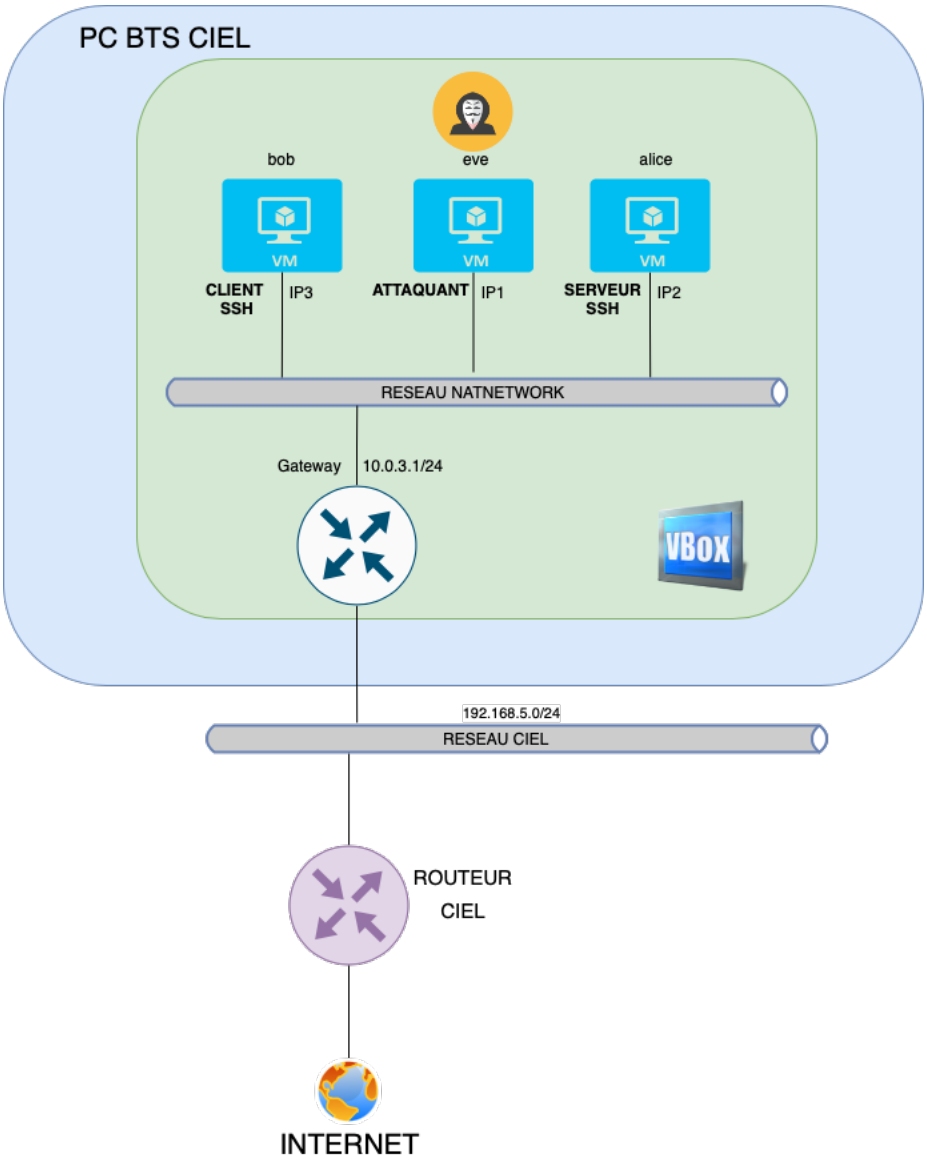
ATTAQUE MAN-IN-THE-MIDDLE SSH



1. Création d'une machine virtuelle depuis une image iso :

1.1 Créer une machine virtuelle Debian référence pour le TP avec l'image iso : https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/debian-12.5.0-amd64-netinst.iso

- On nommera cette machine ssh avec un mot de passe ssh
- Avec :
  - 4Go de RAM.
  - 2 coeurs de CPU.
  - Un stockage de 50Go.

- Créer un réseau nat que l'on appellera natSsh avec l'adresse IP réseau 10.0.3.0/24

2. Installation d'utilitaires :

2.1 Installer les utilitaires openssh-server et wireshark sur cette machine virtuelle référence.

3. Création de deux machines virtuelles clone:

3.1 Création de la machine virtuelle alice.

- Créez un clone de la machine référence.
- Sur cette machine, créez un utilisateur alice avec le mot de passe alice.
- Donnez tous les droits à alice.
- Relevez l'adresse IP de la machine alice.
- Supprimez l'utilisateur ssh.
- Supprimez le dossier ssh.
- Rebootez la machine et connectez-vous avec l'utilisateur alice.

3.2 Création de la machine virtuelle bob.

- Créez un deuxième clone de la machine référence.
- Sur cette machine, créez un utilisateur bob avec le mot de passe bob.
- Donnez tous les droits à alice.
- Relevez l'adresse IP de la machine alice.
- Supprimez l'utilisateur ssh.
- Supprimez le dossier ssh.
- Rebootez la machine et connectez-vous avec l'utilisateur bob.

4. Test de la connexion ssh:

4.1 Testez la connexion ssh du client (bob) sur le serveur (alice).

4.2 Lancez Wireshark avec un filtre ssh et analysez le protocole de connexion.

5. Préparation de la machine virtuelle attaquante eve :

Sur la machine virtuelle de référence créée au départ :

- Créez un utilisateur eve avec le mot de passe eve
- Donnez tous les droits à eve
- Supprimez l'utilisateur ssh
- Supprimez le dossier ssh
- Relevez l'adresse IP de eve.

6. Attaque ssh-mitm:

6.1 Réalisez l'attaque man-in-the-middle pour récupérer les identifiants/motdepasse permettant la connexion sur le serveur ssh alice. (vous vous aiderez du document ressource : http://newtonformationsnir.fr/TP/SSH)