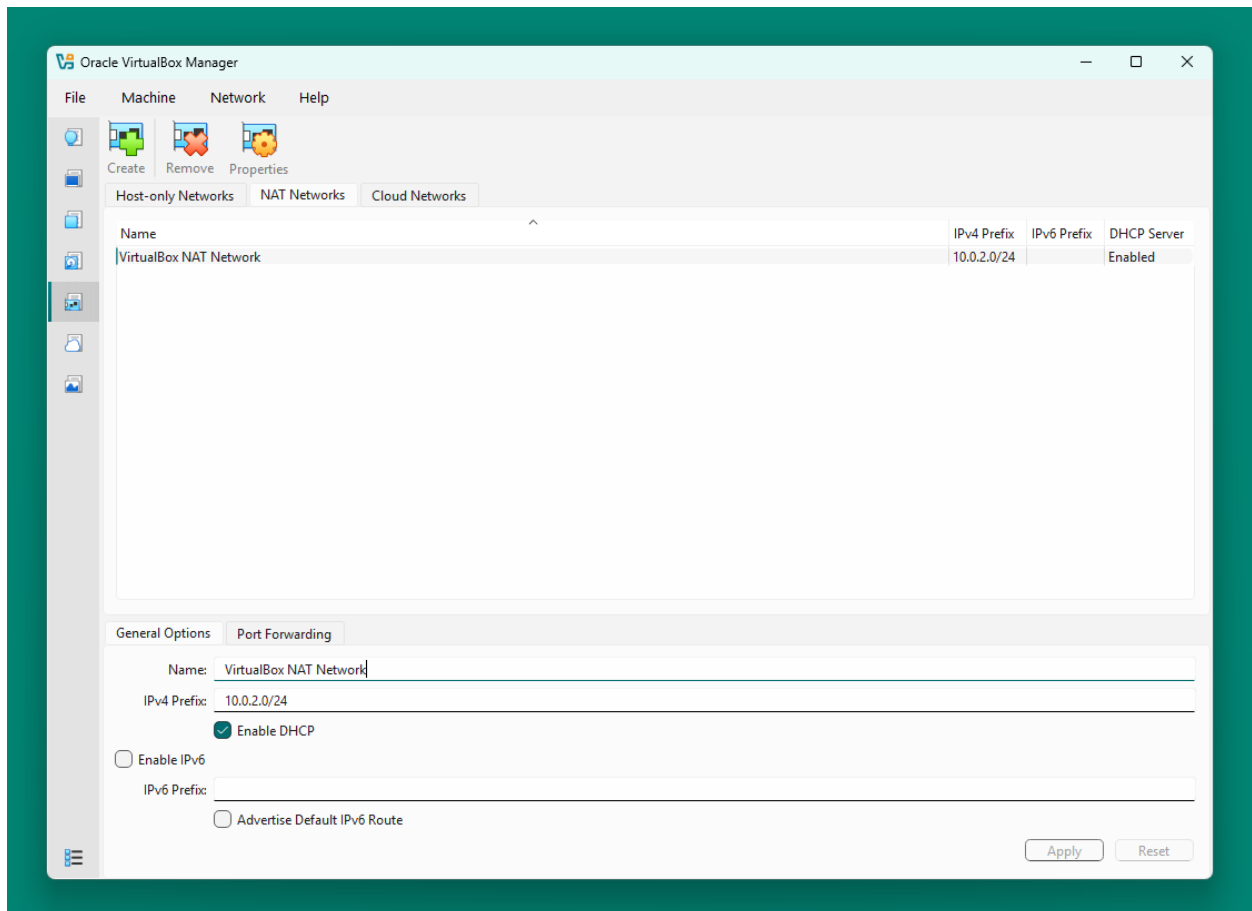


Bartosz Bieniek

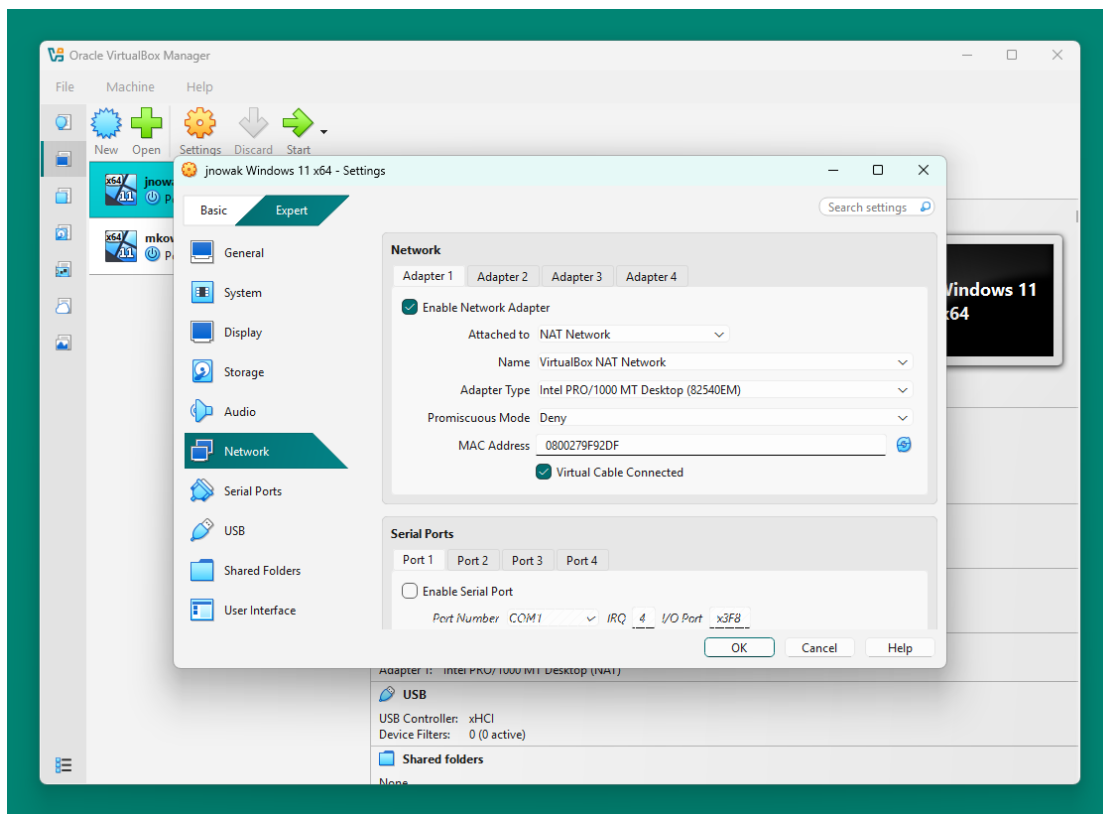
gr. 7, st. 1, sem. 3, Informatyka RMS

Przygotowanie środowiska.

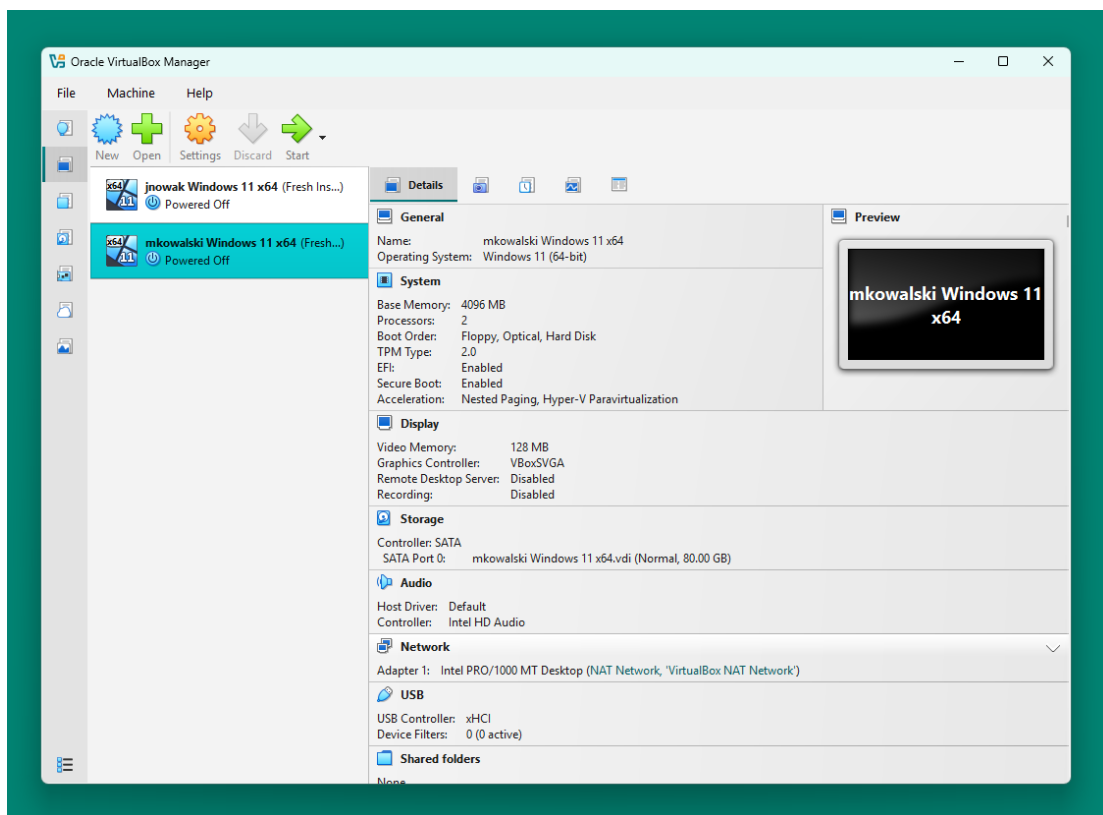
Do realizacji zadania wykorzystam dwie maszyny wirtualne z systemem Windows 11, uruchomione pod kontrolą oprogramowania Oracle VirtualBox. Interfejsy sieciowe obydwu z nich zostaną ustawione w trybie sieci NAT, która pozwala na komunikację maszyn ze sobą i internetem.



Zrzut ekranu 1 Konfiguracja nowej sieci NAT.



Zrzut ekranu 2 Przyłączenie maszyny wirtualnej do utworzonej sieci.

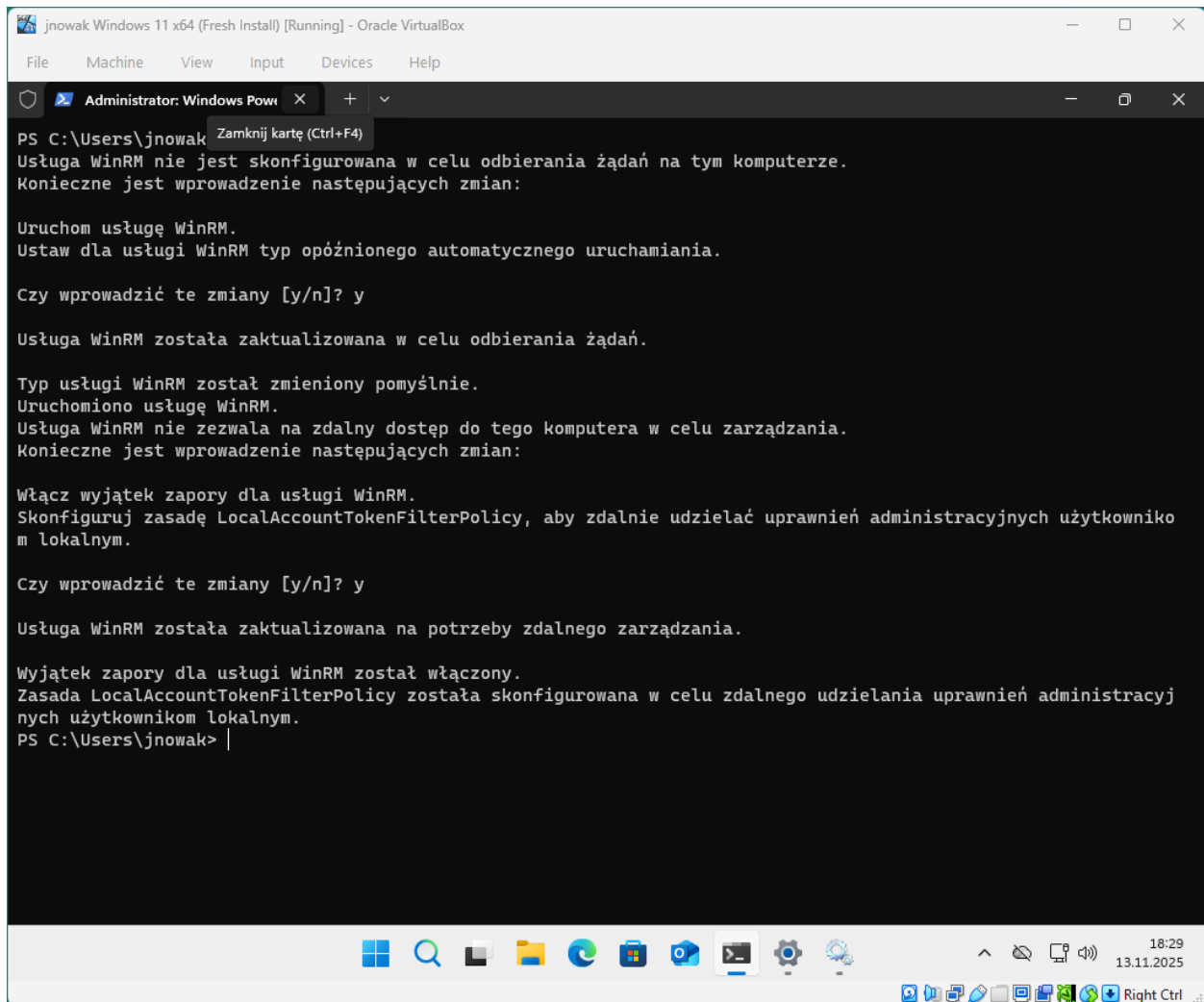


Zrzut ekranu 3 Podsumowanie konfiguracji maszyn wirtualnych.

Zadanie 1. Konfiguracja *WinRM* i *OpenSSH*.

a. *WinRM*

Mechanizm WinRM pozwala zdalnie wykonywać polecenia PowerShell na komputerach z systemem Windows. Aby ją skonfigurować, należy wykonać w wierszu poleceń (uruchomionym jako administrator) polecenie `winrm qc` (`winrm quickconfig`), które skonfiguruje i uruchomi usługę *WinRM*, a także doda wyjątek do zapory sieciowej.



```
jnowak Windows 11 x64 (Fresh Install) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Administrator: Windows PowerShell
PS C:\Users\jnowak> winrm qc
Zamknij kartę (Ctrl+F4)
Usługa WinRM nie jest skonfigurowana w celu odbierania żądań na tym komputerze.
Konieczne jest wprowadzenie następujących zmian:

Uruchom usługę WinRM.
Ustaw dla usługi WinRM typ opóźnionego automatycznego uruchamiania.

Czy wprowadzić te zmiany [y/n]? y

Usługa WinRM została zaktualizowana w celu odbierania żądań.

Typ usługi WinRM został zmieniony pomyślnie.
Uruchomiono usługę WinRM.
Usługa WinRM nie zezwala na zdalny dostęp do tego komputera w celu zarządzania.
Konieczne jest wprowadzenie następujących zmian:

Włącz wyjątek zapory dla usługi WinRM.
Skonfiguruj zasadę LocalAccountTokenFilterPolicy, aby zdalnie udzielać uprawnień administracyjnych użytkownikom lokalnym.

Czy wprowadzić te zmiany [y/n]? y

Usługa WinRM została zaktualizowana na potrzeby zdalnego zarządzania.

Wyjątek zapory dla usługi WinRM został włączony.
Zasada LocalAccountTokenFilterPolicy została skonfigurowana w celu zdalnego udzielania uprawnień administracyjnych użytkownikom lokalnym.
PS C:\Users\jnowak>
```

Zrzut ekranu 4 Szybka konfiguracja usługi WinRM poleceniem `winrm quickconfig`.

