Сертифицированное средство защиты информации

Средство анализа защищенности Сканер-ВС

ДОВЕРЕННАЯ СРЕДА

Сканер-ВС стартует напрямую с компакт-диска (USB-flash), загружая доверенную среду, не модифицируя программные и информационные ресурсы используемой ЭВМ и гарантированно уничтожая временную информацию по завершении работы.

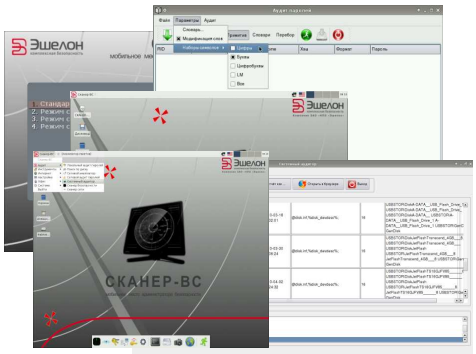
МОБИЛЬНЫЕ РЕШЕНИЯ

Вам не требуется закупать и выделять новую ЭВМ для администратора безопасности, Вы получаете среду и набор инструментов для работы администратора и аудитора безопасности фактически на любой ЭВМ в сети, только тогда, когда Вам это нужно.

АУДИТ ПАРОЛЕЙ

Сканер-ВС содержит мощные средства локального аудита паролей для операционных систем семейства Windows (2000, XP, Vista, 7) и Linux (ОС МСВС, Linux XP, Astra Linux и многих других).

Данный продукт позволяет также проводить проверку стойкости сетевых паролей (Web, E-mail, FTP, SSH и др).



НЕ ТРЕБУЕТ УСТАНОВЛЕННОЙ ОПЕРАЦИОННОЙ СИСТЕМЫ

- определение топологии и ресурсов сети
- поиск уязвимостей
- поиск остаточной информации в памяти
- локальный аудит паролей ОС
- перехват и анализ сетевого трафика
- аудит ПО и аппаратной конфигурации
- аудит паролей к сетевым сервисам

Сканер-ВС – это универсальный инструмент решения широкого спектра задач. Подобно швейцарскому ножу, он содержит модули, подходящие для разнообразных ситуаций, с которыми сталкиваются различные группы потребителей.

Данный продукт используют:

- **Операторы персональных данных**

в качестве средства анализа защищенности информации, перехвата трафика и имитации сетевых атак для выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения.

Механизм сетевого обновления Сканера-ВС позволяет администратору безопасности проверять ваши средства защиты на наличие самых актуальных закладок, уязвимостей и нарушений.

- **Контролирующие органы в ходе инспекционных проверок**

Продукт поможет осуществить контроль целостности ресурсов сети, аппаратной конфигурации ЭВМ, найдет следы несанкционированной активности пользователей (например, использование посторонних USB-устройств), а также проверит стойкость используемых паролей.

- **Объекты Минобороны России и ВС РФ**

для оперативного развёртывания места администратора информационной безопасности. В большинстве случаев не понадобится даже покупать новый компьютер и системное ПО для него – достаточно всего лишь приобрести один загрузочный компакт-диск Сканера-ВС либо заказать поставку средства на USB-носителе. Продукт имеет сертификаты Минобороны России и ФСТЭК России.

- **Испытательные лаборатории и органы аттестации**

Сканер-ВС проверяет подсистему контроля целостности, аутентификации, гарантированной очистки информации, фиксирует КС, тестирует функционал межсетевых экранов, систем обнаружения вторжений и других сетевых и локальных средств защиты информации.

Эшелон
комплексная безопасность

107023, г. Москва,
ул. Электрозаводская, д. 24.
+7(495) 645-38-09,
E-mail: mail@cnpo.ru

Сканер-ВС: защита, доступная везде

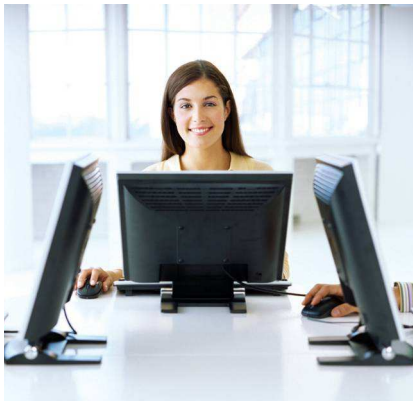
СЕТЕВЫЕ ОБНОВЛЕНИЯ

Продукт обеспечивает целостность и защиту от несанкционированных модификаций дистрибутива, поскольку находится на неперезаписываемом носителе. При этом возможно производить регулярные обновления продукта (например базы уязвимостей сканера безопасности) через Интернет или локальную сеть, Вы можете использовать любой USB-накопитель для их хранения.

