

Vulnerable Active Directory in VMWARE Documentation

Inhalt

Vulnerable Active Directory in VMWARE Documentation	1
Free Disk and Space	1
VMWARE Download Link	1
Local Active Directory Information and Setup.....	1
Created users and Passwords	2
Steps to follow to setup the local Active Directory environment	2
Configuring the Network after deploying the Windows Clients (Windows 11)	6
THEPUNISHER (1.st workstation).....	6
SPIDERMAN (2.nd workstation)	9
Vulnerable AD-Script	11
Export Functions for the Virtual Machines	14
Snapshots.....	16

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.tchsp.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

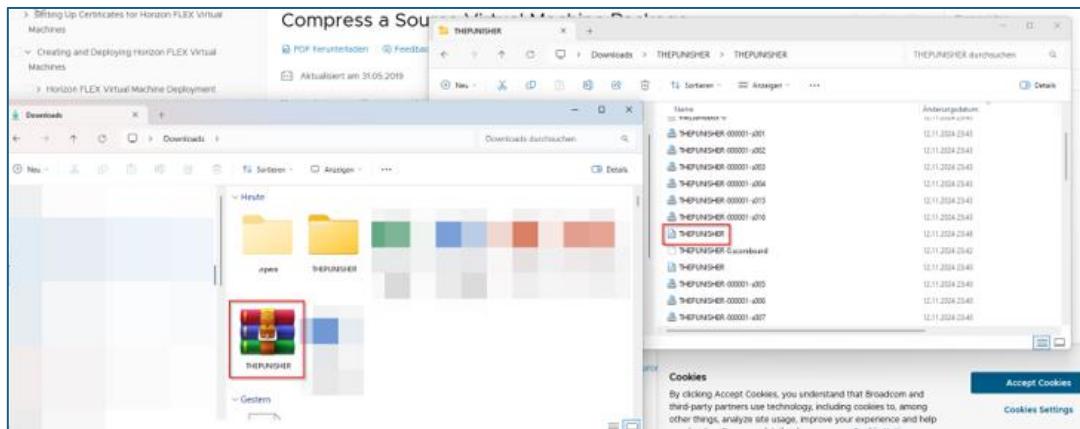
Peter Parker (Login with peterparker) -> Password is -> Passw0rd

Frank Castle (Login with fcastle) -> Password is -> Passw0rd

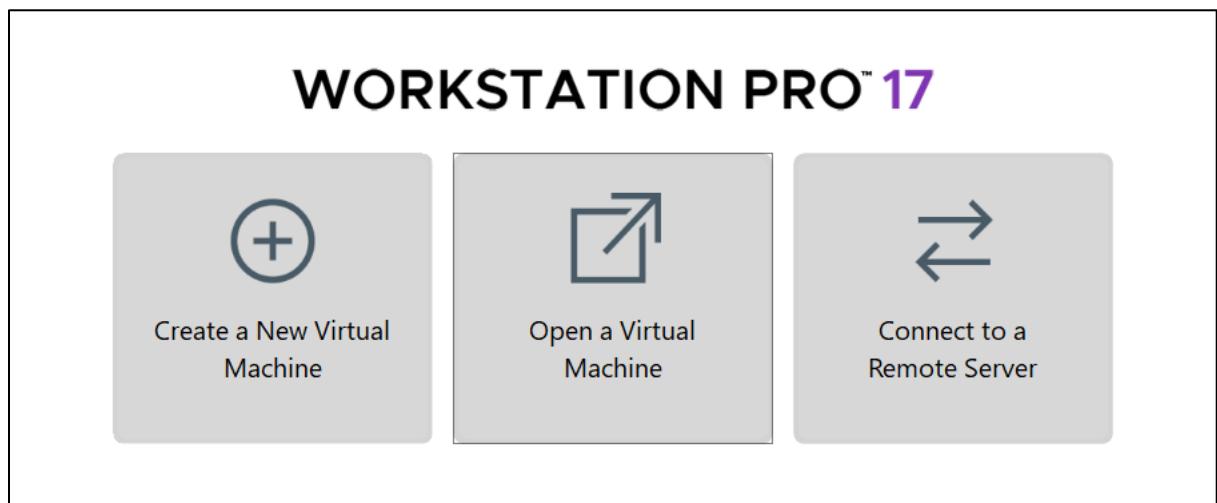
Steps to follow to setup the local Active Directory environment

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!
- **THEPUNISHER 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)



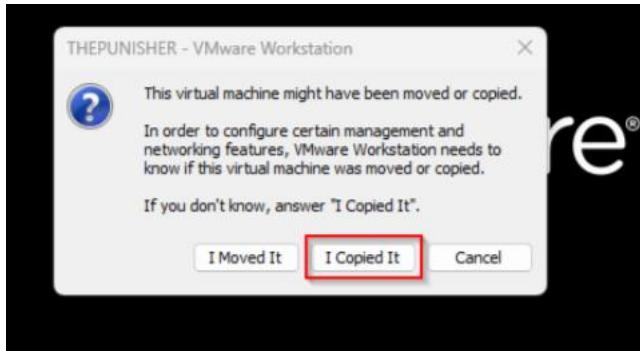
Download all of them and use the „Open a virtual Machine“



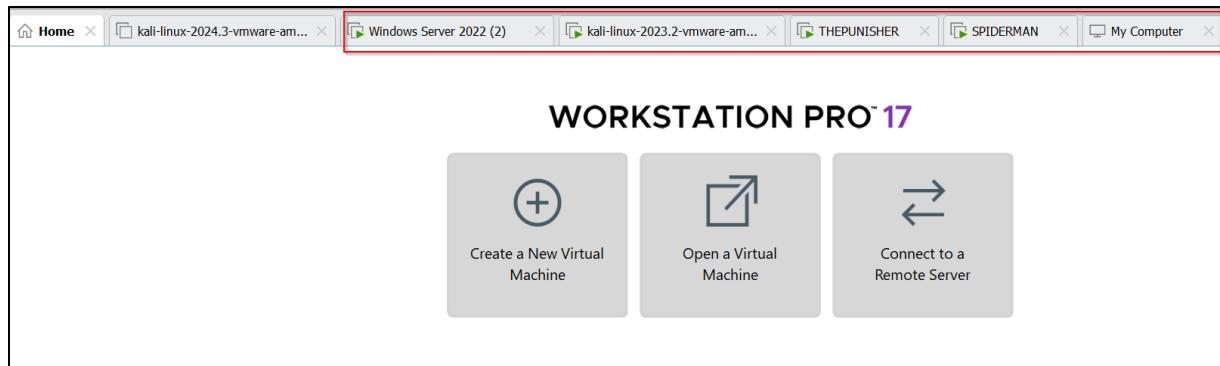
After deploying the 2 Workstations **THEPUNISHER** and **SPIDERMAN** you will be asked for a password and a prompt will be visible.

