СРАВНИТЕЛЬНЫЙ АНАЛИЗ СКАНЕРОВ БЕЗОПАСНОСТИ

ЧАСТЬ 1
ТЕСТ НА ПРОНИКНОВЕНИЕ

Автор исследования

Лепихин Владимир Борисович

Заведующий лабораторией сетевой безопасности Учебного центра «Информзащита»

Москва, сентябрь-октябрь 2008

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ

Сетевые сканеры безопасности подходят для сравнения как нельзя лучше. Они все очень разные. И в силу специфики задач, для решения которых они предназначены, и в силу их «двойного» назначения[1], наконец, ещё и потому, что за каждым таким инструментом стоит полёт «хакерской» (в изначальном смысле этого слова) мысли его создателя.

В любом сравнении главное – это:

- выбор условий сравнения;
- выбор критериев сравнения.

При выборе условий сравнения за основу был взят подход «от задач», таким образом, по результатам можно судить, насколько тот или иной инструмент пригоден для решения поставленной перед ним задачи. Например, сетевые сканеры безопасности могут быть использованы:

- для инвентаризации сетевых ресурсов;
- в ходе проведения «тестов на проникновение»;
- в процессе проверки систем на соответствие различным требованиям.

В настоящем документе представлены результаты сравнения сетевых сканеров безопасности в ходе проведения тестов на проникновение в отношении узлов сетевого периметра. При этом оценивались:

- Количество найденных уязвимостей
- Число ложных срабатываний (False Positives)
- Число пропусков (False Negatives)
- Причины пропусков
- Полнота базы проверок (в контексте данной задачи)
- Качество механизмов инвентаризации и определения версий ПО
- Точность работы сканера (в контексте данной задачи)

Перечисленные критерии в совокупности характеризуют «пригодность» сканера для решения поставленной перед ним задачи, в данном случае – это автоматизация рутинных действий в процессе контроля защищённости сетевого периметра.

[1] Сетевые сканеры безопасности могут быть использованы как для защиты, так и «для нападения», а взлом, как известно, задача творческая.

2. СКАНЕР БЕЗОПАСНОСТИ КАК СРЕДСТВО ЗАЩИТЫ

В настоящее время деятельность многих организаций, так или иначе, зависит от состояния их информационных систем. ИТ инфраструктура организации часто содержит узлы и системы, критичные с точки зрения ведения бизнеса, нарушение доступности которых может привести к нанесению значительного ущерба.

В таких случаях, как правило, после соответствующего анализа рисков формируется перечень актуальных угроз и разрабатывается комплекс мер по их нейтрализации. В итоге строится система управления информационной безопасностью (СУИБ), в состав которой входят различные средства защиты, реализующие необходимые защитные механизмы.

Иногда в состав общей системы управления информационной безопасностью входит система выявления уязвимостей, представляющая собой комплекс организационно-технических мероприятий и предназначенная для контроля защищенности информационных систем и устранения обнаруженных уязвимостей.

Контроль состояния защищённости относится к категории так называемых превентивных защитных механизмов. Его главное назначение – своевременно «заметить» слабость (уязвимость) в защищаемой системе, тем самым предотвратить возможные атаки с её использованием.

Поиск уязвимостей можно осуществлять вручную или с помощью автоматизированных инструментов - сканеров безопасности. В настоящее время наибольшее распространение получили сетевые сканеры безопасности, выполняющие проверки дистанционно, по сети. Проверки, выполняемые сетевыми сканерами безопасности, направлены, прежде всего, на сетевые службы. Но сегодня значительная часть сетевых сканеров безопасности, используя различные способы подключения к исследуемым узлам (SSH, WMI, Remote Registry, SMB/NetBIOS), может осуществлять поиск уязвимостей операционных систем, а также некоторых приложений, установленных на сканируемом узле.

3. МЕТОДОЛОГИЯ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ («PENETRATION TESTING»)

Одно из мероприятий, проводимых в ходе контроля состояния защищённости систем – это так называемый тест на проникновение или на устойчивость к взлому.

Методология тестирования сети на устойчивость к взлому (Тестирование на проникновение, Penetration Testing или Ethical hacking) подразумевает, что субъект, выполняющий оценку, опирается на собственное понимание того, как реализована тестируемая система. Он владеет минимумом информации об объекте тестирования, поэтому иногда такой тест называют «методом чёрного ящика». Цель такого теста – поиск способов получения доступа к системе с помощью инструментов и приёмов, используемых нарушителями. Типовая схема «Penetration Testing» приведена на рис.1.

Рис. 1. Схема тестирования на устойчивость к взлому

Подробное обсуждение этой методологии выходит за рамки данного документа, далее приведены лишь краткие комментарии к каждому этапу.

В процессе планирования определяются цели и задачи теста. Оговариваются условия, список допустимых техник, формируется перечень объектов тестирования[2].

Следующий этап – сбор информации. На этом этапе используются различные методы сбора информации о сети, например, идентификация доступных сетевых устройств, идентификация топологии сети, идентификация открытых портов и т. д.

Далее следует процесс идентификации уязвимостей. Здесь используется собранная ранее информация об узлах, операционных системах, сервисах, приложениях. Главным образом используется информация о сервисах, их версиях, а также о приложениях, реализующих

[2] Иногда перечень узлов формируется непосредственно в ходе теста.

указанные сервисы. Эта информация сопоставляется с информацией об известных уязвимостях, т. е. с какими-либо базами уязвимостей.

Последний этап – подтверждение (верификация) уязвимостей, о наличии которых были сделаны предположения на предыдущем этапе. Этот этап можно назвать основным в рассматриваемой методологии. По сути, на этом этапе иллюстрируется возможность получения доступа к системе.

Как показывает практика, полностью автоматизировать процедуру тестирования на устойчивость к взлому невозможно. Что касается сетевых сканеров безопасности, то они могут быть использованы для автоматизации процессов сбора информации и идентификации уязвимостей. Кроме того, отчёты сканера безопасности могут быть включены в общий отчёт по проводимому тесту.

4. УСЛОВИЯ СРАВНЕНИЯ: ВЫБОР ОБЪЕКТОВ СКАНИРОВАНИЯ

В качестве объектов сканирования были выбраны «реальные мишени» – узлы корпоративных сетей, доступные через Интернет. Это узлы, составляющие периметр корпоративных сетей и узлы так называемой демилитаризованной зоны (ДМЗ, рис. 2).

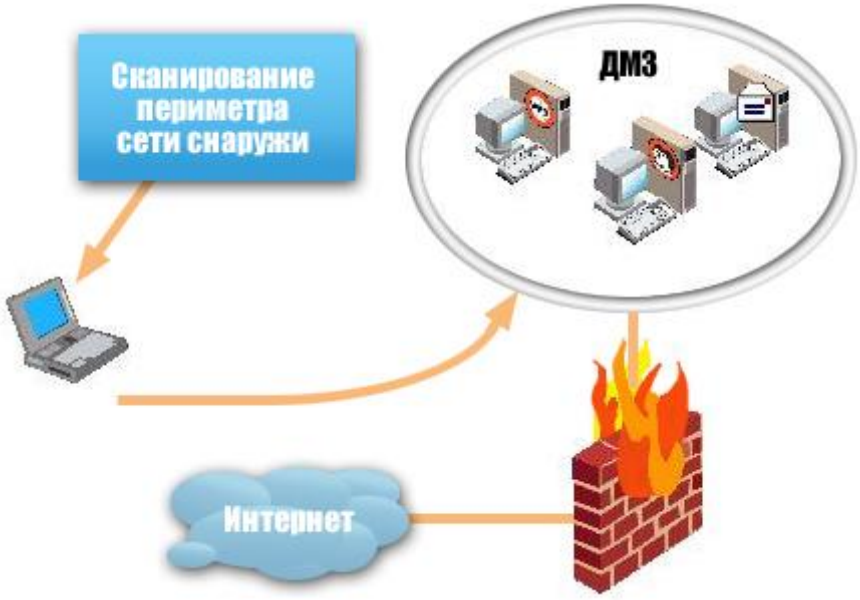

Рис. 2. Расположение сканеров по отношению к объектам сканирования

Следует заметить, что отдельный объект сканирования в данном случае неоднозначен. Это может быть действительно отдельный узел, например, межсетевой экран, периметровый маршрутизатор или многофункциональный сервер (DNS, почта, Web, рис. 3)

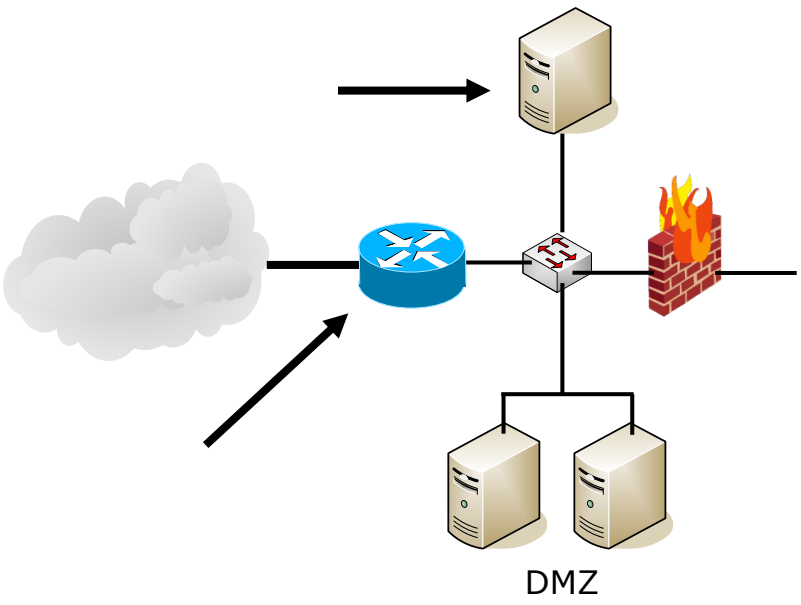

Рис. 3. Пример объекта сканирования

Это может быть и набор из нескольких сетевых сервисов, «объединённых» с помощью трансляции адресов в «один IP-адрес» (рис. 4).

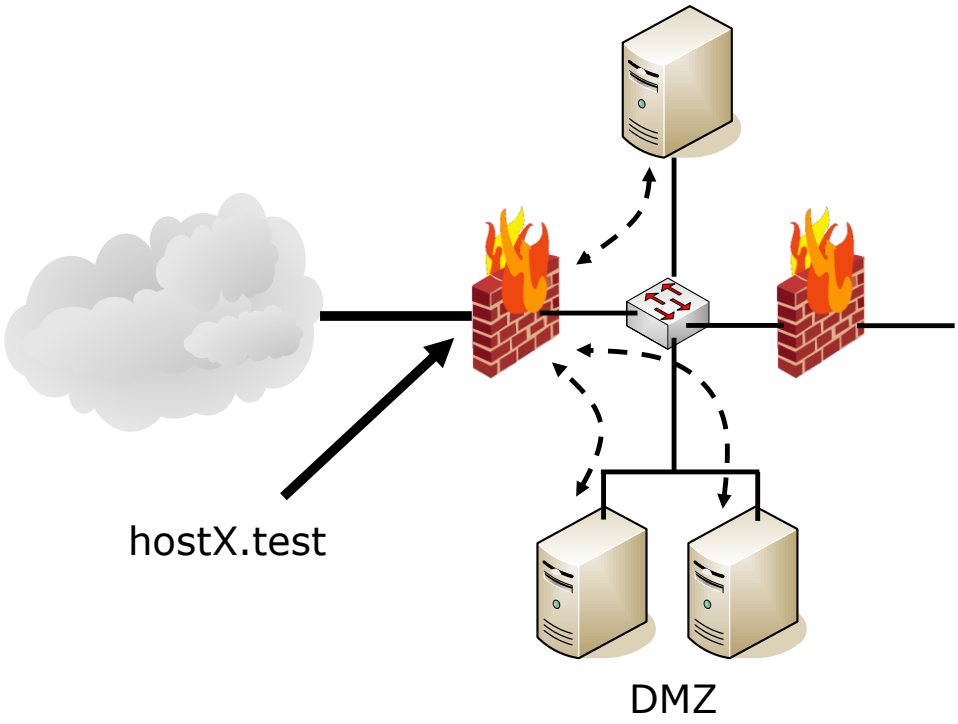

Рис. 4. Пример объекта сканирования

Кроме того, при сканировании узла по доменному имени следует учитывать, что IP-адрес может меняться. В этом случае нужно либо использовать доменное имя, либо проверять перед запуском сканирования соответствие имени и адреса.

Видимо, в данной ситуации лучше привязываться к доменному имени, поскольку оно выглядит наиболее однозначным. Ну и, разумеется, проверять правильность разрешения этого имени[3]. В любом случае, дальше объекты сканирования будут обозначаться доменными именами, например, host1.test. А минимальной «единицей работы» для сканера в данной ситуации следует считать сетевой сервис, уязвимости которого и предстоит выявить.

[3] Некоторые сканеры «не умеют» сканировать узел по имени, как например, Internet Scanner. Тут уж ничего не остаётся, как использовать IP-адреса.

5. КРАТКАЯ ХАРАКТЕРИСТИКА УЧАСТНИКОВ СРАВНЕНИЯ

Перед началом сравнения усилиями портала Securitylab.ru был проведён опрос, целью которого был сбор данных об используемых сканерах и задачах, для которых они используются.

В опросе приняло участие около 500 респондентов (посетителей портала Securitylab.ru). Анализ портрета респондентов по количеству компьютеров в организации (рис. 5) показал, что наибольшая доля опрошенных респондентов (57%) приходится на малый бизнес (менее 100 компьютеров). Вторая по численности группа респондентов попала в категорию от 100 до 1 000 компьютеров в организации (26%). Третья и четвертые группы – это представители крупного бизнеса и федеральных госструктур. Их распределение более 3 000 (11%) компьютеров для третьей и 1 000 – 3 000 (6%) компьютеров для четвертой группы соответственно. Примечательно, что представителей очень крупного бизнеса (более 3 000 компьютеров), принявших участие в опросе, оказалось больше на 5%, чем представителей менее крупного бизнеса (1 000 – 3 000 компьютеров в организации).

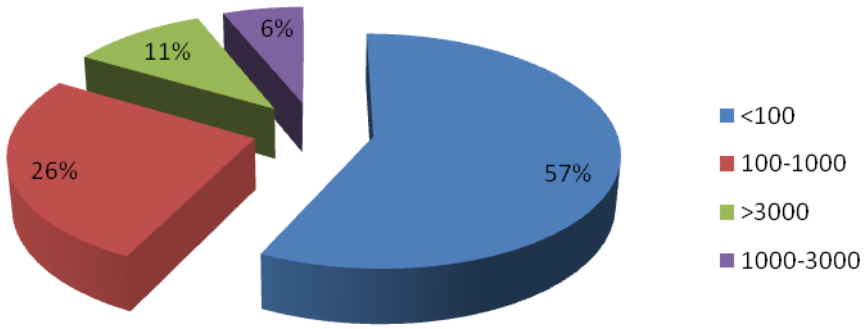

Рис. 5. Распределение респондентов по числу компьютеров в организации

На вопрос об используемых сканерах безопасности в своих организациях, подавляющее большинство респондентов ответило, что они используют хотя бы один сканер безопасности (70%). При этом в организациях, практикующих регулярное применение сканеров безопасности для анализа защищенности своих информационных систем, предпочитают использовать более одного продукта данного класса. 49 % респондентов ответило, что в их организациях используется два и более сканера безопасности (Рис. 6).

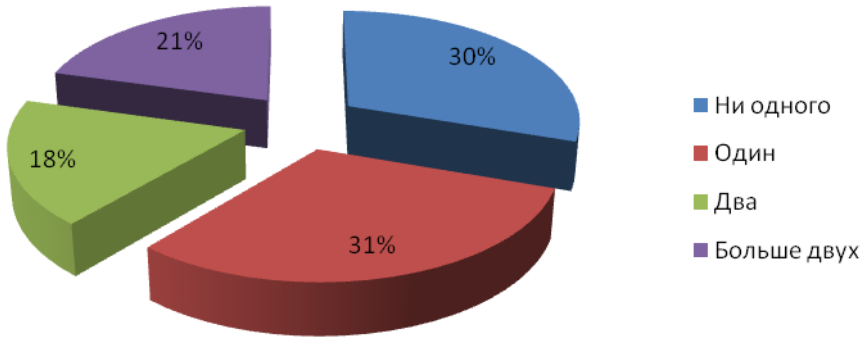

Рис. 6. Распределение организаций опрошенных респондентов по числу используемых сканеров безопасности

Причины, по которым используется более одного сканера безопасности, заключаются в том, что организации относятся с недоверием к решениям одного «вендора» (61%), а также в тех случаях, когда требуется выполнение специализированных проверок (39%), которые не могут быть выполнены комплексным сканером безопасности (Рис. 7).

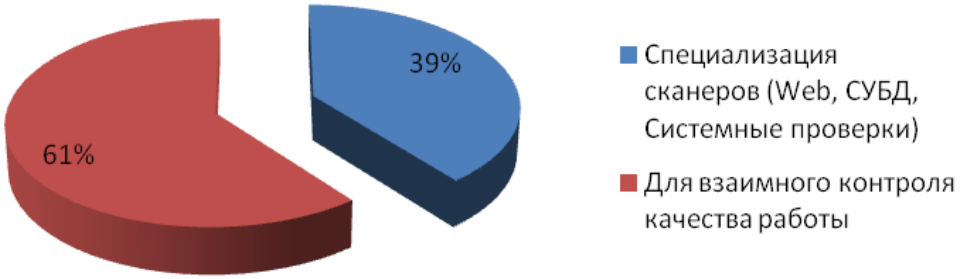

Рис. 7. Причины использования более одного сканера безопасности в организациях опрошенных респондентов

Отвечая на вопрос, для каких целей используются специализированные сканеры безопасности, большинство респондентов ответило, что они используются в качестве дополнительных инструментов анализа защищенности Web-приложений (68%). На втором месте, оказались специализированные сканеры безопасности СУБД (30%), а на третьем (2%) утилиты собственной разработки для решения специфического круга задач по анализу защищенности информационных систем (Рис. 8).

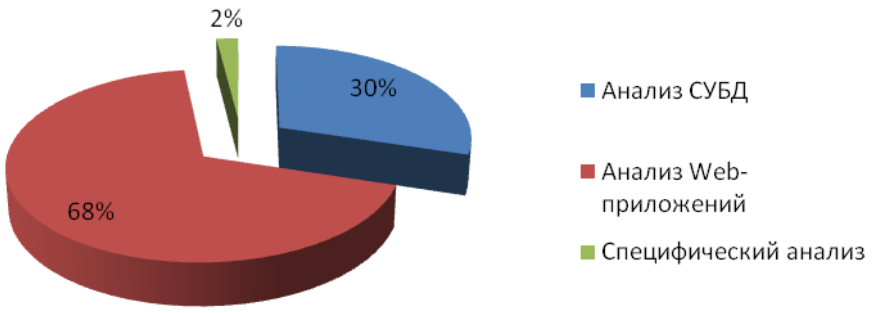

Рис. 8. Цели применения специализированных сканеров безопасности в организациях опрошенных респондентов

Результат опроса респондентов (рис. 9) о конечных продуктах, имеющих отношение к сканерам безопасности, показал, что большинство организаций предпочитают использовать продукт Positive Technologies XSpider (31%) и Nessus Security Scanner (17%).

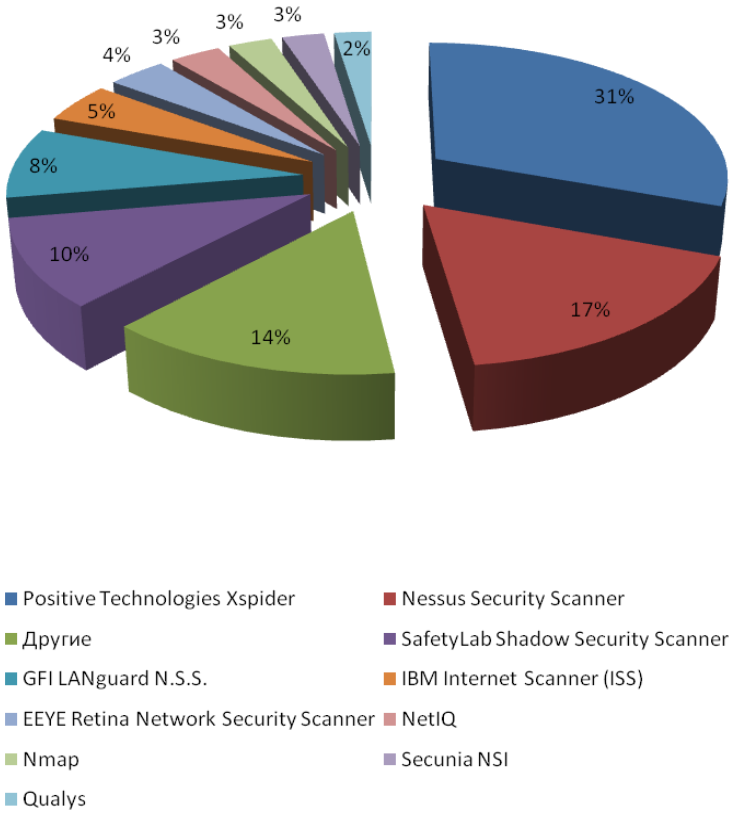

Рис. 9. Используемые сканеры безопасности в организациях опрошенных респондентов

Следующий вопрос, «Какие механизмы сканирования вы применяете?», показывает круг задач, для решения которых применяются сканеры безопасности (рис. 10).

