	Państwowa Wyższa Szkoła Zawodowa w Nysie			Wydział Nauk Technicznych	
	Laboratorium Podstaw Systemów Komputerowych				
Kierunek:	Informatyka	Rok studiów nr:	1	Semestr nr:	2
Rok akademicki:	2020/2021	Grupa administracyjna:	L5	Grupa ćwiczeniowa:	L5g1

SPRAWOZDANIE

Nr ćwiczenia	Temat ćwiczenia
7a	Przykłady usług sieciowych i monitorowania s.o. Linux. Część I
Termin złożenia sprawozdania	
Termin wg listy	
Data faktycznego złożenia sprawoz-dania	
(nie wypełniaj)	

Wykonawcy	Nazwisko	Imię	Nr indeksu	Ocena
	Roszak	Damian		(Nie wypełniane w trybie online)
				(Nie wypełniane w trybie online)

Uwaga: Umieszczenie danych osobowych wykonawców stanowi grupowe i nieodwołalne oświadczenie, że są oni/one (i tylko oni/one) współautorami przedstawionego sprawozdania. Późniejsza zmiana składu zespołu wykonawców nie będzie możliwa.

Nie wypełniać przy składaniu online

Data i podpis prowadzącego ćwiczenia

Wymagania typograficzne

- Tekst główny (w ramkach) należy składać czcionką normalną typu Times 12 pkt.
- Zawartość plików, nazwy ścieżek w systemie plików, polecenia wydawane z konsoli i uzyskiwane odpowiedzi systemu/aplikacji oraz kopie tabulogramów interakcji z powłoką należy składać czcionką normalną typu **`Courier 11 pkt`**. Należy zachować wygląd, w tym pozycjonowanie tekstu.
- Nazwy pozycji menu w programach i nazwy przycisków ekranowych należy składać czcionką pogrubioną typu **Arial 11 pkt**.
- Wykluczone jest zamieszczanie ilustracji graficznych z ciemnym tłem. Tekst powinien z tłem wyraźnie kontrastować.

1. Temat ćwiczenia

(kopia tematu instrukcji, identyczna jak tytuł sprawozdania)

Przykłady usług sieciowych i monitorowania s.o. Linux. Część I

2. Zakres ćwiczenia

Streszczenie treści ćwiczenia oraz ustalenia prowadzącego zajęcia dotyczące wyboru funkcji badanego programu, zastosowanego algorytmu, zbioru przetwarzanych danych, precyzji przedstawienia liczb, liczby wątków i cykli obliczeń, sposobu prezentacji wyników, itp.)

Celem ćwiczenia jest zapoznanie się z podstawowymi usługami systemu Linux oraz możliwościami śledzenia obciążenia systemu. Niektóre z zadań tego ćwiczenia wymagają wykorzystania uprawnień root'a

3. Środowisko realizacji ćwiczenia

(architektura logiczna systemu – sprzęt, elementy składowe, ich cechy i sposób wzajemnego połączenia, schematy; wykorzystywane języki, oprogramowanie, biblioteki, skrypty powłokowe, zasoby sieciowe i dokumentacja)

CentOS Linux 7.5-2G jako maszyna wirtualna stworzona z pomocą oprogramowania wirtualizującego VMware Worksatrion 16 Player uruchomioną w środowisku Windows 10.

4. Przebieg ćwiczenia i uzyskane wyniki

(przedstawienie czynności wykonanych w ramach realizacji ćwiczenia, w kolejności określonej treścią instrukcji.
Dla każdego punktu instrukcji należy przedstawić: nr i tytuł tego punktu, cel działania, sposób wykonania, otrzymany rezultat i jego ocenę). Wymagana jest 100% chronologia zadań, czynności i uzyskanych rezultatów.

4.1 Zadanie nr 1

4.1.1 Nr i treść polecenia wg instrukcji: 2.1.a) Zapoznaj się z usługą sieciową FTP i zredaguj krótki opis funkcjonalny.

4.1.2 Cel czynności: Zapoznanie się z usługą sieciową FTP i zredagowanie krótkiego opisu.

4.1.3 Sposób i rezultat wykonania polecenia (np. polecenia wydane na konsoli i odpowiedź systemu/aplikacji, w postaci wycinka zarejestrowanego logu konwersacji terminalowej w formacie tekstowym). Dopuszcza się zamieszczenie fragmentu zrzutu ekranowego. W każdym przypadku obraz rezultatu ma obejmować wykonania wyłącznie danego punktu (a nie wszystko, co widać w oknie terminala lub konsoli). Log konwersacji musi zawierać następujące bezpośrednio po niej zaproszenie (tzw. *prompt*) powłoki.

Protokół transferu plików, FTP (od ang. File Transfer Protocol) – protokół komunikacyjny typu klient-serwer wykorzystujący protokół sterowania transmisją (TCP) według modelu TCP/IP, umożliwiający dwukierunkowy transfer plików w układzie serwer FTP–klient FTP.

FTP jest protokołem 8-bitowym i dlatego nie wymaga kodowania danych do 7 bitów, tak jak w przypadku poczty elektronicznej.

