XSpider 7.8 – новая версия легендарного сканера

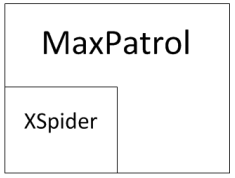
Олег Матыков, руководитель отдела проектных решений, Positive Technologies

XSpider. Как всё начиналось...

- **2 декабря 1998 г.**
  День рождения сканера безопасности XSpider. Первая версия сканера была названа Spider, но после сканер был переименован в XSpider.
- **2000 год. Версия сканера безопасности XSpider выложена в свободный доступ в Интернет. По статистике сервера, на начало 2009 года было скачано более 300 000 бесплатных копий XSpider**
- **2002 год. Основана компания с символичным названием «Positive Technologies». Первоначально основным направлением деятельности были услуги в области защиты информации: аудит внешних и внутренних сетей и др.**
- **16 июля 2003г. Первая коммерческая лицензия XSpider 7.0 №0001 была куплена 16.07.2003г. организацией ООО КБ «Транспортный»**
- **2006г. Выпущено первое комплексное обновление XSpider - версия 7.5.**
- **2006 г. В Учебном центре «Информзащита» разработан учебный курс: «Сканер безопасности XSpider».**

XSpider. Как всё начиналось...

- **2007 год. XSpider сертифицирован МО России**
- **2007 год. XSpider сертифицирован ФСТЭК России**
- **26 марта 2008г. Вышло последнее комплексное обновление XSpider — версия 7.7**
- **2009 год. Окончательно сформирован новый продукт - система контроля защищенности и соответствия стандартам MaxPatrol. Первое внедрение MaxPatrol в ГК «Лукойл». Получен сертификат ФСТЭК и МО.**
- **2011 год. Появление версии XSpider 7.8**
- **26 декабря 2011 года. Получен сертификат ФСТЭК для версии XSpider 7.8**
- **1 января 2012 года. Прекращены продажи версии XSpider 7.7**
- **2012 год. Постепенно все переходим на версию 7.8.**
- **Будущее:**



Переходим на XSpider 7.8!

А что нового? Лучшее осталось

Высокая скорость и качество сканирования

Удобный интерфейс

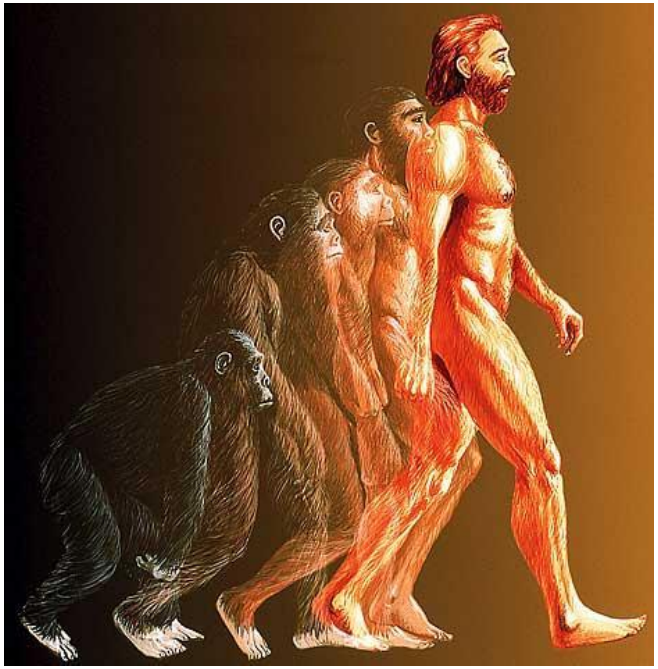
Доступная цена

Подробное описание уязвимости и возможного решения

Русскоязычный интерфейс и отчёты ☺

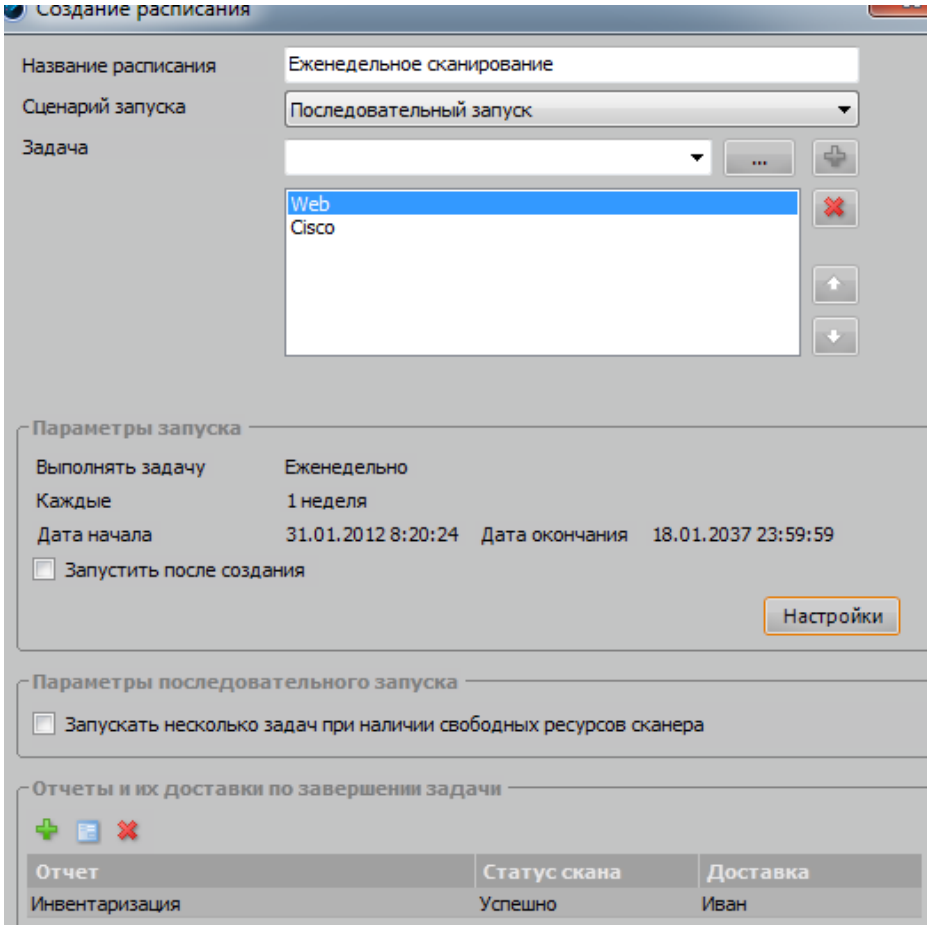
А многое стало лучше!

