

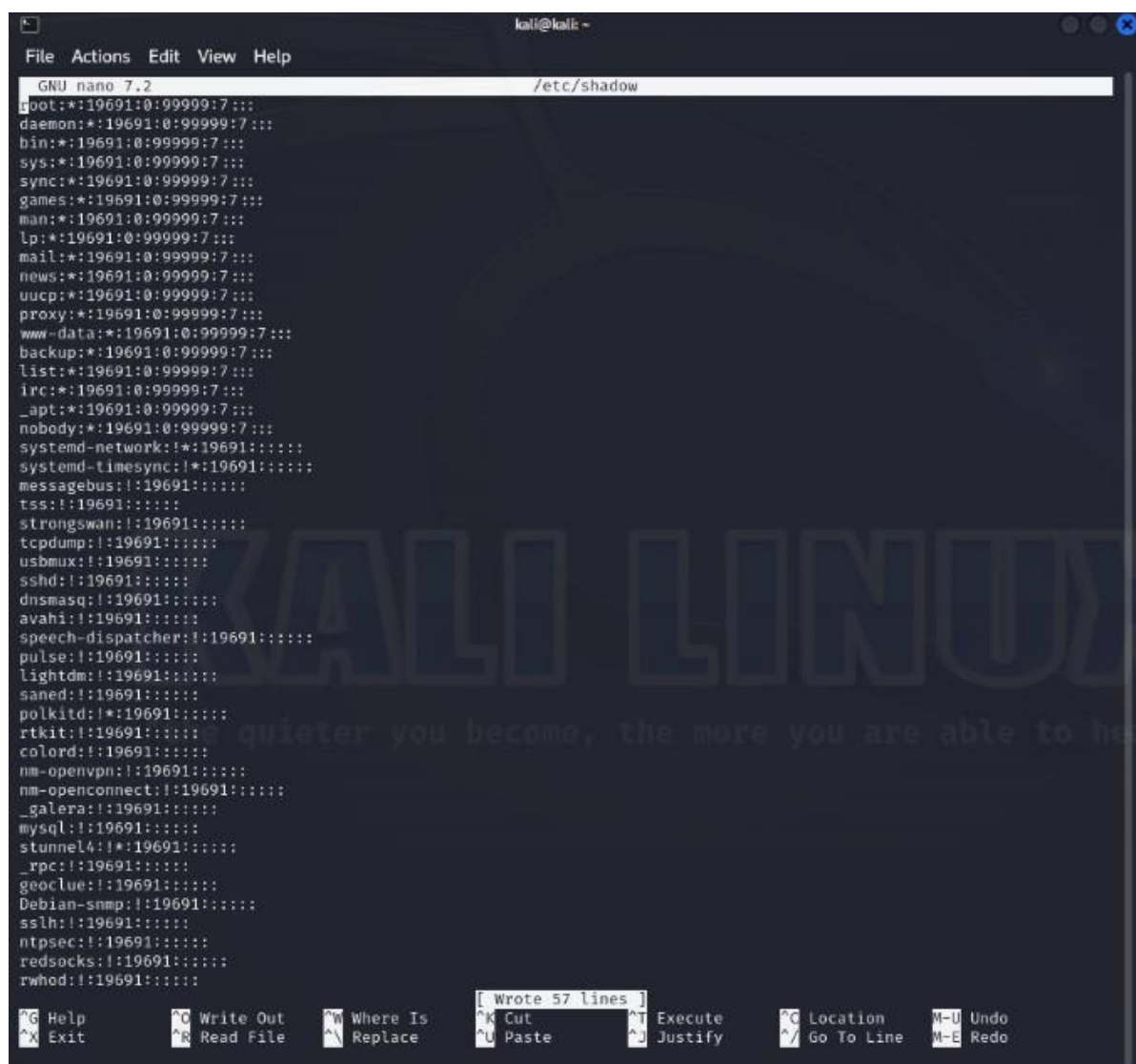
Zanelli Lucas

Compte rendu Kali Linux

Avant de commencer on à vérifiez les dictionnaires de mots passe en tapant la commande « sudo nano/shadow ».

```
(kali@kali)-[~]  
$ sudo nano /etc/shadow  
[sudo] password for kali: 
```

