Universidade Federal do Rio de Janeiro
Escola Politécnica
Departamento de Eletrônica e de Computação

Linguagens de Programação
Trabalho 1

Ewerton Vasconcelos e Gabriel Lopes

1 Introdução

Grande parte das aplicações de software utilizam do recurso de logs para registrar um histório de ocorrências, que pode ser fundamental na solução de um problema em uma processos de *troubleshooting*. É nos arquivos de logs que um administrador de sistemas pode localizar informações que servem como input para a solução de problemas em uma aplicação, rede ou qualquer outro software, e até problemas de hardware.

2 A definição do Problema

É indescutível que os arquivos de log são de extrema importância para a solução de problemas, mas o que geralmente ocorre na prática, é que esses arquivos acabam sendo extremamente extensos devido ao grande número de aplicações que rodam em uma máquina e também à grande quantidade de informações que esses softwares escrevem nos *log files*, que acabam sendo extensos e exigindo um grande ferramental *(expressões regulares, filtros, ...)* de pesquisa para se extrair informações úteis. Visando isso, a aplicação do trabalho, consiste em um software escrito em **C++ e Perl** que une a praticidade do **Perl** para processar os *log files* através de *expressões regulares* e as interfaces dinâmicas que o **C++** para oferecer ao usuário final mais praticidade e precisão na obtenção de informações dos logs de aplicações e sistema.

3 Inputs e Outputs do Software

O usuário terá à sua disposição, **cinco** opções no programa em **Gráfico** que poderão ser incrementadas por sub-opções.

1. Últimos **N** usuários que solicitaram permissões de *Super User* (Potêncialmente capazes de realizar uma modificação perigosa no sistema/rede);
2. Possível ataque intra-net ou via ***SSH*** (Tentativas de login sucessivas sem sucesso, principalmente ao usuário **root**)
3. Últimos **N** softwares instalados no sistema via repositórios (apt-get, yum, ...), e os respectivos autores das instalações.
4.
5.

4 O Papel de Cada Software

Cada software *(C++ e Perl)* terá um diferente papel na aplicação final.

- C++:
  Será responsável por executar os scripts em **Peal** e oferecer ao usuário uma **GUI** *(Grafic User Interface)*, um ambiente amigável e de fácil ultilização.

- Perl:
  Tratar os *Log Files* extraindo as informações solicitadas, formatando e enviando ao software em C++.

5 Inputs e Outputs do Software em C++

- Inputs:
  Opções descritas em seção 3 através de uma **GUI** *(Grafic User Interface)* incluindo filtros por data e/ou usuários.

- Outputs:
  Chamadas aos Scripts em **Perl** responsáveis por explorar os *Log Files*.
  Resultados recebidos do software em **Perl** devidamente formatados na **GUI**.

6 Inputs e Outputs do Software em Perl

- Inputs:
  Chamadas do software em **C++** com os valores dos filtros solicitados pelo usuário.

- Outputs:
  Informações extraídas dos *Log Files* semi formatadas para o software em **C++**.

7 Plataformas

Em um primeiro momento, a proposta é que o programa seja compatível com sistemas baseados em **Linux/Unix**, mais especificamente em distribuições **Debian** *(Ubuntu, Collax, o próprio Debian e outras)*

8 Conclusão

Por serem um histórico de alterações e ações em um sistema, ou rede, manter e explorar arquivos de Log são ações importântes, desta forma, o registro, a coleta e análise de logs são procedimentos vitais em auditorias de segurança dentro de uma organização. Sendo assim, a ferramenta proposta nesse texto se mostra de grande ultilidade, proporcionando uma economia de tempo, e um aumento na segurança dos sistemas computacionais.