ПЕРЕХВАТ ТРАФИКА

При использовании многих распространенных сетевых сервисов и протоколов (HTTP, FTP, SMTP, OSCAR и др.) возможен перехват передаваемой информации, в том числе паролей. Сетевой анализатор из состава Сканер-ВС позволяет перехватить всю передаваемую информацию между любыми узлами коммутируемой сети (с помощью технологии ARP-спуфинга) и выполнить ее анализ, в т.ч. извлечь переданные пароли.

Также возможен перехват шифрованного трафика (HTTPS) с помощью подмены сертификата.



Мы предлагаем Сканер-ВС в различных вариантах поставки и исполнения, с возможностью адаптации его состава для нужд любой организации. Продукт содержит целый арсенал средств для выполнения внутреннего или внешнего аудита сетей, тестирования проникновением, перехвата и анализа трафика, проверки стойкости сетевых и локальных паролей. Поддерживает аудит паролей для широкого спектра современных операционных систем Windows (2000, XP, Vista, 7) и Linux (ОС МСВС, Linux XP, Astra Linux и др.).

Продукт не требует изменения конфигурации локальной ЭВМ и сети, так как загружается с внешнего носителя и автоматически распознает сеть.

Базовые инструменты:

МЫ ОБЕСПЕЧИВАЕМ

- Техническую поддержку
- Онлайн-обновления
- Обучение работе с продуктом
- Различные варианты поставки
- Гарантийное обслуживание
- Сертификат Минобороны России
- Сертификат ФСТЭК России

Эшелон
комплексная безопасность

107023, г. Москва,
ул. Электрозаводская, д. 24.
+7(495) 645-38-09,
E-mail: mail@cnpo.ru

СКАНЕР БЕЗОПАСНОСТИ

Сканер безопасности из состава продукта позволяет проводить инвентаризацию сетевых сервисов, определение типов сетевых устройств и операционных систем, и на основе собранной информации проводить тестирование безопасности путем имитации различных видов атак (используется обновляемая международная база, включающая до 17 000 уязвимостей).

СИСТЕМНЫЙ АУДИТОР

В ходе проверок рабочих мест часто возникает необходимость контроля программно-аппаратной конфигурации. Приложение «Системный аудитор» из состава Сканера-ВС обеспечивает снятие «снимка» текущей аппаратной конфигурации и информации об установленных операционных системах, их приложениях, настройках, событиях (выход в интернет, использование USB-устройств).

На основе собранной информации можно построить подробный отчет, а также сравнить «снимки» за разный период времени.

Правовая база обязательности применения «Сканер-ВС»

ДОКТРИНА ИБ РФ (№ ПР-1895)

«Организационно-техническими методами обеспечения информационной безопасности РФ являются:

… использование методов контроля эффективности средств защиты информации»

ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РФ 2007 г. N 781

«Должен быть обеспечен … постоянный контроль за обеспечением уровня защищенности»

РД. КОНЦЕПЦИЯ ЗАЩИТЫ СВТ И АС ОТ НСД (ГОСТЕХКОМИССИЯ)

«Неотъемлемой частью работ по защите является оценка эффективности средств защиты …. Защита АС должна предусматривать контроль эффективности средств защиты … »

РД. АС. ЗАЩИТА ОТ НСД К ИНФОРМАЦИИ. КЛАССИФИКАЦИЯ АС… (ГОСТЕХКОМИССИЯ)

«Должно проводиться периодическое тестирование функций СЗИ… . **Администратор должен иметь свой терминал и необходимые средства оперативного контроля …»**

ПРИКАЗ ФСТЭК РОССИИ 2010 г. N 58

«Основными методами и способами защиты информации от несанкционированного доступа являются: … анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности)…»

СПЕЦИАЛЬНЫЕ ТРЕБОВАНИЯ…

ТРЕБОВАНИЯ К КЛЮЧЕВЫМ СИСТЕМАМ…

ДРУГИЕ ВЕДОМСТВЕННЫЕ ДОКУМЕНТЫ

ISO 27001

Сертифицированные аналоги

Сканер-ВС	Аналогичный сертифицированный продукт
Локальный аудит паролей	-
Сетевой аудит паролей	-
Сканер безопасности	Обычный сканер безопасности
Системный аудитор	-
Сканер сети	-
Поиск остаточной информации	Обычное средство поиска остаточной информации
Гарантированная очистка информации	Обычное средство гарантированной очистки информации
Программа инспекционного контроля — снятие контрольных сумм	Обычное средство контроля целостности
Анализатор протоколов	-
Наличие операционной системы не требуется	Требуется наличие сертифицированной версии операционной системы

Эшелон
комплексная безопасность

107023, г. Москва,
ул. Электрозаводская, д. 24.
+7(495) 645-38-09,
E-mail: mail@cnpo.ru