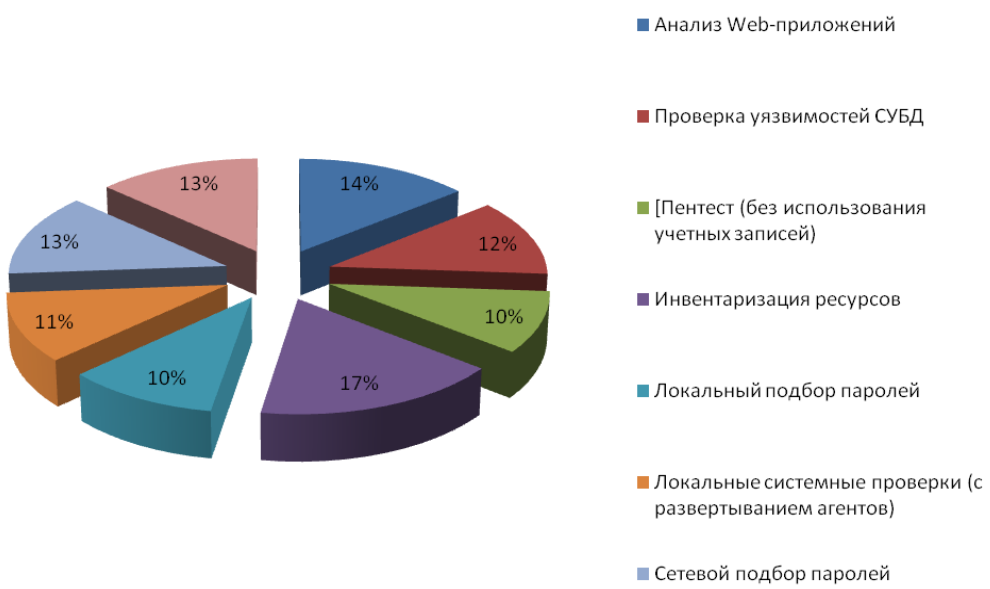

Рис. 10. Применяемые механизмы сканирования в организациях опрошенных респондентов

Наконец, ответы на последние два вопроса характеризуют ситуацию с задачей контроля соответствия стандартам (внутрикорпоративным или международным). Эта задача пока не типична для сканеров безопасности, но в последнее время всё более и более востребована.

Вот как распределились (рис. 11) ответы на вопрос «Существуют ли в организации стандарты по безопасной настройке систем и приложений?».

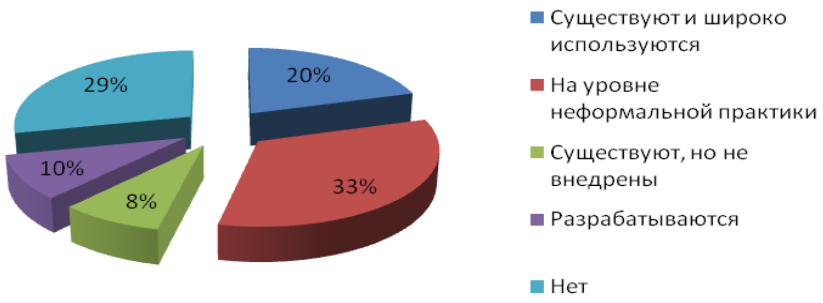

Рис. 11. Распределение организаций по наличию стандартов по безопасной настройке систем и приложений

Т. е. в большинстве случаев (71%) все-таки делаются попытки соответствовать хоть какому-нибудь стандарту.

А вот на вопрос «Используются ли в организации средства автоматизации контроля соответствия стандартам по безопасной настройке систем и приложений?» большая часть респондентов (56%) ответила отрицательно (рис. 12).

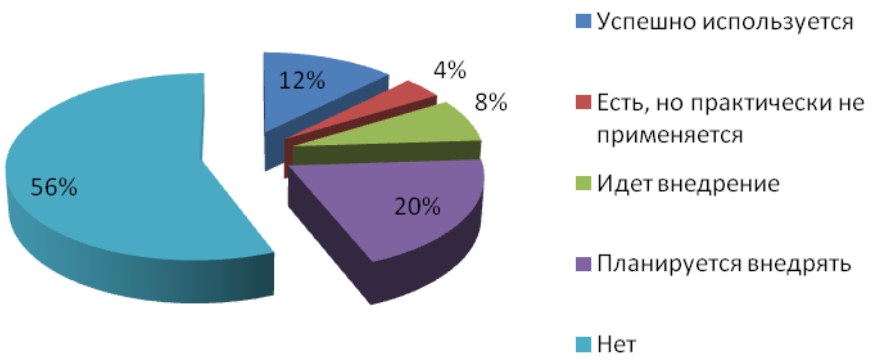

Рис. 12. Распределение организаций по проверке соответствия стандартам по безопасной настройке систем и приложений

Для участия в тестовых испытаниях были отобраны сканеры, представленные в таблице 1.

Таблица 1. Сетевые сканеры безопасности, использованные в ходе сравнения

Название	Версия	Ссылка
Nessus	3.2.1	http://www.nessus.org/download
MaxPatrol	8.0 (Сборка 1178)	http://www.ptsecurity.ru/maxpatrol.asp
Internet Scanner	7.2.58	http://www-935.ibm.com/services/us/index.wss/offering/iss/a1027208
Retina Network Security Scanner	5.10.2.1389	http://www.eeye.com/html/products/retina/index.html
Shadow Security Scanner (SSS)	7.141 (Build 262)	http://www.safety-lab.com/en/products/securityscanner.htm
NetClarity Auditor	6.1	http://netclarity.com/branch-nacwall.html

Итак, первый тест сфокусирован на задаче оценки защищённости систем на устойчивость к взлому.

6. УСЛОВИЯ СРАВНЕНИЯ: НАСТРОЙКИ СКАНЕРОВ

Методология, основанная на восприятии объекта сканирования в виде «чёрного ящика», диктует соответствующие требования к настройкам сканеров. Например, обычно бывают задействованы все методы сбора информации, а также все или почти все проверки. Далее приведены настройки, которые использовались в ходе сравнения.

6.1. Идентификация узлов

Для идентификации узлов были задействованы методы ICMP Ping и TCP Ping. Например, на рис. 13 приведены соответствующие настройки для сканера Nessus.

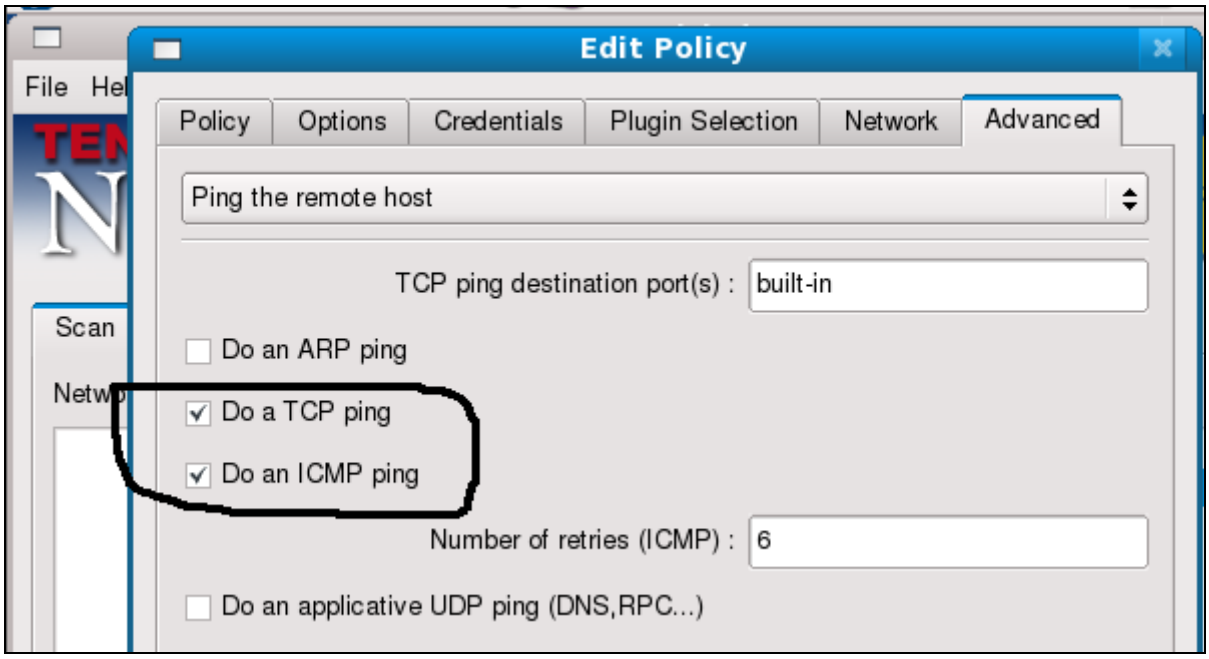

Рис. 13. Включение методов идентификации узлов в сканере Nessus.

Для метода TCP Ping использовался следующий перечень портов:

21, 22, 23, 25, 53, 80, 110, 111, 113, 135, 139, 143, 389, 443, 445, 563, 636, 990, 993, 995, 1521, 1723, 1433, 3128, 3306, 3372, 3389, 4899, 5432, 8080.

Например, область соответствующих настроек сканера Internet Scanner приведена на рис. 14.

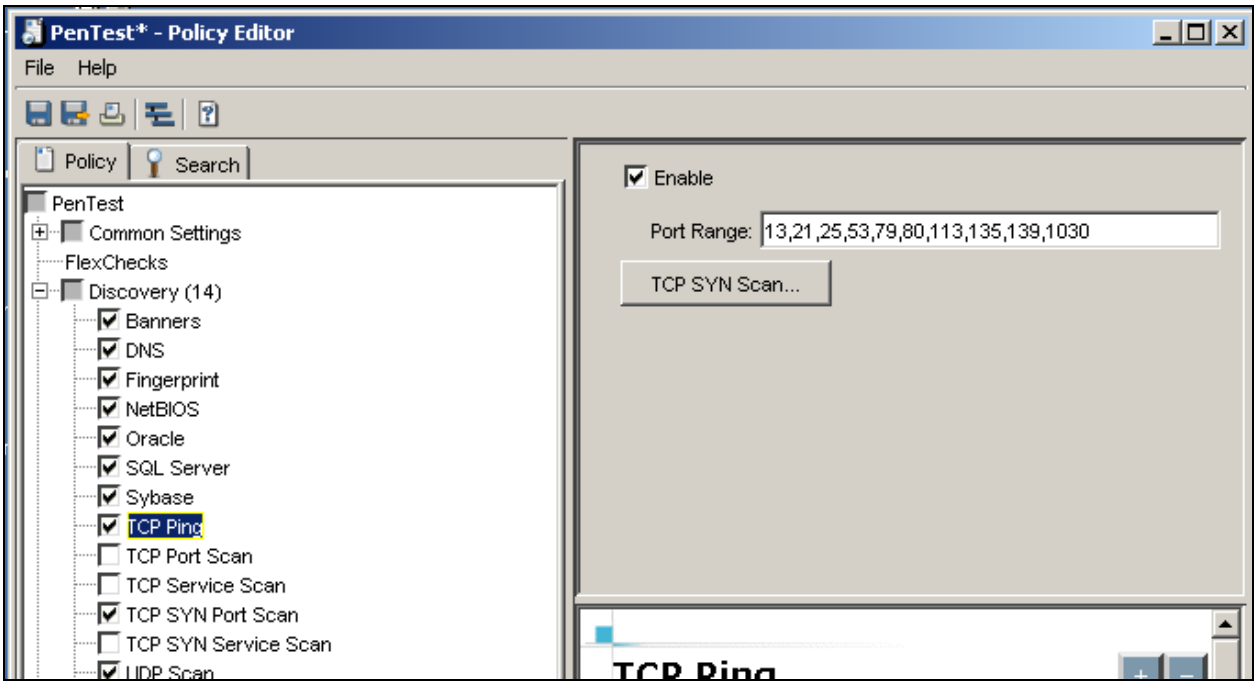

Рис. 14. Задание диапазона портов для метода TCP Ping в сканере Internet Scanner.

6.2. Идентификация открытых портов

Для идентификации открытых портов использовался метод SYNscan, там, где он отсутствовал – TCP connect scan (рис. 15).

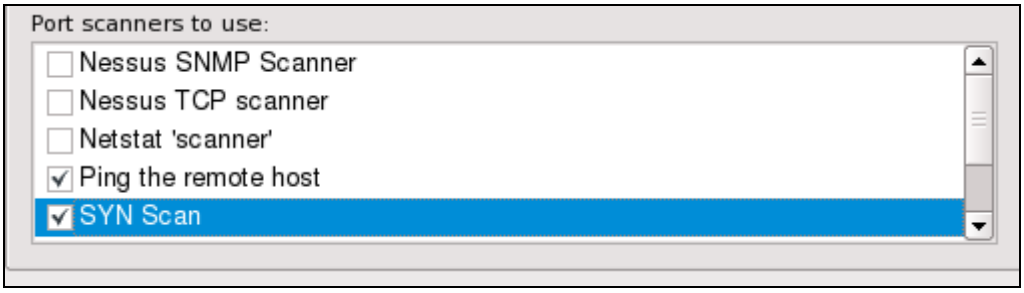

Рис. 15. Включение SYNScan в сканере Nessus

Диапазон сканируемых портов TCP- 1:65535[4] (рис. 16)

Диапазон сканируемых портов UDP - 1:65535

[4] Если задать весь диапазон портов TCP и UDP, процесс сканирования занимает продолжительное время. Поэтому был выбран такой вариант: один сканер запускался по всему диапазону, остальные использовали явно заданный перечень портов.

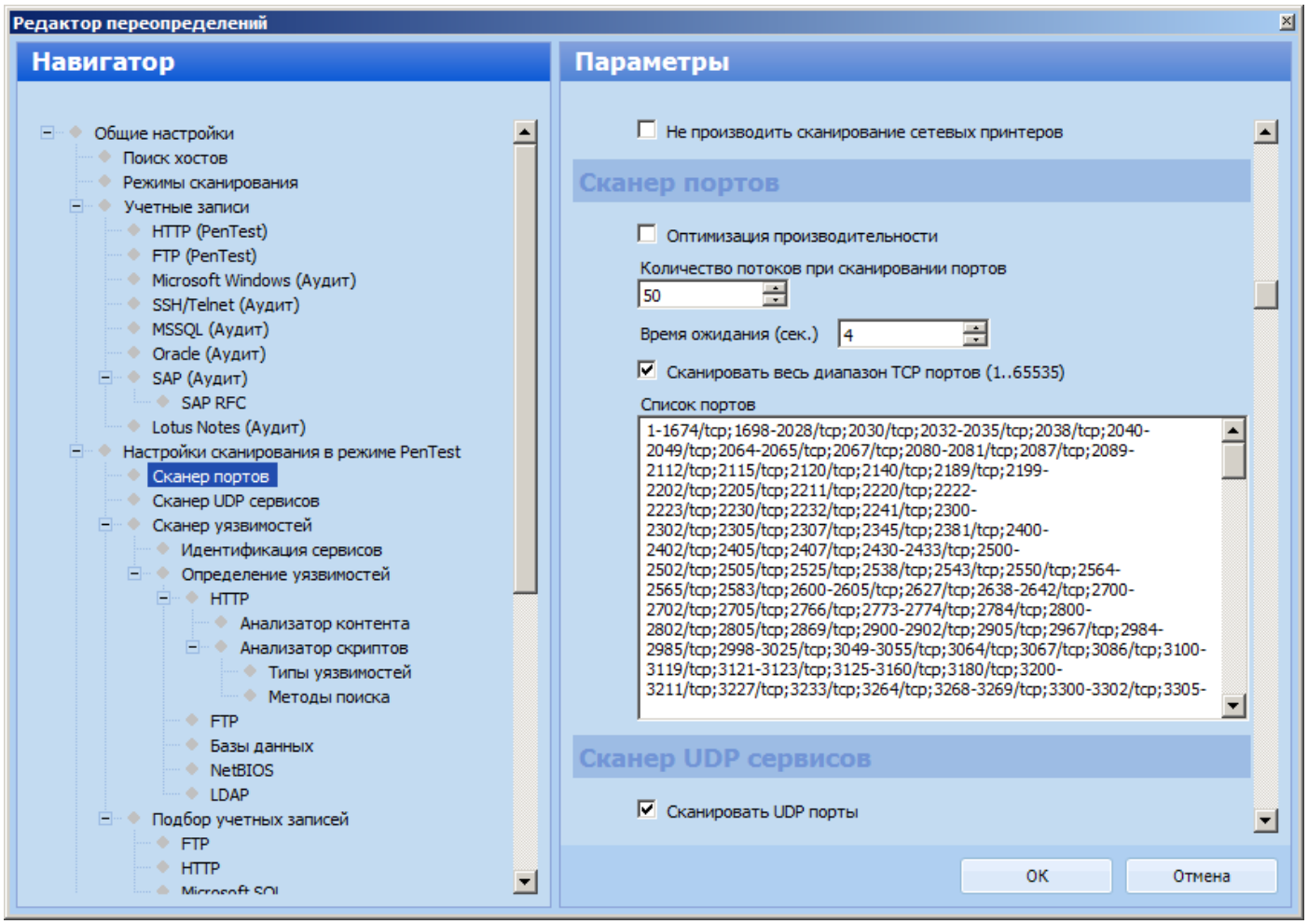

Рис. 16. Настройка диапазона портов в MaxPatrol

6.3. Идентификация сервисов и приложений

В данном случае объект сканирования – это «чёрный ящик», поэтому для идентификации сервисов и приложений должны быть задействованы все поддерживаемые сканером методы (рис. 17).

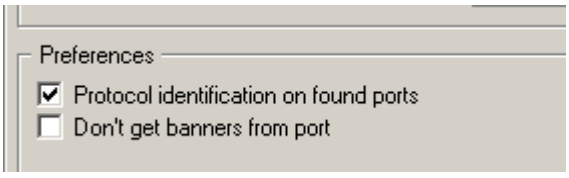

Рис. 17. Включение идентификации сервисов в сканере Shadow Security Scanner

6.4. Идентификация операционных систем

Для идентификации операционных систем были задействованы все имеющиеся в сканерах методы (рис. 18).

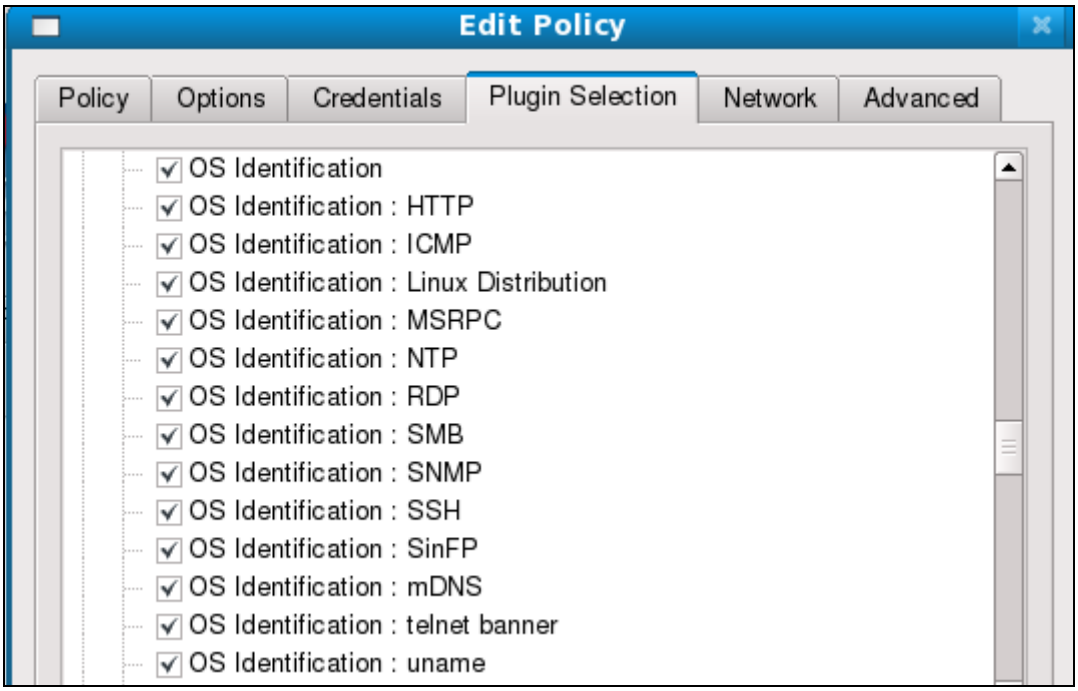

Рис. 18. Настройка индентификации ОС в Nessus

6.5. Идентификация уязвимостей

Для идентификации уязвимостей были включены все имеющиеся проверки, за исключением «опасных» тестов, приводящих к отказу в обслуживании. Как известно, проверки, выполняемые сетевыми сканерами безопасности, можно разделить на две категории:

- Логические выводы (inference) – проверки, основанные на собранной информации, например, на результатах идентификации сервисов и приложений.
- Тесты – проверки, выполняемые путём явных атак или так называемых специальных запросов.

Тесты, в свою очередь, можно поделить на «опасные» и «неопасные». Опасные тесты могут привести к выведению тестируемого сервиса из строя, поэтому в ходе сравнения они не были использованы. На рисунке 19 приведены соответствующие настройки сканера Nessus.

