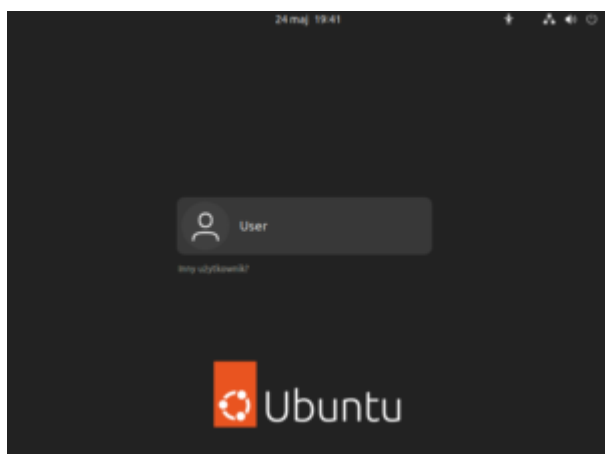


Linux – usługi (SSH, FTP, DNS)

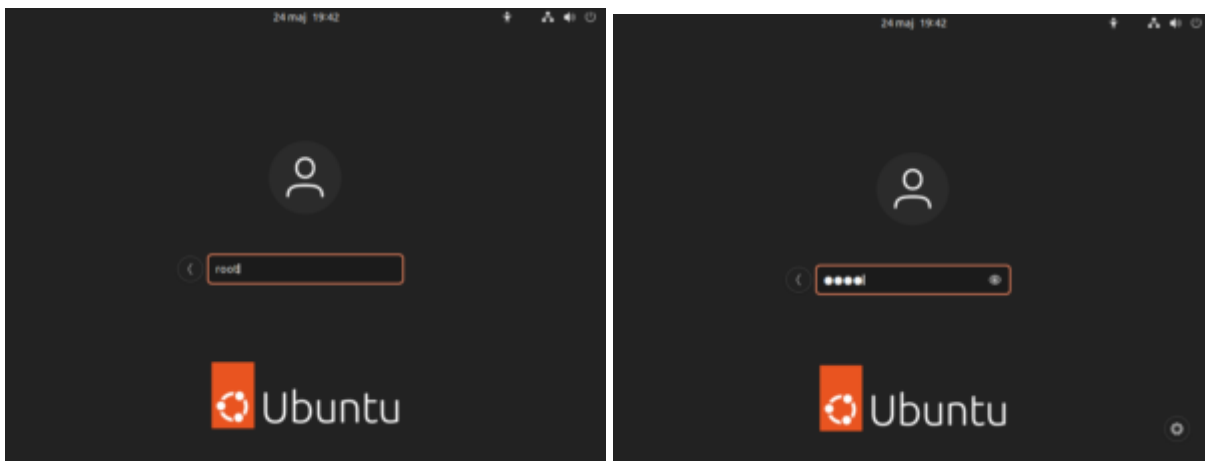
written by archi | 27 maja 2023

Przygotowanie do wdrożenia podstawowych usług sieciowych z wykorzystaniem systemu operacyjnego klasy Linux w wersji Ubuntu 22.04 Desktop

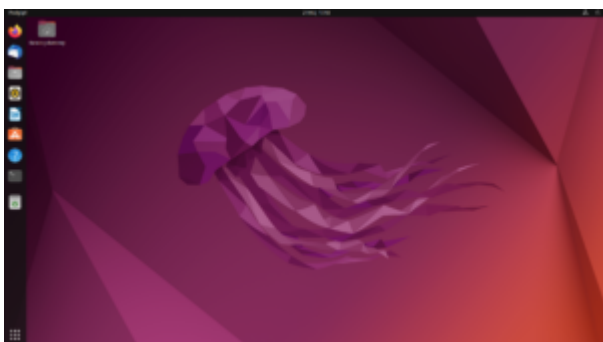
1. Na systemie stacjonarnym uruchom oprogramowanie VMware Workstation
2. Włącz maszynę wirtualną „Ubuntu Desktop”
3. Zaloguj się do niej z wykorzystaniem konta „**root**” i hasłem podanym przez prowadzącego. W celu zmiany użytkownika na ROOT należy kliknąć link poniżej nazwy konta user „Inny użytkownik”



4. Wprowadź nazwę użytkownika „root”, a następnie jego hasło

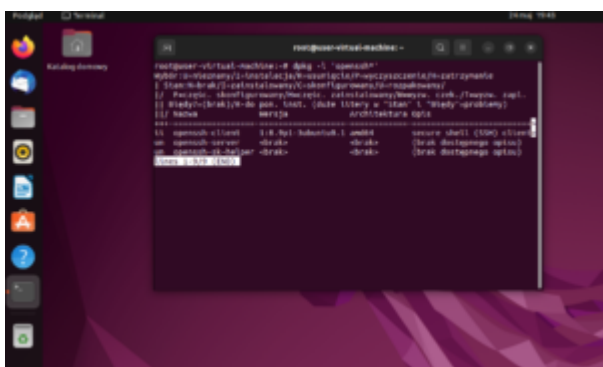


5. Po wykonaniu poprawnego uwierzytelnienia zobaczysz ekran główny systemu



6. Z lewej strony wybieramy terminal. W oknie terminala wykonujemy polecenie:

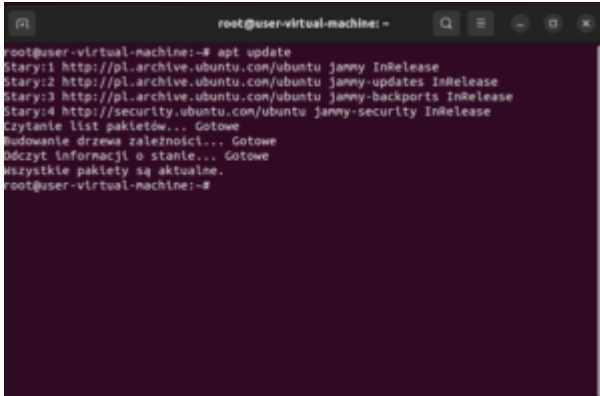
```
dpkg -l 'openssh*'
```



Po wykonaniu polecenia zobaczysz wszystkie pakiety z informacją o ich stanie. Stan „ii” informuje że pakiet zainstalowano, zaś „un” odpowiednio że jest nie zainstalowany. W naszym przypadku interesuje nas pakiet o nazwie „OpenSSH-server” aby uruchomić dostęp zdalny do naszego systemu.