W przypadku, gdy połączenie w ustawieniach systemu będzie skonfigurowane jako „Publiczne” (a nie „Domena” lub „Prywatne”), wyjątek zapory sieciowej nie będzie działać – nie będzie dało się podłączyć zdalnie do komputera.

```
Uruchomiono usługę WinRM.
WSManFault
  Message
    ProviderFault
      WSMANFault
        Message = Wyjątek zapory usługi WinRM nie będzie działać, ponieważ dla jednego z typów połączeń
        sieciowych na tym komputerze ustawiono wartość Publiczne. Zmień typ połączenia sieciowego na Domena lub Pryw
        atne i ponów próbę.

Numer błędu: -2144108183 0x80338169
Wyjątek zapory usługi WinRM nie będzie działać, ponieważ dla jednego z typów połączeń sieciowych na tym komput
erze ustawiono wartość Publiczne. Zmień typ połączenia sieciowego na Domena lub Prywatne i ponów próbę.
PS C:\Users\jnowak>
```

Zrzut ekranu 5 Informacja o błędzie. Wyjątek zapory, konieczny do poprawnego działania usługi WinRM, nie działa w sieciach publicznych.

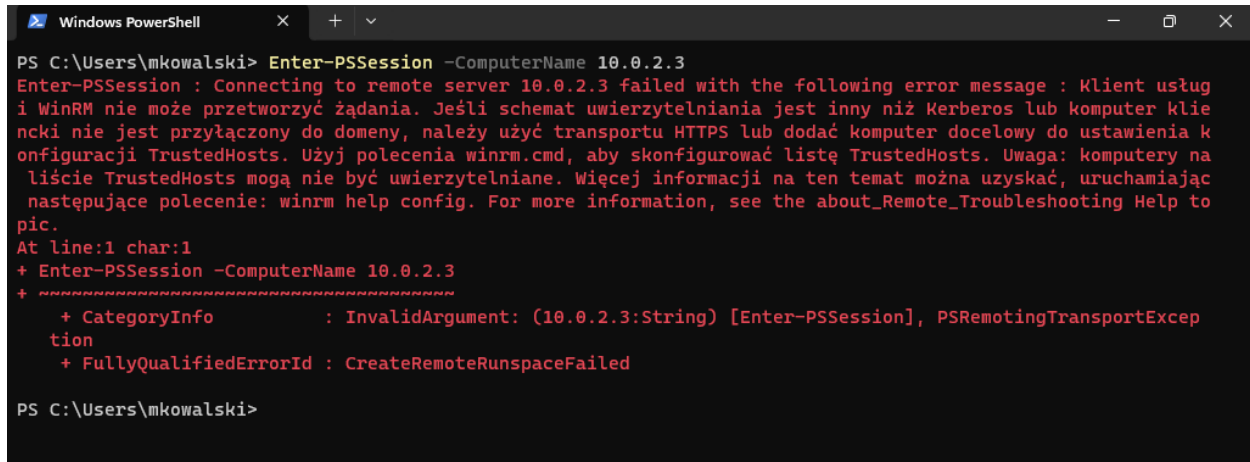
Aktywną konfigurację można sprawdzić poleceniem `winrm e winrm/config/listener`.

```
Administrator: Windows Powe
PS C:\Users\jnowak> winrm e winrm/config/listener
Listener
  Address = *
  Transport = HTTP
  Port = 5985
  Hostname
  Enabled = true
  URLPrefix = wsman
  CertificateThumbprint
  ListeningOn = 10.0.2.3, 127.0.0.1, ::1, fe80::2430:41b5:40c7:facb%5

PS C:\Users\jnowak> |
```

Zrzut ekranu 6 Wynik działania polecenia sprawdzającego aktualną konfigurację WinRM.

Aby podłączyć się przez WinRM do innego komputera, skorzystamy z polecenia `Enter-PSSession -ComputerName <IP>`.



```
PS C:\Users\mkowalski> Enter-PSSession -ComputerName 10.0.2.3
Enter-PSSession : Connecting to remote server 10.0.2.3 failed with the following error message : Klient usług
i WinRM nie może przetworzyć żądania. Jeśli schemat uwierzytelniania jest inny niż Kerberos lub komputer klie
ncki nie jest przyłączony do domeny, należy użyć transportu HTTPS lub dodać komputer docelowy do ustawienia k
onfiguracji TrustedHosts. Użyj polecenia winrm.cmd, aby skonfigurować listę TrustedHosts. Uwaga: komputery na
liście TrustedHosts mogą nie być uwierzytelniane. Więcej informacji na ten temat można uzyskać, uruchamiając
następujące polecenie: winrm help config. For more information, see the about_Remote_Troubleshooting Help to
pic.
At line:1 char:1
+ Enter-PSSession -ComputerName 10.0.2.3
+ ~~~~~
+ CategoryInfo          : InvalidArgument: (10.0.2.3:String) [Enter-PSSession], PSRemotingTransportExcep
tion
+ FullyQualifiedErrorId : CreateRemoteRunspaceFailed

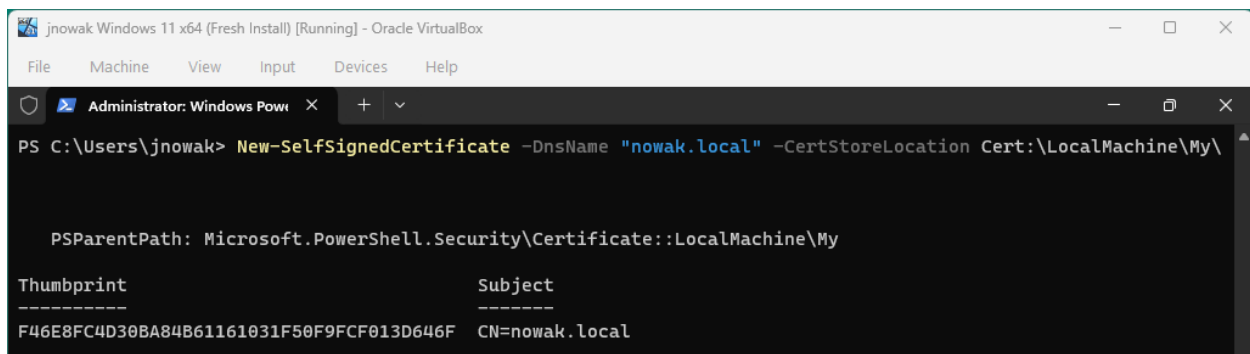
PS C:\Users\mkowalski>
```

Zrzut ekranu 7 Informacja o błędzie. Niewystarczający poziom zabezpieczeń.

Klient nie może skorzystać ze schematu uwierzytelniania *Kerberos* (nie jest w domenie), komputer docelowy nie jest dodany do listy *TrustedHosts*, ani nie używamy połączenia *HTTPS*, stąd generowany jest komunikat o błędzie.

Aby rozwiązać ten problem, możemy, na przykład, skonfigurować połączenie przez *HTTPS*. Konieczne jest wówczas wygenerowanie certyfikatu po stronie komputera docelowego, poniższym poleceniem.

`New-SelfSignedCertificate -DnsName "<nazwa_hosta>" -CertStoreLocation Cert:\LocalMachine\My`



```
jnowak Windows 11 x64 (Fresh Install) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Administrator: Windows Powe
PS C:\Users\jnowak> New-SelfSignedCertificate -DnsName "nowak.local" -CertStoreLocation Cert:\LocalMachine\My

PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My

Thumbprint                               Subject
-----
F46E8FC4D30BA84B61161031F50F9FCF013D646F  CN=nowak.local
```

Zrzut ekranu 8 Generowanie nowego certyfikatu do wykorzystania przy połączeniach WinRM.

Zwróćmy uwagę, że do poprawnego działania usługi *WinRM* konieczne jest ustawienie pełnej kwalifikowanej nazwy domeny albo *adresu IP*. W instrukcji zadania zostaliśmy poproszeni o ustawienie nazwy „nowak.local”, co też zrobimy.

Następnie należy skonfigurować nasłuchiwanie dla protokołu *HTTPS* i wskazać wykorzystywany certyfikat. Służy do tego polecenie poniżej.

```
winrm create winrm/config/listener?Address=*&Transport=HTTPS
'@{HostName="<nazwa_hosta>"; CertificateThumbprint="<...>"}'.
```

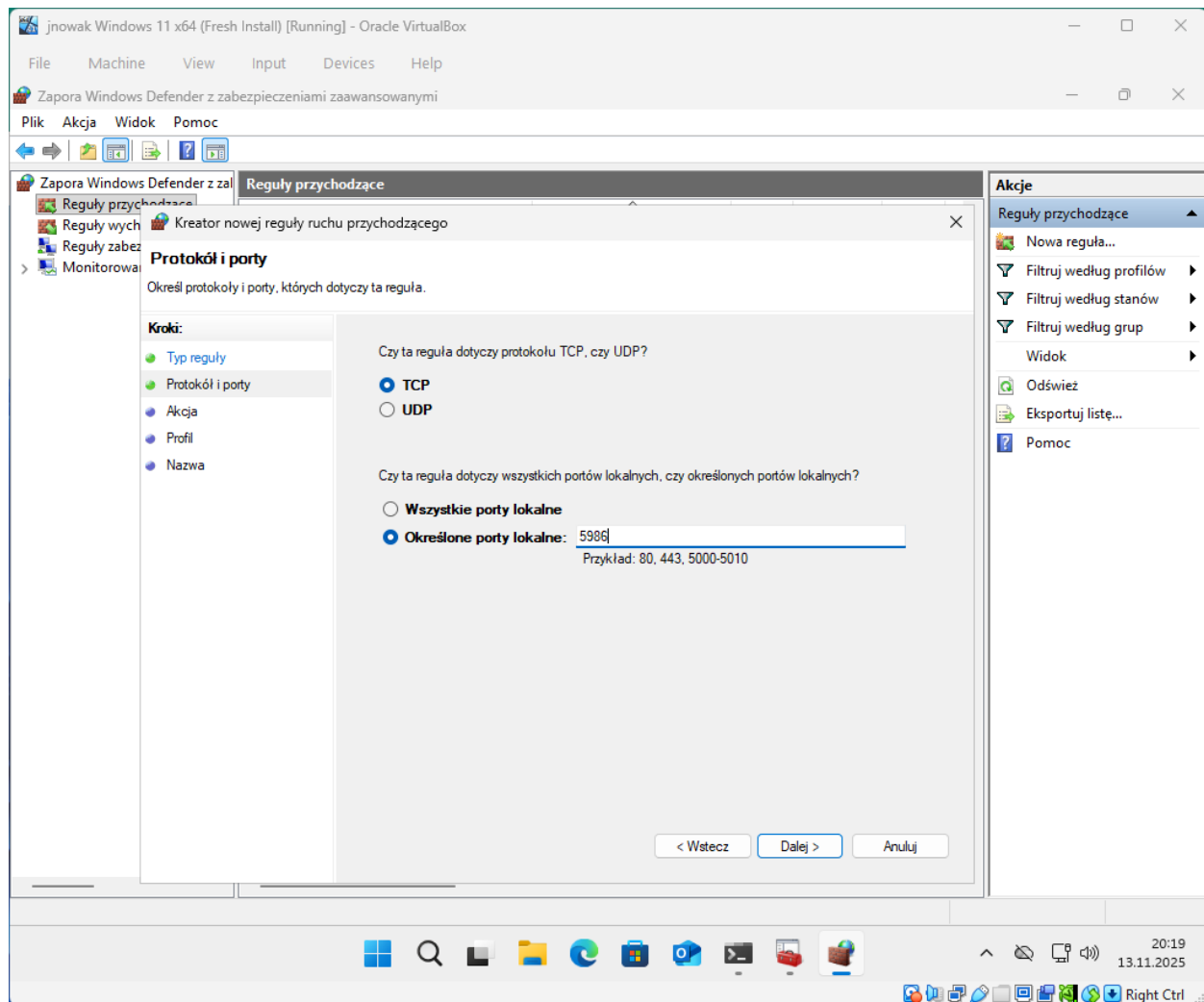
```
PS C:\Users\jnowak> winrm create winrm/config/listener?Address=*&Transport=HTTPS '@{HostName="nowak.local"; CertificateThumbprint="F46E8FC4D30BA84B61161031F50F9FCF013D646F"}'
ResourceCreated
    Address = http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
    ReferenceParameters
        ResourceURI = http://schemas.microsoft.com/wbem/wsman/1/config/listener
    SelectorSet
        Selector: Address = *, Transport = HTTPS

PS C:\Users\jnowak> winrm e winrm/config/listener
Listener
    Address = *
    Transport = HTTP
    Port = 5985
    Hostname
    Enabled = true
    URLPrefix = wsman
    CertificateThumbprint
    ListeningOn = 10.0.2.3, 127.0.0.1, ::1, fe80::2430:41b5:40c7:facb%5

