Національний Технічний Університет України

«Київський Політехнічний Інститут Імені Ігоря Сікорського»

Факультет Інформатики Та Обчислювальної Техніки

Кафедра Обчислювальної Техніки

Лабораторна робота №3

Сервіс передачі файлів

Виконала

Шпак Діана

Група: ІО-з21мп

Київ 2023

2. Завдання на роботу.

2.1. Створити закритий ключ та запит на сертифікат для доменного імені, яке відповідає варіанту завдання. Підписати запит на сертифікат, використовуючи сертифікат і закритий ключ центру сертифікації (CA), створеного в лабораторній роботі № 2.

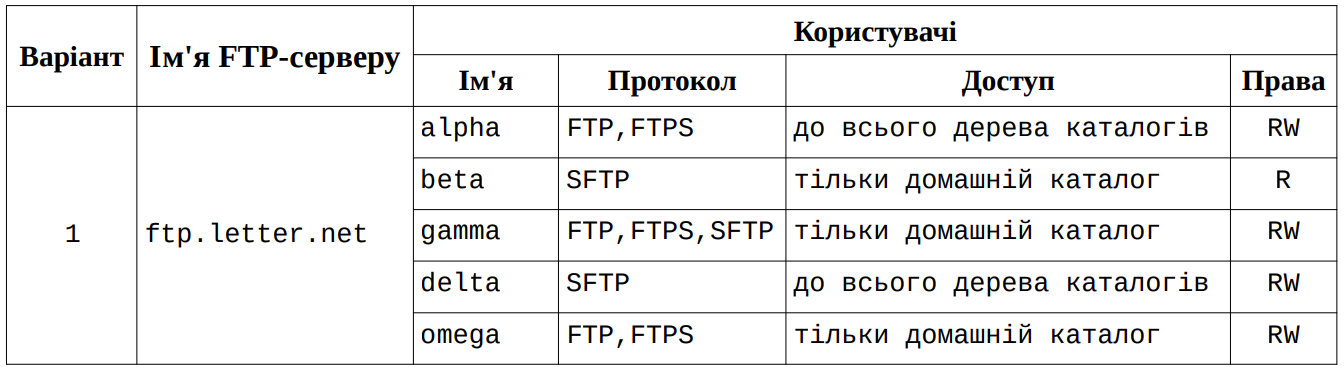
2.2. Встановити та налаштувати файловий сервер, який реалізує протоколи FTP, FTPS та SFTP та відповідає наступним вимогам: - анонімний доступ (користувач ftp або anonymous); - в домашньому каталозі анонімного користувача створені 2 каталоги: pub та incoming, каталог pub має права тільки читання, каталог incoming має права на читання та запис; - створені користувачі з іменами, доступом та правами, які відповідають варіанту завдання; - для створених користувачів забезпечується доступ по протоколам, які відповідають варіанту завдання.

2.3. Виконати аналіз протокольного обміну між клієнтом та сервером під час автентифікації та пересилки файлів.

2.4. Рекомендується використовувати наступне програмне забезпечення: - FTP-сервер: vsftpd + openssh або proftpd; - FTP-клієнт: lftp.

2.5. Для перевірки роботи файлового серверу та аналізу протокольного обміну рекомендується використовувати утиліти: ftp, telnet, netcat, openssl, lftp.

2.6. Додати запис типу A для доменного імені файлового серверу в DNS. Додати сертифікат власного СА у список довірених на вузлі, де запускається FTP-клієнт.



2.1. Створити закритий ключ та запит на сертифікат для доменного імені, яке відповідає варіанту завдання. Підписати запит на сертифікат, використовуючи сертифікат і закритий ключ центру сертифікації (CA), створеного в лабораторній роботі № 2.  
  
#За допомогою openssl створіть новий сертифікат, використовуйте прапорець -days 365 , щоб зробити його дійсним протягом одного року. Тут же зазначимо генерацію закритого 2048-бітного ключа RSA.

