МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Курганский государственный университет»

Кафедра «Безопасность информационных и автоматизированных систем»

АКТИВНЫЙ АУДИТ

Методические указания
по выполнению лабораторной работы по дисциплине «Аудит информационной безопасности» для студентов
направлений 10.05.03 и 10.03.01

Курган 2018

Кафедра: «Безопасность информационных и автоматизированных систем».
Дисциплина: «Аудит информационной безопасности».
Составил: ст. преподаватель В.В. Москвин.

Утверждены на заседании кафедры « 24 » ноября 2017 г.

Рекомендованы методическим советом университета « 12 » декабря 2016 г.

Активный аудит

Цель работы: научиться использовать специальные программные средства активного аудита. Провести анализ защищенности тестовой системы, выявить уязвимости.

Приборы и принадлежности

1 Oracle VM VirtualBox.
2 Windows Server 2003 R2/2008 R2 Standard.
3 3 хоста с ОС Windows XP.
4 3 хоста с ОС Ubuntu 14.04.3-desktop.
5 Microsoft Baseline Security Analyzer v. 2.3.
6 Nmap (zmap или другой форк).
7 Hostmonitor 9.90 (IP-tools 2.58).
8 Сканер-ВС.
9 Audit pro.
10 Shadow Security Scanner.
11 XSpider.

Теоретическое введение

При анализе конфигурации средств защиты и управления межсетевыми взаимодействиями особое внимание обращается на следующие аспекты, определяемые их конфигурацией:

− настройка правил разграничения доступа (правил фильтрации сетевых пакетов) на межсетевых экранах (МЭ) и маршрутизаторах;

− используемые схемы и настройка параметров аутентификации;

− настройка параметров системы регистрации событий;

− использование механизмов, обеспечивающих сокрытие топологии защищаемой сети, включающих в себя трансляцию сетевых адресов (NAT);

− настройка механизмов оповещения об атаках и реагирования;

− наличие и работоспособность средств контроля целостности.

Тестирование системы защиты информационной системы (ИС) проводится с целью проверки эффективности используемых в ней механизмов защиты, их устойчивости в отношении возможных атак, а также с целью поиска уязвимостей в защите. Традиционно используются два основных метода тестирования:

- тестирование по методу «черного ящика»;
- тестирование по методу «белого ящика».

Тестирование по методу «черного ящика» предполагает отсутствие у тестирующей стороны каких-либо специальных знаний о конфигурации и внутренней структуре объекта испытаний. При этом против объекта испытаний реализуются все известные типы атак, и проверяется устойчивость системы защиты в отношении этих атак. Используемые методы тестирования эмулируют действия потенциальных злоумышленников, пытающихся взломать

систему защиты. Основным средством тестирования в данном случае являются сетевые сканеры, располагающие базами данных известных уязвимостей.

Метод «белого ящика» предполагает составление программы тестирования на основании знаний о структуре и конфигурации объекта испытаний. В ходе тестирования проверяются наличие и работоспособность механизмов безопасности, соответствие состава и конфигурации системы защиты требованиям безопасности и существующим рискам. Выводы о наличие уязвимостей делаются на основании анализа конфигурации используемых средств защиты и системного ПО, а затем проверяются на практике. Основным инструментом анализа в данном случае являются программные агенты средств аудита безопасности системного уровня, рассматриваемые ниже.

В настоящее время имеется большое разнообразие как методов анализа безопасности ИС, так и реализующих их программных средств. Приведем примеры некоторых, наиболее распространенных:

- Net Recon;
- XSpider;
- ... .

Арсенал программных средств, используемых для аудита безопасности ИС достаточно широк. Причем во многих случаях свободно распространяемые программные продукты ничем не уступают коммерческим. Достаточно сравнить некоммерческий сканер XSpider с его коммерческими аналогами.

Одним из методов автоматизации процессов анализа и контроля безопасности распределенных компьютерных систем является использование технологии интеллектуальных программных агентов. Система защиты строится на архитектуре консоль/менеджер/агент. На каждую из контролируемых систем устанавливается программный агент, который и выполняет соответствующие настройки ПО и проверяет их правильность, контролирует целостность файлов, своевременность установки пакетов программных коррекций, а также выполняет другие полезные задачи по контролю безопасности ИС. Управление агентами осуществляется по сети программой-менеджером. Менеджеры являются центральными компонентами подобных систем. Они посылают управляющие команды всем агентам контролируемого ими домена и сохраняют все данные, полученные от агентов в центральной базе данных. Администратор управляет менеджерами при помощи графической консоли, позволяющей выбирать, настраивать и создавать политики безопасности, анализировать изменения состояния системы, осуществлять ранжирование уязвимостей и т. п. Все взаимодействия между агентами, менеджерами и управляющей консолью осуществляются по защищенному клиент-серверному протоколу. Такой подход был использован при построении комплексной системы управления безопасностью организации Symantec Enterprise Security Manager (ESM).

Другим широко используемым методом аудита безопасности является активное тестирование механизмов защиты путем эмуляции действии злоумышленника по осуществлению попыток сетевого вторжения в ИС. Для

этих целей применяются сетевые сканеры, эмулирующие действия потенциальных нарушителей. В основе работы сетевых сканеров лежит база данных, содержащая описание известных уязвимостей ОС, МЭ, маршрутизаторов и сетевых сервисов, а также алгоритмов осуществления попыток вторжения (сценариев атак). Рассматриваемые ниже сетевые сканеры XSpider и Symantec NetRecon являются достойными представителями данного класса программных средств аудита безопасности. Таким образом, программные средства аудита безопасности условно можно разделить на два класса. Первый класс, к которому принадлежат сетевые сканеры, иногда называют средствами аудита безопасности сетевого уровня. Второй класс, к которому относятся все остальные рассмотренные здесь средства, иногда называют средствами аудита безопасности системного уровня. Данные классы средств имеют свои достоинства и недостатки, а на практике взаимно дополняют друг друга.

