УТВЕРЖДЕН

RU.83128364.501540-XS-7.8.24-ЛУ

Сетевой сканер безопасности XSpider 7.8.24

Руководство администратора

RU.83128364.501540-XS-7.8.24 93 01

Листов 70

2014

Подп. и дата	
Инв. №	
Взам.	
Подп. и дата	
Инв. №	

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

ОГЛАВЛЕНИЕ

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

1. ОПИСАНИЕ СИСТЕМЫ

Сетевой сканер безопасности XSpider 7.8.24 (далее - сканер XSpider) позволяет выполнять сканирование, сбор данных, их обработку, сохранение в БД и выпуск отчетов. Сканер XSpider включает в себя графический интерфейс администратора. В состав сканера XSpider включена база знаний, содержащая информацию о проверках и уязвимостях, модуль управления и сканирующее ядро. Данные сканирования хранятся во встроенной базе данных. Следует иметь в виду, что при выполнении сканирования XSpider порождает большой объем сетевого трафика, поэтому для работы необходимо высокоскоростное соединение между ним и исследуемыми объектами.

2. ТРЕБОВАНИЯ К СИСТЕМЕ

2.1. Требования к аппаратному и программному обеспечению

Данный раздел содержит информацию о том, какие требования к аппаратному и программному обеспечению предъявляются для развертывания сканера безопасности XSpider.

2.1.1 Требования к аппаратному обеспечению

Базовые требования к аппаратному обеспечению для XSpider определены в Табл. 1.

Табл. 1 Минимальные аппаратные требования к компонентам XSpider

Компонент	Процессор	Оперативная память	Жесткий диск
XSpider	PIV 1,6 ГГц	2 ГБ	5 ГБ

Разрешение монитора для установки и работы с системой должно составлять не менее 1280 x 1024 пикс.

Приведенные требования достаточны для установки системы, однако для работы в масштабных инсталляциях могут потребоваться дополнительные аппаратные ресурсы.

2.1.1.1. Процессор

При сканировании система не предъявляет дополнительных требований к центральному процессору.

Вычислительные процессы XSpider оптимизированы так, чтобы максимально использовать ресурсы сканирующего узла (т.е. узла, где расположен XSpider). В связи с этим существует прямая зависимость между увеличением тактовой частоты процессора и увеличением скорости сканирования. Однако наибольший прирост производительности дает использование нескольких процессоров или многоядерных решений. В Табл. 2 приведена зависимость скорости одновременного сканирования разного количества узлов от типа и количества процессоров компьютера, на котором установлен XSpider.

Табл. 2 Зависимость скорости сканирования (мин.) от количества процессоров

	Одноядерный	Двухъядерный	Два двухъядерных
1 узел	3-20	3-20	3-20
10 узлов	15-60	8-30	9-30
50 узлов	60-250	40-150	25-80
100 узлов	120-250	75-220	50-160

В таблице указан диапазон возможных значений, где границами является время сканирования стандартной рабочей станции Windows (Windows XP + Microsoft Office 2003) и сервера с большим количеством установленного программного обеспечения. При расчетах в зависимости от ситуации можно использовать среднее значение.

Таким образом, для увеличения скорости сканирования можно масштабировать процессорные мощности.

2.1.1.2. Оперативная память

Приведенные минимальные требования к ОЗУ (Табл. 1) достаточны для работы сканера XSpider в большинстве сетей. Однако в случае обработки результатов большого количества сканирований (например, при построении отчетов на основе данных из истории сканирования) может потребоваться дополнительный объем оперативной памяти. Пороговым значением является 300 узлов. В случае если сканер обслуживает более 300 узлов, рекомендуется устанавливать не менее 3 ГБ ОЗУ.

2.1.1.3. Жесткий диск

Требования к объему жесткого диска для сканера XSpider целиком зависят от количества сканируемых узлов и интенсивности сканирования. В Табл. 3 приведена информация о требуемом объеме дискового пространства сканера, обслуживающего различное количество узлов, при различной интенсивности сканирования.

Табл. 3 Требования к объему жесткого диска (МБ) из расчета на год в зависимости от частоты сканирования

	Ежедневно	Еженедельно	Ежемесячно
1 узел	360	55	12
10 узлов	3600	550	120
50 узлов	18000	2750	600
100 узлов	36000	5500	1200
1000 узлов	360000	55000	12000

2.1.2 Программное обеспечение

Сканер XSpider разработан для функционирования на базе операционных систем линейки Windows. В настоящее время работоспособность системы была протестирована при использовании следующих ОС:

- Microsoft Windows XP SP 3 (x86) и старше;
- Microsoft Windows Server 2003 SP 2 (x86, x64) и старше;
- Microsoft Windows Vista SP 2 (x86,x64) и старше;
- Microsoft Windows Server 2008 SP2 (x86, x64) и старше;
- Microsoft Windows 7 (x86,x64) и старше;
- Microsoft Windows Server 2008 R2 (x64) и старше;
- Microsoft Windows 8 (x86,x64) и старше;
- Microsoft Windows Server 2012 (x64) и старше.

Внимание! Список совместимых систем постоянно расширяется. Для получения актуальной информации обратитесь в службу технической поддержки.

При выборе операционной системы следует учитывать, что при ряде проверок система XSpider интенсивно использует стек протоколов TCP/IP операционной системы. В связи с этим применение клиентских версий ОС (например, Windows XP) для проведения сканирования большого количества узлов неэффективно. В частности, уменьшается производительность сканера портов и ряда других механизмов.

Другим аспектом требующим внимания, является совместимость ОС с дополнительными программами, используемыми XSpider. Обязательными компонентами, без которых работа системы невозможна, являются:

- Microsoft Internet Explorer 7.0 и выше;
- Microsoft .NET Framework Version 3.5 SP1;
- Microsoft Runtime Libraries версии 9.0.30729.4148 для x86 систем (дистрибутив по ссылке: http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=11895).

Требуется установка компонента Microsoft .NET Framework Version 3.5 SP1 в случае работы со следующими ОС:

- Microsoft Windows XP SP 3 (x86) и старше;
- Microsoft Windows Server 2003 SP 2 (x86, x64) и старше;
- Microsoft Windows Vista SP 2 (x86,x64) и старше;
- Microsoft Windows Server 2008 R2 (x64) и старше.

И требуется установить компонент Microsoft Internet Explorer 7.0 и выше при работе на следующих ОС:

- Microsoft Windows XP SP 3 (x86) и старше;
- Microsoft Windows Server 2003 SP 2 (x86, x64) и старше.

Загрузить дистрибутивы данных программ можно с сайта компании Microsoft (www.microsoft.com).

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

2.2. Требования к сетевой инфраструктуре

В данном разделе изложена информация, которая поможет интегрировать сканер XSpider в существующую сетевую архитектуру.

2.2.1. Сетевые транспорты

Все параметры сетевой архитектуры тесно связаны с понятием транспорта. Система XSpider реализует концепцию сканирования узлов без применения заранее установленных агентов.

Транспорт – это набор сетевых протоколов, используемых сканером XSpider для проведения сканирования.

В системе XSpider используется транспорт RPC. Номера портов RPC присваиваются автоматически, в диапазоне 1024 – 65535 обычно используются для ОС Windows 2000\XP\2003, а для ОС Windows Vista\2008 используется диапазон 49152 – 65535.

2.2.2. Сетевое взаимодействие с объектом сканирования

Сканер XSpider использует сеть для связи с объектами сканирования. Так, расположение XSpider в непосредственной близости от объекта сканирования позволяет проводить оценку защищенности с минимальной нагрузкой на магистральные каналы связи.

2.2.3. Взаимодействие со средствами защиты

Средства обеспечения безопасности могут оказывать влияние на работу сканера XSpider. В связи с этим, на этапе планирования и развертывания рекомендуется провести тестовые сканирования и использовать методы снижения негативных последствий.

2.2.4. Межсетевые экраны

Межсетевые экраны (МЭ) осуществляют фильтрацию трафика и могут блокировать доступ к сетевым портам, на которых работают протоколы удаленного управления, используемые XSpider при проведении сканирования. Для решения этой проблемы можно использовать два подхода: открытие сетевых портов, используемых сканером на МЭ, или размещение сканера «за» межсетевым экраном в непосредственной близости от объекта сканирования.

Оптимальным с точки зрения достоверности и скорости сканирования является отсутствие межсетевого экрана между объектом сканирования и сканером XSpider.

2.2.5. **Средства защиты прикладного уровня**

Большинство современных сетевых средств обеспечения безопасности содержат модули анализа прикладных протоколов (Stateful Inspection, Application Firewall). Данные механизмы могут вмешиваться в работу сканера, снижая достоверность полученных результатов. Так, например, сканирование веб-приложения через МЭ, поддерживающий функции защиты веб-приложений (Web Application Firewall), не будет достоверным, поскольку МЭ заблокирует ряд потенциально опасных запросов, используемых сканером.

Существуют и другие ситуации, когда фильтр прикладного уровня может оказывать негативное влияние на процесс сканирования. Так, фильтр протокола RPC в Microsoft Internet Security and Acceleration Server (ISA) 2004/2006 по умолчанию блокирует RPC-запросы. Из-за этого снижается производительность сканера, и некоторые проверки невозможно выполнить. Для того чтобы обеспечить полнофункциональное сканирование через ISA Server, необходимо выбрать соответствующее правило в окне Firewall Policy, вызвать контекстное меню и выбрать пункт «Configure RPC protocol». В появившемся окне необходимо отключить опцию «Enforce strict RPC compliance» (Рис. 1).

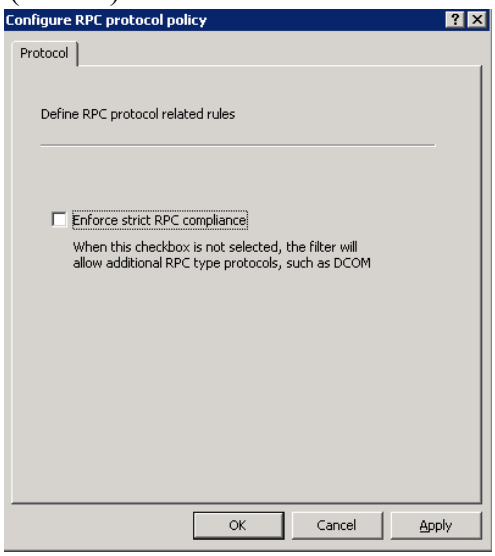


Рис. 1 Отключение проверки RPC в Microsoft ISA Server 2004/2006

В некоторых средствах защиты не существует возможности отключить фильтрацию прикладных протоколов только для отдельных узлов. При возникновении таких ситуаций рекомендуется выносить сканер за МЭ.

2.2.6. **Системы обнаружения и предотвращения атак**

Системы обнаружения/предотвращения атак в большинстве своем реагируют на процесс сканирования как на потенциальную атаку. Получение списка открытых портов, проверка стойкости паролей, доступ к протоколам удаленного управления – все это может привести к срабатыванию средств защиты. В случае если механизм

предотвращения атак не задействован, множественные срабатывания сигнатур приведут только к увеличению объема журналов системы обнаружения атак. Если механизм предотвращения атак включен, то система может вмешаться в процесс сканирования и исказить результаты работы сканера XSpider. В связи с этим, рекомендуется вносить узлы, на которых установлен XSpider, в список исключений системы обнаружения атак.

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

2.2.7. **Средства защиты уровня узла**

В случае использования персональных межсетевых экранов и других средств защиты уровня узла (например, HIPS) на сканируемых объектах необходимо разрешить узлам, на которых установлен XSpider, доступ по используемым протоколам удаленного управления. Для входящего в поставку Microsoft Windows МЭ Windows Firewall это осуществляется путем добавления IP-адресов в параметр групповой политики Computer Configuration - Administrative Templates - Network - Network Connections - Windows Firewall - Domain Profile - Windows Firewall: Allow remote administration exception (Рис. 2). Дополнительно необходимо проверить, что параметр Computer Configuration - Administrative Templates - Network - Network Connections - Windows Firewall - Domain Profile - Windows Firewall: Do not allow exceptions отключен.

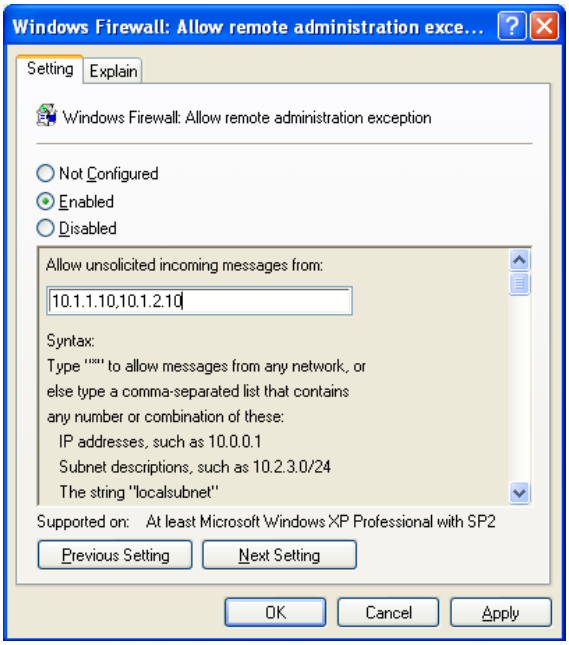


Рис. 2 Настройка исключений в Windows Firewall

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

3. УСТАНОВКА СИСТЕМЫ

3.1. Получение дистрибутива

Дистрибутив XSpider может быть получен на CD-диске в рамках поставки или загружен с сервера обновлений. В последнем случае предоставляется гиперссылка с ограниченным сроком действия, например:

https://service.maxpatrol.com/downloads/96c7247c-a20f-4bc2-a6a1-46791e7d1f90/XSpider-4919-080712.exe

Дистрибутив системы XSpider представляет собой один файл - инсталлятор, имя которого формируется следующим образом:

XSpider-<номер лицензии>-<дата сборки в формате ММДДГГ>.exe

Этот файл содержит мастер установки, компоненты системы и одну лицензию.

3.2. Подготовка к установке

Убедитесь, что технические характеристики системы соответствуют минимальным требованиям.

3.3. Установка сканера

После запуска мастера установки и начального приветствия предлагается выбрать каталог установки.

На следующем этапе необходимо задать пароль учетной записи, которая используется для входа в систему. Имя этой учетной записи (Administrator) фиксировано. Учетная запись Administrator имеет максимальные привилегии по отношению к данному сканеру XSpider.

Внимание! Используйте сложный пароль для учетной записи администратора.

На этом этапе установка сканера XSpider завершается.

Внимание! Правильная настройка даты и времени на сервере имеет большое значение для функционирования системы.

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

3.4. Активация лицензии

Поставляемая в дистрибутиве лицензия является «свободной», т.е. не привязана к конкретному компьютеру. Свободная лицензия позволяет запускать и настраивать сканер. Для использования основных функций XSpider (сканирование, просмотр результатов, выпуск отчетов) необходимо активировать лицензию. При активации лицензия будет привязана к параметрам компьютера.

Внимание! После активации перенос лицензии на другой компьютер невозможен.

Если ключевые аппаратные характеристики компьютера изменятся, то лицензия может стать недействительной. В этом случае необходимо связаться со службой технической поддержки для получения дополнительной информации по обновлению лицензии.

Сканер XSpider автоматически пытается пройти активацию на глобальном сервере обновлений update.maxpatrol.com при первом подключении. При этом используются стандартные настройки (прямое подключение, порт 2002/TCP). В случае если подключение к сети Интернет ограничено (запрещено использование порта 2002/TCP или используется proxy-сервер), следует отказаться от автоматической активации и изменить настройки подключения к серверу обновлений на вкладке Настройки - Основные.

Успешность активации лицензии можно проверить на закладке Настройки – Основные, раздел Лицензия.

3.5. Активация лицензии в изолированной сети

Для активации лицензии XSpider на компьютере, который находится в изолированном от сети Интернет сегменте, необходимо сгенерировать запрос на активацию, разместить его на сервере https://service.maxpatrol.com и, получив ответ, активировать сканер.

Активация сканера XSpider в изолированной сети проводится через специальный веб-интерфейс на сайте https://service.maxpatrol.com (активируемая лицензия должна иметь возможность работать в режиме Offline).

Процедура активации сканера XSpider в изолированной сети через веб-интерфейс:

1 Запустите XSpider. В графическом интерфейсе убедитесь, что установлена опция «Обновление лицензий в Offline - режиме».

