Laboratório – Comparar dados com um hash, verificar vulnerabilidades, propor melhorias (arquivo modificado)

Nome: IGOR EIKI FERREIRA KUBOTA RA: 19.02466-5

Nome: BRUNO BORGIANI TACLA RA: 19.01821-5

Nome: LUCAS REIS AZEVEDO RA: 19.02659-5

Objetivos

Use um programa de hash para verificar a integridade dos dados.

Verificar vulnerabilidades com o uso do Hash

Propor melhorias nos controles de integridade com o uso de hash

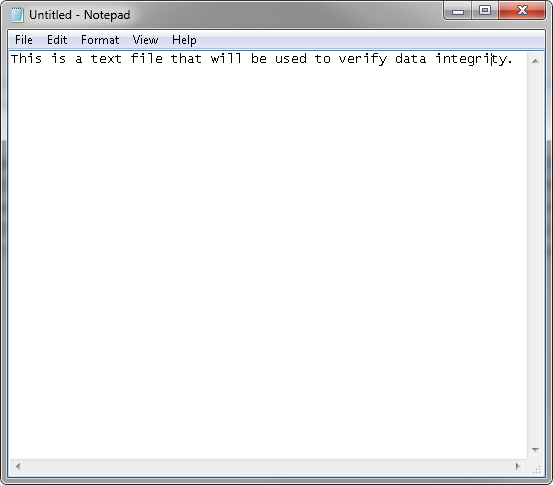
1. Histórico/Cenário

É importante identificar quando os dados foram corrompidos ou adulterados. Um programa de hash pode ser usado para verificar se os dados foram alterados ou se permaneceram intocados. Um programa de hash executa uma função hash nos dados ou em um arquivo, o que gera um valor (geralmente mais curto). Há muitas funções hash diferentes, algumas muito simples e outras muito complexas. Quando o mesmo hash é realizado nos mesmos dados, o valor gerado é sempre o mesmo. Se for feita qualquer alteração nos dados, o valor de hash gerado será diferente.

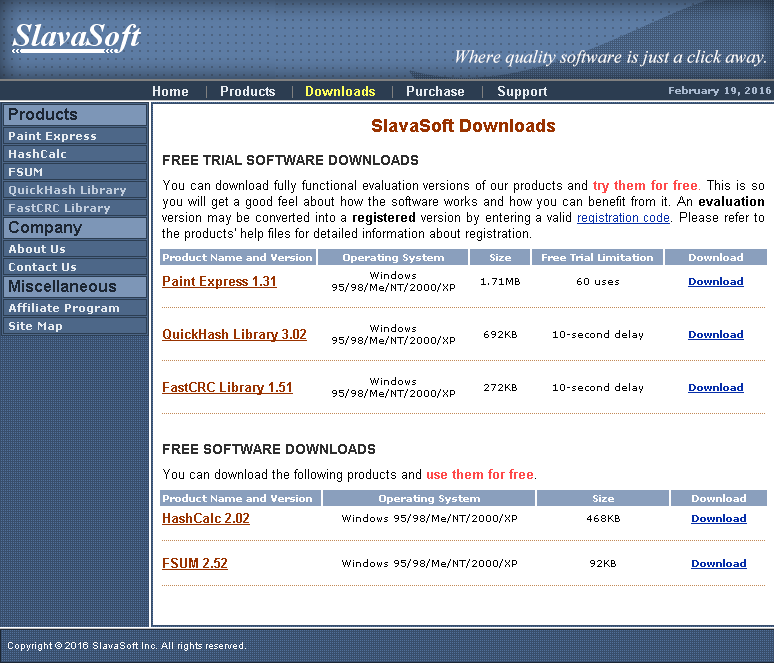
**Observação**: você precisará de privilégios de instalação e algum conhecimento do processo para instalar programas no Windows.

1. Recursos necessários

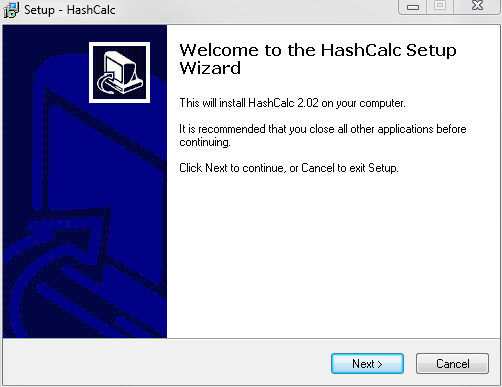
* PC com acesso à Internet
  1. Crie um arquivo de texto
     1. Procure o programa Bloco de Notas em seu computador e abra-o.
     2. Digite algo.



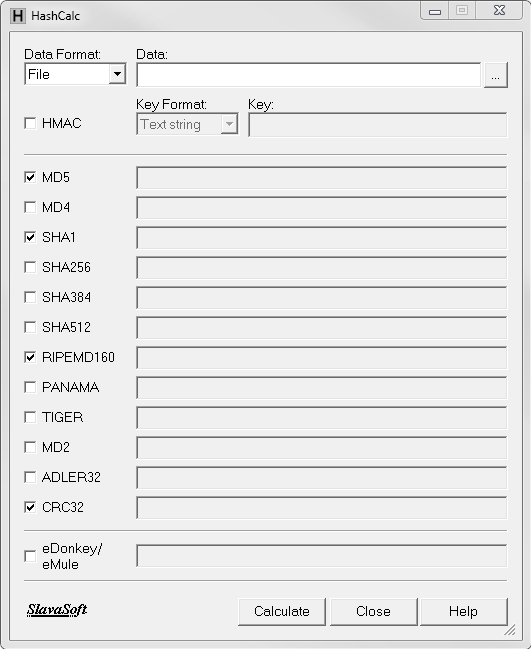
* + 1. Escolha **Arquivo > Salvar**.
    2. Navegue até a **Área de Trabalho**.
    3. Digite **Hash** no campo **Nome do arquivo:** e clique em **Salvar**.
  1. Instale o HashCalc
     1. Abra um navegador da Web e navegue até <http://www.slavasoft.com/download.htm>.



* + 1. Clique em **Download** (Fazer download) na linha **HashCalc 2.02**.
    2. Abra o arquivo **hashcalc.zip** e execute o arquivo **setup.exe**.



* + 1. Siga o assistente de instalação para instalar o HashCalc.
    2. Clique em **Finish** (Concluir) na última tela e feche o arquivo **README** que apareceu. Se desejar, você poderá ler o arquivo.
    3. Agora, HashCalc está instalado e funcionando.



* 1. Calcule um hash do arquivo Readme.txt usando o programa HashCalc ou conforme o link <http://www.fileformat.info/tool/hash.htm>
     1. Defina os seguintes itens no HashCalc:
        1. Formato dos dados: **Arquivo**.
        2. Dados: clique no botão **...** ao lado do campo de dados, navegue até a pasta **HashCalc** e escolha o arquivo **Readme.txt** ou criar um arquivo com um texto usando o link informado
        3. Desmarque a opção **HMAC**.
        4. Desmarque todos os tipos de hash, exceto **MD5**.
     2. Clicar no botão **Calculate** (Calcular).

Qual é o valor ao lado de **MD5**?

***50376608159588ce9c726289fe38891a***

* 1. Faça uma alteração no arquivo Readme.txt
     1. Navegue até a **Área de Trabalho** e abra o arquivo **Readme.txt**.
     2. Faça uma pequena alteração no texto, como a exclusão de uma letra ou adição de um espaço ou período.
     3. Clique em **Arquivo > Salvar** e feche o **Bloco de Notas**.
  2. Calcule um novo hash do arquivo Readme.txt
     1. Clique no botão **Calculate** (Calcular) em HashCalc novamente.

Qual é o valor ao lado de **MD5**?

***bbab29a4e945b59c2a900e02ed8f718e***

O valor é diferente do valor registado na etapa 3? Justifique.

***Sim, como o texto é diferente do valor registrado durante a etapa 3, a criptografia também é diferente.***

* + 1. Coloque uma marca de seleção ao lado dos hashes (MD5, SHA1, SHA256, SHA512).
    2. Clique em **Calcular**.
    3. Observe que muitos dos tipos de hash criam um hash de um comprimento diferente. Justifique.

***Diferentes hashes criam diferentes tamanhos por utilizarem diferentes tipos de criptografia no processo***

* 1. Gerando hash, verificando vulnerabilidades e propostas de melhoria
     1. Quais os valores de Hash (usando o algoritmo SHA1) de "Teste" e "teste" respectivamente (<http://www.fileformat.info/tool/hash.htm>)? Os resultados apresentados são diferentes? Justifique.

Teste = 6d7082969a0681db6fe658a26ff16198600f0923

Teste = 2e6f9b0d5885b6010f9167787445617f553a735f

***Os resultados são diferentes porque a criptografia é case-sensitive, ou seja, tem diferença entre letras maiúsculas e minúsculas.***

* + 1. Gerar um hash da mensagem “1234567890” usando o algoritmo SHA1 em <http://www.fileformat.info/tool/hash.htm> e testar o resultado desse hash em <https://crackstation.net> . É possível retornar o valor inicial com essa mensagem inicial? Justifique.

***Sim, como essa mensagem já é bem utilizada, o hash dela já é bem conhecido, podendo estar contido em diversas bases de dados, assim como a do site do Crackstation.***

* + 1. O que é possível ser realizado no item anterior para minimizar os riscos encontrados com o uso do Hash? Dica: consultar o material do curso “Cybersecurity Essentials” nos tópicos 5.1.2 e 5.1.3. Ver HMAC e Salt.
  + <https://www.symbionts.de/tools/hash/sha256-hash-salt-generator.html>
  + <http://www.freeformatter.com/hmac-generator.html>

***Para minimizarmos os riscos encontrados na utilização do Hash, pode-se aplicar um salt previamente ao Hash, formando assim um Hash diferente para senhas iguais. Pode-se também utilizar um HMAC, uma chave secreta em que apenas o remetente e o destinatário tem acesso.***