



Administrator Linux.Basic

Сети. tcpdump



Проверить, идет ли запись

Меня хорошо видно && слышно?



Преподаватель



Лавлинский Николай

Технический директор «Метод Лаб»

Более 15 лет в веб-разработке

Преподавал в ВУЗе более 10 лет

Более 4 лет в онлайн-образовании

Специализация: оптимизация производительности, ускорение сайтов и веб-приложений

https://t.me/methodlab_tg

<https://www.methodlab.ru/>

<https://www.youtube.com/c/NickLavlinsky>

https://www.youtube.com/@site_support

<https://vk.com/nick.lavlinsky>

Правила вебинара



Активно
участвуем



Off-topic обсуждаем
в Телеграм-чате



Задаем вопрос
в чат или голосом



Вопросы вижу в чате,
могу ответить не сразу

Условные обозначения



Индивидуально



Время, необходимое
на активность



Пишем в чат



Говорим голосом

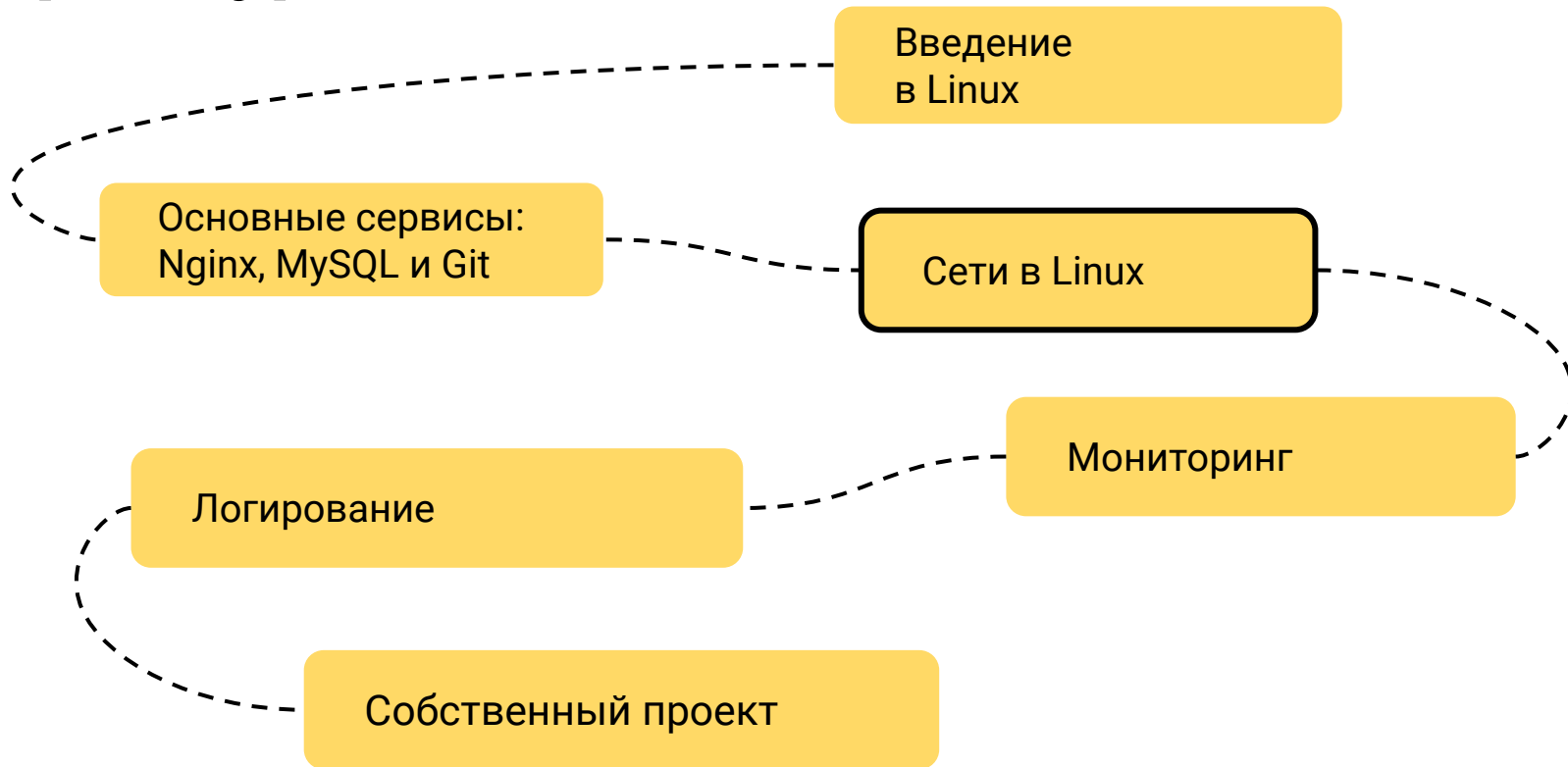


Документ

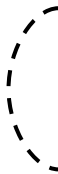


