Lab3: Virus Attack

Steps to fix machine after virus infection:

1. Access machine E through vsphere
2. Reboot machine E and access grub menu and
3. Press a to view boot arguments
4. Add “single” to start up arguments to start machine in run level 1 (single user mode)
5. Type “mount -n -o remount /dev/mapper/VolGroup-lv_root /” in order to use passwd command because fstab and mtab were read only in single user mode
    a. chmod would not work
6. Type “passwd” and change password so that I can ssh into machine E from the terminal on my computer
7. After changing password, type “mount -o remount,rw /dev/mapper/VolGroup-lv_root /” in order to be able to edit fstab because it is missing root mount.
8. After rebooting password was changed, type “pstree” and notice a process runs passwd after I change it.
9. Use “ps -aux” and try to “kill” process but cannot.
10. Looking at “ps -aux” notice that before sleep is called a command is issued from the /usr directory.
11. I type “ls -al” and see a “.” file and when I “cat” the file out I see that it is changing fstab and the root password.
12. Rename “.” to “virus” and delete #bash.. from top of file so it can’t run anymore.

13. Reboot and use “pstree” to see it no longer runs but then it respawns itself somehow.
14. Use “ps -ef” to see where it spawned.
15. Isolate the copy of the virus file and read functions. See that it persists in /bin/ls so when I use the ls command it starts up.
16. Uncomment bootloader wipe function on accident and have to have professor Dehus reinstall everything.
17. Go back to /bin/ls and comment out all functions. Virus no longer functions. Ls command is no longer found though. Check /bin/.ls but it does not exist
18. Reboot machine in run level 3 with “telinit 3” and add root mount to fstab.
19. Then add uuid for /boot to fstab using “blkid /dev/sda1” to find uuid.
20. Search /etc/rc3.d/ to make sure the virus did not attach itself to any init scripts. Use command “grep -l “function change_root_passwd” /etc/rc3.d/S*”
21. Use command “scp /bin/ls 10.21.32.2:/bin/ls” while in Machine A to copy ls to machine E since bin/.ls was blown away somehow.