МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«09» _____ 2021 г.

АНАЛИЗ ЗАЩИЩЕННОСТИ КОМПЬЮТЕРНОЙ СЕТИ С ПОМОЩЬЮ ПРОГРАММ GFI LANGUARD NETWORK SECCURITY SCANNER И XSPIDER

Методические указания по выполнению практических работ
для студентов направления подготовки (специальности)
09.03.02 Информационные системы и технологии

Курск 2021

УДК 004.56.5(076.5)
Составитель: А.Л. Ханис

Рецензент
Кандидат технических наук, доцент кафедры
информационной безопасности А.Л. Марухленко

Анализ защищенности компьютерной сети с помощью программ GFI LANguard Network Security Scanner и XSpider : методические указания по выполнению практических работ студентов всех форм обучения / Юго-Зап. гос. ун-т; сост.: А.Л. Ханис. - Курск, 2021. - 13 с.: ил. 9, Библиогр.: с. 13.

Содержат краткие теоретические положения о методике анализа защищенности операционной системы Windows и компьютерной сети с помощью программ GFI LANguard Network Security Scanner и XSpider.

Методические указания соответствуют требованиям программы по направлению подготовки бакалавров: математическое обеспечение и администрирование информационных систем.

Предназначены для студентов направления подготовки бакалавров 09.03.02.

Текст печатается в авторской редакции

Подписано в печать . Формат 60х84 1/16.
Усл.печ. л. 0,69 Уч.-изд. л. 0,63. Тираж 100 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Практическое занятие
Анализ защищенности компьютерной сети с помощью программ GFI LANguard Network Security Scanner и XSpider .

Введение

Системы анализа защищенности (security assessment systems), или сканеры безопасности (security scanners) – один из видов систем обнаружения атак. Это системы, которые позволяют обнаружить уязвимости информационных объектов до того, как атака будет проведена. Такие системы работают на первом этапе реализации атаки – этапе сбора информации. Системы анализа защищенности выполняют серию тестов по обнаружению уязвимостей. Эти тесты аналогичны применяемым злоумышленниками при осуществлении атак на корпоративные сети. Сканирование с целью обнаружения уязвимостей начинается с получения предварительной информации о проверяемой системе, в частности о разрешенных протоколах и открытых портах, используемой версии операционной системе. Заканчивается сканирование попытками имитации проникновения, используя широко известные атаки, например подбор пароля методом полного перебора. При помощи средств анализа защищенности сетевых протоколов и сервисов можно тестировать не только возможность несанкционированного доступа в корпоративную сеть из сети Интернет. Системы анализа защищенности на уровне сети могут быть использованы как для оценки уровня безопасности организации, так и для контроля эффективности настройки сетевого программного и аппаратного обеспечения.

Средства анализа защищенности операционной системы предназначены для проверки настроек операционной системы, влияющих на ее защищенность. К таким настройкам можно отнести:

- учетные записи пользователей (account), например длину пароля и срок его действия;
- права пользователей на доступ к критичным системным файлам;
- уязвимые системные файлы;
- установленные патчи.

Системы анализа защищенности на уровне ОС могут быть использованы также для контроля конфигурации операционных систем. Кроме возможностей по обнаружению уязвимостей, некоторые системы анализа защищенности на уровне ОС (например System Scanner) позволяет автоматически устранять часть обнаруженных проблем или корректировать параметры системы, не удовлетворяющие политике безопасности, принятой в организации.

Краткие теоретические положения. Система анализа защищенности LANguard

LANguardNetwork Security Scanner – система анализа защищенности операционной системы Windows. Это сетевая система, и она может проверять защищенность любого узла сети по указанному IP-адресу. Однако функций проверки защищенности сети в целом LANguard не имеет.