#Якщо встановити прапори -keyout і -out в те саме значення, закритий ключ і сертифікат будуть знаходитися в одному файлі:

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.pem -out /etc/ssl/private/vsftpd.pem

# C=UA

# ST=Ukraine

# L=Kyiv

# O=KPI

# OU=OT

# CN=letter CA

Can't load /home/vagrant/.rnd into RNG

139761405747648:error:2406F079:random number generator:RAND\_load\_file:Cannot open file:../crypto/rand/randfile.c:88:Filename=/home/vagrant/.rnd

Generating a RSA private key

.........................+++++

...................................+++++

writing new private key to '/etc/ssl/private/vsftpd.pem'

-----

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [AU]:UA

State or Province Name (full name) [Some-State]:Ukraine

Locality Name (eg, city) []:Kyiv

Organization Name (eg, company) [Internet Widgits Pty Ltd]:KPI

Organizational Unit Name (eg, section) []:OT

Common Name (e.g. server FQDN or YOUR name) []:letter CA

Email Address []:alpha@letter.net

2.2. Встановити та налаштувати файловий сервер, який реалізує протоколи FTP, FTPS та SFTP та відповідає наступним вимогам:

- анонімний доступ (користувач ftp або anonymous);

- в домашньому каталозі анонімного користувача створені 2 каталоги: pub та incoming, каталог pub має права тільки читання, каталог incoming має права на читання та запис;

- створені користувачі з іменами, доступом та правами, які відповідають варіанту завдання;

- для створених користувачів забезпечується доступ по протоколам, які відповідають варіанту завдання.

Для виконання даного завдання нам потрібно мати 1 ftp сервер, відповідно для запуску даних серверів локально ми будемо використовувати віртуал бокс і вагрант який дозволяє описати наші ресурси скриптами відповідно дестроїти і запускати їх з консолі, що дасть нам можливість виконувати завдання набагато зручніше.

Пишемо вагрант скрипт для запуску віртуальної машини на яких будим встановлювати ftp, скрипт буде мати наступний вигляд:

Vagrant.configure("2") do |config|

config.vm.define "ftp1" do |ftp1|

ftp1.vm.box\_download\_insecure = true

ftp1.vm.box = "ubuntu/bionic64"

ftp1.vm.network :private\_network, ip: "172.20.1.80"

ftp1.vm.network "forwarded\_port", guest: 22, host: 22

ftp1.vm.hostname = "ftp1"

ftp1.vm.post\_up\_message = "Run vm for FTP1"

ftp1.vm.provider :virtualbox do |vb|

vb.memory = "2048"

end

ftp1.vm.provision "shell" do |s|

s.path = 'ftp1.sh'

end

end

end

при старті віртупльної машини, запускається скрипт ftp1.sh, в який ми винесем встановлення ліб, і налаштування портів

#!/bin/bash

echo "FTP1"

sudo apt-get update

sudo apt upgrade

sudo apt-get -y install vsftpd

sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.orig

echo "y" | sudo ufw status

echo "y" | sudo ufw allow ssh

echo "y" | sudo ufw default deny incoming

echo "y" | sudo ufw default allow outgoing

echo "y" | sudo ufw enable

echo "y" | sudo ufw status verbose

echo "y" | sudo ufw allow 20,21,990/tcp

echo "y" | sudo ufw allow 40000:50000/tcp

echo "y" | sudo ufw status verbose

sudo apt-get install -y openssh-server

sudo systemctl status ssh

sudo systemctl enable ssh

sudo systemctl restart ssh

sudo cp /etc/ssh/sshd\_config /etc/ssh/sshd\_config.backup

cd /etc/ssh/

cat <<EOT >> /etc/ssh/sshd\_config

Match group ftpaccess

ChrootDirectory %h

X11Forwarding no

AllowTcpForwarding no

ForceCommand internal-sftp

EOT

sudo service ssh restart

подальше налаштування користувачів виконуємо через консоль, наведемо приклад для першого користувача, наступні робляться аналогічним чином

# створення юзера в системі виконується наступною командою

sudo adduser alpha

# створення групи в системі виконується наступною командою

sudo addgroup ftpaccess

# дотавання юзера виконується наступною командою

# sudo usermod -a -G ftpaccess alpha

# встановлюємо власника і права на домашню директорію користувача

sudo chown root: /home/alpha

sudo chmod 755 /home/alpha

# створюємо каталок в домашній директорії, встановлюємо до його права, групу і власника

sudo mkdir /home/alpha/www

sudo chmod 755 /home/alpha/www

sudo chown alpha:ftpaccess /home/alpha/www

# оскільки нам потрібен протокол SFTP то для кожного користувача потрібно додати ссш ключ

cd /home/alpha && sudo mkdir .ssh

sudo chmod 755 .ssh/

sudo touch .ssh/authorized\_keys

sudo chmod 777 .ssh/authorized\_keys

sudo chown alpha:alpha .ssh/authorized\_keys

sudo chown alpha:alpha .ssh/

echo "ПУБЛІЧНИЙ ССШ КЛЮЧ" >> .ssh/authorized\_keys

sudo chmod 600 .ssh/authorized\_keys

Далі переходимо до налаштування самого ФТП сервера:

#На цьому етапі ми дозволимо одному користувачеві з локальним обліковим записом підключатися FTP.

