Vulnerable Active Directory in VMWARE Documentation

Inhalt

Free Disk and Space

It will be good if you have at least 60 GB Hard Disk space for every machine and like 7 GB Memory. Later you can put it down if you do not need it

VMWARE Download Link

Vmware Download Link: https://files03.tchspt.com/down/VMware-workstation-full-17.6.1-24319023.exe

if this Link is not working then you can download it from my MEGA: https://mega.nz/file/3RESXRBQ#Lv0ujh7nDRfr6SaLdzKPEJzOe8OvilxfPs-l8j9Xh8E

Local Active Directory Information and Setup

I created **3 different Vmware Files**. This included:
Setting up the Networking
Setting up a local Domain with Full manual setup of the Domain Controller and the 2 Workstations.
Setting up 2 different workstations and joined them in the Domain.
--
As a plus you will need to install a Kali Machine on your vmware and make sure that you reach the Domain Controller (IP) and the 2 workstations

The Domain Name is: **MARVEL.local**
IP-address of the Domain Controller: **192.168.253.133**

2 Workstations (WINDOWS 11)

- **THEPUNISHER (192.168.253.134)**
- **SPIDERMAN (192.168.253.135)**

Beside that i created multiple local Admin users.

Created users and Passwords

Tony Shark Domain Administrator Password = Passw0rd123

SQLService Password = Passw0rd1234

fcastle and Peter parker Password = Passw0rd

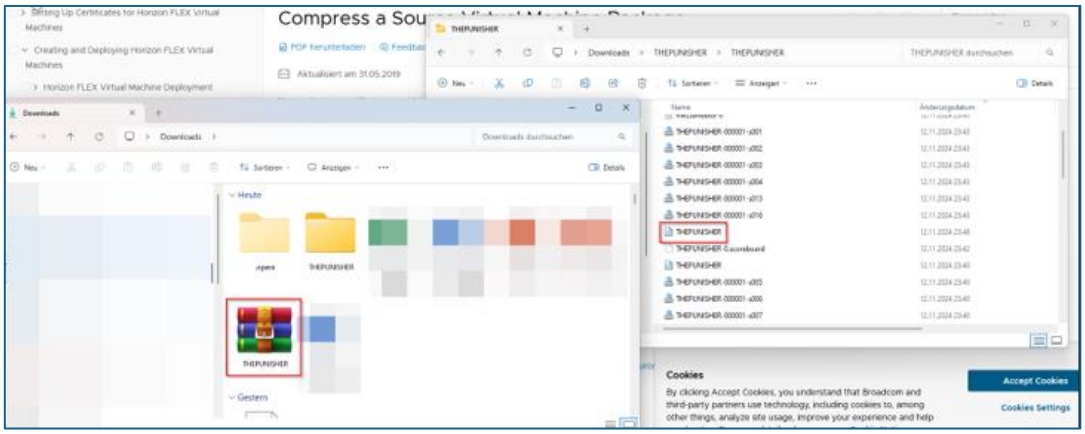
most of the time the Default password will be = Passw0rd

user: Administrator -> Password is: Passw0rd
Peter Parker (Login with peterparker) -> Password is -> Passw0rd
Frank Castle (Login with fcastle) -> Password is -> Passw0rd

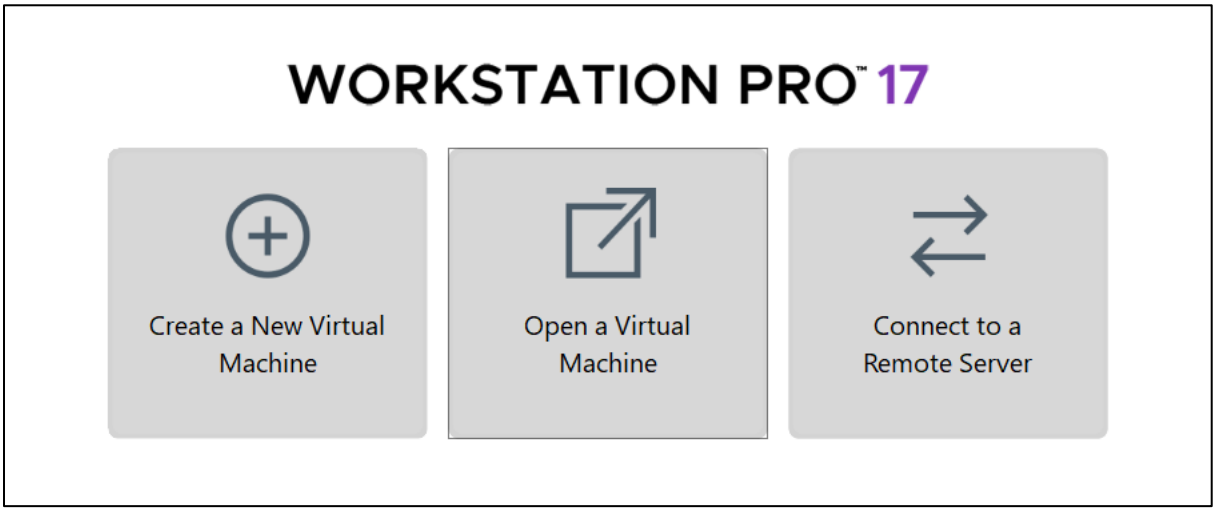
Steps to follow to setup the local Active Directory environment

Install Vmware.

- Download the Domain Controller (Windows Server 2022) from my MEGA Link: https://mega.nz/file/KVMDgLzZ#9LiGk1VQw3f5wGkuKCodj7KFJM6BBXA78vMT-YmGPLo
- Download the 2 Workstations **(THE PUNISHER)** and **(SPIDERMAN)** Link: will be updated soon!
- **THEPUNSHER File:** https://mega.nz/file/fJEVBB5Z#gPqMaWaUSX7qh5NBuOLCfiRgLGcj6LooTke90mP2MhQ
- **SPIDERMAN File:** https://mega.nz/file/rYMRHRyb#nVE-ypJqm622mRQ-75tyicGMQ6aBGSvw4Erx0SaCpjE
  For the Workstations you will need to download the File export the WINRAR File and open the THEPUNISHER and SPIDERMAN File in Vmware.
- Download all of them and open them using „Open a virtual Machine“ (see 2.nd Picture down below)



Download all of them and use the „Open a virtual Machine“

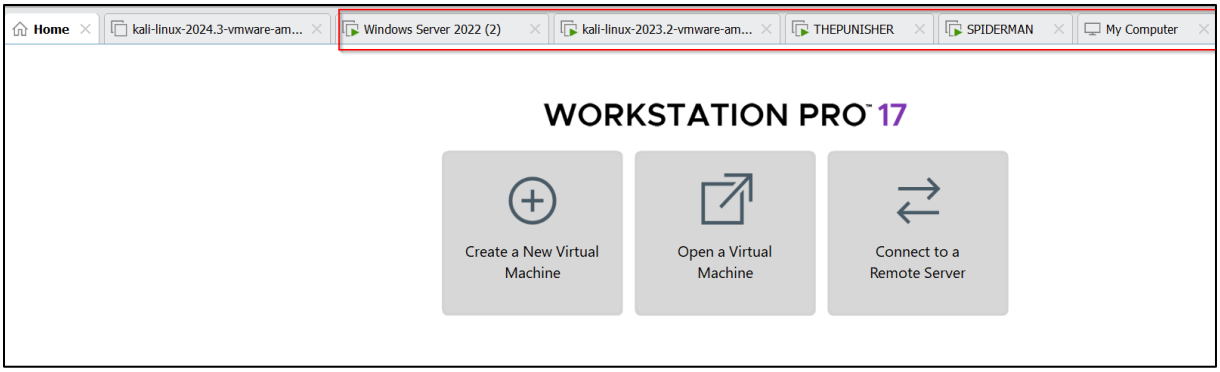


After deploying the 2 Workstations **THEPUNISHER** and **SPIDERMAN** you will be asked for a password and a prompt will be visible.

