Laboratório - Recuperar Senhas

# Objetivos

   Use uma ferramenta para recuperar senhas de usuários.

   Alterar uma senha de usuário para uma senha mais forte.

# Histórico/Cenário

Há quatro contas de usuários, Alice, Bob, Eve e Eric, em um sistema Linux. Há também a conta de superusuário cisco. As contas de usuário na VM não devem ser seguras, pois a VM é um ambiente de sandbox e não é para aplicativos do mundo real. Neste laboratório, você usará John, o Estripador, uma ferramenta de recuperação de senha de código aberto, para recuperar as senhas de todas as cinco contas.

**Recursos necessários**

PC com o **CSE-LABVM** instalado no VirtualBox

**Instruções**

**Parte 1: Abra uma janela de terminal no CSE-LABVM.**

a.     Inicie o **CSE-LABVM.**

b.     Clique duas vezes no ícone **Terminal** para abrir um terminal.

## Parte 2: Combine senhas e nomes de usuário em um arquivo de texto.

a.     Digite o seguinte comando para mudar para o diretório onde John the Ripper está localizado:

cisco@labvm:~$ **cd Downloads/john/run**

cisco@labvm:~/Downloads/john/run$

b.     Use o comando **unshadow** para combinar o arquivo **/etc/passwd** onde as contas de usuário são armazenadas, com o arquivo **/etc/shadow** onde as senhas de usuário são armazenadas, em um novo arquivo chamado **mypasswd**. Insira a **senha** como a senha de superusuário, se solicitado. A sintaxe do comando **unshadow** é a seguinte:

cisco@labvm:~/Downloads/john/run$ **sudo ./unshadow /etc/passwd /etc/shadow > mypasswd**

[sudo] password for cisco: **password**

cisco@labvm:~/Downloads/john/run$

## Parte 3: Execute John, o Estripador, para recuperar as senhas.

a.     Para ver que as senhas ainda não foram recuperadas (quebradas), digite o comando **./john --show mypasswd**.

cisco@labvm:~/Downloads/john/run$ **./john --show mypasswd**

Diretório criado: /home/cisco/.john

0 hashes de senha quebrados, 5 restantes

cisco@labvm:~/Downloads/john/run$

b.     O programa Johnthe Ripper usa um dicionário predefinido chamado **password.lst** com um conjunto padrão de “regras” predefinidas para processar o dicionário e recupera todos os hashes do tipo md5crypt e do tipo crypt. No prompt de comando, digite o seguinte comando para recuperar as senhas armazenadas no arquivo **mypasswd**.

cisco@labvm:~/Downloads/john/run$ **./john --wordlist=password.lst --rules mypasswd --format=crypt**

Carregou 5 hashes de senha com 5 sais diferentes (criptografia, criptografia genérica (3) [? / 64])

Pressione 'q' ou Ctrl-C para abortar, quase qualquer outra tecla de status

password1        (Eric)

password         (cisco)

password         (Eve)

12345            (Bob)

123456           (Alice)

5g 0: 00: 00: 00 100% 6.097g / s 117.0p / s 585.3c / s 585.3C / s #CSE contas de curso do laboratório - Contabilidade de autorização de autenticação..natasha

Use a opção "--show" para exibir todas as senhas quebradas de forma confiável

Sessão concluída!

cisco@labvm:~/Downloads/john/run$

c.     Insira o **comando./john --show mypasswd** novamente para ver se as senhas estão quebradas.

cisco@labvm:~/Downloads/john/run$ **./john --show mypasswd**

cisco: password: 900: 900: Cybersecurity Analyst ,,,: / home / cisco: / bin / bash

Alice: 123456: 1000: 1000 :: / home / alice: / bin / bash

Bob: 12345: 1001: 1001 :: / home / Bob: / bin / bash

Eve: senha: 1002: 1002 :: / home / Eve: / bin / bash

Eric:password1:1003:1003::/home/Eric:/bin/bash

5 hashes de senha quebrados, 0 restantes

cisco@labvm:~/Downloads/john/run$

## Parte 4: Alterar uma senha de usuário para uma versão mais forte e tentar recuperá-la.

a.      Crie sua própria senha forte ou use um gerador de senhas on-line para criar uma.

b.      Encontre um "verificador da força da senha" on-line para testar a força da sua senha. Sua senha deve levar pelo menos milhares de anos para ser descoberta.

c.     Use seus privilégios de superusuário para alterar a senha de Eric de **password1** para o valor da nova senha forte. Certifique-se de receber a mensagem "senha atualizada com sucesso".

cisco @ labvm: ~ / Downloads / john / run $ **sudo passwd Eric**

[sudo] password for cisco: **password**

Nova senha:**<your\_new\_strong\_password>**

Redigite a nova senha: **<your\_new\_strong\_password>**

passwd: senha atualizada com sucesso

cisco@labvm:~/Downloads/john/run$

d.     Execute **unshadow** e, em seguida, **john** novamente para ver se você pode quebrar a senha de Eric. Se você alterou a senha de Eric para uma que seja forte o suficiente para levar milhares de anos para ser invadida, você estará esperando muito tempo. Quando terminar de esperar, digite **q** ou **Ctrl+C** para parar John the Ripper.

cisco@labvm:~/Downloads/john/run$ **./john --wordlist=password.lst --rules mypasswd --format=crypt**

Carregou 5 hashes de senha com 5 sais diferentes (criptografia, criptografia genérica (3) [? / 64])

1 hash de senha restante

Pressione 'q' ou Ctrl-C para abortar, quase qualquer outra tecla de status

0g 0: 00: 00: 17 7% 0g / s 599.6p / s 599.6c / s 599.6C / s reddog1..mark1

Sessão cancelada

e.     Insira o **comando./john --show mypasswd** para ver que apenas quatro senhas estão quebradas e uma fica.

cisco@labvm:~/Downloads/john/run$ **./john --show mypasswd**

cisco: password: 900: 900: Cybersecurity Analyst ,,,: / home / cisco: / bin / bash

Alice: 123456: 1000: 1000 :: / home / alice: / bin / bash

Bob: 12345: 1001: 1001 :: / home / Bob: / bin / bash

Eve: senha: 1002: 1002 :: / home / Eve: / bin / bash

4 hashes de senha quebrados, 1 restante

cisco@labvm:~/Downloads/john/run$

Fim do documento