Linux – usługi (SSH, FTP, DNS)

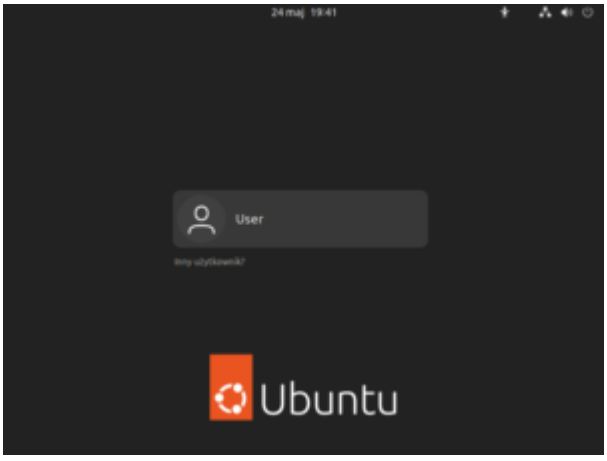
written by archi | 27 maja 2023

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

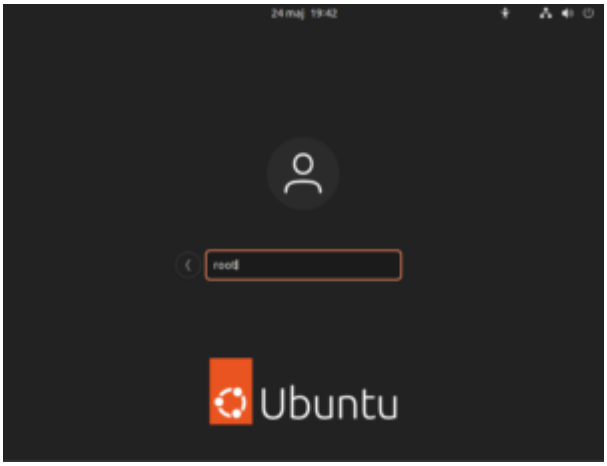
1. Na systemie stacjonarnym uruchom oprogramowanie VMware Workstation

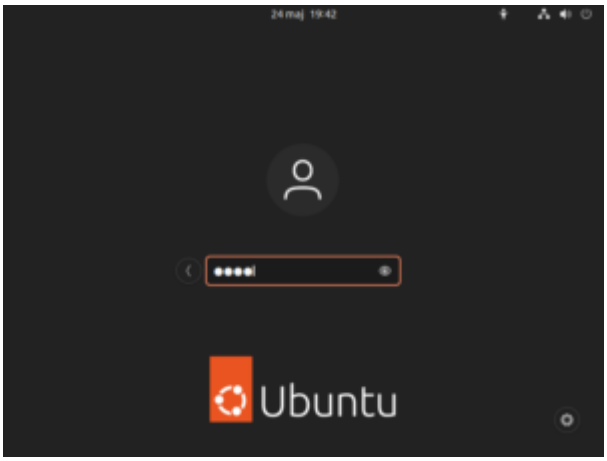
2. Włącz maszynę wirtualną „Ubuntu Desktop”

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”

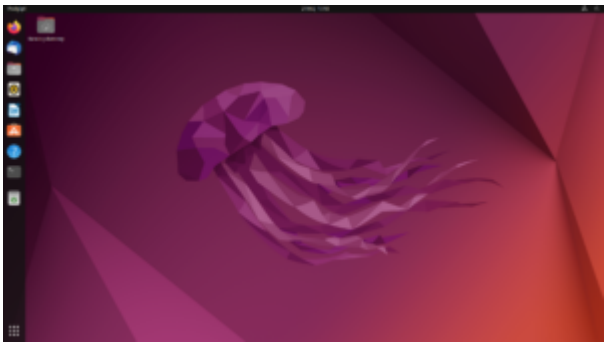


4. Wprowadź nazwę użytkownika „root”, a następnie jego hasło



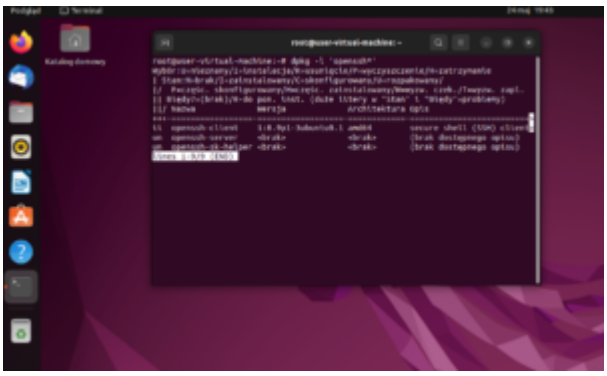


5. Po wykonaniu poprawnego uwierzytelnienia zobaczysz ekran główny systemu



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

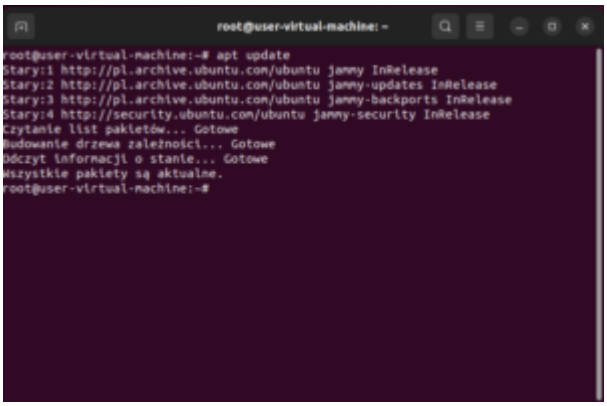
```
dpkg -l 'openssh*'
```



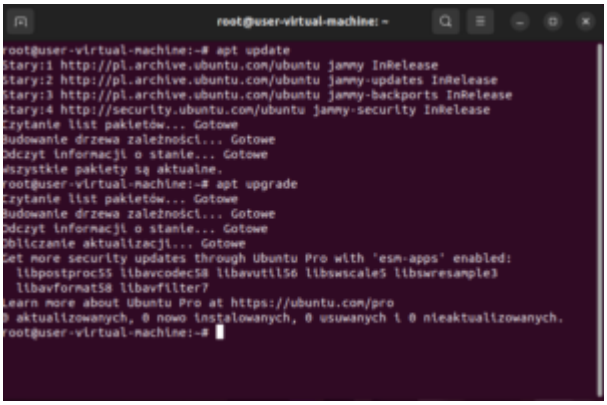
Po wykonaniu polecenia zobaczysz wszystkie pakiety z informacją o ich stanie. Stan „ii” informuje że pakiet zainstalowano, zaś „un” odpowiednio że jest nie zainstalowany. W naszym przypadku interesuje nas pakiet o nazwie „OpenSSH-server” aby uruchomić dostęp zdalny do naszego systemu.