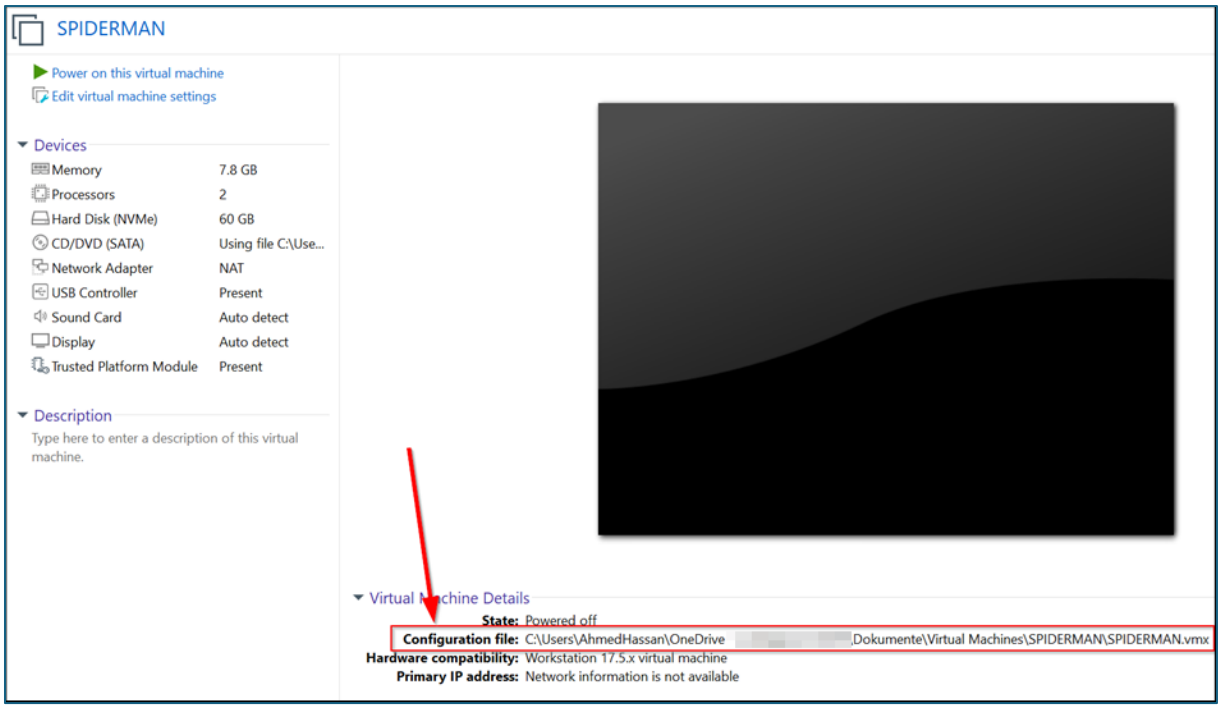
Please type the following Password -> **Passw0rd**

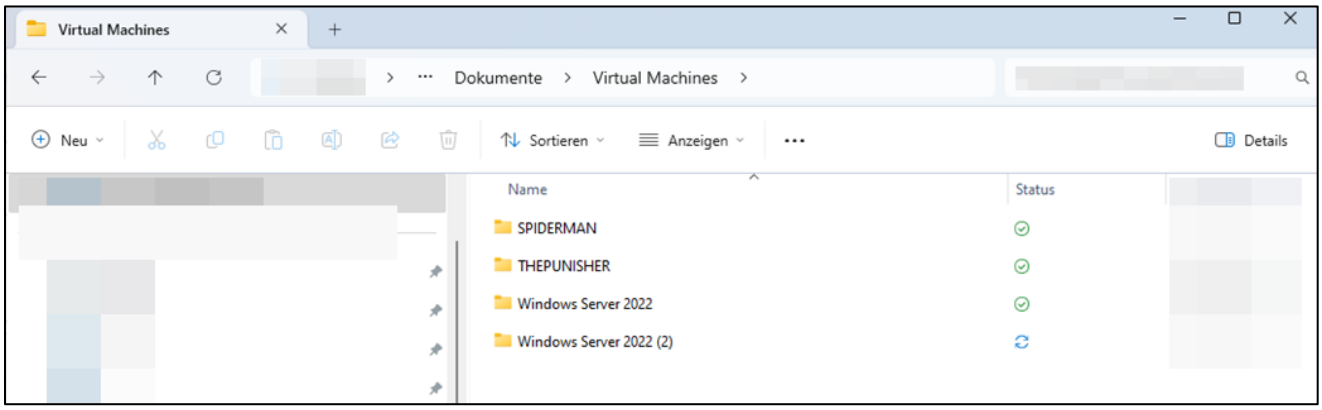
After that please use „I copied it“.