При запуске программы откроется окно со следующей панелью инструментов:

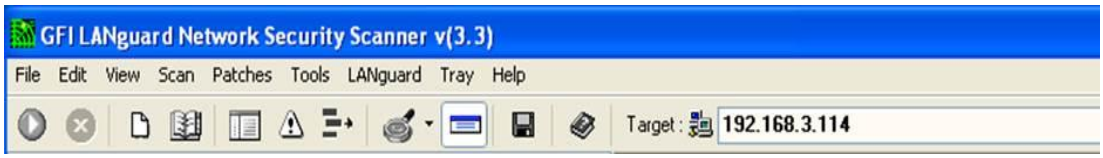

Рис. 1. Панель инструментов

В поле Target по умолчанию программа выводит IP-адрес компьютера, на котором она запущена. Сканирование уязвимостей будет проведено на компьютере с указанным IP-адресом. Объем выполненных запросов будет определяться правами пользователя, запустившего программу. Для пользователя с правами администратора будет выполнен весь возможный перечень запросов, для других пользователей этот список будет ограничен. При сканировании других компьютеров вы выступаете в качестве пользователя с ограниченными правами.

Настройка диапазона сканирования

Чтобы настроить диапазон сканирования, выберите команду меню File/New scan. Откроется окно настройки диапазона

сканирования. Можно указать следующие варианты:

· Сканирование конкретного IP-адреса
· Сканирование диапазона IP-адресов
· Сканирование списка IP-адресов
· Сканирование части домена

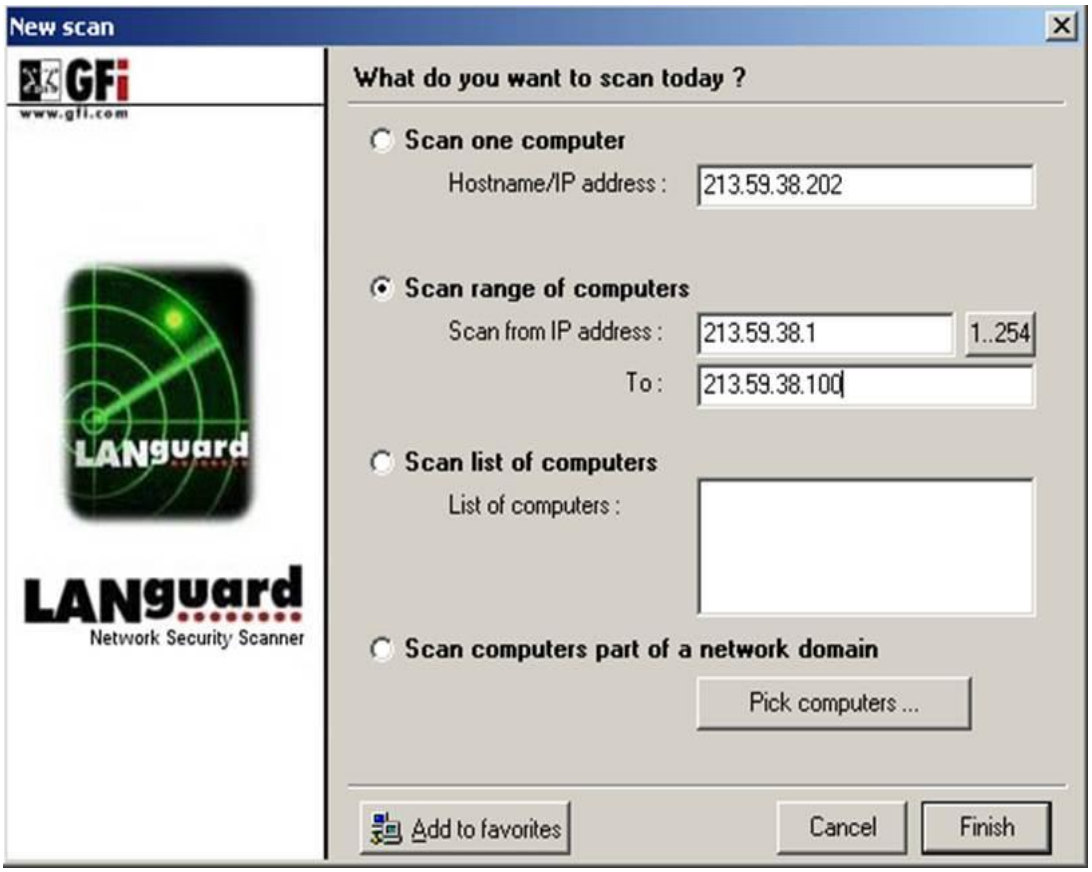

Рис. 2. Окно настройки диапазона сканирования.