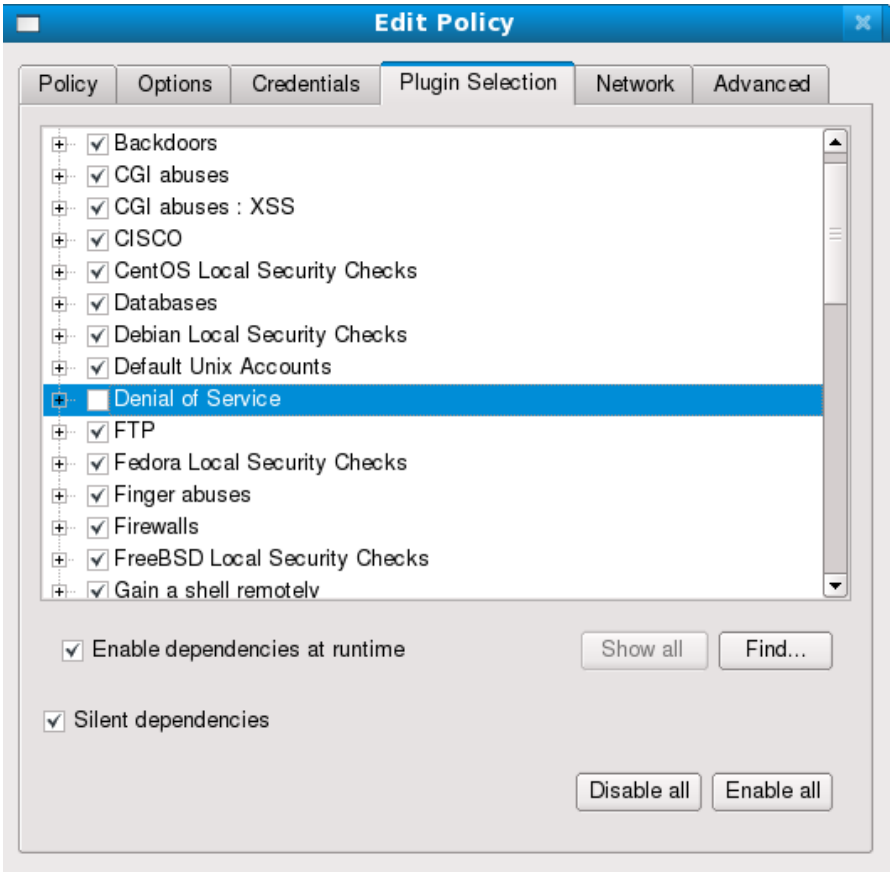

Рис. 19. Отключение DoS проверок («опасных» тестов) в Nessus

Таким образом, идентификация уязвимостей по косвенным признакам была включена, как и идентификация уязвимостей с помощью тестов (если сканер предоставлял возможность выбора, использовались тесты, рис. 20).

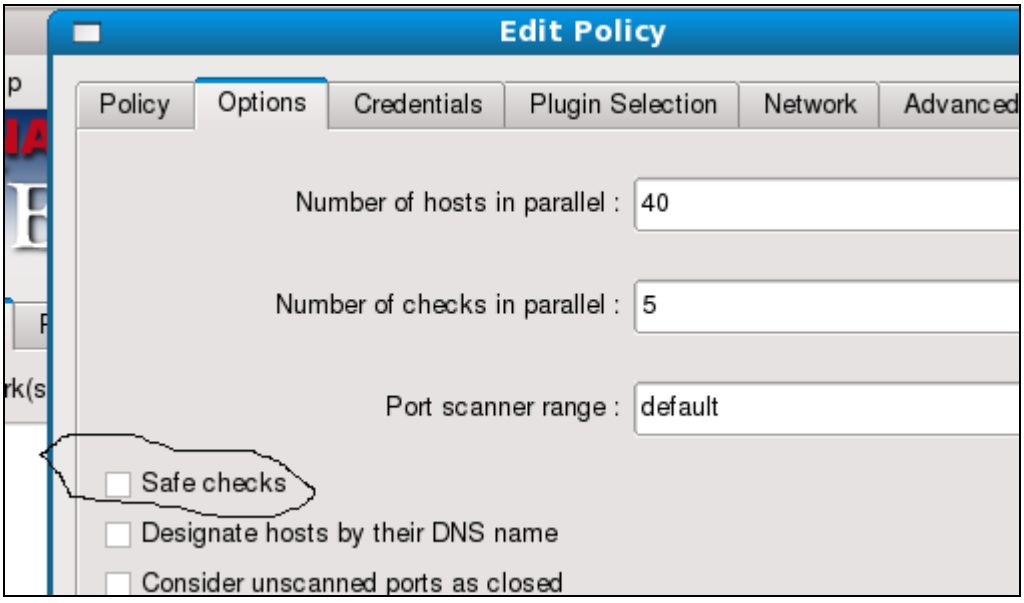

Рис. 20. Включение «тестов»

Отслеживание взаимосвязей проверок было включено. Для подключения к Windows-системам использовался «нулевой сеанс» (рис. 21).

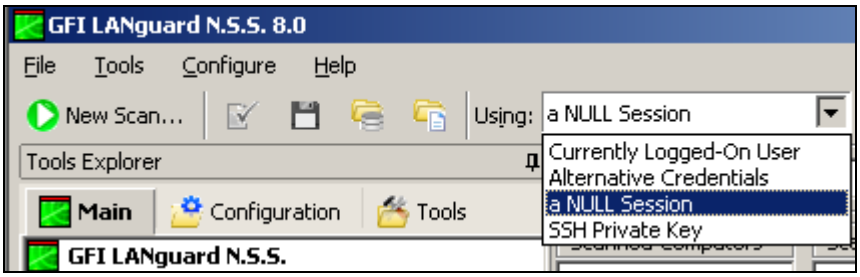

Рис. 21. Настройка аутентификации в GFI LANguard

Однако если сканер поддерживает возможность проводить системные проверки по результатам подбора пароля, то эта опция была задействована (рис. 22).

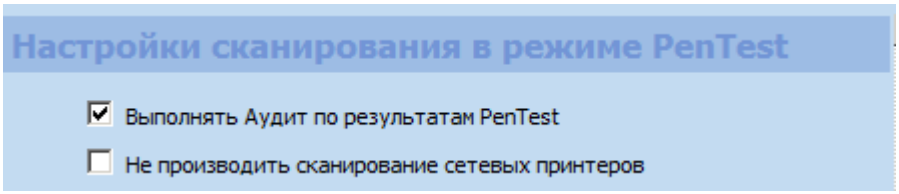

Рис. 22. Функция «Аудит по результам Pentest» в MaxPatrol

Подбор паролей (если такие проверки были, они задействовались) предполагал использование только словарей по умолчанию (не использовались специально подключенные словари).

Наконец, для выяснения причин сбоев и анализа результатов «журналирование» хода работы сканера должно быть включено (рис. 23).

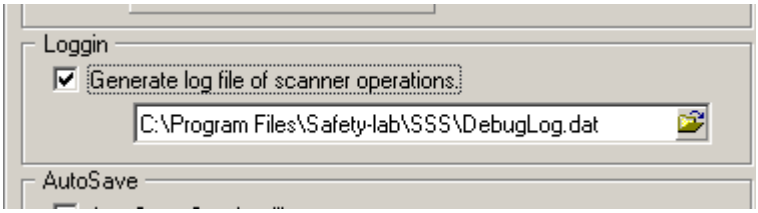

Рис. 23. Включение «журналирования» работы сканера Shadow Security Scanner

7. АНАЛИЗ ЗАДАЧИ

Поскольку в качестве объектов сканирования выступают реальные «мишени», адекватность результатов работы сканеров для сравнения не вызывает сомнений. Но при этом следует понимать, что работа одного сканера может занимать продолжительное время (от нескольких минут до нескольких дней). Если учесть, что сканеры запускались по очереди (одновременное сканирование одного и того же узла разными сканерами было исключено для «чистоты эксперимента»), состояние сканируемого узла могло измениться. Поэтому при анализе результатов были исключены узлы, состояние которых сильно менялось с течением времени. Например, в ходе сканирования был найден узел с пустым паролем администратора. Нетрудно догадаться, что состояние этого узла сильно менялось в ходе сканирования.

Для остальных узлов, прежде всего, составлялся перечень найденных на них сетевых сервисов, который затем приводился «к общему знаменателю», т.е. были оставлены только те сетевые службы, которые были найдены каждым из сканеров. Понятно, что и в этом случае нет никакой гарантии, что конфигурация сканируемого узла не менялась, но тут уж ничего не сделаешь – это ограничение данной методики сравнения.

Из результатов были исключены узлы, на которых слишком много уязвимостей было найдено одним из сканеров. Например, на одном из узлов сканер MaxPatrol нашёл около 150 уязвимостей в одном только сервисе HTTP, тогда как другие сканеры ограничились 10-20-ю уязвимостями. Такие узлы также исключались из сравнения.

8. ОБРАБОТКА РЕЗУЛЬТАТОВ

8.1. Идентификация сервисов и приложений

Как говорилось выше, методология тестирования на устойчивость к взлому рассматривает объект сканирования как «чёрный» ящик, поэтому достоверность результатов сильно зависит от точности идентификации сервисов и реализующих эти сервисы приложений. Кроме того, поскольку объектом сканирования в данном случае были узлы сетевого периметра, задача идентификации сервисов и приложений осложнялась фильтрацией трафика, намеренной подменой баннеров и другими настройками, затрудняющими определение сервисов.

Таким образом, имело смысл оценить отдельно возможности сканеров в плане идентификации сервисов и приложений.

Идентификация открытых портов никак не оценивалась, просто результаты определения открытых портов были приведены к общему знаменателю. Если открытый порт был найден не всеми сканерами, он и связанные с ним уязвимости (если они были найдены другими сканерами) просто исключались из результатов. Вот, например, результат сбора информации по узлу host1.test (табл. 2).

Таблица 2. Результат сбора информации по узлу host1.test

Сбор информации		MP	IS	Retina	Nessus	SSS	NetClarity	Реально
Операционная система		Windows 2003	не опр	не опр	AIX 5.2, Catalist OS 6.3, SCO OpenServer 5.0.7	не опр	не опр	**Windows 2003**
Открытые порты, сервисы, приложения	TCP:21	FTP	FTP	FTP	FTP, Gene6 FTP Server	FTP	FTP	**Gene6 FTP Server v.3.6.0**
	TCP:25	SMTP	SMTP, Mdaemon	SMTP	SMTP	SMTP	SMTP	
	TCP:110	POP3, Mdaemon	POP3, Mdaemon	POP3	POP3	POP3	POP3	**POP3, Mdaemon 9.6.5**
	TCP:1000	HTTP, Web service for Mdaemon	1	HTTP	HTTP, Web service for Mdaemon	HTTP, Wdaemon 3.0	0	**HTTP, Web service for Mdaemon**
	TCP:1723	PPTP, Microsoft	PPTP	PPTP	PPTP, Microsoft	1	PPTP	**PPTP, Microsoft**
	TCP:3000	HTTP, Web service for Mdaemon	1	HTTP	HTTP, Web service for Mdaemon	HTTP, Wdaemon 3.0	0	**Mdaemon/ WorldClient**
	TCP:3389	MsRDP	1	MsRDP	MsRDP	RDP	RDP	**RDP**
		11	**6**	**7**	**11**	**8**	**5**	

На этом узле было найдено 7 открытых портов TCP. При этом все 7 портов были найдены каждым из сканеров.[5] Если сканер смог идентифицировать сервис, в соответствующей ячейке записано название сервиса. Если идентифицировано приложение – его название указано через

[5] Интерфейс сканера NetClarity не позволяет задавать перечень портов для сканирования, поэтому его результаты не приводились «к общему знаменателю». Вряд ли стоит считать это «оправданием» для него.

запятую после названия сервиса. Если сканер не смог идентифицировать сервис, то в ячейку заносится просто «единичка».

Например, 21-й порт используется сервисом FTP, и все сканеры это определили. Сканер Nessus смог идентифицировать приложение – Gene6 FTP Server. Соответственно, в каждой ячейке данной строки указано название сервиса – FTP, а в ячейку, соответствующую сканеру Nessus, внесено также название приложения. Правильно идентифицированный сервис оценивался в 1 балл, правильно идентифицированное приложение – ещё 1 балл. Если сканер ошибся, то вычитался 1 балл.

Например, в данном случае сервис SMTP (порт 25) правильно идентифицировали все сканеры (это +1 балл). Сканер Internet Scanner идентифицировал приложение (MDaemon). Это ещё +1 балл.

Практически аналогичная ситуация с сервисом POP3.

Далее следует порт 1000 – это Web-сервис для MDaemon. Сканер Internet Scanner определил, что порт открыт, но не смог идентифицировать ни сервис, ни приложение – в соответствующем поле стоит просто «единичка» (при этом баллы не начисляются). Сканер NetClarity не определил, что данный порт открыт – в соответствующем поле стоит «ноль».

В итоге, за определение сервисов и приложений сканеры MaxPatrol и Nessus получают по 11 баллов, Shadow Security Scanner – 8 баллов, Internet Scanner – 6 и т.д.

В таблице 3 приведены соответствующие значения.

Таблица 3. Числовые показатели идентификации сервисов и приложений

Сбор информации		**MP**	**IS**	**Retina**	**Nessus**	**SSS**	**NetClarity**	**Реально**
Операционная система		Windows 2003	не опр	не опр	AIX 5.2, Catalist OS 6.3, SCO OpenServer 5.0.7	не опр	не опр	**Windows 2003**
Открытые порты, сервисы, приложения	TCP:21	1	1	1	2	1	1	**Gene6 FTP Server v.3.6.0**
	TCP:25	1	2	1	1	1	1	
	TCP:110	2	2	1	1	1	1	**POP3, Mdaemon 9.6.5**
	TCP:1000	2	0	1	2	2	0	**HTTP, Web service for Mdaemon**
	TCP:1723	2	1	1	2	0	1	**PPTP, Microsoft**
	TCP:3000	2	0	1	2	2	0	**Mdaemon/ WorldClient**
	TCP:3389	1	0	1	1	1	1	**RDP**
		11	**6**	**7**	**11**	**8**	**5**	

8.2. Идентификация уязвимостей

После того как все найденные (всеми сканерами) уязвимости были занесены в таблицу, по каждой из них производилась проверка: существует ли данная уязвимость в действительности. По результатам проверки был заполнен столбец «реально». Далее были заполнены столбцы отдельно по каждому сканеру. Если сканер нашёл уязвимость и её наличие было подтверждено вручную (в столбце «реально» стоит единичка), то в соответствующей ячейке – единица. Если сканер нашёл уязвимость и её наличие НЕ подтверждено вручную (в столбце «реально» стоит ноль), то это «ложное срабатывание» (False Positive), оно обозначается единичкой на красном фоне.

Остальные ситуации – это пропуски (False Negatives). Пропуски могут быть по разным причинам:

- Сканер не выполняет такой проверки (проверка отсутствует в базе сканера)
- Ошибка реализации (проверка есть в базе, но сделана «небрежно», в некоторых случаях могут быть пропуски)
- Требуется аутентификация (для выполнения проверки сканеру необходимо подключение с использованием учётной записи)
- Другие причины

Выяснить причины пропусков – задача довольно трудоёмкая. В данном сравнении выявлялись только ситуации пропусков по причине отсутствия проверки в базе сканера.

Такие пропуски обозначены «нулём» на жёлтом фоне. Пропуски по другим причинам обозначены «нулём» на красном фоне. Таким образом, использовалась следующая система обозначений.

1	Уязвимость найдена правильно
1	Ложное срабатывание (false positive)
0	Уязвимость не найдена, и её действительно нет
0	Пропуск уязвимости (false negative) по причине отсутствия проверки в базе
0	Пропуск уязвимости (false negative) по другим причинам

Далее в качестве примера, иллюстрирующего использование приведённых обозначений, опять приведён узел host1.test (табл. 4).

Таблица 4. Результаты сканирования узла host1.test

Узел 80.69.179.21

Сбор информации		**MP**	**IS**	**Retina**	**Nessus**	**SSS**	**NetClarity**	**реально**
Операционная система		Windows 2003	не опр	не опр	AIX 5.2, CatalystOS 6.3, SCO OpenServer 5.0.7	не опр	не опр	Windows 2003
Открытые порты, сервисы, приложения	**TCP:21**	FTP	FTP	FTP	FTP,Gene6 FTP Server	FTP	FTP	Gene6 FTP Server v3.6.0
	TCP:25	SMTP	SMTP, Mdaemon	SMTP	SMTP	SMTP	SMTP	
	TCP:110	POP3, Mdaemon	POP3, Mdaemon	POP3	POP3	POP3	POP3	Pop3, Mdaemon, 9.6.5
	TCP:1000	HTTP, Web service for Mdaemon	1	HTTP	HTTP, Web service for Mdaemon	HTTP, Wdaemon 3.0	0	HTTP, Web service for Mdaemon
	TCP:1723	PPTP, Microsoft	PPTP	PPTP	PPTP, Microsoft	1	PPTP	PPTP, Microsoft
	TCP:3000	HTTP, Web service for Mdaemon	1	HTTP	HTTP, Web service for Mdaemon	HTTP, Wdaemon 3.0	0	MDaemon/ WorldClient
	TCP:3389	MsRDP	1	MsRDP	MsRDP	RDP	RDP	RDP
		11	**6**	**7**	**11**	**8**	**5**	
Уязвимости		**MP**	**IS**	**Retina**	**Nessus**	**SSS**	**NetClarity**	**реально**
Some POP3 server banners providing information to attacker		**0**	**0**	**0**	**0**	**0**	**1**	**1**
FTP: Переполнение буфера	**CVE-2006-2172 BID (17810)**	**0**	**0**	**0**	**1**	**0**	**0**	**1**
FTP:Найден логин (guest/guest)		**1**	**1**	**0**	**0**	**0**	**0**	**1**
SMTP:EXPN	**CVE-1999-0531**	**1**	**0**	**0**	**0**	**0**	**0**	**0**
SMTP daemon supports EHLO	**CVE-1999-0531**	**0**	**1**	**0**	**0**	**0**	**0**	**1**
HTTP: найдены директории		**0**	**0**	**0**	**1**	**0**	**0**	**1**
HTTP:Незащищенная передача данных		**1**	**0**	**0**	**1**	**0**	**0**	**1**
HTTP:Файл robots.txt		**1**	**0**	**0**	**1**	**0**	**0**	**1**
HTTP:Unknown CGIs arguments torture (подозрение на XSS)		**0**	**0**	**0**	**1**	**0**	**0**	**1**
MsRDP:Удалённое управление		**1**	**0**	**1**	**1**	**0**	**0**	**1**
MsRDP:Несоответствие стандарту FIPS-140		**0**	**0**	**0**	**1**	**0**	**0**	**1**
Всего найдено		**5**	**2**	**1**	**7**	**0**	**1**	**10**
Из них ложных обнаружений (False Positives)		**1**	**0**	**0**	**0**	**0**	**0**	
Пропусков (False Negatives)		**6**	**8**	**9**	**3**	**10**	**9**	
Из них по причине отсутствия в базе		**4**	**7**	**9**	**3**	**9**	**9**	

Всего на данном узле всеми сканерами было найдено 13 уязвимостей, затем подтверждено ручной проверкой 10 уязвимостей. При этом, например, сканер MaxPatrol нашёл 5 уязвимостей, и один раз он «ошибся» (в таблице ложные срабатывания обозначены «единичкой» на красном фоне). Следовательно, сканером MaxPatrol было пропущено 6 уязвимостей из 10. Проанализируем причины ложных срабатываний и пропусков.

Ложное срабатывание произошло в ходе определения поддержки команды EXPN. Вот как выглядит результат ручной проверки (рис. 24):

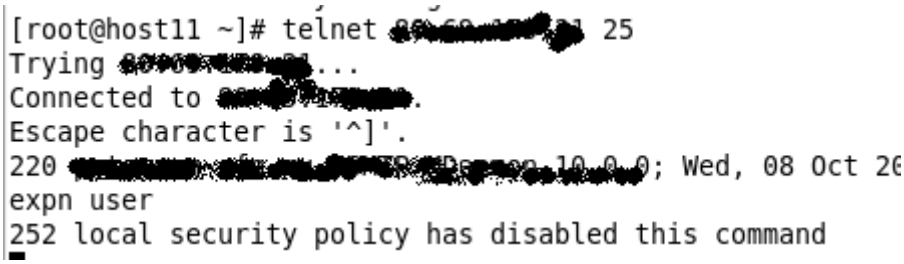

Рис. 24. «Ручная проверка» поддержки команды EXPN

Вполне возможно, что MaxPatrol не совсем корректно обрабатывает код ответа 252, сообщающий о запрете данной команды локальной политикой.

Теперь проанализируем причины пропусков. Четыре пропуска из шести были допущены по причине отсутствия проверок в базе сканера, а именно:

- Предоставление сервисом POP3 «лишней» информации
- Ошибка реализации (переполнение буфера) сервера FTP
- Поддержка команды EHLO
- Несоответствие стандарту FIPS

Эти проверки сканером MaxPatrol просто не выполняются (такие пропуски обозначены «нулём» на жёлтом фоне). Причины двух оставшихся пропусков (подозрение на XSS и каталоги на Web-сервере) – это уже ошибки реализации. Такие проверки сканер выполняет, но в данной ситуации соответствующих уязвимостей найдено не было (такие пропуски обозначены «нулём» на красном фоне).

Internet Scanner нашёл две уязвимости, ложных срабатываний при этом зафиксировано не было. Что касается пропусков, то их было 8, из них 7 – по причине отсутствия в базе соответствующих проверок. Интересно, что факт наличия на узле удалённого управления (RDP) не был определён, потому что для выполнения соответствующей проверки (RdpEnabled) требуются административные привилегии (рис. 25).