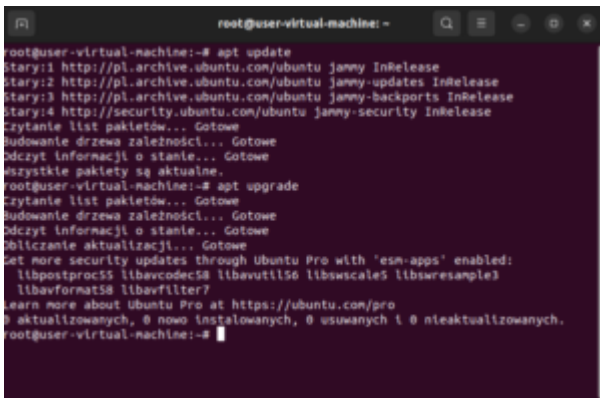
7. Instalujemy pakiet OpenSSH-server. Aktualizujemy bazę informacji o dostępnych najnowszych pakietach do tego systemu poleceniem:

```
apt update
```



```
root@user-virtual-machine:~# apt update
Stary:1 http://pl.archive.ubuntu.com/ubuntu jammy InRelease
Stary:2 http://pl.archive.ubuntu.com/ubuntu jammy-updates InRelease
Stary:3 http://pl.archive.ubuntu.com/ubuntu jammy-backports InRelease
Stary:4 http://security.ubuntu.com/ubuntu jammy-security InRelease
Czytanie list pakietów... Gotowe
Budowanie drzewa zależności... Gotowe
Ściągnij informacje o stanie... Gotowe
Wszystkie pakiety są aktualne.
root@user-virtual-machine:~#
```

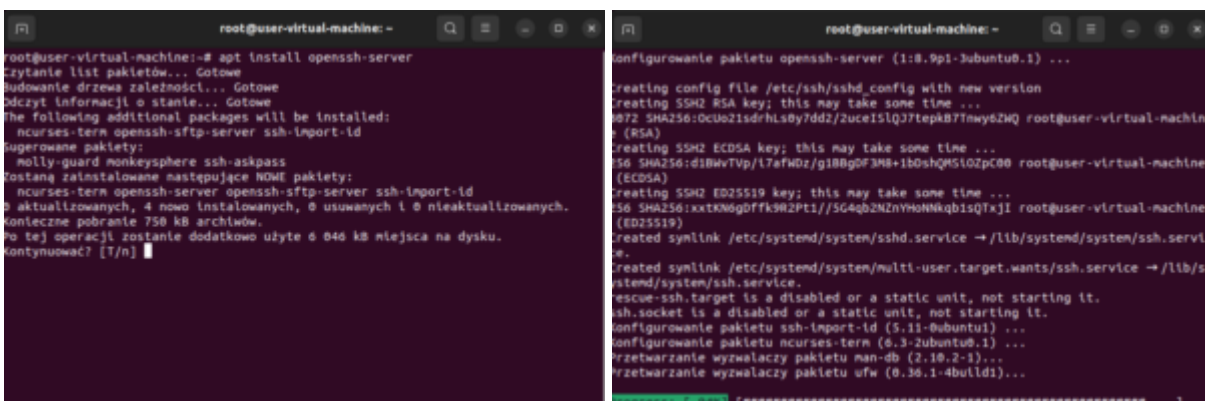
```
apt upgrade
```



```
root@user-virtual-machine:~# apt upgrade
Czytanie list pakietów... Gotowe
Budowanie drzewa zależności... Gotowe
Ściągnij informacje o stanie... Gotowe
Wszystkie pakiety są aktualne.
root@user-virtual-machine:~# apt upgrade
Czytanie list pakietów... Gotowe
Budowanie drzewa zależności... Gotowe
Ściągnij informacje o stanie... Gotowe
Obliczanie aktualizacji... Gotowe
Set more security updates through Ubuntu Pro with 'esm-apps' enabled:
  libpostproc58 libavcodec58 libavutil56 libswscale5 libswresample3
  libavformat58 libavfilter7
Learn more about Ubuntu Pro at https://ubuntu.com/pro
0 aktualizowanych, 0 nowo instalowanych, 0 usuwanych i 0 nieaktualizowanych.
root@user-virtual-machine:~#
```

Na ekranie zobaczysz informacje o tym ile aktualizacji jest wymaganych do zainstalowania (na obrazku wydać zero wymaganych instalacji i sugestią o przejściu do wersji PRO)

```
apt install openssh-server
```



```
root@user-virtual-machine:~# apt install openssh-server
Czytanie list pakietów... Gotowe
Budowanie drzewa zależności... Gotowe
Ściągnij informacje o stanie... Gotowe
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
Sugerowane pakiety:
  molly-guard monkeysphere ssh-askpass
Costaną zainstalowane następujące NOWE pakiety:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 aktualizowanych, 4 nowo instalowanych, 0 usuwanych i 0 nieaktualizowanych.
Kontynuuje pobranie 750 kB archiwów.
Po tej operacji zostanie dodatkowo użyte o 046 kB miejsca na dysku.
Kontynuować? [Y/n]
```

```
konfigurowanie pakietu openssh-server (1:0.9p1-3ubuntu0.1) ...
creating config file /etc/ssh/ssh_config with new version
creating SSH2 RSA key; this may take some time ...
#072 SHA256:0cUo21sd7hL8y7dd2/2uce15lQ37tepaB77mwy6ZwQ root@user-virtual-machine
(RSA)
creating SSH2 ECDSA key; this may take some time ...
#56 SHA256:d1BwvTvp/L7afWdz/g18BgpF3M8-1b0shqMS10Zp00 root@user-virtual-machine
(ECDSA)
creating SSH2 ED25519 key; this may take some time ...
#56 SHA256:xxTKN6gDfFk9R2PT1//5G4qb2NzYH0NNkqbisQTxJI root@user-virtual-machine
(ED25519)
created symlink /etc/systemd/system/ssh.service → /lib/systemd/system/ssh.service
created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /lib/systemd/system/ssh.service
rescue-ssh.target is a disabled or a static unit, not starting it.
ssh.socket is a disabled or a static unit, not starting it.
konfigurowanie pakietu ssh-import-id (5.11-0ubuntu1) ...
konfigurowanie pakietu ncurses-term (6.3-2ubuntu0.1) ...
przetwarzanie wyzwalaczy pakietu man-db (2.10.2-1) ...
przetwarzanie wyzwalaczy pakietu ufw (0.36.1-4build1) ...
Progress: [ 94%] [#####]
```

```
root@user-virtual-machine: ~
Creating config file /etc/ssh/sshd_config with new version
Creating SSH2 RSA key; this may take some time ...
8872 SHA256:0c0a21sdrhLs0y7dd2/2uce1S1QJ7tepK877nwy0ZMQ root@user-virtual-machine
(RSA)
Creating SSH2 ECDSA key; this may take some time ...
256 SHA256:d18wV7Vp/17aFwDz/g18gDF3M8+180shQMS10ZpC00 root@user-virtual-machine
(ECDSA)
Creating SSH2 ED25519 key; this may take some time ...
330 SHA256:xtxKMGdFfk9R2Pt1//5G4qb2NznYHoNkqBisQTxJI root@user-virtual-machine
(ED25519)
Created symlink /etc/systemd/system/ssh.service → /lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /lib/systemd/system/ssh.service.
rescue-ssh.target is a disabled or a static unit, not starting it.
ssh.socket is a disabled or a static unit, not starting it.
Konfigurowanie pakietu ssh-import-id (5.11-0ubuntu1) ...
Przetwarzanie wyzwalaczy pakietu nan-db (2.10.2-1) ...
Przetwarzanie wyzwalaczy pakietu ufw (0.36.1-4build1) ...
root@user-virtual-machine:~#
```

