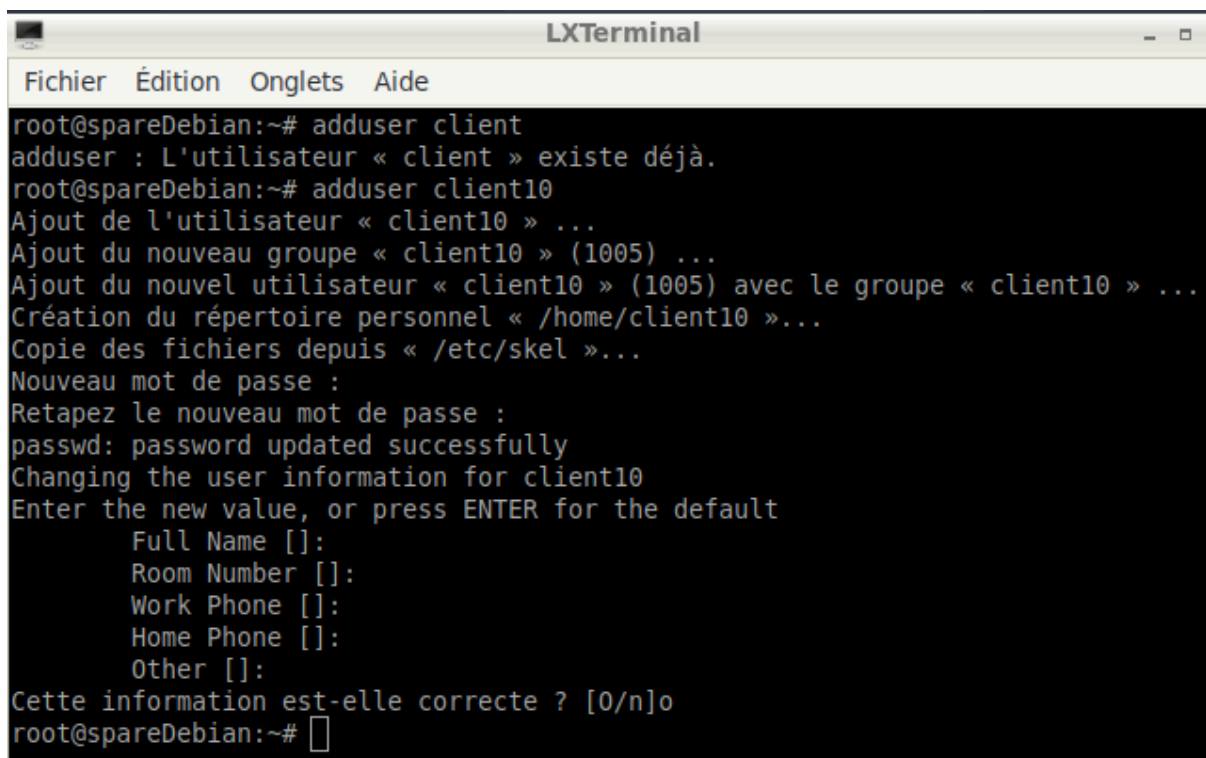


Compte-rendu (Sécurisation des mots de passe)

J'ai commencé par installer John the ripper via Kali puis un OphCrack via Debian.

