ПРОФИЛЬ ЗАЩИТЫ

СИСТЕМА АНАЛИЗА ЗАЩИЩЕННОСТИ ПРОГРАММНОГО И АППАРАТНОГО ОБЕСПЕЧЕНИЯ TCP/IP СЕТЕЙ

(СЕТЕВОЙ СКАНЕР «РЕВИЗОР СЕТИ» ВЕРСИЯ 3.0)

Описание функциональных характеристик

Листов 7

Подп. и дата	
Инв. № дубл.	
Взам. инв. №	
Подп. и дата	
Инв. № подл.	

2018

Содержание

1. ОБЩИЕ СВЕДЕНИЯ

Система анализа защищенности программного и аппаратного обеспечения TCP/IP сетей (сетевой сканер «**Ревизор Сети»** версия 3.0) 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.

Система анализа защищенности программного и аппаратного обеспечения TCP/IP сетей (сетевой сканер «**Ревизор Сети»** версия 3.0) или **Ревизор Сети** представляет собой самостоятельное программное приложение, устанавливаемое на компьютеры, оснащенные процессорами семейства **INTEL X86** или совместимые с ними, и функционирующие под управлением операционных систем Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, Windows Server 2012 R2, Windows 10, Windows Server 2016.

При разработке сетевого сканера **Ревизор Сети** использовались среды программирования Borland Delphi 7.0, Embarcadero Delphi XE4, Microsoft Visual Studio2010.

2. ФУНКЦИОНАЛЬНОЕ НАЗНАЧЕНИЕ И ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

2.1. **Ревизор Сети** предназначен для обнаружения уязвимостей в сетевом программном и аппаратном обеспечении ЛВС, функционирующих с использованием протоколов стека TCP/IP.

2.2. **Ревизор Сети** позволяет проводить тестирование (выполнять заданные наборы 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 идентифицирующихся собственным IP-адресом.

2.3. **Ревизор Сети** имеет полностью русскоязычный интерфейс**.**

2.4. **Ревизор Сети** содержит в своем составе базу данных определений на языке OVAL для проверки уязвимостей и неустановленных обновлений программного обеспечения.

2.5. **Ревизор Сети** позволяет проводить обновление базы выполняемых проверок путем регистрации новых библиотек проверок, поставляемых разработчиками программного продукта.

2.6. Обновление базы выполняемых проверок проводится путем скачивания с WEB-сайта разработчика программного продукта.

2.7. 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.

2.8. Тестирование осуществляется путем создания плана проверок на основе доступных наборов проверок различных категорий, зарегистрированных в базе данных **Ревизора Сети**:

- план проверок строится для любой совокупности доступных узлов сети;
- в план проверок может включаться любая совокупность проверок.

2.9. **Ревизор сети** содержит следующий набор функциональных возможностей:

2.9.1 Ревизор Сети включает наборы проверок по следующим категориям:

2.9.1.1 определение доступности узлов проверяемой сети не менее чем пятью различными методами;

2.9.1.2 определение открытых TCP и UDP портов на узлах проверяемой сети;

2.9.1.3 верификация типа операционной системы, установленной на проверяемых узлах сети;

2.9.1.4 верификация сетевых сервисов;

2.9.1.5 определение NetBios-имен проверяемых узлов сети;

2.9.1.6 определение DNS-имен проверяемых узлов сети;

2.9.1.7 проверки учетных записей для узлов сети, функционирующих под управлением операционных систем семейства Windows;

2.9.1.8 проверки наличия и доступности общих сетевых ресурсов на проверяемых узлах сети;

2.9.1.9 сопоставление служб и сервисов, запущенных на узлах сети портам, назначенным и контролируемым организацией IANA;

2.9.1.10 проверки уязвимостей операционных систем семейства Windows с использованием обновляемой базы данных;

2.9.1.11 проверки неустановленных обновлений операционных систем семейства Windows с использованием обновляемой базы данных;

2.9.1.12 проверки неустановленных обновлений программного обеспечения операционных систем семейства UNIX;

2.9.1.13 проверки сервисов FTP;

2.9.1.14 сбор сведений и поиск уязвимостей устройств с использованием протокола SNMP;

2.9.1.15 проверки Web-сервисов;

2.9.1.16 проведение детального анализа структуры и контента WEB-сайта на предмет наличия разного рода уязвимостей;

2.9.1.17 проверки сервисов электронной почты;

2.9.1.18 проверки удаленного выполнения кода;

2.9.1.19 проверки удаленного получения прав администратора;

2.9.1.20 проверки паролей по умолчанию;

2.9.1.21 подбор паролей через SMB;

2.9.1.22 сбор дополнительной информации об ОС семейства Windows;

2.9.2 **Ревизор Сети** содержит базу данных по доступным проверкам. С наборами проверок возможны следующие действия:

2.9.2.1 регистрация наборов проверок в базе данных **Ревизора Сети** (регистрацию необходимо осуществить при первом запуске программы в соответствии с библиотеками проверок, поставляемыми в составе **Ревизора Сети);**

2.9.2.2 просмотр зарегистрированных проверок (осуществляется в интерфейсной части Ревизора Сети в виде раскрывающегося графического «дерева» проверок);

2.9.2.3 наборы проверок, зарегистрированные в базе данных **Ревизора**

Сети, могут быть удалены из базы данных.

2.9.3 **Ревизор Сети** позволяет осуществлять одновременное параллельное многопоточное тестирование узлов сети.

2.9.4 **Ревизор Сети** позволяет осуществлять параллельное выполнение взаимно независимых проверок в рамках каждого из узлов сети.

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

2.9.6 Тестирование осуществляется в рамках диапазона IP-адресов, заданного при создании новой сессии. Количество тестируемых IP-адресов ограничено количеством, указанным в лицензии при поставке программного продукта.

2.9.7 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.

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

2.9.9 Любая проверка, включенная в сформированный план, может быть удалена из плана до момента начала сканирования.

2.9.10 Любая проверка, отсутствующая в сформированном плане, может быть в него добавлена до момента начала сканирования.

2.9.11 При формировании плана проверок возможно отображение и редактирование входных параметров проверок. Значения входных параметров проверок по умолчанию заполняются автоматически.

2.9.12 **Ревизор Сети** позволяет в динамике отображать процесс выполнения плана проверок в части выполняющихся и закончивших выполнение проверок.

2.9.13 **Ревизор Сети** позволяет в любой момент времени в графическом виде визуализировать процессы обмена информацией между отдельными узлами сети.

2.9.14 **Ревизор Сети** позволяет в любой момент времени прервать выполнение плана проверок.

2.9.15 Результаты выполненных проверок для каждого из сеансов работы сохраняются в базе данных **Ревизора Сети** и в дальнейшем могут быть просмотрены в интерфейсной части сетевого сканера в виде

соответствующего дерева результатов.

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

2.9.17 **Ревизор Сети** позволяет осуществить формирование отчетов (в формате HTML) по результатам работы сетевого сканера. Отчеты формируются для любой совокупности IP-адресов.