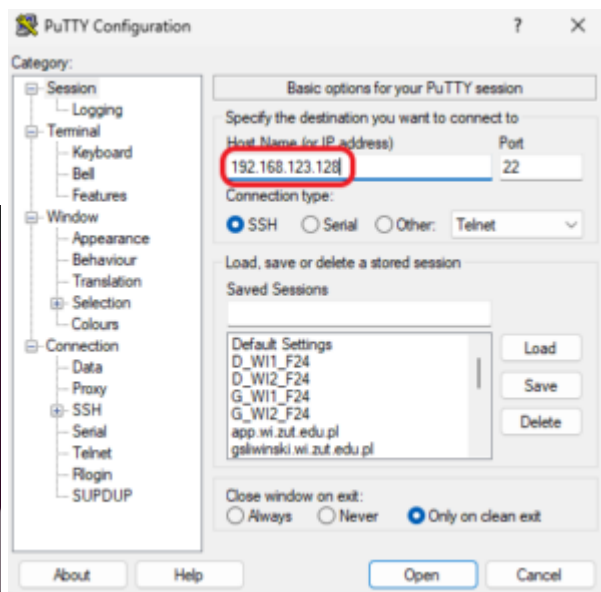
```
root@user-virtual-machine: ~
256 SHA256:xtxKMGdFfk9R2Pt1//5G4qb2NznYHoNkqBisQTxJI root@user-virtual-machine
(ED25519)
Created symlink /etc/systemd/system/ssh.service → /lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /lib/systemd/system/ssh.service.
rescue-ssh.target is a disabled or a static unit, not starting it.
ssh.socket is a disabled or a static unit, not starting it.
Konfigurowanie pakietu ssh-import-id (5.11-0ubuntu1) ...
Przetwarzanie wyzwalaczy pakietu nan-db (2.10.2-1) ...
Przetwarzanie wyzwalaczy pakietu ufw (0.36.1-4build1) ...
root@user-virtual-machine:~# dpkg -l 'openssh*'
Wybór:U=niezany/I=instalacja/R=usuniecie/P=wyczyszczenie/W=zatrzymanie
Stan:N=brak/I=zainstalowany/C=skonfigurowany/U=rozpakowany
/ / P=część, skonfigurowany/M=część, zainstalowany/W=wyzw. czek./T=wyzw. zapl.
| Błędy?=(brak)/R=do pon. inst. (duże litery w "Stan" i "Błędy"=problemy)
|/ Nazwa Wersja Architektura Opis
-----
ii openssh-client 1:0.9p1-3ubuntu0.1 amd64 secure shell (SSH) client
ii openssh-server 1:0.9p1-3ubuntu0.1 amd64 secure shell (SSH) server
ii openssh-sftp-server 1:0.9p1-3ubuntu0.1 amd64 secure shell (SSH) sftp subsystem
ii openssh-sk-helper <brak> <brak> (brak dostępnego opisu)
root@user-virtual-machine:~#
```

Po zakończeniu instalacji możemy poleceniem „**dpkg -l 'openssh*'**” sprawdzić czy pakiet już widnieje jako zainstalowany. Nie ma takiej konieczności bo instalacja zakończyła się poprawnie – sprawdzenie jest jedynie dla celów poglądowych lub w przypadku problemów z instalacją.

8. Wykonamy testowe połączenie do swojego systemu z wykorzystaniem szyfrowanego połączenie terminalowego do konsoli systemu poprzez program Putty.exe, który masz na pasku narzędziowym. Aby się połączyć do systemu potrzebujesz adresu IP twojej maszyny wirtualnej. Uzyskasz go wykonując polecenie:

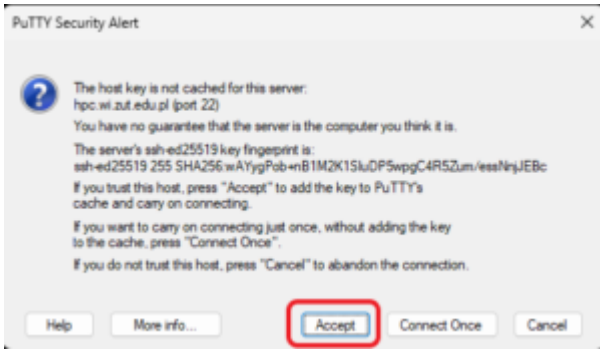
ip a

```
root@user-virtual-machine: ~
ii openssh-client 1:0.9p1-3ubuntu0.1 amd64 secure shell (SSH) client
ii openssh-server 1:0.9p1-3ubuntu0.1 amd64 secure shell (SSH) server
ii openssh-sftp-server 1:0.9p1-3ubuntu0.1 amd64 secure shell (SSH) sftp subsystem
ii openssh-sk-helper <brak> <brak> (brak dostępnego opisu)
root@user-virtual-machine:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:a7:ae:09 brd ff:ff:ff:ff:ff:ff
    altname eno33
    inet 192.168.123.124/24 brd 192.168.123.255 scope global dynamic noprefixroute ens33
        valid_lft 1407sec preferred_lft 1407sec
    inet6 fe80::e08b:c51:cfb:402b/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
root@user-virtual-machine:~#
```

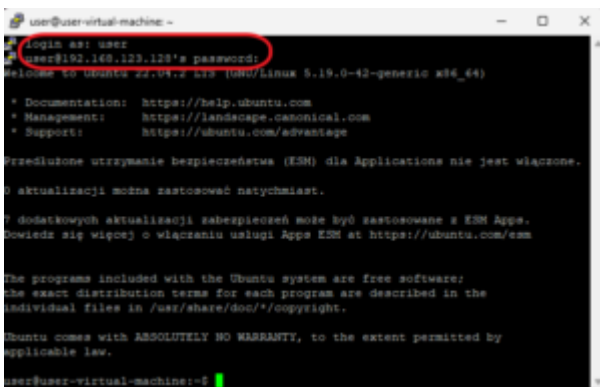


Po wpisaniu adresu zatwierdzamy poprzez „Open” i następnie zatwierdzamy klucze szyfrowania poprzez potwierdzenie certyfikatu serwera do którego

wykonujesz połączenie.

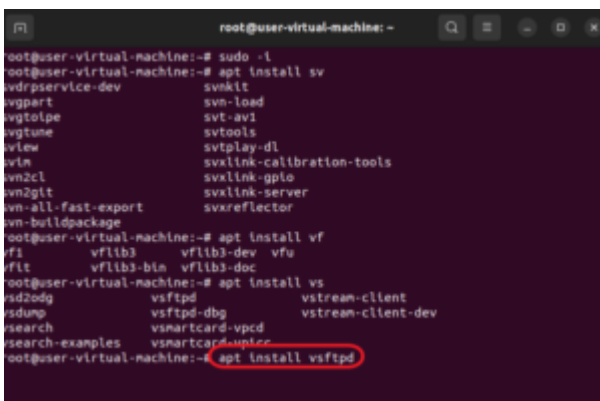


9. Logujemy się jako użytkownik **user** i hasłem **user**.



10. Możemy zamknąć okno putty poprzez skrót klawiszowy **CTRL-D** lub wykonując polecenie „**logout**„. Wracamy do maszyny wirtualnej i w konsoli instalujemy serwer FTP, którym będzie pakiet „vsftpd”. Wykonaj polecenie:

```
apt install vsftpd
```



11. Sprawdzimy czy nasz serwer FTP działa

```
service vsftpd status
```

```
root@user-virtual-machine:~# service vsftpd status
vsftpd.service - vsftpd FTP server
Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: enabled)
Active: active (running) since Wed 2023-05-24 20:08:20 CEST; 29s ago
Process: 4203 execstart=/usr/sbin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
Main PID: 4106 (vsftpd)
Tasks: 1 (limit: 9399)
Memory: 856.0K
CPU: 5ms
CGroup: /system.slice/vsftpd.service
└─4106 /usr/sbin/vsftpd /etc/vsftpd.conf

maj 24 20:08:20 user-virtual-machine systemd[1]: Starting vsftpd FTP server...
maj 24 20:08:20 user-virtual-machine systemd[1]: Started vsftpd FTP server.
root@user-virtual-machine:~#
```

