Advanced Scripting

Exercise 3 “White list capturing”

Using the two log files supplied in myCourses, write a Perl script named WhiteList.pl to report any and all records where the event matches any of the following list of regular expressions:

".\*APPCRASH.\*"

".\*he protected system file.\*"

".\*EMET\_DLL Module logged the following event:.\*"

.\*your virus/spyware.\*

".\*A new process has been created\..\*"

".\*A service was installed in the system\..\*"

".\*A scheduled task was created\..\*"

".\*Logon Type:[\W]\*(3|10).\*"

".\*\\Software\\Microsoft\\Windows\\CurrentVersion\\Run.\*"

".\*service terminated unexpectedly\..\*"

".\*service was successfully sent a.\*"

".\*service entered the.\*"

".\*service was changed from.\*"