ИСП РАН

Основы сканирования в сети

Информационная безопасность и компьютерные сети
Практическое занятие №2

Сканирование удаленных хостов

- Проверка безопасности сети администратором
- «Разведка» при взломе сети

Активное сканирование

- Отправка на целевую машину специально сгенерированных пакетов, анализ полученных ответов
- Может обнаруживаться целевой машиной
- Обладает большей точностью
- Известный представитель ПО: Nmap

Пассивное сканирование

- Анализ пакетов, передаваемых по сети: дополнительные пакеты не генерируются
- Не может быть обнаружено
- Является менее точным
- Известный представитель ПО: p0f

Nmap

- https://nmap.org/

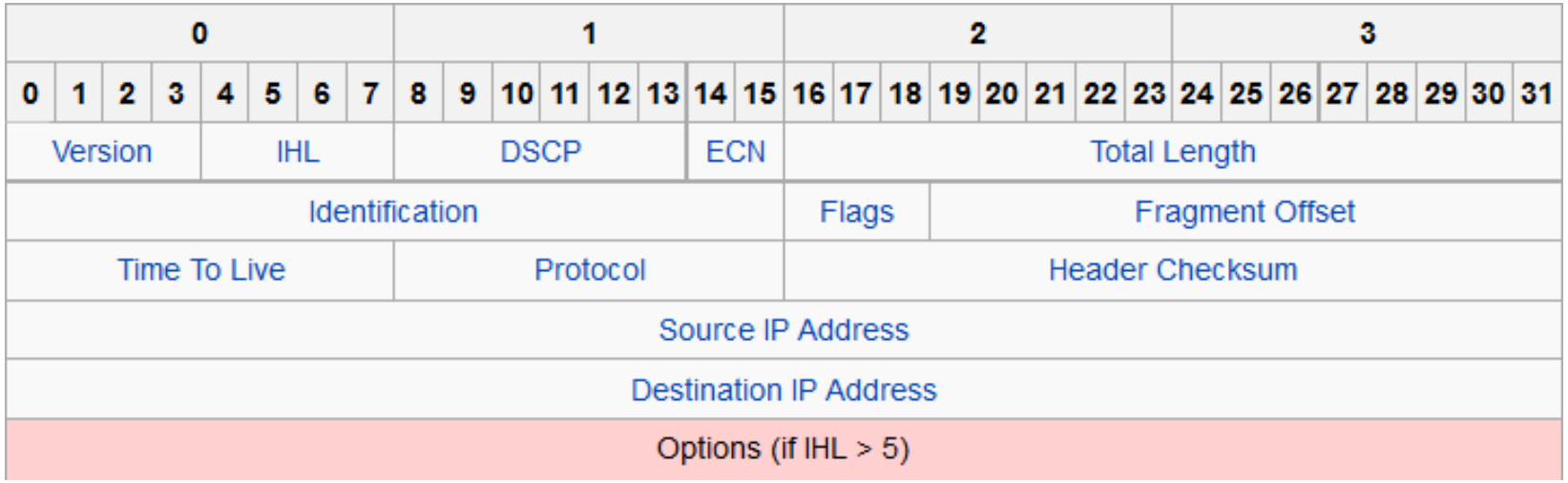
- Сканирование на предмет поиска открытых портов
  - SYN-сканирование:
    - SYN-ACK – порт открыт
    - RST – порт закрыт
  - UDP-сканирование:
    - ICMP «Destination port unreachable» – порт закрыт
  - FIN-сканирование:
    - RST – порт закрыт

```
john@john-VirtualBox: ~/downloads
john@john-VirtualBox:~/downloads$ sudo nmap scanme.nmap.org
[sudo] password for john:

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-03 18:47 MSK
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (1.7s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f0
3c:91ff:fe18:bb2f
Not shown: 994 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
139/tcp   filtered netbios-ssn
1720/tcp  open     h323q931
31337/tcp open     Elite
65000/tcp filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 170.29 seconds
john@john-VirtualBox:~/downloads$
```

