1 AUTHENTIFICATION PAR MOT DE PASSE

Comme vu durant les exercices sur les fonctions de hachage, les outils pour casser les mots de passe sont nombreux et surtout très efficace face à des mots de passe "simples".

1.1. Conseils pour bien gérer ses mots de passe[1]

Messageries, réseaux sociaux, banques, administrations et commerces en ligne, réseaux et applications d'entreprise… La sécurité de l'accès à tous ces services du quotidien repose aujourd'hui essentiellement sur des mots de passe. Face à leur profusion, la tentation est forte d'en avoir une gestion trop simple. Une telle pratique serait dangereuse, car elle augmenterait considérablement les risques de compromettre la sécurité de vos accès.

Voici 10 bonnes pratiques à adopter pour gérer efficacement vos mots de passe.

1.1.1 Utilisez un mot de passe différent pour chaque service

Ainsi en cas de perte ou de vol d'un de vos mots de passe, seul le service concerné sera vulnérable. Comme nous l'avons démontré dans le Labo1, la fuite de données est fréquente.

Dans le cas contraire, tous les services pour lesquels vous utilisez le même mot de passe compromis seraient piratables.

https://www.dailymotion.com/video/x6lv2v2

1.1.2 Utilisez un mot de passe suffisamment long et complexe

Une technique d'attaque répandue, dite par « force brute », consiste à essayer toutes les combinaisons possibles de caractères jusqu'à trouver le bon mot de passe. Réalisées par des ordinateurs, ces attaques peuvent tester des dizaines de milliers de combinaisons par seconde. Pour empêcher ce type d'attaque, il est admis qu'un bon mot de passe doit comporter au minimum 12 signes mélangeant des majuscules, des minuscules, des chiffres et des caractères spéciaux.

1.1.3 Utilisez un mot de passe impossible à deviner

https://www.dailymotion.com/video/x7xagic - « Pourquoi dit-on mot de passe et pas mot de passoire ? »

Une autre technique d'attaque utilisée par les pirates est d'essayer de « deviner » votre mot de passe. Évitez donc d'employer dans vos mots de passe des informations personnelles qui pourraient être faciles à retrouver (sur les réseaux sociaux par exemple), comme le prénom de votre enfant, une date anniversaire ou votre groupe de musique préféré.

Évitez également les suites logiques simples comme 123456, azerty, abcdef… qui font partie des listes de mots de passe les plus courants et qui sont les premières combinaisons qu'essaieront les cybercriminels pour tenter de forcer vos comptes.

[1] https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe (Publié le 23 nov. 2019)

Comment créer un mot de passe solide ?

– La méthode des premières lettres : Un tiens vaut mieux que deux tu l'auras

> 1tvmQ2tl'A

– La méthode phonétique : J'ai acheté huit CD pour cent euros cet après-midi

> ght8CD%E7am

Inventez votre propre méthode connue de vous seul !

1.1.4 Utilisez un gestionnaire de mots de passe

https://www.dailymotion.com/video/x7nwhwd - « La minute info »

Il est humainement impossible de retenir les dizaines de mots de passe longs et complexes que chacun est amené à utiliser quotidiennement. Ne commettez pas pour autant l'erreur de les noter sur un pense-bête que vous laisseriez à proximité de votre équipement, ni de les inscrire dans votre messagerie ou dans un fichier non protégé de votre ordinateur, ou encore dans votre téléphone mobile auquel un cybercriminel pourrait avoir accès. Apprenez à utiliser un gestionnaire de mot de passe sécurisé qui s'en chargera à votre place, pour ne plus avoir à retenir que le seul mot de passe qui permet d'en ouvrir l'accès.

KeePass, un gestionnaire de mots de passe sécurisé et gratuit

Ce petit logiciel libre et en français, certifié par l'ANSSI, permet de stocker en sécurité vos mots de passe pour les utiliser dans vos applications. KeePass dispose aussi d'une fonction permettant de générer des mots de passe complexes aléatoires.

1.1.5 Changez votre mot de passe au moindre soupçon

Vous avez un doute sur la sécurité d'un de vos comptes ou vous entendez qu'une organisation ou société chez qui vous avez un compte s'est faite pirater. N'attendez pas de savoir si c'est vrai ou pas. Changez immédiatement le mot de passe concerné avant qu'il ne tombe dans de mauvaises mains.