Для функционирования сетевого сканера необходим только один компьютер, имеющий сетевой доступ к анализируемым системам, поэтому в отличие от продуктов, построенных на технологии программных агентов, нет необходимости устанавливать в каждой анализируемой системе своего агента (своего для каждой ОС).

К недостаткам сетевых сканеров можно отнести большие временные затраты, необходимые для сканирования всех сетевых компьютеров из одной системы, и создание большой нагрузки на сеть. Кроме того, в общем случае трудно отличить сеанс сканирования от действительных попыток осуществления атак. Сетевыми сканерами также с успехом пользуются злоумышленники.

Системы аудита безопасности, построенные на интеллектуальных программных агентах, являются потенциально более мощным средством, чем сетевые сканеры. Однако, несмотря на все свои достоинства, использование программных агентов не может заменить сетевого сканирования, поэтому эти средства лучше применять совместно. Кроме того, сканеры являются более простым, доступным, дешевым и, во многих случаях, более эффективным средством аудита безопасности.

Сетевые сканеры. Основным фактором, определяющим защищенность информационных систем от угроз безопасности, является наличие в ИС уязвимостей защиты. Уязвимости защиты могут быть обусловлены как ошибками в конфигурации компонентов ИС, так и другими причинами, в число которых входят ошибки и программные закладки в коде ПО, отсутствие механизмов безопасности, их неправильное использование, либо их неадекватность существующим рискам, а также уязвимости, обусловленные человеческим фактором. Наличие уязвимостей в системе защиты ИС, в конечном счете, приводит к успешному осуществлению атак, использующих эти уязвимости.

Сетевые сканеры являются, пожалуй, наиболее доступными и широко используемыми средствами анализа защищенности. Основной принцип их

функционирования заключается в эмуляции действий потенциального злоумышленника по осуществлению сетевых атак. Поиск уязвимостей путем имитации возможных атак является одним из наиболее эффективных способов анализа защищенности ИС, который дополняет результаты анализа конфигурации по шаблонам, выполняемый локально с использованием шаблонов (списков проверки). Сканер является необходимым инструментом в арсенале любого администратора либо аудитора безопасности ИС.

Современные сканеры способны обнаруживать сотни уязвимостей сетевых ресурсов, предоставляющих те или иные виды сетевых сервисов. Их предшественниками считаются сканеры телефонных номеров (war dialers), использовавшиеся с начала 80-х и не потерявшие актуальности по сей день. Первые сетевые сканеры представляли собой простейшие сценарии на языке Shell, сканировавшие различные TCP-порты. Сегодня они превратились в зрелые программные продукты, реализующие множество различных сценариев сканирования.

Современный сетевой сканер выполняет четыре основные задачи:

- идентификацию доступных сетевых ресурсов;
- идентификацию доступных сетевых сервисов;
- идентификацию имеющихся уязвимостей сетевых сервисов;
- выдачу рекомендаций по устранению уязвимостей.

В функциональность сетевого сканера не входит выдача рекомендаций по использованию найденных уязвимостей для реализации атак на сетевые ресурсы. Возможности сканера по анализу уязвимостей ограничены той информацией, которую могут предоставить ему доступные сетевые сервисы.

Принцип работы сканера заключается в моделировании действий злоумышленника, производящего анализ сети при помощи стандартных сетевых утилит, таких как host, showmount, traceout, rusers, finger, ping и т. п. При этом используются известные уязвимости сетевых сервисов, сетевых протоколов и ОС для осуществления удаленных атак на системные ресурсы и осуществляется документирование удачных попыток.

В настоящее время существует большое количество как коммерческих, так и свободно распространяемых сканеров, как универсальных, так и специализированных; предназначенных для выявления только определенного класса уязвимостей. Многие из них можно найти в сети Интернет. Число уязвимостей в базах данных современных сканеров медленно, но уверенно приближается к 1000.

Одним из наиболее продвинутых коммерческих продуктов этого класса является сетевой сканер NetRecon компании Symantec, база данных которого содержит около 800 уязвимостей UNIX, Windows и NetWare систем и постоянно обновляется через Web. Рассмотрение его свойств позволит составить представление обо всех продуктах этого класса.

Сетевой сканер NetRecon (рисунок 1) является инструментом администратора безопасности, предназначенным для исследования структуры сетей и сетевых сервисов и анализа защищенности сетевых сред. NetRecon

позволяет осуществлять поиск уязвимостей в сетевых сервисах, ОС, МЭ, маршрутизаторах и других сетевых компонентах. Например, NetRecon позволяет находить уязвимости (рисунок 2) в таких сетевых сервисах, как ftp, telnet, DNS, электронная почта, Web-сервер и др. При этом проверяются версии и конфигурации сервисов, их защищенность от сетевых угроз и устойчивость к попыткам проникновения. Для поиска уязвимостей используются как стандартные средства тестирования и сбора информации о конфигурации и функционировании сети, так и специальные средства, которые реализуют алгоритмы, эмулирующие действия злоумышленника по осуществлению сетевых атак.