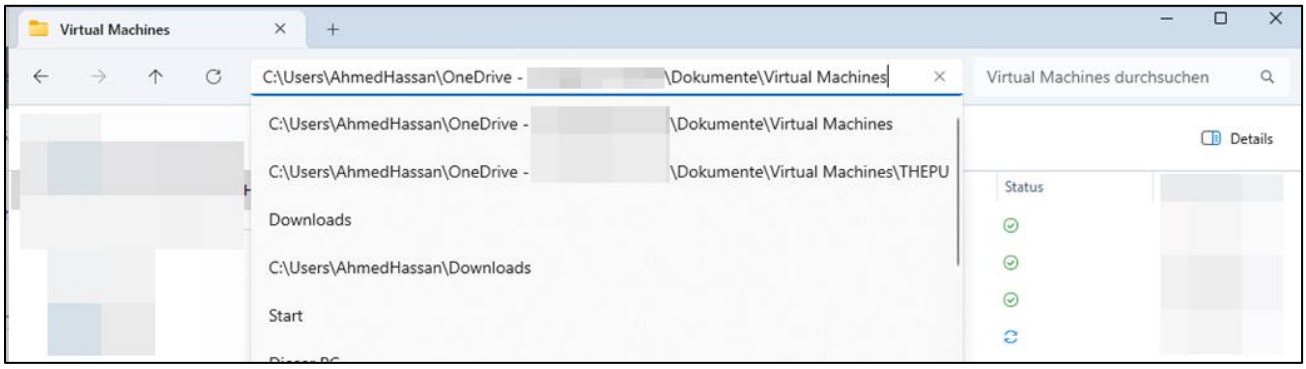
The Machines should be seen like this



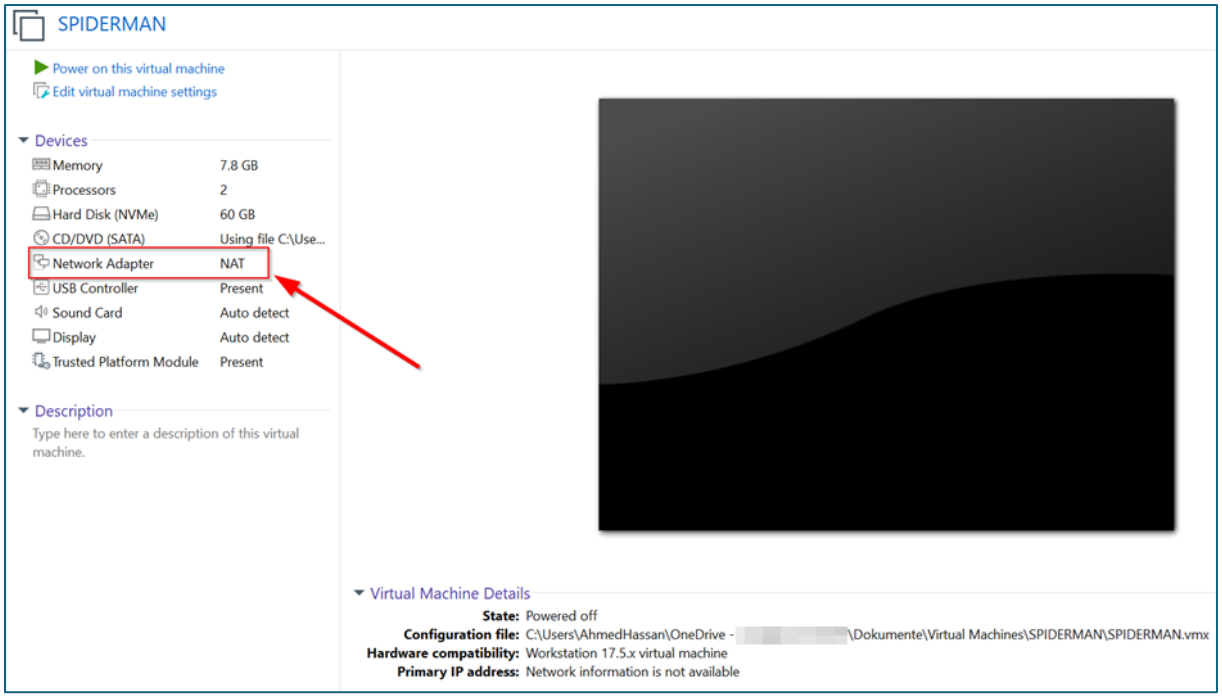
This is the Location oft he Virtual Machines. It is important to save the Directory oft he Virtual Machines as sometimes you need to import them from the start again.


SPIDERMAN
Power on this virtual machine
Edit virtual machine settings
Devices
Memory 7.8 GB
Processors 2
Hard Disk (NVMe) 60 GB
CD/DVD (SATA) Using file C:\Use...
Network Adapter NAT
USB Controller Present
Sound Card Auto detect
Display Auto detect
Trusted Platform Module Present
Description
Type here to enter a description of this virtual machine.
Virtual Machine Details
State: Powered off
Configuration file: C:\Users\AhmedHassan\OneDrive [redacted]\Dokumente\Virtual Machines\SPIDERMAN\SPIDERMAN.vmx
Hardware compatibility: Workstation 17.5.x virtual machine
Primary IP address: Network information is not available


Virtual Machines
Dokumente
Virtual Machines
Neu
Sortieren
Anzeigen
Details
Name
Status
SPIDERMAN
THEPUNISHER
Windows Server 2022
Windows Server 2022 (2)


Virtual Machines
C:\Users\AhmedHassan\OneDrive - [redacted]\Dokumente\Virtual Machines
Virtual Machines durchsuchen
C:\Users\AhmedHassan\OneDrive - [redacted]\Dokumente\Virtual Machines
C:\Users\AhmedHassan\OneDrive - [redacted]\Dokumente\Virtual Machines\THEPU
Downloads
C:\Users\AhmedHassan\Downloads
Start
Details
Status