Listener
    Address = *
    Transport = HTTPS
    Port = 5986
    Hostname = nowak.local
    Enabled = true
    URLPrefix = wsman
    CertificateThumbprint = F46E8FC4D30BA84B61161031F50F9FCF013D646F
    ListeningOn = 10.0.2.3, 127.0.0.1, ::1, fe80::2430:41b5:40c7:facb%5
```

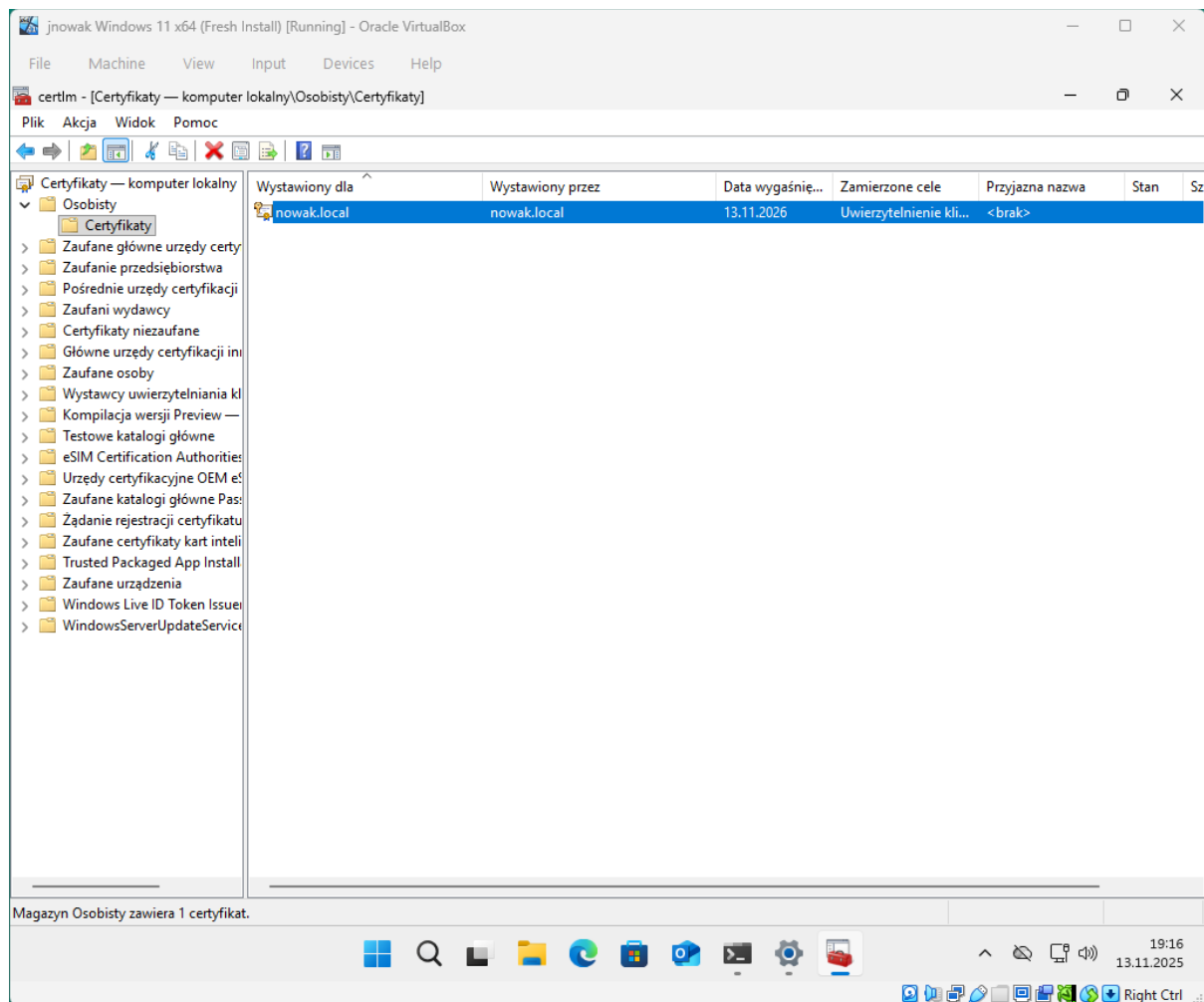
Zrzut ekranu 9 Skonfigurowanie nasłuchiwania dla protokołu *HTTPS*.

WinRM nie skonfiguruje automatycznie nowego wyjątku w zaporze, dlatego musimy to zrobić ręcznie. W kreatorze reguł dla połączeń przychodzących należy wybrać typ „Port”, zaznaczyć protokół TCP i wskazać numer portu do otwarcia.



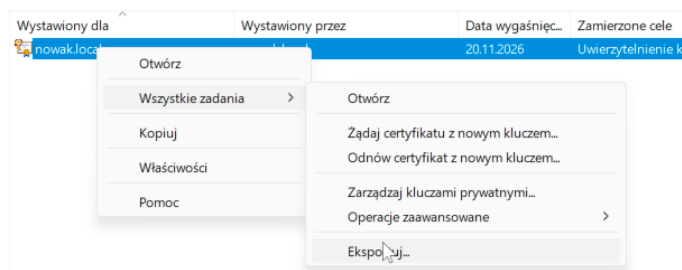
Zrzut ekranu 10 Konfiguracja wyjątku zapory sieciowej dla połączeń WinRM po HTTPS.

Pozostało już tylko wyeksportować i przenieść klucz publiczny na komputer, z którego łączy się klient. Wykorzystamy do tego narzędzie *certlm*.

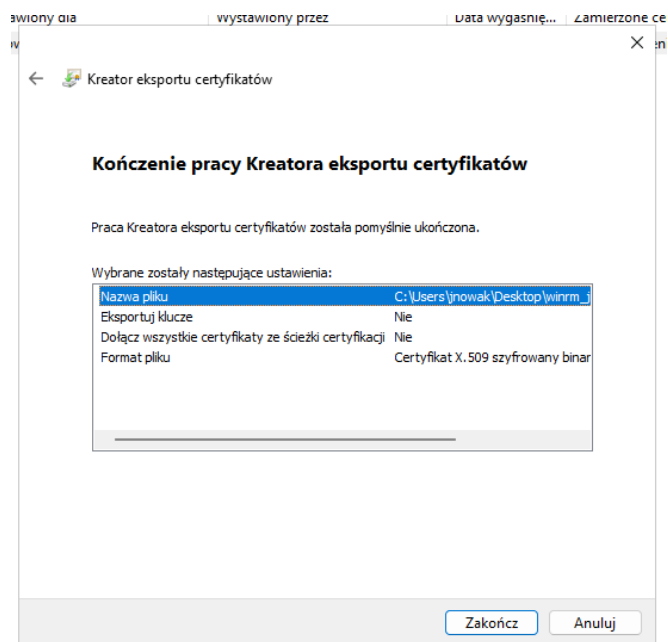


Zrzut ekranu 11 Narzędzie certlm.

Certyfikat znajduje się w folderze „Osobisty” → „Certyfikaty”, zgodnie z tym co wskazaliśmy w poleceniu generującym. Aby go wyeksportować, z menu kontekstowego należy wybrać opcję „Wszystkie zadania” → „Eksportuj” i w kolejnych krokach odznaczyć eksport klucza prywatnego.

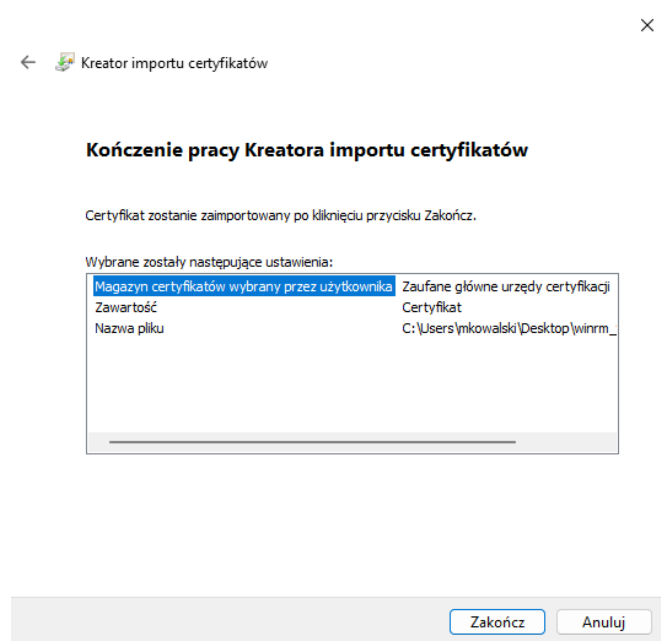


Zrzut ekranu 12 Pozycja eksportu w menu kontekstowym.



Zrzut ekranu 13 Eksportowanie klucza publicznego certyfikatu.

Wyeksportowany plik trzeba teraz przenieść na maszynę kliencką, na przykład wykorzystując przeciąganie plików między komputerem hosta, a maszynami wirtualnymi (konieczne jest wcześniejsze zainstalowanie „dodatków gościa”). Certyfikat należy otworzyć, kliknąć na przycisk „Zainstaluj certyfikat...”, wybrać opcję instalacji dla całego komputera i podać ścieżkę magazynu „Zaufane główne urzędy certyfikacji”.



Zrzut ekranu 14 Import klucza na nowym komputerze

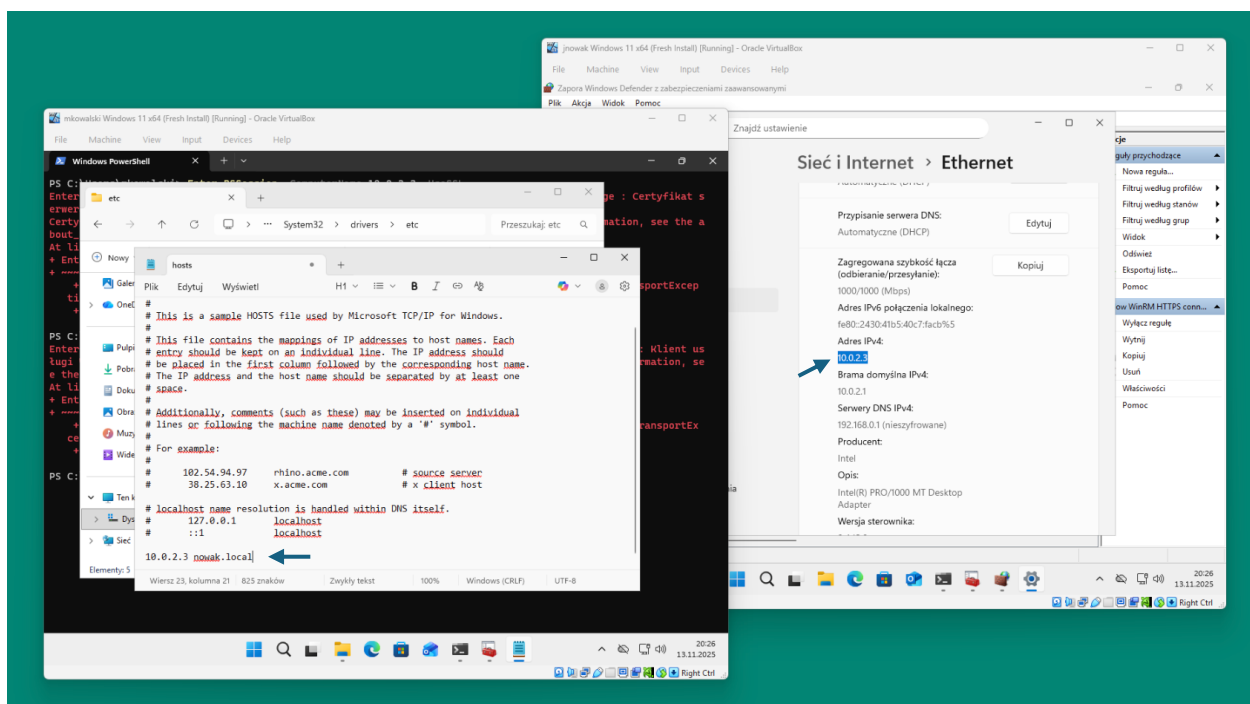
Importu można w analogiczny sposób dokonać także z poziomu wykorzystanego wcześniej narzędzia *certlm*.

Tak przeprowadzona konfiguracja pozwoliłaby na połączenie się do maszyny docelowej, jednak użycie certyfikatu wymaga pełnej zgodności części hosta – certyfikat stworzyliśmy dla domeny *nowak.local*.

```
Windows PowerShell
PS C:\Users\mkowalski> Enter-PSSession -ComputerName 10.0.2.3 -UseSSL
Enter-PSSession : Connecting to remote server 10.0.2.3 failed with the following error message : Certyfikat s
erwera na komputerze docelowym (10.0.2.3:5986) zawiera następujące błędy:
Certyfikat SSL zawiera nazwę pospolitą (CN), która nie pasuje do nazwy hosta. For more information, see the a
bout_Remote_Troubleshooting Help topic.
At line:1 char:1
+ Enter-PSSession -ComputerName 10.0.2.3 -UseSSL
+ ~~~~~
+ CategoryInfo          : InvalidArgument: (10.0.2.3:String) [Enter-PSSession], PSRemotingTransportExcep
tion
+ FullyQualifiedErrorId : CreateRemoteRunspaceFailed
```

Zrzut ekranu 15 Błąd informujący o niezgodności części hosta z tą zapisaną w certyfikacie.

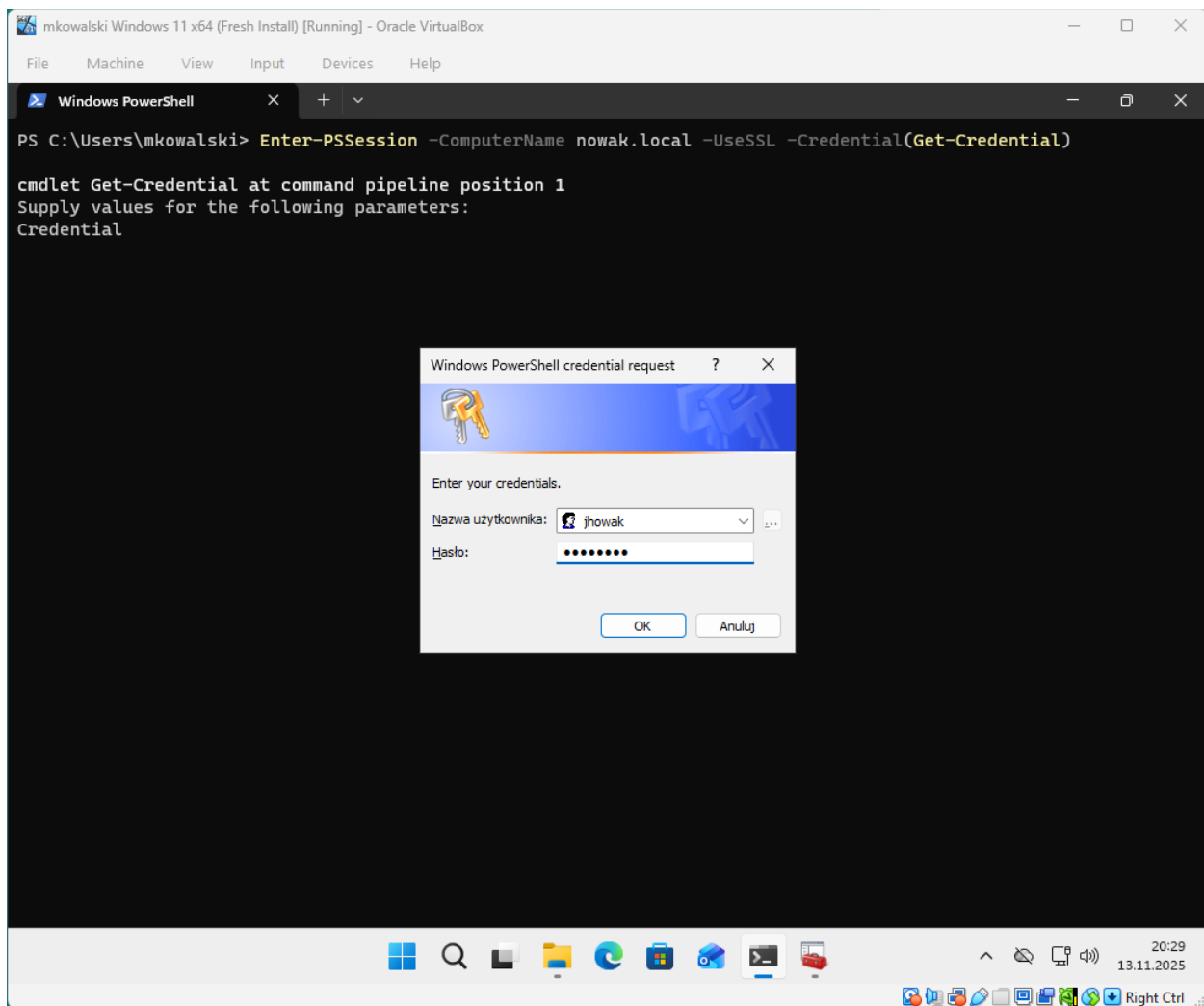
W systemie Windows można dodać nowy wpis do pliku
C:\Windows\System32\drivers\ets\hosts, który spowoduje zmianę nazwy
mnemonicznej na znany nam adres IP komputera.



Zrzut ekranu 16 Konfiguracja w pliku hosts.