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

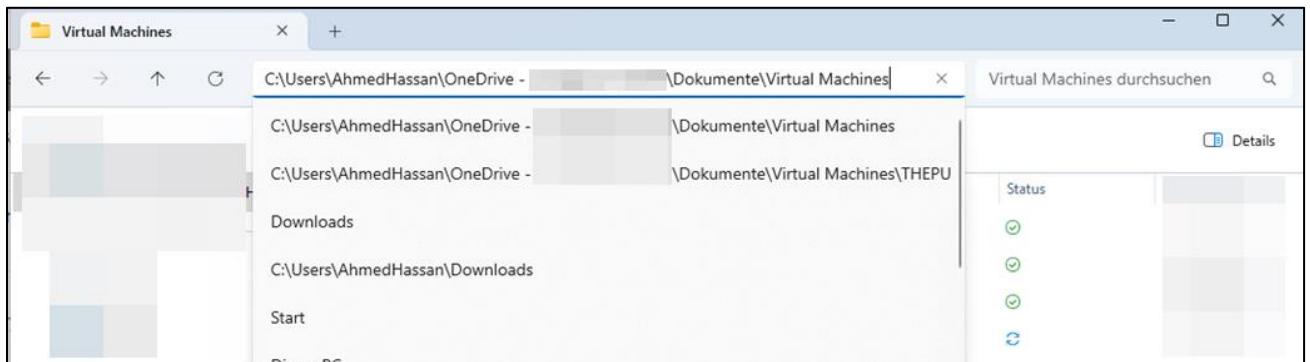
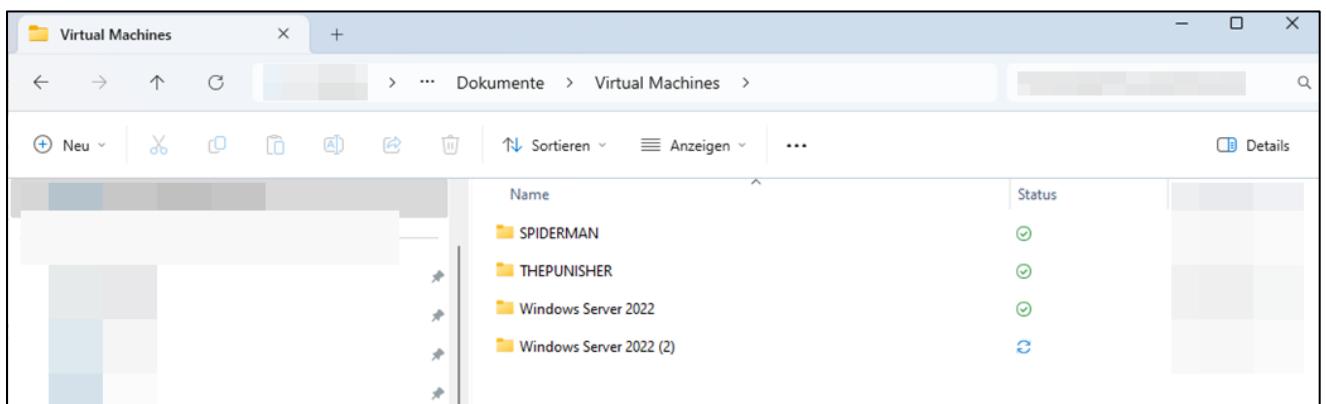
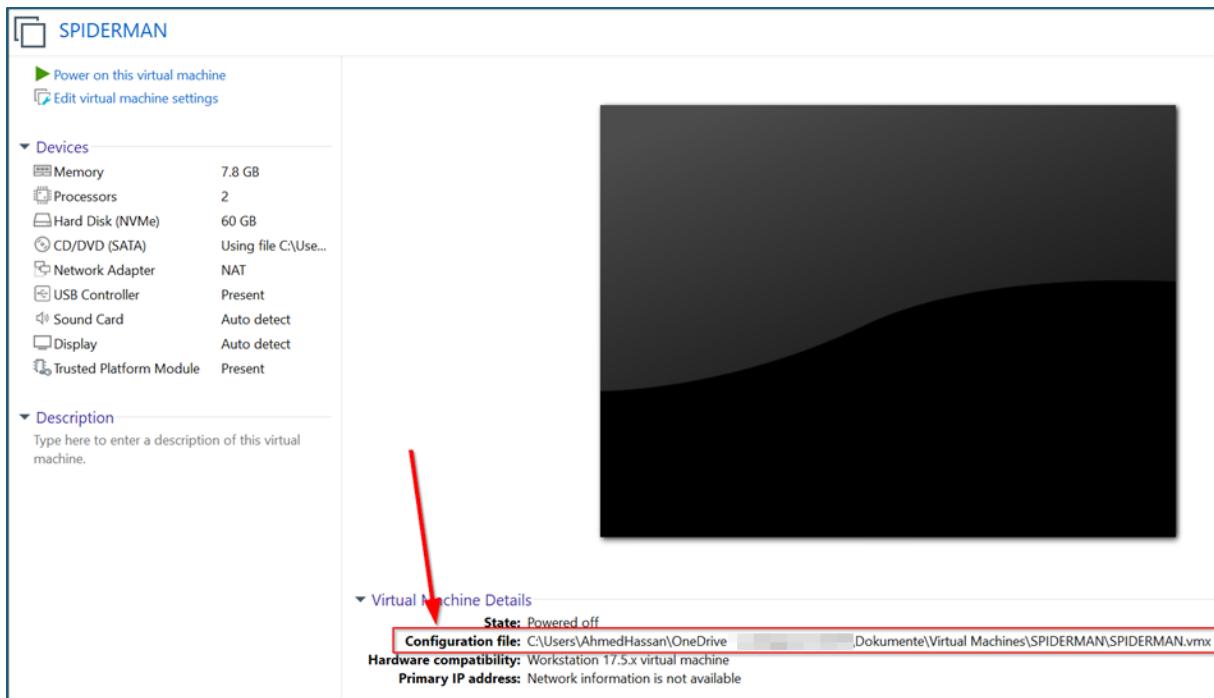
After that please use „I copied it“.