1.1.6 Ne communiquez jamais vos mots de passe à un tiers

Votre mot de passe doit rester secret. Aucune société ou organisation sérieuse ne vous demandera jamais de lui communiquer votre mot de passe par messagerie ou par téléphone. Même pour une « maintenance » ou un « dépannage informatique ». Si l'on vous demande votre mot de passe, considérez que vous êtes face à une tentative de piratage ou d'escroquerie.

1.1.7 N'utilisez pas vos mots de passe sur un ordinateur partagé

Les ordinateurs en libre accès que vous pouvez utiliser dans des hôtels, cybercafés et autres lieux publics peuvent être piégés et vos mots de passe peuvent être récupérés par un criminel. Si vous êtes obligé d'utiliser un ordinateur partagé ou qui n'est pas le vôtre, utilisez le mode de « navigation privée » du navigateur, qui permet d'éviter de laisser trop de traces informatiques, veillez à bien fermer vos sessions après utilisation et n'enregistrez jamais vos mots de passe dans le navigateur. Enfin, dès que vous avez à nouveau accès à un ordinateur de confiance, changez au plus vite tous les mots de passe que vous avez utilisés sur l'ordinateur partagé.

1.1.8 Activez la « double authentification » lorsque c'est possible

https://www.dailymotion.com/video/x6x85yy - *« La minute pratique »*

Pour renforcer la sécurité de vos accès, de plus en plus de services proposent cette option. En plus de votre nom de compte et de votre mot de passe, ces services vous demandent un code provisoire que vous pouvez recevoir, par exemple, par SMS sur votre téléphone mobile ou qui peut être généré par une application ou une clé spécifique que vous contrôlez. Ainsi grâce à ce code, vous seul pourrez autoriser un nouvel appareil à se connecter aux comptes protégés.

Quelques services proposant la double authentification

- *Outlook, Gmail, Yahoo Mail…*
- *Facebook, Instagram, LinkedIn, Twitter…*
- *Skype, WhatsApp…*
- *Amazon, eBay, Paypal…*
- *Apple iCloud, Dropbox, Google Drive, OneDrive…*

1.1.9 Changez les mots de passe par défaut des différents services auxquels vous accédez

De nombreux services proposent des mots de passe par défaut que vous n'êtes parfois pas obligé de changer. Ces mots de passe par défaut sont souvent connus des cybercriminels. Aussi, il est important de les remplacer au plus vite par vos propres mots de passe que vous contrôlez.

1.1.10 Choisissez un mot de passe particulièrement robuste pour votre messagerie

https://www.dailymotion.com/video/x7ny0l6 - *Gérer ses mots de passe*

Votre adresse de messagerie est généralement associée à beaucoup de vos comptes en ligne. Cela permet notamment de recevoir les liens de réinitialisation des mots de passe de vos autres comptes. Un cybercriminel qui réussirait à pirater votre messagerie pourrait facilement utiliser la fonction « mot de passe oublié » des différents services auxquels vous pouvez accéder, comme votre compte bancaire, pour en prendre le contrôle.

Votre mot de passe de messagerie est donc l'un des plus importants à protéger.

Article officiel repris du lien → https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe (Publié le 23 nov. 2019)

Suite à la lecture de cet article, commencez à rédiger un rapport personnel que vous nommerez **Lab2-UE19-Nom_Prénom.docx**. Numérotez-y vos chapitres (***1. Conseils à appliquer***). Reporter la liste des conseils que vous devrez suivre pour la bonne gestion de vos mots de passe (ceux que vous n'appliquez pas toujours).

2 LA DOUBLE AUTHENTIFICATION (2FA)

il s'agit d'ajouter un niveau d'authentification. Ainsi, lorsque l'on souhaite accéder à un service internet ou un appareil ou sur un logiciel, on doit s'authentifier via deux systèmes distincts. Le but est de protéger l'accès lorsque le mot de passe est compromis. Entre le phishing, les piratages de comptes clients, la fuite de bases de données, la seule protection par mots de passe n'est plus considérée comme sûre.

