

DIY VM Infrastructure Lab

💡 DIY VM Labs via VMware Workstation are a great way to build and test your own environments for pretty much any project.

In this case, we are going to take the recent Assessment 1 and tweak it for a local VM environment you build from scratch & thus DIY Infrastructure.

Don't worry, we will still use vCenter as our main environment for this course. The nice thing about a local environment is it allows additional practical hands-on practice, and allows you to build/test/demo your own VMware Workstation environments across your classes and self projects (with snapshots!).

This local infrastructure will include the configuration of a fw, domain controller, dhcp server and a windows workstation ... just locally that you build, config and own even more so than Vcenter environments.

Prerequisites

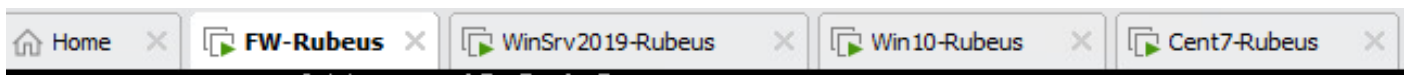
ISOs to Build VMs

Refer to the `X:\ISOs\F22\sys255-265` mounted on every cyber.local workstation via AD GPO (and not your Vcenter environment), and copy over the ISOs onto your cyber.local workstation (which will take a moment, even on our [1 GbE network](#)):

- Pfsense Firewall
- Windows Server
- Windows Client
- CentOS7

Reminder: In Canvas\Module 0.0, there's a Student Resources doc, which contains how to remote to cyber.local via Viewportal + RDP. Best test and confirm this makes sense, otherwise it just means labs will be completed onsite.

Final Objective: To build the Assessment 1 environment on local VMs ==>





Be mindful of your Storage Path as you build new VMs!

Also, when you're done & VMs are powered down in good manner, you can copy them onto a SSD external hard drive which supports USB v3 ... basically providing infrastructure in your backpack.

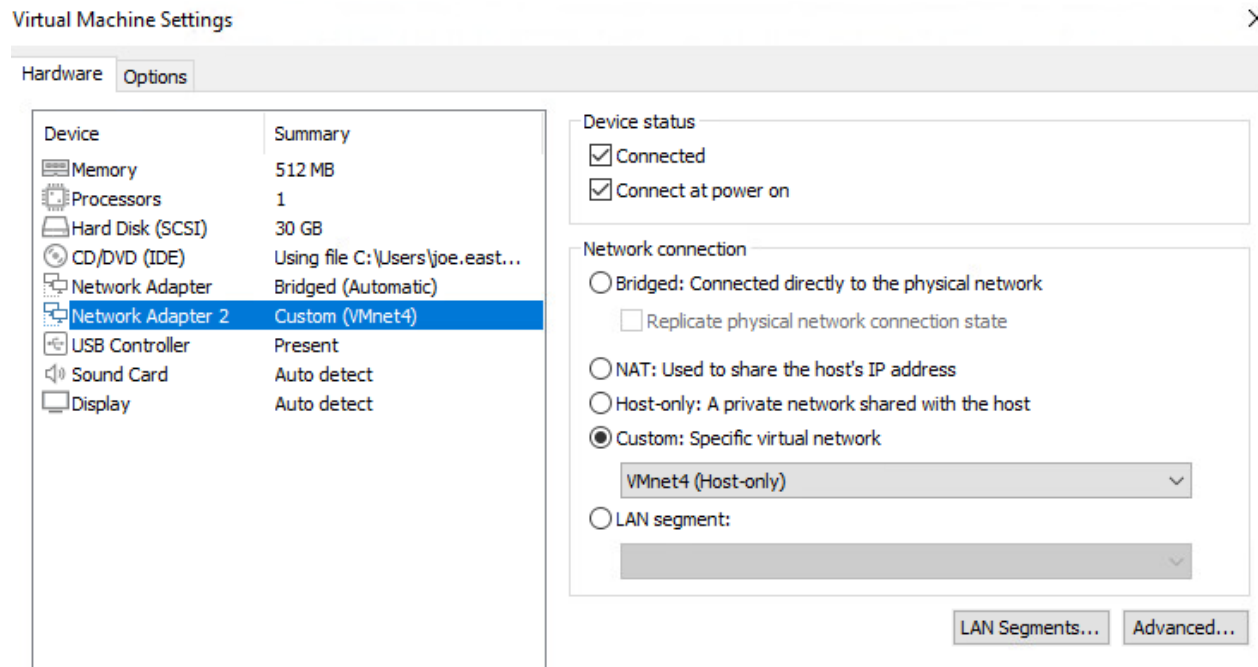
FW-YourName (Pfsense)

You're all familiar with setting up VMs via VMware. So first creating the new Firewall (FW) VM:

- Name VMs with our usual format (ex: FW-Rubeus, AD-Rubeus, etc)
- As for resources (memory, proc, storage) we do not need a lot, and our cyber.local workstations are healthy hosts (32G RAM, SSD SATA storage, i7-level proc).
- For FW (like most Linux/Unix distro's), we usually need just above/near minimums.
- Networking ... This will be the larger "tweak" you'll need to do, though it is straightforward since it uses very similar concepts and processes you're familiar with.

How is Networking different here? Well, instead of selecting pre-built & pre-configured network "cables" via Vcenter01, you'll need to take the same concepts (WAN + LAN on the correct VMs) and apply them using VMware Workstation's adapter and VMnets.


As you go through the FW VM build, make sure the first default VM Network Adapter (i.e. our "WAN") is set to Bridged mode (it is going to be a "Bridge" linking the same traffic/connectivity between that NIC and our cyber.local network). Next, we then Add... (same settings window > select Add > win) a second Network Adapter (i.e. our "LAN") to a custom VMnet:



Pro Tip: Every LAN interface **must** be networked on the **same** custom **VMnet**, similar to vSphere's WAN & LAN setup (i.e. Servers, Win10, Cent = LAN only). Being this will be FW, you will "install" a 2nd NIC to have 1 NIC for "WAN", & 1 NIC for "LAN" ... exactly like your previously FW VM in Vcenter.

If you incur VM networking challenges, then here's one obvious spot to look at (i.e. checking your VM "cabling"). While your VMnet# may change, it is best practice to actually look at the settings to make sure that a) they make sense, and b) they're consistent across every LAN interface. If a Virtual Network subnet is different (say, 10.0.4.0 instead of 10.0.6.0), then that's no big deal ... just re-IP *every LAN interface* to match the Virtual Network's subnet.

How can you find those Virtual Network subnet configs? → Here is the actual VMware Workstation > Edit's *Virtual Network Editor* defining the actual subnet configs for various "LAN" settings (naturally workstations in cyber.local, you don't have Admin privileges to modify those configs #LeastPrivilege. If you have VMware installed on your own system, then you can make this whatever you want ... and number of Prof's do:

 Virtual Network Editor
 ✕

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet1	Host-only	-	Connected	Enabled	192.168.75.0
VMnet4	Host-only	-	Connected	-	10.0.4.0
VMnet5	Host-only	-	Connected	-	10.0.5.0
VMnet6	Host-only	-	Connected	-	10.0.6.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.229.0

Add Network...
Remove Network
Rename Network...

VMnet Information

☐ Bridged (connect VMs directly to the external network)

Bridged to:
Automatic Settings...

☐ NAT (shared host's IP address with VMs)
 NAT Settings...

☒ Host-only (connect VMs internally in a private network)

☒ Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet4

☐ Use local DHCP service to distribute IP address to VMs
 DHCP Settings...

Subnet IP: 10 . 0 . 4 . 0
 Subnet mask: 255 . 255 . 255 . 0

⚠ Administrator privileges are required to modify the network configuration.
Change Settings

Restore Defaults
Import...
Export...
OK
Cancel
Apply
Help

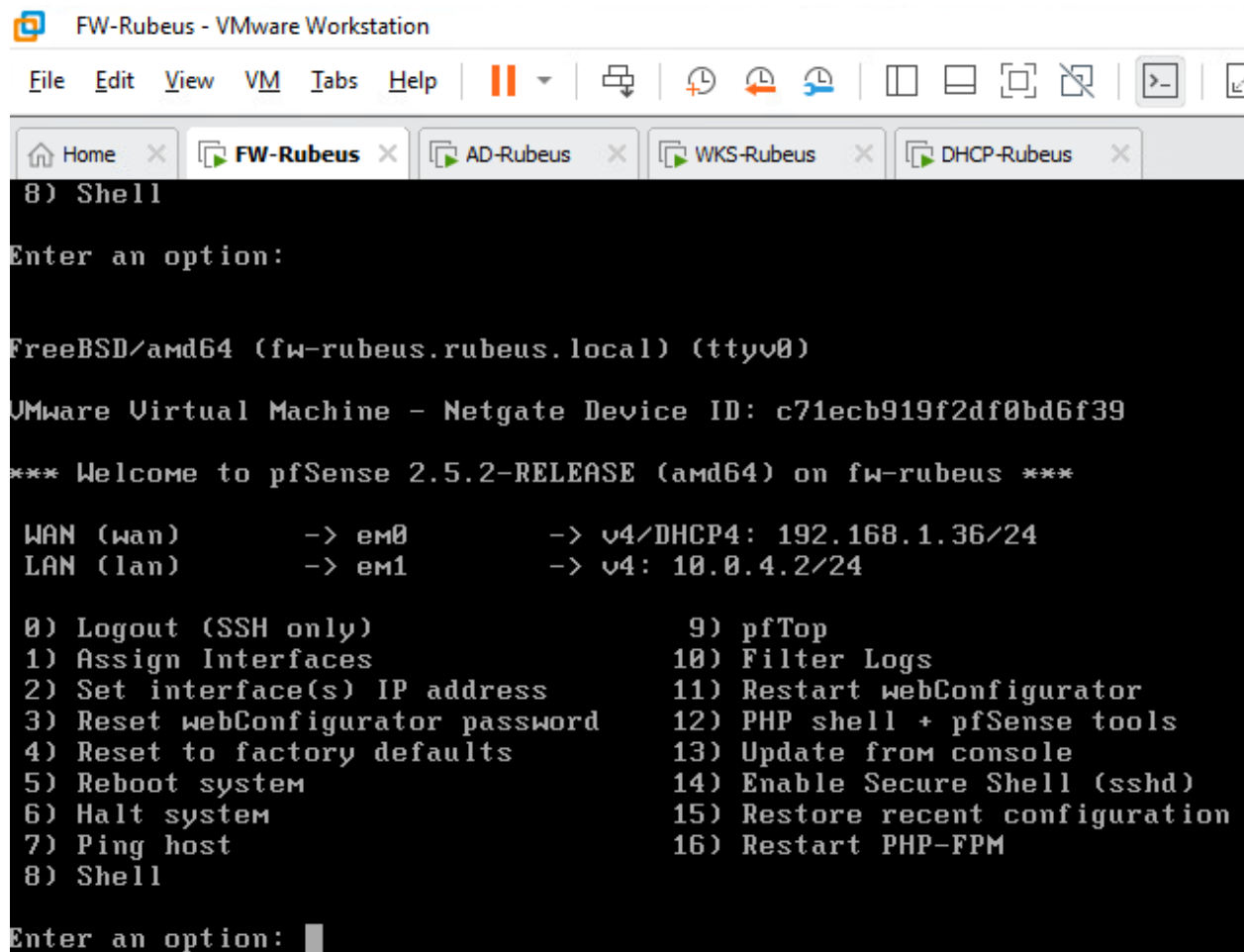
With that, go ahead & select VMnet4 as an example, which shows it is “Host-only” (look at what it is showing us via VMnet Info section ... “connect VMs internally in a private network” ... i.e. our “LAN”), as well as a Network ID of 10.0.4.0/24. Cool, we have everything we need to IP our LAN.

Ok ... now you’re ready to complete the new VM using the Pfsense ISO off your local workstation. It’s not particularly difficult, even if it may be your 1st time doing it. Like similar install config screens & processes, most of them are intuitive.

For this install, using the BIOS setting while installing Pfsense is rather painless (you’ll see it on a screen). When the Pfsense FW install is done, then we are right back to our good friend Pfsense.

With that, there's one thing to keep in mind and that is FW's WAN & LAN IP settings. LAN process is the same you've done numerous times now: assign the 10.0.4.2/24 in your new "host-only" subnet as FW's LAN Gateway IP which all other LAN VMs use for their Gateway IP.

WAN is slightly different, but rather easier tbh. Actually take a look at it ... WAN has a DHCP IP assigned by cyber.local's DHCP service as the WAN NIC is "Bridged" to the cyber.local network. So instead of IP's being assigned via some sheet with Unique Static IPs for Student WAN em0 NIC's ... we are letting DHCP do that work for us! Recall your DHCP server and its scope settings you provided to WKS a couple times now... Gateway, subnet mask, domain, DNS, a leased IP, etc? It's the same exact process going on for all of our local WAN NICs, and cyber.local's DHCP settings take care of all that. #ThanksDHCP!



```
FW-Rubeus - VMware Workstation
File Edit View VM Tabs Help
Home x FW-Rubeus x AD-Rubeus x WKS-Rubeus x DHCP-Rubeus x
8) Shell
Enter an option:
FreeBSD/amd64 (fw-rubeus.rubeus.local) (ttyv0)
VMware Virtual Machine - Netgate Device ID: c71ecb919f2df0bd6f39
*** Welcome to pfSense 2.5.2-RELEASE (amd64) on fw-rubeus ***
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.36/24
LAN (lan)      -> em1      -> v4: 10.0.4.2/24
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell
Enter an option: 
```

With that, we don't need to do anything with WAN.

For LAN, set its LAN interface to **10.0.4.2/24** & no need for upstream gateways, no IPv6, no DHCP server, & keep HTTPS webConfigurator.

Pro Tip: Probably wise for some quick connectivity tests via FW's shell after initial setup for good luck.

WKS-YourName (Win10)

Ok, the new VM process is similar to the FW VM build, except WKS will only use 1 Network Adapter (its default). Make sure WKS is on the right VMnet, and usually assigned 5+Gig RAM, +20 Gig more storage than its default amount, and with 4 Processors (does not matter the make up between number of processors vs. number of cores per proc).

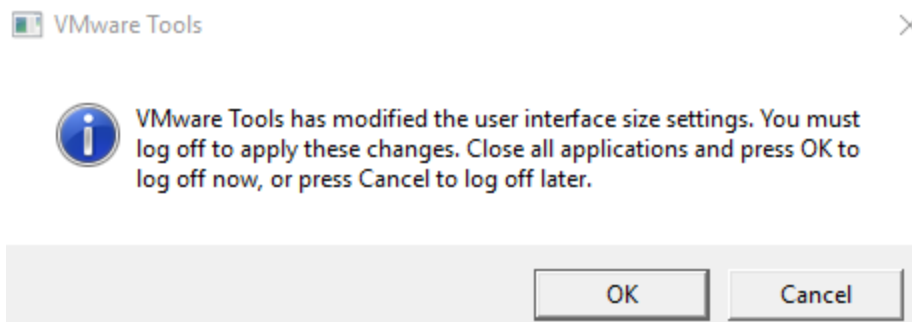
Another heads up: during initial install, you might encounter a message referencing "Cannot find Microsoft software license" ... it's Microsoft "asking" for a license on a device it has access to per BIOS boot order atm: the virtual floppy drive, which is enabled in VM settings by default ... So fix that.

Sweet, now that the WKS VM is completed, power it up & run through its initial setup using the usual yourname-loc as a local account, and assign the usual .100 static IP in the same subnet range.

Pro Tips For VMWare Workstation:

- Ctrl + Alt + Insert == Ctrl + Alt + Delete
- Toolbar > VM > Send Ctrl + Alt + Del
- Ctrl + Alt == gets out of VM window to physical host
- Ctrl + G == gets inside VM window from physical host

FYI: VMware Workstation installs VMware Tools onto Window VMs, which allows copying/pasting between Windows VMs and desktops, dynamic display modification, and other fun "extras". There's no need to log off yet for these display settings, if you get this info window:



Ok, now it's back to the usual flow of things ...

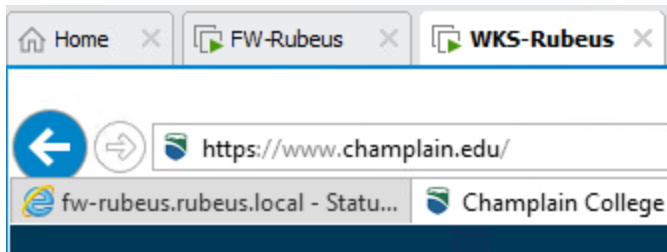
On WKS, setup FW via its web GUI config:

- Hostname = FW-YourName
- Local named privileged -loc account
- Similar configs from Lab01
 - **Except WAN Adapter = DHCP**

Also, since these are fresh installs straight from Microsoft, I would **highly recommend disabling Windows Auto Update** (yes, updates are necessary ... and no, we don't want terabytes of unnecessary updates flooding our precious network).

- **Start > Services > Windows Update > Properties > Type = Disabled > Stop > OK/Close out**

Browse to www.champlain.edu on WKS for a network connectivity spot check:



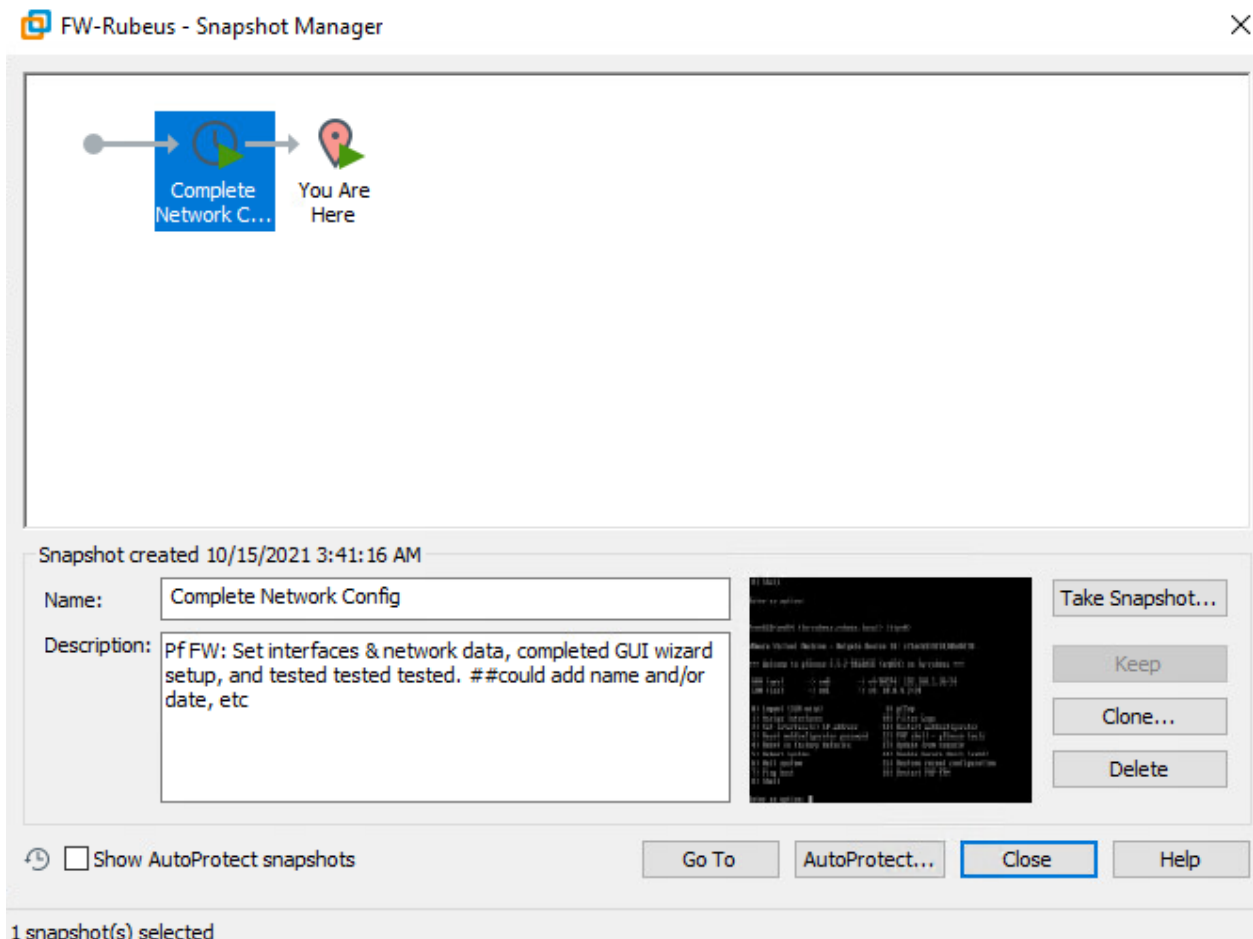
Snapshots

Congrats ... you just created & tested another successful FW setup. It is always a good idea to make a quick VMware Workstation snapshot of the FW as a backup of a “known good state”. Snapshots are super helpful and seem like a game's “save point”, but we should not use them completely blind without knowing how they work, and how you manage them.

Best practice → Power down > make a snapshot with a quick note > power up. Otherwise, if you make snapshots of live systems, you capture the OS's **live state** at that point of time (if memory is live, then snapshots take local host disk space for every snapshot created), it is not instantaneous (comes with own progress bar in bottom of VMware Workstation window, so wait until completed), and you are tempting fate involving Windows AD's replication of objects between Domain Servers & Clients. #You'veBeenWarned

Additionally, power sequence is a thing for Windows Active Directory (AD) connected hosts: power down AD Clients, & then any Member Servers (joined to domain but are not DC's), and

finally AD Domain Controllers servicing your domain (again, because of replication), and power them up in reverse order.



Now you're ready to build & test your new environment using the "You Are Here" current VM state, and can roll back to "Complete Network Config" Snapshot if needed.

AD-YourName (Server 2019)

- Create new VM w/ usual VM name & settings
 - Add 6+ RAM & 4-Proc because you know Windows likes that > power on
- Hostname: AD-yourname
- IP: 10.0.4.6/24
- Gateway = FW's LAN IP
- Initial DNS Server = FW's LAN IP
- Using "sconfig" via Powershell > Set Windows Update = Manual > Exit
- Install ADDS role
- Promote to a Domain Controller via new Domain: yourname.local

- Create a regular named AD user, and create a power AD -adm:
 - first.lastname
 - first.lastname-adm
- DNS Zones + Records
- Test, test, test

DHCP-YourName (CentOS7)

- Create new VM w/ usual VM name & settings, then power on
- Install > Installation Summary
 - System : Installation Destination
 - Select the device to install to > get Check > Done
 - Network & Hostname
 - Auto Connection = On
 - Could try the GUI for similar network adapter settings, or usual CLI ... your choice > Done
 - Begin Installation > Set Root Password > Done
 - Voila ... a brand new Linux VM is born!
- OS hostname: dhcp-yourname
- IP: 10.0.4.66/24
- Gateway: FW's LAN IP
- Initial DNS: FW's LAN IP
- Search domain: yourname.local
- Named sudo user
- DHCP Service Configuration: identical to the one created in the DHCP Lab with the following exceptions:
 - IP address for the local DNS server
 - DHCP Pool: 200 to 225
- Test w/ nslookup
- Just like the DHCP lab earlier, for Deliv05 re-IP DHCP server to 10.0.4.8 and then update necessary items to show DHCP Lease modifications

WKS-YourName (Win10)

- Create new VM w/ usual VM name & settings
 - Add some RAM & Proc because you know Windows likes that > power on
- OS Hostname = WKS-YourName
- Eventual IP = Dynamically assigned
- Subnet = /24
- Gateway = FW's LAN IP
- Initial DNS = FW's LAN IP
- Turn off windows updates
- Create named "power" -loc account

- Then use it going forward for initial setup pre-AD join
- Join WKS to AD domain yourname.local
 - Then use the AD -adm account going forward post-AD join

Deliverables

Deliverable 1: On WKS using powershell or cmd.exe, provide screenshots similar to the one below that shows:

- whoami (1 Point)
looking for a named domain user account
- ipconfig /all (1 Points)
looking for DHCP provided IP in the 200-250 range, correct gateway, DNS, domain as well as a properly named host
- tracert -h 3 champlain.edu (1 Point)
looking for first three hops through your LAN default gateway, the SYS255 default gateway and the CYBER.LOCAL default gateway

WKS-Rubeus - VMware Workstation

File Edit View VM Tabs Help

Home FW-Rubeus WKS-Rubeus AD-Rubeus DHCP-Rubeus

Windows PowerShell

```
PS C:\Users\rubeus-adm> whoami
rubeus\rubeus-adm
PS C:\Users\rubeus-adm> ipconfig /all

Windows IP Configuration

Host Name . . . . . : wks-rubeus
Primary Dns Suffix . . . . . : rubeus.local
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : rubeus.local

Ethernet adapter Ethernet0:

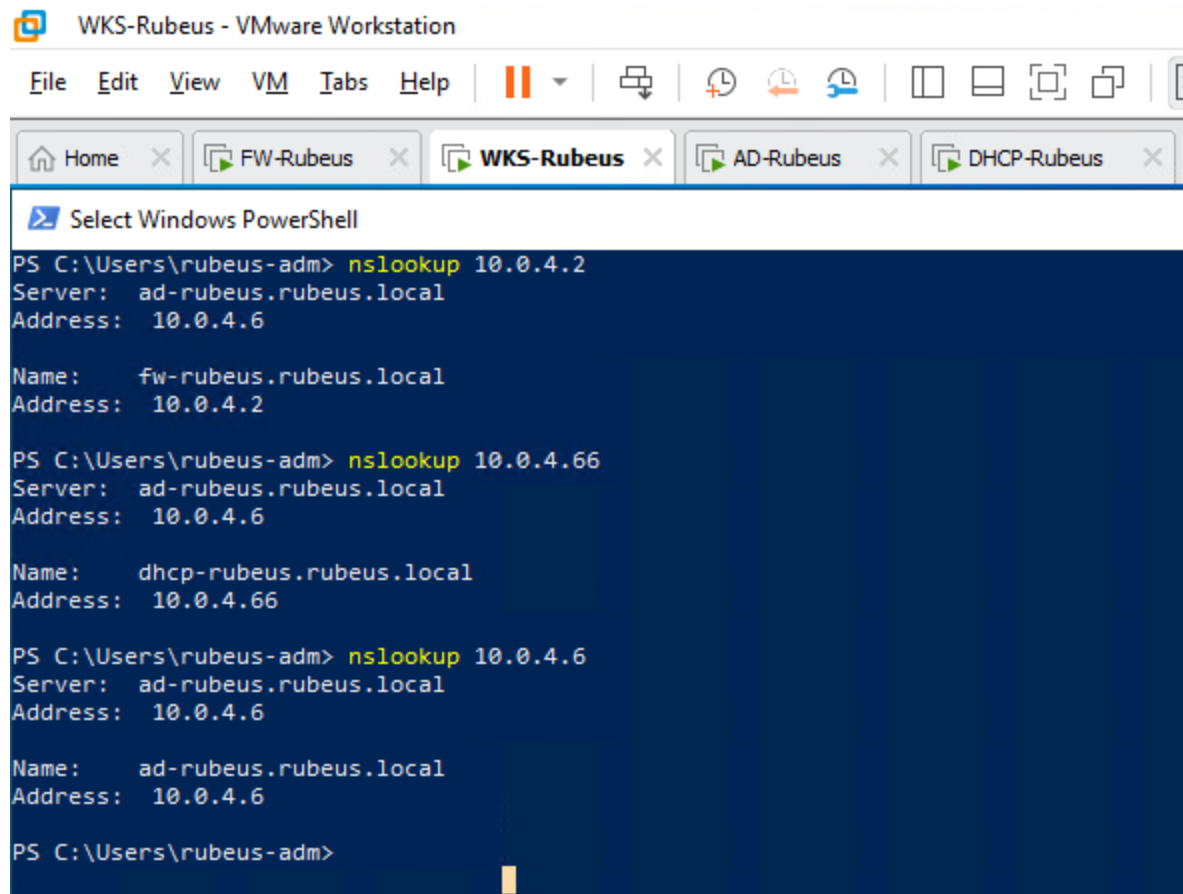
Connection-specific DNS Suffix . : rubeus.local
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-5C-41-6E
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 10.0.4.200(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Friday, October 15, 2021 5:46:30 AM
Lease Expires . . . . . : Friday, October 15, 2021 5:46:30 PM
Default Gateway . . . . . : 10.0.4.2
DHCP Server . . . . . : 10.0.4.66
DNS Servers . . . . . : 10.0.4.6
NetBIOS over Tcpip. . . . . : Enabled
PS C:\Users\rubeus-adm> tracert -h 3 champlain.edu

Tracing route to champlain.edu [208.115.107.132]
over a maximum of 3 hops:

 1  <1 ms    <1 ms    <1 ms  fw-rubeus.rubeus.local [10.0.4.2]
 2   1 ms     1 ms     1 ms   192.168.1.250
 3  31 ms     1 ms     <1 ms  192.168.9.254

Trace complete.
PS C:\Users\rubeus-adm>
```

Deliverable 2: Provide a screenshot that shows a nslookup/PTR lookup of the following IP addresses from WKS (1 points):
10.0.6.2, 10.0.6.6, 10.0.6.66. Looking for appropriately named A records. Server should not be "unknown".



The screenshot shows the VMware Workstation interface with the 'WKS-Rubeus' virtual machine selected. A Windows PowerShell window is open, displaying the results of three nslookup commands. The first command for 10.0.4.2 returns 'ad-rubeus.rubeus.local' and '10.0.4.6', with a PTR record 'fw-rubeus.rubeus.local'. The second command for 10.0.4.66 returns 'ad-rubeus.rubeus.local' and '10.0.4.6', with a PTR record 'dhcp-rubeus.rubeus.local'. The third command for 10.0.4.6 returns 'ad-rubeus.rubeus.local' and '10.0.4.6', with a PTR record 'ad-rubeus.rubeus.local'. The server for all lookups is 'ad-rubeus.rubeus.local'.

```
PS C:\Users\rubeus-adm> nslookup 10.0.4.2
Server: ad-rubeus.rubeus.local
Address: 10.0.4.6

Name: fw-rubeus.rubeus.local
Address: 10.0.4.2

PS C:\Users\rubeus-adm> nslookup 10.0.4.66
Server: ad-rubeus.rubeus.local
Address: 10.0.4.6

Name: dhcp-rubeus.rubeus.local
Address: 10.0.4.66

PS C:\Users\rubeus-adm> nslookup 10.0.4.6
Server: ad-rubeus.rubeus.local
Address: 10.0.4.6

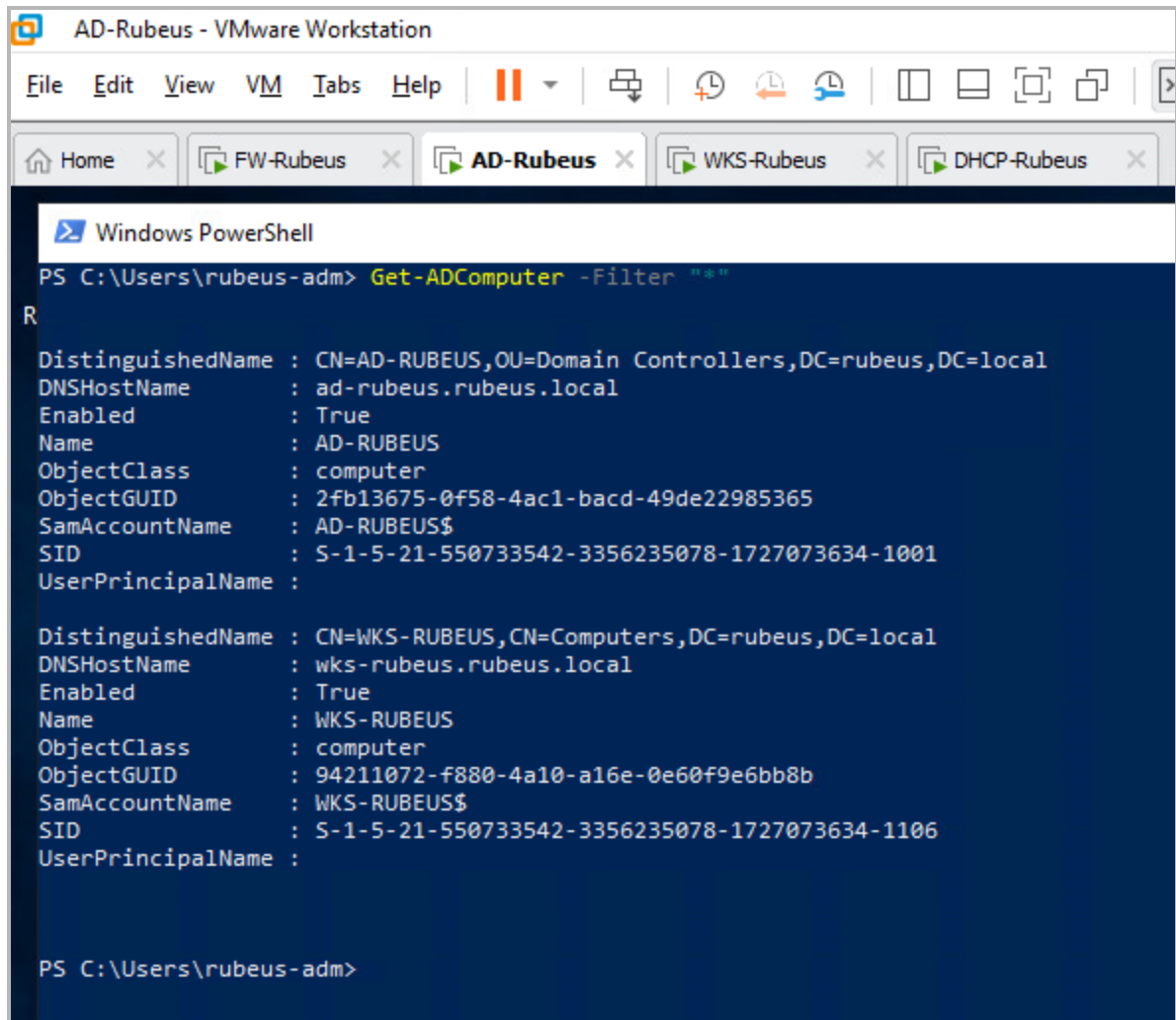
Name: ad-rubeus.rubeus.local
Address: 10.0.4.6

PS C:\Users\rubeus-adm>
```

Deliverable 3: On AD as the named -adm domain admin, provide the output of the following commands:

- `Get-ADComputer -Filter "*" (1 points)`

Looking for AD and WKS and you better be logged in as a named administrative user.



```
PS C:\Users\rubeus-adm> Get-ADComputer -Filter "*"

R
DistinguishedName : CN=AD-RUBEUS,OU=Domain Controllers,DC=rubeus,DC=local
DNSHostName       : ad-rubeus.rubeus.local
Enabled           : True
Name              : AD-RUBEUS
ObjectClass       : computer
ObjectGUID        : 2fb13675-0f58-4ac1-bacd-49de22985365
SamAccountName    : AD-RUBEUS$
SID               : S-1-5-21-550733542-3356235078-1727073634-1001
UserPrincipalName :

DistinguishedName : CN=WKS-RUBEUS,CN=Computers,DC=rubeus,DC=local
DNSHostName       : wks-rubeus.rubeus.local
Enabled           : True
Name              : WKS-RUBEUS
ObjectClass       : computer
ObjectGUID        : 94211072-f880-4a10-a16e-0e60f9e6bb8b
SamAccountName    : WKS-RUBEUS$
SID               : S-1-5-21-550733542-3356235078-1727073634-1106
UserPrincipalName :

PS C:\Users\rubeus-adm>
```

- `Get-ADGroup (1 points)`

Looking for the named admin and user. Use the following Powershell commands:

- `Get-ADGroup -Identity "Domain Users" -Property member`
- `Get-ADGroup -Identity "Domain Admins" -Property member`

AD-Rubeus - VMware Workstation

File Edit View VM Tabs Help

Home x FW-Rubeus x AD-Rubeus x WKS-Rubeus x DHCP-Rubeus x

Windows PowerShell

```
PS C:\Users\rubeus-adm> Get-ADGroup -identity "Domain Users" -Property member
R
DistinguishedName : CN=Domain Users,CN=Users,DC=rubeus,DC=local
GroupCategory     : Security
GroupScope        : Global
Name              : Domain Users
ObjectClass       : group
ObjectGUID        : cde10c12-6091-40db-b7f3-e99a76ee963a
SamAccountName    : Domain Users
SID               : S-1-5-21-550733542-3356235078-1727073634-513

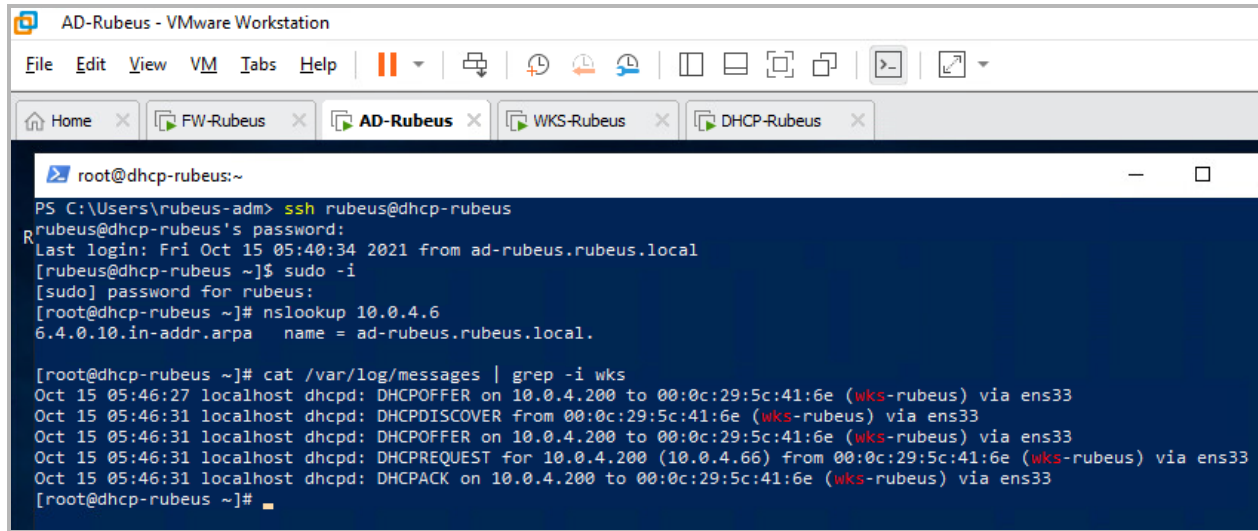
PS C:\Users\rubeus-adm> Get-ADGroup -identity "Domain Admins" -Property member

DistinguishedName : CN=Domain Admins,CN=Users,DC=rubeus,DC=local
GroupCategory     : Security
GroupScope        : Global
member            : {CN=rubeus-adm,CN=Users,DC=rubeus,DC=local, CN=Administrator,CN=Users,DC=rubeus,DC=local}
Name              : Domain Admins
ObjectClass       : group
ObjectGUID        : febbffe1-c02b-4287-bfb2-c93cf05c36b8
SamAccountName    : Domain Admins
SID               : S-1-5-21-550733542-3356235078-1727073634-512

PS C:\Users\rubeus-adm>
```

Deliverable 4: On DHCP, provide a screenshot showing the following:

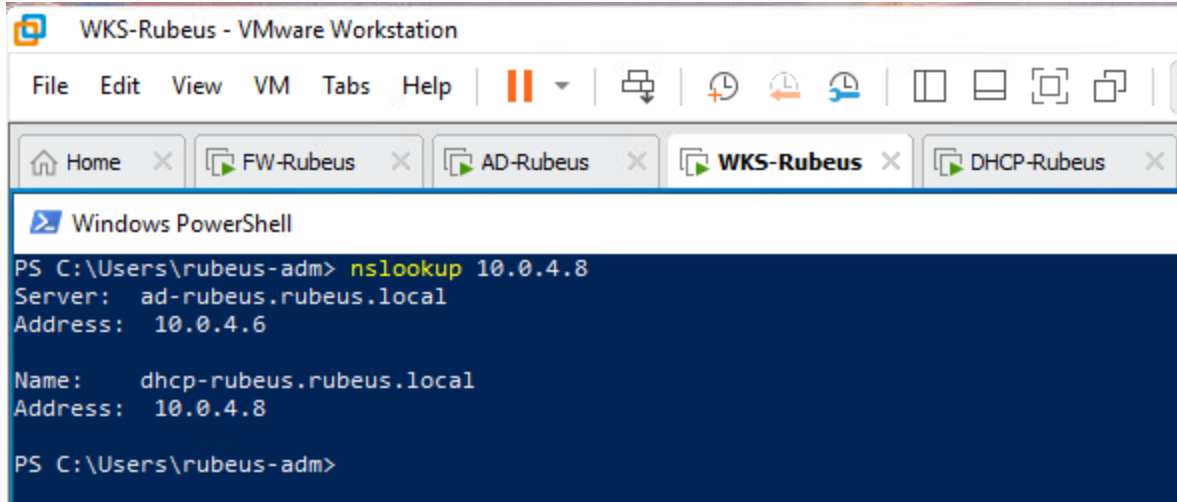
- login as a named user and sudo -i to root (1 points)
 - nslookup 10.0.4.6 (1 point)
 - cat /var/log/messages | grep -i wks (1 points)
- looking for indications that WKS received an IP address from DHCP.



```
root@dhcp-rubeus:~
PS C:\Users\rubeus-admin> ssh rubeus@dhcp-rubeus
rubeus@dhcp-rubeus's password:
Last login: Fri Oct 15 05:40:34 2021 from ad-rubeus.rubeus.local
[rubeus@dhcp-rubeus ~]$ sudo -i
[sudo] password for rubeus:
[root@dhcp-rubeus ~]# nslookup 10.0.4.6
6.4.0.10.in-addr.arpa   name = ad-rubeus.rubeus.local.

[root@dhcp-rubeus ~]# cat /var/log/messages | grep -i wks
Oct 15 05:46:27 localhost dhcpd: DHCPOFFER on 10.0.4.200 to 00:0c:29:5c:41:6e (wks-rubeus) via ens33
Oct 15 05:46:31 localhost dhcpd: DHCPDISCOVER from 00:0c:29:5c:41:6e (wks-rubeus) via ens33
Oct 15 05:46:31 localhost dhcpd: DHCPOFFER on 10.0.4.200 to 00:0c:29:5c:41:6e (wks-rubeus) via ens33
Oct 15 05:46:31 localhost dhcpd: DHCPREQUEST for 10.0.4.200 (10.0.4.66) from 00:0c:29:5c:41:6e (wks-rubeus) via ens33
Oct 15 05:46:31 localhost dhcpd: DHCPACK on 10.0.4.200 to 00:0c:29:5c:41:6e (wks-rubeus) via ens33
[root@dhcp-rubeus ~]#
```

Deliverable 5 (1 Point). On DHCP, modify its IP to 10.0.4.8 & update necessary configs & DNS records. After obtaining new ipconfig data on WKS, run an nslookup 10.0.6.8 on it. Looking for indications that you adjusted the PTR and A records for DHCP. Provide a screenshot similar to the following:



```
WKS-Rubeus - VMware Workstation
File Edit View VM Tabs Help
[Icons: Pause, Copy, Paste, Undo, Redo, Window Management]
Home x FW-Rubeus x AD-Rubeus x WKS-Rubeus x DHCP-Rubeus x
Windows PowerShell
PS C:\Users\rubeus-adm> nslookup 10.0.4.8
Server: ad-rubeus.rubeus.local
Address: 10.0.4.6

Name: dhcp-rubeus.rubeus.local
Address: 10.0.4.8

PS C:\Users\rubeus-adm>
```