XSpider

XSpider - уникальный продукт с более чем десятилетней историей, представляющий собой универсальную систему для работы с уязвимостями на разных уровнях - от системного до прикладного. XSpider проверяет все возможные уязвимости независимо от программной и аппаратной платформы узлов: начиная от рабочих станций под Windows и заканчивая сетевыми устройствами Cisco (не исключая *nix, Solaris, Novell, AS400 и др.). В частности, XSpider включает мощный и глубокий анализатор защищенности веб-серверов и веб-приложений, что делает его незаменимым средством для выявления «узких мест» Интернет-магазинов и других объектов электронной коммерции. Гарантия высочайшей достоверности результатов сканирования снискала популярность и широкое применение XSpider в госучреждениях, промышленных, торговых и финансовых предприятиях, в сфере телекоммуникаций и высоких технологий.

Возможности и особенности XSpider

- **Эвристический метод определения типов и имен серверов (HTTP, FTP, SMTP, POP3, DNS, SSH)**
  Определение настоящего имени сервера и корректной работы проверок в случаях, когда конфигурация WWW-сервера скрывает его настоящее имя или заменяет его на другое.
- **Полная идентификация сервисов на случайных портах**
  Проверка на уязвимости серверов со сложной нестандартной конфигурацией, когда сервисы имеют произвольно выбранные порты.
- **Обработка RPC-сервисов (Windows и *nix) с их полной идентификацией**
  Возможности выявления уязвимостей в RPC-сервисах и определение детальной конфигурации компьютера в целом.
- **Проверка слабости парольной защиты**
  Оптимизированный подбор паролей практически во всех сервисах, требующих аутентификации, помогает выявить слабые пароли.
- **Глубокий анализ контента веб-сайтов**
  Анализ всех скриптов HTTP-серверов и поиск в них разных уязвимостей: SQL-инъекций, инъекций кода, запуска произвольных программ, получения файлов, межсайтовый скриптинг (XSS), HTTP ResponseSplitting.
- **Анализатор структуры HTTP-серверов**
  Осуществление поиска и анализа директорий, доступных для просмотра и записи, с возможностью находить слабые места в конфигурации.
- **Проведение проверок на нестандартные DoS-атаки**
  Возможность включения проверок «на отказ в обслуживании», основанных на опыте предыдущих атак и хакерских методах.
- **Минимальная вероятность ложных срабатываний**
  Использование специальных методов и механизмов, уменьшающих вероятность ошибочного определения уязвимостей в различных видах проверок.
- **Ежедневное добавление новых уязвимостей и проверок**
  Уникальная технология обновления программы предоставляет каждый день актуальную базу уязвимостей при минимальном трафике и временных затратах, не прекращая при этом работы программы, а также обеспечивает регулярное обновление программных модулей.

Сертификат ФСТЭК № 3247 (РД НДВ (4), ТУ) от 24.10.2014. Действителен до 24.10.2020.

Наши контактные данные:

ул. Ленина, д.20, (четвертый этаж), каб. 422, 423. Остановка "Яблонька".
e-mail: info@ooo-skb.ru(ссылка для отправки email)
тел. 53-20-18