

Windows Pwning

Blackhoodie Workshop - Luxembourg '19

Scenario	2
Requirements	2
Lab Setup	2
I've got no time - quick version	3
Let me do it myself - longer version	5
Getting the ISOs	5
Getting the tools	5
Virtualization setup	5
CL01 - Installing the Windows 10 Client	6
CL01 - Install VirtualBox Guest Additions	10
CL01 - Post Installation configuration	11
CL01 - Check IP setup the GUI way (optional)	12
DC01 - Installing the Domain Controller	12
DC01 - Install VirtualBox Guest Additions	13
DC01 - Post installation configuration	14
DC01 - Installing Active Directory Domain and Services (AD DS)	15
CL01 - joining CL01 to the Domain - The Powershell way	16
CL01 - joining CL01 to the Domain - The GUI way	17
Final Setup Checks	18

Scenario

Congrats, you've made it, after some exploit shenanigans you've got your first foothold on a Windows client at **Kitty Corporation**. Now what? Where to go from here? Where am I? Who am I? Who can I (pretend to) be? And what can I do? We'll explore some tools and techniques that help us try to answer those questions.

This is going to be a starter workshop to get a first feeling on how to have fun with (domain joined) Windows systems. We'll be focusing on the basic concepts of a Windows based infrastructure that you'll usually find in corporate environments. This will include authentication protocols and weaknesses as well as tools that let's you have fun in those infrastructures.

Requirements

Ability to run 2 Windows based VMs at the same time (≥ 8 GB RAM, ≥ 60 GB free disk). That's it, detailed knowledge of Windows is not required to attend the training, we'll start with the basics and explore this playground together.

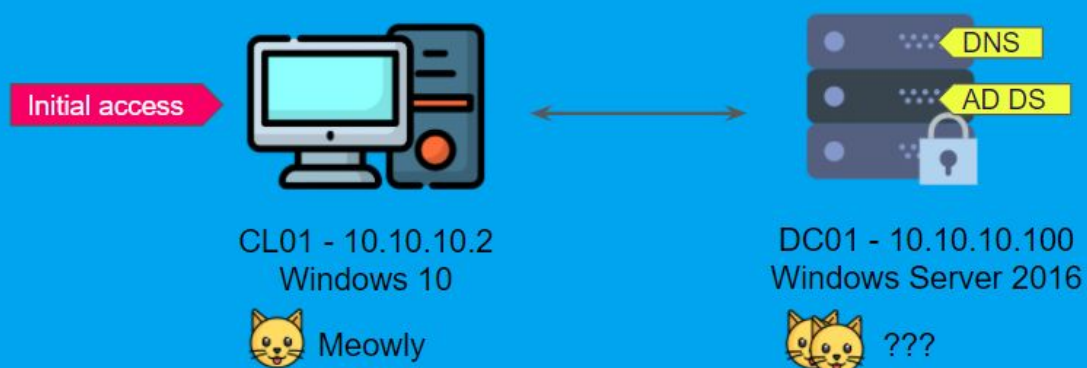
Lab Setup

For our workshop lab we will setup a small environment because we don't have that much resources on our small laptops. It should be enough to simulate some basic scenarios though.

In a production environment you would usually find multiple domain controllers and most likely even multiple domains and forests (we'll touch on what those are during the workshop).

For our lab we'll setup:

- one domain controller running on a Windows 2016 server
- one (domain joined) client running Windows 10 1903



For the lab setup you can choose between two ways, a quick version where you download my VMs, just setup the network configuration and import the VMs. This shouldn't take too long.

The other option is to follow my documentation and setup the lab yourself. If you've got the time to do this, I would highly recommend going this way. Take it as a warm-up for the workshop. Personally it really helped me understand what's behind the scene when building it up myself. And after the workshop you're able to setup your own (small) AD lab, might come in handy in the future, who knows (:

I created some small scripts whenever possible so that you shouldn't need too much mouse clicking.

I've got no time - quick version

Okay no worries if you don't have enough time to setup the lab yourself you can download both VMs over here and just import them:

DC01 - Windows Server 2016: [<URL TBD>](#)

CL01 - Windows 10: [<URL TBD>](#)

Please make sure that you setup the network so that both VMs can talk to each other. The VMs are configured with the following static IP addresses:

DC01

IP: 10.10.10.100

Subnet: 255.255.255.0

Gateway: 10.10.10.1

DNS: 10.10.10.100, 127.0.0.1

CL01

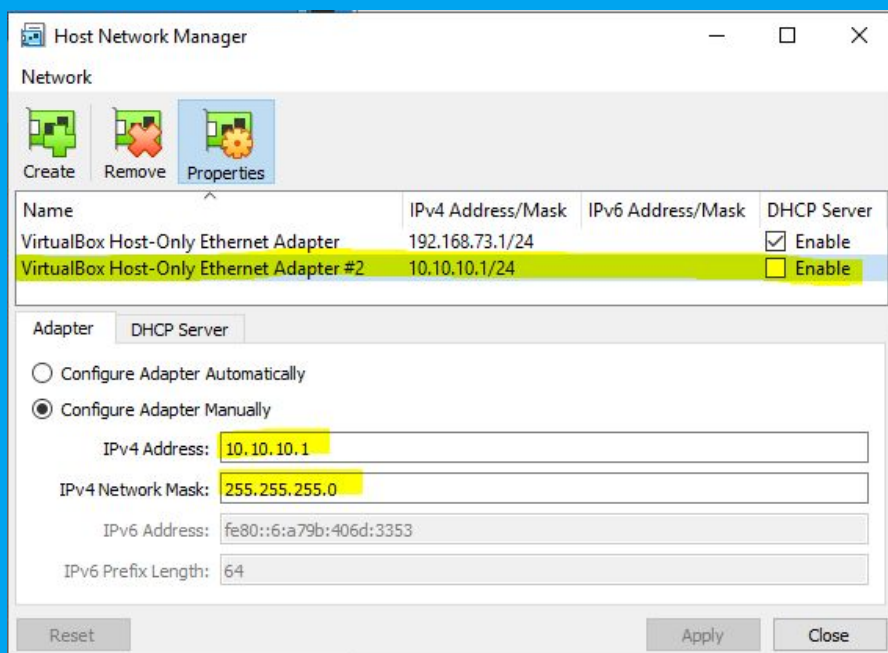
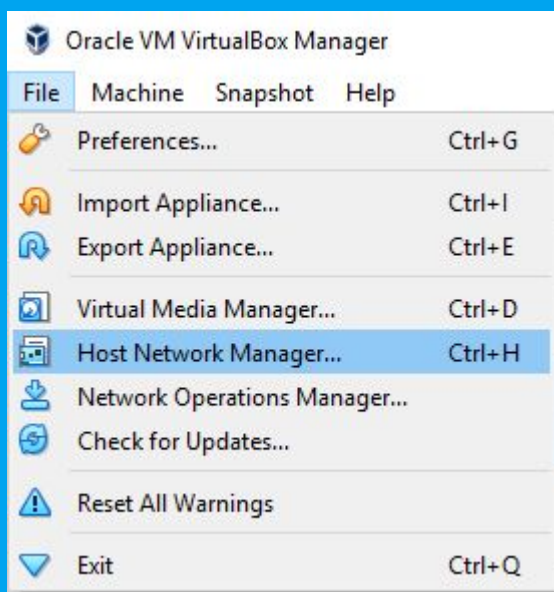
IP: 10.10.10.2

Subnet: 255.255.255.0

Gateway: 10.10.10.1

DNS: 10.10.10.100

In Virtual Box you can go ahead and open the 'Host Network Manager' and create a new 'Host-only network' with the following settings:



Start up DC01, give it some time to boot, login with:

KITTYCORP\Administrator:Blackhoodie2019

After this, start up CL01 and try logging into CL01 with the following credentials (DC01 must be up and running):

KITTYCORP\Luke:Blackhoodie2019

If this works, you're ready for the workshop (:

You can either shutdown both VMs or suspend them.