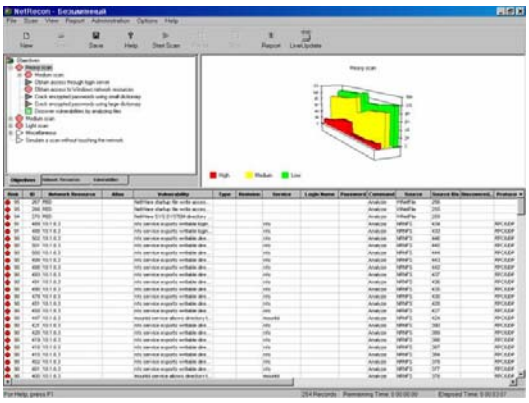

Рисунок 1 – Сетевой сканер NetRecon

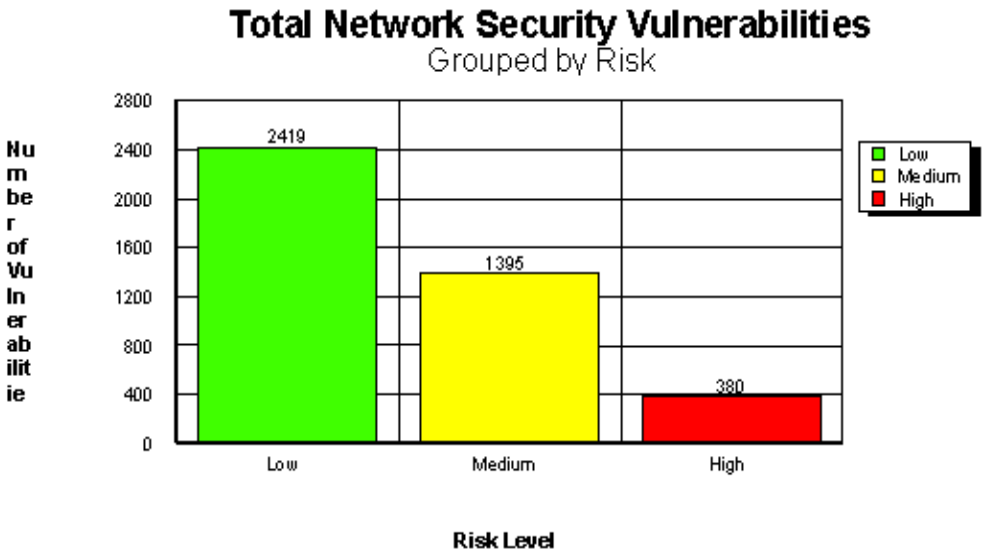

Рисунок 2 – Суммарное количество уязвимостей, обнаруженных сканером NetRecon

Программа работает в среде ОС Windows NT и имеет удобный графический интерфейс, позволяющий определять параметры сканирования, наблюдать за ходом сканирования, генерировать и просматривать отчеты о результатах сканирования. Результаты отображаются в графической и в табличной форме в реальном масштабе времени.

Создаваемые NetRecon отчеты содержат подробную информацию о найденных уязвимостях, включая слабость паролей пользователей,

подверженность определенных сервисов угрозам отказа в обслуживании, уязвимые для сетевых атак конфигурации ОС и многие другие. Наряду с сообщениями о найденных уязвимостях и их описаниями, приводятся рекомендации по их устранению. Отчет о результатах сканирования позволяет наметить план мероприятий по устранению выявленных недостатков.

Для генерации отчетов в NetRecon используется ПО Crystal Report, предоставляющее удобные средства для просмотра отчетов и их экспорта во все популярные форматы представления данных. Найденные уязвимости ранжируются, при этом каждой из них присваивается числовой рейтинг, что позволяет отсортировать их по степени критичности для облегчения последующего анализа результатов сканирования.

Пример описания уязвимости в отчете, сгенерированном сканером NetRecon, приведен на рисунке 3. В NetRecon используется следующий формат описания уязвимости (который, однако, является общим и для всех остальных сетевых сканеров):

- Vulnerability Name (Название уязвимости);
- Risk (Уровень риска);
- Description (Описание уязвимости);
- Solution (Способы ликвидации уязвимости);
- Additional Information (Дополнительная информация);
- Links (Ссылки на источники информации о данной уязвимости);
- of Network Resources (Кол-во сетевых ресурсов, подверженных данной уязвимости);
- Network Resources (Список сетевых ресурсов).

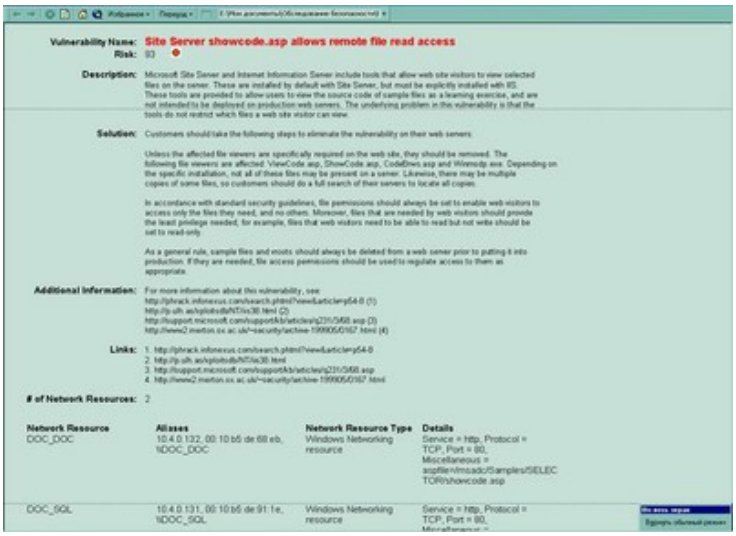

Рисунок 3 − Описание уязвимости в отчете, сгенерированном сканером NetRecon

NetRecon самостоятельно определяет конфигурацию сети и позволяет выбрать сетевые ресурсы для сканирования. Может осуществляться параллельное сканирование всех сетевых ресурсов, сканирование по диапазону сетевых адресов, сканирование отдельных систем или подсетей. Сеанс

сканирования может включать в себя все виды проверок либо отдельные проверки по выбору пользователя. Глубина сканирования определяется продолжительностью сеанса сканирования, которая задается пользователем. Например, проверки, связанные с подбором пользовательских паролей по словарю, сопряжены с существенными временными затратами и не могут быть завершены в течение короткого сеанса сканирования.