- Детектирование ОС удаленного хоста

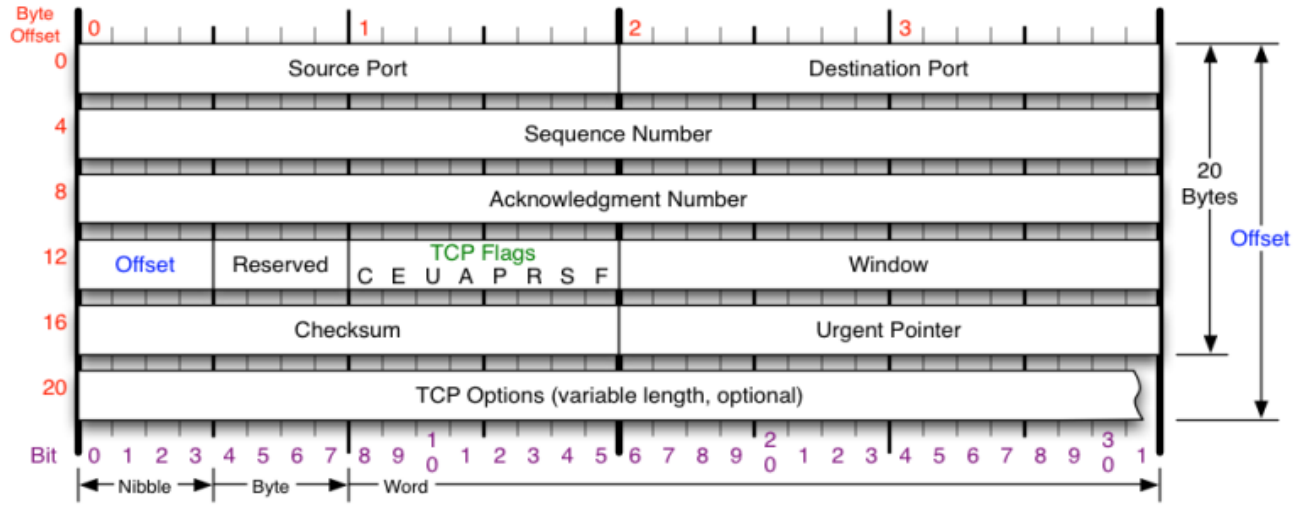
Особенности реализации IPv4 в различных ОС

- Фрагментация
  - Генерация значений поля «Identification»
- Time To Live (TTL)
  - Начальное значение
- Flags
  - Установка флага DF для пакетов, не требующих фрагментации
- Размер:
  - ICMP-ответ «Destination port unreachable» содержит фрагмент отправленного пакета, размер фрагмента не зафиксирован в RFC



Особенности реализации TCP в различных ОС

- Номер последовательности (sequence number)
  - Выбор начального значения
- Ответы на некорректные комбинации флагов/полей
- Размер окна
- Опции и порядок их передачи:
  - Максимальный размер сегмента
  - Масштабирование окна
  - Избирательное подтверждение
  - Отметка времени



TCP Flags

C E U A P R S F

Congestion Window
C 0x80 Reduced (CWR)
E 0x40 ECN Echo (ECE)
U 0x20 Urgent
A 0x10 Ack
P 0x08 Push
R 0x04 Reset
S 0x02 Syn
F 0x01 Fin

Congestion Notification

ECN (Explicit Congestion Notification). See RFC 3168 for full details, valid states below.

Packet State	DSB	ECN bits
Syn	0 0	1 1
Syn-Ack	0 0	0 1
Ack	0 1	0 0
No Congestion	0 1	0 0
No Congestion	1 0	0 0
Congestion	1 1	0 0
Receiver Response	1 1	0 1
Sender Response	1 1	1 1

TCP Options

0 End of Options List
1 No Operation (NOP, Pad)
2 Maximum segment size
3 Window Scale
4 Selective ACK ok
8 Timestamp

Checksum

Checksum of entire TCP segment and pseudo header (parts of IP header)