Do komunikacji wykorzystywane są dwa połączenia TCP. Jedno z nich jest połączeniem sterującym, za pomocą którego przesyłane są polecenia, a drugie służy do transmisji danych. Połączenie za pomocą protokołu FTP może działać w dwóch trybach: aktywnym i pasywnym:

- jeżeli połączenie FTP działa w trybie aktywnym, używa portu 21 dla poleceń (zestawiane przez klienta) i portu 20 do przesyłu danych (zestawiane przez serwer)
- jeżeli połączenie FTP pracuje w trybie pasywnym, używa portu 21 dla poleceń i portu o numerze powyżej 1024 do transmisji danych (obydwa połączenia zestawiane są przez klienta).

W sieciach chronionych zaporą sieciową komunikacja z serwerami FTP wymaga zwolnienia odpowiednich portów na tej zaporze lub routerze. Możliwe jest zainstalowanie wielu serwerów FTP na jednym routerze. Warunkiem jest rozdzielenie portów przez router dla każdego serwera.

Serwer FTP, zależnie od konfiguracji, może pozwalać na anonimowy, czyli bez podawania hasła uwierzytelniającego, dostęp do jego zasobów. Najczęściej jednak serwer FTP autoryzuje każde połączenie za pomocą loginu i hasła.

4.1.4 Ocena/wnioski/komentarze dotyczące wykonania danego zadania.

4.2 Zadanie nr 2

4.2.1 Nr i treść polecenia wg instrukcji: 2.1. b) Wykonaj tabelaryczne zestawienie 15-20 ważniejszych poleceń protokołu FTP (nazwa polecenia, opis funkcji, zastosowanie lokalne/zdalne)

4.2.2 Cel czynności: Tabelaryczne zestawienie 15-20 ważniejszych poleceń protokołu FTP.

4.2.3 Sposób i rezultat wykonania polecenia (np. polecenia wydane na konsoli i odpowiedź systemu/aplikacji, w postaci wycinka zarejestrowanego logu konwersacji terminalowej w formacie tekstowym). Dopuszcza się zamieszczenie fragmentu zrzutu ekranowego. W każdym przypadku obraz rezultatu ma obejmować wykonania wyłącznie danego punktu (a nie wszystko, co widać w oknie terminala lub konsoli). Log konwersacji musi zawierać następujące bezpośrednio po niej zaproszenie (tzw. *prompt*) powłoki.

Nazwa polecenia	`GET`
Opis funkcji	Polecenie pozwala pobrać plik z katalogu roboczego, wiele klientów pozwala w ramach egzekucji tego polecenia na zmianę nazwy pliku w miejscu docelowym.
Zastosowanie lokalne/zdalne	lokalne

Nazwa polecenia	`AUTH`
Opis funkcji	Autentykacja - uwierzytelnienie podaniem loginu i hasła
Zastosowanie lokalne/zdalne	zdalne

Nazwa polecenia	`CHMOD`
Opis funkcji	Zmiana uprawnień do zasobów.
Zastosowanie lokalne/zdalne	zdalne

Nazwa polecenia	`DELE`
Opis funkcji	Usuń plik. Parametr polecenia to nazwa ścieżki pliku. Akceptacja `DELE` wiąże się z odpowiedzią 250, gdy plik zostanie usunięty, oraz kodami 450 lub 550, gdy usuwanie nie powiedzie się
Zastosowanie lokalne/zdalne	zdalne

Nazwa polecenia	`FEAT`
Opis funkcji	Listuje wszystkie komendy wspierane przez dany serwer (ang. FEATure, umiejętność). Nie posiada argumentów ani parametrów.
Zastosowanie lokalne/zdalne	zdalne

Nazwa polecenia	`HELP`

Opis funkcji	Zwraca informacje o sposobie działania danej komendy, w innym przypadku zwraca ogólne informacje pomocy.
Zastosowanie lokalne/zdalne	zdalne

Nazwa polecenia	`HOST`
Opis funkcji	Identyfikuje pożądany wirtualny host na serwerze poprzez jego nazwę.
Zastosowanie lokalne/zdalne	zdalne

Nazwa polecenia	`LANG`
Opis funkcji	Ustawienie języka.
Zastosowanie lokalne/zdalne	zdalne

Nazwa polecenia	`LIST`
Opis funkcji	Zwraca informacje o pliku lub ścieżce jeśli są wyspecyfikowane, w innym przypadku zwraca informacje o aktualnie używanym katalogu.
Zastosowanie lokalne/zdalne	zdalne

Nazwa polecenia	`MODE`
Opis funkcji	Ustawia tryb transferu (Stream, Block, or Compressed). Obecnie nieużywany, serwer przyjmie „`MODE S`” / „`MODE s`” i zwróci kod 200, w innych przypadkach zwróci kod 504.
Zastosowanie lokalne/zdalne	zdalne

Nazwa polecenia	`PASV`
Opis funkcji	Wejście w tryb pasywny.
Zastosowanie lokalne/zdalne	zdalne