Let me do it myself - longer version

Awesome, I appreciate you motivation (;

The time it will take to setup everything is about 1 1/2 hours, but no need to do it all at once. In this documentation we'll use Oracle VirtualBox 6.0 as our virtualization platform. Feel free to take any other platform, just make sure that your network setup is done in the same way so that both machines can reach each other. They don't need internet connection. I'll provide an example for how to do this in VirtualBox.

Getting the ISOs

Download the ISOs here:

Windows Server 2016:

<https://www.microsoft.com/de-de/evalcenter/evaluate-windows-server-2016/>

Windows 10 1903:

<https://www.microsoft.com/de-de/evalcenter/evaluate-windows-10-enterprise>

(you don't need to provide valid information in the form fields)

Getting the tools

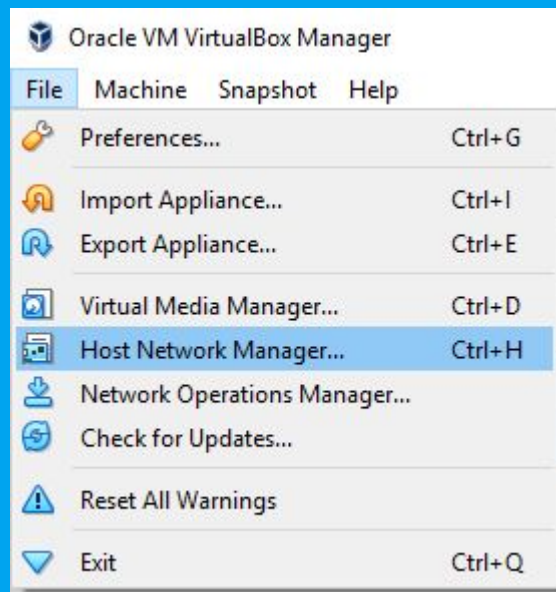
I've collected all (and probably a little bit more) of the tools that we're going to use during the workshop. You can download them here:

<LINK TBD>

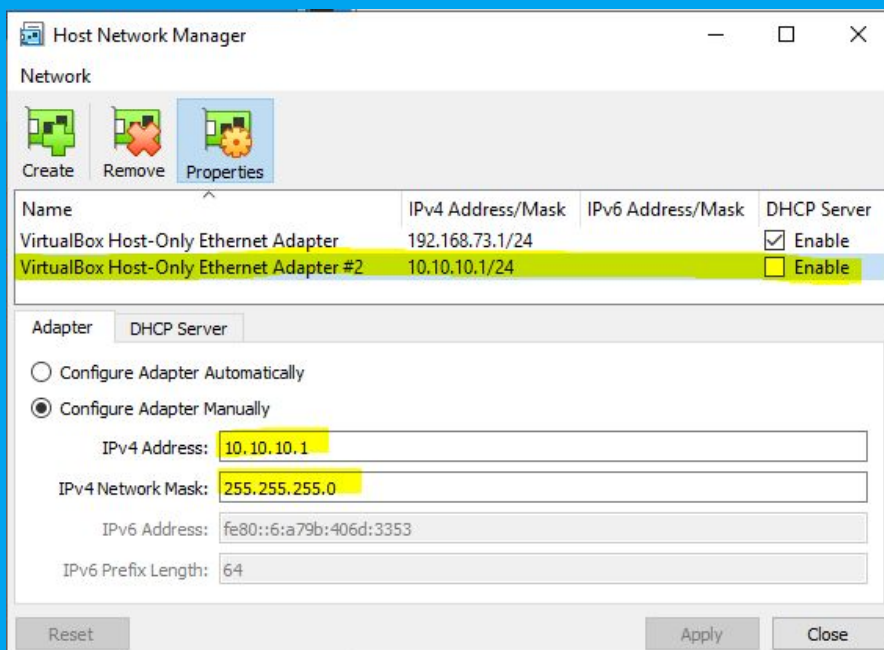
Since Windows Defender is detecting some of the tools, the ZIP is password protected. The password is "infected". For this installation, just extract the "the first layer", you'll just need the 'provisioning' folder.

Virtualization setup

First we create our network. Open Virtualbox, click on 'File' in the left menu, click on 'Host Network Manager' in the menu.

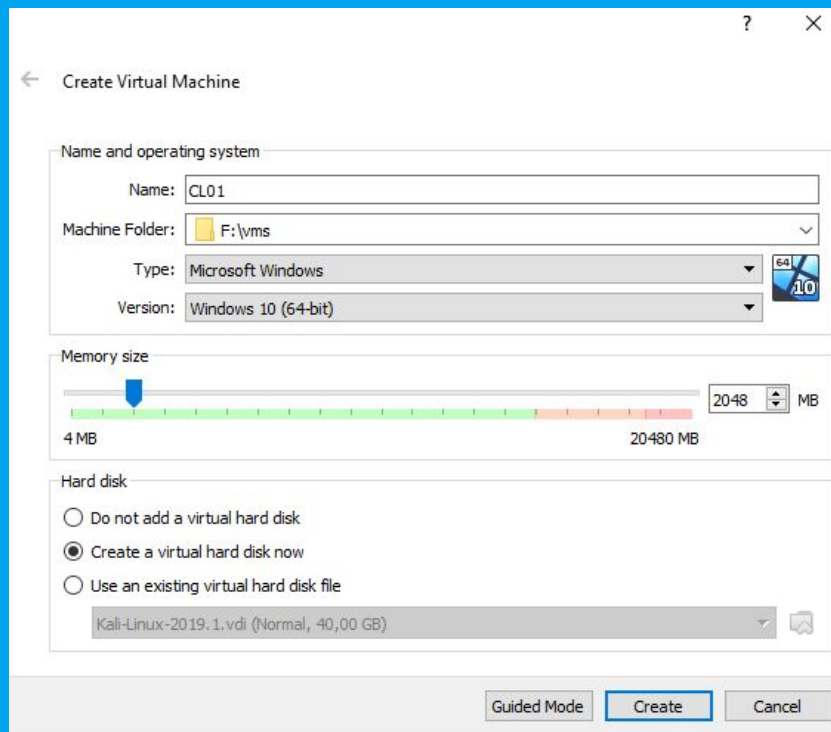


In the new window click 'Create' to create a new Host-Only network .
Give it the following settings:

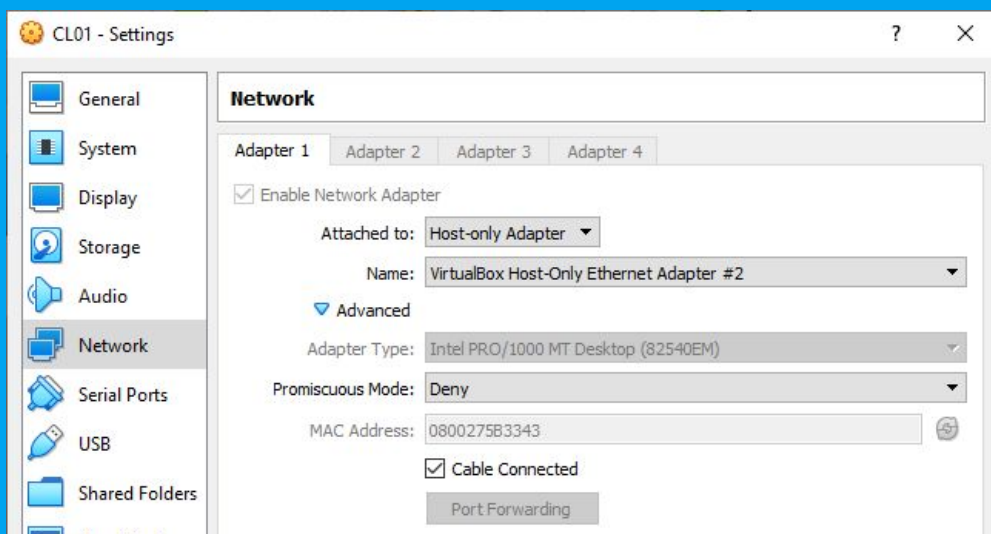


CL01 - Installing the Windows 10 Client

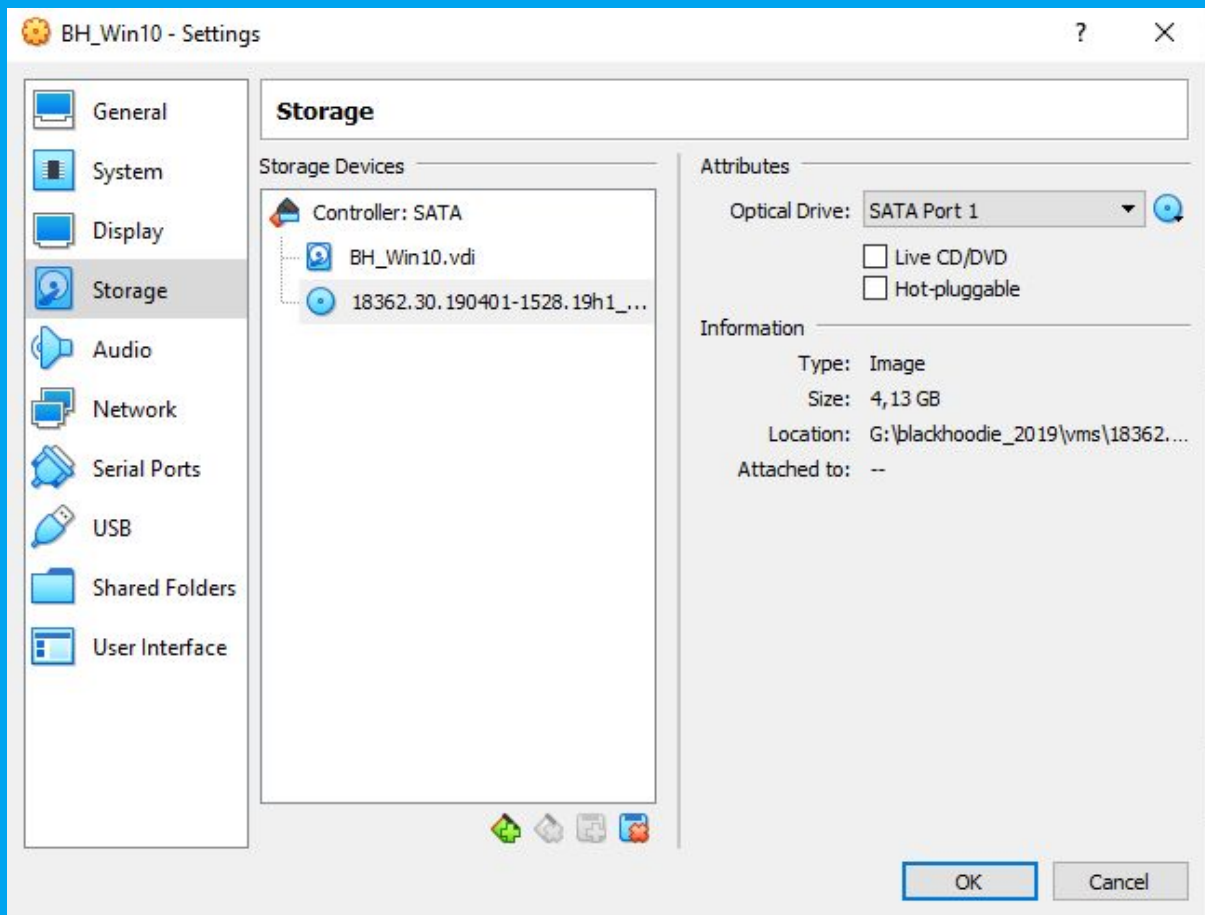
Create the Client VM, name it 'CL01' and give it at least 2GB of RAM and a disk capacity of at least 20GB.



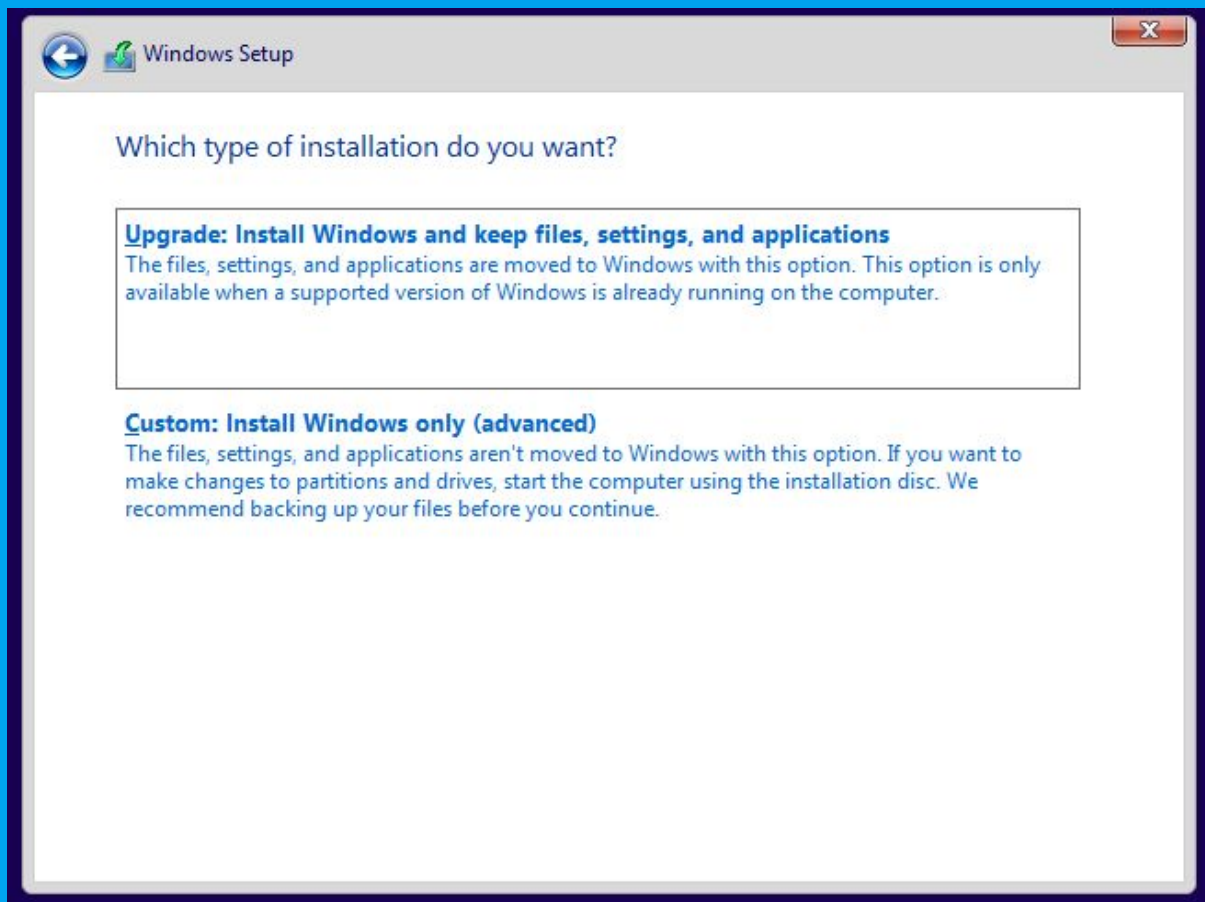
And the following network settings:



Under 'Storage' insert the ISO you downloaded for the Windows 10 Client into the Optical drive.



