Since NIS is running, this project mostly involves only information gathering and configuration examination:

1) What is the NIS domain name of your machine. Report the command you ran to find this out and the domain name.

2) What NIS server is your machine using. Report the command you ran to find this out and the server name.

3) How many password lines does NIS deliver on your machine. Report: the exact command you used and the number of lines.

4) Examine the NIS password information arriving at your machine. For your 476 account *report* the exact line of information that arrives. You are NOT allowed to use the same yp command you used in the previous question, use another command to match the line in the password file. Report the exact command you used to get that information.

5) Examine the `/var/yp` directory tree on your machine. Report: what in this subtree is dependent upon your domain name.

6) Examine your `yp.conf` file, what is there.

7) Examine the start-up code for the yp client program. What is the exact (full) pathname of the program that is run (that means the name starting with the `/`). Under what condition is this program started?

8) Examine your `nsswitch.conf`. Is it set up to use yp for passwords? How do you know?

9) On cheetah, examine the `/etc/netgroup` file. Report: How many machines are in the `cslabd` netgroup.

10) On the machine you administer, the groups that `cheetah` is delivering using NIS are being used. Do the following. Turn off the use of NIS groups on your machine. (A HUP is not necessary in this case.) An `ls -l ~sue` should give the number 145 instead of a name for the "group" of sue's files. When this works, turn back on the use of NIS groups. Again use the `ls -l ~sue`, this time to make sure that a name is given for the group of sue's files. Report: What did you do to turn on/off the use of NIS groups?