Nazwa polecenia	`PASS`
Opis funkcji	Autentykacja hasła. Klient FTP nie powinien wysyłać PASS (hasła), przed wysłaniem polecenia `USER`. Serwer akceptuje `PASS` kodem 230 co znaczy, że dostęp został udzielony, lub kodem 202, co znaczy, że dostęp został nadany od razu w odpowiedzi na polecenie `USER`, ale również z kodem 332, co oznacza, że dostęp zostanie przyznany po wysłaniu zapytania `ACCT`. Serwer może zwrócić kod 503 w sytuacji, gdy uprzednio nie wysłano polecenia `USER`, albo gdy nazwa użytkownika i hasło nie są poprawne
Zastosowanie lokalne/zdalne	zdalne

Nazwa polecenia	`OPEN`
Opis funkcji	Polecenie, którego parametrem jest adres serwera FTP.
Zastosowanie lokalne/zdalne	zdalne

Nazwa polecenia	PWD
Opis funkcji	Zwraca katalog hosta. Jeśli zaakceptuje to kod odpowiedzi powinien wynieść 257 oraz ścieżka katalogu np. „/home/joe”. W razie odrzucenia kod odpowiedzi to 550. Polecenie zamienne z XPWD.
Zastosowanie lokalne/zdalne	zdalne

Nazwa polecenia	PUT
Opis funkcji	Polecenie załadowania pliku z wybranej lokalizacji do katalogu roboczego na serwerze FTP. Parametrem jest nazwa ścieżki do pliku. Porównaj z poleceniem MPUT.
Zastosowanie lokalne/zdalne	oba

Nazwa polecenia	REST
Opis funkcji	Restartuj transfer od podanego miejsca.
Zastosowanie lokalne/zdalne	zdalne

Nazwa polecenia	RMD
Opis funkcji	Usuń ścieżkę / katalog. Parametrem polecenia jest nazwa ścieżki katalogu. W przypadku usunięcia kod zwracany przez serwer to 250, a odrzucenie polecenia wiąże się z kodem 550. Stosowane wymiennie z XRMD.
Zastosowanie lokalne/zdalne	zdalne

4.2.4 Ocena/wnioski/komentarze dotyczące wykonania danego zadania.

4.3 Zadanie nr 3

4.3.1 Nr i treść polecenia wg instrukcji: 2.1. c) Sprawdź, czy serwer FTP jest zainstalowany i uruchomiony w Twojej maszynie wirtualnej. Jeśli nie, to zainstaluj i uruchom go.

4.3.2 Cel czynności: Posiadanie i uruchomienie serwera FTP.

4.3.3 Sposób i rezultat wykonania polecenia (np. polecenia wydane na konsoli i odpowiedź systemu/aplikacji, w postaci wycinka zarejestrowanego logu konwersacji terminalowej w formacie tekstowym). Dopuszcza się zamieszczenie fragmentu zrzutu ekranowego. W każdym przypadku obraz rezultatu ma obejmować wykonania wyłącznie danego punktu (a nie wszystko, co widać w oknie terminala lub konsoli). Log konwersacji musi zawierać następujące bezpośrednio po niej zaproszenie (tzw. *prompt*) powłoki.

