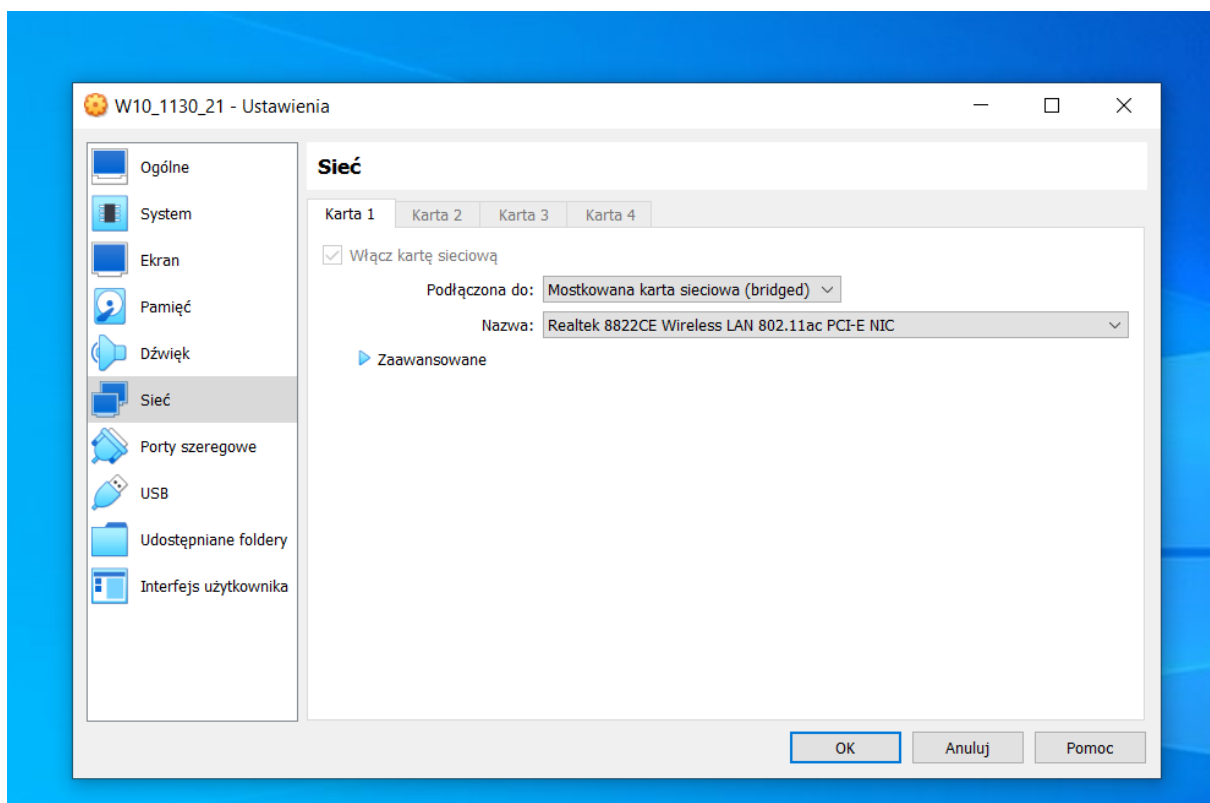


1. W maszynie wirtualnej *VirtualBox* ustawić kartę sieciową w trybie „Karta mostkowana (bridged)”.



2. W środowisku maszyny wirtualnej sprawdzić przydzielony adres IP za pomocą polecenia konsolowego **ipconfig**.

```
C:\Users\Win10_A>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2a00:f41:833:ddcd:509b:27e6:ee1b:5037
    Temporary IPv6 Address. . . . . : 2a00:f41:833:ddcd:a099:f4bb:8a7e:bba3
    Link-local IPv6 Address . . . . . : fe80::a4e4:ab8f:802d:b8d0%13
    IPv4 Address. . . . . : 192.168.248.218
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::8076:c7ff:fe65:3199%13
                                192.168.248.90
```

3. W środowisku gospodarza sprawdzić przydzielony adres IP za pomocą polecenia konsolowego **ipconfig**.

```

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2a00:f41:833:ddcd:d732:f566:42:8cf4
    Temporary IPv6 Address. . . . . : 2a00:f41:833:ddcd:90d6:d61d:32de:47b2
    Link-local IPv6 Address . . . . . : fe80::35fc:fd4e:8b05:92dc%5
    IPv4 Address. . . . . : 192.168.248.104
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::8076:c7ff:fe65:3199%5
                                192.168.248.90

```

4. W środowisku gospodarza upewnić się, czy maszyna wirtualna odpowiada na zapytania poleceniem konsolowym **ping**

```

C:\Users\admin>ping 192.168.248.218

Pinging 192.168.248.218 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.248.218:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

```

Nie odpowiada

5. a) wyłączyć Zaporę Windows

### Sieć prywatna

Sieci w domu lub w miejscu pracy, w których znajdują się znajome i zaufane osoby i urządzenia, a urządzenie jest ustawione jako wykrywalne.