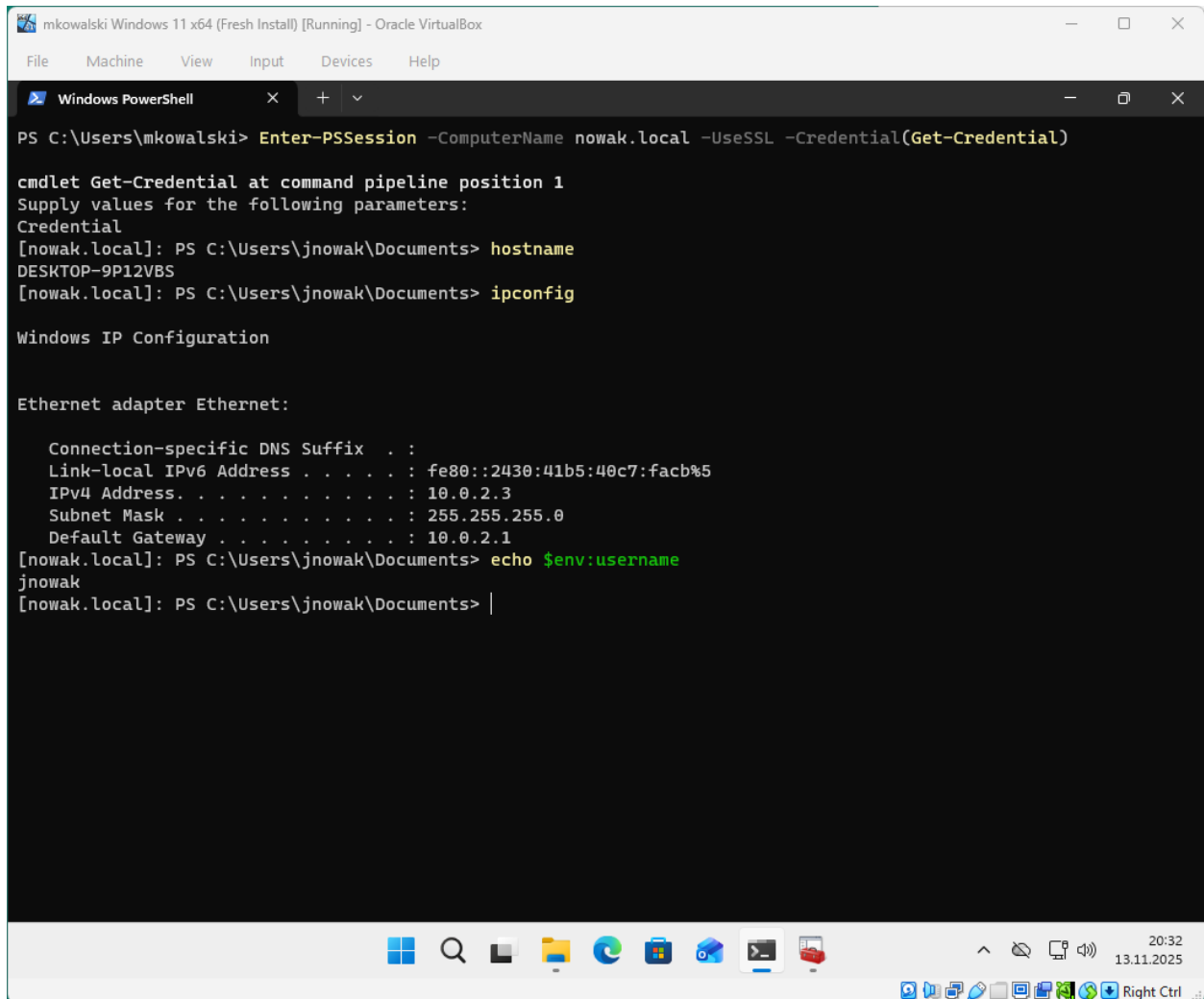
Teraz możemy już bez problemów podłączyć się do komputera docelowego, do czego wykorzystamy poniższe polecenie.

```
Enter-PSSession -ComputerName nowak.local -UseSSL -
Credential(GetCredential)
```



Zrzut ekranu 17 Logowanie do zdalnego komputera.

Gdy jesteśmy już podłączeni, możemy wykonać kilka poleceń, które potwierdzą, że polecenia wykonujemy na komputerze zdalnym – na przykład wypisać nazwę komputera, użytkownika czy adres IP.



```
PS C:\Users\mkowalski> Enter-PSSession -ComputerName nowak.local -UseSSL -Credential(Get-Credential)

cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
[nowak.local]: PS C:\Users\jnowak\Documents> hostname
DESKTOP-9P12VBS
[nowak.local]: PS C:\Users\jnowak\Documents> ipconfig

Windows IP Configuration

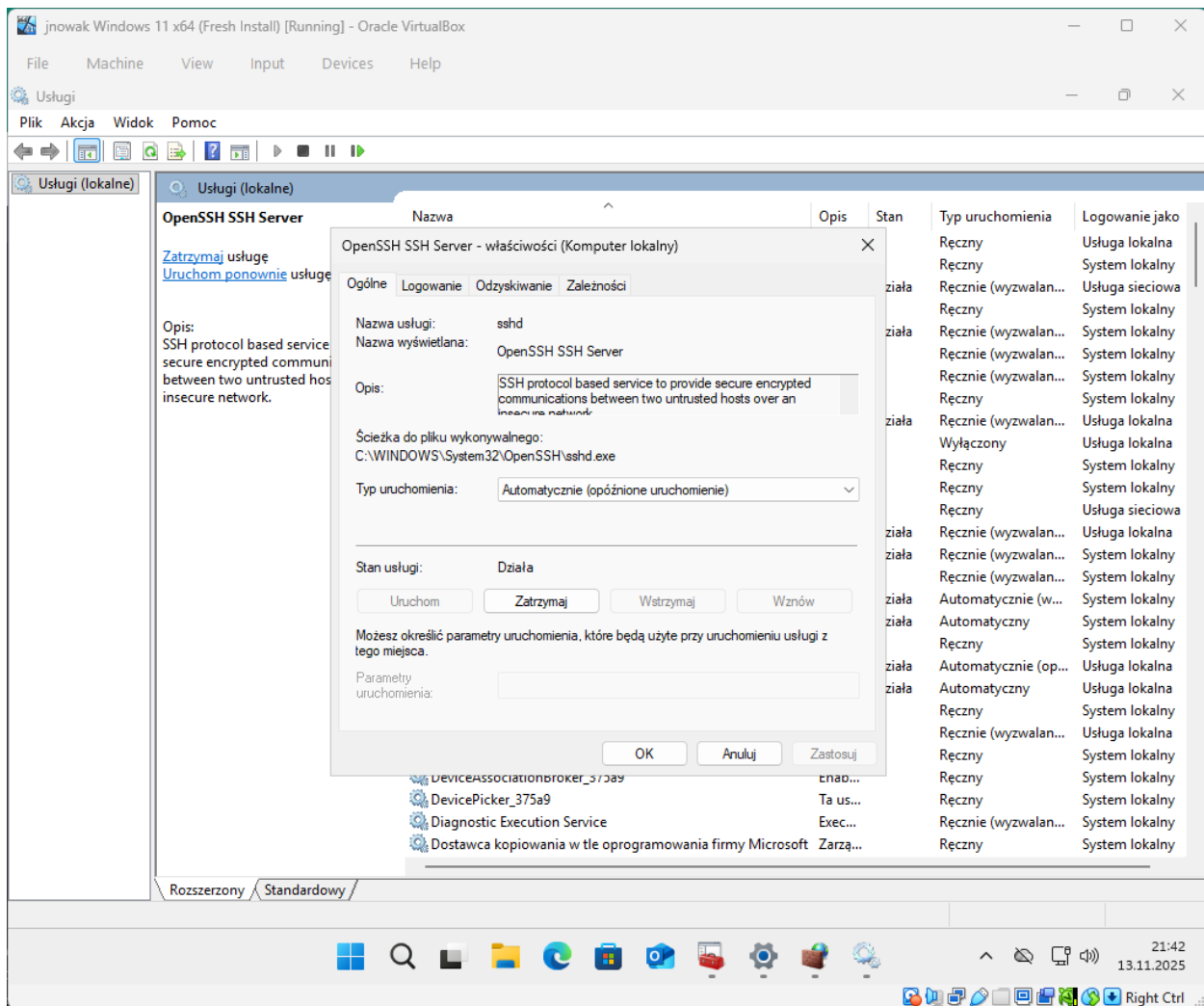
Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::2430:41b5:40c7:facb%5
    IPv4 Address. . . . . : 10.0.2.3
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.2.1
[nowak.local]: PS C:\Users\jnowak\Documents> echo $env:username
jnowak
[nowak.local]: PS C:\Users\jnowak\Documents> |
```

Zrzut ekranu 18 Wypisanie przykładowych informacji o komputerze z poziomu sesji zdalnej WinRM.

b. OpenSSH

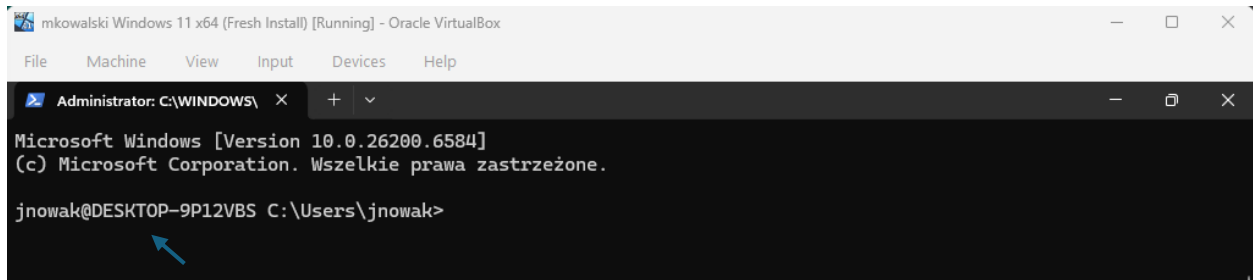
Do nawiązania połączenia przez SSH konieczne jest zainstalowanie serwera OpenSSH na urządzeniu zdalnym oraz klienta na komputerze, z którego planujemy się połączyć. W przypadku systemu Windows, konieczne jest doinstalowanie jedynie tego pierwszego. Można to zrobić z poziomu ustawień systemu w zakładce „System” → „Funkcje opcjonalne” → „Wyświetl funkcje” → „Zobacz dostępne funkcje”, następnie odszukać na liście „Serwer OpenSSH” i zainstalować. Po instalacji można uruchomić ponownie system, albo włączyć usługę ręcznie.



Zrzut ekranu 19 Ręczne włączenie usługi serwera OpenSSH.

Aby podłączyć się do tak skonfigurowanego komputera zdalnego, wystarczy skorzystać z polecenia `ssh <nazwa_użytkownika>@<host>`, na przykład `ssh jnowak@10.0.2.3`.

Aby potwierdzić poprawność połączenia się ze zdalnym komputerem, możemy na przykład wykonać te same polecenia, co dla mechanizmu WinRM albo sprawdzić zawartość prefiksu wejścia w terminalu.



```
Administrator: C:\WINDOWS\ X + v
Microsoft Windows [Version 10.0.26200.6584]
(c) Microsoft Corporation. Wszelkie prawa zastrzeżone.

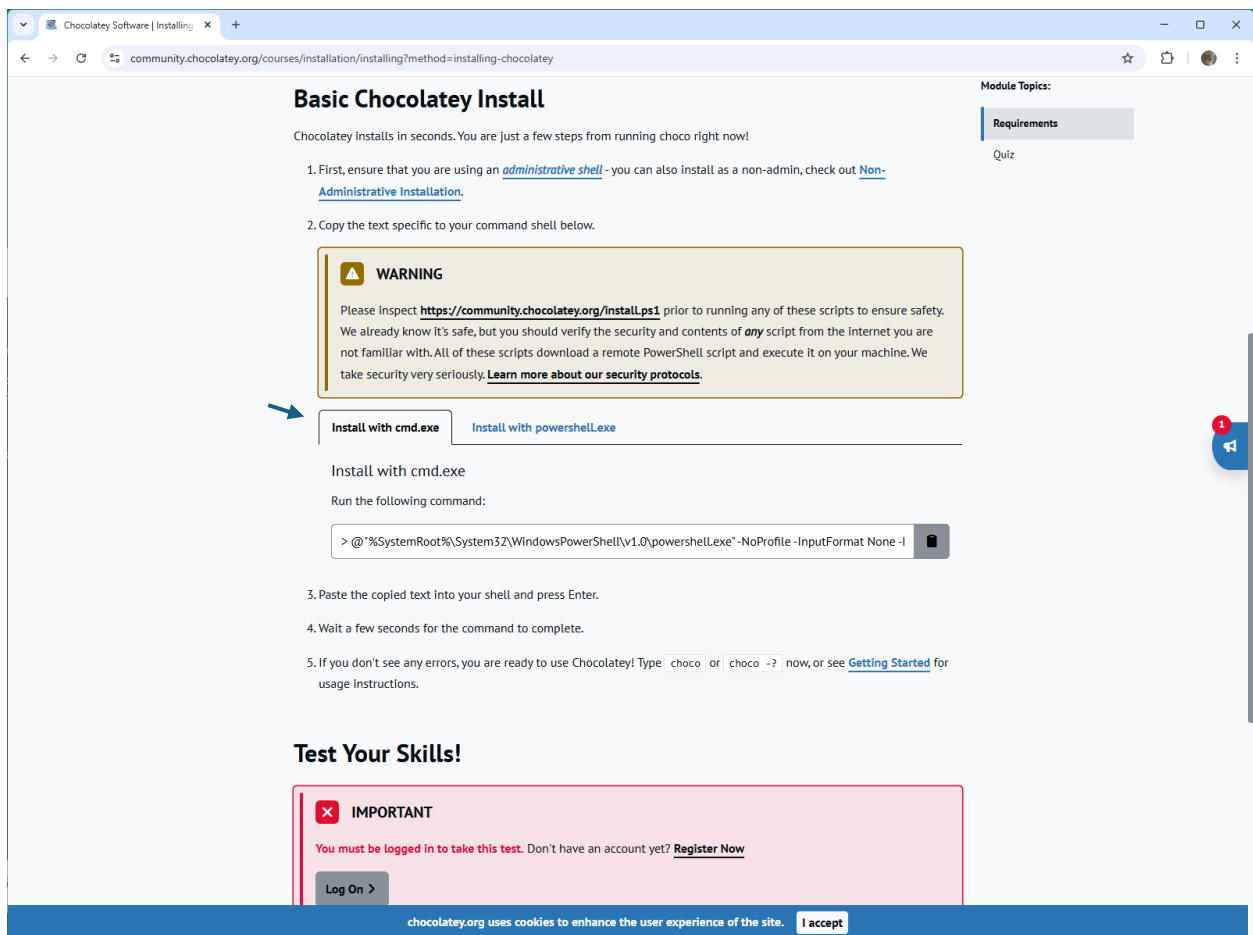
jnowak@DESKTOP-9P12VBS C:\Users\jnowak>
```

Zrzut ekranu 20 Udał się połączenie do komputera zdalnego na użytkownika jnowak.

Zadanie 2. Instalacja oprogramowania Chocolatey.

Chocolatey to menedżer pakietów, który umożliwia instalowanie i zarządzanie programami z poziomu terminala. Do jego instalacji wykorzystuje się specjalny skrypt, który sam pobierze wszystkie wymagane składniki. Przechodząc do dokumentacji można znaleźć dodatkowe opcje instalacji, między innymi taką wykorzystującą cmd.exe (a nie PowerShell, który nie jest bezpośrednio dostępny przez SSH).

community.chocolatey.org/courses/installation/installing?method=installing-chocolatey



The screenshot shows a web browser window with the URL `community.chocolatey.org/courses/installation/installing?method=installing-chocolatey`. The page title is "Basic Chocolatey Install". It contains a list of steps for installation, a warning box, and a command to run in cmd.exe. A blue arrow points to the "Install with cmd.exe" button. The warning box contains a warning icon and text about security. The command box shows the command to run in cmd.exe. The page also has a sidebar with "Module Topics" and a footer with a cookie notice.

Basic Chocolatey Install

Chocolatey installs in seconds. You are just a few steps from running choco right now!

1. First, ensure that you are using an [administrative shell](#) - you can also install as a non-admin, check out [Non-Administrative Installation](#).
2. Copy the text specific to your command shell below.