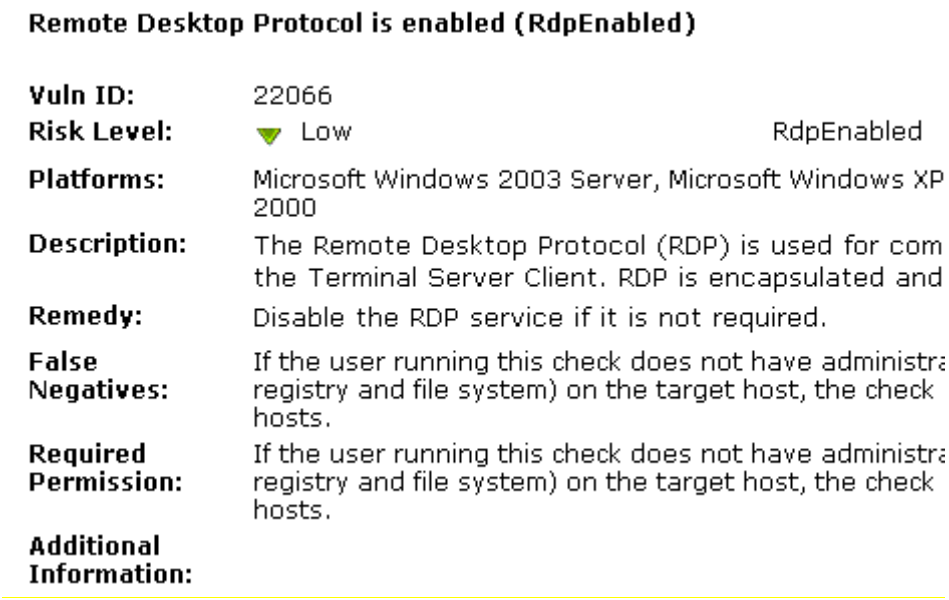

Рис. 25. Проверка «RdpEnabled» в сканере Internet Scanner

Сканер Retina нашёл только одну уязвимость из десяти возможных, остальные проверки отсутствуют в его базе, Nessus выявил 7 уязвимостей, пропустил 3 по причине отсутствия проверок в базе.

Shadow Security Scanner не нашёл ни одной уязвимости, 9 пропусков было допущено по причине отсутствия проверок в базе, один – из-за реализации самой проверки. Остановимся подробнее на пропуске данным сканером уязвимости сервера FTP Gene6. Такая проверка действительно имеется в сканере SSS (рис. 26).

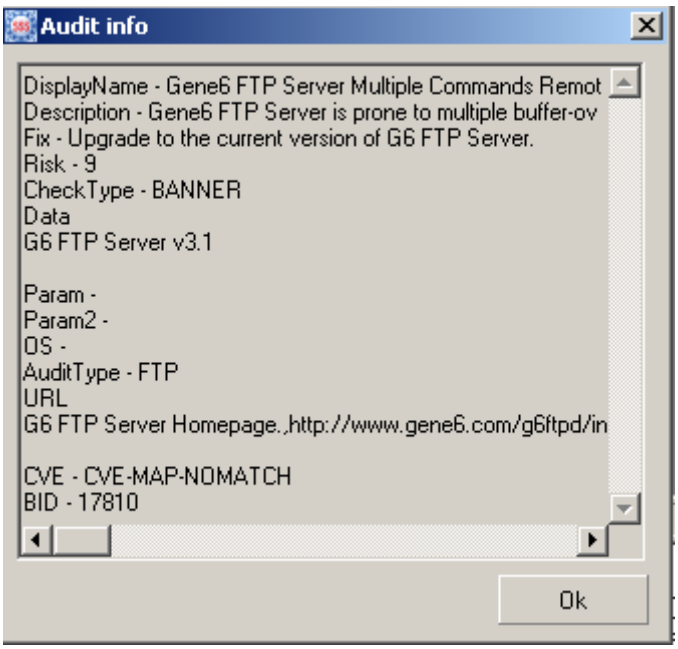

Рис. 26. Проверка «BID 17810» в сканере SSS

Из её описания можно понять, что проверка находит уязвимость, если версия сервера, извлечённая из баннера – 3.1. В данном случае «действительная» версия сервера FTP – 3.6.0. Разумеется, сканер SSS не нашёл данной уязвимости.

На рис. 27 представлено описание этой уязвимости в базе SecurityFocus. Действительно, там упоминается именно версия 3.1.

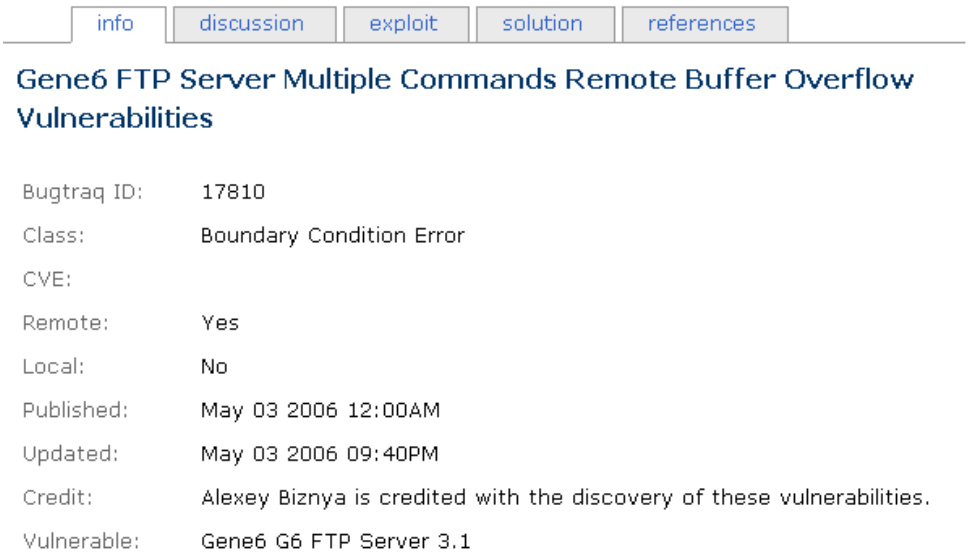

Рис. 27. Описание уязвимости «BID 17810»

С другой стороны, описание этой же уязвимости в базе XForce (рис. 28) отличается от приведённого выше.

Gene6 FTP Server MKD and XMKD command denial of service

gene6-ftp-mkd-xmkd-dos (26237) Low Risk

Description:

Gene6 FTP Server is vulnerable to a denial of service attack. A remote attacker could send a specially-crafted MKD or XMKD command to cause the server to crash.

Platforms Affected:

- Gene6, Gene6 FTP Server 3.7.0

Remedy:

Upgrade to the latest version of Gene6 FTP (3.8.0.34 or later), available from the Gene6 FTP Web site. See References.

Consequences:

Denial of Service

References:

- BugTraq Mailing List, 2006-05-03 9:41:08, Re: FTP Fuzzer at http://marc.theaimsgroup.com/?l=bugtraq&m=114667586518975&w=2.
- BugTraq Mailing List, Sat Nov 12 2005 - 17:42:01 CST, FTP Fuzzer at http://archives.neohapsis.com/archives/bugtraq/2006-05/0023.html. *(Timestamp appears to be wrong)*
- Gene6 FTP Server Web site, Gene6 FTP Server at http://gene6.com/.
- BID-17810: Gene6 FTP Server Multiple Commands Remote Buffer Overflow Vulnerabilities

Рис. 28. Описание уязвимости «BID 17810» в базе XForce

Здесь речь идёт уже о версии 3.7.0. То же самое, кстати, говорит и база уязвимостей osvdb (рис. 29).

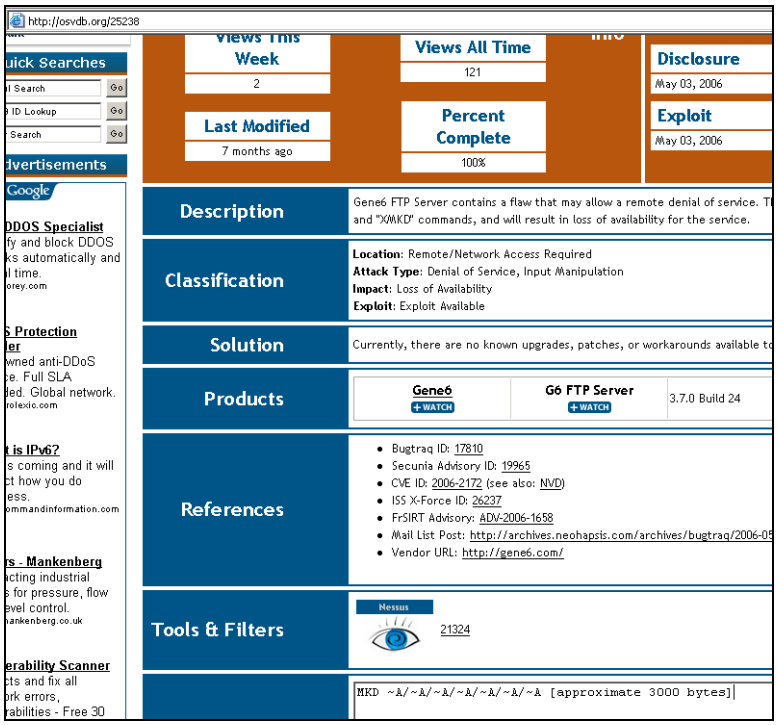

Рис. 29. Описание уязвимости «BID 17810» в базе osvdb

Поэтому в данной ситуации разумнее «поверить» сканеру Nessus, чем SSS. Ну и, наконец, в базе сканера NetClarity большинства проверок нет, поэтому его результат – одна найденная уязвимость.

8.3. Результаты и комментарии по отдельным узлам

Далее приведены таблицы с результатами по отдельным объектам сканирования, а также краткие пояснения к ним.

8.3.1. Узел 2 (host2.test)

Роль узла очевидна – сервер SSH, с идентификацией сервиса и приложения все сканеры справились одинаково (табл. 5).

Таблица 5. Результаты сканирования узла host2.test

Сбор информации			MP	IS	Retina	Nessus	SSS	NetClarity	реально
Операционная система			не опр	не опр	не опр	Linux Kernel 2.6	не опр	не опр	
Открытые порты, сервисы, приложения	TCP:22		SSH, OpenSSH_4.3	SSH, OpenSSH_4.3	SSH, OpenSSH_4.3	SSH, OpenSSH_4.3	SSH, OpenSSH_4.3	SSH, OpenSSH_4.3	SSH, OpenSSH_4.3
			2	2	2	2	2	2	
Уязвимости			**MP**	**IS**	**Retina**	**Nessus**	**SSS**	**NetClarity**	**реально**
SSH: Отказ в обслуживании	CVE-2006-5051	BID (20241)	1	0	0	0	1	0	1
SSH: ПОВЫШЕНИЕ ПРИВИЛЕГИЙ	CVE-2008-1657	BID (28531)	1	0	0	0	0	0	1
SSH: Разглашение информации	CVE-2008-1483	BID (28444)	1	0	0	0	0	0	1
SSH: Подмена данных в log-файле	CVE-2007-3102	BID (26097)	1	0	0	0	0	0	1
SSH: Разглашение информации	CVE-2006-5052	BID (20245)	1	0	0	0	1	0	1
SSH: Отказ в обслуживании	CVE-2006-4925		1	0	0	0	0	0	1
SSH: Доступ к именам пользователей	CVE-2007-2243	BID (23601)	1	0	0	0	0	0	1
SSH: Обход ограничений безопасности	CVE-2006-5794	BID (20956)	1	0	0	0	0	0	1
SSH: DoS-атака	CVE-2006-4924	BID (20216)	1	0	0	0	1	1	1
SSH: SSH Servers : OpenSSH SKey Remote Information Disclosure Vulnerability	CVE-2005-2798	BID (14729)	0	0	0	0	1	0	0
IcmpTstamp: ICMP timestamp requests	CAN-1999-0524		0	1	1	1	0	0	1
WinXP IP vulnerability	CAN-2005-0048	BID (13116)	0	0	0	0	0	1	0
The remote host does not discard TCP SYN packets which have the FIN flag set		BID (7487)	0	0	0	0	0	1	1
Traceroute: возможно определение сетевой топологии	CVE-1999-0525		0	1	1	1	0	1	1
Всего найдено			9	2	2	2	4	4	12
Из них ложных обнаружений			0	0	0	0	1	1	
Пропусков			3	10	10	10	9	9	
Из них по причине отсутствия в базе			3	10	9	1	3	9	
Вызванных необходимостью аутентификации			0	0	1	5	0	0	

А вот дальше, собственно, начинается сопоставление версии SSH и перечня известных уязвимостей (см. выше краткое описание методологии тестирования на устойчивость к взлому). Как видно из таблицы, наиболее корректно и качественно это сопоставление выполнено сканером MaxPatrol. Если проанализировать результаты остальных сканеров, то, получается, что Internet Scanner и Retina просто не выполняют большинства соответствующих проверок («нули» на жёлтом фоне). Пропуск уязвимости CVE-2008-1657 сканером Retina объясняется тем, что для выполнения этой проверки требуется аутентификация.

Сканер SSS нашёл три уязвимости в сервисе SSH, при этом было зафиксировано одно ложное срабатывание и несколько пропусков.

Причины пропусков уязвимостей сканером SSS две:

- «Небрежное» построение проверки (учёт ограниченного числа версий, аналогично рассмотренной выше проверке сервера FTP)
- Использование только одной базы уязвимостей (www.securityfocus.com/bid)

Вот, например, проверка CVE-2008-1483 в сканере SSS (рис. 30).

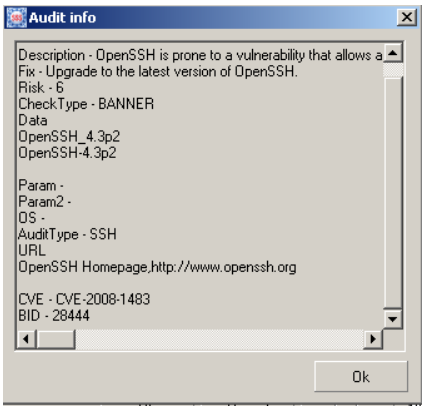

Рис. 30. Проверка CVE-2008-1483 в сканере SSS

Как и расммотренном выше случае с FTP, видно, что проверка учитывет только отдельные версии, хотя беглый просмотр каталога CVE уже говорит о том, что и другие версии также могут содержать данную уязвимость (рис. 31).

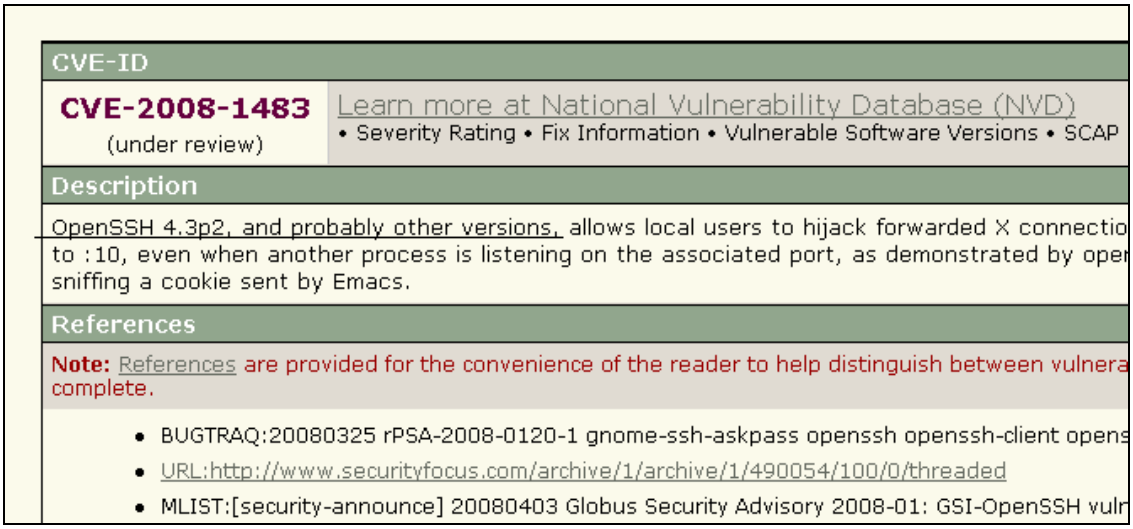

Рис. 31. Проверка CVE-2008-1483 в каталоге уязвимостей

Часть пропусков Nessus-а связана с тем, что для выполнения проверки требуется аутентификация (таких пропусков было зафиксировано 5), оставшиеся пропуски можно объяснить неполнотой самой проверки (как и в сканере SSS).

Таблица 6. Обнаружение двух «одинаковых» уязвимостей сканером MaxPatrol

Операционная система			
Открытые порты, сервисы, приложения	TCP:22		
Уязвимости			
SSH: Отказ в обслуживании	Средняя	CVE-2006-5051	BID (20
SSH: Выполнение произвольного кода		CVE-2006-5051, 5052	BID (20
SSH: ПОВЫШЕНИЕ ПРИВИЛЕГИЙ		CVE-2008-1657	BID (28
SSH: Разглашение информации		CVE-2008-1483	BID (28
SSH: Подмена данных в log-файле		CVE-2007-3102	BID (26
SSH: Разглашение информации		CVE-2006-5052	BID (20
SSH: Отказ в обслуживании		CVE-2006-4925	
SSH: Доступ к именам пользователей		CVE-2007-2243	BID (23

Следует ещё добавить, что MaxPatrol тоже был в данном случае не идеален. Из-за накладок, связанных с переходом на новую базу проверок, возникли «раздвоения». Например, в

следующем рабочем фрагменте таблицы (табл. 6) видно, что уязвимости CVE-2006-5051 и CVE-2006-5052 были найдены дважды.

8.3.2. Узел 5 (host5.test)

Это FreeBSD с рядом сервисов, в процессе идентификации которых сканеры столкнулись с некоторыми сложностями (табл. 7).

Таблица 7. Результаты сканирования узла host3.test

Сбор информации			MP	IS	Retina	Nessus	SSS	NetClarity	реально
Операционная система			не опр	FreeBSD	FreeBSD 5.2-CURRENT (Jan 2004) on X86	FreeBSD 5.3, FreeBSD 5.4, FreeBSD 5.5	не опр	не опр	FreeBSD
Открытые порты, сервисы, приложения	TCP:21		FTP	FTP	FTP	FTP	FTP	FTP	FTP
	TCP:22		SSH, OpenSSH_3.8.1 p1 FreeBSD	SSH, OpenSSH_3.8.1 p1 FreeBSD	SSH, OpenSSH_3.8.1 p1 FreeBSD	SSH, OpenSSH_3.8.1 p1 FreeBSD	SSH, OpenSSH_3.8.1 p1 FreeBSD	SSH, OpenSSH_3.8.1 p1 FreeBSD	SSH, OpenSSH_3.8.1 p1 FreeBSD
	TCP:53		DNS, BIND	DNS, BIND	DNS, BIND	DNS, BIND 9.3.4	DNS, BIND 9.3.4	DNS	DNS, BIND 9.3.4
	TCP:110		POP3, popa3d POP3 Server	POP3	POP3	POP3	POP3	POP3	POP3, popa3d POP3 Server
	TCP:443		SSH, OpenSSH Server engine	HTTPS	SSH, OpenSSH Server engine	SSH, OpenSSH Server engine	SSH, OpenSSH Server engine	1	SSH, OpenSSH Server engine
	TCP:2601		Telnet	1	1	BGPd, Quagga	1	0	BGPd, Quagga
	TCP:2604		Telnet	1	1	BGPd, Quagga	1	0	BGPd, Quagga
	TCP:3306		MySQL	MySQL	MySQL	MySQL	1	0	MySQL
	TCP:3310		1	1	1	clamd, Clam Antivirus	1	0	clamd, Clam Antivirus
	TCP:5252		Skype	1	1	FTP	1	0	NNTP
	UDP:53		DNS, BIND	DNS, BIND 9.3.4	1	DNS, BIND 9.3.4	1	0	DNS, BIND
			11	6	9	14	8	5	
Уязвимости			**MP**	**IS**	**Retina**	**Nessus**	**SSS**	**NetClarity**	**реально**
FTP: Анонимный FTP			1	1	1	1	1	1	1
FTP: Анонимный FTP на запись	CVE-1999-0497		1	0	1	1	1	0	1
FTP: файл .rhosts на сервере FTP			0	0	0	1	0	0	1
FTP: VisNetic and Titan FTP Server traversal			0	0	0	1	0	1	0
FTP: ST FTP traversal	CVE-2003-0392	BID (7674)	0	0	0	1	0	1	0
FTP: Generic FTP traversal			0	0	0	1	0	1	0
SSH: DoS-атака	CVE-2006-4924	BID (20216)	1	0	0	0	1	1	1
SSH: ПОВЫШЕНИЕ ПРИВИЛЕГИЙ	CVE-2008-1657	BID (28531)	1	0	0	0	1	0	1
SSH: OpenSSH GSSAPI Credential Disclosure Vulnerability	CVE-2005-2798	BID (14729)	1	0	0	0	1	0	0
SSH: OpenSSH-portable PAM Authentication Remote Information Disclosure Vulnerability	CAN-2003-0190	BID (11781)	0	0	0	0	1	0	1
SSH: Отказ в обслуживании	CVE-2006-5051	BID (20241)	1	0	0	0	1	0	1
SSH:Разглашение информации	CVE-2008-1483		1	0	0	0	0	0	1
SSH:Сканирование портов	CVE-2004-1653		1	0	0	0	0	0	1
SSH:Включение переадресации X11	CVE-2005-2797	BID (14727)	1	0	0	0	0	0	1
SSH:Разглашение информации	CVE-2006-5052		1	0	0	0	0	0	1
SSH:Отказ в обслуживании	CVE-2006-4925		1	0	0	0	0	0	1
SSH:Отказ в обслуживании	CVE-2006-0883	BID (16892)	1	0	0	0	0	0	1
SSH:Доступ к именам пользователей	CVE-2007-2243	BID (23601)	1	0	0	0	0	0	1
SSH:Обход ограничений безопасности	CVE-2006-5794	BID (20956)	1	0	0	0	0	0	1
SSH:Повышение привилегий	CVE-2006-0225	BID (16369)	1	0	0	0	0	0	1
SSH:Разглашение информации	CVE-2005-2666		1	0	0	0	0	0	1
DNS:Подмена DNS-данных	CVE-2008-1447		1	0	0	0	0	0	1
DNS:Отказ в обслуживании	CVE-2008-0122		1	0	1	0	0	0	1
DNS: отравление кэша	CVE-2007-2926	BID (25037)	1	0	1	1	1	1	1
DNS: отравление кэша	CVE-2008-1447	BID (30131)	1	0	1	0	0	0	1
DNS: bind-hostname-disclosure (18836)			0	1	0	0	0	1	0
IcmpTstamp: ICMP timestamp requests	CAN-1999-0524		0	1	1	1	0	0	1
Traceroute: возможно определение сетевой топологии	CVE-1999-0525		0	1	1	1	0	1	1
Всего найдено			20	4	7	9	8	8	23
Из них ложных обнаружений			1	1	0	3	0	4	
Пропусков			4	20	16	17	15	19	
Из них по причине отсутствия в базе			2	18	14	4	10	18	
Вызванных необходимостью аутентификации			0	2	0	6	0	0	

Прежде всего, сервис SSH в данном случае использует два порта: 22 и 443. Internet Scanner не справился с задачей идентификации SSH, использующего порт 443. Это произошло потому, что он не пытается выполнять идентификацию сервиса SSH, использующего порт, отличный от 22-го. Вторая сложность - пакет Quagga Routing Software Suite. Демоны Quagga имеют собственный оконечный интерфейс или VTY (Virtual TeletYpe). Это означает, что можно соединиться с демоном, используя протокол telnet. Лучше остальных с идентификацией данного программного обеспечения справился Nessus, сканер MaxPatrol ограничился только идентификацией сервиса.