2 Нажмите кнопку «Активировать лицензию»  для активации лицензии. Если требуется обновление лицензии нажмите на кнопку «Сформировать запрос на обновление лицензии»  .

3 Сохраните на съемный носитель файлы *.of r с запросом на активацию или обновление лицензии.

4 Загрузите файл запроса (*.ofr) через интерфейс offline-активации лицензий https://service.maxpatrol.com/ (необходимо наличие компьютера, подключенного к сети Интернет, и учетной записи для авторизации на данном ресурсе*).

5 После обработки появится соответствующее сообщение и ссылка для скачивания файла-ответа (*.ofl).

6 Скачайте файл *.ofl по указанной ссылке; имя ofl-файла соответствует имени ofr-файла.

7 Если возможность подключения к сети Интернет отсутствует, необходимо передать любым возможным способом файл запроса (*.ofr) разработчику. В ответ Вы получите файл *.ofl.

8 Чтобы загрузить *.ofl, нажмите кнопку  (импортировать лицензию в режиме offline) на вкладке « Сервер» панель «Лицензии» во вкладке « Настройки».

В случае возникновения вопросов Вы можете связаться со службой технической поддержки по тел. +7 (495) 744-01-44.

*Чтобы получить учетную запись для активации на странице https://service.maxpatrol.com, необходимо зарегистрироваться на сайте технической поддержки компании Positive Technologies (https://support.ptsecurity.ru) и отправить заявку с темой «Получение учетной записи для offline-активации лицензий XSpider». Вы получите учетную запись на указанный в заявке электронный адрес.

3.6. Обновление системы

Для корректной работы системы автоматического обновления необходимо наличие соединения с сервером обновлений (update.maxpatrol.com).

Для обновления переключитесь на закладку «Настройки – Основные» и нажмите кнопку «Обновить» в панели «Обновления».

Внимание! В ходе обновления консоль потеряет соединения с сервером и в течение некоторого времени (одной-двух минут) не сможет подключиться к системе.

3.7. Защита установки

Операционная система и дополнительные компоненты, используемые XSpider, могут содержать различные уязвимости и недочеты в стандартных настройках. Для устранения уязвимостей рекомендуется после установки провести сканирование компьютера, на котором установлен сканер XSpider, и устранить обнаруженные недочеты в соответствии с полученными рекомендациями.

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

3.8. Использование XSpider в виртуальной среде с привязкой к электронным ключам eToken

Использование ключа eToken обеспечивает лицензионную защиту компонентов XSpider при работе в виртуальном окружении. На текущий момент такая возможность официально реализована только для виртуальных машин VMware ESXI 4.1 и Workstation 6.0 и выше.

При использовании других виртуальных машин данная функция реализуется с помощью программного или аппаратного обеспечения типа USB over IP Network.

Компания ЗАО «Позитив Текнолоджиз» обеспечивает техническую поддержку решений, которые базируются только на виртуальных машинах VMware ESXI 4.1 и Workstation 6.0 и выше. Если вы используете решения типа USB over IP Network, по всем вопросам, связанным с работой eToken, необходимо обращаться в службу технической поддержки компании-разработчика этого программного обеспечения.

Наличие постоянно подключенного ключа eToken является обязательным условием для работы XSpider на виртуальной машине.

3.8.1 Порядок использования XSpider с eToken

Для использования ПО XSpider в виртуальной среде необходимо запросить дистрибутив и соответствующую лицензию. Предоставление права использования ПО XSpider осуществляется по лицензионным договорам. Одновременно с передачей права использования ПО XSpider клиенту передается ключ eToken.

При отсутствии у клиента доступа к сети Интернет для инициализации и обновления ПО XSpider, необходимо уведомить об этом разработчика до момента оформления ключа eToken. Разработчик проведет его «привязку» к соответствующей лицензии на стадии формирования дистрибутива ПО XSpider.

Ключ eToken передается клиенту в безвозмездное пользование на весь срок действия лицензии.

В случае утраты ключа eToken по запросу клиента выпускается дополнительный ключ eToken на безвозмездной основе. В этом случае доставка ключа eToken клиенту осуществляется за его счет и с использованием его ресурсов.

В случае повторной и последующей утраты ключа eToken клиент приобретает дополнительный ключ eToken самостоятельно у компании Aladdin (http://www.aladdin-rd.ru/) и передает разработчику для его инициализации. Получение ключа eToken после инициализации осуществляется за счет клиента и с использованием его ресурсов.

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

Клиенты, которые ранее приобрели ПО XSpider и у которых есть необходимость перейти на использование ПО XSpider в виртуальной среде, обращаются в техническую поддержку ЗАО «Позитив Текнолоджиз» с запросом на переоформление действующей лицензии. Одновременно с оформлением соответствующей лицензии формируется ключ eToken. Формирование ключа осуществляется бесплатно. Доставка ключа eToken клиенту осуществляется курьером компании ЗАО «Позитив Текнолоджиз» или по договоренности курьером компании клиента.

Для переноса рабочей инсталляции в виртуальное окружение необходимо дополнительно произвести конвертирование аппаратного сервера в виртуальный (см. раздел Перенос компонентов XSpider с аппаратного сервера в виртуальную среду).

3.8.2 Особенности установки компонентов XSpider с использованием eToken

После получения дистрибутива и ключа eToken можно приступить к развертыванию XSpider в виртуальном окружении. Алгоритм развертывания представлен ниже:

- Подготовьте виртуальную машину на базе VMware ESXI 4.1 или Workstation 6.0 и выше.
- При настройке аппаратных ресурсов VMware необходимо руководствоваться требованиями раздела 2.1 Требования к аппаратному и программному обеспечению.
- Установите XSpider из полученного дистрибутива. Процесс установки необходимо проводить при отключенном ключе eToken. Драйверы для ключа eToken интегрированы в дистрибутив и будут установлены автоматически, при этом события установщика драйверов записываются в конец Setup Log (журнал событий мастера установки системы XSpider). По умолчанию Setup Log расположен в каталоге C:\Program Files\Positive Technologies\ XSpider \server\Logs. Если ПО XSpider устанавливается в каталог, отличный от указанного, то журнал событий расположен в каталоге %путь к установке XSpider %\server\Logs.
- Подключите полученный ранее ключ eToken в USB-порт сервера VMware.
- В разделе “Settings” созданной виртуальной машины необходимо последовательно подключить USB controller и USB device. Если к VMware подключено несколько электронных ключей, необходимо выбрать ключ, полученный от ЗАО “Позитив Текнолоджиз”.

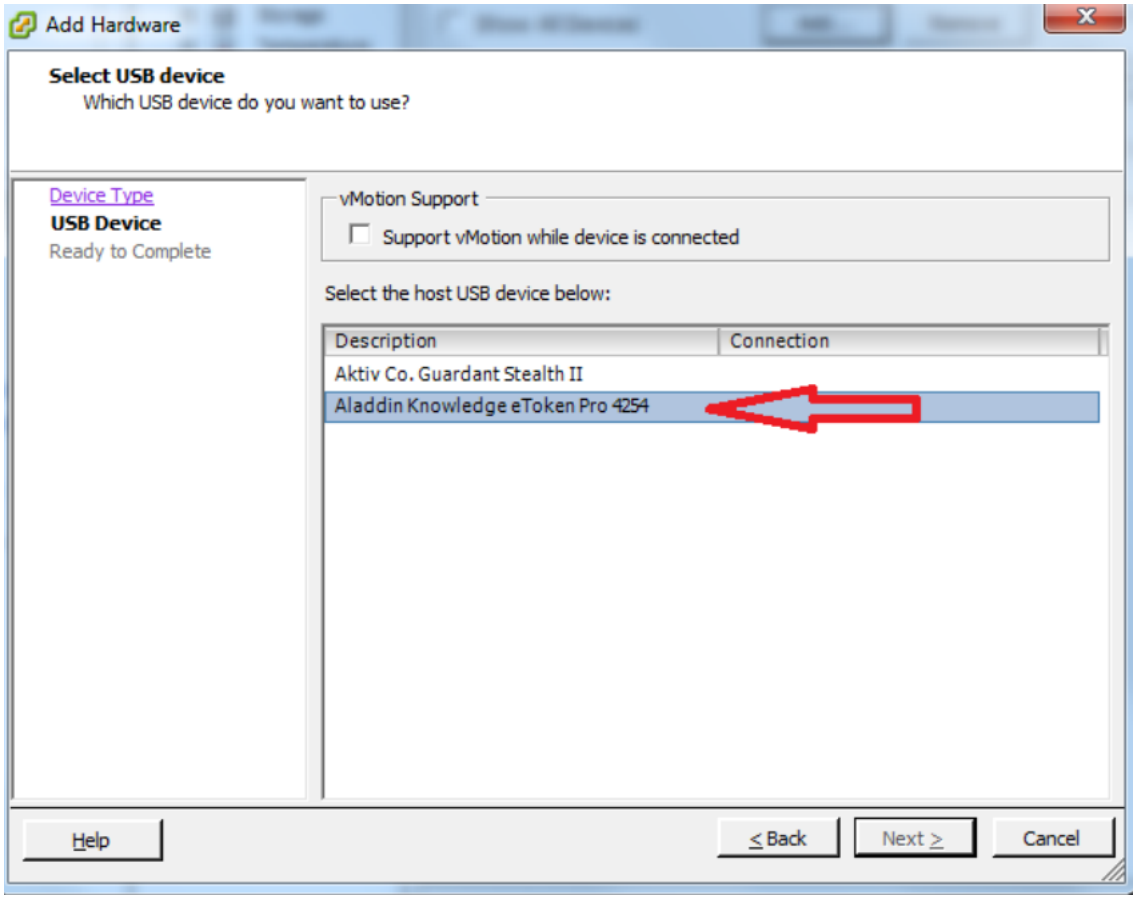


Рис. 3 Выбор электронного ключа

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

- Запустите консоль XSpider. Перейдите на вкладку “Настройки” -> ”Сервер”. Активируйте лицензию XSpider согласно инструкции, приведенной в разделе 3.4 Активация лицензии Руководства администратора системы MaxPatrol. В процессе активации проверяется наличие подключенного ключа eToken и действительной лицензии. В дальнейшем для сохранения работоспособности XSpider требуется наличие постоянно подключенного ключа eToken. В случае отключения ключа eToken XSpider блокирует возможность работы с системой до подключения ключа eToken.

3.8.3 Перенос компонентов XSpider с аппаратного сервера в виртуальную среду

Для переноса компонентов XSpider с аппаратного сервера на виртуальную машину можно воспользоваться утилитой VMware Converter.

Скачать VMware vCenter Converter с официального сайта VMware
http://downloads.vmware.com/d/info/datacenter_downloads/vmware_vcenter_converter_standalone/4_0

Подробно процесс конвертирования описан в документе VMware vCenter Converter Documentation на сайте производителя VMware
http://www.VMware.com/support/pubs/vcc_pubs.html

По вопросам, связанным с конвертированием аппаратного сервера в виртуальный, следует обращаться в службу технической поддержки VMware. Компания ЗАО “Позитив Текнолоджиз” не несет ответственности за возможные проблемы, связанные с использованием утилиты VMware vCenter Convertor.

По окончании процесса конвертирования используйте полученный ранее дистрибутив XSpider с поддержкой eToken для повторной установки системы на виртуальной машине. Помните, что процесс установки должен происходить без подключенного ключа eToken.

В ходе установки используйте следующие параметры:
- режим установки “Переустановить XSpider ”;
- использовать данные предыдущей установки? Ответ – “Да”.

После завершения процесса установки подключите полученный ключ eToken в USB-порт сервера VMware.

В разделе “Settings” созданной виртуальной машины необходимо проверить доступность USB controller и подключить USB device (eToken).

В случае если к VMware подключено несколько электронных ключей, необходимо выбрать ключ, полученный от ЗАО “Позитив Текнолоджиз”.

Запустите консоль MaxPatrol. Перейдите на вкладку “Настройки” -> ”Сервер”. Активируйте лицензию MaxPatrol согласно инструкции, приведенной в разделе 3.4 Активация лицензии. В процессе активации проверяется наличие подключенного ключа

eToken и действительной лицензии. В дальнейшем для сохранения работоспособности XSpider требуется наличие постоянно подключенного ключа

eToken. В случае отключения ключа eToken XSpider блокирует возможность работы с системой до подключения ключа eToken.

3.8.4 Диагностика и решение проблем

При проверке правильности установки драйверов eToken можно воспользоваться стандартными средствами диагностики Windows.

Если устройство не обнаружено, проверьте наличие неизвестных устройств в диспетчере устройств Windows. В случае успешной установки драйверов для eToken вы увидите устройство USB Token в разделе Universal Serial Bus Controllers.

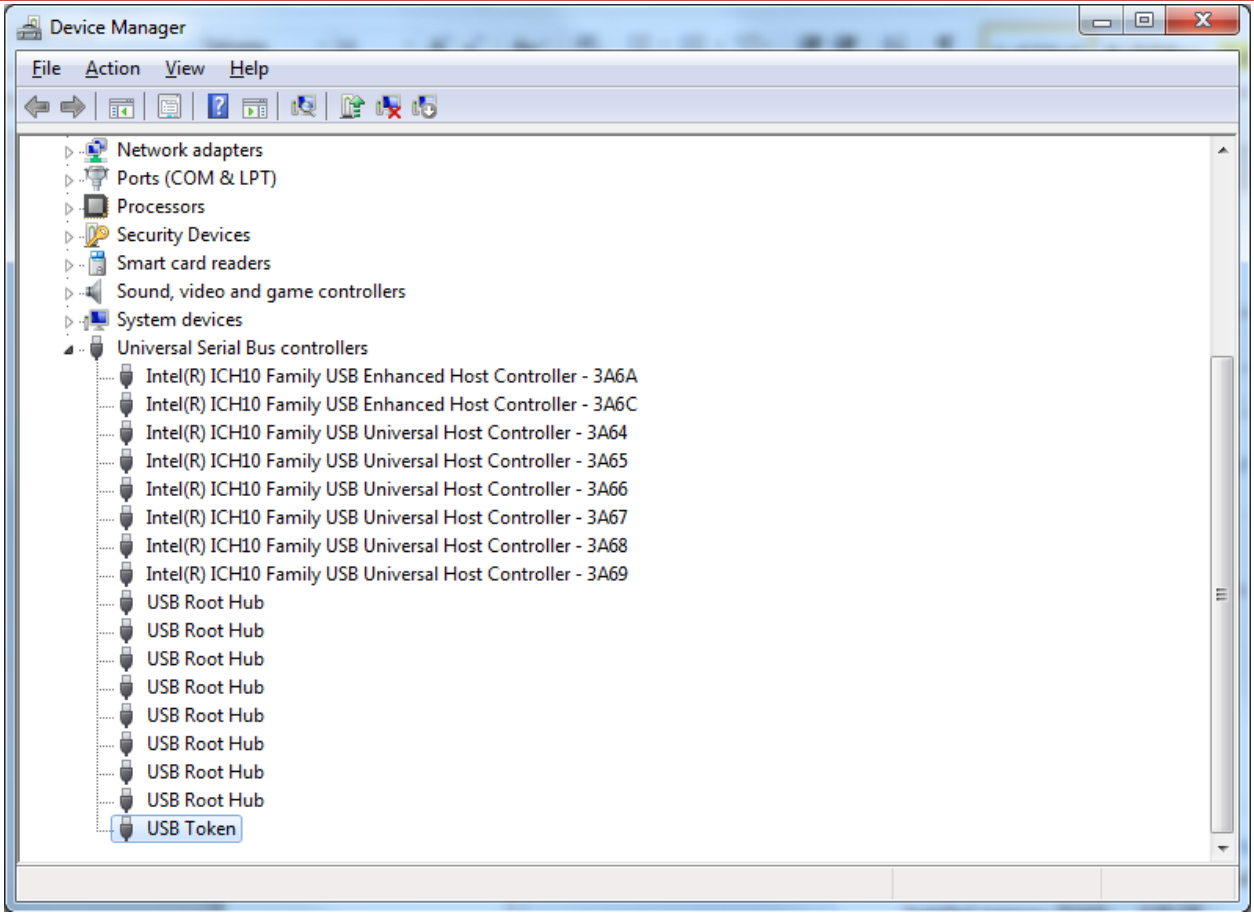


Рис. 4 Диспетчер устройств Windows

В случае отсутствия устройства USB Token, проверьте журнал Setup Log на наличие ошибок. Журнал Setup Log расположен в каталоге установки ПО XSpider. Стандартный каталог: C:\Program Files\Positive Technologies\ XSpider \server\Logs. Если ПО XSpider установлено в каталог, отличный от указанного, то журнал событий расположен в каталоге %путь к установке XSpider %\server\Logs. В случае успешной установки в разделе Driver install start не должно быть статусов Failure.