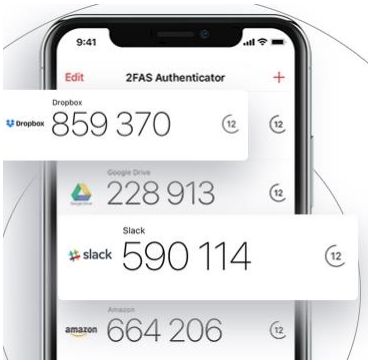
On trouve différentes méthodes de double authentification. La plus courante consiste à utiliser un mot de passe à usage unique (**OTP**, de l'anglais one-time password) qui est un mot de passe qui n'est valable que pour une session ou une transaction. Ces **OTP** ne peuvent pas être mémorisés, par conséquent, ils nécessitent des technologies complémentaires afin de s'en servir.

Certains utilisent des jetons d'authentification électroniques qui génèrent des **OTP** en utilisant un petit écran.

Il y a aussi des **OTP** générés du côté du serveur et envoyés à l'utilisateur en utilisant un canal de télécommunication (un message SMS la plupart du temps).

Enfin, dans certains systèmes, les OTP sont imprimés sur du papier que l'utilisateur est tenu de garder avec lui.

2.1. Mise en œuvre d'une 2FA



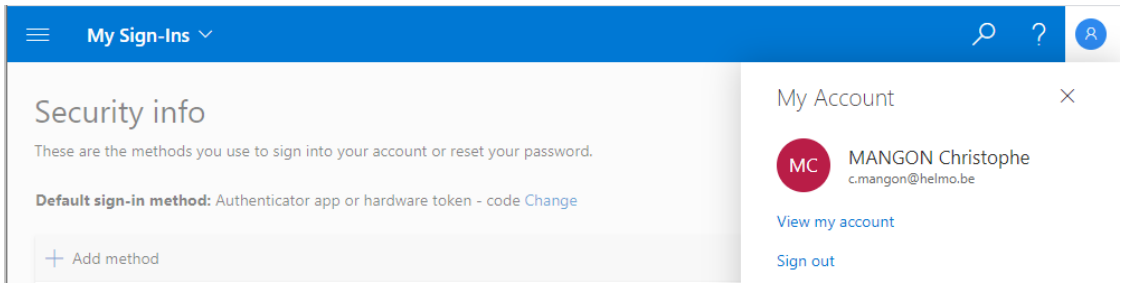
(***2. Procédure 2FA***) En tant que spécialiste en sécurité informatique, rédigez une procédure à destination de vos connaissances néophytes en IT.

Cette procédure doit décrire l'activation de la double authentification à partir d'un login personnel de votre choix (gmail, facebook, twitter, amazon, paypal, etc.). Réalisez des captures d'écran afin de dynamiser votre procédure et maquillez vos identifiants.

Utilisez votre smartphone, pour y installer une application 2FA de votre choix. Exemple : https://2fas.com/

2.2. Activez la 2FA sur votre compte Microsoft HELMo.

(***3. Procédure 2FA Microsoft HELMo***) Rédigez la même procédure en activant la 2FA sur votre compte Microsoft HELMo. Connectez-vous avec votre identifiant **...@student.helmo.be** sur la page https://mysignins.microsoft.com/security-info et ajoutez une méthode en utilisant la même application 2FA de l'exercice précédent sur votre smartphone (pas Microsoft Authentification app nécessairement). Finalisez cette procédure par une capture d'écran qui démontre l'activation de la 2FA sur votre compte. Exemple :



3 AUTHENTIFICATION DE WINDOWS

3.1. Analyse des systèmes disponibles

Lisez l'article https://www.malekal.com/windows-hello-options-connexion-windows-10/

(***4. Authentification Windows 10***) Répondez aux questions suivantes dans votre rapport :

1. Quels sont les dangers des comptes Microsoft ? Comment Microsoft a-t-il résolu ces risques de sécurité ?

2. Suite à cette lecture, quels sont les méthodes d'authentification que vous recommanderiez sur un Windows 10 ?

3. Pourquoi le code PIN de moins de 6 caractères est-il plus sécurisant qu'un mot de passe sur Windows 10 ?

4. Qu'est-ce que Windows Hello ? Tous les systèmes sous Windows 10 peuvent-ils l'utiliser et pourquoi ?

3.2. Mise en place de l'authentification sous Windows 10 (ou MacOS)

Afin que votre PC ne soit pas ouvert aux quatre vents, activez une sécurité au redémarrage ou à la sortir de veille.

Complétez le début de procédure pour sécuriser l'authentification sous Windows 10, ci-dessous.