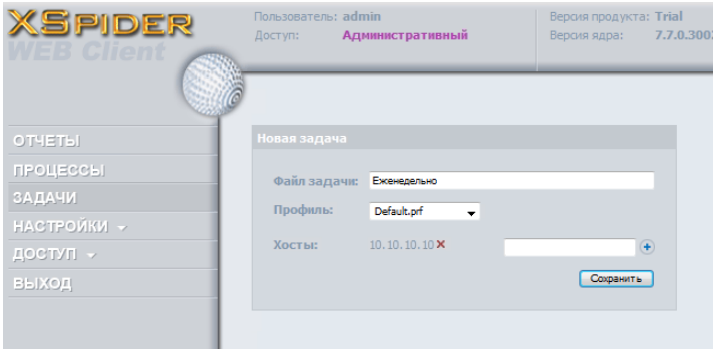
Улучшены прежние функции

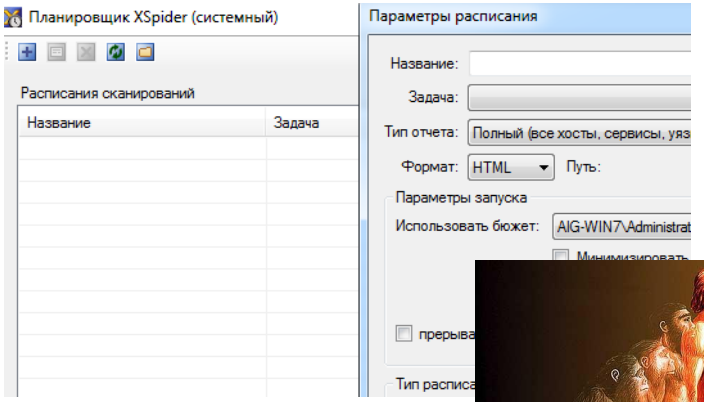


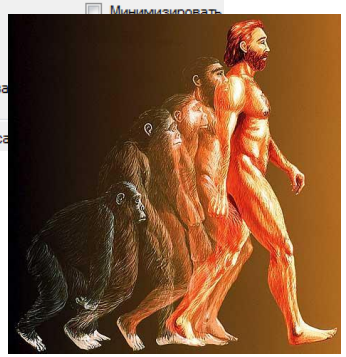
Улучшены прежние функции

Новый планировщик





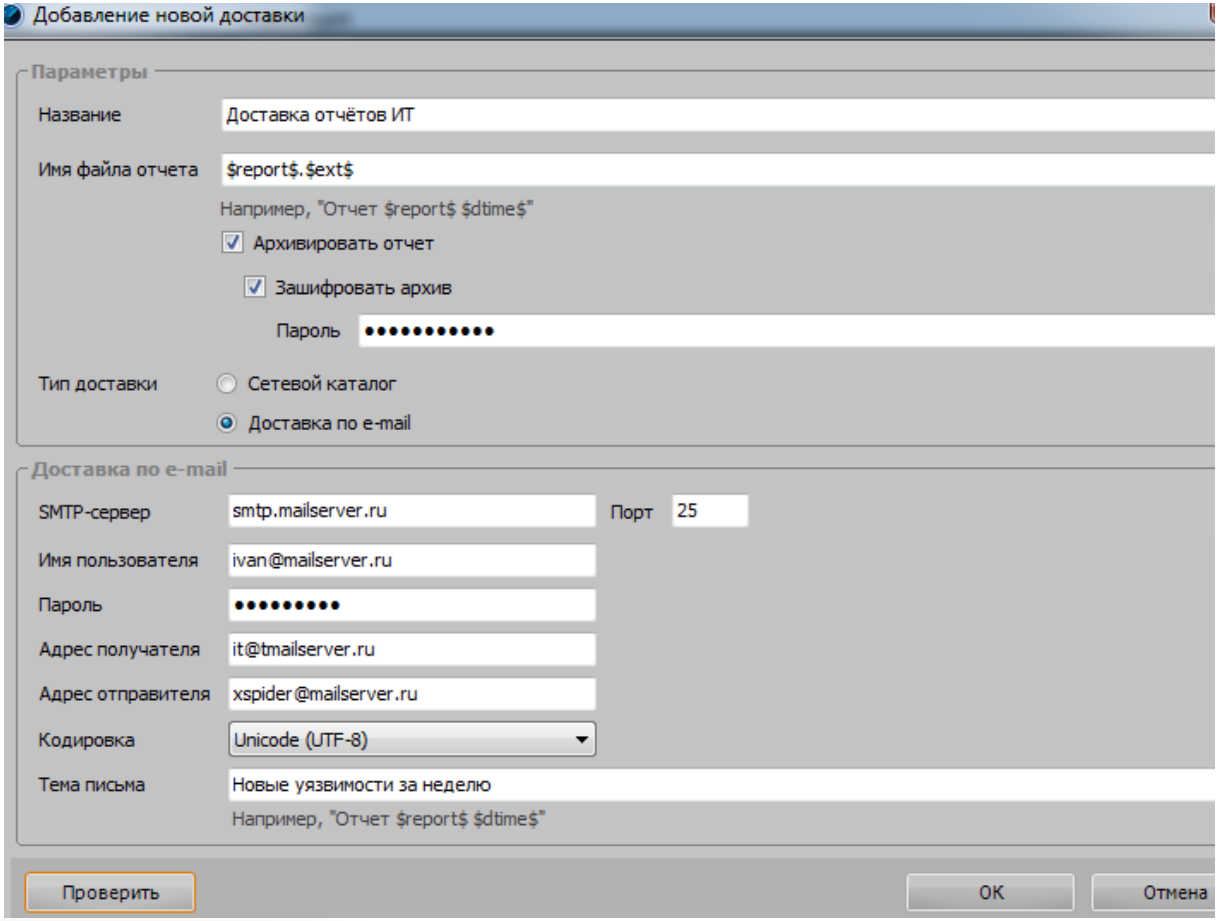


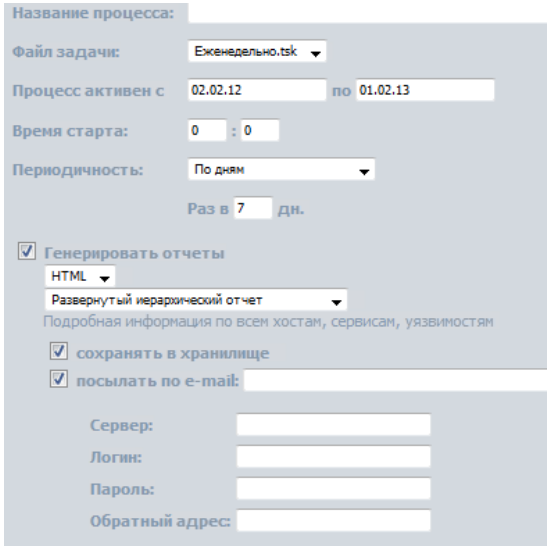


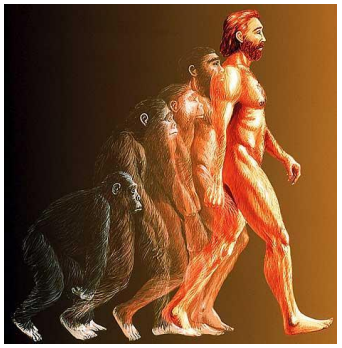
POSITIVE TECHNOLOGIES

Улучшены прежние функции

Доставка отчётов

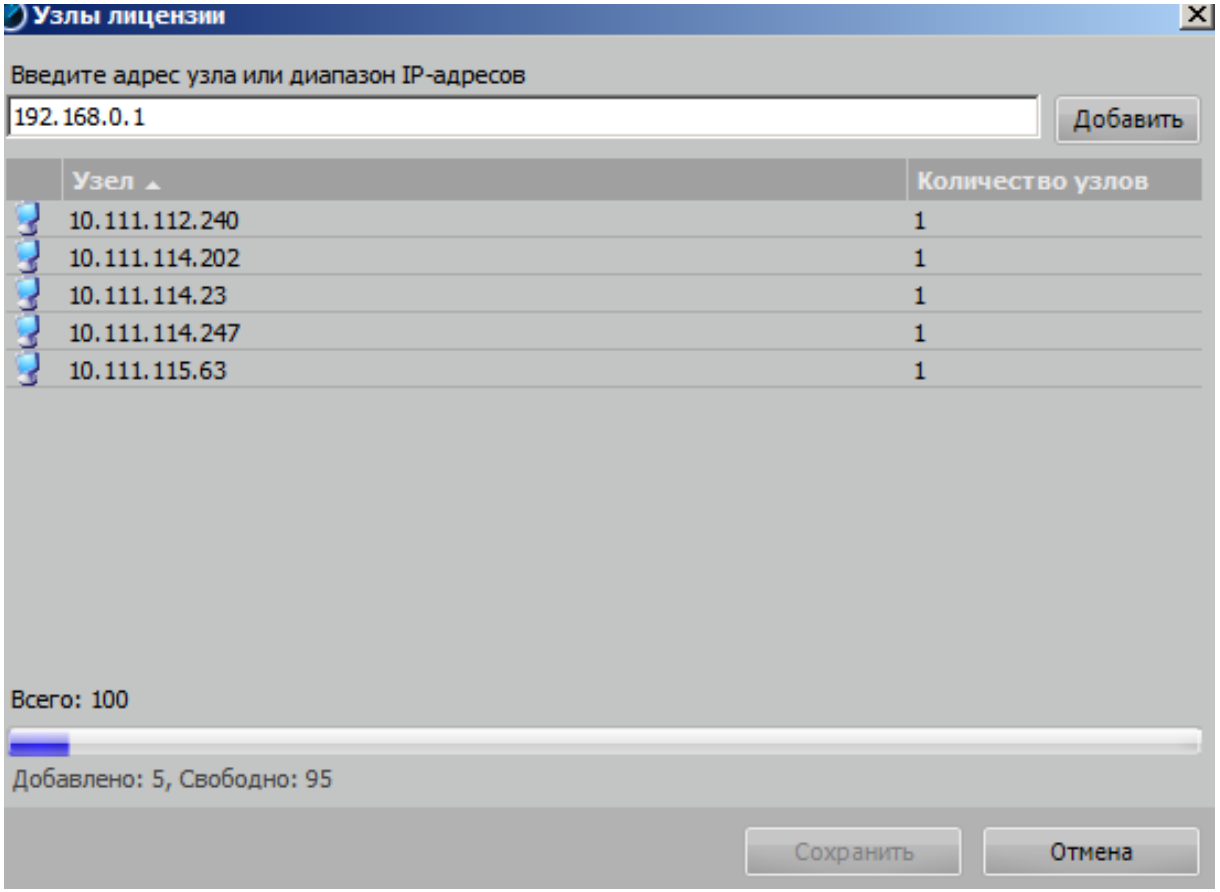


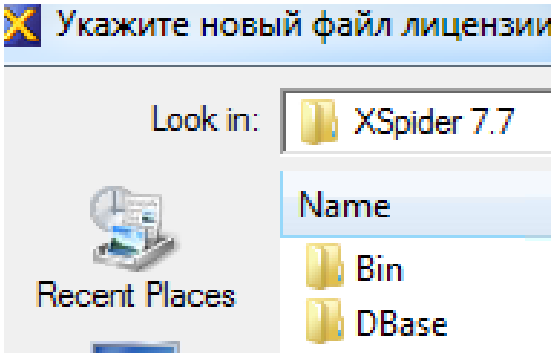




Улучшены прежние функции

Управление узлами в лицензии

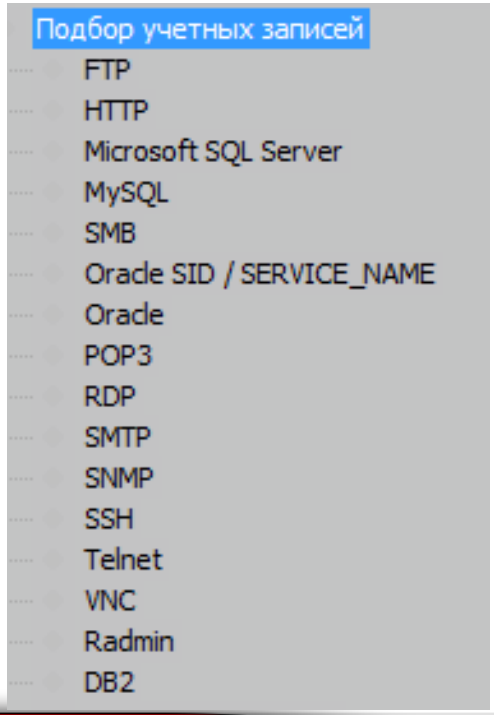


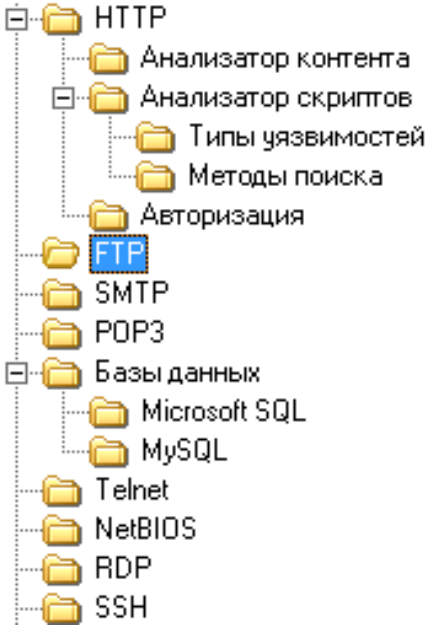


Улучшены прежние функции

Подбор паролей

Реализован подбор учетных записей для VNC, RAdmin, DB2
Улучшена скорость и достоверность подбора паролей Telnet, SSH, Oracle, RDP





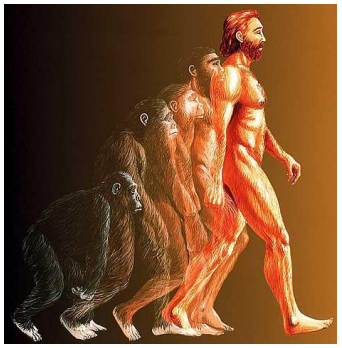
Улучшены прежние функции

Идентификация сервисов и операционных систем

Увеличено количество определяемых сервисов:
UDP: IKE, Open VPN, XDMCP, SIP, LLMNR, DB2 DAS
