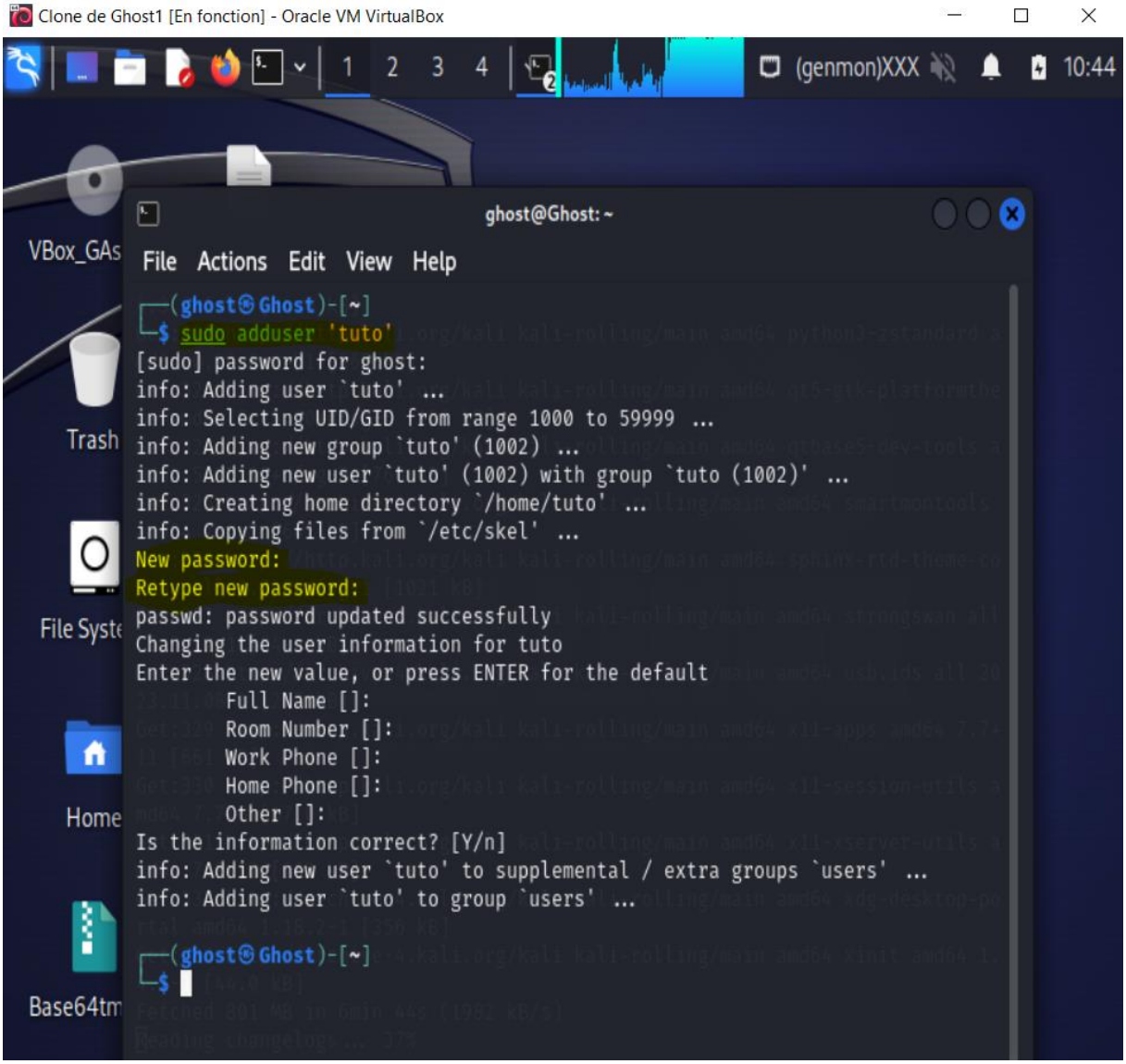
Avant tout, on va faire une mise à jour du système avec les commandes :

Sudo apt-get update

Sudo apt-get upgrade

Tout d'abord, avant de désactiver le compte root, on va en créer un nouveau et le donner toutes les autorisations :



On va ensuite se connecter au conpte pour vérifier :

```
┌──(ghost㉿Ghost)-[~]
└─$ su tuto
Password:
┌──(tuto㉿Ghost)-[/home/ghost]
└─$
```

On va enfin lui donner les droits root :

```
┌──(ghost㉿Ghost)-[~]
└─$ sudo usermod -aG sudo tuto

┌──(ghost㉿Ghost)-[~]
└─$ sudo chsh -s /bin/bash tuto
Password:
```

On va enfin désactiver le compte root :

Pour se faire, on va ouvrir le fichier /etc/passwd avec vim :

Sudo vim /etc/passwd :

```
┌──(ghost㉿Ghost)-[~]
└─$ sudo vim /etc/passwd

┌──(ghost㉿Ghost)-[~]
└─$
```

Puisqu’on veut modifier le fichier, on va sélectionner l’option E :

