

Laboratório – Como decifrar senhas

Objetivos

Use uma ferramenta de quebra de senha para recuperar a senha de um usuário.

Histórico/Cenário

Há quatro contas de usuários, Alice, Bob, Eve e Eric, em um sistema Linux. Você recuperará essas senhas usando John the Ripper, uma ferramenta de quebra de senha de código aberto.

Recursos necessários

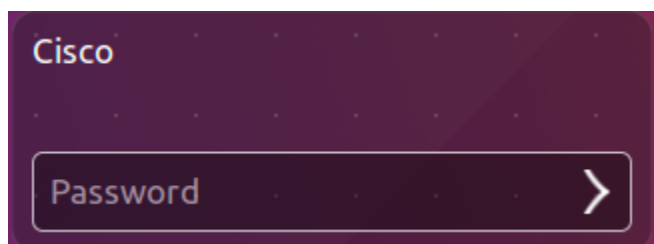
- PC com Ubuntu 16.04 Desktop LTS instalado em um VirtualBox ou em uma máquina virtual VMware.

Passo 1: Abra uma janela de terminal no Ubuntu.

- Inicie uma sessão no Ubuntu usando as seguintes credenciais:

Usuário: **cisco**

Senha: **password**



- Clique no ícone do terminal para abrir um terminal.



Passo 2: Execute John the Ripper.

- No command prompt (prompt de comando), digite o seguinte comando para mudar para o diretório em que John the Ripper está localizado:

```
cisco@ubuntu:~$ cd ~/Downloads/john-1.8.0/run
```

- b. No command prompt (prompt de comando), digite o seguinte comando:

```
cisco@ubuntu:~/Downloads/john-1.8.0/run$ sudo ./unshadow /etc/passwd /etc/shadow > mypasswd
```

```
cisco@ubuntu:~/Downloads/john-1.8.0/run$ sudo ./unshadow /etc/passwd /etc/shadow > mypasswd
```

Esse comando combinará o arquivo /etc/passwd em que contas de usuário estão armazenadas, com o arquivo /etc/shadow em que as senhas dos usuários são armazenadas, em um novo arquivo chamado "mypasswd".

Passo 3: Recuperar senhas.

- a. Digite o seguinte comando no terminal:

```
cisco@ubuntu:~/Downloads/john-1.8.0/run$ ./john --show mypasswd
```

```
cisco@ubuntu:~/Downloads/john-1.8.0/run$ ./john --show mypasswd
0 password hashes cracked, 5 left
```

Como mostrado acima, não há senhas decifradas nesse ponto.

- b. No command prompt (prompt de comando), digite o seguinte comando:

```
cisco@ubuntu:~/Downloads/john-1.8.0/run$ ./john --wordlist=password.lst --rules mypasswd --format=crypt
```

```
cisco@ubuntu:~/Downloads/john-1.8.0/run$ ./john --wordlist=password.lst --rules mypasswd --format=crypt
```

O programa John the 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.

Os resultados a seguir exibem as senhas de cada conta.

```
Loaded 8 password hashes with 8 different salts (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
password1      (Eric)
12345          (Bob)
123456         (Alice)
password       (cisco)
password       (Eve)
5g 0:00:20:50 100% 0.003998g/s 125.4p/s 376.6c/s 376.6C/s Tnting..Sssing
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

- c. No command prompt (prompt de comando), digite o seguinte comando:

```
cisco@ubuntu:~/Downloads/john-1.8.0/run$ ./john --show mypasswd
```

```
cisco@ubuntu:~/Downloads/john-1.8.0/run$ ./john --show mypasswd
cisco:password:1000:1000:Cisco,,:/home/cisco:/bin/bash
Alice:123456:1001:1001::/home/Alice:
Bob:12345:1002:1002::/home/Bob:
Eve:password:1003:1003::/home/Eve:
Eric:password1:1004:1004::/home/Eric:

5 password hashes cracked, 3 left
cisco@ubuntu:~/Downloads/john-1.8.0/run$
```

Quantas senhas foram decifradas?

Referências

John the Ripper: <http://www.openwall.com/john/>