#Дві ключові налаштування для цього вже задано у файлі vsftpd.conf

sudo nano /etc/vsftpd.conf

#Відкриваємо файл і переконуємося, що для директиви anonymous\_enable встановлено значення NO ,

#а для директиви local\_enable - YES :

#Ці параметри забороняють анонімний доступ до сервера FTP і дозволяють доступ локальним користувачам.

#Пам'ятайте, що дозвіл локальних користувачів означає, що будь-який звичайний користувач, вказаний

#у файлі /etc/passwd, може бути використаний для входу FTP.

#Деякі команди FTP дозволяють користувачам додавати, змінювати або видаляти файли та каталоги

#у файловій системі сервера. Увімкніть ці команди, розкоментувавши параметр write\_enable .

#Для цього треба видалити символ ґрат (#) перед цією директивою:

#Також розкоментуйте директиву chroot\_local\_user , щоб запобігти доступу користувача підключеного по FTP,

#до файлів або директорій за межами домашньої директорії:

#Потім додайте директиву user\_sub\_token , значенням якої є змінна оточення $USER .

#Також додайте директиву local\_root і вкажіть шлях /home/$USER/ftp , який також включає змінну

#оточення $USER . Ці директиви роблять так, що користувачі при вході в систему будуть

#перенаправлятися до свого домашнього каталогу. Додайте ці параметри до кінця конфігураційного файлу:

user\_sub\_token=$USER

local\_root=/home/$USER/ftp

pasv\_min\_port=40000

pasv\_max\_port=50000

userlist\_enable=YES

userlist\_file=/etc/vsftpd.userlist

userlist\_deny=NO

#Директива userlist\_deny має два сенси: якщо встановлено значення YES, користувачам зі списку буде

#відмовлено у доступі до FTP, якщо встановлено значення NO, доступ буде дозволено лише користувачам

#зі списку.

#Коли ви закінчите вносити зміни, збережіть файл і вийдіть із редактора. Якщо ви використовували

#nano для редагування файлу, ви можете це зробити, натиснувши CTRL + X, Y, потім ENTER.

#На закінчення додайте свого користувача до файлу /etc/vsftpd.userlist . Використовуйте прапорець

#-a утиліти tee для додавання до файлу:

echo "alpha" | sudo tee -a /etc/vsftpd.userlist

echo "beta" | sudo tee -a /etc/vsftpd.userlist

echo "gamma" | sudo tee -a /etc/vsftpd.userlist

echo "delta" | sudo tee -a /etc/vsftpd.userlist

echo "omega" | sudo tee -a /etc/vsftpd.userlist

#Перевіримо, що додавання відбулося так, як очікувалося:

cat /etc/vsftpd.userlist

#Тепер перезапe демон vsftpd, щоб застосувати зміни конфігурації:

sudo systemctl restart vsftpd

#Ми налаштували наш FTP сервер так, щоб дозволити підключення користувачів alpha, beta, gamma, delta, omega.

#Ми відключили анонімний FTP доступ, перевіримо це, спробувавши підключитися анонімно.

#Якщо конфігурація налаштована правильно, анонімним користувачам буде відмовлено у доступі

#на сервер FTP. Відкрийте ще одне вікно командного рядка та виконайте команду для підключення

#до сервера за протоколом FTP- ftp 172.20.1.80.

#Коли з'явиться запит на введення імені користувача, спробуйте увійти в систему під неіснуючим

#користувачем, наприклад anonymous , і ви отримаєте таке повідомлення:

ftp 172.20.1.80

#Connected to 172.20.1.80.

#220 (vsFTPd 3.0.3)

#Name (172.20.1.80:chygyk): omega

#331 Please specify the password.

#Password:

#230 Login successful.

#Remote system type is UNIX.

#Using binary mode to transfer files.

#ftp> bye

#421 Timeout.

#Закрийте з'єднання, ввівши команду bye :

#Користувачі, які відрізняються від alpha, beta, gamma, delta, omega, також не зможуть підключитися. Спробуйте підключитися

#від імені вашого користувача, який має права sudo в системі. Йому також має бути відмовлено у

#доступі, і це має статися до того, як Ви введете пароль:

ftp 172.20.1.80

#Connected to 172.20.1.80.

#220 (vsFTPd 3.0.3)

#Name (172.20.1.80:chygyk):

#530 Permission denied.

#ftp: Login failed

#ftp> bye

#221 Goodbye.

