с помощью соответствующей кнопки ( ).

Выполнение сформированного плана проверок осуществляется по кнопке «Выполнить план проверок» (рис. 1.19).

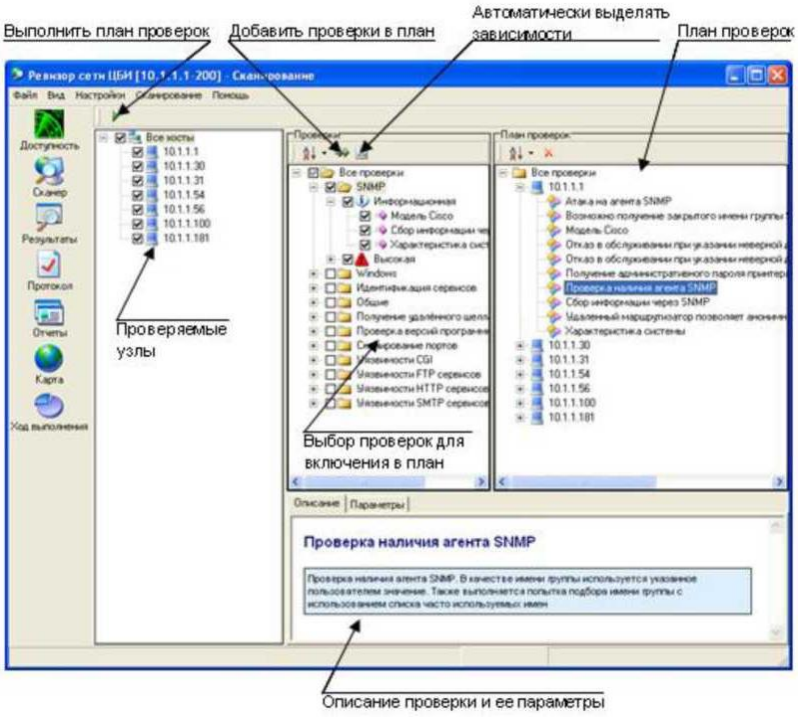


Рис. 1.19. Сканирование

Если пользователь пытается сформировать план, включающий в себя количество IP-адресов большее, чем установлено в лицензии, то в план проверок попадут только те адреса, которые уже сканировались ранее, или же новые, но по количеству не превышающие соответствующий параметр лицензии.

Таким образом, необходимо внимание при проставлении отметок для узлов, которые необходимо включить в план, чтобы в него не попали те доступные узлы, сканирование которых не предполагается.

После нажатия на кнопку «Начать сканирование» начинается процесс сканирования сети.

Выполнение проверок, протокол хода выполнения

После начала процесса сканирования сети автоматически осуществляется переход в окно отображения динамики выполняемых проверок.

В данном окне можно просмотреть информацию о наименованиях выполняющихся проверок, количестве запущенных проверок на каждый из IP-адресов, количестве выполненных проверок.

Гистограммы, отображаемые для каждого узла, позволяют оценить информацию по количеству и типам проверок, давших положительный результат и не давших никакого результата.

При нажатии на кнопку «Протокол» панели инструментов в левой части экрана, появляется окно протокола выполнения плана проверок (рис. 1.20).

В этом окне можно просмотреть информацию о выполненных проверках, проверках, находящихся в ожидании выполнения и проверках, обнаруживших уязвимости (давших положительный результат работы).

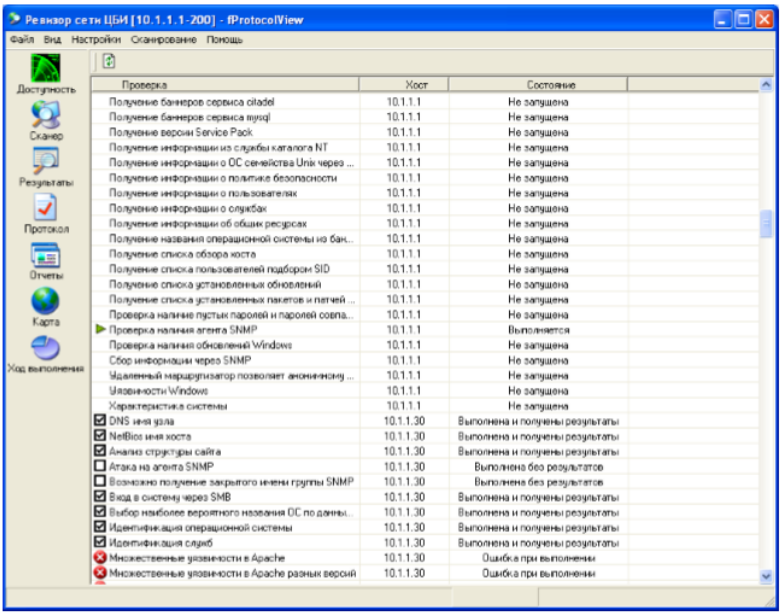


Рис. 1.20. Протокол выполнения

Просмотр результатов работы

Результаты работы сетевого сканера можно просмотреть в соответствующем окне, открывающемся при нажатии кнопки «Результаты» панели инструментов, или через основное меню программы (рис. 1.21).

«Ревизор Сети» предоставляет следующие режимы просмотра результатов:

- общая информация об узлах сети (DNS и NetBios имена узлов, предполагаемый тип операционной системы, имя домена);
- информация о найденных уязвимостях;
- информация об открытых TCP и UDP портах;
- информация о пользователях и группах, зарегистрированных на узле сети; информация о доступных сетевых ресурсах;
- подробная информация по узлу.

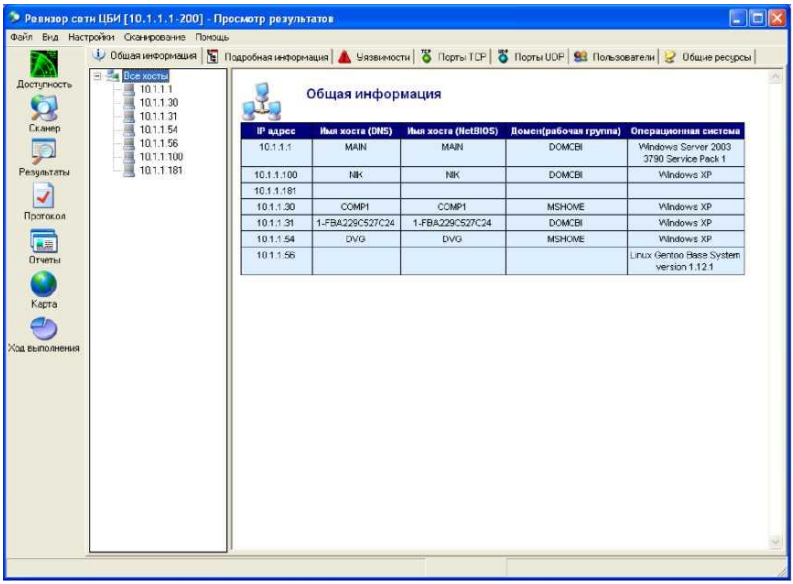


Рис. 1.21. Просмотр результатов

Для просмотра информации обо всей сети или группе узлов необходимо выделить соответствующую группу в дереве узлов в левой части экрана.

Для просмотра информации о конкретном узле необходимо выделить этот узел.

При выборе режима просмотра подробной информации по узлу, результаты отображаются в виде дерева объектов, при этом свойства выбранного объекта отображаются в нижней части экрана.

Результаты работы привязываются к соответствующему IP-адресу узла. Подробная информация может быть особенно полезна для администраторов систем и технических специалистов.

Формирование отчетов

Данные, полученные в результате выполнения проверок, сохраняются в базе данных «Ревизора Сети» и могут быть представлены в виде отчетов в формате HTML или Microsoft Word.

Для формирования отчетов необходимо с помощью панели инструментов или через главное меню программы перейти в соответствующее окно.

Окно формирования отчетов разделено на две части.

В левой части осуществляется выбор узлов (IP-адресов), для которых формируется отчет.

В правой части окна осуществляется выбор типа отчета (общий, детальный и т.д.). При этом существует возможность отметить определенные виды и типы результатов, которые должны быть помещены в отчет (рис. 1.22).

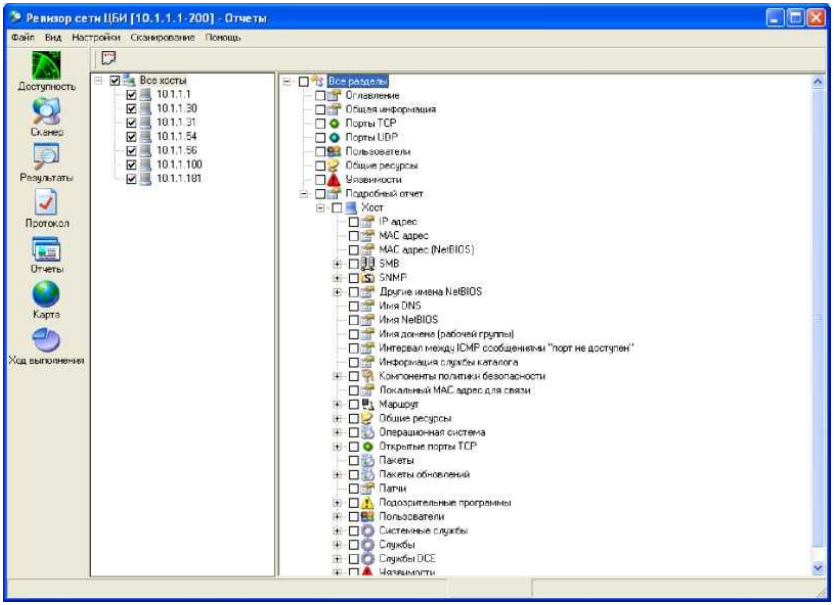


Рис. 1.22. Формирование отчета

Формирование отчета начинается при нажатии на кнопку «Создать отчет» на панели инструментов. В диалоге выбора файла для сохранения отчета также нужно указать формат отчета (Word или Html).

При большом количестве результатов сканирования и выбранных для отчета узлов сети возможна некоторая задержка во времени при формировании обобщенных видов отчетов, что обусловлено процессами обработки информации, содержащейся в базе данных «Ревизора Сети».

Сценарий выполнения лабораторной работы

1. Проведение инвентаризации состава технических и программных средств отдельного персонального компьютера с использованием стандартных средств операционной системы

Данная лабораторная работа выполняется на АРМ под управлением ОС Windows (рис. 1.23).

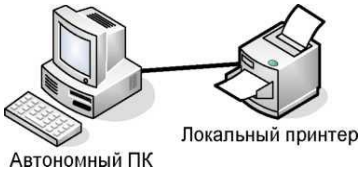


Рис. 1.23. Схема стенда при проведении инвентаризации состава автономного СВТ

Для начала выполнения лабораторной работы необходимо выполнить вход в ОС Windows.

Проведение инвентаризации состава технических средств отдельного ПК.

После загрузки ОС необходимо произвести запуск диспетчера устройств, для этого:

1. Зайдите в меню «Пуск» => «Панель управления» => «Администрирование» => «Управление компьютером» (рис. 1.24);

В появившемся окне выберите «Диспетчер устройств»;

В появившемся справа списке подключенных устройств, выберите интересующее вас устройство, подробную информацию о

котором можно просмотреть, щелкнув по нему два раза левой кнопкой мыши.

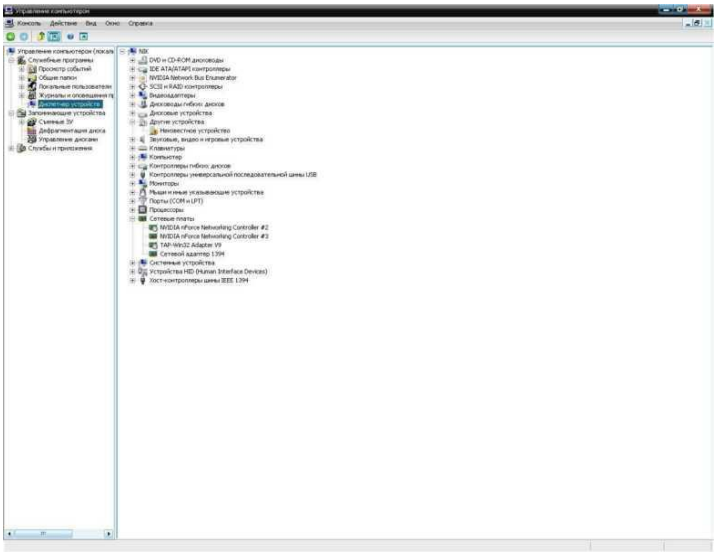


Рис. 1.24. Окно Диспетчера устройств

2. Полученные данные занесите в заранее подготовленную таблицу (табл. 1.5).

Таблица 1.5. **Сводный отчет по инвентаризации состава ТС ПК**

Наименование ТС	**Номер версии**	**Производитель**	**Всего установлено**
-	-	-	-
-	-	-	-
-	-	-	-
-	-	-	-
-	-	-	-
-	-	-	-

2. Проведение инвентаризации состава программных средств отдельного ПК

Для определения установленного ПО необходимо провести следующие действия:

1. Зайдите в меню «Пуск» => «Панель управления» => «Установка и удаление программ» (рис. 1.25).

2. Просмотрите подробную информацию об установленном ПО.

3. Полученные данные занесите в заранее подготовленную таблицу (табл. 1.6).

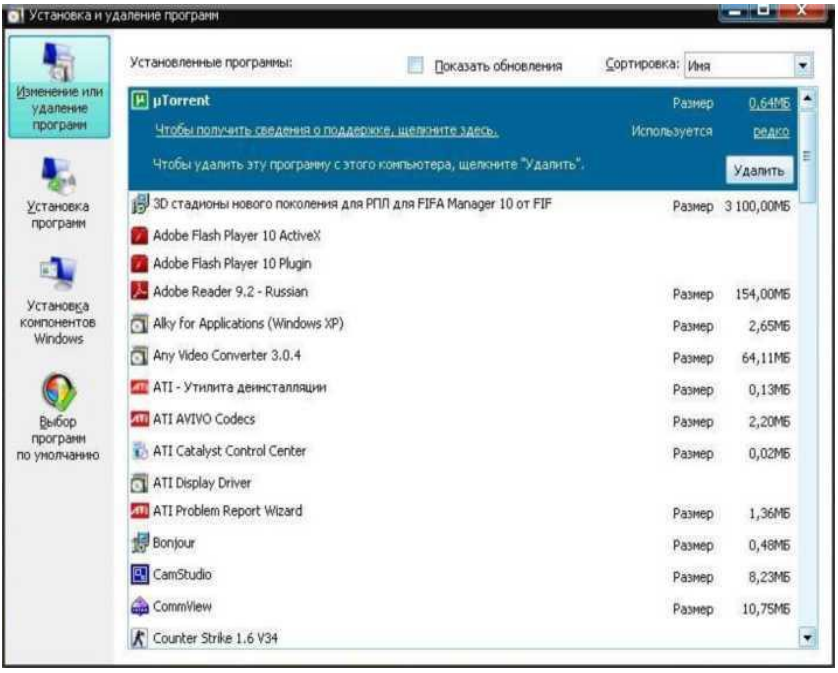


Рис. 1.25. Окно установки удаления программ

Таблица 1.6. **Сводный отчет по инвентаризации состава ПО ПК**

Название ПО	Номер версии	Издатель	Всего установлено
-	-	-	-
-	-	-	-
-	-	-	-
-	-	-	-
-	-	-	-

3. Проведение инвентаризации состава технических и программных средств отдельного ПК с использованием специализированных средств системного сканирования ПЭВМ

В данном пункте лабораторной роботы используется сертифицированное программное обеспечение «Агент инвентаризации».

Выполните установку и запуск ПО согласно пункту «Выполнение программы».

Для сбора информации о системе используется кнопка  панели инструментов. После ее нажатия на экране появляется диалоговое окно, в котором можно за несколько шагов настроить параметры сбора информации.

Шаг 1. Настройка параметров работы программы.

На этом шаге устанавливаются основные параметры, определяющие работу программы. Прежде всего, это имя файла для сохранения результатов (указывается с помощью кнопки ().