********** Driver install start ********** Check if the eToken libraries are already installed.

Success.

Creating current directory

Already exit

Current directory: C:\WINDOWS\system32\Setup\PT\eToken

Extracting driver files... Success.

Installing the USB drivers.

Read the .INF file: C:\WINDOWS\system32\Setup\PT\eToken\aksup.inf

Opening the .INF file...

Get the device class GUID and Name... Parsing the manufactures list...

Parsing the devices list: DeviceList...

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

SetupCopyOEMInfA... Success.

Installing the scard drivers.
Read the .INF file: C:\WINDOWS\system32\Setup\PT\eToken\aksifdh.inf
Opening the .INF file...
Get the device class GUID and Name... Parsing the manufactures list...
Parsing the devices list: DeviceList... Creating device info set.
Registering devices.
Updating PnP Devices... Updated: *AKS0001
Updated: *AKS0009
Success.

********** End log **********

В случае возникновения ошибки “отказ в доступе” при работе с компонентами XSpider необходимо убедиться, что ключ eToken подключен и виден для системы.

При возникновении ошибок, связанных с подключением и настройкой eToken, необходимо обратиться в службу технической поддержки компании ЗАО “Позитив Текнолоджиз” (https://support.ptsecurity.ru). Для этого необходимо создать запрос, в котором подробно описать суть проблемы и приложить необходимые файлы журналов: Setup Log и PTkernel.log. По умолчанию эти файлы расположены в каталоге C:\Program Files\Positive Technologies\ XSpider \server\Logs.

Для более детального анализа проблем может также потребоваться файл DxDiag.log. В этом журнале содержится информация, которая позволяет определить присутствие USB-носителя в системе, а также определить версию драйвера, используемого при работе с устройством. Чтобы получить DxDiag.log, необходимо при помощи командной строки запустить утилиту dxdiag.exe и на вкладке System выбрать Save All Information. Полученный файл журнала следует отправить в службу технической поддержки компании ЗАО “Позитив Текнолоджиз”.

Компания ЗАО “Позитив Текнолоджиз” обеспечивает техническую поддержку решений, которые базируются только на виртуальных машинах VMware ESXI 4.1 и Workstation 6.0 и выше. Если вы используете решения типа USB over IP Network, то по всем вопросам, связанным с работой ключей eToken, необходимо обращаться в службу технической поддержки компании-разработчика этого программного обеспечения.

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

4. РАБОТА С СИСТЕМОЙ

4.1. Подключение к серверу

Сканер XSpider автоматически пытаются пройти активацию на глобальном сервере обновлений update.maxpatrol.com при первом подключении. При этом используются стандартные настройки (прямое подключение, порт 2002/TCP). В случае если подключение к сети Интернет ограничено (запрещено использование порта 2002/TCP или используется proxy-сервер), следует отказаться от автоматической активации и изменить настройки подключения к серверу обновлений.

Если система предложит провести автоматическую активацию лицензии, следуют отказаться и в открывшемся окне консоли перейти на закладку Настройки – Соединения. В окне по умолчанию будет присутствовать только одно соединение с сервером update.maxpatrol.com, порт 2002/TCP. Для модификации настроек следует выделить соединение, щелкнуть правой кнопкой мыши и в появившемся контекстном меню выбрать пункт Изменить.

4.2. Сканирование

Для проведения сканирования необходимо создать задачу, указать сканируемые узлы, настроить профиль сканирования и запустить сканирование.

Все основные операции по управлению сканированием осуществляются из вкладки Сканирования (Рис. 5).

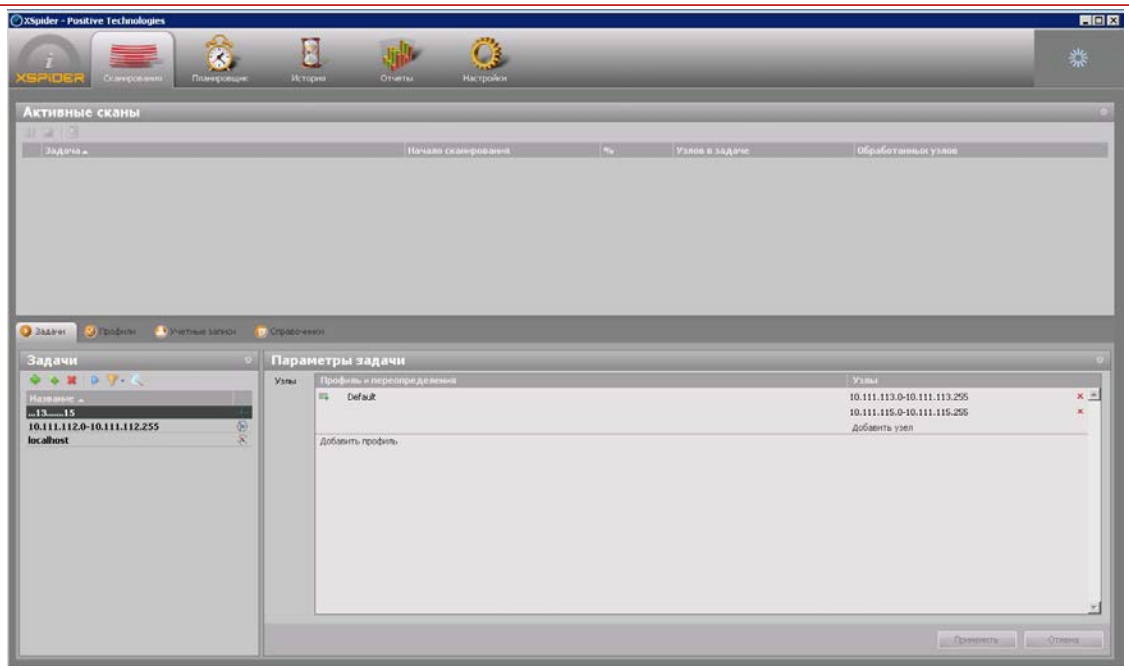


Рис. 5 Вкладка «Сканирование»

Вкладка Сканирования предназначена для отображения информации об активных сканах и управления ими, а также для управления профилями сканирования, которые задают настройки, используемые при сканировании.

4.2.1 Создание задачи

Основные операции по управлению задачами осуществляется из вкладки Задачи, открываемой по умолчанию при переходе на вкладку Сканирования. В панели Задачи во вкладке Задачи отображается список имеющихся в системе задач.

Существует два метода создания задачи: добавление новой и копирование существующей.

Для создания новой задачи:

1. Нажмите кнопку (Добавить задачу) в панели Задачи.
2. Укажите название задачи в поле Название диалогового окна Создать новую задачу (Рис. 6). Только этот параметр является обязательным.
3. Нажмите кнопку OK.

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

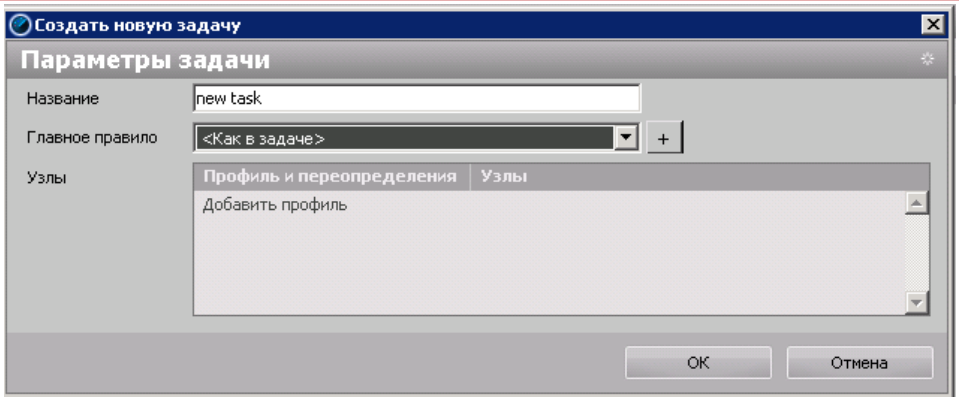


Рис. 6 Диалоговое окно *Создать новую задачу*

Для создания задачи на основе существующей:

1. Выделите копируемую задачу в списке задач.
2. Нажмите кнопку (Копировать задачу) в панели Задачи.
3. Задайте необходимые параметры в диалоговом окне Редактировать задачу (Рис. 7).
4. Нажмите кнопку ОК.

После выполнения этих операций задача появится в списке задач и активируется в окне Параметры задачи.

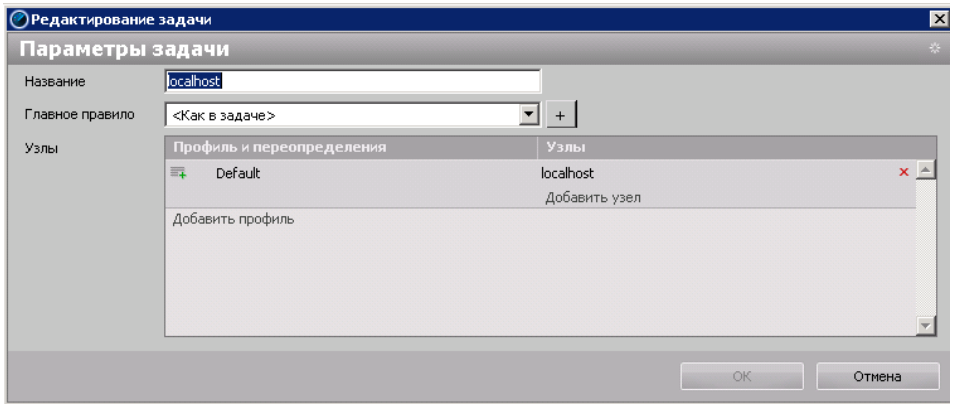


Рис. 7 Диалоговое окно *Редактировать задачу*

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

4.2.2 Настройка профиля сканирования

Настройка профиля сканирования осуществляется в списке Узлы панели Параметры задачи. Для выбора профиля необходимо нажать на ссылку Добавить профиль (Рис. 8).

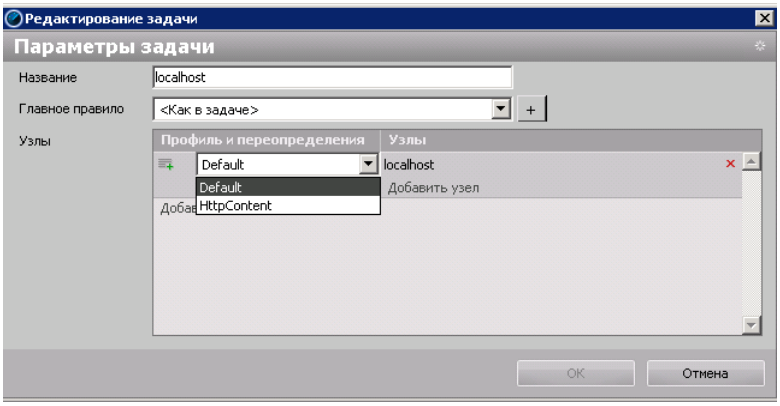


Рис. 8 Добавление профиля

Отображаемые в списке профили сканирования создаются на вкладке Сканирования - Профили. Детальная информация по настройке профиля приведена в разделе Настройка профиля сканирования.

В случае необходимости значения профиля могут быть переопределены для всей задачи или для отдельных узлов/группы узлов. Для добавления переопределения необходимо нажать на кнопку Добавить переопределение . После этого откроется окно редактора профиля и появится возможность модифицировать параметры сканирования. Для удаления переопределений профиля и возвращения к настройкам, указанным в профиле, необходимо нажать кнопку Удалить переопределение .

После переопределения профиля и добавления узлов сохраните изменения, нажав на кнопку Применить.

4.2.3 Список узлов

Ввод сканируемых узлов осуществляется в списке Узлы панели Параметры задачи. Для выбора узла нужно нажать на ссылку Добавить узел (Рис. 9).

В строке редактирования узлов можно указывать IP-адреса, NetBIOS и DNS-имена (FQDN) сканируемых узлов. Существует возможность указывать список узлов с разделителями «;», «,» или «перевод строки».

Для ввода подсетей или диапазонов IP-адресов используется разделитель «-», например, 192.168.0.1-192.168.0.25.

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

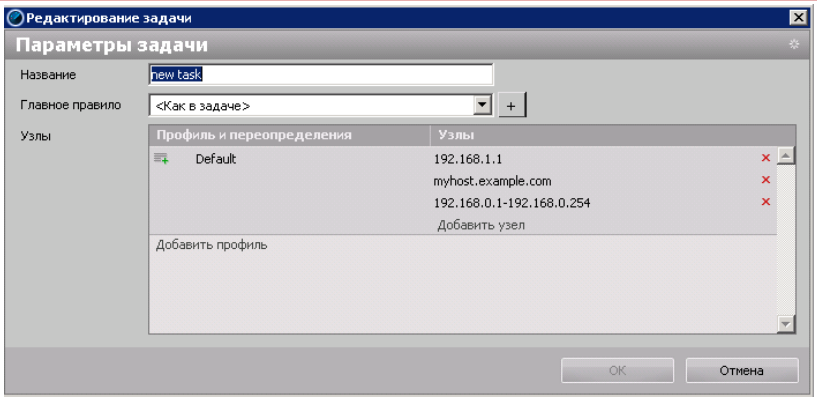


Рис. 9 Добавление узла

Для удаления узла или диапазона адресов необходимо нажать кнопку Удалить узел .

После переопределения профиля и добавления узлов сохраните изменения, нажав на кнопку Применить.

4.2.4 Запуск задачи

В системе XSpider существует несколько режимов запуска задач на выполнение:

- Собственно запуск задачи
- Сканирование выбранных узлов
- Режим Host discovery

Рассмотрим эти режимы подробнее.

Для запуска задачи необходимо выбрать её в списке Задачи и нажать на кнопку Запустить задачу . После этого задача появится в панели Активные сканы.

Существует возможность приостановить или завершить работу той или иной задачи в процессе сканирования. После завершения сканирования результаты работы помещаются в историю сканирования.

4.2.4.1. Сканирование выбранных узлов

Система позволяет запустить сканирование отдельных узлов задачи с параметрами, указанными в соответствующем профиле сканирования. В соответствующем меню нужно выбрать узлы и нажать кнопку «Запустить задачу».

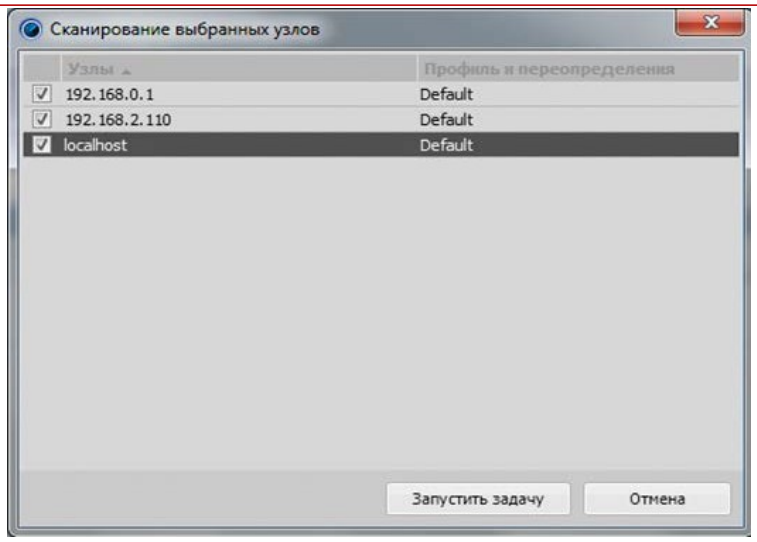


Рис. 10 Сканирование выбранных узлов

4.2.4.2. Режим Host discovery

Режим Host discovery позволяет провести сканирование, направленное только на определение доступности узлов, указанных в задаче, и некоторых ключевых для сканирования параметров. Доступность узлов определяется по следующим параметрам:

- ICMP ping – проверить доступность узла по ICMP ping
- TCP ping – проверить доступность узла по TCP ping
- ICMP и TCP ping - проверить доступность узла по ICMP и TCP ping
- Определение имен – определить имена доступных узлов.

