Steve Cary

Security Part 1

For this lab assignment I used the “keep it simple stupid” approach. For each item (1-3) in the assignment I created a separate script. I then scheduled each of those scripts to run starting at 2am everyday via a cronjob.

For item 1, I used a basic nmap command to scan for IP address on my network. My thinking here is that all the IP address on my network, especially at this time of day should be the same. I could parse through this data to identify any suspicious IP addresses.

For item 2, I used a couple different methods to monitor the directories. First I use sha1sum to generate a hash of the directory as it is currently, I then used the inotifywatch command included in the inotify-tools rpm, to watch the directories for changes. If any are made, the notifications would be redirected to a text file.

For item 3, I decided to monitor the hidden files in my /root directory. To do this, I first list all the hidden files each time the script is run, this way I can see if any new ones have appeared, or if any existing files have been removed. I then used the stat command to view deeper information about the files such as last modification date, number of blocks.

Ideally I should enhance the monitoring of network traffic. I realize the command I have currently is not enough to monitor for suspicious activity. Other enhancements that could be made include deeper monitoring of startup files, and other things like /etc/password. While I monitor the /etc directory, more focus should be put on files within that directory.