Для поиска сетевых уязвимостей в NetRecon используется запатентованная технология UltraScan. Производимые NetRecon проверки тесно взаимосвязаны и результаты одной проверки используются для выполнения другой. Как и в случае реальных атак, в технологии UltraScan информация об обнаруженных уязвимостях используется для выявления других связанных с ними уязвимостей. Например, если NetRecon удалось получить доступ к файлу, содержащему пароли пользователей, и расшифровать несколько паролей, то эти пароли будут использованы для имитации атак на другие системы, входящие в состав сети.

NetRecon дает возможность пользователю отслеживать путь поиска уязвимости, представляющий собой последовательность проверок производимых NetRecon, которая привела к выявлению данной уязвимости. Путь поиска уязвимости позволяет проследить действия возможного нарушителя, осуществляющего атаку на сетевые ресурсы.

Используемая NetRecon база данных содержит описание известных уязвимостей и сценариев атак. Она регулярно пополняется новыми данными. Обновление этой базы данных производится через Web-узел компании Symantec автоматически, при помощи механизма LiveUpdate.

Сетевой сканер XSPIDER — первый российский сканер безопасности.

XSpider — программное средство сетевого аудита, предназначенное для удаленной диагностики различных элементов сети на предмет поиска уязвимостей. На текущий момент, XSpider по возможностям не уступает, а местами и превосходит известные сканеры безопасности, такие как ISS Internet Scanner, Nessus, Retina. (Сравнительные таблицы 1, 2, 3, 4, 5, 6 − http://www.bytemag.ru/articles/detail.php?ID=8773&phrase_id=451).

Таблица 1 − Характеристики сравниваемых сетевых сканеров

Оцениваемый фактор	Ревизор сети	XSpider	Retina	NeWT	IS
Поддержка CVE (MITRE)	-	-	+	+	+
Примерные требования к объему дискового пространства, Мбайт	50	10	30	45	300
Механизм обновлений	Удаленный сервер	Удаленный/ локальный сервер	Удаленный сервер	Удаленный сервер	Удаленный сервер
Ориентировочная стоимость лицензии на 100 IP-адресов, у.е.	4000	1200	4080	Бесплатно для сетей класса С; 1200 − полная лицензия	11319

Таблица 2 – Результаты сканирования портов (в баллах)

	Windows 2000 Professional SP3	MCBC 3.0	Windows Server 2003	Общий балл
TCP-сканирование				
Ревизор сети	+1	+18	+7	+26
XSpider	+3	+12	+17	+32
Retina	+3	+22	+5	+30
NeWT	+1	+10	+17	+28
IS	-5	-28	-5	-38
UDP-сканирование				
Ревизор сети	0	Ошибка	-6	-
XSpider	-5	-14	-16	- 35
Retina	-6	-16	-20	- 42
NeWT	-6	-16	-16	- 38
IS	+4	Ошибка	-20	-

Таблица 3 – Результаты идентификации ОС (в баллах)

	Windows'95 OSR2	Windows'98	Windows NT 4.0 Server SP1	Windows 2000 Professional SP3	Windows Server 2003	MCBC 3.0	Red Hat Linux 7.1	Общий балл
Ревизор сети	-1	-1	0	+1	0	-1	-1	-3
XSpider	+1	+1	+3	+1	+1	+1	+1	+9
Retina	-1	-1	+3	+3	+3	-1	-1	+5
NeWT	+3	+3	+3	+3	+3	+3	+3	+21
IS	-1	-1	+3	+3	+3	-1	-1	+5
Нестандартная настройка стека								
Ревизор сети				-3	-3			-6
XSpider				+1	+1			+2
Retina				-1	-1			-2
NeWT				+3	+3			+6
IS				-1	-1			-2

Таблица 4 – Результаты идентификации сервисов (в баллах)

	Windows NT 4.0 Server SP1	Windows 2000 Professional SP3	Windows Server 2003	MCBC 3.0	Общий балл
TCP-сервисы					
Ревизор сети	+24	+10	+5	+19	+58

XSpider	+33	+26	+42	+10	+111
Retina	+23	+22	+12	+24	+81
NeWT	+30	+24	+30	+22	+106
IS	+8	+3	-5	+11	+17
UDP-сервисы					
Ревизор сети	+1	+1	0	-66	-64
XSpider	-1	-3	-7	-2	-13
Retina	-5	-5	-9	-2	-21
NeWT	-5	-3	-9	-12	-29
IS	-5	-5	-9	-12	-31

Таблица 5 − Показатели возможностей обнаружения уязвимостей (в баллах)

	Windows NT 4.0 Server SP1	Windows 2000 Professional SP3	Windows Server 2003	MCBC 3.0	Общий балл
Ревизор сети	-5	-1	-2	-1	-9
XSpider	-4	0	+2	+8	+6
Retina	0	-3	+2	+3	+2
NeWT	-8	+9	+14	+11	+26
IS	+8	-11	-7	-5	-20