Сервис NNTP был ошибочно идентифицирован обоими сканерами как Skype и FTP. Стоит ли говорить, что остальные сканеры вообще не справились с идентификацией указанных сервисов.

В ходе идентификации уязвимостей также возник ряд интересных моментов.

Результаты поиска уязвимостей в сервисе SSH, вобщем-то, аналогичны предыдущим узлам, за исключением проверки CVE-2005-2798. Это уязвимость, эксплуатация которой возможна только при включенной поддержке аутентификации gssapi. Поскольку в данном случае она выключена, то это не было зачтено как найденная уязвимость. Только сканер Nessus, выполняя данную проверку, выясняет, включена ли аутентификация GSSAPI. Очень интересный момент, во всяком случае, в пользу сканера Nessus.

8.3.3. Узел 4 (host4.test)

Это маршрутизатор CISCO, интересный с точки зрения сканирования узел (табл. 8).

Пожалуй, здесь стоит «похвалить» результаты сканеров MaxPatrol, Internet Scanner и Nessus. Но победа здесь, всё-таки, за MaxPatrol. Nessus «отличился» тем, что проверки в отношении CISCO построены на основе базы securityfocus, а в ней замечены явные расхождения с CVE и уж тем более - с бюллетенями Cisco. Internet Scanner, в целом, выполнил сканирование довольно качественно, но с пропусками. Кстати, здесь замечена довольно нетипичная причина пропуска уязвимости CVE-2004-1060. Эта проверка выполняется путём явной атаки, причём есть вероятность выведения узла из строя (рис. 32). По условиям сравнения такие проверки были отключены.

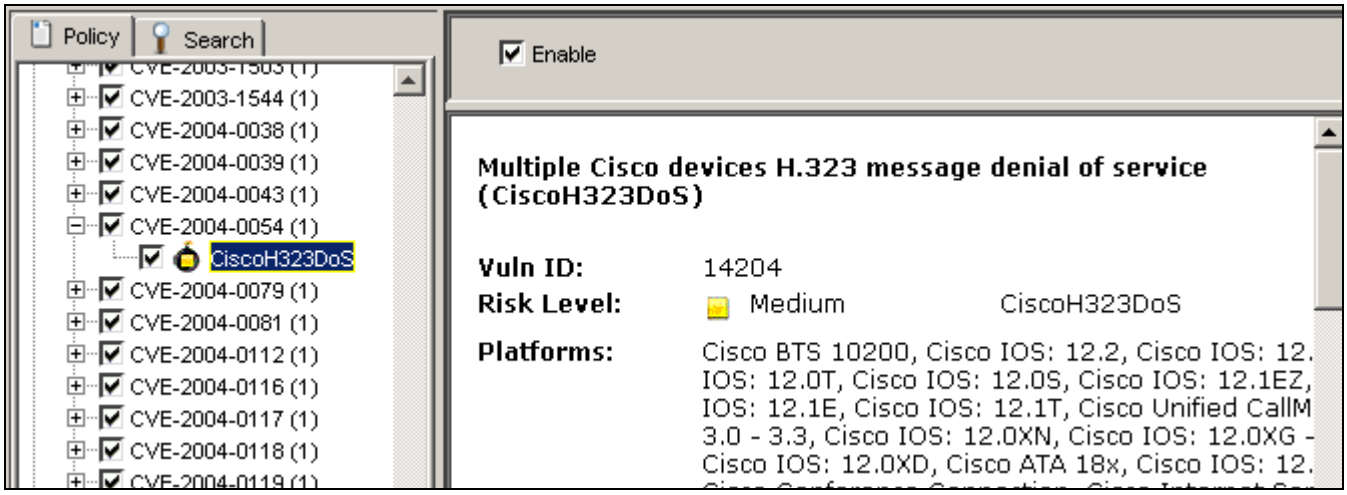

Рис. 32. Проверка CVE-2004-0054 в Internet Scanner

Таблица 8. Результаты сканирования узла host4.test

Сбор информации			MP	IS	Retina	Nessus	SSS	NetClarity	реально
Операционная система			Cisco C1700-K9O3SV3Y7-M, IOS 12.2(15)T8	Cisco IOS C1700-K9O3SV3Y7-M	Cisco 2960G switch (IOS 12.2)	CISCO IOS 12.2(15)T8	не опр	0	
Открытые порты, сервисы, приложения	TCP:23		Telnet	Telnet	Telnet	Telnet	Telnet	Telnet	Telnet
	UDP:161		SNMP	SNMP	SNMP	SNMP	SNMP	SNMP	SNMP
			2	2	2	2	2	2	
Уязвимости			**MP**	**IS**	**Retina**	**Nessus**	**SSS**	**NetClarity**	**реально**
Telnet:Незащищенный протокол	CVE-1999-0619		1	0	1	1	0	1	1
SNMP:Утечка информации	CVE-2007-4285		1	0	0	0	0	0	1
SNMP:Отказ в обслуживании (cisco-ios-ipv6-header-dos)	CVE-2007-4286		1	0	0	0	0	0	1
SNMP:Отказ в обслуживании	CVE-2007-4291 CVE-2007-4292 CVE-2007-4293 CVE-2007-4294 CVE-2007-4295		1	0	0	0	0	0	1
SNMP:Отказ в обслуживании	CVE-2007-2813		1	0	0	0	0	0	1
SNMP:Разглашение информации	CVE-2007-2586 CVE-2007-2587		1	0	0	0	0	0	1
SNMP:Переполнение буфера	CVE-2005-3481		1	0	0	0	0	0	0
SNMP:Несанкционированный доступ	CVE-2005-2105		1	0	0	0	0	0	1
SNMP:Неавторизованный доступ	CVE-2005-1057 CVE-2005-1058		1	0	0	1	0	1	1
SNMP:Отказ в обслуживании	CVE-2004-0054		1	0	0	0	0	0	1
SNMP:Отказ в обслуживании	CVE-2003-1109		1	0	0	0	0	0	1
SNMP:Учетная запись (public)	CVE-1999-0517		1	1	1	1	1	1	1
SNMP:Отказ в обслуживании	CVE-2006-3894		1	0	0	0	0	0	1
SNMP:Отказ в обслуживании	CVE-2006-0340		1	0	0	1	0	0	1
SNMP:Отказ в обслуживании	CVE-2004-1060		1	0	0	0	0	0	1
SNMP:Отказ в обслуживании	CVE-2005-1020 CVE-2005-1021		1	0	0	0	0	0	1
SNMP:Перезагрузка устройства	CVE-2005-0186		1	0	0	0	0	0	1
SNMP:Отказ в обслуживании	CVE-2004-0714		1	0	0	0	0	0	0
SNMP:Отказ в обслуживании	CVE-2002-1024		1	0	0	0	0	0	0
SNMP:Утечка информации	CVE-2002-0339		1	0	0	0	0	0	0
SNMP:Перезагрузка устройства	CVE-2007-0199		1	0	0	0	0	0	1
SNMP:Отказ в обслуживании	CVE-2005-2451		1	0	0	0	0	0	1
SNMP:Отказ в обслуживании			1	0	0	0	0	0	1
SNMP:Отказ в обслуживании			1	0	0	0	0	0	1
SNMP:SNMPv1Discovery: SNMP version 1 detected	CVE-1999-0615 CVE-2002-0013		0	1	1	0	0	0	1
SNMP:SNMPv2Discovery: SNMP version 2 detected	CVE-1999-0615		0	1	0	0	0	0	1
CiscoIosAccountBruteforce: Cisco IOS could allow an attacker to determine valid accounts (12745)	CVE-2003-0512	8292	0	1	0	0	0	0	0
CiscoIosIpv6Type0Dos: Cisco IOS IPv6 Type 0 routing header denial of service (31715)	CVE-2007-0481	22210	1	1	1	0	0	0	1
CiscoIosBgpPacketDos: Cisco IOS BGP packet denial of service and gain full control (19074)	CVE-2005-0196		0	1	0	0	0	0	1
CiscoIosIpv6Dos: Cisco IOS IPv6 denial of service and gain full control (19072)	CVE-2005-0195	12368	1	1	0	0	0	0	1
CiscoIpOptionCodeExecution: Cisco IOS and IOS XR IP option code execution (31725)	CVE-2007-0480	22211	1	1	1	1	0	0	1
CiscoTcpIpv4Dos: Cisco IOS TCP listener IPv4 memory leak denial of service	CVE-2007-0479	22208	1	1	0	1	0	0	1
Perimeter Router: SNMP perimeter router identification			0	1	0	1	0	0	1
snmp: SNMP can reveal possibly sensitive information about hosts	CVE-1999-0615		0	1	0	1	0	1	1
SNMPShowInterface: SNMP agents reveal information about network interfaces			0	1	0	1	0	1	1
SNMPShowRMON: SNMP RMON agents can monitor network and application activity			0	1	0	1	0	1	1
SNMPShowRoutes: SNMP agents reveal information about network routing			0	1	0	1	0	1	1
SnmpSysdescr: SNMP SysDescr variable can be returned from remote system			0	1	0	1	0	1	1
Cisco IOS Telnet Service Remote Denial of Service Vulnerability	CAN-2004-1464	11060	0	0	1	0	0	0	0
Traceroute: возможно определение сетевой топологии	CVE-1999-0525		0	1	1	1	0	1	1
IcmpTstamp: ICMP timestamp requests	CAN-1999-0524		0	1	1	1	0	0	1
CISCO : Cisco IOS HTTP Service HTML Injection Vulnerability	CVE-2005-3921	15602	0	0	0	0	1	0	1
CISCO : Cisco IOS Multiple Unspecified EIGRP Vulnerabilities		14877	0	0	0	0	1	0	1
Cisco IOS ICMP redirect routing vulnerability	CVE-2003-1398	6823	0	0	1	0	0	0	0
Cisco IOS AAA RADIUS Authentication Bypass Vulnerability		14092	0	0	0	1	0	0	1
CISCO: IOS has flaw in its telephony service		12307	0	0	0	1	0	0	1
Cisco IOS TCLSH AAA Command Authorization Bypass Vulnerability	CVE-2006-0485 CVE-2006-0486	16383	0	0	0	1	0	0	1
Всего найдено			28	17	9	17	3	9	40
Из них ложных обнаружений			4	1	2	0	0	0	
Пропусков			16	24	33	23	37	31	
Из них по причине отсутствия в базе			16	23	25	19	33	31	
Вызванных необходимостью аутентификации			0	1	5	1	0	0	

8.3.4. Узел 5 (host5.test)

Это гибридный узел (табл. 9), поддерживающий сразу несколько сервисов (DNS, HTTP, FTP, SSH).

Таблица 9. Результаты сканирования узла host5.test

Сбор информации			**MP**	**IS**	**Retina**	**Nessus**	**SSS**	**NetClarity**	**реально**
Операционная система			Unix	UNIX	Buffalo TerraStation	не опр	не опр	0	
Открытые порты, сервисы, приложения	**TCP:21**		FTP	FTP	FTP	FTP	FTP	FTP	FTP, Pure-FTPd
	TCP:53		DNS, ISC BIND	DNS, ISC BIND	DNS, ISC BIND	DNS, ISC BIND	DNS	DNS, ISC BIND 9.3.0	DNS, ISC BIND 9.3.0
	TCP:80		HTTP, Nginx HTTP Server	HTTP	HTTP, Nginx HTTP Server	HTTP, nginx	HTTP, nginx	HTTP	HTTP, Nginx HTTP Server
	TCP:35752		SSH, OpenSSH_4.6	1	1	SSH, OpenSSH_4.6	1	0	SSH, OpenSSH_4.6
	UDP:53		DNS, ISC BIND	DNS, ISC BIND	DNS, ISC BIND	DNS, ISC BIND	0	0	DNS, ISC BIND
			7	**4**	**5**	**7**	**4**	**3**	
Уязвимости			**MP**	**IS**	**Retina**	**Nessus**	**SSS**	**NetClarity**	**реально**
HTTP: Найдены адреса Email на web-сайте			**1**	**0**	**0**	**1**	**1**	**0**	**1**
HTTP:Ошибка в скрипте			**1**	**0**	**0**	**0**	**0**	**0**	**1**
HTTP:Межсайтовый скриптинг (7 уязвимых параметров)			**1**	**0**	**0**	**0**	**0**	**0**	**1**
HTTP:Файл robots.txt			**1**	**0**	**0**	**1**	**0**	**0**	**1**
SSH:Повышение привилегий	**CVE-2008-1657**		**1**	**0**	**0**	**0**	**0**	**0**	**1**
SSH:Разглашение информации	**CVE-2008-1483**		**1**	**0**	**0**	**0**	**0**	**0**	**1**
SSH:Доступ к именам пользователей	**CVE-2007-2243**		**1**	**0**	**0**	**0**	**0**	**0**	**1**
DNS: ISC BIND DNSSEC Validation Multiple RRsets Denial of Service	**CVE-2007-0494**	**BID (22231)**	**0**	**0**	**0**	**0**	**0**	**1**	**0**
HTTP:Plain Text Authentication Forms			**0**	**0**	**0**	**1**	**0**	**0**	**1**
IcmpTstamp: ICMP timestamp requests	**CAN-1999-0524**		**0**	**1**	**1**	**1**	**0**	**0**	**1**
Traceroute: возможно определение сетевой топологии	**CVE-1999-0525**		**0**	**1**	**1**	**1**	**0**	**1**	**1**
WinXP IP vulnerability	**CAN-2005-0048**	**BID (736)**	**0**	**0**	**0**	**0**	**0**	**1**	**0**
Всего найдено			**7**	**2**	**2**	**5**	**1**	**3**	**10**
Из них ложных обнаружений			**0**	**0**	**0**	**0**	**0**	**2**	
Пропусков			**3**	**8**	**8**	**5**	**9**	**9**	
Из них по причине отсутствия в базе			**3**	**8**	**7**	**2**	**6**	**9**	
Вызванных необходимостью аутентификации			**0**	**0**	**0**	**0**	**0**	**0**	

На этом узле для сервиса SSH используется нестандартный порт (35752). Правильно идентифицировать сервис удалось только сканерам MaxPatrol и Nessus. Как следствие, MaxPatrol правильно идентифицировал 3 уязвимости в сервисе SSH. А вот сканер SSS из-за того, что не идентифицировал данный сервис, пропустил эти уязвимости, хотя соответсвующие проверки имеются в его базе. Это ещё раз подтверждает тот факт, что для данной задачи крайне необходима качественная идентификация сервисов и приложений.

9. ПОДВЕДЕНИЕ ИТОГОВ

Аналогичным образом были посчитаны результаты по остальным узлам. После подсчёта итогов получилась следующая таблица (табл. 10).

Таблица 10. Итоговые результаты по всем объектам сканирования

Показатель	MaxPatrol	Internet Scanner	Retina	Nessus	Shadow Security Scanner	NetClarity Auditor
Идентификация сервисов и приложений, баллы	**108**	66	80	98	79	54
Найдено уязвимостей, всего	**163**	51	38	81	69	57
Из них ложных срабатываний (false positives)	8	**3**	4	7	36	14
Найдено правильно (из 225 возможных)	**155**	48	34	74	33	43
Пропуски (false negatives)	**70**	177	191	151	192	182
Из них по причине отсутствия в базе	63	170	165	**59**	150	179
Из них вызванные необходимостью аутентификации	**0**	6	16	36	**0**	**0**
По другим причинам	7	**1**	10	56	42	3

9.1. Идентификация сервисов и приложений

По результатам определения сервисов и приложений баллы были просто просуммированы, при этом за ошибочное определение сервиса или приложения вычитался один балл (рис. 33).

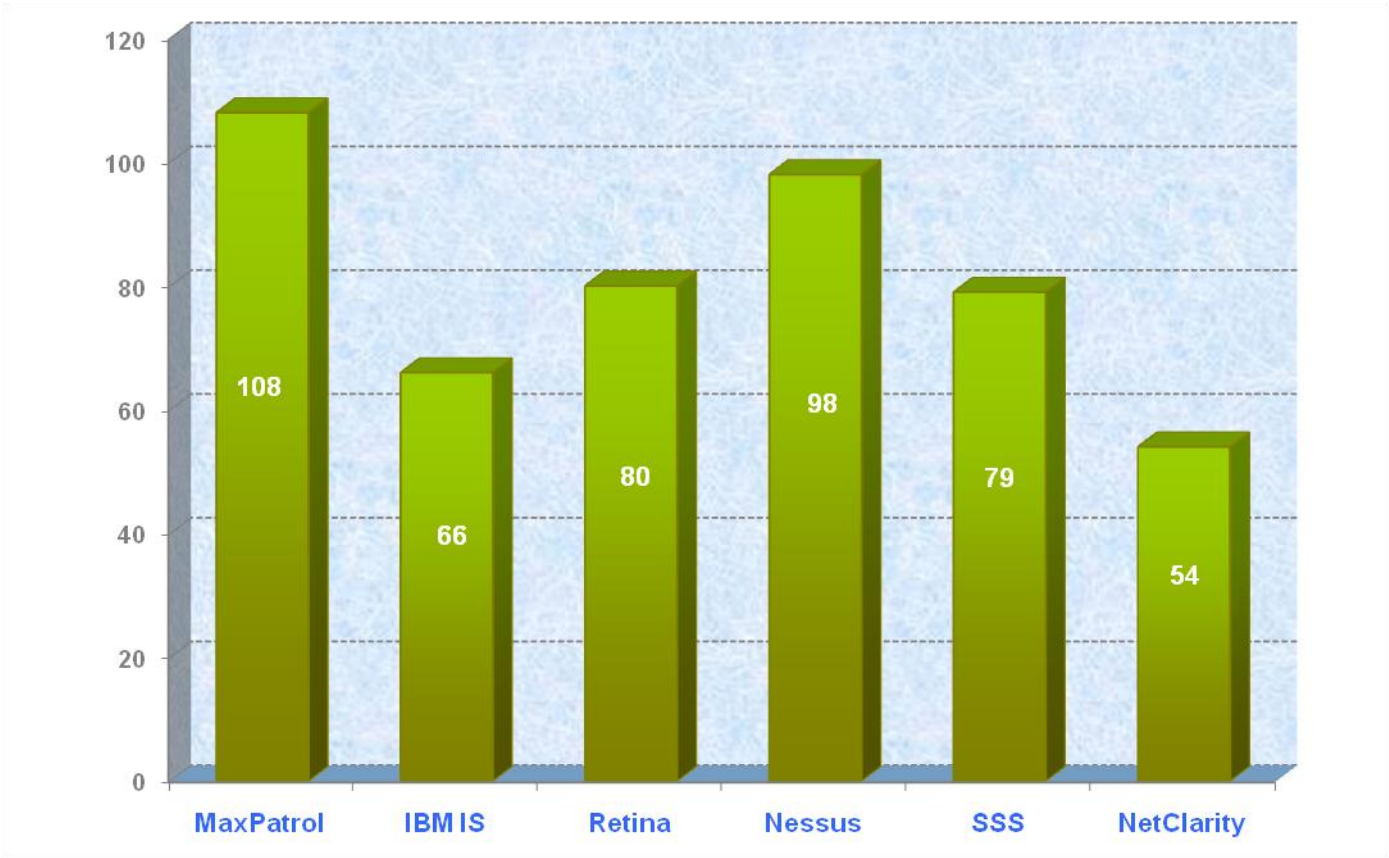

Рис. 33. Результаты идентификации сервисов и приложений

Наибольшее количество баллов (108) набрал сканер MaxPatrol, чуть меньше (98) – сканер Nessus. Действительно, в этих двух сканерах процедура идентификации сервисов и приложений реализована очень качественно. Данный результат можно назвать вполне ожидаемым.