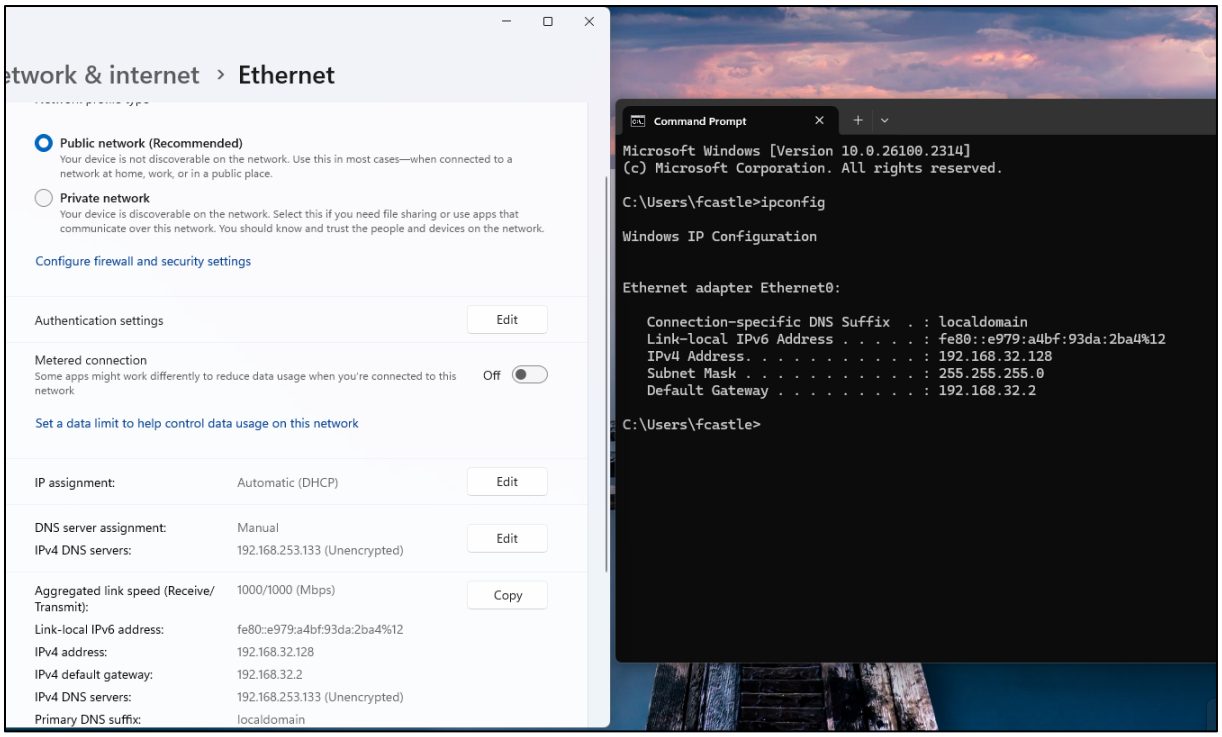
Network Config should be NAT



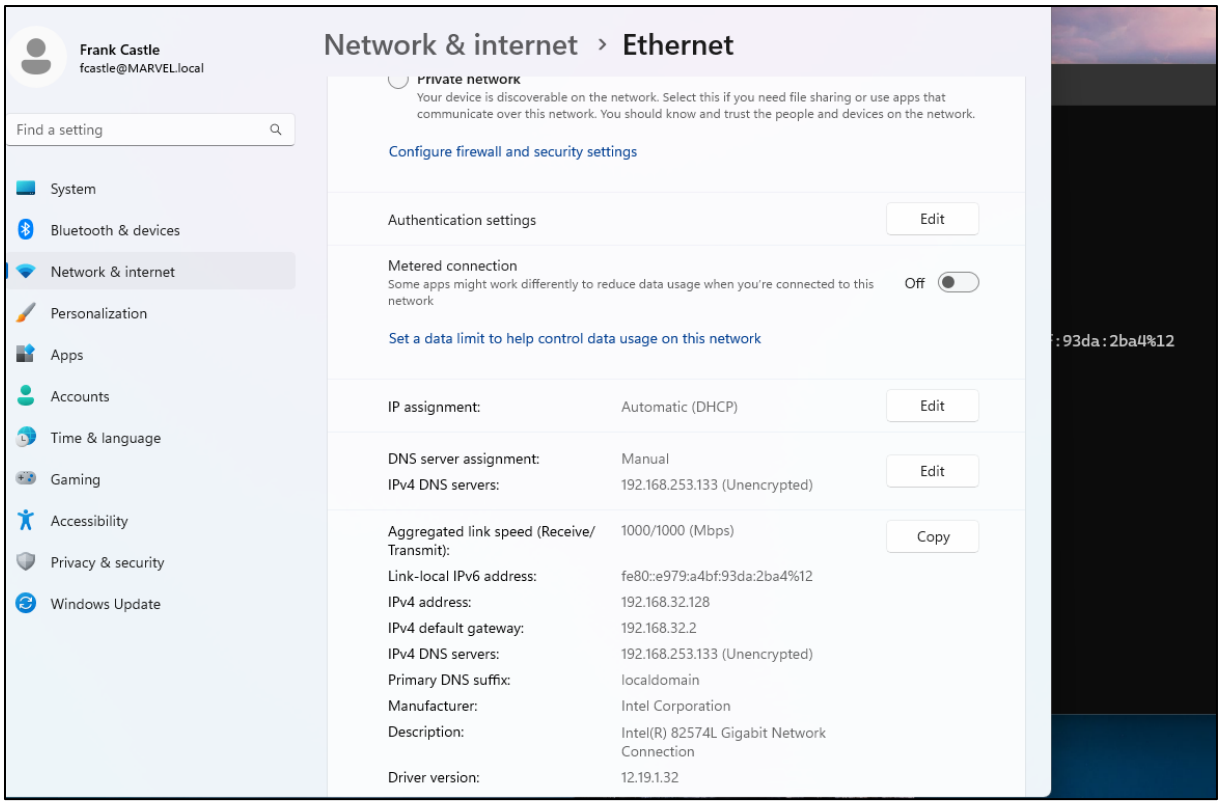
Configuring the Network after deploying the Windows Clients (Windows 11)

THEPUNISHER (1.st workstation)

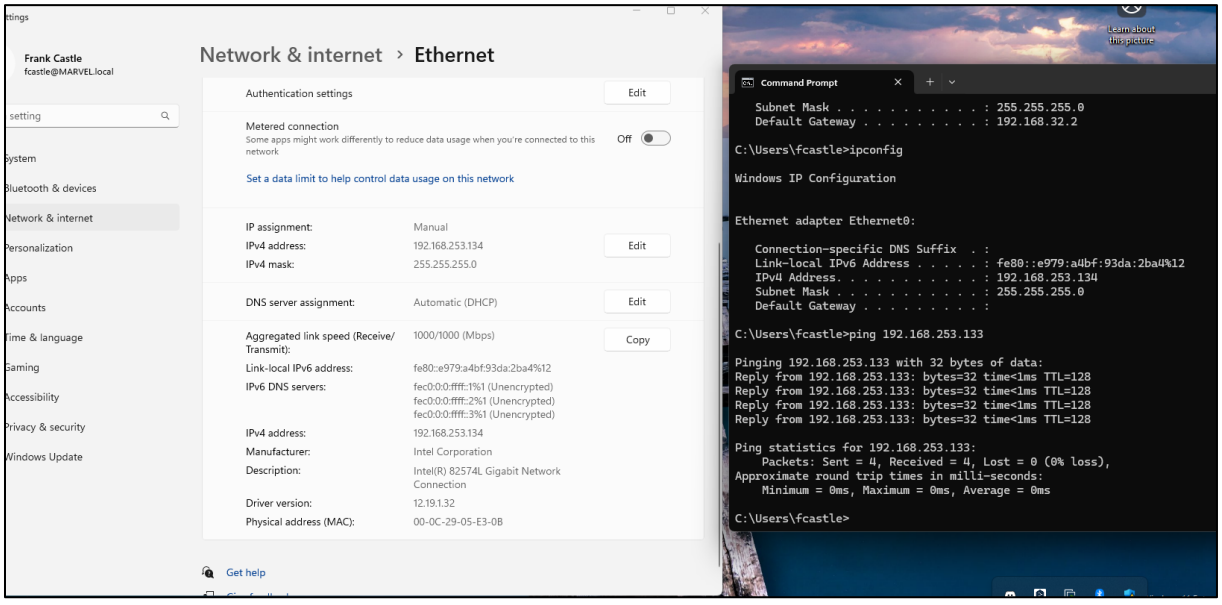
If you have the issue that the Windows Client (Windows 11) does not have the same Subnet like the Domain Controller then you need to do the following.



