

Основы построения защищенных компьютерных сетей

Лекция 4 Анализ сетевого трафика

Семён Новосёлов

2021





Wireshark

Самый популярный инструмент для анализа сетевого трафика.

- Поддерживает сотни протоколов
- Есть поддержка расшифровки IPsec, SSL/TLS, WEP, WPA/WPA2
- <https://www.wireshark.org/>
- Консольная версия: **tshark**

Сбор трафика для анализа

На удалённом сервере без графического интерфейса (при работе по **ssh**):

1. **Сбор:**

```
[sudo] tcpdump -w имя_файла
```

2. **Загрузка:**

```
scp пользователь@адрес_сервера:путь_к_файлу/имя_файла  
имя_файла_для_сохранения
```

3. **Анализ:** открыть в Wireshark

Пример. VDS (virtual dedicated server)

- Виртуальный выделенный сервер, арендуется у провайдера (например, firstvds).
- Сразу после запуска на сервере начинается:
 - сканирование различными ботами и компаниями из ИБ
 - перебор паролей для SSH
 - попытки применения эксплойтов к запущенным сервисам

В дальнейших примерах используются дампы трафика на VDS с адресом novsem1.fvds.ru

Сбор трафика для анализа II

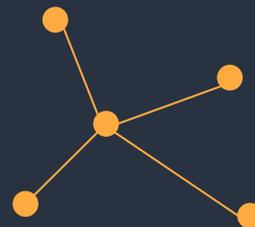
Трафик Wi-Fi:

1. перевести карту в неразборчивый режим (через `aircrack-ng`)
 2. запустить `wireshark/tcpdump`
- Трафик **не шифруется** для подключенных к сети устройств
 - известен пароль сети \Rightarrow можно сделать дамп зашифрованного трафика сети и расшифровать потом в `wireshark` без подключения к сети

Сбор трафика для анализа III

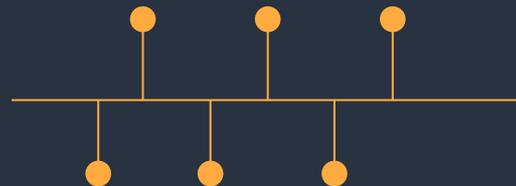
Сеть Ethernet:

- Многие роутеры поддерживают сбор трафика в сети
- В топологии “звезда” сбор трафика возможен через атаки типа MiTM:
ARP-poisoning



Топология “звезда”

- от других хостов видны только широковещательные запросы



Топология “шина”

- видны все пакеты всем хостам



Wireshark. Интерфейс

Список пакетов

No.	Time	Source	Destination	Protocol	Length	Info
2185	22.426688	10.252.38.183	224.0.0.251	MDNS	278	Stand...
2186	22.529595	10.252.42.166	224.0.0.251	MDNS	270	Stand...

Разбор пакета

```
> Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \D...
> Ethernet II, Src: IntelCor_1d:6f:e6 (64:5d:86:1d:6f:e6), Dst: IPv4mcast_fb (01:00:
> Internet Protocol Version 4, Src: 10.252.44.236, Dst: 224.0.0.251
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353
```

Сырые данные пакета

```
0000  01 00 5e 00 00 fb 64 5d 86 1d 6f e6 08 00 45 00  ..^...d] ..o...E.
0010  00 44 2c 91 00 00 01 11 74 35 0a fc 2c ec e0 00  .D,.... t5...,.
0020  00 fb 14 e9 14 e9 00 30 72 c0 00 00 00 00 00 01  .....0 r.....
0030  00 00 00 00 00 00 0b 5f 67 6f 6f 67 6c 65 63 61  ....._ googleca
0040  73 74 04 5f 74 63 70 05 6c 6f 63 61 6c 00 00 0c  st_tcp local..
0050  00 01
```

Байты 54-77: Name (dns qry.name)

Пакеты: 2186 · Показаны: 2186 (100.0%)

Профиль: Default



Wireshark. Фильтры

- интересные пакеты находятся среди кучи других пакетов
- необходимо отфильтровать лишние

строка для ввода фильтров

Захват из Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония

Применить дисплейный фильтр ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
2185	22.426688	10.252.38.183	224.0.0.251	MDNS	278	Stand...
2186	22.529595	10.252.42.166	224.0.0.251	MDNS	270	Stand...

> Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \E
> Ethernet II, Src: IntelCor_1d:6f:e6 (64:5d:86:1d:6f:e6), Dst: IPv4mcast_fb (01:00:
> Internet Protocol Version 4, Src: 10.252.44.236, Dst: 224.0.0.251
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353

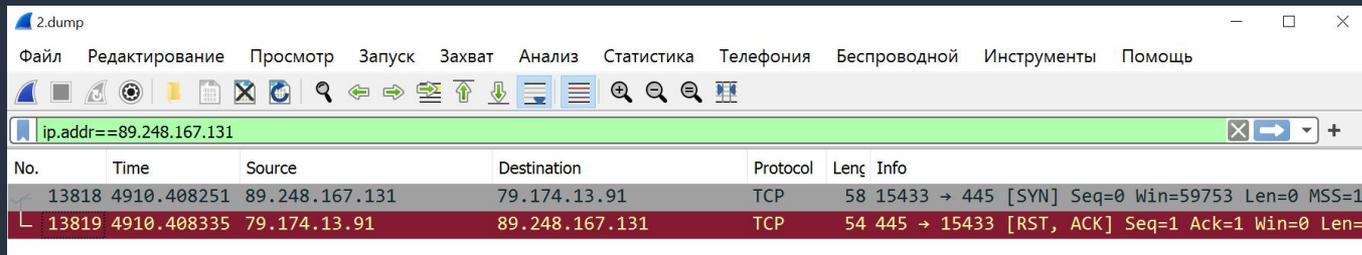
```
0000 01 00 5e 00 00 fb 64 5d 86 1d 6f e6 08 00 45 00  ..^...d] ..o...E.  
0010 00 44 2c 91 00 00 01 11 74 35 0a fc 2c ec e0 00  .D,..... t5...,...  
0020 00 fb 14 e9 14 e9 00 30 72 c0 00 00 00 00 00 01  .....0 r.....  
0030 00 00 00 00 00 00 0b 5f 67 6f 6f 67 6c 65 63 61  ....._googleca  
0040 73 74 04 5f 74 63 70 05 6c 6f 63 61 6c 00 00 0c  st_tcp.local..  
0050 00 01
```

Байты 54-77: Name (dns.qry.name) | Пакеты: 2186 · Показаны: 2186 (100.0%) | Профиль: Default

Основные фильтры

- Показ трафика (исходящего/входящего) определенного хоста:
`ip.addr == 192.168.0.1`
- Фильтрация по протоколу:
`http`
`tcp`
`smb`
- Логические операторы (И, ИЛИ, НЕ):
`ip.src==192.168.0.0/16 and ip.dst==192.168.0.0/16`
- Поиск по содержимому пакетов:
`data contains "string"`
`http contains "string"`

Отображение доменных имён хостов



2.dump

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

ip.addr==89.248.167.131

No.	Time	Source	Destination	Protocol	Length	Info
13818	4910.408251	89.248.167.131	79.174.13.91	TCP	58	15433 → 445 [SYN] Seq=0 Win=59753 Len=0 MSS=1460
13819	4910.408335	79.174.13.91	89.248.167.131	TCP	54	445 → 15433 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0



По-умолчанию
отключено.

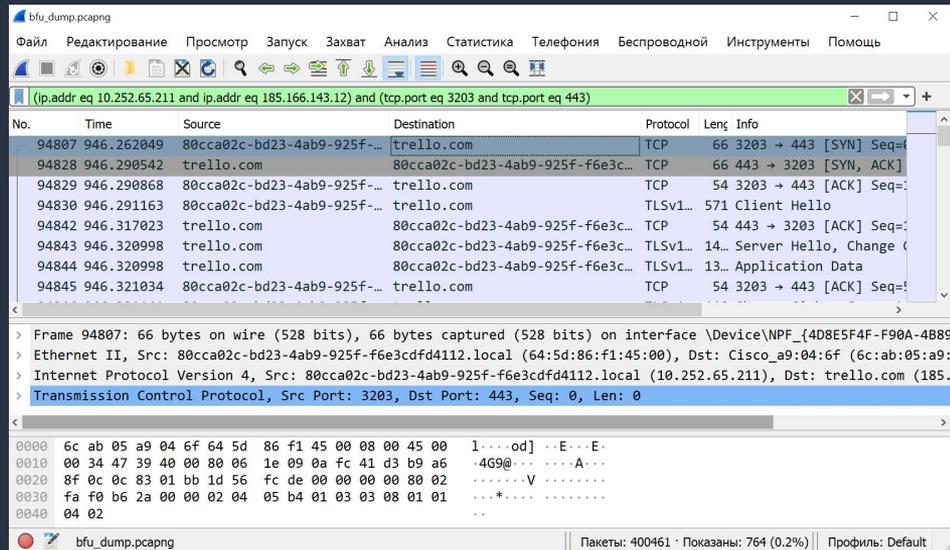
Включение:

Edit ⇒ Preferences ⇒ Name Resolution ⇒ Resolve Network (IP) addresses

Выделение соединений

Wireshark поддерживает выборку пакетов соединений (поточков)

- Выделить Пакет ⇒ Follow ⇒ TCP Stream
- Выделить Пакет ⇒ Conversation Filter ⇒ TCP



Пример. Подключение к trello.com по TLS

База GeoIP

Для отображения информации о местоположениях IP-адресов:

1. Скачать базы MaxMind (достаточно **GeoLite2 Free**)
2. Указать их в Edit ⇒ Preferences ⇒ Name Resolution ⇒ MaxMind Database Directory
3. Информация о локациях доступна через: Statistics ⇒ Endpoints



Wireshark · Endpoints · vds.dump

Ethernet · 7 IPv4 · 455 IPv6 · 2 TCP · 2102 UDP · 83

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	A
79.174.186.103	16	864	8	432	8	432	Russia	St Petersburg	62205	U
80.82.65.247	6	324	3	162	3	162	Netherlands	Amsterdam	202425	IF
group-ib.ru	2	108	1	54	1	54	Seychelles	Anse aux Pins	202425	IF
dojo.census.shodan.io	2	112	1	58	1	54	Netherlands	Amsterdam	202425	IF
80.82.77.240	2	108	1	54	1	54	Netherlands	Amsterdam	202425	IF
relay.alarm-motors.ru	4	240	2	132	2	108	Russia	—	20632	P
82.156.44.208	2	128	1	74	1	54	China	—	45090	S
static.158.189.99.88.clients.your-server.de	4	224	2	116	2	108	Germany	—	24940	H
hostby.fcloud.biz	3	162	2	108	1	54	Germany	—	209132	A
rs-zap808770-1.zap-srv.com	2	922	1	447	1	475	Germany	—	30823	ci
metro.denizli.bel.tr	4	240	2	132	2	108	Turkey	Pamukkale	9121	T
recyber.net	634	34k	317	17k	317	17k	United Kingdom	—	202425	IF

Name resolution Limit to display filter

Endpoint Types ▾

Copy ▾ Map ▾ Close Help

Пример: Анализ дампа трафика с VDS, видно адреса компаний из ИБ, сканирующих сеть.

Генерация правил для файервола

Wireshark поддерживает автоматическую генерацию правил доступа для различных файерволов.

- Tools ⇒ Firewall ACL Rules

The image shows a Wireshark network traffic capture window. The main window displays a list of packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. Two packets are visible:

No.	Time	Source	Destination	Protocol	Length	Info
25915	9198.327410	group-ib.ru	novsem1.fvds.ru	TCP	54	60000 → 1177 [SYN] Seq=0 Win=1024 Len=0
25916	9198.327498	novsem1.fvds.ru	group-ib.ru	TCP	54	1177 → 60000 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

A dialog box titled "Wireshark - Firewall ACL Rules - vds.dump" is open, showing the configuration of Netfilter (iptables) rules for the selected packet (No. 25916). The rules are:

```
# Netfilter (iptables) rules for vds.dump, packet 25916. Change eth0 to a valid interface if needed.

# IPv4 source address.
iptables --append INPUT --in-interface eth0 --source 79.174.13.91/32 --jump DROP

# IPv4 destination address.
iptables --append INPUT --in-interface eth0 --source 80.82.70.228/32 --jump DROP

# Source port.
iptables --append INPUT --in-interface eth0 --protocol tcp --source-port 1177 --jump DROP

# Destination port.
iptables --append INPUT --in-interface eth0 --protocol tcp --source-port 60000 --jump DROP

# IPv4 source address and port.
```

The dialog also includes a dropdown menu for "Create rules for" (set to "Netfilter (iptables)"), checkboxes for "Inbound" and "Deny" (both checked), and buttons for "Save", "Close", "Copy", and "Help".

At the bottom of the Wireshark window, the status bar shows: "Transmission Control Protocol (tcp), 20 bytes" on the left, "Packets: 30098 · Displayed: 2 (0.0%)" in the middle, and "Profile: Default" on the right.

Пример: правило для блокировки group-ib.ru

База GeoIP. Фильтрация по стране

После установки баз GeoIP можно фильтровать пакеты по стране:

`ip and ip.geoip.country == "China"`

ip and ip.geoip.country == "China"

No.	Time	Source	Destination	Protocol	Length	Info
43	13.890390	39.129.9.180	novsem1.fvds.ru	TCP	74	5424 → 22 [SYN] Seq=0 Win=29200 Len=0
44	13.890465	novsem1.fvds.ru	39.129.9.180	ICMP	102	Destination unreachable (Port unreachable)
45	13.905160	222.186.42.213	novsem1.fvds.ru	TCP	66	27374 → 22 [ACK] Seq=872 Ack=1122 Win=
46	13.905790	222.186.42.213	novsem1.fvds.ru	SSHv2	146	Client: Elliptic Curve Diffie-Hellman
47	13.905817	novsem1.fvds.ru	222.186.42.213	TCP	66	22 → 27374 [ACK] Seq=1122 Ack=952 Win=
48	13.906861	novsem1.fvds.ru	222.186.42.213	SSHv2	378	Server: Elliptic Curve Diffie-Hellman
49	14.157419	222.186.42.213	novsem1.fvds.ru	TCP	66	27374 → 22 [ACK] Seq=952 Ack=1434 Win=
50	14.158349	222.186.42.213	novsem1.fvds.ru	SSHv2	82	Client: New Keys
51	14.199331	novsem1.fvds.ru	222.186.42.213	TCP	66	22 → 27374 [ACK] Seq=1434 Ack=968 Win=
53	14.452907	222.186.42.213	novsem1.fvds.ru	SSHv2	130	Client: Encrypted packet (len=64)

Key Exchange (method:ecdh-sha2-nistp256)
Message Code: Elliptic Curve Diffie-Hellman Key Exchange Init (30)
ECDH client's ephemeral public key length: 65
ECDH client's ephemeral public key (Q_C): 04374df6b29019f5d6aa438b59b6a2f2f7b82194fc4fdde6b8c80066b1ff12a20870...
Padding String: a49886745e

```
0040 37 67 00 00 00 4c 05 1e 00 00 00 41 04 37 4d f6 7g...L...A-7M...
0050 b2 90 19 f5 d6 a6 aa 43 8b 59 b6 a2 f2 f7 b8 21 .....C+Y.....!
0060 94 fc f4 fd de 6b 8c 8c 00 66 b1 ff 12 a2 08 70 .....k...f....p
0070 a9 9b fd fc 2d 34 b3 05 1c ad f6 ee 10 3f d5 7d .....4...?..}
0080 0e b2 c8 6a a9 d3 09 24 d5 c7 09 fa 64 a4 98 86 ...j...$....d...
```

ECDH client's ephemeral public key (Q_C) (ssh.ecdh.q_c), 65 bytes | Packets: 30098 · Displayed: 4913 (16.3%) | Profile: Default

Пример: Анализ дампа трафика с VDS, видно китайские хосты, перебирающие ключи SSH.

Анализ TLS-трафика

В перехваченном TLS-трафике доступен только анализ заголовков IP/TCP.

Расшифровка трафика на своём компьютере:

Linux/Windows:

1. установить переменную окружения
`SSLKEYLOGFILE=путь_к_файлу/sslkey.log`
2. В Wireshark указать путь к файлу `sslkey.log` в настройках TLS

Linux:

переменная `LD_PRELOAD` для переопределения функций `read/send/write`

Можно
перехватить
cookie

The screenshot shows a Wireshark capture of an HTTP2 stream. The top pane displays a list of packets, with packet 13828 selected. The middle pane shows the packet details for the selected packet, highlighting the 'Cookie' header field. The bottom pane shows the raw packet bytes in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Lenç	Info
13818	138.057695	nginx-1.kantiana.ru	526768db-91a1-41e5-8661-3400c...	HTTP2	13...	HEADERS[3]: 200 OK, DATA[3]
13826	138.058500	nginx-1.kantiana.ru	526768db-91a1-41e5-8661-3400c...	HTTP2	124	DATA[3]
13828	138.058705	526768db-91a1-41e5-8661-...	nginx-1.kantiana.ru	HTTP2	159	HEADERS[9]: GET /wp-content/plugins/revsl...
13829	138.058777	526768db-91a1-41e5-8661-...	nginx-1.kantiana.ru	HTTP2	169	HEADERS[11]: GET /wp-content/plugins/wpfr...
13836	138.059884	nginx-1.kantiana.ru	526768db-91a1-41e5-8661-3400c...	HTTP2	14...	DATA[3] [TCP segment of a reassembled PDU
13840	138.060561	nginx-1.kantiana.ru	526768db-91a1-41e5-8661-3400c...	HTTP2	178	DATA[3]
13844	138.060561	nginx-1.kantiana.ru	526768db-91a1-41e5-8661-3400c...	HTTP2	14...	DATA[3] [TCP segment of a reassembled PDU
13848	138.061537	526768db-91a1-41e5-8661-...	nginx-1.kantiana.ru	HTTP2	154	HEADERS[13]: GET /wp-content/plugins/wp-pi...
13850	138.062137	526768db-91a1-41e5-8661-...	nginx-1.kantiana.ru	HTTP2	149	HEADERS[15]: GET /wp-content/uploads/maxm...

Header: referer: https://kantiana.ru/
Header: accept-encoding: gzip, deflate, br
Header: accept-language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7
Header: cookie: _ym_uid=1548187011187073595
Header: cookie: _ga=GA1.2.955929483.1551448522
Header: cookie: vm_d=1627030908

0000 00 00 43 01 25 00 00 00 09 80 00 00 07 ff 82 d6 ..C.%... ..
0010 87 04 a7 63 c5 6b 10 f5 24 b5 25 8a e8 b6 63 54 ...c.k..\$.%...cT
0020 86 2c 2f 74 50 69 0b 63 15 db 1d 06 23 03 42 0a ..,/tPi.c...#·B·

Frame (159 bytes) | Decrypted TLS (76 bytes) | Decompressed Header (879 bytes)

Stream (http2.stream), 76 bytes | Packets: 59033 · Displayed: 1590 (2.7%) | Profile: Default

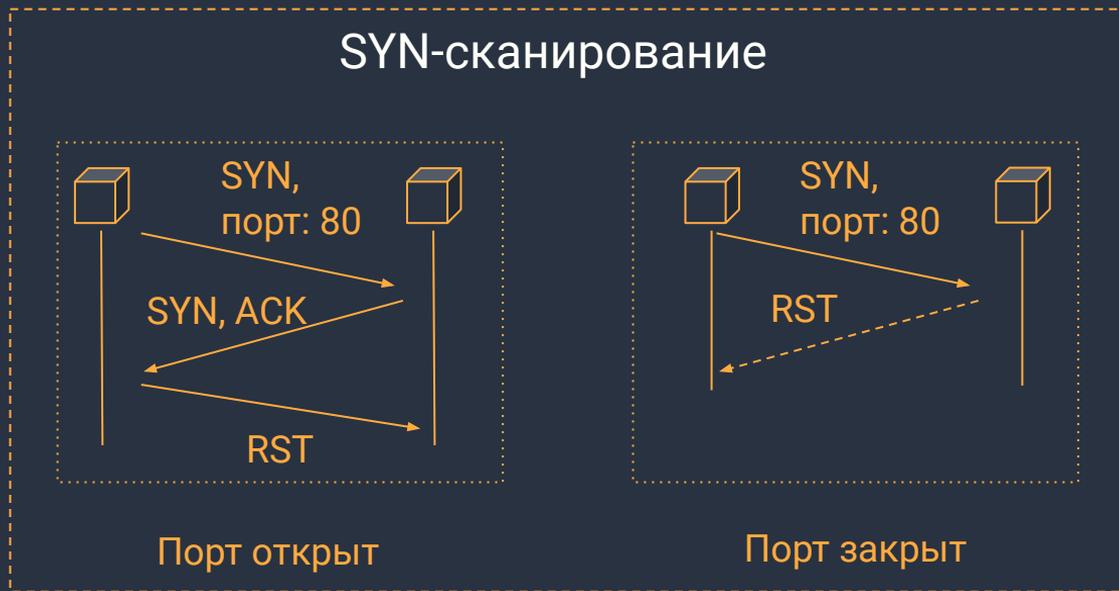
Пример: подключение по https к kantiana.ru

Важно: установка переменных среды **SSLKEYLOGFILE** отрывает дыру в безопасности, так как позволяет следить за трафиком пользователя системы

Определение источника сканирования портов

ищем последовательности
пакетов вида:

1. SYN (\Rightarrow), SYN+ACK (\Leftarrow), RST (\Rightarrow)
2. SYN (\Rightarrow), RST+ACK (\Leftarrow)



No.	Time	Source	Destination	Protocol	Len	Info
80578	29310.3652...	recyber.net	novsem1.fvds.ru	TCP	54	43891 → 19350 [SYN] Seq=0
80579	29310.3653...	novsem1.fvds.ru	recyber.net	TCP	54	19350 → 43891 [RST, ACK]
80581	29310.4396...	recyber.net	novsem1.fvds.ru	TCP	54	43891 → 19350 [RST] Seq=1

Литература и ссылки

- Дуглас Э. Камер - Сети TCP IP. Принципы, протоколы и структура (2003)
- Дампы трафика Wireshark:
<https://gitlab.com/wireshark/wireshark/-/wikis/SampleCaptures>