Sprawdzam czy serwer `vsftpd` jest zainstalowany wpisując polecenie `vsftpd`. Okazało się, że nie, więc go zainstalowałem.

```
[szarik102@centos75 ~]$ yum install vsftpd
-bash: vsftpd: nie znaleziono polecenia
[szarik102@centos75 ~]$
[szarik102@centos75 ~]$ yum install vsftpd
Wczytane wtyczki: fastestmirror
Należy być zalogowanym jako root, aby wykonać to polecenie.
[szarik102@centos75 ~]$ sudo su -
```

```
[sudo] hasło użytkownika szarik102:
Ostatnie logowanie: pią maj 28 10:35:39 CEST 2021 na tty1
[root@centos75 ~]# yum install vsftpd
Wczytane wtyczki: fastestmirror
Loading mirror speeds from cached hostfile
epel/x86_64/metalink                                     |  28 kB     00:00
 * base: centos.slaskdatacenter.com
 * epel: ftp-stud.hs-esslingen.de
 * extras: centos.slaskdatacenter.com
 * updates: centos.slaskdatacenter.com
base                                                     | 3.6 kB     00:00
epel                                                     | 4.7 kB     00:00
extras                                                   | 2.9 kB     00:00
updates                                                  | 2.9 kB     00:00
(1/2): epel/x86_64/updateinfo                              | 1.0 MB   00:02
(2/2): epel/x86_64/primary_db                              | 6.9 MB   00:09
(2/2): epel/x86_64/primary 0% [                ]  0.0 B/s |    0 B   --:-- ETA

(2/2): epel/x86_64/primary 1% [                ]  0.0 B/s | 148 kB   --:-- ETA

(2/2): epel/x86_64/primary 5% [-               ] 471 kB/s | 448 kB   00:16 ETA

(2/2): epel/x86_64/primary 16% [==-            ] 625 kB/s | 1.3 MB   00:10 ETA

(1/2): epel/x86_64/updateinfo                              | 1.0 MB   00:02

(2/2): epel/x86_64/primary 21% [===            ] 655 kB/s | 1.7 MB   00:09 ETA

(2/2): epel/x86_64/primary 22% [===-           ] 629 kB/s | 1.8 MB   00:10 ETA

(2/2): epel/x86_64/primary 25% [====           ] 649 kB/s | 2.1 MB   00:09 ETA

(2/2): epel/x86_64/primary 31% [====-          ] 692 kB/s | 2.5 MB   00:08 ETA

(2/2): epel/x86_64/primary 35% [=====-         ] 719 kB/s | 2.8 MB   00:07 ETA

(2/2): epel/x86_64/primary 40% [======         ] 757 kB/s | 3.2 MB   00:06 ETA

(2/2): epel/x86_64/primary 45% [=======        ] 783 kB/s | 3.6 MB   00:05 ETA

(2/2): epel/x86_64/primary 49% [=======-       ] 799 kB/s | 3.9 MB   00:05 ETA

(2/2): epel/x86_64/primary 51% [========       ] 794 kB/s | 4.1 MB   00:04 ETA

(2/2): epel/x86_64/primary 55% [========-      ] 806 kB/s | 4.4 MB   00:04 ETA

(2/2): epel/x86_64/primary 60% [=========-     ] 831 kB/s | 4.8 MB   00:03 ETA

(2/2): epel/x86_64/primary 64% [==========     ] 841 kB/s | 5.1 MB   00:03 ETA

(2/2): epel/x86_64/primary 68% [==========-    ] 854 kB/s | 5.4 MB   00:03 ETA

(2/2): epel/x86_64/primary 71% [===========    ] 857 kB/s | 5.7 MB   00:02 ETA

(2/2): epel/x86_64/primary 74% [===========-   ] 848 kB/s | 5.9 MB   00:02 ETA

(2/2): epel/x86_64/primary 79% [============-  ] 874 kB/s | 6.3 MB   00:01 ETA
```

```
(2/2): epel/x86_64/primary 81% [=============   ] 848 kB/s | 6.5 MB   00:01 ETA

(2/2): epel/x86_64/primary 85% [=============-  ] 857 kB/s | 6.8 MB   00:01 ETA

(2/2): epel/x86_64/primary 90% [==============  ] 884 kB/s | 7.2 MB   00:00 ETA

(2/2): epel/x86_64/primary 95% [============== ] 907 kB/s | 7.6 MB   00:00 ETA

(2/2): epel/x86_64/primary_db                                | 6.9 MB   00:09
Rozwiązywanie zależności
--> Wykonywanie sprawdzania transakcji
---> Pakiet vsftpd.x86_64 0:3.0.2-28.el7 zostanie zainstalowany
--> Ukończono rozwiązywanie zależności

Rozwiązano zależności

================================================================================
 Package          Architektura     Wersja                  Repozytorium   Rozmiar
================================================================================
Instalowanie:
 vsftpd           x86_64           3.0.2-28.el7            base           172 k

Podsumowanie transakcji
================================================================================
Instalacja  1 Pakiet

Całkowity rozmiar pobierania: 172 k
Rozmiar po zainstalowaniu: 353 k
Is this ok [y/d/N]: y
Downloading packages:
vsftpd-3.0.2-28.el7.x86_64.rpm                               | 172 kB   00:01
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Instalowanie             : vsftpd-3.0.2-28.el7.x86_64                    1/1
  Sprawdzanie              : vsftpd-3.0.2-28.el7.x86_64                    1/1

Zainstalowano:
  vsftpd.x86_64 0:3.0.2-28.el7

Ukończono.
[root@centos75 ~]#
```

Następnie przystąpiłem do uruchomienia.:

```
[root@centos75 ~]# systemctl start vsftpd
[root@centos75 ~]# systemctl enable vsftpd
[root@centos75 ~]#
```

4.3.4 Ocena/wnioski/komentarze dotyczące wykonania danego zadania.

4.4 Zadanie nr 4

4.4.1 Nr i treść polecenia wg instrukcji: 2.1. d) Zapoznaj się z plikiem konfiguracyjnym usługi FTP `/etc/vsftpd/conf` i opisz najważniejsze – Twoim zdaniem – ustawienia

4.4.2 Cel czynności: Zrozumienie pliku konfiguracyjnego usługi FTP `/etc/vsftpd/conf`

4.4.3 Sposób i rezultat wykonania polecenia (np. polecenia wydane na konsoli i odpowiedź systemu/aplikacji, w postaci wycinka zarejestrowanego logu konwersacji terminalowej w formacie tekstowym). Dopuszcza się zamieszczenie fragmentu zrzutu ekranowego. W każdym przypadku obraz rezultatu ma obejmować wykonania wyłącznie danego punktu (a nie wszystko, co widać w oknie terminala lub konsoli). Log konwersacji musi zawierać następujące bezpośrednio po niej zaproszenie (tzw. *prompt*) powłoki.

Zaczynam od otwarcia pliku konfiguracyjnego `vsftpd`:

```
[root@centos75 ~]# nano /etc/vsftpd/vsftpd.conf
```

1. Dostęp FTP
Umożliwienie dostępu do serwera FTP tylko lokalnym użytkownikom: dyrektywy `anonymous_enable` i `local_enable`:

```
/etc/vsftpd/vsftpd.conf
anonymous_enable=NO local_enable=YES
```

2. Włączanie przesyłania
`write_enable` ustawienie umożliwia zmiany w systemie plików, takie jak przesyłanie i usuwanie plików.

```
/etc/vsftpd/vsftpd.conf
write_enable=YES
```

3. Chroot
Zapobieganie użytkownikom FTP uzyskiwania dostępu do plików spoza ich katalogów domowych poprzez odkomentowanie dyrektywy `chroot` .

```
/etc/vsftpd/vsftpd.conf
chroot_local_user=YES
```

Domyślnie, gdy `chroot` jest włączony, `vsftpd` odmawia przesyłania plików, jeśli katalog, w którym użytkownicy są zablokowani, jest zapisywalny. Ma to na celu zapobieganie podatności na zagrożenia.