4.1. Procédure d'authentification Windows 10

Cliquez sur l'icône **Windows** en bas à gauche puis sur **Paramètres**, **Comptes**, **Options de connexion**.

….

4.1.1 Programmez le verrouillage

….

4.1.2 Sécurisez le PC avec un code PIN

….

4.1.3 Sécurisez le PC sans mot de passe avec Windows Hello

….

4 SSH SERVEUR SOUS LINUX

4.1. Qu'est-ce que SSH et OpenSSH

- Secure Shell (SSH) est un programme. Mais aussi, un protocole de communication sécurisé. Grâce à SSH, on peut se connecter à distance sur une machine, transférer des fichiers.
- OpenSSH (OpenBSD Secure Shell) est un ensemble d'outils informatiques libres permettant des communications sécurisées sur un réseau informatique en utilisant le protocole SSH.

4.2. Installation du serveur OpenSSH

Sur Kali Linux, pour vérifier que le package est installé :

```
sudo apt list --installed openssh-server
Listing... Done
openssh-server/kali-rolling,now 1:8.3p1-1 amd64 [installed,automatic]
```

Pour réaliser l'installation, si celui-ci n'est pas installé :

```
sudo apt install openssh-server
```

4.3. Configuration du serveur OpenSSH

Activez le service OpenSSH au démarrage

```
sudo systemctl enable --now ssh.service
```

Pour configurer le serveur OpenSSH, il vous faut éditer le fichier **/etc/ssh/sshd_config** (**nano** ou **vi**).
Les consignes sont les suivantes :

1. Changez le port par défaut du service SSH (22), comme par exemple le port 1922.
2. Configurez uniquement le fichier de clé ed25519 que vous allez générer par après.
3. Configurez l'audit des tentatives de connexion avec le niveau AUTH.INFO.
4. N'autorisez pas la connexion en root (super administrateur sous Linux).
5. Pour éviter les attaques de type brut-force, n'autorisez que 6 tentatives consécutives.
6. Autorisé l'authentification par clé publique.
7. Ignorez le mécanisme de systèmes de confiance repris dans le fichier rhosts.
8. Autorisez l'authentification par mot de passe et bloquez les mots de passe vide.
9. Faite affichez le contenu du fichier /etc/issue.net que vous créerez par la suite.

(***5. Configuration SSH Linux***) Dans votre rapport faite un copié/collé du résultat de la commande : **grep -v '^\s*$\|^\s*\#' sshd_config**

Cette commande affiche le contenu de la configuration en retirant les lignes de commentaires commençant par un # ou les lignes vides. Remarquez l'utilisation d'une expression régulière.

4.4. Le banner SSH

Configurez le fichier /etc/issue.net avec le texte suivant :

```
sudo figlet SecSy Lab > /etc/issue.net
```

Faite un copié/collé de ce bloc dans votre **shell** :

```
sudo cat <<EOT >> /etc/issue.net
**********************************************************************
*                                                                    *
* This system is for the use of authorized users only.  Usage of     *
* this system may be monitored and recorded by system personnel.     *
*                                                                    *
* Anyone using this system expressly consents to such monitoring     *
* and is advised that if such monitoring reveals possible            *
* evidence of criminal activity, system personnel may provide the    *
* evidence from such monitoring to law enforcement officials.        *
*                                                                    *
**********************************************************************
EOT
```

Vérifiez que votre message banner affiché avant la connexion ssh est correct :
`cat /etc/issue.net`

4.5. Générer sa paire de clés SSH

Il s'agit des clés qui vont être liées à votre système linux. Elles doivent donc être recréées si vous copiez votre VM pour créer un nouvel environnement ou si elles ont été compromises. Ces clés garantissent l'authenticité de votre système, pour autant qu'elles soient vérifiées lors de la première connexion d'un nouveau client SSH.

