

# Blackbelt File Transfer Lab and Assignment

💡 File transfer is one of those fundamental skills that all technical disciplines need to have. Here are a handful of methods used to transfer files from one system to another.

## Windows Powershell (AD02) -> linux

💡 Depending on when you take this lab, you will have a dhcp server or a blog server. Use one of these for those items labeled "**linux**".

Create a file on ad02 (the assumption is that this version of Windows Server has an ssh client). Push this file to linux using scp. The example shows the creation of a text file that contains the running tasks on ad02.

- `tasklist > tasklist.txt`


ad-assessment-SY S255-02-rubeus.hagrid

```
Windows PowerShell
vmtoolsd.exe           5404 Console           1      15,368 K
svchost.exe            5968 Services           0       6,416 K
RtLockApp.exe          5976 Console           1      45,172 K
RuntimeBroker.exe      1428 Console           1      23,268 K
svchost.exe            5464 Services           0      11,088 K
svchost.exe            4884 Services           0      18,664 K
svchost.exe            5700 Services           0       7,636 K
SecurityHealthService.exe 5484 Services           0      12,528 K
dllhost.exe            4224 Console           1      12,556 K
spssvc.exe             8128 Services           0      12,536 K
powershell.exe         4640 Console           1      74,248 K
conhost.exe            5612 Console           1      18,604 K
powershell.exe         5648 Console           1      78,988 K
conhost.exe            2312 Console           1      17,836 K
mmc.exe                7544 Console           1      14,532 K
ssh.exe                7160 Console           1       7,624 K
tasklist.exe           7600 Console           1       7,800 K
PS C:\Users\rubeus-adm> tasklist > tasklist.txt ; nslookup blog02-rubeus
Server: localhost
Address: 127.0.0.1


Name:      blog02-rubeus.rubeus.local
Address:  10.0.5.11

PS C:\Users\rubeus-adm> scp .\tasklist.txt rubeus@blog02-rubeus:
rubeus@blog02-rubeus's password:
tasklist.txt                                     100% 17KB 358.0KB/s 00:00
PS C:\Users\rubeus-adm>
```

Deliverable 1. Provide a screenshot similar to the one below that shows a SSH session from ad02>linux and the listing of the contents of the transferred task list.


 rubeus@blog02-rubeus:~

```
PS C:\Users\rubeus-adm> ssh rubeus@blog02-rubeus
rubeus@blog02-rubeus's password:
Last login: Sat Dec  4 16:17:39 2021 from ad02-rubeus.rubeus.local
Last login: Sat Dec  4 16:17:39 2021 from ad02-rubeus.rubeus.local
[rubeus@blog02-rubeus ~]$ tail -n 5 tasklist.txt
 c o n h o s t . e x e                2 3 1 2   C o n s o l e
    1                1 7 , 8 3 6   K
 m m c . e x e                7 5 4 4   C o n s o l e
    1                1 4 , 5 3 2   K
 s s h . e x e                7 1 6 0   C o n s o l e
    1                7 , 6 2 4   K
 t a s k l i s t . e x e          7 3 9 6   C o n s o l e
    1                7 , 7 9 6   K
[rubeus@blog02-rubeus ~]$
```

 Note, the PuTTY program can also be used for this purpose. It's version of scp is called pscp and is very reliable but not installed by default.

## Windows scp <- linux

Deliverable 2. Pull the /etc/passwd file from linux to ad02 using scp or pscp, and provide a screenshot showing the /etc/passwd on ad02.

