
Компьютерные сети. Обучение в записи

Урок 9. Семинар. Основы компьютерных сетей. Транспортный уровень. UDP и TCP

Оглавление

Задача 1. Работа с Wireshark. Фильтры.....	2
Задача 2. Работа с Wireshark. Фильтры.....	4
Домашнее задание.....	5


Задача 1. Работа с Wireshark. Фильтры

Задача 1. Wireshark. Фильтры

proxies

Необходимо найти незашифрованный сайт (можно в гугл настроить соответствующую выдачу по запросу с ключом "inurl:http" в конце) и перехватить логин/пароль.

Skillbox
proxies



Поставьте видео на паузу и выполните задание

Ход выполнения задания 1:

Установка соединения с сайтом

acunetix

acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

go

[Browse categories](#)

[Browse artists](#)

[Your cart](#)

[Signup](#)

[Your profile](#)

[Our guestbook](#)

[AJAX Demo](#)

Links

[Security art](#)

If you are already registered please enter your login information below:

Username :

Password :

login

You can also [signup here](#).

Signup disabled. Please use the username **test** and the password **test**.

PS C:\Users\user> ping testphp.vulnweb.com

Обмен пакетами с testphp.vulnweb.com [44.228.249.3] с 32 байтами данных:
Превышен интервал ожидания для запроса.
Ответ от 44.228.249.3: число байт=32 время=189мс TTL=51
Ответ от 44.228.249.3: число байт=32 время=189мс TTL=51
Ответ от 44.228.249.3: число байт=32 время=188мс TTL=51

Статистика Ping для 44.228.249.3:
Пакетов: отправлено = 4, получено = 3, потеряно = 1
(25% потерь)
Приблизительное время приема-передачи в мс:
Минимальное = 188мсек, Максимальное = 189 мсек, Среднее = 188 мсек

Перехват логина и пароля:

Беспроводная сеть

Файл Правка Вид Запуск Захват Анализ Статистика Телефония Беспроводная связь Инструменты Справка

http.request.method == "POST"

No.	Time	Source	Destination	Protocol	Length	Info
300	47.892468	192.168.50.72	44.228.249.3	HTTP	743	POST /userinfo.php HTTP/1.1

Frame 300: 743 bytes on wire (5944 bits), 743 bytes captured (5944 bits) on interface \Device\NPF{...} Ethernet II, Src: TplinkPte_42:e4:d3 (98:25:4a:42:e4:d3), Dst: ASUSTekCOMPU_32:cb:48 (a...)

Internet Protocol Version 4, Src: 192.168.50.72, Dst: 44.228.249.3

Transmission Control Protocol, Src Port: 60465, Dst Port: 80, Seq: 1075, Ack: 5497, Len...

Hypertext Transfer Protocol

HTML Form URL Encoded; application/x-www-form-urlencoded

Form item: "uname" = "login-proverka"
Key: uname
Value: login-proverka

Form item: "pass" = "PASSWORD_PROVERKA"
Key: pass
Value: PASSWORD_PROVERKA

Ethernet

Type

Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7

username=login-proverka&pass=PASSWORD_PROVERKA

HTTP/1.1 302 Found
Server: nginx/1.19.0
Date: Sun, 06 Apr 2025 01:51:18 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Location: login.php


Задача 2. Работа с Wireshark. Фильтры

Задача 2. Wireshark. Фильтры

proxies

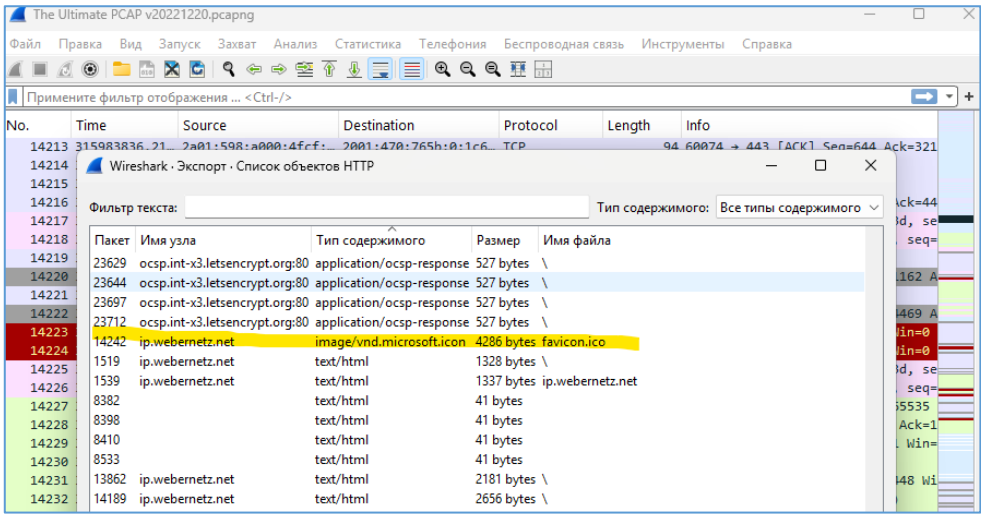
В приложенном файле “The Ultimate PCAP.pcap” найти картинку, какая буква изображена на картинке?