Należy użyć jednej z poniższych metod, aby zezwolić na przesyłanie, gdy włączony jest `chroot`.

Metoda 1. – Jest zalecaną metodą zezwalania na przesyłanie. Jest to włączenie `chroot` i skonfigurowanie katalogów FTP. W tym miejscu utworzy się katalog ftp w katalogu domowym użytkownika, który będzie służył jako `chroot` oraz zapisywalny katalog uploads do przesyłania plików.

```
/etc/vsftpd/vsftpd.conf
user_sub_token=$USER local_root=/home/$USER/ftp
```

Metoda 2. - Inną opcją jest dodanie następującej dyrektywy do pliku konfiguracyjnego `vsftpd`. Używana, jeśli trzeba przyznać użytkownikowi prawo do zapisu w jego katalogu domowym.

```
/etc/vsftpd/vsftpd.conf
allow_writeable_chroot=YES
```

4. Pasywne połączenia FTP
`vsftpd` może używać dowolnego portu do pasywnych połączeń FTP. Określić należy minimalny i maksymalny zasięg portów, a później otworzyć zasięg w firewall'u, np.:

```
/etc/vsftpd/vsftpd.conf
pasv_min_port=30000 pasv_max_port=31000
```

5. Ograniczanie logowania użytkownika
Aby zezwolić tylko niektórym użytkownikom na logowanie się do serwera FTP, należy dodać następujące wiersze po wierszu `userlist_enable=YES` :

```
/etc/vsftpd/vsftpd.conf
userlist_file=/etc/vsftpd/user_list userlist_deny=NO
```

Gdy ta opcja jest włączona, trzeba jawnie określić, którzy użytkownicy mogą się zalogować, dodając nazwy użytkowników do `/etc/vsftpd/user_list` (jeden użytkownik na linię).

6. Zabezpieczanie transmisji za pomocą SSL / TLS
Aby zaszyfrować transmisje FTP za pomocą SSL / TLS, trzeba mieć certyfikat SSL i skonfigurować serwer FTP, aby go używał.

Można użyć istniejącego certyfikatu SSL podpisanego przez zaufany urząd certyfikacji lub utworzyć samopodpisany certyfikat.

W tym ćwiczeniu pokażę sposób na wygenerowanie samopodpisany certyfikat SSL za pomocą polecenia `openssl`.

Następujące polecenie utworzy 2048-bitowy klucz prywatny i samopodpisany certyfikat ważny przez 10 lat. Zarówno klucz prywatny, jak i certyfikat zostaną zapisane w tym samym pliku:

```
openssl req -x509 -nodes -days 3650 -newkey rsa:2048 -keyout
/etc/vsftpd/vsftpd.pem -out /etc/vsftpd/vsftpd.pem
```

Po utworzeniu certyfikatu SSL tworzę (lub odkomentowuję jeśli istnieje) wpis w pliku konfiguracyjnym `vsftpd`:

Dyrektywy `rsa_cert_file` i `rsa_private_key_file`, zmieniam ich wartości na ścieżkę pliku `pam` i ustawiam dyrektywę `ssl_enable` na YES :

```
/etc/vsftpd/vsftpd.conf
rsa_cert_file=/etc/vsftpd/vsftpd.pem rsa_private_key_file=/etc/vsftpd/vsftpd.pem
ssl_enable=YES
```

Jeśli nie określono inaczej, serwer FTP będzie używał tylko TLS do nawiązywania bezpiecznych połączeń.

Nieudane próby logowania
Ograniczenie ilości prób logowania może spowolnia zautomatyzowane ataki siłowe na hasło. Przy pomocy parametru `max_login_fails` można ustawić maksymalną ilość prób, po przekroczeniu której połączenie zostanie unicestwione przez serwer FTP. Mamy także do dyspozycji opcje `delay_failed_login` oraz `delay_successful_login`, które są w stanie opóźnić ponownie próby logowania (czas w sekundach):

```
max_login_fails=3
```

```
delay_failed_login=10000
delay_successful_login=0
```

Komunikaty zwracane przez serwer
Po zalogowaniu się użytkownika, serwer FTP może zwrócić mu określoną wiadomość. Jeśli to ma być w miarę krótka informacja, to można ją określić bezpośrednio w parametrze `ftpd_banner` . W przypadku, gdy chcemy się nieco wysilić i stworzyć bardziej rozbudowaną wiadomość, to możemy wskazać plik tekstowy przy pomocy opcji `banner_file` :

```
ftpd_banner= FTP grupy Damian Roszak.
#banner_file=
```

