


# **XSpider 7.8** – новая версия легендарного сканера

**Олег Матыков**, руководитель  
отдела проектных решений,  
Positive Technologies



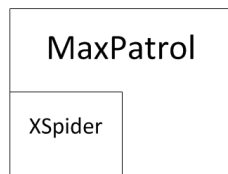
# XSpider. Как всё начиналось...

-  **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**

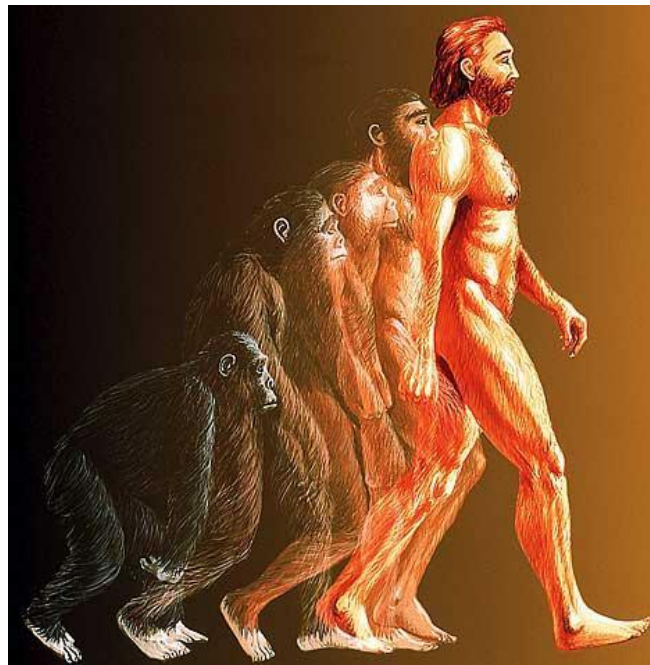
**Подробное описание уязвимости и возможного решения**

**Русскоязычный интерфейс и отчёты 😊**



**А многое стало лучше!**

**Улучшены прежние функции**



# Улучшены прежние функции

## Новый планировщик

Создание расписания

Название расписания: Еженедельное сканирование

Сценарий запуска: Последовательный запуск

Задача: Web  
Cisco

Параметры запуска

Выполнять задачу: Еженедельно  
Каждые: 1 неделя  
Дата начала: 31.01.2012 8:20:24    Дата окончания: 18.01.2037 23:59:59  
 Запустить после создания

Параметры последовательного запуска

Запускать несколько задач при наличии свободных ресурсов сканера

Отчеты и их доставки по завершении задачи

Отчет	Статус скана	Доставка
Инвентаризация	Успешно	Иван

XSPIDER WEB Client

Пользователь: admin    Версия продукта: Trial  
Доступ: Административный    Версия ядра: 7.7.0.300

ОТЧЕТЫ  
ПРОЦЕССЫ  
ЗАДАЧИ  
НАСТРОЙКИ  
ДОСТУП  
ВЫХОД

Новая задача

Файл задачи: Еженедельно  
Профиль: Default.prf  
Хосты: 10.10.10.10 X

Сохранить

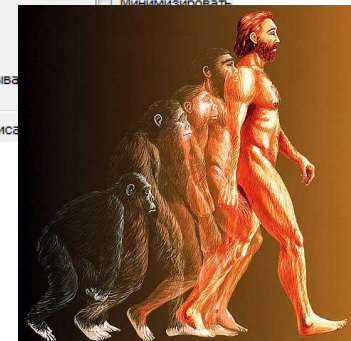
Планировщик XSpider (системный)

Расписания сканирований

Название	Задача

Параметры расписания

Название:   
Задача:   
Тип отчета: Полный (все хосты, сервисы, уязв.)  
Формат: HTML    Путь:   
Параметры запуска  
Использовать бюджет: AIG-WIN7\Administrat  
 Минимизировать  
 прерыва  
Тип расписания



# Улучшены прежние функции

## Доставка отчётов

Добавление новой доставки

Параметры

Название: Доставка отчётов ИТ

Имя файла отчета: \$report\$. \$ext\$  
Например, "Отчет \$report\$ \$dtime\$"

Архивировать отчет

Зашифровать архив

Пароль: .....