Effacez les clés fournies par défaut sur votre installation Kali Linux
`rm -v /etc/ssh/ssh_host_*`

Pour créer sa paire de clés, on utilise l'utilitaire **ssh-keygen**. Mais attention, il faut générer des clés SSH suffisamment robustes ! L'historique **ssh-keygen -t rsa -b 1024** est à proscrire de nos jours. Je vous conseille de créer une clé **RSA** de 4096 octets ! Ou mieux, préférez la création de clés basés sur des courbes elliptiques: **ECDSA**, **Ed25519**.
`ssh-keygen -t ed25519 -f ssh_host_ed25519_key -N "" < /dev/null`

```
Explication des arguments :
      -t → type de clé
      -f → nom du fichier de clés
      -N → mot de passe sur le trousseau de clés
```

Protéger votre clé privée en lecture

Afin d'éviter la création d'autres types sur votre système, créez des fichiers vides associés.
`touch ssh_host_rsa_key ssh_host_ecdsa_key ssh_host_dsa_key`

Une fois, la configuration finalisée redémarrez le service SSH :

`sudo systemctl restart ssh.service`

4.6. Vérifier l'empreinte digitale de votre clé publique

Cette étape est TRES importante. On ne compte pas le nombre d'administrateurs systèmes qui se connectent à leurs environnements de production sans vérifier l'authenticité de la clé publique présentée à la première connexion SSH. Obtenez l'empreinte SHA256 de votre clé publique. Toujours sous VMware, exécutez la commande suivante dans un **shell** (Attention, l'empreinte affichée dans ce document ne peut être la même que la vôtre) :

```
ssh-keygen -lv -E sha256 -f /etc/ssh/ssh_host_ed25519_key.pub
256 SHA256:rabECeJL0YVIKxWZSHg7/VFdapMYWQXOOgvEUgETRlI root@kali-2020 (ED25519)
+--[ED25519 256]--+
|oo=*Eoo..+o+o    |
|oo+= =   o=.o    |
|..ooo +.. B      |
| .o..+.   + .    |
|  o.o...S .      |
| . o o.o +       |
|  o    + +       |
| . . . o         |
|  .    .         |
+----[SHA256]-----+
```

4.7. Connexion ssh

4.7.1 Sous Linux

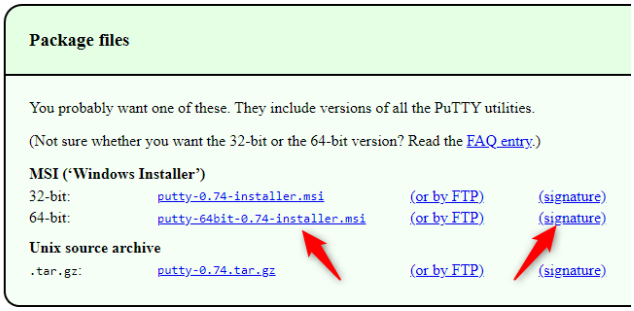
Sous linux, en ligne de commande :

```
ssh -o VisualHostKey=yes -p 1922 louis@127.0.0.1
The authenticity of host '[127.0.0.1]:1922 ([127.0.0.1]:1922)' can't be established.
ED25519 key fingerprint is SHA256:rabECeJL0YVIKxWZSHg7/VFdapMYWQXOOgvEUgETRlI.
+--[ED25519 256]--+
|oo=*Eoo..+o+o    |
|oo+= =   o=.o    |
|..ooo +.. B      |
| .o..+.   + .    |
|  o.o...S .      |
| . o o.o +       |
|  o    + +       |
| . . . o         |
|  .    .         |
+----[SHA256]-----+
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[127.0.0.1]:1922' (ED25519) to the list of known hosts.
 ____            ____        _          _
/ ___|  ___  ___/ ___| _   _| |    __ _| |__
\___ \ / _ \/ __\___ \| | | | |   / _` | '_ \
 ___) |  __/ (__ ___) | |_| | |__| (_| | |_) |
|____/ \___|\___|____/ \__, |_____\__,_|_.__/
                       |___/
*****************************************************************
*                                                               *
* This system is for the use of authorized users only.  Usage of *
* this system may be monitored and recorded by system personnel. *
*                                                               *
* Anyone using this system expressly consents to such monitoring *
* and is advised that if such monitoring reveals possible        *
* evidence of criminal activity, system personnel may provide the *
* evidence from such monitoring to law enforcement officials.    *
*                                                               *
*****************************************************************
louis@127.0.0.1's password:
```

Le système fonctionne, mais utilise encore une authentification par mot de passe !

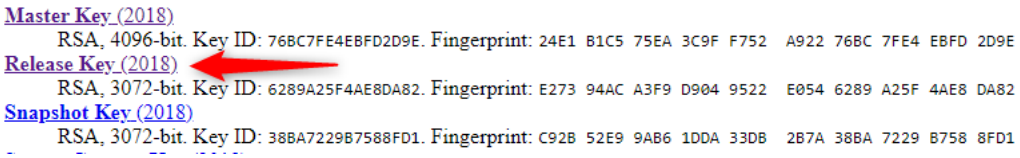
4.7.2 Sous Windows

Téléchargez l'application puTTY sur https://www.putty.org/ et le fichier de signature et de checksum.