Шаг 2. Определение состава получаемой информации (дополнительно).

Пользователю предоставляется возможность более точно определить состав получаемой информации. Выполните действия согласно рис. 12.26, рис. 12.27.

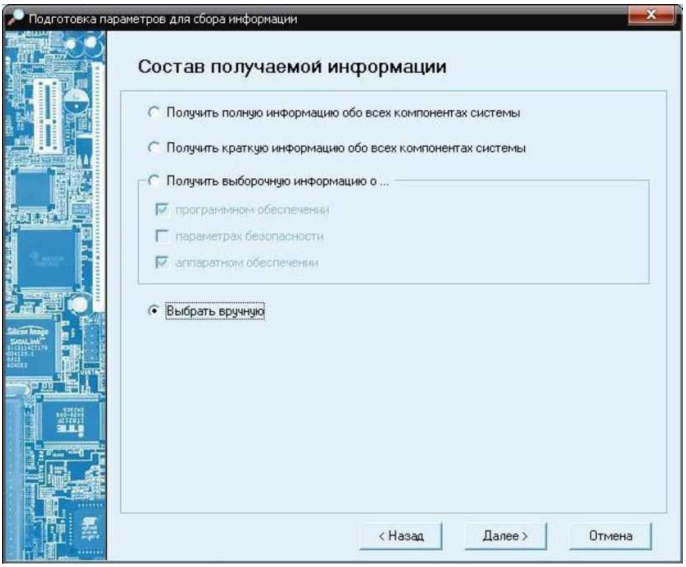


Рис. 1.26. Определение состава получаемой информации

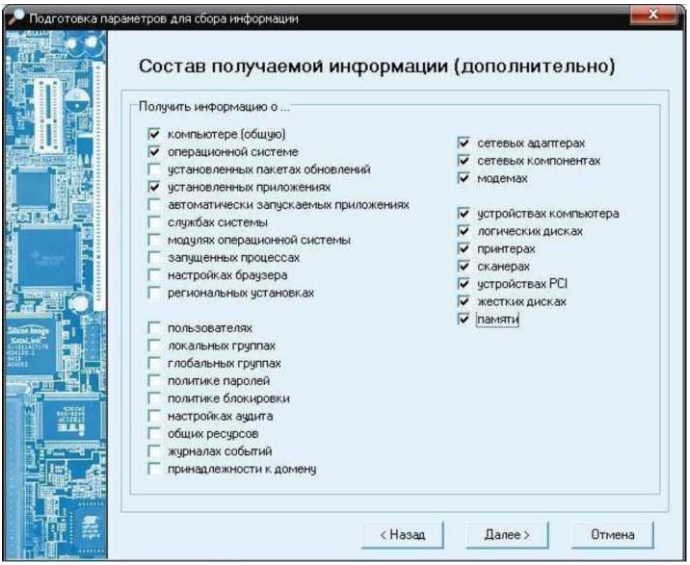


Рис. 1.27. Определение состава получаемой информации (дополнительно)

Шаг 3. Завершение формирования параметров.

На этом этапе формирование параметров уже завершено, и на экран выводится командная строка, которая будет использована при запуске основного исполняемого модуля. Эта строка может быть скопирована и использована в дальнейшем для запуска основного исполняемого модуля без использования графического интерфейса (рис. 1.28).

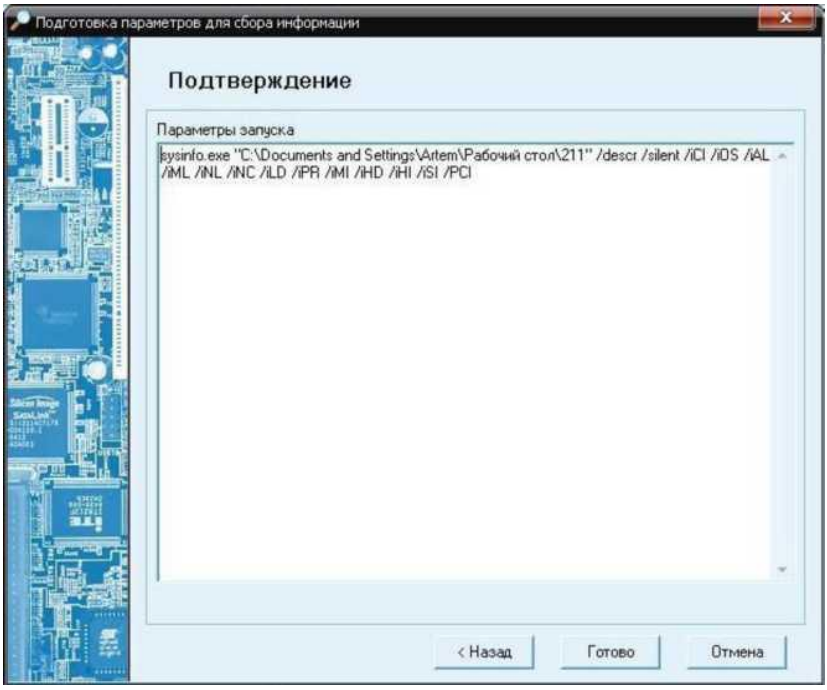


Рис. 1.28. Завершение подготовки параметров

По нажатию кнопки «Готово» выполняется запуск основного исполняемого модуля и ожидание завершения его работы. Все результаты сохраняются в файл, указанный в шаге № 1. После завершения, результаты работы отображаются в главном окне программы.

Шаг 4. Формирование отчета

Выполнение данного шага осуществляется согласно пункту «Формирование отчетов».

В полученном отчете содержится подробная информация об установленных ТС и ПО на данном ПК.

4. Проведение инвентаризации состава технических и программных средств ЛВС с использованием специализированных средств сетевого и системного сканирования ЛВС

Подготовьте к работе стенд в соответствии с методическими материалами по выполнению работы. Общая функциональная схема стенда дана на рис. 1.29.

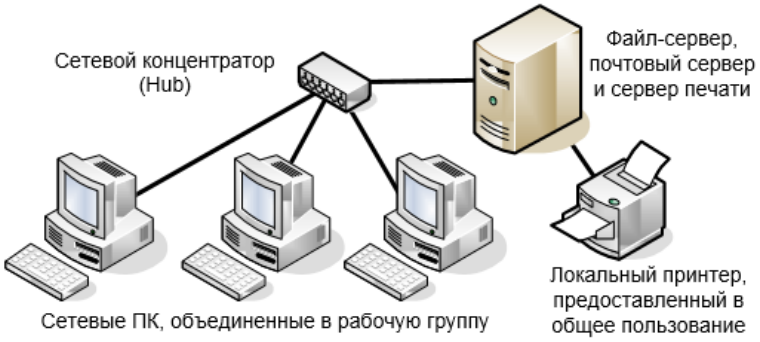


Рис. 1.29. Схема стенда при проведении инвентаризации состава ЛВС

Выполните установку ПО «Ревизор Сети» согласно пункту «Установка ПО «Ревизор Сети». После установки запустите программу посредством меню Пуск => Программы рабочего стола Windows или путем клика левой кнопкой мыши на ярлыке «Ревизор Сети», размещенном на рабочем столе после инсталляции ПО.

Перед запуском программы не забудьте подключить к USB порту электронный ключ защиты. При первом запуске программы необходимо зарегистрировать библиотеки, входящие в состав дис-

трибутива. Для этого в меню Файл => Регистрация библиотек выбираются библиотеки с модулями проверок для дальнейшего использования. Выберите все библиотеки.

Далее открывается главное окно программы (рис. 1.30).

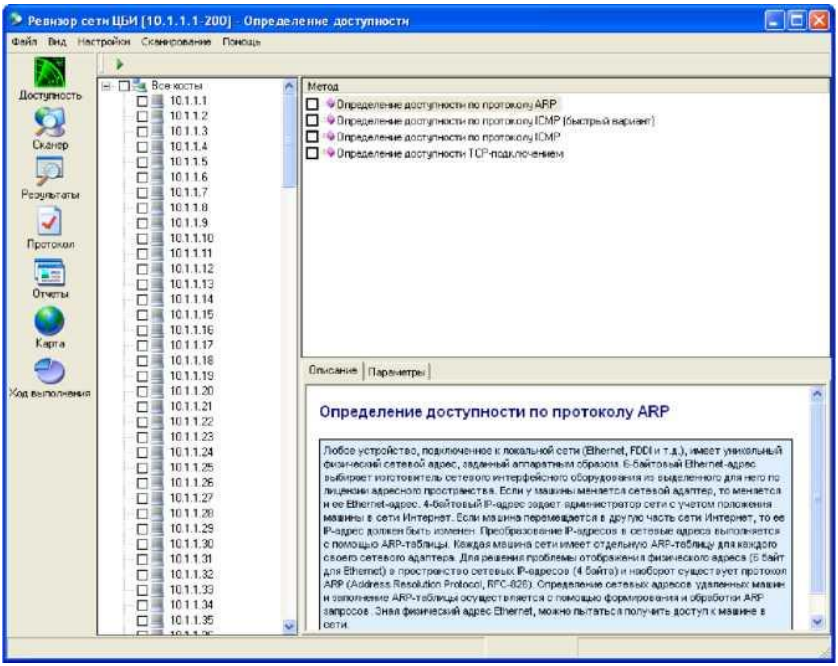


Рис. 1.30. Главное окно программы

Установите параметры сессии согласно пункту, описанному выше, и начните сканирование.

Данные, полученные в результате выполнения проверок, сохраняются в базе данных «Ревизора Сети» и могут быть представлены в виде отчетов в формате HTML или Microsoft Word.

Для формирования отчетов необходимо с помощью панели инструментов или через главное меню программы перейти в соответствующее окно.

Начните формирование отчета, нажав на кнопку «Создать отчет» на панели инструментов. В диалоге выбора файла для сохранения отчета также нужно указать формат отчета Html.

Подготовка отчета для сдачи лабораторной работы

1. В отчёте кратко описать выполненные действия.
2. Провести анализ полученных в работе результатов.
3. Полученные результаты (html файлы) оформить в виде протоколов.

Вопросы по лабораторной работе

1. Какую информацию во время работы получает ПО «Агент инвентаризации» о программном и аппаратном обеспечении в составе АРМ в ходе своей работы?
2. Как определяется доступность узлов сети в момент проведения сеанса работы ПО «Агент инвентаризации».
3. Какие наборы проверок по категориям включает в себя ПО «Ревизор Сети»?
4. Опишите основные шаги проведения инвентаризации состава программных средств отдельного ПК средствами ПО «Агент инвентаризации».
5. Опишите основные шаги проведения инвентаризации состава технических и программных средств отдельного ПК с использованием специализированных средств системного сканирования ПЭВМ.
6. Опишите основные шаги проведения инвентаризации состава технических и программных средств ЛВС с использованием специализированных средств сетевого и системного сканирования ЛВС

ЛАБОРАТОРНАЯ РАБОТА № 2

Поиск отличий реально полученной информации от информации, заявленной в исходных данных на объекте информатизации

Цель: Поиск отличий реально полученной информации от информации, заявленной в исходных данных на объекте информатизации. Проведение аттестационных испытаний автоматизированной системы (АС) по требованиям безопасности информации в части защиты от НСД в соответствии с требованиями нормативной и методической документации.

Сценарий выполнения работы

Выполнение данной лабораторной работы возможно только после выполнения лабораторной работы «Проведение инвентаризации состава технических и программных средств отдельного персонального компьютера и ЛВС с использованием стандартных и специализированных средств операционной системы».

Этапы выполнения лабораторной работы:

1) Изучение содержания отчета лабораторной работы «Организация аттестации автоматизированных систем по требованиям безопасности информации в части защиты от НСД. Проверка документации».

2) Изучение содержания отчетов лабораторной работы «Проведение инвентаризации состава технических и программных средств отдельного персонального компьютера и ЛВС с использованием стандартных и специализированных средств операционной системы».

3) Поиск отличий результатов инвентаризации и информации, заявленной в исходных данных.

4) Составление отчета с указанием отличий реально полученной информации от информации, заявленной в исходных данных на объекте информатизации.

Для проведения аттестации, Заказчик должен предъявить органу по аттестации ряд исходных данных по объекту информатизации. Для принятия решения об аттестации объекта информатизации, органу по аттестации должны быть представлены исходные данные, не отличающиеся от реально полученной информации по аттестуемому объекту информатизации в ходе специальных проверок.

Порядок выполнения работы

1. ***Изучение содержания отчета лабораторной работы «Организация аттестации автоматизированных систем по требованиям безопасности информации в части защиты от НСД. Проверка документации»***

Для выполнения этого пункта вам понадобится отчет о выполнении лабораторной работы «Организация аттестации автоматизированных систем по требованиям безопасности информации в части защиты от НСД. Проверка документации». Изучите перечень исходных данных, содержащихся в этом отчете.

2. ***Изучение содержания отчетов лабораторной работы «Проведение инвентаризации состава технических и программных средств отдельного персонального компьютера и ЛВС с использованием стандартных и специализированных средств операционной системы»***

Для выполнения этого пункта, понадобятся отчеты о выполнении лабораторной работы «Проведение инвентаризации состава технических и программных средств отдельного персонального компьютера и ЛВС с использованием стандартных и специализированных средств операционной системы». Изучите результаты инвентаризации, содержащиеся в этом отчете:

– результаты инвентаризации с помощью специализированных средств;
– результаты инвентаризации с помощью стандартных средств.

3. ***Поиск отличий результатов инвентаризации и информации, заявленной в исходных данных***

Для выполнения этого пункта вам необходимо сверить данные отчетов, которые были изучены в пунктах 1 и 2 данной лабораторной работы.

4. ***Составление отчета с указанием отличий реально полученной информации от информации, заявленной в исходных данных на объекте информатизации***

Составьте общий отчет, в котором укажите отличия (если таковые имеются) результатов инвентаризации и представленных исходных данных на объект информатизации.

Вопросы по лабораторной работе

1. В чем может заключаться отличие реально полученной информации от информации, заявленной в исходных данных на объекте информатизации?
2. Приведите пример исходных данных, которые Заказчик должен предъявить органу по аттестации для ее проведения аттестации.
3. Опишите какие результаты инвентаризации могут быть получены с помощью специализированных средств?

ЛАБОРАТОРНАЯ РАБОТА № 3

Контроль уязвимостей на уровне сети

Цель: Изучение основ обеспечения защиты сетей от несанкционированного доступа и принципов работы с сетевыми сканерами безопасности.

Введение

В связи с расширением использования корпоративных сетей и сети Internet специалисты в этой области все больше осознают необходимость анализа и управления потенциальными рисками безопасности в сетях и системах. Основным источником проблем служат так называемые уязвимости или, как их еще называют, «дыры» в программном обеспечении. Уязвимости позволяют постороннему свободно проникать в сеть. Последствия такого вторжения могут быть разными: от утечки конфиденциальной информации до полной потери данных.

Анализ уязвимостей — это процесс обнаружения, оценки и ранжирования рисков, связанных с системами и устройствами, функционирующими на сетевом и системном уровнях, с целью рационального планирования применения информационных технологий. Инструменты, реализующие этот процесс, позволяют установить собственную политику безопасности, автоматизировать анализ уязвимостей и создать отчеты, которые эффективно связывают информацию об обнаруженных уязвимостях с подробными корректирующими действиями на всех уровнях организации. Основным средством обнаружения уязвимостей служат сетевые сканеры безопасности.

Одновременное использование систем анализа защищенности, функционирующих на сетевом и системном уровнях, обеспечивает

мощнейшую защиту против трех типов уязвимостей, появляющихся от поставщика, администратора и пользователя.

Все риски можно разделить на три категории:

Риски, связанные с ПО, поставляемым поставщиком – включают ошибки, неустановленные обновления (patch и hotfix) операционной системы, уязвимые сервисы и незащищенные конфигурации по умолчанию.

Риски, связанные с действиями администратора –включают доступные, но неправильно используемые настройки и функции системы, не отвечающие политике безопасности требования к минимальной длине пароля и несанкционированные изменения в конфигурации системы.

Риски, связанные с деятельностью пользователя – включают уклонение от предписаний принятой политики безопасности, то есть любые несанкционированные действия.