Запуск процесса сканирования

Для запуска процедуры сканирования уязвимостей нужно нажать кнопку . После завершения сканирования в правом окне (где выводится протокол) будет выведено: Ready. До этого момента идет процесс сканирования.

Анализ результатов сканирования

По окончании сканирования его результаты будут выведены в нижней части окна программы в двух панелях (левой и правой). Окно будет выглядеть примерно так:

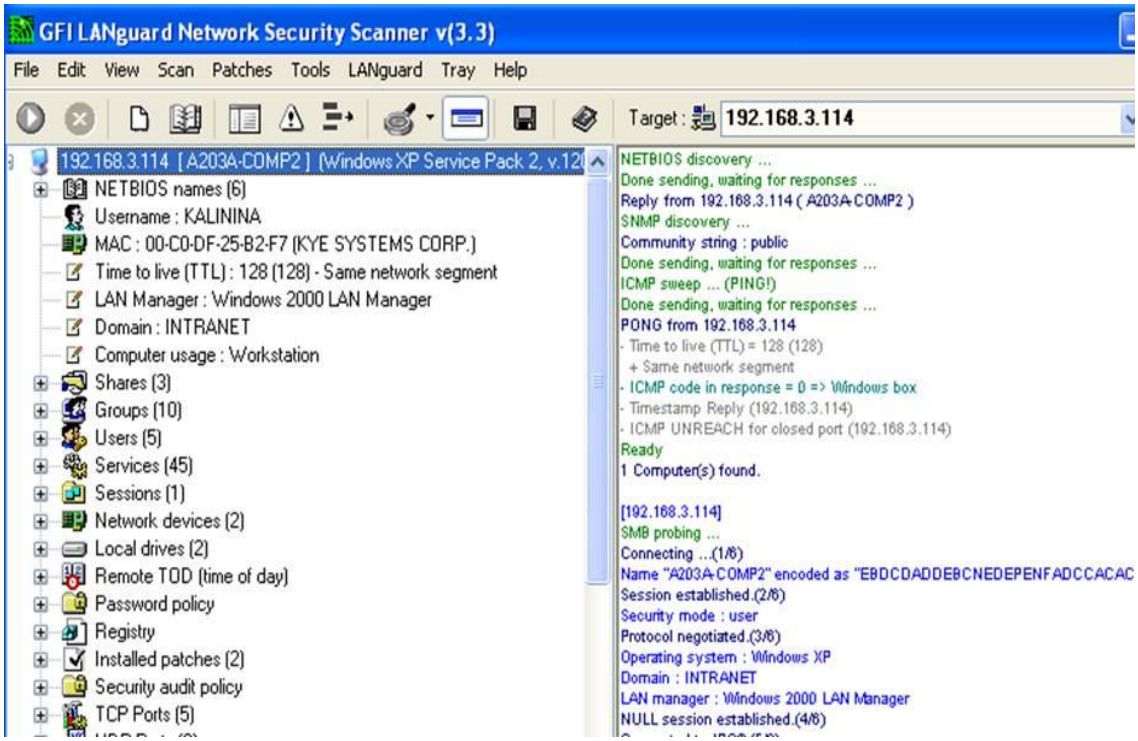

Рис. 3. Результаты сканирования.

В левой панели выводится результат сканирования (отчет), в правой панели – протокол выполненных для этого действий. Если пункт отчета по результатам сканирования помечен знаком “+”, то он содержит вложенный список, который можно раскрыть щелчком мыши.