Ответьте себе или
задайте вопрос

Карта курса



Маршрут вебинара



Анализ трафика с tcpdump

Использование Wireshark

Цели вебинара

После занятия вы сможете

1. Захватывать нужные пакеты для анализа
2. Проводить анализ в Wireshark

Смысл

Зачем вам это уметь

1. Диагностировать работу сетевых приложений
2. Анализировать трафик

Утилита tcpdump



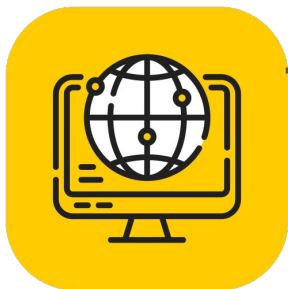
Что такое, зачем?



Источник и назначение

Клиент IP 4.2.3.4
Порт: random

```
src ip 4.2.3.4 src port random  
dst ip 1.2.3.4 dst port 80
```



Веб-сервер IP 1.2.3.4
Порт: 80

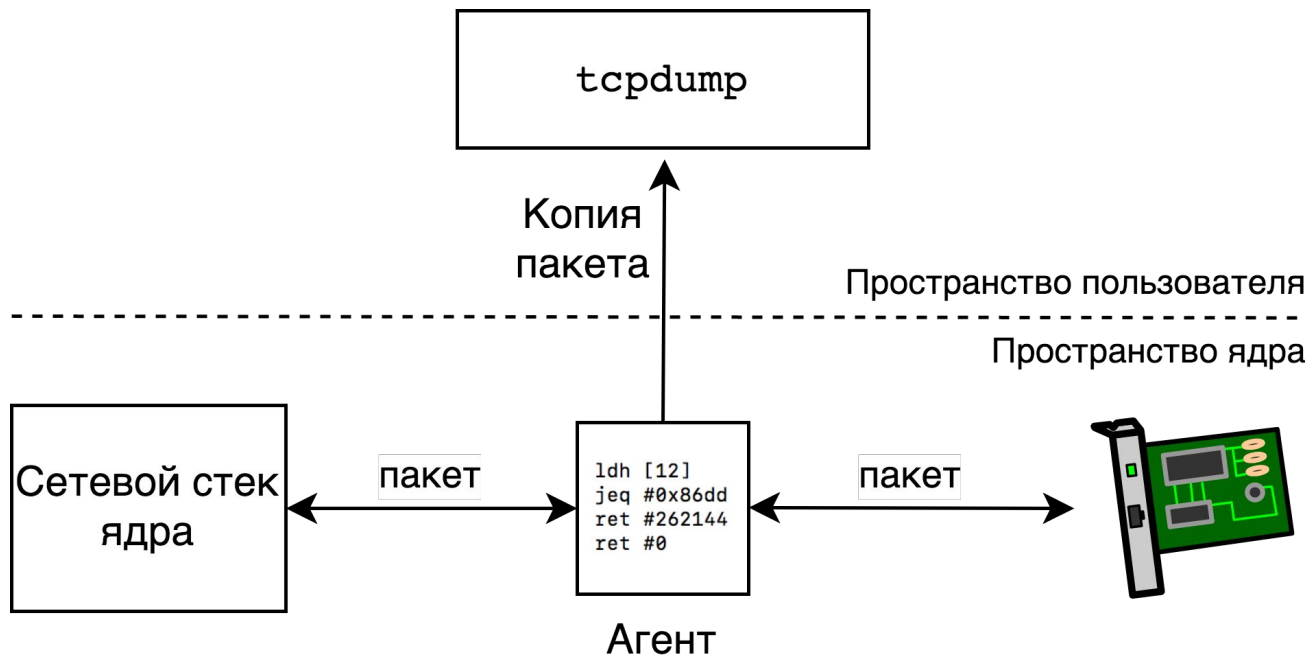
```
src ip 1.2.3.4 src port 80  
dst ip 4.2.3.4 dst port random
```



Утилита tcpdump

- Получает копию пакета до фильтрации через netfilter
- Перехват трафика с фильтрацией по условиям
- Запись пакетов в файл
- Установка: `# apt install tcpdump -y`