Таблица 6 − Оценка удобства и полноты интерфейса (в баллах)

Оцениваемый фактор	Ревизор сети	XSpider	Retina	NeWT	IS
Наличие планировщика	-	+2	+2	-	+2
Возможность создания профилей проверок	+ 3	+ 3	+ 3	+ 3	+ 3
Возможность генерации отчета для технического специалиста	+ 3	+ 3	+ 3	+ 3	+ 4
Возможность генерации отчета для руководителя	+ 3	+ 3	+ 3	-	+ 3
Возможность приостановки сканирования	-	+2	-	+2	-
Возможность пересканирования отдельных сервисов	-	+2	-	-	-
Удобство интерфейса пользователя	+4	+5	+4	+3	+4
Документация на русском языке	+2	+2	-	-	-
Общий балл	+15	+22	+15	+11	+16

Сетевой сканер XSpider может рассматриваться в качестве достойной альтернативы коммерческим сканерам. XSpider является свободно распространяемым и постоянно обновляемым программным продуктом. Удобный графический интерфейс (рисунок 5) позволяет определять параметры

сеанса сканирования, наблюдать за ходом сканирования, создавать и просматривать отчеты.

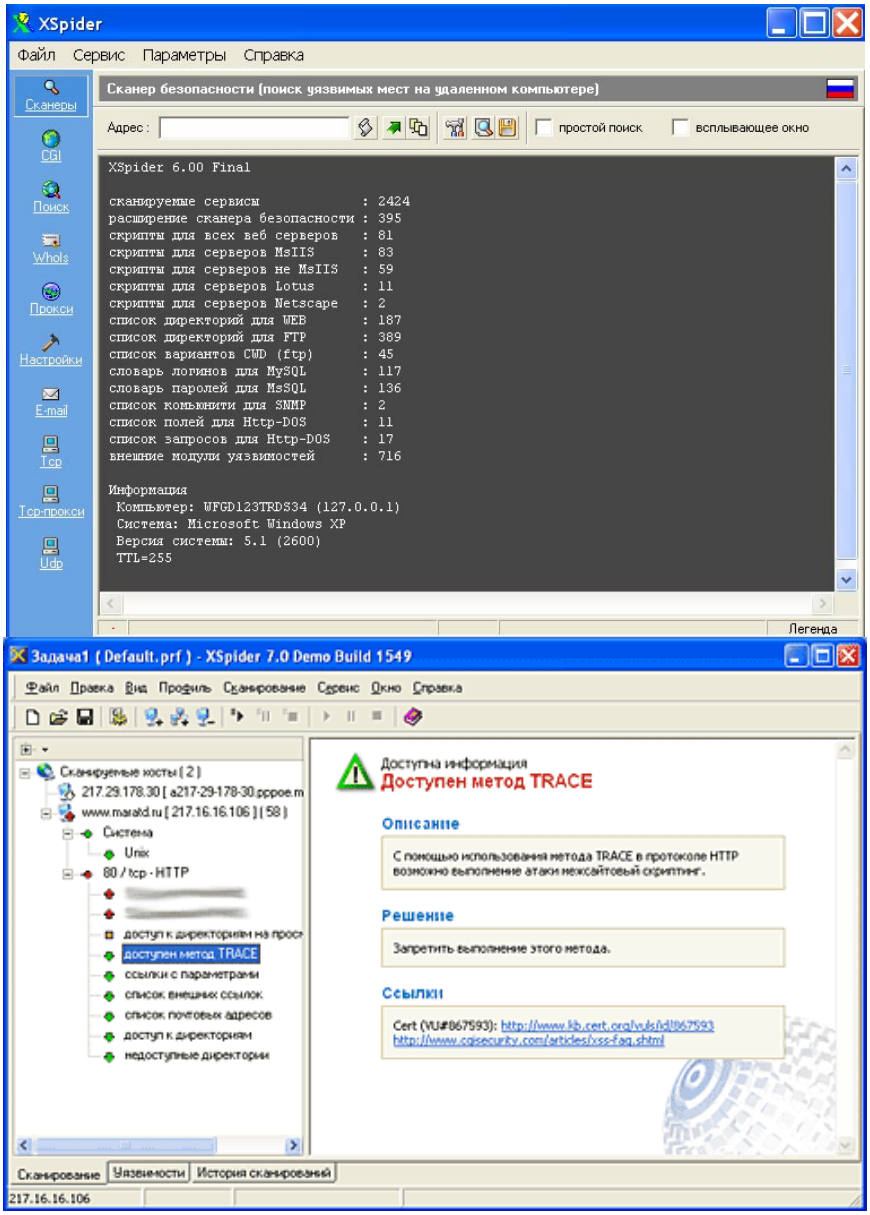

Рисунок 5 – Внешний вид продукта XSpider

Высокое качество работы XSpider-а обеспечивают:

- интеллектуальный подход к распознаванию сервисов;
- многочисленные ноу-хау, использующиеся при поиске уязвимостей;
- уникальная обработка RFC-сервисов всех стандартов с их полной идентификацией;
- анализатор структуры и метод интеллектуального распознавания уязвимостей веб-серверов;
- постоянное обновление встроенной базы уязвимостей.

Одними из отличительных особенностей XSpider-а являются:

- многочисленные ноу-хау используемые в поиске уязвимостей;
- интеллектуальный подход к распознаванию сервисов;

- уникальная обработка RFC-сервисов всех стандартов с их полной идентификацией;
- анализатор структуры и метод интеллектуального распознавания уязвимостей веб-серверов;
- постоянное обновление;
- бесплатное распространение (для российских пользователей);
- поддержка нескольких языков.

