Menu interactif pour gestion simplifiée des serveurs Linux

1. Connexion SSH sécurisée entre l'host (W11) et le guest (Debian12)

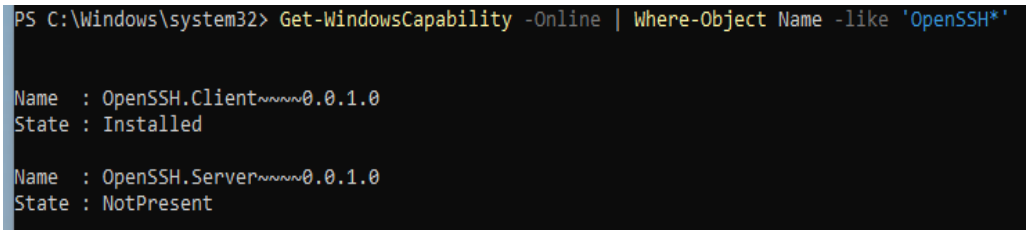
A- Sur l'host Windows 11(HOST), utilisez OpenSSH (intégré à Windows 10/11).

Pour installer **OpenSSH** avec PowerShell sur Windows 11, procédez comme suit :

1. Exécutez PowerShell en tant qu'administrateur.

2. Assurer vous qu'OpenSSH est disponible.

« Get-WindowsCapability -Online | Where-Object Name -like 'OpenSSH*' »



3. Ensuite, installez les composants selon vos besoins.

Install the OpenSSH Client
« Add-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0 »
Install the OpenSSH Server
« Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0 »

4. Générez la paire de clés **SSH** avec une longueur de **4096 bits** en exécutant :

« ssh-keygen -b 4096»

5. Lorsque vous êtes invité à **"Enter file in which to save the key"**, appuyez sur Entrée pour accepter l'emplacement par défaut (~/.ssh/id_rsa

6. Entrez une passphrase sécurisée lorsque vous y êtes invité. Cette passphrase protégera votre clé privée. Choisissez une passphrase robuste, longue et unique.
7. Une fois la génération de clés terminée, le fichier **id_rsa.pub** contient votre clé publique. Uploadez ce fichier sur un service de partage sécurisé comme un serveur SFTP ou un service de stockage cloud chiffré.

Quelques notes supplémentaires

- Protéger la clé privée (id_rsa) et ne jamais la partager.
- Utiliser un gestionnaire de mots de passe pour stocker la passphrase de manière sécurisée.
- Utiliser un service de partage sécurisé et chiffré, et supprimé après l'avoir téléchargé sur le serveur.

B- Sur le guest Debian 12(GUEST)

1. Mettez à jour les paquets et installez le serveur OpenSSH :

« sudo apt update »
« sudo apt install openssh-server »

2. Vérifiez le statut du service SSH :

« sudo systemctl status ssh »

3. Si le service n'est pas démarré, démarrez-le et activez-le pour qu'il démarre automatiquement au redémarrage :

« sudo systemctl start ssh »

« sudo systemctl enable ssh »

4. Créez un nouvel utilisateur non-root avec des privilèges sudo (remplacez 'votreprenom' par votre prénom) :

« sudo adduser votreprenomdm »

« sudo usermod -aG sudo votreprenomdm »

5. Connectez-vous avec le nouvel utilisateur :

« su – votreprenomdm »

6. Installez **wget** pour télécharger le fichier de clé publique partagé :

« sudo apt install wget »

7. Téléchargez le fichier de clé publique partagé (remplacez <URL_DU_FICHIER_PARTAGE> par l'URL réelle) :

« wget <URL_DU_FICHIER_PARTAGE> »

8. Créez le répertoire **.ssh** et définissez les permissions appropriées :

«mkdir ~/.ssh chmod 700 ~/.ssh »

9. Ajoutez la clé publique au fichier **authorized_keys** et définissez les bonnes permissions :

« cat id_rsa.pub >> ~/.ssh/authorized_keys »

« chmod 600 ~/.ssh/authorized_keys »

10. Modifiez le fichier de configuration **/etc/ssh/sshd_config** :

« sudo nano /etc/ssh/sshd_config »

11. Décommentez la ligne **PubkeyAuthentication yes** et remplacez #**AuthorizedKeysFile** par **AuthorizedKeysFile .ssh/authorized_keys**.

12. Désactivez l'authentification root pour plus de sécurité en ajoutant **PermitRootLogin no.**

```
PubkeyAuthentication yes
PermitRootLogin no

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile.ssh/authorized_keys
```

13. Redémarrez le service **SSH** pour prendre en compte les modifications :

« sudo systemctl restart sshd »

C- Connectez-vous depuis Windows (Host)

1. Trouvez l'adresse IP du guest avec

« ip addr show »

2. Sur PowerShell Windows,

« ssh root@ip_guest »

Assurez-vous d'utiliser un service de partage sécurisé et de supprimer le fichier partagé après l'avoir téléchargé sur le serveur

2. Envoie du script et du fichier HTML sur le serveur Debian12

A- Transférer les fichiers sur le serveur Debian

1. Ouvrez PowerShell sur votre machine Windows 11.

2. Naviguez jusqu'au répertoire où se trouve le fichier **menu_à_finir.sh** en utilisant la commande

« cd C:\Users\VotreUtilisateur\Documents) »

3. Une fois dans le bon répertoire, utilisez la commande **scp** pour copier les fichiers via SSH vers le serveur Debian 12

« scp menu_à_finir.sh votreprenomdm@adresse_ip_debian12:/home/votreprenomdm/ »

« scp index.html votreprenomdm@adresse_ip_debian12:/home/votreprenomdm/ »

B- Lancer le script

1. Lancer le script avec la commande

« ./menu_a_finir.sh »

Si vous rencontrez le message d'erreur **"$'\r' : commande introuvable"** cela indique que le script contient des caractères de retour chariot, qui peuvent provenir de sa création ou de son édition sur un système d'exploitation différent.

Pour résoudre ce problème, vous pouvez utiliser l'outil `dos2unix` pour convertir le format de fin de ligne du script de DOS/Windows (`\r\n`) en format UNIX (`\n`).

« sudo apt-get update »

« sudo apt-get install dos2unix »

« dos2unix menu_à_finir.sh »

Après cela, vous devriez être en mesure d'exécuter le script sans rencontrer d'erreurs liées aux caractères de retour chariot.

3. Mise à jour du automatique du site

1. Accédez à l'IP **192.168.145.128** pour vérifier le site actuel.
2. Modifiez le fichier **index.html** sur votre machine Windows 11.

3. Transférez le nouveau **index.html** sur le serveur Debian avec :

« scp index.html votreprenomdm@adresse_ip_debian12:/home/votreprenomdm/ »

4. Relancez le script avec **./menu_à_finir.sh** et choisissez l'option :

« "**7. Mise à jour du site**". »

5. Si vous obtenez un problème de droits, exécutez

« sudo chown -R votreprenomdm:votreprenomdm /var/www/html»

pour donner les droits à votre utilisateur sur le répertoire web.

6. Relancez l'option "**7. Mise à jour du site**" du script

7. Vérifiez que le site a été mis à jour en rafraîchissant **192.168.145.128**.