Возможности сетевого сканирования

Сетевой сканер должен быть первым инструментом, используемым в процессе анализа защищенности. Он обеспечивает быстрый обзор уязвимостей самой высокой степени риска, которые требуют немедленного внимания. Анализ уязвимостей при сканировании на сетевом уровне поможет обнаружить очень серьезные уязвимости, такие как неправильно сконфигурированные межсетевые экраны (МСЭ) или уязвимые Web-сервера в демилитаризованной зоне (DMZ), которые могут предоставить потенциальную возможность для проникновения хакеров и позволить им скомпрометировать систему защиты организации. Сканирование на сетевом уровне обеспечивает быстрый и детальный анализ сетевой инфраструктуры организации как со стороны внешнего, так и со стороны внутреннего наблюдателя.

Основные случаи необходимости проведения мониторинга

– установлены не все необходимые патчи на компьютерах (возможно, когда устанавливался важный патч, какой-то компьютер был недоступен, или на каком-то компьютере недавно переуста-

навливалась новая операционная система, или в сети появился ноутбук, принесенный из дома, или был установлен виртуальный компьютер под VMware Workstation/ Microsoft Virtual PC). В современных суровых условиях даже один непропатченный компьютер (особенно принесенный из дома поработавший в сети ноутбук) может принести администраторам большие неприятности. Это относится не только к патчам операционных систем, но и других программных продуктов, например, SQL Server;

– мониторинг появления новых общих ресурсов, особенно на клиентских компьютерах. Очень часто такие несанкционированные сервера становятся источником проблем (поскольку пользователи обычно не утруждают себя назначением каких-либо разрешений или аудита) – через них может «уйти» важная информация, или данные в этом общем ресурсе могут быть стерты другим пользователем (а резервное копирование рабочих станций производится далеко не везде);

– появление дополнительных служб и открытых портов (особенно относящихся к удаленному администрированию). Это вполне могут быть троянские программы или незащищенные средства удаленного администрирования. Троянские программы, конечно, лучше обнаруживать не только при помощи сканеров безопасности, но и при помощи антивирусов;

– появление неизвестных администратору пользователей. Многие сканеры (например, LANGuard) показывают количество входов в сеть и время последнего входа в сеть для каждого пользователя. При помощи этой возможности иногда можно определить, когда появился тот или иной пользователь;

– ошибки в конфигурации компьютера. Ошибки допускаются всеми, и, иногда, в сети организации можно найти сервер Oracle с паролями привилегированных пользователей, установленными по умолчанию, или SQL Server, для учетной записи SA которого назначен пустой пароль, или другие продукты с оставленными по умолчанию паролями. Использовать такие ошибки для получения

полного контроля над системой (а иногда и доменом) совсем несложно, поэтому есть смысл регулярно проверять сеть на предмет наличия таких проблем в настройках.

Предварительная подготовка

Создание виртуального компьютера с помощью VMware Workstation

Создание виртуального компьютера необходимо для того, чтобы использовать для работы не реальный сервер, обеспечивающий работу сети, а виртуальный, работоспособность которого никак не повлияет на текущую работу сети.

Для создания виртуального компьютера удобно использовать программу VMware Workstation.

Для этого в главном меню программы надо выбрать file => New => New Virtual Machine или нажать Ctrl+N.

1. Перед вами появится окно New Virtual Machine Wizard. В меню Virtual Machine Configuration необходимо выбрать Typical => Next (рис. 3.1).

2. Выберите с чего производить установку: с физического устройства либо iso-файла (рис. 3.2).

3. Затем вам предложат выбрать операционную систему. В меню Guest Operating System выбрать Windows Server 2003 Enterprise Edition => Next. Далее вводим ключ к Windows Server 2003 Enterprise Edition (рис. 3.3).

4. Далее вам предложат задать имя виртуального компьютера и его месторасположение. Например, Virtual Machine Name: WinServ_2003_EE, Location: C:\Program Files\My Virtual Machines\WinServ 2003 EE => Next.

5. Затем идет выбор «жесткого» диска. Выберите емкость диска. Поскольку программа выделяет под диск реальное количество места на диске. Виртуальный диск следует создать объемом 8.0GB. => Next.

6. Далее программа покажет созданный файл, в котором храниться информация о диске. Finish.

Рис. 3.1. Шаг 1. Главное меню New Virtual Machine Wizard

Рис. 3.2. Шаг 2. Выбор устройства

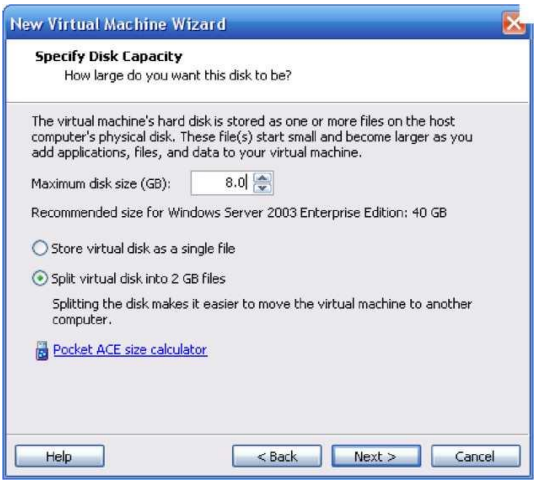


Рис. 3.3 . Шаг 3. Выбор ОС

Рис. 3.4. Шаг 5. Выбор «жесткого» диска

Таким образом, появился новый виртуальный компьютер.

Установка операционной системы на нем абсолютно аналогична реальному компьютеру. Включение и выключение вирту-

ального компьютера осуществляется кнопками «Power on» (Ctrl+B) и «Power off» (Ctrl+E) на главной панели.

Установка операционной системы на нем абсолютно аналогична реальному компьютеру.

После установки Windows Server 2012 настройте сетевое подключение. Задайте IP-адрес (например, 192.168.1.1) и маску подсети (например, 255.255.255.0).

Подключение одновременно нескольких пользователей

Для того чтобы была возможность подключения к виртуальной машине сразу нескольких пользователей (студентов) необходимо установить Remote Administrator 2.2 на виртуальную машину и машины студентов.

Подключение к виртуальной машине необязательно, но оно дает более наглядное представление о сканировании, т.к. в момент тестирования сервер выдает всевозможные замечания о переполнении буфера и др.

Установка происходит обычным способом.

Важно отметить, что при вводе пароля для Remote Administrator Server не следует ставить галочку в *NT security.* (рис. 3.5).

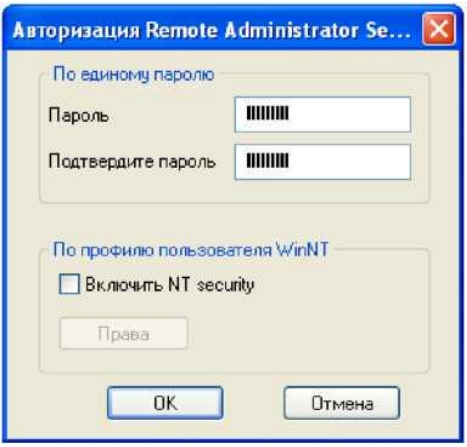


Рис. 3.5. Ввод пароля для Remote Administrator Server

Далее необходимо произвести перезагрузку компьютера (рис. 3.6)

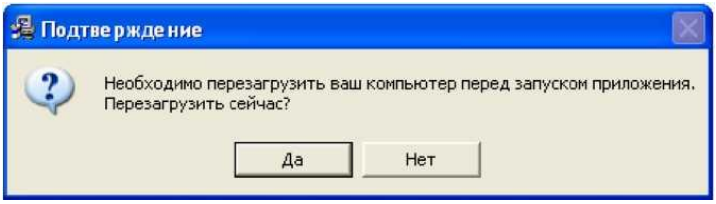


Рис. 3.6. Перезагрузка

После установки необходимо создать новые соединения со всеми клиентскими компьютерами на виртуальном компьютере, а также на клиентских компьютерах с виртуальным Windows Server 2012. Для создания соединения необходимо в меню «Соединения» выбрать «Подключиться к...» ввести IP-адрес машины, к которой создается подключение, и нажать «Подключиться» (рис. 3.7, рис. 3.8.).

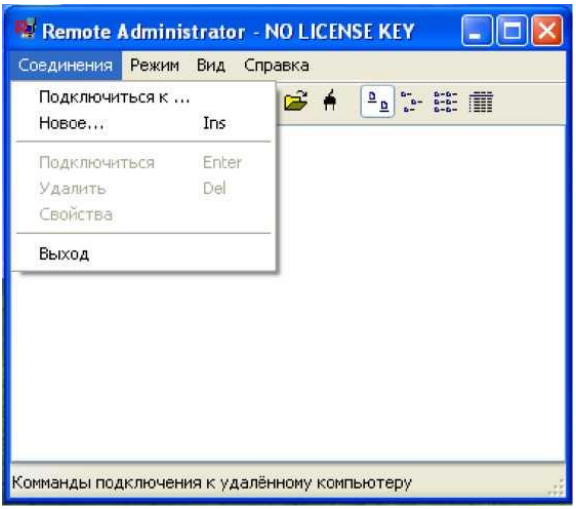


Рис. 3.7. Подключение

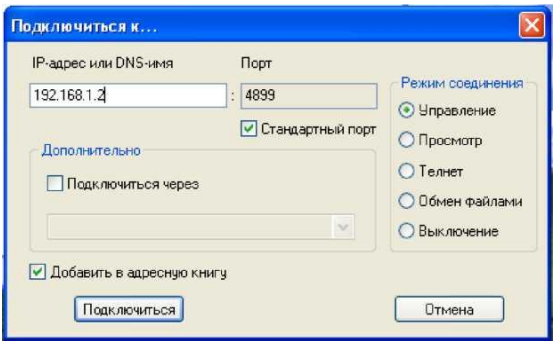


Рис. 3.8. Ввод IP-адреса

Рабочее задание

Раздел 1. «Ревизор Сети»

Часть 1

1. Если включен Remote Administrator, то отключите его.
2. Запустите «Ревизор Сети» на своем компьютере.
3. Настройте параметры сессии.
4. Сформируйте план сканирования сети.
5. Выполните план проверки.
6. По окончании сканирования сформируйте отчет и проанализируйте его.

Часть 2

1. Зайдите на виртуальную машину с помощью программы Remote Administrator v2.2.
2. Запустите «Ревизор Сети» на своем компьютере.
3. Настройте параметры сессии.
4. Сформируйте план сканирования сети.
5. Выполните план проверки.
6. По окончании сканирования сформируйте отчет и проанализируйте его.
7. Сравните отчеты из первой и второй части.

Раздел 2. Выводы по сканированию

1. Сделайте анализ возможных уязвимостей.
2. Объясните результаты сканирования.

Примечание

В результате выполнения данной лабораторной работы может быть установлено, что программное обеспечение без обновлений содержит немалое количество уязвимостей, которые критическим образом могут сказаться на работе системы. Необходимо отметить, что нельзя с уверенностью сказать, что это все уязвимости в данном продукте. Это только часть уязвимостей, которые уже выявлены. Поскольку уязвимости имеют свойства появляться спонтанно, нет гарантии, что в данном программном обеспечении со временем не найдется еще одна лазейка для хакера. Таким образом, очень важно уделять безопасности должное внимание и делать соответствующие проверки регулярно, т.к. проблема обеспечения безопасности не сводится к разовому аудиту системы.

Вопросы по лабораторной работе

1. Что такое анализ уязвимостей? В чем заключается его специфика?
2. Назовите риски, связанные с ПО, поставляемым поставщиком.
3. Назовите риски, связанные с действиями администратора.
4. Назовите риски, связанные с деятельностью пользователя.
5. Опишите возможности сетевого сканирования.

ЛАБОРАТОРНАЯ РАБОТА № 4

Контроль уязвимостей на уровне операционных систем и прикладного ПО

Цель: Получение практических навыков анализа работы сканера безопасности «Ревизор Сети» на уровне закрытия уязвимостей.

Введение

Интенсивное внедрение сетевых компьютерных технологий во многие сферы жизни общества обусловило появление сложной и острой проблемы защиты информации в компьютерных сетях. Только в глобальной сети Internet ежегодно регистрируется несколько тысяч серьезных нарушений безопасности информации. В России развернуты и функционируют десятки крупных компьютерных сетей, защита информации в которых также представляет собой серьезную проблему.

Средства защиты информации разделяются на два класса:

1) средства защиты информации в компьютерах (серверах и рабочих станциях);

2) средства защиты информации, циркулирующей в компьютерной сети.

Одними из самых распространенных программных и программно-аппаратных средств анализа уязвимостей компьютерной сети являются сканеры безопасности.

Сканеры безопасности подразделяются по типам обнаруживаемых уязвимостей на подгруппы:

1) средства анализа (верификации) алгоритмов программно-аппаратного обеспечения;

2) средства поиска уязвимостей программно-аппаратных средств реализации компьютерной сети на основе анализа исход-

ных текстов и на основе исполняемого кода (в том числе путем анализа размера и даты файла, проверки времени выполнения кода, правильности использования памяти, переполнения стека, правильности вызова функций, а также на основе использования системы генерации тестов, дизассемблирования и использования сканеров первой группы, имитации атак);

3) средства поиска уязвимостей программно-аппаратных средств обеспечения функционирования сети (сетевых сервисов и протоколов), операционной системы и сетевого прикладного программного обеспечения (по параметрам учетных записей, длине и сроку действия паролей, по правам пользователей на до доступа к критичным ресурсам, например, системным файлам, к системному реестру и др.).

Рабочее задание

Раздел 1. «Ревизор Сети»

1. Запустите «Ревизор Сети» на своем компьютере.
2. Настройте параметры сессии. Особое внимание обратите при вводе IP- адреса вашего компьютера.
3. Сформируйте план сканирования сети.
4. Выполните план проверки.
5. По окончании сканирования сформируйте отчет и проанализируйте его.

Раздел 2. Выводы по сканированию

1. Обоснуйте результаты сканирования.

Ожидаемые результаты

В результате проведенной лабораторной работы может быть получен 1 отчет по поискам уязвимостей сканером безопасности «Ревизор Сети» (табл. 4.1).

Исходя из полученных результатов, рекомендуется использовать не один сканер безопасности в сети.

Таблица 4.1. **Результаты поискам уязвимостей**

Найдено уязвимостей	**«Ревизор Сети»**
Серьезные	1
Уязвимость	6
Информация	-

Вопросы по лабораторной работе

1. Что такое сканеры безопасности? В чем заключается его принцип работы?
2. На какие типы по обнаруживаемым уязвимостям подразделяются сканеры безопасности?
3. Расскажите, в чем заключается принцип работы сканера безопасности «Ревизор Сети» на уровне закрытия уязвимостей.
4. Опишите средства защиты информации в компьютерах (серверах и рабочих станциях).
5. Опишите средства защиты информации, циркулирующей в компьютерной сети.

ЛАБОРАТОРНАЯ РАБОТА № 5

Контроль уязвимостей на уровне системы управления базами данных

Цель: Получение практических навыков работы со сканерами баз данных с целью предотвращения несанкционированных действий с базами данных. Получение навыков поиска уязвимостей в составе и настройках прикладного программного обеспечения (СУБД Oracle) с помощью специально разработанных средств – сканеров безопасности баз данных.

Сценарий проведения лабораторной работы

1. Установить на учебном стенде сканер безопасности баз данных AppDetectivePro (Trial версия).
2. Настроить AppDetectivePro для выявления уязвимостей базы данных на учебном стенде.
3. Выполнить PenTest (тест по выявлению уязвимостей в обнаруженных базах данных) средствами тестера AppDetectivePro.
4. Выполнить аудит базы данных по вопросам парольной политики, доступа к таблицам, допустимости ролей пользователей и др.
5. Выявить права пользователей (user rights) в базе данных.
6. Сформировать отчеты по результатам выявления уязвимостей базы данных посредством AppDetectivePro.

Реализация сценария лабораторной работы

Установка AppDetectivePro

AppDetectivePro сложный и ёмкий продукт. Он включает базу знаний большого объема (690 Мб), в которой содержатся сведения о возможных уязвимостях баз данных под управлением наиболее известных СУБД. База знаний постоянно поддерживается в актуальном состоянии фирмой Application Security – разработчиком AppDetectivePro.