#Оскільки FTP не шифрує дані передачі, включаючи облікові дані користувачів, рекомендується

#включити TLS/SSL для забезпечення шифрування даних. Першим кроком буде створення SSL-сертифікатів

#для використання разом із vsftpd.

#За допомогою openssl створіть новий сертифікат, використовуйте прапорець -days 365 , щоб зробити

#його дійсним протягом одного року. Тут же зазначимо генерацію закритого 2048-бітного ключа RSA.

#Якщо встановити прапори -keyout і -out в те саме значення, закритий ключ і сертифікат будуть

#знаходитися в одному файлі:

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.pem -out /etc/ssl/private/vsftpd.pem

# C=UA

# ST=Ukraine

# L=Kyiv

# O=KPI

# OU=OT

# CN=letter CA

#Вам буде запропоновано вказати інформацію для вашого сертифіката.

#Замініть виділені значення своєю інформацією. Ці дані не дуже важливі.

#Найголовніше тут це Common Name, в нього треба ввести або IP адресу вашого сервера або його

#ім'я (хостнейм), за яким ви будете до нього підключатися

#Після створення сертифікатів знову відкрийте конфігураційний файл vsftpd:

sudo nano /etc/vsftpd.conf

#У нижній частині файлу будуть два рядки, що починаються з rsa\_ .

#Закоментуйте їх, додавши перед кожною решітки знак #:

rsa\_cert\_file=/etc/ssl/certs/ssl-cert-snakeoil.pem

rsa\_private\_key\_file=/etc/ssl/private/ssl-cert-snakeoil.key

#Після цих рядків додайте наступні рядки, які вказують на створений вами сертифікат

#та закритий ключ:

rsa\_cert\_file=/etc/ssl/private/vsftpd.pem

rsa\_private\_key\_file=/etc/ssl/private/vsftpd.pem

#Далі додайте наступні рядки, щоб заборонити анонімні з'єднання через SSL і вимагати

#SSL для передачі даних і при вході в систему:

allow\_anon\_ssl=NO

force\_local\_data\_ssl=YES

force\_local\_logins\_ssl=YES

#Також настройте сервер на використання TLS протоколу, який прийшов на зміну SSL,

#додавши наступні рядки:

ssl\_tlsv1=YES

ssl\_sslv2=NO

ssl\_sslv3=NO

#І насамкінець, додайте дві останні опції. Перша не вимагатиме повторного використання SSL,

#оскільки це може зламати багато FTP-клієнтів. Друга вимагатиме "високих" шифрів, що в

#даний час означає довжину ключа, рівну або перевищує 128 біт:

require\_ssl\_reuse=NO

ssl\_ciphers=HIGH

#збережіть та закрийте файл. Тепер перезапустимо сервер vsftpd,

#щоб зміни набули чинності:

sudo systemctl restart vsftpd

#На цьому етапі ви більше не зможете підключитися за допомогою небезпечного FTP

#клієнта командного рядка, як це робили раніше за прикладом цієї статті. Якщо ви

#спробуєте підключитися, отримайте таке повідомлення про помилку:

#Тепер, коли ми дозволили цим двом користувачам отримати доступ до нашого FTP-сервера

#(і закрили його для всіх інших), останнє, що нам потрібно зробити, це налаштувати їхні

#домашні папки.

#Для цього створіть папку /etc/vsftpd/user\_config\_dir/ і створюємо файли з однаковими

#іменами користувачів:

sudo mkdir /etc/user\_config\_dir/

sudo touch /etc/user\_config\_dir/alpha

sudo touch /etc/user\_config\_dir/beta

sudo touch /etc/user\_config\_dir/gamma

sudo touch /etc/user\_config\_dir/delta

sudo touch /etc/user\_config\_dir/omega

sudo touch /etc/user\_config\_dir/anonymous

#Відразу після цього відредагуйте файлb таким чином:

#alpha

sudo nano /etc/user\_config\_dir/alpha

local\_root=/home

write\_enable=YES

#beta

sudo nano /etc/user\_config\_dir/beta

local\_root=/home/beta/www

write\_enable=NO

#gamma

sudo nano /etc/user\_config\_dir/gamma

local\_root=/home/gamma/www

write\_enable=YES

#delta

sudo nano /etc/user\_config\_dir/delta

local\_root=/home

write\_enable=YES

#omega

sudo nano /etc/user\_config\_dir/omega

local\_root=/home/gamma/www

write\_enable=YES

#anonymous

sudo nano /etc/user\_config\_dir/anonymous

local\_root=/home/anonymous

write\_enable=YES

sudo nano /etc/vsftpd.conf

# Setup the virtual users config folder

user\_config\_dir=/etc/user\_config\_dir/

sudo systemctl restart vsftpd

#Наведені вище параметри зрозумілі самі за себе: ми, по суті, кажемо VSFTP дозволити

