2019 DC

[ALL NAT]
Detected as windows server 2016 -> its okay
Version -> Windows server 2016 Standard
OS to install -> Windows Server 2019 Standard Evaluation (Desktop Experience)
After Install
-> Install VMWare Tools
Restart Later

Type computer -> View PC Name -> Rename PC -> HYDRA-DC
Restart

Manage -> Add Roles and Features
Next -> Role-based or Feature Based -> Next -> Next -> Active Directory Domain Services -> Add Features -> Next
All Defaults -> Install

Yellow Alert Flag -> Click on It
Promote this server to domain controller -> Add a new Forest -> MARVEL.local -> Next
DSRM Password -> give it a password
All defaults -> Next
Install and it reboots machines

Login [MARVEL\Administrator]

/////DC Setup compete

-----> Setup Client Machine [Any no of machines]
Windows 10 Enterprise

When Sign in with microsoft pops up -> Domain Join Instead
Frank Castle
> Install VMWare Tools
Restart Later

Type computer -> View PC Name -> Rename PC -> THEPUNISHER
Restart

-----> Setup users, and policies
Hydra-DC

Tools -> Active Directory Users and Computers
Expand Marvel.local
WE see a few OUs
We see a lot of groups in Users
Right click on Marvel.local and create a new OU named groups
In Users -> click, scroll and select all groups and send them over to groups so that we have a clean user section

Right click -> New User
Frank Castle
fcastle

Next -> Same password as before -> Password never expires -> Finish

*Create another user
Right click on Adminsitrator -> Copy
Tony Stark
tstark

Give a password -> Password never expires -> Finish

*Right click on Frank Castle -> Copy
Peter Parker
pparker

Give a password -> Password never expires -> Finish

*create a service account [NOT Needed]
Creating it as a domain Administrator -> Never do this [Service accounts as domain administrator]

Right Click on Tony Stark -> Copy
SQL Service
SQLService

Give a password -> Password never expires -> Finish

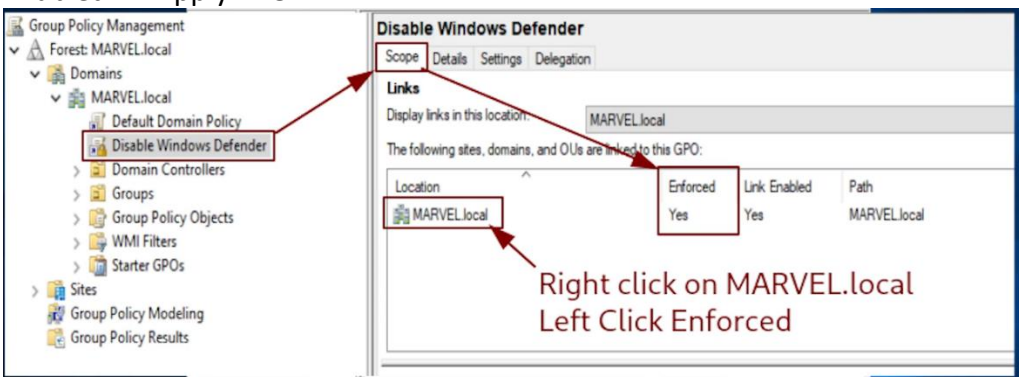
-----> Creating a File Share
In Server manager -> Click on File and Storage Services -> Shares
Click on Tasks -> New Share
Defaults -> Next -> hackme
All Defaults -> create and close

Create an SPN [NOT Needed]
open cmd as admin
setspn -a HYDRA-DC/SQLService.MARVEL.local:60234 MARVEL\SQLService
{You can pick any port}

Making sure it is set
setspn -T MARVEL.local -Q */*

Open Group Policy Management [Run as Admin]
Right click on Marvel.local -> Create a GPO -> Name: Disable Windows Defender

Right click this policy and edit
Computer Configuration -> Policies -> Admin Temp -> Windows Components
Browse to Windows Defender Antivirus
Click on "Turn off Windows Defender Antivirus"
Enabled -> Apply -> OK



***

Joining Machines to our Domain

On Frank Castle Machine
Goto C drive
Right Click -> New Folder -> Share -> Right click -> properties -> Sharing -> Share