Puis en mettant le mot de passe (kali) un page est apparu :



```
kali@kali: ~  
File Actions Edit View Help  
GNU nano 7.2 /etc/shadow  
root:*:19691:0:99999:7:::  
daemon:*:19691:0:99999:7:::  
bin:*:19691:0:99999:7:::  
sys:*:19691:0:99999:7:::  
sync:*:19691:0:99999:7:::  
games:*:19691:0:99999:7:::  
man:*:19691:0:99999:7:::  
lp:*:19691:0:99999:7:::  
mail:*:19691:0:99999:7:::  
news:*:19691:0:99999:7:::  
uucp:*:19691:0:99999:7:::  
proxy:*:19691:0:99999:7:::  
www-data:*:19691:0:99999:7:::  
backup:*:19691:0:99999:7:::  
list:*:19691:0:99999:7:::  
irc:*:19691:0:99999:7:::  
_apt:*:19691:0:99999:7:::  
nobody:*:19691:0:99999:7:::  
systemd-network:*:19691:0:99999:7:::  
systemd-timesync:*:19691:0:99999:7:::  
messagebus:*:19691:0:99999:7:::  
tss:*:19691:0:99999:7:::  
strongswan:*:19691:0:99999:7:::  
tcpdump:*:19691:0:99999:7:::  
usbmux:*:19691:0:99999:7:::  
sshd:*:19691:0:99999:7:::  
dnsmasq:*:19691:0:99999:7:::  
avahi:*:19691:0:99999:7:::  
speech-dispatcher:*:19691:0:99999:7:::  
pulse:*:19691:0:99999:7:::  
lightdm:*:19691:0:99999:7:::  
sane:*:19691:0:99999:7:::  
polkitd:*:19691:0:99999:7:::  
rtkit:*:19691:0:99999:7:::  
colord:*:19691:0:99999:7:::  
nm-openvpn:*:19691:0:99999:7:::  
nm-openconnect:*:19691:0:99999:7:::  
_galera:*:19691:0:99999:7:::  
mysql:*:19691:0:99999:7:::  
stunnel4:*:19691:0:99999:7:::  
_rpc:*:19691:0:99999:7:::  
geoclue:*:19691:0:99999:7:::  
Debian-snmpp:*:19691:0:99999:7:::  
ssh:*:19691:0:99999:7:::  
ntpsec:*:19691:0:99999:7:::  
redsocks:*:19691:0:99999:7:::  
rwhod:*:19691:0:99999:7:::  
[ Wrote 57 lines ]  
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute  
^X Exit      ^R Read File  ^_ Replace    ^U Paste      ^J Justify  
^C Location  M-U Undo  
^_ Go To Line M-E Redo
```

On à aussi vérifiez tous les mots de passe cryptés en utilisant la commande suivante « sudo nano/etc /passwd ».

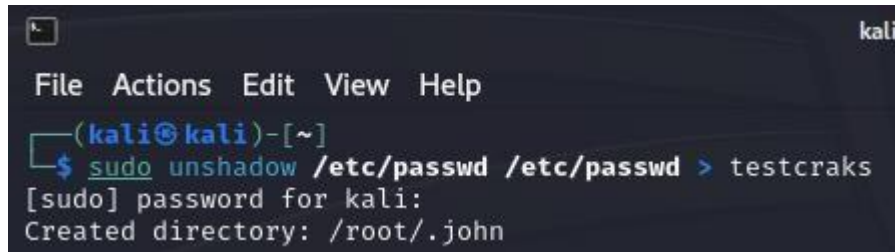
```
File Actions Edit View Help
(kali@kali)-[~]
$ sudo nano /etc/passwd
[sudo] password for kali:
```

Ensuite un page de ce type est apparu.

```
kali@kali: ~
File Actions Edit View Help
GNU nano 7.2 /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:usr/sbin/nologin
systemd-timesync:x:992:992:systemd Time Synchronization:/:usr/sbin/nologin
messagebus:x:100:102::/nonexistent:/usr/sbin/nologin
tss:x:101:104:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:102:65534::/var/lib/strongswan:/usr/sbin/nologin
tcpdump:x:103:105::/nonexistent:/usr/sbin/nologin
usbmux:x:104:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
dnsmasq:x:106:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
avahi:x:107:108:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
speech-dispatcher:x:108:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
pulse:x:109:110:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
lightdm:x:110:112:Light Display Manager:/var/lib/lightdm:/bin/false
saned:x:111:114::/var/lib/saned:/usr/sbin/nologin
polkitd:x:991:991:polkit:/nonexistent:/usr/sbin/nologin
rtkit:x:112:115:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:x:113:116:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
nm-openvpn:x:114:117:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
nm-openconnect:x:115:118:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin
_galera:x:116:65534::/nonexistent:/usr/sbin/nologin
mysql:x:117:120:MariaDB Server,,,:/nonexistent:/bin/false
stunnel4:x:990:990:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin
_rpc:x:118:65534::/run/rpcbind:/usr/sbin/nologin
geoclue:x:119:122::/var/lib/geoclue:/usr/sbin/nologin
Debian-snmpp:x:120:123::/var/lib/snmpp:/bin/false
ssllh:x:121:124::/nonexistent:/usr/sbin/nologin
ntpsec:x:122:127::/nonexistent:/usr/sbin/nologin
redsocks:x:123:128::/var/run/redsocks:/usr/sbin/nologin
rwho:x:124:65534::/var/spool/rwho:/usr/sbin/nologin
[ Read 57 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^\ Replace    ^U Paste       ^J Justify
              ^C Location   ^M-U Undo
              ^_ Go To Line ^M-E Redo
```