TCP: NFS, iSCSI, Net.TCP Port Sharing, DB2, Sybase, сервисы Oracle, сервисы RPC, сервисы SAP и другие.

Анализируется больше сервисов для определения версии ОС:
SNMP, SMB, AFP, LDAP, JUNOScript-specific protocol.

Реализованы новые проверки:
IKE, ICMP, RPC, NetBIOS, RDP, Oracle, Cisco



Улучшены прежние функции

Конструктор отчёта

Параметры пользовательского отчета

Название отчета: Default name

Комментарий: No comments

Фильтрация

Добавляемые уязвимости:

Включать порты (номера через запятую):

- [ ] исключать указаные порты
- [x] строгая фильтрация

Веса уязвимостей для расчета интегральной уязвимости: 1 | 2 | 3 | 4 | 5

Включать блоки:

- [ ] Легенда
- [ ] Данные о фильтрации
- [ ] Уязвимость хостов (график)
- [ ] Уязвимость сервисов (график)
- [ ] Уязвимости (график)
- [ ] Топ20 уязвимых хостов (график)
- [ ] Топ20 уязвимых сервисов (график)
- [ ] Топ20 уязвимостей (график)
- [ ] Топ20 неуязвимых хостов (график)
- [ ] Топ20 неуязвимых сервисов (график)
- [ ] Топ20 редких уязвимостей (график)
- [ ] Защищенность С-сетей (график)
- [ ] Перечень хостов

Параметры основного блока уязвимостей

- [ ] Не включать блок уязвимостей
- [x] включать инструкции по исправлению

Порядок сортировки:

- Хосты -> Сервисы -> Уязвимости
- Сервисы -> Хосты -> Уязвимости
- Хосты -> Уязвимости -> Сервисы
- Сервисы -> Уязвимости -> Хосты
- Уязвимости -> Хосты -> Сервисы
- Уязвимости -> Сервисы -> Хосты

Направление сортировки:

- [ ] по убыванию — IP хоста
- [ ] по убыванию — номера порта
- [x] по убыванию критичности уязвимости
- [x] включать заголовки с информацией о хосте
- [x] включать заголовки с информацией о сервисе

OK | Cancel

Улучшены прежние функции

Конструктор отчёта

Название: Серьезные уязвимости отдела

Комментарий:

Формат: MHTML file (.mht)

Язык: Russian

Тип отчета
- (•) Информация
- ( ) Дифференциальный

Исходные данные
- (•) По скану
- ( ) По задаче/задачам

Тип данных
PenTest

Выбор задачи и скана
Задача: localhost [...] Скан: [...]

