Внешний аудит безопасности корпоративных сетей

Лекция 2
Базовые сетевые протоколы и их безопасность

Семён Новосёлов

2021

Crypto Kantiana

БФУ имени И. Канта

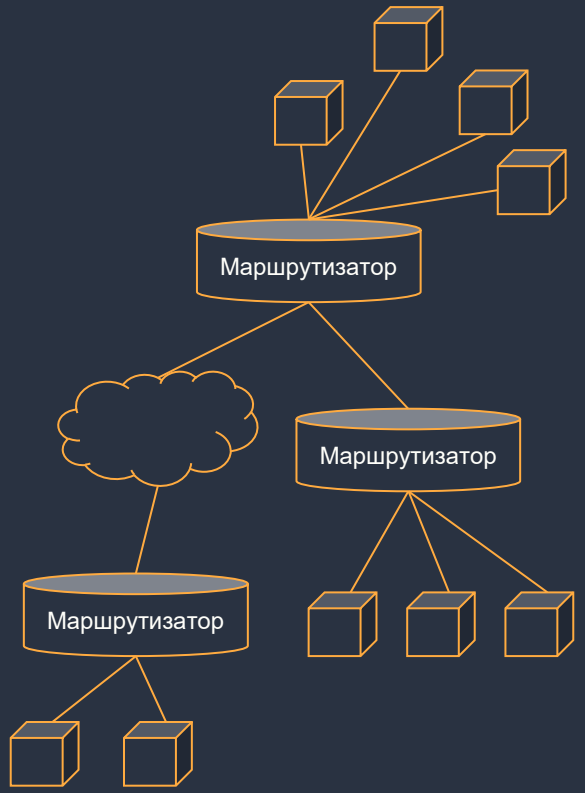
Устройство сети Интернет

Стек TCP/IP - базовый набор протоколов на котором строится Интернет.

- данные разбиваются на кусочки (сегменты, кадры, пакеты) и передаются по очереди
- организован по принципу “матрёшки”
- делится на уровни, которые вкладываются друг в друга:
  - Канальный уровень - физическая передача данных (Ethernet, Wi-Fi, L2TP)
  - Сетевой уровень - передача данных между физ. сетями (IPv4, IPv6, ICMP)
  - Транспортный уровень - установление базовых каналов передачи данных (TCP, UDP)
  - Прикладной уровень - протоколы приложений и сервисов (DNS, HTTP, SSH)

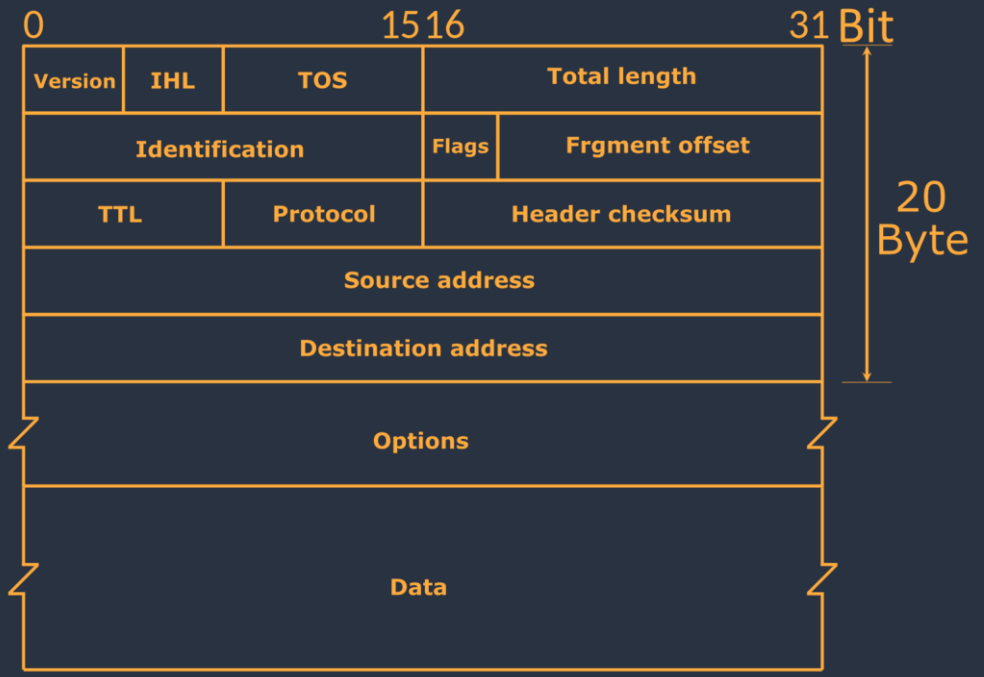
Протокол IP

- предполагается, что можно передавать данные по физическому каналу
- отвечает за маршрутизацию
  - каждому узлу назначается адрес (IP-адрес, 32 бит в IPv4, 128 бит в IPv6)
- для передачи пакетов по физическим сетям с разной пропускной способностью используется фрагментация
- нет гарантий доставки пакета



Формат пакета

- чтобы передать пакет необходимо сформировать заголовок с IP-адресом отправителя и получателя и данные



Traceroute. 1/2

Проследить путь пакета до заданного узла позволяют инструменты traceroute/tracepath/tracert