Помимо сканера безопасности XSpider включает в себя дополнительные утилиты:

- простые сканеры (TCP и UDP портов);
- CGI-сканер с Brute-словарём;
- определитель исходящего трафика на удаленном компьютере;
- Whols-сервис;
- проверка анонимности прокси-сервера;
- TCP и UDP клиенты;
- TCP-прокси (позволяет пропускать TCP пакеты через себя, с возможностью их коррекции);
- работа с почтой, удаление ненужной почты с сервера;
- локальные настройки безопасности компьютера.

Эти и многие другие особенности позволяют XSpider-у не только находить максимальное количество существующих уязвимостей, но и выдавать минимальное количество ошибочных диагностик, что является распространенной «болезнью» многих других продуктов подобного класса. XSpider позволяет обнаруживать уязвимости на компьютерах, работающих под управлением различных операционных систем: AIX, Solaris, Unix-системы, Windows и другие. Программа работает под управлением MS Windows (95/98/ME/NT/2000/XP/.NET).

Следует сказать, что трудно выделить абсолютно лучший сканер безопасности − все сканеры по-разному справляются с различными задачами. Их достоинства и недостатки в сравнении иллюстрирует многопараметрическая диаграмма (рисунок 6).

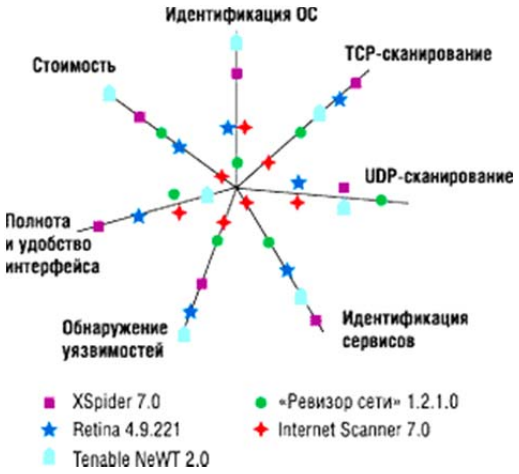

Рисунок 6 − Результаты сравнительного анализа сканеров

В то же время можно сделать некоторые общие выводы.

1 Все сканеры недостаточно качественно идентифицируют UDP-сервисы, что, очевидно, связано с особенностями метода UDP-сканирования.

2 Сканеры лучше работают с ОС линейки Windows NT, чем с Linux. Возможно, этот результат связан с большей стандартизованностью ОС Microsoft.

3 Самый дорогостоящий сканер IS продемонстрировал в ряде случаев весьма невысокие результаты, тогда как представитель семейства Nessus, доступный на некоммерческой основе, оказался одним из лучших.

4 В лабораторных условиях NeWT и XSpider обеспечили наилучшие показатели (разница между ними находится в пределах статистической погрешности), хорошие результаты показал сканер Retina, несколько отстают IS и «Ревизор сети».

Таким образом, можно говорить о целесообразности использования нескольких сканеров уязвимостей при аудите безопасности или в ходе аттестационных и сертификационных испытаний информационных систем и межсетевых СЗИ.

Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer (MBSA) – свободно распространяемое средство анализа защищенности операционных систем Windows и ряда программных продуктов компании Microsoft (Internet Information Services, SQL Server, Internet Explorer и др.). Термин «Baseline» в названии MBSA следует понимать как некоторый эталонный уровень, при котором безопасность ОС можно считать удовлетворительной. MBSA позволяет сканировать компьютеры под управлением операционных систем Windows на предмет обнаружения основных уязвимостей и наличия рекомендованных к установке обновлений системы безопасности. Критически важно знать, какие обновления установлены, а какие еще следует установить на вашей ОС. MBSA обеспечивает подобную проверку, обращаясь к постоянно пополняемой Microsoft базе данных в формате XML, которая содержит информацию об обновлениях, выпущенных для каждого из программных продуктов Microsoft. Работать с программой MBSA можно через графический интерфейс и командную строку.

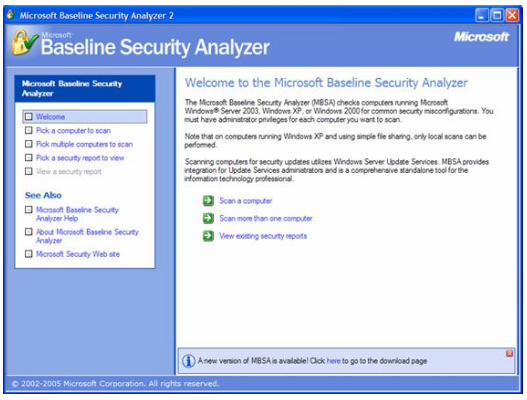

Рисунок 7 − Главное окно программы Microsoft Baseline Security Analyzer

Интерфейс MBSA выполнен на основе браузера Internet Explorer. Главное окно программы разбито на две области (рисунок 7). Так как сеанс работы с MBSA настраивается с помощью мастера, то в левой области представлены шаги мастера, а в правой – основное окно с описанием действий каждого шага.

Nmap. Nmap – это аббревиатура от «Network Mapper». Nmap – набор инструментов для сканирования сети. Он может быть использован для проверки безопасности, просто для определения сервисов запущенных на узле, для идентификации ОС и приложений, определения типа фаерволла используемого на сканируемом узле. Утилита кроссплатформенна, поддерживаются операционных системы Linux, Windows, FreeBSD, OpenBSD, Solaris, Mac OS X.