Отчет по результатам сканирования содержит следующие разделы (указаны не все из имеющихся):

- NETBIOS names – список NETBIOS имен компьютеров и сетевых служб, обнаруженных в данном сегменте локальной сети;

-Shares – список общих сетевых ресурсов;

-Groups – список зарегистрированных групп пользователей;

-Users – список зарегистрированных пользователей;

-Services – список работающих в ОС сервисов;

-Password policy – установленная политика паролей;

-Security audit policy – установленная политика аудита событий безорасности;

-TCP ports – список открытых портов протокола TCP;

-UDP ports – список открытых портов протокола UDP;

-Alerts – список предупреждений о найденных уязвимостях.

В списке открытых портов могут быть зеленые и красные значки. Если программа определяет открытый порт как порт

известного «троянского коня», он отмечается красным цветом, в остальных случаях – зеленым.

Самая важная часть отчета – Alerts. Это список предупреждений о найденных уязвимостях. Каждое предупреждение содержит комментарий и рекомендацию по устранению данной уязвимости. Ее можно увидеть, щелкнув мышью на знаке “+” возле выбранного предупреждения.

Практическое задание №1.

1) Выполнить сканирование уязвимостей своего компьютера сканером LANguard.

2) Сделать анализ каждого выданного предупреждения и предложить средство устранения данной уязвимости. Сделать вывод о серьезности каждой обнаруженной уязвимости для безопасности системы и о состоянии защищенности системы в целом.

3) Настроить вид файла отчета и сохранить результаты сканирования в файле.

4) Сделать отчет по лабораторной работе, который должен содержать анализ каждого выданного предупреждения и предложенные меры по устранению данной уязвимости.

Система анализа защищенности XSpider 7.0

Ключевым для системы XSpider 7.0 является понятие задачи. Любые действия по сканированию уязвимостей всегда происходят в рамках определенной задачи (даже если вы для этого ничего не делали). Пустая задача всегда создается при первоначальном запуске XSpider 7.0. Понятие «задача» включает в себя элементы:

· список проверяемых хостов;
· набор настроек для сканирования (так называемый профиль);
· историю прошлых сканирований (отображается на закладке **История сканирований**).

XSpider 7.0 может сканировать одновременно несколько хостов. Добавление хоста для сканирования происходит по команде меню Правка/ Добавить хост. В открывшемся окне необходимо ввести IP-адрес или доменное имя хоста.

Использование профилей

Профиль задачи – это набор параметров для сканирования уязвимостей. Профили хранятся в файлах с расширением .prf. Когда вы запускаете XSpider 7.0, создается новая задача с профилем по умолчанию Default.prf. Система имеет набор стандартных профилей. Выбор профиля для применения к текущей задаче происходит в пункте меню Профиль/ Применить существующий. Редактировать стандартные профили (кроме некоторых параметров) невозможно, однако есть возможность создавать собственные профили с индивидуальными настройками.

Запуск процесса сканирования

Процесс сканирования запускается командой Сканирование/Старт. Протокол сканирования выводится на закладке «Сканирование». Протокол имеет следующий вид:

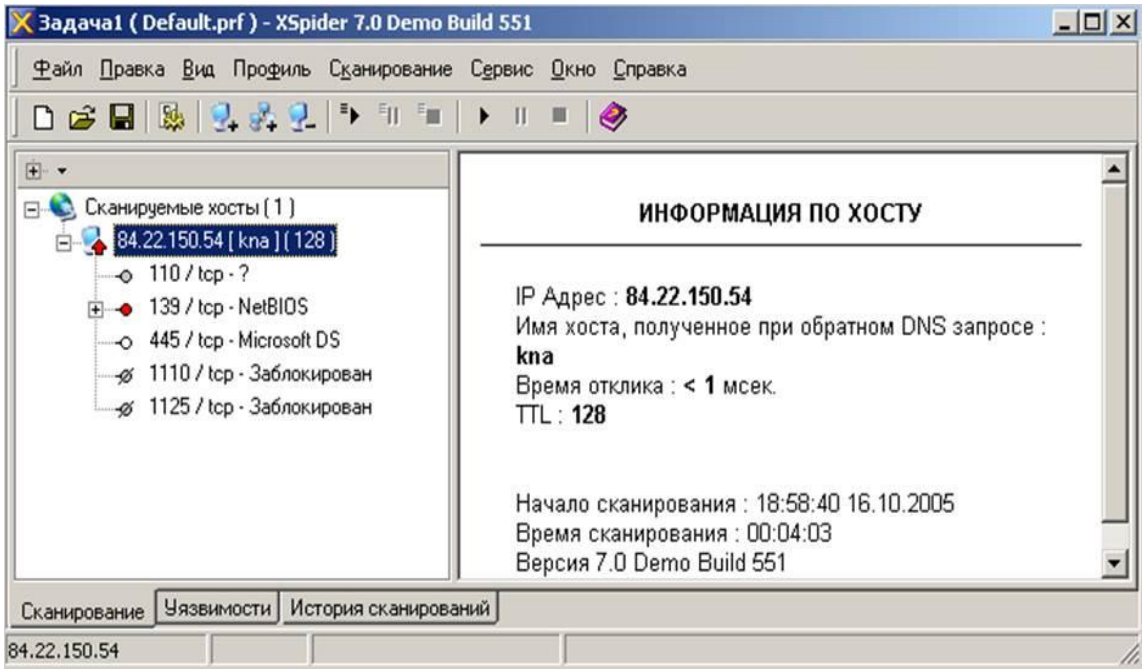

Рис. 4. Протокол сканирования.

На закладке «Уязвимости» выводится перечень найденных уязвимостей следующего вида:

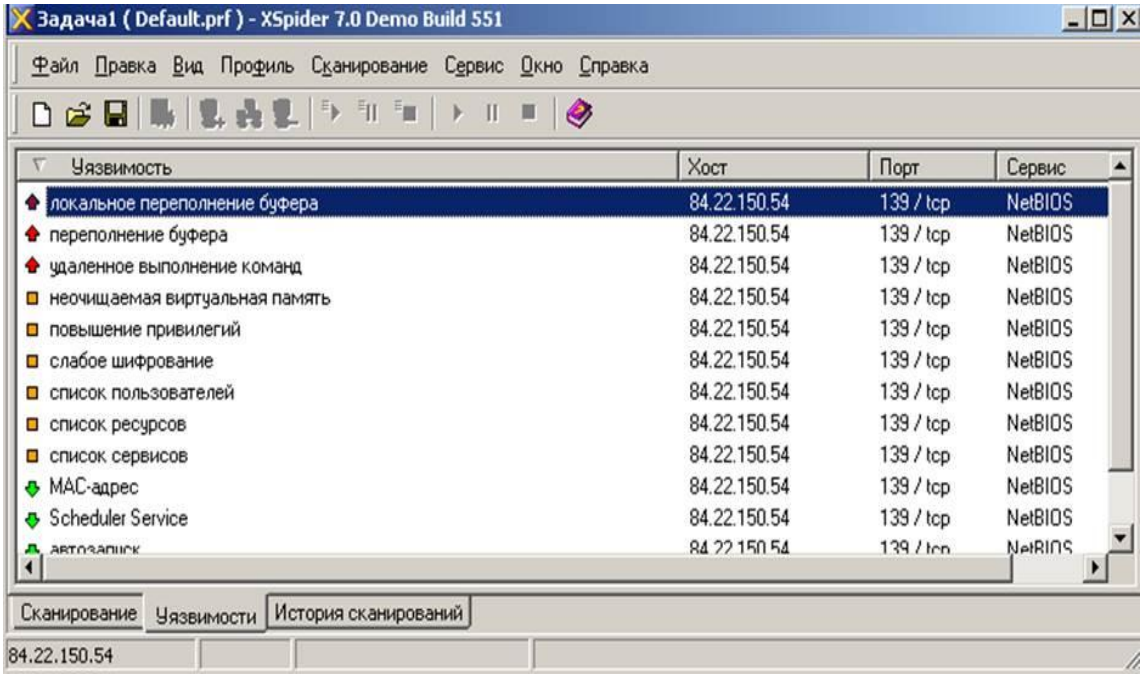

Рис. 5. Список уязвимостей.