#доступ до FTP лише локальним користувачам, яких ми розмістимо у файлі user\_list, отримавши

# їхню конфігурацію з папки /user\_config\_dir/

force\_local\_logins\_ssl=NO

force\_local\_data\_ssl=NO

Після всіх змін конфігураційний файл буде мати наступний вигляд:

# Example config file /etc/vsftpd.conf

#

# The default compiled in settings are fairly paranoid. This sample file

# loosens things up a bit, to make the ftp daemon more usable.

# Please see vsftpd.conf.5 for all compiled in defaults.

#

# READ THIS: This example file is NOT an exhaustive list of vsftpd options.

# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's

# capabilities.

#

#

# Run standalone? vsftpd can run either from an inetd or as a standalone

# daemon started from an initscript.

listen=NO

#

# This directive enables listening on IPv6 sockets. By default, listening

# on the IPv6 "any" address (::) will accept connections from both IPv6

# and IPv4 clients. It is not necessary to listen on \*both\* IPv4 and IPv6

# sockets. If you want that (perhaps because you want to listen on specific

# addresses) then you must run two copies of vsftpd with two configuration

# files.

listen\_ipv6=YES

#

# Allow anonymous FTP? (Disabled by default).

anonymous\_enable=YES

#

# Uncomment this to allow local users to log in.

local\_enable=YES

#

# Uncomment this to enable any form of FTP write command.

#write\_enable=YES

#

# Default umask for local users is 077. You may wish to change this to 022,

# if your users expect that (022 is used by most other ftpd's)

#local\_umask=022

#

# Uncomment this to allow the anonymous FTP user to upload files. This only

# has an effect if the above global write enable is activated. Also, you will

# obviously need to create a directory writable by the FTP user.

#anon\_upload\_enable=YES

#

# Uncomment this if you want the anonymous FTP user to be able to create

# new directories.

#anon\_mkdir\_write\_enable=YES

#

# Activate directory messages - messages given to remote users when they

# go into a certain directory.

dirmessage\_enable=YES

#

# If enabled, vsftpd will display directory listings with the time

# in your local time zone. The default is to display GMT. The

# times returned by the MDTM FTP command are also affected by this

# option.

use\_localtime=YES

#

# Activate logging of uploads/downloads.

xferlog\_enable=YES

#

# Make sure PORT transfer connections originate from port 20 (ftp-data).

connect\_from\_port\_20=YES

#

# If you want, you can arrange for uploaded anonymous files to be owned by

# a different user. Note! Using "root" for uploaded files is not

# recommended!

#chown\_uploads=YES

#chown\_username=whoever

#

# You may override where the log file goes if you like. The default is shown

# below.

#xferlog\_file=/var/log/vsftpd.log

#

# If you want, you can have your log file in standard ftpd xferlog format.

# Note that the default log file location is /var/log/xferlog in this case.

#xferlog\_std\_format=YES

#

# You may change the default value for timing out an idle session.

#idle\_session\_timeout=600

#

# You may change the default value for timing out a data connection.

#data\_connection\_timeout=120

#

# It is recommended that you define on your system a unique user which the

# ftp server can use as a totally isolated and unprivileged user.

#nopriv\_user=ftpsecure

#

# Enable this and the server will recognise asynchronous ABOR requests. Not

# recommended for security (the code is non-trivial). Not enabling it,

# however, may confuse older FTP clients.

#async\_abor\_enable=YES

#

# By default the server will pretend to allow ASCII mode but in fact ignore

# the request. Turn on the below options to have the server actually do ASCII

# mangling on files when in ASCII mode.

# Beware that on some FTP servers, ASCII support allows a denial of service

# attack (DoS) via the command "SIZE /big/file" in ASCII mode. vsftpd

# predicted this attack and has always been safe, reporting the size of the

# raw file.

# ASCII mangling is a horrible feature of the protocol.

#ascii\_upload\_enable=YES

#ascii\_download\_enable=YES

#

# You may fully customise the login banner string:

#ftpd\_banner=Welcome to blah FTP service.

