Cyber Report: The Chicago Outfit

1. Each assignment has a goal. What is the assignment and how will you find the solution?

The purpose of this lab is to create seven unique users, assigning each into specific groups based on the provided table below. The three groups created are Executive, Staff and IT. One user (MichaelR) will be assigned two groups, IT and Domain Admin. Finally, a shared folder system will be created for internal file sharing purposes.

Users and Credentials

User	Group	Password
JamesM	Executive	ChicagoOutfit!
MichaelS	Executive	ChicagoOutfit!
LouisM	Executive	ChicagoOutfit!

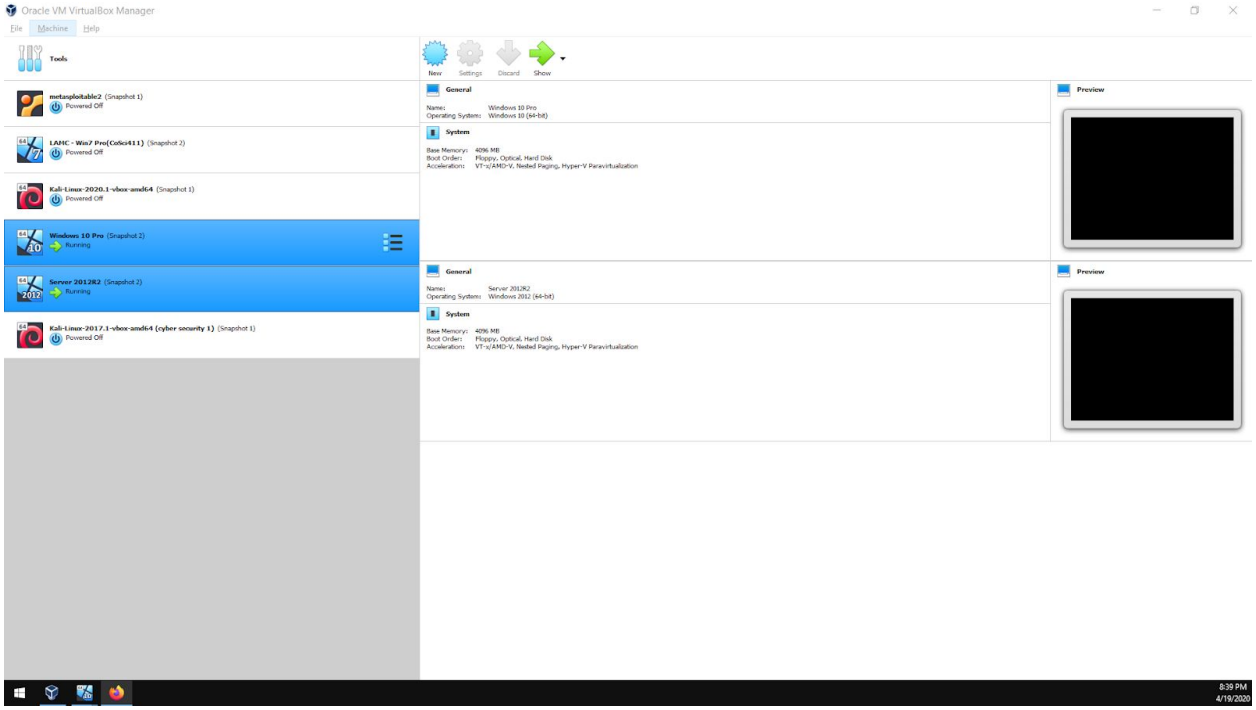
User	Group	Password
RobertS	Staff	ChicagoOutfit!
NicholasF	Staff	ChicagoOutfit!
MichaelT	Staff	ChicagoOutfit!

User	Group	Password
Michael R	IT and Domain admin	ChicagoOutfit!

User, group, and passwords for each user in the lab.

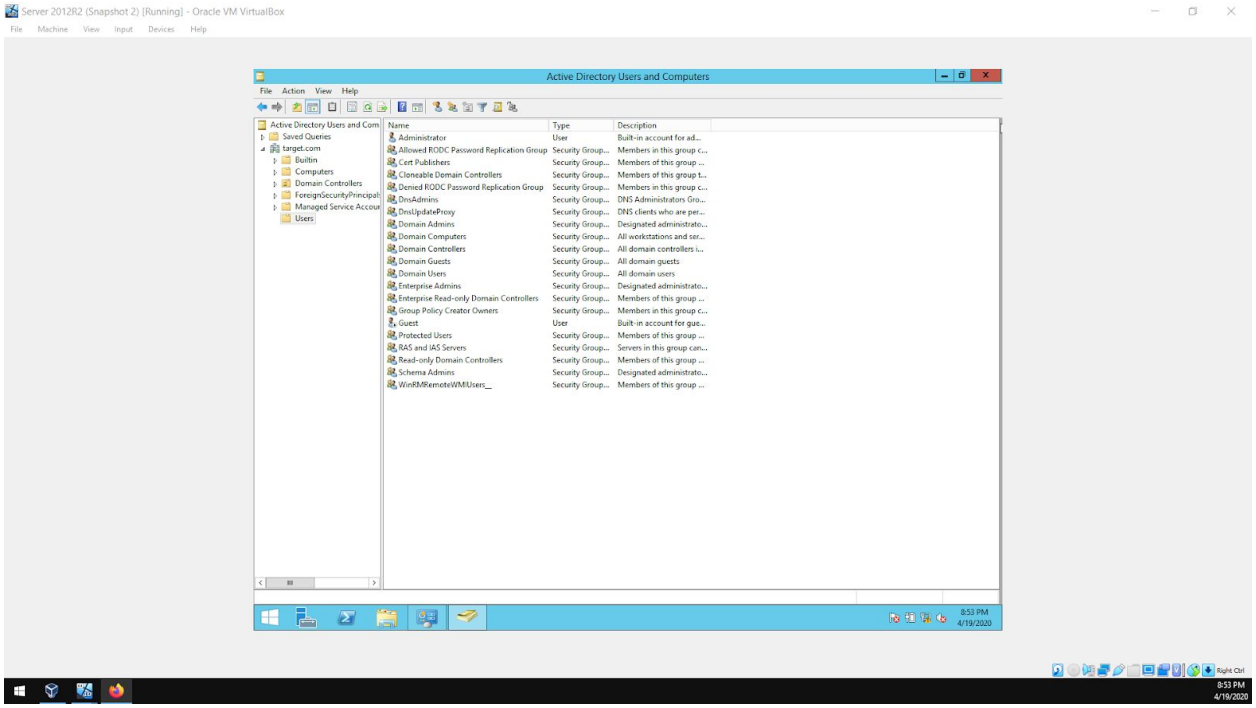
2. Demonstration of the steps taken with screenshots (snipping tool) from your computer. You need to show the steps you took as you took them.

Virtual Box - Main menu



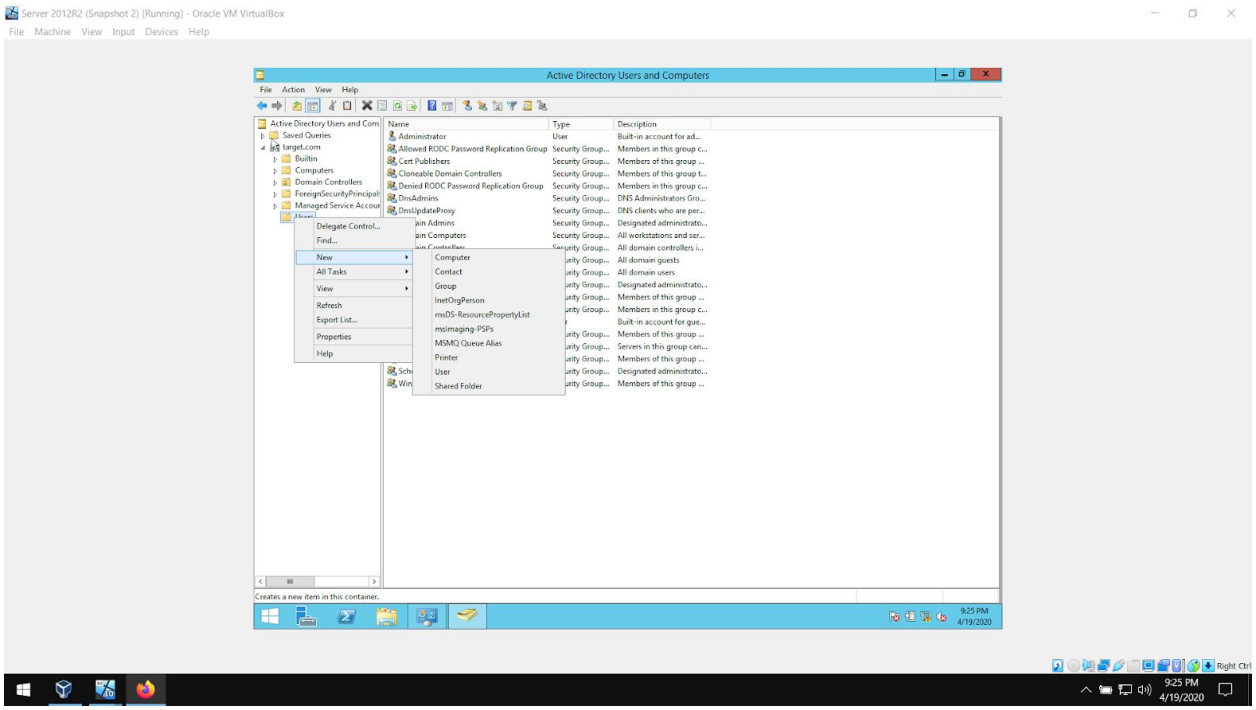
The lab will work within the Windows 10 Professional and Server 2012R2 environments. The Server 2012R2 Administrator password had expired. A new one was recorded. (Passw0rd!)

Active Directory Users and Computers



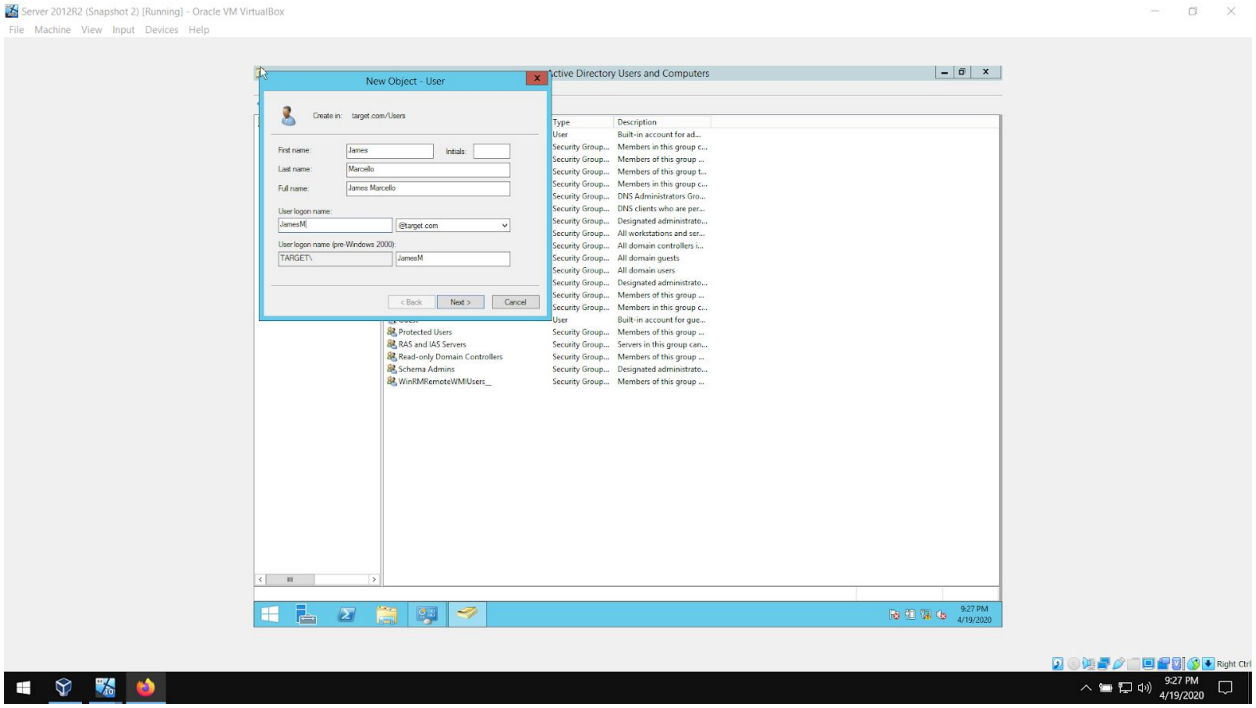
A total of six users will be created in Active Directory Users and Computers on the Server 2012R2 VM.

New Object - User



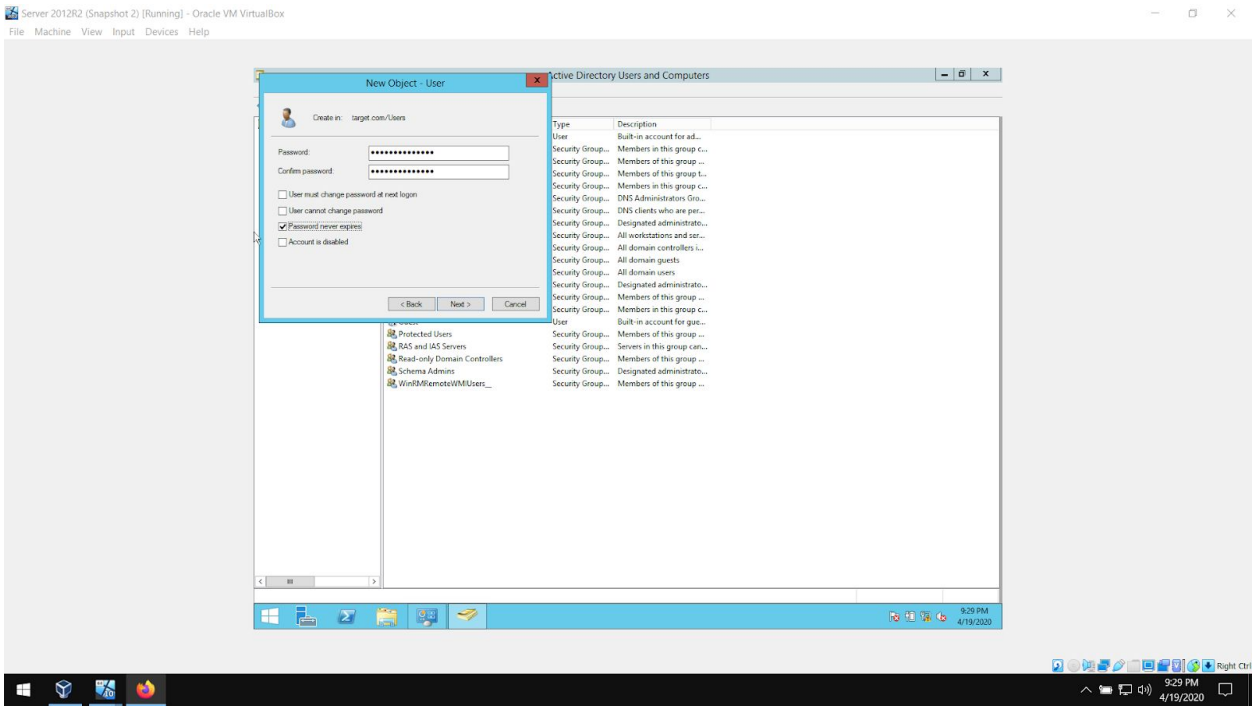
Right click on Users and then choose New → User.