Skillbox proxies



Поставьте видео на паузу и выполните задание

Ход выполнения задания 2:



Домашнее задание

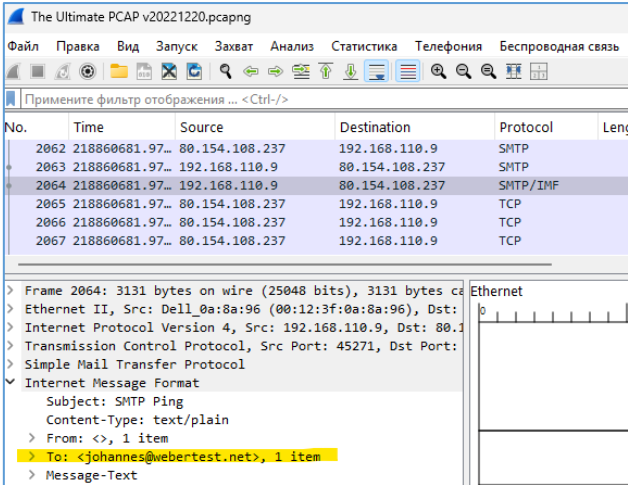
Компьютерные сети. Обучение в записи

Урок 9. Семинар. Основы компьютерных сетей. Транспортный уровень. UDP и TCP

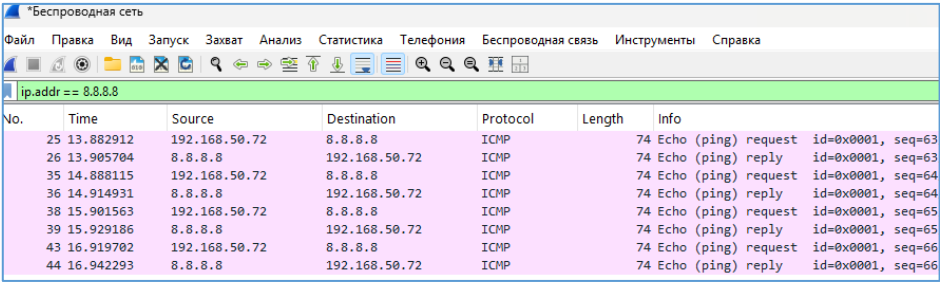
1. В приложенном файле "The Ultimate PCAP.pcapng" (из раздаточного материала) найти e-mail. Что внутри письма и для кого оно?
2. Закрепите навыки фильтрации. Запустите трейс до 8.8.8.8. И перехватите его в Wireshark. Проанализируйте.
3. Закрепите навыки фильтрации. Найдите еще один сайт без шифрования с возможностью ввода логина/пароля. (можно в гугл настроить соответствующую выдачу по запросу с ключом "-inurl:https" в конце). Перехватите их в Wireshark, построив фильтр.
- 4*. На сайте <https://launchpad.net/ubuntu/+archivemirrors> представлены зеркала с образами Убунту по странам. Скачайте файл ls-IR.gz из Чили и с Яндекса. Снимите два дампа для каждого скачивания. Проанализируйте скорость скачивания и посмотрите tcptrace. Прикиньте средний RTT и поищите максимальный RWND для скачивающего. Предоставить скриншоты графиков скорости и tcptrace. Есть ли разница? В чем она?

