Сканер-ВС

швейцарский нож администратора безопасности

Митков Максим,

заместитель директора департамента программных разработок

ЗАО «НПО «Эшелон»

Назначение

- Оперативный контроль (сканирование)
- Мониторинг и анализ защищенности системы от атак (программно-аппаратных воздействий)

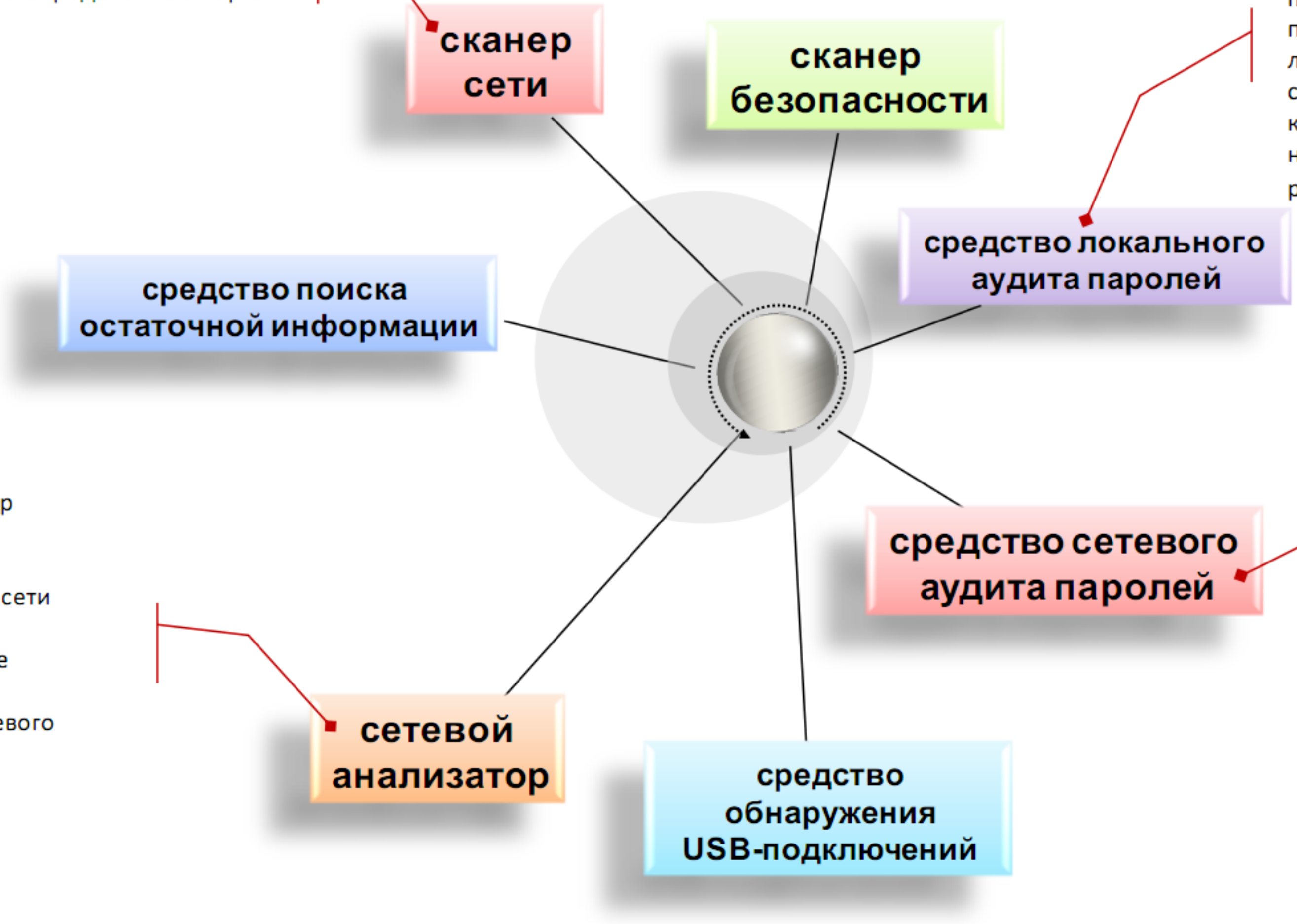
- Контроль соблюдения требований защищенности, а также инвентаризации сети.