Get IP from DC

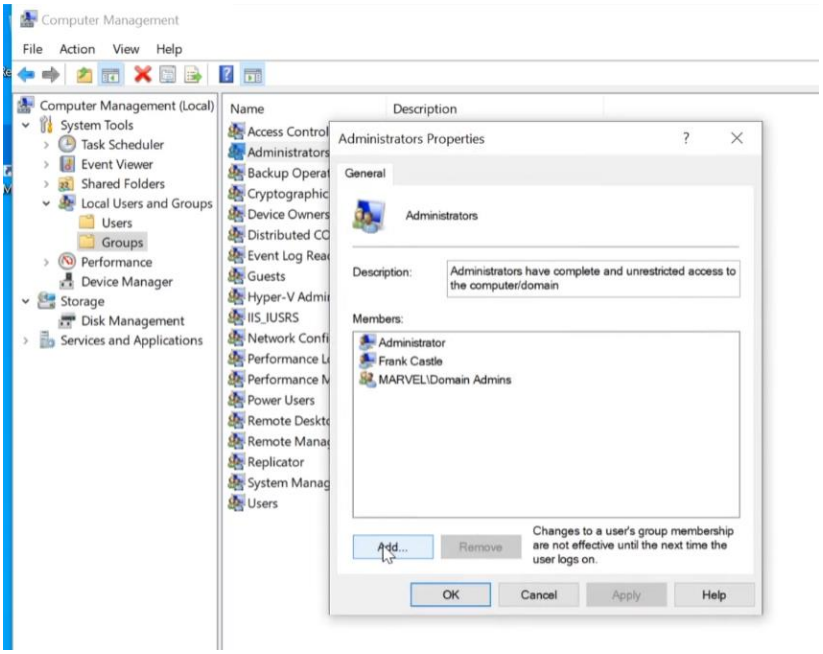
Change Adapter options -> Change DNS to DC IP

search domain -> Access work or school -> connect
At bottom -> Join this device to a local Active Directory domain
Type Domain Name -> MARVEL.local
User: Adminsitrator
Pass:
SKIP the next prompt
Restart Now

Select Other User [We are logging as fcastle]
fcastle
pass:
Login

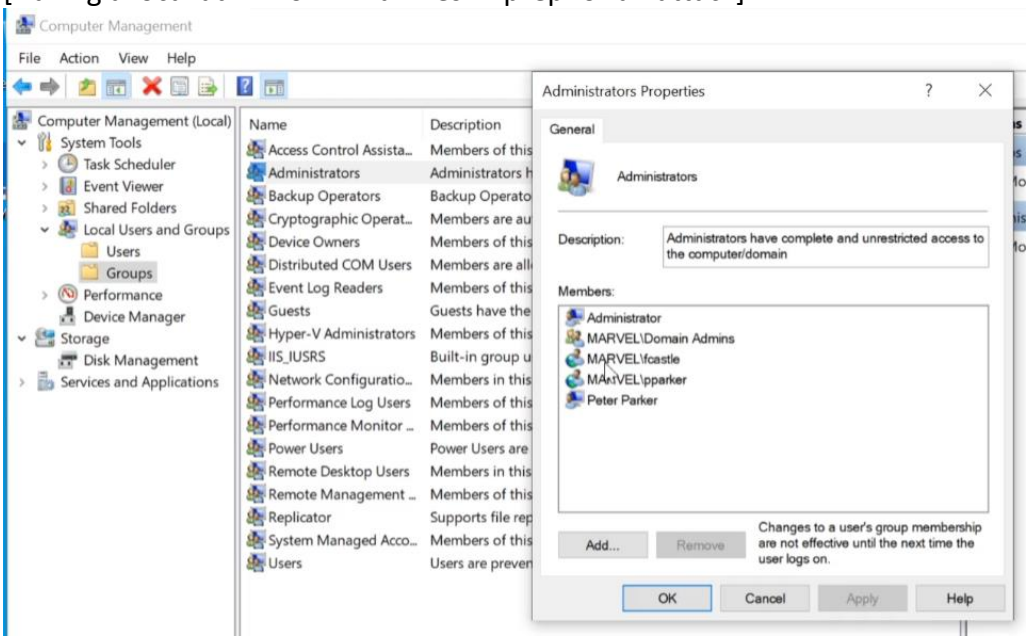
Sign out now and sign in as admin
Select other user
marvel\administrator
pass:
login

Lets enable frank castle to be local admin
search -> computer management
local users and groups
groups
double click Admin



Add -> fcastle -> check names -> apply -> ok

[Repeat same proces on other machine]
Now lets, add both frank castle and peter parker as admins on spiderman
[Having a local admin on 2 mahines -> prep for an attack]



Goto DC:
In active directory users and computers, both machines showed up in computers OU.