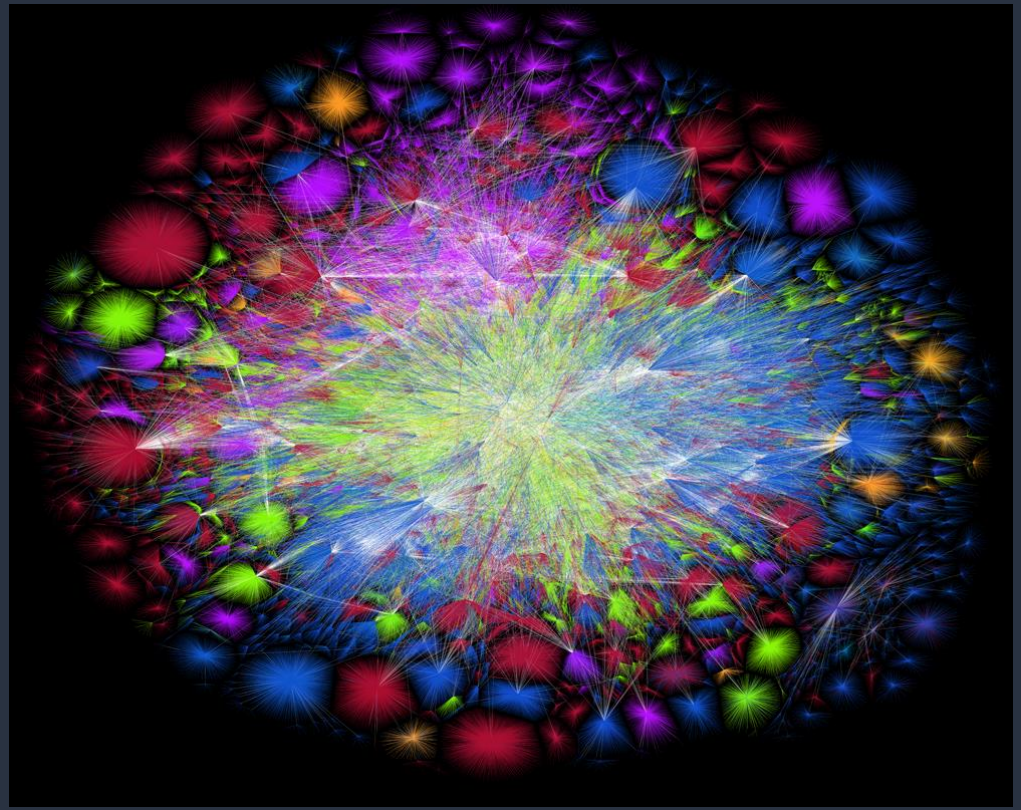
Они используют поле “время жизни пакета” (TTL) - число промежуточных хостов.

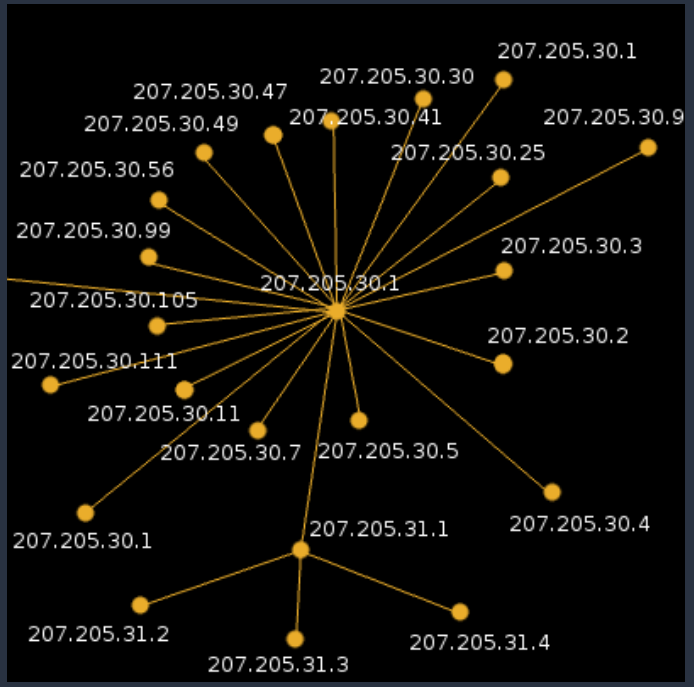
- TTL уменьшается на единицу при прохождении каждого узла
- если TTL = 0, то хост отправляет сообщение ICMP Time Exceeded
- утилита отправляет последовательно пакеты с TTL=1,2,3, …
- промежуточные узлы возвращают пакет ICMP Time Exceeded с IP-адресом узла в адресе отправителя

Traceroute. 2/2

```
n7v@n7v-laptop:~$ tracepath -b yandex.ru
 1?: [LOCALHOST]                      pmtu 1400
 1:  _gateway (192.168.1.1)                                1.343ms
 1:  _gateway (192.168.1.1)                                0.780ms
 2:  37-147-176-1.broadband.corbina.ru (37.147.176.1)      1.460ms
 3:  81.211.111.30 (81.211.111.30)                         1.861ms
 4:  spb-62-141-124-161.sovintel.spb.ru (62.141.124.161)   4.811ms
 5:  pe16.Moscow.gldn.net (79.104.235.207)                36.149ms
 6:  no reply
```

Карта сети Интернет - 2015 (The Opte Project)





Пример узла сети

Протокол IP. Безопасность

- адрес отправителя/получателя можно подделать (IP-spoofing)
- фрагментация может использоваться для обхода систем защиты
  - для анализа содержимого пакета его нужно собрать
  - для этого требуется хранить фрагментированные пакеты в буфере, который имеет ограниченный размер
  - хакер может посылать пакеты с задержками по времени и в разном порядке, что в нагруженных системах может привести к полному заполнению буфера пакетов и пропуску не проверенных пакетов в сеть (обход антивирусов, СОВ, файерволов)

Протокол IP. Безопасность

- перебор адресов получателя и отправка ping-запросов по протоколу ICMP позволяет идентифицировать узлы сети
- в протоколе отсутствует шифрование

Порты

- протокол IP позволяет передать данные между узлами сети
- для распределения данных по сервисам (напр., программам на компьютере) служат порты - номера сервисов
- Протоколы: UDP/TCP

Примеры

80	HTTP/Skype
443	HTTPS
22	SSH

Транспортный уровень. Протокол UDP

UDP = IP + Порты + Контрольная сумма (заголовка)

- Доставка пакета и порядок пакетов не гарантируется
- Используется там, где это не критично (напр., передача видео)

Транспортный уровень. Протокол TCP

TCP = IP + Порты + Гарантии доставки пакета

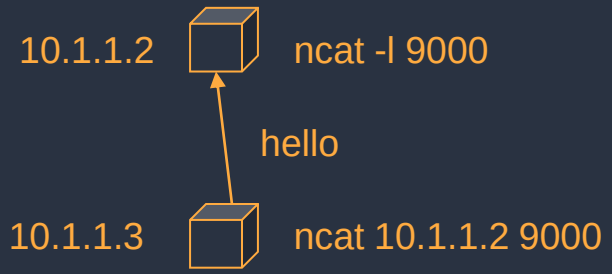
- Поддерживается создание соединения
- Основной принцип: если не получено подтверждение доставки от получателя (ответный пакет с флагом ACK) в течении некоторого времени, то отослать пакет заново.

Утилита netcat

- используется для подключения по TCP/UDP и отсылки данных, введенных в консоли
- nc в Linux
- ncat из состава Nmap в Windows/Linux
- подключится можно к любому компьютеру/серверу в сети Интернет

Пример. Чат по TCP между двумя компьютерами. 1/2

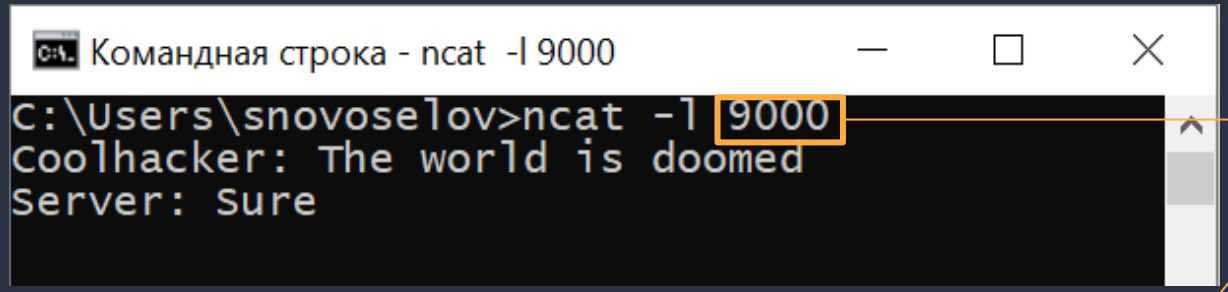
1. Для создания соединения следует один из компьютеров выбрать в качестве сервера
2. Второй компьютер к нему подключается
3. После подключения все введенные данные отправляются в обе стороны



- Связь работает в рамках локальной сети
  - например, компьютеры подключены к одной Wi-Fi точке доступа и нет изоляции клиентов
- Для связи по сети Интернет необходимо, чтобы один из компьютеров имел внешний (не локальный) IP-адрес

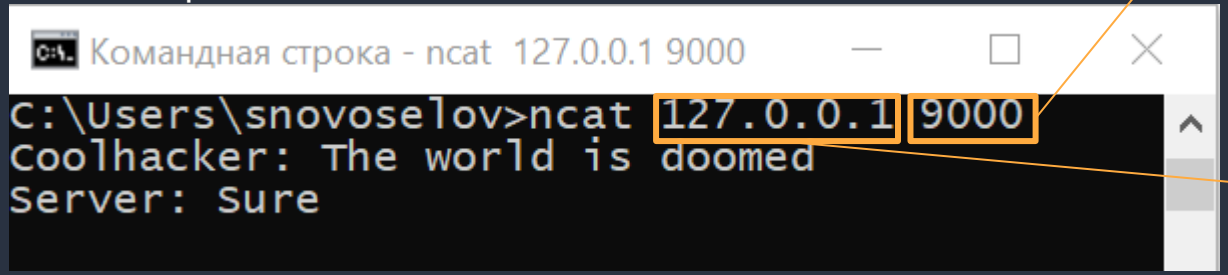
Пример. Чат по TCP между двумя компьютерами. 2/2

Компьютер-сервер



Порт, можно выбрать любое значение

Компьютер-клиент:

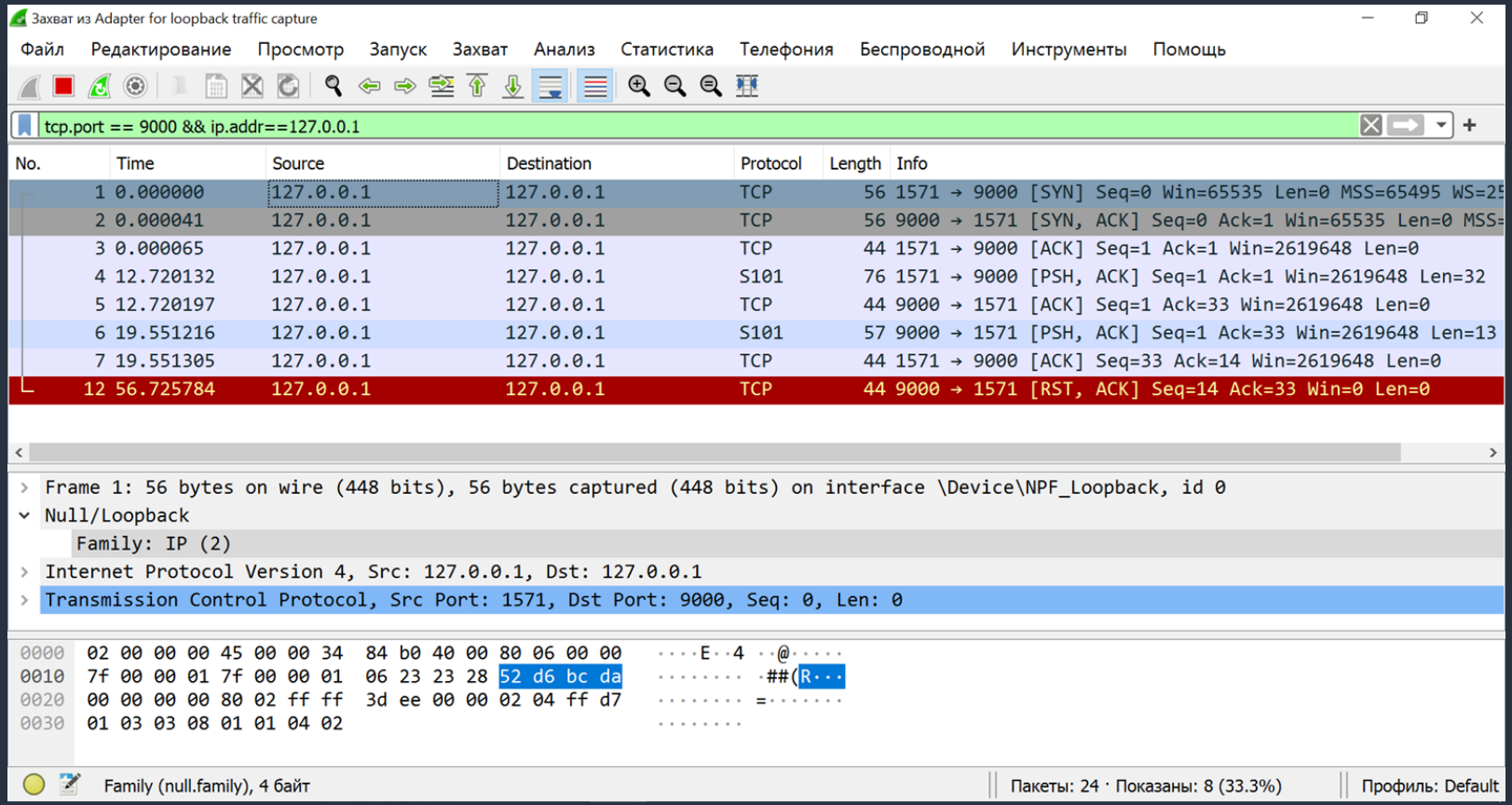


IP-адрес сервера, может быть любой адрес в Интернете

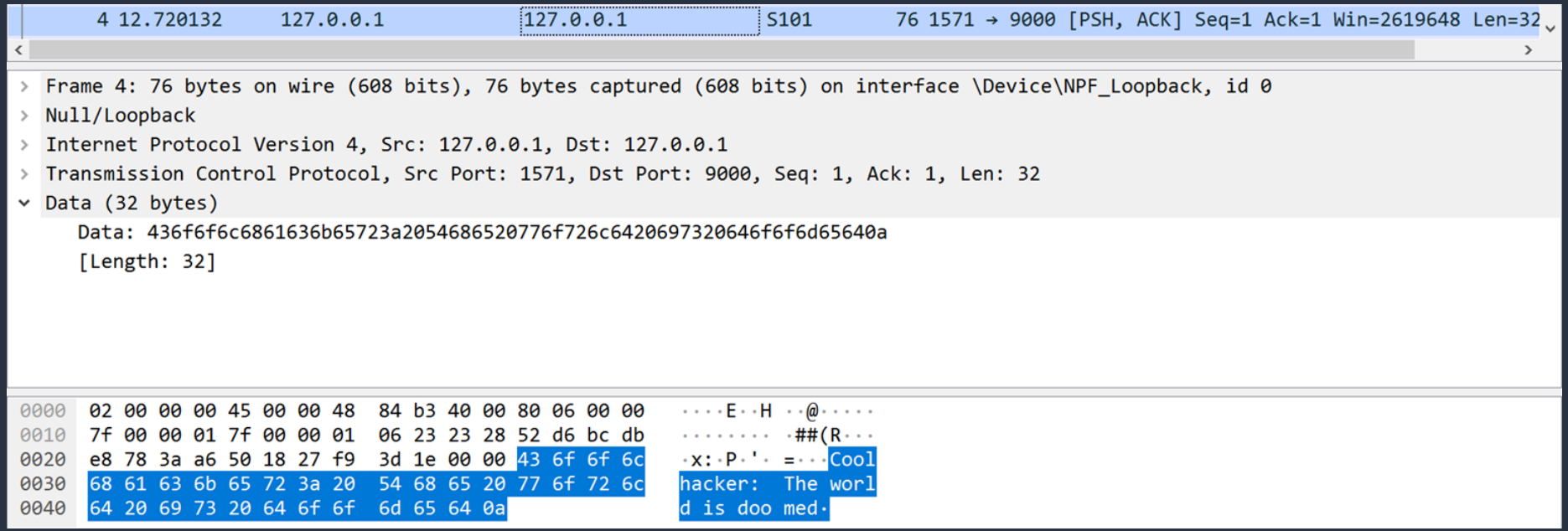
Как это выглядит на уровне сетевых пакетов?

Для просмотра пакетов используются анализаторы сетевого трафика.

Wireshark - наиболее известный и продвинутый анализатор (www.wireshark.org)



Пакеты TCP для примера с чатом.



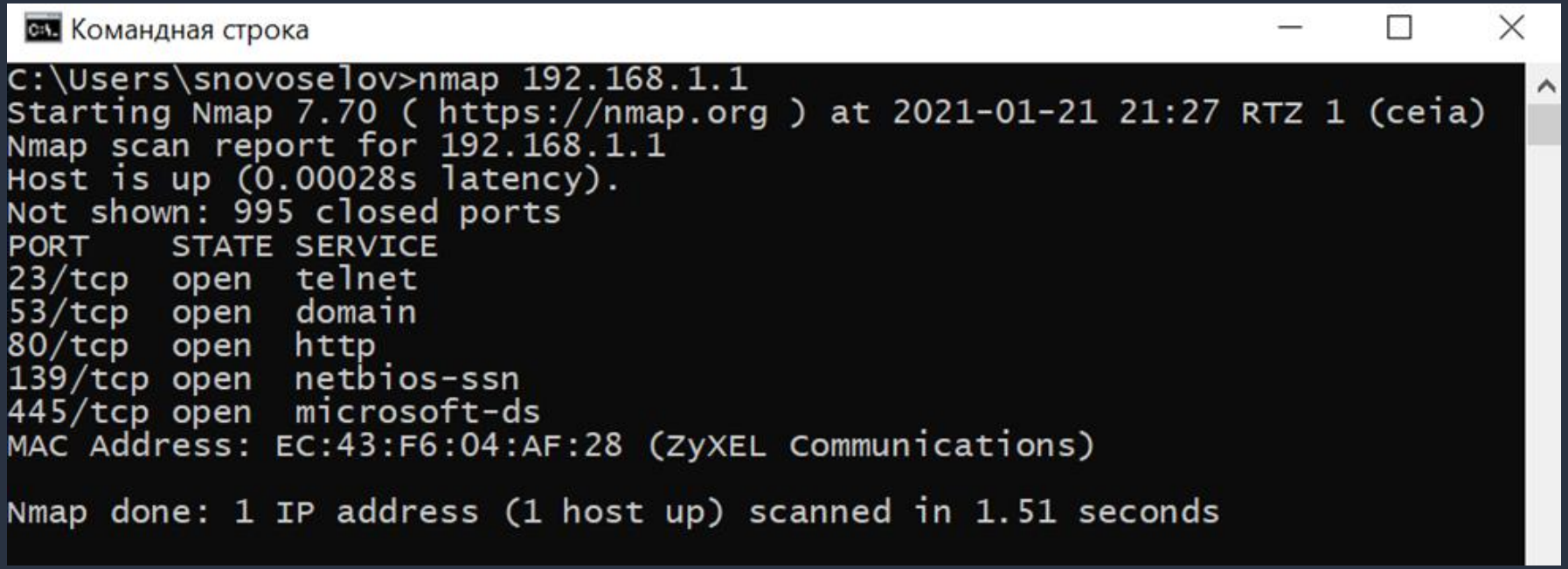
Пакет TCP сообщением от компьютера-клиента.

Шифрование не предусмотрено (нужно использовать TLS-протокол).

Сканирование портов

- Для нахождения сервисов и программ доступных на целевой системе можно использовать перебор
- В протоколе TCP/UDP предусмотрено всего 65535 портов
- Для сканирования есть множество различных техник с целью добится ответа от системы в том числе при наличии средств защиты
- В основном техники основаны на манипуляциях с полями в заголовке протокола

Сканирование портов. Пример для роутера



как видно здесь есть telnet, можно попытаться подобрать пароль:
nmap -p 23 --script telnet-brute 192.168.1.1

Определение версий ПО. 1/2

- определение версии ОС
  - анализ ответов хоста на нестандартные IP/UDP/TCP пакеты
  - значения по-умолчанию для заголовков пакетов (например, размер окна TCP)
  - используемые начальные значения последовательностей
  - статистические характеристики генераторов случайных чисел
- определение версий сервисов и программ
  - часто при подключении сервер возвращает строку-баннер с версией
    пример: “Server: nginx/1.4.2”
  - “отпечатки” с ответами на специально составленные запросы

Определение версий ПО. 2/2

- сканер nmap содержит реализацию большинства техник и вместе с базами запросов (nmap-service-probes)
- после определения версий ПО, их можно проверить по базам уязвимостей и эксплойтов (NVD, exploit-db.com)

Пример. Определение версий с помощью Nmap

Определение версий сервисов на машине с Metasploitable 2

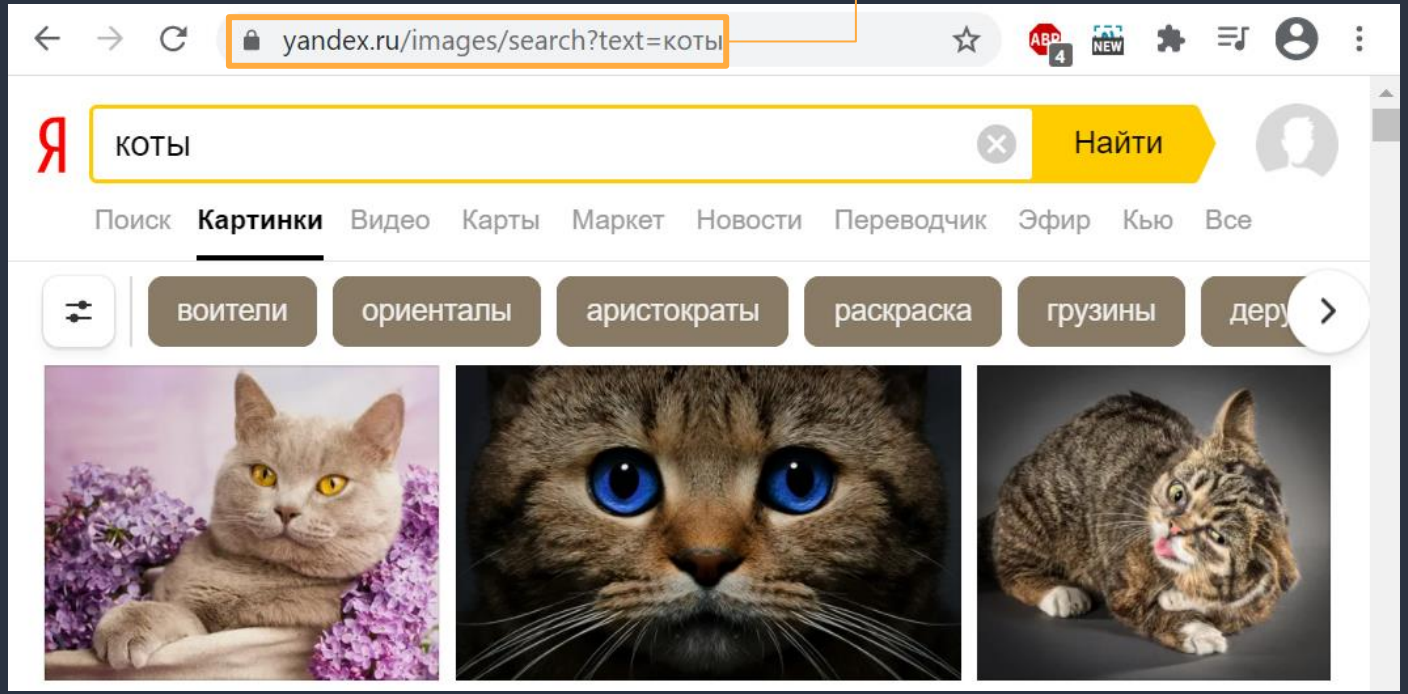
nmap -sV 192.168.1.45

```
Nmap scan report for 192.168.1.45
Host is up (0.000015s latency).
Not shown: 977 filtered ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploi
table.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Прикладные протоколы

- DNS (Domain Name System) - преобразование удобных для человека строк (доменных имён) в IP-адреса.
- HTTP - протокол лежащий в основе сети World Wide Web (WWW)
- HTTPS - протокол HTTP, вложенный в протокол TLS

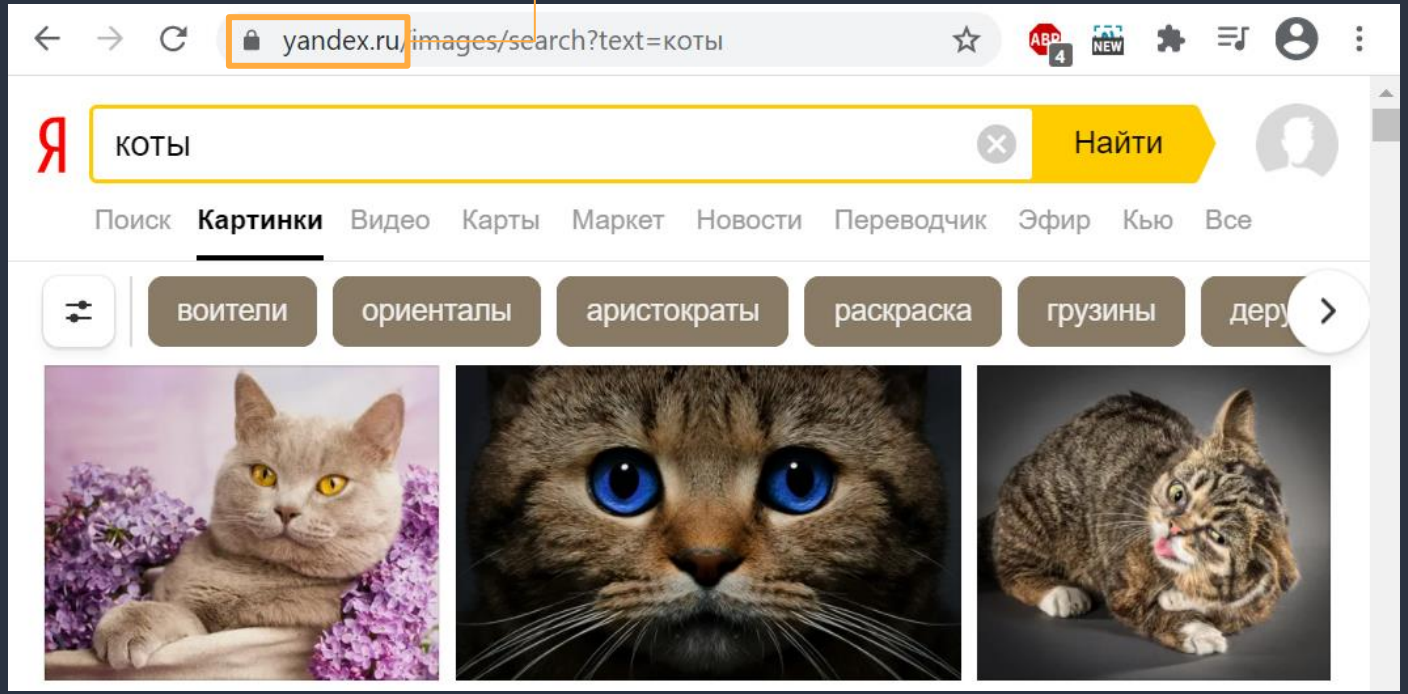
Что происходит при открытии ссылки в браузере? 1/5



Шаг 1. Браузер разбивает ссылку (URL) на части:

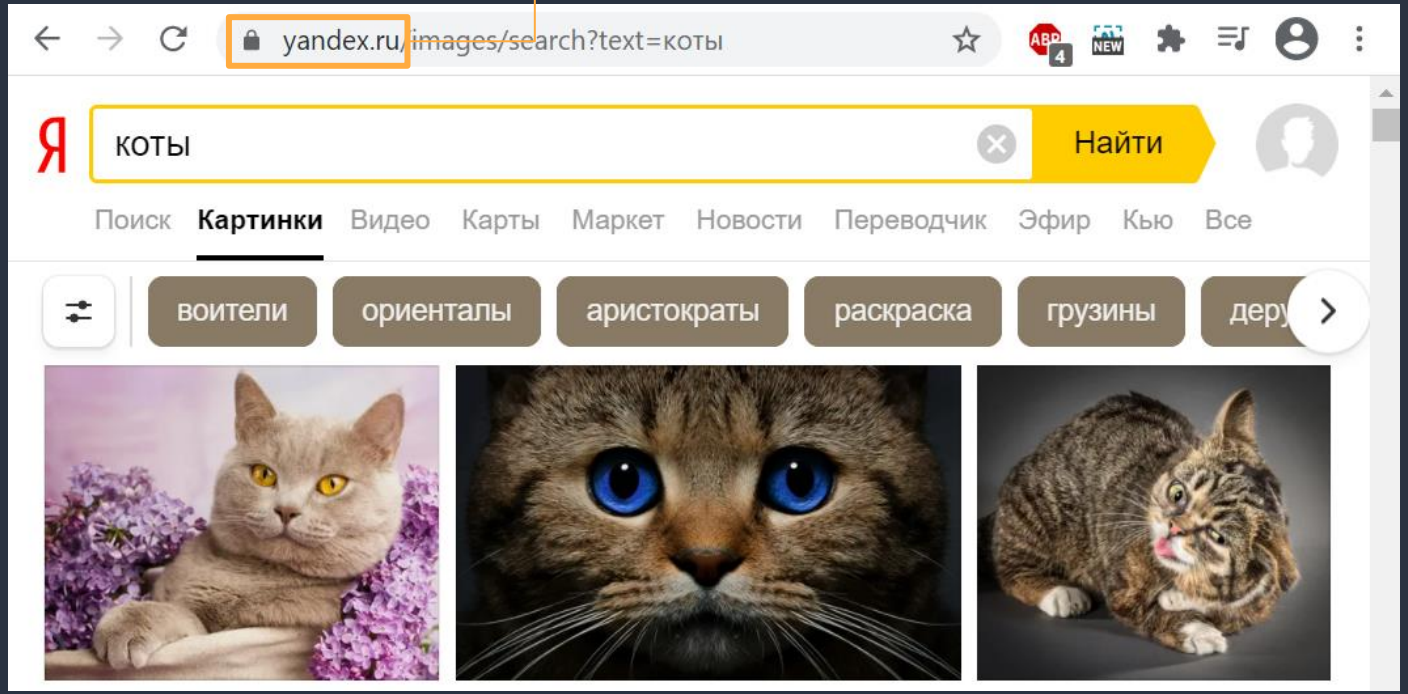
1) yandex.ru - имя хоста
2) /images/search?text=коты - путь и параметры запроса

Что происходит при открытии ссылки в браузере? 2/5



Шаг 2. Браузер преобразует yandex.ru в IP-адрес 77.88.55.50 с помощью DNS

Что происходит при открытии ссылки в браузере? 3/5



Шаг 3. Браузер подключается по протоколу TCP к IP-адресу 77.88.55.50 с портом 80 (HTTP) или 443 (HTTPS, в этом случае дополнительно используется TLS)

Что происходит при открытии ссылки в браузере? 4/5

Шаг 4. Браузер посылает строку (HTTP-запрос) вида:

```
GET /images/search?text=%D0%BA%D0%BE%D1%82%D1%8B HTTP/1.1
Host: yandex.ru
```

В ответ получает:

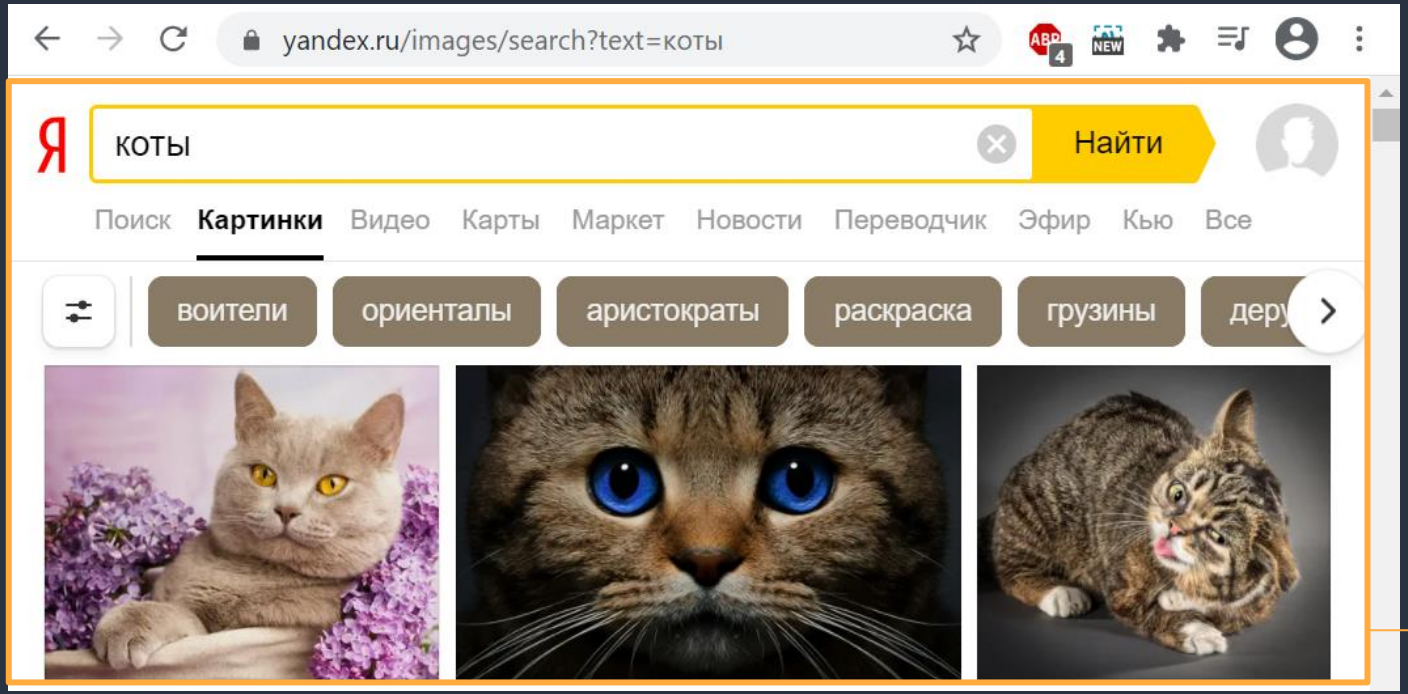
```
HTTP/1.1 200 OK
Cache-Control: private, max-age=3600
Content-Type: text/html; charset=utf-8
...
Date: Thu, 21 Jan 2021 15:35:47 GMT
```

HTTP-заголовки ответа

```
<!DOCTYPE html><html class="i-ua_js_no i-ua_css_standard" lang="ru">
<head><meta charset="utf-8"><meta http-equiv="X-UA-Compatible"
content="IE=edge"><title>Яндекс.Картинки</title>
...
```

html-код

Что происходит при открытии ссылки в браузере? 4/4



Шаг 5. Браузер разбирает и отрисовывает html-код, подгружая аналогичным образом картинки (GET-запросы HTTP) и другие ресурсы

Протокол HTTP

Основные HTTP-методы: GET/POST/HEAD

- GET - запрос данных
- HEAD - запрос только заголовков, без тела ответа
- POST - отправка данных на сервер (пример: формы, файлы)

Протокол HTTP не хранит состояние, т.е. сервер не хранит информацию о прошлых запросах.

Информацию нужно передавать в заголовках запроса (Cookie) и/или её запоминают в базе скрипты, вызываемые сервером (пример: PHP, Ruby, Python)

Протокол HTTP. Безопасность

- протокол не включает в себя шифрование
  - например, в публичной Wi-Fi сети все данные по HTTP можно перехватить
  - это один из каналов утечки паролей/логинов пользователей при заходе на сайт
- необходимо использовать HTTPS = HTTP + TLS
- для обработки запроса на сервере используются скрипты (PHP/Python/Ruby), куда передаются параметры запроса (пример, text=коты)
- ошибки в работе скриптов - основной источник уязвимостей на сайтах
- как правило, уязвимости находятся подстановкой нестандартных значений в параметры HTTP-запросов

Литература и ссылки

- Дуглас Э. Камер - Сети TCP IP. Принципы, протоколы и структура (2003)
- Metasploitable 2 и 3 - системы для тренировки
  - https://sourceforge.net/projects/metasploitable/
  - https://github.com/brimstone/metasploitable3/releases
- Gordon Lyon. Nmap Network Scanning. The Official Nmap Project Guide to Network Discovery and Security Scanning (2011) (http://nmap.org/book/)
- Список скриптов Nmap: https://nmap.org/nsedoc/