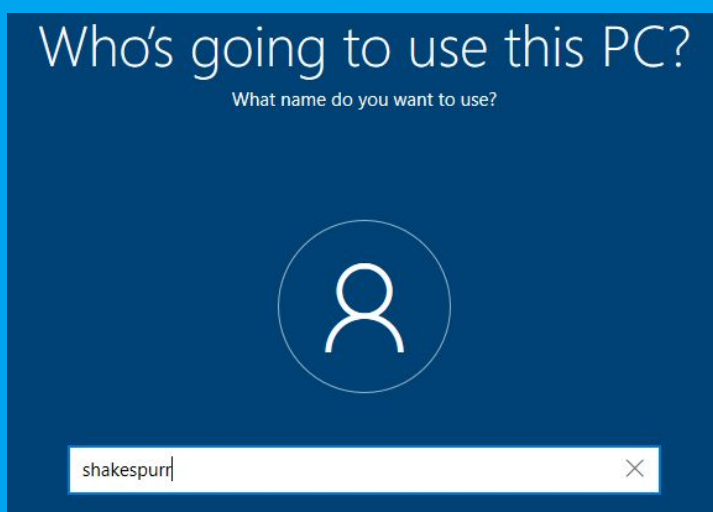
Start the virtual machine, installation of Windows 10 should start now.



Choose "Custom: Install Windows only (advanced)"

When you're asked for an internet connection click the link in the left corner that says 'I don't have internet'. In the next screen click 'Continue with limited setup', also in the left corner.

During installation, when prompted create a user named 'shakespurr' with the password of 'blackhoodie2019'. Also answer all three required security questions with 'blackhoodie2019'.



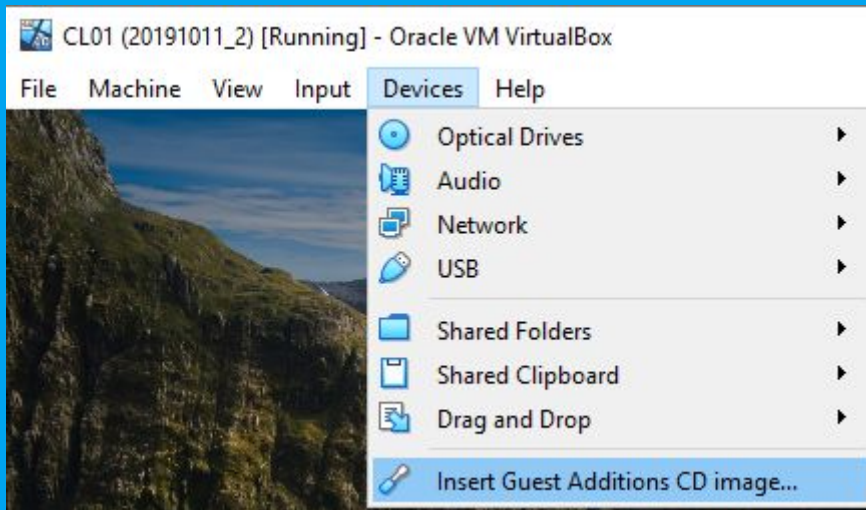
After this you'll be asked for a lot of different settings, answer them with 'No', 'Don't use online speech recognition', 'No', 'No', 'Basic', 'No', 'No'.

Now Windows is getting things ready for you (:

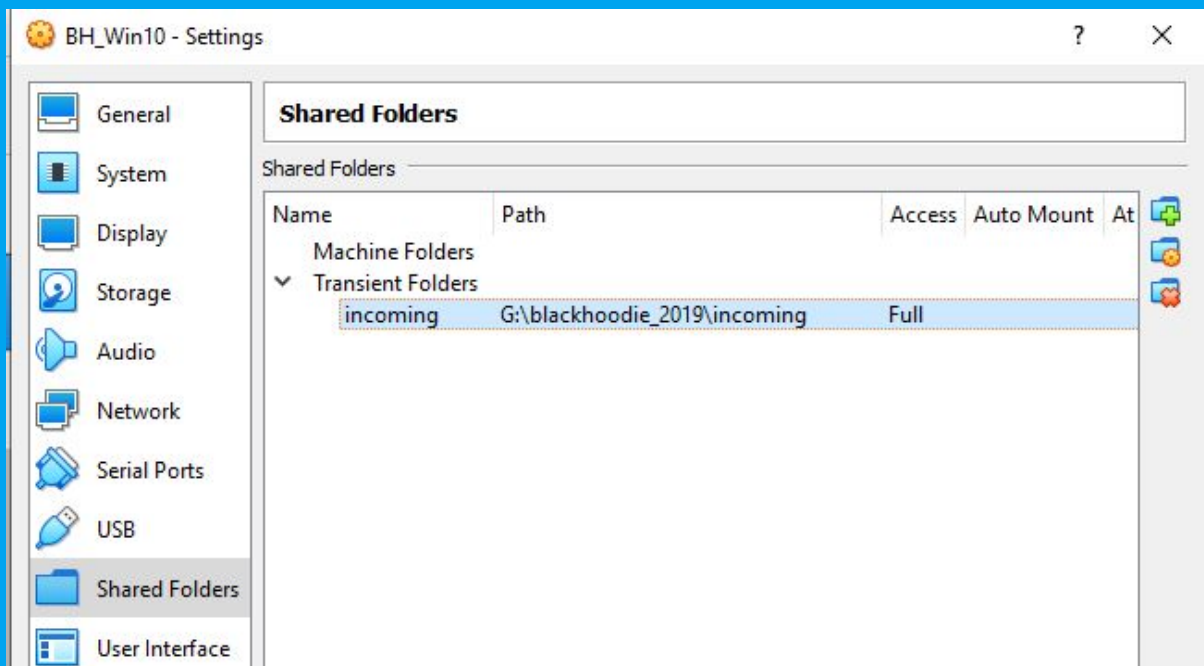
After this, login with the account you just created.

CL01 - Install VirtualBox Guest Additions

Insert the VirtualBox Guest Additions via the menu and install them.



After a successful install you should be able to create a shared folder between your host and CL01:



Copy the following ZIP into the shared folder on your host:

<LINK TO FOLDER TBD>

In your VM you can access the shared folder by opening up an explorer window and typing \\vboxsrv into the address bar.

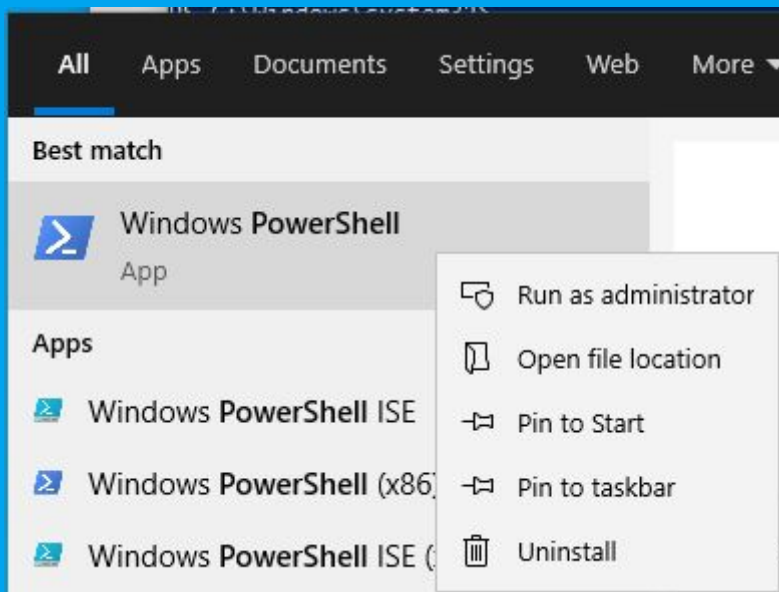
Copy the ZIP into C:\tools\.

(Hint: Just extract the first ZIP, not the one inside, since Windows Defender is still running it might delete some files it detects as 'harmful'. We'll do this in the workshop.)