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

```
apt update
```

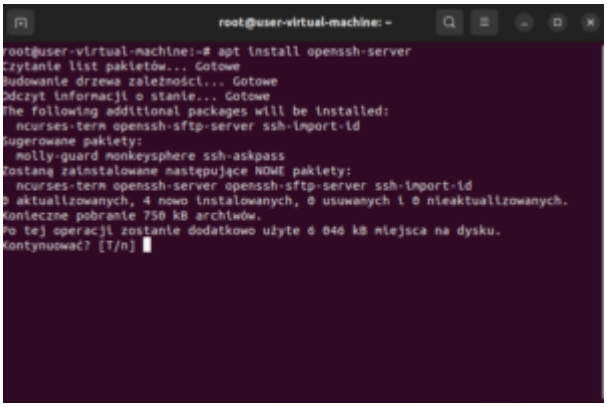


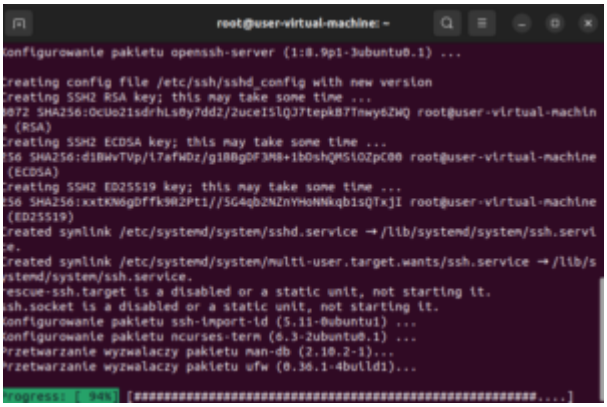

```
apt upgrade
```

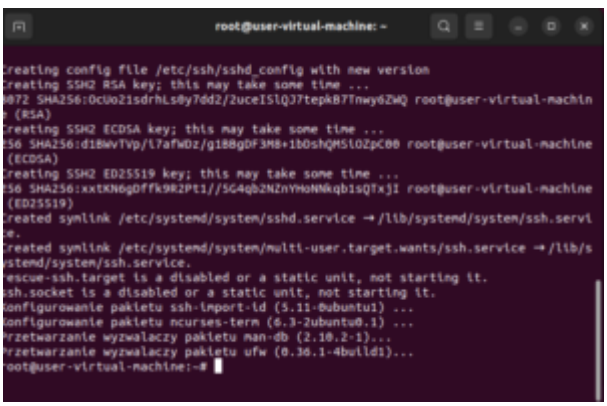


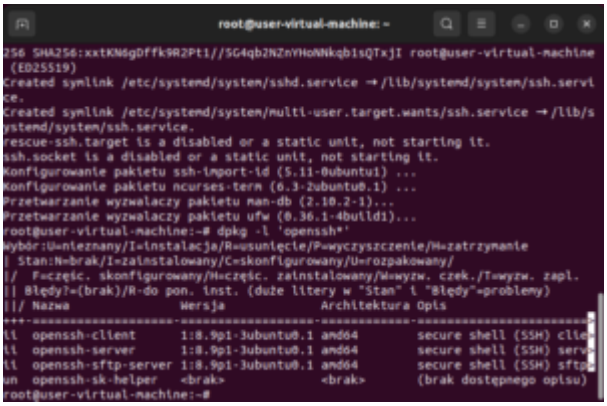
Na ekranie zobaczysz informacje o tym ile aktualizacji jest wymaganych do zainstalowania (na obrazku wydać zero wymaganych instalacji i sugestię o przejściu do wersji PRO)

```
apt install openssh-server
```





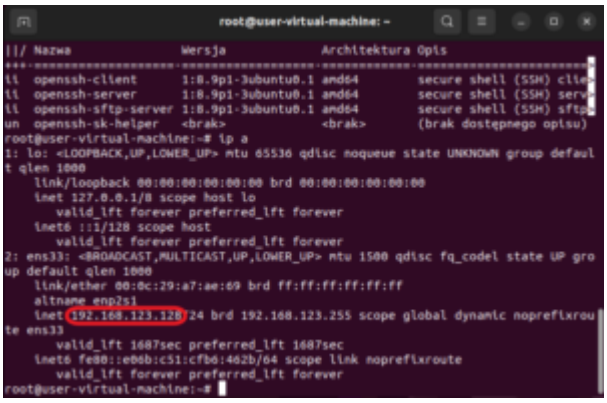


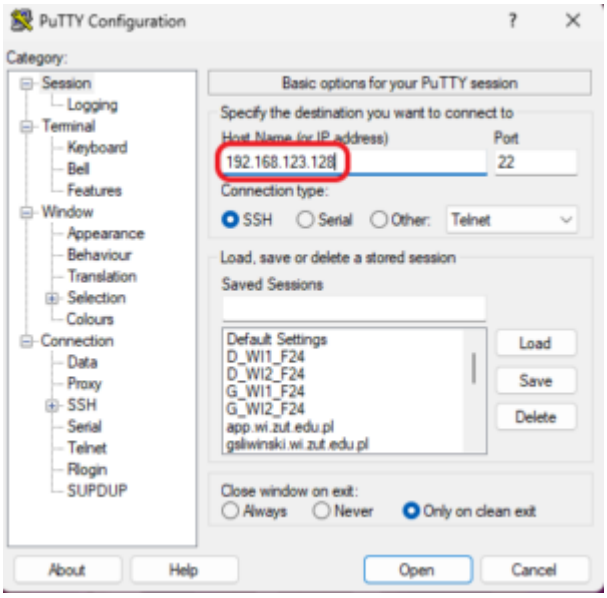


Po zakończeniu instalacji możemy poleceniem „**dpkg -l 'openssh***'” sprawdzić czy pakiet już widnieje jako zainstalowany. Nie ma takiej konieczności bo instalacja zakończyła się poprawnie – sprawdzenie jest jedynie dla celów poglądowych lub w przypadku problemów z instalacją.