При этом используются следующие обозначения:

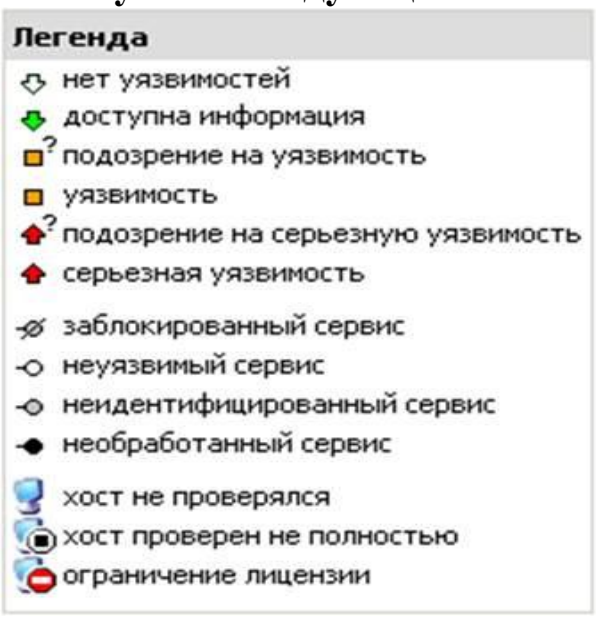

Рис. 6. Обозначения уязвимостей

Создание отчета

Создание отчета выполняется по команде меню Сервис/ Создать отчет. Открывается окно выбора варианта отчета:

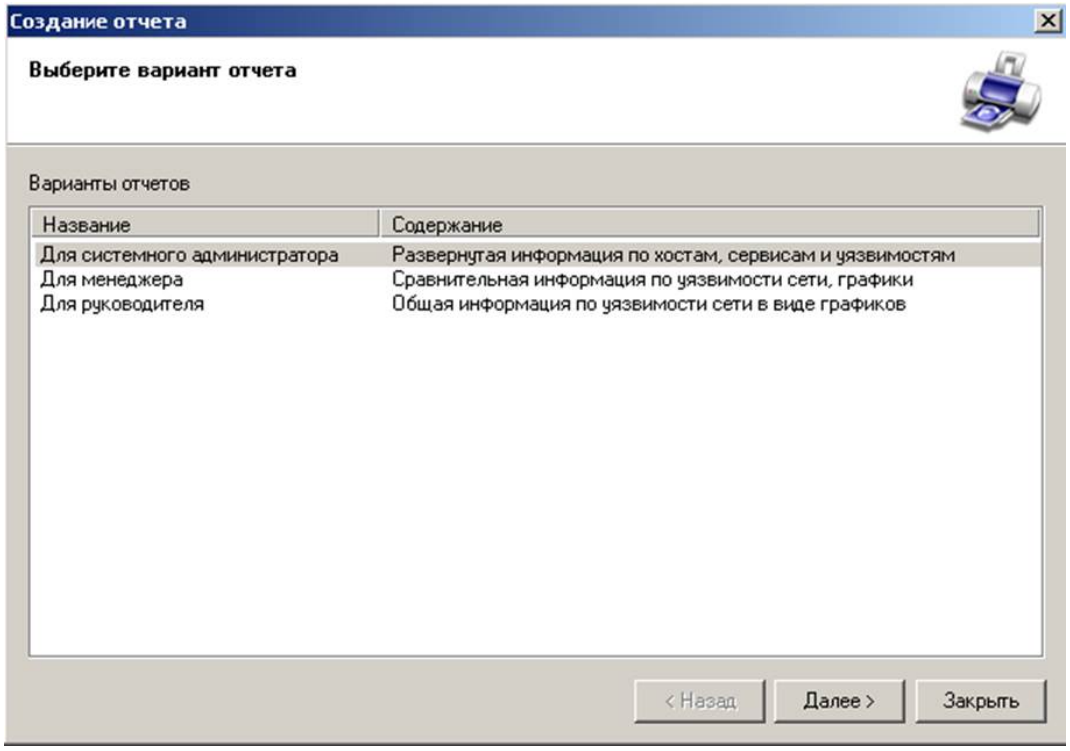

Рис. 7. Окно выбора варианта отчета.

В следующем окне нужно указать, для каких хостов создаем отчет (в случае, если сканировалось несколько хостов):

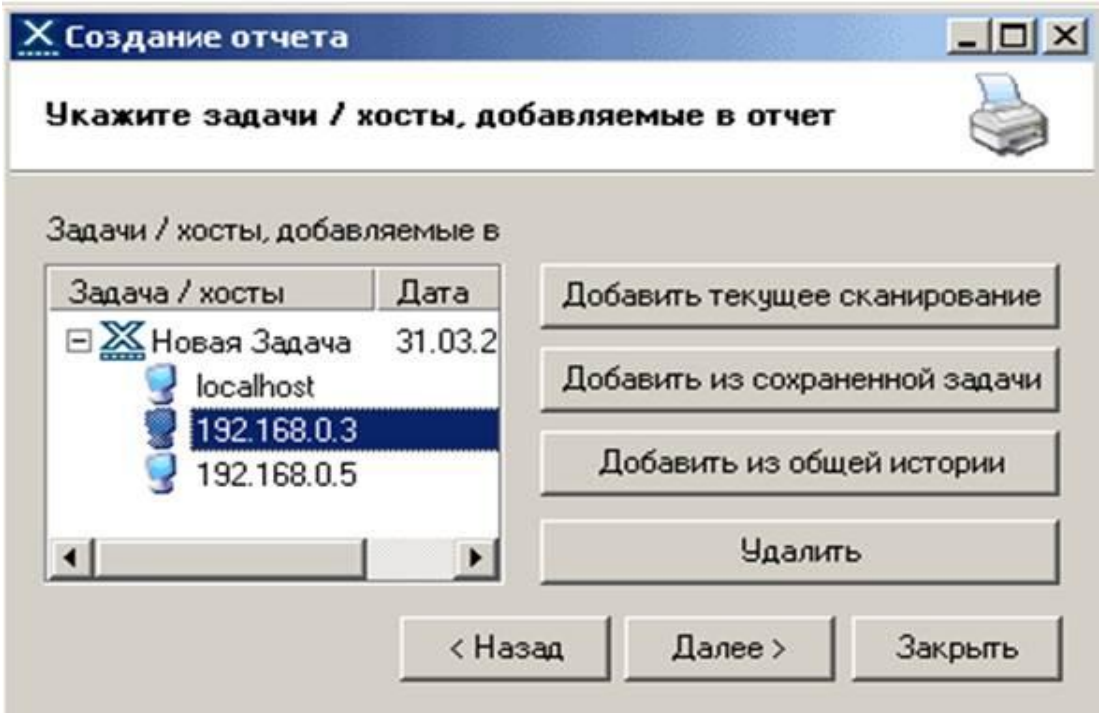

Рис. 8. Окно выбора хостов.