### Aktywne sieci prywatne

 Sieć 2

### Zapora Microsoft Defender

Pomaga chronić urządzenie w sieci prywatnej.



Zapora prywatna jest wyłączona. Urządzenie może być podatne na zagrożenia.

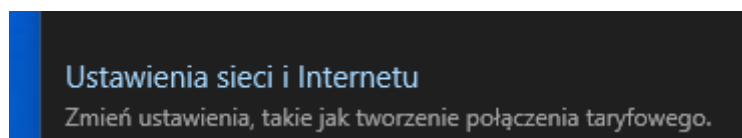


Wyłączone

b) wybrać odpowiednią regułę z istniejących i nieaktywnych reguł zapy

c) utworzyć nową regułę w Zaporze Windows, która zezwala na odpowiedzi polecenia **ping**

Klikamy Ustawienia sieci i Internetu



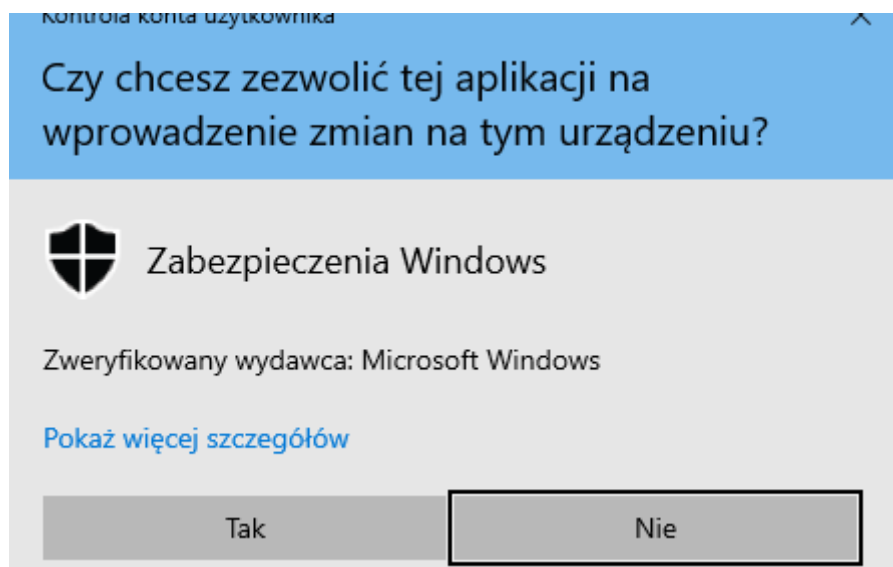
Potem Zapora systemu Windows

[Zapora systemu Windows](#)

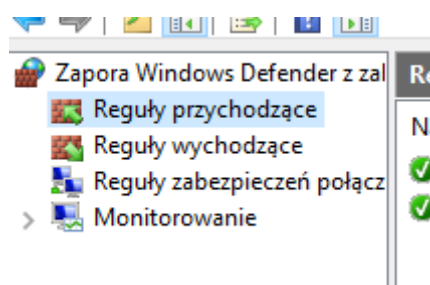
Potem Ustawienia zaawansowane

[Ustawienia zaawansowane](#)