#

# You may specify a file of disallowed anonymous e-mail addresses. Apparently

# useful for combatting certain DoS attacks.

#deny\_email\_enable=YES

# (default follows)

#banned\_email\_file=/etc/vsftpd.banned\_emails

#

# You may restrict local users to their home directories. See the FAQ for

# the possible risks in this before using chroot\_local\_user or

# chroot\_list\_enable below.

#chroot\_local\_user=YES

#

# You may specify an explicit list of local users to chroot() to their home

# directory. If chroot\_local\_user is YES, then this list becomes a list of

# users to NOT chroot().

# (Warning! chroot'ing can be very dangerous. If using chroot, make sure that

# the user does not have write access to the top level directory within the

# chroot)

#chroot\_local\_user=YES

#chroot\_list\_enable=YES

# (default follows)

#chroot\_list\_file=/etc/vsftpd.chroot\_list

#

# You may activate the "-R" option to the builtin ls. This is disabled by

# default to avoid remote users being able to cause excessive I/O on large

# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume

# the presence of the "-R" option, so there is a strong case for enabling it.

#ls\_recurse\_enable=YES

#

# Customization

#

# Some of vsftpd's settings don't fit the filesystem layout by

# default.

#

# This option should be the name of a directory which is empty. Also, the

# directory should not be writable by the ftp user. This directory is used

# as a secure chroot() jail at times vsftpd does not require filesystem

# access.

secure\_chroot\_dir=/var/run/vsftpd/empty

#

# This string is the name of the PAM service vsftpd will use.

pam\_service\_name=vsftpd

#

# This option specifies the location of the RSA certificate to use for SSL

# encrypted connections.

#rsa\_cert\_file=/etc/ssl/certs/ssl-cert-snakeoil.pem

#rsa\_private\_key\_file=/etc/ssl/private/ssl-cert-snakeoil.key

rsa\_cert\_file=/etc/ssl/private/vsftpd.pem

rsa\_private\_key\_file=/etc/ssl/private/vsftpd.pem

ssl\_enable=YES

#

# Uncomment this to indicate that vsftpd use a utf8 filesystem.

#utf8\_filesystem=YES

user\_sub\_token=$USER

local\_root=/home/$USER/ftp

pasv\_min\_port=40000

pasv\_max\_port=50000

userlist\_enable=YES

userlist\_file=/etc/vsftpd.userlist

userlist\_deny=NO

user\_config\_dir=/etc/user\_config\_dir/

allow\_anon\_ssl=YES

force\_local\_data\_ssl=NO

force\_local\_logins\_ssl=NO

ssl\_tlsv1=YES

ssl\_sslv2=NO

ssl\_sslv3=NO

require\_ssl\_reuse=NO

ssl\_ciphers=HIGH

2.3. Виконати аналіз протокольного обміну між клієнтом та сервером під час автентифікації та пересилки файлів.

Робимо перевірку роботи нашого серверу, для початку юзера anonymous користуючись утилітою FTP

ftp 172.20.1.80

Connected to 172.20.1.80.

220 (vsFTPd 3.0.3)

Name (172.20.1.80:chygyk): anonymous

230 Login successful.

Remote system type is UNIX.

Using binary mode to transfer files.

Відповідно до завдання в домашній директорії маємо ще дві з різними правами, incoming з правами читання і запису, pub тільки з правами читання

ftp> ls

229 Entering Extended Passive Mode (|||40707|)

150 Here comes the directory listing.

drwxrwxrwx 3 0 0 4096 Jun 25 00:57 incoming

dr-xr-xr-x 2 0 0 4096 Jun 25 00:59 pub

ftp> ls

229 Entering Extended Passive Mode (|||41171|)

150 Here comes the directory listing.

drwx------ 2 111 116 4096 Jun 25 01:00 New directory

226 Directory send OK.

ftp> mkdir test

257 "/incoming/test" created

ftp> get test.txt

local: test.txt remote: test.txt

229 Entering Extended Passive Mode (|||47734|)

150 Opening BINARY mode data connection for test.txt (9 bytes).

100% |\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*| 9 258.50 KiB/s 00:00 ETA

226 Transfer complete.

9 bytes received in 00:00 (23.68 KiB/s)

ftp> mkdir test

550 Create directory operation failed.

ftp>

як бачимо з логу вссе працює вірно.

Далі перевіримо роботу протоколу SFTP:

sftp alpha@172.20.1.80

Connected to 172.20.1.80.

sftp> ls

www

sftp> cd www

sftp> ls

New directory

sftp>

протокол працює вірно, для деяких юзерів він має бути вимкнений

sftp omega@172.20.1.80

omega@172.20.1.80: Permission denied (publickey).

Connection closed.

Connection closed

все працює вірно.