WARNING

Please inspect <https://community.chocolatey.org/install.ps1> prior to running any of these scripts to ensure safety. We already know it's safe, but you should verify the security and contents of *any* script from the Internet you are not familiar with. All of these scripts download a remote PowerShell script and execute it on your machine. We take security very seriously. [Learn more about our security protocols](#).

Install with cmd.exe [Install with powershell.exe](#)

Install with cmd.exe

Run the following command:

```
> @"%SystemRoot%\System32\WindowsPowerShell\v1.0\powershell.exe" -NoProfile -InputFormat None -I
```

3. Paste the copied text into your shell and press Enter.
4. Wait a few seconds for the command to complete.
5. If you don't see any errors, you are ready to use Chocolatey! Type `choco` or `choco -?` now, or see [Getting Started](#) for usage instructions.

Test Your Skills!

IMPORTANT

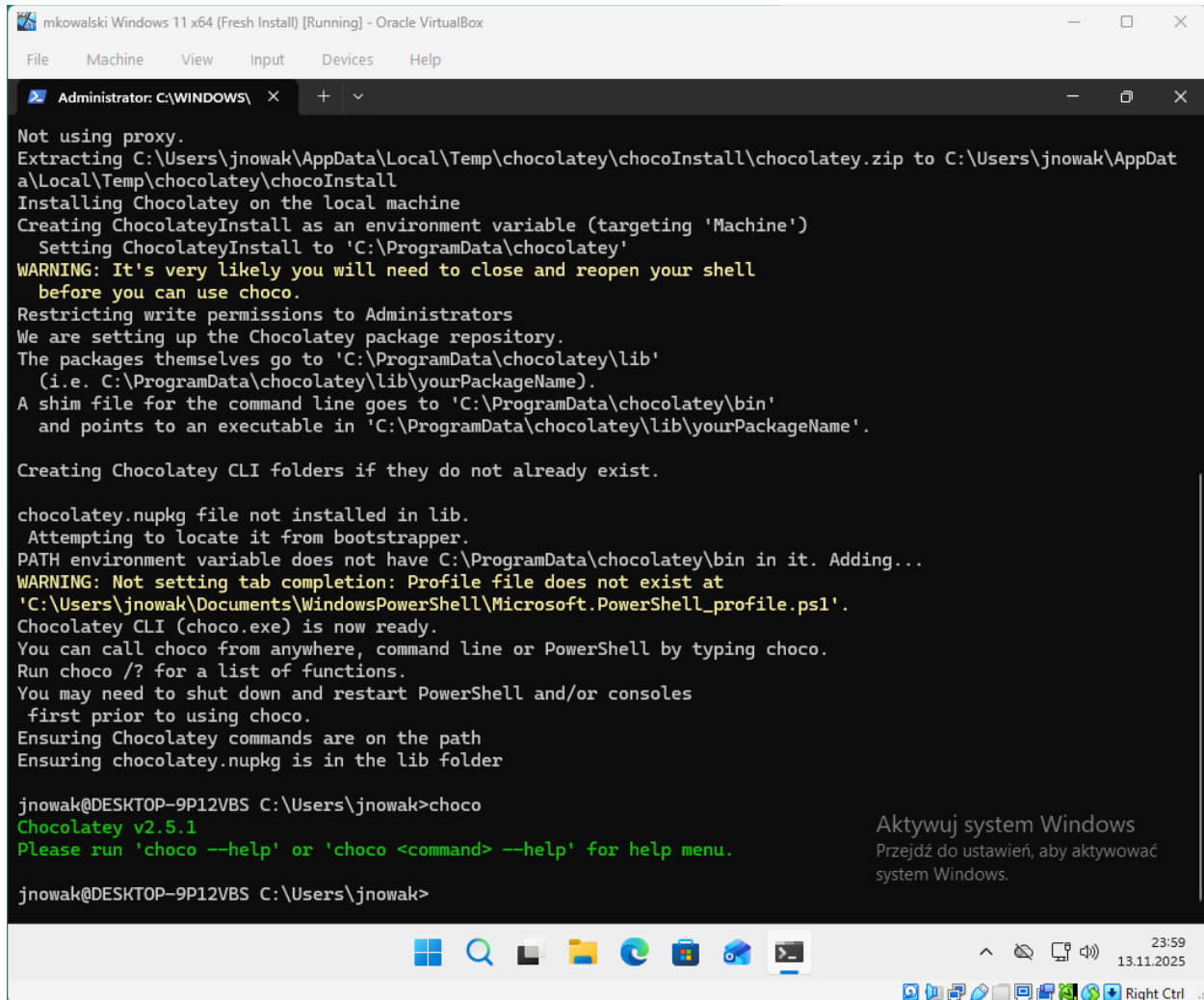
You must be logged in to take this test. Don't have an account yet? [Register Now](#)

[Log On >](#)

chocolatey.org uses cookies to enhance the user experience of the site. [I accept](#)

Zrzut ekranu 21 Strona ze skryptem instalacyjnym.

Po wklejeniu i uruchomieniu polecenia przez SSH, na komputerze zdalnym zostanie zainstalowany program Chocolatey.



```
Administrator: C:\WINDOWS\ X + v
Not using proxy.
Extracting C:\Users\jnowak\AppData\Local\Temp\chocolatey\chocoInstall\chocolatey.zip to C:\Users\jnowak\AppData\Local\Temp\chocolatey\chocoInstall
Installing Chocolatey on the local machine
Creating ChocolateyInstall as an environment variable (targeting 'Machine')
Setting ChocolateyInstall to 'C:\ProgramData\chocolatey'
WARNING: It's very likely you will need to close and reopen your shell
before you can use choco.
Restricting write permissions to Administrators
We are setting up the Chocolatey package repository.
The packages themselves go to 'C:\ProgramData\chocolatey\lib'
(i.e. C:\ProgramData\chocolatey\lib\yourPackageName).
A shim file for the command line goes to 'C:\ProgramData\chocolatey\bin'
and points to an executable in 'C:\ProgramData\chocolatey\lib\yourPackageName'.

Creating Chocolatey CLI folders if they do not already exist.

chocolatey.nupkg file not installed in lib.
Attempting to locate it from bootstrapper.
PATH environment variable does not have C:\ProgramData\chocolatey\bin in it. Adding...
WARNING: Not setting tab completion: Profile file does not exist at
'C:\Users\jnowak\Documents\WindowsPowerShell\Microsoft.PowerShell_profile.ps1'.
Chocolatey CLI (choco.exe) is now ready.
You can call choco from anywhere, command line or PowerShell by typing choco.
Run choco /? for a list of functions.
You may need to shut down and restart PowerShell and/or consoles
first prior to using choco.
Ensuring Chocolatey commands are on the path
Ensuring chocolatey.nupkg is in the lib folder

jnowak@DESKTOP-9P12VBS C:\Users\jnowak>choco
Chocolatey v2.5.1
Please run 'choco --help' or 'choco <command> --help' for help menu.

jnowak@DESKTOP-9P12VBS C:\Users\jnowak>
```

Zrzut ekranu 22 Instalacja programu Chocolatey. Sprawdzenie zainstalowanej wersji Chocolatey.

Po udanej instalacji możemy doinstalować pakiet narzędzi sieciowych bind-toolsonly, zawierającą między innymi polecenie dig (look-up DNS).

```
jnowak@DESKTOP-9P12VBS C:\Users\jnowak>choco search bind-toolsonly
Chocolatey v2.5.1
bind-toolsonly 9.16.28 [Approved]
1 packages found.

jnowak@DESKTOP-9P12VBS C:\Users\jnowak>choco install bind-toolsonly
Chocolatey v2.5.1
Installing the following packages:
bind-toolsonly
By installing, you accept licenses for the packages.
Downloading package from source 'https://community.chocolatey.org/api/v2/'
Progress: Downloading chocolatey-compatibility.extension 1.0.0... 100%
```

```
chocolatey-compatibility.extension v1.0.0 [Approved]
chocolatey-compatibility.extension package files install completed. Performing other installation steps.
Installed/updated chocolatey-compatibility extensions.
The install of chocolatey-compatibility.extension was successful.
Deployed to 'C:\ProgramData\chocolatey\extensions\chocolatey-compatibility'
Downloading package from source 'https://community.chocolatey.org/api/v2/'
Progress: Downloading chocolatey-core.extension 1.4.0... 100%

chocolatey-core.extension v1.4.0 [Approved]
chocolatey-core.extension package files install completed. Performing other installation steps.
Installed/updated chocolatey-core extensions.
The install of chocolatey-core.extension was successful.
Deployed to 'C:\ProgramData\chocolatey\extensions\chocolatey-core'
Downloading package from source 'https://community.chocolatey.org/api/v2/'
Progress: Downloading chocolatey-windowsupdate.extension 1.0.5... 100%

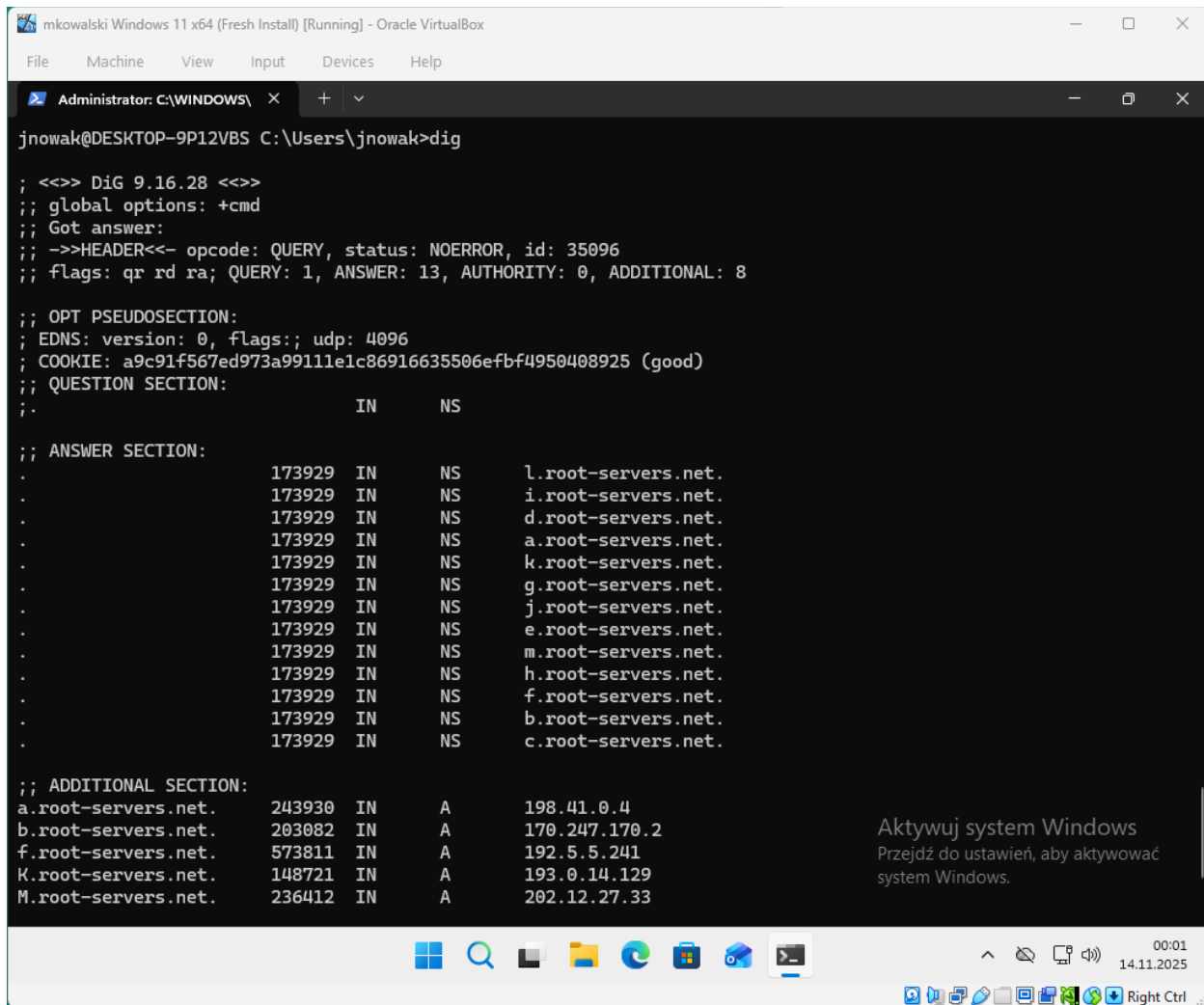
chocolatey-windowsupdate.extension v1.0.5 [Approved]
chocolatey-windowsupdate.extension package files install completed. Performing other installation steps.
Installed/updated chocolatey-windowsupdate extensions.
The install of chocolatey-windowsupdate.extension was successful.
Deployed to 'C:\ProgramData\chocolatey\extensions\chocolatey-windowsupdate'
Downloading package from source 'https://community.chocolatey.org/api/v2/'
Progress: Downloading KB2919442 1.0.20160915... 100%

KB2919442 v1.0.20160915 [Approved]
KB2919442 package files install completed. Performing other installation steps.
The package KB2919442 wants to run 'ChocolateyInstall.ps1'.
Note: If you don't run this script, the installation will fail.
Note: To confirm automatically next time, use '-y' or consider:
choco feature enable -n allowGlobalConfirmation
Do you want to run the script?([Y]es/[A]ll scripts/[N]o/[P]rint): A
```

Aktywuj system Windows
Przejdź do ustawień, aby aktywować system Windows.

Zrzut ekranu 23 Instalacja pakietu narzędzi bind-toolsonly. Potwierdzenie chęci uruchomienia skryptów instalacyjnych.

