Lab 4

Tasks:

- cksum securecopy.txt and save the output as screen shot.

```
[root@f98b3c176660 ~]# cd mydir
[root@f98b3c176660 mydir]# cksum securecopy.txt
2766876939 488142 securecopy.txt
[root@f98b3c176660 mydir]#
```

- open ~/mydir/securecopy.txt with nano OR vim editor and replace all "root" keywords with yourname and exit the nano.

- again cksum securecopy.txt and save the output as screen shot and write your observation.
- use the find command to find yourname.txt in your environment and save the output as screen shot.

```
[root@f98b3c176660 mydir]# nano securecopy.tx
t




[root@f98b3c176660 mydir]# cksum securecopy.t
xt
482409504 488147 securecopy.txt
[root@f98b3c176660 mydir]# cd ~
[root@f98b3c176660 ~]# find . -iname yourname
.txt
./mydir/mydir2/yourname.txt
```

- Use man page with the "useradd" command and save the output in "useradd-man.txt" using what you have learned in "stdin/stdout" lesson, then grep the

word "password" from the "useradd-man.txt" you have created and take a
screen shot for the grep output.


```
[root@f98b3c176660 ~]# useradd-man.txt > man useradd | grep password useradd-man.txt
-bash: useradd-man.txt: command not found
        The number of days after a password expires until the account is permanently disabled. A value of 0
        disables the account as soon as the password has expired, and a value of -1 disables the feature.
        Example: -K PASS_MAX_DAYS=-1 can be used when creating system account to turn off password aging, even
        though system account has no password at all. Multiple -K options can be specified, e.g.:
    -p, --password PASSWORD
        The encrypted password, as returned by crypt(3). The default is to disable the password.
        Note: This option is not recommended because the password (or encrypted password) will be visible by
        You should make sure the password respects the system's password policy.
        The number of days after a password has expired before the account will be disabled.
        /etc/group (with the same name, same password, and same GID).
        The maximum number of days a password may be used. If the password is older than this, a password
        The minimum number of days allowed between password changes. Any password changes attempted sooner than
        The number of days warning given before a password expires. A zero means warning is given only upon the
        Shadow password suite configuration.
        can't update password file
[root@f98b3c176660 ~]#
```