Результаты сканирования можно просмотреть на вкладке «История».

Обратите внимание, что включение любой из указанных опций увеличивает время сканирования.

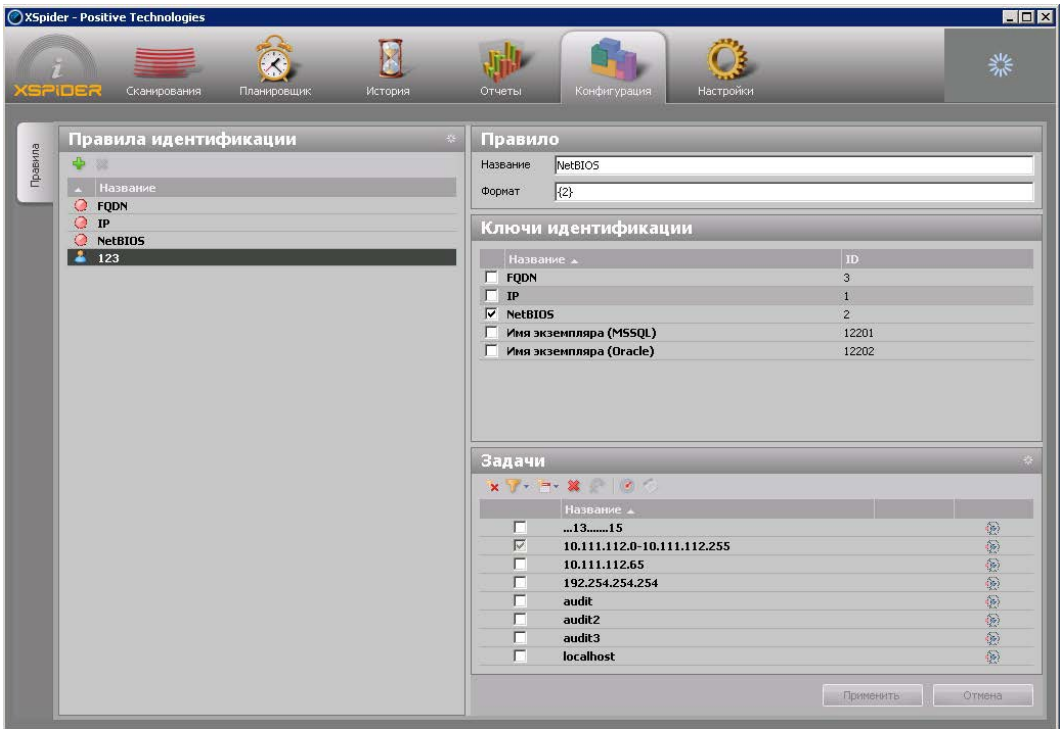
4.2.5 Идентификация сканов в результатах сканирования

Интерфейс управления правилами идентификации сканов разработан для настройки идентификации узлов в результатах сканирования. Эта новая возможность используется для решения двух основных задач:

- разделение в результатах сканирования узлов, представляющих разные сущности, но имеющих при этом одинаковые имена в задаче (различные экземпляры БД на одном узле);
- сопоставление результатов сканирования одного и того же узла в разных сканах, если доступ к нему был произведен по разным именам (например, по IP-адресу и по DNS-имени).

На вкладке Конфигурация – Правила расположен интерфейс, который позволяет создавать правила идентификации сканов.

Обратите внимание: идентификация узлов крайне важна при построении отчетов!



Доступны следующие способы именования узлов в результатах сканирования: как в задаче, по главному правилу. Главное правило – это одно из правил, которые связаны с задачей (для настройки используется закладка Конфигурация - Правила).

При установке новой версии для всех задач, у которых был установлен способ именования узлов в результатах сканирования, соответствующее правило автоматически назначается главным (IP, NetBIOS, FQDN). Например, для задачи со способом именования узлов по IP-адресу будет установлено главное правило «IP». Обратите внимание, что остальные правила по умолчанию НЕ ПРИМЕНИМЫ к задаче. Для того чтобы сделать их применимыми, следует явно установить настроить применимость в интерфейсе правил (панель Задачи, закладка Конфигурация-Правила). Обратите внимание: если правило не применимо к задаче, то ее узлы не могут быть идентифицированы по этому правилу, и отчет с такой идентификацией будет пуст.

4.3. Планировщик задач

Для формираования запланированных действий используется вкладка Планировщик. Возможно выполнить следующие сценарии запуска задачи:

- Последовательный запуск;
- Выпуск отчета;
- Host Discovery.

Для создания нового расписания необходимо на панели инструментов выбрать кнопку  Создать. Откроется новое диалоговое окно Создание расписания, в котором можно выбрать необходимый сценарий запуска и указать параметры его запуска.

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

4.3.1 Сценарий последовательный запуск

Сценарий запуска Последовательный запуск выполняет последовательный запуск задач сканирования по заданному расписанию.

При наступлении интервалов времени работы последовательно запускаются задачи, но следующая задача запускается только при условии, что предыдущая задача выполнена или ее запуск существенно не повлияет на скорость выполнения уже запущенной задачи.

Для данного сценария предусмотрена возможность выпуска отчетов. Генерация и доставка отчетов происходит после каждой завершенной задачи по различным условиям:

- после успешного завершения сканирования,
- после неудачного завершения сканирования,
- после завершения сканирования с ошибкой,
- в любом случае.

4.3.2 Сценарий выпуск отчета

Сценарий запуска Выпуск отчета выполняет генерацию и доставку отчета по последнему проведенному скану в соответсвии с заданным расписанием.

4.3.3 Сценарий Host Discovery

Сценарий Host Discovery позволяет определить доступность узлов до проведения сканирования задачи, что позволяет уменьшть время сканирования, исключив из нее неотвечающие узлы. Запуск сценария Host Discovery осуществляется по заданному расписанию.

При сканировании в режиме Host Discovery возможно включить дополнительные опции:

- проверка узла на запросы ICMP ping,
- проверка узла на запросы TCP ping,
- определение имен для доступных узлов,
- определение ОС, установленных на доступных узлах.

После завершения сканирования для данного сценария возможно производить генерацию и доставку отчетов по различным условиям:

- после успешного завершения сканирования,
- после неудачного завершения сканирования,
- после завершения сканирования с ошибкой,
- в любом случае.

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

4.4. Анализ результатов

Для анализа результатов можно использовать историю сканирования или механизм генерации отчетов.

4.4.1 История сканирования

Для просмотра истории сканирования необходимо перейти на вкладку «История». В этой вкладке отображается список задач, календарь сканирований и список сканов для выбранных задач.

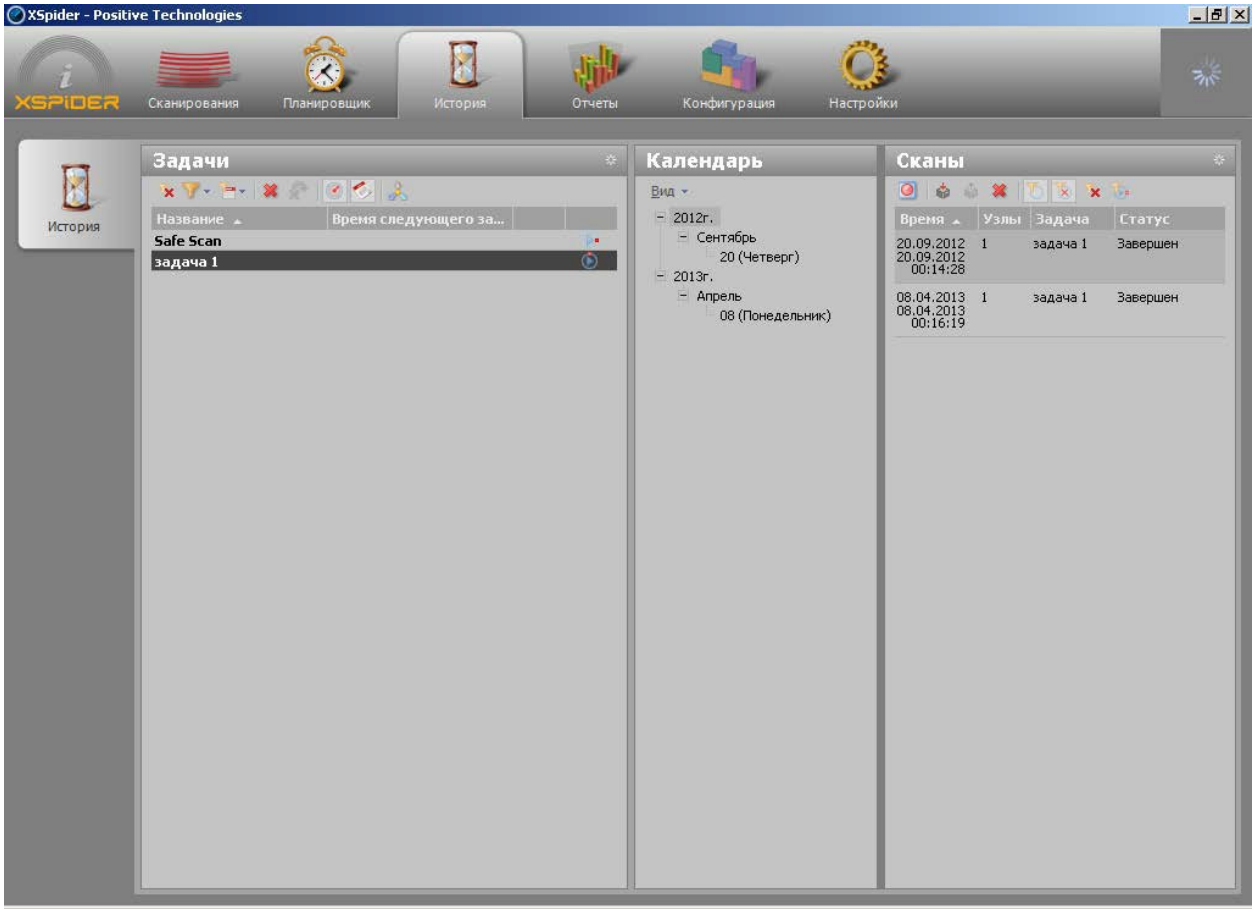


Рис. 11 История сканирований

Для просмотра результатов необходимо выбрать нужный скан в списке сканов и дважды щелкнуть на нем левой кнопкой мыши, либо выбрать пункт Документ сканирования в контекстном меню.

Существует возможность сформировать отчет по текущему скану непосредственно из вкладки История. Для этого на выбранном скане необходимо щелкнуть правой кнопкой мыши и указать в контекстном меню пункт «Отчеты» (Рис. 12).

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

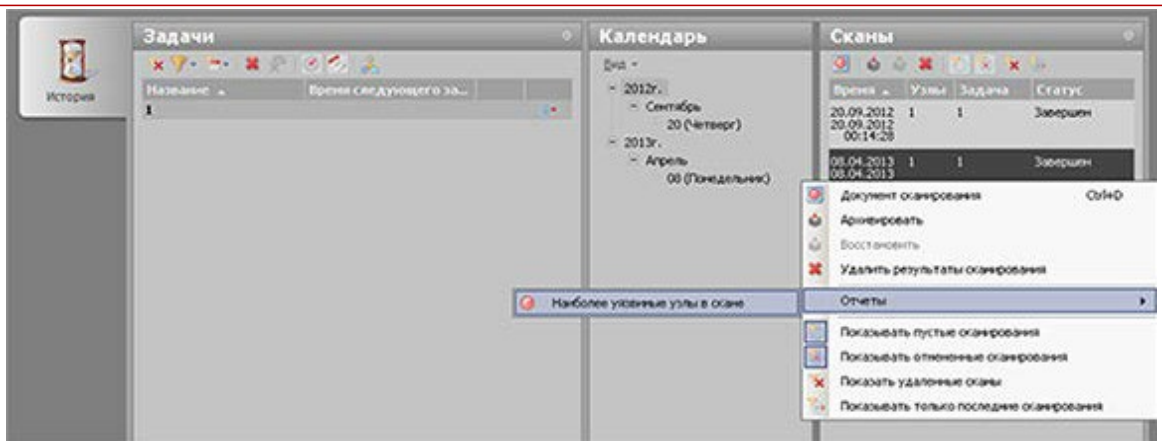


Рис. 12 Создание отчета из вкладки «История»

После генерации отчета отобразится диалоговое окно, позволяющее просмотреть или доставить отчет.

А также существует возможность архивации результатов сканирования. Это функция используется для экономии свободного места на жестком диске. Для архивации одного или нескольких сканов необходимо предварительно выбрать их в списке результатов сканирования и в контекстном меню нажать на кнопку Архивировать. Перед архивацией будет открыто окно с предупреждением о том, что после архивации скана результаты сканирования будут удалены из базы и сохранены в файл. Для просмотра необходимо предварительно разархивировать выбранные сканы, нажав на кнопку Восстановить. Архивацию можно совершать по расписанию.

4.4.2 Генерация отчетов

Система XSpider предоставляет пользователю два способа работы с результатами сканирования. Во-первых, для каждого скана создается документ сканирования, который содержит все подробные данные о результатах сканирования без предварительной обработки, группировки или фильтрации; этот документ динамически обновляется в процессе сканирования. В большинстве случаев такие подробные данные по одному сканированию неудобно использовать, т.к. эти данные могут быть излишне детальными для большинства случаев, а также такое представление данных сильно затрудняет анализ и сравнение.

Кроме того, для работы с данными сканирования пользователь может использовать отчеты. Модуль отчетов в сканере безопасности XSpider позволяет пользователям получать в удобном структурированном виде данные о результатах сканирования одной или нескольких задач (сканов) с возможностью фильтрации и группировки, сравнивать данные различных сканирований, получать общие оценки состояния системы и строить регламентированные отчеты. Отчет позволяет получить требуемые сведения для детального анализа текущей ситуации в системе или для составления общего отчета для руководства. Кроме того, можно выгрузить данные сканирования в отдельный документ и затем использовать для управления системой или для проведения анализа данных.

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

Отчет строится на основании данных сканирования. Пользователь может выбрать необходимый ему тип отчета. Использование конкретного типа зависит от задач, которые пользователь системы хочет решить с помощью отчета (см. раздел 4.4.2.1 Типы отчетов). Пользователь должен выбрать исходные данные – скан(ы), на основании которых будет построен отчет. Данные можно объединять и фильтровать (см. раздел 4.4.2.5 Общая схема построения отчетов). Результаты, которые представлены в виде файла выбранного формата, также можно фильтровать и группировать. Очевидно, что отчеты системы XSpider являются гибким инструментом получения и анализа данных.

В системе существует несколько системных шаблонов отчетов. Это наиболее часто используемые видыотчетов, которые нам удалось выявить. Чтобы воспользоваться ими, пользователь должен задать лишь исходные данные.

Для собственных целей можно создавать свои шаблоны отчетов или отчеты с уже заданными исходными данными, которые будут генерироваться по требованию или по расписанию.

Система XSpider позволяет проводить сканирование и генерировать отчеты по расписанию (см. раздел 4.4.2.2 Выпуск отчетов по расписанию и доставки). Системный планировщик по указанному расписанию запускает задачи, по результатам сканирования которых выпускается указанный отчет. Этот отчет можно сохранить в сетевой папке или отправить по электронной почте указанному адресату.

Дифференциальный отчет используется для сравнения данных сканирования с эталонным сканом. Это позволяет узнать, насколько текущее состояние системы отлично от эталонного и сделать соответствующие выводы.

Обратите внимание, что не рекомендуется строить отчет по данным сканирования 50 и более узлов с детализацией, т.к. генерация таких отчетов не оптимизирована. Попытка построения отчета по большому количеству данных может привести к тому, что время ожидания существенно увеличится или даже к неполучению отчета (в этом случае пользователь получит ошибку генерации отчета).

4.4.2.1. Типы отчетов

В системе XSpider существует 2 типа отчетов. Пользователь выбирает тот из них, который подходит для решения его задачи.

4.4.2.1.1. Информационный отчет

Это отчет по скану или задаче (задачам). Отчет типа «Информация» является наиболее простым. Это презентативный отчет, который позволяет выделить из документов сканирования указанного скана (сканов) только требуемые данные. Следующие задачи можно решить с помощью этого типа отчетов:

- узнать о состоянии транспортов при сканировании;
- провести инвентаризацию с выводом сводной информации или с фильтрацией данных по контрольным спискам, по узлам;

- вывести данные по уязвимостям с различными фильтрами и группировками.