Dodatkowo, w każdym katalogu można umieścić plik `.message`, który będzie czytany po włączeniu opcji `dirmessage_enable` . Jeśli taki plik zostanie odnaleziony w katalogu, do którego przeszedł klient, to zostanie mu wyświetlona jego zawartość. Nazwę samego pliku również można zmienić za pomocą parametru `message_file` :

```
dirmessage_enable=YES
message_file=.message
```

W tym miejscu należy uruchomić ponownie usługę `vsftpd`
Po zakończeniu edycji plik konfiguracyjny `vsftpd` (bez komentarzy) powinien wyglądać mniej więcej tak:

```
/etc/vsftpd/vsftpd.conf
anonymous_enable=NO
local_enable=YES
write_enable=YES
local_umask=022
dirmessage_enable=YES
xferlog_enable=YES
connect_from_port_20=YES
xferlog_std_format=YES
chroot_local_user=YES
listen=NO
listen_ipv6=YES
pam_service_name=vsftpd
userlist_enable=YES
userlist_file=/etc/vsftpd/user_list
userlist_deny=NO
tcp_wrappers=YES
user_sub_token=$USER
local_root=/home/$USER/ftp
pasv_min_port=30000
pasv_max_port=31000
rsa_cert_file=/etc/vsftpd/vsftpd.pem
rsa_private_key_file=/etc/vsftpd/vsftpd.pem
ssl_enable=YES
```

Należy zapisać plik i uruchomić ponownie usługę `vsftpd`, aby zmiany odniosły skutek:

```
systemctl restart vsftpd
```

Otwieranie zapory
Aby otworzyć port 21 (port poleceń FTP), port 20 (port danych FTP) i 30000-31000 (zakres portów pasywnych), należy wydać następujące polecenia:

```
firewall-cmd --permanent --add-port=20-21/tcp sudo firewall-cmd --permanent --add-port=30000-31000/tcp
```

Ponownie załadować reguły zapory, wpisując:

```
firewall-cmd --reload
```

Tworzenie użytkownika FTP
Aby przetestować serwer FTP, należy utworzyć użytkownika, tak jak każdego innego w systemie Linux.

Jeśli użytkownik, któremu chcę przyznać dostęp przez FTP już jest, pomijam pierwszy krok. Jeśli ustawię `allow_writeable_chroot=YES` w pliku konfiguracyjnym, pomijam trzeci krok.
Utworzenie nowego użytkownika o nazwie `newftpuser` :

```
adduser newftpuser
```

Następnie trzeba ustawić hasło użytkownika:

```
passwd newftpuser
```

Dodać użytkownika do listy dozwolonych użytkowników FTP:

```
echo "newftpuser" | tee -a /etc/vsftpd/user_list
```

Utworzyć drzewo katalogów FTP i ustawić odpowiednie uprawnienia:

```
mkdir -p /home/newftpuser/ftp/upload sudo chmod 550 /home/newftpuser/ftp sudo chmod 750 /home/newftpuser/ftp/upload sudo chown -R newftpuser: /home/newftpuser/ftp
```

Użytkownik będzie mógł przesłać swoje pliki do katalogu `ftp/upload` .

W tym momencie serwer FTP jest w pełni funkcjonalny i powinienem być w stanie połączyć się z serwerem za pomocą dowolnego klienta FTP, który można skonfigurować do korzystania z szyfrowania TLS, takiego jak FileZilla.

Wyłączanie dostępu do powłoki
Domyślnie podczas tworzenia użytkownika, jeśli nie zostanie to wyraźnie określone, użytkownik będzie miał dostęp SSH do serwera.

Aby wyłączyć dostęp do powłoki, utworzę nową powłokę, która po prostu wydrukuje komunikat informujący użytkownika, że jego konto jest ograniczone tylko do dostępu FTP.

Uruchamiam następujące polecenia, aby utworzyć powłokę `/bin/ftponly` i uczynić ją wykonywalną:

```
echo -e '#!/bin/sh\necho "To konto jest ograniczone do FTP wyłącznie."' | tee
-a /bin/ftponly echo -e '#!/bin/sh\necho " To konto jest ograniczone do FTP wy-
łącznie."' | tee -a /bin/ftponly sudo chmod a+x /bin/ftponly
```

Dołączam nową powłokę do listy prawidłowych powłok w `/etc/shells` :

```
echo "/bin/ftponly" | tee -a /etc/shells
```

Zmieniam powłokę użytkownika na `/bin/ftponly` :

```
usermod newftpuser -s /bin/ftponly
```

4.4.4 Ocena/wnioski/komentarze dotyczące wykonania danego zadania.

4.5 Zadanie nr 5

4.5.1 Nr i treść polecenia wg instrukcji: 2.1. e) Skonfiguruj usługę `vsftpd` tak, aby:

a. Zgłaszała się komunikatem „`FTP grupy Imię1 Nazwisko1 + Imię2 Nazwisko2`” (bez cudzysłowów; pomiń lub dodaj imię i nazwisko, odpowiednio do liczebności grupy), np. „`FTP grupy Adam Nowak + Iwo Bach`”

b. Anonimowi użytkownicy (jak się logują do FTP?) mieli dostęp do plików (w którym katalogu?), ale bez możliwości tworzenia nowych katalogów,

c. Lokalni użytkownicy (posiadający konta w systemie) mieli możliwość logowania się do FTP i prawo do zapisywania plików.