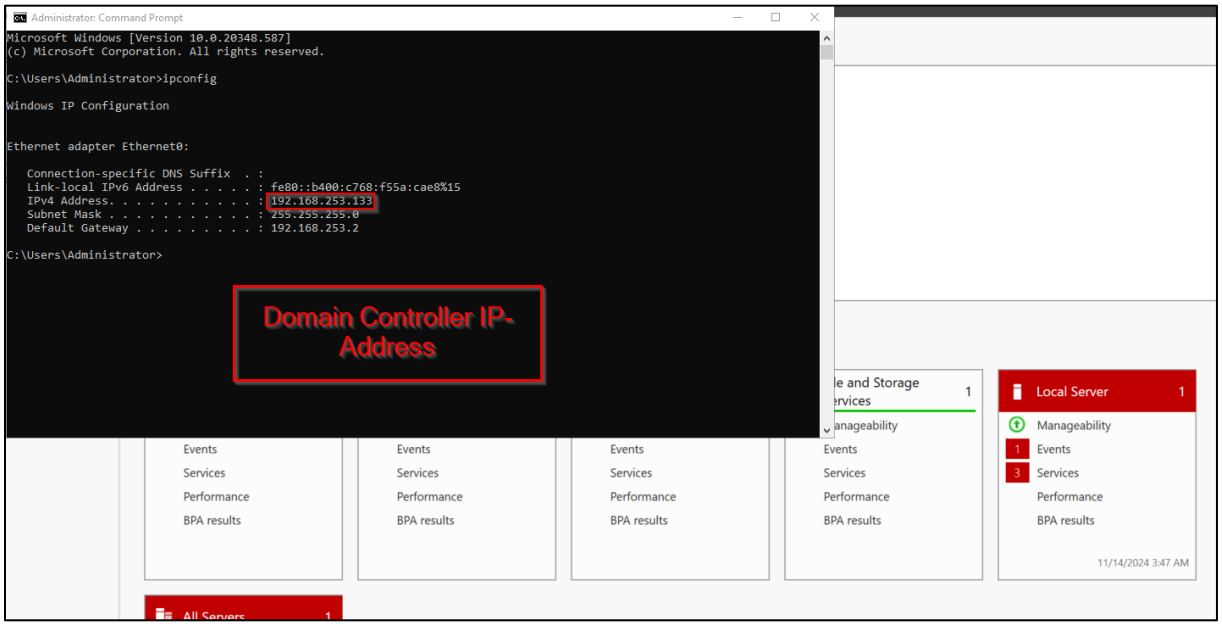
Open the Network Configruation

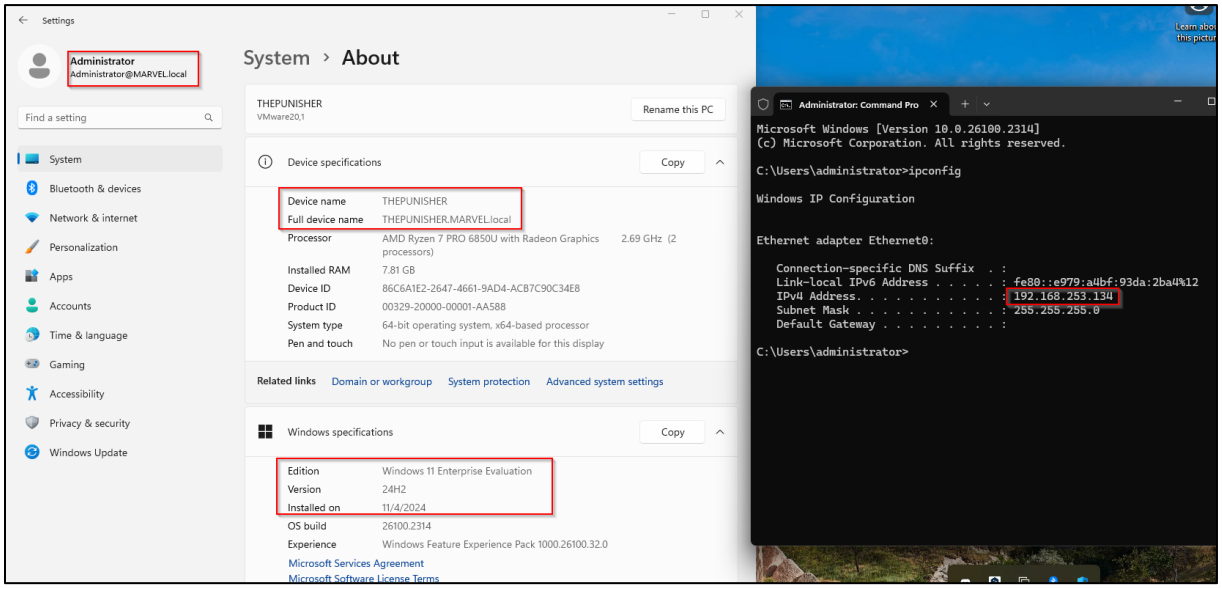


Change the Network settings to the settings down below in the screenshot to adapt it tot he correct Network confiugrations.



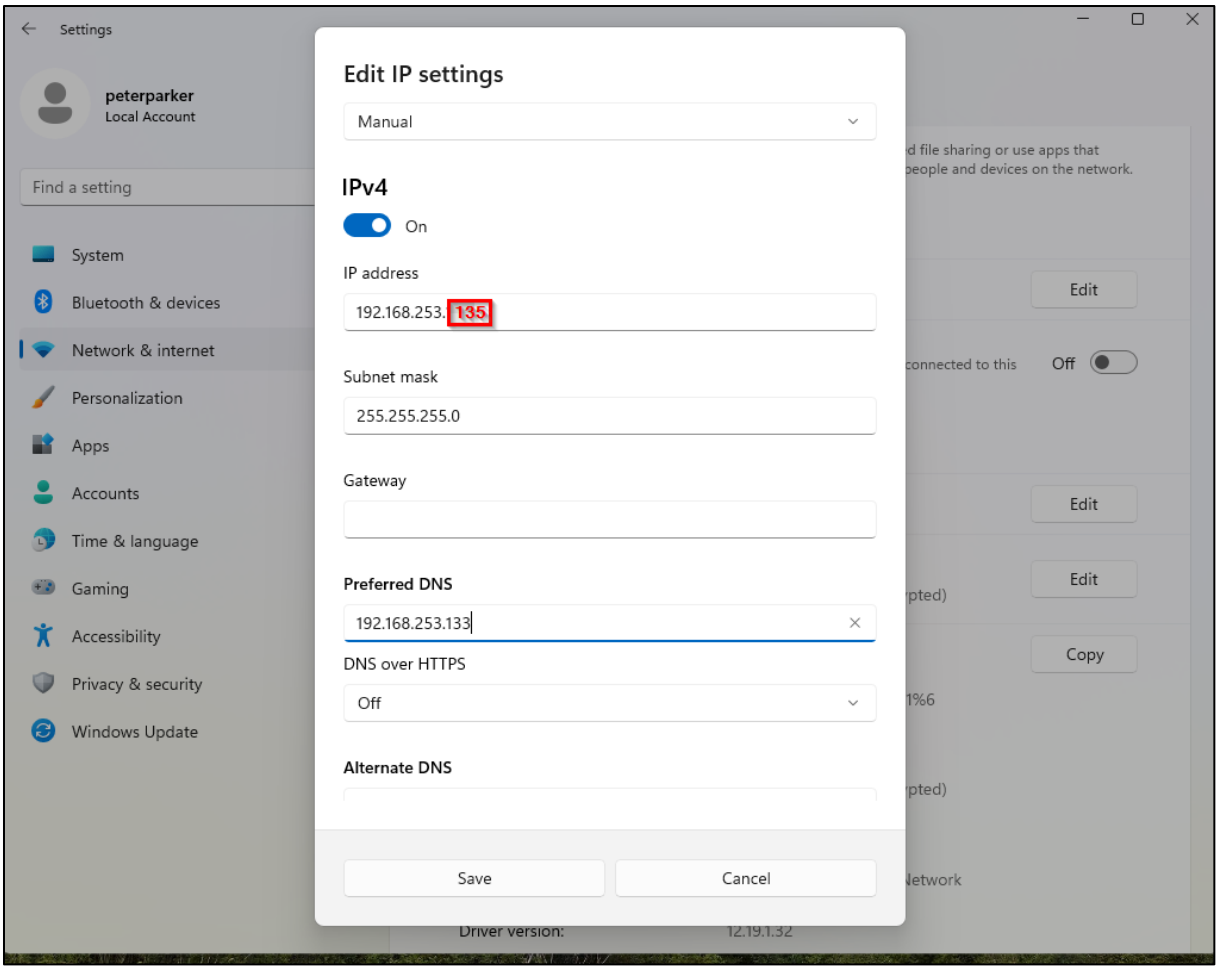
And as you can see we are in the same Subnet and Network like the Domain Controller and we can ping it as well + we are domain-joined.