Способ представления данных
Группировать по: По узлам

Параметры отчета
- [x] Легенда
- [x] Статистика
- [x] Проверенные узлы
- [ ] Уязвимые службы/ПО
- [x] Все службы/ПО
- [x] Уязвимость узлов
- [ ] Описание уязвимостей
- [ ] Состояние транспортов

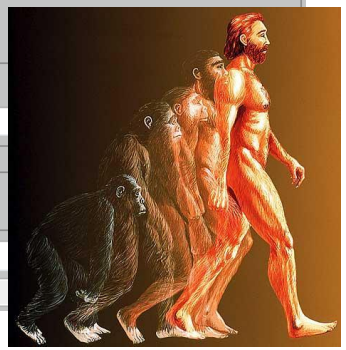
Топ
- [x] Топ уязвимостей
- [ ] Топ уязвимых сервисов
- [ ] Топ уязвимых узлов

Количество ТОПов
Количество ТОПов: 10

Фильтр узлов
Достоверность результатов: любая (все результаты)
Включать узлы, отмеченные как: <Все>
- [ ] Включать узлы, сканирование которых завершено с ошибкой
- [ ] Включать узлы, данные о которых отсутствуют

Дополнительный
IP-адреса: Включить: 10.111.118.10-10.111.118.20

Фильтр данных
- [x] По уровню: Серьезная уязвимость
- [ ] По полю

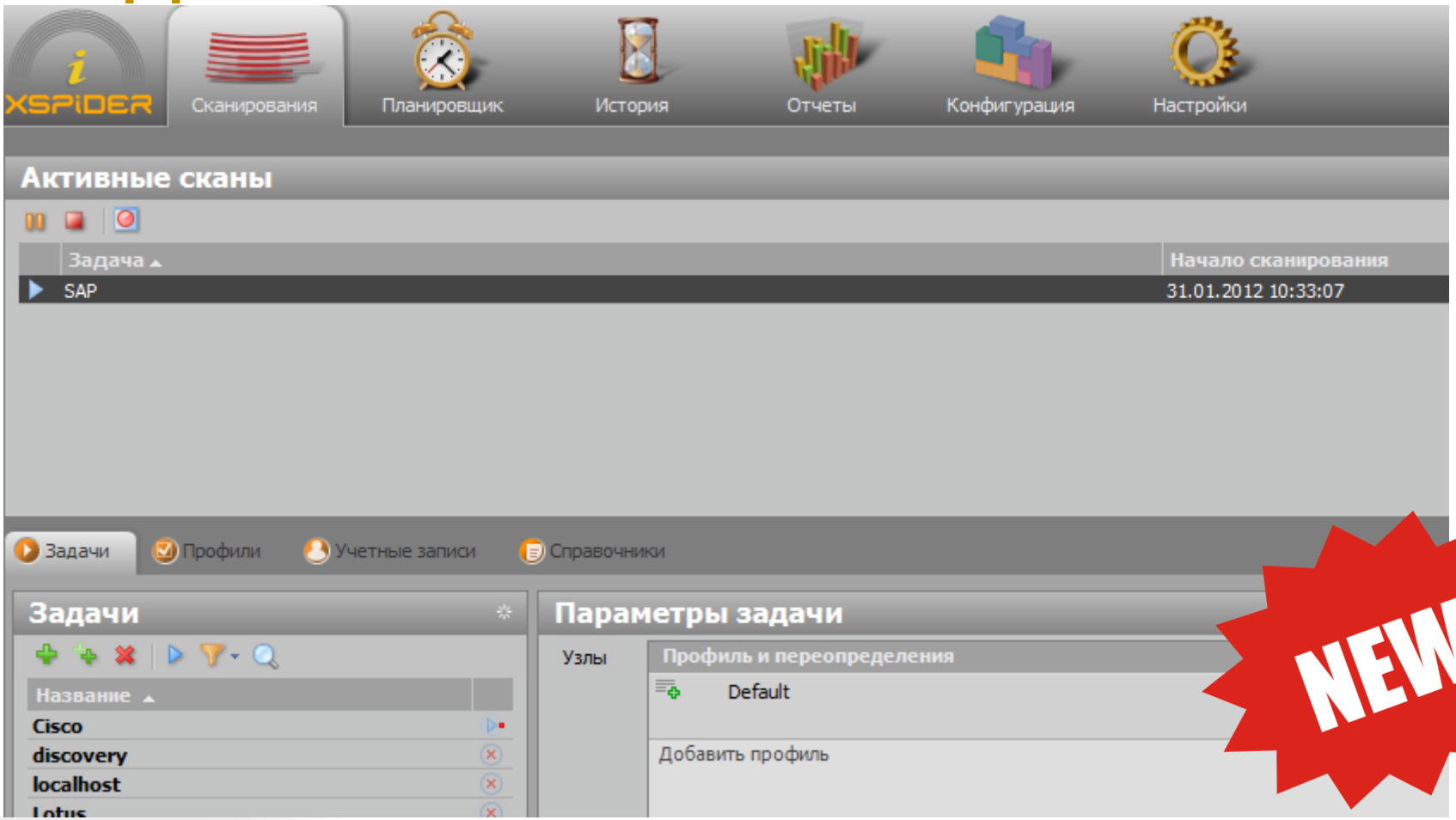


Новенькое ☺

Новые функции

Новые функции

Интерфейс



Новые функции

Режим Host Discovery

Host discovery [Начало: 31.01.2012 11:13; Длительность: 00:00:20]