Offset

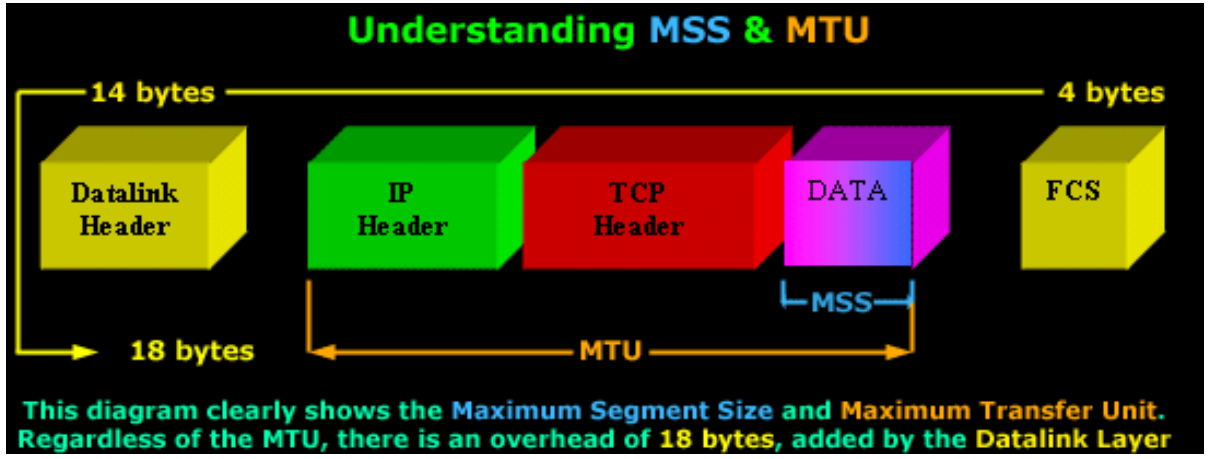
Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

RFC 793

Please refer to RFC 793 for the complete Transmission Control Protocol (TCP) Specification.