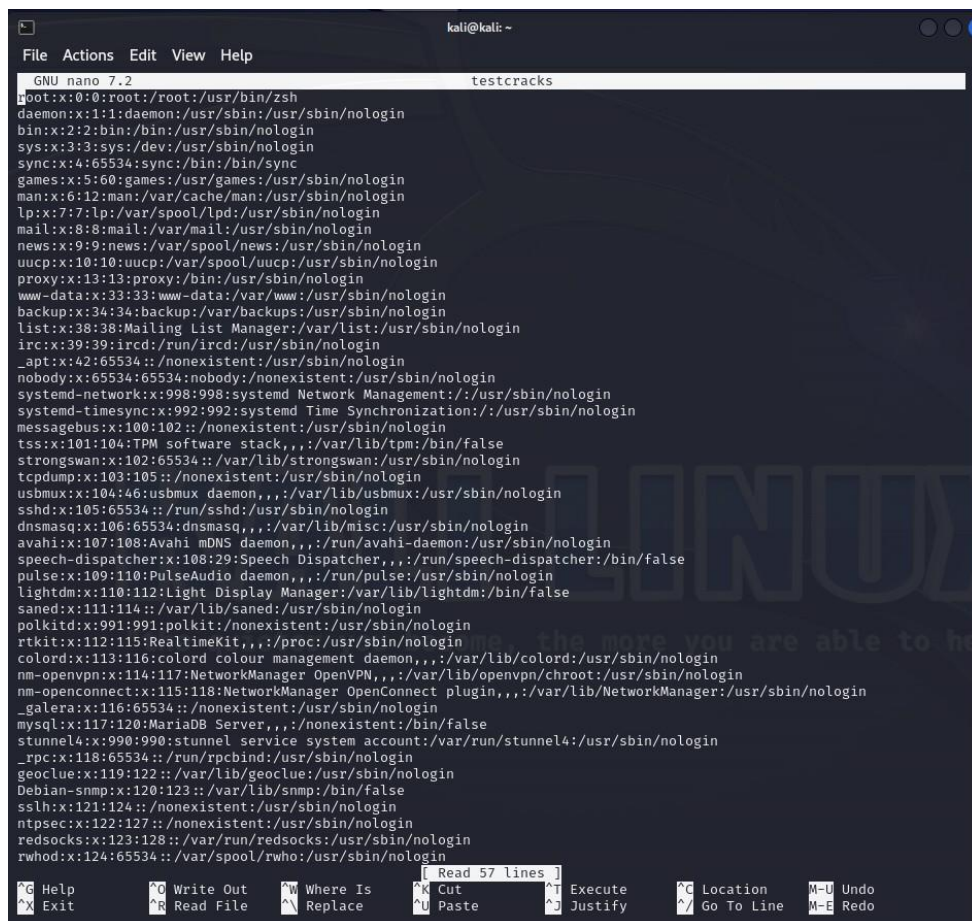
Après avoir vérifié les dictionnaires de mots de passe et d'utilisateur nous avons cracké les mots de passe à l'aide des noms d'utilisateurs.