CL01 - Post Installation configuration

After installation open an administrative Powershell. Type:

'powershell' into the field and right click on the available option and click 'run as administrator':



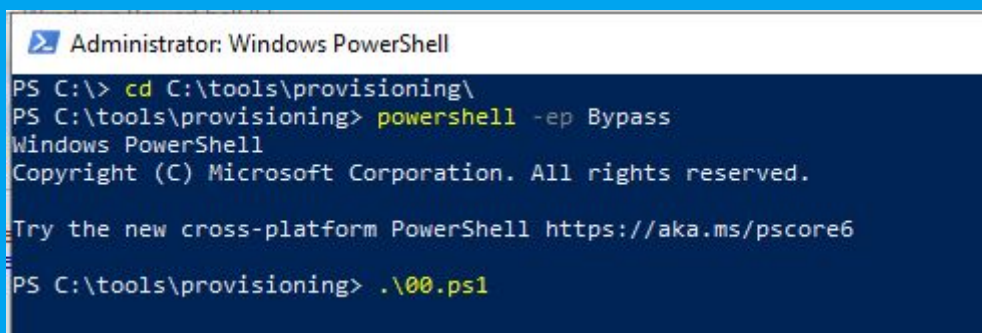
Navigate to the 'C:\tools\provisioning\CL01' folder you just extracted by typing:

```
> cd C:\tools\provisioning\CL01
```

```
> powershell -ep Bypass
```

Start the CL01-00.ps1 script by typing:

```
> .\CL01-00.ps1
```



This will change the hostname to 'CL01' and perform an instant reboot.

Log back into the client with 'shakespurr:blackhoodie2019', open a new administrative Powershell like above and continue with CL01-01.ps1.

This will add another local user 'meowly' with the password 'blackhoodie', set the static IP of CL01 to 10.10.10.2 and configure the DNS to be used to 10.10.10.100 (which will be our Domain Controller in a few minutes).

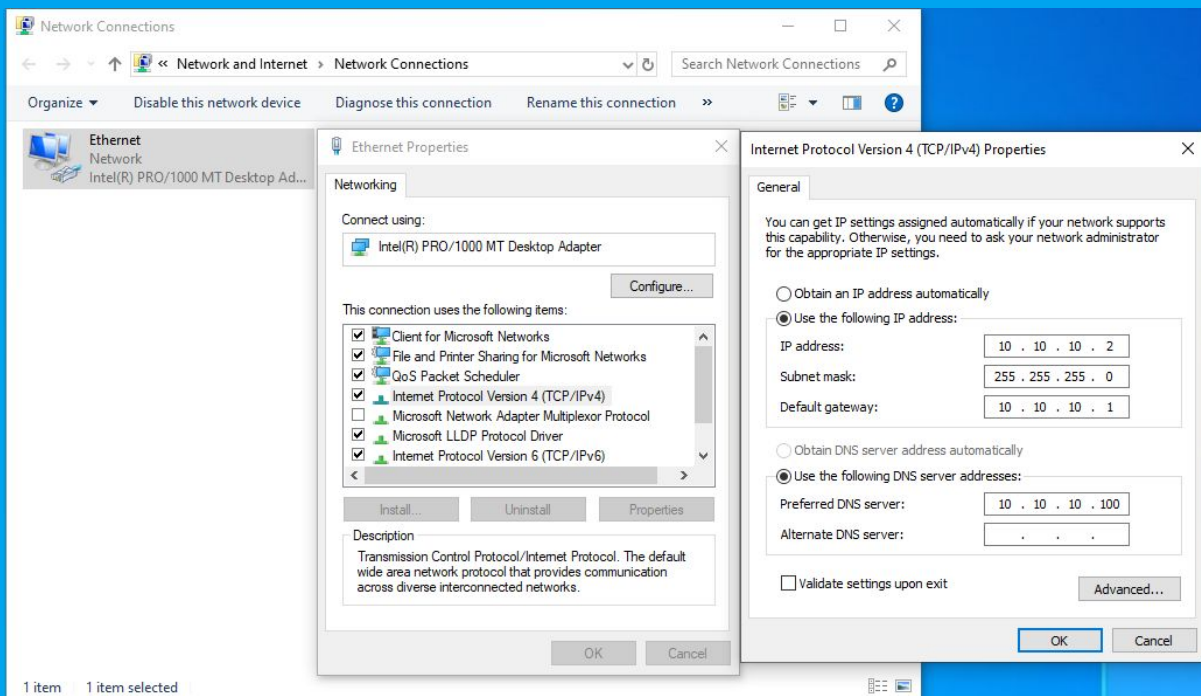
With that, we're done with first basic setup of CL01 (:

We'll come back to CL01 in order to join it to the domain as soon as we've set up our domain on DC01.

You can optionally check the setup if you're curious, otherwise continue with [DC01 - Installing the Domain Controller](#) .

CL01 - Check IP setup the GUI way (optional)

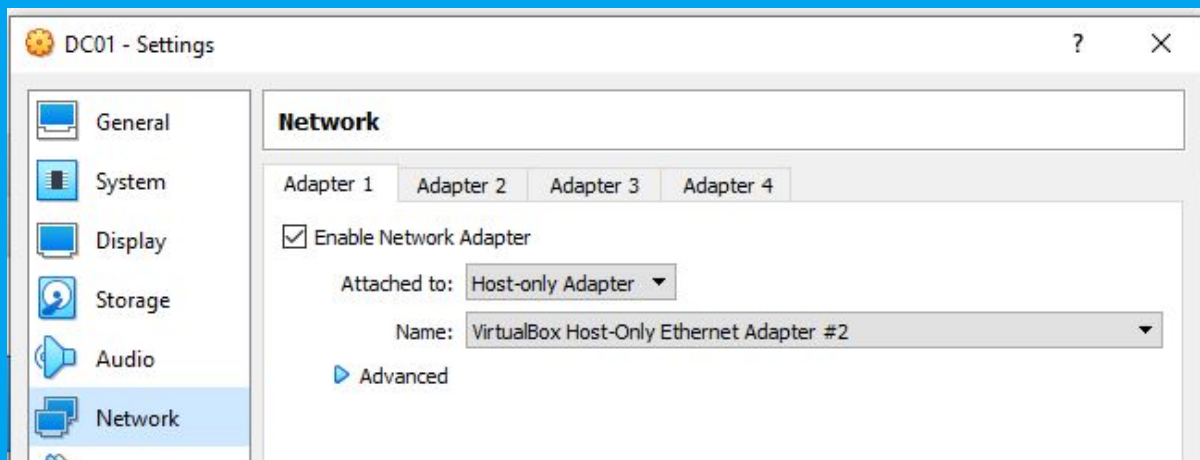
In case you want to check what the Powershell script did, you can do this by running 'ncpa.cpl' (in the search/run bar), right click on 'Ethernet' -> 'Properties', scroll down to 'Internet Protocol Version 4 (TCP/IPv4)' and click 'Properties':



Now we're done with the Client. Let's move on to the installation of our Domain Controller.

DC01 - Installing the Domain Controller

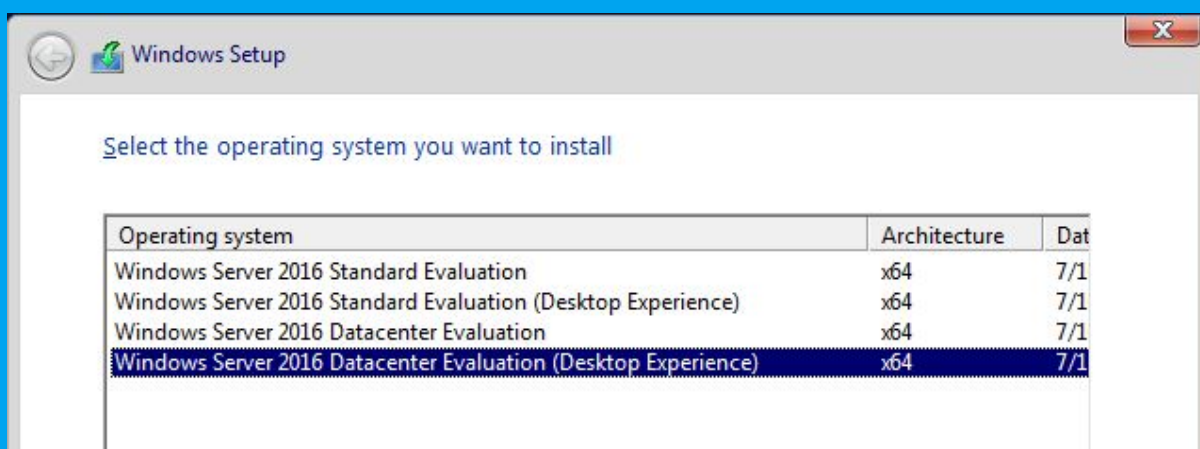
We also need to install a Domain Controller. Create a new virtual machine in VirtualBox, name it 'DC01', give it at least 4GB of RAM, a disk capacity of at least 20GB and the following network settings:



Under 'Storage' insert the ISO you downloaded for the Windows Server 2016 into the optical drive.