Эшелон
комплексная безопасность

Возможности

- Загрузка доверенной среды с любого компьютера (по технологии Live-CD/Live-flash) с автоматическим определением сетевого оборудования, подключенного к вычислительной сети
- Поиск остаточной информации на накопителях (поддерживаются различные кодировки, словари паттернов)
- Локальный (на любом ПК) и сетевой аудит парольной защиты
- инвентаризация (фиксация) ресурсов компьютерной сети (узлов, портов, сервисов)
- Выявление (сканирование) уязвимостей сетевых сервисов
- Проверка возможности осуществления атак на отказ в обслуживании и подмены адреса
- Анализ сетевого трафика (в т.ч. в коммутируемых сетях, физически разделенных)
- Аудит парольной информации для множества протоколов
- Аудит общесистемной информации и истории подключений USB-устройств.

Состав комплекса



сканер сети

Сканер сети предназначен для проверки безопасности сети посредством поиска хостов, в которых открыты определенные порты.

сканер безопасности

средство локального аудита паролей

Средство локального аудита паролей предназначено для поиска и выявления паролей, содержащих легко подбираемые символьные комбинации, непосредственно на рабочей станции.

средство поиска остаточной информации

средство сетевого аудита паролей

Средство сетевого аудита паролей предназначено для удаленного поиска и выявления паролей, содержащих легко подбираемые символьные комбинации.

сетевой анализатор

Сетевой анализатор предназначен для использования администратором сети при проверке и детальном анализе правильности конфигурации сетевого программного обеспечения.

средство обнаружения USB-подключений

Преимущества

- Организация выделенного или виртуального рабочего места администратора безопасности
- Возможность применения при проведении сертификационных и аттестационных испытаний
- Активное выявление уязвимостей сетевых сервисов
- Аудит парольной информации для множества протоколов
- Контроль памяти и трафика
- В комплект поставки входит бесплатный курс обучения администратора «Сканер-ВС»

Варианты поставки

1. CD-ROM
2. Flash-носитель
3. Ноутбук с уже предустановленным средством

Эшелон
комплексная безопасность

Нормативные основания применения

1) Приказ ФСТЭК России от 5 февраля 2010 г. N 58 г. Москва "**Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных**". Регистрационный №16456.

- **Пункты Положения:** 2.4, 2.6.

2) Постановление Правительства РФ от 17 ноября 2007 г. N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных".Пункты Положения: 11. д)

Эшелон
комплексная безопасность

Нормативные основания применения

3) **Руководящий документ.** Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации.

- **Требование руководящего документа к классам защищенности:** 3Б, 3А, 2Б, 2А, 1Д, 1Г, 1В, 1Б, 1А о периодическом тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД.

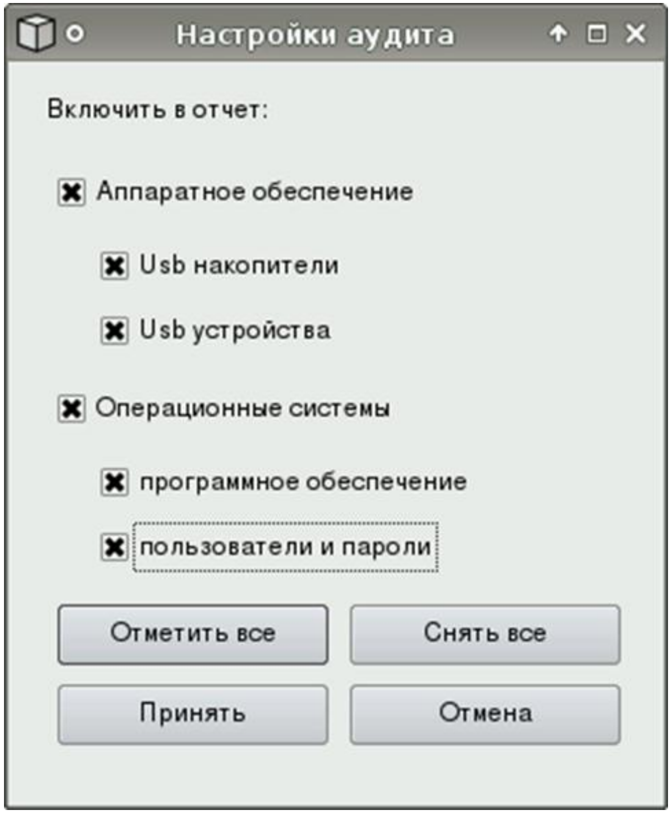
5) **Доктрина информационной безопасности Российской Федерации**, утвержденная Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895.