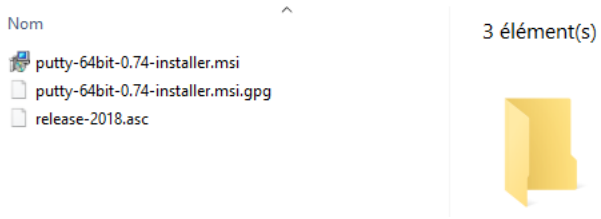


Pour récupérer la clé publique de puTTY visitez
https://www.chiark.greenend.org.uk/~sgtatham/putty/keys.html#pgpkeys

Vous devrez importer la Release Key de puTTY dans votre trousseau de clés.



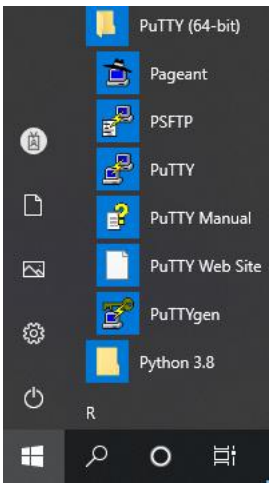
Pour valider l'authenticité de votre téléchargement, vous devriez avoir ces trois fichiers.



Ouvrez une invite de commande et importez la public key de puTTY :
```
gpg --import release-2018.asc
```

Vérifiez ensuite que le téléchargement correspond à la signature GPG :
```
gpg --verify putty-64bit-0.74-installer.msi.gpg putty-64bit-0.74-installer.msi
```

Si l'intégrité et l'authenticité du package sont vérifiées, réalisez l'installation de puTYY.



Pour éviter l'usage du traditionnel mot de passe, générez votre trousseau de clés SSH personnel :

Sur votre système Linux générez vos clés comme suit :

```
ssh-keygen -o -a 256 -t ed25519 -C "$(hostname)-$(date +'%d-%m-%Y')"
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/louis/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):
Enter same passphrase again: TAPEZ UNE PASSPHRASE QUE VOUS RETIENDREZ !!!
Your identification has been saved in /home/louis/.ssh/id_ed25519
```

```
Your public key has been saved in /home/louis/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:wPT0bKPRL9dQCGsQw6veVibsHDIcjyUPSUweso1stlg kali-2020-25-11-2020
The key's randomart image is:
+--[ED25519 256]--+
|     .o+.=... .. |
|    . Oo+.* ...  |
|     E.=.o.O .   |
|    = .=.o= o o  |
|   . .. @S . o . |
|      * * oo     |
|     . * =       |
|      . =        |
|       .         |
+----[SHA256]-----+
```

Vous avez deux clés créées dans votre dossier **~/.ssh**

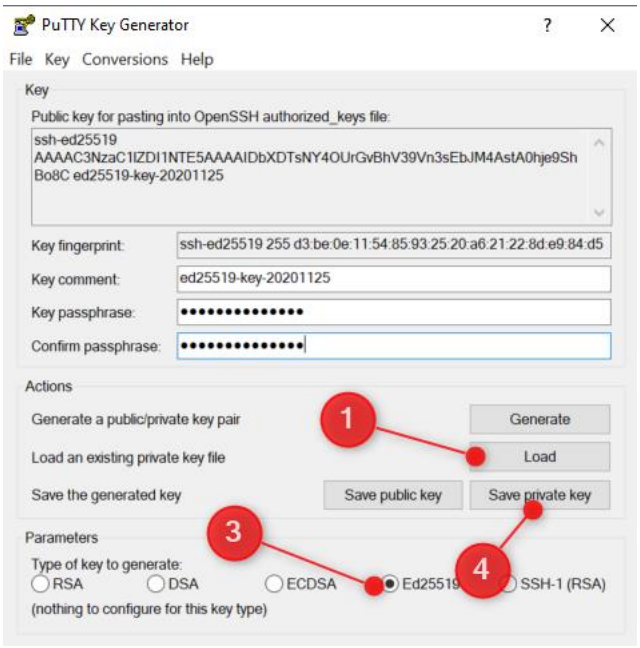
```
cd ~/.ssh
cat id_ed25519.pub > authorized_keys
```