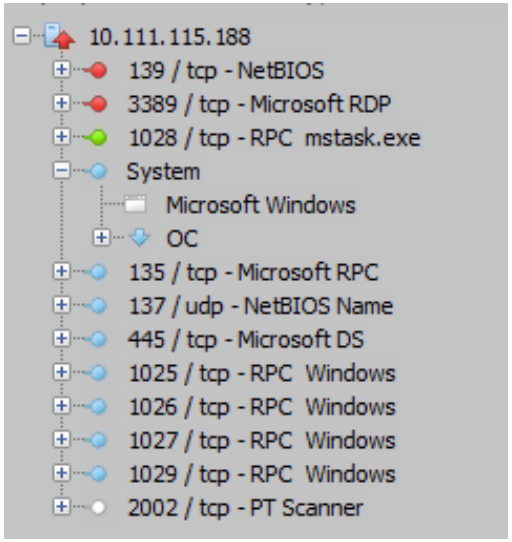
Информация

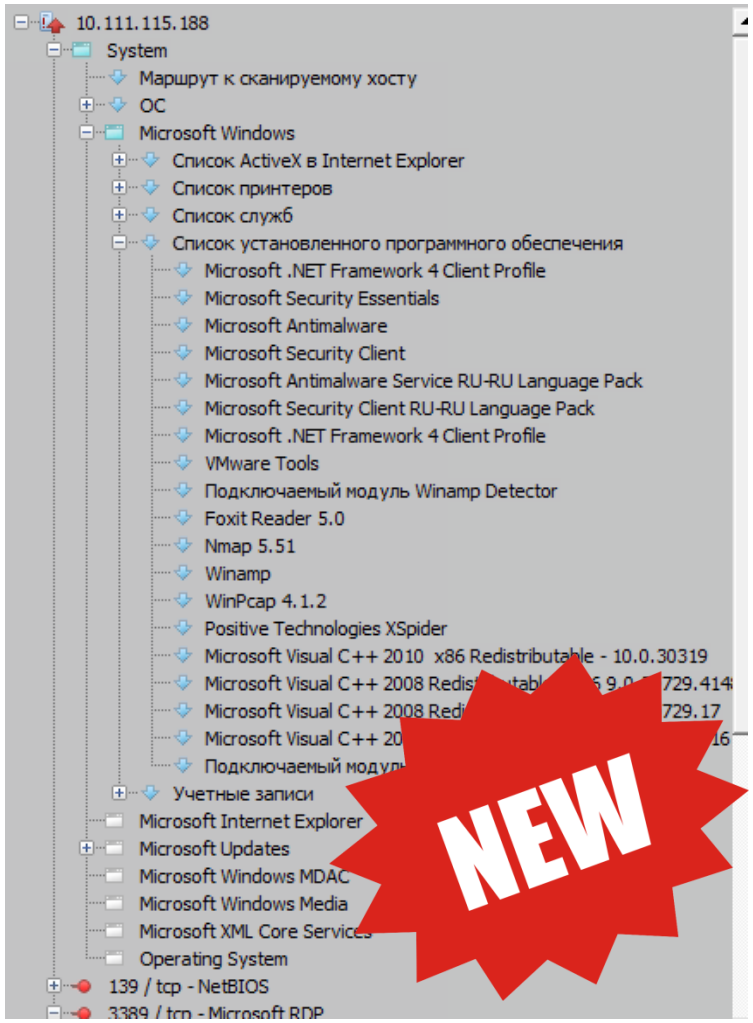
id	IP-адрес	Имя в задаче	Имя NetBIOS	Имя FQDN
1	10.111.115.0	10.111.115.0	PC-win7-iis-75	PC-win7-iis-75
2	10.111.115.1	10.111.115.1		
12	10.111.115.11	10.111.115.11	SCANNER_01	SCANNER_01
18	10.111.115.17	10.111.115.17	SCANNER_7	SCANNER_7
19	10.111.115.18	10.111.115.18	SCANNER_8	SCANNER_8
28	10.111.115.27	10.111.115.27		
31	10.111.115.30	10.111.115.30		10.111.115.30
33	10.111.115.32	10.111.115.32	FORAUDITWIN7	FORAUDITWIN7
43	10.111.115.42	10.111.115.42	ORACLE	ORACLE
48	10.111.115.47	10.111.115.47	WIN2k8x64	WIN2k8x64
50	10.111.115.49	10.111.115.49	PC-win7-iis-75	PC-win7-iis-75
61	10.111.115.60	10.111.115.60		10.111.115.60
64	10.111.115.63	10.111.115.63	WIN-DT372U3M7UU	WIN-DT372U3M7UU
73	10.111.115.72	10.111.115.72	115-72-TEST3	115-72-TEST3
78	10.111.115.77	10.111.115.77		10.111.115.77
79	10.111.115.78	10.111.115.78	MYGROUP	MYGROUP
96	10.111.115.95	10.111.115.95	WIN-RYP9SV72ER9	WIN-RYP9SV72ER9
109	10.111.115.108	10.111.115.108	PWIN2003ENTSP2X	PWIN2003ENTSP2X
112	10.111.115.111	10.111.115.111		10.111.115.111
114	10.111.115.113	10.111.115.113		10.111.115.113
115	10.111.115.114	10.111.115.114	PWIN7x86SP1	PWIN7x86SP1
116	10.111.115.115	10.111.115.115	SERVICES	SERVICES
132	10.111.115.131	10.111.115.131	Win7	Win7
134	10.111.115.133	10.111.115.133	WINXPTECHSUPP	WINXPTECHSUPP
152	10.111.115.151	10.111.115.151		pc_for_testing.ptsecuri..