Контрольные списки используются для создания отчетов, в которых производится сравнение списка программного обеспечения или операционных систем, присутствующего на узле или узлах со списком программного обеспечения или операционных систем, заданным пользователем. Контрольные списки задаются в справочнике (вкладка Сканирования - Справочники) с форматом Текст. Каждая строка справочника представляет собой регулярное выражение. Подробнее о синтаксисе, который используется для написания регулярных выражений можно прочитать по ссылке: http://www.boost.org/doc/libs/1_49_0/libs/regex/doc/html/boost_regex/syntax/perl_syntax.html.

Информационный отчет предоставляет следующие дополнительные возможности:

- Для отчета по задачам можно настроить отчет так, что будет автоматически проводиться выбор скана требуемой достоверности сканирования в заданном диапазоне времени сканирования
- Для отчета этого типа следует указать тип информации, которая включается в отчет (например, инвентаризационные данные, уязвимости по способу определения)
- Уязвимости в отчете можно фильтровать по группам, уровням опасности и пр.

4.4.2.1.2. Дифференциальный отчет

Этот тип отчетов применяется для сравнения данных одного или нескольких сканирований и отображения изменений в состоянии узлов. Ключевой параметр данного типа отчетов – выбор способа идентификации узлов в сканах, т.е. механизма, с помощью которого делается вывод о том, что два скана относятся к одному и тому же узлу или к разным узлам. В процессе построения отчета этого типа система XSpider определяет состояние узла в двух заданных интервалах – эталонном и изучаемом – и выводит запрошенную информацию. Дифференциальный отчет позволяет решать следующие задачи:

- вывод результатов сравнения с различными группировками и фильтрами:
- например, только неустраненные уязвимости;
- вывод результатов сравнения с указанием новых данных, изменившихся, устраненными или оставшихся без изменений.

4.4.2.2. Выпуск отчетов по расписанию и доставки

Система XSpider позволяет создавать расписания, по которым будут запускаться сканирования. Когда сканирование завершено, системный планировщик может направить отчет по указанному электронному адресу или сохранить его в указанную сетевую папку. Отчет задается шаблоном, в который планировщик подставляет полученные данные. Благодаря этому механизму можно запускать сканирования в ночное время или в выходные и праздничные дни и получать результаты наиболее удобным способом.

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

4.4.2.3. Создание фильтров в отчете

Фильтрацию узлов возможно осуществить, включив в отчет результаты по выбранному уровню достоверности, а также можно применить дополнительный фильтр, указав узел или диапазон узлов, которые необходимо будет включить или исключить из отчета.

После окончания редактирование нужно сохранить настройки отчета.

4.4.2.4. XSLT-преобразования

В системе XSpider XSLT-преобразования используются для создания отчетов по заранее подготовленным шаблонам в формате XSL. Файлы XSLT-преобразований должны находиться в каталоге, расположенном по пути XSpider\server\Integration\XSLT. Если ПО XSpider установлено в каталог, отличный от каталога по умолчанию, то файлы XSLT-преобразований должны быть размещены в <%Путь к установке XSpider%> server\Integration\XSLT.

Для создания нового отчета необходимо перейти во вкладку Отчеты. Отчет, в котором используются XSLT-преобразования, должен быть в формате XML file. Возможно построить отчет двух типов: Информация и Дифференциальный. В строке Шаблон в выпадающем меню необходимо выбрать требуемый шаблон XSLT-преобразования.

В шаблонах XSLT-преобразований существует возможность задействовать диалоговые параметры, которые впоследствии появляются в диалоговом окне создания отчета в виде нового блока данных – Данные для XML отчета. Под диалоговыми параметрами подразумеваются данные о справочниках или группах (папки). Диалоговые параметры задаются в блок по XSD-схеме. Она расположена в каталоге C:\Program Files\Positive Technologies\XSpider\console\maxpatrol80- dialog-parameters.xsd или в <%Путь к установке XSpider%>console\maxpatrol80- dialog-parameters.xsd в случае, если ПО XSpider установлено в каталог, отличный от каталога по умолчанию. Детальное описание диалоговых параметров можно получить, обратившись в службу технической поддержки компании Positive Technologies по тел. +7 (495) 744-01-44 или https://support.ptsecurity.ru.

4.4.2.5. Общая схема построения отчетов

Для создания отчета по сканированию необходимо перейти в раздел Отчеты. Система XSpider предусматривает следующие типы построения отчетов:

- системные шаблоны;
- пользовательские шаблоны.

Раздел Отчеты делится на две вкладки: Отчеты и Доставки. Во вкладке Отчеты представлен список, как системных шаблонов, так и пользовательских шаблонов существующих в системе. Во вкладке Доставки отображается список существующих в

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

системе доставок. Доставки могут осуществляться как на заданный ящик электронной почты, так и в сетевую папку.

4.4.2.5.1. Системные шаблоны отчетов

Во вкладке Отчеты выбрать необходимый отчет и открыть параметры отчета. Для системных шаблонов отчета необходимо заполнить поля с указанием периода времени и задачи, для которой необходимо построить отчет. В зависимости от типа и назначения отчета нужно будет указать дополнительные параметры. Например, эталонный скан.

4.4.2.5.2. Пользовательские шаблоны отчетов

Пользовательские шаблоны отчетов можно создавать новые или на примере уже существующих шаблонов.

4.4.2.5.2.1. Создание нового пользовательского шаблона отчета

Для создания нового пользовательского шаблона отчета необходимо в диалоговом окне Отчеты на панели инструментов выбрать кнопку - Добавить отчет (Ins).

Откроется новое вспомогательное окно для создания нового пользовательского шаблона отчета. В нем нужно указать Название отчета, Комментарий (если необходимо), Формат (формат, в котором необходимо получить отчет – MHTML file, Adobe Acrobat Document, XML), Язык (язык, на котором будет выпущен отчет) и Тип отчета. В зависимости от выбранного Типа отчета будут указываться параметры.

При создании отчета можно указать только его имя, тип и перечень блоков, а при выпуске отчета указывать задачу и скан, по которому его следует выпускать. В этом случае отчет можно сохранить с другим именем, чтобы впоследствии обращаться к нему непосредственно.

В Информационном отчете указываются параметры исходных данных. Отчет строится по скану или по задаче/задачам. Для отчета по скану далее необходимо выбрать тип данных и выбрать задачу и скан. Для отчета по задаче/задачам нужно указать способ идентификации узлов, тип данных и выбрать скан и задачу. В зависимости от выбранного типа данных (PenTest, Инвентаризация) указываются параметры для отчета. Для типа данных PenTest нужно указать способ представления данных, параметры отчета, топ, задать ограничение количества строк в таблицах и при необходимости используются фильтры узлов. При выбранном типе данных Инвентаризация нужно указать тип данных для вывода, фильтр узлов и задается ограничение количества строк в таблицах.

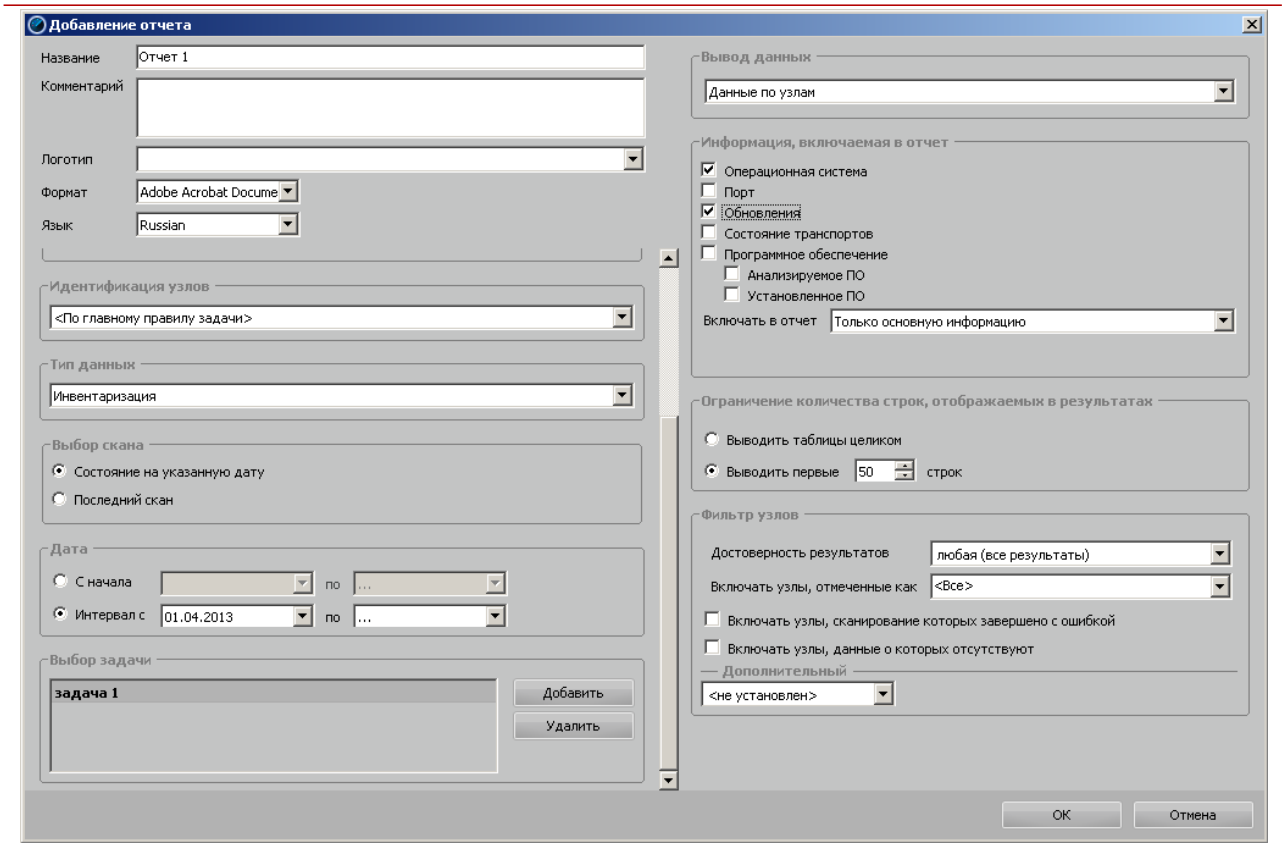


Рис. 13 Создание информационного отчета

В Дифференциальном отчете указываются параметры исходных данных. Отчет строится по скану или по задаче/задачам. Далее необходимо указать способ идентификации узлов в отчете и тип данных (PenTest, Инвентаризация). Для отчета по скану необходимо задать эталонный и изучаемый скан. Для отчета по задаче/задачам требуется выбрать скан, изучаемые данные, эталонные данные. После выбираются изменения, которые учитываются при построении отчета - определение изменений и необходимо задать ограничение количества строк в таблицах. Для типа данных PenTest указываются параметры вывода данных и при необходимости используются фильтр узлов. При выбранном типе данных Инвентаризация нужно выбрать тип отображаемой информации, объекты, задать фильтр узлов, если требуется.

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

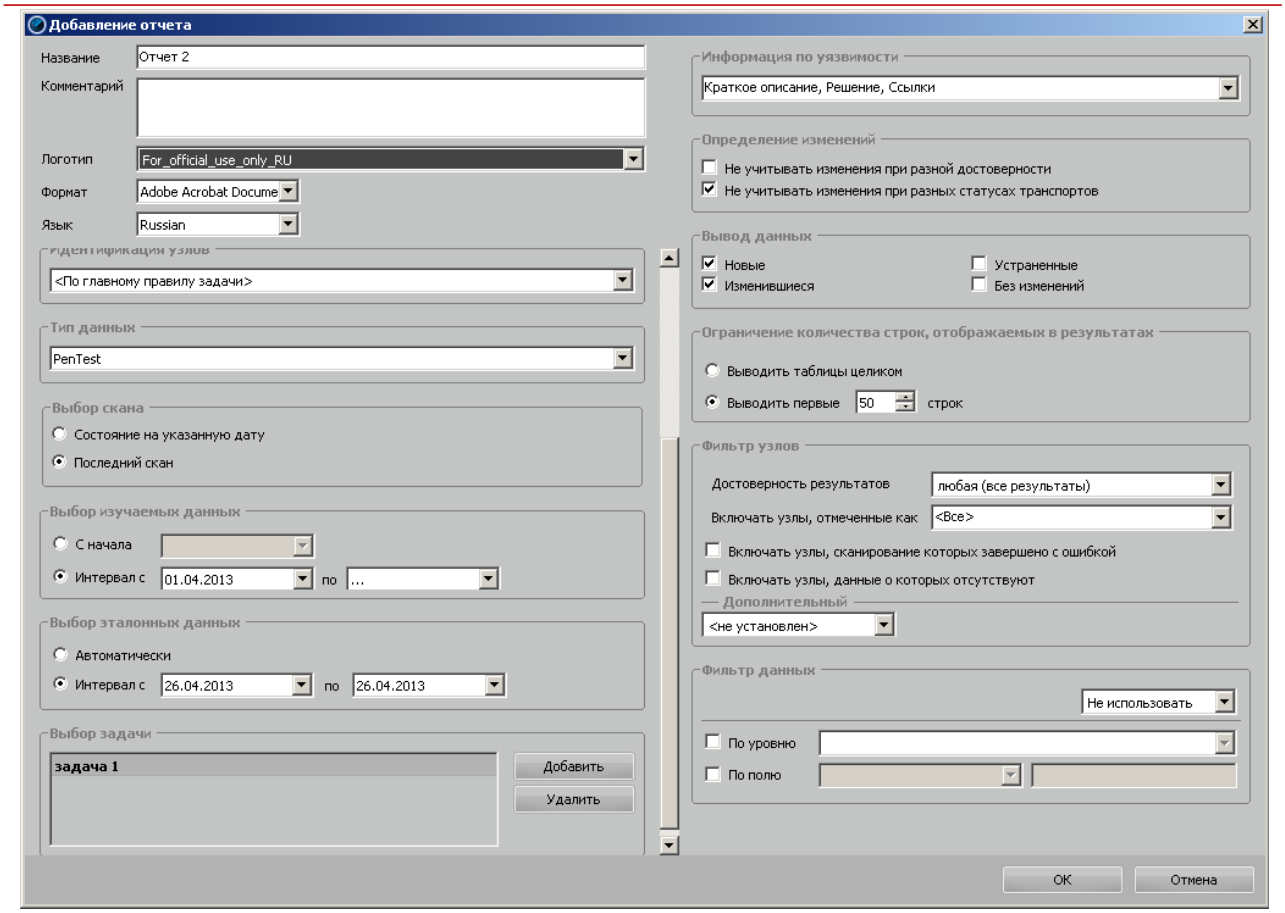


Рис. 14 Создание дифференциального отчета

4.4.2.5.2.2. Создание нового пользовательского шаблона отчета на примере уже существующего шаблона

Для создания нового пользовательского шаблона на примере уже существующего необходимо выбрать исходный шаблон и скопировать его. Для этого в диалоговом окне на панели инструментов выбрать кноп - Копировать (Ctrl+C). открывшемся вн жела изменения для ранее созданного шаблона. После завершения редактирования необходимо сохранить шаблон, нажав кнопку Сохранить.

4.5. Сканирование различных систем

Профиль сканирования определяет логику работы системы. В связи с этим достоверность получаемых результатов в большой степени зависит от корректности его настроек.

В большинстве случаев можно использовать готовые шаблоны профиля, входящие в стандартную поставку системы, модифицируя некоторые параметры (например, учетные записи для сканирования).

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

4.5.1 Редактирование профилей

Основные операции по управлению профилями осуществляется из вкладки Сканирования - Профили. В панели Профили отображается список имеющихся в системе профилей. Панель Навигатор позволяет быстро перемещаться между элементами профиля. В панели Параметры отображается текущее значение элементов профиля и осуществляется их изменение (Рис. 15).