6) **«Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры»** утверждены Заместителем директора ФСТЭК России 18 мая 2007 г.

Системный локальный аудит

Системный аудитор предназначен для сканирования рабочей станции на предмет определения параметров:

- установленных операционных систем;
- системных, коммуникационных и периферийных устройств, в том числе USB-устройств;
- перечень использованных на компьютере USB-носителей;
- снимок программно-аппаратной конфигурации.



Включить в отчет:

☒ Аппаратное обеспечение
  ☒ Usb накопители
  ☒ Usb устройства
☒ Операционные системы
  ☒ программное обеспечение
  ☒ пользователи и пароли

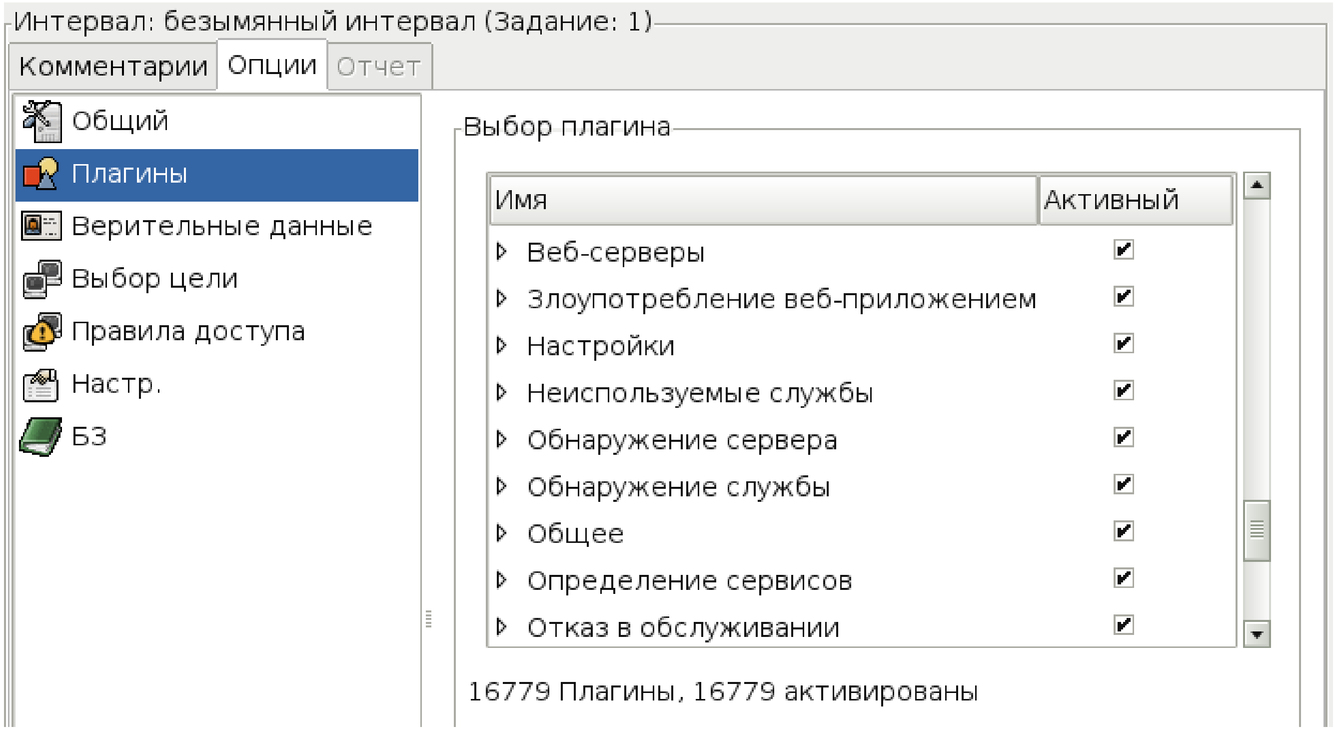
Эшелон
комплексная безопасность

Сканер безопасности

- Сканер безопасности позволяет осуществлять поиск уязвимостей в сетевых сервисах, предлагаемых операционными системами, межсетевыми экранами, маршрутизаторами и другими сетевыми компонентами.
- Для поиска уязвимостей используются как стандартные средства тестирования и сбора информации о конфигурации и функционировании сети, так и специальные средства, эмулирующие действия злоумышленника по проникновению в системы, подключенные к сети.