Nmap имеет GUI, который можно использовать для построения и выполнения команд. Называется Zenmap. Он позволяет выбирать цель, запустить сканирование, отобразить результаты, а также сохранить их и сравнить с другими.

Advanced Host Monitor. Advanced Host Monitor − программа осуществляет постоянный мониторинг доступности и быстродействия серверов. В случае ошибок и сбоев в работе сервера, программа предупреждает администратора (или же пытается исправить проблему самостоятельно). В программе используются 68 методов тестирования, присутствует большое количество настроек. Кроме того, программа позволяет создавать детализированные логи в различных форматах (Text, HTML, DBF и ODBC), имеется встроенный редактор отчетов.

IP-tools. Пакет IP-Tools представляет собой набор из 19 сетевых утилит, объединенных общим интерфейсом.

В состав пакета IP-Tools входят:

1) Local Info − утилита, отображающая информацию о локальном компьютере (тип процессора, память и т.д.);
2) Connection Monitor − утилита, отображающая информацию о текущих TCP- и UDP-соединениях;
3) NetBIOS Info − утилита, отображающая информацию о NetBIOS-интерфейсах локального и удаленного компьютера;
4) NB Scanner − сканер разделяемых сетевых ресурсов;
5) SNMP Scanner − сканер SNMP-устройств в сети;
6) Name Scanner − сканер сетевых имен компьютеров;
7) Port Scanner − TCP-сканер портов;
8) UDP Scanner − UDP-сканер портов;
9) Ping Scanner − IP-сканер с использованием процедуры пингования;
10) Trace − утилита для отслеживания маршрута прохождения пакетов;
11) WhoIs − утилита, позволяющая собирать информацию об узлах в Интернете;
12) Finger − утилита, собирающая и предоставляющая информацию о пользователях удаленного ПК по протоколу Finger;

13) NS LookUp − утилита, позволяющая поставить в соответствие IP-адрес и имя домена;
14) GetTime − утилита, позволяющая синхронизировать время локального ПК и заданного сервера времени;
15) Telnet − утилита для поиска клиентов сети, у которых установлена служба Telnet;
16) HTTP − утилита для поиска клиентов сети, у которых установлена служба HTTP;
17) IP-Monitor − утилита для отображения IP-трафика в реальном времени;
18) Host Monitor − утилита для отслеживания состояния узлов сети (подключен/отключен).

Сканер-ВС. Программный комплекс «Средство анализа защищенности «Сканер-ВС» (далее «Сканер-ВС») предназначен для поиска уязвимостей сетей, исследования топологии сети и инвентаризации сетевых сервисов, сетевого и локального аудита паролей, поиска остаточной информации и анализа сетевого трафика, гарантированного уничтожения информации, контрольного суммирования и аудита беспроводных сетей. «Сканер-ВС» может успешно применяться в качестве мобильного места администратора информационной безопасности, а также как средство расследования инцидентов информационной безопасности и для мониторинга сети.

К основным функциям «Сканер-ВС» относятся:

- контроль использования сертифицированных средств защиты информации;
- обеспечение доверенной загрузки операционной системы;
- обеспечение автоматизированного анализа конфигурационных параметров подсистемы обеспечения информационной безопасности;
- обеспечение анализа безопасности и обнаружения уязвимостей сетевых сервисов;
- выполнение анализа стойкости парольной подсистемы;
- удаленная идентификация операционных систем;
- проведение низкоуровневого анализа сетевого трафика;
- выполнение аудита беспроводных сетей;
- выполнение гарантированного уничтожения информации;
- выполнение контрольного суммирования заданных файлов, дисков;
- антивирусная защита файлов;
- аудит обновлений ОС Windows.

Сканер сети предназначен для проверки безопасности сети посредством поиска хостов, в которых открыты определенные порты. Сканер сети позволяет определять тип операционной системы удаленного хоста с использованием отпечатков стека TCP/IP, неактивные хосты методом параллельного ping-опроса и наличие пакетных фильтров, проводить невидимое сканирование, динамическое вычисление времени задержки и повтор передачи пакетов, параллельное сканирование, сканирование с

использованием ложных хостов, прямое RPC-сканирование, сканирование с использованием IP-фрагментации.

Сканер безопасности позволяет осуществлять поиск уязвимостей в сетевых сервисах, предлагаемых операционными системами, межсетевыми экранами, маршрутизаторами и другими сетевыми компонентами. Для поиска уязвимостей используются как стандартные средства тестирования и сбора информации о конфигурации и функционировании сети, так и специальные средства, эмулирующие действия злоумышленника по проникновению в системы, подключенные к сети.

Средство локального аудита паролей предназначено для поиска на локальной рабочей станции паролей неустойчивых к взлому и содержащих легко подбираемые символьные комбинации.

Средство сетевого аудита паролей предназначено для поиска и выявления на удаленных рабочих станциях неустойчивых к взлому паролей (содержащих легко подбираемые символьные комбинации). Выявление неустойчивых к взлому паролей осуществляется с помощью попытки взлома паролей. Сетевой аудит паролей – многопоточный сканер, поддерживающий подбор паролей для множества сервисов.

Сетевой анализатор предназначен для использования администратором сети при проверке и детальном анализе конфигурации сетевого программного обеспечения.

Системный аудитор предназначен для сканирования локальной системы, определения параметров установленных на рабочей станции операционных систем и идентификации системных, коммуникационных и периферийных устройств, в том числе носителей информации и USB-устройств.