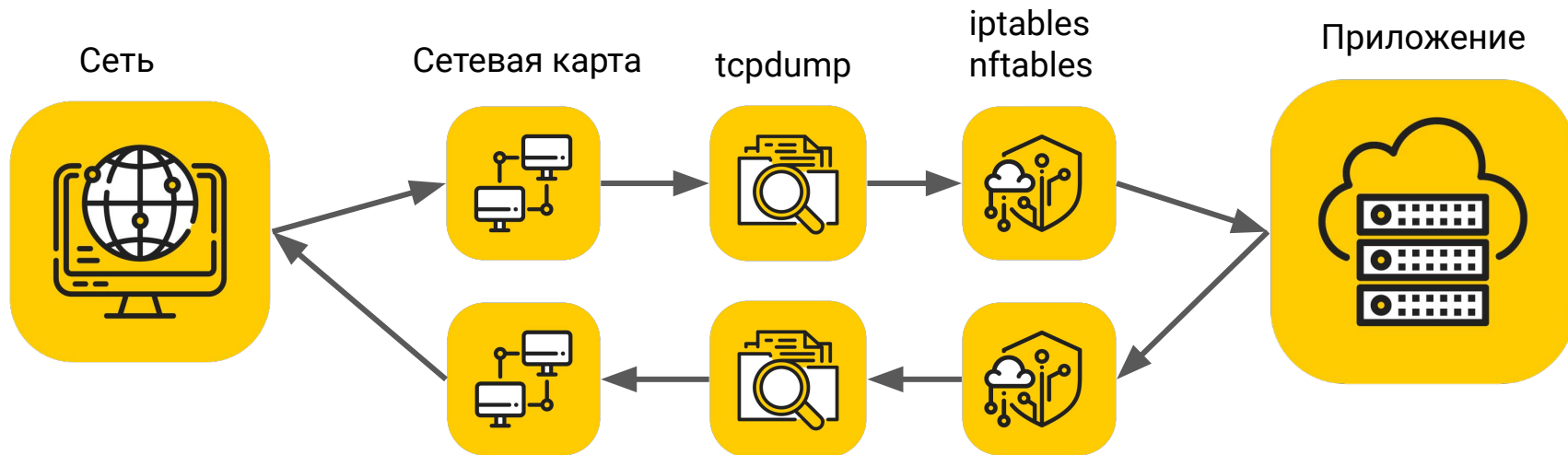
Принцип работы и VPF



<https://habr.com/ru/post/493880/>

Входящие и исходящие пакеты

Входящий трафик



Исходящий трафик

Использование tcpdump

- Установка: `apt install tcpdump`
- Список интерфейсов: `tcpdump -D`
- Захват всего трафика интерфейса: `tcpdump -i enp0s3`
- Запись пакетов в файл: `tcpdump -i enp0s3 -w dump.pcap`
- Вывод данных в цифровой форме: `tcpdump -nni enp0s3`
- Повышенная детализация: `tcpdump -nnvAi enp0s3`
- Только 80 порт: `tcpdump 'tcp port 80' -nnvAi enp0s3`

<https://www.howtouselinux.com/post/tcpdump-cheat-sheet>

Примеры фильтров tcpdump

- `tcpdump 'tcp src port 80' -nnvi enp0s3`
- `tcpdump 'tcp dst port 80' -nnvi enp0s3`
- `tcpdump 'tcp port 80' -c 3 -i enp0s3`
- `tcpdump net 192.168.0.0/24`
- `tcpdump 'tcp port 80 and host 192.168.0.88' -i enp0s3`