Далее идут Retina (80 баллов) и Shadow Security Scanner (79 баллов), они «не справились» с некоторыми трудными случаями идентификации сервисов и приложений. Например, они оба «не справились» с идентификацией сервиса SSH, использующего порт 220 (рис. 34-35).

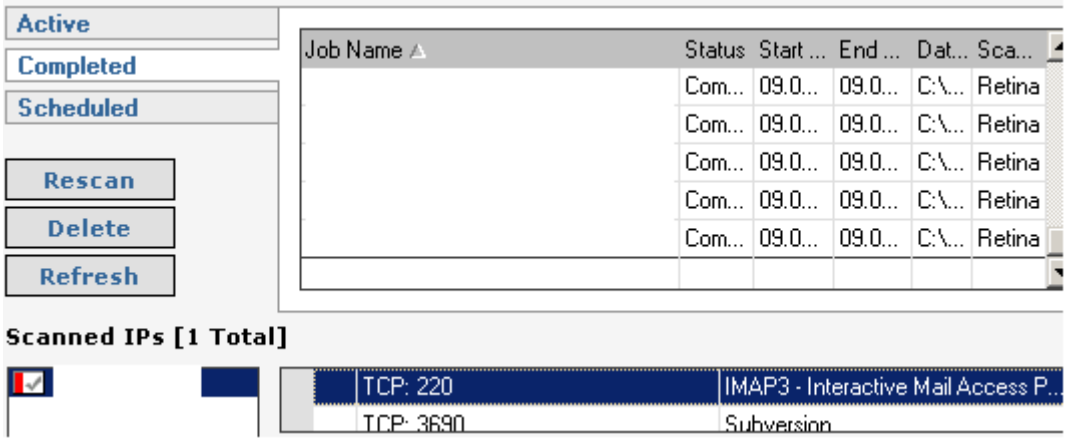

Рис. 34. Ошибочное определение сервиса SSH сканером Retina

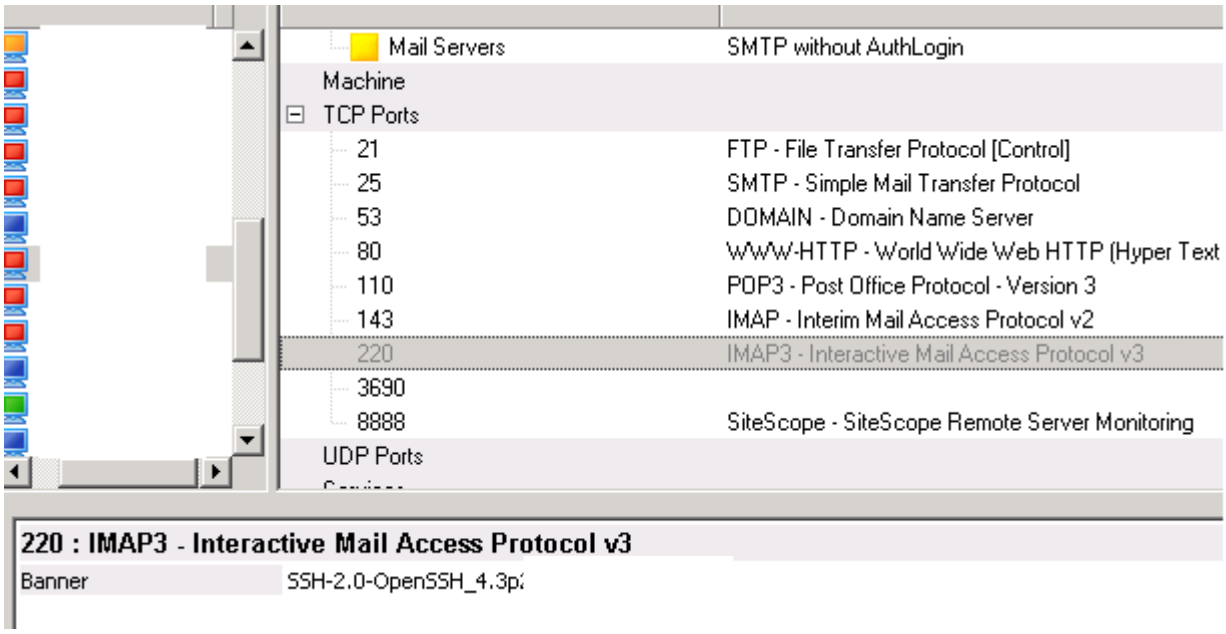

Рис. 35. Ошибочное определение сервиса SSH сканером в SSS

Следующий результат – у сканеров Internet Scanner и NetClarity. Здесь можно упомянуть, что, например, Internet Scanner ориентируется на использование стандартных портов для приложений, этим во многом и объясняется его невысокий результат. Наконец, наихудшие показатели у сканера NetClarity. Хотя он неплохо справляется с идентификацией сервисов (всё-таки он основан на ядре Nessus 2.x), его общий низкий результат можно объяснить тем, что он идентифицировал не все открытые порты.

9.2. Идентификация уязвимостей

На рис. 36 представлено общее число найденных всеми сканерами уязвимостей и число ложных срабатываний. Наибольшее число уязвимостей было найдено сканером MaxPatrol. Вторым (правда, уже со значительным отрывом) опять оказался Nessus.

Лидером по количеству ложных срабатываний оказался сканер Shadow Security Scanner. В принципе, это объяснимо, выше были приведены примеры ошибок, связанные как раз с его проверками.

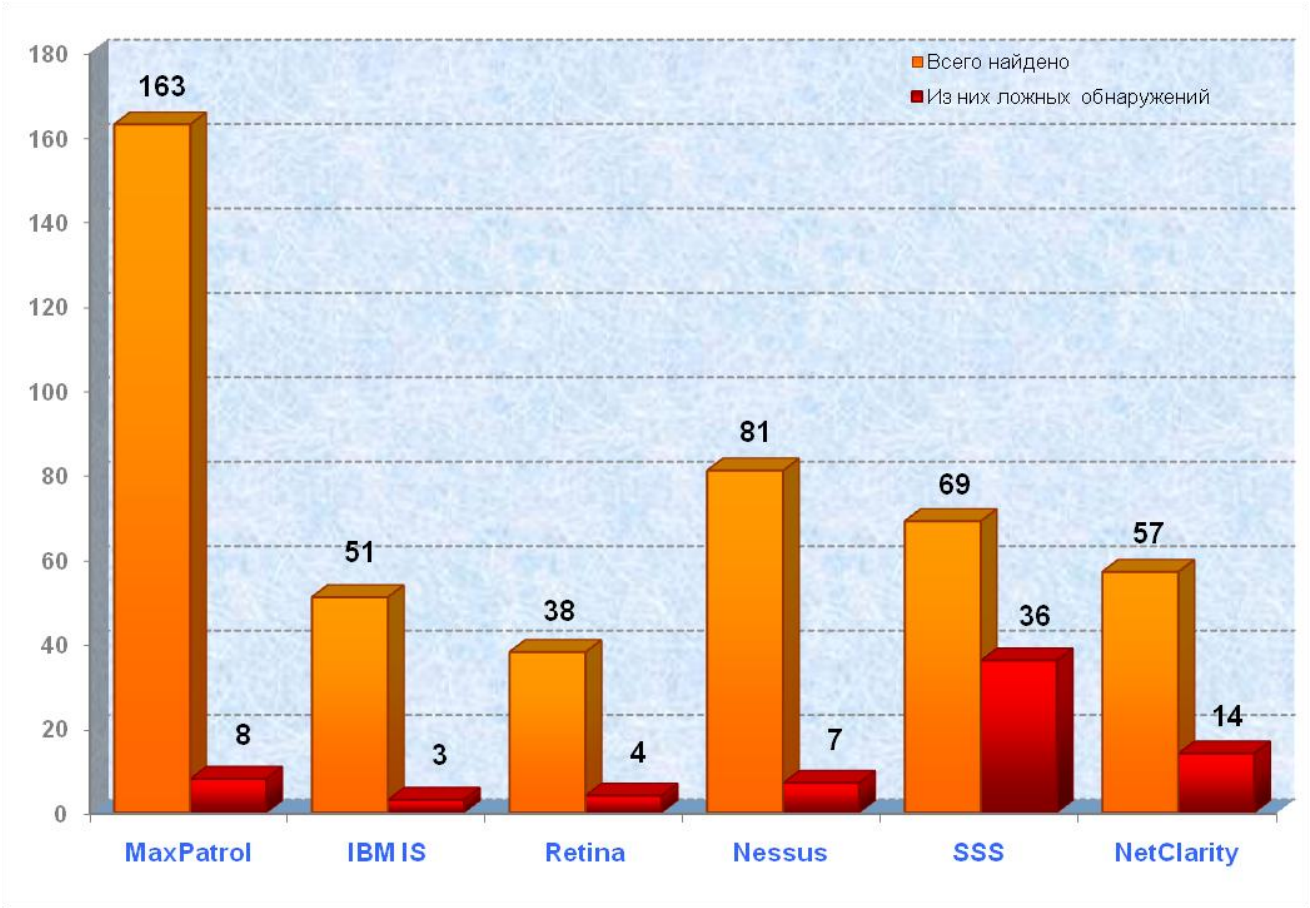

Рис. 36. Найденные уязвимости и ложные срабатывания

Всего на всех 16 узлах всеми сканерами было найдено (и впоследствии подверждено ручной проверкой) 225 уязвимостей. Результаты распределились так, как на рис. 37. Наибольшее число уязвимостей – 155 из 225 возможных – было выявлено сканером MaxPatrol. Вторым оказался сканер Nessus (его результат практически в два раза хуже). Следующим идёт сканер Internet Scanner, затем NetClarity.

В ходе сравнения были проанализированы причины пропусков уязвимостей и были отделены те, которые были сделаны по причине отсутствия проверок в базе. На следующей диаграмме (рис. 38) представлены причины пропусков уязвимостей сканерами.

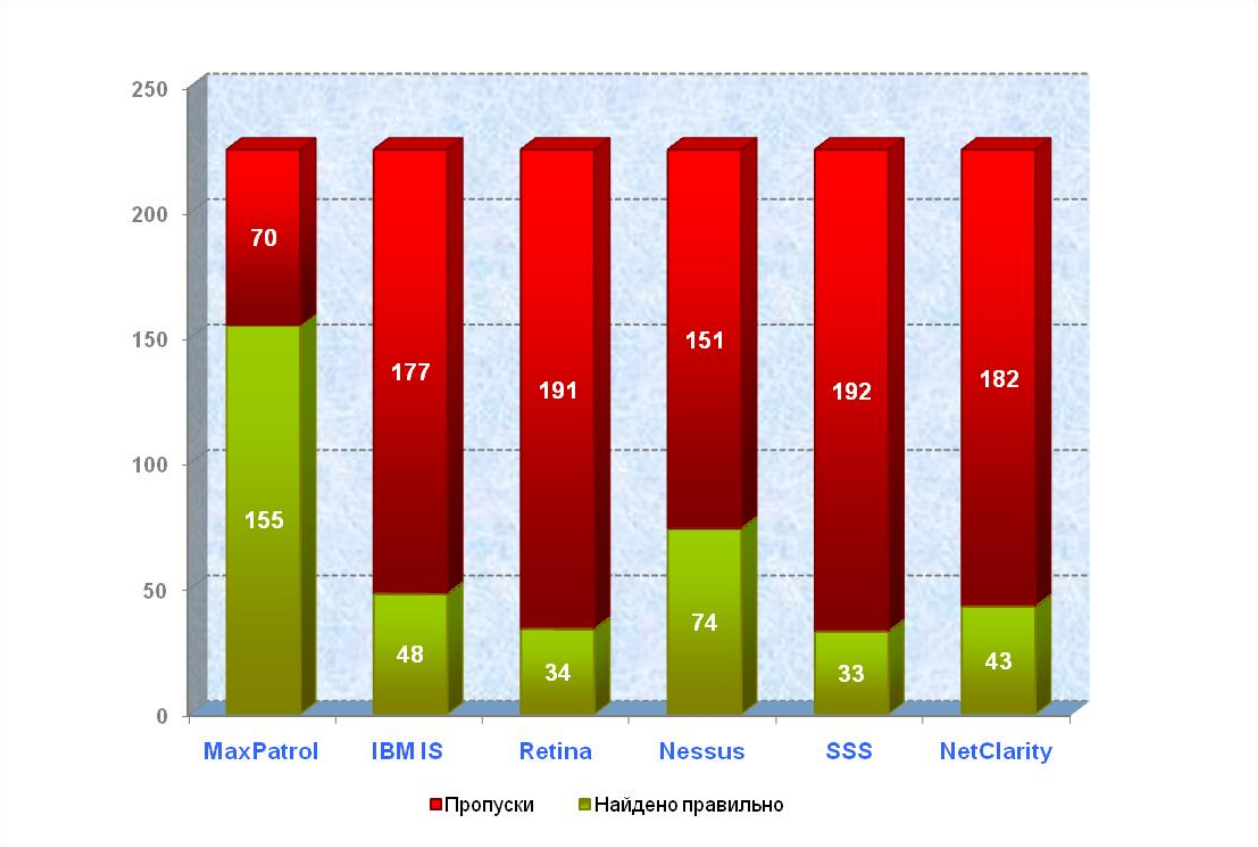

Рис. 37. Найденные уязвимости и пропуски

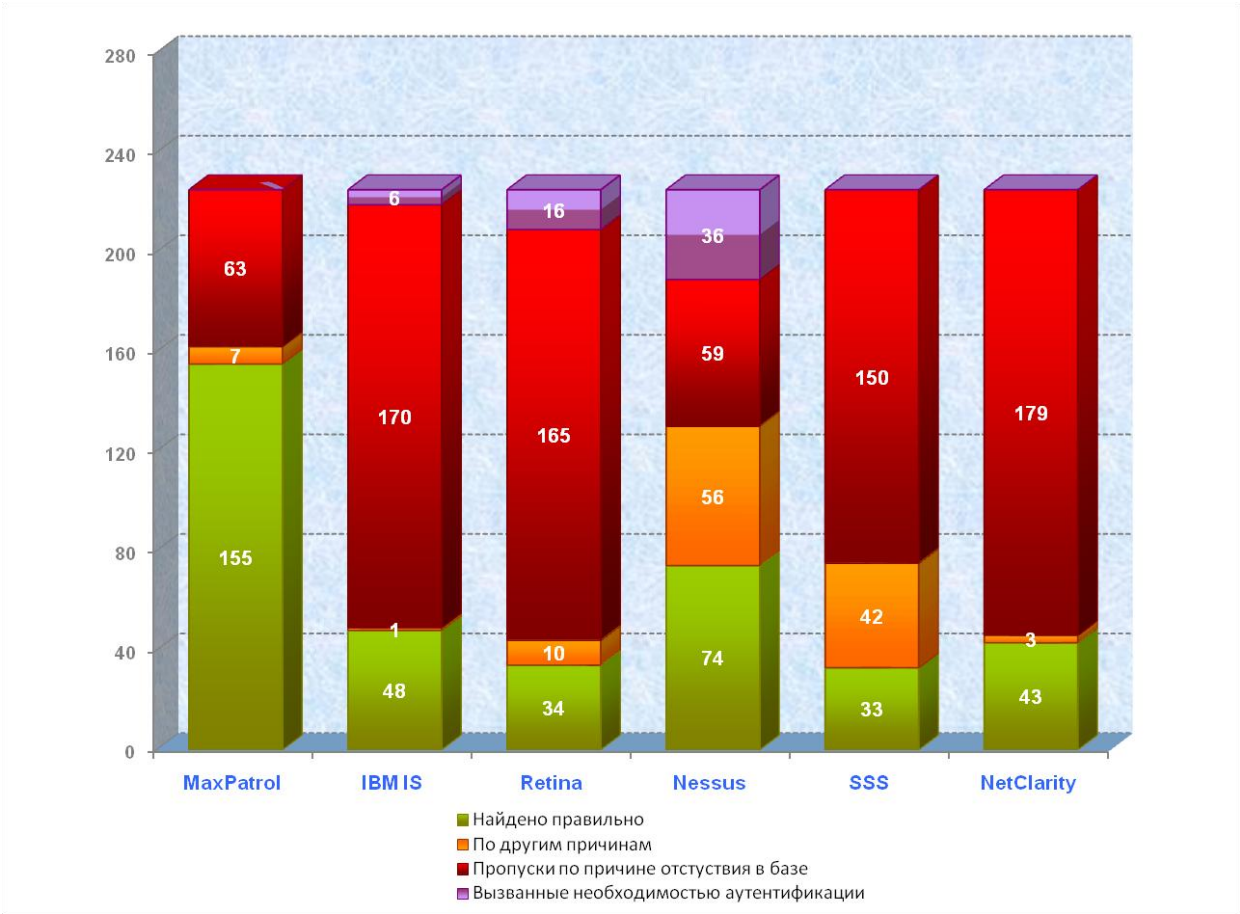

Рис. 38. Причины пропусков уязвимостей

Теперь несколько показателей, получившихся в результате подсчётов.

На рис. 39 представлено отношение числа ложных срабатываний к общему числу найденных уязвимостей, этот показатель в определённом смысле можно назвать точностью работы сканера. Ведь пользователь, прежде всего, имеет дело с перечнем найденных сканером уязвимостей, из которого необходимо выделить найденные правильно.

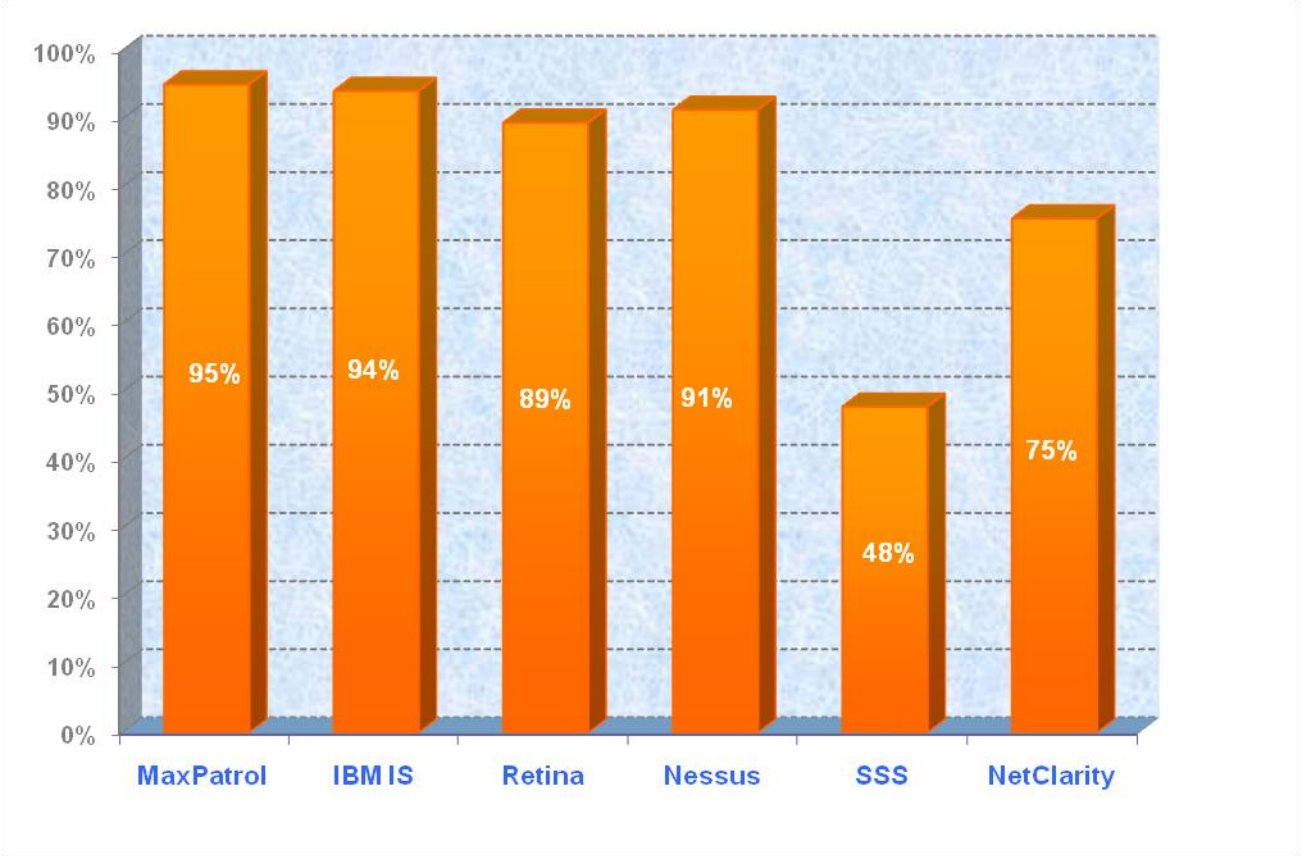

Рис. 39. Точность работы сканеров

Из этой диаграммы видно, что наивысшая точность (95%) достигнута сканером MaxPatrol. Хотя число ложных срабатываний у него не самое низкое, такой показатель точности достигнут за счёт большого количества найденных уязвимостей. Следующим по точности определения идёт Internet Scanner. Он показал самое низкое число ложных срабатываний. Самый низкий результат у сканера SSS, что неудивительно при таком большом количестве ложных срабатываний, которое было замечено в ходе сравнения.

Ещё один расчётный показатель – это полнота базы (рис. 40). Он рассчитан как отношение числа уязвимостей, найденных правильно, к общему числу уязвимостей (в данном случае - 225) и характеризует масштабы «пропусков».