Средство поиска информации предназначено для поиска информации по ключевым словам на носителях данных (жестких дисках, дискетах, оптических дисках).

Аудитор беспроводных сетей предназначен для обнаружения, сканирования и выбора точек доступа для проведения атак для выявления пароля к точке доступа.

Гарантированное уничтожение информации предназначено для удаления информации путем затирания файла случайным набором символов, что предотвращает восстановление информации.

Audit pro. Программное обеспечение AuditPro Базовая версия позволяет управлять IT-активами организации – аппаратными и программными. Помимо инвентаризации программного и аппаратного обеспечения AuditPro Базовая версия решает проблемы управления лицензиями на ПО и распределения ответственности.

Возможности владельцев AuditPro:

- перенос ответственности за установленное ПО на конечных пользователей компьютеров;
- отслеживание, какие программы используются для основных задач класса (а не все, что установлено на жесткий диск в расчете на возможную

необходимость), и эффективная оптимизация политики лицензирования на основании этой информации;
- ограничение использования нелегального ПО и предотвращение нарушения законов об охране авторских прав в организации;
- рационализация процедуры администрирования лицензий на ПО в компании;
- сокращение затрат на приобретение оборудования и лицензий на программное обеспечение;
- ограничение нежелательных действий пользователей ПК (таких как запуск игр в рабочее время, нецелевое использование корпоративного канала интернет-доступа, хранение личных фотографий и музыки и др.). Эти действия могут вызывать перезагрузку сетей, потерю свободного места на жестких дисках и отвлекают от выполнения рабочих обязанностей;
- соответствие международному стандарту ISO 19770;
- внедрение постоянно обновляемой системы учета активов корпоративных компьютеров, программного обеспечения, лицензий, установленных копий приложений и оборудования.

Shadow Security Scanner. Shadow Security Scanner − сканер сетевой безопасности который благодаря уникальным методам позволит надежно проверить Ваш сайт или сеть на наличие дыр и позволит надежно защитить Вашу сеть от проникновения хакеров.

− при сканировании системы, Shadow Security Scanner производит анализ данных, выявляет уязвимые места, возможные ошибки в настройке сервера и предложит возможные пути исправления недочетов и уязвимых мест в системе, подскажет, откуда можно загрузить патч или обновленное программное обеспечение. Shadow Security Scanner умеет автоматически (Fix-It) исправлять найденные ошибки в безопасности одним нажатием на кнопку в меню Fix-It.

− Shadow Security Scanner сканирует не только машины на которых стоят операционные системы Windows, но так же разные операционные системы Unix (Linux,*BSD,Solaris, etc) роутеры, файрволы и системные устройства. В него входит аудит таких модулей как TCP/IP, UDP, FTP, DNS, SMTP, POP3, HTTP, CGI, NetBIOS, Registry, Users accounts, Password checks, Services, LDAP, DoS атаки, и многое другое.

− используя Редактор Правил и установки, пользователи могут выбрать для сканирования только те порты и сервисы, которые он считает нужным, и не тратить время на сканирование других сервисов. Гибкость настройки позволяет администратору управлять как полнотой так и глубиной сканирования, что позволяет ускорить сканирование не в ущерб качеству.

− после окончания сканирования Вы имеете возможность сохранения детального отчета по его результатам. Только SSS имеет возможность сохранения отчета как в html формате так и в форматах xml, pdf, rtf, chm.

Задание на выполнение

Использовать средства для анализа: внутренней физической сети и хостов на наличие уязвимостей – внутренний акт. аудит; виртуальной − на базе гостевых систем VirtualBox или VMWare (1 серв, 3 хоста – как смешанные, так и однородные (win, linux)) – для пентеста (внешний активный аудит). Используемые средства: MBSA, Nmap (zmap или другой форк), hostmonitor (IP-tools), сканер-ВС, audit pro, Shadow Security Scanner, XSpider.

Варианты конфигурации

1) windows-guest (только windows системы) – нечетные по списку студенты;
2) windows-linux-guest (смешанные) – четные по списку студенты.

Порядок выполнения работы

1 Изучить возможности программных средств анализа уязвимостей.

2 Привести ссылки на сайты разработчиков этих средств, тип лицензии (GPL, BSD или другая), наличие сертификатов.

3 Создать требуемый набор виртуальных машин (в соответствие с вариантом) и объединить их в локальную сеть.

4 Гостевые системы настроить таким образом, чтобы в одной из них стояли все обновления безопасности, работал антивирус и файрвол, включен парольный вход, установлен офис; во второй − отсутствовали обновления безопасности; в третьей – не было обновлений, отключены антивирус, файрвол, вход – беспарольный.

5 Выполнить сканирование хостовой системы и локальной сети.

6 Выявить существующие уязвимости.

7 Приложить отчеты утилит и проанализировать их содержание.

8 Сделать вывод по проделанной работе (сравнить функциональные возможности программных средств).

Москвин Владимир Викторович

АКТИВНЫЙ АУДИТ

Методические указания
по выполнению лабораторной работы по дисциплине «Аудит информационной безопасности» для студентов очной формы обучения направлений 10.05.03 и 10.03.01

Редактор Н.Н. Погребняк

Подписано к печати 25.06.18	Формат 60×84 1/16	Бумага 65г/м^2
Печать цифровая	Усл. печ. л. 1,25	Уч. изд. л. 1,25
Заказ 126	Тираж 25	Не для продажи

БИЦ Курганского государственного университета.
640020, г. Курган, ул. Советская, 63/4.
Курганский государственный университет.