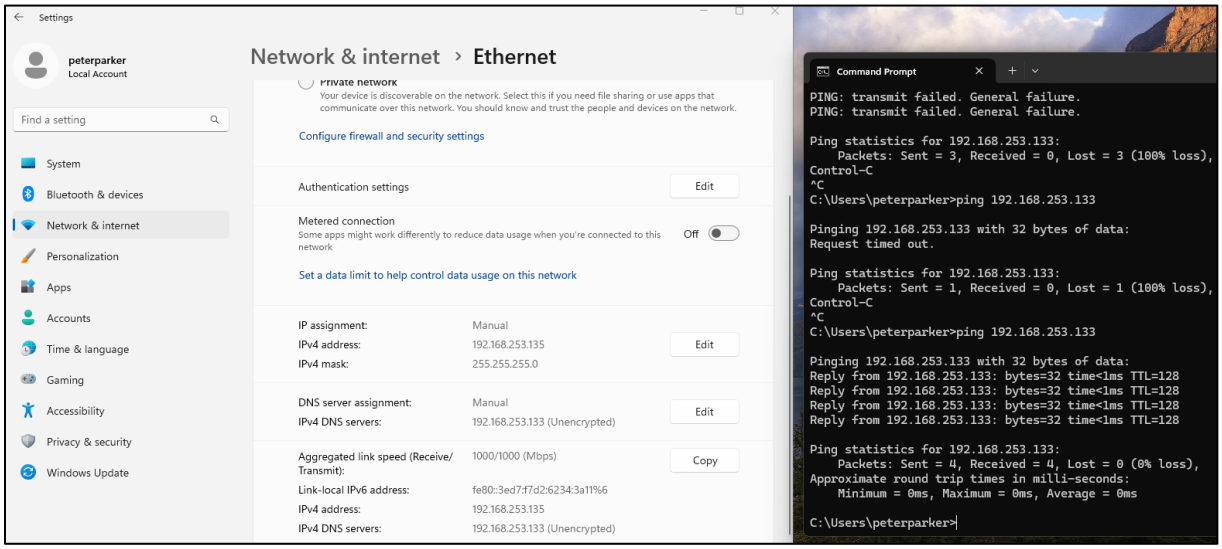


SPIDERMAN (2.nd workstation)

Please follow the same process as workstation 1 and adapt the settings here like the screenshots down below.



Use on the 2.nd Machine the IP-Address 192.168.253.135



If everthing is okay then you will be able to ping the Domain Controller with the IP 192.168.253.133

Vulnerable AD-Script

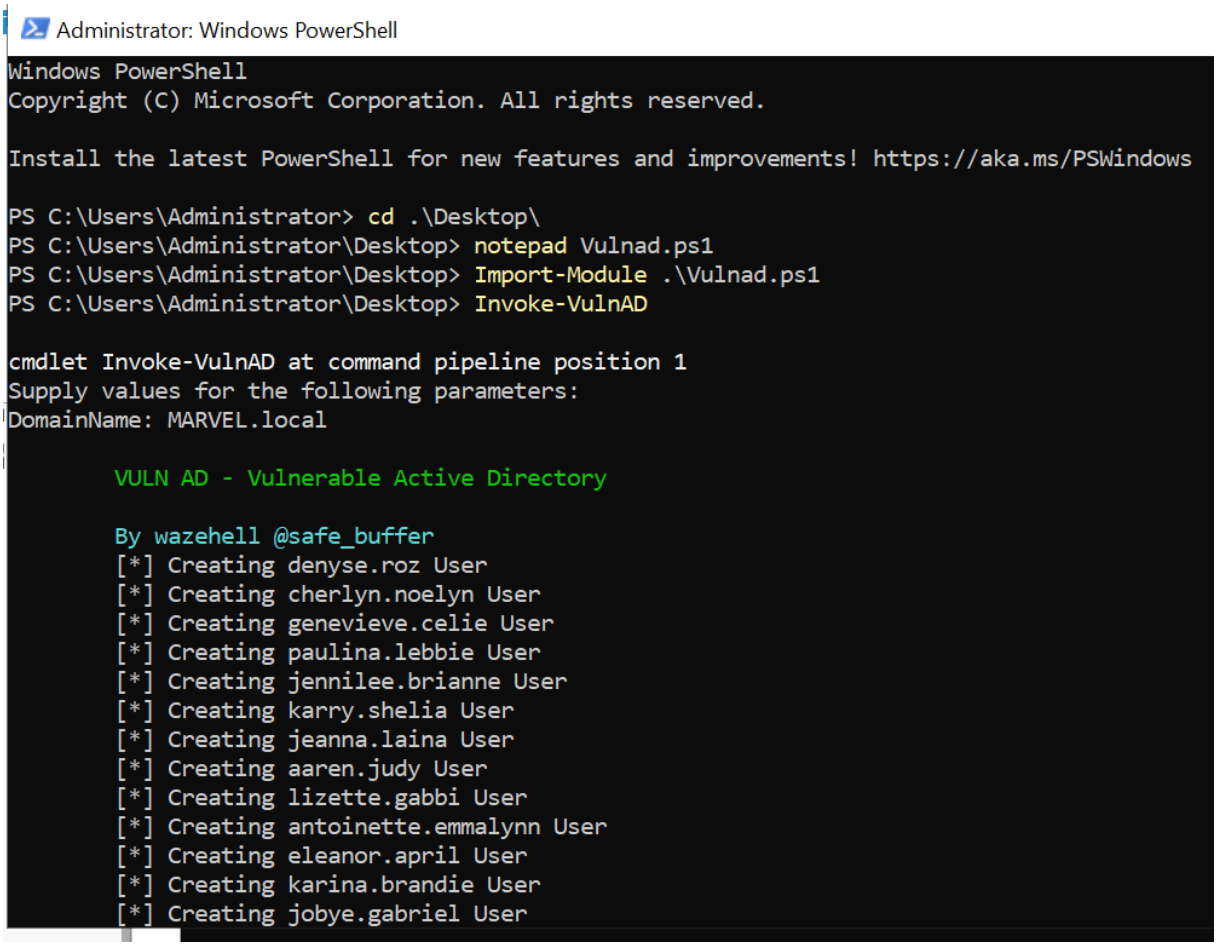
As we now have our Domain Controller and setup we want to add some Vulnerabilities, users, Misconfigurations in the ACL, Kerberoasting etc.

This is not included and must be done from your side as i wanted to make sure the File oft he Virtual Machine for uploading is not too big. 😉

