**Objectives:** The objective of this lab was to use Active Directory to manage permissions and resources for various domain user accounts.

**Equipment List:** Hyper 3, lab printer, & lab computer.

**Notes & Observations:** To start this lab, Justin and I accessed the Active Directory Users and Computers, under domain3.local, to create a “Main” folder which housed our Marketing, HR, Accounting, and IT Organizational Units. In each Organizational Unit (excluding IT), we created at least one account. We then accessed the “users” folder and added our accounts to the domain admins security group and we also added our accounts to the IT Organizational Unit.

After we created our user accounts, we created an “All” folder under our Local Disk (C:) where we then created a folder for each group. After we had our folders set up, we went back to the Active Directory and added the members of each Organizational Unit to their own Global Group. We then added each Global Group to its own Domain Local Group.

Once we had our Global and Domain Local Groups set up properly, we set the share permissions for the “All” folder to allow all domain users to see it. We then accessed the security options for each folder and added the corresponding Domain Local Groups with full permissions. We also allowed the HR Domain Local Group to have read permissions for each folder.

After we had all of the permissions correct for each folder, we then accessed the Local Disk (C:) security permissions and removed the “users” group so regular users wouldn’t have access to write to our created folders. We then went back into each folder’s advanced securtiy options and disabled inheritance and removed “domain users” so they couldn’t open files in files they didn’t have access to.

Finally, after setting up what we thought were all of the correct permissions, we added “Domain Users” to the “Remote Desktop Users” on our Win10 Machine so we could remote desktop into each account to test their permissions. All of our users were able to access the folders they had permissions to and could not access folders they didn’t have permissions to. The last step of this lab was to follow the directions linked in the “References” section of this report to add a printer and print a test sheet from it.

**Diagrams, Flowcharts, & Figures: N/A**

**References:** <https://www.tactig.com/install-configure-print-services-windows-server/>

**Questions:** N/A

**Conclusion and Reflection:** To start this lab Justin and I created a “Main” folder in Active Directory which housed the four Organizational Units we created and the users within them. We then created an “All” folder which housed the corresponding folders for each OU. Once we had all of our folders created, we set the security permissions to only allow users from the correct Domain Local Group access. Finally, after we set up all of the correct permissions, we were able to remote desktop into each user and confirm the folder permissions were working properly. The only difficulty we ran into was figuring out that we had to remove “users” from the security permissions of our Local Disk (C:) so that unwanted users couldn’t open files within locked folders.