Перевіряємо FTPS, як бачимо при запиті на сервер клієнт запитує чи є цей сертифікат довіреним

Щоб перевірити безпечне з’єднання з FTP-сервером, потрібно буде скористатися деякими додатковими параметрами, оскільки сьогодні більшість FTP-серверів використовують явний TLS.Це означає, що початкове підключення до сервера не є захищеним, і рукостискання TLS відбувається лише після того, як клієнт видає команду.

openssl s\_client -tls1\_2 -crlf -connect 172.20.1.80:21 -starttls ftp

Параметр -starttls smtp повідомляє OpenSSL, що ви хочете підключитися як клієнт FTP за допомогою явного TLS.Якщо потрібно перевірити підключення до FTP-сервера за допомогою неявного TLS на порту 990, просто виключіть параметр -starttls ftp з команди.

CONNECTED(00000003)

Can't use SSL\_get\_servername

depth=0 C = UA, ST = Ukraine, L = Kyiv, O = KPI, OU = OT, CN = letter CA, emailAddress = ftp.letter.net

verify error:num=18:self-signed certificate

verify return:1

depth=0 C = UA, ST = Ukraine, L = Kyiv, O = KPI, OU = OT, CN = letter CA, emailAddress = ftp.letter.net

verify return:1

---

Certificate chain

0 s:C = UA, ST = Ukraine, L = Kyiv, O = KPI, OU = OT, CN = letter CA, emailAddress = ftp.letter.net

i:C = UA, ST = Ukraine, L = Kyiv, O = KPI, OU = OT, CN = letter CA, emailAddress = ftp.letter.net

a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256

v:NotBefore: Jun 25 10:34:13 2023 GMT; NotAfter: Jun 24 10:34:13 2024 GMT

---

Server certificate

-----BEGIN CERTIFICATE-----

MIID2TCCAsGgAwIBAgIUCMNg/ihb0SJJz/cx+r8iMPFP0VswDQYJKoZIhvcNAQEL

BQAwfDELMAkGA1UEBhMCVUExEDAOBgNVBAgMB1VrcmFpbmUxDTALBgNVBAcMBEt5

aXYxDDAKBgNVBAoMA0tQSTELMAkGA1UECwwCT1QxEjAQBgNVBAMMCWxldHRlciBD

QTEdMBsGCSqGSIb3DQEJARYOZnRwLmxldHRlci5uZXQwHhcNMjMwNjI1MTAzNDEz

WhcNMjQwNjI0MTAzNDEzWjB8MQswCQYDVQQGEwJVQTEQMA4GA1UECAwHVWtyYWlu

ZTENMAsGA1UEBwwES3lpdjEMMAoGA1UECgwDS1BJMQswCQYDVQQLDAJPVDESMBAG

A1UEAwwJbGV0dGVyIENBMR0wGwYJKoZIhvcNAQkBFg5mdHAubGV0dGVyLm5ldDCC

ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMGkT9eBvKepCm4Om5Rj/deo

QKOGgIAmqvworcTy9xExVT3Dlxi2YqPWDubCq7ytbdhxjEugqOuepx4ppWSmaUWT

R6m3c4tmSG7WSnPUxmfP4MPtqXMGU+8qJwMSp2r/A8nKtNIL3toYW7Zn7X9emUYL

fK+VuLlfgFWJ0afE23VrTBCI9CD2Dcz6OQXWxMlMAYWJzw9ZqIyXMuRRD/EdxIdh

oahJ8Sh9v1QFNlNCjyaZY5kAJXZiYwqXunUfvfAnayGv4qySb+H+mzZswM4Gu9QP

rSXpt0cp6wi5l30/3duxpGTPLrjFoknL5Tf898dRIPkgZhRrdCktTJ7qsCbQHfMC

AwEAAaNTMFEwHQYDVR0OBBYEFLoDYT/wi6vROZ63aH4FlYIHzXSpMB8GA1UdIwQY

MBaAFLoDYT/wi6vROZ63aH4FlYIHzXSpMA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZI

hvcNAQELBQADggEBACVqbyujiSVK2nt12VxaqB/0okUUvviiFtkZwml3ROOc0LHD

GF0V7n88TwIzjTmy6mq3BTW8IMpbGl68OnYMFrvaS1QvCqsqcWL8OKm67A3Vcs2F

h8UNHWivzZRntObQd3wBfTRwV7OFWfP7EiwKZzC4IAfqIJm7OJd4PyJd8Dv4meF4

kb5oDkpL4X02b5y24PpboNOLzTF6T1maOepBCHwHHt4U38Q9h5UUKsoD3Vv81jeK

3xuaS2uoRKp33kBlQSTLnCZlT451FQj7YZSVfE5nzPs7uakjhLncu/NS/MGKXCEG

cXV/GsgFhAG6py10UwJItc7HO51JVGHUjILla9Q=

-----END CERTIFICATE-----

subject=C = UA, ST = Ukraine, L = Kyiv, O = KPI, OU = OT, CN = letter CA, emailAddress = ftp.letter.net

issuer=C = UA, ST = Ukraine, L = Kyiv, O = KPI, OU = OT, CN = letter CA, emailAddress = ftp.letter.net