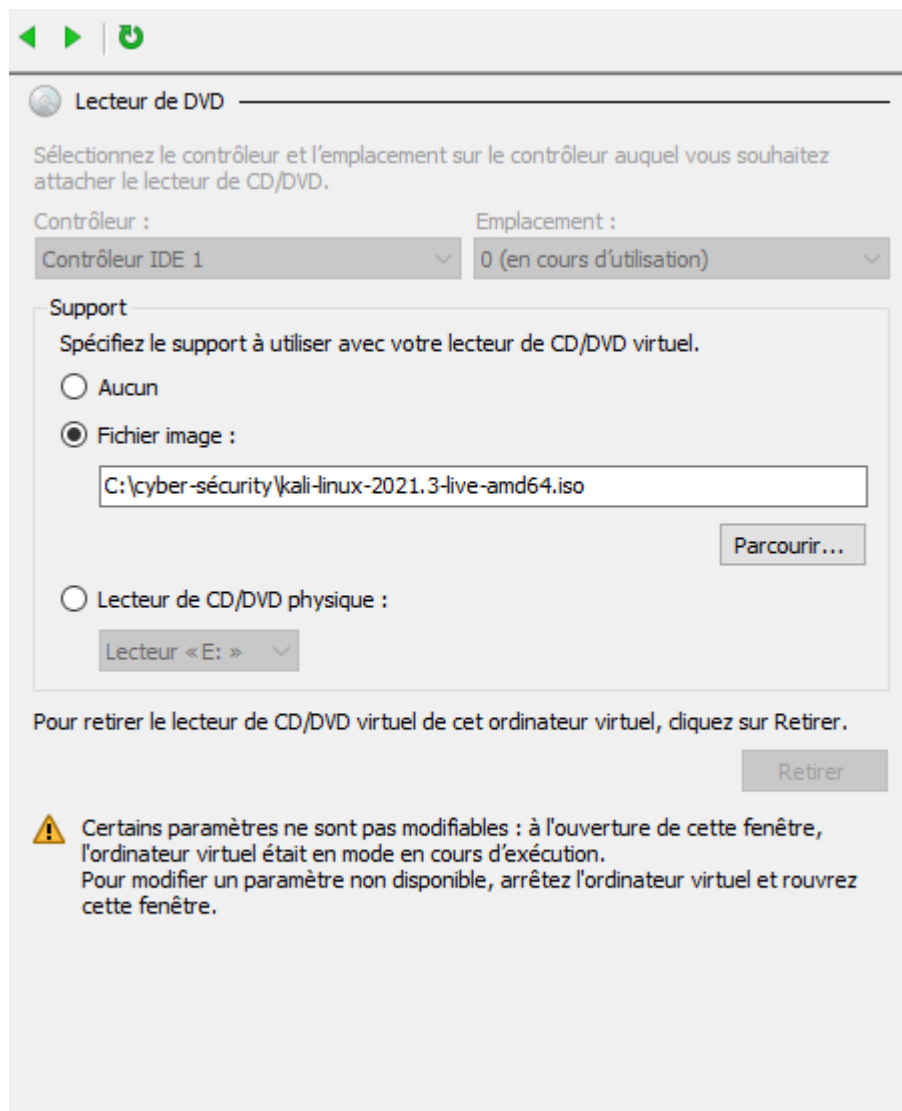
Nous sommes les Black hat car on n'a pas d'informations sur la cible.

Ensuite, j'ai créé 2 deux utilisateurs avec des mot de passe différent un inférieur à 8 caractères et l'autre supérieur à 8 caractères sur ma VM linux.



```
LXTerminal
Fichier  Édition  Onglets  Aide
root@spareDebian:~# adduser client
adduser : L'utilisateur « client » existe déjà.
root@spareDebian:~# adduser client10
Ajout de l'utilisateur « client10 » ...
Ajout du nouveau groupe « client10 » (1005) ...
Ajout du nouvel utilisateur « client10 » (1005) avec le groupe « client10 » ...
Création du répertoire personnel « /home/client10 »...
Copie des fichiers depuis « /etc/skel »...
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd: password updated successfully
Changing the user information for client10
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Cette information est-elle correcte ? [0/n]o
root@spareDebian:~#
```

Une fois j'ai créé les 2 utilisateurs, il faudra mettre une Iso Kali linux Live, pour cela il faut aller dans les paramètres de la vm puis il faudra booter sur un lecteur de disque.



Une fois la vm est en marche il faudra changer le clavier QWERTY en AZERTY à l'aide de la commande **setxkbmap fr**.