 Windows PowerShell

```
PS C:\Users\rubeus-adm> scp blog02-rubeus:/etc/passwd .
rubeus\rubeus-adm@blog02-rubeus's password:
passwd                                100% 1345    84.5KB/s   00:00
PS C:\Users\rubeus-adm> cat .\passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
```

## fw02 > linux scp

scp works for linux-to-linux transfer. Here's the output of ifconfig on fw1 being sent to linux. It is followed up by a remote ssh command from fw1 to linux to list the last 3 lines in the transferred file (You will need to enter the fw01 bash shell using option 8):

Deliverable 3. Provide a screenshot similar to the one below that shows the transfer and remote listing of the fw1.ifconfig file.

```
fw-assessment-SYS255-02-rubeus.hagrid Enforce US Keyboard Layout View Fullscreen Send Ctrl+Z

[2.5.2-RELEASE][root@fw02-rubeus.rubeus.local]/root: ifconfig > fw1.ifconfig
[2.5.2-RELEASE][root@fw02-rubeus.rubeus.local]/root: head -n 2 fw1.ifconfig
em0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
    options=81009b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM, VLAN_HW
FILTER>
[2.5.2-RELEASE][root@fw02-rubeus.rubeus.local]/root: scp fw1.ifconfig rubeus@10.
0.5.11:/tmp
rubeus@10.0.5.11's password:
fw1.ifconfig 100% 1316 1.2MB/s 00:00
[2.5.2-RELEASE][root@fw02-rubeus.rubeus.local]/root: ssh -t rubeus@10.0.5.11 "ta
il -n 2 /tmp/fw1.ifconfig"
rubeus@10.0.5.11's password:
pfsync0: flags=0<> metric 0 mtu 1500
    groups: pfsync
Connection to 10.0.5.11 closed.
[2.5.2-RELEASE][root@fw02-rubeus.rubeus.local]/root: █
```

## Windows or Linux <- Windows or Linux/Python SimpleHTTPServer

Python and other scripting languages can be leveraged to enable ad-hoc http file transfer. Here we are creating a simple python based http server on blog02:8009.

```
ad-assessment-SYS255-02-rubeus.hagrid

rubeus@blog02-rubeus:~
[rubeus@blog02-rubeus ~]$ sudo firewall-cmd --add-port 8009/tcp --permanent ; sudo firewall-cmd --reload
success
Rsuccess
[rubeus@blog02-rubeus ~]$ python -m SimpleHTTPServer 8009
Serving HTTP on 0.0.0.0 port 8009 ...
```

Deliverable 4. Provide a screenshot showing the tasklist file served from linux to a web browser.

**ad-assessment-SYS255-02-rubeus.hagrid**

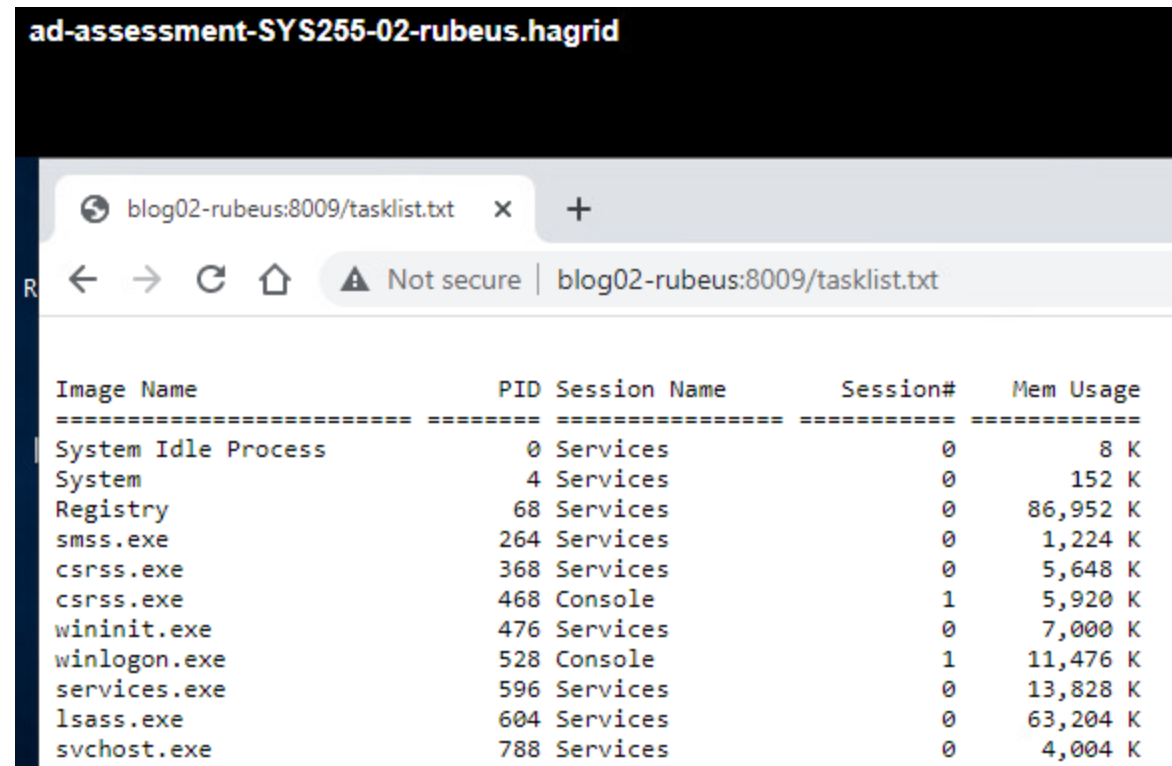
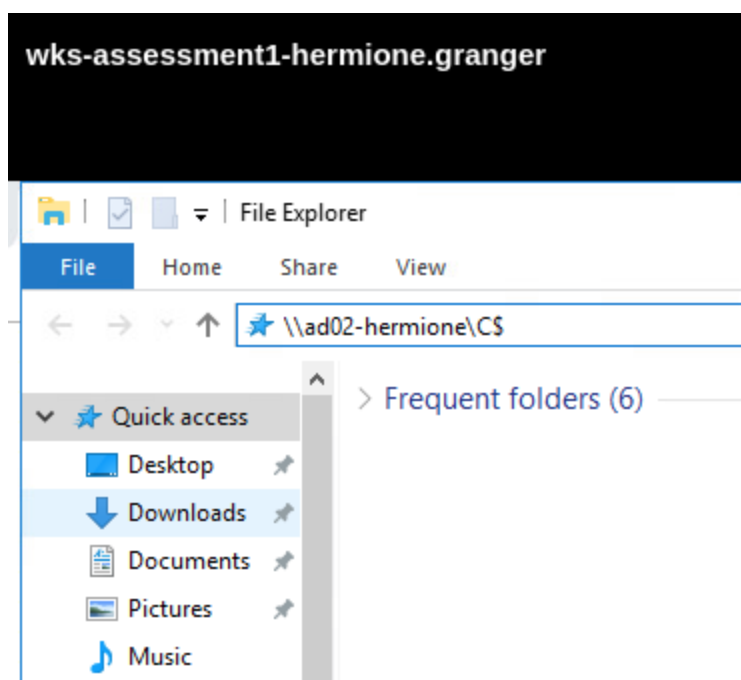
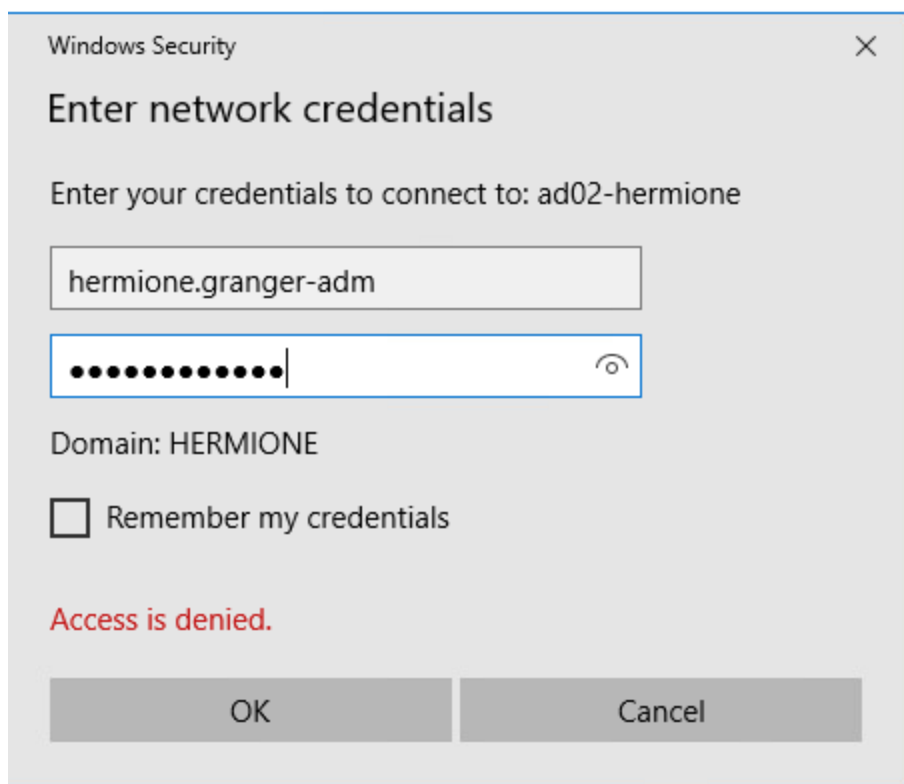


Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	8 K
System	4	Services	0	152 K
Registry	68	Services	0	86,952 K
smss.exe	264	Services	0	1,224 K
csrss.exe	368	Services	0	5,648 K
csrss.exe	468	Console	1	5,920 K
wininit.exe	476	Services	0	7,000 K
winlogon.exe	528	Console	1	11,476 K
services.exe	596	Services	0	13,828 K
lsass.exe	604	Services	0	63,204 K
svchost.exe	788	Services	0	4,004 K

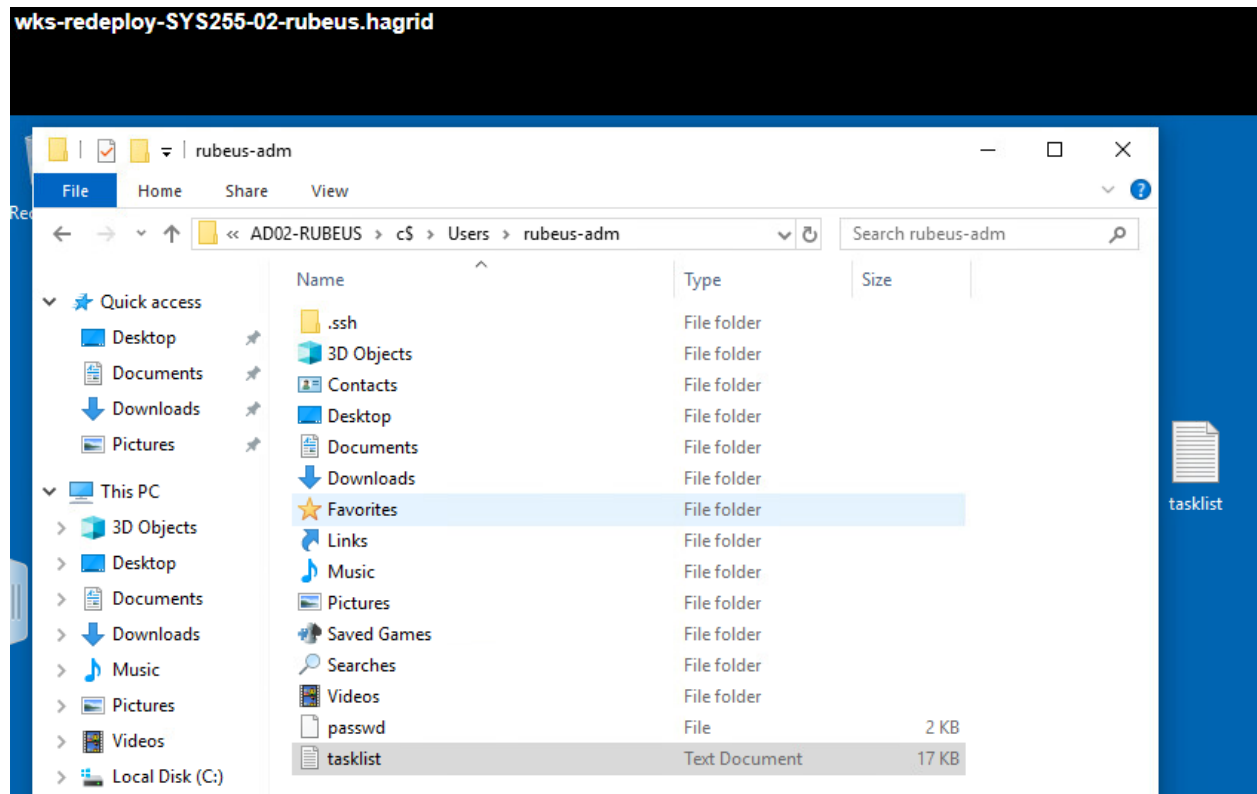
Copying things to and from a Windows Server is not that complex. The mysterious hidden share C\$ can help. The following screenshot shows a Windows user navigating to a hidden share on ad02 from wks.