Start the virtual machine, installation of Windows Server 2016 should start now.

Select "Windows Server 2016 Datacenter Evaluation (Desktop Experience):

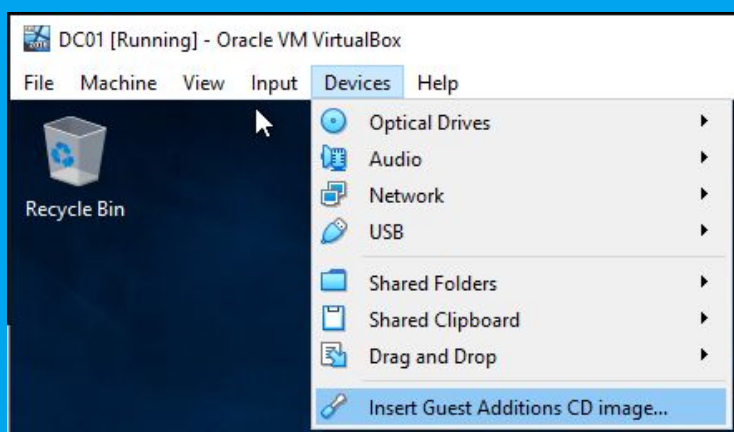


During installation, when prompted, create a user named 'Administrator' (should be the default name) with the password of 'Blackhoodie2019'.

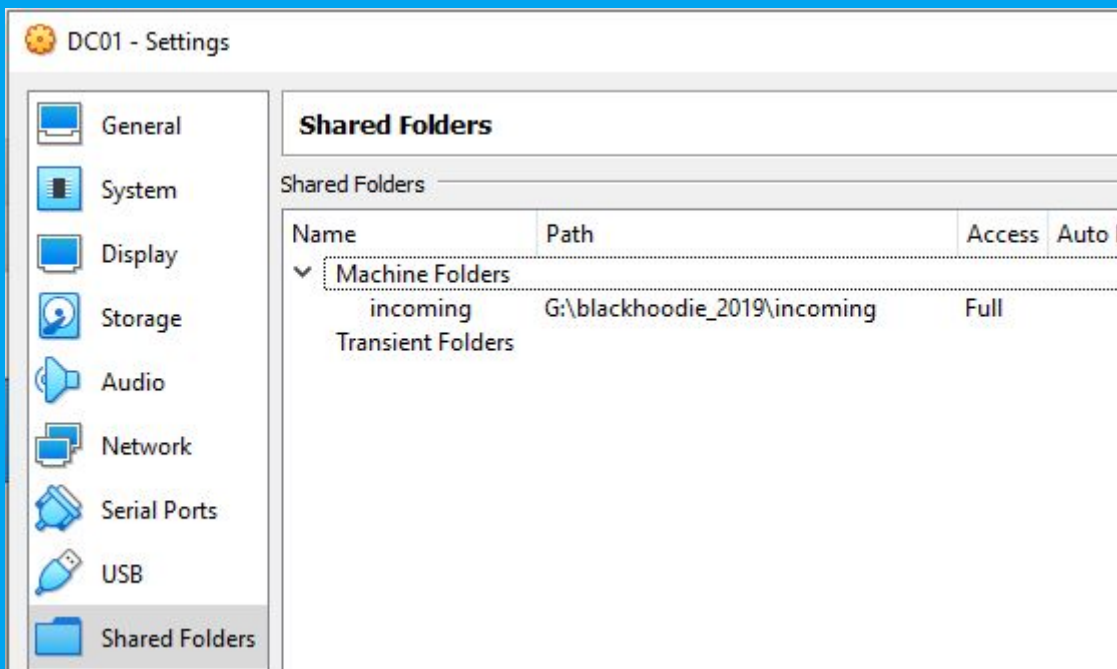
After the installation, log into DC01 with 'Administrator:Blackhoodie2019'.

DC01 - Install VirtualBox Guest Additions

Insert the VirtualBox Guest Additions via the menu and install them.



After a successful install you should be able to create a shared folder between your host and DC01:



Copy the following ZIP into the shared folder on your host:

<LINK TO FOLDER TBD>

In your VM you can access the shared folder by opening up an explorer window and typing \\vboxsrv into the address bar.

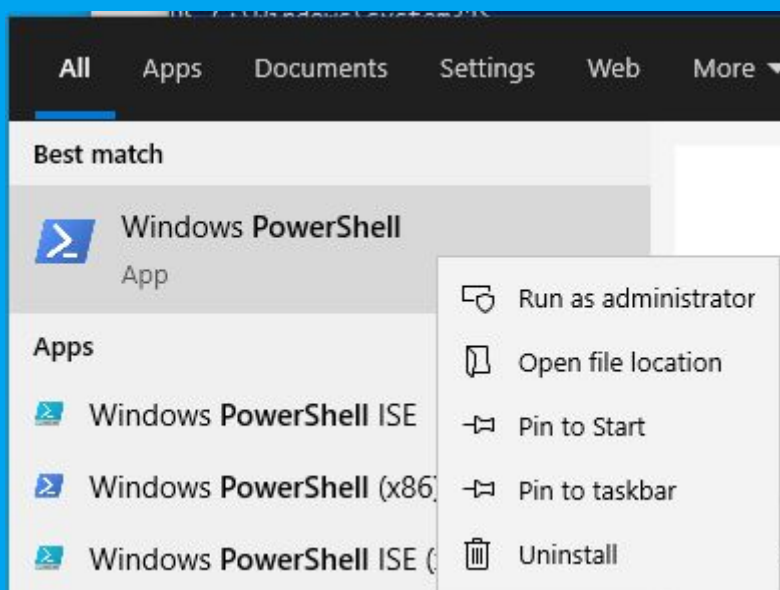
Copy the ZIP into C:\tools\.

(Hint: Just extract the first ZIP, not the one inside, since Windows Defender is still running it might delete some files it detects as 'harmful'. We'll do this in the workshop.)