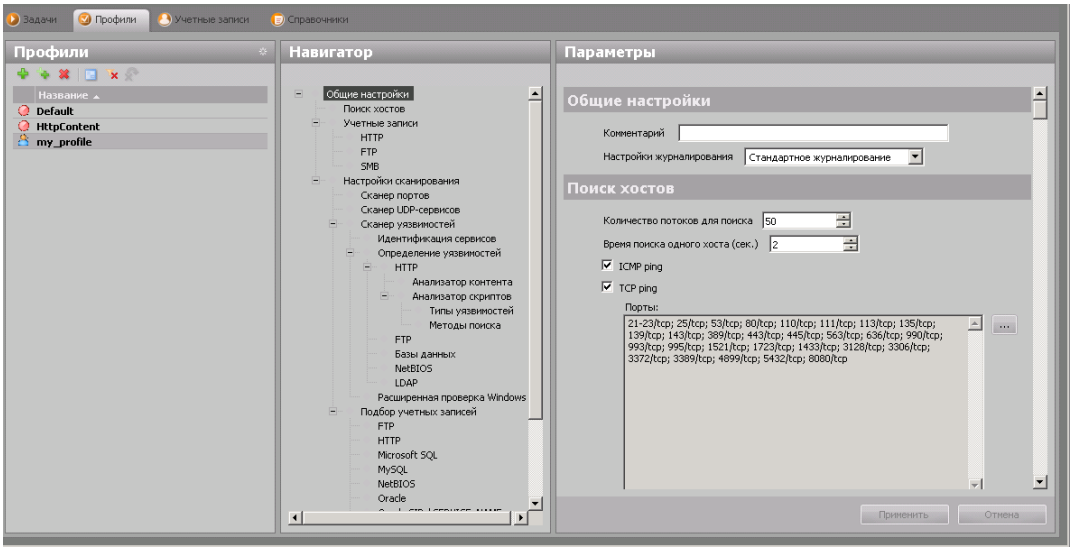


Рис. 15 Вкладка «Профили»

Существует возможность изменения параметров профиля для отдельных узлов задачи через интерфейс редактирований задач.

4.5.2 Определение операционной системы узла

В режиме сканирования PenTest определение операционной системы происходит по механизму баннерных методов определения. Операционная система в момент ее определения может быть только одна (в отличие от всего остального ПО), но при этом существует несколько методов ее определения. Для каждого существует своя точность и достоверность определения. Из-за чего операционная система определяется в конце сканирования.

В ходе проведения сканирования в режиме PenTest можно определить следующие операционные системы:

- Cisco IOS,
- Cisco Nexus 1000/5000/7000,
- Cisco PIX,
- Debian,
- FreeBSD,
- Huawei NodeB,
- Huawei VRP,
- Juniper JUNOS,

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

- Linux,
- Mac OS X,
- Microsoft Windows,
- Netware,
- SuSE Linux,
- StoneGate,
- Sun Solaris,
- Ubuntu,
- VMWare ESX,
- VMWare ESXi.

Для определения операционных систем специальных настроек в профиле сканирования не требуется. Большинство информации, позволяющей определить операционную систему, получается на этапе определения сервисов, но есть исключения и используются следующие методы:

- Regisrty OS Info - получение информации о версии из реестра,
- NTP - получение информации через сервис NTP,
- RDP - получение информации через сервис RDP (в профиле сканирования должен быть включен поиск уязвимостей, либо подбор учетных записей по RDP),
- SNMP - получение информации через сервис SNMP (учетная запись должна быть задана явно или подобрана во время проведения сканирования),
- Nmap OS - получение информации через сервис Nmap (в профиле сканирования должна быть включена функция Использовать Nmap для поиска портов и определения ОС),
- Counter OS Info - метод основан на информации, получаемой во время сканирования о портах или сервисах (данный механизм определения не работает без включенной проверки Поиск уязвимостей).

Методы определения операционных систем представлены в таблице ниже.

Табл. 4 Методы определения ОС

Название ОС	Метод определения
Apple Mac OS X	NTP (123/udp) AFP (548/tcp) Nmap OS Heuristic HTTP OS (80/tcp, 443/tcp)
Cisco IOS	SNMP (1 6 1/u dp) HTTP
Cisco Nexus 1 00 0/ 50 00 /70 00	SNMP
Cisco PIX	SNMP

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

Название ОС	Метод определения
FreeBSD	NTP Nmap OS Heuristic HTTP OS Heuristic SSH OS (22 /t c p) Counter OS Info HTTP SSH (2 2 /t c p)
SunSolaris	SNMP Service Tags (6481/tcp)Dtspcd (6112/tcp) Heuristic SSH OS Nmap OS
Ericsson OSE	SSH FTP (21/tcp)
Microsoft Windows	Registry OS Info NetBIOS (139/tcp, 445/tcp) SNMP Nmap OS LDAP Group (389/tcp) Microsoft RDP (3389/tcp) Heuristic SSH OS Heuristic HTTP OS HTTP UPnP (1900/upd) Counter OS Info
Linux	SNMP NTP Nmap OS Heuristic SSH OS Heuristic HTTP OS mDNS (5353/udp) UPnP Counter OS Info HTTP

Название ОС	Метод определения
Debian	Heuristic SSH OS Heuristic HTTP OS HTTP SSH
Ubuntu	Heuristic SSH OS Heuristic HTTP OS HTTP SSH

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

4.5.3 Настройки профиля

Табл. 5 Настройки профиля

Параметр	Производительность	Достоверность	Безопасность
Поиск хостов			
Количество потоков для поиска	Увеличение значения повышает скорость работы. Рекомендуется 50 для однопроцессорных систем.	На слабых узлах и каналах большое значение может приводить к искажению результатов.	Данная группа настроек может существенно влиять на объем трафика в процессе сканирования. В случае использования слабых каналов связи или устаревшего сетевого оборудования большое количество запросов может привести к возникновению временного отказа в обслуживании.
Время поиска одного хоста	Снижение значения повышает скорость работы.	На слабых каналах низкое значение может приводить к искажению результатов.	
ICMP ping			
TCP ping			
Сканировать неотвечающие хосты	Существенно снижает производительность сканирования в связи с дополнительными затратами на сканирование портов. Особенно на отключенных или заблокированных МЭ узлах.	Отключение опции может приводить к пропуску узлов, не отвечающих на ICMP или TCP-запросы по стандартным портам.	
Учетные записи			

HTTP	Наличие учетной записи для веб-приложений, требующих авторизации увеличивает количество проверок и время работы.	Отсутствие учетной записи для веб- приложений, требующих авторизации, снижает достоверность оценки защищенности.	См. общие замечания по сканированию Web (HTTP)
Использовать авторизацию для всех проверок			
Учетная запись			
FTP	Наличие учетной записи для FTP-серверов, требующих авторизации увеличивает количество проверок и время работы.	Отсутствие учетной записи для FTP- серверов, требующих авторизации снижает достоверность оценки защищенности.	
Использовать анонимный вход			
Использовать учетную запись			
Учетная запись			
SMB		Отсутствие учетной записи снижает достоверность оценки защищенности.	
Настройки сканирования			
Фильтрация уязвимостей		В отчет включаются только уязвимости выбранной группы	

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

Не производить сканирование сетевых принтеров	Отключение опции приводит к блокированию ряда проверок, что снижает время сканирования.	Отключение опции приводит к блокированию ряда проверок, что негативно сказывается на результатах.	В большинстве случаев сетевые принтеры настроены с нарушением требований безопасности, и их сканирование может приводить к негативным последствиям (сброс настроек, печать «мусорных»
Параметр	Производительность	Достоверность	Безопасность
Сканер портов			
Ограничить количество одновременных соединений			
Количество потоков при сканировании портов	Увеличение значения повышает скорость работы. Рекомендуется 50 для однопроцессорных систем.	На слабых узлах и каналах большое значение может приводить к искажению результатов.	Данная группа настроек может существенно влиять на объем трафика при сканировании. В случае использования слабых каналов связи или устаревшего сетевого оборудования большое количество запросов может привести к возникновению временного отказа в обслуживании.
Время ожидания (сек.)	Снижение значения повышает скорость работы.	На слабых каналах низкое значение может приводить к искажению результатов.	
Сканировать весь диапазон TCP-портов (1..65535)	Существенно снижает производительность сканирования в связи с дополнительными затратами на сканирование портов. Особенно на отключенных или заблокированных МЭ узлах.	Включение опции позволяет получить наиболее достоверные результаты сканирования.	
Список портов			

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

Использовать Nmap для поиска портов и определения ОС	Позволяет повысить производительность в режиме сканирования портов.		Поскольку использование данной опции приводит к запуску внешнего приложения с повышенными привилегиями (LocalSystem), необходимо использовать приложение, полученное из доверенного источника. Учтите, что Nmap нельзя использовать для поиска портов на локальном узле, а
Путь к приложению			

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

Параметр	Производительность	Достоверность	Безопасность
Параметры Nmap			
Количество одновременных процессов Nmap			
Сканер UDP-сервисов			
Сканировать UDP порты	В связи с недетерминированностью протокола UDP идентификация UDP- служб может занять продолжительный промежуток времени.	Включение опции позволяет получить наиболее достоверные результаты.	
Сканер уязвимостей			
Искать уязвимости		Если эта опция отключена, то проводится только инвентаризация	Рекомендуется отключать при предварительном сканировании неизвестных систем
Определять операционную систему			
Время обработки TCP-сервисов (сек.)	Снижение значения повышает скорость работы.	На слабых каналах низкое значение может приводить к искажению результатов.	
Время обработки UDP-сервисов (сек.)	Снижение значения повышает скорость работы.	На слабых каналах низкое значение может приводить к искажению результатов.	
Задержка между подключениями к TCP или UDP-портам (сек.)	Снижение значения повышает скорость работы.	На слабых каналах низкое значение может приводить к искажению результатов.	
Идентификация сервисов			

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

Параметр	Производительность	Достоверность	Безопасность
Эвристический метод для определения версий сервисов	Отключение опции повышает скорость работы.	Включение опции позволяет получить наиболее достоверные результаты сканирования.	
Определение уязвимостей			
При некоторых проверках (HTTP прокси, UPnP и т.д.) использовать этот IP-адрес		Для повышения достоверности сканирования данный параметр должен содержать IP-адрес сканера с которым сканируемый узел сможет установить TCP и UDP-соединение.	
Определять уязвимости по баннерам		Повышает количество определяемых уязвимостей, но увеличивает количество ложных срабатываний.	
Определять уязвимости по баннерам в старых		Повышает количество определяемых уязвимостей, но увеличивает количество ложных срабатываний.	
Использовать финальные проверки	Отключение опции повышает скорость работы.	Включение опции позволяет получить наиболее достоверные результаты сканирования.	
Размер буфера для DoS-атак (Кб.)	Увеличение буфера приводит к увеличению продолжительности сканирования.	Возможны ложные срабатывания в случае проблем со связью	
Проверять на известные DoS-атаки	Отключение опции повышает скорость работы.		Проверки могут вызвать отказ в обслуживании системы
Проверять на новые DoS-атаки (эвристический метод)	Отключение опции повышает скорость работы.	Позволяет идентифицировать новые уязвимости методом фаззинга (fuzzing). Возможны ложные срабатывания в случае проблем со связью	Проверки могут вызвать отказ в обслуживании системы

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

Параметр	Производительность	Достоверность	Безопасность
HTTP			
Искать уязвимости в веб-приложениях (поиск по ответу)		Возможны ложные срабатывания	
Искать уязвимости в веб- приложениях (поиск по			
Включить анализатор контента	Существенно увеличивает время сканирования веб-приложений	Отключение механизма приводит к блокированию всех эвристических проверок веб-приложений (Cross- Site Scripting, SQL Injection и т.д.).	Эвристические проверки могут приводить к нарушению целостности (автоматическое заполнение и отправка форм) и доступности тестируемых приложений. В связи с этим, рекомендуется отключать данный параметр при предварительном сканировании
Включить анализатор каталогов	Существенно увеличивает время сканирования веб-приложений	Отключение механизма приводит к блокированию ряда эвристических проверок веб-приложений	
Искать межсайтовый скриптинг в методах Trace и Track			
Другие проверки			
Количество проверяемых на подбор пароля каталогов	Увеличивает время сканирования веб-приложений при наличии функций аутентификации		
Выполнять проверку на			Позволяет идентифицировать

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

Параметр	Производительность	Достоверность	Безопасность
Анализатор контента			
Стартовая страница для анализатора	Параметр позволяет ограничить зону работы эвристических механизмов и снизить затраты		
Не выходить за пределы стартового каталога			
Использовать запрос для стартовой страницы		При использовании сложных схем авторизации и отслеживания сессий данный параметр может использоваться для указания «сырого» HTTP-запроса, позволяющего обратиться к серверу	
Запрос		При использовании сложных схем авторизации и отслеживания сессий данный параметр может использоваться для указания параметров основного запроса, позволяющего обратиться к серверу.	
Дополнительные поля запроса		При использовании сложных схем авторизации и отслеживания сессий данный параметр может использоваться для указания дополнительных полей, позволяющих обратиться к серверу	
Использовать словарь при сборе контента	Увеличивает время сканирования веб-приложений	Отключение механизма приводит к блокированию ряда эвристических проверок веб-приложений	
Искать старые файлы (.old, .bak и др.)	Увеличивает время сканирования веб-приложений	Отключение механизма приводит к блокированию ряда эвристических проверок веб-приложений	

Параметр	Производительность	Достоверность	Безопасность
Искать вредоносный код в страницах			
Время ожидания HTTP-пакетов (сек.)	Снижение значения повышает скорость работы.	На слабых каналах низкое значение может приводить к искажению результатов.	
Максимальное количество проверяемых прикладных сценариев	Снижение значения повышает скорость работы.	Снижение значения негативно сказывается на достоверности работы.	
Количество циклов вложенных проверок	Снижение значения повышает скорость работы.	Снижение значения негативно сказывается на достоверности работы.	
Список дополнительных ссылок			
Список игнорируемых ссылок			Позволяет указать список «опасных» ссылок, работа с которыми может вызвать негативные последствия (формы обратной связи и т.д.).
Анализатор сценариев			
Поиск уязвимостей в GET запросах	Увеличивает время сканирования веб-приложений	Отключение механизма приводит к блокированию ряда эвристических проверок веб-	
Поиск уязвимостей в POST запросах	Увеличивает время сканирования веб-приложений	Отключение механизма приводит к блокированию ряда эвристических проверок веб-	
Сложная проверка прикладных сценариев	Увеличивает время сканирования веб-приложений	Отключение механизма приводит к блокированию ряда эвристических проверок веб-	

Параметр	Производительность	Достоверность	Безопасность
Сложная проверка прикладных сценариев (всех)	Увеличивает время сканирования веб-приложений	Отключение механизма приводит к блокированию ряда эвристических проверок веб-приложений	
Типы уязвимостей			
SQL инъекция	Увеличивает время сканирования веб-приложений	Отключение механизма приводит к блокированию ряда эвристических проверок веб-приложений	Возможно негативное влияние на целостность сервера в случае наличия уязвимостей SQL Injection в операторах Update или Insert.
Удаленное выполнение команд			
Просмотр произвольных файлов			
Межсайтовый скриптинг (XSS)			
Server Side Includes (SSI)			
HTTP Response Splitting			
Выполнение кода, взятого с удаленного сервер			
Методы поиска			
Referer	Увеличивает время сканирования веб-приложений	Отключение механизма приводит к блокированию ряда эвристических проверок веб-приложений	
User-Agent			
Cookie			
FTP			
Искать скрытые директории	Увеличивает время сканирования FTP-серверов		
Базы данных			

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

Параметр	Производительность	Достоверность	Безопасность
Проверять уязвимости в NetBIOS и Registry	Увеличивает время сканирования Windows-систем		
Расширенная проверка Windows			
Выполнять расширенную проверку Windows	Увеличивает время сканирования Windows-систем.	Включение опции позволяет получить наиболее достоверные	
Учетная запись			
Имя домена			
Предварительная провера доступности транспортов	Уменьшает время разбора ситуаций при некорректно указанной учетной записи или		
Максимальное время проверки ключевых портов (сек)	Снижение значения повышает скорость работы.	На слабых каналах низкое значение может приводить к искажению результатов.	
LDAP			
Максимальное количество записей RDN (Relative Distinguished Name) первого уровня	Увеличивает время сканирования LDAP		
Максимальное количество атрибутов в каждом RDN (Relative Distinguished	Увеличивает время сканирования LDAP		
Подбор учетных записей			
Подбор учетных записей для различных протоколов	Существенно увеличивает время сканирования систем	Отключение данных функций блокирует проверки стойкости паролей.	Подбор учетных записей может блокировке учетных записей. В связи с этим, рекомендуется отключать данный параметр отключать при предварительном сканировании неизвестных систем.