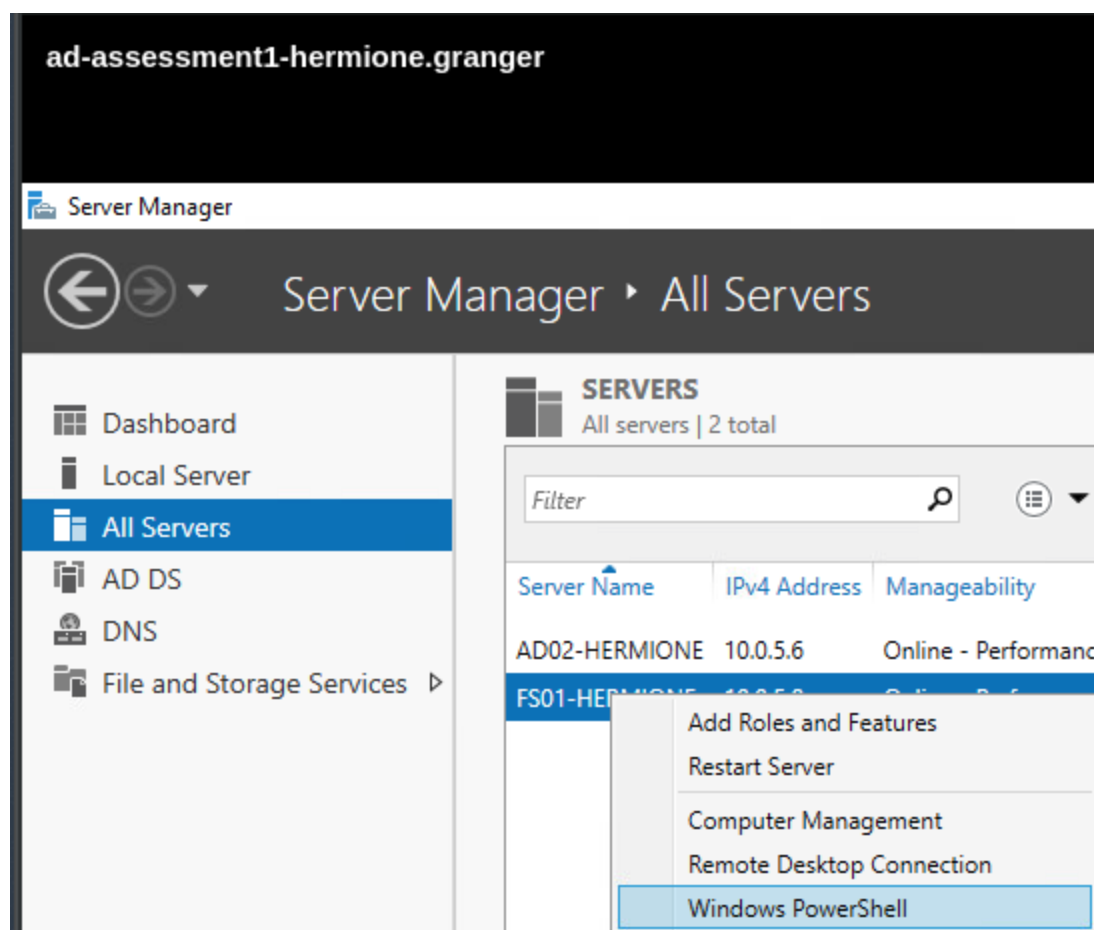
If not logged in with sufficient privileges, then the user is prompted to enter elevated credentials such as:



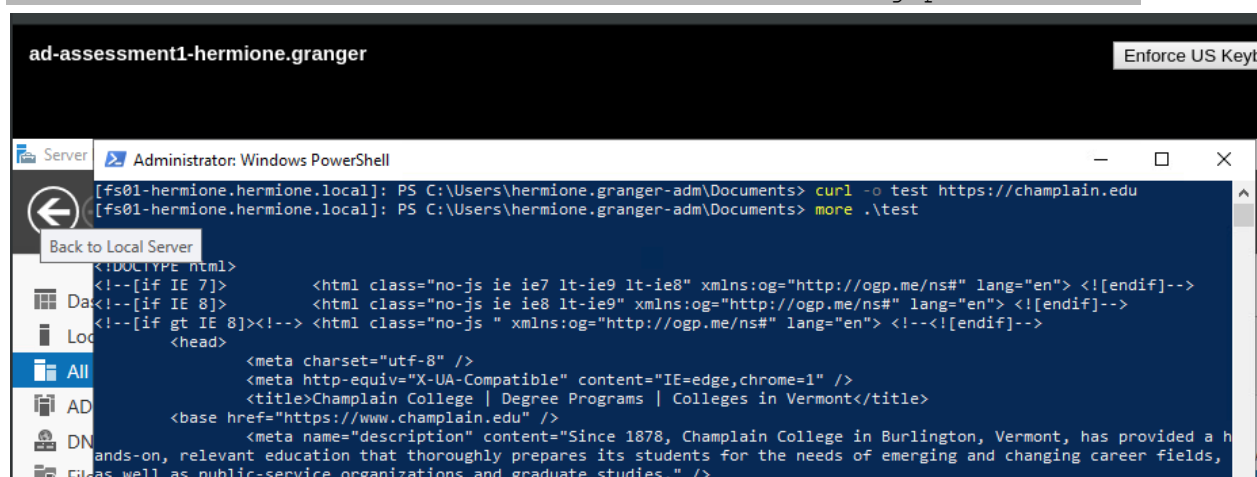
Deliverable 5. Provide a screenshot similar to the one below that shows navigation to ad02's C:\ Drive from wks01 and file being copied from ad02 to your wks02 desktop.



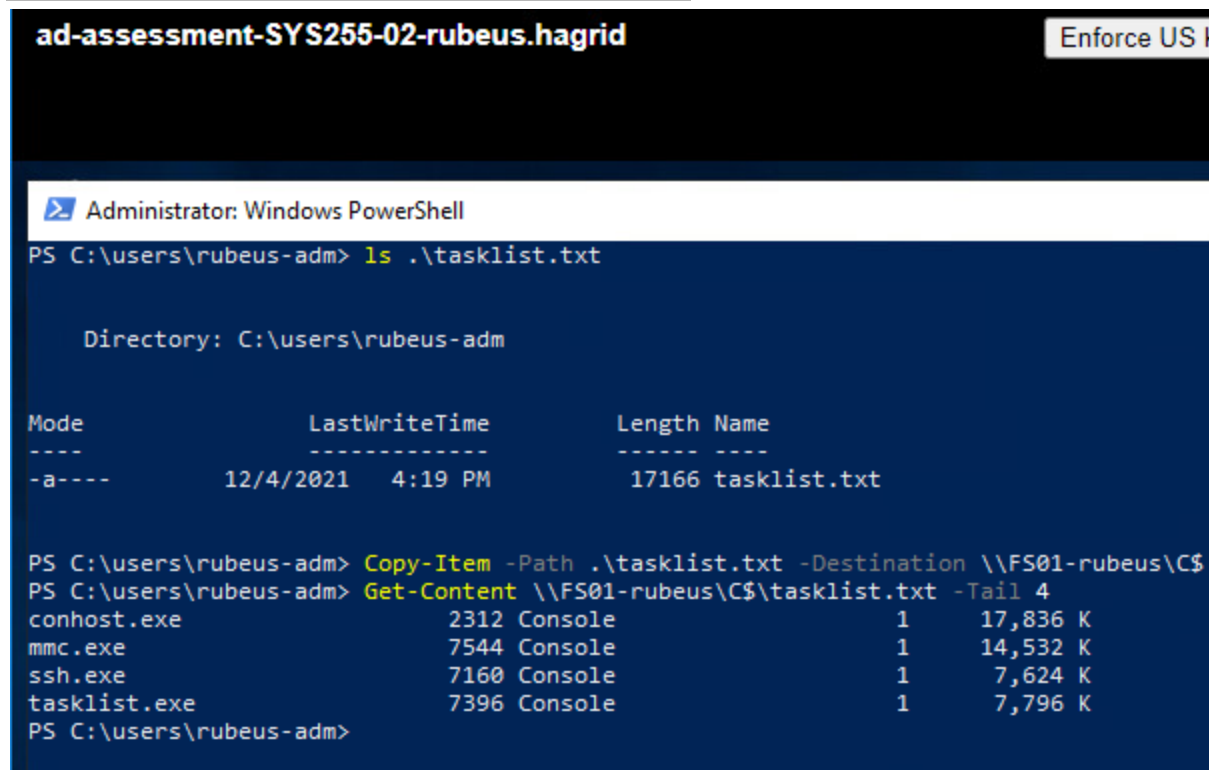
Invoke a remote powershell session from ad02 to fs01.



Deliverable 6. Within your remote powershell session on FS01, use the curl command or one of the other aliases for Invoke-WebRequest on fs01 to pull a file down from the internet. Provide a screenshot similar to the one below that shows the file being pulled down.



Deliverable 7. Investigate the Copy-Item and Get-Content commands on ad02. They can both be used to copy and list the remote file contents of the tasklist file transferred from ad02 to fs01. Provide a screenshot similar to the one below:



The screenshot shows a Windows PowerShell terminal window titled "Administrator: Windows PowerShell". The window displays the following commands and output:

```
PS C:\users\rubeus-adm> ls .\tasklist.txt
```

Directory: C:\users\rubeus-adm

Mode	LastWriteTime	Length	Name
-a----	12/4/2021 4:19 PM	17166	tasklist.txt

```
PS C:\users\rubeus-adm> Copy-Item -Path .\tasklist.txt -Destination \\FS01-rubeus\C$
PS C:\users\rubeus-adm> Get-Content \\FS01-rubeus\C$\tasklist.txt -Tail 4
```

conhost.exe	2312	Console	1	17,836 K
mmc.exe	7544	Console	1	14,532 K
ssh.exe	7160	Console	1	7,624 K
tasklist.exe	7396	Console	1	7,796 K

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

#### Deliverables 8,9,10

Investigate how to use git clients on Windows and Linux to save, clone and update repositories. Provide 3 Screenshots that show the contents of a new git repo called "FileTransferLab" ...

- on github (Deliverable 8)
- and that same repository on linux (Deliverable 9)
- and one of your Windows systems (Deliverable 10)

Your git repo should have files that have content generated from Windows and Linux.