Ход выполнения домашнего задания:

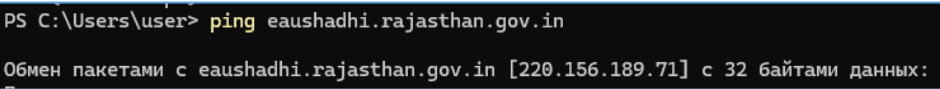
Задание 1:

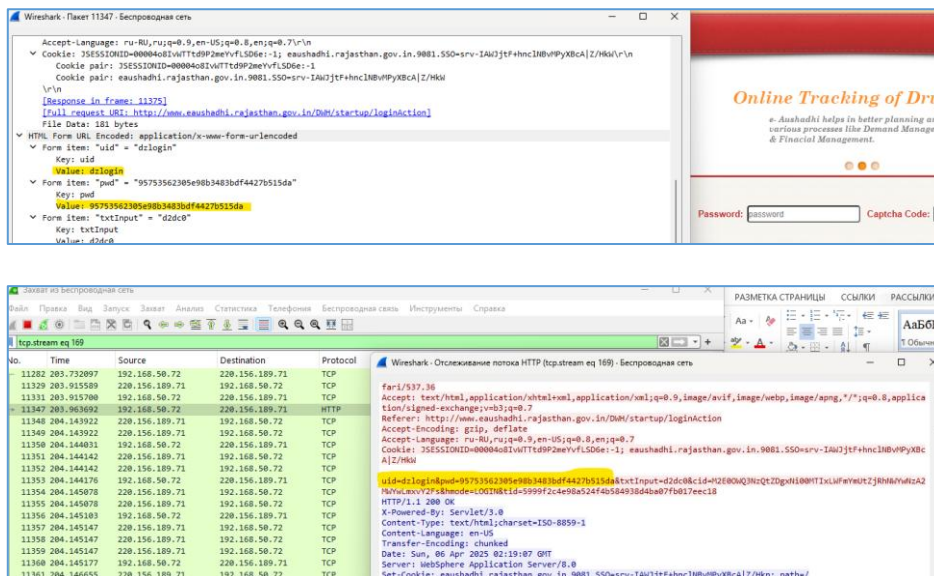


Задание 2:



Задание 3:





Задание 4*:

4*. На сайте <https://launchpad.net/ubuntu/+archivemirrors> представлены зеркала с образами Убунту по странам. Скачайте файл ls-IR.gz из Чили и с Яндекса. Снимите два дампа для каждого скачивания. Проанализируйте скорость скачивания и посмотрите tcptrace. Прикиньте средний RTT и поищите максимальный RWND для скачивающего. Предоставить скриншоты графиков скорости и tcptrace. Есть ли разница? В чем она?

Установка соединения с сайтом <https://launchpad.net/ubuntu/+archivemirrors>
(Чили: <https://mirror.hnd.cl/ubuntu/>)

```
PS C:\Users\user> ping mirror.hnd.cl

Обмен пакетами с mirror.hnd.cl [138.186.10.35] с 32 байтами данных:
Ответ от 138.186.10.35: число байт=32 время=275мс TTL=51
Ответ от 138.186.10.35: число байт=32 время=275мс TTL=51
Ответ от 138.186.10.35: число байт=32 время=281мс TTL=51
Ответ от 138.186.10.35: число байт=32 время=275мс TTL=51

Статистика Ping для 138.186.10.35:
Пакетов: отправлено = 4, получено = 4, потеряно = 0
(0% потерь)
Приблизительное время приема-передачи в мс:
Минимальное = 275мсек, Максимальное = 281 мсек, Среднее = 276 мсек
```

Яндекс: <https://mirror.yandex.ru/ubuntu/>)

```
PS C:\Users\user> ping mirror.yandex.ru

Обмен пакетами с mirror.yandex.ru [213.180.204.183] с 32 байтами данных:
Ответ от 213.180.204.183: число байт=32 время=52мс TTL=54
Ответ от 213.180.204.183: число байт=32 время=51мс TTL=54
Ответ от 213.180.204.183: число байт=32 время=152мс TTL=54
Ответ от 213.180.204.183: число байт=32 время=46мс TTL=54

Статистика Ping для 213.180.204.183:
Пакетов: отправлено = 4, получено = 4, потеряно = 0
(0% потерь)
Приблизительное время приема-передачи в мс:
Минимальное = 46мсек, Максимальное = 152 мсек, Среднее = 75 мсек
```

настройка фильтрации в Wireshark и отслеживание скачивания пакетов:

Чили

TCP · 1UDP							
Адрес A	Порт A	Адрес B	Порт B	Пакеты	Байт	ИД потока	Всего пакетов
192.168.50.72	60778	138.186.10.35	443	27 047	33 МБ	20	27 047

Отфильтровано в процентах	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
100.00%	4 350	237 кБ	22 697	33 МБ

Абс. время начала	Продолжительность	Bits/s A → B	Bits/s B → A	Потоки
00:21:43.901	54.7612	34 kbps	4802 kbps	43

