**Assignment 3**

1. No they are not good documentation for when you are developing kernel modules. This is emphasized in tutorial 5 where he provides two links to Linux documentation for creating modules implying that the man pages are not good enough.
2. When you load a kernel module the function that is guaranteed to run is the init() function. This function will run with supervisor mode because it is now a part of the kernel and the kernel needs privileged access to do its job properly.
   1. You can see what modules are loaded on your machine by running lsmod.
   2. You can blacklist the module by typing modprobe.blacklist=name\_of\_module.
   3. One of the main problems that you could run into is a segmentation fault because you are trying to write to memory that has not been allocated yet.
3. Changing the class name changes where the config files are saved in the filesystem.
4. In order to safely access userspace memory we have to make a call to copy\_to\_user, copy\_from\_user, get\_user, put\_user. We have made a call to put\_user in newgetpid.c in the newgetpid\_read() function. We make calls to copy\_to\_user in remember.c in function remember\_read and a call to copy\_to\_user in the function remember\_write function.
5. In order to make newgetpid.c to respond to write requests we need to add .write = newgetpid\_write to the file\_operations stuct. Then we need to create the function newgetpid\_write(struct file \*f, char \*buff, size\_t len, loff\_t \*offset) so that we can get the write request from the user and actually write it to the device file.
6. No fsck.ext4 cannot repair the filesystem when we have destroyed all the super blocks in that filesystem. This is because the superblocks contains information about where the file blocks are saved in memory. If this is corrupted then it no longer contains the map to where any of the filesystems data is located and so fsck.ext4 cannot fix it because it does not know where to look.
7. I would expect to find files in the lost+found directory when there is a file that has no links to it anywhere and is basically inaccessible by any means. Those files are only placed in the lost+found directory when there is a command to run fsck.
   1. This question is important because it is letting the user know that the computer cannot verify that the host is who they say they are. So instead of connecting automatically it gives you the choice to back out if you do not choose to trust the host.
   2. A fingerprint is a unique identifying token given to your system. This allows the host to identify the people connected to it by the fingerprint that was issued to them.
   3. No the files will not have the same uid.
   4. No only the owner of the file will be able to read it. Anyone else who tries to access it gets denied.
8. In order to make the file take up virtually no memory on disk we need to make a filesystem out of the file. This way it turns hundreds megabytes of data into a couple hundred kilobytes stored on disk with the rest stored virtually.