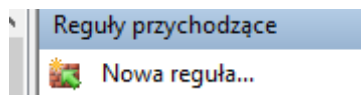
Klikamy Tak



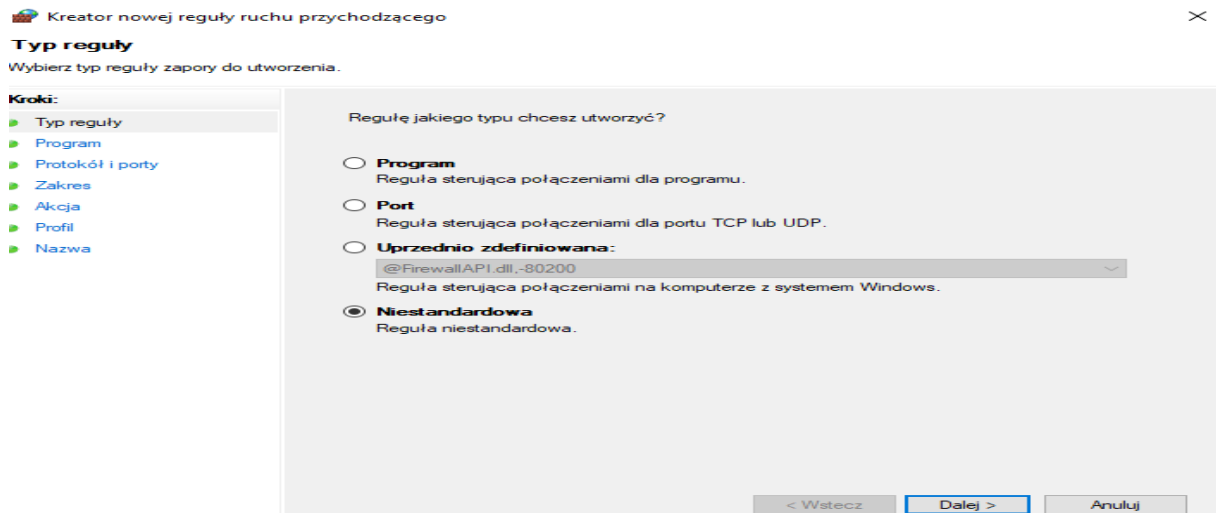
Klikamy Reguły przychodzące



Klikamy nową regułę



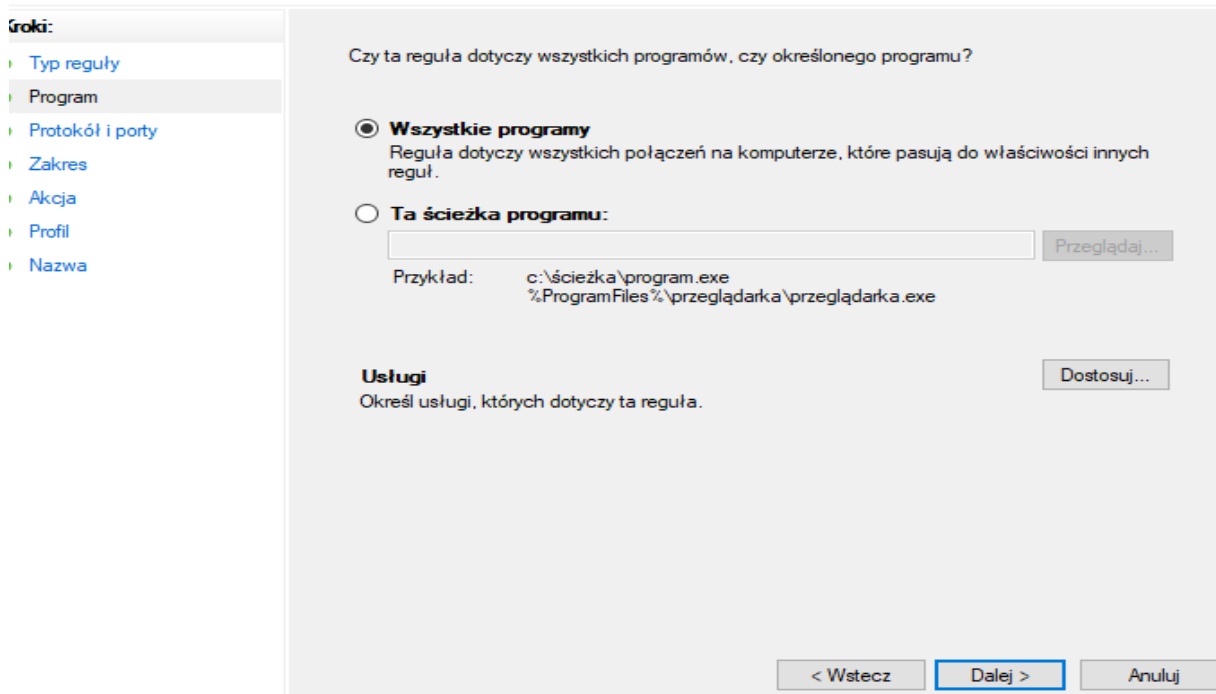
Wybieramy Niestandardowa i klikamy dalej



Wybieramy Wszystkie programy i klikamy dalej

#### Program

Określ pełną ścieżkę i nazwę pliku wykonywalnego programu, którego dotyczy ta reguła.



Wybieramy ICMPv4 i klikamy dostosuj

Kreator nowej reguły ruchu przychodzącego

## Protokół i porty

Określ protokoły i porty, których dotyczy ta reguła.

**Kroki:**

- Typ reguły
- Program
- Protokół i porty**
- Zakres
- Akcja
- Profil
- Nazwa

Których protokołów i portów dotyczy ta reguła?

