

le système est censé vous répondre avec ce message :

```
GNU nano 6.4 /etc/shadow
root:$y$j9T$ubofw2nyDXiSj8DEP8GDs/$fAxJXkofHxhWXjOW3.pHUUJcFgv07dH9ef/Iot1qAdN2:19388:0:99999:7:::
daemon:*:19331:0:99999:7:::
bin:*:19331:0:99999:7:::
sys:*:19331:0:99999:7:::
sync:*:19331:0:99999:7:::
games:*:19331:0:99999:7:::
man:*:19331:0:99999:7:::
lp:*:19331:0:99999:7:::
mail:*:19331:0:99999:7:::
news:*:19331:0:99999:7:::
uucp:*:19331:0:99999:7:::
proxy:*:19331:0:99999:7:::
www-data:*:19331:0:99999:7:::
backup:*:19331:0:99999:7:::
list:*:19331:0:99999:7:::
irc:*:19331:0:99999:7:::
_apt:*:19331:0:99999:7:::
nobody:*:19331:0:99999:7:::
systemd-networkd!*:19331:0:99999:7:::
systemd-timesyncd!*:19331:0:99999:7:::
messagebus!:19331:0:99999:7:::
tss!:19331:0:99999:7:::
strongswan!:19331:0:99999:7:::

^G Help      ^O Write Out  ^W Where Is   | Read 58 lines | Execute
^X Exit      ^R Read File  ^\ Replace    | Cut         | ^T Execute
              ^Y Paste      ^_ Justify    | ^C Location  | M-U Undo
              |             |             | ^G Go To Line| M-E Redo
```

II – Les premières commandes concrètes

Après avoir découvert comment afficher les dictionnaires nous allons maintenant essayer de cracker les mots de passe à l'aide des noms d'utilisateurs

Nous allons à présent taper une commande qui va pouvoir prendre les mots de passe dans le fichiers /etc /passwd et les noms d'utilisateurs dans le /etc /shadow pour créer un seul fichier qui va regrouper les deux

Voici la commande suivante :

`sudo unshadow /etc/passwd /etc/shadow > testcracks`

```
File Actions Edit View Help
(kali@kali)-[~]
└─$ sudo unshadow /etc/passwd /etc/shadow > testcracks
```

Nous allons maintenant afficher le fichier testcrack qui contenait les mots de passe crypté ainsi que les noms d'utilisateurs avec cette commande :

« `sudo nano testcrack` »

```
(kali@kali)-[~]
└─$ sudo nano testcrack
```

Le système est censé vous répondre sous cette forme

```

GNU nano 6.4 testcrack
root:~$ cat /etc/passwd
daemon:*:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:*:2:2:bin:/bin:/usr/sbin/nologin
sys:*:3:3:sys:/dev:/usr/sbin/nologin
sync:*:4:65534:sync:/bin:/bin/sync
games:*:5:60:games:/usr/games:/usr/sbin/nologin
man:*:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:*:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:*:8:8:mail:/var/mail:/usr/sbin/nologin
news:*:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:*:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:*:13:13:proxy:/bin:/usr/sbin/nologin
www-data:*:33:33:www-data:/var/www:/usr/sbin/nologin
backup:*:34:34:backup:/var/backups:/usr/sbin/nologin
list:*:38:38:Mail List Manager:/var/list:/usr/sbin/nologin
irc:*:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:*:42:65534::/nonexistent:/usr/sbin/nologin
nobody:*:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-networkd:*:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesyncd:*:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:!:100:107::/nonexistent:/usr/sbin/nologin
tss:!:101:109:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:!:102:65534::/var/lib/strongswan:/usr/sbin/nologin

```

III – Le crackage de John

Maintenant que toutes les étapes sont faites, John va s’occuper de tout le reste, vous n’aurez plus qu’à taper ces quelques dernière commande :

« john testcrack -format=crypt »

```

(kali@kali)-[~]
└─$ john testcrack -format=crypt
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descript 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]
ded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
kali (kali)
lg 0:00:00:00 DONE 1/3 (2022-03-20 18:07) 1.010g/s 96.96p/s 96.96c/s 96.96C/s kali..kk
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

```

Cette commande va permettre de voir les 3600 mots de passe et voir si nots utilisateurs contiennent les mots de passes dans la liste

sudo nano /usr/share/john/password.lst

```

(kali@kali)-[~]
└─$ sudo nano /usr/share/john/password.lst
[sudo] password for kali:

```

le systeme va devoir nous envoyé ce document

```
#!/comment: For more wordlists, see https://www.openwall.com/wordlists/
123456
12345
password
password1
123456789
12345678
1234567890
abc123
computer
tigger
1234
qwerty
money
carmen
mickey
secret
summer
internet
a1b2c3
123
Service
```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo

Pour finir, nous allons taper cette dernière commande qui va nous afficher les utilisateurs qui contiennent les mots de passe

John -show testcrack

```
(kali@kali)-[~]
└─$ john -show testcrack
root:kali:0:0:root:/root:/usr/bin/zsh
kali:kali:1000:1000:,,,:/home/kali:/usr/bin/zsh
rick:kali:1001:1001:kali,kali,kali,kali,kali:/home/rick:/bin/bash

3 password hashes cracked, 1 left
```