Яндекс

TCP · 4UDP							
Адрес A	Порт A	Адрес B	Порт B	Пакеты	Байт	ИД потока	Всего пакетов
192.168.50.72	60415	213.180.204.183	443	3	162 байты	3	3
192.168.50.72	60418	213.180.204.183	443	3	164 байты	2	3
192.168.50.72	60429	213.180.204.183	443	5	330 байты	24	5
192.168.50.72	60430	213.180.204.183	443	31 603	33 МБ	25	31 603

Отфильтровано в процентах	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
100.00%	2	108 байты	1	54 байты
100.00%	2	108 байты	1	56 байты
100.00%	5	330 байты	0	0 байты
100.00%	5 334	327 кБ	26 269	33 МБ

Абс. время начала	Продолжительность	Bits/s A → B	Bits/s B → A	Потоки
00:13:00.476	0.0393	21 kbps	10 kbps	0
00:13:00.476	0.0521	16 kbps	8604 bits/s	0
00:13:01.962	15.0288	175 bits/s	0 bits/s	0
00:13:01.962	17.1751	152 kbps	15 Mbps	8

Wireshark · Свойства файла захвата · Беспроводная сеть

Подробности

Файл

Имя: C:\Users\user\AppData\Local\Temp\wireshark_Беспроводная сетьRCFV42.pcapng
Длина: 38 MB
Хэш (SHA256): e340601c7a71cc929e96f5f4be9a248c39f8e03b0ecbddd7b5c39f37b5ba84
Хэш (SHA1): 3c8d76188d0e91e875957fddae36160584afd101
Формат: Wireshark/... - pcapng
Инкапсуляция: Ethernet

Время

Первый пакет: 2025-04-11 00:21:32
Последний пакет: 2025-04-11 00:23:03
Прошло: 00:01:31

Захват

Оборудование: 12th Gen Intel(R) Core(TM) i7-12700 (with SSE4.2)
ОС: 64-bit Windows 11 (24H2), build 26100
Приложение: Dumpcap (Wireshark) 4.4.5 (v4.4.5-0-g47253bcf3773)

Интерфейсы

Интерфейс	Потерянные пакеты	Фильтр захвата	Тип соединения	Ограничение на размер пакета (snaplen)
Беспроводная сеть	0 (0.0%)	нет	Ethernet	262144 Б

Статистика

Измеряемые параметры	Захвачено	Показано	Отмечено
Пакеты	31715	27047 (85.3%)	—
Временной промежуток, с	91.570	54.761	—
В среднем, пакетов/с	346.3	493.9	—
Средний размер пакета, Б	1195	1224	—
Байты	37886853	33107400 (87.4%)	0
В среднем байт/с	413 к	604 к	—
В среднем бит/с	3309 к	4836 к	—

Wireshark · Свойства файла захвата · Беспроводная сеть

Подробности

Файл

Имя: C:\Users\user\AppData\Local\Temp\wireshark_Беспроводная сетьSK2X42.pcapng
Длина: 35 MB
Хэш (SHA256): 13c47f2b6bcbfaf1f1b873912f6706e3119e3c5af8f43ed778da59e49d257311
Хэш (SHA1): 73e57247af640943f4b0e4028b160fc51e020e6
Формат: Wireshark/... - pcapng
Инкапсуляция: Ethernet

Время

Первый пакет: 2025-04-11 00:13:00
Последний пакет: 2025-04-11 00:13:26
Прошло: 00:00:25

Захват

Оборудование: 12th Gen Intel(R) Core(TM) i7-12700 (with SSE4.2)
ОС: 64-bit Windows 11 (24H2), build 26100
Приложение: Dumpcap (Wireshark) 4.4.5 (v4.4.5-0-g47253bcf3773)

Интерфейсы

Интерфейс	Потерянные пакеты	Фильтр захвата	Тип соединения	Ограничение на размер пакета (snaplen)
Беспроводная сеть	0 (0.0%)	нет	Ethernet	262144 Б

Статистика

Измеряемые параметры	Захвачено	Показано	Отмечено
Пакеты	32883	31614 (96.1%)	—
Временной промежуток, с	25.636	18.662	—
В среднем, пакетов/с	1282.7	1694.1	—
Средний размер пакета, Б	1050	1054	—
Байты	34538835	33334901 (96.5%)	0
В среднем байт/с	1347 к	1786 к	—
В среднем бит/с	10 М	14 М	—

Ссылка на репозиторий:

<https://github.com/olgashenkel/GeekBrains-specialization-ELECTIVES/tree/main/08.%20Computer%20networks>