Prochainement, il faut gerer la partition Linux avec le commande **fdisk -l** puis on cherche la partition la plus volumineuse.

```
root@kali: ~  
File Actions Edit View Help  
#  
(root@kali)~  
# fdisk -l  
  
Disk /dev/sda: 8 GiB, 8589934592 bytes, 16777216 sectors  
Disk model: Virtual Disk  
Units: sectors of 1 * 512 = 512 bytes  
Sector size (logical/physical): 512 bytes / 512 bytes  
I/O size (minimum/optimal): 512 bytes / 512 bytes  
Disklabel type: dos  
Disk identifier: 0xdef132f3  
  
Device      Boot      Start         End      Sectors  Size Id Type  
/dev/sda1   *          2048      14774272    14774272    7G 83 Linux  
/dev/sda2             14778366  16775167    1996802    975M  5 Extended  
/dev/sda5             14778368  16775167    1996800    975M 82 Linux swap / Solaris  
  
Disk /dev/loop0: 3.33 GiB, 3574292480 bytes, 6981040 sectors  
Units: sectors of 1 * 512 = 512 bytes  
Sector size (logical/physical): 512 bytes / 512 bytes  
I/O size (minimum/optimal): 512 bytes / 512 bytes  
  
(root@kali)~  
#
```

Pour moi c'était sda1, et vous pouvez voir la partition avec la
mount /dev/sda1 /mnt

```
root@kali: /usr/share/wordlists  
File Actions Edit View Help  
root@kali: /usr/share/wordlists x root@kali: ~ x  
egate,memory_recursiveprot)  
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)  
none on /sys/fs/bpf type bpf (rw,nosuid,nodev,noexec,relatime,mode=700)  
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=29,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=20654)  
debugfs on /sys/kernel/debug type debugfs (rw,nosuid,nodev,noexec,relatime)  
tracefs on /sys/kernel/tracing type tracefs (rw,nosuid,nodev,noexec,relatime)  
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime,pagesize=2M)  
mqueue on /dev/mqueue type mqueue (rw,nosuid,nodev,noexec,relatime)  
configfs on /sys/kernel/config type configfs (rw,nosuid,nodev,noexec,relatime)  
fusectl on /sys/fs/fuse/connections type fusectl (rw,nosuid,nodev,noexec,relatime)  
sunrpc on /run/rpc_pipefs type rpc_pipefs (rw,relatime)  
tmpfs on /tmp type tmpfs (rw,nosuid,nodev,relatime)  
binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc (rw,nosuid,nodev,noexec,relatime)  
tmpfs on /run/user/1000 type tmpfs (rw,nosuid,nodev,relatime,size=193248k,nr_inodes=48312,mode=700,uid=1000,gid=1000)  
gvfsd-fuse on /run/user/1000/gvfs type fuse.gvfsd-fuse (rw,nosuid,nodev,relatime,user_id=1000,group_id=1000)  
/dev/sda1 on /mnt type ext4 (rw,relatime)  
  
(root@kali)~/usr/share/wordlists  
#
```

