--What is Windows Server?

1) Ask who has used Windows Server
2) Talk about how it's basically the same thing as Windows 10 (2016 and 2019).
3) Talk about the different use cases of Windows Server.

Learn RDP

1) Talk about what RDP is, see who knows about it, it's use cases.

Enable RDP

1) Turn on your Windows Servers.
2) Log in using the administration user.
3) Open the start menu and type "Allow remote".
4) Select "Allow remote access to your computer".
5) Click "Allow remote connections to the computer" and unselect the "Allow connections only from computers..."
6) Apply everything.+

Test that it now works

1) On your computer open your RDP client (remmina, Remote Desktop Connection, etc.)
2) Enter the IP of the Windows Server
    a) Open a Command Prompt on the Windows Server
    b) Enter "ipconfig"
    c) Look for "IPv4 Address..." then some IP
3) When prompted enter the credentials for your user account.

Learn Server manager

1) Server manager is where you will actually interact with the main parts of a Windows Server.

Active Directory

Install Active Directory

1) In Server Manager, click on "Manage" then "Add Roles and Features".
2) In the wizard, click next until you are on the "Server Roles" pane on the left.
3) Select "Active Directory Domain Services".
4) You will need to install features that are required for Active Directory, click "Add Features"
5) Click next until you are on the "Confirmation" pane on the left.
6) Select the "Restart the destination…" at the top. Then click "Install".
7) Now as that installs, lets enable RDP on all of our other machines.

Create a Domain

1) In Server Manager, there is a little flag at the top and it should have a warning symbol on it. Click it.
2) We now see a message saying "Post-deployment Configuration…" this is telling us that the server we just installed Active Directory on needs to be configured. Click on "Promote this server to a domain controller".
3) This opens the Active Directory Configuration Wizard.
4) We want to create a domain, but domains have to be apart of a forest, think of a domain as house that has people and groups inside of it, and then the forest is the entire city. The city can just be one house (one domain) or it can be many houses that are all different but can interact because they are in the same city.

   So we will select "Add a new forest" to create a new domain/forest.
5) In the "Root domain name", you can make the domain anything you want. To make things simple, make it your username followed by ".local". So for example "user1.local" then click next.
6) We don't need to change any of the settings for this demonstration so just go ahead to the "Directory Services Restore Mode password". Go ahead and use the administrator password.

   This is used so that if for some reason you are able to completely

mess up your Active Directory you can change things in the database to fix stuff.

7) Now keep clicking "Next" until you hit the "Prerequisites Check" pane on the left.
8) The Prerequisites check gives some warnings but these shouldn't matter to this demonstration we are doing. Go ahead and click "Install" to start the configuration of the server. *IF* you cannot click install, try to troubleshoot the issue.
9) The server will now restart to configure all of the changes.
10) Once RDP is enabled and tested on all 4 machines, go ahead and play around on the 2nd Windows Server 2016s Server Manager to see what different roles there are and anything you can find.

User/Group Management

1) In Server Manager click on the "Tools" button.
2) Because we have now installed Active Directory we have 5 new options at the very top all starting with "Active Directory", there are more that Active Directory has created and we will look at another one later. The main one we use is "Active Directory Users and Computers". Go ahead and click on it.
3) This opens the "Active Directory Users and Computers" window. This is where you can create user accounts, manage Security Groups, and much more.
    a) Organizational Units
    b) Users
    c) Security/Distribution Groups
    d) Computers
4) Let's create your user account. You could use Administrator all of the time but we want security and apart of security is knowing who is doing what and not sharing accounts. Open the "Users" folder.
5) You will see a long list of Security Groups and Users that have been already created for you in Active Directory. A lot of these you will never even touch in the real world.
6) Right click in the white space to the right of the description field and hover over the "New" option. This will show you all of the different items that you can create like User, Security Group, Computer, etc. Since we want a User go ahead and click that.
7) You are now on the User creation wizard. Go ahead and fill out the following fields:
    a) First name
    b) Last name

c) User logon name (make this your NKU username to make things easy).