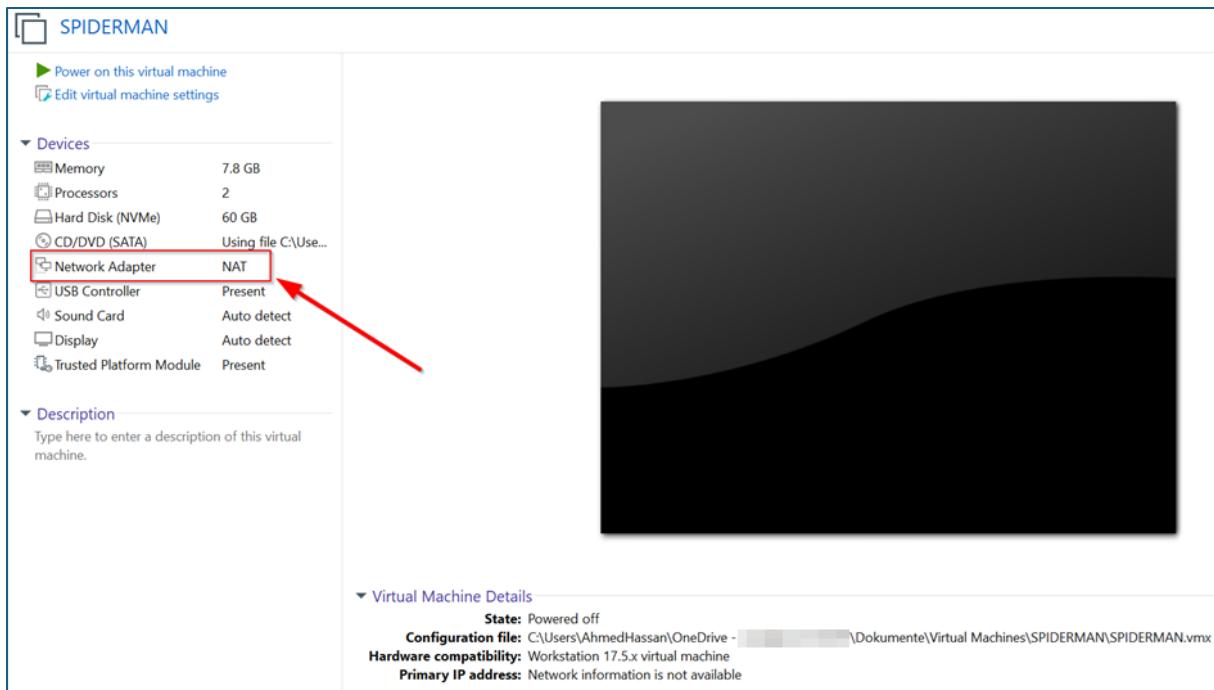
The Machines should be seen like this



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



Network Config should be NAT



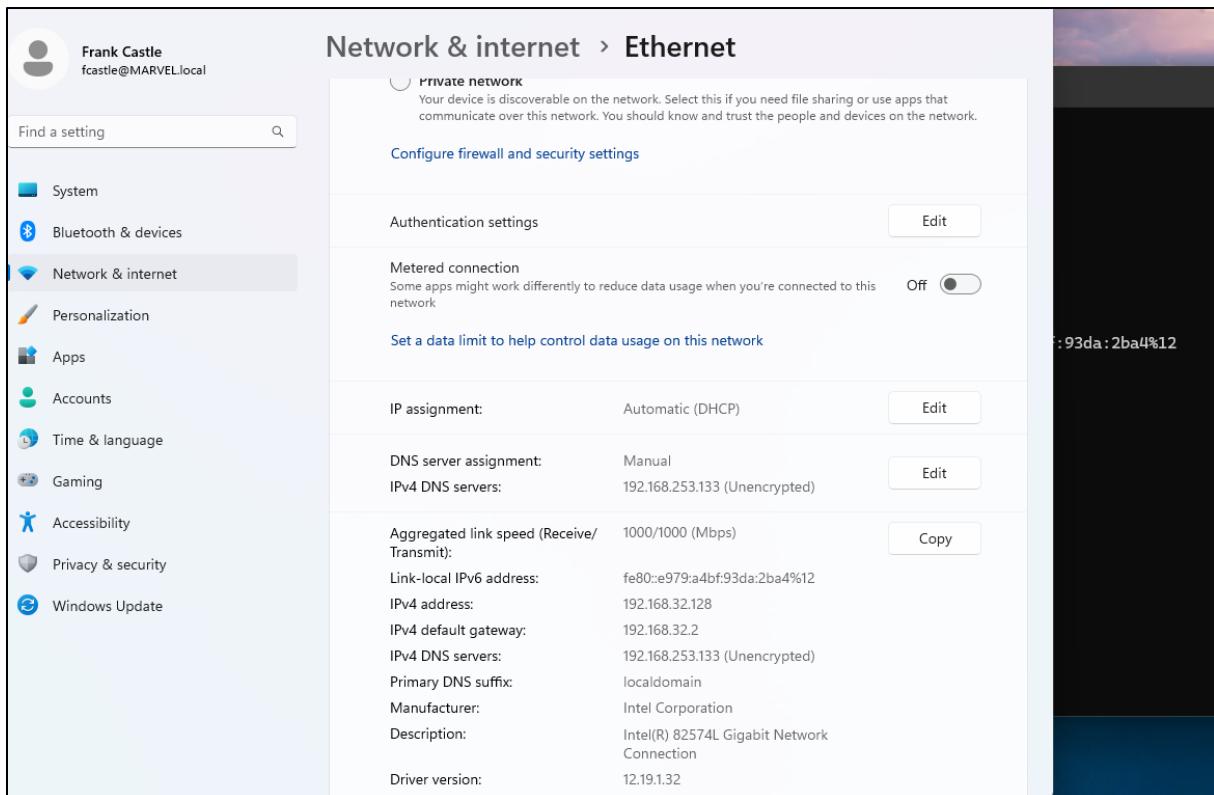
Configuring the Network after deploying the Windows Clients (Windows 11)