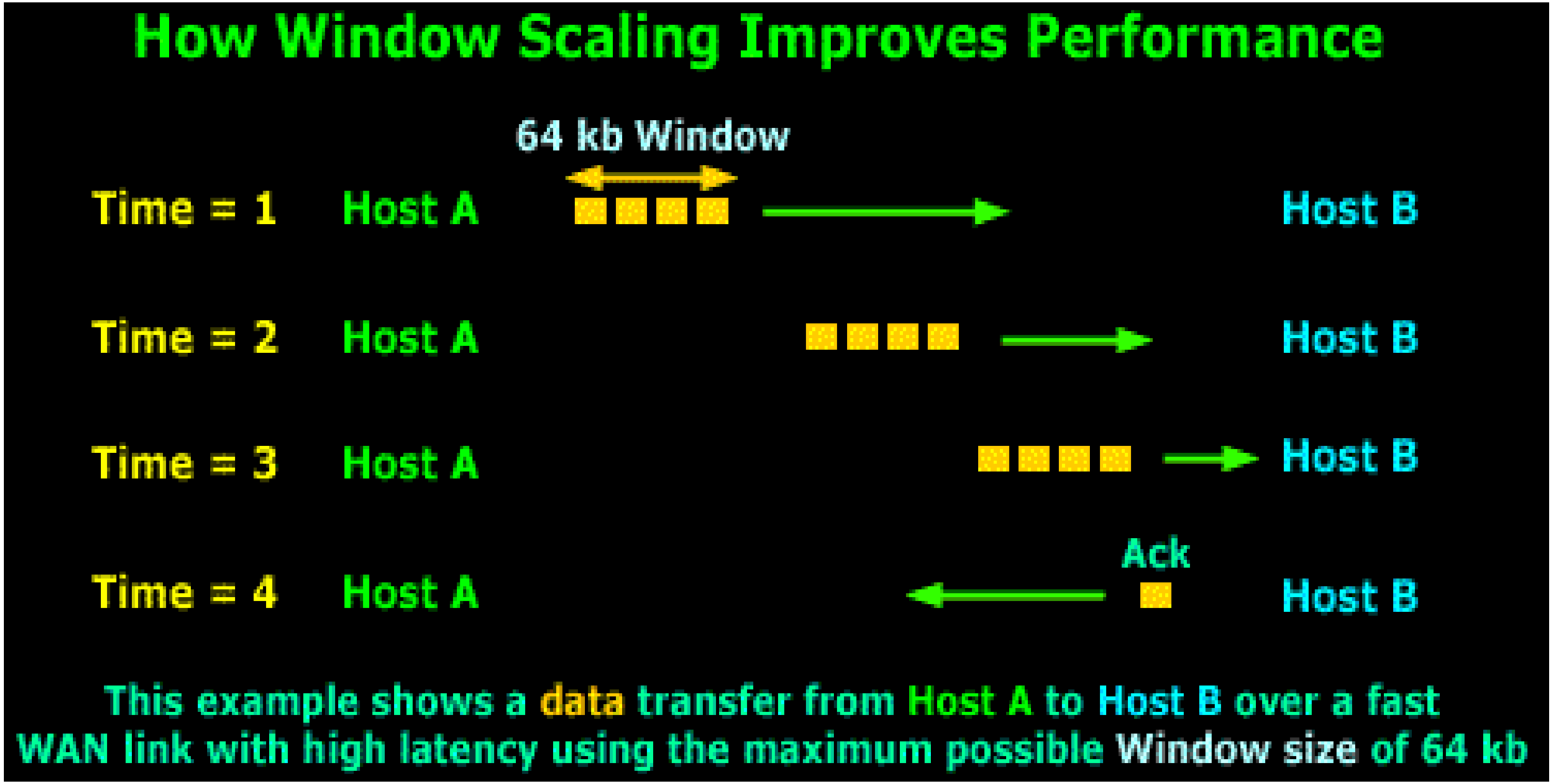
TCP-опции: максимальный размер сегмента

- Определяется при организации TCP-соединения
- По умолчанию используется значение 536 (RFC 1122)



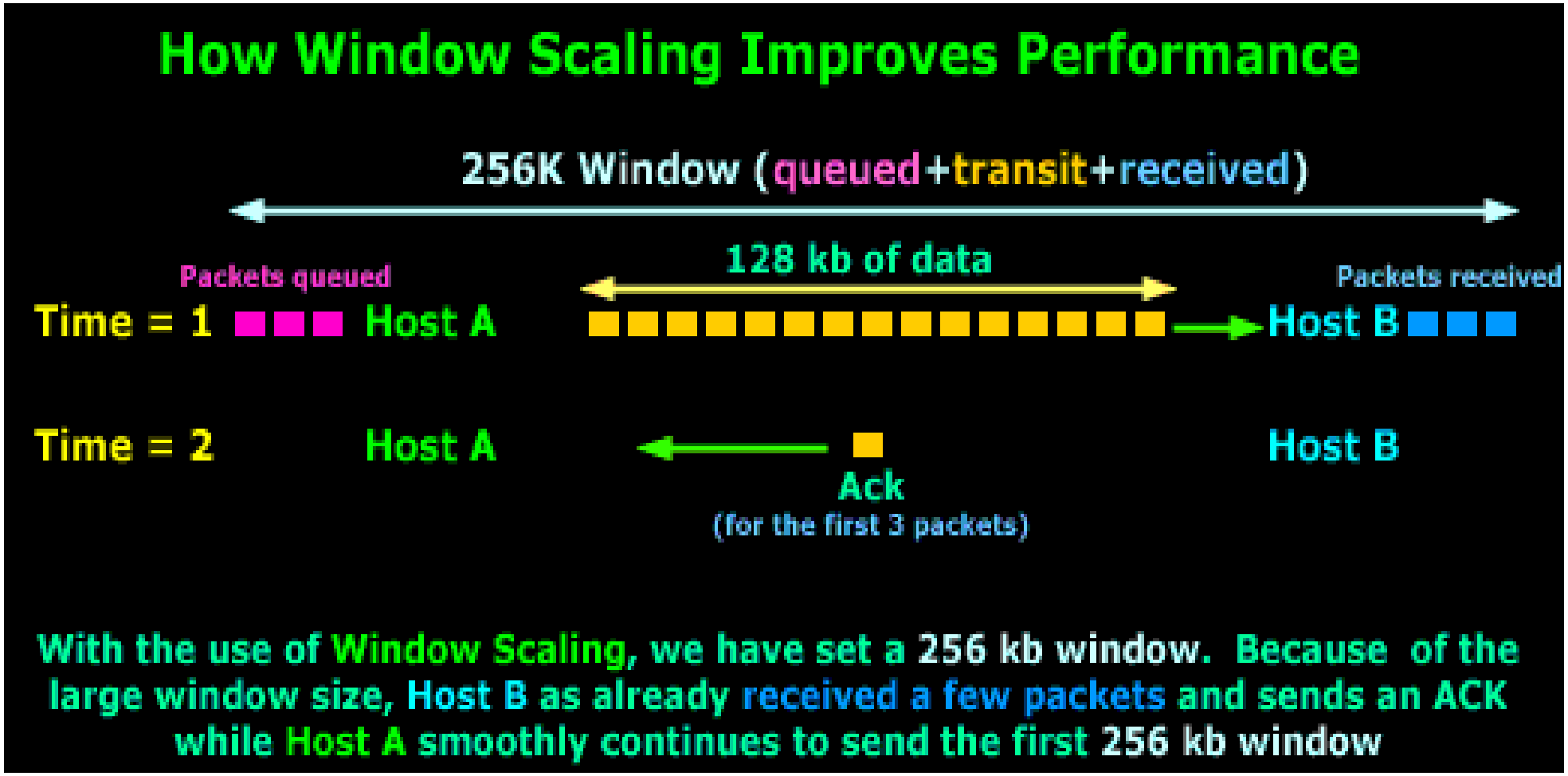

```
▷ Ethernet II, Src: AsustekC_b3:01:84 (00:1d:60:b3:01:84),
▷ Internet Protocol, Src: 192.168.1.16 (192.168.1.16), Dst
▽ Transmission Control Protocol, Src Port: 49214 (49214),
    Source port: 49214 (49214)
    Destination port: http (80)
    Sequence number: 0    (relative sequence number)
    Header length: 40 bytes
  ▷ Flags: 0x02 (SYN)
    Window size: 5840
  ▷ Checksum: 0xb1df [validation disabled]
  ▽ Options: (20 bytes)
      Maximum segment size: 1460 bytes
      SACK permitted
      Timestamps: TSval 5356733, TSecr 0
      NOP
      Window scale: 7 (multiply by 128)
```