Перечень компонентов, требуемых для установки AppDetectivePro, появляется при запуске программы установки appdetective_setup.exe и включает восемь элементов:

- Microsoft XML Core Services 4.0 SP2;
- Microsoft .NET Framework 2.0 SP1 (x86);
- Microsoft Visual Studio 2005 C++ Redistributable (x86);
- SQL Server 2005 Backwards Compatibility (x86);
- Datable Component 2.3;
- SHATTER knowledgebase 2.4;
- WinPcap
- AppDtectivePro.

Среди этих компонентов есть WinPcap, который находится в режиме свободного распространения и свободно доступен для ОС Windows вплоть до 10 версии.

Его и надо установить еще до установки AppDetectivePro. WinPcap – сокращение от Windows Packet Capture (сбор пакетов Windows).

При наличии установленных WinPcap 3.1, Windows installer 3.1 установка AppDetectivePro проходит гладко без особых приключений. Надо только внимательно смотреть за сообщениями мастера установки и реагировать соответствующим образом. Реакция заключается, в частности, в согласии с лицензионным соглашением, в согласии устанавливать очередной компонент, а также (в одном из сообщений) – в выборе варианта хранения базы знаний: в ACCESS или в MS SQL. Вариант ACCESS предпочтительней при работе с trial версией AppDetectivePro, во-первых, по той причине, что в этой версии AppDetectivePro позволяет работать только с одним сервером базы данных Oracle и с одной инстанцией, а во-вторых, в связи с этим ограничением, высокая относительно ACCESS производительность MS SQL сервера не потребуется.

Настройка AppDetectivePro для выявления уязвимостей базы данных на учебном стенде

Работа со сканером AppDetectivePro начинается с создания сессии. В ходе создания сессии сканер выполняет предварительные действия по настройке своей работы – логическое группирование приложений и сканера перед выполнением собственно тестирования. В частности, в базе знаний тестера выделяется группа правил для тестирования СУБД выбираемого типа, в исполняемых программах тестера осуществляется логическая привязка именно к этим разделам базы знаний. Завершается создание сессии процессом Discovery – выявлением всех серверов по указанным при формировании сессии IP-адресам и номерам портов.

При запуске сканера (пуск => Все программы => AppSecInc => AppDetectivePro => AppDetectivePro) появляется экран (рис. 5.1).

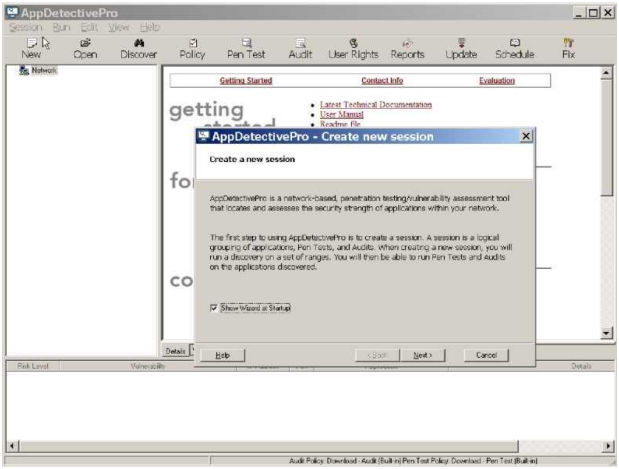


Рис. 5.1. Приглашение к созданию сессии

При нажатии кнопки «Next» выполняется переход к экрану с определением возможности прямого указания списка IP-адресов или выбора их из файла. Выбираем верхнюю радиокнопку (рис. 5.2).

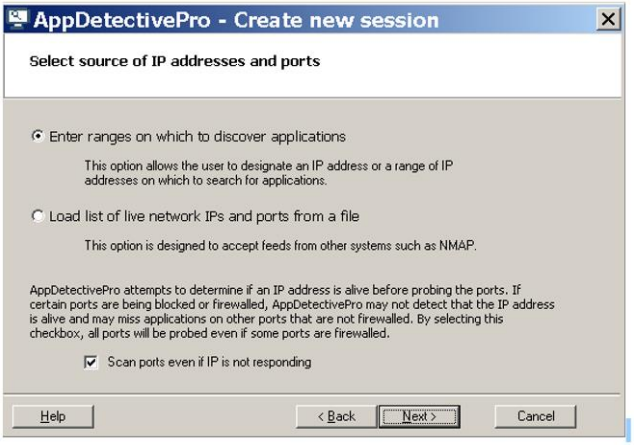


Рис. 5.2. Выбор источника IP-адресов и портов

Здесь же (рис. 5.2) заполнена checkbox, заставляющая сканировать порты даже в том случае, если IP-адрес не «отзывается». Далее следует указать конкретный (конкретные) IP-адрес(а), по которым будет проходить сканирование (рис. 5.3).

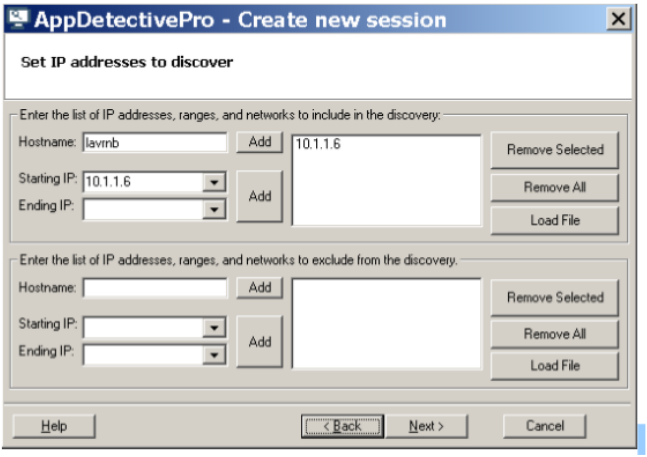


Рис. 5.3. Окно для указания диапазона IP адресов для сканирования

Здесь же (рис. 5.3) предлагается установить адреса, по которым сканеру не следует обращаться при обнаружении серверов баз данных.

Далее выбираем тип СУБД (рис. 5.4), сканирование баз данных под управлением которых мы собираемся осуществить.

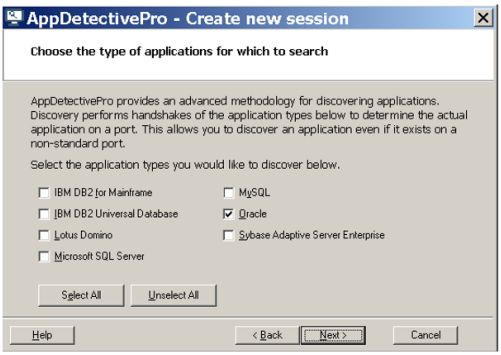


Рис. 5.4. Выбор типа СУБД для сканирования

Так как мы работаем с СУБД Oracle, мы отмечаем соответствующую checkbox. Далее сканер предлагает определить порты, с которыми он будет работать (рис. 5.5). Здесь мы укажем порты «по умолчанию». Для Oracle 10g это, в частности, порт «по умолчанию» 1521, на котором «слушает» listener.

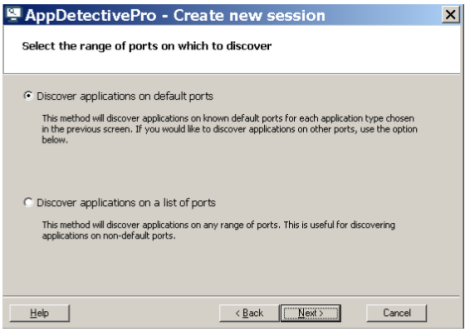


Рис. 5.5. Окно выбора сканируемых портов
для ранее указанных IP-адресов

Наконец, нам предлагается ввести название сессии (рис. 5.6), перечень задач для исполнения сканером (рис. 5.7), после чего сканер начинает свою работу поиска (discovery – открытия) баз под управлением указанной (указанных) СУБД.

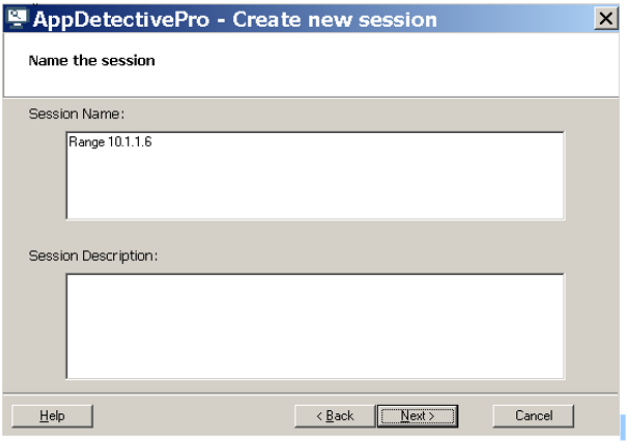


Рис. 5.6. Экран для задания названия сессии

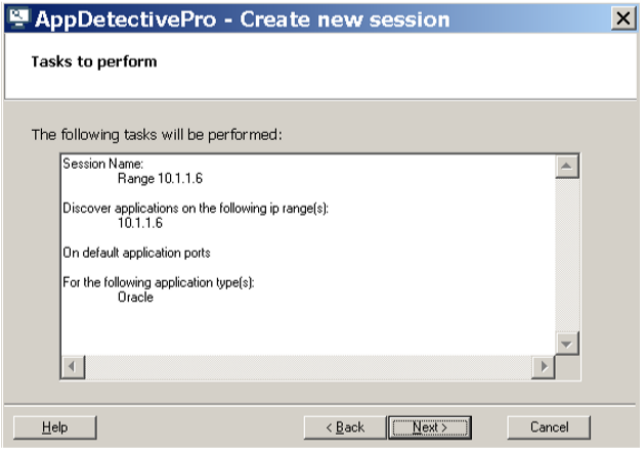


Рис. 5.7. Экран со сформированной на выполнение задачей

После завершения процесса «Discovery» (окно выполняемого процесса показано на рис. 5.8) в левом верхнем углу основного экрана AppDetectivePro рядом с «пикчей» «Network» слева появляется знак «+» (рис. 5.9). Это означает, что процесс «Discavery» обнаружил в сети сервер(ы) баз данных. При нажатии на «плюс» появляются обнаруженные сервера с указанием IP-адреса, порта для listener (при сканировании Oracle), базы данных (рис. 5.9).

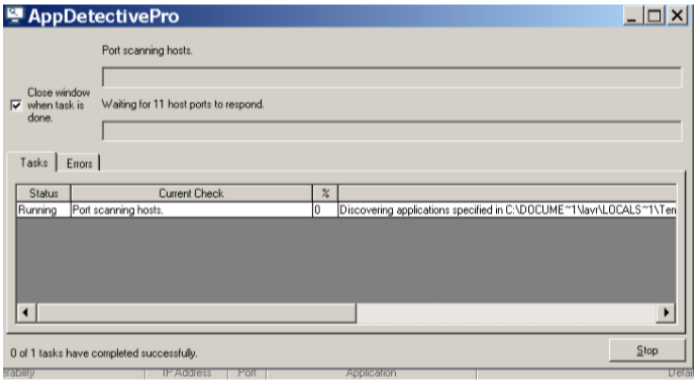


Рис. 5.8. Экран, демонстрирующий выполнение процесса «Discavery»

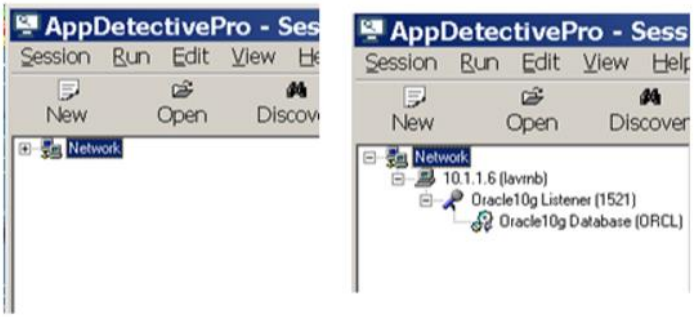


Рис. 5.9. Завершение процесса «Discovery»

Вариант создания сессии, который мы выше рассмотрели, связан с созданием новой сессии. AppDetectivePro сохраняет создан-

ные сессии, позволяет открывать предыдущие сессии, объединять предыдущие сессии.

Выполнение PenTest (тест по выявлению уязвимостей в обнаруженных базах данных) средствами тестера AppDetectivePro

Запуск PenTest-а показан на рис. 5.10.

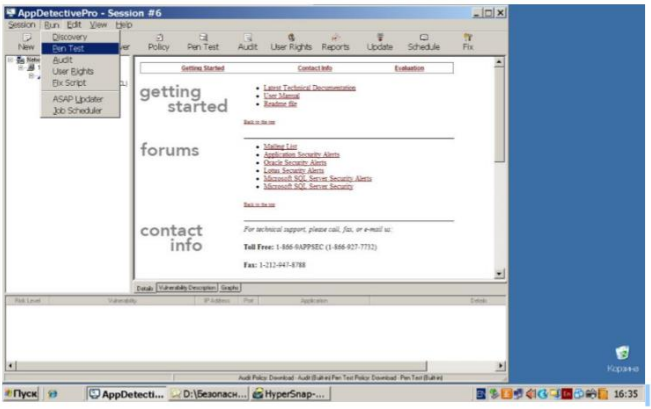


Рис. 5.10. Запуск PenTest-а в тестере AppDetectivePro

При запуске PenTest-а требуется отметить те базы, для которых предполагается выполнить этот тест (рис. 5.11).

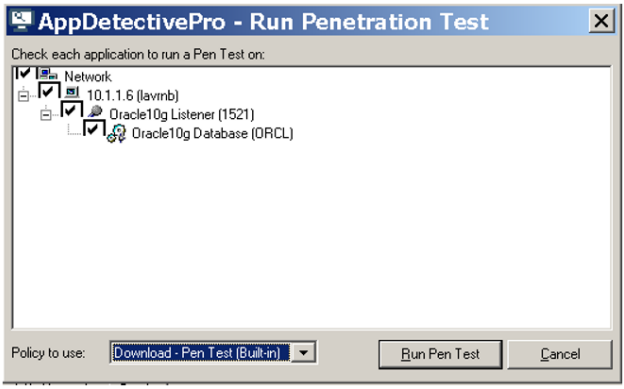


Рис. 5.11. Экран с выбором баз данных для тестирования

Перед запуском теста тестировщик предупреждается (рис. 5.12) о том, что в связи с попыткой связи с сервером Oracle по отдельным предустановленным аккаунтам (при установке сервера Oracle появляется ряд пользователей, пароли которых известны; тестер проверяет эти пароли и сигнализирует об уязвимости, если эти пароли не изменялись).

Рис. 5.12. Предупреждение о возможном блокировании некоторых пользователей Oracle в связи с проверкой их паролей

При ответе «Yes» тест начинает свою работу (рис. 5.13).

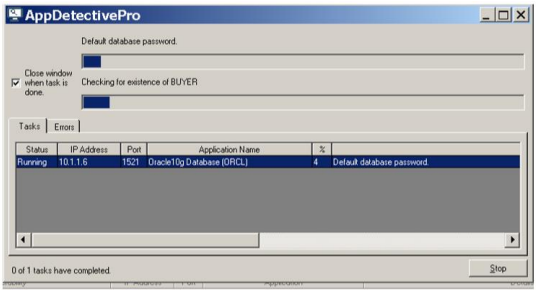


Рис. 5.13. Фрагмент процесса тестирования (проверяется существование пользователя BUYER и его пароль по умолчанию)

По завершению PenTest-а выводится список обнаруженных уязвимостей (рис. 5.14, 5.15). При выводе курсора на строку с вы-

явленной уязвимостью справа выше списка разворачивается текст с объяснением этой уязвимости.

