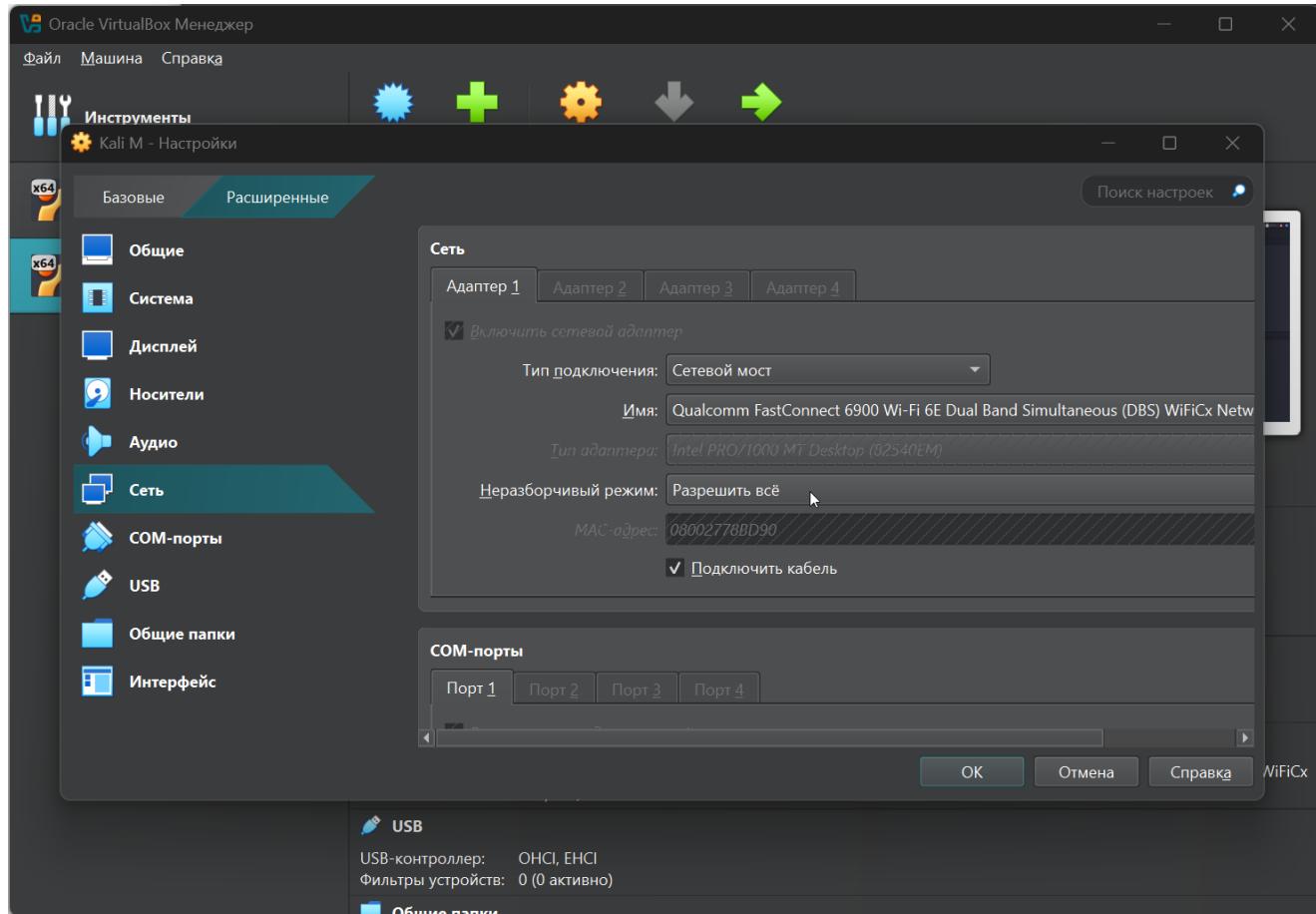


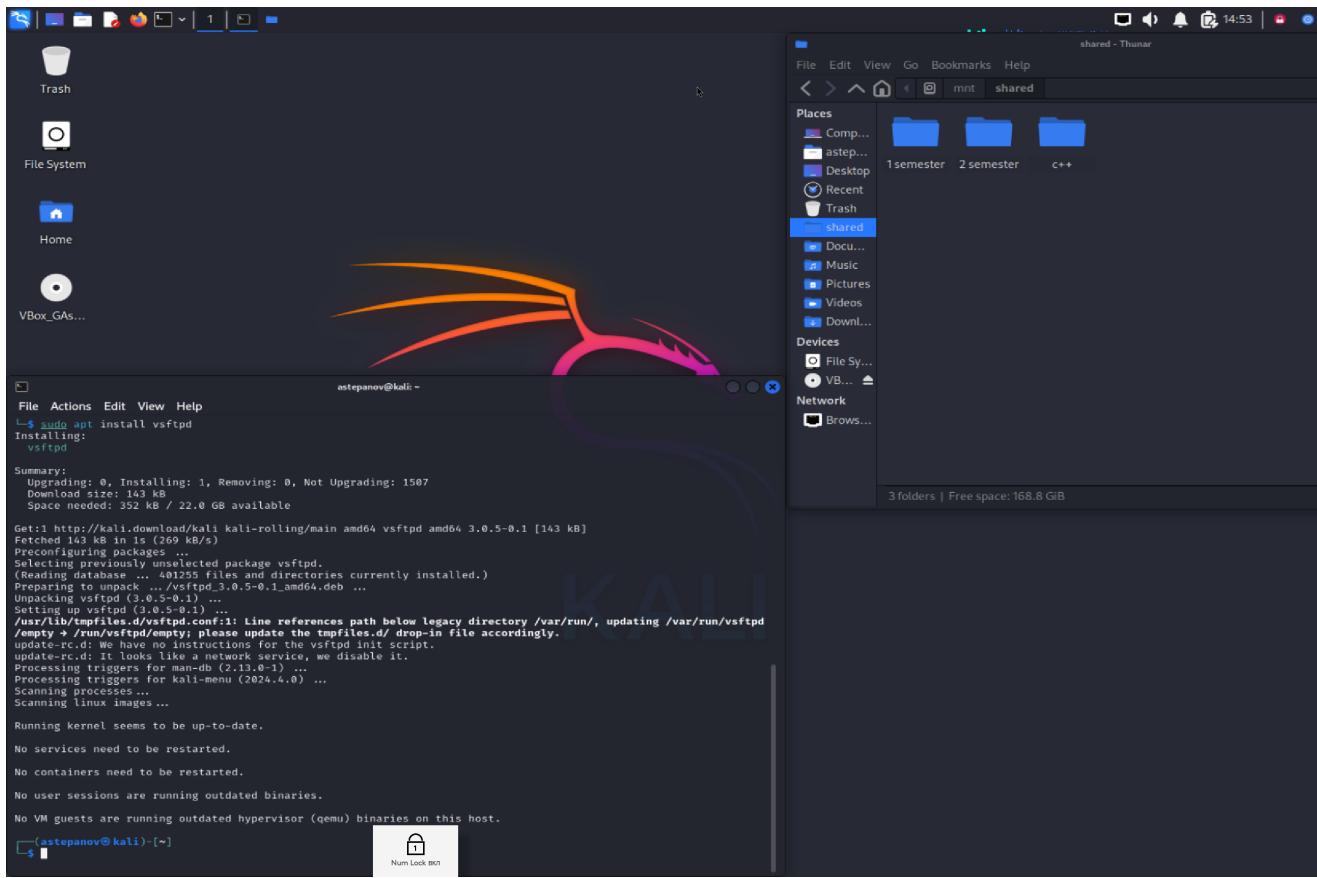
Модуль 2. Сканирование сетей (HW)