12. Jeśli serwer (usługa) działa to możemy przejść do utworzenia konta użytkownika (dodatkowego) któremu damy dostęp do serwera FTP. W tym celu utworzymy konto „ftuser” z hasłem „user”

```
root@user-virtual-machine:~# adduser ftuser
Dodawanie użytkownika "ftuser" ...
Dodawanie nowej grupy "ftuser" (1001)...
Dodawanie nowego użytkownika "ftuser" (1001) w grupie "ftuser"...
Tworzenie katalogu domowego "/home/ftuser"...
Kopowanie plików z "/etc/skel" ...
Nowe hasło:
BŁĘDNE HASŁO: Hasło jest krótsze niż 8 znaków
Proszę ponownie wpisać nowe hasło:
Hasła się nie zgadzają.
Nowe hasło:
BŁĘDNE HASŁO: Hasło jest krótsze niż 8 znaków
Proszę ponownie wpisać nowe hasło:
password: hasło zostało zmienione
Zmień informacje o użytkowniku ftuser
Wpisz nową wartość lub wciśnij ENTER by przyjąć wartość domyślną
Imię i nazwisko []: FTP User
Numer pokoju []:
Telefon do pracy []:
Telefon domowy []:
Inne []:
Czy informacja jest poprawna? [Y/n]
```

13. Wykonamy kilka poleceń do przygotowania środowiska FTP dla tego użytkownika:

Przejdziemy do katalogu użytkowników

```
cd /home
```

Poleceniem poniżej sprawdzimy jakie foldery tam są:

```
ls
```

Utworzymy folder dla danych ftp

```
mkdir /home/ftuser/ftp
```

Zmienimy właściciela tego utworzonego folderu na NIKT bo będziemy również uruchamiać dostęp do niego w trybie anonimowym (anonymous) czyli jako

dowolny użytkownik z internetu

```
chown nobody:nogroup /home/ftpuser/ftp
```

Zabierzemy prawa zapisu do tego folderu dla dowolnego (other) użytkownika

```
chmod a-w /home/ftpuser/ftp
```

Utworzymy folder dla wgrywania danych wewnątrz folderu ftp

```
mkdir /home/ftpuser/ftp/upload
```

Nadamy uprawnienia dla ftpuser aby mógł w tym folderze tylko on wgrywać dane

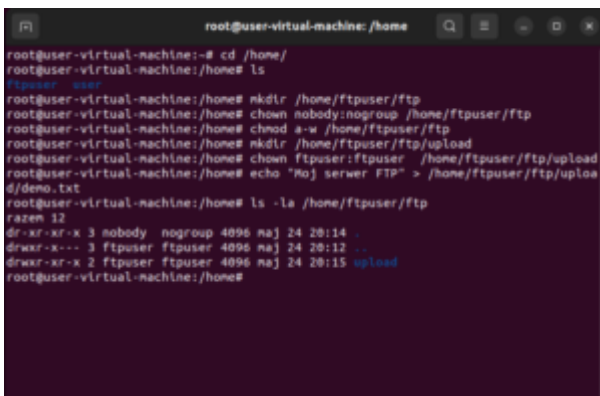
```
chown ftpuser:ftpuser /home/ftpuser/ftp/upload
```

Utworzymy tam przykładowy plik „demo.txt” z zawartością „Mój serwer FTP”

```
echo "Mój serwer FTP" > /home/ftpuser/ftp/upload/demo.txt
```

Sprawdzimy czy uprawnienia są poprawne w folderze

```
ls -al /home/ftpuser/ftp
```

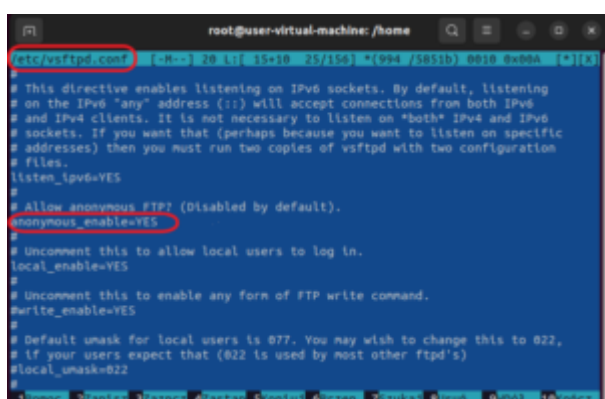


```
root@user-virtual-machine: /home
root@user-virtual-machine:~# cd /home/
root@user-virtual-machine:/home# ls
ftpuser  user
root@user-virtual-machine:/home# mkdir /home/ftpuser/ftp
root@user-virtual-machine:/home# chown nobody:nogroup /home/ftpuser/ftp
root@user-virtual-machine:/home# chmod a-w /home/ftpuser/ftp
root@user-virtual-machine:/home# mkdir /home/ftpuser/ftp/upload
root@user-virtual-machine:/home# chown ftpuser:ftpuser /home/ftpuser/ftp/upload
root@user-virtual-machine:/home# echo "Mój serwer FTP" > /home/ftpuser/ftp/upload/demo.txt
root@user-virtual-machine:/home# ls -la /home/ftpuser/ftp
razem 12
dr-xr-xr-x 3 nobody nogroup 4096 naj 24 20:14 .
drwxr-x--- 3 ftpuser ftpuser 4096 naj 24 20:12 ..
drwxr-xr-x 2 ftpuser ftpuser 4096 naj 24 20:15 upload
root@user-virtual-machine:/home#
```

14. Strukturę i konta mamy gotowe – teraz czas na przygotowanie funkcjonalne serwera FTP. W tym celu musimy edytować konfigurację serwera która jest w pliku „/etc/vsftpd.conf”. Wykorzystamy w celu uproszenia oprogramowanie mc które jest nakładką graficzną na system plików. Uruchamiamy polecenie: mc i przechodzimy do folderu /etc

wykorzystują kursory z klawiatury (nie myszka) i klawisza Enter na polu „...” jeśli chcesz wyjść o folder w górę. Znajdź z /etc plik vsftpd.conf i będziemy go edytować poprzez klawisz F4. Przy pierwszym uruchomieniu edytora system zapyta którego chcesz użyć – KONIECZNIE wybierz mcedit (powinna to być opcja 2) potwierdzając wybór cyfrą i enter.