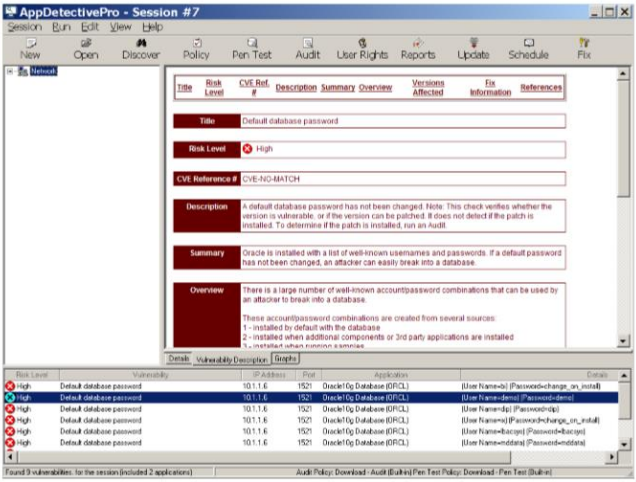


Рис. 5.14. Выявленная уязвимость: пароль, установленный по умолчанию,не изменялся

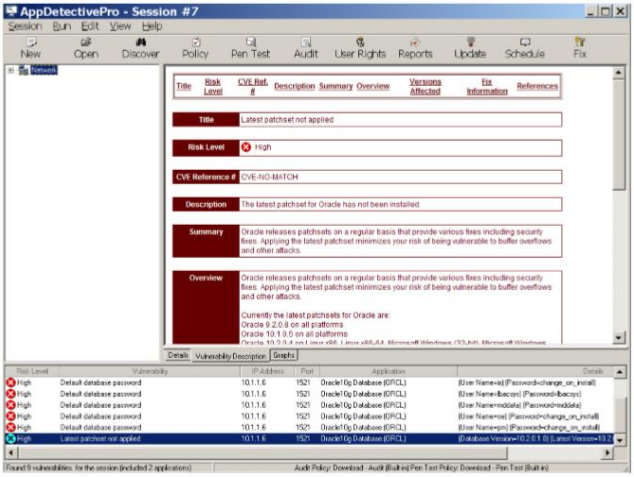


Рис. 5.15. Выявлена уязвимость: не установлен требуемый patch

По завершению работы PenTest-а в графическом виде можно увидеть общий результат его работы (рис. 5.16).

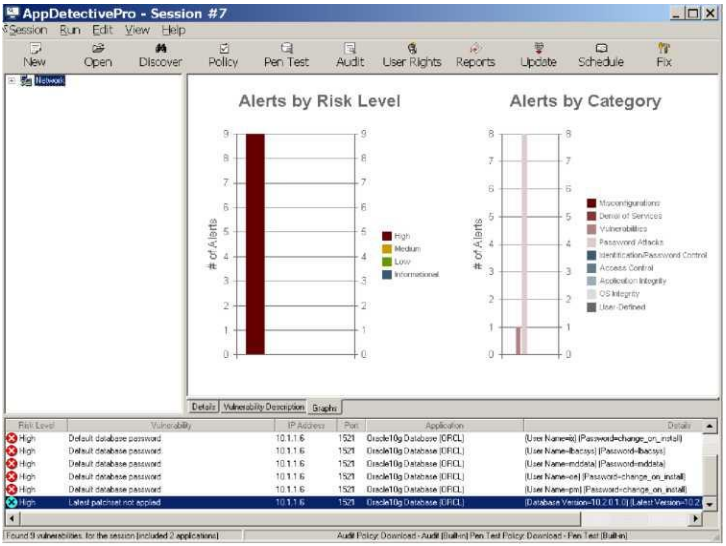


Рис. 5.16. Графическое представление результата работы PenTest-а

Левый график сообщает, что уровень риска по обнаруженным уязвимостям самый высокий (из четырех уровней), правый указывает категории уязвимостей (в данном примере их две из возможных девяти категорий).

Выполнение аудита базы данных по вопросам парольной политики, доступа к таблицам, допустимости ролей пользователей и др. На рис. 5.17, 5.18 показаны запуск аудита в тестере и выбор базы данных для тестирования.

Далее, чтобы запустить аудит, AppDetectivePro предлагает ввести имя пользователя и пароль (рис. 5.19). Для того чтобы такой ввод состоялся, надо кликнуть мышкой на строку «(Usemame=)(Password=)…». После чего надо ввести имя пользователя и его пароль (рис. 5.20).

Рис. 5.17. Запуск аудита в тестере

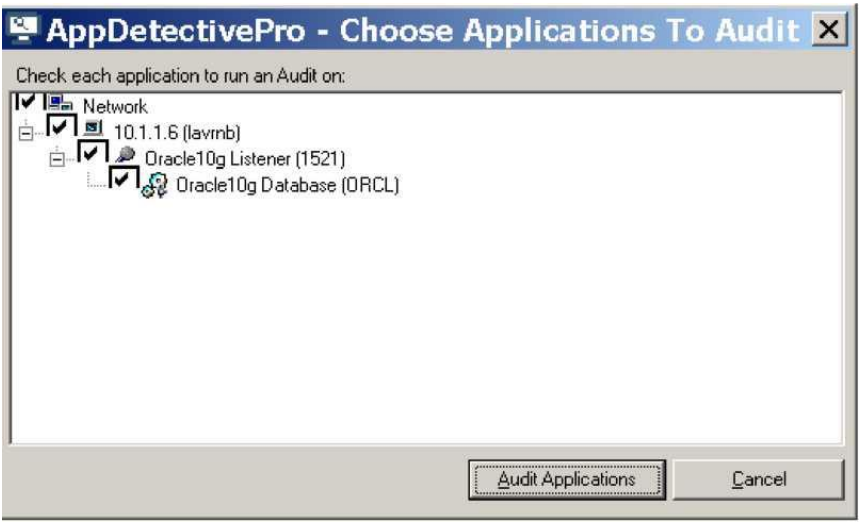


Рис. 5.18. Выбор базы данных для тестирования

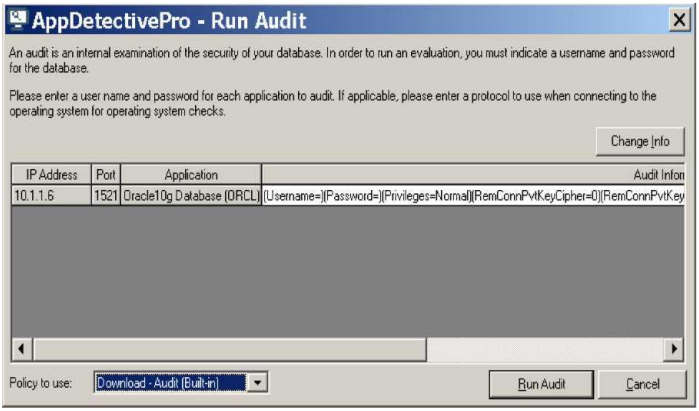


Рис. 5.19. Начало процесса аудита предполагает инициировать ввод имени и пароля (кликнуть мышкой на строку «(Username=)...»

Рис. 5.20. Предлагаемое для ввода имени и пароля окно

В окне, предлагаемом для ввода имени и пароля, есть кнопка проверки возможности соединения с базой данных с этими именем и паролем «Test DB connect». При нажатии этой кнопки появляется сообщение (рис. 5.21).

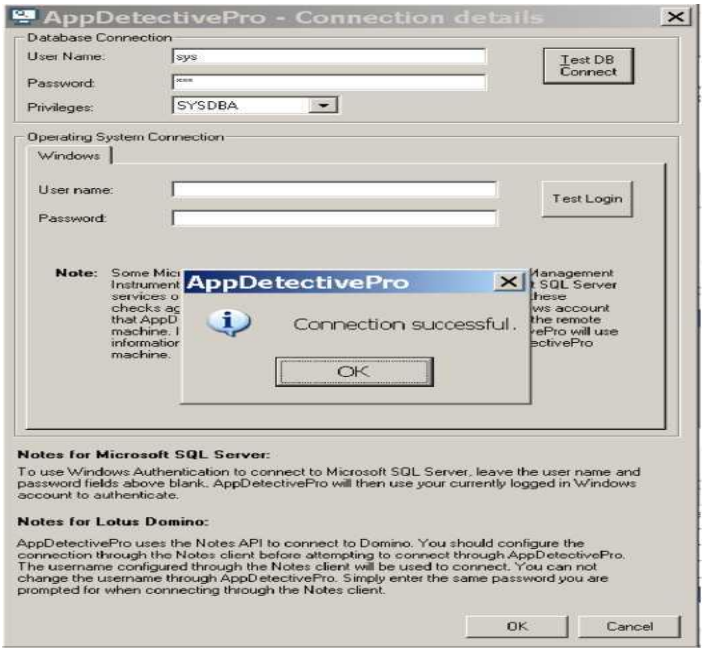


Рис. 5.21. Проверка соединения с базой данных для введенных аккаунтов

После подтверждения возможности соединения с базой данных надо нажатием «OK» вернуться к окну процесса аудита (рис. 5.22) для того, чтобы стартовать этот процесс.

После нажатия «Run Audit» инициализируется процесс аудита (рис. 5.23), выполняется аудит сложности пароля (рис. 5.24), аудит привилегий по работе со словарем базы данных (рис. 5.25), аудит объектных привилегий, назначаемых схеме «Public» (рис. 5.26).

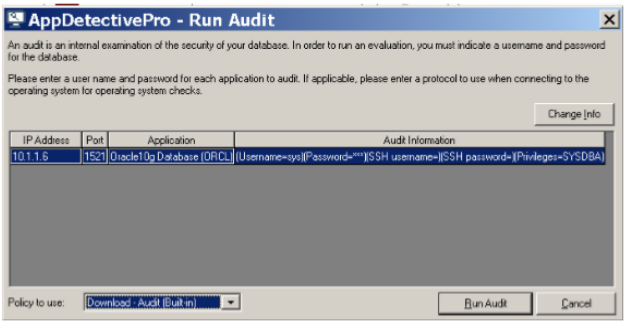


Рис. 5.22. Окно запуска процесса аудита

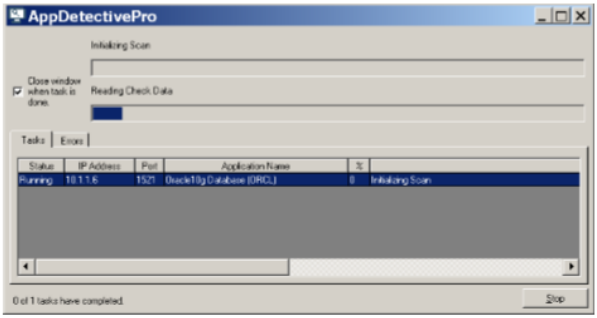


Рис. 5.23. Начало процесса аудита

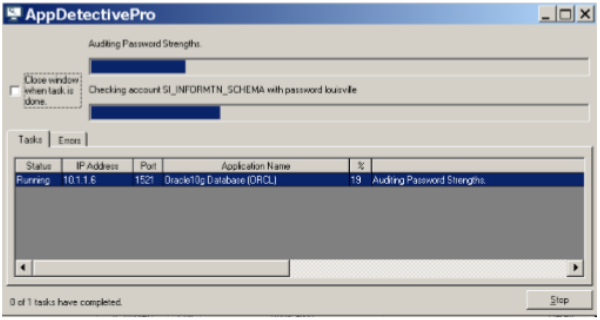


Рис. 5.24. Фрагмент процесса аудита сложности пароля

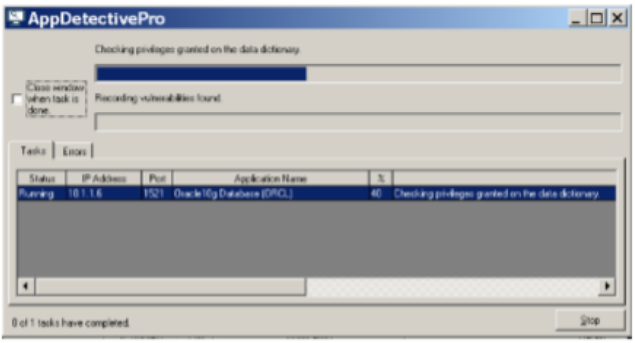


Рис. 5.25. Фрагмент процесса аудита привилегий
для работы со словарем базы данных

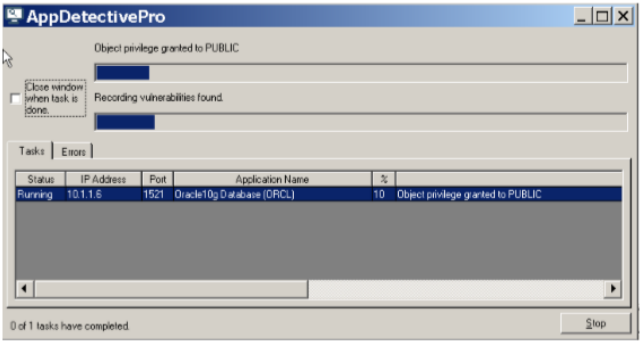


Рис. 5.26. Фрагмент процесса аудита объектных привилегий
схеме «Public»

По завершении процесса аудита формируется список обнаруженных уязвимостей, а также информационных сообщений. Список формируется в продолжение того списка, который был создан после выполнения PenTest-а.

Список уязвимостей настолько полон, что по нему можно учить администраторов настройке безопасности базы данных под управлением СУБД Oracle.

Первыми в списке появляются сообщения об уязвимостях с высоким уровнем нарушения безопасности (рис. 5.27). На рис. 5.27 выделена строка, показывающая, что пользователю ANYA предоставлена привилегия «Create library». Эта привилегия дает возможность пользователю дополнять ОС исполняемыми (binary) файлами.

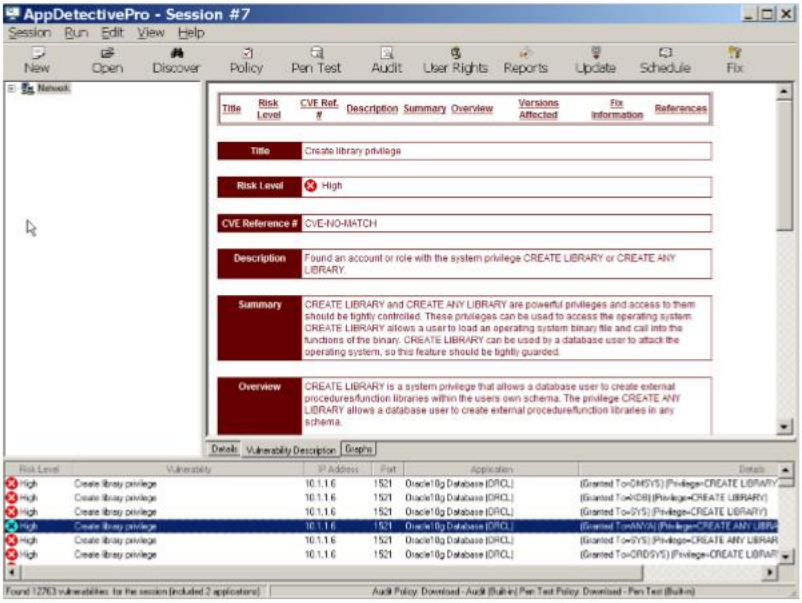


Рис. 5.27. Фрагмент сообщений аудита об уязвимости «create library privilege»

На рис. 5.28 следует отметить два сообщения. Первое – с высоким уровнем уязвимости (remote login password file not disabled), сообщает нам о том, что среди пользователей базы данных может быть несколько пользователей с привилегией «sysdba», так как параметр «remote_login_passwordfile» файла инициализационных параметров установлен в значение «exclusive». Второе – со сред-

ним уровнем уязвимости, сообщает нам о том, что пользователю ANYA предоставлена привилегия «ALTER SYSTEM». Здесь же в тексте выше дается пояснение, в чем состоит уязвимость (возможность менять системную дату), связанная с использованием этой привилегии.