Лабораторная работа №1 (HW)

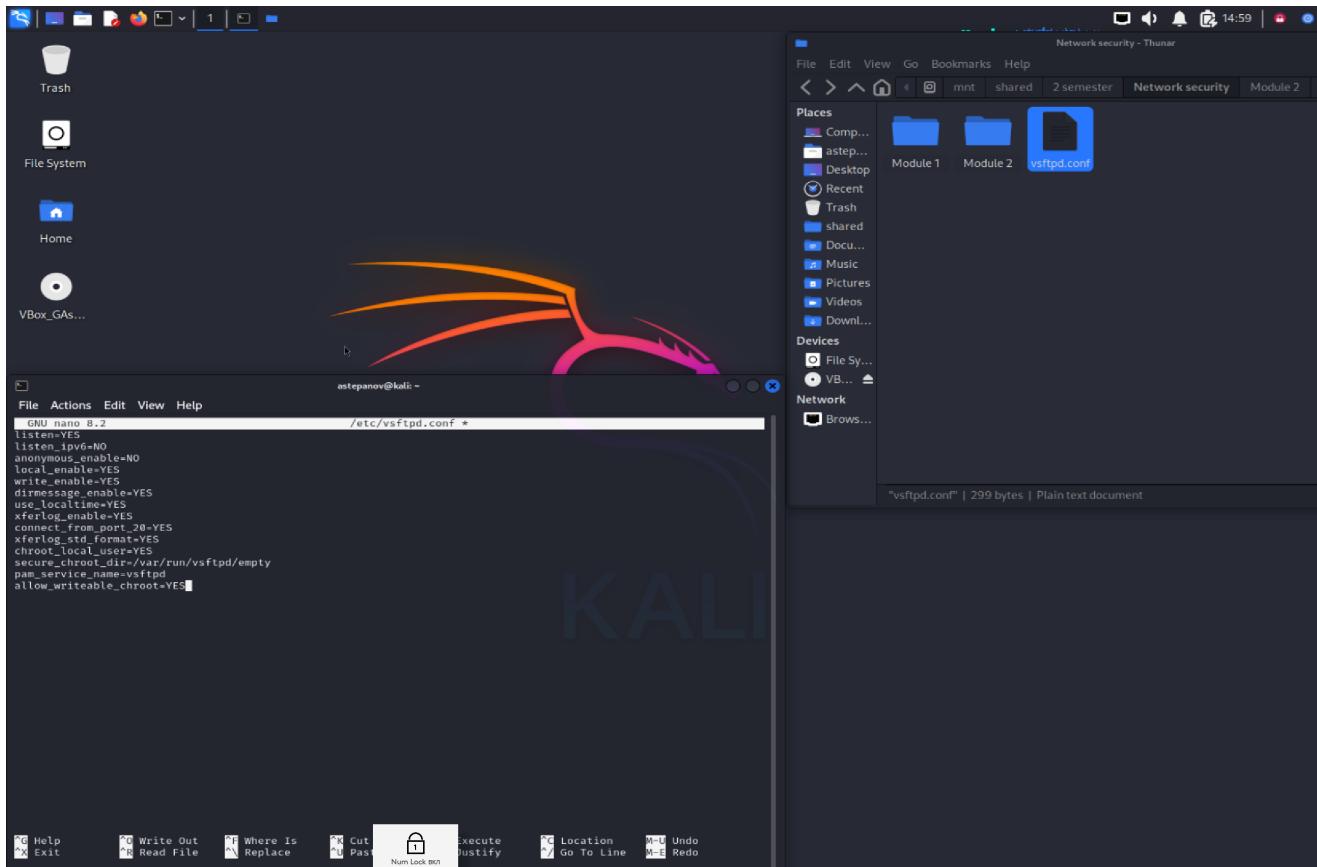
Шаг 1. Настраиваем сетевой мост между хост-системой Windows и VM Kali Linux



