

Lab - Decifrar Palavras-passe

Objetivos

Usar uma ferramenta de quebra de palavras-passe para recuperar a palavra-passe de um utilizador.

Contexto/Cenário

Há quatro contas de utilizador, **Alice, Bob, Eve e Eric**, num sistema Linux. Irá recuperar estas palavras-passe usando a ferramenta **John the Ripper**, uma ferramenta de quebra de palavras-passe de código aberto.

Recursos necessários

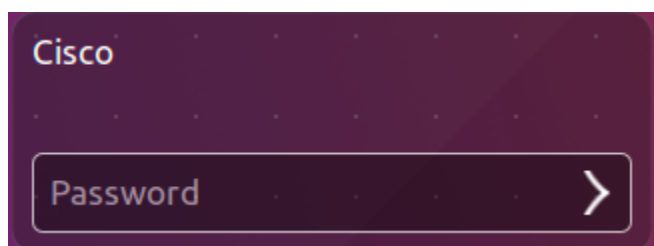
- Um PC com o Ubuntu 16.04 Desktop LTS instalado no VirtualBox ou numa máquina virtual VMware.

Passo 1: Abra uma janela de terminal no Ubuntu.

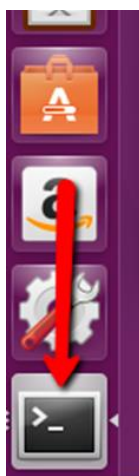
- Faça login no Ubuntu usando as seguintes credenciais:

Utilizador: **cisco**

Palavra-passe: **password**



- Clique no ícone do terminal para abrir uma janela terminal.



Passo 2: Execute a ferramenta John the Ripper

- Na linha de comandos, introduza o seguinte comando para mudar para o diretório onde a ferramenta **John the Ripper** está localizada:

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

- b. Na linha de comandos, introduza 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
```

Este comando irá combinar o ficheiro `/etc/passwd` onde as contas de utilizador estão armazenadas, com o ficheiro `/etc/shadow` onde as palavra-passe dos utilizadores estão armazenadas, num novo ficheiro chamado “mypasswd”.

Passo 3: Recuperar Palavras-passe.

- a. Introduza 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 se mostra em cima, neste momento não há palavras-passe recuperadas.

- b. Na linha de comandos, introduza 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
```

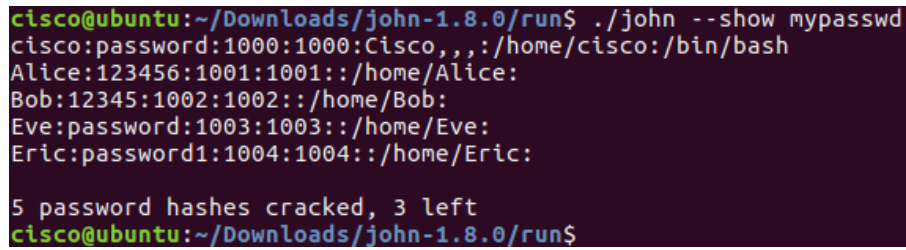
O programa, **John the Ripper**, usa um dicionário predefinido chamado **password.lst** com um conjunto padrão de “regras” predefinidas para lidar com o dicionário e recuperar todos os hashes das palavras-passe do tipo md5crypt e crypt.

Os resultados em baixo apresentam as palavras-passe recuperadas, 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. Na linha de comandos, introduza 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 palavras-passe foram recuperadas?

SKUs

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