THEPUNISHER (1.st workstation)

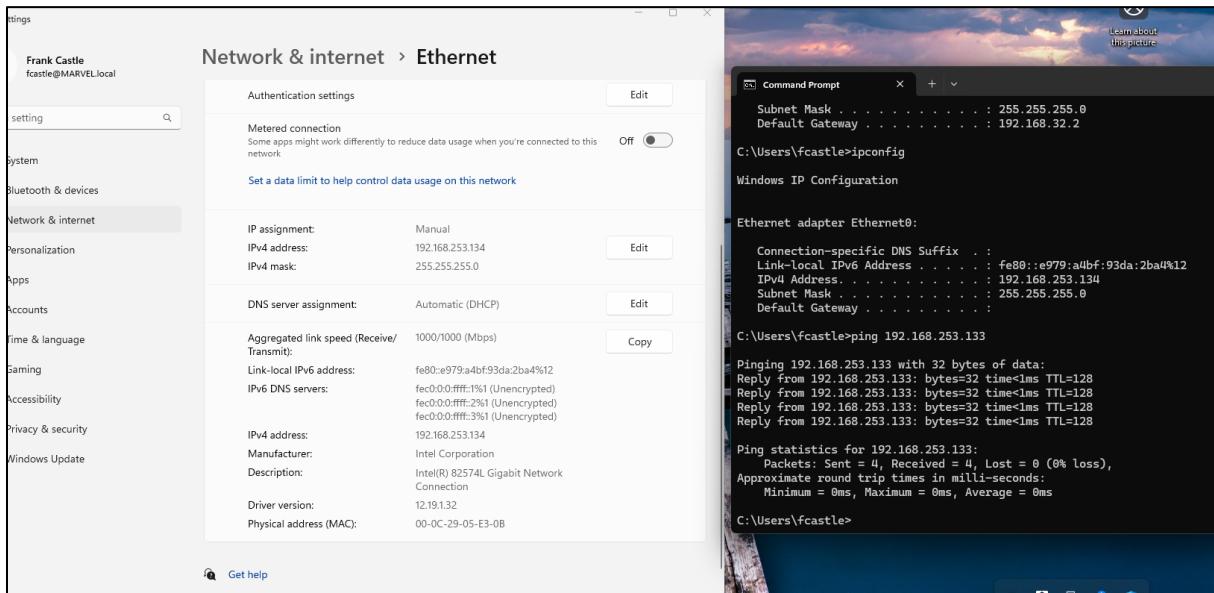
If you have the issue that the Windows Client (Windows 11) does not have the same Subnet like the Domain Controller then you need to do the following.

The screenshot shows two windows side-by-side. On the left is the 'Network & internet > Ethernet' settings page. It displays two network profiles: 'Public network (Recommended)' and 'Private network'. Below these are sections for 'Configure firewall and security settings', 'Authentication settings', 'Metered connection' (disabled), and 'IP assignment' (Automatic (DHCP)). Further down are fields for DNS server assignment, IPv4 and IPv6 addresses, and gateway information. On the right is a 'Command Prompt' window titled 'Windows [Version 10.0.26100.2314]'. It shows the output of the 'ipconfig' command, detailing the configuration for the 'Ethernet adapter Ethernet0'. The output includes the Connection-specific DNS Suffix (localdomain), Link-local IPv6 Address (fe80::e979:a4bf:93da:2ba4%12), IPv4 Address (192.168.32.128), Subnet Mask (255.255.255.0), and Default Gateway (192.168.32.2).