Сканер безопасности

Выбор плагинов:



Интервал: безымянный интервал (Задание: 1)

Выбор плагина

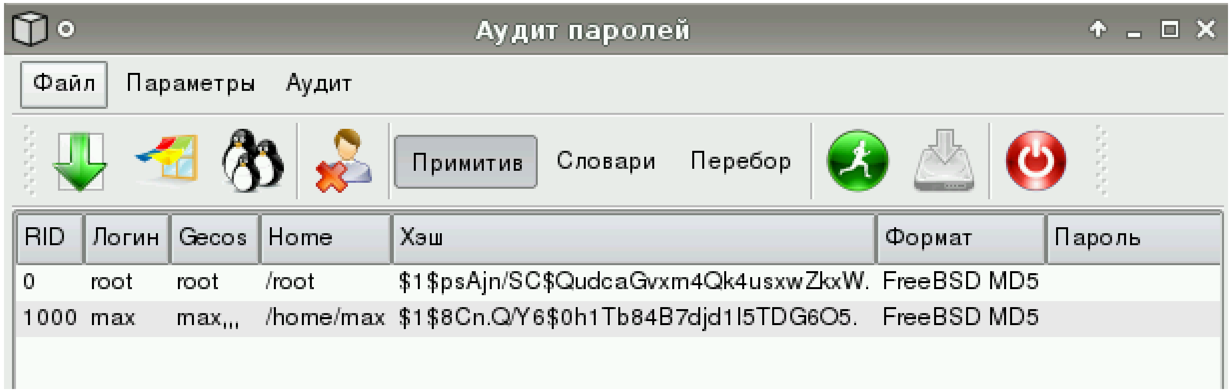
Имя	Активный
Веб-серверы	☑
Злоупотребление веб-приложением	☑
Настройки	☑
Неиспользуемые службы	☑
Обнаружение сервера	☑
Обнаружение службы	☑
Общее	☑
Определение сервисов	☑
Отказ в обслуживании	☑

16779 Плагины, 16779 активированы

Аудит паролей локальный

Средство предназначено для поиска и выявления паролей, содержащих легко подбираемые символьные комбинации, непосредственно на рабочей станции.

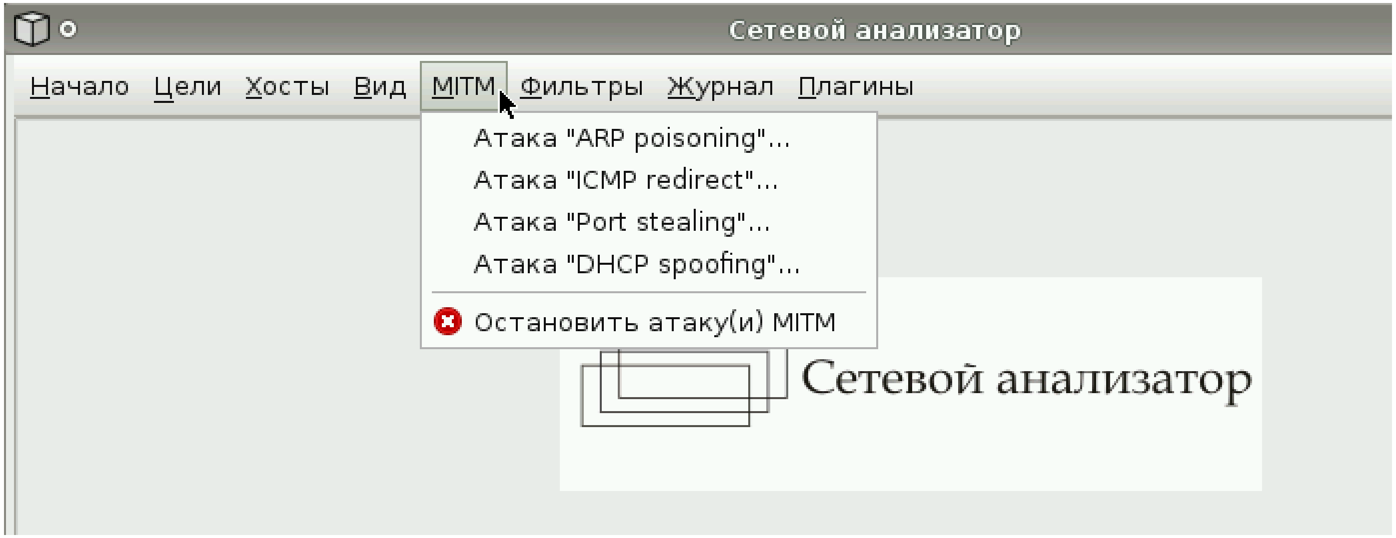
➢ Широкий перечень поддерживаемых ОС: Windows (2000, XP, Vista, 7), Linux (ОС МСВС, Linux XP, Astra Linux).



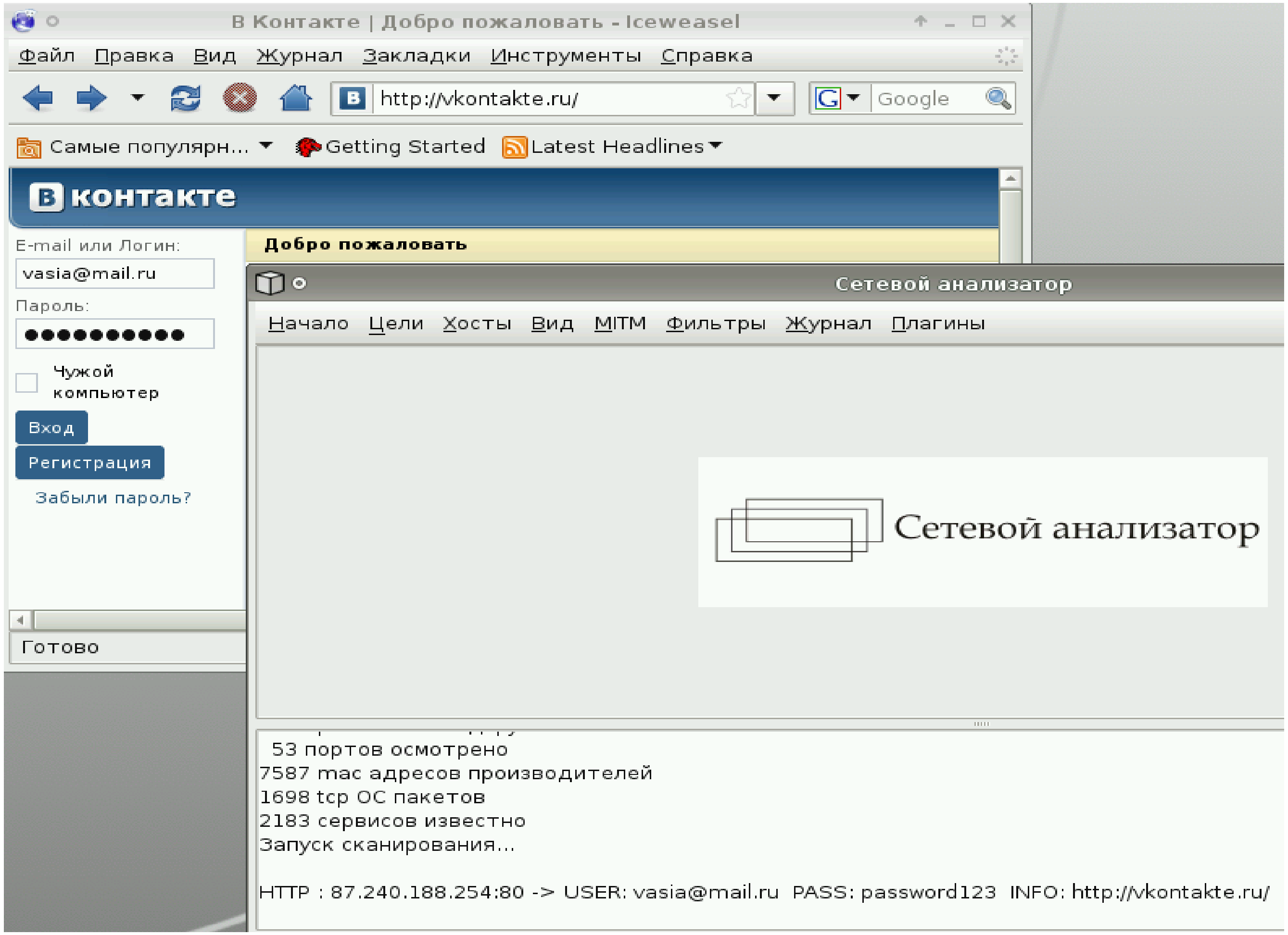
RID	Логин	Gecos	Home	Хэш	Формат	Пароль
0	root	root	/root	1psAjn/SC$QudcaGvxm4Qk4usxwZkxW.	FreeBSD MD5	
1000	max	max,,,	/home/max	$1$8Cn.Q/Y6$0h1Tb84B7djd1I5TDG6O5.	FreeBSD MD5	