<https://www.howtouselinux.com/post/tcpdump-cheat-sheet>

Захват пакетов LIVE

Wireshark

Wireshark – анализ дампа пакетов

The image shows the Wireshark network protocol analyzer interface. The main window displays a list of captured packets in the 'Packet List' pane. The selected packet is the first one, a DNS Standard query from 192.168.0.101 to 192.168.0.254. The 'Packet Details' pane on the right shows the hierarchical structure of the selected packet: Ethernet II, Internet Protocol Version 4, and UDP. The 'Packet Bytes' pane at the bottom shows the raw data in hexadecimal and ASCII. The status bar at the bottom indicates that 999 packets are displayed (100.0%) and the profile is Default.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.101	192.168.0.254	DNS	87	Standard query 0x84f7 A www.methodlab.ru
2	0.000902	192.168.0.254	192.168.0.101	DNS	129	Standard query response 0x84f7 A www.met
3	0.153123	192.168.0.101	95.213.164.227	TCP	74	57134 → 443 [SYN] Seq=0 Win=64240 Len=0 M
4	0.156277	192.168.0.101	95.213.164.227	TCP	74	57136 → 443 [SYN] Seq=0 Win=64240 Len=0 M
5	0.156327	95.213.164.227	192.168.0.101	TCP	74	443 → 57134 [SYN, ACK] Seq=0 Ack=1 Win=65
6	0.159378	95.213.164.227	192.168.0.101	TCP	74	443 → 57136 [SYN, ACK] Seq=0 Ack=1 Win=65
7	0.249998	192.168.0.101	95.213.164.227	TCP	74	57138 → 443 [SYN] Seq=0 Win=64240 Len=0 M
8	0.253100	95.213.164.227	192.168.0.101	TCP	74	443 → 57138 [SYN, ACK] Seq=0 Ack=1 Win=65

Frame 1: 87 bytes on wire (696 bits), 87 bytes captured (696 bits)
Ethernet II, Src: PcsCompu_7c:30:56 (08:00:27:7c:30:56), Dst: Tp-LinkT_a3:1d:b2 (64:70:02:a3:1d:b2)
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.254
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 73
Identification: 0x6a59 (27225)
Flags: 0x4000, Don't fragment
Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0x4d97 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.0.101
Destination: 192.168.0.254

0000 64 70 02 a3 1d b2 08 00 27 7c 30 56 08 00 45 00 dp |0V..E..
0010 00 49 6a 59 40 00 40 11 4d 97 c0 a8 00 65 c0 a8 .IjY@.M...e..
0020 00 fe 97 08 00 35 00 35 82 fa 84 f7 01 00 00 015.5.....
0030 00 00 00 00 00 01 03 77 77 77 09 6d 65 74 68 6fw ww.metho
0040 64 6c 61 62 02 72 75 00 00 01 00 01 00 00 29 02 dlab.ru.....
0050 00 00 00 00 00 00 00 00

Internet Protocol Version 4 (ip), 20 bytes

Packets: 999 - Displayed: 999 (100.0%) Profile: Default

<https://www.youtube.com/c/ChrisGreer>

Wireshark – фильтры пакетов

Параметр	Пример	Описание
ip.addr	ip.addr==1.1.1.1	IP-адрес
protocol	dns	Протокол
tcp.port	tcp.port==443	Порт TCP
in	tcp.port in {80,443}	Список портов TCP
udp.port	udp.port==53	Порт UDP
tcp.analysis.flags	tcp.analysis.flags	Флаги TCP
!()	!(arp or dns or icmp)	Отрицание условия
http.request http.response	http.response.code == 200	HTTP-запросы и ответы
tcp.flags.syn==1	tcp.flags.reset	Наличие флага TCP
	tcp.port == 80 udp.port == 80	Объединение нескольких условий
&&	tcp.dstport == 443 && tcp.srcport == 57134	Пересечение нескольких условий

<https://www.youtube.com/c/ChrisGreer>



Анализ пакетов в Wireshark LIVE

Практика



Домашнее задание

1. Снять дамп обращения к веб-серверу, проанализировать пакеты (начиная с первого).
2. Описать на примере снятого дампа, как устанавливается сессия TCP.



Сроки выполнения: указаны в личном кабинете



Что мы изучили?

Подведем итоги

1. Возможности захвата и анализа пакетов в Linux
 2. Использование WireShark
-

Список материалов для изучения

1. <https://habr.com/ru/post/493880/>
2. <https://habr.com/ru/companies/alexhost/articles/531170/>
3. <https://www.howtouselinux.com/post/tcpdump-cheat-sheet>
4. <https://www.youtube.com/c/ChrisGreer>
5. <https://www.wireshark.org/>



Вопросы?



Ставим "+",
если вопросы есть



Ставим "-",
если вопросов нет

Рефлексия

Рефлексия



Что было самым полезным на занятии?



Как будете применять на практике то, что узнали на вебинаре?



Следующий вебинар



Мониторинг



Ссылка на вебинар
будет в ЛК за 15 минут



Материалы
к занятию в ЛК —
можно изучать



Обязательный материал
обозначен красной
лентой

**Заполните, пожалуйста,
опрос о занятии
по ссылке в чате**

Спасибо за внимание!

Приходите на следующие вебинары



Лавлинский Николай

Технический директор “Метод Лаб”

https://t.me/methodlab_tg

<https://www.methodlab.ru/>

<https://www.youtube.com/c/NickLavlinsky>

https://www.youtube.com/@site_support

<https://vk.com/nick.lavlinsky>