Тип доставки:  Сетевой каталог  Доставка по e-mail

Доставка по e-mail

SMTP-сервер: smtp.mailserver.ru Порт: 25

Имя пользователя: ivan@mailserver.ru

Пароль: .....

Адрес получателя: it@mailserver.ru

Адрес отправителя: xspider@mailserver.ru

Кодировка: Unicode (UTF-8)

Тема письма: Новые уязвимости за неделю  
Например, "Отчет \$report\$ \$dtime\$"

Проверить OK Отмена

Название процесса:

Файл задачи: Ежедневно.task

Процесс активен с: 02.02.12 по 01.02.13

Время старта: 0 : 0

Периодичность: По дням  
Раз в 7 дни.

Генерировать отчеты

HTML

Развернутый иерархический отчет

Подробная информация по всем хостам, сервисам, уязвимостям

сохранять в хранилище

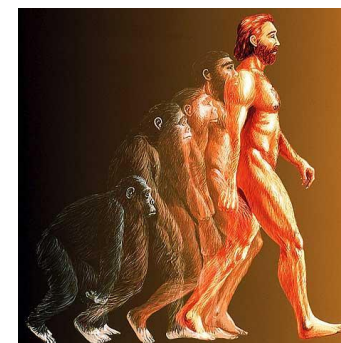
посылать по e-mail:

Сервер: \_\_\_\_\_

Логин: \_\_\_\_\_

Пароль: \_\_\_\_\_

Обратный адрес: \_\_\_\_\_





# Улучшены прежние функции

## Управление узлами в лицензии

Узлы лицензии

Введите адрес узла или диапазон IP-адресов

192.168.0.1 Добавить

Узел ▲	Количество узлов
10.111.112.240	1
10.111.114.202	1
10.111.114.23	1
10.111.114.247	1
10.111.115.63	1

Всего: 100

Добавлено: 5, Свободно: 95

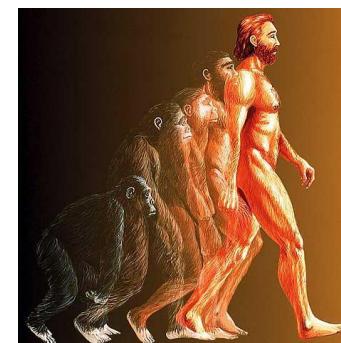
Сохранить Отмена

Укажите новый файл лицензии

Look in: XSpider 7.7

Recent Places

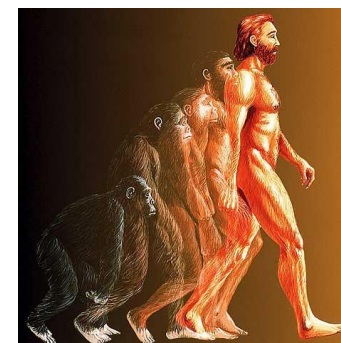
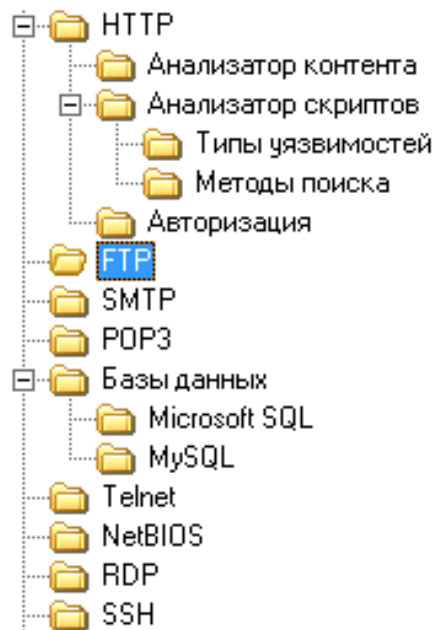
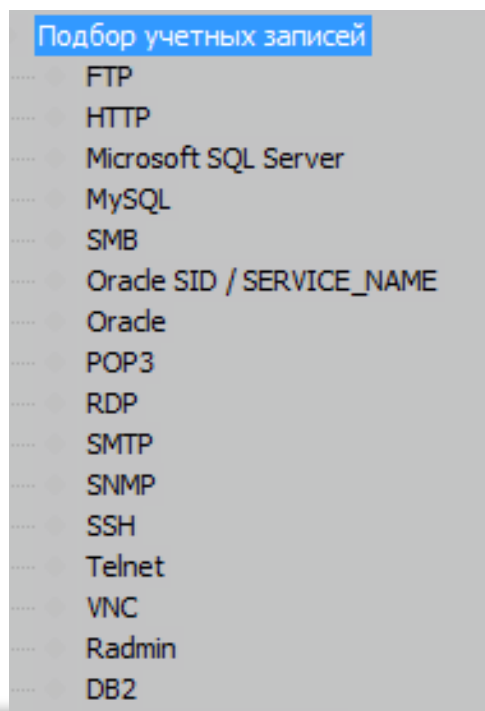
- Bin
- DBase