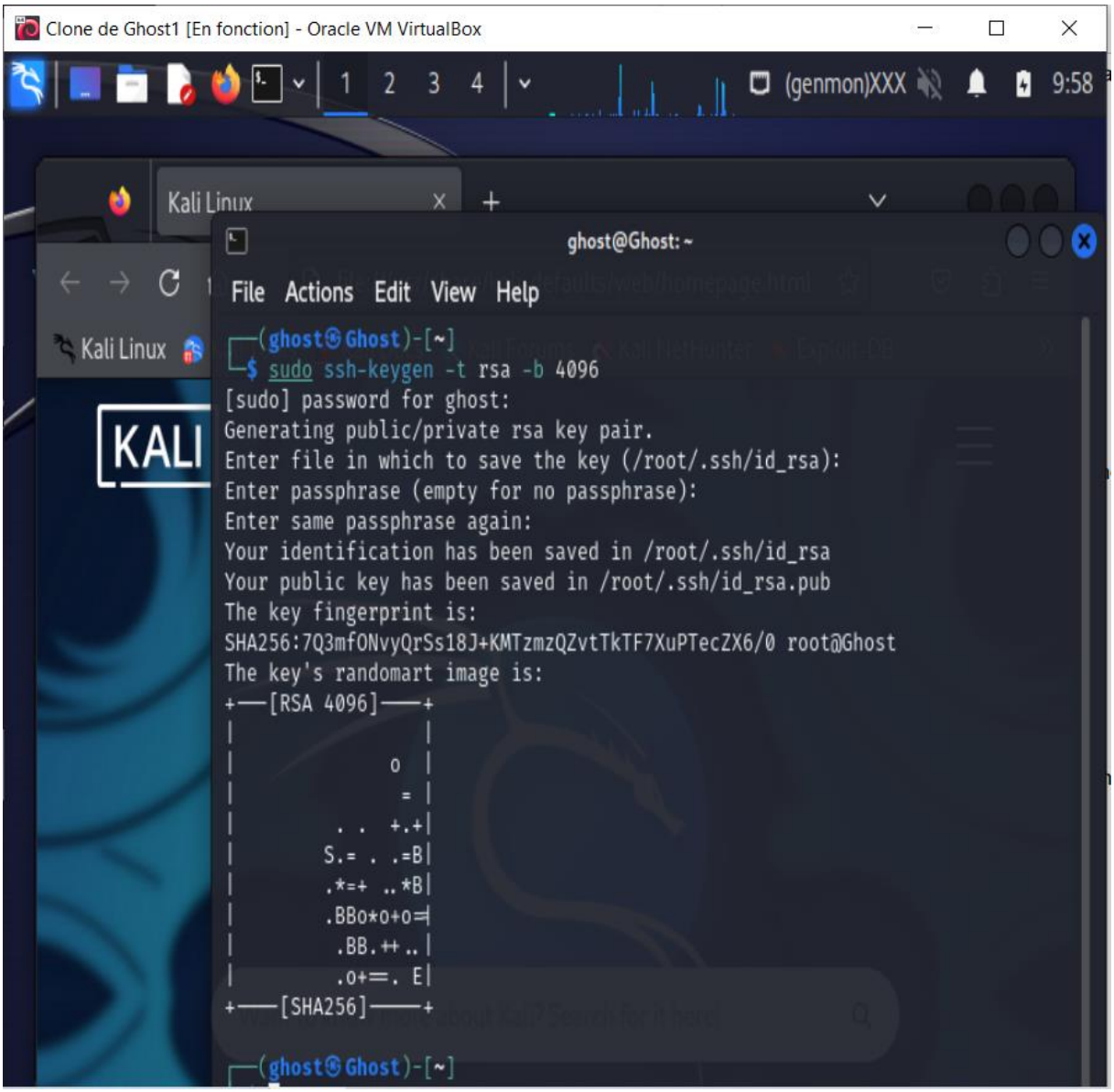
```
ghost@Ghost: ~
File  Actions  Edit  View  Help
E325: ATTENTION
Found a swap file by the name "/etc/.passwd.swp"
          owned by: root   dated: Thu Dec 07 09:20:12 2023
         file name: /etc/passwd
          modified: YES
         user name: root   host name: Ghost
        process ID: 1813
While opening file "/etc/passwd"
             dated: Thu Dec 07 10:44:32 2023
       NEWER than swap file!

(1) Another program may be editing the same file.  If this is the case,
    be careful not to end up with two different instances of the same
    file when making changes.  Quit, or continue with caution.
(2) An edit session for this file crashed.
    If this is the case, use ":recover" or "vim -r /etc/passwd"
    to recover the changes (see ":help recovery").
    If you did this already, delete the swap file "/etc/.passwd.swp"
    to avoid this message.

Swap file "/etc/.passwd.swp" already exists!
[O]pen Read-Only, (E)dit anyway, (R)ecover, (D)elete it, (Q)uit, (A)bort:
```

On va modifier cette partie du fichier :

