Madison Rockwell

To log in when no password works:

1. Go to the grub menu
2. Press e to enter **********
3. Add "rd.break" so that when the machine starts, the root password is reset
4. You will be prompted by: **switch_root:/#**
5. Run the command: **mount –o rw,remount /sysroot** to set the sysroot directory to be readable and writable.
6. Now run: **chroot /sysroot** to make sysroot your root directory.
7. Next type: **passwd root** to change the root password
8. Run: **exit** twice to continue booting.
9. When prompted, choose **root** as the login and then use the new password you created.

To find the Virus:

1. Mark Dehus gave the hint of looking in the /etc/systemd/system directory
2. When I ran ls on that directory, I saw a file that didn't belong named **eDuZ1n.service**
3. I ran "**cat eDuZ1n.service**" to see what it contained
4. I noticed there was a long file in the usr directory that's address is being put into /dev/null
5. I ran **vim <really long file name>** to see what was inside
6. The file contained the code for the virus
7. Reading through the code showed that there were three things that needed to be fixed
    a. .ps needed to be copied back into ps and then deleted
    b. The root and boot lines of /etc/fstab needed to be added back into the file
    c. All copies of the virus needed to be deleted

To fix the ps command:

1. First **cd /bin**
2. Then run the move command to move the contents of .ps into ps and delete it: **mv .ps ps**
3. This should solve the bug in ps

To fix /etc/fstab:

1. First **vim /etc/fstab**
2. Add the following two lines:
   /dev/mapper/centos-root / xfs defaults 1 1
   UUID=71438877-2509-4eb2-9c1d-dd119fb7b77f /boot xfs defaults 1 2

To make sure you find and delete all copies of the virus:

1. Search for all hidden .sh files by running: **find .*.sh** in the /usr directory
2. Check to see if copies of virus (I found no others)

3. Remove the copies by running the **rm** command on each file name
4. Go to /etc/systemd/system to remove the **eDuZ1n.service** file
5. Run the rm command on that file:
   rm eDuZ1n.service

Last step is to reboot and make sure that the root password hasn't been changed again. This means that the virus is gone.