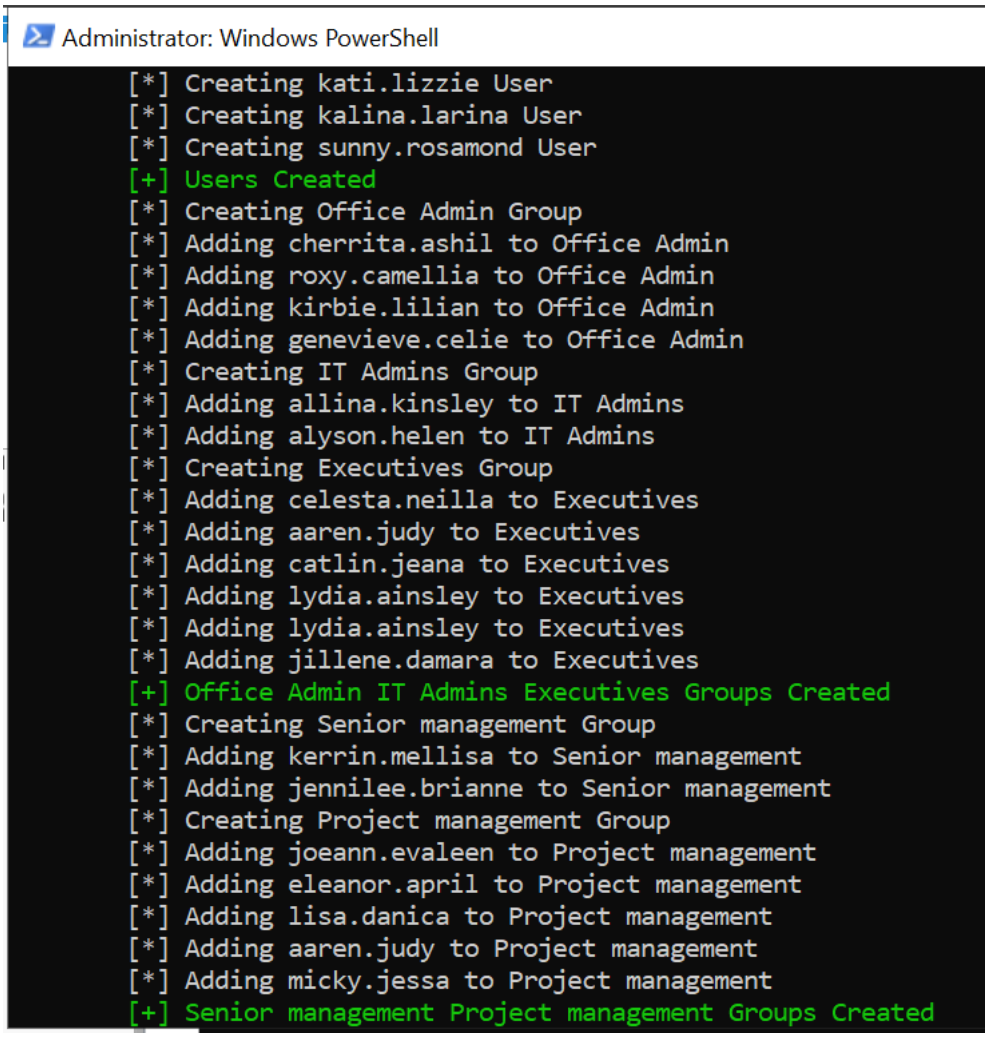
For that we will this GitHub Repo: https://github.com/safebuffer/vulnerable-AD

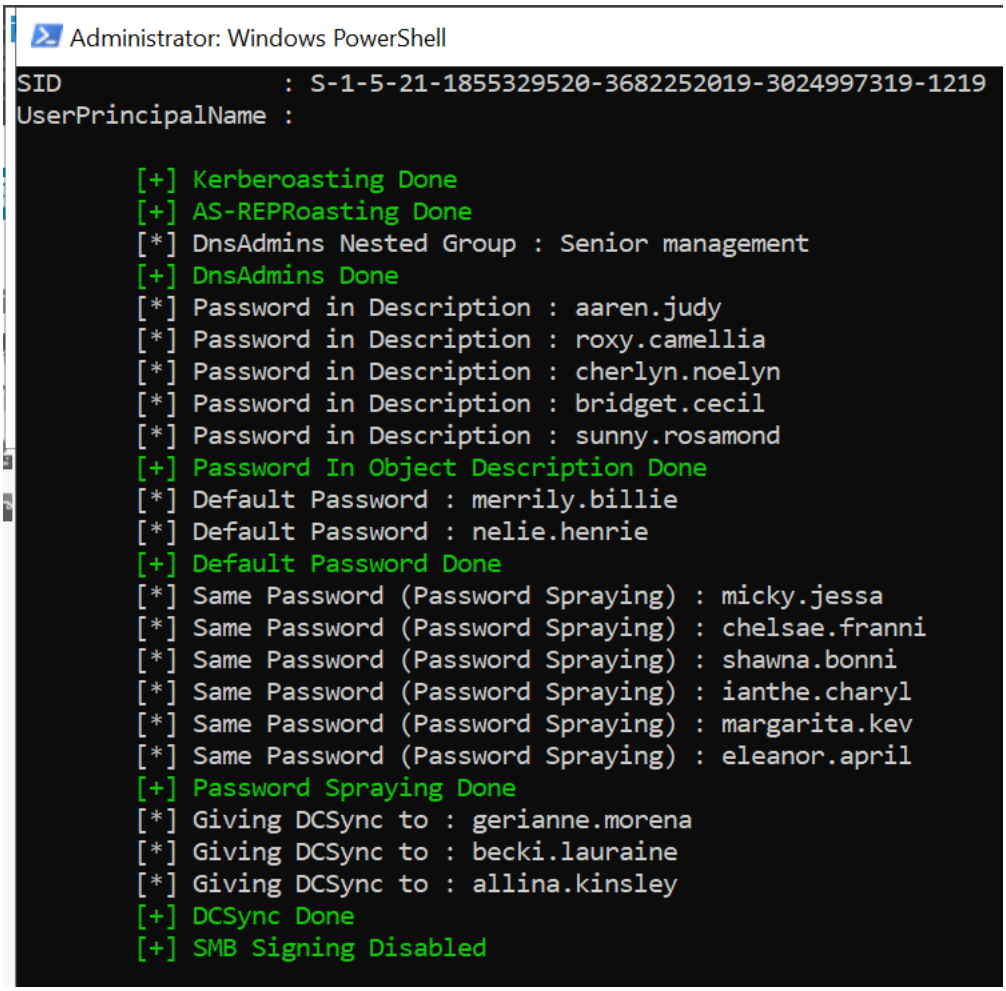
Video-Link: https://www.youtube.com/watch?v=Vk4SI3SIhzM

Copy the https://github.com/safebuffer/vulnerable-AD/blob/master/vulnad.ps1 Content and create a File as an Administrator on the Domain Controller like this. Paste the VulbAD.ps1 Content in the Notepad File and save it.