TCP-опции: масштабирование окна



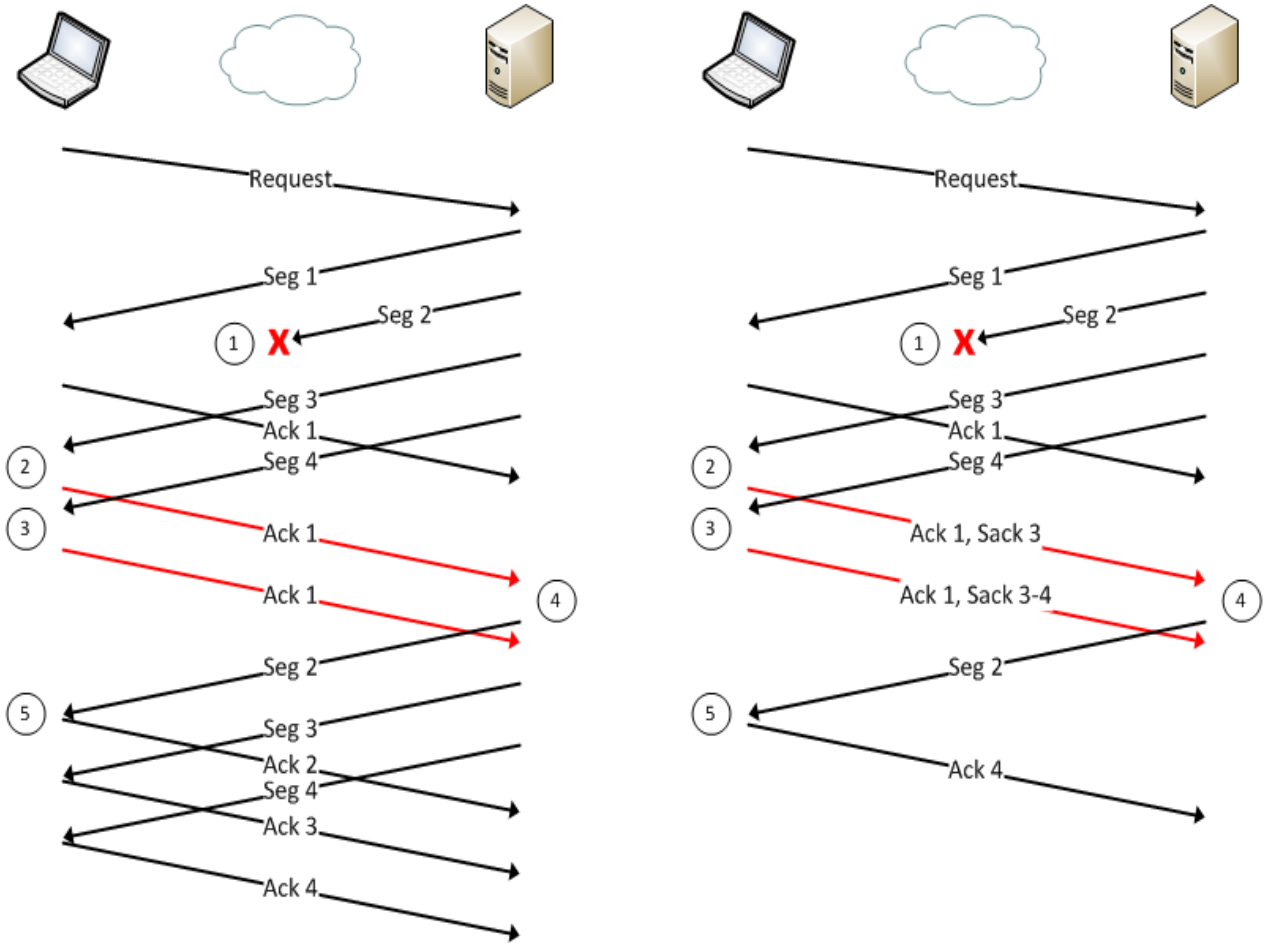
TCP-опции: масштабирование окна

- https://tools.ietf.org/html/rfc7323



TCP-опции: выборочное подтверждение

- https://tools.ietf.org/html/rfc2018

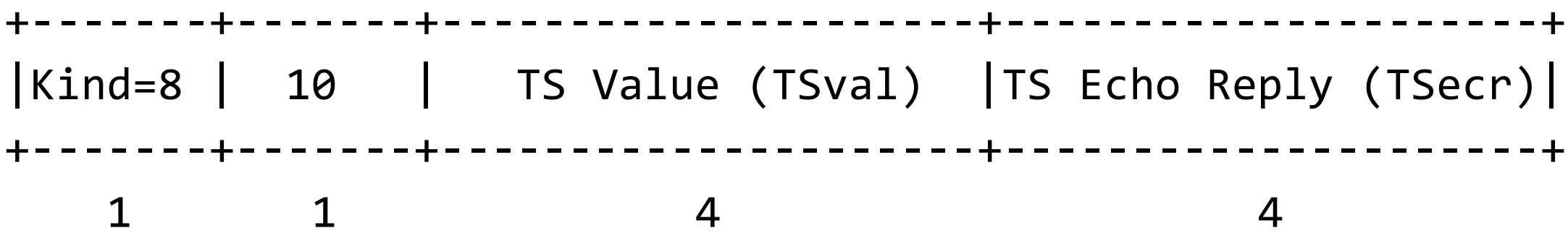



```
▷ Frame 31 (78 bytes on wire, 78 bytes captured)
▷ Ethernet II, Src: AsustekC_b3:01:84 (00:1d:60:b3:01:84), Dst: Action
▷ Internet Protocol, Src: 192.168.1.3 (192.168.1.3), Dst: 63.116.243.9
▽ Transmission Control Protocol, Src Port: 58816 (58816), Dst Port: ht
    Source port: 58816 (58816)
    Destination port: http (80)
    [Stream index: 0]
    Sequence number: 461    (relative sequence number)
    Acknowledgement number: 17377    (relative ack number)
    Header length: 44 bytes
  ▷ Flags: 0x10 (ACK)
    Window size: 40704 (scaled)
  ▷ Checksum: 0x34b6 [validation disabled]
  ▽ Options: (24 bytes)
      NOP
      NOP
      Timestamps: TSval 1545583, TSecr 2375917095
      NOP
      NOP
    ▽ SACK: 18825-20273
        left edge = 18825 (relative)
        right edge = 20273 (relative)
  ▷ [SEQ/ACK analysis]
```

```
0030  01 3e 34 b6 00 00 01 01  08 0a 00 17 95 6f 8d 9d   .>4..... .....
0040  9e 27 01 01 05 0a a3 c4  ca 28 a3 c4 cf d0         .'...... .(..
```

