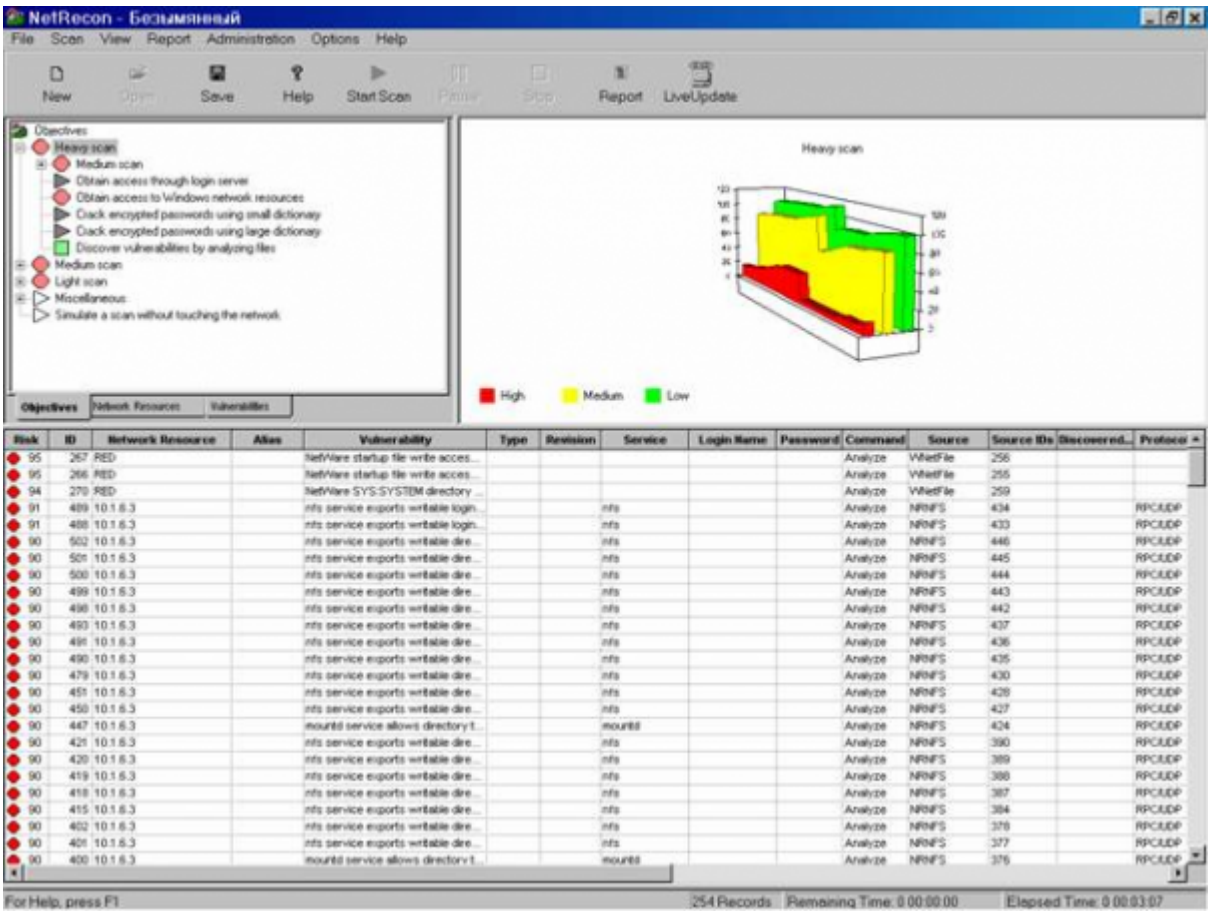
Идентификация технических уязвимостей

написано Александр Астахов | 10 июня, 2023

Идентификация технических уязвимостей(см. рисунок) производится для внешнего и внутреннего периметра корпоративной сети. Внешний периметр – это совокупность всех точек входа в сеть. К внутреннему периметру (внутренней ИТ инфраструктуре) мы относим все хосты и приложения, доступные изнутри.