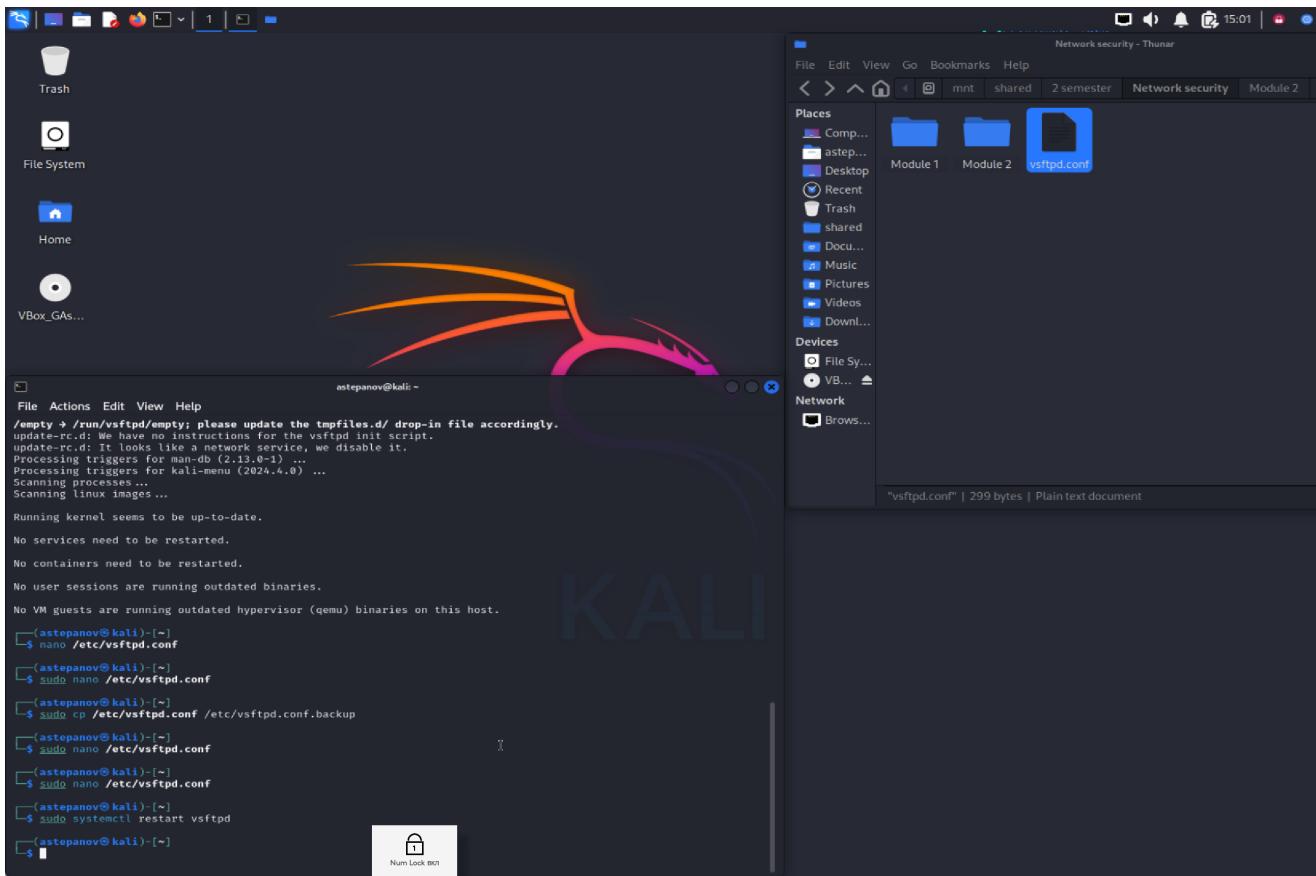
Шаг 2. Устанавливаем vsftpd на Kali Linux



Шаг 3. Создаем новый конфиг для vsftpd



Шаг 4. Перезагружаем службу



Шаг 5. Создаем нового пользователя ftpuser с паролем 123456

The screenshot shows a terminal window with the title 'astepanov@kali: ~'. It displays a series of commands used to create a new user account named 'ftpuser' and set its password. The user is prompted for a new password, which is then confirmed.

```
File Actions Edit View Help  
No containers need to be restarted.  
No user sessions are running outdated binaries.  
No VM guests are running outdated hypervisor (qemu) binaries on this host.  
└─(astepanov㉿kali)-[~]  
$ nano /etc/vsftpd.conf  
└─(astepanov㉿kali)-[~]  
$ sudo nano /etc/vsftpd.conf  
└─(astepanov㉿kali)-[~]  
$ sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.backup  
└─(astepanov㉿kali)-[~]  
$ sudo nano /etc/vsftpd.conf  
└─(astepanov㉿kali)-[~]  
$ sudo nano /etc/vsftpd.conf  
└─(astepanov㉿kali)-[~]  
$ sudo systemctl restart vsftpd  
└─(astepanov㉿kali)-[~]  
$ sudo useradd ftpuser  
└─(astepanov㉿kali)-[~]  
$ sudo mkhomedir_helper ftpuser  
└─(astepanov㉿kali)-[~]  
$ sudo passwd ftpuser  
New password:  
Retype new password:  
passwd: password updated successfully  
└─(astepanov㉿kali)-[~]  
$
```

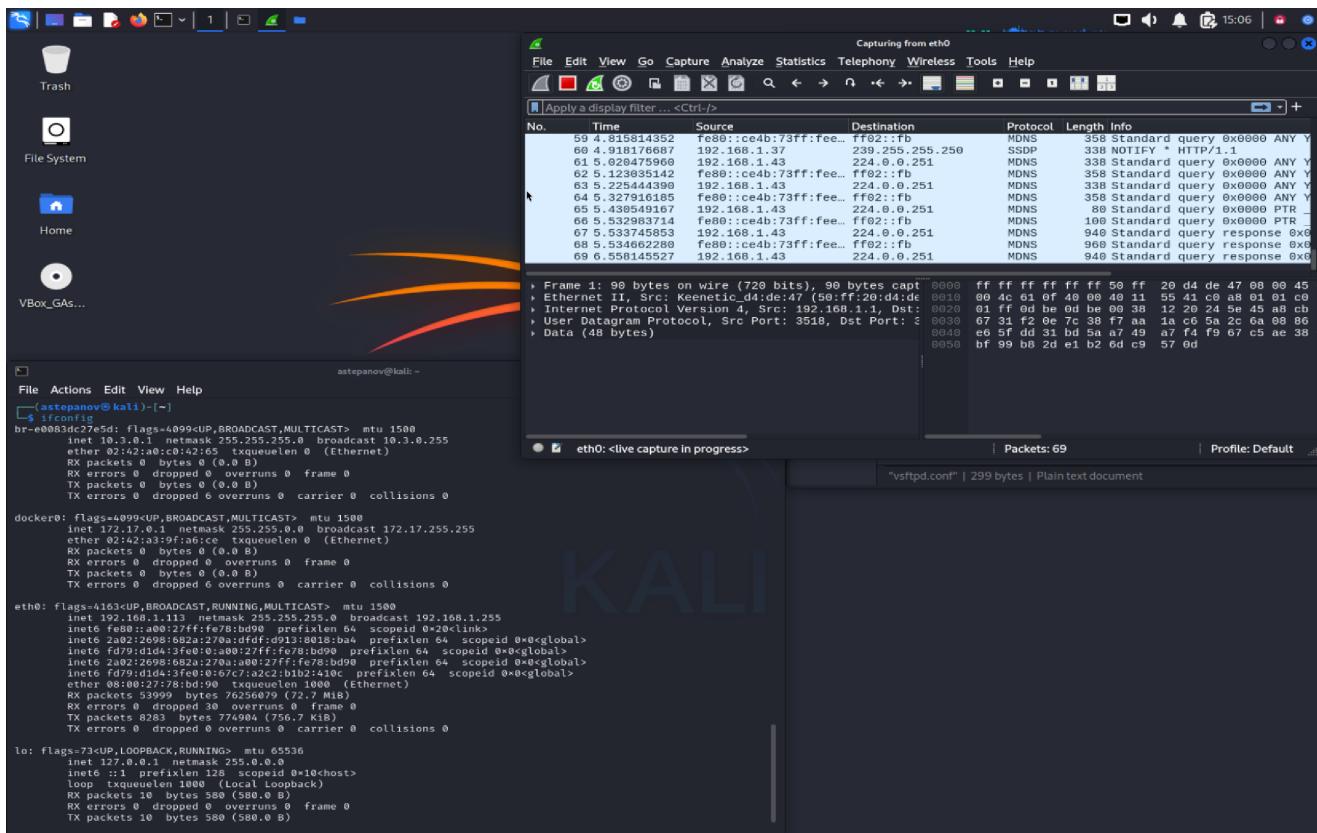
Шаг 6. Создаем в домашней директории нового пользователя файл helloworld.txt

```

astepanov@kali: ~
File Actions Edit View Help
└─(astepanov@kali)─[~]
$ sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.backup
└─(astepanov@kali)─[~]
$ sudo nano /etc/vsftpd.conf
└─(astepanov@kali)─[~]
$ sudo nano /etc/vsftpd.conf
└─(astepanov@kali)─[~]
$ sudo systemctl restart vsftpd
└─(astepanov@kali)─[~]
$ sudo useradd ftpuser
└─(astepanov@kali)─[~]
$ sudo mkhomedir_helper ftpuser
└─(astepanov@kali)─[~]
$ sudo passwd ftpuser
New password:
Retype new password:
passwd: password updated successfully
└─(astepanov@kali)─[~]
$ sudo touch /home/ftpuser/helloworld.txt
└─(astepanov@kali)─[~]
$ nano /home/ftpuser/helloworld.txt
└─(astepanov@kali)─[~]
$ 
└─(astepanov@kali)─[~]
$ sudo nano /home/ftpuser/helloworld.txt
└─(astepanov@kali)─[~]
$ 