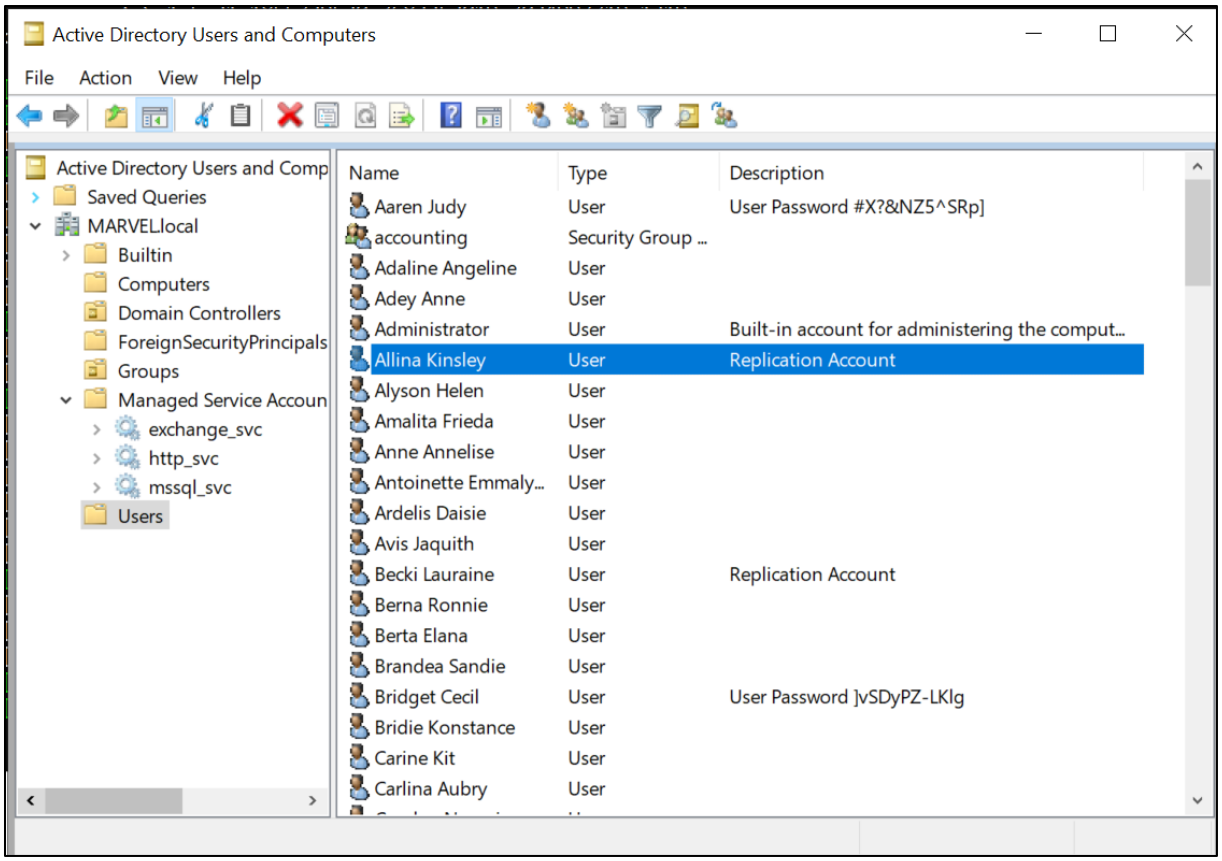


When you see this then the Creation is sucessful.


Administrator: Windows PowerShell
[*] Creating kati.lizzie User
[*] Creating kalina.larina User
[*] Creating sunny.rosamond User
[+] Users Created
[*] Creating Office Admin Group
[*] Adding cherrita.ashil to Office Admin
[*] Adding roxy.camellia to Office Admin
[*] Adding kirbie.lilian to Office Admin
[*] Adding genevieve.celie to Office Admin
[*] Creating IT Admins Group
[*] Adding allina.kinsley to IT Admins
[*] Adding alyson.helen to IT Admins
[*] Creating Executives Group
[*] Adding celesta.neilla to Executives
[*] Adding aaren.judy to Executives
[*] Adding catlin.jeana to Executives
[*] Adding lydia.ainsley to Executives
[*] Adding lydia.ainsley to Executives
[*] Adding jillene.damara to Executives
[+] Office Admin IT Admins Executives Groups Created
[*] Creating Senior management Group
[*] Adding kerrin.mellisa to Senior management
[*] Adding jennilee.brianne to Senior management
[*] Creating Project management Group
[*] Adding joeann.evaleen to Project management
[*] Adding eleanor.april to Project management
[*] Adding lisa.danica to Project management
[*] Adding aaren.judy to Project management
[*] Adding micky.jessa to Project management
[+] Senior management Project management Groups Created



From here all this users can be found on the Domain Controller with all the Misconfigurations, Passwords in Description etc.



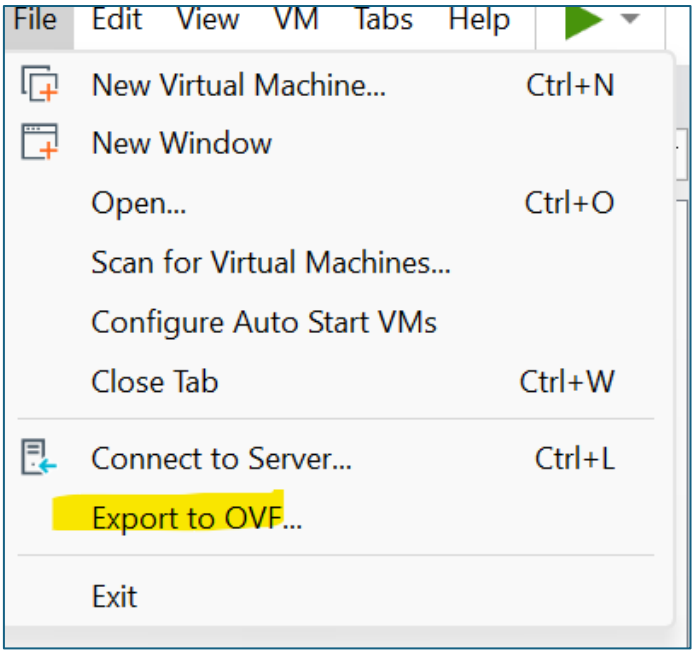
Export Functions for the Virtual Machines

its important to export all 3 Machines so we can use them anywhere on other devices.

Windows Server 2022 (EXPORT)

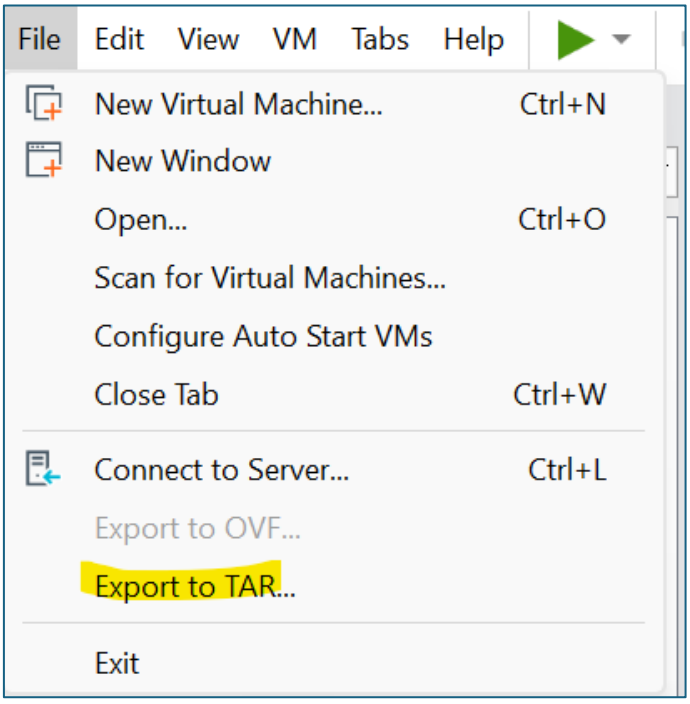
For that we will export the Domain Controller Windows Server 2022 first. For that we need to

- Power off the Machines
- Click on it -> Go to File and choose „Export to OVF“



2 Workstations Export

- Power off the Machines
- Click on it -> Go to File and choose „Export to TAR“
- This will export the Machine as a WINRAR File. For importing it into vmware again you need to extract the Files into a new File and choose the File „THEPUNISHER“. As soon as you try to import it in vmware, vmware will automatically show you the correct File and you only need to click and choose it.



Snapshots

Before starting the Scans ist recommended to make Snapchots as in case anything goes wrong you can go back to the saved place. This should be done after installing and setting up all the machines.