

The background is a solid blue color. In the top-left corner, there is a faint, semi-transparent image of a globe showing the continents. On the right side, there are several overlapping, semi-transparent white geometric shapes, including concentric arcs and a larger, more complex polygonal shape, suggesting a technical or digital theme.

Internet Scanner

Назначение продуктов компании ISS

Автоматизация процесса поиска уязвимостей узлов, протоколов и служб IP - сетей



Автоматизация процесса обнаружения атак на узлы, протоколы и службы IP - сетей, реагирование на атаки



Программные продукты компании ISS

Internet Scanner - поиск уязвимостей уровня сети

System Scanner - поиск уязвимостей уровня операционной системы

Database Scanner - поиск уязвимостей уровня баз данных

RealSecure OS Sensor - обнаружение атак на уровне операционной системы

RealSecure Network Sensor - обнаружение атак на уровне сети



www.iss.net/xforce - база данных обнаруженных уязвимостей с возможностью подписки

Место продуктов компании ISS в комплексе средств безопасности

Уязвимости

Атаки

Приложения

Базы данных

Операционные системы

Сети

Database Scanner	
System Scanner	RealSecure OS
Internet Scanner	RealSecure Network

Анализ защищенности на уровне сети

Моделирование действий внешних хакеров

Анализ сетевых устройств, сервисов и протоколов

Обнаружение неизвестных устройств

Инвентаризация всего ПО и сетевого оборудования

Централизованное сканирование

Взгляд на безопасность сети «со стороны»



Анализ защищенности сетевых служб и протоколов стека TCP/IP

Анализ защищенности рабочих станций (Windows 3.x, 9x, NT, UNIX), маршрутизаторов, межсетевых экранов, Web-серверов, принтеров и т.п.

Единственная сертифицированная
Гостехкомиссией России
система анализа защищенности

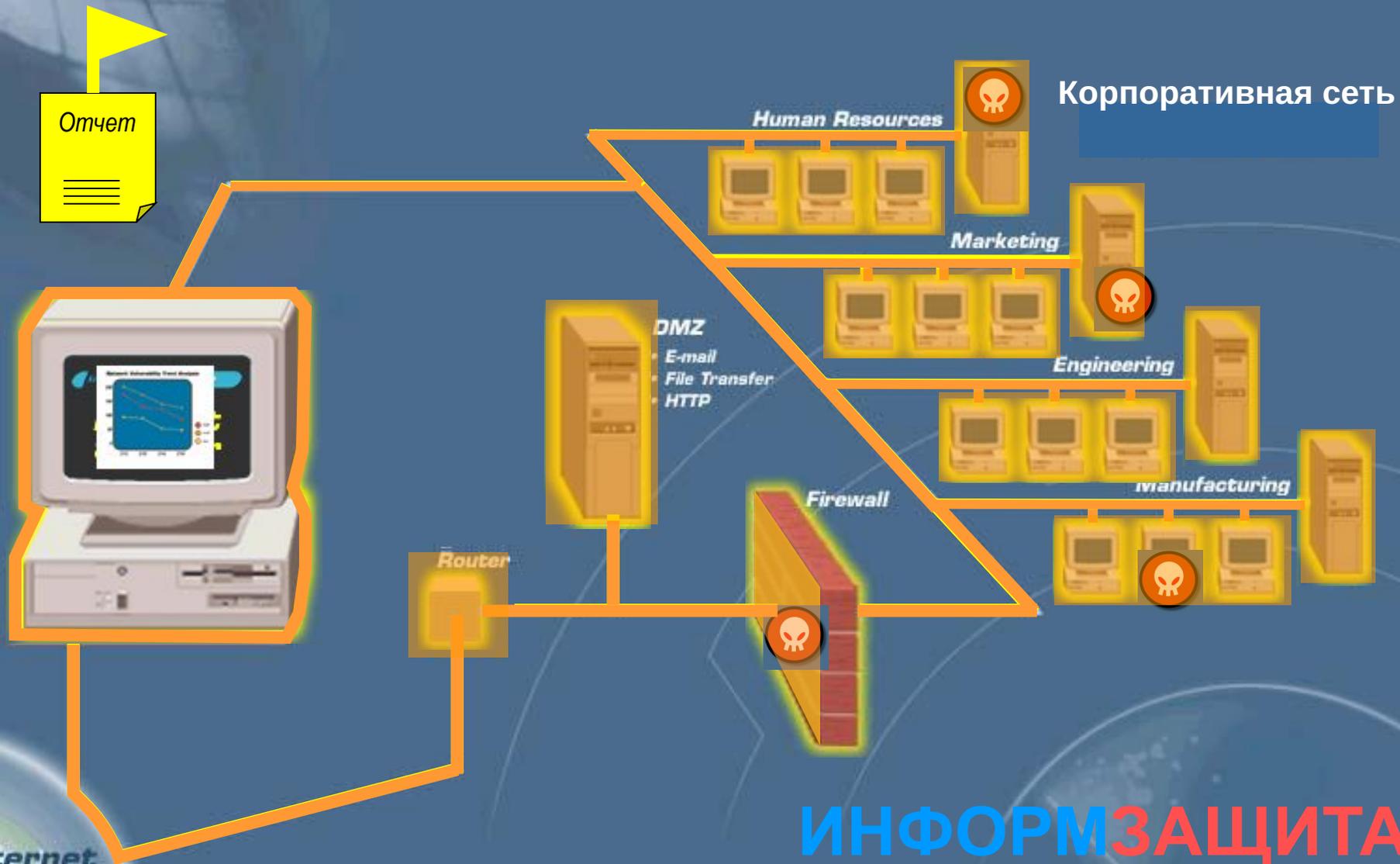
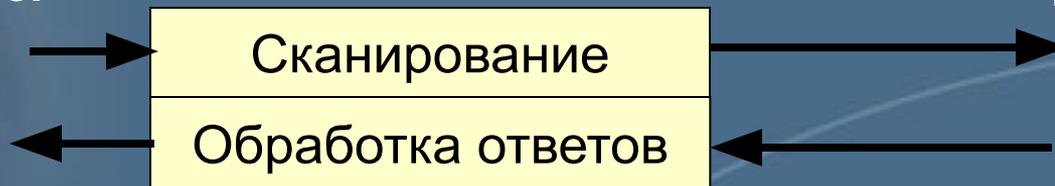


Схема работы системы Internet Scanner

Internet Scanner



Сканируемый узел



- Модуль сканирования
- Интерфейс пользователя
- Модуль генерации отчётов
- База данных проверок

Принципы работы Internet Scanner

Сканирование

механизм пассивного анализа, с помощью которого сканер пытается определить наличие уязвимости без фактического подтверждения ее наличия - по косвенным признакам.

Зондирование

механизм активного анализа, который позволяет убедиться, присутствует или нет на анализируемом узле уязвимость путем имитации атаки, использующей проверяемую уязвимость.

ИНФОРМАЦИЯ

СКАННЕР^{МТ}

Характеристики

Почти 800 проверок

Гибкая настройка

Параллельное сканирование до 128 узлов сети

Запуск по расписанию

Работа из командной строки

Различные уровни детализации отчетов

Создание собственных проверок

Типы отчетов

- Для руководства компании
- Для руководителей отделов
- Для технических специалистов

Итоговый отчет по уязвимостям

Дата: Апрель 28, 1999

Описание отчета:

Этот отчет описывает подверженность организации к атакам информации политик безопасности. График описывает уязвимости различной степени риска, процентно-отношение, а также общее число обнаруженных уязвимостей. Уязвимости с высокой степенью риска: высокая (High), средняя (Medium) и низкая (Low). Уязвимости высокой степени риска приводят к нежелательным доступу к жести, данным, сети. Уязвимости средней степени риска могут привести к нежелательному доступу к важным данным, что позволяет разработать уязвимости высокой степени риска. Уязвимости низкой степени риска приводят к нежелательному доступу к не очень важным данным. Рекомендуется как можно скорее устранить уязвимости высокой степени риска.

Имя сессии:	Session1	ID сессии:	6
Шаблон:	Light Scan	Статус:	Finished
Имя файла:	Session_90002		
Общие сведения о сканировании:			
Число хостов:	1	Начало:	1999-04-27 16:06:1
Активный:	1	Конец:	1999-04-27 16:11:1
Поиск уязвимостей:		Общая время:	00:04:52



Особенности Internet Scanner Начиная с версии 6.0

Усовершенствованный интерфейс

Аналогичен проводнику Windows

Встроенный редактор политик Policy Editor

Проверка портов UDP

Утилита X-Press Update

*Возможность обновления
тестов на уязвимость*

Недостатки Internet Scanner

Сбои при определении служб UDP

Повышенные требования к полосе пропускания сети

Отсутствие централизованного управления



Политики сканирования

Level 1

Типы
операционных
систем узлов

Level 2

Запущенные на узлах службы

Level 3

Возможность атак со стороны
неквалифицированных злоумышленников

Level 4

Возможность атак с помощью различных
инструментальных средств

Level 5

Высокая квалификация атакующего, проверка неверных конфигураций

Сессии сканирования

Определение

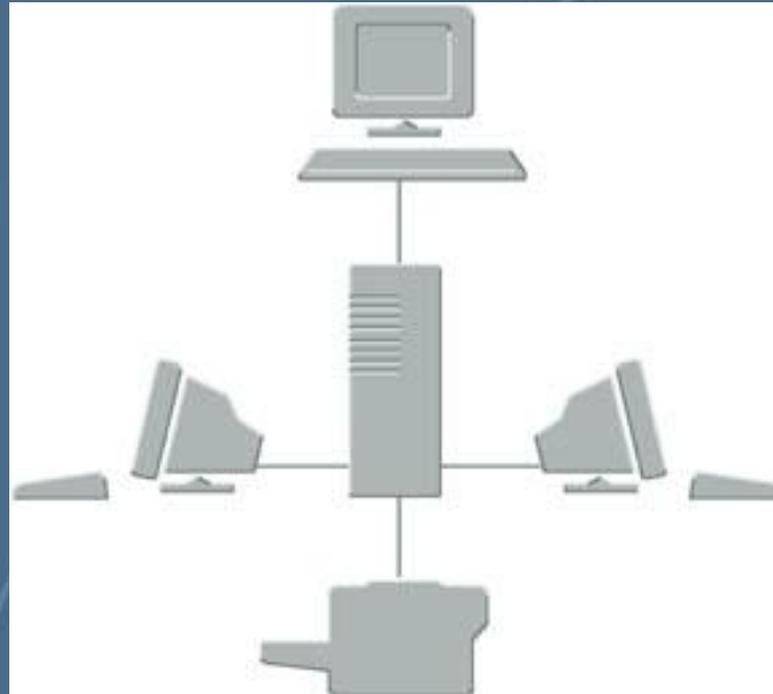
Политика



Ключ



Множество устройств



Ключ лицензирования

Key = характеризует лицензию на Internet Scanner.



Необходимые компоненты

Дистрибутив

Key file – файл с ключом лицензирования

Windows NT или Windows 2000 Professional CD



Способы сканирования

Main window



Iss_WinNT.exe.lnk

Console Mode

```
ISS Internet Scanner
Key Name: C:\Program Files\ISS\Scanner6\scan.key
Policy Name: L2 Classification
Scanning 1 Host(s)...
Scanning Host: 200.0.0.125
-
```

Command line



_default.pif