Typ protokołu: ICMPv4

Numer protokołu: 1

Port lokalny: Wszystkie porty

Port zdalny: Wszystkie porty

Przykład: 80, 443, 5000-5010

Przykład: 80, 443, 5000-5010

Ustawienia protokołu komunikacyjnego sterowania Internetem (ICMP): Dostosuj...

< Wstecz Dalej > Anuluj

Wybieramy Określone typy ICMP i Żądanie echa oraz klikamy OK

Dostosowywanie ustawień protokołu ICMP

Zastosuj tę regułę do następujących połączeń używających protokołu komunikacyjnego sterowania Internetem ICMP:

☐ Wszystkie typy ICMP

☒ Określone typy ICMP

- ☐ Zbyt duży pakiet
- ☐ Miejsce docelowe nieosiągalne
- ☐ Wygaszenie źródła
- ☐ Przekieruj
- ☒ Żądanie echa
- ☐ Anons routera
- ☐ Żądanie routera
- ☐ Przekroczony limit czasu
- ☐ Problem z parametrem
- ☐ Żądanie sygnatury czasowej
- ☐ Żądanie maski adresu

Ten typ ICMP:

Typ: 0 Kod: Dowolne Dodaj

OK Anuluj

## Klikamy dalej

lokalne i zdalne adresy IP, których dotyczy ta reguła.

The screenshot shows a configuration window for an IPsec rule. On the left is a sidebar with a tree view containing the following items: 'reguły', 'ram', 'skół i porty', 'es', 'a', 'l', and 'na'. The main area is titled 'Których lokalnych adresów IP dotyczy ta reguła?' (Which local IP addresses does this rule apply to?). It has two radio button options: 'Dowolny adres IP' (selected) and 'Te adresy IP:'. Below the second option is a large empty text box for specifying IP addresses. To the right of this box are three buttons: 'Dodaj...', 'Edytuj...', and 'Usuń'. Below this section is a label 'Dostosuj typy interfejsów, których dotyczy ta reguła:' followed by a 'Dostosuj...' button. The next section is titled 'Których zdalnych adresów IP dotyczy ta reguła?' (Which remote IP addresses does this rule apply to?). It also has two radio button options: 'Dowolny adres IP' (selected) and 'Te adresy IP:'. Below the second option is another large empty text box. To the right of this box are three buttons: 'Dodaj...', 'Edytuj...', and 'Usuń'. At the bottom right of the window are three buttons: '< Wstecz', 'Dalej >' (highlighted with a blue border), and 'Anuluj'.

## Wybieramy Zezwalaj na połączenie i klikamy dalej

w przypadku, gdy połączenie spełnia warunki określone w regule.

The screenshot shows the 'Action' tab of the IPsec rule configuration window. The title is 'Jaką akcję należy wykonać, gdy połączenie spełnia określone warunki?' (What action should be taken when the connection meets the specified conditions?). There are three radio button options: 'Zezwalaj na połączenie' (selected), 'Zezwalaj na połączenie, jeśli jest bezpieczne', and 'Zablokuj połączenie'. The 'Zezwalaj na połączenie' option has a description: 'Obejmuje połączenia chronione za pomocą protokołu IPsec, jak i połączenia niechronione.' The 'Zezwalaj na połączenie, jeśli jest bezpieczne' option has a description: 'Obejmuje tylko połączenia uwierzytelnione przy użyciu protokołu IPsec. Połączenia będą zabezpieczane przy użyciu ustawień określonych we właściwościach protokołu IPsec i reguł zawartych w węźle Reguła zabezpieczeń połączenia.' Below the descriptions is a 'Dostosuj...' button. At the bottom right of the window are three buttons: '< Wstecz', 'Dalej >' (highlighted with a blue border), and 'Anuluj'.

Klikamy dalej

Kiedy ma zastosowanie ta reguła?

- ☒ **Domena**  
Ma zastosowanie, gdy komputer jest połączony ze swoją domeną firmową.
- ☒ **Prywatny**  
Ma zastosowanie, gdy komputer jest połączony z lokalizacją w sieci prywatnej, na przykład w domu lub w miejscu pracy.
- ☒ **Publiczny**  
Ma zastosowanie, gdy komputer jest połączony z lokalizacją w sieci publicznej.

< Wstecz Dalej > Anuluj

Wpisujemy nazwę i klikamy Zakończ

Nazwa:  
PING ICMPv4

Opis (opcjonalnie):

< Wstecz Zakończ Anuluj

Reguły przychodzące		
Nazwa	Grupa	Profil
PING ICMPv4		Wszys...
@FirewallAPI.dll,-80201	@FirewallAPI.dll,-80200	Wszys...

Teraz polecenie ping działa

```
C:\Users\admin>ping 192.168.248.218

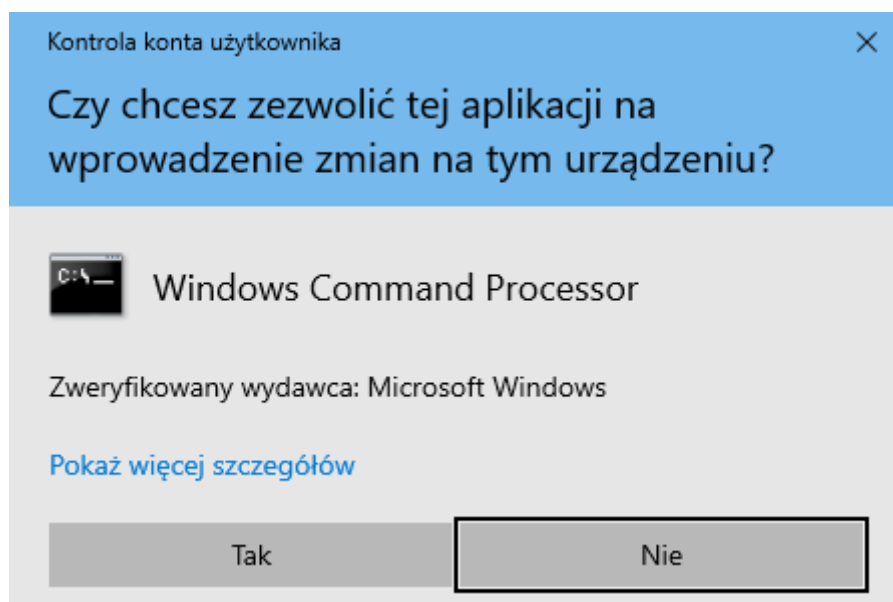
Pinging 192.168.248.218 with 32 bytes of data:
Reply from 192.168.248.218: bytes=32 time<1ms TTL=128
Reply from 192.168.248.218: bytes=32 time<1ms TTL=128
Reply from 192.168.248.218: bytes=32 time<1ms TTL=128
Reply from 192.168.248.218: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.248.218:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\admin>
```

6. Utworzyć nowe konto użytkownika z niepustym hasłem w maszynie wirtualnej.

Uruchamiamy wiersz poleceń jako administrator



Wyświetlamy listę kont

```
C:\Windows\system32>net user

Konta użytkowników dla \\DESKTOP-OGGFAFO

-----
Administrator          Gość                    Konto domyślne
WDAGUtilityAccount      Win10_A
Polecenie zostało wykonane pomyślnie.

C:\Windows\system32>
```

Wpisujemy net user {nazwa konta} {hasło} /ADD



```
C:\Windows\system32>net user NOWE_KONTO haslo123PL /ADD
Polecenie zostało wykonane pomyślnie.
```

Sprawdzamy

```
C:\Windows\system32>net user NOWE_KONTO
Nazwa użytkownika          NOWE_KONTO
Pełna nazwa
Komentarz
Komentarz użytkownika
Kod kraju/regionu          000 (Domyślne ustawienia systemu)
Konto jest aktywne         Tak
Wygasanie konta            Nigdy

Hasło ostatnio ustawiano    17.03.2023 23:20:24
Ważność hasła wygasa        28.04.2023 23:20:24
Hasło może być zmieniane    17.03.2023 23:20:24
Wymagane jest hasło         Tak
Użytkownik może zmieniać hasło Tak
```

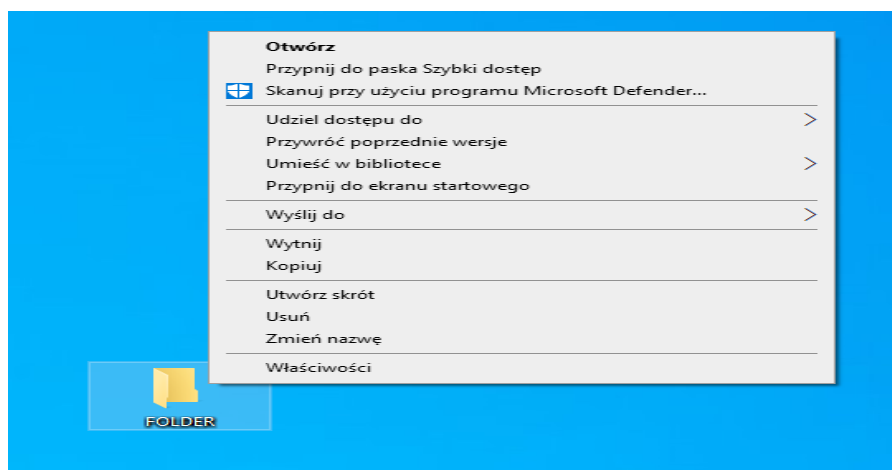
Nowe konto zostało utworzone razem z niepustym hasłem

```
C:\Windows\system32>net user

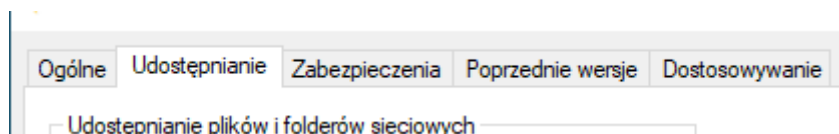
Konta użytkowników dla \\DESKTOP-OGGFAFO
-----
Administrator      Gość      Konto domyślne
NOWE_KONTO          WDAGUtilityAccount Win10_A
Polecenie zostało wykonane pomyślnie.
```

7. Ustawić uprawnienia NTFS do folderu, aby zezwolić na zapis tylko dla tego użytkownika i odczyt wszystkim innym użytkownikom.

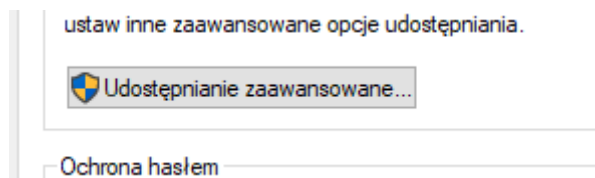
Klikamy na folder prawym przyciskiem i klikamy Właściwości



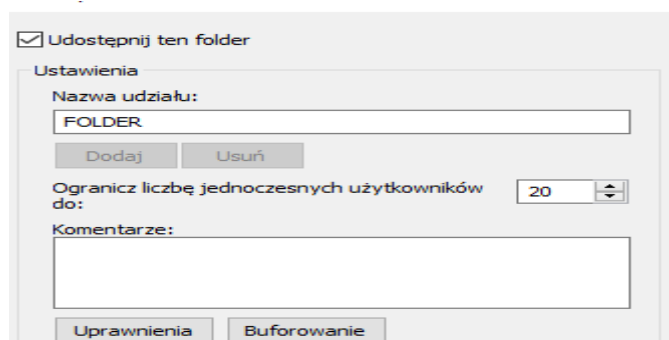
## Klikamy Udostępnianie



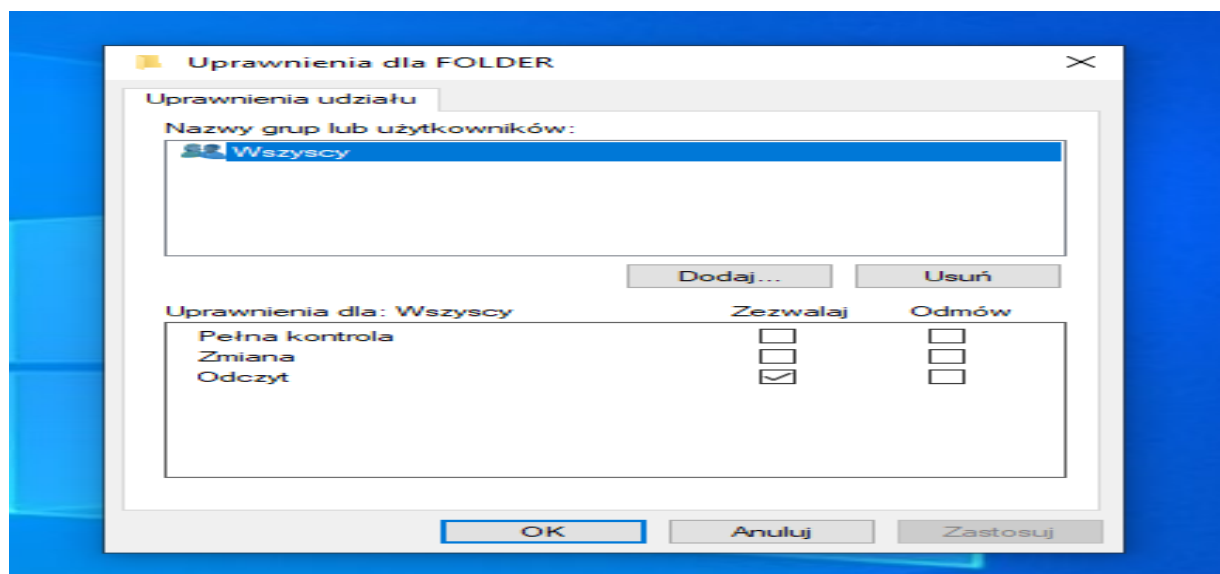
## Klikamy Udostępnianie zaawansowane



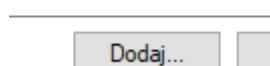
## Zaznaczamy Udostępnij ten folder i klikamy Uprawnienia



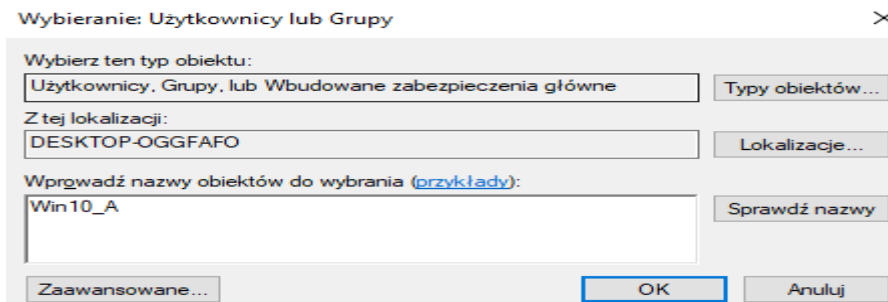
## Zaznaczamy odczyt dla Wszystkich



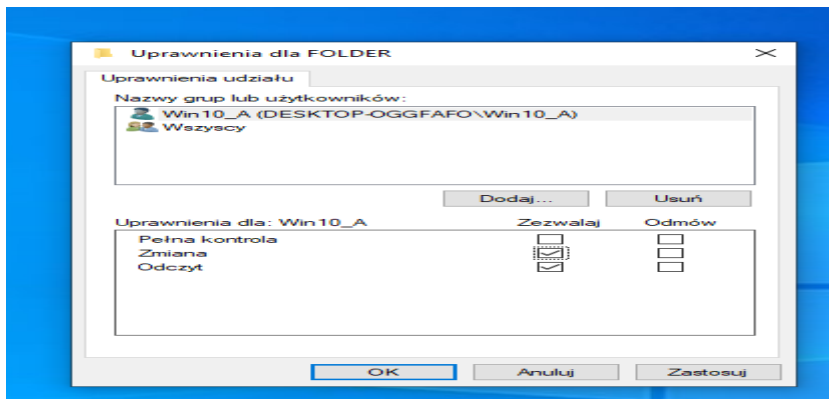
## Klikamy Dodaj...



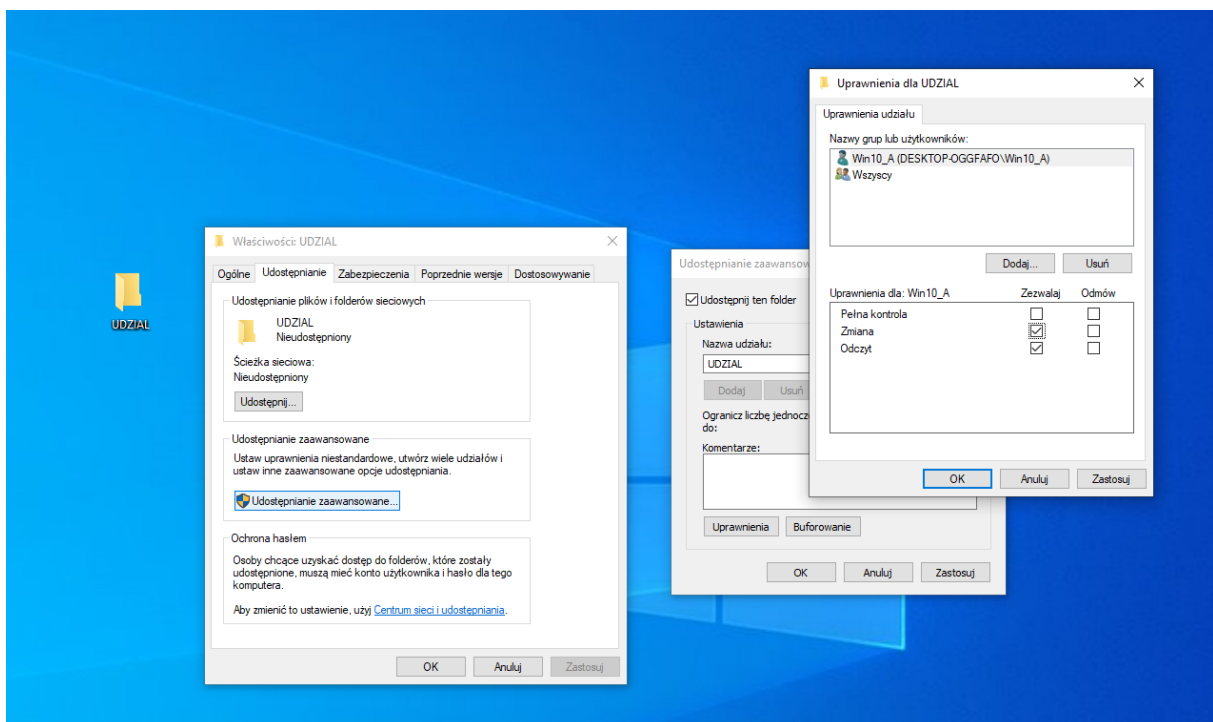
Wpisujemy nazwę Win10\_A i klikamy OK

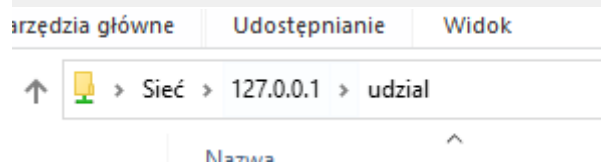
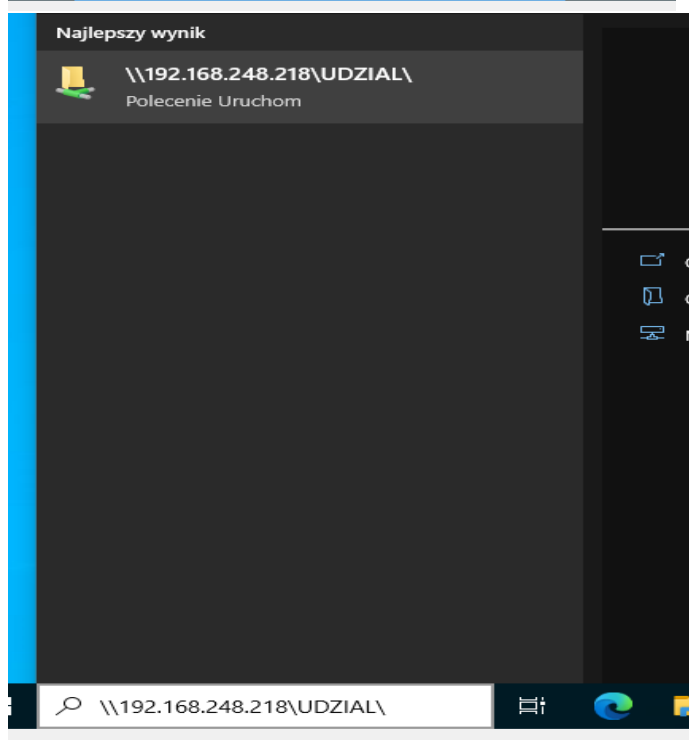
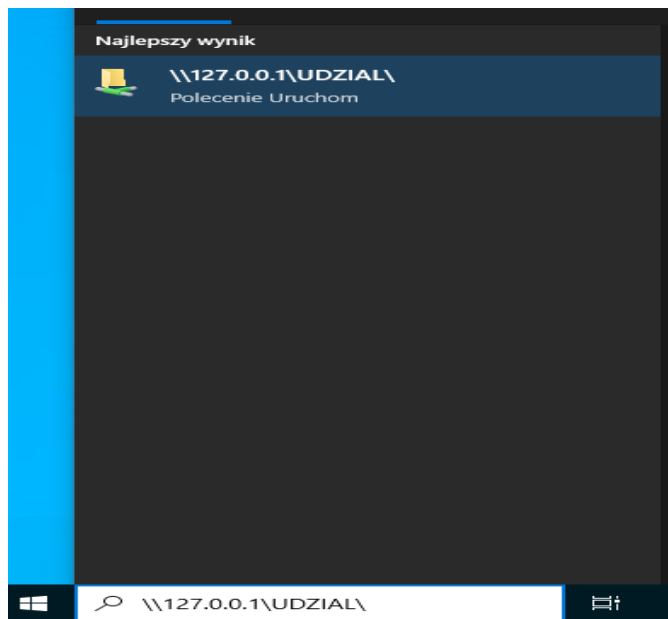


Klikamy Win10\_A i zaznaczamy Zmiana i klikamy OK



8. W maszynie wirtualnej udostępnić katalog (folder) o nazwie UDZIAŁ w trybie umożliwiającym również zapis dla aktualnego użytkownika.





9. Z systemu operacyjnego gospodarza wejść do udostępnionego katalogu i dodać w nim pusty plik tekstowy.

Zabezpieczenia Windows

Wprowadzanie poświadczeń sieciowych

Wprowadź poświadczenia, aby połączyć z: 192.168.248.218

☐ Zapamiętaj moje poświadczenia

OK

Anuluj