8) Some of the fields will fill themselves in while you type, leave those to fill in automatically. Click Next once those fields are filled in.
9) Now you are brought to the Password field. For the password, enter the same password as administrator just to make things easier.
10) Deselect all of the check boxes.
11) Click "Next" and then click "Finish".
12) Let's now make your user a Domain Administrator so that they will have administrator rights on all domain computers.
13) Right click on your user and select "Properties".
14) This is where you can edit the properties of a user like their name, address, account information, and some more technical information. Click on the "Member Of" tab.
15) We can see that our user is apart of the "Domain Users" group. This group is automatically assigned to any users that you create in AD. Click the "Add" button.
16) This is where you type in the group that you want to add the user to, so type "Domain Admins". You can now either go ahead and click "OK" if you know that you typed the correct group and that the group exists, or you can check your work by clicking the "Check Names" button and seeing that it is now underlined with the proper group.
17) Now to test the account try to RDP to the machine using your newly created account.

Domain joining a computer

1) In order to domain join a computer, the computer needs to be using a DNS server that has a pointer to the AD. When we installed Active Directory onto the Windows Server machine, it automatically installed and configured a basic DNS server. We will have to configure our Windows 10 machine to use the Windows Server as a DNS server.
2) **Maybe have them try without DNS first?**
3) Open "Control Panel" by searching for it in the search bar. Click on the "Network and Internet" option and then open "Network and Sharing Center".
4) Click on "Change adapter settings" on the left.
5) There should now be 1 or more network adapters. There will be one labeled "Ethernet..". Find the one that on the bottom line has "Intel(R)..." as this is the one that our VM is using for internet and then double click it.
6) Click "Properties". Double click on "Internet Protocol Version 4(TCP/IPv4)".

7) Near the bottom is an option to "Use the following DNS server addresses", select it to allow stuff to be typed into the fields below.
8) In the "Preferred DNS Server" field, type in the IP address of the Windows Server that you created and then click "Ok" and "Close" until you are back to the adapter selection screen.
9) We are now going to try to domain join the computer. Search for "system" in the search bar and open it.
10) On the right side, click "Change settings" under the "Computer name, domain, and workgroup settings" section.
11) The "System Properties" window will now open, near the bottom click "Change" next to "To rename this computer…"
12) Here you can now change the computer to any name that you want. Let's change the computer name to Win10Week1 **but do not click enter or "Ok" yet.**
13) In "Member of", select the "Domain" option. We then want to enter the domain that we created, which would be our username.local so "user1.local" for me. Then click "Ok"
14) You should now be prompted for credentials to join the domain. The user needs to have domain admin privilege or be a custom role that has the ability to add computers to a domain. The user account you created for yourself should suffice. So enter your username and then the password you made for the account.
15) If everything was done properly it should say you are now apart of a domain. Click "Ok" on all of the windows until you are back to the "System Properties" window, click "Close" on it. You will now be asked if you want to "Restart Now" or "Restart Later", go ahead and "Restart Now".
16) Once the computer boots back up, we will try to log into the domain account that you created for yourself. On the login screen click "Other User" in the bottom right. Now under the place for your credentials you will see "Sign in to: USERNAME" where it's your username. This is the domain that you created. Enter the credentials for your account, username is NKU username, password in the same password as everything else.
17) If you are domain joined properly and enter the proper credentials, you should now login to your newly created domain account.

GPO

1) Talk about what GPOs are
2) Talk about their use cases
3) Give some examples

Show how to make a GPO

1) Login to the Windows Server hosting your AD.
2) Open Server Manager.
3) Click "Tools" > "Group Policy Management"
4) This is where you make GPOs for different domains and groups. Expand the forest, then expand "Domains", now you should see your domain so expand it.
5) Here is where you work with the GPOs for a domain. You will be able to see Organizational Units ****How much do we actually want to cover these?****, and the actual GPOs themselves. GPOs are stored in the "Group Policy Objects" folder under the domain. If we open this folder, we can see that there are already some policies made, these are default policies that come as apart of AD when it is first made. Let's look at the "Default Domain Policy" by double clicking it.
6) Clicking on the "Settings" tab, you can see all of the different things that this GPO does. There's a lot of different things and you could go through everything to see what each thing does.
7) Now looking over on the right pane, directly underneath the domain name is another item named "Default Domain Policy" and the icon has a little arrow in the bottom left. This is a "Link" to the GPO that is under "Group Policy Objects". All GPOs are stored under the folder named "Group Policy Objects" and then "linked" to certain parts of the domain. So for example, "Default Domain Policy" is underneath the domain that you created. That means the entire GPO is applied to the entire domain.
8) Another example of this is the Organizational Unit named "Domain Controllers". If you open it up there is a GPO link to a GPO named "Default Domain Controllers Policy". The actual GPO is located in the "Group Policy Objects" folder. The only settings the GPO affects are the Organizational unit that the policy is on and any OUs inside of it.
9) Let's create a quick sample GPO that will keep users passwords for the previous 24 times and requires them to change it every month because we don't like them.
10) Right click the "Group Policy Objects" folder.
11) Click on the "New" option.
12) Here you can insert a name for the GPO. Let's name ours "Password Change". Then you could select a template GPO but let's keep ours none. Hit "OK".
13) Now if we look under the GPO Folder there is our GPO, Password Change. Go ahead and double click it to open the GPO.

14) As you can see there is some stuff already under the "General" portion of the GPO. This is just information about that GPO itself and doesn't need to be changed in order for the GPO to work.
15) Right click anywhere on the right pane and then click the "Edit.." option.
16) This will now open the "Group Policy Management Editor". This is where you will set up the settings for the GPO.
17) Now we will need to find where our options are located. This is something that can be complicated but once you get some experience or research it, it should become easier. You also need to think about the setting you want to change and follow logically where it might be located. Because we want to change password settings, we should look in "Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Account Policies -> Password Policy".
18) Clicking on Password Policy allows us to see all of the settings we can control using a GPO. The two settings we wanted to change were the "Enforce password history" and "Maximum password age".
19) Go ahead and double click on the "Enforce password history" to open the properties of that control. We want to define this policy (defining is basically the same as enabling in this case) and then we want to set the number of passwords to remember. 24 is the maximum number for this so that's what we will go with. After entering that click "Apply" then "OK".
20) The other setting we wanted to apply was the "Maximum password age". Go ahead and double click it to open it. Define this policy setting and set it to be 30 days for 1 month. Now click Accept. You will notice that it wants to enforce the "Minimum password age" policy now. Go ahead and allow that by clicking "OK".
21) Let's allow our users to change their passwords as often as they would like so go to the "Minimum password age" option and double click it. We want them to be able to change it as often as they like so change the number to 0 and then click "Apply" and "OK".
22) We have now defined our password policy. Go ahead and close out of the window by clicking the X in the top right. When editing a GPO it saves your changes as you do it so you do not need to save your changes.
23) If we now refresh the GPO by selecting it in the left pane and then clicking the refresh icon on the top that looks like a green arrow making a circle, we can see the changes to our policy on the bottom by scrolling down.
24) We now have a GPO with our custom security policies but they are not currently attached to anything, they just exist in our list of GPOs. In order to apply the GPO, we need to create a link of it to whatever object we want to put it on, so the entire domain in this case. In order to do that, just click on the GPO and then drag it onto the object, the domain in this case, you want it on. You will then be prompted if you want to link the GPOs to the object you selected. Click "OK".

25) Now there is a link of the GPO to the domain. Now your policy is being applied to the entire domain!
26) GPOs are something that I would recommend you look into on your own time outside of here as they are very important in business settings and can get complicated. There are also application specific GPOs for applications that support it so you can look into that. Google Chrome has good examples of this.

Hyper-V

1) Now we are going to discuss something that will help you the most not only in NKCyber but in the Informatics world. This entire time you have been working on Virtual Machines or VMs for short. VMs are a way of running any operating system on top of another. So if you are running a Windows machine and need to develop something for a Linux machine, you can run a VM that is any version on Linux you may need.
2) Another use case might be if you want to simulate a business network *COUGH COUGH* you can run a bunch of VMs in a way that would represent a business network.
3) Windows 10 Pro, NOTE IT MUST BE PRO NOT HOME, has the built in ability to create, run, and host VMs directly on that computer. It is called **Hyper-V**. Hyper-V is a built-in hypervisor in windows, and that is how it gets its name. A hypervisor is what controls all of the VMs on the host computer.
4) Since we don't have much time tonight, all that I will show you is how to install Hyper-V. This will give you the opportunity to research it on your own after tonight.
5) On either Windows 10 box, go to the search bar in the bottom and type in "Hyper-V". You should see "Turn Windows features on or off" be the best match. Go ahead and open that.
6) You will now see a list of features that Windows has. Some are disabled by default and some are enabled. Let's enable Hyper-V by clicking the checkbox next to it and then click "OK". Windows will now search for required files and prepare the feature to be installed. Once it is done you will need to restart the machine as prompted. Click "Restart now".
7) After the restart you can now search for Hyper-V and you will find it. This is the part where you will need to go research the rest about Hyper-V and VMs on your own until we have a week dedicated to them.

8) Being an NKU student means that you do get some Windows Keys and VMWare software keys. For VMWare related software, google "NKU vmware store". For Windows related software, check Azure for Education and sign in with your NKU email and password.

PowerShell Exists

- Basically a lesser version of Terminal on Linux
- Can be used to change Windows settings
- Can use Command Prompt commands but Command Prompt cannot use all Powershell commands
- Used for more automation reasons then basic usage.

```
Get-Aduser -filter * | export-csv C:\users.csv
                                        Export users
                                Powershell remoting is cool
                              New-pssession otherservername

                    Create users and mailboxes for exchange from csv is quick


                                                    Disable smb v1
                        set-smbserverconfiguration -enablesmb1protocol $false

                    Installing chocolatey to install firefox because IE is ass
                                $source = "https://chocolatey.org/install.ps1"
                                            $destination = "c:\choco.ps1"
                                    $web = New-Object System.Net.WebClient
                                $web.DownloadFile($source, $destination)
                                 Set-ExecutionPolicy RemoteSigned -Force
                                        Invoke-Expression "C:\choco.ps1"
```

SEC-001 AD security
Security Groups: see user/group security checklist
Management Tools: ADUC
Security checklist:

	ITEM	Action	Description	Rationale
☐	Change Password	**Go through AD gui to right click user and change the password**	= Change current account pw = Change arbitrary account pw	Default credentials will be attempted
☐	AD Permissions	**Go through AD user permissions checklist**	= Dumps entire DBMS with ease on live server	Make sure AD user permissions aren't screwed
☐	Create initial list of users	**PS: Get-Aduser -filter * | export-csv C:\users.csv**	= Gives a list of users on the domain	Gives us an initial list of users to compare against check if users have been added.
☐	Backup GPO's	**PS: Backup-Gpo -All -Path C:\GpoBackups**	= Backups all GPO's to specified directory	Incase resetting the GPO's breaks them we can restore from backup.
☐	Reset GPO's	**DCGPOFIX /target:Both**	= Resets the two initial GPO's to default settings	Using screen will be useful for running multiple terminals on boxes with only single terminal acce
☐	Apply Secure GPO Baseline	**Follow** https://github.com/nsacyber/Windows-Secure-Host-Baseline	= Gives reasonably secure GPO settings	Security
☐	Audit Everything	**GPO enable auditing**	= Audit things for IR	For IR
☐	Disable NTLM/Force NTLMv2	**Computer Configuration > Windows Settings > Local Policies > Security > Network Security:**	= Disables NTLM, forces the use of kerberos for authentication = Force the use of NTLMv2 if NTLM is needed.	NTLM is vulnerable to having passwords cracked and MitM attacks, kerberos is significantly more secure. Forcing NTLMv2 if NTLM is required prevents NTLM or LM vulnerabilities being used b attackers. Baseline above does not include these settings.
☐	Powershell Auditing	**Computer Configuration > Administrative Templates > Windows Components > Windows Powershell >**	Turn on PowerShell Script Block Logging Turn on PowerShell transcript	Logs all Powershell stuff
☐	Protected Users	**PS; Get-Aduser -filter * | add-adgroupmember "protected users"**	Move users to the protected users group	Make users protected
☐				
☐				
☐				

SEC-003 Exchange Security
Security Groups: Organization Management, Recipient Management
Management Tools: https://hostname/ecp, powershell management console
Security Checklist:

- Mail flow
- Make sure ssl is required for website
- Have TLS enabled for SMTP
- Check website contents
- Add mail flow rule to filter macro enabled documents as attachments
  - .docm
  - .dotm
  - .xlm
  - .xlsm
  - .xltm
  - .xla
  - .pptm
  - .potm
  - .ppsm
  - .sldm

	ITEM	Action	Description	Rationale
☐	Audit Security Groups	**Go through ADUC gui**	= Audit admins	Make sure only administrators have access to modify exchange
☐	DNS Zone security	**Go through DNS gui security tab**	= Make sure permissions are good	Only Administrators should be able to modify DN entries.
☐	Audit DNS records	**Go through DNS gui, look at actual entries**	= Audit records	Gives us a list of systems on the domain, make su a DNS rebinding attack hasn't been used.
☐	Audit conditional forwarders	**DNS gui, conditional forwarders**	= Audit entries	
☐	Audit DNS Forwarders	**DNS gui, computer name, properties, Forwarders**	= Audit entries	Make sure we're forwarding unknown dns entrie: to secure location.

Windows Security (SEC-007)

Security checklist:

	ITEM	Action	Description	Rationale
☐	Change Password	**Go through computer management gui to change local admin password**	= Change current account pw = Change arbitrary account pw	Default credentials will be attempted.
☐	Local Group Permissions	**Go through user permissions checklist**	= Verifies that everyone is not a local admin for example	Make sure local user permissions aren't screwed.
☐	Install anti-virus	**Install malwarebytes**	= checks sums & reports error	Gives basic security against already known threat
☐	Check Autoruns	**Download, run and look through autoruns.**	= Autoruns gives a comprehensive list of things that run at startup and scheduled tasks	Finds persistence.
☐	Check Hostfile	**C:\Windows\System32\Drivers\etc\hosts**	= hostfile is basically a list of DNS entries checked before DNS	Prevent DNS rebinding attacks.
☐	Disable PSremoting	**PS: Disable-psremoting**	= Prevents powershell remoting	Reduces attack surface.
☐	Disable RDP	**Control Panel > System > Advanved System Settings > Remote**	= Prevents RDP connections to computer	Reduces attack surface.
☐	Disable local GPO	Local Computer Policy > Computer Configuration > Administrative Templates > All Settings Local Computer Policy > User Configuration > Administrative Templates > All Settings	= Disables local GPO's	Having centralized GPO management at the AD is made easier by not having to deal with the exceptions caused by having local GPO's setup. Prevents local GPO's from being modified in an insecure fashion.
☐	Firewall Rules	**Install tinywall Disable outbound traffic**	= Restrict unnecessary traffic on a host basis	Help restrict outbound shells, overall attack surfa
☐	Disable NETBIOS	Network adapter, ipv4, properties, advanced, WINS	= Disable NETBIOS	NETBIOS is unneeded and vulnerable.
☐	Secure needed service(s)	**Go through checklist for specific service(s)**	= Varies	Keeping critical services secure is important.
☐	Remove unneeded service(s)	**Varies**	= Varies	Reducing the attack surface is important.
☐	Run Sigcheck	**Sigcheck -u -s -v C:\ > C:\asdf.txt**	= Outputs list of files with unsigned files, or non-zero detection by virustotal to asdf.txt	Gives list of suspicious files to investigate.
☐	Disable ipv6	**In adapter settings uncheck ipv6**	= Prevents the use of ipv6	Reduces attack surface.

☐	Check routes	**CMD: netstat /r**	= Outputs routing table	Verify that we aren't routing traffic to someplace insecure.
☐	Disable SMB	**PS; set-smbserverconfiguration -enablesmb2protocol $false**	Disables SMB 2	2012 or up
☐	Disable SMB	**PS; set-smbserverconfiguration -enablesmb1protocol $false**	Disables SMB 1	2008 and above
☐	Audit Network Shares	**net share**	Check all drives mapped on a box	Could have a drive not being shown mapped with malicious code
☐	Enable safe Dll search mode	**create the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode registry value and set it to 1 of type DWORD**	Enable DLL safe search mode	Prevents DLLs from being unsafely loaded
☐	Enable Centralized Logging	**Download OSSEC and install**	Centralized logging	Centralized logs

Sysmon