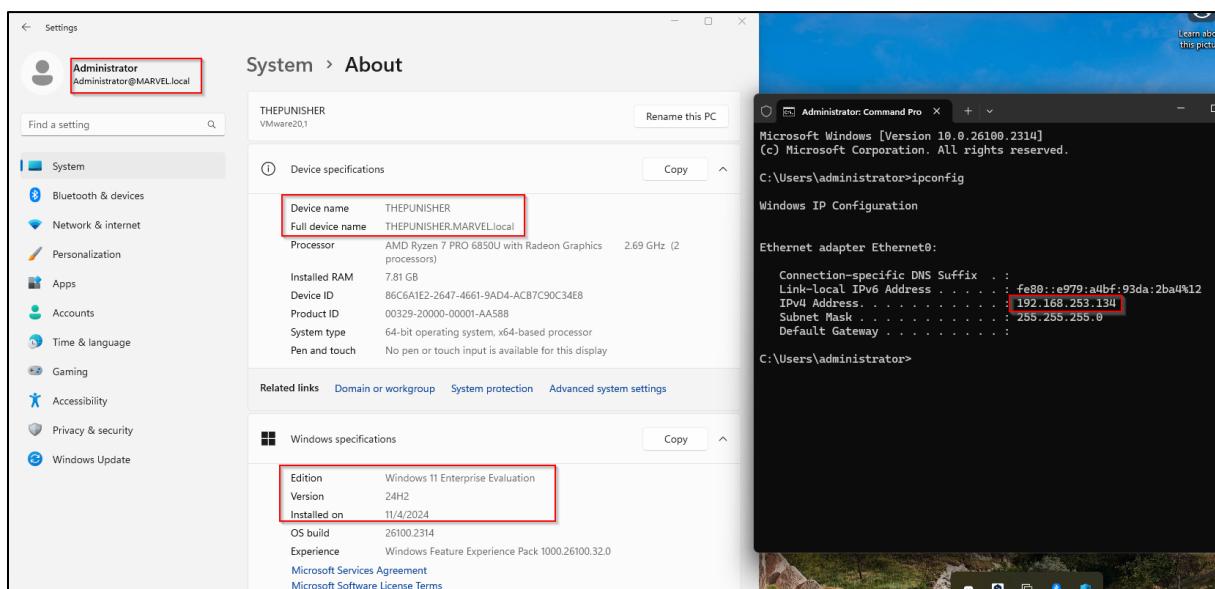
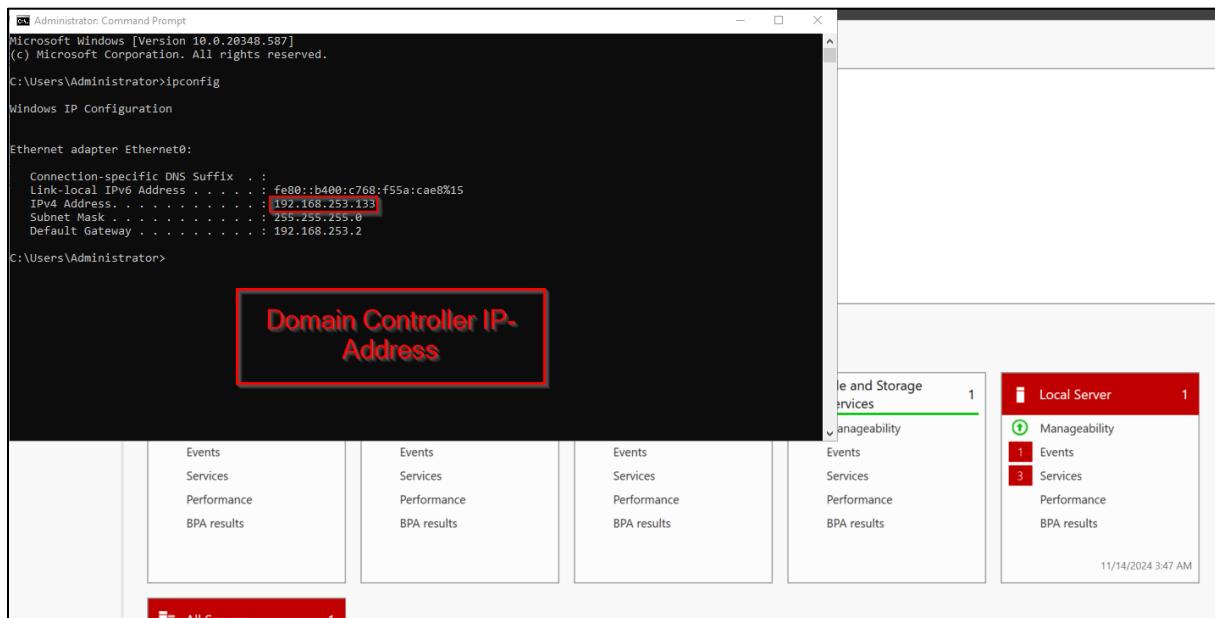
Open the Network Configuration



Change the Network settings to the settings down below in the screenshot to adapt it to the correct Network configurations.

