1. Before starting on this activity, please make sure you have completed all of the steps from both the RH124 and RH134 additional activities documents.
2. Discover all of the services, redirect your output to /root/services.txt.
3. Verify that the ssh service is enabled, direct the output to /root/ssh-service.txt.
4. Show the default target, direct our output to /root/default-target.txt.
5. Modify the boot process on station1 to boot to command line only
6. Add a second virtual NIC to your station1 VM, make sure that the second NIC is on the same host only network as the original NIC for your VM. Once the second virtual NIC has been added, configure a team using both NIC's on station1 using an "activebackup" configuration named team0
7. Configure station1 as a caching name server
8. Configure station1 as a postfix null client
9. Configure station1 to provide an iSCSI LUN of 512M
10. Use server1 to discover iSCSI storage on station1
11. On server1, mount the newly discovered iSCSI LUN to /iSCSI as an XFS file system.
12. Create an NFS export on station1, use server1 to discover and mount the share to /nfs
13. Create a new NFS export called my_secure_nfs, protect the NFS export with kerberos on station1.
    1. You will need to download http://server1.example.com/pub/materials/krb5.keytab and put it in /etc/ on station1.
14. Create a samba share on station1 called my_samba that shares out the folder /samba on station1.
15. Mount the newly created samba share on server1
16. Create a second samba share on station1 that meets the following requirements.
    1. Share out the folder called /groupshare
    2. Members of the group scifi will have read/write access to the share
    3. Users not in the group scifi will have read only permission to the share
    4. The users dargo and john will need to be in the scifi group.
    5. The users dargo and john will need to be samba only users and should not be able to log in locally on station1.
    6. The passwords for users dargo and john should be redhat.
    7. setup a credentials file in /etc/named smb_creds.smb on server1 so that the samba share can be mounted during boot using the fstab.
17. Configure mariadb to meet the following requirements
    1. Install mariadb and create a database called test
    2. Setup the Mariadb to require root to use a password and not be able to connect remotely
    3. Add two database users named larry and moe that have grant insert, update, delete and update privileges.
    4. Add another database user named curly that has only the grant select privilege.
    5. Backup the newly imported database to a file named /root/mybackup.dump
    6. Transfer the database backup to server1
    7. Import the database into mariadb on server1, then connect to the db from station1
18. Configure web services on station1 that meet the following criteria
    1. 3 virtual hosts named geeks/dorks/dweebs.example.com
    2. All .crt and .key files can be found at http://server1.example.com/pub/materials/certs/
    3. All http data should be found in /srv/vhost/name
    4. Each virtual host site should contain an index.html files that contains the text "Welcome to {virtual hostname here}
    5. geeks.example.com should be accessible using port 444 and serve a basic hello world cgi app

6. dweebs.example.com should be accessible using 443
7. dorks.example.com should be available on port 80 that uses php.info

19. Write script that will accept as arguments a list of users to create and set all passwords to the same and require the users to change their passwords on first login - then modify the script to test if the user exists before trying to create the user account
20. Configure station1 and server1 to use ipv6 and ipv4 simultaneously using fd07:de11:2015:324::2/64 for station1 and fd07:de11:2015:324::1/64 for server1, verify you can ping server1 from station1 using ipv6