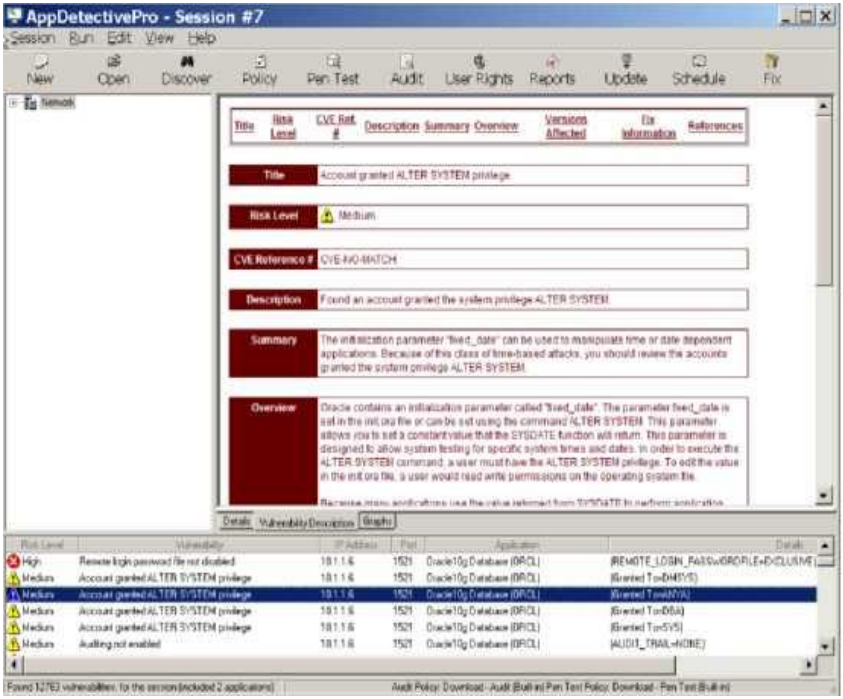


Рис. 5.28. Фрагмент сообщений аудита базы данных
(первая строка – сообщение с высоким уровнем уязвимости)

На рис. 5.29 показана группа выявленных уязвимостей среднего уровня «Database demonstration objects», связанных с тем, что учетные записи демонстрационных схем имеют пароли по умолчанию, которые не были изменены после установки СУБД Oracle.

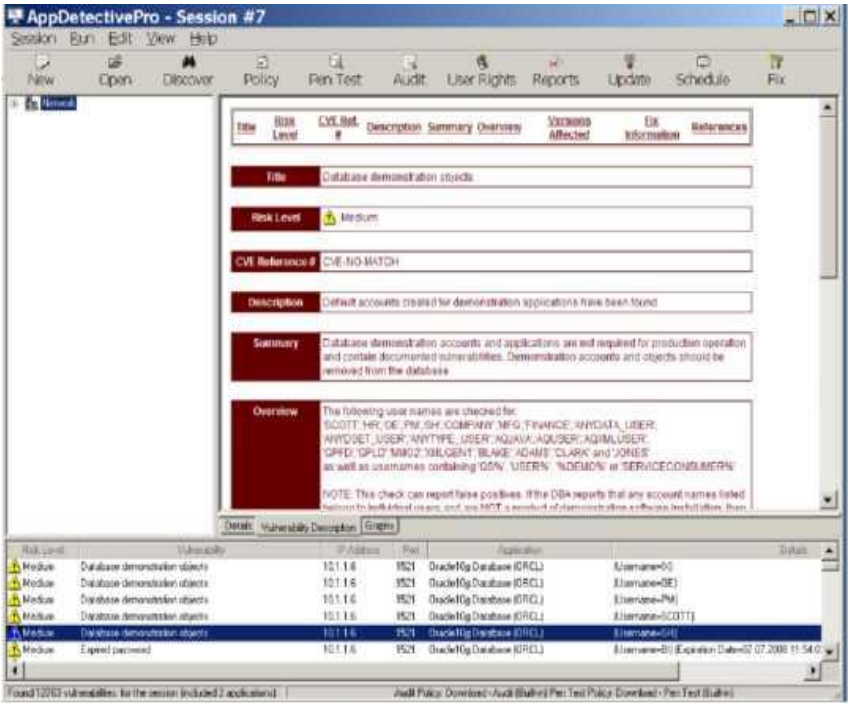


Рис. 5.29. Фрагмент сообщений аудита с выявленными уязвимостями по учетным записям демонстрационных схем

На рис. 5.30 показана группа выявленных уязвимостей среднего уровня «Expired Password». С такой уязвимостью пользователи не допускаются к работе с базой данных без того, чтобы пользователь поменял свой пароль.

На рис. 5.31 показан фрагмент сообщений аудита с группой выявленных уязвимостей среднего уровня «Overdue password change». Эта уязвимость сообщает нам о том, что пароль пользователя слишком долгое время не изменялся, что предоставляло потенциальному взломщику возможность определить его подбором.

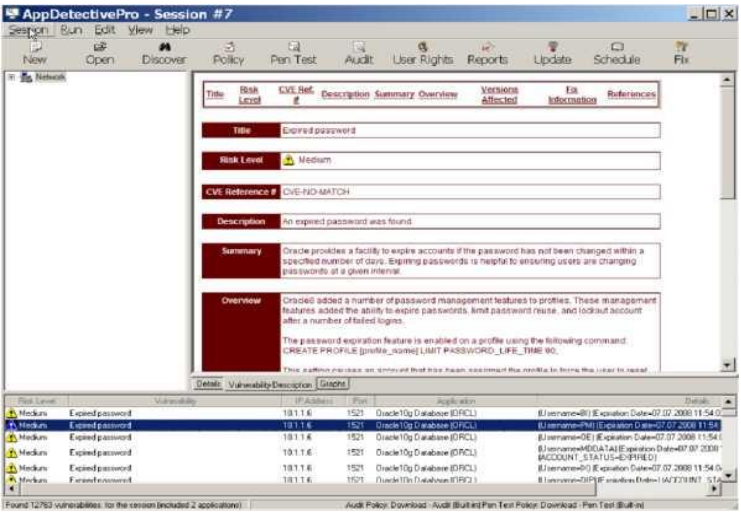


Рис. 5.30. Фрагмент сообщений аудита с выявленными уязвимостями пользователей, пароль которых должен быть изменен

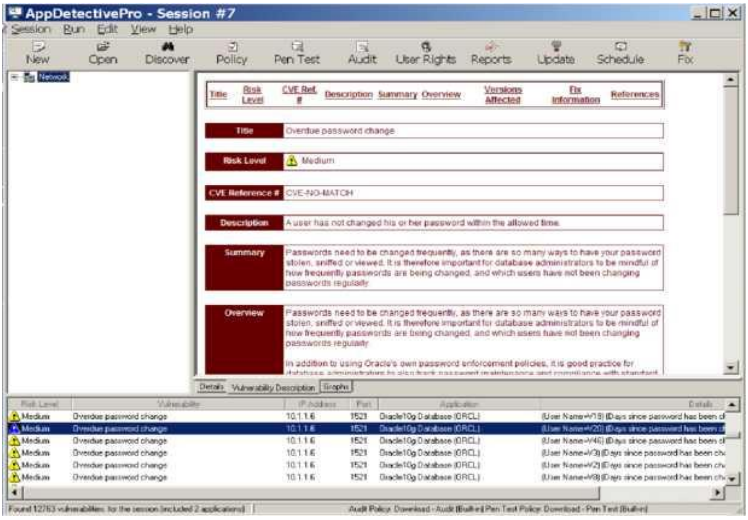


Рис. 5.31. Фрагмент сообщений аудита с найденными пользователями, пароль которых недопустимо долгое время не менялся

На рис. 5.32 показан фрагмент сообщений аудита, в котором отметим две позиции. Первая (SYS operations not audited) сообщает о том, что действия пользователя SYS с объектами базы данных (select, insert и т.д.) не регистрируются. Следующие сообщения говорят о назначении пользователям системных привилегий «напрямую», а не через роль, что значительно усложняет работу администратора.

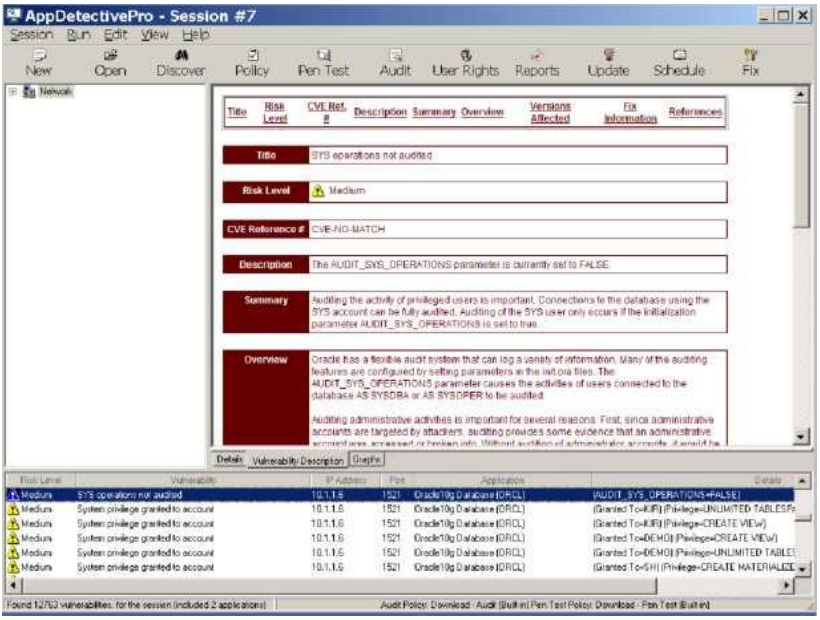


Рис. 5.32. Фрагмент сообщений аудита об отсутствии контроля действий пользователя SYS и о выдаче «напрямую» системных привилегий ряду пользователей

На рис. 5.33 показан фрагмент сообщений аудита о выявлении группы пользователей с профилем «DEFAULT». Некоторые параметры в профиле «DEFAULT» не ограничены, что создает дополнительные возможности для потенциального взломщика.

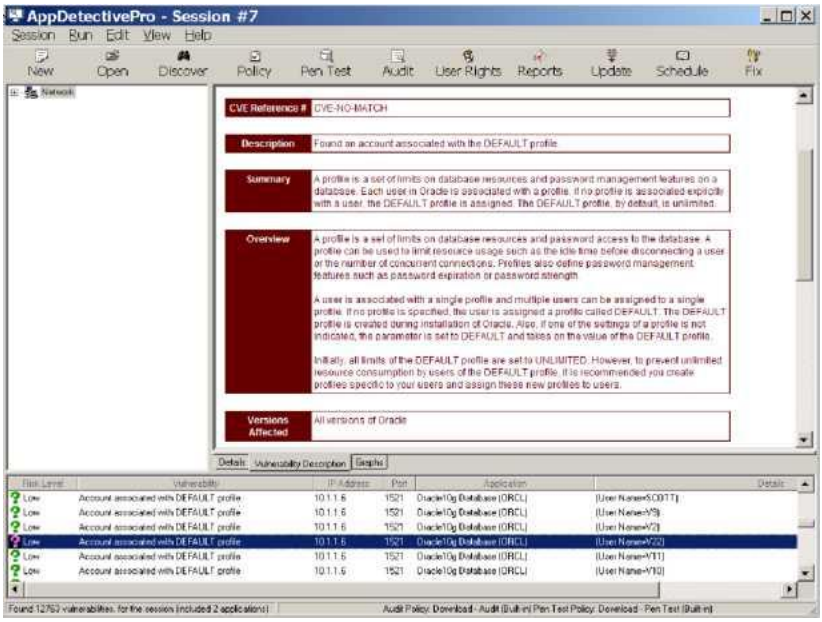


Рис. 5.33. Фрагмент сообщений аудита
с выявленной группой пользователей с профилем «DEFAULT»

На рис. 5.34 представлен фрагмент сообщений аудита с выявленной уязвимостью (низкого уровня) предоставления предопределенной роли «RESOURCE» группе пользователей. Эта роль позволяет пользователю создавать таблицы, программные коды.

На рис. 5.35 показан фрагмент сообщений аудита с возможной уязвимостью низкого уровня, заключающейся в том, что владелец объекта выдает объектную привилегию на свой объект с правом передачи этой привилегии другим пользователям. Вот это право передачи объектной привилегии другим пользователям ставится под сомнение. Внимание разработчика приложения фиксируется на этом моменте, чтобы разработчик еще раз проверил правильность столь важной добавки «WITH GRANT OPTION» в команду выдачи объектной привилегии.

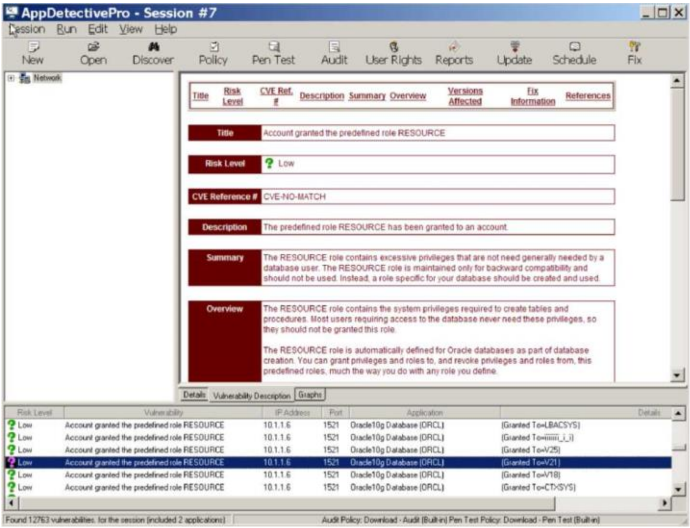


Рис. 5.34. Фрагмент сообщений аудита с выявленными пользователями, получившими предопределенную роль «RESOURCE»

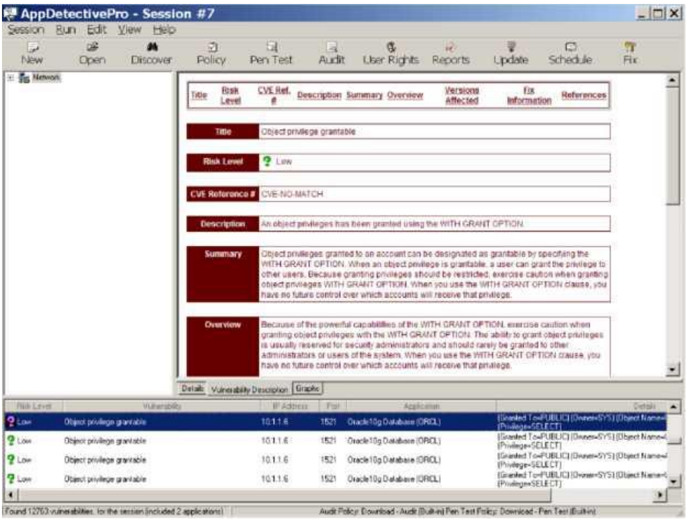


Рис. 5.35. Фрагмент сообщений аудита с выявленными пользователями, получившими объектную привилегию с правом передачи

На рис. 5.36 показан фрагмент сообщений аудита о предоставлении объектных привилегий пользователям «напрямую», а не через роль, что значительно усложняет работу администратора при разграничении полномочий пользователей.

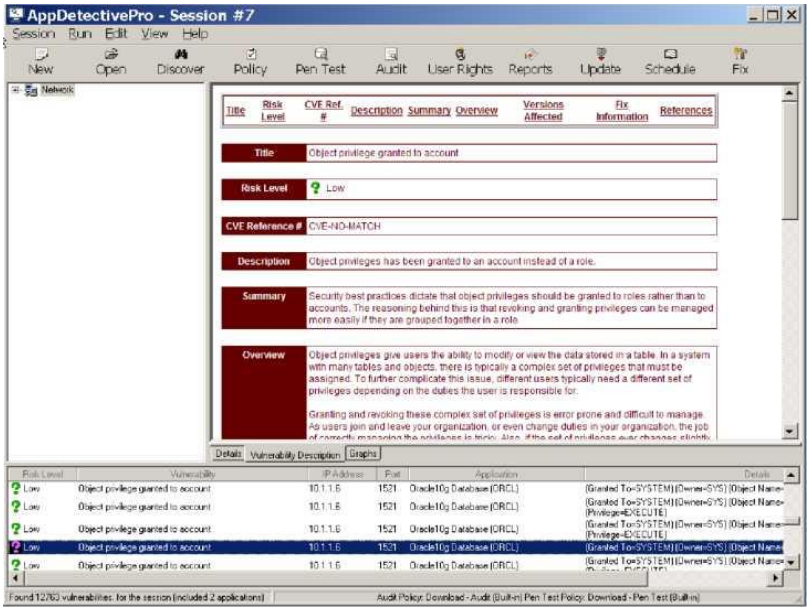


Рис. 5.36. Фрагмент сообщений аудита
с выявленной группой пользователей, которым назначены «прямые», не через роль объектные привилегии

На рис. 5.37 представлены сообщения аудита о выдаче группе пользователей системных привилегий с опцией «WITH ADMIN OPTION». Получившие с этой опцией системную привилегию пользователи могут передавать эту привилегию другим пользователям.