Новые функции

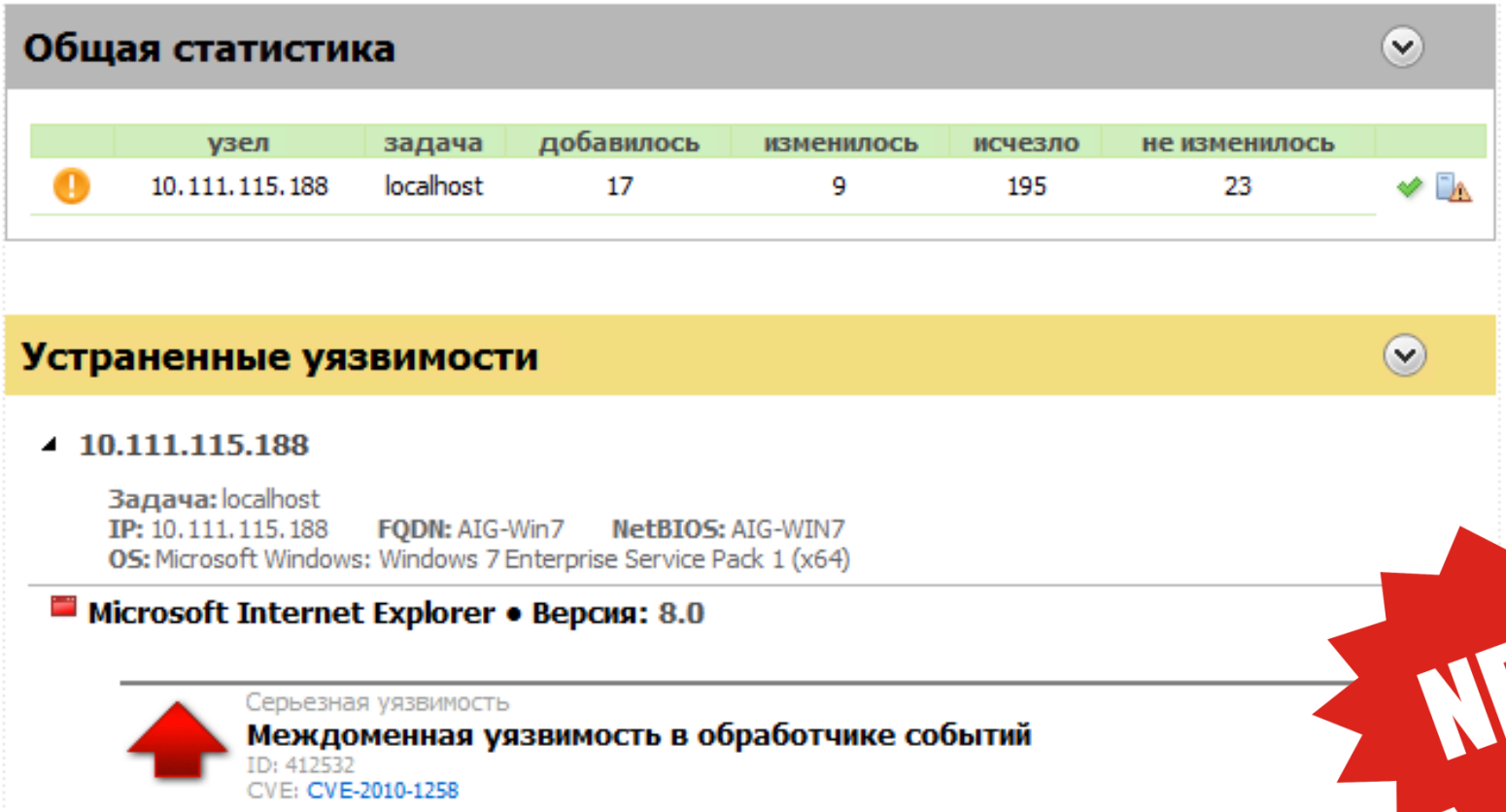
Расширенные проверки Windows

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



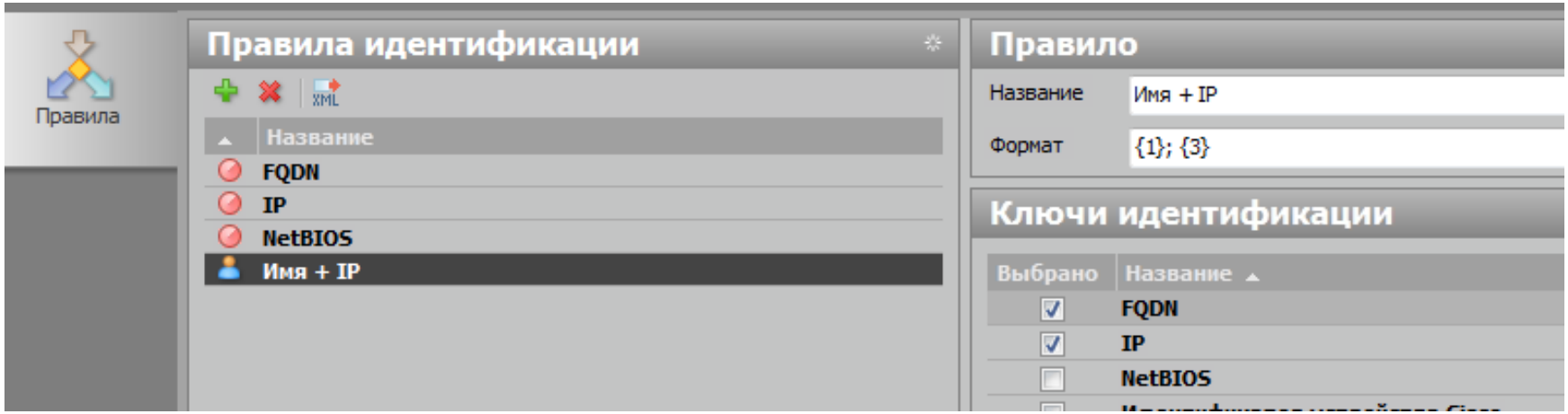


Контроль изменений: дифференциальные отчёты



Новые функции

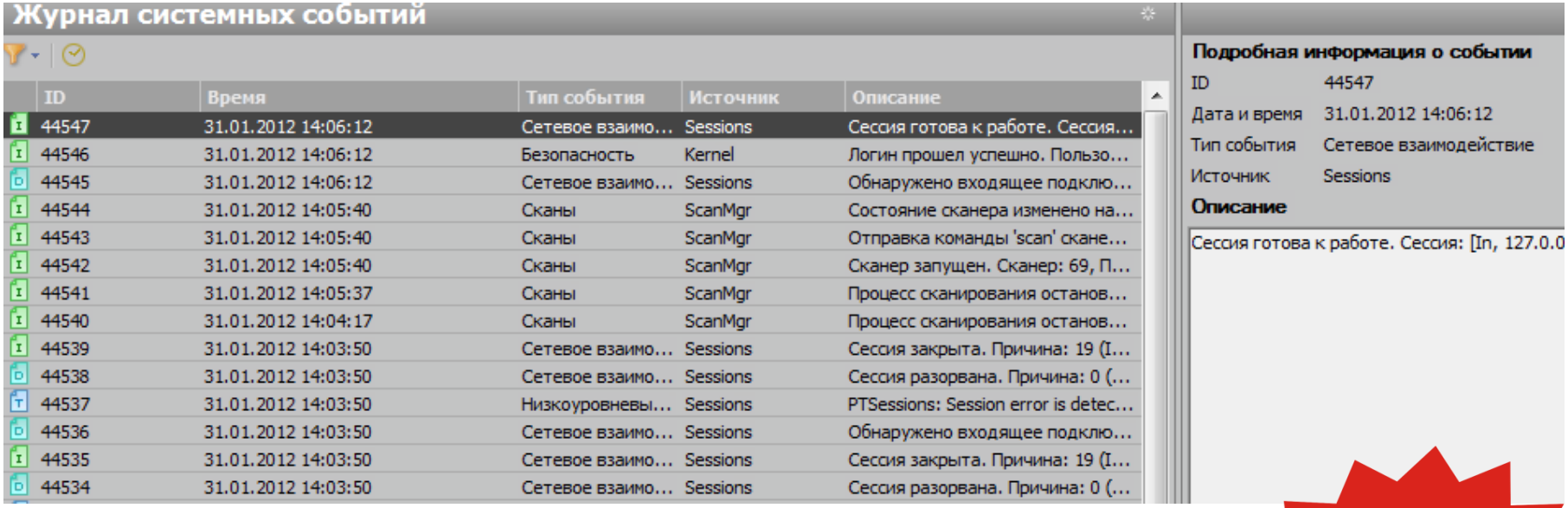
Правила идентификации



NEW

Новые функции

Интерфейсный журнал



Основные задачи XSpider 7.8

- **Повышение качества процесса анализа уязвимости за счёт автоматизации рутинной работы специалистов ИБ и ИТ**
  - **поиск уязвимостей,**
  - **наличие описания уязвимостей,**
  - **контроль появления и устранения уязвимостей,**
  - **уведомление об обнаружении уязвимостей.**
- **Инвентаризация узлов в сети**
- **Контроль изменений состава сетевых узлов, появления и устранения уязвимостей, изменения состава ПО**

Функциональные возможности XSpider 7.8

- **Удаленное сканирование сетевых узлов без использования агентов**
  - Обнаружение узлов сети
  - Сканирование портов TCP\UDP
  - Идентификация ОС и сетевых сервисов
  - Обнаружение уязвимостей в сервисах
  - Подбор паролей
  - Сбор инвентаризационной информации
- **Автоматизация процессов**
  - Расписание по сканированию в указанные интервалы
  - Генерация и доставка отчётов в указанное время
- **Анализ и вывод изменений между сканированиями**
  - Дифференциальные отчёты по уязвимостям
  - Дифференциальные отчёты по инвентаризации