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:

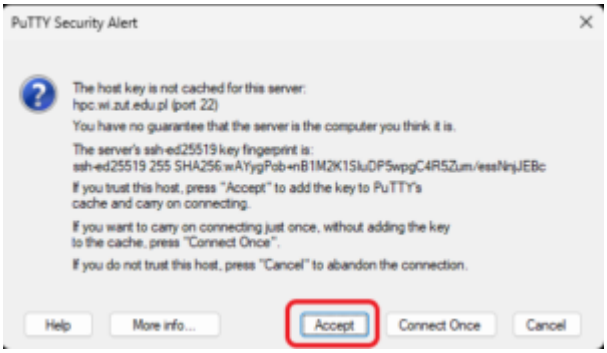
```
ip a
```



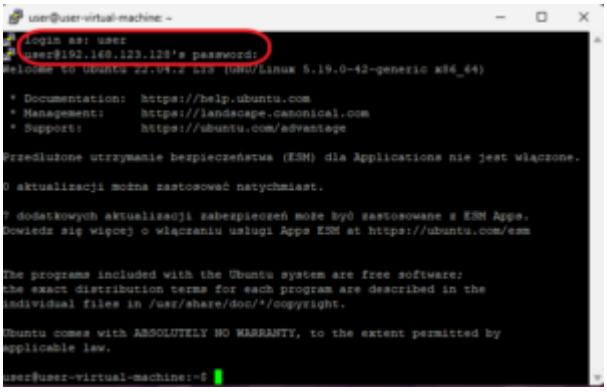


Po wpisaniu adresu zatwierdzamy poprzez „Open” i następnie zatwierdzamy klucze szyfrowania poprzez potwierdzenie certyfikatu serwera do którego

wykonujesz połączenie.

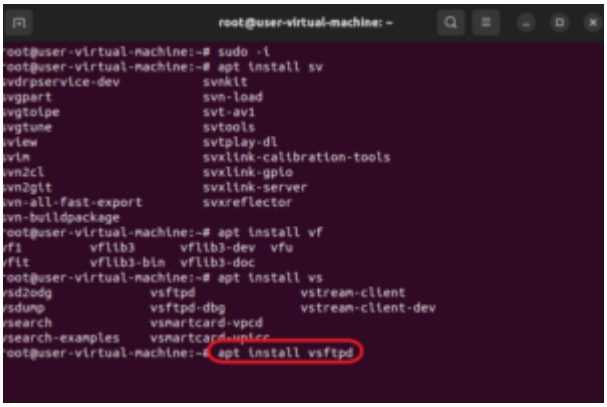


9. Logujemy się jako użytkownik **user** i hasłem **user**.



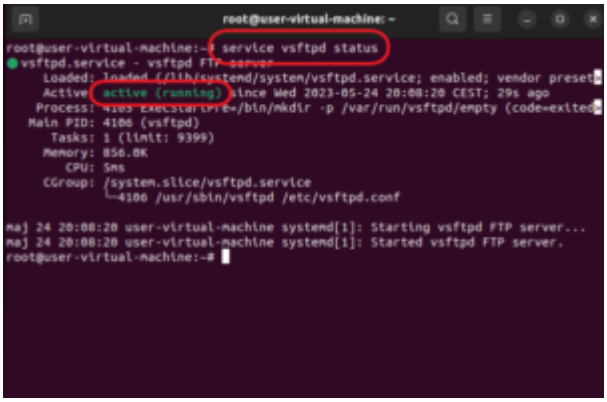
10. Możemy zamknąć okno putty poprzez skrót klawiszowy **CTRL-D** lub wykonując polecenie „**`logout`**„. Wracamy do maszyny wirtualnej i w konsoli instalujemy serwer FTP, którym bedzie pakiet „vsftpd”. Wykonaj polecenie:

```
apt install vsftpd
```

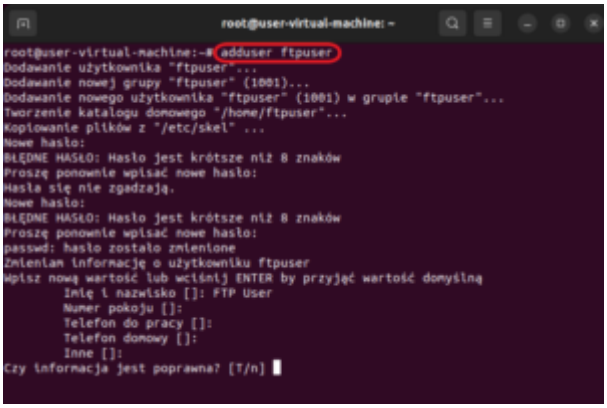


11. Sprawdzimy czy nasz serwer FTP działa

```
service vsftpd status
```



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



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/ftpuser/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 any mógł w tym folderze tylko on wgrywać dane

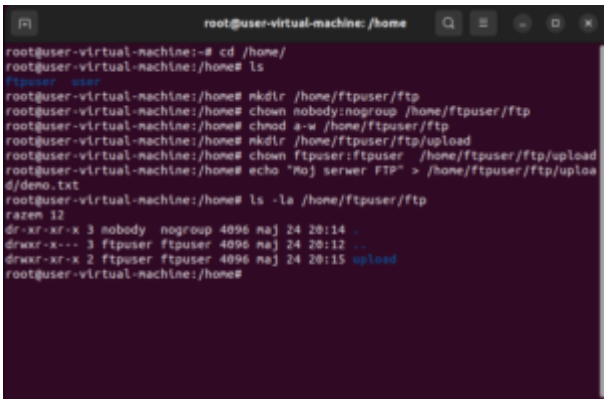
```
chown ftpuser:ftpuser /home/ftpuser/ftp/upload
```

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

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

Sprawdzimy czy uprawnienia są poprawne w folderze

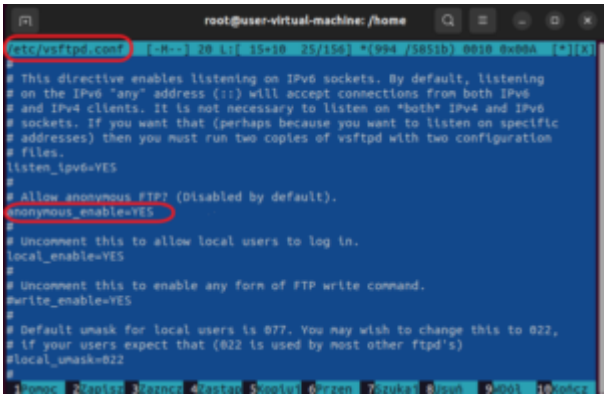
```
ls -al /home/ftpuser/ftp
```



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.

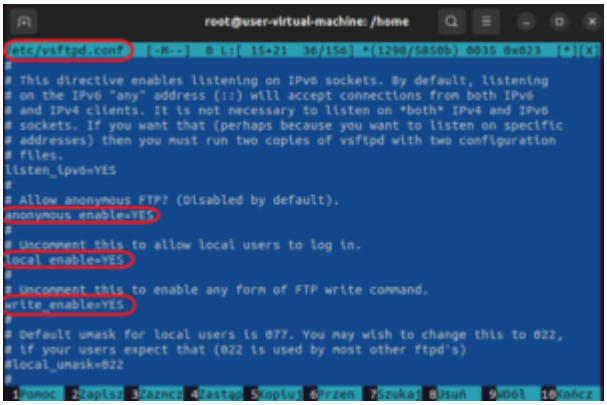
W pierwszej kolejności włączamy logowanie anonimowe ustawiając opcję „**anonymous_enable=YES**” (nie może być znaku hash „**#**” bo to oznacza komentarz



15. Następnie włączamy kolejno opcje:

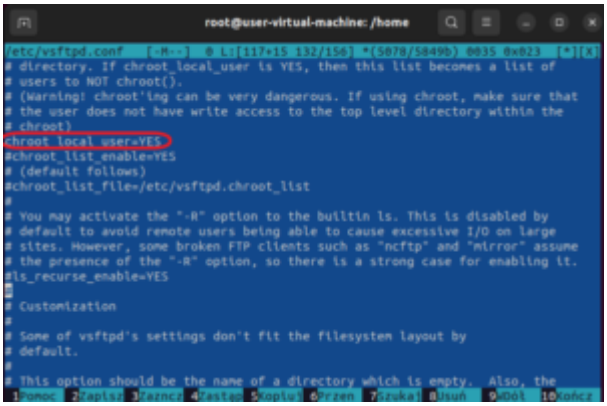
local_enable=YES

write_enable=YES



16. Dalej modyfikując konfigurację niżej w pliku włączamy opcję

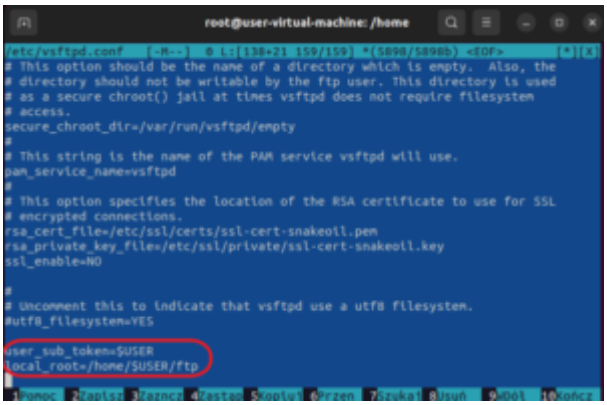
chroot_local_user=YES



17. Dodajemy na końcu pliku

user_sub_token=$USER

local_root=/home/$USER/ftp

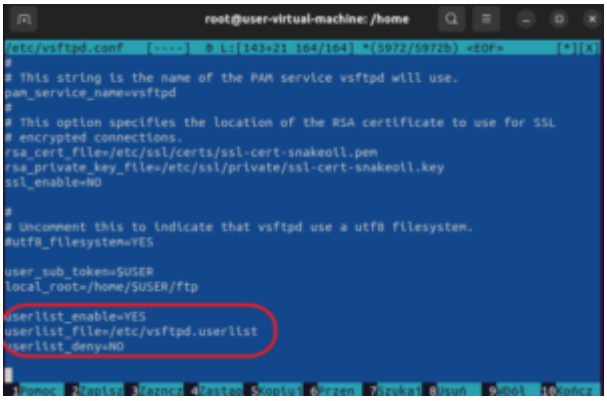


Przypiszemy kto może korzystać z FTP

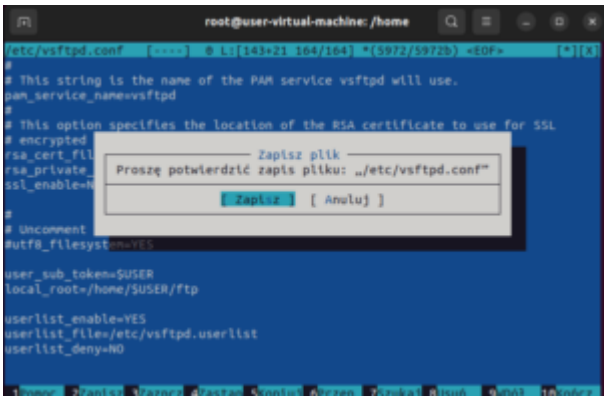
userlist_enable=YES

userlist_file=/etc/vsftpd.userlist

userlist_deny=NO

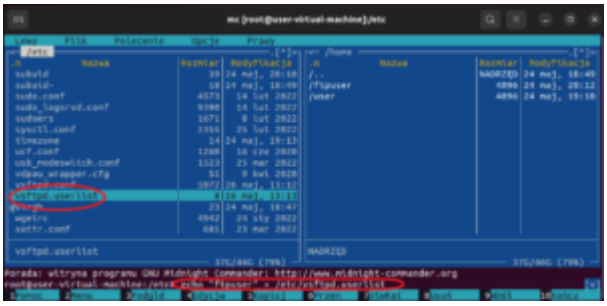


18. Zapisujemy plik konfiguracji poprzez klawisz F2 i zatwierdzamy poprzez Enter



19. Musimy utworzyć plik listy kont które mają dostęp do serwera FTP. Dodamy użytkownika ftpuser poleceniem

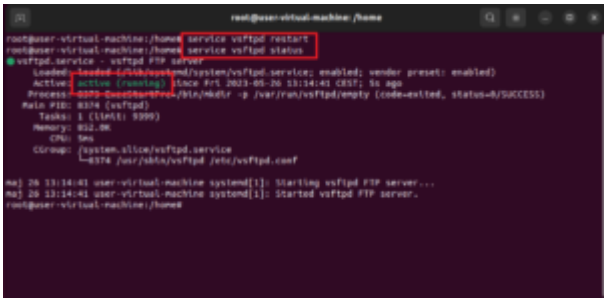
```
echo "ftpuser" > /etc/vsftpd.userlist
```



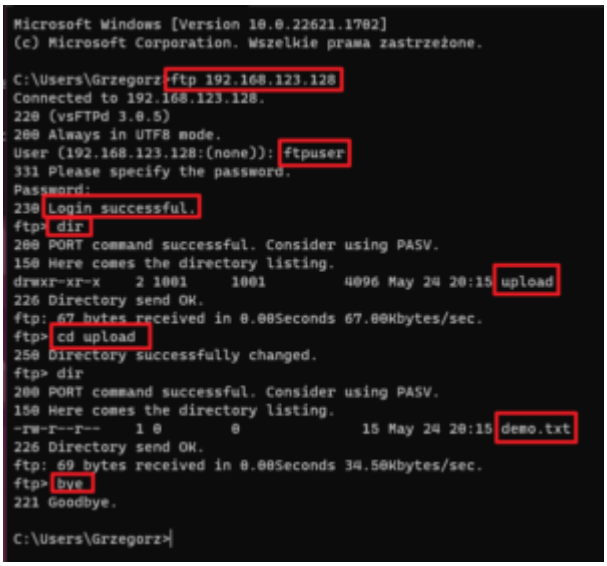
20. Restartujemy serwis vsftpd i sprawdzamy czy działa poprawnie

```
service vsftpd restart
```

```
service vsftpd status
```



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



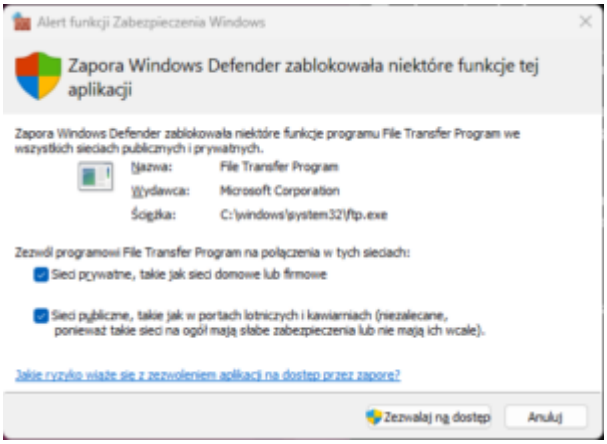
Wykonaj kolejno polecenia:

`ftp` *<tu swój adres IP>*

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

po prawidłowym zalogowaniu wykonaj komendę `dir`

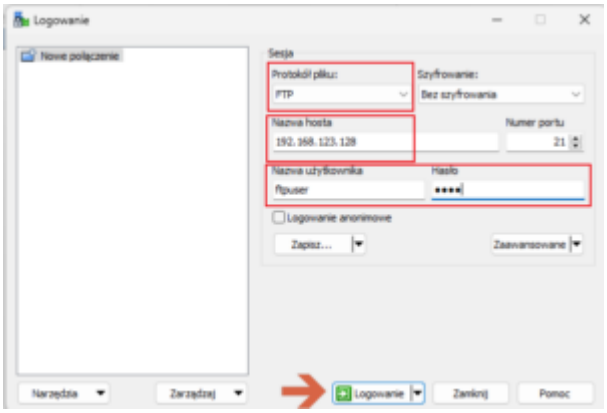
UWAGA – może pojawić się prośba o dopuszczenie komunikacji w ramach Firewall Windows – zezwój na nią w obu typach sieci Prywatnej i Publicznej



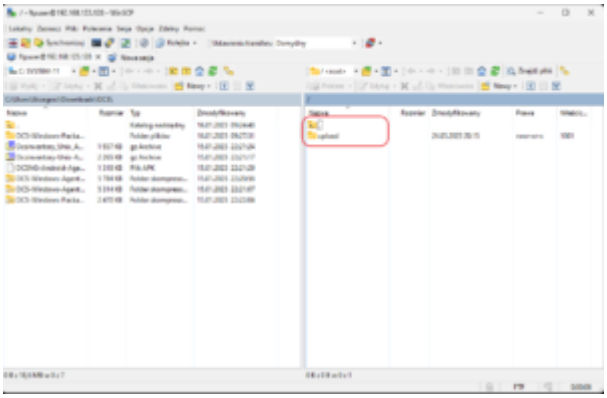
Przejdziemy do folderu **upload** i zobaczymy co zawiera poprzez polecenie `dir`

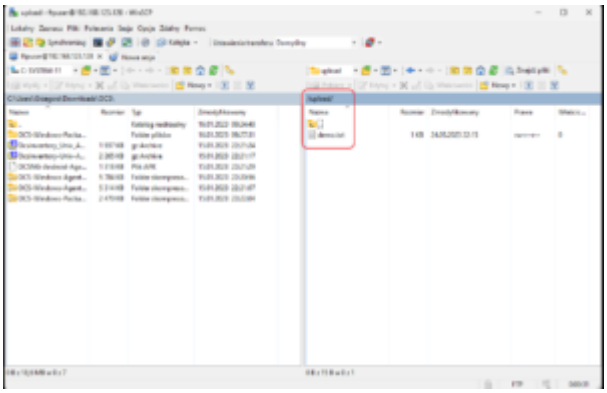
Na koniec rozłączymy się poleceniem bye

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”



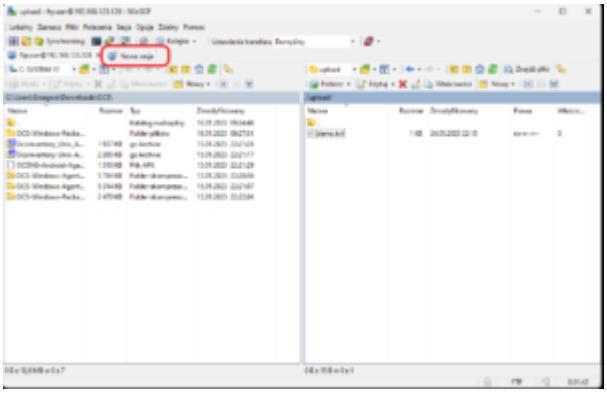
23. Po poprawnym zalogowaniu się dostaniesz się znowu do folderu ftp tego konta



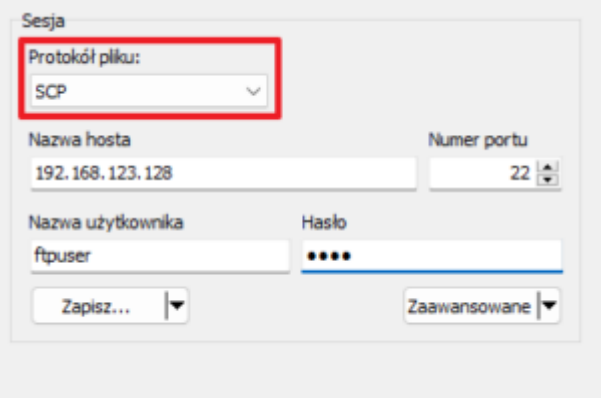


Połączenie po protokole FTP jest niezabezpieczone i przesyłane dane można w prosty sposób posłuchać – w tym loginy i hasła. Lepszym zabezpieczeniem było by wykorzystanie protokołów szyfrowanych. Może to być zrealizowane na bazie serwera FTP jednak należy wygenerować klucze publiczne i prywatne i odpowiednio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

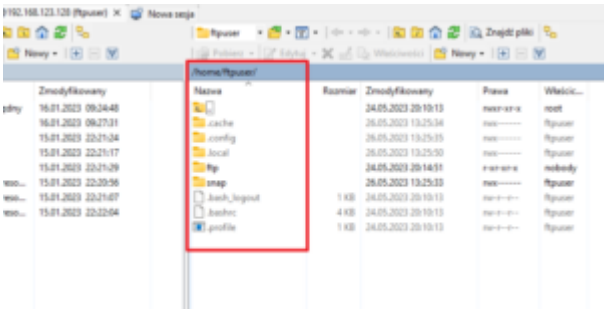
24. Otwórz nową sesję w ramach programu WinSCP.



Tym razem wybieramy protokół SCP i reszta bez zmian.

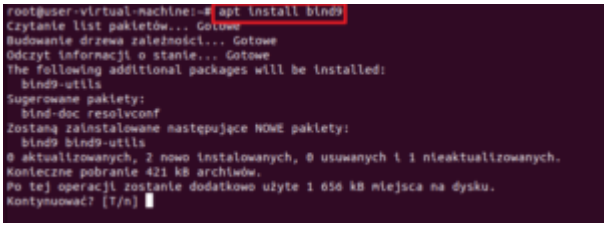


25. Po połączeniu zauważysz że widzisz więcej danych ponieważ nie ogranicza cię ustawienia serwera ftp. W tym przypadku otrzymujesz pełny dostęp do swojego konta i uprawnień jakie ono ma. Wadą tego rozwiązania jest niemożliwość połączenia się w trybie anonimowym.



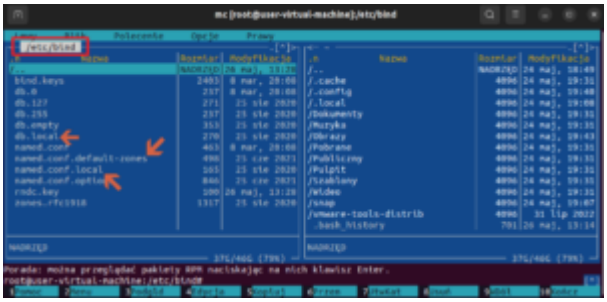
26. Przejdziemy do konfiguracji własnego serwera DNS. Potrzebujemy zainstalować takowy na naszym hoście – w tym celu wykonaj polecenie:

```
apt install bind9
```

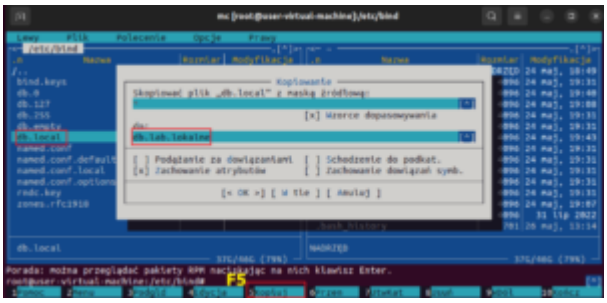


27. Uruchom polecenie `mc`. Przejdź do folderu `/etc/bind9`. Wewnątrz zobaczysz pliki konfiguracyjne serwera. Dla nas będą istotne:

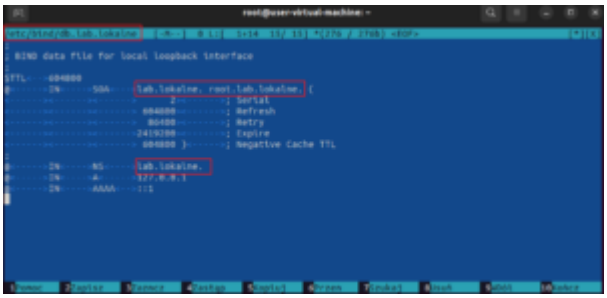
`db.local`
`named.conf.default-zones`
`named.conf.local`



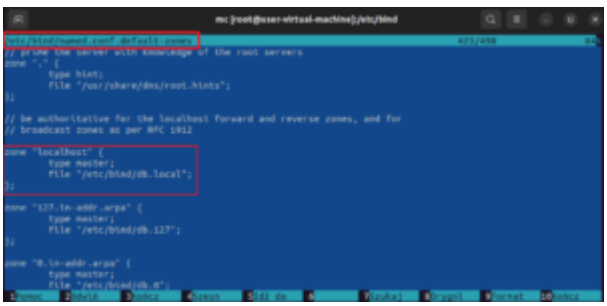
28. Ustaw się znacznikiem na pliku `db.local` i używając klawisza F5 wykonasz kopię tego pliku pod nową nazwą `db.lab.lokalne`



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

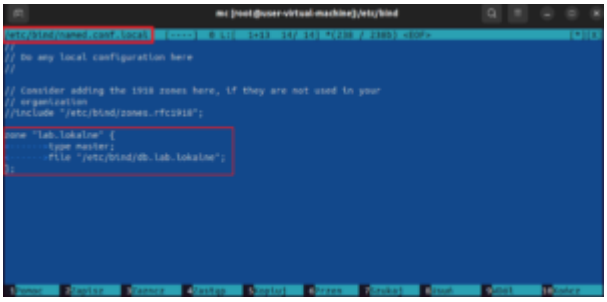


30. Teraz musimy edytować plik `named.conf.default-zones`. Z niego weźmiemy definicję strefy localhost (zaznaczony na obrazku obszar) i przeniesiemy dane do pliku `named.conf.local`



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

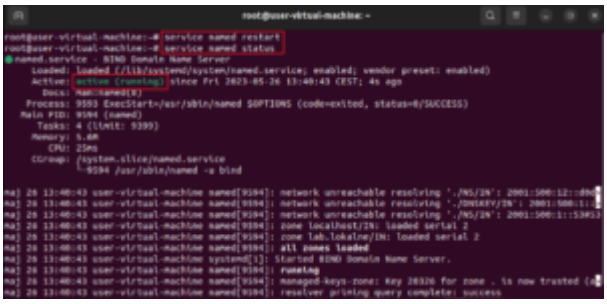
i poprawiamy informację o strefie (zamiast localhost -> lab.lokalne) oraz zmieniamy nazwę pliku strefy (zamiast db.local -> db.lab.lokalne)



32. Zrestartuj usługę DNS i sprawdź czy działa poprawnie.

```
service named restart
```

```
service named status
```



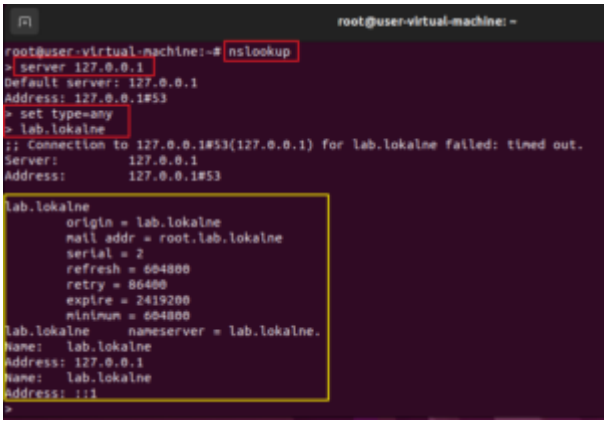
33. Wykonaj test działania serwera DNS. Wydaj w konsoli następujące polecenia jak na obrazku poniżej.

```
nslookup
```

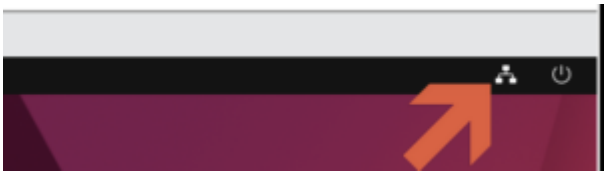
```
server 127.0.0.1
```

```
set type=any
```

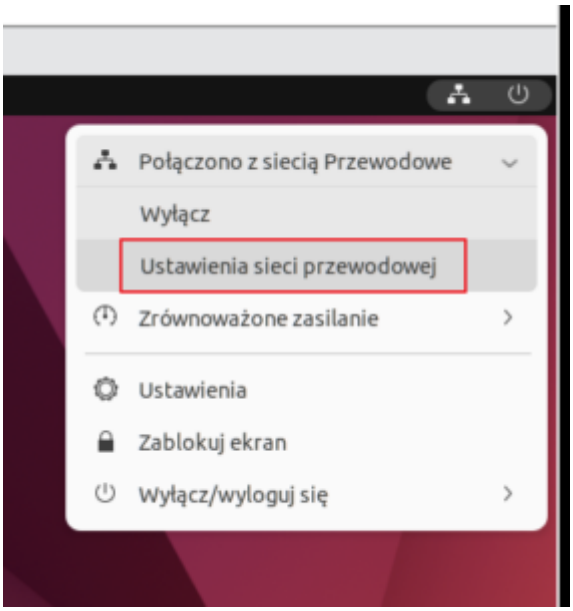
```
lab.lokalne
```



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

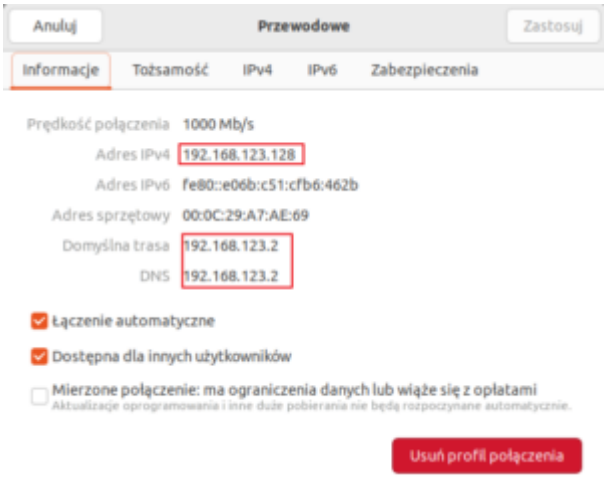


35. Wybierz ustawienia sieci przewodowej



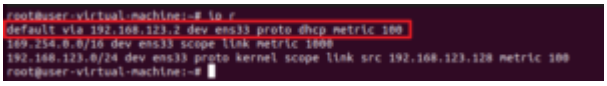
36. W ramach sieci wybierz ustawienia

37. Sprawdź dane ustawień sieciowych swojego komputera.

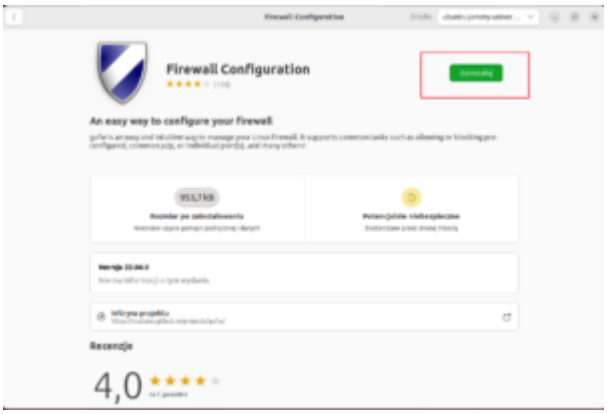


38 Teraz z konsoli postaramy się odczytać te dane bez wykorzystywania środowiska graficznego.

```
ip r
```

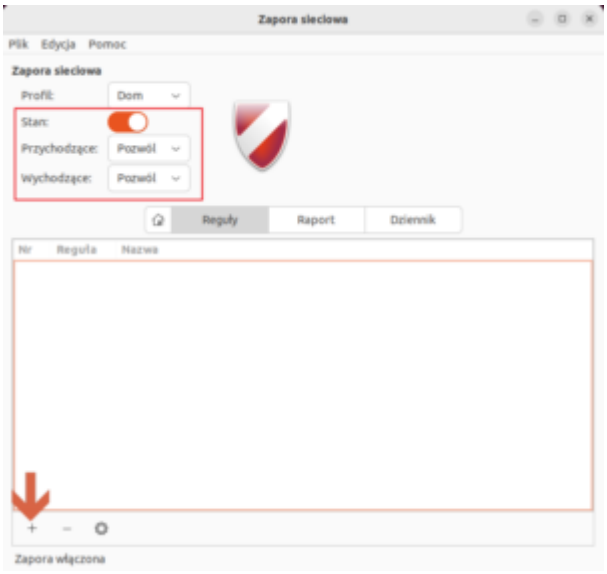


39. Zabezpieczenie swojej stacji jest bardzo ważne. Z każdego miejsca możemy spodziewać się ataku i próby przejęcia hosta. Powinnyśmy zadbać aby najlepiej jak można zabezpieczyć swój system. Ustawimy zaporę ogniową – FireWall. W pierwszej kolejności musimy doinstalować oprogramowanie do zarządzania oprogramowaniem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

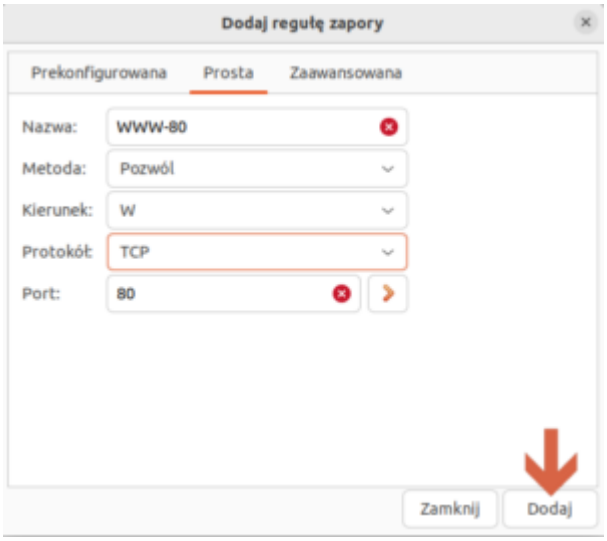


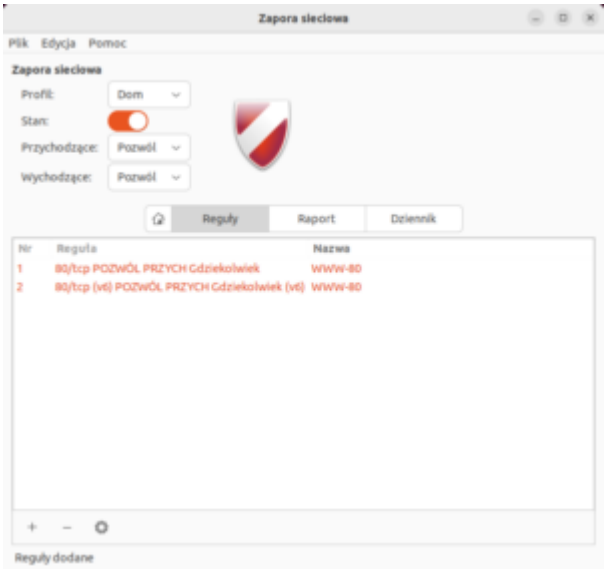
40. Uruchom oprogramowanie z dostępnych w aplikacjach.

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



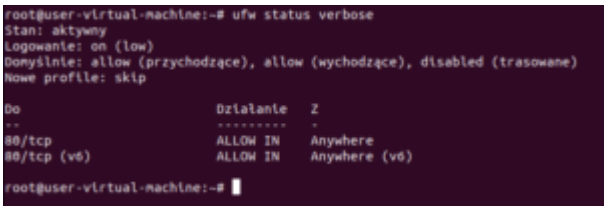
42. Poprzez znak + dodaj nową regułę pozwalającą na ruch przychodzący do serwera WWW działającego na porcie 80. Nazwij tą regułę WWW-80.





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

```
ufw status verbose
```



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