ИСП РАН

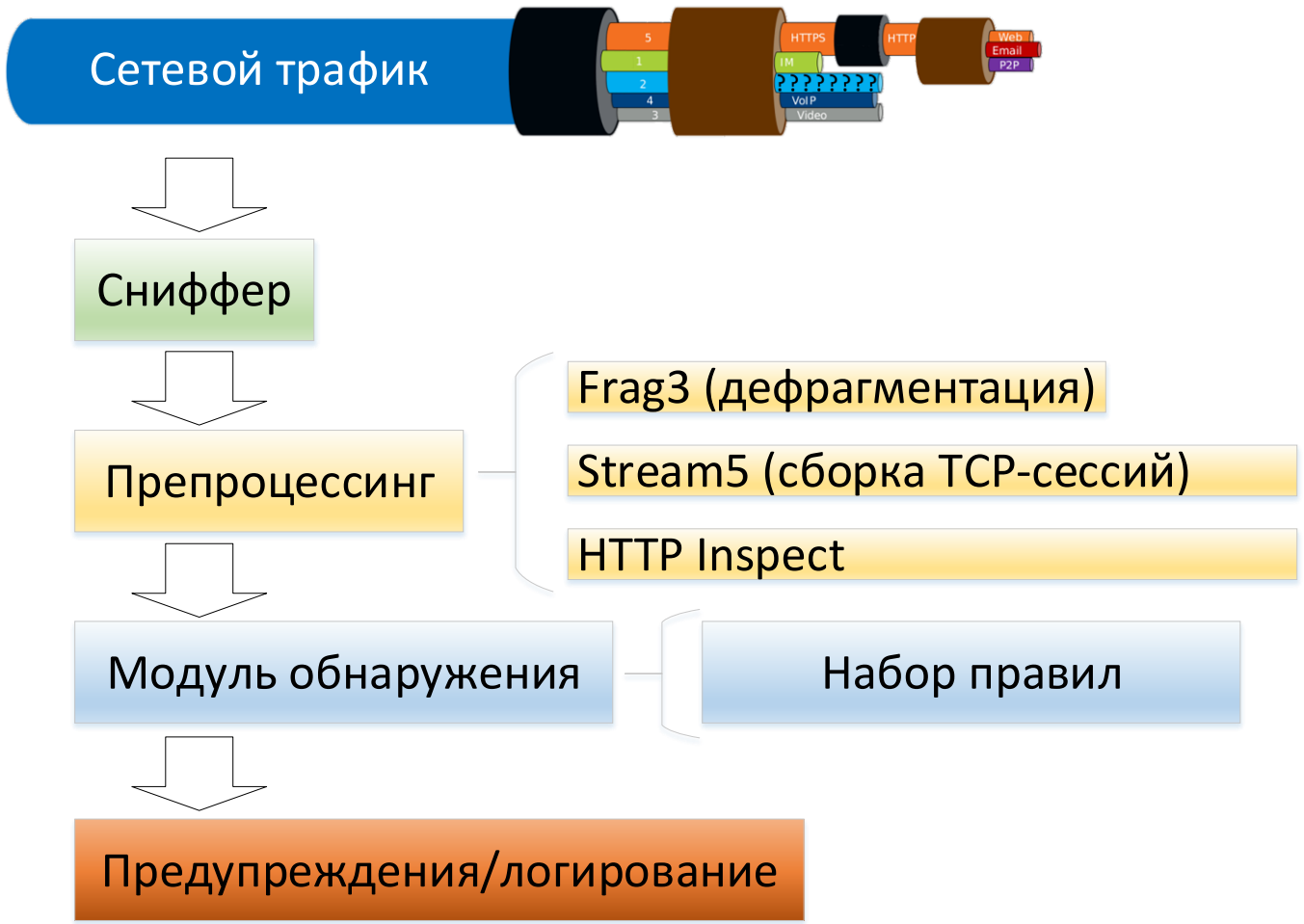
TCP-опции: отметка времени



- RTTM (Round-Trip Time Measurement)
  - измерение времени кругового обхода

- PAWS (Protect Against Wrapped Sequence numbers)
  - защита от перехода порядкового номера через верхнюю границу