Сертификация XSpider 7.8

XSpider 7.8 уже сертифицирован ФСТЭК и может использоваться для анализа защищенности информационных систем персональных данных до 1 класса включительно.

Копия сертификата: http://www.ptsecurity.ru/licenses.asp

Выдан 26 декабря 2011 г.
Действителен до 26 декабря 2014 г.

Настоящий сертификат удостоверяет, что **сетевой сканер безопасности XSpider 7.8**, разработанный и производимый ЗАО «Позитив Текнолоджиз» в соответствии с техническими условиями ТУ 5015-001-83128364-11, функционирующий в среде операционных систем, указанных в формуляре 5015-001-83128364-11 30 01, является средством автоматизированного анализа защищенности и обнаружения уязвимостей автоматизированных систем, обрабатывающих информацию, не содержащую сведений, составляющих государственную тайну, соответствует требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) - по **4** уровню контроля, технических условий и может применяться для анализа защищенности автоматизированных систем до класса **1Г** включительно и информационных систем персональных данных до **1** класса включительно.

Хочу ознакомительную версию XSpider 7.8

- **В отличие от XS 7.7 нет специального дистрибутива с пробной версией**
- **Для запроса лицензии достаточно написать запрос на адрес: pt@ptsecurity.ru**

XSPIDER

Спасибо за внимание!

Positive Technologies

pt@ptsecurity.ru

+7 (495) 744-0144

POSITIVE TECHNOLOGIES