КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- Контроль изменений на сканируемых узлах, дающий полную картину защищенности в динамике.
- Инвентаризация всех сетевых устройств в организации.
- Эвристический метод определения типов и имен сервисов (HTTP, FTP, SMTP, POP3, DNS, SSH и др.) даже на нестандартных портах.
- Обработка RPC-сервисов (Windows и *nix) с полной идентификацией, включая точное определение конфигурации компьютера.
- Проверка слабости парольной защиты: оптимизированный подбор паролей практически во всех сервисах, требующих аутентификации.
- Глубокий анализ веб-сайтов, включая выявление уязвимостей: SQLi, XSS, запуск произвольных программ и др.
- Анализ структуры HTTP-серверов для поиска слабых мест в конфигурации.
- Расширенная проверка узлов под управлением Windows.
- Проведение проверок на нестандартные DoS-атаки.

XSPIDER: ВЕДУЩИЙ РОССИЙСКИЙ СКАНЕР УЯЗВИМОСТЕЙ

С развитием информационных систем в государственных организациях и частных компаниях растет и количество уязвимостей, которые могут быть использованы для нанесения серьезного ущерба. Согласно исследованию Positive Technologies, в 2015 году 94% систем крупных компаний содержали серьезные уязвимости, позволяющие злоумышленнику получить полный контроль над критически важными ресурсами, такими как ERP, электронная почта и базы данных.

При этом даже самые современные антивирусы не защищают от атак. Согласно M-Trends Report, в 2014 году все без исключения жертвы крупных взломов имели у себя своевременно обновляемый антивирус, но это им не помогло. Необходимы альтернативные технологии защиты, среди которых анализ защищенности — первый шаг к построению реальной безопасности.

С этим связано и ужесточение стандартов безопасности: последние нормативы регулирующих организаций, таких как Банк России, ФСТЭК и PCI Council, требуют выявления и оперативного устранения уязвимостей. Решение этих задач в компаниях, использующих сотни копий различного ПО, невозможно без эффективных автоматизированных средств анализа защищенности.

Интеллектуальный сканер XSpider способен выявить максимальное количество уязвимостей в информационной системе клиента до того, как они будут обнаружены и использованы злоумышленниками. Регулярное автоматическое сканирование с помощью XSpider почти не требует вмешательства специалиста. После сканирования система выдает четкие рекомендации по устранению обнаруженных уязвимостей и решению других проблем безопасности.

XSpider отличается широким покрытием программного обеспечения информационных систем, включая различные ОС (Windows, *nix, Mac OS), СУБД, сетевые устройства, АСУ ТП. Сканер выявляет уязвимости как для системного, так и для прикладного ПО, проводит анализ веб-приложений. Система работает удаленно, никаких агентов и дополнительного ПО на проверяемые узлы ставить не требуется. Во время сканирования заметной нагрузки на проверяемый узел не создается.

База уязвимостей XSpider обновляется автоматически и регулярно и содержит свыше 20 000 проверок. Благодаря эвристическим алгоритмам сканер способен выявлять еще не опубликованные уязвимости и отличается крайне низким уровнем ложных срабатываний.

ПРЕИМУЩЕСТВА ДЛЯ СПЕЦИАЛИСТОВ

- Наглядный и удобный интерфейс.
- Быстрая установка и настройка, не требующая высокой квалификации.
- Гибкий планировщик заданий для автоматизации работы.
- Одновременное сканирование большого числа компьютеров.
- Работа при нестандартных конфигурациях ПО и низком качестве каналов связи.
- Ведение полной истории проверок и генерация отчетов с разным уровнем детализации.
- Встроенная документация, в том числе контекстная справка и учебник.
- Работа под управлением Windows XP, Server 2003, Vista, 2008, 2008 R2/7, а также Windows 10.
- Низкие аппаратные требования.
- Удобная схема лицензирования.
- Наличие сертификата ФСТЭК на соответствие ТУ и 4-му уровню контроля отсутствия НДВ.

XSPIDER: СФЕРЫ ИСПОЛЬЗОВАНИЯ

Более 2000 российских и зарубежных компаний успешно применяют XSpider для анализа и контроля защищенности своих систем, а также для предоставления услуг в области ИБ. Сканер развивается с учетом опыта разработки всей экосистемы средств безопасности Positive Technologies. XSpider позволяет обеспечить максимальное соответствие государственным и международным стандартам безопасности. Основные отрасли применения XSpider:

Банки и финансовые организации. Критически важные приложения (ДБО, CRM, банковские, трейдинговые) должны соответствовать стандартам безопасности индустрии платежных карт PCI DSS и требованиям регулирующих органов. Однако часто в подобных приложениях возникают опасные уязвимости, вызванные ошибками в коде или недостатками конфигурации. Поэтому требуется регулярное сканирования сетей организации на наличие уязвимостей.

Медицина, образование, государственные учреждения. В приказе ФСТЭК России от 11.02.2013 № 17 прописана необходимость использования сертифицированных средств анализа защищенности в государственных информационных системах. А приказ от 18.02.2013 № 21 обязывает использовать сертифицированные средства анализа защищенности при работе с персональными данными.

Телеком-операторы. Имеют множество различных приложений, включая порталы самообслуживания, VAS/MSS-порталы для клиентов, мобильные и облачные приложения. Телекоммуникационные компании тоже обязаны, согласно приказу № 21, использовать при работе с персональными данными сертифицированные ФСТЭК средства анализа защищенности.

ВАРИАНТЫ ИСПОЛЬЗОВАНИЯ XSPIDER

- Анализ защищенности рабочих станций пользователей
- Анализ защищенности серверов и сетевого оборудования
- Анализ защищенности веб-сайтов
- Анализ защищенности внешнего периметра организации
- Инвентаризация узлов в сети

О компании Positive Technologies

Positive Technologies — лидер европейского рынка систем анализа защищенности и соответствия стандартам. Деятельность компании лицензирована Минобороны РФ, ФСБ и ФСТЭК, продукция сертифицирована «Газпромом» и ФСТЭК. Более 3000 организаций из 30 стран мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телекомов. В 2013 году компания заняла третье место на российском рынке ПО для безопасности и стала лидером по темпам роста на международном рынке систем управления уязвимостями.

POSITIVE TECHNOLOGIES

pt@ptsecurity.com ptsecurity.ru