# SYS-255 - Assessment 1

💡 What is an assessment? In this case, it is a practical hands on exercise to see if you can build a subset of your week 5 environment on your own. This will include the configuration of a firewall, domain controller, dhcp server and a windows workstation.

Recommendation, read the assessment from front to end before starting.

## Rules for this assessment:

- Open internet searching, open notes, but no open classmates or outside support. You are ON YOUR OWN for the submission, so no communications with others.

# Assessment Grading

Submitted within 24 hours from class end = -0%

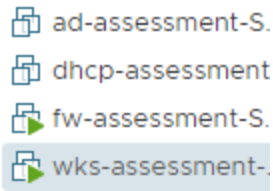
Submitted after 24-47 hours from class end = -15%

Submitted after 48 hours from class end = -25%

Not submitted before next class = -100%

## Hostnames

You have four new Vsphere systems, use the following hostnames:



| vmware virtual machine name | configured hostname |
|---|---|
| ad-assessment1 | ad02-yourname |
| dhcp-assessment1 | dhcp02-yourname |
| wks-assessment1 | wks02-yourname |
| fw-assessment | fw02-yourname |

## VMWare Networking

Make sure that ad02, dhcp02 and wks02 are all on your SYS255-LAN student Network.

> 💣 Be aware, internal LAN IP addresses and system hostnames may have some changes from your previous configurations.

## fw02 Requirements

Your firewall should be configured exactly the same (including unique WAN IP's), other than the updated hostname.

## ad02 Requirements

VMWare Network Settings:

- Hostname = ad02-yourname
- IP = 10.0.5.**6** /24
- Gateway = fw02's LAN interface
- Initial DNS = fw02's LAN interface
- The AD DS Role has already been installed, so when you are ready, promote ad02 to become a new Domain Controller in your new AD: yourname.local
- Create a named domain regular <*first.lastname*> user, and named domain admin <*first.lastname-adm*> user
- All LAN interfaces need to resolution names

## dhcp02 Requirements

- Hostname = dhcp02-yourname
- IP = 10.0.5.**4**

- Netmask = 255.255.255.0
- Gateway = fw02's LAN interface
- DNS = Local DNS Server IP
- Search domain = yourname.local
- Create a named sudo user called <*yourname*>
- DHCP Service Configuration is configured <u>exactly</u> the same, other than local DNS Server IP, scope 150-175, and using default leases.

## wks02 Requirements

- Hostname = wks02-yourname
- Eventual IP = Automatically assigned IP configurations via DHCP
- Joined to your name.local AD domain

## Deliverables

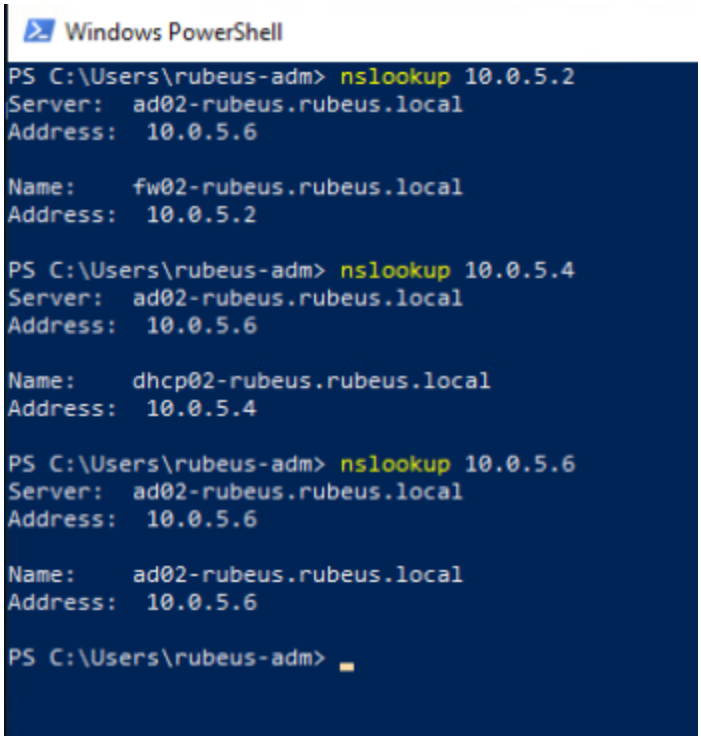
💡 Deliverables are the similar synapsis + targeted screenshots as prior labs..

```
Deliverable 1:  On wks02 as a domain user using powershell, provide
screenshots similar to the one below that shows:
   ● whoami (1 Point)
     looking for a named domain user account
   ● ipconfig /all (2 Points)
     looking for DHCP provided ip in the 150-175 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
```

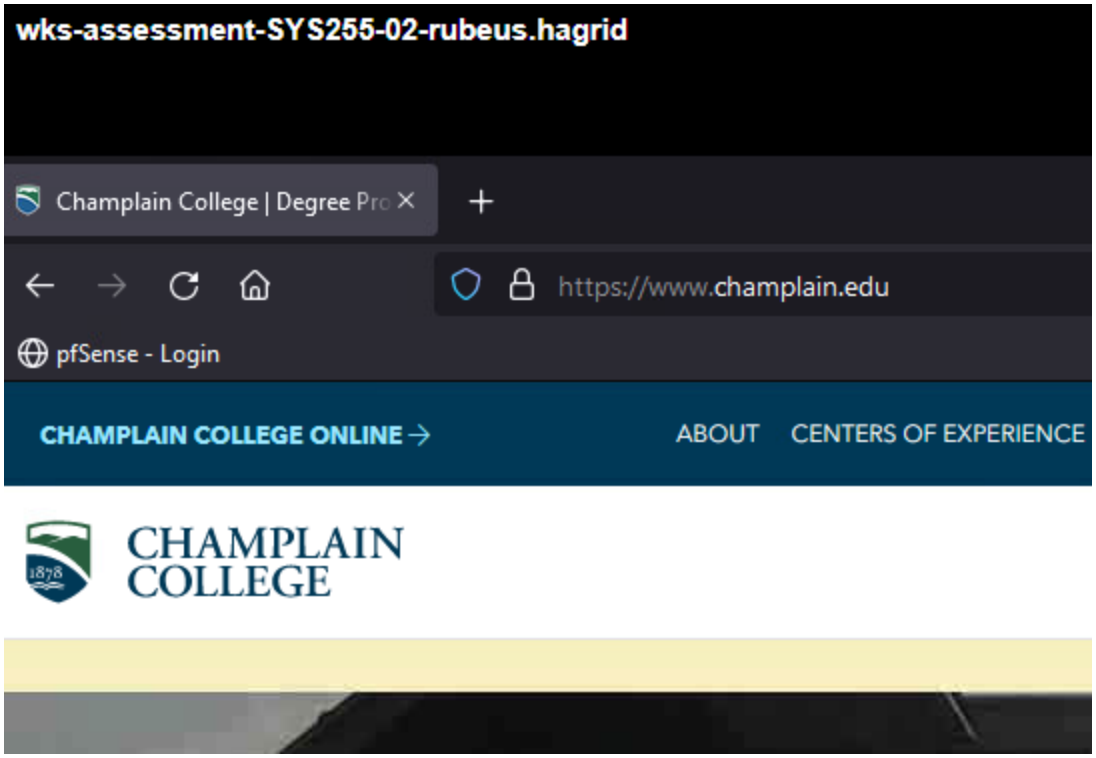
Windows PowerShell

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

Windows IP Configuration

   Host Name . . . . . . . . . . . . : wks02-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. . . . . . . . . : 00-50-56-B3-E2-A3
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 10.0.5.150(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Saturday, October 2, 2021 12:41:53 PM
   Lease Expires . . . . . . . . . . : Sunday, October 3, 2021 12:41:53 AM
   Default Gateway . . . . . . . . . : 10.0.5.2
   DHCP Server . . . . . . . . . . . : 10.0.5.4
   DNS Servers . . . . . . . . . . . : 10.0.5.6
   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  fw02-rubeus.rubeus.local [10.0.5.2]
  2     1 ms    <1 ms    <1 ms  10.0.17.2
  3     6 ms     1 ms     1 ms  192.168.4.252

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

Deliverable 2: Provide a screenshot that shows a nslookup/PTR lookup of the following IP addresses from WKS02 (4 points): 10.0.5.2, 10.0.5.4, 10.0.5.6. Looking for appropriately named A records. Server should not be "unknown".




Deliverable 3: Provide a screenshot showing a browsing session between wks02 and champlain.edu,& make sure to grab the wks02 banner for your screenshot.(2 Points)


wks-assessment-SYS255-02-rubeus.hagrid
Champlain College | Degree Pro
https://www.champlain.edu
pfSense - Login
CHAMPLAIN COLLEGE ONLINE
ABOUT
CENTERS OF EXPERIENCE
CHAMPLAIN COLLEGE

Deliverable 4: On AD02, as the named domain admin, provide the output of the following commands:

- Get-ADComputer -Filter "*" (2 points)

  Looking for ad02 and wks02, and being logged in as a named administrative user.

  Windows PowerShell

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


DistinguishedName : CN=AD02-RUBEUS,OU=Domain Controllers,DC=rubeus,DC=local
DNSHostName       : ad02-rubeus.rubeus.local
Enabled           : True
Name              : AD02-RUBEUS
ObjectClass       : computer
ObjectGUID        : 4242026a-3e0e-4ab1-8339-839e1b8ec17f
SamAccountName    : AD02-RUBEUS$
SID               : S-1-5-21-772654505-3620324312-3824521170-1000
UserPrincipalName :

DistinguishedName : CN=WKS02-RUBEUS,CN=Computers,DC=rubeus,DC=local
DNSHostName       : wks02-rubeus.rubeus.local
Enabled           : True
Name              : WKS02-RUBEUS
ObjectClass       : computer
ObjectGUID        : a88345df-e9ba-4220-a29e-e68c51c61e3e
SamAccountName    : WKS02-RUBEUS$
SID               : S-1-5-21-772654505-3620324312-3824521170-1105
UserPrincipalName :
```

- 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

```
Windows PowerShell
PS C:\Users\rubeus-adm> Get-ADGroup -Identity "Domain Users" -Property member


DistinguishedName : CN=Domain Users,CN=Users,DC=rubeus,DC=local
GroupCategory     : Security
GroupScope        : Global
Name              : Domain Users
ObjectClass       : group
ObjectGUID        : fd735406-3bb7-4ced-90d6-0fdf517fc80c
SamAccountName    : Domain Users
SID               : S-1-5-21-772654505-3620324312-3824521170-513



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        : a754a451-13d2-44fe-bb6e-38d1626e0c74
SamAccountName    : Domain Admins
SID               : S-1-5-21-772654505-3620324312-3824521170-512



PS C:\Users\rubeus-adm> I love Powershell!  =)
```

Deliverable 5: On DHCP02, provide a screenshot (with vSphere dhcp02 banner) showing the following:

- login as a named user and sudo -i to root (2 points)
- nslookup 10.0.5.6 (1 point)
- cat /var/log/messages | grep -i wks (2 points)
  looking for indications that WKS02 received an IP address from DHCP02.

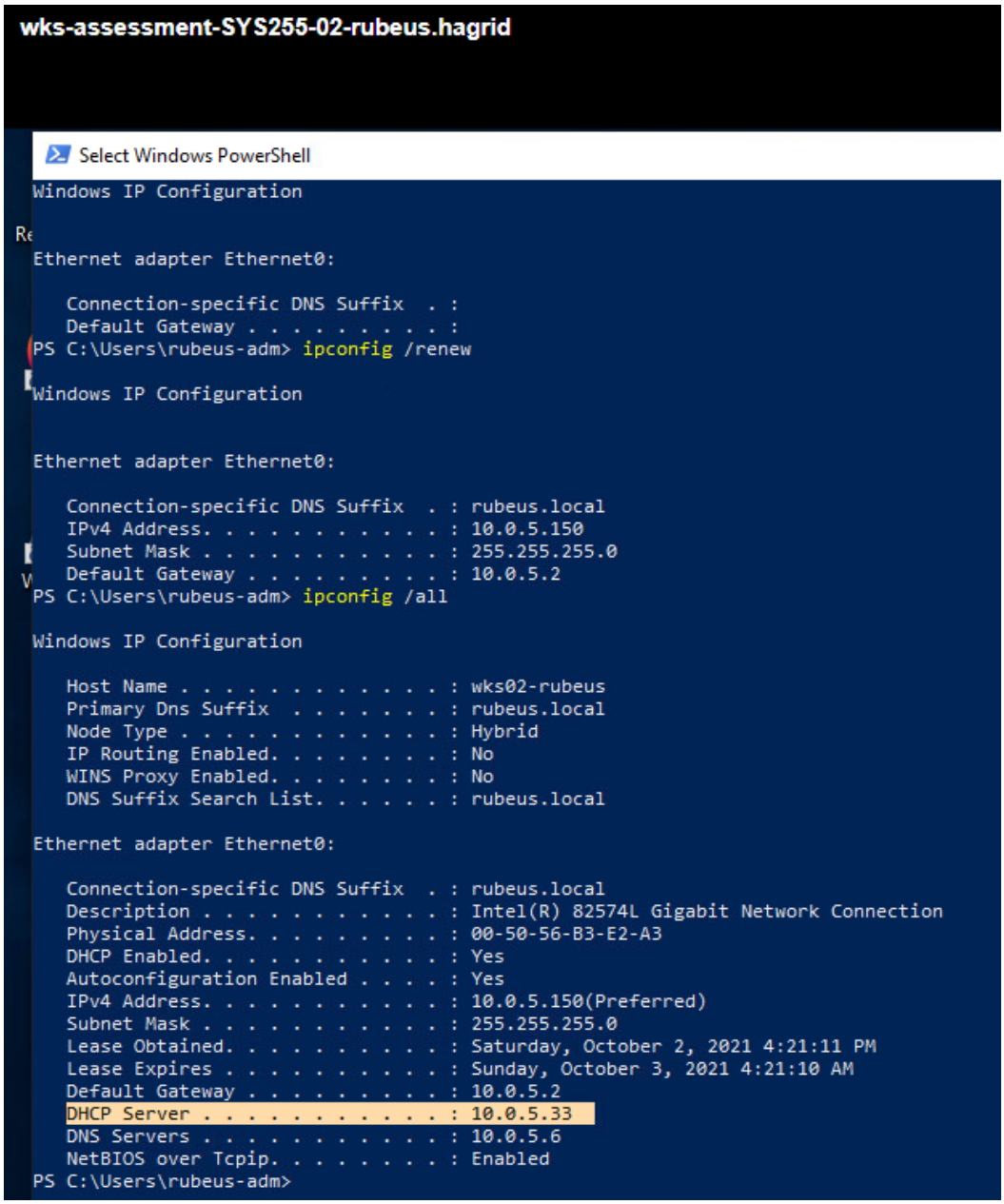
```
dhcp-assessment-SYS255-02-rubeus.hagrid                    Enforce US Keyboard Layout   View Fu

[rubeus@dhcp02-rubeus ~]$ sudo -i
[sudo] password for rubeus:
[root@dhcp02-rubeus ~]# nslookup 10.0.5.6
6.5.0.10.in-addr.arpa   name = ad02-rubeus.rubeus.local.

[root@dhcp02-rubeus ~]# cat /var/log/messages | grep wks
Oct  2 15:41:38 localhost dhcpd: DHCPOFFER on 10.0.5.150 to 00:50:56:b3:e2:a3 (wks02-rubeus) via ens
192
Oct  2 15:41:38 localhost dhcpd: DHCPREQUEST for 10.0.5.150 (10.0.5.4) from 00:50:56:b3:e2:a3 (wks02
-rubeus) via ens192
Oct  2 15:41:38 localhost dhcpd: DHCPACK on 10.0.5.150 to 00:50:56:b3:e2:a3 (wks02-rubeus) via ens19
2
Oct  2 15:41:49 localhost dhcpd: DHCPRELEASE of 10.0.5.150 from 00:50:56:b3:e2:a3 (wks02-rubeus) via
 ens192 (found)
Oct  2 15:41:53 localhost dhcpd: DHCPOFFER on 10.0.5.150 to 00:50:56:b3:e2:a3 (wks02-rubeus) via ens
192
Oct  2 15:41:53 localhost dhcpd: DHCPREQUEST for 10.0.5.150 (10.0.5.4) from 00:50:56:b3:e2:a3 (wks02
-rubeus) via ens192
Oct  2 15:41:53 localhost dhcpd: DHCPACK on 10.0.5.150 to 00:50:56:b3:e2:a3 (wks02-rubeus) via ens19
2
[root@dhcp02-rubeus ~]# _
```

Deliverable 6 (2 Points).

- Re-configure DHCP02 to have the IP address of: 10.0.5.**33**
- Make sure you update the A and PTR records for DHCP02 IP in DNS
- On WKS02, release and renew your ip address
    - ipconfig /release
    - ipconfig /renew

Provide a screenshot that similar to the one below that shows ipconfig /all

looking for a new DHCP server as well as a valid IP address



Deliverable 7 (1 Point). On WKS02, run an nslookup 10.0.5.**33**. Looking for indications that you adjusted the PTR and A records for dhcp02. Provide a screenshot similar to the following:

Windows PowerShell

```
PS C:\Users\rubeus-adm> nslookup 10.0.5.33
Server:  ad02-rubeus.rubeus.local
Address:  10.0.5.6

Name:    dhcp02-rubeus.rubeus.local
Address:  10.0.5.33

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