Ensuite, les logins et mots de passe sur une Debian se trouvent dans les fichiers `/mnt/etc/passwd` et `/etc/shadow`.

```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~ x root@kali: ~ x  
GNU nano 5.4 /mnt/etc/passwd  
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/no>  
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin  
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin  
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr>  
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sb>  
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin  
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin  
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin  
pi:x:1000:1000:pi,,,:/home/pi:/bin/bash  
systemd-coredump:x:999:999:systemd Core Dumper:./usr/sbin/nologin  
usbmux:x:106:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin  
rtkit:x:107:112:RealtimeKit,,,:/proc:/usr/sbin/nologin  
avahi:x:108:113:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin  
geoclue:x:109:114::/var/lib/geoclue:/usr/sbin/nologin  
pulse:x:110:115:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin  
lightdm:x:111:117:Light Display Manager:/var/lib/lightdm:/bin/false  
client1:x:1001:1001:client1,,,:/home/client1:/bin/bash  
client2:x:1002:1002,,,:/home/client2:/bin/bash  
client3:x:1003:1003,,,:/home/client3:/bin/bash  
client:x:1004:1004:client,,,:/home/client:/bin/bash  
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute  
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify
```

```
root@kali: ~
File Actions Edit View Help
GNU nano 5.4 /etc/shadow
root:*:19269:0:99999:7:::
daemon:*:18876:0:99999:7:::
bin:*:18876:0:99999:7:::
sys:*:18876:0:99999:7:::
sync:*:18876:0:99999:7:::
games:*:18876:0:99999:7:::
man:*:18876:0:99999:7:::
lp:*:18876:0:99999:7:::
mail:*:18876:0:99999:7:::
news:*:18876:0:99999:7:::
uucp:*:18876:0:99999:7:::
proxy:*:18876:0:99999:7:::
www-data:*:18876:0:99999:7:::
backup:*:18876:0:99999:7:::
list:*:18876:0:99999:7:::
irc:*:18876:0:99999:7:::
gnats:*:18876:0:99999:7:::
nobody:*:18876:0:99999:7:::
_apt:*:18876:0:99999:7:::
systemd-timesync:*:18876:0:99999:7:::
systemd-network:*:18876:0:99999:7:::
systemd-resolve:*:18876:0:99999:7:::
mysql:! :18876:0:99999:7:::

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

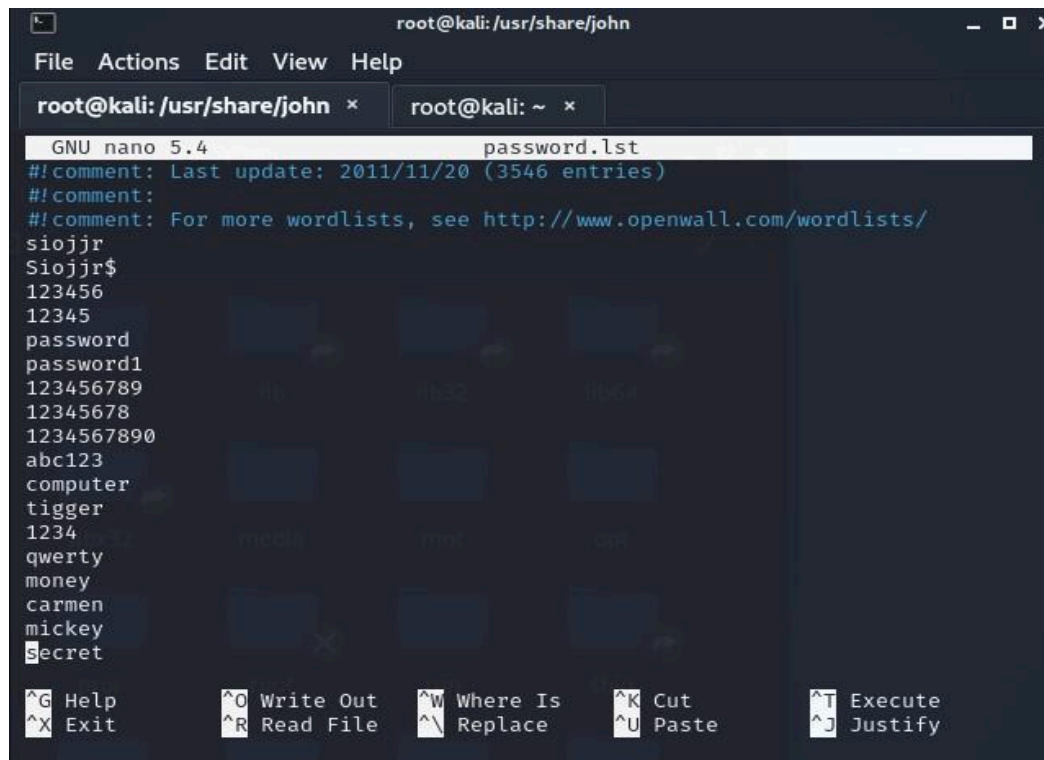
Maintenant, on va commencer par exécuter les différentes attaques proposées par l'outil John the ripper comme une attaque par dictionnaire (par défaut, le dictionnaire est **password.lst**).

