

Franck Ridel

```
# dnf install freedom
```

Qubes OS: Ouvrir les liens et documents dans une autre appVM



QUBES OS
A REASONABLY SECURE OPERATING SYSTEM

Dans [Qubes OS](#), il est possible (*Même recommandé*) d'ouvrir automatiquement les liens suspects dans une autre [VM](#). Nous allons nous baser sur [un article de Micah Lee](#) et en étendre le principe aux PDF et aux images.

Présentation de Qubes OS

Jusqu'à présent je n'en ai jamais parlé ici, mais j'utilise Qubes OS depuis la version 3.1 que j'ai découverte en mai dernier.

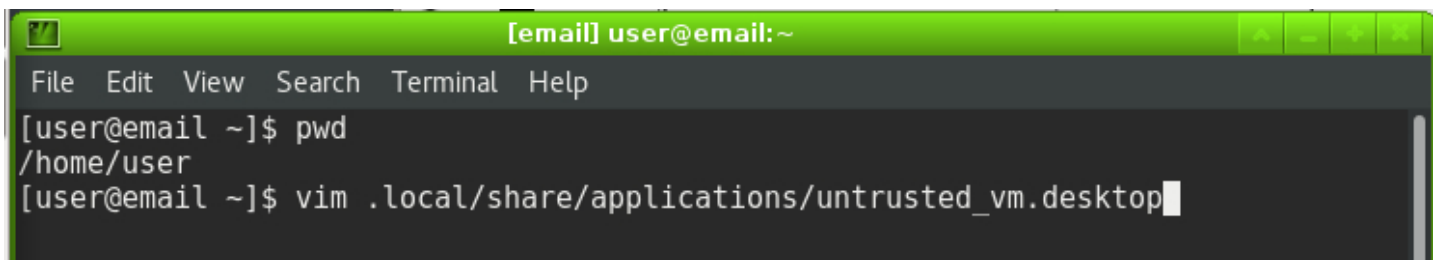
Qubes OS est basé sur [Xen](#) (un [hyperviseur](#) de type 1 ou bare-metal), dont les particularités sont d'utiliser un [micro-noyau](#) et de [sécuriser par l'isolation](#). Il permet de faire tourner, entres autres, des distrib comme [Fedora](#), [Debian](#), ou aussi [Whonix](#) (un OS divisé en 2 parties qui utilise le [réseau Tor](#)), dans des [VM](#) toutes

[cloisonnées](#). Il est possible d'ajouter d'autres systèmes d'exploitation [à partir de ceux déjà installés](#), et aussi d'y installer [Windows](#). Cette isolation entre les VM ainsi que son système à [micro-noyau](#) permettent de renforcer la sécurité et d'avoir différentes [configurations réseaux](#) ou offline sur un même ordi, gérées par des [netVM](#) et administrées sur un même [manager](#).

à méthode de Micah Lee

Translate »

L'idée est d'utiliser la commande [qvm-open-in-vm](#) dans un fichier .desktop afin d'automatiser l'ouverture d'un lien vers une autre VM, ceci afin d'éviter toute compromission en cas de mail frauduleux. Tout d'abord, créons ce fichier .desktop dans lequel nous allons écrire le script. Ici, je l'ai appelé **untrusted_vm** parce-qu'il redirigera l'ouverture des documents dans la VM nommée « untrusted ». Mais si vous voulez l'ouvrir dans une autre VM, adaptez le nom (*Rien d'obligatoire dans le choix du nom, c'est juste pour se repérer*).



```
[email] user@email:~
File Edit View Search Terminal Help
[user@email ~]$ pwd
/home/user
[user@email ~]$ vim .local/share/applications/untrusted_vm.desktop
```

Ensuite, entrez-y le code suivant :

```
[Desktop Entry]
Encoding=UTF-8
Name=BrowserVM
Exec=qvm-open-in-vm untrusted %u
Terminal=false
X-MultipleArgs=false
Type=Application
Categories=Network;WebBrowser;
MimeType=x-scheme-handler/unknown;x-scheme-
handler/about;text/html;text/xml;application/xhtml+xml;application/xml;appli
cation/vnd.mozilla.xul+xml;application/rss+xml;application/rdf+xml;image/gif
;image/jpeg;image/png;x-scheme-handler/http;x-scheme-handler/https;
```

```
[email] user@email:~
File Edit View Search Terminal Help
[Desktop Entry]
Encoding=UTF-8
Name=BrowserVM
Exec=qvm-open-in-vm untrusted %u
Terminal=false
X-MultipleArgs=false
Type=Application
Categories=Network;WebBrowser;
MimeType=x-scheme-handler/unknown;x-scheme-handler/about;text/html;text/xml;appl
ication/xhtml+xml;application/xml;application/vnd.mozilla.xul+xml;application/rs
s+xml;application/rdf+xml;image/gif;image/jpeg;image/png;x-scheme-handler/http;x
-scheme-handler/https;
```

À la ligne `Exec=qvm-open-in-vm`, remplacez « **untrusted** » par le nom de la VM vers laquelle vous voulez rediriger l'ouverture des liens.