W pierwszej kolejności włączamy logowanie anonimowe ustawiając opcję „**anonymous_enable=YES**” (nie może być znaku hash „#” bo to oznacza komentarz

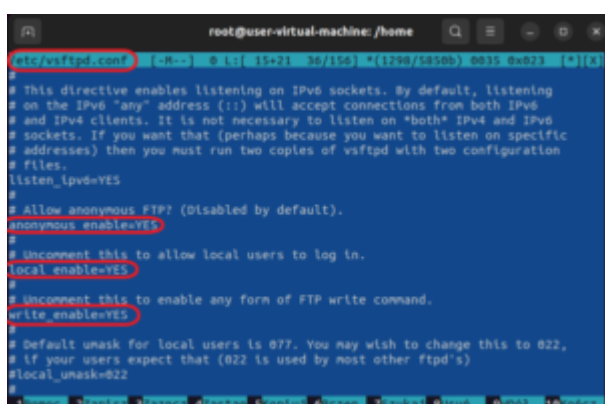


```
root@user-virtual-machine: /home
/etc/vsftpd.conf 15+10 25/155 (104/8515) 0010 0x00A
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and 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
```

15. Następnie włączamy kolejno opcje:

local_enable=YES

write_enable=YES



```
root@user-virtual-machine: /home
/etc/vsftpd.conf 15+21 36/156 *(1298/5850b) 0035 0x021
# 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
```

16. Dalej modyfikując konfigurację niżej w pliku włączamy opcję

chroot_local_user=YES


```
root@user-virtual-machine: /home
/etc/vsftpd.conf [-R--] @ L:[117+15 132/156] *(5878/5849b) @035 0x021
# 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
ssl_enable=NO
# Uncomment this to indicate that vsftpd use a utf8 filesystem.
utf8_filesystem=YES
# user_sub_token=$USER
# local_root=/home/$USER/ftp
```

17. Dodajemy na końcu pliku

user_sub_token=\$USER

local_root=/home/\$USER/ftp

```
root@user-virtual-machine: /home
/etc/vsftpd.conf [-R--] @ L:[138+21 159/159] *(5898/5898b) <EOF>
# 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
ssl_enable=NO
# Uncomment this to indicate that vsftpd use a utf8 filesystem.
utf8_filesystem=YES
# user_sub_token=$USER
# local_root=/home/$USER/ftp
```

Przypiszemy kto może korzystać z FTP

userlist_enable=YES

userlist_file=/etc/vsftpd.userlist

userlist_deny=NO


```
root@user-virtual-machine: /home
root@user-virtual-machine: /home service vsftpd restart
root@user-virtual-machine: /home service vsftpd status
vsftpd.service - vsftpd FTP server
Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; vendor preset: enabled)
Active: active (running) since Fri 2023-05-26 13:14:41 CEST; 5s ago
Process: 4079 /usr/bin/vsftpd -/bin/mkdir -p /var/ran/vsftpd/empty (code=exited, status=0/SUCCESS)
Main PID: 4074 (vsftpd)
Tasks: 1 (limit: 5995)
Memory: 452.0K
CPU: 10s
CGroup: /system.slice/vsftpd.service
└─4374 /usr/sbin/vsftpd /etc/vsftpd.conf

maj 26 13:14:41 user-virtual-machine systemd[1]: Starting vsftpd FTP server...
maj 26 13:14:41 user-virtual-machine systemd[1]: Started vsftpd FTP server.
root@user-virtual-machine: /home
```

21. Wykonamy teraz test połączenia do serwera FTP. W tym celu uruchom w Windows konsole polecenie CDM i wewnątrz niej polecenie FTP

```
Microsoft Windows [Version 10.0.22621.1702]
(c) Microsoft Corporation. Wszelkie prawa zastrzeżone.

C:\Users\Grzegorz> ftp 192.168.123.128
Connected to 192.168.123.128.
220 (vsFTPd 3.0.5)
200 Always in UTF8 mode.
User (192.168.123.128:(none)): ftpuser
331 Please specify the password.
Password:
230 Login successful.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  2 1001  1001    4096 May 24 20:15 upload
226 Directory send OK.
ftp: 67 bytes received in 0.00Seconds 67.00Kbytes/sec.
ftp> cd upload
250 Directory successfully changed.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--  1 0 0    15 May 24 20:15 demo.txt
226 Directory send OK.
ftp: 69 bytes received in 0.00Seconds 34.50Kbytes/sec.
ftp> bye
221 Goodbye.

C:\Users\Grzegorz>
```

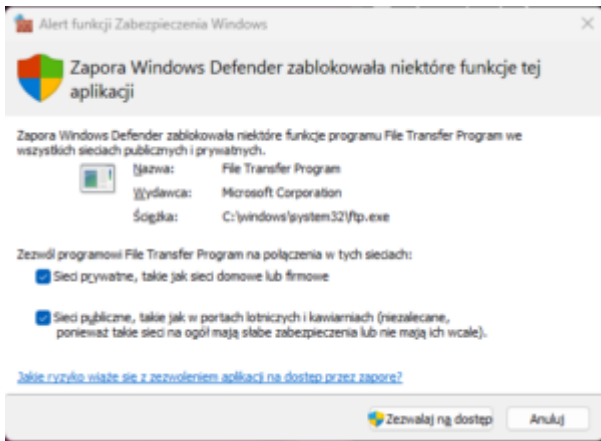
Wykonaj kolejno polecenia:

`ftp <tu swój adres IP>`

zaloguj się jako **ftpuser** z hasłem **user**

po prawidłowym zalogowaniu wykonaj komendę `dir`

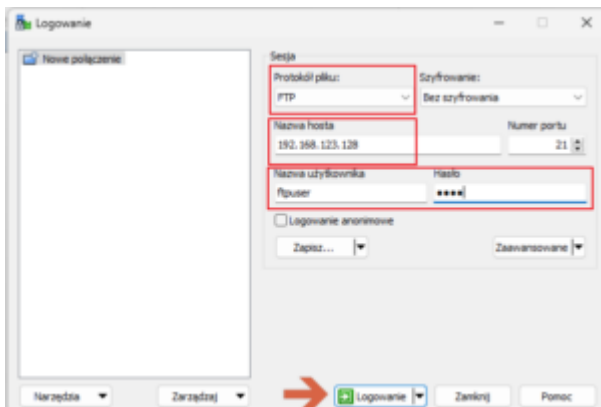
UWAGA - może pojawić się prośba o dopuszczenie komunikacji w ramach Firewall Windows - zezwól na nią w obu typach sieci Prywatnej i Publicznej



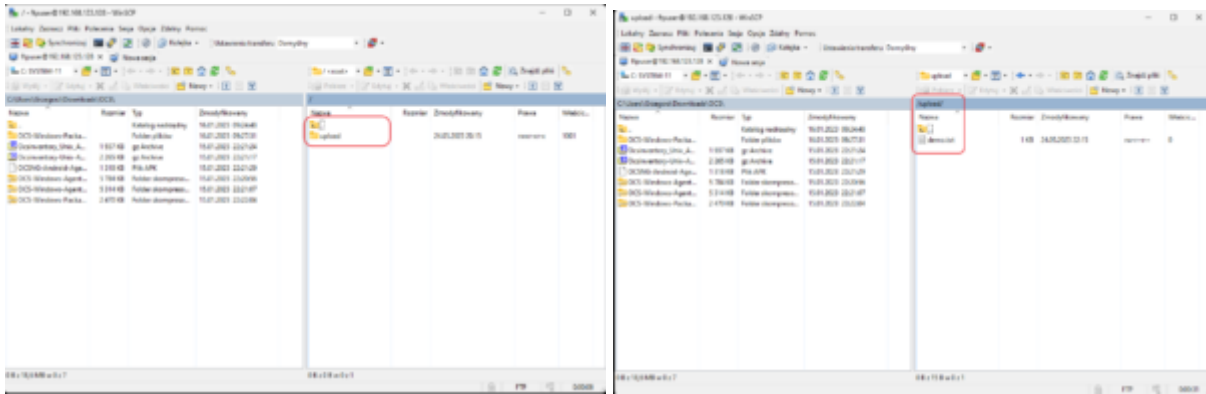
Przejdziemy do folderu **upload** i zobaczymy co zawiera poprzez polecenie `dir`

Na koniec rozłączymy się poleceniem `bye`

22. Wykonamy połączenie do serwera FTP z wykorzystaniem oprogramowania WinSCP. Masz go dostępnego na pasku narzędziowym. Odpowiednio do obrazka wybierz protokół FTP, adres IP twojej maszyny wirtualnej (nie ten co na obrazku), użytkownika ftpuser i jego hasło user. Następnie połącz się poprzez przycisk „logowanie”

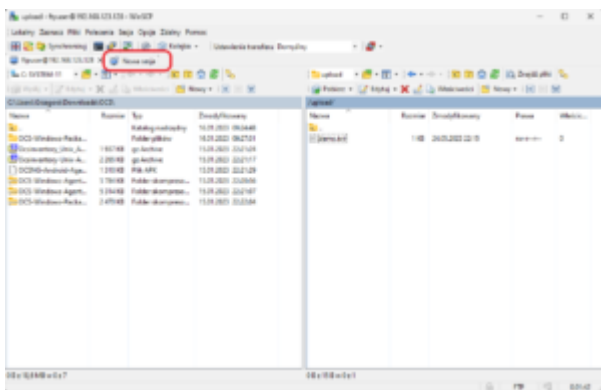


23. Po poprawnym zalogowaniu się dostaniesz się znowu do folderu ftp tego konta



Połączenie po protokole FTP jest niezabezpieczone i przesyłane dane można w prosty sposób posłuchać – w tym loginy i hasła. Lepszym zabezpieczeniem byłoby wykorzystanie protokołów szyfrowanych. Może to być zrealizowane na bazie serwera FTP jednak należy wygenerować klucze publiczne i prywatne i odpowiednio podpiąć je do serwera, co pozwoliło by na połączenia Sftp. Prostszy rozwiązaniem byłoby wykorzystanie usługi która jest od razu przystosowana do takich połączeń – SSH. Secure Shell pozwala na terminalowe połączenia ale również na transfer danych.

24. Otwórz nową sesję w ramach programu WinSCP.



Tym razem wybieramy protokół SCP i reszta bez zmian.

Sesja

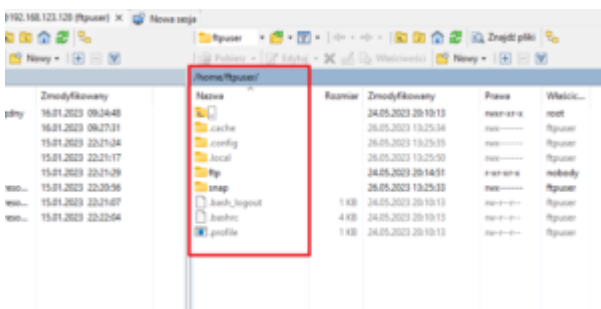
Protokół pliku:
SCP

Nazwa hosta: 192.168.123.128 Numer portu: 22

Nazwa użytkownika: ftpuser Hasło: ●●●●

Zapisz... Zaawansowane

25. Po połączeniu zauważysz że widzisz więcej danych ponieważ nie ogranicza cię ustawienia serwera ftp. W tym przypadku otrzymujesz pełny dostęp do swojego konta i uprawnień jakie ono ma. Wadą tego rozwiązania jest niemożliwość połączenia się w trybie anonimowym.



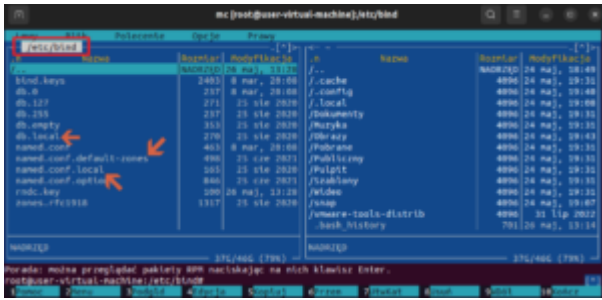
26. Przejdziemy do konfiguracji własnego serwera DNS. Potrzebujemy zainstalować takowy na naszym hoście - w tym celu wykonaj polecenie:

```
apt install bind9
```

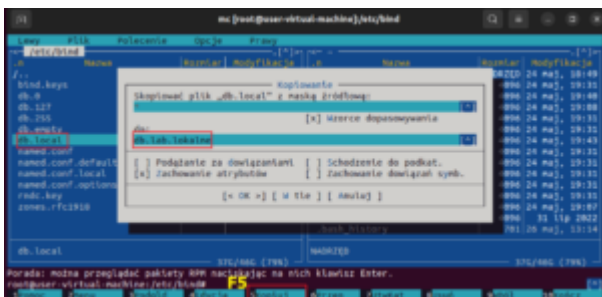
```
root@user-virtual-machine:~# apt install bind9
Czytanie list pakietów... Gotowe
Budowanie drzewa zależności... Gotowe
Odczyt informacji o stanie... Gotowe
The following additional packages will be installed:
  bind9-utils
Sugerowane pakiety:
  bind-doc resolvconf
Zostaną zainstalowane następujące NOWE pakiety:
  bind9 bind9-utils
0 zaktualizowanych, 2 nowe instalowanych, 0 usuwanych i 1 nieaktualizowanych.
konieczne pobranie 421 kB archiwów.
Po tej operacji zostanie dodatkowo użyte 1 656 kB miejsca na dysku.
Kontynuować? [Y/n]
```

27. Uruchom polecenie mc. Przejdź do folderu /etc/bind9. Wewnątrz zobaczysz pliki konfiguracyjne serwera. Dla nas będą istotne:

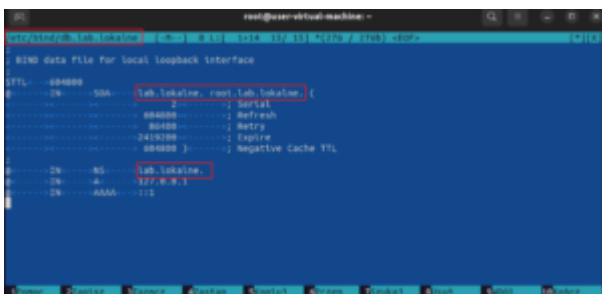
```
db.local
named.conf.default-zones
named.conf.local
```



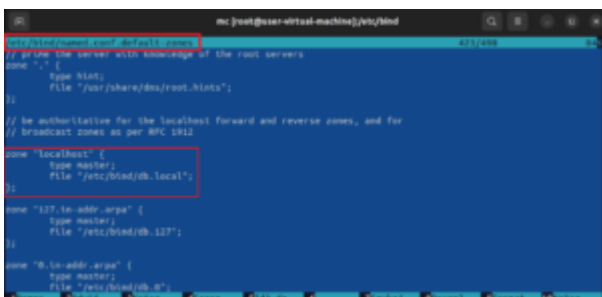
28. Ustaw się znacznikiem na pliku db.local i używając klawisza F5 wykonasz kopię tego pliku pod nową nazwą db.lab.lokalne



29. Edytuj nowo powstały plik i zmień w nim wszystkie wystąpienia localhost na lab.lokalne.

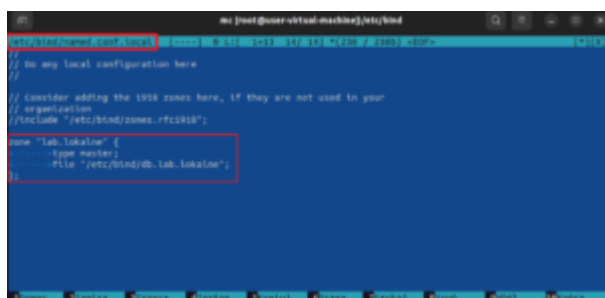


30. Teraz musimy edytować plik named.conf.default-zones. Z niego weźmiemy definicję strefy localhost (zaznaczony na obrazku obszar) i przeniesiemy dane do pliku named.conf.local



31. Wpisujemy skopiowane dane do pliku named.conf.local na jego końcu

i poprawiamy informację o strefie (zamiast localhost -> lab.lokalne) oraz zmieniamy nazwę pliku strefy (zamiast db.local -> db.lab.lokalne)

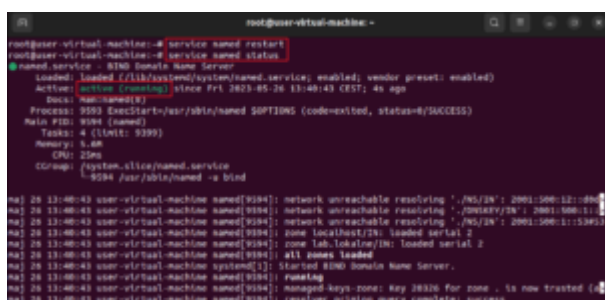


```
root@user-virtual-machine:~/etc/bind#  
// Do any local configuration here  
//  
// Consider adding the 1938 zones here, if they are not used in your  
// organization  
//INCLUDE "/etc/bind/zones.rfc1938";  
  
zone "lab.lokalne" {  
    type master;  
    file "/etc/bind/db.lab.lokalne";  
};
```

32. Zrestartuj usługę DNS i sprawdź czy działa poprawnie.

service named restart

service named status



```
root@user-virtual-machine:~# service named restart  
root@user-virtual-machine:~# service named status  
named.service - BIND Domain Name Server  
loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)  
active: active (running) since Fri 2023-05-26 13:40:43 CEST; 4s ago  
Docs: man:named(8)  
Process: 9392 ExecStart=/usr/sbin/named SOFTDNS (code=exited, status=0/SUCCESS)  
Main PID: 9394 (named)  
Tasks: 4 (limit: 9399)  
Memory: 1.6M  
CGroup: /system.slice/named.service  
          └─9394 /usr/sbin/named -s bind  
  
[1] 26 13:40:43 user-virtual-machine named[9394]: network unreachable resolving ".NS/24": 2001:500:12::c8e  
[1] 26 13:40:43 user-virtual-machine named[9394]: network unreachable resolving ".DNSKEY/28": 2001:500:12:  
[1] 26 13:40:43 user-virtual-machine named[9394]: network unreachable resolving ".NS/24": 2001:500:1:1:3093:  
[1] 26 13:40:43 user-virtual-machine named[9394]: zone localhost/25: loaded serial 2  
[1] 26 13:40:43 user-virtual-machine named[9394]: zone lab.lokalne/28: loaded serial 2  
[1] 26 13:40:43 user-virtual-machine named[9394]: all zones loaded  
[1] 26 13:40:43 user-virtual-machine systemd[1]: Started BIND Domain Name Server.  
[1] 26 13:40:43 user-virtual-machine named[9394]: running  
[1] 26 13:40:43 user-virtual-machine named[9394]: managed-keys-zone: Key 28326 for zone . is now trusted [1]  
[1] 26 13:40:43 user-virtual-machine named[9394]: resolve: initiating query complete: success
```

33. Wykonaj test działania serwera DNS. Wydadź w konsoli następujące polecenia jak na obrazku poniżej.

nslookup

server 127.0.0.1

set type=any

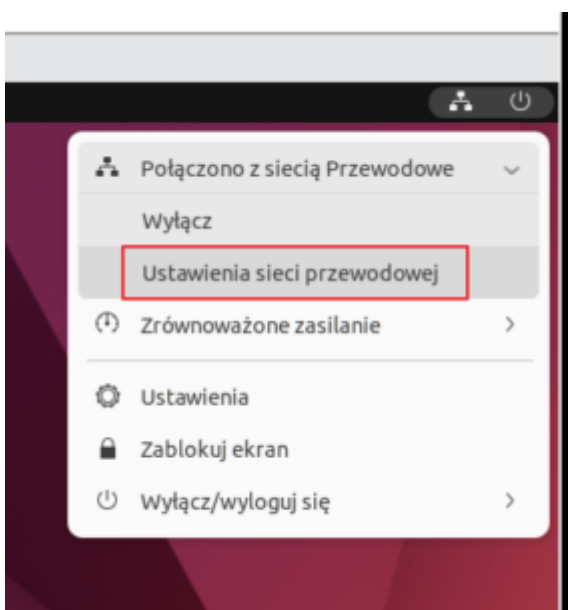
lab.lokalne


```
root@user-virtual-machine: ~  
root@user-virtual-machine:~# nslookup  
> server 127.0.0.1  
Default server: 127.0.0.1  
Address: 127.0.0.1#53  
> set type=any  
> lab.lokalne  
;; Connection to 127.0.0.1#53(127.0.0.1) for lab.lokalne failed: timed out.  
Server:      127.0.0.1  
Address:    127.0.0.1#53  
  
lab.lokalne  
origin = lab.lokalne  
mail addr = root.lab.lokalne  
serial = 2  
refresh = 604800  
retry = 86400  
expire = 2419200  
minimum = 604800  
lab.lokalne nameserver = lab.lokalne.  
Name: lab.lokalne  
Address: 127.0.0.1  
Name: lab.lokalne  
Address: ::1  
>
```

34. Przejdź do konsoli graficznej i wybierz ikonę ustawień sieci.



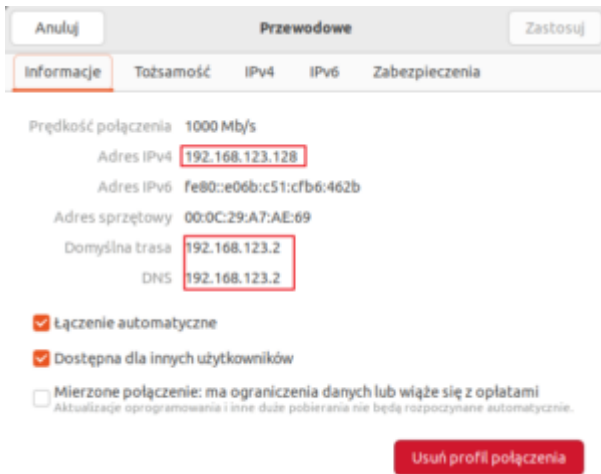
35. Wybierz ustawienia sieci przewodowej



36. W ramach sieci wybierz ustawienia



37. Sprawdź dane ustawień sieciowych swojego komputera.

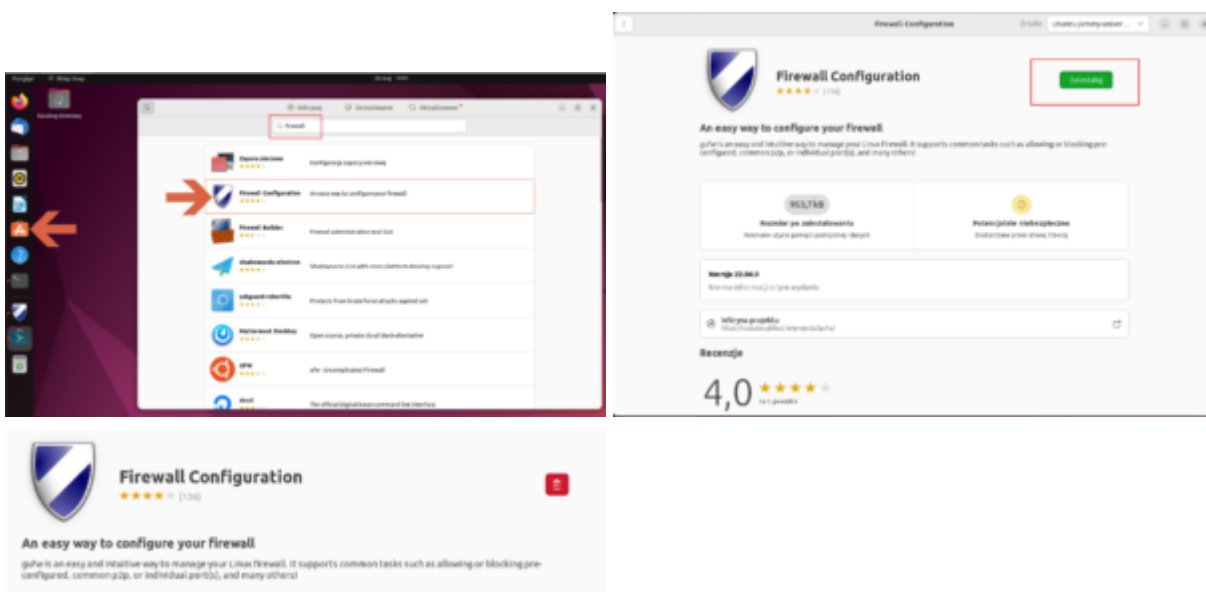


38 Teraz z konsoli postaramy się odczytać te dane bez wykorzystywania środowiska graficznego.

ip r

```
root@user-virtual-machine:~# ip r
default via 192.168.123.2 dev ens33 proto dhcp metric 100
169.254.8.0/16 dev ens33 scope link metric 1000
192.168.123.0/24 dev ens33 proto kernel scope link src 192.168.123.128 metric 100
root@user-virtual-machine:~#
```

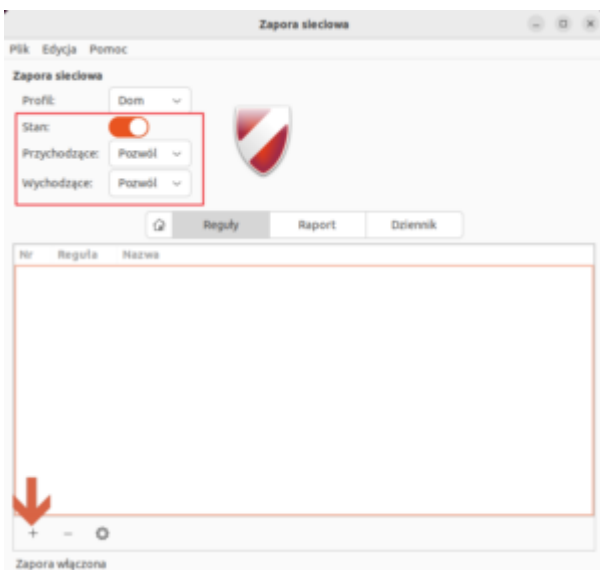
39. Zabezpieczenie swojej stacji jest bardzo ważne. Z każdego miejsca możemy spodziewać się ataku i próby przejęcia hosta. Powinniśmy zadbać aby najlepiej jak można zabezpieczyć swój system. Ustawimy zaporę ogniową – FireWall. W pierwszej kolejności musimy doinstalować oprogramowanie do zarządzania oprogramowaniem UFW. Nie jest ono wymagane bo można wszystkie polecenia wydać z konsoli. Zobacz obrazek poniżej.



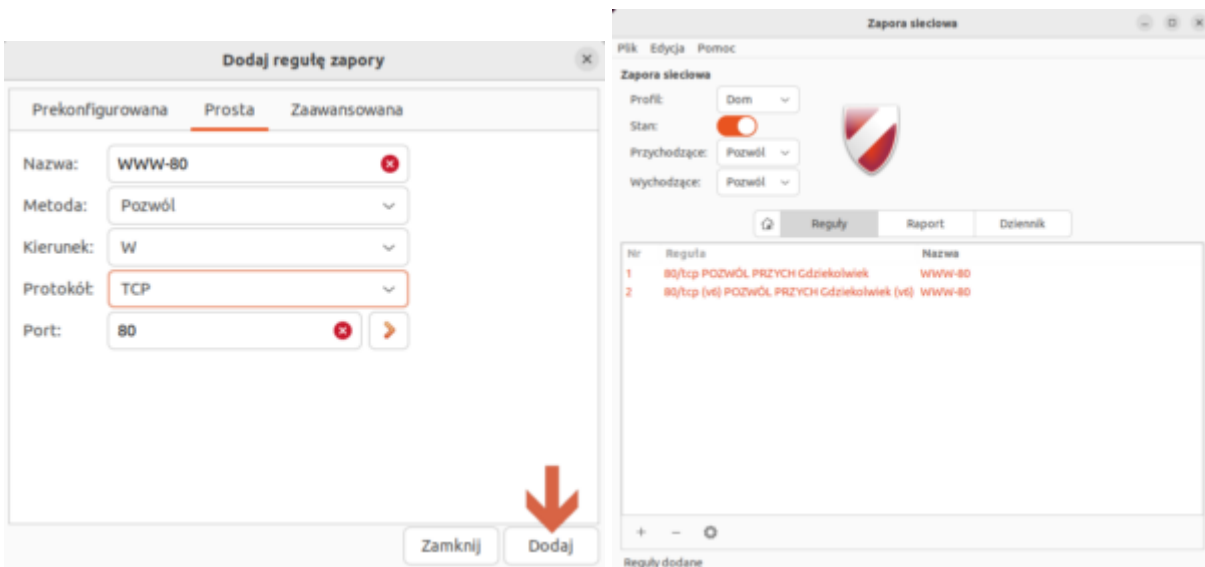
40. Uruchom oprogramowanie z dostępnych w aplikacjach.



41. Włącz zaporę i ustaw pozwolenia dla danych wchodzących i wychodzących do systemu.



42. Poprzez znak + dodaj nową regułę pozwalającą na ruch przychodzący do serwera WWW działającego na porcie 80. Nazwij tą regułę WWW-80.



43. Pojawiły się dwa wpisy – dlaczego? Zobacz ustawione reguły w konsoli serwera wydając polecenie

```
ufw status verbose
```

```
root@user-virtual-machine:~# ufw status verbose
Stan: aktywny
Logowanie: on (low)
Domyślnie: allow (przychodzące), allow (wychodzące), disabled (trasowane)
Nowe profile: skip

Do          Działanie  Z
--          -
80/tcp      ALLOW IN   Anywhere
80/tcp (v6) ALLOW IN   Anywhere (v6)

root@user-virtual-machine:~#
```

44. Zgłoś prowadzącemu zakończenie i pokaż swoje wyniki. Wyjaśnij dlaczego były dwa wpisy w ustawieniach FireWall.