На рис. 5.38 показан фрагмент сообщений аудита с выявленными пользователями, которым предоставлена мощная системная привилегия с опцией «ANY». С этой привилегией пользователи могут выполнять действия не только в своей, но и в любой схеме.

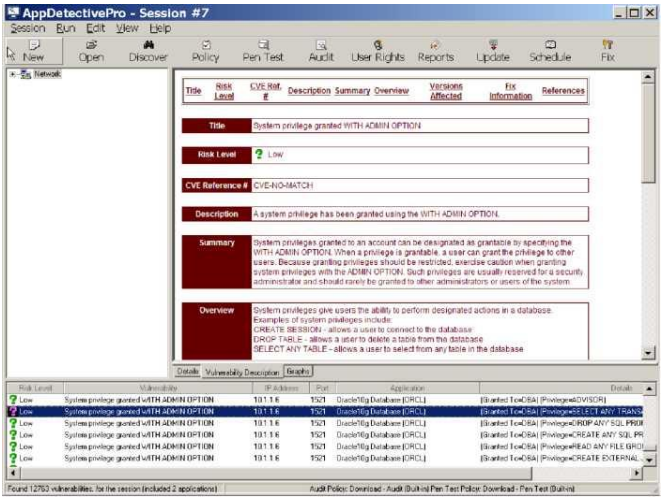


Рис. 5.37. Фрагмент сообщений аудита
с выявленной группой пользователей с системной привилегией,
которую они могут передавать другим пользователям

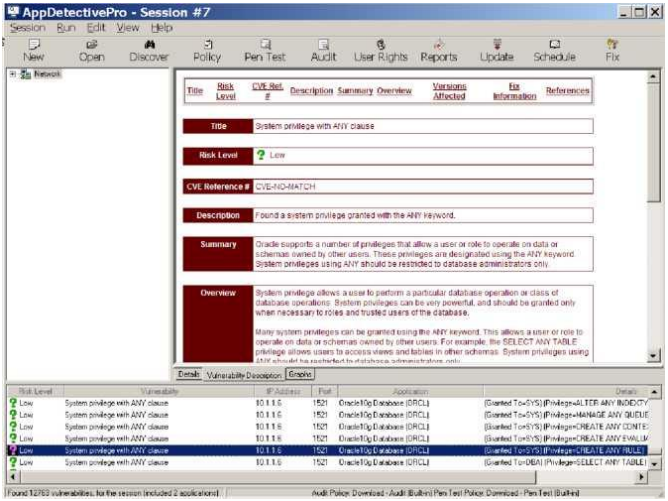


Рис. 5.38. Фрагмент сообщений аудита с выявленной группой
пользователей, имеющих системную привилегию с опцией «ANY»

На рис. 5.39 показан фрагмент информационных сообщений аудита о выявленных пользователях с заблокированным аккаунтом.

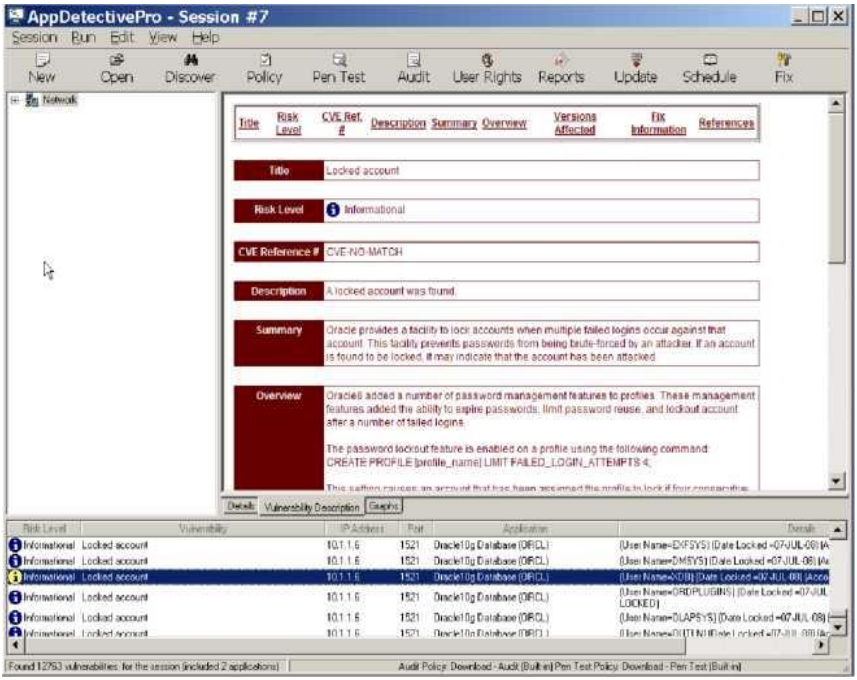


Рис. 5.39. Фрагмент сообщений аудита
о пользователях с заблокированным аккаунтом

Выявление прав пользователей (user rights) в базе данных

Администратору безопасности полезно иметь общую сводку прав отдельных или даже всех пользователей базы данных. Права включают прямые системные и объектные привилегии, эти же привилегии, но даваемые пользователям через роли, наконец, роли, назначенные пользователям.

Для получения такой информации в AppDetectivePro предусмотрена утилита UserRights (запуск ее показан рис. 5.40).

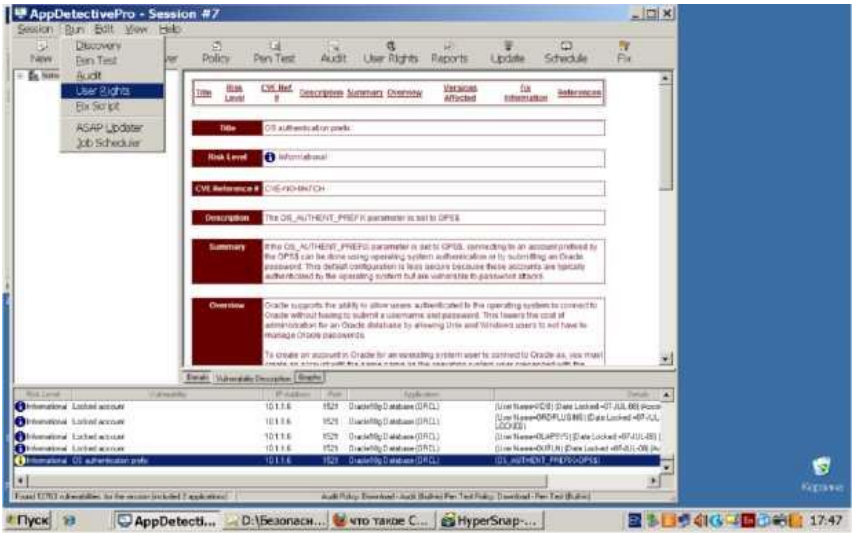


Рис. 5.40. Запуск утилиты UserRights

Для запуска утилиты предлагается окно выбора сервера (рис. 5.41).

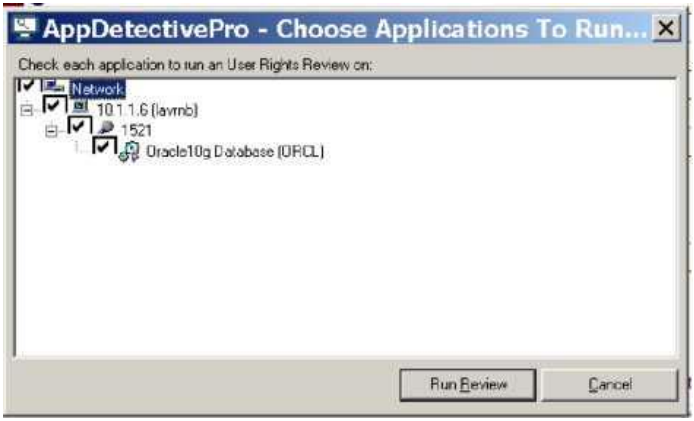


Рис. 5.41. Окно выбора сервера

Затем необходимо в появившемся окне процесса проверки прав пользователей (рис. 5.42) нажать мышкой на строку «(Username=)(Password=)».

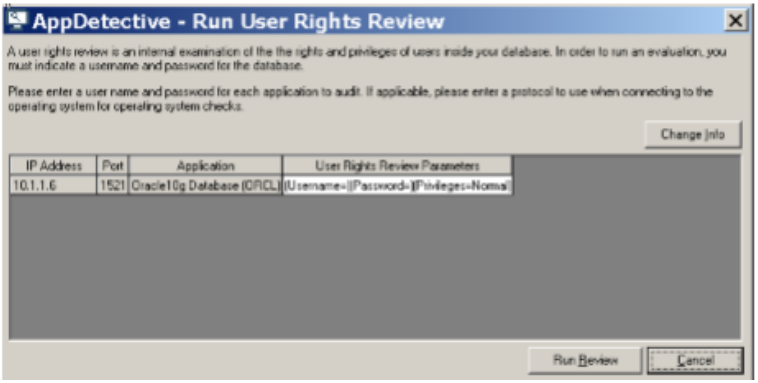


Рис. 5.42. Окно процесса проверки прав пользователей

После нажатия на строку «(Username)(Password)» появляется окно для ввода имени пользователя, пароля и типа пользователя (рис. 5.43).

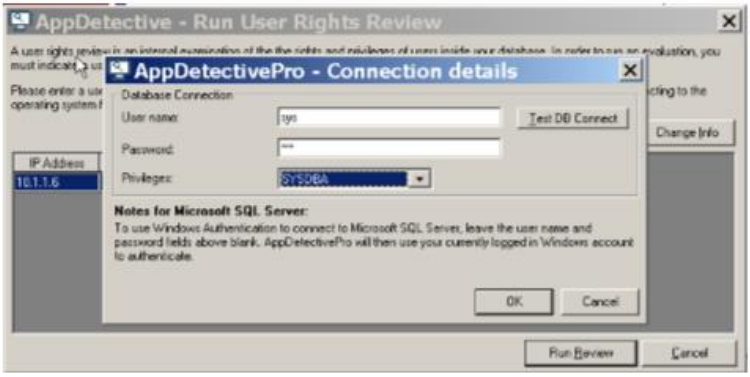


Рис. 5.43. Окно для аутентификации пользователя

Для проверки соединения справа вверху (рис. 5.43) надо нажать кнопку «Test DB Connect». После чего надо получить подтверждение успешной аутентификации (рис. 5.44).

После проверки аккаунтов анализируемого пользователя надо нажать две разные кнопки «OK» и выйти к готовому к запуску окну процесса проверки прав пользователя (рис. 5.45).

Рис. 5.44. Экран подтверждения аутентификации

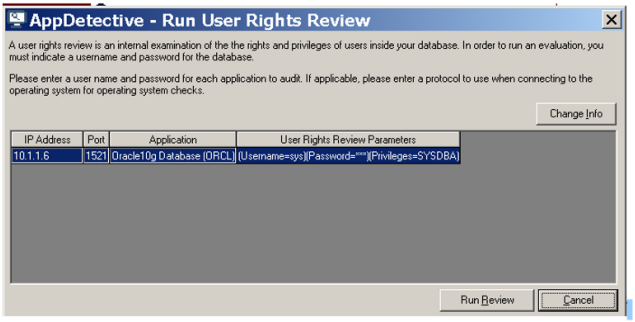


Рис. 5.45. Окно процесса проверки прав пользователя (SYS), готового к запуску

На рис. 5.46 показано промежуточное состояние процесса проверки прав пользователя SYS. В ходе работы в этом окне показывается число учтенных объектов пользователя и общее число этих объектов (таблиц, представлений, процедур и т.д.).

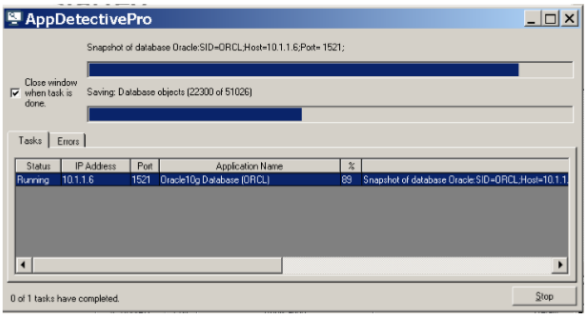


Рис. 5.46. Промежуточное состояние процесса проверки прав пользователя SYS

В ходе работы утилиты «User Rights» процесс проверки сопровождается появлением окон проверки объектов выбранного пользователя (рис. 5.46), всех столбцов (таблиц и представлений) этого пользователя (рис. 5.47), объектных привилегий пользователя (рис. 5.48), ролей (и входящих в них привилегий), принадлежащих данному пользователю (рис. 5.49).

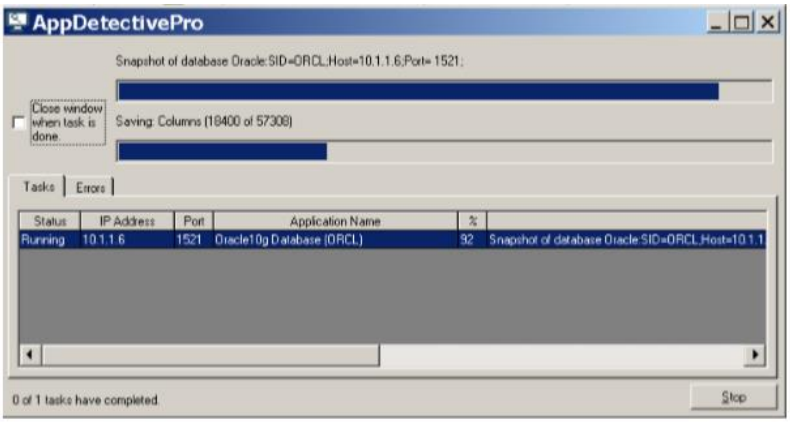


Рис. 5.47. Проверка прав пользователя SYS по работе со столбцами таблиц и представлений

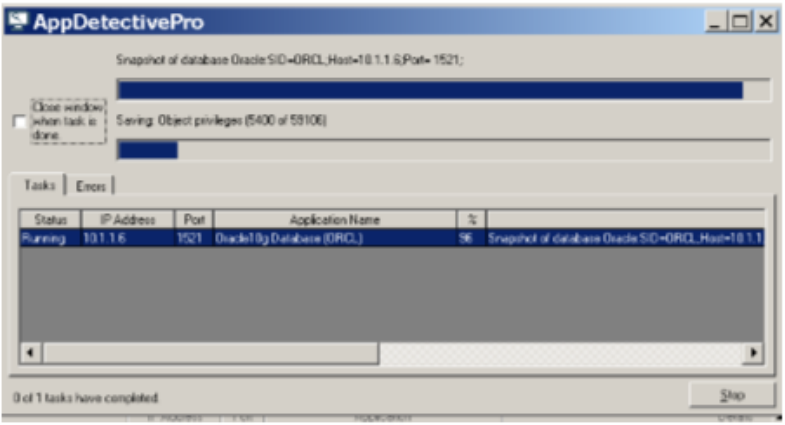


Рис. 5.48. Проверка объектных привилегий пользователя SYS

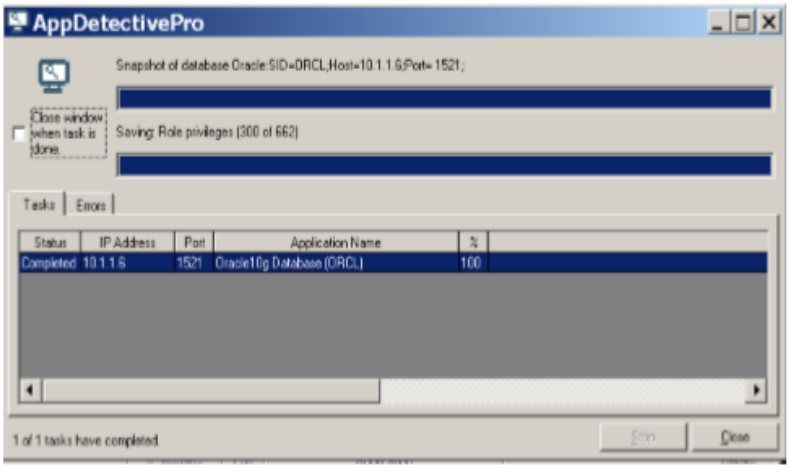


Рис. 5.49. Проверка ролей пользователя SYS

Результат работы утилиты «UserRights» можно просмотреть в отчетах AppDetectivePro. В настоящем описании возможности AppDetectivePro по составлению отчетов будут рассмотрены в следующем пункте.

Формирование отчетов по результатам выявления уязвимостей базы данных посредством AppDetectivePro

Работа с утилитой «Report» начинается с нажатия на кнопку «Report» в главном меню AppDetectivePro (рис. 5.50)

На рис. 5.50 видна возможность выбора в формировании отчета отдельно для Audit и PenTest-a, отдельно для проверки UserRights. На рис. 5.51–5.55 показаны окна, предъявляемые пользователю при формировании отчета для выполненных Audit-a и PenTest-a. На рис. 5.51 показано окно выбора варианта отчета. На рис. 5.52 показано окно выбора типа отчета. На рис. 5.53 показано окно выбора формы отчета. На рис. 5.54 показано окно проверки параметров формируемого отчета. На рис. 5.55 показано окно небольшого фрагмента итогового отчета.

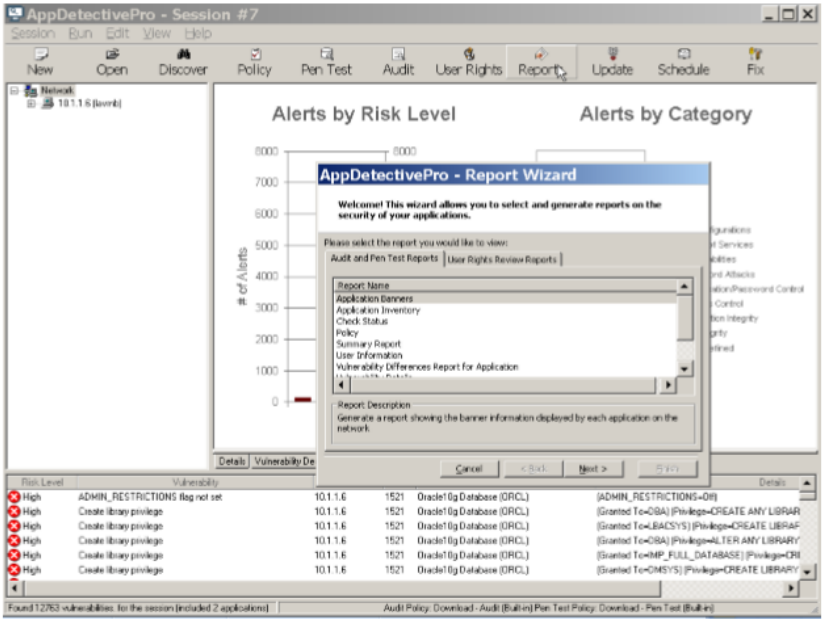


Рис. 5.50. Запуск утилиты формирования отчетов в AppDetectivePro

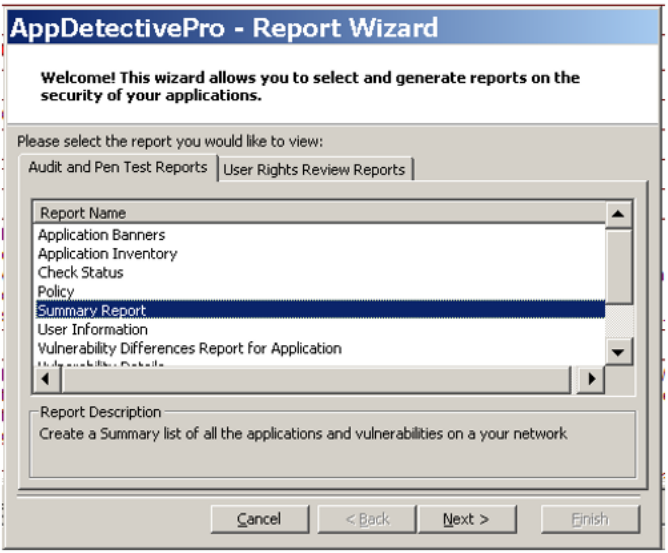


Рис. 5.51. Выбор варианта отчета

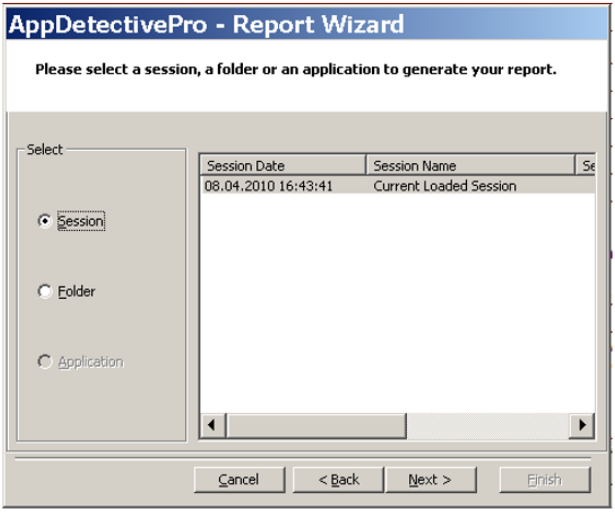


Рис. 5.52. Выбор типа отчета

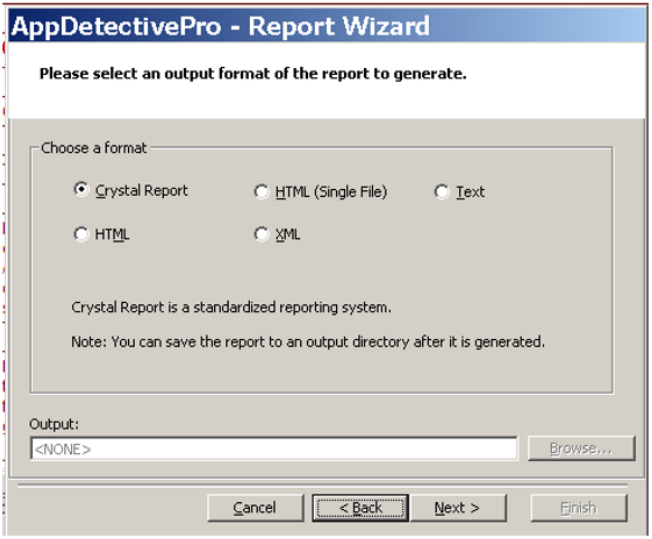


Рис. 5.53. Выбор формы отчета

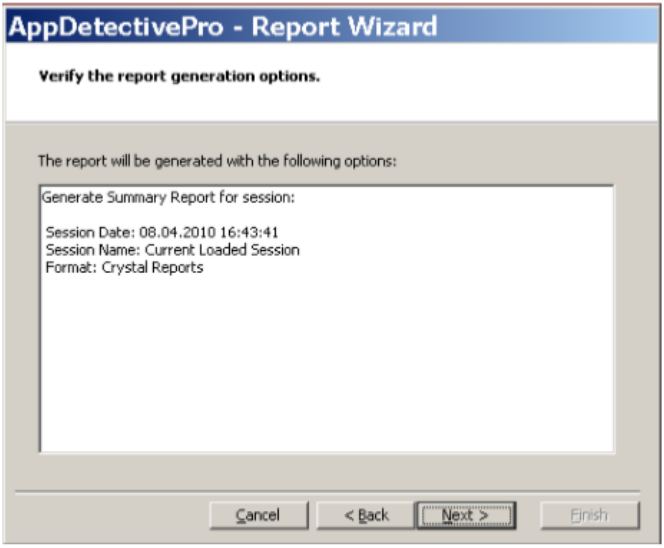


Рис. 5.54. Проверка параметров формируемого отчета перед его выполнением

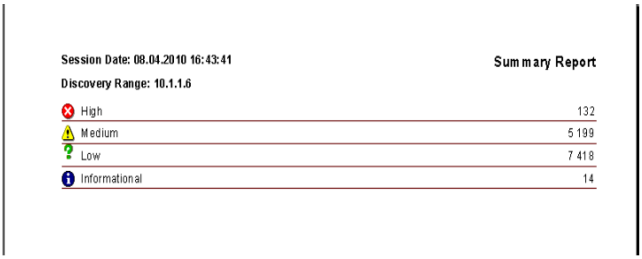


Рис. 5.55. Небольшой фрагмент итогового отчета с выявленными уязвимостями на основании выполнения Audit-а и PenTest-а

На рис 5.56, 5.57 показаны возможные варианты выбора отчета, формируемого по результатам выполнения утилиты «UserRights». В отличие от работы утилит «Audit» и «PenTest», результаты которых видны сразу же после выполнения, результаты работы утилиты «UserRights» можно увидеть только здесь, при формировании отчетов.

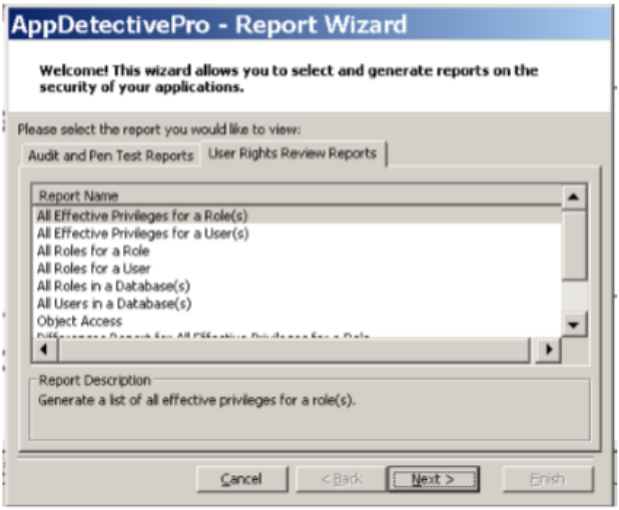


Рис. 5.56. Выбор варианта отчета по привилегиям пользователей в базе данных

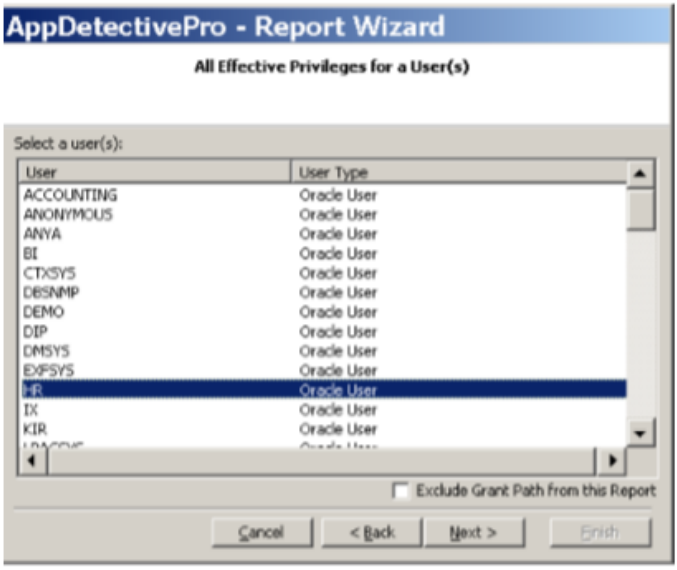


Рис. 5.57. Определение пользователя, отчет по которому на основании работы утилиты «UserRights» выдаст утилита «Report»

Сдача лабораторной работы

Сдача лабораторной работы заключается в следующем:

1. Демонстрация преподавателю на учебном стенде настроек сканера безопасности баз данных AppDetectivePro.

2. Демонстрация преподавателю отлавливания сканером безопасности AppDetectivePro специально введенных преподавателем уязвимостей пароля пользователей.

Примеры таких уязвимостей:

а) имя пользователя совпадает с его паролем

б) пароль пользователя представлен простым словом (‘world’, ‘welcome’, 'database', 'account', 'user', 'password', 'oracle', 'computer', 'abcd')

в) пароль пользователей SYS, SYSTEM не менялся после установки СУБД Oracle

3. Ответы на вопросы преподавателя по отчету, сформированному сканером безопасности AppDetectivePro при выявлении уязвимостей учебной базы данных.

Вопросы по лабораторной работе

1. Расскажите в чем заключается принцип работы сканеров безопасности баз данных? В чем их специфика работы?
2. В чем заключается настройка сканера безопасности на примере работы ПО AppDetectivePro.
3. В чем заключается принцип атаки по словарю при подборе пароля к учетной записи в базе данных?
4. Перечислите несколько методов, обеспечивающих повышение безопасности в базе данных.

СПИСОК СОКРАЩЁННЫХ ОБОЗНАЧЕНИЙ

АРМ – Автоматизированное рабочее место
АС – Автоматизированная система
БД – База данных
НСД – Несанкционированный доступ к информации
ОС – Операционная система
ПАК – Программно-аппаратный комплекс
ПО – Программное обеспечение
ПЭВМ – Персональная электронно-вычислительная машина
СВТ – Средство вычислительной техники
СУБД – Система управления базами данных
ЭВМ – Электронно-вычислительная машина
DNS – Domain Name System
HTML – HyperText Markup Language
IANA – Internet Assigned Numbers Authority
FTP – File Transfer Protocol
RTC – Real Time Clock

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Федеральный закон «Об информации, информационных технологиях и о защите информации». № 149-фз http://pravo.gov.ru/proxy/ips/?docbody&nd=102108264.
2. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г. – https://fstec.ru/component/attachments/download/298.
3. Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации. – М.: Стандартинформ, 2005. – 16 с.
4. Р 50.1.056-2005. Техническая защита информации. Основные термины и определения. – М.: Стандартинформ, 2006. – 20 с.
5. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – М.: Стандартинформ, 2008. – 12 с.
6. ГОСТ Р 53113.1-2008. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Ч. 1. – М.: Стандартинформ, 2008. – 12 с.
7. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. – М.: Стандартинформ, 2009. – 20 с.
8. ГОСТ Р 57429-2017. Судебная компьютерно-техническая экспертиза. Термины и определения. – М.: Стандартинформ, 2008. – 12 с.
9. ГОСТ Р 59853-2021. Информационные технологии. Комплекс стандартов на автоматизированные системы Автоматизирован-

ные системы. Термины и определения. М.: Российский институт стандартизации, 2021. – 16 с.
10. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. https://fstec.ru/component/attachments/download/297.
11. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. https://fstec.ru/component/attachments/download/296.
12. Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну. Утв. приказом ФСТЭК России от 29 апреля 2021 г. № 77. – https://fstec.ru/component/attachments/download/3075/.
13. Маркина Т.А. Средства защиты вычислительных систем и сетей. Уч. пособие. – СПб: Университет ИТМО, 2016. – 71 с.

Учебное издание

Бурлаков Михаил Евгеньевич,
Осипов Михаил Николаевич

КОНТРОЛЬ ЗАЩИЩЕННОСТИ ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА ЛАБОРАТОРНЫЙ ПРАКТИКУМ

Практикум

Публикуется в авторской редакции
Редакционно-издательская обработка Л. Р. Дмитриенко
Компьютерная верстка Л. Р. Дмитриенко

Подписано в печать 14.06.2022. Формат 60x84 1/16.
Бумага офсетная. Печ. л. 7,25.
Тираж 120 экз. (1-й з-д 1-25). Заказ № .

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САМАРСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА С.П. КОРОЛЕВА»
(САМАРСКИЙ УНИВЕРСИТЕТ)
443086, Самара, Московское шоссе, 34.

Издательство Самарского университета.
443086, Самара, Московское шоссе, 34.