UNIVERSIDADE ABERTA
www.uab.pt

Ministério da Educação e Ciência

e-Fólio

U.C. 21077

Linguagens de Programação

e-Fólio A – Linguagem OCaml

-- INSTRUÇÕES --

1) O e-fólio tem uma cotação de 4 valores.

2) Qualquer tentativa de plágio resultará numa nota final de zero valores.

3) Este e-fólio deve ser resolvido usando a linguagem OCaml.

4) Deve ser submetido um ficheiro comprimido (ZIP ou RAR) com o nome e número de estudante contendo:

a) Código do programa;

b) Ficheiro readme.txt com a informação necessária para compilar e executar o programa;

c) Relatório até 4 páginas descrevendo a solução apresentada e os testes efetuados.

E-fólio A

Em sistemas Unix, a informação dos utilizadores é mantida em vários ficheiros, incluindo: o ficheiro *passwd*, o ficheiro *shadow* (com informação encriptada dos utilizadores) e no ficheiro *groups* onde é mantida informação dos grupos a que os utilizadores pertencem.

Pretende-se elaborar um programa que analise o ficheiro passwd [1] e o ficheiro group [2] (recebidos por parâmetro) e identifique todas as vulnerabilidades de segurança. Estas vulnerabilidades podem incluir:

Vul.1 Acesso superutilizador, o utilizador *root* pode fazer login na máquina (a sua shell devia estar configurada com o valor /sbin/nologin, /bin/false ou não ter nenhum valor definido).
Vul.2 Contas de utilizador que são configuradas com acesso root (UID = 0 ou GID = 0).
Vul.3 Contas de utilizador que pertencem ao grupo root/wheel no ficheiro (etc/group).
Vul.4 Contas de serviços de sistema (postfix, mysql, daemon, lp, lpd...) que têm acesso à linha de comandos (ver Vul.1).

A análise a fazer pelo programa deve ter em conta o grau de risco associado a cada vulnerabilidade, como se sumariza na Tabela 1.

Tabela 1 - Graus de risco das vulnerabilidades

Grau de Risco	Vulnerabilidade(s)
Alto	Vul.1, Vul.2
Médio	Vul. 3
Baixo	Vul. 4

O seu programa deve implementar as seguintes funcionalidades:

1. Leitura dos ficheiros (ou respetivo conteúdo em strings) com o formato /etc/passwd [1] e /etc/group [2].
2. Identificação da vulnerabilidade associada a um determinado utilizador. Nota que alguns utilizadores podem não ter nenhuma vulnerabilidade associada.
3. Estatísticas dos graus de risco identificados, segundo a Tabela 1, após a análise de todos os registos dos ficheiros.

Nota:
São disponibilizados dois ficheiros *passwd* e *groups* que podem ser usados para testar o seu programa.

Referências:
[1] Estrutura do ficheiro */etc/passwd*, disponível em: https://linux.die.net/man/5/passwd
[2] Estrutura do ficheiro */etc/group*, disponível em: https://linux.die.net/man/5/group