Перехват трафика

Сетевой анализатор предназначен для использования администратором сети при проверке и детальном анализе правильности конфигурации сетевого программного обеспечения.



Перехват трафика



E-mail или Логин: vasia@mail.ru

Пароль: ●●●●●●●●●●●

☐ Чужой компьютер

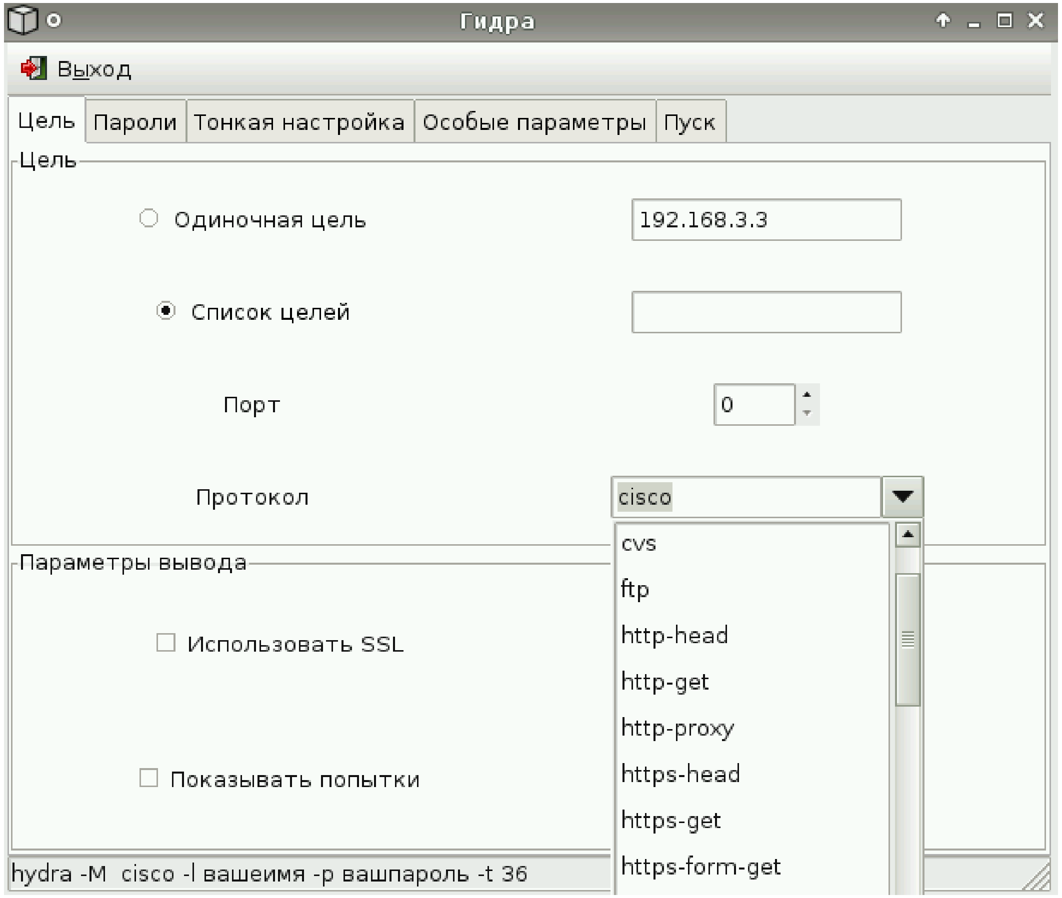
```
 53 портов осмотрено
7587 mac адресов производителей
1698 tcp ОС пакетов
2183 сервисов известно
Запуск сканирования...

HTTP : 87.240.188.254:80 -> USER: vasia@mail.ru  PASS: password123  INFO: http://vkontakte.ru/
```

Эшелон
комплексная безопасность

Подбор сетевых паролей

- Поддержка множества сетевых протоколов
- Перебор по словарю
- Многопоточный перебор



○ Одиночная цель 192.168.3.3

● Список целей

Порт 0

Протокол cisco

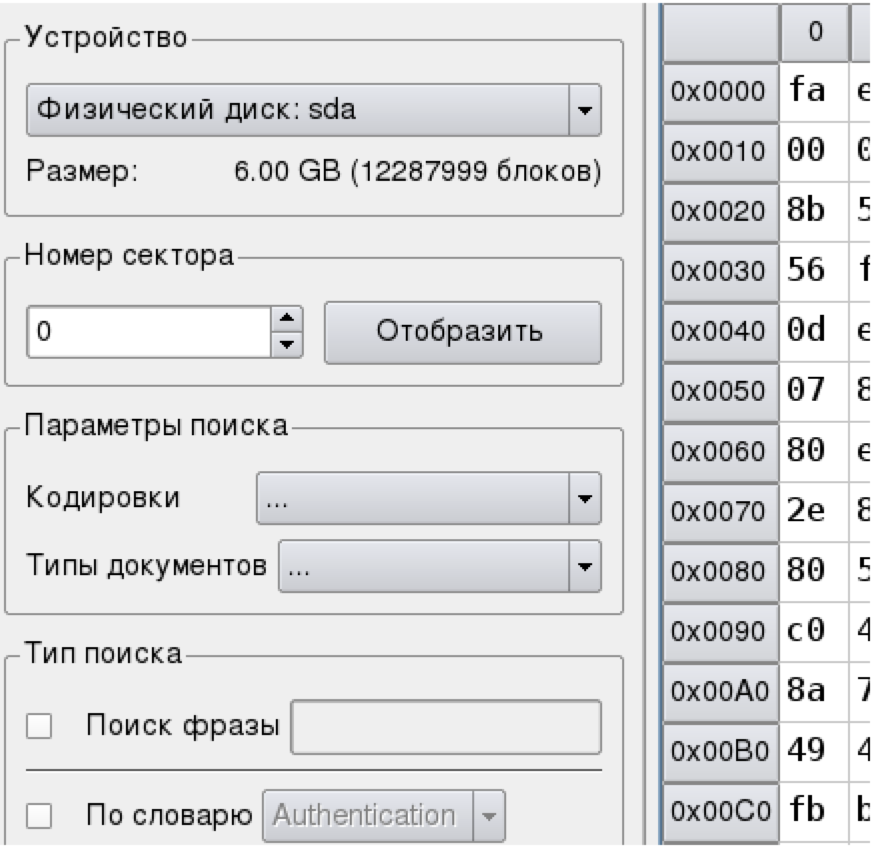
☐ Использовать SSL

☐ Показывать попытки

```
hydra -M  cisco -l вашеимя -p вашпароль -t 36
```

Поиск информации

Средство поиска по диску предназначено для поиска информации по ключевым словам на носителях данных (жестких дисках, дискетах, оптических дисках).



Устройство

Физический диск: sda

Размер: 6.00 GB (12287999 блоков)

Номер сектора

0

Параметры поиска

Кодировки: ...

Типы документов: ...

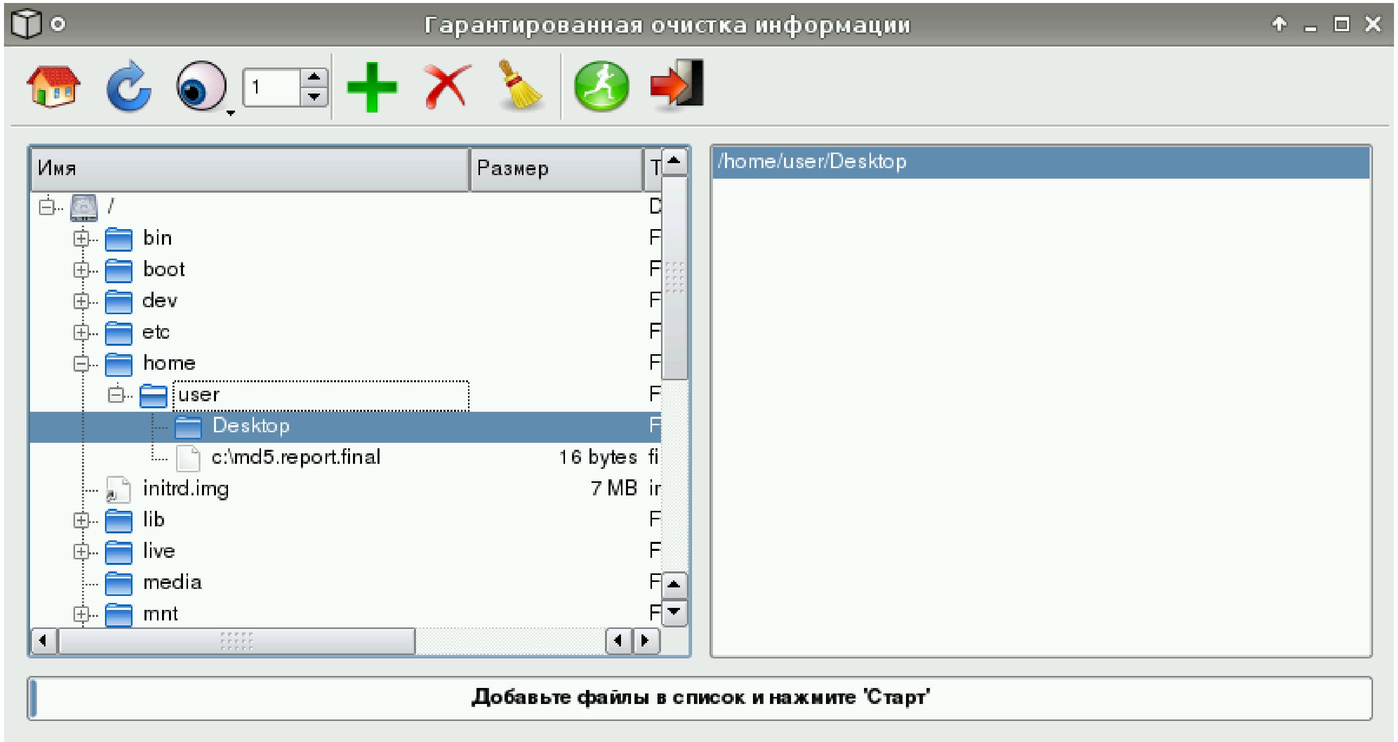
Тип поиска

☐ Поиск фразы

☐ По словарю: Authentication

```
        0
0x0000  fa
0x0010  00
0x0020  8b
0x0030  56
0x0040  0d
0x0050  07
0x0060  80
0x0070  2e
0x0080  80
0x0090  c0
0x00A0  8a
0x00B0  49
0x00C0  fb
```

Гарантированное уничтожение информации



Имя	Размер	Т
/		D
bin		F
boot		F
dev		F
etc		F
home		F
user		F
Desktop		F
c:\md5.report.final	16 bytes	fi
initrd.img	7 MB	ir
lib		F
live		F
media		F
mnt		F

/home/user/Desktop

Добавьте файлы в список и нажмите 'Старт'

- ✓ Реализует алгоритм Питера Гутмана
- ✓ Вплоть до 32 итераций стирания

Эшелон
комплексная безопасность

Сравнение продуктов

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

Сертификаты

Сертификат Минобороны России

Сертификат ФСТЭК России

Контакты для приобретения

ЗАО "НПО "Эшелон"

107023, ул. Электрозаводская, д. 24

Телефоны и факсы: +7(495) 645-38-09, 645-38-10, 645-38-11

E-mail: mail@npo-echelon.ru

www.npo-echelon.ru

Эшелон
комплексная безопасность