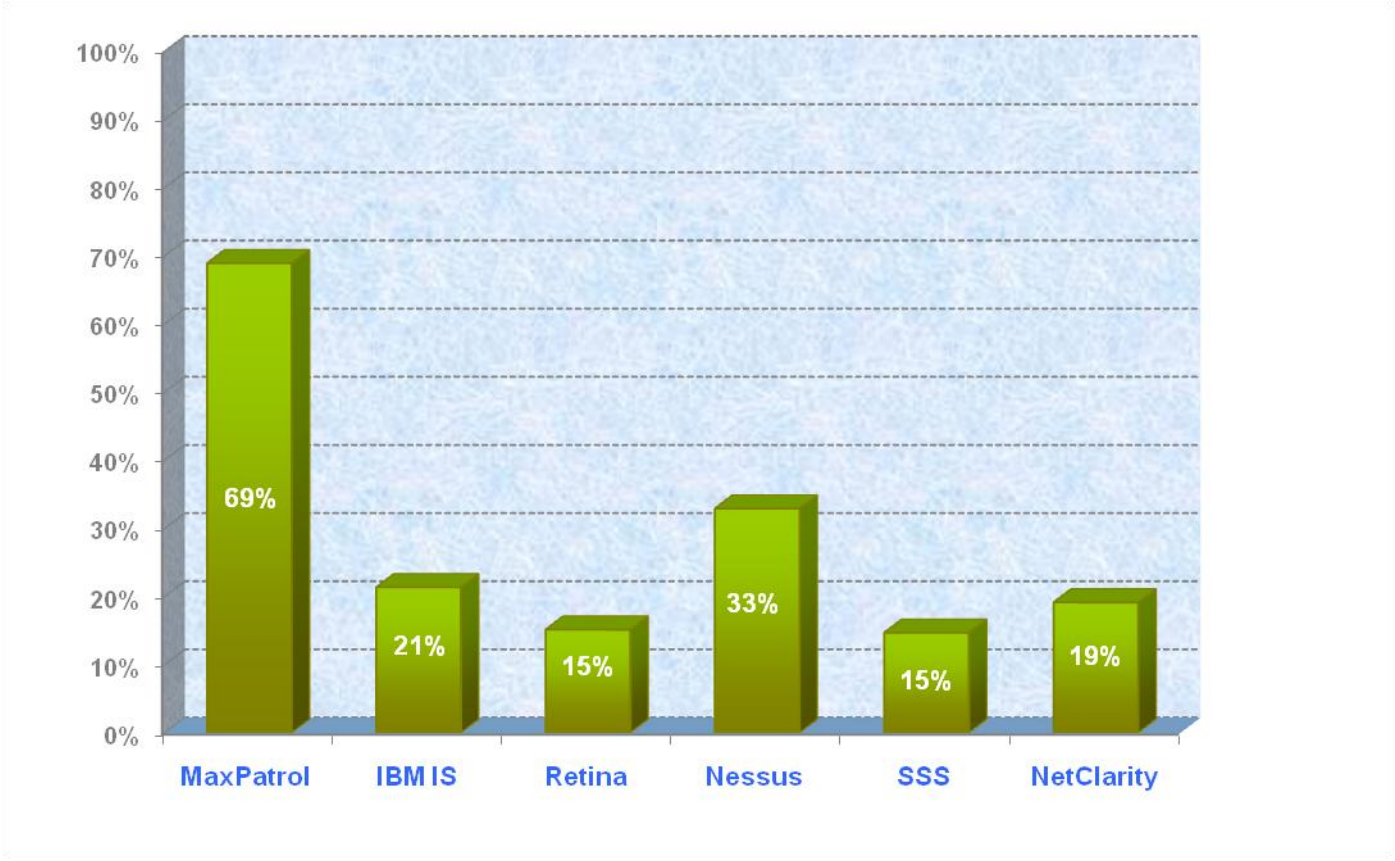

Рис. 40. Полнота базы

Из этой диаграммы видно, что база сканера MaxPatrol наиболее адекватна поставленной задаче.

10. ЗАКЛЮЧЕНИЕ

10.1. Комментарии к результатам лидеров: MaxPatrol и Nessus

Первое место по всем критериям данного сравнения достаётся сканеру MaxPatrol, на втором месте – сканер Nessus, результаты остальных сканеров существенно ниже.

Здесь уместно вспомнить один из документов, подготовленный национальным институтом стандартов и технологий США (NIST), а именно - «Guideline on Network Security Testing». В нём говорится, что в ходе контроля защищённости компьютерных систем рекомендуется использовать как минимум два сканера безопасности.

В полученном результате, по сути, нет ничего неожиданного и удивительного. Не секрет, что сканеры XSpider (MaxPatrol) и Nessus пользуются популярностью как среди специалистов по безопасности, так и среди «взломщиков». Это подтверждают и приведённые выше результаты опроса. Попробуем проанализировать причины явного лидерства MaxPatrol (частично это касается и сканера Nessus), а также причины «проигрыша» других сканеров. Прежде всего – это качественная идентификация сервисов и приложений. Проверки, основанные на выводах (а их в данном случае использовалось довольно много), сильно зависят от точности сбора информации. А идентификация сервисов и приложений в сканере MaxPatrol практически доведена до совершенства. Вот один показательный пример. На одном из объектов сканирования был обнаружен сервис POP3 (реализуемый Microsoft Exchange) с подменённым баннером (рис. 41). MaxPatrol, тем не менее, смог точно идентифицировать сервис, тогда как Nessus, например, не только неверно определил сервис, но и сделал ошибочные выводы (рис. 42).

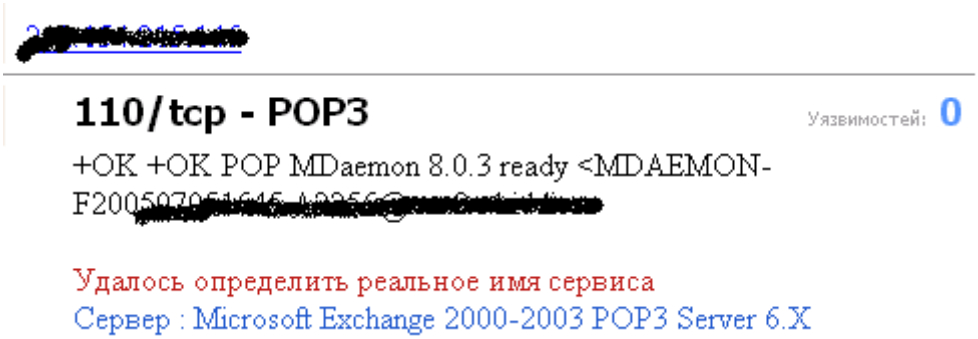

Рис. 41. Результат идентификации сервиса POP3 сканером MaxPatrol

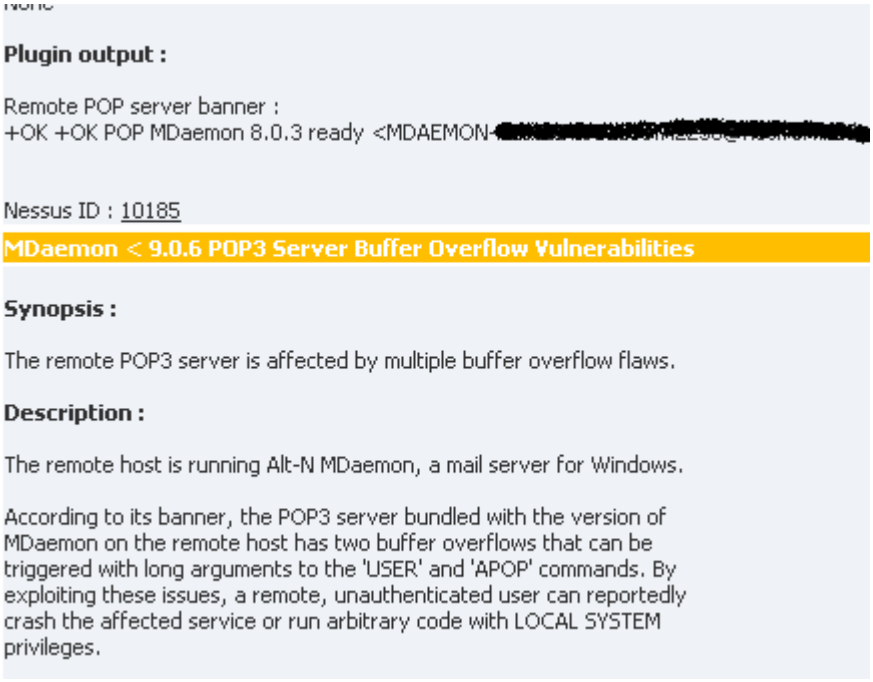

Рис. 42. Результат идентификации сервиса POP3 сканером Nessus

Вторая причина успеха MaxPatrol – полнота базы и её адекватность поставленной задаче и вообще «сегодняшнему дню». По результатам заметно, что база проверок в MaxPatrol значительно расширена и детализирована, в ней «наведён порядок», при этом явный «крен» в сторону web-приложений компенсируется и расширением проверок в других областях, например, произвели впечатление результаты сканирования представленного в сравнении маршрутизатора Cisco[6].

Третья причина – качественный анализ версий приложений с учётом операционных систем, дистрибутивов и различных «ответвлений». Можно также добавить и использование разных источников (базы уязвимостей, уведомления и бюллетени «вендоров»).

Наконец, можно ещё добавить, что MaxPatrol имеет очень удобный и логичный интерфейс, отражающий основные этапы работы сетевых сканеров безопасности. А это немаловажно. Связка «узел, сервис, уязвимость» очень удобна для восприятия[7]. И особенно для данной задачи.

Теперь о недостатках и «слабых» местах. Поскольку MaxPatrol оказался лидером сравнения, то и критика в его адрес будет «максимальной».

Во-первых, так называемый «проигрыш в мелочах». Имея очень качественный движок, важно предложить и соответствующий дополнительный сервис, например, удобный инструментарий, позволяющий что-то сделать вручную, средства поиска уязвимостей, возможность «тонкой» настройки системы. MaxPatrol продолжает традицию XSpider и максимально ориентирован на идеологию «нажал и заработало». С одной стороны это неплохо, с другой стороны – ограничивает «дотошного» аналитика.

Во-вторых, остались «неохваченными» некоторые сервисы (можно судить об этом по результатам данного сравнения), например, IKE (порт 500).

[6] Как выяснилось позднее, в рамках сотрудничества российского представительство Cisco Systems и Positive Technologies было достигнуто соглашение о технологическом сотрудничестве, в рамках которого Positive Technologies получает информацию об уязвимостях непосредственно у производителя.

[7] Это субъективное мнение автора сравнения.

В-третьих, в некоторых случаях не хватает элементарного сопоставления результатов двух проверок друг с другом, например, как в описанном выше случае с SSH. Т. е. нет выводов, основанных на результатах нескольких проверок. Например, операционная система узла host4 была определена как Windows, а «вендор» сервиса PPTP классифицирован как Linux. Можно сделать выводы? Например, в отчёте в области определения операционной системы указать, что это «гибридный» узел.

В-четвёртых, описание проверок оставляет желать лучшего. Но здесь следует понимать, что MaxPatrol находится в неравных условиях с другими сканерами: качественный перевод на русский язык всех описаний – очень трудоёмкая задача.

Сканер Nessus показал, в целом, неплохие результаты, а в ряде моментов он был точнее сканера MaxPatrol. Главная причина отставания Nessus – это пропуски уязвимостей, но не по причине отсутствия проверок в базе, как у большинства остальных сканеров, а в силу особенностей реализации. Во-первых (и этим обусловлена значительная часть пропусков), в сканере Nessus наметилась тенденция развития в сторону «локальных» или системных проверок, предполагающих подключение с учётной записью. Во-вторых, в сканере Nessus учтено меньше (в сравнении с MaxPatrol) источников информации об уязвимостях. Это чем-то похоже на сканер SSS, основанный по большей части на базе SecurityFocus.

10.2. Комментарии к результатам остальных сканеров

Теперь проанализируем причины слабых результатов остальных сканеров.

10.2.1. Shadow Security Scanner (SSS)

Используя Shadow Security Scanner (SSS), нужно быть готовым к значительному проценту ложных срабатываний и пропусков. Его результаты требуют тщательной последующей проверки, кроме того, существенен процент пропусков именно по причине ошибок реализации. Да и просто есть элементарные ошибки, например, на одном из узлов была найдена одна и та же уязвимость в сервисе SSH (рис. 43).

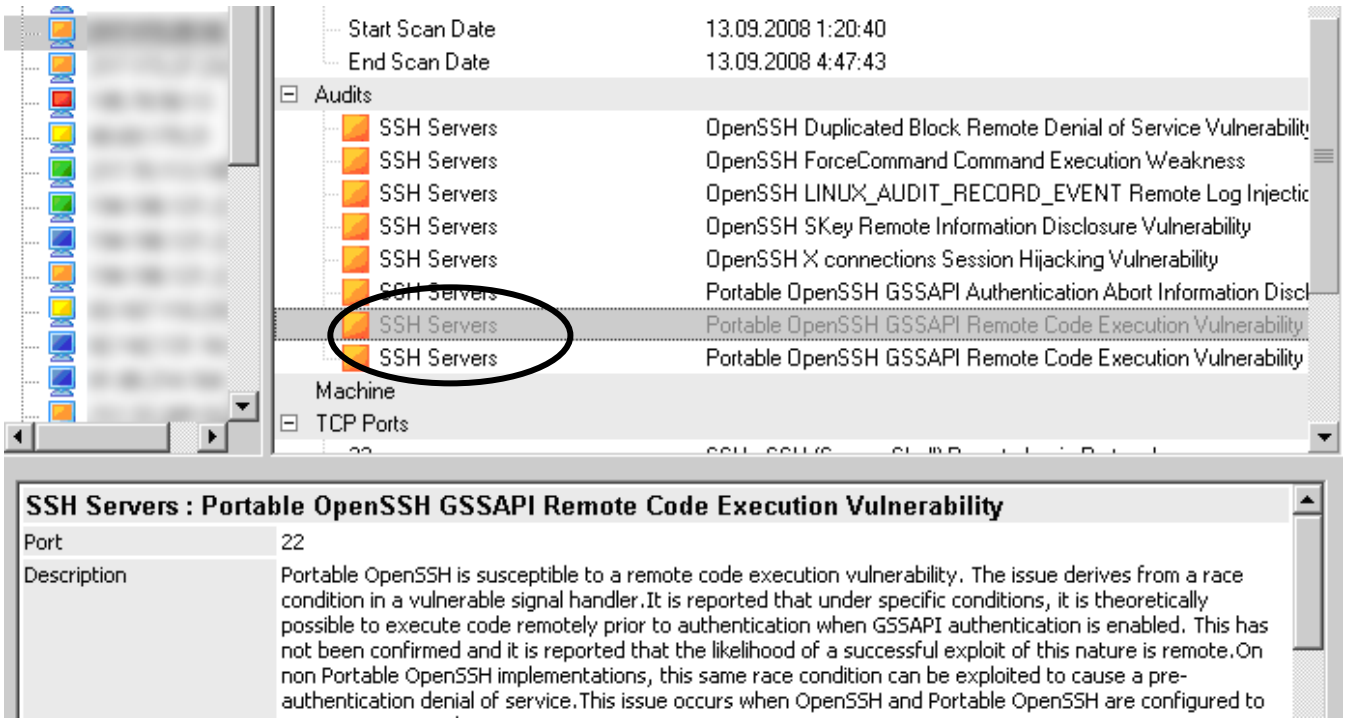

Рис. 43. Обнаружение двух «одинаковых» уязвимостей сканером SSS

База проверок сделана так, что отсутствуют ссылки на каталог CVE для некоторых записей, например, вот описание одной из уязвимостей (рис. 44), где поле CVE имеет значение CVE-MAP-NOMATCH.

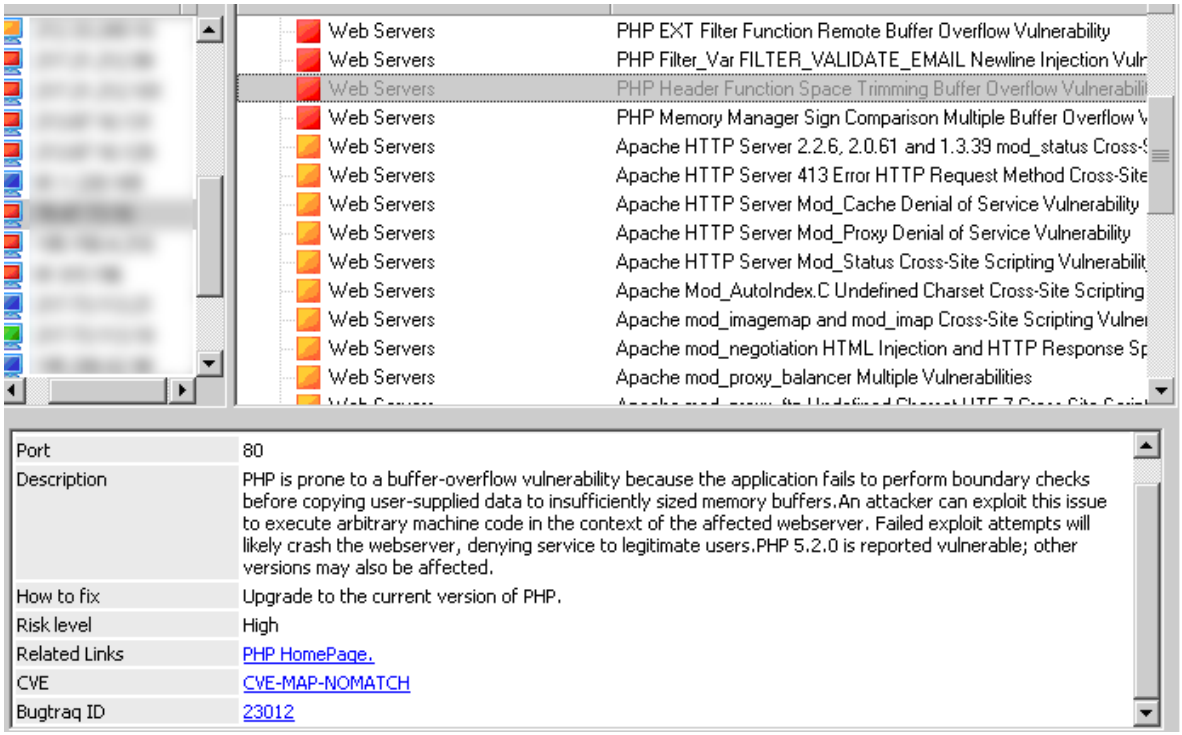

Рис. 44. Отсутствующий индекс CVE в проверке BID 23012

С другой стороны, BID=23012 соответствует индекс CVE=CVE-2007-1900, это иллюстрирует рисунок 45.

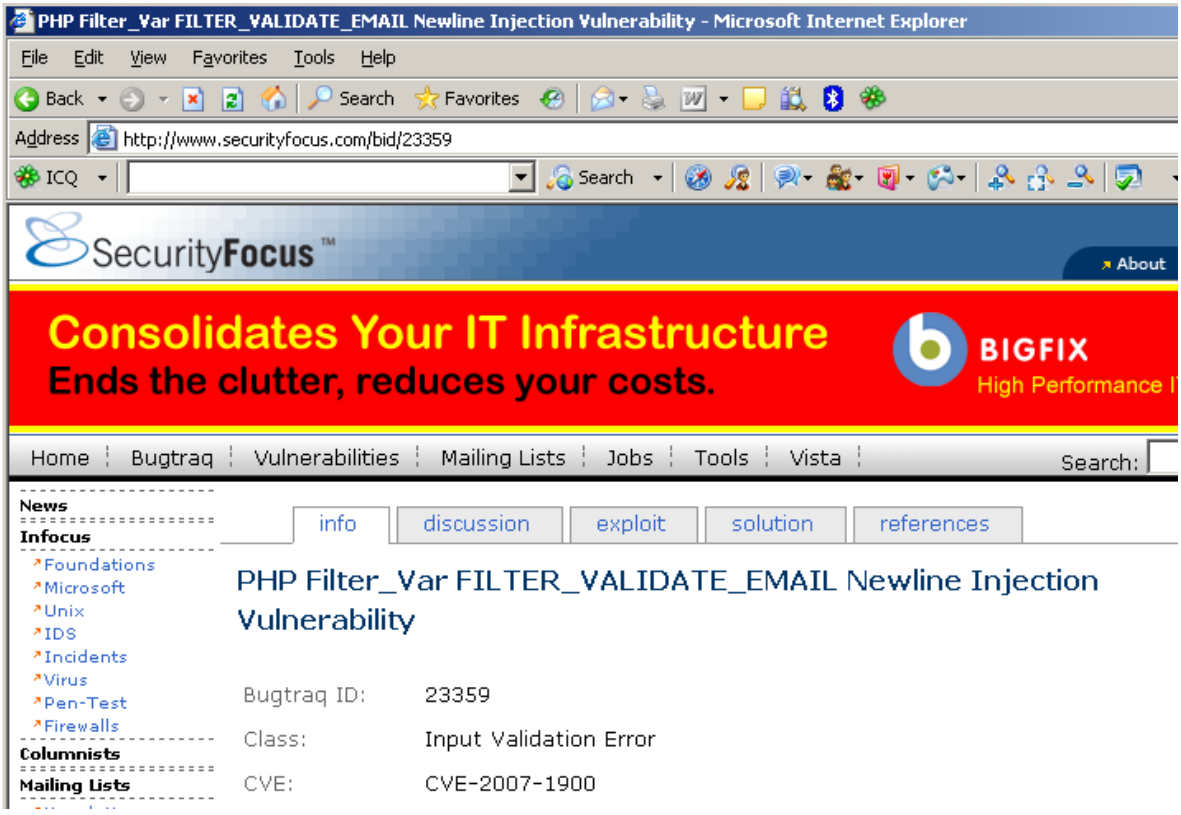

Рис. 45. Уязвимость CVE-2007-1900 в базе уязвимостей SecurityFocus

Встречаются и просто ошибочные ссылки на каталог CVE (рис. 46).

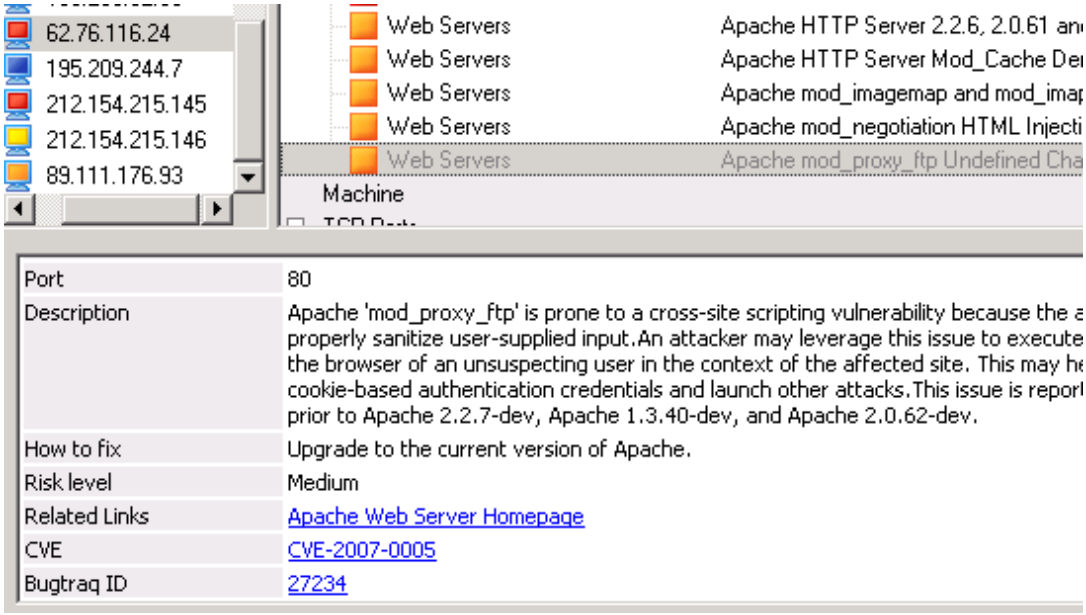

Рис. 46. Ошибочная ссылка на каталог CVE в сканере SSS.

В действительно же индекс CVE совсем другой (рис. 47).

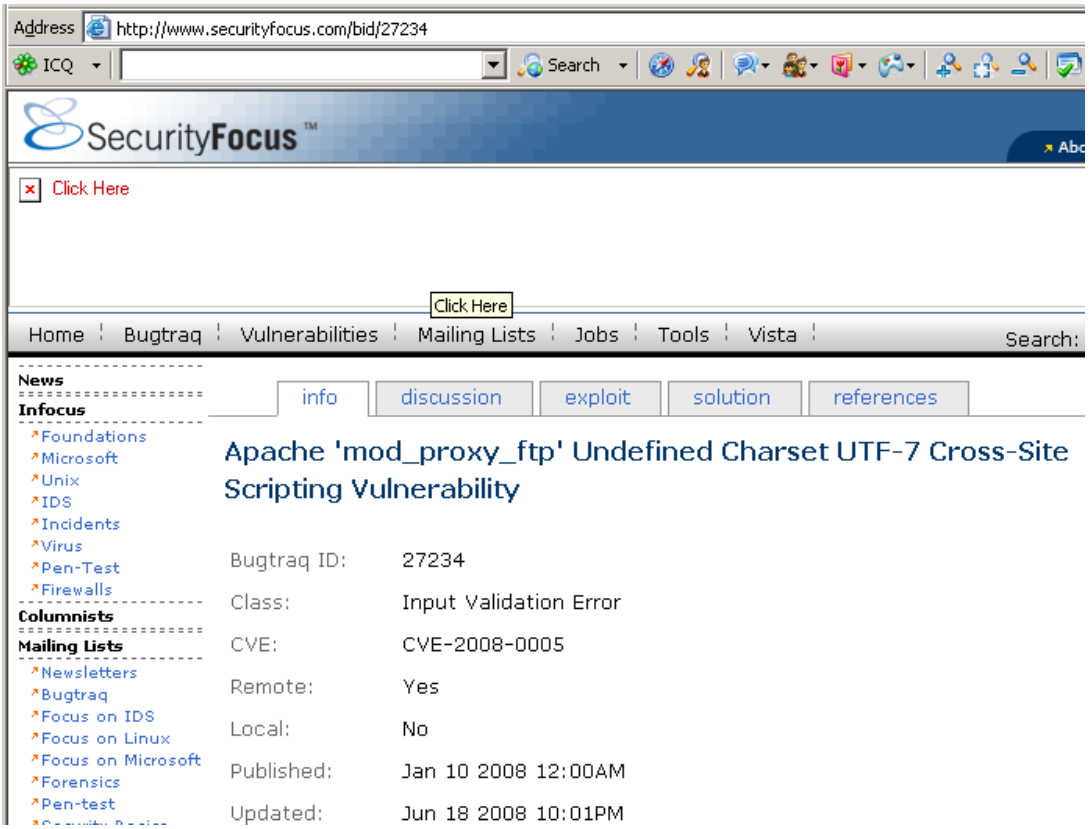

Рис. 47. Уязвимость 27234 в базе данных SecurityFocus

Очень неудобно отсутствие возможности группирования уязвимостей и средств удобного поиска[8]. Поиск вообще обычно завершается ошибкой (рис. 48).

[8] Кстати, этого нет и у лидера сравнения – сканера MaxPatrol.

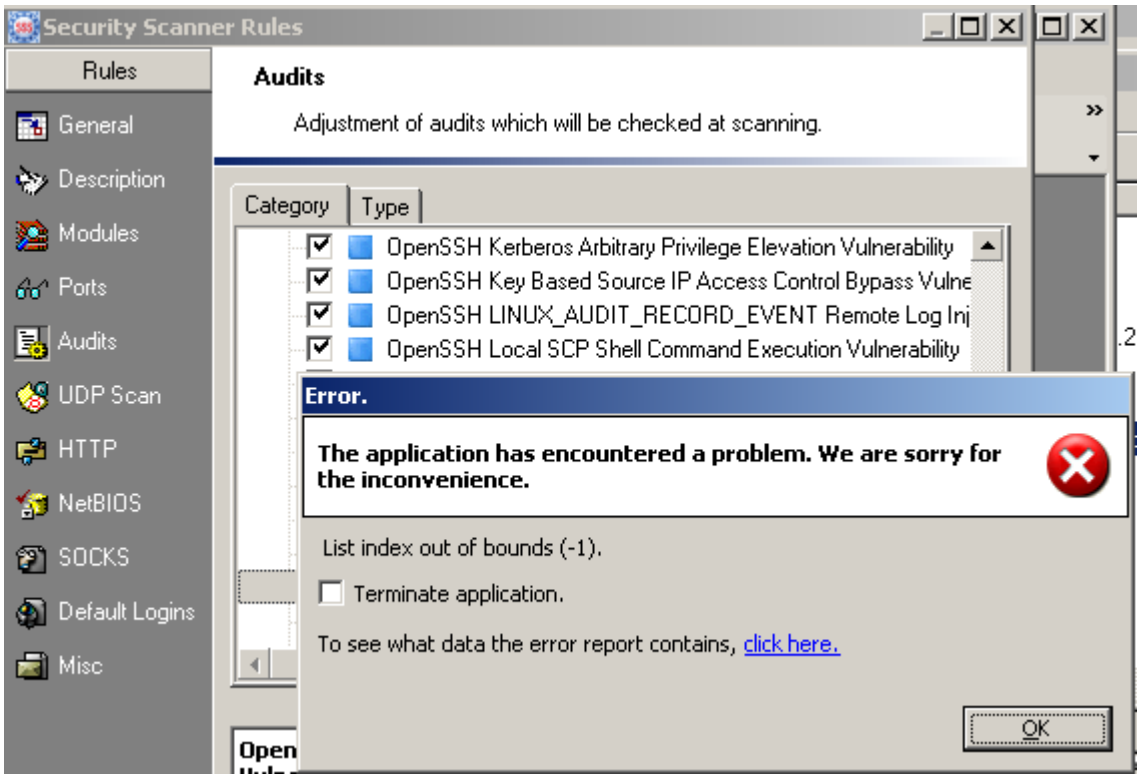

Рис. 48. Ошибка поиска в SSS

При выборе в списке уязвимостей порой вообще не видно её описания или оно показывается «через раз» (рис. 49).

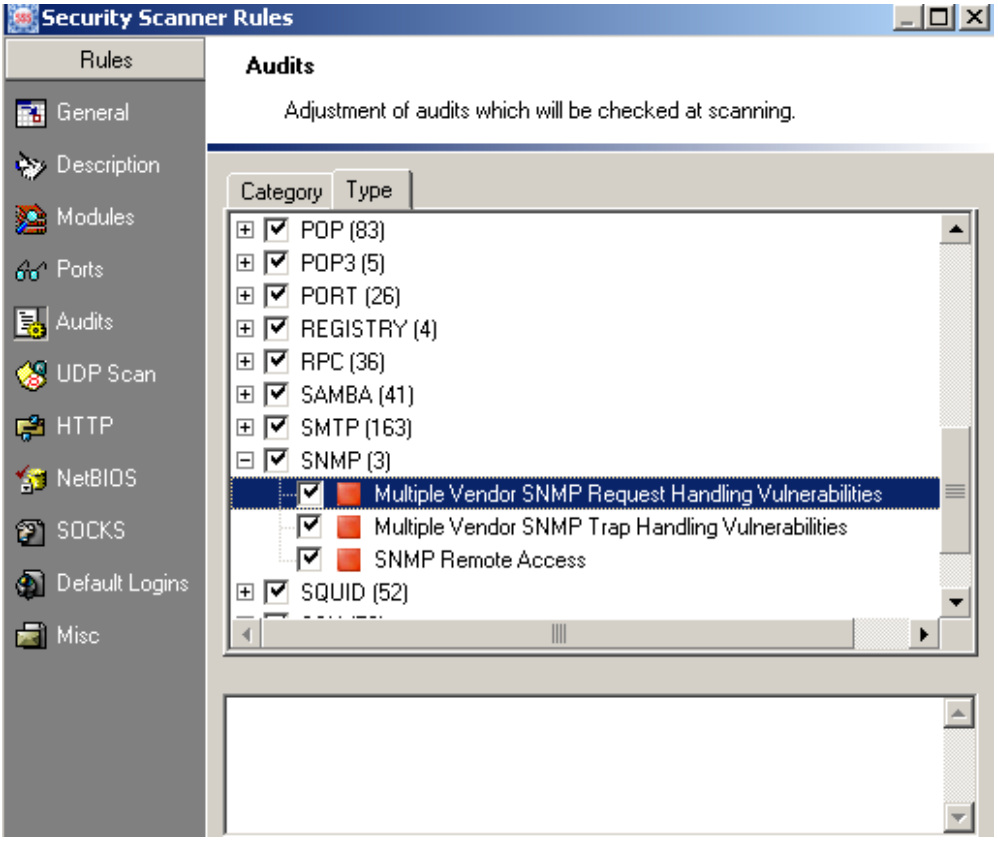

Рис. 49. Отсутствие описания уязвимостей в SSS

И этот список замечаний можно продолжать бесконечно. В общем, если проводить автомобильную аналогию, этот сканер напоминает «Жигули», которые всё время ломаются.

Наконец, в сканере SSS за основу взята база securityfocus, а ориентироваться только на один источник, как было показано выше, не совсем правильно.

10.2.2. Internet Scanner

Система анализа защищённости Internet Scanner появилась очень давно – в начале 90-х. Сейчас она напоминает «старичка», который по современным меркам умеет немного, но делает это хорошо. Безусловно, «лучшие годы» этого сканера приходятся на конец прошлого века и начало нынешнего[9]. Очень жаль, но он так и остался в конце 90-х. Развитие этого сканера в последние годы идёт «вслед за Windows», достаточно посмотреть на состав его обновлений: большая часть проверок направлена на обычный контроль обновлений Windows-систем (рис. 50), которым сейчас никого уже не удивишь.

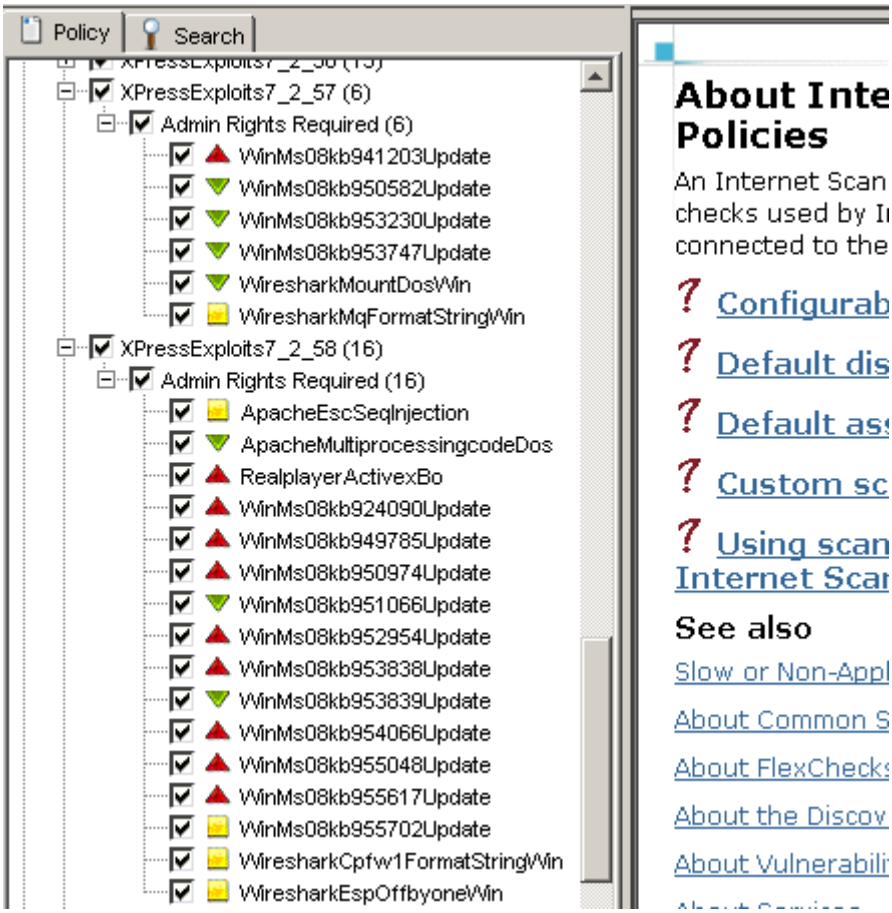

Рис. 50. Состав последних обновлений в Internet Scanner

Кстати сказать, и тут не обошлось без мелких недостатков, например, проверки Apache почему-то вдруг стали требовать наличия административных привилегий. Это видно из следующего описания (рис. 51).

[9] Например, довольно удачной была версия 6.2.1.

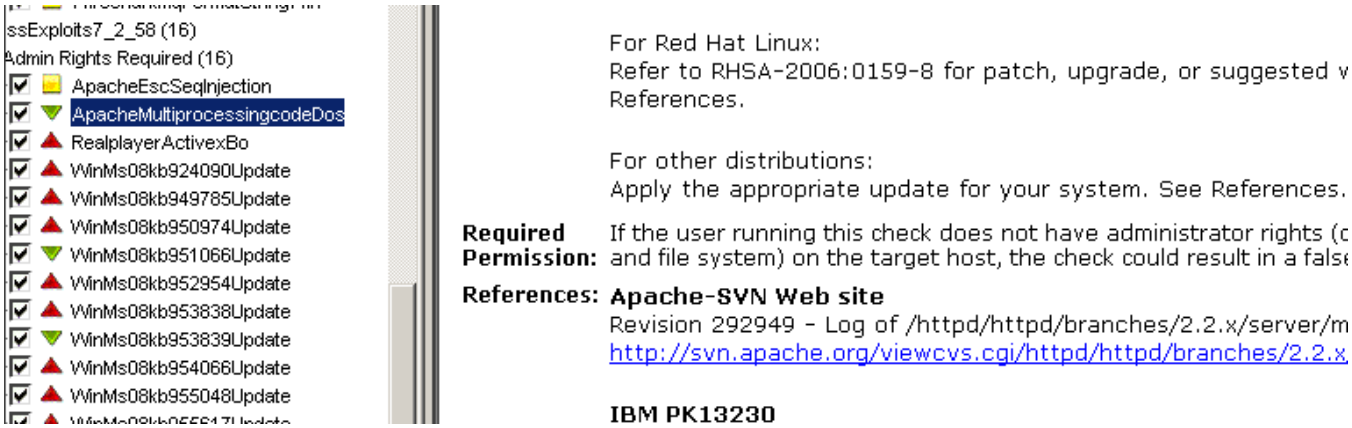

Рис. 51. Одна из проверок сервера Apache

Вобщем, если проанализировать найденные этим сканером уязвимости, это будут в основном, «возможность определения сетевой топологии» (CVE-1999-0525), «поддержка почтовым сервером команды EHLO» (CVE-1999-0531) и т. п. Может, это и было актуально в конце 90-х, но сейчас времена изменились. Пожалуй, только проверки маршрутизатора Cisco были выполнены на хорошем уровне, результаты по остальным узлам довольно слабы. Что касается идентификации сервисов и приложений, Internet Scanner уверенно работает с известными, «крупными» приложениями, например, IIS, Sendmail, Apache. При этом он игнорирует использование сервисами нестандартных портов. А для данной задачи эта «мелочь» оказалась существенной.

10.2.3. NetClarity Auditor

Эта система представляет собой программно-аппаратный комплекс («железо» + Linux + Nessus). В ходе сравнения он был условно назван «Зелёный Nessus». За основу в нём взята «ветка» сканера Nessus с открытым кодом (2.x). Относительно оригинальным в этой системе можно назвать, наверное, само устройство. Всё-таки для сканеров безопасности программно-аппаратный комплекс - это пока редкость.

Достоинств у этой системы два:

- Собственно программно-аппаратный комплекс
- Сканер Nessus

Результат эта система показала в целом не очень хороший, это можно объяснить следующими соображениями:

- За основу взята не самая удачная ветвь сканера Nessus. За последние несколько лет Nessus изменился, уменьшилось число ложных срабатываний, повысилось качество проверок. Здесь же за основу взят устаревший вариант сканера Nessus с его ложными срабатываниями и «тяжёлым наследием прошлого».
- Нет возможности задать перечень портов для сканирования. Мелочь, но очень неприятная. Многие пропуски в данном сравнении объясняются именно ей.

Позиционирование этой системы вообще не очень понятно. На сайте производителя она позиционируется как система, которую можно применить в комплексе средств безопасности «Network Access Control». То есть при попытке доступа в сеть систему (например, принесённый кем-то ноутбук) вначале сканируют на предмет уязвимостей, а затем допускают или не допускают. Можно провести аналогию, например, с аэропортом: вас обыскивают, а затем допускают в самолёт. С другой стороны, система не позволяет проводить проверки с учётной записью, а в данном случае логично было бы делать именно так. Но в «этом ящике» реализован

только режим «Penetration Test». Получается, что по прямому назначению систему использовать неразумно из-за отсутствия режима аудита, а для «Penetration Test» она тоже не годится по приведённым выше соображениям.

10.2.4. Retina

Это сканер производит впечатление в меру качественного и удачного продукта. База проверок имеет явные тенденции в сторону «локальных» проверок, процент ложных срабатываний невелик, а пропуски обусловлены либо отсутствием проверки в базе, либо необходимостью аутентификации. Идентификация сервисов и приложений реализована «средне». Как было показано выше, некоторые сложные случаи Retina «не осилила». Этот сканер можно охарактеризовать как «разумное сочетание» качества, возможностей и удобства использования.

11. ОГРАНИЧЕНИЯ ДАННОГО СРАВНЕНИЯ

В ходе сравнения были изучены возможности сканеров в контексте только одной задачи – тестирование узлов сетевого периметра на устойчивость к взлому. Например, если проводить автомобильную аналогию, мы увидели, как разные автомобили ведут себя, допустим, на скользкой дороге. Однако есть и другие задачи, решение которых этими же сканерами может выглядеть совершенно иначе. В ближайшее время планируется сделать сравнение сканеров в ходе решения таких задач, как:

- Проведение аудита систем с использованием учётной записи
- Оценка соответствия требованиям стандарта PCI DSS
- Сканирование Windows-систем

Кроме того, планируется сделать сравнение сканеров и по формальным критериям.

В ходе данного сравнения был протестирован только сам «движок» или, выражаясь современным языком, «мозг» сканера. Возможности в плане дополнительного сервиса (отчёты, запись информации о ходе сканирования и т. п.) никак не оценивались и не сравнивались.

Также не оценивались степень опасности и возможности по эксплуатации найденных уязвимостей. Некоторые сканеры ограничились «незначительными» уязвимостями низкой степени риска, другие же выявили действительно критичные уязвимости, позволяющие получить доступ к системе.