Zrestartuj `vsftpd`.

4.5.2 Cel czynności: Konfiguracja usługi `vsftpd` wg podanego schematu.

4.5.3 Sposób i rezultat wykonania polecenia (np. polecenia wydane na konsoli i odpowiedź systemu/aplikacji, w postaci wycinka zarejestrowanego logu konwersacji terminalowej w formacie tekstowym). Dopuszcza się zamieszczenie fragmentu zrzutu ekranowego. W każdym przypadku obraz rezultatu ma obejmować wykonania wyłącznie danego punktu (a nie wszystko, co widać w oknie terminala lub konsoli). Log konwersacji musi zawierać następujące bezpośrednio po niej zaproszenie (tzw. *prompt*) powłoki.

Ad.a)
W pliku konfiguracyjnym ustawiam następujący wpis:

```
#
# You may fully customise the login banner string:
ftpd_banner=FTP grupy Damian Roszak.
#
```

Ad.b)

Użytkownicy anonimowi. Są to tacy klienci, którzy identyfikują się loginem `ftp` lub `anonymous`. W zależności od przeznaczenia FTP'a możemy skonfigurować go tak, by wpuszczał takich użytkowników bez podania hasła lub też możemy założyć im hasło. Ustawiamy zatem odpowiednio parametry `anonymous_enable` oraz `no_anon_password` :

```
anonymous_enable=YES
no_anon_password=YES
```

W przypadku, gdy `no_anon_password` jest ustawiony na NO, anonimowi klienci będą musieli podać jakieś hasło. Nie jest dobrym wyjściem nadawanie każdemu takiemu użytkownikowi tego samego hasła. Po pierwsze, system będzie ich w stanie odróżnić jeśli będą się oni posługiwać innymi hasłami. A po drugie, jeśli jedno z haseł zostanie skompromitowane, to zawsze można je zablokować. Ten mechanizm w `vsftpd` konfiguruje się za pomocą parametrów `deny_email_enable` i `secure_email_list_enable` :

```
deny_email_enable=YES
banned_email_file=/etc/vsftpd/banned_emails

secure_email_list_enable=YES
email_password_file=/etc/vsftpd/email_passwords
```

Hasła, z których użytkownicy nie mogą skorzystać wpisuje się do pliku określonego przez opcję `banned_email_file`. Podobnie postępujemy w przypadku haseł dozwolonych, z tym, że wpisujemy je do pliku, który widnieje w parametrze `email_password_file`.

Jeśli chcemy, by użytkownik anonimowy był w stanie wysyłać pliki na FTP, to musimy jeszcze dopisać do konfiguracji parametr `anon_upload_enable` :

```
anon_upload_enable=YES
```

Definiujemy też podstawowe uprawnienia do plików dla klienta anonimowego. Po pierwsze musimy oddelegować konkretne konto w systemie, na którym będą operować ci klienci.
Zwykle do tego celu jest wyznaczany `nobody`. Niemniej jednak, jest on używany do szeregu innych rzeczy i raczej nie powinniśmy z niego korzystać. Zamiast tego powinniśmy w systemie utworzyć dedykowanego użytkownika, np. `ftp` i określić go w parametrze `ftp_username` :

```
ftp_username=ftp
```

Użytkownik anonimowy po zalogowaniu się na FTP'a musi znaleźć się w określonym katalogu roboczym. Ten katalog jest określany przez parametr `anon_root`. Pamiętać należy, że użytkownik ftp musi być w stanie zapisywać określony katalog. W przeciwnym razie klienci anonimowi nie będą mogli wysyłać plików. Nie jest zatem dobrym pomysłem zmiana uprawnień głównego katalogu FTP'a. Lepiej stworzyć wewnątrz niego podkatalog i to jemu nadać prawa do zapisu przez anonimowych klientów:

```
anon_root=/media/ftp/
```

Jeśli użytkownicy anonimowi mają być w stanie tworzyć nowe katalogi na FTP'ie, musimy to wyraźnie określić za sprawą opcji `anon_mkdir_write_enable`. Trzeba też pamiętać, że użytkownik taki, musi mieć prawa do zapisu danego katalogu oraz, że opcja `write_enable` musi być aktywna:

```
anon_mkdir_write_enable=YES
```

Przy pomocy parametru `anon_other_write_enable` jesteśmy w stanie rozszerzyć nieco uprawnienia anonimowych użytkowników. Standardowo nie mogą oni zmieniać nazw czy usuwać plików z serwera. Mogą oni jedynie zapisywać pliki i ewentualnie tworzyć nowe katalogi:

```
anon_other_write_enable=YES
```

W przypadku, gdybyśmy chcieli uniemożliwić użytkownikom anonimowym pobieranie plików, które mają uprawnienia, np. 640, to możemy pokusić się o przestawienie parametru `anon_world_readable_only` na YES :

```
anon_world_readable_only=NO
```

Wszystkie pliki, które są przesyłane przez anonimowych użytkowników mogą podlegać pod przepisanie uprawnień. Ten mechanizm możemy włączyć przy pomocy opcji `chown_uploads`.

Natomiast jeśli chodzi o nowego właściciela plików i prawa to nich, to określamy to w `chown_username` oraz `chown_upload_mode` , przykładowo:

```
chown_uploads=YES
chown_username=morfik
chown_upload_mode=0644
```

Ad.c)

Użytkownicy lokalni
Do serwera FTP mogą mieć także dostęp użytkownicy lokalni, tj. ci, którzy mają fizyczne konto w systemie. By zalogować się na FTP przy pomocy takiego konta, trzeba podać jego login i hasło. Tych użytkowników możemy włączyć lub wyłączyć za pomocą opcji `local_enable` :

```
local_enable=YES
```

Podobnie jak w przypadku użytkowników anonimowych, musimy określić odpowiedni katalog roboczy, do którego ci użytkownicy zostaną przeniesieni po zalogowaniu. Standardowo jest to folder domowy.
Możemy go przepisać, tak by każdy użytkownik po zalogowaniu znalazł się w konkretnym katalogu przy pomocy opcji `local_root` :

```
local_root=/media/ftp/
```

Problem z takim rozwiązaniem jest taki, że użytkownicy lokalni mogą sobie biegać praktycznie po całym drzewie katalogów, co nie jest zbytnio bezpieczne. Przydałoby się zatem zastosować mechanizm `chroot`, tak by nie mogli oni opuścić głównego katalogu FTP'a. Możemy to zrobić przy pomocy parametru `chroot_local_user` . Musimy jednak mieć gdzie ten `chroot` wykonać. Ścieżkę do pustego katalogu, który nie może być zapisywalny przez użytkownika ftp podajemy w `secure_chroot_dir` :

```
chroot_local_user=YES
secure_chroot_dir=/run/vsftpd/empty/
```

Nie zawsze jednak wszyscy użytkownicy muszą podlegać temu mechanizmowi ochrony. Opcje `chroot_list_enable` oraz `chroot_list_file` aktywują listę, która może zawierać pewne określone nazwy kont systemowych. W takim przypadku, jeśli użytkownik zaloguje się na konto znajdujące się na liście, to nie będzie chroot'owany:

```
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/chroot_list
```

Po wprowadzonych zmianach restartuję serwer FTP.:

```
[root@centos75 ~]# systemctl restart vsftpd
[root@centos75 ~]#
```

4.5.4 Ocena/wnioski/komentarze dotyczące wykonania danego zadania.

4.6 Zadanie nr 6

4.6.1 Nr i treść polecenia wg instrukcji: 2.1.f) W katalogu przeznaczonym na pliki publiczne (który to?) jako `root` umieść co najmniej jeden podkatalog. W katalogu publicznym i jego podkatalogu umieść po 2-3 nieduże pliki tekstowe. Sprawdź zawartość katalogów i plików.

4.6.2 Cel czynności: Znalezienie katalogu przeznaczonego na pliki publiczne i umiejętność umieszczenia tam plików.

4.6.3 Sposób i rezultat wykonania polecenia (np. polecenia wydane na konsoli i odpowiedź systemu/aplikacji, w postaci wycinka zarejestrowanego logu konwersacji terminalowej w formacie tekstowym). Dopuszcza się zamieszczenie fragmentu zrzutu ekranowego. W każdym przypadku obraz rezultatu ma obejmować wykonania wyłącznie danego punktu (a nie wszystko, co widać w oknie terminala lub konsoli). Log konwersacji musi zawierać następujące bezpośrednio po niej zaproszenie (tzw. *prompt*) powłoki.

Katalog przeznaczony na pliki publiczne to: `/var/ftp/pub`

Umieszczam w tym katalogu 3 pliki tekstowe.:

```
[root@centos75 ~]# cd /var/ftp/pub
[root@centos75 pub]# pwd
/var/ftp/pub
[root@centos75 pub]# ls --help > ls.help
[root@centos75 pub]# man man > man.help
<standard input>:977: warning [p 7, 3.5i, div `3tbd1,0', 0.0i]: cannot adjust line
<standard input>:986: warning [p 7, 3.5i, div `3tbd4,0', 0.0i]: cannot adjust line
[root@centos75 pub]# touch --help > touch.help
[root@centos75 pub]# ls
ls.help  man.help  touch.help
[root@centos75 pub]#
```

Tworzę w nim nowy katalog i też umieszczam w nim 3 pliki.:

```
[root@centos75 pub]# mkdir nowy
[root@centos75 pub]# ls
ls.help  man.help  nowy  touch.help
[root@centos75 pub]# cd nowy
[root@centos75 nowy]# man mkdir > mkdir.help
[root@centos75 nowy]# ls
mkdir.help
[root@centos75 nowy]# vsftpd --help > vsftpd.hlp
[root@centos75 nowy]# ls
mkdir.help  vsftpd.hlp
[root@centos75 nowy]#  touch plik
[root@centos75 nowy]# ls
mkdir.help  plik  vsftpd.hlp
[root@centos75 nowy]#
```

4.6.4 Ocena/wnioski/komentarze dotyczące wykonania danego zadania.

5. Wnioski z przeprowadzonych prac

(podsumowanie celu ćwiczenia i osiągniętych wyników, wnioski dotyczące zastosowanych środków programowych i uzyskanych wyników, samoocena stopnia osiągnięcia celu ćwiczenia)

6. Inne uwagi