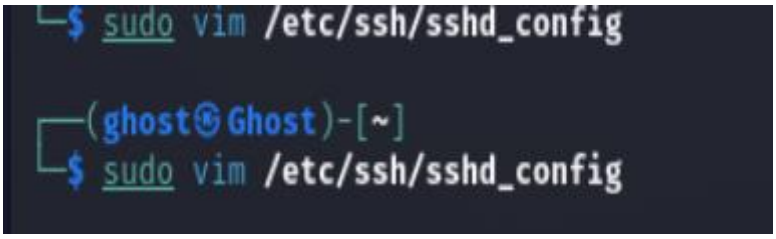
```
root:x:0:0:root:/root:/sbin/nologin
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
```

On quitte ensuite avec : Echap + : + wq. Cela va quitter le fichier en le sauvegardant.

Génération de la clé RSA



Désactivation de l'authentification par mot de passe dans le fichier /etc/ssh/sshd_config avec vim :



Modification du fichier, permission de yes en no :

```
# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication no
#PermitEmptyPasswords no
```

On va à présent activer la double authentification avec Google autrhentificator

Installation de Google authenticator :

```
┌──(ghost㉿Ghost)-[~]
└─$ sudo apt install libpam-google-authenticator
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  libpam-google-authenticator
0 upgraded, 1 newly installed, 0 to remove and 15 not upgraded.
Need to get 45.5 kB of archives.
After this operation, 138 kB of additional disk space will be used.
Get:1 http://archive-4.kali.org/kali kali-rolling/main amd64 libpam-google-au
thenticator amd64 20191231-2 [45.5 kB]
Fetched 45.5 kB in 1s (88.7 kB/s)
Selecting previously unselected package libpam-google-authenticator.
(Reading database ... 404421 files and directories currently installed.)
Preparing to unpack .../libpam-google-authenticator_20191231-2_amd64.deb ...
Unpacking libpam-google-authenticator (20191231-2) ...
Setting up libpam-google-authenticator (20191231-2) ...
Processing triggers for kali-menu (2023.4.6) ...
Processing triggers for man-db (2.12.0-1) ...
```

On va ensuite modifier le fichier se trouvant via :

Cd /etc/pam.d/

Sudo nano common-auth car le fichier est protegé

```
┌──(ghost㉿Ghost)-[~]
└─$ cd /etc/pam.d/

┌──(ghost㉿Ghost)-[/etc/pam.d]
└─$ ls
chfn                common-session-noninteractive  newusers   sshd
chpasswd            common.auth                    other      su
chsh                cron                           passwd     su-l
common-account      lightdm                        ppp        sudo
common-auth         lightdm-autologin              runuser    sudo-i
common-password     lightdm-greeter                runuser-l
common-session      login                          samba

┌──(ghost㉿Ghost)-[/etc/pam.d]
└─$ nano common-auth

┌──(ghost㉿Ghost)-[/etc/pam.d]
└─$ sudo nano common-auth
[sudo] password for ghost:

┌──(ghost㉿Ghost)-[/etc/pam.d]
└─$ sudo nano common-auth

┌──(ghost㉿Ghost)-[/etc/pam.d]
└─$
```

On va ensuite rajouté cette ligne :

```
# here are the per-package modules (the "Primary" block)
auth    required                        pam_google_authenticator.so echo_ver>
auth    [success=1 default=ignore]      pam_unix.so nullok
# here's the fallback if no module succeeds
auth    requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around

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

On va à present lancer le google-authenticator :

Pendant ce temps, j’ai téléchargé l’application google-authenticator sur mon téléphone et j’ai scanné le QR code. On obtient un code à 6 chiffres à taper sur la machine pour s’authentifier :

```
Your new secret key is: P55OYDJRSJ4P7BTHX2HKDFRRQA
Enter code from app (-1 to skip): 866894
Code confirmed
Your emergency scratch codes are:
  80934432
  33050562
  88263867
  33619906
  92972794

Do you want me to update your "/home/ghost/.google_authenticator" file? (y/n) y

Do you want to disallow multiple uses of the same authentication
token? This restricts you to one login about every 30s, but it increases
your chances to notice or even prevent man-in-the-middle attacks (y/n) y

By default, a new token is generated every 30 seconds by the mobile app.
In order to compensate for possible time-skew between the client and the server,
we allow an extra token before and after the current time. This allows for a
time skew of up to 30 seconds between authentication server and client. If you
experience problems with poor time synchronization, you can increase the window
from its default size of 3 permitted codes (one previous code, the current
code, the next code) to 17 permitted codes (the 8 previous codes, the current
code, and the 8 next codes). This will permit for a time skew of up to 4 minutes
between client and server.
Do you want to do so? (y/n) y

If the computer that you are logging into isn't hardened against brute-force
login attempts, you can enable rate-limiting for the authentication module.
By default, this limits attackers to no more than 3 login attempts every 30s.
Do you want to enable rate-limiting? (y/n) y

┌──(ghost㉿Ghost)-[/etc/pam.d]
└─$
```