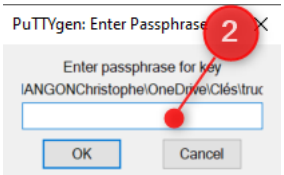
Copiez le contenu de votre fichier clé privé vers un fichier temporaire sur votre système windows.

truc-much.key

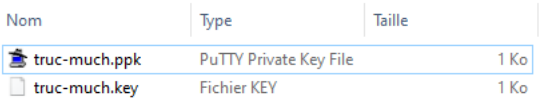
```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAABBACmFlczI1Ni1jdHIAAAAGYmNyeXB0AA
7sY70H8VZH/qR2AAABAAAAAAEAAAAzAAAAC3NzaC1lZDI1NTE5AAAA
XjLS1VnjrLQvI1HmahJ+/dnPJ1SsAAAAoOU+eerl/n6lAqbTEW6ggO
wLTJ29Bc4+qrisjqqftZEGgA5qpbMhbhNgiInc5a+JifjkTpCYkkbC
RNH8GdXvhIJdYfGyO/diAP/765LhqNJdA+HoKK5Y9rL5KOu+ynWFj5
gaiCSE5Axq88I8FxfZKbuIx85GuSMJY2X4Tq0=
-----END OPENSSH PRIVATE KEY-----
```

Sur votre système Windows ouvrez le PuTTYgen pour importer la clé privée en clé PuTTY compatible :

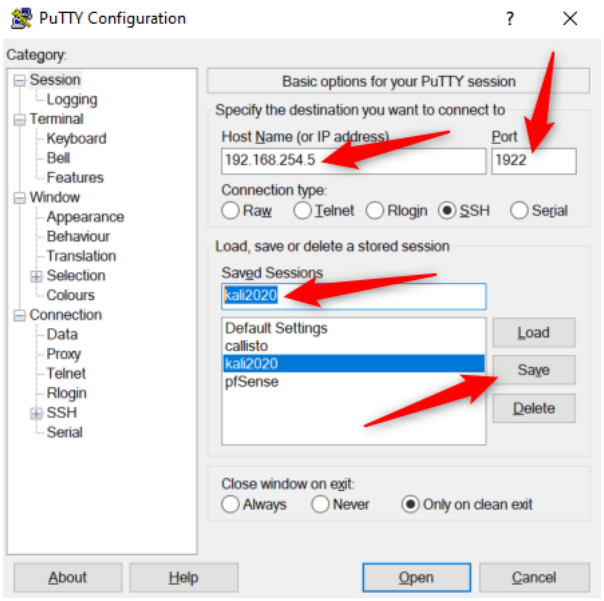




Suite à cette manipulation, vous obtenez un fichier .ppk qui est votre clé privée compatible PuTTY

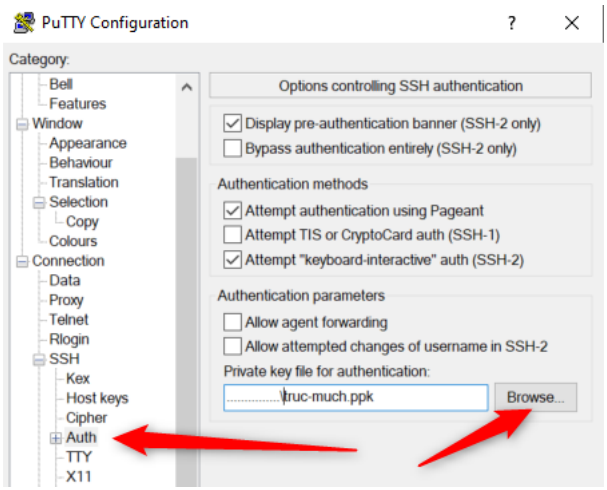


Le fichier .key peut être effacé, il ne vous sera plus d'aucune utilitée.



Dans puTTY, nous allons sauvegarder une session vers notre VM Kali Linux.

ATTENTION, TOUS LES PARAMETRAGES QUE NOUS ALLONS APPLIQUER DEVRONT ETRE SAUVEGARDER DANS LA CATEGORIE SESSION.



Essayez d'ouvrir votre connexion ssh via PuTYY
Si cela fonctionne, vous pouvez sécuriser votre configuration.