Od razu po instalacji możemy sprawdzić działanie jednego z zainstalowanych przed momentem programów.



```
Administrator: C:\WINDOWS\ X
jnowak@DESKTOP-9P12VBS C:\Users\jnowak>dig

; <<>> DiG 9.16.28 <<>>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35096
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 8

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: a9c91f567ed973a99111e1c86916635506efbf4950408925 (good)
;; QUESTION SECTION:
i-
                                IN      NS

;; ANSWER SECTION:
i-
173929 IN      NS      l.root-servers.net.
.
173929 IN      NS      i.root-servers.net.
.
173929 IN      NS      d.root-servers.net.
.
173929 IN      NS      a.root-servers.net.
.
173929 IN      NS      k.root-servers.net.
.
173929 IN      NS      g.root-servers.net.
.
173929 IN      NS      j.root-servers.net.
.
173929 IN      NS      e.root-servers.net.
.
173929 IN      NS      m.root-servers.net.
.
173929 IN      NS      h.root-servers.net.
.
173929 IN      NS      f.root-servers.net.
.
173929 IN      NS      b.root-servers.net.
.
173929 IN      NS      c.root-servers.net.

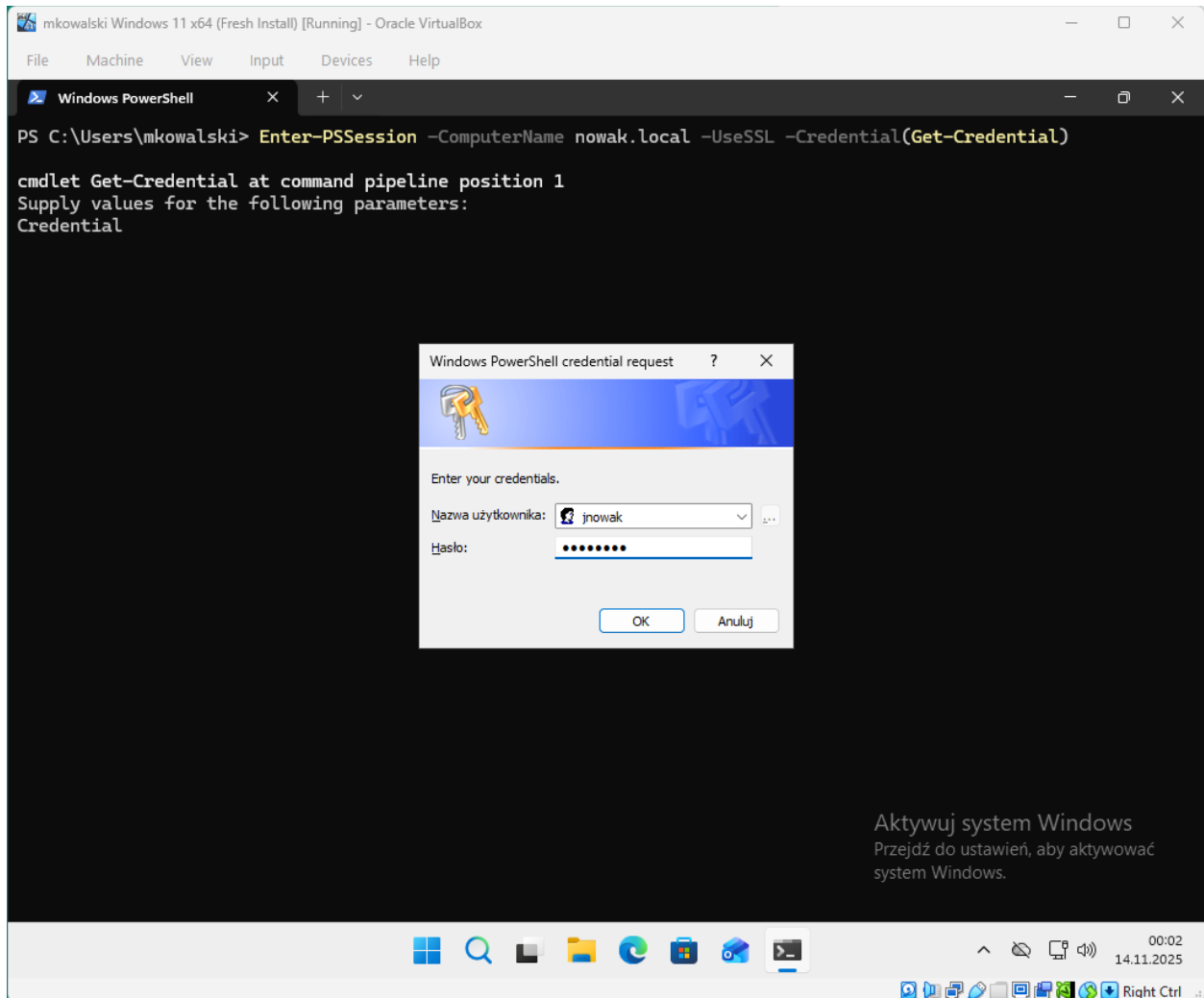
;; ADDITIONAL SECTION:
a.root-servers.net. 243930 IN      A       198.41.0.4
b.root-servers.net. 203082 IN      A       170.247.170.2
f.root-servers.net. 573811 IN      A       192.5.5.241
k.root-servers.net. 148721 IN      A       193.0.14.129
m.root-servers.net. 236412 IN      A       202.12.27.33

Aktywuj system Windows
Przejdź do ustawień, aby aktywować
system Windows.
```

Zrzut ekranu 24 Sprawdzenie poprawności instalacji jednego z programów wchodzących w pakiet bind-toolonly.

Zadanie 3. Zdalna konfiguracja komputera.

Przed przystąpieniem do zadania, połączyłem się zdalnie do drugiego komputera przy użyciu mechanizmu *WindowsRM*.

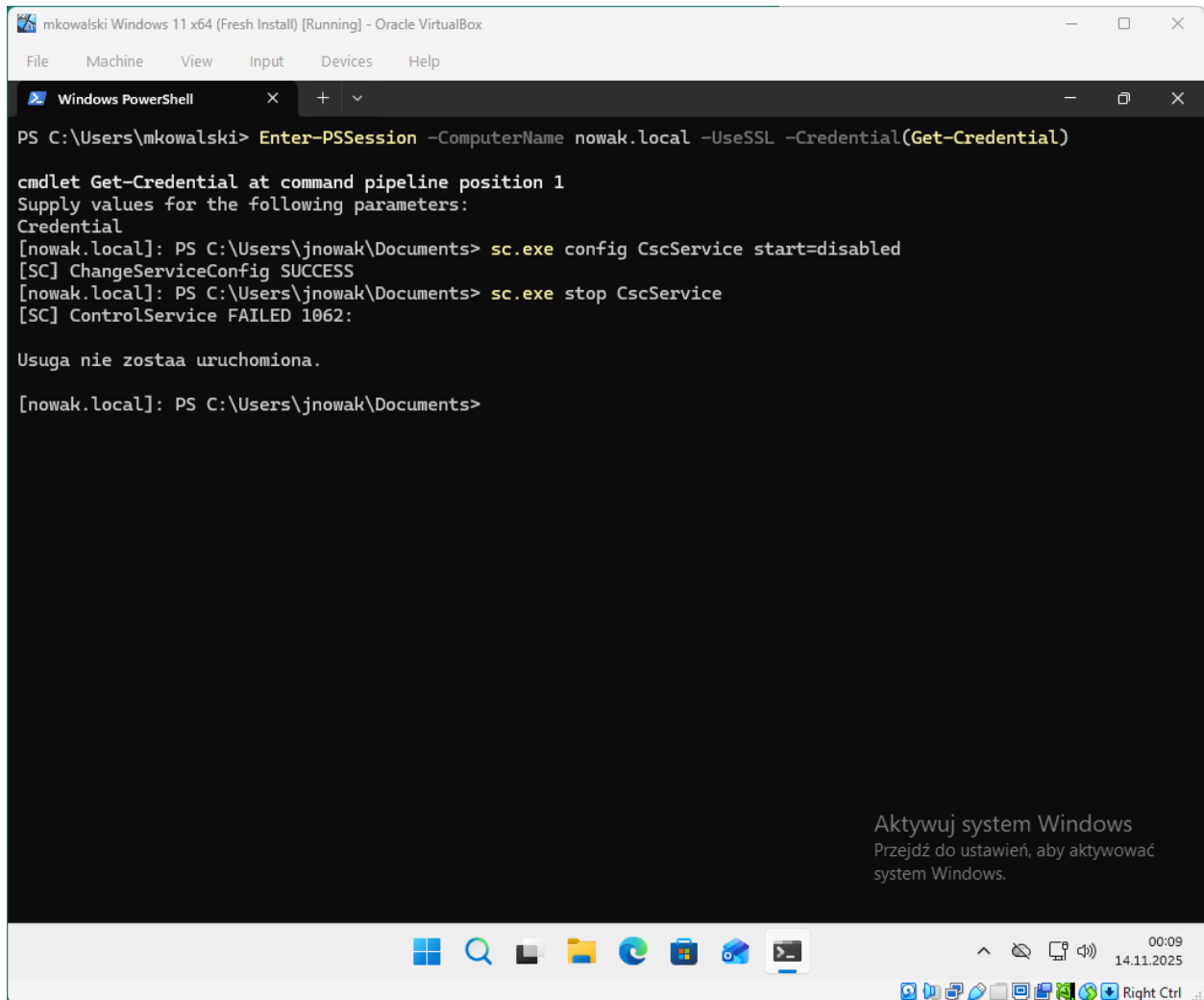


Zrzut ekranu 25 Zdalne połączenie się z komputerem z wykorzystaniem mechanizmu *WindowsRM*.

a. Zarządzanie usługami.

Do zarządzania usługami służą dwa polecenia – net oraz sc. Pierwsze z nich jest starsze i nie pozwala zmieniać typu startu serwisu. Stąd, aby wyłączyć na stałe usługę wykorzystam komendę sc.

```
sc.exe config <nazwa_serwisu> start=disabled  
sc.exe stop <nazwa_serwisu>
```



```
PS C:\Users\mkowalski> Enter-PSSession -ComputerName nowak.local -UseSSL -Credential(Get-Credential)  
  
cmdlet Get-Credential at command pipeline position 1  
Supply values for the following parameters:  
Credential  
[nowak.local]: PS C:\Users\jnowak\Documents> sc.exe config CscService start=disabled  
[SC] ChangeServiceConfig SUCCESS  
[nowak.local]: PS C:\Users\jnowak\Documents> sc.exe stop CscService  
[SC] ControlService FAILED 1062:  
  
Usuga nie zostaa uruchomiona.  
  
[nowak.local]: PS C:\Users\jnowak\Documents>
```

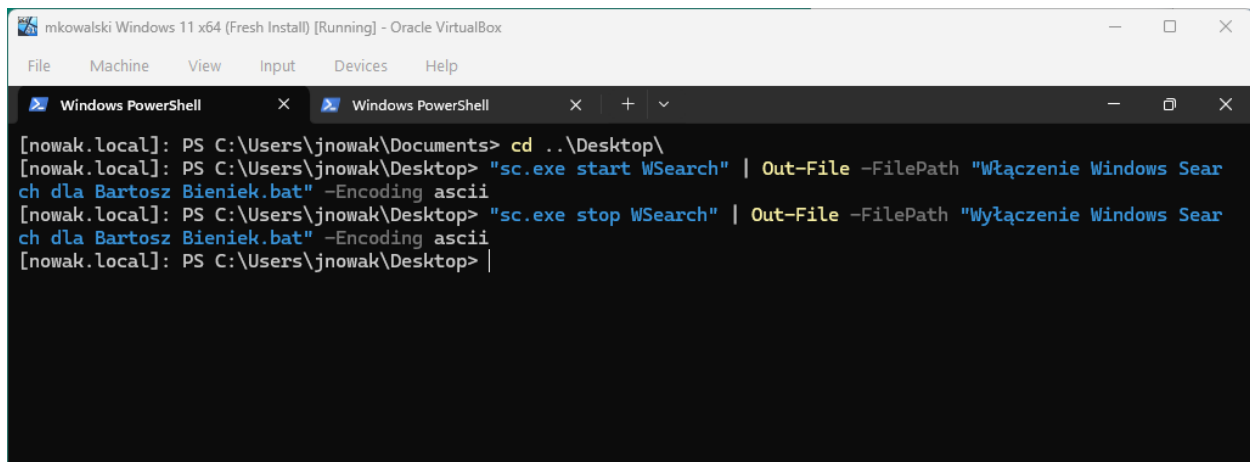
Zrzut ekranu 26 Efekt wywołania polecenia wyłączającego uruchamianie się usługi wraz ze startem systemu oraz jej zatrzymanie.

Komenda zatrzymująca serwis zwróciła błąd, ponieważ CscService było już zatrzymane.

b. Skrypty Batch, tworzenie i zapis do plików.

Wykonywanie pewnych czynności można zautomatyzować tworząc skrypty w języku Batch. Są to pliki zawierające całe sekwencje komend (albo choćby jedno polecenie), które można później łatwo wywołać.

Przykładowo, możemy stworzyć skrypty uruchamiające i zatrzymujące usługę *Windows Search*. Do utworzenia plików wykorzystam polecenie `Out-File -FilePath „ścieżka” -Encoding ascii`, które zapisuje pod wskazaną lokalizacją dane ze strumienia. Ważne jest, aby ustawić kodowanie na `ascii`, gdyż inaczej tak utworzone skrypty nie będą chciały się wykonywać.

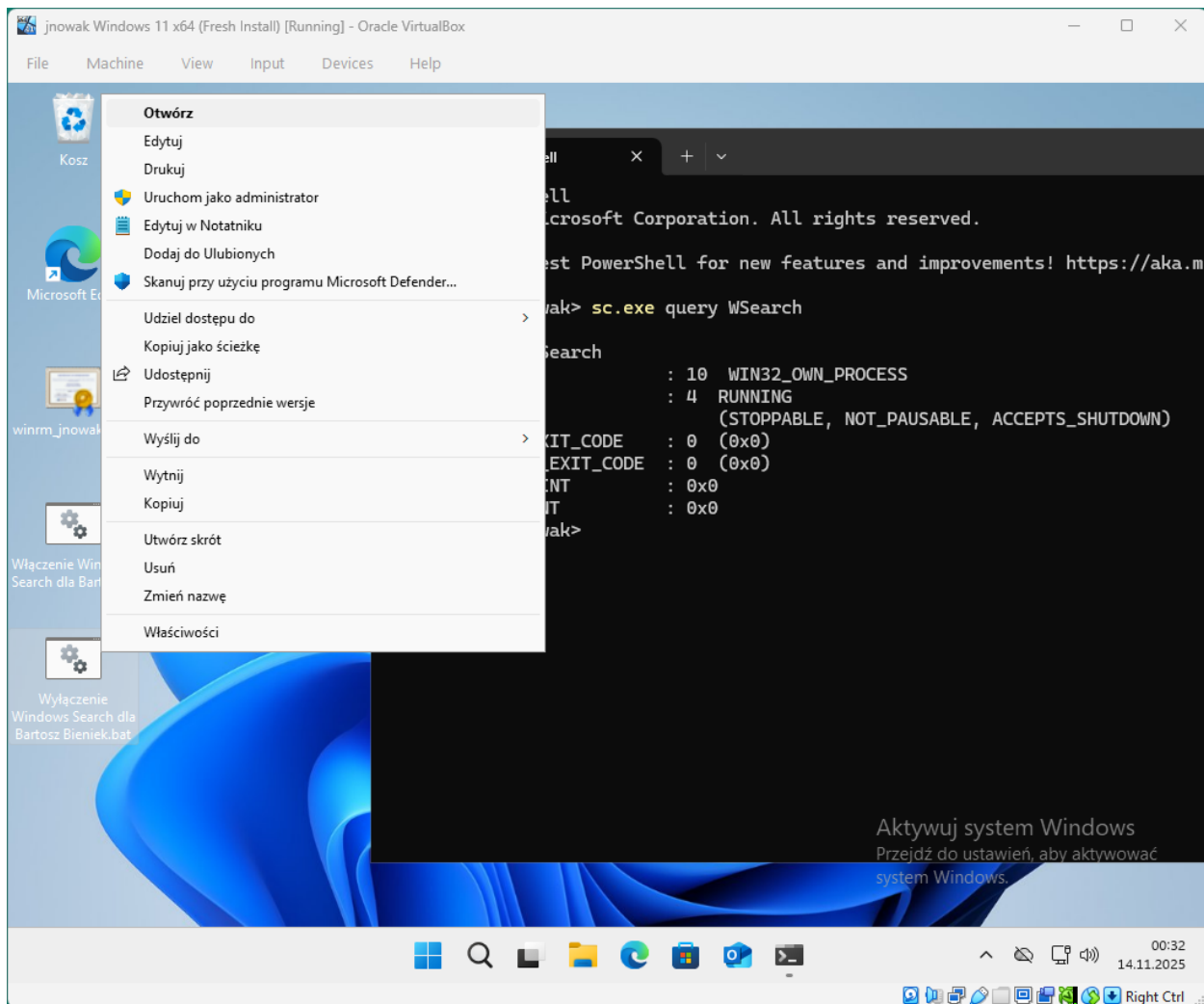


```
[nowak.local]: PS C:\Users\jnowak\Documents> cd ..\Desktop\  
[nowak.local]: PS C:\Users\jnowak\Desktop> "sc.exe start WSearch" | Out-File -FilePath "Włączenie Windows Search dla Bartosz Bieniek.bat" -Encoding ascii  
[nowak.local]: PS C:\Users\jnowak\Desktop> "sc.exe stop WSearch" | Out-File -FilePath "Wyłączenie Windows Search dla Bartosz Bieniek.bat" -Encoding ascii  
[nowak.local]: PS C:\Users\jnowak\Desktop> |
```

Zrzut ekranu 27 Tworzenie prostych skryptów Batch.

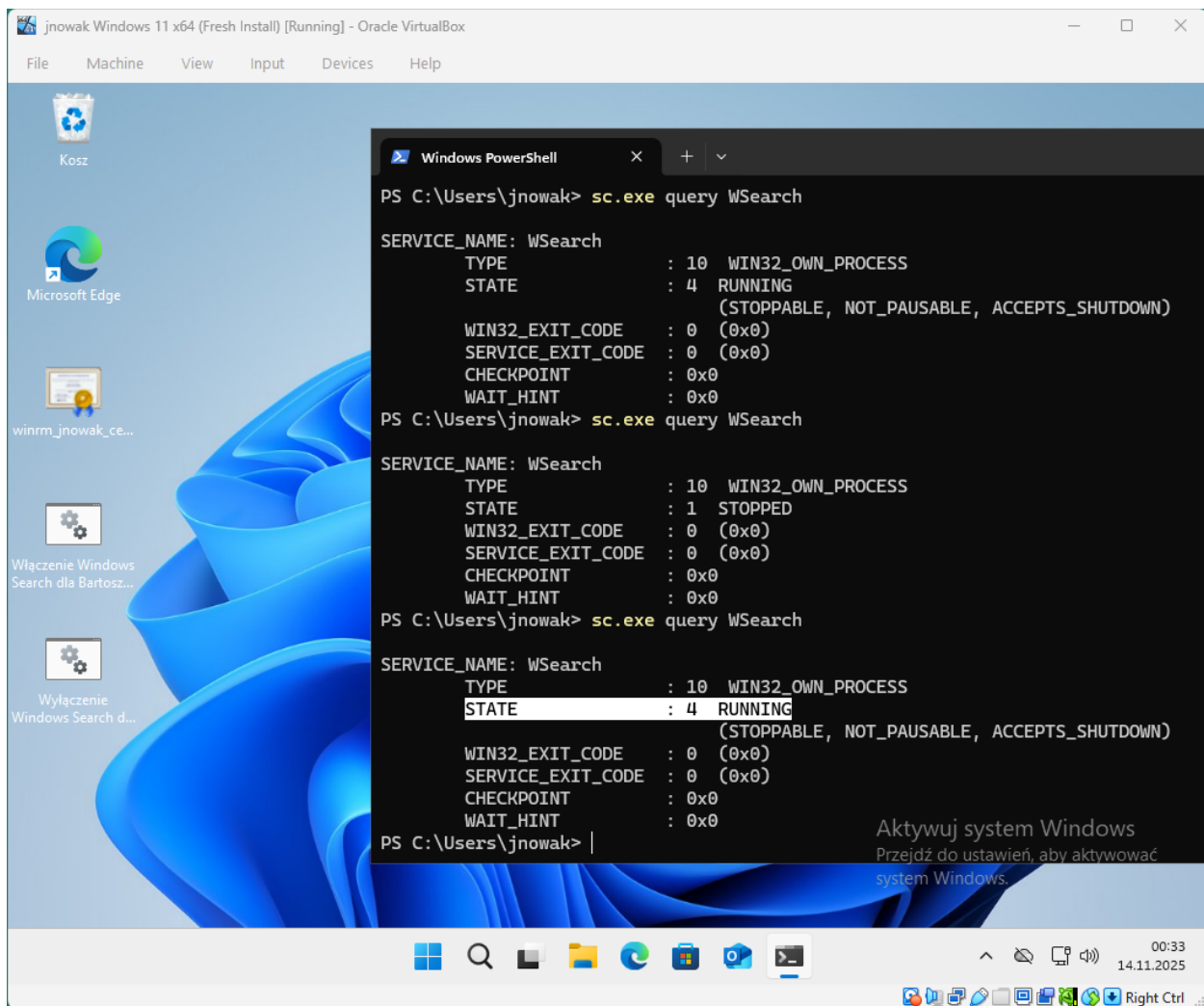
Do bardziej skomplikowanych edycji można by było wykorzystać polecenie (edytor) *edit*.

Tak utworzone skrypty można teraz przetestować. Ponieważ będziemy zatrzymywać i startować usługi, warto najpierw sprawdzić jaki jest ich obecny stan. Służy do tego polecenie `sc.exe query <nazwa_usługi>`.



Zrzut ekranu 28 Sprawdzenie stanu działania usługi Windows Search.

Jak widać, usługa Windows Search jest na startcie uruchomiona (RUNNING). Najpierw uruchomię skrypt zatrzymujący serwis (jako administrator), a następnie uruchomię ją ponownie drugim skryptem, w międzyczasie sprawdzając stan działania usługi. Efekt wykonania poleceń został przedstawiony na poniższym zrzucie ekranu.

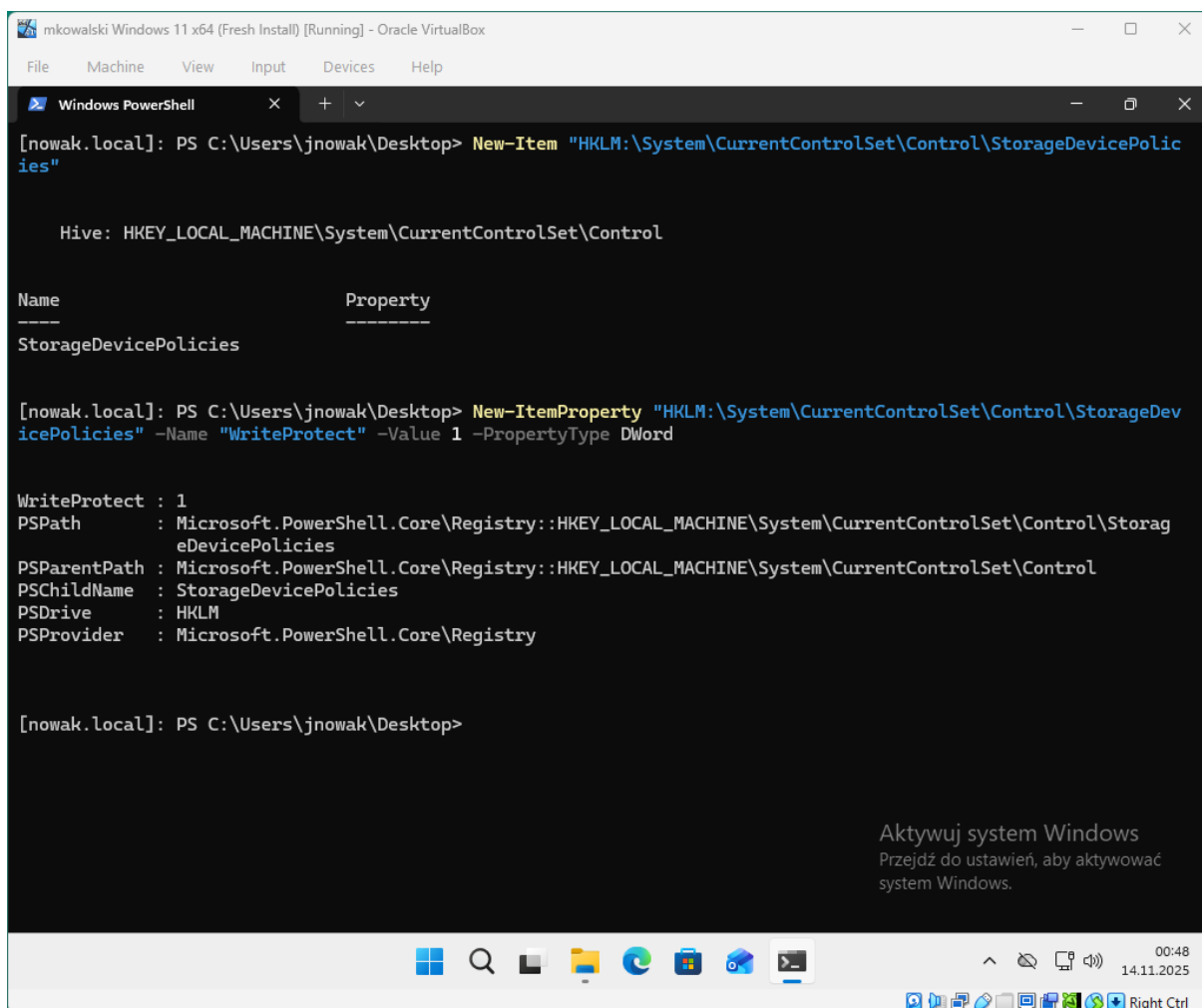


Zrzut ekranu 29 Zmieniający się stan usługi Windows Search po wykonaniu pierwszego i drugiego skryptu.

c. Edycja rejestru.

Rejestr systemu można edytować z poziomu powłoki PowerShell poleceniami New-Item, Get-Item, Set-Item, Remove-Item, New-ItemProperty, Get-ItemProperty, Set-ItemProperty, Remove-ItemProperty. Pierwsza grupa poleceń, to jest *-Item, umożliwia zarządzanie kluczami rejestru, a druga grupa, *-ItemProperty, pozwala zarządzać wartościami pod danym kluczem.

Przykładowo, aby włączyć blokadę zapisu na dyskach USB należy w kluczu "HKLM:\System\CurrentControlSet\Control\StorageDevicePolicies" dodać wartość "WriteProtect" ustawioną na 1 (DWord). Ponieważ taki klucz nie istnieje, trzeba go najpierw utworzyć poleceniem New-Item "<ścieżka_do_klucza>", a następnie ustawić (dodać) wskazaną wartość komendą New-ItemProperty "<ścieżka_do_klucza>" -Name "<nazwa_wartości>" -Value <wartość> -PropertyType <typ>.



```
mkowalski Windows 11 x64 (Fresh Install) [Running] - Oracle VirtualBox
File Machine View Input Devices Help

Windows PowerShell
[nowak.local]: PS C:\Users\jnowak\Desktop> New-Item "HKLM:\System\CurrentControlSet\Control\StorageDevicePolicies"

Hive: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control

Name                Property
----                -
StorageDevicePolicies

[nowak.local]: PS C:\Users\jnowak\Desktop> New-ItemProperty "HKLM:\System\CurrentControlSet\Control\StorageDevicePolicies" -Name "WriteProtect" -Value 1 -PropertyType DWord

WriteProtect : 1
PSPath       : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\StorageDevicePolicies
PSParentPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control
PSChildName  : StorageDevicePolicies
PSDrive      : HKLM
PSProvider   : Microsoft.PowerShell.Core\Registry

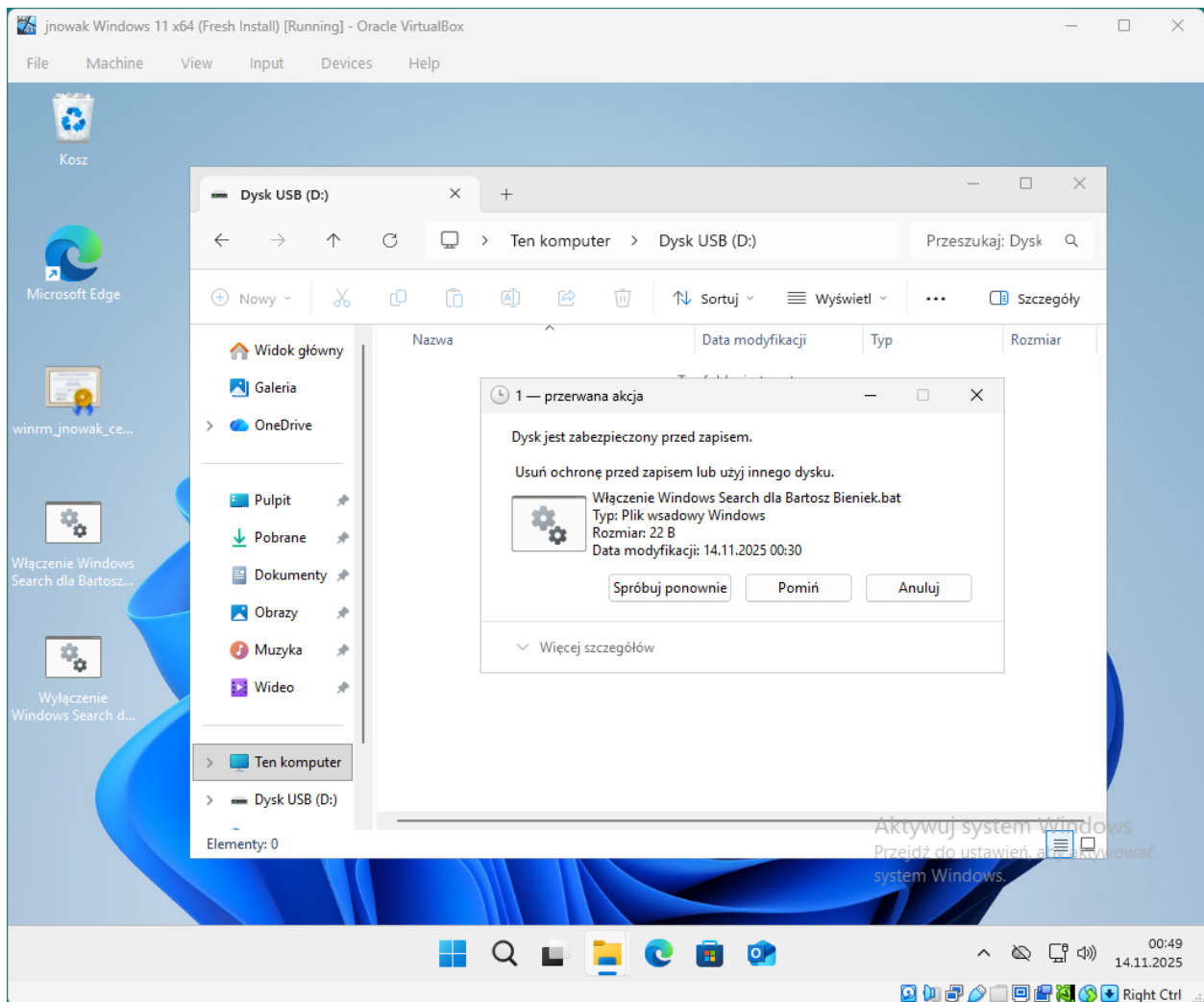
[nowak.local]: PS C:\Users\jnowak\Desktop>

Aktywuj system Windows
Przejdź do ustawień, aby aktywować system Windows.

00:48
14.11.2025
```

Zrzut ekranu 30 Edycja rejestru z poziomu wiersza poleceń.

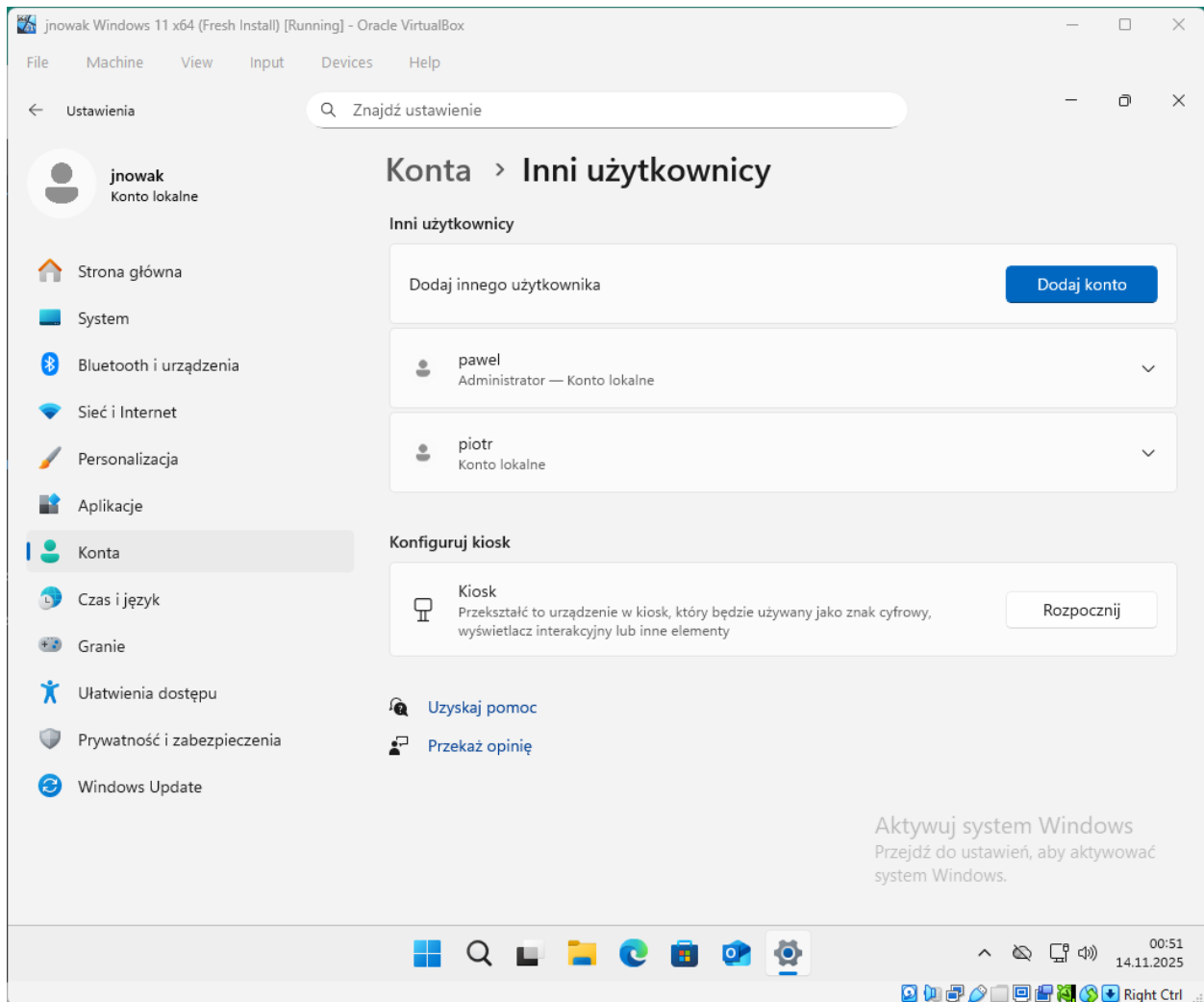
Od teraz, przy próbie zapisu danych na nośnikach wymiennych, wyświetlać będzie się błąd.



Zrzut ekranu 31 Blokada zapisu danych na nośniku wymiennym.

Zadanie 4. Zapobieganie usuwaniu drukarek. Zasady grupy i narzędzie MMC.

Celem realizacji zadania jest wyłączenie możliwości usuwania drukarek przez użytkowników nieposiadających uprawnień administratora. Aby przetestować później działanie wdrożonego mechanizmu, utworzę dwa dodatkowe konta – pawel (administrator) i piotr (użytkownik).

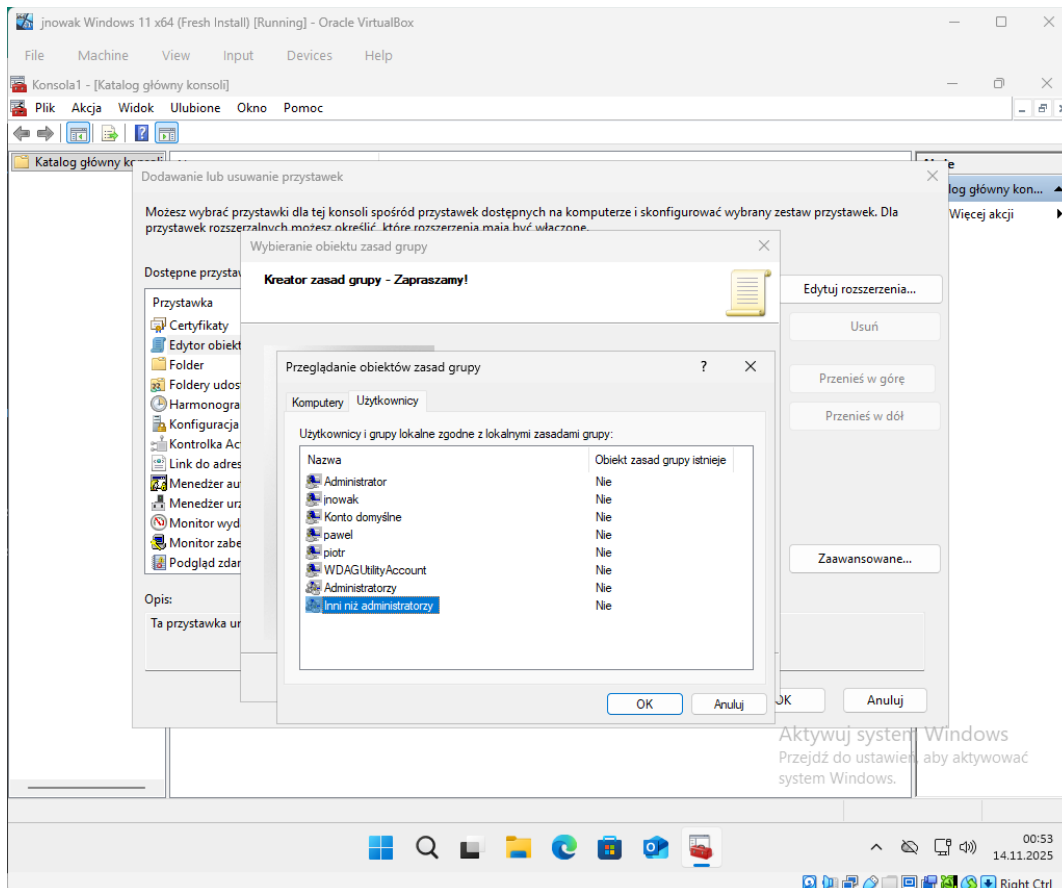


Zrzut ekranu 32 Utworzenie użytkowników testowych.

Wprowadzenie zmian korzystając bezpośrednio z narzędzia zasad grup, spowodowałoby, że zmiany zauważyłby tylko aktualnie zalogowany użytkownik (administrator). Zamiast tego, skorzystamy z narzędzia Microsoft Management Console, które umożliwia wskazanie konkretnych użytkowników i grup.

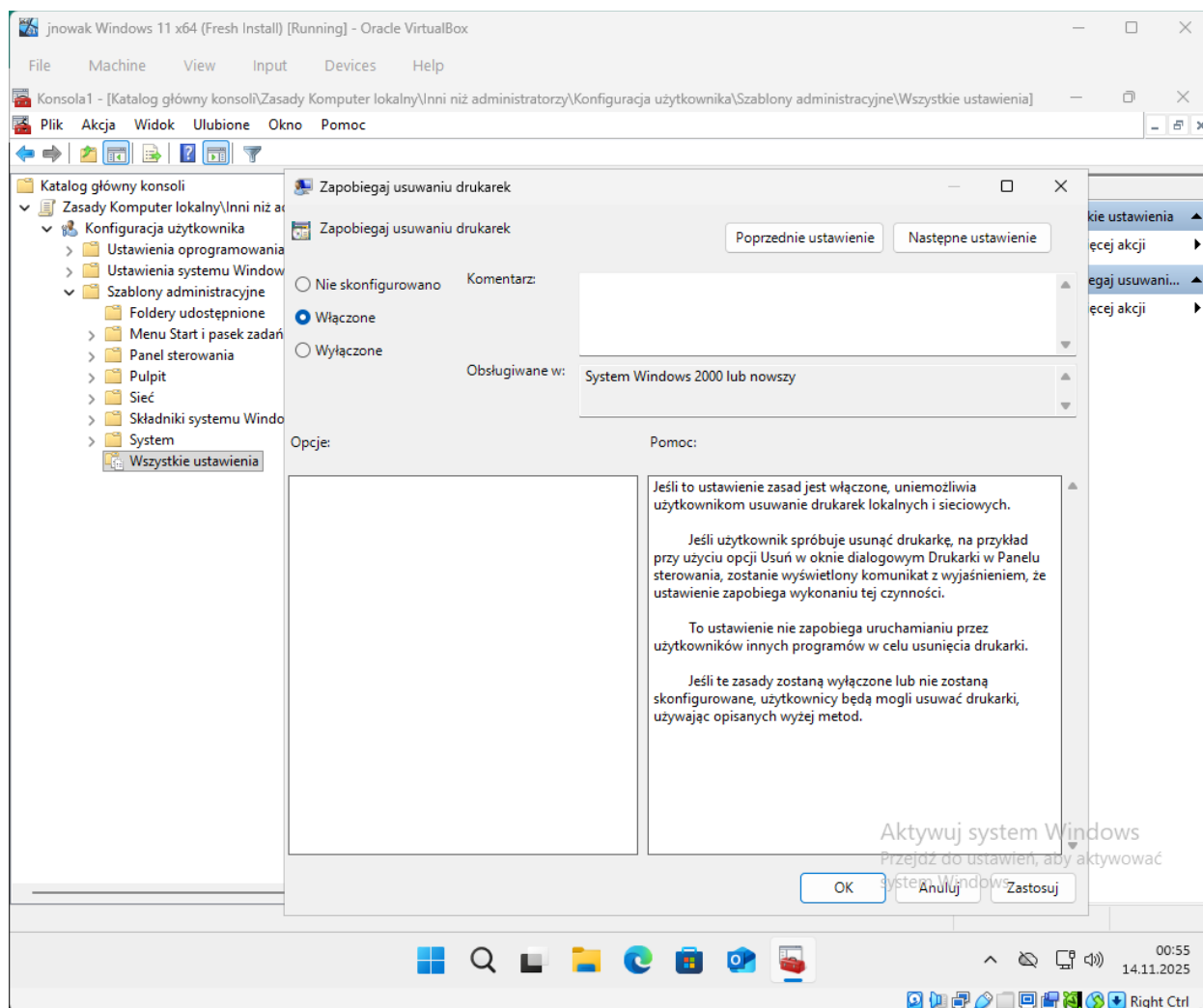
Aby skonfigurować zasady grupy dla wybranych obiektów, z górnego menu wybieramy opcję „Plik” → „Dodaj lub usuń przystawkę...” i przerzucamy „Edytor obiektu zasad grupy”.

W otwierającym się okienku klikamy przycisk „Przeglądaj...” i w zakładce „Użytkownicy” wskazujemy grupę „Inni niż administratorzy”.



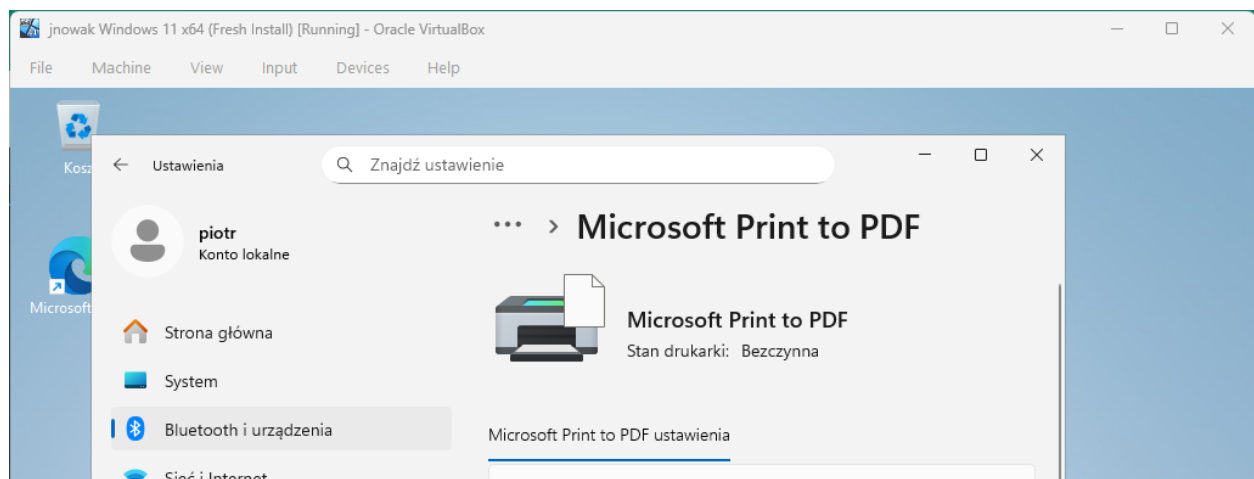
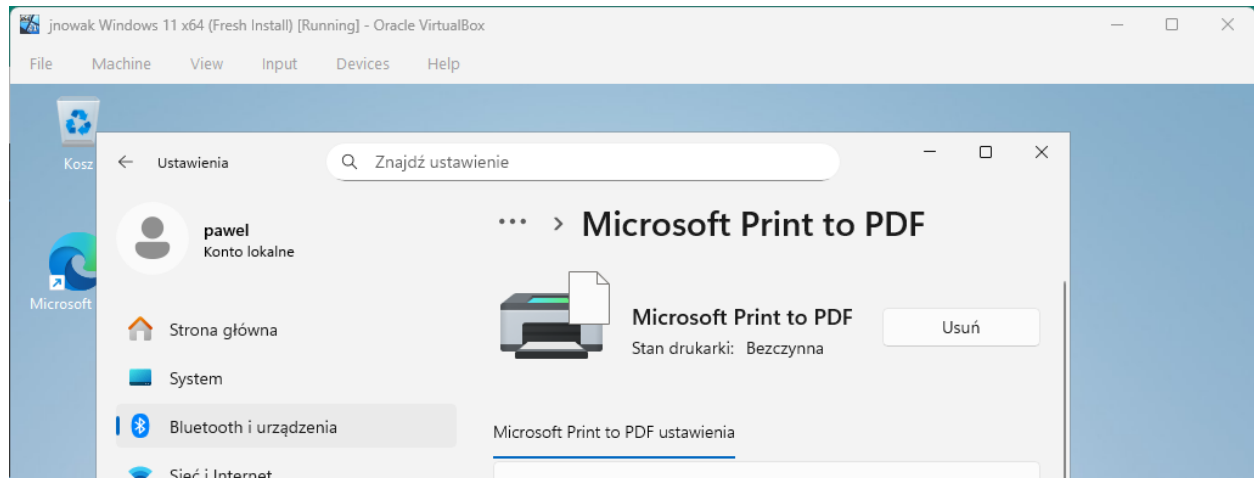
Zrzut ekranu 33 Narzędzie Microsoft Management Console. Konfigurowanie obiektu zasad grupy.

Zmiany zapisujemy, odszukujemy w lewym panelu ustawienia blokującego usuwanie drukarek i włączamy je. Od teraz nie-administratorzy nie będą mogli usunąć z systemu tych urządzeń.



Zrzut ekranu 34 Włączenie zasady blokującej możliwość usuwania drukarek z systemu.

Sprawdźmy poprawność wprowadzonych zmian. Utworzone na początku zadania konto administracyjne “pawel” dalej ma możliwość usuwania drukarek, ale użytkownikowi “piotr” taka opcja zniknęła.



Zrzut ekranu 35 Sprawdzenie poprawności blokady usuwania drukarek dla kont bez uprawnień administratora.