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

4.5.4 Сканирование

4.5.4.1. Общие настройки

Сканирование направлено на получение оценки защищенности со стороны внешнего злоумышленника. Ниже приведены основные характеристики этого процесса:

- использование минимальных привилегий по отношению к тестируемой системе (анонимный доступ или доступ уровня пользователя);
- идентификация и анализ уязвимостей серверного программного обеспечения;
- эвристические алгоритмы идентификация типов и версий сетевых служб по особенностям протоколов;
- механизмы защиты от ложных срабатываний и уточнения наличия уязвимостей;
- поиск уязвимостей и отсутствующих обновлений Microsoft Windows без использования учетной записи;
- эвристический анализ веб-приложений;
- проверка стойкости паролей.

Ниже приведены подробные описания некоторых настроек профиля сканирования.

4.5.4.2. Сканер портов

Основой сканирования является сканер портов, который позволяет идентифицировать доступные на узле сетевые службы. Пользователь имеет возможность настраивать параметры производительности, а также указывать сканируемый диапазон.

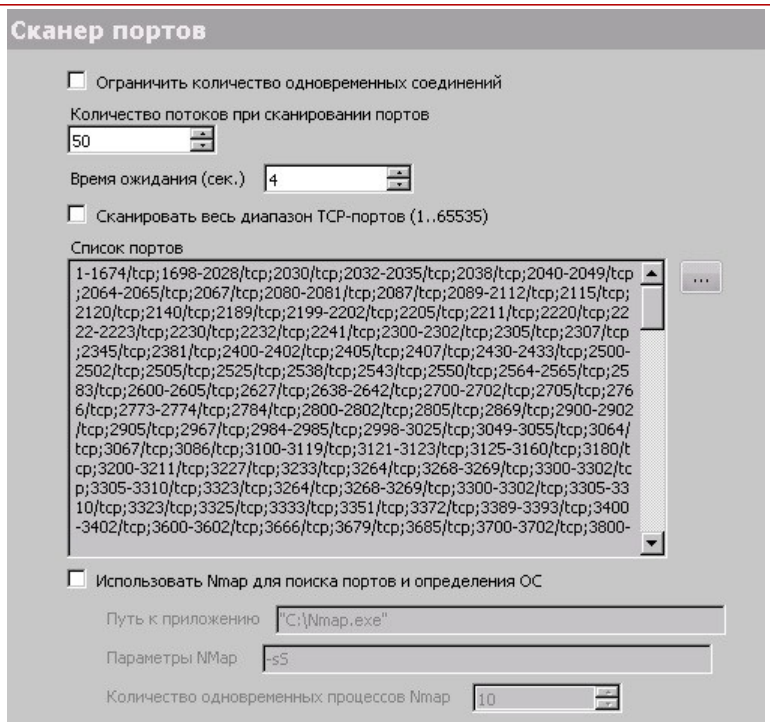


Рис. 16

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

Для оптимизации сканирования можно задействовать внешние сканеры, такие как Nmap. Использование Nmap позволяет значительно ускорить сканирование портов в ходе инвентаризации. Для работы этой функции на узле, на котором установлен сканер XSpider, должен располагаться сканер Nmap, путь к которому указывается в профиле сканирования. При необходимости можно задавать и дополнительные опции. Учтите, что Nmap нельзя использовать для поиска портов на локальном узле, а также то, что Nmap может работать некорректно, если сетевому интерфейсу назначено несколько IP-адресов. Данное ограничение связано с тем, что Nmap пытается использовать только первый IP-адрес сетевого интерфейса.

Для идентификации доступных UDP-служб используются специализированные эвристические алгоритмы. Необходимость применения этих алгоритмов связана с особенностями протокола UDP, не позволяющего определить доступность порта в рамках протокола транспортного уровня.

Для уменьшения времени сканирования можно ограничивать список проверяемых сервисов UDP.

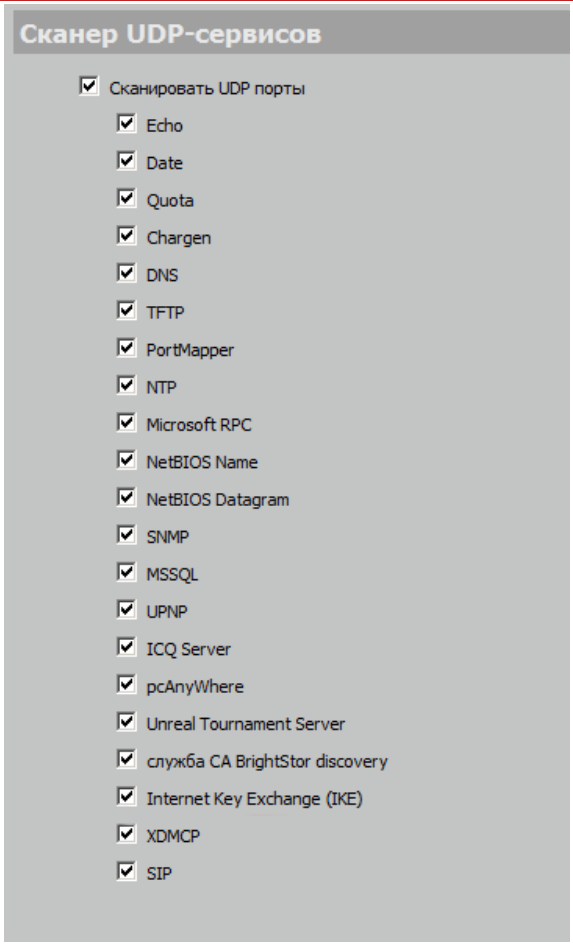


Рис. 17

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

4.5.4.3. Безопасность сканирования

Поскольку сканирование может вызвать временный отказ в обслуживании плохо сконфигурированных систем, рекомендуется проводить предварительную подготовку.

Как правило, процесс сканирования разбивается на два этапа:
инвентаризационный и производственный.

В ходе инвентаризационного сканирования отключаются все эвристические механизмы, подбор паролей и потенциально опасные проверки. Это позволяет получить базовую информацию о системах с минимальным риском возникновения негативных последствий.

Как правило, в ходе инвентаризационного сканирования рекомендуется использовать следующие настройки:

- Не производить сканирование сетевых принтеров – включено;
- Проверять на известные DoS-атаки – отключено;
- Проверять на новые DoS-атаки (эвристический метод) – отключено.
- HTTP - Включить анализатор контента – отключено;
- HTTP - Включить анализатор директорий – отключено;
- Подбор учетных записей – подбирать учетные записи – отключено.

В ходе производственного сканирования данные опции могут быть задействованы с учетом возможных негативных последствий.

4.5.4.4. Подбор паролей

Система XSpider поддерживает подбор паролей для следующих групп сетевых служб и протоколов:

- Протоколы электронной почты
  - SMTP
  - POP3
- Службы передачи файлов
  - SMB
  - FTP
  - HTTP
- Протоколы удаленного управления
  - Telnet
  - SNMP
  - Microsoft RDP
  - SSH
  - VNC
  - Radmin
- Базы данных
  - Microsoft SQL
  - Oracle
  - Oracle SID/ SERVICE_NAME
  - MySQL

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

4.5.4.5. Настройки профиля

Чтобы задействовать механизм подбора паролей той или иной службы необходимо явно указать это в профиле сканирования. Для этого в разделе «Профиль сканирования – Настройки сканирования – Подбор учетных записей» профиля сканирования выбирается соответствующий протокол. Если функции подбора паролей для него реализованы, то в окне настройки будут присутствовать связанные опции, например, «использовать словарь». В случае необходимости, подбор паролей может быть отключен для всех протоколов с помощью отключения опции «Подбирать учетные записи».

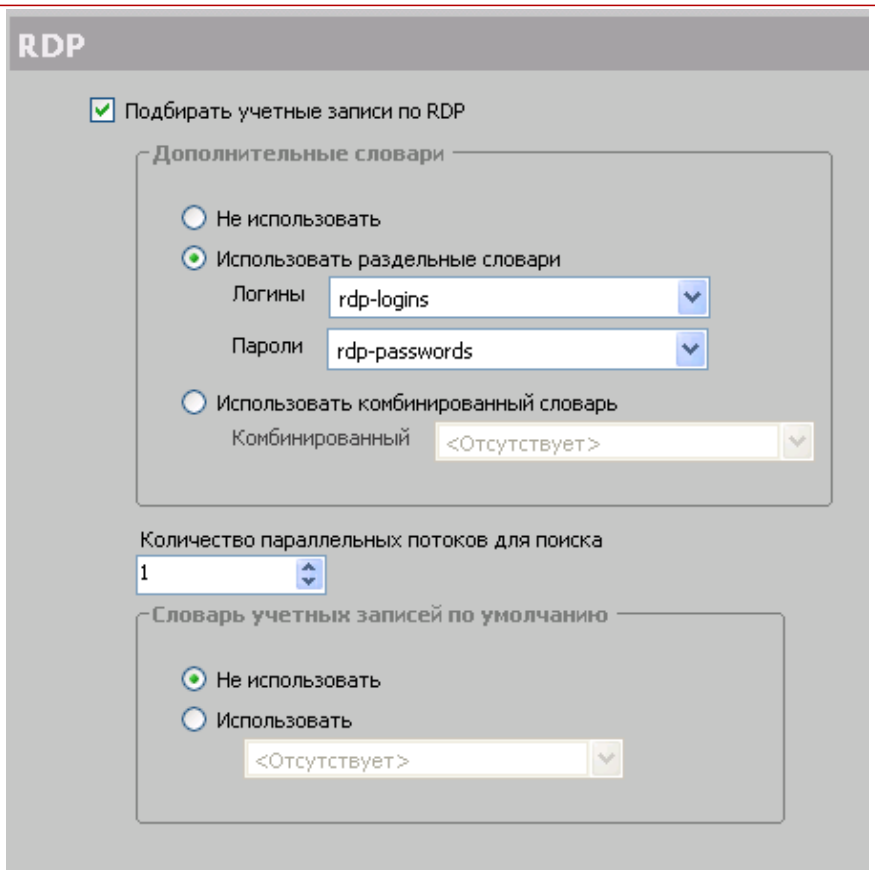


Рис. 18

Расширенные словари представляют собой текстовые файлы, содержащие имена пользователей и пароли. Словари сохраняются в разделе «Справочники» закладки «Сканирования».

Определено три типа словарей:

- логины – содержит имена учетных записей;
- пароли – содержит пароли;
- комбинированный – содержит сочетание имен пользователей и паролей.

В стандартную поставку входят различные справочники распространенных паролей, включая стандартные пароли для различных систем и популярные пароли, полученные командой Positive Technologies в ходе тестов на проникновение и аудитов безопасности.

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

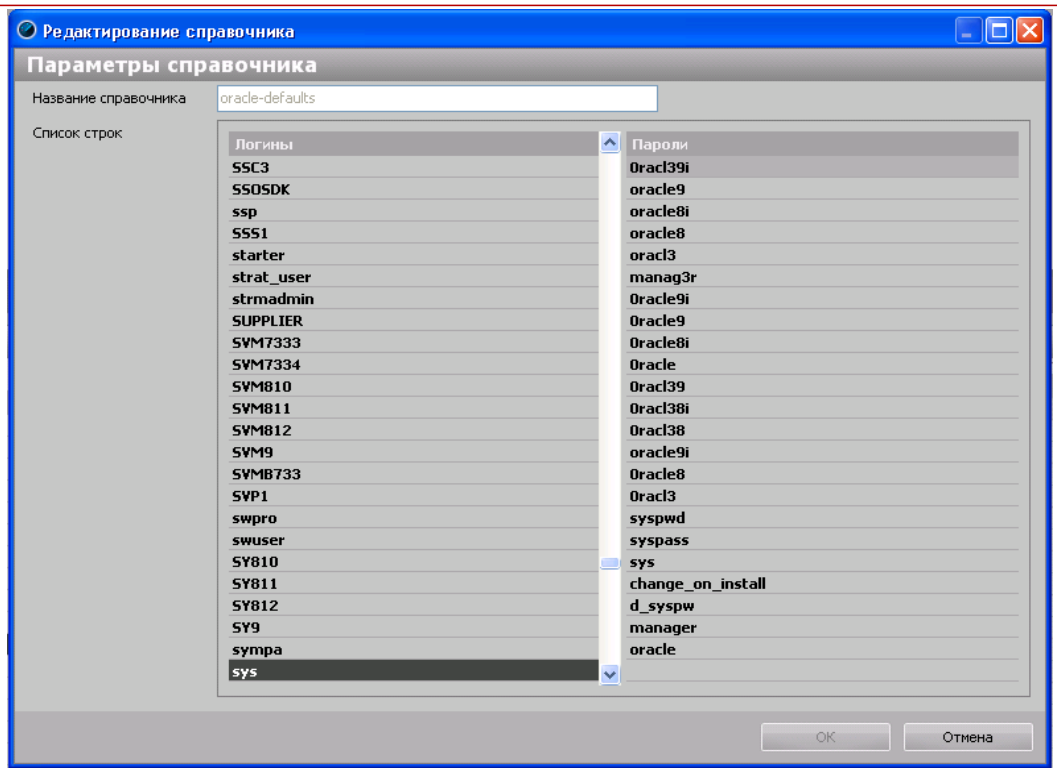


Рис. 19 Параметры справочника

Для большинства протоколов справочники учетных записей и паролей разнесены. Исключением являются SNMP (в протоколе не предусмотрено использование имени пользователя) и Oracle в связи со спецификой работы данной группы проверок.

4.5.4.6. Работа системы

Если в ходе идентификации приложений XSpider обнаруживает сетевую службу, для которой реализован механизм подбора паролей, система строит список учетных записей, подлежащих перебору. Список учетных записей формируется на основе встроенных данных, файлов словарей (если эта опция задействована) и ранее обнаруженных логинов.

Для поиска учетных записей пользователей используются различные механизмы, такие как «NULL Session» в Windows.

Затем определяется поддерживаемый сервером механизм аутентификации. Если сервер поддерживает несколько методов, выбирается наиболее эффективный с точки зрения подбора.

Следующим этапом является непосредственно подбор пароля. В результате в отчете могут появляться подобранные имена пользователей и паролей. В некоторых случаях XSpider снижает степень риска, связанного с уязвимостью. Это означает, что по тем или иным причинам аутентификация была успешна, но войти в систему не удалось. Характерной ситуацией является попытка удаленного подключения в Windows XP SP 2 от имени учетной записи с пустым паролем или учетных записей, для которых ограничен интерактивный вход по протоколу Remote Desktop (RDP).

Результаты проверок передаются между модулями подбора для различных протоколов. Например, если при работе с NetBIOS был получен список пользователей и подобран пароль пользователя user, эти данные будут использованы в ходе подбора паролей к службе RDP данного сервера.

4.5.4.7. Безопасность сканирования

Использование подбора паролей в ходе сканирования может вызывать негативные последствия. Наиболее распространенной ситуацией является блокирование учетных записей в доменах Active Directory. Если сканер сумел получить список пользователей, и количество тестируемых паролей превышает максимальное число неудачных входов в систему, то заблокированными могут оказаться все учетные записи кроме учетной записи администратора.

В сканер встроены механизмы, позволяющие определить, что в системе задействован механизм блокировки учетных записей. Не смотря на это, в подобной ситуации рекомендуется отключать функции подбора паролей.

4.5.4.8. Сканируемое программное обеспечение в ОС Windows

В ОС Windows XSpider осуществляет сканирование и проверку на наличие уязвимостей в программном обеспечении и сервисах для:

- Microsoft Windows;
- Microsoft Updates;
- Microsoft SQL Server;
- Microsoft Internet Explorer;
- Microsoft Windows MDAC;
- Microsoft Internet Information Services;
- Microsoft WINS Server;
- Microsoft DNS Server;
- Microsoft Windows Media;
- Microsoft ESMTP MAIL Service;
- Microsoft XML Core Services.

В режиме расширенных проверок система XSpider идентифицирует уязвимости в Microsoft SQL Server. Эти уязвимости могут быть устранены установкой исправлений. Но уязвимости, связанные с конфигурацией обнаружены не будут.

4.5.5 Сканирование веб-приложений

Одной из отличительных особенностей сканера XSpider является наличие модуля эвристического анализа веб-приложений. Модуль позволяет определять наиболее распространенные уязвимости прикладных систем, построенных с использованием веб-технологий. Использование проверок, спроектированных признанными экспертами отрасли, позволяет проверять не только распространенные системы, такие как Oracle Application, Microsoft Sharepoint, но и приложения собственной разработки.

4.5.5.1. Обзор возможностей

В части анализа веб-приложений XSpider поддерживает следующие возможности:

- автоматическое определение веб-приложений на произвольных портах;
- анализ приложений, защищенных SSL/TLS;
- автоматический индексатор сайта с поддержкой функции поиска скрытых каталогов и резервных копий файлов (Forced Browsing);
- поддержка аутентификации типа Basic и нестандартных схем аутентификации;
- автоматическое отслеживание сессий;
- обработка Javascript и других клиентских расширений;
- поиск уязвимых и вредоносных сценариев (например,php-shell) по содержимому страницы;
- эвристическое определение основных типов уязвимостей в веб-приложениях,
- определение уязвимостей в полях заголовка HTTP-запроса.

4.5.5.2. Настройка профиля

Залогом качественного сканирования является правильно настроенный профиль. Профиль определяет логику работы сканера, а также используемые методы поиска уязвимостей.

4.5.5.2.1. Настройка индексатора сайта

Для того чтобы задействовать механизмы поиска уязвимостей, прежде всего, необходимо включить функцию анализатора контента (Профиль сканирования – Настройки сканирования – Сканер уязвимостей – Определение уязвимостей – HTTP – включить анализатор контента).

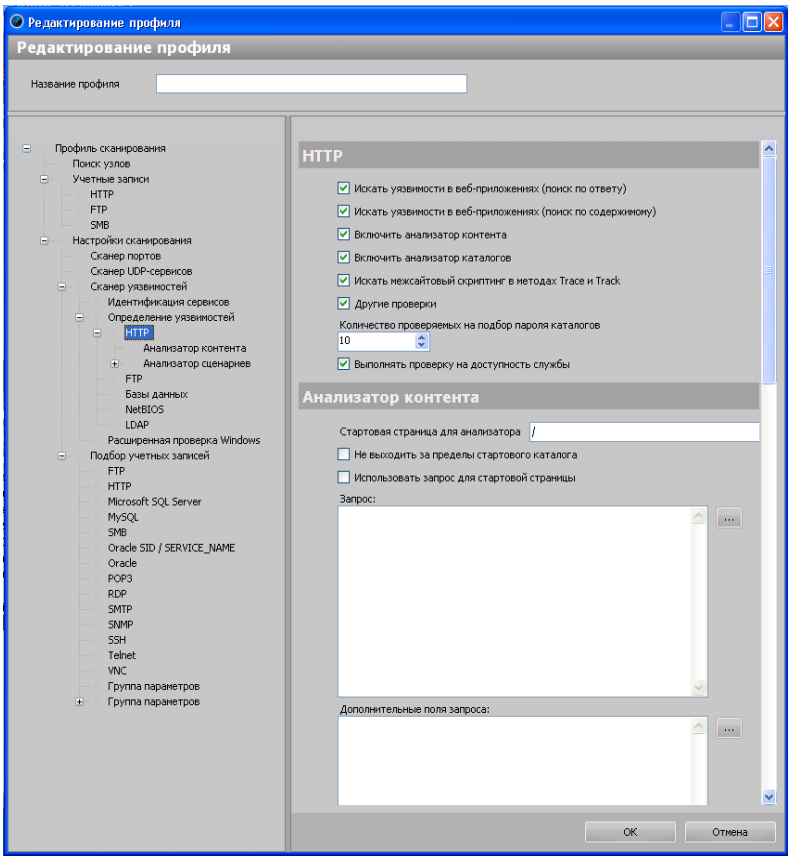


Рис. 20 Редактирование профиля

Также в этом разделе расположена опция «включить анализатор директорий», которая задействует механизмы определения возможностей просмотра содержимого и записи в директории веб-сервера.

Раздел «Анализатор контента» (Профиль сканирования – Настройки сканирования – Сканер уязвимостей – Определение уязвимостей – HTTP – Анализатор контента) содержит основные настройки индексатора.

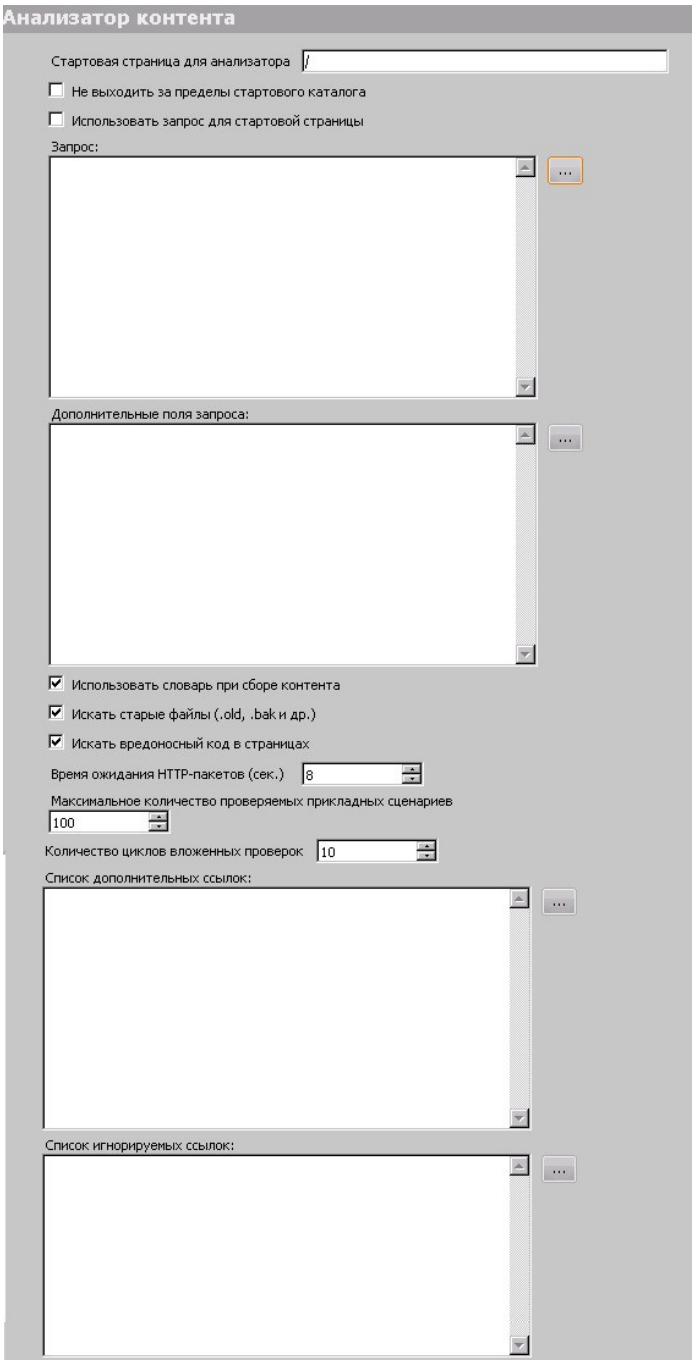


Рис. 21 Анализатор контента

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

Параметр «стартовая страница для анализатора» позволяет указать, с какого из разделов веб-сервера необходимо начать индексацию. Если задействована опция «не выходить за пределы стартовой директории», то сканер будет анализировать только сценарии, находящиеся по указанному пути и ниже. Использование этих настроек полезно, когда необходимо проанализировать конкретный раздел веб- сервера или отдельный сценарий. Кроме того, с их помощью можно разделить проверку больших веб-серверов на несколько задач, что облегчает последующий анализ результатов. Параметр «Запрос» относится к механизмам аутентификации и будет рассмотрен далее.

Опции «использовать словарь при сборе контента» и «искать старые файлы» включают механизм поиска скрытых файлов и папок. Поиск проводится по обширному встроенному словарю, содержащему распространенные имена файлов и расширения. Данный механизм, несмотря на свою простоту, может быть весьма эффективным средством. Экспертам Positive Technologies приходилось сталкиваться с ситуациями, когда простой подбор по именам позволял получать доступ к базам данных сервера (например, /database/database.mdb) или к резервным копям исходных текстов сайтов.

Параметр «Список дополнительных ссылок» содержит пути к каталогам и сценариям, которые должны быть добавлены к спискам проверяемых. Данная опция полезна для проверки веб-сайтов, использующих сложные для автоматического анализа технологии на стороне клиента (например, Java, Flash и т.д.). Для сбора списка сценариев в этом случае можно использовать различные HTTP-снифферы или proxy-серверы, например, WebScarab (http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project). Также к индексатору относится файл «Список игнорируемых ссылок». В него заносятся пути и сценарии, которые не должны обрабатываться индексатором, и, соответственно, поиск уязвимостей в них осуществляться не будет.

Эти настройки могут быть использованы с различными целями. Например, если сайт реализует собственный механизм аутентификации, сюда могут быть занесены сценарии выхода из системы, чтобы сканер не прерывал собственную сессию. Также сюда могут быть внесены сценарии, автоматическое обследование которых может вызвать нежелательные последствия. Например – привести к передаче большого количества сообщений электронной почты или SMS. Однако, по мнению Positive Technologies, использование таких сценариев без дополнительных тестов Тьюринга является уязвимостью класса «Недостаточное противодействие автоматизации» (Inefficient Anti-Automation).

4.5.5.2.2. Механизмы аутентификации

Настройки аутентификации расположены в разделе «Профиль сканирования – Учетные записи – HTTP». Здесь можно указать имя пользователя и пароль, используемый для аутентификации типа Basic.

Включение опции «использовать расширенные словари логинов и паролей» в разделе «Профиль сканирования – Настройки сканирования – Подбор учетных записей – HTTP» задействует механизм подбора паролей.

В случае если сервер использует собственные механизмы аутентификации, можно использовать один из двух вариантов.

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

Первый из них – использование собственного стартового запроса (Профиль сканирования – Настройки сканирования – Сканер уязвимостей – Определение уязвимостей – HTTP – Анализатор контента - Запрос). В этом случае в поле указывается HTTP-запрос, используемый сканером при первом обращении к сайту. Получить содержимое запроса можно с помощью любого сетевого анализатора или генератора HTTP-запросов, такого как TamperData для Mozilla Firefox.

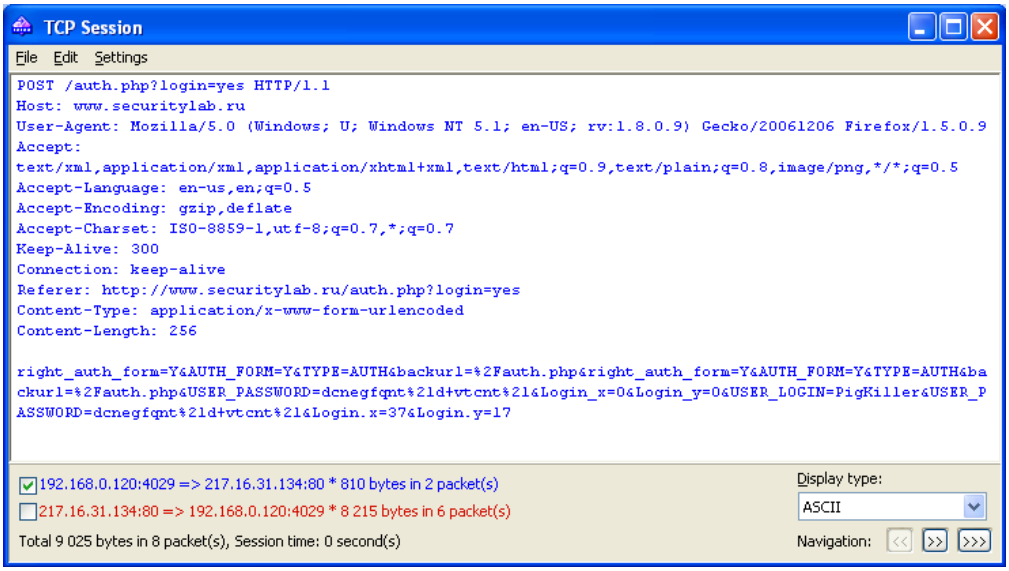


Рис. 22

В этом случае на совести пользователя лежит корректность сформированного HTTP-запроса, поскольку сканер будет использовать его «как есть», без каких либо модификаций.

Второй метод удобно использовать, когда управление авторизаций распределено между несколькими сайтами, как сделано в различных системах типа «Passport». Например, сайты Yandex используют централизованную систему Яндекс-Паспорт, устанавливающую значение Cookie для всего домена .yandex.ru:

Set-Cookie: yafolder=10537279%3A1290000000001899275; domain=.yandex.ru; path=/;

В этом случае в поле «Профиль сканирования – Настройки сканирования – Сканер уязвимостей – Определение уязвимостей – HTTP – Анализатор контента – Запрос» добавляются HTTP-заголовки, которые будут пересылаться в каждом HTTP-запросе. Примером таких заголовков могут быть параметры Cookie, устанавливаемые сервером после входа в систему.

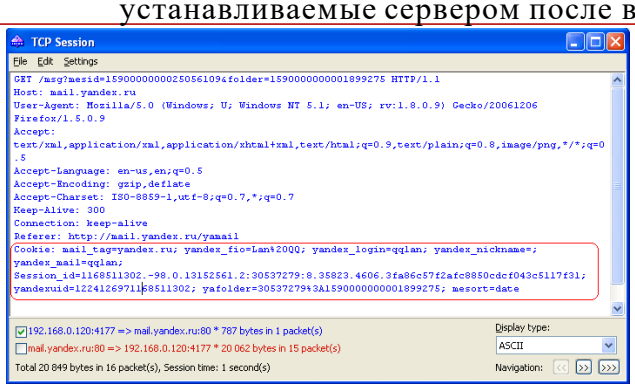


Рис. 23

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

В разделе «Профиль сканирования – Настройки сканирования – Сканер уязвимостей – Определение уязвимостей – HTTP – Анализатор сценариев» можно указать, какие из HTTP-методов будут использоваться в ходе эвристических проверок.

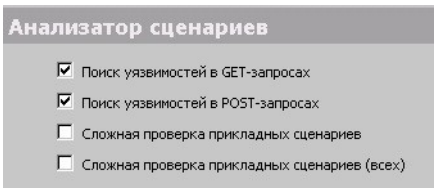


Рис. 24

Опция «сложная проверка прикладных скриптов» используется для работы с серверами, использующими нестандартную схему именования запросов. Например, таких, в которых изменение значения параметра запроса в URL приводит к вызову различных серверных сценариев.

Раздел «Типы уязвимостей» позволяет указать, какие из типов уязвимостей веб-серверов будут обнаружены.

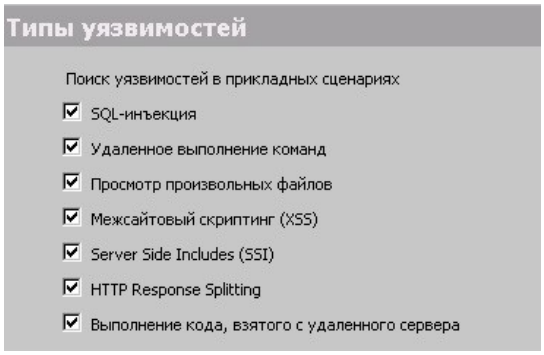


Рис. 25

Настройки раздела «Методы поиска» позволяют задействовать при поиске уязвимостей редко используемые поля, такие как заголовок Referer. Включение этих поверок увеличивает общее время проверок и нагрузку на сеть.

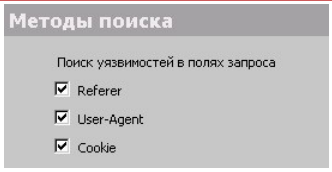


Рис. 26

4.5.5.3. Дополнительные настройки

Поскольку в ходе сканирования используются различные эвристические алгоритмы поиска уязвимостей, на узлах, содержащих серьезные ошибки, сканирование может привести к негативным эффектам.

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

5. СПИСОК ПРОВЕРЯЕМЫХ ОБЪЕКТОВ ДЛЯ РАЗЛИЧНЫХ СИСТЕМ

5.1. Список проверяемых объектов для OCWindows

5.1.1 Реестр

5.1.1.1. Доступ на чтение

Необходимо разрешить доступ на чтение к следующим ключам реестра (включая подключи):

HKLM\SOFTWARE\

HKCU\SOFTWARE\ HKCU\Environment\

HKEY_USERS\<…>\SOFTWARE\

HKEY_CURRENT_CONFIG\

5.1.2 Дисковые операции

5.1.2.1. Доступ на чтение

Необходимо разрешить доступ на чтение к следующим каталогам (включая подкаталоги):

%SYSTEMROOT%\

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ докум.	Входящий № сопроводи-тельного докум. и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения