

Uniwersytet Morski w Gdyni

przedmiot:

Narzędzia Informatyczne

Ćw. ~~6~~ Dostęp i kontrola zdalna

1. Cel ćwiczenia

Celem ćwiczenia jest przedstawienie sposobów kontroli zdalnej urządzeń z systemami Windows.

2. Wprowadzenie

System operacyjny Windows posiada wbudowane narzędzia służące do zdalnej kontroli systemu operacyjnego. Istnieją też dedykowane systemowi Windows rozwiązania firm trzecich. Najpopularniejszymi narzędziami do zdalnego dostępu są:

- Pomoc zdalna – program wbudowany w system operacyjny Windows służący do udzielania zdalnej pomocy. Wymaga od użytkownika wysłania pliku dostępowego oraz hasła, następnie osoba otrzymująca te dane może połączyć się z komputerem i udzielić pomocy. Jest to proste rozwiązanie, służące raczej do udzielania pomocy w obsłudze jakiegoś programu drugiej osobie.
- TeamViewer – jest to program służący do udzielania zdalnej pomocy. Wymaga od użytkownika podania identyfikatora i hasła, następnie osoba otrzymująca te dane może połączyć się z komputerem i udzielić pomocy. Rozwiązanie jest to bardziej rozbudowanym odpowiednikiem Pomocy zdalnej, ponieważ pozwala na kontrolę komputera w szerokim zakresie.
- Pulpit zdalny – program wbudowany w system operacyjny Windows służący do przejęcia kontroli nad drugim komputerem w sieci. Nie wymaga żadnych danych dostępowych (jedynie adres IP, nazwa użytkownika i hasło). Rozwiązanie świetnie nadaje się do przejmowania kontroli nad serwerami z poziomu serwera głównego (np. kontrola serwerów znajdujących się w innych placówkach firmy przez administratora znajdującego się w placówce macierzystej).
- TightVNC – jest to bardzo mały program służący do kontroli zdalnej. Jest odpowiednikiem pulpitu zdalnego dostępnym dla szerokiego zakresu systemów operacyjnych. Wymaga jedynie adresu IP, nazwy użytkownika oraz hasła. Zastosowania są identyczne jak w przypadku pulpitu zdalnego.
- Putty – jest to program pozwalający na zdalne wydawanie poleceń terminalowych przez protokół SSH. Rozwiązanie dostępne jest na szerokim zakresie systemów operacyjnych. Narzędzie to świetne jest w przypadku, gdy administrator potrzebuje dostępu jedynie do terminala (by wydawać polecenia tekstowe), a GUI jest zbędne. Taka sytuacja występuje głównie w środowiskach Linux'owych, m.in. do kontroli serwerów.

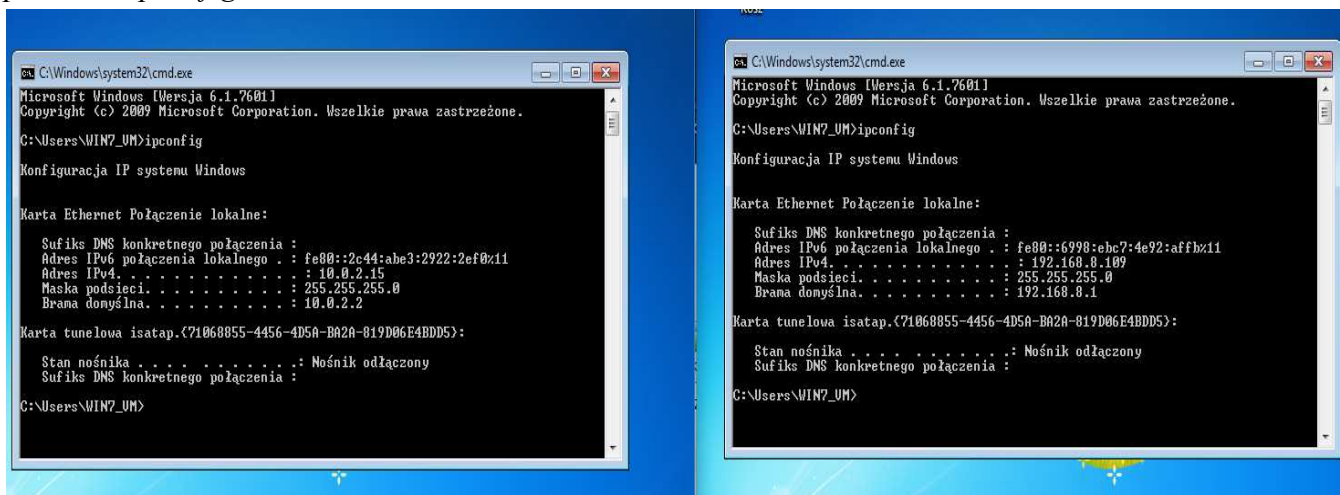
3. Przykłady

Poniższa instrukcja przedstawia przykładowe zastosowanie Pomocy zdalnej, TeamViewera, Pulpitu

Zdalnego, Pulpitu zdalnego oraz TightVNC.

W pierwszej kolejności zajmijmy się programami do pomocy zdalnej, czyli *Pomoc zdalna* oraz *TeamViewer*. Skonfigurujemy karty sieciowe wirtualnych maszyn z Windowsem, tak aby działały różnych sieciach i połączenie musiało odbywać się przez Internet. Interfejs sieciowy maszyny, która będzie zdalnej pomocy udzielała skonfigurujemy jako *NAT*. Natomiast interfejs maszyny, której pomoc będzie udzielana jako *Mostkowana karta sieciowa* - można by skonfigurować ten interfejs również jako *NAT*, ale nie chcemy aby komputer znajdował się w podwójnej translacji (pierwszej wynikającej z konfiguracji VirtualBox jako *NAT*, a drugiej z powodu podłączenia komputera macierzystego do routera z włączoną translacją *NAT*), ponieważ program *Pomoc zdalna* może nie poradzić sobie z taką infrastrukturą sieciową i nie będzie w stanie prawidłowo obsłużyć żądań połączenia. *TeamViewer* natomiast nie powinien mieć żadnych problemów, ponieważ do obsługi połączenia używane są zewnętrzne serwery (nie jest to połączenie P2P, jak w przypadku *Pomoc zdalna*).

W tym przypadku na maszynie pierwszej skonfigurowano interfejs jako *NAT*, a na drugiej jako *Mostkowana karta sieciowa*. Następnie sprawdzono adresację na obu komputerach za pomocą polecenia *ipconfig*.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Wersja 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Wszelkie prawa zastrzeżone.

C:\Users\WIN7_UM>ipconfig

Konfiguracja IP systemu Windows

Karta Ethernet Połączenie lokalne:

    Sufiks DNS konkretnego połączenia :
    Adres IPv6 połączenia lokalnego . : fe80::2c44:abe3:2922:2ef0x11
    Adres IPv4 . . . . . : 10.0.2.15
    Maska podsieci . . . . . : 255.255.255.0
    Brana domyślna . . . . . : 10.0.2.2

Karta tunelowa isatap.{71068855-4456-4D5A-BA2A-819D06E4BDD5}:

    Stan nośnika . . . . . : Nośnik odłączony
    Sufiks DNS konkretnego połączenia :

C:\Users\WIN7_UM>
```

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Wersja 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Wszelkie prawa zastrzeżone.

C:\Users\WIN7_UM>ipconfig

Konfiguracja IP systemu Windows

Karta Ethernet Połączenie lokalne:

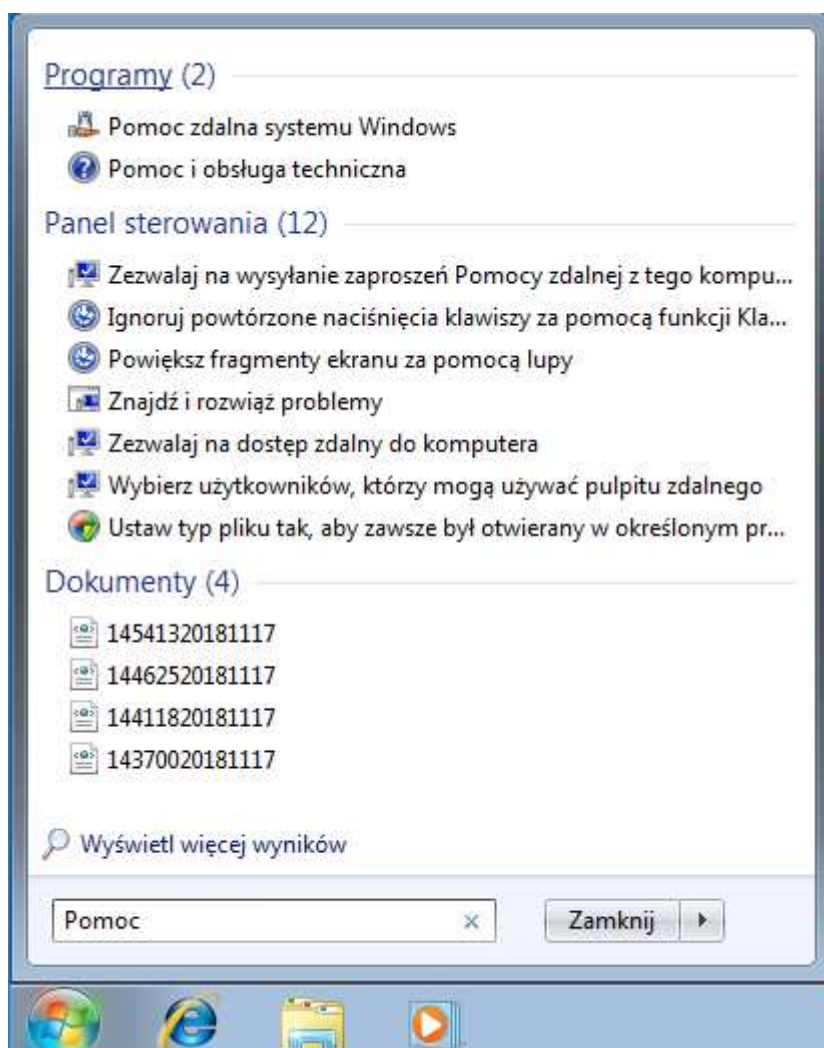
    Sufiks DNS konkretnego połączenia :
    Adres IPv6 połączenia lokalnego . : fe80::6990:abc7:4e92:affbx11
    Adres IPv4 . . . . . : 192.168.8.109
    Maska podsieci . . . . . : 255.255.255.0
    Brana domyślna . . . . . : 192.168.8.1

Karta tunelowa isatap.{71068855-4456-4D5A-BA2A-819D06E4BDD5}:

    Stan nośnika . . . . . : Nośnik odłączony
    Sufiks DNS konkretnego połączenia :

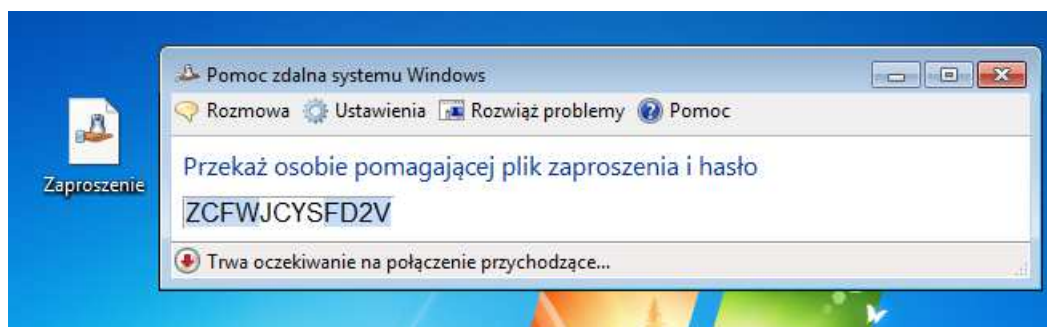
C:\Users\WIN7_UM>
```

Na maszynie drugiej uruchomiono *Pomoc zdalna systemu Windows*



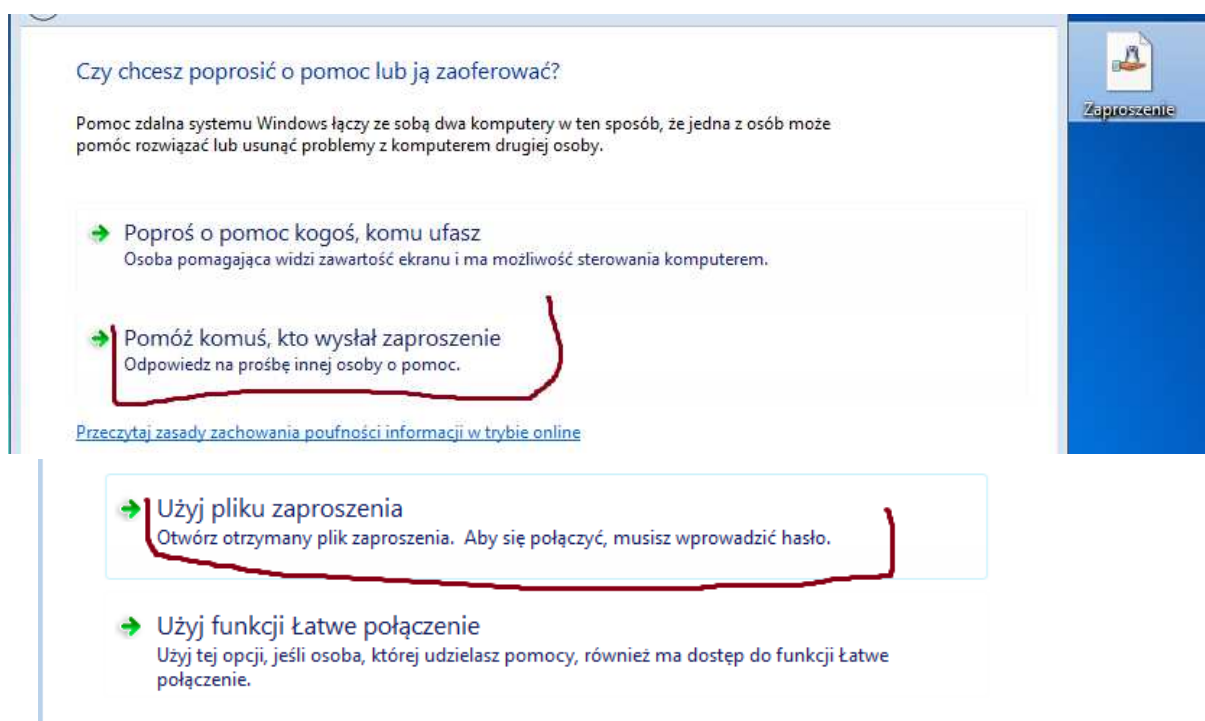
Wybrano opcję *Poproś o pomoc kogoś, komu ufasz*, a następnie *Zapisz to zaproszenie jako plik*.

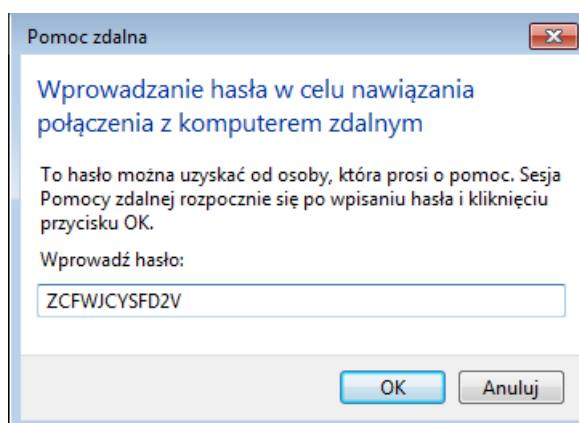
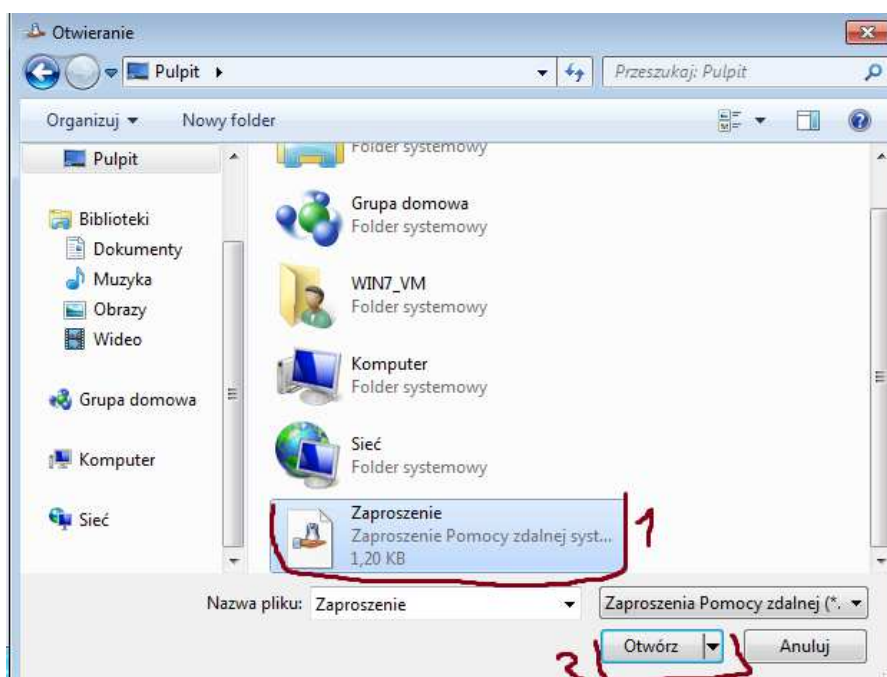
- ➔ **Poproś o pomoc kogoś, komu ufasz**
Osoba pomagająca widzi zawartość ekranu i ma możliwość sterowania komputerem.
- ➔ **Pomóż komuś, kto wysłał zaproszenie**
Odpowiedz na prośbę innej osoby o pomoc.
- ➔ **Zapisz to zaproszenie jako plik**
W przypadku używania poczty e-mail w sieci Web można wysłać to zaproszenie jako załącznik.
- ➔ **Użyj poczty e-mail do wysłania zaproszenia**
Jeśli używany program poczty e-mail jest zgodny, wybranie tej opcji spowoduje uruchomienie go i dołączenie pliku zaproszenia.
- ➔ **Użyj funkcji łatwe połączenie**
Użyj tej opcji, jeśli osoba pomagająca również ma dostęp do funkcji łatwe połączenie.



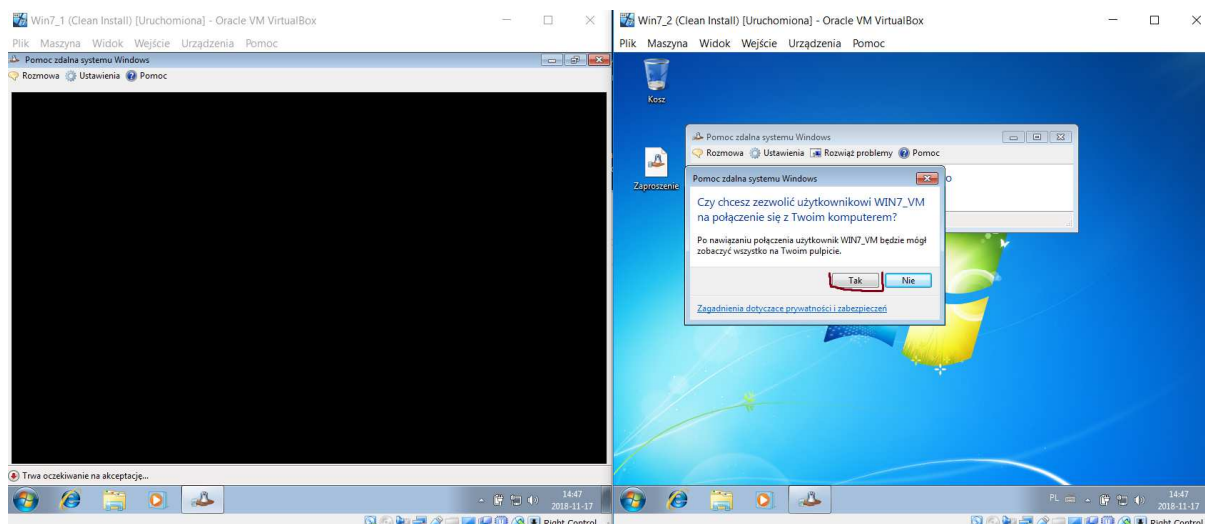
Skopiowano plik zaproszenia i hasło na maszynę pierwszą.

Uruchomiono narzędzie pomocy, wybrano opcję *Pomóż komuś, kto wysłał zaproszenie*, następnie *Użyj pliku zaproszenia* oraz wybrano plik i wprowadzono hasło.

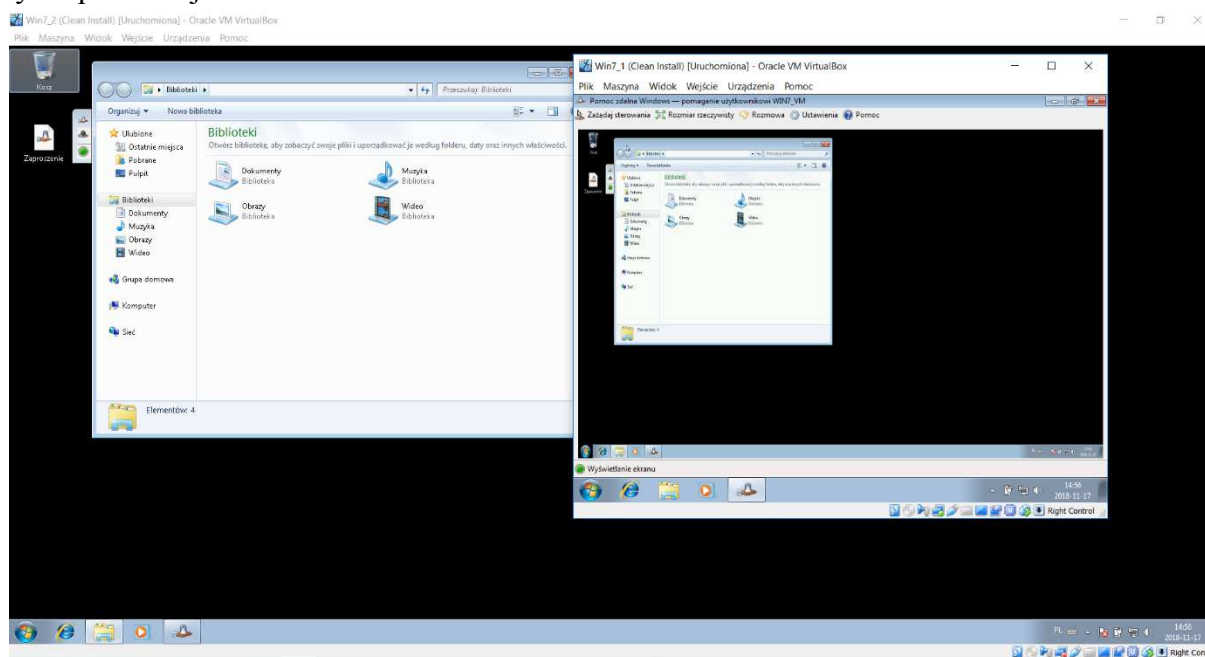




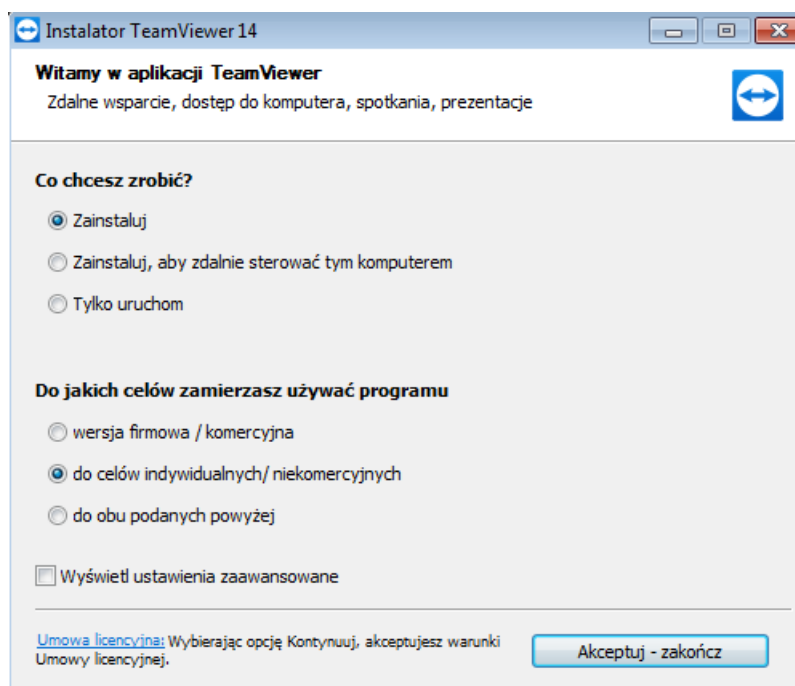
Aby połączenie się powiodło należy zaakceptować je na maszynie drugiej.



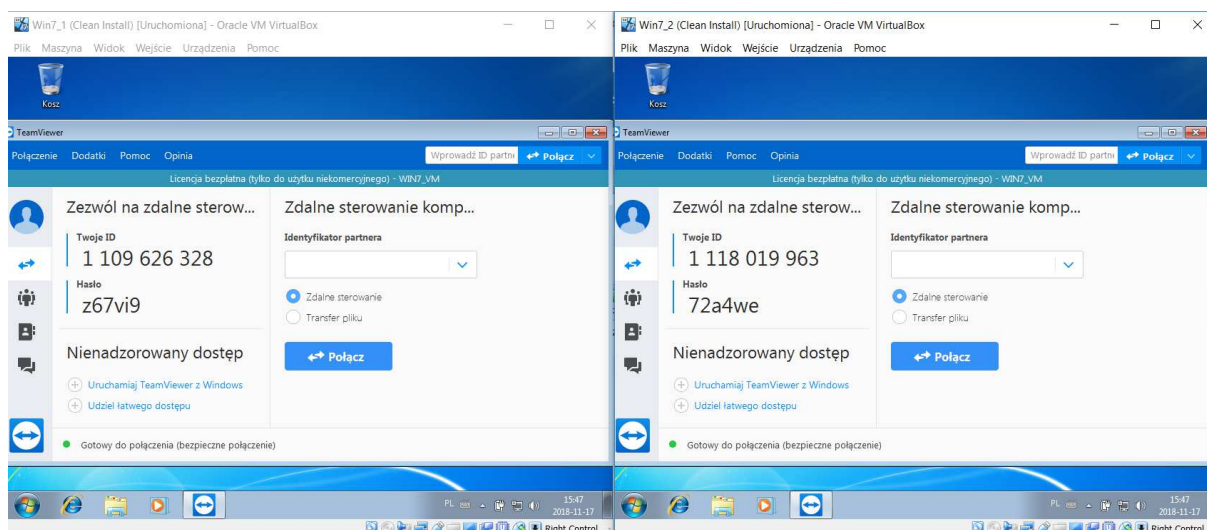
Rozpocznie się proces łączenia, który zakończy się uzyskaniem widoku Pulpit maszyny drugiej na maszynie pierwszej.



Dokonajmy teraz połączenia pomocy zdalnej za pomocą programu *TeamViewer*. Na obu maszynach skonfigurujmy Interfejs sieciowy jako *NAT*. Na obu maszynach musimy dokonać instalacji programu.



Następnie uruchamiamy program na obu maszynach.



Na maszynie pierwszej wprowadzamy identyfikator maszyny drugiej, a następnie jej hasło.

Zdalne sterowanie komp...


Identyfikator partnera

1118019963

☒ Zdalne sterowanie
☐ Transfer pliku

Pojłącz

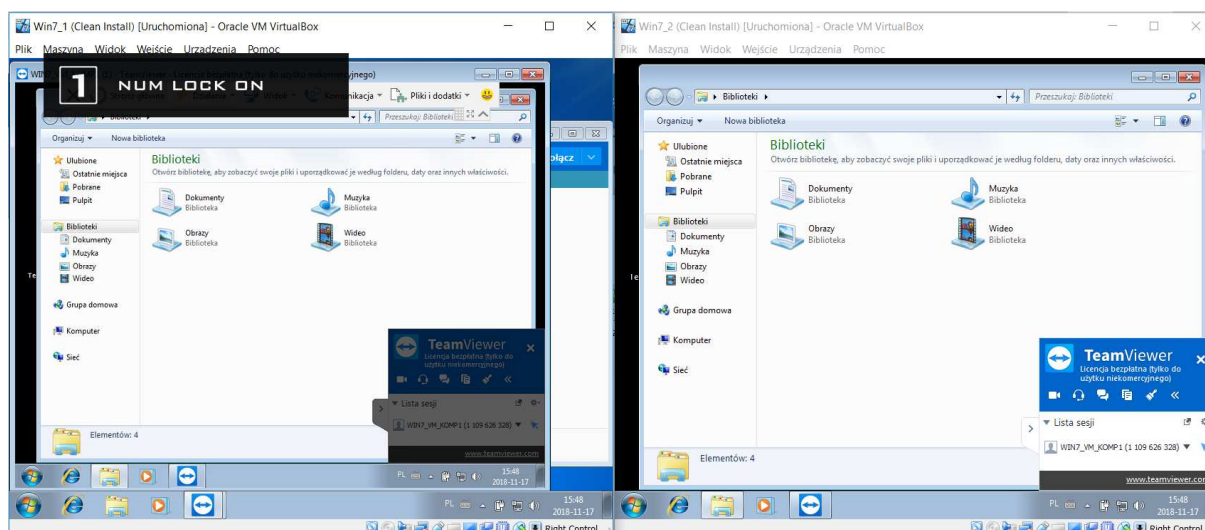
Uwierzytelnianie TeamViewer

 Wprowadź hasło wyświetlone w komputerze twojego partnera.

Hasło:

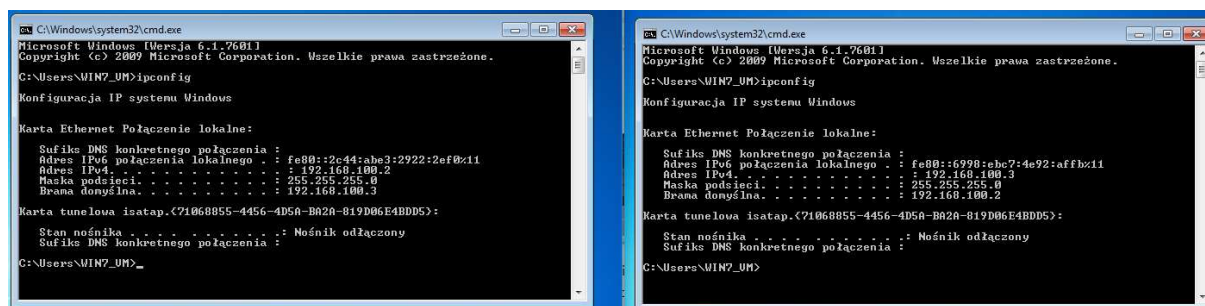
Zaawansowane **Zaloguj się** **Anuluj**

Dokonane zostanie połączenie.

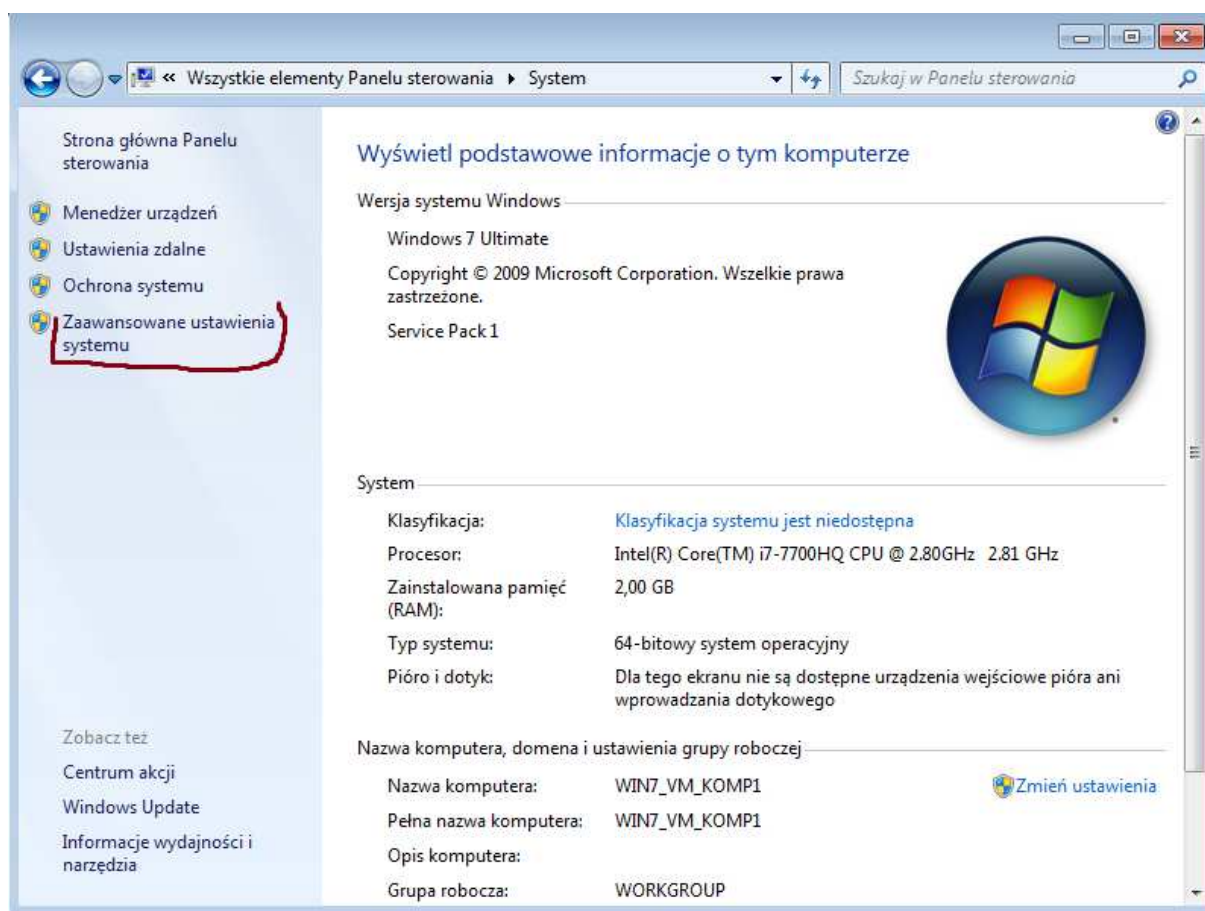


Zaletą *TeamViewer*'a jest praktycznie całkowita niezależność od typu infrastruktury sieciowej – wystarczy aby oba komputery były podłączone do Internetu. Jako, iż jest to instalowany program, automatycznie odblokowuje on sobie wymagane porty w Zaporze systemu Windows, dzięki czemu jest bardzo przyjazny dla użytkowników.

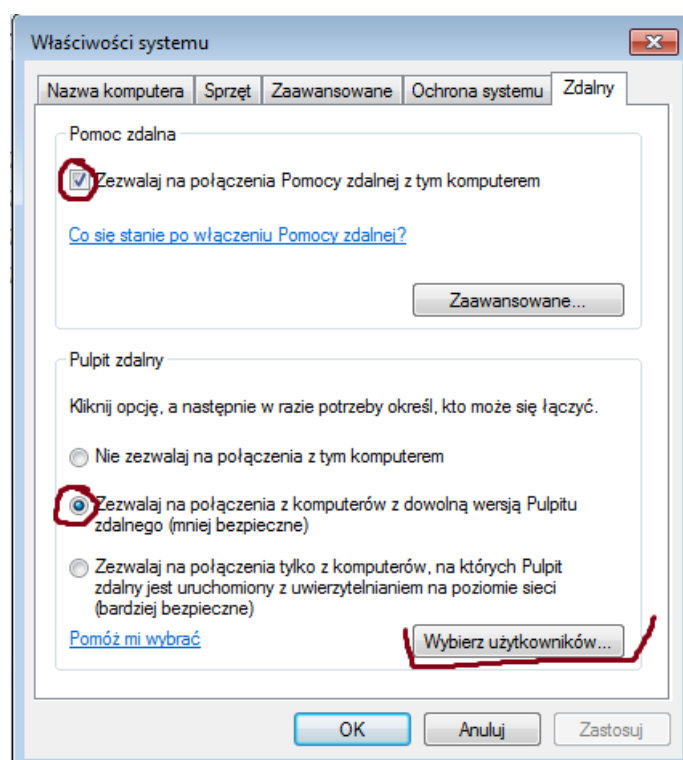
Następny etapem jest uruchomienie *Pulpitu zdalnego*, *TightVNC* oraz połączenia SSH. Umieścmy komputery w tej samej podsieci (w tym przypadku Sieć wewnętrzna switch1 o statycznym adresowaniu maszyny pierwszej 192.168.100.2 i maszyny drugiej 192.168.100.3 oraz lokalizacji Sieć publiczna).



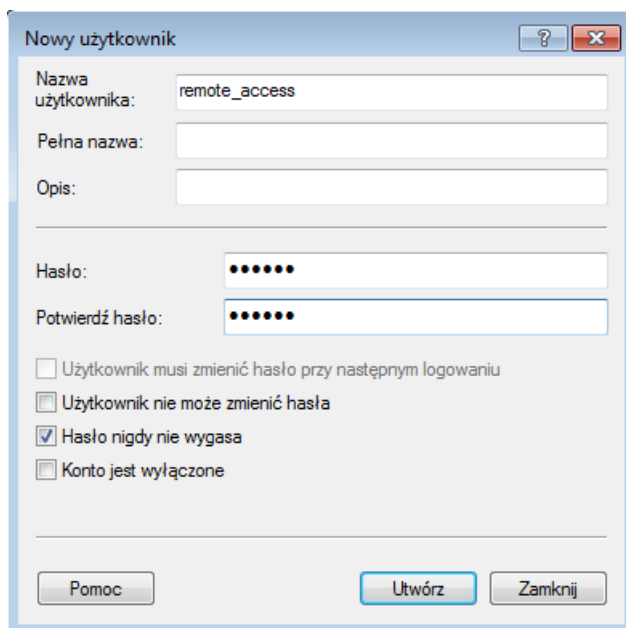
Następnym krokiem jest włączenie *Pulpitu zdalnego* na maszynie drugiej. Należy przejść do *Zaawansowanych ustawień systemu*



A następnie w zakładce *Zdalny* zezwolić na połączenie poprzez *Pulpit zdalny*.



Należy także wybrać użytkownika poprzez którego będzie można się łączyć. Należy tego użytkownika teraz stworzyć.



Nowy użytkownik

Nazwa użytkownika: remote_access

Pełna nazwa:

Opis:

Hasło:

Potwierdź hasło:

☐ Użytkownik musi zmienić hasło przy następnym logowaniu

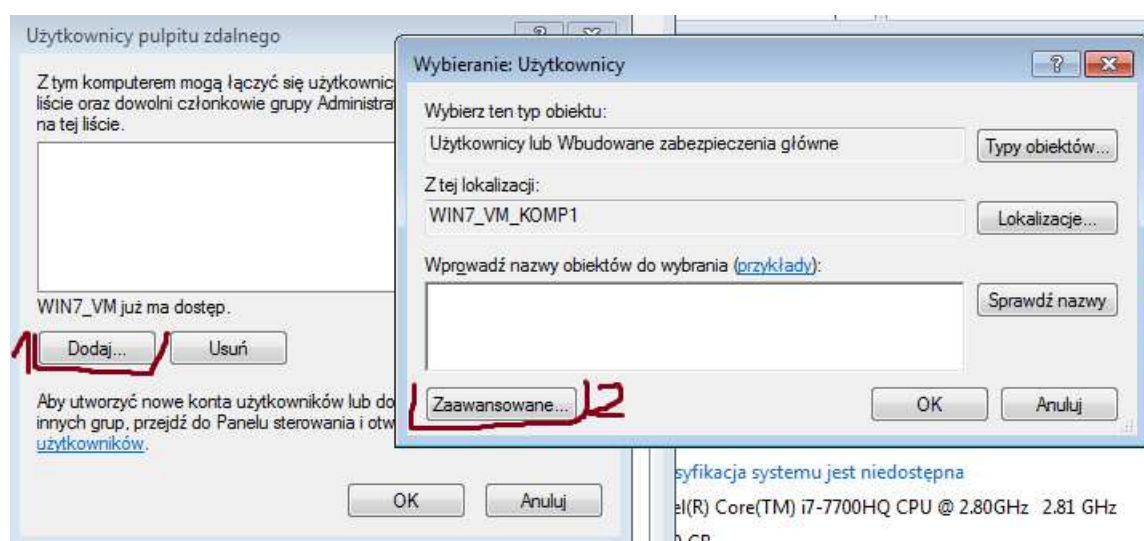
☐ Użytkownik nie może zmienić hasła

☒ Hasło nigdy nie wygasa

☐ Konto jest wyłączone

Pomoc Utwórz Zamknij

Skoro mamy już użytkownika możemy przejść do dodania go jako obsługującego Pulpit zdalny.





Wybieranie: Użytkownicy

Wybierz ten typ obiektu:
Użytkownicy lub Wbudowane zabezpieczenia główne

Typy obiektów...

Z tej lokalizacji:
WIN7_VM_KOMP1

Lokalizacje...

Zwykłe zapytania

Nazwa: Rozpoczyna się od

Opis: Rozpoczyna się od

☐ Konta wyłączone

☐ Hasło niewygasające

Liczba dni od ostatniego logowania:

Kolumny...

Znajdź teraz

Zatrzymaj

Wyniki wyszukiwania:

Nazwa (RDN)	W folderze
-------------	------------



Wybieranie: Użytkownicy

Wybierz ten typ obiektu:
Użytkownicy lub Wbudowane zabezpieczenia główne

Z tej lokalizacji:
WIN7_VM_KOMP1

Zwykłe zapytania

Nazwa: Rozpoczyna się od

Opis: Rozpoczyna się od

☐ Konta wyłączone

☐ Hasło niewygasające

Liczba dni od ostatniego logowania:

Wyniki wyszukiwania:

Nazwa (RDN)	W folderze
GRUPA TWÓ...	
HomeGroupU...	WIN7_VM_KO...
INTERAKTY...	
IUSR	
LOGOWANIE...	
LOGOWANIE...	
PRAWA WŁ...	
remote_access	WIN7_VM_KO...
SIEĆ	
SYSTEM	

Użytkownicy pulpitu zdalnego

Z tym komputerem mogą łączyć się użytkownicy wyświetleni na poniższej liście oraz dowolni członkowie grupy Administratorzy, nawet jeśli nie ma ich na tej liście.

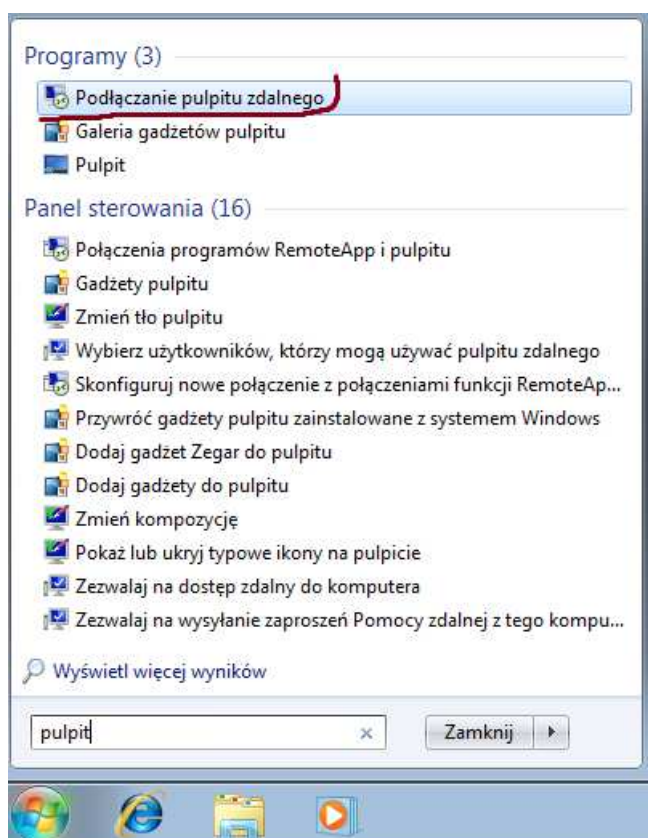
remote_access

WIN7_VM już ma dostęp.

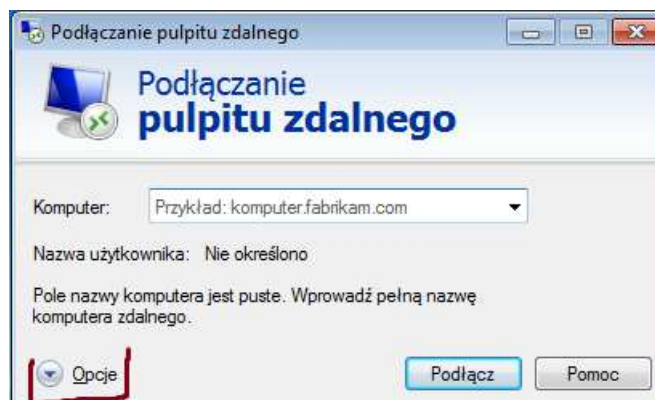
Dodaj... Usun

Aby utworzyć nowe konta użytkowników lub dodać użytkowników do innych grup, przejdź do Panelu sterowania i otwórz aplet [Konta użytkowników](#).

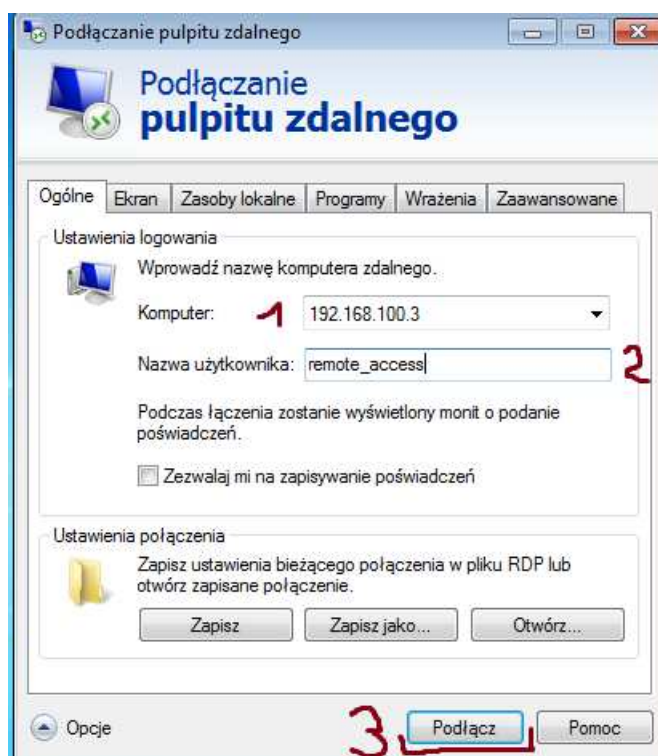
Następnie na maszynie pierwszej uruchamiamy *Podłączenie pulpitu zdalnego*



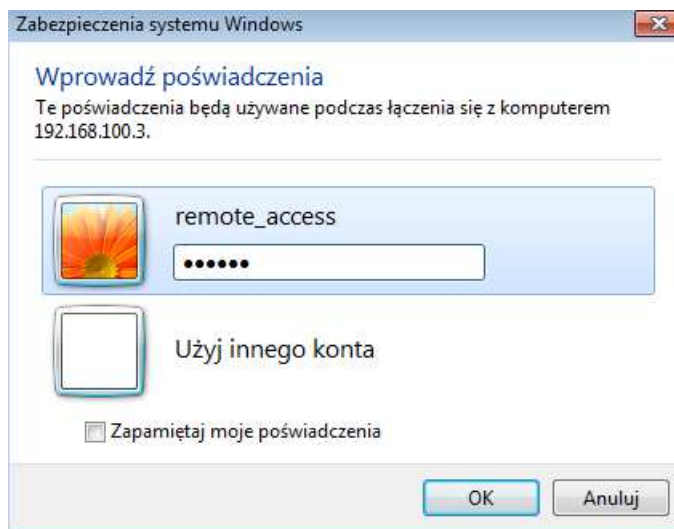
Rozwijamy *Opcje*



Wprowadzamy adres IP komputera, nazwę użytkownika i klikamy *Podłącz*



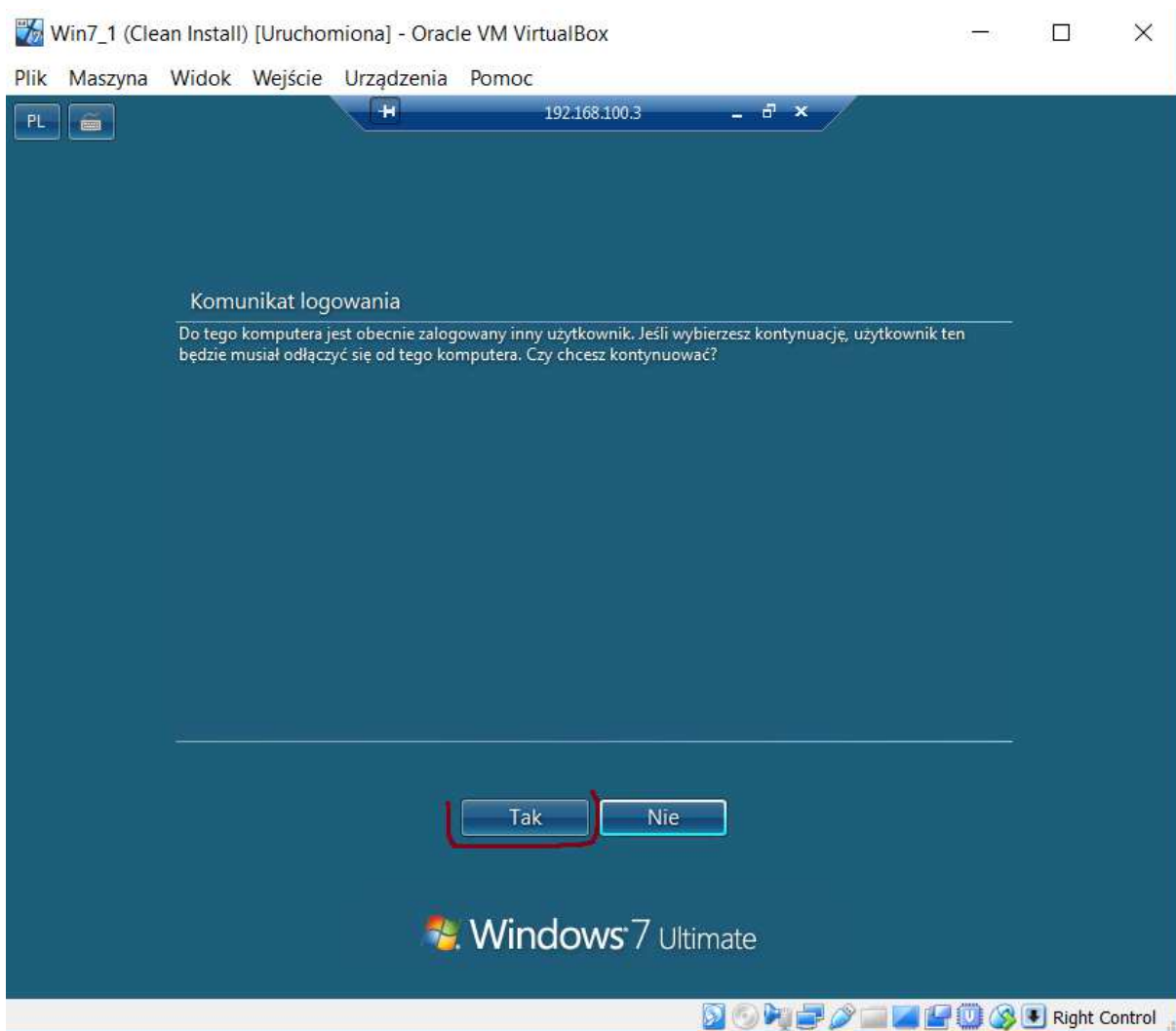
Następnie wprowadzamy hasło



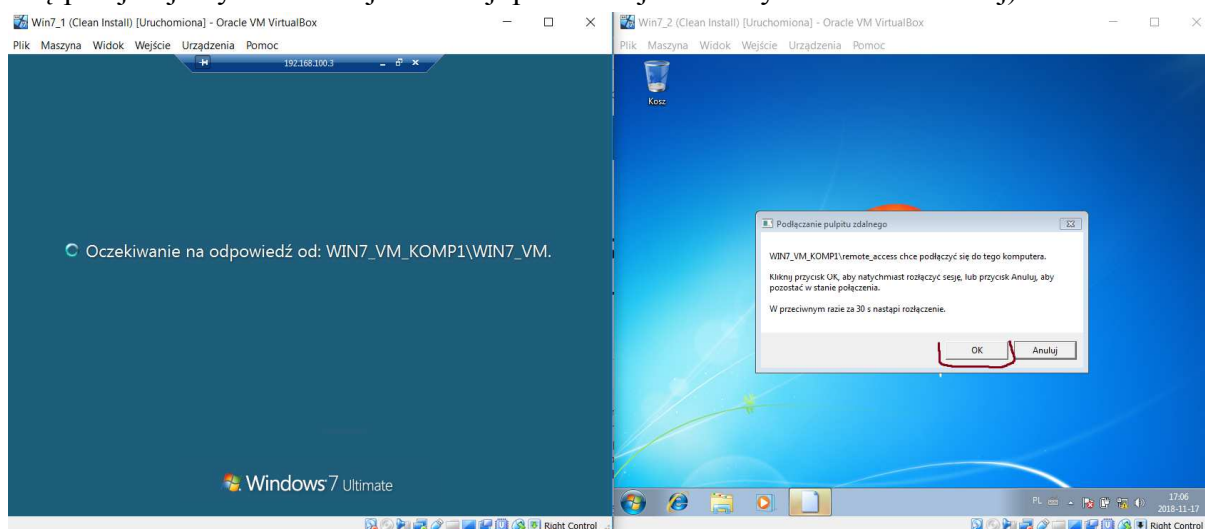
Kolejnym krokiem jest zgodzenie się na kontrolę komputera, który nie posiada certyfikatu



Zostaniemy połączeni z komputerem, jako, że na maszynie drugiej zalogowany jest inny użytkownik musimy zaakceptować jego wylogowanie na czas kontroli zdalnej

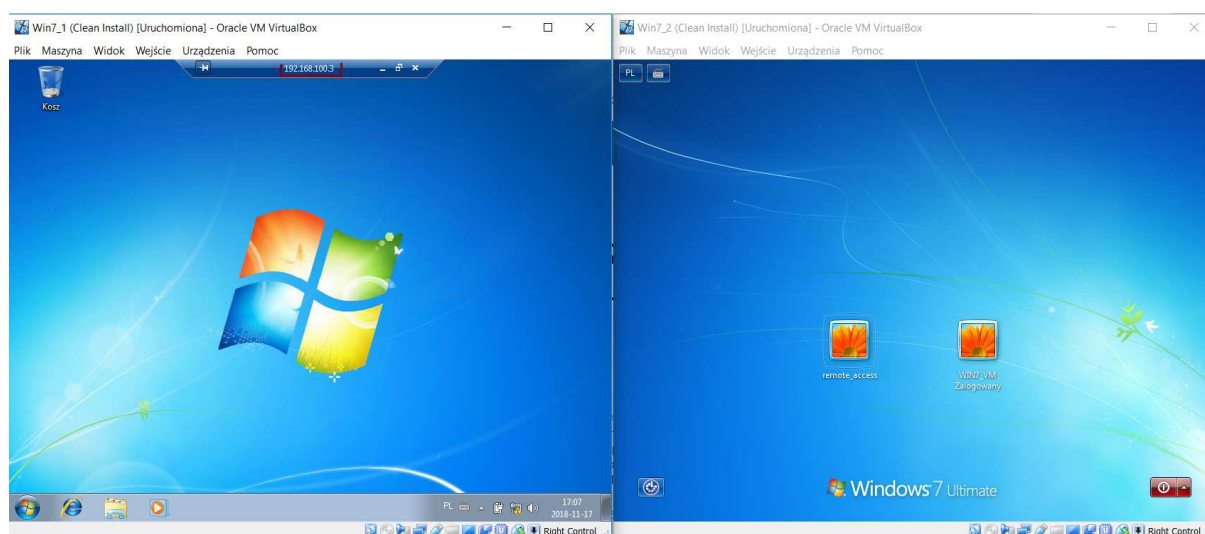


Na maszynie drugiej musimy wyrazić zgodę na kontrolę zdalną (zgoda jest potrzebna tylko i wyłącznie za pierwszym razem gdy wykonujemy kontrolę zdalną i tylko i wyłącznie w przypadku gdy na maszynie drugiej zalogowany jest inny użytkownik, jeśli nie jest zalogowany inny użytkownik kontrolę przejmujemy bez żadnej interakcji potrzebnej na maszynie kontrolowanej).

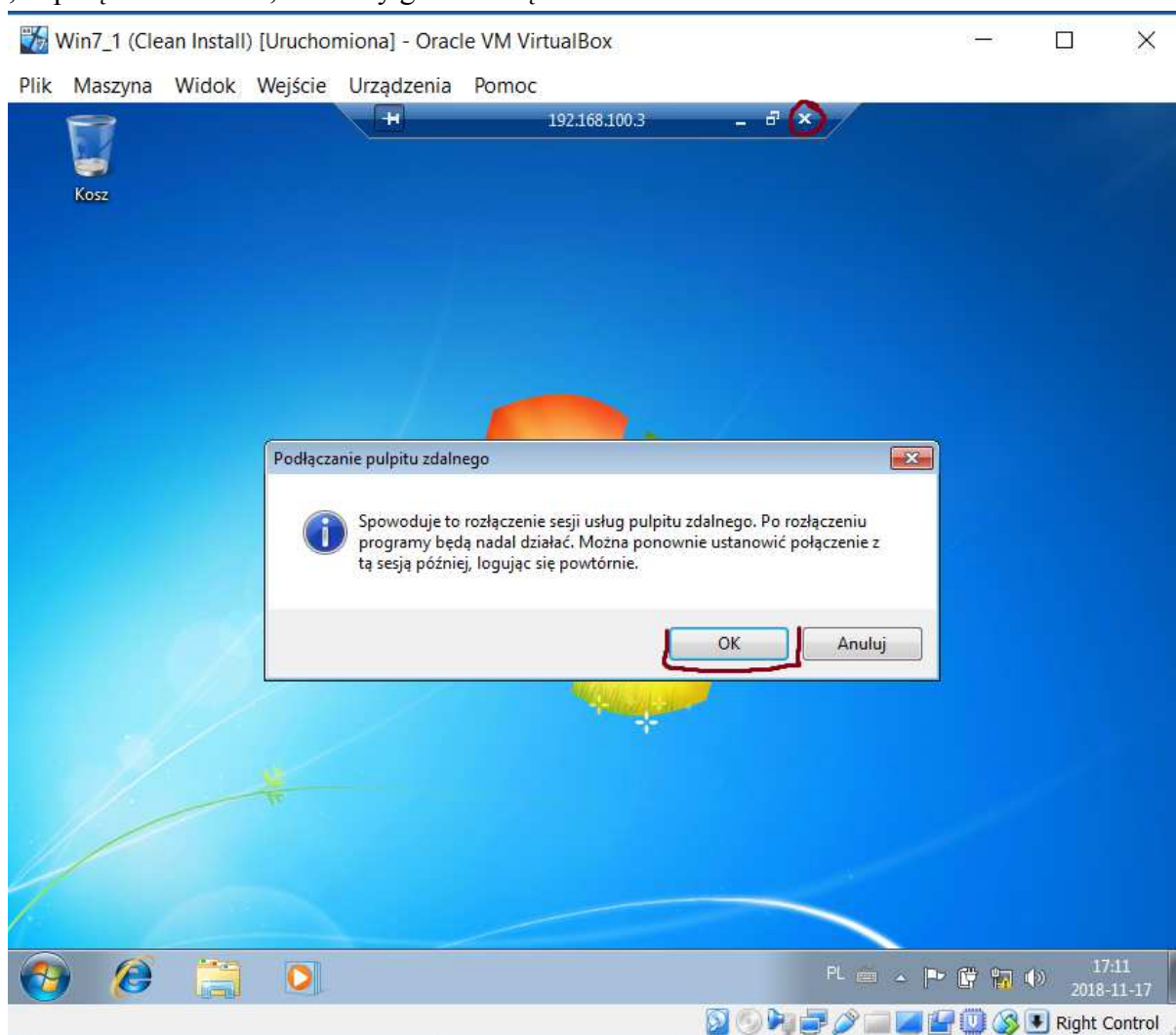


Na maszynie pierwszej przejmujemy kontrolę zdalnie nad maszyną drugą.

Projekt „SezAM wiedzy, kompetencji i umiejętności” jest współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego w ramach Programu Operacyjnego Wiedza Edukacja Rozwój

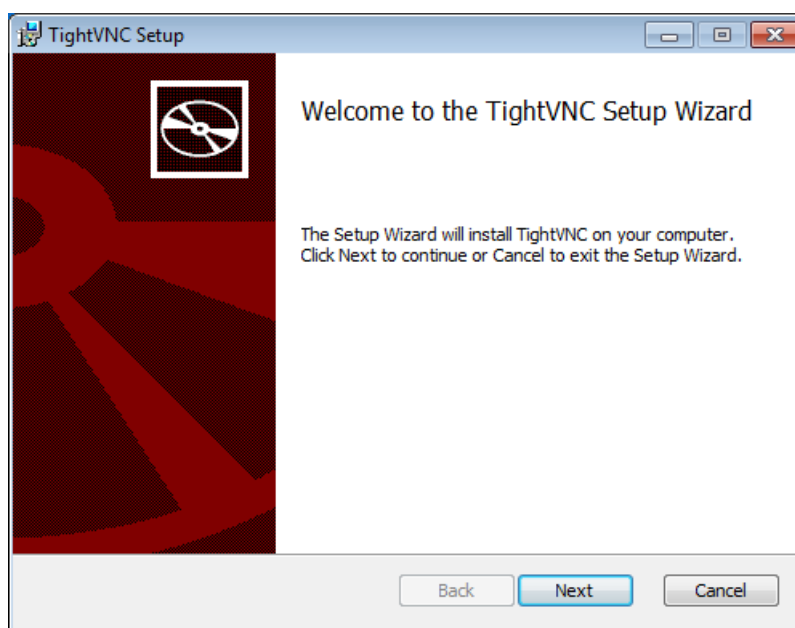


Jako, iż połączenie działa, możemy go zamknąć.

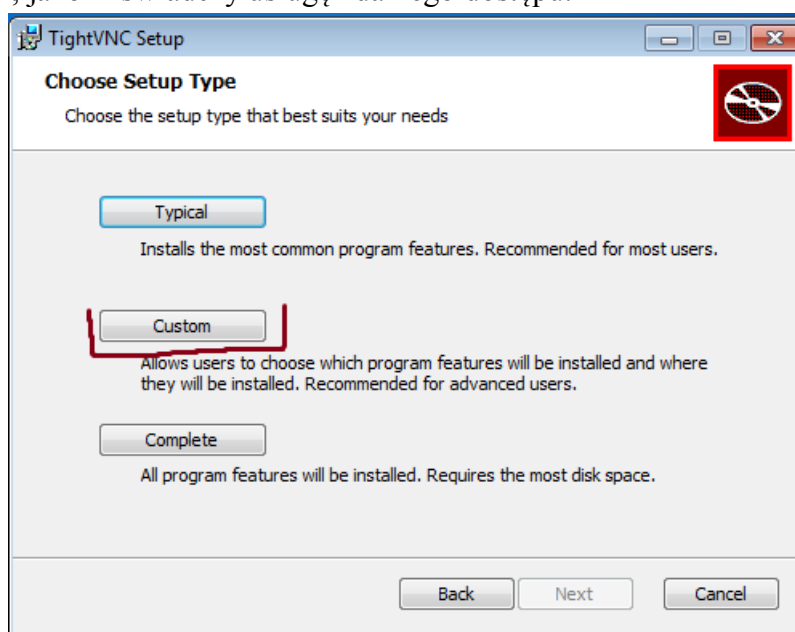


Zamiennikiem *Pulpitu zdalnego* jest *TightVNC* (lub *RemoteVNC*). Aby skorzystać z *TightVNC* musimy zainstalować go na obu maszynach.

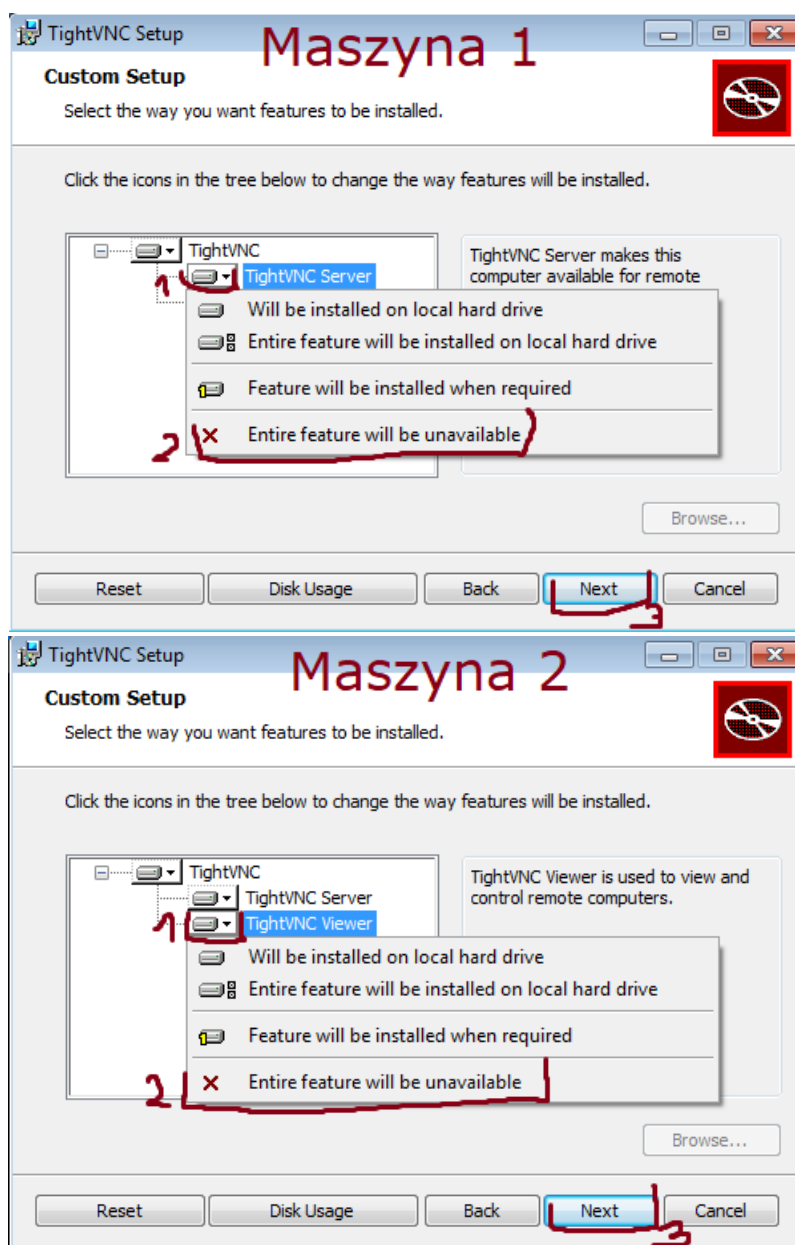
Uruchamiamy więc instalator



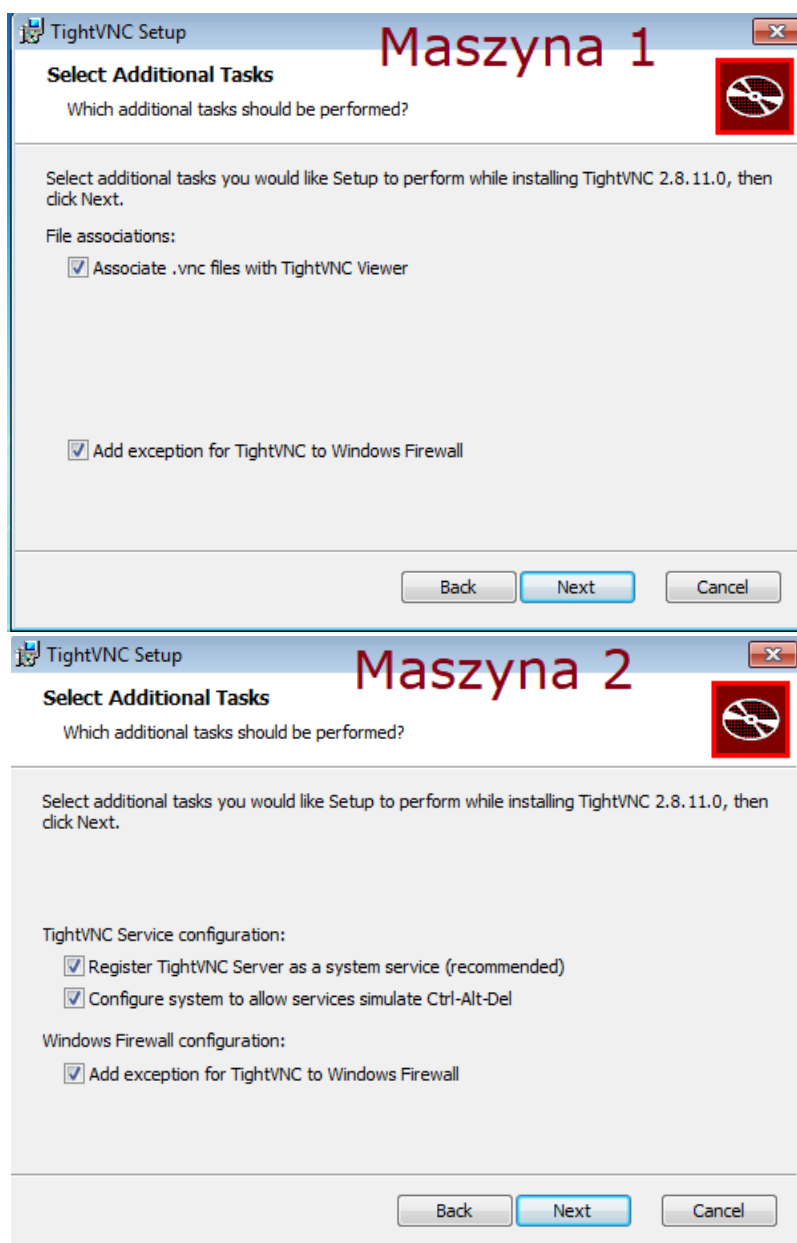
Jako typ instalacji wybieramy *Custom*, ponieważ aplikacja składa się z dwóch składników: *Viewer* i *Server*. Na maszynie pierwszej potrzebujemy *Viewer*, jako iż jest to klient, a na maszynie drugiej potrzebujemy *Server*, jako iż świadczy usługę zdalnego dostępu.



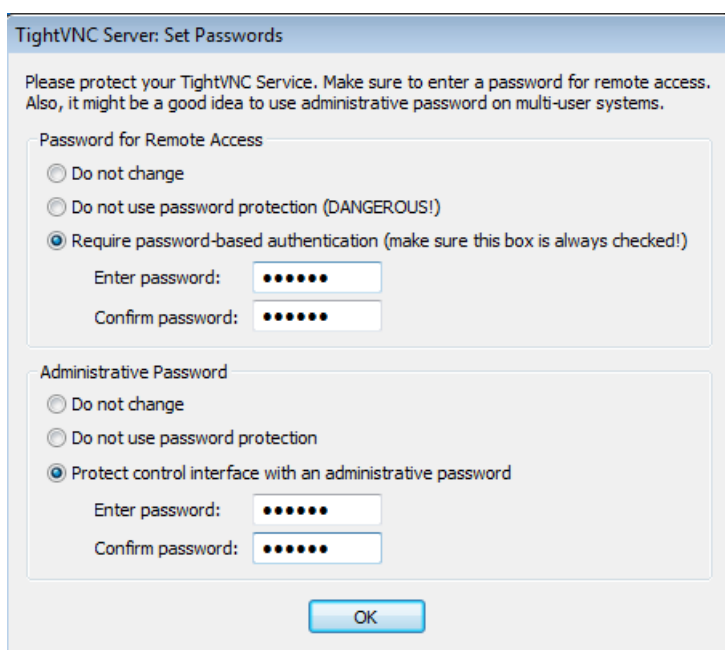
Na maszynie pierwszej więc odznaczamy instalację składnika *Server*, a na maszynie drugiej składnika *Viewer*.



W następnym kroku będziemy mogli dostosować czynności poinstalacyjne. W przypadku Maszyny 1 będzie to skojarzenie plików o rozszerzeniu vnc z klientem *TightVNC* oraz dodanie odpowiednich reguł do *Zapory systemu Windows*. W przypadku Maszyny 2 będzie to dodanie *TightVNC Server* jako usługi systemowej (oznacza to, że *TightVNC* będzie usługą w *services.msc*, będzie uruchamiana automatycznie przy uruchomieniu komputera), zezwolenie na emulację skrótu klawiszowego *Ctrl+Alt+Del* oraz dodanie reguły do *Zapory systemu Windows*. Wszystkie opcje pozostawiamy zaznaczone.



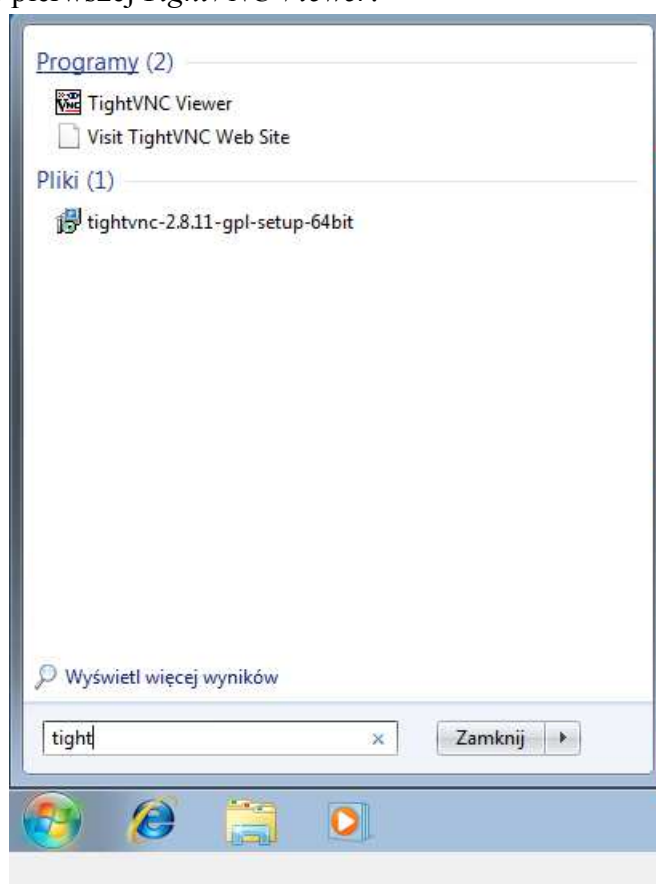
Na Maszynie 2 zostaniemy poproszeni o wprowadzenie hasła do kontroli zdalnej (*TightVNC* nie korzysta z użytkowników systemowych do uwierzytelnienia, więc użytkownik `remote_access` jest tu zbędny)



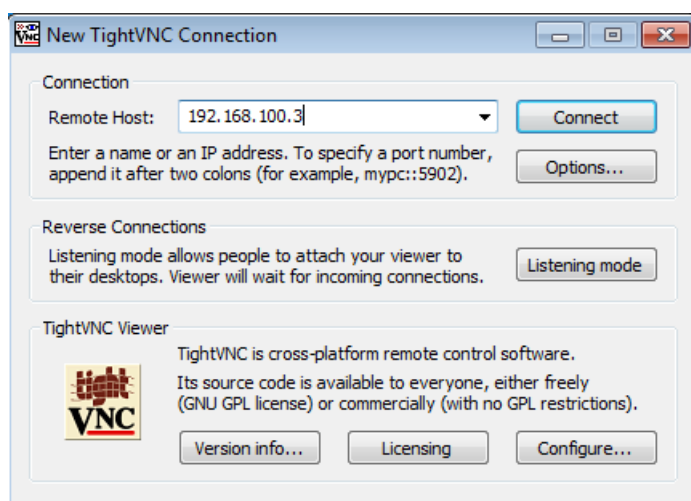
Instalacja zostanie ukończona, a usługa serwerowa uruchomiona (pojawia się ikonka w zasobniku systemowym)



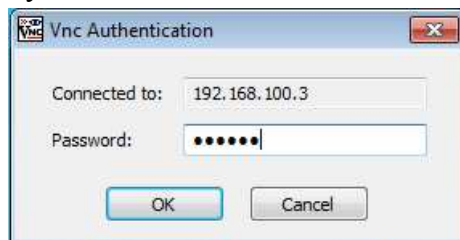
Uruchommy na maszynie pierwszej *TightVNC Viewer*.



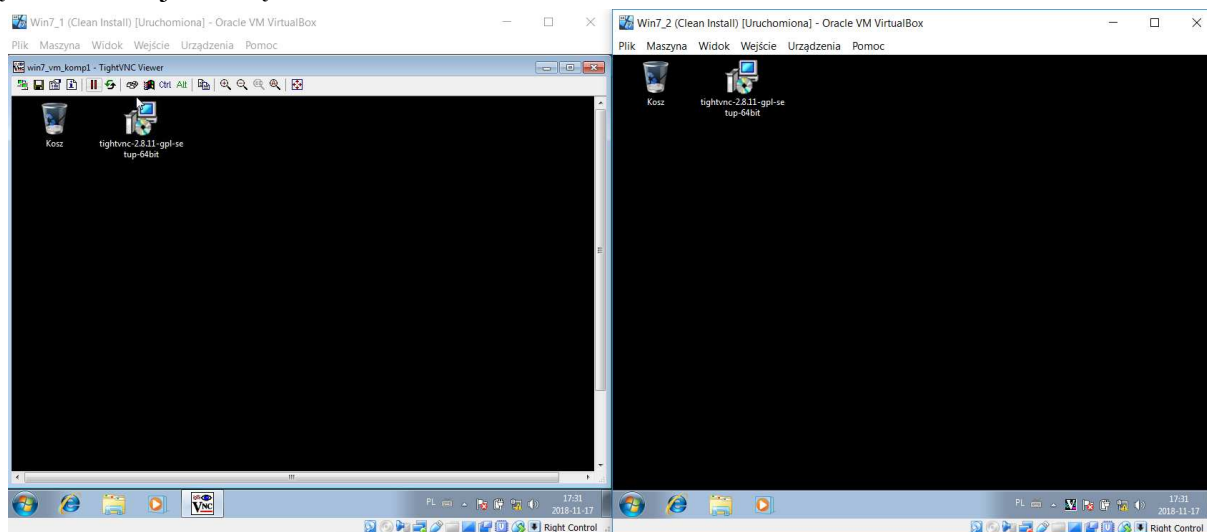
Wprowadźmy adres IP maszyny drugiej i kliknijmy *Connect*



Następnie podajemy hasło i klikamy *OK*



Połączenie zostaje nawiązane

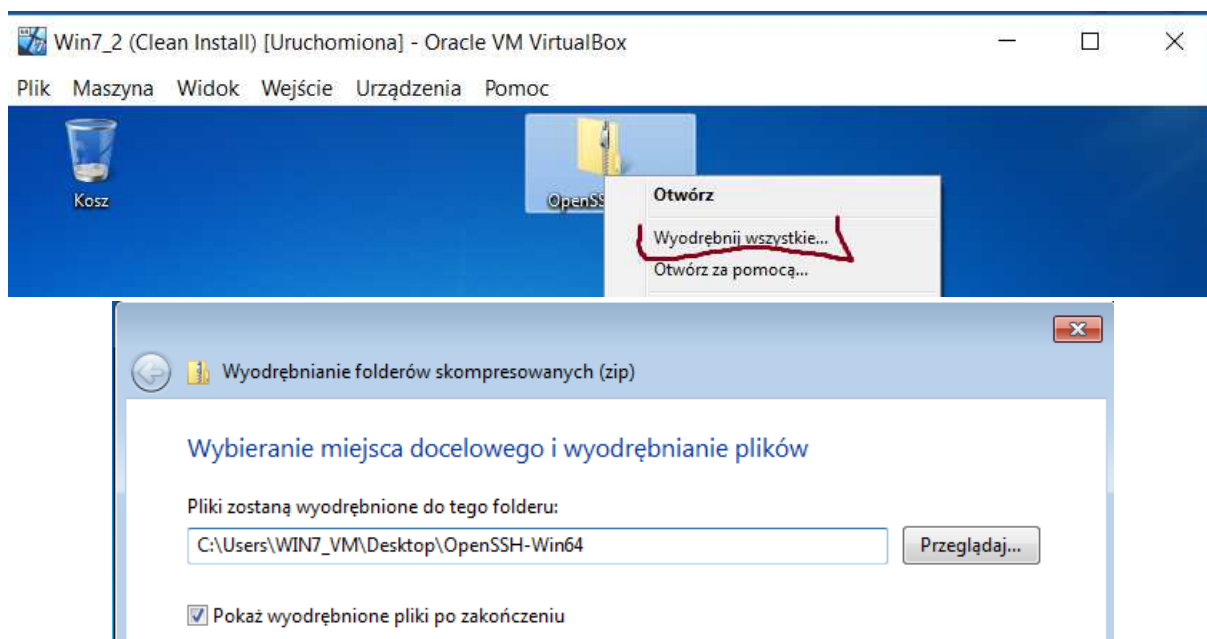


Przewagą *TightVNC* nad *Pulpitem zdalnym* jest to, że nie wylogowuje użytkowników z komputera kontrolowanego, więc nie zaburza jego pracy. Nie korzysta też z mechanizmu autoryzacji poprzez użytkownika systemu Windows (mechanizm raczej mało bezpieczny).

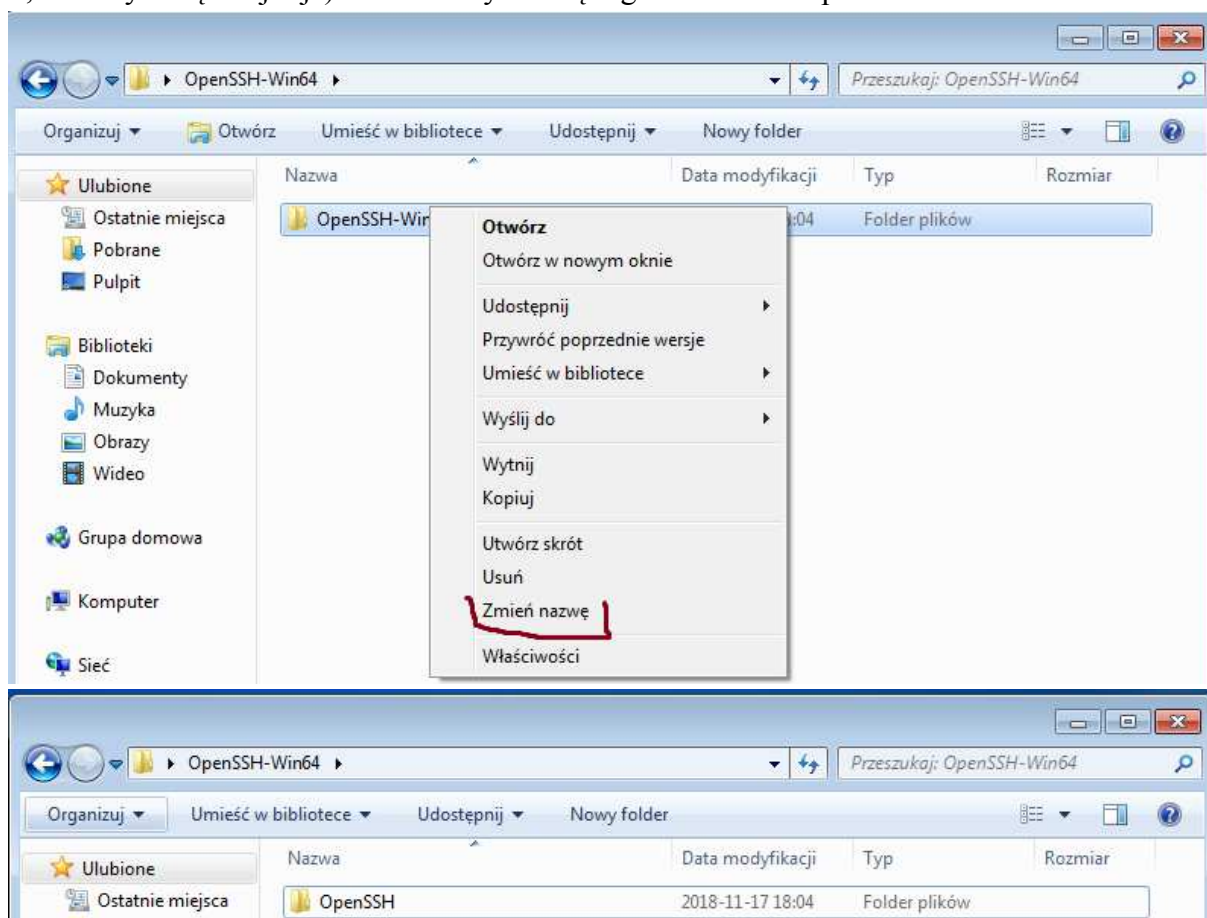
Kolejną metodą kontroli jest połączenie przez SSH – jest to najbezpieczniejsza metoda, ponieważ cały ruch sieciowy jest szyfrowany. Aby kontrolować maszynę przez SSH potrzebujemy klienta SSH np. *Putty* oraz usługi serwerowej SSH np. *OpenSSH* (w przypadku Windows 10 taka usługa jest już elementem systemu, lecz Windows 7 musi bazować na programach zewnętrznych).

Zainstalujemy więc usługę *OpenSSH* na maszynie drugiej.

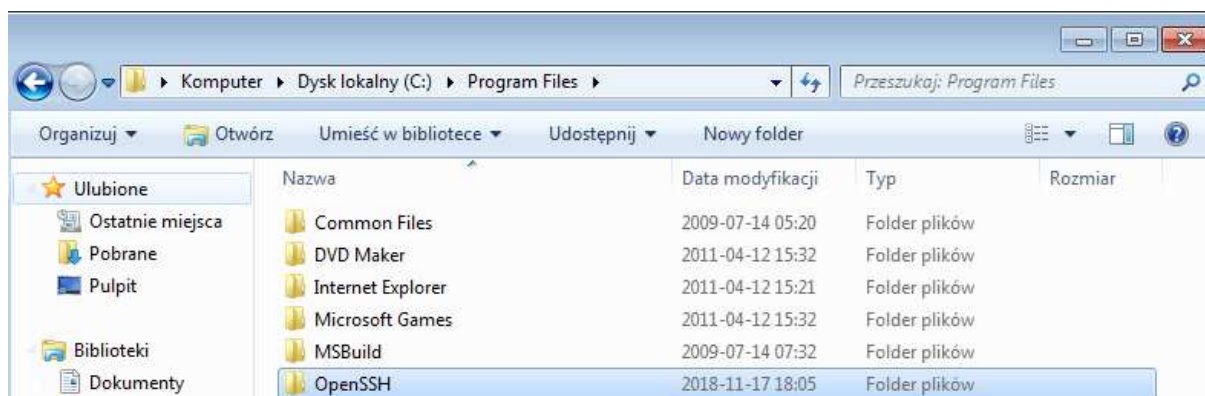
Wypakowujemy archiwum *OpenSSH-Win64* (lub *OpenSSH-Win32*, w zależności od architektury procesora)



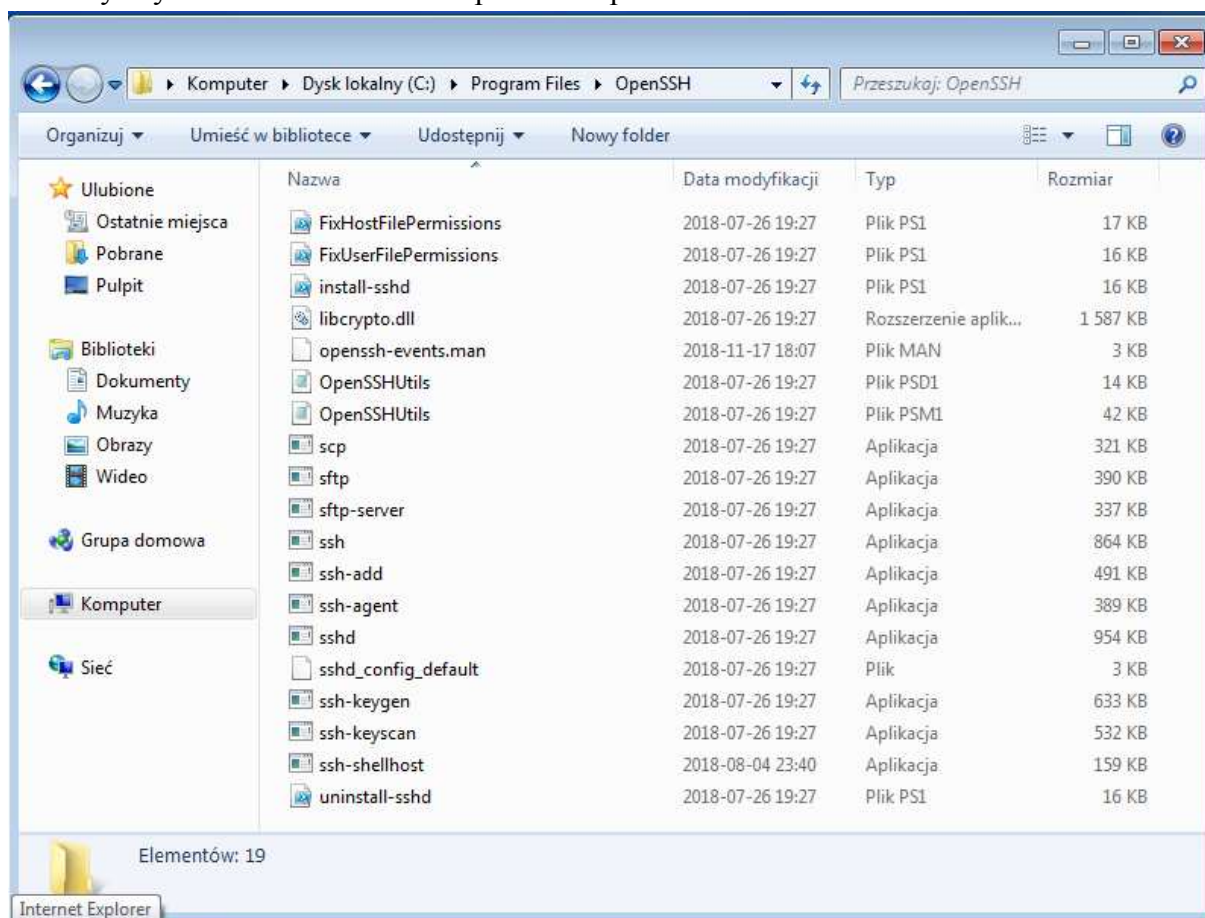
Otwieramy wypakowany folder. Znajduje się tam folder OpenSSH-Win64 (taka sama nazwa jak folder, w którym się znajduje). Zmieniamy nazwę tego folderu na OpenSSH



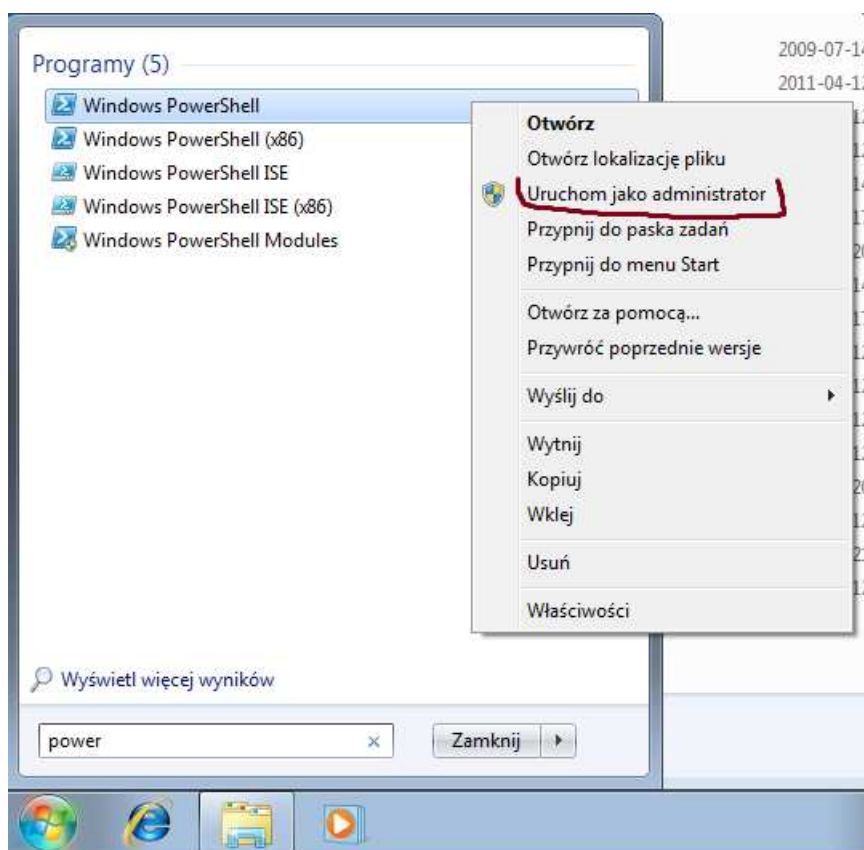
Przenosimy ten folder do C:\Program Files\



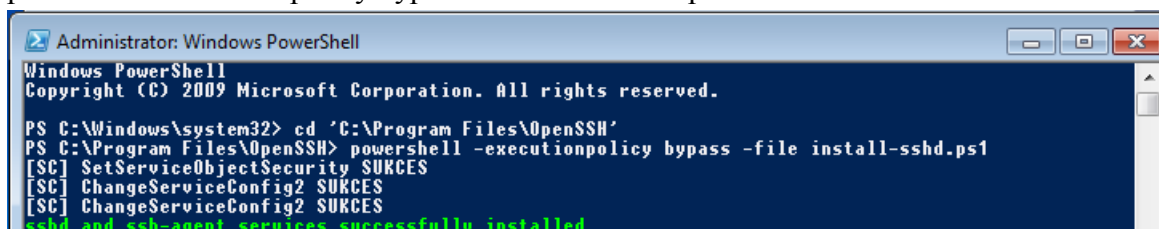
Sprawdzamy czy folder zawiera w sobie potrzebne pliki



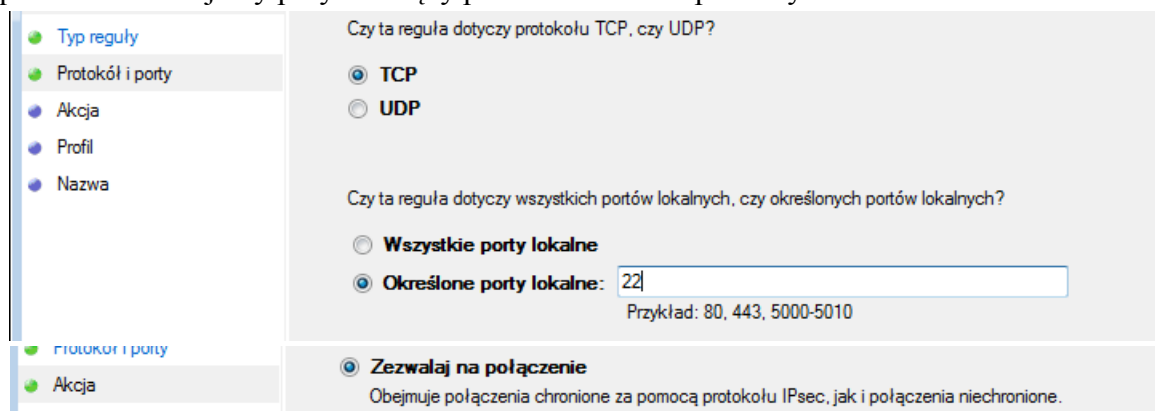
Uruchamiamy *PowerShell* z uprawnieniami administracyjnymi

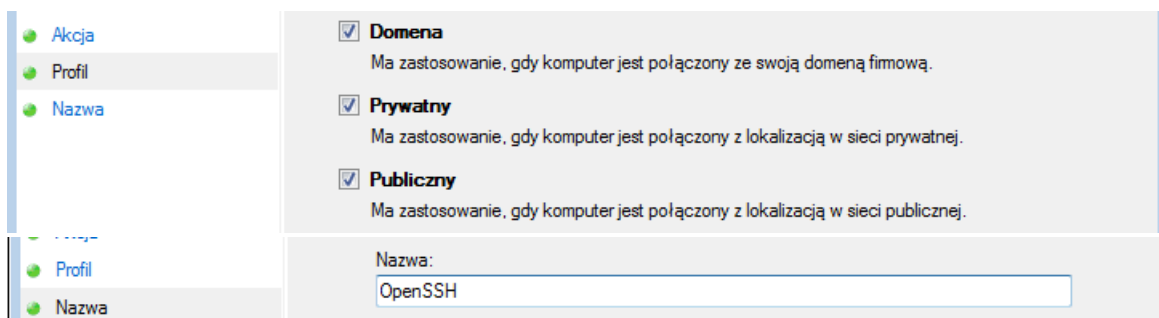


Następnie wpisujemy poniższe komendy
`cd 'C:\Program Files\OpenSSH'`
`powershell -executionpolicy bypass -file install-sshd.ps1`



Następnie odblokowujemy przychodzący port TCP 22 w Zaporze systemu Windows



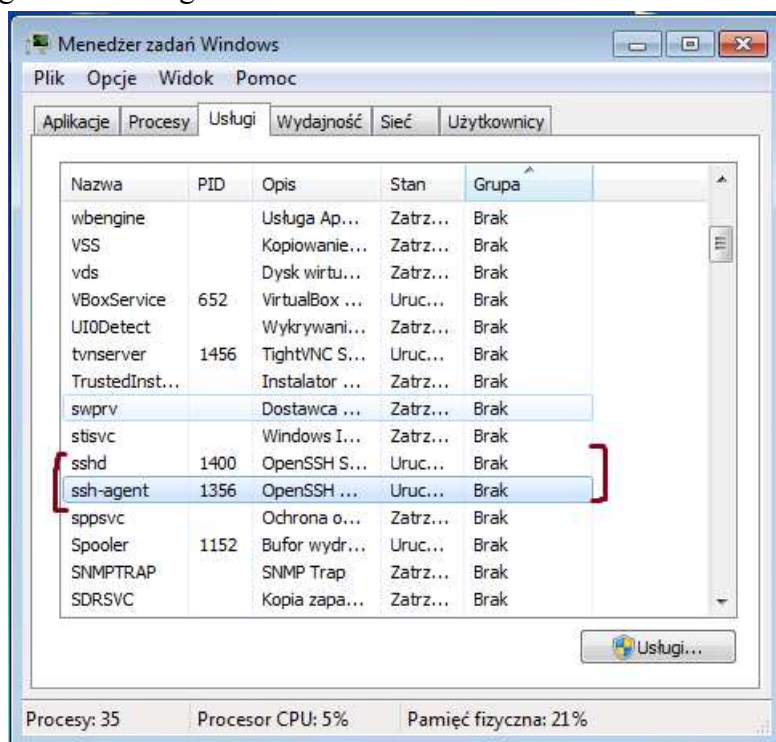


Wpisujemy w PowerShell (z uprawnieniami administracyjnymi) następujące komendy

Set-Service sshd -StartupType Automatic

Set-Service ssh-agent -StartupType Automatic

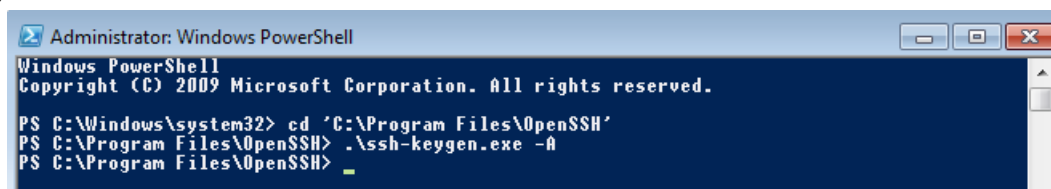
Następnie ponownie uruchamiamy maszynę. Po ponownym uruchomieniu sprawdzamy, czy uruchomione są usługi sshd i ssh-agent.



Uruchamiamy PowerShell (z uprawnieniami administracyjnymi i wpisujemy poniższe komendy:

cd 'C:\Program Files\OpenSSH'

.\ssh-keygen.exe -A

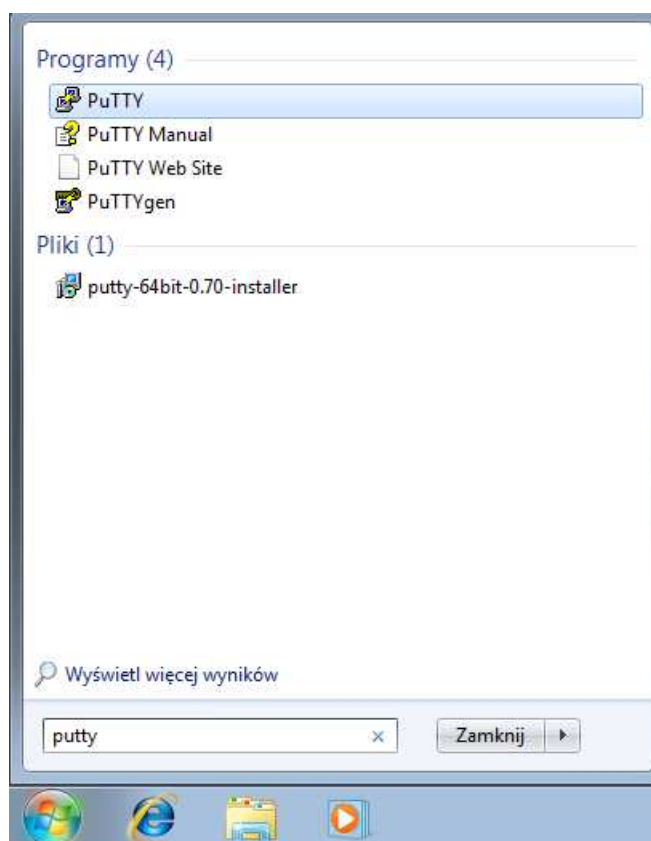


Ponownie uruchamiamy maszynę.

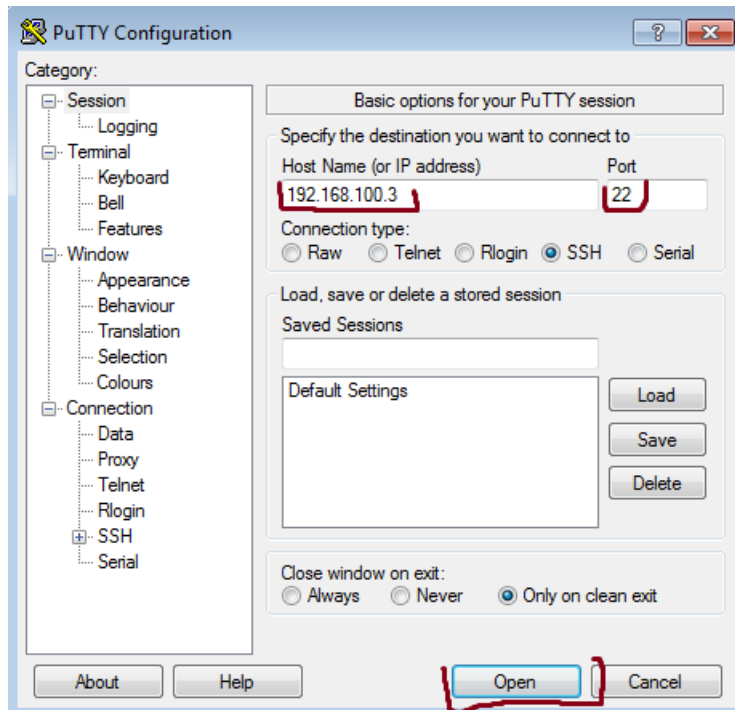
Przechodzimy do instalacji klienta SSH (*Putty*) na maszynie pierwszej.

Uruchamiamy instalator *Putty* i przeprowadzamy instalację nie wprowadzając żadnych zmian.

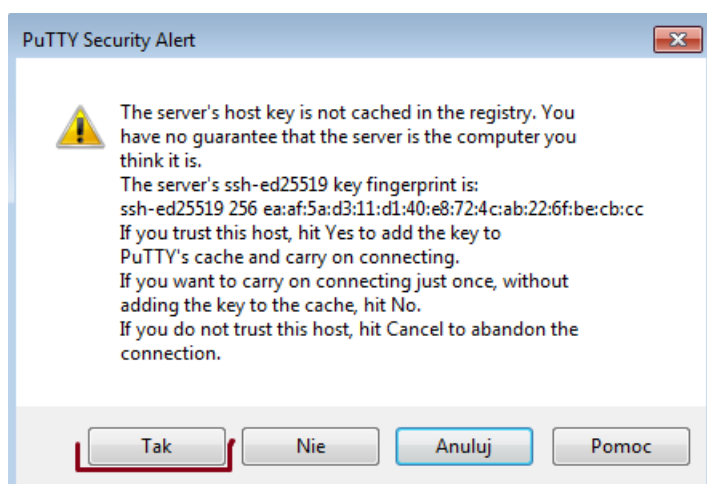
Uruchamiamy *Putty*



W okienku konfiguracyjnym wpisujemy adres IP oraz port, następnie klikamy *Open*

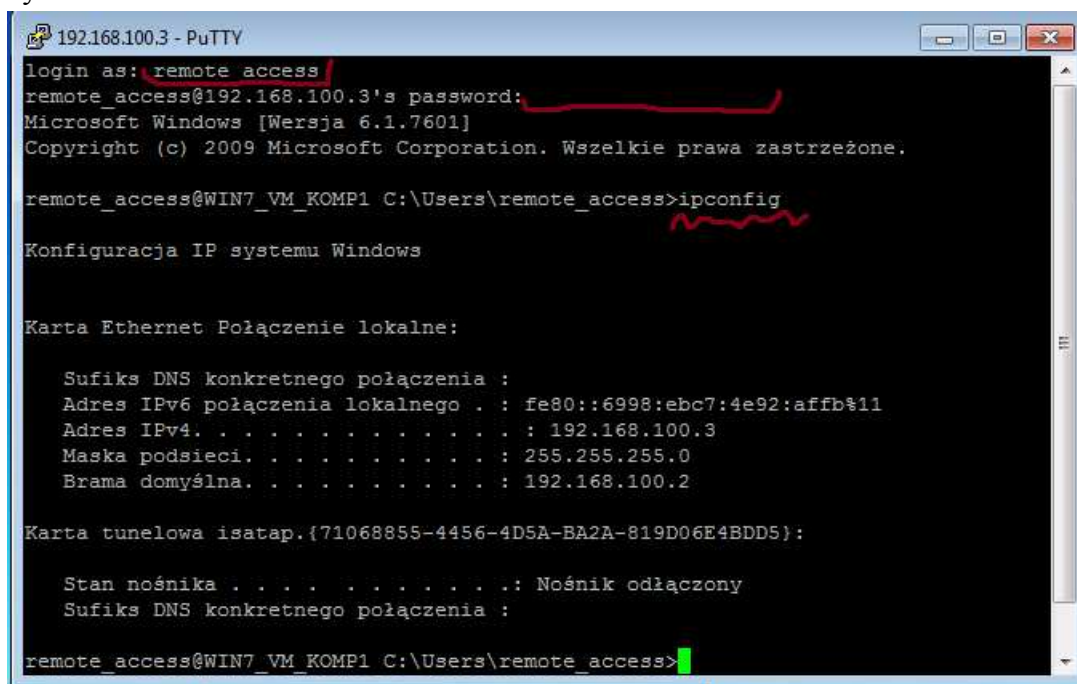


Zostanie wyświetlony nam komunikat, że *Putty* nie zna tego klucza publicznego i czy mimo to chcemy się z tym komputerem połączyć. Klikamy *Tak*



Wpisujemy nazwę użytkownika (w tym przypadku `remote_access`) i hasło.

Następnie wykonujemy dowolną komendę, aby sprawdzić czy otrzymany rezultat zgadza się z oczekiwanym.

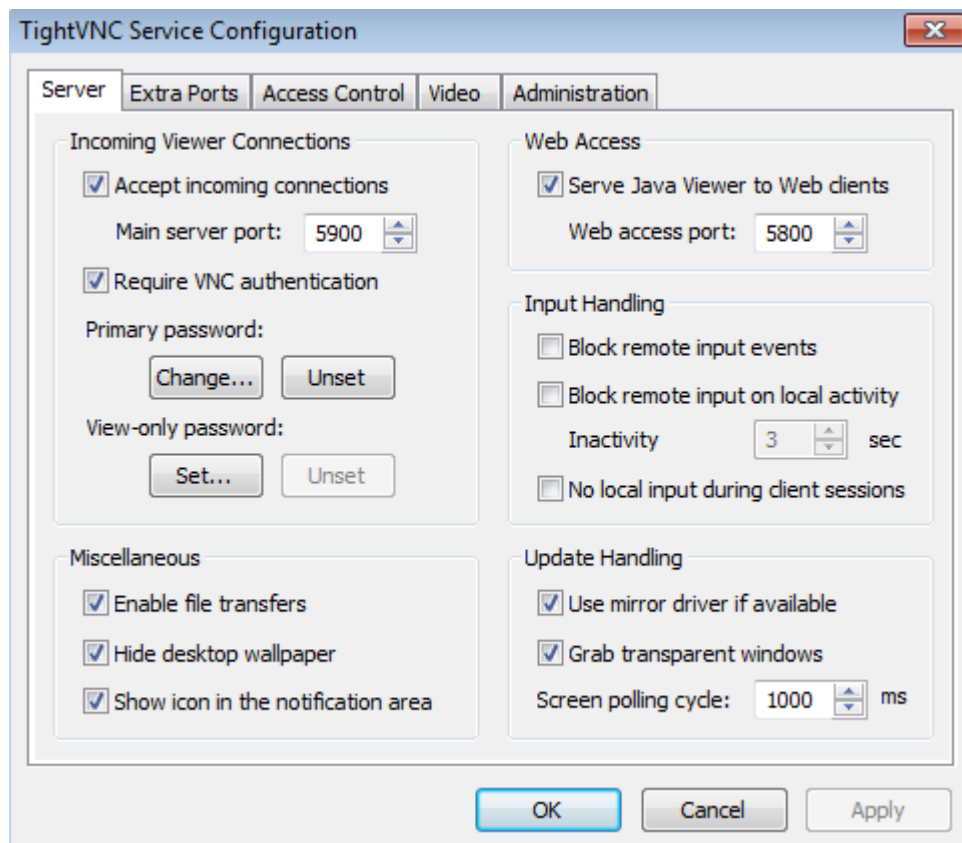


Przedstawiono narzędzia Pomocy zdalnej, których możemy używać poprzez Internet, lecz narzędzia Pulpitu zdalnego działają w tym momencie jedynie lokalnie. Aby mieć możliwość połączenia poprzez sieć globalną należy przekierować porty routera na maszynę kontrolowaną (w tym przypadku maszyna druga). Pulpit zdalny nasłuchuje portu TCP i UDP 3389, OpenSSH portu TCP 22. Sprawdźmy jakiego portu nasłuchuje TightVNC Server.

Kliknijmy dwukrotnie ikonkę w zasobniku systemowym



Zostanie otwarte okno konfiguracyjne *TightVNC Server*.



Wygląda na to, że domyślne połączenia przychodzące nasłuchiwane są na porcie 5900.

Dokonajmy więc odpowiedniej konfiguracji infrastruktury sieciowej maszyn wirtualnych (Maszyna 1 jako *Mostkowana karta sieciowa*, Maszyna 2 jako *Sieć wbudowana* połączona z LAN wirtualnego routera, wirtualny router skonfigurowany tak jak zawsze). Następnie przekierujmy porty 22, 3389 i 5900.

PODPOWIEDŹ! Komendy to (należy oczywiście zmienić adres 192.168.200.200 na odpowiedni):
ip firewall nat

addaction=dst-nat chain=dstnat dst-port=677 protocol=tcp to-addresses=192.168.200.200 to-ports=22

addaction=dst-nat chain=dstnat dst-port=678 protocol=tcp to-addresses=192.168.200.200 to-ports=3389

addaction=dst-nat chain=dstnat dst-port=679 protocol=tcp to-addresses=192.168.200.200 to-ports=5900

```
[admin@MikroTik] /ip firewall nat> print
Flags: X - disabled, I - invalid, D - dynamic
0 chain=srcnat action=masquerade out-interface-list=WAN
1 chain=dstnat action=dst-nat to-addresses=192.168.200.200 to-ports=22
  protocol=tcp dst-port=677
2 chain=dstnat action=dst-nat to-addresses=192.168.200.200 to-ports=5900
  protocol=tcp dst-port=679
3 chain=dstnat action=dst-nat to-addresses=192.168.200.200 to-ports=3389
  protocol=tcp dst-port=678
```

Następnie sprawdzamy po kolei czy usługi działają

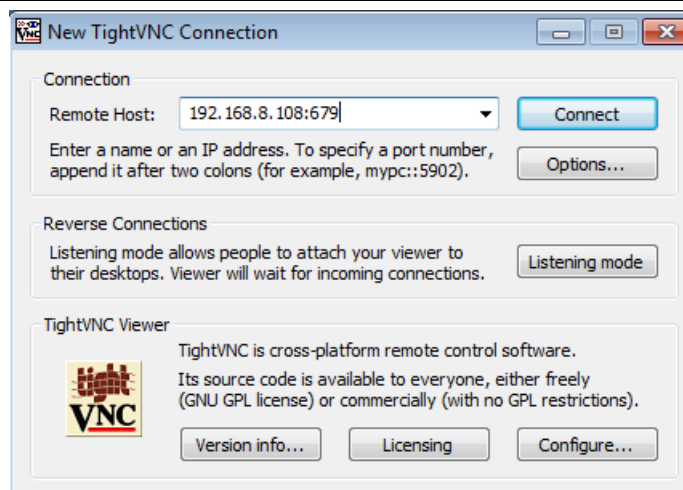
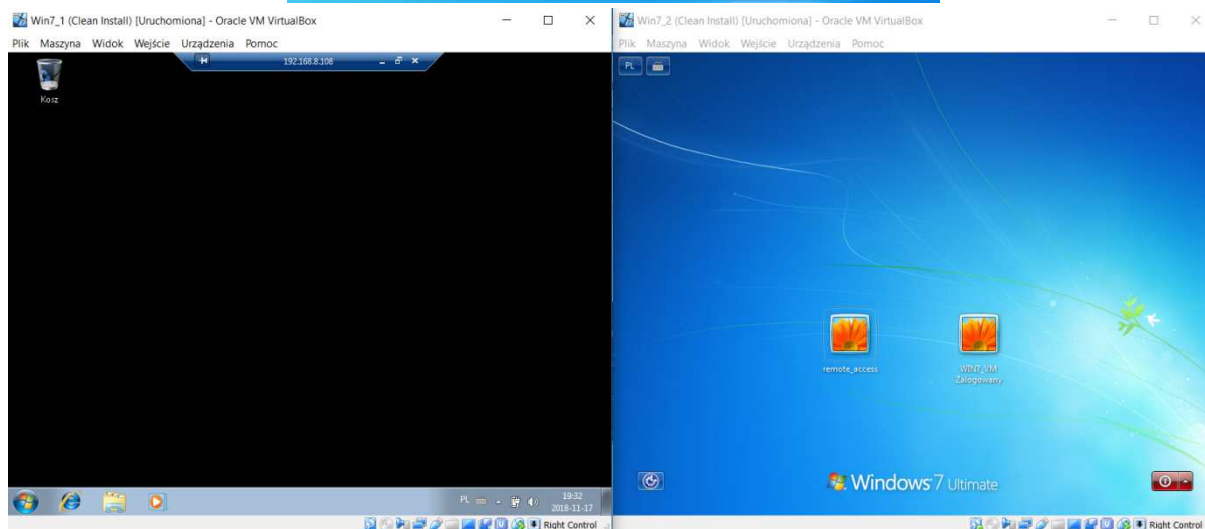
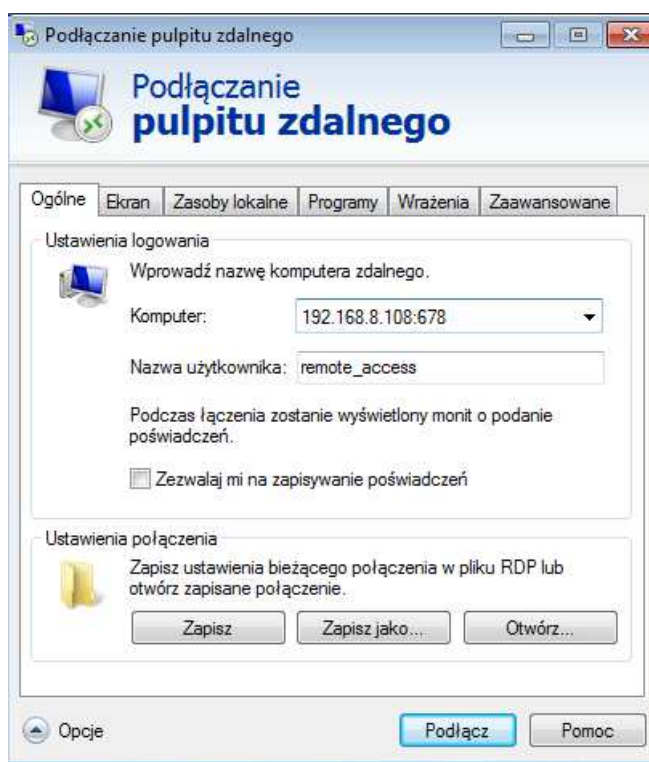


Fundusze Europejskie
Wiedza Edukacja Rozwój

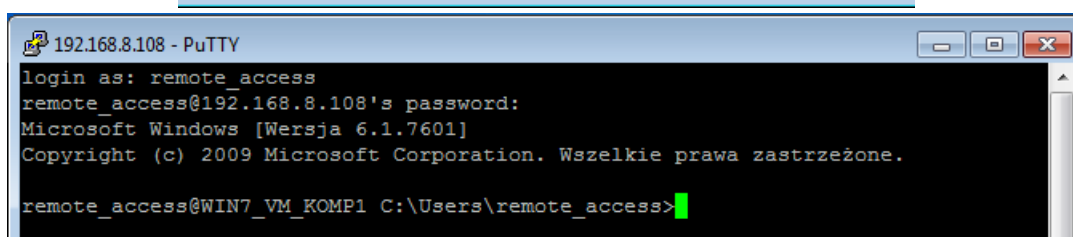
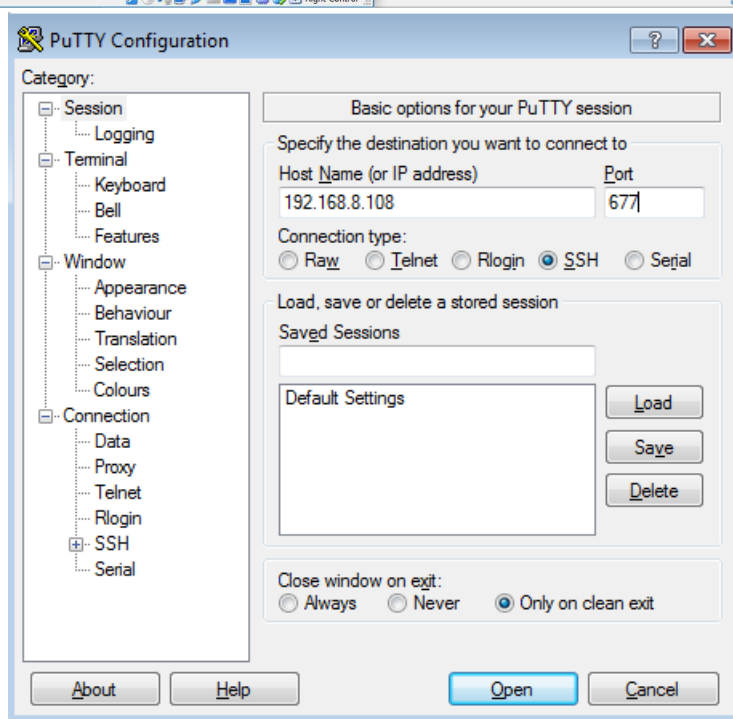
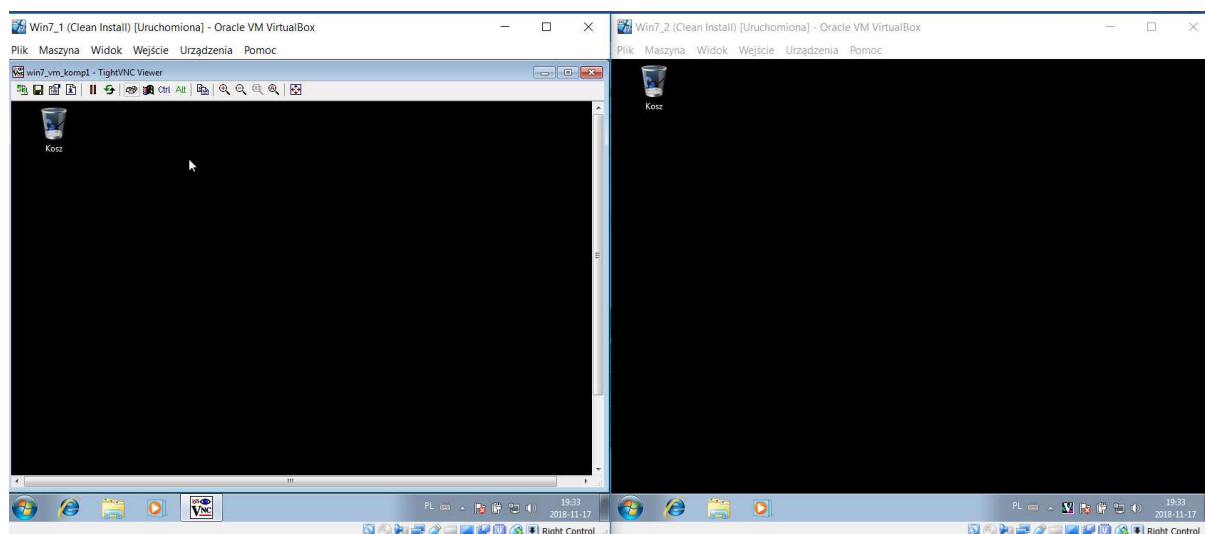


Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz Społeczny



Projekt „SezAM wiedzy, kompetencji i umiejętności” jest współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego w ramach Programu Operacyjnego Wiedza Edukacja Rozwój



Wygląda na to, że przekierowanie portów się udało i mamy dostęp do kontroli zdalnej z poziomu sieci zewnętrznej. Pamiętajmy, że jeśli przekierowanie portów nie działa tak jak powinno, możemy je przetestować za pomocą programów paping i PortListener.

4. Zadania

Na każdym etapie zadania twórz screenshot'y (w nazwach powinna znajdować się numeracja

wskazująca wykonywaną kolejność kroków), a następnie spakuj do archiwum zip o nazwie WdKZ_LAB_NrAlbumu oraz wyślij na adres e-mail podany przez prowadzącego zajęcia laboratoryjne.

4.1 Skonfiguruj i przetestuj działanie programów do pomocy zdalnej

- Umieść maszyny w oddzielnych sieciach (pamiętaj by nie używać podwójnej translacji NAT w maszynie poddawanej zdalnej pomocy)
- Uruchom udzielanie Zdalnej

4.2 Dokonaj konfiguracji i testów działania zdalnej kontroli systemu Windows

- Umieść obie maszyny w tej samej podsieci lokalnej (dowolna metoda)
- Skonfiguruj narzędzie Pulpitu zdalnego na jednej z maszyn i dokonaj połączenia z drugiej
- Zainstaluj i skonfiguruj narzędzie TightVNC Server na maszynie drugiej i TightVNC Viewer na maszynie pierwszej.
- Dokonaj

4.3 Wykonaj kontrolę zdalną maszyny za translacją NAT z maszyny z sieci zewnętrznej.

- Umieść maszynę pierwszą w sieci zewnętrznej, a maszynę drugą za NAT wirtualnego routera
- Dokonaj przekierowania potrzebnych portów
- Dokonaj

Literatura

1. A. Kisielewicz, Wprowadzenie do informatyki, Helion, Gliwice 2002
2. Scott H. A. Clark, W sercu PC – wg Petera Nortona, Helion, Gliwice 2002
3. J. Shim, J. Siegel, R. Chi, Technologia Informacyjna, Dom Wydawniczy ABC, Warszawa, 1999
4. A. Silberschatz, P.B. Galvin, G. Gagne, Podstawy systemów operacyjnych, WNT, Warszawa 2006
5. A. S. Twenbaum, Systemy operacyjne, Helion, Gliwice 2010
6. P. Beynon-Davies, Systemy baz danych, WNT, Warszawa 2000
7. W. Stallings, Systemy operacyjne, Struktura i zasady budowy, PWN, Warszawa 2006
8. A. Jakubowski, Podstawy SQL. Ćwiczenia praktyczne, Helion, Gliwice 2004