DC01 - Post installation configuration

After installation open an administrative Powershell. Type:

'powershell' into the field and right click on the available option and 'Run as administrator':



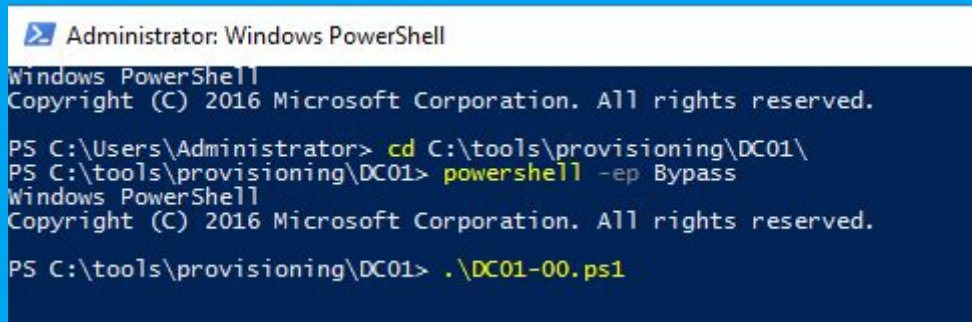
Navigate to the 'C:\tools\provisioning\DC01' folder you just extracted by typing:

```
> cd C:\tools\provisioning\DC01
```

```
> powershell -ep Bypass
```

Start the DC01-00.ps1 script by typing:

```
> .\DC01-00.ps1
```



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> cd C:\tools\provisioning\DC01\
PS C:\tools\provisioning\DC01> powershell -ep Bypass
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\tools\provisioning\DC01> .\DC01-00.ps1
```

This will change the hostname to 'DC01' and reboot.

Log back into the server with the user 'Administrator', open a new administrative Powershell like above and continue with DC01-01.ps1.

This will set the static IP of DC01 to 10.10.10.100 and configure the DNS for 10.10.10.100 and 127.0.0.1.

DC01 - Installing Active Directory Domain and Services (AD DS)

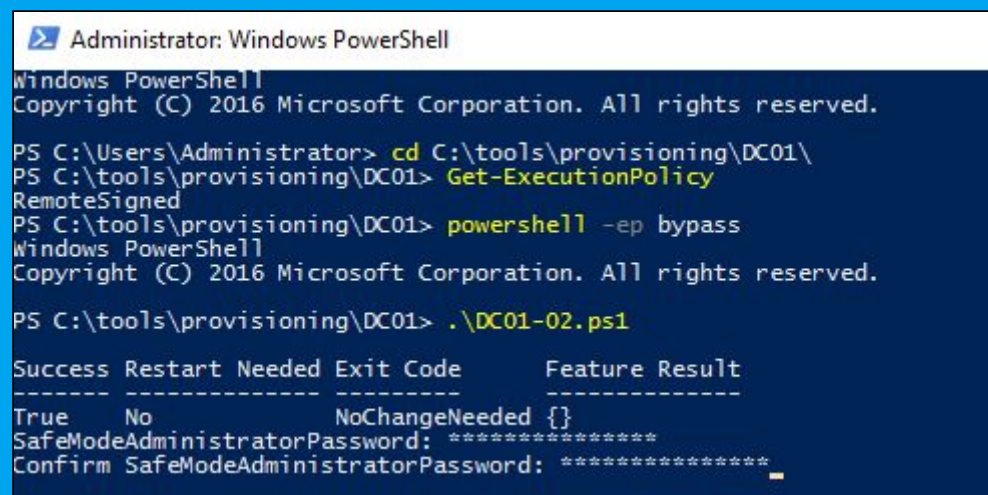
Now we need to install the AD DS role. For this, open an administrative Powershell and type:

```
> cd C:\tools\provisioning\DC01
```

```
> powershell -ep Bypass
```

Start the DC01-02.ps1 script by typing:

```
> .\DC01-02.ps1
```



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> cd C:\tools\provisioning\DC01\
PS C:\tools\provisioning\DC01> Get-ExecutionPolicy
RemoteSigned
PS C:\tools\provisioning\DC01> powershell -ep bypass
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\tools\provisioning\DC01> .\DC01-02.ps1

Success Restart Needed Exit Code      Feature Result
-----
True      No             NoChangeNeeded {}
SafeModeAdministratorPassword: *****
Confirm SafeModeAdministratorPassword: *****
```

(Note: The first time you'll run this the ExitCode should state 'Success' instead of 'NoChangeNeeded'.)

Powershell will prompt you for a password and a confirmation of the password, provide 'Blackhoodie2019'. This will be the password of the dsrm account (you don't have to worry about this account for now).

The installation will automatically log you out, reboot the server and when it comes back up (which may take some time) it's running your Active Directory Domain Services (:

Now let's import some users to our new Domain.

For this, open an administrative Powershell again and type:

```
> cd C:\tools\provisioning\DC01
```

```
> powershell -ep Bypass
```

Start the DC01-03.ps1 script by typing:

```
> .\DC01-03.ps1
```

Everything is fine if your output looks like this:

```
PS C:\tools\provisioning\DC01> .\DC01-03.ps1
Created user : Charles Lickens
Created user : Cat Damon
Created user : Paw McCatney
Created user : Luke Skywhisker
Created user : David Meowie
Created user : Demi Meower
Created user : Santa Claws
Created user : Kitty Purry
Created user : Cleo Catra
Created user : Brad Kitt
Created user : Catrick Stewart
Created user : Leopardo DeCatrio
Created user : Just Kittin
Created user : srv_mssql01
Checking domain DC=kittycorp,DC=com

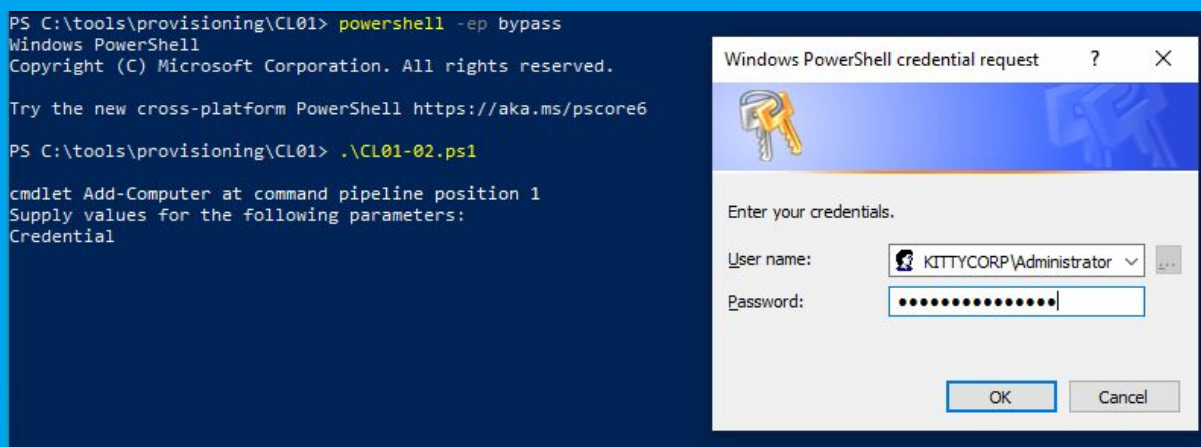
Registering ServicePrincipalNames for CN=srv_mssql01\ ,CN=Users,DC=kittycorp,DC=com
MSSQLSvc/mssql01.kittycorp.com
Updated object
14 Kittens just joined Kittycorporation.
PS C:\tools\provisioning\DC01>
```

Now all that is left, is to join the CL01 to the domain.

Back to the Client! /o/

CL01 - joining CL01 to the Domain - The Powershell way

Log into CL01 with 'shakespurr:blackhoodie2019', open an administrative Powershell again and call the CL01-02.ps1 which will join CL01 to the Kittycorp domain.



In the Pop-Up provide the credential of KITTYCORP\Administrator:Blackhoodie2019. Take care that you add the Domain KITTYCORP in front of it:

User name: KITTYCORP\Administrator

Password: Blackhoodie2019

The Client will restart and afterwards you've got a Domain-joined system.