Ensuite, nous allons définir ce script comme navigateur par défaut avec la commande `xdg-settings set default-web-browser untrusted_vm.desktop`

```
[email] user@email:~
File Edit View Search Terminal Help
[user@email ~]$ xdg-settings set default-web-browser untrusted_vm.desktop
[user@email ~]$
```

Étendons le principe aux images et aux PDF

Maintenant que nous avons automatisé l'ouverture des liens vers une autre VM, nous allons utiliser le même script pour l'appliquer à l'ouverture de fichiers.

Lorsque nous avons entré la commande `xdg-settings`, un fichier mimeapps.list a été créé dans `/home/user/.config/`. Ouvrons le.

```
[email] user@email:~
File Edit View Search Terminal Help
[user@email ~]$ vim .config/mimeapps.list
```

[illegible]

```
[email] user@email: ~
File Edit View Search Terminal Help

[Default Applications]
text/html=untrusred_vm.desktop
x-scheme-handler/http=untrusred_vm.desktop
x-scheme-handler/https=untrusred_vm.desktop
x-scheme-handler/about=untrusred_vm.desktop
x-scheme-handler/unknown=untrusred_vm.desktop

image/pdf=untrusred_vm.desktop
image/jpg=untrusred_vm.desktop
image/gif=untrusred_vm.desktop
image/png=untrusred_vm.desktop
~
~
~
~
~
~
~
~
~
~
-- INSERT -- 13,1 All
```

Nous pouvons maintenant tester. Je vais prendre le mail d'un pirate pré-pubère qui tente [un phishing](#) aussi ridicule que lui.

↩ Reply ➡ Forward 📁 Archive 🗑 Junk 🗑 Delete ⌵ More

From L'équipe Gmail <cenacletanamakoa@gmail.com> ☆

Subject **Connexion Suspecte** 12/23/2016 07:30 AM

To

Bcc Me ☆

Bonjour,

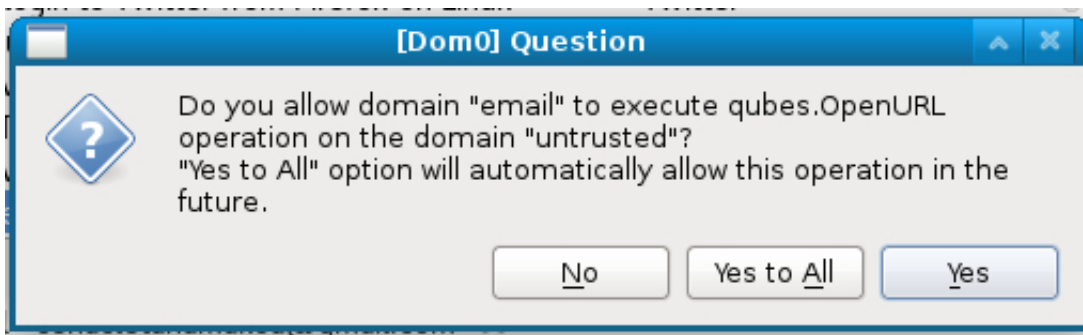
Nous avons constaté que vous accédez à votre compte Gmail Mail depuis une application de messagerie non-Gmail qui utilise peut-être une méthode de connexion moins sécurisée. L'utilisation d'une application de messagerie avec une méthode de connexion moins sécurisée peut rendre votre compte Gmail plus vulnérable aux menaces.

Nous recommandons vivement d'améliorer la sécurité de votre compte en cliquant

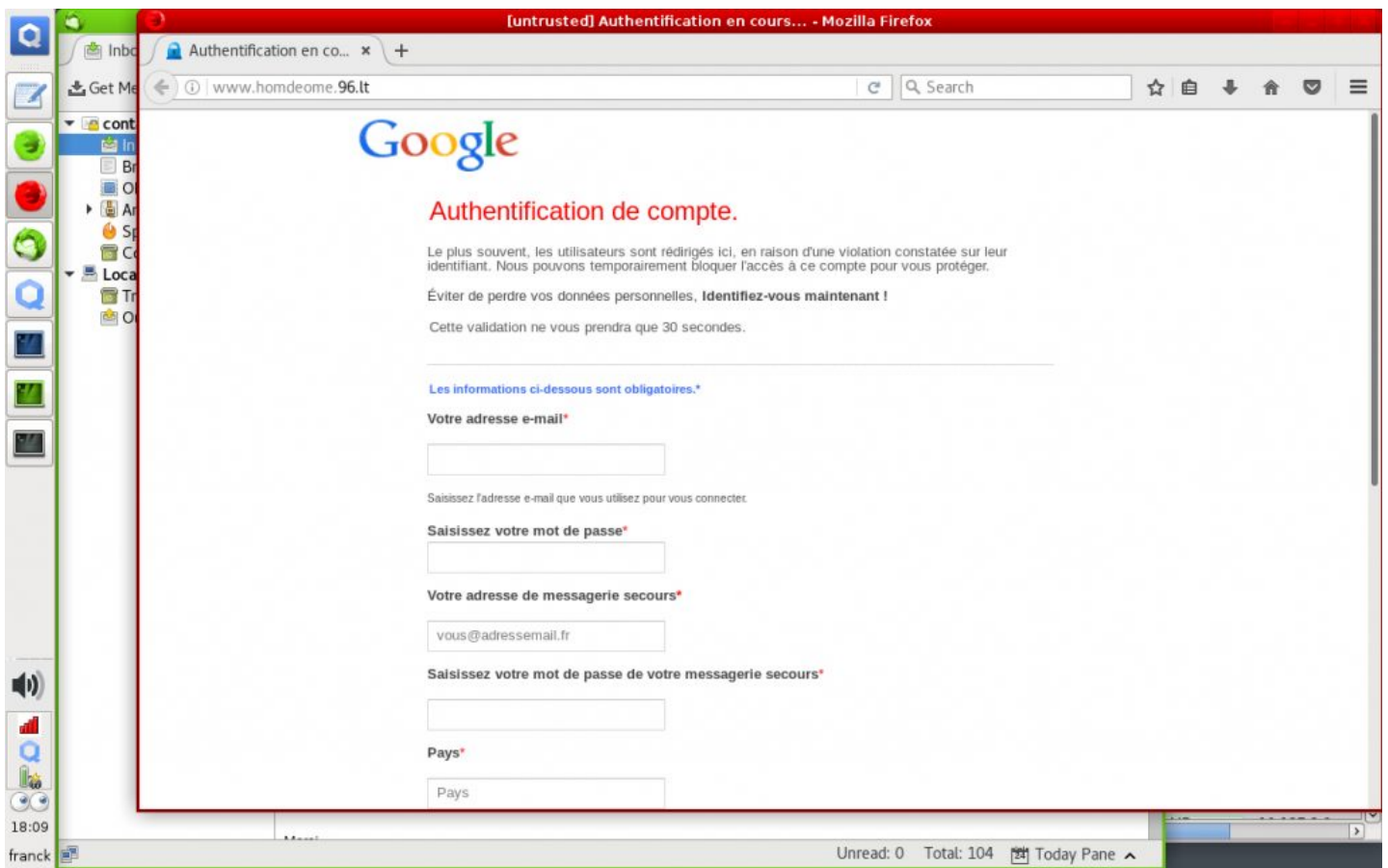
[Je sécurise mon compte](#)

.. .

Quand je clique sur le lien « Je sécurise mon compte », ce message apparaît (*Il apparaît juste la première fois*).



Je clique sur « Yes to All », et le lien s'ouvre bien dans l'appVM Untrusted



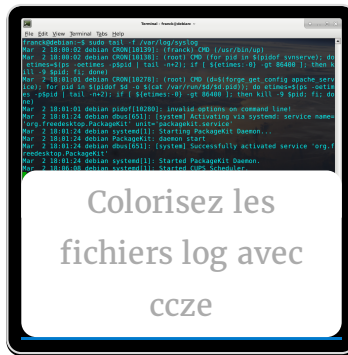
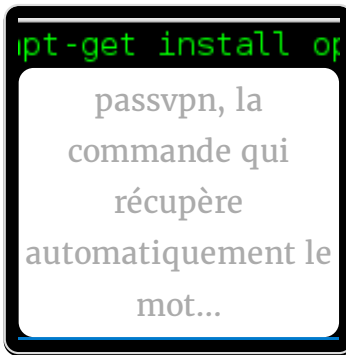
L'action est similaire pour l'ouverture des PDF et images.

Améliorations à faire

J'ai tenté rapidement de remplacer, dans le fichier .desktop à la ligne Exec, le nom de la VM par la variable `$dispvm` ou d'utiliser la commande [qvm-open-in-dvm](#) afin de rediriger vers une disposableVM (*Une VM jetable*). Avec la variable `$dispvm`, l'ouverture des liens s'effectue bien mais la connection échoue. Le problème doit

être minime mais je n'ai pas encore trouvé la solution. J'essaierai d'y remédier.

Articles similaires :



Franck Ridel / décembre 25, 2016 / Blog, GNU/Linux / appvm, dispvm, linux, qubes, script

Créé et édité par [Franck Ridel](#)

Certains droits réservés 

Les petits cailloux que vous semez derrière vous :

Vous êtes connecté depuis l'adresse IP : **159.50.16.169**

Vous êtes arrivé ici depuis : <http://franck-ridel.fr/tag/dispvm/>

Votre système d'exploitation est : **Windows**

Votre navigateur est : **Chrome**