```

Шаг 7. Запускаем Wireshark и начинаем слушать интерфейс eth0, который находится в одной локальной сети с хост-машиной Windows.



Шаг 8. Подключаемся по ftp с хостовой машины на машину Kali по ip-адресу интерфейса eth0 (192.168.1.113)

```
Администратор: C:\Windows\system32\cmd.exe - ftp 192.168.1.113
Microsoft Windows [Version 10.0.26100.2894]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\lmz>ftp 192.168.1.113
Связь с 192.168.1.113.
220 (vsFTPd 3.0.5)
200 Always in UTF8 mode.
Пользователь (192.168.1.113:(none)): ftpuser
331 Please specify the password.
Пароль:

230 Login successful.
ftp> █
```

Вводим логин и пароль юзера ftpuser - подключение успешно выполнено

Шаг 9. Загружаем созданный файл по ftp

1. После подключения по ftp переходим в бинарный режим (для скачивания файлов)
2. Скачиваем файл командой get
3. Проверяем командой dir, что файл сказался в директорию хост-машины

Hyper

Администратор: C:\Windows\system32\cmd.exe

```
Microsoft Windows [Version 10.0.26100.2894]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\lmz>ftp 192.168.1.113
Связь с 192.168.1.113.
220 (vsFTPd 3.0.5)
200 Always in UTF8 mode.
Пользователь (192.168.1.113:(none)): ftpuser
331 Please specify the password.
Пароль:

230 Login successful.
ftp> binary
200 Switching to Binary mode.
ftp> get helloworld.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for helloworld.txt (13 bytes).
226 Transfer complete.
ftp: 13 байт получено за 0.00 (сек) со скоростью 13.00 (КБ/сек).
ftp> buy
Недопустимая команда.
ftp> bye
221 Goodbye.

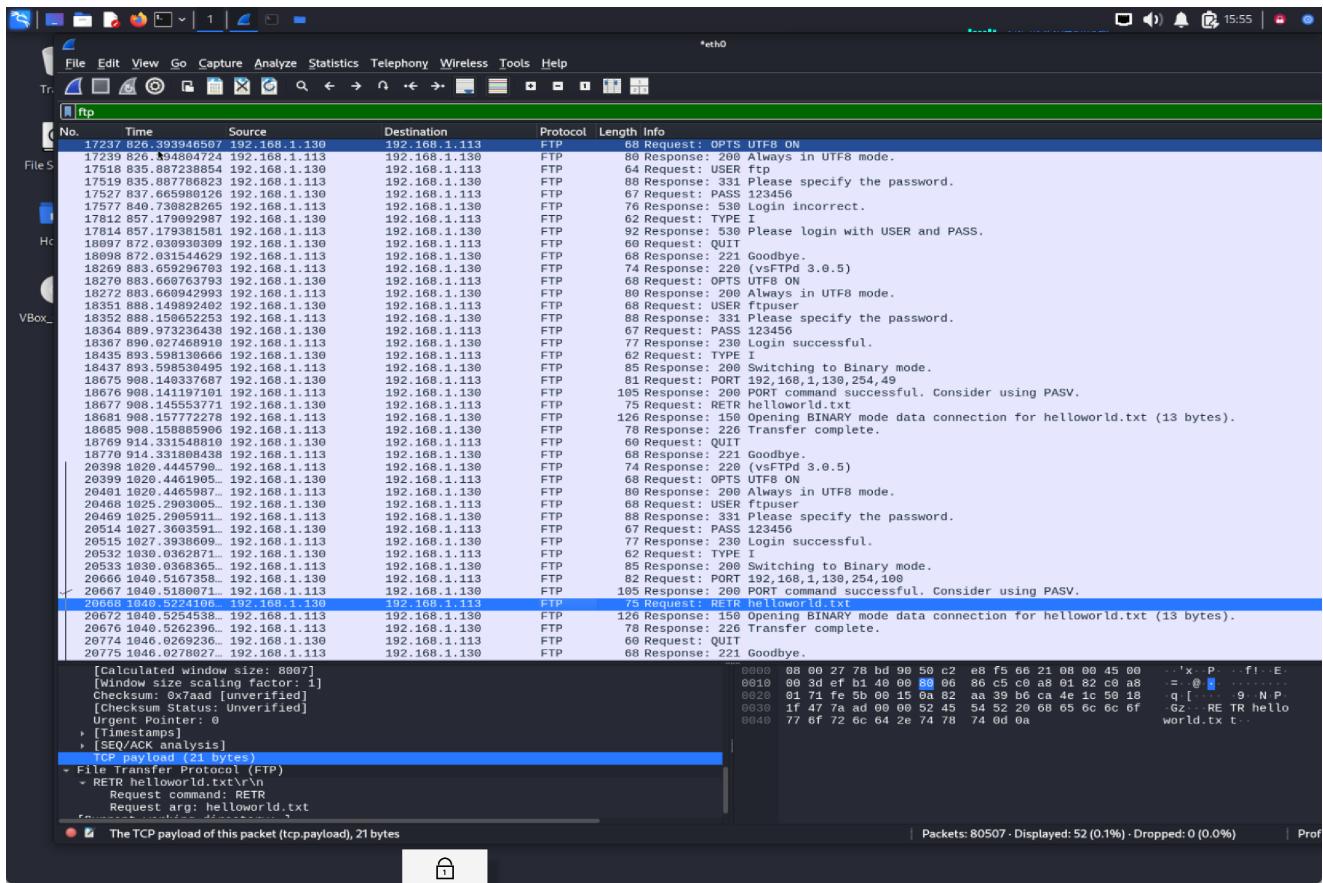
C:\Users\lmz>dir
Том в устройстве С имеет метку Windows 11
Серийный номер тома: 7A0F-C434

Содержимое папки C:\Users\lmz

13.03.2025 23:23    <DIR>      .
07.03.2025 22:01    <DIR>      ..
09.03.2025 20:42    <DIR>      .aws
09.03.2025 20:42    <DIR>      .azure
10.03.2025 00:34        93 .bash_history
09.03.2025 21:18    <DIR>      .docker
09.03.2025 21:31        4 169 .hyper.js.backup
09.03.2025 21:32        4 149 .hyper.js.backup2
09.03.2025 15:12    <DIR>      .rest-client
13.03.2025 22:50    <DIR>      .VirtualBox
07.03.2025 22:55    <DIR>      .vscode
10.03.2025 22:20        22 .wslconfig
07.03.2025 22:01    <DIR>      Contacts
09.03.2025 22:24    <DIR>      Desktop
08.03.2025 11:42    <DIR>      Documents
10.03.2025 18:58    <DIR>      Downloads
07.03.2025 22:01    <DIR>      Favorites
13.03.2025 23:23        13 helloworld.txt
07.03.2025 22:01    <DIR>      Links
07.03.2025 22:01    <DIR>      Music
09.03.2025 21:11        2 883 584 NTUSER.DAT
16.01.2025 23:46    <DIR>      OneDrive
07.03.2025 22:01    <DIR>      Pictures
07.03.2025 22:01    <DIR>      Saved Games
07.03.2025 22:02    <DIR>      Searches
08.03.2025 12:06        9 start
07.03.2025 22:09    <DIR>      Videos
    7 файлов       2 892 039 байт
    20 папок   199 521 722 368 байт свободно

C:\Users\lmz>
C:\Users\lmz>
```

