**Module 3 Lab 2:**

**SAMBA**

On server 1 enable your Nat adapter and disable your NIC on VMNET 10

1. Ensure that you have cups version 2.2.6 installed using the appropriate rpm command
   1. If it is not installed perform and installation of cups
2. Change your working directory to /etc/cups
3. Make a backup of the cupsd.conf original file
4. Open the **cupsd.conf** in the editor of your choice ( I suggest VIM)
   1. Look for **listen localhost:631** and change it to 0.0.0.0:631 or the IP address of your Static NIC on VMNet 10.   
      This will inform the server on which NIC to listen on, 0.0.0.0:631 specifies all Nics should listen on port 631
   2. Under **restrict access to the server** we need to specify who can access this server.  
      Above the **Order allow, deny** directive add the following  
      **Allow all** (this will allow any one to access the server)  
      **Allow from 10.0.\*.\*** (This will allow any one with an ip starting with 10.0.)  
      **Allow localhost** (only the server itself can access itself)

**Allow @local** (clients on the same subnet)

Add the Allow All directive

1. It is much easier to manage cups using the web interface. We want to restrict access to the admin page of the print server so only specified addresses can access the Administrator page
   1. Under **#restrict access to the admin pages** above the **Orderr allow,deny** objective we need to specify who is able to access the admin page. Like the above we can specify **Allow all, Allow Local host, Allow @Local** or **Allow from \*.\*.\*.\*** where \*.\*.\*.\* is the IP address of a specific client or subnet
   2. Use the **allow all** directive or specify your static ip as **Allow from \*.\*.\*.\*** where \*.\*.\*.\* is your static interface
2. From the cups web interface we want to restrict access to the configuration file of the print server so only specified addresses can access the configuration file from the web interface
   1. Just like the above directives we need to specify who, which ip, or which networks are permitted to access the configuration files from the web interface. You can allow all for the purpose of this lab or specify your static ip.
3. In order to administer the cups server and add/modify printers you will need to authenticate yourself using one of the following account types  
   root  
   sudo user  
   any user that has been added to the printadmin group
   1. Create a new account name PrintersSuck and have it added to the printadmin group
   2. Set a password for the PrintersSuck account
4. Go back into the cupsd.conf file if it is not still open and locate the   
   # **All administration operations require an administrator to authenticate**
   1. In the **Require user** option add your **PrintersSuck** user after **@System**
5. Restart the cups service
6. Launch Firefox and navigate to localhost:631
7. Click on the Administration tab, if you get forbidden you need to go back in your config and verify your settings.

You would now be ready to go in and create printers for sharing. Due to constraints of the lab we are unable to add and test printers. If you ever find yourself working in a CUPS environment RHEL has great documentation for cups found [here.](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/deploying_different_types_of_servers/configuring-printing_deploying-different-types-of-servers)