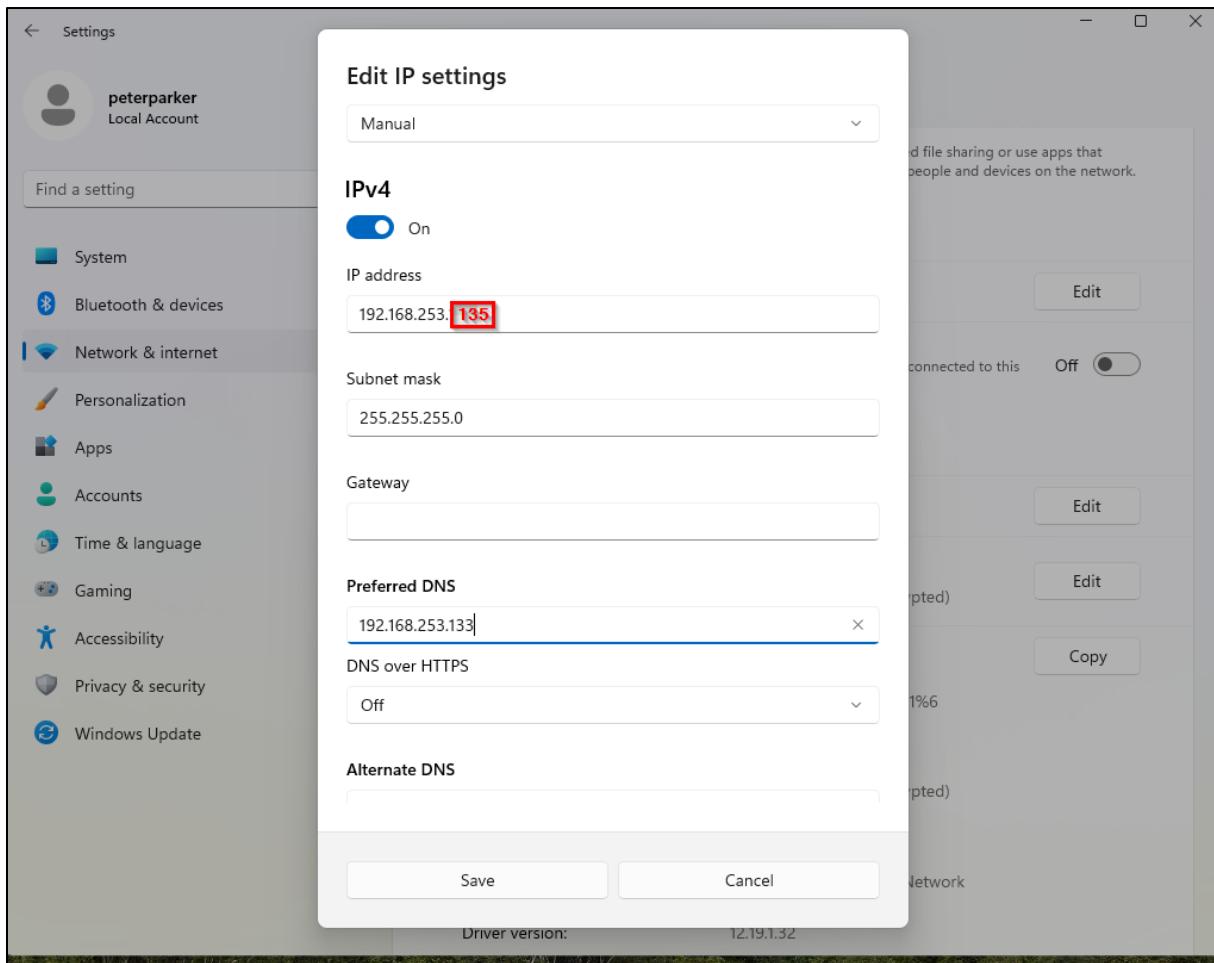


And as you can see we are in the same Subnet and Network like the Domain Controller and we can ping it as well + we are domain-joined.

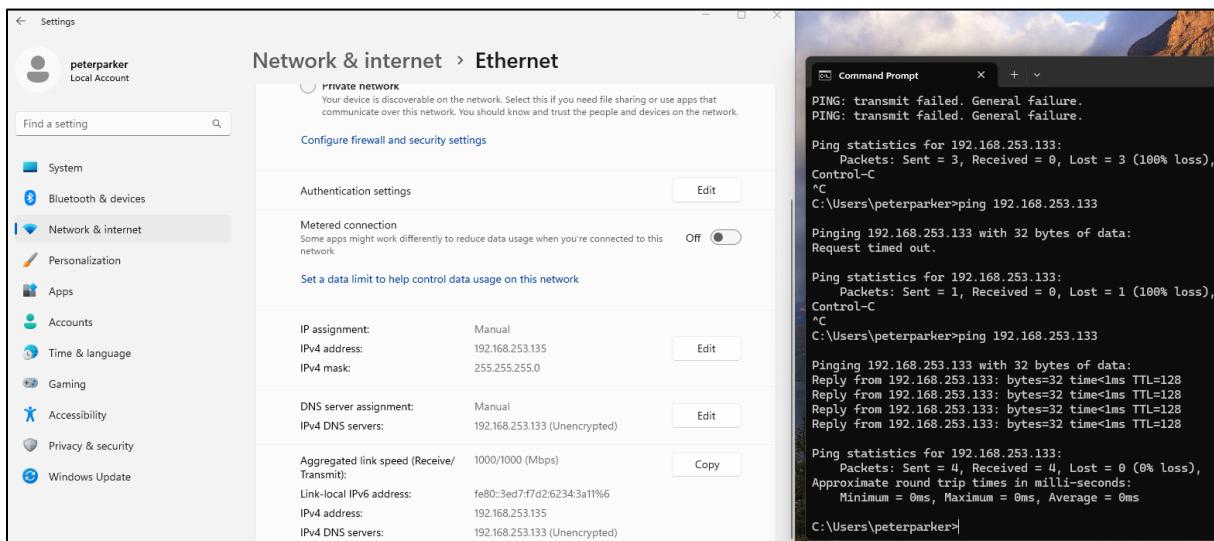


SPIDERMAN (2.nd workstation)

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

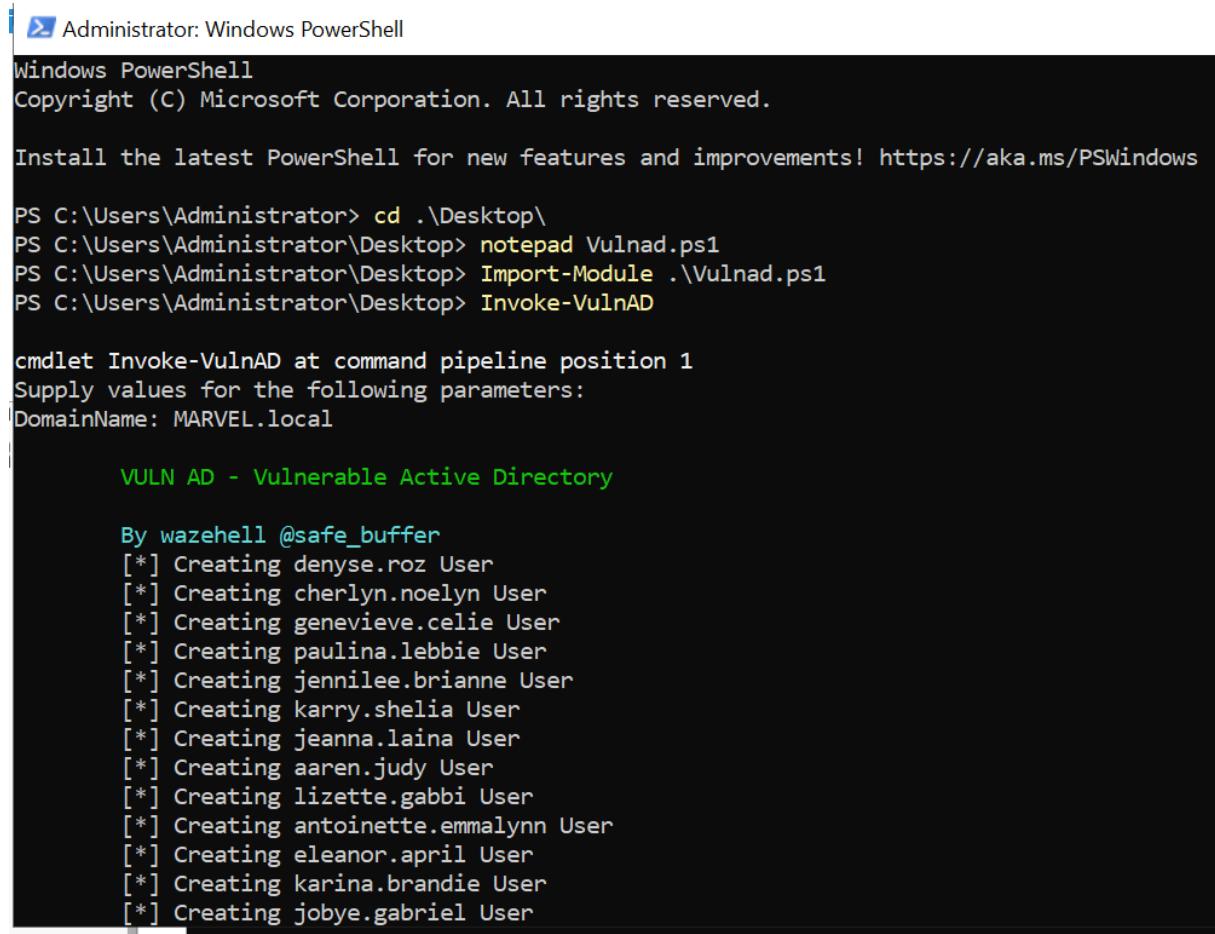
As we now have our Domain Controller and setup we want to add some Vulnerabilities, users, Misconfigurations in the ACL, Kerberoasting etc.