New Object - User



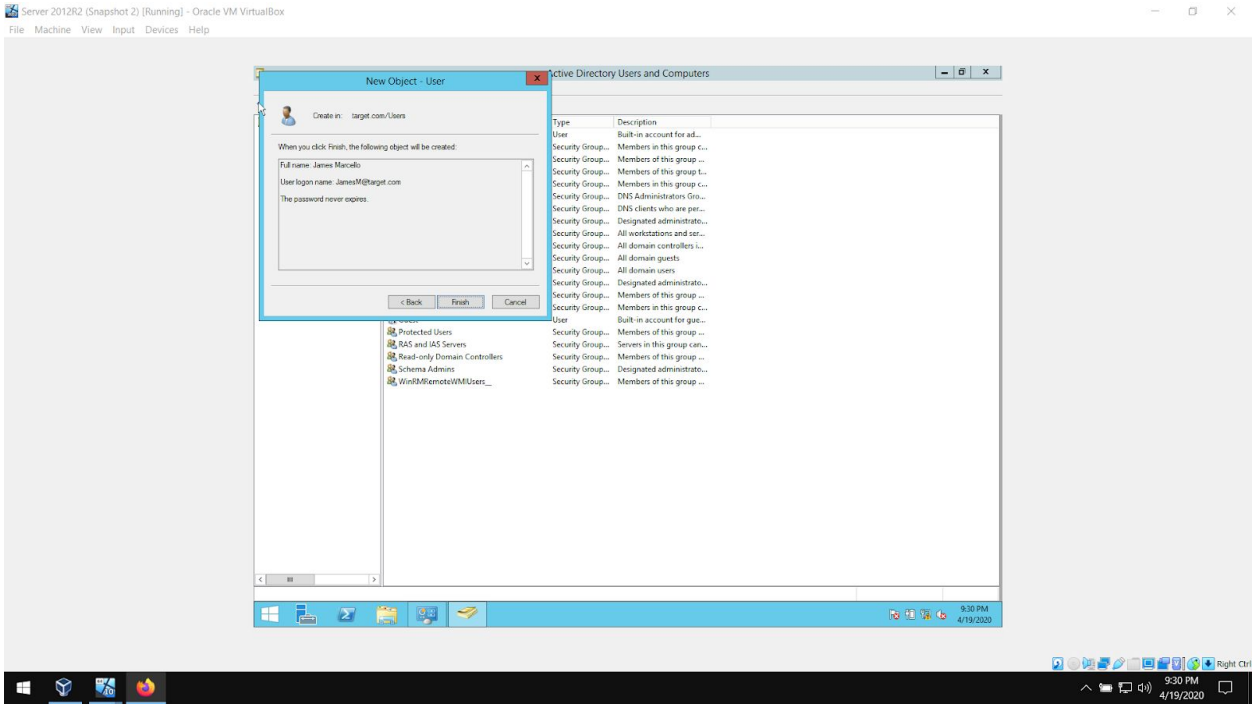
The first user will be James M.

New Object - User



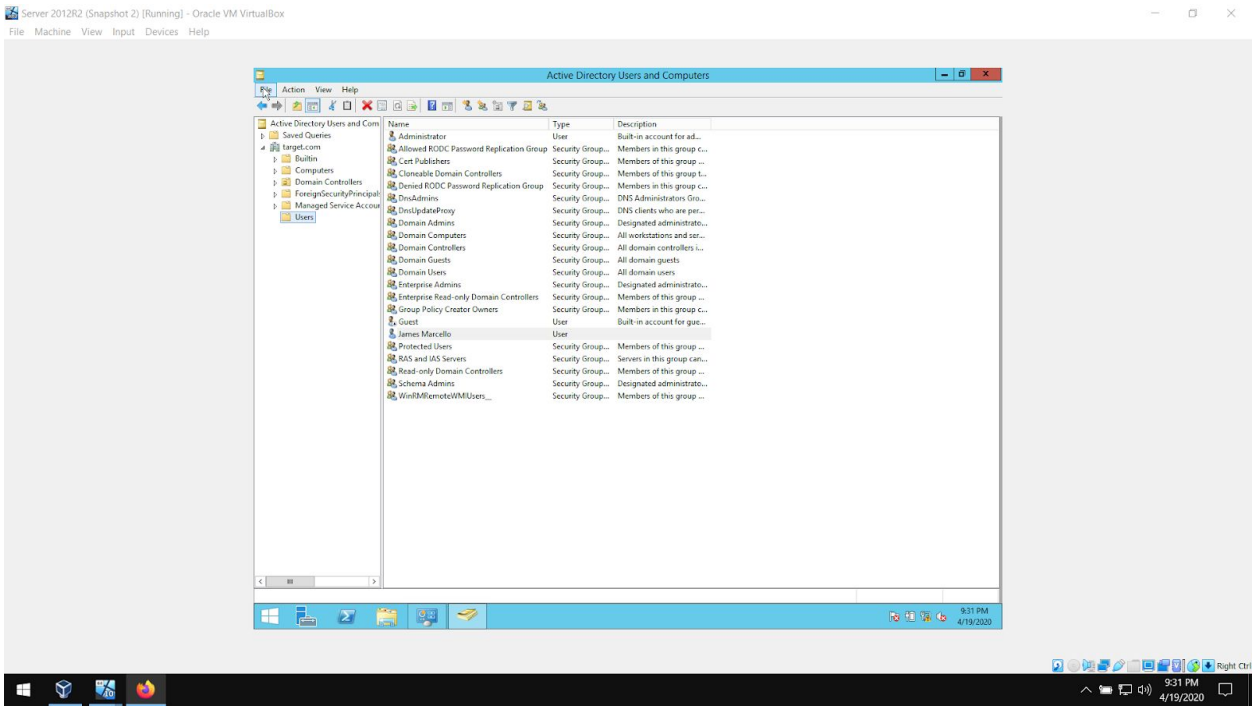
The password is set. Unchecked reset password at logon and checked Password never expires.

New Object - User



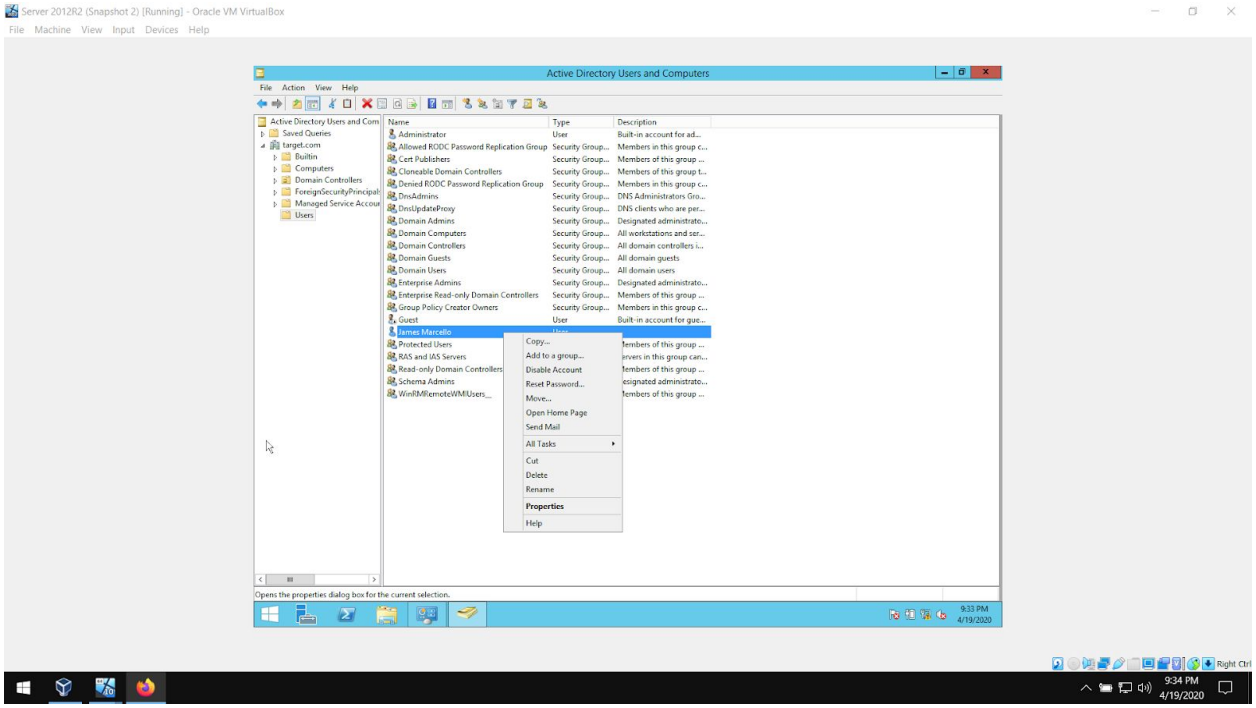
Confirmation of the new user information.

Active Directory User and Computers



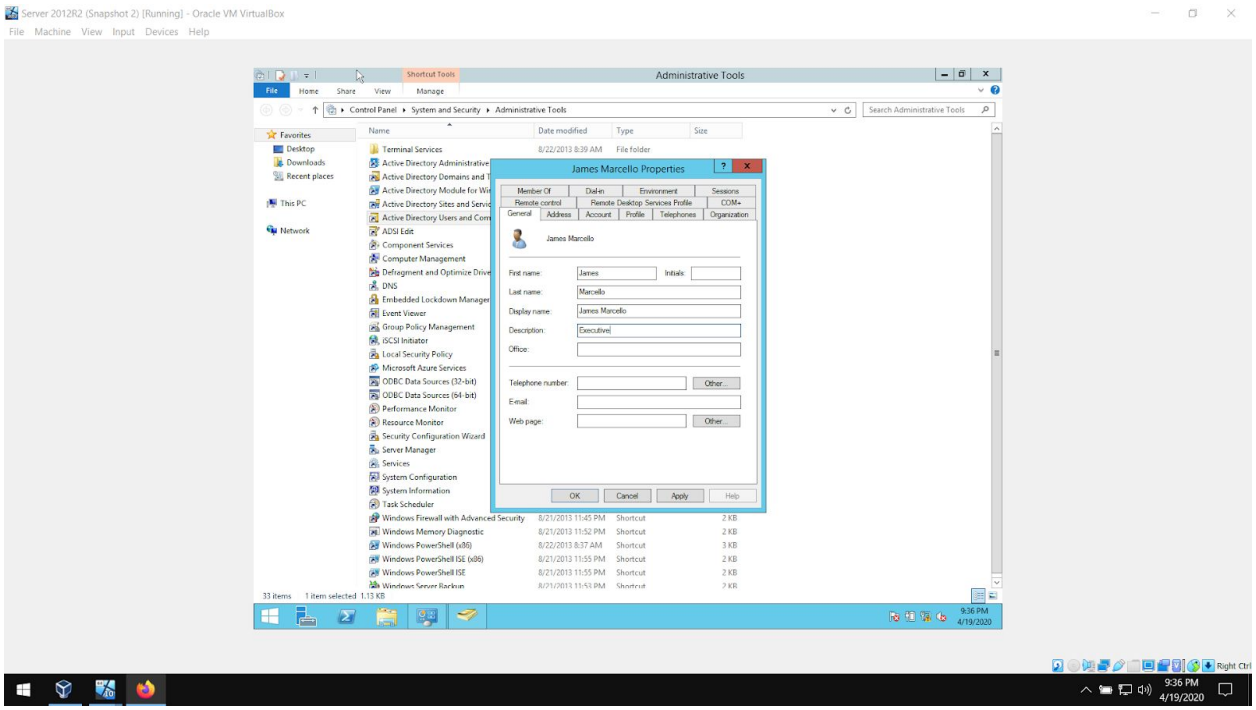
The new user James Marcello is made.

Active Directory Users and Computers



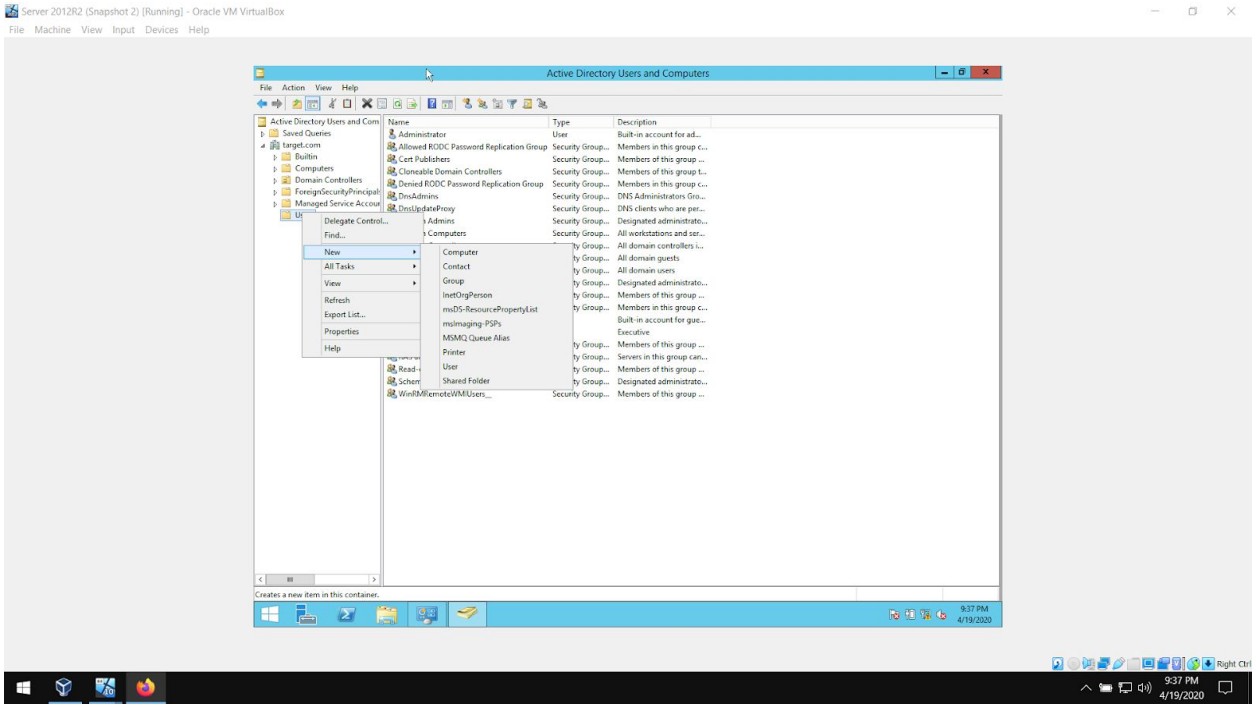
The description of the new user can be set by right clicking on the user and then selecting Properties.

James Marcello Properties



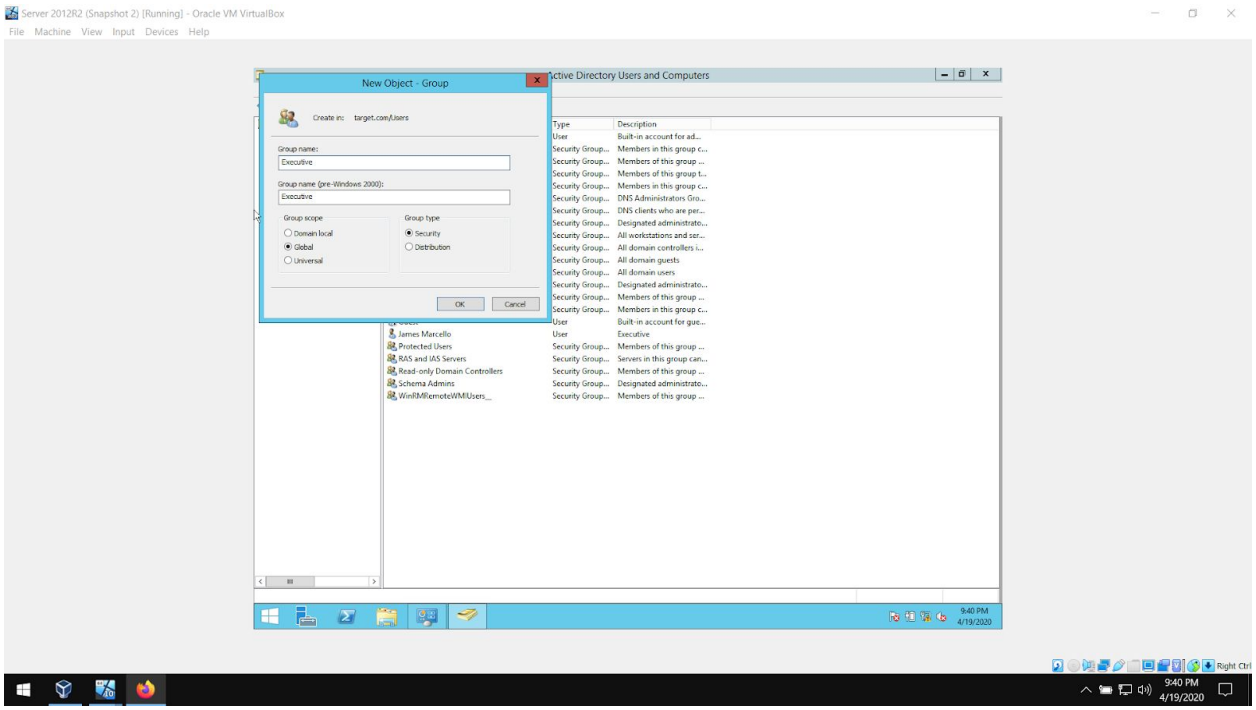
The Description is updated with what role the user will have in the organization.