# 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**

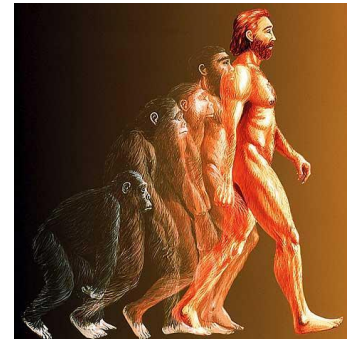
**TCP: NFS, iSCSI, Net.TCP Port Sharing, DB2, Sybase, сервисы Oracle, сервисы RPC, сервисы SAP и другие.**

**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:

Комментарий:

Фильтрация

Добавляемые уязвимости:

Включать порты (номера через запятую):

исключать указанные порты  
 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)
- Top20 уязвимых хостов (график)
- Top20 уязвимых сервисов (график)
- Top20 уязвимостей (график)
- Top20 неязвимых хостов (график)
- Top20 неязвимых сервисов (график)
- Top20 редких уязвимостей (график)
- Защищенность С-сетей (график)
- Пеленг хостов

Параметры основного блока уязвимостей

Не включать блок уязвимостей

Порядок сортировки:  
**Хосты -> Сервисы -> Уязвимости**  
Сервисы -> Хосты -> Уязвимости  
Хосты -> Уязвимости -> Сервисы  
Сервисы -> Уязвимости -> Хосты  
Уязвимости -> Хосты -> Сервисы  
Уязвимости -> Сервисы -> Хосты

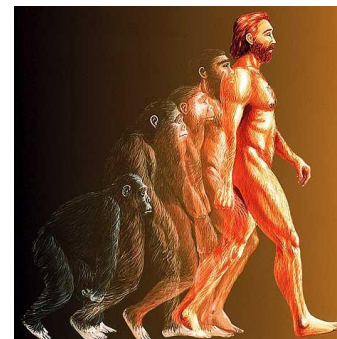
включать инструкции по исправлению

Направление сортировки:

- по убыванию IP хоста
- по убыванию номера порта
- по убыванию критичности уязвимости

включать заголовки с информацией о хосте  
 включать заголовки с информацией о сервисе