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 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 эмитируют 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 проверяется наличие и работоспособность механизмов безопасности, соответствие состава и конфигурации системы защиты требованиям безопасности. Выводы о наличии уязвимостей делаются на основании анализа конфигурации используемых средств защиты и системного ПО, а затем проверяются на практике. Основным инструментом тестирования в данном случае являются средства анализа защищенности системного уровня, хостовые сканеры и списки проверки.

Для интентификации технических уязвимостей проводятся следующие организационно-технические мероприятия по анализу защищенности:

- ручные проверки системной конфигурации;
- сетевое и хостовое сканирование;
- тестовые испытания;
- тесты на проникновение;
- социальные тесты;
- анализ программных кодов.

Современные методы анализа защищенности информационных систем настолько разнообразны, что им можно было бы посвятить отдельную книгу. Далее мы ограничимся кратким рассмотрением лишь некоторых из этих методов.

Ручная проверка системной конфигурации

Ручная проверка системной конфигурации производится с использованием списков проверки, рекомендаций разработчиков и независимых экспертов, политик и технических стандартов, а также собственного опыты проверяющего.

Оформление результатов ручных проверок производится точно так же, как и для организационных уязвимостей.

На следующем рисунке приведен фрагмент отчета с описанием уязвимостей антивирусной системы.

Таблица. Результаты проверки антивирусной подсистемы (фрагмент)

Задачи:	1. Проверка конфигурации антивирусной подсистемы2. Проверка лицензий на антивирусное ПО3. Проверка установки последних обновлений антивирусных БД и ПО4. Проверка настройки параметров карантина
Свидетельства:	1. Все рабочие станции, серверы и почтовая система защищены антивирусным ПО в соответствии с Политикой антивирусной защиты2. Лицензии имеются3. Обновление антивирусных БД устанавливаются каждый час
Уязвимости/недостатки:	1. Не настроены параметры карантина, что приводит к потере подозрительных файлов
Рекомендации:	1. Произвести настройку параметров антивирусного карантина, определив место и время хранения подозрительных файлов

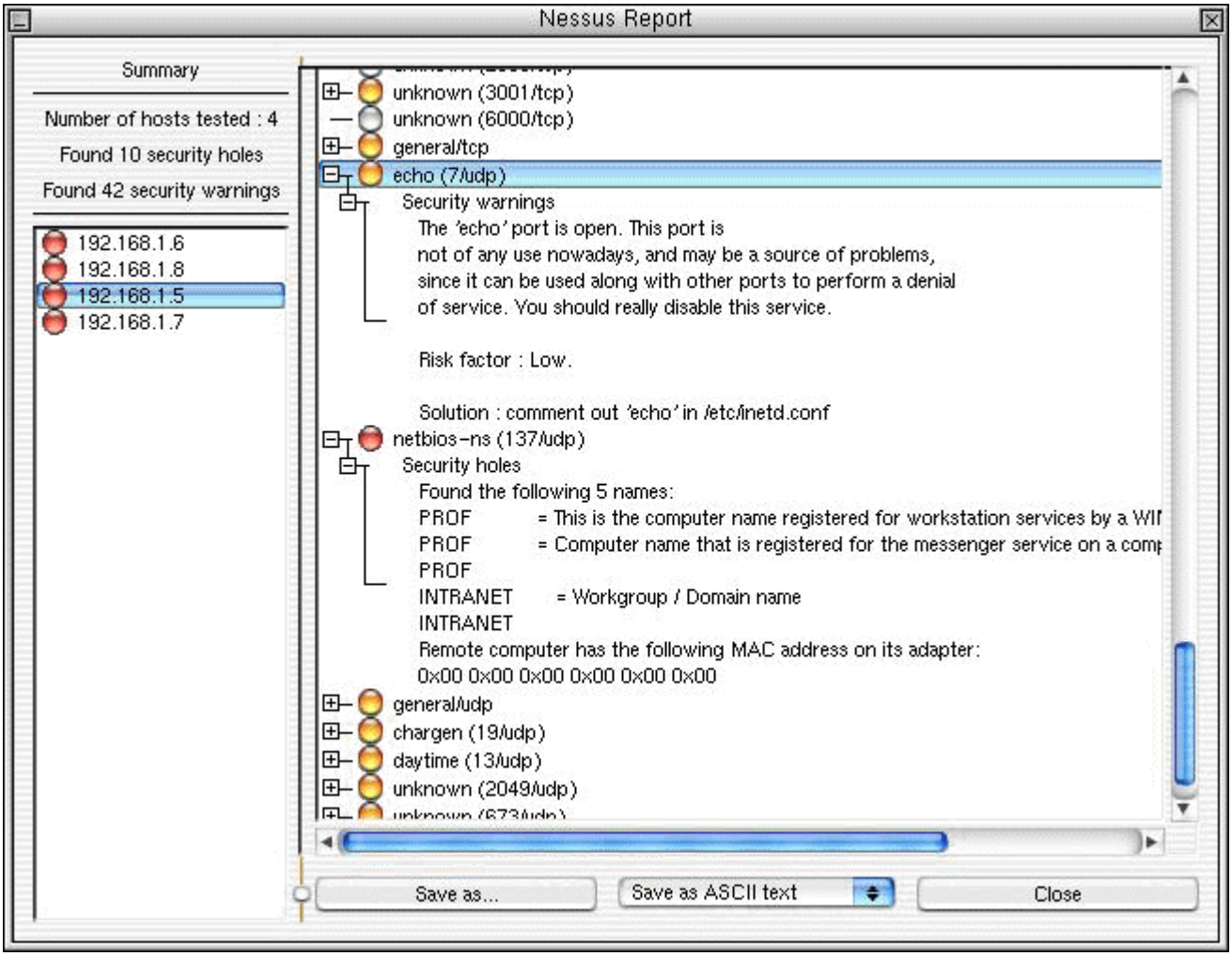
При анализе конфигурации средств защиты внешнего периметра ЛВС

и управления межсетевыми взаимодействиями особое внимание обращается на следующие аспекты, определяемые их конфигурацией:

- настройку правил разграничения доступа (правил фильтрации сетевых пакетов) на МЭ и маршрутизаторах;
- используемые схемы и настройка параметров аутентификации;
- настройку параметров системы регистрации событий;
- использование механизмов, обеспечивающих скрытие топологии защищаемой сети, включающих в себя трансляцию сетевых адресов (NAT), «маскарадинг» и использование системы split DNS;
- настройку механизмов оповещения об атаках и реагирования;
- наличие и работоспособность средств контроля целостности;
- версии используемого ПО и наличие установленных пакетов программных коррекций.

Сетевое сканирование

Большая часть технических уязвимостей выявляется в автоматическом режиме при помощи сетевых и хостовых сканеров, которые способны одновременно выполнять тысячи проверок сразу на многих хостах. Обычно сканеры создают очень подробные отчеты об уязвимостях, к которым следует относиться весьма критически. Мы называем эти отчеты гипотезами об уязвимостях, требующими дальнейших ручных проверок.



На рисунке представлены результаты сканирования в сканере Nessus.

Сетевые сканеры выполняют четыре основные задачи:

- идентификация доступных сетевых ресурсов;
- идентификация доступных сетевых сервисов;
- идентификация имеющихся уязвимостей сетевых сервисов;
- выдача рекомендаций по устранению уязвимостей.

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 определенных классов уязвимостей, ориентированных на определенные программно-аппаратные платформы и приложения. Их можно найти в сети Интернет. Число уязвимостей в базах данных современных сканеров исчисляется тысячами.

Результаты сканирования систем должны быть отсортированы по степени критичности обнаруженных уязвимостей. Описание уязвимости должно включать в себя: ее название или идентификационный номер CVE (Common Vulnerabilities and Exposures – общепризнанный репозиторий уязвимостей), адреса и имена хостов, подверженных данной уязвимости, описание угрозы для конкретной организации, связанной с данной уязвимостью, а также рекомендации по устранению уязвимости либо уменьшению ее влияния на безопасность организации (обычно с ссылкой на соответствующие источники информации и программные коррекции).

Таблица. Результаты сетевого сканирования (фрагмент)

Уязвимость (CVE)	IP адрес/имя	Описание угрозы	Рекомендации
Высокий риск			
Уязвимость сервера БД ToolTalk(rpc.ttdbserverd). Переполнение буфера в сервисе «Ttdbserverd» (RPCUNIX).CVE: CVE-2002-0679	10.x.x.x10.x.x.x	Атакующий может использовать переполнение буфера для выполнения кода с привилегиями сервера ToolTalkRPC, который обычно выполняется от лица суперпользователя.	Установить патч от вендора.http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0679
Сервис «snmpXdmid». Множественные уязвимости в реализации протокола SNMP.CVE: CVE-2002-0012CVE: CVE-2002-0012	10.x.x.x10.x.x.x10.x.x.x	Возможность получение контроля над сетевым оборудованием.	Установить патч от вендора.http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013
Средний риск			
ddi-tcp-1 (8888/tcp): Возможность подключения к портам, защищенным файерволлом на удаленном хосте с исходящего порта 20.BID: 5279	10.x.x.x	Атакующий может подключиться к сервисам на удаленном хосте, минуя файерволл	Заблокировать на файерволле все пакеты с исходящим портом 20.
Уязвимость сервиса bootparamdRPC, используемого бездисковыми клиентами для получения загрузочной информации.CVE: CVE-1999-0647	10.x.x.x	Атакующий может использовать функцию BOOTPARAMPROC_WHOAMI для получения имени домена NISc сервера, затем используя его для получения доступа к файлу паролей NIS	Настроить фильтрацию входящего трафика для предотвращения доступа к сервисам portmapperи bootparam

Тестовые испытания

Тестовые испытания могут включать в себя любые виды проверок: ручные, автоматические, оценку соответствия и т.п. Кроме этого, они позволяют убедиться в работоспособности механизмов контроля и проверить правильность обработки информации на тестовых данных. Примером могут служить аттестационные испытания объектов информатизации по требованиям безопасности информации, сертификационные испытания средств вычислительной техники (СВТ), а также приемо-сдаточные испытания систем, вводимых в эксплуатацию.

Для проведения тестовых испытаний необходимо определить требования безопасности, предъявляемые к испытываемым системам, разработать программу и методику испытаний в соответствии с этими требованиями, подготовить наборы входных и выходных данных.

Фрагмент программы аттестационных испытаний информационной системы обработки персональны данных (ИСПДн) по требованиям безопасности информации может выглядеть, например, следующим образом:

Наименование и порядок испытаний	**Пункт методи**
Проверка реализации требований по защите каналов связи, используемых для обмена персональными данными	4.2.1
Проверка реализации требований по физической защите помещений, в которых ведется работа с персональными данными	4.2.2
Проверка реализации требований по защите персональных данных от НСД	4.2.3
Проверка реализации требований по обеспечению доступности и незамедлительного восстановления персональных данных	4.2.4

Проверка реализации требований по контролю уровня защищенности персональных данных	4.2.5
Проверка правильности и полноты реализации организационно-технических мероприятий по обеспечению безопасности персональных данных	4.2.6
Проверка наличия утвержденного списка лиц, допущенных к работе с персональными данными	4.2.7
Проверка реализации требований по регистрации запросов на получение персональных данных	4.2.8
Проверка регламента (процедуры), определяющего порядок предоставления персональных данных и порядок действий в случае обнаружения нарушений порядка предоставления персональных данных	4.2.9

Методика испытаний для каждого пункта Программы определяет проверяемые требования безопасности, способы их реализации в испытываемой системе и методы проверки их реализации.

Фрагмент методики аттестационных испытаний системы Банк-Клиент показан на рисунке.

Требование безопасности	**Реализация требования в системе Банк-Клиент**	**Методика проверки**
должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно постоянного действия длиной не менее шести символов	Идентификация и аутентификация пользователя при доступе к АРМ Банка: -защита ПК от НСД “SecretNet” (имя и пароль не менее 6 символов); -доступ к локальной сети Банка (имя, пароль); -доступ к АРМ Банка (имя, пароль); -доступ к ЭЦП (имя, пароль); -доступ к почтовому серверу СОД (имя, пароль). Идентификация и аутентификация пользователя при доступе к АРМ Клиента: -доступ к АРМ Клиента (имя, пароль); -доступ к ЭЦП (имя, пароль); -доступ к почтовому серверу СОД (имя, пароль). Идентификация и аутентификация абонента при доступе к СОД: осуществляется по X.400 адресу, имени и паролю.	Проверка осуществляется путем выполнения процедур локального и удаленного (сетевого) входа в ОС и в приложение на АРМ Банка, АРМ Клиента и на сервере СОД. Проверяется установка ограничения на минимальную длину пароля. Удаленный доступ к серверу СОД осуществляется по протоколу FTP.

Другим примером тестовых испытаний может служить тестирование планов обеспечения непрерывности бизнеса, фрагмент программы которого показан на рисунке.

Программа тестирования плана обеспечения непрерывности бизнеса

№	Название проверки	Описание проверки	Пункты Плана	Ответственный	Дата	Примечание
1.	**Первоначальное тестирование**	Проверка наличия и доступности документации: • список оповещения • телефонный справочник • регламент резервного копирования и восстановления данных • инструкция по резервному копированию и восстановлению • схема организационной структуры • структурная схема ЛВС • перечни оборудования и ПО • реестр информационных ресурсов • схемы размещения оборудования серверных комнат • схема СКС • контактная информация поставщиков оборудования и ПО • сервисные контракты • инструкции по эксплуатации оборудования и средств связи	9-15	Руководитель аварийного планирования Руководитель группы технической поддержки и сопровождения		Первоначальное тестирование связано с запуском операционной системы, восстановлении тех файлов или драйверов дисков, проверке систем связи. Дальнейшая работа потребует проверки всего прикладного программного обеспечения, которое признано важным для работы организации. Ключ к успеху - отмечать в плане успехи и неудачи и вносить в него изменения так, чтобы следующий тест прошел успешно.

По результатам испытаний оформляются протоколы и заключения, в которых отражаются выявленные недостатки.

Протокол тестирования плана обеспечения непрерывности бизнеса

№	Название проверки	Описание проверки	Пункты Плана	Результат	Примечание
1.	**Первоначальное тестирование**	Проверка наличия и доступности документации: • список оповещения • телефонный справочник • регламент резервного копирования и восстановления данных • инструкция по резервному копированию и восстановлению • схема организационной структуры • структурная схема ЛВС • перечни оборудования и ПО • реестр информационных ресурсов • схемы размещения оборудования серверных комнат • схема СКС • контактная информация поставщиков оборудования и ПО • сервисные контракты • инструкции по эксплуатации оборудования и средств связи • план резервной системы Проверка запуска операционной системы, СУБД и критичных приложений в резервных серверных комнатах	9-15	Выполнено успешно	

Тестовые испытания информационных систем различного назначения позволяют идентифицировать свойственные для этих систем как организационные, так и технические уязвимости.