The topic I have selected for my final project is “how to detect and resolve a process that is hidden”. This is important in part of finding malware, spyware, and other malicious code that may already be running on a system without the administrator’s knowledge. My plan in approaching this problem is to use a utility called “Unhide”. It is included in many Linux distributions, and it’s job is to utilize various methods of detecting hidden processes in order to prevent loss of sensitive information or keep system performance at peak. Some examples include brute force, which checks every PID running on the system to ensure there are none hidden, and file comparisons. File comparisons would be something such as comparing the /proc and /bin/ps directories. If there is a process in one and not the other, it will be reported. Once a hidden process is found, it should be able to be terminated with standard commands, e.g. pidof, kill, killall. My proposal is this; I will show every method Unhide uses to detect these hidden processes and do my best to provide examples of each. If all goes according to plan, I can incorporate it into a script that after running a test, will scan the log file output and kill any hidden processes that Unhide finds.