OK Cancel



# Улучшены прежние функции

## Конструктор отчёта

Название

Комментарий

Формат

Язык

Тип отчета

Информация

Дифференциальный

Исходные данные

По скану

По задаче/задачам

Тип данных

Выбор задачи и скана

Задача  Скан

Способ представления данных

Группировать по

Параметры отчета

Легенда  Все службы/ПО

Статистика  Уязвимость узлов

Проверенные узлы  Описание уязвимостей

Уязвимые службы/ПО  Состояние транспортов

Топ

Топ уязвимостей  Топ уязвимых узлов

Топ уязвимых сервисов

Количество ТОПов

Количество ТОПов

Фильтр узлов

Достоверность результатов

Включать узлы, отмеченные как

Включать узлы, сканирование которых завершено с ошибкой

Включать узлы, данные о которых отсутствуют

Дополнительный

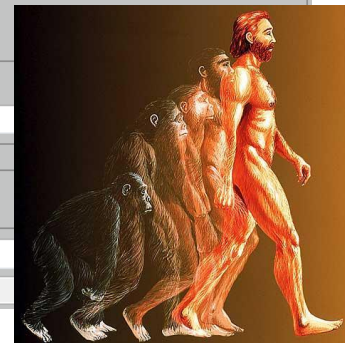
IP-адреса

Включить

Фильтр данных

По уровню

По полю



## Новые функции



# Новые функции

## Интерфейс

The screenshot displays the XSPIDER software interface. At the top, there is a navigation bar with icons and labels for: XSPIDER, Сканирования, Планировщик, История, Отчеты, Конфигурация, and Настройки. Below this is a section titled "Активные сканы" containing a table with columns "Задача" and "Начало сканирования". The table lists a task named "SAP" with a start time of "31.01.2012 10:33:07".

At the bottom, there are two main panels:

- Задачи:** A list of tasks with columns for "Название" and "Статус". The list includes "Cisco", "discovery", "localhost", and "Lotus".
- Параметры задачи:** A configuration panel for the selected task, showing "Узлы" (Nodes) and "Профиль и переопределения" (Profile and overrides). The profile is set to "Default".

A red starburst graphic with the word "NEW" is overlaid on the bottom right of the interface.



# 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..

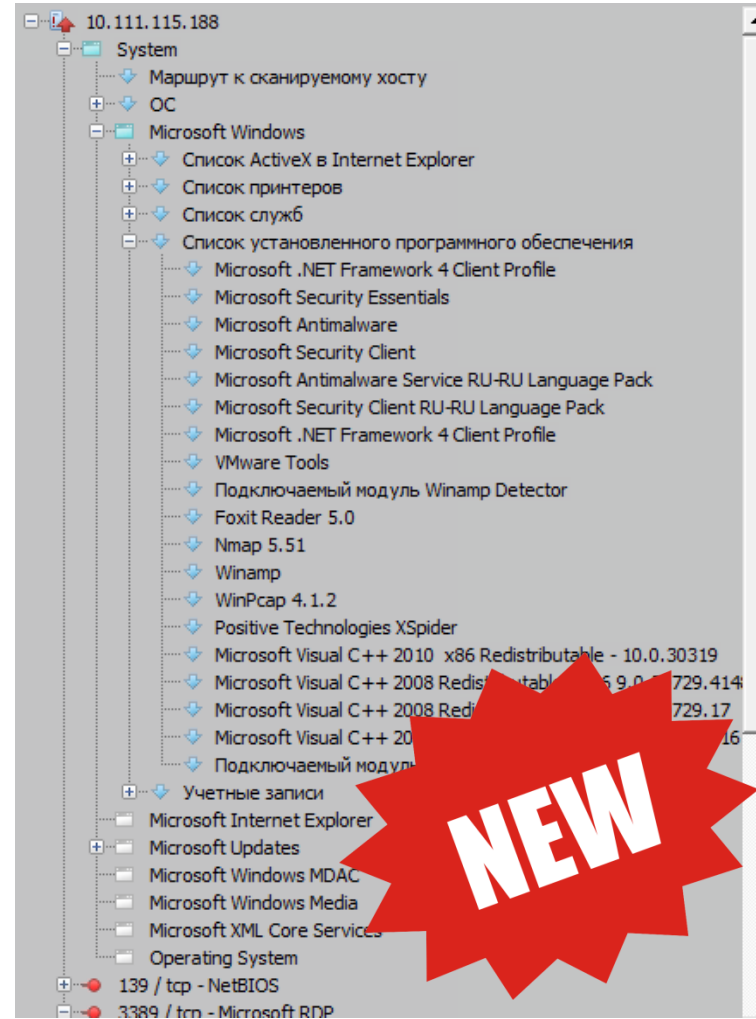
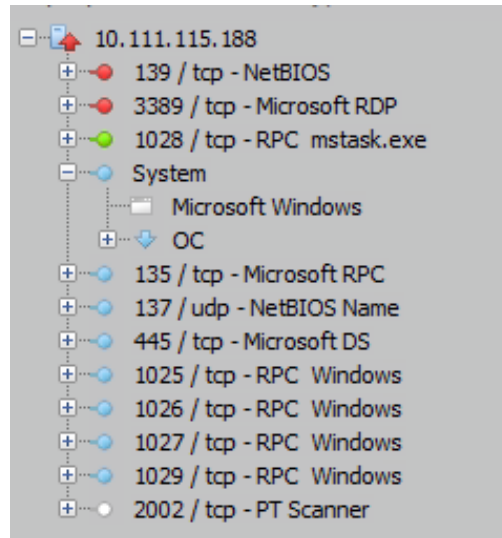




