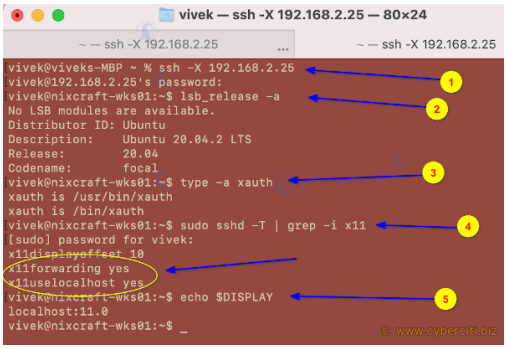
Utilisation de Wireshark dans un serveur distant



Utiliser Wireshark avec le transfert X11 via SSH (`ssh -X`) permet d'exécuter l'interface graphique de Wireshark sur un serveur distant et de l'afficher localement sur votre machine. Voici comment configurer et utiliser cette méthode dans une architecture LAMP.

Étapes

1. Pré-requis

1. **Wireshark** installé sur le serveur distant.
2. **X11 forwarding** activé sur votre serveur SSH.
3. **SSH** configuré pour permettre le transfert X11.
4. Un client X11 (comme XQuartz sur macOS ou Xming sur Windows) installé sur votre machine locale.

2. Configuration du serveur SSH pour le transfert X11

Assurez-vous que le transfert X11 est activé dans la configuration SSH du serveur distant. Modifiez le fichier de configuration `/etc/ssh/sshd_config` et assurez-vous que les lignes suivantes sont présentes et non commentées :

```
X11Forwarding yes
X11DisplayOffset 10
X11UseLocalhost yes
```

Après avoir modifié ce fichier, redémarrez le service SSH pour appliquer les modifications :

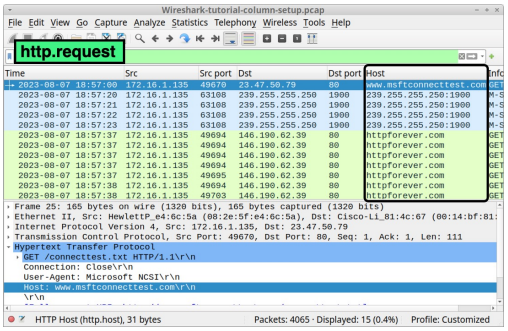
```
sudo systemctl restart ssh
```

3. Connexion au serveur avec transfert X11

Depuis votre machine locale, connectez-vous au serveur distant en utilisant l'option `-X` (ou `-Y` pour un transfert plus sécurisé mais moins strict) :

```
ssh -X user@remote_server
```

4. Lancer Wireshark sur le serveur distant



Une fois connecté au serveur distant via SSH avec X11 forwarding, lancez Wireshark en utilisant la ligne de commande :

```
sudo wireshark &
```

Cette commande ouvrira l'interface graphique de Wireshark sur votre machine locale tout en exécutant le programme sur le serveur distant.

Remarques

1. **Performances** : Le transfert X11 peut être lent, surtout pour les applications graphiques lourdes comme Wireshark. Utilisez cette méthode principalement pour des analyses légères ou lorsque l'accès direct n'est pas possible.
2. **Sécurité** : Utilisez des connexions SSH sécurisées et assurez-vous que le transfert X11 est correctement configuré pour éviter les problèmes de sécurité.

Capture de paquets avec Wireshark

Avec Wireshark lancé sur le serveur distant et affiché sur votre machine locale, vous pouvez maintenant sélectionner l'interface réseau appropriée et commencer la capture de paquets. Voici comment procéder :

1. **Sélectionnez l'interface réseau** sur laquelle vous souhaitez capturer le trafic (par exemple, `eth0`).
2. **Cliquez sur "Start"** pour démarrer la capture.
3. Utilisez les filtres de Wireshark pour affiner les résultats et analyser les paquets d'intérêt.

Alternatives

Si le transfert X11 est trop lent ou pose des problèmes, voici deux alternatives :

Utiliser `tcpdump` pour capturer les paquets et analyser localement

1. **Capturer les paquets avec `tcpdump`** sur le serveur distant et les sauvegarder dans un fichier :

   ```
   sudo tcpdump -i eth0 -w /tmp/capture.pcap
   ```

2. **Transférer le fichier de capture vers votre machine locale** :

   ```
   scp user@remote_server:/tmp/capture.pcap
    /local/path/
   ```

3. **Ouvrir le fichier de capture dans Wireshark** pour analyse :

   ```
   wireshark /local/path/capture.pcap
   ```

Utiliser `wireshark-qt` ou `tshark`

Si vous préférez utiliser une interface en ligne de commande :

1. **Installez `tshark`** sur le serveur distant :

   ```
   sudo apt-get install tshark
   ```

2. **Capturez les paquets avec `tshark`** et sauvegardez-les dans un fichier :

   ```
   sudo tshark -i eth0 -w /tmp/capture.pcap
   ```

3. **Transférez le fichier de capture vers votre machine locale** et analysez-le avec Wireshark.

Conclusion

Ces méthodes vous permettent de capturer et analyser le trafic réseau sur un serveur distant dans une architecture LAMP, en utilisant Wireshark efficacement et de manière sécurisée.