Log back into CL01 with the local account 'shakespurr:blackhoodie2019' (note: by default CL01 will now try to authenticate via the domain, which you can see in the login screen when it states 'kittycorp'. To log in locally you'll have to provide the username in the following way:

.\shakespurr

Run one last setup script by opening an administrative Powershell again and call the CL01-03.ps1 which will make the final configurations we'll need for the workshop:

> cd C:\tools\provisioning\CL01

> powershell -ep Bypass

Start the CL01-03.ps1 script by typing:

> .\CL01-03.ps1

```
PS C:\Windows\system32> cd C:\tools\provisioning\CL01\
PS C:\tools\provisioning\CL01> powershell -ep Bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

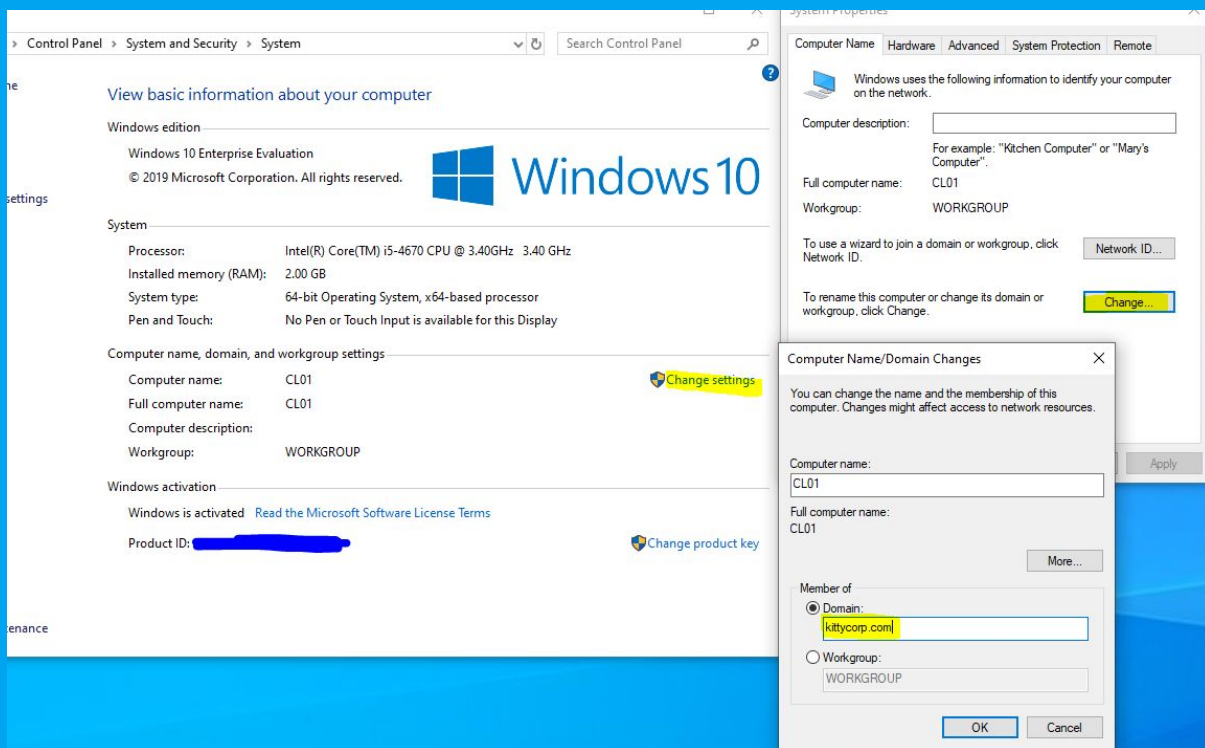
PS C:\tools\provisioning\CL01> .\CL01-03.ps1
PS C:\tools\provisioning\CL01> █
```

Alright, your configurations are ready for the workshop (:

If you like you can go through the [Final Setup Checks](#) to make sure everything works.

CL01 - joining CL01 to the Domain - The GUI way

After we've successfully installed the Domain and the Client we can join the CL01 to the Domain:

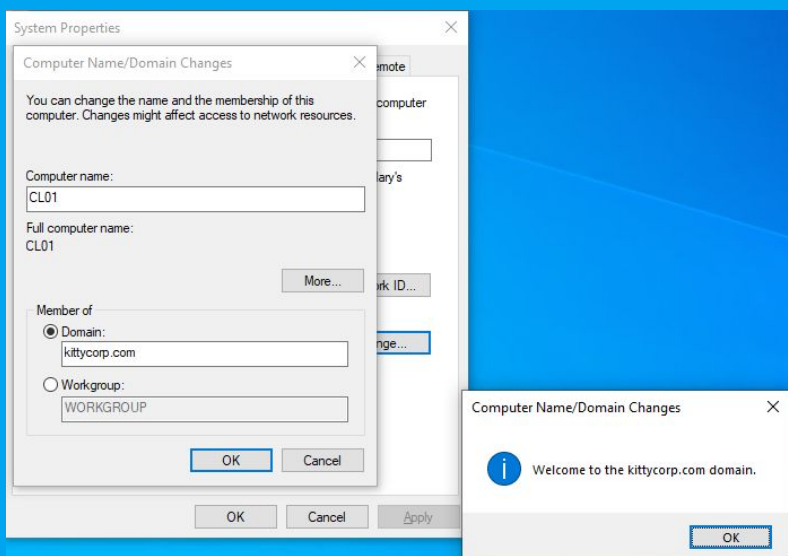


On CL01 navigate to Computer -> Properties -> Click the 'Change' Button, Select 'Member of Domain:' and type 'kittycorp.com'. Hit 'Ok'.

You'll be prompted for Credentials, insert:

KITTYCORP\Administrator with the password you supplied during the installation of the DC (if you followed this instruction the password will be 'Blackhoodie2019').

After this you should be greeted with the 'Welcome to the kittycorp.com domain' pop-up.



And yes, Welcome to the Domain (:

Open an administrative Powershell again and call the CL01-03.ps1 which will make the final configurations we'll need:

```
> cd C:\tools\provisioning\CL01
```

```
> powershell -ep Bypass
```

Start the CL01-03.ps1 script by typing:

```
> .\CL01-03.ps1
```

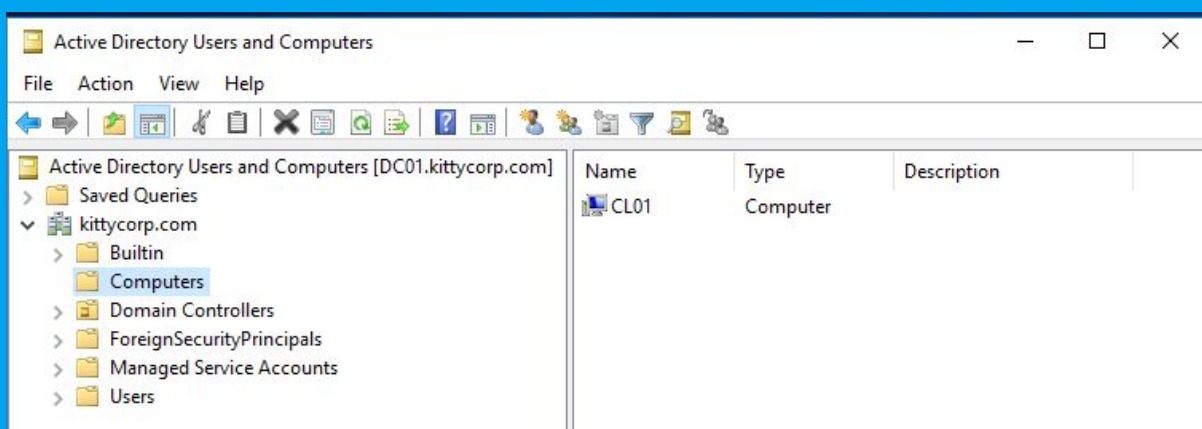
```
PS C:\Windows\system32> cd C:\tools\provisioning\CL01\  
PS C:\tools\provisioning\CL01> powershell -ep Bypass  
Windows PowerShell  
Copyright (C) Microsoft Corporation. All rights reserved.  
  
Try the new cross-platform PowerShell https://aka.ms/pscore6  
  
PS C:\tools\provisioning\CL01> .\CL01-03.ps1  
PS C:\tools\provisioning\CL01>
```

Alright, your configurations are ready for the workshop (:

Final Setup Checks

After joining CL01 to the domain you can check on DC01 that the CL01 is now a computer object that is part of the Domain:

For this you can start the “Active Directory Users and Computers” or simply type ‘dsa.msc’ in the command prompt on DC01. In the new window navigate to: kittycorp.com -> Computers and you should see the following:



That's it, you're ready for the workshop.

See you soon (: