

T: FTP (File Transfer Protocol).

Zadanie1:

Odszukaj w serwisie internetowym Wikipedii informacje na temat usługi FTP.

FTP (ang. File Transfer Protocol) – protokół transferu plików umożliwiający dwukierunkowy przesył plików w sieci komputerowej w układzie klient-serwer. Do komunikacji wykorzystywane są dwa połączenia TCP. Jedno z nich jest połączeniem kontrolnym za pomocą którego przesyłane są polecenia, a drugie służy do transmisji danych. Połączenie za pomocą protokołu FTP (krótko: połączenie FTP) może działać w dwóch trybach:

- aktywnym – wykorzystuje port 21 dla poleceń i port 20 do przesyłu danych,
- pasywnym – wykorzystuje port 21 dla poleceń i port o numerze powyżej 1024 do transmisji danych.

Zadanie2:

Sprawdź dostępną w systemie pomoc na temat klienta ftp (`man ftp`).

W celu odnalezienia informacji o zainstalowanych programach usługi ftp należy uruchomić YaST i przejść do Zarządzania oprogramowaniem lub w konsoli tekstowej wydać polecenie:

```
rpm -qa | grep ftp
```

Do połączenia się ze zdalnym serwerem możemy wykorzystać klienta konsoli tekstowej wydając polecenie:

```
ftp server.domena.pl  
ftp 127.0.0.1
```

Dostępne polecenia klienta tekstowego możemy wywołać poleceniem `help`.

W trybie graficznym do połączenia się ze zdalnym serwerem możemy wykorzystać menedżery plików lub przeglądarki internetowe wpisując następującą składnię w polu adresu:

<ftp://username:password@server.domena.pl/path/filename>

Serwer ftp wykorzystuje dwa porty (aktywne): 20 tcp – do przesyłania danych, 21 tcp – do komunikacji z serwerem. Stan portów w lokalnym komputerze sprawdzimy poleceniem:

```
netstat -ant
```

Lista kont użytkowników, którzy nie mogą korzystać z usługi lokalnego serwera ftp wymienieni są w pliku:

```
/etc/ftpusers
```

Zadanie3:

Sprawdź zainstalowane oprogramowanie serwera ftp, a w razie potrzeby przeprowadź instalację pakietu np. `vsftpd-2.0.5-78.rpm` oraz `yast2-ftp-server-2.15.9-24.rpm` z podanej przez nauczyciela lokalizacji. Odszukaj konfigurację serwera ftp w centrum sterowania YaST.

Zadanie4:

Przeanalizuj plik `/etc/vsftpd.conf`. Do czego służy? Jak uruchomić serwer telnetu?

<http://forum.suse.pl/index.php?topic=24337.0;wap2>

Zadanie5:

Wykonaj i przeanalizuj poniższe polecenia:

```
/etc/init.d/vsftpd restart  
/usr/sbin/vsftpd &  
wireshark &  
tcpdump -i eth0
```

Oto kolejne czynności, które należy wykonać gdy wystąpią błędy serwera dla localhost (błędy programistów):

```
/etc/init.d/xinetd stop
mkdir /etc/vsftpd
mv /etc/vsftpd.conf /etc/vsftpd/vsftpd.conf
/etc/init.d/xinetd start
```

Przykładowa treść pliku /etc/vsftpd.conf:

```
anon_mkdir_write_enable=NO
anon_other_write_enable=NO
anon_umask=022
anon_upload_enable=NO
anon_world_readable_only=YES
anonymous_enable=YES
chroot_local_user=YES
connect_from_port_20=YES
data_connection_timeout=120
dirmessage_enable=YES
dual_log_enable=NO
ftpd_banner="Witam na testowym serwerze ftp."
hide_file={*.mp3,.hidden}
hide_ids=YES
idle_session_timeout=900
listen_port=21
listen=YES
local_enable=YES
#uprawnienia plików tworzonych przez użytkowników 0=rwx,1=rw-,2=r-x,
#0-prefiks dla liczb ósemkowych,          3=r--,4=-wx,5=-w-,6---x,7=---,
#domyślnie 022=rwxr-xr-x
local_umask=0027
log_ftp_protocol=YES
max_clients=10
max_per_ip=3
pam_service_name=vsftpd
pasv_enable=YES
pasv_max_port=40500
pasv_min_port=40000
secure_chroot_dir=/srv/www
setproctitle_enable=NO
ssl_enable=NO
ssl_sslv2=NO
ssl_sslv3=NO
ssl_tlsv1=YES
syslog_enable=YES
vsftpd_log_file=/var/log/vsftpd.log
write_enable=YES
```

Serwer vsftpd może być uruchamiany z poziomu xinetd, wówczas należy przeanalizować plik /etc/xinetd.d/vsftpd, którego treść może być następująca:

```
service ftp
{
#   log_on_success        += DURATION USERID
#   log_on_failure        += USERID
#   socket_type            = stream
#   protocol              = tcp
#   wait                  = no
#   user                  = root
#   server                 = /usr/sbin/vsftpd
#   disable                = yes
}
```

Za pomocą parametru disable można włączyć (no) bądź wyłączyć (yes) serwer ftp.

Instrukcja postępowania w przypadku wystąpienia błędu 500 w Linux Open SUSE 10.0

W standardowy już sposób uruchom YaST i kliknij Usługi sieciowe | Usługi sieciowe (xinetd). Kliknij Włącz, znajdź na liście /usr/sbin/vsftpd i naciśnij przycisk Włącz/Wyłącz. Jeżeli system poprosi o pozwolenie na doinstalowanie pakietów, nie przeszkadzaj mu. Zaakceptuj zmiany, zamknij YaST. Nadszedł czas na odrobinę krytyki: serwer nazywa się Very Secure FTP Daemon, ale powinien zyskać nazwę, Przeróżająco Toporny, a nie Bardzo Bezpieczny. W samym SUSE Linuksie masz na to przykład. Uruchom Terminal i wpisz ftp 127.0. 0.1. Oczywiście (oczywiście!!) serwer nie działa i wyświetla komunikat o błędzie: "500 OOPS: could not bind listening IPv4 socket". Myślisz, że problem dotyczy konfliktu w portach albo źle skonfigurowanego firewalla. To spróbuj poniższej sztuczki (z konta roota): /etc/init.d/xinetd stop mkdir /etc/vsftpd mv /etc/vsftpd.conf /etc/vsftpd/vsftpd.conf /etc/init.d/xinetd start Te polecenia kolejno: 1. "Zabijają" serwer FTP wraz z superserwerem xinetd. 2. Tworzą katalog /etc/vsftpd. 3. Przenoszą plik konfiguracyjny VSFTPD do utworzonego właśnie katalogu. 4. Uruchamiają ponownie superserwer. Okazuje się, że komunikat o błędzie był zupełnie z innego świata, a problemy spowodowali programiści, chcący zachować zgodność VSFTPD z LSB. Szkoda tylko, że deweloperzy SUSE Linuksa się nie zorientowali... To jeszcze nie koniec drogi przez mękę tak samo jak w Windows (dla FileZilli), również w SUSE musimy otworzyć zaporę sieciową. Wybierz YaST | Zabezpieczenia i użytkownicy | Zapora sieciowa | Dozwolone usługi, kliknij Zaawansowane. W pole Porty TCP wpisz 20,21, a w pole Protokoły IP - TCP. Zignoruj komunikat, że nazwa portu 20,21 nie jest znana w systemie. Otwórz teraz z konta roota (najlepiej poleceniem mcedit) plik vsftpd.conf, przejdź do wiersza 102. i skasuj znak # na początku wiersza anon_upload_enable=YES. Zrestartuj serwer (polecenie /etc/init.d/xinetd restart). Po połączeniu się z serwerem powinieneś uzyskiwać dostęp tylko do odczytu do katalogu /srv/ftp.

Treść pliku /etc/vsftpd.conf z komentarzami:

```
# Ustawiamy tutaj, z poziomu jakiego użytkownika ma być uruchamiany nasz serwer:
nopriv_user=root
# Uruchomienie serwera w trybie standalone. Jeśli chcemy aby nasz vsftpd był
# uruchamiany w trybie inetd, rezygnujemy z tej opcji, ponieważ domyślnie jest
# ona ustawiona na "NO":
listen=YES
# Definiujemy, tutaj na jakim porcie ma nasłuchiwać serwer (domyślnie jest to port 21):
listen_port=21
# Zabronienie logowania anonimowych użytkowników:
anonymous_enable=NO
# Zezwolenie logowania dla lokalnych użytkowników
local_enable=YES
# Pozwolenie do zapisu we własnym katalogu
write_enable=YES
# Umask (022 jest używany przez większość serwerów ftp)
local_umask=022
# Włączenie logowania
xferlog_enable=YES
# Ścieżka do pliku z logami
xferlog_file=/var/log/xferlog.log
# Logi w formacie xferlog (jest wykorzystywany m.in. przez wu-ftpd)
xferlog_std_format=YES
# Maksymalna liczba połączonych użytkowników
max_clients=5
# Maksymalna liczba użytkowników mogących się połączyć z tego samego adresu IP
max_per_ip=2
# Banner, który będzie wyświetlany przy każdym połączeniu z serwerem
ftpd_banner="Prywatny serwer FTP - Powered by: vsftpd"
# Użytkownicy nie mogą wychodzić poza swój katalog domowy
chroot_local_user=YES
# Ustawiamy katalog dla chroot'a:
secure_chroot_dir=/var/chroot/vsftpd
# Lista użytkowników, którzy mogą wychodzić poza swój katalog domowy,
```

```
# musisz utworzyć ten plik.  
# np: touch /var/chroot/vsftpd/vsftpd.chroot_list  
# Dodanie użytkownika odbywa się poprzez dopisanie nazwy usera do tego pliku.  
# np: echo "tomek" >> /var/chroot/vsftpd/vsftpd.chroot_list  
chroot_list_enable=YES  
chroot_list_file=/var/chroot/vsftpd/vsftpd.chroot_list
```

Wyświetlenie informacji o połączeniach (who lub w)

```
telnet host 11
```

Uruchamianie usługi ftp za pomocą inetd – plik /etc/inetd.conf

```
ftp stream tcp nowait root /usr/etc/ftpd ftpd
```

Warto pamiętać o usłudze **tftp** wykorzystującej port 69 tcp. Jeżeli odzyskamy taki port na zdalnym serwerze:

```
tftp  
tftp>connect serwer  
tftp>get /etc/passwd /hack/twoje_passwd  
tftp>quit
```