---

No client certificate CA names sent

Client Certificate Types: RSA sign, DSA sign, ECDSA sign

Requested Signature Algorithms: ECDSA+SHA256:ECDSA+SHA384:ECDSA+SHA512:Ed25519:Ed448:RSA-PSS+SHA256:RSA-PSS+SHA384:RSA-PSS+SHA512:RSA-PSS+SHA256:RSA-PSS+SHA384:RSA-PSS+SHA512:RSA+SHA256:RSA+SHA384:RSA+SHA512:ECDSA+SHA224:ECDSA+SHA1:RSA+SHA224:RSA+SHA1:DSA+SHA224:DSA+SHA1:DSA+SHA256:DSA+SHA384:DSA+SHA512

Shared Requested Signature Algorithms: ECDSA+SHA256:ECDSA+SHA384:ECDSA+SHA512:Ed25519:Ed448:RSA-PSS+SHA256:RSA-PSS+SHA384:RSA-PSS+SHA512:RSA-PSS+SHA256:RSA-PSS+SHA384:RSA-PSS+SHA512:RSA+SHA256:RSA+SHA384:RSA+SHA512:ECDSA+SHA224:RSA+SHA224:DSA+SHA224:DSA+SHA256:DSA+SHA384:DSA+SHA512

Peer signing digest: SHA256

Peer signature type: RSA-PSS

Server Temp Key: ECDH, prime256v1, 256 bits

---

SSL handshake has read 1761 bytes and written 336 bytes

Verification error: self-signed certificate

---

New, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384

Server public key is 2048 bit

Secure Renegotiation IS supported

Compression: NONE

Expansion: NONE

No ALPN negotiated

SSL-Session:

Protocol : TLSv1.2

Cipher : ECDHE-RSA-AES256-GCM-SHA384

Session-ID: 09682A5D88D9061822BA26A83090B494ED7C7BA7A7C50558DBBFAE9C26FBB783

Session-ID-ctx:

Master-Key: CF641C5FF3C67990A454E21FD5132FD5F0C352FDDC688DBFDD08810B4C4F1982FB4CA4FEE366C82C84D680EC3AEEAC7F

PSK identity: None

PSK identity hint: None

SRP username: None

TLS session ticket lifetime hint: 7200 (seconds)

TLS session ticket:

0000 - 3e 30 56 97 d2 ca 09 fc-06 e1 de f6 a7 05 10 a5 >0V.............

0010 - d4 ce ba 1b 9c fe dd c3-b8 85 78 0e a6 5d b4 9d ..........x..]..

0020 - 6a 47 ef 9a 6b 3f 69 5b-e5 88 30 b8 c9 35 fc eb jG..k?i[..0..5..

0030 - 33 d0 c6 d9 38 87 82 2b-8f d8 ce 63 48 31 8b 23 3...8..+...cH1.#

0040 - 2f b6 24 4b 13 4d 43 0a-4f 56 03 3e 67 d0 d4 72 /.$K.MC.OV.>g..r

0050 - ee 27 56 f3 a5 c6 fa 37-12 14 23 aa cd 61 18 09 .'V....7..#..a..

0060 - 19 16 d1 82 7a 75 04 c1-96 6e f5 c5 9a 89 7e a6 ....zu...n....~.

0070 - d5 37 79 ce 27 d8 63 7a-75 29 cd b2 48 9c 34 03 .7y.'.czu)..H.4.

0080 - d3 fc fc cf c2 d1 49 6b-a7 7a cd e9 e8 99 67 07 ......Ik.z....g.

0090 - a5 48 53 92 96 07 2c 5e-cf dd d4 bf e2 dd f7 20 .HS...,^.......

Start Time: 1687695567

Timeout : 7200 (sec)

Verify return code: 18 (self-signed certificate)

Extended master secret: yes

---

220 (vsFTPd 3.0.3)

40F703C3447F0000:error:0A00010B:SSL routines:ssl3\_get\_record:wrong version number:../ssl/record/ssl3\_record.c:331: