Piratage de mot de passe

Objectifs

Utiliser un outil de piratage de mot de passe pour récupérer le mot de passe d'un utilisateur.

Contexte/Scénario

Quatre comptes d'utilisateurs, Alice, Bob, Ève et Éric, se trouvent sur un système Linux. Vous récupérerez ces mots de passe à l'aide de John the Ripper, un outil open source de piratage de mot de passe.

Ressources requises

- Ordinateur équipé d'Ubuntu 16.04 Desktop LTS dans une machine virtuelle VirtualBox or VMware

Étape 1 : Ouvrez une fenêtre de terminal dans Ubuntu.

a. Connectez-vous à Ubuntu à l'aide des informations d'identification suivantes :

Utilisateur : **cisco**

Mot de passe : **password**

b. Cliquez sur l'icône du terminal pour ouvrir un terminal.

Étape 2 : Lancez John the Ripper.

a. À l'invite de commandes, saisissez la commande suivante pour modifier le répertoire où se trouve John the Ripper :

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

b. À l'invite de commandes, saisissez la commande suivante :

```
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
```

Cette commande regroupera le contenu du fichier /etc/passwd où sont stockés les comptes d'utilisateurs et celui du fichier /etc/shadow où les mots de passe sont stockés pour les placer dans un nouveau fichier nommé « mypasswd ».

Étape 3 : Récupérez les mots de passe.

a. Saisissez la commande suivante dans le 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
```

Comme il apparaît ci-dessus, aucun mot de passe n'a été piraté à ce stade.

b. À l'invite de commandes, saisissez la commande suivante :

```
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
```

Le programme John the Ripper utilise un dictionnaire prédéfini appelé **password.lst** et une série standard de « règles » prédéfinies pour exploiter ce dictionnaire et récupérer tous les hashs de mots de passe de type md5crypt et crypt.

Les résultats ci-dessous présentent les mots de passe pour chaque compte.

```
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. À l'invite de commandes, saisissez la commande suivante :

```
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$
```

Combien de mots de passe ont été piratés ?

Références

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