

David Thomsen

SYS-255

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

- whoami (1 Point)
- ipconfig /all (1 Points)
- tracert -h 3 champlain.edu (1 Point)

```
C:\Users\david.thomsen>whoami
wks-david\david.thomsen

C:\Users\david.thomsen>ipconfig /all

Windows IP Configuration

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

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : david.local
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-66-E3-BF
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::f476:18b4:4fca:4664%3(Preferred)
IPv4 Address. . . . . : 10.0.4.200(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Sunday, November 28, 2021 4:28:19 PM
Lease Expires . . . . . : Monday, November 29, 2021 4:28:19 AM
Default Gateway . . . . . : 10.0.4.2
DHCP Server . . . . . : 10.0.4.66
DHCPv6 IAID . . . . . : 100666409
DHCPv6 Client DUID. . . . . : 00-01-00-01-29-2D-C7-A2-00-0C-29-66-E3-BF
DNS Servers . . . . . : 10.0.4.6
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\david.thomsen>tracert -h 3 champlain.edu

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

 0  <1 ms    <1 ms    <1 ms    fw-david.david.local [10.0.4.2]
 1  1 ms     1 ms     1 ms     192.168.7.250
 2  1 ms     1 ms     1 ms     192.168.9.254

Trace complete.
```

Deliverable 2: Provide a screenshot that shows a nslookup/PTR lookup of the following IP addresses from WKS (1 points):
10.0.4.2, 10.0.4.6, 10.0.4.66. Looking for appropriately named A records. Server should not be "unknown".

```
C:\Users\david.thomsen>nslookup 10.0.4.2
Server:  ad-david.david.local
Address: 10.0.4.6

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


C:\Users\david.thomsen>nslookup 10.0.4.6
Server:  ad-david.david.local
Address: 10.0.4.6

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


C:\Users\david.thomsen>nslookup 10.0.4.66
Server:  ad-david.david.local
Address: 10.0.4.6

Name:    dhcp-david.david.local
Address: 10.0.4.66
```

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

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

```
PS C:\Users\david.thomsen-adm> Get-ADComputer -Filter "*"

DistinguishedName : CN=AD-DAVID,OU=Domain Controllers,DC=david,DC=local
DNSHostName       : AD-david.david.local
Enabled           : True
Name              : AD-DAVID
ObjectClass       : computer
ObjectGUID        : 185c04cc-93c2-49da-a3e6-8ddbce98f1d9
SamAccountName    : AD-DAVID$
SID               : S-1-5-21-4131893085-2543218818-4286819957-1001
UserPrincipalName :

DistinguishedName : CN=WKS-DAVID,CN=Computers,DC=david,DC=local
DNSHostName       : WKS-david.david.local
Enabled           : True
Name              : WKS-DAVID
ObjectClass       : computer
ObjectGUID        : 19977b2f-f29a-4388-a476-2613621f2b10
SamAccountName    : WKS-DAVID$
SID               : S-1-5-21-4131893085-2543218818-4286819957-1106
UserPrincipalName :
```

- Get-ADGroup(1 points)

```
PS C:\Users\david.thomsen-adm> Get-ADGroup -identity "Domain Users"-Property member

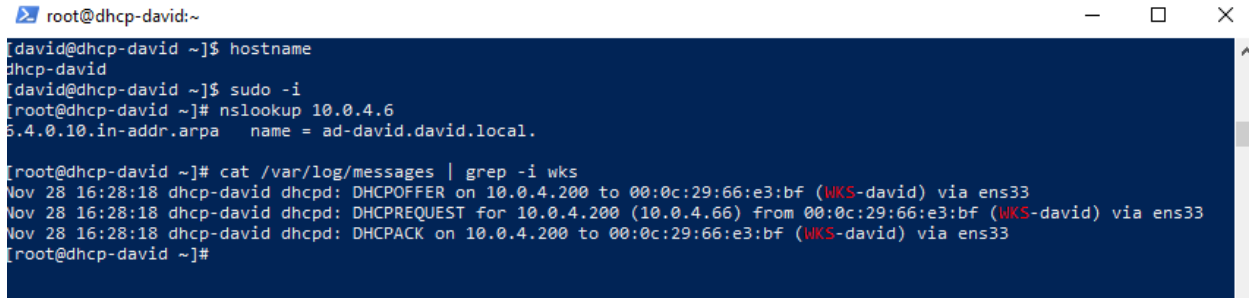
DistinguishedName : CN=Domain Users,CN=Users,DC=david,DC=local
GroupCategory     : Security
GroupScope        : Global
Name              : Domain Users
ObjectClass       : group
ObjectGUID        : 14d6744b-aebe-4957-ad6a-e12f67533182
SamAccountName    : Domain Users
SID               : S-1-5-21-4131893085-2543218818-4286819957-513

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

DistinguishedName : CN=Domain Admins,CN=Users,DC=david,DC=local
GroupCategory     : Security
GroupScope        : Global
member            : {CN=david.thomsen-adm,CN=Users,DC=david,DC=local, CN=Administrator,CN=Users,DC=david,DC=local}
Name              : Domain Admins
ObjectClass       : group
ObjectGUID        : 9a79c2df-94dc-4bbd-85d9-453689b581dc
SamAccountName    : Domain Admins
SID               : S-1-5-21-4131893085-2543218818-4286819957-512
```

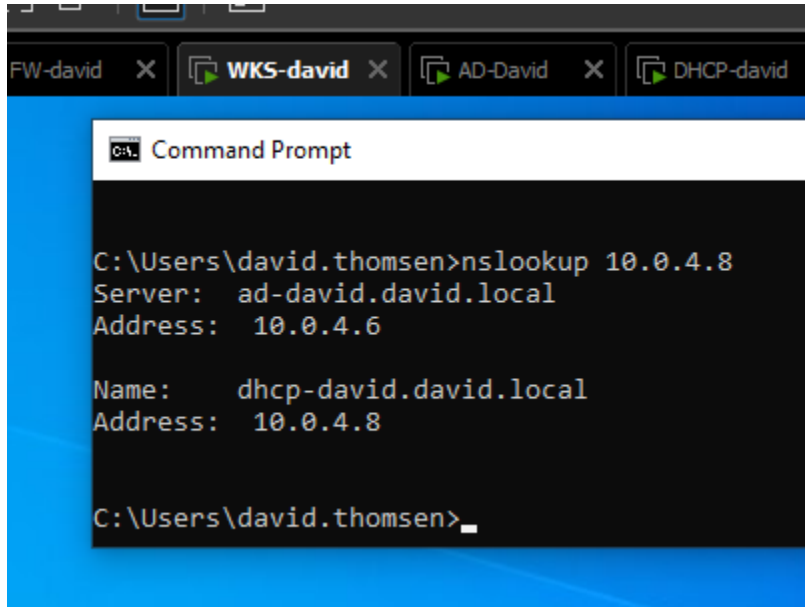
Deliverable 4: On DHCP, provide a screenshot showing the following:

- 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)



```
root@dhcp-david:~  
[david@dhcp-david ~]$ hostname  
dhcp-david  
[david@dhcp-david ~]$ sudo -i  
[root@dhcp-david ~]# nslookup 10.0.4.6  
5.4.0.10.in-addr.arpa  name = ad-david.david.local.  
  
[root@dhcp-david ~]# cat /var/log/messages | grep -i wks  
Nov 28 16:28:18 dhcp-david dhcpd: DHCPOFFER on 10.0.4.200 to 00:0c:29:66:e3:bf (WKS-david) via ens33  
Nov 28 16:28:18 dhcp-david dhcpd: DHCPREQUEST for 10.0.4.200 (10.0.4.66) from 00:0c:29:66:e3:bf (WKS-david) via ens33  
Nov 28 16:28:18 dhcp-david dhcpd: DHCPACK on 10.0.4.200 to 00:0c:29:66:e3:bf (WKS-david) via ens33  
[root@dhcp-david ~]#
```

Deliverable 5 (1 Point). Nslookup 10.0.4.8 for DHCP



```
FW-david X WKS-david X AD-David X DHCP-david  
C:\Users\david.thomsen>nslookup 10.0.4.8  
Server: ad-david.david.local  
Address: 10.0.4.6  
  
Name: dhcp-david.david.local  
Address: 10.0.4.8  
  
C:\Users\david.thomsen>
```