Snort IDS/IPS: архитектура и конфигурирование



Конфигурационный файл *snort.conf*:

1. Переменные:
   - `ipvar HOME_NET any`
   - `ipvar EXTERNAL_NET !$HOME_NET`
   - `ipvar HTTP_SERVERS $HOME_NET`
2. Параметры препроцессоров:
   - `stream5_tcp, smtp, dns, ssh`
3. Подключаемые правила:
   - `include $RULE_PATH/rpc.rules`
   - `include $RULE_PATH/imap.rules`
   - `include $RULE_PATH/web-attacks.rules`

ИСП РАН

Snort IDS/IPS: формат правил

```
alert tcp any any -> 192.168.1.0/24 111 (
      content:"|00 01 86 a5|";msg:"mountd access";sid:1000001;)
```

Action	Protocol	IP	Port	Direction	IP	Port	Options
alert	tcp	any	any	->	192.168.1.0 /24	111	(content:"|00 01 86 a5|"; msg:"mountd access"; sid:1000001;)
alert log pass	tcp udp icmp ip	!10.10.14.11 $HOME_NET any [192.168.1.0 /24, 10.1.1.0/24]	1:1024 !1:100 :6000 500:	-> <>			general payload non-payload post-detection
drop reject sdrop							(key_1:value_1;...)

Snort IDS/IPS: rule options

1. general
   - `msg:"<text>"; sid:<rule id>;`
2. payload
   - `content:[!]"<content string>";`
   - `pcre:[!]"(/<regex>/|m<delim><regex><delim>)[ismxAEGRUBPHMCOIDKYS]";`
3. non-payload
   - `ttl:[<, >, =, <=, >=]<number>;`
   - `flags:[!|*|+]<FSRPAUCE0>[,<FSRPAUCE>];`
   - `flow:[(established|not_established|stateless)]`
     `[,(to_client|to_server|from_client|from_server)]`
     `[,(no_stream|only_stream)][,(no_frag|only_frag)];`
4. post-detection
   - `session:[printable|binary|all];`

ИСП РАН

Домашнее задание

- Написать snort-правила для обнаружения пакетов, отправляемых nmap-ом при детектировании ОС
- Прислать файл с правилами на insecon@ispras.ru, установить тему письма «2022_snort_vs_nmap»
  - до 14.11.2022 23:59
  - не более одного письма в день
- Пакеты для детектирования ОС с помощью Nmap (IPv4):
  - https://nmap.org/book/osdetect-methods.html
  - рекомендуем записать сетевую трассу с помощью Wireshark
- Как писать SNORT-правила:
  - http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node27.html

ИСП РАН

Домашнее задание: пояснения [1]

- Запуск SNORT на сетевом интерфейсе **lo** с файлом конфигурации «/etc/snort/snort.conf»:

```
$ sudo snort -i lo -A console -c /etc/snort/snort.conf
```

- Запуск Nmap в режиме детектирования ОС локально:

```
$ sudo nmap -O localhost
```

Группа пакетов	Количество пакетов	Значение поля “msg”	Значение поля “sid”
Sequence generation (SG)	6	“SG-1”, “SG-2”, …, “SG-6”	1000001 – 1000006
ICMP echo (IE)	2	“IE-1”, “IE-2”	1000007, 1000008
TCP explicit congestion notification (ECN)	1	“ECN-1”	1000009
TCP (T2–T7)	6	“T-2”, “T-3”, …, “T-7”	1000010 – 1000015
UDP (U1)	1	“U-1”	1000016

ИСП РАН

Домашнее задание: пояснения [2]

- 16 правил: 1 правило ~ 1 пакет
  - Требуется **максимально точное описание пакетов** – пакеты, обладающие частичным набором свойств, не должны детектироваться (покрыто и проверяется тестами)
- Имя файла с правилами: «фамилияио-группа-вуз-local.rules»
  - например, «ivanovii-123-mipt-local.rules»
- Первая строка файла с правилами – ФИО, номер группы (латиницей)
  - разумеется, в виде комментария
- Для каждого правила:
  - Использовать действие «alert»
  - Использовать IP-адреса и номера портов «any»