Active Directory Users and Computers



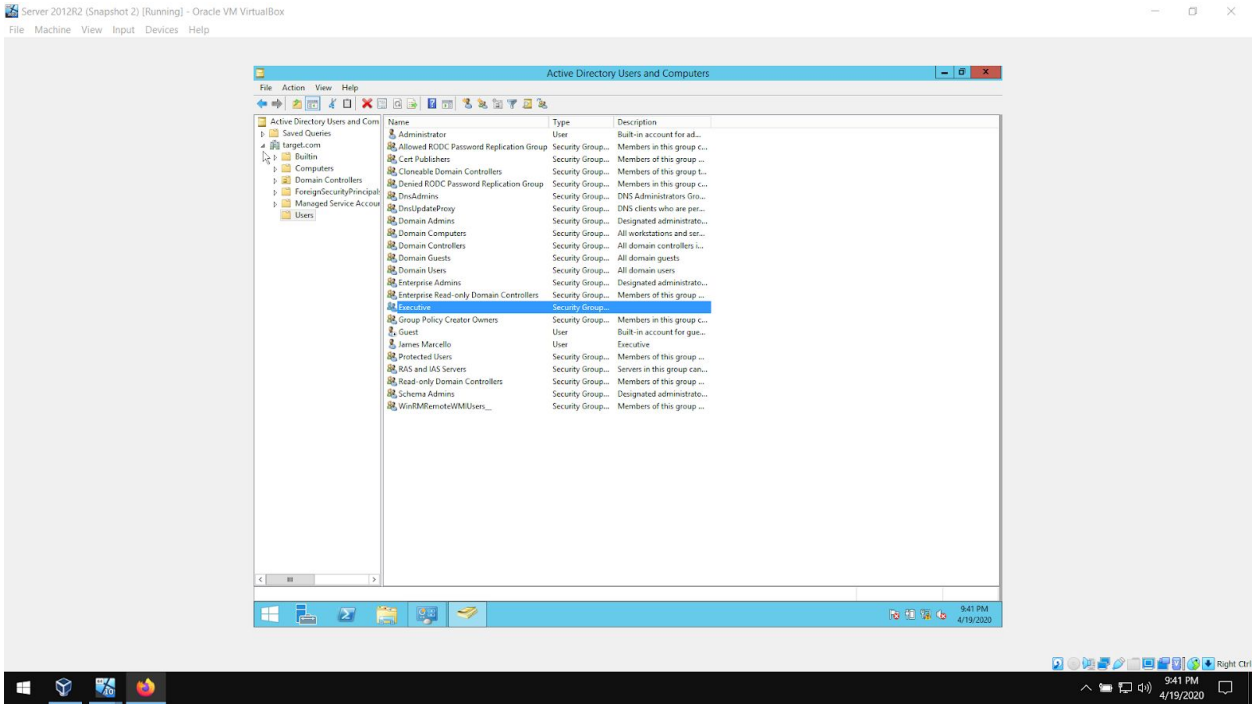
Next the Exec group needs to be created. Right click on Users → New → Group.New Object - Group.

New Object - Group



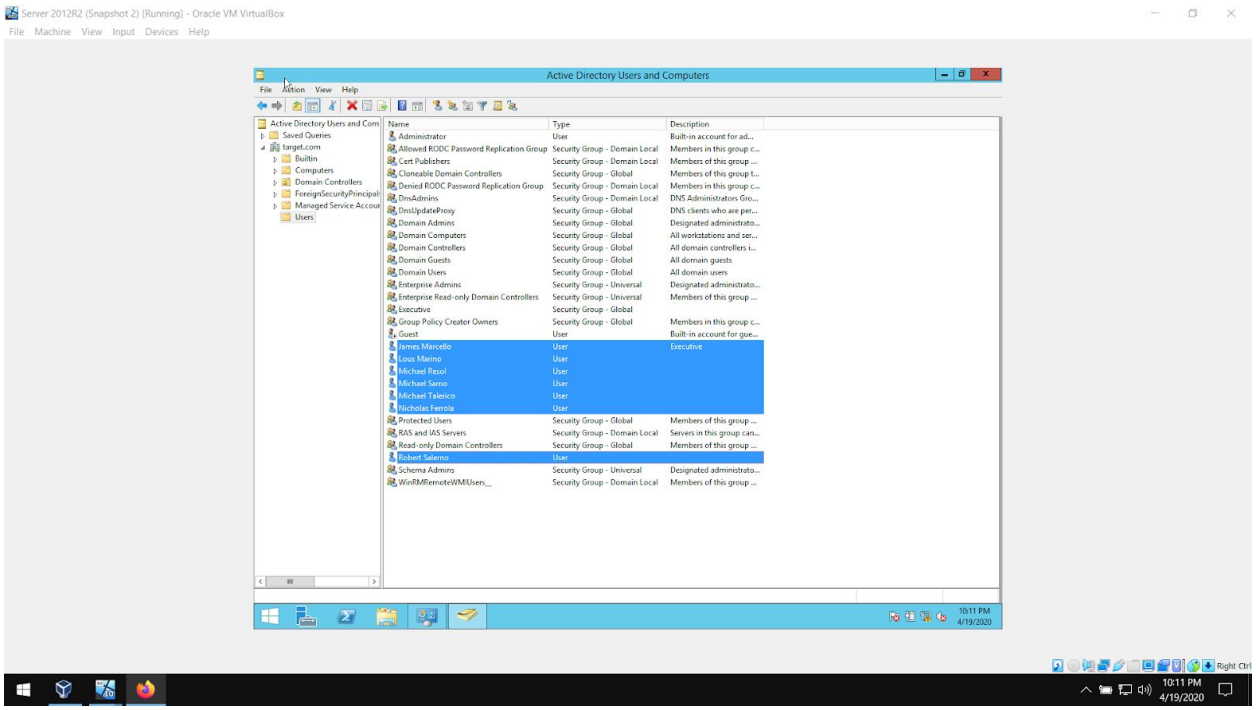
Group Executive creation.

Active Directory Users and Computers



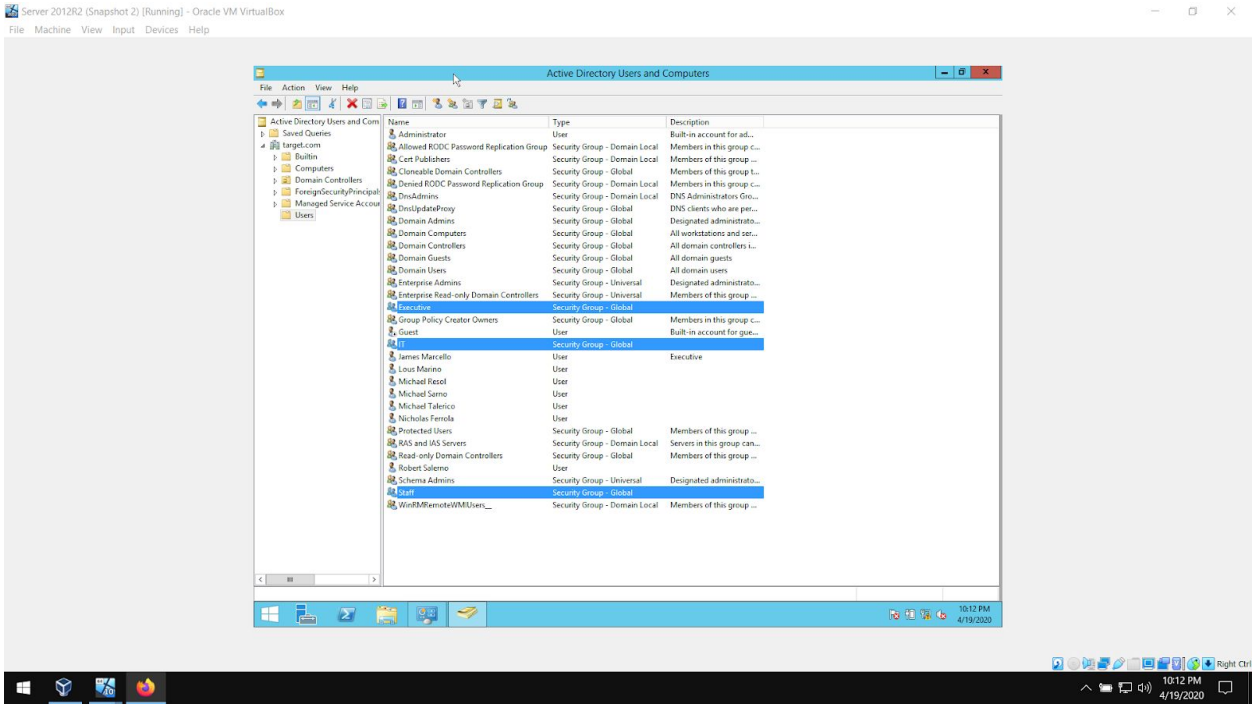
The Executive group has been created.

Active Directory Users and Computers



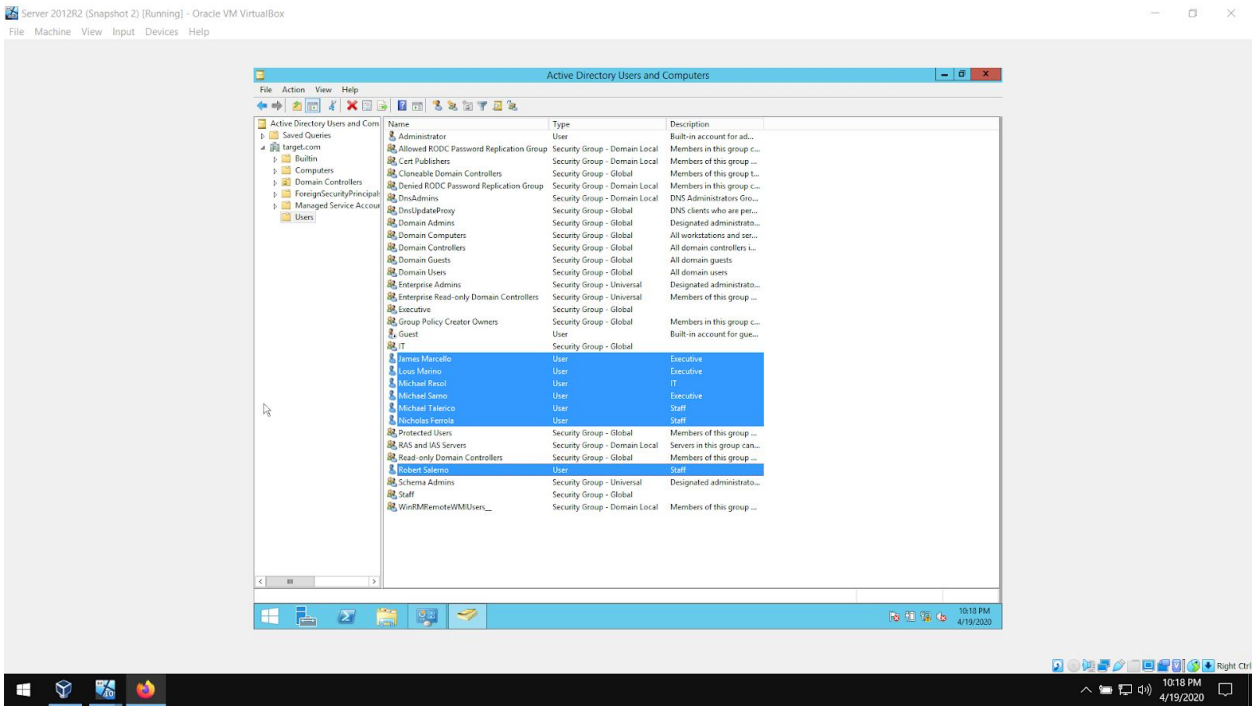
The other users were made but have not been added to any group yet.

Active Directory Users and Computers



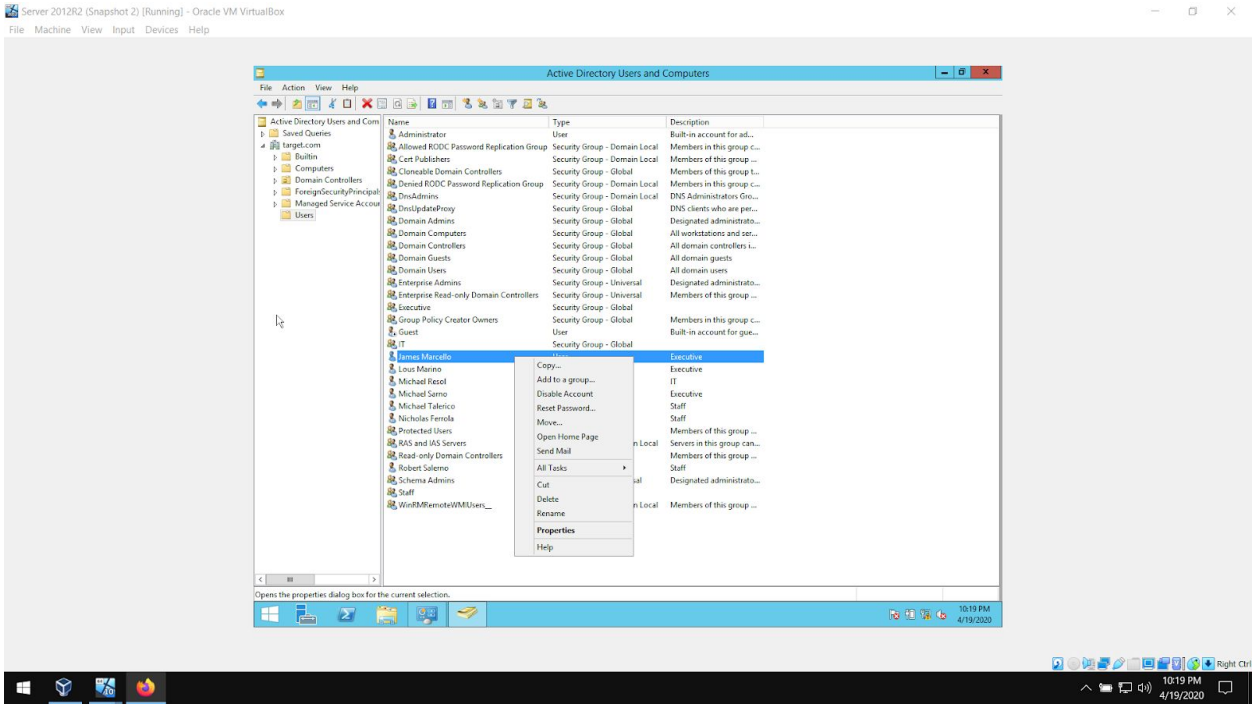
Now the other two groups were made, Staff and IT.