Шаг 10. Изучаем содержимое пакетов в Wireshark



Для удобства пакеты были отфильтрованы в Wireshark по протоколу FTP.

Общие выводы по работе протокола FTP

Сам протокол довольно простой.

Клиент (192.168.1.130) и сервер (192.168.1.113) общаются между собой, обмениваясь пакетами типа "ЗАПРОС" - "ОТВЕТ", передавая внутри пакета простые команды.

Запрос представляет из себя команду с 2 (основными) полями - тип команды и аргумент команды.

Ответ так же содержит 2 (основных) поля - код ответа и аргумент ответа.

Порядок взаимодействия клиента и сервера:

- Клиент инициирует взаимодействие с FTP-сервером, передавая TCP-пакет на 21-ый управляющий порт FTP-сервера
- Сервер отвечает клиенту по FTP-протоколу, передавая 220 код, сообщающий о готовности к ftp-сессии с новым пользователем
- Клиент передает серверу команду OPTS с аргументом UTF8 ON, определяющую кодировку в формате UTF-8
- Далее клиент и сервер обмениваются информацией о пользователе и пароле, производя аутентификацию
- В момент перед началом передачи данных с сервера на клиент, клиент отправляет на сервер данные об ip-адресе и о порте, через который будет произведена передача данных с сервера командой с кодом **PORT** и аргументом **192,168,1,130,254,100**, где два последних числа определяют порт передачи бинарных данных: **254*256+100=65124**
- Сервер сообщает клиенту о том, что порт успешно открыт и передача данных будет производится в пассивном режиме

7. Клиент посыпает серверу команду RETR (retrieve - получить), с именем файла в аргументе, на получение файла. Сервер проверяет, существует ли файл и есть ли у клиента права на его скачивание. Если файл доступен, сервер открывает соединение для передачи данных и начинает отправку файла. Клиент получает файл и сохраняет его.
8. По окончанию скачивания сервер присыпает клиенту ответ об успешном скачивании файла.
9. Клиент закрывает соединение
10. Сервер закрывает соединение

Часть 2

Шаг 1. Устанавливаем и запускаем сервис vsftpd

The screenshot shows a terminal window titled 'astepanov@kali: ~'. The terminal output is as follows:

```
(astepanov㉿kali)-[~]
$ sudo apt update && sudo apt install -y vsftpd
[sudo] password for astepanov:
Hit:1 http://http.kali.org/kali kali-rolling InRelease
1507 packages can be upgraded. Run 'apt list --upgradable' to see them.
vsftpd is already the newest version (3.0.5-0.1).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1507

(astepanov㉿kali)-[~]
$ sudo systemctl start sftpd
Failed to start sftpd.service: Unit sftpd.service not found.

(astepanov㉿kali)-[~]
$ sudo systemctl start vsftpd
(astepanov㉿kali)-[~]
$ sudo systemctl enable vsftpd
Synchronizing state of vsftpd.service with SysV service script with /usr/lib/systemd/systemd-sysv-in
Executing: /usr/lib/systemd/systemd-sysv-install enable vsftpd
Created symlink '/etc/systemd/system/multi-user.target.wants/vsftpd.service' → '/usr/lib/systemd/syste
m/service'.

(astepanov㉿kali)-[~]
$
```

Шаг 2. Создаем SSL-сертификат шифрования

Флаг	Значение
openssl	Запускает утилиту OpenSSL (для работы с криптографией)
req	Использует модуль OpenSSL для создания запроса на сертификат (CSR) или самоподписанного сертификата
-x509	Генерирует самоподписанный сертификат (без запроса CSR)
-nodes	Означает " No DES " – создается ключ без пароля (не шифруется, чтобы сервер мог загружаться без ввода пароля)
-days 365	Срок действия сертификата 365 дней
-newkey rsa:2048	Создает новую пару ключей : приватный и публичный, используя RSA с длиной 2048 бит
-keyout /etc/ssl/private/vsftpd.pem	Указывает, куда сохранить приватный ключ (и сертификат, т.к. они объединены в один файл)
-out /etc/ssl/private/vsftpd.pem	Указывает, куда сохранить самоподписанный сертификат

Шаг 3. Настройка vsftpd для работы с FTPS

```

File Actions Edit View Help
astepanov@kali: ~ x astepanov@kali: ~ x astepanov@kali: ~ x
GNU nano 8.2
/etc/vsftpd.conf
listen=YES
listen_ipv6=NO
local_enable=YES
write_enable=YES
listen=YES
listen_ipv6=NO
chroot_local_user=YES
ssl_enable=YES
rsa_cert_file=/etc/ssl/private/vsftpd.pem
rsa_private_key_file=/etc/ssl/private/vsftpd.pem
force_local_data_ssl=YES
force_local_logins_ssl=YES
ssl_tlsv1=YES
ssl_ssly2=NO
ssl_ssly3=NO
ssl_ciphers=HIGH:!aNULL:!MD5:!RC4
anonymous_enable=NO
allow_writeable_chroot=YES
pasv_enable=YES
pasv_min_port=40000
pasv_max_port=50000
pasv_address=192.168.1.113

```

File browser view of /home/ftpuser:

Filename	Filesize	Filertype	Last modified	Filename
..		Directory	03/13/2025 03...	..
config		Directory	03/13/2025 03...	helloworld.txt
java		Directory	03/13/2025 03...	
local		Directory	03/13/2025 03...	
.bash_logout	220	File	03/13/2025 03...	
.bashrc	5,351	File	03/13/2025 03...	
.bashrc.original	3,526	original-file	03/13/2025 03...	
face	11,759	File	03/13/2025 03...	
total 11,759				

Server/Local file Directory Remote file Size Priority Status

[Read 30 lines]

^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute ^C Location M-U Undo
 ^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-A Set Mark
 M-6 Copy

Описание настроек конфига vsftpd.conf

Параметр	Описание
listen=YES	Включает режим standalone (прослушивание входящих подключений).
listen_ipv6=NO	Отключает прослушивание IPv6, оставляя только IPv4.
local_enable=YES	Разрешает локальным пользователям вход в FTP.
write_enable=YES	Разрешает пользователям выполнять операции записи (создавать, изменять, удалять файлы).
chroot_local_user=YES	Ограничивает пользователей их домашним каталогом (chroot jail).

Параметр	Описание
allow_writeable_chroot=YES	Разрешает запись в корневую директорию пользователя в chroot-режиме (иначе vsftpd может отказать в запуске).
ssl_enable=YES	Включает поддержку SSL/TLS для безопасного соединения.
rsa_cert_file=/etc/ssl/private/vsftpd.pem	Указывает путь к SSL-сертификату для шифрования соединений.
rsa_private_key_file=/etc/ssl/private/vsftpd.pem	Указывает путь к закрытому ключу SSL.
force_local_data_ssl=YES	Принудительно шифрует весь FTP-трафик (данные).
force_local_logins_ssl=YES	Принудительно требует шифрованный вход (логин и пароль передаются через TLS/SSL).
ssl_tlsv1=NO	Отключает использование устаревшего протокола TLS 1.0.
ssl_tlsv1_2=YES	Разрешает использование TLS 1.2.
ssl_tlsv1_3=YES	Разрешает использование TLS 1.3.
ssl_sslv2=NO	Отключает устаревший и небезопасный SSLv2.
ssl_sslv3=NO	Отключает устаревший и небезопасный SSLv3.
anonymous_enable=NO	Запрещает анонимные подключения к FTP.
pasv_enable=YES	Включает пассивный режим FTP (необходим для работы за NAT или файрволами).
pasv_min_port=40000	Устанавливает минимальный порт для пассивных FTP-соединений.
pasv_max_port=50000	Устанавливает максимальный порт для пассивных FTP-соединений.
pasv_address=192.168.1.113	Указывает IP-адрес сервера, который будет использоваться для пассивного режима (нужно при работе через NAT).

⚠️ Если pasv_address не задан, сервер может отправить клиенту свой внутренний IP, и соединение не установится, если клиент снаружи сети. Данную настройку нужно устанавливать, если клиент подключается из другой сети.

⚠️ `allow_writeable_chroot=YES` - этот параметр потребовалось добавить в конфиг, так как без него подключение выдавало ошибку "refusing to run with writable root inside chroot()". Причина заключается в том, что по умолчанию vsftpd запрещает подключение, если корневая папка (chroot) пользователя доступна для записи, так как это представляет потенциальную угрозу безопасности, а на шаге 5 мы как раз выдаем полный доступ на домашнюю папку пользователя.

Шаг 4. Перезапускаем vsftpd для сохранения настроек

The screenshot shows a terminal window with three tabs, each displaying a shell prompt. The terminal is connected to a server via SSH, with the user 'astepanov' at the host 'kali'. The session is encrypted, as indicated by the green padlock icon in the top right corner. The terminal output is as follows:

```
astepanov@kali: ~
astepanov@kali: ~
astepanov@kali: ~

└─(astepanov㉿kali)-[~]
$ sudo systemctl status vsftpd
[sudo] password for astepanov:
● vsftpd.service - vsftpd FTP server
  Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; preset: disabled)
  Active: active (running) since Thu 2025-03-13 19:02:25 EDT; 1 day 11h ago
    Invocation: aa609eeb6c1544d086a339e318590db4
    Main PID: 35063 (vsftpd)
      Tasks: 1 (limit: 4555)
     Memory: 1.4M (peak: 19M)
        CPU: 807ms
       CGroup: /system.slice/vsftpd.service
               └─35063 /usr/sbin/vsftpd /etc/vsftpd.conf

Mar 13 19:02:25 kali systemd[1]: vsftpd.service: Deactivated successfully.
Mar 13 19:02:25 kali systemd[1]: Stopped vsftpd.service - vsftpd FTP server.
Mar 13 19:02:25 kali systemd[1]: Starting vsftpd.service - vsftpd FTP server ...
Mar 13 19:02:25 kali systemd[1]: Started vsftpd.service - vsftpd FTP server.

└─(astepanov㉿kali)-[~]
$ sudo systemctl restart vsftpd
└─(astepanov㉿kali)-[~]
$ sudo systemctl restart vsftpd.service
└─(astepanov㉿kali)-[~]
$ sudo systemctl start vsftpd.service
└─(astepanov㉿kali)-[~]
$ sudo systemctl enable vsftpd.service
Synchronizing state of vsftpd.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable vsftpd
└─(astepanov㉿kali)-[~]
$ sudo nano /etc/ssl/private/vsftpd.pem
```

Шаг 5. Добавляем пользователя для FTPS

```
astepanov@kali: ~ x astepanov@kali: ~ x astepanov@kali: ~ x
File Actions Edit View Help astepanov@kali: ~

└── (astepanov㉿kali)-[~]
    └── $ sudo adduser ftpuser
        fatal: The user 'ftpuser' already exists.

└── (astepanov㉿kali)-[~]
    └── $ sudo passwd ftpuser
        New password:
        Retype new password:
        passwd: password updated successfully

└── (astepanov㉿kali)-[~]
    └── $ sudo usermod -d /home/ftpuser ftpuser
        usermod: no changes

└── (astepanov㉿kali)-[~]
    └── $ sudo chmod -R 755 /home/ftpuser

└── (astepanov㉿kali)-[~]
    └── $ sudo chown ftpuser:ftpuser /home/ftpuser

└── (astepanov㉿kali)-[~]
    └── $ █
```

Flags: 0x01B (PSH, ACK)
Window: 512
[Calculated window size: 65536]
[Window size scaling factor: 128]
Checksum: 0x846a [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), No-Operation
[Timestamps]
[SEQ/ACK analysis]
TCP payload (17 bytes)
- File Transfer Protocol (FTP)
- priv_sock_get_cmd
 Response arg: priv_sock_get_cmd
 [Current working directory:]

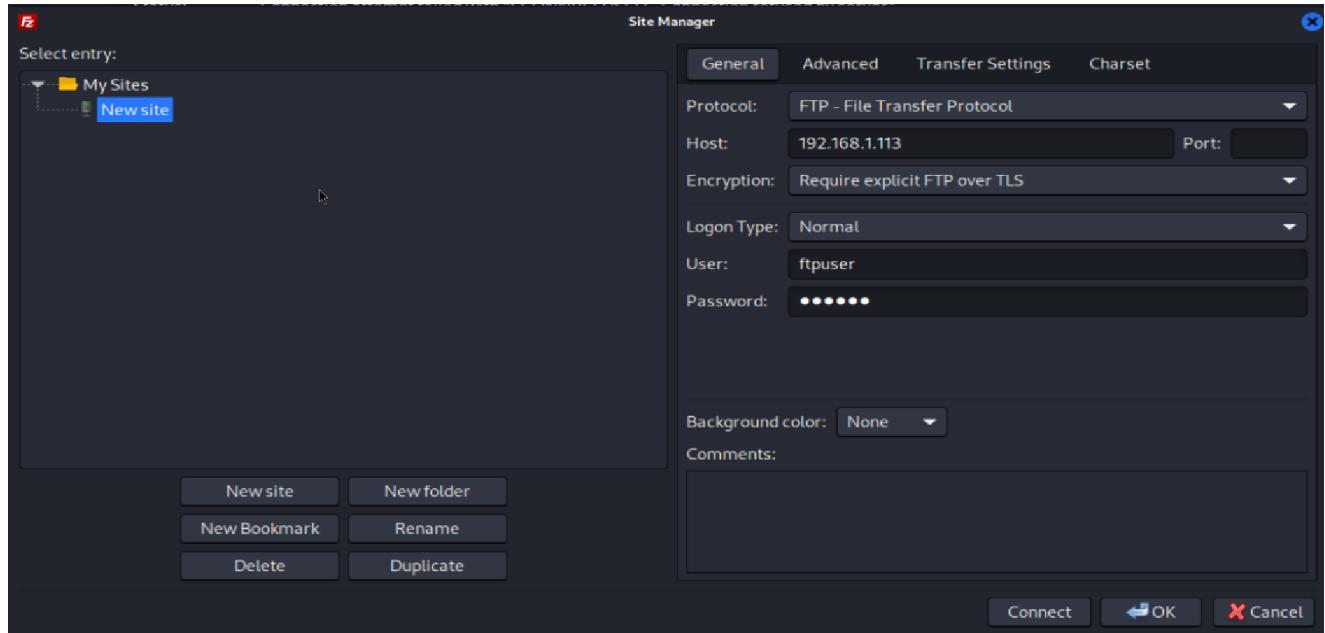
● Response arg (ftp.response.arg), 17 bytes

Разбор команд

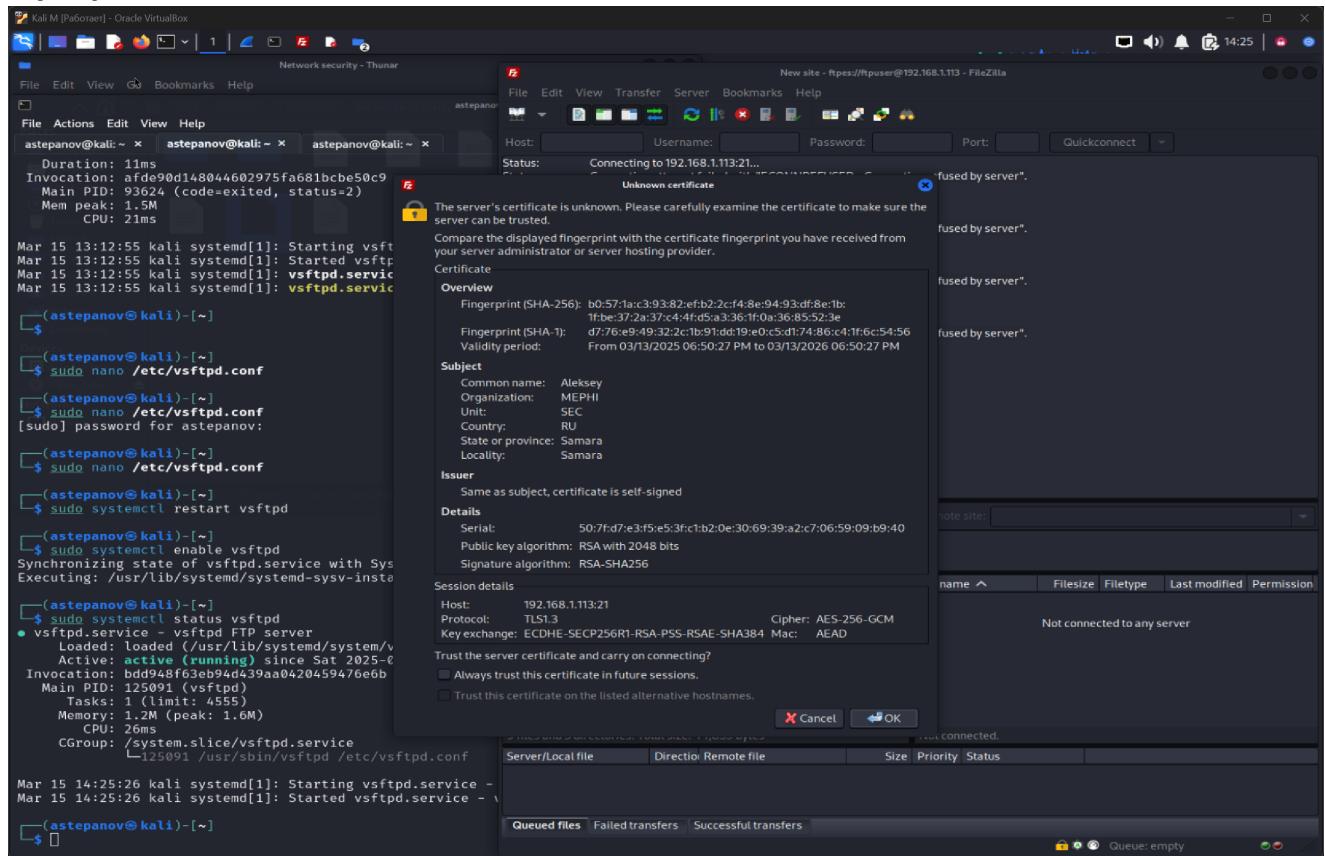
Команда	Описание
<code>sudo adduser ftpuser</code>	Создаёт пользователя <code>ftpuser</code> с домашней директорией <code>/home/ftpuser</code> .
<code>sudo passwd ftpuser</code>	Устанавливает пароль для <code>ftpuser</code> .
<code>sudo usermod -d /home/ftpuser ftpuser</code>	Устанавливает <code>/home/ftpuser</code> как домашнюю папку пользователя.
<code>sudo chmod -R 755 /home/ftpuser</code>	Даёт <code>ftpuser</code> полный доступ (<code>rwx</code>), остальным (<code>r-x</code>).
<code>sudo chown ftpuser:ftpuser /home/ftpuser</code>	Назначает владельцем <code>ftpuser</code> и устанавливает его группу.

Шаг 6. Проверяем соединение

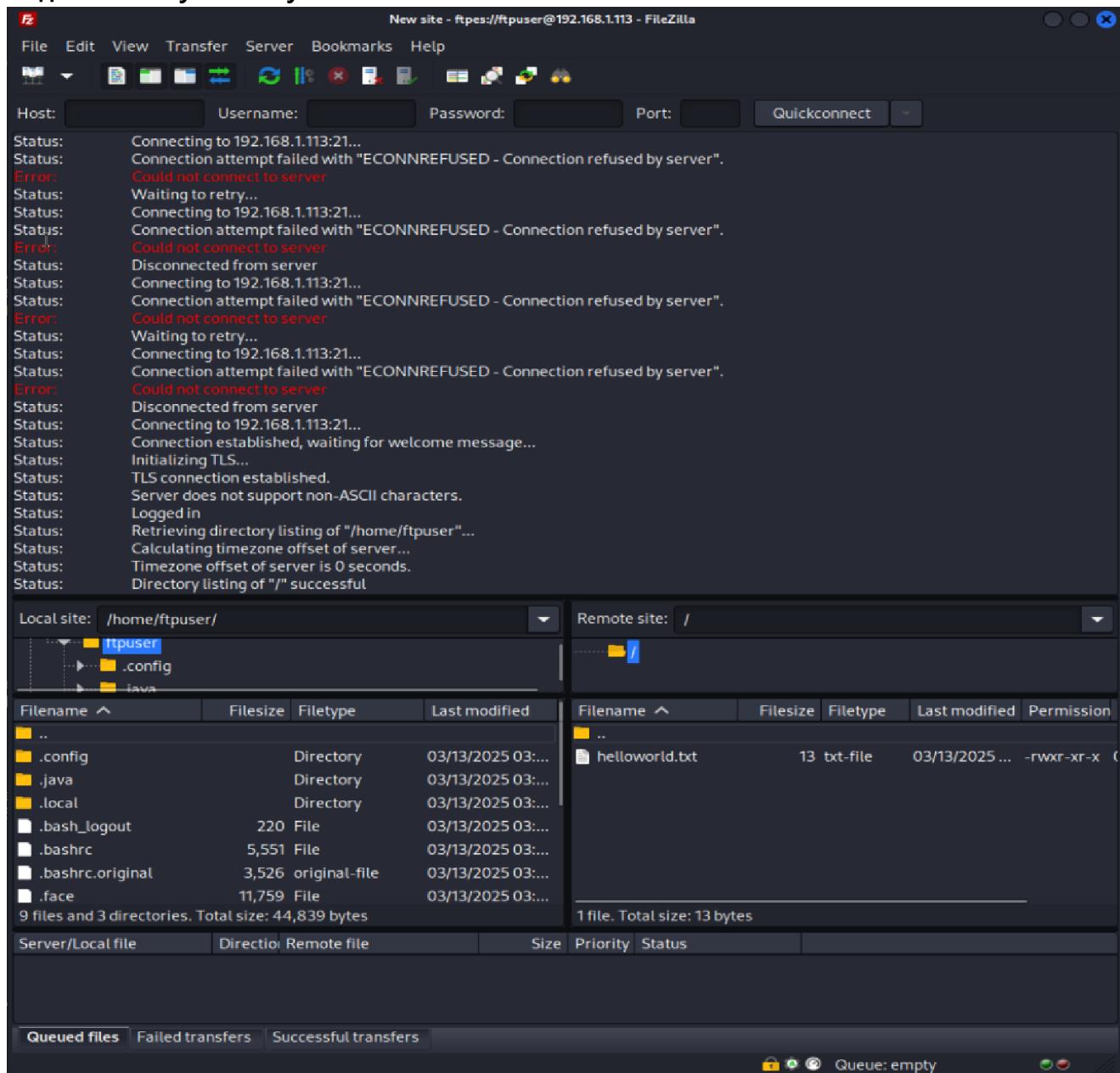
Настройки ftp подключения в FileZilla



Подключаемся к ftp-серверу. Подключение предлагает принять ранее созданный нами tls-сертификат



Подключение успешно установлено



Шаг 7. Сканирование FTP-трафика в Wireshark

Ключевое отличие в передаче трафика заключается в том, что теперь подключение по FTP – шифруется и, при перехвате трафика, содержимое пакетов нельзя просто так прочитать. Это

обеспечивает безопасность при передаче данных по FTP.