В заключительном окне диалога создания отчета нужно выбрать вид действия (просмотр, печать или сохранение отчета):

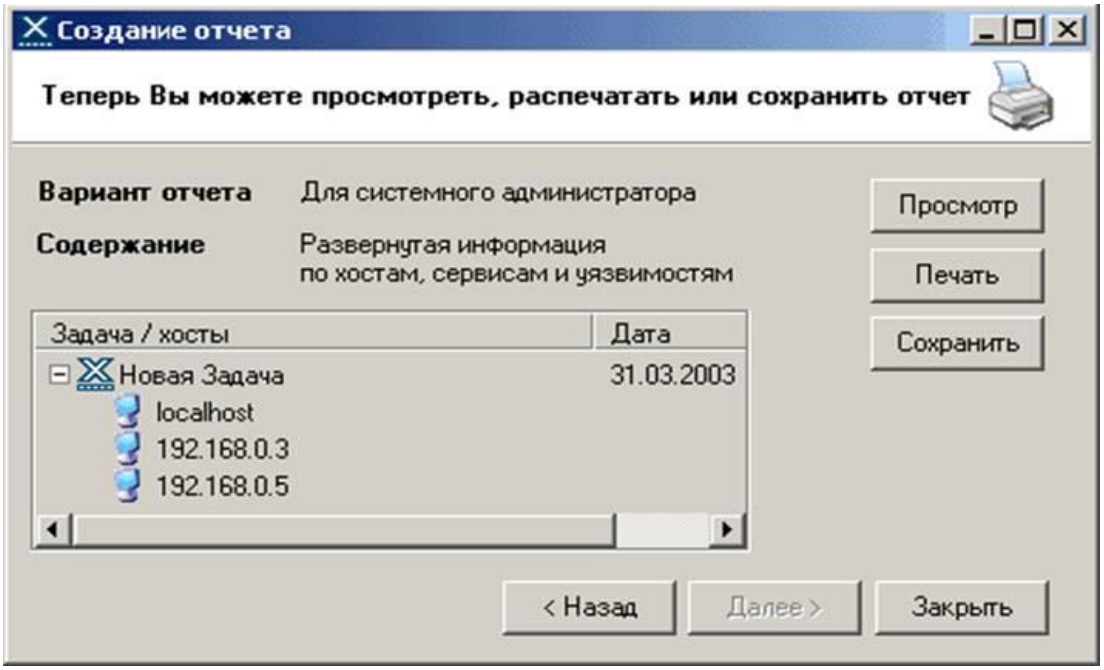

Рис. 9. Окно выбора хостов.

Практическое задание №2

1) Выполнить сканирование уязвимостей своего компьютера сканером XSpider, применив профиль DefaultOff.prf.

2) Создать отчет для системного администратора и сохранить его в виде файла. Сохранить текущую задачу.

3) Создать новый профиль на базе DefaultOff.prf, дополнительно отключив опцию проверки на известные DoS-атаки.

4) Выполнить сканирование созданным профилем.

5) Создать отчет для системного администратора и сохранить его в виде файла.

6) Проанализировать оба отчета об уязвимостях и сделать рекомендации по защите хоста.

Список контрольных вопросов

1) В чем состоит концепция адаптивного управления безопасностью? Перечислите основные компоненты модели адаптивной безопасности.

2) Каков общий принцип работы средств анализа защищенности сетевых протоколов и сервисов?

3) Каков общий принцип работы средств анализа защищенности операционной системы?

4) Перечислите основные требования к выбираемым средствам анализа защищенности.

5) Дайте общий обзор современных средств анализа защищенности.

6) Каковы методы анализа сетевой информации, используемые в средствах обнаружения сетевых атак?

7) Какова классификация систем обнаружения атак?

8) Перечислите основные компоненты системы обнаружения атак.

9) Каковы положительные и отрицательные стороны систем обнаружения атак на сетевом и операционном уровнях?

10) Дайте общий обзор современных средств обнаружения сетевых атак.

Список литературы

1. Тихонов В. А. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты [текст]: учебное пособие / В. А. Тихонов, В. В. Райх. – М.: Гелиос АРВ, 2006. - 528 с.

2. Игнатьев В. А. Защита информации в корпоративных информационно-вычислительных сетях [Текст]: монография.- Старый Оскол: ТНТ, 2005. – 552 с.

3. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В. Ф. – М. : ДМК Пресс, 2010.-544 с.