Active Directory Users and Computers



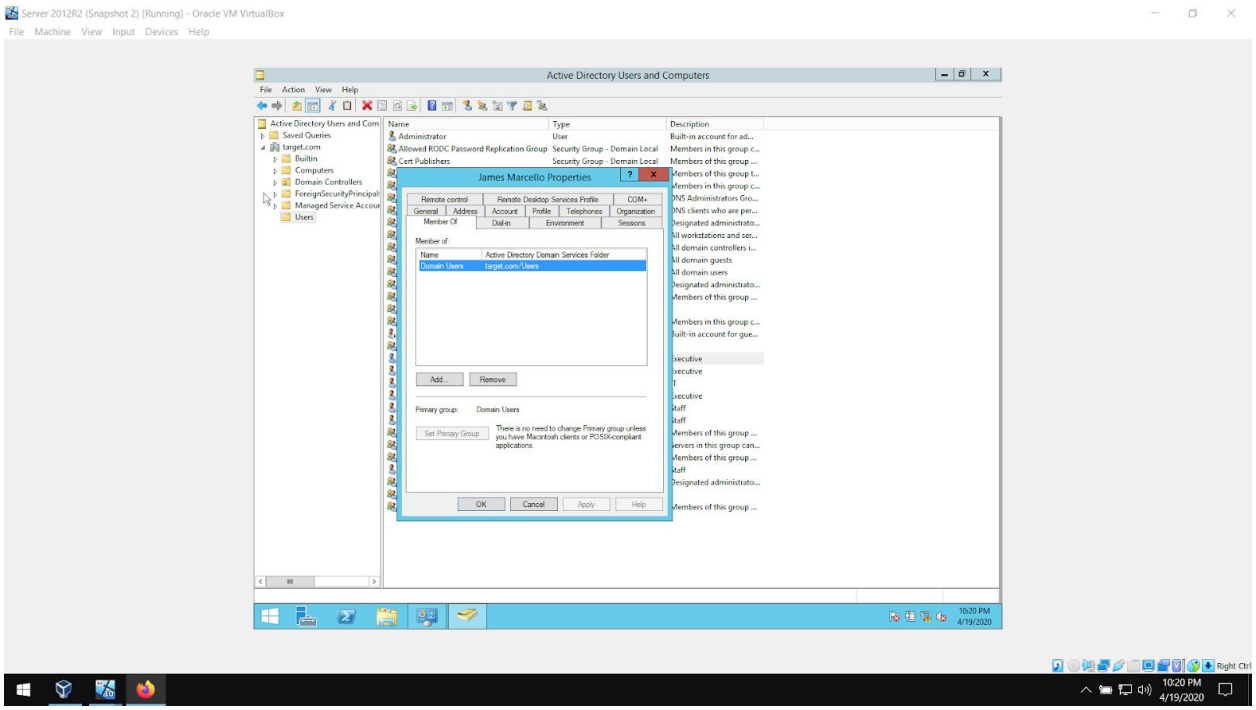
User descriptions were updated by right clicking on the user then selecting Properties.

Active Directory Users and Computers



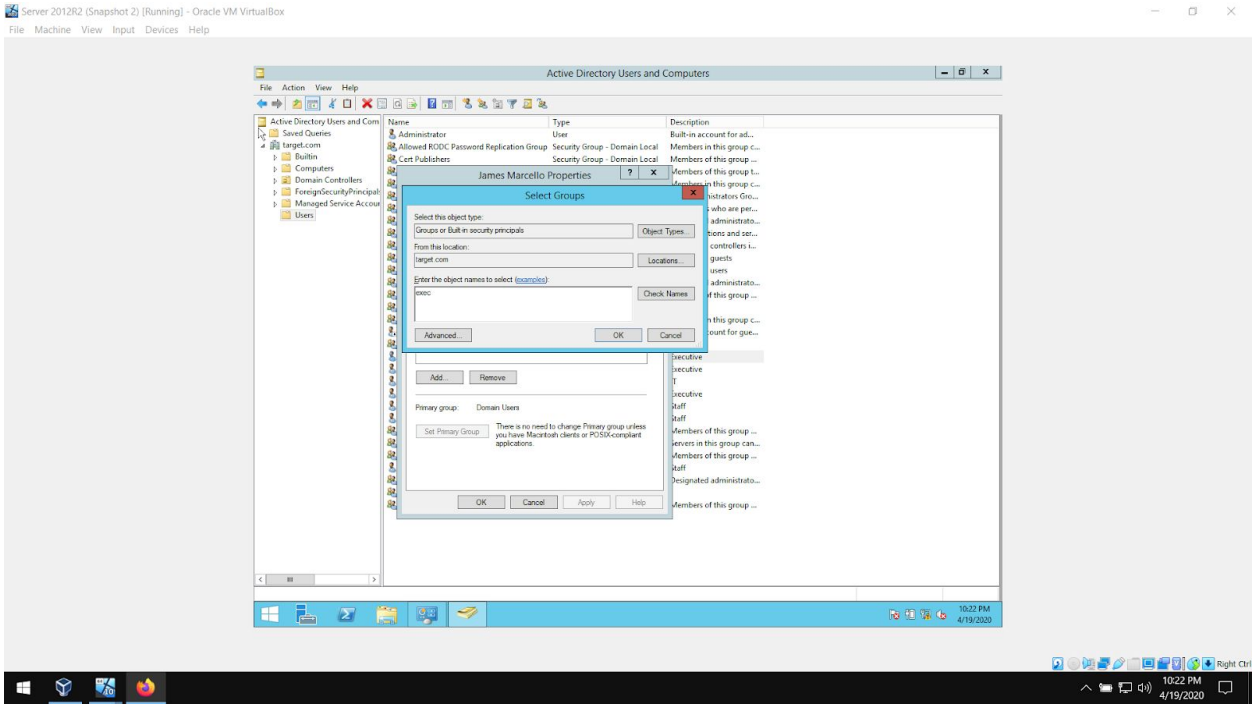
Now the Memberships of each user must be defined. Right click on the user and then select Properties.

James Marcello Properties



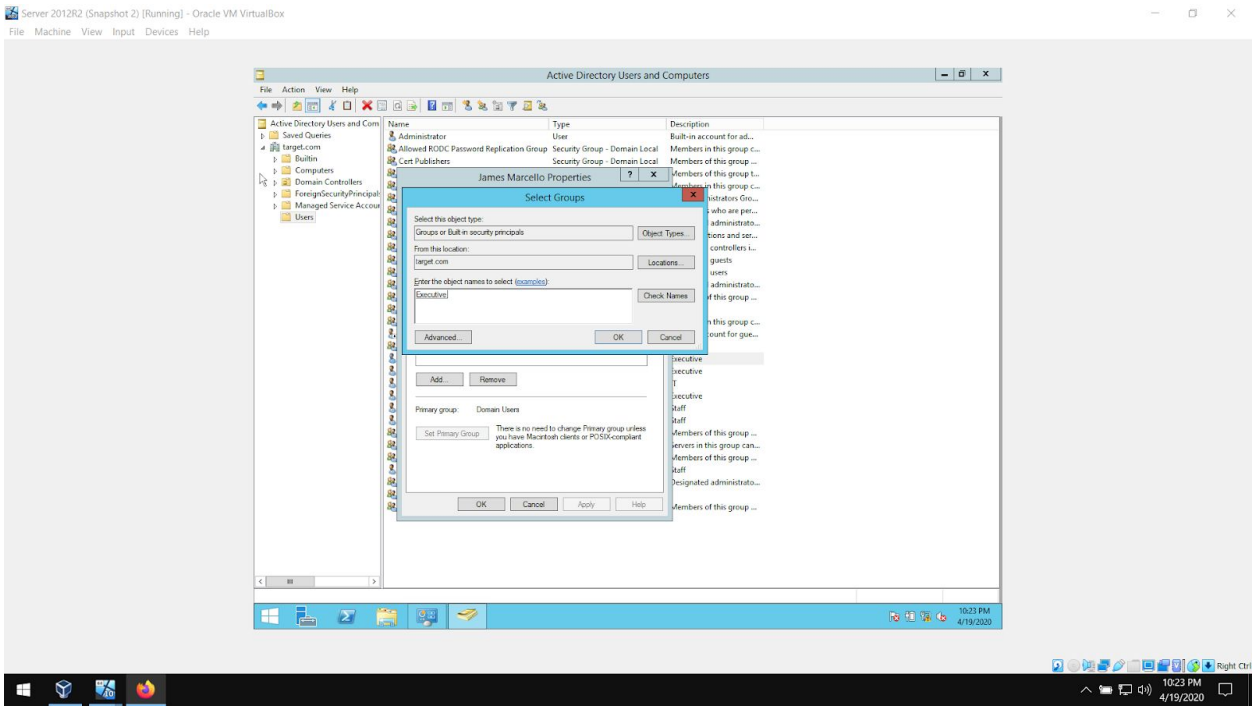
Selecting the Member Of tab and then selecting Add.

Select Groups



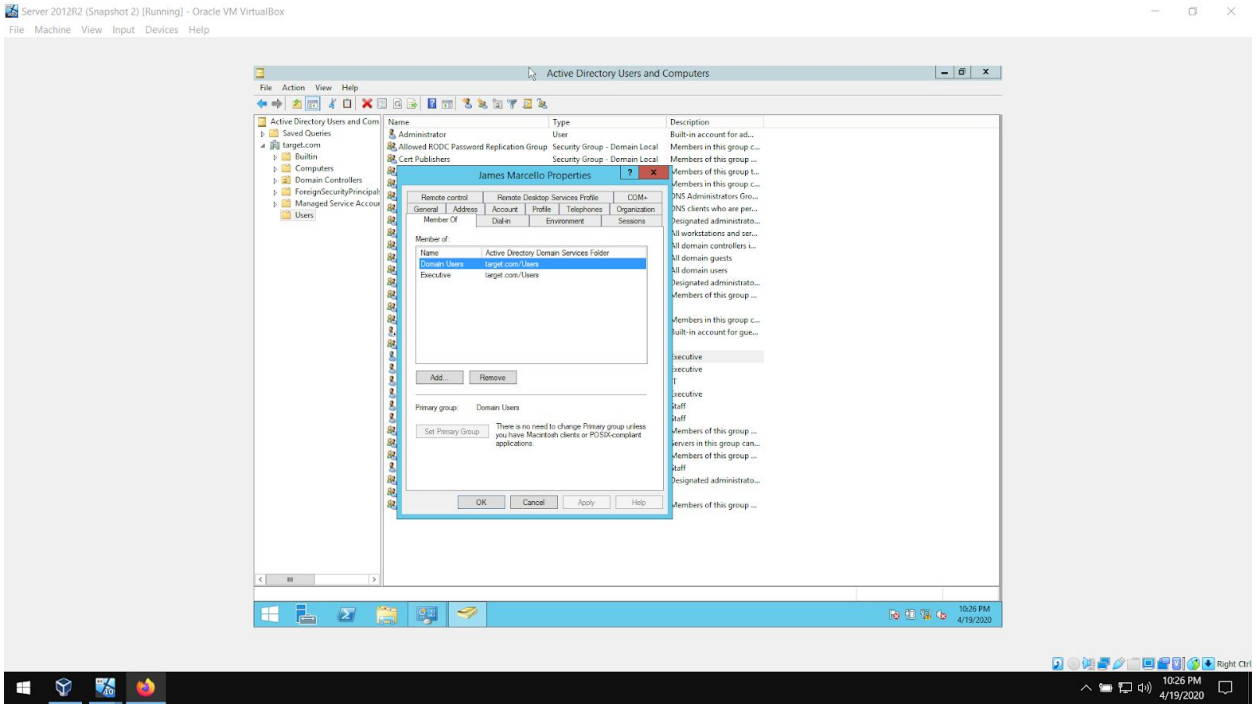
Entering the first few letters of the prior created group is required for the Check Names option to work.

Select Groups



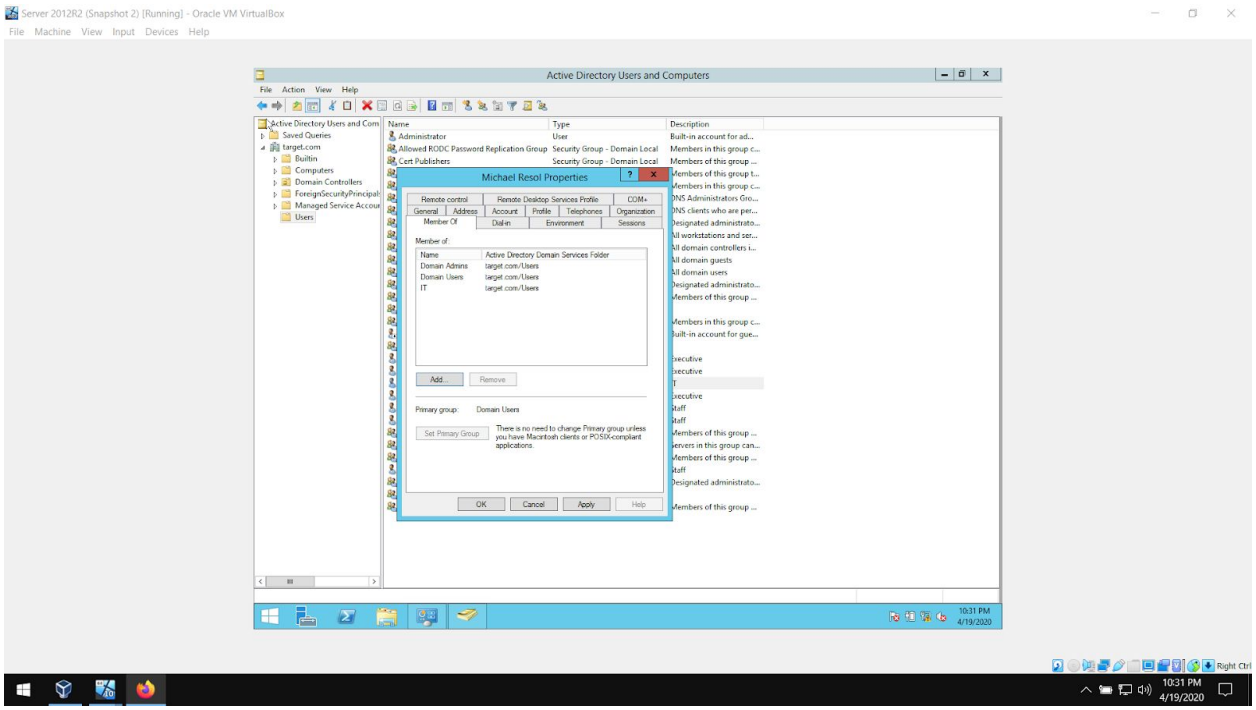
After selecting Check Names, the executive group pops up.

James Marcello Properties



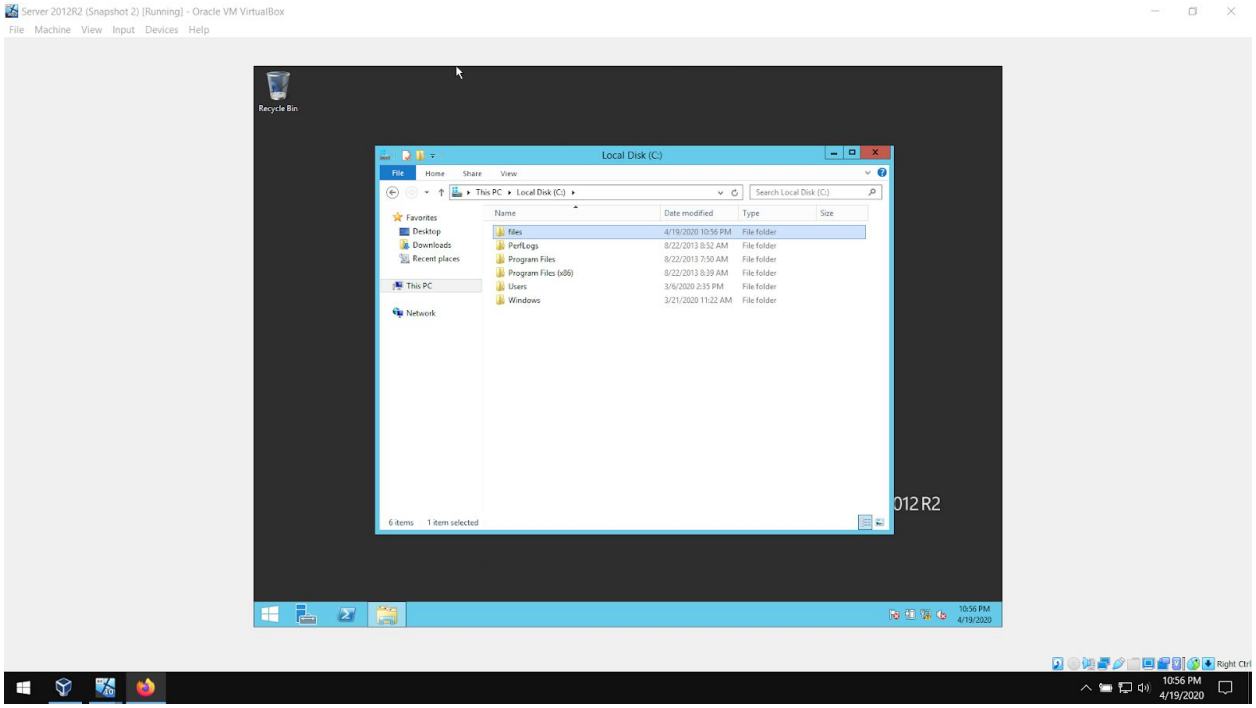
JamesM is now a member of the Executive group. All the other appropriate groups were set for each user.

Michael Resol Properties



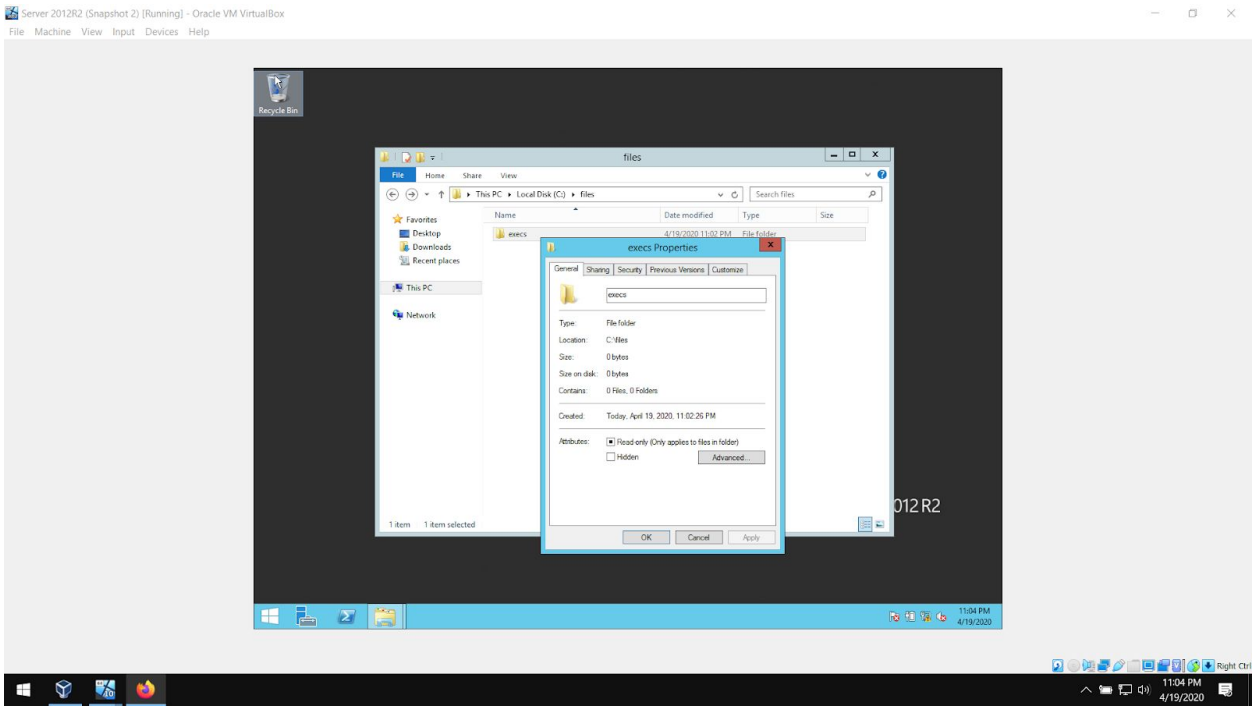
MicahelR gets an additional membership to Domain Administrators. At this point all users have been created and assigned their appropriate memberships. Next a shared folder will be created.

Local Disk (C:)



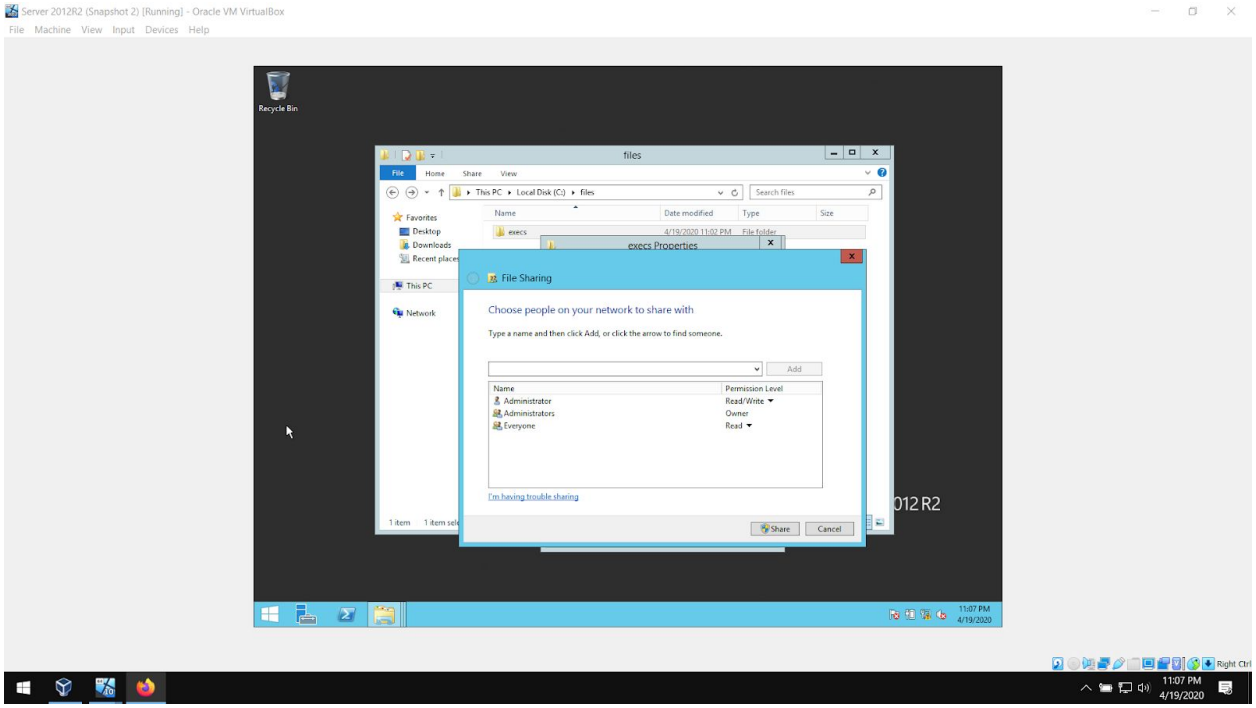
A files folder was created.

execs Properties



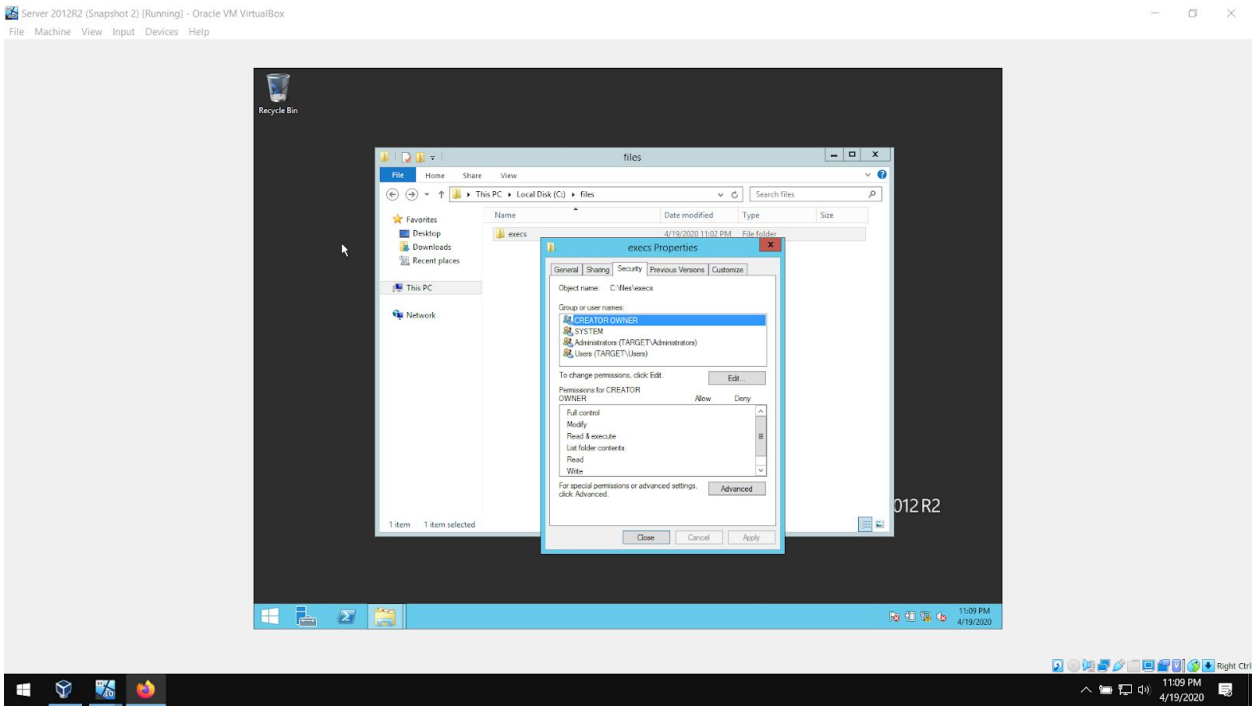
Right clicking on the execs folder then selecting Properties. Then the sharing tab.

File Sharing



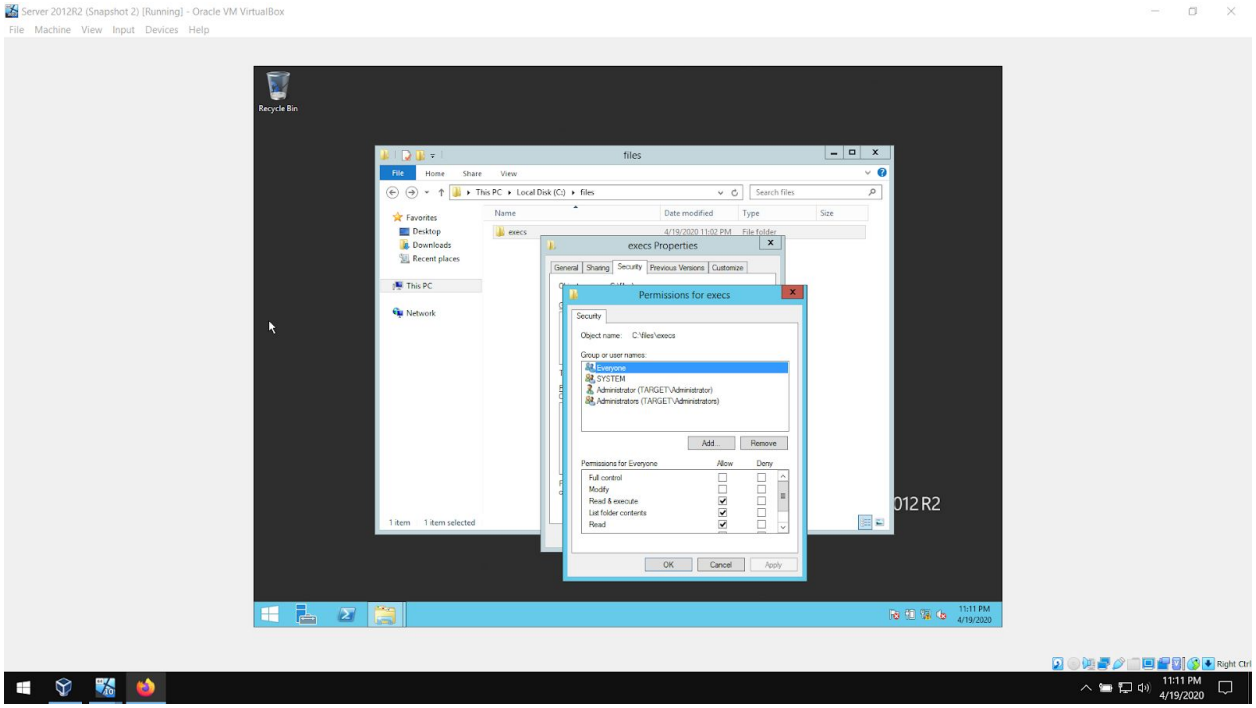
Each user must be given a folder permission. For this lab, the group Everyone was selected with Read access.

execs Properties



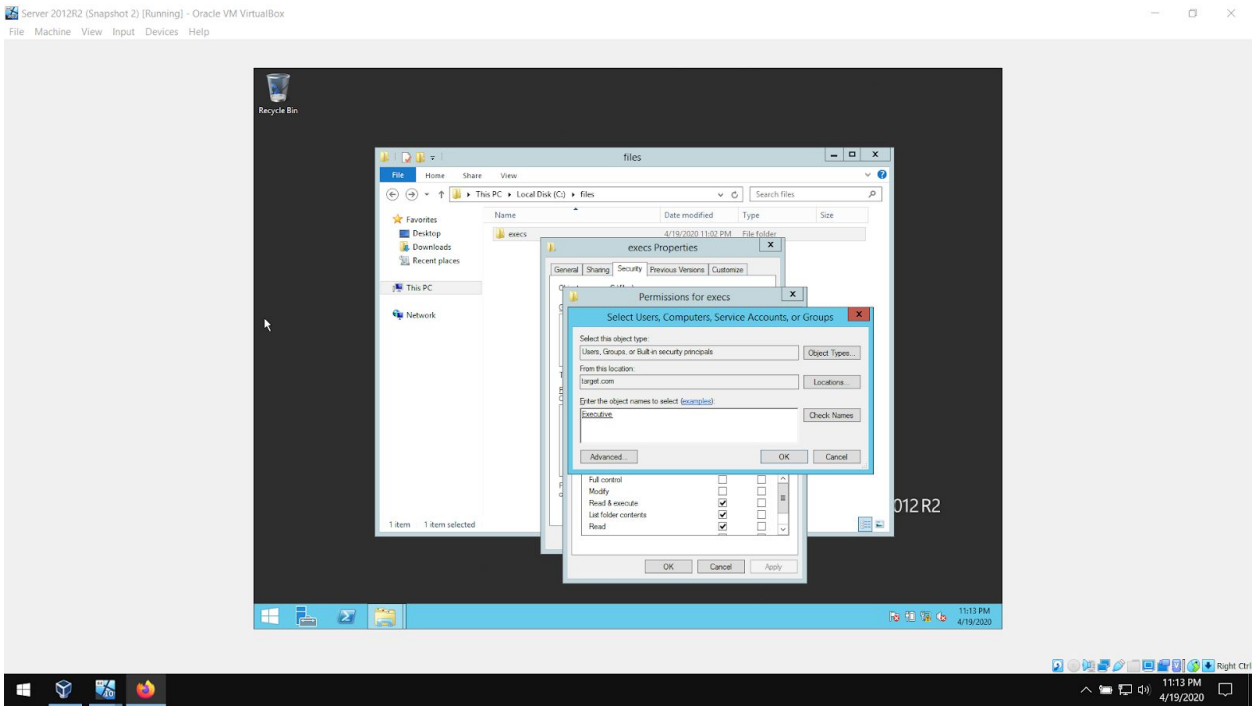
Now switching over to the Security tab and clicking on Edit on the CREATOR OWNER.

Permissions for execs



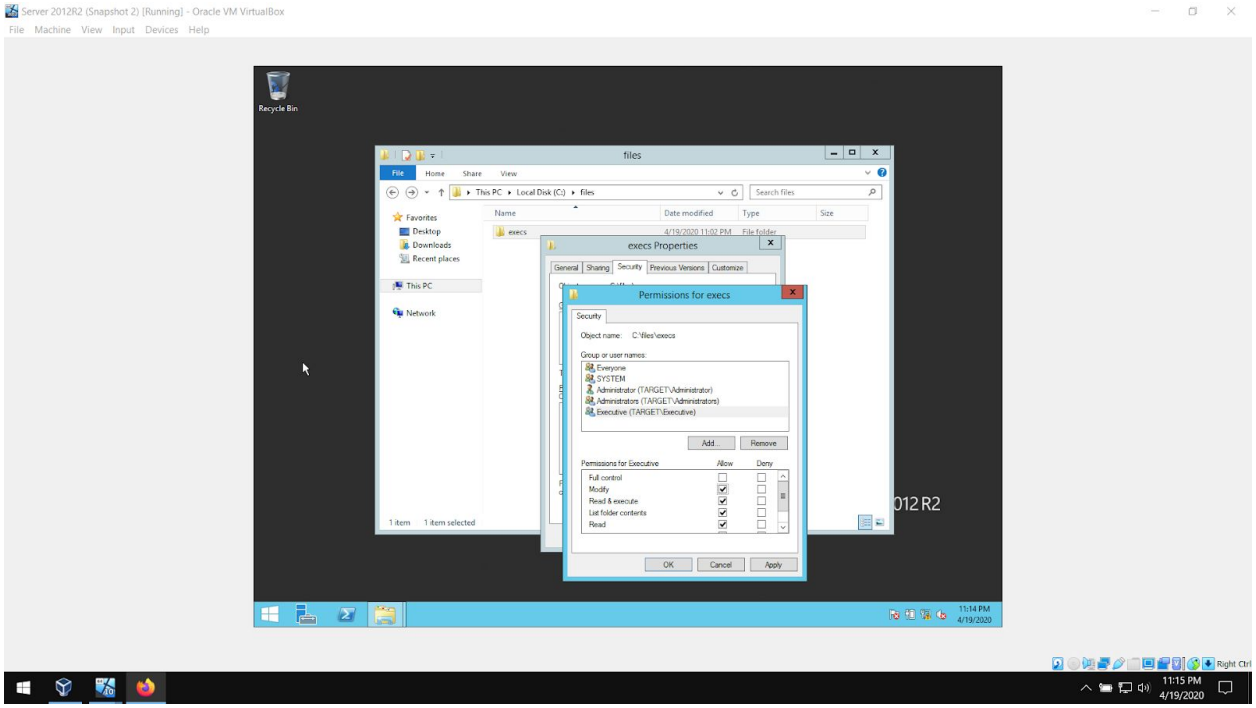
We have to add the Executive group to the folders permissions by clicking Add while selecting Everyone.

Select Users, Computers, Service accounts, or Groups.



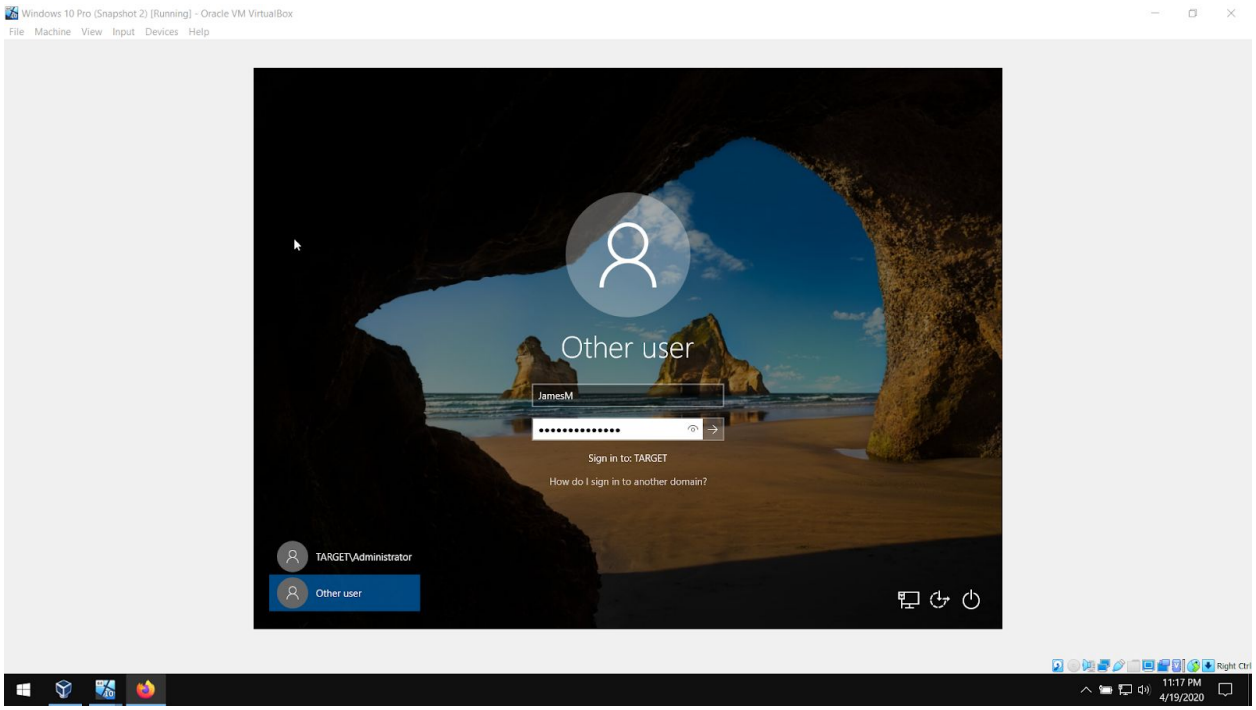
The Executive group is found and selected.

Permissions for execs



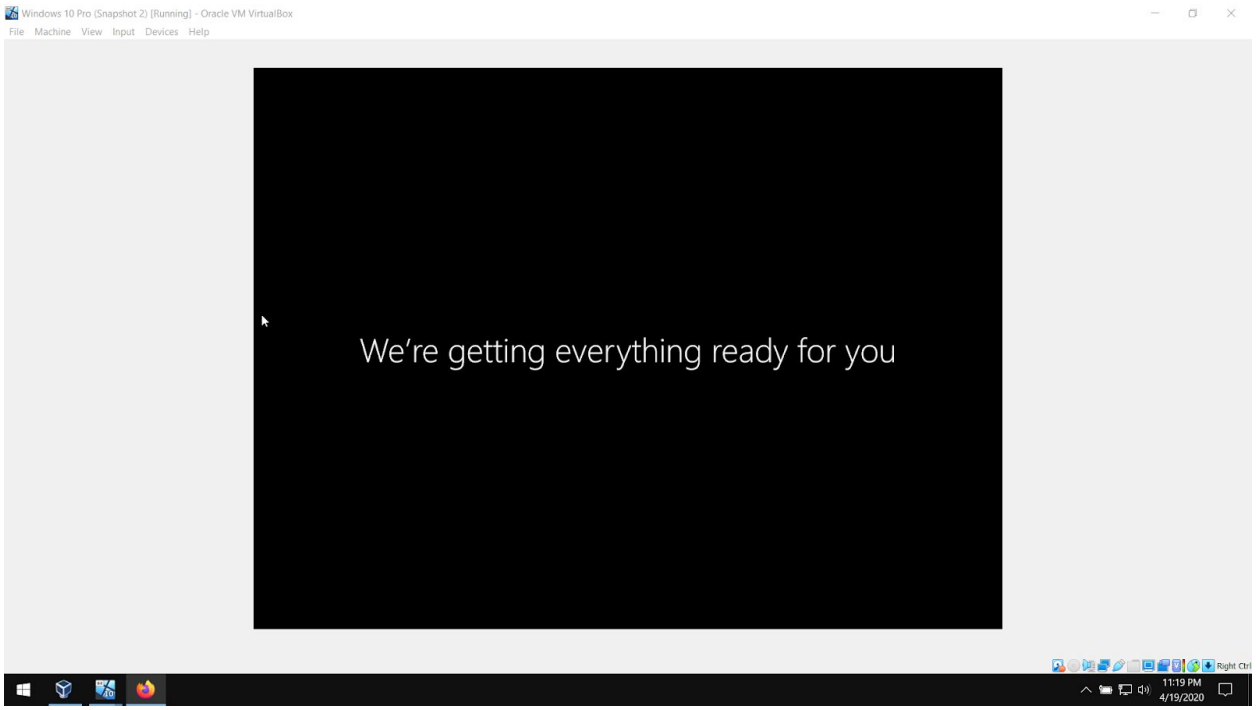
The Executive group is given Modify permissions for execs.

Logon - Windows 10 Pro



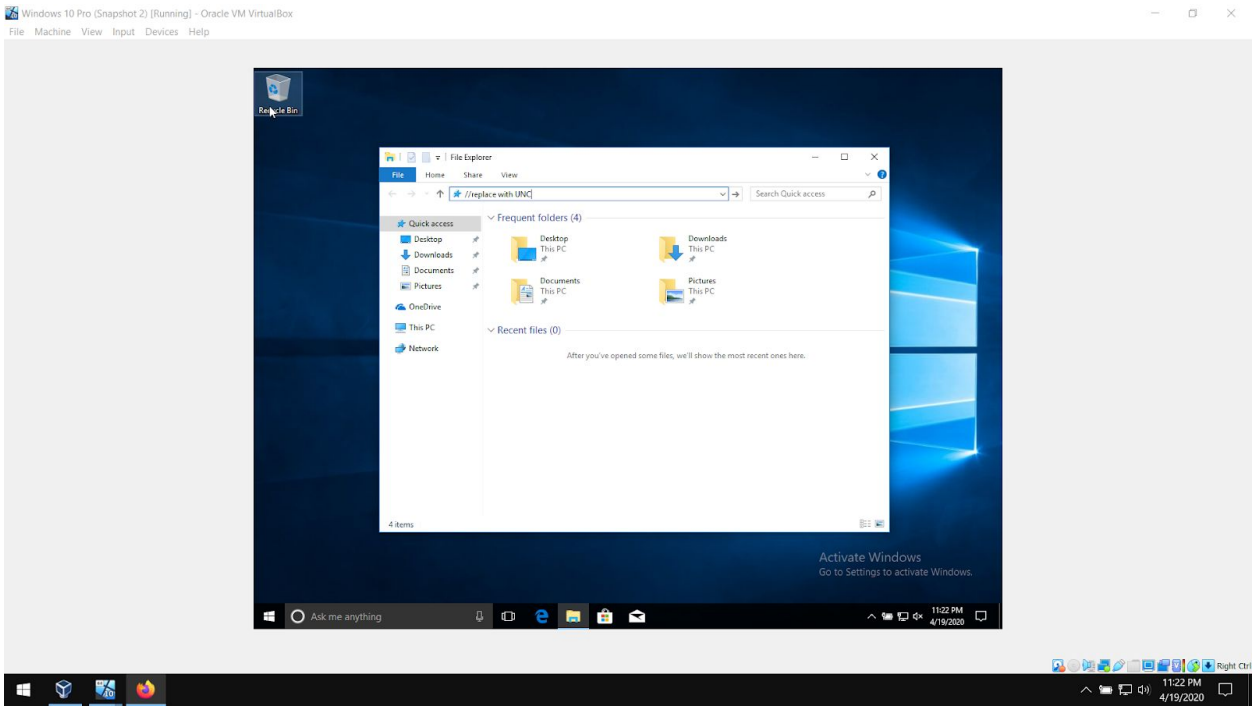
This Windows 10 Pro VM was set up with administrative rights initially. Now another user will be added.

Windows 10 Pro



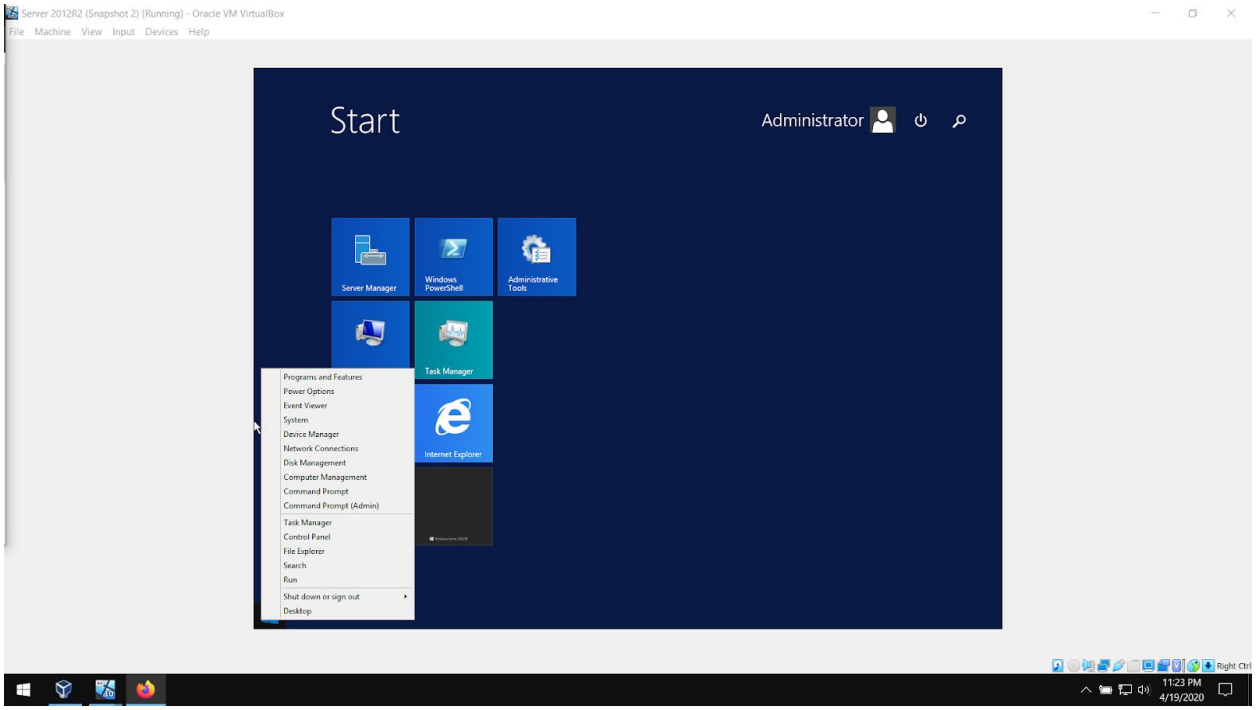
Initial setting up procedure for first time login for JamesM.