# Новые функции

## 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 ESMTMP MAIL Service
- Microsoft DNS Server
- Microsoft WINS Server



**NEW**



# Новые функции

## Контроль изменений: дифференциальные отчёты

### Общая статистика

	узел	задача	добавилось	изменилось	исчезло	не изменилось	
!	10.111.115.188	localhost	17	9	195	23	✓ ⚠

### Устраненные уязвимости

#### ▲ 10.111.115.188

Задача: localhost

IP: 10.111.115.188

FQDN: AIG-Win7

NetBIOS: AIG-WIN7

OS: Microsoft Windows: Windows 7 Enterprise Service Pack 1 (x64)

#### Microsoft Internet Explorer • Версия: 8.0



Серьезная уязвимость

**Междоменная уязвимость в обработке событий**

ID: 412532

CVE: [CVE-2010-1258](#)



# Новые функции

## Правила идентификации

The screenshot displays the 'Правила идентификации' (Identification Rules) configuration window. On the left, a sidebar shows a list of rules: FQDN, IP, NetBIOS, and 'Имя + IP' (Name + IP), which is currently selected. The main area shows the configuration for the 'Имя + IP' rule, including its name and format. Below this, a section titled 'Ключи идентификации' (Identification Keys) shows a list of keys with checkboxes indicating they are selected.

Выбрано	Название
<input checked="" type="checkbox"/>	FQDN
<input checked="" type="checkbox"/>	IP
<input type="checkbox"/>	NetBIOS
<input type="checkbox"/>	...



# Новые функции

## Интерфейсный журнал

### Журнал системных событий




ID	Время	Тип события	Источник	Описание
44547	31.01.2012 14:06:12	Сетевое взаимо...	Sessions	Сессия готова к работе. Сессия...
44546	31.01.2012 14:06:12	Безопасность	Kernel	Логин прошел успешно. Пользо...
44545	31.01.2012 14:06:12	Сетевое взаимо...	Sessions	Обнаружено входящее подклю...
44544	31.01.2012 14:05:40	Сканы	ScanMgr	Состояние сканера изменено на...
44543	31.01.2012 14:05:40	Сканы	ScanMgr	Отправка команды 'scan' скане...
44542	31.01.2012 14:05:40	Сканы	ScanMgr	Сканер запущен. Сканер: 69, П...
44541	31.01.2012 14:05:37	Сканы	ScanMgr	Процесс сканирования остано...
44540	31.01.2012 14:04:17	Сканы	ScanMgr	Процесс сканирования остано...
44539	31.01.2012 14:03:50	Сетевое взаимо...	Sessions	Сессия закрыта. Причина: 19 (I...
44538	31.01.2012 14:03:50	Сетевое взаимо...	Sessions	Сессия разорвана. Причина: 0 (...
44537	31.01.2012 14:03:50	Низкоуровневы...	Sessions	PTSessions: Session error is detec...
44536	31.01.2012 14:03:50	Сетевое взаимо...	Sessions	Обнаружено входящее подклю...
44535	31.01.2012 14:03:50	Сетевое взаимо...	Sessions	Сессия закрыта. Причина: 19 (I...
44534	31.01.2012 14:03:50	Сетевое взаимо...	Sessions	Сессия разорвана. Причина: 0 (...

#### Подробная информация о событии

ID 44547  
Дата и время 31.01.2012 14:06:12  
Тип события Сетевое взаимодействие  
Источник Sessions  
**Описание**  
Сессия готова к работе. Сессия: [In, 127.0.0



# 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 недеklarированных 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](mailto:pt@ptsecurity.ru)

# XSPIDER





**Спасибо за внимание!**

**Positive Technologies**

**pt@ptsecurity.ru**

**+7 (495) 744-0144**



**POSITIVE TECHNOLOGIES**