```
root@kali: /usr/share/john
File Actions Edit View Help
root@kali: /usr/share/john x root@kali: ~ x
(root@kali)-[/usr/share/john]
# nano password.lst
Completing file
padlock2john.py* pdf2john.pl* pgpsda2john.py* pse2john.py*
pass_gen.pl* pem2john.py* pgpwe2john.py* ps_token2john.py*
password.lst pfx2john.py* potcheck.pl* pwsafe2john.py*
pcap2john.py* pgpdisk2john.py* prosody2john.py*

home lib libx2 libx4
libx12 media tmp opt
```

Dans le dictionnaire, on peut ajouter notre propre mot de passe.

J'ai ajouté mes 2 mots de passe siojrr et Siojrr\$.



The screenshot shows a terminal window with the title bar "root@kali: /usr/share/john". The window contains the nano text editor editing a file named "password.lst". The editor's menu bar includes "File", "Actions", "Edit", "View", and "Help". The status bar at the bottom displays various keyboard shortcuts: ^G Help, ^X Exit, ^O Write Out, ^R Read File, ^W Where Is, ^\ Replace, ^K Cut, ^U Paste, ^T Execute, and ^J Justify. The content of the file "password.lst" is as follows:

```
GNU nano 5.4 password.lst
#!/comment: Last update: 2011/11/20 (3546 entries)
#!/comment:
#!/comment: For more wordlists, see http://www.openwall.com/wordlists/
siojrr
Siojrr$
123456
12345
password
password1
123456789
12345678
1234567890
abc123
computer
tigger
1234
qwerty
money
carmen
mickey
Secret
```


On a utilisé la commande **john --wordlist /mnt/etc/shadow** pour afficher les mots de passe.

```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~ x root@kali: ~ x  
# cd  
(root@kali)-[~]  
# rm -rf .john  
(root@kali)-[~]  
# john --wordlist /mnt/etc/shadow  
Created directory: /root/.john  
Using default input encoding: UTF-8  
Loaded 6 password hashes with 6 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])  
Cost 1 (iteration count) is 5000 for all loaded hashes  
Press 'q' or Ctrl-C to abort, almost any other key for status  
siojrr (client1)  
Siojrr$ (client)  
siojrr (client2)  
siojrr (root)  
siojrr (pi)  
5g 0:00:00:02 DONE (2022-09-28 11:03) 2.040g/s 1448p/s 1709c/s 1709C/s basf..  
sss  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed  
(root@kali)-[~]  
#
```

On peut aussi utiliser le dictionnaire Rockyou.txt normal ou avec les règles .

```
root@kali: /usr/share/wordlists
File Actions Edit View Help
root@kali: /usr/share/wordlists x root@kali: ~ x

(root@kali)-[~]
# cd /usr/share/wordlists

(root@kali)-[/usr/share/wordlists]
# ls
dirb          fasttrack.txt  metasploit    rockyou.txt
dirbuster     fern-wifi      nmap.lst      wfuzz