Windows 10 Pro



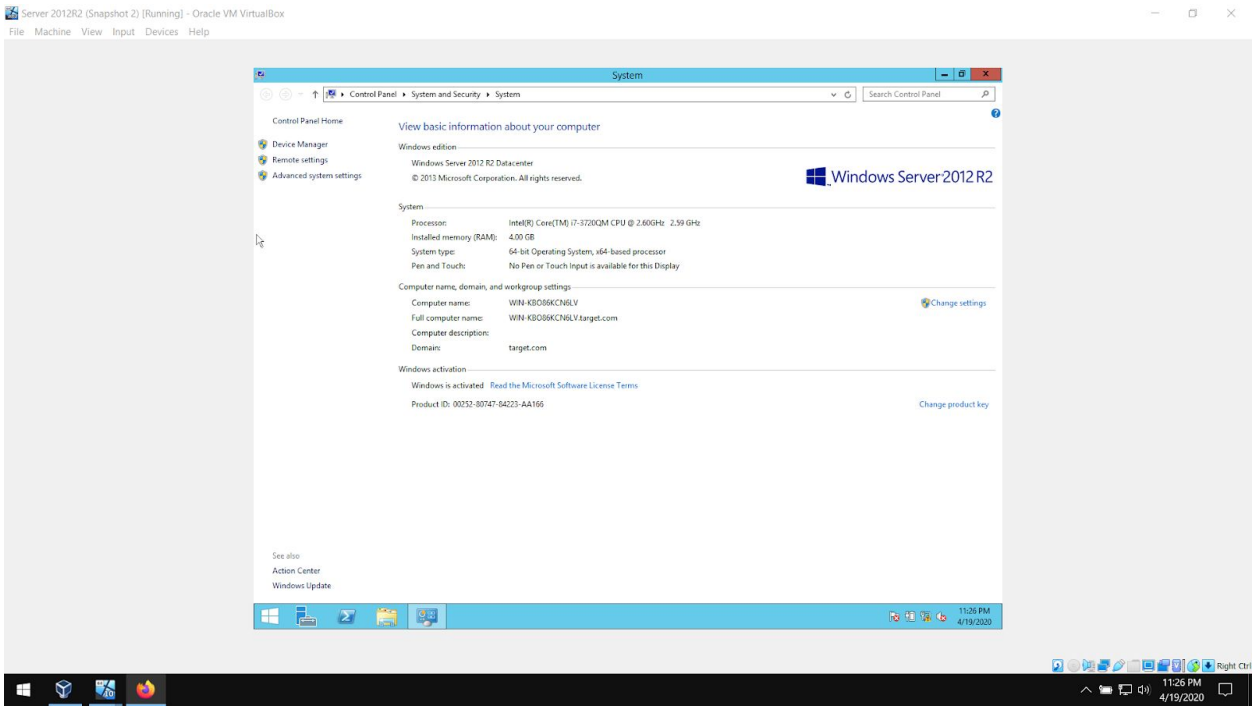
To access the network folder, the proper UNC must be entered. The UNC can be found on the Server2012R2 VM.

Server 2012R2



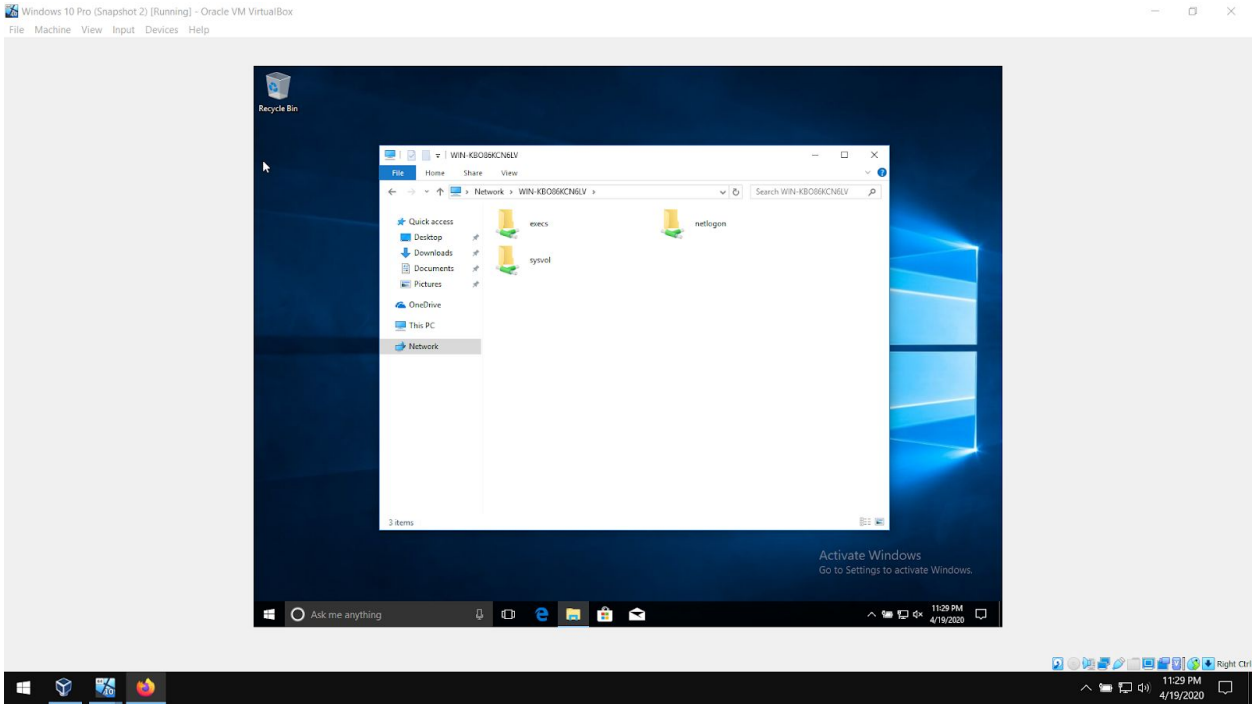
To get the folders UNC, right click on the Windows icon then select System.

Server 2012R2



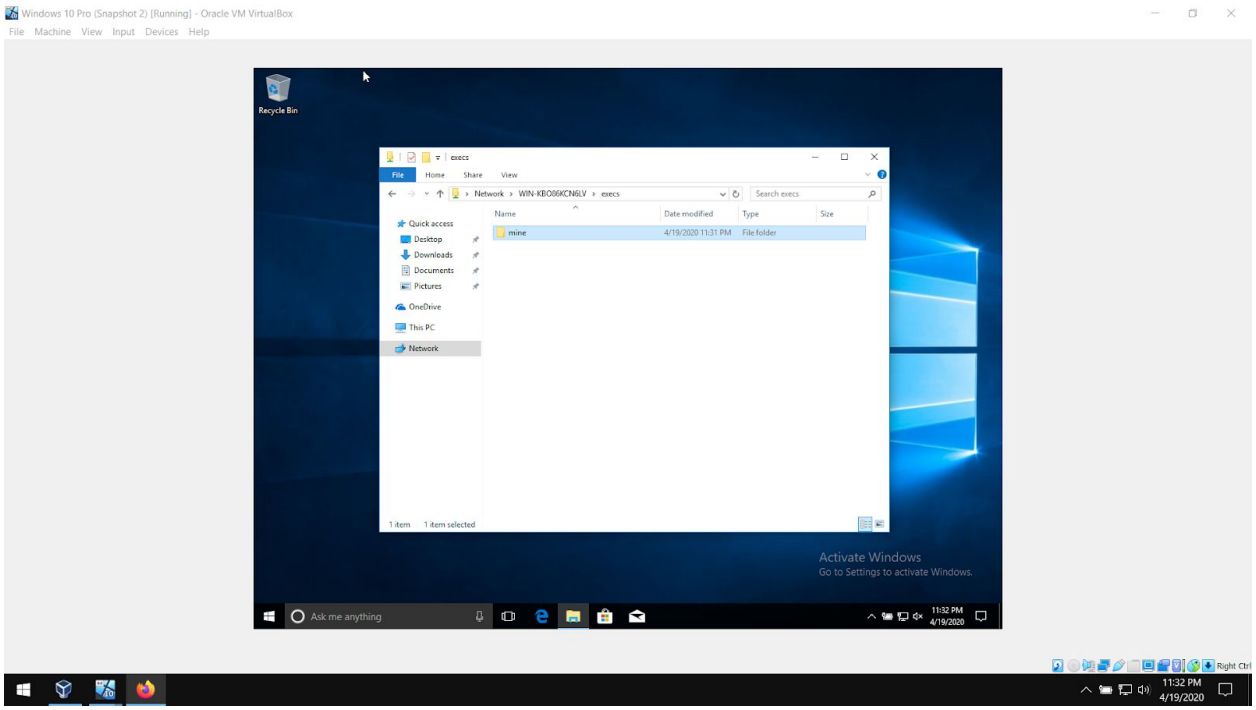
The Server 2012R2 name is displayed.

Windows 10 Pro WIN-KBO86KCN6LV



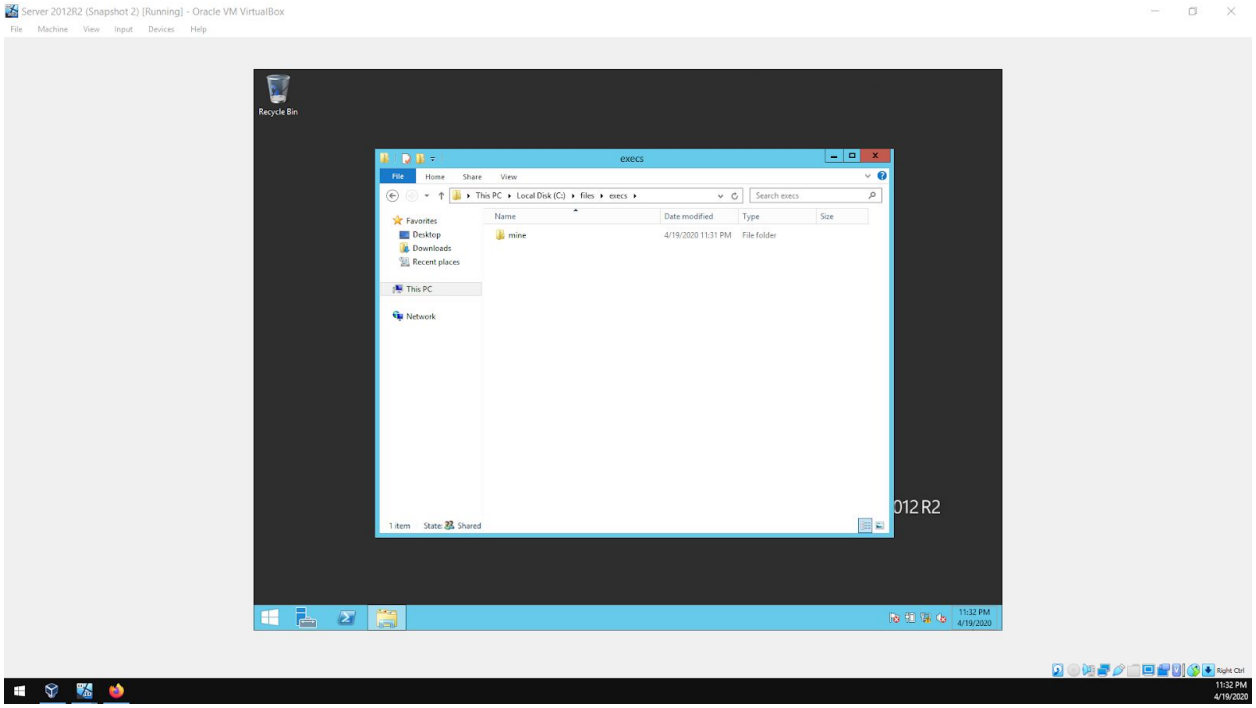
Typing in the Server 2012R2 VM's name, then access to the execs folder is present.

Windows 10 Pro - execs - mine folder



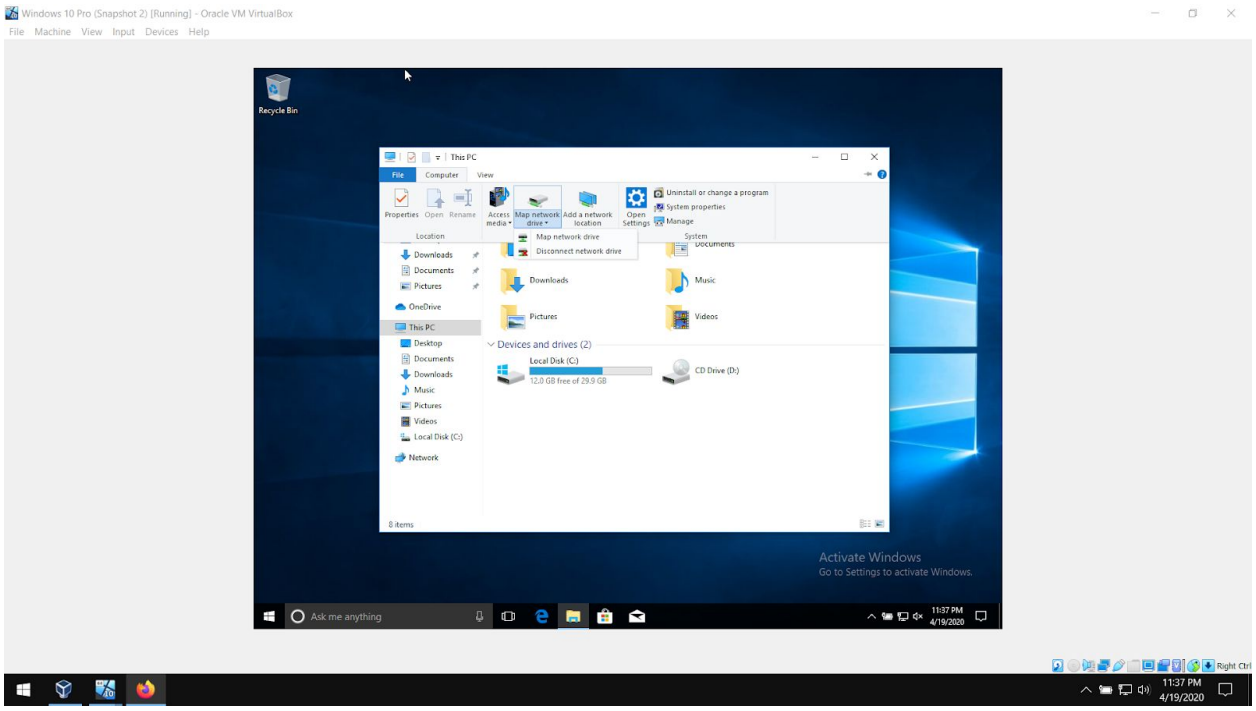
To test network connectivity with the Server 2012R2 VM, a folder was created within Windows 10 Pro (JamesM) in the network folder.

Server 2012R2 - execs folder



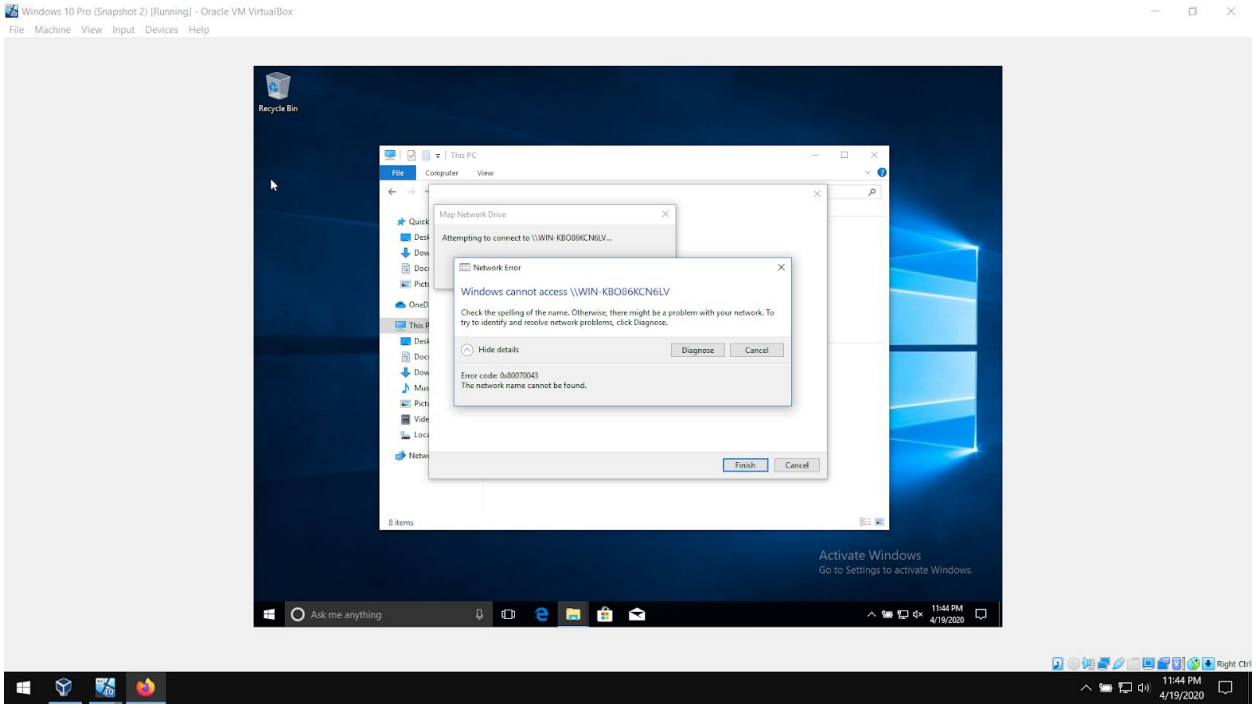
The mine folder shows up in the Server 2012R2 VM.

Windows 10 Pro - This PC



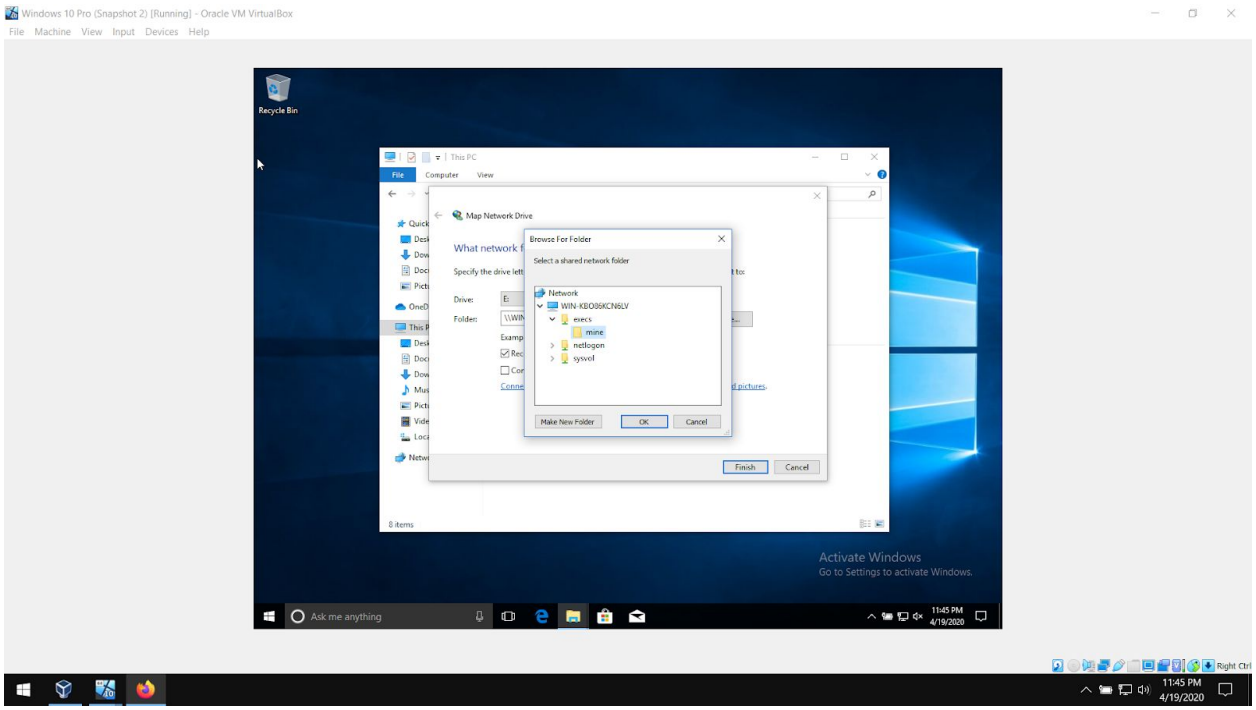
To make network folder access easier for the user, map network drive will be selected from This PC → Computer at the top → Map network drive.

Windows 10 Pro - Map Network Drive



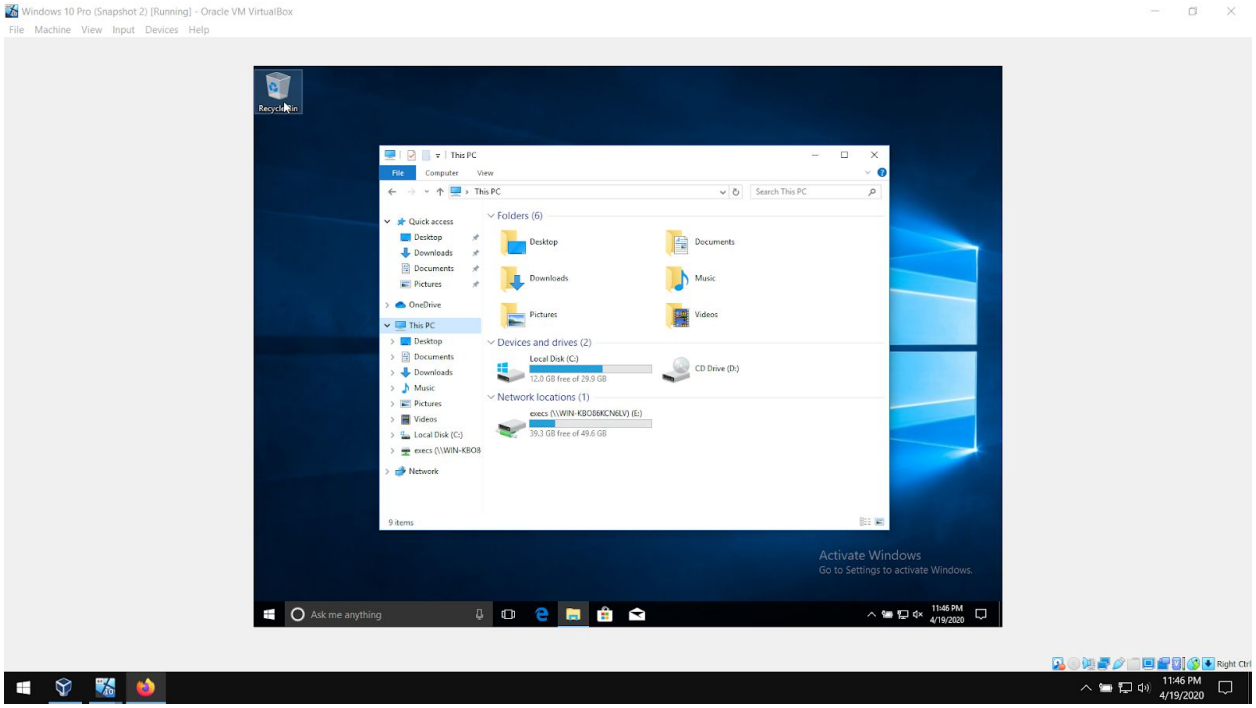
This is the exec folder so a drive letter of E: will be used. But there seems to be an error. The network name cannot be found.

Browse For Folder



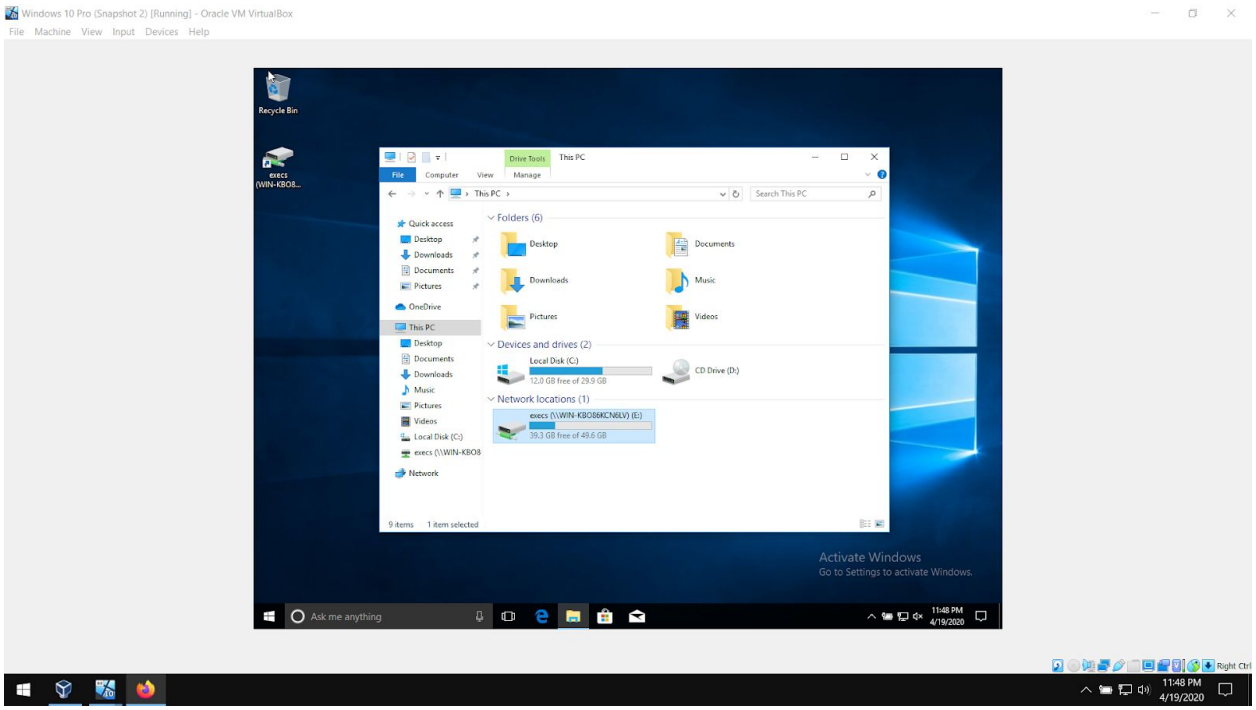
However, clicking on Browse, locates the execs folder.

This PC



Located in Network locations, the folder execs if found!

execs map drive shortcut



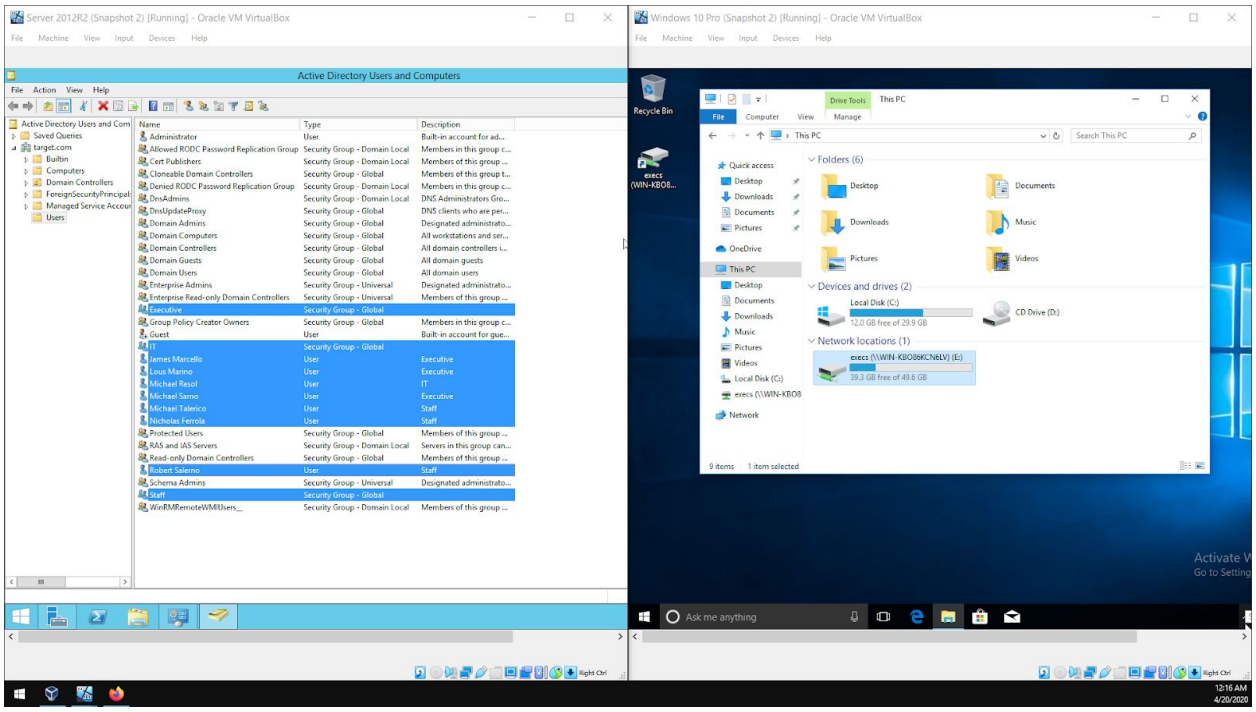
A shortcut to the network drive was created.

3. Surprises. Things rarely go as planned. Include this in your report. If things aren't working, documenting the problem can help you to find the solution.

> When mapping the network drive, Windows couldn’t find the drive initially. However, after selecting browse the network folder was present. Selecting to turn off Network Discovery when initially setting up the Windows 10 Pro system may be to blame.

4. A screenshot of the final result of the assignment.

Server 2012R2 and Windows 10 Pro



On the left the newly created and assigned users and groups. On the right the Network Drive setup.

5. Summary. Did it work as expected? Did you need more research?

The lab was successful with one error during the Map Network Drive step. First off, the Windows 10 Pro environment was initially set up with Network Discovery set to off. My hunch is that Network Discovery was to blame for the network not being found after manual entry of the folder UNC. After doing some research, Microsoft explains

> "Network discovery is a setting that affects whether your computer can see (find) other computers and devices on the network and whether other computers on the network can see your computer. It's one of several settings that are turned on when you turn on network sharing. You can turn network discovery on or off independently of network sharing, but we **discourage this**. Here's why. If you're connected to a network in a public location and you decide to turn on network discovery but leave network sharing turned off, the network discovery setting will be on for every public network you connect to from then on. This wouldn't be safe. That's why we recommend using the network sharing setting instead."[1]

On a side note, Microsoft discourages independent controls with Network Discovery with Network Sharing in a public setting, good to know. The Map Network Drive error could have occured because I had set Network Discovery to off in the initial setup of Windows while not having enabled Network Sharing. But Microsoft explains that Network Discovery and Network Sharing work independently of each other. Besides, Network Sharing could be independent of how the folder was shared. More likely a typo in the Map Network Drive input occured. Which makes sense given the network folder was present after clicking on browse. Microsoft goes on to explain that Network Sharing is

> "...only available for Wi‑Fi, Ethernet, VPN (non-domain), and dial-up (non-domain) connections. It's unavailable for domain networks. On VPN or dial-up connections, you must connect to the network first, then press and hold or right-click the network name to change the network sharing setting."[2]

This could mean that our lab process somehow supersedes the Network Sharing service or is unrelated to both Network Sharing and Network Discovery as previously mentioned. More research can be done into how Network Sharing and Network Discovery relate to each other on Server and Home environments and if any known vulnerabilities or backdoors have been established on domain networks.

[1] http://hs.windows.microsoft.com/hhweb/content/m-en-us/p-6.2/id-6ddfa83c-01c8-441e-b041-1fd912c3fe60/
[2] http://hs.windows.microsoft.com/hhweb/content/m-en-us/p-6.2/id-6ddfa83c-01c8-441e-b041-1fd912c3fe60/