Pour commencer nous avons taper la commande « `sudo unshadow /etc/passwd /etc/passwd > testcraks` » se qui nous permet de créer un fichier qui va regrouper l'ensemble des informations.



```
(kali@kali)-[~]  
$ sudo unshadow /etc/passwd /etc/passwd > testcraks  
[sudo] password for kali:  
Created directory: /root/.john
```

Ensuite nous avons afficher le fichier testcrack qui contient les mots de passe cryptés et aussi les noms d'utilisateurs avec la commande « `sudo nano testcracks` ».



```
GNU nano 7.2 testcracks  
root:x:0:0:root:/root:/usr/bin/zsh  
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin  
bin:x:2:2:bin:/bin:/usr/sbin/nologin  
sys:x:3:3:sys:/dev:/usr/sbin/nologin  
sync:x:4:65534:sync:/bin:/bin/sync  
games:x:5:60:games:/usr/games:/usr/sbin/nologin  
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin  
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin  
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin  
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin  
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin  
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin  
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin  
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin  
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin  
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin  
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin  
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin  
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin  
systemd-timesync:x:992:992:systemd Time Synchronization:/:/usr/sbin/nologin  
messagebus:x:100:102::/nonexistent:/usr/sbin/nologin  
tss:x:101:104:TPM software stack,,,:/var/lib/tpm:/bin/false  
strongswan:x:102:65534::/var/lib/strongswan:/usr/sbin/nologin  
tcpdump:x:103:105::/nonexistent:/usr/sbin/nologin  
usbmux:x:104:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin  
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin  
dnsmasq:x:106:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin  
avahi:x:107:108:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin  
speech-dispatcher:x:108:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false  
pulse:x:109:110:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin  
lightdm:x:110:112:Light Display Manager:/var/lib/lightdm:/bin/false  
saned:x:111:114::/var/lib/saned:/usr/sbin/nologin  
polkitd:x:991:991:polkit:/nonexistent:/usr/sbin/nologin  
rtkit:x:112:115:RealtimeKit,,,:/proc:/usr/sbin/nologin  
colord:x:113:116:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin  
nm-openvpn:x:114:117:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin  
_galera:x:116:65534::/nonexistent:/usr/sbin/nologin  
mysql:x:117:120:MariaDB Server,,,:/nonexistent:/bin/false  
stunnel4:x:990:990:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin  
_rpc:x:118:65534::/run/rpcbind:/usr/sbin/nologin  
geoclue:x:119:122::/var/lib/geoclue:/usr/sbin/nologin  
Debian-snmpp:x:120:123::/var/lib/snmpp:/bin/false  
sslh:x:121:124::/nonexistent:/usr/sbin/nologin  
ntpsec:x:122:127::/nonexistent:/usr/sbin/nologin  
redsocks:x:123:128::/var/run/redsocks:/usr/sbin/nologin  
rwhod:x:124:65534::/var/spool/rwho:/usr/sbin/nologin
```

Après avoir réalisé les 2 étapes nous avons laissé John s'occuper du reste et pour cela il nous restait à taper la commande « `john testcracks -format=crypt` »


```
(kali@kali)-[~]
$ john testcracks -format=crypt
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 94 candidates buffered for the current salt, minimum 96 needed for performance.
kali (kali)
1g 0:00:00:00 DONE 1/3 (2024-02-12 17:07) 1.694g/s 159.3p/s 159.3c/s 159.3C/s kali..Kali9
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Ensuite nous avons taper la commande « `sudo nano /usr/share/john/password.lst` » qui permet de voir les mots passe et de vérifier si les utilisateurs possèdent un mot de passe référencé dans la liste.

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

Puis le système nous à envoyer la liste suivante

```
kali@kali: ~
File Actions Edit View Help
GNU nano 7.2 /usr/share/john/password.lst
#comment: This list has been compiled by Solar Designer of Openwall Project
#comment: in 1996 through 2011. It is assumed to be in the public domain.
#comment:
#comment: This list is based on passwords most commonly seen on a set of Unix
#comment: systems in mid-1990's, sorted for decreasing number of occurrences
#comment: (that is, more common passwords are listed first). It has been
#comment: revised to also include common website passwords from public lists
#comment: of "top N passwords" from major community website compromises that
#comment: occurred in 2006 through 2010.
#comment:
#comment: Last update: 2011/11/20 (3546 entries)
#comment:
#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

canada
hello
ranger
shadow
baseball
donald
harley
hockey
letmein
maggie
mike
mustang

[ Read 3559 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^N Replace    ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo
```

Et pour finir nous avons taper la commande qui affiche les utilisateurs qui contiennent les mots de passe en tapant la commande suivante « john -show testcracks ».

```
(kali㉿kali)-[~]  
$ john -show testcracks  
kali:kali:1000:1000:,,,:/home/kali:/usr/bin/zsh  
  
1 password hash cracked, 0 left
```