PONTIFÍCIA UNIVERSIDADE CATÓLICA DO PARANÁ
DEPARTAMENTO DE ENGENHARIA
SEGURANÇA DA INFORMAÇÃO

Relatório projeto AAP 2

Méllanie Padilha, Gabriely de Andrade da Costa, Ana Lídia Almeida.

Relatório Técnico

Curitiba/ PR
2022

Relatório projeto AAP 2

Projeto sistema de login e ataque de força bruta

Projeto prático apresentado a matéria de segurança da informação, como parte dos requisitos necessários à obtenção da nota do projeto final da matéria.

Resumo

O desafio proposto foi criar um sistema de login e autenticação utilizando o algoritmo hash como sistema de proteção para a senha, depois usar um sistema de ataque bruto para quebrar este sistema, a partir dessa proposta desenvolvemos um programa utilizando a linguagem python e para a quebra foi utilizado o hashcat um código de força bruta encontrado depois de algumas pesquisas na internet. Foram realizados 3 testes que serão explicados posteriormente.

O sistema de login

No sistema utilizamos os requisitos estabelecidos pelo professor, usuário e senha com 4 dígitos, a senha foi definida a partir do número 0000 ao 9999. Foi utilizado o algoritmo hash para a proteção inicial também para realizar o reforço do código.

O algoritmo de quebra e testes

Para a quebra utilizamos o Hashcat, é uma ferramenta de recuperação de senha. Após a instalação foram realizados 3 testes.

O primeiro foi realizado com a senha de 4 dígitos transformado em hash, após a execução **a ferramenta levou de 0.5 milissegundo a 1 segunda para realizar a quebra.**

O segundo, reforçamos o código adicionando dois números aleatórios (entre 0 e 9) ao final da senha. Então estes 6 dígitos foram transformados em hash e foi realizado um segundo teste, após a execução **a ferramenta levou de 2 a 5 segundos para realizar a quebra.**

E o por fim no terceiro, para garantir uma maior segurança transformamos o hash da senha em uma chave de um novo hash, aplicamos um hash sobre o hash, após isso foi realizado a tentativa de quebra com a ferramenta, entretanto **não foi possível realizar a quebra** pois a chave possuía 32 caracteres. (O teste 3 foi rodado durante 30 minutos até a máquina não suportar o processamento e a ferramenta crashar).