This is not included and must be done from your side as i wanted to make sure the File of the 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=Vk4SI3IhzM>

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.



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

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> cd .\Desktop\
PS C:\Users\Administrator\Desktop> notepad Vulnad.ps1
PS C:\Users\Administrator\Desktop> Import-Module .\Vulnad.ps1
PS C:\Users\Administrator\Desktop> Invoke-VulnAD

cmdlet Invoke-VulnAD at command pipeline position 1
Supply values for the following parameters:
DomainName: MARVEL.local

    VULN AD - Vulnerable Active Directory

    By wazehell @safe_buffer
    [*] Creating denyse.roz User
    [*] Creating cherlyn.noelyn User
    [*] Creating genevieve.celie User
    [*] Creating paulina.lebbie User
    [*] Creating jennilee.brianne User
    [*] Creating karry.shelia User
    [*] Creating jeanna.laina User
    [*] Creating aaren.judy User
    [*] Creating lizette.gabbi User
    [*] Creating antoinette.emmalynn User
    [*] Creating eleanor.april User
    [*] Creating karina.brandie User
    [*] Creating jobye.gabriel User
```

When you see this then the Creation is sucessful.

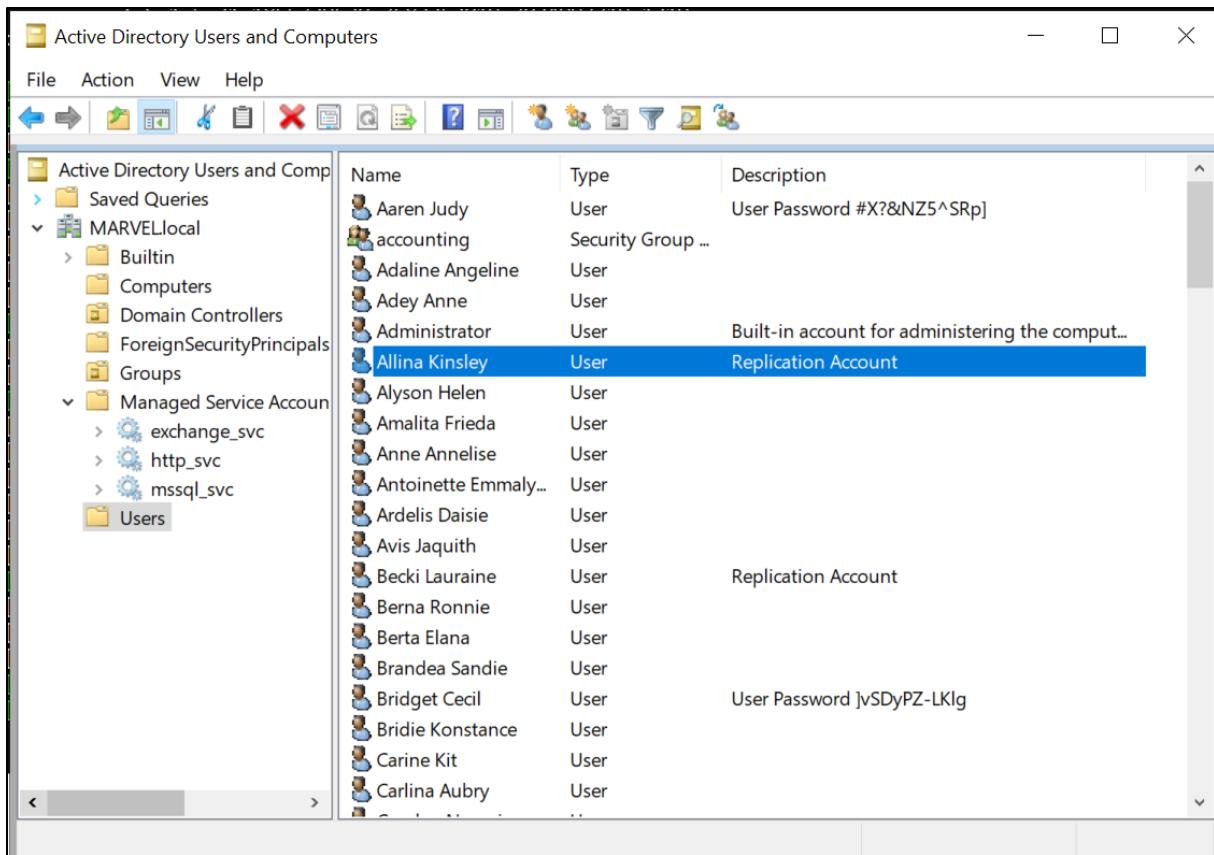
 Administrator: Windows PowerShell