(root@kali)-[/usr/share/wordlists]
# john --wordlist=rockyou.txt /mnt/etc/shadow
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (sha512crypt, crypt(3) $6$ [S
HA512 256/256 AVX2 4x])
Remaining 1 password hash
Cost 1 (iteration count) is 5000 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
█
```

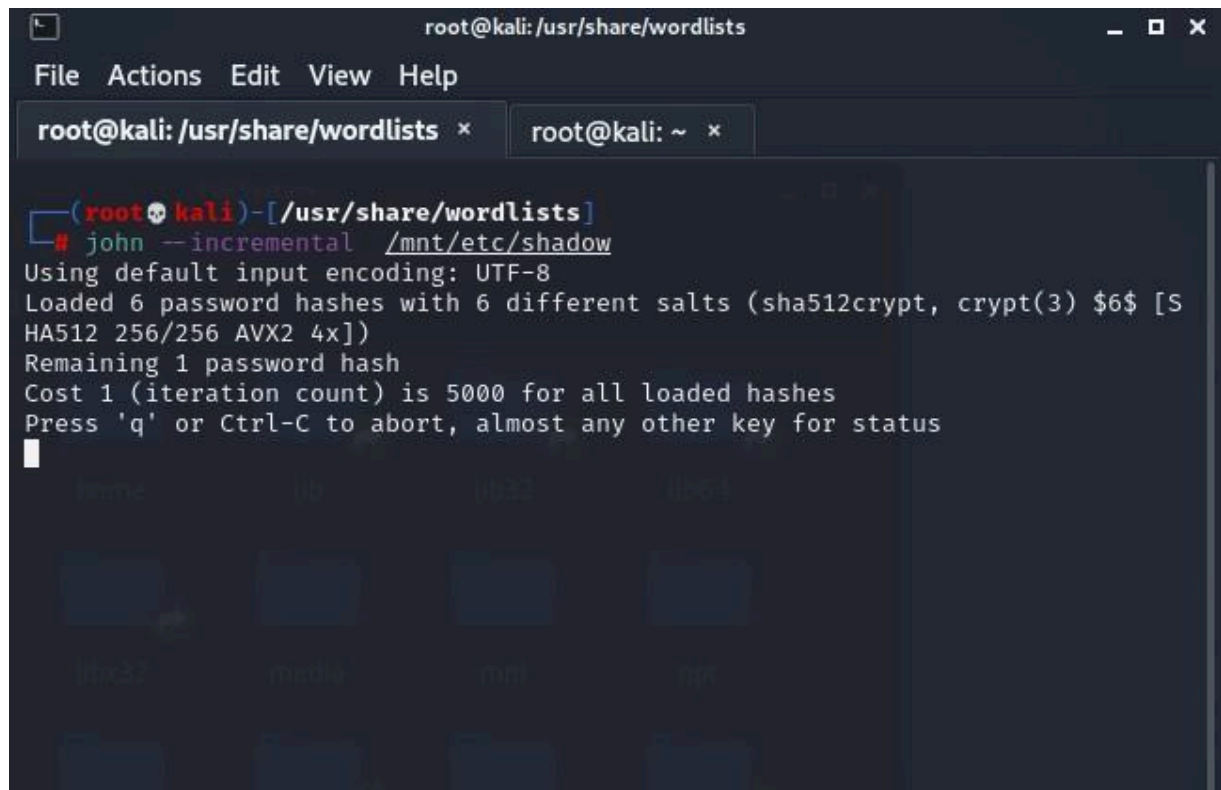
```
root@kali: /usr/share/wordlists
File Actions Edit View Help
root@kali: /usr/share/wordlists x root@kali: ~ x

(root@kali)-[/usr/share/wordlists]
#

(root@kali)-[/usr/share/wordlists]
# john --wordlist=rockyou.txt --rules /mnt/etc/shadow
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (sha512crypt, crypt(3) $6$ [S
HA512 256/256 AVX2 4x])
Remaining 1 password hash
Cost 1 (iteration count) is 5000 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
█
```


Enfin, on peut aussi faire une attaque incrémental (Force brute: test toute les combinaisons possible)

john --incremental /mnt/etc/shadow

A screenshot of a terminal window titled 'root@kali: /usr/share/wordlists'. The window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. Below the menu bar, there are two tabs: 'root@kali: /usr/share/wordlists' and 'root@kali: ~'. The terminal shows the command '(root@kali)-[/usr/share/wordlists] # john --incremental /mnt/etc/shadow'. The output of the command is: 'Using default input encoding: UTF-8', 'Loaded 6 password hashes with 6 different salts (sha512crypt, crypt(3) \$6\$ [SHA512 256/256 AVX2 4x])', 'Remaining 1 password hash', 'Cost 1 (iteration count) is 5000 for all loaded hashes', and 'Press \'q\' or Ctrl-C to abort, almost any other key for status'. A cursor is visible on the line following the status message. The terminal background is dark, and the text is light-colored.

Pour sécuriser l'authentification sur un poste, il faut avoir un mot de passe supérieur à 12 caractères avec une majuscule, nombres et des caractères spéciaux.