```
[*] 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
```

```
i [+] Administrator: Windows PowerShell
SID : S-1-5-21-1855329520-3682252019-3024997319-1219
UserPrincipalName :

[+] Kerberoasting Done
[+] AS-REPRoasting Done
[*] DnsAdmins Nested Group : Senior management
[+] DnsAdmins Done
[*] Password in Description : aaren.judy
[*] Password in Description : roxy.camellia
[*] Password in Description : cherlyn.noelyn
[*] Password in Description : bridget.cecil
[*] Password in Description : sunny.rosamond
[+] Password In Object Description Done
[*] Default Password : merrily.billie
[*] Default Password : nelie.henrie
[+] Default Password Done
[*] Same Password (Password Spraying) : micky.jessa
[*] Same Password (Password Spraying) : chelsae.franni
[*] Same Password (Password Spraying) : shawna.bonni
[*] Same Password (Password Spraying) : ianthe.charyl
[*] Same Password (Password Spraying) : margarita.kev
[*] Same Password (Password Spraying) : eleanor.april
[+] Password Spraying Done
[*] Giving DCSync to : gerianne.morena
[*] Giving DCSync to : becki.lauraine
[*] Giving DCSync to : allina.kinsley
[+] DCSync Done
[+] SMB Signing Disabled
```

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



The screenshot shows the Windows Active Directory Users and Computers management console. The left pane displays a tree view of the directory structure under 'MARVELlocal'. The right pane is a grid view of users, showing columns for Name, Type, and Description. A specific user, 'Allina Kinsley', is selected and highlighted with a blue background. The 'Description' column for this user contains the text 'Replication Account'.

Name	Type	Description
Aaren Judy	User	User Password #X?&NZ5^SRp]
accounting	Security Group ...	
Adaline Angeline	User	
Adey Anne	User	
Administrator	User	Built-in account for administering the comput...
Allina Kinsley	User	Replication Account
Alyson Helen	User	
Amalita Frieda	User	
Anne Annelise	User	
Antoinette Emmaly...	User	
Ardelis Daisie	User	
Avis Jaquith	User	
Becki Lauraine	User	Replication Account
Berna Ronnie	User	
Berta Elana	User	
Brandea Sandie	User	
Bridget Cecil	User	User Password JvSDyPZ-LKlg
Bridie Konstance	User	
Carine Kit	User	
Carlina Aubry	User	
..		

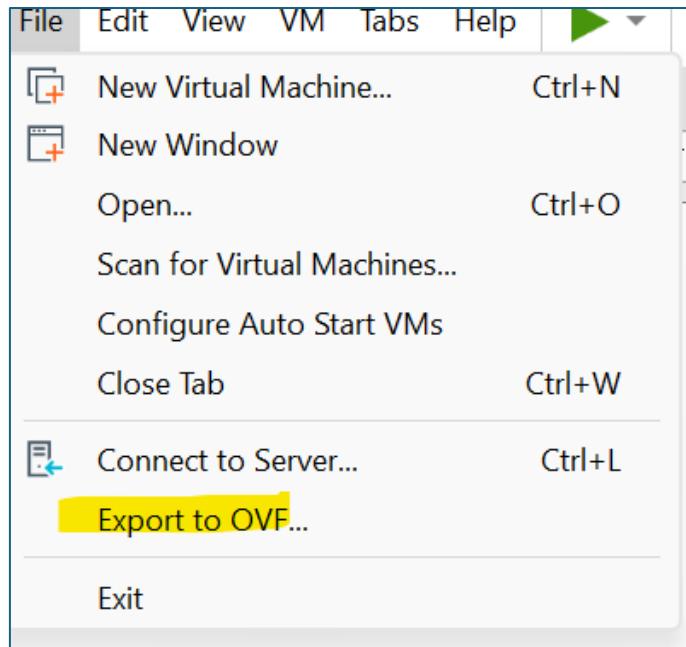
Export Functions for the Virtual Machines

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

Windows Server 2022 (EXPORT)

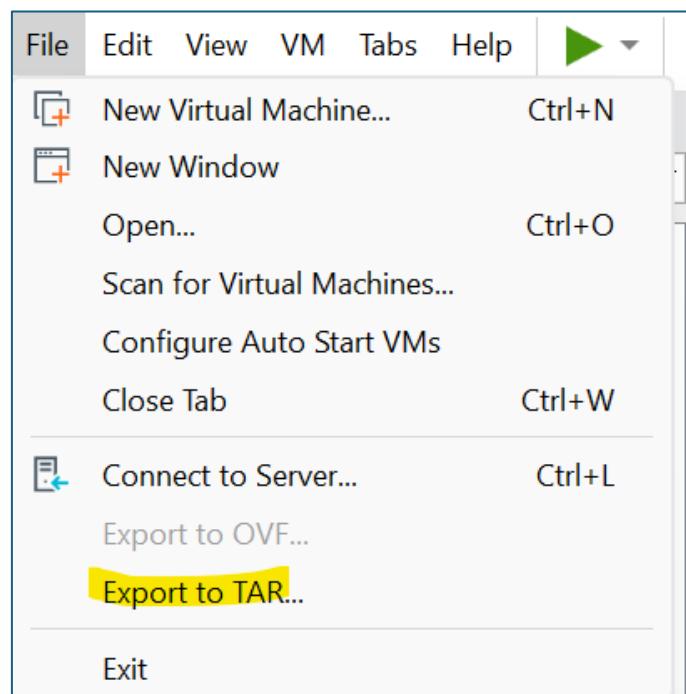
For that we will export the Domain Controller Windows Server 2022 first. For that we need to

- 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 Snapshots 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.

